N° d'ordre :
N° de série :

REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE
MINISTERE DE L'ENSEIGNEMENT SUPERIEUR ET DE LA RECHERCHE SCIENTIFIQUE

UNIVERSITEE Hamma Lakhdar D'EL-OUED
Faculté de Technologie
Département de génie électrique

Mémoire de fin d'études présenté
Pour l'obtention du diplôme de

MASTER

Domaine : **Sciences et techniques**
Filière : **Electronique**
Spécialité : **Télécommunications**

Présenté par : Berra Messaoud

Guenoua Faiçal

Réseau VLAN sécurisé par ACL étendu

Soutenu le Mai 2017

Devant le jury composé de :

M	Touhami Ridha	MAA	Présidente
M.	Ajgou Riadh	MCB	Examinateur
M.	Boulila Mohamed	MAA	Directeur du mémoire

2016-2017

DEDICACE

Je dédie ce travail :

A la mémoire de mon Père

A ma très chère mère

A Ma femme

A Mon ange Salah

A Mes frères et mes sœurs

A mes neveux et nièces

A Toute La famille

A Mes amis et collèges

Je vous dédie ce travail avec tous mes vœux de bonheur, de santé et de prospérité.

Faiçal

DEDICACE

Je dédie cette mémoire :

A mes très chères parents Mabrouk et maya

A tous mes frères et sœurs, ainsi que leurs enfants

A toute ma famille, petits et grands

A mes chers amis

A mes chers collègues surtout Fayçal

A tous ceux qui m'ont donnés la force de continuer….

Messaoud

Remerciement

Nous tenons tout d'abord à remercier Dieu le tout puissant et miséricordieux, qui nous a donné la force et la patience d'accomplir ce Modeste travail.

En second lieu, nous tenons à exprimer toute nos reconnaissances à notre directeur du projet Monsieur Boulila Mohamed. Nous le remercions de nous avoir encadrés, orientés, aidés et conseillés.

Nous adressons nos sincères remerciements à tous les professeurs de la promotion deuxième année Master Télécoms pour leurs soutiens pendant toute l'année, leurs encouragements, et leurs conseils en citant : Ajgou Riadh, Lakhdar Neceredine, Medjouri Abdelkader, Zaim Bahia.

À tous, nous présentons nos remerciements, notre respect et notre gratitude.

Sommaire

Chapitre 2 : Sécurisation des réseaux

Chapitre 3 : Conception et implantation d'un réseau VLAN

Liste des Figures

Chapitre 01 : Généralités sur les réseaux

Chapitre 2 : Sécurisation des réseaux

Chapitre 3 : Conception et implantation d'un réseau VLAN

Liste des tableaux

Chapitre 01 : Généralités sur les réseaux

Chapitre 2 : Sécurisation des réseaux

Chapitre 3 : Conception et implantation d'un réseau VLAN

Abréviations

A

ANS1 Abstract Syntax Notation

ARP Address Resolution Protocol

ASCII American standard code for information interchange

ATM Asynchronous transfer mode

C

CCITT Consultative committee for international telegraphy and telephony

D

DOD Department of Defense

DNS Domain Name System

F

FTP File Transfer Protocol

H

HDLC High level data link control

HTML Hypertext Markup Language

HTTP Hypertext transfer protocol

I

IP Internet Protocol

IPV4 IP version 4

IPV6 IP version 6

ICMP Internet Control Message Protocol

ISO International Standards Organization

L

LAN Local Area Network

M

MAN Metropolitan Area Network

MPLS Multi-protocol label switching

N

NMS Network Management System

NFS Network File System

O

OSI Open Systems Interconnexion Référence Model

P

PDU Protocol Data Unit

PAN Personnel Area Network

P2P Peer to peer

R

RIP Routing Information Protocol

RARP Reverse Address Resolution Protocol

RAN Regional Area Network

S

SMTP Simple Mail Transfer Protocol

SNMP Simple Network Management Protocol

T

Telnet Network Virtual Terminal Protocol

TFTP Trivial File Transfer Protocol

TLD Top Level Domain

TCP Transmission Control Protocol)

U

UDP User Datagram Protocol

URL Uniform Resource locator

W

WWW World Wide Web

WAN Wide Area Network

Introduction Générale

Les réseaux et systèmes informatique sont devenus des outils indispensables au fonctionnement des établissements et entreprises. Ils sont aujourd'hui déployés dans tous les secteurs professionnels : les entreprises de communication, les administrations, Les banques, les assurances, La médecine ou encore le domaine militaire.

Ce développement phénoménal s'accompagne naturellement de l'augmentation du nombre d'utilisateurs. Ces utilisateurs ne sont pas forcément pleins de bonnes intentions vis-à-vis de ces réseaux. Ils peuvent exploiter les vulnérabilités des réseaux et systèmes pour essayer d'accéder à des informations sensibles dans le but de les lire les modifier ou les détruire.

Des lors que ces réseaux sont apparus comme des cibles d'attaques potentielles, leur sécurisation est devenue un enjeu incontournable. Cette sécurisation va garantir la confidentialité l'intégrité et la disponibilité et la non répudiation. Et pour cela des nombreux moyens sont disponibles tels que les solutions matérielles, logiciels, ou les systèmes de détection d'intrusion, l'antivirus, les réseaux privés ou encore les firewalls (pare feu) qui est un élément matériel ou logiciel permettant de filtrer les paquets de données qui traversent un réseau en bloquent certain et autorisant d'autres. Ce mécanisme de sécurité offre plusieurs fonctionnements qui aident à mettre en place une politique de sécurité efficace.

1.1 Introduction aux reseaux

Les réseaux sont nés du besoin de transporter des données d'un ordinateur à un autre ordinateur. Ces données étant mises sous la forme des fichiers, l'application de base des réseaux est donc le transfert des fichiers. Un peu plus tard, le "transactionnel" est apparu pour permettre à un utilisateur de réaliser des transactions avec un ordinateur distant, par exemple réserver une place d'avion. Une session correspond à l'ensemble des transactions d'un même utilisateur pour réaliser une tâche donnée. Et avec l'application du Web, le service transactionnel s'est diversifié afin de permettre la recherche d'information par le biais de lien. Ces applications s'appellent client-serveur, c'est-à-dire qu'un client s'adresse à un serveur pour obtenir de l'information.

L'étape suivante des réseaux a été par caractérisée le pair-à-pair, ou P2P (peer-to-peer). Dans cette application, tous les éléments connectés au réseau sont équivalents et peuvent être distribués dans le réseau. Les applications pair-à-pair sont bien connues, en particulier de ceux qui recherchent les fichiers audio ou vidéo sur Internet. Et les applications sous-jacentes en fait sont très nombreuses, allant de la téléphonie à la recherche d'informations diverses et variées.

Sans que cela supprime les applications de transfert de fichiers, qu'elles soient client-serveur ou pair à pair, le nouveau service Internet qui se développe depuis les années 2010 est le Cloud, ou "nuage". Jusqu'à l'arrivée des Clouds, le réseau Internet avait pour objectif de transporter des données pour réaliser un service à distance. Les entreprises permettaient aux itinérants de connecter à leurs serveurs par le biais d'Internet. Elles possédaient tous les serveurs nécessaires à cela, comme la messagerie électronique, les applications métiers ou les serveurs d'archivage, ainsi que la puissance de calcul nécessaire. Aujourd'hui, il est possible de réaliser dans le Cloud ce qui se faisait auparavant dans l'entreprise: calcul, stockage, application métier, messagerie, téléphonie, etc.

Les avantages sont nombreux : le client peut accéder à ces services de n'importe où : ils peuvent être sécurisés par de la redondance; on peut ajouter instantanément de nouveaux services, de la puissance de calcul, de l'espace de stockage, etc.., au fur et à mesure des besoins, en ne payant que ce qui est utilisé.

Cette nouvelle génération met en œuvre le concept de virtualisation, par lequel les ressources dont l'entreprise ou le particulier à besoin peuvent se trouvent n'importe où, voire se déplacer en fonction du cout des serveurs. [1]

1.2 Les reseaux informatique

Les réseaux informatiques sont nés du besoin de relier des terminaux distants à un site central puis des ordinateurs entre eux et enfin des machines terminales, telles que stations de travail ou serveurs. Dans un premier temps, ces communications étaient destinées au transport des données informatiques. Aujourd'hui, l'intégration de la parole téléphonique et les vidéos est généralisées dans les réseaux informatiques.

On distingue généralement cinq catégories de réseaux informatiques, différenciées par la distance maximale séparant les points les plus éloignés du réseau (Figure (1.1)) :

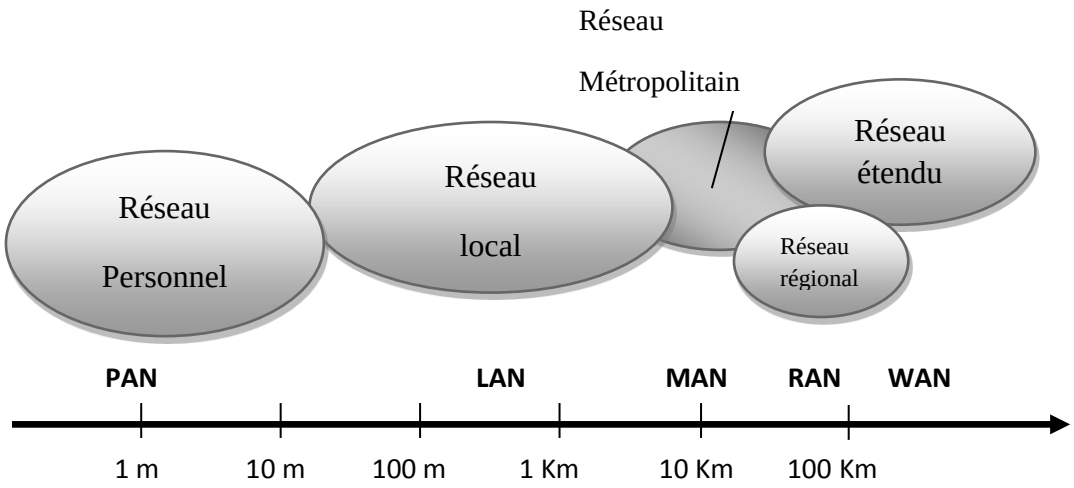
1.2.1 Les réseaux personnels : PAN (Personnel Area Network), qui interconnectent sur quelques mètres des équipements personnels tels que téléphone mobile, portables, etc.., d'un même utilisateur.

1.2.2 Les réseaux locaux : LAN (Local Area Network), qui correspondent par leur taille aux réseaux intra-entreprises. Ils servent au transport de toutes les informations numériques de l'entreprise. En règle générale, les bâtiments à câbler s'étendent sur des centaines de mètres. Les débits de ces réseaux vont aujourd'hui de quelques mégabits à plusieurs centaines de mégabits par seconde.

1.2.3 Les réseaux métropolitains : MAN (Metropolitan Area Network), qui permettent l'interconnexion des entreprises ou éventuellement des particuliers sur un réseau spécialisé à haut débit qui est géré à l'échelle d'une métropole, Ils doivent être capables d'interconnecter les réseaux locaux des différentes entreprises pour leur donner la possibilité de communiquer avec l'extérieur.

1.2.4 Les réseaux régionaux : RAN (Régional Area Network), ont pour objectif de couvrir une large surface géographique. Dans le cas des réseaux sans fil, les RAN peuvent avoir une cinquantaine de Kilomètres de rayon, ce qui permet, à partir d'une seule antenne, de connecter un très grand nombre d'utilisateurs.

1.2.5 Les réseaux étendus : WAN (Wide Area Network), sont destinés à transporter des données numériques sur des distances à l'échelle d'un pays, voire d'un continent ou de plusieurs continents. Le réseau est soit terrestre, il utilise en ce cas des infrastructures au niveau du sol, essentiellement les grands réseaux de fibre optique, soit hertzien, comme les réseaux satellite, mais seulement pour des applications particulières à débit faible. [1]



PAN (Personnel Area Network) **MAN** (Metropolitan Area Network)

LAN (Local Area Network) **RAN** (Regional Area Network)

WAN (Wide Area Network)

Figure (1.1) : Les catégories des réseaux informatiques [1]

1.3 Avantages des réseaux (Qu'apportent les réseaux)

En réalité il y a une grande variété des services et avantages offertes par les réseaux, on peut citer :

1.3.1 Une communication rapide et facile

Lorsque le réseau informatique fonctionne correctement, vous arriverez à utiliser facilement les supports et matériels de communication comme les e-mails, la messagerie instantanée, les lignes téléphoniques, la vidéoconférence, toutes les personnes dans le groupe peuvent pleinement en profiter.

Avoir un réseau informatique, vous permet également d'optimiser votre temps sur le partage des fichiers et données informatiques. C'est l'un des principaux avantages d'un réseau, avec une capacité de partage, les utilisateurs arrivent à trouver et partager les données dont ils auront besoin. Depuis des années, ce système du réseau informatique est devenu le plus utilisé par les grandes organisations afin de maintenir leurs données d'une manière organisée et facilite les accès pour les personnes souhaitées.

Un autre avantage important du réseau aussi est sa capacité à diminuer l'achat et l'utilisation de plusieurs matériels en même temps. Le réseau peut faire en sorte qu'il n'y a pas besoin d'avoir des importantes individuelles pour chaque ordinateur dans l'entreprise. Cela permettra de réduire considérablement le coût de l'achat de matériel.

1.3.2 Partage des logiciels

Les utilisateurs peuvent facilement partager les logiciels au sein du réseau. La majorité des grandes entreprises optent déjà pour cette pratique afin de réduire les achats des logiciels. Le partage et transfert de fichiers au sein des réseaux est très rapide, en fonction du type de réseau. Cela permettra d'économiser du temps tout en maintenant l'intégrité des fichiers.

1.3.3 Données informatiques bien sécurisées

Des fichiers et des programmes sensibles sur un réseau peuvent être protégés à l'aide des mots de passe ou des programmes adéquats. Ces fichiers seront uniquement accessibles par des personnes autorisées. Cette démarche permet de réduire les préoccupations autour de la sécurité informatique. Aussi chaque utilisateur a son propre ensemble de privilèges pour empêcher toutes personnes d'accéder aux fichiers et programmes.

1.4 Les modèles d'interconnexion

Il existe deux modèles de d'interconnexion dans les réseaux : le modèle client-serveur et le modèle Pair-à-Pair (Peer to Peer). [2]

1.4.1 Le modèle client-serveur

Un serveur est un ordinateur (équipé d'un logiciel serveur) dont le rôle est de répondre aux requêtes envoyées par des ordinateurs clients (équipés d'un logiciel client) (Figure 1.2). Le client envoie une requête au serveur, le serveur traite la requête et retourne une réponse, par exemple :

- Un serveur WEB met à disposition du client des pages web
- Un serveur FTP permet au client le téléchargement ou le dépôt des fichiers
- Un serveur de messagerie sert à la gestion de transfère de courrier électronique

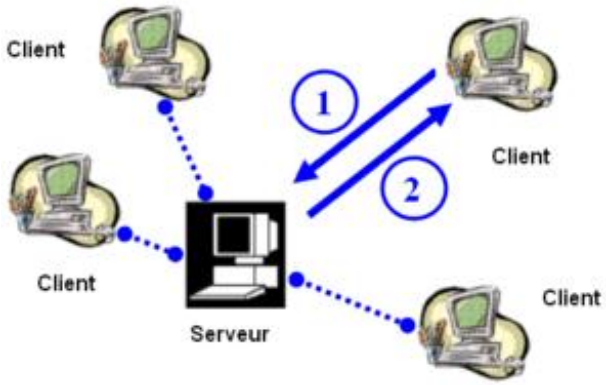


Figure (1.2) : Le modèle client-serveur [2]

1.4.2 Le modèle Pair-à-Pair (Peer to PeerP2P)

Dans ce modèle, tous les ordinateurs ont le même rôle. Ils sont équipés d'un logiciel (assimilé à un logiciel client-serveur) et peuvent communiquer et échanger les informations entre eux (Figure 1.3).

Les applications de partage de fichiers reposent sur ce modèle.

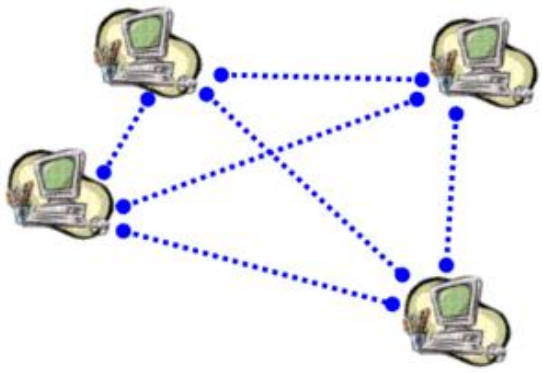


Figure (1.3) : Le modèle P2P [2]

1.5 Modèle de communication OSI

1.5.1 Définition :

Les données à transmettre d'une machine à une autre sont fragmentées a l'´émission en petit blocs de quelques centaines d'octets munis de l'adresse du destinataire, envoyées sur le réseau et réassemblées a la réception pour reproduire les données d'origine. Ce concept facilite le partage des possibilités physiques du réseaux (bande passante) et est parfaitement adapte pour une implémentation sur machines séquentielles travaillant en temps partagé (plusieurs communications peuvent alors avoir lieu simultanément et sur une même machine).

Partant de ce concept, un modèle d'architecture pour les protocoles de communication a été développe par l'ISO (International Standards Organisation) entre 1977 et 1984. Ce modèle sert souvent de référence pour décrire la structure et le fonctionnement des protocoles de communication, mais n'est pas une contrainte de spécification.

Ce modèle est nommé OSI comme (Open System Interconnexion Référence Model). Les constituants de ce modèle sont si largement employés qu'il est difficile de parler de réseaux sans y faire référence.

La forme d'organisation de ce modèle n'est pas due au hasard, c'est celle sur laquelle les informaticiens ont beaucoup travaillé dans les années soixante pour définir les caractéristiques des systèmes d'exploitation. [3]

1.5.2 Architecture du modèle

Le modèle OSI est constitué de sept couches. A chaque couche est associée une fonction bien précise, l'information traverse ces couches, chacune y apporte sa particularité.

Une couche ne définit pas un protocole, elle délimite un service qui peut être réalise par plusieurs protocoles de différentes origines. Ainsi chaque couche peut contenir tous les protocoles que l'on veut, pourvu que ceux-ci fournissent le service demandé à ce niveau du modèle (Figure 1.4).

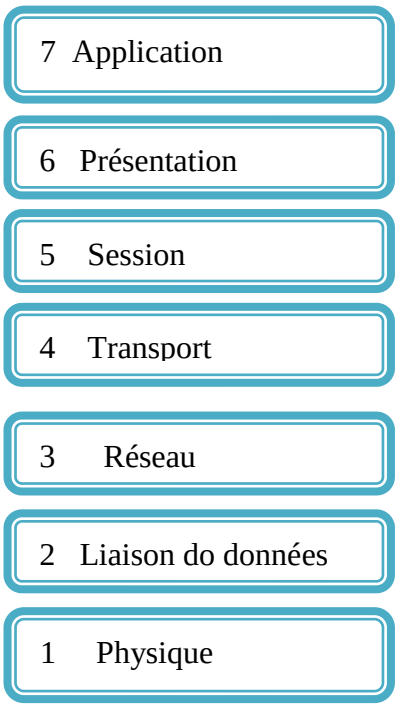


Figure (1.4) : Modèle de communication OSI [3]

1.5.3 Les couches du modèle de référence

Le modèle de référence OSI comportes sept niveaux protocolaires plus un médium physique. Le medium physique que l'on appelle le niveau 0, correspond au support physique de communication chargé d'acheminer les éléments binaires d'un point à un autre jusqu'au récepteur final .ce medium peut prendre diverses formes allons du câble métallique aux signaux hertziens, en passant par la fibre optique et l'infrarouge. [1]

1.5.3.1 La couche physique (Niveau élément binaire)

La couche physique contient les règles et procédures à mettre en œuvre pour acheminer les éléments binaires sur le medium physique. On trouve dans la couche physique les équipements réseau qui traitent l'élément binaire, comme les modems, concentrateurs, ponts, hubs, etc.

Les différentes topologies de support physique affectent le comportement de la couche physique. Dans les entreprises les palans de câblages ont une importance parfois déterminante pour le reste de l'architecture. La couche physique nécessite de surcroit un matériel fiable, et il faut parfois dupliquer ou mailler le réseau pour obtenir des taux de défaillances acceptables.[1]

1.5.3.2 La couche liaison (Niveau trame)

La trame est l'entité transportée sur les lignes physiques. Elle contient un certain nombre d'octets transportés simultanément. Le rôle du niveau trame consiste à envoyer un ensemble d'éléments binaires sur une ligne physique de telle façon qu'il puisse être récupérés correctement par le récepteur. Sa première fonction est de reconnaitre, lors de l'arrivée des éléments binaires, les débuts et fins de trame. C'est la aujourd'hui le rôle principal de cette couche, qui a été fortement modifiée depuis son introduction dans le modèle de référence.

Au départ, elle avait pour fonction de corriger les erreurs susceptibles de se produire sur le support physique, de sorte que le taux d'erreur résiduelle reste négligeable. En effet, s'il est impossible de corriger toutes les erreurs, le taux d'erreur non détectée doit rester négligeable. Le seuil partir duquel on peut considérer le taux d'erreur comme négligeable est dépendant de l'application et ne constitue pas une valeur intrinsèque.

La solution préconisée aujourd'hui pour traiter les erreurs est d'effectuer la correction d'erreur non plus au niveau trame, mais au niveau application. On peut déterminer un taux d'erreur limite entre l'acceptable et l'inacceptable. Comme les medias physiques sont les plus en plus performants, il est généralement inutile de mettre en œuvre des algorithmes complexes de correction d'erreur. En effet, seules les applications pour lesquelles un taux d'erreur donné peut devenir inacceptable doivent mettre en place des mécanismes de reprise sur erreur.

La couche2 comporte également les règles nécessaires au partage d'un même support physique entre plusieurs stations. Beaucoup de normes et de recommandations concernant cette couche provenant de l'ISO, la norme HDLC (High level data link control) a été la première vraie norme à codifier les procédures de communication entre ordinateurs.

L'ISO a mis au point un ensemble de normes additionnelles de niveau trame concernant les réseaux locaux, les méthodes d'accès et le protocole de liaison. [1]

1.5.3.3 La couche réseau (Niveau paquet)

La couche 3 est appelée couche réseau dans le modèle de référence parce que l'échange de paquets de bout en bout donne naissance à un réseau. Le niveau paquet doit permettre d'acheminer correctement les paquets d'infirmation jusqu'à l'utilisateur final. Pour aller de l'émetteur au récepteur, il faut passer par des nœuds de transfert intermédiaires ou par des passerelles, qui interconnectent deux ou plusieurs réseaux.

Un paquet n'est pas une entité transportable sur une ligne physique, car si l'on émet les bits directement sur le support, il n'est pas possible de détecter la limite entre deux paquets arrivant au récepteur. Il y a donc obligation d'encapsuler les paquets dans des trames pour permettre leur transport d'un nœud vers un autre nœud (Figure 1.5).

Le niveau paquet nécessite trois fonctionnalités principales : le contrôle de flux, le transfert (routage ou commutation) et l'adressage.

- **Contrôle de flux** : Evite les embouteillages de paquets dans le réseau. Le retard provenant des surcharges de certaines parties du réseau peuvent en effet rendre le temps de réponse inacceptable pour l'utilisateur. Si le contrôle de flux échoue, un contrôle de congestion fait normalement revenir le trafic à une valeur acceptable par le réseau.

- **Routage et commutation** : permettent d'acheminer les paquets d'information vers leurs destinations au travers du maillage des nœuds de transfert. Dans la commutation les paquets suivent toujours le même chemin, alors que le routage, la route peut changer. Le routage ou la commutation ne remplace pas le contrôle de flux mais peut être vue comme une de ces composantes, dont il faut tenir compte pour optimiser le temps de réponse. Les techniques de commutation peuvent être centralisé ou distribuées, suivant l'option choisis par le gestionnaire de réseau : soit les tables de routage ou de commutation sont conçues par un nœud central, soit elles sont créées par chaque nœud.

- **L'Adressage** : La dernière grande fonction de la couche réseau consiste à gérer les adresses des équipement terminaux, pour cela, il faut ajouter des adresses complètes dans les différents paquets, pour ce qui concerne le routage, ou dans le paquet de signalisation qui ouvre le chemin, pour la commutation. Les adresses forment un vaste ensemble qui doit regrouper toutes les machines terminales du monde. L'ISO a dû prévoir une norme d'adressage susceptible de répertorier l'ensemble des équipements terminaux. Dans le monde TCP/IP un adressage par réseau a été choisi.

Pour mettre en place et développer les fonctionnalités de la couche réseau il est possible de choisir entre deux grandes méthodes d'accès :

- **Le mode avec connexion** : dans lequel l'émetteur et le récepteur se mettent d'accord sur un comportement commun et négocient les paramètres et les valeurs a mettre en œuvre.

- **Le mode sans connexion :** qui n'impose pas de contrainte a l'émetteur par rapport au récepteur.

Le mode avec connexion concerne les techniques de commutation dans lesquels un chemin doit être mis en place. Avec l'aide de la signalisation, la connexion est mise en place avant que débute le transfert de trames. Les modes ATM et MPLS font partie de ces catégories. Le protocole IP travaille en mode sans connexion : le transfert des paquets démarre immédiatement sans que les deux extrémités se mettent d'accord sur les caractéristiques de la communication. [1]

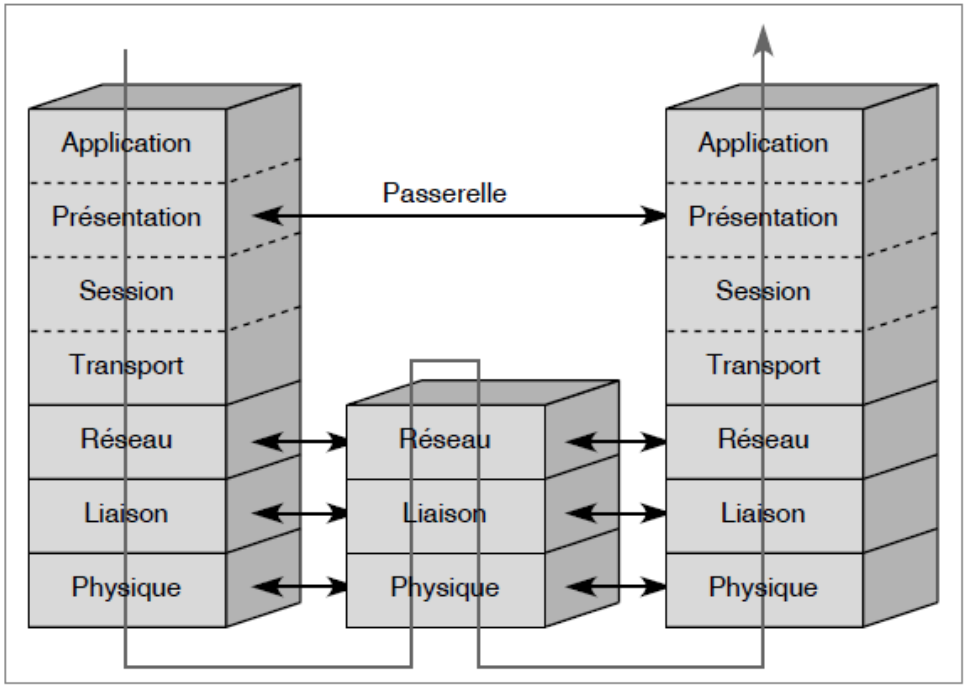


Figure (1.5) : couche réseau (Niveau paquet) [1]

1.5.3.4 La couche de transport (Niveau message)

Le niveau message prend en charge le transport du message de l'utilisateur d'une exteremité a une autre du reseau. Ce niveau est appelé couche transport pour bien indiquer qu'il s'agit de transporter les données de l'utilisateur. Il represente le quatriemme niveau de 'architecture, son nom est aussi couche 4.

Le service de transport doit optimiser l'utilisation des infrastrictures sous-jacentes en vue d'un bon rapport qualité prix.

La couche 4 optimise les ressources d'un réseau de communication en gérant un contrôle de flux ou un multiplexage des messages sur une connexion réseau. Cette couche de contrôle est l'ultime niveau qui s'occupe de l'acheminement de l'information. Elle permet de complété le travail accompli par les couches précédentes. C'est grâce à elle que l'utilisateur obtient la qualité de service susceptible de la satisfaire. Le protocole de niveau message à mettre en œuvre à ce niveau dépond du service rendu par les trois premières couches et de la demande de l'utilisateur.

La couche 4 aujourd'hui la plus utilisée provient de l'architecture du monde internet et plus exactement de la norme TCP (Transmission Control Protocol). Et la norme UDP (User Datagram Protocol). [1]

1.5.3.5 La couche Session (Niveau connexion)

Le rôle de la couche session est de fournir aux entités de présentation les moyens nécessaires à l'organisation et à la synchronisation de leur dialogue. A cet effet, cette couche fournit les services permettant l'établissement d'une connexion, son maintien et sa libération, ainsi que ceux permettant des interactions entre les entités de présentation.

Ce niveau est aussi le premier de l'architecture réseau a se situer hors de la communication proprement dite. Comme nom l'indique, la couche session a pour fonction d'ouvrir et de fermer des sessions entre utilisateurs. Il est intitule d'émettre de l'information s'il n y a personne à l'autre extrémité pour récupérer ce qui a été envoyé. Il faut donc s'assurer que l'utilisateur que l'on veut atteindre ou du moins son représentant qui peut être une boite aux lettres électroniques par exemple est présent.

La couche 5 comporte des fonctionnalités rendant possibles l'ouverture la fermeture et le maintien de la connexion. Les mises en correspondances des connexions de session et des connexions de transport sont effectuées une à une.

De nombreuse autres possibilités peuvent être ajoutées aux commandes de base, appelées primitives, indispensables à la mise en place de la session. La pose de point de resynchronisation, par exemple, est recommandée. Ils permettent en cas de problème de disposer d'un point précis sur lequel il y a accord entre les deux parties communicantes a partir duquel l'échange peut redémarrer. La gestion des interruptions et des reprises de session est également une fonctionnalité souvent implémentée.

Pour ouvrir une connexion avec une machine distante la couche session doit posséder un langage qui soit intelligible par l'autre extrémité. C'est pourquoi avant d'ouvrir une connexion il est obligatoire de passer par le niveau présentation qui garantit l'unicité du langage, et le niveau application qui permet de travailler sur des paramètres définis d'une façon homogène. [1]

1.5.3.6 La couche Présentation (Niveau syntaxe)

La couche de présentation se charge de la syntaxe des informations que les entités d'application se communiquent. Deux aspects complémentaires sont définit dans la norme :

La représentation de données transférées entre entités d'application

La représentation de la structure de données a laquelle les entités se réfèrent au cours de leur communication et la représentation de l'ensemble des actions effectuées sur cette structure de données.

En d'autres termes la couche présentation s'intéresse à la syntaxe tandis que la couche application se charge de la sémantique. La couche présentation joue un rôle important dans un environnement hétérogène. C'est un intermédiaire indispensable pour une compression commune de la syntaxe des documents transportés sur le réseau. Les différentes machines connectées n'ayant pas la même syntaxe pour exprimer les applications qui s'y effectuent, si on les interconnecte directement, les données de l'une ne peuvent généralement pas être comprises de l'autre. La couche 6 procure un langage syntaxique commun à l'ensemble des utilisateurs connectés.

Si Z est le langage commun, et si une machine X veut parler à a une machine Y, elles utilisent des traducteurs X-Z pour discuter entre elles. Si toutes les machines terminales possèdent en natif un langage syntaxique commun, les traductions deviennent inutiles.

La syntaxe abstraite ANS1 (Abstract Syntax Notation) normalisée par l'ISO est le langage de base de la couche présentation. Fondé sur la syntaxe X.409 du CCITT (consultative commite for international tegraph and telephone), ASN1 est une syntaxe suffisamment complexe pour prendre facilement en compte les grandes classes d'applications comme la messagerie électronique, le transfert de fichiers le transactionnel, etc.

La normalisation de la couche comprend les normes suivantes :

- ISO 824, ou CCITT X.208 qui définit la syntaxe ASN 1
- CCITT X.216 et X.226, qui définissent le service et le protocole de la couche session. [1]

1.5.3.7 La couche application (Nouveau sémantique)

La couche application est la dernière du modèle de référence, elle fournit au processus applicatifs le moyen d'accéder à l'environnement réseau. Ces processus échangent leurs informations de type sémantique par l'intermédiaire des entités d'application.

De très nombreuses normes ont été définies pour cette couche. En ce qui concerne la définition de la couche même, c'est la norme ISO 9545, ou CCITT X.207 qui décrit sa structure.

La couche application contient toutes les fonctions impliquant des communications entre systèmes, en particulier si elles ne sont pas réalisées par les niveaux inferieur. Elle s'occupe essentiellement de la sémantique, contrairement à la couche présentation, qui prend en charge la syntaxe. [1]

1.6 Le protocole TCP/IP

1.6.1 Définition :

Dans les années 1970, le département de la défense américain, ou DOD (Departement Of Defense) décide devant le foisonnement de machines utilisant des protocoles de communication différents et incompatibles, de définir sa propre architecture. Elle est aussi adoptée par de nombreux réseaux privés, appelés intranet. [1]

Les deux principaux protocoles définis dans cette architecture sont les suivants :

- **IP (Internet Protocol)** : de niveau réseau, qui assure un service sans connexion.
- **TCP (Transmission Control Protocol)**: de niveau transport qui fournit un service fiable avec connexion. [1]

Le TCP/IP définit une architecture en couches qui incluent également, sans qu'elle soit définie explicitement, une interface d'accès au réseau. En effet de nombreux sous-réseaux distincts peuvent être pris en compte dans l'architecture TCP/IP, de type aussi bien local qu'étendu.

Cette architecture est illustrée à la **figure (1.6).** Il faut noter dans cette figure l'application d'un autre protocole de niveau message (Couche 4) UDP (User Datagram Protocol). Ce protocole utilise un mode sans l'autre connexion, qui permet d'envoyer des messages sans l'autorisation du destinataire. [1]

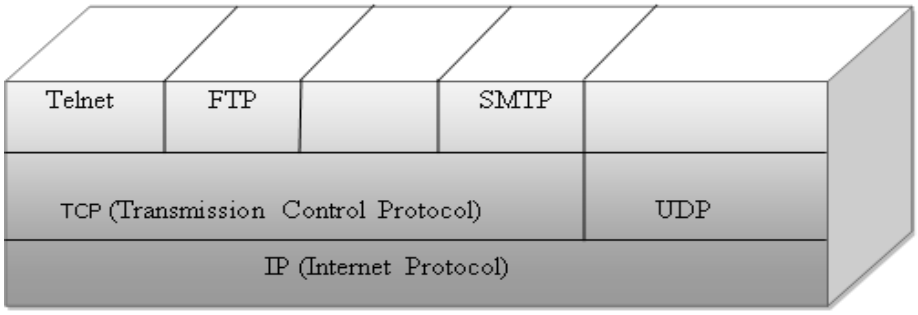


Figure (1.6) : Architecture TCP/IP [1]

Cette architecture a pour socle le protocole IP, qui correspond au niveau paquet (Couche3) de l'architecture du modèle de référence. En réalité, il ne correspond que partiellement à ce niveau.

Le protocole IP a été conçu comme protocole d'interconnexion, définissant un bloc de données d'un format bien défini et contenant une adresse, mais sans autre fonctionnalité. Son rôle était de transporter ce bloc de données dans un paquet selon n'importe quelle autre technique de transfert de paquets. Cela vaut pour la première génération du protocole IP appelées IPV4, qui est encore massivement utilisée aujourd'hui. La deuxième version du protocole IP, IPV6 joue réellement un rôle de niveau paquet, avec de nouvelles fonctionnalités permettant de transporter les paquets d'une extrémité du réseau a un autre avec une certaine sécurité. [1]

Les paquets IP sont indépendant les uns des autres et sont routés individuellement dans le réseau par le biais de routeurs. La qualité de service proposée par le protocole IP est très faible, sans détection de paquets perdus ni de possibilité de reprise sur erreur.

Le protocole TCP regroupe les fonctionnalités de niveau message (Couche4) du modèle de référence. C'est un protocole assez complexe, qui comporte des nombreuses options permettant de résoudre tous les problèmes de pertes de paquet dans les niveaux inférieurs. En particulier, un fragment perdu peut être récupéré par retransmission sur le flot d'octets. Le protocole TCP est en mode avec connexion, contrairement à UDP, ce dernier protocole se positionne aussi au niveau transport mais dans un mode sans connexion et n'offre pratiquement aucune fonctionnalité. Il ne peut prendre en compte que les applications qui demandent peu de service de la couche transport. [1]

Les protocoles situés au-dessous de TCP et UDP sont de type applicatif.

Toute la puissance de cette architecture repose sur la souplesse de sa mise en œuvre au-dessous de n'importe quel réseau existant. Soi, par exemple X et Y respectivement un réseau local et réseau étendu à commutation de cellules ou de paquets. Le protocole IP est implémenté sur toutes les machines connectées à ces deux réseaux. Pour qu'il soit possible de passer d'un réseau a l'autre, un routeur, dont le rôle est décapsuler le paquet arrivant du réseau X et de récupérer le paquet IP, est mis en place. Apres traitement du routage le paquet IP est encapsulé dans le paquet du réseau Y. le rôle du routeur est comme son nom l'indique, le routage du paquet vers la bonne destination. [1]

L'architecture d'interconnexion du réseau Internet est illustrée à la figure (1.7).

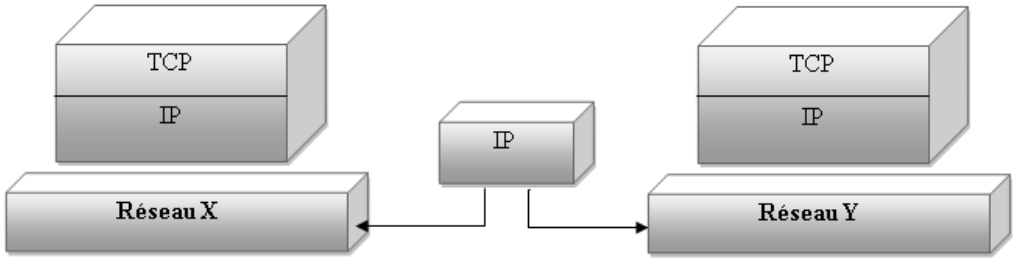


Figure (1.7) : Architecture d'interconnexion du réseau Internet [1]

La souplesse de cette architecture peut parfois être un défaut, dans le sens ou l'optimisation globale du réseau est effectuées sous-réseau par sous-réseau, c'est-à-dire qu'elle est obtenue par une succession d'optimisations locales.

Une particularité importantes de l'architecture TCP/IP est que l'intelligence et le contrôle du réseau se trouvent en presque totalité dans la machine terminale et non pas dans le réseau. C'est le protocole TCP qui se charge d'envoyer plus ou moins de paquets dans le réseau en fonction de l'occupation de celui-ci. L'intelligence de contrôle se trouve dans le PC extrémité et plus précisément dans le logiciel TCP. La fenêtre de contrôle de TCP augmente ou diminue le trafic suivant la vitesse requise pour faire un aller-retour. Le cout de l'infrastructure est extrêmement bas puisque le nombre de logiciels, et donc l'essentiel de l'intelligence, se trouvent dans les machines terminales. Le service rendu par ce réseau est de type best-effort, ce qui signifie que le réseau fait de son mieux pour écouler le trafic. [1]

Le protocole IPV6 apporte une nouvelle dimension, puisqu'il introduit des fonctionnalités inédites qui rendent les nœuds du réseau plus intelligents. Les routeurs de nouvelle génération possèdent des algorithmes de gestion de qualité de service en vue d'assurer un transport capable de satisfaire à des contraintes temporelle ou de perte de paquets. Ce pendant le protocole IPV4 à bien réagi aux nouveautés par IPV6, en modifiant certains champs pour proposer les mêmes améliorations.

Dans la version classique d'IPV4 chaque nouveau client n'est pas traité différemment de ceux qui sont déjà connecté, et les ressources sont distribuées équitablement entre tous les utilisateurs.

Les politiques d'allocation des ressources des opérateurs de télécommunications sont totalement différent, un client possédant déjà une certaine qualité de service ne devant pas être pénalisé par l'arrivée d'un nouveau client. Comme nous le verrons la solution aujourd'hui préconisée dans l'environnement Internet est de favoriser, dans la mesure possible les clients ayant des exigences de temps réel, et ce par des protocoles adaptés.

Les applications disponibles au-dessus de l'environnement TCP/IP sont nombreuses et variées. Elles incluent la messagerie électronique (SMTP) le transfert de fichier (FTP), les bases de données distribuées avec le World Wide Web (WWW) et bien d'autre. [1]

1.6.2 Architecture de TCP/IP

La plupart des descriptions de TCP/IP définissent une architecture de protocole comportant quatre niveaux fonctionnels (du bas vers le haut) :

- **Couche Accès réseau** : Comporte les routines permettant d'accéder aux réseaux physiques
- **Couche Internet** : Définit le datagramme et prend en charge le routage des données.
- **Couche Transport (TCP / UDP)** : Assure les services de transmission de données de bout en bout.
- **Couche Application** : Comporte les applications et processus utilisant le réseau. [4]

1.6.2.1 Couche Accès réseau

C'est la couche la plus basse qui représente la connexion physique avec les câbles, les circuits d'interfaces électriques (transceivers), les cartes coupleurs, les protocoles d'accès au réseau. Cette couche réseau TCP/IP intègre généralement les fonctions des deux couches inférieures du modèle de référence OSI (Liaison de Données et Physique).

Les utilisateurs ignorent souvent cette couche, la conception de TCP/IP cachant les fonctions des couches inférieures. Etant donné que les protocoles de cette couche font partie intégrante du système d'exploitation, ils apparaissent souvent sous la forme d'une combinaison de pilotes de périphériques (Drivers) et de programmes associés. [4]

1.6.2.2 Couche Internet

La couche Internet doit fournir une adresse logique pour l'interface physique. L'implémentation du modèle TCP/IP de la couche Internet est IP (Internet Protocol). Cette couche fournit un mappage entre l'adresse logique et l'adresse physique fournie par la couche Accès réseau grâce aux protocoles ARP (Address Resolution Protocol – RFC 826) et RARP (Reverse Address Resolution Protocol).

Les incidents, les diagnostics et les conditions particulières associées au protocole IP relèvent du protocole ICMP (Internet Control Message Protocol), qui opère aussi au niveau de la couche Internet.

La couche Internet est aussi responsable du routage des paquets de données, les datagrammes, entre les hôtes. Cette couche est utilisée par les couches plus hautes du modèle TCP/IP. [4]

1.6.2.3 Couche Transport

La couche Transport hôte à hôte ou Transport en abrégé, définit les connexions entre deux hôtes sur le réseau. Le modèle TCP/IP comprend deux protocoles hôte à hôte :

- **TCP (Transmission Control Protocol)**: protocole responsable du service de transmission fiable de données avec détection et correction d'erreurs. TCP permet aussi les connexions simultanées. Plusieurs connexions TCP peuvent être établies sur un hôte, et les données sont envoyées simultanément. TCP permet des connexions full-duplex.

- **UDP (User Datagram Protocol)**: protocole peu fiable, utilisé par des applications qui n'exigent pas la fiabilité comme le TCP. [4]

1.6.2.4 Couche Application

La couche Application constitue le sommet de l'architecture TCP/IP. Elle permet aux applications d'utiliser les protocoles de la couche hôte à hôte (TCP et UDP) pour transmettre leurs données. Parmi les protocoles d'applications les plus répandus (orientés utilisateurs), on trouve (qu'on va les détailler dans ce chapitre) :

- **TELNET :** le protocole de terminal de réseau (Terminal Emulation), permettant l'ouverture d'une session à distance sur un réseau.
- **FTP (File Transfert Protocol)** : le protocole de transfert de fichiers
- **SMTP (Simple Mail Transfer Protocol):** le protocole de transfert de courrier électronique, il est aussi (orientés administrateurs).
- **DNS (Domain Name Service)** : également appelé Name service qui permet d'établir la correspondance entre les adresses IP et les noms attribués aux hôtes du réseau.
- **RIP (Routing Information Protocol)** : permettant de gérer la fonction de routage.
- **NFS (Network File System)** : permettant de partager des fichiers entre différentes machines-hôtes du réseau. [4]

1.7 Comparaison des modèles OSI et TCP/IP

Comme dans le modèle OSI, les données sont transmises de haut en bas dans la pile lors de leur envoi sur le réseau, et de bas en haut dans la pile lors de leur réception à partir du réseau.

Chaque couche de la pile ajoute des informations de contrôle, un en-tête, de manière à garantir une transmission des données correcte.

Chaque couche possède ses propres structures de données indépendantes. La terminologie utilisée pour décrire les données au niveau de chaque couche diffère dans les deux modèles :

Dans le modèle OSI, l'expression PDU (Protocol Data Unit) est employée pour décrire les données d'une couche.

Dans le modèle TCP/IP les termes message et flot sont utilisés au niveau de la couche application, les termes segment et paquet, au niveau de la couche hôte à hôte ; le terme datagramme au niveau de la couche Internet, et le terme trame au niveau de la couche accès réseau (voir la figure 1.8). [5]

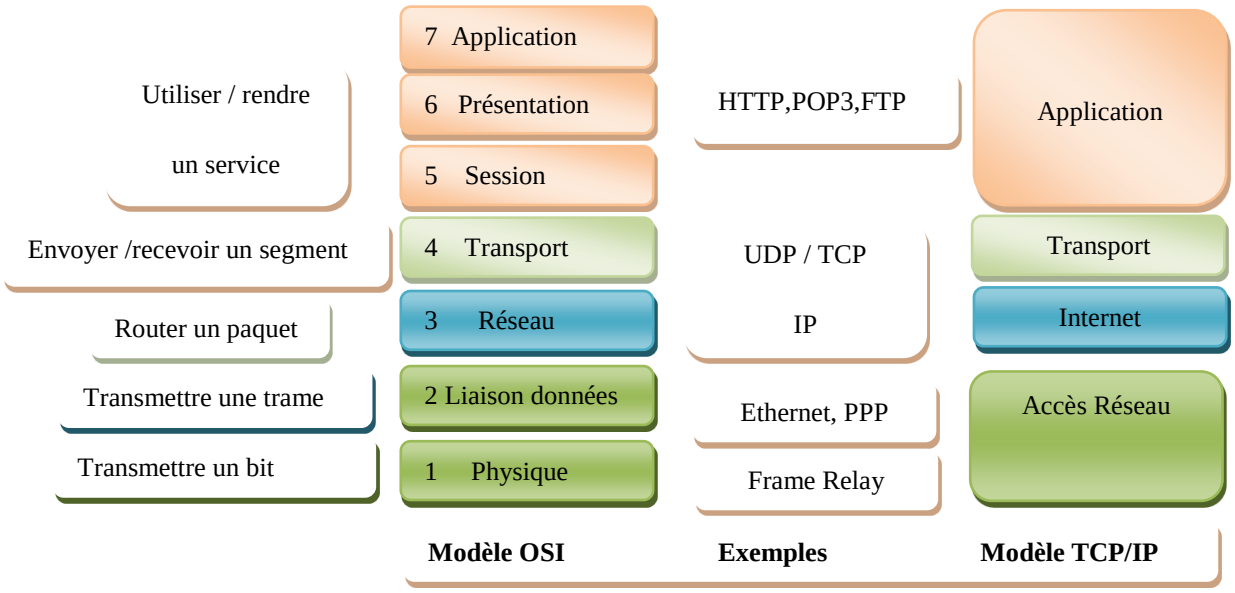


Figure (1.8) : **Comparaison des modèles OSI et TCP/IP** [5]

1.8 L'adressage IP

1.8.1 Définition

En réalité l'Internet est un réseau virtuel, construit par interconnexion de réseaux physiques via des passerelles. Nous allons décrire : l'adressage le maillon essentiel du protocole TCP/IP, qui fait apparaitre l'internet comme une entité homogène.

Un système de communication doit pouvoir permettre a n'importe quel hôte de se mettre en relation avec n'importe quel autre. Afin qu'il n'y ait pas d'ambiguïté pour la reconnaissance des hôtes possibles, il est absolument nécessaire d'admettre un principe général d'identification.

Lorsque l'on veut établir une communication, il est intuitivement indispensable de posséder trois informations : le nom de la machine distante, son adresse, la route à suivre pour y parvenir.

En règle générale les utilisateurs préfèrent des noms symboliques pour identifier les machines tandis que les processeurs de ces mêmes machines ne comprennent que les nombres exprimés au format binaire.

Les adresses IP (IPV4) sont standardisées sous forme d'un nombre de 32 bits qui permet à la fois l'identification de chaque hôte et du réseau auquel il appartient. Le choix des nombres composants d'une adresse IP n'est pas laissé au hasard, au contraire il fait l'objet d'une attention particulière notamment pour faciliter les opérations de routage.

Chaque adresse IP contient donc deux informations élémentaires, une adresse de réseau et une adresse d'hôte. La combinaison des deux adresse désigne de manière unique une machine et une seule sur le réseau Internet, sous réserve que cette adresse ait été attribuée par un organisme ayant pouvoir de le faire. [6]

1.8.2 Délivrance des adresses IPv4

On distingue deux types d'adresses IP :

1.8.2.1 Les adresses privées : Que tout administrateur de réseau peut s'attribuer librement pourvu qu'il ne cherche pas à les router sur l'Internet.

Les adresses à utiliser sur les réseaux prives sont :

Préfixe	Plage IP	Nombre d'adresses
10.0.0.0	10.0.0.0 - 10.255.255.255	16 777 216
172.16.0.0	172.16.0.0 - 172.31.255.255	1 048 576
192.168.0.0	192.168.0.0 - 192.168.255.255	65 536

Tableau (1.1) : Les adresses privées [7]

1.8.2.2 Les adresses publiques : délivrées par une structure mondiale qui en assurent l'unicité de chaque adresse. Ce dernier point est capital pour assurer l'efficience du routage.

Les routeurs (par exemple : votre modem) disposent d'une adresse IP publique côté internet, ce qui rend votre box visible sur internet. Et aussi, lorsque vous accédez à un site web vous utilisez l'adresse publique du serveur web.

Une adresse IP publique est unique dans le monde, ce qui n'est pas le cas des adresses privées qui doivent être unique dans un même réseau local mais pas au niveau planétaire étant donné que ces adresses ne peuvent pas être routées sur internet.

Les adresses IP publiques représentent toutes les adresses IP des classes A, B et C qui ne font pas partie de la plage d'adresses privées de ces classes ou des exceptions de la classe A **(**127.0.0.0 et 0.0.0.0). [7]

1.8.3 Anatomie d'une adresse IP

Une adresse IP est un nombre de 32 bits que l'on a coutume de représenter sous forme de quatre entiers de huit bits s´éparés par des points. La partie réseau de l'adresse IP vient toujours en tête et la partie hôte est donc toujours en queue, on a principalement les formes suivantes dite classification des réseaux :

- Classe A : Un octet réseau, trois octets d'hôtes.
- Classe B : Deux octets réseau, deux octets d'hôtes.
- Classe C : Trois octets réseau, un octet d'hôte.
- Classe D
- Classe E

1.8.4 Classification des réseaux

Chaque adresse IP appartient à une classe qui correspond à une plage d'adresses IP. Ces classes d'adresses sont au nombre de 5 c'est-à-dire les classes A, B, C, D et E. Le fait d'avoir des classes d'adresses permet d'adapter l'adressage selon la taille du réseau (le besoin en terme d'adresses IP).

Pour distinguer les classes il faut examiner les bits de poids fort de l'octet de poids fort, si le premier bit est 0, l'adresse est de classe A. On dispose de 7 bits pour identifier le réseau et de 24 bits pour identifier l'hôte. On a donc les réseaux de 1 à 127 et 224 hôtes possibles, c'est-à-dire 16 777 216 machines différentes (de 0 à 16 777 215). La machine 0 n'est pas utilisée, tout comme la machine ayant le plus fort numéro dans le réseau (tous les bits de la partie hôte a 1, ici 16 777 215), ce qui réduit de deux unités le nombre des machines nommables. Il reste donc seulement 16 777 214 machines adressables dans une classe A.

Si les deux premiers bits sont 10, l'adresse est de classe B. Il reste 14 bits pour identifier le réseau et 16 bits pour identifier la machine. Ce qui fait 2(14) = 16 384 réseaux (128.0 à 191.255) et 65 534 (65 536 − 2) machines.

Si les trois premiers bits sont 110, l'adresse est de classe C. Il reste 21 bits pour identifier le réseau et 8 bits pour identifier la machine. Ce qui fait 2(21) = 2 097 152 réseaux (de 192.0.0 a 223.255.255) et 254 (256 − 2) machines.

Si les quatre premiers bits de l'adresse sont 1110, il s'agit d'une classe d'adressage spéciale, la classe D. Cette classe est prévue pour faire du " multicast ", ou multipoint. RFC1112 [6]

Contrairement aux trois premières classes qui sont dédiées à l'unicast ou point à point.

Si les quatre premiers bits de l'adresse sont 1111, il s'agit d'une classe expérimentale la classe E La RFC 1700, les adresses sont réservées pour des futures utilisations. [13]

- La classe A de l'adresse IP 0.0.0.0 à 126.255.255.255 (adresses privées et publiques).
- La classe B de l'adresse IP 128.0.0.0 à 191.255.255.255 (adresses privées et publiques).
- La classe C de l'adresse IP 192.0.0.0 à 223.255.255.255 (adresses privées et publiques).
- La classe **D** de l'adresse IP 224.0.0.0 à 239.255.255.255 (adresses de multicast).
- La classe **E** de l'adresse IP 240.0.0.0 à 255.255.255.255 (adresses réservées)

1.9 Commutation et routage

Les réseaux modernes sont apparus au cours des années 1960 à la faveur d'une technologie totalement nouvelle permettant de transporter de l'information d'une machine à une autre.

Ces machines étaient alors des ordonnateurs de première génération nettement moins puissant qu'un Smartphone actuel. Les réseaux de téléphonie existaient quand a ceux depuis longtemps. Ils utilisaient la technique dite commutation de circuits et le support de lignes physiques reliant l'ensemble des téléphones par le biais des commutateurs. Lors d'une communication ces lignes physiques ne pouvaient être utilisées que par les deux utilisateurs en contact. Le signal qui y transitait était de type analogique.

La première révolution des réseaux a été apportée par la technologie numérique des codecs (codeur-décodeur), qui permettaient de transformer les signaux analogiques en signaux numériques c'est-à-dire suite de 0 et 1.

Le fait de traduire tout type d'information sous forme de 0 et 1 permettait d'unifier les réseaux. Dans cette génération la commutation des circuits était toujours fortement utilisée. Les circuits étant devenus numérique, la question s'est posée de faire passer simultanément sur un même circuit plusieurs flots, correspondant à des applications différentes. C'est ainsi qu'on a pu par exemple avoir 1 octet (8Bits) de téléphonie suivi de deux bits de transfert de fichier puis de 8 bits d'application vidéo. Cette solution ne s'est toutefois quasiment pas développée et a laissé la place au transfert de paquets.

Le transfert de paquets a permis de prendre en compte la forte irrégularité du débit de la commutation entre deux ordinateurs, alternant les périodes de débit important et les périodes de silence, résultant du fait que, par exemple, un ordinateur doit attendre la réponse d'un autre ordinateur.

Dans la commutation de circuit, le circuit reste inutilisé pendant les périodes de silence, induisant un important gaspillage des ressources. A l'inverse, le transfert de paquets n'utilise les ressources du réseau que lors de l'émission effective des paquets. L'idée s'est donc de constituer des blocs d'information de longueur variable et de les envoyer de nœuds de transfert en nœud de transfert jusqu'à atteindre la destination. Les ressources d'une liaison entre deux nœuds ne sont de la même sorte utilisées pendant le transfert des paquets, les différents paquets provenant d'un même utilisateur et d'une même application forment un flot. Une fois les paquets de ce flot parvenus à destination, il est possible d'utiliser la même liaison et les mêmes ressources du réseau pour le passage d'autres paquets provenant d'autres flots.

Parmi de nombreuses solutions de transfert de paquets qui ont été proposées, deux ont résisté au temps, le routage de paquets et la commutation de paquets. Dans le routage de paquets, les paquets sont aiguillés par chaque nœud de transfert en fonction de leur destination. La route choisie peut être différente selon l'état du réseau, de telle sorte que deux paquets d'un même flot peuvent suivre une route différente. Des tables de routage sont implémentées dans ces nœuds afin d'optimiser le transport en fonction de l'état du réseau.

Issue du monde des télécommunications, la commutation de paquets consiste à mettre en place, avant d'envoyer le moindre paquet, un chemin entre les entités en communication, chemin que tous les paquets d'un même flot doivent emprunter. Ce chemin (Path en anglais) a pendant longtemps été appelé circuit virtuel parce que les paquets utilisant d'autres chemins peuvent utiliser les mêmes ressources. Il n y donc pas de ressource réservée.

Chacune de ces techniques présentes des avantages et des inconvénients. Le routage est une technique souple. Dans la mesure où chaque paquet transporte l'adresse du destinataire, la route peut varier sans difficulté, et le paquet ne jamais perdu. En revanche, il est très difficile d'y assurer une qualité de service, c'est-à-dire de garantir que le service de transport sera capable de respecter une performance déterminée. Avec la commutation de paquets la qualité de service est plus facilement assurée. Puisque tous les paquets suivent un même chemin et qu'il est possible de réserver des ressources ou de déterminer par calcul si un flot donné a la possibilité de traverser le réseau sans encombre.

La principale faiblesse de la commutation de paquets réside dans la mise en place du chemin que vont suivre les différents paquets d'un flot. Ce chemin est ouvert par une procédure spécifique, appelée signalisation, on signale au réseau l'ouverture d'un chemin lequel doit en outre être (marqué) afin que les paquets du flot puissent le suivre. Cette signalisation exige d'importantes ressources, ce qui rend les réseaux à commutation de paquets sensiblement plus chers que les réseaux à routage de paquets.

Aujourd'hui, tous les deux sont en concurrence pour le transport des applications multimédias. Leurs avantages et inconvénients auraient plutôt tendance à faire choisir la commutation des paquets par les opérateurs et les grandes entreprises et le routage par les petites et moyennes entreprises.

Les techniques de routage n'ont que peu changé. Le protocole IP (Internet Protocole) en constitue le principal déploiement, le paquet IP contenant l'adresse complète du destinataire est routé dans des nœuds de transfert appelé routeurs.

A l'inverse, les protocoles liés à la commutation ont beaucoup évolué. La première grande norme de commutation, X25, a vu le jour dans les années 80, cette solution exigeait des opérations importantes pour effectuer la commutation. Avec les croissances vertigineuses des nombres de flot, une nouvelle signalisation a été introduite avec le relais de trames avec la technique ATM (Asynchronous Transfer Mode), et aujourd'hui de nouvelles solutions se mettent en place avec les techniques SDN (Software Defined Network). [1]

1.10 Routeur et commutateur

1.10.1 Introduction :

Les commutateurs acheminent les paquets vers le récepteur en utilisant des références, également appelées identificateurs ou étiquette (en anglais labels). Une référence est une suite de chiffres accompagnant un bloc (trame, paquet) pour lui permettre de choisir une porte de sortie au sein d'une table de commutation. Les routeurs utilisent une table de routage pour diriger les paquets vers leur destination.

Ces deux possibilité sont assez différentes puisque dans la commutation le chemin que suivent les paquets de nœud en nœud est toujours le même alors que dans le routage les paquets est routé à l'entrée de chaque nœud grâce à l'adresse complète du récepteur.

Une fois le chemin ouvert, les mesures montrent que pour une puissance donnée, un commutateur atteint un débit d'une dizaine de fois à celui d'un routeur. Cette différence a toutefois tendance à se réduire avec les routeurs gigabit, dits Giga routeurs capable de router de 100 000 paquets IP toutes les secondes. [1]

1.10.2 Les commutateurs

En anglais, les commutateurs sont appelés (Label switches) ou plus fréquemment (Switches) pour bien insister que les commutateurs utilisent des références (labels).

L'un des atouts majeurs des systèmes de commutation réside dans l'architecture des commutateurs, Plusieurs types d'architecture ont été proposés, dont les trois principaux sont dits à mémoire partagée (Shared-memory) a support partagé (Shared-medium) et a division spatiale (Space-division). Etant donné les vitesses des lignes de transmission, les commutateurs doivent pouvoir commuter les paquets à débits extrêmement élevés tout en étant capables de traiter plusieurs milliers de chemins et donc de gérer des tables de commutation à plusieurs milliers d'entrées. De tels commutateurs sont réalisés de façon matérielle plutôt que logicielle.

Les différents commutateurs se distinguent les uns des autres en fonction de critères de fonctionnement internes, tel que l'architecture, le type de liaison, la technique de commutation, le contrôle et la gestion des blocages par les mémoires tampons. [1]

1.10.2.1 L'architecture interne :

Se différencient par le nombre d'étapes à traverser. Une étape peut être considérée comme un bloc monolithique. Traversé en une seule tranche de temps de base. Plus le nombre d'étapes est faible plus le temps de réponse est court.

1.10.2.2 La liaison : La liaison à l'intérieur du commutateur de paquets peut être soit dédiée, soit statique. Sur une liaison dédiée, les paquets vont d'une porte d'entrée à une porte de sortie, en transitant toujours par le même chemin. Dans le cas d'une liaison statique, tout paquet est apte à emprunter une liaison quelconque à l'intérieur du commutateur. Le routeur est alors déterminé par un algorithme de contrôle.

1.10.2.3 Les techniques de commutation : Les techniques de commutation interne peuvent être classées en deux grandes catégories : la répartition dans l'espace et la répartition dans le temps. Dans une répartition dans l'espace, plusieurs liaisons parallèles peuvent être mise en place pour véhiculer les paquets. Dans la répartition dans le temps, les paquets se partagent les ressources dans le temps. Il peut aussi y avoir superposition des deux techniques de commutation, plusieurs liaisons mettant chacune en œuvre un multiplexage temporel.

1.10.2.4 Le contrôle du commutateur : S'effectue à l'aide d'algorithme de gestion des ressources. Ces algorithmes concernent le routage des paquets et les contrôles de flux et de congestion. [1]

1.10.3 Routeur

Les routeurs sont des équipements réseau capables de router les blocs d'informations qui leur arrivent. Ces blocs peuvent être des paquets (pour ce qui concerne le niveau3) ou des trames (pour le niveau 2). Les routeurs les plus connus sont les routeurs IP, puisqu'un paquet IP possède l'adresse complète du destinataire du paquet. On a tendance à faire l'amalgame entre routeur et routeur IP puisque le paquet IP s'est imposé comme le standard unique de niveau 3. L'apparition toute récente des routeurs de niveau 2 vise à améliorer les performances en traitant directement la trame.

Les routeurs IP se différencient des commutateurs par le traitement de l'adresse du destinataire. Dans un routeur, le traitement s'exerce sur l'adresse complète et la consultation de la table routage. Dans un commutateur, le traitement s'effectue sur la référence et utilise la table de commutation (voir la figure 1.9). [1]

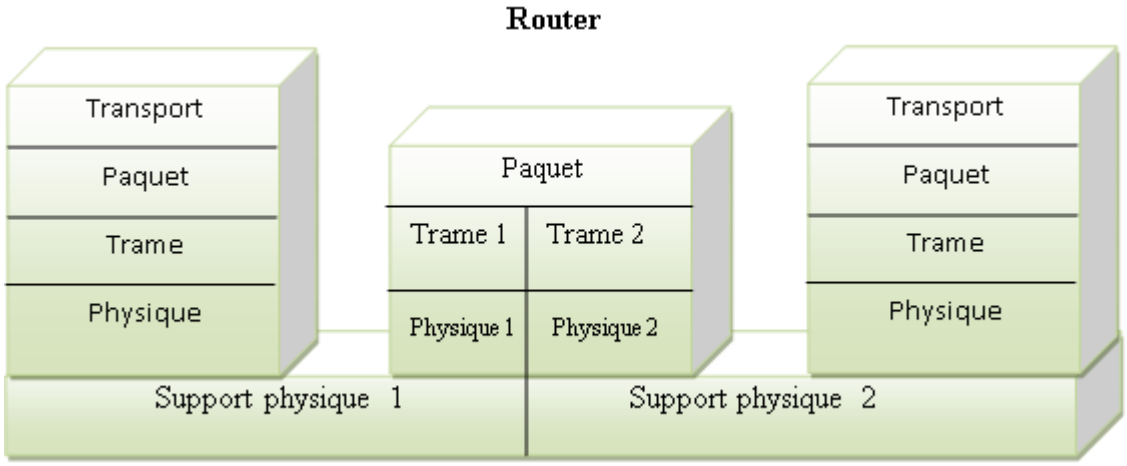


Figure (1.9) : Architecture protocolaire d'un routeur niveau 3 [1]

1.11 Les principaux protocoles utilisés

Les principaux protocoles utilisés par la couche transport et les couches aux dessus sont:

1.11.1 DNS (Domain Name System)

Chaque station possède une adresse IP propre. Cependant il est nettement plus simple de travailler avec des noms de stations ou des adresses plus explicites comme par exemple http://www.cisco.com, qu'avec des adresses IP. Pour répondre à cela, le protocole DNS permet d'associer des noms en langage courant aux adresses numériques. [8]

1.11.2 FTP et TFTP

1.11.2.1 FTP

FTP est un protocole fiable et orienté connexion qui emploie TCP pour transférer des fichiers entre les systèmes qui supportent ce protocole. Le but principal du FTP est de transférer des fichiers à partir d'un ordinateur à un autre en copiant et/ou en déplaçant des fichiers des serveurs aux clients, et des clients vers les serveurs.

Le protocole FTP est assigné au port 21 par défaut. Quand des fichiers sont copiés d'un serveur, FTP établit d'abord une connexion de contrôle entre le client et le serveur. Alors une deuxième connexion est établie, qui est un lien entre les ordinateurs par lequel les données sont transférées.

Le transfert de données peut se faire en mode Ascii ou en mode binaire. Ces modes déterminent le codage utilisé pour le fichier de données, qui dans le modèle OSI est une tâche de couche présentation. Après que le transfert de fichiers ait fini, la connexion de transfert de données se coupe automatiquement. La connexion de contrôle est fermée quand l'utilisateur se déconnecte et clôt la session. [8]

1.11.2.2 TFTP

TFTP est un service non orienté connexion qui emploie UDP. TFTP (Trivial FTP) est employé sur un routeur pour transférer des dossiers de configuration et des images d'IOS de Cisco et aussi pour transférer des fichiers entre les systèmes qui supportent TFTP.

TFTP est conçues pour être léger et simple à utiliser. Néanmoins il peut lire ou écrire des fichiers sur un serveur à distance mais il ne peut pas lister les répertoires et ne supporte pas une authentification utilisateur. Il est utile dans certains LANs parce qu'il fonctionne plus rapidement que le FTP. [8]

1.11.3 HTTP

Le protocole de transfert hypertexte (HTTP) fonctionne avec le World Wide Web, qui est la partie la plus utilisée et la plus importante d'Internet. Une des raisons principales de cette croissance extraordinaire est la facilité avec laquelle il permet l'accès à l'information.

Un navigateur web est une application client/serveur, qui implique l'existence d'un client et d'un serveur, composant spécifique installé sur les 2 machines afin de fonctionner.

Un navigateur web présente des données dans un format multimédia, c'est-à-dire un contenu réagissant aux actions de l'utilisateur. Le contenu peut être du texte, des graphiques, du son, ou de la vidéo.

Les pages web sont écrite en utilisant l'HTML (HyperText Markup Language): un navigateur web reçoit la page au format HTML et l'interprète de manière à afficher la page d'une manière beaucoup plus agréable qu'un document texte.

Pour déterminer l'adresse IP d'un serveur HTTP distant, le navigateur utilise le protocole DNS pour retrouver l'adresse IP à partir de l'URL. Les données qui sont transférées au serveur http contiennent la localisation de la page Web sur le serveur.

Le serveur répond à la requête par l'envoi au navigateur du code HTML ainsi que des différents objets multimédia qui agrémente la page (son, vidéo, image) et qui sont indiqués dans les instructions de la page HTML.

Le navigateur rassemble tous les fichiers pour créer un visuel de la page Web, et termine la session avec le serveur. Si une autre page est demandée, le processus entier recommence. . [8]

1.11.4 SMTP (Simple Mail Transfer Protocol)

Les serveurs d'email communiquent entre eux en employant le SMTP pour envoyer et recevoir du courrier. Le protocole SMTP achemine des messages email dans le format Ascii en utilisant TCP. On l'utilise souvent en tant que protocole d'envoi de mail, rarement en tant que protocole de récupération d'email, car il est peu sécurisé et surtout n'offre aucune authentification. [8]

1.11.5 SNMP (Simple Network Management Protocol)

Le SNMP est un protocole de la couche application qui facilite l'échange d'information de gestion entre les dispositifs d'un réseau. Le SNMP permet à des administrateurs réseau de contrôler l'état du réseau, détecter et résoudre des problèmes de réseau, et de prévoir le développement du réseau, si jamais celui-ci arrive à saturation. Le SNMP emploie le protocole UDP en tant que protocole de couche transport.

Un réseau contrôlé par SNMP comprend les trois composants clés suivants:

- **Système de gestion de réseau (NMS / Network Management System)** : NMS exécute les applications qui supervisent et contrôle les dispositifs gérés. Un ou plusieurs NMS doivent exister sur n'importe quel réseau géré.
- **Dispositifs managés** : Les dispositifs managés sont des nœuds du réseau qui contiennent un agent SNMP et qui résident sur un réseau managé. Les dispositifs managés rassemblent et stockent des informations de gestion et rendent cette information disponible à NMS à l'aide des dispositifs SNMP. Les dispositifs managés, parfois appelés éléments de réseau, peuvent être des routeurs, des serveurs d'accès, des commutateurs, et des ponts, des concentrateurs, des ordinateurs hôtes, ou des imprimeurs.
- **Agents** : Les agents sont des modules de logiciel réseau - gestion qui résident dans des dispositifs managés. Un agent a la connaissance locale d'information de gestion et traduit cette information en un format compatible avec SNMP. [8]

1.11.6 Telnet (Network Virtual Terminal Protocol)

Le protocole Telnet est un protocole standard d'Internet permettant l'interfaçage de terminaux et d'applications à travers Internet. Ce protocole fournit les règles de base pour permettre de relier un client à un interpréteur de commande (côté serveur).

Le protocole Telnet s'appuie sur une connexion TCP pour envoyer des données au format ASCII codées sur 8 bits entre lesquelles s'intercalent des séquences de contrôle Telnet.

Le protocole Telnet repose sur trois concepts fondamentaux :

- Le paradigme du terminal réseau virtuel (NVT).
- Le principe d'options négociées.
- Les règles de négociation.

Ce protocole est un protocole de base, sur lequel s'appuient certains autres protocoles de la suite TCP/IP (FTP, SMTP, POP3, etc.).

Les spécifications de Telnet ne mentionnent pas d'authentification, car Telnet est totalement séparé des applications qui l'utilisent (le protocole FTP définit une séquence d'authentification au-dessus de Telnet).

En outre, le protocole Telnet est un protocole de transfert de données non sûr, c'est-à-dire que les données qu'il véhicule circulent en clair sur le réseau (de manière non chiffrée). Lorsque le protocole Telnet est utilisé pour connecter un hôte distant à la machine sur lequel il est implémenté en tant que serveur, ce protocole est assigné au port 23. RFC 854 [6]

1.12 Conclusion

Nous avons abordé dans ce premier chapitre les différents définitions liées à l'architecture des réseaux touchant en particulier l'aspect sécurisation des réseaux dont nous avons pu situer les éléments essentiels qui entrent en jeu dans la conception, l'organisation et le fonctionnement d'un réseau informatique, dans une approche générale visant à situer les éléments clés constituant les mécanismes de sécurité des réseaux dans la technologie évolue avec le volume et les capacités de traitement qui doivent impérativement rester puissant, fiable pour une meilleur mis en œuvre en service des équipes compétentes qui veillent sur l'acheminement d'une information rigoureuse, fiable et précise.

2.1 Introduction

La sécurité informatique c'est l'ensemble des moyens mis en œuvre pour réduire la vulnérabilité d'un système contre les menaces accidentelles ou intentionnelles. Il convient d'identifier les exigences fondamentales en sécurité informatique. Elles caractérisent ce à quoi s'attendent les utilisateurs de systèmes informatiques en regard de la sécurité.

Ces exigences se résument dans les points essentiels qui suivent : la disponibilité, la confidentialité et l'intégrité.

- **Disponibilité** : Demande que l'information sur le système soit disponible aux personnes autorisées.

- **Confidentialité** : Demande que l'information sur le système ne puisse être lue que par les personnes autorisées.

- **Intégrité :** Demande que l'information sur le système ne puisse être modifiée que par les personnes autorisées.

Ces mécanismes tels que confidentialité ou intégrité des données peuvent être intégrés à tous les niveaux et sur les différents tronçons qui composent le réseau. Et la gestion des clés cryptographiques sera par exemple réalisée manuellement.

De même l'identification, l'authentification, la non répudiation, les autorisations sont des procédures mises en œuvre dans le réseau d'accès (sans fil par exemple), le réseau de transport (IP), le réseau de destination (intranet …). Et peuvent être également offerts au niveau applicatif. [9]

2.2 Les risques et les menaces liés aux systèmes informatiques

Risques et menaces sont deux concepts fondamentaux pour la compréhension des techniques utilisés dans le domaine de la sécurité. Le risque est une fonction de paramètres qu'on peut maîtriser à la différence de la menace qui est liée à des actions ou des opérations émanant de tiers. Dans un réseau, a fortiori dans un grand réseau, la sécurité concerne non seulement les éléments physiques (câble, modems, routeurs, commutateurs…) mais aussi les éléments logiques, voire volatile, que représentent les données qui circulent. Le responsable de la sécurité doit analyser l'importance des risques encours, les menaces potentielles et définir un plan général de protection qu'on appelle politique de sécurité. [10]

2.2.1 Les Risques

Les risques se mesurent en fonction de deux critères principaux : la vulnérabilité et la sensibilité. La vulnérabilité désigne le degré d'exposition à des dangers. Un des points de vulnérabilité d'un réseau est un point facile à approcher. Un élément de ce réseau peut être vulnérable tout en présentant un niveau se sensibilité très faible : le poste de travail de l'administrateur du réseau, par exemple, dans la mesure où celui-ci peut se connecter au système d'administration en tout point du réseau.

La sensibilité désigne le caractère stratégique d'un composant du réseau. Celui-ci peut être sensible, vu son caractère stratégique mais quasi invulnérable, grâce à toutes les mesures de protection qui ont été prise pour le prémunir contre la plupart des risques. Exemple : le câble constituant le média d'un réseau local lorsqu'il passe dans des espaces de services protégés, l'armoire de sauvegarde des logiciels de tous les commutateurs du réseau…On peut classer les risques en deux catégories : structurels, ils sont liés à l'organisation et la démarche d'une entreprise ; accidentels, ils sont indépendants de l'entreprise.

Enfin, selon les niveaux de sensibilité et de vulnérabilité, on distingue souvent quatre niveaux de risques, selon qu'ils sont acceptables, courants, majeurs ou inacceptables.

- **Acceptables** : ils n'induisent aucune conséquence grave pour les entités utilisatrices du réseau. Ils sont facilement rattrapables : pannes électriques de quelques minutes, perte d'une liaison…
- **Courants** : ce sont ceux qui ne portent pas un préjudice grave. Ils se traduisent, par exemple, par une congestion d'une partie du réseau. La mauvaise configuration d'un équipement peut causer la répétition des messages émis, un opérateur peut détruire involontairement un fichier de configuration.

- **Majeurs** : ils sont liés à des facteurs rares. Ils causent des préjudices ou des dégâts importants, mais ils peuvent encore être corrigés. Un incendie a ravagé le centre de calcul d'une entreprise. La conséquence se traduit par le remplacement de l'ensemble du matériel ; mais, heureusement, tous les logiciels et les données avaient été sauvegardés et archivés dans un local anti feu.
- **Inacceptable** : ils sont, en général, fatals pour l'entreprise. Ils peuvent entraîner son dépôt de bilan. [11]

2.2.2 Les Menaces

On peut également classer les menaces en deux catégories selon qu'elles ne changent rien ou qu'elles perturbent effectivement le réseau.

- **Les menaces passives** : consistent essentiellement à copier ou à écouter l'information sur le réseau, elles nuisent à la confidentialité des données. Dans ce cas, celui qui prélève une copie n'altère pas l'information elle-même. Il en résulte des difficultés à détecter ce type de malveillance, car elles ne modifient pas l'état du réseau. La méthode de prélèvement varie suivant le type de réseau. Sur les réseaux câblés, on peut imaginer un branchement en parallèle grâce à des appareils de type analyseurs de protocole. Sur les faisceaux hertziens, des antennes captent les lobes secondaires des faisceaux.
- **Les menaces actives** : nuisent à l'intégrité des données. Elles se traduisent par différents types d'attaques. On distingue le brouillage, le déguisement (modification des données au cours de leur transmission, modification de l'identité de l'émetteur ou du destinataire), l'interposition (création malveillante de messages en émission ou en réception). Les niveaux de piratage sont très variables. La gamme des pirates s'étend de l'amateur sans connaissances particulières du réseau qu'il pénètre ou tente d'infiltrer au professionnel ; souvent membre de l'entreprise et au courant des procédures du réseau. Les mécanismes de sécurité doivent donc prendre en considération aussi bien le sondage aléatoire, pratiqué par l'amateur à la recherche d'un mot de passe, que la lecture, aux conséquences désastreuses, du catalogue central des mots de passe, des codes de connexion ou des fichiers. [12]

2.3 Éléments d'une politique de sécurité

Il ne faut pas perdre de vue que la sécurité est comme une chaîne, guère plus solide que son maillon le plus faible. En plus de la formation et de la sensibilisation permanente des utilisateurs, la politique de sécurité peut être découpée en plusieurs parties :

2.3.1 Défaillance matérielle : Tout équipement physique est sujet à défaillance (usure, vieillissement, défaut…) L'achat d'équipements de qualité et standard accompagnés d'une bonne garantie avec support technique est essentiel pour minimiser les délais de remise en fonction. Seule une forme de sauvegarde peut cependant protéger les données.

2.3.2 Défaillance logicielle : Tout programme informatique contient des bugs. La seule façon de se protéger efficacement contre ceux-ci est de faire des copies de l'information à risque. Une mise à jour régulière des logiciels est indispensable.

2.3.3 Accidents (pannes, incendies, inondations…): Une sauvegarde est indispensable pour protéger efficacement les données contre ces problèmes. Cette procédure de sauvegarde peut combiner plusieurs moyens fonctionnant à des échelles de temps différentes :

Pour des sites particulièrement importants (site informatique central d'une banque…) il sera nécessaire de prévoir la possibilité de basculer totalement et rapidement vers un site de secours. Ce site devra donc contenir une copie de tous les logiciels et matériels spécifiques à l'activité de la société.

2.3.4 Erreur humaine : Outre les copies de sécurité, seule une formation adéquate du personnel peut limiter ce problème.

Vol via des dispositifs physique (disques et bandes) :

- Contrôler l'accès à ces équipements
- Ne mettre des unités de disquette, bandes… que sur les ordinateurs où c'est essentiel.
- Mettre en place des dispositifs de surveillances.

2.3.5 Virus provenant de disquettes : Ce risque peut-être réduit en limitant le nombre de lecteur de disquettes en service. L'installation de programmes antivirus peut s'avérer une protection efficace mais elle est coûteuse, diminue la productivité, et nécessite de fréquentes mises à jour.

2.3.6 Piratage et virus réseau : Cette problématique est plus complexe et l'omniprésence des réseaux, notamment l'Internet, lui confère une importance particulière. Les problèmes de sécurité de cette catégorie sont particulièrement dommageables dans les réseaux et font l'objet de l'étude qui suit. [13]

2.4 La politique de sécurité

2.4.1 Les stratégies de la sécurité informatique

Les coûts d'un problème informatique peuvent être élevés et ceux de la sécurité le sont aussi. Il est nécessaire de réaliser une analyse de risque en prenant soin d'identifier les problèmes potentiels avec les solutions avec les coûts associés.

L'ensemble des solutions retenues doit être organisé sous forme d'une politique de sécurité cohérente, en fonction du niveau de tolérance au risque. On obtient ainsi la liste de ce qui doit être protégé. Il faut cependant prendre conscience que les principaux risques restent : câble arraché, coupure secteur, crash disque, mauvais profil utilisateur, attaque de l'intérieur ou de l'extérieur du réseau.

Voici quelques éléments pouvant servir de base à une étude de risque:

- Quelle est la valeur des équipements, des logiciels et surtout des informations ?
- Quel est le coût et le délai de remplacement ?
- Faire une analyse de vulnérabilité des informations contenues sur les ordinateurs en réseau.
- Quel serait l'impact sur la clientèle d'une information publique concernant des intrusions sur les ordinateurs de la société ?

2.4.2 Établissement d'une politique de sécurité

Suite à l'étude des risques et avant de mettre en place des mécanismes de protection, il faut préparer une politique à l'égard de la sécurité. C'est elle qui fixe les principaux paramètres, notamment les niveaux de tolérance et les coûts acceptables. Voici quelques éléments pouvant aider à définir une politique :

- Quels furent les coûts des incidents informatiques passés ?
- Quel degré de confiance pouvez-vous avoir envers vos utilisateurs internes ?
- Qu'est-ce que les clients et les utilisateurs espèrent de la sécurité ?
- Quel sera l'impact sur la clientèle si la sécurité est insuffisante, ou tellement forte qu'elle devient contraignante ?
- Y a-t-il des informations importantes sur des ordinateurs en réseaux ? Sont-ils accessible de l'externe ?
- Quelle est la configuration du réseau et y a-t-il des services accessibles de l'extérieur ?

- Quelles sont les règles juridiques applicables à votre entreprise concernant la sécurité et la confidentialité des informations (ex: loi « informatique et liberté », archives comptables…) ? [13]

2.5 Services de la sécurité

L'ISO a défini six services de sécurité : authentification, contrôle d'accès, confidentialité et intégrité des données, non-répudiation et protection contre l'analyse du trafic. Différents types de mécanismes (chiffrement, signature numérique, listes de contrôle d'accès, bourrage, notarisation…) servent pour assurer ces services. Ils diffèrent par leur sophistication, leurs coûts, les efforts nécessaires pour leur implantation, leur maintenance et leurs besoins en ressources humaines. [13]

2.5.1 Authentification

Le service d'authentification garantit l'identité des correspondants ou des partenaires qui Communiquent. On distingue deux cas d'authentification simple et un cas d'authentification mutuelle :

2.5.1.1 L'authentification de l'entité distante: Elle garantit que le récepteur est celui souhaité. Son action peut intervenir à l'établissement de la communication ou pendant le transfert des données. Son objectif principal est la lutte contre le déguisement, également appelé usurpation d'identité (Spoofing).

2.5.1.2 L'authentification de l'origine : Elle assure que l'émetteur est celui prétendu. Le service est inopérant contre la duplication d'entité. Comme le précédent, il s'agit d'authentification simple.

2.5.1.3 L'authentification mutuelle : Elle assure que les deux entités émettrice et réceptrice se contrôlent l'une l'autre.

Le service d'authentification est inutilisable dans le cas d'un réseau fonctionnant en mode sans connexion dans les réseaux, comme dans la vie courante, l'authentification nécessite un échange entre les deux partenaires.

Exemple

À la banque, pour prouver votre identité, vous montrez une carte nationale d'identité. Le guichetier effectue un rapide contrôle visuel, entre votre visage et la photo qui est sur la carte. Il y a bien échange entre vous et le guichetier.

Un niveau de sécurité supplémentaire consiste à vous faire signer en présence du guichetier: celui-ci vérifie la signature manuscrite présente sur la carte. Dans les deux cas de cet exemple, le guichetier fait confiance aux autorités qui délivrent la carte d'identité pour avoir vérifié l'authenticité de votre identité. [13]

2.5.2 Contrôle d'accès

Le service de contrôle d'accès empêche l'utilisation non autorisée de ressources accessibles par le réseau. Par utilisation, on entend les modes lecture, écriture, création ou suppression.

Les ressources sont les systèmes d'exploitation, les fichiers, les bases de données, les applications… Pour contrôler les accès aux ressources, il faut d'abord authentifier les utilisateurs afin de s'assurer de leur identité qui est transportée dans les messages d'initialisation et ensuite établir une liste des droits d'accès associés à chacun. L'annuaire LDAP fournit en général les données nécessaires à la mise en œuvre d'un tel mécanisme. [13]

2.5.3 Confidentialité des données

Garantir la confidentialité des données empêche une entité tierce (non autorisée, le plus souvent en état de fraude passive) de récupérer ces données et de les exploiter. Seuls les utilisateurs autorisés doivent être en mesure de prendre connaissance du contenu des données.

Un message ou un échange des messages sa confidentialité garantie dès lors que tout utilisateur non autorisé qui aurait pu le récupérer ne peut pas l'exploiter. Il n'est pas obligatoire de mettre en place des procédures pour empêcher cette « récupération ».

Exemple

Certaines chaînes de télévision payantes sont transmises cryptées de telle sorte que seuls les possesseurs de décodeurs appropriés peuvent regarder leurs émissions favorites. Les autres peuvent toujours rester devant un écran zébré ! [13]

2.5.4 Intégrité des données

Garantir l'intégrité des données assure au récepteur que les données reçues sont celles qui ont été émises. Les données ont pu être altérées, de manière accidentelle ou de manière délibérée à la suite d'une fraude active. On distingue différents niveaux de service selon les mécanismes mis en œuvre.

Par ailleurs, l'intégrité possède une portée plus ou moins grande (le message complet ou un champ spécifique du message seulement). Lorsque la communication a lieu en mode non connecté, seule la détection des modifications peut être mise en œuvre

Les principes de la protection contre les erreurs est d'ajouter un bloc de contrôle d'erreur qui est le résultat d'un algorithme connu appliqué au message. Le récepteur refait le calcul sur le message qu'il a reçu et compare les deux blocs de contrôle d'erreurs. Il vérifie ainsi l'intégrité du message, cette seule méthode est insuffisante pour détecter des messages insérés dans un flux de données. Les protections mises en œuvre s'inspirent du même principe. [13]

2.5.5 Non-répudiation

La non-répudiation de l'origine fournit au récepteur une preuve empêchant l'émetteur de contester l'envoi d'un message ou le contenu d'un message effectivement reçu. La non-répudiation de la remise fournit à l'émetteur une preuve empêchant le récepteur de contester la réception d'un message ou le contenu d'un message effectivement émis.

Exemple

Vous postez un courrier en recommandé avec accusé de réception. La Poste ajoute à votre courrier un document qui sera signé par le récepteur et qui sera ensuite renvoyé à l'expéditeur. Pour vous, la possession de cet accusé de réception interdit au récepteur de prétendre qu'il n'a rien reçu. La Poste joue un rôle d'intermédiaire entre vous et votre correspondant, elle rend le service de non-répudiation du courrier dans cette opération, elle ne vérifie pas votre identité et encore moins le contenu de votre lettre ! Votre correspondant peut soutenir avoir reçu une enveloppe vide. [13]

2.5.6 Protection contre l'analyse de trafic

Le secret du flux lui-même empêche l'observation du flux de transmission de données, source de renseignements pour les pirates. Ce cas s'applique aux situations où on a besoin de garder la confidentialité sur l'existence même de la relation entre les correspondants.

2.6 Mécanisme de sécurité

Les exemples précédents viennent de la vie courante (banque, poste…). Dans la transmission de messages sur un réseau, il y a une énorme différence : un message électronique peut être dupliqué sans que rien ne permette la distinction entre l'original et celui qui est dupliqué puisque ce sont toujours des suites de données binaires. Il faut donc adapter les solutions de sécurité au monde électronique.

On a imaginé plusieurs mécanismes pour mettre en œuvre et offrir les services de sécurité énumérés précédemment. Il s'agit principalement du chiffrement (qui intervient dans presque tous les mécanismes), de la signature numérique, des techniques d'utilisation d'identificateur et de mots de passe, de bourrage et de notarisation. [13]

2.6.1 Chiffrement

Le chiffrement transforme tout ou partie d'un texte dit clair en cryptogramme, message chiffré ou protégé. Si une communication utilise des dispositifs de chiffrement, les données sont transmises sous une forme « brouillée », de manière qu'elles ne puissent être comprises par un tiers (Figure 2.1).

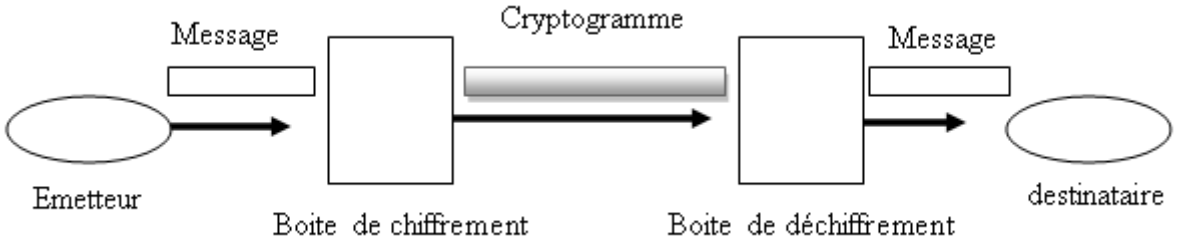


Figure (2.1) : Cycle de Chiffrement [13]

2.6.2 Signature numérique

La signature numérique consiste à utiliser un chiffrement particulier appelé chiffrement irréversible. Celui-ci transforme un message (a priori long) en un bloc de données (de petite taille) tel qu'il est impossible de reconstruire le message à partir du bloc. Les algorithmes utilisés sont appelés fonction de hachage ou fonction de condensation. Le bloc est appelé condensé ou signature. Une bonne fonction de hachage doit produire des condensés différents pour des messages différents : si deux messages différents avaient le même condensé, il serait possible pour un utilisateur malveillant de substituer un message à l'autre, tout en conservant le condensé correct. Cela rend la modification du message indétectable.

On obtient une signature numérique en appliquant (avec une clé) la fonction de hachage au message transmis. Celui-ci devient signé. On envoie le message et sa signature. Le propre de la signature est qu'elle est vérifiable par ceux qui possèdent la clé, mais inimitable.

Les algorithmes les plus connus du type irréversible sont MD5 (Message Digest5) et SHA1 (Secure Hash Algorithm1). Nous verrons leurs principes plus loin.

On garantit l'intégrité d'une unité de données ou d'un champ spécifique d'une unité de données par les codes de contrôle cryptographique, dont le mécanisme est identique à celui des signatures numériques.

L'intégrité d'un flot de données peut être assurée par le même mécanisme de cryptographie auquel s'ajoutent des codes de détection d'erreurs ainsi que la numérotation des unités de données par horodatage. [13]

2.6.3 Mots de passe

Lorsque les entités homologues et les moyens de communication sont sûrs, l'identification des entités homologues peut se faire par un identificateur d'utilisateur (login) et un mot de passe. La sécurité ne peut pas se fonder sur l'identificateur seul. Celui-ci est habituellement de notoriété publique, tel le numéro d'identification de l'employé. De plus, on ne peut pas le changer facilement du fait que beaucoup d'informations s'y rattachent.

Dans certaines applications, l'utilisateur ne connaît même pas son mot de passe qui est inscrit dans une carte magnétique contenant un NIP (numéro d'identification personnel).

Dans d'autres applications, seul l'utilisateur connaît son numéro, et une fonction lui permet de changer son mot de passe. Le cas des guichets bancaires est particulier : le client doit introduire une carte contenant son code, plus une clé secrète.

Le responsable de la sécurité doit porter une attention particulière au protocole qui transporte le mot de passe et au fichier système qui stocke les mots de passe des utilisateurs: inutile de mettre en place un système d'identification avec identificateur et mot de passe si ceux-ci circulent en clair dans le réseau. Lorsque les moyens de communication ne sont pas sûrs, les mots de passe ne suffisent plus à réaliser le mécanisme ; il faut alors y adjoindre des procédures de chiffrement. [13]

2.6.4 Liste de contrôle d'accès

Le mécanisme des listes de contrôle d'accès (ACL, Access Control List) utilise l'identité authentifiée des entités et des informations fiables pour déterminer leurs droits d'accès au réseau ou aux ressources sur le réseau. De plus, il est susceptible d'enregistrer sous forme de trace d'audit et de répertorier les tentatives d'accès non autorisées. Tout utilisateur qui se trompe dans son mot de passe laisse une trace. Il est ainsi possible de détecter les programmes automatiques qui cherchent à pénétrer le système en essayant tous les mots de passe. Les informations utilisées sont : les listes de droits d'accès, maintenues par des centres, les mots de passe, les jetons de droits d'accès, les différents certificats, les libellés de sensibilité des données.

Le mécanisme de contrôle d'accès peut avoir lieu aux deux extrémités de la communication équipement d'accès et ressource du réseau. Dont la deuxième sera détaillée dans ce chapitre. [13]

2.6.5 Bourrage et contrôle de routage par gestion dynamique de la bande passante

Le bourrage simule des communications dans le but de masquer les périodes de silence et de banaliser les périodes de communication réelles. Cela évite d'attirer l'attention des pirates lors des démarrages de transmission.

On obtient un mécanisme de bourrage en envoyant, entre deux émissions de messages utiles, des séquences de messages contenant des données dépourvues de sens. De plus, pour mieux créer l'illusion des vrais messages, le générateur de messages respecte la fréquence des lettres et des digrammes2 de l'alphabet employé.

Enfin, après détection d'une attaque sur une route donnée, ou tout simplement pour prévenir cette attaque, les systèmes d'extrémités ou les réseaux peuvent, par le mécanisme de gestion dynamique de la bande passante, sélectionner une route plus sûre. Dans certains cas, la modification périodique est programmée afin de déjouer toutes les tentatives malveillantes.[13]

2.7 Le protocole Ethernet

Ethernet est un protocole de réseau informatique à commutation de paquets implémentant la couche physique et la sous-couche Medium Access Control du modèle OSI mais ce protocole est classé dans la couche de liaison, car les formats de trames que le standard supporte est normalisé et peut être encapsulé aussi dans d'autres protocoles que les couches physiques MAC et physique de l'Ethernet, ces couches physiques faisant l'objet de normes séparées en fonction des débits, du support de transmission, longueur et conditions environnementales.

L'Ethernet est basé sur le principe de membres (pairs) sur le réseau, envoyant des messages dans ce qui était essentiellement un système radio, captif à l'intérieur d'un fil ou d'un canal commun, parfois appelé *l'éther*. Chaque pair est identifiée par une clé globalement unique, appelée adresse MAC, pour s'assurer que tous les postes sur un réseau Ethernet aient des adresses distinctes.

Une technologie connue sous le nom de détection de porteuse avec accès multiples et détection de collision (Carrier Sense Multiple Access with Collision Detection) ou CSMA/CD régit la façon dont les postes accèdent au média.

Au départ développé durant les années 1960 en utilisant la radio, la technologie est relativement simple comparée à Token-Ring ou aux réseaux contrôlés par un maître.

En pratique, ceci fonctionne comme une discussion ordinaire, où les gens utilisent tous un médium commun (l'air) pour parler à quelqu'un d'autre. Avant de parler, chaque personne attend poliment que plus personne ne parle. Si deux personnes commencent à parler en même temps, les deux s'arrêtent et attendent un court temps aléatoire. Il y a de bonnes chances que les deux personnes attendent un délai différent, évitant donc une autre collision. Des temps d'attente exponentiels sont utilisés lorsque plusieurs collisions surviennent à la suite.

Comme dans le cas d'un réseau non commuté, toutes les communications sont émises sur un médium partagé, toute information envoyée par un poste est reçue par tous les autres, même si cette information était destinée à une seule personne. Les ordinateurs connectés sur l'Ethernet doivent donc filtrer ce qui leur est destiné ou non. Ce type de communication " quelqu'un parle, tous les autres entendent " d'Ethernet est une de ses faiblesses, car, pendant que l'un des nœuds émet, toutes les machines du réseau reçoivent et doivent, de leur côté, observer le silence. Ce qui fait qu'une communication à fort débit entre seulement deux postes peut saturer tout un réseau local.

De même, comme les chances de collision sont proportionnelles au nombre de transmetteurs et aux données envoyées, le réseau devient extrêmement congestionné au-delà de 50 % de sa capacité (indépendamment du nombre de sources de trafic). Pour résoudre ce problème, les commutateurs ont été développés afin de maximiser la bande passante disponible.

Suivant le débit utilisé, il faut tenir compte du domaine de collusion régi par les lois de la physique et notamment le déplacement électronique dans un câble de cuivre. Si l'on ne respecte pas ces distances maximales entre machines, le protocole CSMA/CD n'a pas lieu d'exister. [14]

2.7.1 Les différentes normes utilisées par le protocole Ethernet:

- Ethernet à 10 Mbits/s : 10BASET, 10BASE5, 10BASE2 et 10BASEF(802.3).
- FastEthernet à 100 Mbits/s : 100BASET (802.3u).
- Gigabit Ethernet (GigE) à 1 Gbits/s : 1000BASELX, 1000BASESX, 1000BASECX, 1000BASELH (802.3z) et 1000BASET (802.3ab).
- Déca gigabit Ethernet à 10 Gbits/s : (10 Gigabit Ethernet). [14]

2.8 Les réseaux virtuels

Un ensemble d'outils important pour le control et la gestion de réseau provient des VLAN (Virtual Local Area Network) et des VPN (Virtual Private Network), Les VLAN ont pour objectif de rassembler des machines dispersées dans un réseau.

Les VPN ont objectif assez différent, qui permettre à un opérateur de commercialiser des réseaux privés virtuels de telle sorte que le client pense qu'il dispose d'un réseau dédié. En ait, le réseau du client utilise des ressources du réseau de l'operateur. L'avantage de 'opérateur est de multiplexer les ressources de son réseau entre tous ses clients. L'avantage du client est d'avoir un réseau personnel dont le cout est beaucoup plus abordable que s'il essayait de construire son propre réseau avec une infrastructure privée. [1]

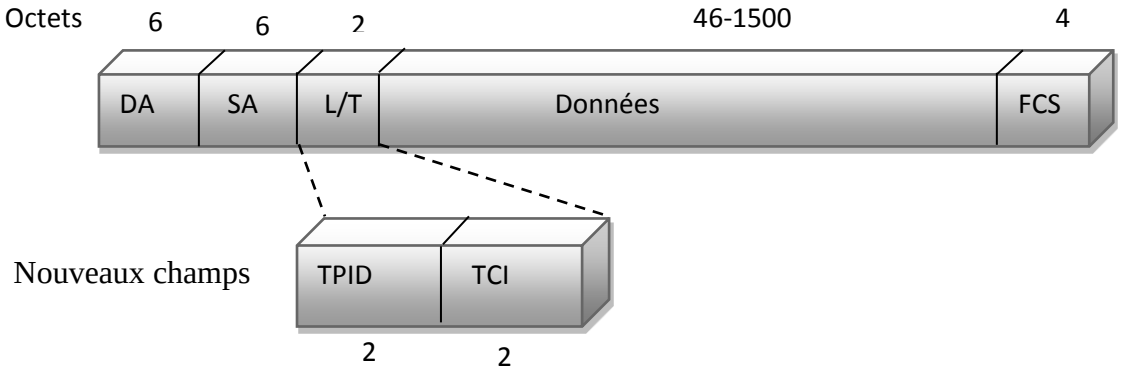
2.8.1 Virtual Local Area Network (VLAN)

On peut assimiler un VLAN à un VPN qui utiliserait comme réseau d'interconnexion le réseau local de l'entreprise au lieu du réseau d'un opérateur. La définition d'un VLAN peut prendre diverses formes, en fonction des éléments suivants: numéro de port, protocole utilisé, adresse MAC utilisé, adresse IP, adresse IP multicast, application utilisée.

Un VLAN peut aussi être déterminé par une combinaison des critères précédents ainsi que par d'autres critères de gestion, comme l'utilisation d'un logiciel ou d'un matériel commun.

Les VLAN offrent une solution pour regrouper les stations et les serveurs en ensembles indépendant, de sorte à assurer une bonne sécurité des communications. Ils peuvent être de différentes tailles, mais il est préférable de recourir à de petits VLAN, de quelques dizaines de stations tout au plus. Il faut en outre éviter de regrouper des stations qui ne sont pas situées dans la même zone de diffusion, Si c'est le cas, il faut gérer les tables de routage dans les routeurs d'interconnexion. [1]

Les champs d'extension permettant de réaliser cette diffusion vers l'ensemble des point d'accès du VLAN sont situés dans la structure de trame illustrée à la figure (2.2)



DA (Destination Address) : adresse de destination

SA (Source Adresse) : adresse source

L/T (Length/ Type) : longueur/type

FCS (Frame Check Sequence)

TPID (Tag Protocol identifier)

TCI (Tag Control Information)

Figure (2.2) : Structure et champs d'extension de la trame Ethernet pour les VLAN [1]

2.8.2 Le champ Tag Control Information TCI : Ce champ comprend (Figure 2.3) :

Un champ de niveaux priorités sur trois éléments binaires, qui permet de déterminer jusqu'à huit niveaux de priorité.

Un bit CFI (Canonical Format Indicator) qui indique que les données de la trame sont sous un format non canonique, c'est-à-dire non déterminé par des règles classiques.

Un champ VLAN ID, qui identifie l'appartenance au VLAN de la trame et permet son routage vers les différents points du VLAN.

Les trois bits de priorité jouent un rôle de plus en plus important dans les VLAN avec qualité de service. Ils permettent de mettre en place une correspondance entre la gestion de la qualité de service DiffServ et le niveau trame du réseau Ethernet. Par exemple, un VLAN de téléphonie IP permet de réserver la plus haut priorité utilisateur, celle correspondant à la classe Expedited Forwarding (EF), de DiffServ, aux applications de téléphonie.

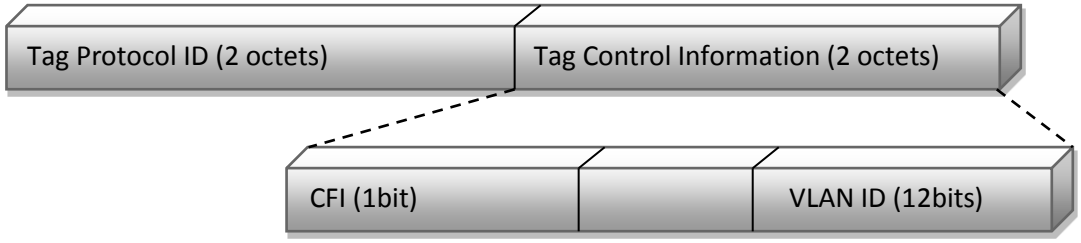


Figure (2.3) : Structure du champ TCI [1]

La valeur du champ TPID (Tag Protocol Identifier) n'a été définie que pour le cas Ethernet, sa valeur est 0x8100

- **User Priority** : priorité de l'utilisateur
- **CFI** (Canonical Format Indicator) : Identificateur du format canonique
- **VLAN ID :** Identificateur du VLAN [1]

2.8.3 Fonctionnement des VLAN

Une règle assez utilisée est de permettre à une trame de n'être associée qu'à un seul VLAN. Outre cette règle assez générale, il est possible de refuser par programmation que la trame d'une machine appartenant à un VLAN puisse s'adresse à une machine qui n'est pas dans le VLAN. Cela permet de créer des groupes fermés et d'assurer ainsi une forte sécurité.

2.8.4 Le mode Trunk

2.8.4.1 Définition

Le Trunk est le mécanisme qui permet d'insérer l'identifiant du VLAN sur une trame utilisateur. Toute trame se propageant sur plusieurs switchs conservera toujours l'information de son appartenance à son VLAN. Et le switch de destination saura avec quels ports la trame peut être commutée (ports appartenant au même VLAN).Cette configuration de lien Trunk s'effectue sur les liens entre switchs, souvent appelé Suplink. [15]

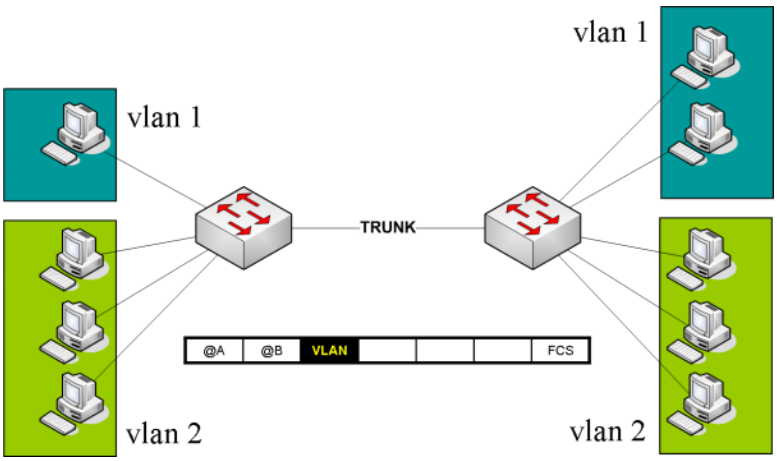


Figure (2.4) : Le mécanisme du Trunk [15]

Dans le schéma ci-dessous (Figure 2.4), on configure le lien inter-switch en Trunk. Toutes les trames qui sortiront sur ce lien (switch de droite ou de gauche), se verront appliquer une étiquette supplémentaire qui contient l'identifiant du VLAN (en noir sur la trame).

Historiquement, Cisco avait créé son propre protocole de Trunk entre ses Switchs, nommé ISL (Inter-Switch Link). Mais très rapidement, cette fonctionnalité plus qu'essentielle, demanda une interopérabilité avec d'autres constructeurs. La norme Trunk 802.1Q fut sortie et Cisco l'implémenta aussi dans ses switchs. D'où la possibilité sur certains Switchs Cisco de décider quel Trunk on souhaite faire, ISL ou 802.1Q. [15]

2.8.4.2 Le mode Trunk ISL

Le Trunk propriétaire Cisco ISL a la particularité d'encapsuler toute la trame de l'utilisateur dans une nouvelle trame, nommée trame ISL. Voici à quoi ressemble une trame ISL (Figure 2.5):

Entête ISL	Trame Ethernet Utilisateur	FCS
26 octets	0-1500 octets	4 octets

Figure (2.5) : La trame ISL [15]

Remarque: comme cette trame a un format particulier, il est obligatoire que le switch d'en face puisse comprendre ce format. Il faut donc configurer le port du Switch d'en face en Trunk ISL.

Pour information, la colonne native VLAN permet de mettre dans le VLAN 1 une trame qui arriverait non encapsulée ISL sur ce port (on en reparle un peu plus loin).

2.8.4.3 Le mode Trunk 802.1Q

Le trunk normalisé 802.1Q n'encapsule pas toute la trame de l'utilisateur comme ISL mais casse la trame et y insère une étiquette ou tag, nommée TAG 802.1Q. Voici à quoi ressemble une trame utilisateur avec le rajout du TAG 802.1Q (Figure 2.6):

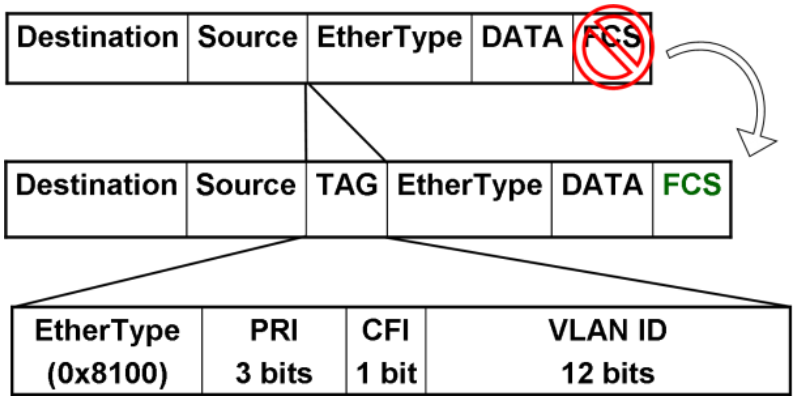


Figure (2.6) : Le mode Trunk 802.1Q [15]

La première trame est celle de l'utilisateur qui arrive sur le switch. Dès que cette trame sort vers un port configuré en Trunk 802.1Q, le switch insère l'étiquette TAG (trame n°2 dans le schéma).

En inspectant le contenu de ce TAG, on remarque les champs suivants (trame n°3 dans le schéma):

- **Ethertype**: permet de préciser que c'est une trame 802.1Q, la valeur en hexa est 0x8100
- **PRI:** champs de priorité sur 3 bits qui permet de classifier le trafic utilisateur pour lui appliquer de la qualité de service (voix, vidéo…). Ce champ est aussi appelé 802.1P ou COS – Class Of Service.
- **CFI** : Canonical Format Identifier: permet la compatibilité d'un réseau Ethernet avec un réseau TokenRing. Champ à oublier car il n'existe quasiment plus du réseau TokenRing aujourd'hui.

• **VLAN ID** : VLAN Identifier: codé sur 12bits: valeur numérique du VLAN auquel la trame utilisateur appartient. C'est le champ le plus important à connaitre.

Le tableau suivant représente une comparaison entre le Trunk ISL Cisco et le Trunk 802.1Q:

ISL Inter Switch Link	**802.1Q**
Propriétaire	Normalisé
Encapsulation	Tag
Indépendant du niveau 2	Dépend du protocole Ethernet
Encapsule l'ancienne trame dans une nouvelle	Ajoute un champ dans l'entête de la trame initiale

Tableau (2.1) : Comparaison entre le Trunk ISL Cisco et le Trunk 802.1Q [15]

2.8.4.4 Le VLAN natif

La particularité du Trunk 802.1Q vient du fait que pour un VLAN en particulier, le Trunk ne casse pas la trame de l'utilisateur et donc ne lui rajoute pas le TAG. Le Trunk laisse la trame transiter sans aucun changement (voir figure 2.7).

Il faut revenir sur l'historique des réseaux: On pouvait se trouver dans le cas où des PC connectés à un HUB étaient lui-même connecté à 2 Switchs. On se trouvait alors dans le schéma suivant:

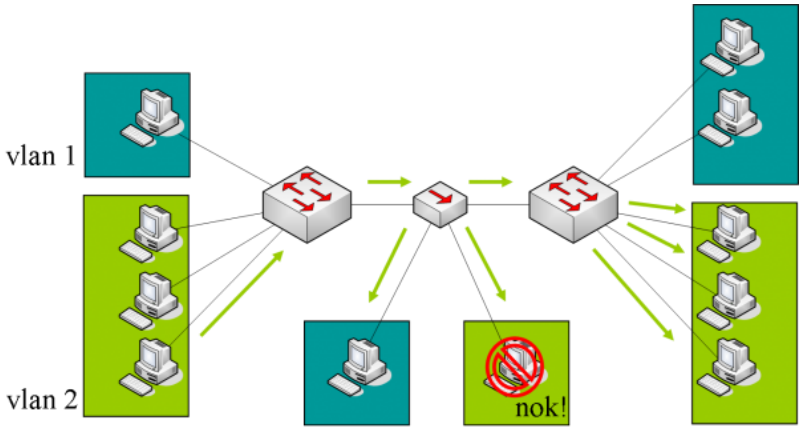


Figure (2.7) : Schéma sans VLAN natif [15]

Prenons le cas où les PC dans le VLAN 2 souhaitent communiquer:

- Un PC de gauche envoi du trafic.
- Le switch de gauche ajoute le TAG VLAN=2 dans la trame et envoi la trame au HUB.
- le HUB diffuse la trame taguée sur tous ses ports.
- le switch de droite reçoit la trame taguée, enlève le TAG et commute la trame vers les ports appartenant au même VLAN (2 ici).
- le PC du bas reçoit une trame taguée! Comme le PC ne sait pas lire le TAG, il rejette la trame.

On voit ici que le PC du bas ne pourra jamais recevoir de trame provenant d'autres PC qui appartiennent au même VLAN que lui.

Donc dans la norme 802.1Q, il a été défini que pour un VLAN en particulier, appelé VLAN natif, les switchs laisseraient passer la trame initiale sans ajouter de TAG. [13]

Regardons maintenant le même comportement avec un PC appartenant au VLAN n°1, configuré comme VLAN natif (Figure 2.8):

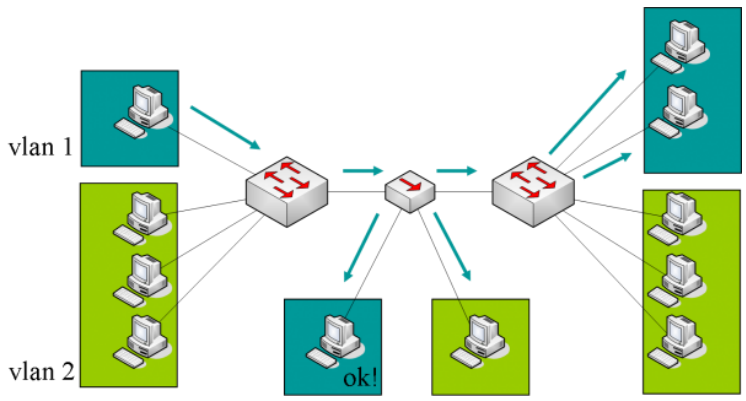


Figure (2.8) : Schéma avec VLAN natif [15]

Reprenons le cas où les PC souhaitent communiquer mais cette fois ci ils appartiennent au VLAN natif 1:

- Un PC de gauche envoi du trafic.
- Le Switch de gauche n'ajoute pas le TAG VLAN=1 dans la trame et envoi la trame au HUB.

- Le HUB diffuse la trame non taguée sur tous ses ports.
- Le Switch de droite reçoit la trame non taguée, donc sait qu'elle appartient au VLAN natif (1 ici) et commute la trame vers les ports appartenant au même VLAN.
- Le PC du bas reçoit une trame non taguée donc la traite comme toute trame classique.

On voit ici que le PC du bas peut communiquer sans aucun souci avec d'autres PC qui appartiennent au même VLAN que lui. [15]

2.9 Les listes de contrôle d'accès (ACL)

Les listes de contrôle d'accès, ou ACL (Access Control List), pour IP permettent à un routeur de supprimer certains paquets en fonction de critères définis à l'avance. Le but de ces listes, appelées filtres, est de protéger le réseau contre tout trafic indésirable. Elles peuvent servir à différents usages:

• Filtrer le trafic réseau en fonction des adresses et des protocoles de couches supérieures (autoriser le trafic de messagerie, bloquer le trafic Telnet …).

• Contrôler le flux du trafic en empêchant les informations de mises à jour de routage d'un réseau particulier de se propager n' importe où.

• Fournir un niveau de sécurité d'accès réseau de base.

Une liste d'accès implique un traitement en deux étapes : recherche de correspondance et action.

La première consiste à examiner chaque paquet afin de déterminer s'il correspond à l'une des instructions access-list de la liste. Si une correspondance est trouvée, deux actions sont possibles : autoriser le paquet (permit) ou l'interdire (deny). Les critères de comparaison spécifiés dans les ACL peuvent se fonder sur des champs d'entêtes IP, TCP et UDP.

Il existe deux catégories principales de listes de contrôle d'accès pour IP : standard et étendus. Les ACL étendus peuvent examiner les adresses IP sources et destination ainsi que les numéros de ports sources et destinataires, et plusieurs autres champs. Les ACL standard ne peuvent examiner que l'adresse IP source (voir la figure 2.9). [16]

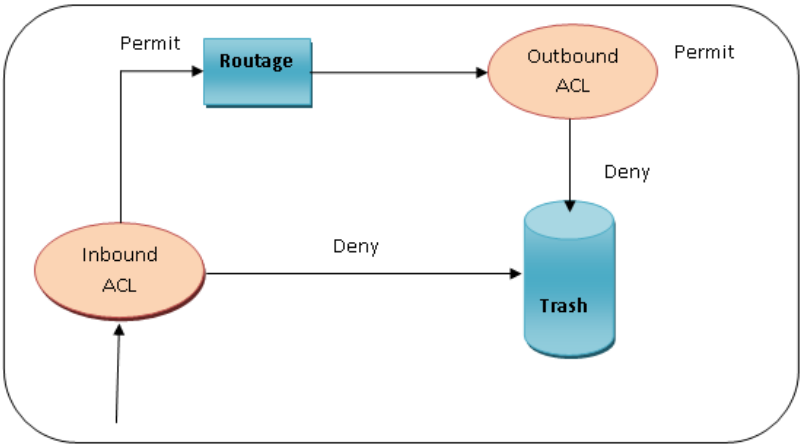


Figure (2.9) : Algorithme de l'ACL [16]

2.9.1 Les différents types des listes de contrôle d'accès

2.9.1.1 Listes de contrôle d'accès standard

Les listes de contrôle d'accès standard sont le plus ancien type de liste de contrôle d'accès. Elles remontent à l'époque du logiciel Cisco IOS version 8.3. Les listes de contrôle d'accès standard contrôlent le trafic en comparant l'adresse source des paquets IP aux adresses configurées dans la liste de contrôle d'accès.

2.9.1.2 Listes de contrôle d'accès étendu

Les Listes de contrôle d'accès étendu ont été introduites dans le logiciel Cisco IOS version 8.3. Les listes de contrôle d'accès standard contrôlent le trafic en comparant les adresses source et de destination da paquets IP aux adresses configurées dans la liste de contrôle d'accès.

2.9.1.3 L'identification d'une liste d'accès

Une liste d'accès est identifiable par son numéro, attribué suivant le protocole et le type. A la création d'une ACL un numéro unique est assigné par l'administrateur qui va permettre au routeur d'identifier la liste d'accès. L'affectation des numéros de listes d'accès gouvernée par des règles. [17]

Chaque type de liste d'accès à un bloc de numéros réservé indirectement, le numéro détermine le type de liste d'accès. Le tableau suivant illustre les différents types des ACLs et les blocs de numéros associés :

Type de liste d'accès	Blocs de numéros
IP standard	1-99
IP étendue	100-199
Protocole type-code	200-299
48 bit MAC adresse	700-799
IPX standard	800-899
IPX étendue	900-999

Tableau (2.2) : Les différentes listes d'accès [17]

2.9.1.4 Vérification des paquets

Lorsque le routeur détermine s'il doit acheminer ou bloquer un paquet, la plate-forme logicielle Cisco IOS examine le paquet en fonction de chaque instruction de condition dans l'ordre dans lequel les instructions ont été créées. Si le paquet arrivant du routeur satisfait à une condition, il est autorisé ou refusé (suivant l'instruction) et les autres instructions ne sont pas vérifiés. Si un paquet ne correspond à aucune instruction dans l'ACL, le paquet est rejeté.[12]

2.9.1.5 Assignation des ACLs aux interfaces

Les listes de contrôle d'accès sont affectées à une ou plusieurs interfaces et peuvent filtrer du trafic entrant ou sortant, selon la configuration. Nous verrons plus loin où placer les ACLs de façon optimale selon le type d'ACL créée. [12]

2.10 Conclusion

Au cours de ce chapitre, nous avons vu les différents aspects liés à la sécurité dans les réseaux, en utilisant les ACL autant qu'outil fiable et robuste de sécurisation, ce qui donne à l'administrateur la faveur et le pouvoir de filtrer les autorisations d'accès des utilisateurs. Celui-ci consistera le noyau du chapitre suivant.

3.1 Introduction

De nos jours, toutes établissements ou entreprises possèdent un réseau local, qui est connecté aux réseaux extérieurs (internet). Cette ouverture vers l'extérieur est indispensable, et dangereuse aux même temps, et pour parer à ces attaques il faut implémenter une architecture bien sécurisé contre les attaques de l'extérieur, de même de l'intérieur.

Dans notre travail nous allons essayer de satisfaire les besoins de la faculté de technologie comme exemple et adapter un réseau selon leur objectif. Donc nous voulons améliorer la performance de réseaux et établir une sécurité demandée pour protéger quelques VLANs et les machines spécifiques.

3.2 Objectif du travail

On peut résumer notre objectif du travail dans les points suivants :

1. Maîtriser la configuration de réseau en générale (interfaces, routage, accès…).
2. Comprendre l'entité d'un VLAN.
3. Comprendre comment créer un VLAN.
4. Pouvoir faire communiquer plusieurs réseaux VLAN par l'utilisation de mode tronc (Trunk).
5. Montrer les avantages de VLAN.
6. Comprendre de l'entité ACL.
7. Connaitre comment configurer (créer et affecter) une liste de contrôle d'accès ACL demandée.
8. Comment utiliser et tester les ACL.
9. Exprimer les avantages des ACL

3.3 Problème posé

Avant de commencer la configuration du réseau il faut prendre en considération les contraintes posées par les points suivants :

a. Connexion lourd : C'est à cause de l'augmentation rapide du nombre d'utilisateurs et l'échanges volumineux de fichiers entre les utilisateurs, en gardant la possibilité des extensions au futur.

b. Déférents trafic circulant : Comme la messagerie, le web, la vidéo…

c. Collision entre les réseaux.

d. Les messages de diffusion Broadcast.

3.4 Solution proposé : pour résoudre les contraintes citées ci-dessus on applique les solutions suivantes :

- Segmentation de réseau par la création des VLANs, pour séparer le trafic et réduire les messages de diffusion pour optimiser le routage.
- Sécuriser des accès jugés important soit entrant ou sortant par des ACLs fonctionnant au niveau réseau (IP ACL) et au niveau ports.

3.5 Logiciel simulateur

Dans ce chapitre on essaye de configurer notre modèle type en utilisant le simulateur (Cisco Packet Tracer) qui est le programme le plus utilisé dans le domaine de simulation des réseaux locaux.

3.5.1 Présentation

Packet Tracer est un logiciel de CISCO (permettant de construire un réseau physique virtuel et de simuler le comportement des protocoles réseaux sur ce réseau. L'utilisateur construit son réseau à l'aide d'équipements tels que les routeurs, les commutateurs ou des ordinateurs. Ces équipements doivent ensuite être reliés via des connexions (câbles divers, fibre optique, …). Une fois l'ensemble des équipements reliés, il est possible pour chacun d'entre eux, de configurer les adresses IP, les services disponibles, etc . . .

Le Cisco Packet Tracer est un simulateur puissant qui permet aux étudiants d'expérimenter le comportement du réseau. En effet, Packet Tracer fournit la simulation, la visualisation, la création, l'évaluation et les capacités de collaboration et facilite l'enseignement et l'apprentissage des technologies complexes (Figure 3.1).

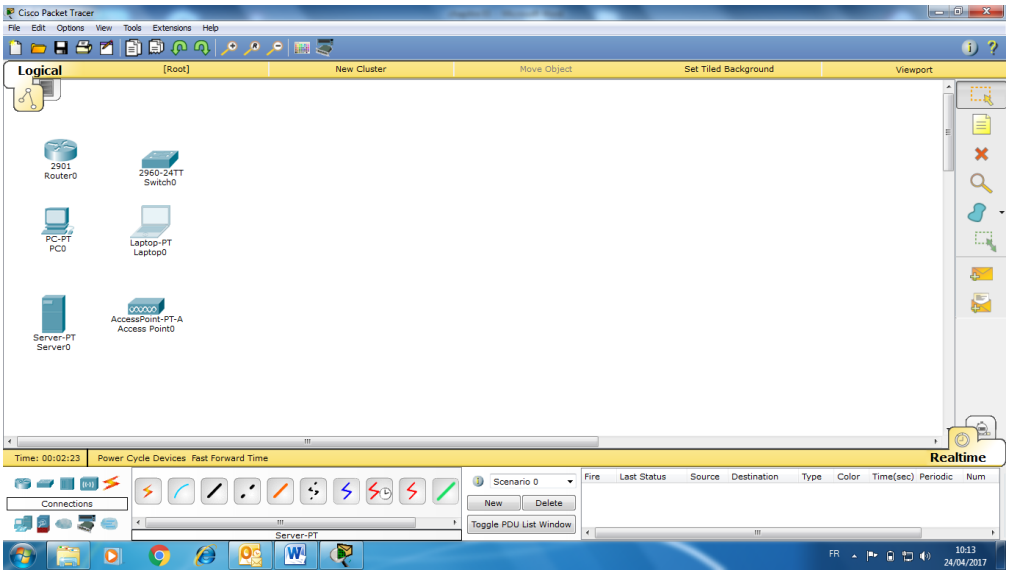


Figure (3.1) : Cisco Packet Tracer

3.5.2 Méthode de configuration des équipements

Pour configurer les équipements dans notre projet on utilise l'interface ou le CLI (Command line Interface) (Figure 3.2).

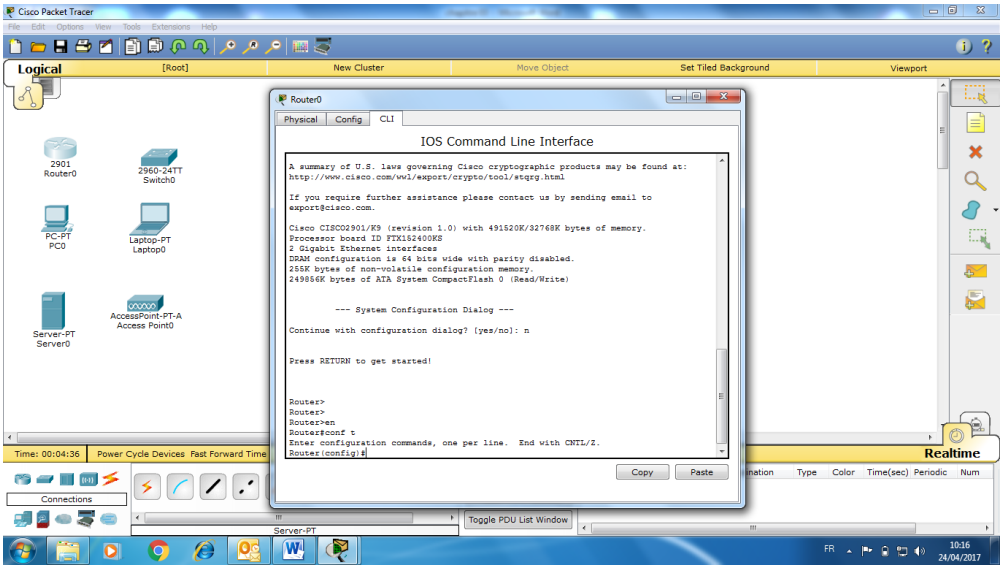


Figure (3.2) : Interface CLI

3.6 Réalisation du projet

3.6.1 Choix d'équipement : Ci-dessous la liste des équipements a utilisé dans notre réseau.

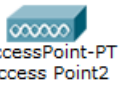
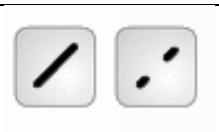
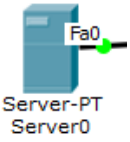
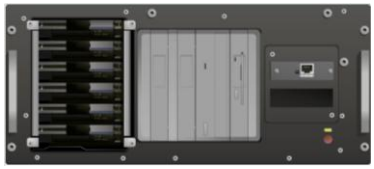
Nom de l'équipement	Figure	Equipement
Routeur 2811		
Switch2960		
Point d'acces Wifi		
Terminaux		
Connexions		
Serveur de service		

Tableau (3.1) : La liste des équipements

3.6.2 Plan d'adressage

- **Plan d'adressage des services**

Service	Emplacement	Adresse réseau	Adresse sous réseau
Service 1	Quatrième étage	192.168.1.0	255.255.255.0
Service 2	Quatrième étage	192.168.2.0	255.255.255.0
Service 3	Troisième étage	192.168.3.0	255.255.255.0
Service 4	Troisième étage	192.168.4.0	255.255.255.0
Service 5	deuxième étage	192.168.5.0	255.255.255.0
Service 6	premier étage	192.168.6.0	255.255.255.0
Réception	Rez-de-chaussée	192.168.7.0	255.255.255.0

Tableau (3.2) : Plan d'adressage sous réseau

- **Plan d'adressage des utilisateurs des services**

Utilisateur	VLAN	Adresse IP	Passerelle
Doyen de la faculté	VLAN 10	192.168.1.2	192.168.1.1
Secrétariat du doyen de la faculté	VLAN 10	192.168.1.3	192.168.1.1
Vice-Doyen chargé des études	VLAN 20	192.168.2.2	192.168.2.1
Secrétariat Vice-Doyen	VLAN 20	192.168.2.3	192.168.2.1
Chef de service de l'enseignement	VLAN 20	192.168.2.4	192.168.2.1
Chef de service de l'évaluation et de l'éducation	VLAN 20	192.168.2.5	192.168.2.1
Chef de service des statistiques	VLAN 20	192.168.2.6	192.168.2.1
Vice-Doyen chargé de la post- graduation et de la recherche et des relations extérieures	VLAN 30	192.168.3.2	192.168.3.1
Secrétariat Vice-Doyen	VLAN 30	192.168.3.3	192.168.3.1
Chef de service de suivi de la formation post de graduation	VLAN 30	192.168.3.4	192.168.3.1
Chef de service de suivi des activités de recherche	VLAN 30	192.168.3.5	192.168.3.1
Chef de service des statistiques	VLAN 30	192.168.3.6	192.168.3.1
Responsable de la bibliothèque	VLAN 40	192.168.4.2	192.168.4.1
Chef de service de gestion	VLAN 40	192.168.4.3	192.168.4.1
Chef de service de l'orientation et de recherche	VLAN 40	192.168.4.4	192.168.4.1
Chef de service de l'orientation et de recherche	VLAN 50	192.168.5.2	192.168.5.1
Secrétaire général de la faculté	VLAN 50	192.168.5.3	192.168.5.1
Secrétariat du secrétaire général	VLAN 50	192.168.5.4	192.168.5.1
Chef de service des personnels	VLAN 50	192.168.5.5	192.168.5.1
Direction des personnels	VLAN 50	192.168.5.6	192.168.5.1
Direction des enseignants	VLAN 50	192.168.5.7	192.168.5.1
Chef de service des activités scientifiques culturelles et sportives	VLAN 50	192.168.5.8	192.168.5.1
Chef de service trésorier et comptabilité	VLAN 50	192.168.5.9	192.168.5.1
Direction trésorier	VLAN 50	192.168.5.10	192.168.5.1
Chef de service des moyens et de maintenance	VLAN 50	192.168.5.11	192.168.5.1
Direction des moyens	VLAN 50	192.168.5.12	192.168.5.1
Direction de maintenance	VLAN 50	192.168.5.13	192.168.5.1
Chef de département adjoint chargé de l'enseignement et formation de graduation	VLAN60	192.168.6.2	192.168.6.1
Secrétariat du Chef de département	VLAN60	192.168.6.3	192.168.6.1
Chef de département adjoint chargé de l'enseignement et formation de graduation	VLAN60	192.168.6.4	192.168.6.1
Chef de service de l'enseignement	VLAN60	192.168.6.5	192.168.6.1
Chef de service de suivi enseignement et évaluation	VLAN60	192.168.6.6	192.168.6.1
Chef de département adjoint chargé de formation post de graduation	VLAN60	192.168.6.7	192.168.6.1
Chef de service chargé de formation post de graduation	VLAN60	192.168.6.8	192.168.6.1
Chef de service chargé de suivi des recherches	VLAN60	192.168.6.9	192.168.6.1
Réception	VLAN70	192.168.7.3	192.168.7.1

Tableau (3.3) : Plan d'adressage des utilisateurs

- **Plan d'adressage des responsables de la faculté**

Utilisateur	Adresse IP
Doyen de la faculté	192.168.1.2
Vice-Doyen chargé des études	192.168.2.2
Vice-Doyen chargé de la post-graduation et de la recherche et des relations extérieures	192.168.3.2
Responsable de la bibliothèque	192.168.4.2
Secrétaire général de la faculté	192.168.5.2
Chef de département adjoint chargé de l'enseignement et formation de graduation	192.168.6.2

Tableau (3.4) : Plan d'adressage des responsables

- **Plan d'adressage des secrétariats des services**

Utilisateur	Adresse IP
Secrétariat du doyen de la faculté	192.168.1.3
Secrétariat Vice-Doyen chargé des études	192.168.2.3
Secrétariat Vice-Doyen chargé de la post-graduation et de la recherche et des relations extérieures	192.168.3.3
Responsable de la bibliothèque	192.168.4.3
Secrétariat du secrétaire général	192.168.5.3
Secrétariat du Chef de département	192.168.6.3
Réception	192.168.7.3

Tableau (3.5) : Plan d'adressage des secrétariats

- **Plan d'adressage des ports du routeur**

Type de port	Numéro du port	Adresse IP
FastEthernet	0/0.1	192.168.1.1
FastEthernet	0/0.2	192.168.2.1
FastEthernet	0/0.3	192.168.3.1
FastEthernet	0/0.4	192.168.4.1
FastEthernet	0/0.5	192.168.5.1
FastEthernet	0/0.6	192.168.6.1
FastEthernet	0/0.7	192.168.7.1

Tableau (3.6) : Plan d'adressage des ports du routeur

6.3 Organigramme :

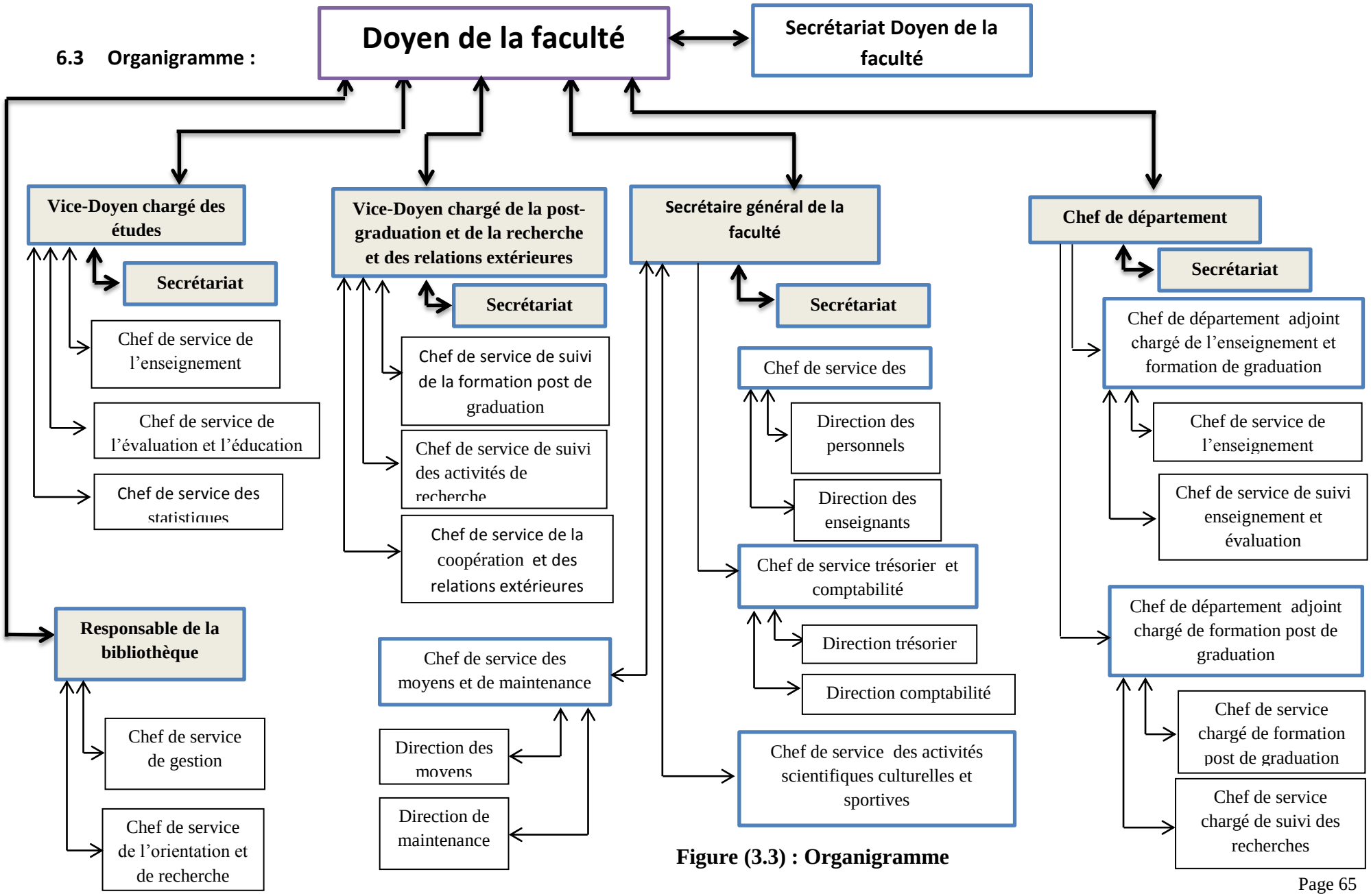


Figure (3.3) : Organigramme

3.6.4 Description de l'architecture du réseau

Dans notre architecture on a devisé le réseau LAN de la faculté en plusieurs sous réseaux, chaque sous réseau représente un service, soit donc cinq services plus le sous réseau du doyen qui regroupe le doyen avec son secrétariat.

En implantant la notion ACL on a créé deux groupes avec des autorisations d'accès bien définies, le premier regroupe le doyen avec les responsables des services dans un réseau fermé, et le deuxième contient tous les secrétariats avec la réception pour assurer la coordination entre tous les services, chaque responsable et son secrétariat se situent dans un réseau avec tous les utilisateurs de son service, donc on peut résumer notre réseau dans les point ci-dessous :

- Les utilisateurs des services ne peuvent communiquer qu'avec le responsable du service et son secrétariat, cette topologie nous donne une première barrière de sécurité du réseau.
- Toutes communications entre les services passent toujours par les secrétariats ce qui donne une organisation de la coordination entre les services.
- Le doyen et les responsables des services peuvent communiquer librement dans un réseau, pour assurer plus de sécurité des informations échangés.

3.6.5 Schémas de l'architecture par service

- Schéma du service : Doyen de la faculté

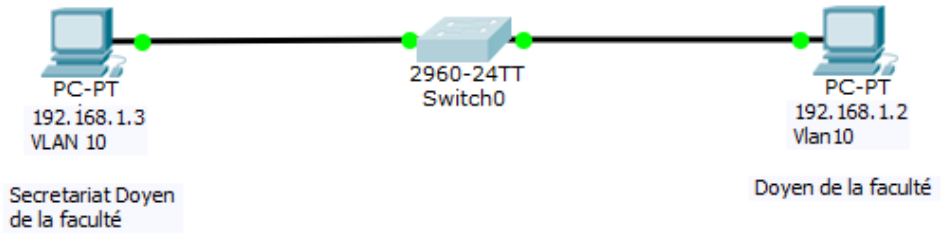


Figure (3.4) : Schéma du service : Doyen de la faculté

- Schéma de service : Vice-Doyen chargé des études :

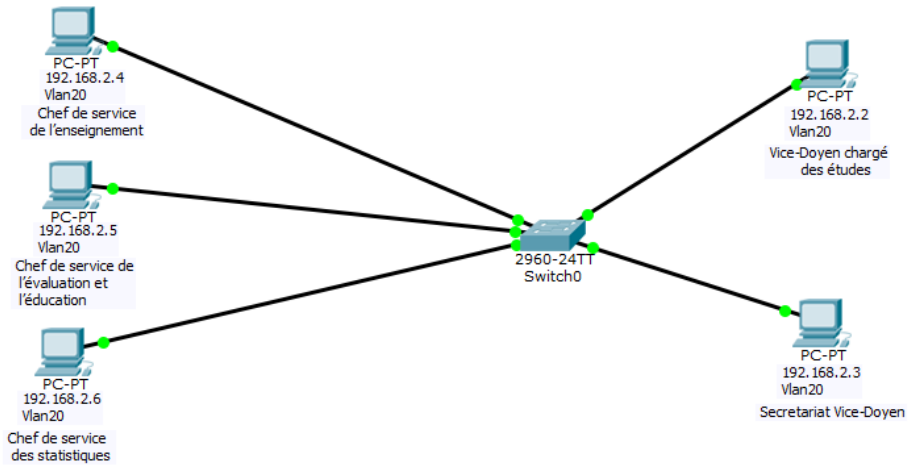


Figure (3.5) : Schéma de service : Vice-Doyen chargé des études

- Schéma de service : Vice-Doyen chargé de la post-graduation et de la recherche et des relations extérieures :

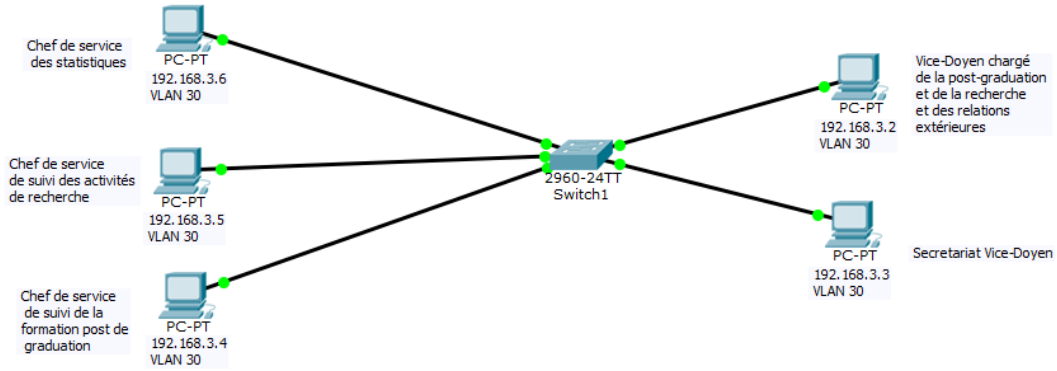


Figure (3.6) : Schéma de service : Vice-Doyen chargé de la post-graduation et de la recherche et des relations extérieures

- Schéma du service : Secrétaire général de la faculté :

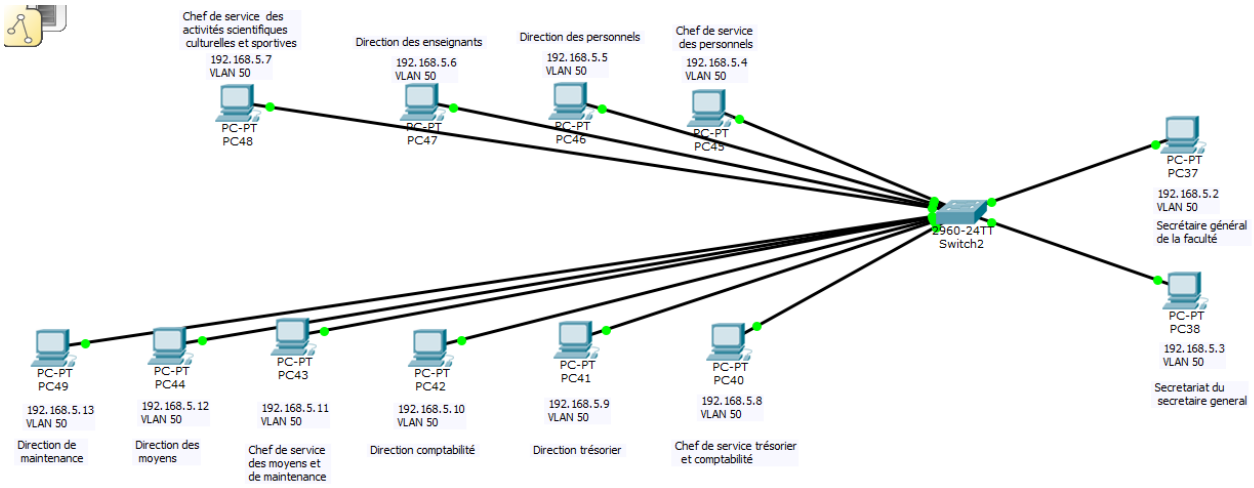


Figure (3.7) : Schéma du service : Secrétaire général de la faculté

- Schéma du service : Chef de département**:**

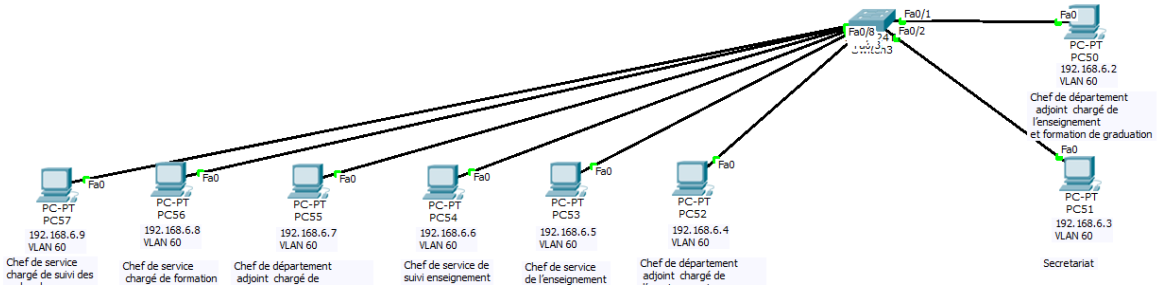


Figure (3.8) : Schéma du service : Chef de département

- Schéma du service: Responsable de la bibliothèque

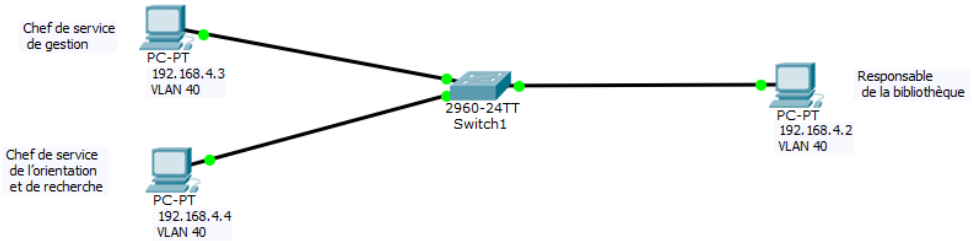


Figure (3.9) : Schéma du service: Responsable de la bibliothèque

- Réseau Doyen et responsables des services

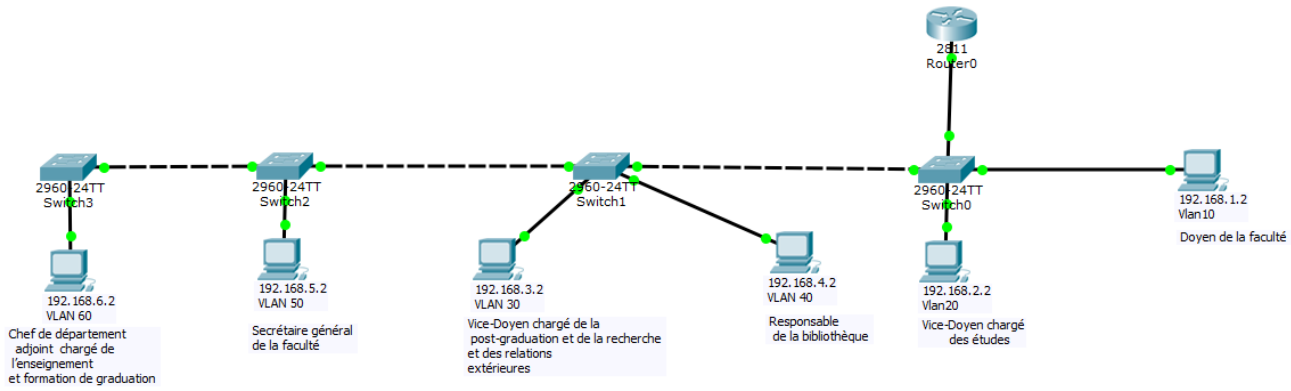


Figure (3.10) : Réseau Doyen et responsables des services

- Réseau entre les secrétariats et la réception :

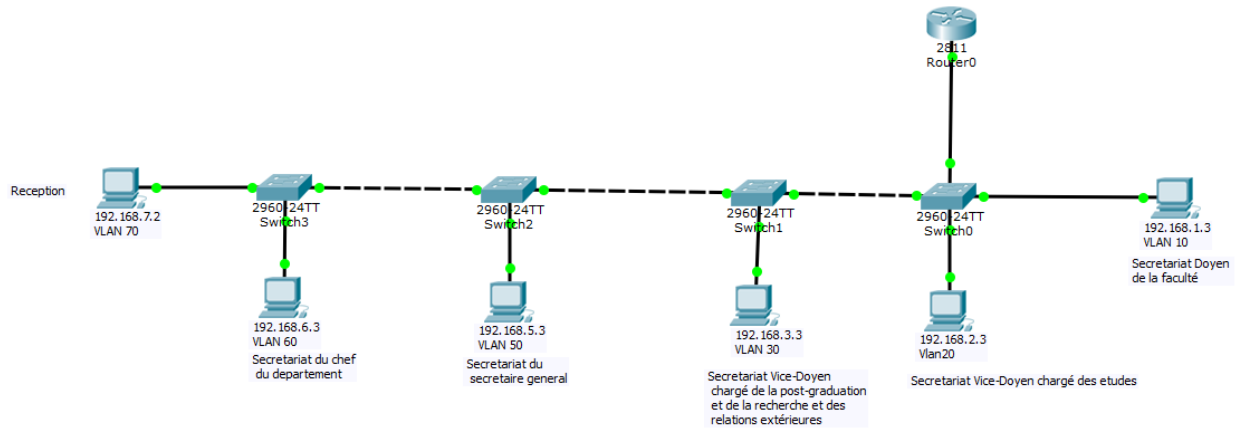


Figure (3.11) : Réseau entre les secrétariats et la réception

- **Architecture générale de la faculté**

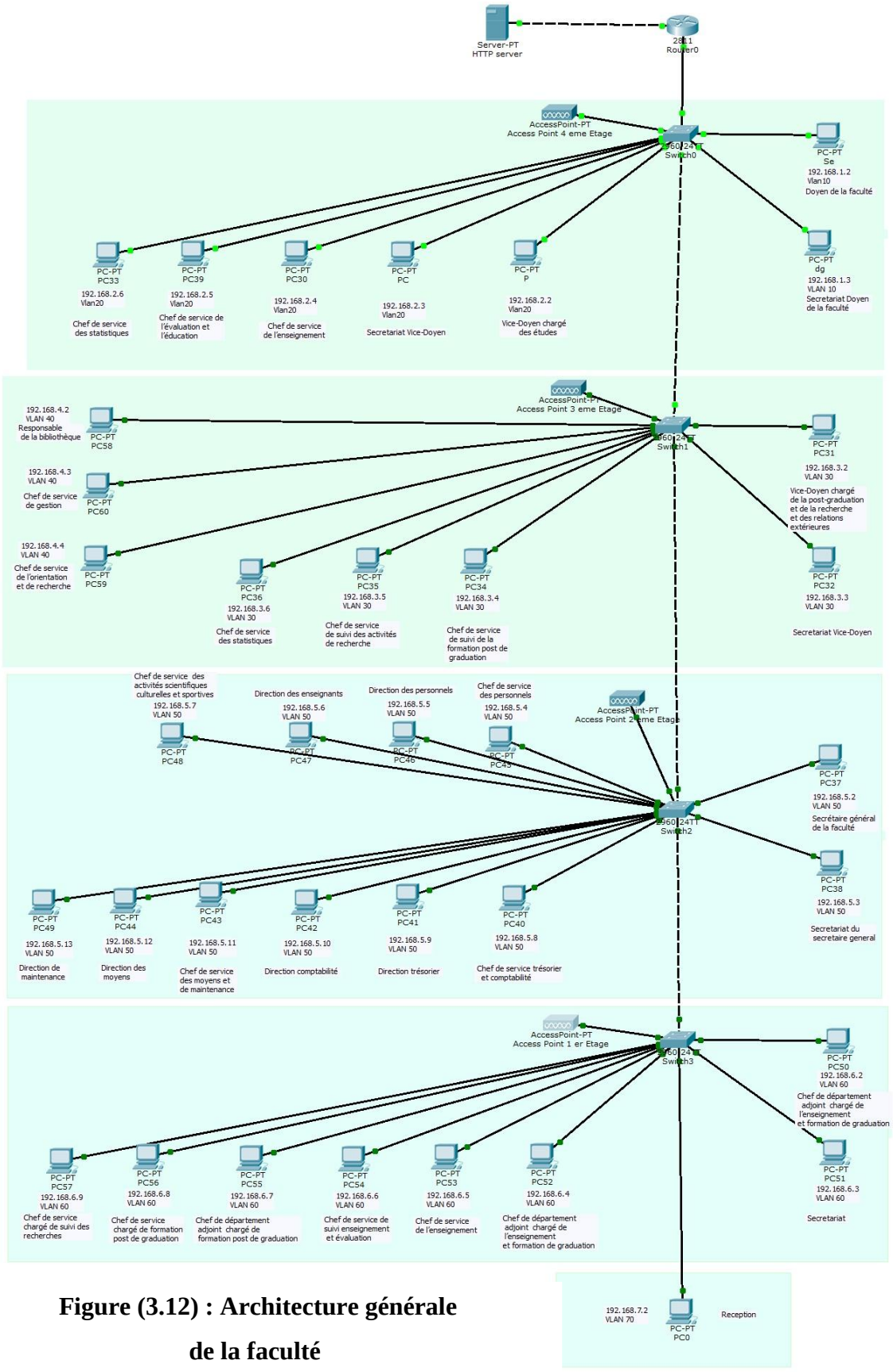


Figure (3.12) : Architecture générale de la faculté

3.6.6 Configuration des terminaux

Configuration des adresses IP des postes des utilisateurs : Voici un exemple du poste de chef de service, et de la même façon on configure tous les autres terminaux (voir la figure 3.13).

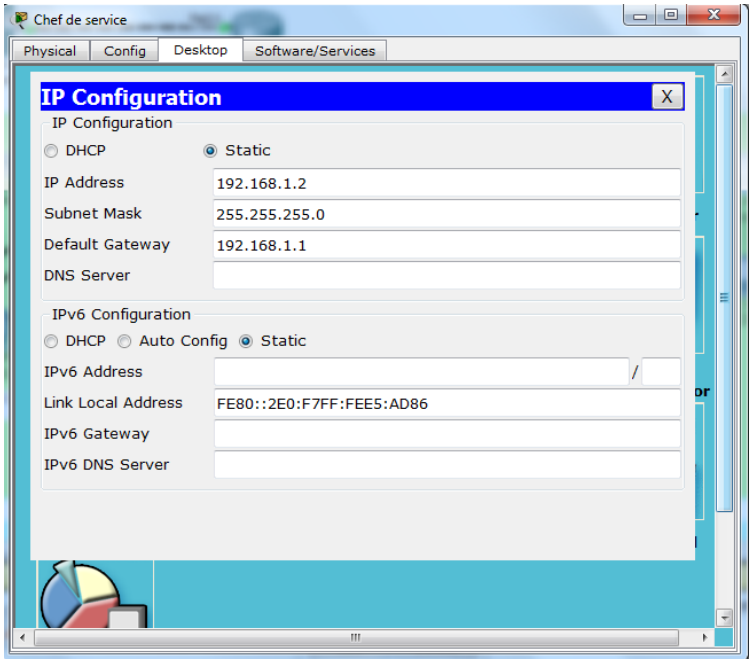


Figure (3.13) : Configuration IP d'un utilisateur

3.6.6.1 Configuration des switchs :

- **Création des Vlans :**

On va configurer les Vlans de notre réseau comme suit :

Réseau	Localité	Vlan ID	Switch
192.168.1.0	4eme Etage	Vlan 10	Switch0
129.168.2.0	4eme Etage	Vlan 20	Switch0
192.168.3.0	3eme Etage	Vlan 30	Switch1
129.168.4.0	3eme Etage	Vlan 40	Switch1
129.168.5.0	2eme Etage	Vlan 50	Switch2
129.168.6.0	1eme Etage	Vlan 60	Switch3
129.168.7.0	Rez-de-chaussée	Vlan 70	Switch3

Tableau (3.7) : Réseaux VLANs

Creation des VLANs dans les switch 0 :

```
Switch>enable
Switch#configure terminal
Switch(config)#vlan 10
Switch(config-vlan)#exit
Switch(config)#vlan 20
Switch(config-vlan)#exit
Switch(config)#vlan 30
Switch(config-vlan)#exit
Switch(config)#vlan 40
Switch(config-vlan)#exit
Switch(config)#vlan 50
Switch(config-vlan)#exit
Switch(config)#vlan 60
Switch(config-vlan)#exit
Switch(config)#vlan 70
Switch(config-vlan)#exit
```

- **Configuration des Ports**

Configuration du Port 0/1, et de la même façon pour les autres ports du mode access

```
Switch(config)#
Switch(config)#interface fastEthernet 0/1
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 10
Switch(config-if)#
```

Configuration du Port 0/23 et 0/24 en mode Trunk

```
Switch(config)#interface fastEthernet 0/23
Switch(config-if)#switchport mode trunk
Switch(config-if)#interface fastEthernet 0/24
Switch(config-if)#switchport mode trunk
Switch(config-if)#
```

- **Configuration des Switch2, Switch3 et Switch4 :** la même configuration du Switch0.

3.6.6.2 Configuration du routeur

- **Etape 1 :**

Configuration du Port 0/0 au niveau du routeur, en utilisant dans notre cas les sous interfaces pour pouvoir utiliser les VLANs avec les commandes suivantes :

- **encapsulation dot1Q 10** : pour déclarer le VLAN.
- **ip address** : affectation IP.
- **no shutdown** : pour allumer le port.

```
Router(config)#interface fastEthernet 0/0.1
Router(config-subif)#encapsulation dot1Q 10
Router(config-subif)#ip address 192.168.1.1 255.255.255.0
Router(config-subif)#no shutdown

Router(config)#interface fastEthernet 0/0.2
Router(config-subif)#encapsulation dot1Q 20
Router(config-subif)#ip address 192.168.2.1 255.255.255.0
Router(config-subif)#no shutdown

Router(config)#interface fastEthernet 0/0.3
Router(config-subif)#encapsulation dot1Q 30
Router(config-subif)#ip address 192.168.3.1 255.255.255.0
Router(config-subif)#no shutdown

Router(config)#interface fastEthernet 0/0.4
Router(config-subif)#encapsulation dot1Q 40
Router(config-subif)#ip address 192.168.4.1 255.255.255.0
Router(config-subif)#no shutdown

Router(config)#interface fastEthernet 0/0.5
Router(config-subif)#encapsulation dot1Q 50
Router(config-subif)#ip address 192.168.5.1 255.255.255.0
Router(config-subif)#no shutdown

Router(config)#interface fastEthernet 0/0.6
Router(config-subif)#encapsulation dot1Q 60
Router(config-subif)#ip address 192.168.6.1 255.255.255.0
Router(config-subif)#no shutdown

Router(config)#interface fastEthernet 0/0.7
Router(config-subif)#encapsulation dot1Q 70
Router(config-subif)#ip address 192.168.7.1 255.255.255.0
Router(config-subif)#no shutdown
```

- **Etape 2 :** Configuration du Port 0/1 pour l'accès extérieur

```
Router(config)#
Router(config)#interface fastEthernet 0/1
Router(config-if)#ip address 10.0.0.1 255.255.255.0
Router(config-if)#no shutdown
```

- **Etape 3 :** Configuration de la statique route

```
Router(config)#

Router(config)#ip route 192.168.0.0 255.255.255.0 10.0.0.2

Router(config)#
```

3.6.7 Contrôle d'accès ACL

Les ACLs utilise un contrôle d'accès par liste qui contient des adresses IP ou des numéros de port pour autoriser ou interdire des utilisateurs a accéder au postes des autres utilisateurs, et au différents service disponibles.

Les ACLs sont devisés en deux catégories : standards et étendus.

- ACLs Standards : contrôle les accès à partir de l'adresse IP source en utilisant le masque générique.

- ACLs Etendus : contrôle les accès à partir de l'adresse source et destination en utilisant le masque générique.

Dans notre travail on va limiter les accès selon l'organigramme proposé comme suit :

- Chaque utilisateur ne peut communiquer qu'au niveau interne avec les utilisateurs du même service, et ne peut accéder qu'au service autorisé (par exemple le service de navigation).
- Le responsable peut communiquer avec les utilisateurs du service, et aussi avec les responsables des autres services.
- Le secrétariat de chaque service peut communiquer avec les utilisateurs du même service, et aux secrétariats des autres services.

Donc on est obligé d'utiliser les ACLs étendus qui utilisent les adresses source et destination comme suit :

Etape 1 :

Pour permettre la communication entre les responsables des services on va créer une access-list nommé Liste1, et ensuite configurer les permutations d'accès de tous les responsables des services.

```
Router>enable
Router(config)#ip access-list
Router(config)#ip access-list extended Liste1
Router(config-ext-nacl)#
```

Etape 2 :

Ci-dessous la configuration entre le Doyen de la faculté (IP : 192.168.1.2) avec le poste Vice-Doyen chargé des études (IP : 192.168.2.2).

```
Router(config-ext-nacl)#permit ip 192.168.1.2 ?
A.B.C.D Source wildcard bits
Router(config-ext-nacl)#permit ip 192.168.1.2 0.0.0.0 192.168.2.2 ?
A.B.C.D Destination wildcard bits
Router(config-ext-nacl)#permit ip 192.168.1.2 0.0.0.0 192.168.2.2 0.0.0.0
Router(config-ext-nacl)#
```

Etape 3 :

Configuration de tous les autres postes de la même façon avec la même commande.

```
Extended IP access list Liste1
10 permit ip host 192.168.2.2 host 192.168.1.2
20 permit ip host 192.168.1.2 host 192.168.2.2
30 permit ip host 192.168.1.2 host 192.168.3.2
40 permit ip host 192.168.3.2 host 192.168.1.2
50 permit ip host 192.168.4.2 host 192.168.1.2
60 permit ip host 192.168.1.2 host 192.168.4.2
70 permit ip host 192.168.2.2 host 192.168.3.2
80 permit ip host 192.168.3.2 host 192.168.2.2
90 permit ip host 192.168.4.2 host 192.168.2.2
100 permit ip host 192.168.2.2 host 192.168.4.2
110 permit ip host 192.168.3.2 host 192.168.4.2
120 permit ip host 192.168.4.2 host 192.168.3.2
```

Etape 4

Pour permettre la communication entre les secrétariats et la réception on va configurer les permutations d'accès.

Ci-dessous la configuration entre le poste Secrétariat Doyen de la faculté (IP : 192.168.1.3) avec le poste Secrétariat Vice-Doyen (IP : 192.168.2.3).

```
Router>enable
Router(config)#ip access-list extended Liste1
Router(config-ext-nacl)#permit ip 192.168.1.3 0.0.0.0 192.168.2.3 0.0.0.0
Router(config-ext-nacl)#
```

Configuration de tous les autres postes secrétariats de la même façon avec la même commande :

```
Extended IP access list post1
10 permit ip host 192.168.2.3 host 192.168.1.3
20 permit ip host 192.168.1.3 host 192.168.2.3
30 permit ip host 192.168.1.3 host 192.168.3.3
40 permit ip host 192.168.3.3 host 192.168.1.3
50 permit ip host 192.168.4.3 host 192.168.1.3
60 permit ip host 192.168.1.3 host 192.168.4.3
70 permit ip host 192.168.2.3 host 192.168.3.3
80 permit ip host 192.168.3.3 host 192.168.2.3
90 permit ip host 192.168.4.3 host 192.168.2.3
100 permit ip host 192.168.2.3 host 192.168.4.3
110 permit ip host 192.168.3.3 host 192.168.4.3
120 permit ip host 192.168.4.3 host 192.168.3.3
```

Etape 5

La configuration de la permutation pour tous les postes pour l'accès vers l'extérieur

```
Extended IP access list post1
130 permit ip 192.168.0.0 0.0.255.255 host 10.0.0.2
140 permit ip host 10.0.0.2 192.168.0.0 0.0.255.255
```

Etape 6

Activation de la liste au niveau des sous interfaces **: fa 0/0**

```
Router(config)#interface fastEthernet 0/0.1
Router(config-subif)#ip access-group Liste1 in
Router(config)#interface fastEthernet 0/0.2
Router(config-subif)#ip access-group Liste1 in
Router(config)#interface fastEthernet 0/0.3
Router(config-subif)#ip access-group Liste1 in
Router(config)#interface fastEthernet 0/0.4
Router(config-subif)#ip access-group Liste1 in
Router(config)#interface fastEthernet 0/0.5
Router(config-subif)#ip access-group Liste1 in
Router(config)#interface fastEthernet 0/0.6
Router(config-subif)#ip access-group Liste1 in
Router(config)#interface fastEthernet 0/0.7
Router(config-subif)#ip access-group Liste1 in
Router#
```

3.7 Conclusion

Apres la réalisation du réseau LAN de la faculté de la technologie, en utilisant le logiciel de simulation du Cisco Paket Tracer, on est arrivée à :

- Comprendre la conception d'un réseau local, avec tous les composants hardwares (Routeur, switch, PC …) en reliant ces équipements avec des différents types de liaison tels que les câbles directs et croisées et le Wifi. Et de configurer les paramètres de chaque équipement.
- Comment partager et optimiser le réseau (partage sous réseau et VLANs).
- Configurer la sécurisation d'un réseau local en utilisant les VLANs et les ACLs.

Conclusion générale

Le concept réseau dans le domaine informatique est devenue le cœur des réseaux de transmission et des réseaux mobile, donc on voit aujourd'hui qu'il est indispensable pour les personnes qui travaillent dans le domaine du télécommunication que ce soit ingénieurs, techniciens, ou chercheurs , d'avoir toutes les notions de base sur les réseaux.

Dans notre mémoire on a étudié les étapes de réalisation d'un réseau d'entreprise ou établissement de gestion, en utilisant les VLAN (Vertual local area network) qui représentent le cœur de la configuration de réseau local, qui est le noyau des réseaux MAN (Metropolitan Area Network), et WAN (Wide Area Network).

Et aussi la conception d'un mécanisme de sécurité qui a le rôle de filtrer tous les menaces et les attaques de l'intérieur et de l'extérieur. Cette conception vient d'une part de la répartition hardware du réseau et l'implantation des VLANs, et d'autre part par l'utilisation des listes de contrôle d'accès ACLs, qui se basent sur le filtrage des paquets entrants ou sortants, par l'utilisation des adresses IP source et IP destination selon le besoin.

Une sécurité optimisé par l'empêche des hôtes ou des réseaux indésirable ou suspect, ce que diminuer le risque de violations de confidentialité. Les VLAN gèrent de frontière virtuel présente une citadelle plus immunisante ne pouvant être franchies que par le biais de fonctionnalités de routage, donc la sécurité communication et bien renforcée.

Efficacité de la gestion sans devoir changer les liens physiques nous pouvant rapidement et simplement faire de modification dans le réseau. Tous ces dernier offre un gain de temps et un coût réduit.

La politique qu'on a utilisé pour réaliser le réseau d'établissement est de limiter l'accès de chaque utilisateur selon les critères donnés par l'administrateur, plus la protection contre le attaques et les menaces qui peuvent intervenir de la connexion avec le réseau extérieur de même du réseau interne.

En terme d'innovations et perspectives il reste néanmoins de souligner qu'il est impératif de procéder au développement dans le sens d'améliorer les performances en terme d'aspect sécuritaire des réseaux informatiques afin de véhiculer et protéger l'information en amont et en aval et en terme d'évaluation cette information qui constitue la devise d'une entreprise sur le plan développement et productivité et per formance.

Références

[1] Guy Pujolle « Les réseaux», 8eme édition, Eyrolles Paris, 2014.

[2] Karine SILINI « Certificat Informatique et Internet, niveau 1, réf v2 », Université du Littoral Côte d'Opale

[3] Guy Pujolle «Initiation aux réseaux, cours et exercices», Edition, Eyrolles Paris, 2012.

[4] Christian Bulfone «Le protocole IP », Licence MIASS, 2012.

[5] Etienne Duris « Réseaux », Université Paris Est, Marnela Vallée, Janvier 2010.

[6] Request for Comments RFC (Internet protocole).

[7] François Laissus « Cours d'introduction a TCP/IP», Version du 25 février 2009.

[8] « CCNA Module 1 », Essentiel International University, Release 09/2008.

[9] LESCOP Yves « Sécurité », Version 1.6, 2002.

[10] Aurélien Roux « Configurez routeurs et commutateurs: Exercices et corrigés», 3ème édition, 2011.

[11] Daniel Dromard et Dominique Seret « Architecture des réseaux », Pearson Education France.2009.

[12] Claude Servin, « Réseaux et télécom ». 2ème édition, Dunod, 2010.

[13] Jean-Christophe GALLARD « Sécurité et Réseaux», Version 2.0, Octobre 2005

[14] Techno-science.net

[15] Cyril, «Réussir son CCNA », Copyright 2015.

[16] STIC-Informatique, Master 2Professionnel « Les ACL Cisco », Université de Reims Champagne Ardenne.

[17] Jean François, « La sécurité informatique dans la petite entreprise ». ENI édition, France, 2003.

[18] André Vaucamps « Rappel sur la notion de VLAN (Virtual Local Area Network) »Eni éditions, 2013.

[19] Philippe Atelin « réseaux informatique notions fondamentales » 3ème édition, Paris 2014.

[20] F Andreasen, B Foster « Media Gateway Control Protocol (MGCP*)* », RFC 3435, IETF, January 2003.

[21] Pascal Nicolas « Cours de réseaux, Maîtrise d'informatique », U.F.R Sciences de l'Université d'Angers.

Résumé

La sécurité des réseaux privés représente un objectif précieux à l'échelle de qualité de service offerte, on ne peut pas juger qu'un service est fiable sans sécurité convenable.

Il y a plusieurs niveaux de sécurités mais ceux de niveau de routage sont les plus importants car ; en outre de protection contre les paquets indésirables ; ils optimisent les ressources de réseau (contrôle de flux).

Dans notre travail nous allons implémenter une méthode de sécurité des réseaux privés par les listes de contrôle d'accès ACL.

Nous allons montrer comment mettre une configuration générale de base d'un réseau local qui représente le noyau de tous les réseaux informatiques, en construisant des VLAN (Virtuel area network), et comment le sécuriser par l'utilisation des listes de contrôle d'accès, de type étendus, cette configuration répond au besoin supposés de la faculté technologie de l'université d'El Oued.

Mots clés : Réseau VLAN, adressage des réseaux, routage, ACL.

Abstract

The security of private networks is a valuable objective in terms of the quality of service offered, and it cannot be judged that a service is reliable without adequate security.

There are several levels of security but those of routing level are the most important because, In addition to protection against unwanted packets, they optimize network resources (flow control).

In our project we will implement a method of security of the private networks by the ACLs.

We will show how to put a basic general configuration of a LAN that represents the core of all computer networks, building VLANs (virtual area network), and how to secure it through the use of ACLs , by using extended ACL, this configuration corresponds to the supposed need of the faculty of technology of the university of El Oued.

Keywords: VLAN, network addressing, routing, ACL.

ملخص

أمن الشبكات الإلكترونية يبقى الهدف الأول والأسمى من أجل ضمان جودة الخدمة المقدمة، و لا يمكننا الحكم على أي شبكة بالجودة دون الرجوع إلى درجة أمن المعلومات الموجودة بها.

هناك عدة مستويات لأمن المعلومات ولكن يبقى تأمين المعلومة انطلاقا من مسارها هو أهم هاته المستويات أي حجب أو حذف الحزم غير المرغوب في وصولها إلى الوجهة او حتى دخولها إلى شبكة معينة مما يضمن لنا الاستخدام الأمثل للموارد المتاحة.

في إطار عملنا المقدم سوف نقوم بإنشاء شبكة خاصة وتأمينها بواسطة استخدام قوائم التحكم للدخول إلى شبكة معينة ACL .

وسوف نعرض كيفية إعداد قاعدة بيانات مشتركة داخل شبكة محلية و التي تمثل جوهر كل شبكات الحاسوب عبر العالم، ومن ثم إنشاء شبكة محلية باستخدام الشبكات الافتراضية VLAN ، و كذلك كيفية تأمينها باستخدام قوائم التحكم للدخول، كل ذلك من أجل الوصل إلى شبكة تتماشى و الحاجة المطلوبة من طرف إدارة معهد التكنلوجيا بجامعة الوادي .

الكلمات المفتاحية : الشبكة المحلية، الشبكة المحلية الافتراضية، أمن الشبكات، ACL .