République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique
Université Abderrahmane MIRA de Béjaïa
Faculté des Sciences Exactes
Département d'Informatique

Mémoire De Fin De Cycle

En vue d'obtention du diplôme de Master professionnel en Informatique spécialité : Administration et Sécurité des Réseaux

Thème

Optimisation du réseau et de sa partie sécurité de la RTC-SONATRACH de Béjaïa

Réalisé par :

M^{elle}. SOUMARI Soumia et M^{elle}. TARAFT Cilia

Soutenu devant le jury composé de :

D^{r}. AMAD Mourad	**Président**
M^{me}. HALFOUNE Nadia	**Examinatrice**
D^{r}. BOUDRIES Abdelmalek	**Encadreur**
M^{r}. ARKOUB Malek	**Encadreur**

Promotion 2014 /2015

Avant tout, nous remercions Dieu tout puissant de nous avoir donné le courage et la patience de terminer ce travail.

Nous tenons à remercier et exprimer notre profonde gratitude et vifs remerciements à notre encadreur Mr A.M.BOUDRIES pour ses encouragements, ses conseils et ses efforts à fin de terminer ce travail.

Nous exprimons aussi notre gratitude et remerciements aux Président et membres de jury pour l'intérêt qu'ils ont porté à notre travail et pour l'honneur qu'ils nous font de bien vouloir le juger.

Nous exprimons une attitude vis-à-vis de Mr M.ARKOUB l'encadreur de stage pour sa patience, ses encouragements et sa disponibilité.

Nos sincères remerciements s'adressent à nos parents, nos frères, nos sœurs ainsi qu'à toute la famille pour leur soutien moral, leur encouragement inconditionnel et leurs aisés financiers.

Sans oublier de remercier tous les enseignants et enseignantes qui, pendant notre cursus universitaire, ont veillé pour notre formation et réussite.

Tous les mots restent faibles pour exprimer notre profonde reconnaissance à tous ceux qui nous ont aidé de prés ou de loin pour la réalisation de ce travail, en particulier tous nos ami(e)s pour leur soutien moral et leur présence à nos côtés.

Louange à Dieu, le miséricordieux, sans lui rien de tout cela n'aurait pu être.

Je dédie ce modeste travail et ma profonde gratitude à ma mère et mon père pour l'éducation qu'ils m'ont prodigué, avec tous les moyens et au prix de tous les sacrifices qu'ils ont consentis à mon égard, pour le sens du devoir qu'ils m'ont enseigné depuis mon enfance; Que dieu leur procure bonne santé et longue vie.

À mes frères et sœurs. À tous(tes) mes amis(es) dont la liste est longue.

À mon binôme Cilia, ainsi qu'à toute sa famille.

À toute personne qui ma aider et encourager de prêt ou de loin toute au long de mes études.

SOUMARI. Soumia

Je dédie ce modeste travail à mes très chers et respectueux parents qui m'ont soutenus tout en long de ma vie, Que dieu leur procure bonne santé et longue vie. À mes frères et sœurs.

À mes amis(e) et collègues de la promo. A mon binôme Soumia, ainsi qu'à toute sa famille.

À touts ceux qui me sont proches et ceux qui ont contribué à ma formation.

TARAFT.Cilia

Table des matières

CHAPITRE II: Organisme d'accueil

CHAPITRE III: Planification & Réalisation

Liste des figures

Liste des tableaux

Liste des abréviations

AD	**A**ctive **D**irectory
AVVID	**A**rchitecture for **V**oice, **V**ideo and Integrated **D**ata
CIFS	**C**ommon **I**nternet **F**ile **S**ystem
CLI	**C**ommand **L**anguage **I**nterface
DHCP	**D**ynamic **H**ost **C**onfiguration **P**rotocol
DMZ	**D**e**M**ilitarized **Z**one
DNS	**D**omain **N**ame **S**ystem
DRGB	**D**irection **R**égionale de **T**ransport de **B**éjaïa
FTP	**F**ile **T**ransfer **P**rotocol
GPO	**G**roup **P**oliciers **O**bject
HTTP	**H**yper **T**ext **T**ransfer **P**rotocol
IBM	**I**nternational **B**usiness **M**achines
ISO	**I**nternational **S**tandardization **O**rganization
LAN	**L**ocal **A**rea **N**etwork
LMS	**L**AN **M**anagemen**t** **S**olution
MAN	**M**etropolitan **A**rea **N**etwork
NCP	**N**etware **C**ore **P**rotocol
NetBEUI	**Net**Bios **E**xtended **U**ser **I**nterface
NFS	**N**etwork **F**ile **S**ystem
OSI	**O**pen **S**ystems **I**nterconnection
PAN	**P**ersonal **A**rea **N**etwork
PC	**P**ersonal **C**omputer
RAN	**R**egional **A**rea **N**etwork
RTC	**R**égion **T**ransport **C**entre

SGBD	**S**ystème de **G**estion De **B**ase **D**onnées
SMB	**S**erver **M**essage **B**lock
SMTP	**S**imple **M**ail **T**ransfer **P**rotocol
SONATRACH	**SO**ciété **NA**tional de **TRA**nsport par **C**analisation des **H**ydrocarbures
SPX	**S**equenced **P**acket e**X**change
SQL	**S**tructured **Q**uery **L**anguage
STP	**S**hielded **T**wisted **P**air
TCP/IP	**T**ransmission **C**ontrol **P**rotocol / **I**nternet **P**rotocol
UDP	**U**ser **D**atagram **P**rotocol
UTP	**U**nshielded **T**wisted **P**air
VLAN	**V**irtual **L**ocal **A**rea **N**etwork
VTP	**V**LAN **T**runking **P**rotocol
WAN	**W**ide **A**rea **N**etwork

Introduction générale

Depuis les premières inventions des systèmes informatiques jusqu'à nos jours, on constate que chaque époque est marquée par une évolution technologique. Actuellement, la technologie des réseaux prend de plus en plus d'ampleur dans les systèmes informatiques. Aujourd'hui, l'utilisation de cette dernière pour développer et renforcer notre réseau arrive à un tournant. La rapidité avec laquelle les réseaux se sont intégrés à notre quotidien est tout simplement stupéfiante. Les interconnexions complexes entre périphériques et supports électroniques qui constituent le réseau sont transparentes pour les millions d'utilisateurs qui ont fait du réseau un élément important et personnel dans leur vie.

Un réseau peut être considéré comme un ensemble de ressources mises en place pour offrir un ensemble de services. Pour parvenir à une meilleure gestion de leurs ressources et informations, nombreuses sont les entreprises qui se sont dotées d'un réseau. Bien que la croissance d'une entreprise soit généralement souhaitée, elle s'accompagne d'un certain nombre de contraintes, telle que l'augmentation rapide du nombre d'utilisateurs, résultant ainsi un volume accru du trafic généré par ces derniers. Par conséquent, on rencontre le problème de baisse des performances du réseau. Donc, une bonne organisation du réseau remédiera à ces problèmes.

Le stage que nous avons effectué à la SONATRACH (RTC) de Béjaïa, nous a permit de découvrir leur réseau, leur partie sécurité et de comprendre leurs fonctionnement, le but de notre travail est d'optimiser le réseau et de sa partie sécurité de la RTC de Béjaïa avec des critiques et des solutions proposées plus modernes et fiables pour ce dernier afin que la communication entre les différentes stations distantes soit bien effectuée.

Afin d'atteindre les objectifs sollicités, nous avons organisé ce travail en trois chapitres : Le premier chapitre sera consacré à la partie **« Généralités sur les réseaux informatiques »** il a pour objectifs de définir les principaux concepts pour la compréhension des réseaux informatiques.

Le deuxième chapitre sera basé à la partie **« Organisme d'accueil »**. En effet, nous présenterons la structure d'accueil de SONATRACH et le centre où nous avons effectué notre stage et la présentation de l'architecture réseau ainsi que la partie système et la partie sécurité.

Le dernier chapitre concerne **« Planification & Réalisation »**, il comporte la simulation, l'implémentation des VLANs et la présentation des critiques avec une étude descriptible et la mise en œuvre des solutions proposées, ainsi que les tests de validation pour vérifier si vraiment les objectifs ont été atteints. Enfin, nous compléterons ce mémoire par une conclusion générale.

chapitre I

Généralités sur les réseaux informatique

Introduction

Les réseaux informatiques sont nés du besoin de faire communiquer des terminaux distants avec un site central, puis des ordinateurs entre eux, et enfin de connecter des machines terminales telles que des stations de travail avec leurs serveurs.

Les réseaux informatiques sont devenus incontournables aujourd'hui. Omniprésents dans les entreprises et chez les particuliers, ils servent à mettre en œuvre des applications très diverses, des plus simples aux plus sophistiquées. La plus populaire est la navigation sur le web, grâce à laquelle il est facile de partager des informations de toutes natures (textes, photos, vidéos, etc.) via Internet.

L'objectif de ce chapitre est de présenter les concepts de base liés aux réseaux informatiques. Ces notions formeront la base nécessaire à notre contribution.

I.1. Définition d'un réseau informatique

Ils sont destinés à relier des équipements informatiques (serveurs, ordinateurs, etc.) pour permettre l'échange de données binaires issus d'applications ou de processus informatiques tels que les traitements de textes, les bases de données, ou les navigateurs Internet.

Ils permettent aussi le partage de ressources informatiques (imprimantes, disques durs, etc.). Ces réseaux étaient uniquement destinés au transport des données informatiques, mais la tendance actuelle est vers le transport du son et de la vidéo **[1]**.

I.2. Utilité des réseaux

On distingue deux types d'objectifs principaux des réseaux **[2]**:

I.2.1. Les objectifs techniques

- Partage des ressources logicielles et matérielles, ce qui permet de diminuer les coûts.
- La fiabilité (un réseau permet une duplication des données et limite ainsi les pertes de ces données).

I.2.2. Les objectifs des utilisateurs

- La communication est l'aspect le plus intéressant pour un utilisateur. Elle peut prendre la forme de courrier électronique, téléphonie mobile, etc.
- L'accès distant à l'information (banques, bourses, bibliothèque en ligne, etc.).

I.3. Classification des réseaux

Les caractéristiques permettant de différencier les familles de réseaux portent sur la distance et le mode de transmission de données. On peut classifier les réseaux en cinq types comme le montre la figure I.1 **[3]** :

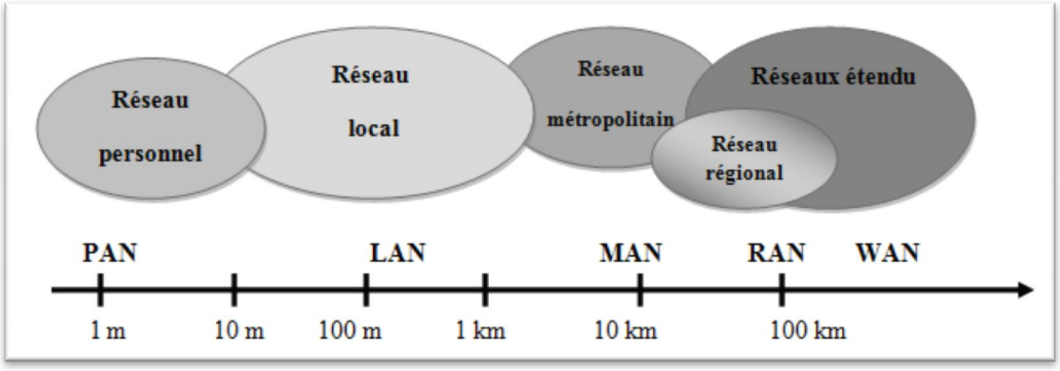


Figure I.1 : Types de réseaux

I.3.1. Les réseaux PAN : Les réseaux personnels, ou PAN (Personal Area Network), interconnectent sur quelques mètres des équipements personnels tels que les portables, d'un même utilisateur.

I.3.2. Les réseaux LAN : Local Area Network ou réseau local, permettent de connecter deux à plusieurs centaines de machines à l'intérieure d'une même enceinte. Il s'agit de la plupart des réseaux informatiques présents dans les entreprises.

I.3.3. Les réseaux MAN : Métropolitain Area Network, il s'agit d'un réseau dont la couverture s'étale à une ville. Le principe est de relier les différents réseaux locaux mais les normes des transmissions sont différentes. Un MAN est une série de réseaux locaux interconnectés à l'échelle d'une ville.

I.3.4. Les réseaux RAN : Les réseaux régionaux, ou RAN (Regional Area Network), ont pour objectif de couvrir une large surface géographique. Dans le cas des réseaux sans fil, les RAN peuvent avoir une cinquantaine de kilomètres de rayon, ce qui permet, à partir d'une seule antenne, de connecter un très grand nombre d'utilisateurs.

I.3.5. Les réseaux WAN : Wide Area Network ou réseau de grande taille, interconnecte des réseaux MAN pour assurer une couverture et une interconnexion au niveau d'un pays, voire à travers le monde .Ce type de réseau utilise les satellites pour certaines interconnexions. Le WAN le plus célèbre est le réseau public Internet, dont le nom provient de cette qualité : Inter Networking, ou interconnexion de réseaux.

I.4. Topologies des réseaux

Une topologie caractérise la façon dont les différents équipements réseaux sont positionnés les une par rapport aux autres. On distingue la topologie physique, relative au plan du réseau et la topologie logique qui précise la façon dont les informations circulent au plus bas niveau. Les interconnexions entre nœuds du réseau s'effectuent en liaison point à point, c'est à un dire un avec un, ou en multipoint, soit n à n **[3]**.

I.4.1. La topologie physique

I.4.1.1. En bus

La topologie en bus (support linéaire) comme le montre la figure I.2 repose sur un câblage, sur lequel viennent se connecter des nœuds (postes de travail, équipements d'interconnexion, périphériques).Il s'agit d'un support multipoints. Le câble est l'unique élément matériel constituant le réseau et seuls les nœuds génèrent les signaux.

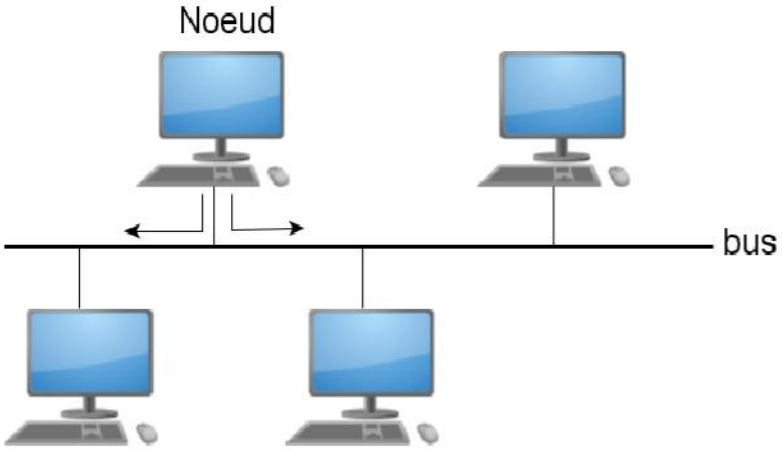


Figure I.2 : Architecture en bus

La topologie en bus ne nécessite pas une grande quantité de câbles ni de point centraux, par contre son inconvénient majeur est dû au fait que si le bus est coupé, les stations ne pourront pas s'échanger des informations sur le réseau.

I.4.1.2. En étoile

La topologie en étoile repose, quant à elle, sur des matériels actifs. Un matériel actif remet en forme les signaux et les régénère.

Ces points centraux sont appelés des concentrateurs (hubs). Il est possible de créer une structure hiérarchique en constituant un nombre limité de niveaux.

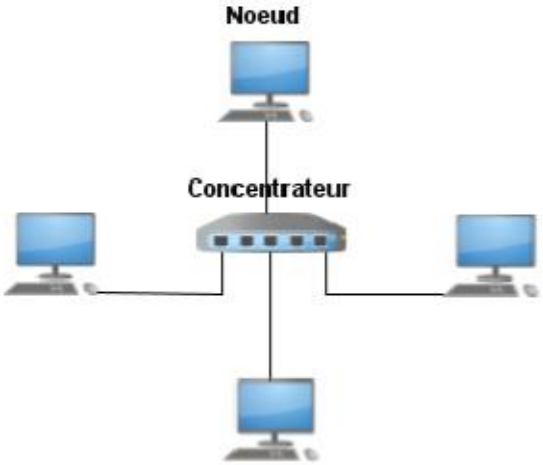


Figure I.3 : Architecture en étoile

La figure I.3 illustre une topologie en étoile, dans ce type de topologie une panne ne touche qu'une seule branche (sauf si c'est le point central qui est touché).

I.4.1.3. En anneau

Cette topologie repose sur une boucle fermée, en anneau (ring), constituée de liaisons point à point entre périphériques. Les trames transitent par chaque nœud qui se comporte comme un répéteur (élément actif).La figure I.4 illustre une topologie en anneau, Il existe soit la topologie en anneau simple soit la topologie en double boucle FDDI (Fiber Distributed Data Interface), qui permet une redondance et qui comme son nom l'indique est formé de deux anneaux.

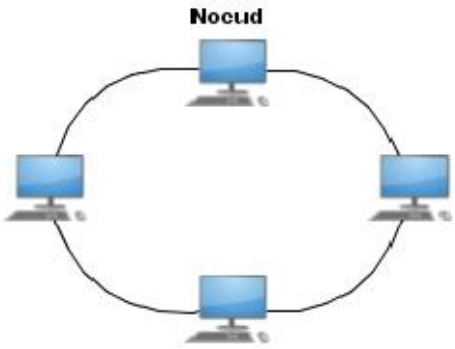


Figure I.4 : Architecture en anneau

I.4.2. La topologie logique

La topologie logique représente la manière dont les équipements s'échangent les données sur le réseau local. Mais elle ne dépend pas de la façon dont les équipements sont raccordés entre eux. Pratiquement, deux topologies logiques sont à considérer : le bus et l'anneau. Deux types de connexion existent :

I.4.2.1. Point à Point

Par une interface réseau sans fils, deux nœuds peuvent communiquer directement. On parle également de liaison de type pair à pair (Peer to Peer) ou ad hoc. Une telle configuration est possible dans les techniques Bluetooth ou Wifi.

I.4.2.2. Multipoints

Les réseaux sans fil peuvent aussi être mis en œuvre par un nombre plus important d'ordinateurs à travers un point d'accès sans fils ; celui-ci permet d'interconnecter plusieurs ordinateurs en faisant office de passerelle pour l'accès au réseau local (Physiquement câblé).

I.5. Architectures des réseaux

I.5.1. Le modèle OSI (Open System Interconnect)

Le modèle OSI a été utilisé pour concevoir les réseaux ARPANET. Normalisé par ISO (International Standard Organization), le modèle OSI est le standard en matière de normalisation de tous les systèmes ouvert.

Le modèle OSI présente une structure en couche. Chaque couche fournit des services à la couche directement supérieure.

Les concepts architecturaux utilisés pour décrire le modèle de référence à sept couches, proposé par l'ISO, sont décrits dans la norme ISO 7498-1. La figure 1.5 schématise le fonctionnement du modèle OSI **[3]**.

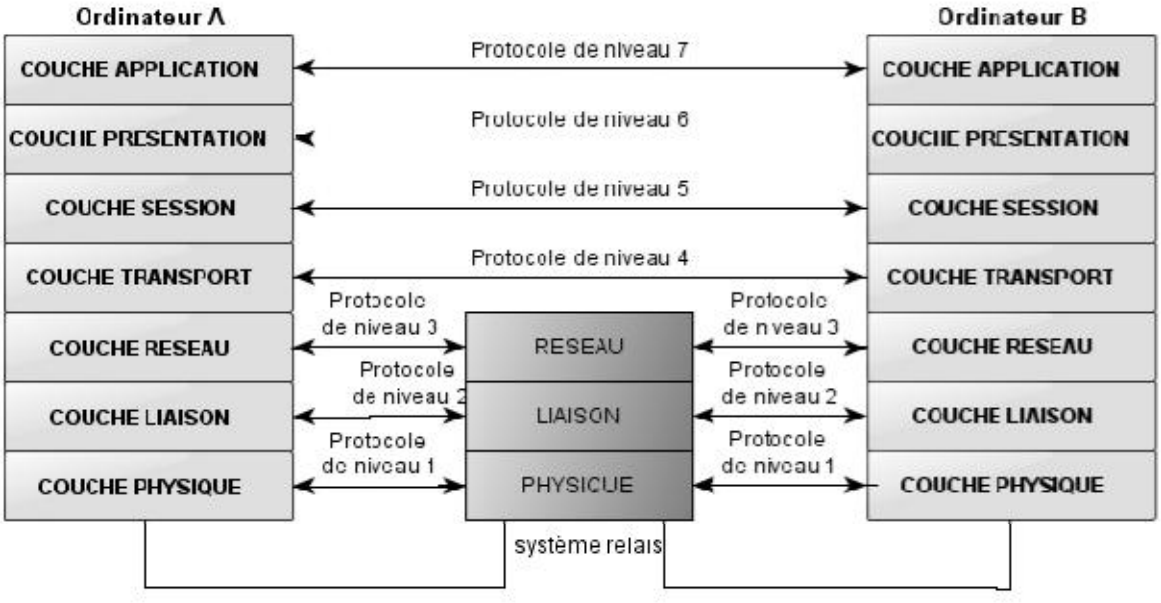


Figure I.5 : Modèle OSI

- **La couche Physique :**

  Elle assure le transfert des bits sur le support de transmission. À cet effet, elle définit les spécifications mécaniques (connecteur), électriques (niveau de tension), et les spécifications fonctionnelles des éléments de raccordement nécessaires à l'établissement, au maintien et à la libération de la ligne.

- **La couche Liaison :**

  Elle assure un service de transfert de blocs de données (trames) entre deux systèmes adjacents en assurant le contrôle, l'établissement, le maintien et la libération du lien logique entre les entités. Elle permet en outre, de détecter les erreurs inhérentes aux supports physiques.

- **La couche Réseaux :**

  La couche réseau doit permettre d'acheminer correctement les paquets d'informations jusqu'à l'utilisateur final. Pour aller de l'émetteur au récepteur, il faut passer par des nœuds de transfert intermédiaire interconnectant deux ou plusieurs réseaux. Cette couche assure trois fonctionnalités principales : le contrôle de flux, le routage et l'adressage.

- **La couche Transports :**

  Elle est la couche pivot du modèle OSI. Elle assure le contrôle du transfert de bout en bout lors du transfert des informations (messages) entre les deux extrémités communicantes. Elle est la dernière couche de contrôle des informations, elle doit assurer aux couches supérieures un transfert fiable quelle que soit la qualité du sous-réseau de transport utilisé.

- **La couche Session :**

  Elle gère l'échange de données entre les applications distantes. La fonction essentielle de cette couche est la synchronisation des échanges et la définition de points de reprise.

- **La couche Présentation :**

  Cette couche assure la mise en forme des données pour qu'elles soient accessibles à l'utilisateur. Elle effectue les fonctions de codage, compression, cryptage, décryptage, etc.

- **La couche Application :**

  Cette couche est le point de contact entre l'utilisateur et le réseau, c'est donc elle qui apporte à l'utilisateur les services de base offerts par le réseau, comme par exemple le transfert de fichiers, la messagerie, etc.

I.5.2. Le modèle TCP / IP

L'architecture TCP/IP porte le nom des protocoles principaux qui la constituent, à savoir TCP (Transmission Control Protocol) et IP (Internet Protocol), on l'a définie dans les années 1960 pour le réseau ARPANET. Elle s'est considérablement développée avec le succès d'Internet [**4]**.

Cette architecture est constituée de quatre couches, telle qu'elle est décrite dans la figure I.6 **[5]** :

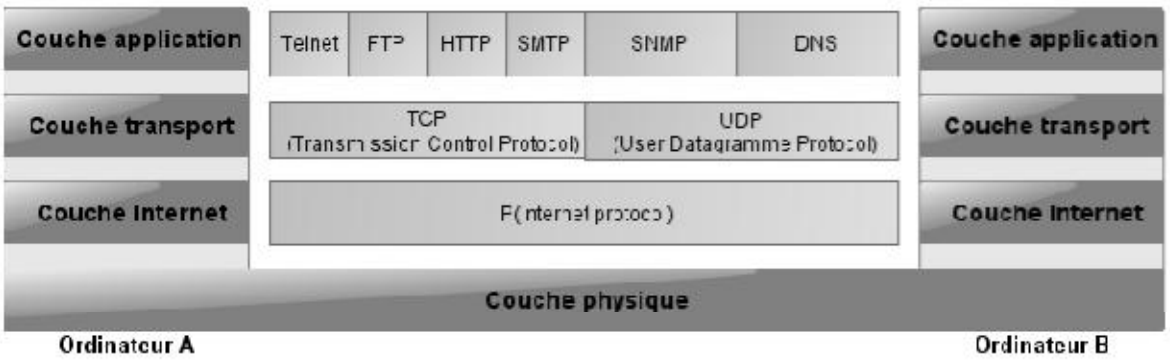


Figure I.6 : Modèle TCP / IP

- **La couche Physique**

  Aucune caractéristique particulière n'est requise pour l'infrastructure du ou des réseaux physiques traversés. La couche physique est donc quelconque.

- **La couche Internet**

  Elle assure la communication entre les réseaux grâce au protocole IP. On utilise la commutation de paquets de type datagramme. Le protocole IP gère les datagrammes, il les achemine jusqu'à leur destinataire, IP définit un service sans garantie de délai ou de fiabilité de communication.

- **La couche Transport**

  Elle définit deux protocoles de transport, un en mode connecté TCP, et un autre en mode non connecté UDP (User Datagram Protocol). Le protocole TCP est destiné à fiabiliser les

échanges avec le contrôle de flux, le contrôle d'erreur et le contrôle de séquence entre les deux extrémités. Le protocole UDP est non fiable, il sert aux applications dites temps réel qui nécessite des temps de traitement optimisés telle que la vidéo.

- **La couche Application**

  Elle contient tous les protocoles de haut niveau qu'un utilisateur souhaite avoir à sa disposition tels que Telnet (utilitaire permettant l'utilisation de programmes sur des machines distantes via un réseau), FTP (File Transfer Protocol), SMTP (Simple Mail Transfer Protocol), HTTP (Hyper Text Transfer Protocol), et autres.

I.6. Modes de communication

Il existe deux modes de communication dans le réseau : le modèle client/serveur et le modèle point à point.

I.6.1. Mode clients/serveurs

Le modèle client/serveur présentée dans la figure I.7 désigne un mode de communication, dans un réseau, qui définit une machine généralement très puissante en terme de capacité d'entrée-sortie, qui est le serveur, fournissant des services à un ensemble machines (une ou plusieurs) qui sont des clients qui lui envoient des requêtes. Les services fournis sont exploités par des programmes s'exécutant sur les machines clientes **[6]**.

Figure I.7 : Mode client/serveur

Le tableau I.1 montre les avantages et les inconvénients de modèle client / serveur :

Les avantages	Les inconvénients
Les sauvegardes de données sont centralisées, donc beaucoup plus faciles à mettre en œuvre. Les systèmes d'exploitation de serveurs proposent des fonctions avancées de sécurité que l'on ne trouve pas sur les réseaux "Peer to Peer". Un administrateur gère le fonctionnement du réseau et les utilisateurs n'ont pas à s'en préoccuper. Les serveurs sont conçus pour le partage de ressources et ne servent pas de station de travail. Il suffit de les dimensionner en fonction de la taille du réseau et du nombre de clients susceptibles de s'y connecter. Ils proposent également des fonctions avancées à l'usage des utilisateurs comme par exemple les profils itinérants qui permettent à un utilisateur (sous certaines conditions) de retrouver son environnement de travail habituel, même s'il change de poste de travail.	La mise en place d'un tel réseau est beaucoup plus lourde qu'un cas simple de "poste à poste". Si un serveur tombe en panne, ses ressources ne sont plus disponibles. Il faut donc prévoir des solutions plus ou moins complexes, plus ou moins onéreuses, pour assurer un fonctionnement au moins minimum en cas de panne. Elle nécessite impérativement la présence d'un administrateur possédant les compétences nécessaires pour faire fonctionner le réseau. Le coût est évidemment plus élevé puisqu'il faut la présence d'un ou de plusieurs serveurs.

Tableau I.1 : Avantages et inconvénients du mode client/serveur

I.6.2. Mode point à point

Dans le modèle point à point (voir la figure I.8), contrairement au mode client/serveur, il n'y a pas de serveur dédié, c'est à dire que chaque ordinateur est à la fois serveur et client. Cela signifie que chaque ordinateur du réseau est libre de partager ses ressources.

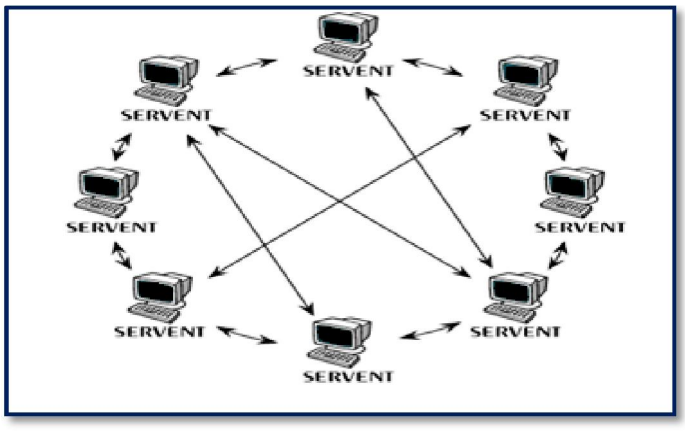


Figure I.8 : Mode point à point

Le tableau I.2 décrit les avantages et les inconvénients du mode point à point :

Les avantages	Les inconvénients
Il est facile de mettre en réseau des postes qui étaient au départ isolés. Chaque utilisateur peut décider de partager l'une de ses ressources avec les autres postes. Dans un groupe de travail, l'imprimante peut être utilisée par tous. Cette méthode est pratique et peu coûteuse pour créer un réseau domestique.	Chaque utilisateur a la responsabilité du fonctionnement du réseau. Les outils de sécurité sont très limités. Si un poste est éteint ou s'il se "plante", ses ressources ne sont plus accessibles. Le système devient ingérable lorsque le nombre de postes augmente. Lorsqu'une ressource est utilisée sur une machine, l'utilisateur de cette machine peut voir ses performances diminuer.

Tableau I.2 : Avantages et inconvénients du mode point à point

I.7. Protocoles réseaux

- **NetBEUI**

  Développé par Microsoft et IBM à l'époque des premiers réseaux de PC, ce protocole simplissime fonctionne très bien sur de petits réseaux. Malheureusement, son efficacité décroît avec le nombre de postes. De plus, il n'est pas "routable", ce qui fait que l'on ne peut interconnecter des réseaux NetBEUI autrement que par des ponts.

- **IPX/SPX**

  Développé par la société NOVELL, qui s'est octroyé la part du lion dans les premiers réseaux de PC avant que Microsoft ne développe Windows NT. Plus efficace que NetBEUI pour les gros réseaux, ce protocole est plus routable ce qui augmente les possibilités d'interconnexions.

- **DNS**

  Le Domain Name System (système de noms de domaine) est un service permettant d'établir une correspondance entre une adresse IP et un nom de domaine et, plus généralement, de trouver une information à partir d'un nom de domaine.

- **DHCP**

  Le protocole DHCP (Dynamic Host Configuration Protocol) est un standard IP conçu pour simplifier la gestion de la configuration d'IP hôte. Le standard DHCP permet d'utiliser des serveurs DHCP comme une méthode de gestion d'affectation dynamique d'adresses IP et d'autres détails de configuration correspondants pour les clients DHCP d'un réseau **[7]**.

I.8. Configuration matérielle

I.8.1. La carte réseau

La carte réseau montrée dans la figure I.9 est employée pour faire communiquer le PC avec d'autres éléments, tels que des ordinateurs, des serveurs ou des imprimantes. Elle vient aussi s'intégrer sur la carte mère. Il faut prendre en compte certains éléments pour la sélection d'une carte :

- Type de réseau : 10, 100 ou 1000Mbps, c'est à dire la vitesse de communication.
- Type de média : C'est en fait le type de câble qui va être utilisé pour relier la carte réseau à un autre élément réseau. Ce type peut être une fibre optique, un câble à paire torsadée ou des ondes radio (pour les réseaux sans fil).
- Type de bus : C'est en fait le bus sur lequel on va brancher notre carte, cela peut être PCI ou ISA.

Une carte réseau communique de manière parallèle avec la carte mère et de manière sérielle avec le réseau **[3]**.

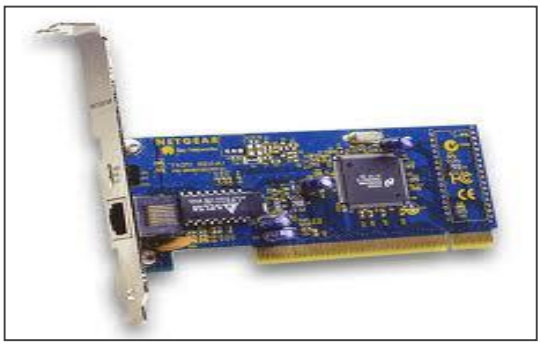


Figure I.9 : Carte réseau

I.8.2. Supports de transmission

Les supports de transmissions transportent des données sous forme de signaux, entre les interfaces réseau. Il existe différents types de supports en fonction du prix, de la simplicité d'installation, de la vitesse, de la résistance aux interférences. On distingue les supports limités, des supports non limités **[3]**.

I.8.2.1. Supports limités

Ce sont des supports palpables, tels que des fils ou des câbles qui conduisent l'électricité ou la lumière. Les principaux supports limités sont la paire torsadée, le câble coaxial, la fibre optique.

- **La paire torsadée :**

Une paire torsadée dans sa forme la plus simple comme l'illustre la figure I.10, est constituée d'une ou de plusieurs paires de fils électriques agencés en spirale. Ce type de support convient à la transmission aussi bien analogique que numérique. Il existe deux types de paires torsadées : la paire torsadée non blindée (UTP – Unshielded Twisted Pair**)** et la paire blindée (STP – Shielded Twisted Pair).

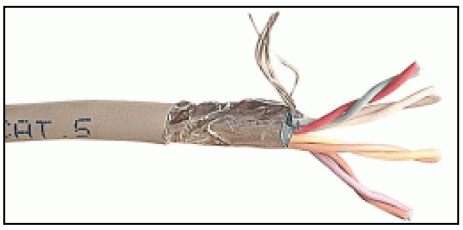


Figure I.10 : Paire torsadée

Il existe différents types de connecteurs pour la paire torsadée, dont voici les principaux :

- RJ-11 câble téléphonique à 2 paires torsadées
- RJ-14 câble téléphonique à 3 paires torsadées
- RJ-45 câble réseau à 4 paires torsadées.

Le connecteur RJ-45 illustré dans la figure I.11 est utilisé aujourd'hui partout, qu'il s'agisse de la connectique réseau ou télécom. Il est même parfois utilisé en téléphonie, à la place du RJ11.

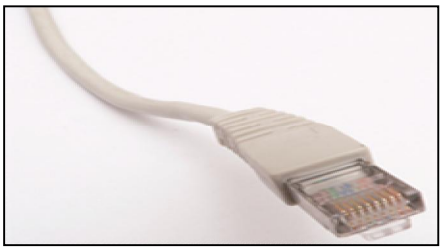


Figure I.11 : Prise RJ-45

- **Le câble coaxial :**

Il est constitué d'un conducteur central en cuivre appelé âme, d'un isolant (ou diélectrique), puis d'un deuxième conducteur comme l'illustre la figure I.12, sous forme de métal tressé, assurant le blindage et enfin d'une gaine plastique assurant la protection mécanique de l'ensemble.

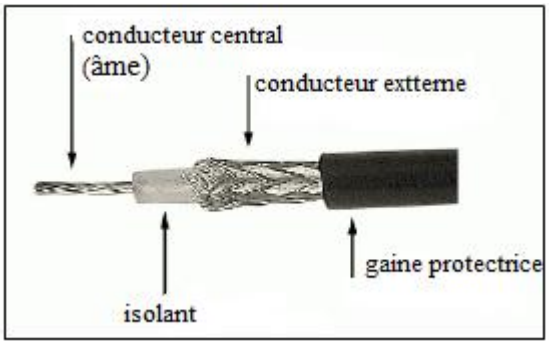


Figure I.12 : Câble coaxial

Le câble coaxial connecté à un connecteur BNC (British Naval Connector) a longtemps été le support privilégié des réseaux locaux. On en retrouve encore dans les milieux industriels.

- **La fibre optique :**

Une fibre optique représentée sur la figure I.13 est un fil en verre ou en plastique très fin qui a la propriété d'être un conducteur de la lumière et sert dans la transmission de données. Elle offre un débit nettement supérieur à celui des câbles coaxiaux. La fibre optique est un guide d'onde qui exploite les propriétés réfractrices de la lumière. Lorsqu'un rayon lumineux entre dans une fibre optique à l'une de ses extrémités avec un angle adéquat, il subit de multiples réflexions et se propage jusqu'à l'autre extrémité en empruntant un parcours en zigzag.

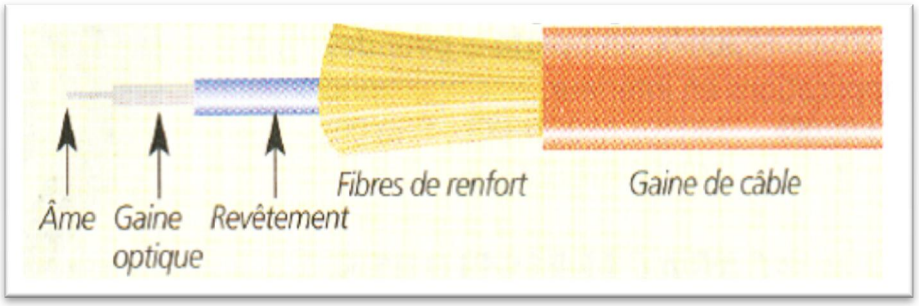


Figure I.13 : Fibre optique

La fibre optique exploite différents connecteurs, qui ont évolué au fil des années. Ainsi, le modèle ST, de forme arrondi avec une baïonnette a tendance à disparaitre.

On retrouve plus couramment l'usage du connecteur à corps extérieur carré de type SC.

De même forme que le SC, le connecteur LC est beaucoup plus petit. Il est inspiré du principe du connecteur RJ45.

Dans le tableau I.3, nous proposons un récapitulatif des principaux supports utilisés **[3]**.

Caractéristiques	Paire torsadée Non blindée (UTP)	Paire torsadée blindée (FTP)	Fibre optique
Prix du câble	Peu chers, (immeubles souvent précâblés)	Plus cher que UTP	Le plus cher des supports
Longueur d'un segment	Environ 100 m	Légèrement plus que UTP	2000 m
Débits courants	100 Mbps	100 Mbps	De 100 Mbps à 2 Gbps
Installation	Très simple	Très simple	Chaque connexion fibre doit être réalisée de manière à ne pas obstruer le passage de la lumière. De plus, un rayon de courbure minimum doit être respecté
Atténuation	Elevée	Faible	Aucune
Sensibilité aux interférences	Sensible	Peu sensible	Aucune
Utilisation habituelle	Réseaux de bureau ou de taille moyenne	Environnements perturbés ou de grande taille	Nécessités de forts débits, interconnexions entre répartiteurs ou bâtiments.

Tableau I.3 : Comparaison des supports de transmission

I.8.2.2. Supports non limités

Les technologies de réseaux sans fils ne sont pas encore au point de remplacer les supports limités, surtout à cause de leurs faibles bandes passantes, mais deviennent de très bons compléments.

- **L'infrarouge :**

Un faisceau de lumière infrarouge est utilisé pour transmettre les données. Ces signaux sont très sensibles à un éclairage trop fort. Il est toutefois possible d'atteindre des vitesses de l'ordre de 10 Mbps sur des distances de 330 mètres maximum.

- **Le laser :**

Comme pour la transmission par infrarouge en visibilité directe, cette technique nécessite un champ de visibilité directe, sensible au problème d'alignement (entre le laser et la

photodiode). Cependant, elle est résistante aux interférences et aux perturbations, mais sensible aux conditions atmosphériques.

- **Les ondes radios terrestres :**

Les technologies de transmission par ondes radio sont les plus prisées actuellement, quelle que soit la taille du réseau. Les usages de ces réseaux sont multiples**.** Par exemple, des ponts sans fils permettent d'interconnecter des réseaux locaux, sans utiliser des supports limités. L'avènement des ordinateurs portables et autres périphériques mobiles a démocratisé l'usage des ondes radio pour les utilisateurs, à travers Bluetooth ou Wifi.

- **Les ondes radios par satellites :**

Les systèmes micro-ondes permettent d'interconnecter des bâtiments répartis sur des zones relativement peu étendues. C'est la méthode la plus utilisée aux Etats-Unis pour transmettre sur des longues distances. Des résultats excellents sont obtenus sur deux points, en visibilité directe (un satellite en orbite géostationnaire et une liaison terrestre, entre deux bâtiments ou sur de grandes étendues).Il est nécessaire de disposer d'une homologation, de deux émetteurs-récepteurs radios, ainsi que d'antennes directionnelles qui doivent être précisément positionnées.

I.8.3. Les outils d'interconnexion

Des matériels sont donc utilisés pour interconnecter les réseaux entre eux. Ils permettent également de segmenter les réseaux de taille importante, en domaines plus petits.

I.8.3.1. Les répéteurs

Un répéteur (transceiver) agit au niveau de la couche physique du modèle OSI. Il reconditionne les données reçues et les retransmet, afin d'accroitre la distance de transmission. En effet, les signaux numériques étant sujets à une forte atténuation, il est nécessaire de retransformer le signal en données, puis les données en signaux **[3]**.

I.8.3.2. Les concentrateurs (hub)

Le hub (voir la figure I.14) est l'élément de base de toute topologie arborescente qu'on rencontre avec le câblage 10BaseT. Le hub agit comme un répéteur, il a une fonction d'amplification du signal et travaille sur la couche physique du modèle OSI. Outre cette fonction première, certains hubs « intelligents » sont capables de remonter des informations

sur le trafic, la charge réseau, les erreurs survenues à l'administrateur réseau pour que celui-ci ait un état de son réseau **[1]**.

Figure I.14 : Hub

I.8.3.3. Les ponts

Un pont (bridge) agit au niveau de la couche liaison de donnée. Il permet ainsi de lier deux ou plusieurs supports physiques différents (voir figure I.15), à condition que les mêmes formats d'adresses MAC soient utilisés des deux cotés **[3]**.

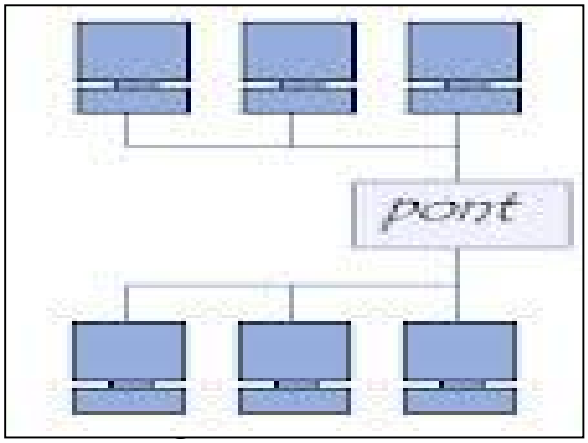


Figure I.15 : Pont

I.8.3.4. Les commutateurs (Switch)

Le Switch illustré sur la figure I.16 est un équipement réseau qui permet d'interconnecter des segments ou des équipements à 10 et/ou 100 Mb/s. Il fonctionne au niveau 2 ou 3 du modèle OSI, tous les ports d'un Switch sont des domaines de collision différents, chaque port d'un Switch apprend dynamiquement les adresses MAC (Ethernet) des équipements qui lui sont connectés.

Le Switch est capable d'apprendre 1024 ou 2048 adresses par port, Certains modèles de Switch peuvent adapter la vitesse de leurs ports (10 ou 100 Mb/s) à la vitesse de l'équipement connecté (auto sensing) **[3]**.

Figure I.16 : Switch

I.8.3.4. Les routeurs

Les routeurs sont plus puissants, ils sont capables d'interconnecter plusieurs réseaux utilisant le même protocole entre eux.

Ils travaillent au niveau de la couche 3 du modèle OSI (couche réseau) et tous les protocoles n'utilisent pas cette couche, c'est pourquoi l'on parle de protocoles "routables" ou "non routables". (NetBEUI n'est pas routable, TCP/IP et IPX/SPX sont des protocoles routables).

Les routeurs disposent d'une table de routage qui leur permet d'aiguiller les trames vers le bon réseau, ils permettent une structure maillée, indispensable pour la construction de l'internet **[7]**. La figure I.17 illustre un routeur :

Figure I.17 : Routeur

I.8.3.5. Les passerelles

Pris au sens large, une passerelle est un outil permettant de passer d'un réseau à un autre telle qu'elle est montrée dans la figure I.18. Dans un réseau TCP/IP, l'adresse du routeur dans le réseau est dite "adresse de passerelle".

Au sens strict du terme, une passerelle est un outil permettant de faire communiquer deux réseaux n'utilisant pas le même protocole **[7]**.

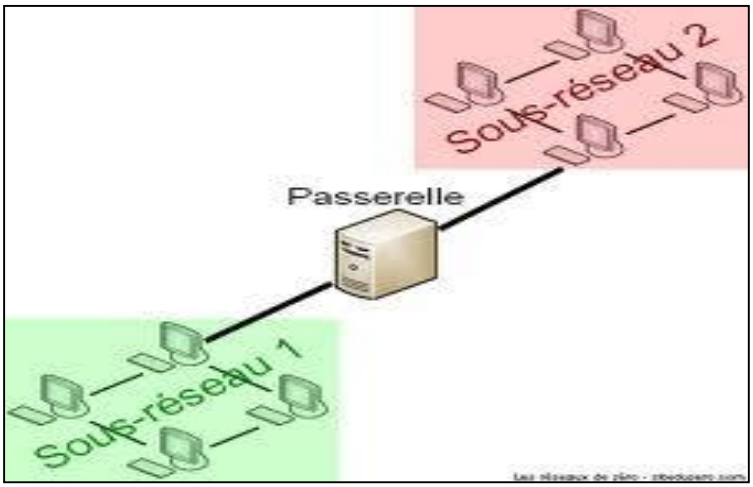


Figure I.18 : Passerelle

I.9. Adressage

I.9.1. L'adresse MAC

Une adresse MAC Ethernet est une valeur binaire de 48 bits exprimée sur 12 chiffres hexadécimaux. Cette adresse est un identifiant physique, stockée dans la mémoire de la carte réseau. Elle identifie donc l'interface réseau de la machine. Le format des adresses peut apparaître sous une forme semblable à 00-05-9A-3C-78-00, 00:05:9A:3C:78:00 ou 0005.9A3C.7800.

Tous les périphériques connectés à un réseau local Ethernet présentent des interfaces dotées d'une adresse MAC. La carte réseau se sert de l'adresse MAC pour déterminer si un message doit être transmis aux couches supérieures à des fins de traitement.

L'adresse MAC est codée en permanence dans une puce de mémoire morte sur une carte réseau. Le terme employé pour désigner ce type d'adresse MAC est « adresse fixe ». Certains constructeurs autorisent la modification locale de l'adresse MAC **[3]**.

I.9.2. L'adresse IP

L'adressage utilisé dans l'internet est un adressage logique. Chaque équipement possède un nom symbolique auquel on fait correspondre une adresse logique appelée « adresse IP ».Celle-ci se décompose en deux parties : l'identifiant du réseau où se trouve l'équipement

et l'identifiant de l'équipement lui-même. L'ensemble tient sur 32 bits, soit 4 octets, chaque adresse est liée à un masque de sous-réseau. Ce qui permet de définir sur quel réseau elle se trouve. L'adresse IP est le plus souvent écrite en notation décimale pointée : les octets sont séparés par des points, et chaque octet représente, en codage binaire naturel, un nombre décimal compris entre 0 et 255. Plusieurs classes d'adresses sont définies : un réseau doté de nombreuses machines dispose d'une adresse avec un champ « identifiant de réseau » court et un champ « identifiant de machine » long. En revanche, dans un petit réseau local, l'identifiant de machine sera codé sur peu de bits. Il existe 5 classes d'adresse IP est qui sont **[5]**:

- **Classe A**

  Cette classe est faite pour les très grands réseaux. Seul le premier octet est utilisé pour la partie réseau, ce qui laisse donc 3 octets pour la partie hôte. Ce premier octet est compris entre 1 et 126. Cette classe peut accueillir plusieurs millions d'hôtes.

- **Classe B**

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

- **Classe C**

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

- **Classe D**

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

- **Classe E**

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

I.10. Réseaux Locaux Virtuels (VLANs)

I.10.1. Définition d'un VLAN

Un VLAN ou réseau virtuel est un regroupement de machines. Ces machines pourront communiquer comme si elles étaient sur le même segment. Un VLAN est assimilable à un domaine de diffusion (Broadcast Domain). Ceci signifie que les messages de diffusion émis par une machine d'un VLAN ne sont reçus que par les machines de ce VLAN.

Les VLANs n'ont été réalisables qu'avec l'apparition des commutateurs (Switchs). Avant, pour réaliser des domaines de diffusion, il était nécessaire de créer des réseaux physiques. Les VLANs permettent de constituer autant de réseaux logiques que l'on désire sur une seule infrastructure physique, réseaux logiques qui auront les mêmes caractéristiques que des réseaux physiques **[5]**.

I.10.2. Avantages d'un VLAN

Le VLAN permet de définir un nouveau réseau au-dessus du réseau physique et à ce titre offre les avantages suivants :

1. La réduction des messages de diffusion (notamment les requêtes ARP) limités à l'intérieur d'un VLAN ainsi les diffusions d'un serveur peuvent être limitées aux clients de ce serveur.
2. La création de groupes de travail indépendants de l'infrastructure physique ; possibilité de déplacer la station sans changer de réseau virtuel.
3. L'augmentation de la sécurité par le contrôle des échanges inter-VLAN utilisant des routeurs (filtrage possible du trafic échangé entre les VLANs).
4. Ils optimisent la bande passante, en réalisant des réseaux disjoints, donc en réalisant des domaines de collision disjoints **[8]**.

I.10.3. Inconvénients d'un VLAN

1. Ils nécessitent une configuration lourde et contraignante sur chaque switch.
2. La sécurité est beaucoup plus faible **[8]**.

I.10.4. Caractéristiques d'un VLAN

- Un VLAN supprime les contraintes physiques relatives aux communications d'un groupe de travail,
- Un VLAN peut couvrir tout un bâtiment, relier plusieurs bâtiments ou encore s'étendre au niveau d'un réseau plus large (WAN),
- Une station peut appartenir à plusieurs VLAN simultanément **[9]**.

I.10.5.Typologie de VLAN

Il existe plusieurs types de VLAN, en fonction de leurs méthodes de travail, nous pouvons les associer à une couche particulière du modèle OSI **[10]** :

- VLAN de niveau 1 associé à la couche physique,
- VLAN de niveau 2 associé à la couche liaison,
- VLAN de niveau 3 associé à la couche réseau.

I.10.5.1.VLAN par port

Un VLAN par port, aussi appelé VLAN de niveau 1, est obtenu en associant chaque port du commutateur à un VLAN particulier. Les VLANs par port manquent de souplesse. Tout déplacement d'une station nécessite une reconfiguration des ports. De plus, toutes les stations reliées sur un port par l'intermédiaire d'un concentrateur, appartiennent au même VLAN.

I.10.5.2.VLAN par adresse IEEE

Un VLAN par adresse IEEE, ou VLAN de niveau 2 est constitué en associant les adresses MAC des stations à chaque VLAN.L'intérêt de ce type de VLAN est surtout l'indépendance vis à vis de la localisation. La station peut être déplacée sur le réseau physique, son adresse physique ne changeant pas, il est inutile de reconfigurer le VLAN. Les VLANs par adresse MAC sont très adaptés à l'utilisation de stations portables. La configuration peut s'avérer rapidement fastidieuse puisqu'elle nécessite de renseigner une table de correspondance avec toutes les adresses du réseau. Cette table doit aussi être partagée par tous les commutateurs, ce qui peut engendrer un trafic supplémentaire sur le réseau.

I.10.5.3.VLAN par sous-réseaux

Egalement appelé VLAN de niveau 3, un VLAN par sous-réseau utilise les adresses IP sources des datagrammes émis. Un réseau virtuel est associé à chaque sous-réseau IP. Dans ce cas, les commutateurs apprennent automatiquement la configuration des VLANs et il est possible de changer une station sans reconfiguration des VLANs.

Conclusion

Ce chapitre a été axé sur les généralités des réseaux, où nous avons commencé par introduire les concepts des réseaux, leurs objectifs et leurs applications. Ensuite, nous avons défini les déférentes composantes matérielles qui entre dans la composition d'un réseau informatique et les protocoles pour le traitement des données, aussi on a parlé des différentes architectures physiques d'un réseau et leurs topologies logiques, avec l'adressage. Enfin, nous avons pu avoir une notion de base sur les VLANs à savoir ce qui est un VLAN et ses différents types. Dans le chapitre suivant nous allons présenter l'organisme d'accueil de SONATRACH et sa structure.

chapitre II
Organisme d'accueil

Introduction

Dans ce chapitre on s'intéresse à la présentation dans le détail de l'infrastructure réseau, sécurité informatiques et système de la Région Transport Centre de Béjaïa, ainsi nous étudions l'organisation de ces services, c'est-à-dire, de découvrir les différents équipements informatiques que ça soit matériels, logiciels, ou système qui gèrent le bon fonctionnement de cette entreprise.

II.1. Présentation de l'organisme d'accueil

II.1.1. Présentation de SONATRACH

SONATRACH (**SO**ciété **Na**tionale pour le **TRA**nsport par **C**analisation des **H**ydrocarbures): est une entreprise publique algérienne et un acteur majeur de l'industrie pétrolière. C'est une compagnie nationale d'envergure internationale, c'est la clé de voûte de l'économie algérienne.

Le groupe pétrolier et gazier SONATRACH intervient dans l'exploration, la production, le transport par canalisation, la transformation et la commercialisation des hydrocarbures et de leurs dérivés.

II.1.1.1. Historique et mission de SONATRACH

Afin d'assurer le contrôle et la gestion du secteur naissant dans les années 1950 des hydrocarbures, une Direction de l'Energie et des Carburants a été mise en place en Algérie. Des indicateurs significatifs d'une évolution peu probable du secteur des hydrocarbures ont été constatés.

Après l'indépendance, l'Etat algérien se dota d'un instrument permettant la mise en œuvre d'une politique énergétique en créant le 31-12-1963 par décret n° 63 / 491 la société nationale pour le transport et la canalisation d'hydrocarbures. Cette société a changé de statuts le 22-07-1966 décrets n° 66/292, pour devenir « SONATRACH ».

La volonté de l'Algérie de récupérer ses richesses naturelles et d'assurer pleinement le contrôle de leur exploitation, amena à nationaliser la production des hydrocarbures le 24/02/1971 par la signature d'une ordonnance, définissant le cadre d'activité des sociétés étrangères en Algérie. Grâce à cette nationalisation, l'entreprise SONATRACH est passée d'une petite entreprise de 33 agents en 1963 à un effectif de 103000 employés la fin des années 1980, et qui compte aujourd'hui 120 000 employés.

II.1.1.2. Activités de base de SONATRACH

Les activités de base de SONATRACH ont été fixé en 1992 afin d'atteindre ses objectifs en :

- L'exploitation et la recherche ;
- L'exploitation des gisements d'hydrocarbures ;
- La liquéfaction et la transformation du gaz ;
- Le transport par canalisation ;
- La commercialisation.

Pour la réalisation de ces objectifs, SONATRACH est divisé en cinq branches différentes représentées par la figure II.1 :

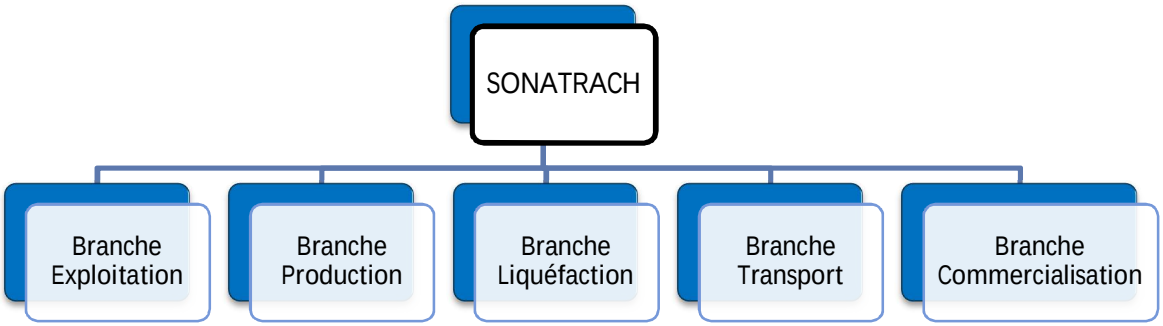


Figure II.1 : Branches de SONATRACH

II.1.2. Activité de la branche transport par canalisation (TRC)

L'activité de transport par canalisation (TRC) est en charge de l'acheminement des hydrocarbures pétroles brut, gaz et condensat vers les ports pétroliers, les zones de stockages et les pays d'exploitation.

Les missions affectées à la branche transport par canalisation sont :

- La gestion et l'exploitation des ouvrages et canalisations de transport d'hydrocarbures ;
- La coordination et le contrôle de l'exécution des programmes de transport arrêtés en fonction des impératifs de production et de commercialisation ;
- La maintenance, l'entretien et la protection des ouvrages et canalisation ;
- L'exécution des révisions générales, des machines tournantes et équipements ;
- Les installations de pompage et de stockage pour répondre aux besoins de SONATRACH dans les meilleures conditions d'économie, de qualité, de sécurité et de respect de l'environnement ;
- Gère l'interface transport des projets internationaux du groupe ou en partenariat.

La SONATRACH possède cinq directions régionales de transport des hydrocarbures :

1. La direction régionale Est (Skikda)
2. La direction régionale Centre (Béjaïa),
3. La direction régionale Ouest (Arzew),
4. La direction régionale de Haoud-EL-Hamra,
5. La direction régionale d'Ain Amenas.

II.1.3. Présentation de la RTC (Région Transport Centre)

La direction régionale de transport de Béjaïa, est l'une des cinq directions régionales de transport des hydrocarbures de la SONATRACH (TRC). Elle a pour mission de transporter, stocker et livrer les hydrocarbures liquides et gazeux. Elle est chargée de l'exploitation de deux oléoducs, d'un gazoduc et d'un port pétrolier.

II.1.4. Structure de la DRGB

Figure II.2 : Organisation de la direction régionale de Béjaïa

Comme on peut le voir dans la figure II.2, la direction régionale de transport suit l'organisation suivante :

a) **Direction régionale :** Est dirigée par un directeur régional aidé par des assistants et un secrétariat.

b) **Secrétariat**

c) **Assistant de sûreté interne :** Sa mission est de protéger et de sauvegarder le patrimoine humain et matériel de la DRGB.

d) **Centre informatique :** Il regroupe les moyens d'exploitation et de développement des applications informatiques pour l'ensemble des structures de la DRGB, ainsi que la gestion du réseau informatique interne.

e) **Sous direction Technique :** Elle a pour mission d'assurer la maintenance et la protection des ouvrages. Elle est organisée en quatre départements: département maintenance, département protection des ouvrages, département approvisionnement et transport et département des travaux neufs.

f) **Sous direction Exploitation :** Elle est chargée de l'exploitation des installations de la région, et de maintenir le fonctionnement des trois ouvrages en effectuant des réparations en cas de fuite, de Sabotage ou de panne pour les stations de pompage. Elle est composée de deux départements : le département exploitation liquide et le département exploitation gaz.

g) **Sous direction Finances et juridique :** Elle a pour missions d'effectuer la gestion financière, le budget et le contrôle de gestion et de prendre en charge les affaires juridiques de la DRGB. Elle est organisée en trois départements : département finances, département juridique, département budget et contrôle de gestion.

h) **Sous direction Administration :** Elle a pour mission la gestion des ressources humaines et les moyens généraux. Elle est organisée en trois départements : département administration et social, département ressources humaines et communication, département moyens généraux.

II.2. Présentation du centre informatique

Le centre informatique est chargé du développement et de l'exploitation des applications informatiques de gestion pour le compte de la direction régionale de Béjaïa (DRGB) et des autres régions.

II.2.1. Organisation structurelle

L'organisation du centre ne cesse de subir des changements et l'évolution rapide de l'informatique pousse le centre à adopter des actions nouvelles à chaque fois afin de subvenir aux nouveaux besoins de l'entreprise.

Pour mener à bien sa mission, le centre informatique s'organise en trois services tels qu'ils sont schématisés dans la figure II.3 :

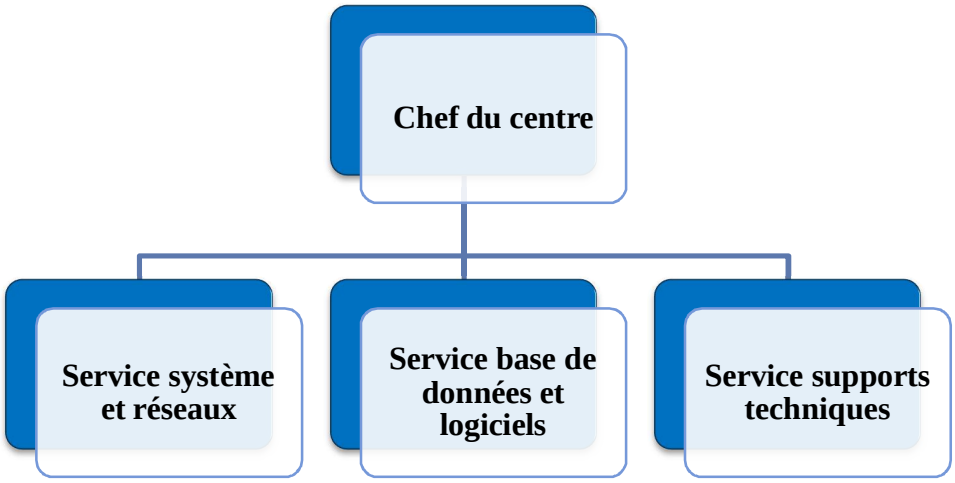


Figure II.3 : Organigramme du centre Informatique

II.2.1.1. Organisation fonctionnelle

Chaque service a sa propre fonction, on va définir et citer les différentes taches de chacun ci-dessous :

a) Service système et réseaux

- **Système**
  - choix des équipements informatique et logiciel de base.
  - Mettre en œuvre les solutions matériels et logiciels retenues.
  - Installation et configuration des systèmes.
  - Orienter les travaux de l'équipe de développement par une bonne utilisation des ressources de l'ordinateur.
  - Mise en œuvre des nouvelles versions de logiciels.
- **Réseau**
  - Assure le bon fonctionnement, la fiabilité des communications, l'administration du réseau et organise l'évolution de sa structure.
  - Conduite de l'étude pour le choix de l'architecture du réseau à installer.

- Participer à la mise en place des réseaux.
- Définir les droits d'accès à l'utilisation du réseau.
- Assure la surveillance permanente pour détecter et prévenir les pannes
- Traitement des dysfonctionnements et incidents survenant sur le réseau

b) Service base de données et logiciels

- **Base de données**
  - Conçoit les bases de données et assure l'optimisation et le suivi de la gestion des données informatiques.
  - Installer, configurer et exploiter le SGBD et ses bases.
  - Mise en œuvre et gestion des procédures de sécurité (accès, intégrité).
  - Gérer la sauvegarde, la restauration et la migration des données.
  - Assure la cohérence et la qualité des données introduites par les utilisateurs.

- **Logiciels**
  - Etude et conception des systèmes d'information.
  - Développement et maintenance des applications informatiques pour TRC.
  - Déploiement des applications et formations des utilisateurs.

c) Service supports techniques

Assistance aux utilisateurs en cas de problèmes software et hardware. Installation des logiciels de gestion, technique et bureautique. Formation aux nouveaux produits installés.

II.3. Data center

Data center d'une entreprise est un centre de traitement des données se présentant comme un lieu où se trouvent différents équipements.

II.3.1. La définition des équipements utilisés dans le réseau de la DRGB

II.3.1.1. Les serveurs

- **Serveur de fichier :** Un serveur de fichiers permet de partager des données à travers un réseau. Le terme désigne souvent l'ordinateur (serveur) hébergeant le service applicatif. Il possède généralement une grande quantité d'espace disque où sont déposés des fichiers. Les

utilisateurs peuvent ensuite les récupérer au moyen d'un protocole de partage de fichiers. On utilise généralement l'un des quatre protocoles suivant **[11]**:

- **FTP** (File Transfer Protocol)
- **CIFS** (Common Internet File System) anciennement nommé SMB (Server Message Block)
- **NFS** (Network File System)
- **NCP** (Netware Core Protocol).

- **Serveur de bases de données :** Un serveur de base de données répond à des demandes de manipulation de données stockées dans une ou plusieurs bases de données. Il s'agit typiquement de demandes de recherche, de tri, d'ajout, de modification ou de suppression de données. Le serveur de base de données fait partie d'un système de gestion de base de données - logiciel qui manipule une base de données - qui comporte un logiciel client et un logiciel serveur. Les demandes de manipulation de données sont souvent créées par un logiciel de gestion sous forme de requêtes en langage SQL, puis le client les transmet au serveur en utilisant un protocole propre au SGBD **[12]**.
- **Serveur LMS :** Serveur LAN Management Solution (LMS) offre un ensemble robuste d'applications dédiées à l'administration, la surveillance et le dépannage des environnements LAN commutés Cisco. Complément majeur des architectures matérielles de réseau Cisco AVVID (Architecture for Voice, Video and Integrated Data) ce produit a été conçu dans l'objectif de maximiser la disponibilité de service du réseau en fournissant aux équipes techniques un puissant outil d'administration de bout en bout, capable de démultiplier l'efficacité de chaque action d'administration **[13]**.

II.3.1.2. Les Commutateurs (Switch)

Le réseau de la DRGB contient deux types de commutateurs :

- **Des commutateurs intelligents :** en plus de leur fonction ils peuvent faire le routage.

  Dans le réseau de la DRGB, on trouve quatres exemples de ce type qui sont :

  - **Définition de la gamme Catalyst Cisco 6509 :** La gamme Catalyst 6509 représenté sur la figure II.4 offre des moyens pour soutenir la capacité de la bande passante du système et des capacités améliorées de gestion des câbles. Elle fournit également des flux d'air d'avant en arrière qui est optimisé pour les conceptions allée chaude et froide dans le centre de données co-localisées et les déploiements de services. En outre elle offre une protection exceptionnelle des investissements en soutenant plusieurs générations de produits sur le

même châssis, réduisant ainsi les coûts totaux de propriété. Le cadre Cisco Catalyst 6509 supporte à la fois la gamme Cisco Catalyst 6500 Supervisor Engine 32 et Cisco Catalyst 6500 Series Supervisor Engine 720 familles, avec LAN associés, WAN, et des modules de services **[14]**.

Figure II.4: Gamme Catalyst Cisco 6509

- **Définition de la gamme Catalyst Cisco 3750 :** La gamme Cisco Catalyst 3750 est une ligne de commutateurs innovants qui améliorent l'efficacité de l'exploitation des réseaux locaux grâce à leur simplicité d'utilisation et leur résilience la plus élevée disponibles pour des commutateurs empilables. Cette gamme de produits dispose de la technologie Cisco StackWise^{TM}, interconnectant les commutateurs au sein d'une même pile à 32 Gbps qui permet de construire un système unique de commutation à haute disponibilité. En outre, elle est optimisée pour les déploiements Gigabit Ethernet haute densité et comprend un large éventail de commutateurs qui répondent aux exigences en matière d'accès, d'agrégation ou de connectivité dorsale pour de petits réseaux **[15]**.

La figure II.5 montre la gamme Cisco 3750 à configuration empilable.

Figure II.5: Gamme Catalyst Cisco 3750

- **Définition de la gamme Catalyst Cisco 3550 :** Le Cisco Catalyst 3550 Séries Switch est un empilable, commutateur multicouche qui offre une haute disponibilité, la qualité de service (QoS) et de la sécurité afin d'améliorer l'exploitation du réseau **[15]**.

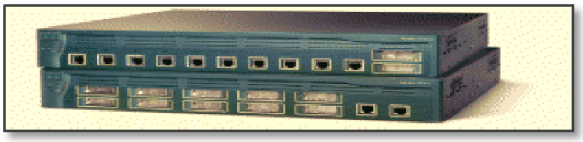


Figure II.6: Gamme Catalyst Cisco 3550

- **Des commutateurs non intelligents :** ce type de commutateurs ne permet pas de faire le routage.

Le réseau de la DRGB contient le type suivant :

- **Définition de la gamme Catalyst 2950 :** Le Cisco Catalyst 2950 Séries Switch est une configuration fixe, empilable commutateur autonome qui fournit un accès rapide à vitesse filaire Ethernet et Gigabit Ethernet. Le Catalyst 2950 représenté sur la figure II.7 dispose de deux ensembles distincts de fonctionnalités du logiciel et une gamme de configurations pour permettre aux petits environnements, de taille moyenne et les succursales d'entreprise et industriels à choisir la bonne combinaison pour la périphérie du réseau. Standard Image Software offre Cisco IOS fonctions du logiciel pour les données de base, la voix et des services vidéo. Pour les réseaux aux exigences de sécurité supplémentaires, qualité de service (QoS), et la haute disponibilité **[16]**.

Figure II.7: Gamme Catalyst Cisco 2950

II.3.1.3. Les routeurs

Le réseau de la DRGB possède deux types de routeurs suivants :

- **CISCO 1700 :** Le Cisco 1700 Séries routeur d'accès modulaire illustré sur la figure II.8 offre Internet rapide, fiable et sécurisé et d'accès au réseau par le biais de diverses technologies à haute vitesse d'accès WAN **[17]**.

Figure II.8 : Routeur Cisco 1700

- **Routeur Wimax :** Le Wimax représenté dans la figure II.9 est un standard de transmission sans fil qui permet de rendre, de façon rapide et économique, l'Internet haut débit accessible pour les abonnés, qu'ils soient professionnels ou particuliers. Fonctionnant à 70 Mbit/s, il est prévu pour connecter les points d'accès Wifi à un réseau de fibres optiques **[18]**.

Figure II.9: Routeur Wimax

Et ci dessus la figure II.10 montre le matérielles utilisés à SONATRACH.

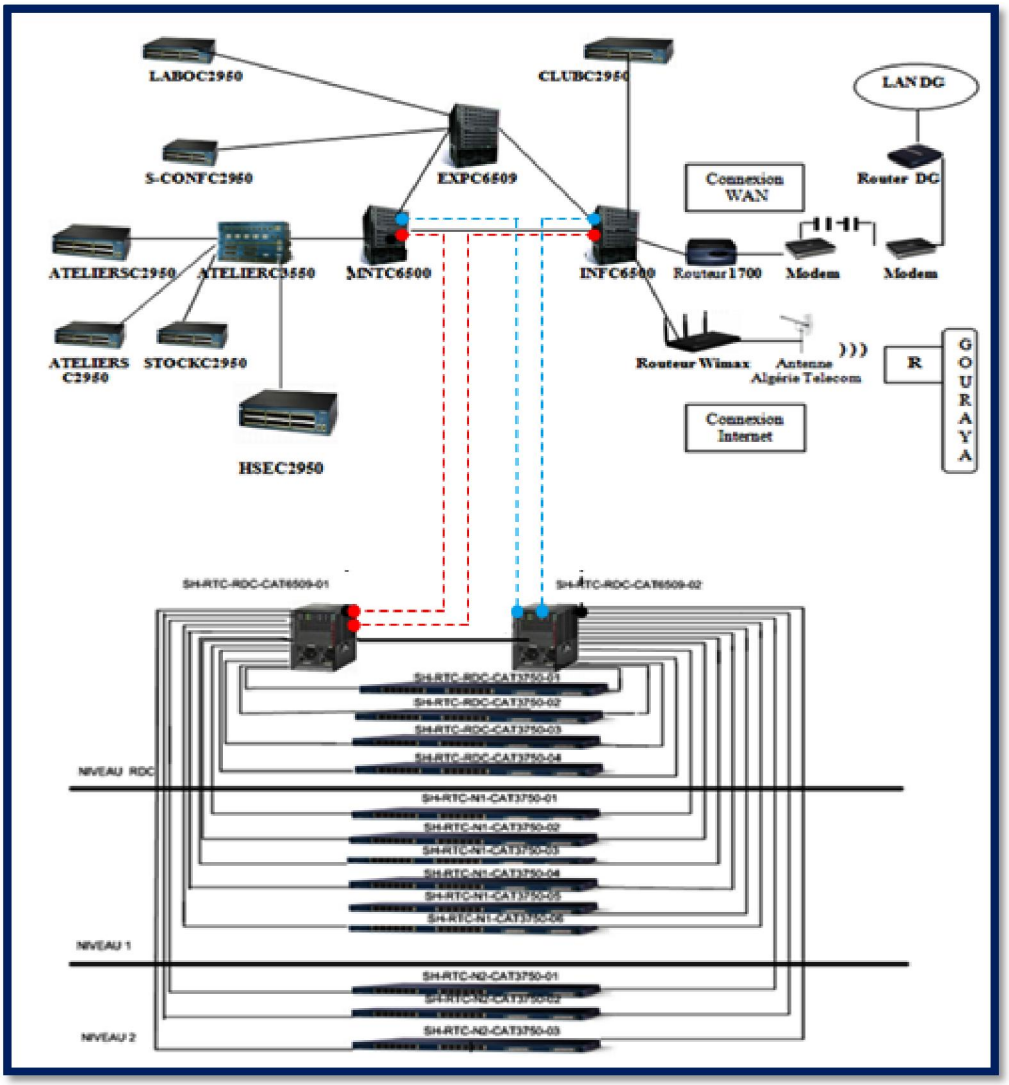


Figure II.10: Architecture de liaison entre l'ancien et le nouveau bâtiment

II.3.2. La définition des équipements de sécurité

- **Serveur Antivirus « F-Secure »:** Il peut être difficile et coûteux de combattre des virus une fois qu'ils sont entrés sur le réseau. Les solutions de sécurité **F-Secure** pour serveurs protègent contre les virus et autres menaces, empêchent les machines infectées de propager leurs virus sur le réseau. Elles sont conçues pour fonctionner de manière transparente en tâche de fond pour empêcher les perturbations du réseau, la baisse de productivité et les menaces sur les données confidentielles. Le serveur F-Secure offre la possibilité de gestion à distance à partir d'un emplacement central unique. C'est cette gestion que utilise la RTC pour effectuer des mises à jours à partir d'un seul poste centralisé et de les transmettre à tous les autres postes via ce serveur **[19]**.

- **Websense Filtrage :** Le filtrage web peut aider les entreprises à équilibrer les besoins personnels des employés relativement à Internet tout en réduisant les risques de responsabilité légale, en maintenant les niveaux adéquats de bande passante réseau et en améliorant la productivité **[20]**.

- **Serveur Reporting :** Est un outil complet qui permet d'identifier tous les problèmes possibles avec accès à Internet ou à la consommation de la bande passante réseau en générant des rapports détaillés, des résumés ou des graphiques. Il est utilisé pour montrer comment la connexion Internet est utilisée et pour affiner vos stratégies de filtrage afin de maximiser les ressources du réseau **[20]**.

- **Proxy Bluecoat SG510 :** Le Proxy Bluecoat SG 510 montré dans la figure II.11 offre un appareil abordable montage en rack pour les petites entreprises et les succursales qui nécessitent un accès direct à Internet. Proxy SG 510 accélère les applications d'affaires à travers l'entreprise distribuée. Le Proxy SG 510 plate-forme permet également le trafic Internet de contrôle pour empêcher les logiciels malveillants et les applications non autorisées de compromettre la sécurité du réseau ou la performance **[21]**.

Figure II.11: Proxy bluecoat SG 510

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

Figure II.12: Firewall Juniper SSG 550

Firewall Juniper SSG 550 représenté dans la figure II.12 contient un ensemble de règles structuré en trois zones qui se présentent comme suite :

- **La zone trust :** C'est la zone la plus confiante, car elle autorise le trafic sortant et interdit le trafic entrant et c'est pour cela que la RTC lui a confiée son réseau LAN.
- **La zone untrust :** C'est une zone qui autorise le trafic entrant et interdit le trafic sortant.
- **La DMZ** (**DEM**ILITARIZED **Z**ONE) **:** Est une zone tampon d'un réseau d'entreprise, située entre le réseau local et Internet, derrière le pare-feu. Il s'agit d'un réseau intermédiaire regroupant des serveurs publics (HTTP, DHCP, mails, DNS, etc.). Ces serveurs devront être accessibles depuis le réseau interne de l'entreprise et, pour certains, depuis les réseaux externes. Le but est ainsi d'éviter toute connexion directe au réseau interne.

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

- **La DMZ ADMIN (Administrateur):** Contient Site protector, Internet Scanner, Station admin, Websense Reporting et ISS GX4002.
- **La DMZ Filtrage WEB:** Contient Proxy Bluecoat, Websense filtrage.
- **La DMZ Reverse :** Est un type de serveur proxy, habituellement placé en frontal de serveurs web. Il est à différencier dans son utilisation des serveurs mandataires traditionnels. Le proxy inverse est implémenté du côté des serveurs Internet. L'utilisateur du web passe par son intermédiaire pour accéder aux applications de serveurs internes.

Cette technique permet entre autres de protéger un serveur web des attaques provenant de l'extérieur. Cette technologie est employée dans les solutions de sécurité applicative **[22]**.

- **ISS Proventia GX 4002 :** ISS Prevention GX4002 représenté dans la figure II.13 étend la protection de l'industrie de la technologie Proventia aux segments distants de votre réseau, en aidant à prévenir les attaques avant qu'elles n'affectent votre entreprise. Proventia GX4002 peut assurer la sécurité globale, la performance et la fiabilité dans une solution qui est simple à déployer et à gérer **[23]**.

Figure II.13: ISS Proventia GX 4002

- **ISS Proventia GX 5108 :** ISS Proventia GX 5108 illustré dans la figure II.14 offre une protection sans compromis pour votre réseau avec 1,2 Gbps de débit dans quatre segments de réseau configurés de manière flexible et protégées, Proventia GX5108 peut apporter des solutions globales de sécurité, de performance et de fiabilité dans une solution qui est simple à déployer et à gérer, il offre egalement une protection préventive de votre réseau **[23]**.

Figure II.14: ISS Proventia GX 5108

- **ISS Proventia GX 5008 :** ISS Proventia GX 5008 montré dans la figure II.15 s'étend de l'industrie de la protection de la technologie Proventia à la périphérie du réseau, où il peut contribuer à bloquer les menaces extérieures avant qu'ils n'affectent votre entreprise. Avec 400 Mbps de débit à travers quatre segments de réseau flexible configurés, Proventia Network IPS GX5008 peut assurer la sécurité globale, la performance et la fiabilité dans une solution qui est simple à déployer et à gérer **[23]**.

Figure II.15: ISS Proventia GX 5008

La figure II.16 montre le schéma de sécurité de la RTC.

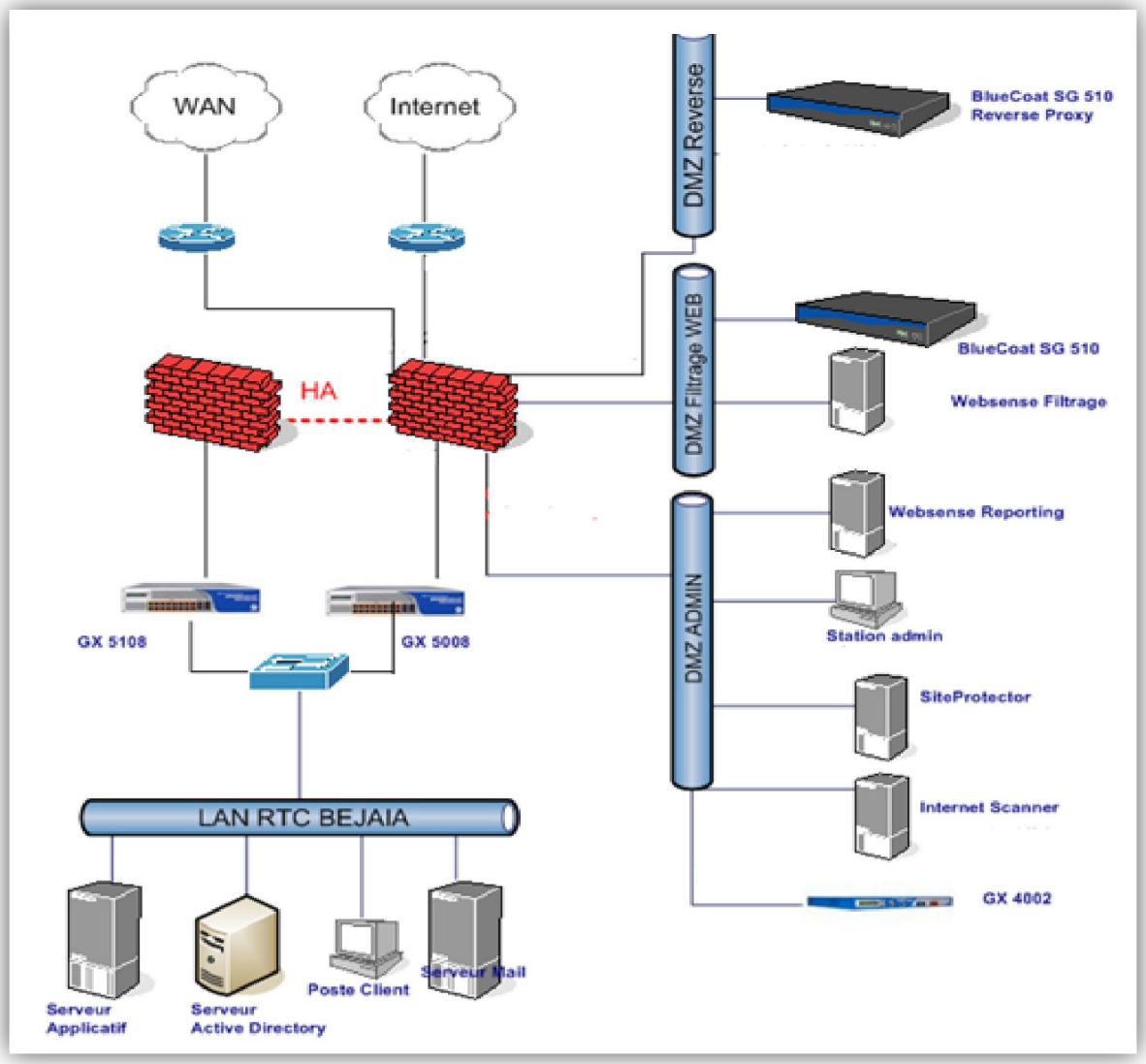


Figure II.16: Architecture des équipements de sécurité de la RTC

II.3.3. La définition des équipements système

Dans cette partie on va définir le contrôleur de domaine, l'annuaire Active Directory et d'autres serveurs comme celui de la messagerie électronique et le serveur applicatif.

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

Protocol) central. En raison de leur importance, les contrôleurs de domaine doivent toujours être stockés dans des emplacements physiques sécurisés et accessibles uniquement au personnel administratif qualifié. Lorsque les contrôleurs de domaine doivent être stockés dans des emplacements moins sûrs, dans une filiale par exemple, plusieurs paramètres de sécurité peuvent être réglés pour limiter les dommages éventuels résultant de menaces physiques **[24]**. La RTC dispose d'un contrôleur de domaine principale et d'un autre secondaire installés sur des serveurs de type Dell Power Edge 2800 qui sont complémentaire, si l'un cesse de fonctionner l'autre prend son rôle.

- **Définition du serveur Dell Power Edge 2800 :** Le système PowerEdge 2800 comprend un processeur, de la mémoire et des connecteurs d'E/S locaux intégrant les technologies les plus récentes. Le serveur PowerEdge 2800 montré dans la figure II.17 combine de grandes performances et une importante capacité de stockage, ce qui en fait un produit idéal pour les projets de consolidation du stockage et des serveurs. Le châssis adaptable peut être déployé en tour ou en rack **[25]**.

Figure II.17: Contrôleur de domaine power Edge 2800

- **Annuaire Active Directory :** Active Directory (AD) est la mise en œuvre par Microsoft des services d'annuaire LDAP pour les systèmes d'exploitation Windows. L'objectif principal d'Active Directory est de fournir des services centralisés d'identification et d'authentification à un réseau d'ordinateurs utilisant le système Windows. Il permet également l'attribution et l'application de stratégies, la distribution de logiciels, et l'installation de mises à jour critiques par les administrateurs. Active Directory répertorie les éléments d'un réseau administré tels que les comptes des utilisateurs, les serveurs, les postes de travail, les dossiers partagés, les imprimantes, etc. Un utilisateur peut ainsi facilement trouver des ressources partagées, et les

administrateurs peuvent contrôler leurs utilisations grâce à des fonctionnalités de distribution, de duplication, de partitionnement et de sécurisation des accès aux ressources répertoriées. Si les administrateurs ont renseigné les attributs convenables, il sera possible d'interroger l'annuaire pour obtenir par exemple : « Toutes les imprimantes couleurs à un étage d'un bâtiment » **[24]**. Et la RTC dispose d'un Annuaire Active Directory qui est installé au niveau du serveur contrôleur de domaine qui contrôle l'accès de ses différents utilisateurs en offrant à chacun d'eux une session accessible par un mot de passe et un login gérer par une stratégie de groupe.

- **Présentation des stratégies de groupe :** La stratégie de groupe du rôle de serveur Contrôleurs de domaine est une stratégie de base. Le terme Stratégie désigne la configuration logicielle du système par rapport aux utilisateurs. A la suite d'une installation de Windows, aucune stratégie n'est configurée, et tout est permis (en fonction des droits des groupes d'utilisateurs prédéfinis: Administrateurs, Utilisateurs, Utilisateurs avec pouvoir...). Les stratégies de groupe ou GPO (Group Policiers Object) permettent de configurer des restrictions d'utilisation de Windows où des paramètres à appliquer soit sur un ordinateur donné soit sur un compte utilisateur donné. Il est ainsi possible d'agir sur :
  - La définition d'un environnement adapté : Il est possible par exemple de rediriger certains répertoires leurs contenus.
  - Le déploiement de logiciels: Une automatisation complète de l'installation des programmes sur les postes clients est possible en fonction du profil de l'utilisateur.
  - L'application des paramètres de sécurité : Le contexte de sécurité de l'environnement utilisateur peut être modifié **[24]**.Voici un exemple de stratégie de groupe qu' utilise la RTC pour mieux gérer les fonctionnalités de tous ses employés ainsi que leurs droits d'accès et les limites de chacun d'eux en créant des groupes d'utilisateurs qui ont accès à Internet(centre informatique, et les cadres des autres département) et des groupes qui n'en ont pas à cause des contraintes du débit. Création aussi d'une GPO offrant le montage des lecteurs sous différents noms selon les droits d'accès tel que : Le lecteur **S :** partagé par tous les employeurs de la direction. Le lecteur **Y :** partagé par tous les employeurs de la même structure. Le lecteur **T :** c'est un lecteur personnel. Les lecteurs **X** et **W :** Sont réservés aux applications.

- **Serveur d'applications :** Un serveur d'applications est un serveur sur lequel sont installées les applications utilisées par les usagers. Ces applications sont chargées sur le serveur d'applications et accédées à distance, souvent par réseau. Un serveur d'applications peut être un serveur qui centralise toutes les applications utilisées par les postes clients. Pour le cas de la RTC, les serveurs d'applications sont l'ES40 et le DS20 **[26]**.

- **Exchange Server 2004 :** Microsoft Exchange Server est un logiciel collaboratif pour serveur de messagerie électronique créé par Microsoft, très utilisé dans les grandes entreprises, conçu pour la messagerie électronique, mais aussi pour la gestion d'agenda, de contacts et de tâches, qui assure le stockage des informations et permet des accès à partir de clients mobiles et de clients Web (navigateurs tels que IE, Firefox, Safari...). Exchange Server 2004 est installé sous Windows serveur 2003, la RTC a mis au point quelques stratégies de boite aux lettres comme celle de la capacité de stockage qui est limitée à 250 Mo. Si une boite dépasse ce volume de stockage un message d'avertissement sera envoyé au poste correspondant par le serveur afin que l'utilisateur prenne en charge le message signalé pour libérer un espace mémoire précis. Exchange Server Offre aussi la possibilité de créer des dossiers publics pour le partage des fichiers et des dossiers volumineux, parmi ces dossiers on trouve : Dossier informatique: appartenant aux informaticiens. Dossier cellule communication : destinée pour la cellule communication pour la diffusion de revues. Dossier syndicat : Pour diffusion de rapports liés au syndicat **[27]**.

II.4. Structure hiérarchique du réseau

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

- **La couche accès :** La couche accès sert d'interface avec les périphériques finaux, tels que les ordinateurs, les imprimantes et les téléphones sur IP, afin de fournir un accès au reste du réseau. La couche accès peut inclure des routeurs, des commutateurs, des ponts, des concentrateurs et des points d'accès sans fil. Le rôle principal de la couche accès est de fournir

un moyen de connecter des périphériques au réseau, ainsi que de contrôler les périphériques qui sont autorisés à communiquer sur le réseau.

- **La couche distribution :** La couche distribution regroupe les données reçues à partir des commutateurs de la couche accès, avant qu'elles ne soient transmises vers la couche cœur de réseau, en vue de leur routage vers la destination finale. La couche de distribution gère le flux du trafic réseau à l'aide de stratégies. Elle délimite les domaines de diffusion via des fonctions de routage entre des réseaux locaux virtuels (VLAN) définis au niveau de la couche accès. Les commutateurs de la couche de distribution sont généralement des périphériques très performants qui offrent une disponibilité et une redondance élevées afin de garantir la fiabilité.
- **La couche cœur :** Cette couche va s'occuper de switcher le trafic vers le bon service, de la manière la meilleure et la plus rapide qui soit. La couche cœur de réseau est essentielle à l'inter connectivité entre les périphériques de la couche de distribution. Par conséquent, il est important qu'elle bénéficie d'une disponibilité et d'une redondance élevée. La zone principale peut également se connecter à des ressources Internet **[28]**.

Conclusion

Dans ce chapitre on a commencé par présenter l'organisme d'accueil « SONATRACH » et sa structure, puis nous avons étudié les équipements utilisés dans les parties réseau, sécurité et système. Dans le chapitre suivant on va voire les étapes à suivre pour implémenter les différents VLANs et la présentation des critiques avec une étude descriptible et la mise en œuvre des solutions proposées.

chapitre III
Planification & Réalisation

Introduction

Dans le chapitre précédant nous avons étudié le coté théorique du réseau de la RTC de Béjaïa et dans ce dernier chapitre on s'intéresse à la simulation en utilisant le logiciel Cisco Packet Tracer pour implémenter les différents $VLAN_{s.}$ Enfin, on présente des critiques avec une étude descriptible et la mise en œuvre des solutions proposées.

III.1. Présentation du simulateur Cisco Packet Tracer

Packet tracer est un simulateur de réseau puissant développé par Cisco Systems pour faire des plans d'infrastructure de réseau en temps réel.il offre la possibilité de créer ,visualiser et de simuler les réseaux informatique. L'objectif principal de simulateur, est de schématiser, configurer et de voir toute les possibilités d'une future mise en œuvre réseau. Cisco Packet Tracer est un moyen d'apprentissage de la réalisation de divers réseaux et découvrir le fonctionnement des différents éléments constituants un réseau informatique **[29]**.

III.2. Les différents VLANs à implémenter et leur plan d'adressage

L'adresse du réseau est 192.168.0.0/24 avec une possibilité de création de 255 sous réseaux, avec un masque 255.255.255.0

L'adressage du réseau local et de toutes les stations, se basera sur une adresse privée. Les machines affiliées à un VLAN, vont prendre toutes les adresses IP d'une même adresse sous-réseau.

Le tableau III.1 montre la liste des VLANs disponibles sur le réseau, ainsi que leur adresse IP.

Vlan-ID	Description	Adresse IP	Passerelle
1	Par défaut	192.168.1.250/24	--
2	Direction	192.168.2.0/24	192.168.2.254
3	Informatique	192.168.3.0/24	192.168.3.254
4	HSE	192.168.4.0/24	192.168.4.254
5	Sûreté interne	192.168.5.0/24	192.168.5.254
6	Sous Direction exploitation	192.168.6.0/24	192.168.6.254
7	Sous Direction technique	192.168.7.0/24	192.168.7.254
8	Sous Direction administrative	192.168.8.0/24	192.168.8.254
9	Sous Direction finance et juridique	192.168.9.0/24	192.168.9.254
10	Les serveurs (DC, EXCH, patte Juniper)	192.168.10.0/24	192.168.10.254
11	Les serveurs base de données	192.168.11.0/24	192.168.11.254
12	Salles (conférence, formation, technique)	192.168.12.0/24	192.168.12.254
13	WAN	192.168.13.0/24	192.168.13.254
14	WIFI	192.168.14.0/24	192.168.14.254
20	Manager	172.17.0.0/24	172.17.0.254

Tableau III.1 : Liste des noms des VLANS de la RTC de Béjaïa et leur plan d'adressage

III.3. Interface commande de Packet Tracer

Toutes les configurations des équipements du réseau est au niveau de CLI (commande langage interface) qu'elles seront réalisées. CLI est une interface de simulateur Packet Tracer qui permet la configuration des équipements du réseau à l'aide d'un langage de commandes, c'est-à-dire qu'à partir des commandes introduites par l'utilisateur du logiciel, que la configuration est faite **[29]**.

III.4. Architecture de mise en œuvre

La figure III.1 illustre la topologie physique du réseau de la RTC de Béjaïa captée sous le simulateur Packet Tracer.

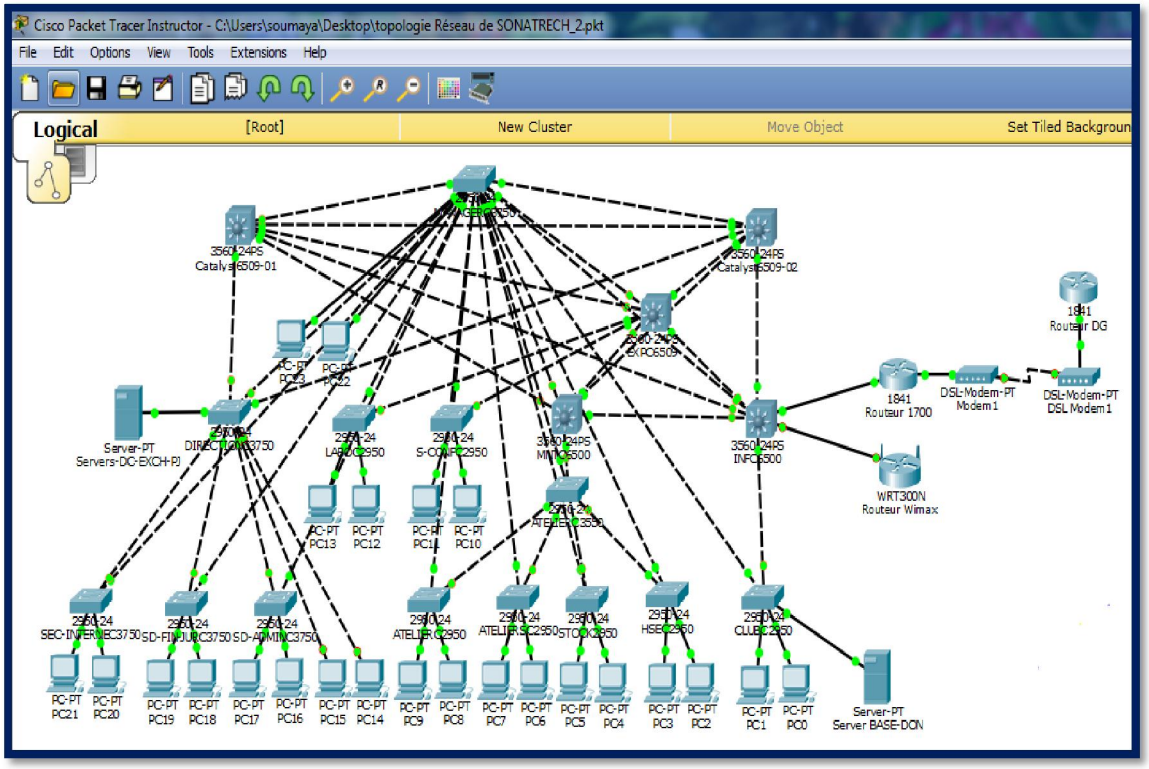


Figure III.1 : Topologie physique du réseau de la RTC

III.5. Configuration des équipements

Une série de configuration sera réalisée à travers les équipements du réseau, en montrant un exemple de chaque configuration.

III.5.1. Configuration des interfaces des stations et des serveurs

Configuration des paramètres réseau (IP Adresses, Subnet Mask, Gateway) des stations et des serveurs (voir figure III.2).

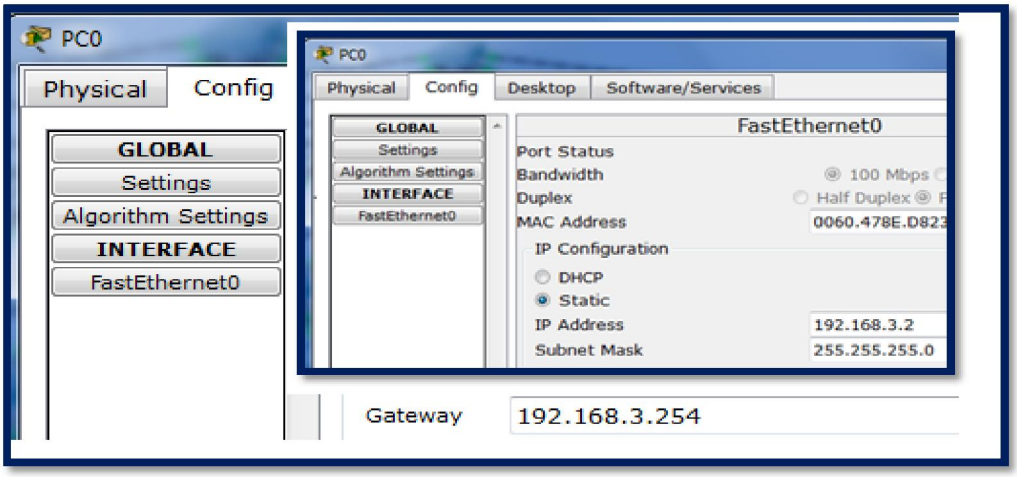


Figure III.2 : Configuration des paramètres réseaux

III.5.2. Configuration des commutateurs (Switchs)

III.5.2.1. Configuration de base des commutateurs

Exemple de configuration du commutateur HSEC2950

```
Passer en mode privilégié puis en mode de configuration :
Switch>enable
Passer en mode configuration globale :
Switch#configure terminal
Attribuer le nom du commutateur
Switch (config)#hostname HSEC2950
Désactiver la recherche DNS
HSEC2950 (config) #no ip domain-lookup
Configurer la passerelle
HSEC2950 (config) #ip default-gateway 192.168.40.4
```

III.5.2.2. Configuration du protocole VTP (Virtual Trunking Protocol)

Le protocole VTP permet à un administrateur réseau de configurer un commutateur pour qu'il propage des configurations VLAN à d'autres commutateurs du réseau. Le commutateur peut être configuré dans le rôle d'un serveur VTP ou d'un client VTP.

- VTP simplifie l'administration de réseaux locaux virtuels sur plusieurs commutateurs en répliquant les configurations VLAN entre les commutateurs.
- Un domaine VTP définit les commutateurs d'un réseau devant être configurés de manière similaire concernant la configuration VLAN.
- Le mode serveur VTP permet la création, la suppression et la modification de réseaux locaux virtuels.
- Le mode client VTP empêche la modification des réseaux locaux virtuels et permet uniquement de recevoir des informations VLAN par l'intermédiaire d'annonces VTP **[30]**.

- **Configuration du protocole VTP sur les Switchs Cœur**

L'ensemble des commutateurs Core de LAN seront configurés comme des server-VTP.Donc, ce sont eux qui gèrent l'administration de l'ensemble des VLANs. Un nom de domaine est attribué.

La figure III.3 représente la configuration du VTP server au niveau de Switch multifonctions.

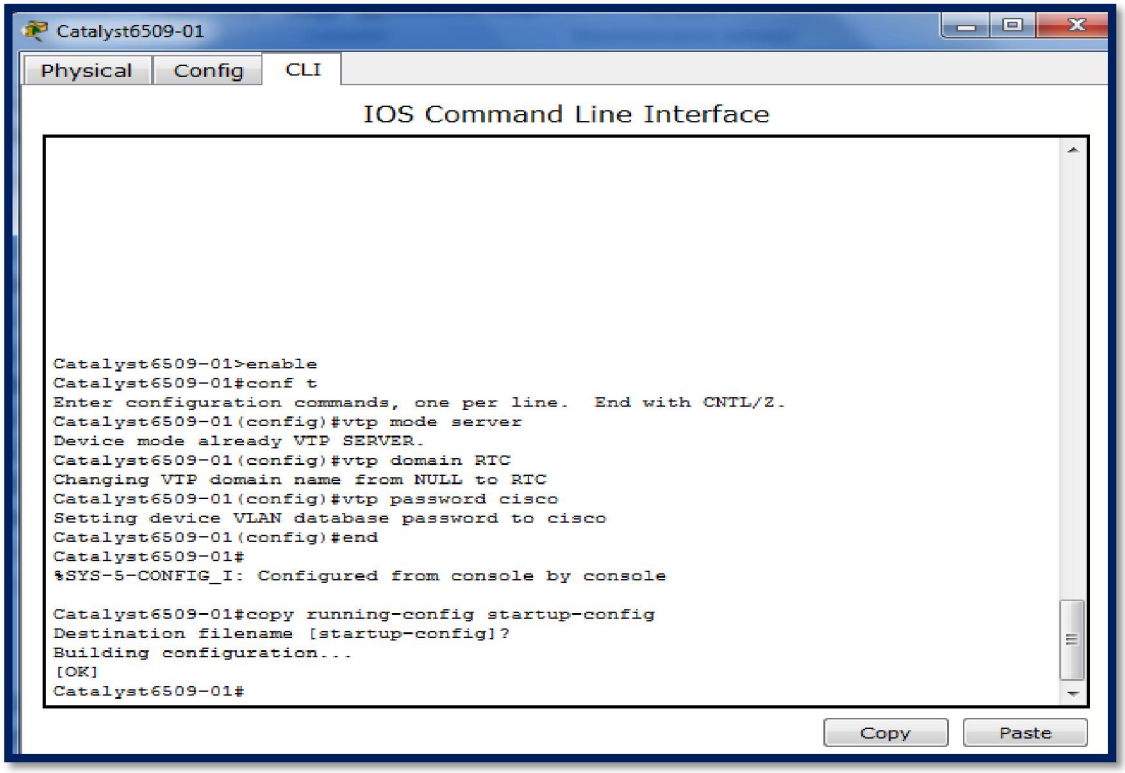


Figure III.3 : Configuration des VTP server

- **Configuration du protocole VTP sur les autres Switchs**

Par ailleurs, la configuration des clients-VTP sera au niveau de tous les commutateurs Accès+Distribution.

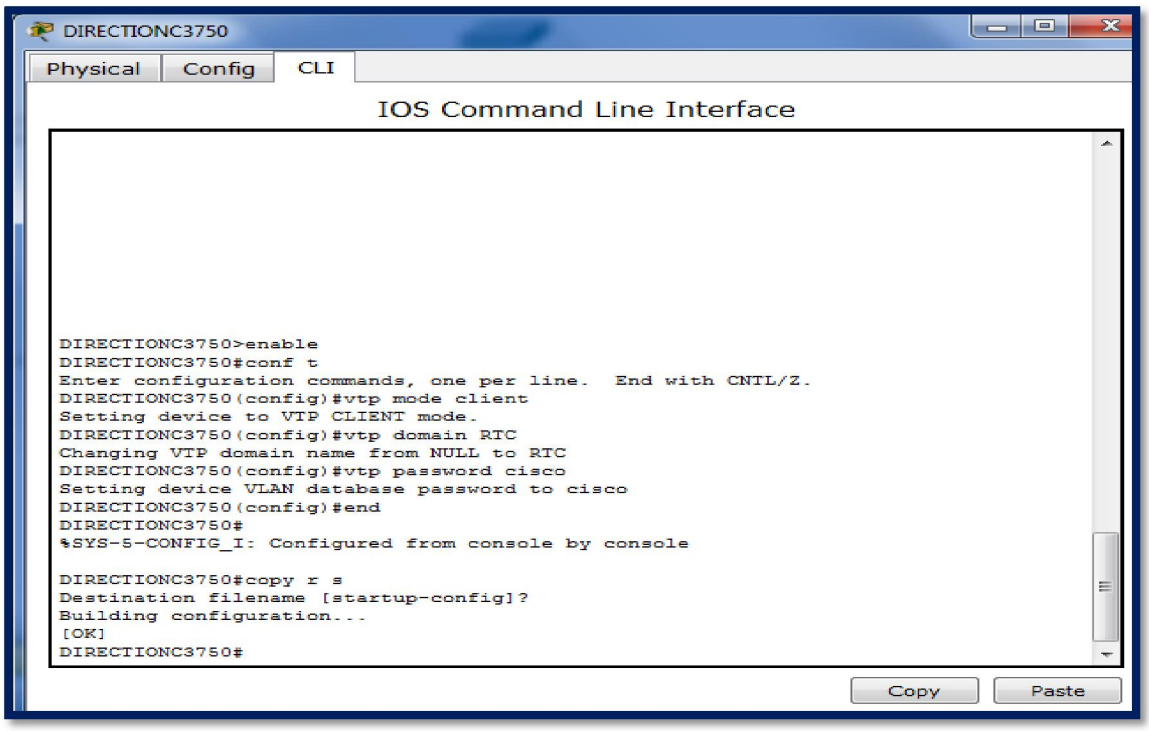


Figure III.4 : Configuration client-VTP

Pour déterminer le mode de fonctionnement du protocole VTP pour tous les Switchs on utilise la commande **« show vtp status »**.

III.5.2.3. Configuration des $VLAN_S$ sur le serveur VTP

La configuration des $VLAN_S$ est faite au niveau des serveurs VTP, comme le montre la figure III.5 ci-dessous :

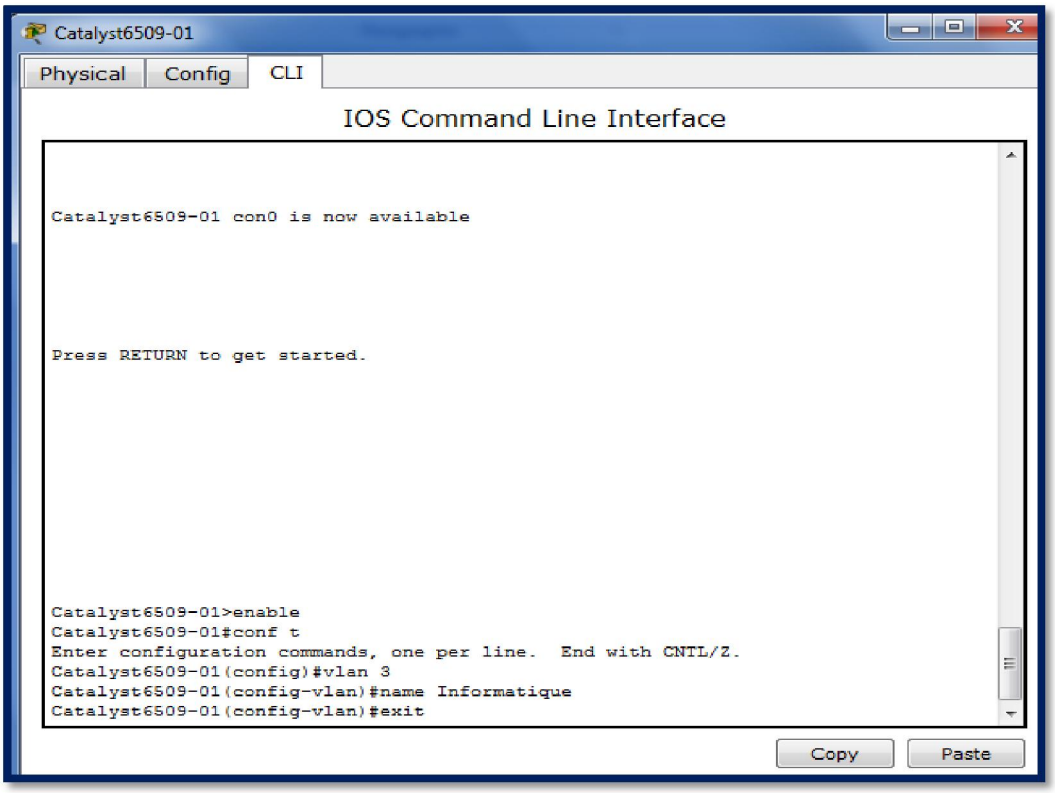


Figure III.5 : Création des $VLAN_S$

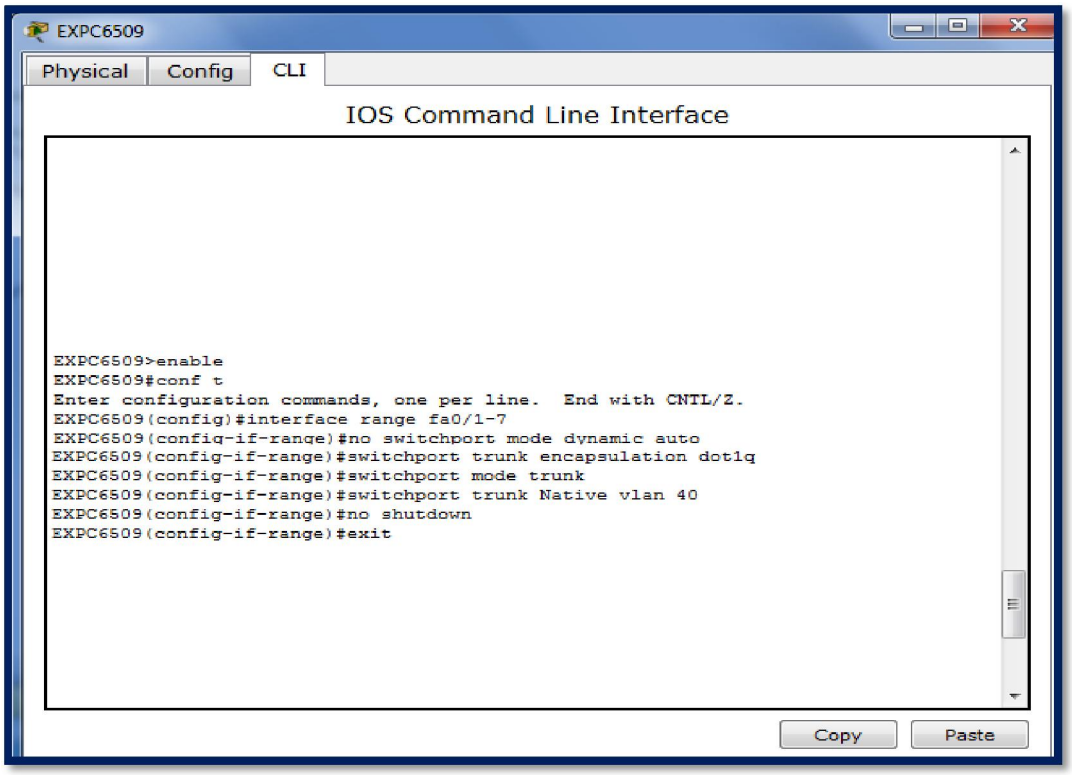
Pour vérifier si les réseaux locaux virtuels ont effectivement été créés on utilise la commande **« show vlan brief »**.

III.5.2.4. Configuration des ports d'agrégation et désignation du VLAN Natif pour les agrégations

Les agrégations sont des connexions entre les commutateurs permettant des échanges d'informations pour tous les réseaux locaux virtuels. Un port d'agrégation fait partie par défaut de tous les VLAN, contrairement à un port d'accès qui lui fait uniquement partie d'un seul VLAN. Dans notre simulation nous avons utilisé un autre réseau local virtuel natif que le VLAN 1.

- **Les ports des Switchs multifonctions**

Les commandes suivantes nous permettent d'associer des ports d'agrégation pour tous les commutateurs en s'aidant de la commande **range** qui pourra réunir toutes les interfaces en une seule fois.



III.6 : Attribution des ports d'agrégation aux commutateurs

- **Les ports des autres Switchs**

Les commandes suivantes nous permettent d'associer un port à un d'agrégation à un commutateur.

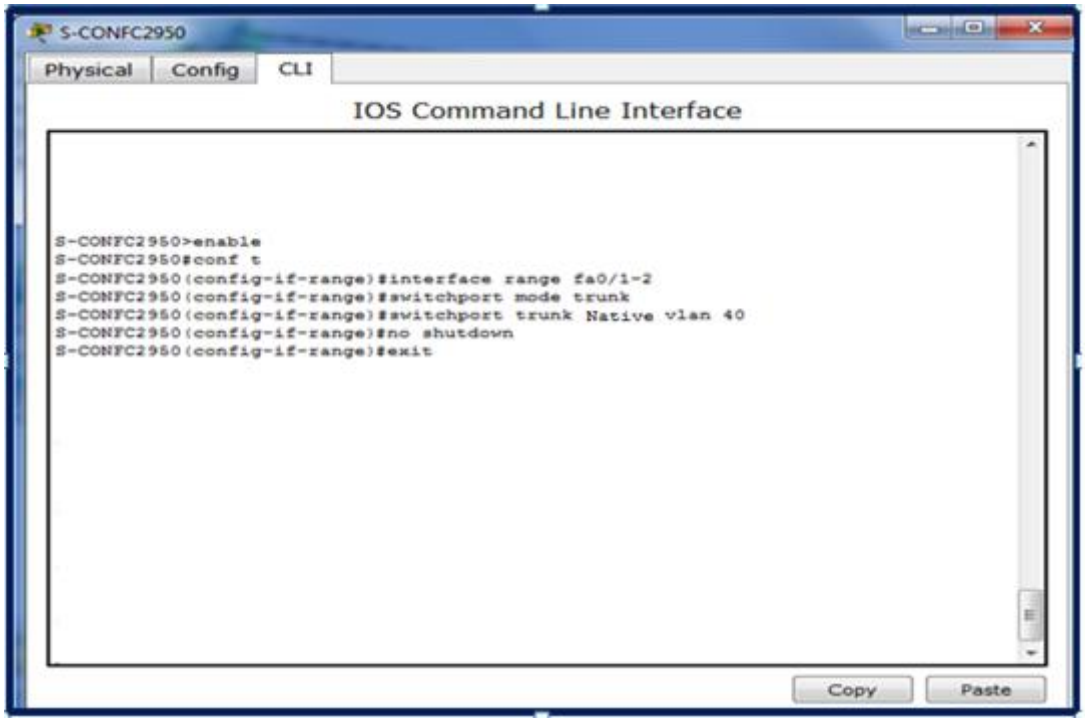


Figure III.7: Configuration des ports d'agrégation aux autres Switchs

Pour assurer que les agrégations ont effectivement été configurées on utilise la commande **« show interface trunk »**.

Pour la vérification de la distribution sur tous les commutateurs clients des réseaux locaux virtuels créés sur le serveur-VTP, on exécute la commande **show vlan brief**

III.5.2.5. Configuration de l'adresse de l'interface de gestion sur tous les commutateurs

La figure III.8 illustre un exemple de configuration de l'interface de gestion.

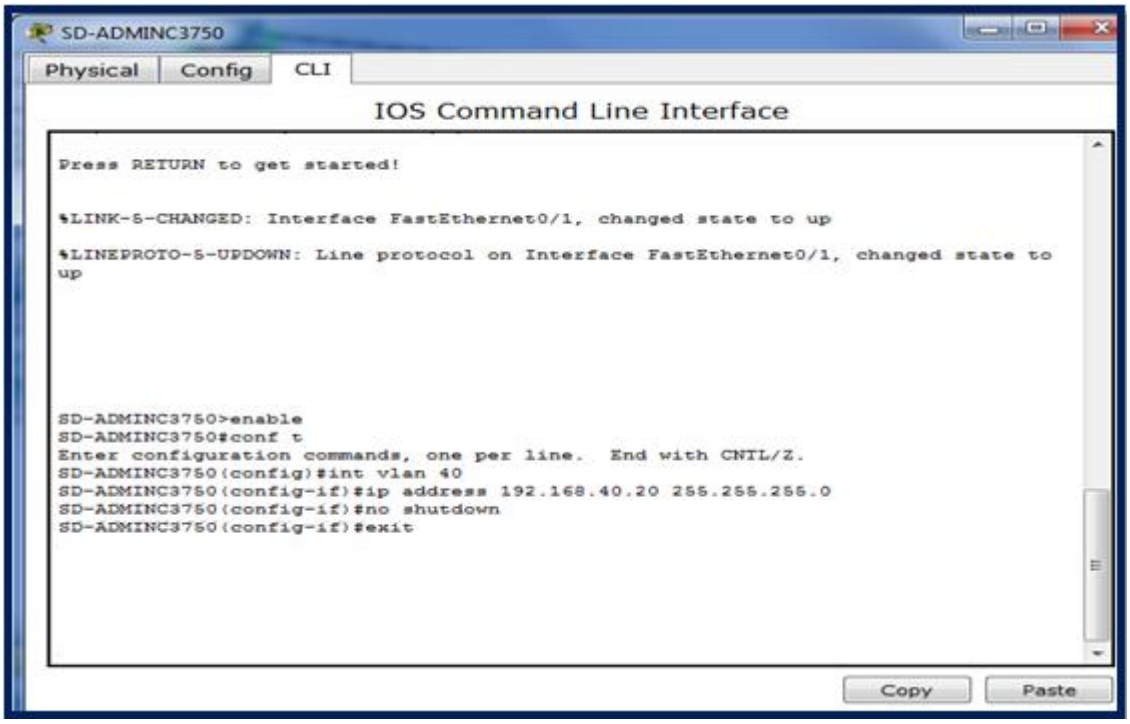


Figure III.8 : Configuration de l'interface de gestion

III.5.2.6. Activation des ports du commutateur au VLAN

- **Le mode Access :** est utilisé pour la connexion des périphériques (PC, imprimante…) appartenant à un seul VLAN. Les commandes de la figure III.9 nous permettent d'associer un port à un VLAN en mode Access :

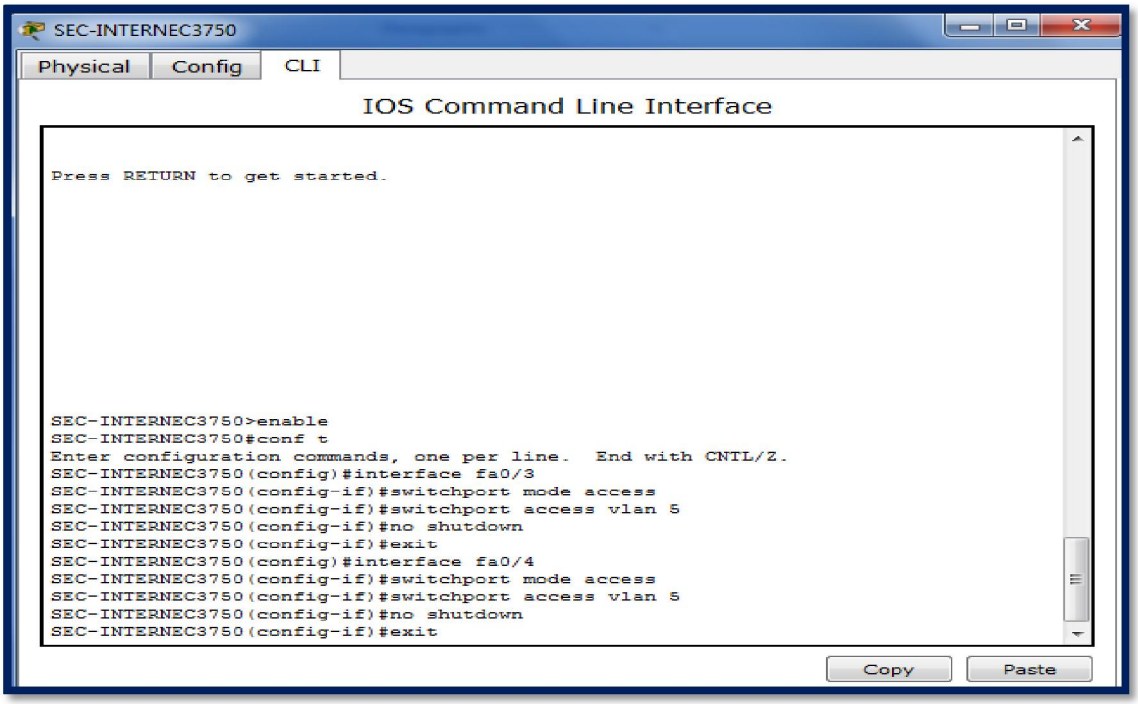


Figure III.9 : Attribution des ports des commutateurs aux VLAN$_s$

III.5.2.7. Configuration des interfaces VLAN

La configuration des interfaces VLAN est faite au niveau de chaque commutateur de chaque station en donnant des adresses IP pour le VLAN.

La figure III.10 illustre un exemple de configuration de l'interface VLAN.

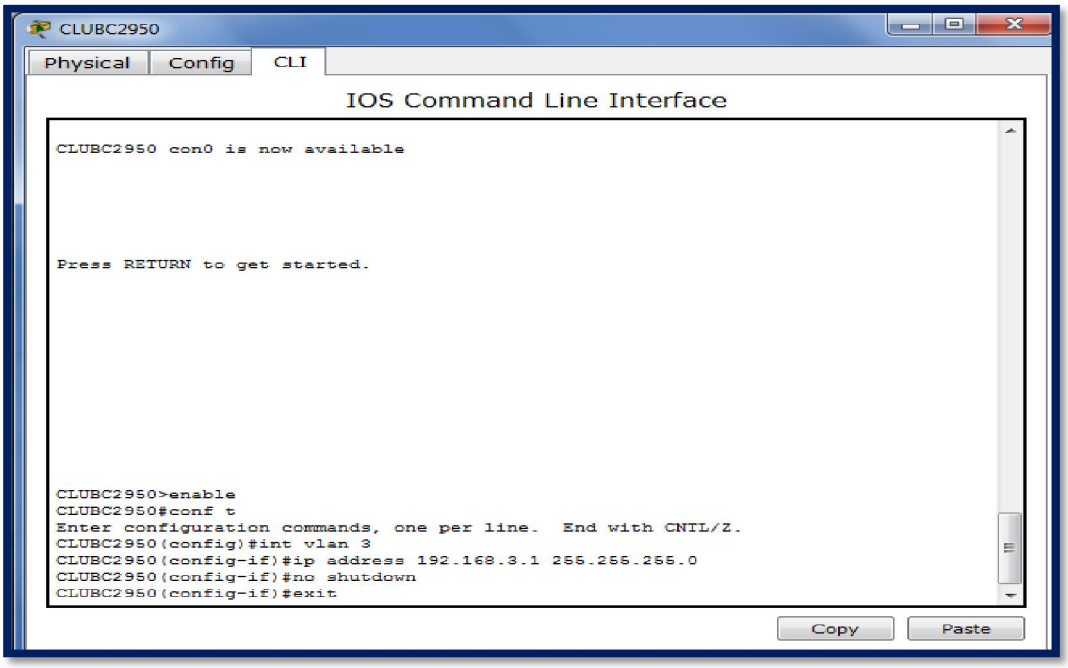


Figure III.10 : Configuration des interfaces VLAN

III.5.3. Configuration des routeurs (Routeur 1700 et Routeur DG)

La figure III.11 représente la configuration des routeurs.

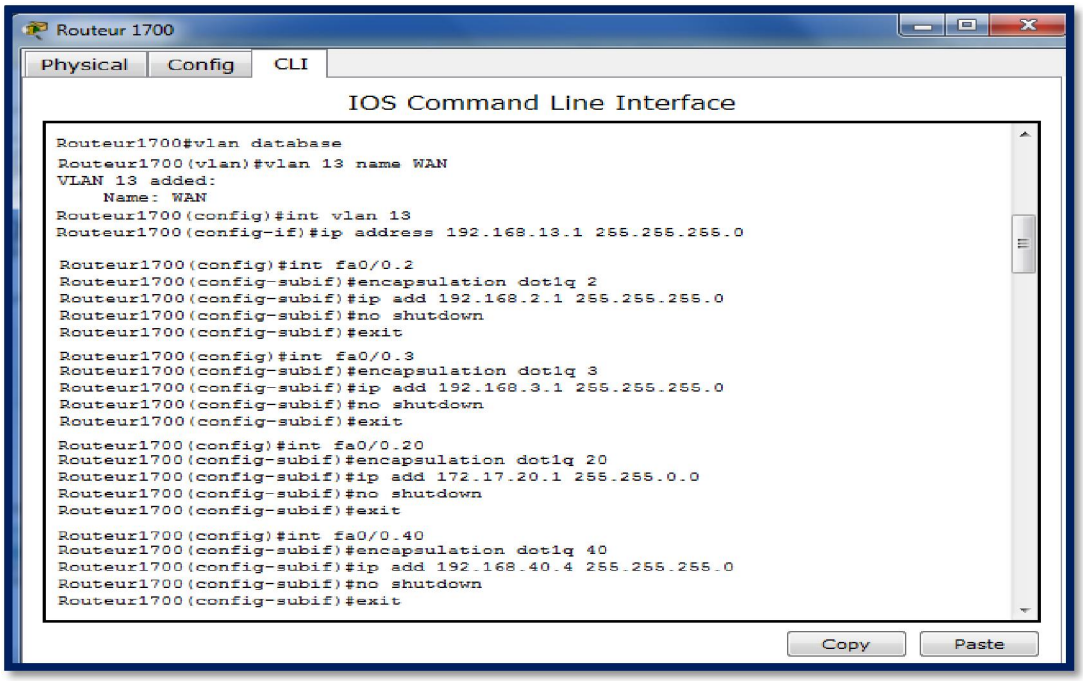


Figure III.11 : Configuration des routeurs

Pour visualiser la table de routage on utilise la commande **« show IP route »**

III.5.4. Configuration du routeur Wimax

La figure III.12 représente la configuration du routeur Wimax.

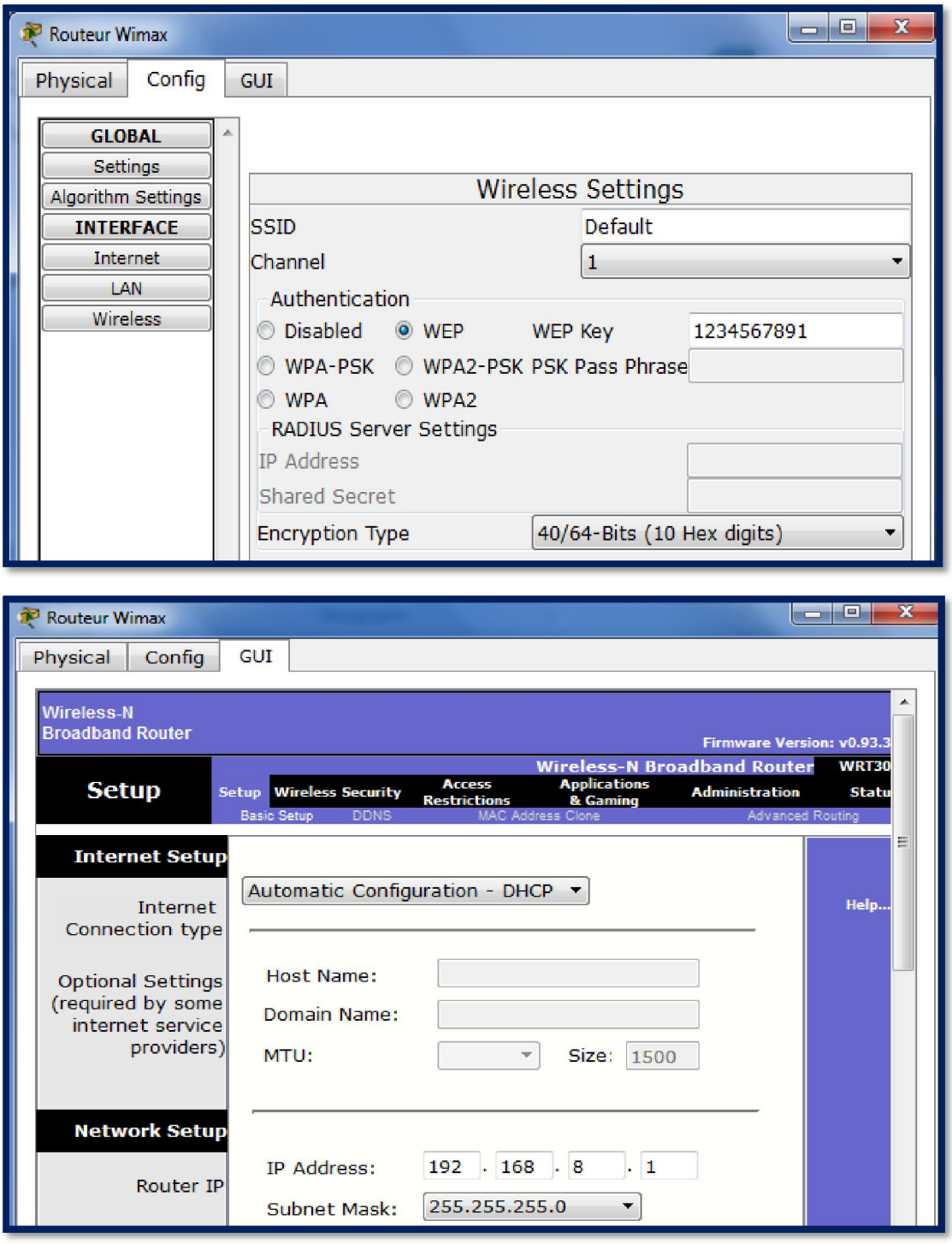


Figure III.12 : Configuration du routeur Wimax

III.5.5. Configuration des PC Wireless

La figure III.13 montre la configuration des PC Wireless.

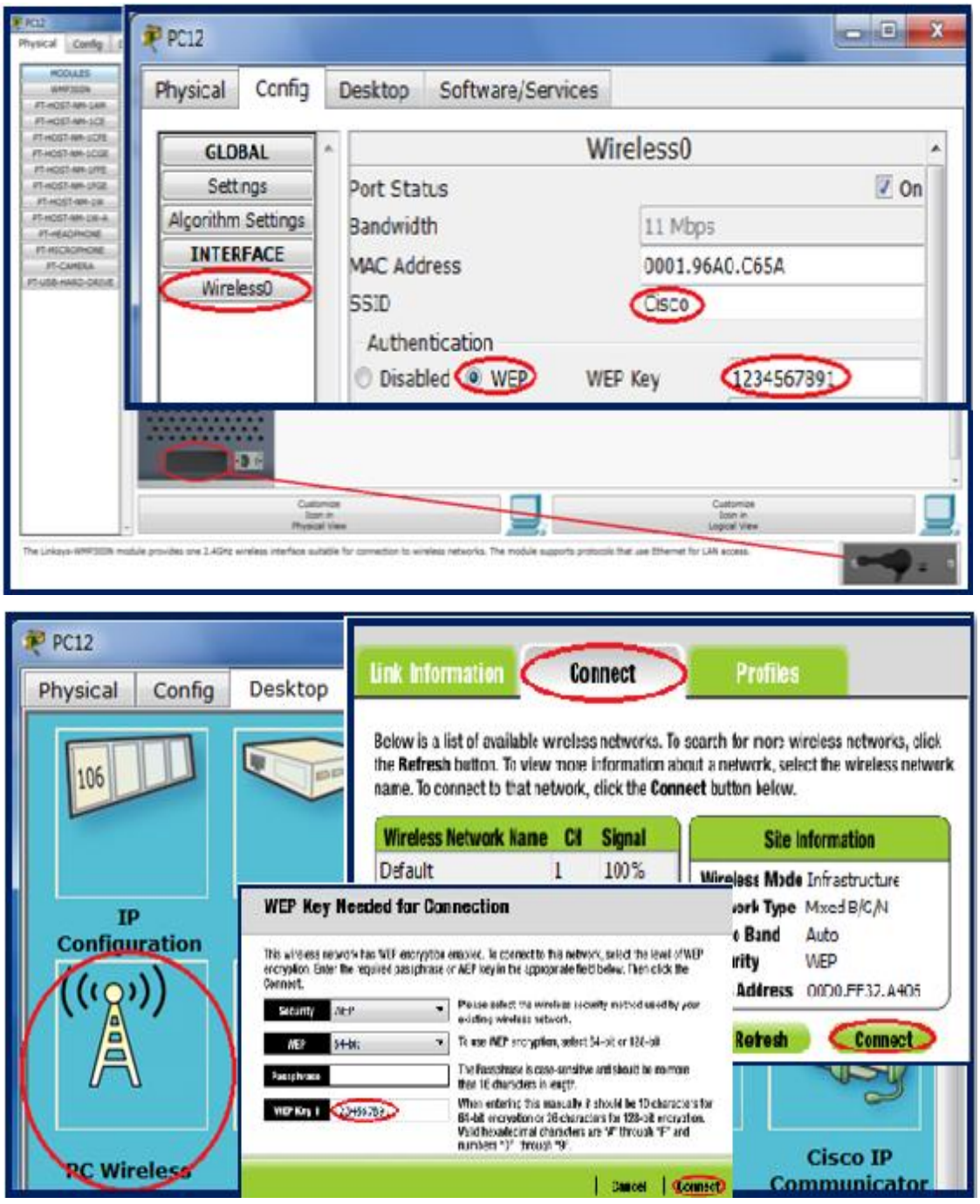


Figure III.13 : Configuration des PC Wireless

A travers ces étapes, nous avons réalisé une partie importante de la configuration d'un réseau local intégrant des $VLAN_s$, voici l'architecture simulée du réseau de la RTC obtenue illustrée dans la figure III.14:

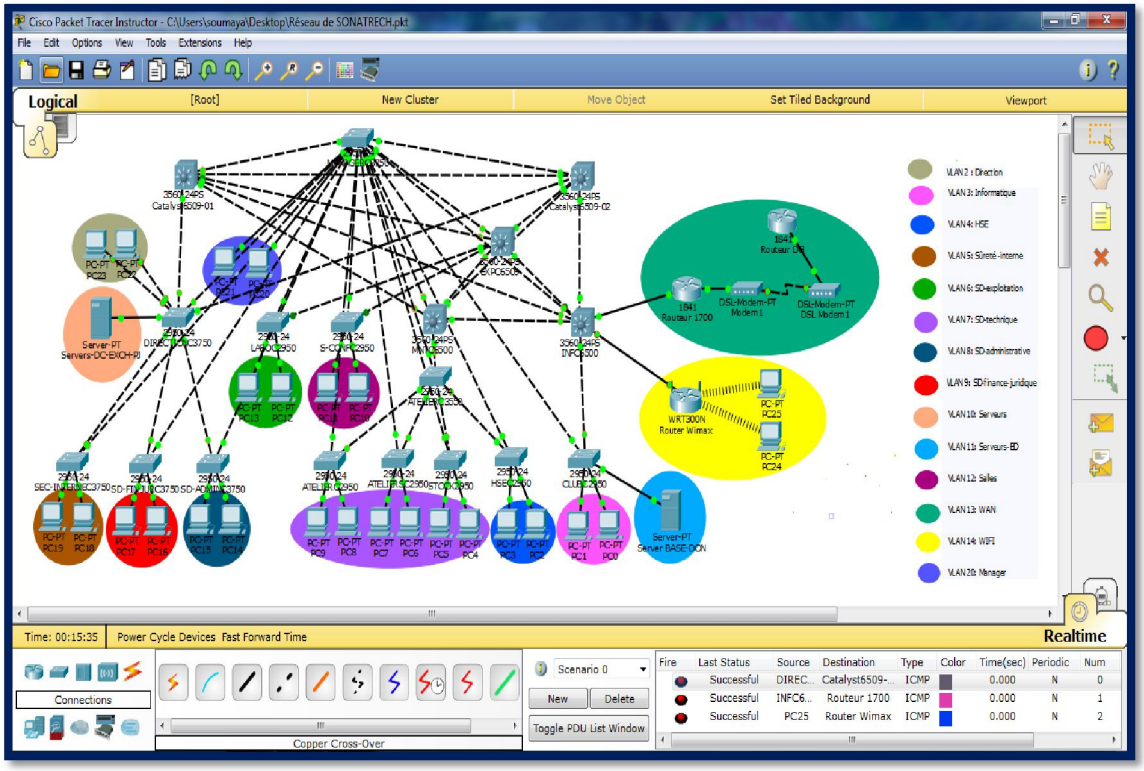


Figure III.14 : Architecture simulée du réseau de la RTC

III.6. Problématiques et solutions proposées

III.6.1. Etude critique sur l'architecture réseau existante

Après l'étude de l'architecture physique du réseau de la RTC on a déduit quelques critiques qui sont:

- Mauvaise répartition de l'architecture du réseau.
- La structure hiérarchique n'est pas respecter dans l'ancien bâtiment et sa topologie est en hybride (en étoile et en annaux).
- Topologie trop compliqué (voir figure III.1).
- Switchs supplémentaires.
- Plusieurs VLAN.
- Vulnérabilité du réseau et intrusion.
- Les différents équipements ne sont pas sécurisés.

III.6.2. Les solutions proposées

Afin de répondre aux différentes problématiques, nous avons suggéré selon notre compréhension des concepts durant notre stage un ensemble de propositions et solutions pouvant renforcer et performer les points faibles du réseau.

1. Notre travail se consacrera et se basera sur la liaison de l'ancien bâtiment d'une façon hiérarchique qui est appliqué dans le nouveau bâtiment et rendre sa topologie physique en étoile. Donc on va supprime le Switch EXPC6509 et on mettra les deux Switch INFC6509, MNTC6509 au niveau de la couche cœur, la redondance sera avec un lien physique et cinq Switch Catalyst Cisco 3750 au niveau de la couche distribution accès.

La figure III.15 représente la nouvelle architecture de l'ancien bâtiment.

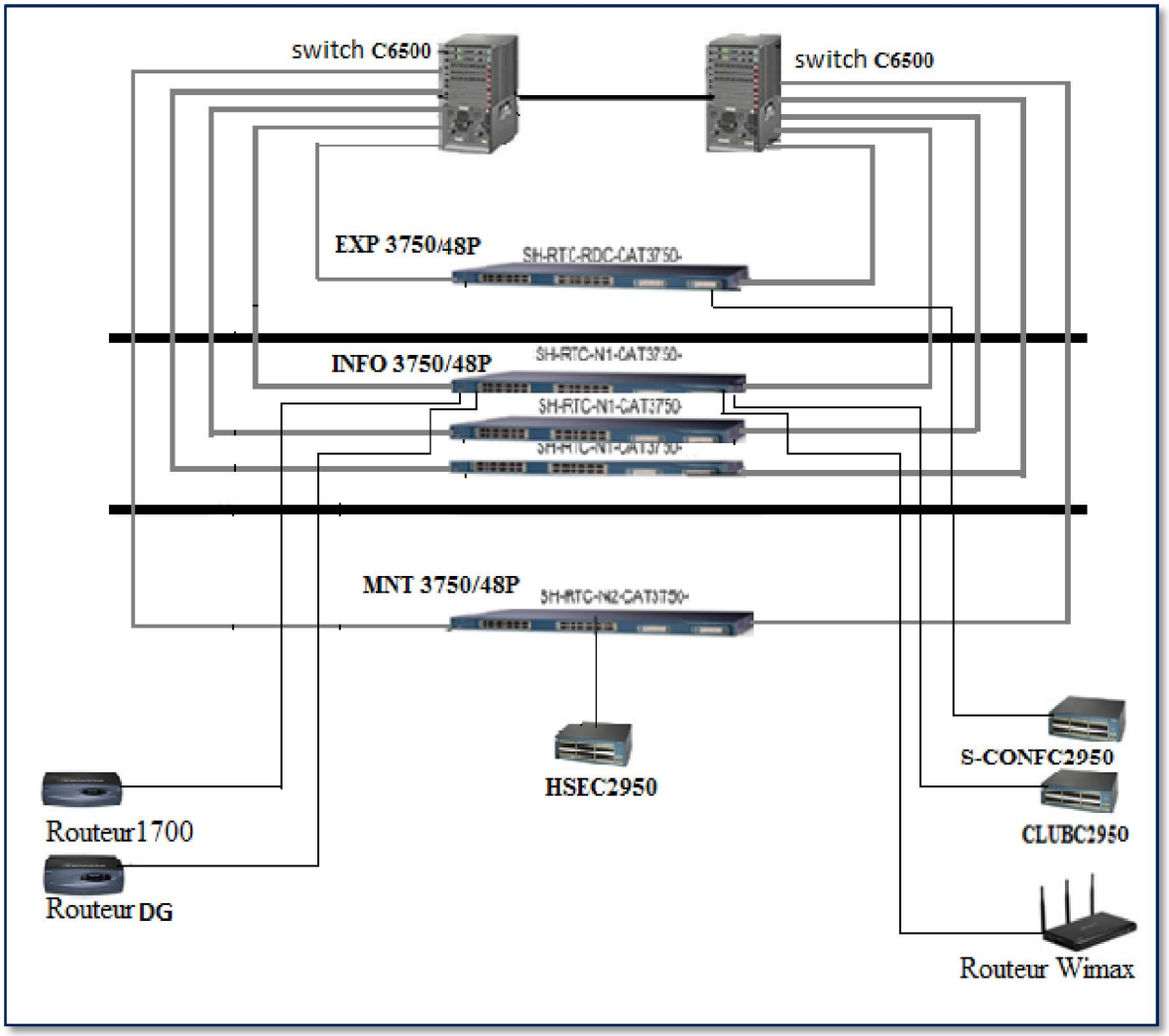


Figure III.15 : Nouvelle architecture de l'ancien bâtiment

2. Minimiser le nombre de Switchs
3. Regrouper les $VLAN_s$.
4. Sécuriser l'accès aux périphériques à l'aide des mots de passe.

La figure III.16 suivante représente l'architecture simulée du réseau de la RTC après l'amélioration

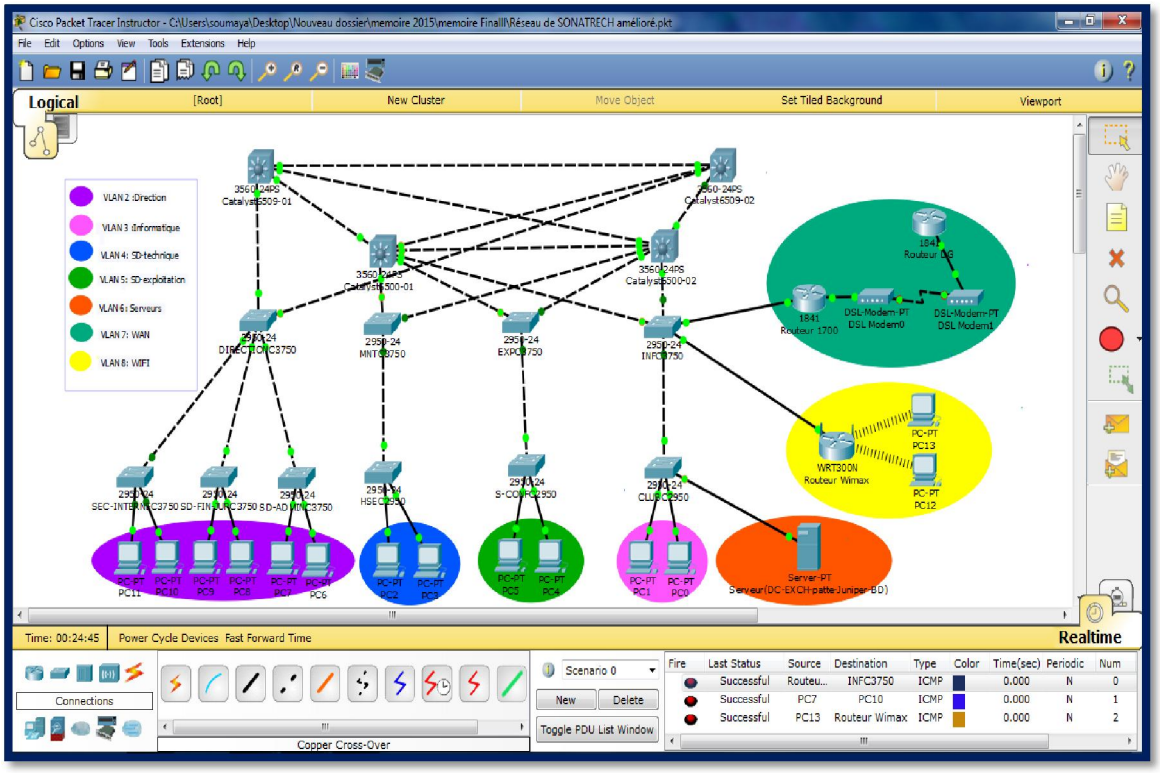
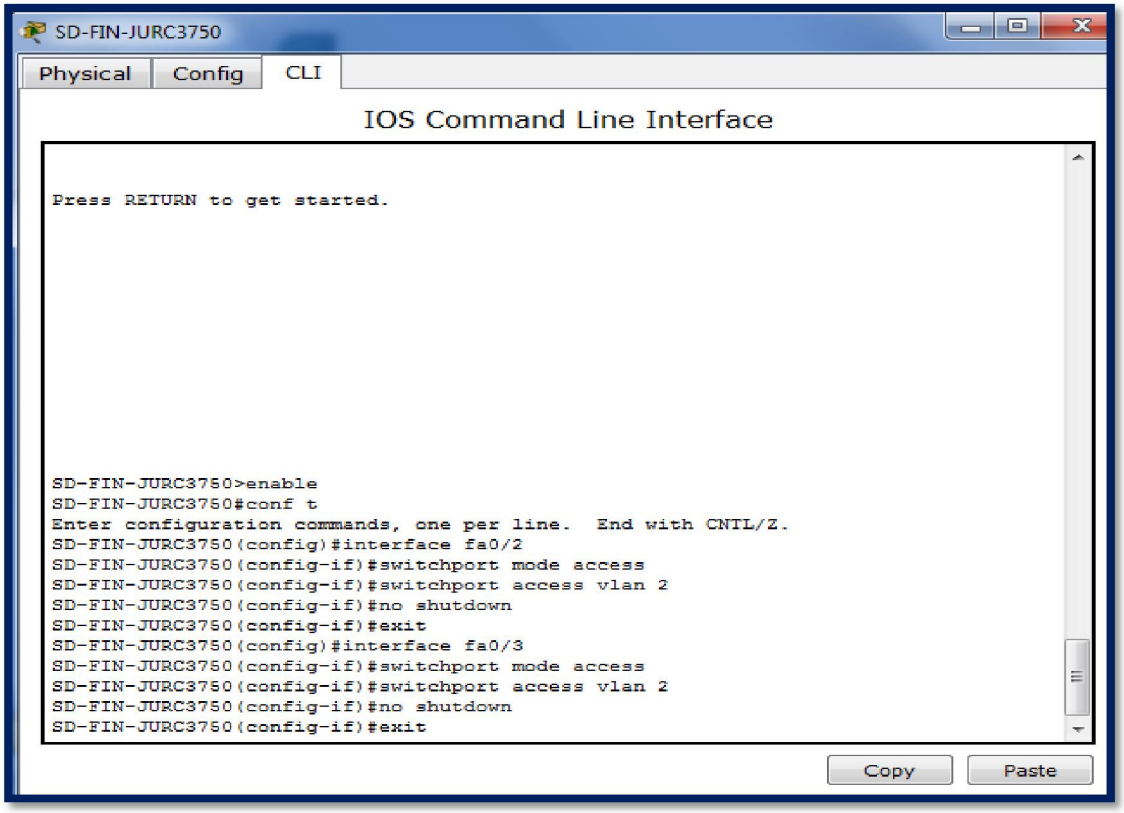


Figure III.16 : Architecture simulée du réseau de la RTC amélioré

III.6.2.1. Configuration des Switchs des sous directions

La figure III.17 montre la configuration des Switchs des sous directions regroupées en un seul VLAN avec celui de la direction.



III.17: Configuration des Switchs des sous directions

III.6.2.2. Sécurisation de l'accès aux périphériques

Il faut s'avoir qu'ISO utilise des modes organisés hiérarchiquement pour faciliter la protection des périphériques. Dans le cadre de ce dispositif de sécurité, ISO peut accepter plusieurs mots de passe, ce qui nous permet d'établir différent privilèges d'accès au périphérique.

La figure III.18 présente le mot de passe qu'on a affecté.

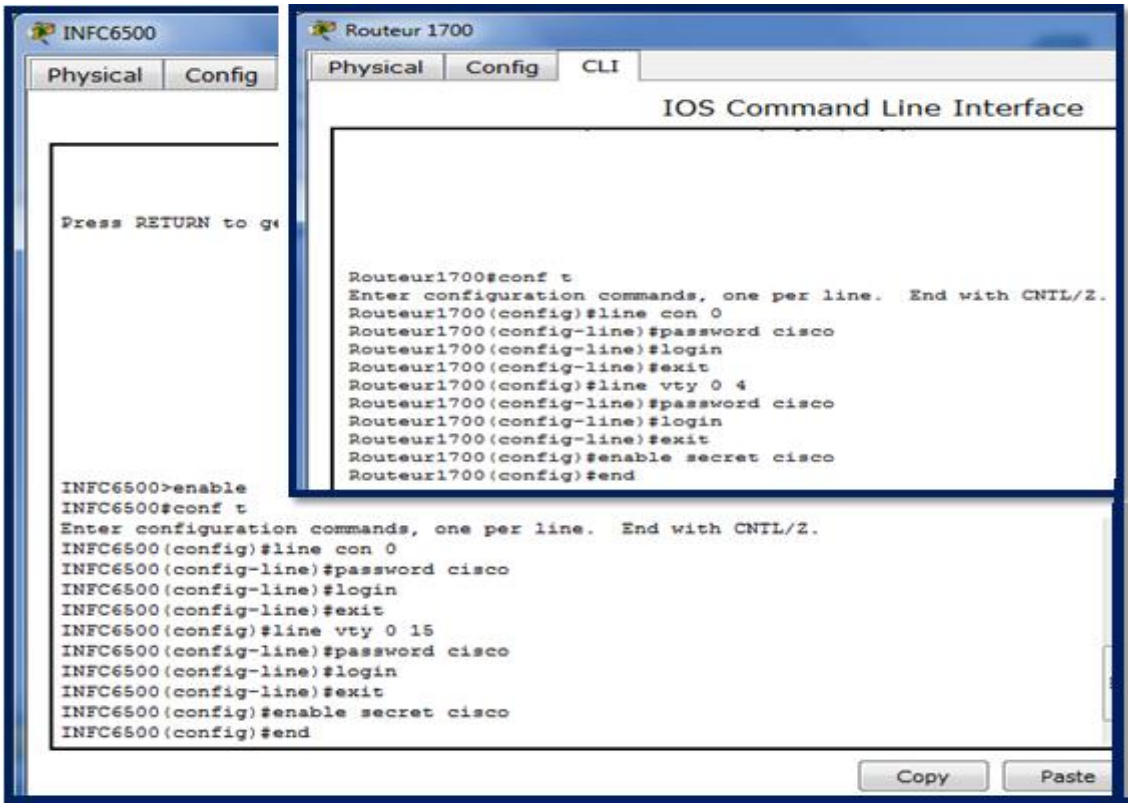


Figure III.18 : Configuration de mot de passe

III.7. Tests de validation

Dans cette partie, l'ensemble des tests de validation consiste à vérifier l'accessibilité de l'ensemble des équipements en utilisant la commande « Ping » qui teste la réponse d'un équipement sur le réseau. Donc, si un équipement veut communiquer avec un autre, le Ping permet d'envoyer des paquets au destinataire. Si l'équipement récepteur reçoit ces paquets donc la communication est réussie.

III.7.1. Vérification de la communication entre les équipements d'interconnexion

La figure III.19 montre le succès du teste effectuer entre le commutateur Accès et commutateur Cœur.

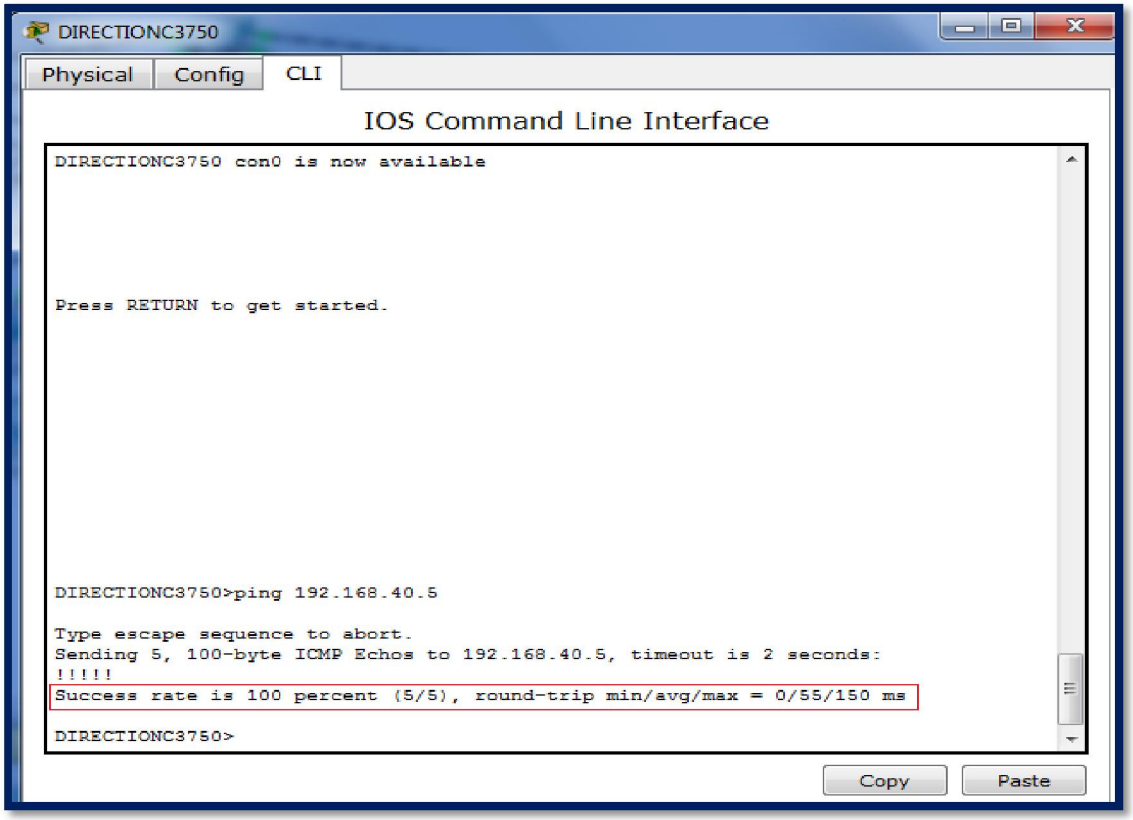


Figure III.19 : Test entre le Switch Accès et Cœur

III.7.2. Vérification de la communication entre les PC

- **Test entre des PC de même VLAN et commutateur distincts**

  Vérifiant l'accessibilité des PC appartenant au même VLAN situé dans un réseau local commun. Depuis le PC7 (192.168.2.3) essayons d'accéder au PC10 (192.168.2.6) tel que, les deux se trouvent dans le même VLAN et des commutateurs accès différents.

La figure III.20 suivante illustre le succès du teste effectué entre différents PC et commutateurs.

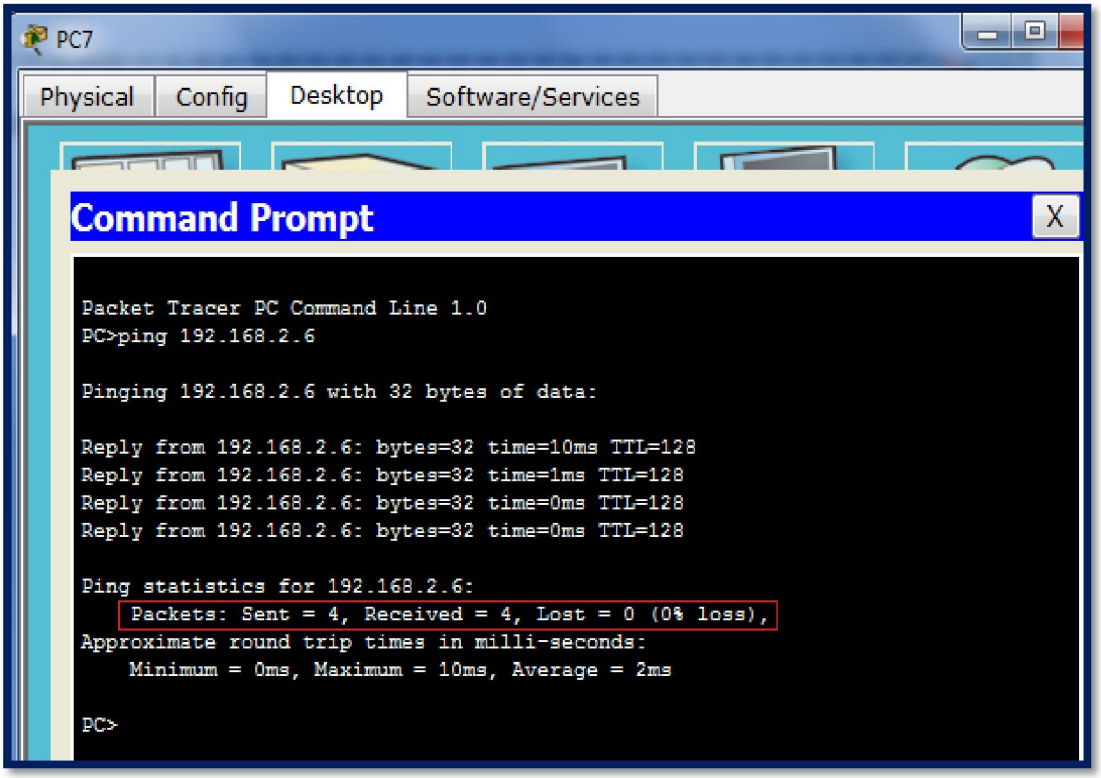


Figure III.20 : Test entre des machines du même VLAN et commutateurs distincts

III.7.3. Vérification du routage entre réseaux locaux virtuels (routage inter-VLAN)

Dans ce cas de figure on teste la connectivité entre les routeurs (routeur1700 et routeur DG) et les commutateurs distincts. On effectue donc un Ping à partir du routeur 1700 en essayant d'accéder au commutateur DIRECTIONC3750.

La figure III.21 montre le succès du test effectué entre le routeur 1700 et le commutateur (DIRECTIONC3750).

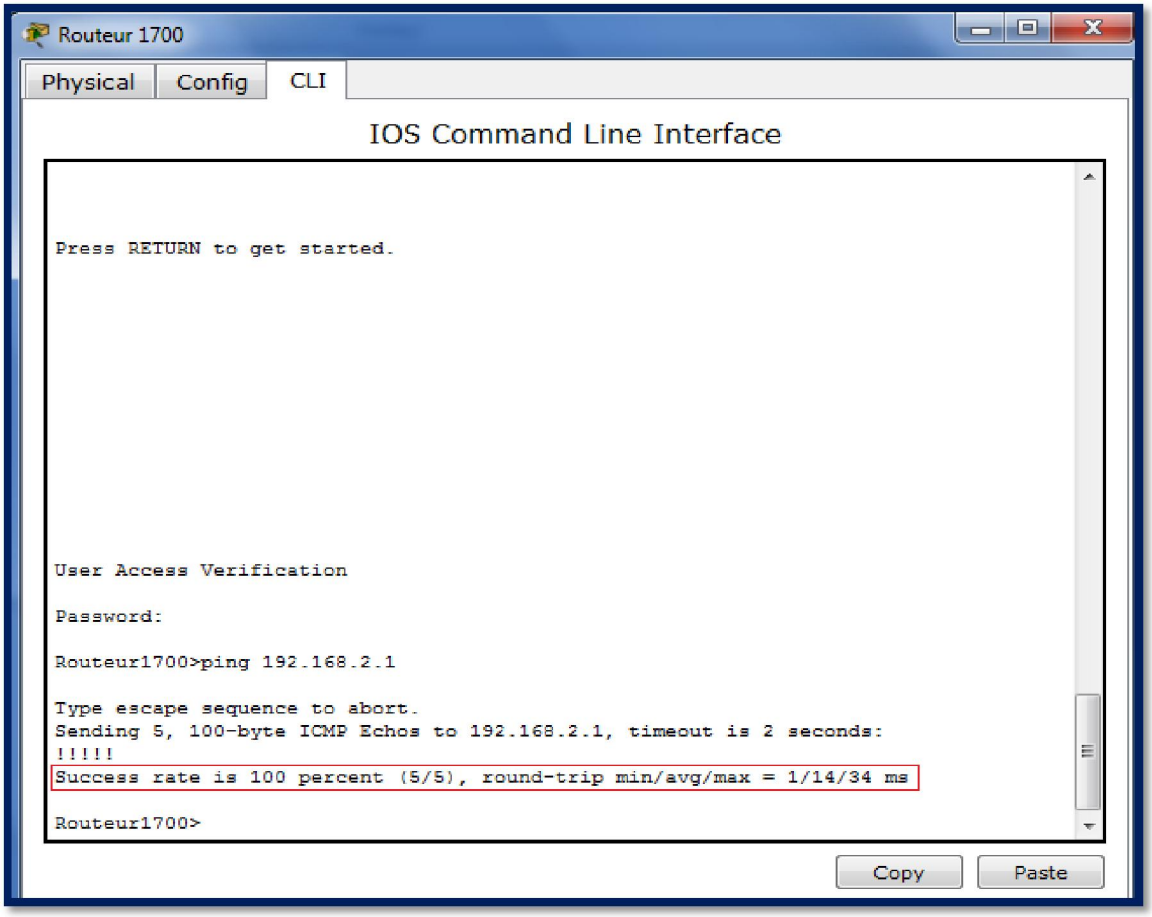


Figure III.21 : Test entre les routeurs WAN et les commutateurs

III.8. Etude critique sur l'architecture de sécurité

Nous avons remarqué dans l ' architecture de sécurité que l'ISS GX 4002 qui est relié à la DMZ ADMIN sécurise uniquement cette partie et afin de sécuriser toute la DMZ on a proposé la solution suivante :

- Du moment que le l'ISS Proventia GX4002 a juste 2 ports et le ISS Proventia GX 5008 a plus que 2, donc on met le ISS GX4002 à la place de l'ISS GX5008 et ce dernier on le place entre le firewall et toute la DMZ.

La figure III.22 illustre le schéma de sécurité de la RTC amélioré.

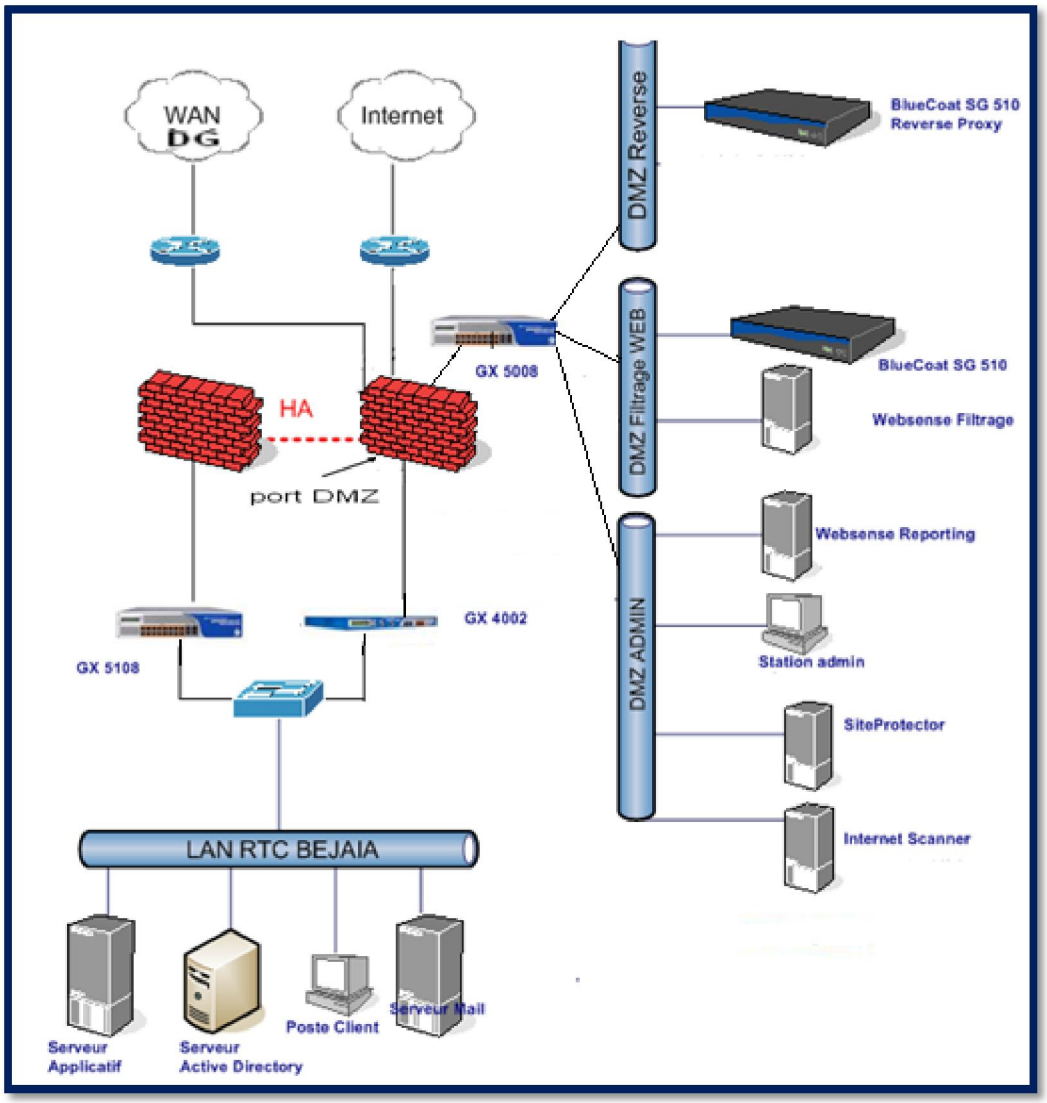


Figure III.22 : Schéma de sécurité de la RTC amélioré

Conclusion

A l'issu de ce chapitre, nous connaissons désormais le minimum qu'il faut apporter à notre réseau pour le rendre plus rigide et plus performant. Nous savons alors comment améliorer les liaisons afin d'avoir une meilleure tolérance aux fautes, Les étapes à suivre pour la mise en œuvre des VLANs .Ainsi l'étude critique nous permettra de donner naissance à une nouvelle architecture dans laquelle les "points faibles" cités n'existeront plus et nous aurons alors une architecture plus résistante.

Conclusion générale et perspectives

Au terme de ce projet, il convient de dire, d'une part, que sa réalisation s'est révélée très enrichissante et bénéfique, et d'autre part, ce projet nous a permis de mettre en pratique les connaissances acquises durant le cycle de notre formation, de se familiariser avec un environnement dynamique et d'avoir une idée plus profonde et plus pratique sur l'importance du réseau dans une entreprise.

L'organisation des réseaux locaux de SONATRACH, leur interconnexion et la conception d'un réseau local virtuel ainsi que la sécurité était notre objectif durant ce projet.

Afin d'accomplir notre travail et d'aboutir au résultat escompté, nous avons choisi le simulateur Packet Tracer pour les différents avantages qu'il présente, la mise en évidence avec une grande exactitude de l'architecture du système à réaliser en précisant les différents composants, ainsi que la simplicité de la clarté des matériaux dont on aura besoin, se qui facilite considérablement leur configuration sur Packet Tracer.

En effet, l'intégration des VLANs dans un réseau local améliore les performances de ce dernier et lui offre des avantages.

La réalisation de ce projet a été bénéfique et fructueux pour nous dans le sens où il nous a permis d'approfondir et d'acquérir de nouvelles connaissances qui seront utiles et déterministes pour notre avenir.

Nous souhaitons que ce travail puisse servir comme un outil d'aide et de documentation pour les étudiants à l'avenir, et une base de travail pour les utilisateurs concernés.

En guise de perspectives, ce travail peut être repris avec un élargissement de la liste de critère pour la partie sécurité afin de la renforcée.

Références

Bibliographie

[1] Guy Pujolle, Cours Réseaux et Télécoms, EYROLLES, 2008

[2] Bertrand Petit, Architectures des Réseaux, ELLIPSES, 2006

[3] Philippe ATELIN, Réseaux Informatiques (Notions fondamentales), 3éme éditions ENI, Janvier 2009, ISBN : 978-2-7460-4681-8

[4] Servin Claude, Réseaux et Télécoms, 2éme édition, Dunod, 2006

[5] Danièle DROMARD, Dominique SERET, Architecture des Réseaux, PEARSON France, 2013, ISBN : 978-2-7440-7664-0

[6] Doglace COMER, réseaux (Architectures, Protocoles, Applications), InterEditions, 2005

[7] Andrew Tanenbaum, Architectures et Protocoles des Réseaux, InterEdition, 2009

[12] Paul haigh, serveur base de données, 04 aout 1998-[consulté mars 2014]. Disponible sur : http://www.slee@ile-maurice.com.

[24] Michel Galka-Cortes, Contrôleur de Domain, 2008-[consulté avril 2014]. Disponible sur : http://www.neolan.org.

Webographie

[8] http://www.reseaucerta.org/docs/didactique/VLAN.pdf

[9] http://www.awt.be/web/res/index.aspx?page=res,fr,fic,120,002

[10] http://www.ec2lt.sn/sites/default/files/rapports_vlans.pdf

[11] http://www.ybet.be/hardware2_ch2/hard2_ch2.php

[13] http://www.cisco.com/,cisco systems

[14] http://www.cisco.com/c/en/us/products/switches/catalyst-6509-neb-a-switch/index.html

[15] https://www.cisco.com/web/offer/emear/dg20/CPQRG-110813-PDF.pdf

[16] http://www.cisco.com/c/en/us/products/switches/catalyst-2950-series-switches/index.html

[17] http://www.cisco.com/c/en/us/products/routers/1700-series-modular-access routers/index.html

[18] http://www.cisco.com/web/FR/solutions/sp/mobile_internet/wimax.html

[19] https://www.f-secure.com/fr_BE/web/home_be/anti-virus

[20] http://www.websense.com/content/Regional/France/WebFilter.aspx

[21] http://www.edgeblue.com/SG510-Proxy.asp

[22] http://www.juniper.net/us/en/local/pdf/datasheets/1000143-en.pdf

[23] http:// www.iss.net/support/

[25] http://www.dell.com/PowerEdge

[26] http://www.systrancia.com

[27] http://www. squasta@microsoft.com

[28] http://www.nolot.eu/Download/Cours/reseaux/m2pro/ASR0708/Cours2-ArchiReseaux.pdf

[29] http://www.cisco.com/web/learning/netacad/demos/CCNPIv30/ch1/1_1_1/index.html

[30] www.cisco.com/cisco/web/support/CA/fr/109/.../1092443_21vtp.html

Résumé

La majorité des entreprises ne peuvent plus ignorer désormais d'intégrer la sécurité des réseaux, et en particulier l'organisation des réseaux locaux, afin de faciliter la communication entre les différents sous réseaux. Ce mémoire explique tout d'abord ce qui est un réseau informatique et réseau local virtuel, ainsi que toutes leurs notions de base, il présente une étude de sécurité du réseau de SONATRACH de Béjaïa (RTC) puis propose une nouvelle architecture. Nous avons présenté les concepts fondamentaux de l'architecture existante et de son fonctionnement à savoir la partie sécurité et la partie système, puis on a analysé les différents éléments qui composent un réseau local, leur architecture ainsi que les VLANS, et son implémentation en utilisant le logiciel Cisco Packet Tracer. Nous avons concentré notre attention sur les critiques à l'encontre de l'architecture du réseau existant au sein de RTC Béjaia (Région Transport Centre), et la proposition de solutions pour pallier aux points faibles. Enfin nous avons mis en œuvre les solutions proposées.

Mots clé : Sécurité des réseaux, Réseaux locaux, VLAN, RTC.

Abstract

The majority of the companies cannot ignore now integrate the networks, security and in particular the organization of local networks, in order to facilitate the communication between the different ones under networks. This memory explains first of all what is a data-processing network and LAN, like all their basic concepts, it presents a network security study of SONATRACH of Béjaïa (RTC) then proposes a new architecture. We present the fundamental concepts of existing architecture and its operation to knowing the safety part and the system part and then it analyzes the various elements which compose a LAN, their architecture as well as the VLANs, and its implementation by using the software Cisco Packet Tracer. We focus our attention on criticisms against the existing network architecture within RTC Bejaïa (Regional Transport Centre), and the proposal for solutions to mitigate the weak points; finally we implemented the proposed solutions.

Keywords: Networks security, LANs, VLAN, RTC.