REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE

MINISTERE DE L'ENSEIGNEMENT SUPERIEUR ET DE LA RECHERCHE SCIENTIFIQUE

UNIVERSITE YAHIA FARES DE MEDEA



Faculté de **T**echnologie

Mémoire de fin d'études de Master

Filière : Télécommunications.
Spécialité : Systèmes des télécommunications.

Conception d'un cahier des charges téchnique de réseau intranet Pour le nouveau pôle d'ouezra

---

Présenté par :

Mr. Bellarbi Ali

Mr. Bedda Ahmed El Amine

Proposé et Dirigé par :

Mr. Benaissa Khireddine

Promotion 2020

Remerciment

Au terme de ce travail, nous tenons tout d'abord à remercier ALLAH. Le tout-puissant de nous avoir donné le courage et la volonté pour

L'aboutissement de ce modeste travail.

Nous adressons nos remerciements à notre respectable encadreur Mr. Benaissa Khireddine qui a accepté d'encadrer notre travail en nous fournissant ses précieux conseils et encouragements ainsi que sa confiance et disponibilité.

Nos vifs remerciements vont également aux membres du jury pour l'intérêt qu'ils ont porté à notre recherche en acceptant d'examiner notre travail et de l'enrichir par leurs propositions.

Nous tenons à exprimer nos sincères remerciements à toutes les professeures et tous les professeurs qui nous ont enseigné et qui par leurs compétences nous ont soutenu dans la poursuite de nos études.

Enfin, nous tenons également à remercier nos amis qui ont participé de près ou de loin à la réalisation de ce travail.

Dédicaces

الحمد لله

Je dédie ce travail à **mon père** un héro dans ma vie et à **ma mère** mon ange. Qui m'ont soutenu durant toute ma vie, et qui m'ont donné la volonté d'arriver jusque-là. Je pense que je ne serai arrivé à ce stade que grâce aux

Encouragements ET aides apportés.

À mes frères **Saleh**, **Mohamed** et **Fouad.**

À mes sœurs **Samia, Amel et Hayet.**

À toute la famille **Bellarbi.**

À toute mes amis spécialement **Noufel (rabi yerhmou) et Badro, Amine, Hasni, Habib, Khaled et Ami Rachid** qui m'ont toujours poussé à faire de mon mieux.

À mon binôme **Ahmed Bedda** et sa famille. **Hamza** et **nour** bien sûr pour leur soutient .

À mon promoteur **Benaissa khire Eddine**.

Que toute personne m'ayant aidé de près ou de loin, trouve ici l'expression de ma reconnaissance.

#Akilo

Je dédie ce mémoire à…

Mon père et ma mère. qui ont attendu, et espérer ma réussite, ont toujours veillé sur moi avec beaucoup d'amour et de patience.

Mon frère Oussama et mes Sœurs Djihad, Roumaissa, Ikhlasse et Noussaiba. Présents dans tous mes moments de difficulté par leurs soutien et conseils. Vous vous êtes dépensés pour moi sans compter.

Mes grands parrents. Qui ont de près ou de loin contribué à ma formation. Affectueuse reconnaissance.

Hamza, Nour, mon équipe de Victoria ainsi que tous mes amis Qui m'ont encouragé en ce projet.

Et évidemment mon coéquipier Ali En témoignage de l'amitié qui nous uni et des souvenirs de tous les moments que nous avons passé ensemble.

Bedda Ahmed

ملخص

في الوقت الحاضر، يعد تنظيم الشبكات المحلية أمرا ضروريا، ويتطلب دراسة جيدة فيما يتعلق بتجزئتها من اجل تسهيل الاتصال بين الشبكات الفرعية المختلفة. الهدف من هذا المشروع هو بناء مواصفات تقنية لشبكة محلية للجامعة (شبكة الحرم الجامعي)، من خلال توفير ربط جيد بين مختلف الشبكات الافتراضية وكذلك التوافر العالي (10 جيجابايت) لتسهيل التواصل بين الشبكات المحلية المختلفة. في الممارسة العملية، يتم تقسيم الشبكات بواسطة الشبكات الافتراضية من خلال اعتماد استراتيجية الشبكات الافتراضية الوظيفية لتجميع المستخدمين. لقد ذكرنا أيضا البروتوكولات لمختلفة اللازمة للتشغيل الجيد للشبكة بالإضافة الى استراتيجية الحماية على مستوى هاته الأخيرة.

كلمات مفتاحية: شبكة مؤسسة، شبكة محلية، شبكة افتراضية، حماية، بروتوكول

Résumé

De nos jours, l'organisation des réseaux locaux est primordiale, elle nécessite une bonne étude concernant sa segmentation afin de faciliter la communication entre les différents sous réseaux. L'objectif de ce projet est la construction de cahier de charge d'un réseau technique local d'une université (réseau de campus), en proposant une bonne interconnexion entre les différents VLANs ainsi qu'une haute disponibilité (10 Go) pour faciliter la communication entre les différents réseaux locaux. En pratique, les LANs sont segmentés par des VLANs en adoptant la stratégie de VLAN fonctionnelle pour regrouper les utilisateurs. Nous avons en plus mentionné les différents Protocol nécessaire pour le bien marche de réseau ainsi que la stratégie de sécurité au niveau de ce dernier

Mots clés : Réseau de campus, Réseau locaux, VLAN, sécurité, Protocol.

Abstract

Today, the organization of local networks is paramount; it requires a good study on its segmentation to facilitate communication between different subnets. The objective of this project is setting up a technical conditions book for a local network of university (campus network), offering a good interconnection between different VLANs and a high availability (10 Go) to facilitate communication between different LANs. In practice, the LANs are segmented by VLANs in VLAN adopting the functional strategy to group users. We have also mentioned the different protocols necessary for the proper functioning of the network as well as the security strategy at the level of this later

Keywords: Campus network, Local network, VLANs, Security, Protocols.

sommaire

LISTE DES FIGURES I
LISTES DES TABLEAUX II
LISTES DES ACRONYMES III
Introduction générale 1
CHAPITRE I : Généralités sur les réseaux informatiques 2
I.1.Introduction 3
I.2.Définitions 3
I.2.1.Réseau informatique 3
I.2.2.Internet 3
I.2.3.Intranet 3
I.3.Objectif d'utilisations d'un réseau informatique 4
I.4.Classification des réseaux 4
I.4.1.Classification selon l'étendue géographique 4
I.4.1.1.Les réseaux personnels (PAN) 4
I.4.1.2.Les réseaux locaux (LAN) 5
I.4.1.3.Les réseaux métropolitains (MAN) 5
I.4.1.4.Les réseaux étendues (WAN) 5
I.4.2.Classification selon l'architecture 5
I.4.2.1.Le réseau poste à poste (Peer to Peer) 5
I.4.2.2.Le réseau client serveur 6
I.5.Topologies des réseaux 7
I.5.1.Topologie en bus 7
I.5.2.Topologie en étoile 8
I.5.3.Topologie en étoile étendue 8
I.5.4.Topologie en anneau 9
I.5.5.Topologie maillé 9
I.6.Les supports de transmission 9
I.6.1.Avec fil 10
I.6.2.Sans fil 11
I.7.Les équipements d'interconnexions réseau : 12
I.8.Architecture des réseaux 15
I.8.1.L'architecture OSI 15
I.8.2.L'architecture TCP/IP 16
I.9.Les Protocoles de réseau 17

I.9.1.TCP/IP (Transmission Control Protocol / Internet Protocol).....17
I.9.2.Le protocole IPX (Inter Packet exchange).....18
I.9.3.Le Protocol NetBeui.....19
I.10.Conclusion 19
CHAPITRE 2: Etude de l'existant et construction du cahier des charges 20
II.1.Partie 01 : Description de champs de l'étude 21
II.1.1.Introduction.....21
II.1.2.Présentation de pôle universitaire d'ouzera.....21
II.1.2.1.Présentation de la ville d'ouzera 21
III.1.2.1.1.Situation et délimitation de la ville.....21
II.1.3.Le Campus d'ouzera.....22
II.1.3.1.Le projet du campus universitaire 22
II.1.3.2.Organigramme du pole d'Ouzera.....22
II.1.4.Architecture de pôle universitaire d'ouzera.....23
II.1.5.Les Prises informatiques.....24
II.1.5.1.La faculté des sciences 25
II.1.5.2.La faculté de sciences humaines et sociales.....26
II.1.5.3.La faculté de sport.....27
II.2.Partie 02 :Conception technique.....30
II.2.1.Description du projet 30
II.2.2.Partie génie civil 30
II.2.2.1.Caniveau de câblage.....30
II.2.3.Modèle de réseau 31
II.2.3.1.Modèle de conception hiérarchique à trois couches.....31
II.2.3.1.1.La couche d'accès (Access Layer).....31
II.2.3.1.2.La couche de distribution (Distribution Layer) 32
II.2.3.1.3.La couche cœur de réseau (Core Layer) 32
II.2.3.1.4.Avantage d'un réseau hiérarchique.....32
II.2.3.1.5.Principes du modèle d'un réseau hiérarchique 33
II.2.4.Solutions proposées 33
II.2.4.1.Solution globale 33
II.2.4.2.Differentes solutions proposées.....34
II.2.4.2.1.Solution normalisé.....34
Le Cout de cette proposition : 36
II.2.4.2.2.Solution basique 40

Le Cout de cette proposition : 42
II.2.4.2.3.Notre proposition (la solution optimisée) 45
Le cout de la solution proposée : 48
II.2.4.3.Comparaison entre les différentes propositions 51
II.2.5.Construction de cahier de charge 52
II.2.5.1.Description de la partie passive 52
II.2.5.1.1.Classes d'application et Bandes Passantes 52
II.2.5.1.1.1.Classes d'applications : 52
II.2.5.1.1.2.Câblage 52
II.2.5.1.1.3.Protocoles réseau 54
II.2.5.1.2.Les éléments Passifs 54
II.2.5.1.2.1.Topologie physique 54
II.2.5.1.2.2.Armoire de brassage 54
II.2.5.1.2.3.Eléments de brassage 54
II.2.5.1.2.4.Les Connecteurs RJ 55
II.2.5.1.2.5.Canalisation Des Bureaux 56
II.2.5.1.2.6.Canalisation Faux Plafonds 56
II.2.5.2.Description de la partie active 56
II.2.5.2.1.Description technique du Switch Fédérateur 56
II.2.5.2.2.Description technique du Switch de distribution 57
II.2.5.2.3.Description technique du Switch d'accès : 59
II.2.5.2.4.Description technique de la Firwall 60
II.2.5.2.5.Description technique du serveur 61
II.2.5.2.6.Description du Switch 24 ports Gigabit smart PoE 61
II.2.5.2.7.Description technique du Switch 48 ports Gigabit smart PoE 62
II.2.6.Conclusion 63
CHAPITRE 3: Architecture et sécurité des réseaux 64
III.1.Introduction 65
III.2.Les protocoles LAN 65
III.2.1.Les Virtual LAN,VLAN 65
III.2.1.1.Définition 65
III.2.1.2.Typologie de VLAN 65
III.2.1.2.1.VLAN de niveau 1 ou VLAN par port 65
III.2.1.2.2.VLAN de niveau 2 ou VLAN MAC 65
III.2.1.2.3.VLAN de niveau 3 ou VLAN d'adresses réseaux 66

III.2.2.Protocole VTP 66
III.2.2.1.Définition 66
III.2.2.2.Principe de fonctionnement 66
III.2.2.2.1.Mode serveur VTP 66
III.2.2.2.2.Mode client VTP 67
III.2.2.2.3.Mode transparent VTP 67
III.2.3.Trafic Entre-VLAN 67
III.2.4.Protocole STP (Spanning Tree Protocol) 68
III.2.4.1.Problèmes 68
III.2.4.1.1.Tempête de broadcast 68
III.2.4.1.2.Réception multiple d'une trame 68
III.2.4.1.3.Instabilité de la table des adresses Mac 69
III.2.4.2.Solution spanning tree 69
III.2.4.3.Bridge Protocol Data Unit (BPDU) 69
III.2.4.4.Rôle des ports 69
III.2.4.5.Types de protocoles STP 70
III.2.4.5.1.Le protocole Pvst+ 70
III.2.4.5.2.Le protocol Rapid PVST+ 72
III.2.5.Le protocole Etherchannel 73
III.2.6.Le protocole ARP 74
III.2.7.Le protocole ICMP 74
III.2.8.L'adressage 74
III.2.8.1.L'adressage dynamique 74
III.2.8.1.1.Protocole DHCP 74
III.2.8.1.2.Avantage DHCP 75
III.2.8.2.L'adressage statique 75
III.2.8.2.1. La technique VLSM 75
III.2.8.3.Notre plan d'adressage 77
III.3.Attaques et moyens de sécurité réseau 79
III.3.1.Quelques types d'attaques 79
III.3.1.1.Attaque sur le réseau 79
III.3.1.2.Attaque sur le mot de passe 80
III.3.2.La politique de Sécurité réseau 80
III.3.2.1.Principe d'une politique de sécurité réseau 80
III.3.3.Securité niveau 2 81

III.3.3.1.Port security 81
III.3.3.2.AAA et 802.1x 83
III.3.3.3.Private Vlan 84
III.3.3.4.DHCP Snooping 85
III.3.3.5.Spanning tree 86
III.3.3.6.VACL 87
III.3.4.Solution Firewall 88
III.3.4.1.Firewall à filtrage de paquets 88
III.3.4.1.1.Firewall State full Inspection 88
III.3.4.2.Firewall Applicatif 88
III.4..Réseau sans fils (solution wifi) 89
III.4.1.Definition 89
III.4.2.Reseau sans fil wlan 90
III.4.3.Architecture réseau WIFI 90
A.Le mode Infrastructure 90
B.Le mode Ad-Hoc 91
III.4.3.La norme (802.11) 92
III.4.3.1.Les équipements de transmission : 94
III.4.3.2.Les modes d'interconnexion 96
A.Access Point (AP) : 96
B.Wireless Bridge : 96
C.Multi point Bridge 96
D. Wireless Client: 97
III.5. Conclusion 97
Conclusion Générale 99
BIBLIOGRAPHIE 101
Annexe
Annexe A1 faculté de sciences
Annexe A2 faculté de sciences humaines
Annexe A3 faculté de sport
Annexe B Les normes wifi

LISTE DES FIGURES

FIGURE I.1 *TYPES DE RESEAUX SELON L'ETENDUE GEOGRAPHIQUE* 4
FIGURE I.2 *ARCHITECTRE POSTE A POSTE* 5
FIGURE I.3 *ARCHITECTURE CLIENT SERVEUR* 6
FIGURE I.4 *TOPOLOGIE DE RESEAU EN BUS* 8
FIGURE I.5 *TOPOLOGIE DE RESEAU EN ETOILE* 8
FIGURE I.6 *TOPOLOGIE DE RESEAU EN ETOILE ETENDUE* 8
FIGURE I.7 *TOPOLOGIE DE RESEAU EN ANNEAU* 9
FIGURE I.8 *TOPOLOGIE MAILLE* 9
FIGURE I.9 *SCHEMA D'UN CABLE COAXIAL* 10
FIGURE I.10 *CABLE COAXIAL* 10
FIGURE I.11 *UNE PAIRE TORSADEE* 10
FIGURE I.12 *FIBRE OPTIQUE* 11
FIGURE I.13 *CARTE RESEAU* 13
FIGURE I.14 *FONCTIONEMENT D'UN REPETEURS* 13
FIGURE I.15 *UN CONCENTRATEURS (HUB)* 13
FIGURE I.16 *FONCTIONNEMENT D'UN PONT* 13
FIGURE I.17 *UN SWITCH* 14
FIGURE I.18 *FONCTIONNEMENT D'UN PAR-FEU* 15
FIGURE I.19 *LE MODELE OSI* 17
FIGURE I.19 *LE MODELE TCP/IP* 17
FIGURE I.21 *LE PROTOCOL DNS* 18

FIGURE II.1 *SITUATION D'OUZERA DANS LA WILLAYA DE MEDEA* 21
FIGURE II.2 *ORGANIGRAMME DU POLE D'OUEZRA* 22
FIGURE II.3 *SCHÉMA DU SITE GLOBAL* 23
FIGURE II.4 *L'INFRASTRUCTURE INTERIEUR* 30
FIGURE II.5 *SCHÉMA GENERAL DU CANIVEAU* 31
FIGURE II.6 *MODÈLE DU RÉSEAU HIÈRARCHIQUE* 31
FIGURE II.7 *MODÈLE HIRÈRARCHIQUE À TROIS COUCHES* 32
FIGURE II.8 *ARCHITECTURE DU RÉSEAU SOLUTION NORMALISÉ* 34
FIGURE II.9 *ARCHITECTURE DU RÉSEAU SOLUTION BASIQUE* 40
FIGURE II.10 *SCHÉMA GENERAL DE CARNIVEAU DE FIBRE* 46
FIGURE II.11 *SCHÉMA DE LA LIAISON FIBRE OPTIQUE ENTRE LES DÉPARTEMENT* 46
FIGURE II.12 *ARCHITECHTURE DU RESEAU DE LA SOLUTION proposé* 47
FIGURE III.1 *DIFFÉRENTS CHAMINS* 68
FIGURE III.2 *TOMPETE DE BROADCAST* 68
FIGURE III.3 *RÉSEAU AVEC STP* 69
FIGURE III.4 *GESION DES PORTS PAR LE PROTOCOL STP* 70

FIGURE III.5 *LE PROTOVOLE PVST+* 71
FIGURE III.6 *LE PROTOCOL RAPID PVST+* 72
FIGURE III.7 *LE PROTOCLE ETHERCHANNEL* 74
FIGURE III.8 *SYSTÈME D'ADRESSAGE DE 4 RÉSEAUX* 76
FIGURE III.9 *FONCTIONNEMENT DE EPA* 83
FIGURE III.10 *PRIVATE VLAN* 85
FIGURE III.11 *LES BPDU GUARD ET ROOT GUARD DANS LE SPANNING TREE* 87
FIGURE III.12 *LES VACL* 88
FIGURE III.13 *LE MODE INFRASTRUCTURE* 91
FIGURE III.14*LE MODE AD_HOC* 92
FIGURE III.15 *UN RÉSEAU CABLE ASSOCIÉ À UN OINT D'ACCÉS* 95
FIGURE III.16 *UN RÉSEAU CABLE TRADITIONNEL* 95
FIGURE III.17 *POINT D'ACCÉS EN MODEM SANS FIL* 96
FIGURE III.18 *POINT D'ACCÉES EN MODE MULTI PONTS* 97

Liste des tableaux

TABLEAU II.1 *PLACES PEDAGOGIQUES ET BATIMENTS POUR CHAQUE DEPARTEMENT* 25
TABLEAU II.2 *NOMBRE DES PRISES POUR LA FACULTE DE SCIENCE* 26
TABLEAU II.3 *NOMBRE DES PRISES POUR LA FACULTE DE SOCIOLOGIE* 28
TABLEAU II.4 *NOMBRE DES PRISES POUR LA FACULTE DE SPORT* 29
TABLEAU II.5 *NOMBRE DE PRISES INFORMATIQUE* 30
TABLEAU II.6 *DÉTAILS DE L'ARCHITECTURE DU RÉSEAU SOLUTION NORMALISÉ* 36
TABLEAU II.7 *LE COUT DE LA SOLUTION NORMALISÉ* 37
TABLEAU II.8 *DÉTAIL DE L'ARCHITECTURE DE LA SOLUTION BASIQUE* 42
TABLEAU II.9 *LE COUT DE LA SOLUTION BASIQUE* 43
TABLEAU II.10 *ARCHITECTURE DE LA SOLUTION CHOISIE* 48
TABLEAU II.11 *TABLEAU DES COUTS DE LA SOLUTION CHOISIE* 49
TABLEAU II.12 *PRIX TOTALE POUR CHAQUE SOLUTION* 52
TABLEAU III.1 *LISTE DES VLAN* 79
TABLEAU III.2 *DÉBITS ET PORTÉ DE LA NORME 802.11* 98

Liste des abréviations

TCP : Transmission Control Protocol

IP : Internet Protocl

FTP : File Transfer Protocol

PAN : Personale Area Network

LAN : local Area Network

MAN : Métropolitain Area Network

WAN : Wide Area Network

MBPS : Megabits Per Second

PC : Personal Computer

PDA : Personal Digital Assistant

IRDA : Infrared Data Association

WIFI : Wireless Fidelity

OSI : Open Système Interconnexion

TELNET : terminal network ou telecommunication network, ou encore teletype network

TFTP : Trivial File Transfer Protocol

HTTP : HyperText Transfert Protocol

IRC : Internet Relay Chat

NTP : Network Time Protol

P2P : Peer To Peer

NNTP : Network News Transfert Protocol

SSH : Secure Shell

SMTP : Simple Mail Trasfert Protocol

DNS : Domain Name Server

POP3 : Poste Office Protocol 3

IPX : Inter Packet exchange

VLAN : Virtual Local Area Network

MAC : Media Access Control

VTP : Vlan Trunking Protocol

NVRAM : Non-Volatile Random-Access Memory

IEEE: Institute of Electrical and Electronics Engineers

SW : Switch

DIST : Distrubution

STP : Spanning Tree Protocol

DEC : Digital Equipment Corporation

BPDU : Bridge Protocol Data Unit

BID : Bridge Identity Document

ID : Identity Document

CST : Common Spanning Tree

PVST : Per Vlan Spanning Tree

RSTP : Rapid Spannig Tree

LACP : Link Aggregation Control Protocol

PAGP : Port Aggregation Protocol

ARP : Adress Resolution Protocol

ICMP : Internet Control Message Protocol

DHCP : Dynamic Host Configuration Protocol

SNMP: Simple Network Management Protocol

MDP : Mot De Passe

WPA: Simple Network Management Protocol

EAP : Extensible Authentification Protocol.

DMZ : Demilitarized Zone

PVLAN : Per Virtual LAN

VACL : Vlan Access List

FR : Frame Realy

DTE : Data Terminal Equipment

DCE : Distributed Computing Environment

DLCI : Data Link Connection Identifiers

ATM : Automated Teller Machine

MPLS : Multiprotocol Label Switching

TDM : Time Division Multiplexing

USB : Universal Serial Bus

DSSS : Direct Sequence Spread Spectrum

FHSS : Frequency Hopping Spread Spectrum

PCMCIA : Personal Computer Memory Card International Association

OFDMA : Orthogonal Frequency-Division Multiple Access

AP : Access Point

SFP : Small form-Factor Pluggable

IS-IS : Intermediate System to Intermediate System

RIP : Routing Information Protocol

IGMP : Internet Group Management Protocol

PBR : Policy-Based Routing

RIPNG : Routing Information Protocol Next Generation

MLD : Multicast Listener Discovery

QOS : Quality Of Service

ACL : Access Control List

RMON : Remote Network MONitoring

IPSEC : IP Security

VPN : Virtual Private Network

ECC : Error-Correcting Code

SDDC : Software-Defined Data Center

SAS : Serial Attached SCSI

SSD : Solid-State Drive

SD : Sales and Distribution

POE : Power Over Ethernet

MDI : Medium Dependent Interface

UTP : Unshielded Twisted Pair

DSCP : Differentiated Services Code Point

COS : Class Of Service

SP : **S**trict Priority

WRR : Weighted Round Robin

Introduction générale



Introduction générale

Parmi les éléments essentiels à l'existence humaine, le besoin de communication arrive juste après le besoin de survie. Par conséquence, le partage de l'information est devenu l'un des domaines d'étude les plus importants.

Depuis l'antiquité, l'homme n'a jamais cessé de fournir des efforts afin de trouver des moyens ou des outils pour maintenir la communication dans sa vie quotidienne, et parmi ces outils, il existe l'ordinateur qui est une machine qui permet la manipulation des données.

D'un point de vue initial, l'idée de relier plusieurs ordinateurs entre eux a pris sa part d'étude et de recherche d'où est apparue la notion des réseaux informatiques.

Le réseau informatique est composé d'un ensemble d'équipements (ordinateurs, routeurs, Switch…), qui échangent des informations de multiples formes (texte, image, vidéo……) entre eux via un dispositif de communications.

Pour relier un réseau à un autre, il faudra utiliser un périphérique d'interconnexion de niveau trois du modèle OSI (routeur, passerelle…). Ces derniers consistent à choisir la manière de transmettre un paquet IP à travers les divers réseaux.

L'objectif principal de notre projet consiste justement à configurer et à mettre en place un réseau de campus universitaire, ainsi qu'à assurer l'échange des informations entre l'ensemble des équipements de ce dernier.

Notre rapport se subdivise en trois principaux chapitres :

Dans le premier chapitre on décrit d'une manière générale les réseaux informatiques les éléments indispensables qui contribuent à la réalisation de ce dernier.

Dans deuxième chapitre nous allons établir une description générale de campus universitaire d'ouezra ainsi que les différents équipements et les ressources informatique qui disposent la construction de cahier de charge de ce réseau universitaire.

Enfin, nous allons expliquer les concepts des VLANs et l'étude de quelques protocoles et nous allons proposer un plan d'adressage et une polytique de sécurité au niveau 2 ensuie la solution Firewall en plus de la solution WIFI.

Chapitre I

Généralités sur les réseaux informatiques



I.1. Introduction

L'histoire des réseaux et des télécommunications pourrait se résumer à une perpétuelle course au débit ou ce qu'on appelle aussi largeur de bande. Le principe du réseau local est apparu dans les années 70 pour interconnecter les équipements de mini-informatique (terminaux, imprimantes, disques, ...). En effet, la plupart des échanges de données dans une entreprise s'effectue localement, voir par groupes de travail. C'est pourquoi, avec la généralisation des micro-ordinateurs à la fin des années 80, le réseau local à affirmer sa vocation.

I.2. Définitions

I.2.1. Réseau informatique

Un réseau informatique est un ensemble d'élément matériel et logiciels relié entre eux dans le but de permettre aux utilisateurs de partager des ressources et d'échanger des informations sous forme numérique. Un réseau est constitué d'équipements appelées nœuds. En fonction de leur étendue et de leur domaine d'applications, ces réseaux sont catégorisés.

I.2.2. Internet

Internet est un réseau informatique mondial constitué d'un ensemble de réseaux nationaux, régionaux et privés. L'ensemble utilise un même protocole de communication : TCP/IP, (Transmission Control Protocol / Internet Protocol).

L'internet propose trois types de services fondamentaux :

- Le courrier électronique (e-mail) ;
- Le Web (les pages avec liens et contenus multimédia de ses sites Web) ;
- L'échange de fichiers par FTP (*File Transfer Protocol*).

Le réseau Internet sert également, et de plus en plus, aux communications téléphoniques et à la transmission de vidéos et d'audio en direct (ou streaming), c'est-à-dire à la manière d'un téléviseur ou d'un récepteur radio.

I.2.3. Intranet

Le terme intranet est utilisé pour désigner un réseau informatique qui est développé au sein d'une entreprise ou d'un organisme et réservé aux collaborateurs de celle-ci, qui fonctionne avec les mêmes composantes qu'internet.

Un intranet peut donc être constitué de plusieurs services et applications tels que l'utilisation de la messagerie électronique, mise en place de groupes de discussions, accès à des bases de données, publication des documents aux formats HTML, mise à disposition des fichiers ou encore des procédures de gestion (Administrative, comptable ou de production).

I.3. Objectif d'utilisations d'un réseau informatique

L'objectif premier des réseaux est la mise en commun de ressources, assurant notamment :

- Le partage de l'information. En informatique, celle-ci existe sous différentes formes : Fichiers ; documents ; données...
- La communication entre personnes grâce au courrier électroniques, la discussion en direct, ...
- La garantie de l'unicité de l'information lors d'une mise à jour de bases de données
- la mise en place d'outils de travail collaboratif.
- La communication entre processus.

I.4. Classification des réseaux

Un réseau est constituer d'équipements appelées nœuds, en fonction de leur étendue et de leur domaine d'applications, ces réseaux sont classifiés on distingue :

I.4.1. Classification selon l'étendue géographique

Selon l'étendue géographique, on peut distinguer quatre types de réseaux :

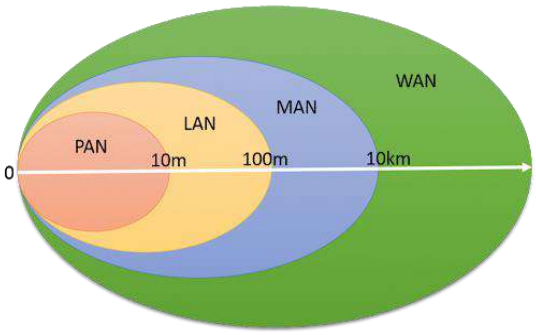


Figure I.1 Types de réseaux selon l'etendue géographique

I.4.1.1. réseaux personnels (PAN)

La plus petite étendue de réseau est nommée en anglais Personale Area Network (PAN), centrée sur l'utilisateur, elle désigne une interconnexion d'équipements Informatiques dans un

espace d'une dizaine de mètres de celui-ci. Il est appelé aussi réseau individuel ou réseau domestique. [1]

I.4.1.2. Les réseaux locaux (LAN)

De taille supérieure, s'étendant sur quelques dizaines à quelques centaines de mètres, le local Area Network (LAN) , en français réseau local d'entreprise est une infrastructure de communications reliant des équipements informatiques variés, sur une aire géographique limitée, dans le but de partager des ressources communes. [1]

I.4.1.3. Les réseaux métropolitains (MAN)

Un réseau métropolitain, ou Métropolitain Area Network (MAN), est également nommé réseau fédérateur .Il assure des communications sur des plus longues distances, interconnectant souvent plusieurs réseaux LAN

I.4.1.4. Les réseaux étendues (WAN)

Les réseaux étendus sont capables de transmettre les informations sur des milliers de kilomètres à travers le monde entier. Le WAN (Wide Area Network), le plus célèbre est le réseau public internet, dont le nom provient de cette qualité : Inter Networking ou interconnexion de réseaux. [1]

I.4.2. Classification selon l'architecture

On trouve:

I.4.2.1. Le réseau poste à poste (Peer to Peer)

Chaque poste connecté est à la fois serveur lorsqu'il met ses ressources (imprimantes, dossiers) à disposition des autres postes, et client lorsqu'il bénéficie des ressources des autres postes. Il n'existe pas de gestion centralisée des ressources du réseau. [2]

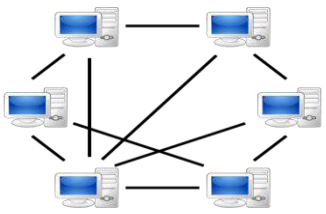


Figure I.2 Architecture poste à poste

Les réseaux poste à poste ne nécessitent pas les mêmes niveaux de performance et de sécurité que les logiciels réseaux pour serveurs dédiés.

Tous les systèmes d'exploitation intègrent toutes les fonctionnalités du réseau poste à poste.

I.4.2.2. Le réseau client serveur

Un ou plusieurs ordinateurs appelés serveur assurent des fonctions centralisées d'administration qui permettent d'authentifier des utilisateurs et de leurs accorder des permissions sur les ressources du réseau. Les serveurs peuvent être spécialisés : serveur de fichiers, d'application, d'impression, de communication. Ils offrent des services à des programmes clients (client de messagerie, de base de données antivirales, etc.…). [2]

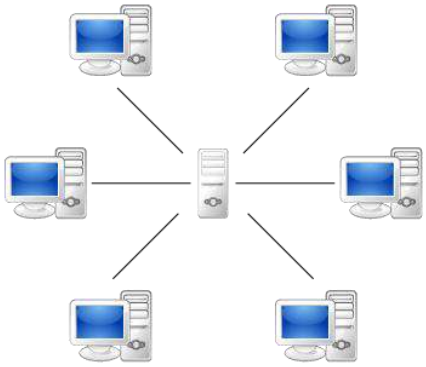


Figure I.3 Architecture client serveur

Les deux types de réseau présentent des avantages dont on peut citer :

- **Le modèle client/serveur**

Est particulièrement recommandé pour des réseaux nécessitant un grand niveau de fiabilité, ses principaux atouts sont :

- **Des ressources centralisées :** étant donné que le serveur est au centre du réseau, il peut gérer des ressources communes à tous les utilisateurs, comme par exemple une base de données centralisée, afin d'éviter les problèmes de redondance et de contradiction.
- **Une meilleure sécurité :** car le nombre de points d'entrée permettant l'accès aux données est moins important.
- **Une administration au niveau serveur :** les clients ayant peu d'importance dans ce modèle, ils ont moins besoin d'être administrés.
- **Un réseau évolutif :** grâce à cette architecture il est possible de supprimer ou rajouter des clients sans perturber le fonctionnement du réseau et sans modification majeure.

- **Le modèle Peer to Peer**

Il y'a :

- **un coût réduit :** pas de matériel évolué et donc cher, pas de frais d'administration.
- **une grande simplicité :** la gestion et la mise en place du réseau et des machines sont peu compliquées.

Note : l'administration d'un réseau ou de machines désigne la gestion des utilisateurs, la mise à disposition des ressources, la maintenance des applications et des données et l'installation et mise à niveau des logiciels utilisateurs.

Il existe un certain nombre d'inconvénients que l'entreprise doit connaître avant de faire son choix.

- L'architecture client/serveur a tout de même quelques lacunes parmi lesquelles :
  - Un coût élevé dû à la technicité du serveur.
  - Un maillon faible : le serveur est le seul maillon faible du réseau client/serveur, étant donné que tout le réseau est architecturé autour de lui ! Heureusement, le serveur a une grande tolérance aux pannes (notamment grâce au système RAID).
- Pour l'architecture poste à poste
  - Ce système n'est pas du tout centralisé, ce qui le rend très difficile à administrer.
  - La sécurité est moins facile à assurer, compte tenu des échanges transversaux
  - Aucun maillon du système ne peut être considéré comme fiable.

Ainsi, les réseaux égaux à égal sont préférentiellement utilisés pour des applications ne nécessitant pas un haut niveau de sécurité ni une disponibilité maximale (il est donc déconseillé pour un réseau professionnel avec des données sensibles).

I.5. Topologies des réseaux

La topologie réseau définit la structure du réseau, elle désigne la configuration du câblage ou du média (comment les machines sont reliées entre elles).

I.5.1. Topologie en bus

Repose sur un câblage sur lequel viennent se connecter des nœuds (postes de travail, équipements d'interconnections, périphériques…). Il s'agit d'un support multipoints .Le câble est l'unique élément matériel constituant le réseau et seul les nœuds génèrent le signal. [3]

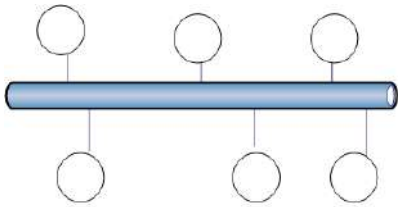


Figure I.4 Topologie de réseau en bus

I.5.2. Topologie en étoile

Cette topologie repose quant à elle, sur des matériels actifs ou chaque équipement est relié à un nœud central. Les performances d'un réseau en étoile dépendent principalement du nœud central ; ce type de réseau est relativement efficace et économique. La plupart de réseau locaux fonctionne sur ce principe ; en utilisant un Switch central reliant tous les ordinateurs au même nœud. [3]

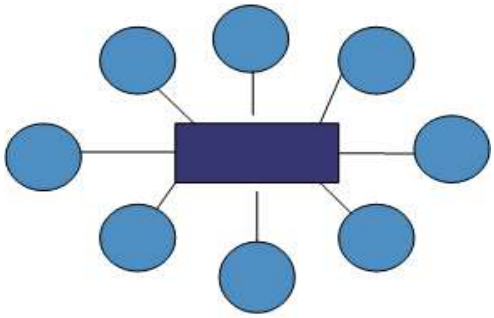


Figure I.5 Topologie de réseau en étoile

I.5.3. Topologie en étoile étendue

Ce réseau repose sur la topologie en étoile. Il relie les étoiles individuelles entre elles en reliant les nœuds centraux. [3]

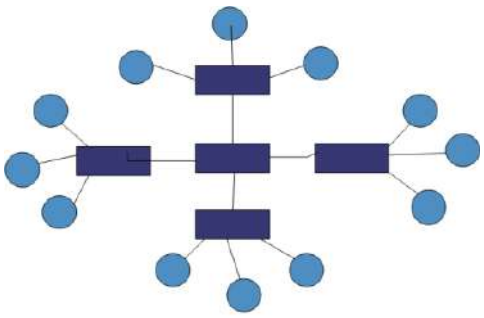


Figure I.6 Topologie de réseau en étoile étendue

I.5.4. Topologie en anneau

Dans ce type de topologie les ordinateurs sont placés en cercle sur un câble sans terminaison (en fait ils sont reliés par des câbles aller/retour à un concentrateur passif qui relie chaque ordinateur au suivant). Chaque Ordinateur joue le rôle de répéteur pour amplifier le signal et le faire repartir. La Méthode d'Accès à ce type de câblage est celle du passage de « jeton ». Pour pouvoir transmettre un ordinateur doit être en possession du jeton libre ce qui évite toute collision sur le réseau. [3]

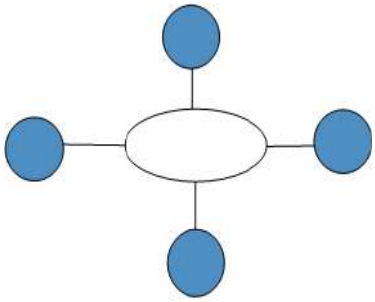


Figure I.7 Topologie de réseau en anneau

I.5.5. Topologie maillé

Un réseau maillé est caractérisé par le fait que 2 nœuds quelconques sont reliés l'un à l'autre, les nœuds forment un graphe complet. [3]

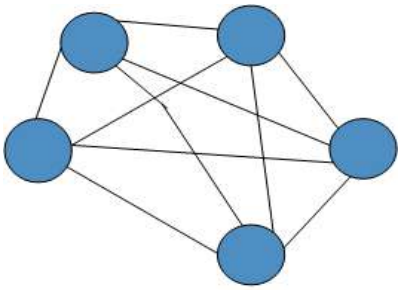


Figure I.8 Topologie maillé

I.6. Les supports de transmission

Un réseau suppose plusieurs équipements informatiques (ordinateurs fixes ou portables, divers équipements électroniques, téléphones, assistants numériques personnels…) situés à distance les uns des autres.

La première chose à mettre en œuvre pour constituer le réseau est la transmission des informations d'un équipement à un autre en utilisant des supports de transmission. C'est le support (généralement filaire, c'est-à-dire sous forme de câble, de plus en plus non filaire) qui

relie les ordinateurs entre eux. Les principaux supports physiques utilisés dans les réseaux locaux sont les suivants :

I.6.1. Avec fil

• Le câble coaxial supporte un débit de 10 Méga bits par seconde (10 Mips) ; il est constitué d'un conducteur central en cuivre, d'un isolant puis d'un deuxième conducteur se forme de métal tressé, assurant le blindage et en fin d'une gaine isolante assurant la protection mécanique de l'ensemble comme se figure au-dessus :

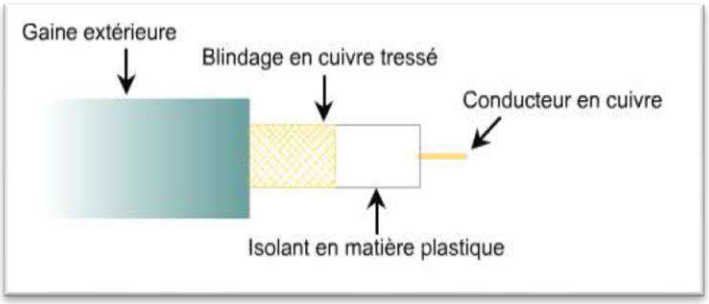


Figure I.9 Schéma d'un câble coaxial



Figure I.10 Schéma d'un câble coaxial

• La paire torsadée ressemble à un câble téléphonique. Suivant sa catégorie elle supporte de 10 à 100 Mbps sur 100 mètres.

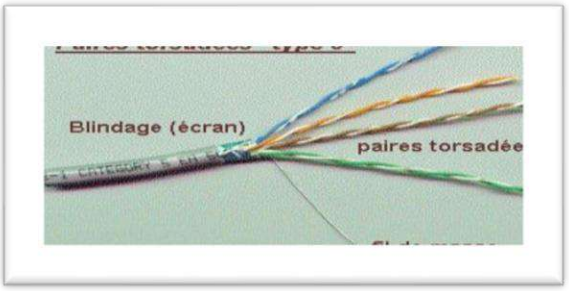


Figure I.11 Une paire torsadée

• La fibre optique maintient un débit de 155 Mbps à 10 Gbps Sur plusieurs kms. La fibre transfert les données se forme d'impulsions lumineuse modulée. Il existe deux types de fibre optique :

La multi mode : utilisées pour les trop grandes distances.

La monomode : utiliser en local pour la connexion des appareils réseau. [4]



Figure I.12 Fibre optique

I.6.2. Sans fil

a. **Infrarouge :** L 'IRDA, appelé infrarouge, est encore aujourd'hui une technologie de transmission sans fil très répandue (PC portable, PDA, téléphone portable, etc.). Le protocole IrDA est conçu pour le transfert des données, en utilisant la lumière infrarouge. Avec une connectivité rapide, sans installation. Faible coût. Sécurisation de transmission.

b. **Bluetooth :** La technologie Bluetooth est une technologie de réseaux sans fils d'une faible portée, de l'ordre de quelques dizaines mètres à un peu moins d'une centaine de mètres, permettant de relier des périphériques (imprimantes, téléphones portables, appareils domestiques, oreillettes sans fils, souris, clavier, etc.) et des ordinateurs et assistants personnels (PDA) entre-deux sans liaison filaire.

Il a comme Avantages : la faible consommation d'énergie, la bonne gestion de la communication de la voix, équipements de taille réduite. Technologie adaptée à la mobilité et un faible coût.

Inconvénients : Nombre de périphériques limité dans un réseau Faible porté et un débit limité.

c. **Wifi :** Le Wifi, pour Wireless Fidelity, est une technologie standard d'accès sans fil à des réseaux locaux. Le principe est d'établir des liaisons radio rapides entre des

équipements et des bornes reliées aux réseaux Haut Débit. Grâce au Wifi, il est possible de créer des réseaux locaux sans fils à haut débit.

Le Wifi possède deux modes de fonctionnement : Le mode infrastructure auquel se connectent toutes les stations (appareils équipés d'un équipement Wifi) à un point d'accès ou un routeur, et le mode ad-hoc où les stations se connectent les unes aux autres sans passer par un point d'accès.

d. Wi max : le Wi max est un standard de transmission sans fil à haut débit. Fonctionnant à 70 Mbit/s, il est prévu pour connecter les points d'accès Wifi à un réseau de fibres optiques, ou pour relayer une connexion partagée à haut débit vers de multiples utilisateurs.

Cette technologie apparue en France en décembre 2003 menace sur le papier le Wifi grâce à des débits théoriques sept fois supérieurs et une couverture qui s'étend jusqu'à 50 kilomètres là où les bornes Wifi se limitent à quelques centaines de mètres.

I.7. Les équipements d'interconnexions réseau :

Un réseau local est constitué d'ordinateurs reliés par un ensemble d'éléments matériels et logiciels. Les éléments matériels qui permettent d'interconnecter les ordinateurs sont les suivants :

- **La carte réseau :** parfois appelé coupleur, il s'agit d'une carte connectée sur la carte mère de l'ordinateur ou partie intégrante de la Carte mère qui relie à l'aide d'un câble ou d'ondes radios un ordinateur au reste du réseau. Sa vitesse était autrefois de 10 Mbps, la majorité du Parc est en 100Mbps et aujourd'hui les dernières cartes sont en 1 000 Mbps.



Figure I.13 Carte réseau

- **Les répéteurs :** permettant de régénérer automatiquement un signal ; ce qui permette de prolonger la portée du support.

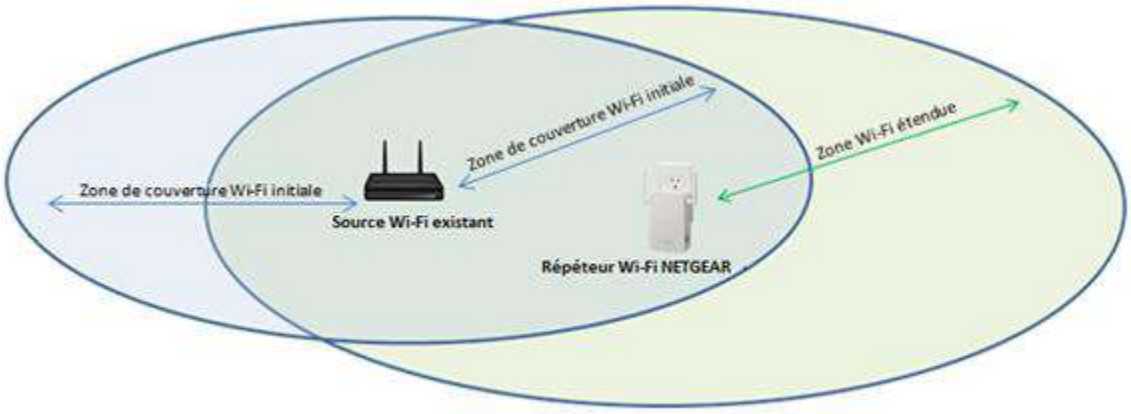


Figure I.14 Fonctionnement d'un répéteurs

- **Les concentrateurs (hubs) :** permettant de connecter entre eux plusieurs hôtes. Ils sont non intelligents. Ils envoient le signal pour toutes les stations compris la station destinatrice.



Figure I. 15 Un concentrateur (hub)

- **Les ponts (bridges) :** permettant de relier des réseaux locaux de mêmes types.

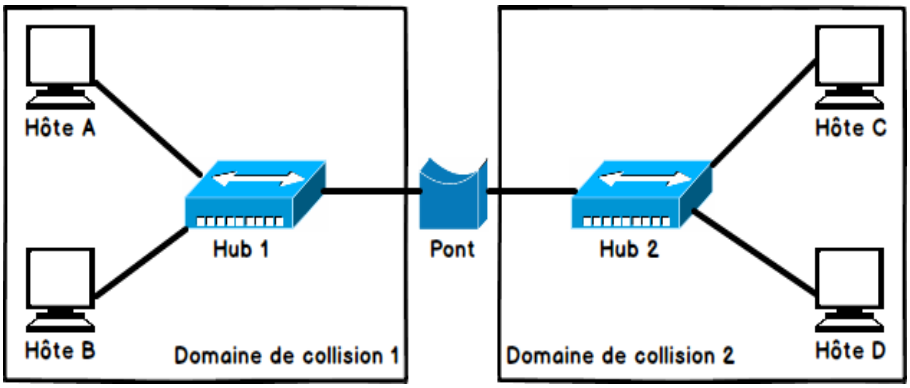


Figure I.16 Fonctionnement d'un pont

- **Les commutateurs (Switch) :** Au-delà d'un certain nombre de « nœuds » connectés avec des hubs, les performances du réseau peuvent chuter nettement. Ceci se produit quand le réseau est surchargé en équipements.

Le commutateur va jouer le même rôle que le concentrateur, cependant, il sera plus performant lorsque le réseau est surchargé en équipements.

Contrairement au concentrateur qui envoie l'information à l'ensemble des ordinateurs connectés au réseau, le commutateur va établir une liaison seulement entre les ordinateurs intéressés par l'information.



Figure I. 17 Un switch

- **Les passerelles (Gateway) :** permettant de relier des réseaux locaux de types différents.
- **Les routeurs :** Ce dispositif permet l'échange des informations entre deux réseaux, il permet l'interconnexion de réseaux. Il dispose d'un port (connecteur RJ45) par réseau, d'un système d'exploitation, et d'un logiciel chargé d'aiguiller (router) les informations. Il est la pièce essentielle pour l'accès à Internet.
- **Les B-routeurs** : associant les fonctionnalités d'un routeur et d'un pont.
- **Un pare-feu :** est un appareil de protection du réseau qui surveille le trafic entrant et sortant et décide d'autoriser ou de bloquer une partie de ce trafic en fonction d'un ensemble de règles de sécurité prédéfinies.

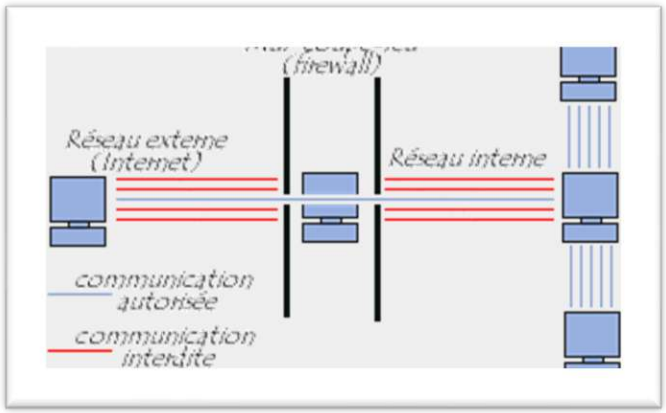


Figure I.18 Fonctionnement d'un par-feu

Les pare-feu constituent la première ligne de défense des réseaux depuis plus de 25 ans. Ils établissent une barrière entre les réseaux internes sécurisés et contrôlés qui sont dignes de confiance et les réseaux externes non fiables tels qu'Internet.

Un pare-feu peut être un équipement physique, un logiciel ou une combinaison des deux.

- **Point d'accès sans fil** est un dispositif qui permet aux périphériques sans fil de se connecter à un réseau câblé ou un réseau internet à l'aide d'une connexion radio, le point d'accès en tant que dispositif autonome est habituellement relié à un routeur (par l'intermédiaire d'un réseau câblé), mais il peut aussi faire partie intégrante du routeur lui-même.

I.8. Architecture des réseaux

Grace à l'évolution des capacités réseaux, le traitement automatisé des informations à considérablement évoluer depuis une quarantaine d'années. Succédant aux grands systèmes propriétaires centralisées, plusieurs architectures sont désormais possibles. [5]

I.8.1. L'architecture OSI

Le modèle OSI (Open Système Interconnexion) : destiné à normalisée les échanges entre deux machines. Il définit ainsi ce quoi doit être une communication réseau complète. L'ensemble du processus est ainsi découpée en sept couches hiérarchiques. Chaque couche se comporte comme un prestataire de service pour la couche immédiatement supérieure ; chacune d'elles ajoute un en-tête spécifique à la trame reçue. [5]

- **La couche physique (Couche 1) :** Rassemble les moyens électriques, mécaniques, optiques ou hertziens par lesquels les informations sont transmises. Les unités sont donc des bits (0 ou 1). [6]

- **La couche liaison de donnée (couche 2) :** Gère la fiabilité de transfert des bits d'un nœud à l'autre du réseau, comprenant entre autres les dispositifs de détection et correction d'erreur, ainsi que le système de partage des supports. L 'unité de donné à ce niveau est appelée une trame. [6]
- **La couche réseau (couche 3) :** Aiguille les données à travers un réseau à commutation. L'unité de données s'appelle en général un paquet.
- **La couche transport (couche 4) :** Regroupe les règles de fonctionnement de bout en bout, assurant ainsi la transparence du réseau vis-à-vis des couches supérieures .Elle traite notamment l'adressage, l'établissement des connexions et la fiabilité de transport.
- **La couche session (couche 5) :** Réunit les procédures de dialogue entre les applications, établissement et interruptions de la communication, cohérence et synchronisation des opérations.
- **La couche présentation (couche 6) :** Traite les formes de représentation des données permettant la traduction entre machines différentes.
- **La couche application (couche 7) :** Source et destination de toutes les informations à transporter, la couche application rassemble toutes les applications qui ont besoin de communiquer par le réseau : messagerie électronique, transfert de fichiers, gestionnaire de base de données. [5]

I.8.2. L'architecture TCP/IP

Le modèle TCP/IP peut en effet être décrit comme une architecture réseau à 4 couches dans laquelle les protocoles TCP et IP jouent un rôle prédominant, car ils en constituent l'implémentation la plus courante.

Par abus de langage, TCP/IP peut donc désigner deux choses le modèle TCP/IP et la suite de deux protocoles TCP et IP.

- **La couche accès réseau:** Cette couche regroupe les couches physiques et liaison de données du modèle OSI.
- **La couche internet :** Cette couche est la plus importante dans cette architecture ; elle réalise l'interconnexion des réseaux distant sans connexion, permet l'injection des paquets indépendamment les uns des autres jusqu'à la destination.
- **La couche transport:** Son rôle est le même que celui de la couche transport du modèle OSI : permettre à des entités paires de soutenir une conversation.

- **La couche application :** Contrairement au modèle OSI, c'est la couche immédiatement supérieure à la couche transport, elle contient les protocoles de haut niveau TELNET, TFTP, … ; Le point important pour cette couche est le choix du protocole de transport à utiliser. [6]

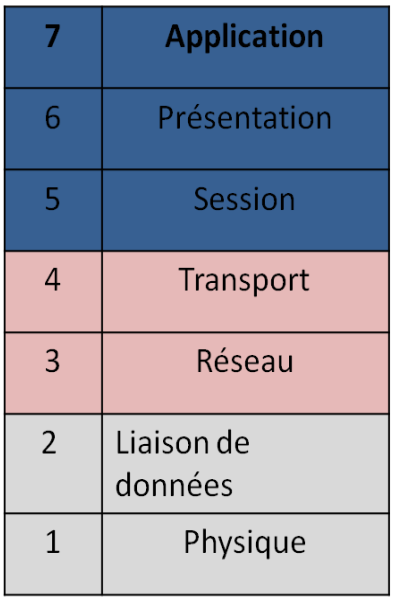


Figure I. 19 Le modèle OSI

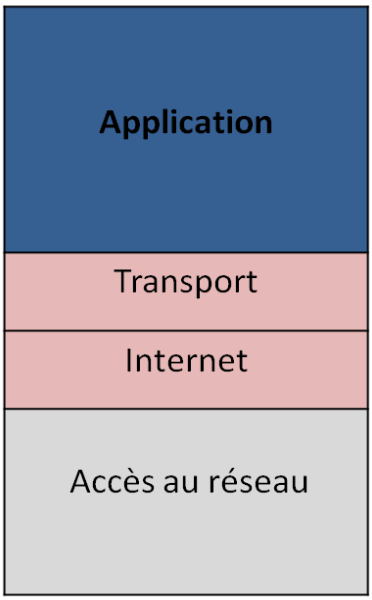


Figure I.20 Le modèle TCP/IP

I.9. Les Protocoles de réseau

Un protocole est une méthode standard qui permet la communication entre deux machines. Ensemble de règles et de procédures à respecter pour émettre et recevoir des données sur le réseau. Parmi lequel on site :

I.9.1. TCP/IP (Transmission Control Protocol / Internet Protocol)

Définit la norme de communication, (en fait un ensemble de protocoles) des ordinateurs reliés à Internet.

Ce modèle définit les règles que les ordinateurs doivent respecter pour communiquer entre eux sur le réseau Internet. Nous vous proposons de découvrir plus en détails ses caractéristiques et son fonctionnement.

Il existe d'autre protocole comme :

- **FTP** sert à transporter des fichiers d'un ordinateur à l'autre.
- **IRC** permet de créer des «salons» de discussion en direct. • ICQ permet de savoir si quelqu'un est en ligne et de dialoguer avec lui.
- **NTP** permet de mettre les ordinateurs à l'heure par internet à 500 millisecondes près.
- **P2P** permettent de partager des fichiers à grande échelle.

- **NNTP** permet d'accéder à des forums de discussion sur des milliers de sujets différents.
- **SSH** permet d'avoir un accès sécurisé à des ordinateurs distants.
- **SMTP** permet d'envoyer des emails, et le protocole POP3 de les recevoir.
- **DNS :** Domain Name Server : système de nom de domaine ou système d'affectation de nom, il permet de retrouver une adresse IP à partir d'un nom de domaine (un peu comme un annuaire). C'est un système distribué de bases de données et de serveurs qui assure la traduction des noms de domaine utilisés par les internautes en numéros IP utilisables par les ordinateurs. Mis au point pour permettre aux internautes d'utiliser des noms dans la rédaction des adresses (beaucoup plus facile à manipuler que des suites de chiffres).

Exemples : nom : www.unice.fr -> IP : 134.59.1.71

Nom : bach.ebgm.jussieu.fr -> IP : 134.157.50.1

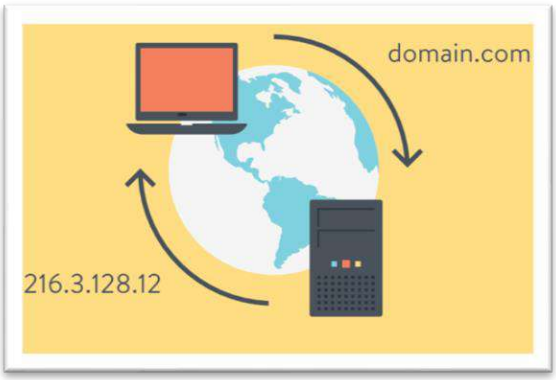


Figure I.21 Le protocol DNS

- **TELNET :** protocole standard permettant l'interfaçage de terminaux et d'applications à travers Internet. Ce protocole fournit les règles de bases pour permettre de relier un client (système Composé d'un affichage et d'un clavier) à un ordinateur distant (côté serveur).

Remarque : TELNET est un protocole de transfert non sûrs, c'est-à-dire que les données circulent en clair sur le réseau.

I.9.2. Le protocole IPX (Inter Packet exchange)

Un protocole de niveau réseau développé et commercialisé par la société Novell et intégré à son système d'exploitation réseau. Les paquets XP peuvent être acheminées d'un

réseau à l'autre aux couches trois et quatre du modèle de référence OSI (Open System Interconnexion). [7]

I.9.3. Le Protocol NetBeui

Un protocole plus rapide que TCP/IP et IPX, il est utilisé par les petits réseaux LAN, sa rapidité du traitement exprime son utilité. [7]

I.10. Conclusion

Ce chapitre a montré des notions sur les réseaux informatiques tel que les différents types de réseau et on a décrit quelques concepts qui définissent les réseaux informatiques, à savoir les topologies, et les modèles des réseaux OSI et TCP/IP et on 'a expliqué quelques équipements d'interconnexions.

Chapitre II

Etude de l'existant et construction du cahier des charges



II.1. Partie 01 : Description de champs de l'étude

II.1.1. Introduction

Afin d'améliorer nos connaissances dans le domaine du réseau, il est indispensable de développer nos capacités professionnelles. Pour cela, nous avons fait ce travail informatique de nouveau pôle de Médéa (pole ouzera) que nous allons vous présenter ci-dessous.

Le réseau informatique prend une place de plus en plus importante dans l'activité de ce pôle universitaire d'ouzera. Pour cela, ses informations doivent être gérées, centralisées et accessibles en temps réel.

II.1.2. Presentation de pôle universitaire d'ouzera

II.1.2.1. Présentation de la ville d'ouzera

Ouzera est une commune de la wilaya de Médéa en Algérie, située en pleine région montagneuse, sur un plateau inséré entre l'atlas de BLIDA et le massif de la ville de BERROUAGHIA. Située à 3 km au Sud-Est du chef-lieu de la wilaya de Médéa, elle dispose d'une position privilégiée dans l'armature urbaine régionale .Ouzera est chef –lieu de daïra des communes de Ben Chicao et El Hamdania. Occupant une superficie de 10100km². [8]

II.1.2.1.1. Situation et délimitation de la ville

Ouzera est une commune de la wilaya de Médéa en Algérie, située en pleine région montagneuse, sur un plateau inséré entre l'atlas de BLIDA et le massif de la ville de BERROUAGHIA.



FigureII.1 Situation de Ouzera dans la willaya de Médéa

Située à 3 km au Sud-Est du chef-lieu de la wilaya de Médéa, dispose d'une position privilégiée

dans l'armature urbaine régionale .Ouzera est chef –lieu de daïra des communes de **Ben Chicao** et **El Hamdania.** Occupant une superficie de **10100 km².**

Délimitation

La commune d'Ouzera est délimitée comme suit :

- Au Nord par la commune d'El Hamdania
- Au Sud par la commune de Ben-Chicao
- A l'Est par les Communes d'El Omaria et d' Ouled Brahim.
- à l'Ouest par les Communes de Médéa et de Ain Deheb (Damiette). [8]

II.1.3. Le Campus d'ouzera

II.1.3.1. Le projet du campus universitaire

Le ministère de l'enseignement supérieur et de la recherche scientifique a donné son aval à la réalisation d'un nouveau campus a ouzera 6km environ à l'est du chef-lieu de wilaya de Médéa initialement prévu sur une autre assiette non loin de l'actuel pole.

Le projet a été délocalisé et transfèré vers la commune de ouzera ou les conditions naturelles du site choisi sont plus favorable pour sa réalisation au plan de délai et du cout. Le terrain d'assiette choisi par l'autorité locale se trouve à proximité de la RN1 et à l'entrée ouest de la ville. Retenu dans le cadre de programme quinquennal le nouveau campus universitaire aura une capacité d'actuel de 8000 places pédagogique.

II.1.3.2. Organigramme du pôle d'Ouzera

Pour la réalisation de ses objectifs, le nouveau pôle d'Ouzera est divisé en trois facultés.

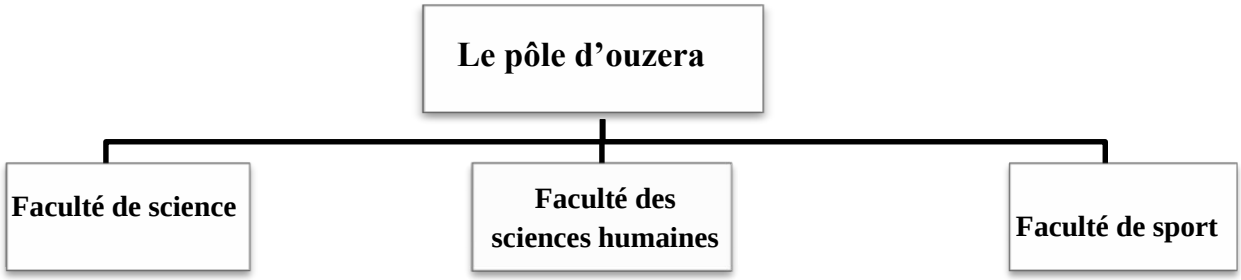


Figure II.2 Organigramme du pôle d'Ouezra

II.1.4. Architecture de pôle universitaire d'Ouzera

Le pôle universitaire d'Ouezra est l'un des trois attachements de l'université de Yahia Fares de Médéa, il est composé de trois facultés :

Faculté des sciences, Faculté des sciences humaines et sociologies, Faculté de sport.

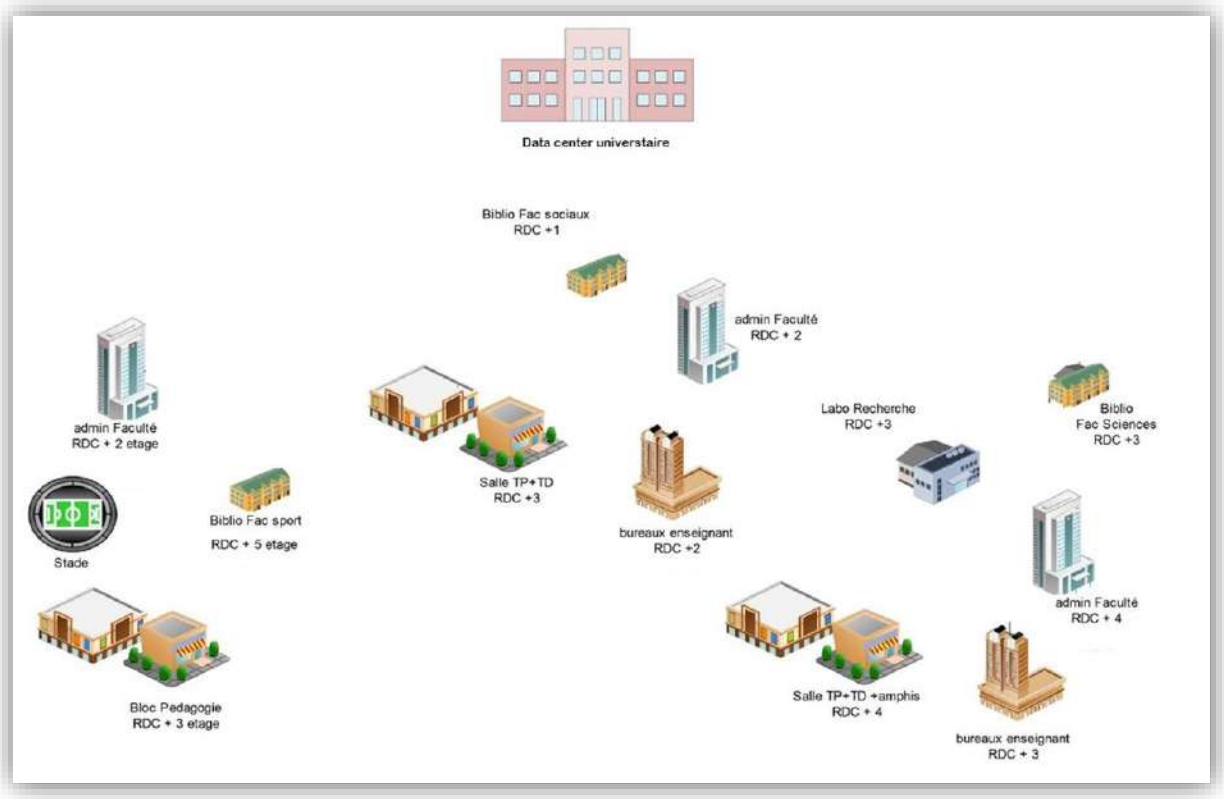


Figure II.3 Schéma du site global

- La faculté des sciences aura une capacité de 3500 places pédagogique, elle est composée de cinq bâtiments :
  - Administration (RDC+4)
  - Amphis/salle td/salle TP (RDC+4)
  - labo de recherche (RDC+3)
  - bureaux d'enseignant (RDC+3)
  - bibliothèque (RDC+3)

- La faculté des sciences humaines et sociologies aura une capacité de 2500 places pédagogique elle est composé de cinq bâtiments

- Administration (RDC+2)
- Amphis (RDC+1)
- salle td/salle TP (RDC+3)
- bureaux d'enseignant (RDC+2)
- bibliothèque (RDC+1)

❖ La faculté de sport aura une capacité de 2000 places pédagogiques elle composé de quatre bâtiments :

- Administration (RDC+2)
- Amphis(RDC)
- salle td/salle TP/salle cours (RDC+3)
- bibliothèque (RDC+5)

Tableau II.1 places pédagogiques et bâtiments pour chaque département

Département	**Science**	**Sciences humaines et sociologies**	**Sport**
Places pédagogiques	3500	2500	2000
Batiments	❖ Administration. ❖ Amphis/salles TD/salles TP ❖ Laboratoire de recherche ❖ Bureau d'enseignant ❖ Bibliothèque	❖ Administration ❖ Amphis ❖ salles TD/salles TP ❖ bureau d'enseignant ❖ bibliothèque	❖ Administration ❖ Amphis ❖ sallesTD/sallesTP ❖ Bibiotheque

À partir des plans génie civil (Annexe) nous obtenons les informations et les détails de chaque bâtiment dans chaque faculté comme la suite :

II.1.5. Les Prises informatiques

Les parties visibles d'un système de câblage sont les prises utilisateur, également appelées prises VDI (voix, donnés, images) installés dans les bureaux. Elles sont regroupées par blocs de 2 à 4, appelées boitiers VDI une densité courante est d'un bloc VDI pour 7 à 10 m de bureau.

D'après notre étude sur les plans génie civil de trois facultés et leurs nombres des bureaux en prenant en considération leurs surface, nous avons proposé une estimation de nombres du prises informatiques comme suit :

II.1.5.1. La faculté des sciences

Tableau II.2 nombre des prises pour la faculté de science

Bloc d'administration				
Niveau	**Nombre de bureau**	**Nombre de salles**	**Nombre de prise**	**Total prises**
Sous sol	**0**	**0**	**0**	
RDC	**7**	**1**	**26**	**26**
1 ere	**14**	**0**	**43**	**43**
2 eme	**10**	**1**	**35**	**35**
3 eme	**14**	**0**	**43**	**43**
4 eme	**9**	**1**	**32**	**32**
Total prises				179
Bloc bibliothéque				
Niveau	**Nombre de bureau**	**Nombre de salles**	**Nombre de prise**	**Total prises**
sous sol	**3**	**2**	**15**	**15**
RDC	**Prêt**	**3**	**10+15+20**	**45**
1 ere	**0**	**3**	**45**	**45**
2 eme	**0**	**2**	**30**	**30**
3 eme	**7**	**1**	**52**	**52**
Total prises				187
Bloc Amphi / salle TD				
Niveau	**Nombre de bureau**	**Nombre de salles**	**Nombre de prise**	**Total prises**
sous sol	**0**	**4**	**2+2*5+2**	**8**
RDC	**5**	**7**	**19+12+2**	**33**
1 ere	**0**	**6**	**4+2*20**	**44**
2 eme	**0**	**14**	**14**	**14**
3 eme	**0**	**14**	**14**	**14**
4 eme	**0**	**6**	**6**	**6**
Total prises				119
Bloc Bureau d'enseignant				
Niveau	**Nombre de bureau**	**Nombre de salles**	**Nombre de prise**	**Total prises**
sous sol	**0**	**0**	**0**	**0**
RDC	**8**	**1**	**25+10**	**35**
1 ere	**14**	**0**	**42**	**42**
2 eme	**14**	**0**	**42**	**42**

3 eme	**14**	**0**	**42**	**42**
Total prises				161
Bloc laborotoire				
Niveau	**Nombre de bureau**	**Nombre de salles**	**Nombre de prise**	**Total prises**
sous sol	**0**	**0**	**0**	**0**
RDC	**2**	**5**	**8+5*7**	**43**
1 ere	**4**	**5**	**15+35**	**50**
2 eme	**4**	**5**	**14+35**	**49**
3 eme	**4**	**5**	**14+35**	**49**
Total prises				191
Nombre total des prises				837

II.1.5.2. La faculté de sciences humaines et sociales

Tableau II.3 nombre des prises pour la faculté de sociologie

Bloc d'adminstration				
Niveau	**Nombre de bureau**	**Nombre de salles**	**Nombre de prise**	**Total prises**
RDC	**15**	**2**	**5+3*14+8+2*2**	**59**
1 ere	**17**	**3**	**66**	**66**
2 eme	**16**	**0**	**53**	**53**
Total prises				**178**
Bloc bibliothéque				
Niveau	**Nombre de bureau**	**Nombre de salles**	**Nombre de prise**	**Total prises**
sou sol	**4**	**2**	**11+2**	**13**
RDC	**4**	**4**	**9+10+10+2*20**	**69**
1 ere	**2**	**0**	**6**	**6**
Total prises				**88**
Bloc Amphi				
Niveau	**Nombre de bureau**	**Nombre de salles**	**Nombre de prise**	**Total prises**

1 ere	**6**	**3**	**6*2+3*3**	**21**
Total prises				**21**
Bloc Bureau d'enseignant				
Niveau	**Nombre de bureau**	**Nombre de salles**	**Nombre de prise**	**Total prises**
RDC	**16**	**1**	**6*3+10*2+2**	**40**
1 ere	**19**	**0**	**10*3+4*4+5*3**	**61**
2 eme	**16**	**0**	**8*3+4*4+4*2**	**48**
Total prises				**149**
Bloc laboratoire				
Niveau	**Nombre de bureau**	**Nombre de salles**	**Nombre de prise**	**Total prises**
sou sol	**0**	**4**	**80**	**80**
RDC	**0**	**0**	**0**	**0**
1 ere	**0**	**0**	**0**	**0**
2 eme	**0**	**0**	**0**	**0**
3 eme	**0**	**0**	**0**	**0**
Total prises				**80**
Nombre total des prises				**516**

II.1.5.3. La faculté de sport

Tableau II.4 nombre des prises pour la faculté de sport

Bloc d'Administration				
Niveau	**Nombre de bureau**	**Nombre de salles**	**Nombre de prise**	**Total prises**
RDC	**5**	**2**	**13**	**13**
1 ere	**18**	**1**	**13*2+4*3+4+5**	**47**
2 eme	**13**	**1**	**10*2+4+2*3+5**	**35**
Total prises				**95**

Bloc bibliothéque				
Niveau	**Nombre de bureau**	**Nombre de salles**	**Nombre de prise**	**Total prises**
RDC	**1**	**2**	**2+8**	**10**
1 ere	**0**	**3**	**12**	**12**
2 eme	**0**	**3**	**8**	**8**
3 eme	**0**	**4**	**24**	**24**
4 eme	**4**	**4**	**12+6**	**18**
5 eme	**2**	**1**	**5**	**5**
Total prises				**77**
Bloc Amphi 1				
Niveau	**Nombre de bureau**	**Nombre de salles**	**Nombre de prise**	**Total prises**
RDC amphi 1	**0**	**0**	**1**	**1**
RDC amphi 2	**0**	**0**	**1**	**1**
RDC amphi 3	**0**	**0**	**1**	**1**
Total prises				**3**
Bloc Amphi 2				
Niveau	**Nombre de bureau**	**Nombre de salles**	**Nombre de prise**	**Total prises**
sou sol	**0**	**1**	**2**	**2**
RDC	**0**	**0**	**0**	**0**
1 ere	**0**	**3**	**6**	**6**
2 eme	**0**	**3**	**6**	**6**
Total prises				**14**
Bloc Amphi 3				
Niveau	**Nombre de bureau**	**Nombre de salles**	**Nombre de prise**	**Total prises**
RDC	**0**	**0**	**0**	**0**

1 ere	**1 stock**	**1**	**3**	**3**
2 eme	**0**	**3**	**6**	**6**
Total prises				**9**
bloc Amphi 3				
Niveau	**Nombre de bureau**	**Nombre de salles**	**Nombre de prise**	**Total prises**
RDC	**0**	**0**	**0**	**0**
1 ere	**2**	**1**	**8**	**8**
2 eme	**11**	**1**	**8*2+3*3+3**	**28**
3 eme	**21**	**1**	**20+13+4+2**	**39**
Total prises				**75**
Nombre total des prises				**273**

Et voilà le nombre total des prises informatiques pour chaque faculté

Tableau II.5 Nombre de prises informatique

Faculté	**Faculté de science**	**Faculté de sociologies**	**Faculté de sport**	**Nombre total**
Nombre des prises informatique	**837**	**516**	**273**	**1626**

II.2. Partie 02 : Conception technique

II.2.1. Description du projet

La mise en place d'une infrastructure réseau LAN au niveau de pole de Ouezra fait partie du projet d'extension du réseau intranet déjà installé au niveau de tous l'université les équipes techniques du Centre de Ressources Informatiques ont procédé à une étude de solution adaptée qui répond aux besoins de notre Université en termes de performance, compatibilité avec le réseau existant et dimensionnement, en considération des dernières évolutions des réseaux informatiques, pour sa partie active.

II.2.2. Partie génie civil

II.2.2.1. Caniveau de câblage

Pour le câblage entre les différentes facultés on a lié les bâtiments de chaque faculté avec le bâtiment d'administration et en suite on a lié les bâtiments d'administration de la faculté de sciences et de la faculté du sport avec le bâtiment d'administration de la faculté de sciences humaines et sociologies et on a obtenue alors le schéma suivant :

- **L'Infrastructure à l'intérieur du pôle universitaire**

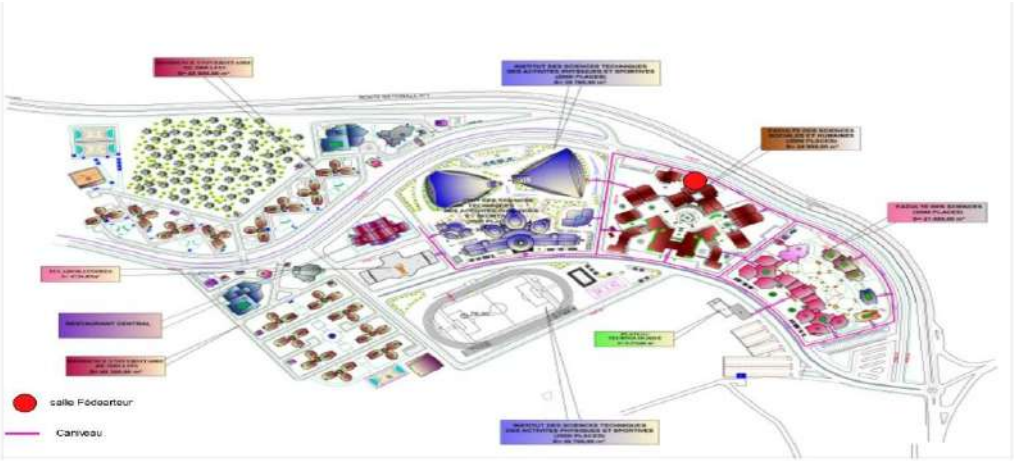


Figure II.4 L'infrastructure à l'intérieur

A la base de l'infrastructure à l'intérieur du nouveau pôle universitaire le schéma de caniveau est comme suit :

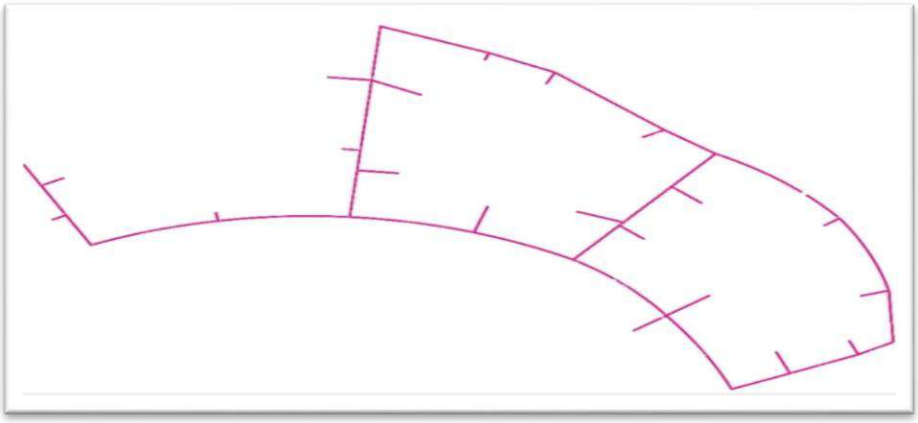


Figure II.5 Schéma général du caniveau

II.2.3. Modèle de réseau

Afin de mieux répondre aux besoins des entreprises, la conception d'un réseau doit s'effectuer suivant un modèle hiérarchique.

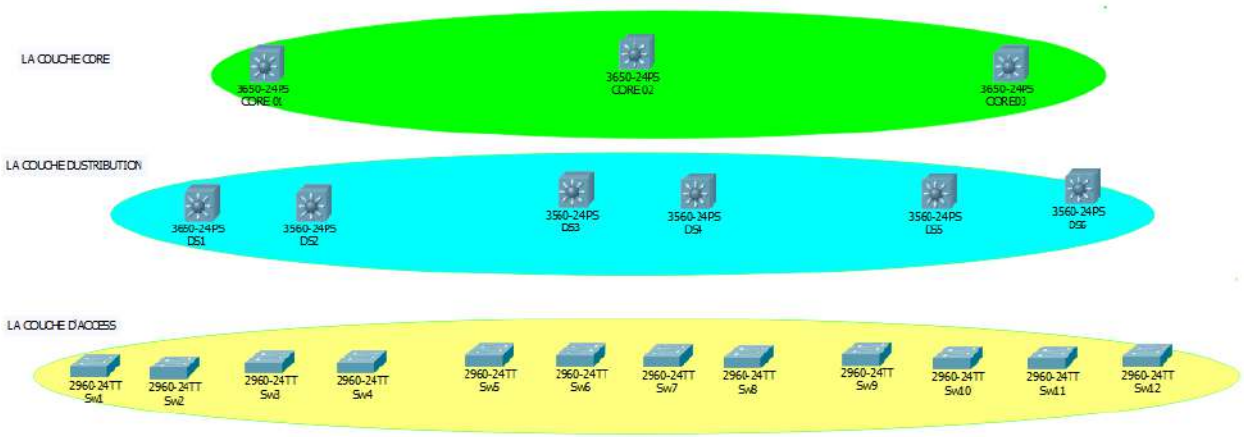


Figure II.6 **modèle du réseau hiérarchique**

II.2.3.1. Modèle de conception hiérarchique à trois couches

Cisco a développé un modèle à trois couches pour concevoir un réseau de campus :

II.2.3.1.1. La couche d'accès (Access Layer)

Cette couche est constituée des périphériques finaux tels que les ordinateurs, les imprimantes et les téléphones IP. Elle peut aussi contenir des routeurs, des commutateurs, des concentrateurs et des points d'accès sans fil.

Le rôle de cette couche est de connecter les périphériques finaux au reste du réseau et de vérifier s'ils sont autorisés.

II.2.3.1.2. La couche de distribution (Distribution Layer)

Cette couche contient essentiellement des commutateurs de niveau 2 et 3 (Fonction de routage) et sert d'interconnexion entre la couche d'accès et la couche de cœur de réseau. Son rôle et de gérer le flux du trafic à l'aide de stratégies et de délimiter les domaines de diffusion via des fonctions de routage inter VLAN.

II.2.3.1.3. La couche cœur de réseau (Core Layer)

La couche cœur et considérée comme étant le réseau fédérateur à haut débit de l'inter réseau et assure la connexion aux ressources internet. Le trafic au niveau de cette couche est Important et rapide.

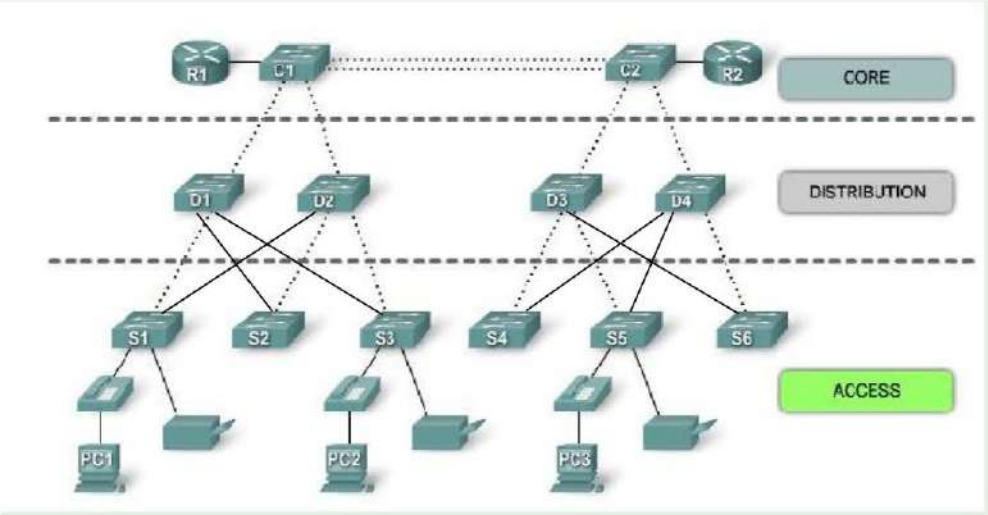


Figure II.7 Modèle hirèrarchique à trois couches

II.2.3.1.4. Avantage d'un réseau hiérarchique

- **Evolutif** : ces réseaux peuvent s'étendre plus facilement.

- **Redondant** : la redondance au niveau de la couche cœur de réseau et de la couche de distribution permet d'assurer une continuité de service pour la couche d'accès.
- **Performant** : la mise en place d'agrégat de liens entre les commutateurs de la couche de distribution et ceux de la couche cœur du réseau permet d'augmenter la vitesse.
- **Sécurité** : la sécurité du réseau peut être renforcée avec la mise en place de la sécurité des ports au niveau de la couche d'accès et la mise en place des stratégies de sécurité et/ou des listes de contrôle d'accès au niveau de la couche de distribution.
- **Cout de gestion diminué** : la cohérence de paramétrage entre les différents commutateurs de même couche permet une simplification de la gestion.
- **Maintenance** : la conception modulaire d'un réseau hiérarchique permet une mise à jour plus aisée.

II.2.3.1.5. Principes du modèle d'un réseau hiérarchique

Pour mettre en place correctement un réseau hiérarchique, il faut commencer par étudier la couche d'accès et définir les périphériques finaux. Pour les autres couches, il faut étudier ces elements:

- **Les liens agrégés** : il faut identifier les ports permettant la liaison entre les commutateurs de chaque couche et surtout estimer les débits nécessaires et disponibles pour mettre en place les liens agrégés permettant d'augmenter la bande passante disponible.
- **Les liens redondants** : en plus des liens agrégés, il faut prévoir des liens redondants permettant d'assurer la continuité de service sur la couche de distribution et la couche cœur de réseau en cas de défaillance d'un commutateur sur ces couches.

II.2.4. Solutions proposées

II.2.4.1. Solution globale

Nous préconisons une architecture réseau basée sur une topologie en étoile depuis le répartiteur général installé au niveau du bloc administration de la faculté de science humaine et sociale où sera installé le switch core vers les répartiteurs secondaires installés dans les autres blocs de la facultés et les autre facultés de sport et de science ayant comme supports de transmission un câble fibre optique multimode.

A l'intérieur de chaque bloc, la distribution sera également basée sur une topologie en étoile depuis le Switch de distribution (installé dans le Répartiteur Secondaire du bloc) vers les switch d'accès (Sous Répartiteur Secondaire).

II.2.4.2. Differentes solutions proposées

Pour le cahier de charge technique du nouveau pôle d'Ouzera on a proposé trois solutions, l'une est la solution normalisée et l'autre c'est la solution basique et le troisième c'est notre choix est une solution combinée entre la solution normalisé et la solution basique.

II.2.4.2.1. Solution normalisée

Pour cette proposition on a l'architecture composé de 3 switchs core et 9 switchs de distribution et les switchs d'accès.

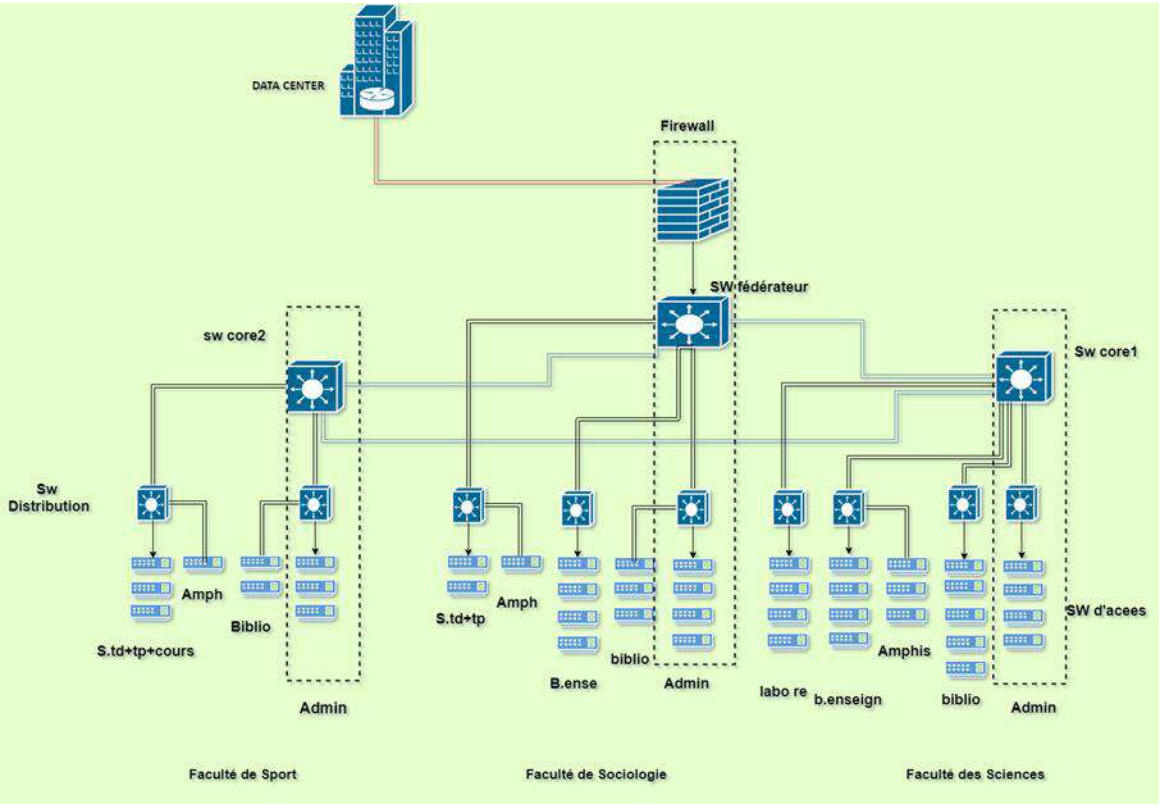


Figure II.8 Architecture du réseau solution normalisé

Tableau II.6 détails de l'architecture du réseau solution normalisé

Faculté	Bloc	nbr de posts	armoire	Terroir optique	modem Wi-Fi	switch d'accès		Switch distribution 24	Switch core	Pare-feu	Controller	Panneaux de Brass age 24
				12		24	48					
Faculté des Sciences	**Admin**	179	6u	1	1	1	3	1	1	0	0	8
	Biblio	192	6u	1	1	1	4	1	0	0	0	9
	Amphi + Salle TD	119	4u	1	1	1	2	0	0	0	0	5
	Bureau Enseignants	161	5u	1	0	1	3	1	0	0	0	7
	Labo TP	191	5u	1	1	0	4	1				8
Faculté des Sciences Humaines et Socials	**Admin**	178	8u	1	1	0	4	1	1	1	1	9
	Biblio	108	5u	1	1	1	2	1				5
	Amphi	21	2u	1	1	1	0	0	0	0	0	1
	Bureau Enseignants	149	5u	1	0	0	4	1	0	0	0	8
	Labo TP + Salle TD	80	3u	1	1	0	2	0	0	0	0	4
Institus de Sport	**Admin**	95	6u	1	1	1	2	1	1	0	0	6
	Biblio	77	3u	1	1	0	2	0	0	0	0	5
	Amphi	3	2u	1	1	1	0	1	0	0	0	1
	Salle TD+Salle Cours + Salle TP	98	4u	1	1	1	2	0	0	0	0	8
Total		**1651**		**14**	**12**	**9**	**34**	**9**	**3**	**1**	**1**	**85**

- **Le coût de cette proposition**

Tableau II.6 le coût de la solution normalisé

Désignation	**Unité**	**Quantité**	**Prix Unité (Da)**	**Prix totale**
1. MATERIEL PASSIF CUIVRE:				
Goulotte 100x50	Ml	400	365.00	**146 000.00**
Goulotte 20x40	Ml	300	275.00	**82 500.00**
Câble FTP 4 paires catégorie 6 classe A	Ml	49530	120.00	**5 943 600.00**
Prises informatiques Prise RJ45 catégorie6 FTP	U	1651	2 000.00	**3 302 000.00**
Cordons de brassage FTP RJ45/RJ45 de 1 m catégorie 6 classe A	U	1651	650.00	**1 073 150.00**
2. MATERIEL PASSIF FIBRE				
Tiroir Optique OM3 pour 12 connecteurs sc/sc duplex	U	17	9117.00	**154 989.00**
Coupleur multimode sc duplex	U	112	137.00	**15 344.00**
Connecteur multimode sc duplex	U	112	400.00	**44 800.00**
Jarretière optique multimode OM3 2 mètres duplex sc/lc	U	56	2416.00	**135 296.00**
Jarretiére optique multimode OM3 2 métres duplex lc/lc	U	14	2568.00	**35 952.00**

Fibre multimode OM3 de 8 brins entre le bloc Administration et bureaux des enseignants (faculté des sciences)	MI	80	525.00	**42 000.00**
Fibre multimode OM3 de 8 brins entre le bloc de bureau d'enseignant et salles TD+ amphis (faculté des sciences)	Ml	100	525.00	**52 500.00**
Fibre multimode OM3 de 8 brins entre le bloc Administration et Bibliothèque (faculté des sciences)	Ml	110	525.00	**57 750.00**
Fibre multimode OM3 de 8 brins entre le bloc Administration et labo de recherche (faculté des sciences)	Ml	120	525.00	**63 000.00**
Fibre multimode OM3 de 8 brins entre le bloc Administration et bibliothèque (faculté des sociologie)	Ml	320	525.00	**168 000.00**
Fibre multimode OM3 de 4 brins entre le bloc Amphis et salle TD+laboratoires TP (faculté de sociologie)	Ml	50	320.00	**16 000.00**
Fibre multimode OM3 de 8 brins entre le bloc Administration et salle td+labo tp (faculté de sociologie)	Ml	400	525.00	**210 000.00**
Fibre multimode OM3 de 8 brins entre le bloc Administration et bureau d'enseignat (faculté de sociologie)	Ml	200	525.00	**105 000.00**
Fibre multimode OM3 de 8 brins entre le bloc bibliothéque et administration (faculté de sport)	Ml	320	525.00	**168 000.00**
Fibre multimode OM3 de 4 brins entre le bloc Amphis et bloc salle td +tp (faculté de sport)	Ml	350	320.00	**112 000.00**

Fibre multimode OM3 de 8brins entre le bloc de salle TD +TP et le bloc administration (faculté de sport)		100	525.00	**52 500.00**
Fibre multimode OM3 de 8 brins entre le bloc Administration de la faculté des sciences et le bloc administration du faculté de sociologie lien redondant	MI	250	525.00	**131 250.00**
Fibre multimode OM3 de 8 brins entre le bloc Administration de la faculté de sport et le bloc administration de la faculté de sociologie lien redondant	MI	300	525.00	**157 500.00**
Fibre multimode OM3 de 8 brins entre le bloc Administration de la faculté de sport et le bloc administration de la faculté de science lien redondant	MI	500	525.00	**262 500.00**
3. MATERIEL PASSIF				
Baies de brassage informatique 8U avec 02 ventilateurs	U	01	52 878.00	**52 878.00**
Baies de brassage informatique 6U avec 02 ventilateurs	U	03	43 000.00	**129 000.00**
Baies de brassage informatique 6U avec 02 ventilateurs	U	04	43 000.00	**172 000.00**
Baies de brassage informatique 4U avec 02 ventilateurs	U	02	34 643.00	**69 286.00**
Baies de brassage informatique 3U avec 1 ventilateur	U	02	23 112.00	**46 224.00**
Baies de brassage informatique 2U avec 1 ventilateur	U	02	18 220.00	**36 440.00**
Panneaux de brassage 24 ports RJ45 catégorie 6 classe A , connecteur accessible par la face avant.	U	80	15 195.00	**1 215 600.00**

Bandeau d'alimentation 08Prises + Disjoncteur + para foudre	U	14	60 50.00	**84 700.00**
Onduleur on line 3000 VA rackable + Carte SNMP	U	14	650 00.00	**910 000.00**
Switch de distribution /24 port+ 4 modules SFP	U	09	310000.00	**2 790 000.00**
Switch d'accès /24 port+ 2 module SFP	U	09	71 000.00	**639 000.00**
Switch d'accès /48 port+ 2 modules SFP	U	34	180000.00	**6 120 000.00**
Switch core 24 port SFP	U	1	755882.00	**755 882.00**
Switch core 12 port SFP	U	2	510000.00	**1 020 000.00**
Pare-feu	U	01	982550.00	**982 550.00**
Modules Gbic 10GBase SR lc/pc	U	59	156 00.00	**920 400.00**
Controleur point d'accés	U	01	178000.00	**178 000.00**
Point d'accés	U	30	30000.00	**900 000.00**
Serveur	U	6	780000.00	**4 680 000.00**
Coût total				**34 233 591.00**

✓ **Les avantages**

- la fiabilité.
- La redondance
- la simplicité d'adaptation aux évolutions.
- la capacité de gérer un trafic énorme
- isolation rapide des problèmes

✓ **Les inconvénients**

- Coût élevé
- La difficulté de réalisation

- Configuration compliqué.

II.2.4.2.2. Solution basique

Pour cette solution basique on 'a proposé une architecture composé par un switch fédérateur et 3 switch de distribution (un switch par faculté) et les switches d'accès

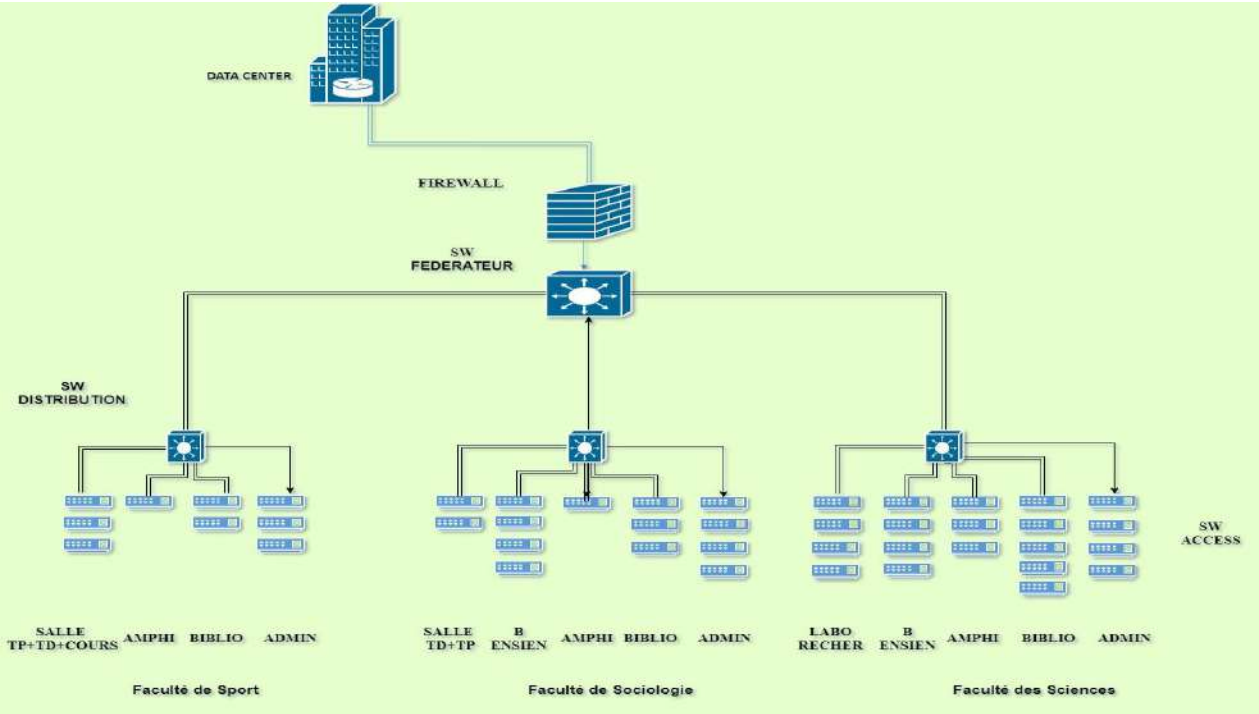


Figure II.9 Architecture du réseau de la solution basique

Tableau II.8 détails de l'architecture de la solution basique

Faculté	Bloc	nbr de posts	armoire	Tiroire optique	modem wifi	switch accée		Switch distribution 24	Switch core	Pare-feu	Controller	Panneaux de Brassage 24
				12		24	48					
Faculté des Sciences	Admin	179	6u	1	1	1	3	1	0	0	0	7
	Biblio	192	6u	1	1	1	4	0	0	0	0	7
	Amphi + Salle TD	119	4u	1	1	1	2	0	0	0	0	5
	Bureau Enseignants	161	5u	1	0	1	3	0	0	0	0	4
	Labo TP	191	5u	1	1	0	4	0	0	0	0	5
Faculté des Sciences Humaines et Socials	Admin	178	8u	1	1	0	4	1	1	1	1	8
	Biblio	108	4u	1	1	1	2	0	0	0	0	5
	Amphi	21	2u	1	1	1	0	0			0	1
	Bureau Enseignants	149	5u	1	0	0	4	0	0	0	0	5
	Labo TP + Salle TD	80	3u	1	1		2	0	0	0	0	4
Institus de Sport	Admin	95	5u	1	1	1	2	1	0	0	0	6
	Biblio	77	3u	1	1	0	2	0	0	0	0	4
	Amphi	3	2u	1	1	1	0	0	0	0	0	1
	Salle TD+Salle Cours + Salle TP	98	4u	1	1	1	2	0	0	0	0	5
Total		**1651**		**14**	**12**	**9**	**34**	**3**	**1**	**1**	**1**	**67**

- **Le coût de cette proposition :**

Tableau II.9 le coût de la solution basique

Désignation	Unité	Quantité	Prix Unité (Da)	Prix totale
1. MATERIEL PASSIF CUIVRE:				
Goulotte 100x50	Ml	300	365	**109 500.00**
Goulotte 20x40	Ml	200	275	**55 000.00**
Câble FTP 4 paires catégorie 6 classe A	Ml	49530	120.00	**5 943 600.00**
Prises informatiques Prise RJ45 catégorie6 FTP	U	1651	2 000.00	**3 302 000.00**
Cordons de brassage FTP RJ45/RJ45 de 1 m catégorie 6 classe A	U	1651	650.00	**1 073 150.00**
2. MATERIEL PASSIF FIBRE				
Tiroir Optique OM3 pour 12 connecteurs sc/sc duplex	U	17	9 117.00	**154 989.00**
Coupleur multimode sc duplex	U	112	137.00	**15 344.00**
Connecteur multimode sc duplex	U	112	400.00	**44 800.00**
Jarretière optique multimode OM3 2 mètres duplex sc/lc	U	56	2 416.00	**135 296.00**
Jarretiére optique multimode OM3 2 métres duplex lc/lc	U	14	2 568.00	**35 952.00**
Fibre multimode OM3 de 8 brins entre le bloc Administration et bureaux des enseignants (faculté des sciences)	MI	80	525.00	**42 000.00**
Fibre multimode OM3 de 8 brins entre le bloc d'administration et salles TD+ amphis (faculté des sciences)	Ml	120	525.00	**63 000.00**
Fibre multimode OM3 de 8 brins entre le bloc Administration et Bibliothèque (faculté des sciences)	Ml	110	525.00	**57 750.00**
Fibre multimode OM3 de 8 brins entre le bloc Administration et labo de recherche (faculté des sciences)	Ml	120	525.00	**63 000.00**

Fibre multimode OM3 de 8 brins entre le bloc Administration et bibliothéque (faculté des sociologie)	Ml	320	525.00	**168 000.00**
Fibre multimode OM3 de 4 brins entre le bloc d'administration et les amphis (faculté de sociologie)	Ml	420	320.00	**134 400.00**
Fibre multimode OM3 de 8 brins entre le bloc Administration et salle td+labo tp (faculté de sociologie)	Ml	400	525.00	**210 000.00**
Fibre multimode OM3 de 8 brins entre le bloc Administration et bureau d'enseignat (faculté de sociologie)	Ml	200	525.00	**105 000.00**
Fibre multimode OM3 de 8 brins entre le bloc bibliothéque et administration (faculté de sport)	Ml	320	525.00	**168 000.00**
Fibre multimode OM3 de 4 brins entre le bloc Amphis et bloc d'administration (faculté de sport)	Ml	110	320.00	**35 200.00**
Fibre multimode OM3 de 8brins entre le bloc de salle TD +TP et le bloc administration (faculté de sport)		100	525.00	**52 500.00**
Fibre multimode OM3 de 8 brins entre le bloc Administration de la faculté des sciences et le bloc administration du faculté de sociologie lien redondant	MI	250	525.00	**131 250.00**
Fibre multimode OM3 de 8 brins entre le bloc Administration de la faculté de sport et le bloc administration de la faculté de sociologie lien redondant	MI	300	525.00	**157 500.00**
3. MATERIEL PASSIF				
Baies de brassage informatique 8U avec 02 ventilateurs	U	01	52 878.00	**52 878.00**
Baies de brassage informatique 6U avec 02 ventilateurs	U	02	43 000.00	**86 000.00**
Baies de brassage informatique 5U avec 02 ventilateurs	U	04	43 000.00	**129 000.00**
Baies de brassage informatique 4U avec 02 ventilateurs	U	03	34 643.00	**103 929.00**
Baies de brassage informatique 3U avec 1 ventilateur	U	02	23 112.00	**46 224.00**
Baies de brassage informatique 2U avec 1 ventilateur	U	02	18 220.00	**36 440.00**

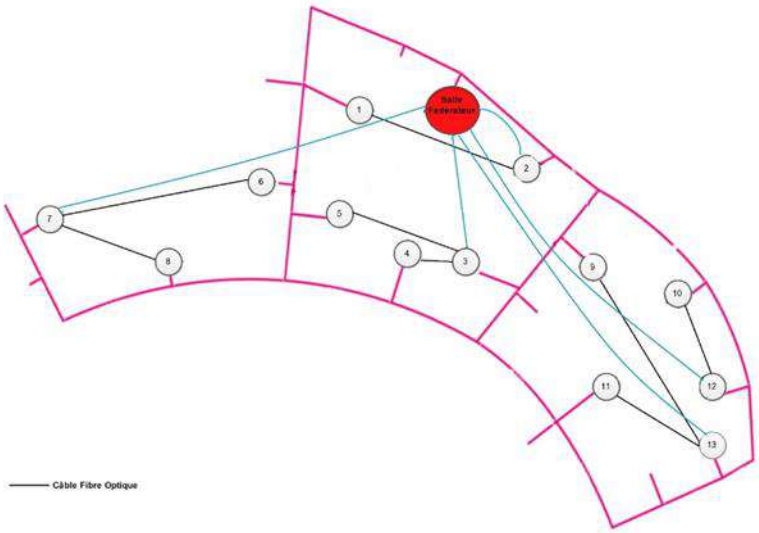
Panneaux de brassage 24 ports RJ45 catégorie 6 classe A , connecteur accessible par la face avant.	U	80	15 195.00	**1 215 600.00**
Bandeau d'alimentation 08Prises + Disjoncteur + para foudre	U	14	6 050.00	**84 700.00**
Onduleur on line 3000 VA rackable + Carte SNMP	U	14	65 000.00	**910 000.00**
Switch de distribution /24 port+ 4 module SFP	U	03	310 000.00	**930 000.00**
Switch d'acces/24 port+ 2 module SFP	U	09	71 000.00	**639 000.00**
Switch d'accés /48 port+ 2 module SFP	U	34	180 000.00	**6 120 000.00**
Switch core 24 port SFP	U	1	755 882.00	**755 882.080**
Pare-feu	U	01	822 750.00	**822 750.00**
Modules Gbic 10GBase SR lc/pc	U	59	15 600.00	**920 400.00**
Controleur point d'accés	U	01	178 000.00	**178 000.00**
Point d'acces	U	30	15 400.00	**462 000.00**
Serveur	U	6	420 000.00	**2 520 000.00**
Coût total				**28 270 034.00**

- ✓ **Les avantages**
  - Moins couteuse
  - Simple à configurer
  - La facilité de réalisation
- ✓ **Les inconvénients**
  - il n'a pas une redondance
  - la saturation du switch (pourcentage d'une panne et très élevé)
  - pas d'un équilibrage entre les switches de la distribution

II.2.4.2.3. Notre proposition (la solution optimisée)

A l'aide des propositions précédentes on a essayé de faire une solution optimale pour réduire le cout et respecté les normes de réalisation.

Cette proposition est notre choix de réalisation du réseau au niveau de nouveau pôle a ouezra .On commençant par le caniveau de fibre optique



FigureII.10 Schéma général de caniveau de fibre

A l'aide de cette figure on 'a fait des liaisons fibre optique entre les différents départements comme suite

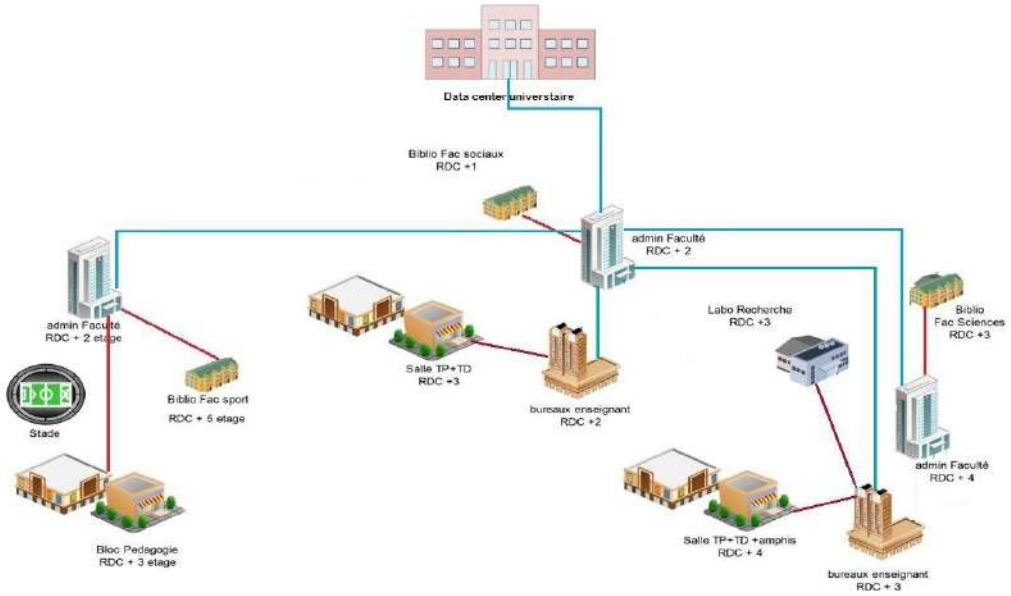


Figure II.11 Schéma de la liaison fibre optique entre les départements

A partir de cette schéma on 'a l'architecture suivant :

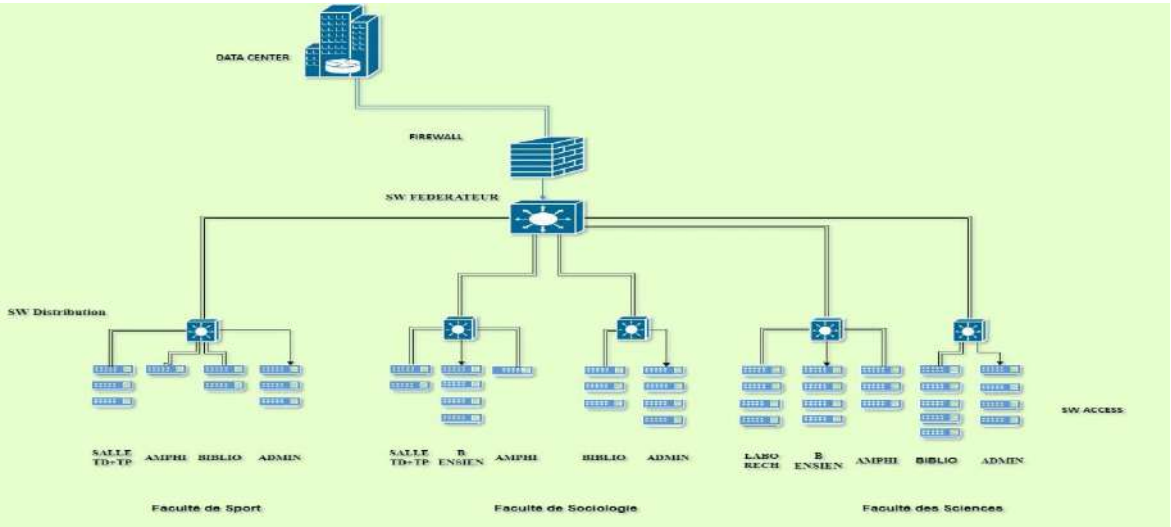


Figure II.12 Architecture du réseau de la solution proposée

Tableau II.10 architecture de la solution choisie

Faculté	**Bloc**	**nbr de posts**	**armoire**	**Tiroire optique**	**modem wifi**	**switch accée**		**Switch distribution 24**	**Switch core**	**Pare-feu**	**Panneaux de Brassage 24**
				12		**24**	**48**				
Faculté des Sciences	**Admin**	179	6u	1	1	1	3	1	0	0	7
	Biblio	192	6u	1	1	1	4	0	0	0	7
	Amphi + Salle TD	119	4u	1	1	1	2	0	0	0	5
	Bureau Enseignants	161	6u	1		1	3	1	0	0	6
	Labo TP	191	5u	1	1	0	4	0	0	0	6
Faculté des Sciences	**Admin**	178	8u	1	1	0	4	1	1	1	9
	Biblio	108	4u	1	1	1	2	0	0	0	5
	Amphi	21	2u	1	1	1	0	0	0	0	2

Humaines et Socials	**Bureau Enseignants**	149	6u	1	0	0	4	1	0	0	6
	Labo TP + Salle TD	80	3u	1	1	0	2	0	0	0	4
Institus de Sport	**Admin**	95	5u	1	1	1	2	1	0	0	6
	Biblio	77	3u	1	1	0	2	0	0	0	5
	Amphi	3	2u	1	1	1	0	0	0	0	1
	Salle TD+Salle Cours + Salle TP	98	4u	1	1	1	2	0	0	0	6
Total		**1651**		**14**	**12**	**9**	**34**	**5**	**1**	**1**	**74**

- **Le coût de la solution proposée :**

Tableau II.11 Tableau des couts de la solution choisie

Désignation	Unité	Quantité	Prix Unité (Da)	Prix totale
1. MATERIEL PASSIF CUIVRE:				
Goulotte 100x50	Ml	350	365.00	**127 750.00**
Goulotte 20x40	Ml	250	275.00	**68 750.00**
Câble FTP 4 paires catégorie 6 classe A	Ml	49530	120.00	**5 943 600.00**
Prises informatiques Prise RJ45 catégorie6 FTP	U	1651	2 000.00	**3 302 000.00**
Cordons de brassage FTP RJ45/RJ45 de 1 m catégories 6 classe A	U	1651	650.00	**1 073 150.00**
2. MATERIEL PASSIF FIBRE				
Tiroir Optique OM3 pour 12 connecteurs sc/sc duplex	U	15	9 117.00	**136 755.00**
Coupleur multimode sc duplex	U	132	137.00	**18 084.00**
Connecteur multimode sc duplex	U	132	400.00	**52 800.00**

Jarretière optique multimode OM3 2 mètres duplex sc/lc	U	66	2 416.00	**159 456.00**
Jarretière optique multimode OM3 2 mètres duplex lc/lc	U	23	2 568.00	**59 064.00**
Fibre multimode OM3 de 12 brins entre le bloc de labo de recherche et bureaux des enseignants (faculté des sciences	MI	80	525.00	**42 000.00**
Fibre multimode OM3 de 8 brins entre le bloc de bureau d'enseignant et salles TD+ amphis (faculté des sciences)	Ml	100	525.00	**52 500.00**
Fibre multimode OM3 de 12 brins entre le bloc Administration et Bibliothèque (faculté des sciences)	Ml	110	525.00	**57 750.00**
Fibre multimode OM3 de 4 brins entre le bloc Amphis et bloc bureaux d'enseignants (faculté de sociologie)	Ml	50	320.00	**16 000.00**
Fibre multimode OM3 de 8 brins entre le bloc des salles td+labo tp et bureaux d'enseignants (faculté de sociologie)	Ml	400	525.00	**210 000.00**
Fibre multimode OM3 de 8 brins entre le bloc bibliothèque et administration (faculté de sport).	Ml	200	525.00	**105 000.00**
Fibre multimode OM3 de 4 brins entre le bloc Amphis et bloc d'administration (faculté de sport)	Ml	320	525.00	**168 000.00**
Fibre multimode OM3 de 8brins entre le bloc de salle TD +TP et le bloc administration (faculté de sport)	Ml	350	320.00	**112 000.00**
Fibre multimode OM3 de 8 brins entre le bloc Administration de la faculté des sciences et le bloc administration du faculté de sociologie lien redondant	MI	100	525.00	**52 500.00**
Fibre multimode OM3 de 8 brins entre le bloc bureaux d'enseignants de la faculté des sciences et le bloc administration du faculté de sociologie lien redondant	MI	250	525.00	**131 250.00**
Fibre multimode OM3 de 8 brins entre le bloc bureaux d'enseignants de la faculté de sociologie et le bloc administration du faculté de sociologie lien redondant	MI	120	525.00	**63 000.00**
Fibre multimode OM3 de 8 brins entre le bloc Administration de la faculté de sport et le bloc administration de la faculté de sociologie lien redondant	MI	300	525.00	**157 500.00**
3. MATERIEL PASSIF				
Baies de brassage informatique 8U avec 02 ventilateurs	U	01	52 878.00	**528 78.00**

Baies de brassage informatique 6U avec 02 ventilateurs	U	04	43 000.00	**172 000.00**
Baies de brassage informatique 5U avec 02 ventilateurs	U	02	43 000.00	**86 000.00**
Baies de brassage informatique 4U avec 02 ventilateurs	U	03	34 643.00	**103 929.00**
Baies de brassage informatique 3U avec 1 ventilateur	U	02	23 112.00	**46 224.00**
Baies de brassage informatique 2U avec 1 ventilateur	U	02	18 220.00	**36 440.00**
Panneaux de brassage 24 ports RJ45 catégorie 6 classe A, connecteur accessible par la face avant.	U	80	15 195.00	**1 215 600.00**
Bandeau d'alimentation 08Prises + Disjoncteur + para foudre	U	14	6 050.00	**84 700.00**
Onduleur on line 3000 VA rackable + Carte SNMP	U	14	65 000.00	**910 000.00**
Switch de distribution /24 port+ 4 module SFP	U	5	310 000.00	**1550 000.00**
Switch d'acces/24 port+ 2 module SFP	U	09	71 000.00	**639 000.00**
Switch d'accés /48 port+ 2 module SFP	U	34	180 000.00	**6 120 000.00**
Switch core 24 port SFP	U	1	755 882.00	**755 882.00**
Pare-feu	U	01	900 000.00	**900 000.00**
Modules Gbic 1000 Base XX lc/upc	U	112	15 600.00	**1 747 200.00**
Controleur point d'accés	U	01	178 000.00	**178 000.00**
Point d'accés	U	30	25000.00	**750 000.00**

Serveur	U	6	720 000.00	**4 320 000.00**
Cout total				**31776762.00**

- **Les avantages**
  - Scalabilite
  - La redondance
  - Performance
  - Sécurité
  - Administration facile
  - La facilité de maintenance
- **Les inconvénients**
  - la configuration est un peu compliquée

II.2.4.3. Comparaison entre les différentes propositions

Tableau II.12 prix totale pour chaque solution

Proposition	Solution normalisée	Solution basique	Solution proposée
Prix total	**34 233 591.00**	**28 270 034.00**	**31 776 762.00**

La solution normalisé c'est une bonne solution pour un réseau universitaire elle permet d'obtenir une bonne vitesse pour la circulation du données et une très bonne disponibilité, le niveau de la sécurité et aussi élevé, elle assure une redondance entre les différents départements mais aussi elle est très couteuse et le budget du projet ne nous permet pas de la mettre en œuvre.

Par contre la solution basique en terme du budget elle est réalisable et moins chère mais elle n'est pas recommandé vu qu'elle ignore plusieurs aspects technique (la qualité, la sécurité..).

Donc elle nous reste la solution mixte qui combine les deux autres propositions et leur avantage c'est que est une solution réalisable et respecte le budget du notre projet.

II.2.5. Construction de cahier de charge

II.2.5.1. Description de la partie passive

II.2.5.1.1. Classes d'application et Bandes Passantes

Les normes définissent deux types de liaisons :

- **Le Lien (LINK) :** représente le câblage générique, il est constitué d'un câble horizontal de 90m maximum, il a été défini comme étant la portion du canal situées entre la première connectique de brassage et la prise terminale.
- **Le canal (CHANNEL) :** Il est constitué de l'ensemble du matériel de câblage compris entre le terminal utilisateur et l'équipement électronique installé dans le répartiteur d'étage. IL représente le support entre les deux systèmes électroniques : la carte réseau dans le PC ou station et le concentrateur installé dans le répartiteur d'étage. Sa longueur maximale est de 100m.

II.2.5.1.1.1. Classes d'applications

Le standard ISO définit les exigences minimales d'installation d'un système de câblage numérique. Cinq classes ont été identifiées, dont quatre pour le câble à paires torsadées en cuivre. Les critères et les conditions que doivent respecter les liens pour pouvoir supporter les applications sont :

- **Classes A** : application à Basses fréquences (Jusqu'à 100KHZ)
- **Classes B** : Application moyen débit (Jusqu'à 1MHZ)
- **Classes C** : Application haut débit ((Jusqu'à 16MHZ)
- **Classes D** : Application très haut débit (Jusqu'à 100MHZ)

Classes FO n'a pas en générale une limite pour la BP des appareils utilisés dans un système de câblage, pour la connexion en câble cuivre, l'exigence de la qualité de transmissions est exprimée principalement par la valeur de L'ACR.

Nous préconisons, l'utilisation de la nouvelle classe D, pour le câblage cuivre. Tous les liens existant devront être au moins de cette classe.

II.2.5.1.1.2. Câblage

Le système de câblage doit être indépendant de l'équipement de transmission utilisé (Ordinateur, Station, Imprimante) ainsi que le protocoles (ETHERNET, Fast Ethernet, TCP/IP, Token Ring), et cela en tenant compte de la demande toujours croissante en BP. Tous les

éléments du canal (câble horizontal, Prise brassage, prise terminal, cordons de brassage) doivent être de Catégorie 6

Les caractéristiques suivantes doivent être spécifiées lors des tests :

- NEXT
- PSNAXT
- ATTÉNUATION
- ELFEXT
- PEELFEXT
- TETURN LOSS
- TEMPS DE PROPAGATION
- DELAI DE PROPAGATION
- ACR
- PSACR

A cet effet, nous insistons sur le fait qu'un grand soin doit être pris lors de la pose et de la connexion des câbles et cela selon toutes les règles de l'art qui s'imposent.

Véhiculer des signaux 1000 Mhz sur du cuivre (tel que Gigabit Ethernet), impose un respect strict et rigoureux des normes. Pour cela certaines précautions doivent être prises durant la pose du câble, à savoir :

- Un câble ne se dévide pas, il se déroule.
- Respecter le rayon de courbure lors de la pose du câble.
- Eviter au maximum que le câble se bloque ou se coince.
- Eviter de donner les coups de fouet en cas de blocage.
- Les colliers de fixation ne doivent pas écraser la gaine du câble.
- Ne jamais marcher sur le câble.
- Eviter les arêtes vives.
- Couper les câbles sur longueurs plutôt que les lover.

L'installateur doit remettre lors de la livraison du matériel les fiches techniques de tous les produits utilisées en particulier :

- ✓ Le câble
- ✓ Les cordons de brassages
- ✓ Les connecteurs RJ45

II.2.5.1.1.3. Protocoles réseau

Le câblage installé devra au moins supporter la série des standards 8802.xet en particulier les protocoles suivants :

- 100 Base TX
- 1000 Base TX
- Gigabit Ethernet
- 10Gigabit Ethernet

II.2.5.1.2. Les éléments Passifs

II.2.5.1.2.1. Topologie physique

La topologie physique des raccordements et du type hiérarchique, cette topologie permet de réaliser un réseau avec plusieurs topologies logiques, d'autres architectures et protocoles par l'ajout ou le changement d'éléments actifs. L'interconnexion d'éléments actifs. L'interconnexion des sites par fibre optique mono mode Armé avec un minimum de huit (08) brins.

II.2.5.1.2.2. Armoire de brassage

Pour un assemblage standard des panneaux de brassages et des autres équipements, prévoir des châssis normalisés 19'' équipés de deux montants latéraux, ceux-ci doivent être :

- Suffisamment ventilée.
- Totalement vitrée à l'avant.

Equipée d'une barrette d'alimentation d'au moins 08 prises, d'un disjoncteur différentiel et d'une connexion constante au conducteur de protection de la terre.

II.2.5.1.2.3. Eléments de brassage

a. Tiroirs optiques

C'est un support normalisé 19'' avec une unité de hauteur. Il devra permettre de recevoir des prises. Il est préférable qu'il soit accompagnées d'accessoires de câblage appropriés tels que les bobines de lovage, les colliers, passes fils…) Une étiquette d'identification doit être placée en face de chaque port permettant ainsi de situer les points d'affectation du câble.
Les jarretières optiques seront du type multimode LC/SC et de type LC/LC selon le matériel actif prévu.

b. Panneaux de brassage

Ils doivent être :

- ✓ Equipés de RJ45 FTP de catégorie 6 a.
- ✓ Système modulaire avec face arrière équipée d'un organisateur de câbles.
- ✓ Montage et démontage des embases par l'avant du panneau.

Chaque panneau de brassage doit être associés à un panneau guide câble, permettant ainsi d'assurer un cheminement correct des câbles

Les cordons de brassage doivent être flexibles de type FTP conformes à la catégorie 6 en général et la catégorie 6a spécialement.

II.2.5.1.2.4. Les Connecteurs RJ

Les prises doivent être de type RJ45 FTP Catégorie 6a. Pour une performance optimale du réseau et pour assurer un fonctionnement à haut débit, les connecteurs RJ45 installés sur la prise doivent être identiques à ceux montés sur les panneaux de brassage.

Les prises RJ45 doivent être du type à sertir (Sans soudure ni circuit imprimé), elles doivent permettre le contrôle du dépairage.

Les caractéristiques de diaphonie (NEXT et FEXT) sont particulièrement sensibles au torsadage des paires, aussi au minimum de dépairage doit être observé à la connexion, celui-ci ne doit jamais dépasser 13 mm comme régit par les normes.

Les prises doivent disposées d'une coquille de blindage à une seule pièce, pour assurer une bonne continuité de masses. La reprise du blindage doit se faire sur 360°.

Le respect du rayon de courbure du câble (25mm min) est lui aussi un facteur important garantissant les performances de la connexion

Les prises doivent avoir la possibilité :

- ❖ D'être démontées et remontées (en cas d'erreur de câblage) sans diminution de leurs caractéristiques
- ❖ D'être facilement raccordées
- ❖ De permettre aisément la vérification du codage couleur utilisé

Les connecteurs et/ou les supports doivent être identifiés et étiquetés d'une manière unique et visible pour l'utilisateur.

II.2.5.1.2.5. Canalisation Des Bureaux

A l'intérieur des bureaux, il convient d'utiliser une goulotte d'installation en PVC rigide, antichoc et résistance aux agents chimiques, lors de son installation on veillera à préserver au maximum l'esthétique des locaux.

La goulotte doit être munie d'accessoires assurant le respect des rayons de courbures (25mm min).

Afin d'assurer l'esthétique de l'installation, la totalité des conduits doit être réalisé à l'aide de la même gamme de produits.

II.2.5.1.2.6. Canalisation Faux Plafonds

L'acheminement des câbles cuivre à l'intérieur de faux plafond doit se faire dans des gaines en ressort (entre chemin de câble et le bureau) selon les règles qui s'imposent permettant ainsi une protection convenable des câbles

II.2.5.2. Description de la partie active

II.2.5.2.1. Description technique du Switch Fédérateur

Le Switch fédérateur c'est un commutateur très performant elle est une capacité de connecter plusieurs appareils comme les téléphones IP, les points d'accès sans fil, les stations de travail et d'autres périphériques réseau, tels que des serveurs, des routeurs, ainsi que d'autres commutateurs

❖ Fiche technique du switch fédérateur

- Type de périphérique : Commutateur - 12 ports - C3 - Géré - empilable
- Type de boîtier : Montable sur rack 1U
- Sous-type : 10 Gigabit Ethernet
- Ports : 12 x 1 Gigabit / 10 Gigabit SFP+
- Performances : Capacité de commutation: 320 Gbits/s ¦ Bande passante d'empilage: 480Gbps

- Capacité : Routes IPv4: 24000 ¦ Entrées NetFlow: 24000 ¦ Interfaces virtuelles (VLAN): 4000 ¦ Interfaces virtuelles commutées (SVI): 1000
- Taille de la table d'adresses MAC : 32 000 entrées
- Support de cadre Jumbo : 9198 octets
- Protocole de Routage : IS-IS, RIP-1, RIP-2, IGMPv2, IGMP, IGMPv3, routage à base de règles (PBR), RIPng, MLDv2, MLD
- Normes de conformité : IEEE 802.3z, IEEE 802.1D, IEEE 802.1Q, IEEE 802.1p, IEEE 802.3x, IEEE 802.3ad (LACP), IEEE 802.1w, IEEE 802.1x, IEEE 802.1s
- Alimentation : CA 120/230 V (50 - 60 Hz)

❖ Caractéristiques du Module transmetteur SFP+ 10 GBase-SR - LC/PC multimode

- Description du produit : module transmetteur
- Type de périphérique : Module transmetteur SFP+
- Facteur de forme : Module enfichable
- Type d'interface (bus) : 1 x Ethernet 10GBase-SR - LC/PC multi-mode x 2
- Type de câblage : 10GBase-SR
- Protocole de liaison de données : 10 GigE
- 400 m : Distance de transfert maximum
- 10 Gbits/s : Débit de transfert de données
- IEEE 802.3ae : Conformité aux normes [9]

Deux cartes à 48 ports RJ45 seront installées afin de connecter les utilisateurs du bloc administration au réseau local.

Un système en double alimentation électrique est prévu pour l'alimentation du châssis.

II.2.5.2.2. Description technique du Switch de distribution

Ces commutateurs intelligents apportent aux postes de travail une connectivité FastEthernet et Gigabit Ethernet, optimisent les services de LAN sur les réseaux d'entreprise, intermédiaires et les réseaux de succursale. Ils offrent une sécurité intégrée avec contrôle de l'admission sur le réseau (NAC), qualité de service (QoS) évoluée et résilience, pour distribuer des services intelligents à la périphérie du réseau.

❖ Fiche technique du switch de dustribution

- Type de périphérique : Commutateur
- Type de boîtier : Montable sur rack 1U
- Sous-type : 10 Gigabit Ethernet
- Ports : 4 x 1 Gigabit / 10 Gigabit SFP+
- Performances : Capacité de commutation: 92 Gbits/s ¦ Bande passante d'empilage: 480 Gbps
- Capacité : Routes IPv4: 24000 ¦ Entrées NetFlow: 24000 ¦ Interfaces virtuelles (VLAN): 4000 ¦ Interfaces virtuelles commutées (SVI): 1000
- Taille de la table d'adresses MAC : 32 000 entrées
- Support de cadre Jumbo : 9198 octets
- IEEE 802.1D Spanning Tree Protoco ,IEEE 802.1p CoS Prioritization , IEEE 802.1Q VLAN , IEEE 802.1s ,IEEE 802.1w , IEEE 802.1X , IEEE 802.1X-Rev ,IEEE 802.11 ● IEEE 802.1ab (LLDP) , IEEE 802.3ad , IEEE 802.3x full duplex on 10BASE-T, 100BASE-TX, and 1000BASE-T ports , IEEE 802.3 10BASE-T , IEEE 802.3u 100BASE-TX , IEEE 802.3ab 1000BASE-T , IEEE 802.3z 1000BASE-X , RMON I and II standards , SNMP v1, v2c, and v3
- Alimentation : CA 100/240 V (50 - 60 Hz)

❖ Avantages

- Fonctionnalités intelligentes à la périphérie du réseau, par exemple des listes de contrôle d'accès (ACL) élaborées et une sécurité optimisée
- Liaisons ascendantes à deux fonctions favorisant la flexibilité de la liaison montante Gigabit Ethernet et permettant d'utiliser du cuivre ou de la fibre optique. Chaque port de liaison ascendante à deux fonctions offre un port10/100/1000 Ethernet et un port Gigabit Ethernet SFP (Small Form – Factor Pluggable), un seul étant actif à la fois.
- Contrôle du réseau et optimisation de la bande passante grâce aux fonctions de qualité de service évoluée, de limitation granulaire du débit, de listes de contrôle d'accès et de services multicast

- Sécurité du réseau assurée par une série de méthodes d'authentification, des technologies de cryptage des données et le contrôle des admissions sur le réseau basé sur les utilisateurs, les ports et les adresses MAC
- Simplicité de la configuration réseau, des mises à niveau et du dépannage grâce au logiciel Cisco Network Assistant
- Configuration automatique des applications spécialisées à l'aide de Smart ports

II.2.5.2.3. Description technique du Switch d'accés

❖ Fiche technique du switch d'accès 24 ports 10/100/1000,4 T/SFP

RAM: 128 Mo Mémoire flash: 64 Mo

Quantité de ports Ethernet RJ-45 de commutation de base : 24

Quantité de ports Combo SFP : 4

Taux de transfert de paquets : 35,7 Mpps

Protocole de liaison de données : Ethernet, Fast Ethernet

Ports réseau auxiliaires : 44 ports 10/100/1000Base - T à 4 liaisons ascendantes à deux fonctions présente un port Ethernet 10/100/1000 et un port SFP, 1 seul port actif à la fois.

Protocole de gestion à distance : SNMP 1, RMON, Telnet, SNMP 3, SNMP 2c

Mode de communication : full duplex

Caractéristiques : Niveau 4 switching, Niveau 3 switching, Niveau 2 switching, IGMP snooping

Alimentation CA 120/230 V (50/60 Hz) [9]

❖ Fiche technique du Switch d'accès : 24 Port 10 Go, 2T/SFP

RAM : 128 Mo Mémoire flash : 64 Mo

Quantité de ports Ethernet RJ-45 de commutation de base : 24

Quantité de ports Combo SFP : 2

Nombre de Vilans : 255

Taux de transfert de paquets : 4,4 Mpps

Protocole de liaison de données : Ethernet, Fast Ethernet

Ports réseau auxiliaires : 2x10/100/1000Base -T/SFP (mini - GBIC) (uplink)

Protocole de gestion à distance : SNMP 1, RMON, Telnet, SNMP 3, SNMP 2c

Mode de communication : full duplex

Caractéristiques : Niveau 4 switching, Niveau 3 switching, Niveau 2 switching, IGMP snooping Alimentation CA 120/230 V (50/60 Hz) [9]

- Fiche technique du switch d'accés 48 ports Go + 2 uplink T/SFP

RAM : 128 Mo Mémoire flash : 64 Mo

Quantité de ports Ethernet RJ-45 de commutation de base : 48

Quantité de ports Combo SFP : 2

Nombre de VLANs : 255

Taux de transfert de paquets : 10,1 Mpps

Protocole de liaison de données : Ethernet, Fast Ethernet

Ports réseau auxiliaires : 2x10/100/1000Base - T/SFP (mini - GBIC) (uplink)

Protocole de gestion à distance : SNMP 1, RMON, Telnet, SNMP 3, SNMP 2c

Caractéristiques : Niveau 4 switching, Niveau 3 switching, Niveau 2 switching, IGMP snooping Alimentation CA 120/230 V (50/60 Hz) [9]

II.2.5.2.4. Description technique de la Firwall

Type de périphérique : Dispositif de sécurité

RAM installée : 1.25 Go

Mémoire flash installée : 320 Mo

Facteur de forme : Montable sur rack

Technologie de connectivité : Filaire

Protocole de liaison de données : Ethernet, Fast Ethernet, Gigabit Ethernet

Protocole réseau / transport : IPSec

Performances : Rendement du firewall 300 Mbps ¦ Débit de firewall + services anti-x 150 Mbps ¦ Rendement du VPN 170 Mbps

Capacité : Homologues VPN IPSec 250 ¦ Homologues VPN SSL 2 ¦ Sessions simultanées 50000

Caractéristiques : Protection par firewall, Prise en charge VPN, prise en charge du réseau local (LAN) virtuel

Algorithme de chiffrement : DES [9]

II.2.5.2.5. Description technique du serveur

Gamme de processeurs Intel® Xeon® E5-2600 v4

Sockets de processeur : 2

Disponibilité :

- Mémoire ECC
- Technologie SDDC (correction des données pour un seul périphérique)
- Rangée de mémoire de réserve
- Disques durs enfichables à chaud
- Blocs d'alimentation redondants enfichables à chaud
- Contrôleur iDRAC8 avec Lifecycle Controller
- Prise en charge de la mise en cluster haute disponibilité
- Prêt pour la virtualisation
- Double module SD interne (hyperviseur Failsafe)
- Module TPM 1.2

Stockage: SAS, SATA, SAS NearLine, SSD [9]

Noyau processeur disponible : 8

Mémoire cache du processeur : L3 20 Mo

Vitesse minimale du processeur : 2,2 GHz

Format (entièrement configuré) : 1U

Châssis format : Rack

Alimentation électrique : 2x500W

Mémoire : 120 Go / CC / 2133 MHz / PC4-17000 / DDR4 SDRAM

Description du lecteur : 8 Lecteurs SAS/SATA/SSD

II.2.5.2.6. Description du Switch 24 ports Gigabit smart PoE

Interface: 24 10/100/1000Mbps RJ45 Ports, Auto Negotiation/Auto MDI/MDIX), 4 Combo 100/1000Mbps SFP Slots

Interface réseau : 10BASE-T: UTP category 3, 4, 5 ,6 câble (maximum 100m)

100BASE-TX/1000Base-T: UTP category 5, 5e, 6 or above cable (maximum 100m), 1000BASE-X: MMF, SMF

Nombre de ventilateurs : 3

Alimentation : 100~240VAC, 50/60Hz

Consommation Maximum (PoE on) : 216W (220V/50Hz)

Maximum (PoE off): 36W (220V/50Hz)

Ports PoE+ (RJ45): Standard: 802.3at/af Compliant, PoE+ Ports: 24 Ports

Power Supply: 180W

Bande passante : 48 gbps

Tableau addresses MAC: 8k

Caractéristiques :

Support 802.1p CoS/DSCP priority

Support 4 priority queues

Queue scheduling: SP, WRR, SP+WRR

Port/Flow- based Rate Limiting

Voice VLAN

Supports up to 512 VLANs simultaneously (out of 4K VLAN IDs) [9]

II.2.5.2.7. Description technique du Switch 48 ports Gigabit smart PoE

Interface: 48 10/100/1000Mbps RJ45 Ports (Auto Negotiation/Auto MDI/MDIX)

Interface reseau: 10BASE-T: UTP category 3, 4, 5, 6 cable (maximum 100m) 100BASE-TX/1000BASE-T: UTP category 5, 5e, 6 or above cable (maximum 100m)

Nombre de ventilateurs : 2

Alimentation : 100-240VAC, 50/60Hz

Consommation : Maximum : 29.8W (220V/50Hz)

Capacity de commutation: 96Gbps

Tableau addresses MAC: 8k

Caractéristiques :

Support 802.1p CoS/DSCP priority

Support 4 priority queues

Queue scheduling: SP, WRR, SP+WRR

Port/Flow- based Rate Limiting

Voice VLAN

Supports up to 512 VLANs simultaneously (out of 4K VLAN IDs)

II.2.6. Conclusion

Dans ce chapitre, nous avons fait une étude approfondie sur le nouveau pôle de Ouezra, afin de garantir une bonne conception aux clients.

En se basant sur cette étude, nous avons proposé deux solutions différentes pour le câblage et le matériel utilisé, et même pour l'architecture réseaux en se basant sur le cout dans la première solution, et sur la qualité dans la deuxième solution. Ensuite nous avons essayé de proposer une troisième solution plus optimale qui garantit la qualité et le cout au même temps.

Chapitre III

Architecture et sécurité du réseau



III.1. Introduction

Dans ce chapitre on présente brièvement quelques notions théoriques utiles dans un réseau local qu'on vise à appliquer dans notre solution et on définit les protocoles et les mécanismes utilisés. On commence par les protocoles au niveau 02 (commutation) et ensuite la sécurité au niveau 02 en plus la solution firewall et enfin la solution wifi.

III.2. Les protocoles LAN

III.2.1. Les Virtual LAN, VLAN

III.2.1.1. Définition

Un VLAN (Virtual Local Area Network ou Virtual LAN) est un réseau local regroupant un ensemble de machines utilisant la technologie Ethernet pour regrouper les éléments du réseau (utilisateurs, périphériques, etc.) selon des critères logiques (fonction, partage de ressources, appartenance à un département, etc.), sans se heurter à des contraintes physiques (dispersion des ordinateurs, câblage informatique inapproprié, etc.). [10]

III.2.1.2. Typologies des VLANs

On distingue généralement trois techniques pour construire des VLAN, en fonction de leurs méthodes de travail, nous pouvons les associer à une couche particulière du modèle OSI

III.2.1.2.1. VLAN de niveau 1 ou VLAN par port

On affecte chaque port des commutateurs à un VLAN. Les ports sont donc affectés statiquement à un VLAN.

Si on déplace physiquement une station il faut désaffecter son port du VLAN puis affecter le nouveau port de connexion de la station au bon VLAN. Si on déplace logiquement une station (on veut la changer de VLAN) il faut modifier l'affectation du port au VLAN. [10]

III.2.1.2.2. VLAN de niveau 2 ou VLAN MAC

On affecte chaque adresse MAC à un VLAN. En fait il s'agit, à partir de l'association Mac/VLAN, d'affecter dynamiquement les ports des commutateurs à chacun des VLAN en fonction de l'adresse MAC de l'hôte qui émet sur ce port.

L'intérêt principal de ce type de VLAN est l'indépendance vis-à-vis de la localisation géographique. Si une station est déplacée sur le réseau physique, son adresse physique ne changeant

pas, elle continue d'appartenir au même VLAN (ce fonctionnement est bien adapté à l'utilisation de machines portables). [10]

III.2.1.2.3. VLAN de niveau 3 ou VLAN d'adresses réseaux

On affecte une adresse de niveau 3 à un VLAN. L'appartenance d'une trame à un VLAN est alors déterminée par l'adresse de niveau 3 ou supérieur qu'elle contient. En fait, il s'agit à partir de l'association adresse niveau 3/VLAN d'affecter dynamiquement les ports des commutateurs à chacun des VLAN.

Dans ce type de VLAN, les commutateurs apprennent automatiquement la configuration des VLAN en accédant aux informations de couche 3. Ceci est un fonctionnement moins rapide que le VLAN de niveau 2.

III.2.2. Protocole VTP

III.2.2.1. Définition

VTP est chargé de gérer les VLANs d'une manière centralisée et évite ainsi aux administrateurs du réseau de se connecter autant de fois qu'il y a de commutateurs dans un réseau pour ajouter, modifier ou supprimer la configuration d'un appelé serveur VTP, afin de distribuer ces informations de configuration VLAN d'un bout à l'autre du réseau commuté. Un tel protocole réduit les délais d'administration et de maintenance des réseaux VLAN. A noter que ce protocole s'applique au niveau de la couche liaison de données du modèle OSI. [11]

III.2.2.2 Principe de fonctionnement

Le protocole VTP définit la notion de domaine VTP. Un domaine VTP est composé d'un ou plusieurs équipements interconnectés qui partagent le même nom. Il regroupe des commutateurs pour qu'ils échangent leurs informations de configurations envoyés par le serveur VTP de chaque domaine concerné et plusieurs domaines VTP peuvent cohabiter dans le même réseau local.

Dans un environnement VTP, un commutateur peut assurer un des trois rôles qui définissent les trois modes de fonctionnement suivants :

III.2.2.2.1. Mode serveur VTP

Un commutateur en mode serveur est chargé de diffuser la configuration aux commutateurs du domaine VTP en envoyant des messages connus sous le nom « trames VTP », c'est le seul

commutateur du domaine capable d'ajouter, supprimer ou renommer des VLAN dans le domaine VTP concerné.

III.2.2.2.2. Mode client VTP

Un commutateur en mode client est chargé d'appliquer la configuration émise par un commutateur en mode serveur, ce mode ne donne pas la possibilité de créer, modifier ou supprimer des informations VLAN. [12

III.2.2.2.3. Mode transparent VTP

Un commutateur en mode transparent ne fait que diffuser les annonces VTP et les configurations du domaine VTP auquel il appartient. Donc, le commutateur transparent joue le rôle d'un intermédiaire de communication pour permettre aux clients VTP d'échanger les informations de configuration VLAN avec le serveur VTP.

III.2.3. Trafic Inter-VLAN

Le trafic Inter-VLAN est assuré par un équipement de niveau 3 (routeur/ multi-layer switch). En effet pour que les machines puissent communiquer d'un VLAN à un autre, il est nécessaire de passer par un routeur en subdivisant logiquement l'interface liée au commutateur en sous-interfaces virtuelles, telle que, chaque sous-interface est attribuée à un VLAN donné. Le nombre des sous-interfaces à créer, est lié au nombre de VLANs existants. Ces sous-interfaces fournissent une solution pour le routage entre les différents VLANs. Le concept d'agrégation ou bien le trunk est indispensable, il consiste à regrouper plusieurs liaisons virtuelles sur une liaison physique unique, la fonction d'un trunk est de transporter les informations des VLANs entre plusieurs commutateurs interconnectés et donc d'étendre la portée des VLANs à un ensemble de commutateurs.

Les interfaces entre le commutateur distribution (SW-Dist) et tous les commutateurs Accès (SW-Accès), ainsi que l'interface entre le SW-Dist et le router, doivent être toutes configurées en mode trunk, afin qu'elles puissent transporter les informations des différents VLANs. [12]

III.2.4 Protocol STP (Spanning Tree Protocol)

Une topologie redondante vise à éliminer les risques de pannes du réseau provoquées par un composant unique pour améliorer leur fiabilité. [13]

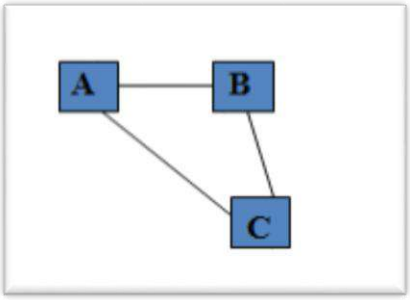


Figure III.1 Différents Chemins

III.2.4.1. Problèmes

III.2.4.1.1. Tempête de broadcast

Si une station reliée au switch A envoie une trame Broadcast alors :

- Le switch A l'envoi sur tous ces ports
- Les switches C et B reçoivent la trame et puisque c'est une trame de broadcast alors ils la diffusent sur tous leurs ports.
- Le switch A va recevoir de nouveau la trame et il va refaire le même travail. [14]

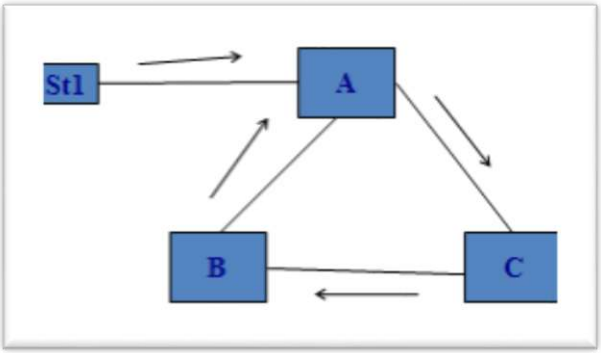


Figure III.2 Tempête de broadcast

III.2.4.1.2. Réception multiple d'une trame

Dans le schéma qui suit, il est tout à fait possible que le matériel B (Poste B) reçoive via le commutateur A et le commutateur B la même trame en provenance du poste A. Les matériels ne sont pas capables de gérer ce type de communication d'où une perturbation importante des communications.

III.2.4.1.3. Instabilité de la table des adresses Mac

Dans le cas où la trame est dupliquée et transite du poste A vers le commutateur A en passant par son port 0 et si dans le même temps, cette trame est envoyée du commutateur B vers le commutateur A sur son port 1. Alors, la table des adresses MAC du commutateur A va constamment se remettre à jour en indiquant une fois sur 2 (lors de l'envoi par le commutateur B) un port erroné ou du moins non optimum.

III.2.4.2. Solution spanning tree

Pour éviter ces phénomènes, il est nécessaire de mettre en place un processus de suppression des boucles de façon logique : le spanning tree (STP).

Ce protocole travaille au niveau 2 de la couche OSI et est implémenté généralement sur les commutateurs, ponts et routeur (matériels pontés). Historiquement créé par DEC (Digital Equipment Corporation), l'algorithme est ensuite normalisé par l'IEEE sous la dénomination 802.1d. Ce protocole permet d'éviter les boucles en bloquant certains ports sur les matériels précités et en les débloquant en cas de panne.

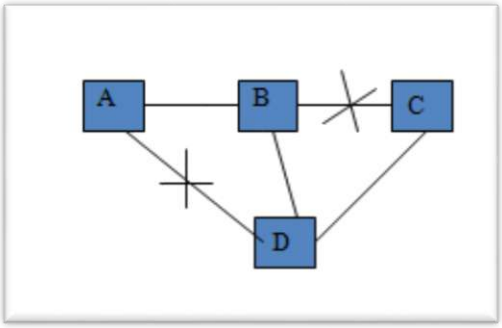


Figure III.3 réseaux avec STP

III.2.4.3. Bridge Protocol Data Unit (BPDU)

Le BPDU est la trame de message échangé par les commutateurs pour le protocole STP. Il contient une valeur de priorité, l'adresse MAC du commutateur émetteur et un ID du système étendu facultatif. La valeur BID la plus faible est déterminée par la combinaison de ces trois champs.

III.2.4.4. Rôle des ports

Dans le fonctionnement du STP, les ports commutateur (pont) peuvent jouer quatre rôles :

- **Ports racine :** Les ports de commutateur les plus proches de pont racine.

- **Ports désignés :** Tous les ports non racine qui sont autorisés à acheminer le trafic sur le réseau. Il transmet les trames.
- **Ports non désignés :** Tous les ports configurés dans un état de blocage pour empêcher la formation de boucles. Ce port ne transmet pas les trames.
- **Port désactivé :** est un port qui a été administrativement arrête. C'est un port qui ne rentre pas dans le processus du protocole STP. Ce port ne transmet pas les trames.

La figure suivante montre les types des ports existant dans le protocole STP

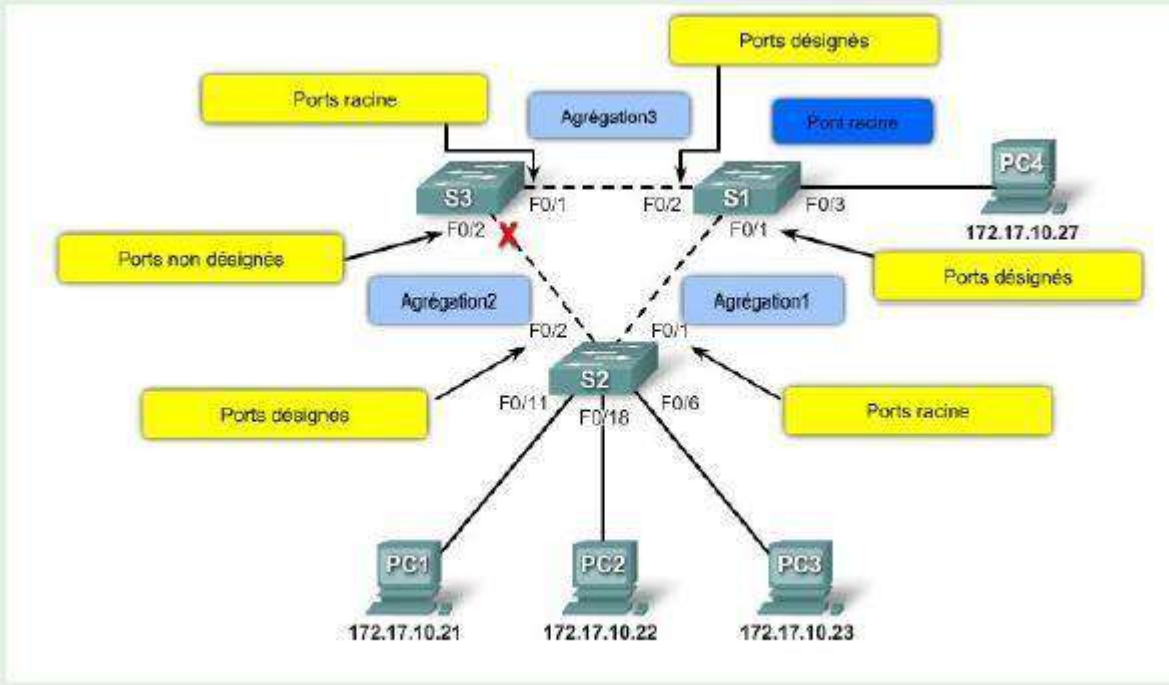


Figure III.4 Gestion des ports par le protocole STP

III.2.4.5. Types de protocoles STP

III.2.4.5.1. Le protocole Pvst+

Avec PVST+, il est possible pour le port trunk d'un commutateur d'être bloqué pour un VLAN donné, mais ouvert pour les autres VLAN. Le protocole PVST+ peut être utilisé pour implémenter l'équilibrage de la charge de couche 2. Étant donné que chaque VLAN utilise une instance distincte du protocole STP, les commutateurs d'un environnement PVST+ requièrent davantage de temps de traitement du processeur et de bande passante BPDU qu'une implémentation CST traditionnelle de STP.

Dans un environnement PVST+, les paramètres Spanning Tree peuvent être ajustés de manière à ce que la moitié des VLAN réacheminent les données sur chaque trunk de liaison ascendante. Dans cette figure, le port F0/3 de S2 est le port de réacheminement pour VLAN 20 et F0/2 de S2 est le port de réacheminement pour VLAN 10. Pour ce faire, un commutateur est configuré de manière à être défini comme pont racine pour la moitié des VLAN du réseau, et un second commutateur pour être défini comme pont pour l'autre moitié des VLAN. Dans la figure, S3 est le pont racine pour VLAN 20 et S1 est le pont racine pour VLAN 10. Définir plusieurs ponts racine STP par VLAN augmente la redondance du réseau.

Les réseaux utilisant PVST+ présentent les caractéristiques suivantes :

- Un équilibrage optimal de la charge peut être atteint.
- Une instance Spanning Tree pour chaque VLAN peut impliquer un gaspillage important en termes de cycles de processeur pour l'ensemble des commutateurs du réseau (outre la bande passante utilisée pour chaque instance afin d'envoyer sa propre trame BPDU). Cela peut être problématique si le réseau compte un grand nombre de VLAN. [15]

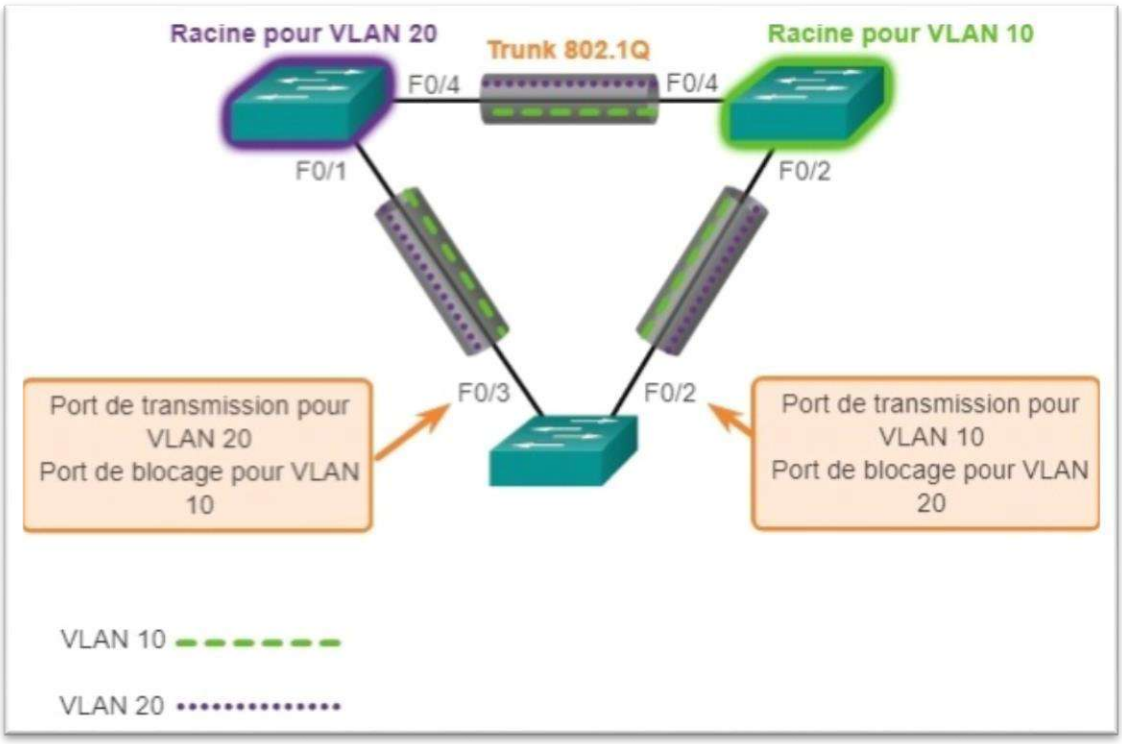


Figure III.5 Le protocole PVST+

III.2.4.5.2 Le protocole Rapid PVST+

Grâce à Rapid PVST+, une instance séparée de RSTP est exécutée sur chaque VLAN.

La figure ci-contre illustre un réseau fonctionnant sous RSTP. S1 est le pont racine, avec deux ports désignés en état de réacheminement. RSTP prend en charge un nouveau type de port : le port F0/3 sur S2 est un port alternatif en état de mise à l'écart. Notez que le réseau ne comporte aucun port en état de blocage. En effet, le protocole RSTP n'autorise pas l'état de blocage d'un port. Il définit les états suivants pour les ports : mise à l'écart (discarding), apprentissage ou acheminement.

Le protocole RSTP optimise le recalcule de l'arbre recouvrant lorsque la topologie d'un réseau de couche 2 change. Il assure un temps de convergence beaucoup plus rapide dans un réseau correctement configuré, parfois de l'ordre de quelques centaines de millisecondes. Il redéfinit le type des ports et leur état. Si un port est configuré en tant que port alternatif ou port de sauvegarde, il peut immédiatement passer à l'état de réacheminement sans avoir à attendre la convergence du réseau. Les caractéristiques du protocole RSTP sont décrites brièvement ci-dessous :

- Le protocole RSTP est le protocole le plus adapté pour garantir qu'il n'y a pas de boucles de couche 2 dans un environnement de réseau commuté. [16]

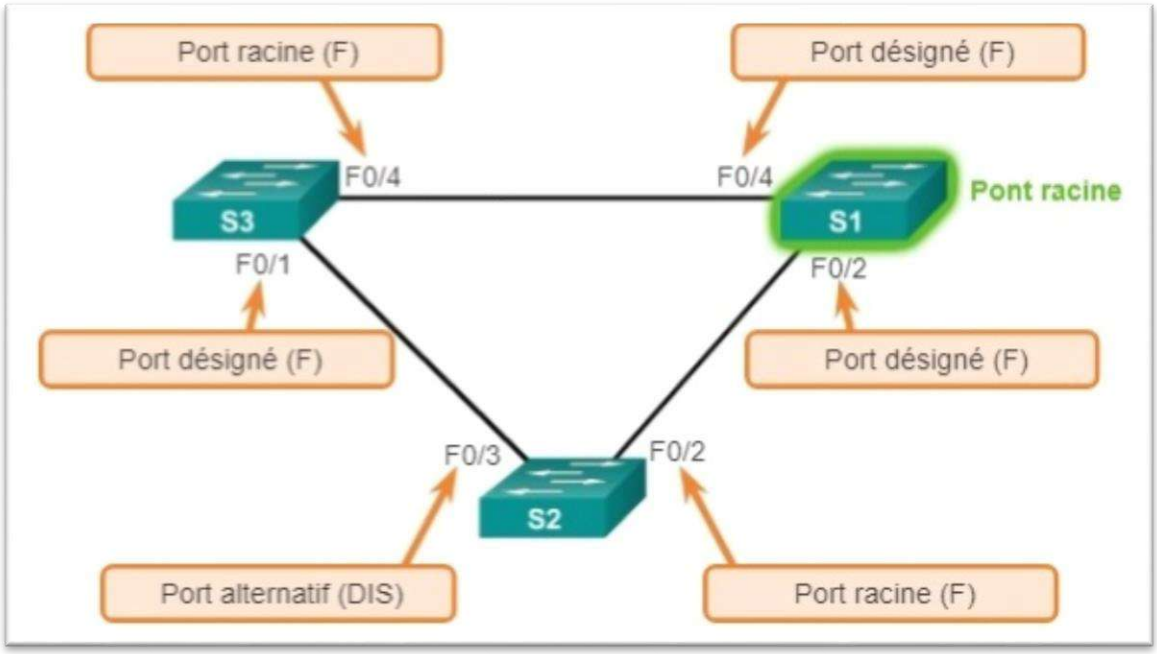


Figure III.6 Le protocol Rapid PVST+

III.2.5. Le protocole Etherchannel

Le mécanisme mis en œuvre pour grouper des ports sur les switchs Cisco est **Etherchannel** (nommé trunk chez d'autres constructeurs). Il s'agit de créer une interface logique (Port Channel x, x étant le numéro du port) associée à plusieurs ports physiques. Etherchannel se charge de :

- Faire du load balancing en répartissant le trafic sur les ports physiques.
- Faire renvoyant immédiatement le trafic sur un autre port du groupement si un port physique « tombe ».

Etherchannel permet aussi d'appliquer de façon globale des configurations sur tous les ports d'un même groupement

Pour qu'un groupement de ports fonctionne, il faut que tous les ports aient les mêmes caractéristiques (vitesse, full ou half duplex), et ce, en local sur le switch mais aussi sur l'équipement auquel le switch est raccordé. De plus, il va de soi que tous les ports d'un groupement appartiennent au même VLAN ou sont configurés 802.1q.

Etherchannel est une technologie qui fonctionne en autonome sur le switch. Deux équipements raccordés entre eux doivent avoir une configuration parfaitement symétrique sous peine de dysfonctionnement (attention aux boucles sur le réseau Ethernet).

En complément de Etherchannel, afin de rendre plus transparente la mise en place des mécanismes de groupement de ports, des protocoles existent pour que les équipements dialoguent entre eux afin de décider si un port peut faire partie d'un groupement. Ces protocoles sont les suivants :

- LACP (normalisé IEEE 802.3ad)
- PAGP (propriétaire Cisco)

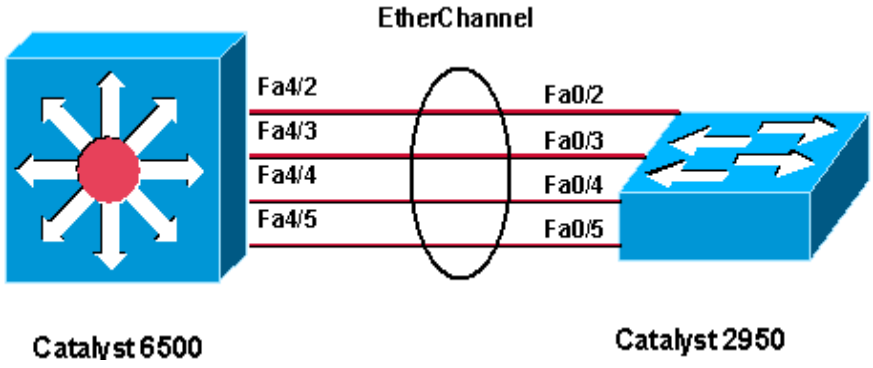


Figure III.7 Le protocole Etherchannel

III.2.6 Le protocole ARP

Le protocole de résolution d'adresse (ARP, Address Résolution Protocol) est un protocole effectuant la traduction d'une adresse de protocole de couche réseau (typiquement une adresse IPv4) en une adresse MAC (typiquement une adresse ethernet), ou même de tout matériel de Couche Il se situe à l'interface entre la couche réseau (couche 3 du modèle OSI) et la couche de liaison (couche 2 du modèle OSI).

III.2.7. Le protocole ICMP

Le protocole ICMP (Internet Control Message Protocol) est un protocole qui permet de gérer les informations relatives aux erreurs aux machines connectées. Etant donné le peu de contrôles que le protocole IP réalise, il permet non pas de corriger ces erreurs mais de faire part de ces erreurs aux protocoles des couches voisines. Ainsi, le protocole ICMP est utilisé par tous les routeurs, qui l'utilisent pour signaler une erreur (appelé : Delivery Problem).

III.2.8. L'adressage IP

III.2.8.1. L'adressage dynamique

III.2.8.1.1. Protocole DHCP

Le protocole DHCP (Dynamic Host Configuration Protocol) fournit une configuration dynamique des adresses IP et des informations associées aux ordinateurs configurés pour l'utiliser (clients DHCP). Ainsi chaque hôte du réseau obtient une configuration IP dynamiquement au moment du démarrage, auprès du serveur DHCP. Le serveur DHCP lui attribuera notamment une adresse IP, un masque et éventuellement l'adresse d'une passerelle par défaut.

Un serveur DHCP (Dynamic Host Configuration Protocol) a pour rôle de distribuer des adresses IP à des clients pour une durée déterminée.

III.2.8.1.2. Avantages de DHCP

- Le protocole DHCP offre une configuration de réseau TCP/IP fiable et simple, empêche les conflits d'adresses et permet de contrôler l'utilisation des adresses IP de façon centralisée**.** Ainsi, si un paramètre change au niveau du réseau, comme, par exemple l'adresse de la passerelle par défaut, il suffit de changer la valeur du paramètre au niveau du serveur DHCP.
- Les postes itinérants sont plus faciles à gérer.

III.2.8.2. L'adressage statique

III.2.8.2.1 La technique VLSM

Consiste à utiliser des sous –réseaux pour structurer le réseau. Il existe plusieurs raisons de diviser le réseau en sous-réseaux :

- L'emplacement physique
- Le regroupement logique
- La sécurité
- Les besoins en matière d'applications
- Le confinement des diffusions
- La conception de réseau hiérarchique

Par exemple, si une entreprise met en place un réseau 10.0.0.0, elle peut utiliser un schéma d'adresse du type 10.X.Y.0, où X représente un site géographique et Y un bâtiment ou un étage sur ce site. Ce schéma d'adresse permet : 255 sites géographiques différents, 255 bâtiments sur chaque site, 254 hôtes dans chaque bâtiment.

- **Processus de base de création de sous-réseau**

Avec un système d'adressage hiérarchique, il est possible de déterminer un grand nombre d'informations en examinant simplement une adresse IP et un masque de sous-réseau au format avec barre oblique (/x). Par exemple, une adresse IP de 192.168.1.75 /26 indique les informations suivantes :

- Masque de sous-réseau décimal
- /26 se traduit par le masque de sous-réseau 255.255.255.192.

- **Nombre de sous-réseaux créés**

Si, au début, nous avions le masque de sous-réseau par défaut /24, nous avons emprunté 2 bits d'hôtes supplémentaires pour le réseau. Ceci permet de créer 4 sous-réseaux (2^2 = 4).

- **Nombre d'hôtes utilisables par sous-réseau**

Il reste six bits côté hôte, permettant ainsi de créer 62 hôtes par sous-réseau (2^6 = 64 - 2 = 62).

- **Adresse réseau**

En utilisant le masque de sous-réseau pour déterminer l'emplacement des bits de réseau, on obtient la valeur de l'adresse réseau. Dans cet exemple, la valeur est 192.168.1.64.

Première adresse d'hôte utilisable

Les bits d'hôtes ne peuvent pas contenir uniquement des 0, car ces derniers représentent l'adresse réseau du sous-réseau. Par conséquent, la première adresse d'hôte utilisable dans le sous-réseau .64 est .65.

- **Adresse de diffusion**

Les bits d'hôtes ne peuvent pas contenir uniquement des 1, car ces derniers représentent l'adresse de diffusion du sous-réseau. Dans cette diffusion, l'adresse de diffusion est .127. 128 commence l'adresse réseau du sous-réseau suivant.

Système d'adressage : exemple de 4 réseaux

Sous-réseau	Adresse réseau	Plage d'hôtes	Adresse de diffusion
0	192.168.1.0/26	192.168.1.1 - 192.168.1.62	192.168.1.63
1	192.168.1.64/26	192.168.1.65 - 192.168.1.126	192.168.1.127
2	192.168.1.128/26	192.168.1.129 - 192.168.1.190	192.168.1.191
3	192.168.1.192/26	192.168.1.193 - 192.168.1.254	192.168.1.255

Figure III.8 Système d'adressage de 4 réseaux

- **Masquage de sous-réseau de longueur variable '(VLSM)**

VLSM permet l'utilisation de masques différents pour chaque sous-réseau. Une fois qu'une adresse réseau est divisée en sous-réseaux, toute autre division de ces sous-réseaux entraîne la création de « sous-sous-réseaux ».

Ainsi, le réseau 10.0.0.0/8, qui a le masque de sous-réseau /16, se subdivise en 256 sous-réseaux, tous capables de prendre en charge l'adressage de 16 382 hôtes.

- 10.0.0.0/16
- 10.1.0.0/16

- 10.2.0.0/16 jusqu'à 10.255.0.0/16 [17]
- Le changement de plan d'adressage est facilité par le dynamisme d'attribution.

III.2.8.3. Notre plan d'adressage

Dans notre solution on cherche à faciliter la maintenance tout en assurant la sécurité, donc on a proposé un plan d'dressage en utilisant la technique VSLM.

Tableau III.1 liste des VLANs

ID	Le nom de vlan	Adresse réseaux	Masque de réseaux	Nombre d'utilisateur	passerelle	1er Adresse	Dernier adresse
10	Management (switch)	10.0.1.0	255.255.255.0	254	10.0.1.1	10.0.1.2	10.0.1.254
20	Serveur	10.0.2.0	255.255.255.0	254	10.0.2.1	10.0.2.2	10.0.2.254
30	Super enseignant	10.0.3.0	255.255.255.0	254	10.0.3.1	10.0.3.2	10.0.3.254
40	Navigation internet (étudiants)	10.0.4.0	255.255.252.0	1022	10.0.4.1	10.0.4.2	10.0.7.254
50	Biblio Fac-science	10.0.8.0	255.255.254.0	512	10.0.8.1	10.0.8.2	10.0.9.254
51	Biblio Fac-sociaux	10.0.10.0	255.255.254.0	512	10.0.10.1	10.0.10.2	10.0.11.254
52	Biblio Fac-sport	10.0.12.0	255.255.255.0	255	10.0.12.1	10.0.12.2	10.0.12.254
60	USER SCOLARITE (App)	10.0.13.0	255.255.255.0	254	10.0.13.1	10.0.13.2	10.0.13.254
70	USER –simple	10.0.60.0	255.255.254.0	512	10.0.60.1	10.0.60.2	10.0.61.254
80	Chercheures	10.0.15.0	255.225.255.0	254	10.0.15.1	10.0.15.2	10.0.15.254
81	ENS-Fac-science	10.0.16.0	255.255.254.0	512	10.0.16.1	10.0.16.2	10.0.17.254
82	ENS-Fac-sociaux	10.0.18.0	255.255.255.0	254	10.0.17.1	10.0.18.2	10.0.18.254
83	ENS-Fac-sport	10.0.19.0	255.255.255.0	254	10.0.18.1	10.0.19.2	10.0.19.254
100	Internet (Firewall)	10.0.20.0	255.225.255.0	254	10.0.20.1	10.0.20.2	10.0.20.254
Laboratoires de la faculté N°1 (science)							
141	LABO1-01	10.0.30.0	255.255.255.224	30	10.0.30.1	10.0.30.2	10.0.30.30
142	LABO1-02	10.0.30.32	255.255.255.224	30	10.0.30.33	10.0.30.34	10.0.30.62
143	LABO1-03	10.0.30.64	255.255.255.224	30	10.0.30.65	10.0.30.66	10.0.30.94
144	LABO1-04	10.0.30.96	255.255.255.224	30	10.0.30.97	10.0.30.98	10.0.30.126
145	LABO1-05	10.0.30.128	255.255.255.224	30	10.0.30.129	10.0.30.130	10.0.30.158
146	LABO1-06	10.0.30.160	255.255.255.224	30	10.0.30.161	10.0.30.162	10.0.30.190
147	LABO1-07	10.0.30.192	255.255.255.224	30	10.0.30.193	10.0.30.194	10.0.30.222
148	LABO1-08	10.0.30.224	255.255.255.224	30	10.0.30.225	10.0.30.226	10.0.30.254
149	LABO1-09	10.0.31.0	255.255.255.224	30	10.0.31.1	10.0.31.2	10.0.31.30
150	LABO1-10	10.0.31.32	255.255.255.224	30	10.0.31.33	10.0.31.34	10.0.31.62
151	LABO1-11	10.0.31.64	255.255.255.224	30	10.0.31.65	10.0.31.66	10.0.31.94
152	LABO1-12	10.0.31.96	255.255.255.224	30	10.0.31.97	10.0.31.98	10.0.31.126
153	LABO1-13	10.0.31.128	255.255.255.224	30	10.0.31.129	10.0.31.130	10.0.31.158
154	LABO1-14	10.0.31.160	255.255.255.224	30	10.0.31.161	10.0.31.162	10.0.32.190
155	LABO1-15	10.0.31.192	255.255.255.224	30	10.0.31.193	10.0.31.194	10.0.32.222
156	LABO1-16	10.0.31.224	255.255.255.224	30	10.0.31.225	10.0.31.226	10.0.32.254
157	LABO1-17	10.0.32.0	255.255.255.224	30	10.0.32.1	10.0.32.2	10.0.32.30
158	LABO1-18	10.0.32.32	255.255.255.224	30	10.0.32.33	10.0.32.34	10.0.32.62
159	LABO1-19	10.0.32.64	255.255.255.224	30	10.0.32.65	10.0.32.66	10.0.32.94
160	LABO1-20	10.0.32.96	255.255.255.224	30	10.0.32.97	10.0.32.98	10.0.32.126
Laboratoires de la faculté N°2(sociaux)							
101	LABO2-01	10.0.40.0	255.255.255.224	30	10.0.40.1	10.0.40.2	10.0.40.30
102	LABO2-02	10.0.40.32	255.255.255.224	30	10.0.40.33	10.0.40.34	10.0.40.62
103	LABO2-03	10.0.40.64	255.255.255.224	30	10.0.40.65	10.0.40.66	10.0.40.94
104	LABO2-04	10.0.40.96	255.255.255.224	30	10.0.40.97	10.0.40.98	10.0.40.126
105	LABO2-05	10.0.40.128	255.255.255.224	30	10.0.40.129	10.0.40.130	10.0.40.158
106	LABO2-06	10.0.40.160	255.255.255.224	30	10.0.40.161	10.0.40.162	10.0.40.190
107	LABO2-07	10.0.40.192	255.255.255.224	30	10.0.40.193	10.0.40.194	10.0.40.222
108	LABO2-08	10.0.40.224	255.255.255.224	30	10.0.40.225	10.0.40.226	10.0.40.254
109	LABO2-09	10.0.41.0	255.255.255.224	30	10.0.41.1	10.0.41.2	10.0.41.30
110	LABO2-10	10.0.41.32	255.255.255.224	30	10.0.41.33	10.0.41.34	10.0.41.62

111	**LABO2-11**	**10.0.41.64**	**255.255.255.224**	**30**	**10.0.41.65**	**10.0.41.66**	**10.0.41.94**
112	**LABO2-12**	**10.0.41.96**	**255.255.255.224**	**30**	**10.0.41.97**	**10.0.41.98**	**10.0.41.126**
Laboratoires de la faculté N°3 (sport)							
171	**LABO3-01**	**10.0.50.0**	**255.255.255.224**	**30**	**10.0.50.1**	**10.0.50.2**	**10.0.50.30**
172	**LABO3-02**	**10.0.50.32**	**255.255.255.224**	**30**	**10.0.50.33**	**10.0.50.34**	**10.0.50.62**
173	**LABO3-03**	**10.0.50.64**	**255.255.255.224**	**30**	**10.0.50.65**	**10.0.50.66**	**10.0.50.94**
174	**LABO3-04**	**10.0.50.96**	**255.255.255.224**	**30**	**10.0.50.97**	**10.0.50.98**	**10.0.50.126**
175	**LABO3-05**	**10.0.50.128**	**255.255.255.224**	**30**	**10.0.50.129**	**10.0.50.130**	**10.0.50.158**
176	**LABO3-06**	**10.0.50.160**	**255.255.255.224**	**30**	**10.0.50.161**	**10.0.50.162**	**10.0.50.190**
177	**LABO3-07**	**10.0.50.192**	**255.255.255.224**	**30**	**10.0.50.193**	**10.0.50.194**	**10.0.50.222**
178	**LABO3-08**	**10.0.50.224**	**255.255.255.224**	**30**	**10.0.50.225**	**10.0.50.226**	**10.0.50.254**
179	**LABO3-09**	**10.0.51.0**	**255.255.255.224**	**30**	**10.0.51.1**	**10.0.51.2**	**10.0.51.30**
180	**LABO3-10**	**10.0.51.32**	**255.255.255.224**	**30**	**10.0.51.33**	**10.0.51.34**	**10.0.51.62**
181	**LABO3-11**	**10.0.51.64**	**255.255.255.224**	**30**	**10.0.51.65**	**10.0.51.66**	**10.0.51.94**
182	**LABO3-12**	**10.0.51.96**	**255.255.255.224**	**30**	**10.0.51.97**	**10.0.51.98**	**10.0.51.126**
183	**LABO3-13**	**10.0.51.128**	**255.255.255.224**	**30**	**10.0.51.129**	**10.0.51.130**	**10.0.51.158**
184	**LABO3-14**	**10.0.51.160**	**255.255.255.224**	**30**	**10.0.51.161**	**10.0.51.162**	**10.0.51.190**
210	**Wifi**	**10.0.70.0**	**255.255.240.0**	**4064**	**10.0.70.1**	**10.0.70.2**	**10.0.85.254**
220	**Free-wifi**	**10.0.22.0**	**255.255.252.0**	**1022**	**10.0.22.1**	**10.0.22.2**	**10.0.25.254**

III.3. Attaques et moyens de sécurité réseau

Le réseau local est le cœur de la majeure partie de l'activité informatique de nos organismes. A ce titre tout effort de sécurisation est nécessaire. Cette considération justifie à elle seule d'accorder une attention particulière à la sécurisation des réseaux locaux.

Par ailleurs, il est généralement estimé que la majorité des malveillances informatiques ont une origine complicité interne aux organismes (la malveillance constituant déjà la catégorie la plus significatives des pertes par rapport aux deux autres accidents et erreurs). Devant cette spécificité il donc essentiel d'examiner dans une optique sécuritaire l'infrastructure du réseau local dès sa conception.

Il est donc nécessaire d'établir des configurations de systèmes d'exploitation comprenant leurs réseaux et multiples branches, sécurisés avec les techniques les plus sophistiquées en matière de « firewalls » et de contrôles d'accès.

III.3.1. Quelques types d'attaques

III.3.1.1. Attaque sur le réseau

Les principales techniques d'attaques sur le réseau sont :

Le Sniffing : technique permettant de récupérer toutes informations transitant sur le réseau. Elle est généralement utilisée pour récupérer les mots de passe des applications qui ne chiffrent pas leurs communications.

Usurpation d'identité (Spoofing) : technique consistant à prendre l'identité d'une autre personne ou d'une autre machine. Elle est généralement utilisée pour récupérer des informations

- Absence d'un système de détection d'intrusion interne provoque l'accès non autorisé depuis l'extérieur

III.3.1.2. Attaque sur le mot de passe

Les attaques sur les mots de passe peuvent consister à faire de nombreux essais jusqu'à trouver le bon mot de passe (force brute) et l'intrus peut mener une attaque pour collecter les mots de passe afin d'accéder aux ressources matériels mises en question.

- La majorité des failles et incidents de sécurité sont dus à des erreurs humains, des utilisateurs sont encore inconscient ou ignorant des risques qu'ils encourent l'ors de l'utilisation d'un programme mal veillant.
- L'absence de session offre à l'intrus la possibilité de collecter un ensemble d'information sur la cible (nom d'utilisateur, partage).
- Les postes client sont intégrés dans le WORKGROUP, ou le compte d'accès par défaut est administrateur sur les postes client ce qui provoque Requêtes nombreuses provenant des postes clients qui veulent devenir le "maitre de Workgroups".

III.3.2. La politique de Sécurité réseau

La politique de sécurité est une démarche de toute entreprise visant à protéger son personnel et ses biens d'éventuels incidents de sécurité pour son activité. La politique de sécurité réseau fait éventuellement partie de la démarche sécuritaire de l'entreprise.

III.3.2.1. Principe d'une politique de sécurité réseau

La politique de sécurité réseau vise à satisfaire les critères suivants :

- **Authentification :** information permettant de valider l'identité pour vérifier que la personne est celle qui prétend l'être.
- **Identification** : information permettant d'indiquer la personne inscrite.
- **Autorisation :** information permettant d'indiquer les ressources de l'entreprise auxquelles un utilisateur identifié aura accès ainsi que les actions autorisées sur ses ressources.
- **Intégrité** : regroupe les mécanismes garantissant qu'une information n'a pas été modifiée ou altérée.
- **Disponibilité :** regroupe les mécanismes garantissant que les ressources de l'entreprise sont accessibles.
- **Non-répudiation** : mécanisme permettant de prouver qu'un message a bien été envoyé par un émetteur et reçu par un récepteur.
- La politique de sécurité réseau couvre les éléments suivants :
- **Sécurité d'accès** : détermine la sécurité d'accès aux ressources de l'entreprise que soit localement ou via un accès distant, ainsi que la gestion des utilisateurs et leurs droit d'accès aux systèmes d'information de l'entreprise.

- **Sécurité de l'infrastructure** : couvre la sécurité des équipements et des connexions réseaux.
- **Sécurité de l'intranet face à internet** : couvre la sécurité logique des accès aux ressources de l'entreprise et l'accès aux ressources extérieures (internet).

III.3.3. Sécurité niveau 2

Il est important de sécuriser le niveau 2 dans un réseau, car il s'agit de la porte d'entrée de ce dernier.

De nombreuses menaces existent, ainsi que de nombreuses méthodes de sécurité. Nous allons voir certaines de ces menaces, ainsi que la configuration à mettre en place pour s'en protéger.

III.3.3.1. Port security

Commençons par la sécurité la plus connu sur les switches : la sécurité de port. Le but sera ici d'appliquer une restriction en fonction de l'adresse MAC source. Seul un certain nombre d'adresses seront autorisées.**A quoi sert la sécurité de port ?**

- A limiter le nombre d'adresse MAC dernière un port
- A se protéger du MAC Address Flooding[1]
- A restreindre l'accès à certaines adresses MAC
- A désactiver le port / envoyer des logs en cas de violation

Ainsi, le switch va remplir sa table d'adresse MAC, jusqu'à ce qu'elle soit pleine. Une fois la table pleine, le switch ne pouvant pas en apprendre plus, il va passer en mode HUB. Il va alors retransmettre tous les frames qu'il reçoit sur tous les ports. Cela peut être une technique d'attaque pour capter du trafic.

Il y a trois options de gestion des adresses MAC :

- **Dynamique**
- **Static**
- **Sticky**

[1] Le MAC Address Flooding consiste à envoyer des centaines / milliers de messages en indiquant à chaque fois une adresse MAC source différente.

- En mode **Static**, nous définissons nous même les adresses Mac autorisées. Cette solution n'est pas très évolutive, et peut être longue à configurer. L'avantage est que les adresses définies sont conservées en permanence.
- En mode **Dynamic**, le switch apprend automatiquement les adresses. Il se base sur les frames reçus. Les Mac autorisées seront donc les premières apprises. Par contre, les adresses Mac ne sont pas conservées dans la configuration.

C'est pour cela qu'il y a l'option Sticky. Elle permet au mode Dynamique d'enregistrer les adresses. Nous les retrouvons alors dans la configuration comme si elles avaient été configurées en Statique.

Il existe 3 options pour la violation[1] de port :

- **Shutdown**
- **Protect**
- **Restrict**

En mode Shutdown, le port est désactivé s'il y a violation. Il passe en Err-Disabled.

En mode Protect, les adresses MAC en trop sont ignorées, Les messages avec une adresse Mac source non connue sont ignorés.

Le mode **Restrict** fait la même chose que le mode Protect, en plus, une Trap SNMP est envoyée, un message Syslog est logué et le compteur de violation augmente.

Il y a deux moyens de sortir un port du mode Err-Disabled.

- Soit en allant sur le port et en faisant un **Shutdown** puis **No-Shutdown**.
- Soit en configurant le port pour qu'il remonte au bout d'un certain temps.

Le Port Security Aging permet d'oublier les adresses Mac après un certain temps. Il existe 2 **Types** :

- Inactivity : l'adresse Mac est supprimée si elle est inactive pour le temps spécifié
- Absolute : l'adresse Mac est supprimée après le temps spécifié

Il est possible de rajouter l'option **Static** pour que les adresses configurées à la main puissent aussi être supprimées. Trap SNMP est envoyée, un message Syslog est logué et le compteur de violation augmente. [18]

[1] On appel violation de port, quand les règles de sécurité ne sont pas respectées (ex : nombre d'adresse MAC dépassé)

III.3.3.2. AAA et 802.1x

802.1x est un standard permettant d'améliorer la sécurité de notre réseau. Le principe est simple, quand l'utilisateur se connecte au réseau, un Login / MDP va lui être demandé. Cela peut être valable pour les connexions Wifi (le plus courant) et / ou pour les connexions Ethernet.

Le plus souvent, le 802.1x est utilisé sur les réseaux Wifi. Au lieu d'une clé wifi, l'utilisateur doit fournir ses identifiants. En entreprise, les identifiants correspondent en général au compte de l'utilisateur sur le domaine.

Dans un réseau sans fil, WPA Entreprise implémente 802.1x.

Pour la suite, nous considérerons l'utilisation de 802.1x sur un switch.

Nous allons pouvoir choisir quels ports devront être contrôlés par 802.1x. Sur ces ports-là, les utilisateurs devront s'authentifier.

Tant qu'ils ne sont pas authentifiés, ils n'ont pas accès au réseau, ou bien ils seront placés dans un VLAN invité (avec des droits limités). C'est à l'administrateur de choisir le fonctionnement voulu.

De plus, il est possible de placer dans un VLAN invité, les clients ne prenant pas en charge EAP.

Voici un schéma du fonctionnement :

Lors-ce que le PC se connecte au switch, celui-ci lui demande ses identifiants grâce au protocole **EAP – Extensible Authentification Protocol**.

EAP permet différents types d'authentification. La liste donnée ci-dessus n'est pas exhaustive.

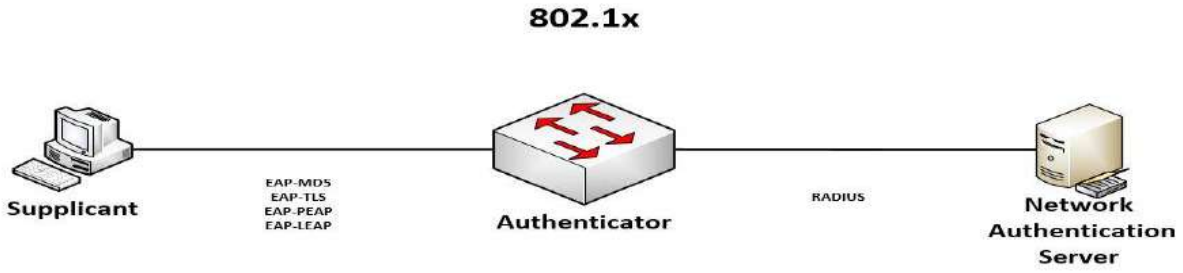


Figure III.9 Fonctionnement de EPA

La plus simple est EAP-MD5. L'EAP-PEAP est la méthode la plus populaire.

En 802.1x le switch aura pour rôle de faire l'intermédiaire entre le client et le serveur d'authentification.

EAP permet au switch de demander les identifiants à l'utilisateur, pour ensuite l'authentifier sur un serveur RADIUS.

Comme vous pouvez le voir, il existe 3 rôles en 802.1x :

- **Supplicant** : la machine connectée à un port Access, qui a besoin de s'authentifier

- **Authenticator** : l'équipement (switch ou borne wifi) qui contrôle l'accès au réseau
- **Network Authentication Server** : serveur qui sera interrogé pour l'authentification des utilisateurs

III.3.3.3. Private Vlan

Le Private VLAN a été inventé afin d'isoler les hôtes au niveau 2 , Vous me direz que les VLAN standards font déjà cela, et vous aurez raison. Mais parfois, l'utilisation des VLAN devient abusive.

Imaginons le cas où nous avons 10 serveurs à connecter au réseau, et que ces serveurs ne doivent pas pouvoir discuter entre eux (cas typique d'une DMZ).

Ou encore que nous souhaitions faire un réseau invité, ou les machines ne peuvent joindre que la passerelle. Il nous faudrait alors 1 VLAN par machine.
Il en découlera alors une création de très nombreux sous réseau, et un gaspillage d'adresse relativement important.

L'idéal serait d'avoir un VLAN (et donc un sous réseau), dans lequel les utilisateurs ne peuvent pas discuter.

C'est ce que permettent les PVLAN. PVLAN se compose d'une association de VLAN :

- Un VLAN **Primary**
- Un ou plusieurs VLAN **Secondary**

Le VLAN **Secondary** peut être de deux types :

- **Isolated** : les membres de ce VLAN ne peuvent pas communiquer entre eux
- **Community** : les membres de ce VLAN peuvent communiquer entre eux
- Enfin, le port d'un switch peut fonctionner dans l'un des deux modes suivants :
- **Host** : Le port à un comportement qui découle du type de PVLAN auquel il est associé (Isolated ou Community)
- **Promiscuous** : le port peut communiquer avec les ports membres du même VLAN

Voici un schéma représentant cela :

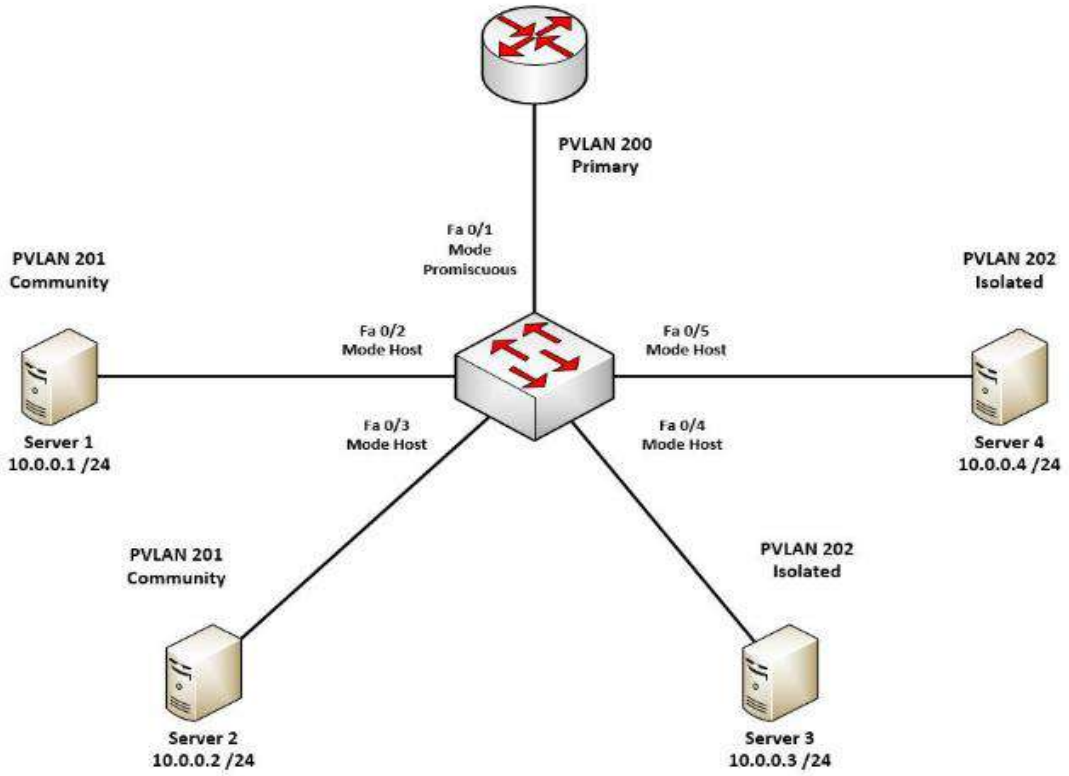


Figure III.10 private VLAN

Commençons par le routeur. Il est dans le PVLAN primaire, et le port auquel il est connecté est en mode Promiscuous. Tout le monde sera donc capable de communiquer avec le routeur.

Les serveurs 1 et 2 sont dans un PVLAN du type Community et les ports auxquels ils sont connectés en mode Host.

Ces deux serveurs seront donc capables de communiquer entre eux, ainsi qu'avec le routeur. Les serveurs 3 et 4 sont dans un PVLAN du type Isolated, et les ports auxquels ils sont connectés en mode Host.

Les deux serveurs ne pourront donc pas communiquer entre eux, mais seulement avec le routeur. De plus, vous remarquerez que toutes les machines sont dans le même sous réseau [18]

III.3.3.4. DHCP Snooping

Le DHCP Snooping est une fonctionnalité qui permet d'améliorer la sécurité d'une infrastructure utilisant un DHCP. Il permet de

- Choisir les ports derrière lesquels peut se trouver un DHCP
- S'assurer que les hôtes utilisent l'IP qui leur a été associée
- Définir un maximum de requêtes DHCP par port.

Choisir les ports derrière lesquels un DHCP peut être placé est important.

En effet, si un attaquant met en place un DHCP, cela peut créer des erreurs sur le réseau. Pire encore, l'attaquant pourrait contrôler le trafic sur le réseau [18]

III.3.3.5. Spanning tree

Nous avons déjà comment configuré Spanning Tree. Voyons ici comment ajouter de la sécurité au processus Spanning Tree.

Première option à activer sur les ports Access, le **BPDU Guard**. Cette option va simplement désactiver le port (en Err-Disabled) si des BPDU sont reçus sur le port, pour empêcher un attaquant de prendre la place du Root Bridge.

En effet, pour devenir le Root Bridge, l'attaquant devrait envoyer des BDPU, ce qui aurait pour effet de couper le port.

La deuxième option est le Root Guard. Cette option est à activer sur le Root Bridge et le Backup Bridge. Nous pouvons alors choisir derrière quel port ne peut pas se trouver un Root Bridge. Cela permet à nouveau de s'assurer que le Root Bridge est bien le switch désiré.

Concrètement, nous devons activer cette fonctionnalité sur un port d'un switch. Ensuite, si des BPDU avec Bridge ID plus faible (que celui du switch) sont reçus sur ce port, ce dernier passe en mode Root-inconsistent. Le port va alors écouter les BPDU. Il sera réactivé lors-ce que le switch d'en face cessera d'envoyer des BPDU avec une BID plus faible.

Voici un schéma résumant l'utilisation de BPDU Guard et Root Guard

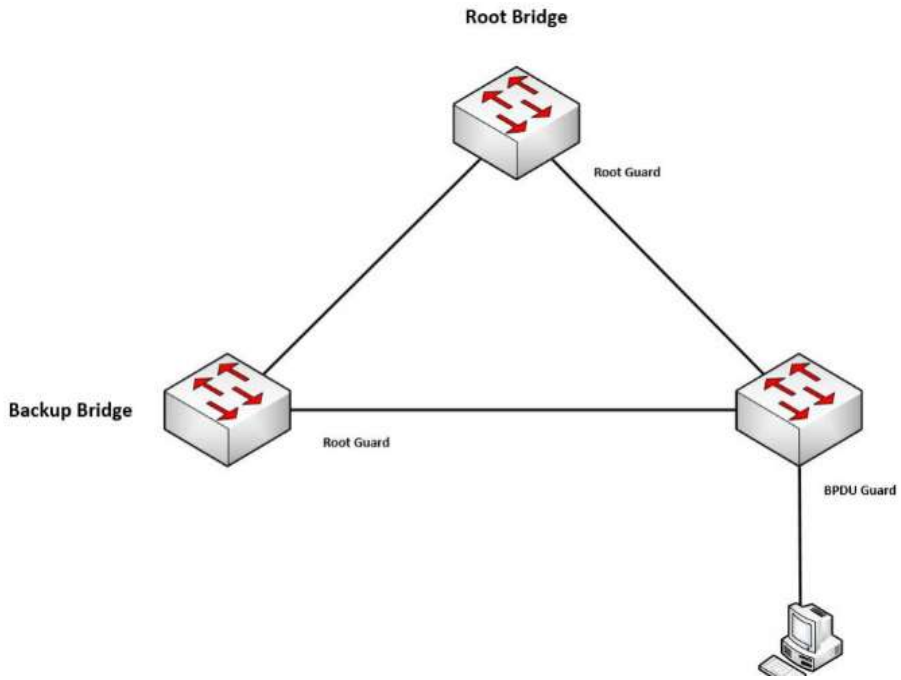


Figure III.11 Les BPDU GUARD et ROOT GUARD dans le spanning tree

Enfin, il existe une option nommée **BPDU Filter**. Quand cette option est configurée de manière globale, tous les ports en mode Portfast arrêtent d'envoyer et de recevoir des BPDU,par contre, si un BPDU est reçu sur un port, ce dernier repasse en mode de fonctionnement normal. [18]

III.3.3.6. VACL

Les VACL ou Vlan ACL sont des Access List à appliquer sur des VLAN. Elles se configurent sur un switch.

A la différence des ACL classiques qui s'appliquent sur un routeur, et qui ne peuvent que filtrer qu'entre les VLANs, les VACL permettent de filtrer le trafic au sein d'un même VLAN.

Prenons l'exemple suivant

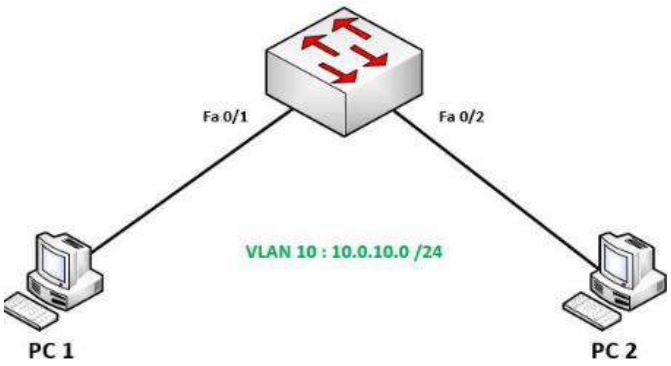


Figure III.12 Les VACL

PC 1et PC 2 sont dans le même VLAN.

A l'aide d'une VACL, nous pouvons empêcher les PC de s'envoyer des Ping. [18]

III.3.4. Solution Firewall

La solution de filtrage consiste à déployer trois niveaux de filtrage sur les ressources du réseau, comme écrit ci-dessous :

III.3.4.1. Firewall à filtrage de paquets

La majorité des équipements de routage actuels disposent d'une fonctionnalité de firewalling basé sur le filtrage de paquets. Cette technique permet de filtrer les protocoles, les sessions, les adresses sources, les ports sources et destination et même l'adresse MAC.

III.3.4.1.1. Firewall State full Inspection

Cette solution sera implémentée par un équipement firewall matériel qui agit en tant que passerelle, afin de garantir la sécurité entre le trafic du réseau interne, public et démilitarisé Au niveau architecture du réseau, le firewall propose trois domaines de sécurité :

Zone interne : Représente le réseau local de l'organisme. Cette zone contient le plus haut niveau de sécurité

Zone externe : représente la zone publique par laquelle passe tout le trafic de destination internet.

Zone démilitarisée : représente la zone contenant les serveurs visibles de l'extérieur dont l'accès est public.

III.3.4.2. Firewall Applicatif

Un Firewall applicatif sera installé sur tous les postes client et les serveurs afin de protéger en premier lieu des tentatives d'intrusion interne.

L'utilisation d'un firewall applicatif permet de contrôler les connexions depuis et vers ces machines, de renforcer la confidentialité des données et de se protéger contre les programmes malveillants.

On peut citer par exemple un Firewall : Mod_security et Mod_Proxy.

III.4. Réseau sans fils (solution wifi)

La technologie Ethernet est la technologie la plus utilisée dans les LAN. Pour interconnecter les machines dans une technologie filaire il faut utiliser : des cartes réseaux, utiliser différents types de câbles (paire torsadées UTP/STP, fibre optique, …), Utiliser les Hub ou les commutateurs. Donc un câblage est nécessaire, ceci va être ingérable si le nombre de stations est dynamique et les stations sont mobiles.

III.4.1 Définition

Un réseau sans fil ou Wireless network est un réseau dans lequel au moins deux terminaux peuvent communiquer sans liaison filaire en utilisant des ondes radioélectriques.

Un réseau sans fil est un réseau informatique qui connecte différents postes (Ordinateur, laptop, PDA, Caméra wifi, etc.) entre eux par ondes radio.

Un réseau sans fil est constitué d'une station de base (BTS) avec une couverture de type Point à Point ou Point – Multipoint dit cellulaire. Ce dernier type utilisé dans la plupart des réseaux locaux permet de desservir un ensemble d'abonnés d'une zone prédéfinie. Les liaisons hertziennes de la BTS vers les abonnées sont dites voies descendantes (downstream) tandis que les voies montantes (UpStream) désignent les liaisons des abonnés vers la BTS.

Commençons tout d'abord avec notre solution Wi-Fi (la norme ISO 802.11). Ce Wireless Fidelity se propage par les ondes radio sur une fréquence de 2.4Ghz. Afin de pouvoir disposer de plusieurs réseaux sur la même surface. Le Wifi permet, grâce à un routeur ou un point d'accès, de desservir une zone de couverture d'un rayon de cent mètres théorique. Ceci étant, comme pour les réseaux filaires, l'atténuation du signal se détériore très vite en fonction de la distance du point d'accès, mais également en fonction du nombre et du type d'obstacles rencontrés entre le routeur et le poste client. Toutefois, il est possible d'associer plusieurs points d'accès Wifi sur le même réseau pour étendre de manière significative le signal et la qualité de la ligne radio pour le confort de l'utilisateur final.

Du côté des débits, le Wifi permet d'assurer une bande passante allant jusqu'à 54Mbps pour la norme G (le Super G de Dlink) et 11Mbps pour la norme B.

Pour les appareils légers comme les PDA ou bien encore les téléphones portables, de nombreuses applications sont venues faciliter la tâche de tout le monde comme par exemple la synchronisation des contacts avec une station de travail ou bien encore le transfert d'images.

III.4.2 Réseau sans fil WLAN

Les réseaux locaux sans fil (WLAN pour Wireless Local Area Networks) : Technologies WiFi, Hyperlan. La percée de Wi-Fi ces dernières années a fait connaître les réseaux sans fil. La famille Wi-Fi s'agrandit peu à peu. Dans le domaine des réseaux locaux sans fil, seul l'Hiperlan II tente de le concurrencer. Cependant la montée en puissance des réseaux personnels jusqu'à présent limités à quelques mètres, montre des velléités de briser les barrières (ce fut le cas avec les annonces de Bluetooth 2.0 ou plus récemment avec les évolutions d'UWB). A l'inverse, WiFi a été utilisé au niveau métropolitain du fait du manque jusqu'à présent de réseaux sans fil plus appropriés.

Le réseau local sans fil (noté WLAN pour Wireless Local Area Network) est un réseau permettant de couvrir l'équivalent d'un réseau local d'entreprise, soit une portée d'environ une centaine de mètres. Il permet de relier entre eux les terminaux présents dans la zone de couverture. Il existe plusieurs technologies concurrentes :

Le Wifi (ou IEEE 802.11), soutenu par l'alliance WECA (Wireless Ethernet Compatibility Alliance) offre des débits allant jusqu'à 54Mbps sur une distance de plusieurs centaines de mètres.

III.4.2.1. Architecture réseau WIFI

Il existe deux modes de fonctionnement

A. Le mode Infrastructure

Le mode infrastructure se base sur une station spéciale appelée Point d'Accès (PA). Ce mode permet à des stations wifi de se connecter à un réseau (généralement Ethernet) via un point d'accès. Elle permet à une station wifi de se connecter à une autre station wifi via leur PA commun. Une station wifi associée à un autre PA peut aussi s'interconnecter.

L'ensemble des stations à portée radio du PA forme un BSS (Basic Service Set). Chaque BBS est identifié par un BSSID (BSS Identifier) de 6 octets qui correspond à l'adresse MAC du PA.

Chaque ordinateur se connecte à un point d'accès via une liaison sans fil. L'ensemble formé par le point d'accès et les stations situées dans sa zone de couverture est appelé ensemble de services de base BSS (basic service set).

Il est possible de relier plusieurs BSS (basic service set) par une liaison appelée système de distribution (DS,Distribution System) afin de constituer un ensemble de services étendu (extended service set ou ESS). Le système de distribution (DS) peut être un réseau filaire, ou un câble entre deux points d'accès. Un ESS (Extended Service Set) est repéré par un ESSID (Extended Service Set Identifier), qui est un nom du réseau.

Lorsqu'un utilisateur nomade passe d'un BSS (basic service set) à un autre en se déplaçant l'adaptateur réseau sans fil de sa machine est capable de changer de point d'accès selon la qualité des signaux provenant des différents points d'accès. Les points d'accès communiquent entre eux, Cette caractéristique permet aux stations de passer de façon transparente d'un point d'accès à un autre (roaming)



Figure III.13 Le mode Infrastructure

B. Le mode Ad-Hoc

Le fonctionnement de ce mode est totalement distribué, il n'y a pas d'élément structurant hiérarchiquement la cellule ou permettant de transmettre les trames d'une station à une autre. Ce mode permet la communication entre deux machines sans l'aide d'une infrastructure. Les stations se trouvant à portée de radio forment un IBSS (Independant Basic Service Set). En mode ad hoc les ordinateurs sans fil clients se connectent les uns aux autres pour constituer un réseau point à

point (peer to peer), c'est un réseau dans lequel chaque ordinateur est un client et un point d'accès. Cet ensemble est appelé, IBSS (indépendant basic service set).

Dans un réseau ad hoc, la portée du IBSS est déterminée par la portée de chaque station. Contrairement au mode infrastructure, le mode ad hoc ne propose pas de diffuser régulièrement une trame balise d'une station à une autre. Ainsi un IBSS est par définition comme un réseau sans



Figure III.14 Le Mode AD_HOC

fil restreint.

III.4.3. La norme (802.11)

Le WIFI (Wireless Fidelity), la norme IEE802.11 est un standard décrivant le réseau local sans fils (WLAN). Avec le wifi, il est possible de mettre en place des réseaux locaux sans fils à haut débit sous réserve d'être à proximité d'un point d'accès. Le wifi permet de relier des ordinateurs portables, des machines de bureau, des assistants personnels (PDA) et tous les périphériques de liaison à haut débit sur un rayon de plusieurs dizaines de mètres.

La norme 802.11 définit les couches basses du modèle OSI pour une liaison sans fil utilisant des ondes électromagnétiques :

La couche physique (DSSS, FHSS, Infrarouge), proposant trois types de codage de L'information.

La couche liaison de données, constituée de deux sous-couches, le contrôle de liaison logique (Logical Link Control, ou LLC) et le contrôle d'accès au support (Media Access Control, ou MAC).

A. Différents débits et portées

Les normes 802.11a, 802.11b et 802.11g, appelées « normes physiques » correspondent à des révisions du standard 802.11 et proposent des modes de fonctionnement, permettant d'obtenir différents débits en fonction de la portée.

Tableau III.2 Débits et porté de la norme 802.11

Standard	Bande de fréquence (GHZ)	Débit (Mbit/s)	Portée(m)
802.11a	5	54	10
802.11b	2.4	11	100
802.11g	2.4	54	100

a. 802.11 a

La norme 802.11a permet d'obtenir un débit théorique de 54 Mbit/s, soit cinq fois plus que le802.11b, pour une portée d'environ une trentaine de mètres seulement. La norme 802.11 a s'appuie sur un codage du type (Orthogonal Frequency Division Multiplexing ; OFDM) sur la bande de fréquence 5 GHz et utilisent 8 canaux qui ne se recouvrent pas.

b. 802.11 b

La norme 802.11b permet d'obtenir un débit théorique de 11 Mbit/s, pour une portée d'environ une cinquantaine de mètres en intérieur et jusqu'à 200 mètres en extérieur (et même au-delà avec des antennes directionnelles).

REMARQUE : les équipements 802.11a ne sont donc pas compatibles avec les équipements 802.11b. Il existe toutefois des matériels intégrant des puces 802.11a et 802.11b, on parle alors de matériels « dual band ».

c. 802.11 g

La norme **802.11g** permet d'obtenir un débit théorique de **54 Mbit/s** pour des portées équivalentes à celles de la norme **802.11b**. D'autre part, dans la mesure où la norme **802.11 g** utilise la bande de fréquence **2,4GHZ** avec un codage **OFDM**, cette norme est compatible avec les **matériels 802.11b**, à l'exception de certains anciens matériels.

Pour plus de détails sur les portés de ces normes voire l'annexe

III.4.3.1. Les équipements de transmission :

Il existe différents types d'équipements pour la mise en place d'un réseau sans fil WiFi :

- **La carte réseau sans fil PCI** : Dans un ordinateur de bureau, la carte est habituellement installée à l'intérieur de l'ordinateur, le plus généralement dans un des emplacements de PCI qui sont communs dans la tour ou les configurations de bureau de PC. Sur une carte sans fil, une antenne courte, environ 10cm (4 pouces) dépasse en dehors de l'ordinateur et peut être pivotée environ pour recevoir le meilleur signal.
- **La Carte PCMCIA** : Dans un ordinateur portable, la carte serait très probablement installée dans une des fentes de PCMCIA dans le côté de l'ordinateur portable. Sur une carte sans fil, environ 2cm (3/4 pouces) de la carte dépasse au-delà de la fente pour agir en tant qu'antenne. Sur des ordinateurs d'Apple Macintosh, la carte d'aéroport est installée à l'intérieur de l'ordinateur et n'est pas évidente de l'extérieur.
- **Les Adaptateurs Sans Fil Ou Cartes d'accès** : En anglais (Wireless Adapters) ou network interface contrôler, noté NIC. Il s'agit d'une carte réseau à la norme 802.11 permettant à une machine de se connecter à un réseau sans fil. Les adaptateurs WiFi sont disponibles dans de nombreux formats (carte PCI, carte PCMCIA, adaptateur USB, carte compact flash,). On appelle station tout équipement possédant une telle carte. A noter que les composants WiFi deviennent des standards sur les portables (label, Centrino, d'Intel).
- **Une carte fil connecté à un port USB** : Une troisième possibilité est de connecter la carte par l'intermédiaire d'un câble d'USB à l'ordinateur. Dans ce cas-ci, l'antenne sera sur la carte,

qui peut être placée n'importe où que le câble d'USB lui permettra, qui pourrait être jusqu'à 5 mètres partir de l'ordinateur. La carte est actionnée bien que le câble d'USB, ainsi aucune alimentation d'énergie supplémentaire ne soit exigée

- Une troisième possibilité est de connecter la carte par l'intermédiaire d'un câble d'USB à l'ordinateur. Dans ce cas-ci, l'antenne sera sur la carte, qui peut être placée n'importe où que le câble d'USB lui permettra, qui pourrait être jusqu'à 5 mètres partir de l'ordinateur. La carte est actionnée bien que le câble d'USB, ainsi aucune alimentation d'énergie supplémentaire ne soit exigée.

- Les Points d'accès : Notés AP pour (Access point), parfois appelés bornes sans fil, fait office de relais entre les ordinateurs portables et le réseau câblé (auquel il est raccordé) aux différentes stations avoisinantes équipées de cartes WiFi.

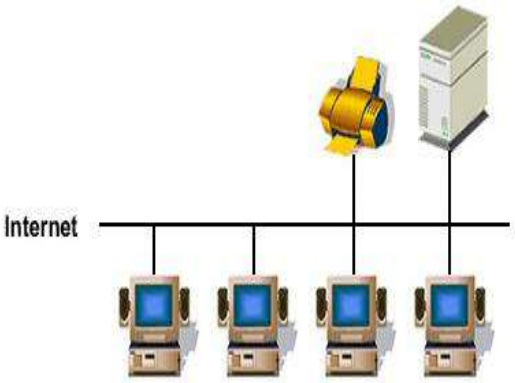


Figure III.15 un réseau câblé traditionnel

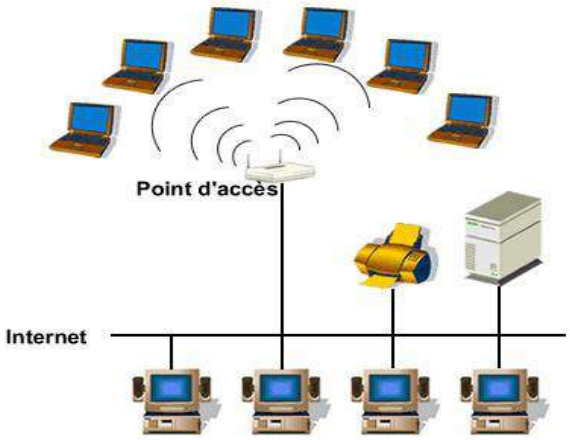


Figure III.16 Un réseau câblé associé à un point d'accès

- Repeater (Répéteur) : permet d'augmenter la distance de fonctionnement du réseau Wireless en renvoyant bit à bit le signal vers son destinataire.

III.4.3.2. Les modes d'interconnexion

A. Access Point (AP) :

Ce mode permet de créer un réseau à part entière en interconnectant les diverses connexions sans fil.

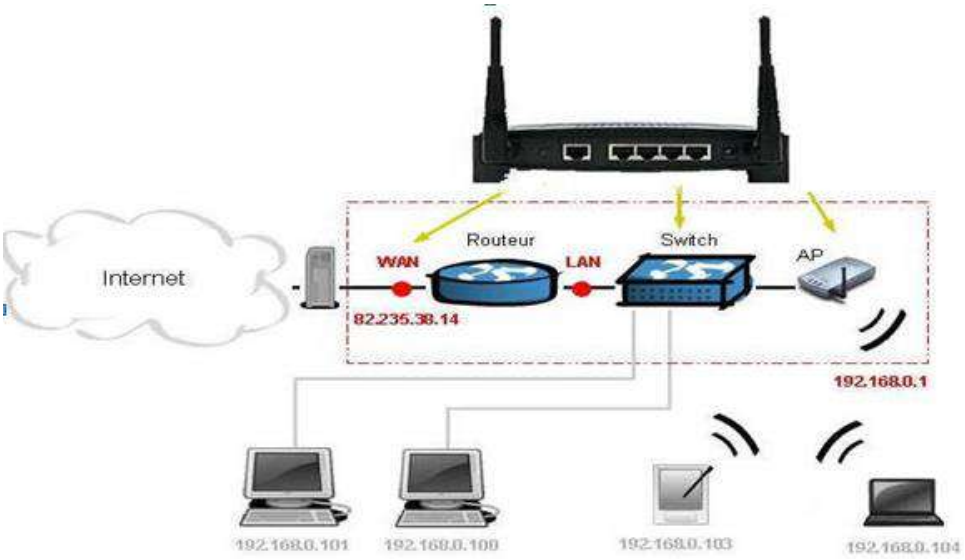


Figure III.17 point d'accès en modem sans fil

B. Wireless Bridge :

Ce mode permet d'interconnecter deux réseaux entre eux par un "pont sans fil". Ainsi, le réseau A disposant de 2 ordinateurs reliés à un routeur pourra être interconnecté avec le réseau B disposant de 2 ordinateurs reliés entre eux avec un hub ou un switch puis à l'AP

C. Multi point Bridge

Similaire au précédant si ce n'est que l'on peut relier plusieurs "points d'accès" entre eux et disposer ainsi du roaming.

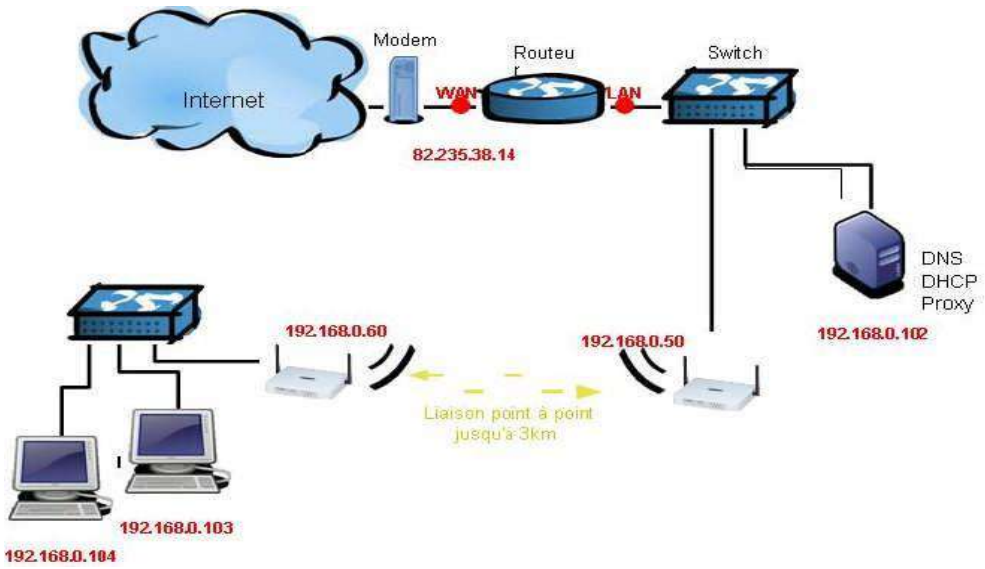


Figure III.18 points d'accès en mode multi ponts

D. Wireless Client :

Permet de transformer toute carte réseau classique avec fil, une fois connecté à l'AP, en carte réseau Wireless en mode client.

III.5 Conclusion

Dans cette partie, nous avons étudié des concepts sur les VLANs et les différents protocoles et on à proposer une liste des VLANs et un plan d'adressage. Cette étude nous facilitera la tâche de configuration pour entamer directement la simulation de notre réseau informatique du nouveau pôle.

Conclusion générale



Conclusion générale

Dans le cadre de nos études en matière de réseaux informatique à campus universitaire et dans le but de mieux appréhender nos connaissances théoriques et les mettre en pratique, nous sommes amenés à réaliser nos travail qui a pour objectif la construction et mise en œuvre d'un cahier de charge technique d'un réseau local et partage réseau des ressources informatique au sein de campus universitaire de Ouezra Ainsi dans le cadre de ce travail, nous sommes amenés à appliquer les notions et les différents concepts retenus en (Réseaux) En effet, le réseau informatique est indispensable à toute organisation car il facilite la transmission, la duplication, le partage des dossiers et des périphériques. Il permet aussi le traitement et la consultation des bases de données et une transmission rapide et fiable des données.

Ce projet a pour but d'assurer le fonctionnement optimal des ressources réseaux de campus universitaire et assurer à ses membres un accès rapide à l'information et un partage facile des données.cet environnement permet aux administrateurs de bénéficier d'une sécurité et d'une facilité de gestion et aux utilisateurs d'effectuer leurs taches le plus efficacement possible.

Le travail qui a été réalisé n'est qu'un début d'implémentation, par rapport à tout ce qu'il y'a à faire pour que l'administration réseau puisse être effective.

Références

Bibliographiques



BIBLIOGRAPHIE

[1] P. ATELIN, Notions fondamentales sur les réseaux informatiques, 2009

[2] Christian. Draux,Les réseaux, 2006.

[3] A. Hakim, Généralités sur les réseaux et la transmission des données, Oeud Smar, Alger: ESI, 2018.

[4] Bertrand. PETIT, Architectures des réseaux, Ellipses, 2006.

[5] G.pugolle, Lesréseaux, EYROLLES, 1997

[6] Chabane.T, mémoire, installationet configuration d'un réseauinformatique, Béjaia, 2006.

[7] T. Barkahoum, Configurationduréseau local de l'entreprise NAFTAL Bejaia en vue de partage des ressources informatiques via active directory, Béjaia, 2012.

[8] wikipedia , Ouzera, available : https://fr.wikipedia.org/wiki/Ouzera, 06 Aout 2019 , [Accés le 5 juin 2020]

[9] TP_LINK, available : https://www.tp-link.com/dz/business-networking/smart-switch, [Acc és le 18 juin 2020]

[10] KOUASSI T. ingénieur en conception informatique, Centre d'expertise et de perfectionnement en informatique ,Etude et optimisation du réseau local,2007

[11] Meilleur pratique en matière de vlan, livre blanc, IN www.fluKenetworks.com, fluKe corporation, 2004.

[12] : Djama K, réalisation d'un réseau campus commuté, mémoire de fin de cycle master 2, université Abderrahmane mira 'Targa ouzemour, promotion 2013-2014.

[13] : Djama K. réalisation d'un réseau campus commuté, mémoire de fin de cycle master 2, université Abderrahmane mira 'Targa ouzemour, promotion 2013-2014.

[14] Amroche H. Cours VLAN. L'école supérieure d'informatique ESI ex INI : Alger . 2019

[15] :Présentation de protocole PVST+, available : https://summarynetworks.com/ccna/ccna3/course/module2/2.2.2.1/2.2.2.1.html

[16] Présentation de protocole rapid PVST+, available : https://summarynetworks.com/ccna/ccna3/course/module2/2.2.3.1/2.2.3.1.html

[17] FORMIP,VSLM, available :https://formip.com/vlsm/

[18] NetworkLab ,sécurité niveau 2 , available : https://www.networklab.fr/securite-de-niveau-2/

Annexes

1- Le nombre de bureaux par étage

Tableau 1 : niveau d'étage et nombre de bureaux pour chaque étage

Bâtiment		Administration	Amphis/salles TD/salles TP	Labo de recherche	Bureaux d'enseignants	bibliothèque
Niveau d'étage		RDC+4	RDC+4	RDC+3	RDC+3	RDC+3
Nombre de bureaux	Sous sole	0	3	0	0	5
	RDC	8	11	7	8	3
	1er	14	6	9	14	3
	2eme	11	14	9	14	2
	3eme	14	14	9	14	8
	4eme	10	6	/	/	/

2- Les surfaces des bureaux

Tableau 2 : les surfaces des bureaux dans la faculté de la science

Département	Bâtiment	Niveau d'étage	espace	Surface (m^2)
Science	Administration	RDC	Salle d'archive01	52 ,44
			B01	11,38
			B02	12,33
			B03	11,38
			B04	13,28
			B05	13,28
			B06	11,38
			B07	12,58
			B08	12,87
			B09	12,04
			B10	15,20

		1er	B11	12,04
			B12	11,97
			B13	12,33
			B14	12,56
			B15	12,90
			B16	12,00
			B17	12,56
			B18	12,33
			B19	11,97
			B20	13,28
			B21	13,28
			Salle de réunion	52,95
		2éme	B22	11,97
			B23	11,97
			B2	12,33
			B25	12,56
			B26	12,30
			B27	12,56
			B28	12,33
			B29	11,97
			B30	13,28
			B31	13,28
		3éme	B32	12 ,87
			B33	12,04
			B34	15,20
			B35	12,04
			B36	11,97
			B37	11,97
			B38	12,33
			B39	12,56
			B40	12,90
			B41	12,56

			B42	12,33
			B43	13,28
			B44	13,28
			B45	13,28
		4éme	Salle de réunion	55,12
			Salle d'archive	13,28
			B46	12,46
			B47	12,33
			B48	11,97
			B49	11,97
			B50	12,33
			Salle d'attente	12,04
			secrétariat	13,25
			Bureau de directeur	33,66
	Bibliothèque	Sous sole	B01	28,69
			B02	19,23
			Salle de rayonnement	769,63
			B03	18.42
		RDC	Salle de lecture	258,15
			Salle de revues et périodique	258,15
			Salle de recherche biblio	242,15
		3eme	Salle d'internet d'enseignant	78,41
			B01	33,81
			B02	16,88
			B03	22,50
			B04	22,50
			B05	16,88
			B06	33,81
			B07	20,29

	AMPHIS + salle TD+ laboratoire TP	Sous sole	Salle de tirage	115,98
			Salle d'archive01	144,14
			Salle d'archive02	144,14
		RDC	B01	14,38
			B02	12,15
			B03	20,48
			B04	14,38
			B05	11,68
			Amphis 25p	285,4
			Amphi 300p	325,65
			Amphi 250p	327,65
			Amphi 300p	328,65
			Amphi 300p	285,45
			Amphi 250p	365,36
			Foyer	19,76
		1er	Labo de lang01	71,95
			Labo de lang02	71,95
	Bureaux d'enseignant	RDC	Foyer	60,29
			B01	12,68
			B02	11,98
			B03	15,01
			B04	12,00
			B05	12,96
			B06	12,67
			B07	11,10
			B08	13,11
		1er	B09	11,97
			B10	12,58
			B11	12,58
			B12	11,85
			B13	12,11
			B14	12,58

			B15	11,97
			B16	12,87
			B17	12,08
			B18	13,95
			B19	12,43
			B20	11,97
			B21	13,28
			B22	13,28
		2eme	B23	11,97
			B24	12,58
			B25	12,30
			B26	12,03
			B27	12,08
			B28	12,58
			B29	11 ,97
			B30	12,80
			B31	12,08
			B32	13,95
			B33	12,43
			B34	11 ,97
			B35	13,28
			B36	13,28
		3eme	B37	11,97
			B38	12,58
			B39	12,43
			B40	12,15
			B41	12,08
			B42	12,58
			B43	11,97
			B44	12,87
			B45	12,08
			B46	13,95

			B47	12,43
			B48	11,97
			B49	13,28
			B50	13,28
	Laboratoire de recherche	RDC	Salle de préparation 01	16,83
			Salle de préparation02	16,29
			Labo01	66,15
			Labo02	66,15
			Labo03	64,03
			Labo04	66,15
			Labo05	64,50
		1er	Salle de préparation01	11,96
			Salle de préparation02	11,96
			Salle de préparation03	17,71
			Salle de préparation04	16,29
			Labo01	66,15
			Labo02	66,15
			Labo03	64,03
			Labo04	66,15
			Labo05	64,50
		2eme	Salle de préparation01	11,96
			Salle de préparation02	11,96
			Salle de préparation03	17,71
			Salle de préparation04	16,29

			Labo01	66,15
			Labo02	66,55
			Labo03	64,09
			Labo04	66,30
			Labo05	64,50
		3eme	Salle de préparation01	11,96
			Salle de préparation02	11,96
			Salle de préparation03	17,71
			Salle de préparation04	16,29
			Labo01	66,15
			Labo02	66,55
			Labo03	64,09
			Labo04	66,30
			Labo05	64,50

1- Le nombre de bureaux par étage

Tableau 1 : niveau d'étage et nombre du bureau pour chaque étage

Bâtiment		**Administration**	**Bibliothèque**	**Amphis**	**Bureaux d'enseignant**	**Salles TD+Salles TP**
Niveau d'étage		RDC+2	RDC+1	RDC+1	RDC+2	RDC+3
Nombre de bureaux	**Sous sole**	/	6	/	/	4
	RDC	17	7	/	16	0
	1er	20	2	9	19	0
	2eme	16	/	/	16	0
	3eme	/	/	/	/	0
	4eme	/	/	/	/	/

2- Les surfaces des bureaux

Tableau 2 : surfaces des bureaux dans la faculté des sociaux

Département	**Bâtiment**	**Niveau d'étage**	**Espace**	**Surface (m²)**
Sociaux	**Administration**	RDC	Salle de réunion	76.60
			Salle d'archive 01	146.60
			Salle d'archive 02	58.40
			B1	13.64
			B2	12.65
			B3	19.40
			B4	12.17
			B5	13.80
			B6	13.00
			B7	12.60
			B8	13.80
			B9	13.00
			B10	12.35

			B11	12.00
			B12	12.00
			B13	12.00
			B14	12.00
			B15	13.70
		1er	Salle de réunion	38.00
			Salle de divers 01	34.00
			Salle de divers 02	46.60
			B1	21.70
			B2	17.65
			B3	13.64
			B4	12.65
			B5	19.40
			B6	12.17
			B7	13.80
			B8	13.00
			B9	12.60
			B10	12.60
			B11	13.00
			B12	12.38
			B13	12.00
			B14	12.40
			B15	12.00
			B16	12.00
			B17	13.70
		2eme	B18	33.80
			B19	13.80
			B20	13.00
			B21	12.60
			B22	12.60
			B23	13.00
			B24	10.50

			B25	12.40
			B26	12.40
			B27	12.00
			B28	12.00
			B29	12.00
			B30	20.00
			B31	14.85
			B32	10.00
			B33	13.64
	Biblio	**Sous sole**	B1	11.89
			B2	11.48
			B3	24.00
			B4	12.38
			Salle de stockage	1000.2
		RDC	Salle de recherche biblio	635.10
			Salle d'internet 01	100.00
			Salle d'internet 02	100.00
			B1	11.95
			B2	10.83
			B3	11.22
			B4	12.32
		1er	Salle de lecture	644.30
			Salle de lecture d'enseignant	186.00
			Salle d'internet	200.00
			B1	11.89
			B2	12.32
	Amphis	**1er**	Amphi 255 pp	285.21
			Amphi 300 pp	325.65
			Amphi 255 pp	300.80
			Amphi 255 pp	290.90
			Amphi 300 pp	328.21

			Amphi 300 pp	327.65
			B1	12.68
			B2	15.01
			B3	12.67
			B4	13.11
			B5	13.95
			B6	12.43
	Bureau	**RDC**	Foyer	79.22
			B1	12.28
			B2	11.10
			B3	15.20
			B4	12.33
			B5	11.72
			B6	11.02
			B7	10.88
			B8	12.39
			B9	12.36
			B10	14.22
			B11	12.23
			B12	17.50
			B13	14.02
			B14	12.68
			B15	11.62
			B16	11.35
		1er	B17	12.43
			B18	12.54
			B19	12.33
			B20	11.66
			B21	11.14
			B22	12.96
			B23	12.00
			B24	13.66

			B25	13.80
			B26	11.95
			B27	11.22
			B28	14.03
			B29	15.05
			B30	11.23
			B31	11.22
			B32	12.00
			B33	11.80
			B34	10.20
			B35	11.12
		2eme	B36	11.95
			B37	12.43
			B38	12.50
			B39	12.15
			B40	13.43
			B41	12.00
			B42	11.97
			B43	11.97
			B44	12.13
			B45	11.97
			B46	13.11
			B47	12.45
			B48	12.66
			B49	12.00
			B50	12.03
			B51	13.66
	Tp	**Sous sol**	Salle informatique 01	127.06
			Salle informatique 02	122.04
			Salle informatique 03	120.90
			Salle informatique 04	129.40

1- Le nombre de bureaux par étage

Tableau 1 : niveau d'étage et nombre du bureau pour chaque étage

Bâtiment		Administration	Bibliothèque	Amphis	Salle td+salle cour+ labo TP
Niveau d'étage		RDC+2	RDC+5	RDC	RDC+3
Nombre de bureaux	Sous sole	/	/	/	1
	RDC	7	3	3	0
	1er	19	3	/	8
	2eme	14	3	/	18
	3eme	/	4	/	21
	4eme	/	6	/	/
	5eme	/	3	/	/

2- Les surfaces des bureaux

Tableau 2: les surfaces des bureaux pour la faculté du sport

Département	Batiment	Niveau d'etage	Espace	Surface(m^2)
Sport	Administration	RDC	Salle d'archive 01	140.08
			Salle d'archive 02	138.90
			B01	13.38
			B02	12.05
			B03	11.95
			B04	13.45
			B05	13.05
		1er	Salle de reunion	55.02
			B06	11.95
			B07	13.25

			B08	12.05
			B09	12.75
			B10	13.38
			B11	12.56
			B12	12.90
			B13	12.33
			B14	11.97
			B15	11.97
			B16	12.56
			B17	13.38
			B18	11.97
			B19	12.04
			B20	12.13
			B21	12.87
			B22	15.20
			B23	12.24
		2eme	Salle de reunion	54.90
			B24	13.38
			B25	12.05
			B26	11.95
			B27	13.45
			B28	12.56
			B29	13.38
			B30	12.04
			B31	11.97
			B32	11.97
			B33	13.38
			B34	12.04
			B35	13.45
			B36	13.45
		RDC	Salle de recherche	230.90
			B01	15.02

	Biblio	**1er**	Salle d'internet	108.80
		2eme	Salle de lecture	230.04
		3eme	Salle de lecture 01	221.04
			Salle de lecture 02	230.50
			Salle de lecture 03	217.06
			Salle de lecture 04	227.15
		4eme	Salle de lecture 01	240.08
			Salle de lecture 02	238.10
			B02	11.97
			B03	12.04
			B04	13.45
			B05	.13.38
		5eme	B06	15.02
			B07	12.89
	Laboratoire Tp1	**Sous sole**	Salle tp 01	66.04
		1er	Salle tp02	70.05
			Salle tp 03	63.40
			Salle tp 04	67.90
		2eme	Salle tp 05	64.20
			Salle tp 06	63.80
			Salle tp 07	68.00
	Laboratoire Tp2	**1er**	Salle tp 01	68.04
			Salle de stock	50.07
		2eme	Salle tp 02	66.07
			Salle tp 03	63.04
			Salle tp 04	62.33
	Laboratoire Tp3	**1er**	Salle tp 01	59.09
			B01	12.04
			B02	13.54
			Salle tp 02	60.80
			B03	12.04

		2éme	B04	12.18
			B05	13.38
			B06	13.45
			B07	12.54
			B08	11.97
			B09	11.97
			B10	12.30
			B11	12.45
			B12	13.83
			B13	12.30
		3éme	Foyer	80.96
			B14	11.97
			B15	11.97
			B16	12.04
			B17	15.20
			B18	13.38
			B19	14.23
			B20	11.97
			B21	12.45
			B22	12.05
			B23	13.45
			B24	12.55
			B25	13.38
			B26	13.45
			B27	12.87
			B28	15.02
			B29	14.39
			B30	12.75
			B31	11.97
			B32	12.04
			B33	11.97
			B34	15.04

1- La norme 802.11a

Tableau 1 :**Débit et porté de la norme 802.11a**

Débit théorique (Mbits/s)	Portée intérieure	Portée extérieure
11	50 m	200 m
5,5	75 m	300 m
2	100 m	400 m
1	150 m	500 m

1- La norme 802.11b

Tableau 2: **Débits et portés de la norme 802.11 b**

Débit théorique (Mbits/s)	Portée intérieure	Portée extérieur
54	27 m	75 m
48	29 m	100 m
36	30 m	120 m
24	42 m	140 m
18	55 m	180 m
12	64 m	250 m
9	75 m	350 m
6	90 m	400 m

1- La norme 802.11g

Tableau 3 : Débits et portées de la norme 802.11 g

Débit théorique (Mbits/s)	Portée intérieure	Portée éxterieur
54	27 m	75 m
48	29 m	100 m
36	30 m	120 m
24	42 m	140 m
18	55 m	180 m
12	64 m	250 m
9	75 m	350 m
6	90 m	400 m