Ministère de l'Enseignement Supérieur et de la Recherche Scientifique
Université Abderrahmane Mira de Béjaïa
Faculté des Sciences Exactes
Département d'Informatique

Mémoire de Fin de Cycle

En Vue de l'Obtention du Diplôme de Master en Informatique

Option : Réseaux et Systèmes Distribués

Thème :

Proposition d'une configuration sécurisée : cas du réseau intranet de SONATRACH

Réalisé par :

M^{lle} MAHFOUF Sabrina & M^{lle} KHIROUN Kafia

Devant le jury composé de :

Président :	M^{r} AMROUN	Kamel	, M.A.A.
Examinateur :	M^{r} TOUAZI	Djoudi	, M.A.A.
Examinateur :	M^{r} DEMOUCHE	Mouloud	, M.A.B.
Encadreur :	D^{r} boukram	Mawloud	, M.C.B.
Co-Encadreur :	M^{r} SAADI	Mustapha	, M.A.A.

Juin 2014

Dédicaces

Je dédie ce modeste travail :

à mes parents, à mes grands parents
À mes frères et sœurs , À ma belle sœur,
à mon marie qui ma soutenu durant le travaile ,
À mes nièces et mes neveux :
Amer, Teyeb,Haytem, Dida, Wassila, Fareh,
à mes oncles, à mes tantes, à tous mes cousins,
à toute ma famille de prés et de loin , à mes collègues, à tous
les étudiants de master2 informatique(promotion2014), à tous mes amis,
`Sabrina`

Je dédie ce modeste travail *:*

à mes parents, à mes grands parents
à mon frère Samir et sa femme Tassadite
à mes deux nièces Alyssia et Chanez
à mon frère Nabil et sa femme Sabrina
à mon frère Sofiane à mes sœurs Thinhinane et Sélia
à mes oncles et mes tantes à mes cousins et cousines
à toute ma famille de prés et de loin à mes amis à mes collègues,
à tous les étudiants de master2 informatique (promotion 2012),
à tous mes amis : Thiziri, Kahina, Dahia, je pense particuliérement
à mes meilleures amies : Hamida Cherfa, Dalal Toudji, Ratiba Belkassemi,et leurs familles.
`Nassima`

Que la paix d'Allah soit avec tous... !

Table des matières

Table des figures

Liste des tableaux

Liste d'abréviation

AAA Authentication Autorisation Acounting

ACL List de Control d'Accès

AD Active Directory

ARP Address Resolution Protocol

ATM Asynchronous Transfer Mode

BNC Bayonet -Neil-Concelman

CIFS Common Internet File System

CSMA/CD Carrier Sense Multiple Colhision Detection

DHCP Dynamic Host Configuration Protocol

DMZ Zone Demilitarisée

DNS Domain Name System

DOS Disk Operating System

FDDI Fiber Distributed Data Interface

FTP File Transport Protocol

GPO Group Policiers Object

HDLC High-Level Data Link Control

H-IDS Host Intrusion Detection System

HSRP Hot Standby Routing Protocol

HTTP Internet Engineering Task Force

ICMP Internet Control Message Protocol

IEEE Institute of Electrical and Electronics Engineers

IGMP Internet Group Management Protocol

IP Internet Protocol

LAN Local Area Network

L2TP Layer 2 Turnneling Protocol

MAC Media Access Control

MAN métropolitain Area Network

MAU Multistation Access Unit

MD5 Message Digest 5

Net BEUI Net Bios Extended User Interface

NEEF National Environmental Education Foundation

N-IDS Network Based Intrusion Detection System

OSI Open Systems Interconnection

PCI Pro Conseil Industries

PPTP Point-to-Point Turnneling Protocol

RADIUS Remote Authentication Dial-In User Service

RARP Reverse Address Resolution Protocol

SG510 Blue Coat SG510 Quick Start Guide

SHA Secure Hash Algorithm

SMB Serveur Message Block

SMTP Simple Mail Transfer Protocol

SQL Structured Query Language

STP Spanning Tree Protocol

SSL Secure Sockets Layers

TCP Transmission Control Protocol

TFTP Trivial File Transfer Protocol

UDP User Datagram Protocol

UTP Unshielded Twiseted Pair

VTP Vlan Trunking Protocol

VLAN Virtual Local Area Network

VPN Virtuel Private Network

WAN Wide Area Network

Introduction générale

L'utilisation croissante des réseaux informatiques dans les entreprises et leurs interconnexions à internet ont fait émerger aujourd'hui de nouvelles préoccupations sécuritaires. La majorité des entreprises ne peuvent plus ignorer désormais d'intégrer la sécurité informatique de leurs réseaux dans leurs cahiers des charges, si elles ne veulent pas risquer de voir leurs outils de travail perturbés par une attaque ciblée ou non, généralisée, véhiculée par le réseau mondial ou par leurs propres réseaux locaux. Pour ne pas perdre d'informations névralgiques, une stratégie de défense sécuritaire en conséquence s'impose. Et vue la diversité des attaques évolutives dans le temps, il faut constamment rechercher de nouvelles solutions pour sécuriser le réseau.

La sécurité des réseaux est devenue un élément-clé de la continuité des systèmes informatiques de l'entreprise quelque soit son activité, sa taille et sa répartition géographique. L'entreprise SONATRACH de Béjaïa ne fait pas exception à cette règle. Avec la communauté des utilisateurs (directeur, chefs de services, employés.) qui ne cesse d'augmenter la nécessité de partager les données stratégiques et les services disponibles, les risques sécuritaires augmentent également. La fragilité du réseau actuel vis-à-vis d'éventuelles attaques internes et/ou externes, nous pousse à élaborer des mesures de sécurité plus résistantes à tout cela ! C'est dans ce contexte que se situe notre travail, avec comme principal objectif : - proposition d'une configuration sécurisée du réseau intranet.

Structure du mémoire

Dans le chapitre 1, nous présentons les généralités sur les réseaux informatiques. Le chapitre 2, est consacré aux différentes techniques d'attaques, à la présentation de la politique de sécurité et sa mise en œuvre. Les objectifs et les stratégies de sécurité y sont présentés également. Le chapitre3, fait l'objet d'une étude critique de l'architecture du réseau intranet de la société en question tel qu'il est utilisé en ce moment. Nous présentons de nouvelles propositions et suggestions pour définir une nouvelle configuration plus sécurisée pour cette architecture. Le quatrième chapitre n'est autre que la partie implémentation d'un réseau avec sa configuration sous le simulateur Packet Tracer.

Enfin, nous terminons notre mémoire par une conclusion générale résumant les points forts accomplis dans ce travail, tout en spécifiant quelques perspectives futures pour mener à bien ce travail qui s'inscrit dans les systèmes complexes de la sécurité informatique.

Chapitre 1

Généralites sur les réseaux informatiques

Introduction

Un réseau informatique est un ensemble de moyen qui permet la communication entre des processus d'application où les tâches sont réparties sur des matériels informatique de tout type. Ces matériels communiquent entre eux grâce à des protocoles.

Un protocole est un ensemble de règles structurées selon lesquelles deux entités différentes peuvent communiquer sans aucune ambigüité.

L'objectif d'une telle communication est de pouvoir partager des informations et des ressources matérielles.

L'objectif de ce chapitre est de présenter les concepts de base liés aux réseaux informatiques.

Ces notions formeront la base nécessaire à notre contribution.

1.1 Définition d'un réseau informatique

Un réseau informatique, est un ensemble d'équipements matériels et logiciels interconnectés les uns avec les autres dans le but de partager des ressources (données). Ces équipements peuvent être éloignés ou rapprochés.[4]

Suivant l'éloignement entre ces équipements, on distingue les réseaux suivants :

– **LAN** (Local Area Network) 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 plusieurs centaines de mètres. Les débits

de ces réseaux vont aujourd'hui de quelques mégabits à plusieurs centaines de mégabits par seconde.

– **MAN** (métropolitain Area Network) 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 dialoguer avec l'extérieur.

– **WAN** (Wide Area Network) sont destinés à transporter des données numérique sur des distances à l'échelle d'un pays, voire d'un continent ou de plusieurs continents. Le réseau peut ètre terrestre, il utilise dans ce cas des infrastructures au niveau du sol, essentiellement de grands réseaux de fibre optique, ou hertzien, comme les réseaux satellite.

1.2 Réseau internet/intranet

Le mot internet vient d'InterNetwork, C'est un réseau international d'ordinateurs, ou plus précisément un réseau d'ordinateurs, qui communiquent entre eux grâce à un protocole d'échange de données standard (TCP/IP) [19][15]. La communication entre les différents ordinateurs connectés au réseau internet est transparente pour l'utilisateur.

Le terme intranet quant à lui, il est utilisé pour faire référence à une connexion privée de réseaux locaux et étendus qui appartiennent à une connexion qui a été conçue de manière à être uniquement accessible aux membres, aux employés d'une organisation ou à d'autres personnes disposant d'une autorisation[19].

1.3 Objectifs des réseaux

La nécessité de communication et de partage des informations en temps réel, imposent aujourd'hui aux entreprises ainsi qu'aux individus la mise en réseau de leurs équipements informatiques en vue d'améliorer leurs rendements.

1.3.1 Apport pour les entreprises

les réseaux permettent aux entreprises de :

- Partager des ressources "imprimantes, disque dur, processeur, etc
- Réduire les couts.
  Exemple : au lieu d'avoir une imprimante pour chaque utilisateur qui sera utilisée 1 heure par semaine, on partage cette même imprimante entre plusieurs utilisateurs.
- Augmenter la fiabilité : dupliquer les données et les traitements sur plusieurs machines. Si une machine tombe en panne une autre prendra la relève.
- Fournir un puissant média de communication : (e-mail, conférence virtuelle " Netmeeting ", etc...).

1.3.2 Apports pour les individus

Les réseaux permettent aux individus :

- L'accès facile et rapide à des informations pertinentes : Informations de type financier : payement de factures, consultation de soldes, etc.....
- L'accès au système de type Toile (Web) : recherche des informations de tout genre (sciences, arts, cuisine, sports, etc).
- La communication entre les individus : Vidéoconférence, courrier électronique, groupes d'intérêts (newsgroups) etc...
- L'envoie de textes, de sons et d'images.
- L'accès aux Jeux interactifs : Toutes sortes de jeux (jeux d'échec, de combats, etc)

1.4 Les différents types de réseaux

On distingue généralement deux types de réseaux bien différents, ayant tout de même des similitudes.

- Les réseaux organisés autour de serveurs (client /serveur) appelés aussi les réseaux en mode de diffusion
- Les réseaux poste à poste (Peer to Peer / égal à égal)

Ces deux types de réseaux ont des capacités différentes. Le type de réseau à installer dépend des critères suivants :

- Taille de l'entreprise,
- Niveau de sécurité nécessaire,
- Niveau de compétence d'administration disponible.

1.4.1 Réseau client-serveur ou Mode de diffusion (serveur dédié))

Dans un réseau à serveur dédié, on distingue le serveur et les stations clientes. Il n'y a pas d'utilisateur sur le serveur dédié. Le serveur dédié a pour seule fonction de servir les autres machines. Le système d'exploitation du serveur doit être multitâches (Unix, Novell Netware, Windows NT). On veille généralement à ce que cette machine soit plus performante notamment aux niveaux des entrées/sorties (bus et périphériques rapides).

Ce type de réseau est très performant et parfaitement adapté aux activités exigeantes en sécurités et à celles qui sont génératrices de transfert de données intensives (beaucoup d'utilisateurs) ou importantes (gros fichiers) à travers le réseau. On l'utilisera pour gérer l'ensemble du système d'information global de l'entreprise.

Pour des petits réseaux, le serveur dédié fait simultanément fonction de serveur de fichiers, de serveur d'impression et de serveur de messagerie.[26]

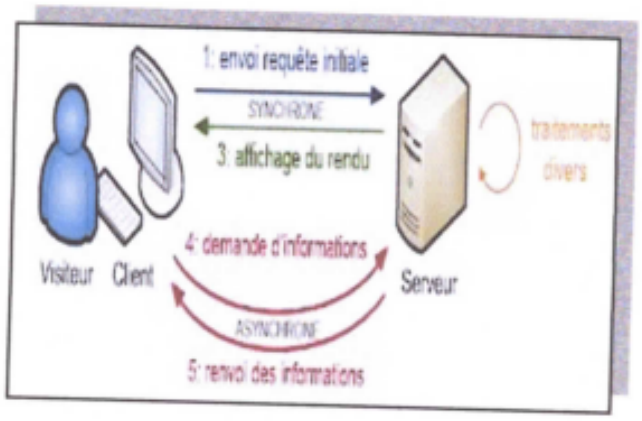


FIGURE 1.1 – Mode de diffusion

- **Avantages :**

– Les systèmes d'exploitation de serveurs proposent des fonctions avancées de sécurité que l'on ne trouve pas sur les réseaux "peer to peer".
– Ils proposent également des fonctions avancées à l'usage des utilisateurs comme par exemple les profils itinérants qui permettent à des utilisateurs (sous certaines conditions) de retrouver leur environnement de travail habituel, même s'ils changent de poste de travail.
– Les serveurs étant toujours en service (sauf en cas de panne...), les ressources sont toujours disponibles pour les utilisateurs.
– Les sauvegardes de données sont centralisées, donc beaucoup plus faciles à mettre en œuvre.
– Il est beaucoup plus complexe qu'un réseau poste à poste et engendre des coûts d'installation, de configuration, d'administration et de maintenance.

- **Inconvénients :**

– La mise en place d'un tel réseau est beaucoup plus lourde qu'un cas simple de " poste à poste ".
– Elle nécessite impérativement la présence d'un administrateur possédant les compétences nécessaires pour faire fonctionner le réseau.
– Si un serveur tombe en panne, ses ressources ne sont plus disponibles. Il faut donc prévoir des solutions plus ou moins complexes, plus ou moins onéreuses, pour assurer un fonctionnement au moins minimum en cas de panne.

1.4.2 Réseau peer to peer

Dans un réseau poste à poste (peer to peer), chaque machine peut fonctionner comme serveur et client. Le système d'exploitation réseau est présent sur toutes les machines ce qui leur permet de mettre à disposition des autres imprimantes ou fichiers de manière horizontale. Bon marché, simples à installer, des produits comme personal NetWare, Lantastic ou Windows

95 rendent moins de services qu'un serveur dédicacé et génèrent un trafic plus intense.[26]

- **Avantages :**

– Il est facile de mettre en réseau des postes qui étaient au départ isolés.
– Chaque utilisateur peut décider de partager l'une de ses ressources avec les autres postes.
– Dans un groupe de travail, l'imprimante peut être partout.
– Cette méthode est pratique et peu couteuse pour créer un réseau domestique.

- **Inconvénients :**

– Chaque utilisateur a la responsabilité du fonctionnement du réseau.
– Les outils de sécurité sont très limités.
– Si un poste c'éteint ou se plante, ses ressources ne sont plus accessibles.
– Le système devient ingérable lorsque le nombre de postes augmente.
– Administration décentralisée et donc parfois incohérente
– Difficulté de gérer la sécurité et les droits d'accès.
– Les postes sont peu nombreux (pas plus d'une dizaine).
– Les utilisateurs restent attachés à un poste dont ils sont responsables.

1.5 Les constituants matériels d'un réseau informatique

Les éléments matériels qui permettent d'interconnecter les ordinateurs dans un réseau, sont les suivants [1] :

1.5.1 La carte réseau

C'est une interface qui permet de connecter un ordinateur au support de transmission utilisé par le réseau. Chaque carte réseau possède une adresse exclusive[7] . Elle sert à identifier la carte réseau lorsque les informations sont envoyées ou reçues au sein du réseau. Une fois installée dans un ordinateur, la carte réseau permet à ce dernier de faire partie d'un réseau.

1.5.2 Transceiver

Il permet d'assurer la transmission des signaux circulant sur le support physique, aussi bien à l'émission qu'a la réception.

1.5.3 Les équipements de transmission

Les équipements de transmission sont des supports (canaux physiques) d'interconnexion, qui relient les ordinateurs entre eux pour construire un réseau. Il sont généralement filaires, de plus en plus non filaires.

Avant d'opter pour un type de support de transmission, afin de créer ou d'étendre un réseau, il convient de prendre en considération un certain nombre de facteur qui sont :

- **Le coût :** le coût du support de transmission influe grandement sur le coût total d'un réseau.

- **L'extensibilité :** il est important qu'un réseau puisse être agrandi pour admettre de nouveaux utilisateurs et matériels.

- **La largeur de bande :** elle correspond à la quantité d'informations qui peut être transférée à l'aide d'un support de transmission. Elle est mesurée en mégabits par seconde (Mbps).

- **La détérioration du signal :** plus le signal parcourt une distance importante, plus il devient faible, car chaque support permet de transmettre des signaux sur une certaine distance.

- **Support physique d'interconnexion :** C'est le support permettant de relier les ordinateurs entre eux. Les principaux supports physiques utilisés dans les réseaux locaux sont les suivants :

– Le câble coaxial : c'est un câble électrique (cuivre) blindé coaxial exp : câbles TV. Malgré de bonnes qualités intrinsèques (faible sensibilité aux perturbations Électromagnétiques), les câbles coaxiaux sont de moins en moins utilisés et laissent de plus en plus la main aux paires torsadées

– La paire torsadée : Les câbles électriques (cuivre) à paires torsadées, ressemblent aux câbles Téléphoniques. Les torsades diminuent la sensibilité aux perturbations Électromagnétiques, la diaphonie (mélange de signaux entre paires) et L'atténuation du signal tout au long du câble. Il existe des versions blindées (STP Shielded Twisted Pair) et non blindées (UTP Unshielded Twisted Pair). Les Câbles à paires torsadées sont actuellement les plus utilisés.

– La fibre optique : Les câbles à fibres optiques transmettent les informations par modulation d'un faisceau lumineux. Ils ont composé d'une fibre d'émission et une fibre de réception.
– Support hertzien (onde électromagnétique) : Les communications par faiscceaux hertziens se font en ligne directe de la tour d'émission à la tour de réception et ont un rayonnement trés directif (line of sight). Ce type de transmission permet le multiplexage de nombreux caneaux de communication autorisant ainsi un trés grand débit de données.

1.5.4 Les outils d'interconnexion

Des équipements spécifiques sont nécessaires pour assurer la communication et l'interconnexion. Ces principaux équipements sont [2] :

- **Répéteur :** C'est un équipement permettant de régénérer le signal entre deux nœuds de réseau, il permet de prolonger facilement un support de transmission existant et d'interconnecter deux segments d'un même réseau.

- **Hub (concentrateur) :** C'est un boitier qui a la fonction de répéteur, mais sa fonction principale est de pouvoir concentrer plusieurs lignes. Il sert d'emplacement central pour relier les ordinateurs et autre périphériques (imprimante, etc.) [7] Le concentrateur dispose d'un certain nombre de ports auxquels viennent se connecter les PC clients. On utilise quelque fois le terme de répéteur multi port car il transfère ou répètent tous les paquets qu'il reçoit à tous ses ports. Les concentrateurs n'effectuent aucun contrôle ou filtrage de données qui les traversent.

- **Pont (bridge) :** C'est un dispositif matériel ou logiciel permettant de relier des réseaux travaillant avec les mêmes protocoles. Il permet aux différentes parties d'un réseau d'échanger et de filtrer des informations, la connexion des réseaux similaires et la création d'inter-réseaux.

- **Switch :** Aussi appelé commutateur, en général, les stations de travail d'un réseau Ethernet sont connectés directement à lui. Un commutateur relie les hôtes qui y sont connectées en lisant leurs l'adresses MAC comprise dans les trames. Intervenant au niveau de la couche 2, il ouvre un circuit virtuel unique entre les noeuds d'origine et de destination, ce qui limite la communication à ces deux ports sans affecter le trafic des autres ports.

- **Routeur :** Aussi appelé commutateur de niveau 3 car il effectue le routage et l'adressage, il permet d'interconnecter deux ou plusieurs réseaux. Possédant les mêmes composants de base qu'un ordinateur, le routeur sélectionne le chemin approprié (au travers de la table de routage) pour diriger les messages vers leurs destinations. Cet équipement est qualifié de fiable car il permet de choisir une autre route en cas de défaillance d'un lien ou d'un routeur sur le trajet qu'empreinte un paquet.

- **Passerelle (gateway) :** Système logiciel et/ou matériel gérant le passage d'un environnement réseau à un autre, en assurant la conversion des données d'un format un autre [3]. La passerelle peut se présenter sous la forme d'un connecteur physique au réseau et être utilisée comme une interface pour transférer les informations entre les différents réseaux. Elle peut également se présenter sous forme d'un logiciel conçu pour permettre à deux protocoles différents d'échanger des informations.

- **Firewall :** Très souvent pour sa mise en place, le firewall nécessite deux composants essentiels : deux routeurs qui filtrent les paquets ou datagrammes et une passerelle d'application qui renforce la sécurité.

  En général le filtrage de paquets est géré dans des tables configurées par l'administrateur ; ces tables contiennent des listes des sources/destinations qui sont verrouillées et les règles de gestion des paquets arrivant et allant vers d'autres machines. Très souvent des machines Unix jouent le rôle de routeur. La passerelle d'application quant à elle intervient pour surveiller chaque message entrant /sortant ; transmettre/rejeter suivant le contenu des champs de l'en-tête, de la taille du message ou de son contenu.

- **MODEM (MOdulateur-DEModulateur) :** Est le périphérique utilisé pour transférer des informations entre plusieurs ordinateurs via les lignes téléphoniques. Le modem

module les informations numériques en ondes analogiques, en sens inverse il retranscrit les données sous forme analogique en données numériques.

1.6 Les réseaux locaux

Un réseau local (ou en anglais LAN, local area network) est une infrastructure de communication qui permet d'interconnecter des équipements informatiques et de partager certaines ressources (de calcul, de stockage, d'impression,. . ...etc.) dans des espaces limitées à quelques centaines de mètres [02].
Voici quelque caractéristiques des réseaux locaux :

- La simplicité de sa configuration ;
- Les adresses sont attribuées aux équipements dès leurs instalations. Ceux-ci peuvent ètre insérés ou retirés, ou encore être inactifs sur le réseau, sans pour autant perturber son fonctionnement ;
- Le coût de câblage intervient pour une part non négligeable dans l'installation du réseau.

1.7 Topologie des réseaux

Il existe deux types de topologie dans les réseaux locaux [15][17], le premier est la topologie de câblage ou topologie physique. Le second est la topologie d'accès ou topologie logique.

1.7.1 La topologie physique

La topologie d'un réseau varie selon la nature de celui-ci.
Théoriquement, il existe 5 topologies différentes.[25]

- **Le réseau maillé :**est caractérisé par le fait que deux nœuds quelconques sont reliés l'un à l'autre. Ce type de réseau permet plus de souplesse et de fiabilité dans son utilisation, mais il est difficilement envisageable pour un grand nombre de nœuds. Généralement, le maillage n'est pas parfait (il y a certains nœuds qui ne sont pas reliés,) on dit alors que c'est un réseau partiellement maillé. Tous les autres types de réseaux sont des sous-ensembles de ce type, obtenus en posant des conditions sur les liens entre les nœuds.

- **Le réseau en étoile :** est un réseau centralisé, un seul nœud est relié directement à tous les autres sans que ceux-ci aient de liens entre eux. Le nœud centrale supporte toute la charge du réseau.

- **Le réseau en arbre** est un réseau hiérarchique réparti sur plusieurs niveaux, les nœuds d'un même niveau n'ont pas de liens entre eux mais sont reliés à un nœud du niveau supérieur. Le réseau téléphonique est exemple caractéristique de ce type de réseau.

- **Le réseau en anneau** : est un réseau ou chaque nœud est relié à deux nœuds. C'est un réseau décentralisé de type point-à-point.

- **Le réseau en bus :**est un réseau où tous les nœuds sont connectés sur le même support. C'est un réseau à diffusion.
  La figure suivante illustre les déffirents topologie physiques.

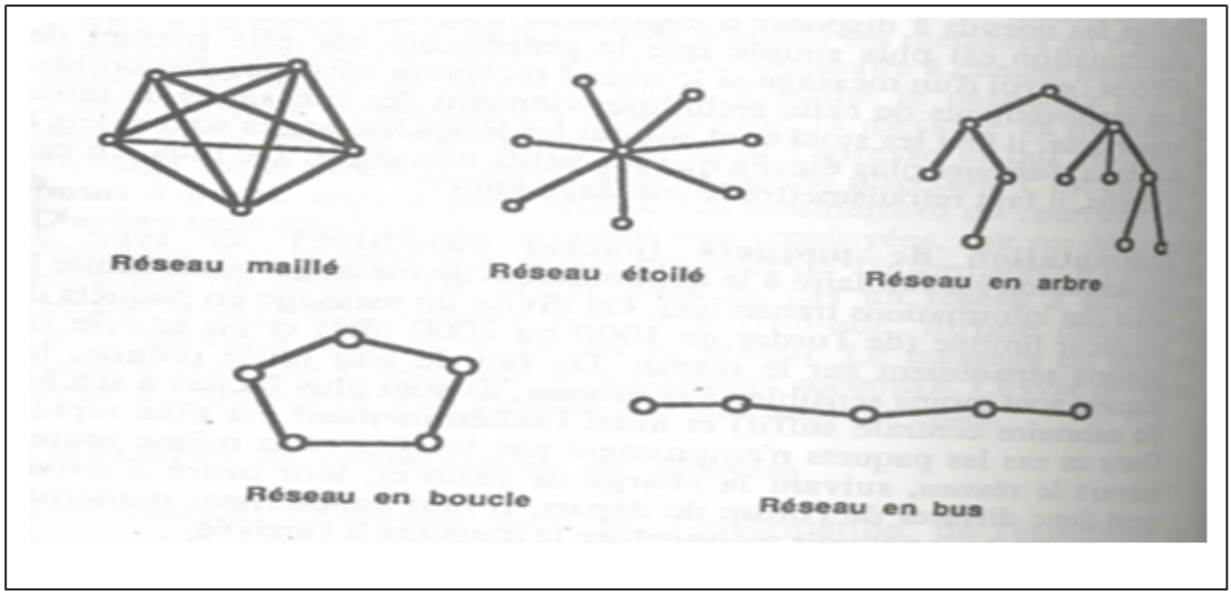


FIGURE 1.2 – Différentes topologies d'un réseau

1.7.2 La topologie logique

Elle correspond à la manière de faire circuler le signal parmi les composantes physiques (on parlera des méthodes d'accès au canal). Par opposition à la topologie logique, représente la façon dont les données transitent dans les lignes de communication. Les topologies logiques les plus courantes sont Ethernet, Token Ring et FDDI.

- **Topologie Ethernet** Ethernet est aujourd'hui l'un des technologies les plus utilisés en local. Il repose sur une topologie physique de type bus linéaire, c'est-à-dire tous les ordinateurs sont reliés à un seul support de transmission. Dans un réseau Ethernet, la communication se fait à l'aide d'un protocole appelé CSMA/CD (Carrier Sense Multiple Access with Collision Detection [01][17], ce qui fait qu'il aura une très grande surveillance des données à transmettre pour detect mais il n'evite pas. Par conséquent un poste qui veut émettre doit vérifier si le canal est libre avant d'émettre.

- **Le Token Ring** Token Ring repose sur une topologie en anneau (ring). Il utilise la méthode d'accès par jeton (token). Dans cette technologie, seul le poste ayant le jeton a le droit de transmettre. Si un poste veut émettre, il doit attendre jusqu'à ce qu'il ait le jeton. Dans un réseau Token Ring, chaque nœud du réseau comprend un MAU (Multi station Access Unit) qui peut recevoir les connexions des postes. Le signal qui circule est régénéré par chaque MAU[17].

Mettre en place un réseau Token Ring coute cher, et la panne d'une station MAU provoque le disfonctionnement du réseau.

- **Le FDDI** La technologie LANFDDI (Fibre Distributed Data Interface) est une technologie d'accès réseau utilisant des câbles fibres optiques. Le FDDI est constitué de deux anneaux : un anneau primaire et anneau secondaire.

  L'anneau secondaire sert à rattraper les erreurs de l'anneau primaire.

  Le FDDI utilise un anneau à jeton qui sert à détecter et à corriger les erreurs. Ce qui fait que si une station MAU tombe en panne, le réseau continuera de fonctionner.

- **L'ATM** L'ATM (asynchronous Transfer Mode, c'est -à -dir mode de transfert asynchrone) est une technologie très récente qu'Ethernet, Token et FDD. Il s'agit d'un protocole de niveau 2, qui a pour objectif de segmenter les données en cellules de taille unique.

  L'en-tête de chaque cellule comprend des informations qui permettent à la cellule d'emprunter son chemin. les cellules ATM son envoyées de manière asynchrone, en fonction des données à transmettre, mais sont insérées dans le flux de données synchrones d'un protocole de niveau inférieur pour leur transport.

1.8 Modèle de référence OSI

Le modèle OSI (Open Systems Interconnection) a été adopté pour faciliter l'échange des données provenant des matériels des différents constructeurs. Ce modèle de référence a été défini en 7 couches qui communiquent entre elles.

Il décrit le fonctionnement d'un réseau à commutation des paquets.
– Nous décrivons ci-dessous le rôle de chaque couche du modèle OSI [04].

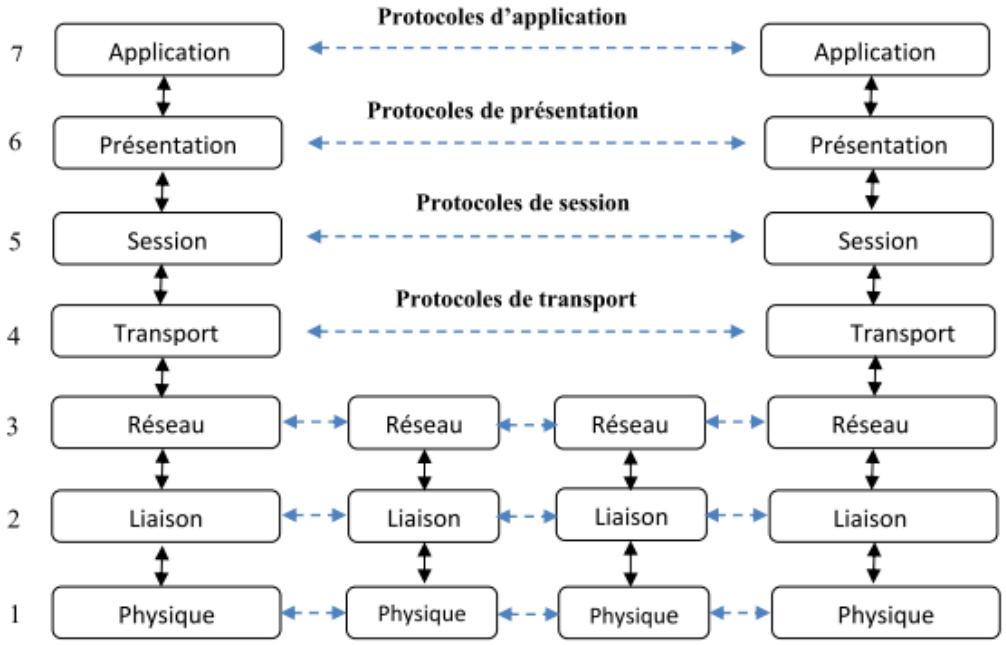


FIGURE 1.3 – L'architecture en couche du modèle OSI

1.8.1 Couche physique

(niveau 1) C'est la couche la plus basse : elle décrit les caractéristiques électriques et les équipements de transmission (câbles, faisceaux, hertziens,...). Elle s'occupe de la connexion physique de la station au réseau et elle définit si la transmission est synchrone ou asynchrone.[25]

1.8.2 Couche liaison de données

(niveau 2) [data link],Elle est appelée aussi couche ligne, elle à pour but la transmission des données sans erreurs. Pour pouvoir détecter et corriger les erreurs, les données sont structurées en trames. En cas d'erreur, les données sont retransmises. Le protocole HDLC [High-level Data Link Control] est un exemple de protocole de ce niveau. En plus du protocole de structuration, les réseaux locaux ont des protocoles particuliers de méthode d'accès tel le CSMA/CD[Carrier Sense Multiple Access with Collision Detection] ou encore, ceux faisant intervenir un jeton [token] ;[25]

- **Le protocole HDLC :** [High-level Data Link Control] il est basé sur le bit (car un caractère peut consister en 6, 7 ou 8 bits)et ainsi toutes les informations sont considérées comme des séquences de bits.

- **CSMA/CD :**[Carrier Sense Multiple Access with Collision Detection], dont la signification est écoute porteuse, accès multiples avec détection de collision, est un protocole de communication qui permet de traiter les collisions occasionnées par l'envoi simultané de plusieurs messages sur le réseau.

1.8.3 Couche réseau

(niveau 3) Elle sert essentiellement à assurer la communication et le routage des paquets de données entre les nœuds du réseau. Elle effectue aussi un contrôle de flux d'informations permettant d'éviter la congestion (trop de paquets à traiter) et en déroutant, si nécessaire, les paquets sur d'autre nœuds.[25]

1.8.4 Couche de transport

(niveau 4) C'est une couche de bout en bout : elle permet l'établissement, le maintien et la rupture de connexions de transport. Selon les fonctionnalités offertes par le réseau (les couches inférieures), c'est elle qui doit fournir les fonctions nécessaires à un service constant. Si les capacités des couches inférieures sont limitées, elle doit y pallier.[25]

1.8.5 Couche session

(niveau 5) Elle permet d'établir une connexion logique entre deux applications. Elle assure l'organisation et la synchronisation du dialogue. C'est à ce niveau que l'on décide du mode de transmission : simplexe, semi-duplex ou duplex ;

1.8.6 Couche présentation

(niveau 6) Elle s'occupe des questions de présentation (la syntaxe) des données. Elle s'occupe des conversions de code de format des données. Elle s'occupe aussi de l'obtimisation en compressant les données en garantissant une certaines sécurité en encryptant les données.

1.8.7 Couche application

(niveau 7) Elle fournit les services et les interfaces de communications aux utilisateurs. Elle constitue donc l'ensemble des points d'entrée dans les programmes utilisateurs.[25]

1.9 Encapsulation des données

Les données sont transférées verticalement d'une couche à une autre (du niveau haut vers le bas) en y rajoutant les informations de protocole (en-tête /en queue). Ces informations peuvent être : identifiant de type de données, le service demandé, le destinataire, l'adresse source,etc.

Les informations de contrôle de protocole (en-tête/en queue) sont supprimées à mesure que les données remontent dans les couches (du niveau bas au niveau haut comme l'illustre la figure ci-dessous.)

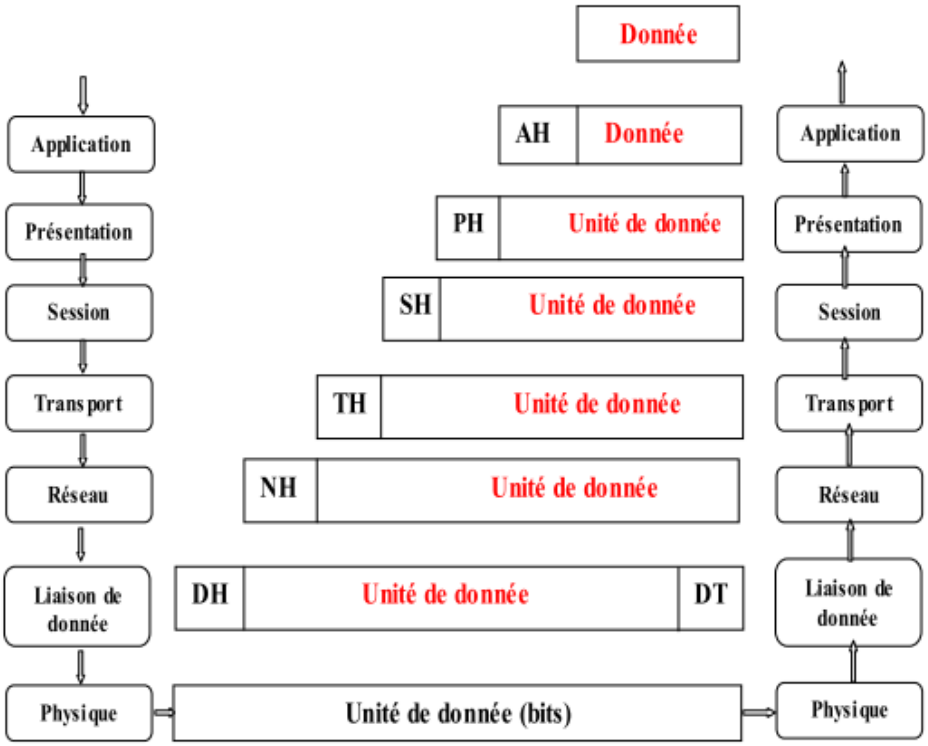


FIGURE 1.4 – Les couches de modèle OSI et l'encapsulation des données

1.10 Le protocole TCP/IP

Le protocole TCP/IP (Transmission Control Protocol/ Internet Protocol) est le protocole le plus utilisé actuellement que ce soit pour des réseaux locaux ou de plus grandes dimensions [06][17].

Il consiste en quatre couche tel que dans chaque couche, le paquet de données change d'aspect, car on lui ajoute un en-tête (encapsulation des données), ainsi les appellations changent suivant les couches :

- Le paquet de données est appelé message au niveau de la couche application ;
- le message est ensuite encapsulé sous forme de segment dans la couche transport.
- le message est donc découpé en morceau avant l'envoi ;
- le segment une fois encapsulé dans la couche Internet prend le nom de datagramme ;
- enfin, on parle de trame au niveau de la couche physique.

1.10.1 Le modèle TCP/IP

La comparaison avec le modèle OSI, on peut ramener l'architecture de communication de données utilisant TCP/IP à un ensemble de quatre couches superposées.

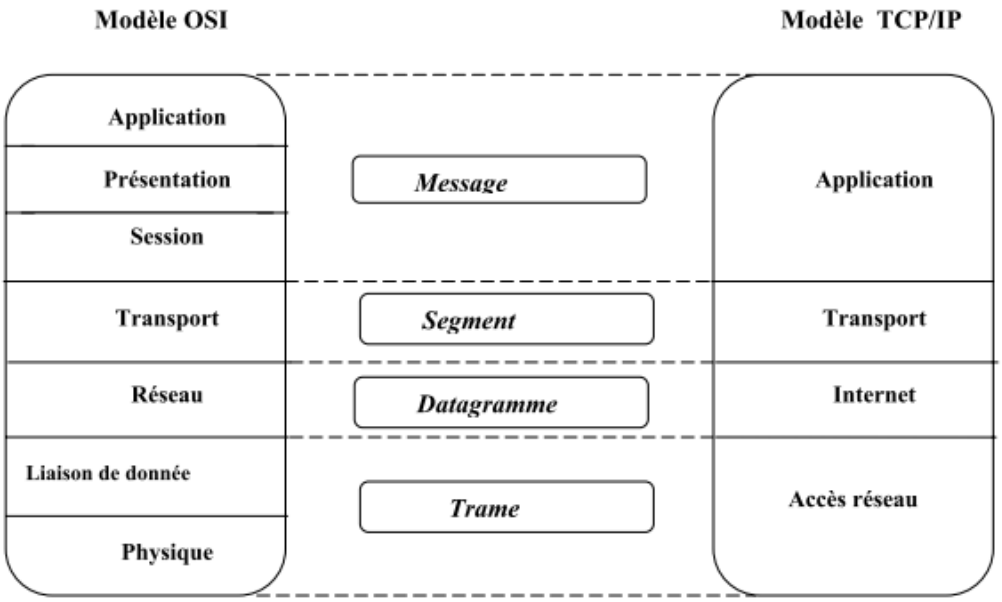


FIGURE 1.5 – l'architecture en couche de modèle TCP/IP

- **Couche1 : Accès réseau :** Cette couche a pour fonction l'encapsulation des datagrammes provenant de la couche IP et la traduction des adresses IP en adresses physiques utilisées sur le réseau. Il Ya donc autant de versions de la couche physique qu'il Ya de type de transport des données.

- **Couche 2 :Internet :** Gère la circulation des paquets à travers le réseau en assurant leur routage.Accès réseau liaisond de donnée. ARP(Adresse Résolution Protocol),

ICMP(Internet Control Message Protocol), IGMP(Internet Group Management Protocol)et RARP(Reverse Adresse Résolution Protocol)[05].

- **Le protocole ARP :** gère les adresses des cartes réseaux. Chaque carte a sa propre adresse d'identification codée sur 48bits.
  Il permet :
  - la resolution d'@IP EN @ MAC.
  - La tenue d'une table de routage.
- **Le protocole ICMP :** gère les informations relatives aux erreurs de transmission. ICMP ne corrige pas les erreurs, mais signale aux autres couches que le message contient des erreurs.

- **Le protocole RARP :** permet à une machine d'obtenir son adresse IP en fonction de son adresse MAC (Medium Access Control) stockée dans une table ARP d'un serveur ou d'une passerelle.

- **Le protocole IGMP :** Le protocole IGMP : est un protocole qui permet à une station de se joindre à un groupe de multicast ou de le quitter.

- **La couche3 : transport** assure tout d'abord une communication de bout en bout en faisant abstraction des machines intermédiaires entre l'émetteur et le destinataire. Elle s'occupe de la régulation du flux de données et assure un transport fiable (données transmises sans erreur et reçus dans l'ordre de leur émission)dans le cas de TCP (Transmission Control Protocol) ou non fiable dans le cas d'UDP (User Datagramme Protocol).

- **Couche 4 : Application :** Elle prend en charge les protocoles d'adressage et d'administration réseau. Elle comporte des protocoles assurant le transfert de fichier, de Courier électronique et de la connexion à distance [06].

- **Le protocole DNS (Domain Name System) :** Ce protocole a été crée afin de permettre la résolution de nom pour les réseaux. Le protocole DNS utilise un ensemble distribué de serveurs pour convertir les noms associés à des adresses IP.

- **Le protocole DHCP (Dynamique Host Configuration Protocol) :** Il permet d'attribuer des adresses IP dynamiquement, c'est-à-dire que l'adresse IP affectée à la machine qui démarre peut changer d'un démarrage à un autre. Ces adresses peuvent être distribuées pour des temps plus ou moins long.

- **Protocole TFTP (Trivial File Transfert Protocole) et FTP (File Transfert Protocole) :** Ces deux protocoles permettent tous les deux de transférer des fichiers d'une machine à une autre. Cependant TFTP bâtit sur UDP alors que FTP utilise TCP [01].

- **Protocole SMTP (Simple Mail Transfert Protocol) :** C'est le protocoles le plus utilisé sur Internet [15]. Il est totalement transparent à l'utilisateur, ce qui le rend convivial, et dispose de clients et de serveurs sur la majorité des architectures. Son but est de permettre le transfert des courriers électroniques par les files d'attentes. Il est

similaire au protocole FTP.

– **Protocole HTTP (Hyper Text Transfer Protocol) :** C'est un protocole TCP/IP conçu uniquement pour la diffusion de documents rédigés en langage HTML (Hyper Text Markup Langage). A l'instar d'autres services d'Internet, il fonctionne selon le modèle Client-serveur.

1.11 L'adressage

1.11.1 L'adressage MAC

L'adresse MAC est une adresse de 48 bits de 12 chiffres hexadécimaux. Cette adresse est un identifiant physique, stockée dans la mémoire de la carte réseau. Elle identifie donc l'interface réseau de la machine.Un format peut apparaitre sous une forme semblable à 00-9A-3C-78-00,00 :055 :9A :3C :78 :00 ou 0005.9A3C.7800.

Tous les périphériques connectés à un réseau local Ethernet présentent des interfaces dotées d'une adresse MAC. La carte réseau se sert de de l'adresse MAC pour déterminer si un message doit être transmis aux couches supérieures à des fins de traitement. L'adresse MAC est codée en permanence dans une puce de mémoire morte sur une carte réseau. Le terme employé pour désigner ce type d'adresse MAC est " "adresse fixe ". Certains constructeurs autorisent la modification (OUI) du numéro d'affectation du constructeur.

1.11.2 L'adresse IP

L'adresse IP est une adresse de 32bits, répartis en 4 fois 8 bits (octets). Cette adresse est un identifiant réseau. On peut ensuite la diviser en 2 parties : réseau et hôte. La première identifie le réseau sur lequel est située la machine et la deuxième identifie la machine elle-même. Pour identifier ces 2 parties, chaque adresse est liée à un masque de sous-réseau. Ce qui permet de définir sur quel réseau elle se trouve.

1. **Les défférentes classes IP**
   Pour différencier entres les tailles de réseau et permettre de mieux identifer des adresses, on a séparé les adresses IP en cinq (5) classes.

   - **Classe A :** Cette classe est destinée pour les très grands réseaux. Seul le premier octet est utilisé pour la partie réseau, ce qui laisse donc 3 octets pour la partie hôte. Ce premier octet est compris entre 1 et 127. Cette classe peut accueillir plusieurs millions d'hôtes.

   - **Classe B :** Cette classe est destinée pour les moyens et grands réseaux. Les 2 premiers octets sont utilisés pour la partie réseau et les 2 suivants pour la partie hôte. Le premier octet est compris entre 128 et 191. Cette classe peut accueillir plusieurs dizaines de milliers d'hôtes.

- **Classe C :** Cette classe est destinée pour les petits réseaux puisqu'elle ne peut accueillir que 254 hôtes. Les 3 premiers octets étant employés pour la partie réseaux, il n'en reste qu'un seul pour la partie hôte. Le premier octet est compris entre 192 et 223.

- **Classe D** C'est une classe utilisée pour le multi-casting. Le premier octet de cette classe est compris entre 224 et 239.

- **Classe E** Cette classe a été définie comme étant une classe pour les ordinateurs de recherches. Le premier octet de cette classe est compris entre 240 et 255.

2. **Sous réseaux**
   un sous réseau est un segment physique d'un environnement TC/IP qui utilise des adresses IP dérivées d'un seul identificateur de réseau. Lorsqu'un réseau est divisé en sous réseaux chaque segment doit utiliser un identificateur de réseau, ou de sous réseaux différent.

   Un identificateur de sous réseau se présente (comme une adresse IP) sous 4 octets séparés par des points (N° réseau, N° sous réseau, N° hôte). Les valeurs du sous réseaux sont obtenues à l'aide des règles suivantes :
   – les chiffres " 1 " dans le masque de sous réseau correspondent à la notion de l'identificateur du réseau et du numéro de sous réseau dans l'dresse IP.
   – Les zéros " 0 " dans le masque de sous réseau correspondent à la position de numéro de l'hôte dans l'adresse IP.
3. **Masque de sous réseau par défaut**
   un masque de sous réseau par défaut est utilisé sur les réseaux TCP/IP qui ne sont pas divisé en sous réseaux. Dans le masque de sous réseau, tous les bits correspondants à l'identificateur réseau sont définies à 1. Tous les bits correspondant à l'identificateur d'hôte sont définis à 0.

Conclusion

Ce chapitre nous a permis de découvrir et de mieux comprendre les notions et les aspects élémentaires des réseaux informatiques à savoir leurs équipements de transmission, leurs outils d'interconnexion, les réseaux locaux, ainsi il nous a permis de différencier entre le modèle OSI qui présente un standard de communications (modèle de reference) entre les ordinateurs d'un réseau et le modèle TCP/IP qui est un ensemble de communication sur internet.
Dans le chapitre qui suit en va parler sur la sécuritée des réseaux informatique.

Chapitre 2

La sécurité d'un réseau informatique

Introduction

Avec l'arrivée de l'internet dans les réseaux , de nombreux problèmes surgissent concernant la sécurité des utilisateurs, également les données de ces utilisateurs. En effet, ouvrir l'organisation vers le monde signifie aussi laisser la porte ouverte aux étrangers pour essayer de pénétrer son réseau local, et y accomplir des comportements malicieux (vol d'informations confidentielles, destruction, etc.). Pour cela la sécurité se place au premier plan pour contrer aux attaques causées par des personnes malveillantes situées à l'intérieur ou à l'extérieur du réseau.

Pour tout problème ayant trait à la sécurité, il faut d'abord comprendre comment fonctionnent ces intrus, avant de pouvoir apporter une solution. Pour cela nous entamerons ce chapitre par une définition et une exposition des objectifs de la sécurité informatique, nous parlerons ensuite brièvement des Vulnérabilités et des menaces qui pèsent sur le réseau, et comment mettre en place une politique de sécurité afin d'élaborer des stratégies (dispositifs) de sécurité, après nous exposerons quelques attaques qui exploitent les faiblesses de réseau informatique, enfin nous bouclerons ce chapitre par une présentation de quelques dispositifs de sécurité tels que les pare-feux, les DZM et les VLANs.

2.1 Définition de la sécurité

Le système d'information est généralement défini par l'ensemble des données et des ressources matérielles et logicielles de l'entreprise permettant de les stocker ou de les faire circuler. Le système d'information représente un patrimoine essentiel de l'entreprise, qu'il convient de protéger.

La sécurité informatique est l'ensemble de moyens mis en œuvre pour minimiser la vulnérabilité d'un système contre des menaces accidentelles (accident dus à l'environnement, les défauts du système) ou intentionnelles (actions malveillantes intentionnelles) [20] dont l'objectif est de garantir :

- **L'intégrité :** Assurer que les informations n'ont pas été altérées par des personnes non autorisées ou inconnues.

- **La disponibilité :** Empêche le démenti (nier) d'engagements ou d'actions précédentes.
- **La non répudiation :** consistant à assurer que seules les personnes autorisées aient accès aux ressources échangées.
- **L'authentification :** D'une information : prouver qu'une information provient de la source annoncée (auteur, émetteur). D'une personne (ou groupe ou organisation), prouver que l'identité est bien celle annoncée.
- **Validation :** les moyens de fournir l'autorisation d'utiliser ou de manipuler des informations.
- **Contrôle d'accès :** Limiter l'accès à des ressources aux personnes privilégiées.
- **Certification :** L'approbation de l'information par une entité de confiance.
- **Réception :** Approuver la réception de l'information.
- **Anonymat :** Cacher l'identité d'une entité impliquée dans un processus.

2.2 Terminologie de la sécurité informatique

2.2.1 Vulnérabilité

C'est une faille ou un point ou le système est susceptible d'être attaqué.

2.2.2 Menaces

Ce sont les violations potentielles de la sécurité. C'est l'ensemble des personnes, choses, événements qui posent danger pour un patrimoine en termes de confidentialité, d'intégrité, et disponibilité.
Il existe deux types de menaces, les menaces accidentelles et les menaces intentionnelles (attaques).

2.2.3 Les contre-mesures

Ce sont des procédures ou techniques permettant de résoudre une vulnérabilité ou de contrer une attaque spécifique.

2.2.4 La politique de sécurité et sa mise en œuvre

L'ors de la configuration d'un réseau local ou étendu, il est important de définir dès le début une politique de sécurité appropriée.

La politique de sécurité est l'ensemble de règles définies et destinées à contrôler les aspects de sécurité comme les droits d'accès et à appliquer des mesures de sécurité destinées à réduire les risques et les dommages, ainsi pour protéger le personnel, préserver la confidentialité, la disponibilité et l'intégrité des biens, des services et des informations et assurer la continuité de fonctionnement du système.

La mise en œuvre d'une politique de sécurité peut se décomposer en quatre étapes [23] :
- L'analyse de la valeur des informations à protéger et l'analyse des risques ;
- L'application de règles et de procédures par les utilisateurs internes de l'organisation (définition d'une politique globale) ;
- Adoption des moyens techniques nécessaires à la réalisation de cette politique (firewall, système de détection d'intrusion,...) ;
- Information, sensibilisation, responsabilisation de chacun.

Avant d'étudier les différentes techniques et outils utilisés pour garantir la sécurité des systèmes informatiques, nous allons d'abord présenter les différents types et techniques d'attaques qui peuvent nuire à ces systèmes.

2.3 Les attaques

Les attaques représentent les moyens d'exploiter une vulnérabilité. Ils s'appuient sur divers types de faiblesses telles que les faiblesses des protocoles, faiblesses d'authentification, faiblesses d'implémentation ou bogues et les mauvaises configurations.

Dans ce qui suit, nous décrivons brièvement la classification des attaques ainsi qu'une description de quelques attaques basées sur ces faiblesses.

Voici un scénario d'intrusion type c'est-à-dire les différentes étapes d'attaques sous forme d'un schéma.

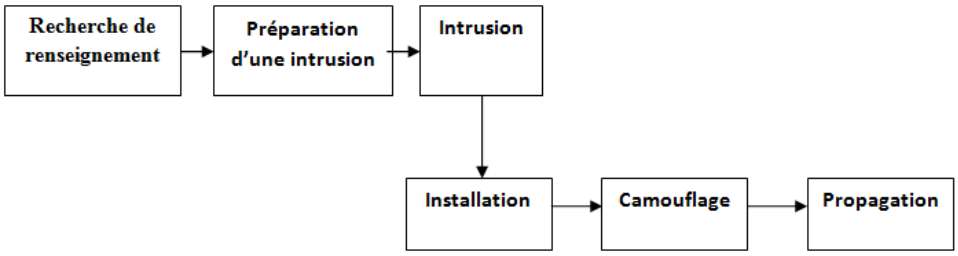


FIGURE 2.1 – Scénario d'intrusion type

2.3.1 Classification des attaques

Les attaques peuvent être classées en deux grandes catégories : Attaques passives et Attaques actives.

- **Attaques passives :** Consistent à écouter et à analyser le trafic échangé sans modifier les données ou le fonctionnement du réseau. Elles sont généralement indétectables mais leur prévention est possible [13].

- **Attaques actives** Les attaques actives concernent celles qui entrainent une modification des données ou création de données incorrectes. Autrement dit, celles qui portent atteinte à l'intégrité, l'authenticité et la disponibilité.

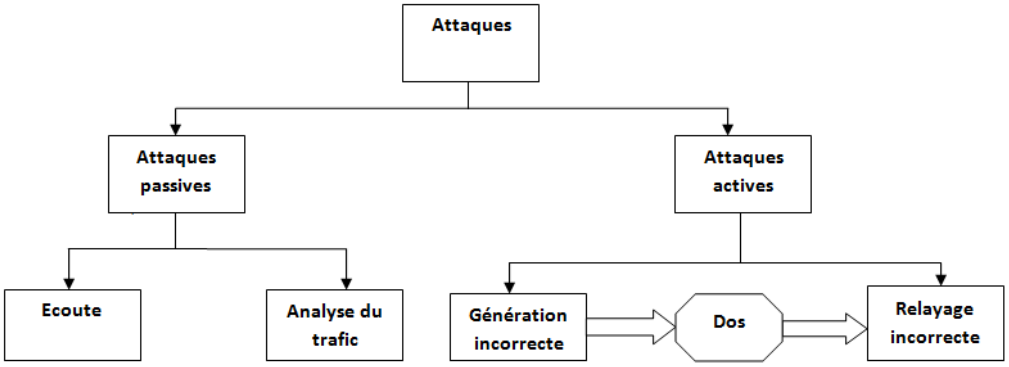


FIGURE 2.2 – Classification des attaques

2.3.2 Description de quelques attaques

Les attaques réseau sont aujourd'hui si nombreuses qu'il serait imaginaire de prétendre les décrire toutes. Elles touchent généralement les trois composantes d'un système : La couche réseau, le système d'exploitation et la couche application. De plus, beaucoup d'attaques peuvent impacter le réseau de manière directe ou indirecte, en voici quelques attaques [7][24].

2.3.2.1 Attaques par déni de service (Dos)

Le déni de service est une attaque qui vise à rendre un service, un système ou un réseau indisponible. Ces attaques se basent généralement soit sur une faiblesse d'implémentation ou bogue, soit, sur une faiblesse d'un protocole.
Il existe plusieurs types de déni de service, on peut citer par exemple le flooding, le smurf ou les DDOS.

1. **Le flooding**
   Cette attaque consiste à envoyer à une machine de nombreux paquets IP de grosse taille. La machine cible ne pourra donc pas traiter tous les paquets et finira par se déconnecter du réseau.
2. **Le smurf**
   Le smurf est une attaque qui s'appuie sur le ping10 (Packet INternet Groper) et les serveurs de broadcaste. On falsifie d'abord son adresse IP pour se faire passer pour la machine cible. On envoie alors un ping sur un serveur de broadcaste. Il le fera suivre à toutes les machines qui sont connectées qui renverront chacune un " pong " au serveur qui fera suivre à la machine cible. Celle-ci sera alors inondée sous les paquets et finira par se déconnecter [20].

2.3.2.2 L'attaque man-in-the-middle

Elle consiste à faire passer les échanges réseaux entre deux systèmes par le biais d'un troisième, sous le contrôle du pirate. Ce dernier peut transformer à sa guise les données à la volée, tout en masquant parfaitement à chaque acteur de l'échange la réalité de son interlocuteur.

2.3.2.3 Attaques permettant d'écouter le trafic réseau (sniffing)

Cette attaque est utilisée pour obtenir des mots de passe en interceptant tous les paquets qui circulent sur un réseau et ceci en configurant l'interface réseau de la station dans un mode spécial, qui permet de recevoir toutes les trames qui circulent sans pour autant en être le destinataire. Il est alors possible de récupérer par exemple les comptes des utilisateurs utilisant FTP ou Telnet8.

2.3.2.4 Le craquage de mots de passe

Le craquage consiste à faire de nombreux essais pour trouver le bon mot de passe.

2.3.2.5 Attaques sur la fragmentation des paquets IP

Elles ont été les premières attaques à passer au travers des éléments de filtrage IP réalisés par les pare-feu. L'attaque consiste à fragmenter sur deux paquets IP une demande de connexion TCP ou d'autres demandes sur machines cibles, tout en traversant et en déjouant par le mécanisme de fragmentation un filtrage IP.

2.4 Stratégies de sécurité

Elles consistent à déployer des moyens visant à sécuriser le système d'information ainsi que de faire appliquer les règles définies dans une politique de sécurité. Plusieurs outils et techniques ont été développés pour remédier à ces différentes attaques.

2.4.1 Pare-feu (firewalls)

La clé pour une bonne sécurité réseau réside dans la mise en place de mécanisme d'isolation entre les différentes composantes de réseau en le structurant en segment, en étudiant plus précisément les trafics qui peuvent être échangés entre ces segments. Pour cela l'outil de base le plus utilisé est le firewall [23].

2.4.1.1 définition d'un firewall (pare-feu)

Un pare-feu est un élément du réseau informatique, logiciel et/ou matériel, qui est aujourd'hui incontournable dans la sécurité de tout système informatique car il permet d'appliquer une politique d'accès aux ressources informatiques. Il a pour principale tâche de contrôler le trafic entre les différentes zones de confiance, en filtrant les flux de données qui y transitent.

Le pare-feu est également intéressant dans le sens ou il constitue un point unique (goulot d'étranglement) ou l'audit et la sécurité peuvent être imposés. Tous les échanges passeront par lui. Il pourra donner des résumés de trafic, des statistiques sur ce trafic, ou encore toutes les connexions entre les réseaux.

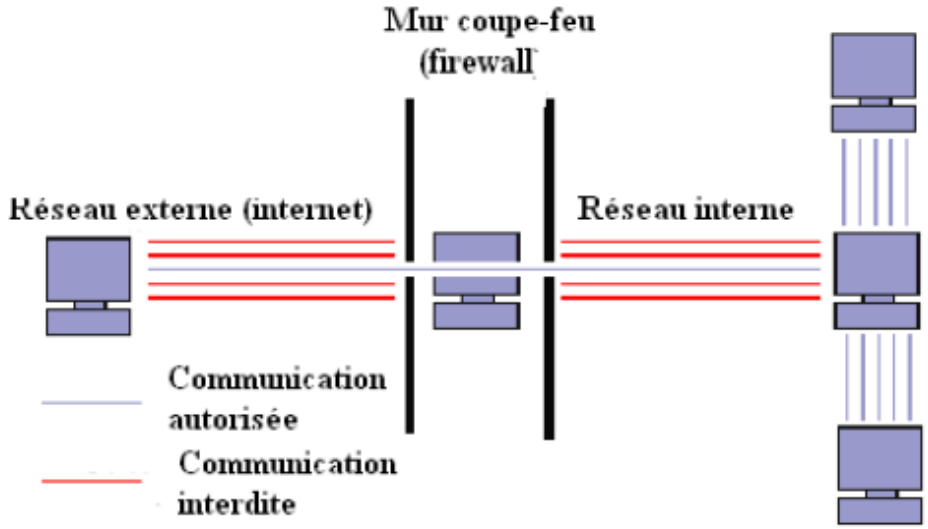


FIGURE 2.3 – Pare-feu (Firewall

2.4.1.2 Principes de fonctionnement d'un pare-feu

Dans ce qui suit nous expliquerons les principes de fonctionnement d'un pare-feu [23].

1. **Le filtrage de paquets (Packet Filtering)**Les paquets sont analysés en les comparant à un ensemble de filtres (c'est-à-dire à un ensemble de règles). Les paquets seront alors soit rejetés. Soit acceptés et transmis au réseau interne. Ce filtrage a lieu sur les couches Réseau (IP) et Transport (TCP/UDP).

   Au niveau de la couche Réseau, le firewall vérifiera 3 informations :
   - L'adresse IP de destination.
   - L'adresse IP de la source.
   - Quelques options présentes à ce niveau.

   Au niveau de la couche Transport. Le firewall analysera d'autres informations telles que :
   - Le port de destination ;
   - Le port de la source ;
   - Le type de protocole utilisé (TCP ou UDP) ;
   - Les flags TCP.

Lorsque les paquets arrivent au firewall, celui-ci analyse les champs IP et TCP/UDP Ils sont confrontés à chacune des règles spécifiées dans la table des autorisations présente dans le firewall, et configurée par l'administrateur du système. Selon les règles qui autorisent ou refusent la transmission des paquets, le firewall obéira aux ordres. Si un paquet ne satisfait à aucune des règles, il est, soit rejeté, soit accepté, suivant la philosophie choisie par l'administrateur réseau :
– Ce qui n'est pas expressément permis est interdit.
– Ce qui n'est pas expressément interdit est permis.
La première de ces deux approches est beaucoup plus sure. La seconde est plus risquée car elle suppose que l'administrateur est certain d'avoir envisagé tous les cas pouvant engendrer des problèmes. L'avantage du filtrage par paquet est sa rapidité. Il est de plus relativement simple à implanter dans un réseau.

2. **La passerelle applicative (Application Gateway) :**A la différence du filtrage de paquets, qui analyse les paquets individuellement, l'application Gateway permet de limiter les commandes à un service plutôt que de l'interdire.

   Ce principe de fonctionnement empêche le trafic direct entre le réseau protégé et l'Internet, et ce dans les deux sens. Le trafic interne n'atteindra jamais Internet, et inversement, aucun trafic Internet ne voyagera sur le réseau interne. En effet, chaque client interne se connectera sur un serveur proxy (qui est la base de ce principe). Toutes les communications se feront par l'intermédiaire de celui-ci. Il déterminera si le service demandé par l'utilisateur est permis et se connectera avec le destinataire en cas de d'autorisation, le destinataire ne connaitra pas l'adresse de son correspondant. Il ne communiquera qu'avec le serveur proxy, qui jouera en réalité le rôle d'un translateur d'adresse réseau (NAT).

   La sécurité est ici très élevée. Agissant au niveau applicatif, on peut notamment la retrouver dans l'authentification par mot de passe des utilisateurs.

3. **Le filtrage de flux :**Le filtrage de flux ne prête pas attention au contenu des paquets transitant sur la connexion. De ce fait ce type de filtrage ne peut être utilisé pour assurer l'authentification des parties, ou la sécurité du protocole par l'intermédiaire duquel a lieu la connexion.

   A la différence du filtrage de paquets, qui est considéré comme permissif, le filtrage de flux est restrictif. En effet, il n'autorisera le flux entre deux entités que si la connexion entre ces deux entités existe. On peut voir ce principe comme la création d'un tunnel entre deux machines. De ce fait, le filtrage de flux ne sera souvent utilisé qu'en complément de l'application Gateway.

2.4.1.3 Limitations d'un pare-feu

Un pare-feu est un composant dédié à la sécurisation du réseau. Il représente une solution aux problèmes de protection de la confidentialité et d'intégrité des ressources sur le réseau et l'authentification du trafic. L'avantage de l'inclure dans une stratégie de sécurité est évident, toute fois un pare-feu s'accompagne des limitations suivantes [8] :

- Un pare-feu ne peut empêcher des utilisateurs ou des attaquants utilisant des modems d'accéder par numérotation à l'extérieur ou à l'intérieur du réseau dans le but de contourner sa protection.
- Un pare-feu ne peut faire respecter une stratégie de mots de passe ni empêcher une mauvaise utilisation de ces derniers. Il est donc important qu'une stratégie expose clairement les comportements acceptables ainsi que les conséquences en cas de non respect des règles.
- Un pare -feu n'est pas efficace contre les risques non technique, tel que l'ingénierie sociale.
- Dans son rôle de porte d'entrée/sortie du réseau, le pare-feu concentre le trafic et la sécurité en un seul point, constituant ainsi un goulet d'étranglement et une source de panne fatale.

2.4.2 Système de détection d'intrusion

Un système de détection d'intrusions (IDS pour Intrusion Detection System) est une composante logicielle qui permet de détecter en temps réel et de façon continue des tentatives d'intrusion en temps réel dans un système informatique ou dans un seul ordinateur, de présenter des alertes à l'administrateur.
Il a pour objectif de détecter toute violation de la politique de sécurité en vigueur sur un système informatique.

Un IDS est un capteur informatique qui écoute de manière furtive le trafic sur un système, vérifie, filtre et repère les activités anormales ou suspectes, ce qui permet ultérieurement de décider de l'action de prévention.
Sur un réseau, l'IDS est souvent réparti dans tous les emplacements stratégiques du réseau.

Il existe deux grandes familles distinctes d'IDS [9]
- Les N-IDS (Network Based Intrusion Detection system), ils assurent la sécurité au niveau du réseau. NIDS est un système capable de contrôler les paquets circulant sur un ou plusieurs liens réseau dans le but de découvrir si un acte malveillant ou anormal a lieu.
- Les H-IDS (Host Based Intrusion Detection system), ils assurent la sécurité au niveau des hôtes. H-IDS réside sur un hôte particulier et la gamme de ces logiciels couvre une grande partie des systèmes d'exploitation tels que Windows, Linux, etc.

2.5 Cryptographie

La cryptographie est une discipline du domaine de la sécurité de l'information et des communications qui permet à travers des primitives mathématiques de fournir un ensemble de services de sécurité telles que la confidentialité, l'intégrité, l'authenticité et la non répudiation. Pour ce faire, des primitives de chiffrement et déchiffrement sont utilisées.
Le chiffrement consiste à transformer les données de telle sorte à ce qu'elles soient pratiquement impossible à lire sans avoir la clé de déchiffrement[18] .

Il existe quatre primitive cryptographique de base qui sont largement répandues et souvent combinées pour sécuriser les communications à travers les réseaux [19] :

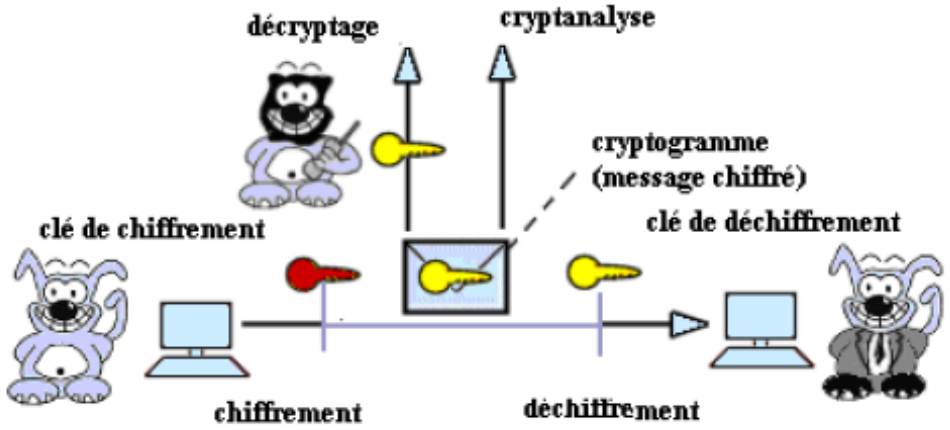


FIGURE 2.4 – Mécanisme de chiffrement

2.5.1 Chiffrement symétrique (à clé secrète)

Le chiffrement symétrique est basé sur une clé partagée entre les deux parties communicantes(Fig.2.5). Cette même clé sert à chiffrer et déchiffré les messages. L'avantage de la Cryptographie symétrique est sa rapidité d'exécution car elle met en œuvre des opérations Simples. Mais, le principal problème est le partage de la clé : comment une clé utilisée pour sécuriser peut être transmise sur un réseau non-sécurisé ? La difficulté engendrée par la génération, le stockage et la transmission des clés limite l'utilisation des clés symétriques Surtout sur Internet. On appelle l'ensemble de ces trois processus la gestion des clés. Les algorithmes informatiques développés pour réaliser des opérations de cryptographie Symétriques sont :

- **DES (Data Encryptions Standard, 1974 :** Inventé par la NSA, encore appelé DEA(ANSI) ou DEA-1 (ISO)) [10] La clé DES est une clé secrète utilisée pour chiffrer à lémission et déchiffrer à la réception. Elle se base sur un algorithme de 56 bits, Travaillant sur des blocs de données de 64 bits à la fois et nécessite 16 étapes D'itérations [11] ;

- **Triple DES ou DES3 (1985) :** L'algorithme Triple DES ou DES3 travaille avec deux Clés de 56 bits et effectue le chiffrement en trois phases. La première phase consiste à Chiffrer les données avec la première clé. La seconde phase effectue un déchiffrement avec la seconde clé. La troisième phase effectue un nouveau chiffrement avec la première clé ;

- **IDEA (International Data Encryptions Algorithme, 1990-1992) ;**
- **AES (Advanced Encryptions Standard, 1997, commercialisation 2001).** Pour résoudre ces problèmes de transmission de clés, les mathématiciens ont inventée le chiffrement asymétrique qui utilise une clé privée et une clé publique.

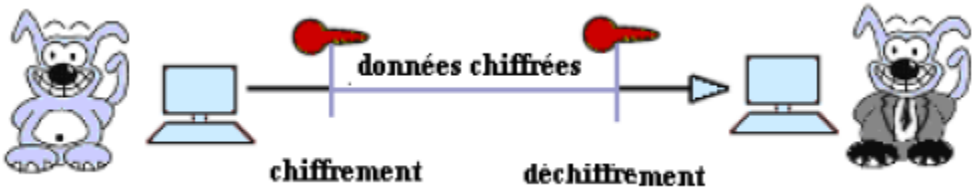


FIGURE 2.5 – chiffrement symétrique

2.5.2 Le chiffrement Asymétrique (clé public)

Ce système de chiffrement utilise deux clés différentes pour chaque utilisateur : une est privée et n'est connue que par l'utilisateur ; l'autre est publique et donc accessible par tout le monde (Fig.2.6).

Les clés publiques et privées sont mathématiquement liées par l'algorithme de chiffrement de telle manière qu'un message chiffré avec une clé publique ne puisse être déchiffré qu'avec la clé privée correspondante [10]. Ce chiffrement présente l'avantage de permettre le placement de signatures numériques dans le message et ainsi permettre l'authentification de l'´emetteur. Le principal avantage de ce chiffrement est de résoudre le problème de l'envoi de clé symétrique sur Un réseau non sécurisé. Bien que plus lent que la plupart des chiffrement de clé Symétrique, Il reste préférable à l'utilisation critique. En pratique il est utilisé pour :

- L'échange d'une clé symétrique ;

- La signature d'un hachage d'un message.

Les trois algorithmes à clé publique suivants sont les plus fréquemment employés :

- **RSA (Rivest-Shamir-Adleman, 1978)** RSA est unique parmi les algorithmes à clé publique utilisés, en ce sens il peut effectuer des opérations de signature Numérique et d'´echange de clés.

- **DSA (Digital Signature Algorithm)** DSA tire sa sécurité de la difficulté du calcul De logarithmes discrets. Cet algorithme peut uniquement être utilisé pour les Opérations de signature numérique (pas pour le cryptage de données).

- **Diffie-Hellman** La sécurité de Diffie-Hellman est liée à la difficulté du calcul des Logarithmes discrets dans un champ fini. L'algorithme de Diffie-Hellman peut uniquement être utilisé pour l'´echange de clés.

Ces algorithmes utilisent des fonctions mathématiques très complexes, par conséquent, ils sont beaucoup plus lents que les algorithmes à clé privée.
- La différence fondamentale entre les clés symétriques et asymétriques provient de leur utilisation :
- La clé symétrique sert à chiffrer des grands volumes de données ;
- La clé asymétrique sert à chiffrer la clé symétrique et à la transporter en sécurité.

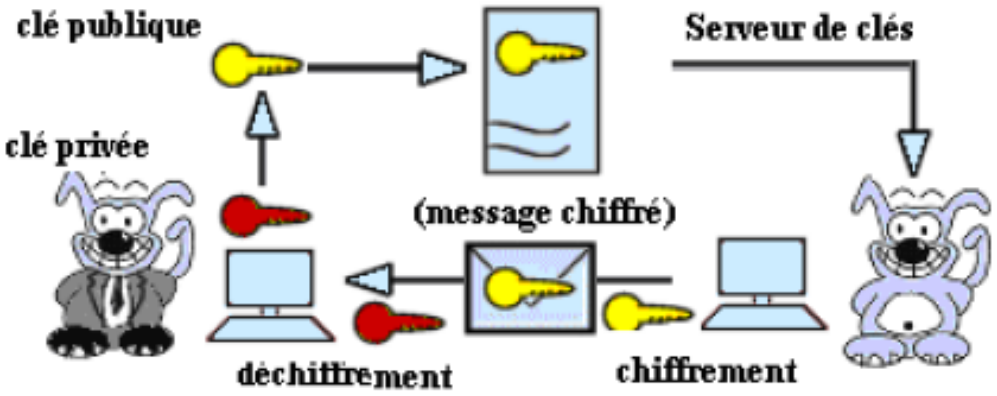


FIGURE 2.6 – Chiffrement asymétrique

2.5.3 Signatures numériques

L'un des avantages majeurs de la cryptographie à clé publique est qu'elle procure une méthode permettant d'utiliser des signatures numériques qui sont des petites portions de Données chiffrées attachées à un message. Les signatures numériques permettent à la personne qui reçoit une information de contrôler l'authenticité de son origine, et également de vérifier que l'information en question est intacte. Ainsi, les signatures numériques des systèmes à clé publique permettent l'authentification, le contrôle d'intégrité des données et la non-répudiation. La méthode de base utilisée pour créer des signatures numériques est : Au lieu de chiffrer l'information en utilisant la clé publique, on chiffre avec la clé privée correspondante. Le déchiffrement sera avec la clé publique.

2.5.4 Fonction de hachage

Une fonction de hachage est une fonction permettant d'obtenir un condensé (haché) d'un texte. La fonction de hachage doit associer un et un seul condensé à un texte en clair. D'autre part, elle doit être une fonction à sens unique, afin qu'il soit impossible de retrouver le message original à partir du condensé. Ainsi, le haché représente en quelque sorte l'empreinte digitale du document. Les fonctions de hachage ne reposent sur aucun secret. Néanmoins, ce sont bien les méthodes de la cryptologie qui permettent de créer de bonnes fonctions de hachage, telles que MD5 et SHA-1, ces deux dernières sont les plus utilisées actuellement [23].

– MD5 (Message Digest 5) produit des hachés de 128 bits en travaillant les données originales par blocs de 512 bits .

– SHA (Secure Hash Algorithm) est comme MD5 fonctionne également à partir de blocs de 512 bits de données et produit par contre des condensés de 160 bits en sortie.

- **DSA (Protocole SSH (Secure Shell) :)** Le cryptage des données circulant sur un réseau public ou privée peut s'effectuer grâce au protocole SSH dans le cas d'un accès à distance.

Le protocole SSH (ou Secure SHell) est un protocole servant à créer une connexion sécurisée entre deux systèmes.

Grâce à SSH, un ordinateur client peut initier une connexion avec un ordinateur serveur et profiter des mesures de sécurité suivantes :

- Après avoir effectué une connexion initiale, le client peut s'assurer de se connecter au même serveur lors des sessions suivantes.

- Le client peut transmettre ses données d'authentification au serveur, telles que son nom d'utilisateur et son mot de passe, en format crypté.

- Toutes les données envoyées et reçues pendant la connexion sont transférées de façon chiffrée, ce qui les rend extrêmement difficiles à déchiffrer et à lire.

2.6 La technologie AAA

Nous vivons dans un monde ou presque tout doit être protégé. Que vous sommes administrateur système, responsable, ingénieur réseau ou étudiant. Lorsque nous accédons à un réseau, nous sommes toujours confrontés aux trois aspects : Authentification,Autorisation, trazabilité [08]

2.6.1 Authentification

il s'agit de la vérification de l'identité d'un utilisateur, elle est généralement assurée au moyen d'un secret partagé ou d'un logiciel approuvé (protocole RADIUS).

2.6.2 Autorisation

Elle intervient à l'issue de l'authentification. Une fois l'utilisateur authentifié, il faut s'assurer qu'il est autorisé à accomplir les actions qu'il demande, tels que l'accès à des fichiers, le droit d'écrire, etc. L'autorisation est gérée au moyen de liste ACL ou des stratégies.

2.6.3 Trazabilité

Elle permet de collecter des informations sur les utilisateurs et les actions qu'ils accomplissent lorsqu'ils sont connectés aux équipements du réseau.

2.7 Les VPN (Virtual Private Network)

Les réseaux privés virtuels permettent à l'utilisateur de créer un chemin virtuel sécurisé entre une source et une destination. Grace à un principe de tunnel (tunneling) dont chaque extrémité est identifiée, les données transitent après avoir été éventuellement chiffrées [22].

Un des grands intérêts des VPN est de réaliser des réseaux privés à moindre côut. En chiffrant les données, tout se passe exactement comme si la connexion se faisait en dehors d'Internet. Il faut par contre tenir compte de la toile, dans le sens où aucune qualité de service n'est garantie [12].

2.7.1 Principe de fonctionnement des VPN

Le principe du VPN est basé sur la technique du tunneling. Cela consiste à construire un chemin virtuel après avoir identifié l'émetteur et le destinataire. La source peut ensuite éventuellement chiffrer les données et les achemine en empruntant ce chemin virtuel.

Les données à transmettre peuvent appartenir à un protocole différent d'IP. Dans ce cas le protocole de tunneling encapsule les données en rajoutant un entête. Permettant le routage des trames dans le tunnel. Le tunneling est l'ensemble des processus d'encapsulation, de transmission et de désencapsulation.

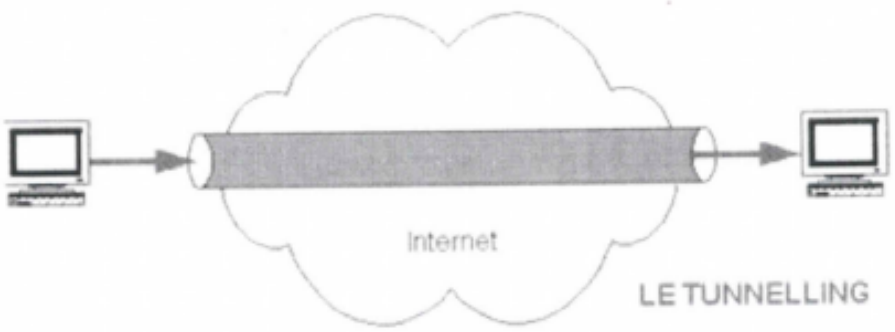


FIGURE 2.7 – Mode de fonctionnement d'un tunnel IP

2.7.2 Interét d'un VPN

Auparavant pour interconnecter deux LANs distants il n'y avait que deux solutions, soit les deux sites distants étaient reliés par une ligne spécialisée permettant de réaliser un WAN entre les deux sites soient les deux réseaux communiquaient par le RTC.

Une des premières applications des VPN est de permettre à un hôte distant d'accéder à l'intranet de son entreprise ou à celui d'un client grâce à Internet tout en garantissant la sécurité des échanges. Il utilise la connexion avec son fournisseur d'accès pour se connecter à Internet et grâce aux VPN, il crée un réseau privé virtuel entre l'appelant et le serveur de VPN

de l'entreprise. Les VPN peuvent également être utilisé à l'intérieur même de l'entreprise, sur l'intranet, pour l'échange de données confidentielles.

2.7.3 Services des VPN

Ces VPN n'ont pas comme seul intérêt l'extension des WAN à moindre cout mais aussi l'utilisation de services ou fonctions spécifiques assurant la Qos et la sécurité des échanges. Les fonctionnalités de sécurité sont matures mais par contre la réservation de bandes passantes pour les tunnels est encore un service en développement limité par le concept même d'Internet [22].

2.7.4 Les différents protocoles utilisés pour l'établissement d'un VPN

Pour qu'un tunnel soit établie entre deux sites distants, il faut que ces deux derniers utilisent le même protocole de tunnelling (ou protocoles d'encapsulation) comme IPSec (Internet Protocol Security), PPTP(Point To Point Tunneling Protocol) ou L2TP(Layer 2 Tunneling Protocol). Récemment, un nouveau type de VPN basé sur SSL (Secure Socket Layer) a été émergé comme principale solution pour l'accès à distance [14][19].

1. **Les protocoles PPTP et L2TP :** Ils opèrent au niveau de la couche liaison des données (couche2)
2. **Le protocole IPsec :**
   IPSec est le standard actuel défini par l'IETF permettant de sécuriser les échanges au niveau de la couche réseau (niveau 3) [14]. Il s'agit en fait d'un protocole apportant des améliorations au niveau de la sécurité au protocole IP en encapsulant les paquets IP dans un en-tête additionnel avant de les transmettre à travers le réseau, afin de garantir la confidentialité, l'intégrité et l'authentification des échanges [14].
3. **Le protocole SSL :**
   SSL est le protocole de sécurité de la couche session du modèle OSI (niveau 5). Il emploie une cle publique pour chiffrer les données qui sont transférées à travers une connexion SSL.

2.8 Les VLANs (Virtual local Area Network)

Le développement rapide d'Internet a mené de nombreuses Enterprises à étendre leurs installations informatiques. La technologie VLAN apporte des solutions nouvelles dans la segmentation et la sécurisation des réseaux locaux, tout en augmentant leurs performances. Par définition un VLAN ou réseau virtuel est un regroupement de postes de travail indépendamment de la localisation géographique sur le réseau. Ces stations pourront communiquer comme si elle étaient sur le même segment.

Un VLAN est assimilable à un domaine de diffusion (Broadcast Domain). Ceci signifie que les messages de diffusion émis par une station d'un VLAN ne sont reçus que par les stations de ce VLAN [16]. Ces derniers n'ont été réalisables qu'avec l'apparition des commutateurs (Switches).

Il existe différents cas où l'utilisation des VLANs est importante par exemple :

1. **Sécurité :**
   Pour séparer des systèmes sensibles ou hébergeant de données sensibles, du reste du réseau. Ainsi, ces systèmes seront protégés des écoutes passives sur le réseau qui est notre objectif pour l'étude des VLANs.
2. **Projets/Applications spécifiques :**
   Un projet ou une application peut nécessiter de travailler sur un réseau spécialisé, où certains noeuds doivent communiquer entre eux, et d'autres non. Avec les VLANs, il est possible de ré-architecturer le réseau au niveau logique, sans toucher au réseau physique.
3. **Performance/Bande-passante :**
   En délimitant les domaines de broadcasts, et en ré-architecturant le réseau logique, on peut gérer de façon plus fine la bande-passante allouée aux utilisateurs, et donc améliorer les performances.
4. **Profil des utilisateurs différents :**
   Dans une entreprise où cohabitent des utilisateurs gourmands en bande passante (ingénierie, multimédia) et des utilisateurs ayant une consommation plus modeste (managers, commerciaux), la mise en place de VLAN va permettre de répartir les ressources aux différents utilisateurs/services, et les séparer pour que les services consommant beaucoup de bande-passante ne viennent pas empiéter sur le réseau des autres services de l'entreprise, et inversement

2.8.1 Typologie des VLANs

Les VLANs différent selon les informations utillisées pour regrouper les stations. Il en existe trois modèles [20].

2.8.1.1 VLANs par port (VLANs de niveau 1)

Les VLANs de niveau1, aussi appelé VLANs par port (Port-Based VLANs) définit un réseau virtuel en fonction des ports de raccordement sur le commutateur. On peut donc regrouper les systèmes en fonction des ports sur lesquels ils sont connectés.

2.8.1.2 VLANs par adresse IEEE (VLANs de niveau 2)

Les VLANs de niveau 2, également appelés VLANs MAC- VLANs par adresse IEEE (MAC adress-Based VLANs). Ils associent les stations de travail à laide de leurs adresses qui sont introduites par l'administrateur. Ce dernier indique au commutateur que telle adresse MAC appartiendra à tel numéro de groupe.

2.8.1.3 VLANs par sous réseau

Les VLANs par sous réseau. Ils associent des sous réseaux IP par masque ou adresse. Les utilisateurs sont affectés dynamiquement à un ou plusieurs VLANs.

2.9 Le protocole VTP

Le VLAN Trunking Protocol (VTP) est nécessaire si l'on veut étendre une configuration de VLAN sur plusieurs commutateurs [24]. VTP est un protocole servant à maintenir la base de données de VLANs sur plusieurs commutateurs. Il est basé sur la norme 802.1Q et exploite une architecture client-serveur avec la possibilité d'instancier plusieurs serveurs.

Il existe deux éléments nécessaires pour un bon fonctionnement du VTP :

- **Définir un nom de domaine VTP** (appelé aussi domaine de gestion). Ne participent à cette gestion que les commutateurs qui appartiennent à un même domaine.
- **Définir pour chaque commutateur un rôle :** soit client, soit transparent, soit, un seul d'entre eux, serveur

1. **Mode serveur :** Il est utilisé lorsque le commutateur introduit de nouveaux VLANs destinés à être publiés vers les autres clients. Il sera le seul autorisé à créer, modifier ou effacer des VLANs.

2. **Mode client :** Utilisé lorsque le commutateur n'introduit pas de nouveau VLAN. Le nombre de configurations manuelles se réduit. Ce mode subit toutes les opérations de modification de VLANs à partir du serveur VTP du même domaine.

3. **Mode transparent :** Permet de configurer manuellement les VLAN sans les publier vers les autres commutateurs. Son objectif c'est d'assurer la connectivité VTP du serveur vers les clients, c'est-à-dire le commutateur reçoit les mises à jour du serveur VTP et les transmet à ses voisins sans les prendre en compte, et il peut aussi créer, modifier ou supprimer ses propres VLANs mais il ne les transmet pas.

2.10 Zones démilitarisée

Si une entreprise doit héberger elle- même un site web public complet avec des serveurs tel qu'un serveur de messagerie, elle pourra envisager l'emploi d'un pare-feu avec deux interface (interne et externe) et lui laisser la tache de créer les règles de traduction qui dirigent le trafic en entrée vers les serveurs appropriés au réseau d'entreprise. Cela peut s'avérer désastreux si un pirate a des vues sur ce réseau. D'où l'idée de recourir à une DMZ (DeMilitarized Zone).

Une DMZ est une interface située entre un réseau connu (réseau interne) et un réseau externe (internet). Une série de règles de connexion configurée sur le pare-feu font de cette interface une zone physiquement isolée entre les deux réseaux. Cette séparation physique permet d'autoriser les accès internet à destination des serveurs placés dans la DMZ et non à ceux destinés au réseau privé (interne).

Le principal avantage de cette configuration est le confinement de toutes les requêtes inconnues au niveau de la DMZ. Cela évite de les recevoir sur le réseau interne, avec tous les risques que cela comporte.

2.11 Listes de contrôle d'accès

Une liste de contrôle d'accès est une collection d'instructions permettant d'autoriser ou de refuser des paquets en fonction d'un certain nombre de critères, tels que :

- L'adresse d'origine
- L'adresse de destination
- Le numéro de port.
- Les protocoles de couches supérieures

Les listes de contrôle d'accès permettent à un administrateur de gérer le trafic et d'analyser des paquets particuliers. Elles sont associées à une interface du routeur, et tout trafic acheminé par cette interface est vérifié afin d'y déceler certaines conditions faisant partie de la liste de contrôle d'accès.

Les ACL peuvent être créés pour tous les protocoles routés. Il faut donc définir une liste de contrôle d'accès dans le cas de chaque protocole activé dans une interface pour contrôler le flux de trafic acheminé par cette interface.

2.11.1 Fonctionnement des listes de contrôle d'accès

Les listes de contrôle d'accès sont configurés pour les appliquer au trafic entrant ou sortant. Elles fonctionnent dans un ordre séquentiel et évaluent les paquets en les validant par rapport à la liste de contrôle d'accès, de haut en bas, une instruction après l'autre.

1. **Listes de contrôle d'accès entrantes**
   les paquets entrants sont traités avant d'être routés vers l'interface de sortie. Une liste de contrôle d'accès entrante est efficace car elle réduit la charge des recherches de routage en cas d'abandon du paquet. Si le paquet est autorisé à l'issue des tests, il est soumis au routage. La figure (Fig2.8) montre la logique d'une liste de contrôle d'accès entrante. Une instruction de refus implicite finale s'applique à tous les paquets qui n'ont pas répondu aux conditions. Elle est souvent appelée instruction implicite " deny any " ou " deny all traffic ".

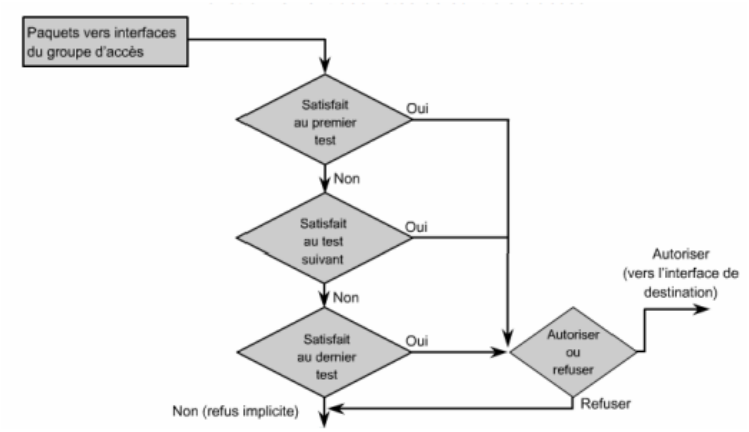


FIGURE 2.8 – Fonctionnement d'une ACL entrante

2. **Listes de contrôle d'accès sortantes :** les paquets entrants sont routés vers l'interface de sortie puis traités par le biais de la liste de contrôle d'accès sortante. La figure (Fig.2.9) illustre la logique d'une liste de contrôle d'accès sortante. Avant l'acheminement d'un paquet vers une interface de sortie, le routeur vérifie la table de routage pour voir si le paquet est routable. Si le paquet n'est pas routable, il est abandonné. Le routeur vérifie ensuite si l'interface de sortie est associée à une liste de contrôle d'accès. Si l'interface de sortie n'est pas associée à une liste de contrôle d'accès sortante, le paquet peut être envoyé à la mémoire tampon de sortie.

   Pour les listes sortantes, " autoriser " signifie envoyer le paquet à la mémoire tampon de sortie, alors que " refuser " signifie abandonner le paquet.

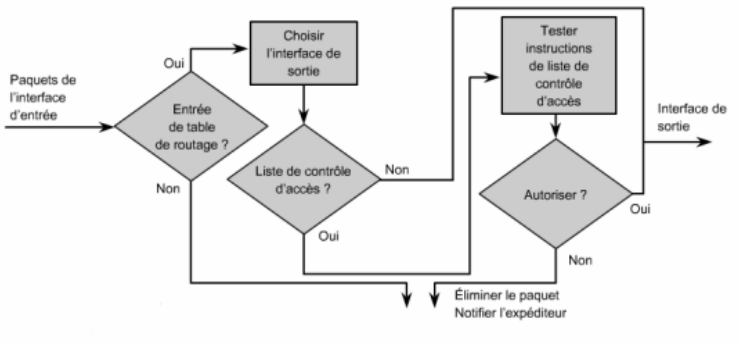


FIGURE 2.9 – Fonctionnement d'une ACL sortantes

2.11.2 Types de liste de contrôle d'accès

1. **Listes de contrôle d'accès standards :** Les listes de contrôle d'accès standard permettent d'autoriser et de refuser le trafic en provenance d'adresses IP source. La destination du paquet et les ports concernés n'ont aucune incidence.

2. **Listes de contrôle d'accès étendues :** lLes listes de contrôle d'accès étendues filtrent les paquets IP en fonction de plusieurs attributs, dont le type de protocole, l'adresse IP source, l'adresse IP de destination, les ports TCP ou UDP source, les ports TCP ou UDP de destination, et les informations facultatives sur le type de protocole pour une meilleure précision du contrôle.

Conclusion

Nous avons vu à travers ce chapitre l'impacte de la sécurité informatique sur les réseaux, la sécurité doit être mise au premier plan. Afin de garantir une meilleure sécurisation, on doit d'abord identifier les vulnérabilités des systèmes pour pouvoir contrer aux différents types d'attaques. Pour cela des outils et des techniques de sécurisation sont mis en place. Comme nous avons vu dans ce chapitre les pare-feux et les VPNs qui sont utilisés pour la sécurité des réseaux mais sans garantir l'intégrité et la confidentialité des données qui sont par contre obtenues par d'autres moyens qui sont la cryptographie.
Dans le chapitre qui suit on va parler sur le réseaux de SONATRACH.

Chapitre 3

Etude de l'existant et proposition

Introduction

Avant de se lancer dans la configuration du réseau Intranet de la SONATRACH, nous allons présenter :

- L'architecture du réseau et sa structure hiérarchique

- Les équipements intermédiaires

Pour étudier ensuite les failles de cette architecture en termes de sécurité afin de proposer une nouvelle configuration sécurisée.

3.1 Présentation du réseau SONATRACH

Le réseau de SONATRACH est un réseau MAN constitué d'une liaison de deux sous réseaux LAN, L'architecture du réseau étudiée est basée sur une topologie en anneaux pour le noyau la ou la connexion est plus dense, et une topologie en étoile pour ses alentours.

Le serveur se trouve dans l'un des bâtiments du noyau, un répartiteur général de type Switch Cisco Catalyst 6509 est mis en place avec le serveur et il est relié à trois répétiteurs Switch Cisco Catalyst 6509 pour former le noyau.

La connexion est ainsi transmise du noyau vers d'autre Switch c2950 aux Alentours du noyau, si le routage est nécessaire on reliera le Switch c2950 avec un Switch 3550 qui permettra le routage.

Pour le nouveau bâtiment, ils ont assemblé deux répétiteur Switch catalyst c6509, qui sont relies à des Switch catalyst c3750 pour chaque étage, l'avantage de installation de ces deux Switch est que si l'un d'eux tombe en panne ou se bloque l'autre le remplace instantanément jusqu'à ce que le principal se remet en marche ou se répare.

Un protocole de routage HSRP (qui est définie ci-dessous) est monté entre les deux équipements catalyst Cisco 6500 pour le département(INFC6500) et un catalyst Cisco 6500 pour le département de maintenance (MNT 6509) afin d'assurer une tolérance au pannes.

Pour la diffusion de ses données dans son réseau, SONATRACH utilise le mode client/serveur.

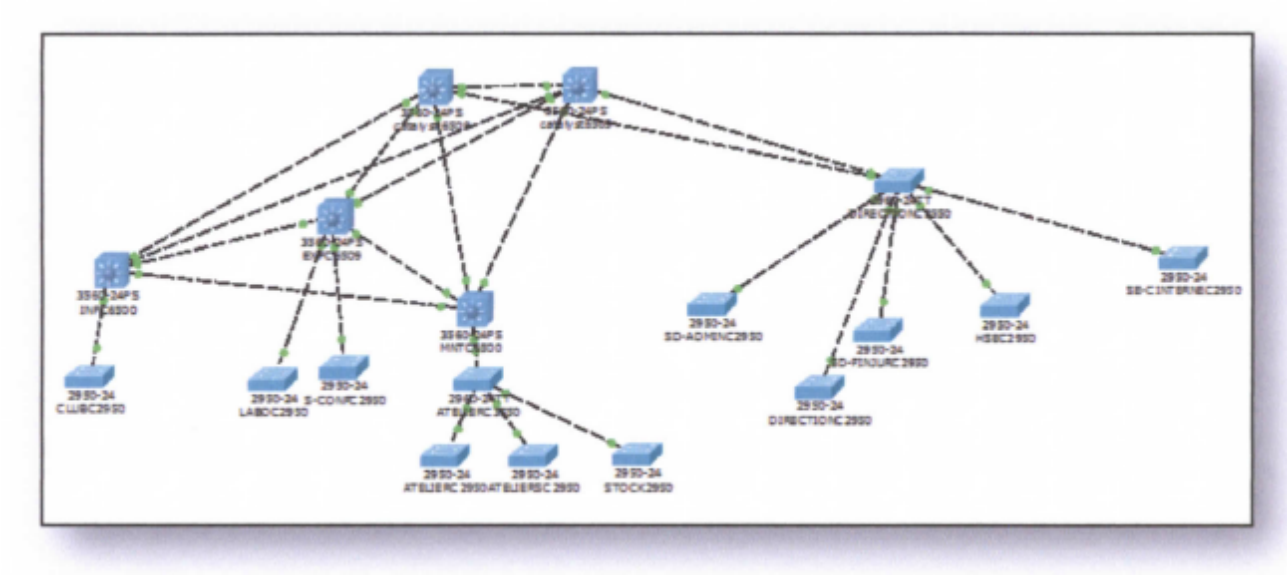


FIGURE 3.1 – Présentation d'une architecture de réseau SONATRACH

3.2 Data center

Le data center d'une entreprise est un centre de traitement de données se présentant comme un lieu ou se trouvent différents équipements.

3.2.1 Composants de data center

3.2.1.1 La définition des équipements réseau

1. **Les serveurs**

- **Serveur de fichier :** Un serveur de fichier permet de partager des données à travers un réseau. Le terme désigne souvent l'ordinateur (serveur) hébergeant le service applicatif. Les utilisateurs peuvent ensuite les récupérer au moyen d'un protocole de partage de fichier.

On utilise généralement l'un des quatre protocoles suivant :

– FTP (File Transfer Protocol)
– CIFS (Common Internet File System) anciennement nommé SMB (Serveur Massage Block)
– NFS (Network File System)
– NCP (Network Core Protocol) est un protocole réseau intégré à PPP pour négocier les options concernant la couche 3 du réseau

- **Serveur de bases de données :** ce sont 2 serveurs sous UNIX liés en redondance et qui gardent toutes les informations nécessaires sur les utilisateurs.

- **Serveur LMS :** c'est un serveur qui s'occupe de la détection de l'emplacement des Switch au niveau de l'entreprise.

2. **Les Switch**

- **Définition de la gamme Catalyst Cisco6509 :** Catalyst 6509 Enhanced Vertical Switch (6509-VE) offre des moyens pour soutenir la capitalist et de la bande passante de système (80Gbit/s par emplacement) jusqu'à 1440 Gb/s et des capacités améliorées de gestion des câbles.

- **Caractéristiques de la gamme Catalyst Cisco 6509 :**La gamme Cisco Catalyst 6509 suporte tous les modules Cisco Catalyst 6500 Séries, y compris :

– Tous les moteurs Supervisor 720 et 32.
– Gigabit Ethernet modules (Modules 10 Gigabit Ethernet)
– 10/100/1000 Ethernet modules (avec option poE IEEE 802.3af)
– Flex WAN MODULES.
– Adaptateurs port commun / processeurs d'interface SPA.
– Service multi-Gigabit modules (Application Control Engine, pare-feu, détection d'intrusion, la sécurité IP [IPsec].

FIGURE 3.2 – La gamme catalyst cisco 6509

- **Définition de la gamme Catalyst Cisco 3750 :**La gamme Cisco Catalyst 3750 est une ligne de commutateurs innovants qui améliorent l'efficacité de l'exploitation des réseaux locaux grâce à leur simplicité d'utilisation et leur résilience la plus élevée disponibles pour des commutateurs empilables. Cette gamme de produits dispose de la technologie Cisco StackWiseTM, interconnectant les commutateurs au sein d'une même pile à 32 Gbps qui permet de construire un système unique de commutation à haute disponibilité, vu comme un simple commutateur virtuel. Catalyst 2960, nouvelle famille de périphériques.

- **Caractéristiques de la gamme Catalyst Cisco 3750 :** La gamme Cisco Catalyst 3750 est disponible dans la version logicielle SMI, commutateur principal met automatiquement à jour toutes les tables de routage pour appliquer les modifications.
  Les mises à niveau sont appliquées universellement et simultanément à tous les les membres de la pile.

FIGURE 3.3 – La gamme Catalyst Cisco 3750

- **Définition de la gamme Catalyst Cisco 3550 :**Le Cisco Catalyst 3550 Séries Switch est un empilable ; commutateur multicouche qui offre une haute disponibilité, la qualité de service (Qos), et la sécurité pour améliorer les opérations du réseau.

- **Caractéristiques de la gamme Catalyst Cisco 3550 :**

– Commutateurs Ethernet 10/100 basiques et intelligents à configuration fixe.
– Commutateurs administrables de 12.24 ou 48 ports 10/100/1000 BaseT
– Liaisons ascendantes : 1000 Base T fixes, 1000 Base SX GBIC

FIGURE 3.4 – La gamme Catalyst Cisco 3550

- **Définition de la gamme Catalyst 2950 :**Nouvelle famille de périphériques autonomes à configuration fixe, apportent aux postes de travail une connectivité Fast Ethernet et Gigabit Ethernet optimisent les services de LAN sur les réseaux d'entreprise d'entrée de gamme, intermédiaires et les réseaux de succursale. La gamme Catalyst 2960 offre une sécurité intégrée avec contrôle de l'admission sur le réseau (NAC), qualité de service (QoS) évoluée et résilience, pour distribuer des services intelligents à la périphérie du réseau.
- **Caractéristiques de la gamme Cisco Catalyst 2950 :**

– Fonctionnalités intelligentes à la périphérie du réseau, par exemple des listes de contrôle d'accès (ACL) élaborées et une sécurité optimisée
– Contrôle du réseau et optimisation de la bande passant grâce aux fonctions de qualité de service évoluée, de limitation granulaire du débit, de listes de contrôle d'accès et de services multicast.
– Sécurité du réseau assurée par une série de méthodes d'authentification, des technologies de cryptage des données et le contrôle des admissions sur le réseau basé sur les utilisateurs, les ports et les adresses MAC.
– Configuration automatique des applications spécialisées à l'aide de Smart ports.

FIGURE 3.5 – La gamme Catalyst Cisco 2950

3. **Les routeurs**
   Elle possède deux routeurs l'un pour le WAN et l'autre pour l'internet.

Ci-dessous une figure qui nous montre le matérièls utilisés par SONOTRACH.

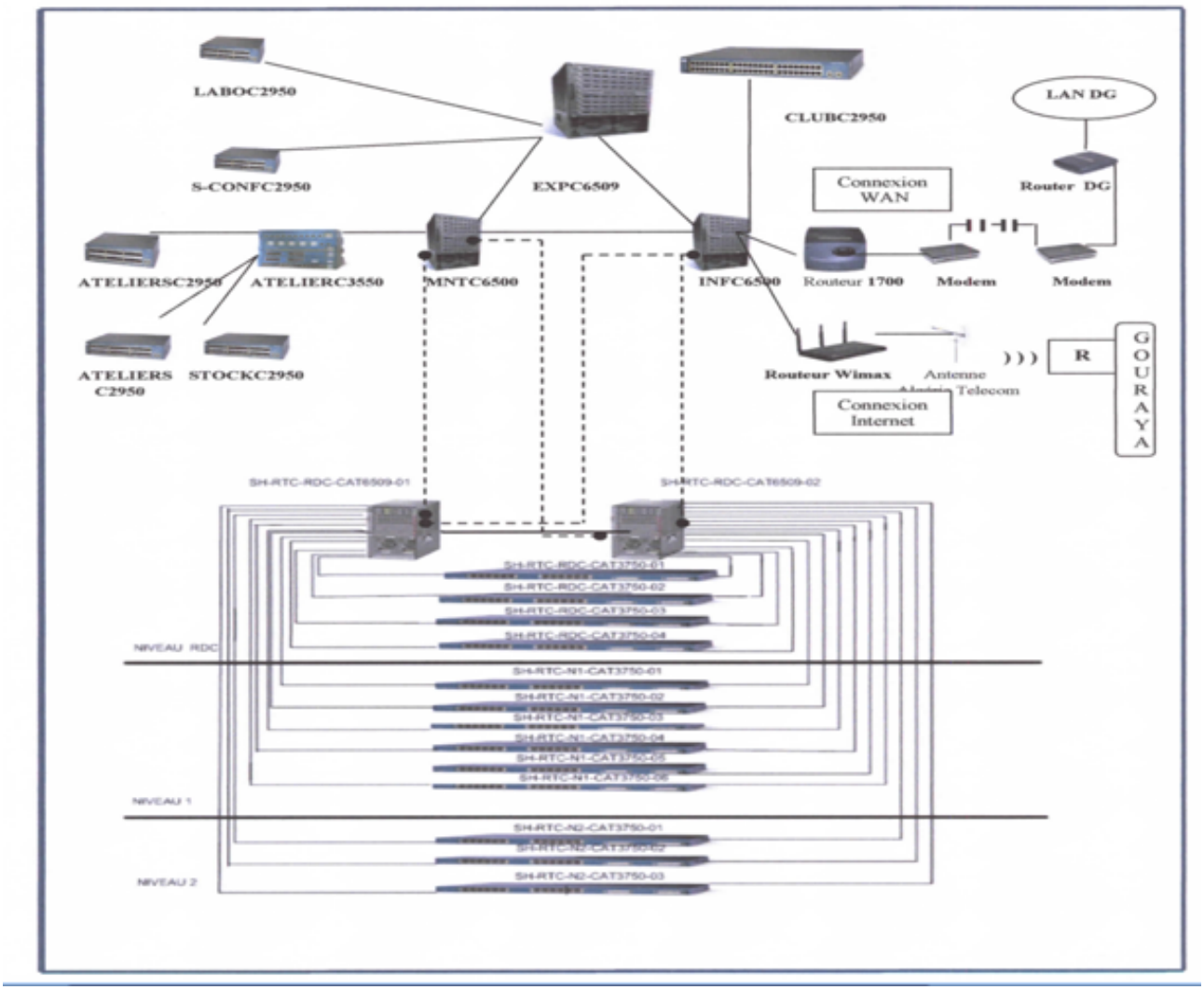


FIGURE 3.6 – Matiriels utilisé par SONATRACH

3.2.1.2 La définition des équipements de sécurité

- **Serveur antivirus :**Les antivirus sont des logiciels conçus pour identifier, neutraliser et éliminer des logiciels malveillants (dont les virus ne sont qu'un exemple). Ceux-ci peuvent se baser sur l'exploitation de failles de sécurité, mais il peut également s'agir de programme modifiant ou supprimant des fichiers, que ce soit des documents de l'utilisateur de l'ordinateur infecté, ou des fichiers nécessaires au bon fonctionnement de l'ordinateur.

Un antivirus vérifie les fichiers et courriers électroniques. Les secteurs de boot (Pour détecter les virus de boot), mais aussi la mémoire vive de l'ordinateur, les médias amovibles

(clefs USB, CD,DVD, etc), les données qui transitent sur les éventuels réseaux (dont internet), etc.

- **Serveur filtrage Web :**permet d'interdire l'accès à des sites au contenu répréhensible ou plus simplement de bloquer les bannières publicitaires. Les règles de filtrage sont mises à jour automatiquement dans l'établissement à partir d'une base de données.

- **Serveur Reporting :**est un outil complet de rapports faciles à utiliser qui permet d'évaluer l'utilisation d'Internet des employés de l'entreprise.

  Il identifie tous les problèmes possibles d'accès à Internet ou à la consommation de la bande passante réseau en générant des rapports détaillés, des résumés ou des graphiques. Il est utilisé pour montrer comment la connexion Internet est utilisée et pour affiner les stratégies de filtrage afin de maximiser les ressources du réseau.

- **Proxy Blue coat SG510 :**Le Blue Coat Proxy SG 510 offre un appareil absorbable à montage en rack pour les petites Enterprises et les succursales qui nécessitent un accès direct à Internet. Poxy SG 510 accélère les applications d'affaires à travers l'entreprise distributrice, fournissant un moyen rapide. La plate-forme Proxy SG 510 permet également le control du trafic Internet pour empêcher les logiciels malveillants et les applications non autorisées de compromettre la sécurité du réseau ou la performance.

FIGURE 3.7 – Proxy blue coat SG510

- **Firewall Juniper SSG 550 :**Représente une nouvelle classe de dispositif de sécurité construite à cet effet qui offre un parfait mélange de haute performance, de sécurité et de connectivité LAN/WAN pour les déploiements du bureau régional et des branches. Avec réseau éprouvé et la protection au niveau application, le SSG 550 peut être mis en œuvre comme dispositif de sécurité autonome pour arrêter les Logiciels espions, Chevaux de Troie, les logiciels malveillants et autres attaques émergentes.

Firewall Juniper SSG 550 contient un ensemble de règles structurées en trois zones qui se présentent comme suit :

- La zone trust : c'est la zone la plus confiante, car elle autorise le trafic sortant et interdit le trafic entrant et c'est pour cela que la RTC (Region Transport Centre) lui a confiée son réseau LAN.
- La zone untrust : c'est une zone qui autorise le trafic entrant et interdit le trafic sortant.

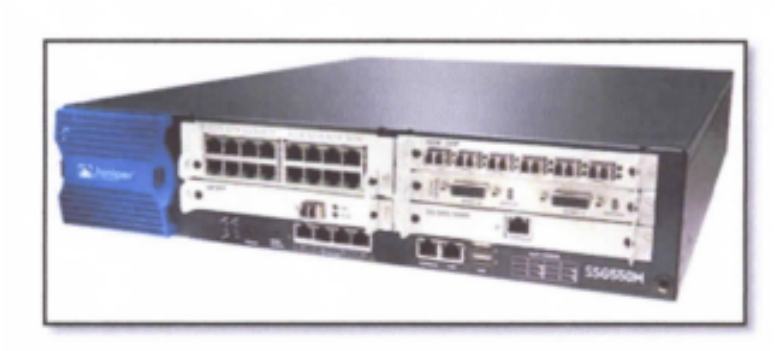


FIGURE 3.8 – Firewall Juniper SSG 550

- La DMZ (DEMILITARIZED ZONE) : est une zone tampon d'un réseau d'entreprise, située entre le réseau local et Internet, derrière le par-feu. Il s'agit d'un réseau intermédiaire regroupant des serveurs publics (http, DHCP, mails, DNS, etc).

Ces serveurs devront être accessibles depuis le réseau interne de l'entreprise et pour certains, depuis les réseaux externes. Le but est ainsi d'éviter toute connexion directe au réseau interne.

Pour des besoins d'administration et d'organisation, la zone DMZ de la RTC est partitionnée en trois sous-zones :

- La DMZ Administrateur (Admin) : contient Station d'admin, websense reporting, ISSgx4002
- La DMZ filtrage : contient Proxy bluecoat, websense filtrage
- La DMZ reverse proxy : est un type de serveur proxy, habituellement placé en frontal de serveurs web. Il est à différencier dans son utilisation des serveurs mandataires traditionnels. Le proxy inverse est implémenté du coté des serveurs Internet. L'utilisateur du web passe par son intermédiaire pour accéder aux applications de serveurs internes.

Cette technique permet entre autres de protéger un serveur web des attaques provenant de l'extérieur. Cette technologie est employée dans les solutions de sécurité applicative.

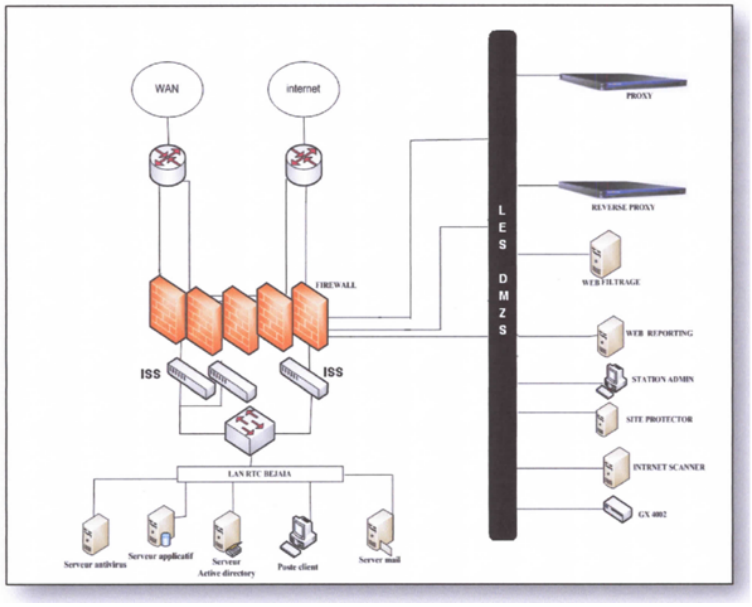


FIGURE 3.9 – Partie sécurité de SONATRACH

3.2.1.3 Définition de sa partie système

1. **PROTOCOLE HSRP**

- **Fonctionnement de HSRP (Hot Standby Routing Protocol) :** Est un protocol propriétaire crée par Cisco et très utilisé aujourd'hui dans nos LAN. De ce protocole est dérivé VRRP (Virtual Router Redundancy Protocol)

  En pratique, HSRP permet qu'un routeur de secours prenne immédiatement, de façon transparente, le relais dès qu'un problème physique apparait.

  En partageant une seule même adresse IP et MAC, plusieurs routeurs peuvent être considérés comme un seul routeur "Virtuel". Les membres du groupe de ce routeur virtuel sont capables de s'échanger des messages d'état et des informations.

  Un routeur physique peut donc être "responsable" du routage et un autre de la redondance.

  Si le routeur, que nous appellerons primaire, a un problème, le routeur secondaire prendra sa place automatiquement. Les paquets continueront de transiter de façon transparente car les 2 routeurs partagent les mêmes adresses IP et MAC !

  Un groupe de routeur va négocier au sein d'un même groupe HSRP (ou stanby group), un routeur primaire (Active router),élu au moyen d'une priorité, pour transmettre les paquets envoyés au routeur virtuel.

  Un autre routeur, le routeur secondaire (Standby router), sera élu lui aussi afin de remplacer le routeur primaire en cas de problème. Le secondaire assumera donc la tâche

de transmettre les paquets à la place du primaire en cas de défaillance.

Le processus d'élection se déroule pendant la mise en place des liens, une fois ce processus terminé, seul le routeur primaire (Active) va envoyer des messages multicast en UDP périodiques HSRP aux autres afin de minimiser le trafic réseau.

Si ces messages ne sont plus reçus par le routeur secondaire(Standby), c'est que le routeur primaire a un problème et le secondaire devient donc Actif.

L'élection se fait un peu à la manière de spaning-tree, en prenant en compte une priorité. Cette priorité est composée d'un paramètre "priority " compris entre 1 et 255 (255 étant le plus prioritaire) et de l'adresse IP de l'interface.

A priorités statiques égales, la plus haute adresse IP sera élue.

Plusieurs groupes HSRP peuvent exister au sein d'un même routeur sans que cela ne pose problème. Seuls les routeurs du même numéro de groupe s'échangeront les messages HSRP.

3.2.1.4 Définition des équipements système

Dans cette partie on va définir le contrôleur de domaine ainsi que ses éléments (l'annuaire Active Directory, le protocole DNS, DHCP) et d'autres serveurs comme celui de la messagerie électronique et le serveur d'anti-virus etc.

- **Définition d'un contrôleur de domaine (Active Directory) :**Le rôle du serveur de contrôleur de domaine est l'un des roles les plus importants à sécuriser dans n'importe quel environnement d'ordinateurs fonctionnant avec Microsoft Windows Server 2003 avec le Service Pack 1 et le service d'annuaire Active Directory. Toute atteinte à l'intégrité d'un contrôleur de domaine ou la perte de ce dernier dans ce type d'environnement pourrait avoir des conséquences graves pour les ordinateurs clients, serveurs et applications s'appuyant sur les contrôleurs de domaine pour l'authentification, la stratégie de groupe et l'annuaire LDAP (Lightweight Directory Access Protocol) central.

  En raison de leur importance, les contrôleurs de domaine doivent toujours être stockés dans des emplacements physiques sécurisés et accessibles uniquement au personnel administratif qualifié. Lorsque les contrôleurs de domaine doivent être stockés dans des emplacements moins surs, dans une filiale par exemple, plusieurs paramètres de sécurité peuvent être réglés pour limiter les dommages éventuels résultant de menaces physiques.

  La RTC dispose d'un contrôleur de domaine principal et d'un autre secondaire installés sur des serveurs de type Dell Power Edge 2800 qui sont complémentaire, si l'un cesse de fonctionner l'autre prend son rôle.

- **Définition du serveur Dell Power Edge 2800 :**Le système Power Edge 2800 comprend un processeur, des mémoires et des connecteurs d'E/S locaux intégrant les technologies les plus récentes. Il est doté d'un biprocesseur Intel XeonTM qui comprend la technologie Intel EM64 prenant en charge à la fois les applications 32 bits et 64 bits, de nouvel ensemble de puces Intel E7520 et allant jusqu'a 12 Go de mémoire DDR21. De plus, il n'inclut pas moins de sept connecteurs PCI/PCI-X ExpressTM.

FIGURE 3.10 – Le controleur de domaine power Edge 2800

- **Annuaire Active Directory :**Active Directory (AD) est la mise en œuvre par Microsoft des services d'annuaire LDAP pour les systèmes d'exploitation Windows. L'objectif principal d'Active Dierctory est de fournir des services centralisés d'identification à un réseau d'ordinateurs utilisant le système Windows. Il permet également l'attribution et l'application de stratégies. La distribution de logiciels, et l'installation de mises à jour critiques par les administrateurs.

- **Présentation des stratégies de groupe :**La stratégie de groupe du rôle de serveur contrôleurs de domaine est une stratégie de base. Le terme Stratégie désigne la configuration logicielle du système par rapport aux utilisateurs. A la suite d'une installation de Windows, aucune stratégie n'est configurée, et tout est permis (en fonction des droits des groupes d'utilisateurs prédéfinis : Administrateurs, Utilisateurs avec pouvoir).

- **Serveur d'applications (messagerie) :**Un serveur d'applications est un serveur sur lequel sont installées les applications utilisées par les usagers. Ces applications sont chargées sur le serveur d'applications et accédées à distance, souvent par réseau.

  Un serveur d'application peut être un serveur qui centralise toutes les applications utilisées par les postes clients. Pour le cas de la RTC, les serveurs d'applications sont l'ES40 et le DS20.

- **Exchange Server 2004 :**Microsoft Exchange Server est un logiciel collaboratif pour serveur de messagerie électronique crée par Microsoft, très utilisé dans les grandes entreprises. C'est un produit de la gamme des serveurs Microsoft, conçu pour la messagerie

électronique, mais aussi pour la gestion d'agenda, de contacts et de tâche, qui assure le stockage des informations et permet des accès à partir de clients mobiles et de clients Web (navigateurs tels que IE, Firefox, Safari) .

Exchange Server Offre aussi la possibilité de créer des dossiers publics pour le partage des fichiers et des dossiers volumineux, parmi ces dossiers on trouve :

- Dossier informatique : appartenant aux informaticiens

- Dossier cellule communication : destinée pour la cellule communication pour la diffusion de revues

- Dossier syndicat : Pour diffusion de rapports liés au syndicat.

3.3 La structure hiérarchique du réseau SONATRACH

La conception d'un réseau hiérarchique implique la division du réseau en couches distinctes. Chaque couche fournit des fonctions spécifiques qui définissent son rôle dans le réseau global. En séparant les différentes fonctions existantes sur un réseau, la conception du réseau devient modulaire, ce qui facilite l'évolutivité et les performances. Le modèle de conception hiérarchique classique se divise en trois couches : la couche d'accès, la couche de distribution et la couche cœur du réseau.

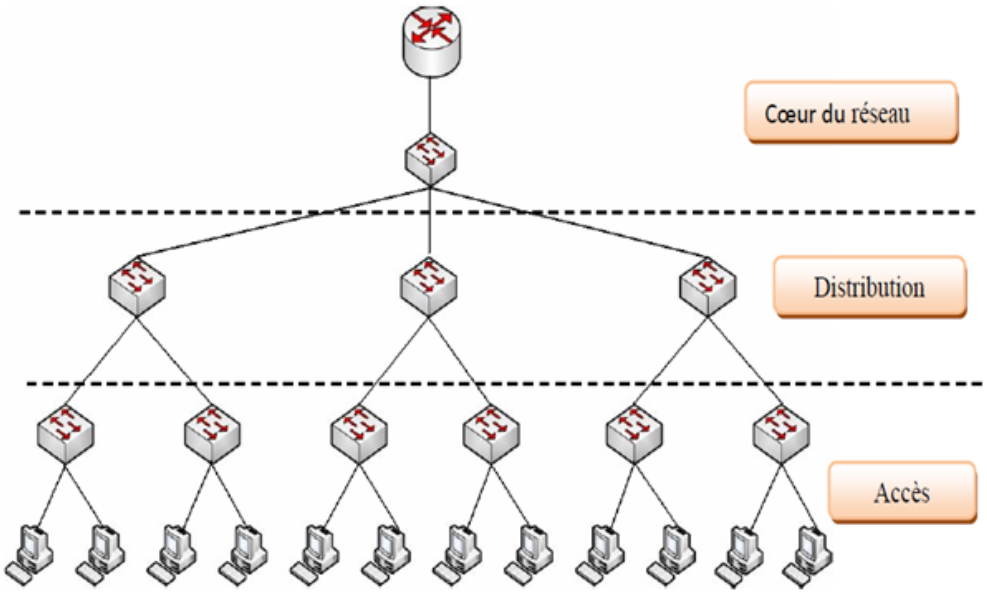


FIGURE 3.11 – Le modèle en couche de l'intranet

3.3.1 La couche accès

Elle sert d'interface avec les périphériques finaux (ordinateurs, les imprimantes et les téléphones sur IP), afin de fournir l'accès au reste du réseau. La couche d'accès peut inclure des routeurs, des commutateurs, des ponts, des concentrateurs et des points d'accès sans fil. Son rôle principal est de fournir un moyen de connecter et de contrôler les périphériques qui sont autorisés à communiquer sur le réseau.

3.3.2 La couche distribution

Elle regroupe les données reçues à partir des commutateurs de la couche d'accès, avant qu'elles ne soient transmises vers la couche coeur de réseau, afin de les transmettre aux destinataires. La couche de distribution gère le flux du trafic réseau. Elle délimite les domaines de diffusion via des fonctions de routage entre des réseaux locaux virtuels (VLANs) définis au niveau de la couche d'accès. Les commutateurs de la couche de distribution sont généralement des périphériques très performants qui offrent une disponibilité et une redondance élevées afin de garantir la fiabilité.

3.3.3 La couche cœur

Elle est essentielle à l'inter-connectivité entre les périphériques de la couche de distribution. Par conséquent, il est important qu'elle bénéficie d'une disponibilité couche de distribution. Elle doit donc être capable de réacheminer rapidement d'importantes quantités de données.

Elle est d'une redondance élevée [14]. La zone principale peut également se connecter à des ressources Internet. La couche coeur de réseau regroupe le trafic provenant de tous les périphériques de la couche de distribution. Elle doit donc être capable de réacheminer rapidement d'importantes quantités de données.

3.4 Etude critique de l'intranet en terme de sécurité

Après avoir étudié l'architecture actuelle du réseau Intranet de cette société, nous avons relevé une absence de politique de sécurité et un ensemble de failles qui peuvent nuire au réseau.

Parmi ces failles nous pouvons citer :

- Pour repérer des activités anormales ou suspectes dans le réseau (failles), il est recommandé de disposer d'un système de détection d'intrusions (IDS) et de prévention.
- Le firewall n'est capable de filtrer que le trafic qui le traverse, donc il est impossible d'interdire les actions malveillantes des utilisateurs via des stations non protégées par celui-ci. Ainsi, les accès au réseau par contournement du firewall ont autant de failles de sécurité.
- Les ordinateurs portables peuvent porter fortement préjudice à la politique de sécurité globale car ils véhiculent parfois des virus qui sont beaucoup plus dangereux que ceux circulant sur internet.

– Les commutateurs non sécurisés entrainent plusieurs problèmes tels que l'accès à des ressources ou données non autorisées.
– Comme les routeurs sont des passerelles vers d'autres réseaux, ils constituent des cibles évidentes et sont soumis à une variété d'attaques.
– L'utilisation de plusieurs Switch et plusieurs VLANs l'architecture est devenue trop complexe. .

3.5 Amélioration de la sécurité Informatique

Après avoir étudié les principales failles de l'intranet de SONATRACH, nous nous sommes fixées comme objectifs de trouver un compromis entre deux besoins essentiels :

- Le besoin d'ouvrir l'intranet pour profiter de nouvelles opportunités commerciales.

- Le besoin de protéger des informations privées ou publiques et surtout de protéger les informations stratégiques.

Dans le passé, le seul périphérique qui venait à l'esprit en matière de sécurité était le pare-feu. Un pare-feu n'est désormais plus suffisant pour sécuriser un réseau. Il est indispensable d'adopter une approche intégrant pare-feu, prévention contre les intrusions et intégrer les réseaux privés virtuels (VPN).

Pour obtenir une meilleure architecture en termes de tolérance aux fautes, il est plus ou moins nécessaire d'établir une liaison entre les blocs. La redondance de liaison améliore la disponibilité du réseau grâce à la mise en place de chemins alternatifs via l'ajout d'équipements et de câbles. Si les données ont la possibilité d'emprunter plusieurs chemins pour traverser le réseau, un chemin peut être coupé sans aucune influence sur la connectivité des périphériques du réseau. Mais cette redondance de liaison peut engendrer une boucle infinie de la circulation des paquets si le protocole STP n'est pas activé sur le commutateur.

Vu le nombre important d'utilisateurs du réseau qui ne cesse de croitre et qui appartiennent à différentes catégories (sous direction Exploitation, sous direction Technique, sous direction Comptabilité...), ajoutée à celà, l'architecture complexe du réseau (vaste domaine de diffusion), il est difficile d'assurer une parfaite sécurisation.

Pour ce faire, nous faisons appel à l'une des technologies qui permet d'obtenir d'excellentes performances réseau. Cette technique consiste à diviser les vastes domaines de diffusion en domaines plus petits à l'aide de réseaux locaux virtuels (VLAN). Avec des domaines de diffusion plus petits, le nombre de périphériques participant aux diffusions est limité.

Les périphériques sont ainsi divisés en groupes fonctionnels, regroupant par exemple les services de bases de données pour un service de comptabilité et les transferts de données à haute vitesse pour un service technique.

Les groupes contenant des données sensibles sont séparés du reste du réseau, ce qui diminue les risques de violation de confidentialité. Les ordinateurs des responsables (Directeur, cadres, fonctionnaires, ...) se trouvent sur un autre VLAN et sont complètement séparés du trafic des données des fonctionnaires et des invités qui sont à leurs tours affectés à des VLANs différents.

La surveillance du serveur DHCP est une fonction CISCO pour les commutateurs qui déterminent quels ports du commutateur sont en mesure de répondre aux requêtes DHCP. Les ports sont identifiés comme étant fiables et non fiables.

Les ports fiables peuvent authentifier la source de tous les messages. Les ports non fiables peuvent uniquement authentifier la source des requêtes. Les ports fiables hébergent un serveur DHCP ou peuvent offrir une liaison montante vers le serveur DHCP. Si un périphérique non autorisé sur un port non fiable tente de transmettre un paquet de requêtes DHCP sur le réseau, le port est fermé.

Pour contrôler l'accès au réseau nous analysons les paquets entrants et sortant à travers le routeur (filtrage des paquet) en utilisant les listes de contrôle d'accès (ACL) que ce soit entre les VLANs ou entre le réseau interne et les réseaux externes (internet).

3.6 Proposition d'une nouvelle configuration sécurisée

L'intranet de SONATRACH est constitué d'un ensemble de commutateurs et d'un routeur qui sont des équipements CISCO. Pour illustrer les propositions citées ci- dessus, nous allons configurer ces équipements d'une manière sécurisée.

3.6.1 Configuration de l'accès à la console des commutateurs

Pour protéger les commutateurs contre tout accès non autorisé, des mots de passe sont configurés pour l'accès à la console, le terminal virtuel et le mode d'exécution,

3.6.2 Configurations sécurisées des ports des commutateurs

Les commutateurs dont les ports ne sont pas sécurisés permettent à un pirate de rallier un système à un port pour rassembler des informations ou mener des attaques...etc. Ainsi la configuration sécurisée des ports s'avère plus que nécessaire :

- Préciser s'il s'agit d'une seule adresse ou d'un groupe d'adresses MAC autorisé sur un port.
- Préciser pour que le port se bloque ou s'arrête automatiquement si les adresses non autorisées sont détectées.

3.6.3 Segmentation du réseau en VLANs

Le réseau actuel est segmenté en VLANs ou en blocs . Cette segmentation n'assure pas la sécurité, vu que dans chaque bloc, on trouve différentes catégories d'utilisateurs. Pour améliorer la sécurité nous proposons de réorganiser la segmentation du réseau selon les différentes catégories d'utilisateurs.

Avant de segmenter ce réseau, nous devons tout d'abord classer l'ensemble des utilisateurs dans les réseaux virtuels. Pour ce faire nous avons procédé à la méthode de construction des VLANs par port car cette dernière procure le niveau de sécurité le plus élevé puisque les stations d'un segment doivent se trouver sur le même réseau virtuel.

L'ensemble de la communauté est organisée par catégorie sociale, ce qui nous a permis de définir les VLANs utilisables comme suit :

VLAN	Description	Adresse réseau
2	Sous directions	10.136.2.0
3	Informatique	10.136.3.0
4	HSE	10.136.4.0
5	Sécurité interne	10.136.5.0

Table 3.1 – Les différents VLANs du réseau SONATRACH.

- VLAN sous directions : regroupe toutes les sous directions (direction, sous direction d'exploitation, sous direction technique, sous direction administrative et sous direction finance et juridique) de SONATRACH.

- VLAN informatique : réservé au personnel qui gère tout le réseau.

- VLAN HSE : Hygiène Sécurité Environnement.

- VLAN sécurité interne : attribué aux personnes qui exécutent une ou plusieurs activités privées de sécurité au bénéfice de l'entreprise.

Comme l'entreprise SONATRACH compte autant de commutateurs, pour configurer tous les VLANs au niveau de chaque commutateur ; alors pour gagner du temps, nous avons utilisé le protocole VTP de commutateurs pour simplifier la gestion de la base de données VLANs sur plusieurs commutateurs. Pour ce faire, nous devons configurer. le commutateur fédérateur comme étant le serveur VTP, et le reste des commutateurs sont des clients VTP.

3.6.4 Configuration de l'accès au routeur

Pour protéger le routeur contre tout accès non autorisé, nous allons définir : un nom utilisateur " username " et un mot de passe" password ".

Un mot de passe fort est l'élément fondamental d'un contrôle d'accès sécurisé à un routeur. Pour une meilleure protection le mot de passe doit être chiffré à l'aide d'une clé cryptographique.

3.6.5 Configuration sécurisé pour des accès administratifs à distance aux périphériques (routeur, commutateur)

A mesure que SONATRACH grandit et que le nombre des équipements augmente, la connexion locale aux périphériques peut rendre le travail des administrateurs plus difficile. Pour gérer efficacement un réseau, il est important de disposer d'un accès à distance aux Périphériques.

L'accès à distance implique généralement l'autorisation de la connexion d'un ordinateur au routeur dans un même inter-réseau.

Dans un premier temps, nous allons commencer par sécuriser les lignes d'administration, pour configurer ensuite le périphérique réseau de manière à chiffrer le trafic dans un tunnel SSH.

Le protocole SSH (Secured SHell) est là pour sécuriser la circulation des informations en les chiffrant. Il permet d'établir un tunnel chiffré entre deux hôtes.

3.6.6 Configuration du routage inter-VLANs

Pour permettre une connexion physique unique sur laquelle on transmet le trafic de plusieurs réseaux virtuels, c'est-à-dire une communication inter-VLANs nous devons configurer des liens trunks sur notre routeur, et ce en créant des sous interfaces, où chacune d'elles est affectée à un VLAN selon une adresse IP appropriée à ce VLAN.

3.6.7 Configurations des ACL au niveau du routeur

Une ACL est une liste d'Access Control Entry (ACE) ou entrée de contrôle d'accès donnant ou supprimant des droits d'accès à une personne ou un groupe (voir chapitre2).

Pour pouvoir autoriser ou refuser l'accès aux ressources disponibles dans le réseau ainsi aux différents VLANs et contrôler le trafic entrant et sortant du réseau , nous avons procédé à la configuration des listes de contrôle d'accès au routeur.

Conclusion

Ce chapitre présente une étude critique sur le plan sécuritaire du réseau intranet d'une grande société qui est SONATRACH.
Des solutions sont proposées :

- Utilisation d'un password et d'un username
- Segmentation du réseau en VLANS

- Contrôle de routage inter VLANs
- Contrôle des ACL
- Contrôle de SSH

Ces solutions sont mises en oeuvre sous CISCO Packet Tracer, un simulateur bien connu de CISCO.
Dans le chapitre qui suit.

Chapitre 4

Mise en oeuvre de la proposition

Introduction

Après avoir décrit notre solution dans le chapitre précédent, nous allons voir dans ce qui suit la simulation de cette dernière avec l'outil CISCO appelé Packet Tracer que nous allons décrire ci-dessous

Packet Tracer

C'est un outil pédagogique et simulateur de réseau, développé par CISCO Systems pour concevoir configurer, dépanner et visualiser le trafic réseau dans un environnement de programmes simulé et contrôlé. Packet Tracer permet d'élaborer des représentations virtuelles de réseaux et d'émuler un grand nombre des fonctions offertes par les périphériques réseau.

Matériel utilisé

Avant d'entamer la configuration nous devons installer le réseau sur Packet Tracer. Pour ce faire, nous aurons besoins du matériels suivants :
- Un routeur.
- 4 Commutateurs Cisco Catalyst 2950 et 5 Commutateurs Cisco Catalyst 3560.
- 8 PC pour le test.
- Des câbles droits pour connecter les commutateurs ou ordinateurs au commutateurs ou routeur.

Le réseau de SONOTRACH sera comme suit sous Packer Tracer :

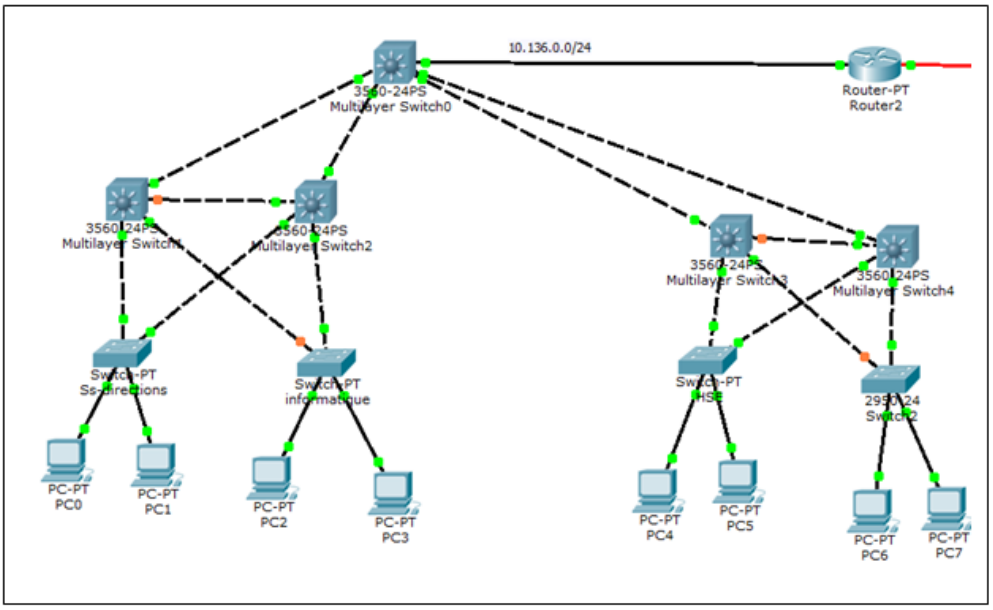


FIGURE 4.1 – Le réseau logique de SONATRACH sous Packet Tracer

4.1 Les étapes de simulation

Nous avons deux étapes de configuration, une pour les commutateurs (ou Switch) et une autre pour le routeur.

4.1.1 Configuration du commutateur

1ière étape

placement des Switch et des liaisons correspondantes sur l'interface Cisco Packet Tracer.

2ième étapes

configuration des Switch

Au début d'une configuration de base du commutateur,on commence par l'attribution d'un nom au commutateur avec la commande suivante :

Switch# ***hostname*** ***<nom-switch >***

- **Pour les Switch serveur (fédérateur) :**

```
Switch> enable
Switch #confi t       /* configuration terminale */
Enter configuration commands, one per line. End with CNTL/Z  /* sortie
Switch(config) #hostname s-fdr /*renomé le Switch*/
S-fdr (config) #exit  /*enregistrer et sortie */
```

- **Pour les switch qui restent :**

```
Switch> enable
Switch #confi t
Enter configuration commands, one per line. End with CNTL/Z
Switch (config) #hostname S0
S0 (config) #exit
```

3ième étape

configuration de ligne pour la console et configuration des mots de passes d'accès :

Pour passer en mode de configuration de ligne pour la console, on tape la commande suivante : **switch (config)#line console 0**

On appelle ligne de console, toute liaison physique entre deux équipements.

Pour lui attribuer un mot de passe, on tape la commande suivante : **S0(config)#password sonatrach**
Différentes commandes à suivre pour la configuration des lignes de console et du mot de passe :

```
Switch> enable
Switch # confi t
Switch (config) # hostname S0
S0 (config) # line console 0 /*configurartion de la ligne console*/
S0 (config) # password sonatrach /*donné un mot de passe au Switch*/
S0 (config) # login
S0 (config) # line vty 0 15 /* permet à 16 administrateurs de passer en même temps sur
l'équipement.
S0 (config)# password sonatrach
S0 (config) # login
S0 (config) # exit
S0 (config) # copy r s
```

Une fois on a terminé de taper ces différentes commandes, la configuration utilisée est générée :

```
Switch>enable
Switch#config
Switch#configure
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hostname s-fdr
s-fdr(config)#line console 0
s-fdr(config-line)#password sonatrach
s-fdr(config-line)#login
s-fdr(config-line)#line vty 0 15
s-fdr(config-line)#password cisco
s-fdr(config-line)#login
s-fdr(config-line)#end
s-fdr#
%SYS-5-CONFIG_I: Configured from console by console

s-fdr#copy r s
Destination filename [startup-config]?
Building configuration...
[OK]
s-fdr#
```

FIGURE 4.2 – Configuration et définition des mots de passe au Switch cœur

4ième étape

configuration d'un domaine VTP sur tous les Switch

Le protocole VTP (VLAN Turing Protocol) de Cisco Packet Tracer (protocole propriétaire Cisco) permet de résoudre des problèmes opérationnels dans des réseaux commutés contenant des VLANs. Son rôle est de maintenir la cohérence de la configuration VLANs sur un domaine d'administration réseau commun.

Le protocole VTP doit être configuré sur tous les commutateurs du réseau en leur attribuant un nom au domaine VTP et un mot de passe. Les commandes de configuration du VTP sont les suivantes :

Switch(config) # vtp mode <server/ client>

Switch (config) # vtp domain <nom_domaine>

Switch (config) # vtp password <mot de passe>

Dans notre cas, nous allons configurer le serveur VTP dans le commutateur fédérateur. Le nom du domaine VTP est : **test**, la figure suivante illustre notre configuration :

```
s-fdr>enable
s-fdr#sh vtp status
VTP Version                     : 2
Configuration Revision          : 0
Maximum VLANs supported locally : 1005
Number of existing VLANs        : 5
VTP Operating Mode              : Server
VTP Domain Name                 : test
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Disabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0x01 0xFC 0xF7 0xCE 0xD6 0x50 0xBA 0x0A
Configuration last modified by 0.0.0.0 at 0-0-00 00:00:00
Local updater ID is 0.0.0.0 (no valid interface found)
s-fdr#
```

FIGURE 4.3 – Configuration du serveur VTP sur les Switch fédérateur

Ensuit, on va créer les pools DHCP pour chaque VLANs, et pour cela on a qu'à suivre les commandes ci-dessous :

S-fdr (config) # ip dhcp pool vlan2

S-fdr (config) # network 10.136.2.0 255.255.255.0

S-fdr (config) # default-router 10.136.2.254

Les autres commutateurs sont les clients VTP du même domaine test. La configuration du premier commutateur est donnée comme suit :

```
sw2>enable
sw2#sh vtp status
VTP Version                     : 2
Configuration Revision          : 0
Maximum VLANs supported locally : 1005
Number of existing VLANs        : 5
VTP Operating Mode              : Client
VTP Domain Name                 : test
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Disabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0x01 0xFC 0xF7 0xCE 0xD6 0x50 0xBA 0x0A
Configuration last modified by 0.0.0.0 at 0-0-00 00:00:00
sw2#
```

FIGURE 4.4 – Configuration du client VTP sur les autres Switch

5ième étape

Configuration des VLANs

Après avoir configuré le serveur VTP, nous allons créer le réseau virtuel. Pour se faire, nous devons créer des VLANs dans le serveur VTP parceque ce dernier diffuse ses configurations, tandis que le client VTP met à jour sa configuration VLANs en fonction des informations reçues du serveur.

La syntaxe des commandes utilisées pour créer les VLANs sont :

Switch (config) # vlan <num_vlan>

Switch (config) # name <nom_vlan>

6ième étape

La configuration des adressas IP des Switch

```
S0 (config) # int vlan3 /* passé a la interface du Switch on lui attribue un VLANs*/
S0 (config-if) # ip address 10.136.3.1 255.255.255.0
S0 (config-if) # no shutdown /*enregistrer et quitté */
S0 (config-if) # exit
```

7ième étape

La configuration en mode trunk ou en mode Access :

Dans cette étape nous configurons tous les ports qui relient les Switch en mode trunk et les ports des Switch qui sont reliés au PC vont être en mode Access.

1ière partie

la configuration en mode trunk
- Le port du switch cœur :

```
sw0 (config) #interface FastEthernet 0/1
sw0 (config-if) # switchport mode dynamic auto
sw0 (config-if) # switchport trunk encapsulation dot1q
sw0 (config-if) # switchport mode trunk
sw0 (config-if) # exit
```

- Les ports des autre Switchs :

```
S0 (config) # interface FastEthernet 0/1
S0 (config) #switchport mode trunk
S0 (config) #exit
```

```
S2(config)#int Fa 0/3
S2(config-if)#swi
S2(config-if)#switchport mode trunk

S2(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state t
o down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state t
o up

S2(config-if)#no shu
S2(config-if)#no shutdown
S2(config-if)#exit
S2(config)#
```

FIGURE 4.5 – Configuration en mode trunk

2ième partie

La configuration en mode Access

```
S0 (config) # interface FastEthernet 0/2
S0 (config) #switchport mode access vlan 3
S0 (config) #exit

S0 (config) # interface FastEthernet 0/3
S0 (config) #switchport mode access vlan 3
S0 (config) #exit
```

8ième partie

Configurations sécurisées des ports des commutateurs
Pour configurer la sécurité des ports sur un port du commutateur, nous utilisons les commandes suivantes :

```
Switch (config) # interface <id_interface>
Switch (config-if) # switchport mode access
Switch (config-if) # switchport port-sécurity
Switch (config-if) # switchport port-sécurity mac-address sticky
Switch (config-if) # switchport port-security violation shutdown
```

4.1.2 Configuration du routeur

Nous avons trois étapes de configuration, la premier pour configurer le routeur, la deuxième pour routage inter VLANs et la dernier pour configurer les listes de contrôle ACL.

1ière étape : Configuration du routeur

- Attribué un nom au routeur

```
routeur> enable
routeur #confi t
routeur (config) # hostname R1
```

- Configuration de mot de passe enable secret :
  R1(config) #enable secret sonatrach

- Configuration domain-name :
  (config)#ip domain-name www.cisco.com

– Cryptage RSA :
R1 (config)# crypto key generate rsa

– Configuration des parameters SSH :
R1 (config) # ip ssh time-out 15
R1 (config) # ip ssh authentication-retries 2
R1 (config) # username memoire password cisco

– Configuration de l'authentification locale VTY.
R1 (config) # line vty 0 4
R1 (config-line) # transport input ssh
R1 (config-line) # login local

2ième étape : Routage-inter VLANs

Le routage intre-VLANs permet à plusieurs VLANs différents de communiquer.
Les commande suivantes sont a suivre pour configurer le routage-inter VLANs :

R1 (config) # interface FastEthernet0/0.2
R1 (config) # encapsulation dot1Q 2
R1 (config) # ip address 10.136.2.254 255.255.255.0

3ième étapes : Création d'une ACL standad :

Les ACLs permettent de filtrer les accès entre les différents réseaux ou de filtrer les accès au routeur lui même.

Les ACLs peuvent être appliquées sur le trafic entrant ou sortant.
Il y a deux actions : soit le trafic est interdit, soit le trafic est autorisé.

Voici la structure d'une ACL standard :
Router (config) # access-list n° de l'ACL deny | permit adresse d'origine masque générique

– Création d'une access-list
R1 (config) # access-list 1 deny 10.136.1.0 0.0.0.255
R1 (config) # access-list 1 permit any

Le numéro de l'ACL est 1 : il s'agit donc d'une ACL ip standard
L'adresse d'origine est 10.136.1 .0 et le masque est 0.0.0.255
On note que les trois premiers octets du masque ne sont constitués que de 0 et que le dernier octet n'est constitué que de 1.
On vérifie donc exactement les trois premiers octets de l'adresse d'origine, mais on ne s'occupe pas du dernier octet.

On a donc bien interdit (deny) tous les postes du réseau 10.136.1.0
La deuxième ligne indique d'autoriser (permit) tout le reste (any), car n'oublions pas qu'il y a toujours une commande implicite " deny any " à la fin des ACLs.

– affectation de cette ACL à une interface du routeur.

R1 (config) # int fa0/0
R1 (config-if) # ip access-group 1 IN

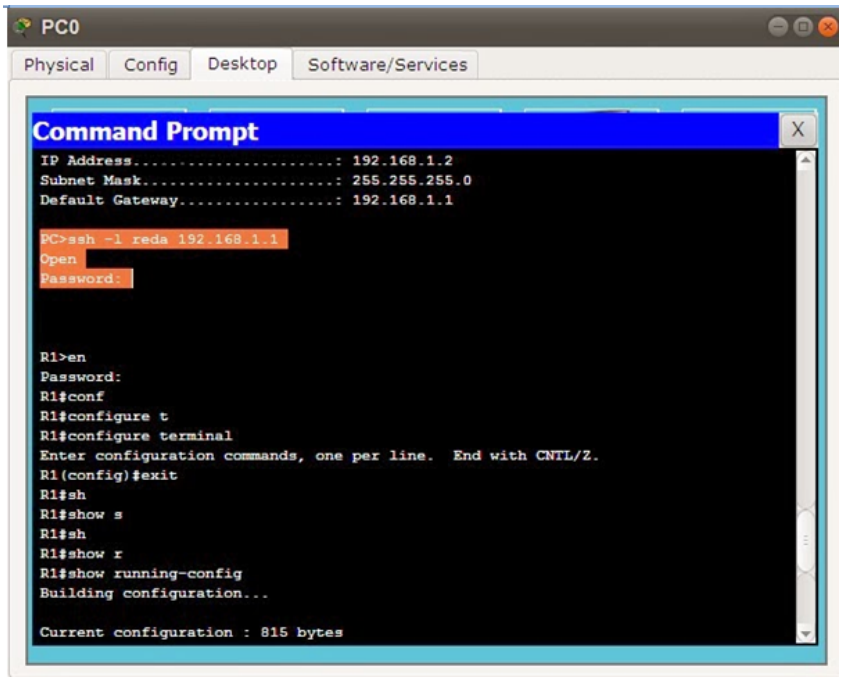
L'ACL est définie en " IN " : on interdit donc le trafic (requête) provenant du réseau " Invité " à entrer sur l'interface du réseau " Comptabilité ".
Si on veut interdire du trafic à sortir sur une interface, on remplace " in " par " out ".

4.2 Les testes éffectué

4.2.1 Accès à distance depuis la machine en utilisant SSH :

Une fois qu'on termine la configuration sur le router , ouvrons "Command Prompt" et entrons les commandes suivantes :

```
PC> ssh -l memoire 10.136.3.254
Open
Password: sonatrach
R1> en
Password: Cisco
```



- la figure suivante illustre le ping entre les différents VLANs

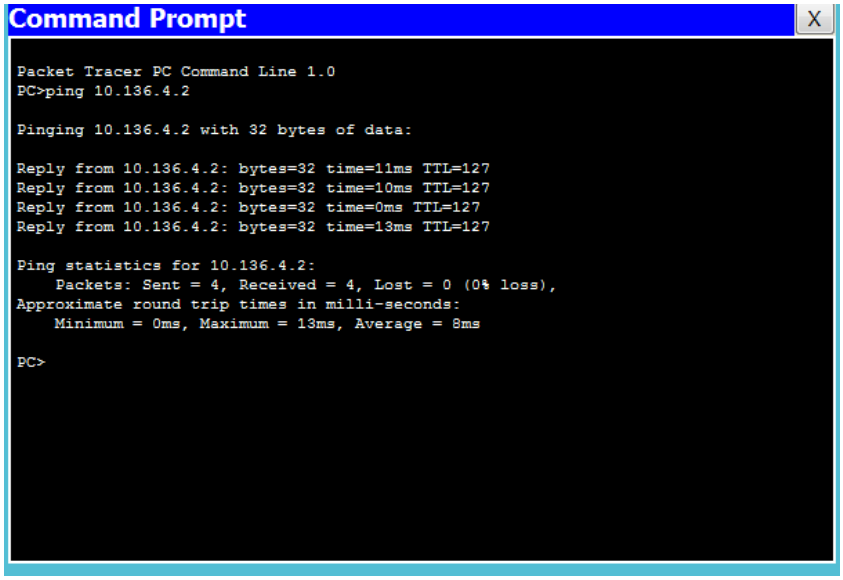


FIGURE 4.6 – Ping entre les différents VLANs

- la figure suivante illustre le ping entre les VLANs de même types

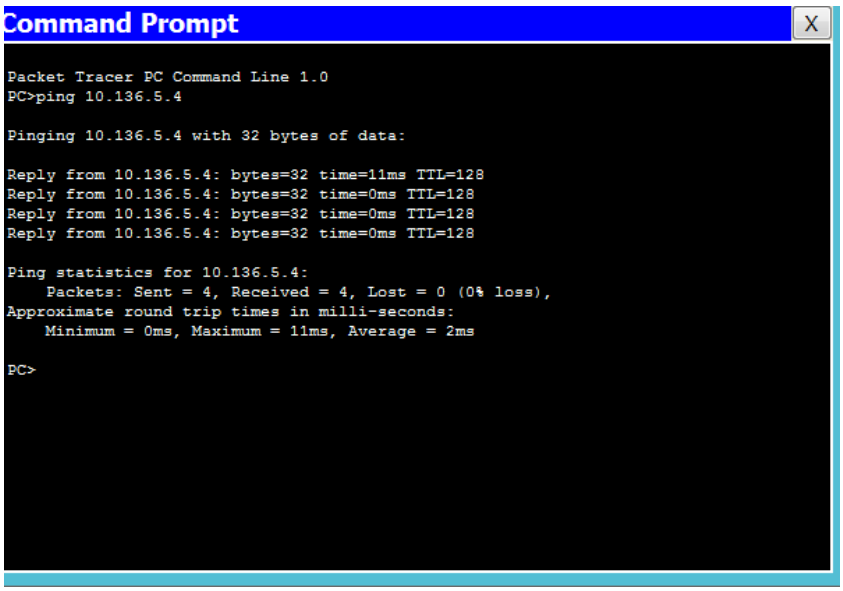


FIGURE 4.7 – Ping entre les VLANs de même types

Conclusion

Ce chapitre s'est concrétisé par :
- La mise en place d'une nouvelle architecture de réseau Intranet étudié, basé sur la sécurité.
- Configuration des VLANs.
- Intégration des noms de domaines et des passwords.
- Controle d'accès (ACL).
- Mots de passe au niveau de routeur.
- Protocole SSH.

Conclusion et Perspectives

Dans ce mémoire, nous avons proposé une nouvelle configuration de l'intranet de SONATRACH dont l'objectif est d'améliorer la sécurité de celui-ci. Cette nouvelle configuration consiste à sécuriser d'abord les équipements d'interconnexion constituant notre réseau (le routeur et les commutateurs) ainsi que l'accès distant des administrateurs réseau à ces équipements, en suite nous avons procédé à une segmentation logique du réseau tout en gardant l'architecture physique de base à l'aide des réseaux locaux virtuels qui seront attribués à chaque catégorie d'utilisateurs en prenant compte des contrôles d'accès pour quelques réseaux virtuels.

Dans le premier temps, nous avons présenté les concepts fondamentaux des réseaux locaux. Nous avons donné un aperçu sur les différentes topologies et les équipements d'interconnexion des réseaux locaux, en suite, nous avons vu les principaux composants matériels des réseaux informatiques. Nous avons mis un accent sur le modèle de référence OSI et le protocole TCP/IP, et enfin nous avons conclu par la présentation de l'adressage IP.

Les différents mécanismes de sécurité ont fait l'objet d'une étude succincte. Pour sécuriser un système informatique il est indispensable de bien connaitre les différentes techniques d'attaques utilisées, pour cela nous avons présenté quelques unes qui sont les plus fréquentes dans les réseaux informatiques et enfin une description de quelques techniques et mesures de sécurité et leurs fonctionnement à savoir les firewalls, les systèmes de détection d'intrusions (IDS), la cryptographie, et les listes de contrôle d'accès (ACL) qui sont appliqués aux équipement matériels comme le routeur. Les réseaux locaux virtuels (VLANs) ainsi qu'une représentation de quelques protocoles d'administration et de gestion des VLANs tels que le VTP.

Nous avons ensuite présenté l'architecture physique existante du réseau intranet de SONATRACH. Cette architecture est en étoile étendue. Cette architecture a fait objet d'une étude critique, qui constitue l'essentiel de notre travail. Elle nous a dévoilé des points faibles, auxquels on a apporté quelques solutions : Configuration sécurisé pour des accès administratifs à distance aux périphériques (routeur, commutateur). Pour contrôler le trafic entrant et sortant du réseau, nous avons procédé à la configuration des listes de contrôle d'accès au routeur.

Nous avons également remarqué :
- l'absence d'IDS afin de détecter et interrompre les actions malveillantes.
- les pare-feu existants ont une architecture pas suffisamment puissante pour filtrer le trafic important du réseau.

L'architecture logique actuelle de l'intranet est segmentée en VLANs selon les catégories à savoir les administrateurs réseaux, les fonctionnaires, les responsables. . .etc. Cette segmentation n'est pas efficace de point de vue de sécurité, puisque d'un coté toute personne (administrateur, responsable, fonctionnaire,. . .) utilisant l'intranet dans un même bloc peut accéder facilement aux postes des autres personnes, d'un autre coté les utilisateurs de la même catégorie ne peuvent pas communiquer entre eux à cause de leurs positionnement dans des VLANs différents.

L'outil de simulation utilisé est bien le Packet Tracer de CISCO. La proposition d'une nouvelle configuration sécurisée qui consiste à sécuriser le routeur et les Switchs par un mot de passe pour l'administration locale et de configurer l'accès a distant des administrateurs par une

connexion SSH pour assurer une administration à distance sécurisée. Pour une communication sécurisée entres les utilisateurs nous avons configuré le routage inter-VLANs, en appliquant quelques listes de contrôle d'accès (ACL).
Notre solution assure un certain degré de sécurité pour le réseau de SONATRACH. Toute fois, il est préférable de configurer un serveur d'authentification tel que RADIUS pour s'assurer que la bonne personne est bien affectée au bon VLANs.

Perspectives futures

Cette ébauche prendra forme d'une solution sécurisée conséquente, une fois que l'intégration d'autres types de menaces sera établie, et équipé :
- d'un système d'authentification puissant.
- d'un firewall robuste.
- des solutions de cryptographie quand c'est nécessaire.
- Configuration d'un serveur d'authentification telque RADIUS pour s'assurer que la bonne personne est bien affectée au bon VLANs.

ANNEXE

Annexe A

.1 Le protocole TCP

Le protocole TCP est Fiable et orienté connexion, assure le contrôle de flux au moyen de fenêtres glissantes et fournit des numéros de séquence et des accusés de réception. Il retransmet toute information non reçue et fournit un circuit virtuel entre les applications des utilisateurs finaux. Ce protocole présente l'avantage de garantir la transmission des segments .

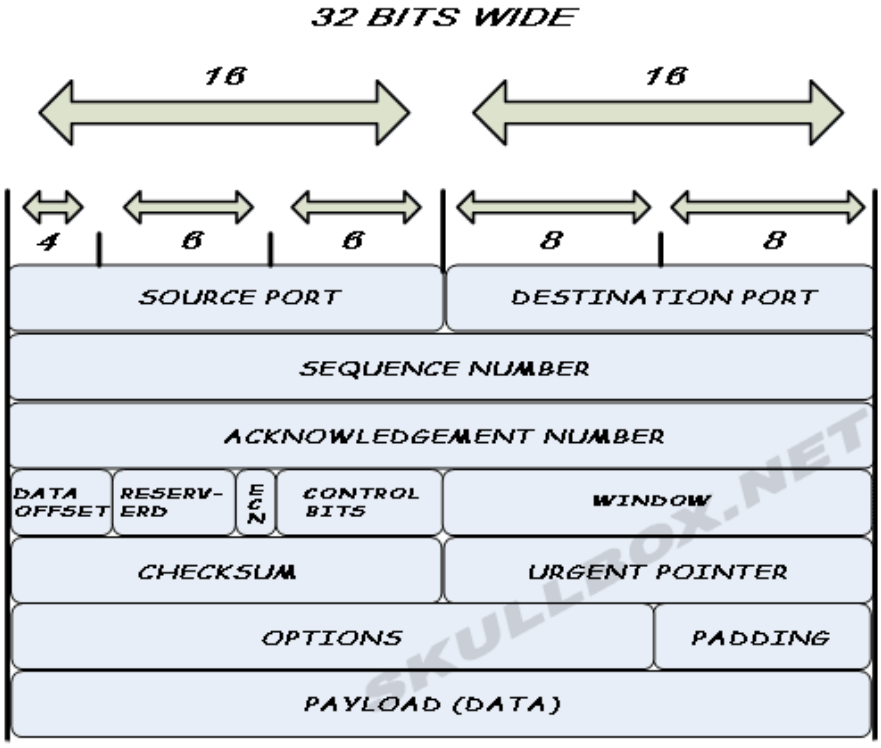


FIGURE 8 – Structure d'un entête TCP

.1.1 Quelques détails de la fifure (5)

- **Source Port (16 bits) :** numéro du port source.

- **Destination Port (16 bits) :** numéro du port destination.

- **Source Port (16 bits) :** Sequence Number (32 bits) :

  - Si SYN = 0, le numéro de séquence est celui du premier octet de données de ce segment.

  - Si SYN = 1, il s'agit du numéro de séquence initiale ISN. Le premier octet de donnée est à ISN+1.

- **Acknowledgment Number (32 bits) :** si le bit ACK = 1, ce champ contient le numéro de séquence attendu par l'´emetteur du segment.

- **Data Offset (4 bits) :** taille de l'en-tête TCP en mots de 32 bits.

- **Reserved (6 bits) :** champ réservé pour une utilisation ultérieure. Les 6 bits doivent être à 0.

- **Control bits (6 bits) :**
- *URG :* Pointeur de données urgentes significatif.
- *ACK :* Accusé de réception significatif.
- *PSH :* fonction push.
- *RST :* réinitialisation de la connexion
- *SYN :* synchronisation des numéros de séquence.
- *FIN :* fin de transmission.

- **Windows (16 bits) :** nombre d'octets de données à partir de celui indiqué par le champ Acknowledgment.

- **Checksum (16 bits) :** somme de contrôle sur 16 bits de l'en-tête et des données.

- **Urgent Pointer (16 bits) :** ce champ est interprété uniquement si le bit de contrôle URG est à 1. Le pointeur donne le numéro de séquence de l'octet qui suit les données " urgentes ".
- **Options :** il existe deux formats d'options : un seul octet de catégorie d'option ou un octet de catégorie d'option suivi d'un octet de longueur d'option et de l'octet des données de l'option.

.2 Le protocole UDP

Le protocole UDP est un protocole non orienté connexion et non fiable. Bien qu'il soit chargé de la transmission des messages, il n'exécute aucune vérification logicielle sur l'acheminement des segments au niveau de sa couche.
L'avantage de ce protocole est sa vitesse. Comme il ne fournit pas d'accusés de réception, le trafic sur le réseau est plus faible, ce qui accéléré les transferts.

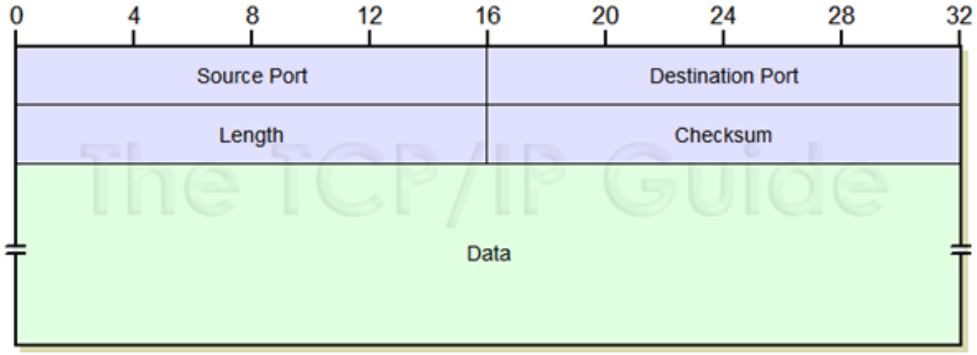


FIGURE 9 – Structure d'un entête UDP

.2.1 En-tête UDP Quelques détails du tableau

- **Source Port (16 bits)** numéro du port source. Ce champ est optionnel.
- **Destination Port (16 bits) :** numéro du port destination.
- **Length (16 bits) :** longueur en octets du datagramme UDP incluant l'en-tête et les données.
- **Checksum (16 bits) :** somme de contrôle sur 16 bits de l'en-tête et des données.

.3 Le protocole IP

Internet Protocol (abrégé en IP) est une famille de protocoles de communication de réseau informatique conçu pour être utilisé par Internet. Les protocoles IP sont au niveau 3 dans le modèle OSI. Les protocoles IP s'intègrent dans la suite des protocoles Internet et permettent un service d'adressage unique pour l'ensemble des terminaux connectés.

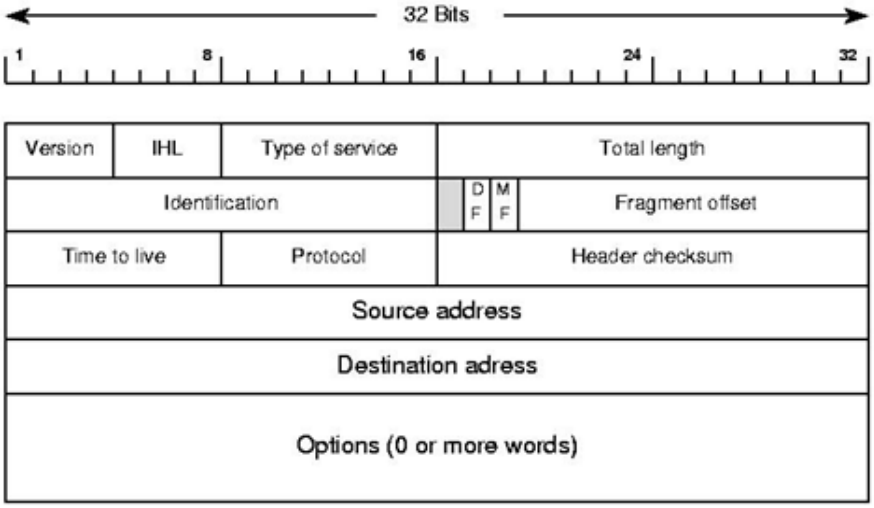


FIGURE 10 – Structure d'un datagramme IP

.3.1 Quelques détails de datagramme IP

- **Version (4 bits) :** renseigne sur le format de l'en-tête internet. Internet Header.
- **Length (4 bits) :** code la longueur de l'en-tête l'unité étant le mot de 32 bits.
- **Type Of Service (8 bits) :** donne une indication sur la qualité de service souhaitée, qui reste cependant un paramètre "abstrait". Le "Type de Service" sert à préciser le traitement effectué sur le datagramme pendant sa transmission à travers Internet.
- **Total Length (16 bits) :** c'est la longueur du datagramme entier y compris en-tête et données.
- **Identification (16 bits) :** chaque paquet IP reçoit un numéro d'identification à sa création. Il est possible qu'un paquet soit découpé en fragments avant d'atteindre sa destination finale. Chaque fragment appartient au même paquet IP. Chaque fragment possède le même numéro d'identification.

.4 Protocole ARP

Est l'acronyme de " Address Resolution Protocol ", la figure suivante montre la stucture de la trame ARP.

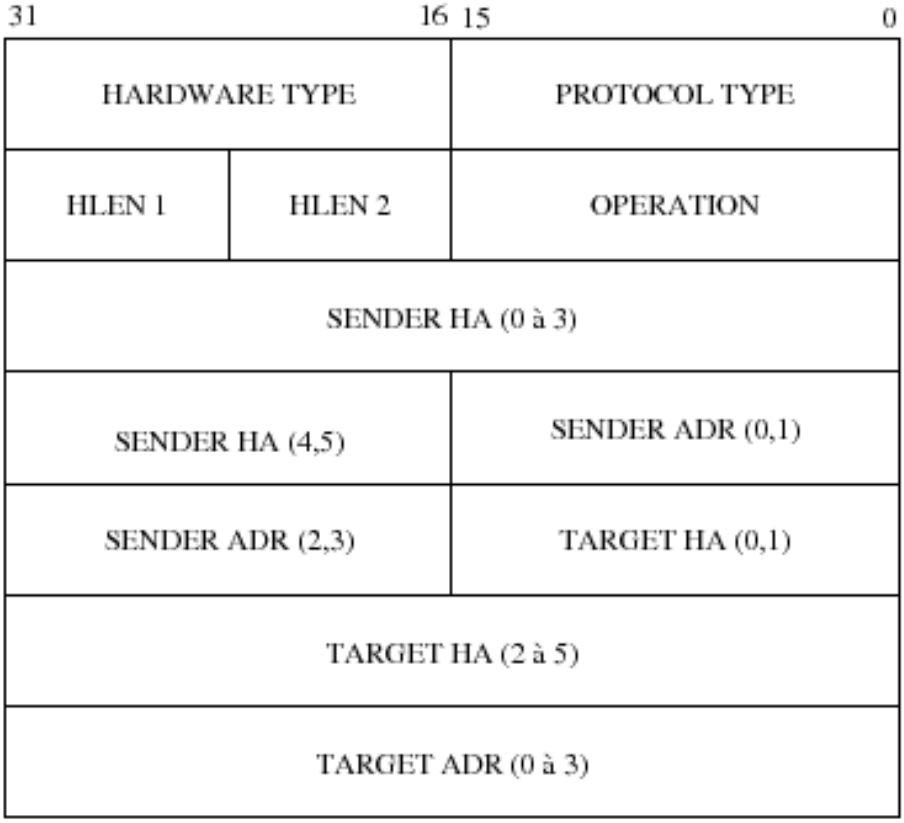


FIGURE 11 – Datagramme ARP

.5 Protocole ICMP

Le protocole ICMP (pour Internet Control Message Protocol) est le protocole de signalisation des problèmes utilisé par le protocole IP. Son but est de tester la connectivité réseau mais aussi d'apporter une aide au diagnostic en cas de problèmes ou de défaillances.

Le format général d'un paquet ICMP est le suivant :

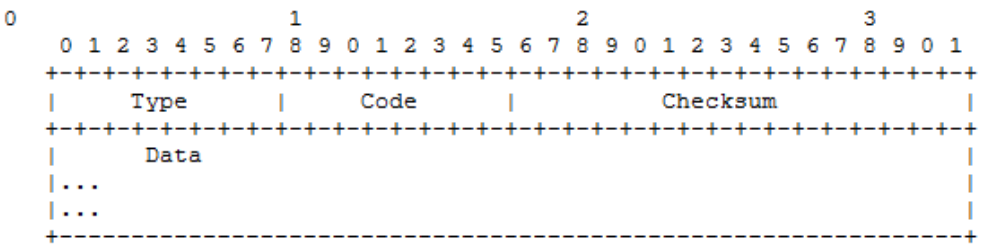


FIGURE 12 – Datagramme ICMP

Les différents champs que l'on peut trouver sont les suivants :

- **le champ "Type" :** correspond au type de message ICMP.
- **le champ "Code" :** sert à affiner le type du message ICMP.
- **le champ "Checksum" :** est la somme de contrôle. Ce champ est le complément à 1 sur 16 bits de la somme des compléments à 1 des octets de la trame ICMP en commençant par le champ Type ICMP. Lors du calcul de ce champ, celui-ci est initialisé à zéro
- **le champ "Data"** contient les données du message ICMP. L'interprétation de son contenu doit se faire en fonction du type de message ICMP.

Annexe B

.6 L'adresse IPv4

IPv4 (Internet Protocol version 4) est la première version d'Internet Protocol (IP) à avoir été largement déployée, et qui forme encore en 2013 la base de la majorité des communications sur Internet, avec l'IPv6. Elle est décrite dans la RFC 791 de septembre 1981, remplaçant la RFC 760, définie en janvier 1980.

Chaque interface d'un hôte IPv4 se voit attribueé une ou plusieurs adresses IP codées sur 32 bits. Au maximum 4 294 967 296 soit 232 adresses qui peuvent donc être attribuées simultanément en théorie (en pratique, un certain nombre ne sont pas utilisables).

L'épuisement des adresses IPv4 a conduit au développement d'une nouvelle version d'IP, IPv6, et à la transition d'IPv4 vers IPv6 afin d'adopter cette nouvelle version. Le manque d'adresse IPv4 est dans un premier temps contourné grâce à l'utilisation de techniques de traduction d'adresses (NAT) ainsi que par l'adoption du système CIDR.

.6.1 Représentation d'une adresse IPv4

Une adresse IPv4 est représentée sous la forme de quatre nombres décimaux séparés par des points comme par exemple 193.43.55.67. Chacun des nombres représente un octet. Pour généraliser, la plage attribuable va donc de 0.0.0.0 à 255.255.255.255 si on fait abstraction des contraintes techniques du protocole (adresse réservée, attribuée...).

En-tête IPv4

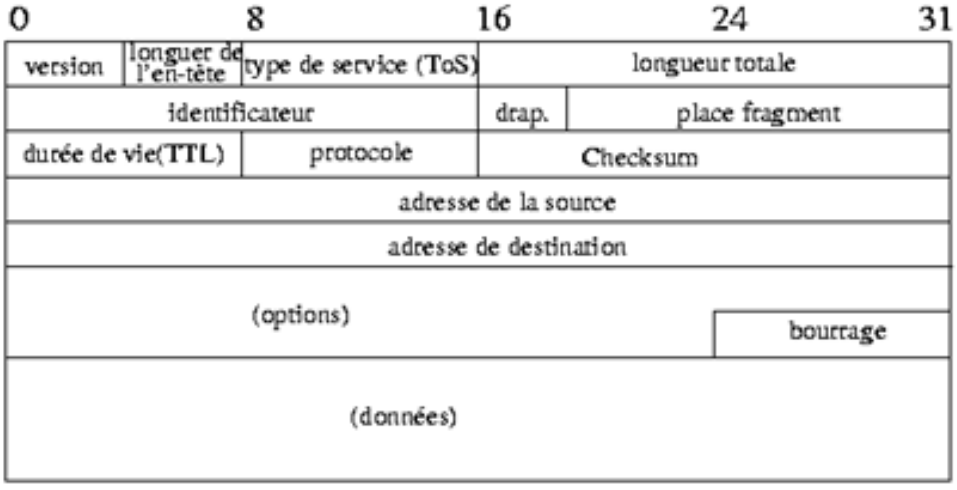


FIGURE 13 – Format d'un datagramme IPv4

- **Version (4 bits) :** Version d'IP utilisée. Ici, 4.

- **Longueur de l'en-tête ou IHL (pour Internet Header Length) (4 bits) :** Nombre de mots de 32 bits, soit 4 octets (ou nombre de lignes du schéma). La valeur est comprise entre 5 et 15, car il y a 20 octets minimum et on ne peut dépasser 40 octets d'option (soit en tout, 60 octets).

- **Type de service ou ToS (pour Type of Service) (8 bits) :** Ce champ permet de distinguer différentes qualité de service différenciant la manière dont les paquets sont traités. Composé de 3 bits de priorité (donc 8 niveaux) et trois indicateurs permettant de différencier le débit, le délai ou la fiabilité.

- **Identification (16 bits) :** Numéro permettant d'identifier les fragments d'un même paquet.

- **Indicateurs ou Flags (3 bits) :**

  - (Premier bit) actuellement inutilisé.

  - (Deuxième bit) DF (Don't Fragment) : lorsque ce bit est positionné à 1, il indique que le paquet ne peut pas être fragmenté. Si le routeur ne peut acheminer ce paquet (taille du paquet supérieure à la MTU), il est alors rejeté.

  - (Troisième bit) MF (More Fragments) : quand ce bit est positionné à 1, on sait que ce paquet est un fragment de données et que d'autres doivent suivre. Quand il est à 0, soit le fragment est le dernier, soit le paquet n'a pas été fragmenté.

- **Fragment offset (13 bits) :** Position du fragment par rapport au paquet de départ, en nombre de mots de 8 octets.

- **Durée de vie ou TTL (pour Time To Live) (8 bits) :** Initialisé par l'émetteur, ce champ est décrémenté d'une unité généralement à chaque saut de routeur. Quand TTL = 0, le paquet est abandonné et un message ICMP est envoyé à l'émetteur pour information.

- **Protocole (8 bits) :** numéro du protocole au-dessus de la couche réseau : TCP = 6, UDP = 17, ICMP = 1. Ce champ permet d'identifier le protocole utilisé par le niveau supérieur :

  - Internet Control Message Protocol où ICMP est repéré par les bits 00000001, qu'on écrit souvent en hexadécimal avec 01
  - Transmission Control Protocol ou TCP par les bits 00000110, soit 06

  - User Datagramme Protocol ou UDP par les bits 00010001, soit 17 en décimal

- **Somme de contrôle de l'en-tête ou Header Checksum (16 bits) :** Complément à un de la somme complémentée à un de tout le contenu de l'en-tête afin de détecter les erreurs de transfert. Si la somme de contrôle est invalide, le paquet est abandonné sans message d'erreur.

- **Adresse source (32 bits) :** Adresse IP de l'émetteur sur 32 bits.

- **Adresse destination (32 bits) :** Adresse IP du récepteur 32 bits.

- **Options (0 à 40 octets par mots de 4 octets) :** Facultatif.

- **Remplissage ou Padding :** Champ de taille variable comprise entre 0 et 7 bits. Il permet de combler le champ option afin d'obtenir un en-tête IP multiple de 32 bits. La valeur des bits de bourrage est 0.

.7 Classification des adresses IP

Il existe quatre classe d'adresses IP, mais la derniere elle réservée à un usage ultérieur. Le tableau suivant montre les differentes classes d'adresse IP.

Classe	Bits de départ	Début	Fin	Notation CIDR	Masque
Classe A	0	0.0.0.0	127.255.255.2552	8	255.0.0.0
Classe B	10	128.0.0.0	191.255.255.255	/16	255.255.0.0
Classe C	110	192.0.0.0	223.255.255.255	24	255.255.255.0
Classe D	1110	224.0.0.0	239.255.255.255	/8	non défini
Classe E	1111	240.0.0.0	255.255.255.255		non défini

TABLE 1 – Classification des adresses IP

.8 Les masques de sous-réseau

Un réseau muni d'une adresse de classe quelconque, le gestionnaire du réseau peut le découper en sous-réseau afin de créer des entités plus petites et plus nombreuses. On peut donc créer des sous-réseaux dans ce même réseau (même domaine d'adressage logique)

Par exemple un sous-réseau pour les administrateurs, un sous réseau pour un service comptable, un autre pour le pôle production d'une entreprise ...

Ce ci permet de définir des entités plus petites où le flux des donées est séparé (meilleure sécurité) et optimisé.

Le masque sous-réseau par défaut se forme en positionnant tous les bits concernant la partie réseau de l'adresse logique à 1.les autre bits, ceux concernant la partie machine auront leurs bits à 0 (voir table).

Classe	1er octet	2eme octet	3eme octet	4eme octet
Classe A	255		0	0
Classe B	255	255	0	0
Classe C	110	255	255	255

TABLE 2 – Masque de sous-réseau par défaut pour les classes A, B et C

Annexe C

.9 Le standard IEEE 802.1Q

IEEE 802.1Q est un mécanisme d'étiquetage VLAN (norme ouverte IEEE) dans les installations de commutation. Le format de la trame Ethernet modifiée avec les 4 octets supplémentaires est présenté ci-dessous.

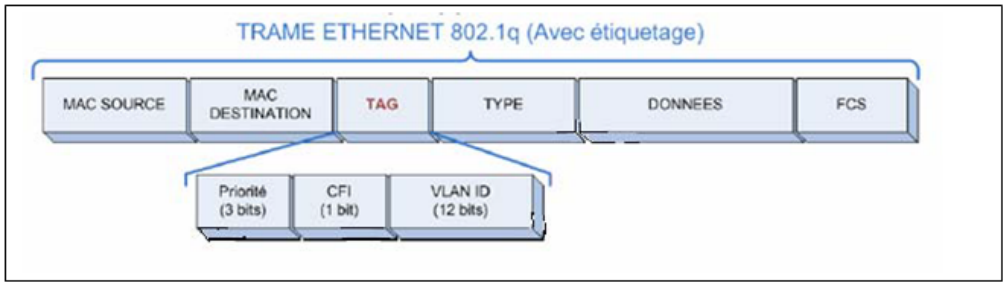


FIGURE 14 – L'encapsulation de la trame Ethernet par 802.1Q

Priorité

Ce champ de 3 bits fait référence au standard IEEE 802.1p1. Sur 3 bits on peut coder 8 niveaux de priorités de 0 à 7. Ces niveaux sont utilisés pour fixer une priorité aux trames d'un VLAN relativement aux autres VLANs. (Exemple d'utilisation : on favorise un VLAN sur lequel on utilise la visioconférence (nécessitant beaucoup de bande passante) par rapport à un VLAN où l'on ne fait qu'envoyer et recevoir des mails).

CFI (Canonical Format Identifier)

Ce champ codé sur 1 bit assure la compatibilité entre les adresses MAC Ethernet et Token Ring. Un commutateur Ethernet fixera toujours cette valeur à 0. Si un port Ethernet reçoit une valeur 1 pour ce champ, alors la trame ne sera pas propagée puisqu'elle est destinée à un port "sans balise".

VID (VLAN identificateur)

Ce champ de 12 bits sert à identifier le réseau local virtuel auquel appartient la trame. Il est possible de coder VLANs avec ce champ

Annexe D

.10 Commandes de base pour commutateur Cisco CATALYST

.10.1 Connexion console au démarrage

Pour la connexion de la console de commutateur, il faut utiliser un câble null modem et utiliser une console ou un émulateur de terminal comme le cas d'utilisation d'HyperTerminal sous Windows.

.10.2 Connexion en mode privilèges

```
Switch>enable
Password :
Switch#
```

.10.3 Suppression du fichier d'informations de la base de données

```
Switch # delete flash :vlan.dat
```

.10.4 Suppression de la configuration de démarrage

```
Switch # erase startup-config ou Switch # erase nvram
```

.10.5 Entrer en mode configuration

```
Switch #configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch (config) #
```

.10.6 Changement de l'adresse IP du Switch

Switch #configure terminal

Utiliser le vlan par défaut (vlan 1) : Switch (config)#interface vlan1

Adresse du commutateur et son masque de sous réseau :

Switch (config-if) #ip address 10.136.0.1 255.255.255.0

Sortir de l'interface vlan 1 :

Switch (config-if) # exit

Ajouter la passerelle par défaut pour le vlan 1

Switch (config) # ip default-gateway 10.136.0.1

Pour revenir en mode privilege

Switch (config) # end

Switch A#

Pour sauvegarder la configuration

Switch # copy running-config startup-config

Destination filename [startup-config] ?

Building configuration...

OK

Switch A#

.10.7 Afficher la configuration du commutateur

a. Afflicter la configuration courante

Switch # show running-config

b. Afficher la configuration utilisée au démarrage

Switch #show startup-config

.10.8 Afficher les informations concernant les VLANs

Switch #show vlan OU Switch #show vlan brief

.10.9 Afficher les informations concernant le protocole VTP

```
Switch #show vtp status
```

.10.10 Pour enlever un VLAN entièrement d'un commutateur

```
Switch # vlan database
Switch (vlan) #no vlan 3
```

.10.10.1 Connexion en mode privilèges

```
Router>enable
```

Pour attribuer un nom au routeur :

```
Router # config t
Router (config) # hostname R1
R1 (config)#
```

.10.10.2 Activer une interface du routeur

```
R1 (config) #interface FastEthernet0/1
R1 (config-if) #no shutdown
```

.10.10.3 Afficher la table de routage

```
R1#show ip route
```

.10.10.4 Afficher les informations sommaires sur la configuration d'une interface

```
R1#show ip interface brief
```

Bibliographie

[1] **Pascal Nicolas**, *"Cours de réseaux,Université d'Anger "*, Web.www.inf.univ-Angers.fr/pub/pn.
.

[2] **Gerardo RUBINO** et **Laurent TOUTAIN** , *"Réseaux locaux "*, Ecole Nationale Supérieure des télécommunications de Bretagne, Campus de rennes.

[3] **Khelalfa, Halim M**,*"Introduction à la sécurité informatique "*, Laboratoire des Logiciels de Base Session, L'année 2002.

[4] **Pierre Erny** , *"rapport de recherche"*, LES RESEAUX INFORMATIQUES D'ENTREPRISE ,1998.

[5] **David TILLOY**, *"David TILLOY"*, Support de cours Réseaux et Télécom, 1998/1999, livre.

[6] **Olivier Hoarau** , *"Introduction aux réseaux locaux et étendus"*. http ://funix.free.fr 2000.

[7] **Cédric Lorens**, *"Informatique et Réseau d'un opérateur de télécommunication"*.

[8] **TOM Thomas**, *"La sécurité des réseaux "* , " first-step", ISBN : 2-7440-17868,2005.

[9] **Frédéric Jacqueuned** , *"Cours Réseaux N5 : les matériels d'interconnexion"*.

[10] **Adello ALTUNAIJI**et **All** , *"Mise en place d'un réseau sécurisé sous Linux "*, université Claude Bernard Ly on 1, France, Novembre 2002.

[11] **André Perez**, *"Architecture des réseaux de télécommunications "*, Hernes sciences Publications, 2002.

[12] **Marc BOGET** , *"étude des vulnérabilités d'un grand réseau d'entreprise et solution de sécurité"*, Mastère SIO 2003.

[13] **S. Bouamet J.Ben-Othman**, *"Protocole de Sécurisation des données à base de routage dans les réseaux ADHOC"*, Université de Versailles, 2004.

[**14**]*"Le grand livre de sécurité informatique"*, http ://www.sécuriteinfo.com,05/06/2009.

[**15**] **Gouy Pujolle**, *"Initiation aux réseaux "*, cours et exercices, 1ère édition Eyrolles, 2003.

[**16**] **Christophe WOLFHUGEL**, *"Déploiements de VLANs 802.1Q/ISL environnement hétérogène, France Telecom Oléane"*.

[**17**] **Jean Luc Montagnier**, *" pratique des réseaux d'entreprise"*, Eyrolles, 1999.

[**18**] **Walid BAGGA**, *"Policy-Based, Cryptography : Théorie and Applications"*,Ecole Nationale Supérieure des Télécommunications, 2006.

[**19**] **Eric BERTHOMIER**, *"Formation Sécurité des Réseaux"*, 2005.

[**20**] **Génail VALET**, *"les LANs virtuels (VLANs)"*, Greta industriel des technologies avancées Greta.

[**21**] **Stephan Natkin**, *"Les protocoles de Sécurité d'internet"*, DUNOD Science SUP, mai 2002.

[**22**] **Guillaune Des george**, *"la Sécurité des réseaux"*, 2000.

[**23**] **Yves Deswarte** et **Ludovic Mé** , *"Sécurité des réseaux et systèmes répartis"*, 2002.

[**24**] **Ignace LAURENT SUPRINO** , *"La theories des VLANs"*,(www.supinfoproject. Com/fr).

[**25**] **P. Zanella** et**Y.Liger**, *"livre sur Architecture et technologie des ordinateurs"*,1 ère édition : 1 ère trimestre, 1989 .

[**26**] **J. Pierre Arnaud**, *"livre sur Réseaux et Télécoms"*,université Paris, 2003 .