الجمهورية الجزائرية الديمقراطية الشعبية

République Algérienne Démocratique et Populaire

Ministère de l'enseignement supérieur et de la recherche scientifique

Université de 8 Mai 1945 – Guelma -

Faculté des Mathématiques, d'Informatique et des Sciences de la matière

Département d'Informatique

Mémoire de Fin d'études Master

Filière : Informatique

Option : Ingénierie des Medias

Thème :

Outils d'aide à la construction, l'administration et le troubleshooting des réseaux des moyennes entreprises.

Encadré Par :

Rabah LEBSIR

Présenté par :

Said CHIHEB,

Djeweyda BELHACENE

Juin 2016

Je dédie ce mémoire

À la mémoire de mon père à ma mère pour leur soutien tout au long de mes études

À mes sœurs et mon frère

Nadia, Ahlem, hamza

A Ma nièce aya

À toute ma famille

À tout mes amis et amies

Et à tous ceux qui m'ont encouragé

DJAOUIDA.

Je dédie ce mémoire

À la mémoire de ma mère à mon cher père à ma chère grand-mère

Pour leur soutien tout au long de mes études

À mon frère Seddik

À mon oncle Zakaria

À toute ma famille

À tous mes chères

À tous mes amis

Et à tous ceux qui m'ont encouragé

SAID.

Remerciements

*En premier lieu et avant tout nous tenons à exprimer nos remerciements au bon « **Dieu** » qui nous a entouré de sa bienveuillance et nous a renforcé avec le courage et la force pour avoir enfin mené à bien ce travail.*

Ensuite, nous exprimons notre profonde gratitude à notre encadreur **Mr RABAH LEBSIR** *pour avoir acceptée de nous suivre, et nos plus vifs remerciements pour son soutien, sa patience, ses conseils judicieux, pertinents, et sa sympathie dont il nous a fait preuve tout au long de l'élaboration de ce travail.*

Nous adressons également nos remerciements, à tous nos enseignants, qui nous ont donné les bases de la science, nous remercions très sincèrement, les examinateurs pour nous avoir fait l'honneur d'évaluer notre travail.

Nos pensées se tournent maintenant vers ***nos parents, nos familles et nos proches*** *qui nous ont entourés par la tendresse et l'amour dévoué depuis notre enfance. Merci de votre soutien de tous les jours et nous espérons que vous soyez aussi fiers de nous que nous le sommes de vous.*

Et finalement à tous ceux qui nous ont aidés de près ou de loin à accomplir ce travail nous disons Merci.

SAID DJEWEYDA

RÉSUMÉ

La construction, l'administration ainsi que le troubleshooting des réseaux de communication pour des moyennes entreprises reste un défi pour les ingénieurs ainsi que les stagiaires dans le domaine des réseaux informatiques à cause de l'abstraction et non visualisation du phénomène ni de la configuration. Afin de pallier à ce problème, beaucoup de solutions ont été proposées, ce qui a créé une nécessité de classification et de comparaison entre ces outils et mettre l'accent sur les avantages et les inconvénients de chaque solution.

Dans ce mémoire, et avec un exemple concret, on va présenter les étapes nécessaires ainsi que les outils qui peuvent être utiles pour la création d'un réseau d'une moyenne entreprise qui soit performant, tolérant aux pannes, facile à maintenir et sécurisé, en passant par une architecture à trois niveaux et en utilisant le modèle TCP/IP comme référence pour la configuration de différents protocoles.

Mots clés : topologie, OSI, TCP/IP, routage, troubleshooting, commutation, simulation et émulation, sécurité.

Table des matières

Table des matières

Liste des figures

Liste des figures

Liste des tableaux

Liste des tableaux

Liste des Abréviations et Acronymes

Liste des Abréviations et Acronymes

ACL: Access Control List.

ARP: Address Resolution Protocol.

CLI: Command Line Interface.

CSMA/CA: Carrier Sense Multiple Access/Collision Avoidance.

DHCP: Dynamic host configuration Protocol.

DNS: Domain Name System.

FTP: File Transfer Protocol.

HTTP: Hypertext Transfert Protocol.

ICMP: Internet Control Message Protocol.

IEEE: Institute of Electrical and Electronics Engineers.

IP : Internet Protocol.

ISO : Organisation internationale de normalisation.

LAN: Local Area Network.

MAC: Media Access Control address.

MAN: Metropolitan Area Network.

NAT: Network Address Translation.

OSI: Open Systems Interconnexion.

PAN: Personal Area Network.

PAT: Port Address Translation.

PPP: Point to Point Protocol.

SMTP: Mail Transfert Protocol SMTP.

SSH: Secure Shell.

TCP: transmission control protocol.

UDP: unit data protocol.

VLAN: Virtual Local Area Network.

VPN: Virtual Private Network.

WAN: Wide Area Network.

WCCP : Web Cache Communication Protocol.

Introduction générale

Introduction Générale

Un réseau informatique d'une moyenne entreprise doit satisfaire plusieurs critères tels que la disponibilité, la tolérance aux pannes et la sécurité. Pour satisfaire ces conditions, plusieurs outils et techniques peuvent être utilisés lors de l'étude et la maintenance du réseau.
Dans ce mémoire, on va présenter les notions de base des réseaux informatiques, et par un cas pratique, les outils d'aide à la construction, l'administration et le troubleshooting des réseaux des moyennes entreprises. Aussi comment peut-on suivre un modèle de communication dans la phase de construction afin d'assurer un réseau qui est tolérant aux pannes et qui soit sécurisé.

Organisation du travail :

Ce mémoire est composé de quatre chapitres Le premier chapitre concerne la présentation du réseau informatiques auxquels on parle brièvement quelques notions théoriques utiles comme la définition d'un réseau, les topologies existantes ainsi que les modèles de communication les plus utilisés. Le second chapitre porte sur la sécurité des réseaux en va parler des dangers encourus et les solutions existantes pour faire une bonne défense contre les attaques. D'autre part nous abordons dans un troisième chapitre les outils de simulation et émulation les plus utilisés dans le domaine des réseaux. Le quatrième chapitre, la conception du modèle dont la procédure de préparation, la schématisation, nomination des équipements, désignation des interfaces, les Vlans, le plan d'adressage et la présentation des protocoles utilisés. Enfin nous terminons par la réalisation du modèle type à travers le simulateur « GNS3 », ainsi le test et la validation de la configuration.

Chapitre I : Présentation des réseaux

I. Présentation des réseaux

I.1. Introduction :

Dans nos jours, toutes les moyennes entreprises utilisent le partage des données et informations entre ses différentes unités et services. Les réseaux informatiques des moyennes entreprises sont nés de ce besoin. Dans ce chapitre on va présenter d'une façon générale les réseaux informatiques.

I.2. Définition d'un réseau informatique :

Selon Andrew Tanenbaum (1), nous pouvons définir un réseau informatique comme étant un ensemble de deux ou plusieurs ordinateurs interconnectés entre eux au moyen des médias de communication avec pour objectifs de réaliser le partage des différentes ressources matérielles et/ou logicielles.
Donc on peut définir un réseau informatique par le résultat de la connexion de plusieurs appareils afin d'échanger des informations.

I.3. Types des réseaux informatiques :

Il existe différentes sortes de réseaux, La (Figure I-1) présente plusieurs systèmes classés en fonction de leurs tailles approximatives. On trouve en premier lieux le réseau personnel ou PAN (Personal Area Network), destiné à une seule personne. Ensuite les réseaux opérant sur de plus longues distances, qui se répartissent en trois catégories : les réseaux locaux ou LAN (Local Area Network), les réseaux métropolitains ou MAN (Metropolitan Area Network) et les réseaux étendus ou WAN (Wide Area Network), leurs tailles augmentent à chaque fois. Enfin, l'interconnexion de plusieurs réseaux s'appelle un inter-réseau, et l'Internet qui fonctionne à l'échelle mondiale, est l'exemple le plus connu d'inter-réseaux. (2)

Distance entre processeurs	Emplacement des processeurs	Exemple
1 m	Un mètre carré	Réseau personnel
10 m	Une salle	Réseau local
100 m	Un immeuble	
1 km	Un campus	
10 km	Une ville	Réseau métropolitain
100 km	Un pays	Réseau longue distance
1 000 km	Un continent	
10 000 km	Une planète	Internet

Figure I-1 *: Classification des réseaux d'après leur taille. (2)*

I.3.1. Le réseau personnel (PAN) :

Les réseaux personnels, ou PAN (Personal Area Networks), permettent aux équipements de communiquer à l'échelle individuelle. Un exemple courant est celui du réseau sans fil, qui relie un ordinateur à ses périphériques. Pratiquement tous les ordinateurs s'accompagnent d'un moniteur, d'un clavier, d'unc souris et d'une imprimante.

Une des technologies utilisées aussi pour éviter tout câblage à ce niveau est le Bluetooth, donc il suffit de connecter des périphériques tels que la souris, le clavier ou même un Smartphone à un ordinateur et cela va créer un réseau PAN (Figure I-2). (2)

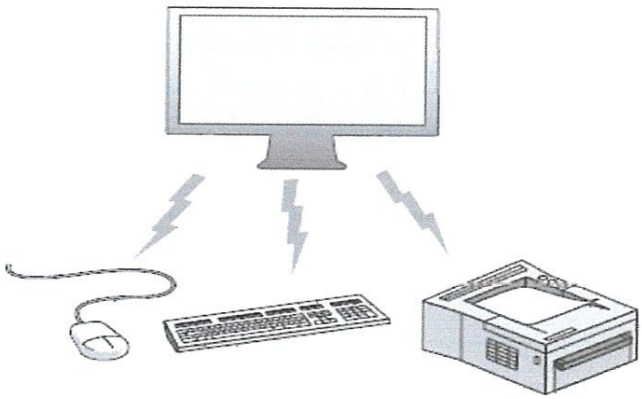


Figure I-2 *: Configuration d'un réseau personnel Bluetooth. (2)*

I.3.2. Le réseau local (LAN) :

Les réseaux locaux, ou LAN (Local Area Networks) sont des réseaux privés, qui fonctionnent dans un seul bâtiment (ou à proximité), comme une maison, un immeuble de bureaux ou une usine. Ils sont fréquemment utilisés pour relier des ordinateurs personnels et des équipements électroniques grand public (par exemple des imprimantes) pour leur permettre de partager des

ressources et d'échanger des informations. Quand ils sont employés par des organisations, on parle de réseaux d'entreprise.

Les LAN sans fil sont très répandus dans nos jours, surtout dans les habitations, les bureaux dans les anciens immeubles, les cafétérias et autres lieux où l'installation de câbles poserait trop de problèmes. Dans ces systèmes, chaque ordinateur dispose d'une carte réseau sans fil pour communiquer avec les autres équipements (Figure I-3). (2)

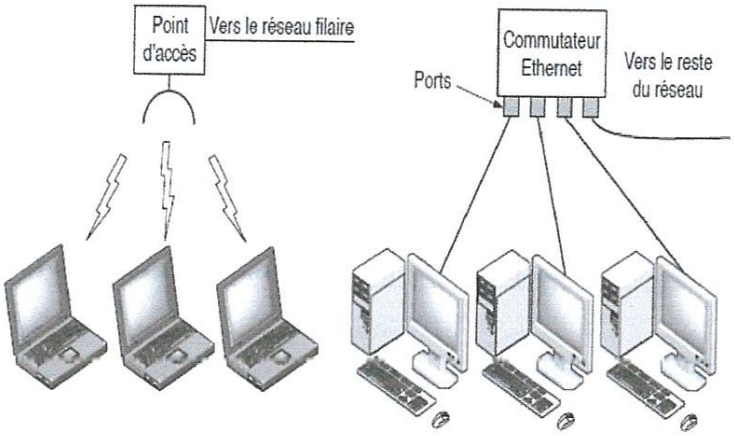


Figure I-3 : *LAN sans fil et filaires. (a) 802.11. (b) Ethernet commuté. (2)*

Il existe pour les LAN sans fil une norme appelée IEEE 802.11, plus connue sous le nom de Wi-Fi, qui est maintenant très répandue. Elle permet des débits d'un à plusieurs centaines de mégabits par seconde.

Les LAN filaires font appel à différentes technologies de transmission. La plupart d'entre elles utilisent du fil de cuivre. Connaître ces restrictions est utile pour la conception des protocoles réseau. Généralement, les LAN filaires offrent des débits de 100 Mbit/s à 1 Gbit/s, un faible délai (de l'ordre de quelques microsecondes ou nanosecondes) et connaissent très peu d'erreurs. Les plus récents peuvent atteindre 10 Gbit/s. Leurs performances sont supérieures en tout point à celles des réseaux sans fil : il est tout simplement plus facile de faire voyager des signaux sur du cuivre ou de la fibre que par voie aérienne. La topologie de nombreux LAN filaires est construite à partir de liens point-à-point. La norme IEEE 802.3, plus connue sous le nom d'Ethernet, est de loin la plus courante pour les LAN filaires. (2)

I.3.3. Le réseau métropolitain(MAN) :

Un réseau métropolitain, ou MAN (Metropolitan Area Network), couvre une ville (Figure I-4). L'exemple le plus connu de MAN est le réseau de télévision. Celui-ci a évolué à partir de

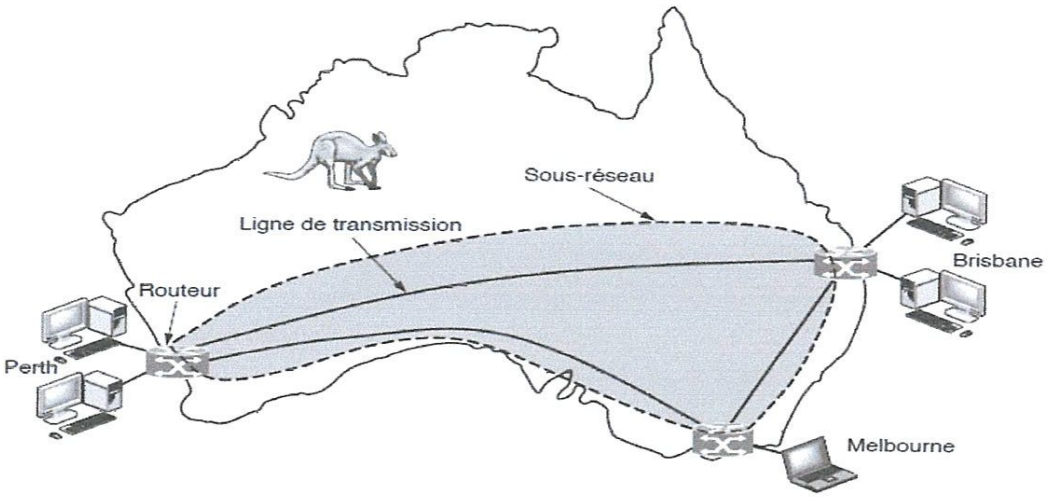


Figure I-5 : *WAN connectant des filiales en Australie. (2)*

Le WAN tel que nous l'avons décrit peut sembler analogue à un grand LAN filaire, mais il présente des différences importantes qui dépassent la question de la longueur des câbles. Généralement, dans un WAN, des personnes différentes possèdent et gèrent les hôtes et le sous-réseau.

Deuxième différence, les routeurs connecteront généralement des réseaux utilisant différents types de technologies. Par exemple, les réseaux internes aux filiales peuvent être en Ethernet commuté, alors que les lignes de transmission longue distance peuvent être des liens SONET[1]. Des équipements doivent leur permettre de communiquer.

Enfin, une dernière différence tient à la nature des éléments connectés. Il peut s'agir d'ordinateurs individuels, comme dans le cas des LAN. C'est ainsi que l'on construit des grands réseaux à partir de plus petits. En ce qui concerne les sous-réseaux, leur rôle est identique.

D'autres types de WAN utilisent intensivement les technologies sans fil. Le réseau téléphonique cellulaire est un exemple de WAN qui s'appuie sur une technologie sans fil. Ce système a déjà connu quatre générations. La première génération était analogique et ne transportait que la voix. La deuxième était numérique, mais toujours dédiée uniquement à la voix. La troisième génération, numérique aussi, a ajouté le transport de données. Chaque station de base couvre une distance beaucoup plus importante qu'un LAN sans fil, avec une portée mesurée en kilomètres et non en dizaines de mètres. Les stations sont connectées entre elles par un réseau

[1] Synchronous Optical Network : c'est un modèle de norme de transmission optique. C'est un protocole de la couche 1 du modèle OSI.

fédérateur (backbone). Les réseaux cellulaires ont un débit de l'ordre de 1 Mbit/s, donc très inférieur à celui d'un LAN sans fil qui peut atteindre 100 Mbit/s. (2)

I.3.5. Autres classifications :

Dans l'une des classifications le critère organisationnel prédomine. Si le réseau est accessible à tous, il est alors dit public , s'il n'est qu'à une communauté d'utilisateurs appartenant à une même organisation, il est alors dit privé. Un réseau public peut être géré par une personne privée (opérateur de télécommunication de droit privé), et un réseau privé peut être sous la responsabilité d'une personne de droit public (réseau d'un ministère...). Un réseau privé est dit virtuel lorsqu'à travers un réseau public on simule (émule) un réseau privé.

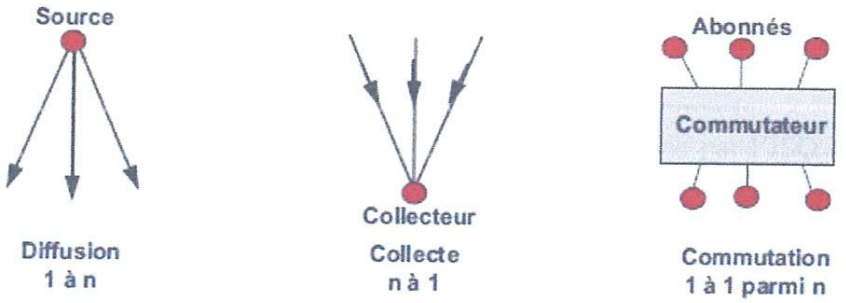


Figure I-6 : *Classification selon les modes de diffusion de l'information. (3)*

Les réseaux se différencient, aussi, selon les modes de diffusion de l'information (Figure I-6). On distingue trois modes :

La source diffuse ses informations vers des stations réceptrices. La relation est unidirectionnelle de 1 à N (réseau de diffusion). Les réseaux de radiodiffusion constituent un exemple de ce type de réseau.

À l'inverse, un ensemble de stations peut envoyer les informations à un seul destinataire. La relation est aussi unidirectionnelle, mais de N à 1 (réseaux de collecte). Les réseaux de Télémesure constituent un exemple de ce mode de fonctionnement.

D'une manière plus générale, un abonné d'un réseau désire pouvoir atteindre tous les autres abonnés ou une partie de ceux-ci. Le réseau doit établir une relation de 1 à 1 parmi N. Ces réseaux, de mise en relation, sont dits réseaux de commutation, le réseau téléphonique (RTC) en est un exemple. (3)

- Routage : la couche réseau fournit des services permettant de diriger les paquets vers un hôte de destination sur un autre réseau. Pour voyager vers d'autres réseaux, le paquet doit être traité par un routeur. Le rôle du routeur est de sélectionner les chemins afin de diriger les paquets vers l'hôte de destination. Ce processus est appelé le routage. Un paquet peut passer par de nombreux périphériques intermédiaires avant d'atteindre l'hôte de destination. Chaque route que le paquet emprunte pour atteindre l'hôte de destination est appelée un saut.
- Décapsulation : lorsque le paquet arrive au niveau de la couche réseau de l'hôte de destination, l'hôte vérifie l'en-tête du paquet IP. Si l'adresse IP de destination dans l'en-tête correspond à l'adresse IP de l'hôte qui effectue la vérification, l'en-tête IP est supprimé du paquet. Ce processus de suppression des en-têtes des couches inférieures est appelé la décapsulation. Une fois la décapsulation effectuée par la couche réseau, la PDU de couche 4 est transmise au service approprié au niveau de la couche transport. (4)

Il existe plusieurs protocoles de couche réseau. Cependant, les deux protocoles les plus utilisés sont Le protocole IP version 4 (IPv4) et Le protocole IP version 6 (IPv6). Il existe d'autres protocoles de couche réseau peu utilisés comme :

- Novell Internetwork Packet Exchange (IPX)
- AppleTalk
- Connectionless Network Service (CLNS/DECNet).

ii.3.1. Le protocole IP version 4 (IPv4) :

C'est la première version d'Internet Protocol (IP) qui encore restent en fonctions et forme jusqu'à nos jour la base de la majorité des réseaux internet communications sur Internet, donc L'adresse IPv4 indique la localisation de la machine dans l'Internet.

A. Le format des adresses IP :

Les adresses IP sont composées de 4 octets. Par convention, on note ces adresses sous forme de 4 nombres décimaux de 0 à 255 séparés par des points. (5)

B. Le masque de réseau :

Le masque de réseau sert à séparer les parties réseau et hôte d'une adresse. On retrouve l'adresse du réseau en effectuant un ET logique bit à bit entre une adresse complète et le masque de réseau.

C. L'adresse de diffusion (broadcast) :

Cette adresse est utilisée quand on veut contacter toutes les machines du réseau.
Les trames Ethernet ne sont pas filtrées par les Switches et cela donne une pollution du réseau.
L'adresse de diffusion est l'adresse où tous les bits machines sont mis à 1 (pour l'adresse réseau tous les bits machine sont à 0).
Pas de calcul en binaire, il suffit d'appliquer la règle ci-dessous.
Faire : 255 – masque = reste
Puis : adresse réseau + reste = adresse de diffusion. (6)

D. Les classes d'adresses :

À l'origine, plusieurs groupes d'adresses ont été définis dans le but d'optimiser le cheminement (ou le routage) des paquets entre les différents réseaux. Ces groupes ont été baptisés classes d'adresses IP.
Ces classes correspondent à des regroupements en réseaux de même taille. Les réseaux de la même classe ont le même nombre d'hôtes maximum. (5)
Les classes les plus utilisé sont les classes : A, B, C.
Classe A : Le premier octet a une valeur comprise entre 1 et 126 ; soit un bit de poids fort égal à 0. Ce premier octet désigne le numéro de réseau et les 3 autres correspondent à l'adresse de l'hôte. (5)
Classe B : Le premier octet a une valeur comprise entre 128 et 191 ; soit 2 bits de poids fort égaux à 10. Les 2 premiers octets désignent le numéro de réseau et les 2 autres correspondent à l'adresse de l'hôte. (5)
Classe C : Le premier octet a une valeur comprise entre 192 et 223 ; soit 3 bits de poids fort égaux à 110. Les 3 premiers octets désignent le numéro de réseau et le dernier correspond à l'adresse de l'hôte. (5)

Classe D : Le premier octet a une valeur comprise entre 224 et 239 ; soit 3 bits de poids fort égaux à 111. Il s'agit d'une zone d'adresses dédiées aux services de multidiffusion vers des groupes d'hôtes (host groups). (5)
Classe E : Le premier octet a une valeur comprise entre 240 et 255. Il s'agit d'une zone d'adresses réservées aux expérimentations. Ces adresses ne doivent pas être utilisées pour adresser des hôtes ou des groupes d'hôtes. (5)

ii.4. La couche Transport :

La couche transport assure un transfert de données transparents entre entités en les déchargeant des détails d'exécution. Elle a pour rôle d'optimiser l'utilisation des services réseaux disponibles afin d'assurer au moindre coût les performances requises par la couche session.
C'est une couche intermédiaire qui se définit par la notion de Qualité de Service
(Q & S). La qualité est évaluée sur certains paramètres avec trois types de valeurs possibles : préféré, acceptable et inacceptable qui est choisis lors de l'établissement d'une connexion. La couche transport surveille alors ces paramètres pour déterminer si la couche réseau sous-jacente assure la qualité de service demandée. (7)
Les deux protocoles de couche transport : TCP (Transmission Control Protocol) et UDP (User Datagram Protocol).

ii.4.1. TCP :

TCP est un protocole de transport fiable, ce qui signifie qu'il comprend des processus permettant d'assurer un acheminement fiable des données entre les applications par l'utilisation d'accusés de réception. Le transport TCP revient à envoyer des paquets qui sont suivis de la source à la destination. Si l'expédition de FedEx est divisée en plusieurs colis, un client peut vérifier en ligne l'ordre des livraisons. (4)

ii.4.2. UDP :

Fournit uniquement des fonctions de base permettant d'acheminer des segments de données entre les applications appropriées avec peu de surcharge et de vérification des données. (4)

ii.5. La couche Session :

Comme leur nom l'indique, les fonctions de la couche session créent et gèrent les dialogues entre les applications source et de destination. La couche session traite l'échange des informations pour commencer et maintenir un dialogue et pour redémarrer les sessions interrompues ou inactives pendant une longue période. (4)

ii.6. La couche Présentation :

La couche présentation fournit une représentation commune des données transférées entre des services de couche application.
Donc la couche présentation remplit trois fonctions principales :
Elle met en forme ou présente les données provenant du périphérique source dans un format compatible pour la réception par le périphérique de destination.
Elle compresse les données de sorte que celles-ci puissent être décompressées par le périphérique de destination.
Chiffrement des données en vue de leur transmission et déchiffrement des données reçues par le périphérique de destination. (4)

ii.7. La couche Application :

La couche application est la plus proche de l'utilisateur final, c'est elle qui sert d'interface entre les applications que nous utilisons pour communiquer et le réseau sous-jacent via lequel nos messages sont transmis. Les protocoles de couche application sont utilisés pour échanger des données entre les programmes s'exécutant sur les hôtes source et de destination. (4)

ii.7.1. Les protocoles de couche application :

Les protocoles les plus connus sont notamment HTTP (HyperText Transfer Protocol), FTP (File Transfer Protocol), DHCP (Dynamic Host Configuration Protocol) et DNS (Domain Name System).

A. FTP (File Transfer Protocol) :

File Transfer Protocol (protocole de transfert de fichiers), ou FTP, est un protocole de communication destiné à l'échange informatique de fichiers sur un réseau TCP/IP. Il permet, depuis un ordinateur, de copier des fichiers vers un autre ordinateur du réseau, ou encore de

supprimer ou de modifier des fichiers sur cet ordinateur. Ce mécanisme de copie est souvent utilisé pour alimenter un site web hébergé chez un tiers. (8)

B. Le protocole http (HyperText Transfer Protocol) :

HTTP est un protocole de la couche application. Il peut fonctionner sur n'importe quelle connexion fiable, dans les faits on utilise le protocole TCP comme couche de transport. Un serveur HTTP utilise alors par défaut le port 80 (443 pour HTTPS). (9)

C. DHCP (Dynamic Host Configuration Protocol) :

Est un protocole réseau dont le rôle est d'assurer la configuration automatique des paramètres IP d'une station, notamment en lui affectant automatiquement une adresse IP et un masque de sous-réseau. (10)

D. DNS (Domain Name Service) :

Est un service permettant de traduire un nom de domaine en informations de plusieurs types qui y sont associées, notamment en adresses IP de la machine portant ce nom. (11)

I.4.1.2. Le Modèle TCP / IP :

Le modèle TCP/IP définit quatre couches, dont chacune assure un service particulier, garanti par le protocole associé. Il signifie Transport Control Protocol/Internet Protocol. Le protocole possède les qualités suivantes :

- La capacité à gérer un taux élevé d'erreurs.
- Une faible surcharge des données.
- La capacité de se prolonger sans difficultés dans des sous réseaux.
- L'indépendance par rapport à un fournisseur particulier ou un type de réseau. (12)

D'une façon générale, les protocoles TCP/IP s'organisent en couche 4 conceptuelles (Figure I-10).

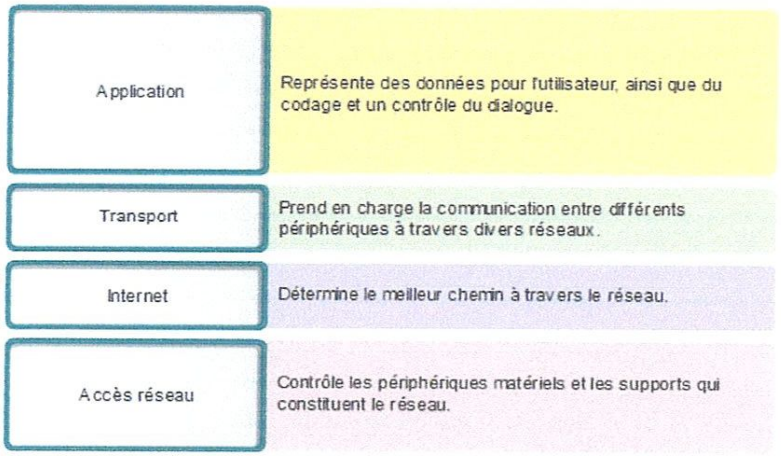


Figure I-10 : *Le modèle de référence TCP/IP. (4)*

- Couche application : à la couche supérieure, les utilisateurs invoquent les applications qui accèdent aux services disponibles via internet TCP/IP. Une application interagit avec l'un des protocoles de la couche transport pour envoyer ou recevoir des données. Chaque application choisit le style de transport nécessaire, qui peut être soit une séquence de messages individuels, soit un flot d'octets continu. L'application envoie les données, au format requis, à la couche transport en vue de leur transmission.
- Couche transport : Son premier objectif est d'assurer la communication entre une application et une autre, communication souvent appelée de bout en bout. La couche transport régule le flux d'information. Elle assure également la fiabilité du transport, C'est-à-dire vérifie que les données arrivent sans erreur et dans le bon ordre. Pour ce faire, le logiciel du protocole de transport fait en sorte que le destinataire transmette des accusés de réception et que l'expéditeur renvoie les paquets perdus. Le logiciel de transport divise le flux de données transmis en petits morceaux (appelés segments) et transfère chaque segment avec une adresse de destination à la couche suivante en vue de sa transmission.
- Couche internet : Gère la circulation des paquets à travers le réseau en assurant leur routage. Parmi ses protocoles : IP (Internet Protocol), ICMP (Internet Control Message Protocol) et IGMP (Internet Group Management Protocol) ARP (Adresse Resolution Protocol), RARP (Revers Adresse Resolution Protocol). (12)
- Couche interface réseau : Le logiciel TCP/IP de cette couche est responsable de la réception des datagrammes IP et de leur transmission sur un réseau physique spécifique. Une interface réseau peut se composer d'un pilote de périphérique (Par exemple, lorsque

la machine accède directement à un réseau local) ou d'un Sous-système complexe qui utilise son propre protocole de liaison de données. (13)

I.4.2. Topologie physique de réseau :

La topologie d'un réseau décrit la manière dont les nœuds sont connectés. Cependant, on distingue la topologie physique, qui décrit comment les machines sont raccordées au réseau, de la topologie logique qui renseigne sur le mode d'échange des messages dans le réseau (topologie d'échange). (3)

I.4.2.1. Les topologies de base :

Les topologies de bases sont toutes des variantes d'une liaison point à point ou multipoint (Figure I-11). (3)

Figure I-11 : *Les modes de liaisons élémentaires. (3)*

I.4.2.2. La topologie en bus :

La plus simple des topologies de base, la topologie en bus qui est une variante de la liaison multipoint. Dans ce mode de liaison, l'information émise par une station est diffusée sur tout le réseau. Le réseau en bus est aussi dit réseau à diffusion (Figure I-12). Dans ce type de topologie, chaque station accède directement au réseau, d'où des problèmes de conflit d'accès (contentions ou collisions) qui nécessitent de définir une politique d'accès. Celle-ci peut être centralisée (relation dite maître/esclave) ou distribuée comme dans les réseaux locaux. (3)

Les réseaux en bus sont d'un bon rapport performance/prix. Ils autorisent des débits importants (>100 Mbit/s sur 100 m). Il est possible d'y insérer une nouvelle station sans perturber les communications en cours. Cependant, la longueur du bus est limitée par l'affaiblissement du signal, il est nécessaire de régénérer celui-ci régulièrement. La distance entre deux régénérations se nomme « pas de régénération ».

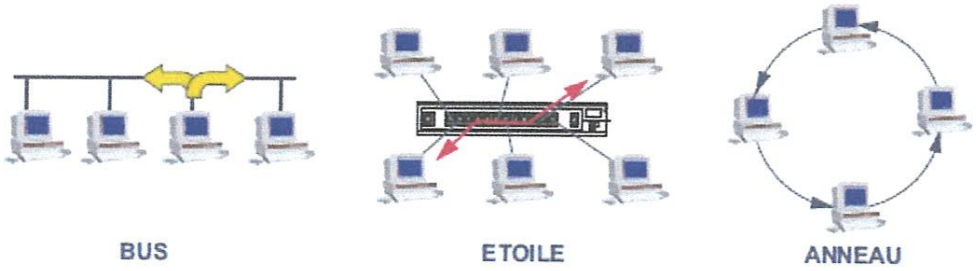


Figure I-12 *: Les topologies de base. (3)*

I.4.2.3. La topologie étoile :

C'est une variante de la topologie en point à point. Un nœud central émule n liaisons point à point (Figure I-12). Tous les nœuds du réseau sont reliés à un nœud central commun : le concentrateur. Tous les messages transitent par ce point central. Le concentrateur est actif, il examine chaque message reçu et ne le retransmet qu'à son destinataire. Cette topologie correspond, par exemple, au réseau téléphonique privé d'une entreprise où le commutateur téléphonique met en relation les différents postes téléphoniques. La topologie en étoile autorise des dialogues inter nœud très performants. La défaillance d'un poste n'entraîne pas celle du réseau, cependant le réseau est très vulnérable à celle du nœud central. (3)

I.4.2.4. La topologie en anneau :

Dans la topologie en anneau, chaque poste est connecté au suivant en point à point (Figure I-12). L'information circule dans un seul sens, chaque station reçoit le message et le régénère. Si le message lui est destiné, la station le recopie au passage. Ce type de connexion autorise des débits élevés et convient aux grandes distances (régénération du signal par chaque station). L'anneau est sensible à la rupture de la boucle. Les conséquences d'une rupture de l'anneau peuvent être prises en compte en réalisant un double anneau. (3)

I.4.2.5. Les topologies construites :

Dérivés des réseaux en étoile, les réseaux arborescents (Figure I-13) sont constitués d'un ensemble de réseaux étoiles reliés entre eux par des concentrateurs jusqu'à un nœud unique (nœud de tête). Cette topologie est essentiellement mise en œuvre dans les réseaux locaux. Ces réseaux, en raison de la concentration réalisée à chaque nœud, sont très vulnérables à la défaillance d'un lieu ou d'un nœud (Figure I-13). (3)

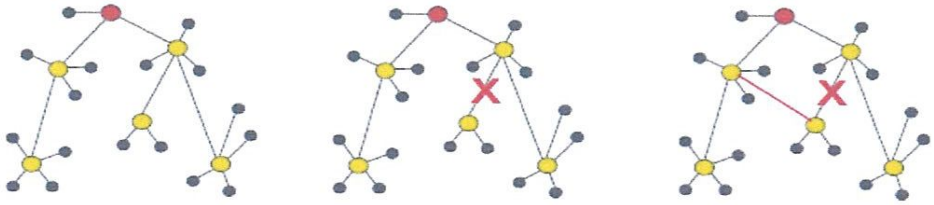


Figure I-13 : *De la topologie hiérarchique à la topologie maillée. (3)*

Pour pallier cet inconvénient on peut imaginer créer des chemins de secours qui peuvent être temporaires ou permanents. Le réseau est alors dit maillé (Figure I-13). Un réseau maillé est un réseau dans lequel deux stations, clientes du réseau, peuvent être mises en relation par différents chemins (Figure I-14). Ce type de réseau, permettant de multiple choix de chemins vers une même destination, est très résistant à la défaillance d'un nœud et autorise une optimisation de l'emploi des ressources en répartissant la charge entre les différents nœuds (voies). Chaque nœud est caractérisé par sa connectivité, c'est-à-dire par le nombre de liens qui le réunit aux autres nœuds du réseau. (3)

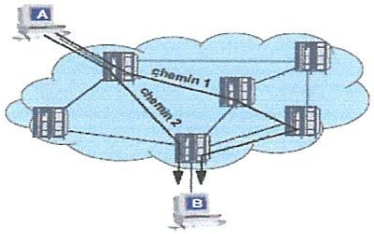


Figure I-14 : *Réseau maillé. (3)*

1.4.3. La topologie logique de réseau :

Le terme topologie logique désigne la façon par laquelle les données transmises entre les nœuds plutôt que la disposition des voies ou chemins qu'empruntent les données.

Une topologie logique s'appelle aussi un système de transport réseau .la topologie logique d'un réseau décrit la manière par laquelle les données sont mises en trames et comment les impulsions électriques sont envoyées sur le support physique du réseau les éléments d'une topologie logique appartiennent à la fois aux couche liaison du modèle OSI.

Chaque topologie logique possède son propre ensemble de principe de signalisation de données, mais impose aussi des exigences particulières au niveau du média de transmission et de la topologie physique.

Ethernet et Token Ring sont les deux systèmes de transport réseau (topologie logique) les plus courants. Mais il y a également d'autres topologies logiques telles que FDDI et LocalTk…etc. (14)

I.4.4. Modélisation Hiérarchique d'un Réseau :

Dans le domaine des réseaux, la conception hiérarchique divise le réseau en couches distinctes. Chaque couche, ou niveau, de la hiérarchie offre des fonctions spécifiques qui définissent son rôle dans le réseau. Ceci permet au concepteur et à l'architecte du réseau de sélectionner le matériel et les logiciels réseaux adaptés, ainsi que les fonctionnalités nécessaires aux rôles de cette couche réseau. Les modèles hiérarchiques appliquent à la fois les conceptions LAN et WAN. (4)

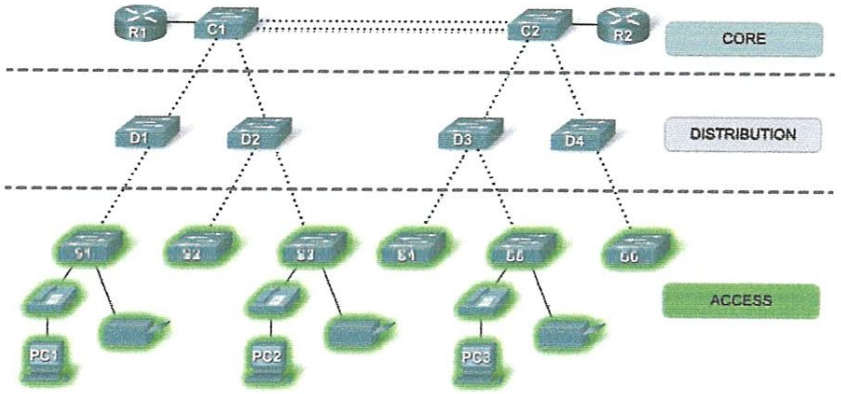


Figure I-15 : *modélisation hiérarchique. (4)*

Le but d'utiliser la modélisation hiérarchique est de :

- Simplifier son administration
- Isoler rapidement les problèmes
- Rendre modulable le réseau et pouvoir facilement l'agrandir

Une conception de réseau typique de LAN hiérarchique comprend les trois couches suivantes :

- Couche d'accès (Access Layer) : Elle permet aux groupes de travail et aux utilisateurs d'accéder au réseau. Cette couche garantie :
  - La commutation de couche 2
  - Disponibilité élevée
  - Sécurité des ports
  - Classification et notation de la qualité de services et limites de confiance
  - Inspection du protocole de résolution d'adresses ARP
  - SpanningTree (pour éviter les boucles)

- Couche de distribution (Distribution Layer) : Elle fournit la connectivité basée sur les stratégies et contrôle la limite entre les couches d'accès et le core. Cette couche permet de :
  - Limiter les zones de broadcast
  - Router les données entre VLAN
  - Eviter certaines données de transiter vers certains VLAN
  - La diffusion de contrôle du domaine, car les routeurs et les commutateurs multicouches ne transmettent pas les diffusions. Point de démarcation entre domaines de diffusion.
- Couche Core de réseau (Core Layer) : assure le transport rapide entre commutateurs de distribution dans le campus d'entreprise. Il doit transférer les données le plus rapidement possible, et aussi apporte la connexion à Internet ou aux autres réseaux de la société via un MAN ou WAN.

I.4.5. Gestion de la communication :

I.4.5.1. Sens de communication :

La transmission d'information entre deux correspondants peut être unidirectionnelle (l'échange n'a lieu que dans une seule direction), on parle alors de liaison simplex (Figure I-16). Chaque correspondant ne remplit qu'une fonction, il est émetteur (source) ou récepteur (puits ou collecteur). Ce type de transmission est utilisé dans la diffusion radio et TV par exemple. Ce mode pressente l'inconvénient de ne pas savoir si tout a été reçu par le destinataire sans erreur. Si les correspondants peuvent, alternativement, remplir les fonctions d'émetteur et de récepteur, la liaison est dite : liaison à l'alternat ou half duplex. Le temps mis par les systèmes pour passer d'une fonction à l'autre est appelé temps de retournement. Ce temps peut être important, jusqu'à 1/3 de seconde. L'exemple le plus typique est la conversation par « talkie/walkie », l'utilisateur est à l'écoute et il doit couper l'écoute s'il désire parler. Par rapport aux transmissions simplex, il est nécessaire de disposer de transmetteur (émetteur) et récepteur aux deux extrémités.
Lorsque l'échange peut s'effectuer simultanément dans les deux sens, sur des voies distinctes ou sur la même voie par utilisation de techniques spécifiques comme le multiplexage fréquentiel, la liaison est appelée bidirectionnelle intégrale ou full duplex. Comme exemple, citons le téléphone. Cette technique nécessite l'utilisation de deux voies de transmission, une pour l'émission, l'autre pour la réception. Notons toutefois qu'une liaison full duplex peut être multiplexée. (2)

simple, dès que quelque chose arrive sur l'un de ses ports, il est automatiquement répété sur tous les autres ports. (12)

- Le pont (bridge) : C'est un équipements relais de Couche 2, Permettant de relier des réseaux locaux de même type (travaillant avec le même protocole), Ils filtrent les données en ne laissant passer que celles destinées aux ordinateurs situés à l'opposé du pont (segment opposé). (12)

  Le commutateur : est une unité de couche 2,il prend des décisions en fonction des adresses MAC (Media Access Control address). En raison des décisions qu'il prend, le commutateur rend le LAN beaucoup plus efficace. (16)
- Le routeur : est la première unité que vous utiliserez qui fonctionne au niveau de la couche réseau du modèle OSI, appelée couche 3. En raison de leur capacité d'acheminer les paquets en fonction des informations de couche 3, les routeurs sont devenus le cœur de réseau d'Internet et exécutent le protocole IP. Le rôle du routeur consiste à examiner les paquets entrants (données de couche 3), à choisir le meilleur chemin pour les transporter sur le réseau et à les commuter ensuite au port de sortie approprié. Sur les grands réseaux, les routeurs sont les équipements de régulation du trafic les plus importants. (16)
- La passerelle (Gateway) : Est un équipement d'interconnexion de deux réseaux totalement différents, elle doit assurer toutes les conversions de protocoles pour garantir les échanges entre deux réseaux. (12)

I.5. Conclusion :

Les réseaux informatiques peuvent être classifiés selon la distance, la topologie et l'architecture. Une bonne étude du réseau conduit à une bonne configuration et ainsi un bon fonctionnement. Il est primordiale pour chaque constructeur de réseaux de connaitre ces bases avant la construction de n'importe quel réseau.

Chapitre II : Principes de sécurisation d'un réseau

système. Une variante de cette attaque consiste à obtenir un compte privilégié créé directement par un administrateur trouvant cette procédure plus « sécurisée ». (19)

II.3.2. Écoute réseau :

Grâce à une table d'écoute (sniffer), il est possible d'intercepter les trames reçues par la carte réseau d'un système pirate et qui ne lui sont pas destinées (Figure II-1).
Le système pirate se situe sur le réseau local et capture tous les paquets réseau transitant sur ce réseau afin d'obtenir des mots de passe, etc. Il n'est pas nécessaire que le sniffer possède une adresse IP sur le réseau qu'il écoute. Une interface réseau active sans adresse IP suffit. L'écoute est alors totalement indécelable au niveau ARP.

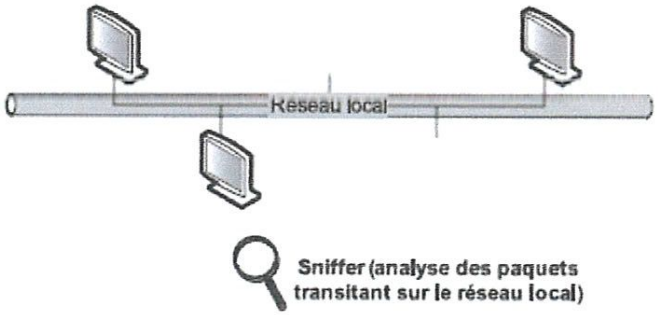


Figure II-1 *: Écoute sur un réseau local. (19)*

Grâce à des outils tels qu'Ethereal ou WinDump/TCPDump, le sniffer peut analyser tous les paquets IP ainsi que les protocoles contenus dans les données du paquet. Par exemple, un sniffer peut analyser un paquet Ethernet susceptible de contenir un paquet IP, qui lui-même pourrait contenir un paquet de type TCP, lequel à son tour pourrait contenir un paquet HTTP renfermant des données HTML.
Si une personne établit une session authentifiée sur un flux réseau non chiffré (Telnet, X11, etc.), son mot de passe transite en clair sur le réseau. De même, il est possible de connaître à tout moment les personnes connectées au réseau, les sessions de routage encours, etc., par une analyse des paquets qui transitent sur le réseau et qui contiennent toutes les informations nécessaires à cette analyse.
Dans un réseau commuté, il n'est théoriquement pas possible d'écouter le réseau, car le commutateur envoie à chaque machine uniquement les paquets de données qui lui sont destinés. Mais comme tout équipement réseau, les commutateurs ont leurs faiblesses. Ainsi, un client qui enverrait des paquets usurpant l'adresse MAC du serveur qu'il désire écouter pourrait recevoir

ces données. Selon les marques et les modèles de commutateur, le comportement diffère totalement. Cela échoue souvent, mais il arrive que cela marche. Dans certains cas, le commutateur panique et se place en déni de service. (19)

II.3.2.1. Analyse des ports :

Les internautes malveillants utilisent fréquemment le balayage des ports pour préparer leurs attaques et réaliser le « finger printing » du système. Lors du balayage des ports, un attaquant potentiel tente de se connecter pendant une courte durée à chaque port sur un système et à établir la carte de tous les programmes qui écoutent le trafic réseau. De cette manière, il peut savoir où attaquer en trouvant tous les services réseau sur le système qui sont vulnérables ou potentiellement intéressants. Dans de nombreux cas, il peut aussi déterminer quel système d'exploitation utilise sa victime, car les services par défaut sont souvent spécifiques à chaque système d'exploitation.

Le premier problème du balayage de port traditionnel est qu'il est assez bruyant – la victime est susceptible de remarquer une tempête ou même un flux régulier de tentatives de connexion à des ports inhabituels. Il n'est pas non plus facile de se cacher ; l'attaquant doit être en mesure de voir les réponses à ses paquets SYN pour savoir si un port est ouvert ou fermé. Les ports ouverts répondent avec SYN+ACK, les ports fermés, avec RST, tandis que les ports filtrés par un pare-feu sont susceptibles de ne générer aucune réponse ou un message ICMP (Internet Control Message Protocol). En conséquence, l'attaquant ne peut pas simplement usurper l'adresse source sur tous les paquets sortants ; il doit révéler son identité en fournissant des adresses sources qui sont routées en retour vers le réseau qu'il écoute pour détecter le trafic entrant. (20)

II.3.2.2. Codes malveillants :

Un code malveillant est un code informatique qui crée des failles de sécurité pour endommager le système informatique.

Un code malveillant est une application auto-exécutable qui peut s'auto-activer et se présenter sous diverses formes (applets Java, commandes ActiveX, contenu transmis automatiquement, plug-ins, langages de script ou autres langages de programmation, etc.) pour enrichir les pages Web et les e-mails. Ce code offre alors aux cybers criminels un accès distant non autorisé au système attaqué. Cette backdoor expose ensuite les données confidentielles de l'entreprise infectée. Grâce à cet accès, les cybers criminels peuvent effacer les données d'un ordinateur ou

même installer des logiciels espions. Même les plus hautes instances d'une administration peuvent être concernées par de telles menaces. (L'U.S. Government Accountability Office a), par exemple, déjà été averti du fait qu'un code malveillant menaçait la sécurité nationale des États-Unis. (21)

II.3.2.3. Programmes furtifs :

Les virus furtifs sont également appelés intercepteurs d'interruptions, car ils prennent le contrôle des interruptions logicielles du système d'exploitation afin de lui faire croire que le système est sain. Cette prise de contrôle de la table d'interruptions s'effectue au tout début de la zone mémoire. Lorsqu'un programme émet une requête d'interruption, celle-ci est habituellement redirigée vers la table d'interruptions qui gère les commandes et permet au programme de faire son travail.
En cas d'infection par un virus furtif, celui-ci intercepte les requêtes et peut les rediriger où il le désire et effectuer toute opération possible selon son bon plaisir.
Cette capacité des virus furtifs à contrôler la table d'interruptions leur permet de se cacher de manière extrêmement efficace, rendant leur détection particulièrement ardue. (19)

II.4.Notions de sécurisation sur le réseau local :

II.4.1. Services de la sécurité :

La sécurité d'un réseau est un niveau de garantie que l'ensemble des machines du réseau fonctionnent de façon optimale et que les utilisateurs des dites machines possèdent uniquement les droits qui leur ont été octroyés. Pour satisfaire ces besoins il faut garantir que les services de sécurité sont appliqués. Les différents services de sécurité sont : le contrôle d'accès au système, l'intégrité, la non répudiation, l'authentification, la confidentialité.
Ces services s'appliquent à l'information comme aux systèmes ainsi qu'aux supports. il est indispensable qu'aucune ne soi forcée, ni oubliée. . (18)

II.4.1.1. Le contrôle d'accès au système :

Il s'agit ici, avant tout, de protéger physiquement le matériel. Il est nécessaire de verrouiller les salles serveurs, mais également désormais les bureaux. Les systèmes d'exploitation et autres logiciels doivent être sécurisés, par paramétrages et installations régulières des correctifs de failles logiciels. Les réseaux peuvent être isolés les uns des autres (utilisation des VLANs), et les communications doivent être filtrées. Des logiciels anti-virus doivent également être

installés et maintenus. Des outils de détection (ID Sintrusion Detection System) peuvent compléter les protections nécessaires. (18)

i. L'intégrité :

L'intégrité des données assure que les messages n'ont pas été changés en transitant le réseau. Avec l'intégrité des données, le récepteur peut vérifier que le message reçu est identique au message envoyé et qu'aucune manipulation ne s'est produite. (22)

ii. La non-répudiation :

C'est un mécanisme permettant de garantir qu'un message a bien été envoyé par un émetteur et reçu par un destinataire. La non-répudiation se fonde sur le fait que seulement l'expéditeur a les caractéristiques ou la signature unique pour la façon dont ce message est traité. Même le dispositif de réception ne peut savoir la façon dont l'expéditeur a traité ce message pour prouver l'authenticité. (22)

iii. Authentification :

L'Authentification garantit qu'un message vient de la source laquelle il prétend venir. L'authentification peut être accomplie avec des méthodes cryptographiques. C'est particulièrement important pour des applications ou des protocoles, comme les courriels.

iv. Confidentialité :

La confidentialité de données assure l'intimité de sorte que seulement le récepteur puisse lire le message. Le cryptage est le processus de brouiller des données de sorte qu'il ne puisse pas être lues par les parties non autorisées. En appliquant le cryptage, les données lisibles s'appellent le texte en clair, alors que celles chiffrées s'appellent le cryptogramme. Le message lisible est converti en cryptogramme, qui est illisible. Le décryptage renverse le processus. Une clé est exigée pour chiffrer et déchiffrer un message. La clé est le lien entre le texte clair et le cryptogramme.

L'utilisation d'une fonction de hachage est une autre manière d'assurer la confidentialité de données. (22)

iv.1. Le chiffrement à clés symétriques :

Les algorithmes de chiffrement symétriques emploient la même clé, appelée la clé secrète, pour chiffrer et déchiffrer des données. La clé doit être pré-partagée. Une clé pré-partagée est connue par l'expéditeur et le récepteur avant que toute communication chiffrée ne débute. Des longueurs de clés plus courtes signifient une exécution plus rapide. Les algorithmes symétriques demandent généralement beaucoup moins de calculs que les algorithmes asymétriques.

Le chiffrement symétrique ou à clé secrète, est la forme de cryptographie la plus utilisée généralement, parce que la longueur de clé plus courte augmente la vitesse de l'exécution. En plus, les algorithmes à clé symétrique sont basés sur des opérations mathématiques simples qui peuvent être facilement accélérées par le matériel. Le chiffrage symétrique est employé souvent pour le chiffrage dans des réseaux informatiques quand la confidentialité des données est exigée, comme pour protéger un VPN.

Avec le chiffrage symétrique, la gestion des clés peut être un défi. Les clés de chiffrage et de déchiffrage sont identiques. L'expéditeur et le récepteur doivent échanger la clé symétrique et secrète en utilisant un canal sûr avant que n'importe quel chiffrage puisse se produire. La sécurité d'un algorithme symétrique repose sur le secret de la clé symétrique. En obtenant la clé, n'importe qui peut chiffrer et déchiffrer des messages.

Les séries des algorithmes de Rivest (RC), qui incluent RC2, RC4, RC5, et RC6, sont tous des algorithmes de chiffrement bien connus qui emploient des clés symétriques.

Les techniques les plus utilisées généralement dans la cryptographie à chiffrement symétrique sont des chiffrements par bloc et des chiffrements par flux. (22)

iv.2. Le chiffrement à clés asymétriques :

Les algorithmes de chiffrement asymétriques emploient différentes clés pour chiffrer et déchiffrer les données. Des messages sûrs peuvent être échangés sans devoir avoir une clé pré-partagée. Puisque les deux parties n'ont pas un secret partagé, des longueurs de clés très longues doivent être employées pour contrecarrer les attaquants. Ces algorithmes requièrent plus de ressources et leur exécution est plus lente. Dans la pratique, les algorithmes asymétriques sont typiquement des centaines à des milliers de fois plus lents que les algorithmes symétriques.

Mais le concept de chiffrement asymétrique avec une clé publique était légèrement antérieur (1976). L'idée générale était de trouver deux fonctions f et g sur les entiers, telles que g(f)=Id, et telle qu'on ne puisse pas trouver f, la fonction de décryptage, à partir de g, la fonction de cryptage. On peut alors rendre publique la fonction g (ou clé), qui permettra aux autres de

crypter le message à envoyer, tout en étant les seuls à connaitre f, donc à pouvoir décrypter. (22)

II.5.Sécurisation de l'interconnexion de réseaux :

II.5.1. Routeur filtrant :

Le moyen le plus simple de protéger le réseau contre les intrusions peut être réalisé avec le routeur d'accès à l'extérieur (Figure II-2).

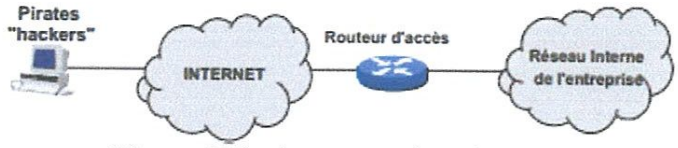


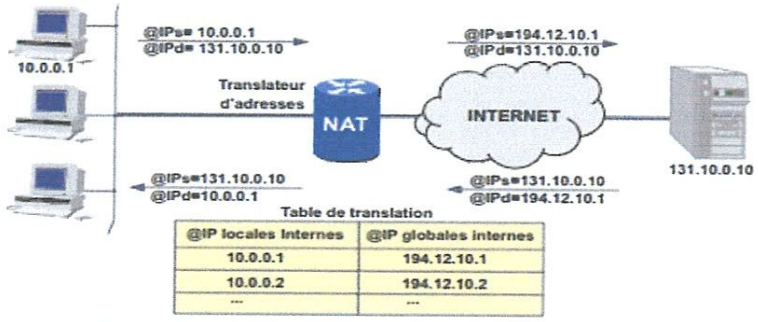
Figure II-2 : *le routeur d'accès. (3)*

Le routeur peut assurer des fonctions simples de filtrage par analyse des adresses source et destination. Le routeur n'a de visibilité que sur les données protocolaires du niveau 3. Ses possibilités de filtre sont donc réduites à ces deux éléments, la sécurité offerte est faible. Les règles de filtrage sont réunies dans des listes (ACL, Access Control List). (3)

II.5.2. Translateur d'adresse :

La translation d'adresse est un moyen de contourner la pénurie d'adresses Internet, mais aussi de masquer le plan d'adressage de l'entreprise (IP masque rade).

La traduction statique fait correspondre à une adresse interne du réseau une adresse externe, généralement une adresse publique. Ce mode de translation résout à la fois le problème de la pénurie d'adresse, du masquage du plan d'adressage local (mascarade) et sécurise le réseau en n'autorisant que certaines stations à accéder à l'Internet.



@IP locales internes	@IP globales internes
10.0.0.1	194.12.10.1
10.0.0.2	194.12.10.2
...	...

Figure II-3 : *traduction statique d'adresse. (3)*

La translation statique limite le nombre de machines ayant accès à l'extérieur au nombre d'adresses publiques attribuées. La traduction dynamique s'affranchit de cette limite. Lorsqu'une machine veut atteindre une machine extérieure, le NAT associe à l'adresse locale interne une adresse globale interne, ou adresse externe, choisie parmi un pool d'adresses mises à sa disposition. Le NAT introduit un protocole à état, indépendamment du fait qu'en cas de défaillance du NAT les relations sont perdues, l'état doit être détruit en fin de communication et l'adresse attribuée rendue disponible pour une autre connexion vers l'extérieur. Un temporisateur est donc associé à chaque connexion, il est réinitialisé à chaque message, la connexion est libérée sur time out. (3)

Cependant, le nombre d'adresses publiques attribuées peut être insuffisant. Le NAPT (Network Address and Port Translation) permet à plusieurs machines de partager une même adresse externe par translation du numéro de port (Figure II-4).

La fonction dite du PAT (Port Address Translation) autorise plusieurs milliers de connexion à se partager une même adresse IP externe dite aussi globale interne. (3)

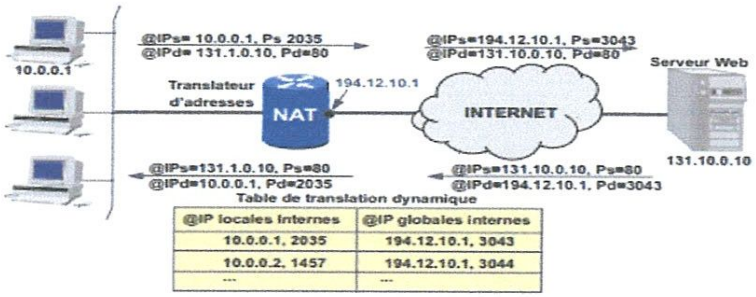


Figure II-4 : *principe de translation de port. (3)*

En translation dynamique, la correspondance Adresse IP interne/Adresse IP externe est initialisée par la machine interne. Pour donner accès, aux machines extérieures, à certains services on peut utiliser la technique dite du « Port forwarding » soit pour accéder directement au service concerné, soit en passant par les services d'un DNS (Domain Name System). La table de translation est pré renseignée de l'adresse du ou des services ouverts (translation statique).

La (Figure II-4) illustre ce principe La machine 10.0.0.1 veut se connecter à une machine sur internet, elle envoi donc un paquet avec comme adresse source la sienne 10.0.0.1, et comme port source 2035. Le paquet arrive au routeur qui fait la NAT, il remplace donc l'adresse IP source par la sienne 194.12.10.1, et le PAT en remplaçant le port TCP/UDP source 2035 par un de son choix, 3043.il garde ces informations de correspondance dans une table NAT. Le paquet arrive à la destination qui le renvoie à 194.12.10.1. Le paquet arrive au routeur .il voit que

l'adresse destination est lui-même, regarde donc le port destination TCP/UDP qui est 3043 .il va regarder dans la table NAT pour avoir la correspondance, il sait qu'il faut envoyer ce paquet à 10.0.0.1 tout en modifiant le port destination 3043 par 2035 qui est le port sous lequel la machine (10.0.0.1) a initialisé la connexion. (3)

II.5.3. Pare-feu :

Le pare-feu (firewall) est un système aux fonctions de filtrage évoluées. Indépendamment des fonctions de routage et de translation d'adresses, chaque paquet reçu est examiné, une décision de rejet ou d'acceptation est prise en fonction de nombreux critères :

- L'adresse destination,
- L'adresse source,
- Le protocole transporté (ICMP, UDP...),
- Le port destination,
- Le port source
- La valeur de certains flags (ACK, SYN....)

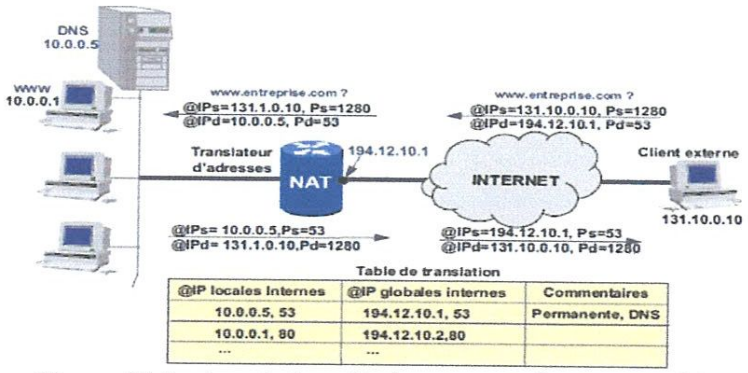


Figure II-5 : *translation d'adresse et trafic entrant. (3)*

La décision est prise pour chaque datagramme, il n'y a pas de notion de contexte. Il existe deux types de pare-feu, le pare-feu à séparation des réseaux qui segmente le réseau en deux tronçons : le réseau interne et le réseau externe, il contrôle le trafic et peut réaliser une translation d'adresses (NAT). Et le pare-feu au fil de l'eau qui n'effectue aucune séparation physique des réseaux. Cependant, comme le pare-feu à séparation des réseaux, il réalise l'isolation des trafics. Les postes ne communiquent qu'avec le pare-feu (passerelle par défaut) et le routeur ne voit que le pare-feu. (3).

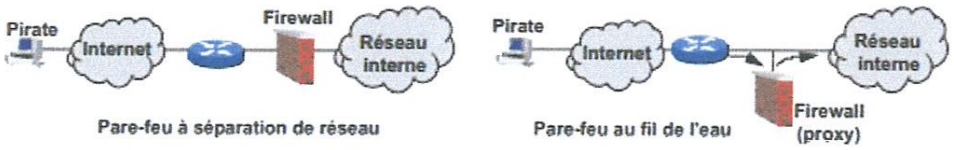


Figure II-6 : *Les différents modes d'utilisation des pare-feu (firewall). (3)*

II.5.4. Proxy :

Les passerelles applicatives (Application Layer Gateway ou Proxy-Server) établissent une double connexion (Figure II-7). Le filtrage s'effectue alors au niveau de chaque service offert. Les services internes sont invisibles de l'extérieur. La passerelle peut réaliser des conversions de protocoles (messagerie...).

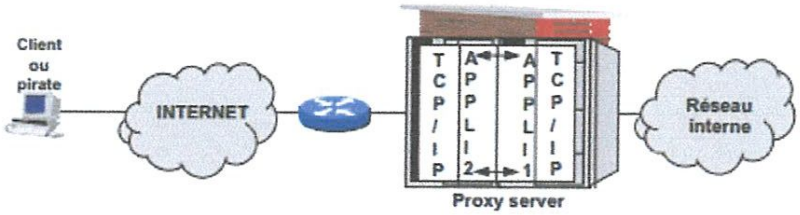


Figure II-7 : *Le filtrage par un proxy-server. (3)*

Les passerelles applicatives, à l'instar des pare-feu, mémorisent toutes les connexions et peuvent en éditer la liste. L'association pare-feu à séparation de réseau et proxy-server (pare-feu au fil de l'eau) constitue une protection efficace contre les intrusions. Mais quels que soient les moyens mis en œuvre, les virus et chevaux de Troie restent indécelables. (3)

II.5.5. Zone démilitarisée :

La mise à disposition d'un serveur public (service Web, messagerie...) est généralement réalisée par la constitution d'une zone de sécurité dite DMZ (De Militarized Zone). Différentes zones de sécurité peuvent être constituées, chacune accessible selon des critères spécifiques (filtres). L'utilisation de deux pare-feu permet de renforcer cette sécurité. Le premier masque, aux pirates éventuels, le second. En choisissant les deux pare-feu de marque différente, on améliore encore la sécurité, les vulnérabilités ou failles de l'un étant différentes de celles de l'autre.

La zone démilitarisée accueillera les différents serveurs accessibles à la fois par le personnel de l'entreprise et par le monde extérieur. Pour différencier les services offerts et les règles de filtrage, il est possible de définir plusieurs DMZ, dans ce cas généralement l'une est accessible à tous, et l'autre aux personnels de l'entreprise. (3)

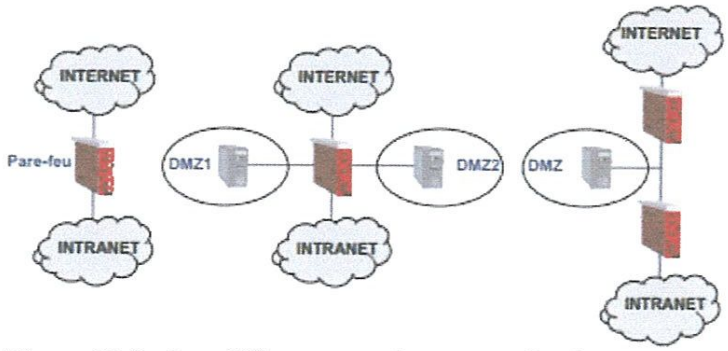


Figure II-8 : *Les différentes architectures de sécurité. (3)*

II.6. Conclusion :

La sécurité constitue une exigence importante dans les systèmes modernes de l'informatique. La construction des réseaux sécurisés est un domaine émergent dans l'ingénierie des réseaux nécessitant des compétences dans la cryptographie, dans la technologie de communication, etc. Dans ce chapitre, nous avons mentionné les exigences de sécurité des systèmes informatiques générales et des réseaux informatiques en particulier, et nous avons décrit les technologies et les techniques les plus utilisées pour accroitre la sécurité d'un réseau d'une moyenne entreprise.

Chapitre III : Outils d'aide à la construction et la configuration

III. Outils d'aide à la construction et la configuration des réseaux :

III.1. Introduction :

Afin de construire, de configurer et de maintenir un réseau qui soit tolérant aux pannes et extensible, plusieurs outils peuvent être utilisés. Dans la première phase de construction de n'importe quel réseau, une phase de simulation de ce dernier est très importante afin de choisir les équipements nécessaires ainsi que l'architecture du futur réseau.

Une fois le réseau construit, l'administrateur aurait besoin d'outils d'accès afin d'administrer ses équipements.

Dans cette partie on va présenter brièvement les outils nécessaires à la construction, l'administration et le troubleshooting des réseaux pour les moyennes entreprises.

III.2. Objectifs de la simulation :

Les simulateurs de réseau sont des logiciels destinés pour l'apprentissage des réseaux Ethernet TCP/IP. Leur but est de simuler le comportement de chaque élément d'une configuration réseau : hub, switch, routeur, et d'autre matériel réseaux, et de rendre observable les principaux concepts associés aux réseaux locaux : topologie, adressage physique et logique, tout sera afficher dans le programme pour faciliter les configurations de réseaux et détecter les failles dans les réseaux facilement, donc les simulateurs peuvent être très utiles dans la phase d'étude et de construction de n'importe quel réseau.

III.3. Exemples de Simulateurs et Emulateurs :

Dans la phase de l'étude de n'importe quel réseau, il est préférable d'utiliser un logiciel de simulation.il existe plusieurs simulateur et émulateur tel que packet Tacer, GNS3 et Dynamips, Parmi ses avantages :

- Un logiciel de simulation permet de simuler un large éventail de technologies de réseau telles que le routage et la commutation, de construire la topologie de l'ensemble du réseau, de simuler le processus en cours d'exécution.

Ses interfaces permettent de réaliser de nombreuses tâches de configuration sans avoir recours à la ligne de commande (CLI).

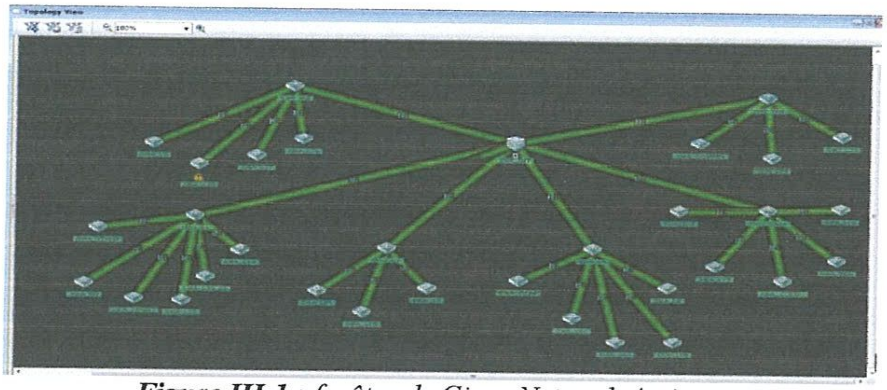


***Figure III-1** : fenêtre de Cisco Network Assistant.*

III.4.3. Cisco Router and Security Device Manager (SDM):

Est un outil de gestion de périphériques convivial qui permet de configurer des fonctions de sécurité Cisco IOS et des connexions réseau par l'intermédiaire d'une interface utilisateur graphique Web extrêmement intuitive.

III.4.4. Comparaison entre les outils :

Par ligne de commande	**Par Cisco Network Assistant ou Cisco Router and Security Device Manager (SDM)**
Il faut maitriser la logique des commandes	Pas besoin de maitriser la logique
Sans interface graphique	Avec une interface graphique
Difficile pour les débitants	Facile
Contrôle total des équipements	Contrôle limité des équipements

***Tableau III-2** : comparaison entre les outils.*

III.5. Conclusion :

Vu que la simulation et l'émulation d'un réseau avant son déploiement réel représente une alternative moins coûteuse et moins lourde que son expérimentation en environnement réel, les outils d'émulation et simulation sont devenus primordiales dans nos jours afin de tester le réseau et assurer son fonctionnement ainsi que sa sécurité avant de passer à la configuration du matériel réel.

Chapitre IV : Implémentation

IV.3.1. Choix du simulateur :

Dans notre travail, on a choisi d'utiliser le GNS3, son principal avantage réside dans l'émulation matérielle, à la différence des simulateurs qui sont souvent une manière limitée de virtualisation du matériel. Grâce à GNS3, on peut tester et estimer, dans des conditions quasi réelles et sans avoir accéder au matériel, les configurations avant de les mettre en place physiquement. Il est préférable de simuler le réseau de n'importe qu'elle entreprise avant l'étape de construction, cela permet de construire un réseau de bonne qualité.

IV.3.2. Modélisation hiérarchique du réseau :

Comme mentionné dans les chapitres précédents, Une conception de LAN hiérarchique comprend les trois couches suivantes : Accès, Distribution et Core. Les équipements réseau utilisées sont présentés dans le (Tableau IV-1) avec leurs nominations :

	core	**Distribution**	**Accès**	**Routeur**
Type de périphérique	Switch multilayer niveau 3 (L3)	Switch niveau 2	Switch niveau 2	Routeur
Nombre de périphériques utilisés	1	6	26	1+1 routeur distant
La nomination	SWF_INT	SWF_MG SWF_CS SWF_OP SWF_S5 SWF_MARK SWF_TRA	SWA_ST SWA_STAND SWA_RH SWA_ACHAT SWA_CONF SWA_INT SWA_COMP1 SWA_SEC SWA_COMPT4 SWA_L02 …etc.	ROUTER_WAN+ R2

Tableau IV-1 : *Les équipements réseau utilisées.*

La (Figure IV-1) montre l'architecture Hiérarchique de notre réseau en utilisant le GNS3.

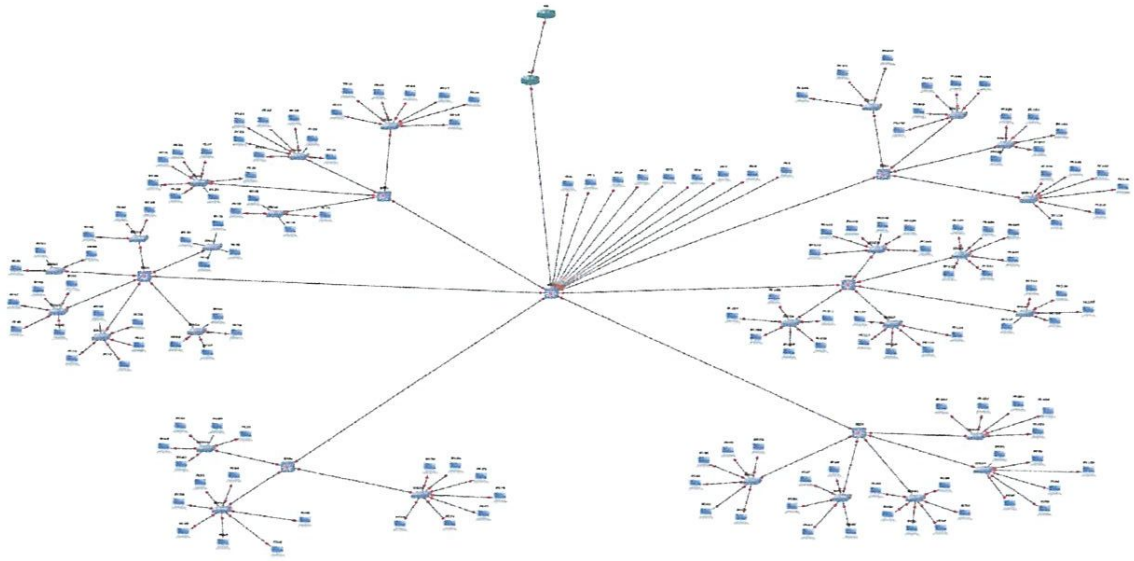


Figure IV-1 : *Modélisation Hiérarchique.*

IV.4. Etude technique :

La branche technique, consiste en une capture des besoins techniques ainsi qu'une conception d'un prototype. Dans cette branche, on a choisi de suivre le modèle TCP/IP, et on a proposé un prototype sous un simulateur.

IV.4.1. Couche interface réseau (accès réseau) :

C'est la couche la plus basse du modèle TCP/IP. Cette couche contient toutes les spécificités concernant la transmission des données sur un réseau, l'acheminement des données sur la liaison.

IV.4.1.1. Type de câblage choisi :

Les câble FTP / Catégorie 5 peuvent être un bon choix pour leurs caractéristiques : Débit jusqu'à 1Gb/s et facilité d'emploi.

i. La fibre optique :

Une utilisation de la fibre optique est nécessaire si la distance entre les périphériques est supérieure à 100 mètres. La fibre optique, peut être aussi utilisée pour connecter les Switches de distribution au Core afin de garder le bénéfice en termes de Débit.

IV.3.1. Choix du simulateur :

Dans notre travail, on a choisi d'utiliser le GNS3, son principal avantage réside dans l'émulation matérielle, à la différence des simulateurs qui sont souvent une manière limitée de virtualisation du matériel. Grâce à GNS3, on peut tester et estimer, dans des conditions quasi réelles et sans avoir accéder au matériel, les configurations avant de les mettre en place physiquement. Il est préférable de simuler le réseau de n'importe qu'elle entreprise avant l'étape de construction, cela permet de construire un réseau de bonne qualité.

IV.3.2. Modélisation hiérarchique du réseau :

Comme mentionné dans les chapitres précédents, Une conception de LAN hiérarchique comprend les trois couches suivantes : Accès, Distribution et Core. Les équipements réseau utilisées sont présentés dans le (Tableau IV-1) avec leurs nominations :

	core	**Distribution**	**Accès**	**Routeur**
Type de périphérique	Switch multilayer niveau 3 (L3)	Switch niveau 2	Switch niveau 2	Routeur
Nombre de périphériques utilisés	1	6	26	1+1 routeur distant
La nomination	SWF_INT	SWF_MG SWF_CS SWF_OP SWF_S5 SWF_MARK SWF_TRA	SWA_ST SWA_STAND SWA_RH SWA_ACHAT SWA_CONF SWA_INT SWA_COMP1 SWA_SEC SWA_COMPT4 SWA_L02 ...etc.	ROUTER_WAN+ R2

Tableau IV-1 : *Les équipements réseau utilisées.*

La (Figure IV-1) montre l'architecture Hiérarchique de notre réseau en utilisant le GNS3.

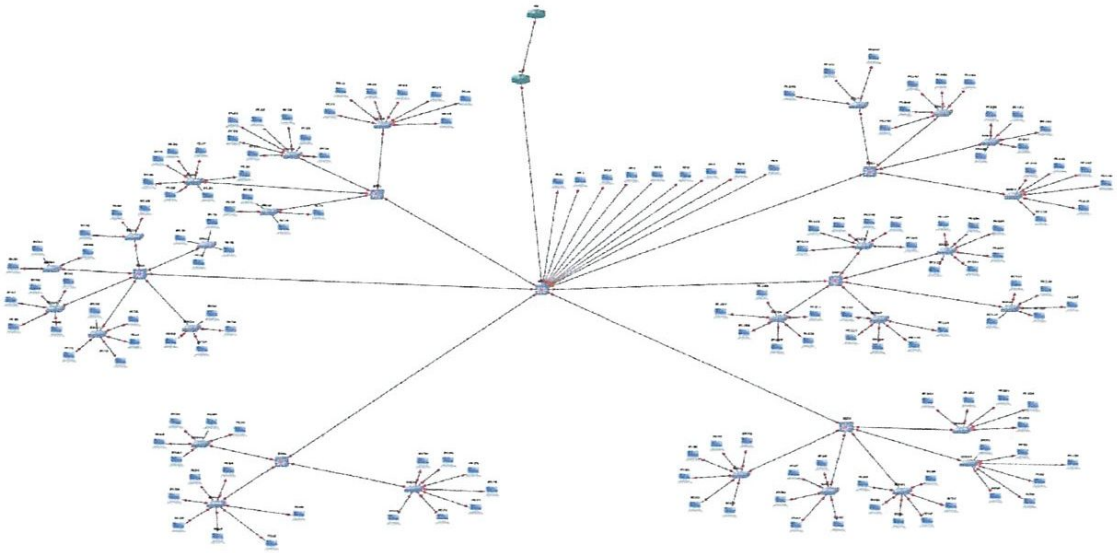


Figure IV-1 : *Modélisation Hiérarchique.*

IV.4. Etude technique :

La branche technique, consiste en une capture des besoins techniques ainsi qu'une conception d'un prototype. Dans cette branche, on a choisi de suivre le modèle TCP/IP, et on a proposé un prototype sous un simulateur.

IV.4.1. Couche interface réseau (accès réseau) :

C'est la couche la plus basse du modèle TCP/IP. Cette couche contient toutes les spécificités concernant la transmission des données sur un réseau, l'acheminement des données sur la liaison.

IV.4.1.1. Type de câblage choisi :

Les câble FTP / Catégorie 5 peuvent être un bon choix pour leurs caractéristiques : Débit jusqu'à 1Gb/s et facilité d'emploi.

La fibre optique :

Une utilisation de la fibre optique est nécessaire si la distance entre les périphériques est supérieure à 100 mètres. La fibre optique, peut être aussi utilisée pour connecter les Switches de distribution au Core afin de garder le bénéfice en termes de Débit.

IV.4.1.2. Topologie utilisée :

Dans notre cas, on a choisi d'utiliser la topologie en étoile, vu qu'elle permet facilement la localiser une panne, le rajout et la suppression des machines, et aussi, la création des réseaux tolérants aux pannes (si une connexion tombe en panne, le reste du réseau reste fonctionnel).

IV.4.1.3. Sécurité de la couche accès réseau :

Pour des raisons de la sécurité et Pour empêcher les accès non autorisés dans notre réseau on peut utiliser la commandes « Shutdown » pour bloquer les adresses MAC non autorisé et anonyme qui se connectes depuis les ports des Switches.

IV.4.2. Couche internet :

La couche Internet définit les datagrammes (paquets de données de la couche IP), Elle permet d'envoyer les datagrammes vers des machines distantes, Cette circulation des paquets (datagrammes) est gérée par le protocole IP.

IV.4.2.1. Adressage :

Le (**Tableau IV-2**) montre l'ensemble des adresses utilisées dans notre configuration.

La classe utilisée	Exemple d'adresses	Cette adresse utilisée dans
A	10.10.8.254	Les VLANs
	10.10.9.254	
	10.10.10.254	
	10.10.20.254	
	10.10.30.254	
	10.10.40.254	
	10.10.50.254	
	10.10.70.254	
	10.10.80.254	
	10.10.90.254	
	10.10.100.254	
	10.10.110.254	
	10.10.120.254	
	10.10.130.254	

	10.10.140.254 10.10.150.254 10.10.160.254 10.10.170.254	
B	172.16.66.254 172.16.66.60 172.16.66.61 172.16.66.62 172.16.66.63 172.16.66.64 172.16.66.65	L'adresse de commutateurs core les adresses de commutateurs de distribution
	172.16.66.48 172.16.66.28 172.16.66.27 172.16.66.26 172.16.66.41 172.16.66.42 172.16.66.46 172.16.66.22 172.16.66.21 172.16.66.19 172.16.66.9 172.16.66.15 172.16.66.13 172.16.66.40 172.16.66.2 172.16.66.3 172.16.66.5 172.16.66.8 172.16.66.44 172.16.66.17 172.16.66.45 172.16.66.43	Les adresses de commutateurs d'accès

	172.16.66.18 172.16.66.47 172.16.66.24 172.16.66.23 172.16.66.112	
C	192.168.1.254	Adresse de routeur

Tableau IV-2 : *les adresses IP utilisés.*

IV.4.2.2. Sécurité de la couche internet :

Dans notre travail, et afin de garantir la sécurité au niveau internet, on a utilisé :

i. Les Vlans :

Un réseau local virtuel (ou VLAN) est un groupe d'unités réseau ou d'utilisateurs qui ne sont pas limités à un segment de commutation physique. Les unités ou les utilisateurs d'un VLAN peuvent être regroupés par fonction, service, application, etc., et ce, quel que soit le segment physique où ils se trouvent. (16)

Les ports d'accès transportent le trafic d'un VLAN spécifique attribué au port. Un port trunk est par défaut membre de tous les VLAN et achemine par conséquent le trafic de tous les VLAN (4) .Pour configurer les Vlans, on a mis toutes les interfaces Switch-Switch en mode Trunk et les interfaces Switch-Machine en mode Access.

```
!
interface Ethernet0/2
 switchport trunk encapsulation dot1q
 switchport mode trunk
 duplex auto
!
```

Figure IV-2 : *Configuration du mode trunk entre commutateur core et commutateur de distribution.*

```
interface Ethernet0/1
 switchport access vlan 10
 switchport mode access
 duplex auto
!
```

Figure IV-3 : *Configuration du mode Access entre commutateur Access et un hôte*

Le vlan de management "Vlan 66" sera utilisé pour l'administration des équipements. Les adresses IP de management seront attribuées aux équipements.

ii. Les ACLs :

Une ACL (Access Control List) est une liste utilisée pour le filtrage des paquets. Les ACLs permettent d'autoriser ou d'interdire des paquets, que ce soit en entrée ou en sortie.
La figure représente un exemple d'une ACL étendu nommée GUEST_ACCESS_DENY a était créé pour que les étrangers de l'entreprise ne peuvent pas communiquer avec les équipements de réseaux interne qui font part aux réseaux 172.16.66.0, 10.10.0.0 ou 172.16.7.0.

```
Extended IP access list GUEST_ACCESS_DENY
    10 deny ip any 10.10.0.0 0.0.255.255
    20 deny ip any 172.16.7.0 0.0.0.255
    30 deny ip any 172.16.66.0 0.0.0.255
    40 permit ip any any
```

Figure IV-4 : *exemple des ACLs.*

IV.4.2.3. Les autres protocoles de la couche internet :

Dans cette couche on a configuré les protocoles suivants :

i. Le WCCP :

Le Web Cache Communication Protocol (WCCP) est un protocole de routage de contenu développé par Cisco. Il fournit un mécanisme de redirection des flux de trafics en temps réel. Il a des fonctionnalités intégrées de répartition de charge, d'évolutivité, de tolérance de panne et de garantie de service. (8)
On a utilisé aussi le WCCP pour activer la redirection vers le proxy. Les serveurs proxy permettent de sécuriser et d'améliorer l'accès à certaines pages Web en les stockant en cache (ou copie) pour réduire le temps d'attente.
On applique la redirection des flux de trafics entrant au routeur sur l'interface de routeur liée au switch core.

```
!
interface FastEthernet0/0
description LINK TO THE INTERFACE SW_CORE_NET f1
ip address 172.16.7.1 255.255.255.252
ip access-group facebook in
ip wccp web-cache redirect in
ip wccp 90 redirect in
```

Figure IV-5: *exemple de l'utilisation de WCCP*

ii. Le NETFLOW :

Le Net Flow est une technologie Cisco IOS qui fournit des statistiques sur les paquets traversant un routeur ou un commutateur multicouche Cisco. NETFLOW est la norme pour la collecte de données opérationnelles IP à partir de réseaux IP. (4)

Dans la (Figure IV-6) on a cité un exemple de notre configuration de net flow. On a choisi deux machines pour enregistrer les statistiques des paquets traversant le routeur.

```
ip flow-export version 5
ip flow-export destination 10.10.201.33 7761
ip flow-export destination 10.10.60.189 9996
!
```

Figure IV-6 : *un exemple de net flow.*

iii. Type de routage utilisé

Le but du routage est de définir une route ou un chemin à un paquet quand celui-ci arrive sur un routeur. Donc son but est d'assurer qu'il existe toujours un chemin pour aller d'un réseau à un autre. Il existe deux modes de routages : routage statique et routage dynamique. Dans notre travail on a utilisé le routage statique vu qu'il offre plusieurs avantages par rapport au routage dynamique, notamment : Les routes statiques ne sont pas annoncées sur le réseau et ça donne une meilleure sécurité ; les protocoles de routage statiques utilisent moins de bande passante que les protocoles de routage dynamiques.

Dans la (Figure IV-7), un exemple de configuration d'un routage statique. La passerelle par default est 10.25.101.161, pour atteindre le réseau 10.10.0.0 ou 172.16.66.0 il faut passer par l'adresse de l'interface du Core liée au routeur.

```
ip route 0.0.0.0 0.0.0.0 10.25.101.161
ip route 10.10.0.0 255.255.0.0 172.16.7.2
ip route 172.16.66.0 255.255.255.0 172.16.7.2
!
```

Figure IV-7: *routage statique.*

IV.4.3. Couche transport :

La couche transport est chargée des questions de qualité de service touchant la fiabilité, le contrôle de flux et la correction des erreurs. (16). Pour garantir la sécurité et le bon fonctionnement à ce niveau on a configuré les protocoles suivants :

IV.4.3.1. Le NAT :

On ne peut pas accéder à Internet avec des adresses IP privées, donc, une translation d'adresse en un public est nécessaire. Dans la (Figure IV-8) l'adresse de la machine 10.10.160.250 sera 193.194.69.193 sur internet.

```
ip nat inside source static 10.10.160.250 193.194.69.193
ip nat inside source static 10.10.201.30 193.194.69.201
```

Figure IV-8 : *exemple de NAT.*

IV.4.3.2. Le PAT :

Le NAT dynamique utilise le mécanisme de translation de port (PAT - Port Address Translation), c'est-à-dire l'affectation d'un port source différent à chaque requête de telle manière à pouvoir maintenir une correspondance entre les requêtes provenant du réseau interne et les réponses des machines sur Internet.
Dans la (Figure IV-9) on a créé un pool d'adresses publiques pour mapper les adresses privées et on a créé une liste d'accès nommé PER_ACC.

```
ip nat pool CRBT 193.194.69.194 193.194.69.200 netmask 255.255.255.240
ip nat inside source list PER_ACC pool CRBT overload
```

Figure IV-9 : *exemple de PAT.*

```
!
ip nat pool CRBT 193.194.69.194 193.194.69.200 netmask 255.255.255.240
ip nat inside source list PER_ACC pool CRBT overload
ip nat inside source static 10.10.160.250 193.194.69.193
ip nat inside source static 10.10.201.30 193.194.69.201
ip nat inside source static tcp 10.10.60.245 8080 193.194.69.202 8080 extendable
ip nat inside source static tcp 10.10.60.230 80 193.194.69.202 8090 extendable
ip nat inside source static tcp 10.10.201.60 80 193.194.69.203 80 extendable
!
!
```

Figure IV-10 : *exemple 2 de PAT.*

IV.4.4. Couche application :

Dans cette couche, Le modèle TCP/IP regroupe en une seule couche tous les aspects liés aux applications et suppose que les données sont préparées de manière adéquate pour la couche suivante. (16). Dans notre configuration on a utilisé les protocoles suivant :

IV.4.4.1. Le DHCP :

L'utilisation d'un serveur DHCP permet de distribuer les adresses IP aux machines automatiquement sans avoir besoin de saisir les adresses manuellement. On a configuré au niveau du routeur un serveur DHCP pour distribuer les adresses automatiquement.

```
ip dhcp pool VLAN8
 network 10.10.8.0 255.255.255.0
 default-router 10.10.8.254
 dns-server 208.67.222.222 208.67.220.220
 domain-name CRBT-D2
!
```

Figure IV-11 : *exemple de DHCP de VLAN 8.*

IV.4.4.2. HTTPS :

On a utilisé le protocole HTTPS parce qu'il permet d'envoyer et de recevoir des informations des serveurs web d'une façon sécurisée en utilisant le cryptage de donnée
La (Figure IV-12) montre notre configuration de ce Protocol, tout d'abord il faut activer le protocole http, ensuite activer le protocole HTTPS au niveau du routeur.

```
ip http server
ip http access-class 24
ip http authentication local
ip http secure-server
```

Figure IV-12 : *activation de protocole HTTPS*

IV.4.4.3. SSH :

Le SSH crypte la session de connexion et empêche ainsi tout agresseur de recueillir des mots de passe. Pour augmenter le niveau de sécurité on a utilisé ce protocole pour tout accès aux équipements.

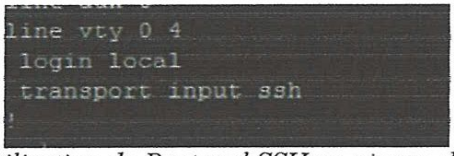


***Figure** IV-13 : utilisation du Protocol SSH au niveau de la ligne virtuel.*

IV.5. Réalisation

Une fois, les besoins fonctionnels et techniques sont établis, on passe à la partie réalisation dans laquelle on injecte toutes nos configurations sur notre prototype.

IV.5.1. Résumé de la configuration

Pour chaque équipement, une configuration est nécessaire pour un bon fonctionnement et une bonne sécurité. Les tableaux ci-dessous montrent un résumé des configurations sur les différents équipements.

IV.5.1.1. La configuration d'un des switches d'accès :

La configuration d'un des switches d'accès	**Description**
hostname SWA_int	nom de commutateur
ip domain-name CRBT-DZ.ORG	Configuration du nom de domaine
ip ssh version 2	L'utilisation du Protocol SSH pour sécuriser l'accès aux commutateurs
interface Ethernet0/1 switchport access vlan 60 switchport mode access	Configurer l'interface 0/1 en mode Access et la rajouter au VLAN 60.
interface Vlan66 ip address 172.16.66.44 255.255.255.0	Définitions de l'adresse de l'équipement
ip default-gateway 172.16.66.254	L'adresse de passerelle pour le vlan 66
snmp-server community lms_mgmt RO snmp-server community lms_mgmt_rw RW	récupérer les informations statistiques sur les équipements
line con 0 line vty 0 4 password crbtpass	Sécuriser vty avec un mot de passe et désactiver le protocole Telnet et utiliser le SSH pour l'accès au commutateur

login local transport input ssh	

Tableau IV-3 : *La configuration d'un des switches d'accès.*

IV.5.1.2. La configuration d'un des commutateurs de distribution :

La configuration d'un commutateur de distribution	**Description**
hostname SWD_OP	Configuration du nom
username lms_user privilege 15 password 7 151E061F11392E3638322631	Configuration d'un username et mots de passe
ip domain-name CRBT-DZ.ORG	Configuration du nom de domaine
ip ssh version 2	Active le protocol ssh
interface Ethernet0/0 switchport trunk encapsulation dot1q switchport mode trunk	Active le mode trunk pour passer différents vlans
interface Ethernet0/1 switchport trunk encapsulation dot1q switchport mode trunk	Active le mode trunk pour passer différents vlans
interface Ethernet0/2 switchport trunk encapsulation dot1q switchport mode trunk	Active le mode trunk pour passer différents vlans
interface Ethernet0/3 switchport trunk encapsulation dot1q switchport mode trunk	Active le mode trunk pour passer différents vlans
interface Ethernet1/3 switchport trunk encapsulation dot1q switchport mode trunk	Active le mode trunk pour passer différents vlans
interface Vlan66 ip address 172.16.66.61 255.255.255.0	Adresse de l'équipement
ip default-gateway 172.16.66.254	L'adresse de passerelle
ip http server	Active le protocol http

ip http secure-server	Active le protocol https
snmp-server community lms_mgmt RO snmp-server community lms_mgmt_rw RW	Pour récupérer les informations statistiques sur les équipements
line vty 0 4 password 7 0508140D355C4F1A0A login local transport input ssh	Sécuriser vty avec un mots de passé et désactiver le protocole Telnet pour l'accès au commutateur

Tableau IV-4 : *configuration d'un des commutateurs de distribution.*

IV.5.1.3. La configuration du routeur :

La configuration de routeur	**Description**
hostname ROUTER_WAN	Nom de routeur
username CRBT privilege 15 password 0 CRBT	Configuration d'un compte administrateur
interface FastEthernet0/0	Choisir l'interface fastethernet0/0 pour la Configuration de l'interface liée avec le commutateur core
description LINK TO THE INTERFACE SW_CORE_NET INT FI1	Ajouter une description
ip address 172.16.7.1 255.255.255.252	L'adresse IP de l'interface liée avec le commutateur core
ip access-group facebook in	Application des ACL d'Access liste nommé Facebook pour les paquete entrante au routeur
ip wccp web-cache redirect in ip wccp 90 redirect in	application du proxy
ip flow ingress ip flow egress	Les statistiques des paquets entrante et sortante de routeur
ip NAT inside	Pour activer le Nat des adresses entrantes sur l'interface
interface FastEthernet0/1	Configuration de l'interface lié avec le router distant

ip address 10.25.101.162 255.255.255.252 ip flow ingress ip flow egress ip nat outside	« L'adresse ip le Netflow des paquets entrante et sortante et activer le nat pour les adresses sortante »
interface FastEthernet1/0 ip address 192.168.1.254 255.255.255.0 ip access-group facebook in	Configuration de la deuxième interface liée avec le router distant et applications de l'acl de facebook pour les paquets entrante au routeur
ip http server ip http access-class 23 ip http secure-server	activation du protocol http activation d'acl pour http activation de protocole https
ip http timeout-policy idle 60 life 86400 requests 10000	La durée de la session inactive
ip flow-export version 5 ip flow-export destination 10.10.201.99 7761 ip flow-export destination 10.10.60.189 9996	Choisir l'adresse de l'hôte qui contient les statistiques des paquets traversant le routeur
ip nat pool CRBT 193.194.69.194 193.194.69.200 netmask 255.255.255.240	Création du pool d'adresses
ip nat inside source list PER_ACC pool CRBT overload	Création du pat
ip nat inside source static 10.10.160.1 193.194.69.193	NAT statique
ip nat inside source static 10.10.201.1 193.194.69.201	NAT statique
ip nat inside source static tcp 10.10.60.245 8080 193.194.69.202 8080 extendable	Configuration du PAT

ip nat inside source static tcp 10.10.60.230 80 193.194.69.202 8090 extendable	Configuration du PAT
ip nat inside source static tcp 10.10.201.60 80 193.194.69.203 80 extendable	Configuration du PAT
ip route 0.0.0.0 0.0.0.0 10.25.101.161	Configuration du routage statique
ip route 10.10.0.0 255.255.0.0 172.16.7.2	Configuration du routage statique
ip route 172.16.66.0 255.255.255.0 172.16.7.2	Configuration du routage statique
ip access-list extended PER_ACC	Configuration d'une ACL étendu nommée
permit ip 10.10.200.0 0.0.0.255 any permit ip host 172.16.66.201 any permit ip host 172.16.66.202 any permit ip 10.10.50.0 0.0.0.255 any permit ip host 10.10.201.10 any permit ip host 10.10.201.20 any permit ip 10.10.10.0 0.0.0.255 any permit ip 10.10.20.0 0.0.0.255 any permit ip 10.10.30.0 0.0.0.255 any permit ip 10.10.40.0 0.0.0.255 any permit ip 10.10.60.0 0.0.0.255 any permit ip 10.10.70.0 0.0.0.255 any permit ip 10.10.80.0 0.0.0.255 any permit ip 10.10.90.0 0.0.0.255 any permit ip 10.10.100.0 0.0.0.255 any permit ip 10.10.110.0 0.0.0.255 any permit ip 10.10.120.0 0.0.0.255 any permit ip 10.10.130.0 0.0.0.255 any permit ip 10.10.140.0 0.0.0.255 any permit ip 10.10.150.0 0.0.0.255 any permit ip 10.10.160.0 0.0.0.255 any	

permit ip 10.10.8.0 0.0.0.255 any permit ip 10.10.170.0 0.0.0.255 any permit ip 10.10.9.0 0.0.0.255 any permit ip host 10.10.201.30 any permit ip host 10.10.201.55 any permit ip host 10.10.201.40 any	
ip access-list extended VPN-out permit tcp any any eq 47 permit tcp any any eq 1723 permit gre any any permit ip any any	Configuration d'une ACL vpn-out
ip access-list extended acl_http permit tcp 10.10.0.0 0.0.255.255 any eq www	Configuration d'acl pour http
ip access-list extended acl_wsas permit ip host 10.10.200.1 any permit ip host 10.10.200.2 any	Configuration d'ACL pour iron port
ip access-list extended facebook deny tcp any 31.13.24.0 0.0.7.255 eq 443 deny tcp any 31.13.64.0 0.0.31.255 eq 443 deny tcp any 31.13.69.0 0.0.0.255 eq 443 deny tcp any 31.13.72.0 0.0.0.255 eq 443 deny tcp any 31.13.73.0 0.0.0.255 eq 443 deny tcp any 31.13.75.0 0.0.0.255 eq 443 deny tcp any 31.13.76.0 0.0.0.255 eq 443	Access liste pour bloquer Facebook

IV.5.1.4. Notre configuration du switch de core :

La configuration du switch de core	Description
hostname SWF_INT	Le nom de switch
username admincrbt privilege 15 secret 4	Configuration d'un utilisateur
ip routing	Activation du Protocol pour le routage inter-vlan
ip dhcp excluded-address 10.10.60.254 ip dhcp excluded-address 10.10.8.254 ip dhcp excluded-address 10.10.10.254 ip dhcp excluded-address 10.10.20.254 ip dhcp excluded-address 10.10.30.254 ip dhcp excluded-address 10.10.40.254 ip dhcp excluded-address 10.10.50.254 ip dhcp excluded-address 10.10.70.254 ip dhcp excluded-address 10.10.80.254 ip dhcp excluded-address 10.10.90.254 ip dhcp excluded-address 10.10.100.254 ip dhcp excluded-address 10.10.110.254 ip dhcp excluded-address 10.10.120.254 ip dhcp excluded-address 10.10.130.254 ip dhcp excluded-address 10.10.140.254 ip dhcp excluded-address 10.10.150.254 ip dhcp excluded-address 10.10.160.254 ip dhcp excluded-address 10.10.170.254	Les adresses IP à ne pas donner par le DHCP
ip dhcp pool VLAN8 network 10.10.8.0 255.255.255.0 default-router 10.10.8.254 dns-server 208.67.222.222 208.67.220.220 domain-name CRBT-DZ	La configuration du pool d'adresse DHCP pour le vlan 8
ip dhcp pool VLAN9 network 10.10.9.0 255.255.255.0	La configuration du pool d'adresse DHCP pour le vlan 9

default-router 10.10.9.254 dns-server 10.10.201.20 208.67.222.222 domain-name crbt.local	
ip dhcp pool VLAN10 network 10.10.10.0 255.255.255.0 default-router 10.10.10.254 dns-server 10.10.201.20 208.67.222.222 domain-name crbt.local	La configuration du pool d'adresse DHCP pour le vlan 10
ip dhcp pool VLAN20 network 10.10.20.0 255.255.255.0 default-router 10.10.20.254 dns-server 10.10.201.20 208.67.222.222 domain-name crbt.local	La configuration du pool d'adresse DHCP pour le vlan 20
ip dhcp pool VLAN30 network 10.10.30.0 255.255.255.0 default-router 10.10.30.254 dns-server 10.10.201.20 208.67.222.222 domain-name crbt.local	La configuration du pool d'adresse DHCP pour le vlan 30
ip dhcp pool VLAN40 network 10.10.40.0 255.255.255.0 default-router 10.10.40.254 dns-server 10.10.201.20 208.67.222.222 domain-name crbt.local	La configuration du pool d'adresse DHCP pour le vlan 40
ip dhcp pool VLAN50 network 10.10.50.0 255.255.255.0 default-router 10.10.50.254 dns-server 10.10.201.20 208.67.222.222 domain-name crbt.local	La configuration du poold'adresse DHCP pour le vlan 50
ip dhcp pool VLAN60 network 10.10.60.0 255.255.255.0 default-router 10.10.60.254 dns-server 10.10.201.20 208.67.222.222 domain-name crbt.local	La configuration du poold'adresse DHCP pour le vlan 60

ip dhcp pool VLAN80 network 10.10.80.0 255.255.255.0 default-router 10.10.80.254 dns-server 10.10.201.20 208.67.222.222 domain-name crbt.local	La configuration du poold'adresse DHCP pour le vlan 80
ip dhcp pool VLAN90 network 10.10.90.0 255.255.255.0 default-router 10.10.90.254 dns-server 10.10.201.20 208.67.222.222 domain-name crbt.local	La configuration du poold'adresse DHCP pour le vlan 90
ip dhcp pool VLAN100 network 10.10.100.0 255.255.255.0 default-router 10.10.100.254 dns-server 10.10.201.20 208.67.222.222 domain-name crbt.local	La configuration du pool d'adresse DHCP pour le vlan 100
ip dhcp pool VLAN110 network 10.10.110.0 255.255.255.0 default-router 10.10.110.254 dns-server 10.10.201.20 208.67.222.222 domain-name crbt.local	La configuration du pool d'adresse DHCP pour le vlan 110
ip dhcp pool VLAN120 network 10.10.120.0 255.255.255.0 default-router 10.10.120.254 dns-server 10.10.201.20 208.67.222.222 domain-name crbt.local	La configuration du pool d'adresse DHCP pour le vlan 120
ip dhcp pool VLAN130 network 10.10.130.0 255.255.255.0 default-router 10.10.130.254 dns-server 10.10.201.20 208.67.222.222 domain-name crbt.local	La configuration du pool d'adresse DHCP pour le vlan 130
ip dhcp pool VLAN140 network 10.10.140.0 255.255.255.0 default-router 10.10.140.254	La configuration du pool d'adresse dhcp pour le vlan 140

dns-server 10.10.201.20 208.67.222.222 domain-name crbt.local	
ip dhcp pool VLAN150 network 10.10.150.0 255.255.255.0 default-router 10.10.150.254 dns-server 10.10.201.20 208.67.222.222 domain-name crbt.local	La configuration du pool d'adresse dhcp pour le vlan 150
ip dhcp pool VLAN160 network 10.10.160.0 255.255.255.0 default-router 10.10.160.254 dns-server 10.10.201.20 208.67.222.222 domain-name crbt.local	La configuration du pool d'adresse dhcp pour le vlan 160
ip dhcp pool VLAN170 network 10.10.170.0 255.255.255.0 default-router 10.10.170.254 dns-server 10.10.201.20 208.67.222.222 domain-name crbt.local	La configuration du pool d'adresse dhcp pour le vlan 170
ip domain-name CRBT-DZ.ORG	La Configuration du nom de domaine
spanning-tree mode pvst spanning-tree extend system-id spanning-tree vlan 1-300 priority 24576	Pour éviter les boucles dans le cas de l'utilisation de lien redondant
ip ssh version 2	Activation de SSH
interface Ethernet1/1 switchport trunk encapsulation dot1q switchport mode trunk interface Ethernet1/0 switchport trunk encapsulation dot1q switchport mode trunk interface Ethernet0/3 switchport trunk encapsulation dot1q switchport mode trunk	La Configuration des interfaces en mode trunk pour envoyer le trafic des differents vilans

interface Ethernet0/2 switchport trunk encapsulation dot1q switchport mode trunk interface Ethernet0/1 switchport trunk encapsulation dot1q switchport mode trunk interface Ethernet1/2 switchport trunk encapsulation dot1q switchport mode trunk	
interface Ethernet0/0 description LINK TO THE ROUTER_WAN PORT FI1 no switchport ip address 172.16.7.2 255.255.255.252 interface Ethernet2/0 switchport access vlan 201 switchport mode access interface Ethernet2/1 description LINK TO MANAGEMENT WSA2 switchport access vlan 66 switchport mode access interface Ethernet2/2 switchport access vlan 10 switchport mode access interface Ethernet2/3 description LINK TO THE WSA1 PORT P1	Configure l'interface liée avec le routeur " l'adresse IP et l'ajout de la description de l'interface " Active le mode Access pour les hôtes connecté directement au commutateur core

switchport access vlan 200 switchport mode access interface Ethernet3/0 description LINK TO THE WSA2 PORT P1 switchport access vlan 200 switchport mode access interface Ethernet3/1 description VLAN MANAGEMENT PORT switchport access vlan 66 switchport mode access interface Ethernet3/2 description VLAN MANAGEMENT PORT switchport access vlan 66 switchport mode access interface Ethernet3/3 description LINK TO THE MANAGEMENT WSA1 switchport access vlan 66 switchport mode access	
interface Vlan8 ip address 10.10.8.254 255.255.255.0 ip access-group GUEST_ACCESS_DENY in interface Vlan9 ip address 10.10.9.254 255.255.255.0 interface Vlan10 ip address 10.10.10.254 255.255.255.0	La configuration des interfaces des vlan On a appliqué l'acl GUEST_ACCESS_DENY sur vlan8 pour permettre l'accès juste à internet

```
interface Vlan20
 ip address 10.10.20.254 255.255.255.0

interface Vlan30
 ip address 10.10.30.254 255.255.255.0

interface Vlan40
 ip address 10.10.40.254 255.255.255.0

interface Vlan50
 ip address 10.10.50.254 255.255.255.0

interface Vlan60
 ip address 10.10.60.254 255.255.255.0
interface Vlan66
 ip address 172.16.66.254 255.255.255.0
 ip access-group
MANAGEMENT_ACCESS_PERMIT in

interface Vlan70
 ip address 10.10.70.254 255.255.255.0

interface Vlan80
 ip address 10.10.80.254 255.255.255.0

interface Vlan90
 ip address 10.10.90.254 255.255.255.0

interface Vlan100
 ip address 10.10.100.254 255.255.255.0

interface Vlan110
 ip address 10.10.110.254 255.255.255.0
```

interface Vlan120 ip address 10.10.120.254 255.255.255.0 interface Vlan130 ip address 10.10.130.254 255.255.255.0 interface Vlan140 ip address 10.10.140.254 255.255.255.0 interface Vlan150 ip address 10.10.150.254 255.255.255.0 interface Vlan160 ip address 10.10.160.254 255.255.255.0 interface Vlan170 ip address 10.10.170.254 255.255.255.0 interface Vlan180 ip address 10.10.180.254 255.255.255.0 interface Vlan192 ip address 192.168.1.254 255.255.255.0 interface Vlan200 ip address 10.10.200.254 255.255.255.0 interface Vlan201 ip address 10.10.201.254 255.255.255.0	
ip http server	Pour active le Protocol http
ip route 0.0.0.0 0.0.0.0 172.16.7.1	Configure le routage statique
ip access-list extended GUEST_ACCESS_DENY	Configure les ACLs

remark PERMIT GUEST TO ACCESS ONLY INTERNET deny ip any 10.10.0.0 0.0.255.255 deny ip any 172.16.7.0 0.0.0.255 deny ip any 172.16.66.0 0.0.0.255 permit ip any any	
ip access-list extended MANAGEMENT_ACCESS_PERMIT permit ip 172.16.66.0 0.0.0.255 10.10.60.0 0.0.0.255 permit ip 10.10.60.0 0.0.0.255 172.16.66.0 0.0.0.255 permit ip host 10.10.201.10 172.16.66.0 0.0.0.255 permit ip host 10.10.201.40 172.16.66.0 0.0.0.255 permit ip 172.16.66.0 0.0.0.255 host 10.10.201.10 permit ip 172.16.66.0 0.0.0.255 host 10.10.201.40 deny ip 10.10.0.0 0.0.255.255 172.16.0.0 0.0.255.255 permit ip any any	Configuration des ACLs
snmp-server community lms_mgmt RO snmp-server community lms_mgmt_rw RW	Pour récupérer les informations statistiques sur les équipements
linc vty 0 4 login local transport input ssh	Désactiver le Telnet pour l'accès au commutateur

Tableau IV-6 : *configuration du switch de core.*

IV.5.2. Test et validation de configuration :

Une fois le prototype soit configuré. Un ensemble de test sera nécessaire pour valider notre configuration. Un test Ping est nécessaire en premier lieu afin de garantir la connectivité entre les équipements et communication entre les VLANs, puis on teste le reste des protocoles activés.

IV.5.2.1. Test du routage inter-Vlans :

La (Figure IV-14) montre un Ping réussis entre le PC40 (10.10.10.1) et le PC10 (10.10.60.1) qui appartiennent aux différents VLANs (pc 40 : vlan 10) et le (pc 10 : vlan 60).

```
PC40> ping 10.10.60.1
84 bytes from 10.10.60.1 icmp_seq=1 ttl=63 time=10.608 ms
84 bytes from 10.10.60.1 icmp_seq=2 ttl=63 time=8.406 ms
84 bytes from 10.10.60.1 icmp_seq=3 ttl=63 time=9.561 ms
84 bytes from 10.10.60.1 icmp_seq=4 ttl=63 time=8.327 ms
84 bytes from 10.10.60.1 icmp_seq=5 ttl=63 time=7.763 ms
```

Figure IV-14 : *Ping avec l'adresse IP 10.10.60.1 avec succès.*

IV.5.2.2. Test de connectivité entre équipements :

Le Ping passe avec succès entre le commutateur Core et une machine (Figure IV-15).

```
core#ping 10.10.10.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.10.10.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 2/5/11 ms
```

Figure IV-15 : *Ping avec l'adresse IP 10.10.10.1 avec succès.*

IV.5.2.3. Test du NAT :

On a testé le Nat sur l'adresse machine 10.10.60.1 en faisant le Ping entre la machine et l'interface du routeur 10.25.101.162, l'adresse est devenue 193.194.69.205.

```
*Mar  1 01:48:23.807: NAT*: s=10.10.60.1->193.194.69.205, d=10.25.101.62 [15090]
R2#
*Mar  1 01:48:25.619: NAT*: s=10.10.60.1->193.194.69.205, d=10.25.101.62 [15091]
R2#
*Mar  1 01:48:27.559: NAT*: s=10.10.60.1->193.194.69.205, d=10.25.101.62 [15092]
R2#
*Mar  1 01:48:29.403: NAT*: s=10.10.60.1->193.194.69.205, d=10.25.101.62 [15093]
R2#
```

Figure IV-16 : *test de Nat.*

IV.5.2.4. Test du NetFlow :

Les statistiques des paquets sont enregistrés au niveau des machines (10.10.201.33) et (10.10.60.189) traversant l'interface du routeur 172.16.7.1, la (Figure IV-17) contient les détails des statistiques.

```
R2#sh ip flow expor
Flow export v5 is enabled for main cache
  Exporting flows to 10.10.201.33 (7761) 10.10.60.189 (9996)
  Exporting using source IP address 172.16.7.1
  Version 5 flow records
  57 flows exported in 47 udp datagrams
  0 flows failed due to lack of export packet
  0 export packets were sent up to process level
  0 export packets were dropped due to no fib
  0 export packets were dropped due to adjacency issues
  0 export packets were dropped due to fragmentation failures
  0 export packets were dropped due to encapsulation fixup failures
```

Figure IV-17 : *les statistiques du netflow.*

IV.5.2.5. Test des ACL :

On a créé le VLAN 8 pour que les étrangers de l'entreprise puissent se connecter à notre réseau afin de se connecter à Internet, sans qu'ils puissent accéder aux serveurs internes. Pour cela on a utilisé les ACLs afin de les limités. L'exemple suivant montre qu'une machine appartenant au VLAN 8 ne pourra en aucun cas atteindre une machine à l'intérieur du réseau.

```
PC26> ping 10.10.60.1
*10.10.8.254 icmp_seq=1 ttl=255 time=11.285 ms (ICMP type:3, code:13, Communication administratively prohibited)
*10.10.8.254 icmp_seq=2 ttl=255 time=4.754 ms (ICMP type:3, code:13, Communication administratively prohibited)
*10.10.8.254 icmp_seq=3 ttl=255 time=4.143 ms (ICMP type:3, code:13, Communication administratively prohibited)
*10.10.8.254 icmp_seq=4 ttl=255 time=3.603 ms (ICMP type:3, code:13, Communication administratively prohibited)
*10.10.8.254 icmp_seq=5 ttl=255 time=4.488 ms (ICMP type:3, code:13, Communication administratively prohibited)
```

Figure IV-18 : *Ping ne passe pas entre machine (10.10.8.1) (vlan 8) et la machine (10.10.60.1)*

IV.6. Conclusion :

Dans ce chapitre, on a montré par notre exemple, comment construire un réseau pour une moyenne entreprise, en suivant le Processus de développement 2TUP, et le Modèle de référence TCP/IP. Dans chaque couche du modèle, plusieurs configurations sont nécessaires afin de garantir la sécurité, la tolérance aux pannes et la facilité du troubleshooting.

Conclusion générale

Conclusion générale

Comment installer un réseau évolutif et tolérant aux pannes, comment choisir ses composants, comment le protéger ?

Dans ce mémoire de fin d'étude, on a montré les techniques de base à suivre pour répondre à ces questions, et on a fait une présentation des outils qui peuvent être utiles dans la construction et le troubleshooting de n'importe quel réseau d'une moyenne entreprise.

Dans l'étape de l'étude du réseau, on a proposé de suivre le processus de développement 2TUP, décomposant ainsi l'étude en deux parties, fonctionnelles et techniques.

Au niveau de l'étude fonctionnelle, on a choisi d'utiliser une architecture à trois niveaux (Access, Distribution et Core), puis une simulation de ce réseau en utilisant un très bon outil, qui est le GNS3. Dans la partie technique, et pour une bonne configuration et sécurisation de notre réseau, on a choisi de suivre le modèle TCP/IP. Pour chaque couche du modèle on a fait un ensemble de choix qui améliore le réseau ainsi que sa sécurité.

Ce mémoire, peut-être une référence pour la construction d'un réseau d'une moyenne entreprise, il permet d'apprendre les notions de bases ainsi que les différentes configurations nécessaires pour la construction d'un réseau tolérant aux pannes, sécurisé et évolutif.

Bibliographie

Bibliographie :

1. Tanenbaum, Andrew. *Les réseaux, interdiction, 3ème Edition.* 1998.

2. Andrew Tanenbaum, David Wetherall. *Réseaux, 5e édition.* france : Pearson Education, 2011.

3. Servin, Claude. *RÉSEAUX ET TÉLÉCOMS.* paris : Dunod, 2003. ISBN 2 10 007986 7.

4. *CCNA* . [pdf] s.l. : CISCO.

5. Latu, Philippe. *Adressage IPv4.* [pdf] Toulouse-france : IUT - Université Toulouse III - Paul Sabatier.

6. EXPLORATION, CISCO. *Comprendre les adresses IP v4.* [pdf] s.l. : cisco.

7. MORGE, Maxime. *Inititation aux réseaux informatiques.* [pdf] sanit-etienne : s.n.

8. wikipedia. *wikipedia.* [En ligne] [Citation : 20 mai 2016.] https://fr.wikipedia.org/wiki/File_Transfer_Protocol.

9. wikipédia. *wikipédia.* [En ligne] [Citation : 25 mai 2016.] https://fr.wikipedia.org/wiki/Hypertext_Transfer_Protocol.

10. wikipédia. *wikipédia.* [En ligne] [Citation : 2 juin 2016.] https://fr.wikipedia.org/wiki/Dynamic_Host_Configuration_Protocol.

11. wikipédia. *wikipédia.* [En ligne] [Citation : 20 avril 2016.] https://fr.wikipedia.org/wiki/Domain_Name_System.

12. Amine, Mr RIAHLA Med. *Modèle TCP/IP.* [pdf] Boumerdes : Université de BOUMERDES UMBB, 2008/2009.

13. Comer, Douglas. *TCP/IP Archetecture,protocoles et application 5e édition.* 2009.

14. Dean, Piette, Bessens, Villeneuve, Simond. *Réseaux informatiques, 2e édition.* s.l. : RYNALD GOULET, 2002. ISBN : 2-89377-266-8.

15. Jaumard, B. *Les équipements d'interconnexion.* [pdf] 2003. IFT3320/IFT6320.

16. Boulbaba, Mr LABIADH. *Mise en place des réseaux LAN interconnectés en redondance par 2 réseaux WAN.* TUNIS : UNIVERSITE VIRTUELLE DE TUNIS, 2010/2011.

17. ATELIN, Philippe. *WI-FI :Réseaux sans fil,2éme édition.*

18. Philippe ATELIN, José DORDOIGNE. *Réseaux informatiques,Notions fondamentales (Protocoles, Architectures, Réseaux sans fil...).* s.l. : Editions ENI, 2006.

19. Cédric Llorens, Laurent Levier, Denis Valois,. *Tableaux de bord de la sécurité réseau 2 éme édition.* Paris : ÉDITIONS EYROLLES, 2006. ISBN2-212-11973-9.

20. Zalewski, Michal. *Menaces sur le réseau.* paris : person, 2008. ISBN-13: 978-2744040313.

21. kaspersky. *kaspersky.* [En ligne] [Citation : 11 mars 2016.] http://www.kaspersky.fr/internet-security center/definitions/malicious-code.

22. rabah, lbsir. *approche de secuité dans les systemes embrauques.* LAGHOUAT-algérie : UNIVERSITE DE LAGHOUAT.

23. Marc Berenguier, Jean-Christophe Fillot. *Dynamips - Un émulateur de routeur Cisco sur PC.* [pdf] Compiègne : Université de Technologie de Compiègne, Service Informatique.

24. FELIX, Patrick. *ASR2 Réseau.* [pdf] Bordeaux : IUT Informatique Bordeaux1 , 2010.

25. Péan, Bruno. *support de cour réseau EISTI.* [pdf] CERGY : EISTI (École internationale des sciences du traitement de l'information), 2001.

26. Pujolle, Guy. *initiation aux réseaux Cours et exercices.* paris : Eyrolles, 2001. ISBN : 2-212-28108-0.

27. cisco. *Utilisation de base de Cisco Network Assistant.* [pdf] USA : cisco, cisco Systems, 2004-2006. OL-11448-01.

28. Amine, Mr RIAHLA Med. *La couche Transport du modéle OSI.* [pdf] BOUMERDES : Université de BOUMERDES UMBB, 2008/2009.