République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

Université A/Mira de Béjaïa
Faculté des Sciences Exactes
Département d'Informatique

Mémoire de fin de cycle, Master professionnelle
en Informatique
Option : Sécurité et Administration des Réseaux

Thème

Sécurité des mises à jour des protocoles de routage dans les réseaux de moyenne dimension : Etude, configuration, mise en place des protocoles RIP, OSPF et EIGRP (cas CIVITAL)

Présenté par

M^{elle} ***Boudjlida*** **Nawel**
M^{elle} ***Djerroud*** **Zahia**

Soutenu devant le jury composé de :

Président	M^{r} ***ALOUI*** **Abdelouhab**
promotrice	M^{me} ***ALOUI*** **Soraya**
co-promoteur	M^{r} ***BAADACHE*** **Abderrahmane**
Examinateur	M^{r} ***HAMOUMA*** **Moumen**
Examinateur	M^{r} ***AMROUN*** **Kamal**

Promotion 2012/2013

Remerciements

Nous tenons d'abord à remercier le bon dieu qui nous a donné le savoir, le courage et la force d'accomplir ce modeste travail.

On voulait aussi exprimer nos plus vifs remerciements a : Notre promotrice Mme. S. ALOUI pour les nombreux conseils, orientations, aide, ses suggestions pertinentes et enfin, pour avoir apporté tant de soins à la réalisation de ce mémoire.

Nous adressons nos sincères remerciements à M. A. BAADACHE, notre deuxième promoteur, pour sa disponibilité, ses explications et suggestions pertinentes et encouragements tout au long de ce travail.

Merci à tous qui ont contribue de prés ou de loin, à la réalisation de ce travail.

Nous remercions aussi les membres du jury qui ont accepté d'évaluer ce mémoire.

Nous remercions aussi tous les enseignants du département informatique pour leurs suivis tout au long de notre cursus.

Dédicaces

Je dédie ce modeste travail à :

A*ma très chère mère Ourida et à mon père Idir pour m'avoir donne goût aux études et m'avoir apporté un grand support moral tout au long de mes études,*

A*mes frères et sœurs : Kaci, Rezek, Karima, Tarik, Sonia, Lounes, Cilia et Faouzi, qui m'ont soutenu durant toute la période d'élaboration de ce mémoire sans oublier de leur souhaiter un brillant succès dans leurs vie,*

A*mes belles sœurs : Zouhra, Hida et Lila,*

A*mes neveux et nièces : Tassadite, Youba, Mayasse, Mouhamed Amine et Rayane,*

A*mon très chère fiancè Larbi et toute sa famille ABID,*

A*ma binôme Nawel et sa famille,*

A*mes amis, mes copines ainsi que toute la famille DJERROUD.*

DJERROUD Zahia

Dédicaces

Je dédie ce modeste travail à :

Je tiens très
respectueusement à dédier ce modeste travail à mes chers parents pour leur soutien,
patience et amour qui m'ont donné la force pour continuer mes études,
Ama grande mère qui n'a jamais cessé de me soutenir et m'encourage,
Ames chers frères Khalil et Ayoub,
A mes chères sœurs loubna et zineb qui m'ont soutenu durant toute la période
d'´elaboration de ce mémoire
sans oublier de leur souhaiter un brillant succès dans leurs vie,
Amon très chère fiancé hamza et sa famille,
Ama binôme Zahia et sa famille,
Atoute mes amie et mes copines et a toute ma famille,
Atous mes enseignants de l'école primaire jusqu'à l'université,
Pour terminer, Merci pour tous ceux qui, par leurs remarques et leurs conseils, ont
contribué à la réalisation de ce travail.

BOUDJLIDA Nawel

Résumé

Le routage est une fonction clé de la couche réseau permettant à des paquets d'être acheminé d'un réseau à un autre. A cet effet, différents protocoles ont été élaborés et différentes classifications de ces protocoles ont été proposées, entre autres, nous trouvons la classe des protocoles à vecteurs de distance comme RIP et IGRP, des protocoles à états de liens comme OSPF et des protocoles hybrides comme EIGRP.
Le routage a été considérée très vulnérable à plusieurs types d'attaque. Cependant, l'attaque contre des protocoles de routage, notamment les protocoles de routage " intera-domaine " RIP, OSPF, EIGRP, peuvent affecter globalement la connectivité de réseau et causer la déconnexion, la modification de donnés et l'instabilité de communication.
Au terme de cette étude, nous avons considéré trois protocoles de routage (RIP, OSPF et EIGRP) et le mécanisme d'authentification MD5 pour sécuriser les mises à jour de routage pour ces protocoles.

Mots-clés : Routage dans WAN, RIP, OSPF, EIGRP, sécurité de routage, authentification MD5.

Abstract

The routing is a key function of the network layer, allowing packets to be routed from one network to another. For this purpose, different protocols have been developed and different classifications of these protocols have been proposed, among other things, we find the class of distance vector protocols like RIP and IGRP protocols, and links state protocols as OSPF and hybrids as EIGRP.
Internet routing has been considered strictly vulnerable to several types of attacks. Routing protocol attacks, especially against the intera-domain routing protocol like RIP, OSPF, EIGRP, can globally affect network connectivity and cause loss of connectivity, instability or even data modification.
Au terme of this study, we considered three routing protocols (RIP, OSPF and EIGRP) and configured MD5 authentication mechanism to secure routing updates to the routing protocols.

Keywords : WAN routing, RIP, OSPF, EIGRP, routing security, MD5 authentication.

LISTE DES ABRÉVIATIONS

ACL	**A**ccess **C**ontrol **L**ist
AS	**A**utonomous **S**ystem
AUX	**A**uxiliaire
BDR	**B**ackup **D**esignated **R**outer
BGP	**B**order **G**ateway **P**rotocol
BIOS	**B**asic **I**nput **O**utput **S**ystem
AC	**A**uthority **o**f **C**ertification
CLI	**C**ommand **L**ine **I**nterface
CPU	**C**entral **P**rocessing **U**nit
DBD	**D**ata **B**ase **D**escription
DES	**D**ata **E**ncryption **S**tandard
DoS	**D**eni **o**f **S**ervice
DR	**D**esignated **R**outer
DTE	**D**ata **T**erminal **E**quipment
DUAL	**D**iffusing **U**pdate **A**lgorithme
DV	**D**istance **V**ictor
EGP	**E**xterior **G**ateway **P**rotocol
EIGRP	**E**nhanced **I**nterior **G**ateway **R**outing **P**rotocol
FAI	**F**ournisseur d'**A**ccès à **I**nternet
FDD	**F**iber **D**istributed **D**ata
FTP	**F**ile **T**ransfert **P**rotocol
GNS3	**G**raphical **N**etwork **S**imulator
HTTP	**H**yper**T**ext **T**ransfer **P**rotocol
IETF	**I**nternet **E**ngineering **T**ask **F**orce
IGP	**I**nterior **G**ateway **P**rotocol

IGRP	**I**nterior **G**ateway **R**outing **P**rotocol
IOS	**I**nternetworking **O**perating **S**ystem
IP	**I**nternet **P**rotocol
IR	**I**nfrarouge
IS-IS	**I**ntermediate **S**ystem to **I**ntermediate **S**ystem
ISO	**I**ternational **S**andard **O**ganisation
LAN	**L**ocal **A**rea **N**etwork
LS	**L**ink **S**tate
LSA	**L**ink **S**tate **A**dvertisement
LSAck	**L**ink **S**tate **A**cknowledgement
LSR	**L**ink **S**tate **R**equest
LSU	**L**ink **S**tate **U**pdate
MAC	**M**edium **A**cces **C**ontrol
MAN	**M**etropolitan **A**rea **N**etwork
MD5	**M**essage **D**igest 5
MTU	**M**aximum **T**ransmit **U**nit
NAT	**N**etwork **A**dresses **T**ranslation
NVRAM	**N**on **V**olatile **R**andom **A**ccess **M**emory
OSI	**O**pen **S**ystems **I**nterconnection
OSPF	**O**pen **S**hortest **P**ath **F**irst
PAN	**P**ersonal **A**rea **N**etwork
PC	**P**ersonal **C**omputer
RAM	**R**andom **A**ccess **M**emory
RC	**R**ivest **C**ipher
RFC	**R**equest **S**ystems **C**omment
RIP	**R**outing **I**nformation **P**rotocol
ROM	**R**ead **O**nly **M**emory
RTC	**R**éseau **T**éléphonique **C**ommute
RTP	**R**eliable **T**ransport **P**rotocol
SPF	**S**hortest **P**ath **F**irst
SRI	**S**tanford **R**esearch **I**nstitute
SSH	**S**ecure **S**hell
TCP	**T**ransmission **C**ontrol **P**rotocol
TFTP	**T**rivial **F**ile **T**ransfer **P**rotocol
TLV	**T**ype **L**ongueur **V**aleur
UDP	**U**ser **D**atagram **P**rotocol
VLSM	**V**ariable **L**enght **S**ubnet **M**asking

VTY	**V**irtual **T**erminal
WAN	**W**ide **A**rea **N**etwork

TABLE DES MATIÈRES

LISTE DES TABLEAUX

TABLE DES FIGURES

INTRODUTION GÉNÉRALE

De nos jours, les réseaux informatique nous ont envahit dans notre vie quotidienne, comme l'Internet qui est devenues un élément incontournable pour beaucoup de gens, et indispensable pour les informaticiens. Elle permet aux personnes de communiquer comme jamais auparavant.

Au centre du réseau se trouve le routeur qui fonctionne au niveau de la couche réseau du modèle OSI. En raison de leur capacité d'acheminer les paquets en fonction des informations de couche, Il est devenu le backbone d'Internet et exécute le protocole IP. Leur rôle consiste à examiner les paquets entrants, à choisir le meilleur chemin pour les transporter sur le réseau et à les commuter ensuite au port de sortie approprié. Sur les grands réseaux, les routeurs sont les équipements de régulation du trafic les plus importants.

Au début, les tables de routage étaient statiques et donc maintenues à jour par des techniciens. Mais avec l'explosion rapide du réseau Internet, il est devenu impossible d'assurer la connectivité avec la même approche. Maintenant, les mises à jour des tables de routage et le calcul du meilleur chemin sont automatiquement propagés sur le réseau par les protocoles de routage dynamique qui ont pour objectif de maintenir les tables de routage du réseau dans un état intègre et cohérent.

Les protocoles de routage ont été considérée très vulnérable à plusieurs types d'attaque et n'implémentent pas de véritable couche de sécurité et lors de l'échange d'information entre les routeurs pour mettre à jour leur table de routage, ces information peuvent être aussi vulnérable aux attaques lors de l'acheminement, cela peut affecter globalement la connectivité de réseau, rediriger le trafic ou causer l'instabilité permanente dans le réseau.

Pour vérifier l'authenticité et la validité de ces informations, nous allons proposer le mécanisme d'authentification md5 pour remédier à certains de ces attaques. Le but de notre

travail est d'implémenté le mécanisme d'authentification md5 sur les paquets des mises à jours des protocoles de routage dynamique RIP, EIGRP et OSPF.

Ce mémoire est organisé en quatre chapitres

Dans le ***chapitre 1***, sera consacré sur un aperçu général sur les réseaux informatiques.

Le ***chapitre 2***, est consacré à l'état de l'art sur les protocoles de routage dynamique (RIP, OSPF et EIGRP). Nous présentons d'abord la notion de routage et ses différentes techniques ainsi que les différentes classifications existantes de ces derniers. Puis, nous allons définir le principe de chaque protocole.

Dans le ***chapitre 3***, nous allons décrire les problèmes liés au routage et les différentes attaques concernant chaque protocole de routage, ensuite nous allons proposer quelque mécanismes pour faire face à ces attaques.

Le ***chapitre 4***, sera consacré à la partie pratique de nôtre travail, dans laquelle nous avons définit les différentes configurations des routeurs et l'implémentation des commandes de sécurité des mises à jour dans les protocoles de routages, puis nous présenterons l'environnement de travail ainsi que le cas d'étude qui consiste à faire une configuration de ces protocoles sur le réseau du groupe Cevital où des résultats de configuration seront présentés.

Enfin, notre travail s'achève par une conclusion générale.

CHAPITRE 1

GÉNÉRALITÉS SUR LES RÉSEAUX INFORMATIQUES

1.1 Introduction

Un réseau informatique permet à plusieurs ordinateurs de communiquer entre elles afin d'assurer des échanges d'informations. Les avancées récentes dans le domaine de communication, le rapprochement de l'informatique et des télécommunications ont eu une profonde influence sur la structuration des systèmes informatiques et la communication devient une partie intégrante de ces derniers.

Dans ce chapitre, nous présentons brièvement quelques notions théoriques sur les réseaux informatiques. D'abord, en commençant par définir le réseau informatique, ensuite nous allons définir le modèle OSI et le modèle TCP/IP en générale et la couche réseaux en particulier.

1.2 Définition d'un réseau

Le terme générique d'un réseau est un ensemble d'objets interconnectes les uns avec les autres. Il permet de faire circuler des éléments entre chacun de ces objets.

Cependant un réseau informatique est un ensemble d'ordinateurs relies entre eux grâce à des lignes physiques et échangeant des informations sous forme de données numériques (des valeurs binaires) [1].

1.3 Topologies d'un réseau

La topologie décrit la manière dont les équipements réseau sont connectés entre eux. Nous différencions deux types de topologie :

1.3.1 Topologie physique

Un réseau informatique est constitué d'ordinateurs relies entre eux grâce à des lignes de communication et des éléments matériels. L'arrangement physique, c'est à dire la configuration spatiale du réseau est appelé topologie physique. Les différentes topologies physique sont :

- la topologie en bus.
- la topologie en étoile.
- la topologie en anneau.
- la topologie en arbre.

- **Topologie en bus** : est l'organisation la plus simple d'un réseau. En effet, Dans une topologie en bus (voir la figure 1.1) tous les ordinateurs sont relies à une même ligne de transmission par l'intermédiaire de câbles, généralement de type coaxial. Cette topologie à pour avantage d'être facile à mettre en œuvre et posséder un fonctionnement simple.

FIGURE 1.1 – Topologie en bus.

- **Topologie en étoile** : dans une topologie en étoile (voir la figure 1.2), les ordinateurs du réseau sont relies à un système matériel central (peut être un concentrateur, un commutateur, un routeur, etc.) qui va diriger toutes les connexions. En revanche, un réseau à topologie en étoile est onéreux qu'un réseau à topologie en bus car un matériel supplémentaire est nécessaire.

FIGURE 1.2 – Topologie en étoile.

- **Topologie en anneau** : dans un réseau structuré en anneau (voir la figure 1.3), les ordinateurs sont situés sur une boucle et communiquent chacun à leur tour. Une trame, appelée jeton, circule autour de l'anneau et s'arrête à chaque nœud. Si un nœud souhaite transmettre des données, il ajoute les données et les informations sur les adresses à la trame. La trame continue de circuler autour de l'anneau jusqu'à ce qu'elle trouve le nœud de destination. Ce dernier récupère alors les données dans la trame. L'avantage de cette topologie est qu'il n'y a pas de risque de collisions de paquets de données.

FIGURE 1.3 – Topologie en anneau.

- **Topologie maillée** : comme le montre la figure 1.4, dans la topologie maillée, chaque poste est reliée directement à tous les postes du réseau. Avec cette topologie peut garantie une meilleure stabilité du réseau en cas d'une panne du nœud. Mais est difficile à mettre en œuvre et ne peut pas être utilisé dans les réseaux internes Ethernet. Il peut facilement devenir très coûteux.

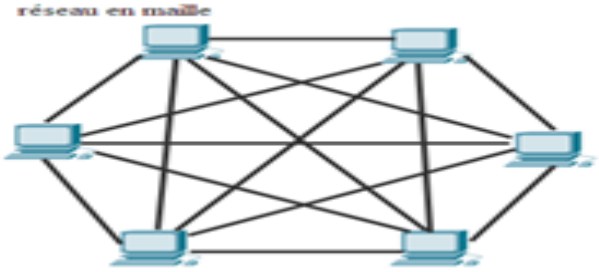

FIGURE 1.4 – Topologie maillée.

1.3.2 Topologie logique

La topologie logique par opposition à la topologie physique, représente la façon dont les données transitent dans les lignes de communication. Les topologies logiques les plus courantes sont : Ethernet, Token Ring et FDDI [2].

1.4 Classification des réseaux

Selon leur taille en termes de nombre de machines, leur vitesse de transfert des données ainsi que leur étendue. Il existe divers types de réseaux comme illustre dans la figure 1.5 [1] :

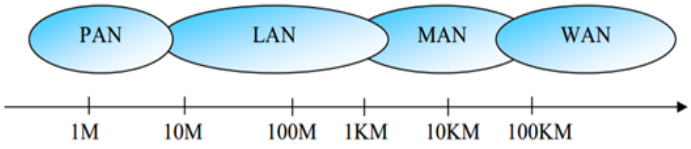

FIGURE 1.5 – Types de réseaux.

- **Les réseaux personnels PAN** : désigne un réseau restreint d'équipements informatiques habituellement utilisés dans le cadre d'une utilisation personnelle. Les technologies les plus utilisés sont Bluetooth, (IR), etc [1].
- **Les réseaux locaux LAN** : désigne un ensemble d'ordinateurs appartenant à une même organisation et reliés entre eux dans une petite aire géographique par un réseau. Sa vitesse de transfert de données peut s'échelonner entre 10 Mbps et 1 Gbps. La taille d'un réseau local peut atteindre jusqu'à 100 voire 1000 machines [1].
- **Les réseaux métropolitains MAN** : interconnectent plusieurs réseaux locaux géographiquement proches avec un débit important. Ainsi un MAN permet à deux machines distantes de communiquer comme si elles faisaient partie d'un même réseau local [1].

- **Les réseaux distants WAN** : un réseau étendu interconnecte plusieurs réseaux à travers de grandes distances géographiques. Les WAN fonctionnent grâce à des équipements réseau appelés routeurs, qui permettent de déterminer le trajet le plus approprié pour atteindre une machine du réseau [1].

1.5 Modèle OSI et le modèle TCP/IP

Il existe deux types de modèles de réseau de base (voir la figure 1.6) : le modèle de référence OSI et le modèle protocolaire TCP/IP.

Un modèle de référence fournit une référence commune pour maintenir la cohérence dans tous les types de protocoles et de services réseau. Le modèle OSI constitue le modèle de référence inter-réseau le plus répandu. Il est utilisé pour la conception de réseaux de données, pour les spécifications de fonctionnement et pour le dépannage.

Un modèle de protocole fournit un modèle qui correspond étroitement à la structure d'une suite de protocoles particulière. Le modèle TCP/IP est un modèle de protocole, car il décrit les fonctions qui interviennent à chaque couche de protocoles au sein de la suite TCP/IP [3].

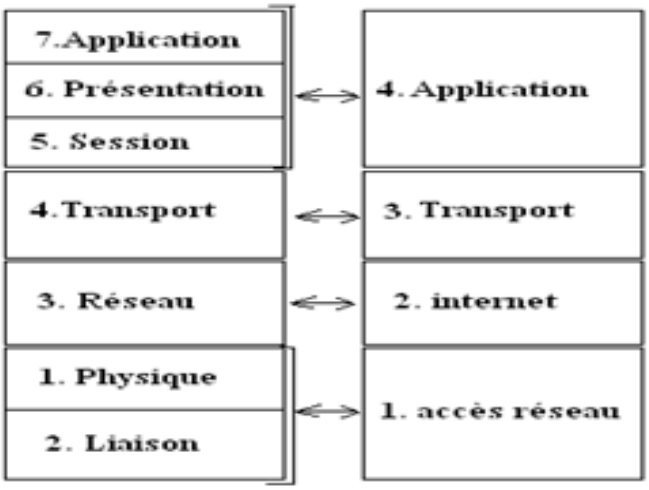

FIGURE 1.6 – Modèle OSI et TCP/IP.

1.5.1 Modèle OSI

OSI est un modèle de base qui a été défini par l'ISO, il est composé de sept couches logiques, chacune comportant des fonctionnalités uniques et se voyant attribuer des services et des protocoles spécifiques. Les rôles des différentes couches sont les suivants [4] [1] :

- **Couche physique** : définit la façon dont les données sont physiquement converties en signaux numériques sur le media de communication (impulsion électriques, modulation de la lumière, etc.). L'unité d'information de cette couche est le bit [4] [1].
- **Couche liaison de données** : définit l'interface avec la carte réseau et le partage du media de transmission. L'unité d'information de la couche liaison de données est la trame [4] [1].
- **Couche réseau** : permet de gérer l'adressage et le routage des données, c'est à dire leur acheminement via le réseau. L'unité d'information de la couche réseau est le paquet [4] [1].
- **Couche transport** : est charger de transport des données, de leur découpage en paquets et de leur gestion des éventuelles erreurs de transmission [4] [1].
- **Couche session** : définit l'ouverture et la destruction des sessions de communication entre les machines du réseau [4] [1].
- **Couche présentation** : définit le format des données manipulées par le niveau applicatif (leur représentation, leur compression et leur chiffrement) indépendamment du système [4] [1].
- **Couche application** : assure l'interface avec les applications. Il s'agit donc du niveau le plus proche des utilisateurs, gère directement par les logiciels [4] [1].

1.5.2 Modèle TCP/IP

Le model TCP/IP reprend l'approche modulaire du modèle OSI mais ne contient, lui, que quatre couches. Ces couches ont des taches beaucoup plus diverses étant donné qu'elles correspondent à plusieurs couches du modèle OSI. Les rôles des différentes couches sont les suivants [1] :

- **Couche accès réseau** : spécifie la forme sous laquelle les données doivent être acheminées quel que soit le type de réseau utilisé [1].
- **Couche Internet** : assure l'acheminement et le routage des données [1].
- **Couche transport** : est chargée de fournir le paquet de données (datagramme), ainsi que les mécanismes permettant de connaitre l'état de la transmission. Les deux principaux protocoles pouvant assuré les services de cette couche sont les suivant [1] :
  - TCP : est un protocole fiable, assurant une communication sans erreur par un mécanisme question/réponse /confirmation/ synchronisation (oriente connexion).
  - UDP : est un protocole non-fiable, assurant une communication rapide mais pouvant contenir des erreurs en utilisant un mécanisme question/réponse (sans connexion).
- **Couche application** : englobe les application standards du réseau [1].

L'acheminement des données entre l'émetteur et le récepteur au travers de différents réseaux se fait dans la couche réseau.

1.6 Représentation détaillée de la couche Internet du modèle TCP/IP

La couche Internet utilise le principe des méthodes de sélection du chemin qui permettent aux équipements de couche 3 (les routeurs) de déterminer la route à suivre pour acheminer les informations au travers de différents réseaux. Les services de routage utilisent les informations de topologie du réseau pour évaluer les chemins. Autrement dit un routage des paquets qui prend en compte divers paramètres.

1.6.1 Routeur CISCO

Un routeur est un type spécial d'ordinateur, il est conçu pour assurer la communication entre deux réseaux et déterminer le meilleur chemin pour les données à travers les réseaux connectés [7].

Les routeurs fonctionnent sur la couche 3 du modèle OSI, et prennent des décisions en fonction des adresses réseau. Les deux fonctions principales d'un routeur sont de sélectionner le meilleur chemin pour les paquets et de commuter ces paquets vers l'interface appropriée. Pour ce faire, les routeurs créent des tables de routage et échangent des informations sur le réseau avec d'autres routeurs.

Les routeurs doivent être équipés d'une plate-forme logicielle IOS pour exécuter les fichiers de configuration. Plus précisément, en utilisant des protocoles de routage, les routeurs décident du meilleur chemin pour les paquets. Les principaux composants internes du routeur (voir la figure 1.7) sont [27] [7] :

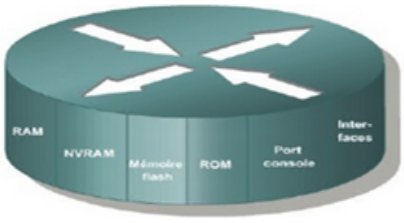

FIGURE 1.7 – Architecture interne d'un routeur Cisco.

- **RAM** : principalement contenant le logiciel IOS, c'est dans laquelle tout sera exécuté un peu à la manière d'un simple ordinateur.

- **NVRAM** : elle est relativement lente et est de taille restreinte (environ 32 Ko), elle permet à l'administrateur de stocker la configuration qu'il aura mise dans le routeur. Elle contient également la configuration de l'IOS.
- **Flash** : également appelé une mémoire non volatile, utilisée pour le stockage d'une image complète de la plate-forme logicielle Cisco IOS.
- **ROM** : sert à stocker de façon permanente le code de diagnostic de démarrage (ROM Monitor). Cette mémoire est l'équivalent du BIOS d'un PC.
- **Interfaces** : connexions réseau situées sur la carte mère ou sur des modules d'interface distincts, grâce auxquelles les paquets entrent dans le routeur et le quittent.
  - Une carte mère qui est en général intégrée au châssis (bordure).
  - Une CPU qui est un microprocesseur Motorola avec un BIOS spécial nommé IOS.

1.6.2 Adressage de la couche réseau

Les protocoles de la couche réseau (protocole TCP/IP) utilisent un système d'adressage garantissant l'unicité des adresses sur le réseau et définissant une méthode d'acheminement des informations entre les réseaux. Ces protocoles utilisent des numéros de 32 bits, que l'on écrit sous forme de 4 numéros allant de 0 à 255, ces numéros servent aux ordinateurs du réseau pour se reconnaître, ainsi il ne doit pas exister deux ordinateurs sur le réseau ayant la même adresse IP.

Il existe deux types d'adresses IP : IP version 4 (IPv4) est la plus utilisée, généralement notée avec quatre nombres compris entre 0 et 255, séparés par des points et IP version 6 (IPv6) pour sa part utilise des adresses de 128 bits sont formées de 8 paquets de 4 chiffres en hexadécimaux séparés par le signe deux-points [5].

1.6.3 Protocole IP

Le protocole IP fonctionne sur la couche Internet de la pile TCP/IP, il détermine où les paquets de données doivent être acheminés en fonction de leurs adresses de destination. IP est un protocole sans connexion.

1.6.4 Définition d'une adresse IPv4

Une adresse IP est une adresse de 32 bits, généralement notée sous forme de quatre nombres entiers séparés par des points. Il existe deux parties dans l'adresse IP [1] :

- Les premiers bits forment l'identifiant réseau ou netID (identificateur du reseau).
- Les bits suivants forment le numéro d'hôte ou hostID (identificateur de la machine) pour distinguer les machines du réseau.

1.6.4.1 Adressage IPv4

Sur Internet, les ordinateurs communiquent entre eux grâce aux protocoles IP, qui utilise les adresses numériques, appelées adresses IP.

1.6.4.2 Format du datagramme IPv4

Le datagramme IP contient l'en-tête IP (voir la figure 1.8) suivi des données IP provenant des protocoles des couches supérieures [5].

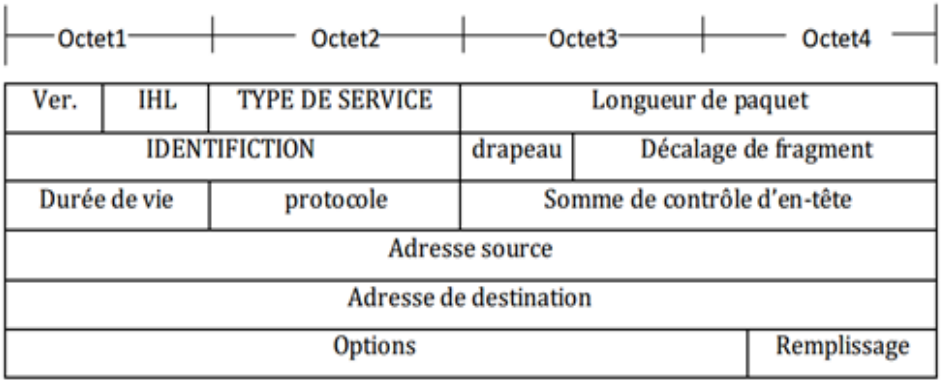

FIGURE 1.8 – En-tête de données de protocole IP.

1.6.4.3 Classes d'adresse IPv4

Les adresses IP sont regroupées en classes, selon le nombre d'octets qui représentent le réseau comme le montre le tableau 1.1 suivant [1] :

Classe d'adresse	Plage de premier octet	Masque par défaut	Nombres de réseaux et d'hôtes
A	1-127	255.0.0.0	2^7-2 réseaux et 2^{24}-2 hôtes
B	128-191	255.255.0.0	2^{14}-2 réseaux et 2^{16}-2 hôtes
C	192-223	255.255.255.0	2^{21}-2 réseaux et 2^8-2 hôtes
D	224-239	Non défini	Non défini
E	240-255	Non défini	Non défini

TABLE 1.1 – Plages d'adresse IPv4.

- **Classe A** : dans une adresse IP de classe A, le premier octet représente le réseau. Le bit de poids fort est à zéro, ce qui signifie qu'il y a 2^7 possibilités de réseaux, soit 128 possibilités. Les deux numéros de réseau, 0 et 127 sont réservés et ne peuvent pas être utilisés comme adresse réseau.

- **Classe B** : dans une adresse IP de classe B, les deux premiers octets représentent le réseau. Les deux premiers bits sont 1 et 0, ce qui signifie qu'il y a 2^{14} possibilités de réseau. Les deux octets de droites représentent les ordinateurs du réseau.
- **Classe C** : dans une adresse IP de classe C, les trois premiers octets représentent le réseau. Les trois premiers bits sont 1, 1 et 0 se qui signifie qu'il y a 2^{21} possibilités de réseaux. L'octet de droite représente les ordinateurs du réseau.
- **Classe D et E** : les deux classes D et E sont réservés, la classe D est réservé pour les multicast, la classe E est une classe expérimentale.

1.6.5 Adresses réservées

Les adresses réservées ne peuvent désigner une machine TCP/IP sur un réseau [5].

- **Adresse d'acheminement par défaut (route par défaut)** : tous les paquets destinés à un réseau non connu, seront dirigés vers l'interface désignée par 0.0.0.0. Elle est utilisée aussi pour connaître son adresse IP.
- **Adresse de bouclage (loopback)** : l'adresse de réseau 127 n'est pas attribuée à une société, elle est utilisée comme adresse de bouclage dans tous les réseaux. Cette adresse sert à tester le fonctionnement de la carte réseau d'une machine. On utilise généralement 127.0.0.1.
- **Adresse de réseau** : est une adresse dont tous les bits d'hôte sont positionnés à 0 (exemple : 128.10.0.0 adresse de réseau du réseau 128.10 de classe B). Elle est utilisée pour désigner tous les postes du réseau. On utilise cette adresse dans les tables de routage.
- **Adresse de diffusion** : est une adresse dont tous les bits d'hôte sont positionnés à 1. Elle est utilisée pour envoyer un message à tous les postes du réseau.
- **Adresses privées** : est un réseau qui utilise les plages d'adressage. Ces adresses ne sont pas routées sur Internet. Le tableau 1.2 répertorie les plages d'adresses IP privées et des masques de réseau respectifs.

Classe	Plage d'adresses IP	Masque de réseau
A	10.0.0.0 - 10.255.255.255	10.0.0.0
B	172.16.0.0 - 172.31.255.255	172.16.0.0
C	192.168.0.0 - 192.168.255.255	192.168.0.0

TABLE 1.2 – Plages d'adresses IP privées.

1.6.5.1 Masque d'un réseau

Le masque du réseau est une suite de 32 bits composée en binaire de N bits à 1 suivit de 32 - N bits à 0. Il est divisé en 4 groupes de 8 bits (1 Octet). Le rôle du masque réseaux est d'identifier précisément les bits qui concernent le numéro de réseau d'une adresse (Identifient Réseaux) et sa on utilisant un ET logique entre l'adresse IP et le masque réseaux comme le montre le tableau 1.3 :

Classe	A	B	C
Adresse IP	50.98.78.67	130.89.67.45	192.168.1.2
Conversion de l'adresse en binaire	00110010.01100010.01001110.01000011	10000010.01011001.01000011.00101101	11000000.1010100.00000001.00000010
Masque de ce réseau	255.0.0.0	255.255.0.0	255.255.255.0
Conversion du masque en binaire	11111111.00000000.00000000.00000000	11111111.11111111.00000000.00000000	11111111.1111111.11111111.00000000
ET logique	00110010.00000000.00000000.00000000	10000010.01011001.00000000.00000000	11000000.1010100.00000001.00000000
Identifient réseaux	50.0.0.0	130.89.0.0	192.168.1.0

TABLE 1.3 – Exemple d'utilisation du Masque réseau.

1.6.6 Sous réseau

Il est possible de découper un réseau en sous-réseaux en utilisant un masque de sous-réseau. Chaque sous-réseau peut être découpé en sous-sous-réseaux et ainsi de suite. On parle indifféremment de réseau IP pour désigner un réseau, un sous-réseau, etc. Chaque sous-réseau sera défini par un masque et une adresse IP.

a- Masque de sous-réseau

Le masque de sous-réseau est un ensemble de 4 octets destiné à isoler le ID (Identificateur) réseau ou ID de sous réseau et ID de l'hôte.

- Soit l'adresse de réseau (ID réseau ou ID sous réseau) en effectuant un ET logique bit à bit entre l'adresse IP et le masque.
- Soit l'adresse de l'hôte (ID hôte) en effectuant un ET logique bit à bit entre l'adresse IP et le complément du masque.

b- Masque variable VLSM

Avec VLSM, un administrateur réseau peut utiliser un masque long sur les réseaux qui ne comportent pas beaucoup d'hôtes et un masque court sur les sous réseaux qui comportent beaucoup d'hôtes. Pour pouvoir utiliser VLSM, un administrateur réseau doit utiliser un protocole de routage compatible avec cette technique.

Les routeurs Cisco sont compatible avec VLSM grâce aux solutions OSPF, BGP, RIPv2, EIGRP, IS-IS et un routage statique. La technique VLSM permet à une entreprise d'utiliser plusieurs sous masque dans le même espace d'dressage réseau.

1.7 Conclusion

Dans ce chapitre, quelques notions de bases sur les réseaux informatiques ont été présenté, à savoir la définition des réseaux, ses différents types et leurs topologies. Nous avons vu le modèle de référence OSI et le modèle TCP/IP, en se basant sur la couche réseau qui gère l'acheminement et le routage des données qu'on va détailler dans le chapitre 2.

CHAPITRE 2

ETAT DE L'ART SUR LES PROTOCOLES DE ROUTAGE DANS LES RÉSEAUX À MOYENNE DIMENSION

2.1 Introduction

La communication entre des hôtes sur un réseau requiert l'interaction de nombreux protocoles différents. Un groupe de protocoles associés entre eux est nécessaires pour remplir une fonction de communication est appelé suite de protocoles. Ces protocoles sont implémentés dans des logiciels et du matériel chargés sur chaque hôte et périphérique réseau.

Le routage est la spécification de directions pour naviguer de réseau en réseau. Ces directions, également appelées routes, peuvent être indiquées de façon dynamique par un autre routeur ou attribuées de façon statique par un administrateur.

Le choix d'un protocole de routage dynamique se fait en fonction de nombreuses considérations. Cette partie détaille les différences entre ces protocoles afin d'aider les administrateurs réseau à faire leur choix.

2.1.1 Routage IP

Le routage est le processus qu'un routeur utilisé pour transmettre des paquets vers un réseau de destination. Un routeur prend des décisions en fonction de l'adresse IP de destination d'un paquet. Tout le long du chemin, les divers équipements se servent de l'adresse IP de destination pour orienter le paquet dans la bonne direction afin qu'il arrive à destination. Pour prendre les bonnes décisions, les routeurs doivent connaître la direction à prendre jusqu'aux réseaux distants [7]. Alors les routeurs utilisent deux types de routage :

- **Routage statique** : les informations doivent être configurées manuellement sur les réseaux distants, toute modification de la topologie réseau oblige l'administrateur à ajouter et supprimer des routes statiques pour tenir compte des modifications.
- **Routage dynamique** : les routeurs peuvent réagir aux changements survenus sur le réseau et modifier leurs tables de routage, sans intervention de la part de l'administrateur réseau.

2.1.2 Table de routage

C'est un regroupement d'informations permettant de déterminer le prochain routeur à utiliser pour accéder à un réseau précis sur lequel se trouve l'hôte de destination [6]. Une table de routage est constituée essentiellement de :

- Destination : adresse IP d'une machine ou d'un réseau de destination.
- Passerelle (Gateway) : adresse IP du prochain routeur dans le chemin de destination.
- Masque : le masque associé au réseau de destination.
- Interface : désigne l'interface physique par laquelle le paquet doit réellement être expédié.

2.2 Protocoles de routage

Un protocole de routage est le système de communication utilisé entre les routeurs. Il permet à un routeur de partager avec d'autres routeurs des informations sur les réseaux qu'il connaît, ainsi que sur leur proximité avec d'autres routeurs. Les informations qu'un routeur reçoit d'un autre routeur, à l'aide d'un protocole de routage, servent à mettre à jour une table de routage.

Un protocole routé sert à diriger le trafic utilisateur. Il fournit suffisamment d'informations dans son adresse de couche réseau pour permettre l'acheminement d'un paquet d'un hôte à un autre en fonction de la méthode d'adressage [7].

Les protocoles de routage dynamique ont été spécifiquement conçus pour mettre à jours la table de routage d'un hôte ou d'un routeur. Pour ce faire, ils s'échangent des paquets de mises à jours de routage contenant des informations destinées à remplir la table de routage.

2.3 Concepts fondamentaux

Avant de définir les différents protocoles de routage, il est important de donner quelques notions fondamentales sur l'interconnexion des réseaux.

2.3.1 Système Autonome AS

Un système autonome est un ensemble de réseaux administrés par une même entité, il est perçu comme une entité unique pour présenter au monde extérieur une vue cohérente du routage. Son objectif est assuré une division de l'inter-réseau global en réseaux plus petits et plus faciles à gérer. Chaque système autonome possède son propre ensemble de règles et un numéro AS unique qui le distinguera des autres systèmes autonomes à travers le monde [7].

Le réseau interne d'une société et le réseau d'un fournisseur de services Internet en sont des exemples.

Un routeur peut router à l'intérieur d'un AS (routage Intra AS) et entre des AS (routage inter AS) comme le montre figure 2.1.

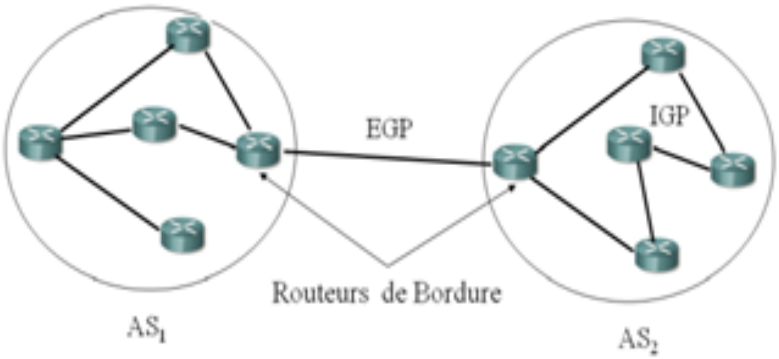

FIGURE 2.1 – Systèmes autonomes et routage intra et inter-domaine.

2.3.2 Zones (Area)

Le réseau est divisé en plusieurs zones de routage qui contiennent des routeurs et des hôtes, les zones (voir Figure 2.2) sont des sous-réseaux qui composent un AS, chaque zone identifiée par un numéro, possède sa propre topologie et ne connaît pas la topologie des autres zones, il existe trois types de zones :

- Zone Backbone ou Area 0.
- Les zones secondaires.
- Les zones terminales (Stub Area).

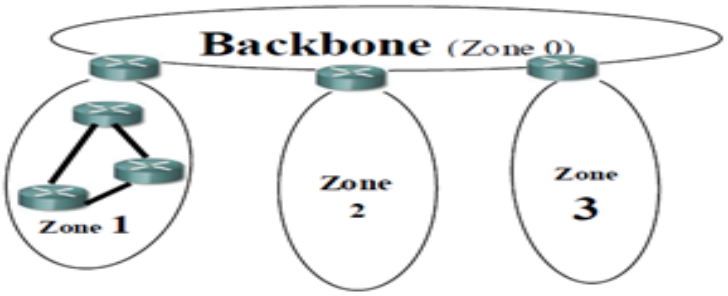

FIGURE 2.2 – Les Zones.

2.3.3 Rapidité de convergence

C'est le temps que mettent l'ensemble des routeurs du réseau à faire l'apprentissage de leurs environnements ou à réagir à un changement du réseau, pour le consigner sur leurs tables de routage.

2.3.4 Métrique

C'est une mesure utilisée par un protocole de routage pour déterminer quelles routes sont les meilleures, on le calcule en fonction d'une seule ou plusieurs caractéristiques du chemin :

- **Saut** : le nombre de routeurs par lesquels un paquet doit passer avant d'arriver à destination.
- **Fiabilité** : il indique en général le taux d'erreurs sur chaque liaison du réseau.
- **Délai** : c'est le temps requis pour acheminer un paquet, pour chaque liaison, de la source à la destination.
- **Charge** : la quantité de trafic sur une ressource réseau telle qu'une liaison où un routeur.
- **Coût** : il est basé en général sur une dépense monétaire attribuée à un lien par un administrateur réseau.
- **MTU** : c'est l'unité de transmission maximale (la taille maximale d'un paquet pouvant être transmis en une seule fois sur une interface).

2.3.5 NAT

NAT est un mécanisme permettant de traduire une adresse réseau interne privée à une adresse IP publique routable. Cela permet de transporter le paquet sur des réseaux externes publics. La fonction NAT offre de grands avantages aux sociétés individuelles et à Internet, Les services NAT permettent aux hôtes du réseau d'emprunter une adresse publique pour communiquer avec des réseaux externes. Bien que les services NAT soient associés à des limitations et à

des problèmes de performances, ils permettent aux clients de nombreuses applications d'accéder à des services sur Internet, sans difficulté majeure [8].

2.3.6 Passerelle et route par défaut

Une route est définie par une paire d'adresses : une destination et une passerelle. Cette paire signifie que pour atteindre cette destination, vous devez passer par cette passerelle. Il y a trois sortes de destination : les machines individuelles, les sous-réseaux et default (la destination par défaut). Si le paquet ne correspond pas à une route plus spécifique de la table de routage, il sera acheminé vers le réseau 0.0.0.0. Une route par défaut consiste en une entrée de table de routage permettant de diriger les paquets pour lesquels le prochain saut n'est pas explicitement indiqué dans la table de routage.

2.4 Classes des protocoles de routage

Les protocoles de routage peuvent être classés en deux catégories : ce qui est intra-domaine appelés IGP et ceux qui inter-domaine appelé EGP. Les protocoles de routage IGP constituent le sujet de notre travail la figure 2.3 illustre la classification des protocoles de routage :

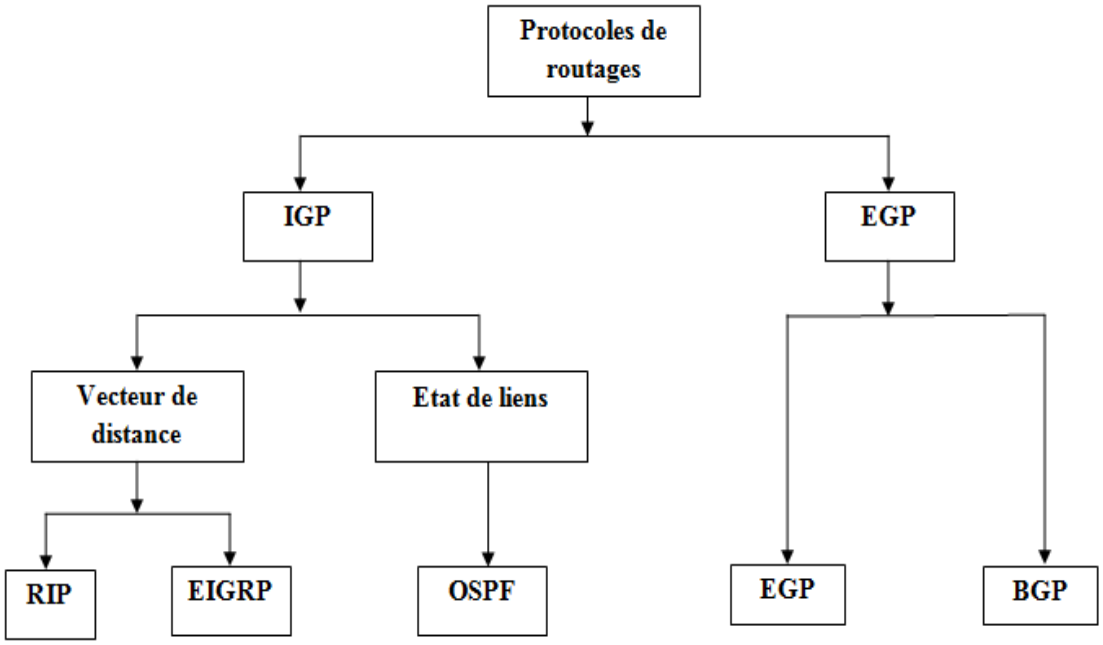

FIGURE 2.3 – Classes des protocoles de routage.

2.4.1 Protocole de routage interne

Les protocoles IGP permettent d'échanger des informations de routage au sein d'un système autonome ou d'une organisation individuelle. L'objectif d'un protocole de routage intérieur consiste à trouver le meilleur chemin possible sur le réseau interne au sens d'une métrique donnée [9]. Cette catégorie de protocole se subdivise encore selon l'algorithme sur lequel il est basé :

Protocole de routage à base de vecteur de distance (DV) et protocole de routage à état de liens (LS).

2.4.1.1 Protocole de routage à base de vecteur de distance (DV)

Cet algorithme appelés algorithmes Bellman-Ford, il se base sur le principe qu'il est possible de calculer les plus courts chemins quand la seule information échangée est le vecteur de ces distances. En outre, l'information n'est échangée qu'entre entités adjacentes, i.e., des entités partageant un réseau commun [10].

Les algorithmes de routage à vecteur de distance transmettent régulièrement des copies de table de routage d'un routeur à l'autre (voir la figure 2.4). Ces mises à jour régulières entre les routeurs permettent de communiquer les modifications topologiques [7].

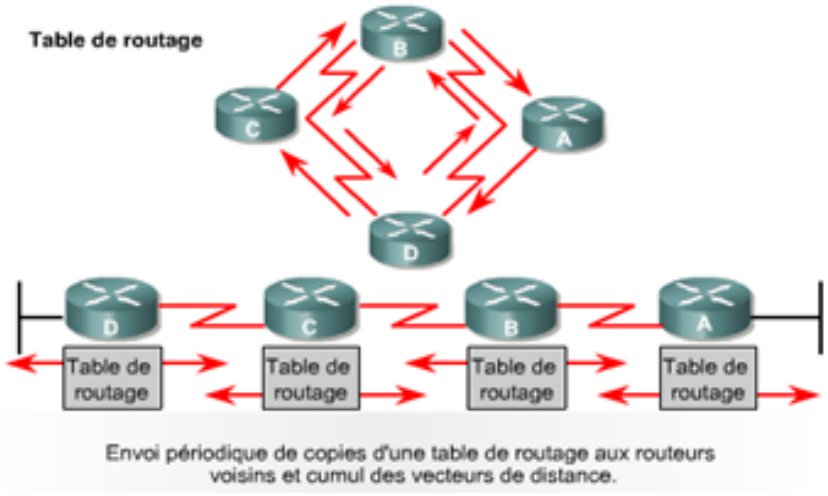

FIGURE 2.4 – Conception de vecteur de distance.

Des boucles de routage peuvent apparaître lorsque des tables de routage incohérentes ne sont pas mises à jour en raison d'une convergence plus lente. Toutefois, pour régler le problème de boucle de routage, les protocoles à vecteur de distance définissent l'infini en tant que nombre maximal spécifique.

Le protocole de routage DV est simple, mais il ne garantit pas le non production de cycle dans un chemin, Ce problème est connu par le nom comptage jusqu'à l'infini.

Plusieurs techniques ont été développées pour éliminer le problème de comptage à l' infini :

- **Split horizon** : définit une règle qui interdit à tout routeur de ne pas envoyer des informations à travers l'interface où elle a appris l'information.
- **Holddown timer (Temporisateur de maintien)** : toute route dispose d'un temporisateur additionnel en plus de son temporisateur normal qui démarre dés que le premier expire et la valeur de la métrique associée à la route affectée est mise a l'infini pour indiquer son caractère inaccessible.
- **Triggered Update** : cette solution consiste à gérer le temps où chaque routeur doit émettre son vecteur de distance. Par ailleurs cette solution exige aux routeurs d'émettre leurs vecteurs de distance dès qu'ils détectent un changement dans leurs tables de routage. Cette procédure accélère la convergence de ce protocole

2.5.1.1.A. Protocole RIP

Le protocole RIP [11], est un protocole à vecteur de distance qui utilise le nombre de sauts comme métrique. S'il existe plusieurs chemins vers une destination, le protocole RIP sélectionne celui qui comporte le moins de sauts.

Ce protocole est limité à 15 sauts, un réseau situé à une distance de plus de 15 sauts il ne peut pas fournir de route pour ce réseau. Les routeurs échangent les informations de routage via des messages de mise à jour qui sont diffusés toutes les 30 secondes. S'il le routeur ne reçoit aucune information de routage de l'un de ces routeurs adjacents pendant 180 secondes (Time out), il mettra à l'infini (métrique = 16) les entrées ayant comme next hop de ce routeur. S'il n'y a toujours aucune mise à jour après 240 secondes, le protocole RIP enlève toutes les entrées dans sa table de routage correspondant au routeur qui ne répond pas.

Avantages de RIP

- RIP destiné principalement à être utilisé sur un petit réseau.
- Il n'engendre qu'une très petite surcharge en termes de bande passante utilisée et de temps de configuration.
- Il est très facile à implémenter, en particulier à une utilisation en tant qu'IGP plus récents.
- La simplicité et les performances de RIP font qu'il est encore largement utilisé aujourd'hui.

Inconvénients de RIP

- RIPv1 ne supporte pas les masques de sous-réseau de longueur variable (VLSM).

- RIP dispose d'un nombre maximal de sauts de 15. Un parcours avec un nombre de sauts supérieur à 15 est considéré comme inaccessible.
- La convergence de RIP est relativement lent par rapport à d'autres protocoles de routage.
- RIPv1 ne prend pas l'authentification en charge.

RIP est décliné en deux versions 1 et 2, RIPv2 étant la plus récente et offre plus de fonctionnalités tout en restant entièrement compatible avec l'ancienne version. RIPv2 remédie à certains inconvénients de RIPv1 et comporte les caractéristiques suivantes :

- permet le routage des sous-réseaux (véhicule le netmask dans le vecteur de distance).
- diffusion multicast (224.0.0.9) : permet aux routeurs RIPv1 d'ignorer les messages RIPv2.
- possibilité d'authentification (cryptée ou non) des messages [12].

Le protocole RIP en particulier RIPv2 est limité aux réseaux dont le plus long chemin implique 15 sauts, ainsi que le problème du comptage à l'infini pour résoudre certaines situations inhabituelles [6].

A.1. Encapsulation du protocole RIPv1 et RIPv2

RIP est un protocole basé sur UDP. Chaque hôte utilisant RIP dispose d'un processus de routage qui envoie et reçoit des datagrammes sur le port UDP numéro 520. Toutes les communications adressées à un processeur RIP d'un autre hôte sont envoyées au port 520. Tous les messages de mise à jour de routage sont envoyés depuis le port 520. Des messages de mise à jour de routage non sollicités ont pour port source et port destination le numéro de port 520. Ceux envoyés en réponse à une requête sont envoyés au port d'où provenait la requête. Des requêtes spécifiques peuvent être envoyées depuis des ports différents de 520, mais sont dirigées vers le port 520 de la machine cible (voir la figure 2.5) [10].

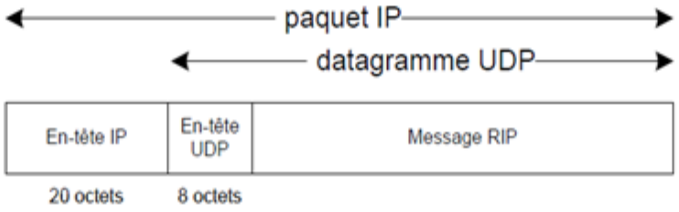

FIGURE 2.5 – Encapsulation de message RIPv1 et RIPv2.

A.2. Format d'un message RIPv1

Les messages au format RIP comme illustre dans la figure 2.6 comportent les paramètres suivants : la commande, version, identificateur de la famille d'adresse, adresse IP et la métrique [10] :

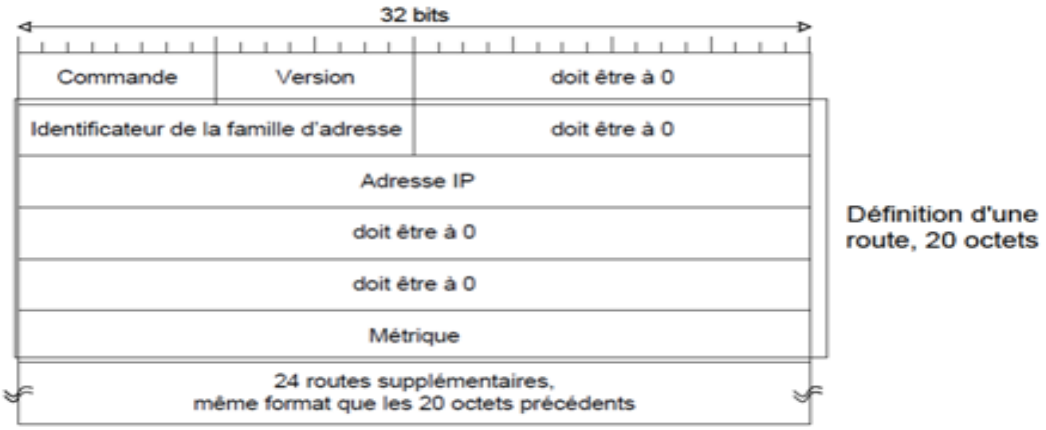

FIGURE 2.6 – Format d'un message RIPv1.

- **Champ Commande** : est utilisé pour spécifier le but de ce message. Ces commandes implémentées dans la version 1 et 2 et permet de distinguer deux types de messages :
  - **requête** : demande au routeur distant d'envoyer tout ou partie de sa table de routage.
  - **Réponse** : message contenant la table de routage.
- **Version** : est positionnée à 1.
  Les 20 octets suivants permettent de décrire une route :
- **Address Family** : toujours à 2 pour le protocole IP.
- **IP Address** : adresse IP de l'hôte ou du réseau concerné.
- **Metric** : métrique associé à l'adresse IP (valeur 15 maximum, 16 pour un réseau inaccessible).

Dans un message RIP, on peut décrire 25 routes au maximum, soit une taille totale du message RIP de 504 octets, Il est souvent nécessaire d'envoyer plusieurs messages pour transmettre la totalité de la table de routage.

A.3. Formats des messages RIPv2

Le même format de message que RIPv1 est utilisé pour RIPv2 [12], comme l'illustre la figure 2.7, sauf qu'elle propose un ensemble d'améliorations par rapport à la version 1 comme le domaine de routage, route tag, masque de sous-réseau et prochain routeur.

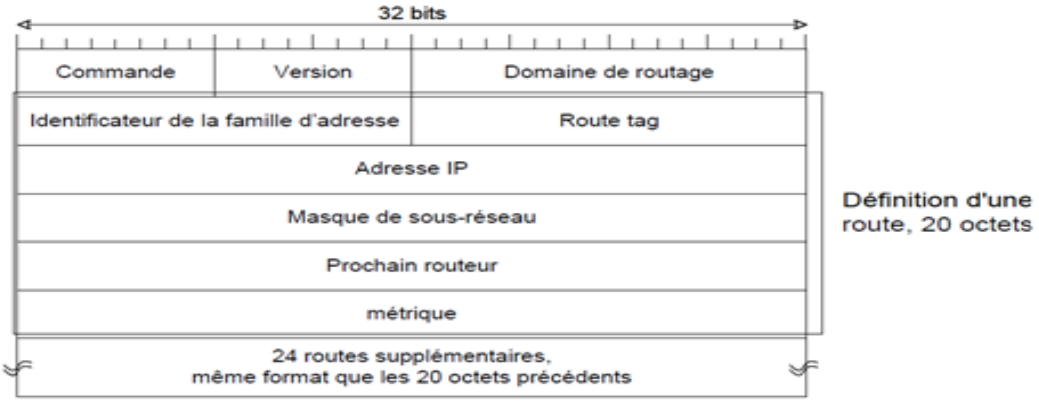

FIGURE 2.7 – Format d'un message RIPv2.

- **Domaine de routage (Routing domain)** : permet d'identifier le démon de routage auquel appartient ce paquet, ce qui permet d'avoir sur un même routeur plusieurs instances de RIP, chacune fonctionnant dans son propre domaine de routage.
- **Route Tag** : permet de supporter des protocoles de routages inter-domaines (EGP), pour lesquels sera véhiculé un numéro de système autonome.
- **Masque de sous-réseau (Subnet Mask)** : s'applique à l'adresse IP correspondante.
- **Prochain router (Next Hop IP Address)** : indique la destination qui sera insérée dans la table de routage du destinataire. Si ce champ est à 0, l'adresse de l'émetteur du message RIP est prise en compte (Utilisation de plusieurs protocoles sur un même routeur).
- **Version** : vaut 2.

2.5.1.1.B. Protocoles de routage IGRP et EIGRP

1. Présentation du protocole IGRP

Le protocole IGRP est un protocole propriétaire développée par Cisco. De par sa conception, le protocole IGRP est doté, entre autres, des caractéristiques suivantes :

- Il s'agit d'un protocole de routage à vecteur de distance.
- La bande passante, la charge, le délai et la fiabilité sont utilisés pour créer une métrique composite.
- Par défaut, les mises à jour du routage sont diffusées toutes les 90 secondes [7].

1. Présentation du protocole EIGRP

EIGRP est un protocole de routage amélioré et propriétaire développé par Cisco dans le but d'améliorer le protocole IGRP et notamment le rendre plus stable. Ce protocole est donc uniquement compatible avec les produits Cisco. EIGRP utilise l'algorithme DUAL qui a été développé à SRI International [13].

Par rapport à l'IGRP, l'EIGRP offre une convergence plus rapide, une évolutivité améliorée et un traitement plus efficace des boucles de routage. L'absence de boucle dans le réseau est garantie par l'utilisation de l'algorithme DUAL.

A. Concepts et terminologie de l'EIGRP

L'EIGRP met à jour trois tables :

- **Table de voisinage** : est la table la plus importante de l'EIGRP, des voisins nouvellement découverts sont acquis, l'adresse et l'interface du voisin sont enregistrées. Ces informations sont stockées dans la structure de données de voisinage.
- **Table topologique** : est constituée de toutes les tables de routage EIGRP du système autonome. L'algorithme DUAL extrait les informations fournies dans la table de voisinage et dans la table topologique et calcule les routes de moindre coût vers chaque destination.
- **Table de routage** : contient les meilleures routes vers une destination donnée. Ces informations sont extraites de la table topologique. Chaque routeur EIGRP tient à jour une table de routage pour chaque protocole de réseau [7].

B. Technologie EIGRP

L'EIGRP inclut un bon nombre de nouvelles technologies, chacune représentant une amélioration sur le plan de l'efficacité d'exploitation, de la vitesse de convergence ou de la fonctionnalité par rapport à l'IGRP et aux autres protocoles de routage [7]. Ces technologies peuvent être classées dans l'une des catégories suivantes :

- Découverte et récupération de voisinage.
- Protocole de transport fiable.
- Algorithme de machine à états finis DUAL.
- Modules dépendant du protocole.

C. Algorithme DUAL

DUAL est le processus de décisions pour le calcul des routes, en les traçant selon les informations de ses voisins. DUAL utilise l'information de distance, de chemins sans boucles pour

insérer ces routes dans une table de routage basée sur les successeurs potentiels. Voici le principe de fonctionnement de l'algorithme DUAL :

Lorsque la topologie du réseau change, DUAL teste le réseau afin de trouver un éventuel successeur [14].

- S'il y a un successeur, DUAL l'utilise ce qui évite un recomptage complet de la route.
- S'il n'y a pas de successeur, un recomptage total de la route est alors effectué afin de trouver un successeur.

Comme le schéma suivant (Figure 2.8), pour atteindre le réseau 192.168.1.0, le routeur A essaye de trouver le meilleur chemin où le coût est le plus faible. Sur ce schéma, on ne peut avoir que deux chemins sans boucle, l'un passant par le routeur B et l'autre par le routeur D.

La particularité d'EIGRP est qu'il va stocker ces deux chemins en les différenciant, l'un est le chemin utilisé et l'autre le chemin potentiel.

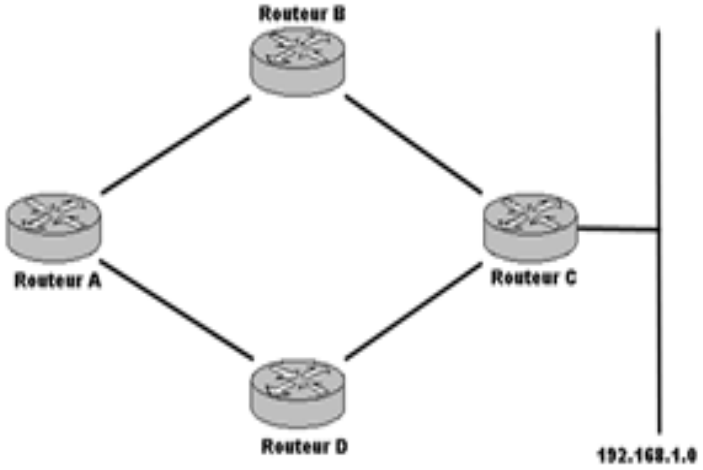

FIGURE 2.8 – Chois d'un chemin sans boucle.

D. Encapsulation EIGRP

La partie donnée d'un message EIGRP est encapsulée dans un paquet. Ce champ de données est nommé Type/Longueur/Valeur ou TLV. Comme indiqué dans la figure 2.9, les types de TLV sont les paramètres EIGRP, des routes IP internes et les routes IP externes.

L'en-tête de paquet EIGRP est inclus dans chaque paquet EIGRP, quel que soit son type. Dans l'en-tête de paquet IP, le champ protocole est défini à 88 pour indiquer EIGRP, et l'adresse de destination est définie à l'adresse multidiffusion 224.0.0.10 [15].

En-tête de trame liaison de données	En-tête paquet IP	En-tête paquet EIGRP	Type/Longueur/Type de Valeur

FIGURE 2.9 – Encapsulation de message EIGRP.

- **En-tête de trame liaison de données** : contient les adresses MAC source et destination.
- **En-tête paquet IP** : contient les adresses IP source et destination.
- **En-tête paquet EIGRP** : contient le numéro de systeme autonome.
- **Type/Longueur/Valeur** : partie données du message EIGRP.

E. Types de paquets avec EIGRP

EIGRP recourt à différents types de paquets pour mettre à jour ses différentes tables et établir des relations complexes avec les routeurs voisins [7]. Les cinq types de paquets EIGRP sont les suivants :

- **HELLO** : les paquets Hello sont utilisés par EIGRP pour découvrir des voisins et former des contiguïtés avec ces voisins. Les paquets Hello EIGRP sont de type multidiffusion et utilisent la livraison non fiable. Il y a un intervalle entre chaque paquet Hello et un délai d'attente et tous ça dépendent de la liaison utilisée.
- **Accusé de réception** : utilise des paquets d'accusé de réception pour indiquer la réception de n'importe quel paquet EIGRP au cours d'un échange fiable. Le RTP peut assurer une communication fiable entre des hôtes EIGRP. Pour être fiable, le message d'un émetteur doit faire l'objet d'un accusé de réception.
- **Mise à jour** : les paquets de mise sont utilisés lorsqu'un routeur découvre un nouveau voisin. Un routeur EIGRP envoie des paquets de mise à jour unicast à ce nouveau voisin afin de pouvoir l'ajouter à sa table topologique. Les paquets de mise à jour sont également utilisés lorsqu'un routeur détecte un changement topologique. Dans ce cas, le routeur EIGRP envoie un paquet de mise à jour multicast à tous les voisins, qui leur signale le changement. Tous les paquets de mise à jour sont envoyés de manière fiable.
- **Requête** : un routeur EIGRP utilise des paquets de requête chaque fois qu'il a besoin d'informations spécifiques sur un ou plusieurs de ses voisins.
- **Réponse** : est utilisé pour répondre à une requête.

F. Métrique

La métrique EIGRP est calculé à l'aide de cette formule :

$$\text{Métrique} = [\text{K1*bande passante} + (\text{K2*bande passante})/(256 - \text{charge}) + \text{K3*délai}] * [\text{K5}/\text{fiabilité} + \text{K4}]$$

Les différents paramètres de cette formule sont les suivants :

- K1 : coefficient rattaché à la bande passante (valeur par défaut = 1).
- K2 : coefficient rattaché à la charge (valeur par défaut = 0).
- K3 : coefficient rattaché au délai (valeur par défaut = 1).
- K4 : coefficient rattaché à la fiabilité (valeur par défaut = 0).
- K5 : coefficient rattaché au MTU (valeur par défaut = 0).

Ainsi, avec les valeurs par défaut, on arrive à la formule simplifiée suivante :

$$\text{Métrique} = [\text{K1*bande passante} + \text{K3*délai}].$$

2.4.1.2 Protocole de routage à état de liens (LS)

Le deuxième algorithme de base utilisé pour le routage est l'algorithme à état de liens, appelés aussi algorithme de Dijkstra ou algorithme SPF (plus court chemin d'abord). Un algorithme de routage à état de liens gère une base de connaissances complète sur les routeurs distants et leurs interconnexions. Par contre, les algorithmes à vecteur de distance comprennent des informations non spécifiques sur les réseaux distants et ne fournissent aucune information sur les routeurs distants comme nous avons définir précédemment.

Ces deux types de protocoles de routage ont pour but de trouver des routes parmi les systèmes autonomes. Les protocoles de vecteur de distance et d'état de liens utilisent des méthodes différentes pour accomplir les mêmes tâches [20].

A. Algorithme du routage à état de liens

L'algorithme de routage à état de liens est utilisé pour le calcul des tables de routage. Le but étant d'établir le chemin le plus court entre une source et sa destination, SPF fait la somme des coûts à partir de lui même (router root) vers tous les réseaux de destinations, s'il y a plusieurs chemins possibles vers une destination, c'est celle qui à le coût le plus faible qui est choisie [6] [16]. Cet algorithme à les caractéristiques suivantes :

- Élaboration d'une carte topologique totale du réseau.
- Convergence rapide.

- Mises à jour pilotées par événement.
- Métrique multiple.
- Conception hiérarchique.

B. Protocole OSPF

L'un des protocoles à état de liens les plus importants est l'OSPF, Il est spécifié dans différentes normes du groupe IETF [7].

Le protocole OSPF est non propriétaire, les caractéristiques clés de ce protocole sont les suivantes :

- Il s'agit d'un protocole de routage à état de liens.
- C'est un protocole de routage de norme ouverte décrit dans les requêtes pour commentaires RFC 2328.
- Il utilise l'algorithme SPF pour calculer le coût le plus bas vers une destination.
- Les mises à jour du routage sont diffusées à mesure des modifications de topologie.

C. Mode de fonctionnement

La table de routage est obtenue grâce à l'application de l'algorithme SPF sur une base d'information décrivant les liens qui unissent les routeurs d'une area.

Un lien est une interface de routeur et son état est la description de cette interface (l'adresse IP, masque, routeurs connectés, etc). Cette base est nommée Link State Database ou Topology Table, elle est identique à tous les routeurs de la zone. Au démarrage, un routeur doit se faire connaître des autres, il utilise le protocole HELLO, puis il génère un LSA représentant tous les états de liens de voisinage du routeur. Cet échange d'état de lien entre les routeurs se fait par inondation. Des mises à jour d'état de lien permettent de mettre à niveau tous les routeurs. Lorsque les bases de données sont synchronisées (identiques entre tous les routeurs de l'area), chaque routeur va calculer l'arbre du chemin le plus court en appliquant l'algorithme SPF. Il construira ainsi sa table de routage [16].

D. Message OSPF

OSPF utilise cinq différents types de messages à communiquer à la fois état de liens et informations générales entre les routeurs au sein d'un système ou d'une zone autonome :

- **En-tête de paquet OSPF** : lorsqu'un routeur lance un processus de routage OSPF sur une interface, il envoie un paquet HELLO qui est constitué de l'en-tête de paquet OSPF. Le champ type est défini à 1 pour le paquet hello, la figure 2.10 représente le format de cet entête [17] :

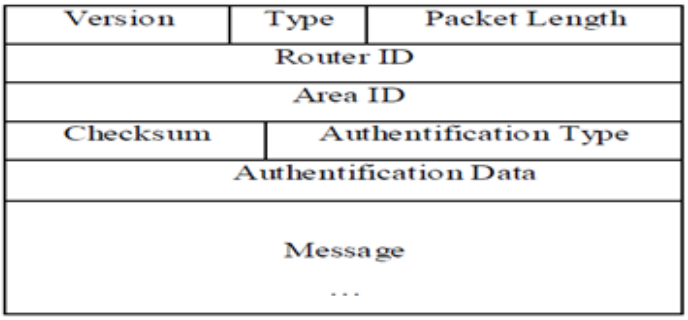

FIGURE 2.10 – Entête d'un paquet OSPF.

- **Paquet HELLO OSPF** : les paquets HELLO transportent des informations, le contenu transporté dans le paquet HELLO doit avoir fait l'objet d'un accord entre tous les voisins pour qu'une contiguïté soit formée et que les informations d'état de liens soient échangées, la figure 2.11 représente le format de cet paquet [17].

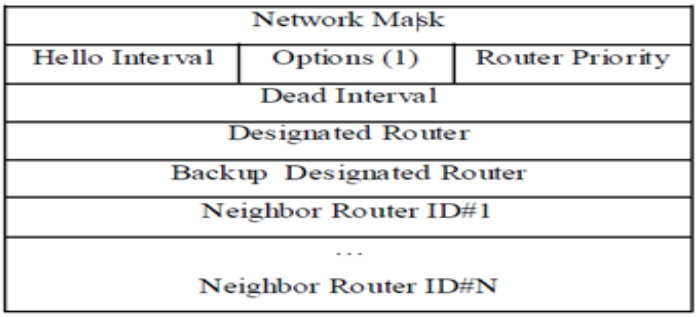

FIGURE 2.11 – Format du paquet Hello.

- **Paquet DataBase Description (DBD)** : il décrit le contenu de la base de données d'état de lien. Ces paquets sont utilisés dans la troisième étape du processus OSPF [17].
- **Paquet LSR (Requête d'état des liaisons)** : c'est le paquet qui permet d'interroger la base de données de l'état de lien [17].
- **Paquet LSU (Mise à jour d'état de liaisons)** : les paquets LSU sont utilisés pour répondre aux LSR, ainsi que pour annoncer de nouvelles informations [17].
- **Accusé de réception d'état des liaisons (LSAck)** : lors de la réception d'une LSU, le routeur envoie un LSAck pour confirmer la bonne réception de cette LSU [17].

E. Déroulement du processus OSPF

Quand un routeur démarre un processus de routage OSPF sur une interface, il envoie un paquet Hello et continue d'envoyer à intervalles réguliers. L'ensemble des règles qui gouvernent cet échange de paquets d'invite OSPF est appelé le protocole Hello. Dans les réseaux à accès multiples, le protocole Hello élit un routeur désigné DR et un routeur désigné de secours (BDR). Le protocole Hello transporte les informations de ceux des voisins qui acceptent de former une adjacence et d'échanger leurs informations d'état de liens. Dans un réseau à accès multiples le DR et le BDR maintiennent les relations d'adjacence avec tous les autres routeurs OSPF du réseau.

Les routeurs adjacents traversent une série d'états. Ils doivent être à l'état complet pour que les tables de routage soient crées et le trafic acheminé. Chaque routeur envoie des mises à jour de routage à état de liens (LSA) dans des paquets de mise à jour d'état de liens (LSU). Ces LSA décrivent toutes les liaisons du routeur. Chaque routeur qui reçoit une LSA de ses voisins l'enregistre dans la base de données d'état de liens. Ce processus est répété pour tous les routeurs du réseau OSPF.

Lorsque les bases de données sont complètes, chaque routeur utilise l'algorithme SPF pour calculer une topologie logique. Le chemin le plus court au coût le plus bas est utilisé dans la construction de cette topologie, ce qui fait que la meilleure route est sélectionnée.

Les informations de routage sont alors mises à jour. En cas de changement de l'état de lien, les routeurs utilisent un processus de diffusion pour avertir tous les autres routeurs du réseau du changement qui est survenu. L'intervalle d'arrêt du protocole HELLO constitue un mécanisme qui permet de déterminer qu'un voisin adjacent est défaillant [19].

F. Métrique OSPF

Par défaut, la bande passante est de 10 à la puissance 8, soit 10^8 bits/s. Les interfaces ayant une bande passante de 10^8 bits/s et plus ont un même coût OSPF de 1, mais la bande passante peut être modifiée pour s'adapter aux réseaux ayant des liaisons d'une rapidité supérieure à soit 10^8 bits/s.

En général, le coût attribuable aux liaisons est en fonction de la bande passante :

$$\text{Métrique} = (10^8 \text{ bits/s}) \ / \ (\text{Bandwidth bits/s}).$$

Par exemple pour 10 Mbit/s la métrique est 10.

2.4.1.3 Authentification

Les protocoles RIPv2, EIGRP, OSPF ainsi que d'autres peuvent tous être configurés afin de chiffrer et d'authentifier leurs informations de routage. L'authentification des informations

de routage transmises est une saine pratique. Elle garantit que les routeurs n'accepteront que les informations en provenance de routeurs aient été configurées avec le même mot de passe ou les mêmes informations d'authentification [15].

2.4.1.4 Tableau récapitulatif

Le Tableau 2.1 suivant montre une comparaison qui été faite selon plusieurs critères entre les trois protocoles étudiés en occurrence RIP, EIGRP et OSPF :

Protocole	RIP	EIGRP	OSPF
Type de protocole	Vecteur distance	Hybride	Etat de lien
Apprentissage de topologie de réseau	Rien	Table topologique limité	Table topologique complète
Mises à jour	Envoi complet de la table de routage à tous les voisins, chaque 30 secondes	- Par événement - Partielle et limitée	- Par événement - Partielle envoyée à tous les routeurs
Accusé de réception après mise à jour	Nom	Paquet ACK	Paquet LSAck
Convergence	Lente	Rapide	Rapide
Problème de boucle	Oui	Nom	Nom
Supporte VLSM	Nom	Oui	Oui
Supporte le routage hiérarchique	Nom	Oui	Oui
Supporte multiple protocoles	Nom	Oui	Nom
Distance Administrative	120	90	100
Métrique	Sauts	Bande passante, Délai Fiabilité, Charge	Bande passante
Autres	- Nombre de sauts maximum : 15 Utilise moins de Capacité et moins de mémoire	Propriété de CISCO - Utilise trois tables : Table des voisins, Table topologique, et table de routage. - Garde une route de secours pour chaque destination.	- Utilise le système de zones - complexe, demande plus de mémoire et plus de processeur

TABLE 2.1 – Comparaison entre RIP, EIGRP et OSPF.

2.4.2 Protocoles de routage externes EGP

Les protocoles EGP sont conçus pour échanger des informations de routage entre différents systèmes autonomes. Étant donné que chaque système autonome est géré par une administration différente et qu'il peut utiliser différents protocoles intérieurs [9].

Le but d'un tel protocole est de pouvoir propager (comme les protocoles de routages internes) des routes connues vers d'autres AS mais cela en pouvant appliquer des restrictions décidés par l'administrateur de chaque AS.

Parmi les protocoles de routage externes EGP sont :

- EGP.
- BGP.

2.4.2.1 Protocole de routage externe EGP

Le EGP est un protocole de routage externe, il est utilisé pour connecté des systèmes autonomes entre eux en échangeant les tables de routages entre les voisins quelque soit les protocoles IGP utiliser à l'intérieur des systeme autonomes [18].

2.4.2.2 Protocole de routage BGP

Le protocole BGP est un protocole de routage extérieur [7]. Les caractéristiques clés de ce protocole sont les suivantes :

- Il s'agit d'un protocole de routage extérieur à vecteur de distance.
- Il est utilisé pour la connexion entre les FAI ou entre les FAI et les clients.
- Il est utilisé pour acheminer le trafic Internet entre des systèmes autonomes.

2.5 Distance Administrative

La distance administrative est la caractéristique utilisée par les routeurs pour sélectionner le meilleur chemin lorsqu'il y'a deux ou plusieurs voies différentes vers la même destination à partir de deux différents protocoles de routage. Distance administrative définit la fiabilité d'un protocole de routage.

Les routeurs utilisent la distance administrative pour sélectionner le meilleur chemin lors de la découverte du même réseau de destination à partir d'au moins deux sources de routage différentes. C'est une valeur entière comprise entre 0 et 255. Plus la valeur est faible, plus la source de la route est privilégiée. Une distance administrative de 0 est idéale. Seul un réseau directement connecté a une distance administrative égale à 0, laquelle ne peut pas être modifiée [15], le tableau 2.2 représente les valeurs des distances administratives.

Source Route	Les valeurs par défaut à distance
Interface connectée	0
Route statique	1
EIGRP	5
BGP	20
EIGRP Interne	90
IGRP	100
OSPF	110
RIP	120
EGP	140
EIGRP Externe	170

TABLE 2.2 – Valeurs des distances administratives.

2.6 Equilibrage de charge

Chaque protocole de routage utilise une mesure pour déterminer la meilleure route d'accès à des réseaux distants. Si deux routes ou plus on les mêmes valeurs identique de la métrique vers la même destination, le routeur ne choisit pas une seule route. Il équilibre la charge entre ces chemins à coût égal. La transmission des paquets se fait via des chemins à coût égal. Tous les protocoles de routage qu'on a vu sont capables d'équilibrer automatiquement la charge du trafic pour quatre routes à coût égal maximum, par contre le protocole EIGRP est capable d'équilibrer la charge sur plusieurs chemins à coût inégal.

2.7 Conclusion

A travers ce chapitre nous avons défini les protocoles de routage dynamique pour l'acheminement des données à travers les réseaux informatiques, et nous avons vu leurs différentes classes. La diversité de ces protocoles de routage et leurs améliorations ont permet d'optimiser l'acheminement des paquets entre les nœuds du réseau, et comme nous avons aussi traité par la suite les différentes étapes de la mise en œuvre des protocoles RIP, EIGRP et OSPF, à travers un ensemble d'états et une multitude de paquets échangés entre les différents routeurs qui constituent le réseau.

CHAPITRE 3

SÉCURITÉ DES MISES À JOUR DES PROTOCOLES DE ROUTAGE

3.1 Introduction

La sécurité des réseaux informatiques est nécessaire pour protéger le réseau d'une entreprise et de se prémunir contre tout type d'attaque pouvant perturber le réseau.

Les protocoles de routage dynamique comme RIP, OSPF et EIGRP s'exposent à diverses attaques et n'implémentent pas de véritable couche de sécurité, ils doivent trouver le moyen d'interdire l'accès au réseau.

Pour cela des mécanismes de sécurité sont mis en place comme le filtrage de trafic de base, les contrôles spécifiques et le mécanisme d'authentification MD5 pour détecter et ignorer les messages hostiles et empêcher des messages non autorisés ou faux, provenant de sources non autorisées.

3.2 Services de sécurité

La sécurité s'appuie sur six concepts de base :

- **Disponibilité** : demande que l'information sur le système soit disponible aux personnes autorisées [21].
- **Intégrité** : garantir que les données ne puisse être modifiée, la fonction de hachage permet d'assurer l'intégrité et l'origine de message. L'algorithme de la fonction de hachage le plus connu est MD5 [22].
- **Confidentialité** : garantir que seules les personnes autorisées puissent accéder à la ressource. La confidentialité des échanges est assurée par le chiffrement [22].

- **Authentification** : c'est la propriété qui consiste à vérifier l'identité avant de donner l'accès à une ressource, elle repose sur le chiffrement des informations nécessaires à sa réalisation comme le mot de passe [22].
- **Non répudiation** : il faut que l'échange d'information entre deux entités ne puisse être modifié, une partie ne doit pas nier un échange qui a eu lieu avec une autre partie [22].
- **Contrôle d'accès** : le service de contrôle d'accès empêche l'utilisation non autorisée de ressources accessibles par le réseau [22].

3.3 Outils de sécurité

Pour faire face aux attaques possibles dans les réseaux informatiques, des outils de sécurité ont été utilisés pour la mise en œuvre des solutions de sécurité. Les outils les plus répandus sont :

3.3.1 Chiffrement

est assuré par des algorithmes de chiffrement utilisant une clé de chiffrement, Il existe deux types de chiffrement [23] :

- **Chiffrement symétrique** : appelé aussi chiffrement clé privée ou chiffrement à clé secrète consiste à utiliser la même clé pour le chiffrement que pour le déchiffrement. Il est donc nécessaire que les deux interlocuteurs se soient mis d'accord sur une clé privée [23].
- **Chiffrement asymétrique** : appelé aussi la cryptographie à clé publique, désigne une méthode cryptographique faisant intervenir une paire de clés asymétriques : une clé publique et une clé privée. il utilise cette paire de clés pour le chiffrement et le déchiffrement. La clé publique est rendue publique et distribuée librement. La clé privée n'est jamais distribuée et doit être gardée secrète [23].

3.3.2 Signature numérique

Une signature numérique est une empreinte d'un document chiffré par la clé privée de l'auteur, cette empreinte chiffrée étant jointe au document originel. La signature permet ainsi de vérifier l'intégrité du document et l'identité de l'expéditeur. On signe un document via des fonctions de hachage [23].

3.3.3 Certificat numérique

Est une structure de données qui est numériquement signée par une autorité de certification (CA). Il sert à assurer l'intégrité des clés publiques. Le CA utilise sa clé privée pour signer le

certificat et assure ainsi une sécurité supplémentaire. Si le récepteur connaît la clé publique du CA, il peut vérifier que le certificat provient vraiment de l'autorité concernée et assuré que le certificat contient donc des informations viables et une clé publique valide [23].

3.3.4 Fonction de hachage

Les fonctions de hachage [22], servent à calculer a partir d'une donnée de taille arbitraire fournie en entrée une empreinte de taille fixe. Cette taille varie en général entre 128 et 512 bits. Cette empreinte, appelée aussi condensé (hache) qui doit dépendre de tous les bits du message et elle est utilisée pour représenter le message de façon compacte .

Une fonction de hachage est un algorithme entièrement public et aucune valeur secrète n'intervient à aucun moment du calcul. Néanmoins, elle appartient à la famille des algorithmes symétriques. Une fonction de hachage doit se comporter idéalement comme une fonction aléatoire. En parallèle, de nombreuses propriétés doivent être respectées. En particulier, il difficile d'inverser la fonction.

Une fonction de hachage H est une fonction qui prend en entrée une donnée de taille aléatoire m, et donne en sortie un condensé de taille fixe n.

Il existe plusieurs algorithmes de cryptage disponibles, mais le MD5 (Message Digest algorithm 5) est un des plus couramment utilisé et le plus largement répandu, il a été créé par Ron Rivers en 1991 pour remplacer la fonction hash MD4. Le MD5 est plus lent que son prédécesseur mais il est plus conservateur et sécuritaire.

L'algorithme MD5 [22], prend comme paramètre un texte d'une longueur arbitraire et produit une empreinte de 128 bits du paramètre. De manière concrète, l'algorithme ne peut pas produire deux messages qui auraient la même empreinte. L'algorithme est prévu pour des applications où de gros fichiers doivent être compressés de manière sécurisée avant d'être cryptés avec une clé de sécurité privée à l'aide d'un système de cryptage à base de clé publique.

3.3.5 Liste de contrôle d'accès

Le mécanisme des listes de contrôle d'accès (ACL) utilise l'identité authentifiée des entités et des informations fiables pour déterminer leurs droits d'accès au réseau ou aux ressources sur le réseau [7].

3.4 Problèmes des protocoles de routage

L'objectif des protocoles de routage est de maintenir les tables de routage du réseau dans un état intègre et cohérent, mais qui n'ont pas été conçus d'une manière sécurisée. Éventuellement,

par le biais de diverses attaques, d'injecter, de modifier ou d'impacter d'une manière ou d'une autre un processus de routage.

Toute attaque ou perturbation du routage peut impacter directement la disponibilité du réseau et de ses services. Parmi les obstacles que rencontrent les protocoles de routage sont :

- **Boucles de routage** : les protocoles de routage ont des mécanismes pour assurer le cheminement sans boucles. Mais les mesures donnent des évidences que ces boucles existent parfois dans le transfert des paquets inter-domaine. La cause exacte de cet effet est peu claire. Il croit que le délai de propagation des messages de routage cause des moments où il y a des contradictions de routage entre les routeurs [25].
- **Croissance de la table de routage** : le nombre des préfixes (adresses de réseau) annoncés sur l'Internet augmente si rapidement cela provoque une surcharge dans la table de routage. Cela cause l'instabilité, rejeter les nouveaux chemins, interrompre les sessions d'échanges de route, ou redémarrer le routeur [25].
- **Mauvaises configurations** : les erreurs de configuration de routage peut perturber ou interrompre la connectivité d'Internet, ces dernières sont nombreuses. La mauvaise configuration est effectivement dangereuse car elle permet aux attaquants de causer à la fois le déni d'accès (blackholing) dans un réseau et le déni de service (DoS) dans un autre réseau [25].

1.1. Attaques visant RIP

Les attaques possibles pour RIP sont :

- **Insertion de fausse route pour rediriger le trafic ou empoisonner la table de routage** : l'attaquant qui connaît bien la topologie du réseau peut injecter des messages pour forcer un routeur à utiliser un chemin particulier afin de renifler les données. Il peut aussi empoisonner la table de routage par de fausses routes pour causer l'instabilité [25].
- **Déni de service DoS contre le port 520 UDP** : l'inondation du port 520 est possible lorsque l'attaquant veut interrompre les échanges de route entre les routeurs [25].

1.2. Attaques visant EIGRP

Une attaque de type déni de service a été découverte dans la gestion du protocole EIGRP sous les équipements Cisco IOS. Comme il implémente un mécanisme permettant aux routeurs de découvrir de manière dynamique ses routeurs voisins pour s'échanger les informations de leur table de routage. Pour cela, les routeurs doivent s'échanger dans un premier temps leur adresse physique, si ces échanger sont effectuées par un équipement malicieux avec des adresses IP forgées spoofing appartenant à la même classe et au même masque réseau que celle utilisée par

un routeur implémentant le protocole EIGRP, alors ce dernier tentera de résoudre ces adresses IP forgées en adresses MAC et saturera ainsi sa capacité mémoire.

1.3. Attaques visant OSPF

OSPF nécessite beaucoup de ressources pour effectuer les calculs de meilleur chemin. Cela permet à l'attaquant de causer l'instabilité en déclenchant périodiquement de faux changements.

Pour réduire les échanges de routage, OSPF propose une structure hiérarchique qui permet de choisir un routeur principal. L'attaquant peut exploiter ce mécanisme d'élection pour devenir le routeur principal et modifier les routes [25].

Les attaques possibles pour OSPF sont :

- **Tentatives pour être élu comme routeur principal** : l'attaquant peut établir un faux routeur de haute priorité et forcer les routeurs à réélire le routeur principal (par un DoS vers le routeur principal courant). Après avoir gagné l'élection, l'attaquant peut modifier les informations de routage comme ce qu'il veut [25].
- **Insertion de fausse route** : l'attaquant peut effectuer un DoS en mettant une grande valeur de séquence ou en envoyant de faux messages LSA qui forcent les routeurs OSPF à renvoyer des LSA afin de saturer les ressources. Il peut aussi injecter un faux chemin avec le numéro de séquence maximal, ce qui ne permet pas au routeur d'origine de ce chemin de corriger le problème [25].

3.5 Mécanismes de sécurité

Par défaut, un routeur s'attend à recevoir les informations de routage d'un autre routeur qui doit les lui envoyer, ces informations ne doivent pas être altérées en chemin.

A toutes ces attaques, il est nécessaire de propose des mécanismes qui peuvent remédier les attaques concernant les protocoles de routage :

3.5.1 Listes de contrôle d'accès

Les listes de contrôle d'accès sont des listes de conditions qui sont appliquées au trafic circulant via une interface de routeur. Ces listes indiquent au routeur les types de paquets à accepter ou à rejeter. Les ACL permettent de gérer le trafic et de sécuriser l'accès à un réseau en entrée comme en sortie d'un réseau [7].

Les principales raisons pour lesquelles il est nécessaire de créer des listes de contrôle d'accès sont [7] :

- Limiter le trafic réseau et accroître les performances.

- Contrôler le flux de trafic. Les ACL peuvent limiter l'arrivée des mises à jour de routage. Si aucune mise à jour n'est requise en raison des conditions du réseau, la bande passante est préservée.
- Fournir un niveau de sécurité d'accès réseau de base. Les listes de contrôle d'accès permettent à un hôte d'accéder à une section du réseau tout en empêchant un autre hôte d'avoir accès à la même section.
- Déterminer le type de trafic qui sera acheminé ou bloqué au niveau des interfaces de routeur.
- Autoriser un administrateur à contrôler les zones auxquelles un client peut accéder sur un réseau.
- Accorder ou refuser aux utilisateurs la permission d'accéder à certains types de fichiers, tels que FTP ou HTTP.

Au moment de configurer les listes de contrôle d'accès d'un routeur, chaque liste doit être identifiée par un numéro unique, ce numéro identifie le type de liste d'accès créé et doit être compris dans la plage de numéros valide pour ce type.

Il existe différents types de listes de contrôle d'accès [7] :

- **Listes de contrôle d'accès standard** : vérifient l'adresse d'origine des paquets IP qui sont routés. Selon le résultat de la comparaison, l'acheminement est autorisé ou refusé pour un ensemble de protocoles complet en fonction des adresses réseau, du sous-réseau et d'hôte.
- **Listes de contrôle d'accès étendues** : sont utilisées plus souvent que les listes d'accès standard car elles fournissent une plus grande gamme de contrôle. Elles vérifient les adresses d'origine et de destination du paquet, mais peuvent aussi vérifier les protocoles et les numéros de port. Cela donne une plus grande souplesse pour décrire ce que vérifie la liste de contrôle d'accès. L'accès d'un paquet peut être autorisé ou refusé selon son emplacement d'origine et sa destination, mais aussi selon son type de protocole et les adresses de ses ports.

3.6 Mécanismes de sécurité pour les protocoles de routage

Pour sécuriser les protocoles de routage RIPv2, EIGRP et OSPF, nous utilisons un contrôle basé sur le mot de passe et la fonction de hachage MD5 qui utilise une clé secrète associée à des données protégées pour calculer un hachage. Lorsque les protocoles envoient des messages, le hash calculé est transmis avec les données. Le récepteur utilise la clé correspondante pour valider la valeur de hachage du message [24].

3.6.1 Authentification RIP avec MD5

RIPv1 ne dispose pas d'un masque de sous-réseau à longueur variable (VLSM) et il ne propose pas non plus de prise en charge pour l'authentification du routeur, ce qui le rend vulnérable aux attaques. Par contre RIPv2 dispose d'un masque de sous-réseau et prend en charge la sécurité avec authentification MD5.

RIPv2 permet l'authentification dans ses mises à jour. Il est possible d'utiliser une combinaison de clés sur une interface comme vérification d'authentification. RIPv2 permet de choisir le type d'authentification à utiliser dans ses paquets. Il peut s'agir de texte en clair ou d'un cryptage basé sur l'algorithme d'authentification MD5. Le type d'authentification par défaut est le texte en clair. L'algorithme MD5 peut être utilisé pour authentifier la source d'une mise à jour de routage [30].

Le porte-clés détermine l'ensemble des touches qui peuvent être utilisées sur une interface. Si un porte-clés n'est pas configuré, l'authentification ne sera pas exécutée sur cette interface.

En général, quand une mise à jour de routage est envoyée, il se produira la séquence d'authentification suivante :

- Un routeur envoie une mise à jour de routage avec une clé et le numéro de clé correspondant au routeur voisin. Les protocoles qui peuvent avoir une seule touche, le numéro de la clé est toujours à zéro. Dans la réception, le routeur voisin vérifie la clé reçue avec la même clé qui est stockée dans une mémoire propre.
- Si les deux clés correspondent, le routeur destinataire accepte le paquet de mise à jour de routage. Sinon, le paquet est rejeté.

Authentification MD5 fonctionne de façon similaire à l'authentification en texte clair, sauf que la clé n'est jamais envoyé sur le fil. Au lieu de cela, le routeur utilise l'algorithme MD5 pour produire un "message digest" de la clé (Hash). Le résumé de message est alors envoyé à la place de la clé elle-même. Cela garantit que personne ne peut espionner sur la ligne et apprendre des clefs lors de la transmission.

Une autre forme d'authentification du routeur voisin consiste à configurer la gestion des clés en utilisant des porte-clés. Lorsqu'un porte-clés est configuré, une série de touches est spécifie avec des durées de vie, et le logiciel Cisco IOS tourne à travers chacune de ces touches. Cela diminue la probabilité que les clés seront compromises [26].

3.6.2 Authentification OSPF avec MD5

La clé d'authentification est utilisée par chaque interface OSPF à l'usage des routeurs qui, envoient des informations aux autres routeurs du segment. Cette clé est un secret partagé entre les routeurs. Elle permet de générer les données d'authentification dans l'en-tête de paquet

OSPF.

La configuration d'une authentification simple est le mot de passe qui est envoyé sous forme de texte en clair. Autrement dit il peut être déchiffré facilement si un paquet OSPF est capturé. Il est recommandé d'envoyer les informations d'authentification cryptées et aussi pour renforcer la sécurité en utilisant l'authentification MD5.

Le principe d'authentification MD5 consiste à crée un condensé de message, Ce dernier est composé de données brouillées qui sont basées sur le mot de passe et sur le contenu du paquet. Le routeur récepteur utilise le mot de passe partagé et le paquet pour recalculer le condensé de message via l'algorithme MD5. Si les résultats (condensés de message) de l'application des algorithmes MD5 correspondent, le routeur détermine que la source et le contenu du paquet n'ont pas été altérés. Dans le cas de l'authentification par algorithme MD5, le champ de données d'authentification contient l'identificateur de clé et la longueur du condensé de message qui est ajouté au paquet [27].

3.6.3 Authentification EIGRP avec MD5

EIGRP supporte l'authentification MD5 [28] pour empêcher l'introduction des messages non autorisés ou faux, provenant de sources non autorisées. L'authentification de voisin EIGRP (ou l'authentification des chemins) peut être configuré dans ces routeurs d'une manière à participer à l'acheminement sur la base de mots de passe prédéfinis. Par défaut, aucune authentification n'est utilisée pour les paquets EIGRP, une fois l'authentification MD5 a été configuré sur un routeur, ce dernier authentifie la source de chaque paquet de mise à jour de routage qu'il reçoit. Pour commencer à utiliser l'authentification MD5 pour le protocole EIGRP, on doit configurer à la fois une clé d'authentification et un identifiant de clé sur le routeur d'envoi et le routeur de réception. Chaque routeur EIGRP prend l'ID de clé et la clé et génère un message digest qui est rapporté à chaque mise a jour de routage et l'envoyé au voisin. Le routeur récepteur calcule le hash MD5 de l'information EIGRP reçu. Si la valeur de hachage correspond à la valeur reçue, le paquet est accepté sinon, le paquet sera retiré silencieusement.

Chaque clé a sa propre ID de clé, qui est localement stocké. La combinaison de l'ID de clé et l'interface sont associe avec le message qui uniquement identifie l'algorithme d'authentification et la clé d'authentification MD5 qui est en cours d'utilisation. L'utilisation des principaux changements fréquents peut augmenter la sécurité de l'authentification MD5 de EIGRP, la définition de plusieurs touches est prise en charge, qui peut être changé sur la base de temps qui est défini dans la configuration. La transition entre les touches est implémentée d'une manière qui permet l'échange sans interruption de mise jour de routage de EIGRP. Les changements de clé doivent être bien planifiés par la synchronisation de l'heure entre les routeurs [28].

Pour gérer les touches EIGRP en utilisant des porte-clés. Chaque définition de la clé dans

la chaine de clé peut spécifier une durée de vie pour quand cette touche est activée, pendant la durée de vie de clé donnée, les paquets de mise à jour sont envoyées avec cette touche activée. Un seul paquet d'authentification est envoyé, quel que soit le nombre de touches valides existent. Les clés de chiffrements sont examinées par le logiciel dans l'ordre du plus bas au plus élevé. Il utilise ensuite la première clé valide rencontrer. Si la clé n'est pas activée alors elle est inutile. Par conséquent, l'authentification du voisin ne peut pas se produire, et les mises à jour de routage échoueront [28].

3.7 Conclusion

Ce chapitre presente la sécurité des mises a jours des protocoles de routage RIP, OSPF et EIGRP, le long de ce chapitre nous avons décrit les services et les outils de sécurité, ensuite nous avons énuméré les problèmes lies au routage et les protocoles de routage ainsi que les attaques visant chacun de ces protocole. Dans le chapitre suivant nous allons définit les mécanismes de sécurité pour chaque protocole.

CHAPITRE 4

CONFIGURATION ET LA MISE EN ŒUVRE DE LA SÉCURITÉ

4.1 Introduction

Dans le but d'illustrer et de compléter ce qui a été traité dans la partie théorique de nôtre mémoire, plus exactement dans les chapitres 2 et 3, nous allons faire une simulation du réseau informatique de l'entreprise Cevital, en commençant par une étude de l'existant puis en configurant sur ce dernier les protocoles présentés dans le chapitre 2 et en appliquant la sécurité des mises a jours de routage sur ces protocoles .

Dans ce chapitre, nous allons présenter les logiciels utilisés et l'environnement de travail ainsi que les différentes configurations utilisées, enfin nous donnerons les résultats obtenus de la configuration.

4.2 Système d'exploitation pour l'interconnexion de réseaux (IOS)

IOS est l'architecture logicielle qui est incorporée dans tous les routeurs Cisco [7]. Ce système est muni d'une interface en ligne de commandes, propres aux équipements de Cisco Systems.

4.2.1 Rôle du système d'exploitation (IOS)

À l'instar d'un ordinateur, un routeur ou un commutateur ne peut pas fonctionner sans système d'exploitation, L'IOS est une technologie centrale qui s'étend pratiquement tous les produits Cisco. Son fonctionnement peut varier suivant les unités d'interconnexion de réseaux

sur lesquelles il est utilisé. L'IOS fournit les services réseau suivants [7] :

- Fonctions de routage et de commutation de base.
- Accès fiable et sécurisé aux ressources en réseau.
- Evolutivité du réseau.

Pour accéder aux services fournis par IOS, en utilisant généralement une interface de ligne de commande (ILC). Les fonctions accessibles à travers ILC varient selon la version de Cisco IOS et le type du périphérique [27].

4.2.2 Méthodes d'accès à Cisco IOS

Il y a plusieurs moyens d'accéder à l'environnement ILC. Les méthodes les plus répandues utilisent [27] :

- Le port de console permettant d'accéder à l'environnement ILC par une session console.
- Le protocole Telnet ou SSH qui permet un accès distant plus sécurisé aux périphériques.
- Le port AUX.

L'architecture suivante (Figure 4.1) représente les ports d'accès au routeur Cisco :

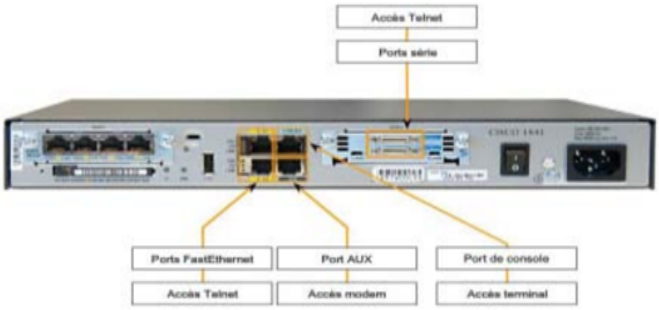

FIGURE 4.1 – Vue l'arrière du routeur Cisco.

4.2.3 Fichiers de configuration

Les périphériques réseau ont besoin de deux types de logiciels pour fonctionner : Le système d'exploitation comme celui d'un quelconque ordinateur, facilite l'exploitation de base des composants matériels du périphérique et les fichiers de configuration quant à eux, contiennent les commandes du logiciel Cisco IOS utilisées pour personnaliser les fonctionnalités d'un périphérique Cisco. Les commandes sont analysées (traduites et exécutées) par le logiciel Cisco IOS au démarrage du système (à partir d'un fichier appelé startup-config) ou lorsqu'elles sont entrées dans l'environnement ILC en mode configuration [27].

4.3 Configuration de base d'un routeur Cisco

La configuration de base d'un routeur Cisco se fait en général via la porte console. Ce dernier, sur un routeur, est configuré comme une interface DTE. Les lignes de configuration d'un routeur sont les suivantes (voir la figure 4.2) [27] :

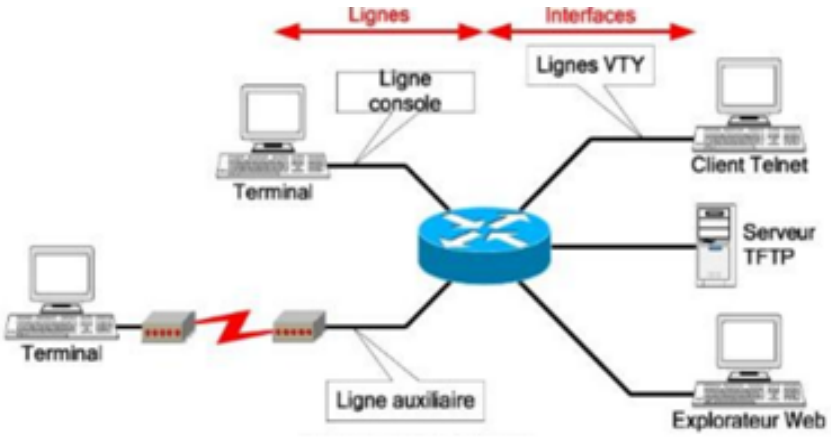

FIGURE 4.2 – Lignes configuration routeur.

Un routeur peut être configuré à partir des sources externes suivantes :

- **Ligne console** : accès primaire, à utiliser si aucun autre accès de configuration n'est disponible.
- **Ligne auxiliaire** : accès à distance via une liaison RTC et modems interposés.
- **Ligne(s) VTY** : accès via un client Telnet.
- **Explorateur Web** : accès utilisant le serveur HTTP interne du routeur.
- **Serveur TFTP et FTP** : import/export de fichiers de configuration.

4.3.1 Modes Cisco IOS

Les modes de l'environnement ILC sont organisés selon une structure hiérarchique, dans l'ordre de haut en bas, les principaux modes sont les suivants [27] :

- Mode d'exécution utilisateur permet de consulter toutes les informations liées au routeur sans pouvoir les modifier. Le shell est le suivant : **Router**>
- Mode d'exécution privilégié permet de visualiser l'état du routeur et d'importer/exporter des images d'IOS. Le shell est le suivant : **Router**#
- Mode de configuration globale permet d'utiliser les commandes de configuration générales du routeur. Le shell est le suivant : **Router(config)**#
- Mode de configuration d'interfaces permet d'utiliser des commandes de configuration des interfaces (Adresses IP, masque, etc.). Le shell est le suivant : **Router(config-if)**#

- Mode de configuration de ligne permet de configurer une ligne (exemple : accès au routeur par Telnet). Le shell est le suivant : **Router(config-line)#**
- Mode spécial RXBoot Mode de maintenance qui peut servir, notamment, à réinitialiser les mots de passe du routeur. Le shell est le suivant : **rommon>**

4.3.2 Configuration du nom d'hôte IOS

Pour configurer un nom d'hôte IOS en utilisant les commandes suivantes [27] :

Router#configure terminal : pour accéder au mode de configuration globale.
Router(config)#hostname r1 : pour entrer le nom d'hôte.
r1(config)#exit : pour quitter le mode de configuration globale.

4.3.3 Limitation de l'accès aux périphériques avec les mots de passe

Les mots de passe présentés ici sont les suivants [27] :

- Pour limiter l'accès au périphérique par une connexion console on utilise un mot de passe de console :

  r1(config)#line console 0
  r1(config-line)#password mot_de_passe
  r1(config-line)#login

- Application d'un mot de passe à l'accès Privilégié, Il faut tout d'abord, se connecter en mode privilégié, puis en mode de configuration globale, ensuite il suffit de taper une seule commande pour appliquer un mot de passe :

  r1(config)#enable password mot_de_passe

Il est recommandé d'enregistrer régulièrement la configuration à l'aide de la commande suivante (à effectuer en mode privilégié) :

r1#Copy running-config startup-config

Mot de passe **enable secret** chiffré, limite l'accès au mode d'exécution privilégié :

r1(config)#enable secret 123

4.3.4 Configuration de l'accès Telnet au routeur

La configuration avec le câble console et HyperTerminal n'étant pas très pratique, il est possible d'autoriser les administrateurs à se connecter au routeur via une session Telnet à partir de n'importe quel poste des deux réseaux [27].

Passez d'abord en mode de configuration globale, puis en mode de configuration de ligne VTY :

r1(config)#line vty 0 4

Cette dernière va configurer la possibilité de 5 sessions telnet simultanées sur ce routeur. Pour activer le Telnet, il suffit juste d'appliquer un mot de passe à la ligne :

r1(config-line)#password mot_de_passe
r1(config-line)#login
r1(config-line)#exit

4.3.5 Commandes IOS de base

Les différentes commandes IOS de base sont :

- **Passage entre les différentes modes d'utilisateurs**

Utilisateur normal : Aucune commande à effectuer, c'est dans ce mode que commence une session. Utilisateur privilégié (à effectuer à partir du mode normal) :

r1>enable :pour acceder en mode privilégié.
r1#configure terminal : est le mode de configuration globale.
r1(config)#interface nom_interface : pour acceder en mode de configuration d'interface.
r1(config)#line nom_de_la_ligne : est le mode de configuration de ligne.

- **Commandes d'information**

Les commandes d'information permettent d'afficher les informations relatives au routeur. Elles commencent toutes avec le préfixe show. Elles sont, pour la plupart, à effectuer à partir du mode privilégié.

r1#show running-config : afficher le fichier de configuration courante du routeur.
r1#show version : afficher les informations sur la configuration matérielle du système et sur l'IOS.
r1#show processes : afficher les processus actifs.
r1#show protocols : afficher les protocoles configurés de couche 3 du modèle OSI.
r1#show memory : afficher les statistiques de mémoire du routeur.
r1#show interfaces nom_interface : afficher des information et statistiques sur une interface.
r1#sh ip route : afficher la table de routage IP.

- **Commandes d'interface**

Ces commandes sont liées à la configuration des interfaces du routeur. Elles sont, pour la plupart, à effectuer à partir du mode de configuration d'interface.

r1(conf-if)#ip address @IP masque : attribution d'une adresse IP à une interface.

r1(conf-if)#no shutdown : Activation de l'interface.

- **Commandes d'enregistrement de la configuration courante**

Ces commandes permettent de sauvegarder la configuration actuelle pour la réappliquer automatiquement en cas de redémarrage du routeur. Elles s'exécutent en mode Privilégié.

r1#Copy running-config startup-config : sauvegarde avec demande de confirmation.

r1#write : sauvegarde sans demande de confirmation.

- **Commandes d'annulation**

Cette commande permet de revenir à la dernière configuration enregistrée, annulant toutes les modifications ayant été faites à la configuration depuis. Elle s'exécute en mode privilégié :

r1#copy startup-config running-config

- **Annulation d'une commande particulière**

Pour annuler une commande particulière, on utilisera le préfix no devant la commande précédemment exécutée.

r1(config-if)#no ip address : pour annuler la configuration d'une interface.

- **Commande de route statique**

r1(config)#ip route adresse_réseau_distant masque_de_réseau @ IP du_routeur_de_saut_suivan : permet de configurer une route statique.

r1(config)#ip route 0.0.0.0 0.0.0.0 @ IP du_routeur_de_saut_suivan : pour créer une route statique par défaut.

4.4 Commande de configuration des protocoles de routage dynamique

Pour configurer les protocoles de routage, en utilisant les commandes suivants :

4.4.1 Configuration de RIP v2

Les commandes liées à la configuration du protocole RIP sont :

r1(config)#router rip : permet d'activer le protocole RIP.

r1(config-router)#version 2 : est la version de RIP.

r1(config-router)#network {adresse réseau} : une fois le protocole rip est activé on peut déclarer les réseaux directement connectés.

r1(config)#no router rip : pour désactiver rip.

- **Dépannage de RIP v2**

Pour vérifie que les routes reçues par les voisins RIP sont installées dans une table de routage on utilise les commandes suivant :

r1#Show ip protocols : affiche les valeurs des protocoles de routage et les informations relatives aux compteurs de routage associées à ce routeur.

r1#show ip route : pour vérifie que les routes reçues par les voisins RIP sont installées dans une table de routage.

r1#Debug ip rip : permet d'afficher les mises à jour de routage RIP lors de leur envoi et de leur réception.

r1#No debug all : pour désactiver toutes les opérations de débogage.

Pour empêcher les transmissions des mises à jour RIP sur une interface précise en utilisant cette commande :

r1(config-router)#passive-interface interface-type interface-connectée : cette commande arrête les mises à jour de routage via l'interface spécifiée.

r1(config)#no auto-summary : pour désactive le résumé automatique.

Une fois le résumé automatique désactivé, RIPv2 ne résume plus les réseaux dans leur adresse par classe au niveau des routeurs.

4.4.2 Configuration de protocole EIGRP

Les commandes pouvant être utilisées pour la configuration du protocole EGRP sont les suivantes :

r1(config)#router eigrp numéro-du-système-autonome : pour activer le protocole EIGRP.

Le paramètre système-autonome est un nombre entre 1 et 65 535 choisi par l'administrateur réseau. Ce nombre est le numéro d'ID de processus (du système autonome), et il est important car tous les routeurs situés sur ce domaine de routage EIGRP doivent utiliser le même numéro d'ID de processus (numéro de système-autonome).

r1(config-router)#network numéro-réseau : toute interface sur ce routeur qui correspond à l'adresse réseau dans la commande network est activée pour envoyer et recevoir des mises à jour EIGRP. Ce réseau (ou sous-réseau) sera inclus dans les mises à jour de routage EIGRP.

r1(config-router)#network adresse_du_réseaux masque_générique : pour configurer EIGRP afin d'annoncer des sous-réseaux spécifiques uniquement on rajoute le masque générique à la commande.
r1#show ip eigrp neighbors : pour visualiser la table de voisinage.

- **Modifier la valeur de la bande passante**

Les commandes utilisées pour modifier la bande passante sont les suivantes :

r1(config-if)#bandwitch 1024 : la bande passante de la liaison entre deux routeurs est de 1024 Kbits/s, a condition que les routeurs devra être paramétrer de la même façon.

Par défaut, EIGRP n'utilise que jusqu'à 50% de la bande passante d'une interface pour les données EIGRP. Cela permet au processus EIGRP de ne pas surcharger une liaison en ne laissant pas suffisamment de bande passante pour le routage du trafic normal.

r1(config-if)#ip bandwidth-percent eigrp sn 50 : est utilisée pour configurer le pourcentage de bande passante pouvant être utilisé par le protocole EIGRP sur une interface.
r1(config-if)#no bandwitch : pour restaurer la valeur par défaut.

- **Vérifier tous les chemins possibles vers un réseau**

R1#show ip eigrp topology all-links : montre tous les chemins possibles vers un réseau, notamment les successeurs, les successeurs potentiels et même les routes qui ne sont pas des successeurs potentiels.

- **Désactive le résumé automatique**

r1(config-router)#no auto-summary : pour désactive le résumé automatique.

- **Configurer le résumé manuel**

Il faut d'abord sélectionner une interface qui transmet des paquets EIGRP. Puis on utilise la commande :

r1(config-if)#ip summary-address eigrp sn @réseaux masque_réseaux : configure le résumé du routage sur toutes les interfaces qui transmettent des paquets EIGRP, donc il faut le faire sur chaque interface utilisé.

- **Mettre en place une route par défaut**

r1(config)#ip route 0.0.0.0 0.0.0.0 interface_de_sortie : pour créer une route statique par défaut.
r1(config-router)#redistribute static : pour inclure cette route statique par défaut dans les mises à jour de routage EIGRP.

- **Configurer les intervalles Hello et le temps d'attente**

  r1(config-if)#ip hello-interval eigrp sn 60 : pour créer une route statique par défaut.

  r1(config-if)#ip hold-time eigrp sn 180 : si l'intervalle Hello est modifie, le temps d'attente doit être également modifie en lui attribuant une valeur supérieure ou égale à celle de l'intervalle Hello. Ici 180 secondes.

4.4.3 Configuration de protocole OSPF

Les commandes utilisées pour la configuration du protocole OSPF sont :

r1(config)#router ospf {id-processus} : pour activer le routage OSPF.

r1(config-router)#network {@_IP_du_réseau} {masque_générique} area {id_zone} : pour indiquer les réseaux IP, le paramètre area indique le numéro de la zone.

- **Configuration d'une adresse d'essai en mode bouclé OSPF**

  Pour créer et affecter une adresse IP à une interface en mode bouclé :

  r1(config)#interface loopback {numéro} : pour garantir la stabilité de l'OSPF, une interface doit être active en permanence pour le processus. À cet effet, en configurant une interface en mode bouclé (ou une interface logique).

  r1(config-if)#ip address {adresse_ip} {masque_sous-réseau} : OSPF utilise alors cette adresse comme ID de routeur, quelle que soit sa valeur sur un routeur possédant plusieurs interfaces en mode bouclé, l'OSPF choisit l'adresse IP en mode bouclé la plus élevée comme ID de routeur.

- **Vérifier le protocole OSPF**

  r1#show ip ospf neighbors : elle est utilisée pour visualiser la table de voisinage et vérifier que OSPF a établi une contiguïté avec ses voisins.

  r1#show ip ospf : peut être utilisée pour examiner l'ID de routeur et l'ID de processus (numéro du système) OSPF. En outre, cette commande affiche les informations de zone OSPF, ainsi que la dernière fois où l'algorithme SPF a été calculé.

  r1#show ip ospf interface : la méthode la plus rapide pour vérifier les intervalles Hello et Dead est d'utiliser la commande show ip ospf interface.

- **Adapter la bande passante OSPF**

  r1(config-if)#auto-cost reference-bandwidth : permet à la bande passante de référence d'être modifiée pour s'adapter aux réseaux ayant des liaisons d'une rapidité supérieure à 100 000 000 bits/s (100 Mbits/s).

Bande passante pour liaisons plus rapide est :

r1(config-router)#auto-cost reference-bandwidth 10000 : la bande passante de référence peut être modifiée pour prendre en compte ces liaisons plus rapides, grâce à la commande OSPF auto-cost reference-bandwidth. Pour que la mesure de routage OSPF reste cohérente, il faut utiliser cette commande sur tous les routeurs.

- **Modifier le coût de liaison**

  r1(config-if)#bandwitch 1024 : la bande passante de la liaison entre deux routeur est de 1024 Kbits/s, a condition que les routeurs devra être paramétrer de la même façon.

- **Contrôler le choix du routeur désigné et de secours**

  r1(config-if)#ip ospf priority 200 : la valeur de priorité par défaut était de 1 pour toutes les interfaces de routeur. C'était donc l'ID de routeur qui déterminait le DR et le BDR. Mais si vous remplacez la valeur par défaut 1, par une valeur plus élevée, le routeur dont la priorité est la plus élevée devient le DR, et celui qui a la seconde priorité devient le BDR.
  r1(config-router)#default-information originate : comme RIP, OSPF nécessite la commande default-information originate pour annoncer la route statique par défaut 0.0.0.0/0 aux autres routeurs de la zone. Si cette commande n'est pas utilisée, la route par défaut (quatre zéros) ne sera pas diffusée aux autres routeurs de la zone OSPF.

- **Configurer les intervalles Hello et DEAD**

  r1(config-if)#ip ospf hello-interval 5 : modifie l'interval Hello, ici 60 secondes. Le fait de modifier de façon explicite le minuteur est une saine pratique, plutôt que de compter sur une fonction automatique d'IOS.
  r1(config-if)#ip ospf dead-interval 20 : après 20 secondes, le compte à rebours du minuteur Dead de R1 se termine. La contiguïté entre R1 et R2 est perdue.

4.5 Configuration d'authentification MD5

Une fois notre configuration de base terminée, en commençant à mettre en place l'authentification MD5. Pour RIP, EIGRP, OSPF pour renforcer la sécurité des mises à jour de routage :

4.5.1 Configuration d'authentification MD5 pour RIP

Pour configurer l'authentification RIPv2 entre deux routeurs en suivant ces étapes :

Etape 1 : Définir un porte-clés avec un nom

r1(config)#key chain rip_chain : permet d'identifier un groupe de clef d'authentification.

Etape 2 : Creation de la clé

r1(config-keychain)#key 1 : permet de créer une clef dans un groupe de clef. L'identifiant de clef peut prendre une valeur de 0 à 2147483647.

Etape 3 : Indiquez le mot de passe au porte-clés

r1(config-keychain-key)#key_string mot de passe : permet de définir un mot de passe pour une clef.
r1(config-keychain-key)#exit : quitter le mode de configuration de la clé.
r1(config-keychain)#exit : quitter le mode de configuration de porte clé.

Etape 3 : Activer l'authentification sur l'interface et spécifier la chaîne de clé à utiliser

r1(config)#interface nom_interface : spécifier l'interface pour configurer l'authentification des messages sur RIP.
r1(config-if)#ip rip authentication key chain rip_chain : active l'authentification RIP sur une interface.
r1(config-if)#ip rip authentication mode MD5 : Configure l'interface pour utiliser l'authentification MD5.
r1(config)#exit : quitter le mode de configuration d'interface.
r1#exit : quitter le mode de configuration globale.

4.5.2 Configuration d'authentification MD5 pour EIGRP

L'authentification des messages EIGRP se compose de plusieurs étapes :

Etape 1 : Création d'un porte-clés et la clé

r1(config)#key chain eigrp_chain : permet de créer des clés.
r1(config-keychain)#key 1 : en mode de configuration des porte-clés, identifier le numéro de clé.
r1(config-keychain-key)#key_string cisco : en mode de configuration de la

clé de porte-clés, identifier la chaîne de clé.
r1#exit : quitter le mode de configuration de la clé.
r1#exit : quitter le mode de configuration de porte clé.

Pour vérifier que les clés sont bien présentées sur le routeur ainsi que leur durée de vie, on utilisant la commande suivante :

r1#show key chain

Etape 2 : Configuration de l'authentification EIGRP d'utiliser ce porte-clés et clé

Une fois un porte-clés et la clé sont crée, en pouvant configurer EIGRP pour effectuer l'authentification du message avec la clé :

r1(config)#interface nom_interface : configurer un type d'interface et accéder à l'interface mode de configuration.
r1(config-if)#ip authentication mode EIGRP 100 md5 : activer l'authentification MD5 dans des paquets EIGRP sur les interfaces des routeurs.
r1(config-if)#ip authentication key chain eigrp 100 eigrp_chain : activer l'authentification des paquets EIGRP.
r1(config-if)#exit : quitter le mode de configuration d'interface.
r1#exit : quitter le mode de configuration globale.
Copy running-config startup-config : pour enregistrer la configuration.

4.5.3 Configuration d'authentification MD5 pour OSPF

Les commandes utilisées pour configurer l'authentification MD5 sont :

r1(config)#interface nom_interface : spécifier l'interface pour configurer l'authentification des messages sur OSPF.
r1(config-if)#ip ospf message_digest_key 1 MD5 cisco : activè l'authentification MD5 pour OSPF.
r1(config-if)#exit : quitter le mode de configuration d'interface.
r1(config)#router ospf 100 : activer le protocole OSPF.
r1(config-router)#area 0 authentication message_digest : activer l'authentification MD5 pour une zone OSPF.
r1(config-router)#exit : désactiver le protocole OSPF. **r1#exit** : quitter le mode de configuration globale.

- **Commandes show associées**

  r1#show ip ospf interface : permet d'afficher la priorité de l'interface.
  r1#show ip protocols : affiche les informations sur les protocoles de routage configurés sur le routeur.
  r1#show ip route : affiche la table de routage du routeur.
  r1#show ip ospf : affiche la durée pendant laquelle le protocole est activé, ainsi que la durée durant laquelle il n'y a pas eu de modification topologique.
  r1#show ip ospf neighbor detail : affiche une liste détaillée des voisins, leur priorité et leur statut.
  r1#show ip ospf database : affiche le contenu de la base de données topologique (router-Id, process-Id).

4.6 Présentation des logiciels utilisés

Cisco propose des outils de simulation des réseaux et capture de trafique, nommé le Packet Tracer, Wireshark et GNS3

4.6.1 Présentation de GNS3

Pour ce travail on a choisi GNS3 comme le logiciel de simulation, pour simuler une topologie sur laquelle on va implémenter les protocoles de routage dynamique et la sécurité des mises à jour qu'on a étudié dans les chapitre 2 et 3 respectivement.

Ce logiciel (GNS3) définit comme un simulateur de réseau graphique, il s'agit plutôt d'une interface qui facilite la mise en œuvre de Dynamips, logiciel qui permet d'émuler des machines virtuelles Cisco [22]. Il est nécessaire d'insister sur le terme émulation, dans la mesure où ces machines s'appuient sur les véritables IOS fournis par Cisco et leur confèrent donc l'intégralité des fonctionnalités originales. Les performances des machines ainsi créer ne sont bien entendu pas équivalentes à celles des machines physiques réelles, mais elles restent amplement suffisantes pour mettre en œuvre des configurations relativement basiques et appréhender les concepts de base des équipements Cisco.

4.6.1.1 Téléchargement et installation de GNS3

On peut télécharger gns3 dans le site officiel de gns3 (http ://www.gns3.net) dans la rebique download, on trouve plusieurs versions, la version 32bits et 64 bits sur plusieurs plateforme (Windows, linux et Mac). Nous avons choisi la version 32 bits de Windows. Une fois télécharge, on passe directement a l'installation on double cliquons sur l'exécutable gns3. L'assistant de

configuration GNS3 va commencer après tout le reste est une question de cliquer sur des boutons suivant ou accord. Une fois l'installation termine on passe à la configuration de gns3.

4.6.1.2 Interface GNS3

Le logiciel gns3 a une interface simple (Voir la figure 4.3), elle se décompose en trois parties. La parité gauche c'est la partie ou on trouve les types de nœuds qu'on peut utiliser (routeur, Switch, etc.), la partie droit, la partie topologie ou il affiche les nœuds et les interfaces qui sont connecté. La partie au milieu, c'est la partie ou en voie l'ensemble de notre topologie (les nœuds, les liaisons et host utilisé).

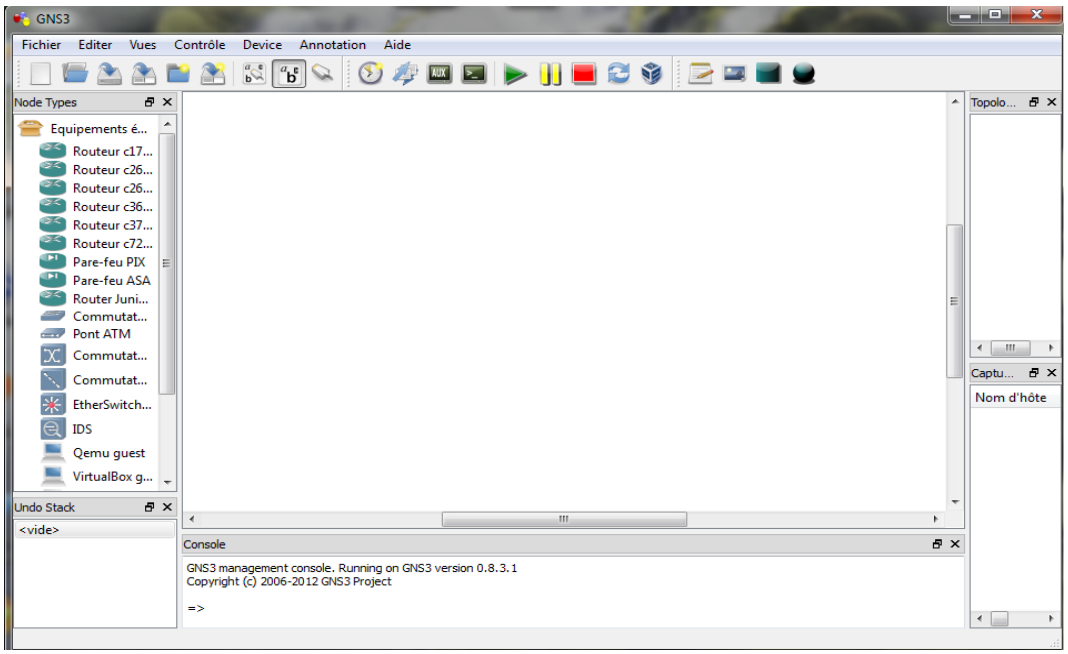

FIGURE 4.3 – Interface graphique de gns3.

4.6.1.3 Définir les Image IOS

Gns3 c'est un logiciel de simulation qui utilise les IOS des routeurs Cisco, alors avant tout implémentation il faut intégrer les IOS Cisco dans le logiciel. Dans le menu Edition, choisissez (Image IOS et hyperviseurs). Puis, sous l'onglet Images IOS (voir la figure 4.4), cliquez sur le bouton "..." et puis trouver votre Cisco IOS fichier et cliquez sur "Ouvrir". Le fichier apparaît sous la forme de votre fichier image. Ensuite, cliquez sur la flèche déroulante à côté de la plate-forme et choisissez la plate-forme qui correspond à votre fichier IOS.

Une fois les images IOS on été inclus, on peut commencé à implémenté les topologies qu'on veut.

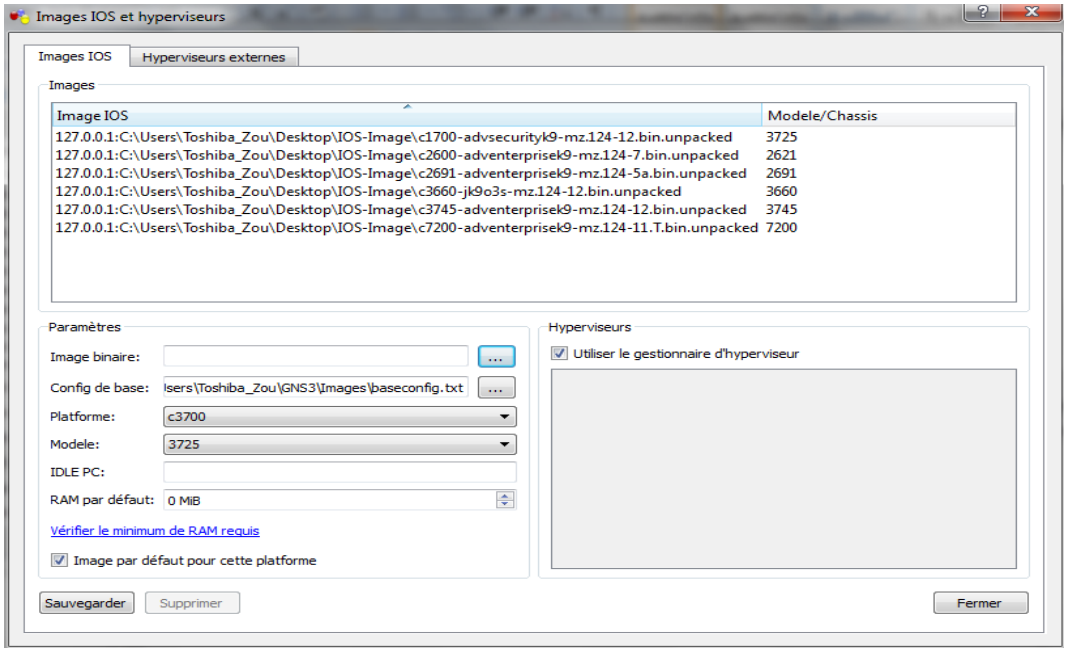

FIGURE 4.4 – Boite de dialogue Image IOS et hyperviseurs du menu Editer.

4.7 Cas d'étude

Nôtre cas d'étude se porte sur la configuration d'un réseau national du groupe Cevital, qui est en constante extension d'où l'intérêt d'y d'appliquer les mécanismes d'authentification MD5 sur les protocoles de routage dynamiques qui est le but de nôtre travail. Ce réseau s'étend actuellement sur six principaux pôles à savoir : Bejaia, Alger, Oran, Bouira, El Kseur (Cojek) et Tizi Ouzou (Lalla Khedidja), en plus des connexions à internet via des FAI, comme le montre la figure 4.5 :

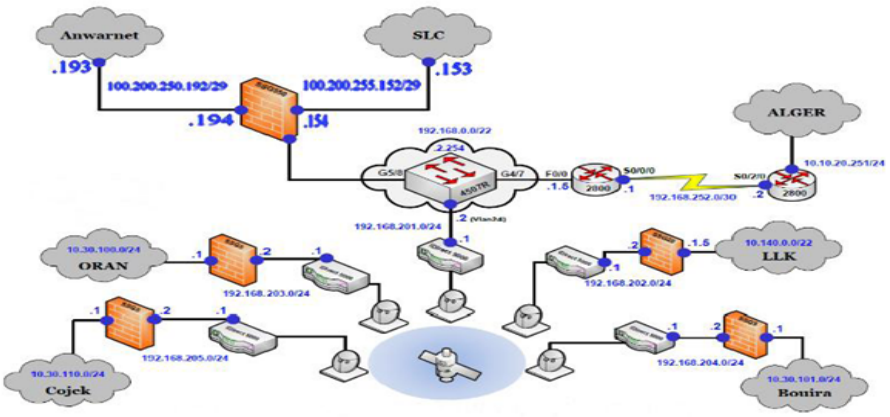

FIGURE 4.5 – Topologie réel du réseau Cevital.

Pour les besoins de la simulation, et pour des raisons de moyens, nous avons choisi de remplacer les liaisons V-SAT ainsi que les différents firewalls par des routeurs Firewall, et les réseaux locaux par des LoopBacks, et les Switchs par des switchs niveau trois avec un IOS d'un routeur pour pouvoir les configurer en y créant des Vlans, et tous ça en respectant les liaisons entre les pôles et leurs adresses réseau respectives. Et nous avons obtenus la topologie suivante (voire la figure 4.6) sur laquelle nous allons implémenter les différents protocoles étudiés précédemment ainsi que leur authentification md5.

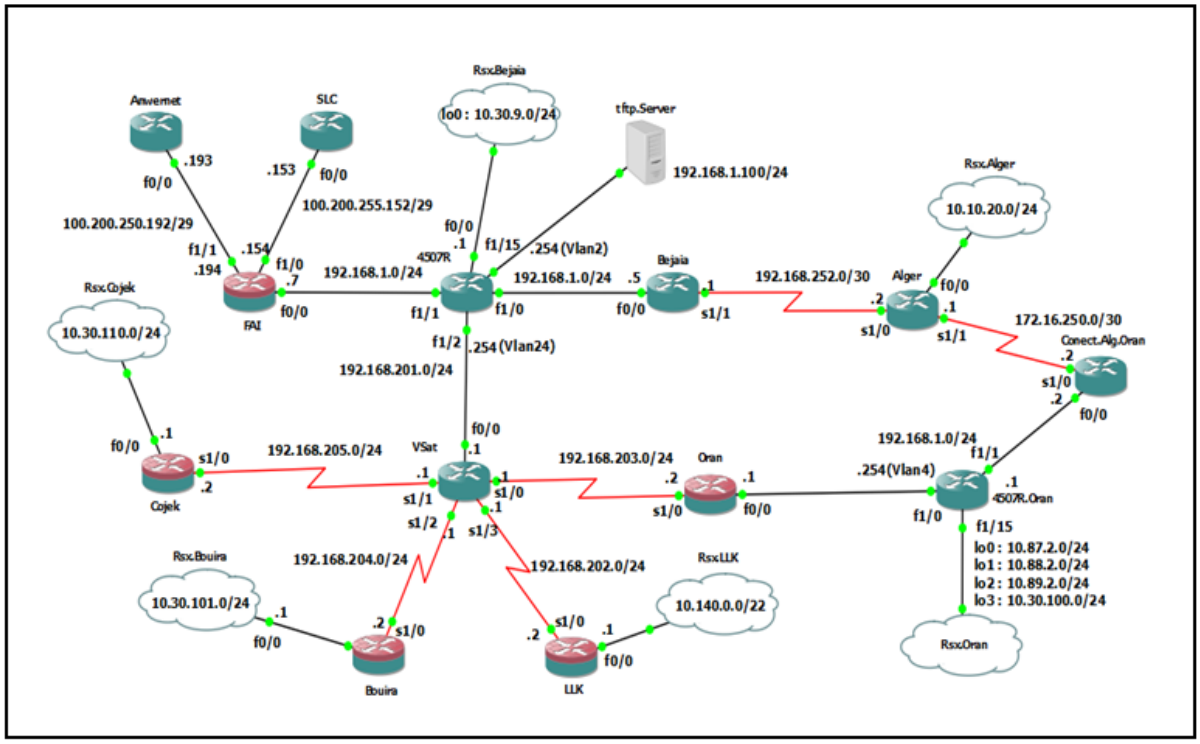

FIGURE 4.6 – Topologie du réseau Cevital sur GNS3.

4.7.1 Configuration existante

La topologie du réseau Cevital dans le cas existant est configuré réellement sur le terrain par le protocole EIGRP et des routes statiques suivant les commandes vues plus haut, les routes statiques ont été configurées sur le Switch 4507R vers les réseaux suivants :

- 10.10.20.0 via 192.168.1.5
- 10.30.100.0
- 10.30.101.0
- 10.30.110.0
- 10.140.0.0 via 192.168.201.1
- 192.168.202.0

– 192.168.203.0
– 192.168.204.0
– 192.168.205.0

Et une route par défaut vers 192.168.1.7 du 4507R et du routeur de Bejaia. Puis des routes statiques aussi à partir de Bejaia vers les réseaux :

– 10.10.20.0
– 10.87.2.0
– 10.88.2.0 via 192.168.252.2
– 10.89.2.0

Puis d'Alger, d'Oran et de Bejaia vers les réseaux suivants

– 10.30.9.0
– 172.16.250.0

Après les routes statiques, chaque routeur de la topologie a été configurée avec le protocole EIGRP suivant les commandes vues précédemment, et attribuant à chacun les adresses réseaux auxquelles il est connecté.

Pour vérifier la connectivité des équipements en affichant la table de routage à l'aide de la commande *#show ip route* (voir la figure 4.7).

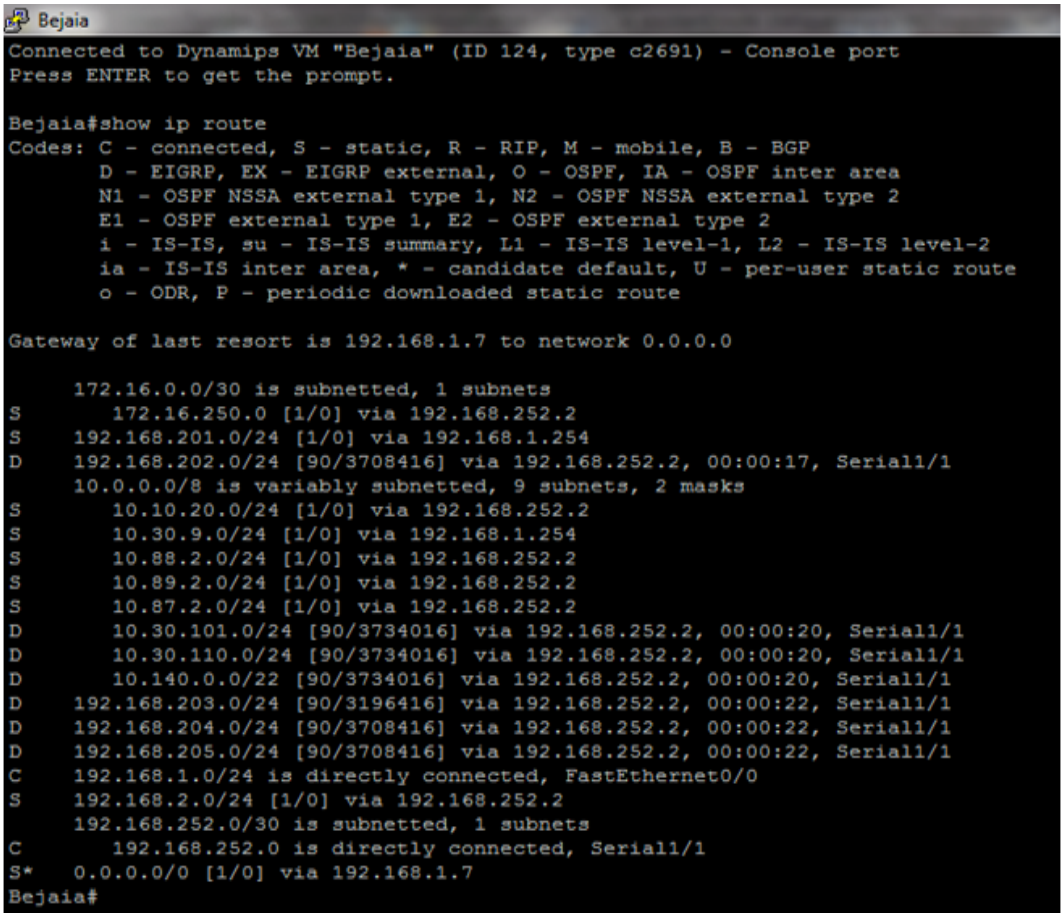

FIGURE 4.7 – Table de routage du routeur Bejaia (Cas Existant).

4.7.2 Configuration avec RIP

D'après les commandes vues précédemment concernant le protocole RIP avec la version 2, on va configurer chaque routeur et Switch respectant les adresses réseaux auxquelles il est connecté.

Une fois la configuration terminée, on peut vérifier la connectivité des équipements en affichant la table de routage à l'aide de la commande *#show ip route* (voir figure 4.8).

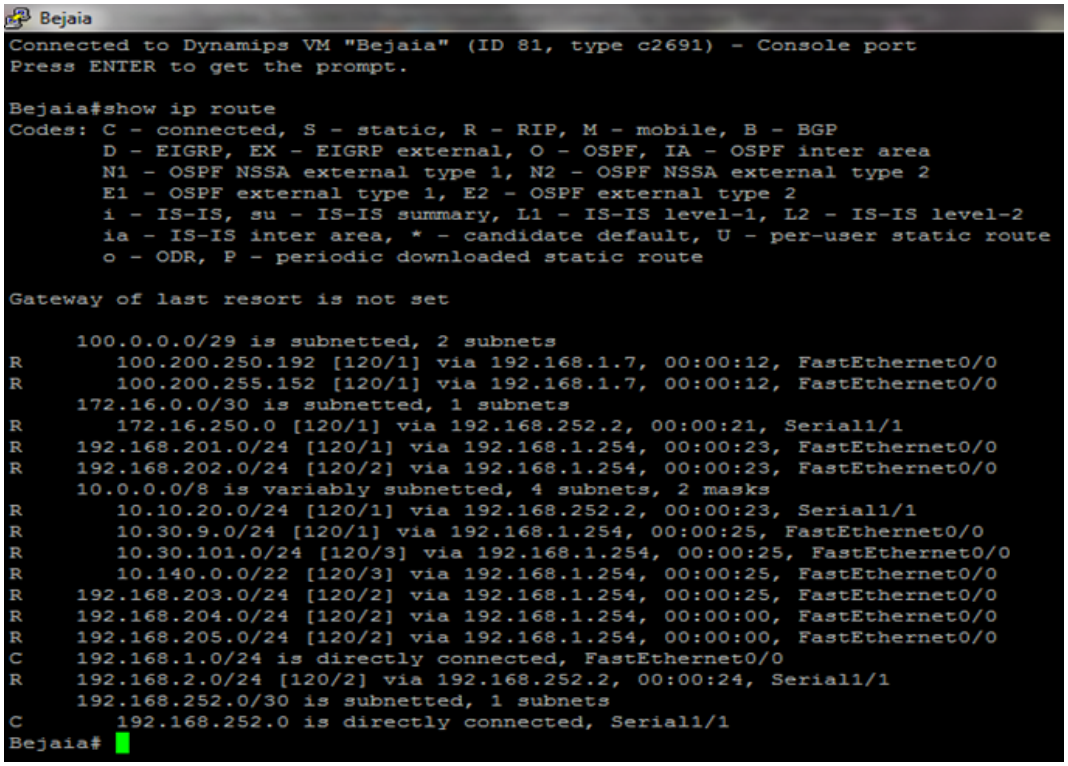

FIGURE 4.8 – Table de routage du routeur Bejaia (Cas RIP).

4.7.3 Configuration avec EIGRP

On va suivre les mêmes étapes qu'EIGRP dans le cas existant mais sans les routes statiques. La figure 4.9 montre la table de routage du routeur Bejaia.

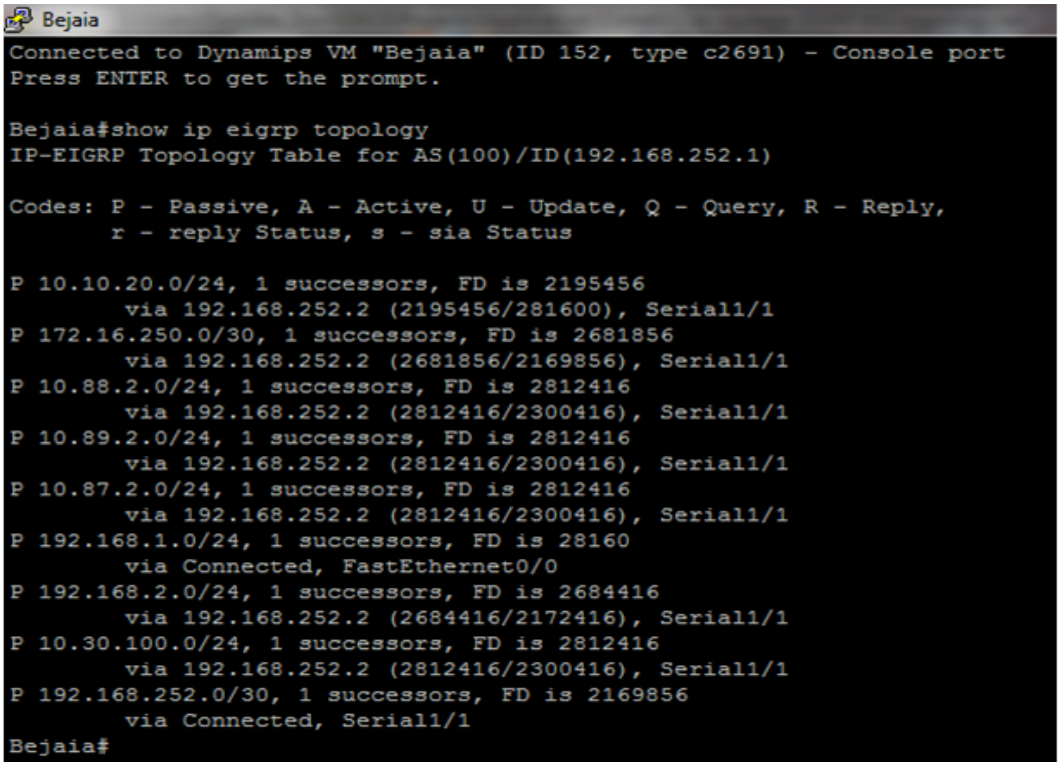

FIGURE 4.9 – Table de routage du routeur Bejaia (Cas EIGRP).

Et sa table topologique on peut l'avoir à l'aide de la commande *#show ip eigrp topology* (voir figure 4.10).

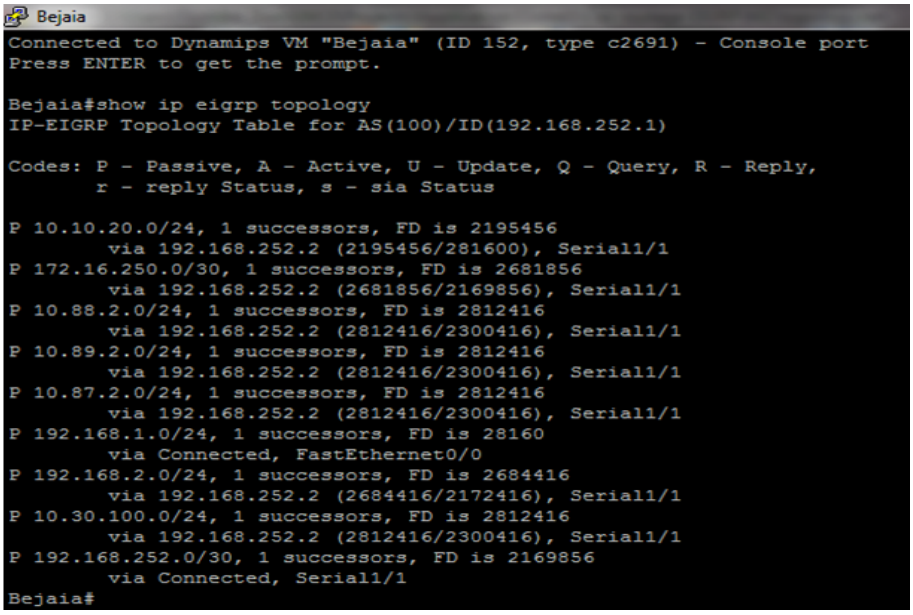

FIGURE 4.10 – Table Topologique du routeur Bejaia (Cas EIGRP).

La table des voisins du routeur Bejaia, obtenu à l'aide de la commande *#show ip eigrp neighbors* comme montre la figure 4.11

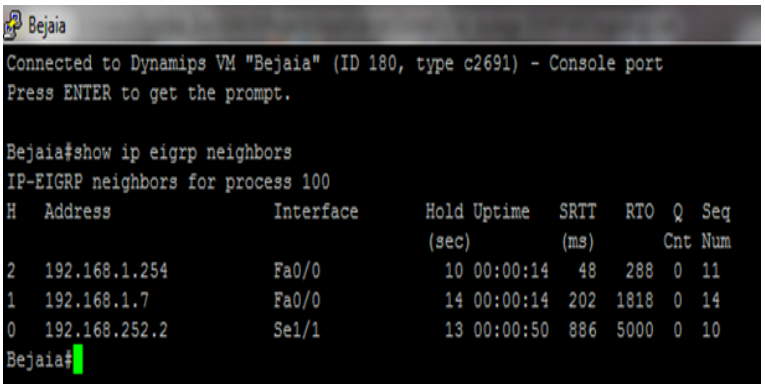

FIGURE 4.11 – Table de voisinage du routeur Bejaia (Cas EIGRP).

4.7.4 Configuration avec OSPF

C'est les mêmes étapes qu'EIGRP ou RIP, mais avec les commandes concernant OSPF. La figure 4.12 montre la table de routage du routeur Bejaia.

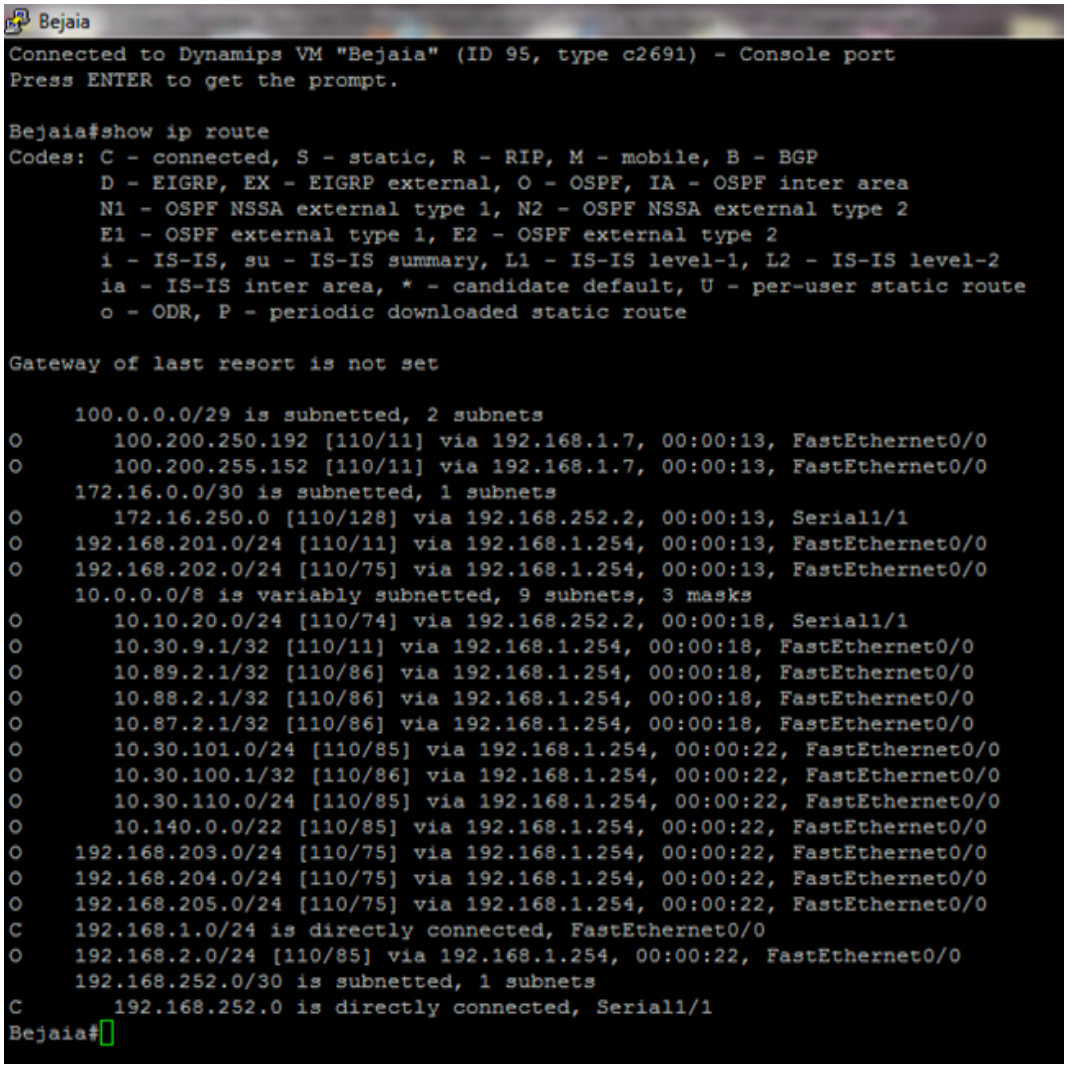

FIGURE 4.12 – Table de routage du routeur Bejaia (Cas OSPF).

La figure 4.13 montre la base de données topologique à l'aide de la commande *#show ip ospf database*.

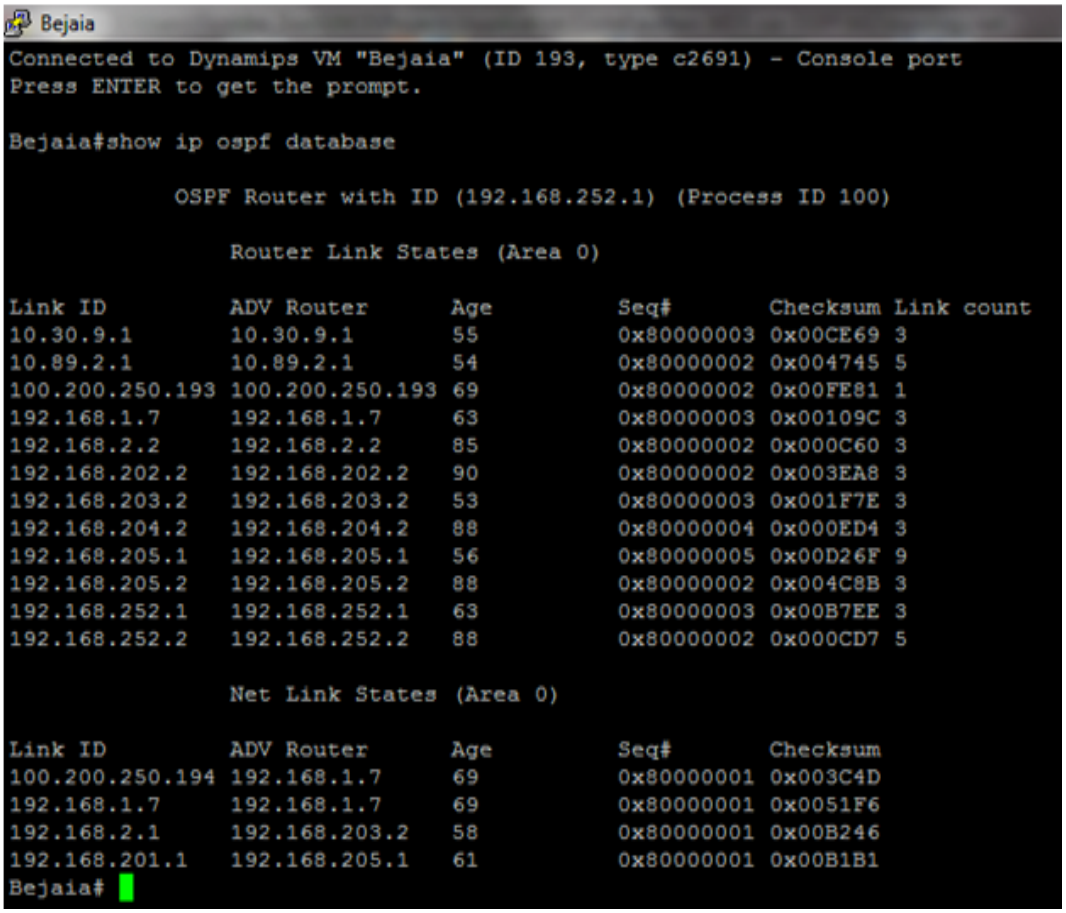

FIGURE 4.13 – DataBase du routeur Bejaia (Cas OSPF).

4.7.5 Configuration d'authentification MD5

Une fois la configuration des protocoles de routage RIP, EIGRP et OSPF terminé, En suivant les étapes vue précédemment concernant l'authentification MD5 pour les configurer sur chacun de ces protocoles.

4.7.5.1 Configuration d'authentification MD5 avec RIP

Dans cette partie, nous allons garder la configuration qui est effectue précédemment, ensuite en appliquant l'authentification md5 sur le protocole RIP de version 2.

En suivants les commandes vues plus haut, nous avons configuré l'authentification md5, ensuite en attribuant à chaque routeur les adresses réseaux auxquelles il est connecté.

La commande *#debug ip rip* permet d'afficher les mises à jour de routage RIP lors de leur envoi et de leur réception (voir la figure 4.14).

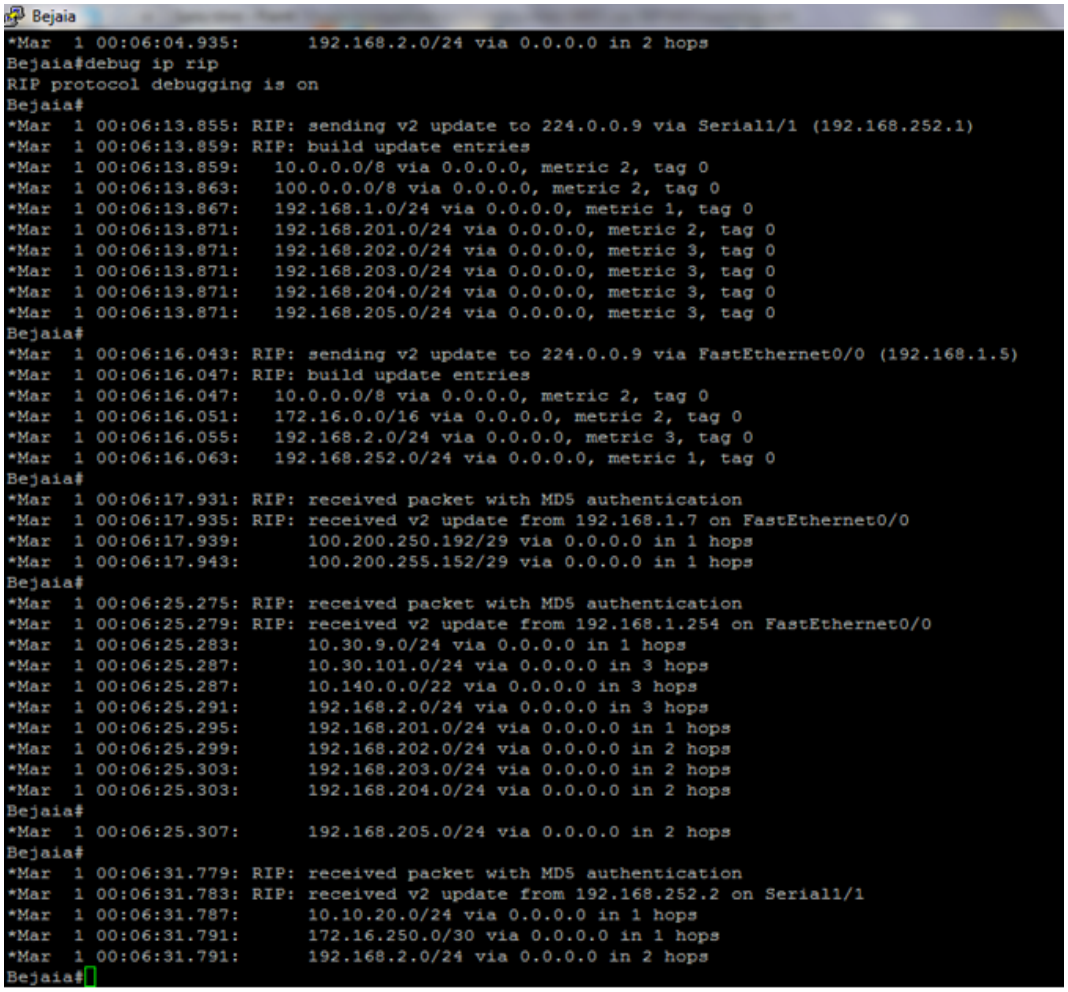

FIGURE 4.14 – Afficher les mises à jour de routage RIP du routeur Bejaia.

4.7.5.2 Configuration d'authentification MD5 avec EIGRP

On va configurer l'authentification md5 en suivant les mêmes étapes que RIP, mais avec des commandes concernant EIGRP.

Pour vérifier les paquets d'authentification EIGRP émis et reçus, en utilisant la commande *#debug eigrp packet* comme montre dans la figure 4.15 suivante.

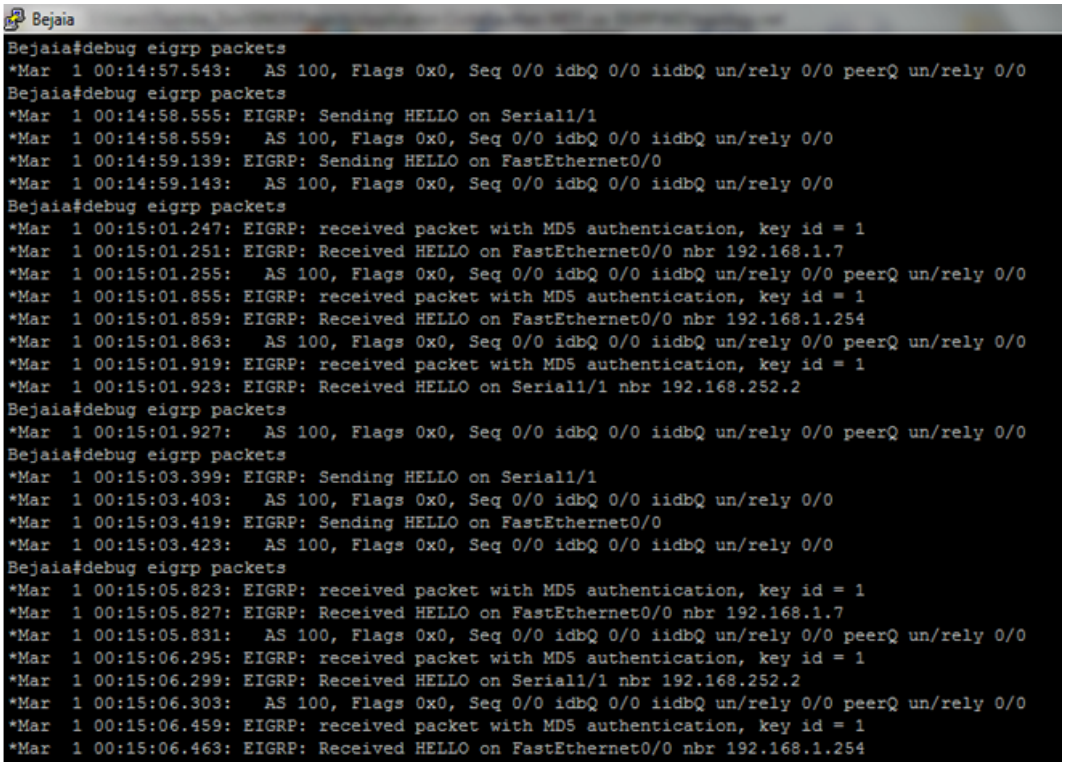

FIGURE 4.15 – Table montrant les paquets d'authentification EIGRP émis et reçus.

Et les informations sur les interfaces configurées pour EIGRP, on peut l'avoir à l'aide de la commande show ip eigrp interfaces (voir la figure 4.16).

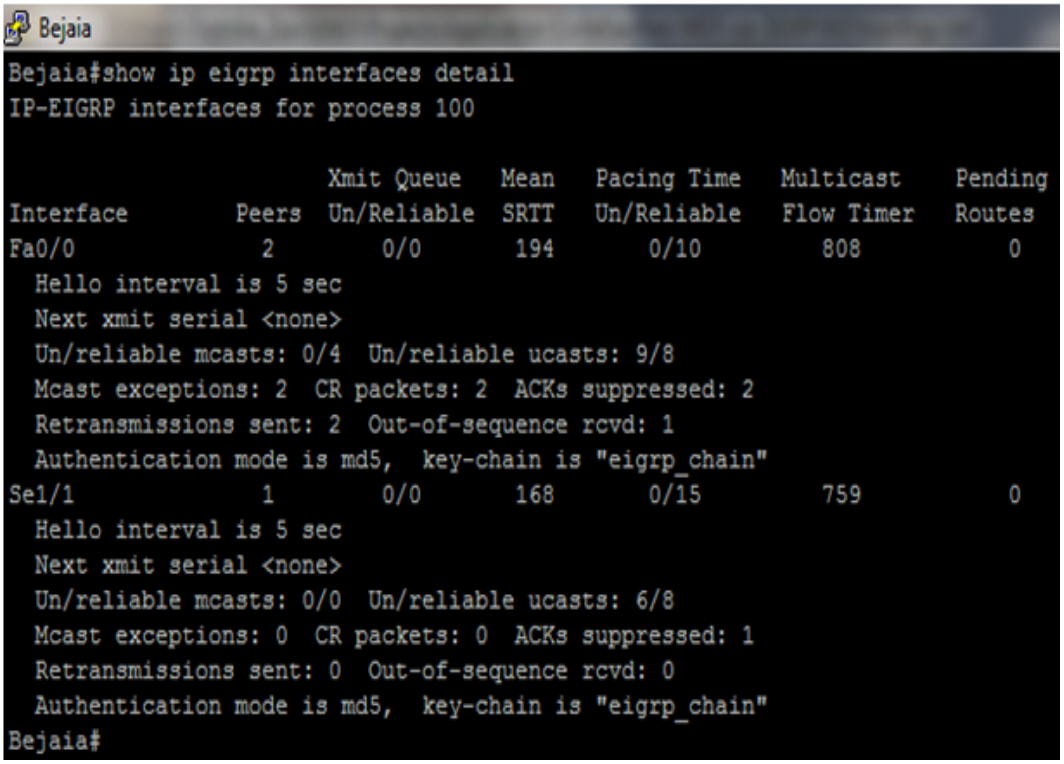

FIGURE 4.16 – Informations relatives aux interfaces participant au processus de routage d'EIGRP du routeur Bejaia (Cas EIGRP).

4.7.5.3 Configuration d'authentification MD5 avec OSPF

On va appliquer les commandes concernant l'authentification md5 avec OSPF. La commande *#debug ip ospf* paquet permet d'affiche des informations sur tous les paquets OSPF qui est reçu par un routeur (la version, le type de paquet, la longueur, ID du routeur, la zone ID,le type et la clé d'authentification) comme le montre dans la figure 4.17.

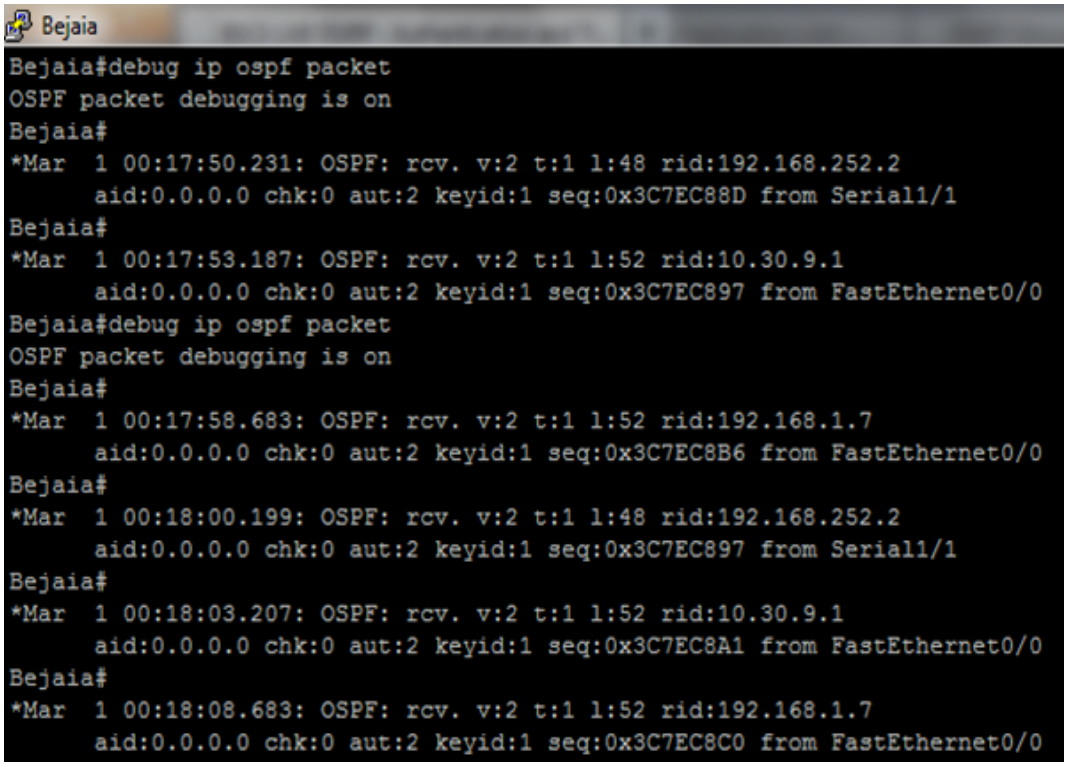

FIGURE 4.17 – Table qui affiche les paquets OSPF reçus du routeur Bejaia (Cas d'authentification OSPF).

La commande *#show ip ospf* interface permet d'afficher les informations d'interface OSPF liées (voir la figure 4.18).

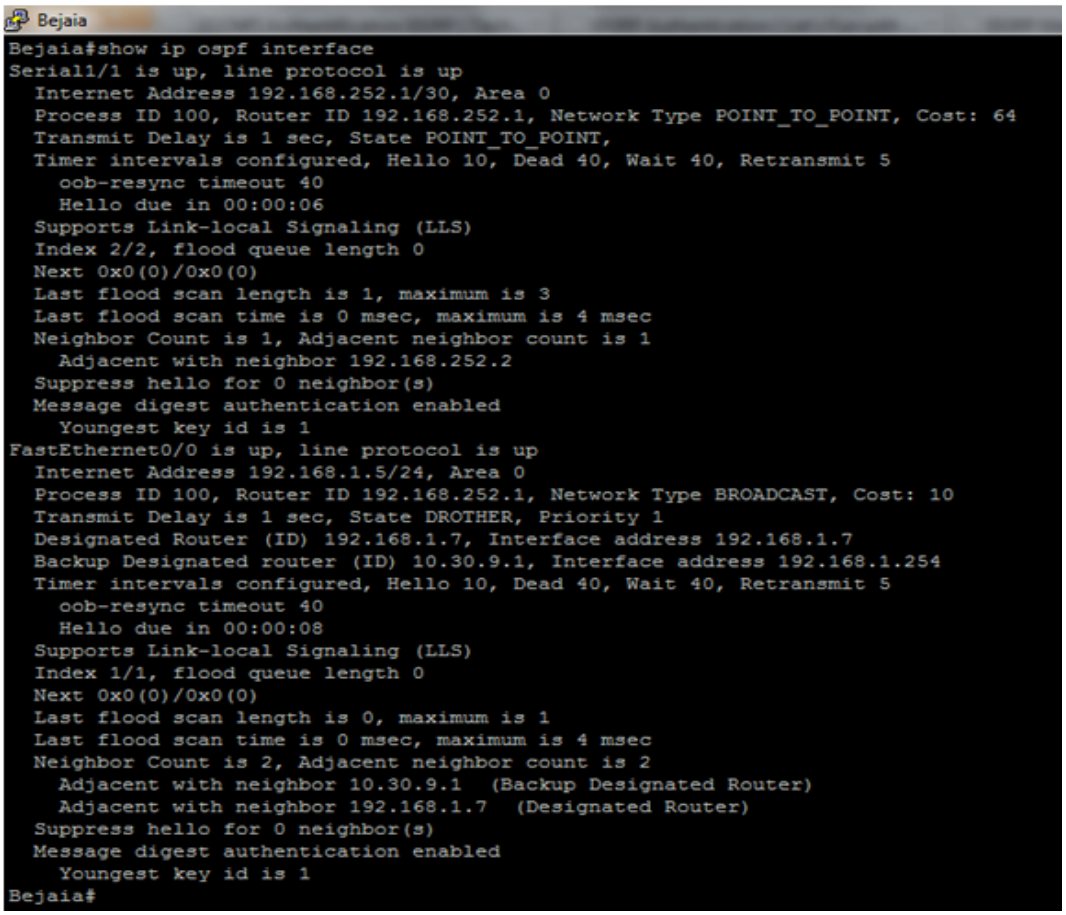

FIGURE 4.18 – Informations sur les interfaces OSPF liées du routeur Bejaia (Cas OSPF).

4.8 Conclusion

Dans ce chapitre, nous avons présenté l'environnement et les outils utilises dans notre travail, puis nous avons décrit les différentes configurations de base des routeurs, les protocoles de routage qu'on a étudiés ainsi que la configuration d'authentification MD5 sur chacun de ces protocoles. Ensuite, nous avons présenté le cas d'étude de l'entreprise CEVITAL sur lequel nous avons implémenté les différents protocoles. Enfin, nous avons donne les résultats de configuration pour illustrer les différentes tables de chacun des protocoles afin tester la connectivité sur la topologie du réseau configuré.

CONCLUSION GÉNÉRALE

Dans ce mémoire, nous avons étudié les protocoles de routage, en particulier les protocoles RIP, EIGRP et OSPF, nous avons montré les avantages et les inconvénients de chacun d'entre eux. les problèmes lies à ces protocoles de routage ont été également présenté, ensuite Nous avons montré comment les configurer sur des routeurs et comment appliquer le mécanisme de sécurité dans les mises à jour de routage, à travers une topologie d'un réseau réel (topologie Cevital).

Au terme de notre étude, nous avons constaté que les protocoles de routage sont vulnérables à plusieurs attaques. Pour cela, le mécanisme d'authentification md5 est considéré efficace pour empêcher les informations de routage incorrectes et malveillantes de s'introduire dans la table de routage d'un routeur et pour assurer l'objectif de sécurité des mises à jour de ces protocoles.

Dans la continuité de notre travail, nous pensons qu'il est nécessaire maintenant d'étudier la sécurité des réseaux en général, en activant les ACLs sur les interfaces des routeurs.

BIBLIOGRAPHIE

[1] Pillou.J. *Tout sur les réseaux et internet, Livre.* Dunod, 2007.

[2] PILLOU.J. *Généralité sur les réseaux informatiques.* livre, Copyright 2003.

[3] TOUAZI.D. *Cours Notions de base sur les réseaux.* CCNA Exploration, Cours master2, 2012.

[4] LAHDIR.M et MEZARI.R. *Réseaux Locaux.* livre, Editions Pages Bleus, 2006.

[5] ICND1. *Interconnexion des périphériques réseau.* CISCO Partie 1, Derniers cours, server 2010.

[6] PUJOLLE.G. *Les réseaux, Livre.* Edition EYROLLES, 2008.

[7] TOUAZI.D. *Cours CCNA 2 : Notions de Base sur les routeurs et le routage.* 2012.

[8] TOUAZI.D. *NAT PAT DHCP.* Cours master2, JANV 2011.

[9] Cisco. *Réseaux, Sécurité, Configuration des systèmes autonome.* 2003 Server.

[10] HEDRICK.C Network Working Group. *Protocole d'Information de Routage (RIP).* Rutgers University, RFC 1058,Juin 1988.

[11] TOUAZI.D. *Cours, Protocole RIP.* 2012.

[12] ATKINSON.R et FANTO.M Network Working Group. *RIPv2 Cryptographic Authentication.* Category : Standards Track, RFC 4822, February 2007.

[13] GALLAND.R. *Le protocole EIGRP.* Supinfo International Universit, juin 2007.

[14] Cisco.

[15] CISCO Networking Academy. *EIGRP.* Cisco Systems, Inc, 2007.

[16] CISCO Networking Academy. *Protocoles de routage Etat de lien et Concepts, Chapitre 10.* Cisco Systems, Inc, Version 4.0, 2007.

[17] KOMPELLA.K et YEUNG.D Network Working Group, KATZ.D. *Traffic Engineering (TE) Extensions to OSPF Version 2.* Memoire, Category : Standards Track, RFC3630, September 2003.

[18] *Routage Externe.* Université Catholique De Louvain, Dernière consultation : 06/06/2012.

[19] TOUAZI.D. *Cours CCNA 03 : Notion de base sur la commutation et le routage intermidiare.* 2012.

[20] Denis Valoise Benjamin Morin Avec la contribution de Olivier Sal vatori Cédric Llorens, Laurent Levier. *Tableaux de bord de la sécurité réseau.* Groupe Eyrolles, 2003, 2006, 2010,3 édition.

[21] ANTIPOLIS.S LA Chi Anh. *Mémoire de fin d'études Etude et validation de l'application du paradigme des pots de miel aux attaques visant les protocoles de routage.* Institut de la Francophonie pour l'Informatique, Septembre 2006.

[22] VAUCAMPS.A. *CISCO, sécurité des routeurs et contrôle du trafic reseau.* edition ENI, décembre 2010.

[23] REMAZEILLES.V. *La sécurité des réseaux avec Cisco, livre.* Edition ENI, fevrier 2009.

[24] CISCO. *Network Protocols Configuration Guide.* Guide de configuration IP Cisco IOS, Version 12.2, 1996.

[25] LA Chi Anh. *Etude et validation de l'application du paradigme des pots de miel aux attaques visant les protocoles de routage.* Institut Eurécom Sophia Antipolis, Septembre 2006.

[26] TOUAZI.D. *Cours Introduction au routage sans classe (routage CIDR).* 2012.

[27] CISCO. *Sample Configuration for Authentication in OSPF.* 2005.

[28] TATOUH.N et DJEBBI.S. *Securisation de routeur cisco.* Université Virtual de Tunis, 2010/2011.