République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique
Université Blida 1- Saad Dahlab

FACULTE DES SCIENCES
DEPARTEMENT D' INFORMATIQUE

Mémoire pour l'obtention
Du Diplôme de Master en Informatique
Option : Systèmes Informatiques et Réseaux

Thème

Conception d'un réseau LAN sécurisé pour une nouvelle agence BADR banque

Présenté par :

Mlle BELLI FERIEL.
Mlle DOUNAS LEILA.

Devant le Jury :

Mr BENYAHIA Mohammed: Encadreur

Mr OULD KHAOUA Mohamed : President

M^{me} GHEBGHOUB Yasmine : Examinatrice

Organisme d'accueil

Banque de l'agriculture et du développement rural (Agence chéraga)

Année universitaire 2020/2021

Remerciement

Nous tenons à remercier en premier lieu DIEU le Tout Puissant, qui nous a donné la force, la volonté et surtout le courage afin d'accomplir ce modeste mémoire.

Nous adressons nos remercîments les plus chaleureux à notre promoteur ***Mr BENYAHIA*** *pour son aide précieuse.*

Nos vifs remerciements à ***Mr YAZID, Mr YOUSEF*** *pour leur suivi tout au long de l'élaboration de ce projet, ainsi que pour leurs conseils, leurs remarques et leurs orientations qui ont été d'une pertinence et d'une clairvoyance remarquable, sans oublier* ***Mr KOHIL****...*

Nous remercions également les membres du jury qui ont pris la peine de juger ce modeste travail.

Nous tenons à remercier sincèrement ***Madame haji kahina*** *de nous avoir donné l'opportunité et l'occasion de suivre un stage pratique au sien de la Banque Agriculture et Développement Rurale (BADR).*

Un grand remerciement a nos enseignants et enseignantes qui ont contribués à notre formation, depuis le cycle primaire au cursus universitaire.

On remercie tous ceux qui ont contribués de prés ou de loin à l'aboutissement de notre travail. Pour tous, merci infiniment.

Dédicace

C'est avec une profonde gratitude et en toute sincérité que je dédie ce modeste travail de fin d'études A ma très chère famille, qui m'a apporté son soutien indéfectible et inconditionnel tout au long de mon parcours étudiant particulièrement mes parents, mes sœurs ainsi tout mes frères surtouts mon frère adoré Tarik. Pour leur précieux et judicieux conseils, leur patience et compréhension, Je vous serai à tout jamais redevable. A tous mes ami(e)s et camarades. Pour leurs encouragements et leurs soutiens qui m'ont été d'une aide précieuse. A toute personne ayant contribué de près ou de loin à l'élaboration de ce travail.

LILA

Dédicace

C'est avec une profonde gratitude et en toute sincérité que je dédie ce modeste travail de fin d'études

A ma très chère famille, qui m'a apporté son soutien indéfectible et inconditionnel tout au long de mon parcours étudiant. Pour leur précieux et judicieux conseils, leur patience et compréhension, Je vous serai à tout jamais redevable. A tous mes ami(e)s et camarades. Pour leurs encouragements et leurs soutiens qui m'ont été d'une aide précieuse. A toute personne ayant contribué de près ou de loin à l'élaboration de ce travail.

Feriel

Résumé

Face au développement des technologies informatiques, les réseaux locaux des entreprises présentent des infrastructures complexes qui doivent répondre à un certain nombre de normes spécifiques aux équipements à interconnecter et aux applications à supporter. C'est pourquoi la technologie de l'implémentation du réseau local offre plusieurs solutions qui doivent être adaptées tout particulièrement à l'architecture de l'organisme concerné et d'accompagner sa croissance tout en sécurisant ses services des attaques qui proviennent de l'intérieure ou de l'extérieure de l'entreprise. Dans ce mémoire nous nous sommes intéressées à « mise en place d'un réseau convergé de l'BADR Banque », Où nous avons essayé de proposer des solutions adéquates aux nombreux problèmes tirés durant l'étude de l'architecteur du réseau de cette entreprise, dont l'implémentation d'un modèle réseau hiérarchique ; et la mise en place d'une nouvelle interconnexion entre les différents sites de l'entreprise, plus précisément RMS, WIMAX. **Mots clés** : Réseaux locaux des entreprises, sécurité, modèle réseau hiérarchique, RMS, WIMAX.

ABSTRACT

Faced with the development of computer technologies, the local networks of companies present complex infrastructures which must meet a certain number of standards specific to the equipment to be interconnected and the applications to be supported. This is why the technology of the implementation of the local network offers several solutions that must be particularly adapted to the architecture of the organization concerned and to support its growth while securing its services from attacks originating from within. Or from outside the company. In this thesis we are interested in « setting up a converged BADR Bank network», where we have tried to propose adequate solutions to the many problems drawn during the study of the network architecture of this company, of which the implementation of a hierarchical network model, and the establishment of a new interconnection between the various sites of the company, more precisely RMS, WIMAX. **Key words**: Local business networks, Security, hierarchical network model, RMS, WIMAX.

ملخص

وفي مواجهة تطور تكنولوجيات الحواسيب , تقدم الشبكات المحلية للشركات هياكل أساسية معقدة يجب أن تستوفي عددا معينا من المعايير الخاصة بالمعدات المراد ترابطها والتطبيقات المراد دعمها وهذا هو السبب في أن تكنولوجيا تنفيذ الشبكة المحلية توفر عدة حلول يجب تكييفها بشكل خاص مع هيكل المنظمة المعنية ودعم نموها مع تأمين خدماتها من الهجمات التي تأتي من الداخل. أو من خارج الشركة وفي هذه ألأطروحة نحن مهتمون بـ "إنشاء شبكة BADR بنك و ومتقاربة حيث حاولنا اقتراح حلول ملائمة للمشاكل العديدة التي وُضعت أثناء دراسة هيكل الشبكة في هذه ألشركة.

Table des matières

Liste Des Figures

Liste Des Tableaux

Introduction

Les réseaux sont nés du besoin d'échanger, transfert des informations de manière simple et rapide entre les machines. La sécurité des réseaux informatiques est un sujet essentiel pour favoriser le développement des échanges dans tous les domaines, dans le but de maintenir la confidentialité, l'intégrité et le contrôle d'accès au réseau pour réduire les risques d'attaques.

Pour faire face à ces enjeux en vas étudier un cas concret, à savoir la mise en service d'un réseau informatique fiable et sécurisée au niveau d'une nouvelle agence bancaire dépendant de la « BADR ».

C'est dans cette optique que nous avons voulu aborder dans notre étude comprendre le concept du réseau au niveau de l'agence afin de définir l'architecture, l'administration, la sécurisation ainsi son rôle dans la facilitation de la gestion des opérations bancaires. Ainsi le réseau sera décortiqué de façon à mieux définir la stratégie de sa protection de façon continue en suivant l'évolution des technologies.

Dans le cadre de cette stratégie, La « BADR »nous a confié la mission de concevoir et déployer une architecture convergée et sécurisé pour une nouvelle Agence appartenant à l'entreprise. Ce travail consiste la mise en place d'une plate-forme IP en tant que service intégré et prêt à l'emploi pour tous les services informatiques et les services support d'une entreprise. Cette mise en place doit prendre en considération toutes entités et composantes organisationnelles de l'entreprise.

Notre mémoire se subdivisera en quatre principaux chapitres, notamment l'approche théorique et pratique. La première approche contient le premier et le deuxième chapitre, et la dernière approche contiendra le troisième chapitre et quatrième.

Le premier chapitre, **Introduction générale** définit notre société la « BADR » et met en relief le problème observé en entreprise.

Le second chapitre, **Définition et Concepts,** décrit les concepts liés aux modèles de conception d'architecture réseau, des technologies d'interconnexion des sites distants et les fondements des protocoles utilisés pour véhiculer les données à travers les réseaux.

Le troisième chapitre, **Topologie de la solution proposé** ou nous mettant une solution adéquate avec les objectifs fixés. Ceci, par la mise en place d'une conception répondant aux exigences actuelles et futures de l'entreprise afin de suivre l'évolution du marché actuel et pour survivre à la rude concurrence imposé par la mondialisation.

Le quatrième chapitre dédier a **Implémentation et test,** nous évoquerons la mise en place de la solution choisie dans le dernier chapitre intitulée

Chapitre I
Introduction générale

Chapitre I. Introduction Générale

I.1 Introduction

Ce chapitre sera dédié à l'exposition du contexte général de notre projet de fin d'études est un point clé. Car, c'est une étape essentielle qui vise à représenter les contraintes sous lesquelles le projet se réalisera. D'abord Citons les informations relatives à l'organisation de l'existant qui nous aideront à déterminer la portée du projet, dont les objectifs de l'entreprise, plateformes matérielles et logicielles ainsi qu'à la stratégie de sécurité appliqué au niveau de la société.

I.1.1 Cadre général

Le présent projet intitulé « Etude et mise en place d'un réseau de nouvelle agence », a été réalisé dans le cadre de la préparation du projet de fin d'études présenté en vue de l'obtention du diplôme de mastère II pour l'année universitaire 2020/2021. Il a été réalisé au sein de la société Banque de l'agriculture et du développement rural (BADR).

I.2 Présentation de l'entreprise

I.2.1 Présentation générale

La Banque de l'agriculture et du développement rural (BADR) est une institution financière algérienne, Elle a pour missions principales le développement du secteur agricole et la promotion du monde rural.

Figure I.1 : Logo de l'BADR.

. Chargée aussi de fournir aux entreprises publiques économiques conseils et assistance dans l'utilisation et la gestion des moyens de paiement mis à leur disposition, et ce, dans le respect du secret bancaire.

I.2.2 Les Objectifs de l'entreprise

- L'augmentation des ressources aux meilleurs coûts et rentabilisation de celles-ci par des crédits productifs et diversifiés dans le respect des règles.
- La gestion rigoureuse de la trésorerie de la banque tant en dinars qu'en devises.
- L'assurance d'un développement harmonieux de la banque dans les domaines d'activités la concernant.
- L'extension et le redéploiement de son réseau.
- La satisfaction de ses clients en leur offrant des produits et services susceptibles de répondre à leurs besoins.
- L'adaptation d'une gestion dynamique en matière de recouvrement.
- Le développement commercial par l'introduction de nouvelles techniques managériales telles que le marketing, et l'insertion d'une nouvelle gamme de produits

.

I.2.3 La Direction Maintenance et Support Informatique (D.M.S.I)

La D.M.S.I est chargée de mettre en œuvre les moyens de télécommunication, d'élaborer les procédures de sécurité et de veiller à la sécurité du système d'information de la BADR, leur mission est:

- De définir l'architecture des réseaux des télécommunications de la banque, en tenant compte de leur adaptation future nouvelles technologie.
- D'assurer la coordination avec tous les opérateurs pour une meilleure prise en charge de tous les incidents pouvant survenir sur liaisons de communication des sites de la BADR.
- De mettre en place les outils de supervision et les procédures de suivi de l'état du réseau de télécommunication.
- De développer et organiser la télétransmission au sein de la banque.
- De participer à toute étude de cahier des charges qui concerne la sécurité des systèmes.
- De définir une politique générale de sécurité informatique.
- De s'assurer de la bonne exécution de la politique de sécurité.
- De mettre en place des procédures et moyens de contrôles pour protéger le système d'informatique.
- De s'assurer que les procédures appliquées et les actions menées dans le cadre de la sécurité des systèmes d'information sont conformes à la politique de sécurité.
- De mener des actions de sensibilisation.
- D'assurer un suivi permanent des incidents et des intrusions.
- De détecter et prévenir tout dysfonctionnement.
- De mener et/ou proposer des actions préventives.
- D'élaborer et de dresser des rapports sur la sécurité informatique avec des propositions pour remédier aux dysfonctionnements constatés.
- De formuler des suggestions sur les performances et les défaillances de la sécurité des systèmes d'information.

I.3 Analyse de l'existant

Une meilleure compréhension de l'environnement informatique aide à déterminer la portée du projet et la solution à implémenter. Il est indispensable de disposer d'informations précises sur l'infrastructure réseau et les problèmes qui ont une incidence le fonctionnement du réseau. En effet ces informations vont affecter une grande partie des décisions que nous allons prendre dans le choix de la solution et de son déploiement.

Notre travail c'est situant au niveau du service d'Administration des réseaux pour la partie conceptuelle et le service de Sécurité Réseau pour la partie sécurité.

I.3.1 Plan Général du réseau informatique de LA BADR

Nous présentons ci-dessus un plan exemplaire des agences appartenant au réseau de la BADR.

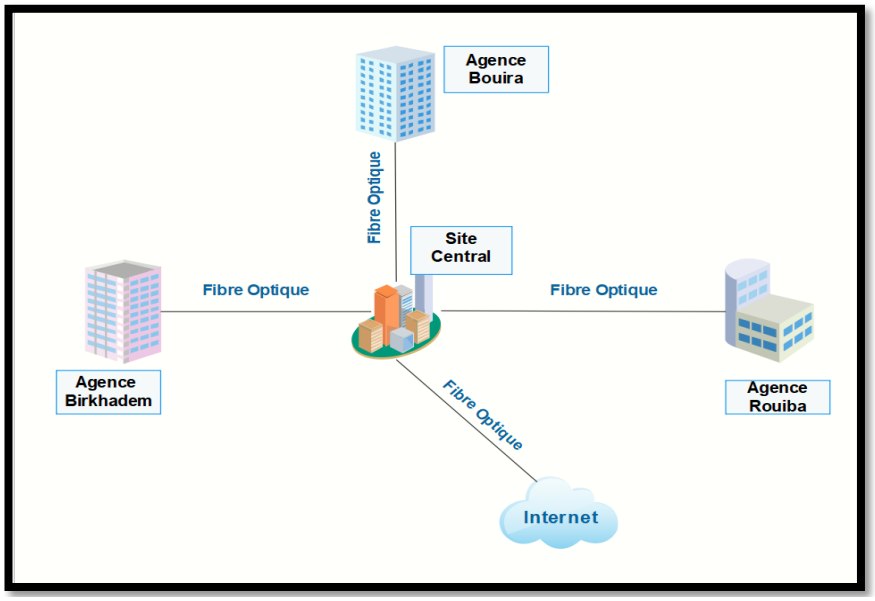


Figure I.2 : Plan Exemplaire du réseau informatique de la BADR.

I.3.2 Plan détaillé du réseau informatique de la BADR EL HACHIMIA

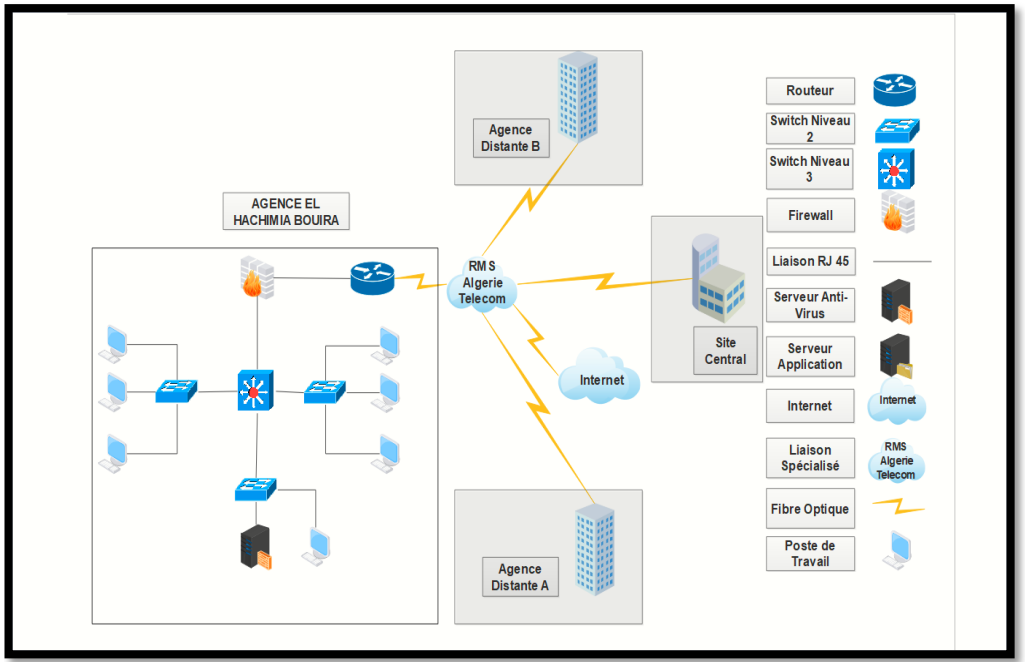


Figure I.3 : Plan détaillé du réseau informatique de l'agence EL HACHIMIA.

I.3.3 Plateforme matérielle et logicielle

Afin de bien gérer notre plan d'étude, nous détaillerons au mieux la plateforme matérielles ainsi que logicielle de notre parc réseau existant.

I.3.3.1 Plateforme matérielle

Le réseau de la BADR il est basé sur la topologie étoile. Les équipements d'interconnexions représentent le cœur d'un réseau dans une architecture, l'infrastructure de la BADR comporte des commutateurs Cisco monté en cascade. Ces équipements par leurs fonctions permettent de segmenter des réseaux par la technologie des VLANs afin de réduire significativement la congestion sur réseau au sein de chaque segment. En générale le schéma du réseau est constitué de

- Un réseau Lan du site central prés-configuré (contenant les sous directions de services).
- Des liaisons spécialisées (RMS Algérie Télécom) câbles concédés servant les agence.
- Un réseau Lan pour l'Agence Local d'Exploitation EL HACHIMIA (AEL).
- Les artères entre ces blocs supportent un débit de 1 Gigabit/s. Tous les commutateurs de réseau sont de type Cisco. Seul le protocole IPv4 est utilisé à ce jour.
- Une salle des serveurs est aménagée au niveau de site central, elle contient tout le cœur du réseau (l'arrivée des câbles concédés, une cascade de Switchs, de routeurs et tous les serveurs).

Le parc de l'agence comprend 50 stations de travail dont 2 serveurs. Celui-ci sera précisé dans le tableau suivant :

Matériels	ALE EL HACHIMIA BOUIRA	Description
Nombre de postes	50	ces postes représentent les différents ordinateurs se trouvant dans les bureaux de l'entreprise.
Nombre de serveurs	2	dispositif informatique qui offre des services à un ou plusieurs clients (parfois des milliers). représentent les postes de données, de fichiers utilisés par le personnel de l'entreprise.
Routeur Cisco	2	il permet d'interconnecter deux ou plusieurs réseaux. Possédant les mêmes composants de base qu'un ordinateur, le routeur sélectionne le chemin approprié (au travers de la table de routage) pour diriger les messages vers leurs destinations.
Firewall	1	un élément du réseau informatique, logiciel et/ou matériel il permet de protéger le réseau des intrusions extérieures, Ce dispositif filtrent les trames, bloquer en cas d'attaques.
Switch 24 ports Cisco 2960	3	Ce Switch est une configuration fixe, empilable commutateur autonome qui fournit un accès rapide à vitesse filaire Ethernet et Gigabits Ethernet.
Switch 24 ports Cisco 3560	2	Le Cisco Catalyst 3560 est un commutateur d'accès idéal pour les réseaux locaux d'entreprise ou leurs succursales. Il permet des configurations mixtes 10/100/1000 et

		PoE pour offrir un maximum de productivité et une protection des investissements tout en permettant le déploiement de nouvelles applications.
Panneau de brassage 24 ports	2	Vous pourrez, grâce à ce panneau de brassage**,** interconnecter vos cordons RJ45 de brassage dans le but de relier différents périphériques entre eux. Par conséquent, vous pourrez relier vos prises murales dont les arrivées sont câblées sur le panneau de brassage à un hub ou des Switchs. Il répartit donc efficacement la charge de votre réseau en se servant de différents hubs ou Switchs. de plus, le panneau de brassage permet, en un coup d'œil, de localiser la source d'un problème réseau grâce à une répartition géographique du réseau.
Armoire de brassage	1	Elle comprend généralement des dispositifs tels que routeurs Ethernet, Switchs. une bonne gestion du câblage permet de réduire les temps de dépannages et permet un refroidissement efficace en favorisant une bonne circulation de l'air

Tableau I.1 : Matériel informatique existant dans la BADR EL HACHIMIA.

I.3.3.2 Plateforme Logicielle

Les logiciels représentent le lien entre les processus de l'entreprise et les départements. Une plateforme Logicielle fournit un ensemble de fonctionnalités qui aident l'entreprise à tirer meilleur partie de son portefeuille d'applications.

La plateforme Applicative est constituée de :

❖ **Application de gestion :**

- Gestion de la paie.
- Gestion de la comptabilité.
- Gestion de budget.
- Logiciel « Sybu » avec ses différents modules de traitement des toutes les opérations bancaires.
- Système Swift pour l'exécution des Operations du commerce international.
- Nouveau plan de comptes au niveau de l'agence.
- Mise en service de la carte de paiement et de retrait.
- Télé- traitement des opérations bancaires à distance.

❖ **Système de gestion de Base de données**

Ce système nous permet de stocker, sauvegarder, analyser ou récupérer les données des applications. Les systèmes de base de donnée gèrent les transactions dans les applications, collectent les données depuis plusieurs systèmes et fournissent de reporting et d'analyse.

I.3.4 Stratégie de sécurité

La bonne réalisation d'une politique de sécurité permet de maitriser au mieux les risques informatiques, tout en réduisant leur probabilité d'apparition et minimiser la vulnérabilité d'un système contre des menaces accidentelles ou intentionnelles.

La BADR à adopter une stratégie de sécurité qui s'applique à l'ensemble de ses systèmes et de son personnel (de la sécurité physique à la sécurité logicielle et applicative).Cette stratégie est représenté dans les points suivant :

- Tous les ordinateurs et les équipements actifs sont branchés sur onduleur.
- Tous les équipements actifs comme les Switchs, routeurs et les firewalls sont placés dans des armoires de brassage afin de les protéger.
- La salle des serveurs qui héberge les équipements actifs et les armoires de brassages possède une bonne climatisation, une armoire de climatisation et des split-système.
- La salle des serveurs est branché directement au groupe électrogène de l'entreprise afin d'éviter une coupure d'électricité.
- Le trafic de données est filtré et protégé par un firewall.
- Le filtrage des informations circulantes dans l'ensemble du réseau sont assurées par les configurations des paramètres des équipements actifs (Switchs et routeurs).
- Tous les postes de travail sont surveillés par un serveur antivirus, en plus de l'antivirus placé sur chaque poste.

- L'entreprise utilise deux postes de managements afin d'assurer le bon fonctionnement de tous les équipements.
- Créations de groupes d'utilisateurs par direction.
- Partage des fichiers entre les utilisateurs et responsable avec des contrôles.
- Création des règles d'accès pour les groupes.
- Utilisation des firewalls pour filtrer les paquets par ouverture ou fermeture de certains ports selon la nécessité.
- Mise à jour des règles de stratégies selon les besoins.

I.3.4.1 VPN

I.3.4.1.1 VPN site à site

La séparation du réseau devient une nécessité primordiale et cela, vu le nombre de poste qui est de plus en plus croissant, il est donc nécessaire d'ajouter une nouvelle ligne spécialisée vers le site centrale pour permettre au réseau d'être moins surchargé, et relier les deux réseaux, qui évolueront désormais indépendamment, par un tunnel sécurisé (VPN), la mise en place d'un VPN site à site assure les propriétés de sécurité ainsi que la confidentialité et l'authentification.

I.3.4.1.2 VPN pour les accès distants

Ce type de VPN peut être utilisé pour accéder à certaines ressources prédéfinies de l'entreprise sans y être physiquement présent. Cette opportunité peut ainsi être très utile aux ingénieurs ou aux cadres qui souhaitent se connecter au réseau de l'entreprise pour divers raisons. En général, l'utilisateur de ce type de VPN possède un accès Internet chez un fournisseur d'accès standard (ISP).

I.3.4.2 Segmentation VLAN

Une meilleure solution pour l'organisation des LANs des stations de la BADR, est la segmentation VLAN en combinant entre les différentes méthodes de regroupement dans un même VLAN. Le mixage des solutions est efficace, vu que chaque méthode apporte un avantage précis. Par conséquent, regrouper les serveurs dans un VLAN pour des besoins de sécurité, ainsi, regrouper les postes des utilisateurs par fonction pour l'accomplissement

Efficace de leur tâches, et s'il y a lieu de regrouper par raison géographique cela permettra d'augmenter les performances réseau, tout en prenant compte du critère de regroupement par volume de trafic pour les ressources fréquemment utilisées ainsi regroupement par apparence logique.

I.3.4.3 Les ACL

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

I.3.4.4 Réseau Multi Services (RMS)

Il existe plusieurs ligne d'interconnection qui suivre la technologie, nous en s'intéresse a Liaison spécialisée qui est une liaison permanente réservée à l'usage exclusif d'un utilisateur. Dédié de chez Algérie Télécom le seul et unique détenteur du marché des lignes spécialisées en Algérie. Elle offre la possibilité de transmission entre deux points de terminaison déterminés du réseau public porte beaucoup d'avantage au réseau de l'entreprise c pour ca en a choisie cette technologie telle que :

- Un transfert rapide de données.
- Une plus grande sécurité dans les émissions/réceptions de données.
- Une communication fiable et de qualité.
- Une interconnexion de sites distants.
- La disposition d'une liaison permanente de manière exclusive évitant ainsi la saturation du réseau.
- Le RMS est un réseau multiservices de nouvelle génération NGN, de type IP/MPLS et d'envergure

  Nationale permet d'ajouter de nouveaux services, tout en simplifiant les réseaux, et en diminuant les coûts des opérations.

Ainsi La solution de raccordement des sites sur notre Backbone RMS permet de garantir et d'offrir:

- Le débit
- La fiabilité
- La qualité de service QOS
- La sécurité
- La disponibilité
- L'extensibilité et la souplesse
- La Redondance (E1 ou DSL)
- De nouveau services (VOIP, Internet, vidéoconférence, ….)

I.3.4.5 WIMAX

En a choisie la technologie WIMAX, il est idéal pour notre entreprise WiMax est une offre complète visant à satisfaire les besoins des entreprises sur une technologie de transmission sans fil à haut débit par ondes radio pouvant atteindre 20Mbits/s avec une portée théorique de 25km.

Cette notion de "sans fil" apporte la rapidité et l'économie de déploiement, une réelle flexibilité, une qualité de service libérée des problèmes des réseaux terrestres. Autrement dit, il est question d'une technologie hertzienne de transmission de données à haut débit. Ce mode de prototype va assurer notre backup de liaison d'interconnexion des deux sites

I.4 Adressage IP Utilisé

Un réseau ne peut bien fonctionner sans une attribution et une configuration correcte de différentes adresses. Le plan d'adressage est une méthode qui s'applique afin de permettre l'accessibilité des différentes entités d'un réseau de la manière la plus optimale.

L'objectif premier du plan d'adressage, est d'éviter la duplication accidentelle des adresses, c'est-à-dire, il permet de désigner un équipement sans ambigüité, car une adresse IP affectée ne doit être réutilisée.

L'élaboration d'un plan d'adressage nécessite la prise en considération de certaines règles, telle que, la classe d'adressage, la définition de sous-réseau, l'attribution statique et/ou dynamique des adresses. De plus, le plan d'adressage élaboré doit comprendre la notion d'évolutivité. En effet, il doit pouvoir s'adapter à la croissance de l'entreprise, permettre un éventuel aménagement avenir et pouvoir accueillir de nouveaux segments VLANs, et tout cela afin de palier aux pénuries d'adresses et sans devoir changer carrément le plan existant.

Après avoir pris ses remarques en considération la DMSI utilise un plan d'adressage IP de type « classe A » qui est la 10.0.0.0.L'adresse de la nouvelle agence sera choisi selon le code numérique de la wilaya qu'elle appartient ainsi que le nombre d'occurrence des agences déjà créer au niveau de cette région.

Pour notre Exemple agence EL HACHIMIA BOUIRA qui prend comme adresse 10.10.10.0/24. Le 10 représente le code numérique de la wilaya de Bouira, le 10 signifie que c'est la 10eme agence créé au niveau de Bouira.

Exemple

Numéro	Nom site	Sous-réseau	Masque
1	Blida	10.9.10.0	255.255.255.0
2	Elhachimia-Bouira	10.10.10.0	255.255.255.0

Tableau I.2 : Les adresses IP attribuées à deux sites de l'entreprise la BADR.

I.5 Critiques et suggestions

Dans cette partie, nous consacrons un ensemble de critiques suite à certaines observations que nous avons faites et nous ont permis de déduire certain suggestions.

I.5.1 Critiques

Nous citons les critiques observés durant notre étude.

- Utilisation de Windows XP au niveau des postes de travails diminue les performances du système.
- Utilisation des machines non performantes qui risque de causer des problèmes du bon fonctionnement du système applicatif de l'agence. Exemple : Installer un Anti-virus Kaspersky qui exige un processeur performant.
- Utilisation des Switchs de 5 ports dans certain bureau diminue le trafic (5 ports en entrée / 1 port en sortie)
- Utilisation du papier comme support de transaction.
- Absence d'un serveur de messagerie.
- Le non fiabilité du réseau en cas de panne d'un équipement informatique au niveau des agences.
- Le non disponibilité de la technologie VoIp dans certaines anciennes agences.
- Effectuation des mis à jours des serveurs de transactions chaque 24 heure peut entrainer des causes de fraude bancaire.
- Non utilisation du déploiement de logicielle dans l'installation d'application au niveau des postes de travails.

I.5.2 Suggestions

Comme nous avons déjà constaté, le réseau de l'entreprise est exposé à un grand risque de pannes. Pour remédier à ce problème, nous allons proposer quelques améliorations pour rendre ce réseau plus fiable. Lors de la conception de la topologie amélioré du réseau, le premier élément dont nous avons tenu compte est le principe d'un modèle de réseau hiérarchique il nous a permis de transformer la topologie du réseau étudiée qui est non hiérarchique en une topologie d'un réseau hiérarchique.

Donc pour le bon fonctionnement de la BADR, nous ne manquerons pas d'apporter notre contribution à travers quelques suggestions par rapport aux remarques faites plus haut.

- Installation de Windows XP Service Pack 3 ou 7 afin de répondre au exigence de l'application logicielle qu'utilise la BADR « Sybu » qui demande la présence du logiciel Internet Explorer 8 ainsi que d'autre logiciels présents dans cette version de Windows.

- Mettre en place des ordinateurs performants qui supportent les critères d'utilisation des logicielle applicatifs de l'entreprise.

- Eliminer le Switch de cinq(5) ports au niveau de chaque bureau et les remplacer par des prises de ports provenant de l'armoire de brassage reliées au Switchs de 24 ports.

- Mettre en place un serveur de messagerie grâce au système MS Exchange 2010 pour assurer le service mail et éliminer la transaction par support de papier.

- Mettre en place la redondance des matériels dans tous les points de réseau pour assurer la fiabilité et la disponibilité du réseau.

- Introduire la technologie VoIP sur le réseau de l'entreprise afin de diminuer les factures téléphoniques et les dépenses de communications.

- Former les employés qui utilisent les applications de gestion sur le principe de fonctionnement des applications et surtout sur l'aspect sécuritaire dans la manipulation de ces logiciels pour une meilleure manipulation et une meilleure performance.

- Proposition d'une solution de mis a jours concernant les transactions afin de les centraliser au niveau d'un serveur central unique (Modèle Flex Cube).

I.6 Problématique

La conception d'architecture du modèle type est l'une des étapes essentielles permettant d'assurer la rapidité et la stabilité d'un réseau. Si un réseau n'est pas conçu adéquatement, de nombreux problèmes imprévus peuvent subvenir, ce qui peut entraver son fonctionnement.

Après l'évaluation des besoins de l'entreprise et l'analyse du périmètre fonctionnel de son réseau, nous retenons en compte quelque élément prise en charge :

- La superficie du local dispose de trois étages dont un rez-de-chaussée.
- Le réseau local doit être subdivisé en plusieurs sous-réseaux.
- Chaque sous-réseau doit appartenir à un groupe de service fonctionnel.
- Chaque étage contient un espace de travails réservé aux utilisateurs de différent groupe de service.
- L'interconnexion est assurée par le bloc du rez-de-chaussée grâce à des liaisons d'interconnexion.
- Le nombre de postes de travail est de 50.
- La sécurité doit être assurée par une stratégie de sécurité fiable afin de protéger les données circulant de l'intérieur du réseau local ou provenant de l'extérieur.
- Autoriser ou interdire les accès à distance.
- Toute sorte de gestion et management d'équipement doit être assuré par un administrateur externe du site distant de la DMSI.
- Garantir la haute disponibilité au niveau des équipements et des liaisons d'interconnexions.
- Utilisation de la technologie VoIp pour les communications téléphoniques.

Nous devons mettre en priorité les performances, le coût, la tolérance de panne, la rapidité des échanges, la sécurité et d'autres principes. Notre mission est de créer un réseau efficace et optimal possible et réduire autant que possible les risques de fuite ou d'infiltration.

I.7 Solution proposée

La solution consiste à segmenter le réseau actuel du Bloc en créant plusieurs sous réseau (Vlan) pour séparer les flux des différents utilisateurs. Cette segmentation va nous permettre d'avantages ; Ainsi que dans chaque équipement on va défini des Listes de Contrôle d'Access pour gérer le flux des différents utilisateurs et de bien administré le réseau.

Finalement nous proposons le modèle hiérarchique en trois-couches nommé par sa version anglaise « tree-layers hierarchical internet working design/model » Comme solution de modèle type de conception ainsi d'autre solution en vas les détailler par la suite.

I.8 Conclusion

Cette étude du réseau de l'entreprise nous a permis de comprendre l'architecture de notre réseau et de matérialiser tout ce qu'on a eu à étudier jusque-là, en effet grâce à cette étude nous avons pu critiquer cette architecture, suggérer quelques solutions et proposer une nouvelle architecture pour le réseau. Cette nouvelle architecture demande certes plus d'investissement financier mais offre sans doute une meilleure sécurité et une meilleure souplesse pour le réseau.

Chapitre II
Définitions & concepts

Chapitre II. Définition et concepts

II.1 Introduction

Dans notre mémoire en vas focaliser sur la mise en place d'une architecteur sécurisée convergée d'un site appartenant a l'entreprise la « BADR », la raison pour laquelle en exposera les modèles d'implantation d'un réseau, les technologies d'interconnexion, les différents protocoles utilisés, ainsi qu'aux différents types de stratégie de sécurité.
Dans ce chapitre nous allons soumettre à la présentation des notions de base utilisées en réseaux informatiques, d'une façon plus claire pour bien aider à mieux assimiler le fonctionnement des réseaux.

II.2 Réseau informatique

II.2.1 Définition

Un réseau est un ensemble d'équipements électroniques (ordinateurs, imprimantes, scanners, modems, routeurs, commutateurs...) interconnectés et capables de communiquer (émettre et recevoir des messages) par l'intermédiaire d'un support de communication.

Un réseau informatique permet donc l'échange d'informations (messageries, transfert de fichiers, interrogation de bases de données...) et l'accès aux ressources (ou mise en commun, partage) de certains ordinateurs du réseau (matériel tel qu'imprimante ou modem, puissance de calcul, logiciels).

Les réseaux informatiques sont plus ou moins vastes selon leur taille (nombre de machines) et leur étendue**. [1]**

II.2.2 Type de réseau

Classification des réseaux est fondée sur la notion d'étendue géographique et le débit.

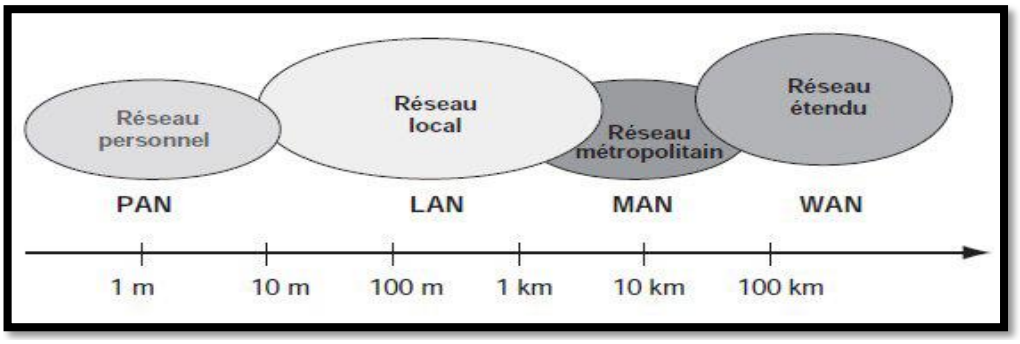


Figure II.4 : Les différents types de réseaux

- **LAN (Local Area Network)** ou réseaux locaux comportent jusqu'à une centaine de machines. C'est le réseau interne de la maison, l'entreprise locale ou de L'établissement scolaire. Deux ordinateurs reliés par un simple câble (pour jouer Par exemple) constituent déjà un LAN. C'est le réseau le plus courant**. [1]**
- **MAN (Metropolitan Area Network)** sont des réseaux étendus à l'ensemble d'une agglomération ou à plusieurs bâtiments d'une entreprise peu éloignés les une des autres. Il s'agit généralement de petits réseaux locaux interconnectés. **[1]**
- **WAN (Wide Area Network)** sont des réseaux étendus à un ou plusieurs pays (succursales d'entreprises) voire au monde entier (Internet). Un WAN regroupe généralement des MAN regroupant eux-mêmes des LAN. **[1]**

II.3 Le modèle OSI (Open Systems Interconnections)

Un aspect important dans l'ouverture des réseaux a été la mise en place d'un modèle de référence, le modèle OSI de l'ISO. Celui-ci définit un modèle en sept couches réseau, présentes sur chaque station qui désire transmettre. Chaque couche dispose de fonctionnalités qui lui sont propres et fournit des services aux couches immédiatement adjacentes. Même si le modèle OSI est très peu implémenté, il sert toujours de référence pour identifier le niveau de fonctionnement d'un composant réseau. Ainsi, paradoxalement aujourd'hui, TCP/IP est mis en œuvre partout et même lorsque l'on parle de ce protocole on l'associe aux couches du modèle OSI (postérieur de 10 ans au modèle TCP/IP). **[2]**

II.3.1 Couche physique

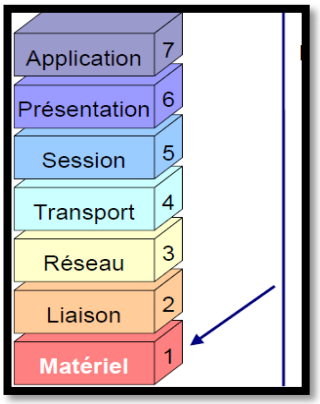


Figure II.5 : couche 1 physique.

Couche matérielle : s'appelle aussi la couche physique Cette première codifie les informations circulant entre machines voisines et gère les données binaires sur le réseau. Elle met en forme des signaux électriques définissant, par valeur de voltage, la mise à 0 ou à 1 des bits et assure le codage des informations. C'est un simple niveau électrique. **[1]**

II.3.2 Couche liaison

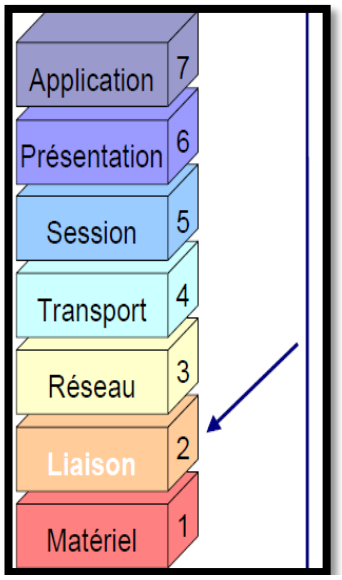


Figure II.6 : Couche 2 liaisons.

La couche liaisons: Si un ordinateur désire envoyer des données sur une autre machine du réseau, en premier lieux il doit connaître son adresse. Tous les composants d'un réseau possèdent en interne une carte ou du matériel compatible avec une adresse physique unique au monde (adresse MAC). Pour assurer la livraison des données, il faut leur y associer l'adresse du destinataire, l'adresse de l'ordinateur expéditeur, des octets de contrôle et le type (ou la longueur) des données à livrer. Toutes ces informations sont regroupées dans une trame. **[1]**

Grâce à sa fiabilité de transfert, comprenant entre autres les dispositifs de détection et de correction d'erreurs, ainsi que les systèmes de partage de supports. Ex Ethernet

II.3.3 Couche réseau

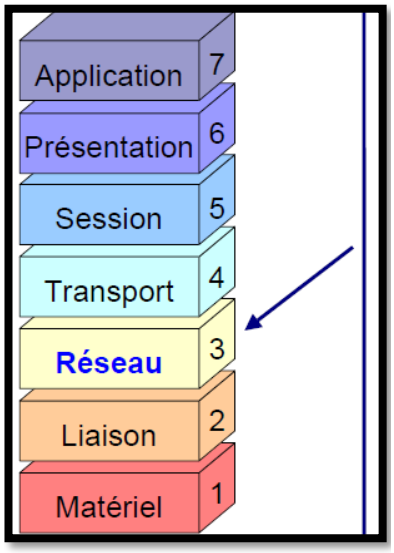


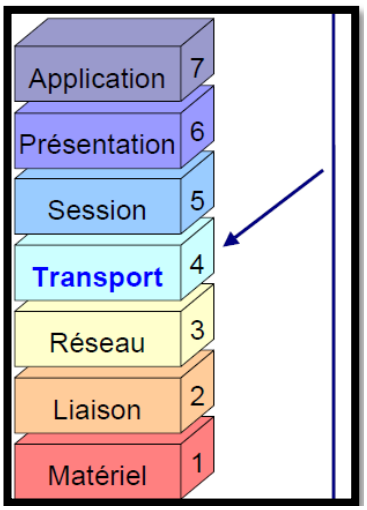
Figure II.7 : couche 3 réseaux.

Couche réseau : consiste à déterminer une route pour acheminer les données à destination le routage des paquets ainsi que l'interconnexion des différents réseaux.

La couche 3 utilise quatre processus de base ; l'adressage, l'encapsulation, le routage, et le décapsulage. **[1]**

Ex protocole IP.

II.3.4 Couche transport

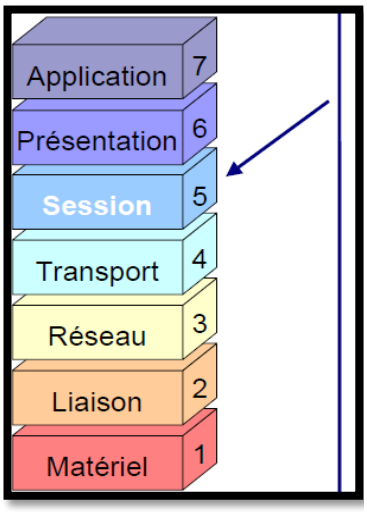


Couche transport : Gère le fractionnement le réassemblages en paquet du flux de données à transmettre, le routage ayant pour conséquence un arrivage des paquets dans un ordre incertain, cette couche s'occupe ainsi réagencement ordonnée de tout les paquets d'un même message.

Les deux protocoles pouvant assuré les services de cette couche sont TCP, UDP. **[1]**

Figure II.8 : Couche 4 transports.

II.3.5 Couche session

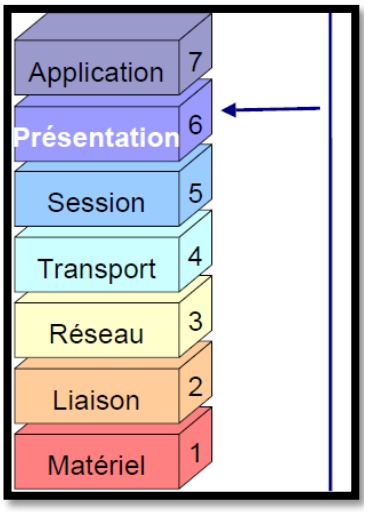


Couche session : Avant même la transmission des données, les deux machines qui veulent Transférer ces données entament un dialogue pour se mettre d'accord sur le

Protocole à utiliser. C'est cette couche qui se charge de ce travail de mise en relation. **[1]**

Figure II.9 : Couche 5 sessions.

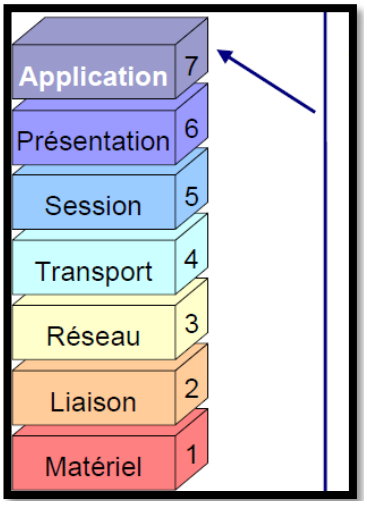
II.3.6 Couche présentation



Couche présentation s'assure que les données reçues sont compatibles avec l'application à laquelle elles sont destinées. Elle s'occupe aussi du cryptage et du décryptage si nécessaire. **[1]**

Figure II.10 : Couche 6 présentations.

II.3.7 Couche application



Couche application : fait le lien entre les logiciels manipulés par l'utilisateur et les utilitaires spécialisés dans les services réseau qui sont transparents pour ce même utilisateur, exemple le transfert de fichier. **[1]**

Figure II.11 : couche 7 applications.

II.3.8 Les Avantages du modèle OSI

Une division de la communication réseau en éléments plus petits et plus simples pour :

- ✓ une meilleure compréhension.
- ✓ L'uniformisation des éléments afin de permettre le développement multi Constructeur.
- ✓ La possibilité de modifier un aspect de la communication réseau sans modifier

Pour communiquer entre les couches et entre les hôtes d'un réseau, OSI a recourt au principe d'encapsulation**.**

Encapsulation : processus de conditionnement des données consistant à ajouter une En-tête de protocole déterminé avant que les données ne soient transmises à la couche Inférieure**. [3]**

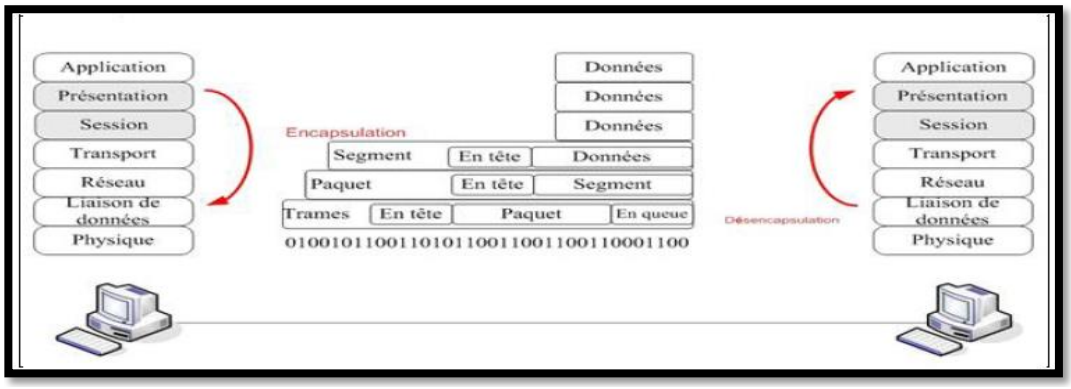
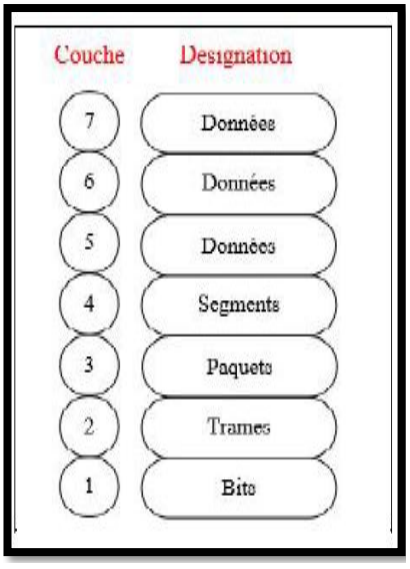


Figure II.12 : Encapsulation / Décapsulation



Lorsque 2 hôtes communiquent, on parle de communication d'égal à égal, c'est-à-dire que la couche N de la source communique avec la couche N du destinataire. Lorsqu'une couche de l'émetteur construit des données, elle encapsule ces dernières avec ses informations puis les passe à la couche inférieure. Le mécanisme inverse à lieu au niveau du destinataire ou une couche réceptionne les données de la couche inférieure, enlève les informations la concernant, puis transmet les informations restantes à la couche supérieure. Les données transitant à la couche N de la source sont donc les mêmes que les données transitant à la couche N du destinataire.

Pour identifier les données lors de leur passage au travers d'une couche,

L'appellation PDU (Unité de données de protocole) est utilisée. **[3]**

Figure II.13 : Désignation de Couches

II.4 Le modèle TCP/IP

II.4.1 Présentation de TCP/IP

TCP/IP représente d'une certaine façon l'ensemble des règles de communication sur internet et se base sur la notion adressage IP, c'est-à-dire le fait de fournir une adresse IP à chaque machine du réseau afin de pouvoir acheminer des paquets de données. Etant donné que la suite de protocoles TCP/IP a été créée à l'origine dans un but militaire, elle est conçue pour répondre à un certain nombre de critères parmi lesquels :

- Le fractionnement des messages en paquets ;
- L'utilisation d'un système d'adresses ;
- L'acheminement des données sur le réseau (routage) ; **[4]**

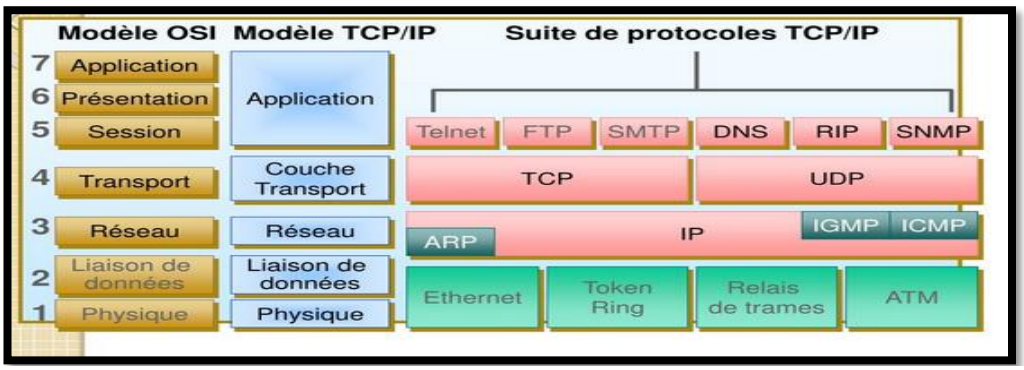
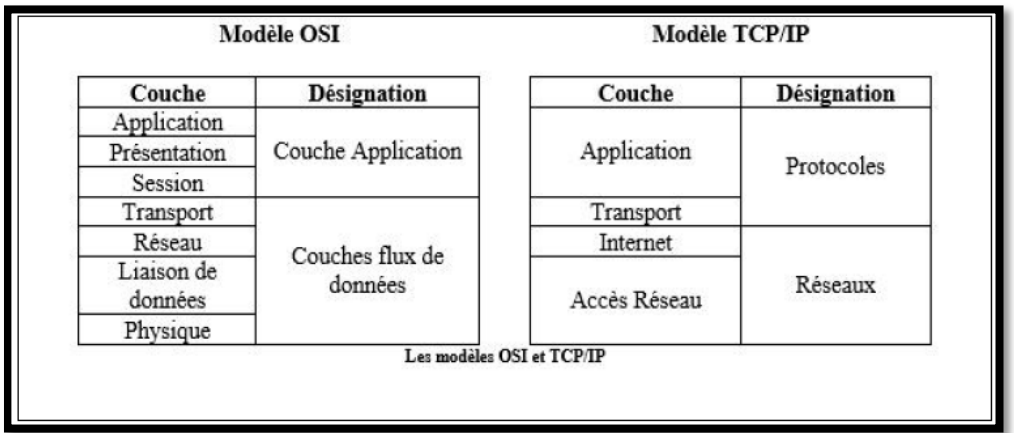


Figure II.14 : différence entre modèle OSI &TCP/IP.

II.4.2 Comparaison entre le modèle TCP/IP et le modèle OSI

Ces deux modèles sont très similaires, dans la mesure où les 2 sont des modèles de Communication à couche et utilisent l'encapsulation de données.
On remarque cependant deux différences majeures :

- TCP/IP regroupe certaines couches du modèle OSI dans des couches plus générales.
- TCP/IP est plus qu'un modèle de conception théorique, c'est sur lui que repose le réseau. **[4] [3]**



Les modèles OSI et TCP/IP

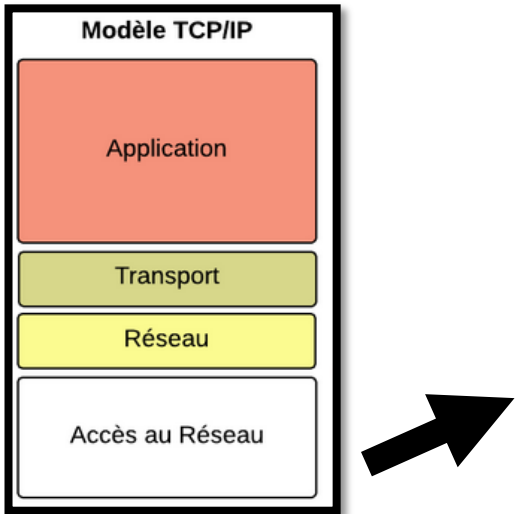
Figure II.15 : Comparaison entre OSI et TCP/IP

II.4.3 Description des couches de TCP/IP

Le modèle TCP/IP est fondé sur **quatre couches** qui enveloppent les messages originaux avant qu'ils soient placés sur le support physique sous forme d'ondes représentant les données de la communication.

Chaque couche assure une fonction de maintenance et de service de la communication. TCP/IP ne se préoccupe pas du contenu (les propos tenus par les utilisateurs dans les messages); il se contente d'assurer des fonctions qui facilitent les communications, le partage et la diffusion des informations**. [4] [5] [6]**

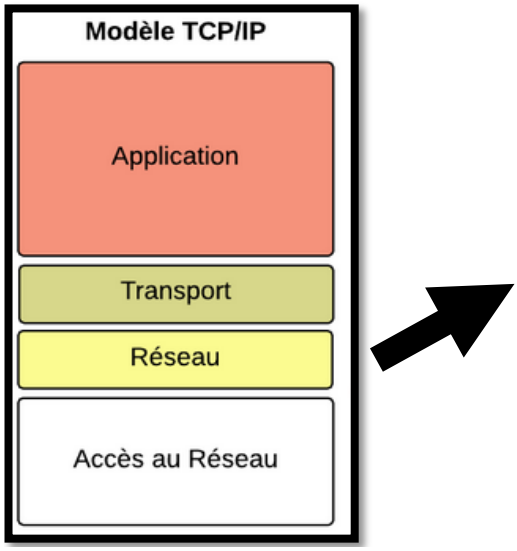
➢ Couche accès au réseau



Accès au réseau : Il regrouper les couches physique et liaison de données du modèle OSI. En fait, cette couche n'a pas vraiment été spécifiée ; la seule contrainte de cette couche, c'est de permettre un hôte d'envoyer des paquets IP sur le réseau. L'implémentation de cette couche est laissée libre. De manière plus concrète, cette implémentation est typique de la technologie utilisée sur le réseau local. Par exemple, beaucoup de réseaux locaux utilisent Ethernet ; Ethernet est une implémentation de la couche hôte-réseau. **[8]**

Figure II.16 : Couche Accès au réseau

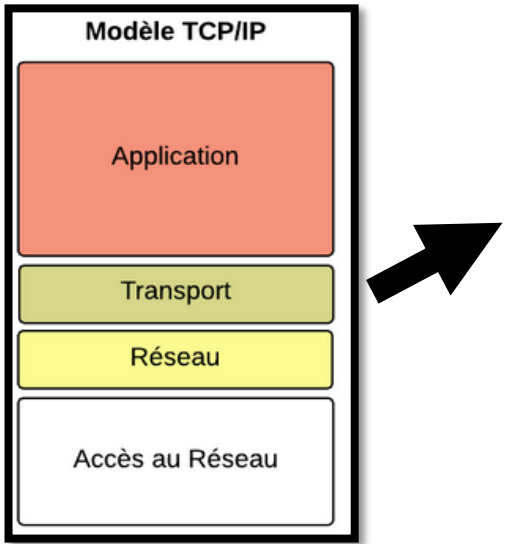
➢ Couche réseau



Réseau : est la couche la plus importante car c'est elle qui définit les datagrammes, et qui gère les notions d'adressage IP. Elle permet l'acheminement des datagrammes (paquets de données) vers des machines distantes ainsi que de la gestion de leur fragmentation et de leur assemblage à réception. Contient 5 protocoles IP, ARP, ICMP. **[8]**

Figure II.17 : Couche Réseau

➢ Couche transport

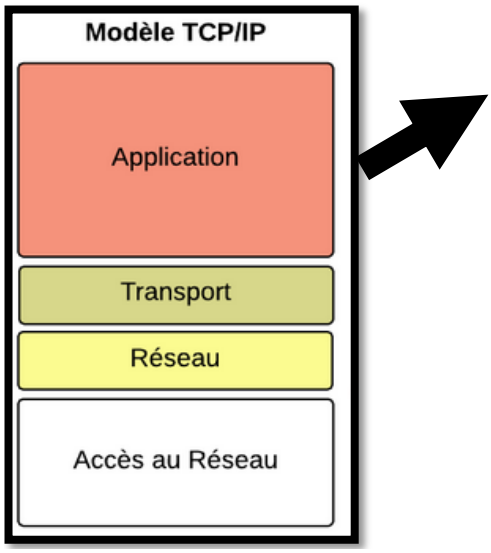


Couche transport : permet à des applications tournant sur des machines distantes de communiquer. Le problème consiste à identifier ces applications. En effet, suivant la machine et son système d'exploitation, l'application pourra être un programme, une tâche, un processus... De plus, la dénomination de l'application peut varier d'un système à un autre, c'est la raison pour laquelle un système de numéro a été mis en place afin de pouvoir associer un type d'application à un type de données, ces identifiants sont appelés port.

Contient 2 protocoles TCP, UDP. **[8]**

Figure II.18 : Couche Transport.

➢ Couche application

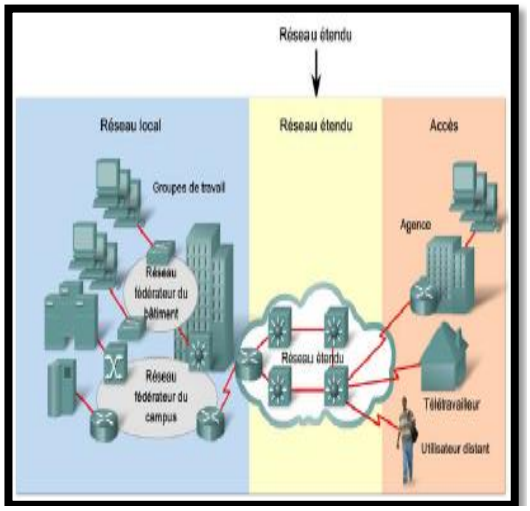


Couche application: située au sommet des couches de protocoles TCP/IP. Celle-ci contient les applications réseaux permettant de communiquer grâce aux couches inférieures. Les logiciels de cette couche communiquent donc grâce à un des deux protocoles de la couche inférieure (la couche transport) c'est-à-dire TCP ou UDP.

Les applications de cette couche sont de différents types, mais la plupart sont des services réseau. **[8]**

Figure II.19 : Couche Application

II.5 Support de transmission dans les réseaux étendus



Pour que deux ordinateurs ou équipements réseau communiquent entre eux, il faut qu'ils soient reliés par quelque chose qui leur permet de transmettre de l'information. Ce quelque chose est ce qu'on appelle un support de transmission, qui est souvent un simple câble réseau, composé d'un fil de cuivre ou de fibre optique. Dans d'autres cas, la transmission se fait sans fils, avec des technologies à base d'infrarouges, d'ondes radio ou de micro-ondes. On pourrait notamment citer le WIFI, le Bluetooth, et bien d'autres. Pour résumer, il existe deux types de supports de communication : les câbles réseaux et les sans-fils**. [7]**

Figure II.20 : exemple réseau étendue.

II.5.1 Les liaisons spécialisées

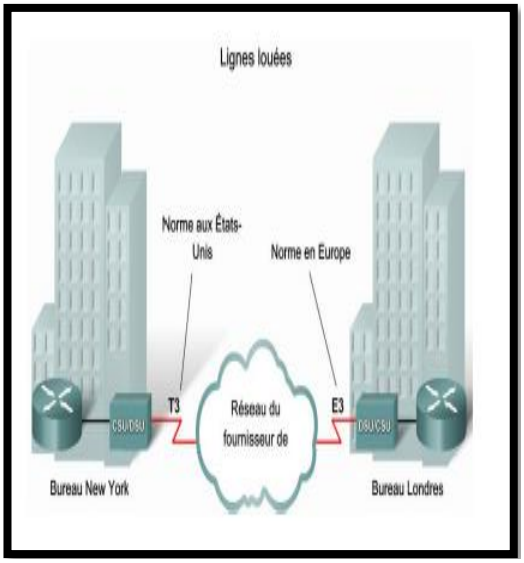


Figure II.21 : exemple lignes louées.

Elle offre la possibilité de transmission entre deux points de terminaison déterminés du réseau public. Appelées aussi lignes louées, fait référence Au fait que l'organisation paie tous les mois un certain montant a un fournisseur de services pour les utiliser. Elles présentent des capacités variées et leur prix dépend de la bande passante requise ainsi que la distance entre les deux points de connexion.

Elles portent plus d'avantage tel que la simplicité la sécurité la disponibilité.

Les liaisons spécialisées reposent sur deux technologies :

- T1 (USA, Canada et Japon) E1 (reste du monde) qui date des années 60.
- HDSL qui date des années 80. **[8]**

II.5.2 LE WIMAX (Worldwide interopérabilité for Microwave Access)

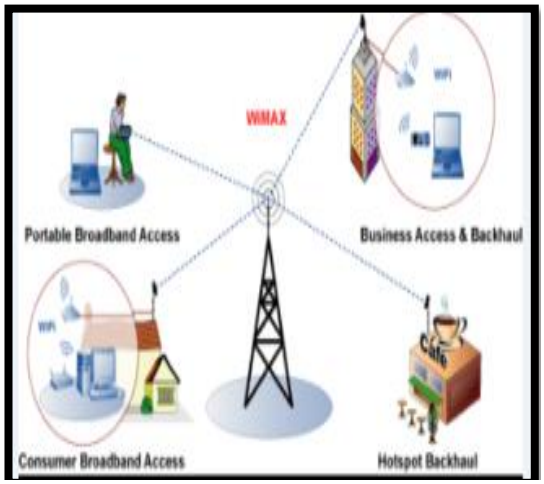


Figure II.22 : WIMAX.

Le WiMax est une technologie radio récent de norme (IEEE 802.16) permettant la transmission de données en haut débit par voie hertzienne.est conçue des le départ pour couverture de zones importante.

Il permet de mettre en place une liaison multipoint entre plusieurs émetteur/récepteur centralisées couvrent une zone ou se situent de multiple terminaux. Le débit réel lors de présence de l'obstacle ne pourra excéder 20Mbit/s.

Il fonctionnera semblablement au wifi mais avec une vitesse plus grand et distance ; et un nombre important des utilisateurs**. [9]**

II.6 Les équipements de base d'un réseau informatique

Les équipements réseau, ou périphériques réseau, sont les équipements physiques nécessaires à la communication et à l'interaction entre les appareils d'un réseau informatique.

Nous avons plusieurs équipements, nous pouvons citer **[10]** :

II.6.1 Les unités hôtes

Les hôtes sont des unités directement connectées à un segment de d'imprimantes. Réseau, nous pouvons les retrouver sous forme d'ordinateurs, de serveurs, de scanners ou

II.6.2 Les commutateurs ou Switchs

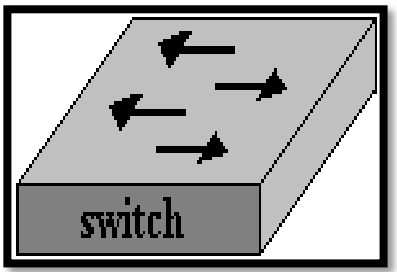
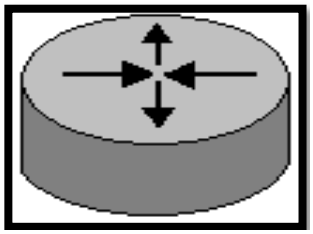


Figure II.23 : SWITCH.

Un commutateur est un équipement qui relie plusieurs câbles ou fibres dans un réseau informatique ou un réseau de télécommunication. Les commutateurs permettent de créer des circuits virtuels et de diriger les informations vers une destination précise sur le réseau. L'utilisation de Switchs permet de sécuriser les informations transmises sur le réseau à la différence des

Concentrateurs qui envoient les informations sur tous les ordinateurs, les Switchs envoient les données uniquement aux destinataires qui doivent les recevoir. La commutation est un mode de transport de trame au sein d'un réseau informatique et de communication. **[10]**

II.6.3 Les routeurs



Un routeur est un élément intermédiaire qui permet de relier deux réseaux. Il assure le routage des paquets d'une interface à une autre. Il opère au niveau de la troisième couche du modèle OSI (la couche réseau).

Figure II.24 : Router.

La plupart des routeurs sont capables de déterminer automatiquement l'itinéraire le plus adapté entre le départ et la destination à l'aide des adresses, ce qui permet d'acheminer le paquet avec le meilleur itinéraire. Pour diriger les informations, le routeur doit comprendre le protocole utilisé, qui est un langage que les ordinateurs utilisent pour communiquer, comme par exemple : TCP/IP, TCP, IP. **[10]**

II.6.4 Les modems (Modulateur-Démodulateur)

Modem est de plus en plus important d'avoir la connexion internet à proximité, où que l'on se trouve désormais. Pour ce faire, il est fréquent que vous entendiez parler modem internet. On en retrouve dans les entreprises, les écoles, dans les maisons et bien d'autres lieux**. [11]**

Figure II.25 : Modem

Est le périphérique utilisé pour adapte les données numériques issues de l'ordinateur en données (analogiques ou numériques) exploitables par le réseau téléphonique. C'est la modulation. La démodulation fait le contraire, elle adapte les données récupérées sur le réseau téléphonique en données compréhensibles par l'ordinateur. **[1]**

II.7 Les protocoles utilisés dans les interconnexions réseau

II.7.1 Les protocoles de niveau physique (couche1)

La couche physique est chargée de la transmission effective des signaux électriques, radiofréquences ou optiques entre les interlocuteurs.

II.7.1.1 La technologie DSL (Digital Subscriber Line)

La DSL «Digital Subscriber Line» est un ensemble de technologies qui permettent de transmettre les données numériques via Internet à travers les câbles téléphoniques. Les lignes de raccordements téléphoniques utilisées dans ce type de transmission sont adaptées pour transmettre les données numériques en plus du signal vocal.

Cette transmission de données numériques se fait donc sans affecter la qualité de la transmission vocale. L'ensemble de ces technologies est reconnu également sous le nom de «ligne d'abonné numérique». La DSL est en général utilisée pour la transmission à haute vitesse des données numériques, elle est compatible pour des applications professionnelles ainsi que résidentielles. Elle est également plus stable que le câble.

On parle souvent de xDSL, qui est tout simplement des variantes de la DSL, le x étant une variable qui varie en fonction de l'application et de la vitesse de la variante DSL. En général, ces variantes sont regroupées en 2 catégories : les variantes symétriques et asymétriques. **[12]**

II.7.2 Les protocoles de niveau liaison (couche 2)

La couche de liaison de données est la couche de protocole qui transfère des données entre les nœuds adjacents d'un réseau étendu (WAN) ou entre des nœuds sur le même segment d'un réseau local (LAN).

II.7.2.1 Le protocole PPP (Point-to-point Protocol)

Le protocole PPP offre des mécanismes standards pour le transport de datagrammes provenant de différents protocoles, sur un lien de point à point. Chaque datagramme est encapsulé dans un paquet PPP, qui a une structure similaire à HDLC.

La partie message d'un paquet PPP a trois champs, soit l'identifiant du protocole utilisé, l'information encapsulée dans le paquet et une zone de "padding", tel qu'illustré ci-dessous (MRU = Maximum Receive Unit = Information + Padding).

On retrouve différents types de protocoles pouvant être encapsulés dans des datagrammes PPP :

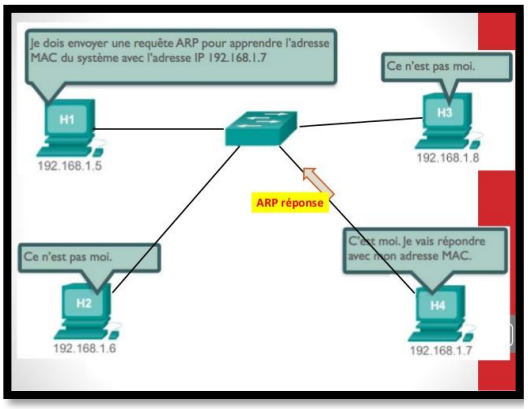
- les protocoles de gestion des datagrammes (ex. Link Control Protocol (LCP)).
- les protocoles de gestion de la couche réseau, appelés les Network Control Protocols (NCP).
- les protocoles de la couche réseau. **[12]**

II.7.3 Les Protocoles de niveau réseau (Couche 3)

II.7.3.1 Protocole IPv4 (Internet Protocol Version 4)

IPv4 désigne la version 4 du protocole Internet (IP). Il s'agit de la version actuellement la plus utilisée dans le monde pour attacher une adresse IP à un ordinateur. Cette dernière prend la forme d'une succession de chiffres décimaux (4 avec l'IPv4), comme 182.23.178.44. L'**IPv4** est encore aujourd'hui à la base d'une grande partie des communications sur Internet. Inventée dans les années 1970, elle est définie par la RFC 791, datée de septembre 1981 (un document décrivant officiellement les aspects techniques d'Internet). Depuis 2011, on annonce le fait qu'elle soit amenée à être progressivement remplacée par l'IPv6. Avec la multiplication du nombre d'ordinateurs reliés au réseau Internet, l'**IPv4** est officiellement arrivée à court de possibilités pour offrir des combinaisons d'adresse IP. La transition vers l'IPv6 permettra d'éviter l'implosion d'Internet. **[13]**

II.7.3.2 Protocole ARP (Address Resolution Protocol)

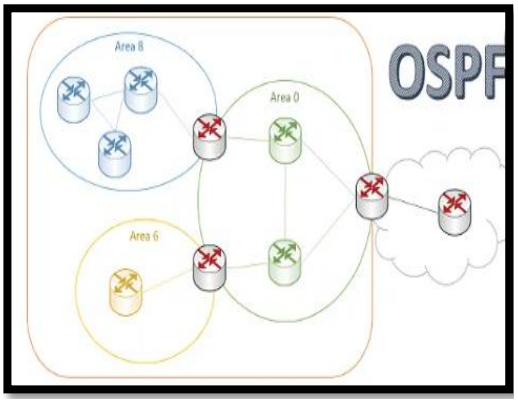


ARP permet de connaitre l'adresse physique d'une carte réseau correspondant à une adresse IP .pour établir cette correspondance, le protocole ARP interroge les machines du réseau pour connaitre leur adresses physiques et crée ainsi une table de correspondance

Figure II.26: Représentation de protocole ARP.

Entre les adresses logiques et les adresses physiques dans une mémoire cache appelée table ARP**. [14]**

II.7.3.3 Protocole OSPF (Open Shortest Path First)



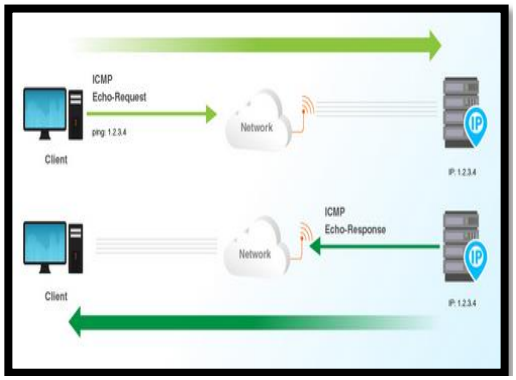
Le protocole OSPF (Open Shortest Path First) est un protocole de routage intérieur qui est utilisé dans les réseaux de grande taille. Avec le protocole OSPF, un routeur qui détecte une modification dans sa table de routage ou dans le réseau envoie immédiatement une mise à jour par multidiffusion à tous les autres routeurs du réseau.

Figure II.27: représentation de protocole OSP

Notez également la caractéristique suivante à propos du protocole OSPF :

- Si vous possédez plusieurs zones OSPF, l'une d'entre elles doit être la zone 0.0.0.0 (la zone principale).
- Toutes les zones doivent être adjacentes à la zone principale. Si ce n'est pas le cas, vous devez configurer une liaison virtuelle à la zone principale. **[15]**

II.7.3.4Protocole ICMP (Internet Control Message Protocol)



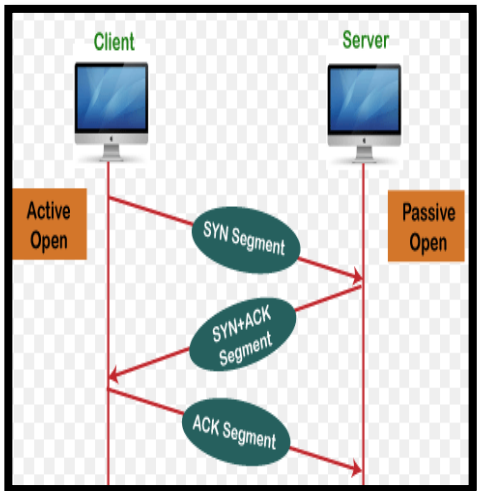
ICMP (Internet Control Message Protocol) est un protocole qui permet de gérer les informations relatives aux erreurs aux machines connectées. Etant donné le peu de contrôles que le protocole IP réalise, il permet non pas de corriger ces erreurs mais de faire part de ces erreurs aux protocoles des couches voisines.

Figure II.28 : représentation de protocole ICMP

Ainsi, le protocole ICMP est utilisé par tous les routeurs, qui l'utilisent pour signaler une erreur (appelé Delivery Problem). Les messages d'erreur ICMP sont transportés sur le réseau sous forme de datagramme, comme n'importe quelle donnée. Ainsi, les messages d'erreur peuvent eux-mêmes être sujet d'erreurs. **[16]**

II.7.4 Les protocoles de niveau transport (Couche 4)

II.7.4.1 Le protocole TCP (Transmission Control Protocol)



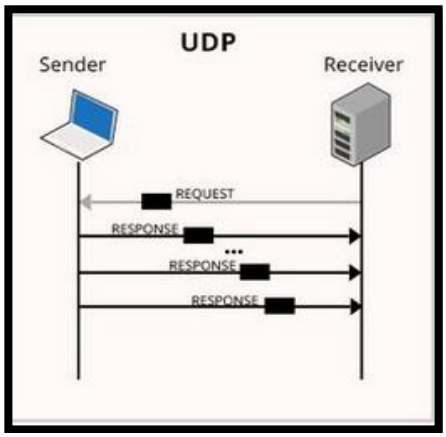
TCP (qui signifie Transmission Control Protocol, est un des principaux protocoles de la couche transport du modèle TCP/IP. Il permet, au niveau des applications, de gérer les données en provenance (ou à destination) de la couche inférieure. Lorsque les données sont fournies au protocole IP, celui-ci les encapsule dans des datagrammes IP, en fixant le champ protocole à 6. **[17]**

Figure II.29 : Représentation de protocole TCP

TCP est un protocole orienté connexion, c'est-à-dire qu'il permet à deux machines qui communiquent de contrôler l'état de la transmission. Les caractéristiques principales du protocole TCP sont les suivantes :

- TCP permet de remettre en ordre les datagrammes en provenance du protocole IP
- TCP permet de vérifier le flot de données afin d'éviter une saturation du réseau
- TCP permet de formater les données en segments de longueur variable afin de les "remettre" au protocole IP
- TCP permet de multiplexer les données, c'est-à-dire de faire circuler simultanément des informations provenant de sources (applications par exemple) distinctes sur une même ligne
- TCP permet enfin l'initialisation et la fin d'une communication de manière courtoise

II.7.4.2Le protocole UDP (User Datagram Protocol)



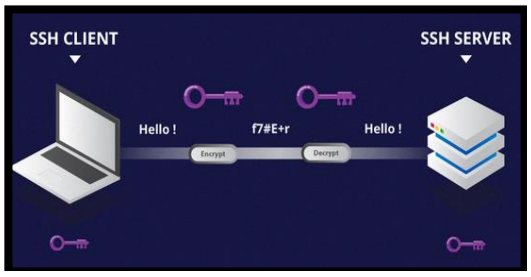
UDP protocole permettant l'**envoi sans connexion de datagrammes** dans des réseaux basés sur le protocole IP. Afin d'atteindre les services souhaités sur les hôtes de destination, le protocole utilise des ports qui constituent un élément essentiel de l'entête UDP, fait partie de la **suite des protocoles Internet.**

Figure II.30 : représentation de protocole UDP

Il intervient au niveau de la **couche transport** et joue ainsi le rôle d'intermédiaire entre la couche réseau et la couche application.

En utilisant UDP, une application peut donc envoyer très rapidement des informations, étant donné qu'aucune connexion au destinataire n'est établie et qu'aucune réponse ne doit être attendue. En revanche, il n'y a aucune garantie que les paquets arrivent **entiers** et dans le même **ordre** que celui dans lequel ils ont été envoyés. Par ailleurs, le protocole n'offre aucune protection contre les manipulations ou accès de tiers. Les paquets erronés peuvent toutefois être identifiés à l'aide d'une **somme de contrôle facultative** (obligatoire avec IPv6). **[17]**

II.7.4.3 Le Protocole SSH (Secure Shell)



SSH permettant à un client (un utilisateur ou bien même une machine) d'ouvrir une session interactive sur une machine distante (serveur) afin d'envoyer des commandes ou des fichiers de manière sécurisée :

Figure II.31: représentation de protocole SSH

Les données circulant entre le client et le serveur sont chiffrées, ce qui garantit leur confidentialité (personne d'autre que le serveur ou le client ne peut lire les informations transitant sur le réseau). Il n'est donc pas possible d'écouter le réseau à l'aide d'un analyseur de trames

- Le client et le serveur s'authentifient mutuellement afin d'assurer que les deux machines qui communiquent sont bien celles que chacune des parties croit être. Il n'est donc plus possible pour un pirate d'usurper l'identité du client ou du serveur (spoofing).
- La version 1 du protocole (SSH1) proposée dès 1995 avait pour but de servir d'alternative aux sessions interactives (shells) telles que Telnet, rsh, rlogin et rexec. Ce protocole possédait toutefois une faille permettant à un pirate d'insérer des données dans le flux chiffré.
- La version 2 du protocole (SSH2) propose également une solution de transfert de fichiers sécurisé (SFTP, Secure File Transfer Protocol). **[18]**

II.8 La haute disponibilité et l'équilibre des charges

II.8.1 Définition de la haute disponibilité

La haute disponibilité est un terme souvent utilisé en informatique, à propos d'architecture de système ou d'un service pour désigner le fait que cette architecture ou ce service a un taux de disponibilité convenable, cette dernière concerne de plus en plus d'entreprises comme de particuliers. On appelle haute disponibilité (high avaiability) toutes les dispositions visant à garantir la disponibilité d'un service, c'est-à-dire assurer le bon fonctionnement de ce dernier. **[12]**

II.8.2 Définition de l'équilibre des charges

L'équilibre des charges est une fonctionnalité standard du logiciel du routeur de Cisco IOS, et est disponible à travers toutes les plateformes de routeur. Il est inhérent au processus de transfert dans le routeur et est automatiquement activé si la table de routage a plusieurs chemins vers une destination. Il est basé sur des protocoles de routage standards, tels que le Protocole d'informations de routage (RIP), (EIGRP) et (OSPF) ou dérivé de mécanismes de transfert de paquets et de routes configurées statiquement. Tels que ces quelques protocoles que nous allons définir ci-dessous, Il permet à un routeur d'utiliser plusieurs chemins vers une destination lors du transfert de paquets. **[12]**

II.8.3 Le Protocole HSRP (Hot Standby Routing Protocol)

HSRP est un protocole propriétaire Cisco qui a pour fonction d'accroitre la haute disponibilité dans un réseau par une tolérance aux pannes. Cela se fait par la mise en commun du fonctionnement de plusieurs routeurs physiques (au minimum deux) qui, de manière automatique, assurerons la relève entre eux, c'est-à-dire d'un routeur à un autre. Plus précisément, la technologie HSRP permettra aux routeurs situés dans un même groupe que l'on nomme "standby group" de former un routeur virtuel qui sera l'unique passerelle des hôtes du réseau local. En se cachant derrière ce routeur virtuel aux yeux des hôtes, les routeurs garantissent en effet qu'il y est toujours un routeur qui assure le travail de l'ensemble du groupe. Un routeur dans ce groupe est donc désigné comme "actif" et ce sera lui qui fera passer les requêtes d'un réseau à un autre. Pendant que le routeur actif travaille, il envoie également des messages aux autres routeurs indiquant qu'il est toujours "vivant" et opérationnel. Si le routeur principal (élu actif) vient de tomber, il sera automatiquement remplacé par un routeur qui était alors jusqu'à présent "passif" et lui aussi membre du groupe HSRP. Aux yeux des utilisateurs

toutefois, cette réélection et ce changement de passerelle sera totalement invisible car ils auront toujours pour unique passerelle le routeur virtuel que forment les routeurs membres du groupe HSRP. Le routeur virtuel aura donc toujours la même IP et adresse MAC aux yeux des hôtes du réseau même si en réalité il y a un changement du chemin par lequel transitent les paquets. **[12]**

II.9 Les virtuel LAN (VLAN)

II.9.1 Définition

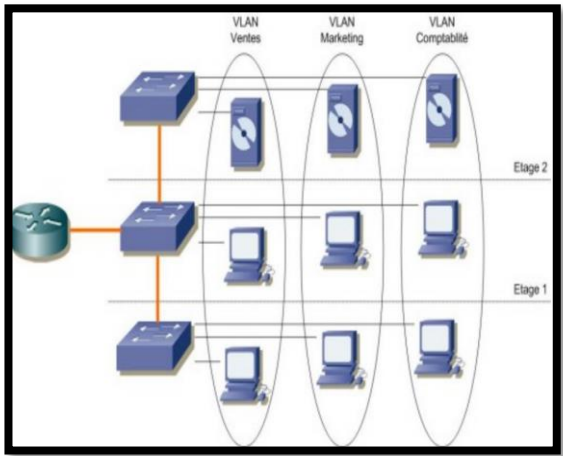


Figure II.32 : Représentation de VLAN

Les réseaux virtuels (Virtual LAN) sont apparus comme une nouvelle fonctionnalité dans l'administration réseau avec le développement des commutateurs. La notion de VLAN est un concept qui permet de réaliser des réseaux de façon indépendante du système de câblage. Ces réseaux permettent de définir des domaines de diffusions restreints, cela signifie qu'un message émis par une station du VLAN ne pourra être reçu que par les stations de ce même VLAN.

Un VLAN, est donc, un regroupement logique, et non physique, de plusieurs stations grâce à des critères (adresses MAC, numéros de port, protocole, etc.). Pour réaliser ce regroupement, on intervient directement, par voie logicielle, sur le ou les éléments actifs que sont les commutateurs VLAN. **[24]**

II.9.2 Type de VLAN

Plusieurs types de VLAN sont définis, selon le critère de commutation et le niveau auquel il s'effectue. **[19]**

- **VLAN niveau 1:**

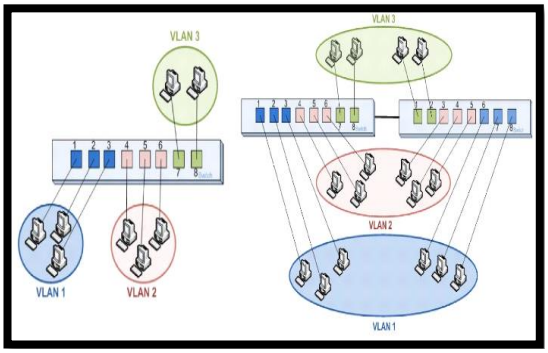
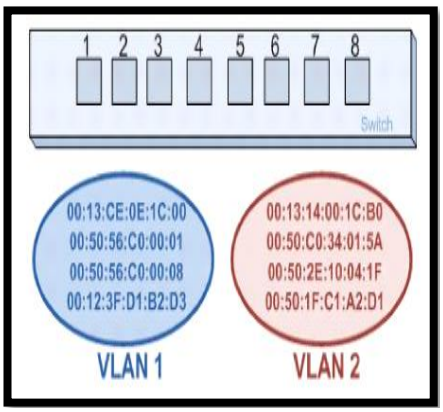


Figure II.33 : exemple de VLAN niveau 1

(Aussi appelés VLAN par port) On affecte chaque port des commutateurs à un VLAN, l'appartenance de chaque port du commutateur à tel ou tel réseau VLAN est configurée manuellement.

- **VLAN niveau 2:**



(Aussi appelé VLAN MAC) consiste à définir un réseau virtuel en fonction des adresses MAC des stations. Ce type de VLAN est plus souple que le VLAN par port car le réseau est indépendant de la localisation de la station.

En faite il s'agit à partir de l'association MAC/VLAN d'affecter dynamiquement les ports des commutateurs à chacun des VLAN.

Figure II.34 : représentation de VLAN niveau 2

- **VLAN niveau 3:** Distingue plusieurs types de VLAN de niveau 3 **[19]**

1. Le VLAN par protocole permet de créer un réseau virtuel par type de protocole regroupant ainsi toutes les machines utilisant le même protocole au sein d'un même réseau.

2. VLAN basés sur les protocoles, protocole de couche 3 transporté par la trame qui permet de déterminer l'appartenance aux réseaux VLAN. Cette méthode peut fonctionner dans un environnement où figurent plusieurs protocoles, mais n'est pas très pratique sur un réseau à prédominance IP.

3. Le VLAN par sous-réseau associe des sous-réseaux selon l'adresse IP source des datagrammes. Ce type de solution apporte une grande souplesse dans la mesure où la configuration des commutateurs se modifie automatiquement en cas de déplacement d'une station

II.9.3 Les avantages du VLAN

- **a flexibilité de segmentation du réseau :** Les utilisateurs et les ressources entre lesquels les communications sont fréquentes peuvent être regroupés sans devoir prendre en considération leur localisation physique. Il est aussi autorisée qu'une station appartienne à plusieurs VLAN en même temps;
- **Performances** : diminution de la taille des domaines de Broadcast.
- **La technologie évolutive et à faible coût :** La simplicité de la méthode d'accès et la facilité de l'interconnexion ont fait d'Ethernet une technologie évolutive à faible coût quelles que soient les catégories d'utilisateurs.
- **L'augmentation considérable des performances du réseau :** Comme le trafic réseau d'un groupe d'utilisateurs est confiné au sein du VLAN qui lui est associé, de la bande passante est libérée, ce qui augmente les performances du réseau **[20]**

II.10 Sécurité Réseau

Cette partie en vas la consacré sur les différent politique de sécurité mise en place dans une architecteur réseau. Cette dernière est devenue une des préoccupations le plus important dans les entreprises soit de protéger le support de stockage, support de transport ainsi les équipements intermédiaires traversés lors du transport**,** tous cherchent à protéger leur données contre des utilisateurs frauduleuses.

- **Interdiction par défaut :** dans la mesure où toutes les menaces ne peuvent être connues à l'avance, il est mieux d'interdire tout ce qui n'est pas explicitement permis que de permettre tout ce qui n'est pas explicitement interdit (sur un firewall, il vaut mieux commencer par fermer tous les ports pour n'ouvrir ensuite que ceux nécessaires).
- **Participation des utilisateurs :** un système de protection n'est efficace que si tous les utilisateurs le supportent, un système trop restrictif pousse les utilisateurs à devenir créatifs.

II.10.1 Les Firewalls

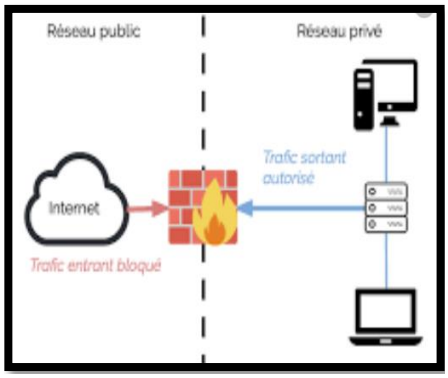


Figure II.35 : exemple de firewal

Un firewall est essentiellement un dispositif de protection qui constitue un filtre entre un réseau local et un autre réseau non sûr tel que l'Internet ou un autre réseau local.

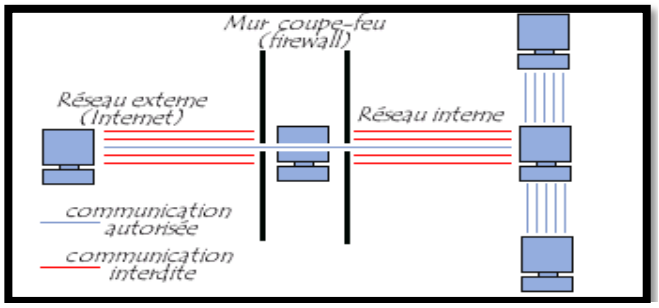
Il laisse entrer le retour légitime du trafic initié d'une zone de confiance comme un LAN. Il tient compte de l'état des sessions de couche 4 établies (TCP, UDP, ICMP, etc.). On parle alors de pare-feu à état **[21]**

Dans un système d'information, les politiques de filtrage et de contrôle du trafic sont placées sur un matériel ou un logiciel intermédiaire communément appelé pare-feu.IL pour fonctionnalités **d'examiner et filtrer le trafic qui le traverse,** L'idée qui prévaut à ce type de fonctionnalité est le **contrôle des flux du réseau TCP/IP.**

Le pare-feu limite le taux de paquets et de connexions actives.

La configuration d'un pare-feu consiste la plupart du temps en un ensemble de règles qui déterminent une action de rejet ou d'autorisation du trafic qui passe les interfaces du pare-feu en fonction de certains critères tels que :

- l'origine et la destination du trafic,
- des informations d'un protocole de couche 3 (IPv4, IPv6, ARP, etc.),
- des informations d'un protocole de couche 4 (ICMP, TCP, UDP, ESP, AH, etc.)
- et/ou des informations d'un protocole applicatif (HTTP, SMTP, DNS, etc.)



Ses règles sont appliquées en fonction de la direction du trafic entrant ou sortant sur une interface, avant ou après le processus de routage des paquets. Cette dernière réalité diffère selon le logiciel ou le matériel choisi pour remplir ces tâches**. [21]**

Figure II.36 : exemple de comportement De firewall

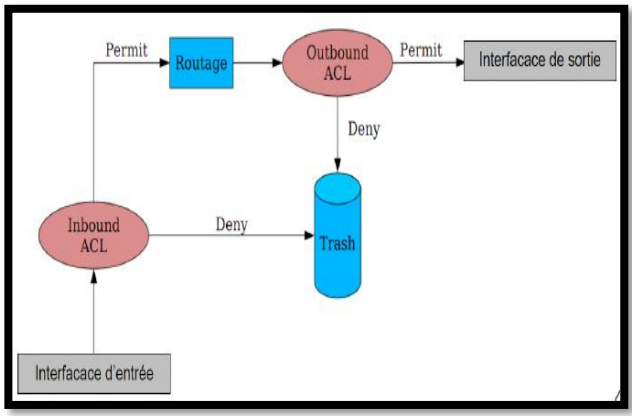
Un système par-feu contient un ensemble des régles cités auparavant permet d'autorisé la connexion, bloque, ou de rejeter.

L'ensemble de ses régles permet de mettre en œuvre une méthode de filtrages dépendant de la politique de sécurité. On distingue habituellement deux types de sécurités

Soit autoriser uniquement les communications ayant été explicitement autorisé **« tout ce qui n'est pas explicitement autorisé est interdit »**.

Soit d'empêcher les échanges qui ont été explicitement interdit. **[21]**

II.10.2 Les ACL



Une liste de contrôle d'accès permet d'autoriser ou de refuser des paquets en fonction d'un certain nombre de critères, tels que :
L'adresse d'origine ; L'adresse de destination ; Le numéro de port. ; Les protocoles de couches supérieures ; Et D'autres paramètres (horaires par exemple). **[22]**

Figure II.37 : Trafic d'ACL

Les listes de contrôle d'accès permettent à un administrateur de gérer le trafic et d'analyser des paquets particuliers ; sont associées à une interface du routeur, et tout trafic acheminé par cette interface est vérifié afin d'y déceler. Certaines conditions faisant partie de la liste de contrôle d'accès.
Les ACL peuvent être créés pour tous les protocoles routés. Il faut donc définir une liste de contrôle d'accès dans le cas de chaque protocole activé dans une interface pour contrôler le flux de trafic acheminé par cette interface.

Nous pourrons résumer le fonctionnement des ACL de la façon suivante :

- Le paquet est vérifié par rapport au 1er critère défini.
- S'il vérifie le critère, l'action définie est appliquée.
- Sinon le paquet est comparé successivement par rapport aux ACL suivants.
- S'il ne satisfait aucun critère, l'action deny (interdire) est appliquée.
- Les critères sont définis sur les informations contenues dans les en-têtes IP, TCP ou UDP.
- Des masques ont été définis pour pouvoir identifier une ou plusieurs adresses IP en une seule définition.
- Ce masque défini la portion de l'adresse IP qui doit être examinée.
- 0.0.255.255 signifie que seuls les 2 premiers octets doivent être examinés.
- deny 10.1.3.0 avec 0.0.0.255 : refus de toutes les IP commençant par 10.1.3
- Les Acls sont donc un composant de sécurité de base, simple et performant.

II.10.2.1 Les différents types d'ACL

Il existe 3 types de liste de contrôle d'accès :

- **Les Acls standards** utilisent des spécifications d'adresses simplifiées et autorisent ou refusent un ensemble de protocole. Les Acls standard sont à appliquer le plus proche possible de la destination en raison de leur faible précision.
- **Les Acls étendues** utilisent des spécifications d'adresses plus complexes et autorisent ou refusent des protocoles précis .Les Acls étendues sont à appliquer le plus proche possible de la source.
- **Les Acls nommées** peuvent être soit standards, soit étendues ; elles n'ont pour but que de faciliter la compréhension et de connaître la finalité de l'ACL. **[23]**

II.11 Conclusion

Nous avons présenté dans ce chapitres Les concepts liés aux technologies de conception et de réalisation d'une architecture réseau informatique ainsi qu'à l'interconnexion des sites distants, les fondements des protocoles utilisés pour véhiculer les données à travers les réseaux ainsi des outils et techniques de sécurisations mis en place, technique que nous avons présentée dans ce chapitre les pare-feux, l, Les VLANs et les ACL, afin de garantir l'intégrité et la confidentialité des données.

Le chapitre suivant va nous présenter tous les éléments qui composent le système actuel de l'entreprise d'accueil, afin d'avoir une connaissance précise du domaine à étudier.

Chapitre III

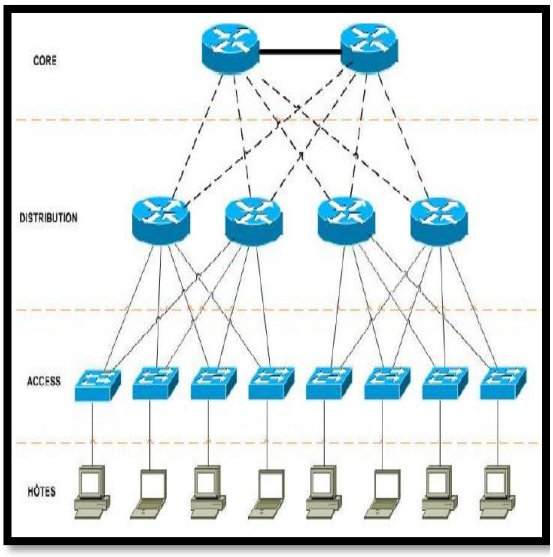
Topologie de la solution Proposée

Chapitre III. Topologie de la solution Proposée

III.1 Introduction

Ce chapitre va décrire l'étude conceptuelle afin la mise en place d'une architecture réseau sécurisé. Cette étude sera réalisée en tenant compte les objectifs de l'entreprise déjà fixés et donnera un aperçu d'un processus de conception d'un modèle type de configuration.
Il sera question de faire des choix du modèle type de conception qui est « design model », les protocoles utilisés pour véhiculer les données de l'entreprise de manière sur et fiable, de l'architecture matérielle avec tous les équipements utilisés pour relier les différents sites de l'entreprise et, enfin, proposer une solution qui garantie une disponibilité accrue des données de l'entreprise.

III.2 Le modèle hiérarchique en trois couches de Cisco



C'est un modèle inventé et diffusé par Cisco. Son principe est de créer un design réseau structuré en trois couches, chaque couche dispose d'un rôle précis impliquant des différences de matériel, performances et outils ce qui rend la conception modulaire et évolutif. **[24]**

Ainsi vous devez respectez certaines règles d'architecture qui leur permettent de répondre aux besoins actuels et futurs des entreprises et de leurs utilisateurs. **[25]**

Figure III.38: Le modèle hiérarchique.

III.2.1 L'importance de « tree-layers hierarchical internetworking design/model »

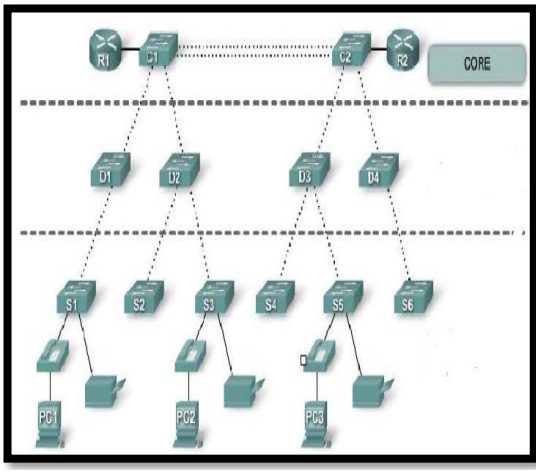
Il faut bien noter que ce modèle il est plus compliqué à mettre en place mais totalement plus efficace, rentable, réfléchi et économe sur le long terme qu'une architecture improvisé au fil du temps. A savoir que chaque couche apporte ses impératifs et ses besoins influençant le matériel mis en place ainsi que les configurations et solutions.

Si un modèle de conception qui facilite le déploiement, la configuration, la maintenance et la mise à jour des infrastructures, on considérera aussi que l'usage d'un tel modèle facilite les achats de matériels et de services**. [25]**

III.2.2 Description des trois couches du modèle type

Dans cette partie en vas décrire en détail les trois couches qui compose « model design ».

➢ La couche cœur « Core layer »



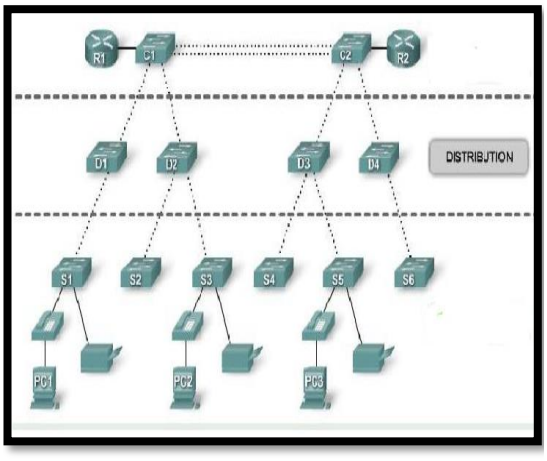
C'est la couche supérieure. Son rôle est relié entre eux les différents segments du réseau, par exemple les sites distants, les LANs ou les étages d'une société. **[26]**

Nous trouvons généralement les routeurs à ce niveau. Il s'appelle aussi Backbone haute vitesse pour transférer rapidement et efficacement les paquets afin d'améliorer la connectivité de réseau.

Figure III.39 : Description la couche cœur

Vue l'importance de cette couche, les périphérique hébergé doivent avoir un degré de fiabilités et de disponibilités .il réagir rapidement au changement de topologie du réseau en redirigeant le trafic, ainsi un degré élever de redondance de périphérique doit adhérer cette couche, aucune manipulation des paquets a ce niveau afin de na pas avoir une ralentit la permutation des paquets. **[26]**

➢ La couche distribution « Distribution layer ».



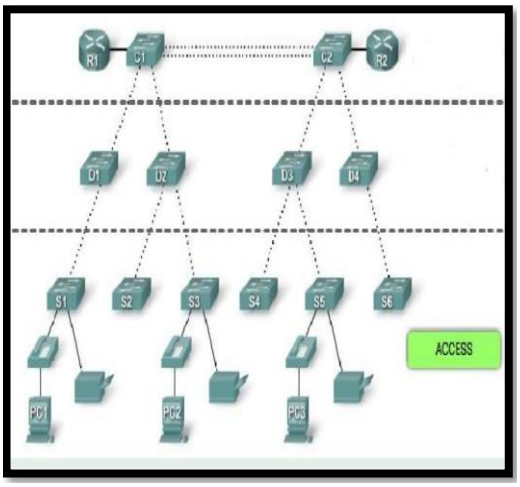
Cette couche a pour rôle de filtrer, de router, d'autoriser ou non les paquets. Cette couche se trouve entre la couche cœur et la couche d'accès c'est-à-dire entre la partie « liaison » et la partie « utilisateur ». La segmentation du réseau commence ici en ajoutant plusieurs switches de niveau 3 qui sont reliés à la fois à la couche cœur et d'accès. **[25]**

Figure III.40 : Description La couche distribution

Ainsi agrégation les connexions des locaux techniques. Il utilise des commutateurs pour segmenter et organiser le système d'information en groupes vlan, profils utilisateurs et afin d'isoler les problèmes. **[24]**

Notamment, nous devrons choisir entre routeur et Switch selon la taille et les moyens de l'entreprise. Plus la société est grande, plus nous aurons besoin de routeur à ce niveau. Par contre pour une petite entreprise, des Switchs suffisent. Ces routeurs/Switchs de distribution vont s'occuper du routage des paquets, de l'application des ACLs, d'assurer la tolérance de panne et de délimiter les domaines de Broadcast.

- **La couche accès « Access layer »**



Cette couche qui est la dernière du modèle hiérarchique permet de connecter les périphériques des utilisateurs finaux « end-user » au réseau, que ce soit en Wifi, Ethernet. A ce niveau, on utilise des switches de niveau 2 car la configuration de ce type de switches pose moins de contraintes**. [25]**

Figure III.41 : Description La couche accès

Le besoin en performance n'est plus vraiment une nécessité car chaque Switch aura un nombre d'utilisateur égal à son nombre de ports (moins 1 ou 2 pour le trunk entre la couche d'Access et de Distribution). Les traitements restent basiques et ne demandent peu de ressources. **[26]**

La couche accès assure les fonctions suivantes :

- Politique et contrôle d'accès suite de la couche de distribution;
- La micro-segmentation;
- Le partage de la bande passante

III.3 Principes d'un modèle de réseau hiérarchique

- **Division du réseau en couches distinctes**

  Le modèle de conception comme en a déjà illustrer se divise en trois couches: la couche d'accès, la couche de distribution et la couche cœur de réseau, ce qui rend la conception modulaire et évolutif **[27]**

- **Diamètre du réseau**

  Lors de la conception d'une topologie de réseau hiérarchique, le premier élément dont il faut tenir compte est le diamètre du réseau. Le diamètre correspond généralement à une mesure de distance, mais dans ce cas, ce terme est utilisé pour mesurer le nombre de périphériques. Le diamètre de réseau correspond au nombre de périphériques que doit traverser un paquet avant d'atteindre sa destination. Lorsque vous maintenez un faible diamètre de réseau, cela garantit une latence faible et prévisible entre les périphériques. **[27]**

- **Redondance**

  La redondance représente une partie de la création d'un réseau à disponibilité élevée.
  La redondance peut se présenter sous différentes formes. Par exemple, doubler les connexions réseau entre les périphériques, ou bien doubler le périphérique eux-mêmes.
  L'implémentation de liaisons redondantes peut être coûteuse. Il serait improbable d'implémenter une redondance sur la couche d'accès, en raison du coût et des fonctionnalités limitées des périphériques finaux. Cependant, la redondance sera implémentée au niveau des couches de distribution et cœur de réseau. **[27]**

III.4 Plan d'adressage

Cette étape consiste à créer une stratégie d'adressage global en assignant des blocs d'adresses à des différent portions du réseau, simplifiant de ce fait la gestion des adresses et résultant en un inter-réseaux plus évolutifs.

Comme nous avons déjà vue dans le chapitre II, l'adresse IP utilisé au niveau de notre réseau bancaire est de classe A qui est 10.0.0.0. Suite à la codification de cette adresse selon le lieu situant de la nouvelle agence ainsi que son occurrence par rapport à cet emplacement. Nous déduisons l'adresse qui représentera ce nouveau site qui est la 10.10.10.0.

Explication

10.	**10.**	**10.**	**0**
	{Code du Wilaya}	{Numéro d'occurrence}	

Tableau III.3 : Codification des adresses de l'entreprise.

Cette adresse est segmentée en plusieurs sous-réseaux selon le groupe de service qu'appartiennent l'utilisateur et le nombre de postes. Les serveurs sont en adressage fixe ; les postes sont en adressage dynamique avec DHCP.

Nous avons utilisé la segmentation afin d'avoir une meilleure performance globales du réseau, augmenter la sécurité, optimiser l'espace réservé à une adresse IP, flexibilité de segmentation de réseau, et Simplicité de l'administration du réseau.

Ainsi, nous retrouvons un autre type d'adresse privé pour assurer le service de management par des stations de travail précises qui seront placé au niveau du site central externe. Ces dernières seront ainsi en adressage fixe.

III.5 Architecture physique globale du Site

Le schéma figure III. Représente le branchement physique des équipements indépendamment de leur appartenance logique. A noté que ce plan représentera notre structure de départ.

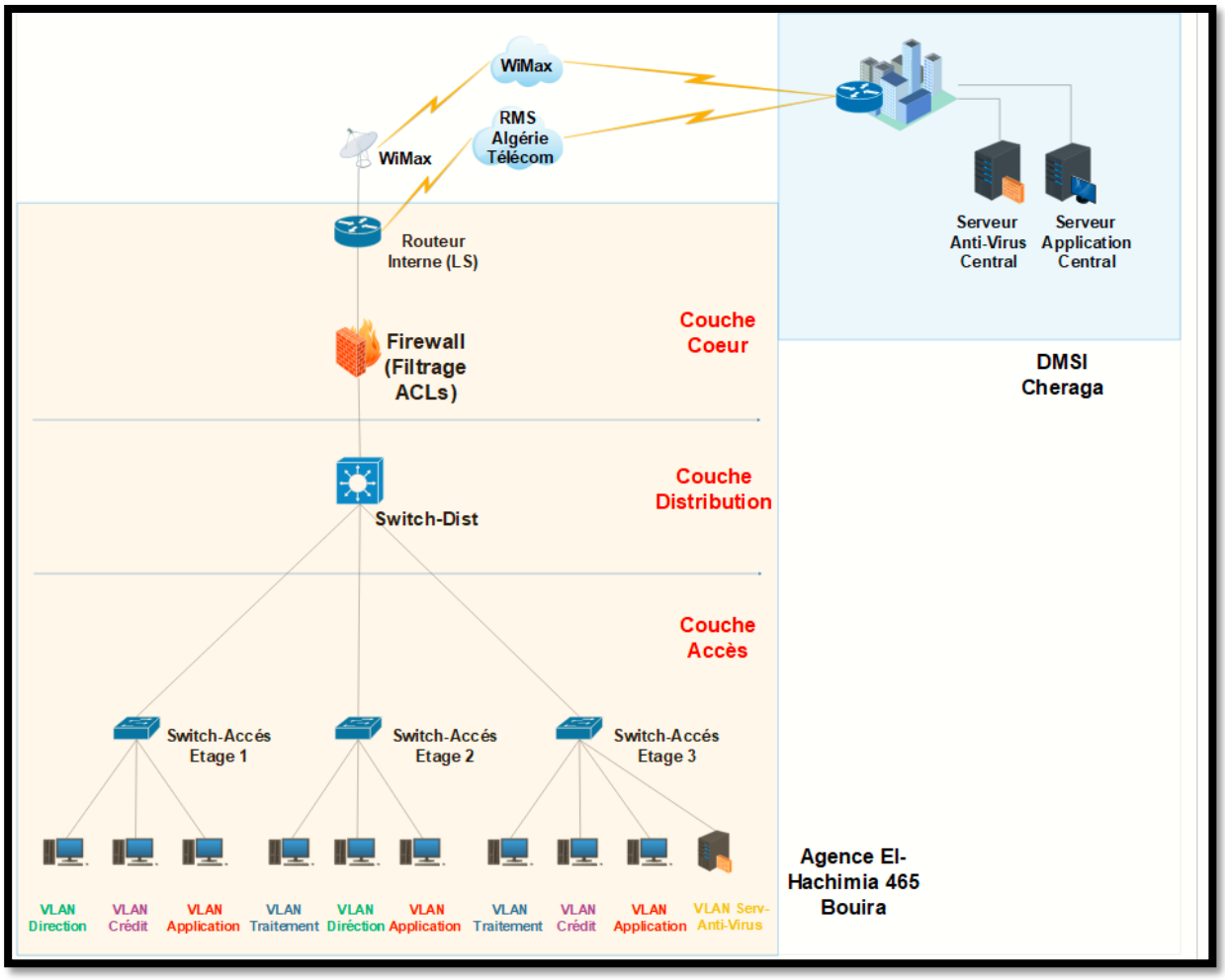


Figure III.42 : Architecture globale de la solution proposée.

III.5.1 Choix de l'architecture matérielle

Nous avons choisi pour notre entreprise de faire appel à une liaison réseau multiservices (RMS) pour relier l'agence au site central.

Ce qui concerne les équipements, notre processus de sélection a impliqué des considérations relatives aux fonctions et caractéristiques des équipements telles que leurs capacités d'extensions et de gestion ainsi Le cout.

Plusieurs autres contraintes ont été prises en considération. En effet, il nous a fallu trouver des équipements permettant d'assurer :

- Une forte distribution.
- Une grande capacité de commutation 2, 3.
- Des connexions Gigabit pour assurer la bande passante montante et descendante.
- Redondance des liens.
- Une forte concentration de port (Stations de travails + imprimantes + VoIP).

III.5.2 Présentation des Equipements utilisés

Tous les équipements utilisés au niveau de l'BADR, sont tous de même marque (Cisco) puisque ce sont des équipements fiables qui ont fait leur preuve. Comme tout le matériel utilisé est de même marque, ce qui évite tout problème de compatibilité entre les protocoles propriétaires. De plus, cela permet d'exploiter pleinement les protocoles développés par le constructeur**. [35]**

Type d'équipement	Fonctionnalité	Localisation	Nombre
Routeur Cisco Catalyst 2811	Routage, Filtrage, Interconnexion, VoIP.	Couche Cœur	2
Pare-feu Cisco ASA 5505	Filtrage IP, Sécurisation.	Couche Cœur	2
Switch Cisco Catalyst 3560-24TS	Routage Inter-VLAN Adressage DHCP, Filtrage IP.	Couche Distribution	2
Switch Cisco Catalyst 2960-24TT	Accès des utilisateurs.	Couche Accès	3
PC de bureau HP	Service fonctionnel.	PC et Serveurs	50
Serveur Anti-virus	Protection Anti-virus.	PC et Serveurs	1

Tableau III.4 : récapitulatif des équipements utilisé lors de notre projet.

Afin de répondre aux exigences croissantes de notre entreprise qui cherche à réduire les frais d'exploitation de leurs réseaux et à accroître la productivité de leurs utilisateurs finaux par l'intermédiaire d'applications réseaux, des solutions plus intelligentes doivent être mises au service des sites distants.

III.5.2.1 Choix du Routeur

Le réseau LAN du site de l'agence **AL HACHIMIA BOUIRA** comprend un router **Cisco 2811.** Le choix de cette dernière repose sur plusieurs caractéristiques en cite fournit des services de sécurité de bout en bout, très évolués et complètement intégrés, ils disposent de fonctions de cryptage matérielles directement embarquées sur la carte mère ainsi que des emplacements pour des DSP Voix. De plus ils disposent en option d'un système de prévention des intrusions (IPS), de fonctions de pare-feu à inspection d'états, du support de la téléphonie et de la messagerie vocale. Ils disposent de nouvelles interfaces haute densité offrant au final un large choix d'options de connectivité Lan / Wan qui associé à une haute densité d'emplacements garanti une évolutivité maximum de la plateforme pour répondre aux besoins d'extension future des réseaux.

Sa conception modulaire nous permet de configurer notre routeur pour l'adapter à nos besoins en constante évolution.

L'architecture Cisco 2811 a été spécifiquement conçue pour répondre aux besoins croissants des sites distants d'entreprise et des PME / PMI en matière d'applications, tant aujourd'hui que dans l'avenir. Cisco 2811 offre l'éventail d'options de connectivité le plus large de l'industrie avec des caractéristiques de disponibilité et de fiabilité à la pointe de la technologie. De plus, la plate-forme logicielle Cisco IOS assure le support d'une série complète de protocoles de transport, d'outils de qualité de service (QoS), de fonctions de sécurité évoluées et d'applications voix. **[28]**

III.5.2.2 Choix du commutateur

- **Commutateur Niveau 3 (Switch Distributeur)**

Le commutateur Cisco 3650 est un commutateur idéal pour les réseaux LAN à une, fiabilité, fonctionnalité et capacité de traitement élevées, Filtrage de paquets, Ce commutateur possède aussi la fonctionnalité de pouvoir créer et gérer des VLAN de niveau 3. Ainsi disposent d'un grand nombre de fonctionnalités de sécurité, permettant aux entreprises de protéger les informations importantes, interdire aux personnes non autorisées l'accès au réseau, préserver la confidentialité, et maintenir un fonctionnement sans interruption. Les commutateurs de distribution ont toujours la responsabilité de traiter les données de la couche 3. Le trafic généré par les dispositifs de la couche d'accès doit être segmenté en VLAN, ce qui exige que les commutateurs de classe supérieure fournissent des fonctions de routage inter-VLAN afin de permettre une communication entre les multiples VLAN. Étant donné que la couche centrale a la lourde tâche de gérer la transmission de volumes de trafic extrêmement élevés, des commutateurs de distribution dotés d'une fonctionnalité de couche 3 sont déployés pour alléger la charge de travail des commutateurs centraux. **[29]**

- **Commutateur niveau 2 (Switch Access)**

Le commutateur de niveau 2 quand vas utiliser afin de relier les utilisateurs au réseau Lan local dans notre architecture est le Cisco 2960 de la gamme Cisco Catalyst 2960.
Le Switch 2960 est un commutateur Ethernet autonome à configuration fixe ; il fournit des Fonctionnalités intelligentes aux périphériques du réseau, par exemple des listes de contrôle D'accès (ACL) élaborées et une sécurité renforcée ; Contrôle du réseau et optimisation de la bande passante grâce aux fonctions de qualité de service évoluée, de limitation granulaire du débit, de listes de contrôle d'accès et de services multicast ainsi fournit la flexibilité de la double connectique des liaisons montantes Gigabit Ethernet, permettant d'utiliser soit du cuivre, soit de la fibre optique. Chaque port Gigabit Ethernet à double connectique et un port Gigabit Ethernet SFP (Small Form-Factor Pluggable), un seul étant actif à la fois. **[29]**

III.5.2.3 Choix de firewall

Pour protéger le réseau contre les attaques de piratage et l'écoute clandestine, l'entreprise utilise au niveau de son site de **BOUIRA** un pare-feu de type Cisco ASA 5005 En effet, le firewall se place en amont d'un serveur dédié et permet de filtrer le flux entrant et sortant. Ce modèle n'est plus commercialisé.

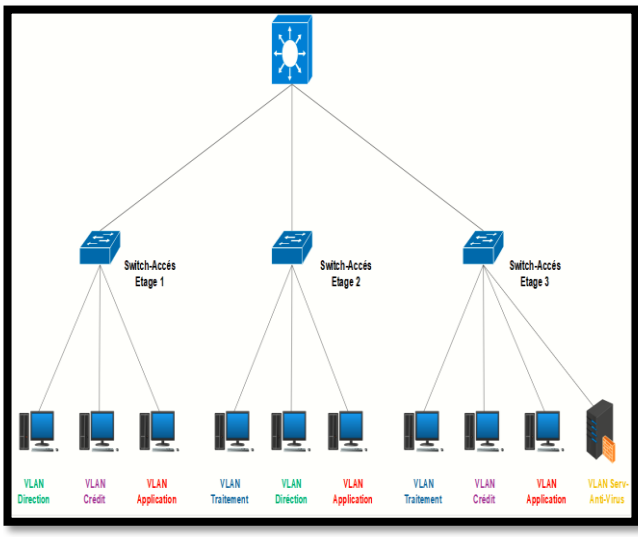
Cisco ASA 5005 est un firewall permettant :

- Une visibilité et contrôle granulaires.
- Renforcement et sécurisation web sur un site ou un Cloud.
- Prévention contre les intrusions grâce au Système de pointe de protection (IPS).
- Protection complète contre les menaces et les programmes malveillants avancés.

Cisco ASA offre une visibilité complète sur les composants du réseau, garantit une protection en temps réel contre les programmes malveillants et les menaces émergentes tout en réduisant les coûts et la complexité. **[30]**

III.6 Architecture Logique du LAN

III.6.1 Architecture logique couche Accès



Le schéma représente l'architecture logique de la couche accès du LAN. Le réseau est subdivisé en plusieurs sous réseaux formant des domaines de Broadcast (VLANs) pour chaque Type de trafic. Les VLAN sont des configurations essentielles dans un réseau d'entreprise. Ils permettent également de séparer logiquement des départements ou des groupes de travail sans pour autant qu'ils soient séparés physiquement.

Figure III.43 : Schéma représentatif de la couche

Dans notre architecture, nous disposons de 3 étages .Sur chaque étage nous retrouvons un ensemble de postes travails appartenant à diffèrent groupe de service.

Ces services sont affectées à des VLAN différents. (Voir tableau III.5)

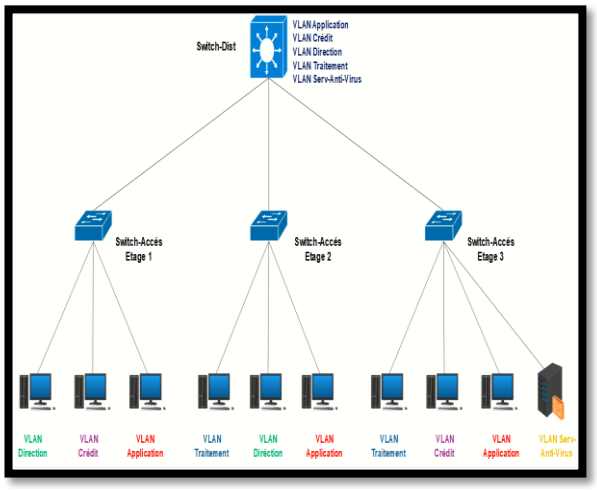
VLAN ID	Nom du VLAN	Description du VLAN
10	VLAN-SRV-ANT	Vlan Serveur Anti-virus
11	VLAN-APP	Vlan service Application
12	VLAN-CDT	Vlan Utilisateur Crédit
13	VLAN-TRT	Vlan Utilisateur Traitement
14	VLAN-DRT	Vlan Utilisateur Direction
100	VLAN-MGT	Vlan Management
101	VLAN-CON	Vlan reliant au firewall

Tableau III.5 : représentant les Vlan utilisés dans notre réseau LAN.

Evidement le réseau peut être divisé avec n'importe quelle logique voulue selon les besoin de l'entreprise.

Sur chaque étage, les stations de travail sont reliées à un switch de niveau 2 (SW-Accès). Chaque port d'un switch peut être assigné à un VLAN différent.

III.6.2 Architecture logique Couche Distribution :



Le schéma suivant représente l'architecture logique de la couche distribution de notre réseau.

Les objectifs de cette couche est :

Limiter les zones de Broadcast.
Transférer les paquets entre VLAN.
Filtrer l'accès entre certains VLAN

Figure III.44 : Schéma représentatif de la couche distribution.

III.6.2.1 Segmentation VLSM et création des VLANs

La technique du VLSM, ou encore « Variable-Length Subnet Mask » a pour but comme l'indique son nom, de créer des sous-réseaux de taille variable. Elle a été conçue dans l'objectif d'optimiser l'efficacité de l'attribution des adresses. **[31]**

Suite à la segmentation de notre adresse 10.10.10.0, nous venons d'identifier un total de 5 sous-réseaux (VLANs). Cependant, le nombre de machines sur chaque sous-réseau est variable. Cela va de 20 à 1 pour chaque VLAN. Les résultats obtenus par le modèle VLSM sont représentés dans le tableau suivant:

NOM VLAN	Nombre d'hôtes	Taille allouée	Adresse de sous-réseau	Masque de sous-réseau	Plage d'adresse	Adresse diffusion
VLAN-Application	20	30	10.10.10.0	255.255.255.224	10.10.10.1 10.10.10.30	10.10.10.31
VLAN-Crédit	17	30	10.10.10.32	255.255.255.224	10.10.10.33 10.10.10.62	10.10.10.63
VLAN-Traitement	13	14	10.10.10.64	255.255.255.240	10.10.10.65 10.10.10.78	10.10.10.79
VLAN-Direction	11	14	10.10.10.80	255.255.255.240	10.10.10.81 10.10.10.94	10.10.10.95
VLAN-Anti-virus	1	2	10.10.10.96	255.255.255.252	10.10.10.97 10.10.10.98	10.10.10.99

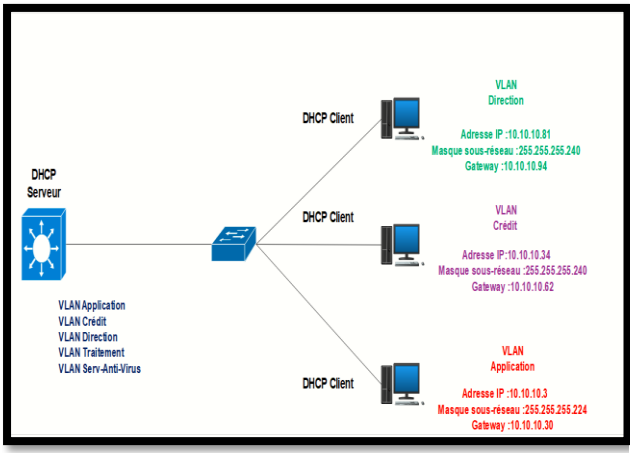
Tableau III.6 : Résultat de la segmentation d'adresse par le modèle VLSM.

Ainsi nous utiliserons une adresse privé local pour représenter le VLAN de gestion d'équipements et de management. Cette adresse aura comme primitive l'accès à distance de l'administrateur à notre LAN. Ce VLAN aura comme adresse : **192.168.1.0/29 (masque : 255.255.255.248).**

III.6.2.2 Adressage DHCP

DHCP sera implémenté au niveau du Switch distributeur Switch-Dist. A chaque VLAN est attribué un POOL d'adresses. Les clients obtiennent automatiquement leur adresse IP et leur passerelle par défaut, ce qui simplifie l'adressage des machines.

Cette activité nous a permis d'approfondir la configuration des routeurs et des switches. Ainsi nous pourrions dire que nous avons paramétré un serveur DHCP au niveau de notre Switchs distributeur.



Il nous suffira juste d'ajouter un poste de travail au niveau du Switchs accès, configurer le switchport de cet utilisateur en lui attribuant le VLAN correspondant à son groupe de service et ce dernier se voit attribuer une adresse IP, un masque ainsi qu'une passerelle par default automatiquement.

Figure III.45 : Attribution des adresses grâce au protocole DHCP.

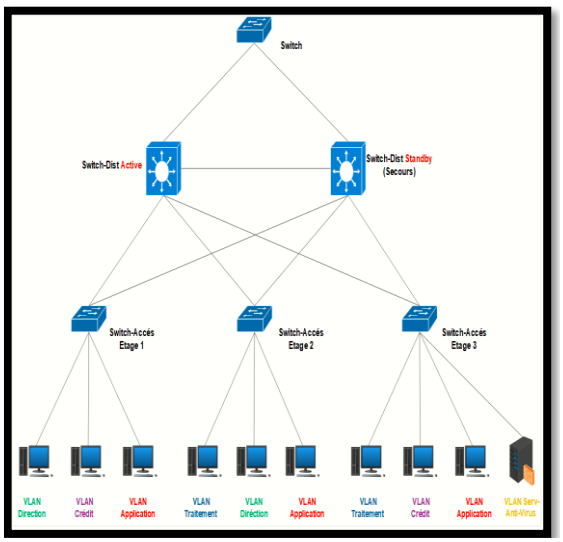
III.6.2.3 La haute disponibilité

Lors de la conception de réseaux informatiques, il est nécessaire que les utilisateurs puissent y accéder pour mettre à jour des activités ou effectuer tout type de travail**.** Par conséquent, les structures doivent disposer d'un protocole pour garantir la continuité des opérations de transfert, ce qui signifie qu'il doit y avoir des plans d'urgence afin que le service ne subisse pas d'interruptions ou de coupures en cas de panne informatique et que les utilisateurs puissent continuez à interagir normalement avec le réseau.

Lorsque les utilisateurs ne peuvent pas entrer dans le réseau, cela signifie que le service n'est pas disponible**,** le temps d'inactivité étant la variable utilisée pour établir le degré de disponibilité du système. **[32]**

❖ Redondance des Switch Distributeurs

Nous allons utiliser le mécanisme de la redondance de commutateurs qui va nous permettre d'avoir une adresse IP virtuelle entre deux commutateurs. Ainsi, si le commutateur nominal est en panne, en maintenance ou bien inaccessible, les équipements qui sont situés derrière ou avant ces commutateurs continuent d'être joignables sans reconfiguration nécessaire



Notre choix de type de redondance de commutateurs s'est porté sur le protocole HSRP car, d'une part, nous avons besoin d'une redondance sur un réseau Cisco et, d'autre part, il apporte une redondance d'adresse IP sur plusieurs commutateurs. Donc tout le trafic est supporté par un seul commutateur tandis que l'autre commutateur est en secours uniquement.

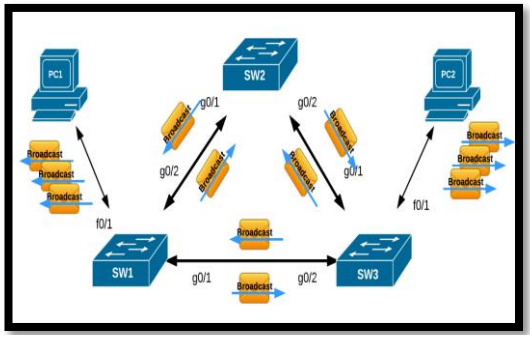
Figure III.46 : Redondance des Switchs Distributeurs.

Les deux commutateurs utilisent le protocole HSRP se partagent une adresse IP virtuelle qui va être utilisé comme route. Par contre, chaque commutateur aura une MAC commune pour cette adresse virtuelle. En cas de panne ou de maintenance sur l'un des commutateurs, le trafic sera redirigé vers le commutateur de secours.

❖ Inconvénient

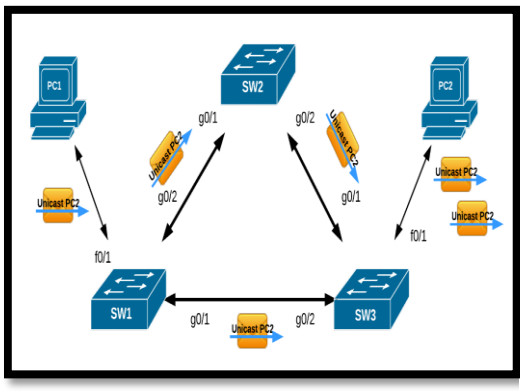
Pour assurer la fiabilité des liaisons entre des commutateurs du LAN il est utile de multiplier les connexions physiques (redondance).

Si les commutateurs transfèrent le trafic de diffusion et Multicast par tous les ports sauf celui d'origine plusieurs problèmes peuvent alors survenir : **[32]**



Tempêtes de diffusion : Les trames circulent en boucles et sont multipliées à chaque passage sur un commutateur. Elles peuvent tourner indéfiniment. **[32]**

Figure III.47 : Tempête de diffusion.



Trames dupliquées : L'arrivé de deux trames identiques à une destination unique.

Dans cet autre exemple, PC1 envoie une trame à PC2, elle arrive en double exemplaire à sa destination. **[32]**

Figure III.48 : Duplication des trames.

Afin de profiter de la redondance tout en évitant la problématique des boucles, nous optons pour l'utilisation du Spanning-Tree.

III.6.3 Architecture Logique Couche Cœur

Notre couche cœur est composée de deux éléments principaux assurant l'interconnexion et la sécurisation de notre réseau LAN.

III.6.3.1 Firewall

Concernant la couche cœur, notre première initiative est de maintenir une architecture complètement sécurisé et protéger.

La politique de sécurité doit englober l'ensemble du réseau informatique. La plupart des tentatives d'intrusions peuvent provenir (volontairement ou non) des utilisateurs autorisés. Pour cela, les mesures de sécurité doivent prendre en considération le réseau local et le réseau externe WAN.

La sécurité de notre système d'information est à l'abri grâce aux solutions firewalls physiques « CISCO ».Il est primordial de sécurisé notre LAN contre les virus, les vols de données et attaques réseau.

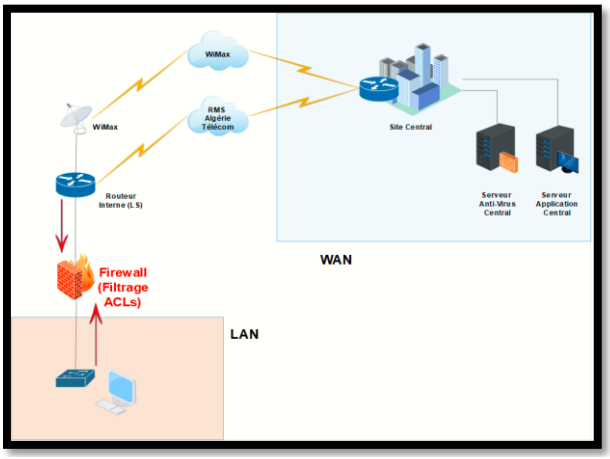


Figure III.49 : Mis en place du firewall.

Le firewall permet d'interconnecter 2 réseaux (ou plus) de niveaux de sécurité différents (par exemple : internet et le réseau interne d'une entreprise). Le firewall joue un rôle de sécurité en contrôlant les flux de données qui le traversent (en entrée ou en sortie). Il permet ainsi de filtrer les communications, de les analyser et enfin de les autoriser ou de les rejeter selon les règles de sécurité en vigueur. **[34]**

Le choix de notre type de firewall s'est porté sur le Firewall sans états (stateless). Il fait un contrôle de chaque paquets indépendamment des autres en se basant sur les règles prédéfinies par l'administrateur qu'on les nomme les Access Control Lists (ACLs).

Ces firewalls interviennent sur les couches réseau et transport. Les règles de filtrages s'appliquent alors par rapport à une d'adresses IP sources ou destination, mais aussi par rapport à un port source ou destination.

III.6.3.2 Politique des règles de filtrage (Les ACLs)

Nous commençons à spécifier que le firewall ne doit laisser passer aucuns paquets. Ensuite, nous ajoutons les règles permettant de choisir les flux que nous souhaitons laisser passer :

- ✓ Seuls les postes de managements situant sur le site central externe pourront se connecter et accéder aux équipements internes de l'agence grâce à un accès distant SSH, ainsi toute maintenance ou reconfiguration d'un équipement sera assuré par des manager distant.
- ✓ Le serveur Anti-virus interne est autorisé d'effectuer des mis à jours depuis le serveur Anti-virus externe du site central et vice versa.
- ✓ Les postes appartenant au service d'application ont le droit de communiquer avec le Serveur d'Application externe afin de maintenir l'exploitation du logicielle applicatif de la banque.
- ✓ Tout autre trafic sera exclu mis à part le Protocol ICMP qui garantira la connectivité des équipements.

III.6.3.3 Routeur

Le déploiement d'un routeur d'extrémité nous permet de relier notre réseau d'agence à au site central. Comme beaucoup de trafic passe par ce routeur les besoins en performance sont conséquents. C'est pour cela nous avons mis en œuvre un routeur de type Cisco 2811. Ce modèle nous permet d'assurer le routage interne ainsi qu'externe en utilisant les deux types de routage statique et dynamique.

Pour une haute disponibilité d'interconnexion et afin d'éviter toute sorte de rupture ou coupure de lien nous avions mis en place deux technologies de liaison :

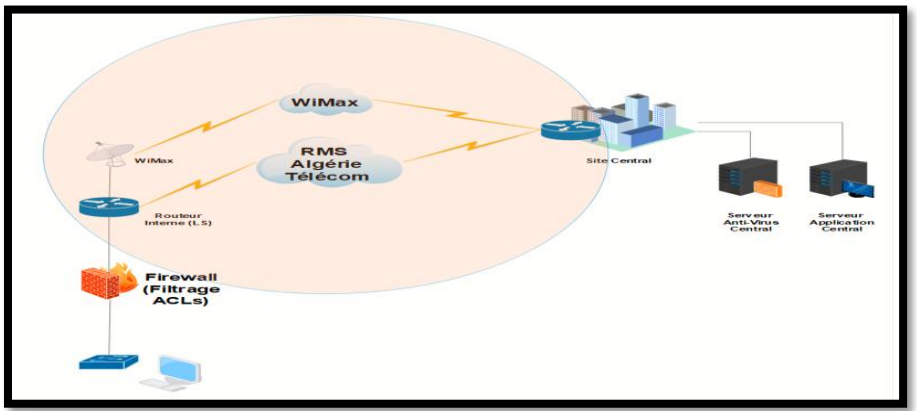


Figure III.50 : Les deux technologies utilisées Pour l'interconnexion.

- Une ligne spécialisé RMS d'Algérie Télécom

  La Liaison spécialisée est une liaison permanente réservée à l'usage exclusif d'un utilisateur. Elle offre la possibilité de transmission entre deux points de terminaison déterminés du réseau public. **[35]**

- ✓ **Avantage :**

  Un transfert rapide de données.

  Une plus grande sécurité dans les émissions/réceptions de données.

  Une communication fiable et de qualité.

  Une interconnexion de sites distants.

  La disposition d'une liaison permanente de manière exclusive évitant ainsi la saturation du réseau.

  Le RMS est un réseau multiservices de nouvelle génération NGN, de type IP/MPLS et d'envergure nationale. **[35]**

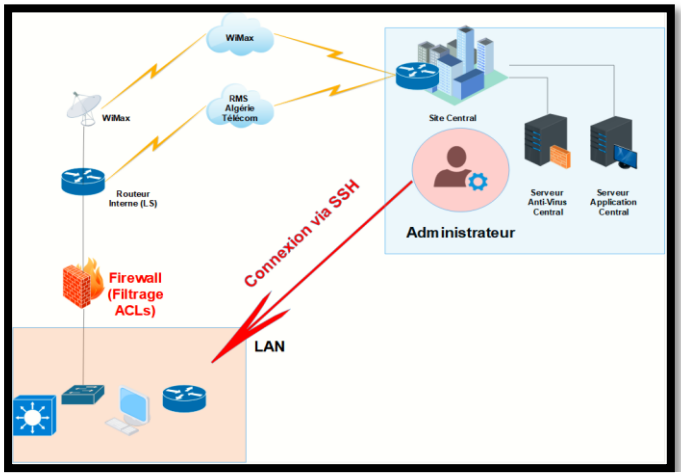
- **La technologie WiMax**

Le WiMax est une technologie de boucle radio local (BLR), ce qui permet donc de bénéficier d'une connexion au réseau Internet par onde hertzienne. La portée est théoriquement de 50 km, mais en pratique on arrive à avoir une connexion à 20 km de l'antenne émettrice. Grâce à cela on peut installer plus rapidement le haut débit dans les zones dites blanches.

Un réseau de stations émettrices a été installé sur des points hauts dans votre département pour le couvrir en WiMax**.** Pour recevoir ce signal radio qui passe sur la bande de fréquences des 3,5 GHz, vous serez équipé d'une antenne radio. Cette antenne est orientée vers une des stations de base installées dans la région**.** Nul besoin de posséder une ligne de téléphone pour profiter d'Internet de façon illimité. **[36]**

Le réseau l'agence de **BOUIRA** est maintenant relié à la DMSI et prêt à l'emploi.

III.7 Sécurisation de l'accès à distance



Afin d'assurer le service de management et gestion des équipements gérer par un expert en informatique appartement à la direction de l'informatique situant sur le site central distant, nous utilisons un protocole d'accès à distance SSH.

.

Figure III.51 : Accès à distance protocole SSH.

Le protocole SSH utilise une communication sécurisée pour éviter que des informations sensibles (configuration, login, mot de passe,…) soient interceptées durant leur transport jusqu'à la console d'administration.

Voici les différentes étapes pour configurer le SSH sur un IOS:

- Définir un compte utilisateur avec le doublet [login/mot de passe]
- Définir un Hostname (par exemple MonRouteurAgence1) à son équipement switch ou routeur, qui sera utilisé pour générer la clé de chiffrement
- Définir un nom de domaine (par exemple cisco.com), qui sera aussi utilisé pour générer la clé de chiffrement
- Générer cette fameuse clé de chiffrement, appelée RSA
- Activer le SSH

Tous les équipements de notre réseau disposent d'une configuration SSH et sont accessibles à distance seulement par l'administrateur réseau de DMSI.

III.8 Concept de téléphonie IP

Afin de réduire les factures des communications téléphoniques de la RTC entre l'agence et la DMSI, nous proposons la mise en place de la technologie VoIP.

La VOIP est une technologie qui permet la communication vocale via un flux internet et non plus via un réseau RTC. VoIP signifie Voice over Internet Protocol. Pour votre entreprise le recours à un système de téléphonie IP vous permettra notamment de faire des économies sur votre facture de communication, mais également d'échanger via des messageries ou faire des partages d'écrans. Des services tels que Messenger, Skype ou Snapchat utilisent des technologies VoIP. **[37]**

III.8.1 Choix du téléphone IP

Comme équipement nous utilisons le téléphone Cisco 7960.

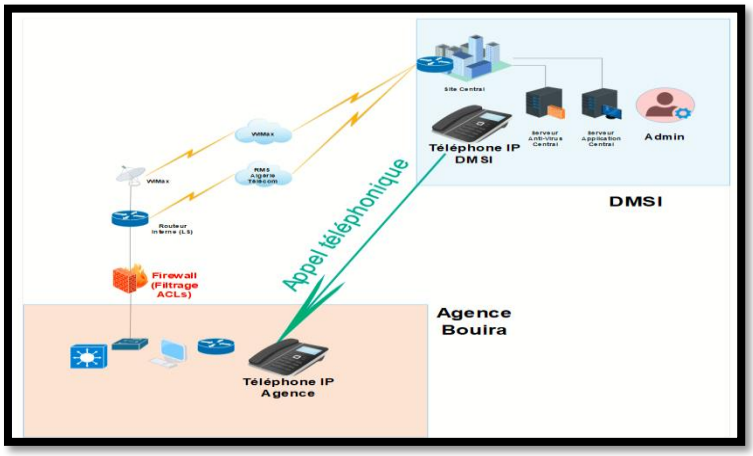


Figure III.52 : Modèle de téléphonie IP VoIP.

Le téléphone IP Cisco 7960 est un téléphone IP multifonction qui répond aux besoins de direction et de gestion. Le Cisco 7960 est doté de six boutons de ligne et de fonction programmables ainsi que de quatre touches interactives qui guident l'utilisateur pour les fonctions d'appel. Le 7960 de Cisco peut gérer jusqu'à 6 lignes simultanément. Il comporte également un grand écran à cristaux liquide. **[38]**

Parmi ses caractéristiques :

- Transfert d'appel, double appel, mise en attente, renvoi automatique.
- Touche Services : donne accès aux services et options qui vous permettent de personnaliser votre téléphone.
- Configuration des protocoles DHCP et TFTP.
- Navigateur XML pour personnaliser vos applications.
- Fonctionnement avec des systèmes de téléphonie IP basés sur la technologie Cisco Call Manager, H.323, le protocole SIP (Session Initiated Protocol) et sur le protocole MGCP (Media Gateway Control Protocol), avec des mises à jour logicielles initialisées par le système. **[38]**

Cette technologie va nous permettre de réduire les factures de communications téléphoniques assurées par RTC et passé à un réseau téléphonique IP. Chaque téléphone sera doté d'une adresse IP et numéro de téléphone précis lequel les utilisateurs peuvent s'appeler .

III.8.2 Paramétrage

La configuration de ces téléphones IP s'effectuera au niveau du routeur de l'agence.

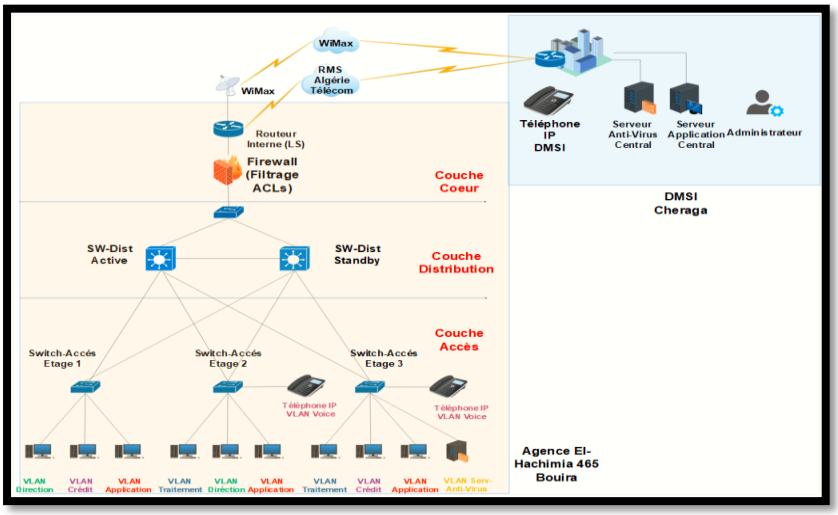


Figure III.53 : Architecture globale finale.

Pour la création du VLAN Voice et l'attribution du pool DHCP de ce nouveau réseau privé, les mêmes paramétrages sont effectués au niveau du Switch Distributeur.

Il suffira juste d'ajouter un téléphone, le brancher sur un Switch, lui attribuer le VLAN-Voice correspondant et ce dernier se verra attribué une adresse IP.

III.9 Secours électrique et climatisation

Afin de garantir un fonctionnement optimal et continu des équipements réseau et des serveurs, des investissements lourds ont été réalisés pour améliorer les conditions environnementales des locaux réseaux et des salles de serveurs.

- **Sécurisation électrique :**

  Nous allons intégrer la sécurisation électrique de tous les équipements réseaux de cœur ainsi que des serveurs, L'ensemble des équipements est doublement alimenté en énergie électrique par l'intermédiaire du réseau public et d'onduleurs. Chaque nœud de cœur de réseau dispose ainsi d'une autonomie permettant une intervention pour la résolution des pannes.

- **Climatisation :**

  Afin de garantir le fonctionnement optimal des équipements et serveur réseau, les capteurs de température interne des équipements sont utilisé pour la supervision du niveau de température dans les locaux réseaux et les salles serveurs.

III.10 Conclusion

Dans ce chapitre, nous avons tenu à proposer une solution basée sur le modèle en 3 couches sur la réalisation d'une architecture réseau ainsi que sont interconnexion avec le site central distant.

La solution proposée permet de mettre en place une plateforme IP de 3 couches (cœur/distribution/accès) avec des équipements informatiques permettant de garantir la disponibilité la fiabilité et la sécurité du réseau de manière physique afin de sécurisé les données de l'entreprise.

Nous avons rajouté à l'entreprise la technologie de téléphonie qui nous permet de recevoir des appels téléphoniques via le réseau IP. L'objet du chapitre suivant sera le déploiement de la simulation de notre solution présentée dans ce chapitre.

Chapitre Iv
Implémentation & test

Chapitre IV. Implémentation & Test

IV.1 Introduction

Dans le but d'illustrer et de compléter ce qui a été traité dans la partie théorique de notre mémoire, plus exactement dans le deuxième et troisième chapitre, nous faisons une simulation de réseau informatique de l'entreprise BADR.

Dans ce chapitre, en vas présenter le logiciel utilisé et l'environnement de travail ainsi que les différentes configurations utilisées de notre simulation, enfin nous donnerons les résultats obtenus de la configuration (une description des tests qui seront effectués sur notre réseau.).

IV.2 Environnement de travail

IV.2.1 Présentation de 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 informatiques. L'objectif principal de simulateur est de schématiser, configurer et de voir toutes 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 constituant un réseau informatique. **[39]**

La figure si dessous montrant l'interface principale du simulateur Cisco Packet Tracer:

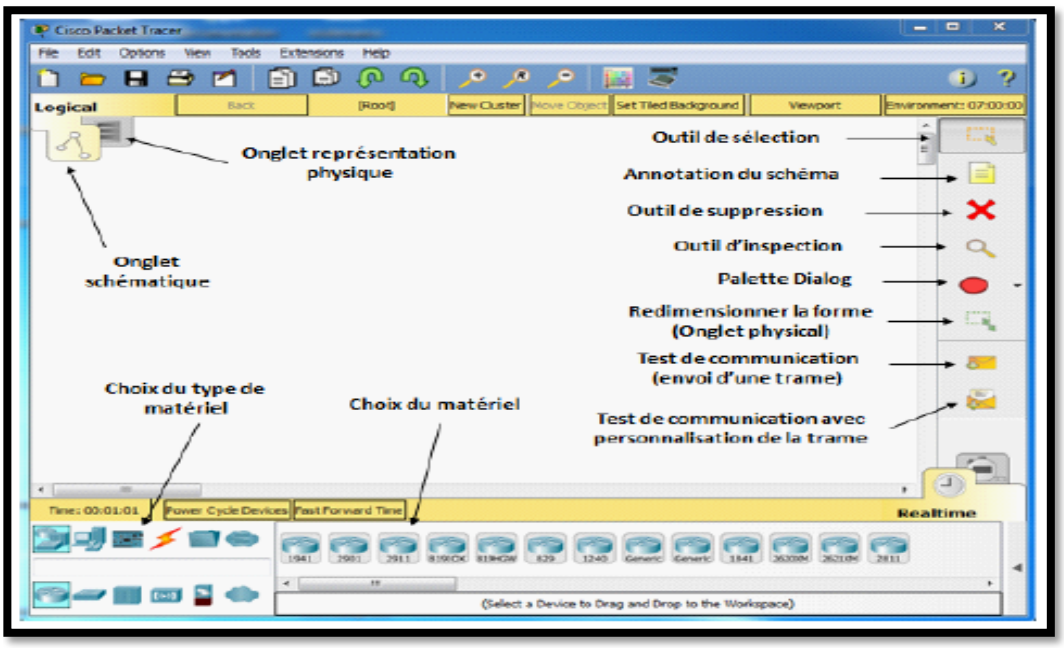


Figure IV.54: Interface de Cisco Packet Tracer.

IV.2.2 Interface commande de Packet Tracer

Toutes les configurations des équipements du réseau, c'est au niveau de CLI (Command Language Interface) quelques 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 qui à partir des commandes introduites par l'utilisateur du logiciel, que la configuration est faite.

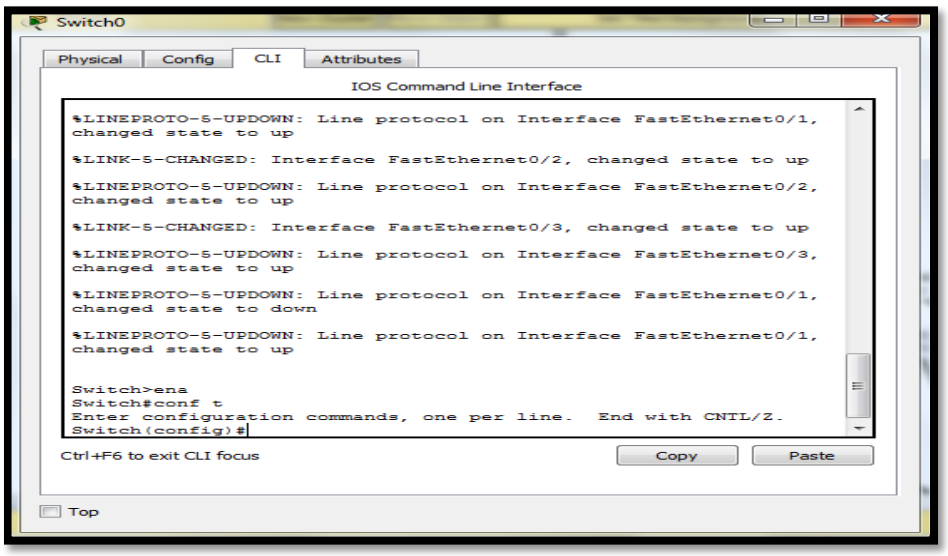


Figure IV.55 : Interface CLI.

IV.2.3 Mode de simulation

Une fois le réseau créé est prêt à fonctionner, il est possible de passer en mode simulation, ce qui permet de visualiser tous les messages échangés dans le réseau. En mode simulation, la fenêtre principale est scindée en deux, la partie de droite permettant de gérer le mode simulation : exécution pas-à-pas, vitesse de simulation, protocoles visibles. La partie gauche de la figure montre les détails obtenus en cliquant sur un message. **[39]**

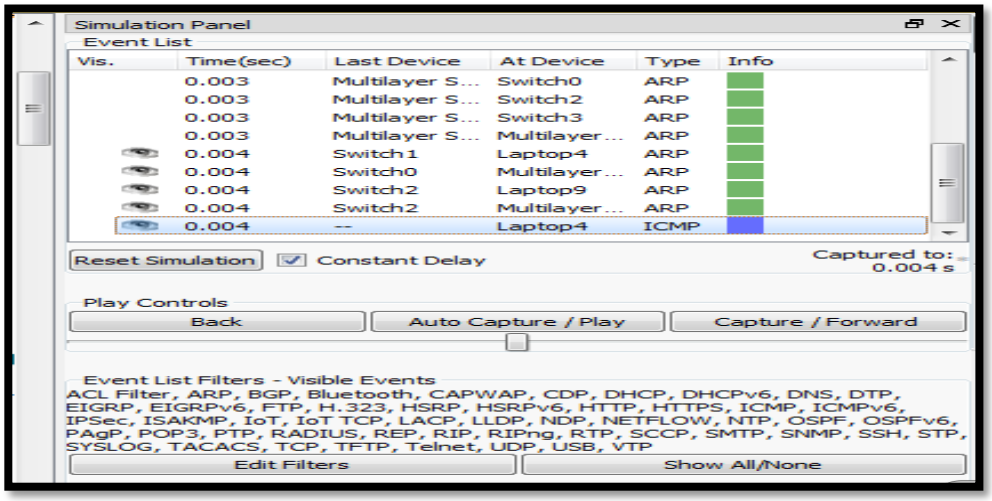


Figure IV.56: Mode Simulateur de Cisco Packet Tracer.

IV.3 Les configurations et mises en place

IV.3.1Présentation de la plateforme de test

Notre plateforme de simulation est constituée des actifs suivants :

- 2 Routeurs au niveau de chaque site, 1 routeur pour la ligne spécialisé LS et 1 routeur pour la technologie WiMax. (dans la couche core)
- Un firewall pour le site Agence.
- Deux commutateurs de niveau 3 au niveau de l'agence, les deux commutateurs configurés en mode Actif/Standby. (la couche distribution)
- Un commutateur de niveau 2 pour la redondance des Switchs niveau 3 de l'agence.
- Trois commutateurs de niveau 2 pour l'agence, un commutateur pour chaque étage d'agence. (la couche accès)
- Un commutateur de niveau 2 pour le téléphone IP de la réception.
- Deux serveurs au niveau de la DMSI (Serveur Anti-virus, Serveur Application) et un serveur (Serveur Anti-virus) pour l'agence. (Dans la couche core)
- 10 postes de travails pour les utilisateurs de l'agence et 1 station pour simuler l'administrateur de la DMSI. (dans la couche accès)
- Trois téléphones IP pour l'agence et un pour la DMSI(Central). (dans la couche core)

Enfin, il faut souligner quelques points essentiels :

- Du fait que le réseau du site central est préconfiguré, nous simulons à ce niveau que les équipements nécessaires pour l'interconnexion avec le site agence.
- Pour la liaison du WiMax, du fait que Packet Tracer ne possède pas la fonctionnalité de simuler cette technologie, nous utilisons deux Routeur (Routeur-Agence-WiMax et Routeur-Central-WiMax) pour représenter cette liaison d'interconnexion.

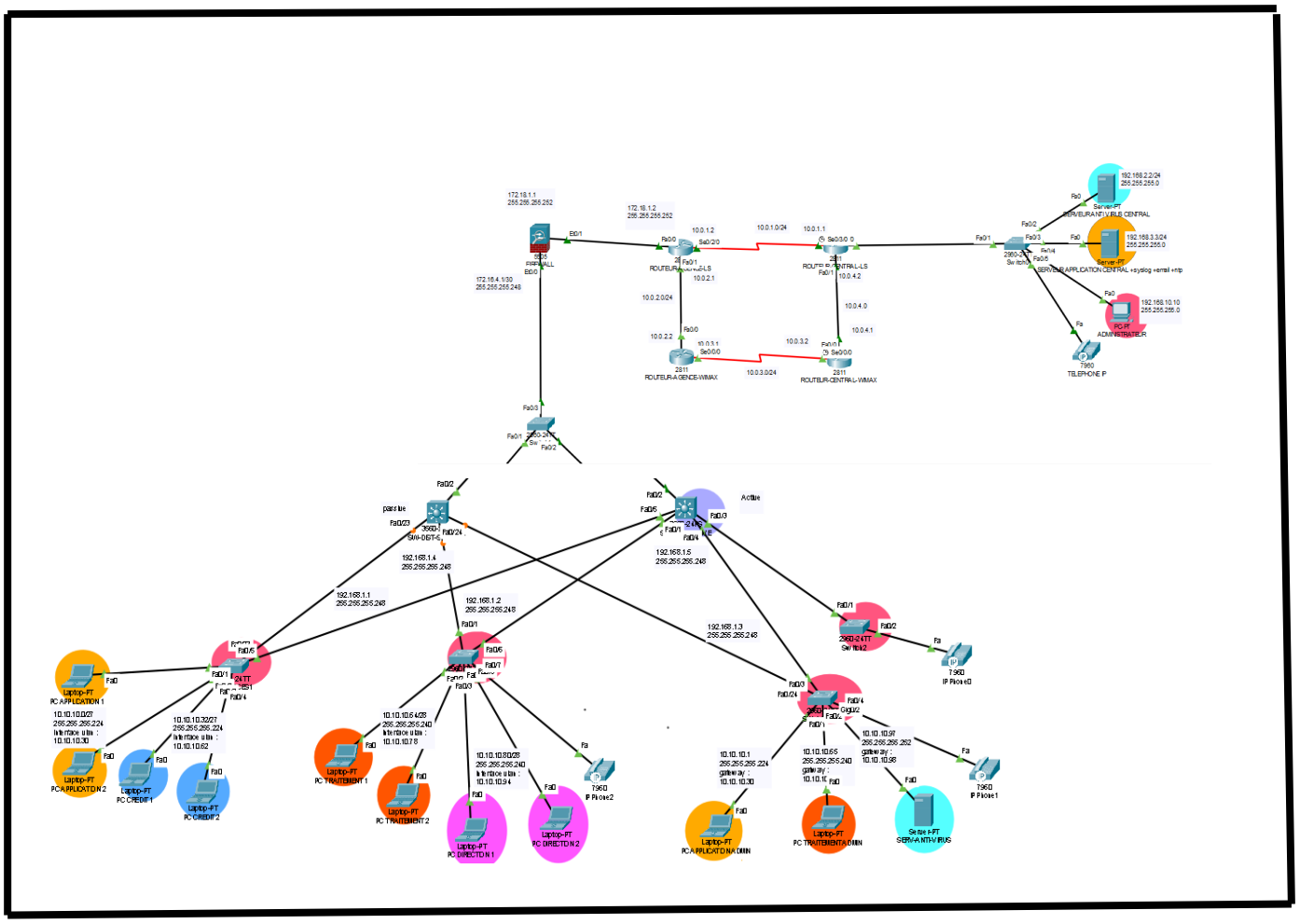


Figure IV.57: Plateforme de test global.

IV.3.2 Configuration des équipements

Dans ce qui suit nous allons présenter la configuration générale de tous les équipements couche par couche suivant notre modèle de conception hiérarchique à trois couches, avec un exemple configuré.

IV.3.3 Configuration Couche Accès

Nous allons configurer les équipements appartenant à cette couche dont les commutateurs de niveau 2, les téléphones IP, le serveur et les postes de travails.

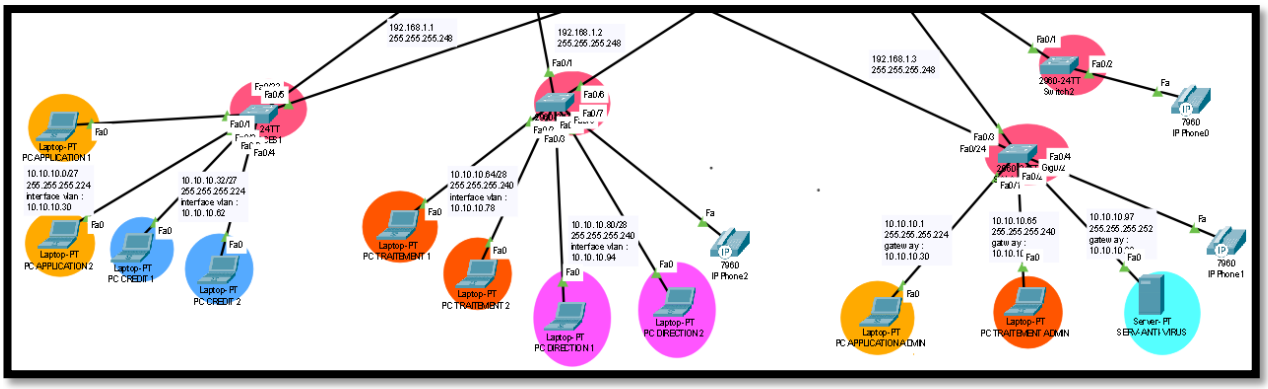


Figure IV. 58: Schéma conceptuelle de la Couche Accès.

En vas débuter notre travail par la mise en place de la couche accès ainsi les différent équipements, ainsi leur configuration.

IV.3.3.1 Configuration des commutateurs niveau 2

La configuration des commutateurs commence par une petite configuration des noms de chaque commutateur, en suit la configuration les différents VLANs existant, ainsi que les interfaces des commutateurs et cela en tenant compte de L'ensemble des protocoles à implémenter, tel que VTP, STP et DHCP. Suivant les étapes ces dessous :

a) **Configuration de Hostname.**
b) **Création des VLAN**
c) **Configuration des interfaces VLAN.**
d) **Configuration les ports**
e) **Configuration d'accès à distance (SSH).**
f) **Activez le port sécurisez en niveau des Switchs accès a fin de mieux sécurisé les équipements.**

a) **Configuration de Hostname :** en tape la commande suivante

```
switch#config t
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)#hostname switch-ACCESS-1
switch-ACCESS-1(config)#
```

Figure IV.59:Configuration de Hostname (SW-ACC).

b) **Création des VLAN :** en tape la commande suivante

```
switch-ACCESS-1(config)#vlan 100
switch-ACCESS-1(config-vlan)#name management
switch-ACCESS-1(config-vlan)#ex
switch-ACCESS-1(config)#vlan 11
switch-ACCESS-1(config-vlan)#name application
switch-ACCESS-1(config-vlan)#ex
switch-ACCESS-1(config)#vlan 12
switch-ACCESS-1(config-vlan)#name credit
switch-ACCESS-1(config-vlan)#ex
```

Figure IV.60:Création des VLAN (SW-ACC).

c) Configuration des interfaces VLAN :

✓ Attribuer pour chaque port reliant une machine ou un téléphone son VLAN identique

```
switch-ACCESS-1(config)#interface range fa0/1-2
switch-ACCESS-1(config-if-range)#switchport mode access
switch-ACCESS-1(config-if-range)#switchport access vlan 11
switch-ACCESS-1(config-if-range)#no shutdown
switch-ACCESS-1(config-if-range)#spanning-tree portfast
```

Figure IV.61:Configuration des interfaces VLAN

Ainsi tous les liens entre le Switchs niveau 2 et les machines seront de type Access.

✓ Créer le VLAN management au niveau des Switchs accès pour accéder à distance aux équipements, nous attribuons aux trois Switchs d'accès des adresses IP du VLAN management (192.168.1.0/29) afin que l'administrateur central parviendra à accéder et configurer les équipements en cas de maintenance.

```
switch-ACCESS-1(config)#int vlan 100
switch-ACCESS-1(config-if)#
%LINK-5-CHANGED: Interface Vlan100, changed state to up

switch-ACCESS-1(config-if)#ip add 192.168.1.1 255.255.255.248
switch-ACCESS-1(config-if)#no shut
```

Figure IV.62:création vlan management (SW-ACC).

✓ Créer default-Gateway au niveau des Switchs accès.

```
switch-ACCESS-1(config)#ip default-gateway 192.168.1.6
```

Figure IV.63:création ip default-Gateway.

d) Configuration les ports des Switchs layer 2 en mode trunk

```
switch-ACCESS-1(config)#interface FastEthernet0/5
switch-ACCESS-1(config-if)#switchport mode trunk

switch-ACCESS-1(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/5,
changed state to down

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

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan100, changed
state to up
```

Figure IV.64:Configuration les ports en mode trunk.

e) Configuration d'accès à distance (SSH)

La configuration du SSH est mise en place en définissant un Domaine-Name ainsi qu'un nom d'utilisateur et mot de passe pour l'authentification, afin de garantir une connexion sécurisé crypté.

```
SW-ACCESS-1(config)#ip domain-name badr.local
SW-ACCESS-1(config)#crypto key generate RSA
The name for the keys will be: SW-ACCESS-1.badr.local
Choose the size of the key modulus in the range of 360 to 2048 for
your
  General Purpose Keys. Choosing a key modulus greater than 512 may
take
  a few minutes.

How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

SW-ACCESS-1(config)#ip ssh version 2
*Mar 1 0:8:13.494: %SSH-5-ENABLED: SSH 1.99 has been enabled
SW-ACCESS-1(config)#username badr password badr
SW-ACCESS-1(config)#line vty 0 15
SW-ACCESS-1(config-line)#transport input ssh
SW-ACCESS-1(config-line)#login local
```

Figure IV. 65:Configuration d'accès à distance (SW-ACC).

f) Activez le port sécurisez en niveau des Switchs accès a fin de mieux sécurisé les équipements.

```
switch_ACCESS_1#interface FastEthernet0/2
switch_ACCESS_1(config-if)# switchport access vlan 11
switch_ACCESS_1(config-if)# switchport mode access
switch_ACCESS_1(config-if)#switchport port-security
switch_ACCESS_1(config-if)#switchport port-security violation restrict
switch_ACCESS_1(config-if)# switchport port-security mac-address 0030.A331.C756
switch_ACCESS_1(config-if)# spanning-tree portfast
```

Figure IV.66:Activez le port sécurisez.

IV.3.3.2 Configuration des stations de travails

Pour les postes de travails, nous allons sélectionner le mode DHCP pour chaque machine afin qu'elle profite du fonctionnement de ce protocole. En vas voir en détail la configuration de protocole DHCP la plage Gateway, l'élimination des adressé dans la couche distribution en niveau de Switch niveau 3.

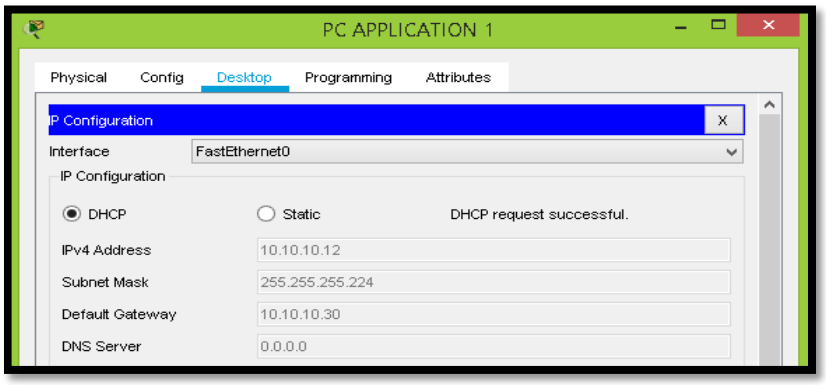


Figure IV.67: Mode DHCP sur les stations de travails.

Le DHCP attribuera une adresse IP, le masque de sous-réseau ainsi qu'une passerelle par default selon le VLAN qu'appartient la machine et tout cela automatiquement.

IV.3.3.3 Configuration des Téléphones IP

Mettre les ports reliant les téléphones en mode Voice, les adresses IP seras effectuer en niveau de couche distribution.

```
switch_ACCESS_3(config)#vlan 200
switch_ACCESS_3(config)#int fa0/4
switch_ACCESS_3(config-if)#switchport mode access
switch_ACCESS_3(config-if)#switchport voice vlan 200
switch_ACCESS_3(config-if)#spanning-tree portfast
```

Figure IV.68:Configuration des Téléphones IP.

IV.3.4 Configuration couche distribution

Nous allons configurer les commutateurs niveau 3, ainsi que la mise en place de la redondance.

IV.3.4.1 Configuration des commutateurs niveau 3

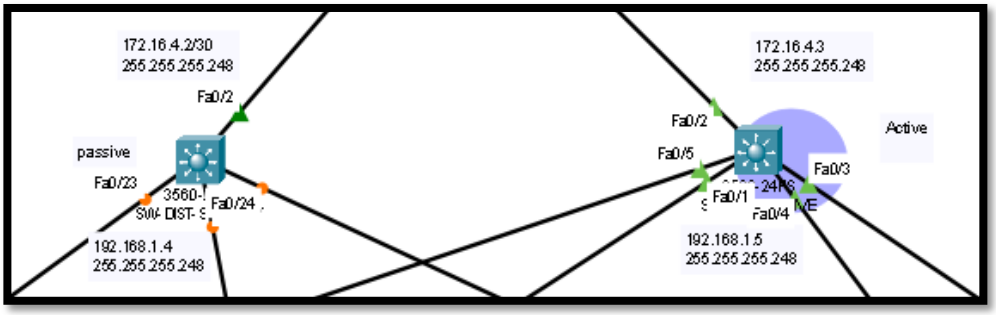


Figure IV.69:Schéma conceptuelle de la Couche Distribution.

En vas débuter la configuration pour chaque commutateur, nous devons suivant les éléments si dessous :

a) **Configuration de Hostname.**
b) **Adressage par DHCP**
c) **Création des vlan ainsi attribution des noms**
d) **Configuration des ports.**
e) **Configuration des routes statiques.**
f) **Configuration du routage inter-vlan.**
g) **Configuration des ACLs.**
h) **Configuration de redondance (Protocole HSRP)**
i) **Configuration d'accès à distance (SSH)**

a) Configuration de Hostname.

```
switch#conf t
Switch(config)#hostname SW-DIST-ACTIVE
SW-DIST-ACTIVE(config)#
```

Figure IV.70:Configuration de Hostname (SW-DIS).

b) Adressage par DHCP

- ✓ Attribution les plages d'adresse de chaque vlan grâce a se protocole automatiquement l'obtention des plages d'adresses, passerelles.

```
SW-DIST-ACTIVE(config)#ip dhcp pool lan-app
SW-DIST-ACTIVE(dhcp-config)#network 10.10.10.0 255.255.255.224
SW-DIST-ACTIVE(dhcp-config)#default-router 10.10.10.30
SW-DIST-ACTIVE(dhcp-config)#ex
SW-DIST-ACTIVE(config)#ip dhcp pool lan-crt
SW-DIST-ACTIVE(dhcp-config)#network 10.10.10.32 255.255.255.224
SW-DIST-ACTIVE(dhcp-config)#default-router 10.10.10.62
SW-DIST-ACTIVE(dhcp-config)#ex
SW-DIST-ACTIVE(config)#ip dhcp pool lan-trt
SW-DIST-ACTIVE(dhcp-config)#network 10.10.10.64 255.255.255.240
SW-DIST-ACTIVE(dhcp-config)#default-router 10.10.10.78
SW-DIST-ACTIVE(dhcp-config)#ex
SW-DIST-ACTIVE(config)#ip dhcp pool lan-drt
SW-DIST-ACTIVE(dhcp-config)#network 10.10.10.80 255.255.255.240
SW-DIST-ACTIVE(dhcp-config)#default-router 10.10.10.94
SW-DIST-ACTIVE(dhcp-config)#ex
SW-DIST-ACTIVE(config)#ip dhcp pool lan-phone
SW-DIST-ACTIVE(dhcp-config)#network 192.168.4.0 255.255.255.0
SW-DIST-ACTIVE(dhcp-config)#default-router 192.168.4.254
SW-DIST-ACTIVE(dhcp-config)#option 150 ip 10.0.1.1
SW-DIST-ACTIVE(dhcp-config)#ex
```

Figure IV.71:Adressage par DHCP.

- ✓ Elimination de quelque adresse utilisable.

```
SW-DIST-ACTIVE(config)#ip dhcp excluded-address 10.10.10.30
SW-DIST-ACTIVE(config)#ip dhcp excluded-address 10.10.10.62
SW-DIST-ACTIVE(config)#ip dhcp excluded-address 10.10.10.78
SW-DIST-ACTIVE(config)#ip dhcp excluded-address 10.10.10.94
SW-DIST-ACTIVE(config)#ip dhcp excluded-address 10.10.10.1
SW-DIST-ACTIVE(config)#ip dhcp excluded-address 10.10.10.33
SW-DIST-ACTIVE(config)#ip dhcp excluded-address 10.10.10.65
SW-DIST-ACTIVE(config)#ip dhcp excluded-address 10.10.10.81
SW-DIST-ACTIVE(config)#ip dhcp excluded-address 10.10.10.2
SW-DIST-ACTIVE(config)#ip dhcp excluded-address 10.10.10.34
SW-DIST-ACTIVE(config)#ip dhcp excluded-address 10.10.10.66
SW-DIST-ACTIVE(config)#ip dhcp excluded-address 10.10.10.82
```

Figure IV.72:Elimination les adresses utilisable.

c) création des vlan ainsi attribuer leur noms

```
SW-DIST-ACTIVE(config)#vlan 10
SW-DIST-ACTIVE(config-vlan)#name lan-ant
SW-DIST-ACTIVE(config-vlan)#ex
SW-DIST-ACTIVE(config)#vlan 11
SW-DIST-ACTIVE(config-vlan)#name lan-app
SW-DIST-ACTIVE(config-vlan)#ex
SW-DIST-ACTIVE(config)#vlan 12
SW-DIST-ACTIVE(config-vlan)#name lan-crt
SW-DIST-ACTIVE(config-vlan)#ex
SW-DIST-ACTIVE(config)#vlan 13
SW-DIST-ACTIVE(config-vlan)#name lan-trt
SW-DIST-ACTIVE(config-vlan)#ex
SW-DIST-ACTIVE(config)#vlan 14
SW-DIST-ACTIVE(config-vlan)#name lan-drt
SW-DIST-ACTIVE(config-vlan)#ex
SW-DIST-ACTIVE(config)#vlan 200
SW-DIST-ACTIVE(config-vlan)#name lan-phone
SW-DIST-ACTIVE(config-vlan)#ex
SW-DIST-ACTIVE(config)#vlan 100
SW-DIST-ACTIVE(config-vlan)#name dist
SW-DIST-ACTIVE(config-vlan)#ex
SW-DIST-ACTIVE(config)#vlan 101
SW-DIST-ACTIVE(config-vlan)#name conx
SW-DIST-ACTIVE(config-vlan)#ex
```

Figure IV.73:Création des VLAN (SW-DIS).

- ✓ En vas attribuer une adresse IP aux interfaces de chaque VLAN afin d'utilisé comme Gateway en niveau des équipements finaux.

```
SW-DIST-ACTIVE(config)#interface vlan 11
SW-DIST-ACTIVE(config-if)#
%LINK-5-CHANGED: Interface Vlan11, changed state to up

SW-DIST-ACTIVE(config-if)#ip address 10.10.10.30 255.255.255.224
SW-DIST-ACTIVE(config-if)#no shutdown
SW-DIST-ACTIVE(config-if)#ex
```

Figure IV.74:Affectation adresse pour vlan (SW-DIS).

- ✓ Créer le VLAN management au niveau de Switch distribution afin d'avoir l'accès a distance en cas de défaillance et le déplacement n'est pas possible :

```
SW-DIST-ACTIVE(config)#interface vlan 100
SW-DIST-ACTIVE(config-if)#
%LINK-5-CHANGED: Interface Vlan100, changed state to up

SW-DIST-ACTIVE(config-if)#ip address 192.168.1.5 255.255.255.248
SW-DIST-ACTIVE(config-if)#no shutdown
SW-DIST-ACTIVE(config-if)#ex
```

Figure IV.75:création vlan management (SW-DIS).

d) Configuration des ports

✓ En vas configurer les ports des Switchs niveau trois comme trunk afin d'éviter d'utiliser plusieurs câbles et la notion DOT1Q afin conserver les numéros de vlan

```
SW-DIST-ACTIVE(config)#interface range  fa 0/1-5
SW-DIST-ACTIVE(config-if)#switchport mode trunk
SW-DIST-ACTIVE(config-if)#switchport trunk encapsulation dot1q
```

Figure IV.76:Configuration des ports.

✓ Le port destiné au firewall sera en mode trunk et aura une adresse privé (172.16.4.0) du VLAN 101.

```
SW-DIST-ACTIVE(config)#interface fa0/2
SW-DIST-ACTIVE(config-if)#switchport trunk encapsulation dot1q
SW-DIST-ACTIVE(config-if)#switchport mode trunk

SW-DIST-ACTIVE(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan11, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan12, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan13, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan14, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan100, changed state to up

SW-DIST-ACTIVE(config-if)#switchport access vlan 101
SW-DIST-ACTIVE(config-if)#no shutdown
SW-DIST-ACTIVE(config-if)#ex
SW-DIST-ACTIVE(config)#int vlan 101
SW-DIST-ACTIVE(config-if)#
%LINK-5-CHANGED: Interface Vlan101, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan101, changed state to up

SW-DIST-ACTIVE(config-if)#ip address 172.16.4.3 255.255.255.248
SW-DIST-ACTIVE(config-if)#no shutdown
SW-DIST-ACTIVE(config-if)#ex
```

Figure IV.77:configuration interface qui destiné au firewall.

e) Configuration des routes statiques

✓ En vas configurer les routes qui mènent au site central à travers Gateway de firewal

```
SW-DIST-ACTIVE(config)#ip route 192.168.10.0 255.255.255.0 172.16.4.1
SW-DIST-ACTIVE(config)#ip route 192.168.3.0 255.255.255.0 172.16.4.1
SW-DIST-ACTIVE(config)#ip route 192.168.2.0 255.255.255.0 172.16.4.1
SW-DIST-ACTIVE(config)#ip route 10.0.1.0 255.255.255.0 172.16.4.1
SW-DIST-ACTIVE(config)#ip route 192.168.5.0 255.255.255.0 172.16.4.1
SW-DIST-ACTIVE(config)#ex
```

Figure IV.78:Configuration des routes statiques.

f) Configuration du routage inter-vlan.

✓ Configuration du routage inter-vlan grâce à la commande **IP Routing.**

```
SW-DIST-ACTIVE(config)#ip routing
```

Figure IV.79:Configuration du routage inter-vlan.

g) Configuration des ACLs

```
SW-DIST-ACTIVE(config)#access-list 101 deny tcp 10.10.10.0 0.0.0.255 host 10.10.10.30 eq 22
SW-DIST-ACTIVE(config)#access-list 101 deny tcp 10.10.10.0 0.0.0.255 host 10.10.10.62 eq 22
SW-DIST-ACTIVE(config)#access-list 101 deny tcp 10.10.10.0 0.0.0.255 host 10.10.10.78 eq 22
SW-DIST-ACTIVE(config)#access-list 101 deny tcp 10.10.10.0 0.0.0.255 host 10.10.10.94 eq 22
SW-DIST-ACTIVE(config)#access-list 101 deny tcp 10.10.10.0 0.0.0.255 192.168.1.0 0.0.0.255 eq 22
SW-DIST-ACTIVE(config)#access-list 101 permit tcp host 192.168.10.10 192.168.1.0 0.0.0.255 eq 22
SW-DIST-ACTIVE(config)#access-list 101 permit ip any any
SW-DIST-ACTIVE(config)#access-list 101 permit icmp any any
```

Figure IV.80:Configuration des ACLs.

✓ Nous activerons cette ACL au niveau des interfaces VLAN en entrée (IN).

```
SW-DIST-ACTIVE#wr
SW-DIST-ACTIVE(config)#int vlan 10
SW-DIST-ACTIVE(config-if)#ip access-group 101 in
SW-DIST-ACTIVE(config-if)#ex
SW-DIST-ACTIVE(config)#int vlan 11
SW-DIST-ACTIVE(config-if)#ip access-group 101 in
SW-DIST-ACTIVE(config-if)#ex
SW-DIST-ACTIVE(config)#int vlan 12
SW-DIST-ACTIVE(config-if)#ip access-group 101 in
SW-DIST-ACTIVE(config-if)#ex
SW-DIST-ACTIVE(config)#int vlan 13
SW-DIST-ACTIVE(config-if)#ip access-group 101 in
SW-DIST-ACTIVE(config-if)#ex
SW-DIST-ACTIVE(config)#int vlan 14
SW-DIST-ACTIVE(config-if)#ip access-group 101 in
SW-DIST-ACTIVE(config-if)#ex
SW-DIST-ACTIVE(config)#int vlan 100
SW-DIST-ACTIVE(config-if)#ip access-group 101 in
SW-DIST-ACTIVE(config-if)#ex
SW-DIST-ACTIVE(config)#int vlan 101
SW-DIST-ACTIVE(config-if)#ip access-group 101 in
SW-DIST-ACTIVE(config-if)#ex
SW-DIST-ACTIVE(config)#
```

Figure IV.81:Activation des ACLs (SW-DIST).

h) Configuration de redondance (Protocole HSRP)

✓ Les flexibilités, la disponibilité est un élément essentiel, donc la redondance de passerelles est la solution adéquate en attribuent une adresse virtuelle aux vlan correspondant, si un des Switchs tombent en pannes l'autre il va prendre la relèves sans reconfigurer quoi que se soit.

```
interface Vlan10
 mac-address 0009.7c2b.5701
 ip address 10.10.10.99 255.255.255.248
 ip access-group 101 in
 standby 10 ip 10.10.10.98
 standby 10 priority 150
 standby 10 preempt
!
interface Vlan11
 mac-address 0009.7c2b.5702
 ip address 10.10.10.1 255.255.255.224
 ip access-group 101 in
 standby 11 ip 10.10.10.30
 standby 11 priority 150
 standby 11 preempt
!
interface Vlan12
 mac-address 0009.7c2b.5703
 ip address 10.10.10.33 255.255.255.224
 ip access-group 101 in
 standby 12 ip 10.10.10.62
 standby 12 priority 150
 standby 12 preempt
```

Figure IV.82:Configuration Protocole HSRP.

✓ La synchronisation entre les deux Switchs se fera au démarrage des Switchs.

```
%HSRP-6-STATECHANGE: Vlan12 Grp 12 state Speak -> Standby
%HSRP-6-STATECHANGE: Vlan13 Grp 13 state Speak -> Standby
%HSRP-6-STATECHANGE: Vlan100 Grp 100 state Speak -> Standby
%HSRP-6-STATECHANGE: Vlan12 Grp 12 state Standby -> Active
%HSRP-6-STATECHANGE: Vlan100 Grp 100 state Standby -> Active
%HSRP-6-STATECHANGE: Vlan10 Grp 10 state Speak -> Standby
%HSRP-6-STATECHANGE: Vlan13 Grp 13 state Standby -> Active
%HSRP-6-STATECHANGE: Vlan10 Grp 10 state Standby -> Active
%HSRP-6-STATECHANGE: Vlan11 Grp 11 state Speak -> Standby
%HSRP-6-STATECHANGE: Vlan11 Grp 11 state Standby -> Active
%HSRP-6-STATECHANGE: Vlan101 Grp 2 state Speak -> Standby
%HSRP-6-STATECHANGE: Vlan101 Grp 2 state Standby -> Active
```

Figure IV.83:La synchronisation.

i) Configuration d'accès à distance (SSH).

Pour accéder à distance aux Switchs distributeurs, nous configurons le protocole SSH suivi d'une adresse IP VLAN 100 qui servira de passerelle pour l'accès à distance.

```
SW-DIST-ACTIVE(config)#ip domain-name badr.local
SW-DIST-ACTIVE(config)#crypto key generate RSA
The name for the keys will be: SW-DIST-ACTIVE.badr.local
Choose the size of the key modulus in the range of 360 to 2048 for
your
  General Purpose Keys. Choosing a key modulus greater than 512 may
take
  a few minutes.

How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

SW-DIST-ACTIVE(config)#ip ssh version 2
*Mar 1 1:25:7.904: %SSH-5-ENABLED: SSH 1.99 has been enabled
SW-DIST-ACTIVE(config)#username badr password badr
SW-DIST-ACTIVE(config)#line vty 0 15
SW-DIST-ACTIVE(config-line)#transport input ssh
SW-DIST-ACTIVE(config-line)#login local
SW-DIST-ACTIVE(config-line)#ex
```

Figure IV.84:Configuration d'accès à distance (SSH).

IV.3.5 Configuration site centrale

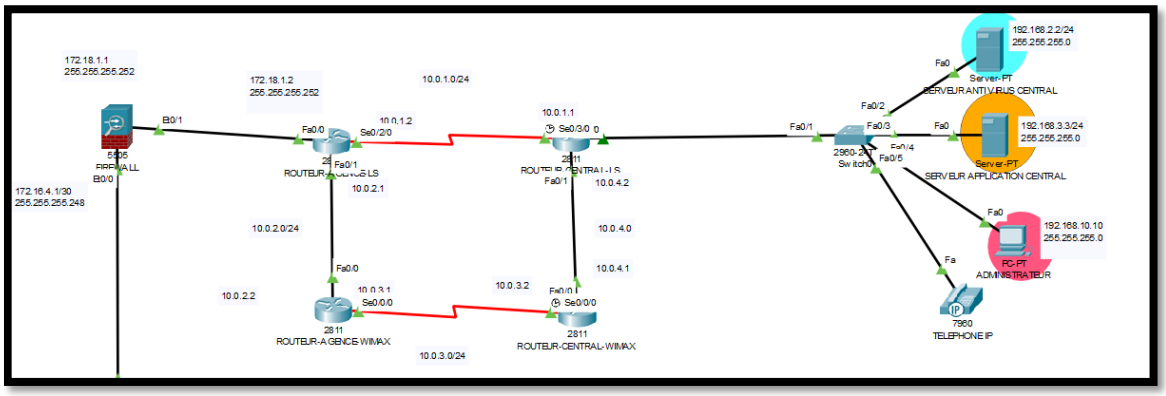


Figure IV.85:Schéma conceptuelle de site central.

En vas débuter la configuration pour chaque routeur nous devons suivant les éléments si dessous :

a) **Configuration de Hostname.**
b) **Assigner une adresse IP ainsi le masque dans chaque interface.**
c) **Configuration des sub-interfaces.**
d) **Configuration de protocole OSPF.**
e) **Configuration des routes statiques.**
f) **Configuration des téléphones VOIP.**
g) **Configuration des ACLs aux niveaux des routeurs.**
h) **Configuration de serveur email, syslog, ntp**

Configuration les équipements de sécurité

i) **Configuration des interfaces firewal.**
j) **Configuration des ACLs en niveau de firewal**

a) Configuration de Hostname.

```
Router(config)#hostname ROUTEUR-CENTRAL-LS
ROUTEUR-CENTRAL-LS(config)#
```

Figure IV.86:configuration de Hostname (ROUTER).

b) Assigner une adresse IP ainsi le masque dans chaque interface.

```
ROUTEUR-CENTRAL-LS(config)#int s0/3/0
ROUTEUR-CENTRAL-LS(config-if)#ip address 10.0.1.1 255.255.255.252
ROUTEUR-CENTRAL-LS(config-if)#no shut

%LINK-5-CHANGED: Interface Serial0/3/0, changed state to down
ROUTEUR-CENTRAL-LS(config-if)#
ROUTEUR-CENTRAL-LS(config-if)#clock rate 64000
```

Figure IV.87:Configuration des interfaces.

c) Configuration des sub-interfaces.

```
Router(config)#interface FastEthernet0/0.1
Router(config-subif)#encapsulation dot1Q 20
Router(config-subif)#ip address 192.168.2.254 255.255.255.0
Router(config-subif)#no shu
Router(config-subif)#ex
Router(config)#interface FastEthernet0/0.2
Router(config-subif)#encapsulation dot1Q 30
Router(config-subif)#ip address 192.168.3.254 255.255.255.0
Router(config-subif)#no sh
Router(config-subif)#ex
Router(config)#interface FastEthernet0/0.3
Router(config-subif)#encapsulation dot1Q 40
Router(config-subif)#ip address 192.168.10.254 255.255.255.0
Router(config-subif)#no sh
Router(config-subif)#ex
Router(config)#interface FastEthernet0/0.4
Router(config-subif)#encapsulation dot1Q 50
Router(config-subif)#ip address 192.168.5.254 255.255.255.0
Router(config-subif)#no sh
Router(config-subif)#ex
Router(config)#interface FastEthernet0/0.100
Router(config-subif)#encapsulation dot1Q 100
Router(config-subif)#ip address 192.168.1.13 255.255.255.248
Router(config-subif)#no sh
Router(config-subif)#ex
```

Figure IV.88:Configuration des sub-interfaces.

d) Configuration de protocole OSPF

En recommandera d'être le plus précis possible dans la désignation d'interface, car il sera plus aisé d'agir, en a recommander d'utiliser OSPF puisque les routeurs en des connaissances complète sur la topologie, la limite du nombre de saut n'est plus nécessaire.

```
ROUTEUR-CENTRAL-LS(config)#router ospf 1
ROUTEUR-CENTRAL-LS(config-router)# network 10.0.1.1 0.0.0.0 area 0
ROUTEUR-CENTRAL-LS(config-router)# network 10.0.4.2 0.0.0.0 area 0
ROUTEUR-CENTRAL-LS(config-router)# network 192.168.2.254 0.0.0.0 area 0
ROUTEUR-CENTRAL-LS(config-router)# network 192.168.3.254 0.0.0.0 area 0
ROUTEUR-CENTRAL-LS(config-router)#network 192.168.10.254 0.0.0.0 area 0
ROUTEUR-CENTRAL-LS(config-router)# network 192.168.5.254 0.0.0.0 area 0
ROUTEUR-CENTRAL-LS(config-router)#ex
```

Figure IV.89:Configuration de protocole OSPF.

e) Configuration des routes statiques en niveau de routeur central.

En vas être plus détaillé sur la configuration des autres équipements

```
ROUTEUR-CENTRAL-LS(config)#ip route 10.10.10.0 255.255.255.0 10.0.1.2
ROUTEUR-CENTRAL-LS(config)#ip route 192.168.1.0 255.255.255.248 10.0.1.2
ROUTEUR-CENTRAL-LS(config)#ip route 172.18.1.0 255.255.255.252 10.0.4.1 120
ROUTEUR-CENTRAL-LS(config)#ip route 10.10.10.0 255.255.255.0 10.0.4.1 120
ROUTEUR-CENTRAL-LS(config)#ip route 192.168.1.0 255.255.255.248 10.0.4.1 120
ROUTEUR-CENTRAL-LS(config)#ip route 192.168.4.0 255.255.255.0 10.0.1.2
ROUTEUR-CENTRAL-LS(config)#ip route 172.16.4.0 255.255.255.248 10.0.1.2
```

Figure IV.90:Configuration des routes statiques.

f) Configuration des téléphones VOIP.

En vas affecter en vlan phone un pool d'adressages.

```
ROUTEUR-CENTRAL-LS(config)#ipdhcp pool Phones
ROUTEUR-CENTRAL-LS(dhcp-config)# network 192.168.5.0 255.255.255.0
ROUTEUR-CENTRAL-LS(dhcp-config)# default-router 192.168.5.254
ROUTEUR-CENTRAL-LS(dhcp-config)# option 150 ip 10.0.1.1
```

Figure IV.91 : Configuration du service de la VoIP.

```
ROUTEUR-CENTRAL-LS(config)#dial-peervoice 1 voip
ROUTEUR-CENTRAL-LS(config-dial-peer)# destination-pattern 1...
ROUTEUR-CENTRAL-LS(config-dial-peer)# session target ipv4:192.168.4.2
ROUTEUR-CENTRAL-LS(config-dial-peer)#
ROUTEUR-CENTRAL-LS(config-dial-peer)#dial-peervoice 2 voip
ROUTEUR-CENTRAL-LS(config-dial-peer)#destination-pattern 1...
ROUTEUR-CENTRAL-LS(config-dial-peer)#session target ipv4:192.168.4.1
ROUTEUR-CENTRAL-LS(config-dial-peer)#
ROUTEUR-CENTRAL-LS(config-dial-peer)#dial-peervoice 3 voip
ROUTEUR-CENTRAL-LS(config-dial-peer)#destination-pattern 1...
ROUTEUR-CENTRAL-LS(config-dial-peer)#session target ipv4:192.168.4.3
ROUTEUR-CENTRAL-LS(config-dial-peer)#
ROUTEUR-CENTRAL-LS(config-dial-peer)#dial-peervoice 4 voip
ROUTEUR-CENTRAL-LS(config-dial-peer)#destination-pattern 2...
ROUTEUR-CENTRAL-LS(config-dial-peer)# session target ipv4:192.168.5.1
```

Figure IV.92:configuration le prototype DHCP pour les téléphones.

Nous définissons un nombre maximal y de numéros avec la commande « max-dn y ».

Nous définissons l'adresse IP du Call manager sur le port 2000 avec la commande « ip source-address 10.0.1.1 port 2000».

Nous autorisons l'ajout automatique des téléphones aux numéros libres avec la commande « auto assign 1 to 10 ».

```
ROUTEUR-CENTRAL-LS(config-dial-peer)#telephony-service
ROUTEUR-CENTRAL-LS(config-telephony)# max-ephones 10
ROUTEUR-CENTRAL-LS(config-telephony)# max-dn 10
ROUTEUR-CENTRAL-LS(config-telephony)# ip source-address 10.0.1.1 port 2000
ROUTEUR-CENTRAL-LS(config-telephony)# auto assign 1 to 10
```

Figure IV.93:Mode telephony-service.

Ensuite nous sortirons du mode 'telephony-service' et nous définissons les numéros de téléphones.

```
Router(config)#ephone-dn 1
Router(config-ephone-dn)#number 1001
Router(config-ephone-dn)#ex
Router(config)#%LINK-3-UPDOWN: Interface ephone_dsp DN 1.1, changed state to up

Router(config)#ephone-dn 2
Router(config-ephone-dn)#number 1002
Router(config-ephone-dn)#ex
Router(config)#%LINK-3-UPDOWN: Interface ephone_dsp DN 2.1, changed state to up

Router(config)#ephone-dn 3
Router(config-ephone-dn)#number 1003
Router(config-ephone-dn)#ex
Router(config)#%LINK-3-UPDOWN: Interface ephone_dsp DN 3.1, changed state to up

Router(config)#ephone-dn 4
Router(config-ephone-dn)#number 2001
Router(config-ephone-dn)#ex
Router(config)#%LINK-3-UPDOWN: Interface ephone_dsp DN 4.1, changed state to up
```

Figure IV.94: définition les numéros de téléphones.

g) Configuration d'un ACL

Nous n'autorisons que le PC administrateur central d'accéder au terminal des routeurs à distance via SSH.

Nous n'autorisons que SERVEUR ANTI VIRUS CENTRAL de site central d'accéder au ser-anti-virus de l'agence.

Nous n'autorisons que SERVEUR APPLICATION CENTRAL de site central de communiquer avec les équipements de l'agence

```
ROUTEUR-CENTRAL-LS(config)#access-list 102 permit tcp host 192.168.10.10 host 10.0.1.1 eq 22
ROUTEUR-CENTRAL-LS(config)#access-list 102 permit tcp host 192.168.10.10 host 10.0.1.2 eq 22
ROUTEUR-CENTRAL-LS(config)#access-list 102 permit icmp any any
ROUTEUR-CENTRAL-LS(config)#access-list 102 permit ip host 192.168.2.2 host 10.10.10.97
ROUTEUR-CENTRAL-LS(config)#access-list 102 permit ip host 192.168.3.3 10.10.10.0 0.0.0.31
ROUTEUR-CENTRAL-LS(config)#access-list 102 permit ip any any
```

Figure IV.95:Configuration des ACLs aux niveaux des routeurs.

- ✓ Nous activerons cette ACL au niveau des sub-interfaces.

```
ROUTER-CENTRAL-LS(config)#interface FastEthernet0/0.1
ROUTER-CENTRAL-LS(config-subif)#ip access-group 102 in
ROUTER-CENTRAL-LS(config-subif)#ex
ROUTER-CENTRAL-LS(config)#interface FastEthernet0/0.2
ROUTER-CENTRAL-LS(config-subif)#ip access-group 102 in
ROUTER-CENTRAL-LS(config-subif)#ex
ROUTER-CENTRAL-LS(config)#interface FastEthernet0/0.4
ROUTER-CENTRAL-LS(config-subif)#ip access-group 102 in
ROUTER-CENTRAL-LS(config-subif)#ex
```

Figure IV.96:Activation des ACLs (ROUTER-CENTRAL-LS).

h) Configuration de serveur email, syslog, ntp

La création des comptes email badr.com de server 192.168.7.7, au niveau de chaque équipement en ajoute la commande logging a fin de garder la traçabilité, et ntp de régler l'heur.

Figure IV.97 : Configuration de serveur email

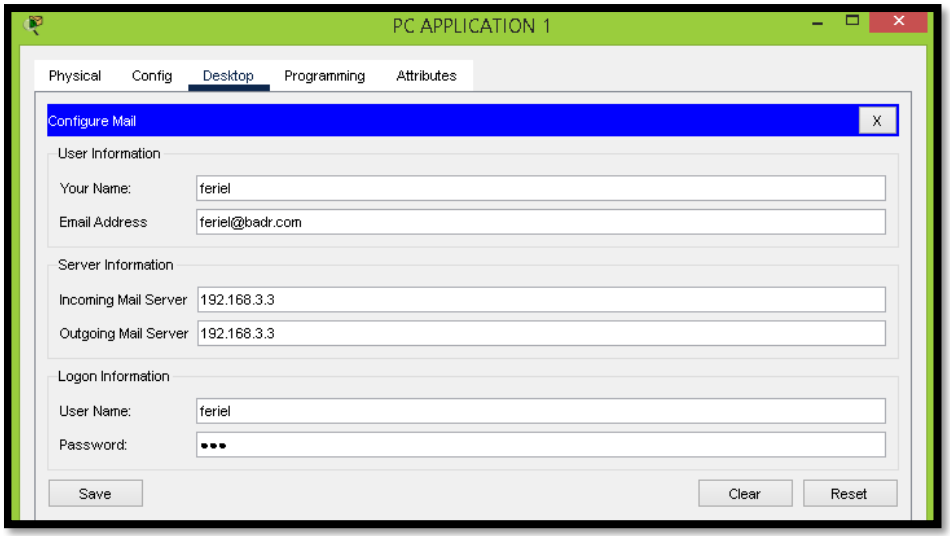


Figure IV.98 : création de compte email

```
ntp server 192.168.3.3
ntp update-calendar
```

Figure IV.99 : Configuration de ntp

```
logging trap debugging
logging 192.168.3.3
```

Figure IV.100 : Configuration de syslog

Configuration les équipements de sécurité de l'agence

i) Configuration des interfaces firewal.

Le principe de notre politique de sécurité est que nous interdissions l'accès externe de tout protocole pouvant provenir sur le réseau local de l'entreprise, et cela, en utilisant la priorité des interfaces du firewall (l'interface de valeur inférieur n'aura pas la possibilité d'accéder à celle qui a une valeur supérieur). Ensuite, nous allons ouvrir l'accès seulement au adresses et aux protocoles voulais via le biais des ACL.

Ce principe est réalisé au niveau interne du réseau de l'agence. Nous pouvons résumer notre politique de sécurité dans les points suivants :

Le niveau de sécurité de l'interface Outside est égale à 0 et donc nous évitons les intrusions de l'extérieur sauf pour les adresses IP autorisé à l'aide des ACL mise en place dans le firewall.

```
FIREWALL(config)#int vlan 2
FIREWALL(config-if)#nameif outside
FIREWALL(config-if)#security-level 0
FIREWALL(config-if)#ip add 172.18.1.1 255.255.255.252
FIREWALL(config-if)#no sh
```

Figure IV.101:Configuration l'interface Outside.

L'interface Inside possède un niveau de sécurité égale à 100, ce qui permet d'autorisé tous les utilisateurs du réseau LAN à accéder au serveur externe des sites distants.

```
FIREWALL#conf t
FIREWALL(config)#int vlan 3
FIREWALL(config-if)#nameif inside
FIREWALL(config-if)#security-level 100
FIREWALL(config-if)#ip add  172.16.4.1 255.255.255.252
FIREWALL(config-if)# no sh
```

Figure IV.102:Configuration l'interface Inside.

j) Configuration des ACLs en niveau de firewal

Dans le but de mise en place notre stratégie de sécurité pour l'entreprise, nous allons configurer des ACL sur le pare-feu qui vont se résumer en une liste d'adresses ou de port autorisés ou interdit par le dispositif de filtrage.

Nous allons créer deux listes ACL pour notre politiques, BADR_IN pour l'interface Inside et une BADR_OUT pour l'interface Outside.

```
FIREWALL(config)#access-list BADR_OUT extended permit tcp host 192.168.2.2 host 10.10.10.97
FIREWALL(config)#access-list BADR_OUT extended permit tcp host 192.168.3.3 10.10.10.0 255.255.255.224
FIREWALL(config)#access-list BADR_OUT extended permit icmp any any
FIREWALL(config)#access-list BADR_OUT extended permit tcp host 192.168.10.10 192.168.1.0 255.255.255.248 eq 22
FIREWALL(config)#access-list BADR_OUT extended permit ip 10.0.1.0 255.255.255.0 192.168.4.0 255.255.255.0
FIREWALL(config)#access-list BADR_IN extended permit tcp host 10.10.10.97 host 192.168.2.2
FIREWALL(config)#access-list BADR_IN extended permit tcp 10.10.10.0 255.255.255.224 host 192.168.3.3
FIREWALL(config)#access-list BADR_IN extended permit tcp 192.168.1.0 255.255.255.248 host 192.168.10.10
FIREWALL(config)#access-list BADR_IN extended permit icmp any any
FIREWALL(config)#access-list BADR_IN extended permit ip 192.168.4.0 255.255.255.0 10.0.1.0 255.255.255.0
```

Figure IV.103:Configuration des ACLs en niveau de firewal.

Ces deux listes nous permettront de :

- Autoriser le serveur application central de communiquer qu'avec les postes appartenant au VLAN application.
- Autoriser le serveur Anti-virus Central de mettre à jours le serveur Anti-virus interne.
- Autorisé l'administrateur central à accéder à distance par SSH à tous équipements appartenant à l'agence.
- Autorisé la communication de la téléphonie IP.

IV.4 Cahier des tests

Pour tester le bon fonctionnement de notre réseau et les communications entre les nœuds, nous allons rédiger dans ce qui suit la liste des tests à effectuer sur notre réseau après l'étape de configuration. Il y aura notamment des tests de connectivités et des tests de fiabilités.

IV.4.1Test et validation de la configuration

Une série de tests serai effectuée afin de valider la configuration et de prouver le bon fonctionnement des équipements. Ces tests consistent à vérifier l'accessibilité de l'ensemble des équipements sur le réseau en utilisant la commande Ping. « Ping » permet d'envoyer des paquets au destinataire dont ce dernier doit recevoir ces paquet pour dire que la communication est réussie autrement elle est échoue.

Nous allons tester progressivement notre configuration en faisant un Ping sur les machines du réseau LAN interne de l'agence.

IV.4.1.1 Test Intra-Vlan

Exemple : Tests réussis entre le PC Crédit 1(10.10.10.36) et le PC Crédit 2 (10.10.10.35) qui appartient au même Vlan12 d'Application.

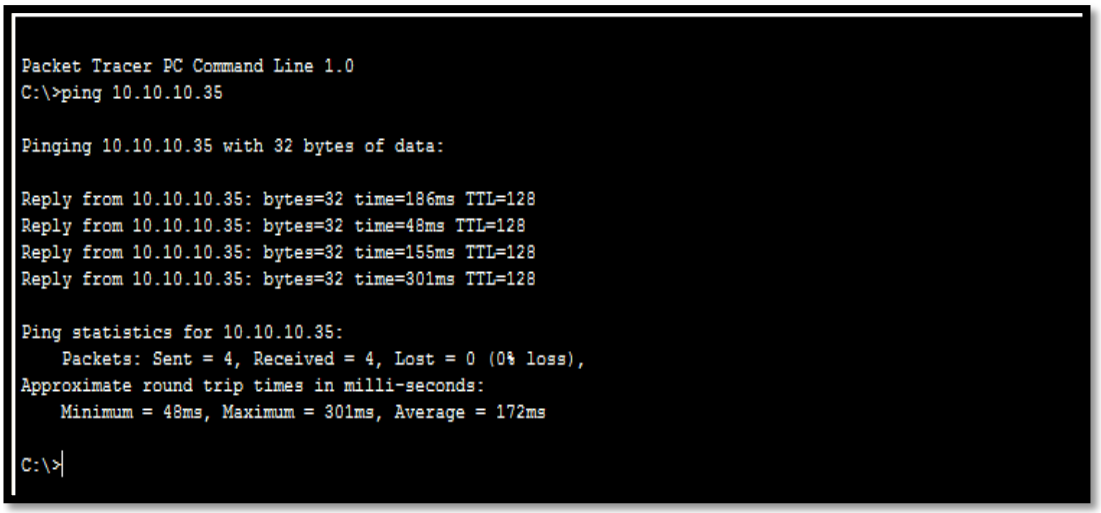


Figure IV.104: Test du Ping intra-vlan.

IV.4.1.2 Test Inter-Vlan

Exemple : Tests réussis entre le PC Crédit 1(10.10.10.36) du Vlan12 et le PC Application (10.10.10.4) du Vlan 11.

```
C:\>ping 10.10.10.4

Pinging 10.10.10.4 with 32 bytes of data:

Reply from 10.10.10.4: bytes=32 time=1720ms TTL=127
Reply from 10.10.10.4: bytes=32 time=12ms TTL=127
Reply from 10.10.10.4: bytes=32 time=649ms TTL=127
Reply from 10.10.10.4: bytes=32 time=1037ms TTL=127
Reply from 10.10.10.4: bytes=32 time=518ms TTL=127

Ping statistics for 10.10.10.4:
    Packets: Sent = 4, Received = 5, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 12ms, Maximum = 1720ms, Average = 787ms
```

Figure IV.105: Test du Ping entre deux VLAN différents.

IV.4.1.3 Test entre site agence et site central

Exemple : le test est effectué à partir d'un poste utilisateur d'application (10.10.10.4) du site agence, vers l'administrateur (192.168.10.10) de la DMSI.

```
Packet Tracer PC Command Line 1.0
C:\>ping 192.168.10.10

Pinging 192.168.10.10 with 32 bytes of data:

Reply from 192.168.10.10: bytes=32 time=230ms TTL=124
Reply from 192.168.10.10: bytes=32 time=244ms TTL=124
Reply from 192.168.10.10: bytes=32 time=152ms TTL=124
Reply from 192.168.10.10: bytes=32 time=100ms TTL=124

Ping statistics for 192.168.10.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 100ms, Maximum = 244ms, Average = 181ms
```

Figure IV.106: Test entre site agence et site central.

IV.4.2 Test de performance Traceroute

Un test de performance a pour objectif de mesurer les temps de réponses d'un système en fonction de sa sollicitation .Car des problèmes, qui ralentissent notre réseau, peuvent surgir, et ce type de problème peut occasionner des pertes de paquets, et, par conséquent des pertes de connectivité.

Même si nous ne perdons pas la connexion, un réseau lent peut être source d'énervement et de baisse de productivité. C'est pourquoi nous avons choisi d'utiliser Traceroute qui va nous permettre de voir ou vont les paquets et d'afficher des statistiques relatives aux performances du réseau.

L'utilitaire Traceroute trace le chemin emprunté par les paquets lorsqu'ils cheminent d'une machine vers leurs destinations, en traversant plusieurs passerelles. Le chemin tracé est simplement un chemin entre la source et la destination.

La commande Traceroute est très utile dans le diagnostic des problèmes de réseaux parce qu'elle permet d'identifier à quel niveau se situe le problème.

La commande retrace le chemin emprunté par notre requête envoyer depuis le site agence pour atteindre notre site distant central.

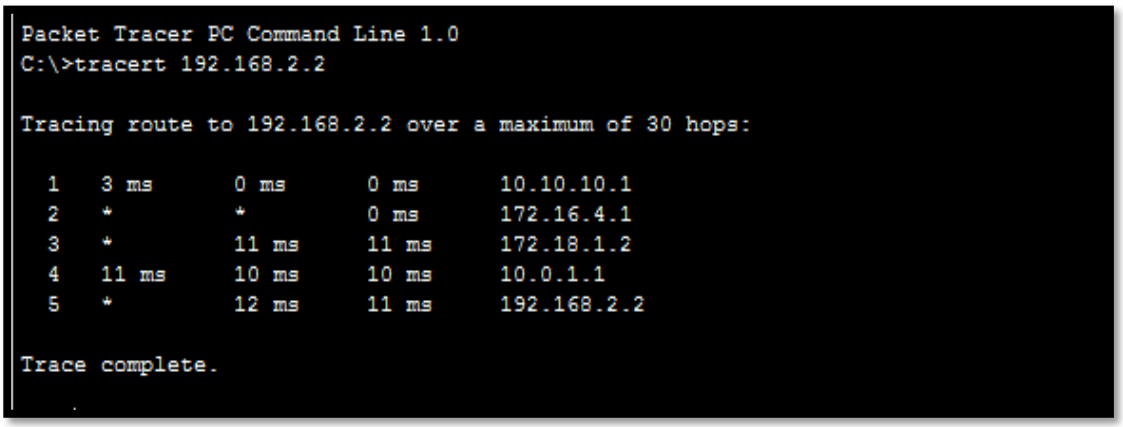


Figure IV.107: Exemple du tracé d'un chemin allant du site agence vers le site

Nous remarquons que la requête est passée par le commutateur actif niveau 3 SW-DIST-ACTIVE (10.10.10.1) puis la route d'interface Inside du firewall (172.16.4.1), passant par le routeur LS de l'agence (172.18.1.2), puis par le routeur LS central (10.0.1.1) pour atteindre sa destination (192.168.2.2).Ceci signifie que la requête est réussie et par suite permet de conclure que le routage est fonctionnel.

IV.4.3 Tests de fiabilité (Haute disponibilité)

IV.4.3.1 Test de redondance physique des commutateurs niveau 3

Pour tester la redondance des Switchs niveau 3 mis dans l'architecture proposé, il faut débrancher ou éteindre l'un des switches et laisser l'autre Switchs fonctionner et puis tester si la connectivité de notre réseau est établie; puis en lance la commande Traceroute pour voir si vraiment les trames de donnée transite par le Switch correspondant.

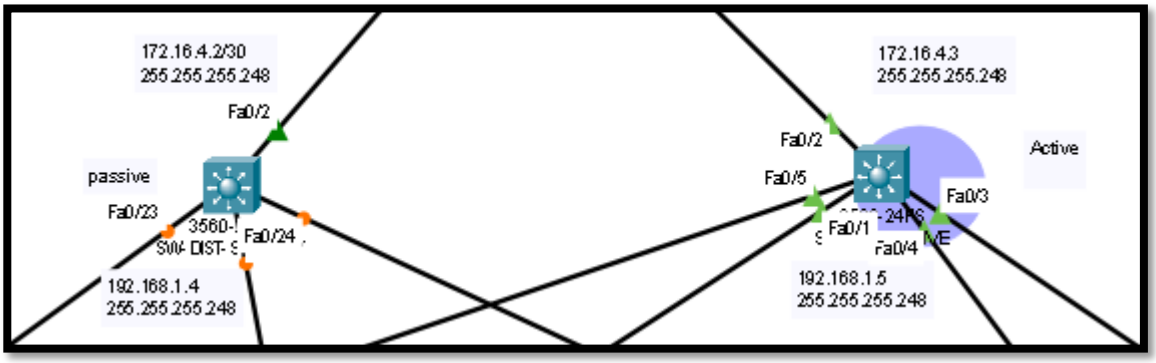


Figure IV.108: Représentation de la redondance physique des commutateurs niveau 3.

Pour voir si la redondance est différents chemins lorsque nous atteindrons le Switch active.

Au début du test nous laissons le Switch SW-DIST-ACTIVE (10.10.10.81) dans l'état actif et le Switch SW-DIST-STANDBY (10.10.10.82) dans l'état standby.

```
Packet Tracer PC Command Line 1.0
C:\>tracert 192.168.2.2

Tracing route to 192.168.2.2 over a maximum of 30 hops:

  1    1 ms      0 ms      0 ms      10.10.10.81
  2    *         0 ms      1 ms      172.16.4.1
  3    15 ms     20 ms     0 ms      172.18.1.2
  4    1 ms      10 ms     1 ms      10.0.1.1
  5    10 ms     10 ms     11 ms     192.168.2.2

Trace complete.
```

Figure IV.109: Traceroute avant d'éteindre le switch active.

Après quand nous atteindrons le Switch SW-DIST-ACTIVE, le trafic bascule automatiquement vers le Switch SW-DIST-STANDBY qui devient en état active et emprunte un chemin différent du premier pour arriver à destination.

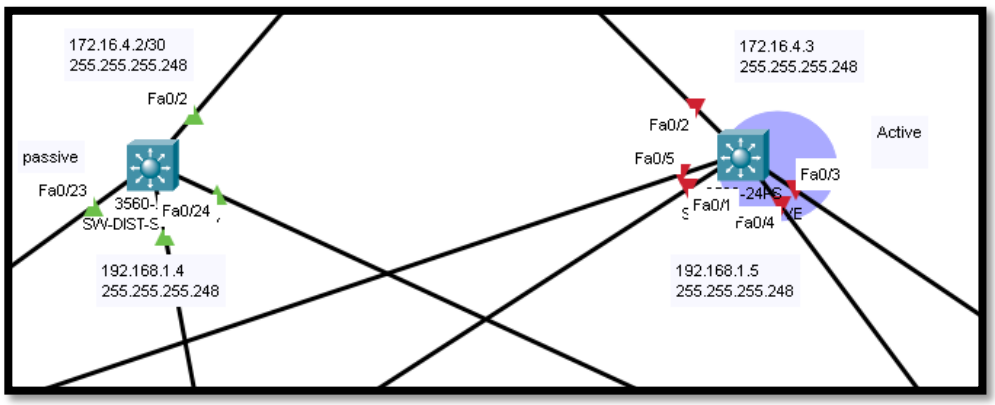


Figure IV.110:Désactiver les ports de SW-DIST-ACTIVE.

Lorsqu'en lance la commande Traceroute sur le pc ca nous donne le résultat suivant, le trafic bascule vers l'adresse 10.10.10.82 en lieu de 10.10.10.81.

```
Packet Tracer PC Command Line 1.0
C:\>tracert 192.168.2.2

Tracing route to 192.168.2.2 over a maximum of 30 hops:

  1    0 ms      0 ms      17 ms     10.10.10.82
  2    *         0 ms      0 ms      172.16.4.1
  3    1 ms      0 ms      0 ms      172.18.1.2
  4    14 ms     10 ms     1 ms      10.0.1.1
  5    10 ms     10 ms     11 ms     192.168.2.2

Trace complete.
```

Figure IV.111: Traceroute après avoir éteint le switch active.

Ceci démontre que la redondance est fonctionnelle et que le protocole HSRP s'exécute de manière.

IV.4.3.2 Test de redondance physique des liaisons d'interconnexion

Pour tester la liaison de backup de technologie WiMax, il faut supprimer la ligne spécialisée et puis tester la connectivité avec Traceroute.

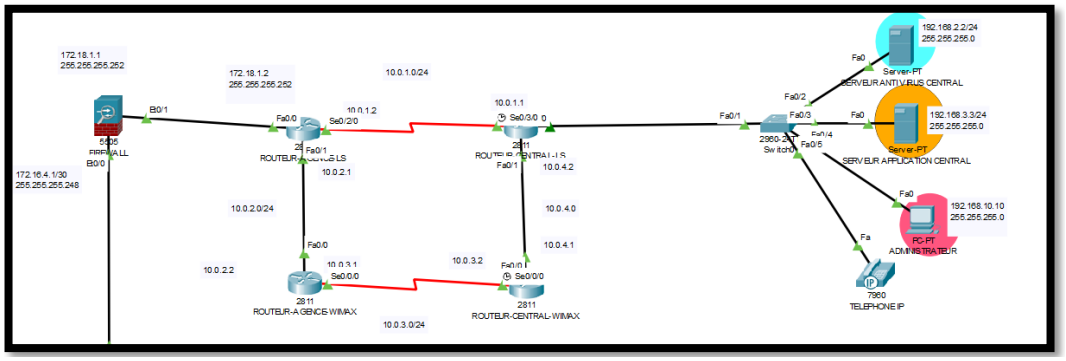


Figure IV.112: Redondance de liaison d'interconnexion Avant coupure.

Au début du test, nous laissons en marche la ligne spécialisé LS (10.0.1.1), pour voir ce qui ca donne le tracé.

```
Packet Tracer PC Command Line 1.0
C:\>tracert 192.168.2.2

Tracing route to 192.168.2.2 over a maximum of 30 hops:

  1    1 ms      0 ms      0 ms      10.10.10.81
  2    *         0 ms      1 ms      172.16.4.1
  3    15 ms     20 ms     0 ms      172.18.1.2
  4    1 ms      10 ms     1 ms      10.0.1.1
  5    10 ms     10 ms     11 ms     192.168.2.2

Trace complete.
```

Figure IV.113: Traceroute avant coupure de ligne spécialisée LS.

Après coupure de la ligne LS, le trafic bascule automatiquement vers le routeur du WiMax (ROUTER-CENTRAL-WIMAX) et emprunte la route du WiMax.

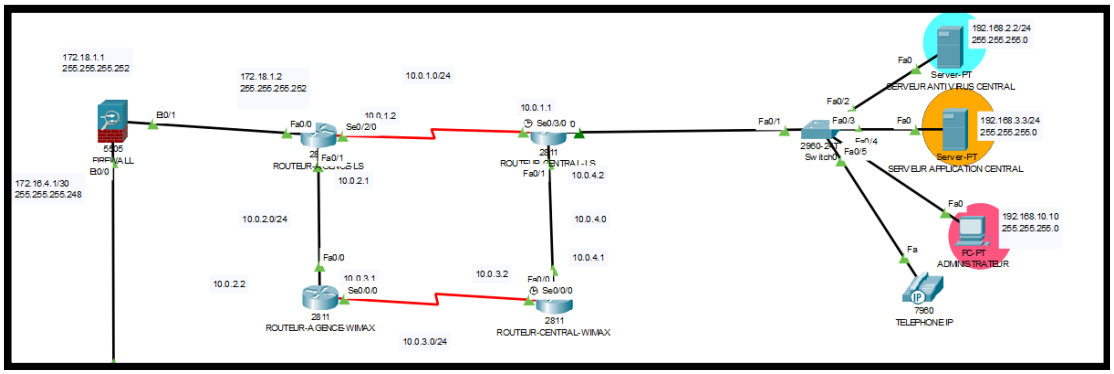


Figure IV.114: Redondance de liaison d'interconnexion Après coupure.

En teste la commande tracert pour voir les résultats, ici le trafic bascule vers l'interfaces 10.0.2.2 puis 10.0.3.2 puis 10.0.4.2 jusqu'a éteindre la destination.

```
C:\>tracert 192.168.2.2

Tracing route to 192.168.2.2 over a maximum of 30 hops:

  1    12 ms      0 ms      1 ms      10.10.10.81
  2    *          *         11 ms     172.16.4.1
  3    10 ms      10 ms     10 ms     172.18.1.2
  4    11 ms      10 ms     10 ms     10.0.2.2
  5    3 ms       11 ms     11 ms     10.0.3.2
  6    12 ms      13 ms     10 ms     10.0.4.2
  7    13 ms      21 ms     15 ms     192.168.2.2

Trace complete.
```

Figure IV.115: Traceroute après coupure de ligne spécialisé LS.

Ceci démontre que la technique du backup de liaison d'interconnexion est fonctionnelle et s'exécute de manière correcte.

IV.4.4 Vérification du Service HTTP et HTTPS

Comme nous accédons au serveur application de l'autre site à l'aide d'une page web, nous pouvons conclure que le service web est fonctionnel.

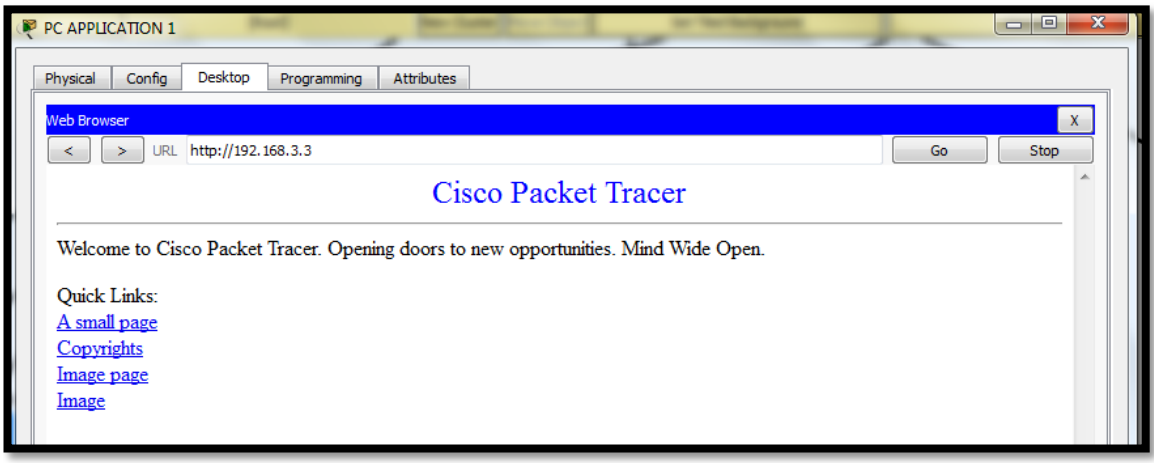


Figure IV.116: Test du service http.

IV.4.5 Vérification de l'accès à distance de l'administrateur

Le protocole d'accès à distance est autorisé qu'au poste de l'administrateur situant au niveau du site central qui a une adresse (192.168.10.10).

Le mode d'accès est assurer par le protocole SSH version 2.Celui-ci est protéger par un nom d'utilisateur et un mot de passe.

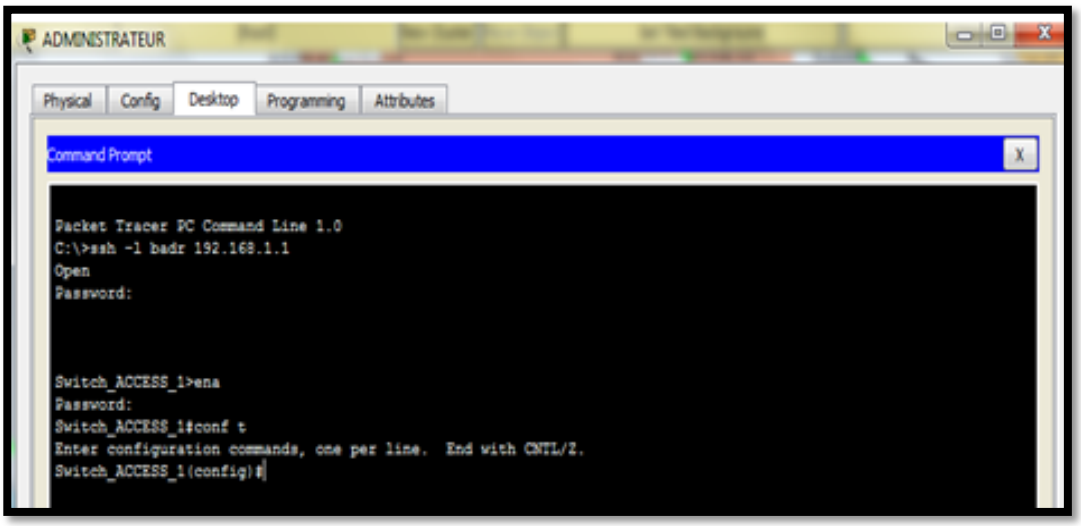


Figure IV.117: Accès à distance

D'autre coté les équipements sont interdit d'accédée a distance aux switches exemple des couche accès.

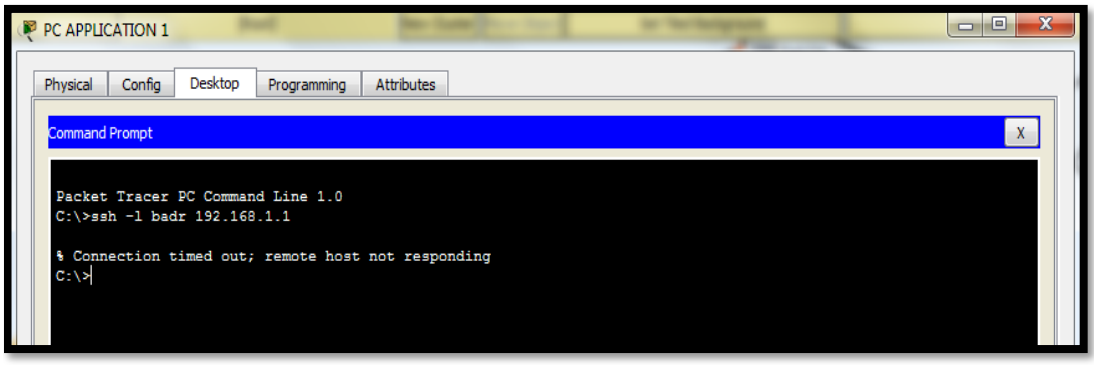


Figure IV.118 : Accès non autorisé

IV.4.6 Vérification du service email

a. Vérification des échanges des emails de l'agence vers le site centrale

Le pc administrateur vas envoyée un email au pc application de l'agence.

Figure IV.119 : Envoyer email

b. vérification de la réception d'émail.

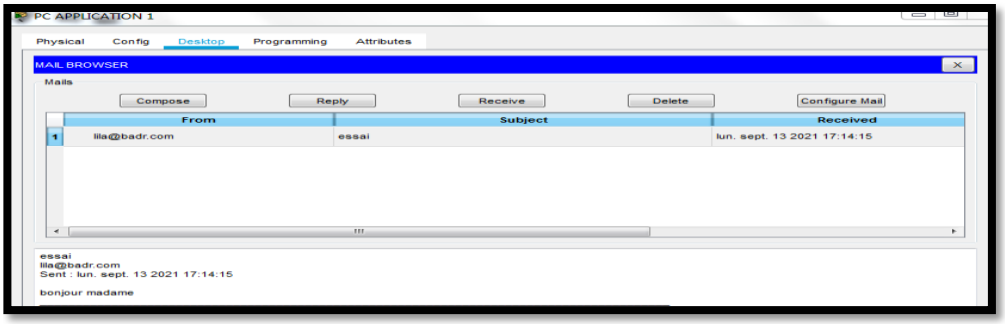


Figure IV.120 : Réception d'émail.

IV.4.7Vérification de syslog

Les logs sont les messages produits par les équipements réseau pour indiquer aux administrateurs les erreurs et les évènements survenant pendant leur fonctionnement.
Cette commande nous permet de voir les informations sauvegardées en niveau de serveur.

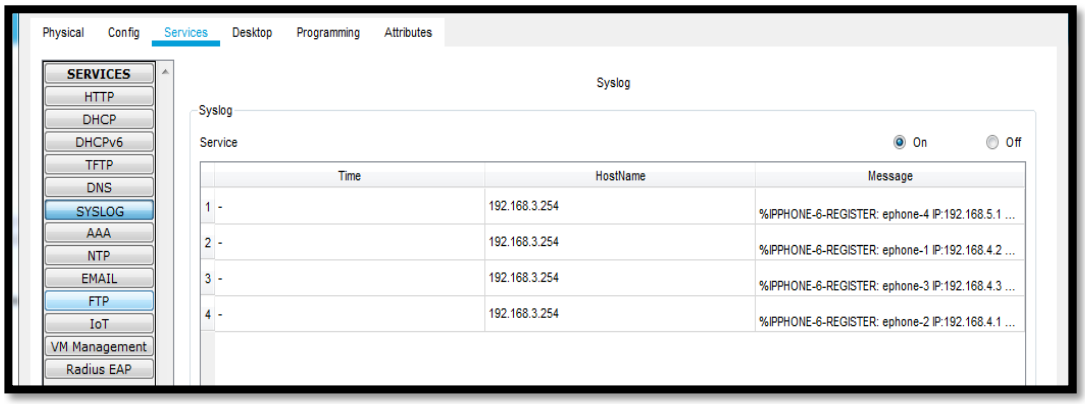


Figure IV.121 : vérification de syslog.

IV.4.8 Vérification du service de téléphonie IP

Nous allons faire un test d'appel téléphonique du site agence vers le site central.

Figure IV.122: Téléphone IP du site agence.

Le téléphone du site agence est doté du numéro 1001.Nous allons appeler le téléphone du site distant par son numéro 2001.

Figure IV.123: Téléphone IP du site central.

Nous retrouvons marqué « The phone is ringing » et « From 1001 » cela signifie que la ligne VoIp fonctionne correctement et les téléphones IP sont joignables.

IV.5 Conclusion

Ce chapitre qui est composée de trois parties dont la première est la présentation de simulateur Cisco Packet Tracer que nous avons utilisée pour la réalisation de notre travail.
La deuxième partie est dédiée à la simulation des différentes configurations que nous avons porte aux équipements utilisés pour la mise en marche de l'architecteur. Afin de nous assurer de la configuration et le bon fonctionnement des équipements, nous avons effectuée des tests de validation dans la troisième partie pour 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 sur pour avoir des réseaux fiables et sécurisée. Nous avons essayé, à travers le biais de ce projet, la mise en place d'une architecture réseau interconnectée et sécurisé à la BADR.
Ce projet nous a permis de mettre en pratique les connaissances acquises durant la période de notre stage pratique au sein de la Banque Algérienne de Développement Rurale d'ALGER chraga (BADR), de nous familiariser avec un environnement dynamique et d'avoir une idée plus profonde et plus pratique sur l'importance du réseau dans une entreprise.

Pour effectuer ce travail, en a focaliser sur une bonne analyse des besoins a été réalisé afin d'identifier tous les besoins de la société, suivie d'une conception minutieuse de notre réseau.

La conception a donné une image sur l'architecture globale de notre structure, le matériel choisi, les protocoles utilisés, une solution de redondance, enfin, une mise en place de la technologie téléphonie IP.

La partie réalisation nous a permis de simuler l'architecture conçue de notre inter-réseaux, et par la suite la configuration de nos équipements.

Ce travail nous a permis d'acquérir et d'enrichir nos connaissances et nos compétences dans de nombreux domaines, il nous a initié au monde de la recherche sur les réseaux surtout ce qui concerne leur sécurisation.

Annexe 1

configuration des Switchs Access :

```
hostname SW-ACCES2
!
enable secret 5 $1$mERr$gZrxqqWa0tvfFtcSiQ6IX/
!
!
!
ip ssh version 2
ip domain-name badr.local
!
username badr privilege 1 password 7 08234D4A1B
username test privilege 1 password 7 0835495D1D
!
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
interface FastEthernet0/1
switchport mode trunk
!
interface FastEthernet0/2
switchport access vlan 13
switchport mode access
spanning-tree portfast
!
interface FastEthernet0/3
switchport access vlan 13
switchport mode access
spanning-tree portfast
!
interface FastEthernet0/4
switchport access vlan 14
switchport mode access
spanning-tree portfast
!
interface FastEthernet0/5
switchport access vlan 14
switchport mode access
spanning-tree portfast
!
interface FastEthernet0/6
switchport mode trunk
!


interface FastEthernet0/7
```

```
switchport mode access
switchport voice vlan 200
!
interface FastEthernet0/8
!
interface FastEthernet0/9
!
interface FastEthernet0/10
!
interface FastEthernet0/11
!
interface FastEthernet0/12
!
interface FastEthernet0/13
!
interface FastEthernet0/14
!
interface FastEthernet0/15
!
interface FastEthernet0/16
!
interface FastEthernet0/17
!
interface FastEthernet0/18
!
interface FastEthernet0/19
!
interface FastEthernet0/20
!
interface FastEthernet0/21
!
interface FastEthernet0/22
!
interface FastEthernet0/23
!
interface FastEthernet0/24
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
interface Vlan1
no ip address
shutdown
!
interface Vlan100
ip address 192.168.1.2 255.255.255.248
!
ip default-gateway 192.168.1.6
!
```

```
!
!
!
line con 0
!
line vty 0 4
login local
transport input ssh
line vty 5 15
login local
transport input ssh
!
!
!
!
End
```

Annexe 2

configuration du commutateur actif :

```
hostname SW-DIST-ACTIVE
!
!
enable secret 5 $1$mERr$gZrxqqWa0tvfFtcSiQ6IX/
!
!
ip dhcp excluded-address 10.10.10.30
ip dhcp excluded-address 10.10.10.62
ip dhcp excluded-address 10.10.10.78
ip dhcp excluded-address 10.10.10.94
ip dhcp excluded-address 10.10.10.1
ip dhcp excluded-address 10.10.10.33
ip dhcp excluded-address 10.10.10.65
ip dhcp excluded-address 10.10.10.81
ip dhcp excluded-address 10.10.10.2
ip dhcp excluded-address 10.10.10.34
ip dhcp excluded-address 10.10.10.66
ip dhcp excluded-address 10.10.10.82
!
ip dhcp pool lan-app
network 10.10.10.0 255.255.255.224
default-router 10.10.10.30
ip dhcp pool lan-crt
network 10.10.10.32 255.255.255.224
default-router 10.10.10.62
ip dhcp pool lan-trt
network 10.10.10.64 255.255.255.240
default-router 10.10.10.78
ip dhcp pool lan-drt
network 10.10.10.80 255.255.255.240
default-router 10.10.10.94
ip dhcp pool lan-ant-virus
ip dhcp pool Phones
network 192.168.4.0 255.255.255.0
default-router 192.168.4.254
option 150 ip 10.0.1.1
!
!
ip routing

!
!
!
!
username badr password 7 08234D4A1B
username test password 7 0835495D1D
```

```
!
!
!
!
!
!
!
!
!
!
ip ssh version 2
ip domain-name badr.local
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
!
!
!
!
!

interface FastEthernet0/1
switchport trunk encapsulation dot1q
switchport mode trunk
switchport nonegotiate
!
interface FastEthernet0/2
switchport access vlan 101
switchport trunk encapsulation dot1q
switchport mode trunk
!
interface FastEthernet0/3
switchport trunk encapsulation dot1q
switchport mode trunk
!
interface FastEthernet0/4
!
interface FastEthernet0/5
!
interface FastEthernet0/6
!
interface FastEthernet0/7
!
interface FastEthernet0/8
!
interface FastEthernet0/9
!
interface FastEthernet0/10
```

```
!
interface FastEthernet0/11
!
interface FastEthernet0/12
!
interface FastEthernet0/13
!
interface FastEthernet0/14
!
interface FastEthernet0/15
!
interface FastEthernet0/16
!
interface FastEthernet0/17
!
interface FastEthernet0/18
!
interface FastEthernet0/19
!
interface FastEthernet0/20
!
interface FastEthernet0/21
!
interface FastEthernet0/22
!
interface FastEthernet0/23
!
interface FastEthernet0/24
!
interface GigabitEthernet0/1
switchport trunk encapsulation dot1q
switchport mode trunk
!
interface GigabitEthernet0/2
switchport trunk encapsulation dot1q
switchport mode trunk
!
interface Vlan1
no ip address
shutdown
!
interface Vlan10
mac-address 0009.7c2b.5701
ip address 10.10.10.99 255.255.255.248
ip access-group 101 in
standby 10 ip 10.10.10.98
standby 10 priority 150
standby 10 preempt
!
```

```
interface Vlan11
mac-address 0009.7c2b.5702
ip address 10.10.10.1 255.255.255.224
ip access-group 101 in
standby 11 ip 10.10.10.30
standby 11 priority 150
standby 11 preempt
!
interface Vlan12
mac-address 0009.7c2b.5703
ip address 10.10.10.33 255.255.255.224
ip access-group 101 in
standby 12 ip 10.10.10.62
standby 12 priority 150
standby 12 preempt
!
interface Vlan13
mac-address 0009.7c2b.5704
ip address 10.10.10.65 255.255.255.240
ip access-group 101 in
standby 13 ip 10.10.10.78
standby 13 priority 150
standby 13 preempt
!
interface Vlan14
mac-address 0009.7c2b.5705
ip address 10.10.10.81 255.255.255.240
ip access-group 101 in
standby 14 ip 10.10.10.94
standby 14 priority 150
standby 14 preempt
!
interface Vlan100
mac-address 0009.7c2b.5706
ip address 192.168.1.5 255.255.255.248
ip access-group 101 in
standby 100 ip 192.168.1.6
standby 100 priority 150
standby 100 preempt
!
interface Vlan101
mac-address 0009.7c2b.5707
ip address 172.16.4.3 255.255.255.248
ip access-group 101 in
standby 2 ip 172.16.4.4
standby 2 priority 150
standby 2 preempt
!
interface Vlan200
mac-address 0009.7c2b.5708
```

```
ip address 192.168.4.254 255.255.255.0
!
ip classless
ip route 192.168.10.0 255.255.255.0 172.16.4.1
ip route 192.168.2.0 255.255.255.0 172.16.4.1
ip route 192.168.3.0 255.255.255.0 172.16.4.1
ip route 10.0.1.0 255.255.255.0 172.16.4.1
ip route 192.168.5.0 255.255.255.0 172.16.4.1
ip route 172.18.1.0 255.255.255.252 172.16.4.1
!
ip flow-export version 9
!
!
access-list 101 deny tcp 10.10.10.0 0.0.0.255 host 10.10.10.30 eq 22
access-list 101 deny tcp 10.10.10.0 0.0.0.255 host 10.10.10.62 eq 22
access-list 101 deny tcp 10.10.10.0 0.0.0.255 host 10.10.10.78 eq 22
access-list 101 deny tcp 10.10.10.0 0.0.0.255 host 10.10.10.94 eq 22
access-list 101 deny tcp 10.10.10.0 0.0.0.255 192.168.1.0 0.0.0.255 eq 22
access-list 101 permit tcp host 192.168.10.10 192.168.1.0 0.0.0.255 eq 22
access-list 101 permit ip any any
access-list 101 permit icmp any any
!
banner motd ^C SW-DIST ^C
!
!
!
!
!
line con 0
!
line aux 0
!
line vty 0 4
login local
transport input ssh
line vty 5 15
login local
transport input ssh
!
!
!
!
End
```

Annexe 3

configuration du commutateur passif :

```
hostname SW-DIST-STANDBY
!
!
enable secret 5 $1$mERr$gZrxqqWa0tvfFtcSiQ6IX/
!
!
ip dhcp excluded-address 10.10.10.30
ip dhcp excluded-address 10.10.10.62
ip dhcp excluded-address 10.10.10.1
ip dhcp excluded-address 10.10.10.33
ip dhcp excluded-address 10.10.10.65
ip dhcp excluded-address 10.10.10.81
ip dhcp excluded-address 10.10.10.2
ip dhcp excluded-address 10.10.10.34
ip dhcp excluded-address 10.10.10.66
ip dhcp excluded-address 10.10.10.82
ip dhcp excluded-address 10.10.10.78
ip dhcp excluded-address 10.10.10.94
!
ip dhcp pool lan-app
network 10.10.10.0 255.255.255.224
default-router 10.10.10.30
ip dhcp pool lan-crt
network 10.10.10.32 255.255.255.224
default-router 10.10.10.62
ip dhcp pool lan-trt
network 10.10.10.64 255.255.255.240
default-router 10.10.10.78
ip dhcp pool lan-drt
network 10.10.10.80 255.255.255.240
default-router 10.10.10.94
ip dhcp pool lan-ant-virus
ip dhcp pool Phones
network 192.168.4.0 255.255.255.0
default-router 192.168.4.254
option 150 ip 10.0.1.1
!
!
ip routing
!
!
!
!
username badr password 7 08234D4A1B
username test password 7 0835495D1D
!
```

```
!
!
!
!
!
!
!
!
!
ip ssh version 2
ip domain-name badr.local
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
!
!
!
!
interface FastEthernet0/1
switchport trunk encapsulation dot1q
switchport mode trunk
switchport nonegotiate
!
interface FastEthernet0/2
switchport access vlan 101
switchport trunk encapsulation dot1q
switchport mode trunk
!
interface FastEthernet0/3
!
interface FastEthernet0/4
!
interface FastEthernet0/5
!
interface FastEthernet0/6
!
interface FastEthernet0/7
!
interface FastEthernet0/8
!
interface FastEthernet0/9
!
interface FastEthernet0/10
!
interface FastEthernet0/11
!
interface FastEthernet0/12
!
```

```
interface FastEthernet0/13
!
interface FastEthernet0/14
!
interface FastEthernet0/15
!
interface FastEthernet0/16
!
interface FastEthernet0/17
!
interface FastEthernet0/18
!
interface FastEthernet0/19
!
interface FastEthernet0/20
!
interface FastEthernet0/21
!
interface FastEthernet0/22
!
interface FastEthernet0/23
switchport trunk encapsulation dot1q
switchport mode trunk
!
interface FastEthernet0/24
switchport trunk encapsulation dot1q
switchport mode trunk
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
interface Vlan1
no ip address
shutdown
!
interface Vlan10
mac-address 0030.f22d.5d01
ip address 10.10.10.100 255.255.255.248
ip access-group 101 in
standby 10 ip 10.10.10.98
standby 10 priority 80
standby 10 preempt
!
interface Vlan11
mac-address 0030.f22d.5d02
ip address 10.10.10.2 255.255.255.224
ip access-group 101 in
standby 11 ip 10.10.10.30
standby 11 priority 80
```

```
standby 11 preempt
!
interface Vlan12
mac-address 0030.f22d.5d03
ip address 10.10.10.34 255.255.255.224
ip access-group 101 in
standby 12 ip 10.10.10.62
standby 12 priority 80
standby 12 preempt
!
interface Vlan13
mac-address 0030.f22d.5d05
ip address 10.10.10.66 255.255.255.240
ip access-group 101 in
standby 13 ip 10.10.10.78
standby 13 priority 80
standby 13 preempt
!
interface Vlan14
mac-address 0030.f22d.5d06
ip address 10.10.10.82 255.255.255.240
ip access-group 101 in
standby 14 ip 10.10.10.94
standby 14 priority 80
standby 14 preempt
!
interface Vlan100
mac-address 0030.f22d.5d07
ip address 192.168.1.4 255.255.255.248
ip access-group 101 in
standby 100 ip 192.168.1.6
standby 100 priority 80
standby 100 preempt
!
interface Vlan101
mac-address 0030.f22d.5d08
ip address 172.16.4.2 255.255.255.248
ip access-group 101 in
standby 2 ip 172.16.4.4
standby 2 priority 80
standby 2 preempt
!
ip classless
ip route 192.168.10.0 255.255.255.0 172.16.4.1
ip route 192.168.2.0 255.255.255.0 172.16.4.1
ip route 192.168.3.0 255.255.255.0 172.16.4.1
ip route 172.18.1.0 255.255.255.252 172.16.4.1
ip route 10.0.1.0 255.255.255.0 172.16.4.1
ip route 192.168.5.0 255.255.255.0 172.16.4.1
!
```

```
ip flow-export version 9
!
!
access-list 101 deny tcp 10.10.10.0 0.0.0.255 host 10.10.10.30 eq 22
access-list 101 deny tcp 10.10.10.0 0.0.0.255 host 10.10.10.62 eq 22
access-list 101 deny tcp 10.10.10.0 0.0.0.255 host 10.10.10.78 eq 22
access-list 101 deny tcp 10.10.10.0 0.0.0.255 host 10.10.10.94 eq 22
access-list 101 deny tcp 10.10.10.0 0.0.0.255 192.168.1.0 0.0.0.255 eq 22
access-list 101 permit tcp host 192.168.10.10 192.168.1.0 0.0.0.255 eq 22
access-list 101 permit ip any any
access-list 101 permit icmp any any
!
banner motd ^C SW-DIST ^C
!
!
!
!
!
line con 0
!
line aux 0
!
line vty 0 4
login local
transport input ssh
line vty 5 15
login local
transport input ssh
!
!
!
!
end
```

Annexe 4

configuration du firewall :

```
hostname firewall
enable password FRc90BKSCmK9ENfj encrypted
names
!
interface Ethernet0/0
!
interface Ethernet0/1
switchport access vlan 2
!
interface Ethernet0/2
!
interface Ethernet0/3
!
interface Ethernet0/4
!
interface Ethernet0/5
!
interface Ethernet0/6
!
interface Ethernet0/7
!
interface Vlan1
nameif inside
security-level 100
ip address 172.16.4.1 255.255.255.252
!
interface Vlan2
nameif outside
security-level 0
ip address 172.18.1.1 255.255.255.252
!
!
route outside 192.168.2.0 255.255.255.0 172.18.1.2 1
route outside 192.168.3.0 255.255.255.0 172.18.1.2 1
route outside 192.168.10.0 255.255.255.0 172.18.1.2 1
route outside 10.0.1.0 255.255.255.0 172.18.1.2 1
route outside 192.168.5.0 255.255.255.0 172.18.1.2 1
route inside 10.10.10.0 255.255.255.0 172.16.4.4 1
route inside 192.168.1.0 255.255.255.0 172.16.4.4 1
route inside 192.168.4.0 255.255.255.0 172.16.4.4 1
!
access-list BADR_OUT extended permit tcp host 192.168.2.2 host 10.10.10.97
access-list BADR_OUT extended permit tcp host 192.168.3.3 10.10.10.0 255.255.255.224
access-list BADR_OUT extended permit icmp any any
access-list BADR_OUT extended permit tcp host 192.168.10.10 192.168.1.0
255.255.255.248 eq 22
```

```
access-list BADR_OUT extended permit ip 10.0.1.0 255.255.255.0 192.168.4.0
255.255.255.0
access-list BADR_IN extended permit tcp host 10.10.10.97 host 192.168.2.2
access-list BADR_IN extended permit tcp 10.10.10.0 255.255.255.224 host 192.168.3.3
access-list BADR_IN extended permit tcp 192.168.1.0 255.255.255.248 host 192.168.10.10
access-list BADR_IN extended permit icmp any any
access-list BADR_IN extended permit ip 192.168.4.0 255.255.255.0 10.0.1.0 255.255.255.0
!
!
access-group BADR_IN in interface inside
access-group BADR_OUT in interface outside
!
aaa authentication ssh console LOCAL
!
username badr password 9mjBfFLU2DUdi7mC encrypted
!
!
!
!
telnet timeout 5
ssh 192.168.10.10 255.255.255.255 outside
ssh timeout 5
!
dhcpd auto_config outside
```

Annexe 5

configuration du routeur Central LS :

```
hostname R_Central
!
!
!
enable secret 5 $1$mERr$gZrxqqWa0tvfFtcSiQ6IX/
!
!
!
ip dhcp pool Phones
network 192.168.5.0 255.255.255.0
default-router 192.168.5.254
option 150 ip 10.0.1.1
!
!
!
no ip cef
no ipv6 cef
!
!
!
username badr password 7 0835495D1D
!
!
!
!
!
!
!
!
!
ip ssh version 2
ip domain-name badr.local
!
!
spanning-tree mode pvst
!
!
!
!
!
!
!
interface FastEthernet0/0
no ip address
duplex auto
speed auto
!
interface FastEthernet0/0.1
```

```
encapsulation dot1Q 20
ip address 192.168.2.254 255.255.255.0
ip access-group 102 in
!
interface FastEthernet0/0.2
encapsulation dot1Q 30
ip address 192.168.3.254 255.255.255.0
ip access-group 102 in
!
interface FastEthernet0/0.3
encapsulation dot1Q 40
ip address 192.168.10.254 255.255.255.0
!
interface FastEthernet0/0.4
encapsulation dot1Q 50
ip address 192.168.5.254 255.255.255.0
ip access-group 102 in
!
interface FastEthernet0/1
ip address 10.0.4.2 255.255.255.0
duplex auto
speed auto
!
interface Serial0/3/0
ip address 10.0.1.1 255.255.255.0
encapsulation ppp
clock rate 2000000
!
interface Vlan1
no ip address
shutdown
!
router ospf 1
log-adjacency-changes
network 10.0.1.1 0.0.0.0 area 0
network 10.0.4.2 0.0.0.0 area 0
network 192.168.2.254 0.0.0.0 area 0
network 192.168.3.254 0.0.0.0 area 0
network 192.168.10.254 0.0.0.0 area 0
network 192.168.5.254 0.0.0.0 area 0
!
ip classless
ip route 10.10.10.0 255.255.255.0 10.0.1.2
ip route 192.168.1.0 255.255.255.248 10.0.1.2
ip route 172.18.1.0 255.255.255.252 10.0.4.1 120
ip route 10.10.10.0 255.255.255.0 10.0.4.1 120
ip route 192.168.1.0 255.255.255.248 10.0.4.1 120
ip route 192.168.4.0 255.255.255.0 10.0.1.2
ip route 172.16.4.0 255.255.255.248 10.0.1.2
!
```

```
ip flow-export version 9
!
!
access-list 102 permit tcp host 192.168.10.10 host 10.0.1.1 eq 22
access-list 102 permit tcp host 192.168.10.10 host 10.0.1.2 eq 22
access-list 102 permit icmp any any
access-list 102 permit ip host 192.168.2.2 host 10.10.10.97
access-list 102 permit ip host 192.168.3.3 10.10.10.0 0.0.0.31
access-list 102 permit ip any any
!
!
!
!
!
!
logging trap debugging
logging 192.168.3.3
dial-peer voice 1 voip
destination-pattern 1...
session target ipv4:192.168.4.2
!
dial-peer voice 2 voip
destination-pattern 1...
session target ipv4:192.168.4.1
!
dial-peer voice 3 voip
destination-pattern 1...
session target ipv4:192.168.4.3
!
dial-peer voice 4 voip
destination-pattern 2...
session target ipv4:192.168.5.1
!
telephony-service
max-ephones 10
max-dn 10
ip source-address 10.0.1.1 port 2000
auto assign 1 to 10
!
ephone-dn 1
number 1001
!
ephone-dn 2
number 1002
!
ephone-dn 3
number 1003
!
ephone-dn 4
number 2001
```

```
!
ephone 1
device-security-mode none
mac-address 0001.6325.1411
type 7960
button 1:1
!
ephone 2
device-security-mode none
mac-address 00D0.58B1.C80B
type 7960
button 1:2
!
ephone 3
device-security-mode none
mac-address 0007.EC68.B827
type 7960
button 1:3
!
ephone 4
device-security-mode none
mac-address 00D0.FFE9.8AC4
type 7960
button 1:4
!
line con 0
!
line aux 0
!
line vty 0 4
login local
transport input ssh
line vty 5 15
login local
transport input ssh
!
!
ntp server 192.168.3.3
!
End
```

Annexe 6

configuration du routeur Central WiMax :

```
hostname Routeur_Central_WiMax
!
!
!
enable secret 5 $1$mERr$gZrxqqWa0tvfFtcSiQ6IX/
!
!
!
!
!
!
no ip cef
no ipv6 cef
!
!
!
!
!
!
!
!
!
!
!
!
!
spanning-tree mode pvst
!
!
!
!
!
!
interface FastEthernet0/0
ip address 10.0.4.1 255.255.255.0
duplex auto
speed auto
!
interface FastEthernet0/1
no ip address
duplex auto
speed auto
!
interface Serial0/0/0
ip address 10.0.3.2 255.255.255.0
clock rate 2000000
!
```

```
interface Serial0/0/1
no ip address
clock rate 2000000
shutdown
!
interface Vlan1
no ip address
shutdown
!
ip classless
ip route 192.168.2.0 255.255.255.0 10.0.4.2
ip route 192.168.3.0 255.255.255.0 10.0.4.2
ip route 192.168.10.0 255.255.255.0 10.0.4.2
ip route 172.18.1.0 255.255.255.252 10.0.3.1
ip route 192.168.1.0 255.255.255.248 10.0.3.1
ip route 10.10.10.0 255.255.255.0 10.0.3.1
ip route 10.0.2.0 255.255.255.0 10.0.3.1
!
ip flow-export version 9
!
!
!
!
!
!
!
!
!
logging trap debugging
logging 192.168.3.3
line con 0
!
line aux 0
!
line vty 0 4
login
!
!
ntp server 10.0.4.2
!
end
```

Bibliographique

❖ Réseau72

[1]https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwi085CM5_nwAhWDg_0HHTB3B5AQFjABegQIAxAD&url=http%3A%2F%2Findus.graph.free.fr%2FCours%2520PDF%2FReseaux72.pdf&usg=AOvVaw2eAttA-5Rte3shvKd5Ircx

❖ Livre gratuit notion fondamentale de modèle OSI

[2]https://books.google.dz/books?hl=fr&lr=&id=nyyW3ANPHrYC&oi=fnd&pg=PA73&dq=livres+gratuit++notion+fondamentale+de+mod%C3%A9le+OSI&ots=1f0So2tv0_&sig=8qNNhJt3mqUbh50geM-fOKyOWL0&redir_esc=y#v=onepage&q=livres%20gratuit%20%20notion%20fondamentale%20de%20mod%C3%A9le%20OSI&f=false

❖ Etude et mise en place d'un réseau VPN

[3]https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwjIwdu6l-rwAhXR66QKHf_QDrwQFjANegQIHhAD&url=https%3A%2F%2Fdl.ummto.dz%2Fbitstream%2Fhandle%2Fummto%2F6669%2FRahmaniTinhinan_SadaouiFadhila.pdf%3Fsequence%3D1&usg=AOvVaw3VHg_ZuObfePwuPum3dqHC

❖ Apprenez le fonctionnement des réseaux TCP/IP

[4] http://coursinformtiqueslibres.e-monsite.com/pages/livres/reseaux.html#page1

https://www.commentcamarche.net/contents/539-tcp-ip

❖ Modèle TCP/IP &OSI

[5] https://cisco.goffinet.org/ccna/fondamentaux/modeles-tcp-ip-osi/

[6] https://www.frameip.com/tcpip/

❖ Les supports de transmissions

[7]https://fr.wikibooks.org/wiki/Les_r%C3%A9seaux_informatiques/Les_supports_de_transmission

❖ Les lignes louées

[8] http://themorrealeworld.free.fr/Francais/Cours/Informatique/TCPIP/CCNA/Chap2-WAN/LignesLouees.html?fbclid=IwAR35rh8rmE12UGXRXAfTUAjXuEWcWsuiJjBLCl4wJzUDfg6qDtgDmlm4Trw

❖ Présentation de WIMAX

[9] https://fr.scribd.com/presentation/256436979/Presentation-Wimax?fbclid=IwAR35rh8rmE12UGXRXAfTUAjXuEWcWsuiJjBLCl4wJzUDfg6qDtgDmlm4Trw

❖ Cas d'étude sonatrach

[10]https://www.academia.edu/34596665/La_haute_disponibilit%C3%A9_des_r%C3%A9seaux_campus_Cas_d_%C3%A9tude_Sonatrach

❖ L'utilisation de modem

[11] https://www.fastconnect.fr/quelle-est-lutilisation-d-un-modem/

❖ La technologie DSL

[12] https://m.radioactif.com/blog/comprendre-les-differents-types-de-technologie-dsl-805039.html

http://www.iro.umontreal.ca/~kropf/ift-6052/notes/ppp/index.html#:~:text=Le%20protocole%20PPP%20offre%20des,une%20structure%20similaire%20%C3%A0%20HDLC.

❖ IPV4 internet protocole version 4

[13] https://www.journaldunet.fr/web-tech/dictionnaire-du-webmastering/1203391-ipv4-internet-protocol-version-4-definition-traduction/

❖ Protocole ARP

[14] https://openspacecourse.com/le-protocole-arp/

❖ Protocole OSPF (Open Shortest Path First)

[15] https://www.watchguard.com/help/docs/fireware/12/fr-FR/Content/fr-FR/dynamicrouting/ospf_about_c.html

❖ Protocole ICMP (Internet Control Message Protocol)

[16] https://web.maths.unsw.edu.au/~lafaye/CCM/internet/icmp.htm

❖ Le protocole TCP (Transmission Control Protocol)

[17] https://web.maths.unsw.edu.au/~lafaye/CCM/internet/tcp.htm

https://www.ionos.fr/digitalguide/serveur/know-how/udp-user-datagram-protocol/

❖ Le Protocole SSH (Secure Shell)

[18] https://web.maths.unsw.edu.au/~lafaye/CCM/crypto/ssh.htm

❖ Réseau virtuels vlan

[19] https://www.coursehero.com/file/53744590/LES-RESEAUX-VIRTUELS-VLANpdf/

[20] https://www.memoireonline.com/04/10/3431/m_Etude-et-optimisation-du-reseau-local-de-inova-si6.html

❖ Les Firewalls

[21] https://cisco.goffinet.org/ccna/filtrage/concepts-pare-feu-firewall/

❖ Les ACL

[22] https://www.academia.edu/5501105/Cisco_les_acl_cours

❖ Les différents types d'ACL

[23]https://www.google.com/url?sa=t&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwiUq7ihlPzwAhVE2qQKHVmyCwAQFjAAegQIAxAD&url=http%3A%2F%2Fwww.univ-bejaia.dz%2Fdspace%2Fhandle%2F123456789%2F1266&usg=AOvVaw2ERzGtZzwELtvVPqPy6Krb

❖ Le modèle hiérarchique en trois couches de Cisco

[24] https://bibabox.fr/topologie-reseau-le-modele-hierarchique-en-3-couches/

❖ **L'importance de « tree-layers hierarchical internet working design/model »**

[25] https://cisco.goffinet.org/ccna/ethernet/principes-conception-lan-cisco/#11-but-dun-mod%C3%A8le-de-conception

❖ **Description des trois couches du modèle type**

[26] http://bits-genius.com/topologie-reseau/

❖ **Optimisation du fonctionnement du réseau informatique Candia**

[27]https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwi-zsHh5cDzAhWE2eAKHeynA20QFnoECAIQAQ&url=http%3A%2F%2Fwww.univ-bejaia.dz%2Fjspui%2Fhandle%2F123456789%2F14501&usg=AOvVaw1sEHbzxOyEY-zAaSU6YcsU

❖ **routeurs**

[28] www.audentia-gestion.fr/cisco/Routeurs_Cisco_2800.pdf

❖ **Description des Switches**

[29] https://community.fs.com/fr/blog/enterprise-switches-everything-you-should-know.html

❖ **Fonctionnement de firewal**

[30] https://www.malekal.com/firewall-definition-et-fonctionnement/

❖ **Présentation VLSM**

[31] https://itmetiers.com/vlsm/

❖ **Haute conception de réseau de disponible**

[32] https://cisco.goffinet.org/ccna/redondance-de-liens/spanning-tree-rapid-stp-pvst-cisco/

❖ Les redondances des liens

[33] https://www.elogedelafuite.fr/dokuwiki/doku.php?id=reseau%3Astp

❖ Fonctionnement de firewal

[34] https://portail-informatique-et-securite-du-web.over-blog.com/2020/02/c-est-quoi-et-comment-fonctionne-un-pare-feu-firewall.html

❖ Réseau Multi Service

[35] https://www.algerietelecom.dz/fr/entreprises/rms-reseau-multiservices-prod24

❖ WIMAX

[36] http://a2cnet.fr/wimax/

❖ Standard téléphonique VOIP

[37] https://choisirpro.com/standard-telephonique/voip

https://www.onedirect.fr/produits/cisco/cisco-ip-7960

❖ Cours Packet tracer

[39] https://www.cours-gratuit.com/cours-packet-tracer/presentation-et-utilisation-de-packet-tracer-en-pdf#google_vignette.

Les figures

[5]https://www.google.com/url?sa=i&url=https%3A%2F%2Fwww.memoireonline.com%2F01%2F12%2F5161%2Fm_tude-et-mise-en-place-d-un-reseau-wimax-dans-la-region-de-Dakar3.html&psig=AOvVaw03eO7AGaCmMG6tVK7_tz51&ust=1634026564603000&source=images&cd=vfe&ved=2ahUKEwiN3uG49cHzAhVFZRoKHbQJBC0Qr4kDegUIARC1AQ

Figure II.22: WIMAX.

[6]https://www.google.com/url?sa=i&url=https%3A%2F%2Ffr.wikiversity.org%2Fwiki%2FMat%25C3%25A9riel_(r%25C3%25A9seau)%2FRouteur&psig=AOvVaw1-jwZjsXlrh9-Stbjsvh5x&ust=1634026710249000&source=images&cd=vfe&ved=0CBsQr4kDahcKEwio6YeK9sHzAhUAAAAAHQAAAAAQAg

Figure II.23 : SWITCH.

Figure II.24 : Router.

Figure II.25 : Modem

[7]https://www.google.com/url?sa=i&url=https%3A%2F%2Fwww.slideshare.net%2FHayderGallas%2Fprotocole-arprarp&psig=AOvVaw2QJTwNF-LG2i9yPq3DEwlQ&ust=1634027158173000&source=images&cd=vfe&ved=2ahUKEwjEr-bT98HzAhURwoUKHVk5BloQr4kDegUIARDIAQ

Figure II.26:représentation de protocole ARP.

[8]https://www.google.com/url?sa=i&url=https%3A%2F%2Fnetworkcorp.fr%2Fprotocole-de-routage-ospf%2F&psig=AOvVaw08r9rMlj5mEMzgDxD_Kddx&ust=1634027200888000&source=images&cd=vfe&ved=2ahUKEwjQvpXo98HzAhUBLxoKHajaCi4Qr4kDegUIARCzAQ

Figure II.27: représentation de protocole OSP

[9]https://www.google.com/url?sa=i&url=https%3A%2F%2Fwww.javatpoint.com%2Ftcp&psig=AOvVaw1O6866mNlKKhpf1bfW6JXO&ust=1634027465035000&source=images&cd=vfe&ved=0CEgQr4kDahcKEwjY_KiA-cHzAhUAAAAAHQAAAAAQAw

Figure II.29 : représentation de protocole TCP

[10]https://www.google.com/url?sa=i&url=https%3A%2F%2Fwww.malekal.com%2Fprotocole-tcp-udp-icmp-fonctionnement-et-differences%2F&psig=AOvVaw1O6866mNlKKhpf1bfW6JXO&ust=1634027465035000&source=images&cd=vfe&ved=2ahUKEwik4I_m-MHzAhUMaRoKHcEwBVgQr4kDegUIARDzAQ

Figure II.30: représentation de protocole UDP

[10]https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwjIwdu6l-rwAhXR66QKHf_QDrwQFjANegQIHhAD&url=https%3A%2F%2Fdl.ummto.dz%2Fbitstream%2Fhandle%2Fummto%2F6669%2FRahmaniTinhinan_SadaouiFadhila.pdf%3Fsequence%3D1&usg=AOvVaw3VHg_ZuObfePwuPum3dqHC

Figure II.32 : représentation de VLAN

Figure II.33 : exemple de VLAN niveau 1

Figure II.34 : représentation de VLAN niveau 2

[11] https://www.academia.edu/5501105/Cisco_les_acl_cours

Figure II.37 : Trafic d'ACL

[11] https://www.google.com/url?sa=i&url=https%3A%2F%2Felearning-deprecated.univ-annaba.dz%2Fpluginfile.php%2F50080%2Fmod_resource%2Fcontent%2F1%2FCours3_Important.pdf&psig=AOvVaw2S08asnLulj_USrpWqgEx9&ust=1634028156239000&source=images&cd=vfe&ved=2ahUKEwi9uduv-8HzAhVBlxoKHf8aDSIQr4kDegUIARCsAQ

Figure III.38 : Le modèle hiérarchique.

Figure III.39 : Description la couche cœur

Figure III.40 : Description La couche distribution

Figure III.41 : Description La couche accès

[12] https://cisco.goffinet.org/ccna/redondance-de-liens/spanning-tree-rapid-stp-pvst-cisco/

Figure III.47: Tempête de diffusion.

Figure III.48: Duplication des trames.