République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique
Université Abderrahmane Mira de Bejaia

Faculté des Sciences Exactes
Département d'Informatique

MÉMOIRE DE FIN DE CYCLE

En vue de l'obtention du diplôme d'un Master Professionnel en Informatique

Option : Administration et Sécurité des Réseaux

Thème

Simulation d'une réorganisation et reconfiguration sécurisé pour le réseau de l'entreprise SONATRACH

Soutenues devant le jury composé de :

Présidente : M^{me} R.SOUADIH

Examinateur : M^{r}A.BAADACHE

Examinateur : M^{r}N.AL SAKAAN

Encadreur : P^{r}A.BOUKERRAM

Co-Encadreur : M^{r}D.TOUAZI

Réalisé par :

M^{elle}SOUFI yasmina

M^{elle}TALBI lydia

Promotion : 2015/2016

Remerciements

Tout acte de recherche n'est que concrétisation d'un travail collectif.

Avant de présenter ce mémoire nous tenons à remercier notre promoteur Pr A. Boukerram pour l'intérêt porté à notre travail, ses conseils, ses encouragements et sa disponibilité.

Notre reconnaissance va également aux membres du Jury pour nous avoir fait l'honneur d'y participer.

Nos vifs remerciements sont également adressés à Mr Touazi, pour ses encouragements et sa disponibilité.

Un grand merci au personnel de la division Informatique de Hassi R'mel SONATRACH et plus particulièrement Mr B.Bouhoune.

Nos sincères remerciements vont à Mr K.Souadih pour sa disponibilité et l'aide qu'il nous a apporté.

Nous ne pourrions clore ces remerciements sans citer Nos Parents sans qui notre travail n'aurait jamais pu aboutir.

Enfin, nous tenons aussi à remercier également tous les membres de jury pour avoir accepter d'évaluer notre travail.

Dédicaces

Louange à Dieu, sans Lui rien de tout cela n'aurait pu être.

A nos trés chers sœurs pour leurs compréhensions et encouragements.

A toutes nos familles grand parents, oncles, tantes, cousins et cousines que Dieu vous protège et vous garde en Bonne Santé.

A tous nos amis.

A toutes les personnes qui nous ont soutenu et participé de prés ou de loin à l'élaboration de ce mémoire.

nous vous dédions ce modeste travail.

Table des matières

Table des figures

Liste des tableaux

Liste des Abréviations

ACL : Access control List.

ARP : Adress Résolution Protocol.

DHCP : Dynamic Host Configuration Protocol.

DNS : Domain Name system.

DRGB : Direction Régionale de Bejaia.

FTP : File Transfer Protocol.

HSRP : Hot Standby Routing Protocol.

HTML : Hypertext Markup Language.

HTTP : HyperText Transfer Protocol.

IP : Internet Protocol.

ISO : International Standards Organization.

LAN : Local Area Network.

MAC : Media Access Control.

MAN : Metropolitan Area Network.

OSI : Open System Interconnexion.

QOS : Quality of Service.

RSTP : Rapid Spanning Tree Protocol.

SONATRACH :Société Nationale de Transport et Commercialisation des hydrocarbures.

SSH : Secure Shell.

STP : Spanning Tree Protocol.

TCP : Transmission Control Protocol.

VLAN : Virtual Local Area Network.

VPN : Virtual Private Network.

VTP : VLAN Trunking Protocol.

WAN : Wide Area Network.

Introduction générale

Le rôle des réseaux a sensiblement évolué ces dernières années, il ne se limite pas au transfert de l'information en toute sécurité mais aujourd'hui il contribue largement à la rationalisation des utilisateurs et à l'optimisation des performances applicatives. De ce fait on a besoin d'un ensemble des moyens et techniques permettant la diffusion d'un message auprès d'un groupe plus ou moins vaste et hétérogène.

Les réseaux informatiques sont de plus en plus répondus et complexes. L'implantation d'un réseau complexe doit être sûr pour avoir des réseaux fiables. Ainsi pour une meilleure gestion et diminuer les risques de pannes, une conception intelligente s'impose.

Dans ce contexte, nous allons implanter un modèle type de configuration d'un réseau qui assure l'identification, l'adoption et le maquettage des futurs projets. Ces projets nécessitent un dossier technique complet et un gain du temps important lors de la réalisation.

Ce manuscrit est composé de quatre chapitres. Le premier chapitre porte sur des réseaux auxquels on va présenter brièvement quelques notions théoriques.

Le second chapitre concerne la présentation du cadre du stage.D'autre part le troisième chapitre qui consiste en la conception du modèle dont la procédure de préparation, la schématisation, la nomination des équipements, la désignation des interfaces, les VLANs, le plan d'adressage et la présentation des protocoles utilisés.

Enfin nous terminons par la réalisation du modèle type à travers le simulateur " Cisco Packet Tracer ", ainsi le test et la validation de la configuration. Une conclusion générale avec des perspectives viennent terminer ce travail.

Chapitre 1

Généralités

1.1 Introduction

Les réseaux ont pour fonction de transporter des données d'une machine terminale à une autre. Une série d'équipements matériels et de processus logiciels sont mis en œuvre pour assurer ce transport, depuis les câbles terrestres ou les ondes radio dans lesquels circulent les données jusqu'aux protocoles et règles permettant de les traiter.

Dans ce chapitre, on commence par définir le réseau informatique. Ensuite on présente le modèle OSI et le modèle TCP/IP. Les équipements et les protocoles réseaux sont également présentés dans de ce chapitre.

1.2 Définition d'un réseau

Le terme générique " réseau " définit un ensemble d'entités (objets, personnes, etc.) interconnectées les unes avec les autres. Un réseau permet ainsi de faire circuler des éléments matériels ou immatériels entre chacune de ces entités selon des règles bien définies.

• **réseau (en anglais network) :**

Ensemble des ordinateurs et périphériques connectés les uns aux autres. Notons que deux ordinateurs connectés ensemble constituent à eux seuls un réseau minimal.

• **mise en réseau (en anglais Networking) :**

Mise en œuvre des outils et des tâches permettant de relier des ordinateurs afin

qu'ils puissent partager des ressources en réseau. [1]

1.3 Objectifs de l'utilisation des réseaux :

les objectifs d'un réseau sont classiquement les suivants :

- **Le partage de ressources :**

Rendre accessible à une communauté d'utilisateurs des programmes, des données et des équipements informatiques (i.e. un ensemble de ressources) indépendamment de leur localisation.

- **La Fiabilité :**

Permettre le fonctionnement même en cas de problèmes matériels (sauvegardes, duplication ...). Penser aux applications militaires, bancaires, au contrôle des centrales nucléaires ou aériennes...

- **La réduction des coûts :**

Les petits ordinateurs (PC par ex.) ont un meilleur rapport prix/performances que les gros. Aujourd'hui, nous trouvons surtout des architectures Client/serveur plus économique, plus souple et permettant un déploiement incrémental aisé (contrairement aux architectures à base de mainframe.)

1.4 Classification des réseaux

- **LAN (Local Area Network = réseau local d'entreprise (RLE en français)) :**

Un réseau local est un réseau d'ordinateurs situé sur un même site. Les communications sur ce type du réseau sont généralement rapides (100 Mbits/s ou 1Gbits/s) et gratuites puisqu'elles ne passent pas, par les services d'un opérateur de télécommunication. Le fait que le réseau soit sur un site bien délimité n'implique pas nécessairement qu'il soit de taille très réduite. Il est souhaitable de le segmenter en sous-réseaux quand le nombre de nœuds y devient important. L'ensemble reste un réseau local tant qu'il est indépendant des services d'un opérateur extérieur.

- **MAN (Metropolitan Area Network = Réseau métropolitain) :**

Lorsqu'un réseau privé, s'étend sur plusieurs kilomètres, dans une ville par exemple les réseaux locaux sont interconnectés via des liaisons téléphoniques à haut débit ou à l'aide d'équipements spéciaux comme des transmissions hertziennes. Ce type de regroupement de réseaux locaux peut se faire au niveau d'une ville et l'infrastructure du réseau métropolitain peut être privée ou publique.

- **WAN (Wide Area Network = Réseau étendu) :**

Ces réseaux relient plusieurs réseaux locaux en les interconnectant via des lignes louées ou via Internet. Ex : les réseaux bancaires qui établissent des liaisons entre les agences et le siège central. Dans le cas de l'utilisation d'Internet, on parle de VPN (VIRTUAL PRIVATE NETWORK) puisqu'on utilise alors un réseau public pour faire transiter des informations privées. [2]

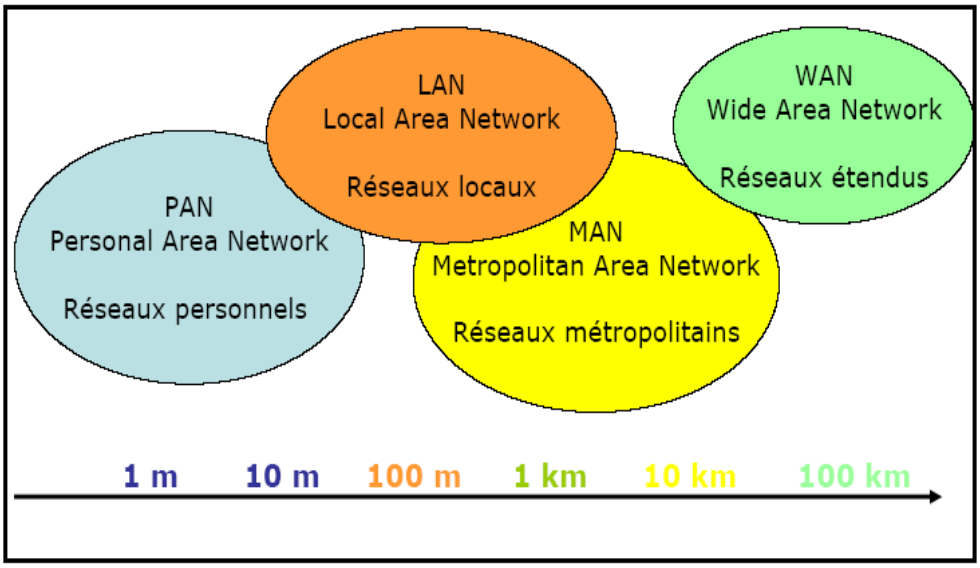

FIG. 1.1 – La classification des réseaux selon leur étendue.

1.5 Le modèle OSI (Open System Interconnection)

Pour faciliter l'interconnexion des systèmes, un modèle dit d'interconnexion des systèmes ouverts, appelé encore OSI (Open Systems Interconnection) a été défini par l'ISO (International Standards Organization).

Le modèle OSI répartit les protocoles utilisés selon sept couches, définissant ainsi un langage commun pour le monde des télécommunications et de l'informatique. Il constitue aujourd'hui le socle de référence pour tous les systèmes de traitement de l'information.

Chaque couche regroupe des dispositifs matériels (dans les couches basses) ou logiciels (dans les couches hautes). Entre couches consécutives sont définies des interfaces sous forme de primitives de service et d'unités de données rassemblant les informations à transmettre et les informations de contrôle rajoutées. [3]

Couche 1 : physique

La couche physique rassemble les moyens électriques, mécaniques, optiques ou hertziens par lesquels les informations sont transmises. Les unités de données sont donc des bits 0 ou 1.

Couche 2 : liaison

La couche liaison gère la fiabilité du transfert de bits d'un nœud à l'autre du réseau, comprenant entre autres les dispositifs de détection et de correction d'erreurs, ainsi que les systèmes de partage des supports. L'unité de données à ce niveau est appelée trame.

Couche 3 : réseau

La couche réseau aiguille les données à travers un réseau à commutation. L'unité de données s'appelle en général un paquet.

Couche 4 : transport

La couche transport regroupe les règles de fonctionnement de bout en bout, assurant ainsi la transparence du réseau vis-à-vis des couches supérieures. Elle traite notamment l'adressage, l'établissement des connexions et la fiabilité du transport.

Couche 5 : session

La couche session réunit les procédures de dialogue entre les applications : établissement et interruption de la communication, cohérence et synchronisation des opérations.

Couche 6 : présentation

La couche présentation traite les formes de représentation des données, permettant la traduction entre machines différentes.

Couche 7 : application

Source et destination de toutes les informations à transporter, la couche application rassemble toutes les applications qui ont besoin de communiquer par le réseau : messagerie électronique, transfert de fichiers, gestionnaire de bases de données, etc.

Fig. 1.2 – Le Modèle OSI.

1.6 Le modèle TCP/IP

le protocole TCP est basé sur les couches OSI, mais il n'en a lui-même que 4. [4]

La couche 1 : Accès réseau

Le nom de cette couche a un sens très large et peut parfois prêter à confusion. On lui donne également le nom de couche hôte-réseau. Cette couche se charge de tout ce dont un paquet IP a besoin pour établir un liaison physique, puis une autre

liaison physique. Cela comprend les détails sur les technologies LAN et WAN, ainsi que tous les détails dans les couches physiques et liaison de données du modèle OSI.

La couche 2 : Internet

Le rôle de la couche Internet consiste à envoyer des paquets sources à partir d'un réseau quelconque de l'inter réseau et à les faire parvenir à destination, indépendamment du trajet et des réseaux traversés pour y arriver. Le protocole qui régit cette couche est appelé protocole IP.

L'identification du meilleur chemin et la communication des paquets ont lieu au niveau de cette couche.

La couche 3 : Transport

La couche transport est chargée des questions de qualité de service touchant la fiabilité, le contrôle de flux et la correction des erreurs. L'un de ses protocoles, TCP , fourni d'excellents moyens de créer, en souplesse, les communications réseau fiables, circulant bien et présentant un taux d'erreurs peu élevé. Le protocole TCP est orienté connexion. Il établit un dialogue entre l'ordinateur source et l'ordinateur de destination pendant qu'il prépare les informations de couche application en unité appelées segments.

La couche 4 : Application

Le modèle TCP/IP regroupe en une seule couche tous les aspects liés aux applications et suppose que les données sont séparées de manière adéquate pour la couche suivante.

FIG. 1.3 – le Modèle TCP/IP.

1.7 Les équipements de base d'un réseau informatique

1.7.1 Les unités hôtes

Les unités directement connectées à un segment de réseau sont appelées hôtes. Ces hôtes peuvent être des ordinateurs, des clients, des serveurs, des imprimantes, des scanners ainsi que de nombreux autres types d'équipements.

1.7.2 Les commutateurs

Un commutateur réseau diffuse la trame reçue vers l'équipement concerné car il est capable de déterminer l'adresse à laquelle cette trame est destinée. Le commutateur s'appuie sur une table des adresses MAC pour diffuser la trame vers l'équipement concerné. Le concentrateur et le commutateur réseau agissent au niveau de la couche de liaison des données du modèle OSI.

1.7.3 Les routeurs

Un routeur assure le routage des paquets entre deux réseaux utilisant ou non le même protocole. Il doit être connecté à deux réseaux pour avoir des trames à router ; il agit au niveau de la couche réseau du protocole OSI. [5]

1.8 Les protocoles LAN

Dans ce suit, nous allons définir les différents outils ainsi les protocoles utilisés dans les réseaux LAN. [6]

1.8.1 Réseaux locaux virtuels (VLANs)

Un réseau local virtuel (VLAN) est un réseau local (LAN) distribué sur des équipements de niveau 2 du modèle OSI (couche liaison). Le domaine de diffusion se retrouve ainsi réparti sur ces mêmes équipements de niveau 2. Ainsi, tous les hôtes appartenant au même réseau local (domaine de diffusion) constituent un groupe logique indépendant de la topologie physique du réseau.

1.8.2 Le protocole VTP (Vlan Trunking Protocol)

VTP ou VLAN Trunking Protocol est un protocole utilisé pour configurer et administrer les Vlans sur les périphériques Cisco. VTP est utilisé entre 2 switchs si le lien les reliant est un trunk. VTP passe sur le native vlan.

Les dispositifs de VTP peuvent être configurés pour fonctionner suivant les trois modes suivants :

- **le mode serveur :**

En mode serveur, il est possible de créer, modifier ou supprimer des VLANs et des les transmettre au domaine.

- **le mode client VTP :**

En mode client, le Switch reçoit les mises à jour, les prend en compte et les transmet à ses voisins. Il ne peut pas faire de modification.

- **le mode transparent :**

En mode transparent, le switch reçoit les mises à jour et les transmet à ses voisins sans les prendre en compte. Il peut créer, modifier ou supprimer ses propres vlans mais ne les transmet pas. [7]

1.8.3 protocole Spanning Tree

Le protocole Spanning Tree (STP) est un protocole de la couche 2 (liaison de données) conçu pour les commutateurs. Le standard STP est défini dans le document IEEE 802.1D-2004. Il permet de créer un chemin sans boucle dans un environnement commuté et physiquement redondant. STP détecte et désactive ces boucles et fournit un mécanisme de liens de sauvegarde. Le standard a été amélioré en incluant IEEE 802.1w Rapid Spanning Tree (RSTP). Cisco dispose de ses propres versions correspondantes a partir des interfaces. [8]

1.9 Les protocoles de niveau 3

1.9.1 Adressage IP

- **Définition d'une adresse IP**

Une adresse IP est une adresse de 32 bits, séparées en groupe de 4 octets par des points. Chaque octet peut donc aller de 0 à 255. On l'écrit d'habitude en décimal mais il est toujours codé en binaire. Chaque adresse IP est formée d'une partie réseau et d'une partie hôte. [10]

- **Les Classes des adresses IP**

Pour différencier différentes tailles de réseau et permettre de mieux identifier des adresses, on a séparé les adresses IP en 5 classes.

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 192 et 223.

Classe D :

C'est une classe utilisée pour le multicasting. 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.

1.9.2 Adresse privées :

Il existe des adresses privées, dans chaque classe :

A –> 10.0.0.0 à 10.255.255.255
B –> 172.16.0.0 à 172.31.255.255
C –>192.168.0.0 à 192.168.255.255

Une adresse IP privée n'est pas visible sur internet, au contraire d'une IP publique. On emploie les adresses privées à l'intérieur du réseau et les adresses publiques sont des adresses internet. En interne, il y aura donc un routeur qui va dire ou aller pour rejoindre une adresse publique. On peut accéder à une adresse publique depuis n'importe ou dans le monde alors qu'on ne pourra jamais arriver sur une adresse

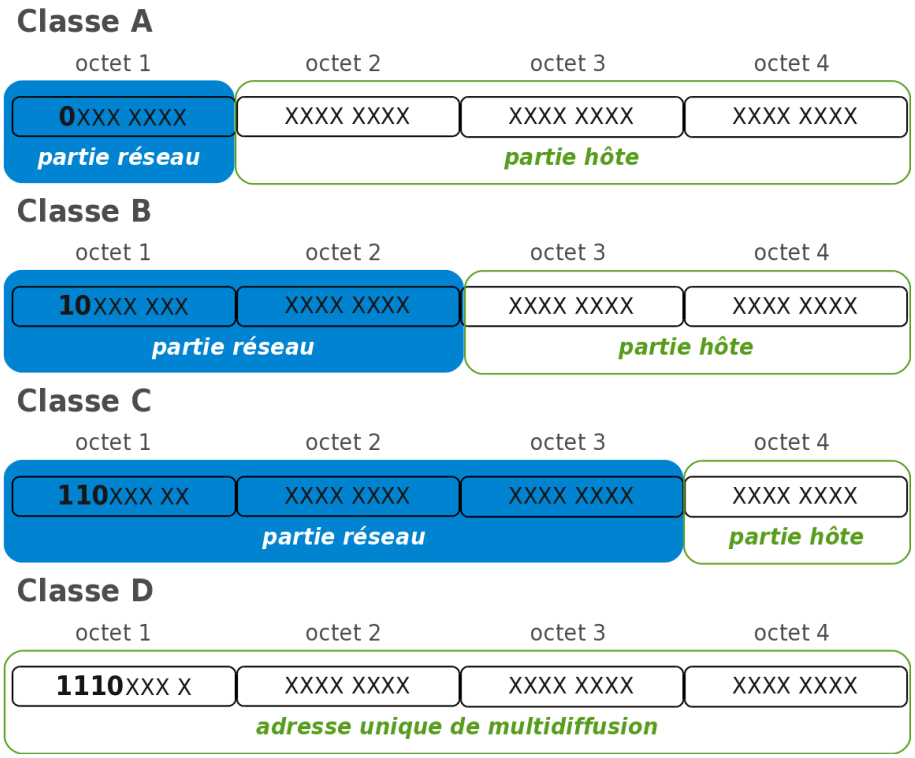

FIG. 1.4 – Les classes des adresses IP.

privée sans être dans le même réseau qu'elle ou à moins de réussir à pirater le réseau.

1.9.3 Adresse réseau et Broadcast

Certaines adresses sont réservées et ne peuvent être utilisés pour les hôtes. C'est le cas de l'adresse de Broadcast et de l'adresse réseau.

•Adresse réseau :

Cette adresse sert à identifier le réseau, chaque bit de la partie hôte de l'adresse est fait de 0. Par exemple pour une classe A, l'adresse réseau serait XXX.0.0.0 et pour une classe C ce serait XXX.XXX.XXX.0. On ne peut pas employer cette adresse pour un hôte, c'est donc une adresse de perdue.

•Adresse Broadcast :

Cette adresse est utilisée pour envoyer un message à toutes les machines d'un réseau. Chaque bit de la partie hôte de l'adresse est fait de 1. Par exemple pour une classe A, l'adresse réseau serait XXX.255.255.255 et pour une classe C ce serait

XXX.XXX.XXX.255. On ne peut pas employer cette adresse pour un hôte, c'est donc une autre adresse de perdue. Le routeur quand il va recevoir une adresse de Broadcast, va envoyer le message dans tous les périphériques du réseau concerné. On peut aussi utiliser l'adresse de Broadcast " générale ", c'est-à-dire envoyé un message à tous les périphériques de tous les réseaux connectés sur le même réseau que nous ; pour cela, il suffit d'employer l'adresse 255.255.255.255.

1.9.4 Le protocole ARP

L'ARP ou Address Resolution Protocol est un protocole qui se situe sur la couche 3 du modèle OSI. On l'assimile parfois à un protocole de couche 2 et demi car il assure la liaison entre le protocole IP qui utilise les adresses IP pour construire ses paquets et les trames Ethernet qui elles utilisent les adresse MAC. En plus simple, c'est un protocole qui permet de retrouver une adresse MAC à partir d'une adresse IP. [11]

1.9.5 ACL

Une Access Control List permet de filtrer les paquets IP, c'est à dire les paquets du niveau 3. Elle permet de définir les actions possibles des utilisateurs du réseau. Ainsi, une ACL va indiquer au routeur les paquets qu'il doit accepter et ceux qu'il doit refuser, notamment en fonction de leur adresse IP de provenance, leur IP destination et les ports source et destination. [12]

1.10 Serveur réseau

Un serveur réseau est un ordinateur spécifique partageant ses ressources avec d'autres ordinateurs appelés clients, même si en pratique, un serveur informatique peut exercer plusieurs fonctions en même temps.

1.10.1 Serveur DHCP

DHCP signifie Dynamic Host Configuration Protocol. Il s'agit d'un protocole qui permet à un ordinateur qui se connecte sur un réseau local d'obtenir dynamiquement et automatiquement sa configuration IP. Le but principal étant la simplification de l'administration d'un réseau. On voit généralement le protocole DHCP comme distribuant des adresses IP. [14]

Chaque ordinateur d'un réseau TCP/IP doit posséder une adresse IP unique. L'adresse IP (avec son masque de sous-réseau associé) identifie l'ordinateur hôte et le sous-réseau auquel il est associé .lors du déplacement d'un ordinateur vers un autre sous réseau, l'adresse IP doit être modifié. DHCP permet d'affecter d'une manière dynamique une adresse IP à un client a partir de la base de données d'une adresse IP du serveur DHCP sur le réseau local :

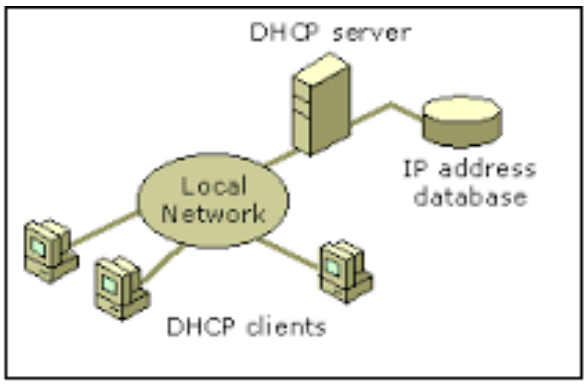

Fig. 1.5 – Fonctionnement de DHCP.

1.10.2 Serveur HTTP

Un serveur http est un logiciel implémentant le protocole http et ouvert aux connections provenant de l'extérieur.

Un serveur HTTP est, comme tout serveur, à l'écoute des connections en provenance de l'extérieur sur un port donné. Le port standard pour un serveur HTTP est le numéro 80. Le client d'un serveur HTTP est généralement le navigateur Internet comme Internet Explorer ou Mozilla Firefox.

A chaque requête qu'il reçoit le serveur présente à l'utilisateur la page demandée. Par exemple quand dans un navigateur internet un internaute saisit l'adresse http ://www.google.fr/, il envoie une requête au serveur HTTP de l'entreprise Google qui transfère des données (une page au format HTML) qui sont interprétées et affichées par votre navigateur.

Quand cela n'est pas précisé le port de connexion est toujours 80. Sur certains serveurs le port d'écoute n'est pas 80 mais par exemple 1234. Dans ce cas on accèdera au serveur par l'adresse suivante : http ://www.site.com :1234/.[15]

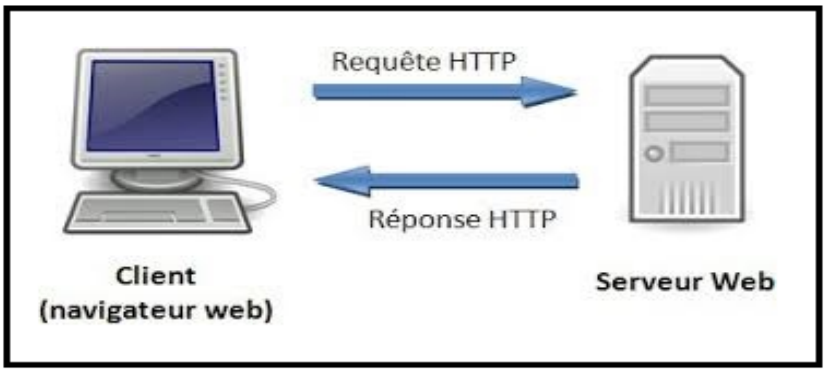

FIG. 1.6 – Serveur http.

1.10.3 Serveur DNS

DNS (Domain Name System) est un système d'appellation d'ordinateurs et de services réseau organisé selon une hiérarchie de domaines. Les réseaux TCP/IP tels qu'Internet utilisent DNS pour localiser des ordinateurs et des services par le biais de noms conviviaux.

Pour faciliter l'utilisation des ressources réseau, des systèmes de noms tels que DNS permettent d'établir une correspondance entre le nom convivial d'un ordinateur ou d'un service et d'autres informations associées à ce nom, comme une adresse IP. Un nom convivial est plus simple à retenir que les adresses numériques qui sont utilisées par les ordinateurs pour communiquer sur un réseau.

La plupart des utilisateurs préfèrent recourir à un nom convivial (par exemple, ventes.fabrikam.com) pour trouver un serveur de messagerie ou un serveur Web sur

un réseau, plutôt qu'à une adresse IP telle que 157.60.0.1. Lorsqu'un utilisateur entre un nom DNS convivial dans une application, les services DNS résolvent le nom en son adresse numérique. [16]

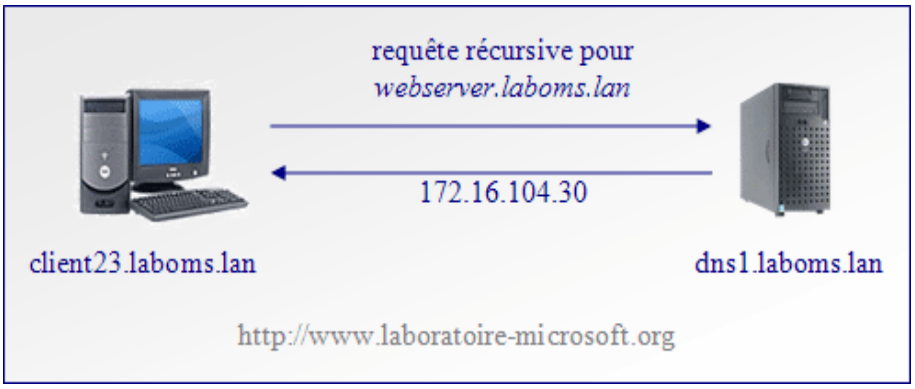

FIG. 1.7 – Serveur DNS.

1.10.4 Serveur FTP

Le protocole FTP (File Transfer Protocol) est, comme son nom l'indique, un protocole de transfert de fichier. [17]

Le protocole FTP définit la façon selon laquelle des données doivent être transférées sur un réseau TCP/IP.

Le protocole FTP a pour objectifs de :

- permettre un partage de fichiers entre machines
- permettre une indépendance aux systèmes de fichiers des machines clientes et serveur
- permettre de transférer des données de manière efficace

Le protocole FTP s'inscrit dans un modèle client-serveur, c'est-à-dire qu'une machine envoie des ordres (le client) et que l'autre attend des requêtes pour effectuer des actions (le serveur).

Lors d'une connexion FTP, deux canaux de transmission sont ouverts :

- Un canal pour les commandes (canal de contrôle).
- Un canal pour les données.

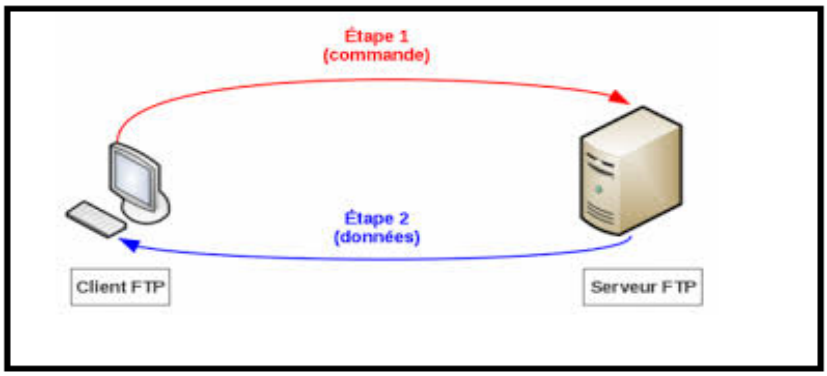

FIG. 1.8 – Serveur FTP.

1.11 Conclusion

Dans ce chapitre nous avons présenté, tout ce qui concerne les réseaux en général à savoir leurs objectifs, leurs classification ; et vu l'importance des modèles de communication nous avons pris le soin de présenter les plus utilisés d'entre eux, le modèle OSI et le modèle TCP/IP. Nous avons aussi défini les protocoles LAN ainsi que les différents protocoles de niveau 3.

Chapitre 2

Présentation de la Division Informatique

2.1 Introduction

Dans ce chapitre, nous présentons la division Informatique Hassi R'Mel SONATRACH, ensuite nous posons la problématique de ce type de reseau et la solution informatique proposée.

2.2 Présentation générale du champ de HASSI-R'MEL

A environ 530 kilomètres au sud d'Alger dans la wilaya de LAGHOUAT ce trouve le point d'eau Hassi R'mel à une altitude de 760M, que donne son nom a la ville de Hassi R'mel et au gisement de gaz découvert en 1951, ce dernier fait parti des plus grands gisements de gaz au monde. L'Algérie, possédant environ 10 % des réserves mondiales en gaz naturel, se place en cinquième rang international. Plus de 50 % de ces réserves connues sont concentrés dans le gisement de HASSI-R'MEL.

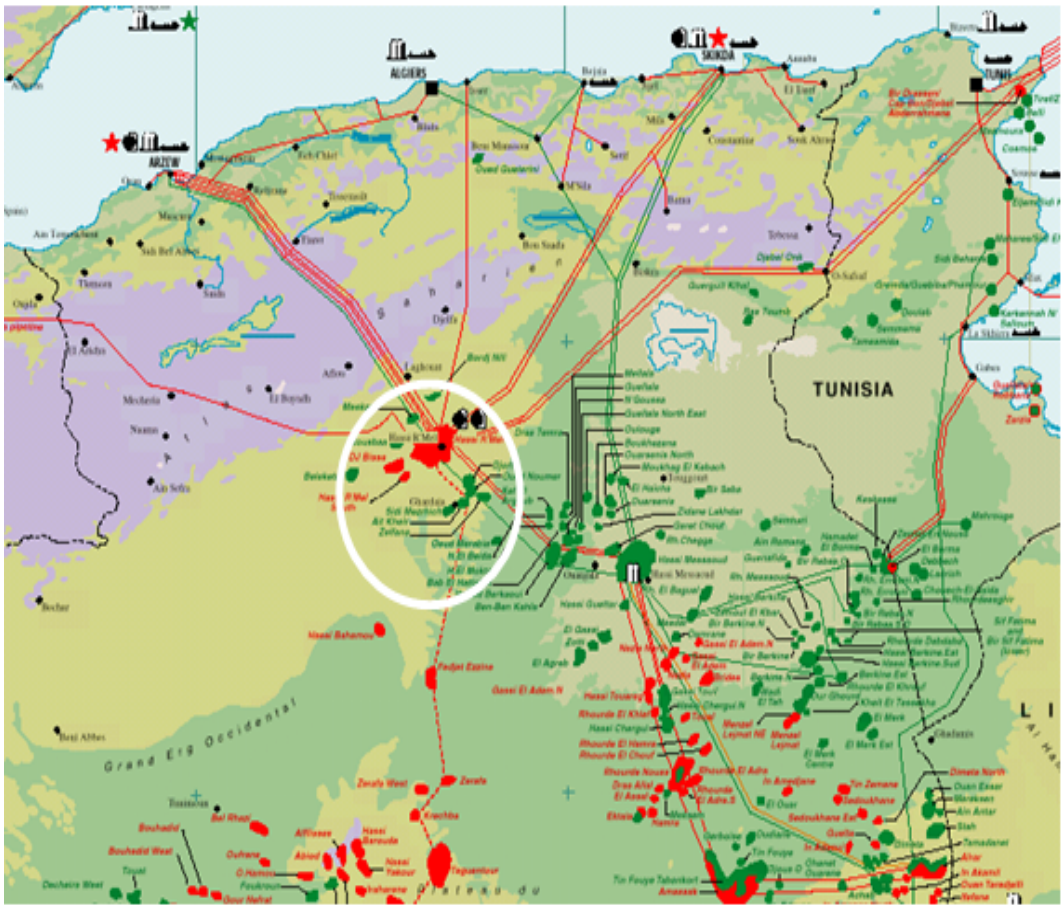

FIG. 2.1 – Les différentes stations liés a la base de Hassi R'mel.

2.2.1 Description générale

Le réservoir de gaz de HASSI-R'MEL se situe approximativement a 500 Km au sud d'Alger, à une altitude de 760 m.

Ce gisement s'étend sur une superficie de 3500 Km2 soit 70 Km environ dans la direction Nord-sud et 50 Km environ dans la direction Ouest.

Le climat est caractérisé par une fiable pluviométrie (140 mm / an) et une humidité moyenne de 19 % en été et 34 % en hiver. Les amplitudes thermiques sont importante et les températures varient entre -5c° et +45c°en été. Les vents dominants sont de direction Nord- Ouest.

2.2.2 Développement du champs de HRM

Le champs de HASSI-R'MEL est une vaste étendue, où sont réparties d'importantes installations, alimentées a partir de puits forés aux différents point du champs. Le premier puits HR1 a été foré en 1956, ce puits a mis en évidence la présence de gaz riche en condensât.

Le développement de HASSI-R'MEL s'est trouvé étroitement lié au développement de l'industrie du gaz dans le monde et les importantes réserves estimé à 32000 milliards m3 ont constitué un atout important pour lancer une politique d'industrie gazière grande envergure pour le pays.

Ce développement se traduit la construction et la mise en exploitation en1961 de la première unité de traitement de gaz appelé (Module 0) d'une capacité de 4 milliards m3 / ans de gaz sec.

Après la nationalisation des hydrocarbures en 1971 la capacité de cette unité fut porte à 4 milliards m3 / an par l'apport de la mise en service de nouvelles installations.

La période de 1975 à 1980 a permis de concrétiser un plant de développement qui concerne l'ensemble du champs de HASSI-R'MEL en mesure de répondre aux besoins énergétique du pays, à moyen et long terme ainsi qu'aux besoins de nos partenaires, ce plant a permis également de doter HASSI-R'MEL d'un modèle d'exploitation de différents produits.

Et maintenant la capacité de traitement a été portée à 94 milliards m3 / an par :

- La réalisation de quatre complexes de traitements de gaz.
- Le forage de plus de 150 puits producteurs.
- La réalisation de deux station de réinjection de gaz.
- Le forage de plus de 52 puits injecteurs.

2.3 Organisation de la région HASSI-R'MEL

2.3.1 Organigramme de la direction régionale

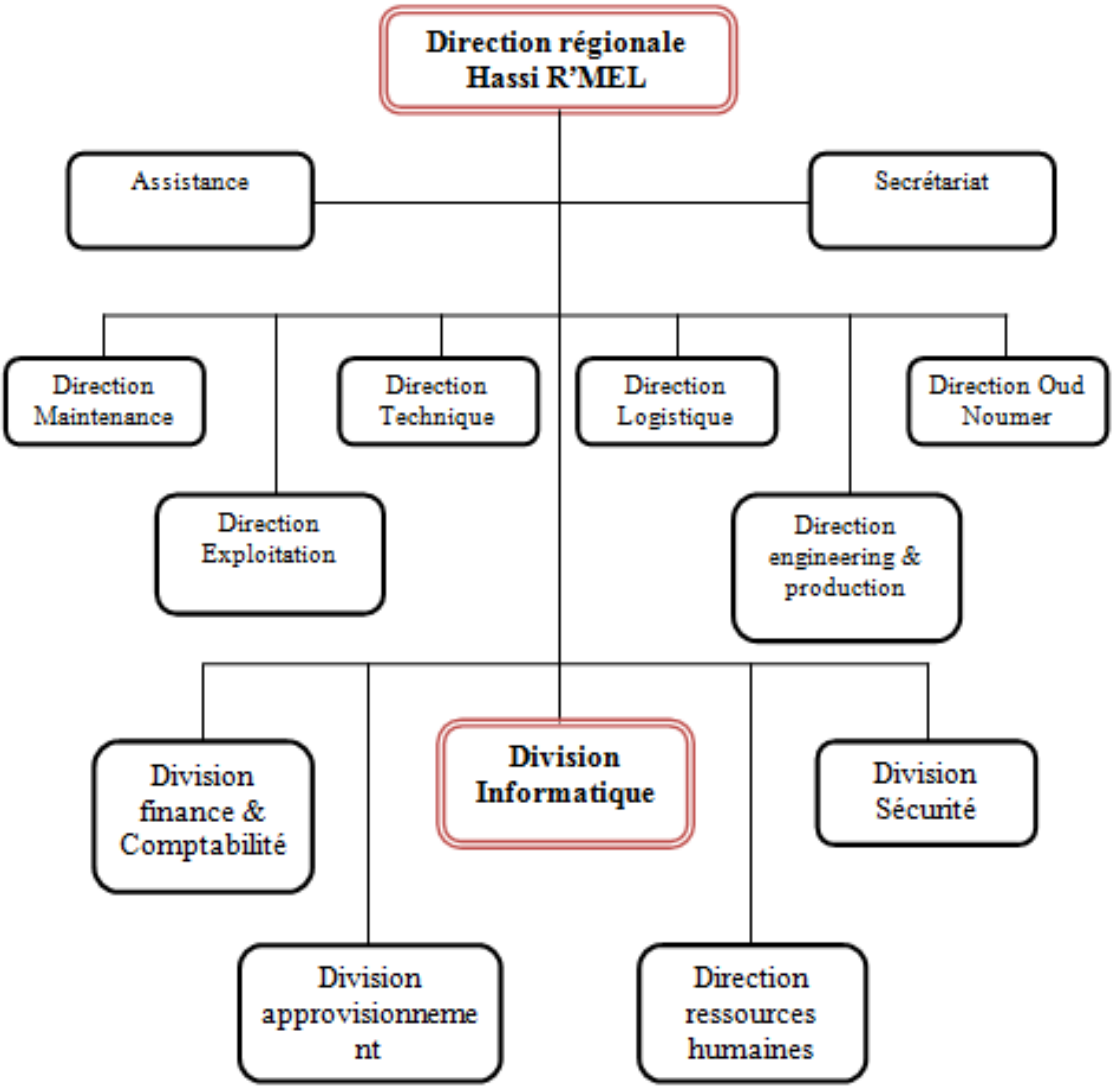

FIG. 2.2 – Organigramme de la direction régionale.

2.3.2 Présentation de la division informatique

Ce service à été crée en 1994, il fait parité de la division Production de l'activité amont. Elle a pour objectif la gestion, le développement et la maintenance de l'outil informatique dans toutes les régions. Il est composé des services suivants :

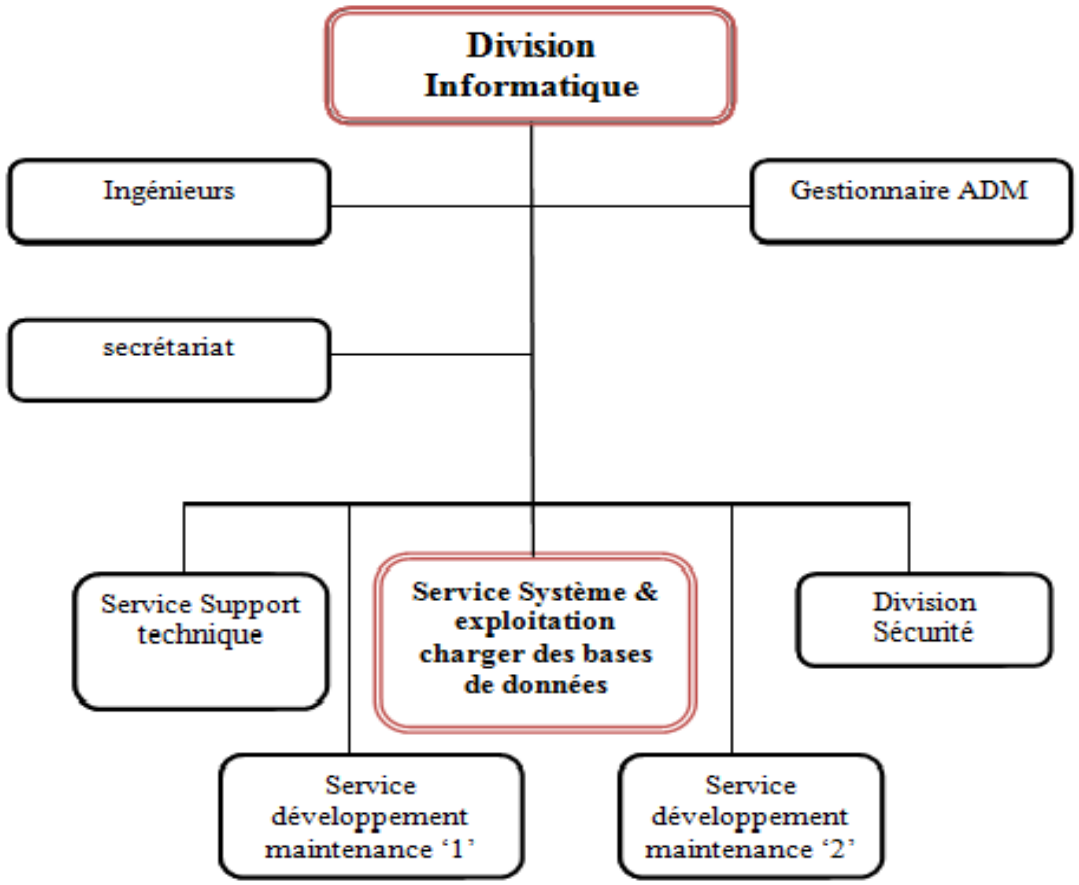

FIG. 2.3 – Organigramme de la division informatique.

2.3.3 Le rôle de la division informatique

Cette division est concernée par les tâches suivantes :

Cette division a pour rôle :

- Cœur de métier informatique, aux structures opérationnelles de la région de Hassi R'mel.
- La mise en place du système d'information de la région HR.
- Intégration des sous-systèmes par la réalisation des interfaces.
- Sécuriser le réseau et les systèmes informatiques.
- Exploiter correctement l'ensemble des systèmes.

- Exploiter à tous les niveaux l'intranet et la messagerie.

Service Développement et maintenance des applications 1 :

Il a pour principales tâches :

- Prise en charge des développements relatifs aux structures finances et approvisionnements
- Assistance aux régions et associations dans l'exploitation et la maintenance des progiciels de gestion financière intégrée (Système développé à Hassi R'mel).
- Généralisation du système GFAO (Gestion Financière assistée par ordinateur) aux régions et Siège de la DP (Division Production).

Service Développement et maintenance des applications 2 :

Il a pour principales tâches :

- Prise en charge du système d'information relatif aux activités : Ressources Humaines, Intendance, Logistique et Sécurité.
- Déploiement de RESHUM (Système de gestion intégrée des ressources humaines) aux régions et Siège DP.
- Assistance continue des utilisateurs dans l'exploitation des applications de gestion.

Service Systèmes Informatiques SCADA-DCS :

Il a pour principales tâches :

- Implémentation et Administration des Systèmes SCADA (système de télémétrie et collecte des données de puits à distance), DCS (Distributed Control System pour le contrôle et le suivi des process de production de Gaz).
- Assister les utilisateurs des Systèmes industriels.
- Maintenir les applications techniques de la direction exploitation : XP applications portail pour le Data management.

Service Systèmes et Exploitation chargé des bases de données :

Il a pour principales tâches :

- Le help desk des utilisateurs de la messagerie, l'intranet et des ressources informatiques de la région.
- L'administration des bases de données.
- Assurer la sécurité des systèmes et des réseaux.
- La gestion de la messagerie et le nom du domaine.

Service Support Technique :

Il a pour principales tâches :

- la prise en charge des besoins en matériels et consommables informatiques.
- Elaboration des budgets et cahiers des charges.
- Gestion de parc d'équipements informatiques de la région.

L'un des fondements de cette structure informatises est le réseau, ce dernier est un ensemble de machine (ordinateur) relier entre elles par un support physique.

L'entreprise, une structure que a un besoin réel en communication pour optimiser sa production, a vite compris l'intérêt d'un tel réseau a fin de pouvoir échanger des informations.

Voici un certain nombre de raisons pour lesquelles un réseau est utile :

- Le partage de fichiers, d'application ...
- La communication entre personnes (grâce au courrier électronique,...)
- La communication entre processus (entre des machines industrielles).
- La garantie de l'unicité de l'information (bases de données).

Les réseaux permettant aussi de standardiser les applications, on parle généralement de gropuware. Par exemple la messagerie électronique et les agendas de groupe qui permettent de communiquer plus efficacement et plus rapidement, voici les avan-

tages de tels systèmes :

- Diminution des coûts grâce aux partages des données et des périphériques.
- Standardisation des applications.
- Accès aux données en temps utile.
- Communication et organisation plus efficace.

2.4 Problème mis en compte :

Les réseaux informatiques sont de plus en plus répandus et complexes. L'implantation d'un Réseau complexe doit être sûr pour avoir des réseaux fiables. Ainsi pour une meilleure gestion et pour diminuer les risques de pannes, une conception intelligente s'impose.

2.5 Solutions proposées :

L'objectif de ce projet est la mise en place d'un modèle type de configuration d'un réseau dans le but de faciliter la préparation et la réalisation des projets de l'entreprise. Ce modèle est basé sur un réseau local, qui sera assuré par des protocoles.

C'est dans ce cadre que s'inscrit notre travail :

- **Tolérance aux pannes :**

Les pannes sont des éléments perturbateurs mettant en cause la sécurité des données qu'elles soient permanentes (dommage physique, erreur de conception du matériel ou du logiciel), transitoires (perturbation électriques, électromagnétiques ou de température), elles peuvent avoir de multiples causes.

Tout dispositif technique permettant de palier a ces différentes pannes sans interrompre la bonne marche du système peut être considérée comme tolérant les pannes. En pratique cela implique presque toujours une redondance du matériel, gérée par un dispositif soft ou hard et assurant la transition active de l'élément défectueux vers celui de réserve.

Autrement dit, le matériel est systématiquement remplacé par un autre aux fonctionnalités équivalentes.

• **Sécurité :**

Les problèmes liés a la sécurité, souvent très onéreux, peuvent être l'indisponibilité des serveurs, du réseau, les vols d'informations, des attaques. Les outils pour y remédier sont tellement disparates (un peu a tous les niveaux).de plus le protocole réseau IP qui n'assure aucune fiabilité ne rend pas cette tache facile.

Vue l'importance de la sécurité, il s'avère utile de coupler plusieurs outils et mécanismes pour au moins s'assurer une meilleur protection.

• **Qualité de service :**

Qui dit la qualité de service dit la capacité à véhiculer dans de bonnes conditions un type de trafic donné, en termes de débit, latence (délai de transmission), taux de perte de paquets, gigue (variation de la latence).

Ce problème ne se pose pas quand la bande passante est a profusion, c'est le cas généralement des LAN. La difficulté augmente avec la présence d'un ou de plusieurs opérateurs. L'utilisation des mécanismes tels que Diffserv(classification du trafic) ou RSVP (réservation de ressources)serait autant de solution pour pallier aux problème de QoS.

2.6 Conclusion

Pour la réalisation de notre projet, nous nous sommes basés sur les besoins de l'entreprise, et cela nous a aidé à définir une problématique, pour présenter ensuite des solutions a leurs besoins. Nous avons par la suite proposé quelques solutions afin de remédier à cette problématique.

Chapitre 3

Conception

3.1 Introduction

La conception d'un réseau constitue un défi important, qui va bien au-delà de la simple interconnexion des ordinateurs. Pour être fiable, évolutif et facile à gérer, un réseau doit posséder un grand nombre de caractéristiques évoluées.

Afin de concevoir des réseaux fiables, gérables et évolutifs, les concepteurs doivent connaître les caractéristiques particulières des principaux composants.

Dans se présent chapitre, nous allons définir Le modèle hiérarchique, ainsi que toutes ses composantes dans le but de faciliter la réalisation de ce dernier.

3.2 Identification et choix d'un modèle de conception de réseau

Les modèles de conception hiérarchiques autorisent une organisation des réseaux en couches. Pour mieux saisir l'importance de ce concept, prenons l'exemple du modèle de référence OSI (Open System Interconnection, interconnexion de systèmes ouverts), qui sert à comprendre et à implémenter la communication entre ordinateurs. L'utilisation de couches lui permet de simplifier les tâches requises entre deux ordinateurs pour communiquer.

Les modèles hiérarchiques font également appel à ce concept afin de faciliter la

mise en œuvre de réseaux. Chaque couche peut être dédiée à des fonctions spécifiques, autorisant de ce fait le concepteur à choisir les systèmes et les fonctionnalités appropriés pour chacune d'elles.

Une conception hiérarchique facilite également les modifications dans un réseau. Le principe de modularité permet de créer des éléments qui peuvent être reproduits au fur et à mesure que le réseau se développe. Lorsqu'un élément doit être mis à jour, le coût et la complexité associés ne portent alors que sur une petite portion du réseau.

Au sein des architectures linéaires ou fortement maillées, les modifications ont tendance à affecter un grand nombre de systèmes. Avec une structuration modulaire en petits éléments de réseau, plus faciles à maîtriser, les incidents sont également plus faciles à localiser et à isoler.
Les administrateurs sont à même d'identifier les points de transition du réseau, ce qui les aide à identifier les pannes. [A]

3.3 Modèle de conception hiérarchique

Une conception hiérarchique implique la présence des trois couches suivantes :

- L'épine dorsale, appelée aussi réseau fédérateur, qui représente la couche centrale assurant le transport optimal des données entre les sites.
- la couche de distribution, qui fournit une connectivité basée sur des règles.
- la couche d'accès local, qui offre aux groupes de travail et aux utilisateurs individuels un accès au réseau.

La Figure 3.1 est une représentation d'ensemble qui montre les diverses facettes d'un réseau hiérarchique. Chaque couche (centrale, distribution et accès) offre des fonctionnalités différentes.

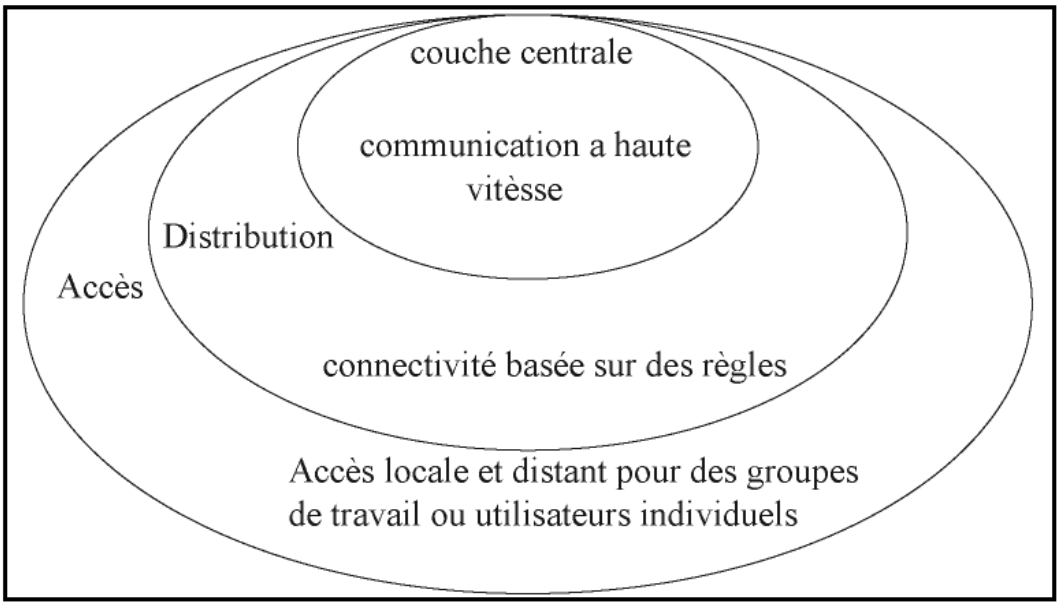

FIG. 3.1 – Modèle de conception de réseau hiérarchique.

3.3.1 Fonctions de la couche centrale

Cette couche est un réseau fédérateur de commutation à haute vitesse qui devrait être conçu pour commuter les paquets le plus rapidement possible. Elle n'est censée opérer aucune manipulation des paquets, telle que les listes d'accès ou le filtrage, afin de ne pas ralentir leur commutation.

3.3.2 Fonctions de la couche de distribution

Cette couche représente la frontière entre la couche d'accès et la couche centrale, et aide à déterminer les caractéristiques distinctives de cette dernière. Son objectif est d'offrir une définition des limites. La manipulation des paquets a lieu à ce niveau.

Dans un environnement de réseau de campus, cette couche peut assurer plusieurs fonctions :

- regroupement d'adresses ou de zones.
- accès au réseau pour les départements ou groupes de travail .
- définition de domaines de broadcast (diffusion générale) ou multicast (diffusion restreinte).
- routage sur des réseaux locaux virtuels ou VLAN (Virtual Local Area Network).
- toute transition de médias nécessaire.

- sécurité.

Dans les autres environnements, cette couche peut faire office de point de redistribution entre des domaines de routage, ou bien de frontière entre des protocoles de routage statique ou dynamique. Les sites distants peuvent également s'en servir de point d'accès au réseau d'entreprise. Sa principale fonctionnalité est d'offrir une connectivité basée sur des règles.

3.3.3 Fonctions de la couche d'accès

Cette couche représente le point d'accès local au réseau pour les utilisateurs finaux. Elle utilise parfois des listes d'accès ou des filtres afin de mieux servir les besoins d'un ensemble d'utilisateurs donné. Dans un environnement de réseau de campus, elle offre les fonctions suivantes :

- bande passante partagée.
- bande passante commutée.
- filtrage au niveau de la couche MAC.
- micro segmentation.

Dans les autres environnements, cette couche peut autoriser des sites distants à accéder au réseau d'entreprise par le biais de certaines technologies longue distance, comme le Frame Relay (relais de trames), RNIS ou des lignes louées.

Certains pensent parfois que ces trois couches (centrale, distribution et accès) existent en tant qu'entités physiques clairement définies, ce qui n'est pas le cas. Elles ont été définies pour aider à la conception de réseaux et représenter les fonctionnalités qui doivent être implémentées.

L'instanciation de chaque couche peut se faire au niveau de routeurs ou de commutateurs distincts, être représentée par un média physique, combinée en un seul équipement, ou encore être complètement omise. La façon dont ces couches sont mises en œuvre dépend des besoins du réseau en cours de conception. Il faut noter toutefois que la structure hiérarchique doit être préservée pour que le fonctionnement du réseau soit optimal.

3.4 Présentation de l'architecture réseau

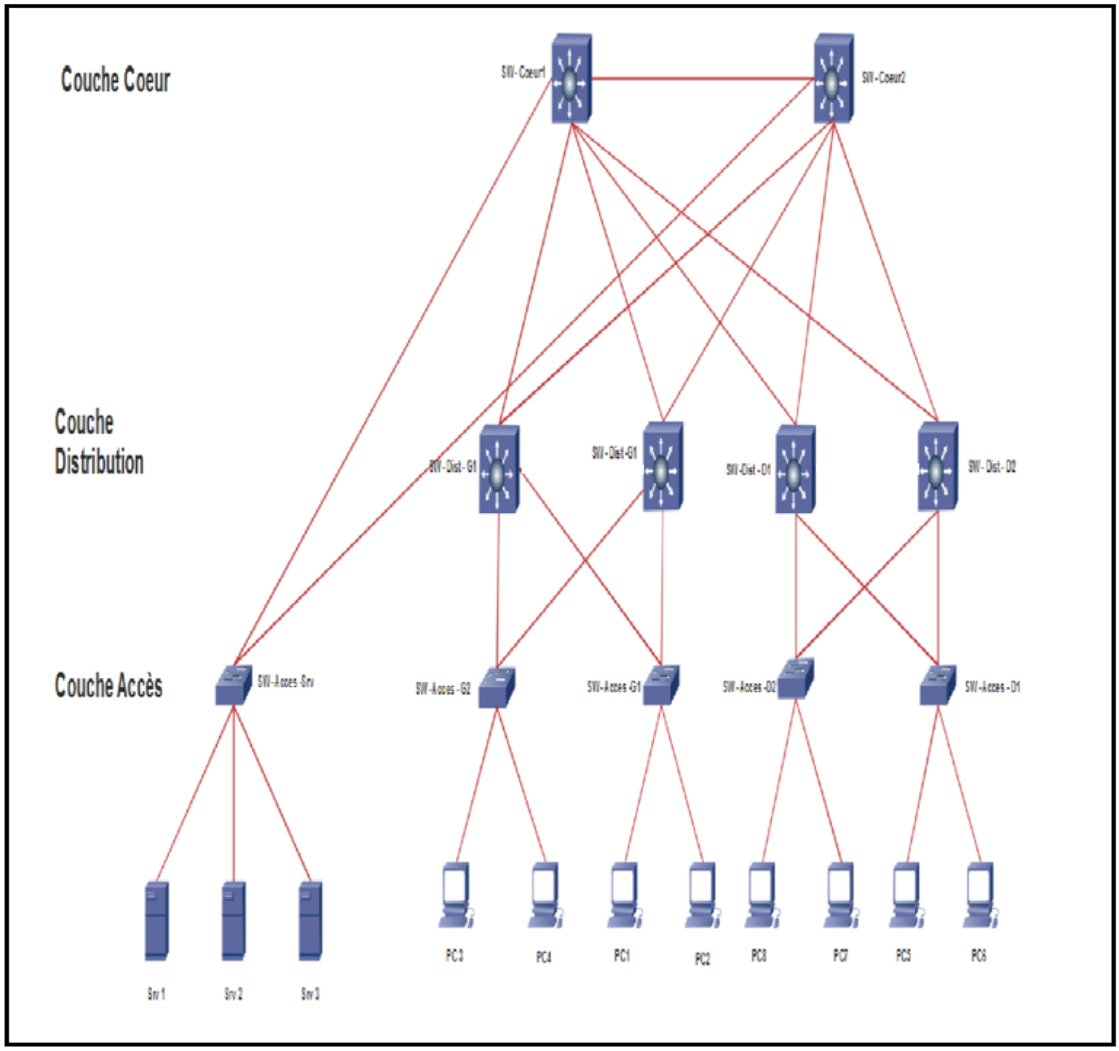

FIG. 3.2 – Le modèle hiérarchique du réseau LAN

Le modèle hiérarchique est composé par les modules suivant :

- Deux switchs cœur de réseau.
- Des switchs de distribution et des switchs d'accès, Pour assurer la disponibilité et la continuité de fonction, chaque switch cœur est liée avec tous les switchs de distribution (ex : SW-Coeur1 est liée avec SW-Dist-G1, SW-Dist-G2, SW-Dist-D1, SW-Dist-D2). De même chaque switch de distribution est liée aux deux switchs d'accès (ex : SW-Dist-G-1 est liée aux SW-Access-G-1 et SW-Access-G-2).

3.5 Présentation des équipements utilisés

Pour l'implémentation de notre projet nous avons utilisé les équipements suivants :

Périphériques utilisés	**Appellation**
Commutateur Coeur	Cisco Catalyst 3560
Commutateur Distribution	Cisco Catalyst 2950
Commutateur Accés	Cisco Catalyst 2950
Serveur	DNS,HTTP,FTP
Terminal (PC)	PC Bureau

TAB. 3.1 – Liste des équipements utilisés.

3.6 Nomination des équipements et désignations des interfaces

3.6.1 Nominations des équipements :

Dans le but de faciliter la conception de notre projet , nous avons nommé les équipements par des nom significatifs . Le tableaux ci-dessous indiquent les noms des équipements :

Couche Coeur	**Couche Distribution**	**Couche Accés**	**Serveurs**	**Terminales(PCs)**
SW-Coeur1	SW-Dist-G1	SW-Acces-G1	Srv1	Gauche(PC1,PC2,
SW-Coeur2	SW-Dist-G2	SW-Acces-G2	Srv2	PC3,PC4)
	SW-Dist-D1	SW-Acces-D1	Srv3	Droite(PC5,PC6,
	SW-Dist-D2	SW-Acces-D2		PC7,PC8)

TAB. 3.2 – Nom des équipements du réseau.

3.6.2 Désignations des interfaces

Les interfaces sur les équipements seront comme indique le tableau ci dessous :

Local Device	Remote Device	Local Interface	Remote Interface
SW-Coeur1	SW-Coeur2	FA0/4	FA0/4
SW-Coeur1	SW-Dist-G2	FA0/2	FA0/1
SW-Coeur1	SW-Dist-G1	FA0/3	FA0/1
SW-Coeur1	SW-Dist-D1	FA0/6	FA0/4
SW-Coeur1	SW-Dist-D2	FA0/5	FA0/4
SW-Coeur1	SW-Acces-Srv	FA0/7	FA0/1
SW-Coeur2	SW-Coeur1	FA0/4	FA0/4
SW-Coeur2	SW-Dist-G2	FA0/6	FA0/4
SW-Coeur2	SW-Dist-G1	FA0/5	FA0/4
SW-Coeur2	SW-Dist-D1	FA0/2	FA0/1
SW-Coeur2	SW-Dist-D2	FA0/1	FA0/1
SW-Coeur2	SW-Acces-serv	FA0/3	FA0/5
SW-Dist-G1	SW-Dist-G2	FA0/5	FA0/5
SW-Dist-G1	SW-Acces-G1	FA0/3	FA0/2
SW-Dist-G1	SW-Acces-G2	FA0/2	FA0/2
SW-Dist-G1	SW-Coeur1	FA0/1	FA0/3
SW-Dist-G1	SW-Coeur2	FA0/4	FA0/5
SW-Dist-G2	SW-Dist-G1	FA0/5	FA0/5
SW-Dist-G2	SW-Acces-G1	FA0/3	FA0/1
SW-Dist-G2	SW-Acces-G2	FA0/2	FA0/1
SW-Dist-G2	SW-Coeur1	FA0/1	FA0/2
SW-Dist-G2	SW-Coeur2	FA0/4	FA0/6
SW-Dist-G1	SW-Dist-D2	FA0/5	FA0/5
SW-Dist-D1	SW-Acces-D1	FA0/3	FA0/1
SW-Dist-D1	SW-Acces-D2	FA0/2	FA0/1
SW-Dist-D1	SW-Coeur1	FA0/4	FA0/6
SW-Dist-D1	SW-Coeur2	FA0/1	FA0/2
SW-Dist-D2	SW-Dist-D1	FA0/5	FA0/5
SW-Dist-D2	SW-Acces-D1	FA0/3	FA0/2
SW-Dist-D2	SW-acces-D2	FA0/2	FA0/2
SW-Dist-D2	SW-Coeur1	FA0/4	FA0/5
SW-Dist-D2	SW-Coeur2	FA0/1	FA0/1
SW-Acces-D1	SW-Dist-D1	FA0/1	FA0/3
SW-Acces-D1	SW-Dist-D2	FA0/2	FA0/3
SW-Acces-D1	PC5	FA0/3	FA0
SW-Acces-D1	PC6	FA0/4	FA0
SW-Acces-D2	SW-Dist-D1	FA0/2	FA0/2
SW-Acces-D2	SW-Dist-D2	FA0/1	FA0/2
SW-Acces-D2	PC7	FA0/3	FA0
SW-Acces-D2	PC8	FA0/4	FA0
SW-Acces-G2	SW-Dist-G1	FA0/2	FA0/3
SW-Acces-G1	SW-Dist-G2	FA0/1	FA0/3
SW-Acces-G1	PC1	FA0/3	FA0
SW-Acces-G1	PC2	FA0/4	FA0
SW-Acces-G2	SW-Dist-G1	FA0/2	FA0/2
SW-Acces-G2	SW-Dist-G2	FA0/1	FA0/2
SW-Acces-G2	PC3	FA0/3	FA0
SW-Acces-G2	PC4	FA0/4	FA0
SW-Acces-Srv	SW-Coeur1	FA0/1	FA0/7
SW-Acces-Srv	Srv1	FA0/2	FA0
SW-Acces-Srv	Srv2	FA0/3	FA0
SW-Acces-Srv	Srv3	FA0/4	FA0

TAB. 3.3 – Désignation des interfaces.

3.7 Les VlANs

Avant l'apparition des technologies de réseaux virtuels, l'architecture logique du réseau était fortement dépendante de l'architecture physique.

Les VLANs permettent de rassemblé dans un même réseau de niveau 2 du modèle OSI (généralement Ethernet) l'ensemble des matériels ayant une corrélation fonctionnelle (même service, même fonctionnalité, etc), ou ayant une nécessité de communiquer entre eux, et ceci, indépendamment du placement physique des matériels. [19]

3.7.1 Les avantages des VLANs

les avantages des VLANs sont les suivants :

- 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 limités aux clients de ce serveur.
- La création de groupes de travail indépendants de l'infrastructure physique ; possibilité de déplacer la station sans changer de réseau virtuel.
- L'augmentation de la sécurité par le contrôle des échanges inter-VLAN (filtrage possible du trafic échangé entre les VLANs).

L'indépendance entre infrastructure physique et groupe de travail implique qu'un commutateur puisse gérer plusieurs VLAN et qu'un même VLANn puisse être réparti sur plusieurs commutateurs. En conséquence, une trame qui circule dans un commutateur et entre les commutateurs doit pouvoir être associée à un VLAN.

Pour répondre aux objectifs des VLAN la règle suivante doit être impérativement respectée : une trame doit être associée à un VLAN et un seul et ne peut pas sortir du VLAN, sinon l'étanchéité du niveau 2 n'est plus respectée. [20]

3.7.2 Les méthodes de construction d'un VLAN

- **VLAN par port**

Un VLAN par port, aussi appelé VLAN de niveau 1 (pour physique), est obtenu en associant chaque port du commutateur avec un VLAN particulier. C'est une solution simple, qui a été rapidement mise en œuvre par les constructeurs. Les premiers VLAN ne permettaient pas de créer un même réseau sur plusieurs commutateurs. [21]

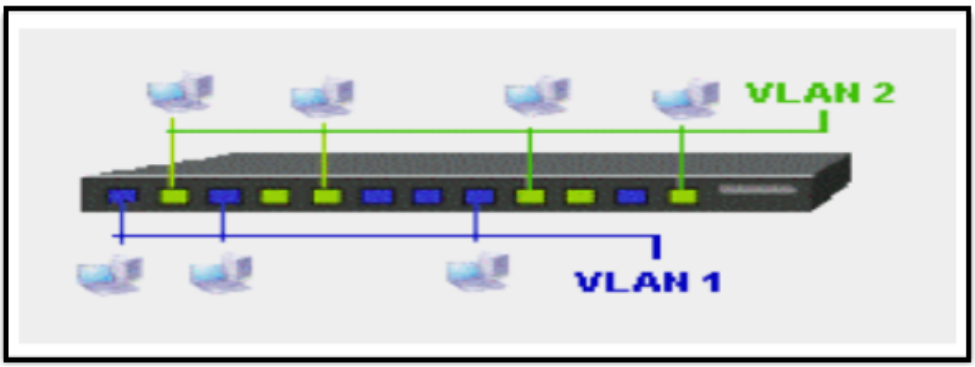

FIG. 3.3 – Les VLANs par port.

Depuis une nouvelle génération de commutateurs permet de le réaliser, grâce à l'échange d'informations entre les commutateurs et au marquage des trames.

Les VLAN 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 même concentrateur, appartiennent au même VLAN.

- **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 de la localisation. La station peut être déplacée, son adresse physique ne changeant pas, il est inutile de reconfigurer le VLAN.

Les VLAN configurables avec l'adresse MAC sont bien adaptes à l'utilisation de stations portables. La configuration peut s'avérer fastidieuse car elle nécessite de renseigner une table de correspondance avec toutes les adresses MAC et elle doit être partagée par tous les commutateurs.

- **VLAN par protocole**

également appelé VLAN de niveau 3, un VLAN par sous réseau utilise les adresses IP. Un réseau virtuel est associé à chaque sous réseau IP. Dans ce cas, les commuta-

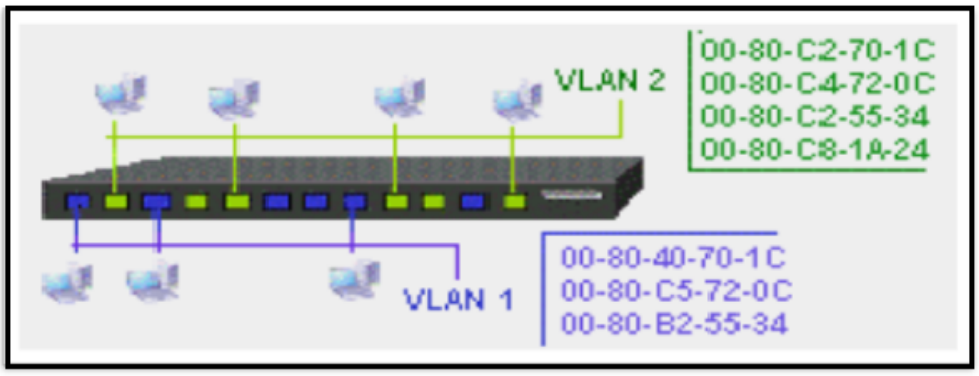

FIG. 3.4 – VLANs par adresse.

teurs apprennent la configuration et il est possible de changer une station de place sans reconfigurer le VLAN.

Cette solution est l'une des plus intéressantes, malgré une petite dégradation des performances de la commutation due a l'analyse des informations.

3.7.3 Nomination des VLANs

Les noms et identificateurs des VLANs à implémenter serons répartis comme suit :

Nom VLAN	**ID VLAN**	**Adresse de sous réseau**	**Description**
VLAN-Mgmt	9	192.168.9.0/24	VLAN pour Management des equipements
VLAN-Finance	10	172.16.10.0/24	VLAN des postes de travail de la direction des Finances
VLAN-Commercial	11	172.16.11.0/24	VLAN des postes de travail de la direction Commerciale
VLAN-Juridique	20	172.16.20.0/24	VLAN des postes de travail de la direction Juridique
VLAN-Technique	21	172.16.21.0/24	VLAN des postes de travail de la direction Technique
VLAN-Srv1	30	172.16.30.0/24	Vlan de Serveur HTTP
VLAN-Srv2	40	172.16.40.0/24	Vlan de Serveur DNS
VLAN-Srv3	50	172.16.50.0/24	Vlan de Serveur FTP

Tab. 3.4 – Nom des VLANs.

3.8 Le VTP (VLAN Trunking Protocol)

VTP règle le problème de la configuration manuelle des VLANs. en effet, si le réseau a une taille considérable, la déclaration de tous les VLANs crées dans tous les commutateurs sera vraiment très difficile a réaliser, et cela est pareil lors de l'ajout d'un nouveau VLAN ou lors de la modification. Donc la mise a jour des VLANs d'un façon manuelle est très difficile. Le protocole VTP, autorise les changements centralisés (ajout, modification et suppression) qui seront communiqués par les VTP-SERVER a tous les autres commutateurs VTP-CLIENT du réseau .VTP permet d'éviter toute incohérence de configuration des VLANs.[22]

Durant la phase de déploiement, nous allons configurer le Switch cœur (SW-Coeur1) en tant que VTP Server alors que les autres switches seront des VTP Client.

Le tableau ci-dessous montre comment le VTP sera configuré :

VTP	**NAME**	**MODE**
SW-coeur1	RTC	Server
SW-coeur2	RTC	Client
tous les autres switchs	RTC	Client

Tab. 3.5 – Le VTP.

3.9 Spanning-Tree Protocol

Dans ce projet nous avons utilisé le Rapid-SpanningTree par Vlan qui représente une version avancée du SpanningTree. Ce mode doit être activé sur tous les switchs du réseau.

3.10 Classification des PC's et Serveurs selon les VLANs

Les interfaces entre tous les switchs d'accès, distribution, cœur seront configures en mode trunk pour qu'elles puissent transporter les informations des différents Vlans. Les interfaces qui seront connectés à des posts de travail seront configurées en mode accès.

La liste illustrée dans le tableau 3.6 ci-dessous présente les VLANs et les adresses IP employées dans le modèle type :

Nom d'Hote N°	**Port de Switch**	**VLAN ID**	**Adresse IP**	**passerelle**
PC1	Port 1 SW-Access-G1	10	172.16.10.1/24	172.16.10.254
PC2	Port 2 SW-Access-G1	11	172.16.11.1/24	172.16.11.254
PC3	Port 3 SW-Access-G2	10	172.16.10.2/24	172.16.10.254
PC4	Port 4 SW-Access-G2	11	172.16.11.2/24	172.16.11.254
PC5	Port 5 SW-Access-D1	21	172.16.21.2/24	172.16.21.254
PC6	Port 6 SW-Access-D1	20	172.16.20.2/24	172.16.20.254
PC7	Port 7 SW-Access-D2	21	172.16.21.1/24	172.16.21.254
PC8	Port 8 SW-Access-D2	20	172.16.20.1/24	172.16.20.254
Srv1	Port 1 SW-Access-Srv	30	172.16.30.1/24	172.16.30.254
Srv2	Port 2 SW-Access-Srv	40	172.16.40.1/24	172.16.40.254
Srv3	Port 2 SW-Access-Srv	50	172.16.50.1/24	172.16.50.254

Tab. 3.6 – VLANs et adressage des PCs et Serveurs.

3.11 Administration des équipements

Le VLAN de management "VLAN 9" sera utilisé pour l'administration des équipements.
Les adresses IP de management seront attribuées aux équipements modèles comme suit :

Nom d'équipement	VLAN-ID	Adresse IP VLAN
SW-Coeur 1	9	192.168.9.1/24
SW-Coeur 2	9	192.168.9.2/24
SW-Dist-D-1	9	192.168.9.6/24
SW-Dist-D-2	9	192.168.9.7/24
SW-Dist-G-1	9	192.168.9.5/24
SW-Dist-G-2	9	192.168.9.4/24
SW-Access-D-1	9	192.168.9.11/24
SW-Access-D-2	9	192.168.9.9/24
SW-Access-G-1	9	192.168.9.10/24
SW-Access-G-2	9	192.168.9.8/24
SW-Access-SRV	9	192.168.9.3/24

Tab. 3.7 – Plan d'adressage du VLAN management.

3.12 Politique de sécurité

3.12.1 Généralités

Avec le développement de l'utilisation d'internet, de plus en plus d'entreprises et des écoles ouvrent leur système d'information (ensemble des moyens dont le fonctionnement fait appel, d'une façon ou d'une autre, à l'électricité et destinés à élaborer, traiter, stocker, acheminer et ou présenter) à des utilisateurs externes (partenaires, fournisseurs, membres de l'administration) au réseau local, il est donc essentiel de connaître les ressources de l'entreprise à protéger et de maîtriser le contrôle d'accès et les droits des utilisateurs du système d'information. Il en va de même lors de l'ouverture de l'accès de l'entreprise sur Internet. [23]

Le système d'information représente un patrimoine essentiel de l'entreprise, qu'il convient de protéger. La sécurité informatique, d'une vue générale, consiste à assurer que les ressources matérielles ou logicielles d'une organisation soient uniquement utilisées dans le cadre prévu. La sécurité vise généralement cinq objectifs :

- L'intégrité, autrement dit garantir que les données sont bien celles que l'on croit être
- La confidentialité, consistant à assurer que les seules personnes autorisées aient accès aux ressources qu'il s échangent

- La disponibilité, permettant de maintenir le bon fonctionnement du système d'information pour assurer un accès permanant
- La non répudiation, assurant la garantie qu'aucune transaction ne peut être niée
- L'authentification, visant la vérification de l'identité des acteurs de la communication.

3.12.2 Vulnérabilité et les attaques

Avec la libre circulation des informations et la haute disponibilité de nombreuses ressources, les responsables doivent connaître toutes les menaces successibles de compromettre la sécurité du fait de la vulnérabilité de leur réseau.

Toute faiblesse dans un SI qui permet à un attaquant de porter atteinte à l'intégrité de ce système, c'est-à-dire à son fonctionnement normal, à la confidentialité et l'intégrité des données qu'il contient est appelée une vulnérabilité.
Au fil des années, la sécurité des SI devient un besoin absolue, alors même que la complexité de ces systèmes s'accroît, ils deviennent donc plus vulnérables aux menaces.

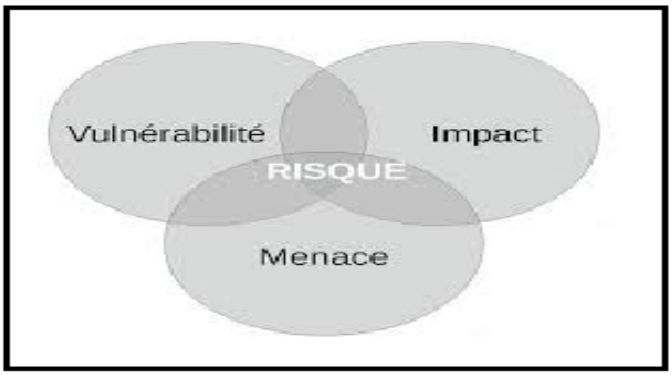

FIG. 3.5 – Evolution du risque en fonction de la vulnérabilité et de la menace.

Cependant les organisations sont peu ou presque pas protégées contre des attaques sur le réseau. Des raisons démontrent pourtant bien cet état de vulnérabilité des systèmes :

- La sécurité est onéreuse, les entreprises n'ont pas souvent de budget attribué à ce domaine, soulignant en parallèle la raison selon laquelle la sécurité ne peut être fiable à 100
- Les organisations attribue un degré de priorité minime ou presque qu'inexistant à la sécurité
- L'utilisation de la cryptographie qui a ses faiblesses, avec des mots de passe pouvant être cassés
- L'attaque d'un système fiable par des personnes abusant de leurs droits légitimes
- Faiblesses dues à la gestion et à la configuration des systèmes
- Emergence de nouvelles technologies, et par là même, de nouveaux points d'attaques.

Les attaques (n'importe quelles actions qui compromettent la sécurité des informations) informatiques constituent aujourd'hui l'un des fléaux de notre civilisation moderne. Il est régulier de suivre que telle entreprise ou tel institut a essuyé de lourdes pertes financières en raison d'une défaillance de la sécurité de son système d'information.

Par conséquent les entreprises ne peuvent pas ignorer ces risques et se croire à l'abri de telles épreuves sachant que les attaques ont des buts précis qui visent des mécanismes de sécurité précis très souvent implémentés dans les réseaux :

- Interruption d'un service : vise la disponibilité des informations.
- Interception des données : vise la confidentialité des informations.
- Modification des données : vise l'intégrité des informations.
- Fabrication des données : vise l'authenticité des informations.

3.12.3 Solution aux problemes de la sécurité

La sécurité des SI fait très souvent l'objet de métaphores. L'on la compare régulièrement à une chaine en expliquant que le niveau de sécurité d'un système est caractérisé par le niveau de sécurité du maillon le plus faible.

Ainsi, une porte blindée est inutile dans un bâtiment si les fenêtres sont ouvertes sur la rue. Cela signifie qu'une solution de sécurité doit être abordée dans un contexte

global et notamment prendre en compte les aspects suivants :

- La sensibilisation des utilisateurs aux problèmes de sécurité.
- La sécurité logique, c'est-à-dire la sécurité au niveau des données, notamment les données de l'entreprise, les applications ou encore les systèmes d'exploitation.
- La sécurité des télécommunications : technologies réseaux, serveurs de l'entreprise, réseaux d'accès, etc.
- La sécurité physique, soit la sécurité au niveau des infrastructures matérielles : salles sécurisées, lieux ouverts au public, espaces communs de l'entreprise, stations de travail des personnels, etc.

Etant donné les enjeux financiers qu'abritent les attaques, les SI se doivent de nos jours d'être protégés contre les anomalies de fonctionnement pouvant provenir soit d'une attitude intentionnellement malveillante d'un utilisateur, soit d'une faille rendant le système vulnérable.

Du fait du nombre croissant de personnes ayant accès ces systèmes par le billet d'Internet, la politique de sécurité se concentre généralement sur le point d'entrée du réseau interne.

La mise en place d'un pare-feu est devenue indispensable à fin d'interdire l'accès aux paquets indésirables. On peut, de cette façon, proposer une vision restreinte du réseau interne vu de l'extérieur et filtrer les paquets en fonction de certaines caractéristiques telles qu'une adresse ou un port de communication. Bien que ce système soit une bastille, il demeure insuffisant s'il n'est pas accompagné d'autres protections, entre autres :

- La protection physique des informations par des accès contrôlés aux locaux.
- La protection contre les failles de configuration par des outils d'analyse automatique des vulnérabilités du système.
- La protection par des systèmes d'authentification fiables pour que les droits accordés à chacun soient clairement définis et respectés, ceci afin de garantir la confidentialité et l'intégrité des données.

Implémenter la sécurité sur les SI, consiste à s'assurer que celui qui modifie ou

consulte des données du système en a l'autorisation et qu'il peut le faire correctement car le service est disponible.

Toujours est il que même en mettant en place tous ces mécanismes, il reste beaucoup de moyens pour contourner ces protections. A fin de les compléter, une surveillance permanente ou régulière des systèmes peut être mise en place à savoir :

- Les systèmes de détections d'intrusions ayant pour but d'analyser tout ou partit des actions effectuées sur le système afin de détecter d'éventuelles anomalies de fonctionnement.
- L'utilisation des antivirus professionnels accompagnées de leurs mises à jour régulière.
- L'utilisation d'un serveur proxy dont le but est d'isoler une ou plusieurs machines pour les protéger. De plus le proxy possède un avantage supplémentaire en termes de performance.
- L'utilisation de la technologie RAID qui signifie " ensemble redondant de disques indépendants " qui permet de constituer une unité de stockage à partir de plusieurs disques et d'y effectuer des sauvegardes régulières à partir de plusieurs disques durs. L'unité ainsi constituée (grappe) a donc une grande tolérance aux pannes ou une plus grande capacité et vitesse d'écriture. Une telle répartition de données sur plusieurs disques permet d'augmenter la sécurité et de fiabiliser les services associés.

3.13 La Qualité de service

Pour arriver à la disponibilité des services réseaux et en particulier du service de téléphonie à un taux de 99,999,et en plus de la résilience des liens et du hardware, il est indispensable de mettre en place une qualité de service pour prioriser certaines applications relativement par rapport à d'autre et en particulier le trafic voix qui est spécifique de par certains paramètres décrit ci-après :

1. Le délai : c'est le temps que met un paquet voix de la source (l'appelant) vers la destination (l'appelée) et ce délai ne doit pas dépasser les 250ms. Une congestion d'un point du réseau peut faire augmenter ce délai avec des conséquences

gênantes sur la qualité de la voix.

2. la variation de délais (Jitter) : C'est la différence de temps entre deux paquets voix. Cette variation doit être plus ou moins stable et ne doit pas excéder 30 ms. La congestion influe d'une manière significative sur cette variation et abaisse la qualité de la voix transmise2. la variation de délais (Jitter) : C'est la différence de temps entre deux paquets voix. Cette variation doit être plus ou moins stable et ne doit pas excéder 30 ms. La congestion influe d'une manière significative sur cette variation et abaisse la qualité de la voix transmise.

3. La perte de paquets : Durant les périodes de congestion les équipements actifs procèdent au rejet aléatoire des paquets et en particulier des paquets voix.

Dans tout les cas de figure, la congestion est la première source de dégradation de la disponibilité ou de la qualité des services en général et de la téléphonie en particulier et afin d'y remédier l'implémentation de la QoS s'impose.

3.14 Conclusion

Nous avons présenté dans ce chapitre tout ce qui concerne la conception d'un réseau LAN, le modèle hiérarchique a trois couches, la présentation des équipements utilisés, leurs nominations et leurs interfaces. Ensuite nous avons cité les différents Vlans et VTP qui seront implémentés par la suite.

Chapitre 4

Réalisation

4.1 Introduction

Après avoir étudié la partie théorique nous allons entamer une étape importante de ce travail qui n'est autre que la réalisation de ce dernier.

Dans ce chapitre, nous allons définir le simulateur que nous avons utilisé " Packet Tracer ", et expliquer les différentes étapes de configuration et les interfaces. Des tests sont effectués pour valider le résultat trouver
.

4.2 Le simulateur Packet tracer

Packet Tracer est un simulateur de matériel réseau Cisco (routeurs, commutateurs). Cet outil est créé par Cisco Systems qui le fournit gratuitement aux centres de formation, étudiants et diplômés participant, ou ayant participé, aux programmes de formation Cisco (Cisco Networking Academy).

Le but de Packet Tracer est d'offrir aux utilisateurs un outil permettant d'apprendre les principes du réseau, tout en acquérant des compétences aux technologies spécifiques de Cisco. Il peut être utilisé pour s'entraîner, se former, préparer les examens de certification Cisco, mais également pour de la simulation réseau.

4.2.1 Architecture réseau sous Packet tracer

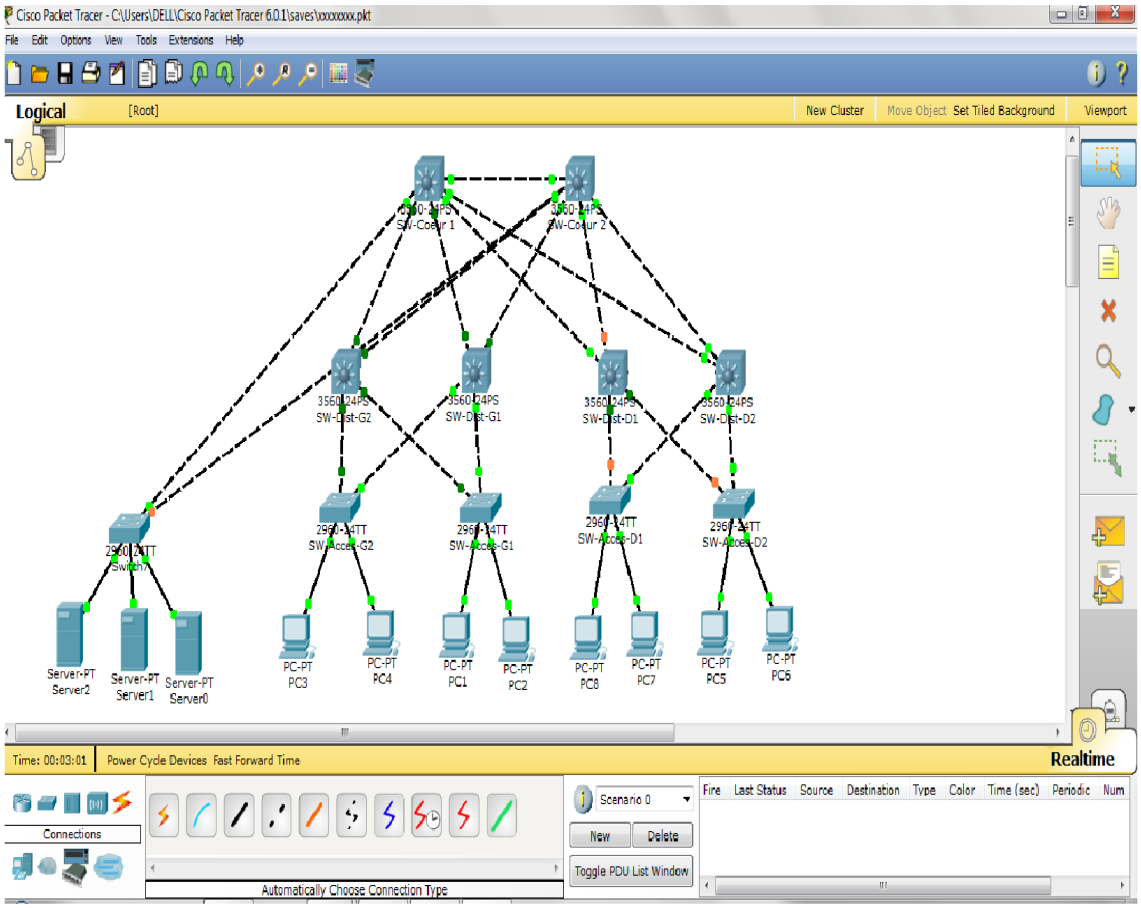

FIG. 4.1 – Architecture réseau sous Packet tracer.

4.3 Méthodes de configuration des équipements

Pour configurer les équipements du modèle on utilise le CLI (Command Language Interface) :

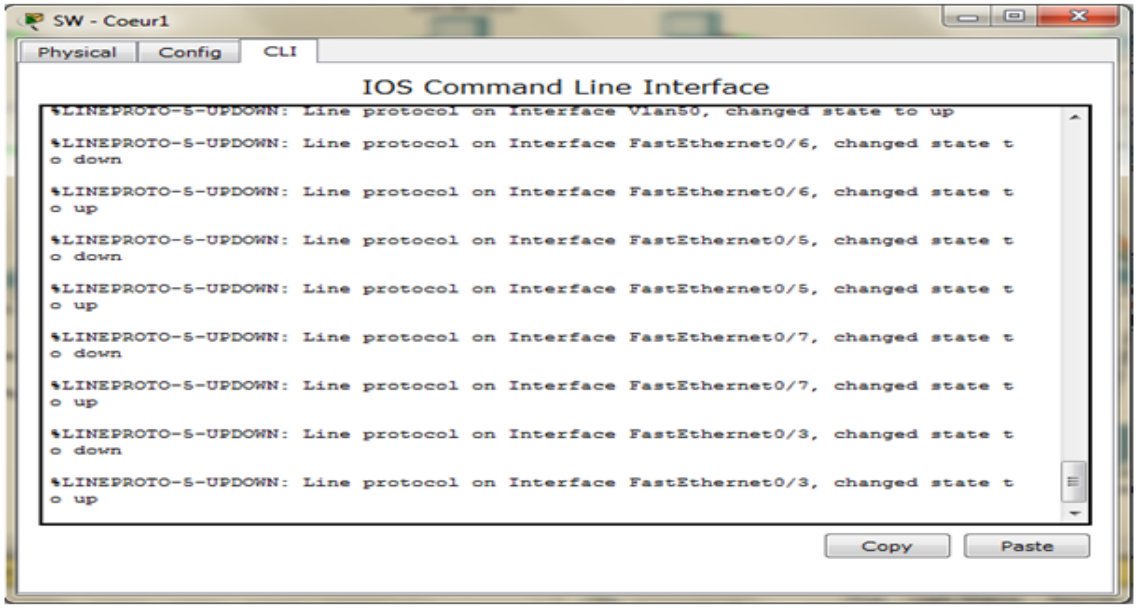

FIG. 4.2 – Interface CLI.

4.4 Configuration des équipements

On va lancé des séries des configurations sur tous les équipements du réseau. Dans ce qui suit on va présenté la configuration en générale de tous les équipements avec un exemple configurée.

4.4.1 Configuration des commutateurs

On configure tout d'abord les VLANs :

```
Switch(config) ♯ vlan 9
Switch(config) ♯ Vlan-Mgmt
Switch(config)♯ exit
Switch(config) ♯vlan10
Switch(config) ♯nameVlan-Finance
Switch(config)♯ exit
Switch(config) ♯vlan 11
Switch(config) ♯nameVlan-Commercial
Switch(config)♯ exit
Switch(config) ♯vlan 20
Switch(config) ♯nameVlan-Juridique
Switch(config)♯ exit
Switch(config) ♯vlan 21
Switch(config) ♯nameVlan-Informatique
Switch(config)♯ exit
Switch(config) ♯vlan 30
Switch(config) ♯name Vlan-Srv1
Switch(config)♯ exit
Switch(config) ♯vlan 40
Switch(config) ♯name Vlan-Srv2
Switch(config)♯ exit
Switch(config) ♯vlan 50
Switch(config) ♯name Vlan-Srv3
Switch(config)♯ exit
```

Ensuite nous suivrons les étapes de configurations illustrées ci-dessous :

1. Configuration de Hostname : (Nomination des équipements sur " Cisco Packet Tracer ").
2. Configuration de VTP.
3. Configuration des VLANs.
4. Configuration des interfaces.
5. Configuration de Spanning-Tree.
6. Configuration de DHCP.

On rappelle que le switch coeur1 (SW-Coeur1) travaille sur la couche 3 de modèle OSI. Exemple de configuration : le switch coeur 1 (SW-Coeur1) :

1. **Configuration de Hostname :**

```
Switch ♯ conf t
Switch(config) ♯ hostname SW-Coeur1
```

2. **Configuration de VTP**

```
SW-Coeur1(config) ♯ VTP domain RTC
SW-Coeur1(config) ♯ VTP mode RTC
SW-Coeur1(config) ♯ exit
```

3. **Configuration des VLANs**

```
SW-Coeur1(config) ♯ interface vlan9
SW-Coeur1(config-if) ♯ip address 192.168.9.254 255.255.255.0
SW-Coeur1(config-if) ♯ exit
SW-Coeur1(config) ♯ interface vlan10
SW-Coeur1(config-if) ♯ip address 192.168.10.254 255.255.255.0
SW-Coeur1(config-if) ♯ exit
SW-Coeur1(config) ♯ interface vlan11
SW-Coeur1(config-if) ♯ip address 192.168.11.254 255.255.255.0
SW-Coeur1(config-if) ♯ exit
SW-Coeur1(config) ♯ interface vlan20
SW-Coeur1(config-if) ♯ip address 192.168.20.254 255.255.255.0
SW-Coeur1(config-if) ♯ exit
SW-Coeur1(config) ♯ interface vlan21
SW-Coeur1(config-if) ♯ip address 192.168.21.254 255.255.255.0
SW-Coeur1(config-if) ♯ exit
SW-Coeur1(config) ♯ interface vlan30
SW-Coeur1(config-if) ♯ip address 192.168.30.254 255.255.255.0
SW-Coeur1(config-if) ♯ exit
SW-Coeur1(config) ♯ interface vlan40
SW-Coeur1(config-if) ♯ip address 192.168.40.254 255.255.255.0
SW-Coeur1(config-if) ♯ exit
SW-Coeur1(config) ♯ interface vlan50
SW-Coeur1(config-if) ♯ip address 192.168.50.254 255.255.255.0
SW-Coeur1(config-if) ♯ exit
```

4. **Configuration des interfaces :**

```
SW-Coeur1(config) ♯ interface FastEthernet 0/2
SW-Coeur1(config-if) ♯no shutdown
SW-Coeur1(config-if) ♯ switchport mode trunk
```

5. **Configuration de Spanning-Tree :**

```
SW-Coeur1(config) ♯ spanning-tree mode rapid-pvst
SW-Coeur1(config) ♯ spanning-tree vlan 9-11,20-21,30,40,50
priority 4096
```

6. **Configuration de DHCP**

   La configuration du DHCP pour le VLAN 10 :

```
SW-Coeur1(config-if) ♯ ip dhcp pool vlan 10
SW-Coeur1(config-if) ♯network 172.16.10.0 255.255.255.0
SW-Coeur1(config-if) ♯ default-router 172.16.10.254
SW-Coeur1(config-if) ♯ ip dhcpexcluded-add 172.16.10.254
```

4.4.2 Configuration des serveurs

Nous avons dans ce modèle trois serveurs que nous allons configurées leurs adresses IP,les masques et les passerelles.

- **Serveur http :**

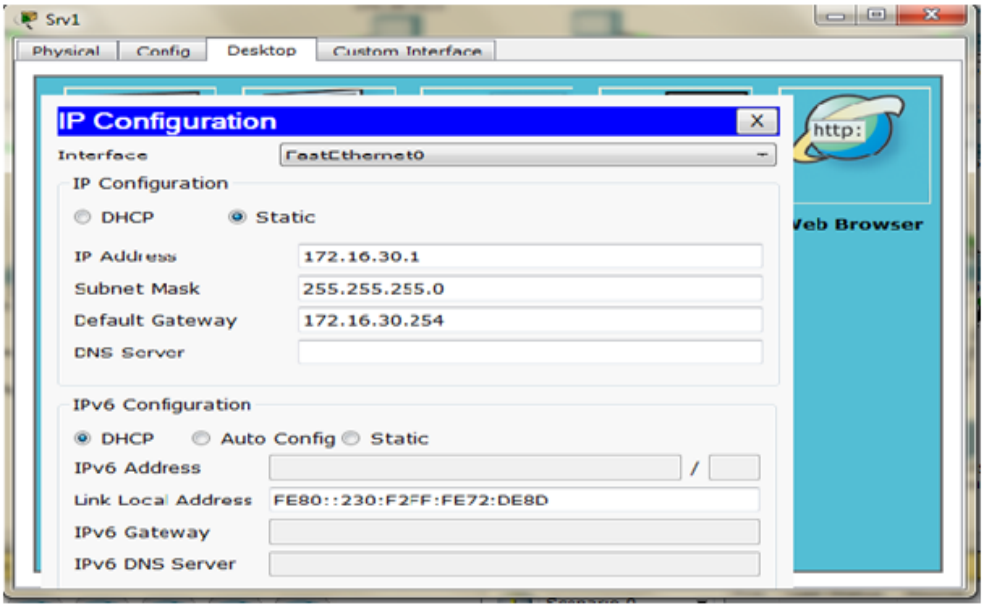

FIG. 4.3 – interface de configuration du serveur HTTP.

- **Le serveur DNS :**

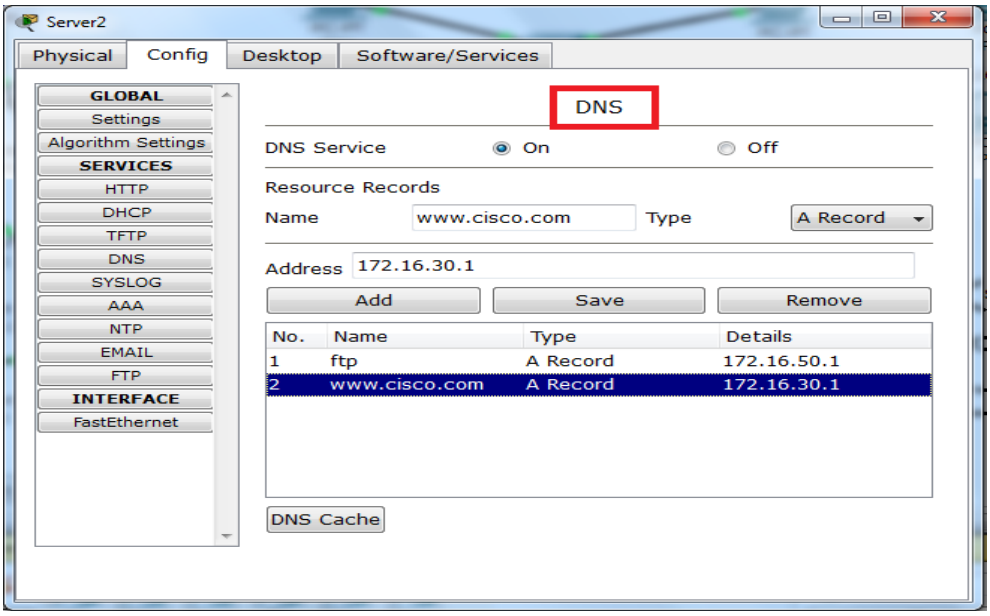

FIG. 4.4 – interface de configuration du serveur DNS.

- **Serveur FTP :**

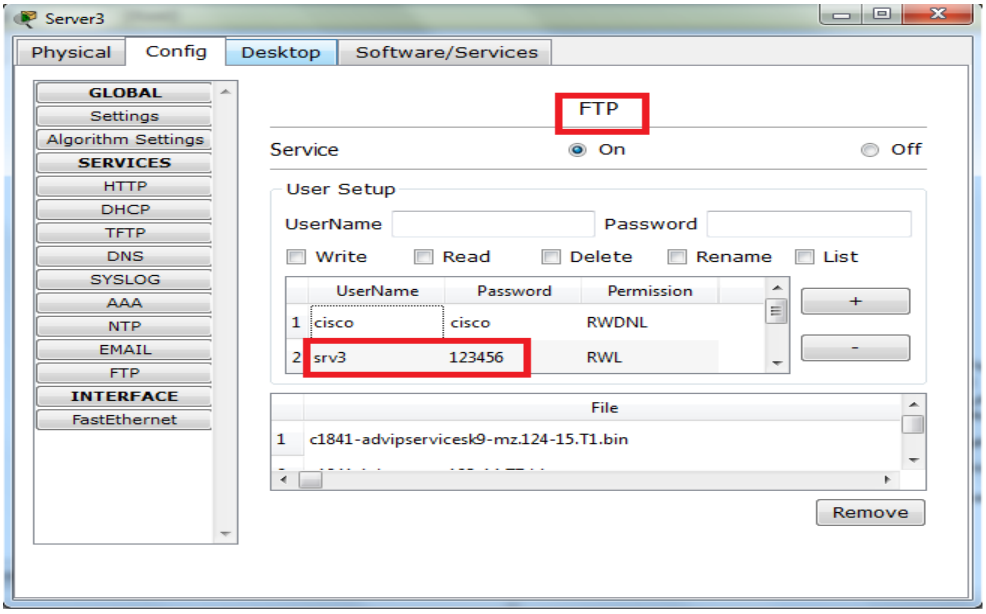

FIG. 4.5 – interface de configuration du serveur FTP.

4.5 Implémentation de la sécurité du réseau LAN

4.5.1 Protection niveau 2

- **Protection du Spanning-Tree :**

Pour assurer un réseau LOOP-FREE et garder la stabilité de la position du 'Root Bridge' dans le réseau, il faut configurer deux options :

BPDU Guard :

Chaque port de switch où un END-USER est connecté. On le configure comme " SPANNING-TREE PORTFAST " pour passer les étapes de négociation du Spanning-Tree et mettre le port directement en mode " Forwarding " parce que dans le cas normal on ne doit pas recevoir des BPDU sur des PORTFAST. Et si on connecte un équipement ou un programme malicieux qui génère des BPDU et créer des boucles. Conséquence : le réseau se mis-en hors-service.

Pour se protéger contre ces types de situations, nous devons accompagner chaque Port-Fast avec un BPDU-Guard, qui va mettre le port en mode " Err-disable " au cas où il détecte qu'il est entrain de recevoir des BPDU :

Sur touts les switchs d'accès :

```
Switch(config) ♯ interface fastethernet 0/1
Switch(config-if) ♯ spanning-tree portfast
Switch(config-if) ♯ spanning-tree bpduguard enable
```

Root Guard :

Une fois le STP est convergé, chaque port est assigné a un rôle bien définit : Root Port, Designated port, Blocking port, Alternate port, et Forwarding port.
Supposons qu'un autre switch est introduit dans le réseau, avec une priorité qui est plus souhaitable (inférieur) à celui du Root-Bridge actuel, le nouveau switch deviendra Root-Bridge, et ce n'est toujours pas désirable car la nouvelle topologie STP peut-être inacceptable et pourra influencer sur la performance du réseau.

La fonction Root-Guard contrôle la position du Root-Bridge et protège la topologie STP, lorsque il détecte un BPDU supérieur (avec priorité faible) il met le port dans un état ROOT-INCONSISTENT, et il ne peu ni envoyer ni recevoir du trafic a l'exception du recevoir des BPDU du Root-Bridge.

Sur tous les switchs d'accès :

```
Switch(config) ♯ interface fastethernet 0/1
Switch(config-if) ♯ spanning-tree guard root
```

4.5.2 Protection des services :

Protection des services de switching (Attaque Mac Flooding) :

On peut envoyer sur le port d'un switch un grand nombre d'adresse MACs pour remplir sa table de switching (CAM), et donc bloquer son fonctionnement normal. Si la table CAM est pleine, le switch est obligé d'envoyer le trafic en Broadcaste sur tous les ports (il se comporte comme un HUB). Cette attaque pourra éventuellement être utilisée comme technique pour capturer un flux.
Pour éviter ce type d'attaque, une fonction qui se nomme " Port Security " permet de limiter le nombre d'adresses MAC sur un port et donc protège le switch contre le " Mac Flooding "
La fonction 'Port Security' offre plusieurs paramètres de configuration sur un port,

et dans le but de garder une flexibilité de changer l'emplacement des ordinateurs, nous avons procédé comme suit :

- Activation de l'option Port-Security, qui va mettre le mode de lecture des adresses MAC en mode dynamique, et a chaque fois qu'on change l'équipement connecté, le Port-Security change automatiquement l'adresse MAC autorisé

Sur touts les switchs d'accès :

```
Switch(config) ♯ interface fastethernet 0/1
Switch(config-if) ♯ switchport port-security
Switch(config-if) ♯ switchport port-security maximum 1
```

4.5.3 Protection management :

• Telnet et SSH (Secure Shell) :

Bien que l'accès Telnet soit facile à configurer et à utiliser, Telnet n'est pas sécurisé. Chaque caractère qu'on tape dans une session Telnet est envoyé en clair, sans cryptage. Par conséquent, il est très facile d'intercepter les sessions Telnet pour récupérer les noms d'utilisateurs et mots de passe. Au lieu du Telnet, on peu utiliser SSH qui utilise un cryptage renforcé pour sécuriser les données de session.

Sur touts les switchs :

```
Switch(config) ♯ line vty 0 4
Switch(config-line) ♯ transport input ssh
```

• Les ACL (Access Control Liste) :

Dans le but de sécuriser l'accès aux équipements de notre réseau (commutateur) nous avons crée une liste de contrôle d'accès qui permet seulement aux poste de vlan 21 (informatique) d'accéder aux commutateurs afin de les gérer.

```
SW-Coeur1(config) ♯ access-list 10 permit 172.16.21.0 0.0.0.255
SW-Coeur1(config) ♯ access-list 10 deny any
```

4.6 Implémentation de la QoS

4.6.1 Implémentation de QoS sur les switchs cœur

```
Switch(config) ♯ class-map match-all Apps-Critique
Switch(config-cmap) ♯ match access-group name Critique
Switch(config-cmap) ♯ exit
Switch(config) ♯ policy-map Mark-Traffic
Switch(config-pmap) ♯ class Apps-Critique
Switch(config-pmap-c) ♯ set ip dscp af32
Switch(config) ♯ exit
```

4.6.2 Configuration de la confiance accordée aux ports

Tous les liens en trunk qui arrivent sur les switches de distribution doivent être en TRUST pour garder le marquage effectué par les switches d'accès

```
Switch(config) ♯ conf t
Switch(config) ♯ Interface fastethernet0/1
Switch(config-if) ♯ mls qos trust dscp
```

4.7 Test et validation de configuration

On test dans cette partie les communications entre tous les équipements en utilisant la commande Ping. Ces tests sont faits entre équipements, inter-Vlans et entre Vlans . Il est à noter que la commande Ping est très utile pour tester la réponse d'un ordinateur sur un réseau. Cette commande envoie des paquets avec le protocole ICMP.

4.7.1 Entre équipements

On teste les communications inter-switchs Exemple : Test réussi entre le switch SW-Coeur1 et le switch SW-Acces-D1

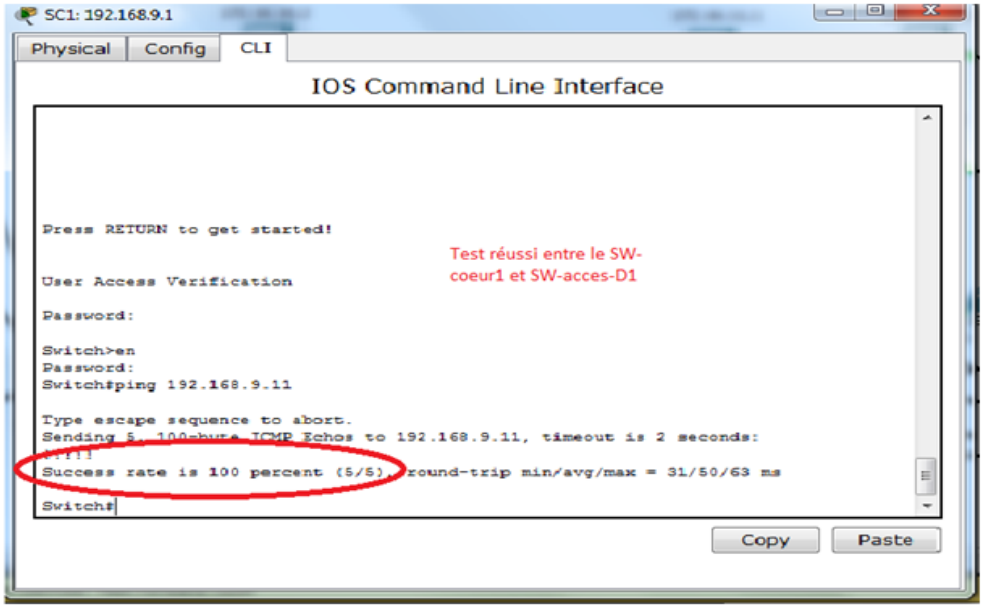

FIG. 4.6 – Test entre SW-Coeur1 et SW-Acces-D1.

4.7.2 Test entre VLANs

Exemple : Tests réussis entre le PC1 (172.16.10.2) et le PC3 (172.16.10.1) qui appartient au même VLAN10.

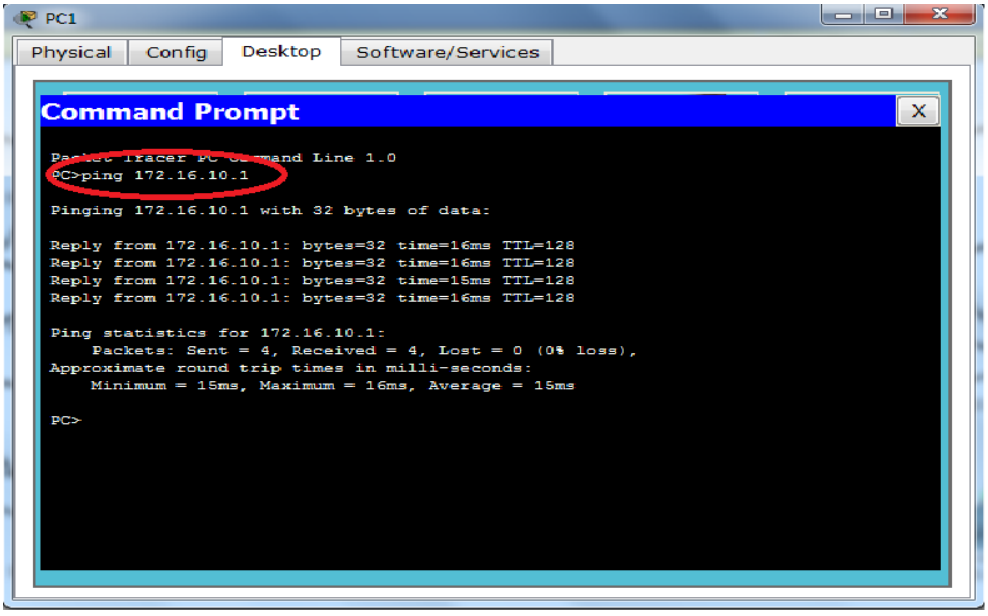

FIG. 4.7 – Test entre PC1 et PC3.

4.7.3 Test inter-VLANs

Exemple : Test réussi entre PC3 (VLAN 10) et PC8 (VLAN 20)

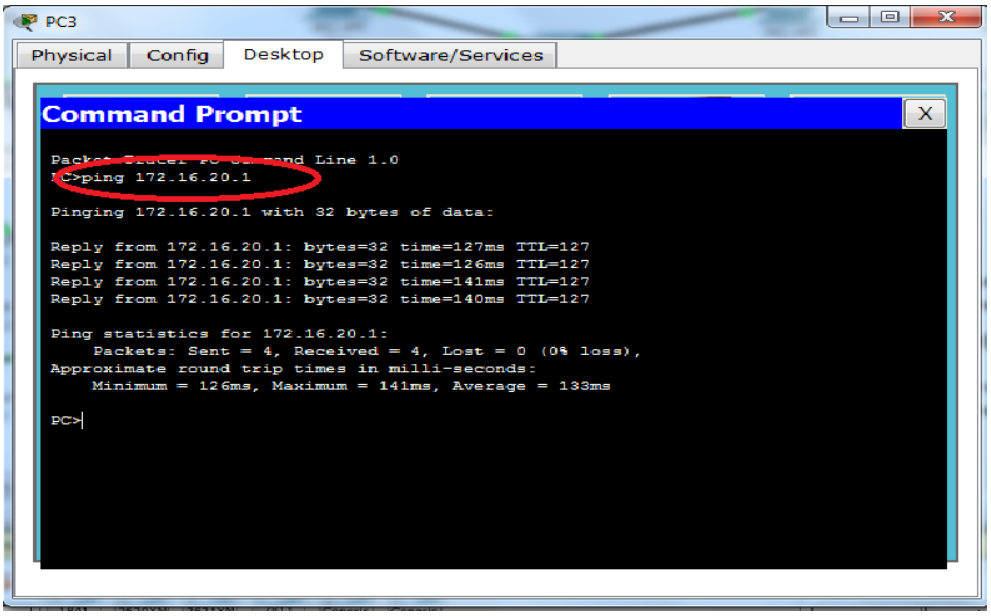

FIG. 4.8 – Test entre PC3 et PC8.

4.7.4 Test de Spanning-Tree Protocol (STP)

On lance la commande ” show Spanning-Tree active ” sur le switch d’accès (SW-Acces-G-1).

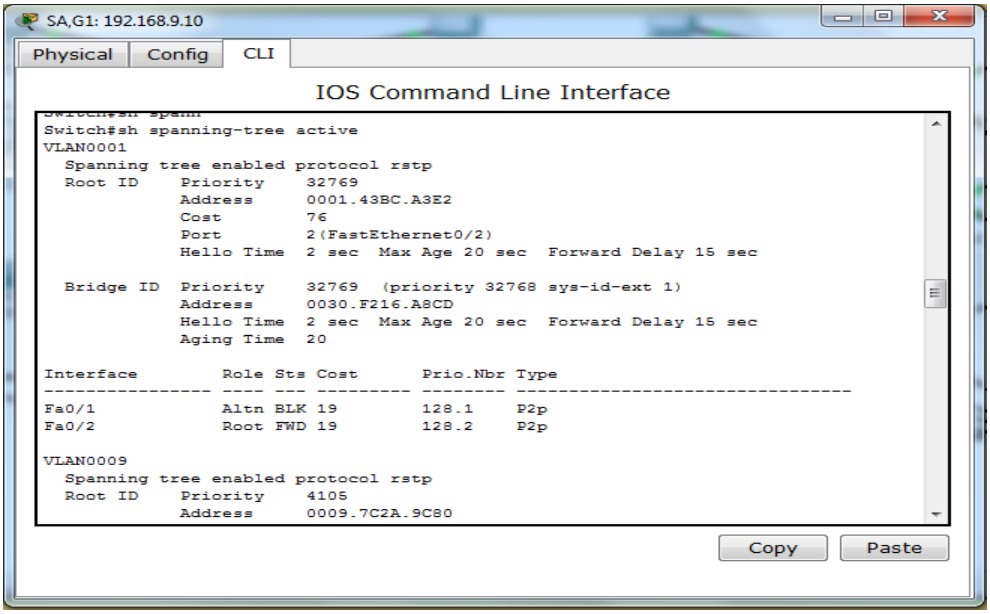

FIG. 4.9 – Test de Spanning-tree.

4.8 Conclusion

Dans ce chapitre, nous avons présenté l'ensemble des configurations réalisées au niveau du réseau LAN, pour sa mise en marche. La configuration de chaque équipement du réseau, assure l'interconnexion entre eux. Enfin, nous avons effectuer un ensemble de tests et de validation , dans le but de prouver l'efficacité des solutions.

Conclusion générale

Les réseaux informatiques sont de plus en plus répondus et complexes.

L'implémentation d'un réseau complexe doit être sûr pour avoir des réseaux fiables .Nous avons essayé, par le biais de ce projet, de configurer un réseau LAN dans le but de faciliter la préparation et la réalisation des projets de l'entreprise, et pour une meilleure gestion du réseau.

Pour cela, nous avons débuté notre projet par des généralités concernant les réseaux informatiques, dans le but de mieux cerner notre travail. L'élaboration du cahier des charges a notamment pris sa place dans ce champ d'étude afin de présenter d'une façon générale notre projet.

Nous avons par la suite, dans la partie conception, mis en œuvre le modèle de conception hiérarchique du réseau LAN. Enfin, nous avons abordé la réalisation en utilisant le simulateur Packet tracer dans le but de configurer les différents équipements et protocoles de ce réseau.

Ce travail nous a permis de nous nous confronté aux difficultés réelles de la gestion, et d'administration des réseaux locaux tel que celui de la SONATRACH et d'acquérir une expérience personnelle et professionnelle très bénéfique. Ce fut une occasion pour nous de se familiariser avec l'environnement du travail et de la vie professionnelle, d'élargir et d'approfondir nos connaissances théorique sur les réseaux informatiques.

Dans le futur, pour la continuité de notre travail, la prudence veut que l'on approfondisse l'étude, afin de compléter la solution. Nous aimerions définir des politiques de sécurité plus robuste et plus fiable, a savoir la mise en place des protocole de sécurité tel que AAA (Authentication, Authorization, Accounting), SNMPv3 et en intégrant d'autre protocoles de la QoS(qualité de services) pour prioriser certaines applications relativement par rapport à d'autre on particulier le trafic voix .

Annexe A

Annexe

Le Protocole 802.1q :

Description de la norme

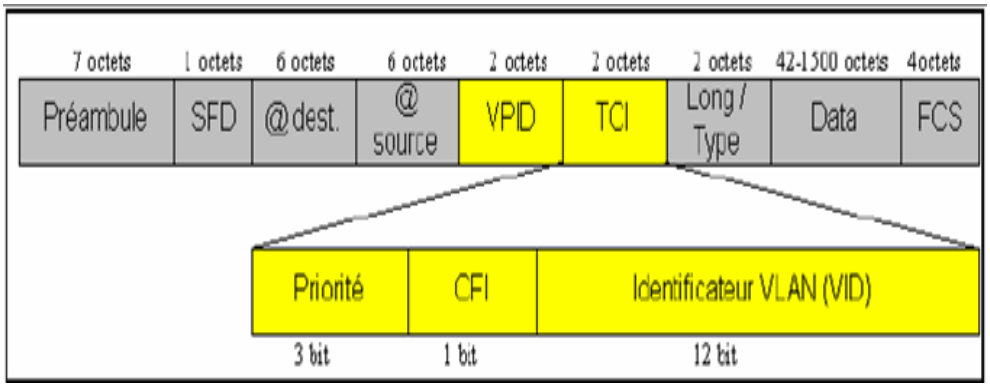

FIG. A.1 – Description de la norme 802.1q .

Elle définit, en premier lieu, l'ajout de 2 octets dans la trâme ethernet. Ces deux octets ajoutent plusieurs champs pour répondre à plusieurs besoins. La norme définit alors sur la trame ethernet le champ VPID à 0x8100 pour désigner la trame 802.1q. La principale fonction de la norme est de transporter les Vlans sur le réseau, pour permettre à deux machines d'un même Vlan de communiquer au travers un nombre non définit d'équipement réseau.

La norme 802.1q prévoit également un mécanisme de prioritisation de flux. Cette prioritisation est définie par la norme 802.1p.

Un champ protocole définit sur 1 bit est prévu pour pouvoir utiliser le 802.1q aussi bien sur ethernet que sur TokenRing.

Enfin, le champ Vlan ID permet de fixer un identifiant sur 12 bits d'un Vlan.

Architecture d'un commutateur 802.1q

Un commutateur respectant la norme 802.1q se décompose en trois couches :

- La couche configuration qui permet d'ecrire les informations dans la MIB et s'occupe des commandes d'administrations de l'OS implémenté sur le switch.

- La couche définition automatique et propagation. Cette couche est chargé d'enregistrer les Vlans présents sur les différents ports du switch et d'avertir le reste du réseau de l'appartenance du switch au Vlan. Il doit donc pour cela maintenir plusieurs tables à jour, que nous détaillerons plus tard.

- La couche relais qui, comme son nom l'indique relais les informations qu'il collecte sur ses ports.

La partie la plus importante dans le protocole 802.1q est la définition automatique et propagation. On rappelle qu'on appelle "trunk" un lien transportant plusieurs Vlans.

Transport statique

Il est possible de configurer le 802.1q à la main pour permettre de transporter les Vlans. Pour cela, il faut configurer chaque port se trouvant sur le chemin d'un port tagué d'un Vlan à un autre. IL faut de plus répeter l'opération pour chaque lien défini. On peut comprendre que le processus s'avère long et fastidieux. La norme prévoit donc un mécanisme qui tague les ports automatiquement suivant les Vlans déclarés.

Transport dynamique : le GVRP

Le protocole GVRP propose différents mécanismes pour la diffusion des informations sur les Vlans reliés à un switch. Avant toutes choses, il faut savoir que seul les switchs supportant le GVRP peuvent faire du GVRP et que des cartes réseaux peuvent, elles aussi supporter le GVRP parfois.

Si le GVRP est actif sur un commutateur, chaque port est automatiquement pris par défaut dans le mécanisme de GVRP. Nous verrons néanmoins plus loin qu'il existe des solutions pour éviter la participation d'un port au GVRP.

Pour pouvoir bien comprendre le problème, supposons qu'un switch soit définit sur un de ses ports sur le Vlan 2. Or, de l'autre coté du réseau, un autre switch possède un port sur le Vlan 2. Le GVRP va permettre de taguer les ports nécessaires pour que les deux ports tagués puissent communiquer.

Le GVRP se décompose en trois parties :

- Une partie applicative que nous appellerons GVRP App. Cette partie contient les informations sur les switchs et les Vlans qu'ils contiennent. Par exemple, on trouvera l'information : "le switch 1 a besoin du Vlan 2"

- Une partie définissant les messages echangés entre les ports d'un même switch que l'on appellera GIP. Cette partie se limite aux echanges internes à un switch.

- Une partie définissant les echanges entre les switchs distants appelé GID.

Bibliographie

[1] http ://www.commentcamarche.net/contents/508-le-concept-reseau .

[2] http ://www.courstechinfo.be/Reseaux/Classif.html..

[3] https ://www.pedagogie.ac-aix-marseille.fr/upload/docs/application/pdf/2012-07/formation-reseau.pdf.

[4] http ://www.opendoc.net/cours/cours-comparaison-modele-osi-modele-tcpip.

[5] http ://www.christian.braesch.fr/page/les-equipements-dun-reseau.

[6] http ://www.inetdoc.net/articles/inter-vlan-routing/inter-vlan-routing.vlan.html.

[7] http ://www.nemako.net/dc2/ ?post/VTP-VLAN-Trunking-Protocol.

[8] http ://cisco.goffinet.org/s3/spanning-tree.VzC0PzE2VgQ.

[9] http ://www.cisco.com/cisco/web/support/CA/fr/109/1091/1091591-ssh.html.

[10] http ://baptiste-wicht.developpez.com/tutoriels/reseau/introduction/ ?page=7.

[11] http ://www.it-connect.fr/quest-ce-que-larp.

[12] http ://www.aidoweb.com/tutoriaux/les-access-control-list-acl-qu-c-comment-s-servir-filtrage-reseau-623.

[13] http ://www.materiel-informatique.be/serveur.php.

[14] http ://cisco.goffinet.org..

[15] http ://www.dicodunet.com/definitions/creation-web/serveur-http.htm..

[16] https ://technet.microsoft.com/fr-fr/library/cc75363528v=ws.1029.aspx.

[17] http ://www.culture-informatique.net/cest-quoi-un-serveur-ftp.

[18] Architecture de réseaux et études de cas Seconde édition Publié par Campus Press France .

[19] http ://www-igm.univ-mlv.fr/ dr/XPOSE2007/vlanparlegrandquinapascomprislesconsignes. (Consulté le 17 avril 2016).

[20] http ://www.reseaucerta.org/cours/les Vlans.

[21] http ://oujdapc.olympe.in/ReseauVlan.htm .

[22] RESEAUX ET TÉLÉCOMS Cours et exercices corrigés,Claude Servin.

[23] Tableaux de bord de la sécurité réseau ,2ieme édition, ÉDITIONS EYROLLES.

RÉSUMÉ

Ce travail consiste en une proposition d'une configuration d'un réseau LAN pour l'entreprise SONATRACH ; Il s'agit de configurer le réseau de cette entreprise et de le sécuriser. Les concepts fondamentaux des réseaux locaux y sont bien explicités, nous avons présenté l'architecture du réseau et les différents mécanismes de sécurité. dans ce mémoire nous avons implémenter un réseau LAN comprenant les protocoles DHCP, VTP , STP et une solution sécurisé basé sur le protocole SSH, ACL ,BPDU Guard, les mots de passe au niveau des switchs, avec le logiciel Cisco Packet Tracer basé sur les VLANs.

Mots clés :DHCP,VTP,STP,SSH, ACL .

ABSTRACT

This work consists of proposal of a configuration of a LAN network company SONATRCH ; This is set up the network of the company and secure. The fundamental concepts of local networks are well explained, we presented the network architecture and the different security mechanism. In this memory we implement a LAN network with DHCP protocols, VTP, STP and secure solution based on SSH, ACL, BPDU Guard, passwords at the switch's level with the Cisco Packet Tracer software based VLANs.

Key words : DHCP,VTP,STP,SSH, ACL .