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

Université Abderrahmane Mira de Béjaïa
Faculté de Sciences Exactes
Département d'Informatique

Mémoire de fin d'étude
En vue d'obtenir le diplôme de Master Professionnel en Informatique

Option : Administration et Sécurité des Réseaux.

Thème

Choix d'un protocole de routage dynamique dans un réseau d'entreprise : Cas de CEVITAL.

Présenté par

BOUABID Amel

Devant le jury composé de :

Présidente : SADOUKI Samia

Examinatrice 1 : KOUICEM Amel

Examinateur 2 : SIDER Abderrahmane

Encadreur : TARI Abdelkamel

YESSAD Hani

Co-encadreur : BAADACHE Abderrahmane

Promotion 2012/2013

Remerciements

Mes vifs remerciements vont d'emblée à Dieu tout puissant qui m'a doté d'une grande volonté et d'un savoir adéquat pour mener à bien ce travail.

Mes remerciements sont adressés également à ma famille ainsi qu'à mon très cher cousin ***Reda*** *pour tous les sacrifices faits à mon égard et leur énorme soutien durant ce travail.*

J'exprime aussi mes remerciements à mon encadreur ***Dr. TARI Abdelkamel*** *et mon co-encadreur* ***Dr. BAADACHE Abderrahmane****, pour l'effort, les conseils, leur patience et leur aide durant mon travail.*

Je remercie les membres de jury d'avoir accepté de faire partie de la commission d'examinateur et à tous mes enseignants et les membres du département Informatique de l'université ***ABDERAHMENE MIRA****. Sans oublier le personnel de Cevital et mon encadreur* ***Mr YESSAD Hani****.*

Je tiens aussi à adresser mes sincères remerciements à tous ceux qui m'ont assisté, supporté, motivé, orienté, encouragé et aidé de n'importe qu'elle manière que ce soit au cours de mes études et pour les fins de la réalisation de ce projet.

Dédicaces

Je dédie ce mémoire à ma très chère mère qui m'a soutenu et encouragé durant la période de mon travail.

Je rends hommage au regretté et très cher père dont l'absence grandit de jour en jour, qu'il repose en paix.

A mon frère ***Mahrez*** *et ma grande sœur* ***Madina****.*

A mes enseignants.

A mes ami(e)s.

A toutes les personnes qui m'ont apporté de l'aide.

Et à tous ceux qui auront posé leurs regards à lire ces lignes.

Table de matières

Chapitre 2 Présentation de l'entreprise.

Chapitre 3 Etude et comparaison des protocoles IGP.

Chapitre 4 Configuration et choix de protocoles de routage dynamique pour un réseau d'entreprise.

Liste des figures

Liste des tableaux

Liste des acronymes

AS : Système Autonome

BDR: Backup Designated Router

DR: Routeur Désigné

EGP: Exterior Gatwy Protocols

EIGRP: Enhanced Interior Gatway Routing Protocol

IGP : Interior Gatway Protocols

LSA : Link State Advertisements

LSU : Link State Update

LSR : Link State Request

OSI: Open Systems Interconnexion

OSPF: Open Shortest Path First

RIP : Routing Information Protocol

SPF: Shortest Path First

TCP/IP: Transmission Control Protocol/ Internet Protocol

VLSM: Variable Length Subnet Mask

Introduction générale

Actuellement, le réseau est entrain de devenir obligatoire dans tous les domaines. En effet, les technologies actuelles des transmissions de données entre sites éloignés, leur traitement et leur restitution , la gestion des réseaux est donc indispensable.

Il faut souvent avoir recours à des techniques d'administration pour pouvoir contrôler son fonctionnement, mais aussi d'exploiter au mieux les ressources disponibles, et de rentabiliser au maximum les investissements réalisés.

La présence d'une multitude d'équipements terminaux oblige, pour les différencier, à définir, au sein d'un réseau, un système d'identification cohérent appelé adressage, de plus, le réseau doit être capable d'acheminer une information vers tout destinataire en fonction de son adresse, grâce à la fonction de routage, un réseau informatique possède donc des principes généraux d'organisation qui définissent la façon dont ses différents équipements communiquent et partagent l'ensemble des ressources : il faut préciser la technique de commutation utilisée, le modèle d'architecture, les règles de communication ou protocoles.
Ces principes d'organisation décrivent aussi bien le comportement des équipements externes qui accèdent au réseau que celui des équipements internes au réseau lui-même **[69]**.

Les protocoles de communication permettent de définir de façon standardisée la manière dont les informations sont échangées entre les équipements du réseau : il s'agit de procédures qui contrôlent le flux d'information entre deux équipements.

Des logiciels spécifiques qui gèrent ces protocoles sont installés sur les équipements d'interconnexion comme les commutateurs réseau, les routeurs, etc. **[70]**.

I. Problématique

La configuration des éléments d'interconnexion auparavant se faisait avec le protocole EIGRP et l'utilisation du routage statique vers certaines destinations, ce qui engendrait beaucoup de problèmes tel que : l'intervention d'un administrateur réseau est obligatoire lors de l'utilisation du routage statique. Concernant le protocole EIGRP, son principal inconvénient est qu'il soit développé et propriétaire à Cisco, il ne peut par conséquent être configuré sous une autre plateforme.

Pour réaliser un lien direct entre le client (antenne de réception) et un système central (le hub), la technologie de transmission VSAT qui utilise un satellite comme relais est adoptée généralement. Cet élément présente des inconvénients parmi lesquels :

Le principal inconvénient du VSAT est son coût. Cette barrière financière relativement importante limite certaines entreprises l'accès à la technologie.

Les VSAT sont constitués d'un élément central « le hub » par lequel toutes les communications passent, si cette élément ne fonctionne plus tout le réseau sera paralysé.

La réalisation d'une opération de communication entre des réseaux locaux et étendus, doit être soigneusement conçue pour assurer un routage simple, rapide et sans conflits, ce qui n'est pas le cas avec la transmission VSAT.

De ce fait, nous avons recours à des éléments d'interconnexions spécialisés, nous nous sommes intéressés à l'utilisation des routeurs Cisco basés sur les trois protocoles de routage dynamique les plus utilisés dans un réseau d'entreprise, à savoir : *RIPv2, OSPF* et *EIGRP,* vue leur rôle crucial au sein d'un réseau d'entreprise.

II. Les protocoles existants

Les protocoles de routage sont utilisés pour faciliter l'échange d'informations de routage entre des routeurs. Ils leur permettent de partager de manière dynamique des informations sur les réseaux distants et d'ajouter automatiquement ces informations à leurs propres tables de routage. Ils déterminent également le meilleur chemin vers chaque réseau, lequel est ensuite ajouté à la table de routage.

L'un des principaux avantages de l'utilisation d'un protocole de routage dynamique est l'échange d'informations de routage entre des routeurs dès lors qu'une topologie est modifiée. Cet échange permet aux routeurs de découvrir automatiquement de nouveaux réseaux et également de trouver d'autres chemins en cas d'échec d'une liaison vers un réseau actif.

Le protocole RIP (*Routing Information Protocol*) est un protocole de routage dynamique appartenant à la famille de protocoles à vecteur de distance , qui fonctionne en tant que protocole interne dans des systèmes autonomes. Il recherche le plus court chemin selon un critère de coût simple : le nombre de routeurs traversés **[19]**.

Il existe deux versions de ce type de protocole à savoir : RIPv1 et RIPv2 et nous nous somme intéressés à la deuxième version vue les améliorations apportées à sa précédente.

OSPF (*Open Shortest Path First*) est un protocole de routage dynamique à état de liens, qui utilise l'algorithme SPF (*Shortest Path First*) pour calculer le plus court chemin vers toutes les destinations d'un système autonome, en se basant sur l'algorithme de Dijkstra, selon un critère de coût comme métrique **[19]**.

EIGRP *(Enhanced Interior Gateway Routing Protocol)* est un protocole de routage à vecteur de distance, qui est propriétaire et ne fonctionne que sur des routeurs Cisco. Il utilise une combinaison de plusieurs composants pour calculer sa métrique **[54]**.

III. Contributions de ce mémoire

L'objectif principal de ce travail à été de mettre en œuvre les trois protocoles de routage dynamique RIPv2, OSPF et EIGRP dans un réseau d'entreprise, qui doivent répondre à plusieurs exigences : robustesse, mobilité et qualité de la connectivité, qui se résumera en *« Choix d'un protocole de routage dynamique dans un réseau d'entreprise : Cas de CEVITAL »*, de réaliser une configuration de ces protocoles et de présenter nos travaux au travers le simulateur *GNS3*.

Nous avons, pour cela, à notre disposition un ensemble d'équipements pour concevoir la configuration.

IV. Organisation du document

Pour présenter tout les aspects nécessaires à l'étude des trois protocoles de routage dynamique cités, nous avons organisé ce rapport en quatre chapitres.

Le premier chapitre est une présentation des concepts liés aux réseaux d'interconnexion, leur caractéristiques, leur classification, leur architectures ainsi que le routage dans les réseaux.

Nous aborderons, également, les éléments utilisés pour faire la comparaison entre ces trois protocoles.

Quand au deuxième chapitre, nous allons faire une présentation de l'organisme d'accueil où se déroule notre stage de fin d'étude et l'architecture réseau de cette entreprise.

Dans le troisième chapitre nous mettrons l'accent sur les trois protocoles de routage qui font objet de ce projet, en l'occurrence les protocoles RIP avec ces deux versions, OSPF et EIGRP, en effet, nous décrirons ceux-ci de manière détaillée et extraire les avantages et difficultés liées au routage dans les réseaux informatiques. Une comparaison sera faite entre ces protocoles, en prenant en considération des critères.

Le quatrième chapitre concerne l'implémentation de l'architecture informatique réseau proposée. Nous présenterons le simulateur utilisé ainsi que les différentes interfaces concernant la configuration de ces éléments. Nous allons aussi choisir un protocole de routage dynamique parmi les trois étudiés qui sera configuré dans le réseau de Cevital.

Ce travail s'achève par une conclusion générale résumant les connaissances acquises durant la réalisation du projet.

CHAPITRE 1

Concepts et généralités sur les protocoles de routage dans les réseaux

1.1 Introduction

Les réseaux informatiques sont nés du besoin de relier des terminaux distants à un site central puis des ordinateurs entre eux et enfin des machines terminales, telles que des stations de travail ou serveurs. Dans un premier temps, ces communications étaient destinées au transport des données informatiques. Aujourd'hui, l'intégration de la parole téléphonique et de la vidéo sont généralisées dans les réseaux informatiques **[1]**.

Dans ce chapitre, nous présenterons les réseaux informatiques, leurs topologies, leurs architectures, leurs classifications. Nous détaillerons aussi les deux types de routage ainsi que la notion de protocoles et nous présenterons les notions qui concernent les deux familles de protocole de routage à vecteur de distance et à état de liens.

1.2. Définition d'un réseau informatique

Un réseau informatique est un ensemble d'équipements informatiques reliés physiquement entre eux par un support de transmission *(câbles)* et qui peuvent communiquer entre eux. Ces équipements sont appelés des *nœuds* ou encore des *stations (ordinateurs, imprimantes, etc.)* **[22]**.

Un réseau informatique a pour but de véhiculer les informations correspondant aux différents besoins des professionnels et du grand public et de partager des ressources de types différents tel que des fichiers. Il sert aussi à établir la communication entre des personnes grâce au courrier électronique, ainsi que la consultation de sites Web **[2]**.

1.3 Topologies des réseaux

Les deux topologies qui assurent le bon fonctionnement d'un réseau à savoir : *physique* et *logique*, permettent ainsi la circulation correcte de l'information entre les différents dispositifs matériels de ce réseau.

La topologie est la manière dont les ordinateurs sont interconnectés *(Topologie physique)* et/ ou la manière dont les données transitent sur les supports de communication *(Topologie logique)* **[30]**.

1.3.1 Topologie physique

La topologie physique est choisie selon l'environnement, l'architecture et les besoins techniques du débit **[21]**. Nous distinguons trois principales topologies :

1.3.1.1 Topologie en bus

Elle est l'organisation la plus simple d'un réseau. En effet, dans une topologie en bus tous les ordinateurs sont reliés à une même ligne de transmission par l'intermédiaire d'un câble. Le mot *« Bus »* désigne la ligne physique qui relie les machines du réseau.

Cette topologie a pour avantage d'être facile à mettre en œuvre et de posséder un fonctionnement simple. En revanche, elle est extrêmement vulnérable étant donné que si l'une des connexions est défectueuse, l'ensemble du réseau en est affecté **[2]**.

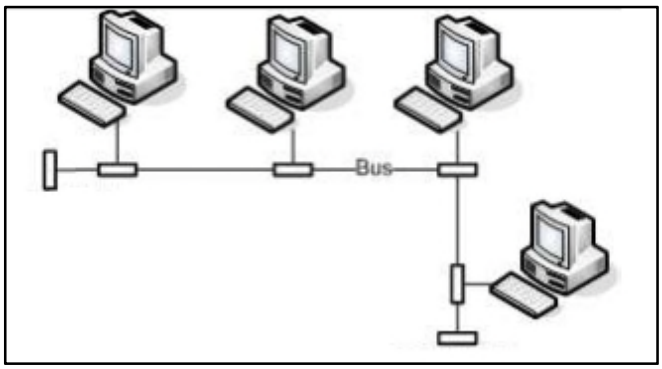


Figure 1.1 : La topologie en bus.

1.3.1.2 Topologie en étoile [2]

Dans ce type de topologie, les ordinateurs du réseau sont reliés à un système matériel central appelé *concentrateur*. Celui-ci a pour rôle d'assurer la communication entre les différentes liaisons inter-réseaux.

Contrairement aux réseaux construits sur une topologie en bus, les réseaux suivant une topologie en étoile sont beaucoup moins vulnérables car une des connexions peut être débranchée sans paralyser le reste du réseau.

Le point faible de ce réseau est le concentrateur, car sans lui plus aucune communication entre les ordinateurs du réseau n'est possible.

En revanche, un réseau à topologie en étoile est plus onéreux qu'un réseau à topologie en bus car un matériel supplémentaire est nécessaire.

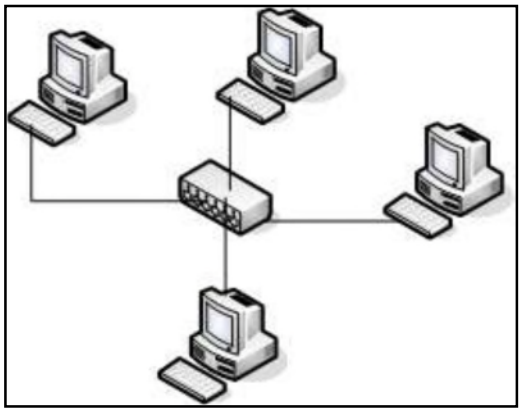


Figure 1.2 : La topologie en étoile.

1.3.1.3 Topologie en anneau

Dans un réseau possédant une topologie en anneau, les ordinateurs sont situés sur une boucle et communiquent chacun à son tour **[3]**.

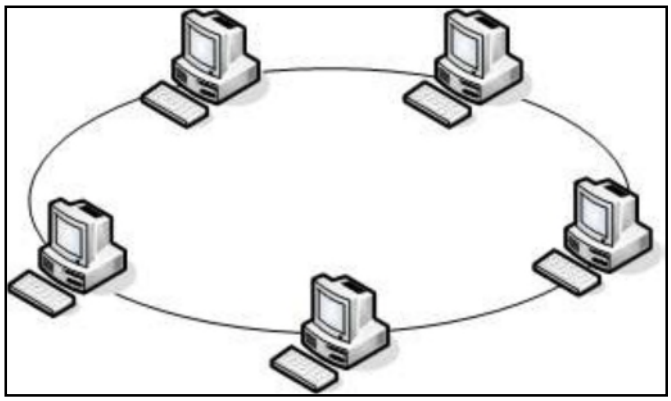


Figure 1.3 : La topologie en anneau.

1.3.1.4 La topologie en arbre

Aussi connu sous le nom de *topologie hiérarchique*, le réseau est divisé en niveaux. Le sommet, de haut niveau, est connecté à plusieurs nœuds de niveau inférieur, dans la hiérarchie. Ces nœuds peuvent être eux-mêmes connectés à plusieurs nœuds de niveau inférieur. Le tout dessine alors un *arbre*, ou une *arborescence* **[31]**.

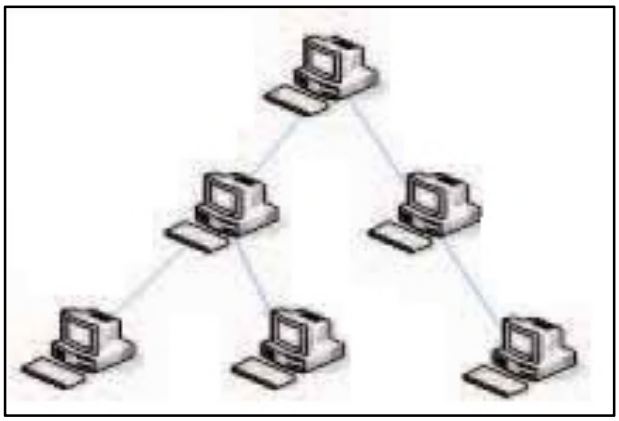


Figure 1.4 : La topologie en arbre.

1.3.1.5 La topologie maillée

Une topologie maillée, est une évolution de la topologie en étoile, elle correspond à plusieurs liaisons points à points. Une unité réseau peut avoir (1, N) connexions point à point vers plusieurs autres unités. Chaque terminal est relié à tous les autres. Cette topologie se rencontre dans les grands réseaux de distribution comme Internet.

L'information peut parcourir le réseau suivant des itinéraires divers, sous le contrôle de puissants superviseurs de réseau, ou grâce à des méthodes de routage réparties. En cas de rupture d'un lien, l'information peut quand même être acheminée **[31]**.

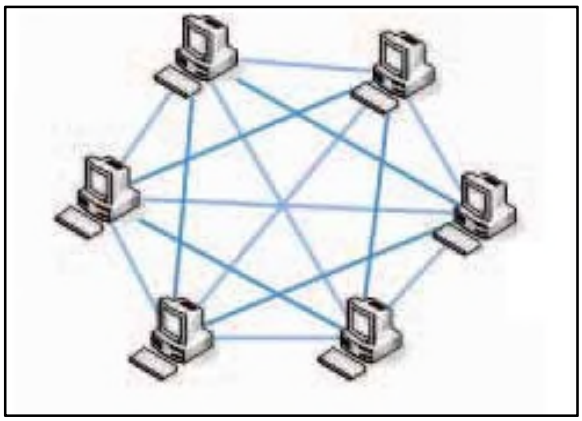


Figure 1.5 : La topologie maillée.

1.3.2 Topologie logique

Elle représente la façon dont les données transitent dans les lignes de communication. Les topologies logiques les plus courantes sont *Ethernet, Token Ring* et *FDDI* (Le protocole FDDI (*Fiber Distributed Data Interface*) est l'un des plus récents représentant des techniques de transmission pour des réseaux locaux à haut débit) **[2]**.

1.4 Classification des réseaux

Les caractéristiques principales qui vont nous permettre de différencier les grandes familles des réseaux sont : leur taille, leur vitesse de transfert de données ainsi que leur étendue.

Nous aurons alors à distinguer quatre types de réseaux : les réseaux personnels *(PAN)*, les réseaux locaux *(LAN)*, les réseaux métropolitains *(MAN)* et les réseaux étendus *(WAN)* **[2]**, qui seront décrits dans ce qui suit :

1.4.1 Les réseaux personnels PAN *(Personal Area Network)*

Un réseau personnel interconnecte *(souvent par des liaisons sans fil)* des équipements personnels tels qu'un ordinateur portable, un agenda électronique, des terminaux GSM, etc. **[2]**.

1.4.2 Les réseaux locaux LAN *(Local Area Network)*

C'est un ensemble d'ordinateurs appartenant à une même organisation et reliés entre eux dans une petite zone géographique *(jusqu'à 10 kilomètres)* par un réseau. La vitesse de transfert de données d'un réseau local peut s'étaler entre *10 Mbits/s* et *1 Gbits/s* **[2]**.

1.4.3 Les réseaux Métropolitain MAN *(Metropolitain Area Network)*

Il interconnecte plusieurs réseaux locaux géographiquement proches *(jusqu'à 50 kilomètres)* à des débits importants. Ainsi un réseau métropolitain permet à deux machines distantes de communiquer.

Il est formé de commutateurs ou de routeurs interconnectés par des liens hauts débits *(fibre optique par exemple)* **[2]**.

1.4.4 Les réseaux Etendus WAN *(Wide Area Network)*

Ces réseaux sont généralement constitués de plusieurs sous-réseaux hétérogènes et s'étendent sur une région ou un pays entier. L'étendue géographique de ce type de réseaux va jusqu'à *100 kilomètres* et plus **[2]**.

Les ordinateurs *(Hôtes)* connectés à un réseau étendu sont souvent reliés par des réseaux publics, tels que le système téléphonique et le plus grand réseau étendu est Internet **[23]**.

1.5 Architectures d'un réseau

Nous pouvons distinguer deux types d'architectures : l'architecture Client/ Serveur et l'architecture Peer To Peer (appelé Poste à Poste).

1.5.1 Architecture Client / Serveur

Dans ce type d'architecture les machines clientes se connectent à un serveur et envoient des requêtes en demandant des services (des programmes fournissant des données tels que des fichiers) et le serveur à son tour répond aux machines clientes en envoyant la réponse désirée **[2]**.

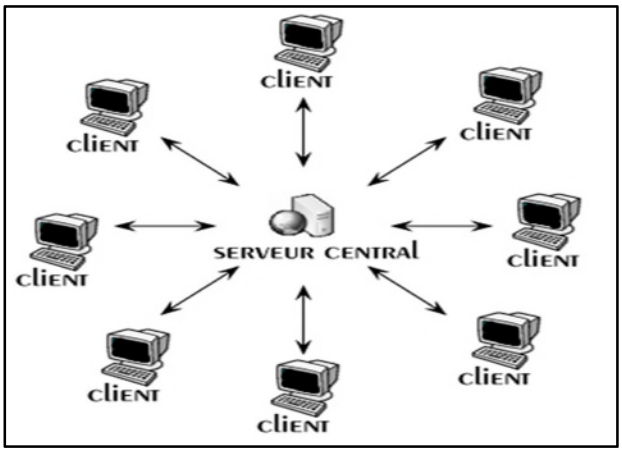


Figure 1.6 : Architecture Client/ Serveur.

1.5.1.1 Les types d'architecture Client/ Serveur

Selon le nombre de niveaux, nous pouvons citer plusieurs types **[31]**:

a) Architecture à 2-tiers

L'architecture à deux niveaux caractérise les systèmes clients/serveurs pour lesquels le client demande une ressource et le serveur la lui fournit directement, en utilisant ses propres ressources. Cela signifie que le serveur ne fait pas appel à une autre application afin de fournir une partie du service, la figure 1.7 présente ce fonctionnement :

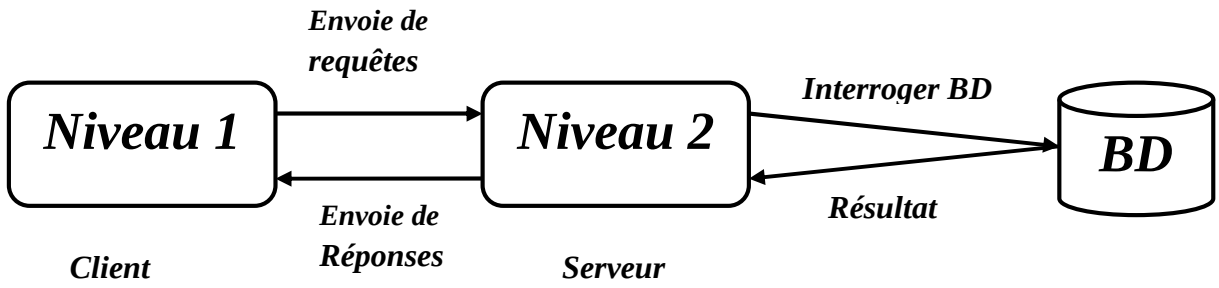


Figure 1.7 : Architecture 2-tiers.

b) Architecture à 3-tiers

Dans l'architecture à trois niveaux, il existe un niveau intermédiaire, c'est-à-dire que nous avons généralement une architecture partagée entre :

- ✓ Un client (l'ordinateur) demandeur de ressources, équipé d'une interface utilisateur (généralement un navigateur web) chargée de la présentation,
- ✓ Le serveur d'application qui est chargé de fournir la ressource, fait appel à un autre serveur,
- ✓ Le serveur de données, fournit au serveur d'application les données dont il a besoin.

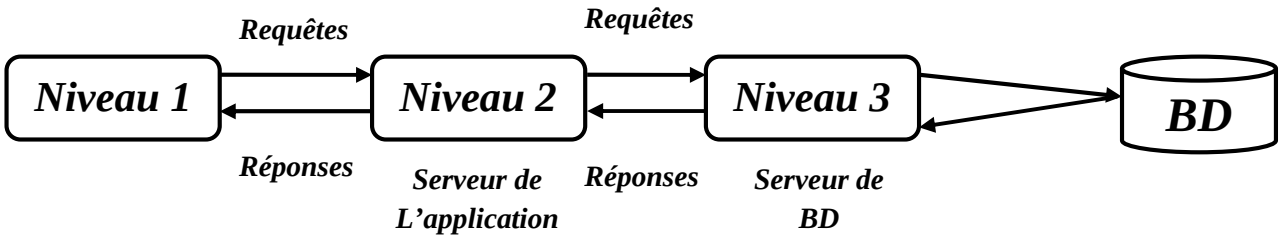


Figure 1.8 : Architecture 3-tiers.

c) Architecture multi-tiers

L'architecture à trois niveaux est une architecture à *N niveaux*, dans ce type d'architecture, chaque serveur (niveaux 2 et 3) effectue une tâche (un service) spécialisé.

Un serveur peut donc utiliser les services d'un ou plusieurs autres serveurs afin de fournir son propre service.

1.5.1.2 Avantages de l'architecture client/serveur [2]

Les atouts de ce système sont nombreux, pour cela nous allons présenter certains d'entre eux:

a) Des ressources centralisées : Le serveur peut gérer des ressources communes à tous les utilisateurs, étant donné qu'il est au centre du réseau,

b) Une meilleure sécurité : Le nombre de points d'entrée permettant l'accès aux données est mois important,

c) Un réseau évolutif : Grâce à cette architecture c'est facile de supprimer ou de rajouter des clients sans perturber le fonctionnement du réseau.

1.5.1.3 Inconvénients de l'architecture client/serveur

Ce type d'architecture mène à plusieurs inconvénients qui sont : son coût est élevé, le serveur est le seul maillon faible du réseau client/serveur, étant donné que tout le réseau est architecturé autour de lui **[2]**.

1.5.2 Architecture Post à Post (Peer to Peer)

Dans l'architecture poste à poste, contrairement à une architecture réseau du type client/ serveur, il n'y a pas de serveur dédié, cela signifie que chacun des ordinateurs du réseau joue le rôle d'un client et d'un serveur au même temps **[2]**.

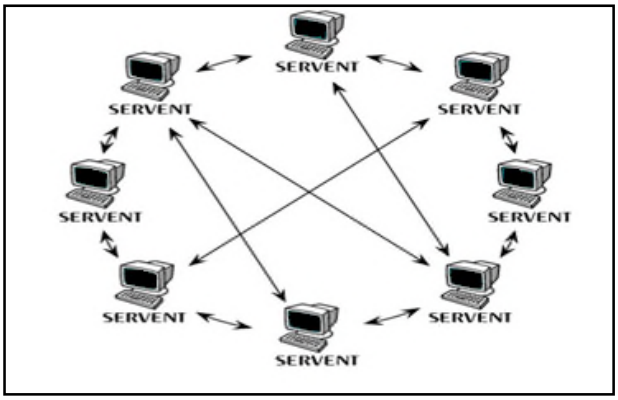


Figure 1.9 : Architecture Poste à Poste.

1.5.2.1 Avantages de l'architecture Poste à Poste

Cet architecture est simple à mettre en œuvre, son coût est réduit par rapport au coût engendré par la mise en œuvre d'une architecture client/ serveur et chaque poste est à la fois client et serveur **[2]**.

1.5.2.2 Les inconvénients de l'architecture Poste à Poste

Ce système n'est pas centralisé, ce qui le rend très difficile à administrer pour cela la sécurité est plus difficile à assurer. Les profils des utilisateurs sont stockés sur le poste, donc les utilisateurs ne peuvent pas changer aisément de machine **[2]**.

1.6 Le modèle de référence

Dans ce qui suit nous décrirons deux modèles de références de réseau : le modèle de référence *OSI* et le modèle de référence *TCP/IP*.

1.6.1 Le modèle de référence OSI

Ce modèle se fonde sur une proposition élaborée par l'organisation internationale de normalisation *(ISO - International Standard Organisation)*, il est appelé Modèle de Référence *OSI (Open Systems Interconnection)* **[3]**.

C'est un modèle qui comporte sept parties appelées *« couches »* et chacune d'elle est responsable de l'un des aspects de communication et à pour rôle de fournir des services à la couche qui lui est immédiatement supérieur.

La couche de niveau « N » d'un ordinateur ne peut communiquer qu'avec la couche de niveau « N » d'un autre ordinateur et cela grâce à des règles définis par un protocole et pour réaliser cette communication, la couche de niveau « N » utilise des services offerts par la couche de niveau « N-1 » et ils sont ensuite offerts à la couche de niveau « N+1 » par le biais de son interface **[5]**.

1.6.1.1 Les sept couches du modèle OSI [3]

Les rôles des différentes couches du modèle de référence OSI sont présentés ci-dessous :

a) Couche Physique : Elle définit la façon dont les données sont physiquement converties en signaux numériques sur le support de transmission et gère aussi le type de transmission du signal (mode synchrone ou asynchrone).

b) Couche Liaison de données : Cette couche définit les règles d'émission et de réception de données, ainsi que la mise en œuvre de la détection et de la correction d'erreurs. Elle gère également le contrôle de flux.

c) Couche Réseau : Cette couche gère l'adressage et le routage des données via le réseau, c'est la façon dont les paquets de données sont acheminés de la source au destinataire.

d) Couche Transport : La fonction de base de cette couche est d'accepter des données de la couche session, de les découper, en plus petites unités (appelés paquets) et de les faire passer à la couche réseau. Elle détermine le type de services à fournir à la couche session et aux utilisateurs du réseau.

e) Couche Session : Elle permet à des utilisateurs travaillant sur différentes machines d'établir des sessions entre eux, permet la gestion du dialogue et la synchronisation également.

f) Couche Présentation : Elle définit le format des données, à la différence des autres couches, qui sont concernées seulement par la transmission fiable des bits d'un point à un autre, cette couche s'intéresse à la syntaxe et à la sémantique de l'information transmise.

g) Couche Application : Cette couche se charge du transfert de fichiers, le courrier électronique ainsi que la lecture des pages web.

1.6.2 Le modèle de référence TCP/IP [2]

Transmission Control Protocol / Internet Protocol (TCP / IP) est une suite de protocoles, l'appellation provient de la combinaison des noms des deux protocoles TCP et IP qui représentent l'ensemble des règles de communication sur internet et se base sur la notion d'adressage IP.

En d'autres termes, il permet de fournir une adresse IP à chaque machine du réseau afin de pouvoir acheminer les paquets de données. La suite de protocoles TCP/IP est conçue pour répondre à un certain nombre de critères, parmi lesquels nous citons : la fragmentation des messages en paquets, l'utilisation d'un système d'adresses, l'acheminement des données sur le réseau (routage) et le contrôle d'erreurs de transmission de données.

1.6.2.1 Les quatre couches du modèle TCP/IP

Le fonctionnement de chaque couche du modèle TCP/IP est présenté ci-après :

a) Couche Accès réseau : Cette couche permet de construire les trames, la mise en place d'une gestion d'erreur sur les trames fournis par la couche supérieure ainsi que la transmission sur les divers supports physiques utilisables **[5]**.

b) Couche Internet : Le rôle de cette couche est de permettre l'injection de paquets dans n'importe quel réseau d'acheminement de ces paquets. Il est possible que les paquets arrivent dans un ordre différent de l'ordre d'émission, auquel cas se sera aux couches supérieures de les réordonner **[3]**.

c) Couche Transport : Elle permet à des entités paires sur des ordinateurs sources et destinations de soutenir une conversation. Deux protocoles ont été définis : le premier est TCP *(Transmission Control Protocol)* qui est un protocole fiable, orienté connexion et le second protocole est UDP *(User Datagram Potocol)* qui est non fiable et sans connexion **[3]**.

d) Couche Application : Elle contient tous les protocoles de haut niveau tel que : le protocole *TELNET* qui est utilisé pour les connexions à distances, le protocole *FTP* qui est utilisé pour le transfert de fichiers, le protocole *SMTP* pour les courriers électroniques ainsi que le protocole *http* qui sert à charger les pages web **[3]**.

Le modèle TCP/IP reprend l'approche modulaire du modèle OSI (utilisation des couches) mais ne contient que quatre couches et chacune d'elle correspond à une ou plusieurs couches du modèle OSI.

Le tableau suivant illustre les correspondances qu'il y ait entre ces deux modèles :

Modèle TCP/IP	***Modèle OSI***
Application	Application
	Présentation
	Session
Transport (TCP)	Transport
Internet (IP)	Réseau
Accès Réseau	Liaison Données
	Physique

Tableau 1.1 : Comparaison entre le modèle OSI et le modèle TCP/IP.

1.7 Le routage

Un environnement internet résulte de l'interconnexion de plusieurs réseaux physique par des routeurs, chaque routeur est connecté directement à deux ou plusieurs réseaux **[1]**.

Le routage d'un datagramme est l'opération qui consiste à trouver le chemin de la station destinatrice sur lequel les datagrammes (appelés paquets) seront transmis d'un réseau à un autre, à partir de son adresse IP. En effet, si la destination ne se situe pas sur le réseau ou sous-réseau local de la machine source, le paquet doit être dirigé vers un routeur qui rapproche de son objectif. Chaque routeur doit connaître l'adresse IP du routeur suivant sur le chemin, c'est pour quoi il doit gérer de manière statique ou dynamique une table de routage qui contient tous les réseaux accessibles et une entrée de routage par défaut pour les destinations qui ne soit pas connus directement. Tout équipement IP, hôte ou routeur possède une table de routage **[6]**.

1.7.1 Objectifs du routage [7]

Le but du routage est la fourniture de l'information nécessaire pour effectuer un routage, c'est-à-dire la détermination d'un chemin à travers le réseau entre une machine émettrice et une machine réceptrice.

Les protocoles de routage ont pour objectif d'établir des règles d'échange entre routeurs pour mettre à jour leurs tables selon des critères de coût, voir : la distance, l'état de la liaison et le débit. Ils améliorent ainsi l'efficacité du routage.

Il y a de très nombreux problèmes à résoudre et l'un qui apparaît lorsqu'il y a une panne dans le réseau et qu'il faut optimiser le calcul des nouvelles routes : une fois la panne détectée, il faut transmettre l'information sur l'événement le plus rapidement possible pour que les différents routeurs recalculent par où faire passer leurs messages en contournant la liaison en panne.

1.7.2 Formes de routage

Nous pouvons distinguer deux formes de routage : *Le routage par remise directe des datagrammes* et *le routage par remise indirecte des datagrammes* **[4]**.

1.7.2.1 Routage par remise directe

La transmission des datagrammes entre deux machines qui veulent communiquer et qui sont situées dans le même réseau ne met pas en jeu des routeurs. L'expéditeur encapsule

le datagramme dans une trame, effectue la correspondance ente l'adresse IP et l'adresse physique et envoi la trame directement et sans passer par le routeur **[1]**.

1.7.2.2 Routage par remise indirecte

Ce type de routage est mis en ouvre chaque fois que les données échangées entre les ordinateurs transitent au moins par un routeur, dans ce cas, le routage consiste à déterminer le routeur par lequel les datagrammes seront transmis **[1]**.

1.7.3 Table de routage

La table de routage est stockée sur un routeur qui est un équipement d'interconnexion de réseaux informatiques permettant d'assurer le routage des paquets entre deux réseaux ou plus afin de déterminer le chemin qu'un paquet de données va emprunter **[28]**, elle garde une trace des routes conduisant à des destinations particulières du réseau et dans certains cas des métriques de routage associées à ces routes.

C'est une table qui permet d'établir une correspondance entre le réseau de destination (auquel appartient le destinataire du paquet) et l'adresse du prochain routeur (prochain saut) permettant d'atteindre la destination finale **[26]**.

1.7.3.1 Compostions d'une table de routage

Pour router un paquet, le routeur fondera sa décision en deux temps : d'abord il regarde dans l'en-tête IP du réseau de destination et compare toutes les entrées dont il dispose dans sa table de routage; ensuite, si le réseau de destination est trouvé, il envoie le paquet sur le bon port de sortie; si ce réseau n'est pas trouvé, le paquet est jeté.

La table de routage est constituée des éléments suivants : l'adresse de destination, le masque de sous réseau, l'adresse du prochain routeur directement accessible, la passerelle et l'interface de sortie **[33]**.

1. **Définition d'une métrique**

La métrique d'une route est la valeur d'une route en comparaison d'autres routes connu par le protocole de routage. Plus sa valeur est faible, meilleure est la route **[33]**.

Chaque protocole de routage utilise sa propre mesure. Ainsi, le protocole RIP utilise le nombre de sauts, le protocole EIGRP utilise une combinaison de bande passante et de délai, tandis que l'implémentation du protocole OSPF par Cisco fait appel à la bande

passante, en plus de ces mesures il existe d'autres qui sont utilisées par les protocoles de routage IP **[44]** :

1.1 Nombre de sauts : Mesure simple qui compte le nombre de routeurs qu'un paquet doit traverser pour atteindre le réseau de destination.

1.2 Bande passante : Influence la sélection du chemin en préférant celui dont la bande passante est la plus élevée.

1.3 Charge : Prend en considération l'utilisation d'une liaison spécifique en termes du trafic.

1.4 Délai : Prend en considération le temps nécessaire à un paquet pour parcourir un chemin.

1.5 Fiabilité : Évalue la probabilité d'échec d'une liaison, calculée à partir du nombre d'erreurs de l'interface ou des échecs précédents de la liaison.

1.6 Coût : Valeur déterminée par l'IOS ou par l'administrateur réseau pour indiquer une route préférée. Le coût peut représenter une mesure, une combinaison de mesures ou une stratégie.

2. Distance administrative [44]

La distance administrative est la mesure utilisée par les routeurs Cisco pour sélectionner le meilleur chemin quand il y a deux ou plusieurs routes différentes vers la même destination à partir de deux protocoles de routage différents.

Elle définit la fiabilité d'un protocole de routage. Chaque protocole de routage est prioritaire dans l'ordre de la plus à la moins fiable en utilisant une valeur de distance administrative. Une valeur numérique inférieure est préférée, par exemple une route OSPF avec une distance administrative de 110 sera choisie sur une route RIP avec une distance administrative de 120. Le tableau 1.2 suivant montre les valeurs de la distance administrative par défaut de chaque protocole :

Origine de la route	Distance administrative
Connecté directement	**0**
Route statique	**1**
EIGRP interne	**90**
OSPF	**110**
RIP	**120**
EIGRP externe	**170**
Résumé de routes EIGRP	**5**

Tableau 1.2 : Tableau des distances administratives.

1.7.4 Temps de Convergence

Lorsque les tables de routage de tous les routeurs ont atteint un état de cohérence, cela signifie que la convergence existe. Lorsque tous les routeurs disposent d'informations complètes et précises sur le réseau, cela signifie que le réseau a convergé.

Le temps de convergence est le temps nécessaire aux routeurs pour partager des informations, un réseau n'est pas complètement opérationnel tant qu'il n'a pas convergé. Les protocoles de routage peuvent être classés en fonction de leur vitesse de convergence : le protocole EIGRP et OSPF convergent rapidement par rapport à RIP avec ces deux version 1 et 2 et EIGRP **[68]**.

1.7.5 Les algorithmes de routage

Un algorithme de routage a pour rôle d'acheminer un paquet de données à travers le réseau et pour chaque nœud d'un réseau, il détermine une table de routage **[5]**. Ces algorithmes peuvent être divisés en deux classes principales : *Routage statique* (les algorithmes non adaptatifs) et le *routage dynamique* (les algorithmes adaptatifs) **[3]**.

1.7.5.1 Routage statique

Le routage statique consiste à construire, dans chaque nœud, une table indiquant, pour chaque destination, l'adresse du nœud suivant. Cette table est construite par l'administrateur du réseau lors de configuration et à chaque changement de topologie **[8]**.

Si le réseau global est complexe, la configuration peut être fastidieuse et source d'erreurs. De plus, lorsqu'un nouveau réseau est ajouté, il faut reconfigurer l'ensemble **[10]**.

Le routage statique n'est pas optimal, il convient parfaitement aux petits réseaux et aux réseaux dans lesquels il n'existe pas de redondance dans les routes et parmi les algorithmes de routage statique nous avons le routage du plus court chemin *(Djikstra)* **[8]**.

1.7.5.2 Routage dynamique

Les informations relatives à la route sont mises à jour automatiquement entre les routeurs **[9]**.

Les algorithmes adaptatifs modifient leurs décisions de routage pour refléter les changements de topologie et du trafic dans le réseau. Ces algorithmes diffèrent selon **[3]** :

- ✓ L'endroit où ils se procurent leurs informations de routage (par exemple localement, sur les routeurs adjacents ou sur tout les routeurs),
- ✓ L'instant où ils changent de route,
- ✓ La métrique d'optimisation utilisée (par exemple, la distance à parcourir ou bien le nombre de sauts).

Parmi les algorithmes adaptatifs nous citons : les algorithmes de routage par vecteur de distance et comme exemple nous avons *RIP (Routing Information Protocol)* et les algorithmes de routage par informations d'état de liens tel que *OSPF (Open Shortest Path First)*.

Remarque

Le routage dynamique permet d'éviter le processus fastidieux de configuration de routes statiques. Avec ce type de routage, les routeurs peuvent réagir aux changements survenus sur le réseau et modifient leurs tables de routage en conséquence, sans intervention de la part de l'administrateur réseau **[27]**.

1.7.6 Comparaison entre le routage statique et dynamique

1.7.6.1 Avantages du routage statique [32]

Le routage statique est plus facile à configurer et à comprendre par l'administrateur car, y a pas la demande de configuration d'un protocole (OSPF par exemple). Il utilise une seule route par défaut car elle facilite la circulation de données sur un réseau de grande taille et elle est utilisée si le prochain saut ne figure pas explicitement dans la table de routage.

La table de routage peut être maintenue facilement dans les réseaux stables de petite taille, grâce au routage statique.

1.7.6.2 Inconvénients du routage statique [32]

Avec ce type de routage, la complexité augmente avec la taille du réseau et il y a risque d'erreurs (problématique sur de grands réseaux), tels que : la perte de temps car la configuration et les mises à jour des routeurs s'effectuent manuellement, ce qui nécessite l'intervention d'un administrateur à chaque modification.

1.7.6.3 Inconvénients du routage dynamique

C'est difficile à mettre en place car il demande à configurer un protocole de routage comme RIP ou OSPF **[32]**.

1.7.6.4 Avantages du routage dynamique

La maintenance et la configuration sont simplifiées lors de l'ajout ou la suppression d'un élément dans un réseau, car il réagit automatiquement aux modifications topologiques, donc la configuration se fait avec moins de risques d'erreurs et il est plus évolutif **[32]**.

1.8 Les protocoles

1.8.1 Définition d'un protocole

Pour que des ordinateurs puissent communiquer, il est nécessaire qu'ils observent des règles communes de communications appelées des *protocoles*.

Un protocole est une méthode standard qui permet la communication entre des processus (s'exécutant sur des machines), c'est un ensemble de règles et de procédures à respecter pour émettre et recevoir des données sur un réseau **[24]**.

1.8.2 Protocole de routage

Les routeurs utilisent des protocoles de routage pour gérer dynamiquement les informations reçues depuis leurs propres interfaces et depuis d'autres routeurs. Les protocoles de routage peuvent être également configurés pour gérer les routes entrées manuellement, ils sont donc utilisés par les routeurs pour échanger entre eux leurs informations et constituer de manière dynamique leurs tables de routage et les protocoles les plus utilisés sont : le protocole RIPv2 et le protocole OSPF **[27]**.

1.8.2.1 Le rôle du protocole de routage dynamique

Un protocole de routage dynamique prend connaissance de toutes les routes disponibles. Il insère les meilleures routes dans la table de routage et supprime celles qui ne

sont plus valides. Le procédé qu'utilise un protocole de routage pour déterminer la meilleure route vers un réseau de destination s'appelle un *algorithme de routage* **[27]**.

1.8.2.2 Les deux grandes classes de protocoles

Un système autonome *(AS)* est un ensemble de réseaux sous la même autorité administrative (autorité de gestion) tel que le domaine *cisco.com*. Au sein d'un système autonome, les routes sont générées par des protocoles de routage intérieurs comme *RIP*, *IGRP*, *EIGRP*, *OSPF* ou *ISIS* et les protocoles de routage qui permettent de connecter les systèmes autonomes entre eux sont des protocoles de routage extérieurs comme *BGP* **[33]**.

Un tel système est constitué de routeurs qui présentent une vue cohérente du routage vers l'extérieur. Il existe deux familles de protocoles de routage : les protocoles *IGP* et les protocoles *EGP* qui seront illustrées dans la figure 1.10 **[29]**.

1. ***Les protocoles IGP (Interior Gatway Protocols):*** ils sont utilisés pour acheminer les données au sein d'un système autonome. Il s'agit des protocoles suivants:
RIP (Routing Information Protocol) qui est un protocole à vecteur de distance, *IGRP (Interior Gateway Routing Protocol)* et *EIGRP (Enhanced Interior Gateway Routing Protocol)* qui sont des protocoles de rouage à vecteur de distance développés et propriétaire à Cisco, *IS-IS (Intermediate System-to-Intermediate System)* et *OSPF (Open Shortest Path First)* qui sont des protocoles de routage à état de liens **[25]**.

2. ***Les protocoles EGP (Exterior Gatway Protocols) :*** ils sont utilisés pour l'acheminement des données entre les systèmes autonomes. Le protocole internet à vecteur de distance *BGP (Border Gateway Protocol)* est un exemple de ce type de protocole **[25]**.

Pour notre cas nous allons travailler sur les protocoles IGP (RIP, OSPF et EIGRP), qui sont les plus utilisés.

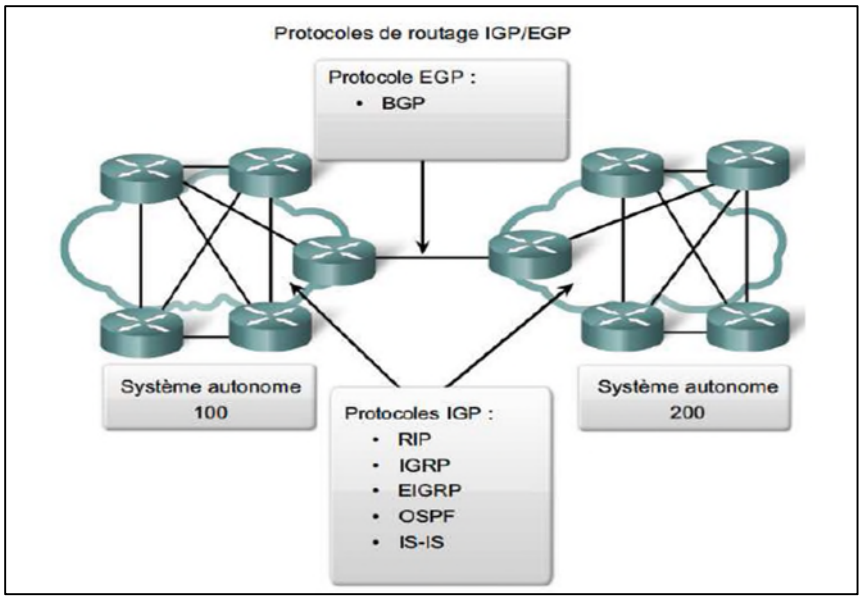


Figure 1.10 : Les protocoles de routage IGP/EGP.

1.9 Protocole de routage à vecteur de distance et à état de liens [8]

Ces deux modes de routage sont nommés *« Algorithmes de routage au moindre coût »* où chaque nœud tient à jour des tables indiquant quel est le plus court chemin pour atteindre le nœud de destination. Chaque lien à un coût affecté ou calculé. À partir de ces informations de coût, chaque routeur détermine le chemin optimal pour joindre une destination.

Ce coût ou métrique peut être exprimé en : nombre de sauts, distance réelle (Kilomètre), temps de latence dans les files d'attente, en délai de transmission, etc.

Les algorithmes de routage au moindre coût diffèrent selon la manière dont ils prennent en compte ces coûts pour construire les tables de routage et nous distinguons deux types d'algorithmes qui sont : *Algorithme à vecteur de distance* et *algorithme à état de lien*.

1.9.1 Protocole de routage à vecteur de distance [8]

Dans le routage à vecteur de distance ou routage de Bellman-Ford *(distance vector routing*), chaque nœud du réseau maintient une table de routage qui comporte une entrée par nœud du réseau et le coût pour joindre ce nœud. Périodiquement chaque nœud diffuse sa table de routage à ses voisins.

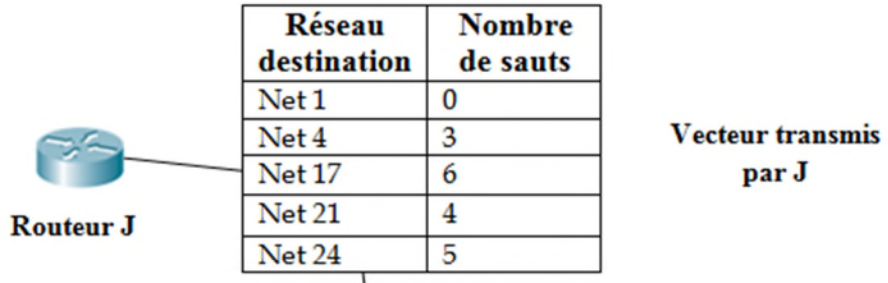
Le nœud destinataire apprend ainsi ce que son voisin est capable de joindre. A la réception, il compare les informations reçues à sa propre base de connaissance et deux cas se présentent :

1. Si la table reçue contient une entrée inconnue, il incrémente le coût de cette entrée du coût affecté au lien par celui qui vient de recevoir de cette table et met cette nouvelle entrée dans sa table. Il a ainsi appris une nouvelle destination.
2. Si la table contient une entrée qu'il connaît déjà et si le coût calculé (coût reçu incrémenté du coût du lien) est supérieur à l'information qu'il possède, il ignore cette information, sinon il met sa table à jour de la nouvelle valeur de cette entrée.

1.9.1.1 Exemple d'application de l'algorithme à vecteur de distance

Dans l'exemple donné (figure 1.11), le routeur A reçoit à un instant donné le vecteur contenant les routes connues par le routeur voisin J. Le routeur A examine chaque route transmise et effectue si nécessaire une mise à jour de sa table de routage.

Ainsi, l'entrée pour atteindre le réseau 4 est modifié car le routeur J connaît une route plus courte. Le nombre de saut transmis est de 3, le routeur A ajoute 1 saut pour aller jusqu'à J. Une nouvelle entrée pour atteindre le réseau 21 est également ajoutée **[6]**.



Réseau destination	Nombre de sauts
Net 1	0
Net 4	3
Net 17	6
Net 21	4
Net 24	5

Routeur J

Vecteur transmis par J

Table de A avant

Réseau destination	Prochain routeur	Nombre de sauts
Net 1	Direct	0
Net 2	Direct	0
Net 4	Routeur L	8
Net 17	Routeur M	5
Net 24	Routeur J	6
Net 30	Routeur K	2

Routeur A

Table de A après

Réseau destination	Prochain routeur	Nombre de sauts
Net 1	Direct	0
Net 2	Direct	0
Net 4	Routeur J	4
Net 17	Routeur M	5
Net 21	Routeur J	5
Net 24	Routeur J	6
Net 30	Routeur K	2

Figure 1.11 : Exemple d'application de l'algorithme à vecteur de distance.

1.9.2 Protocole de routage à état de liens

Le principal inconvénient du routage à vecteur de distance provient du fait que les routeurs n'ont la connaissance d'un changement d'état du réseau que lorsque leur voisin le leur communique, ce qui peut être long **[8]**.

Les protocoles à état de liens ont été conçus pour pallier les limitations des protocoles de routage à vecteur de distance. Ils ont pour avantage de répondre rapidement aux moindres changements sur le réseau en envoyant des mises à jour déclenchées uniquement après qu'une modification soit survenue qui sont nommées *LSA (Link State Advertisement).* Ces protocoles utilisent un algorithme plus efficace *(Dijkstra ou Shortest Path First)* pour déterminer le plus court chemin pour toutes les destinations à partir d'une même source **[34]**.

La figure 1.12 montre un exemple d'application de cet algorithme. Tous les routeurs possèdent à un instant donné la même table des liens. Si le routeur A veut envoyer un paquet vers le routeur C, il calcule le plus court chemin vers C et sélectionne en conséquence le routeur B pour lui envoyer le paquet; B trouve à son tour le plus court chemin vers C qui est direct **[6]**.

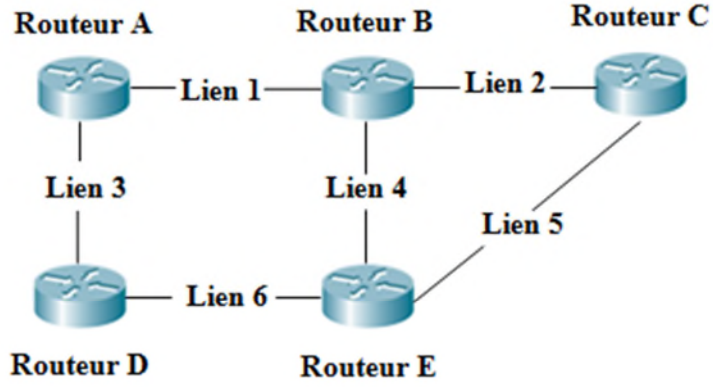


Table des liens

De	à	Lien	Distance
A	B	1	1
A	D	3	1
B	A	1	1
B	C	2	1
B	E	4	1
C	B	2	1
C	E	1	1
D	A	3	1
D	E	6	1
E	B	4	1
E	C	5	1
E	D	6	1

Figure 1.12 : Exemple d'application de l'algorithme état de liens.

1.10 Etat de liens ou vecteur de distance [7]

Les deux principales classes d'algorithmes d'IGP sont « à vecteur de distance » et « l'état de liens ». La première calcule le meilleur chemin selon sa longueur (généralement

exprimée en nombre de routeurs traversés). La seconde calcule le meilleur chemin selon une fonction de coût (le meilleur délai de traversée par exemple).

Ces deux types de protocoles de routage ont pour but de trouver des routes parmi les systèmes autonomes. Ils utilisent des méthodes différentes pour accomplir les mêmes tâches.

Nous allons étudier quelques éléments d'analyse et de comparaison de ces deux familles : *rapidité de convergence de l'algorithme*, *possibilités de métriques différentes*, *choix d'un chemin parmi plusieurs équivalents* et *l'utilisation des routes externes*.

1) Convergence rapide de l'algorithme et sans boucle: Dans un algorithme à vecteur de distance, le nombre d'itérations est proportionnel au nombre de routeurs. Dans le pire cas, il est égal au nombre de routeurs moins 1. Dans un algorithme à état des liens, la convergence s'établit en deux phases : transmission rapide des nouvelles informations puis calcul local du chemin. De plus, cette méthode évite les boucles, puisque tous les chemins calculés sont sains **[7]**.

Les protocoles à état de liens offrent une convergence plus rapide et une meilleure utilisation de la bande passante. Ils prennent en charge la technique VLSM (Variable Length Subnet Mask). Ils sont ainsi adaptés pour les réseaux complexes et évolutifs **[26]**.

2) Métriques multiples : Dans les protocoles à état des liens, plusieurs métriques peuvent êtres supportées en parallèle, sans ralentir la convergence. Cela provient du fait que la topologie est complètement connue pendant le calcul des chemins. Nous pouvons donc choisir la meilleure route en fonction de critères différents, en appliquant des métriques différentes **[7]**.

3) Chemins multiples : Dans un protocole à vecteurs de distance, le choix d'un chemin parmi plusieurs se fait au hasard de la chronologie des échanges de messages. De plus, il n'est prévu qu'un seul routeur suivant dans la table de routage. Malgré une légère modification de l'algorithme, les protocoles à état des liens peuvent tolérer des chemins multiples. Nous pouvons ainsi répartir le trafic entre plusieurs chemins équivalents en termes de coûts. L'équilibrage du trafic dans le réseau est une valeur ajoutée considérable, car elle contribue à la fluidité de la circulation des données et permet un réel contrôle de congestion **[7]**.

L'équilibrage de charge (trafic) est configuré lorsqu'une table de routage ou un routeur dispose de plusieurs chemins vers un réseau de destination avec une mesure (nombre de sauts, bande passante, etc.) équivalente, et ce dans le but d'améliorer l'efficacité et les performances du réseau. L'équilibrage de charge peut être configuré pour utiliser à la fois des protocoles de routage dynamique et des routes statiques **[44]**.

4) Routes externes : Une route externe est une route qui passe par d'autres zones ou d'autres réseaux que celui dans lequel on se trouve. Dans les grands réseaux (Internet par exemple), la connectivité se réalise à travers plusieurs points d'accès à différents réseaux de transit. Les éléments du choix des routes deviendraient trop complexes dans un protocole à vecteurs de distance : il faudrait prendre en compte plusieurs points d'accès, utiliser une route par défaut, etc. Avec la possibilité d'utiliser des métriques multiples, les calculs de chemins intégrant des routes externes se font plus naturellement dans les protocoles à état des liens **[7]**.

1.11 Synthèse

Il est nécessaire de bien comprendre le rôle fondamental du routage. Cette technique est l'action d'acheminer correctement, et de façon optimale, les paquets à travers différents réseaux.

Il existe deux techniques de routage, à savoir le routage dit *« Statique »* et le routage *«Dynamique »*. La différence entre ces deux modes est la façon dont ils acheminent les paquets. Le premier se base sur des routes entrées une à une par l'administrateur réseau et le second utilise un protocole de routage pour déterminer quel est le meilleur chemin à utiliser.

Il y a deux grandes familles d'algorithmes de routage : ceux à vecteur de distance qui calculent le plus court chemin au sens du nombre de routeurs traversés en utilisant l'algorithme du plus court chemin *(SPF pour Shortest Path First),* ceux à états de liens qui estiment le coût des différents tronçons du réseau. Contrairement aux protocoles de routage à vecteur de distance, les protocoles de routage à états de liens possèdent une vue complète de la topologie du réseau. Ils ont une vue détaillée sur les routeurs distants et les réseaux qui leur sont connectés.

Les routeurs échangent entre eux des informations de contrôle dont le but est la construction d'une table de routage pour chacun. Cette table donne, pour chaque destination, la route à emprunter ainsi que son coût. Pour faciliter les opérations de routage, les réseaux sont découpés en systèmes autonomes et le problème est d'abord résolu à l'intérieur d'un

système puis entre deux systèmes, éventuellement avec des protocoles différents pour transporter les informations de routage.

1.12 Conclusion

Le but de ce chapitre était d'introduire les concepts liés aux réseaux informatiques, ceci nous a consenti d'approfondir nos perceptions dans ce domaine.

Nous avons présenté leur définition et leur intérêt, leurs topologies ainsi que les deux types d'architectures. Nous avons vu également le routage qui a un rôle important dans les réseaux et cela pour permettre aux paquets de données de choisir le chemin à suivre pour atteindre la destination. Les différents protocoles de routage et les deux familles d'algorithme de routage ont été démontrés dans ce chapitre.

Le chapitre suivant sera consacré à la présentation de l'entreprise *Cevital* où se déroule notre stage.

CHAPITRE 2

Présentation de l'entreprise

2.1 Introduction

CEVITAL s'est constituée autour de l'idée forte de bâtir un ensemble industriel intégré, concentré en première partie dans le secteur de l'agroalimentaire **[46]**.

Ayant parfaitement réussi dans leur projet initial qui était la fabrication d'huile, margarine et sucre, les gérants de cette entreprise ont décidé de réinvestir leurs bénéfices dans d'autres projets. C'est ainsi que la société est arrivée à en lancer une dizaine dans différents domaines. Ses unités sont installées dans différentes régions du pays. Elle a aussi racheté certaines entreprises comme : le complexe COJEC **[12]**.

Ce chapitre est consacré à la présentation de l'état actuel de la plateforme du réseau et le matériel utilisé de l'entreprise. En premier lieu, nous allons présenter un historique de celle-ci, ensuite nous aborderons ses différentes caractéristiques , ainsi que son organigramme qui illustre les postes représentant cette société.

2.2 Présentation du groupe Cevital [45]

Cevital est un ensemble industriel intégré, concentré en premier lieu dans le secteur de l'agroalimentaire dont le raffinage d'huile et de sucre, produits dérivés, négoce de céréales et distribution de produits destinés à l'alimentation humaine et animale.

L'ensemble industriel a connu une croissance importante et a consolidé sa position de leader dans le domaine agroalimentaire. Il poursuit sa croissance et exploite les groupes en poussant l'intégration des activités agroalimentaires.

Cevital est une société par actions *(SPA)* et a été crée le *12 mai 1998*, l'apparition de celle-ci en tant qu'organe industriel actif, remonte au *14 aout 1999*.

2.3 Le complexe agroalimentaire de Cevital [12]

Le complexe de production se situe dans le port de BEJAIA et s'étend sur une superficie de *45 000 M^2*.

Il a une capacité de stockage de *182 000 tonnes/an* (Silos portuaire), et un terminal de déchargement portuaire de *200 000 tonnes/heure* (réception de matière première). Comme il possède un réseau de distribution de plus de *52 000* points de vente sur tout le territoire national. Exportations Vers l'Europe, le Maghreb et Moyen-Orient. La capacité de production de la raffinerie est de *600* tonnes/jour, pouvant passer après extension à *1200 tonnes/jour*. Cette raffinerie est conçue pour traiter toutes les qualités d'huiles comestibles tel que : le colza, le tournesol, l'olive, le soja etc.

2.4 La structure hiérarchique de Cevital

Cevital est structurée d'une direction générale à la tête de plusieurs directions composées chacune de nombreux services. La direction générale veille sur la sécurité et la gestion optimale de ses ressources.

L'organisation mise en place consiste en la mobilisation des ressources humaines matérielles et financières pour atteindre les objectifs demandés par le groupe. Pour assurer une telle mission, la direction générale est subordonnée de deux directions assistantes : Assistante de la direction générale, d'un secrétariat et elle est composée de quinze directions **[12]**.

2.4.1 Présentation des directions de Cevital

2.4.1.1 La direction Marketing

Pour atteindre les objectifs de l'Entreprise, le Marketing Cevital pilote les marques et les gammes de produits. Son principal objectif est la connaissance des consommateurs, leurs besoins, leurs usages et de veiller sur les marchés internationaux et la concurrence.

Les équipes de marketing produisent des recommandations d'innovation, de rénovation et d'animation publi-promotionnelle sur les marques de Cevital. Une fois ces recommandations, validées elles sont mises en œuvre par des groupes de projets pluridisciplinaires (Développement, Industriel, Approvisionnement, Commercial, Finances) qui sont coordonnés par le Marketing, jusqu'au lancement des différentes marques et à son évaluation **[12]**.

2.4.1.2 La direction des Ventes et Commerciale

Elle a en charge de commercialiser toutes les gammes de produits et le développement du fichier clients de l'entreprise, au moyen d'actions, de détection ou de promotion de projets à base de hautes technologies **[12]**.

2.4.1.3 La direction Système d'information [12]

Elle assure la mise en place des moyens des technologies de l'information nécessaires pour supporter et améliorer l'activité, la stratégie et la performance de l'entreprise. Elle doit ainsi veiller à la cohérence des moyens informatiques et de communication mises à la disposition des utilisateurs, à leur mise à niveau, à leur maîtrise technique et à leur disponibilité et opérationnalité permanente et cela en toute sécurité.

Cette direction définit, également, dans le cadre des plans pluriannuels les évolutions nécessaires en fonction des objectifs de l'entreprise et des nouvelles technologies.

2.4.1.4 La direction des Finances et Comptabilité

Elle a comme tâche de préparer et mettre à jour les budgets, tenir la comptabilité et préparer les états comptables et financiers selon les normes, pratiquer le contrôle de gestion et faire le reporting périodique **[12]**.

2.4.1.5 La direction Industrielle [12]

Elle est chargée de l'évolution industrielle des sites de production et définit, avec la direction générale, les objectifs et le budget de chaque site. Elle analyse les dysfonctionnements sur chaque site (équipements, organisation...) et recherche les solutions techniques ou humaines pour améliorer en permanence la productivité, la qualité des produits et des conditions de travail. Elle anticipe les besoins en matériel et supervise leur achat (étude technique, tarif, installation...). Elle est aussi responsable de la politique environnement et sécurité et participe aux études de faisabilité des nouveaux produits.

2.4.1.6 La direction des Ressources Humaines [12]

Elle définit et propose à la direction générale les principes de gestion ressources humaines en support avec les objectifs du business et en ligne avec la politique RH groupe.

Cette direction assure un support administratif de qualité à l'ensemble du personnel de cevital. Elle pilote les activités du social, assiste à la direction générale ainsi que tous les managers sur tous les aspects de gestion ressources humaines. Elle garantit également le recrutement, chargé de la gestion des carrières et identifie les besoins en mobilité.

2.4.1.7 La direction Approvisionnements [12]

Dans le cadre de la stratégie globale d'approvisionnement et des budgets alloués (investissement et fonctionnement), cette direction met en place les mécanismes permettant de satisfaire les besoins en matières et en services dans les meilleurs délais, avec la meilleure qualité et au moindre coût afin de permettre la réalisation des objectifs de production et de vente.

2.4.1.8 La direction Logistique [12]

Cette direction expédie les produits finis (sucre, huile, margarine, Eau minérale, …), qui consiste à charger les camions à livrer aux clients sur site et des dépôts logistique. Elle assure et gère le transport de tous les produits finis, que ce soit en moyens propres (camions de Cevital), ou en moyens de transport des clients.

Le service transport assure aussi l'alimentation des différentes unités de production en quelques matières premières intrants et packaging et le transport pour certaines filiales du groupe (MFG, SAMHA, Direction Projets, NUMIDIS, etc.). Elle gère les stocks de produits finis dans les différents dépôts locaux (Bejaia et environs) et régionaux (Alger, Oran, etc.).

2.4.1.9 La direction des Silos

Cette direction décharge les matières premières vrac arrivées par navire ou camions vers les points de stockage et stocke dans les conditions optimales les matières premières. Elle expédie et transfère vers les différents utilisateurs de ces produits dont l'alimentation de raffinerie de sucre et les futures unités de trituration et fait également l'entretient et maintient en état de services les installations des unités silos **[12]**.

2.4.1.10 La direction des Boissons

Le Pôle Boissons et plastiques comprend trois unités industrielles situées en dehors du site de Béjaia **[12]**:

Unité *LALLA KHEDIDJA* domiciliée à *Agouni-gueghrane* (Wilaya de *TIZI OUZOU*) a pour vocation principale la production d'eau minérale et de boissons carbonatées à partir de la célèbre source de *LLK*.

Unité *plastique*, installée dans la même localité, assure la production des besoins en emballages pour les produits de Margarine et les Huiles et à terme des palettes, des étiquettes etc.

Unité *COJEK*, implantée dans la zone industrielle d'El KSEUR, Cojek est une SPA filiale de Cevital et qui a pour vocation la transformation de fruits et légumes frais en Jus, Nectars et Conserves.

2.4.1.11 La direction Corps Gras

Le pole corps gras est constitué des unités de production suivantes : une raffinerie d'huile de 1800 T/J, un conditionnement d'huile de 2200T/J, une margarinerie de 600T/J qui sont toutes opérationnelles et une unité inter estérification – Hydrogénation –pate chocolatière –utilités actuellement en chantier à El kseur. La mission principale de cette direction est de raffiner et de conditionner différentes huiles végétales ainsi que la production de différents types de margarines et beurre. Tous ces produits sont destinés à la consommation d'où la préoccupation de cette direction est de satisfaire le marché local et celui de l'export qualitativement et quantitativement **[12]**.

2.4.1.12 La direction Pôle Sucre

Le pôle sucre est constitué de quatre unités de production : une raffinerie de sucre solide 2000T/J, une raffinerie de sucre solide 3000T/J, une unité de sucre liquide 600T/J et une unité de conditionnement de sucre 2000 T/J qui a été mise en service Mars 2010. Sa

vocation est de produire du sucre solide et liquide dans le respect des normes de qualité, de la préservation du milieu naturel et de la sécurité des personnes. Ses produits sont destinés aux industriels et aux particuliers et ce pour le marché local et à l'export **[12]**.

2.4.1.13 La direction QHSE

Cette direction met en place, maintient et améliore les différents systèmes de management et référentiels pour se conformer aux standards internationaux, veille au respect des exigences règlementaires produits, environnement et sécurité.

Elle garantit la sécurité du personnel de l'entreprise et la continuité des installations et contrôle et assure la qualité de tous les produits de Cevital afin de réponse aux exigences clients **[12]**.

2.4.1.14 La direction Energie et Utilités

Cette direction a pour objet, la production et la distribution pour les différentes unités, avec en prime une qualité propre à chaque Process : D'environ 450 m3/h d'eau (brute, osmosée, adoucie et ultra pure) ; de la vapeur *Ultra haute pression* 300T/H et *basse pression* 500T/H. De l'Electricité *Haute Tension*, *Moyenne Tension* et *Basse Tension*, avec une capacité de 50MW **[12]**.

2.4.1.15 La direction Maintenance et travaux neufs [12]

Elle gère et déploie avec le Directeur Industriel et les Directeurs de Pôles les projets d'investissement relatifs aux lignes de production, bâtiments et énergie/utilité (depuis la définition du process jusqu'à la mise en route de la ligne ou de l'atelier). Elle rédige les cahiers des charges en interne et négocie avec les fournisseurs et les intervenants extérieurs.

Cette direction met en place et intègre de nouveaux équipements industriels et procédés, planifie et assure la maintenance pour l'ensemble des installations.

2.5 Organigramme de l'entreprise

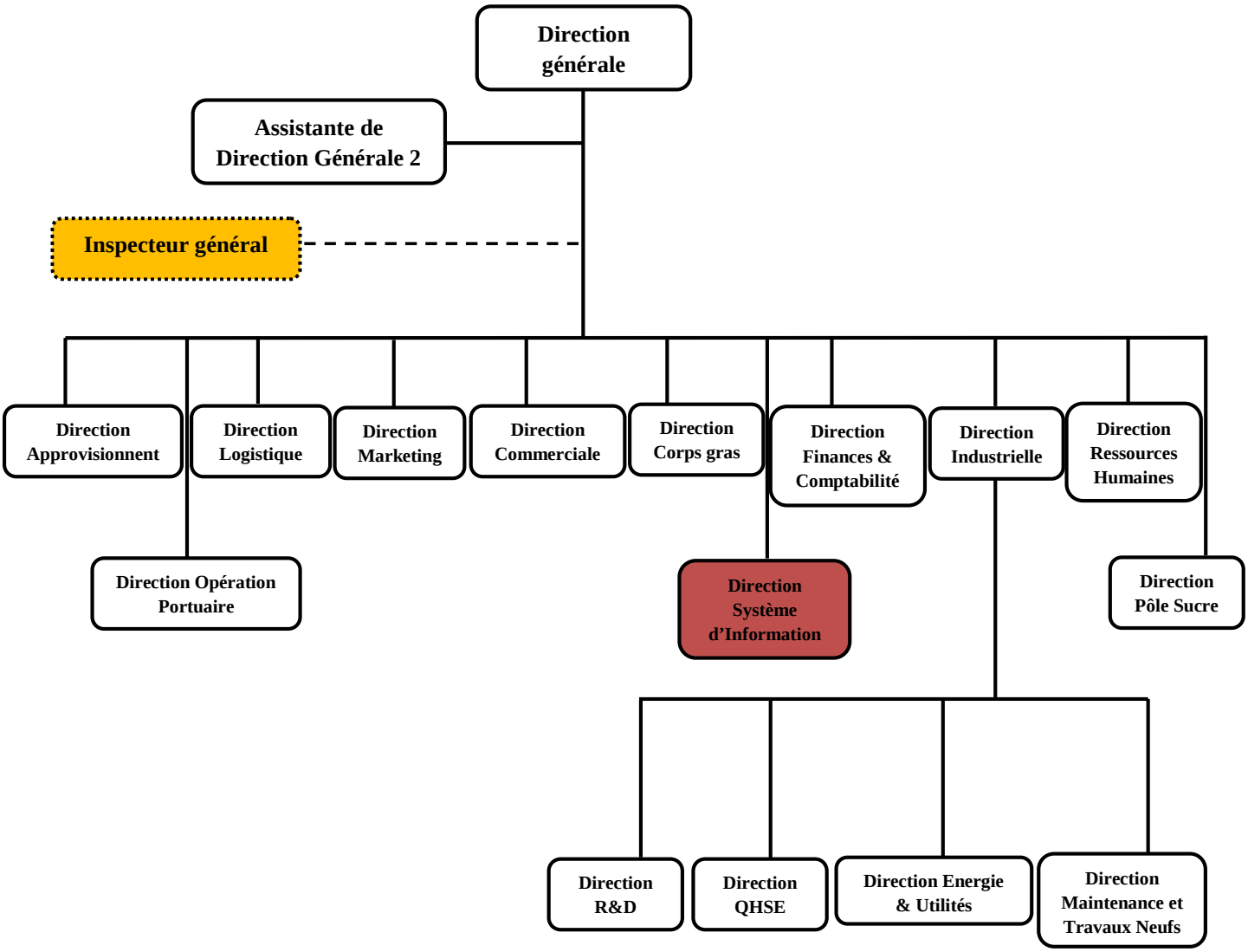


Figure 2.1 : Organigramme général de CEVITAL.

2.6 Architecture du réseau informatique de Cevital

Cevital dispose d'un réseau commuté de taille importante composé d'une plateforme de services reliant les sites locaux dans chacune des entités physiques. Il est constitué de plusieurs équipements dont : un seul Switch *(EntherSwitvh router)* qui a une architecture réseau en étoile, des routeurs et des Firewall, pour la plupart de marque Cisco, ainsi que des équipements satellitaires VSAT *(Very Small Aperture Terminal)* pour établir la communication entre les différents sites interconnectés.

Cette architecture est également composée des opérateurs *SLC* et *Anwarnet* qui sont utilisés comme étant des liaisons d'accès à Internet avec des adresses IP publics.

2.6.1 Les équipements de la topologie

2.6.1.1 Définition d'un routeur [60]

Un routeur est un matériel de communication de réseau informatique destiné au routage. Il est responsable de la transmission de paquets à travers différents réseaux et de déterminer le prochain nœud du réseau auquel un paquet de données doit être envoyé.

La destination du paquet IP peut être un serveur Web se trouvant dans un autre pays ou un serveur de messagerie situé sur le réseau local. Les routeurs doivent transmettre ces paquets de manière rapide et efficace.

2.6.1.2 Définition d'un EntherSwitvhrouter

Les modules Cisco EtherSwitch offrent aux entreprises la possibilité d'intégrer sur une même plateforme la commutation et le routage. Ils réunissent le routage de réseau WAN de niveau 3 avec la commutation non bloquante de niveau 2, ils associent également la simplicité de configuration, la facilité de déploiement et l'administration intégrée **[62]**.

2.6.1.3 Définition d'un firewall

Un pare-feu *(firewall)*, est un outil informatique (matériel et/ ou logiciel) conçu pour protéger un ordinateur ou un réseau d'ordinateurs des intrusions provenant d'un réseau tiers (notamment internet). Il permet d'assurer la sécurité des informations d'un réseau en filtrant les paquets de données échangés avec le réseau **[63]**.

2.6.1.4 Définition d'un DMZ

Dans les réseaux informatiques une zone démilitarisée *(Demilitarized Zone*) est un sous-réseau séparé du réseau local de l'entreprise et du réseau public extérieur (Internet)

par un pare-feu, qui permet d'empêcher les utilisateurs externes d'avoir accès directement à un serveur qui contient des données de l'entreprise, donc le pare-feu bloquera les accès au réseau local pour garantir sa sécurité et les services capables d'être accédés depuis Internet seront situés en DMZ **[63]**.

2.6.1.5 Définition de SLC et Anwarnet [65]

SLC *(Smart Link Communication)* est l'opérateur de WiMAX et Large Bande des entreprises en Algérie, qui permet à ces deniers de partager, traiter et stocker des informations principales à leurs activités en toute sécurité. Il met à la disposition de ses clients une ressource qui combine un réseau WiMAX et Large Bande, une infrastructure IT des réseaux et des solutions de télécommunications.

AnwarNet est un fournisseur d'accès à Internet et opérateur de Téléphonie (VOIP) en Algérie.

2.6.1.6 Définition d'un VSAT

Le VSAT *(Very Small Aperture Terminal)* est un système qui repose sur le principe d'un site principal (le hub) et d'une multitude de points distants (les stations VSAT).
Le hub est le point le plus important du réseau, c'est par lui que transite toutes les données qui circulent dans celui-ci, il est structuré d'une antenne et plusieurs appareils. C'est aussi lui qui gère tous les accès à la bande passante **[64]**.

1. Avantages du VSAT [64]

L'avantage présenté par les solutions satellites est que les stations terrestres ne dépendent plus des infrastructures terrestres existantes à travers le monde et donc peuvent être mobiles. Par ailleurs il est possible de diffuser facilement et de façon économique (en bande) depuis un satellite la même information à de nombreuses stations ou à l'inverse relayer depuis un satellite la synthèse de multiples sources terrestres ou spatiales.

L'évolutivité est aussi un avantage de ce système. En effet, connecter un nouveau point, ne demande pas de gros moyens techniques et financiers.

Comme le hub est le point central de tout le réseau, et en assure la gestion complète. Ceci permet donc de gérer et de superviser l'ensemble du réseau d'un seul et même point.

2. Inconvénients du VSAT [64]

Le principal inconvénient du VSAT est son coût. Cette barrière financière relativement importante limite l'accès à la technologie.

Le fait que toutes les communications passent par le hub et si celui-ci tombe en panne tout le réseau est paralysé et plus une communication ne peut se faire.

Lors du choix d'un satellite, si une zone où un point du réseau doit être connecté prochainement n'est pas couverte, elle ne le sera jamais avec ce satellite, alors que les réseaux filaires évoluent régulièrement ce qui laisse possible l'extension d'un réseau dans des zones qui ne sont pas desservies.

La figure 2.2 suivante illustre l'architecture réseau de l'entreprise , avec présentation de l'interconnexion des différentes unités de production situées dans de différentes régions, à savoir : Alger, Bejaia, Constantine, Elkseur, LLK et Oran de celle-ci :

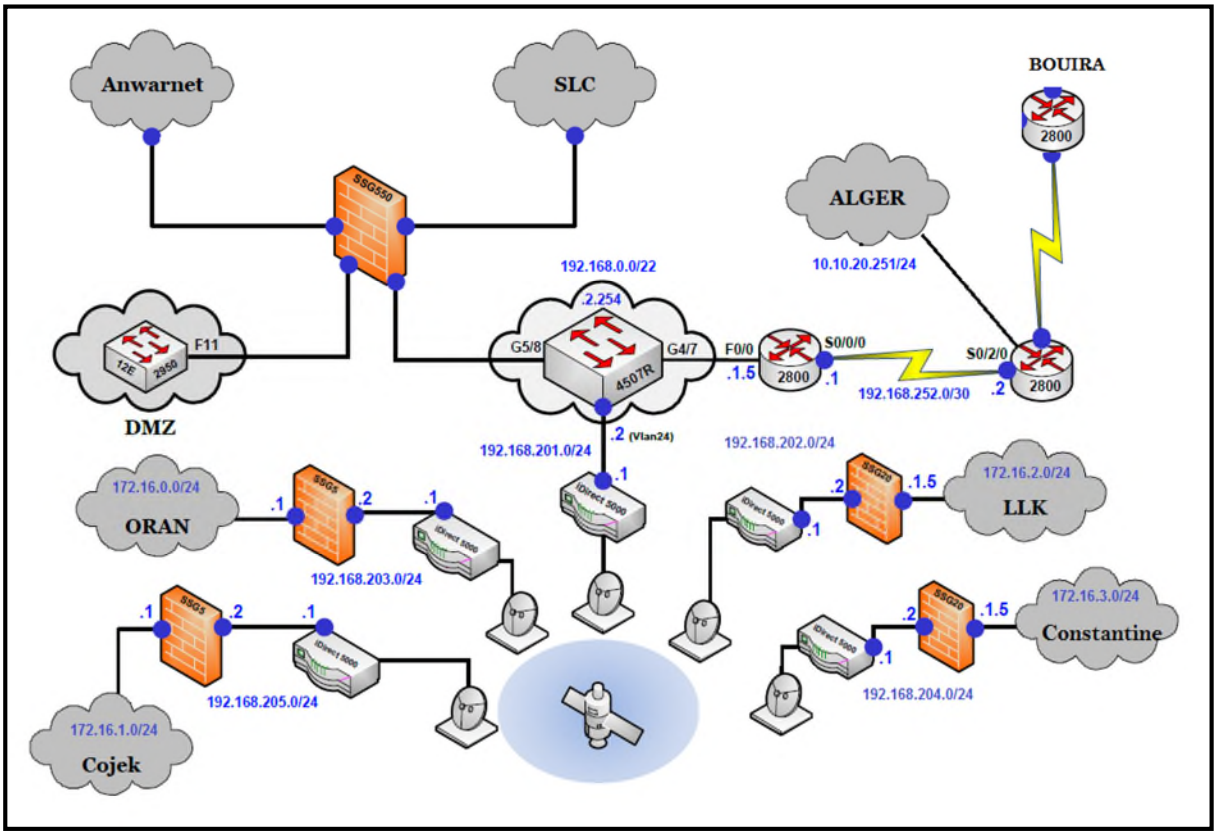


Figure 2.2 : Schéma d'interconnexion réseaux.

La configuration des différents éléments d'interconnexion dans l'entreprise se fait avec l'utilisation du protocole de routage dynamique EIGRP, avec l'ajout des routes statiques vers quelques destinations.

L'un des points forts du routage statique est la facilitée de la configuration par l'administrateur en raison de l'inexistence de la demande de configuration d'un protocole de routage. Néanmoins ce type de routage présente des inconvénients parmi lesquels :

La configuration et les mises à jour (ajout ou suppression d'un élément) prennent du temps , car elles se font manuellement et nécessite l'intervention d'un administrateur réseau.

La complexité augmente avec la taille du réseau. En effet, la configuration manuelle d'un grand nombre d'éléments provoque le risque d'erreurs, donc l'administrateur doit avoir une connaissance complète du réseau.

Cevital utilise des équipements d'interconnexion de type Cisco. Par conséquent, l'administrateur réseau a opté pour configurer ces éléments avec l'utilisation du protocole de routage dynamique EIGRP.

C'est un protocole développé par Cisco, de ce fait, c'est un protocole propriétaire réservé qu'aux produits de marque Cisco. Il ne peut par conséquent être configuré sous une autre plateforme.

La gestion du réseau est à la charge de la direction informatique qui doit veiller à son bon fonctionnement. Cependant, l'augmentation continuelle de la taille du réseau le rend de plus en plus difficile à maintenir dans un état de marche. Pour assurer un routage fiable, le routage statique n'est pas le mieux adapté et avec l'évolution des protocoles de routage et la naissance de nouveaux protocoles mieux appropriées à toutes les plateformes (Cisco, Juniper, etc.). Cette raison, nous a poussé à proposer la configuration des éléments de l'architecture réseau conforme à la topologie avec d'autres protocoles en plus du protocole EIGRP à savoir : RIPv2 et OSPF.

Une étude comparative entre ces trois protocoles sera introduite au chapitre 3 par la sélection du protocole le mieux approprié à l'entreprise Cevital.

2.7 Conclusion

Ce chapitre nous a permis non seulement d'avoir une vue détaillée de l'état de la société, mais aussi de se familiariser avec celle-ci où se déroule notre stage. Le chapitre suivant va être consacré à faire une étude et comparaison entre les protocoles IGP.

CHAPITRE 3

Etude et comparaison des protocoles IGP

3.1 Introduction

Au sein d'un système autonome, les routes sont générées par des protocoles de routage intérieurs IGP (*Interior Gateway Protocols)* comme *RIP, IGRP, EIGRP, OSPF* ou *ISIS* **[43]**.

Ce chapitre est consacré à la description et la comparaison des protocoles de routage dynamique interne que nous allons utiliser dans la topologie à mettre en œuvre. Cela consiste à étudier les trois protocoles RIP, OSPF et EIGRP que nous avons choisi en donnant notamment des informations sur les mesures qu'ils utilisent pour déterminer le meilleur chemin, les avantages et limites que présente l'utilisation de chacun de ces protocoles.

Nous présenterons aussi une comparaison entre ceux-ci par rapport à certains critères qui seront élaborés durant ce chapitre.

3.2 Définition des protocoles IGP [27]

Pour chaque système autonome, nous définissons des protocoles de routage interne qui permettent le dialogue entre les routeurs du système, ces protocoles sont nommés : *IGP (Interior Gateway Protocol).*

Les protocoles *IGP* permettent d'échanger des informations de routage au sein d'un système autonome ou d'une organisation individuelle et ils sont exécutés sur les routeurs internes à l'organisation.

L'objectif d'un protocole de routage intérieur consiste à trouver le meilleur chemin possible sur le réseau interne. Les protocoles RIP (v1 et v2), EIGRP et OSPF sont des exemples des protocoles IGP.

3.2.1 Le protocole de routage dynamique RIP

3.2.1.1 Définition de RIP *(Routing Information Protocol)*

C'est un protocole de routage qui s'appuie sur un algorithme de type vecteur de distance qui utilise l'algorithme de *Belman-Ford* pour la mise à jour des tables de routage et puisqu'il calcule la distance, en nombre de routeurs traversés, entre la source et la destination, cela veux dire que chaque routeur échange avec ses voisins des informations de routage en utilisant des paquets de données brodcast *UDP (User Datagram Protocol)* afin de connaître le plus court chemin pour une destination **[36]**.

Un routeur RIP transmet à ses voisins les adresses réseau qu'il connaît (soit les adresses de ses interfaces, soit les adresses découvertes via les autres routeurs) **[10]**.

3.2.1.2 Le format des paquets RIP [47]

La partie donnée d'un message RIP est encapsulée dans un segment UDP, avec les numéros de ports source et de destination définis sur le port N°520. L'en-tête IP et les en-têtes de liaison de données ajoutent des adresses de destination de diffusion avant l'envoi du message à toutes les interfaces RIP configurée.

Le message RIP est constitué de deux parties : La partie en-tête qui est composée de trois champs spécifiés à quatre octets et la parie entrée de route qui est structuré à son tour de trois champs. La figure 3.1 suivante représente le format d'un message RIP :

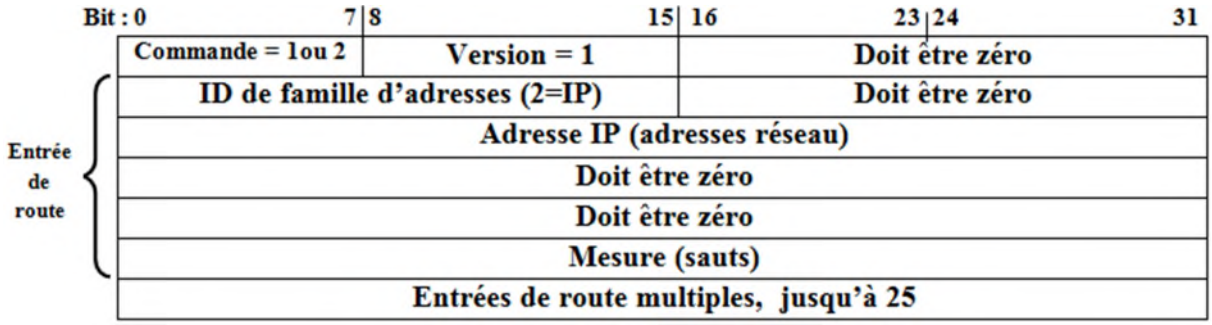


Figure 3.1 : Format de paquet RIPv1 **[47]**.

Les champs d'un paquet RIPv1 sont décrits dans ce qui suit :

1. ***Le champ Commande :*** Identifie le type de message. Le protocole RIP utilise deux types de messages spécifiés dans ce champ: *un message de requête* et *un message de réponse*.
Chaque interface configurée sous RIP envoie un message de requête au démarrage, demandant à ce que tous les voisins RIP envoient leurs tables de routage complètes. Un message de réponse est renvoyé par les voisins RIP. Lorsque le routeur à l'origine de la requête reçoit les réponses, il évalue chaque entrée de route et deux cas se présentent : si une entrée de route est nouvelle, le routeur de réception installe cette route dans la table de routage. Si la route existe déjà dans la table, l'entrée existante est remplacée par la nouvelle si son nombre de sauts est meilleur. Le routeur qui vient de démarrer envoie ensuite une mise à jour déclenchée via toutes les interfaces RIP contenant sa propre table de routage pour communiquer les nouvelles routes aux voisins RIP **[47]**.

2. ***Le champ Version :*** Contient le numéro de version du protocole. Le récepteur l'utilise pour s'assurer qu'il interprète correctement le message et le numéro 1 signifie que le protocole RIP est de version 1 **[47]**.

3. ***Le champ « Doit être à zéro » :*** Les champs « Doit être à zéro » fournissent de la place pour une extension future du protocole **[47]**.

4. ***La partie entrée de route :*** La partie entrée de route du message comprend trois champs avec le contenu suivant : *Identificateur de famille d'adresses* (de valeur 2 pour le protocole IP sauf si un routeur exige une table de routage complète, auquel cas ce champ doit avoir la valeur zéro), *Adresse IP* qui représente l'adresse de la route de destination, qui peut être un réseau, un sous-réseau ou une adresse d'hôte et le champ *Mesure* qui indique le nombre de sauts.

Cette partie du message relative à l'entrée de route représente une route de destination avec sa mesure associée. Une mise à jour RIP peut contenir jusqu'à 25 entrées de route **[47]**.

3.2.1.3 Fonctionnement du protocole RIP [7]

Le protocole RIP est limité aux réseaux dont le plus long chemin implique quinze routeurs au maximum, il utilise des mesures du coût des chemins (ou *métriques*) qui est le nombre de sauts fixes et varient entre 1 et 15 pour comparer les routes alternatives et la valeur 16 correspond à l'infini.

Un routeur RIP calcule des chemins pour différentes destinations, lesquelles sont spécifiées par leurs adresses IP. Le protocole RIP ne spécifie pas le type de l'adresse : les routeurs découvrent la nature du destinataire en analysant les adresses transmises.

Les routeurs RIP sont *actifs* ou *passifs* : Actifs car ils transmettent et reçoivent les routes et diffusent leurs informations aux autres routeurs. Passifs, ils ne font qu'attendre la réception des informations. En fonction de celles-ci, ils calculent leurs tables de routage mais ne partagent pas les résultats de leurs calculs avec d'autres routeurs.

Le routeur RIP actif permet aux autres routeurs de mettre à jour leurs tables de routage toutes les 30 secondes. Si un routeur ne reçoit aucune mise à jour d'un autre routeur dans un délai de 180 secondes, il marque les routes desservies par ce dernier comme inutilisables. S'il n'y a aucune mise à jour après 240 secondes, le protocole RIP supprime toutes les entrées correspondant au routeur qui ne répond pas.

Chaque diffusion RIP contient des paires adresses IP/nombre de routeurs à traverser (ou nombre de *sauts*). Comme le nombre de sauts est la seule mesure utilisée par le protocole, RIP ne garantit pas que le chemin sélectionné soit le plus rapide.

Lorsqu'un événement dans le réseau provoque un changement dans la table de routage d'un routeur actif, celui-ci envoie un message de mise à jour à ses voisins. Si cet événement a un impact sur les voisins, ceux-ci propagent l'information.

3.2.1.4 Amélioration du protocole RIP

1. Description du protocole RIPv2 [48]

La nécessité d'utiliser la notion des masques de sous-réseau de longueur variable *VLSM (Variable Length Subnet Mask)* a incité la définition de la version 2, qui est une amélioration

du protocole RIPv1 mais garde les mêmes caractéristiques de base de celui-ci et remédie à certaines de ces limites.

RIPv2 améliore RIPv1 avec la possibilité d'utiliser VLSM et présente une fonctionnalité de routage *CIDR (Classless InterDomain Routing)*, lui permettant d'envoyer des informations sur les masques de sous-réseau avec la mise à jour des routes, ainsi que l'authentification dans ces mises à jour afin de sécuriser les informations qui circulent dans celui-ci.

2. Format des paquets RIPv2 [48]

À l'instar de la version 1 du protocole RIP, RIPv2 est encapsulé dans un segment UDP via le port 520 et peut transporter jusqu'à 25 routes. Bien que RIPv2 possède le même format de message de base que RIPv1, il y a eu l'exploitation des trois champs : *étiquette de route*, *masque de sous-réseau* et *le saut suivant* pour porter de nouvelles options, ce qui est illustré dans la figure 3.2 qui représente le format du paquet du protocole RIPv2.

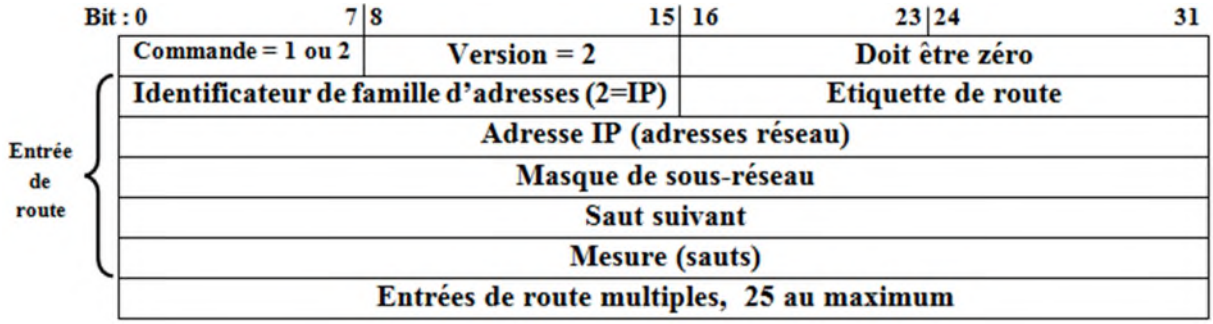


Figure 3.2 : Format de paquet RIPv2 **[47]**.

Les modifications apportées sur le format d'un paquet RIPv1 sont décrits dans ce qui suit **[49]**:

1. ***Champ « Etiquette de route » :*** C'est un attribut affecté à une route qui doit être préservé et nouveau annoncée avec une route. Le but de ce champ est de fournir une méthode permettant de séparer les routes RIP « internes » (vers des réseaux à l'intérieur du domaine de routage RIP) des routes RIP « externes », qui peuvent avoir été importées depuis un EGP ou un autre IGP.

Les routeurs supportant des protocoles différents de RIP devraient être configurables afin de permettre la configuration du marqueur de route pour les routes importées depuis différentes

sources. Par exemple, les routes importées depuis un EGP ou BGP devraient voir leur marqueur de route fixé à une valeur arbitraire, ou au moins au numéro du système autonome depuis lequel elles ont été apprises.

2. Champ «Masque de sous-réseau » : Ce champ contient le masque de sous-réseau qui est appliqué à l'adresse IP et permet de céder la partie non hôte de l'adresse. Si ce champ est égale à zéro, aucun masque de sous-réseau n'a été inclus pour cette entrée.

3. Champ « Saut suivant » : C'est l'adresse IP du saut suivant directement connecté auquel les paquets vers la destination devraient être redirigés. La valeur de 0.0.0.0 est spécifié dans ce champ indiquant que le routage devrait se faire via le routeur à l'origine de l'annonce RIP. Une adresse spécifiée en tant que saut suivant doit, être directement accessible au sous-réseau sur lequel est effectuée l'annonce.

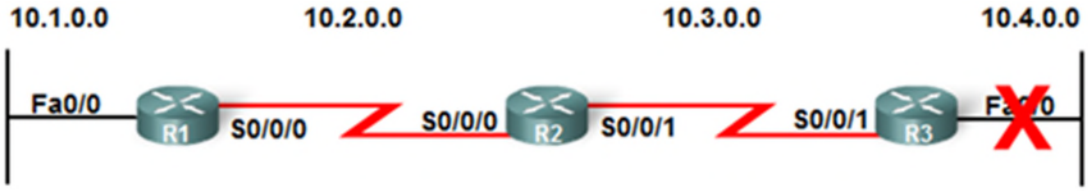
Le but du champ est d'éliminer les paquets routés au travers des sauts supplémentaires dans le système. C'est particulièrement utile quand RIP n'est pas exécuté par tous les routeurs d'un réseau. Le saut suivant est un champ « consultatif », c'est-à-dire que si l'information fournie est ignorée, une route éventuellement sous-optimale, mais néanmoins absolument valide, sera empruntée. Si le prochain saut reçu n'est pas directement accessible, il devrait être traité comme l'est 0.0.0.0.

3.2.1.5 Le problème de comptage à l'infini de RIPv2

C'est une situation qui se produit lorsque des mises à jour de routage inexactes augmentent la valeur de la mesure jusqu'à l'infini pour un réseau qui n'est plus accessible.

Pour arrêter cette incrémentation, l'infini est défini par l'attribution d'une valeur maximale à la mesure. Par exemple, le protocole RIPv2 considère que 16 sauts représentent l'infini, ce qui correspond à une mesure inaccessible. Une fois que les routeurs ont compté jusqu'à l'infini, ils marquent la route comme étant inaccessible.

La figure 3.3 représente un exemple de réseau qui a l'adresse 10.4.0.0 qui n'est plus accessible car le nombre de saut est égal à 16 **[50]**:



Réseau	Interface	Saut
10.1.0.0	Fa0/0	0
10.2.0.0	S0/0/0	0
10.3.0.0	S0/0/0	1
10.4.0.0	S0/0/0	16

Réseau	Interface	Saut
10.2.0.0	S0/0/0	0
10.3.0.0	S0/0/1	0
10.1.0.0	S0/0/0	1
10.4.0.0	S0/0/1	16

Réseau	Interface	Saut
10.3.0.0	S0/0/1	0
10.4.0.0	S0/0/1	16
10.2.0.0	S0/0/1	1
10.1.0.0	S0/0/1	2

Figure 3.3 : Représentation d'un réseau inaccessible.

Pour résoudre le problème du comptage à l'infini, plusieurs solutions ont été proposées :

1. Règle de découpage de l'horizon

Le découpage d'horizon est une méthode qui permet d'empêcher les boucles de routage provoquées par la convergence lente d'un protocole de routage à vecteur de distance. Selon cette règle, un routeur ne doit pas annoncer un réseau par le biais de l'interface dont est issue la mise à jour **[50]**.

1.1 Découpage de l'horizon avec empoisonnement de route

L'empoisonnement de routage est une autre méthode employée par les protocoles de routage à vecteur de distance et son objectif est de marquer la route comme étant inaccessible dans une mise à jour de routage qui est envoyée à d'autres routeurs, c'est-à-dire qu'elle doit être interprété comme une route empoisonnée a une mesure de 16 **[50]**.

1.2 Découpage de l'horizon avec empoisonnement inverse

Selon la règle de découpage d'horizon avec empoisonnement inverse qui est associé à la technique du découpage de l'horizon, lors de l'envoi de mises à jour via une interface spécifique, tout réseau dont l'existence a été apprise sur cette interface est désigné comme étant inaccessible.

Cette technique part du principe qu'il vaut mieux indiquer explicitement à un routeur d'ignorer une route que de lui cacher l'existence de la route **[50]**.

3.2.1.6 Les avantages de RIPv2

Le protocole RIPv2 est fourni et géré gratuitement par tous les routeurs et sa simplicité permet une implémentation facile et rapide. Les risques d'erreurs sont limités et le résultat globale satisfaisant si la topologie du réseau reste simple et les liaisons fiables. Ces avantages font de RIPv2 un protocole de routage très répandu et utilisé **[6]**.

3.2.1.7 Les inconvénients de RIPv2

Le protocole RIP v2 n'autorise pas plus de 15 sauts, de sorte qu'il ne convient qu'aux réseaux qui ne connectent pas plus de 16 routeurs en série. Il envoie périodiquement des copies de la table de routage entière aux voisins directement connectés chaque les 30 seconde ce qui sature le réseau. Dans un grand réseau, cela peut engendrer un trafic réseau important à chaque mise à jour **[42]**.

Pour les réseaux complexes, chaque changement de topologie n'est corrigé que lentement (convergence lente). Pendant le temps nécessaire au calcul, le réseau est dans un état intermédiaire où il peut y avoir des boucles pouvant causer des convergences temporaires **[6]**.

Dans le cas pratique nous allons implémenter le protocole RIP avec sa version 2.

3.2.2 Le protocole de routage dynamique OSPF

3.2.2.1 Définition d'OSPF

Le protocole OSPF *(Open Shortest Path First)* est un protocole à état des liens globalement plus efficace que RIPv2 et qui tend à le remplacer pour le routage interne. Il utilise l'algorithme *SPF (Shortest Path First)* afin d'élire la meilleur route, celle présentant le coût le plus faible sur l'ensemble de ses liens, vers une destination donnée **[6]**.

Pour éviter certains inconvénients du protocole de routage RIPv2 et pour gérer des réseaux complexes, le protocole OSPF est le plus utilisé comme protocole de routage interne dans le monde IP. Dans celui-ci, chaque routeur diffuse sur le réseau les informations décrivant sa topologie locale et cette diffusion permet à chaque routeur d'avoir la totalité de la topologie réseau. Il est également un protocole de routage sans classe qui utilise le concept de zones pour son évolutivité **[11]**.

Les routeurs appliquent l'algorithme de *Dijkstra (Algorithme du Plus Court Chemin)* sur la base de données topologique pour calculer les routes vers toutes les destinations possibles **[11]**.

3.2.2.2 Notion de zones [7]

Le fonctionnement d'OSPF est optimisé si le système autonome est découpé en zones ; il prévoit un découpage avec une hiérarchie à deux niveaux de zones *(Areas).* La zone de niveau le plus élevé est la zone appelée « *backbone zone* » qui interconnecte les routeurs de bordure.

À l'intérieur de chaque zone du second niveau, les routeurs ne connaissent et ne diffusent que des informations internes à leur zone. L'ensemble de ces zones décrit un système autonome.

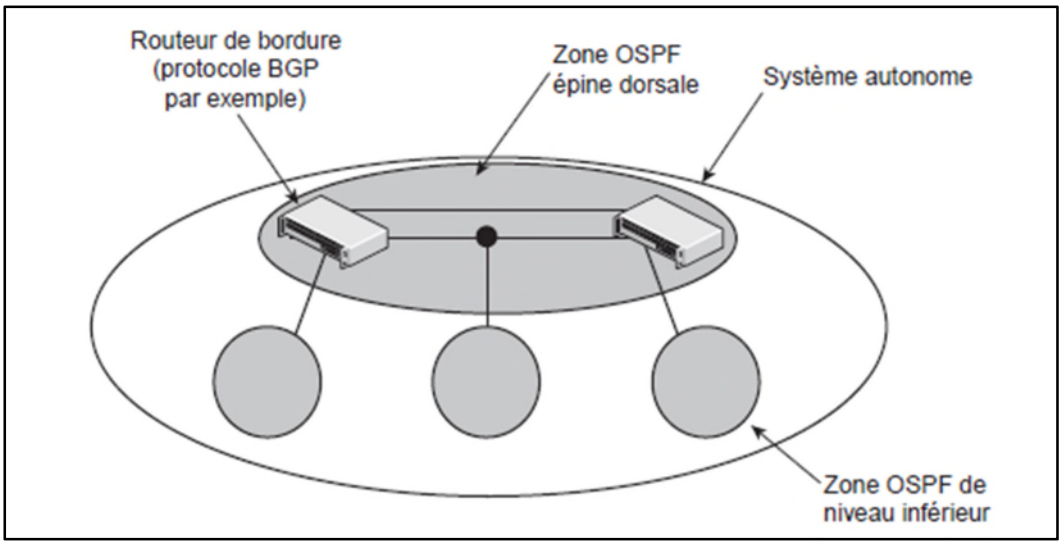


Figure 3.4 : Hiérarchie d'organisation des zones OSPF.

3.2.2.3 Les messages du protocole OSPF

Nous distinguons cinq messages OSPF : *hello, description de base de données, requête d'état de liens, mise à jour d'état de liens* et *acquittement d'état de liens*. Ils transportent des informations sur l'état de liaisons du système autonome et servent à déterminer une fonction de coût plus efficace que dans RIP **[7]** :

1. Message Hello : Un routeur OSPF émet des messages *hello* à intervalles réguliers (environ toutes les dix secondes), sur chacune de ses interfaces. Ces messages établissent les relations d'adjacence avec les routeurs directement liés à l'émetteur de ces messages. Les routeurs qui les ont reçus vérifient que les chemins restent disponibles.

Dans la théorie des graphes, deux nœuds sont adjacents s'ils sont directement reliés. Ici, la notion d'adjacence est légèrement différente, puisqu'elle ajoute une règle supplémentaire : le routeur désigné est adjacent à tous les autres. C'est l'efficacité qui

prévaut : dans un réseau local, il est inutile que tous les routeurs participent au routage, seul l'un entre eux est le routeur désigné, tous les autres lui sont adjacents **[7]**.

2. Message « description de base de données (DBD) »: Sur un réseau possédant au moins deux routeurs, un routeur désigné est élit, c'est-à-dire le responsable qui échange avec les routeurs des réseaux voisins. Il s'occupe de la distribution des messages de mise à jour d'état de liens. Son choix se fait sur la base de la plus petite adresse IP parmi les routeurs susceptibles d'assumer ce rôle.

Deux routeurs *R1* et *R2* établissent une relation d'adjacence si et seulement s'ils sont reliés par un lien direct ou si l'un d'entre eux est routeur désigné. Lorsqu'une nouvelle adjacence s'établit entre deux routeurs, ils synchronisent leurs bases de données d'état de liens par ce type de message **[7]**.

3. Message « requête d'état de liens (LSR-Link-State Request) »: Chaque enregistrement est associé par une temporisation : l'information contenue dans l'entrée de la table de routage sera supprimée si elle n'a pas été rafraîchie récemment. Quand un routeur constate qu'une ou plusieurs des entrées de sa base de données sont périmées, il envoie une *requête d'état de liens* aux routeurs voisins pour faire la mise à jour des données **[7]**.

4. Message « mise à jour d'état de liens (LSU-Link-State Update)» : Ces paquets sont utilisés pour la mise à jour du routage OSPF. Un paquet LSU peut contenir dix types différents d'annonces d'état de liaisons LSA et nous allons illustrer certains dans le tableau 3.1, toutes les LSU contiennent une ou plusieurs LSA **[51,18]**.

5. Message « acquittement d'état de liens (LSA-Link-State Advertisements) » : C'est l'accusé de réception d'une mise à jour : le routeur qui a envoyé ses indications de coût vers ses voisins sait que le message est bien parvenu. La transmission des messages de *description de base de données* est sécurisée : chaque enregistrement est protégé par un total de contrôle et tous les messages sont authentifiés.

Cela évite d'éventuels messages qui contiendraient des informations erronées probablement malveillantes **[7]**.

Types de LSA	*Explication*
Type 1	Le premier type de LSA est émis et propagé par chaque routeur dans une aire. Il contient tous ses liens, avec leurs statuts et leurs coûts.
Type 2	Ce type est transmis et propagé par un routeur désigné dans une aire, il contient également le préfixe du réseau et les identifiants des autres routeurs du réseau.
Type 3	Le troisième type de LSA est émis et propagé par un ABR dans l'aire. Il annonce à une aire les réseaux d'une autre aire, avec leurs métriques.
Type 4	Ce type de LSA est transmis par un ABR vers un ASBR (routeur connectant l'aire vers l'extérieur) et contient le coût de la métrique vers l'ASBR.
Type 5	Il est émis et propagé par un ASBR dans toutes les aires, il annonce aussi les routes externes au système autonome.

Tableau 3.1 : Les types de LSA.

Notons que :

1. ABR (Area Border Router) : C'est un routeur situé à la frontière d'un ou plusieurs domaines dans un réseau OSPF hiérarchique. Il a pour rôle de résumer la base de données topologique pour l'un de ses domaines, il doit aussi maintenir les tables de routage de multiples domaines **[19]**.

2. ASBR (Autonomous System Boundary Router) : C'est un routeur situé entre un système autonome OSPF et un réseau non OSPF (RIPv2 par exemple). Il a pour fonction d'exécuter à la fois le protocole OSPF dans un système autonome et un autre protocole de routage **[19]**.

3.2.2.4 Le format d'en-tête d'un paquet OSPF

La figure 3.5 montre l'en-tête de paquet OSPF. Les champs de cet en-tête seront abordés plus en détail, ci-après.

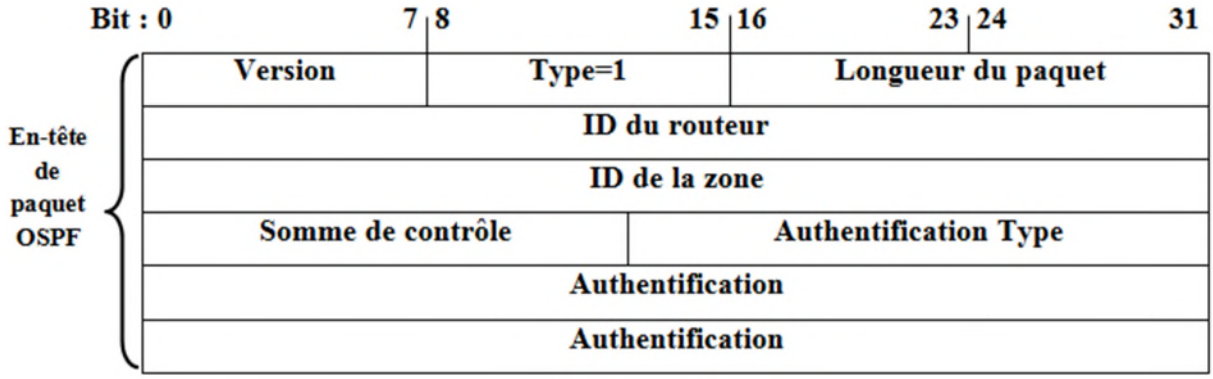


Figure 3.5 : L'en-tête d'un paquet OSPF **[51]**.

Le fonctionnement des champs de ce protocole sont expliqués dans ce qui suit **[13]**:

1. ***Version :*** C'est la version du protocole OSPF et il y a trois : OSPFv1, OSPFv2 et OSPFv3,

2. ***Type :*** C'est le type de paquet OSPF : Hello (1), Listes des liaisons (Database Description) (2), LS Request (requête d'état des liaisons) (3), LS Update (mise à jour d'état des liaisons) (4), LSA (accusé de réception d'état des liaisons) (5),

3. ***ID du routeur :*** Identifiant du routeur d'origine et souvent l'adresse Internet la plus grande du routeur qui est choisi,

4. ***ID de la zone :*** C'est le numéro de l'aire pour laquelle le paquet est actif,

5. ***Somme de contrôle (checksum):*** Il permet de s'assurer de la validité de l'entête : même calcul que dans TCP, UDP et IP,

6. ***Le type d'authentification :*** Le numéro « 0 » signifie que y a pas d'authentification, le « 1 » : par mot de passe en clair dans le paquet (à configurer de façon identique dans tous les routeurs), le « 2 » : par de chiffrement en utilisant l'algorithme de MD5 : un calcul est effectué par l'émetteur à partir du contenu du paquet à émettre et d'un mot de passe. Le résultat de ce calcul est rajouté au paquet émis. Le récepteur refait le même calcul et vérifie le résultat envoyé.

7. ***Authentification :*** Ce champ est utilisé par l'algorithme d'authentification.

3.2.2.5 Le protocole Hello [52]

Lorsqu'un routeur lance un processus de routage OSPF sur une interface, il envoie un paquet Hello et continue d'envoyer des paquets Hello à un intervalle régulier. Les règles qui régissent l'échange des paquets « Hello OSPF » sont appelées protocole Hello.

Les protocoles Hello sont utilisés pour découvrir des voisins OSPF et établir des contiguïtés, annoncer les paramètres sur lesquels les deux routeurs doivent s'accorder pour devenir voisins, pour sélectionner un routeur désigné (DR) et un routeur désigné de secours (BDR) sur des réseaux à accès multiple comme Ethernet.

1. ***Détection des voisins :*** Avant qu'un routeur OSPF puisse diffuser ses liaisons aux autres routeurs, il doit d'abord déterminer s'il existe d'autres voisins OSPF sur une de ses liaisons.

La figure 3.5 permet de nous montrer comment fonctionne la tâche de détection de voisins **[53]**.

2. ***Intervalles des paquets Hello et Dead OSPF :*** Avant que deux routeurs puissent former une contiguïté de voisinage OSPF, ils doivent s'entendre sur les valeurs suivantes : *l'intervalle Hello* et *l'intervalle Dead* (arrêt).

L'intervalle Hello OSPF indique la fréquence à laquelle un routeur OSPF envoie des paquets Hello. Par défaut, les paquets OSPF Hello sont envoyés toutes les 10 secondes sur les segments à accès multiple et point à point.

L'intervalle Dead est la période pendant laquelle le routeur attendra de recevoir un paquet Hello avant de déclarer le voisin « hors service » **[53]**. Ces deux opérations sont illustrées dans la figure 3.6.

3. ***Détection d'un routeur désigné et un routeur désigné de secours :*** Pour réduire le trafic OSPF sur les réseaux à accès multiple, OSPF choisit un routeur désigné (DR) et un routeur désigné de secours (BDR).

Le DR est chargé de la mise à jour de tous les autres routeurs OSPF, lorsqu'une modification a lieu au niveau du réseau à accès multiple. Le BDR surveille le DR et prend sa place en tant que routeur désigné si ce dernier tombe en panne **[53]**.

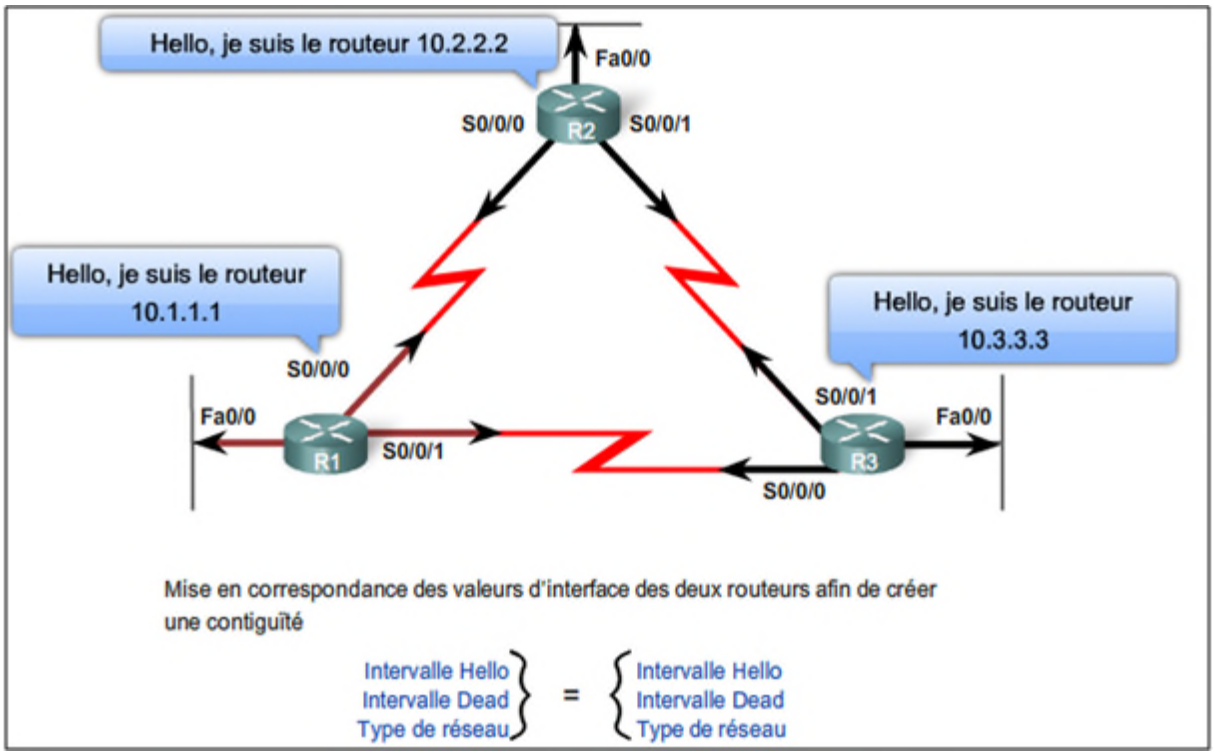


Figure 3.6 : Le fonctionnement du protocole Hello.

Le format général du protocole Hello est présenté dans la figure suivante :

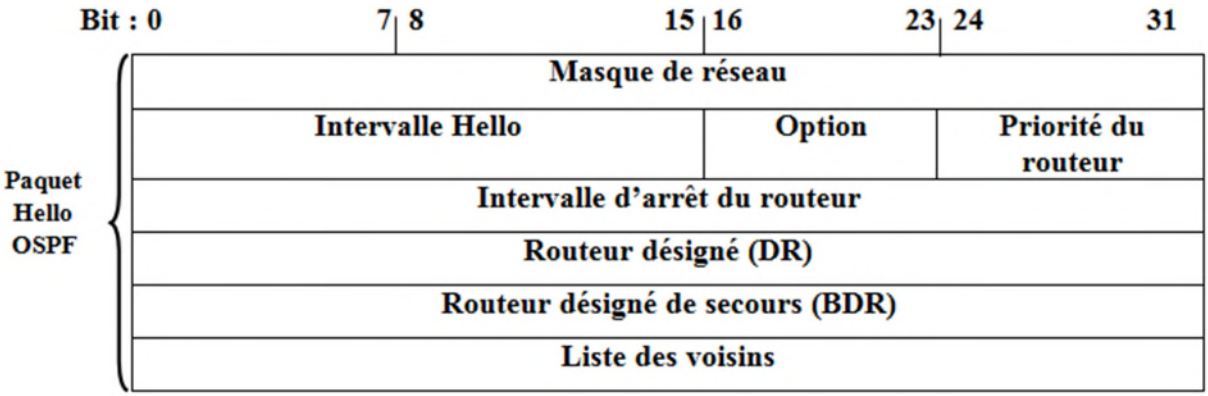


Figure 3.7 : Format du protocole Hello **[51]**.

Description des champs du protocole Hello

1. ***Masque de réseau :*** Le masque pour la liaison configurée dans le routeur qui génère le Hello. Si le champ ne correspond pas au masque configuré pour la liaison dans le routeur destinataire, ce dernier rejette le Hello et n'accepte pas le routeur qui l'a transmis comme voisin **[13]**.

2. **Intervalle Hello :** C'est le nombre de secondes qui s'écoulent entre deux paquets hello d'un routeur **[13]**.

3. Options : Seuls les deux bits de plus faible poids sont définis. Le bit inférieur est T, qui indique si le routeur supporte plusieurs métriques de routage. Ceci semble impliquer qu'un routeur doit appliquer soit une seule métrique, soit toutes les métriques.
Le bit suivant est le bit E, qui implique si le routeur considère l'aire comme une aire à talon ou pas. Si le routeur destinataire n'a pas été configuré de la même manière que le routeur émetteur, le Hello sera rejeté **[13]**.

4. Priorité du routeur : Champ utilisé pour élire le routeur désigné et le routeur désigné de secours. Une priorité de 0 signifie que le routeur ne deviendra jamais routeur désigné ou routeur désigné de secours, même si aucun autre routeur n'est disponible **[13]**.

5. Temps mort : C'est le nombre de secondes qui s'écoulent avant qu'un routeur ne déclare un voisin hors d'usage s'il n'a reçu aucun Hello. C'est le même principe que pour l'intervalle entre Hello, si cette valeur ne correspond pas exactement à la valeur configuré dans le routeur destinataire, ce dernier va rejeter le Hello **[13]**.

6. Routeur désigné (DR): L'identifiant du routeur que le routeur émetteur pense être le routeur désigné (ou 0 si le routeur émetteur pense qu'il n'y a pas de routeur désigné) **[13]**.

7. Routeur désigné de secours (Backup Designated Router - BDR): L'identifiant du routeur que le routeur émetteur pense être le routeur désigné de secours (ou 0 si le routeur émetteur pense qu'il n'y a pas de routeur désigné de secours) **[13]**.

8. Liste des voisins : Ce champ contient des identifiants sur 4 octets des routeurs dont les Hello ont été reçus sur la liaison pendant la durée du temps mort **[13]**.

3.2.2.6 Le fonctionnement du protocole OSPF [7]

Le calcul du plus court chemin est effectué de manière indépendante par tous les routeurs internes d'un système autonome. Grâce à l'algorithme du plus cout chemin, un routeur peut connaître le prochain routeur qui transmettra le message : il trouve les plus courts chemins (en termes de coût) d'un point à un autre, pour que le message arrive de manière optimale à son destinataire, puis il effectue la mise à jour de sa table de routage. Chaque mise à jour de la base de données entraîne celle de la table de routage. Il

y a, comme précédemment, communication entre les routeurs. Celle-ci est régie par le protocole OSPF.

Ce protocole définit les règles et les formats de messages entre routeurs OSPF internes à un système autonome. Il a la particularité de s'appuyer directement sur IP (et non sur UDP comme le protocole RIP) ; c'est une nette amélioration, car le routage devient un traitement interne à la couche réseau.

3.2.2.7 Algorithme SPF (Shortest Path First)

Chaque routeur OSPF conserve une base de données d'état des liaisons contenant les LSA reçues de tous les autres routeurs. Une fois qu'un routeur a reçu toutes les LSA et créé sa base de données d'état des liaisons locale, OSPF utilise l'algorithme du plus court chemin de *Dijkstra (SPF)* pour créer une arborescence SPF qui est ensuite utilisée pour fournir à la table de routage IP des meilleurs chemins vers chaque réseau **[51]**.

L'algorithme de routage de Dijkstra sert à faire les opérations d'OSPF. L'arbre calculé des plus courts chemins permet de construire la table de routage, son fonctionnement est le suivant **[14]**:

Cet algorithme a été proposé par *Edgar Dijkstra* pour calculer les plus courts chemins dans un graphe dont les poids associés aux liens sont positifs ou nul en consistant à constituer un arbre *(Shortest Path Tree-SPT).*

Étant donné un graphe G (V, E) où V, E est l'ensemble des N sommets et M arêtes, respectivement. Pour construire le SPT du nœud S qui appartient à V, nous utilisons deux sous ensembles P et Q où P contient des nœuds visités et Q contient ceux restants. Chaque nœud est assigné une étiquette qui se compose du nœud précédant et la distance temporaire dans le chemin de la racine (S). Au début, P ne contient que S et les étiquettes des (N-1) nœuds restants sont les mêmes : (S, ∞). À chaque itération, nous recalculons la distance temporaire et l'étiquette de chaque nœud en fonction de la procédure présentée dans la figure 3.8 dont l'algorithme est constitué des éléments suivant :
Le champ *Graph g* qui représente le graphe ; le champ *int n* qui est le nombre de sommets dans *g* ; le champ *int source* représentant la source du plus court chemin recherché et le champ *int dest* qui est la destination du plus court chemin recherché. Si cet algorithme renvoie *-1*, c'est qu'aucun chemin n'existe entre la source et la destination.

Avec le protocole OSPF, un réseau peut être modélisé par un graphe; il suffit de considérer les routeurs comme des nœuds et les liaisons de données comme des arcs.

```
Dijkstra (G, source, dest) :
 Pour chaque sommet i dans G
   dist[i] = INFINI
   dist[source] = 0
   S = {source}
 Tant que S non vide
  x = EnleverMinDist (S)
  Si x == dest
    Renvoyer dist[x]
  Pour chaque successeur s de x
    MiseAJour (s, x, G, S)
 Renvoyer -1
```

Figure 3.8 : Algorithme de Dijkstra.

3.2.2.8 Les types de réseaux

Le protocole OSPF définit différents types de liaisons et parmi ceux-ci nous citons : *réseau point à point* et *réseau à accès multiple*.

Un réseau point à point ne comporte que deux périphériques, un à chaque extrémité. La liaison utilisée est nommée liaison point à point, c'est une liaison qui permet de relier un point à un autre. La figure 3.9 montre un exemple de ce type de liaison entre deux routeurs **[57]**:

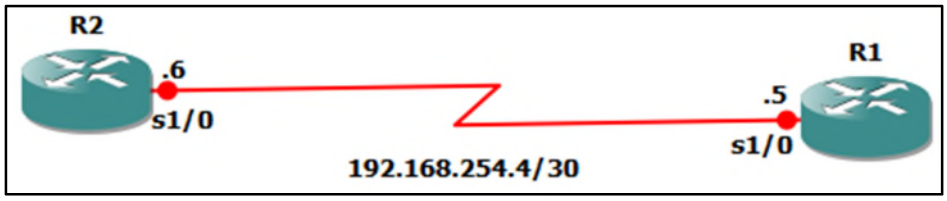


Figure 3.9 : Réseau point à point.

Dans un réseau à accès multiples, il est impossible de savoir à l'avance combien de routeurs seront connectés, donc c'est un réseau comportant plus de deux périphériques sur le même support partagé **[53]**.

La figure 3.10 illustre que le réseau local Ethernet relié à R3 est étendu afin de montrer les différents périphériques qui peuvent être attachés au réseau 172.16.1.16/28.

Les réseaux locaux Ethernet constituent un exemple de réseau à accès multiple de diffusion. Ce sont des réseaux de diffusion car tous les périphériques du réseau peuvent voir toutes les trames et des réseaux à accès multiple également, car de nombreux hôtes, imprimantes, routeurs et autres périphériques peuvent être membres du même réseau **[53]**.

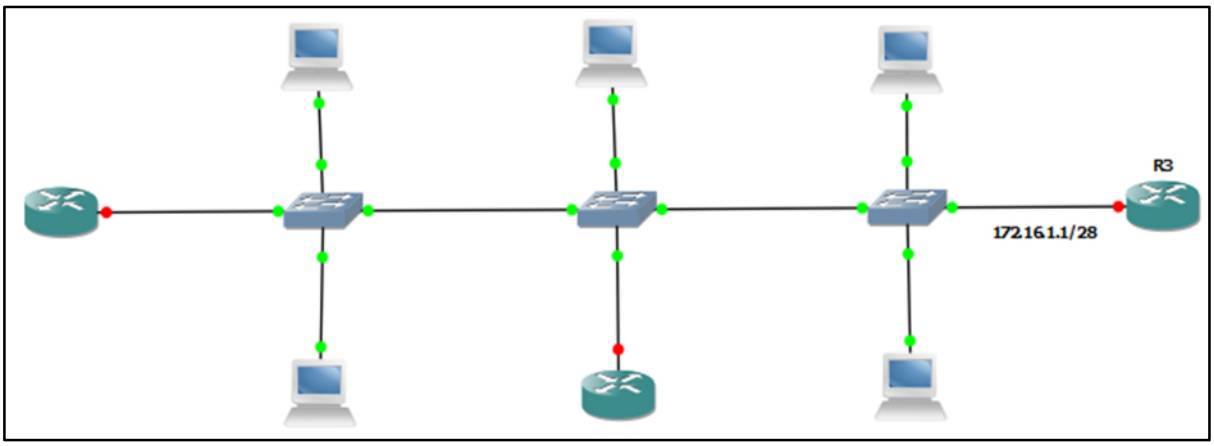


Figure 3.10 : Réseau à accès multiple avec diffusion.

Les LSA envoyées par le protocole de routage OSPF sur les réseaux à accès multiple peuvent présenter deux difficultés pour celui-ci : la création de contiguïtés multiples, une pour chaque paire de routeurs et une diffusion massive de LSA.

1. La création de contiguïtés multiples

La création d'une contiguïté entre chaque paire de routeurs dans un réseau créera un nombre de contiguïtés inutile (une surcharge au niveau des machines).
Nous devons étudier une formule pour mieux comprendre ce problème. Le nombre de routeurs, quel qu'il soit (défini ici par n) d'un réseau à accès multiples donnera le résultat suivant : $n\ (n - 1) / 2$ contiguïtés **[53]**.

Si nous avons une topologie à cinq routeurs, tous rattachés au même réseau à accès multiple Ethernet. S'il n'existe aucun mécanisme permettant de réduire le nombre

de contiguïtés, ces routeurs formeront 10 contiguïtés : *5 (5 - 1) / 2 = 10.* Cela peut sembler peu, mais au fur et à mesure que des routeurs sont ajoutés au réseau, le nombre de contiguïtés augmente de façon considérable.

2. Diffusion des LSA

Dans le cadre d'un réseau à accès multiple, la diffusion des LSA devient excessive car si nous avons une topologie possédant *n* routeur et un routeur envoie une LSA, cet événement déclenche chez tous les routeurs l'envoi d'une LSA, si chaque routeur d'un réseau à accès multiple devait envoyer une LSA, puis un accusé de réception de toutes les LSA qu'il a reçu pour tous les routeurs de ce réseau, le trafic réseau deviendra désordonné car un nombre excessif de LSA circulera entre les routeurs du même réseau **[53]**.

3. Solution utilisée

La solution pour gérer le nombre de contiguïtés et la diffusion des LSA sur un réseau à accès multiple est l'élection d'un routeur désigné (DR). Le protocole OSPF sélectionne un routeur désigné comme point de collecte et de distribution des LSA envoyées et reçues. Un routeur désigné de secours (BDR-backup designated routeur) est également élu en cas de défaillance du routeur désigné. Tous les autres routeurs deviennent des DROTHERS : ce qui signifie qu'ils ne sont ni DR, ni BDR, ces routeurs constituent des contiguïtés avec le DR et le BDR du réseau. Cela signifie qu'au lieu de diffuser les LSA à l'ensemble des routeurs du réseau, ils envoient leurs LSA uniquement au DR et au BDR en utilisant l'adresse multidiffusion de 224.0.0.6 **[53]**.

3.2.2.9 Le principe d'authentification de routage avec OSPF

Chaque interface OSPF peut présenter une clé d'authentification à l'usage des routeurs qui envoient des informations OSPF aux autres routeurs du segment, donc ce protocole peut être configuré pour chiffrer et authentifier celles-ci. La clé d'authentification, ou mot de passe, est partagée entre les routeurs.

Cette opération garantit que les routeurs sécurisent les données échangées avec des routeurs configurés en utilisant le même mot de passe ou les mêmes informations d'authentification **[53]**.

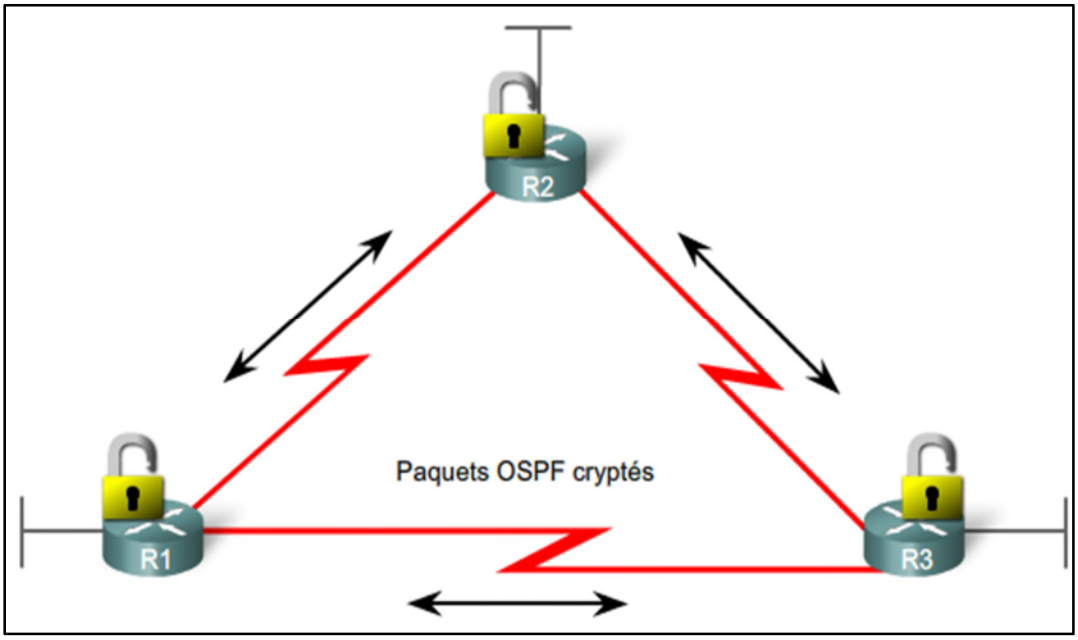


Figure 3.11 : Authentification OSPF.

3.2.2.10 Mesure OSPF [53]

La mesure utilisée par le protocole OSPF est le coût qui est associé au niveau de la sortie de chaque interface du routeur, il est configurable par un administrateur système, plus le coût est faible, plus l'interface sera utilisée pour acheminer le trafic.

Pour calculer ce coût, l'IOS Cisco d'un routeur cumule les bandes passantes des interfaces de sorties depuis un routeur jusqu'au réseau de destination, il est déterminé pour chaque interface grâce à la formule suivante :

$$10^8 \text{ / bande passante Bits/ secondes}$$

3.2.2.11 Inconvénients d'OSPF

OSPF est un protocole relativement complexe car il nécessite des ressources matérielles importantes, mais également de bonnes connaissances et une bonne maîtrise de son fonctionnement avant de pouvoir être implémenté **[38]**.

3.2.2.12 Avantages d'OSPF [38]

OSPF est aujourd'hui l'un des protocoles de routage interne les plus utilisés, de par sa force et sa robustesse, mais également grâce à sa licence basée sur des normes ouvertes, cela signifie qu'il peut être mis en œuvre sur toute plate-forme, à partir de

n'importe quel fournisseur, qui lui confère un avantage sur des protocoles propriétaires tel que EIGRP de Cisco et il offre une convergence rapide.

En revanche de la complexité de mise en œuvre citée précédemment, OSPF augmentera considérablement les performances, la stabilité et la fiabilité du réseau.

3.2.3 Le protocole de routage dynamique EIGRP

3.2.3.1 Définition d'EIGRP

Le protocole *EIGRP (Enhanced Interior Gateway Routing Protocol)* est un protocole de routage à vecteur de distance amélioré propriétaire et est développé par Cisco. Il a été spécifiquement étendu pour pallier les problèmes associés au routage dans de grands réseaux qui dépassaient la portée des protocoles tels que RIP. Il utilise l'algorithme *DUAL (Diffusing Update Algorithme)* qui a été développé à *SRI* International ce qui permet une meilleur convergence du réseau **[42]**.

Il constitue une version perfectionnée du protocole *IGRP (Interior Gateway Routing Protocol)* qui est un protocole de routage à vecteur de distance mit au point par Cisco et uniquement compatible avec ses produits **[37]**.

3.2.3.2 Format de message EIGRP

Les messages du protocole EIGRP sont constitués de plusieurs champs qui sont présenté dans la figure 3.12 **[19]**:

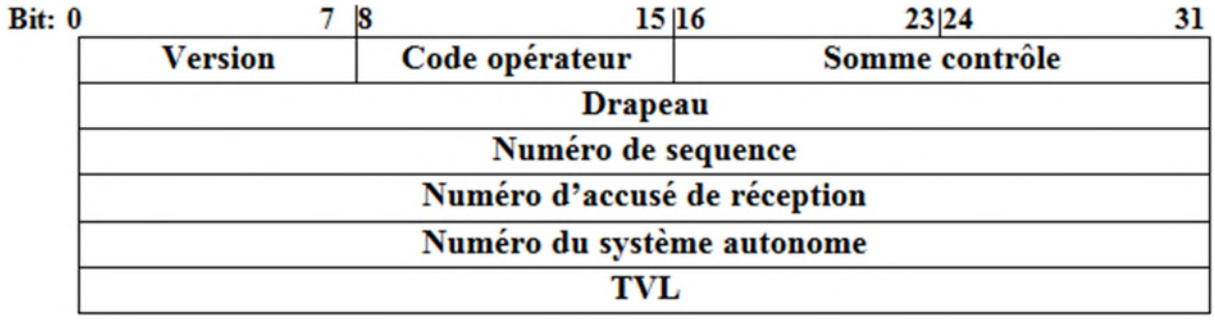


Figure 3.12 : Format d'un message EIGRP.

Description des champs du paquet EIGRP **[19]**:

1. ***Version :*** Représente la version du protocole EIGRP.

2. ***Code opérateur :*** Ce champ spécifie le type de paquet EIGRP (mise à jour, demande, réponse et hello).

3. Drapeau : Le premier bit de ce champ est le bit init (utilisé dans la nouvelle relation de voisinage), le deuxième bit est le bit de réception conditionnel (utilisé dans l'algorithme de mulitcast fiable propriétaire), autres bits ne sont pas utilisés.

4. Somme de contrôle : S'applique à l'ensemble du paquet EIGRP, sauf l'en-tête IP.

5. Numéro de séquence et Numéro d'accusé de réception : Ces deux champs sont utilisés par le RTP pour envoyer des messages de manière fiable.

6. Numéro de système autonome : Identifie le processus de routage EIGRP et il est utilisé pour assurer le suivi de plusieurs instances du protocole EIGRP.

7. Le champ TLV (Type/ Longueur/ Valeurs) : Représente les paramètres du protocole EIGRP, les routes IP internes et les routes IP externes, ces deux types de routes sont représentées différemment dans les mises à jour EIGRP.
Le message de paramètres EIGRP contient les paramètres que le protocole EIGRP utilise pour calculer la mesure composite.

Le message interne IP sert à annoncer les routes EIGRP dans un système autonome, par contre, le message externe IP est utilisé lorsque des routes externes sont importées dans le processus de routage EIGRP. Dans notre cas, nous importerons ou redistribuerons une route statique par défaut dans le protocole EIGRP (nous allons montrer ce cas dans le chapitre suivant) **[19]**.

3.2.3.3 Le protocole RTP *(Reliable Transport Protocol)* [54]

RTP est un protocole de la couche transport qui peut garantir la livraison et la réception des paquets EIGRP à tous les voisins. Sur un réseau IP, les hôtes utilisent TCP pour séquencer les paquets et garantir leur livraison en temps voulu. Cependant, le protocole EIGRP est indépendant de ces protocoles, cela signifie qu'il ne dépend pas du TCP/IP pour échanger des informations de routage comme le font les protocoles RIPv2, et OSPF. Il utilise RTP comme son propre protocole propriétaire pour assurer la livraison des informations de routage.

EIGRP peut faire appel à RTP pour fournir un service fiable ou non fiable selon la situation. Par exemple, les paquets HELLO ne nécessitent pas la surcharge de la livraison fiable car ils sont envoyés fréquemment et sont de taille limitée. Toutefois, la livraison

fiable des autres informations de routage peut accélérer la convergence, parce que les routeurs EIGRP n'attendent pas l'expiration d'un compteur pour retransmettre.

Le protocole RTP peut envoyer des paquets en unicast ou en multidiffusion. Les paquets EIGRP en multidiffusion utilisent l'adresse multidiffusion réservée de 224.0.0.10. Le fonctionnement du protocole RTP est présenté dans la figure 3.13 suivante :

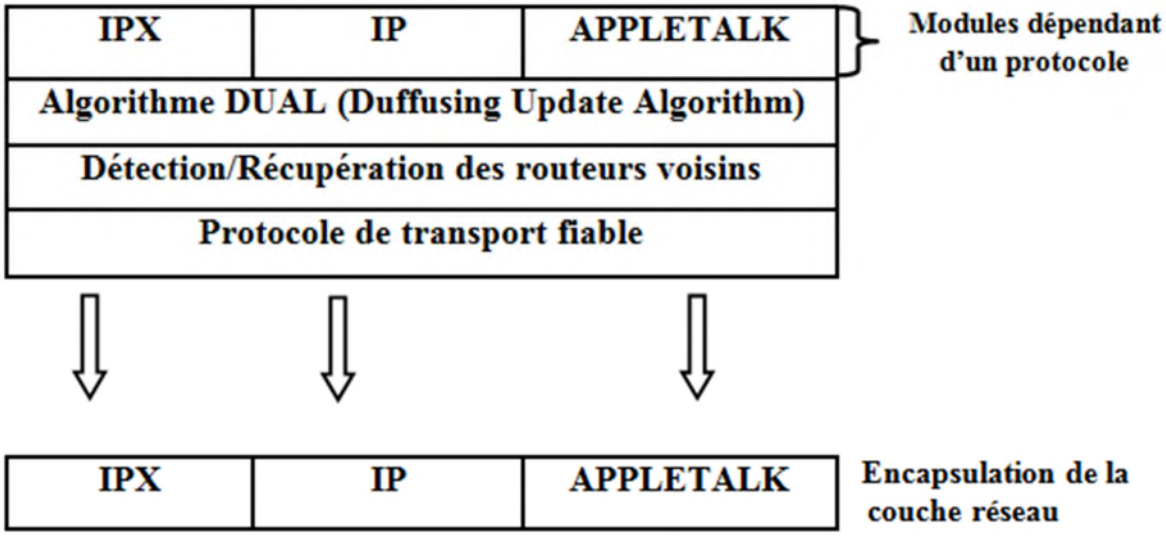


Figure 3.13 : Fonctionnement du protocole RTP.

3.2.3.4 Les types de paquets du protocole EIGRP

Plusieurs types de paquets sont utilisés avec le protocole EIGRP. Les plus répandus sont «*Hello Message*», «*UpdateMessage*», «*Query / Reply Message*» et « *ACK Message* »

1. ***Hello Message:*** Ces messages sont utilisés pour découvrir des voisins et établir des contiguïtés avec ces voisins. Il permet de spécifier que le routeur est actif mais ne comporte pas de données. Les paquets hello EIGRP sont de type multidiffusion et utilisent la livraison non fiable **[39]**.

2. ***Update Message:*** Ces messages sont utilisés pour transporter des informations de routage. Lorsqu'un nouveau voisin est découvert, un unicast Update message est envoyé à celui-ci pour qu'il puisse construire sa table de topologie *« topology table»* **[54]**.

3. ***Query / Reply Message :*** L'algorithme DUAL utilise ce type de message si une destination n'a aucun successeur. *Query message* est la demande envoyée par le routeur et est en multicast, par contre *Replay message* c'est la réponse à une demande d'un routeur

afin de préciser à celui-ci qu'un recomptage n'est pas nécessaire car il existe déjà un successeur **[39]**.

4. ACK Message : Ce type de message est envoyé par EIGRP quand une livraison fiable est utilisée. Le protocole RTP utilise la livraison fiable pour les paquets de mises à jour, de demande et de réponse **[54]**.

3.2.3.5 Type de mises à jour EIGRP [54]

Le protocole EIGRP utilise le terme partiel ou limité pour qualifier ses paquets de mise à jour. Contrairement au protocole RIPv2, EIGRP n'envoie pas de mises à jour périodiques. En revanche, EIGRP envoie ses mises à jour uniquement lorsque la mesure d'une route change.

Le terme *« partiel »* signifie que la mise à jour ne contient que les informations concernant les modifications de routes. EIGRP envoie ces mises à jour incrémentielles lorsque l'état d'une destination change au lieu d'envoyer la totalité du contenu de la table de routage.

Le terme *« limité »* désigne la propagation des mises à jour envoyées uniquement aux routeurs affectés par le changement. La mise à jour partielle est automatiquement limitée, de sorte que seuls les routeurs qui ont besoin de l'information sont mis à jour.
En envoyant uniquement les informations de routage nécessaires aux routeurs qui en ont besoin, EIGRP réduit la bande passante requise pour l'envoi des paquets EIGRP.

3.2.3.6 Principes et fonctionnement

Le protocole EIGRP peut se comporter comme un protocole de routage à état de liens mais il reste toujours un protocole à vecteur de distance.
Le fonctionnement du protocole EIGRP est le suivant : le routeur qui est configuré pour utiliser le protocole EIGRP va garder en mémoire toutes les tables de routage de ces voisins dans une table nommée *table de voisinage*, ce qui permet en cas de défaillance du réseau de trouver très rapidement un chemin alternatif **[40]**.

Le protocole EIGRP ne fait pas de mises à jour périodique de ces tables, ce qui peut s'avérer être un certain inconvénient. En effet, si une route change pour une quelconque raison, le routeur utilisant EIGRP en tant que protocole ne sera pas avertit aussi rapidement que les routeurs utilisant d'autres protocoles, mais

si le protocole EIGRP ne permet pas aux routeurs de faire des mises à jour périodiques, il leur permet néanmoins d'envoyer de partielles mises à jour lorsque la distance pour une route change. Ces informations sur la route qui a changé sont alors uniquement envoyées vers les routeurs qui ont besoin de ces informations **[39]**.

3.2.3.7 Technologies utilisées par le protocole EIGRP [39]

Le protocole EIGRP est plus performant que son prédécesseur IGRP par ce qu'il utilise des technologies plus récentes et plus importantes. En effet, EIGRP se base sur les technologies suivantes :

1. ***Neighbor Discovery/Recovery :*** Les routeurs envoient régulièrement ce type de message à leurs voisins pour vérifier que ceux-ci sont opérationnels, car les messages Neighbor Discovery/Recovery appelé aussi « Hello message » permettent de connaître les routeurs directement connectés au routeur utilisant le protocole EIGRP.

2. ***Reliable Transport Protocol :*** La vérification de l'envoie des paquets, le support de la transmission de paquets unicast ou multicast sont assurés par le protocole RTP.

3. ***DUAL Finite State Machine (FSM DUAL) :*** Une machine à états finis DUAL se compose de nombreux états et des scénarios différents qui permettent de calculer et comparer des routes dans un réseau EIGRP.

4. ***Protocol-dependent modules (PDM):*** Ils sont utilisés par le protocole de routage EIGRP pour prendre des décisions au sujet de l'ajout de routes apprises par d'autres sources, par exemple : d'autres protocoles de routage. EIGRP offre un support pour divers protocoles routés (par exemple : IP, IPX, AppleTalk).

3.2.3.8 Les conceptions de routage

Le protocole EIGRP repose sur plusieurs concepts de base, en effet, il met à jour trois tables de bases de données pour stoker les informations de routage, contrairement à RIPv2 : *Neighbor Tables (table de voisinage), Topology Table (table de topologie)* et *la table de routage* **[39]**:

1. ***Neighbor Tables (table de voisinage):*** L'enregistrement de l'adresse et de l'interface d'un nouveau voisin découvert par un routeur est effectué dans la table de routage pour ses voisins. Lorsqu'un voisin envoie un « Hello message », il est avertit du « Hold time » (il a la valeur de 15 secondes) qui correspond à la période de temps qu'un routeur

doit attendre pour une réponse de la part d'un de ses voisins. S'il n'y a pas de réponse avant la fin de ce temps, alors le chemin est considéré comme indisponible **[39]**.

Le tableau ci-dessous illustre les différents champs d'une table de voisinage avec explication **[39]**:

Nom du champ	***Explication***
Adresse du voisin	Il s'agit de l'adresse réseau du routeur voisin.
Délai de conservation	Intervalle à l'issue duquel la liaison est considérée comme indisponible si aucun signal n'a été reçu du voisin.
Smooth Round-Trip Timer (SRTT)	C'est le temps moyen nécessaire pour envoyer et recevoir des paquets d'un voisin.
Queue count (Q Cnt)	Il s'agit du nombre de paquets en attente d'envoi dans une file d'attente.
Sequence Number (Seq No)	C'est le numéro du dernier paquet reçu de ce voisin. Le protocole EIGRP utilise ce champ pour accuser de réception de la transmission d'un voisin et pour identifier les paquets hors séquence.

Tableau 3.2 : Les champs de la table de voisinage.

2. Topology Table (table de topologie) : Cette table contient toutes les destinations connues par les routeurs voisins. Chaque entrée dans la table de topologie contient l'adresse de destination ainsi que la liste de ses voisins. Cette liste est associée à la métrique qu'utilise le routeur pour atteindre sa destination.

La métrique qu'utilise le routeur dans sa table de routage et celle qu'il emploi pour avertir les autres routeurs est la somme de la meilleure mesure entre la destination et un de ses voisins additionnée à la distance entre lui et ce voisin **[39]**. Cette table inclut les champs suivants : *Distance de faisabilité, source de la route, distance annoncée, informations d'interface* et *état de la route* qui sont décrient dans ci-dessous :

2.1 Distance de faisabilité (Feasible Distance, FD) : C'est la mesure la plus faible calculée pour atteindre le réseau de destination **[55]**.

2.2 Source de la route : Elle représente le numéro d'identification du routeur qui a initialement annoncé cette route **[15]**.

2.3 Distance annoncée (Reported Distance, RD) : La distance de faisabilité annoncée par un voisin EIGRP pour atteindre le même réseau de destination **[55]**.

2.4 Informations d'interface : Elle est l'interface permettant d'atteindre la destination **[15]**.

2.5 État de la route : Une route est identifiée comme étant soit passive (P), c'est-à-dire stables et prêtes à l'utilisation, soit active (A), ce qui signifie qu'elle va être recalculée par l'algorithme DUAL **[15]**.

3. La table de routage : Cette table contient les meilleures routes vers une destination donnée. Chaque routeur EIGRP tient à jour une table de routage pour chaque protocole de réseau. Une route successeur est une route sélectionnée comme route principale à utiliser pour atteindre une destination et il peut y avoir jusqu'à *quatre* routes successeur pour une route particulière. Ces routes peuvent être de coût égal ou différent et elles sont identifiées comme les meilleurs chemins sans de boucles vers une destination donnée **[15]**.

4. Route-States : Les entrées de destinations pour la table de topologie peuvent exister en deux états : actif ou passif. Une destination est passive lorsque le routeur n'a pas besoin de recompter et active lorsque celui doit effectuer un recomptage. Un recomptage est nécessaire lorsqu'une destination n'a pas de successeur. Cette notion de successeur est très importante lors de l'utilisation du protocole EIGRP.

En effet, lorsqu'un routeur veut acheminer un paquet, il a besoin de connaître toutes les routes possibles capables de remplir cette tâche. Ce sont les routeurs voisins qui vont lui indiquer les différents chemins possibles que pourront emprunter les données pour arriver à destination, c'est donc le routeur voisin qui propose le chemin avec le plus faible coût jusqu'à la destination qui sera désigné comme le successeur.
Lors de la comparaison des coûts des différentes routes possibles, le coût le plus faible qui sera alors choisi par EIGRP est appelé le *Feasible Distance (FD)* **[39]**.

3.2.3.9 Concepts de l'algorithme DUAL

Le protocole EIGRP utilise l'algorithme DUAL qui permet de déterminer le meilleur chemin sans boucle et les meilleurs chemins de secours sans boucle.

Cet algorithme utilise plusieurs termes qui seront présentés plus en détail au cours de cette section : *Successeur, distance de faisabilité, successeur potentiel, distance annoncée* et *condition de faisabilité* **[54]**.

1. ***Successeur (Successor):*** C'est un routeur voisin utilisé pour le transfert de paquets et constitue la route à moindre coût jusqu'au réseau de destination **[55]**.

2. ***Successeur potentiel (Feasible Successor, FS) :*** C'est un voisin comportant un chemin de secours sans boucle vers le même réseau que le successeur en satisfaisant à la condition de faisabilité (FC) **[55]**.

3. ***Condition de faisabilité (Feasible Condition, FC) :*** Cette condition est remplie lorsque la distance annoncée d'un voisin vers un réseau donné est inférieur à la distance de faisabilité d'un voisin EIGRP vers le même réseau de destination **[55]**.

3.2.3.10 Algorithme de DUAL *(Diffusing Update Algorithm)*

L'algorithme *DUAL* est l'algorithme de convergence qu'utilise le protocole EIGRP au lieu des algorithmes Bellman-Ford utilisé par les autres protocoles de routage à vecteur de distance comme RIPv2 **[39]**.

Cet algorithme permet d'éviter les boucles à tout moment, grâce au calcul de route. Cela permet à tous les routeurs concernés par une modification de topologie de se synchroniser simultanément. Les routeurs qui ne sont pas affectés par le changement de topologie ne sont pas impliqués dans le nouveau calcul. Cette méthode fournit au protocole EIGRP des temps de convergence plus rapides que ceux des autres protocoles de routage à vecteur de distance **[39]**.

Le fonctionnement de l'algorithme DUAL utilisé par le protocole de routage EIGRP est illustré dans la figure 3.14 et expliqué dans ce qui suit **[16]**:

Pour atteindre le réseau *« LAN2 »,* le *« Routeur A »* essaye de trouver le meilleur chemin où le coût est plus faible. Sur le schéma présenté ci-après, il peut y avoir deux chemins sans boucle :

Le premier passant par le *« Routeur B »* et le deuxième par le « Routeur C », en effet le protocole EIGRP a la particularité de stocker ces deux chemins en les différenciant : l'un est le successeur utilisé et l'autre le successeur potentiel.

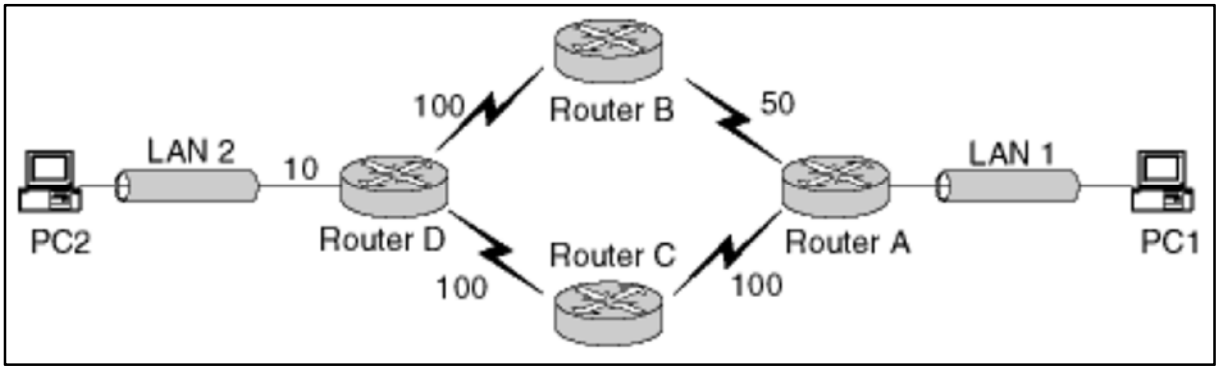


Figure 3.14 : Principe de l'algorithme DUAL.

3.2.3.11 L'authentification avec EIGRP

Comme d'autres protocoles de routage, EIGRP peut être configuré pour l'authentification, afin de chiffrer et d'authentifier ses informations de routage qui circulent entre les routeurs souvent en clair. L'authentification assure que les routeurs n'accepteront que les données en provenance de routeurs qui ont été configurés avec le même mot de passe ou les mêmes informations d'authentification **[54]**.

3.2.3.12 Mesure composite EIGRP et les valeurs K

Tous les protocoles de routage ont une certaine notion de métrique, la valeur utilisée pour calculer le meilleur chemin vers une destination. EIGRP utilise une métrique composite basé sur un certain nombre de paramètres de liaison. Bien qu'il existe quatre paramètres qui sont suivis par ce protocole pour le calcul de métrique : *la bande passante (K1), le délai(K3), la fiabilité (K4,K5)* et *la charge (K2),* il est important de noter que seulement deux d'entre eux sont utilisés par défaut : la bande passante et le délai **[16]**.

La formule composite du protocole EIGRP se compose des valeurs *K1* à *K5*, connues sous le nom de pondérations de mesure EIGRP. Par défaut, *K1* et *K3* ont pour valeur *«1»*, et *K2, K4* et *K5* ont pour valeur *« 0 »*. Le résultat est que seules les valeurs de bande passante et de délai sont utilisées dans le calcul de la mesure composite par défaut et ces valeurs peuvent être modifié **[54]** chose que nous allons voir dans le chapitre suivant.

La formule par défaut est : **Mesure = [K1*bande passante + K3*délai]**

La formule complète est la suivante :

Mesure = [K1*bande passante + (K2*bande passante) / (256 - charge) + K3*délai]*[K5/ (fiabilité + K4)] ⇦ n'est pas utilisée si les valeurs de « K » sont égale à 0

Les paramètres qu'utilise le protocole EIGRP pour le calcul de la métrique sont présentés comme suit **[16]**:

1. ***Bande passante :*** Elle s'affiche en kilobits. Notons que la bande passante par défaut sur les interfaces série est 1544 kilobits quelle que soit la vitesse de connexion réelle configuré. L'utilisation de l'instruction de la bande passante est nécessaire au bon fonctionnement du protocole EIGRP et elle est utilisée par défaut dans le calcul de son indicateur composite.

2. ***Délai :*** C'est la mesure du temps nécessaire à un paquet pour parcourir une route. Le délai n'est pas mesuré de façon dynamique. En d'autres termes, le routeur ne contrôle pas réellement le temps que le paquet prend pour atteindre sa destination. Le protocole EIGRP n'utilise pas ce paramètre par défaut pour le calcul de la métrique.

3. ***La fiabilité :*** C'est une mesure de la probabilité d'un lien est basé sur les données historiques relatives à la durée pendant laquelle un lien est disponible pour transmettre des données. Il s'agit d'une valeur de 1 à 255. Une valeur de 255 indique que le lien est fiable à 100%. Cette mesure n'est par défaut utilisée par EIGRP.

4. ***La charge :*** Cette mesure est utilisée pour déterminer comment utilisé un lien est à un moment donné. Contrairement à la bande passante ou au délai, la charge n'est pas un nombre statique, elle est mesurée de façon dynamique par une valeur comprise entre 0 et 255. Par défaut, le protocole EIGRP n'utilise pas cette mesure pour effectuer le calcul de la métrique.

3.2.3.13 Avantages d'EIGRP [50]

Le protocole EIGRP offre une convergence rapide grâce au calcul des routes avec l'algorithme DUAL qui permet d'insérer des routes de secours dans la table topologique EIGRP, lesquelles sont utilisées en cas de défaillance de la route principale. Étant donné qu'il s'agit d'une procédure locale, le passage à la route de secours est immédiat et n'implique pas d'action au niveau des autres routeurs.

Grâce aux mises à jour limitées, le protocole EIGRP utilise moins de bande passante, surtout dans les grands réseaux avec de nombreuses routes. Il prend en charge plusieurs protocoles de la couche réseau tel que les protocoles IP, IPX et AppleTalk.

3.2.3.14 Inconvénients d'EIGRP [39]

Malgré que le protocole EIGRP est une amélioration du protocole IGRP, il réside toujours quelques défauts : le premier est que l'implémentation d'EIGRP sur Frame Relay ou ATM est assez difficile à réaliser et notamment lors de la configuration du protocole.

Une autre contrainte, avec le protocole EIGRP est qu'il a été développé par Cisco et est donc de ce fait un protocole propriétaire réservé à tous les produits de marque Cisco.

3.3 Comparaison entre le protocole RIPv2 et OSPF

La croissance rapide et l'extension des réseaux ont poussé RIPv2 à ses limites. RIPv2 comporte certaines restrictions qui peuvent causer des problèmes dans les réseaux larges, les caractéristiques comparatives entre ces deux protocoles sont présentées dans le tableau 3.3 suivant **[41]** :

		Protocoles	
		RIPv2	***OSPF***
Critères	***Nombre de sauts***	Le protocole RIPv2 a une limite de 15 sauts, un réseau qui comporte plus de 15 sauts (15 routeurs) est considéré comme inaccessible.	OSPF étant un protocole de routage à état de liens, chaque routeur possède une connaissance complète des réseaux au sein d'une zone (*area*), la limite du nombre de sauts n'est plus nécessaire.
	Convergence	Dans un grand réseau, la convergence doit être rapide mais le protocole RIPv2 converge plus lentement que le protocole OSPF.	OSPF a une meilleure convergence que RIPv2 parce que les changements de routage sont propagés instantanément et non périodiquement de manière incrémentielle grâce aux relations de voisinage entretenues.
	Métrique	Les décisions de routage pour le protocole RIPv2 sont uniquement basées sur le nombre de sauts quelque soit la bande passante.	Le choix du meilleur chemin est basé sur le coût et OSPF utilise la bande passante comme métrique qui peut être définie manuellement sur les interfaces d'un routeur.
	Distance administrative	Le protocole de routage RIPv2 a une valeur de la distance administrative de 120.	La valeur de la distance administrative du protocole OSPF est inférieur à celle du protocole RIPv2 et qui vaut : 110.
	Concept de zones	Il n'y a pas de concept d'*area* (zones) avec le protocole RIPv2.	OSPF permet de découper le réseau en zones, ce qui évitera la propagation inutile des mises à jour d'état de liens sur l'ensemble du réseau.

Tableau 3.3 : Comparaison entre RIPv2 et OSPF.

3.4 Comparaison entre le protocole RIPv2 et EIGRP

Le tableau 3.4 montre une comparaison entre le protocole RIPv2 et le protocole EIGRP, en prenant en compte les critères suivants : le nombre de sauts, la convergence, la métrique utilisée par chaque protocole, la distance administrative attribué par Cisco et le concept de zones **[42]**:

		Protocoles	
		RIPv2	***EIGRP***
Critères	***Nombre de sauts***	RIPv2 est limité aux réseaux simples moins de 15 sauts (routeurs).	le protocole EIGRP est idéal pour les réseaux plus étendus et plus complexes, jusqu'à une taille de 224 sauts.
	Convergence	Le temps de convergence du protocole RIPv2 est lent.	Le protocole EIGRP a une convergence rapide par rapport à RIPv2 grâce à l'utilisation de l'algorithme DUAL.
	Métrique	la distance qui sépare les routeurs d'un réseau IP est déterminée en termes de nombre de sauts.	EIGRP utilise comme métrique une association des paramètres suivants : la bande passante, le délai, la fiabilité et le coût.
	Distance administrative	Par défaut le protocole RIPv2 a une distance administrative de 120.	Le protocole EIGRP est le plus utilisé dans les réseaux avec le matériels Cisco car la valeur de sa distance administrative pour les routes internes est de 90.
	Concept de zones	Le concept de zone n'est pas utilisé par le protocole RIPv2.	Comme le protocole RIPv2, EIGRP n'a pas la particularité du découpage du réseau en plusieurs zones.

Tableau 3.4 : Comparaison entre RIPv2 et EIGEP.

3.5 Comparaison entre le protocole OSPF et EIGRP

Dans le tableau 3 .5 nous allons montrer une comparaison entre les deux protocoles de routage OSPF et EIGRP et cela par rapport aux même critères que nous avons utilisé précédemment :

		Protocoles	
		OSPF	***EIGRP***
Critères	***Nombre de sauts***	Dans le protocole OSPF y a pas de limitation de nombre de sauts étant donné qu'il s'appui sur le principe de zones **[17]**.	Le protocole EIGRP se limite sur les réseaux étendus et complexes, jusqu'à une taille de 224 sauts.
	Convergence	Une des caractéristiques les plus importantes du protocole OSPF est la capacité à s'adapter rapidement aux changements de topologie (convergence rapide) **[17]**.	EIGRP a met en œuvre un nouvel algorithme de convergence connu sous le nom DUAL qui utilise de nouvelles techniques qui permettent à ce protocole de converger très rapidement.
	Métrique	La valeur par défaut pour les métriques OSPF est basée sur la bande passante.	Les valeurs utilisées par le protocole EIGRP pour le calcul de la métrique sont : la bande passante, le délai, la fiabilité et la charge.
	Distance administrative	La distance administrative attribuée par défaut par Cisco pour le protocole OSPF est 110.	Contrairement à OSPF la valeur de la distance administrative du protocole EIGRP pour les routes internes est de 90.
	Concept de zones	Comme cité précédemment, le protocole OSPF a la possibilité de découper le réseau en zones pour résoudre le problème d'envoie de mise à jour d'état de liens.	Contrairement à OSPF le protocole EIGRP n'a pas la possibilité de découper le réseau en plusieurs zones.

Tableau 3.5 : Comparaison entre OSPF et EIGRP.

3.6 Le routage dans une organisation

Chaque protocole de routage utilise ses propres mesures. La mesure utilisée par un protocole de routage n'est pas comparable à celle utilisée par un autre protocole.

Deux protocoles de routage distincts peuvent choisir des chemins différents vers une même destination en raison des mesures qu'ils utilisent, par exemple le protocole RIPv2 choisit le chemin impliquant le moins de sauts, tandis que le protocole EIGRP choisit celui qui présente la bande passante la moins élevée et le délai le plus réduit, par contre le protocole OSPF choisit celui qui a le coût le moins élevé.

Le choix d'un protocole de routage à appliquer dans un réseau d'entreprise est un peu délicat car :

Protocoles	***Explication***
RIPv2	Si l'entreprise est constituée d'un petit réseau, le protocole le mieux adapté est RIPv2 car il n'existera pas le problème de configuration des différentes machines et les routes seront implémentées facilement.
EIGRP	Si l'entreprise choisie est composée d'un grand réseau et les éléments d'interconnexions (routeurs, switch…) sont de la marque Cisco, le protocole qui sera implémenté est EIGRP, car c'est un protocole de routage dynamique développé et propriétaire à Cisco.
OSPF	Si cette entreprise utilise des éléments d'interconnexions de marques différentes (Cisco, Juniper…), le protocole OSPF qui sera implémenté pour bien configurer la topologie de cette entreprise.

Tableau 3.6 : RIPv2, EIGRP et OSPF dans une organisation.

D'après le tableau ci-dessus qui montre une étude comparative des trois protocoles dans un réseau d'entreprise, nous pouvons dire que le protocole de routage dynamique OSPF est le plus utilisé par les grandes entreprises car c'est un protocole standard et il est basé sur des normes ouvertes.

3.7 Synthèse

Nous avons remarqué que les trois protocoles de routage dynamique (RIPv2, OSPF et EIGRP) les plus utilisés malgré les points forts de ces protocoles, ils souffrent de certaines limitations.

RIPv2 constitue un excellent moyen pédagogique pour aborder la problématique du routage dynamique. Mais il est peu utilisé en exploitation car il souffre de certaines limitations et défauts qui le rendent applicable à des réseaux de taille moyenne. Nous avons vu que le diamètre maximum d'un réseau géré avec RIPv2 est limité à 15 routeurs.

RIPv2 est un gros consommateur de bande passante du fait de la méthode utilisée pour diffuser les informations de routage (toutes les 30 secondes, l'intégralité de la table RIPv2 est diffusée même si elle n'a subi aucune modification). La métrique utilisée ne garantit pas que le routage soit optimal.

EIGRP est un protocole défini comme à la fois puissant et simple à configurer, il est particulièrement adapté aux réseaux de grande taille.

C'est un protocole développé par Cisco et est donc, de ce fait, un protocole propriétaire réservé qu'aux produits de marque Cisco. Il ne peut par conséquent être configuré sous une autre plateforme.

Nous avons aussi remarqué que le protocole OSPF est aujourd'hui l'un des protocoles de routage interne le plus utilisé, de par sa force et sa robustesse, mais également grâce à sa licence basée sur des normes ouvertes, qui lui confère un avantage sur des protocoles propriétaires tel que EIGRP de Cisco.

3.8 Conclusion

Ce chapitre nous a montré un aperçu sur le fonctionnement et les objectifs des protocoles IGP. Nous avons choisi les trois protocoles RIPv2, OSPF et EIGRP qui ont été élaboré et cela par l'illustration de leur fonctionnement, leur atouts ainsi que leur inconvénients, nous avons également présenté une comparaison entre ces trois protocoles.

Le chapitre suivant, quand à lui, sera consacré à l'implémentation des trois protocoles dans un réseau d'entreprise, nous exposerons le simulateur *GNS3* utilisé pour les étudier et les configurer avec une topologie réseau . Chose qui se réalisera en détaillant les différentes interfaces qui présenteront les configurations utilisées.

CHAPITRE 4

Configuration et choix de protocoles de routage dynamique pour un réseau d'entreprise

4.1 Introduction

Dans le présent chapitre, nous décrirons les caractéristiques de l'environnement GNS3 et les raisons qui le rend adaptif à la mise en place des topologies réseaux.

Nous allons ensuite, montrer la configuration des différents éléments d'interconnexion, en commençant par la présentation du schéma global de la nouvelle topologie avec le développement du matériel et les technologies utilisées dans les solutions ainsi que la mise en place de celles-ci.

Une présentation et une explication de la configuration de ces éléments seront également illustrées en donnant un aperçu des interfaces, un choix d'un protocole de routage dynamique le mieux adapté à la topologie réseau de l'entreprise sera aussi fait.

4.2 Présentation du projet

Le projet à réaliser s'intitule *«Choix d'un protocole de routage dynamique dans un réseau d'entreprise : Cas de CEVITAL»*.

L'intérêt majeur de ce travail est pour nous, une étude des trois protocoles de routage dynamique pour appliquer les concepts théoriques concernant les routeurs à des cas pratiques afin d'assimiler les notions élémentaires de protocoles, de routage, et plus largement l'activité des éléments actifs d'un réseau.

L'implémentation de ces protocoles sera appliquée dans un environnement de travail nommé GNS3. En effet, la communication entre les sites d'interconnexion devient plus facile et efficace dans cet environnement.

4.3 Problématique

De nombreuses difficultés de communication et de diffusion d'informations sont rencontrées lors de l'utilisation des liaisons satellitaires VSAT, parmi lesquels nous avons le problème du coût. En effet, la hausse de celui-ci ne permet pas à certaines entreprises son achat. En plus, si l'élément central du VAST « le hub » tombe en panne, cela empêche la communication entre les différents sites du réseau.

Pour pallier à ces problèmes, nous avons remplacé ces liaisons par d'autres spécialisées comme des routeurs Cisco.

Sans oublier les problèmes rencontrés lors de l'utilisation du routage statique et du protocole de routage dynamique EIGRP, ce qui nous a encouragés à proposer d'employer d'autres protocoles de routage dynamique, à savoir : RIPv2 et OSPF, en plus d'EIGRP pour choisir le protocole le plus préférable, pour qu'il soit configuré sur la topologie réseau de Cevital.

4.4 Environnement du travail

Pour réaliser notre topologie, nous avons choisi le simulateur graphique GNS3 (version 0.8.3.1), qui est un logiciel utilisé pour la configuration et l'implémentation des réseaux LAN et WAN.

Notre choix s'est focalisé sur GNS3, car il a pour objectif d'apporter de nouvelles technologies de communication aux personnes travaillant dans le domaine de

l'administration réseaux, c'est également une solution pour virtualiser et modéliser les réseaux **[62]**.

Le principal avantage de GNS3 réside dans l'émulation matérielle, car les utilisateurs peuvent tester et évaluer leurs configurations en utilisant celui-ci, avant de les mettre en place physiquement, sans avoir à financer le matériel **[62]**.

Nous présenterons dans ce qui suit cet outil de simulation qui est conçu pour la comparaison et l'évaluation des protocoles de routage dynamique cités ci-dessus.

4.4.1 GNS 3

GNS3 (*Graphical Network Simulator 3)* est un logiciel open source qui permet de simuler graphiquement une architecture réseau. L'utilisateur, via un système simple peut construire un réseau à partir d'un large choix de dispositifs *(switchs, routeurs, hôtes, etc.)* et peut ainsi créer des liens physiques entre eux, autant que les démarrer virtuellement grâce aux émulateurs *Qemu*, *Dynamips* (l'émulateur d'IOS) et *Dynagen* (interface texte pour Dynamips) **[59]**.

4.4.1.1 Dynamips

Dynamips est un émulateur de routeurs Cisco capable de faire fonctionner des images Cisco IOS non modifiées du système d'exploitation. Son rôle n'est pas de remplacer de véritables routeurs, mais de permettre la réalisation de maquettes complexes avec de vraies versions d'IOS. Il fonctionne uniquement en ligne de commande **[60]**.

Les gammes de routeurs émulés sont **[60]**:

- ✓ Cisco 7200 (NPE-100 jusqu'à NPE-400, NPE-G2)
- ✓ Cisco 3600 (3620, 3640, 3660)
- ✓ Cisco 3700 (3725, 3745)
- ✓ Cisco 2600 (2610 à 2651XM, 2691)
- ✓ Cisco 1700 (1710 à 1760)

De différentes instances de l'émulateur peuvent être interconnectées à travers des interfaces qui sont de type **[60]**:

- ✓ Ethernet, FastEthernet, GigabitEthernet,
- ✓ Série,
- ✓ ATM (Cisco 7200 uniquement),

- ✓ POS (Cisco 7200 uniquement).

4.4.1.2 Dynagen [60]

Dynagen est un produit supplémentaire écrit en Python s'interfaçant avec *Dynamips* grâce au mode hyperviseur qui est une instance de Dynamips permettant la gestion des routeurs virtuels locaux (création, suppression, démarrage, arrêt, etc.) et des interconnexions réseau.

Il facilite la création et la gestion de maquettes grâce à un fichier de configuration simple décrivant la topologie du réseau à simuler et une interface texte interactive.

4.4.1.3 QEMU

QEMU est un logiciel libre d'émulation de processeur et de machine virtuelle, permettant d'exécuter un ou plusieurs systèmes d'exploitation dans un environnement où un système d'exploitation est déjà installé sur la machine **[61]**.

4.5 Optimisation [63]

Pour éviter d'avoir la charge de la CPU à 100% et la difficulté de travailler simultanément sur plusieurs routeurs, une solution consiste à modifier l'utilisation de la CPU pour chaque périphérique réseau. Cette optimisation implique de trouver la valeur *« IDLE PC »* optimale pour une image IOS.

Depuis les dernières versions, et notamment la version 0.8.3.1 sur laquelle a été réalisée la configuration de notre topologie réseau, ce calcul est réalisé par le programme. Voici les étapes à suivre :

1) Nous sélectionnons le routeur concerné, et nous cliquons sur IDLE PC :

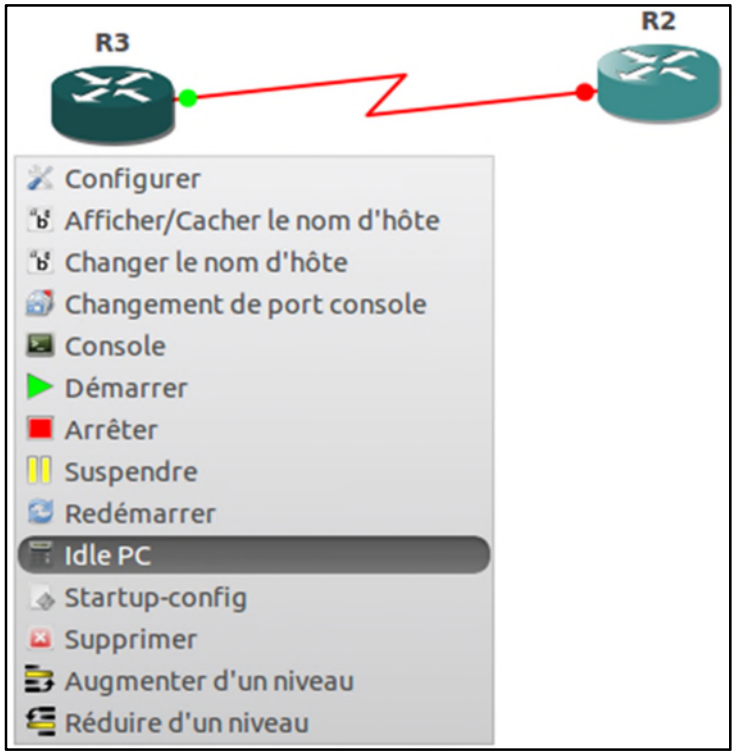


Figure 4.1 : Calcul de la valeur IDLE PC.

2) Le programme affiche les meilleures valeurs potentielles après un calcul effectué et le choix se focalise sur la valeur qui commence par une étoile (*) :

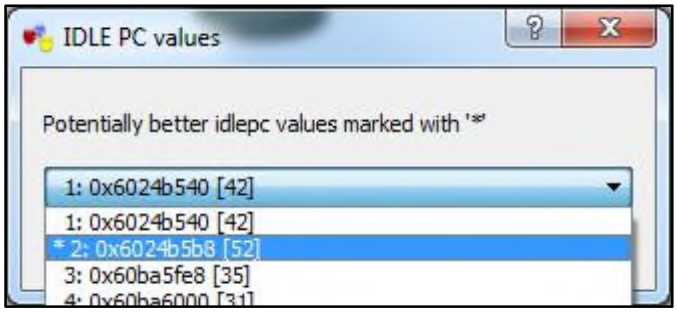


Figure 4.2 : Le choix de la valeur IDLE PC.

4.6 Mise en place d'une topologie

La figure 4.3 illustre la topologie que nous avons utilisée durant notre travail. Elle est composée de huit routeurs nommés : Bejaia, Alger, Bouira, Bejaia 2, Constantine, LLK, Elkseur et Oran, du type Cisco 2691, d'un switch appelé R9 et est émulé par l'interface Cisco 3700 et d'un routeur-firewall R17 du type 2691 également.

Les routeurs sont interconnectés par des liens séries comportant chacun une adresse réseau, le switch utilisé dans cette architecture est de niveau 3 qui a le même rôle et configuration que celui d'un routeur, avec des liaisons Ethernet pour l'interconnecter à d'autre équipements.

Nous avons également représenté les sous réseaux avec des nuages en attribuant des adresses réseaux.

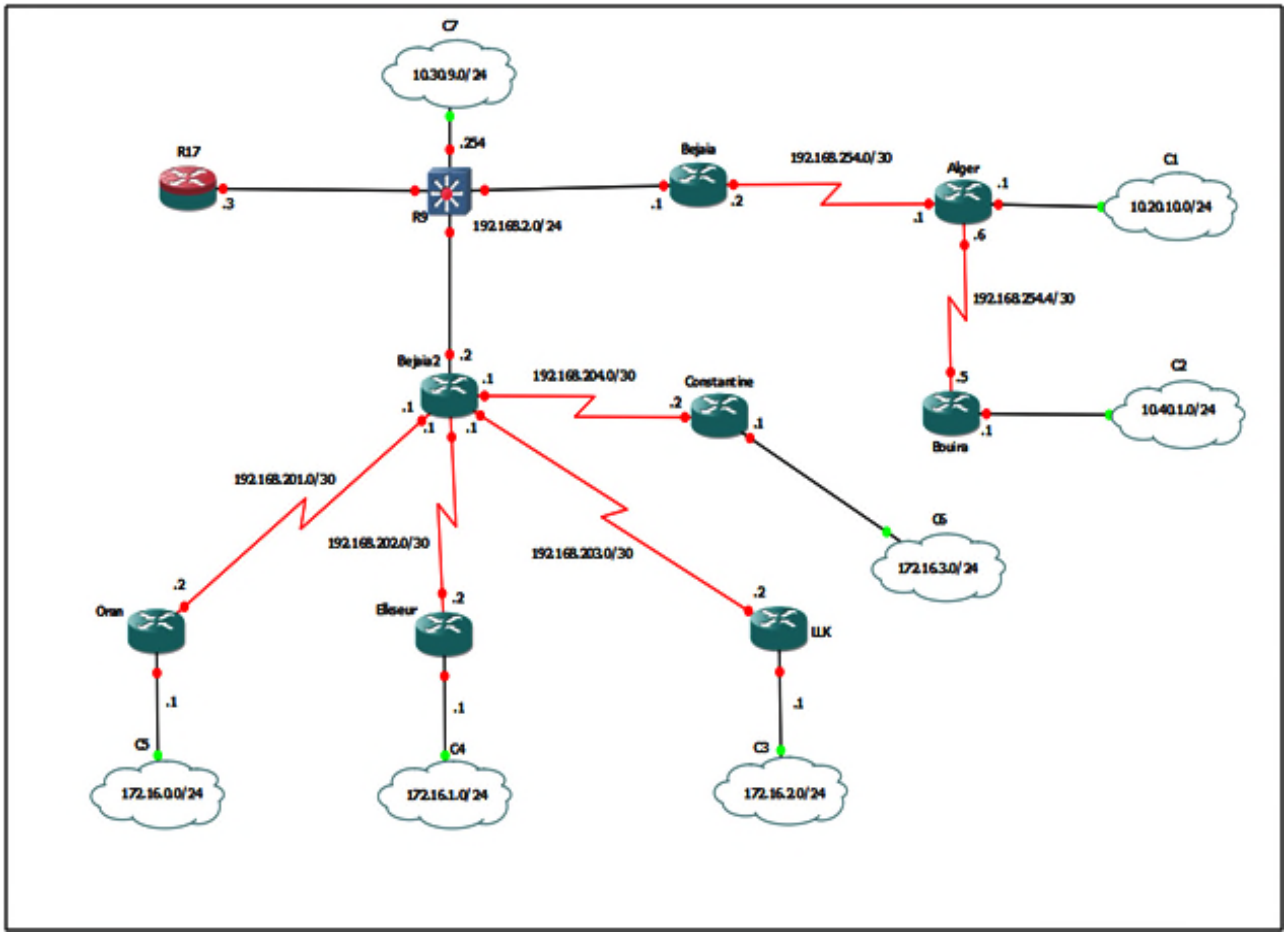


Figure 4.3 : Représentation de la topologie réseau.

4.7 Configuration du protocole RIPv2

4.7.1 La commande router rip

Pour activer le protocole de routage RIP, nous devons passer en mode de configuration global et utiliser la commande « *router rip*». Cette commande fournit un accès permettant de configurer les paramètres du protocole de routage pour activer le routage pour un réseau particulier.

La commande employée qui permet d'ajouter une route à un routeur est la suivante : *« network adresse du réseau »*. Elle est nécessaire car elle permet au processus de routage de déterminer les interfaces qui participeront à l'envoi et à la réception des mises à jour du routage. L'adresse du réseau indique le réseau directement connecté.

Il y a deux versions de ce protocole : RIPv1 et RIPv2. Nous avons utilisé la version 2, ainsi la commande est : « *version 2* ».

```
Bejaia2#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Bejaia2(config)#router rip
Bejaia2(config-router)#version 2
Bejaia2(config-router)#network 192.168.201.0
Bejaia2(config-router)#network 192.168.202.0
Bejaia2(config-router)#network 192.168.203.0
Bejaia2(config-router)#network 192.168.204.0
Bejaia2(config-router)#network 192.168.2.0
Bejaia2(config-router)#end
Bejaia2#
*Mar  1 00:03:01.751: %SYS-5-CONFIG_I: Configured from console by console
Bejaia2#
```

Figure 4.4: Activation du protocole RIPv2.

4.7.2 Consultation des informations relatives au protocole de routage

La commande *« show ip protocol »* vérifie plusieurs éléments critiques, notamment l'activation de RIP, sa version, l'état du résumé automatique et les réseaux inclus dans les instructions réseau.

```
Bejaia2#show ip protocol
Routing Protocol is "rip"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Sending updates every 30 seconds, next due in 11 seconds
  Invalid after 180 seconds, hold down 180, flushed after 240
  Redistributing: rip
  Default version control: send version 2, receive version 2
    Interface             Send  Recv  Triggered RIP  Key-chain
    FastEthernet0/0       2     2
    Serial1/0             2     2
    Serial1/1             2     2
    Serial1/2             2     2
    Serial1/3             2     2
  Automatic network summarization is not in effect
  Maximum path: 4
  Routing for Networks:
    192.168.2.0
    192.168.201.0
    192.168.202.0
    192.168.203.0
    192.168.204.0
  Routing Information Sources:
    Gateway         Distance      Last Update
  Distance: (default is 120)
```

Figure 4.5 : Consultation des informations de routage.

La ligne possédant les informations suivantes : « *Default version control : send version 2, receive version 2*» signifie que les mises à jour sont envoyées et reçu en utilisant le protocole de routage RIP version 2.

Le routeur de cet exemple envoie des mises à jour de routage toutes les *30 secondes* (intervalle configuré), neuf à dix secondes se sont écoulées depuis l'envoi de la dernière mise à jour; la prochaine sera envoyée dans 11 secondes.

Après la ligne « *Routing for Networks* », le routeur indique les routes pour les réseaux affichés.

La dernière ligne *« Distance : (default is 120) »* indique que la distance administrative par défaut du protocole RIP est de *« 120 »*.

4.7.3 Désactivation du récapitulatif automatique

Cette commande n'est pas disponible dans RIPv1. Elle a pour objectif de désactiver le résumé automatique des routes des routeurs et nous pouvons donc désactiver le résumé automatique de routes en utilisant la commande illustrée dans la

figure 4.6. Une fois le résumé désactivé, RIPv2 ne résume plus les réseaux dans leur adresse par classe au niveau des routeurs.

```
Bejaia2#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Bejaia2(config)#router rip
Bejaia2(config-router)#version 2
Bejaia2(config-router)#no auto-summary
Bejaia2(config-router)#end
Bejaia2#
```

Figure 4.6 : La commande « no auto-summray ».

4.7.4 La commande show ip interface brief

Cette commande permet de vérifier l'état de toutes les routes, si nous avons mal configuré une interface en raison de l'absence d'un réseau dans une table de routage, cette commande permet d'afficher l'état et les paramètres globaux associés à des interfaces.

```
Bejaia2#show ip interface brief
Interface                  IP-Address      OK? Method Status                Protocol
FastEthernet0/0            192.168.2.2     YES NVRAM  up                    up
FastEthernet0/1            unassigned      YES NVRAM  administratively down down
Serial1/0                  192.168.204.1   YES NVRAM  up                    up
Serial1/1                  192.168.201.1   YES NVRAM  up                    up
Serial1/2                  192.168.202.1   YES NVRAM  up                    up
Serial1/3                  192.168.203.1   YES NVRAM  up                    up
```

Figure 4.7 : Affichage des interfaces d'un équipement d'interconnexion.

Les différentes interfaces du routeur Bejaia2 sont illustrées dans la figure précédente, les champs d'une ligne sont expliqués comme suit :

Champ	Explication
Interface	Indique le nom de l'interface utilisée.
IP-Address	Représente l'adresse IP de l'interface utilisée.
Status	C'est le mode de l'interface, activé (UP) ou désactivé (DOWN).
Protocol	Indique le mode du protocole utilisé par l'administrateur.

Tableau 4.1 : Les champs de la commande « show ip interface brief ».

4.7.5 La route par défaut RIPv2

L'utilisation de la route statique vers 0.0.0.0/0 comme route par défaut ne dépend pas du protocole de routage. Elle peut être utilisée avec n'importe quel protocole de routage pris en charge.

Cette route statique par défaut est en général configurée sur un routeur qui possède une connexion vers un réseau situé en dehors du domaine de routage RIPv2, par exemple, vers un firewall (le routeur R17).

RIPv2 nécessite l'utilisation de la commande *« redistribute static »* pour inclure cette route dans les mises à jour de routage RIPv2 et lui demande d'inclure cette route dans ces mises à jour vers les autres routeurs.

La figure 4.8 montre la configuration de cette route sur le routeur R9.

```
R9#config t
Enter configuration commands, one per line.  End with CNTL/Z.
R9(config)#ip route 0.0.0.0 0.0.0.0 fa
R9(config)#ip route 0.0.0.0 0.0.0.0 fastEthernet 1/1
R9(config)#router rip
R9(config-router)#version 2
R9(config-router)#redistribute static
R9(config-router)#default-information originate
R9(config-router)#end
R9#
```

Figure 4.8 : Configuration de la route statique par défaut.

Les routes par défaut fournissent un chemin par défaut vers l'extérieur du domaine de routage, dans notre cas tous les paquets utiliseront par défaut l'interface de sortie avec l'adresse IP 192.168.2.254.

L'examen de la table de routage est illustré dans la figure 4.9 suivante :

```
Bejaia2#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is 192.168.2.254 to network 0.0.0.0

     10.0.0.0/24 is subnetted, 1 subnets
R       10.30.9.0 [120/1] via 192.168.2.254, 00:00:29, FastEthernet0/0
C    192.168.2.0/24 is directly connected, FastEthernet0/0
R*   0.0.0.0/0 [120/1] via 192.168.2.254, 00:00:29, FastEthernet0/0
```

Figure 4.9 : Consultation de la table de routage.

La nouvelle ligne contient les informations suivantes :

R : Signifie que la route statique a été acquise au moyen d'une mise à jour de routage RIP.

** :* La route est une route par défaut potentielle.

4.7.6 Vérification des informations de routage

La commande à utiliser pour vérifier la convergence du réseau est *« show ip route »*, elle permet d'afficher le contenu de la table de routage IP actuelle , soit une entrée pour chacun des réseaux et sous-réseaux connus ainsi qu'un code indiquant comment cette information a été obtenue. Il est important de vérifier si la table de routage contient les routes qui doivent y figurer lors de l'utilisation de cette commande.

L'exemple ci-dessous montre les différentes lignes que comporte une table de routage :

```
Bejaia2#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is 192.168.2.254 to network 0.0.0.0

     172.16.0.0/24 is subnetted, 4 subnets
R       172.16.0.0 [120/1] via 192.168.201.2, 00:00:24, Serial1/1
R       172.16.1.0 [120/1] via 192.168.202.2, 00:00:06, Serial1/2
R       172.16.2.0 [120/1] via 192.168.203.2, 00:00:20, Serial1/3
R       172.16.3.0 [120/1] via 192.168.204.2, 00:00:26, Serial1/0
     192.168.201.0/30 is subnetted, 1 subnets
C       192.168.201.0 is directly connected, Serial1/1
     192.168.202.0/30 is subnetted, 1 subnets
C       192.168.202.0 is directly connected, Serial1/2
     10.0.0.0/24 is subnetted, 1 subnets
R       10.30.9.0 [120/1] via 192.168.2.254, 00:00:07, FastEthernet0/0
     192.168.203.0/30 is subnetted, 1 subnets
C       192.168.203.0 is directly connected, Serial1/3
     192.168.204.0/30 is subnetted, 1 subnets
C       192.168.204.0 is directly connected, Serial1/0
C    192.168.2.0/24 is directly connected, FastEthernet0/0
R*   0.0.0.0/0 [120/1] via 192.168.2.254, 00:00:09, FastEthernet0/0
```

Figure 4.10 : Affichage de la table de routage.

Les réseaux découverts par le protocole RIPv2 sont précédés par la lettre « *R* », les réseaux directement connectés et configurés manuellement sont précédés par la lettre « *C* ».

Les routeurs Cisco supportent plusieurs routes différentes sur le même routeur et simultanément. Les résultats qu'affiche cette commande sont les symboles présentés dans la figure 4.10 :

« *I* » dérivé de IGRP ; « *D* » dérivé de EIGRP ; « *O* » dérivé du protocole OSPF ; « *R* » dérivé de RIP ; « *E* » dérivé de EGP et « *B* » dérivé de BGP.

Nous prenons comme exemple la ligne suivante : « *C 192.168.203.0/30 is directely connected, Serial 1/3* ». Il faut la lire ainsi :

C : signifie le réseau directement connecté au routeur et configuré via la commande *Network.*

192.168.203.0/30 : Fournit l'adresse du réseau.

Serial 1/3 : Spécifie par quelle interface le réseau peut être atteint.

4.7.7 La commande debug ip rip

La commande *« debug ip rip »* a pour rôle de voir dynamiquement les échanges d'information sur les routes entre les routeurs voisins pour lesquelles le protocole RIPv2 est activé, donc elle permet d'examiner le contenu des mises à jour de routage envoyées et reçues par un routeur. La figure 4.11 montre le résultat de cette commande :

```
Bouira#debug ip rip
RIP protocol debugging is on
Bouira#
*Mar  1 00:17:03.919: RIP: received v2 update from 192.168.254.6 on Serial1/0
*Mar  1 00:17:03.919:      0.0.0.0/0 via 0.0.0.0 in 3 hops
*Mar  1 00:17:03.923:      10.20.10.0/24 via 0.0.0.0 in 1 hops
*Mar  1 00:17:03.927:      10.30.9.0/24 via 0.0.0.0 in 3 hops
*Mar  1 00:17:03.931:      172.16.0.0/24 via 0.0.0.0 in 4 hops
*Mar  1 00:17:03.931:      172.16.1.0/24 via 0.0.0.0 in 4 hops
*Mar  1 00:17:03.935:      172.16.2.0/24 via 0.0.0.0 in 4 hops
*Mar  1 00:17:03.939:      172.16.3.0/24 via 0.0.0.0 in 4 hops
*Mar  1 00:17:03.943:      192.168.2.0/24 via 0.0.0.0 in 2 hops
*Mar  1 00:17:03.947:      192.168.201.0/30 via 0.0.0.0 in 3 hops
Bouira#
*Mar  1 00:17:03.947:      192.168.202.0/30 via 0.0.0.0 in 3 hops
*Mar  1 00:17:03.951:      192.168.203.0/30 via 0.0.0.0 in 3 hops
*Mar  1 00:17:03.955:      192.168.204.0/30 via 0.0.0.0 in 3 hops
*Mar  1 00:17:03.959:      192.168.254.0/30 via 0.0.0.0 in 1 hops
```

Figure 4.11 : La commande « debug ip rip ».

La ligne *« RIP: received v2 update to 192.168.254.6 on Serial1/0 »* signifie que les informations proviennent d'un routeur qui utilise la commande *« debug ip rip »* après avoir reçu une mise à jour RIPv2.

Après avoir reçu et traité la mise à jour, le routeur envoie les informations récemment modifiées à ses interfaces RIPv2. Les informations affichées indiquent que le routeur utilise le protocole RIP version 2 et reçoit la mise à jour d'une adresse 192.168.254.6 et cela à travers l'interface *Serial1/0*.

4.7.8 Vérification de la configuration courante

Pour afficher le résumé de la configuration globale d'une machine, nous avons utilisé la commande *« show running-config »* comme présenté dans la figure 4.12 suivante :

```
Bejaia2#show running-config
Building configuration...

Current configuration : 1403 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Bejaia2
!
interface FastEthernet0/0
 ip address 192.168.2.2 255.255.255.0
 speed 100
 full-duplex
!
interface FastEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface Serial1/0
 ip address 192.168.204.1 255.255.255.252
 serial restart-delay 0
 no dce-terminal-timing-enable
!
interface Serial1/1
 ip address 192.168.201.1 255.255.255.252
 serial restart-delay 0
 no dce-terminal-timing-enable
!
interface Serial1/2
 ip address 192.168.202.1 255.255.255.252
 serial restart-delay 0
 no dce-terminal-timing-enable
!
interface Serial1/3
 ip address 192.168.203.1 255.255.255.252
 serial restart-delay 0
 no dce-terminal-timing-enable
!
router rip
 version 2
 network 192.168.2.0
 network 192.168.201.0
 network 192.168.202.0
 network 192.168.203.0
 network 192.168.204.0
 no auto-summary
!
```

Figure 4.12 : Affichage de la configuration courante.

4.8 Configuration du protocole EIGRP

4.8.1 La commande router eigrp

L'activation du protocole EIGRP sur un routeur se fait à l'aide de la commande « *router eigrp num système autonome* » dans le mode de configuration globale, avec l'attribution de la valeur « *40* » pour le système autonome.

La commande utilisée pour la configuration des réseaux par classe est *« network adresse du réseau masque générique »*, l'utilisation de l'option « *masque-générique* » avec cette commande est nécessaire pour annoncer uniquement le sous-réseau et non l'intégralité du réseau par classe.

La commande qui permet l'enregistrement de la configuration active dans la mémoire vive non volatile est *« write »* et cela en mode d'exécution privilégié. La figure 4.13 suivante montre l'utilisation de ces commandes sur le routeur Béjaia 2.

```
Bejaia2#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Bejaia2(config)#router eigrp 40
Bejaia2(config-router)#network 192.168.201.0 0.0.0.3
Bejaia2(config-router)#network 192.168.202.0 0.0.0.3
Bejaia2(config-router)#network 192.168.203.0 0.0.0.3
Bejaia2(config-router)#network 192.168.204.0 0.0.0.3
Bejaia2(config-router)#network 192.168.2.0 0.0.0.255
Bejaia2(config-router)#end
Bejaia2#
*Mar  1 00:29:46.779: %SYS-5-CONFIG_I: Configured from console by console
Bejaia2#write
Building configuration...
[OK]
```

Figure 4.13: Activation du protocole EIGRP.

Remarque

Le masque générique est considéré comme l'inverse d'un masque de sous-réseau. L'inverse du masque de sous-réseau 255.255.255.252 est 0.0.0.3, pour effectuer le calcul , nous procédons comme suit :

(255.255.255.255 – 255.255.255.252) = *« 0. 0. 0. 3 »* masque générique utilisé.

Lorsque les réseaux des liaisons séries d'autres routeurs sont ajoutés à la configuration EIGRP (le routeur *Constantine* à *Bejaia2* par exemple), l'algorithme DUAL envoie un message de notification à la console indiquant qu'une relation de voisinage a été établie avec un autre routeur EIGRP comme illustré ci-dessous :

```
LLK#config t
Enter configuration commands, one per line.  End with CNTL/Z.
LLK(config)#router eigrp 40
LLK(config-router)#network 192.168.203.0 0.0.0.3
LLK(config-router)#
*Mar  1 00:01:53.067: %DUAL-5-NBRCHANGE: IP-EIGRP(0) 40: Neighbor 192.1
68.203.1 (Serial1/0) is up: new adjacency
LLK(config-router)#network 172.16.2.0 0.0.0.255
LLK(config-router)#end
*Mar  1 00:02:22.139: %SYS-5-CONFIG_I: Configured from console by conso
le
LLK#write
Building configuration...
[OK]
```

Figure 4.14 : Message de notification de DUAL.

4.8.2 Affichage des voisins EIGRP

Nous avons employé la commande *« show ip eigrp neighbors »* pour afficher la table des voisins du routeur Bejaia2. Il y aura l'affichage de l'adresse IP de chaque routeur adjacent et l'interface qu'utilise le routeur Bejaia2 pour atteindre ces voisins EIGRP.

```
Bejaia2#show ip eigrp neighbors
IP-EIGRP neighbors for process 40
H   Address                 Interface       Hold Uptime   SRTT   RTO  Q  Seq
                                            (sec)         (ms)       Cnt Num
3   192.168.201.2           Se1/1             10 00:00:41 1020  5000  0  3
2   192.168.202.2           Se1/2             14 00:00:51  100   600  0  4
1   192.168.203.2           Se1/3             11 00:00:59   93   558  0  5
0   192.168.204.2           Se1/0             12 00:54:49   70   420  0  6
```

Figure 4.15: Affichage des voisins EIGRP.

La sortie de la commande inclut les champs suivants :

Champ	Explication
Colonne H	Répertorie les voisins dans l'ordre dans lequel ils ont été détectés.
Address	Ce champ contient l'adresse IP du voisin.
Interface	Représente l'interface locale sur laquelle un paquet Hello a été reçu.
Hold	C'est le délai d'attente en cours. Lorsqu'un paquet Hello est reçu, cette valeur revient au temps d'attente maximum de cette interface, puis un compte s'effectue jusqu'à zéro. Si la valeur zéro est atteinte, le voisin est considéré comme « hors service ».
Uptime	C'est la période qui s'est écoulée depuis que le voisin a été ajouté à la table de voisinage.
SRTT (Smooth Round Trip Timer)	Représente le temps moyen nécessaire pour envoyer un message et recevoir sa réponse d'un voisin.
RTO (Retransmission TimeOut)	C'est le temps pendant lequel le logiciel attend avant de renvoyer un paquet de la file d'attente de retransmission à un voisin.
Queue Count (En attente d'envoi)	C'est le nombre de paquets EIGRP (mise à jour, demande et réponse) que le logiciel attend pour envoyer. Si cette valeur est supérieure à « 0 », un problème de congestion pourrait exister (cela signifie que des paquets EIGRP attendent pour être envoyés). La valeur « 0 » indique qu'aucun paquet EIGRP n'est en file d'attente.
Seq Num (Numéro d'ordre)	C'est le numéro de séquence de la dernière mise à jour, requête ou paquet de réponse qui a été reçu d'un voisin.

Tableau 4.2 : Les champs de la table de voisinage EIGRP.

4.8.3 Consultation des informations relatives au protocole EIGRP

Sur le routeur Bejaia2, nous avons utilisé la commande « *show ip protocols* » pour visualiser les informations liées au fonctionnement du protocole de routage. Les informations configurées précédemment : l'identifiant du processus , notamment le protocole, les réseaux et les adresses IP des voisins contigus apparaissent dans la sortie, sans oublier l'affichage des paramètres utilisés pour le calcul de la valeur composite de la métrique EIGRP (K1, K2, K3, K4 et K5).

```
Bejaia2#show ip protocols
Routing Protocol is "eigrp 40"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Default networks flagged in outgoing updates
  Default networks accepted from incoming updates
  EIGRP metric weight K1=1, K2=0, K3=1, K4=0, K5=0
  EIGRP maximum hopcount 100
  EIGRP maximum metric variance 1
  Redistributing: eigrp 40
  EIGRP NSF-aware route hold timer is 240s
  Automatic network summarization is not in effect
  Maximum path: 4
  Routing for Networks:
    192.168.2.0
    192.168.201.0/30
    192.168.202.0/30
    192.168.203.0/30
    192.168.204.0/30
  Routing Information Sources:
    Gateway         Distance      Last Update
    (this router)         90      00:00:26
  Distance: internal 90 external 170
```

Figure 4.16 : Affichage des informations relatives au protocole EIGRP.

Concernant la dernière ligne qui affiche la distance administrative de chaque protocole, nous avons remarqué que la valeur de celle-ci est *« 90 »*, comparé à RIPv2, le protocole EIGRP est préféré. Nous avons également l'affichage de la distance administrative d'une route EIGRP externe qui a la valeur *« 170 »*.

4.8.4 Désactivation du récapitulatif automatique

EIGRP résume, par défaut, les routes afin de préserver les tables de routage. C'est la fonction « *auto-summary* » qui permet ce résumé automatique. Nous allons dans ce qui suit désactiver cette fonction et paramétrer les résumés de routes avec EIGRP et cela sur chacun des routeurs, cette fonction sera désactivée pour forcer le protocole

EIGRP à signaler tous les sous-réseaux , grâce à la commande *« no auto-summary »*. C'est la même commande que celle utilisée par le protocole RIPv2.

```
Bejaia2#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Bejaia2(config)#router eigrp 40
Bejaia2(config-router)#no auto-summary
Bejaia2(config-router)#end
Bejaia2#
*Mar  1 00:01:11.587: %SYS-5-CONFIG_I: Configured from console by console
Bejaia2#
```

Figure 4.17 : La commande « no auto-summary ».

4.8.5 Configuration du résumé manuel

Le protocole EIGRP a la particularité de configurer le résumé manuel. La commande *« ip summary-address eigrp num system autonome adresse du résumé de routes masque du résumé de routes »* permet de configurer le récapitulatif manuel sur chacune des interfaces de sortie connectées aux voisins EIGRP.

Les routes à destination des réseaux 192.168.1.0/30, 192.168.2.0/30, 192.168.3.0/30 et 192.168.4.0/30 peuvent être résumées dans le réseau unique 192.168.0.0/21 avec le masque 255.255.248.0.

```
Bejaia2#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Bejaia2(config)#interface s1/0
Bejaia2(config-if)#ip summary-address eigrp 40 192.168.200.0 255.255.248.0
Bejaia2(config-if)#exit
Bejaia2(config)#interface s1/1
Bejaia2(config-if)#ip summary-address eigrp 40 192.168.200.0 255.255.248.0
Bejaia2(config-if)#exit
Bejaia2(config)#interface s1/2
Bejaia2(config-if)#ip summary-address eigrp 40 192.168.200.0 255.255.248.0
Bejaia2(config-if)#exit
Bejaia2(config)#interface s1/3
Bejaia2(config-if)#ip summary-address eigrp 40 192.168.200.0 255.255.248.0
Bejaia2(config-if)#exit
Bejaia2(config)#interface fa0/0
Bejaia2(config-if)#ip summary-address eigrp 40 192.168.200.0 255.255.248.0
Bejaia2(config-if)#end
Bejaia2#
*Mar  1 00:16:41.963: %SYS-5-CONFIG_I: Configured from console by consolew
Bejaia2#write
Building configuration...
[OK]
```

Figure 4.18 : Configuration du résumé manuel.

Le résumé de route a pour but de réduire le nombre d'entrées (routes) dans la table de routage, ce qui rend le processus de recherche dans cette table plus efficace. Les résumés de routage utilisent moins de bande passante pour les mises à jour de routage parce qu'une seule route peut être envoyée au lieu de plusieurs routes individuelles.

Pour vérifier que le résumé figure dans les mises à jour EIGRP envoyées par le routeur Bejaia2 vers les routeurs voisins, nous avons consulté la table de routage de l'un de ces routeurs (exemple : *Bejaia*).

```
Bejaia#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is 192.168.2.254 to network 0.0.0.0

     172.16.0.0/24 is subnetted, 3 subnets
D       172.16.1.0 [90/2198016] via 192.168.2.2, 00:00:40, FastEthernet0/0
D       172.16.2.0 [90/2198016] via 192.168.2.2, 00:00:41, FastEthernet0/0
D       172.16.3.0 [90/2198016] via 192.168.2.2, 00:00:40, FastEthernet0/0
     10.0.0.0/24 is subnetted, 1 subnets
D       10.30.9.0 [90/30720] via 192.168.2.254, 00:00:41, FastEthernet0/0
C    192.168.2.0/24 is directly connected, FastEthernet0/0
D*EX 0.0.0.0/0 [170/30720] via 192.168.2.254, 00:00:45, FastEthernet0/0
D    192.168.200.0/21 [90/2172416] via 192.168.2.2, 00:00:44, FastEthernet0/0
```

Figure 4.19 : Consultation de la table de routage.

La ligne : *« D 192.168.200.0/21 [90/2172416] via 192.168.2.2, 00 :00 :44, FastEthernet0/0 »* signifie que nous avons résumé les quatre routes (192.168.201.0, 192.168.202.0, 192.168.203.0 et 192.168.204.0) dans une seule route qui a l'adresse IP suivante : *192.168.200.0/21* et cela dans le but de réduire la taille de la table de routage.

Donc les paquets envoyés par les routeurs possédant les adresses citées seront reçu avec la route résumée.

4.8.6 Examen de la table topologique du protocole EIGRP

La topologie EIGRP d'un routeur , le successeur, la distance de faisabilité et tout successeur potentiel, avec sa distance annoncée, sont conservés par le routeur dans sa

table topologique EIGRP qui peut être affichée à l'aide de la commande *« show ip eigrp topology »*, comme indiqué dans la figure 4.20.

Cette table répertorie tous les successeurs et successeur potentiels que l'algorithme DUAL a calculé vers les réseaux de destination.

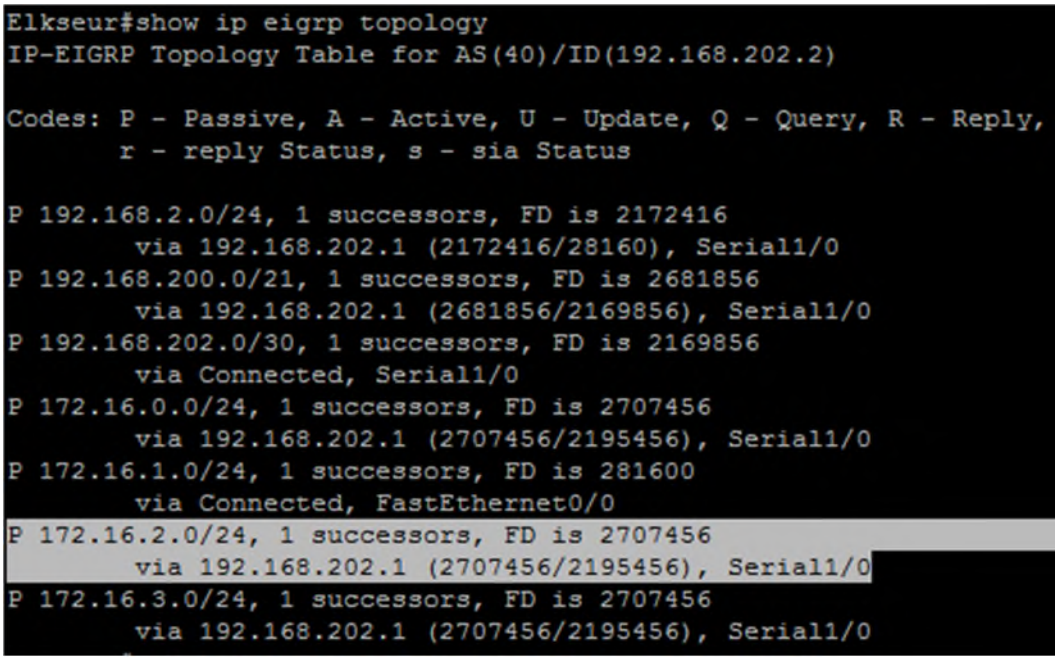


Figure 4.20 : Affichage de la table topologique EIGRP.

Lorsque nous regardons la table topologique du routeur Elkseur dans le schéma, nous voyons que le meilleur chemin EIGRP vers le réseau 172.16.2.0/24 passe par le routeur successeur possédant l'adresse 192.168.202.1 avec une distance de faisabilité de 2195456. La distance de faisabilité vers le réseau de destination (192.168.202.1) est de 2707456, avec l'interface de sortie Serial1/0 permettant d'atteindre ce réseau.

4.8.7 Route par défaut EIGRP

EIGRP nécessite l'utilisation de la commande *« redistribute static »* pour inclure la route statique par défaut dans les mises à jour de routage EIGRP, cette commande demande à EIGRP d'inclure cette route dans ses mises à jour vers les autres routeurs.

La figure 4.21 montre la configuration de la route statique par défaut sur le routeur R9.

```
R9#config t
Enter configuration commands, one per line.  End with CNTL/Z.
R9(config)#ip route 0.0.0.0 0.0.0.0 192.168.2.3
R9(config)#router eigrp 40
R9(config-router)#redistribute static
R9(config-router)#end
R9#
```

Figure 4.21 : Configuration de la route statique par défaut.

La table de routage nous montre que les routes par défaut fournissent un chemin par défaut vers l'extérieur du domaine de routage :

```
Bejaia#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is 192.168.2.254 to network 0.0.0.0

     10.0.0.0/24 is subnetted, 1 subnets
D       10.30.9.0 [90/30720] via 192.168.2.254, 00:00:09, FastEthernet0/0
C    192.168.2.0/24 is directly connected, FastEthernet0/0
D*EX 0.0.0.0/0 [170/30720] via 192.168.2.254, 00:00:09, FastEthernet0/0
```

Figure 4.22 : Consultation de la table de routage.

La nouvelle ligne contient l'information *« D*EX »* qui signifie que la route est une route EIGRP externe, dans ce cas une route statique à l'extérieur du domaine de routage EIGRP.

4.8.8 Les interfaces passives

La commande *« passive-interface nom de l'interface»* est utilisée pour configurer une interface comme passive, afin de contrôler la propagation des informations de routage, elle permet d'empêcher l'envoie des mises à jour de routage sur des interfaces de sous-réseaux et ce pour ne pas surcharger le réseau. Elle permet également des mises à jour pour être échangées normalement sur les autres interfaces.

Dans notre topologie, cette technique est employée sur les interfaces d'entrées vers les sous-réseaux *FastEthernet 0/0* des routeurs suivants : Alger, Bouira, Constantine, LLK, Elkseur et Oran.

```
LLK#config t
Enter configuration commands, one per line.  End with CNTL/Z.
LLK(config)#interface fa0/0
LLK(config-if)#router eigrp 40
LLK(config-router)#passive-interface fa0/0
LLK(config-router)#end
LLK#
```

Figure 4.23 : Configuration d'une interface passive.

4.8.9 Authentification avec le protocole EIGRP

L'ajout de l'authentification des messages EIGRP aux routeurs leur permet d'accepter que les messages de routage des autres routeurs qui connaissent la même clé partagée.

Cette méthode empêche les intrus d'ajouter délibérément ou accidentellement un autre routeur sur le réseau, avec des informations de routage différentes et provoquer un problème. En effet, les tables de routage pourraient être corrompues.

La figure 4.24 illustre les commandes de configuration de l'authentification des messages EIGRP :

```
Bejaia2#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Bejaia2(config)#key chain EIGRP_KEY
Bejaia2(config-keychain)#key 1
Bejaia2(config-keychain-key)#key-string cisco
Bejaia2(config-keychain-key)#interface s1/0
Bejaia2(config-if)#ip authentication mode eigrp 40 md5
Bejaia2(config-if)#ip authentication key-chain eigrp 40 EIGRP_KEY
Bejaia2(config-if)#exit
Bejaia2(config)#interface s1/1
Bejaia2(config-if)#ip authentication mode eigrp 40 md5
Bejaia2(config-if)#ip authentication key-chain eigrp 40 EIGRP_KEY
Bejaia2(config-if)#exit
Bejaia2(config)#interface s1/2
Bejaia2(config-if)#ip authentication mode eigrp 40 md5
Bejaia2(config-if)#ip authentication key-chain eigrp 40 EIGRP_KEY
Bejaia2(config-if)#exit
Bejaia2(config)#interface s1/3
Bejaia2(config-if)#ip authentication mode eigrp 40 md5
Bejaia2(config-if)#ip authentication key-chain eigrp 40 EIGRP_KEY
Bejaia2(config-if)#end
Bejaia2#
*Mar  1 00:07:30.175: %SYS-5-CONFIG_I: Configured from console by console
Bejaia2#write
Building configuration...
[OK]
```

Figure 4.24 : Configuration de l'authentification EIGRP.

4.8.10 Vérification de la configuration courante

La commande *« show running-config »* permet de vérifier les configurations indiquées et expliquées précédemment.

```
Bejaia2#show run
Building configuration...

Current configuration : 2113 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Bejaia2
!
boot-start-marker
boot-end-marker
!
!
no ip domain lookup
ip domain name lab.local
!
!
!
!
!
key chain EIGRP_KEY
 key 1
  key-string cisco
interface FastEthernet0/0
 ip address 192.168.2.2 255.255.255.0
 ip summary-address eigrp 40 192.168.200.0 255.255.248.0 5
 speed 100
 full-duplex
interface Serial1/0
 ip address 192.168.204.1 255.255.255.252
 ip authentication mode eigrp 40 md5
 ip authentication key-chain eigrp 40 EIGRP_KEY
 ip summary-address eigrp 40 192.168.200.0 255.255.248.0 5
 serial restart-delay 0
 no dce-terminal-timing-enable
!
interface Serial1/1
 ip address 192.168.201.1 255.255.255.252
 ip authentication mode eigrp 40 md5
 ip authentication key-chain eigrp 40 EIGRP_KEY
 ip summary-address eigrp 40 192.168.200.0 255.255.248.0 5
 serial restart-delay 0
 no dce-terminal-timing-enable
!
interface Serial1/2
 ip address 192.168.202.1 255.255.255.252
 ip authentication mode eigrp 40 md5
 ip authentication key-chain eigrp 40 EIGRP_KEY
 ip summary-address eigrp 40 192.168.200.0 255.255.248.0 5
 serial restart-delay 0
 no dce-terminal-timing-enable
!
interface Serial1/3
 ip address 192.168.203.1 255.255.255.252
 ip authentication mode eigrp 40 md5
 ip authentication key-chain eigrp 40 EIGRP_KEY
 ip summary-address eigrp 40 192.168.200.0 255.255.248.0 5
router eigrp 40
 network 192.168.2.0
 network 192.168.201.0 0.0.0.3
 network 192.168.202.0 0.0.0.3
 network 192.168.203.0 0.0.0.3
 network 192.168.204.0 0.0.0.3
 no auto-summary
```

Figure 4.25 : Vérification de la configuration.

4.9 Configuration du protocole OSPF

4.9.1 La commande router ospf

Pour activer le protocole OSPF nous avons employé la commande *« router ospf num-processID »*, en mode de configuration globale sur les routeurs de la topologie. Le paramètre *« num-process-ID »* est un nombre choisi par l'administrateur réseau qui représente le numéro du système autonome, à savoir *« 10 »*, il est important car tous les routeurs situés sur ce domaine doivent l'utiliser.

Le paramètre network du protocole OSPF applique une combinaison de « *adresse réseau* » et « *masque générique* » similaire à celle qu'emploie parfois le protocole EIGRP. Contrairement au protocole EIGRP, le protocole OSPF nécessite obligatoirement le masque générique.

Un autre paramètre OSPF nommé « *area-id* » qui fait référence à une zone OSPF qui aura la valeur *« 0 »* sera aussi utilisée dans toutes les instructions network de cette topologie.

```
Bejaia2#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Bejaia2(config)#router ospf 10
Bejaia2(config-router)#router-id 192.168.2.5
Bejaia2(config-router)#network 192.168.201.0 0.0.0.3 area 0
Bejaia2(config-router)#network 192.168.202.0 0.0.0.3 area 0
Bejaia2(config-router)#network 192.168.203.0 0.0.0.3 area 0
Bejaia2(config-router)#network 192.168.204.0 0.0.0.3 area 0
Bejaia2(config-router)#network 192.168.2.0 0.0.0.255 area 0
Bejaia2(config-router)#end
Bejaia2#write
Building configuration...

*Mar  1 00:04:28.723: %SYS-5-CONFIG_I: Configured from console by console[OK]
```

Figure 4.26 : Configuration du protocole OSPF.

Notons que lors de l'ajout d'une liaison série entre le routeur Bejaia2 et le routeur LLK par exemple à la configuration OSPF, ce dernier envoie un message de notification à la console indiquant qu'une relation de voisinage avec un autre routeur a été établie.

```
LLK#config t
Enter configuration commands, one per line.  End with CNTL/Z.
LLK(config)#router ospf 10
LLK(config-router)#router-id 192.168.203.3
LLK(config-router)#network 192.168.203.0 0.0.0.3 area 0
*Mar  1 00:02:50.155: %OSPF-5-ADJCHG: Process 10, Nbr 192.168.2
.5 on Serial1/0 from LOADING to FULL, Loading Done
LLK(config-router)#network 172.16.2.0 0.0.0.255 area 0
LLK(config-router)#end
LLK#writ
*Mar  1 00:03:36.163: %SYS-5-CONFIG_I: Configured from console
by console
LLK#write
Building configuration...
[OK]
```

Figure 4.27 : Affichage de notification avec le protocole OSPF.

Remarque

Nous avons coder les *« router-id »* manuelement dans les configurations OSPF, en effet, par defaut, si cette valeur n'est pas calculé, le routeur choisit auomatiquement l'adresse IP la plus élevée parmi ses interfaces.

L'interêt d'utiliser l'ID du routeur OSPF permet d'identifier de façon unique chaque routeur du domaine de routage OSPF.

4.9.2 Affichage des voisins OSPF

La commande *« show ip ospf neighbor »* permet d'afficher la liste des voisins d'un routeur, la figure 4.28 montre les differents voisins du routeur Bejaia2 qui ont été configurés avec le protocole OSPF.

Notons que, pour le router Bejaia2, il affiche que le DR est le routeur R9, qui porte l'ID de routeur 192.168.2.6 et que le DROTHER est le routeur Bejaia , avec l'ID de routeur 192.168.2.4.

```
Bejaia2#show ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address         Interface
192.168.204.3     0   FULL/  -        00:00:37    192.168.204.2   Serial1/0
192.168.203.3     0   FULL/  -        00:00:34    192.168.203.2   Serial1/3
192.168.202.3     0   FULL/  -        00:00:32    192.168.202.2   Serial1/2
192.168.2.4       1   FULL/DROTHER    00:00:37    192.168.2.1     FastEthernet0/0
192.168.2.6       1   FULL/DR         00:00:30    192.168.2.254   FastEthernet0/0
```

Figure 4.28 : Affichage des voisins OSPF.

Pour chaque voisin, cette commande affiche les éléments suivants :

Champ	Explication
Neighbor ID	Identifiant du routeur voisin.
Pri	Priorité OSPF de l'interface.
State	Etat OSPF de l'interface. L'état FULL signifie que le routeur et son voisin ont des bases de données d'état des liaisons OSPF identiques.
Dead Time	Durée de temps pendant laquelle le routeur attendra un paquet Hello OSPF du voisin. Cette valeur est réinitialisée lorsque l'interface reçoit un paquet Hello.
Address	Adresse IP de l'interface du voisin à laquelle un routeur est directement connecté.
Interface	Interface sur laquelle une contiguïté a été établie par un routeur avec son voisin.

Tableau 4.3 : Les champs de la table de voisinage OSPF.

4.9.3 Consultation des informations relatives au protocole OSPF

Grâce à la commande *« show ip protocol »* nous pouvons consulter les informations relatives au protocole configuré, elle affiche les différents types de sorties spécifiques à chaque protocole de routage.

```
Bejaia2#show ip protocol
Routing Protocol is "ospf 10"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 192.168.2.5
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    192.168.2.0 0.0.0.255 area 0
    192.168.201.0 0.0.0.3 area 0
    192.168.202.0 0.0.0.3 area 0
    192.168.203.0 0.0.0.3 area 0
    192.168.204.0 0.0.0.3 area 0
 Reference bandwidth unit is 100 mbps
  Routing Information Sources:
    Gateway         Distance      Last Update
  Distance: (default is 110)
```

Figure 4.29 : Affichage des informations relatives au protocole OSPF.

Nous avons constaté que la distance administrative du protocole OSPF est inférieure à celle du protocole RIPv2 et elle est supérieure à celle du protocole EIGRP, en effet, sa valeur par défaut est *« 110 »*.

4.9.4 Route par défaut OSPF

Le protocole OSPF nécessite l'utilisation de la commande *« default-information originate »* pour inclure la route statique par défaut dans ses mises à jour. Bien évidemment ce n'est pas la même commande utilisée avec le protocole EIGRP. La configuration de cette route est présentée dans la figure 4.30 suivante :

```
R9#config t
Enter configuration commands, one per line.  End with CNTL/Z.
R9(config)#ip route 0.0.0.0 0.0.0.0 192.168.2.3
R9(config)#router ospf 10
R9(config-router)#default-information originate
R9(config-router)#end
R9#w
*Mar  1 00:06:32.283: %SYS-5-CONFIG_I: Configured from console by console
R9#write
Building configuration...
[OK]
```

Figure 4.30 : Configuration de la route statique par défaut.

La table de routage nous montre que les routes par défaut fournissent un chemin par défaut vers l'extérieur du domaine de routage :

```
Bejaia2#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is 192.168.2.3 to network 0.0.0.0

     10.0.0.0/24 is subnetted, 1 subnets
O       10.30.9.0 [110/2] via 192.168.2.254, 00:02:07, FastEthernet0/0
C    192.168.2.0/24 is directly connected, FastEthernet0/0
O*E2 0.0.0.0/0 [110/1] via 192.168.2.3, 00:02:07, FastEthernet0/0
```

Figure 4.31 : Consultation de la table de routage.

La nouvelle ligne contient l'information *«O* E2 »* qui signifie que la route est une route OSPF externe du type 2, dans ce cas une route statique à l'extérieur du domaine de routage OSPF.

4.9.5 Les interfaces passives

La configuration d'une interface comme passive pour le protocole OSPF se fait à l'aide de la commande *« passive-interface nom de l'interface»*, elle a le même principe que celle configurée avec le protocole EIGRP et RIPv2.

```
Constantine#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Constantine(config)#interface fa0/0
Constantine(config-if)#router ospf 10
Constantine(config-router)#passive-interface fa0/0
Constantine(config-router)#end
```

Figure 4.32 : Configuration d'une interface passive.

4.9.6 Authentification avec le protocole OSPF

Le protocole OSPF permet l'authentification avec l'utilisation de l'algorithme MD5, c'est un processus qui s'effectue en deux étapes : elle est tout d'abord activée sur un routeur, pour une zone définie, puis configurée sur les interfaces de cette zone. En effet, cette authentification s'active sur l'interface connectée au réseau que nous souhaiterons sécuriser. Dans notre cas nous avons sécurisé la connexion sur *« area 0 »* entre l'interface *S1/0* du routeur *« Bejaia »* et l'interface *S1/0* du routeur *« Alger »*.

Les commandes utilisées sont : *« ip ospf message-digest-key 1 md5 mot de passe »* et *« ip ospf authentication message-digest »* sur notre interface *S1/0* (*mot de passe* étant notre mot de passe), nous configurons ensuite le type d'authentification sur le routeur OSPF via la commande : *« area 0 authentication message-digest »* comme illustré dans la figure 4.33.

```
Alger#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Alger(config)#interface s1/0
Alger(config-if)#ip ospf message-digest-key 1 md5 cisco
Alger(config-if)#ip ospf authentication message-digest
Alger(config-if)#exit
Alger(config)#router ospf 10
Alger(config-router)#area 0 authentication message-digest
Alger(config-router)#end
Alger#
*Mar  1 00:06:28.507: %SYS-5-CONFIG_I: Configured from console by console
Alger#write
Building configuration...
[OK]
```

Figure 4.33 : Configuration de l'authentification OSPF.

4.9.7 Vérification des informations de routage

La commande *« show ip route »* affiche la table de routage actuellement utilisée par l'IOS pour choisir le meilleur chemin vers les réseaux de destination, comme présenté avec les deux protocoles cités précédemment.

```
Bejaia2#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is 192.168.2.3 to network 0.0.0.0

     172.16.0.0/24 is subnetted, 4 subnets
O       172.16.0.0 [110/74] via 192.168.201.2, 00:01:21, Serial1/1
O       172.16.1.0 [110/74] via 192.168.202.2, 00:01:21, Serial1/2
O       172.16.2.0 [110/74] via 192.168.203.2, 00:01:21, Serial1/3
O       172.16.3.0 [110/74] via 192.168.204.2, 00:01:21, Serial1/0
     192.168.201.0/30 is subnetted, 1 subnets
C       192.168.201.0 is directly connected, Serial1/1
     192.168.202.0/30 is subnetted, 1 subnets
C       192.168.202.0 is directly connected, Serial1/2
     10.0.0.0/24 is subnetted, 3 subnets
O       10.20.10.0 [110/75] via 192.168.2.1, 00:01:27, FastEthernet0/0
O       10.30.9.0 [110/2] via 192.168.2.254, 00:01:27, FastEthernet0/0
O       10.40.1.0 [110/139] via 192.168.2.1, 00:01:27, FastEthernet0/0
     192.168.203.0/30 is subnetted, 1 subnets
C       192.168.203.0 is directly connected, Serial1/3
     192.168.204.0/30 is subnetted, 1 subnets
C       192.168.204.0 is directly connected, Serial1/0
     192.168.254.0/30 is subnetted, 2 subnets
O       192.168.254.4 [110/129] via 192.168.2.1, 00:01:29, FastEthernet0/0
O       192.168.254.0 [110/65] via 192.168.2.1, 00:01:29, FastEthernet0/0
C    192.168.2.0/24 is directly connected, FastEthernet0/0
O*E2 0.0.0.0/0 [110/1] via 192.168.2.3, 00:01:29, FastEthernet0/0
```

Figure 4.34 : Affichage des informations de routage.

4.9.8 Vérification de la configuration courante

La commande *« show running-config »* permet de vérifier les informations de routage configurées avec le protocole de routage OSPF.

```
Bouira#show run
Building configuration...

Current configuration : 1490 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Bouira
!
interface FastEthernet0/0
 ip address 10.40.1.1 255.255.255.0
 duplex auto
 speed auto
!
interface FastEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface Serial1/0
 ip address 192.168.254.5 255.255.255.252
 ip ospf authentication message-digest
 ip ospf message-digest-key 2 md5 cisco1
 serial restart-delay 0
 no dce-terminal-timing-enable
!
router ospf 10
 router-id 192.168.254.8
 log-adjacency-changes
 area 0 authentication message-digest
 passive-interface FastEthernet0/0
 network 10.40.1.0 0.0.0.255 area 0
 network 192.168.254.4 0.0.0.3 area 0
!
!
```

Figure 4.35 : Vérification de la configuration.

Nous avons configuré le protocole OSPF précédemment avec une seule zone, dans ce qui suit nous allons illustrer les commandes utilisées pour la configuration d'inter-area OSPF (plusieurs zones).

Notre topologie sera composée de quatre zones différentes qui s'attachent à la zone principale *zone 0*, les commandes d'activation du protocole OSPF c'est les mêmes, avec l'ajout des deux nouveaux principes : le premier est celui du *« stub »* et *« Totally stubbed »* et le deuxième est *« Virtual Link »* qui seront expliqués dans ce qui suit.

4.9.9 Configuration du protocole OSPF avec plusieurs zones

Notre topologie est divisée en zones : zone 0, zone 1, zone 2, zone 3 et zone 4. La figure 4.36 montre la configuration du routeur Alger avec deux zones, à savoir les zones 1 et 2 :

```
Alger#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Alger(config)#router ospf 10
Alger(config-router)#router-id 192.168.254.7
Alger(config-router)#network 192.168.254.0 0.0.0.3 area 1
Alger(config-router)#network 192.168.254.4 0.0.0.3 area 2
Alger(config-router)#network 10.20.10.0 0.0.0.255 area 1
Alger(config-router)#end
```

Figure 4.36 : Configuration d'inter-area avec le routeur Alger.

4.9.10 Configuration d'une zone stub

Le moyen qui permet de réduire les échanges est la mise en place de stub Area. En configurant une zone en stub avec la commande area *« num-area stub »*, cela force le routeur ABR (dans notre cas c'est le routeur Bouira) à éliminer toutes les routes externes (LSA type 5) et de les remplacer par une route par défaut.

Cette configuration est utilisée avec la plupart des sous zones de notre topologie, comme illustré dans la figure 4.37 avec le routeur « Bouira ».

```
Bouira#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Bouira(config)#router ospf 10
Bouira(config-router)#area 2 stub
Bouira(config-router)#end
```

Figure 4.37 : Configuration d'une zone stub.

La table de routage montre la nouvelle route qui remplace les LSA type 5 venant de l'extérieur :

```
Bouira#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is 192.168.254.6 to network 0.0.0.0

     10.0.0.0/24 is subnetted, 3 subnets
O IA    10.20.10.0 [110/74] via 192.168.254.6, 00:05:16, Serial1/0
O IA    10.30.9.0 [110/130] via 192.168.254.6, 00:00:40, Serial1/0
C       10.40.1.0 is directly connected, FastEthernet0/0
     192.168.254.0/30 is subnetted, 2 subnets
C       192.168.254.4 is directly connected, Serial1/0
O IA    192.168.254.0 [110/128] via 192.168.254.6, 00:05:16, Serial1/0
O IA 192.168.2.0/24 [110/129] via 192.168.254.6, 00:00:46, Serial1/0
O*E2 0.0.0.0/0 [110/1] via 192.168.254.6, 00:00:32, Serial1/0
O*IA 0.0.0.0/0 [110/65] via 192.168.254.6, 00:03:17, Serial1/0
```

Figure 4.38 : Consultation de la table de routage.

Pour limiter encore plus le trafic, une zone est configurée en *« Totally stubbed »* grâce à l'ajout de la commande *« no-summary »* sur le routeur Bouira. Dans ce cas, tout le trafic inter-zones et externe est éliminé et remplacé par une route par défaut, qui sera configurée automatiquement.

Voila la nouvelle table de routage qui contient seulement les routes directement connecté à notre routeur, avec la nouvelle route par défaut :

```
Bouira#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is 192.168.254.6 to network 0.0.0.0

     10.0.0.0/24 is subnetted, 1 subnets
C       10.40.1.0 is directly connected, FastEthernet0/0
     192.168.254.0/30 is subnetted, 1 subnets
C       192.168.254.4 is directly connected, Serial1/0
O*IA 0.0.0.0/0 [110/65] via 192.168.254.6, 00:08:25, Serial1/0
```

Figure 4.39 : Consultation de la nouvelle table de routage.

4.9.11 Virtual Link

Le protocole OSPF impose que toutes les zones soient connectées à la zone 0. Cependant, dans la pratique ce cas n'est pas toujours possible. Il faut donc créer un lien virtuel qui traverse une aire afin de simuler notre aire (ici aire 2) soit directement connecté.

OSPF dispose d'une fonction dédiée à cela, par conséquent, il est possible d'utiliser un tunnel entre deux routeurs.

Les deux figures suivantes montrent la commande qui permet de créer un *« virtual-link »*, dans la configuration d'OSPF, sur les routeurs *« Bejaia »* et *« Alger »* de l'aire qui est traversée par ce lien virtuel (l'aire 1), dont le but est de résoudre le problème de transmission/réception de routes par le routeur Bouira.

```
Bejaia#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Bejaia(config)#router ospf 10
Bejaia(config-router)#area 1 virtual-link 192.168.254.7
Bejaia(config-router)#end
Bejaia#wri
*Mar  1 00:41:02.919: %SYS-5-CONFIG_I: Configured from console by console
Bejaia#write
Building configuration...
[OK]
```

```
Alger#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Alger(config)#router ospf 10
Alger(config-router)#area 1 virtual-link 192.168.2.4
Alger(config-router)#end
Alger#w
*Mar  1 00:42:35.411: %SYS-5-CONFIG_I: Configured from console by console
Alger#write
Building configuration...
[OK]
```

Figure 4.40: Configuration d'un virtual-link.

La vérification de l'activation du lien virtuel précédemment créé, est illustrée dans la figure 4.41 :

```
Bejaia#show ip ospf virtual-link
Virtual Link OSPF_VL0 to router 192.168.254.7 is up
  Run as demand circuit
  DoNotAge LSA allowed.
  Transit area 1, via interface Serial1/0, Cost of using 64
  Transmit Delay is 1 sec, State POINT_TO_POINT,
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:04
    Adjacency State FULL (Hello suppressed)
```

Figure 4.41 : Vérification du lien virtuel.

4.10 Choix d'un protocole de routage dynamique

Le protocole de routage dans un réseau doit assurer l'acheminement des paquets et le maintien de la connexion entre les nœuds communicants. Il doit prendre en considération les changements de la topologie du réseau, ainsi que d'autres caractéristiques comme la bande passante, le nombre de liens, etc.

Afin de choisir le protocole le mieux approprié au réseau de l'entreprise, cas de Cevital, parmi les trois protocoles exposés, nous avons fait une comparaison entre ces protocoles en se basant sur les critères suivants: *le nombre de sauts, le temps de convergence, la métrique* , *la distance administrative* et *le concept de zones*.

1. Nombre de sauts : Les deux protocoles de routage dynamique OSPF et EIGRP n'ont pas le problème de limitation de sauts. La topologie utilisée n'est pas assez importante concernant le nombre de sauts (inférieur à 15) donc nous pouvons configurer celle-ci avec RIPv2. L'utilisation des deux autres protocoles pour configurer cette topologie est nécessaire, pour éviter toutes difficultés si des modifications sont apportées à celle-ci, car le réseau de l'entreprise est évolutif.

2. Temps de convergence : OSPF et EIGRP converge plus rapidement que RIPv2, car le premier envoie des LSA et utilise l'algorithme SPF pour trouver la meilleur route et s'adapte rapidement aux changements de la topologie, par contre le deuxième applique un nouvel algorithme nommé DUAL lui permettant une convergence rapide si un successeur potentiel existe. Dans le cas de perte d'une route et si le successeur potentiel n'existe pas, EIGRP envoie des requêtes à tout les routeurs voisins jusqu'à ce que la route soit trouvée et si nous avons un grand réseau, EIGRP met du temps pour envoyer un message d'un routeur à un autre d'où la convergence de celui-ci devient lente contrairement à OSPF.

Pour voir la convergence des trois protocoles de routage dynamique, nous avons choisi de désactiver un routeur, en commençant par le protocole OSPF, suivi du protocole EIGRP et enfin RIPv2. Ensuite accéder aux tables de routage de ces voisins pour voir les changements apportés.

```
     172.16.0.0/24 is subnetted, 4 subnets
O       172.16.0.0 [110/74] via 192.168.201.2, 00:01:59, Serial1/1
O       172.16.1.0 [110/74] via 192.168.202.2, 00:01:59, Serial1/2
O       172.16.2.0 [110/74] via 192.168.203.2, 00:01:59, Serial1/3
O       172.16.3.0 [110/74] via 192.168.204.2, 00:01:59, Serial1/0
     192.168.201.0/30 is subnetted, 1 subnets
C       192.168.201.0 is directly connected, Serial1/1
     192.168.202.0/30 is subnetted, 1 subnets
C       192.168.202.0 is directly connected, Serial1/2
     192.168.203.0/30 is subnetted, 1 subnets
C       192.168.203.0 is directly connected, Serial1/3
     192.168.204.0/30 is subnetted, 1 subnets
C       192.168.204.0 is directly connected, Serial1/0
C    192.168.2.0/24 is directly connected, FastEthernet0/0
```

Figure 4.42 : Table de routage OSPF avant de désactiver le routeur « Oran».

```
Gateway of last resort is not set

     172.16.0.0/24 is subnetted, 3 subnets
O       172.16.1.0 [110/74] via 192.168.202.2, 00:00:18, Serial1/2
O       172.16.2.0 [110/74] via 192.168.203.2, 00:00:18, Serial1/3
O       172.16.3.0 [110/74] via 192.168.204.2, 00:00:18, Serial1/0
     192.168.202.0/30 is subnetted, 1 subnets
C       192.168.202.0 is directly connected, Serial1/2
     192.168.203.0/30 is subnetted, 1 subnets
C       192.168.203.0 is directly connected, Serial1/3
     192.168.204.0/30 is subnetted, 1 subnets
C       192.168.204.0 is directly connected, Serial1/0
C    192.168.2.0/24 is directly connected, FastEthernet0/0
```

Figure 4.43 : Table de routage OSPF après la désactivation du routeur « Oran».

Nous avons remarqué que le réseau 171.16.0.0/24 et 192.168.201.0/30 n'existent plus dans la table de routage, donc la ligne du protocole est en mode désactivé ainsi que celle de l'interface (DOWN).

```
     172.16.0.0/24 is subnetted, 4 subnets
D       172.16.0.0 [90/2195456] via 192.168.201.2, 00:00:13, Serial1/1
D       172.16.1.0 [90/2195456] via 192.168.202.2, 00:03:18, Serial1/2
D       172.16.2.0 [90/2195456] via 192.168.203.2, 00:03:07, Serial1/3
D       172.16.3.0 [90/2195456] via 192.168.204.2, 00:03:09, Serial1/0
     192.168.201.0/30 is subnetted, 1 subnets
C       192.168.201.0 is directly connected, Serial1/1
     192.168.202.0/30 is subnetted, 1 subnets
C       192.168.202.0 is directly connected, Serial1/2
     192.168.203.0/30 is subnetted, 1 subnets
C       192.168.203.0 is directly connected, Serial1/3
```

Figure 4.44 : Table de routage EIGRP avant de désactiver le routeur « Oran ».

```
     172.16.0.0/24 is subnetted, 3 subnets
D       172.16.1.0 [90/2195456] via 192.168.202.2, 00:01:24, Serial1/2
D       172.16.2.0 [90/2195456] via 192.168.203.2, 00:01:13, Serial1/3
D       172.16.3.0 [90/2195456] via 192.168.204.2, 00:01:15, Serial1/0
     192.168.202.0/30 is subnetted, 1 subnets
C       192.168.202.0 is directly connected, Serial1/2
     192.168.203.0/30 is subnetted, 1 subnets
C       192.168.203.0 is directly connected, Serial1/3
     192.168.204.0/30 is subnetted, 1 subnets
C       192.168.204.0 is directly connected, Serial1/0
C    192.168.2.0/24 is directly connected, FastEthernet0/0
```

Figure 4.45 : Table de routage EIGRP après la désactivation du routeur « Oran ».

Nous avons remarqué que le réseau 171.16.0.0/24 et 192.168.201.0/30 n'existent plus dans la table de routage, donc la ligne du protocole est en mode désactivé ainsi que celle de l'interface (DOWN).

```
     172.16.0.0/24 is subnetted, 4 subnets
R       172.16.0.0 [120/1] via 192.168.201.2, 00:00:15, Serial1/1
R       172.16.1.0 [120/1] via 192.168.202.2, 00:00:06, Serial1/2
R       172.16.2.0 [120/1] via 192.168.203.2, 00:00:22, Serial1/3
R       172.16.3.0 [120/1] via 192.168.204.2, 00:00:20, Serial1/0
     192.168.201.0/30 is subnetted, 1 subnets
C       192.168.201.0 is directly connected, Serial1/1
     192.168.202.0/30 is subnetted, 1 subnets
C       192.168.202.0 is directly connected, Serial1/2
     192.168.203.0/30 is subnetted, 1 subnets
C       192.168.203.0 is directly connected, Serial1/3
     192.168.204.0/30 is subnetted, 1 subnets
C       192.168.204.0 is directly connected, Serial1/0
C    192.168.2.0/24 is directly connected, FastEthernet0/0
```

Figure 4.46 : Table de routage RIPv2 avant de désactiver le routeur « Oran ».

```
     172.16.0.0/24 is subnetted, 3 subnets
R       172.16.1.0 [120/1] via 192.168.202.2, 00:00:19, Serial1/2
R       172.16.2.0 [120/1] via 192.168.203.2, 00:00:13, Serial1/3
R       172.16.3.0 [120/1] via 192.168.204.2, 00:00:22, Serial1/0
     192.168.202.0/30 is subnetted, 1 subnets
C       192.168.202.0 is directly connected, Serial1/2
     192.168.203.0/30 is subnetted, 1 subnets
C       192.168.203.0 is directly connected, Serial1/3
     192.168.204.0/30 is subnetted, 1 subnets
C       192.168.204.0 is directly connected, Serial1/0
C    192.168.2.0/24 is directly connected, FastEthernet0/0
```

Figure 4.47 : Table de routage RIPv2 après la désactivation du routeur « Oran ».

Après avoir désactivé le routeur Oran, nous avons remarqué que le réseau 171.16.0.0/24 et 192.168.201.0/30 n'existent plus dans la table de routage, donc la ligne du protocole est en mode désactivé ainsi que celle de l'interface (DOWN).

Nous avons remarqué que les deux protocoles de routage dynamique OSPF et EIGRP s'adaptent rapidement aux changements de la topologie, contrairement à RIPv2 car :

Le temps de convergence du protocole OSPF est de 00.02.29 et celui du protocole EIGRP est de 00.04.33, par contre le protocole RIPv2 a convergé en 00.10.30 :

```
*Mar  1 00:02:29.179: %LINEPROTO-5-UPDOWN: Line protocol
*Mar  1 00:02:29.195: %OSPF-5-ADJCHG: Process 10, Nbr 192
own: Interface down or detached
C    192.168.2.0/24 is directly connected, FastEthernet0/
```

```
Bejaia2#
*Mar  1 00:04:33.487: %DUAL-5-NBRCHANGE: IP-EIGRP(0) 40:
Neighbor 192.168.203.2 (Serial1/3) is down: holding time expired
```

```
Bejaia2#
*Mar  1 00:10:30.383: %LINEPROTO-5-UPDOWN: Line protocol
on Interface Serial1/1, changed state to down
```

3. La métrique : Chacun des trois protocoles possède sa propre métrique : RIPv2 emploie le nombre de sauts traversés (routeurs) qu'il utilise comme mesure. En effet, il se limite aux réseaux simples moins de 15 sauts.

Le protocole EIGRP utilise une combinaison de plusieurs métriques pour calculer sa propre mesure, grâce à la formule montrée dans le chapitre 3, mais par défaut il emploi la

bande passante qui est nécessaire pour le bon fonctionnement du protocole EIGRP ainsi que le délai.

Par contre le protocole OSPF emploie le coût comme métrique en se basant sur la bande passante, lui aussi utilise une formule pour calculer sa propre métrique , qui est illustrée dans le chapitre 3 et elle pourra être modifiée manuellement. Plus la valeur est petite, plus la route est préférable.

La commande *« bandwidth »* permet de modifier la valeur de la bande passante employée par l'IOS dans le calcul du coût OSPF. La syntaxe de la commande d'interface est la même que celle du protocole EIGRP :
« Router (config-if)# bandwidth bandwidth-kbps», avec *« bandwidth-kbps»* la nouvelle valeur de la bande passante.

4. Distance administrative : Un réseau utilisant le protocole EIGRP avec une distance administrative de 90 est mieux qu'un réseau configuré avec OSPF ou RIPv2, avec une distance administrative de 110 et 120 respectivement, car avec une petite valeur de la distance administrative, la fiabilité du réseau est assurée.

5. Concept de zones : OSPF nécessite que la topologie du réseau soit hiérarchique, ce qui n'est pas le cas chez les deux autres protocoles. Lors de la configuration du protocole OSPF sur un grand réseau, la hiérarchie est effectuée en divisant le réseau en zones (chose qui a été présentée dans la section 4.9.9).
L'avantage de cette méthode est d'éviter la propagation de mises à jour vers toutes les zones, car la zone principale qui possède les informations de tout le réseau s'occupe de cette tâche, afin d'empêcher la surcharge du réseau.

Remarque

La commande *« Ping »* permet de vérifier si l'adresse de destination est accessible en affichant le temps de réponse de la commande. C'est la première commande à utiliser en cas de dépannage pour vérifier la connectivité, par contre la commande *« traceroute »* est un outil de diagnostic des réseaux, permettant de déterminer le chemin suivi par un paquet.

Cette commande permet ainsi de suivre le chemin qu'un paquet de données (paquet IP) va prendre pour aller d'une machine source à une destination. Elle fournit une sortie

décrivant les noms et adresses IP des routeurs successifs, précédés d'un numéro d'ordre et du temps de réponse minimum, moyen et maximum.

Nous avons testé la connectivité entre le sous-réseau contenant l'adresse IP 172.16.0.0/24 passant par le routeur *« Oran »* et le sous-réseau avec l'adresse 10.40.1.1/24 passant par le routeur *« Bouira»* et ce avec les trois protocoles configurés ci-dessus, grâce à la commande taceroute.

```
Bouira#traceroute 172.16.0.1

Type escape sequence to abort.
Tracing the route to 172.16.0.1

  1 192.168.254.6 40 msec 56 msec 52 msec
  2 192.168.254.2 76 msec 100 msec 48 msec
  3 192.168.2.2 104 msec 48 msec 48 msec
  4 192.168.201.2 140 msec *  160 msec
```

Figure 4.48 : Test de connectivité avec le protocole RIPv2.

```
Bouira#traceroute 172.16.0.1

Type escape sequence to abort.
Tracing the route to 172.16.0.1

  1 192.168.254.6 20 msec 164 msec 92 msec
  2 192.168.254.2 120 msec 84 msec 56 msec
  3 192.168.2.2 364 msec 108 msec 156 msec
  4 192.168.201.2 204 msec *  128 msec
```

Figure 4.49 : Test de connectivité avec le protocole EIGRP.

```
Bouira#traceroute 172.16.0.1

Type escape sequence to abort.
Tracing the route to 172.16.0.1

  1 192.168.254.6 36 msec 88 msec 72 msec
  2 192.168.254.2 96 msec 60 msec 80 msec
  3 192.168.2.2 228 msec 136 msec 124 msec
  4 192.168.201.2 232 msec *  176 msec
```

Figure 4.50 : Test de connectivité avec le protocole OSPF.

4.10.1 Récapitulatif

Le choix d'un protocole de routage pour une entreprise est délicat car : qu'elles que soit les qualités des protocoles propriétaires (EIGRP), ils sont et demeurent propriétaires ce

qui constitue un inconvénient lors de l'évolution du réseau, ou du renouvellement des équipements.

OSPF est un protocole de routage complexe dans sa mise en œuvre (plan d'adressage, initialisation des métriques, etc.), complexe dans son fonctionnement, bien qu'il remédie aux principaux inconvénients de RIPv2 (temps de convergence et boucle).

Le protocole que nous avons choisi pour qu'il soit implémenté plus tard dans le réseau de Cevital est *« OSPF »*, malgré sa complexité, il a l'avantage d'avoir une convergence rapide, pas de limitation de sauts, à noter qu'il est un protocole standard applicable sur toutes les plateformes et tout type d'équipements d'interconnexions.

4.11 Conclusion

Au cour de ce chapitre nous avons présenté des aspects pratiques liés à la configuration des protocoles RIPv2, OSPF et EIGRP, à savoir l'outil de simulation nécessaire GNS3, nous avons illustré aussi quelques interfaces pour bien comprendre les commandes utilisées afin de configurer nos protocoles.

D'après la comparaison effectué dans ce chapitre entre les trois protocoles dans un réseau d'entreprise, en se basant sur les cinq critères étudiés, nous pouvons dire que le protocole de routage dynamique OSPF est le plus utilisé par les grandes entreprises car c'est un protocole standard et il est basé sur des normes ouvertes.

Conclusion générale

Afin de réaliser ce travail, nous avons mis au point une étude comparative des protocoles de routage dynamique IGP, dans un réseau d'entreprise, cas de Cevital, dont le but est de choisir le protocole de routage le mieux approprié à celle-ci.

Notre motivation était le problème du routage statique et la configuration du protocole de routage dynamique EIGRP, ainsi que les problèmes posés par les éléments d'interconnexion VSAT. Pour résoudre ces problèmes, l'objectif était la proposition de la configuration des deux autres protocoles : RIPv2 et OSPF, en plus d'EIGRP, afin de permettre un routage fiable entre les différents sites de la topologie de l'organisme d'accueil.

Vu les problèmes causés par les configurations traditionnelles et celles causés par les VSAT, nous avons proposés d'une part de remplacer ces derniers par d'autres éléments, comme : les routeurs Cisco, d'autre part la configuration des deux protocoles cités.

Notre travail a commencé en premier lieu par une étude axée sur les généralités des réseaux informatiques, le routage ainsi que les protocoles de routage, qui nous ont permis d'approfondir nos connaissances et d'en savoir plus sur ces concepts. Ensuite nous avons entamé le second chapitre qui est consacré à la présentation de l'entreprise où se déroule notre stage.

En ce qui concerne le troisième chapitre, nous avons choisi les trois protocoles IGP, à savoir : RIPv2, OSPF et EIGRP, pour faire notre comparaison, qui sont désormais une référence dans le domaine des réseaux.

Concernant le quatrième chapitre, notre choix s'est focalisé sur l'émulateur GNS3, afin de configurer les trois protocoles de routage dynamique dans le réseau d'organisme d'accueil.

Grâce à GNS3, les utilisateurs peuvent tester et évaluer, dans des conditions quasi réelles et sans avoir à financer le matériel, leurs configurations avant de les mettre en place physiquement. Nous avons également choisi le protocole le plus adapté pour qu'il soit configuré dans la topologie réseau de Cevital dans le futur.

Ce projet nous a été très bénéfique, car nous avons enrichi nos connaissances sur les deux plans : théorique et pratique, concernant le routage et les protocoles de routage. Il nous a aussi permis de découvrir et d'acquérir de nouvelles informations en matière de configuration dans le domaine des réseaux informatiques.

Références bibliographiques

Bibliographie

[1] Guy Pujolle, Les réseaux, EYROLLES, 6eme édition, 2008.

[2] Jean-François PILLOU, Fabric LEMAINQUE, Tout sur les réseaux et Internet, DUNOD, 3ème édition, Paris 2012.

[3] Andrew Tanenbaum, Réseaux, DUNOD, 3ème édition, 1999.

[4] André VAUCAMPS, Protocoles et concepts de routage - Configuration avancée des routeurs, ENI éditions.

[5] Bertrand Petit, Architecture des réseaux, ellipses, 2ème édition, 2006.

[6] Stéphanie Lohier, Aurélie Quideller, Le réseau Internet, DUNOD, 3ème édition, 2010.

[7] Danièle DROMARD, Dominique SERET, Architecture des réseaux, Collection Synthex, Paris 2009.

[8] Claude SERVIN, Réseaux & Télécoms, DUNOD, 2ème édition, Paris 2006.

[9] Jean Robert HOUNTOMEY, Le Routage Statique, AFNOG 2006 -NAIROBI- KENYA.

[10] Pacôme Massol, Initiation au routage, 2ème partie.

[11] John T. Moy, Ospf : Anatomy Of An Internet Routing Protocol, Addison Wesley Pub Co Inc, février 1998.

[12] Brochure d'accueil Cevital, Cevital, Mai 2013.

[13] Etude du protocole OSPF, P.Sicard, Université de JOSEPHE FOURIER (IMA).

[14] Nguyen Van Nam, Amélioration et implémentation d'un algorithme d'évitement des boucles transitoires durant la convergence d'OSPF, Louvain-La-Neuve, 2008-2009.

[15] BOUTAHIR Mounir, CCNA, Switching Basics et Intermediate Routing, Ista Hay Hassani.

[16] Jason Sinclair, Enhanced Interior Gatway Protocol (EIGRP), Certification Zone, 31/05/2005.

[17] Scott Hogg, EIGRP and OSPF Comparison, Project 2, March 14, 2002.

[18] Jean SAQUET, Pierre BLONDEAU, Routage interne : OSPF, M2 ESECURE Réseaux, 21/01/2013.

[19] Ravi Malhotra, IP Routing, O'Reilly & Associates, First Edition, January 2002.

[20] Gerard Maral, VSAT NETWORKS, John Wiley & Sons, Ltd, Second Edition, 2003.

Webographie

[21] Les topologies en bus, anneau, étoile, http://mrproof.blogspot.com/2010/09/cours-les-topologies-en-bus-anneau.html, date de consultation Mars 2013.

[22] GENERALITES, http://www.lri.fr/~barbet/2.htm, date de consultation Mars 2013.

[23] L'optimisation du WAN, http://www.kaistos.eu/kaistosV2/wp-content/pdf/le_wan.pdf, date de consultation Mars 2013.

[24] Protocoles, http://www.commentcamarche.net/contents/internet/protocol.php3, date de consultation Mars 2013.

[25] Protocoles de routage, http://mrim.forumpro.fr/t833-protocoles-de-routage, date de consultation Mars 2013.

[26] Algorithmes de routage, http://malm.tuxfamily.org/doc/qr_chap1_algo.htm, date de consultation Mai 2013.

[27] Routage, http://cttcb.fr/cardoni_ancien_site/discovery2/module6/m6.pdf, date de consultation Mai 2013.

[28] Routeur et Modem, http://ilyse.e-monsite.com/pages/routeur-et-modem/, date de consultation Mai 2013.

[29] Protocoles IGP et EGP, http://mrim.forumpro.fr/t831-protocoles-igp-et-egp, date de consultation Mai 2013.

[30] Les topologies des réseaux, http://www.samomoi.com/reseauxinformatiques/les_topologies_des_reseaux.php, date de consultation Mai 2013.

[31] Topologie des réseaux, http://www.commentcamarche.net/contents/initiation/topologi.php3, date de consultation Mai 2013.

[32] CCNA2 Routage dynamique - généralités et RIPv1, http://quizlet.com/12821967/ccna2-routage-dynamique-generalites-et-ripv1-flash-cards/, date de consultation Mai 2013.

[33] Synthèse sur le routage, http://fr.scribd.com/doc/26417972/Synthese-Sur-Le-Routage-14, date de consultation Mai 2013.

[34] Chapitre 1, Algorithmes de routage, http://malm.tuxfamily.org/doc/qr_chap1_algo.htm, date de consultation Mai 2013.

[35] Protocole de routage OSPF, http://fr.scribd.com/doc/8130669/Protocole-de-Routage-OSPF, date de consultation Mai de consultation Mai 2013.

[36] RIP, http://dictionnaire.phpmyvisites.net/definition-rip-4992.htm, date de consultation 2013.

[37] Protocoles de routage 2, http://mrim.forumpro.fr/t833-protocoles-de-routage, date de consultation Mai 2013.

[38] A la découverte du protocole de routage OSPF, http://www.unixgarden.com/index.php/gnu-linux-magazine/1068, date de consultation 2013.

[39] EIGRP, http://www.reseaumaroc.com/files/EIGRP%2023.pdf, date de consultation Mai 2013.

[40] avantages et inconvénients des protocoles à état de liens, http://fr.scribd.com/doc/51466828/16/Avantages-et-inconvenients-du-protocole-a-etat-de-liens, date de consultation Mai 2013.

[41] OSPF 1. Introduction, http://cisco.goffinet.org/s3/ospf1-introduction, date de consultation 2013.

[42] Comparaison entre le protocole EIGRP et IGRP, http://fr.scribd.com/doc/51466828/32/Comparaison-entre-les-protocoles-EIGRP-et-IGRP.

[43] Synthèse sur le routage, http://cisco.goffinet.org/s2/synthese_routage, date de consultation Mai 2013.

[44] Formation CCNA, Chapitre 3.

[45] Design d'une solution à haute disponibilité, lan, wan, téléphonie, sécurité, http://www.memoireonline.com/06/11/4571/Design-dune-solution--haute-disponibilite-lan-wan-telephonie-securite.html, date de consultation Mai 2013.

[46] Notice d'information, http://www.cosob.org/les-emetteurs-notice-cevital.pdf, date de consultation Mai 2013.

[47] Formation CCNA, Chapitre 5.

[48] CCDA Self-Study: RIP, IGRP, and EIGRP Characteristics and Design, http://www.ciscopress.com/articles/article.asp?p=102174&seqNum=4, date de consultation Mai 2013.

[49] RIP Version 2, http://www.ietf.org/rfc/rfc1723, date de consultation Mai 2013.

[50] Formation CCNA, chapitre 4.

[51] Formation CCNA, chapitre 11.

[52] Protocole de routage OSPF, http://fr.scribd.com/doc/8130669/Protocole-de-Routage-OSPF, date de consultation Mai 2013.

[53] Formation CCNA, chapitre 11.

[54] Formation CCNA, chapitre 9.

[55] Protocole EIGRP, http://baribaud.homelinux.net/HEG/archi/reseau/sem2/chap9a5.pdf, date de consultation Mai 2013.

[56] Plus courts chemins, https://www.enseignement.polytechnique.fr/informatique/INF421/TD/TD8/INF421-TD8-1.php, date de consultation Mai 2013.

[57] Liaison point à point, http://www.techno-science.net/?onglet=glossaire&definition=3772, consultation Mai 2013.

[58] Simulations, GNS3, https://sites.google.com/a/iepscf-uccle.eu/projets-infotech/travaux-anterieurs/archives-actualisation/simulations-gns3, date de consultation Mai 2013.

[59] Dynamips - Un émulateur de routeur Cisco sur PC, http://2007.jres.org/planning/pdf/141.pdf, date de consultation Mai 2013.

[60] QEMU, http://fr.wikipedia.org/wiki/QEMU, date de consultation Mai 2013.

[61] Projet, http://eip.epitech.eu/2013/gns3/fr/project.html, date de consultation Mai 2013.

[62] La simulation sous GNS3, https://sites.google.com/a/iepscf-uccle.eu/projets-infotech/travaux-anterieurs/archives-actualisation/simulations-gns3, date de consultation Mai 2013.

[63] Modules Cisco EtherSwitch pour les routeurs des gammes Cisco 2600, 3600 et 3700, http://www.cisco.com/web/FR/documents/pdfs/datasheet/routers/2600x_ds_fr.pdf, date de consultation Mai 2013.

[64] Commutateur réseau, http://www.techno-science.net/?onglet=glossaire&definition=11362, date de consultation Mai 2013.

[65] Firewall, http://www.futura-sciences.com/fr/definition/t/internet-2/d/firewall_474/, date de consultation Mai 2013.

[66] DMZ (demilitarized zone), http://searchsecurity.techtarget.com/definition/DMZ, date de consultation Mai 2013.

[67] A propos de SLC, http://www.slc.dz/, date de consultation Mai 2013.

[68] Le Concept du Routage, http://aboubakr-rf.blogspot.com/p/carriere.html, date de consultation Mai 2013.

[69] RÉSEAUX INFORMATIQUES, http://www.universalis.fr/encyclopedie/reseaux-informatiques/2-principes-generaux-des-reseaux-informatiques/, date de consultation Mai 2013.

[70] Réseau informatique, http://www.techno-science.net/?onglet=glossaire&definition=3799, Mai 2013.

ANNEXE A

Configuration de base

A.1 Configuration de base d'un routeur

La configuration de base des routeurs de notre topologie a été faite à l'aide des commandes illustrées et expliquées dans le tableau qui suit :

<table>
<tr><th colspan="3">Configuration du nom d'un routeur</th></tr>
<tr><th colspan="2">Commande</th><th>Explication</th></tr>
<tr><td colspan="2">Router ></td><td>Permet l'accès au mode EXEC utilisateur.</td></tr>
<tr><td colspan="2">Router >enable</td><td>Permet de passer en mode d'exécution privilégié.</td></tr>
<tr><td colspan="2">Router #config t</td><td>C'est le passage en mode de configuration globale.</td></tr>
<tr><td colspan="2">Router (config)# hostname R1</td><td>Configuration du nom d'un routeur en tant que R1.</td></tr>
<tr><td colspan="2">R1 (config) # exit</td><td>Ou « ctrl+Z », c'est le retour au mode EXEC privilégié.</td></tr>
<tr><th colspan="3">Configuration d'adresses IP</th></tr>
<tr><th colspan="2">Commandes</th><th>Explication</th></tr>
<tr><td rowspan="5">Configuration des interfaces FastEthernet et des interfaces Serial</td><td>R1 # conf t</td><td>Pour passer en mode de configuration globale.</td></tr>
<tr><td>R1 (config)#interface FastEthernet0/0 ou interface Serial1/0</td><td>Accès à la configuration de l'interface FastEthernet 0/0 ou Serial 1/0.</td></tr>
<tr><td>R1 (config-if)# ip address ip_address mask</td><td>Adresse IP et masque de sous-réseau de l'interface.</td></tr>
<tr><td>R1 (config-if)# no shutdown</td><td>Activation de l'interface.</td></tr>
<tr><td>R1 (config-if)#exit</td><td>Ou «ctrl+Z ».</td></tr>
</table>

Tableau A.1 : Commandes de configuration d'un routeur.

Les figures ci-après montrent l'utilisation de ces commandes avec les différents routeurs de notre topologie, à savoir : le routeur Bejaia, Alger, Bouira, Bejaia2, Constantine, LLK, Elkseur et Oran.

```
Router#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname Bejaia
Bejaia(config)#interface fa0/0
Bejaia(config-if)#ip address 192.168.2.1 255.255.255.0
Bejaia(config)#interface s1/0
Bejaia(config-if)#ip address 192.168.254.2 255.255.255.252
Bejaia(config-if)#end
Bejaia#w
*Mar  1 00:17:46.631: %SYS-5-CONFIG_I: Configured from console by console
Bejaia#write
Building configuration...
[OK]
```

Figure A.1 : Configuration du routeur « Bejaia ».

```
Router#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname Alger
Alger(config)#interface s1/0
Alger(config-if)#ip address 192.168.254.1 255.255.255.252
Alger(config-if)#exit
Alger(config)#interface s1/1
Alger(config-if)#ip address 192.168.254.6 255.255.255.252
Alger(config-if)#exit
Alger(config)#interface f0/0
Alger(config-if)#ip address 10.20.10.1 255.255.255.0
Alger(config-if)#end
Alger#wri
*Mar  1 00:17:15.135: %SYS-5-CONFIG_I: Configured from console by console
Alger#write
Building configuration...
[OK]
```

Figure A.2 : Configuration du routeur « Alger ».

```
Router#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname Bouira
Bouira(config)#interface s1/0
Bouira(config-if)#ip address 192.168.254.5 255.255.255.252
Bouira(config-if)#exit
Bouira(config)#interface fa0/0
Bouira(config-if)#ip address 10.40.1.1 255.255.255.0
Bouira(config-if)#end
Bouira#w
*Mar  1 00:06:36.763: %SYS-5-CONFIG_I: Configured from console by console
Bouira#write
Building configuration...
[OK]
```

Figure A.3 : Configuration du routeur « Bouira ».

```
Router#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname Bejaia2
Bejaia2(config)#interface s1/0
Bejaia2(config-if)#ip address 192.168.204.1 255.255.255.252
Bejaia2(config-if)#exit
Bejaia2(config)#interface s1/1
Bejaia2(config-if)#ip address 192.168.201.1 255.255.255.252
Bejaia2(config-if)#exit
Bejaia2(config)#interface s1/2
Bejaia2(config-if)#ip address 192.168.202.1 255.255.255.252
Bejaia2(config-if)#exit
Bejaia2(config)#interface s1/3
Bejaia2(config-if)#ip address 192.168.203.1 255.255.255.252
Bejaia2(config-if)#exit
Bejaia2(config)#interface fa0/0
Bejaia2(config-if)#ip address 192.168.2.2 255.255.255.0
Bejaia2(config-if)#end
Bejaia2#w
*Mar  1 00:06:19.083: %SYS-5-CONFIG_I: Configured from console by console
Bejaia2#write
Building configuration...
[OK]
```

Figure A.4 : Configuration du routeur « Bejaia2 ».

```
Router#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname Constantine
Constantine(config)#interface s1/0
Constantine(config-if)#ip address 192.168.204.2 255.255.255.252
Constantine(config-if)#exit
Constantine(config)#interface fa0/0
Constantine(config-if)#ip address 172.16.3.1 255.255.255.0
Constantine(config-if)#end
Constantine#write
*Mar  1 00:02:34.055: %SYS-5-CONFIG_I: Configured from console by console
Constantine#write
Building configuration...
[OK]
```

Figure A.5 : Configuration du routeur « Constantine ».

```
Router#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname LLK
LLK(config)#interface s1/0
LLK(config-if)#ip address 192.168.203.2 255.255.255.252
LLK(config-if)#exit
LLK(config)#interface fa0/0
LLK(config-if)#ip address 172.16.2.1 255.255.255.0
LLK(config-if)#end
LLK#write
*Mar  1 00:02:33.931: %SYS-5-CONFIG_I: Configured from console by console
LLK#write
Building configuration...
[OK]
```

Figure A.6 : Configuration du routeur « LLK ».

```
Router#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname Elkseur
Elkseur(config)#interface s1/0
Elkseur(config-if)#ip address 192.168.202.2 255.255.255.252
Elkseur(config-if)#exit
Elkseur(config)#interface fa0/0
Elkseur(config-if)#ip address 172.16.1.1 255.255.255.0
Elkseur(config-if)#end
Elkseur#write
*Mar  1 00:08:04.075: %SYS-5-CONFIG_I: Configured from console by console
Elkseur#write
Building configuration...
[OK]
```

Figure A.7: Configuration du routeur « Elkseur ».

```
Router#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname Oran
Oran(config)#interface s1/0
Oran(config-if)#ip address 192.168.201.2 255.255.255.252
Oran(config-if)#exit
Oran(config)#interface fa0/0
Oran(config-if)#ip address 172.16.0.1 255.255.255.0
Oran(config-if)#end
Oran#write
*Mar  1 00:02:23.163: %SYS-5-CONFIG_I: Configured from console by console
Oran#write
Building configuration...
[OK]
```

Figure A.8 : Configuration du routeur « Oran ».

A.2 Configuration d'un Switch fédérateur

La configuration de ce type de Switch nécessite la configuration des VLANs et cela en suivant les étapes présentées ci-dessous :

A.2.1 Création des VALNs

Pour créer un VLAN, il faut se trouver dans le mode de configuration correspondant, accessible par la commande :

*Switch# **vlan database***

A partir de ce mode, la création d'un VLAN se fait par la commande :

*Switch (vlan)# **vlan {numéro} [name {nom}]***

La commande qui permet d'enregistrer la configuration des VLANs, qui se trouve dans le fichier vlan.dat dans la mémoire Flash est :

*Switch (vlan) # **Apply***
*Switch (vlan) # **exit***

Dans notre cas nous allons créer deux VLANs, à savoir, le VALN numéro 1 et le VLAN numéro 2 et pour chacun d'eux nous attribuerons des adresses IP avec les commandes suivantes :

*Switch # **config t***
*Switch (config) # **interface VLAN {numéro du VLAN} [name {nom}]***
*Switch (config-if) # **ip address ip_adresse mask***
*Switch (config-if) # **no shutdown***
*Switch (config-if) # **exit***

A.2.2 Attribution des ports de switch à un VLAN

Dans une configuration de VLAN statique, les ports du commutateur doivent être attribués à un VLAN, en suivant les étapes décrites ci-après :

Nous passerons dans le mode de configuration de l'interface spécifiée avec la commande :

*Switch (config) # **interface FastEthernet {numéro_interface}***

Spécification du mode de l'interface en utilisant la commande suivante :

*Switch (config-if) # **switchport mode access***

Attribution du vlan spécifié à l'interface avec la commande :

*Switch (config-if) # **switchport access vlan {numéro}***

Les figures ci-dessous montrent l'utilisation de ces commandes avec le EtherSwitch router nommé R9 :

```
R9#VLAN database
R9(vlan)#VLAN 1
VLAN 1 modified:
R9(vlan)#Apply
APPLY completed.
R9(vlan)#exit
APPLY completed.
Exiting....
R9#config t
Enter configuration commands, one per line.  End with CNTL/Z.
R9(config)#interface VLAN 1
R9(config-if)#ip address 10.30.9.254 255.255.255.0
R9(config-if)#no shutdown
R9(config-if)#exit
R9(config)#interface fa 1/0
R9(config-if)#switchport mode access
R9(config-if)#switchport  access VLAN 1
R9(config-if)#no shutdown
R9(config-if)#end
R9#w
*Mar  1 00:23:34.719: %SYS-5-CONFIG_I: Configured from console by console
R9#write
Building configuration...
[OK]
```

Figure A.9 : Configuration du VLAN 1.

```
R9#VLAN database
R9(vlan)#VLAN 2 name netbejaia
VLAN 2 modified:
    Name: netbejaia
R9(vlan)#Apply
APPLY completed.
R9(vlan)#exit
APPLY completed.
Exiting....
R9#config t
Enter configuration commands, one per line.  End with CNTL/Z.
R9(config)#interface VLAN 2
R9(config-if)#ip address 192.168.2.254 255.255.255.0
R9(config-if)#no shutdown
R9(config-if)#exit
R9(config)#interface fa1/1
R9(config-if)#switchport mode access
R9(config-if)#switchport  access VLAN 2
R9(config-if)#no shutdo
*Mar  1 00:09:28.655: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan2,
changed state to up
R9(config-if)#no shutdown
R9(config-if)#exit
R9(config)#interface fa1/2
R9(config-if)#switchport mode access
R9(config-if)#switchport  access VLAN 2
R9(config-if)#no shutdown
R9(config-if)#interface fa1/3
R9(config-if)#switchport mode access
R9(config-if)#switchport  access VLAN 2
R9(config-if)#no shutdown
R9(config-if)#end
R9#wri
*Mar  1 00:11:07.791: %SYS-5-CONFIG_I: Configured from console by console
R9#write
Building configuration...
[OK]
```

Figure A.10 : Configuration du VLAN 2.

ANNEXE B

Simulateur GNS 3

B.1 Présentation de GNS 3

Étape 1: Téléchargement de GNS3

Dans le navigateur web, nous avons utilisé le lien suivant pour télécharger GNS3 : « *http://www.gns3.net* ». La meilleure façon d'installer GNS3 dans un environnement Windows est d'utiliser le fichier : *GNS3 v 0.8.2 all-in-one.exe.*

Nous cliquons sur le bouton *« Enregistrer »*, puis nous allons choisir un emplacement sur le disque dur pour enregistrer le fichier.

Figure B.1 : Téléchargement de GNS3.

Étape 2: Installation de GNS3

Pour lancer l'installation de GNS3, nous devons trouver le fichier que nous avons téléchargé et nous cliquons dessus ; l'assistant de configuration GNS3 va commencer. Nous allons cliquer sur le bouton Suivant. Ensuite, nous cliquons sur le bouton *« I agree »* pour continuer, comme illustré dans les figures ci-dessous :

Figure B.2 : Début d'installation de GNS3 0.8.3.1.

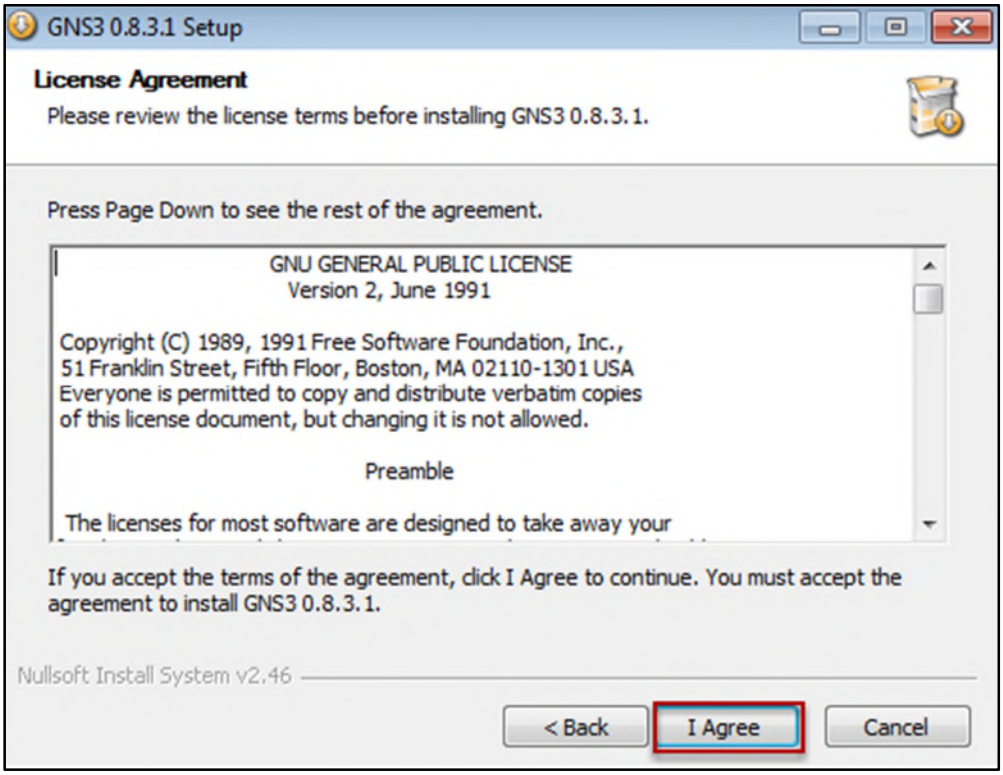


Figure B.3 : Accepter les termes de la licence.

Par défaut GNS3 créé un dossier dans le menu « Démarrer » avec le nom GNS3 en cliquant sur le bouton « Suivant ».

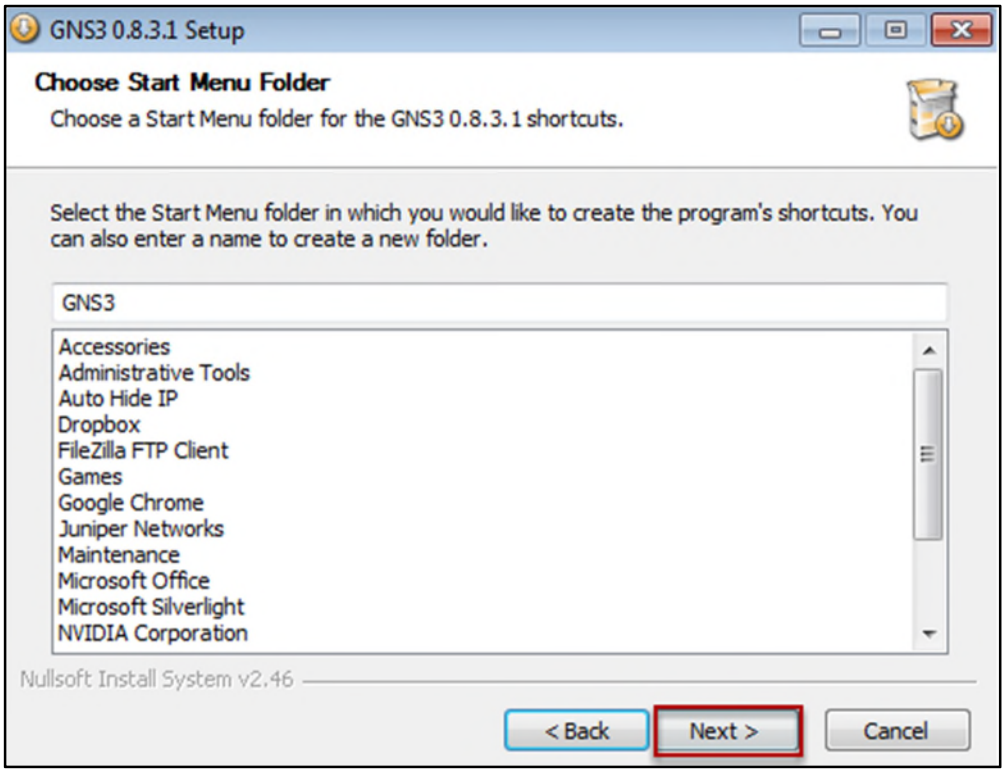


Figure B.4 : Création d'un dossier dans le menu Démarrer.

GNS3 dépend de plusieurs autres programmes pour fonctionner tel que : *WinPCAP*, *Dynamips*, et *Pemuwrapper*. Ces éléments ainsi que GNS3 sont tous choisis par défaut pour l'installation, donc il suffit de cliquer sur le bouton *« Suivant »* pour continuer. La première dépendance pour GNS3 est *« WinPcap »*.

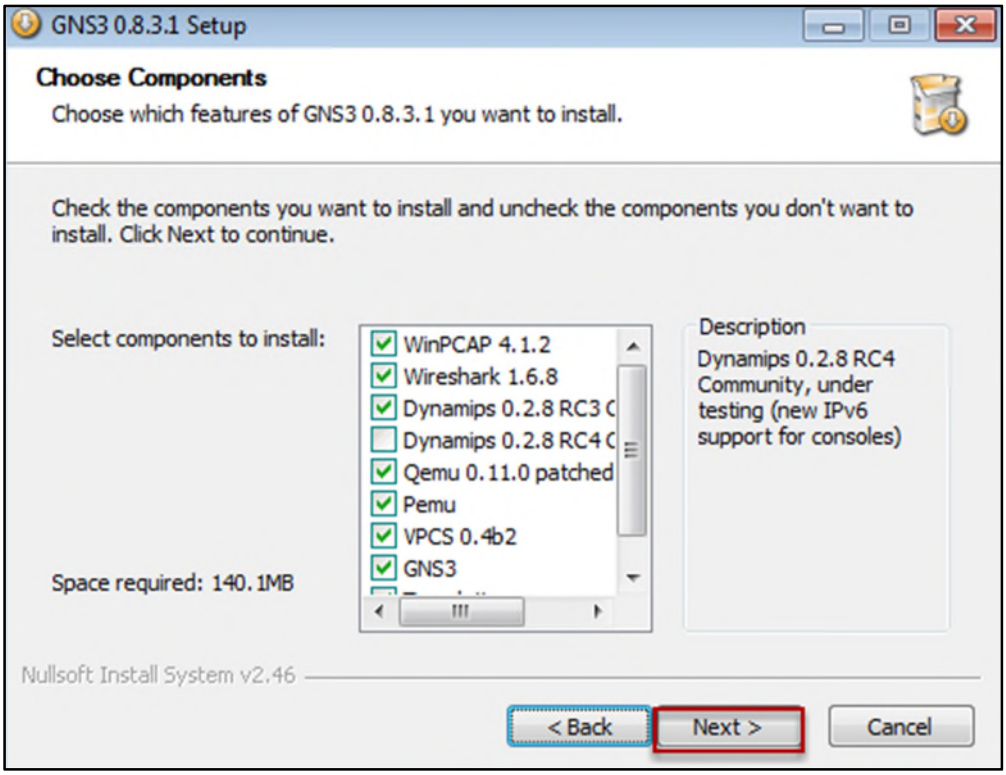


Figure B.5 : Début d'installation de winPCAP.

Un emplacement par défaut est choisi pour GNS3. Nous cliquons sur le bouton *« Installer »* pour accepter cet emplacement et commencer l'installation des fichiers.

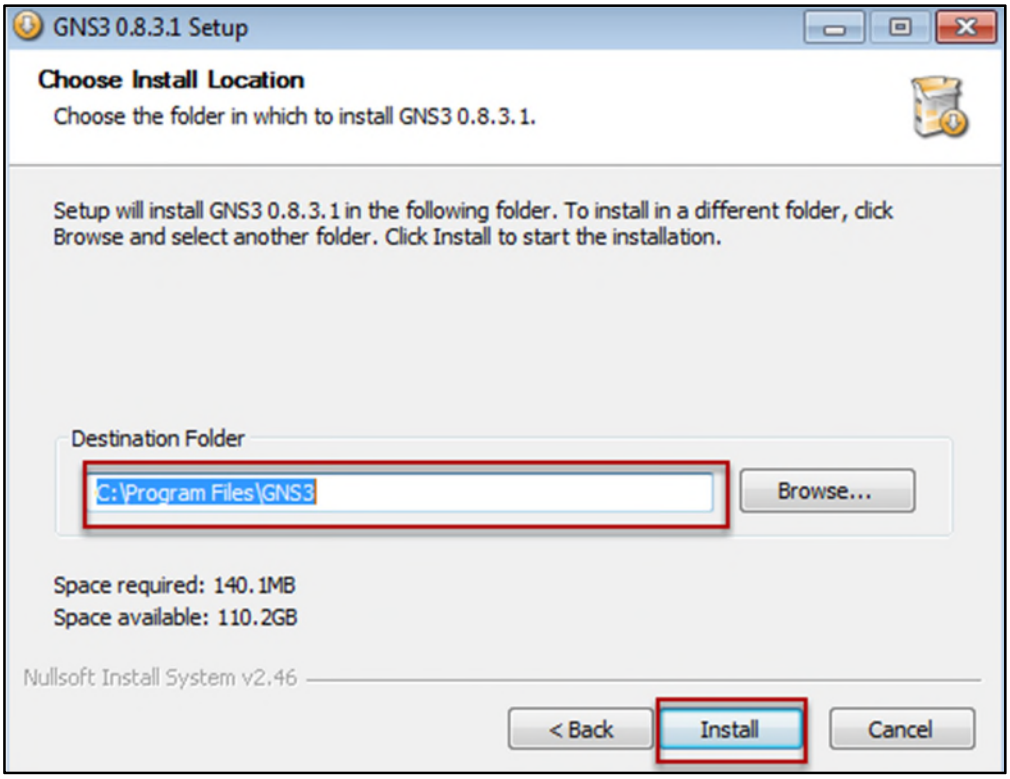


Figure B.6 : Emplacement d'enregistrement.

L'installation de WinPcap est nécessaire; sans cet élément GNS3 ne fonctionnera pas :

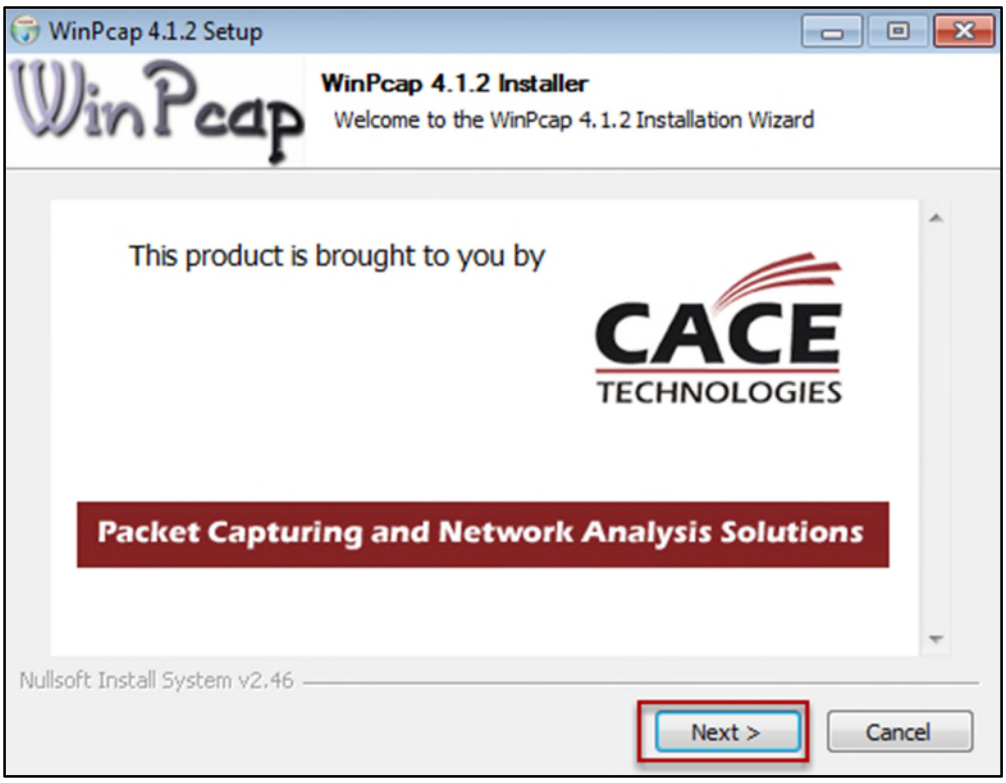


Figure B.7 : Installation de WinPacap.

Après l'installation de WinPcap, l'assistant d'installation GNS3 revient à installer GNS3. Lorsque l'assistant a terminé, nous cliquons sur le bouton *« Terminer »*.

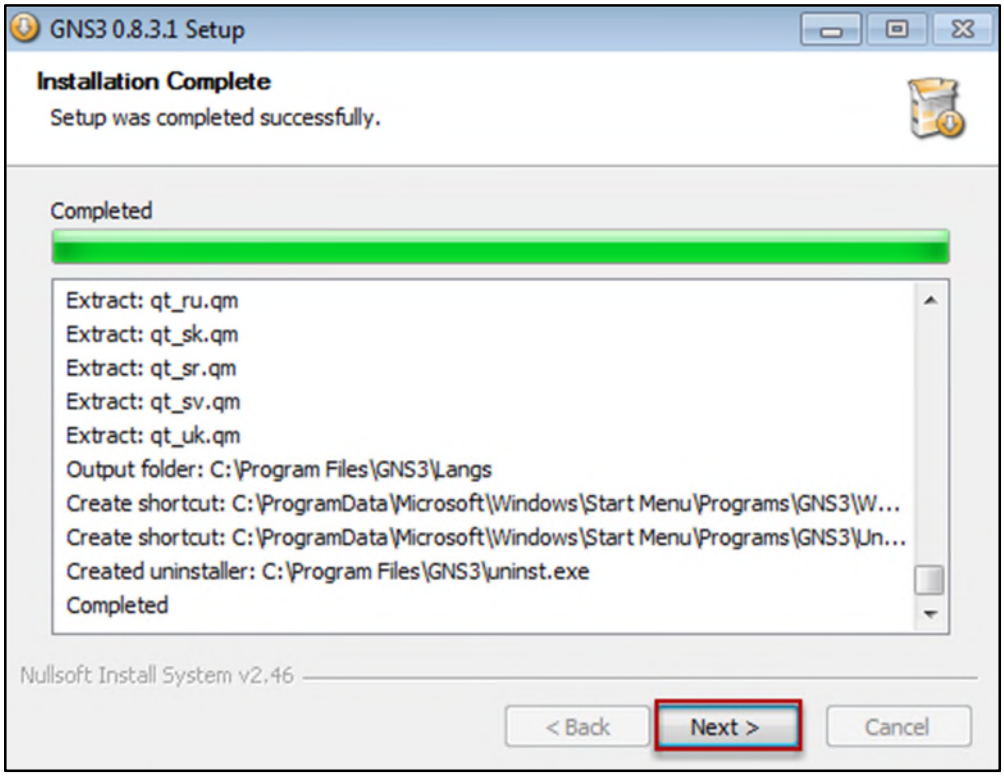


Figure B.8 : Reprise d'installation de GNS3.

Figure B.9 : Fin d'installation de GNS3.

Une fois le logiciel téléchargé et installé, nous pouvons installer et créer notre premier projet comme présenter :

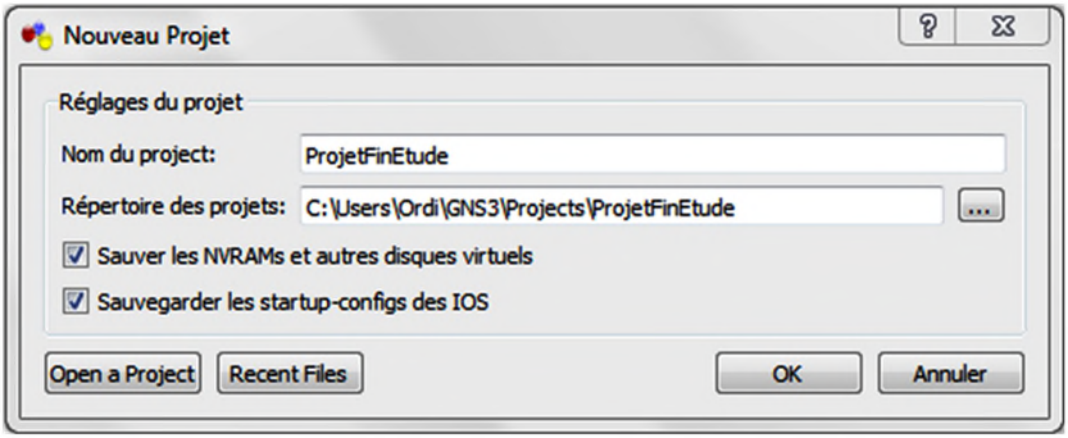


Figure B.10 : Création d'un projet.

Une fois le projet est enregistré, nous arrivons sur l'espace du travail, nous pouvons ainsi voir sur la gauche la liste des éléments actifs et matériels disponibles que nous avons la possibilité d'ajouter dans notre topologie réseau :

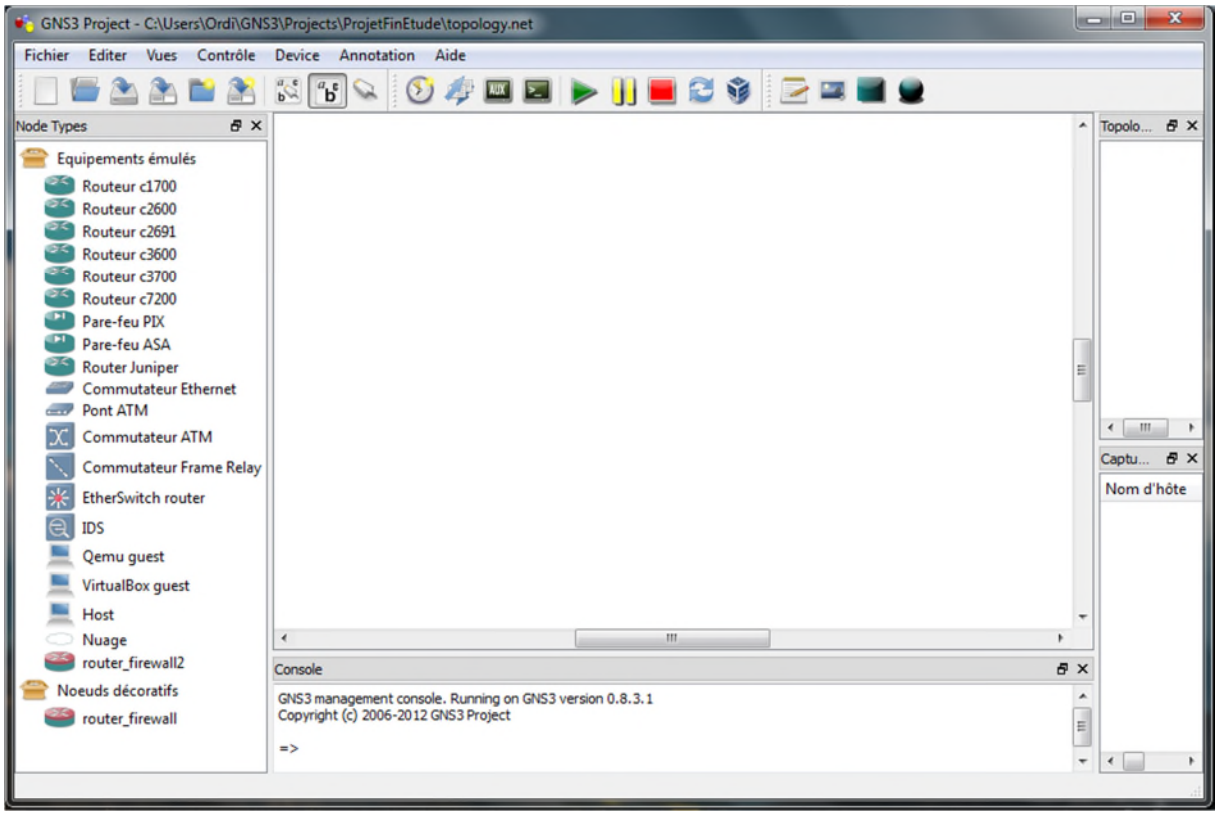


Figure B.11 : Présentation d'interface de GNS 3.

Dans notre topologie nous nous sommes servis d'un routeur Cisco 2691, pour cela nous avons à charger l'IOS correspondant dans GNS3, qui est le système d'exploitation des routeurs Cisco, c'est lui en se basant sur l'architecture matérielle qui gère le routeur, la première étape est donc de lier un IOS a un modèle de routeur, GNS3 se charge d'émuler le matériel.

Il faut donc télécharger l'IOS sous forme de fichier binaire, une fois effectué, allons dans le menu *« Editer »* et faire les opérations comme suit :

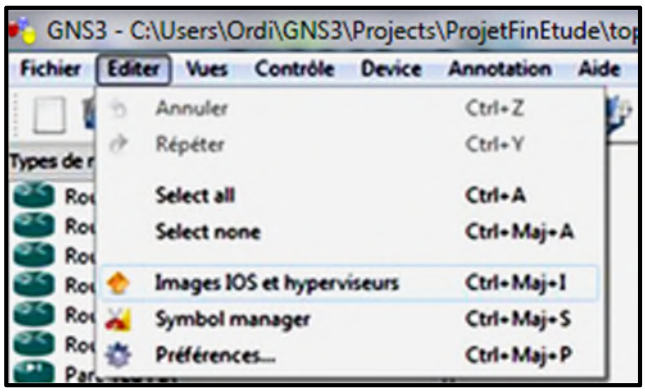


Figure B.12 : Recherche de l'image IOS.

Dans la partie *« Image binaire »*, nous avons à sélectionner le *.bin* de l'IOS Cisco 2691 précédemment téléchargé, le programme demande de décompresser le .bin pour en créer un *.image*, ensuite la validation de cette demande :

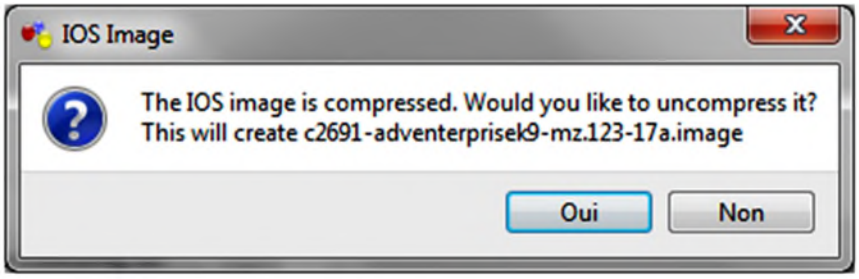


Figure B.13 : Validation de la demande de décompression.

Pour sauvegarder, il faut faire *« sauvegarder »*, pour faire apparaître dans la liste des images du modèle Cisco 2691, puis « valider » :

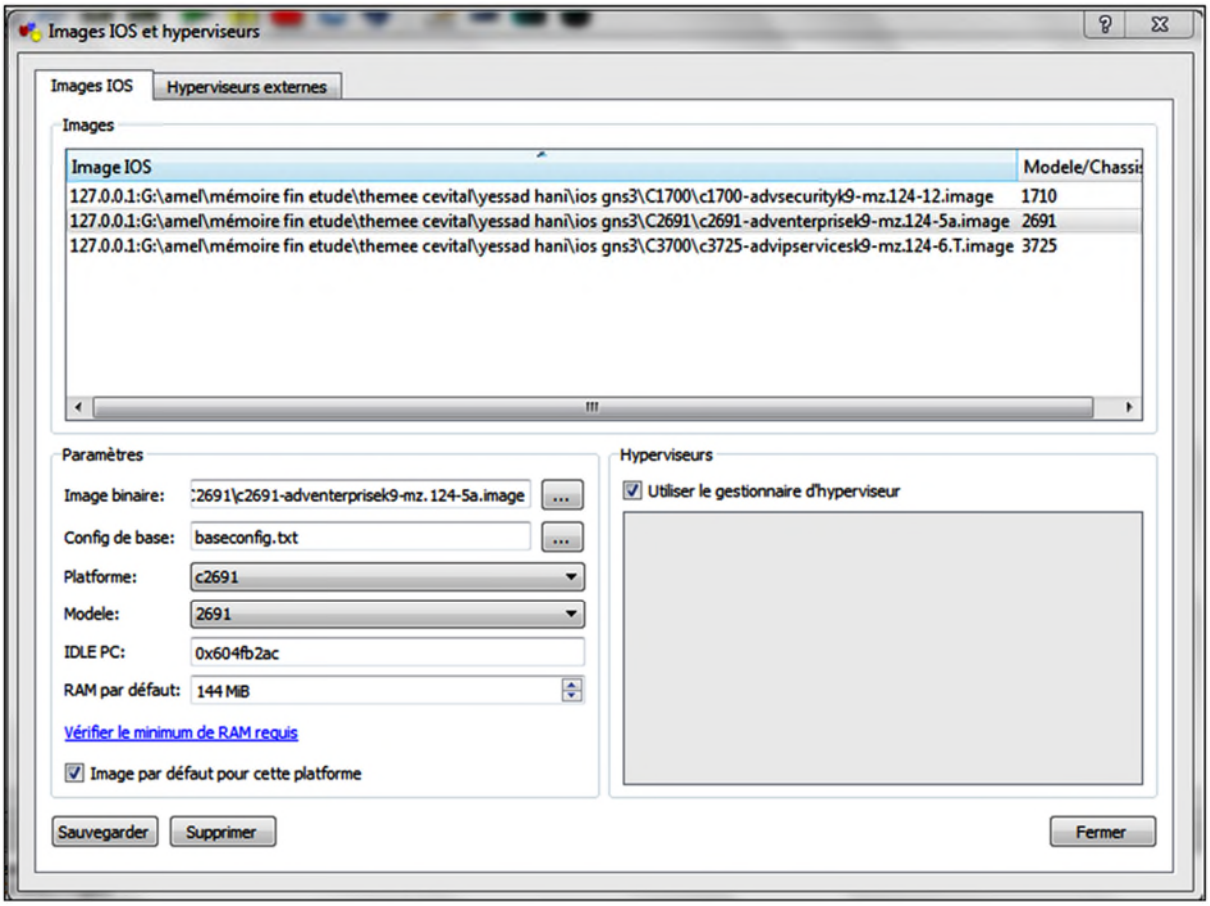


Figure B.14 : Enregistrement de l'image IOS du routeur Cisco 2691.

Résumé

Notre contribution durant ce travail était de résoudre les problèmes liés au routage statique ainsi que ceux du protocole de routage dynamique EIGRP.

Nous nous sommes intéressés au routage dynamique dans une entreprise, c'est pour cette raison que nous avons fait une comparaison entre trois protocoles de routage dynamique internes IGP les plus employés, à savoir : RIPv2, OSPF et EIGRP par la sélection du protocole le mieux approprié dans un réseau d'entreprise : cas de Cevital, afin d'assurer une opération de routage fiable, simple, rapide et sans conflits, entre les nœuds de son architecture.

Afin d'évaluer les protocoles de routage les plus connus, nous avons conçu une architecture réseau qui est configurée avec : RIPv2, EIGRP et OSPF respectivement, en utilisant l'émulateur GNS3.

A l'issu de ce travail, nous recommandons le choix du protocole de routage dynamique OSPF.

Mots-clés : Routage, IGP, RIPv2, OSPF et EIGRP.

Abstract

Our contribution in this work was to solve the problems of static as well as dynamic EIGRP routing protocol.

We are interested at the dynamic routing in a company, it is for this reason that we have made a comparison of three dynamic routing protocols internals IGP more employed, named: RIPv2, OSPF and EIGRP by selecting the best protocol appropriate in a corporate network of Cevital, to ensure reliable operation of routing, simple, fast and without conflict between the nodes of its architecture.

To evaluate the best known routing protocols, we designed a network architecture that is configured with: RIPv2, EIGRP and OSPF respectively, using the emulator GNS3.

At the end of this study, we recommend choosing the OSPF dynamic routing protocol.

Keywords: Routing, IGP, RIPv2, OSPF and EIGRP.