TABLE DES MATIERES

REMERCIEMENTS ..... **i**
TABLE DES MATIERES ..... **ii**
NOTATIONS ..... **v**

INTRODUCTION GENERALE **1**

CHAPITRE 1 RESEAU D'ENTREPRISE **2**

1.1 Introduction **2**

1.2 Quelques notions **2**

1.2.1 Différents types de réseau ***2***

1.2.2 Equipements réseau ***3***

1.2.3 Modèle de référence OSI ***7***

1.2.4 Modèle DoD ***10***

1.2.5 Comparaison entre les deux modèles OSI et TCP/IP ***11***

1.2.6 Adressage IP ***12***

1.2.7 Différents protocoles utilisés ***16***

1.3 Les entreprises monosites **21**

1.4 Les entreprises multi-sites **22**

1.4.1 Commutation de circuits ***23***

1.4.2 Commutation de paquets ***23***

1.4.3 Commutation de cellules ***24***

1.4.4 Services dédiés ***24***

1.5 Conclusion **24**

CHAPITRE 2 PERFORMANCES DES RESEAUX D'ENTREPRISE **25**

2.1 Introduction **25**

2.2 Concepts de trafics **25**

2.2.1 Définitions ***25***

2.2.2 Trafic offert, trafic écoulé ***26***

2.2.3 Profil de charge, charge A et charge B ***27***

2.3 Qualité de service **27**

2.3.1 Définition ***27***

2.3.2 QoS en réseau d'entreprise *27*

2.4 Indicateurs de performances KPI **29**

2.4.1 La bande passante *29*

2.4.2 La latence du réseau (Latency) *29*

2.4.3 La gigue (Jitter) *30*

2.4.4 Le débit réseau (Throughput) *30*

2.4.5 La perte de paquets *30*

2.4.6 Valeurs des indicateurs de performances *31*

2.5 Impact du routage IP sur la performance réseau **31**

2.5.1 Concepts de graphes valués *31*

2.5.2 Algorithme de Bellman-Ford *34*

2.5.3 Algorithme de Dijkstra *36*

2.5.4 Les protocoles de routage dynamique *38*

2.6 Conclusion **42**

CHAPITRE 3 TECHNIQUES D'OPTIMISATION DES RESEAUX INFORMATIQUES **43**

3.1 Introduction **43**

3.2 Besoins en réseau **43**

3.3 Réseaux locaux virtuels ou VLAN **43**

3.3.1 Domaine de diffusion *43*

3.3.2 Principe du VLAN *45*

3.3.3 Avantages offerts par les VLANs *45*

3.4 Modèle de conception hiérarchique **46**

3.4.1 Couche d'accès *47*

3.4.2 Couche de distribution *48*

3.4.3 Couche cœur *48*

3.5 Impacts de l'adressage sur la performance réseau **49**

3.6 Cisco Performance Routing **51**

3.6.1 Problématique et objectif *51*

3.6.2 Généralité sur PfR *54*

3.6.3 Déploiement de PfR *55*

3.6.4 Cycle des opérations de PfR *57*

3.6.5 Topologie typique du réseau d'entreprise *64*

3.6.6 Clients de la technologie PfR *65*

3.7 Conclusion **66**

CHAPITRE 4 SIMULATION **67**

4.1 Introduction **67**

4.2 Présentation du Ministère des Finances et du Budget **67**

4.2.1 Missions du Ministère des Finances et du Budget *67*

4.2.2 Structure générale du MFB *68*

4.2.3 Direction des Systèmes d'Information *69*

4.2.4 Objectifs du projet au sein du MFB *69*

4.3 Présentation de l'outil de simulation : GNS3 ..... **70**

4.4 Prise en charge du réseau existant de MFB **71**

4.4.1 Description générale du réseau *71*

4.4.2 Caractéristiques des différents équipements utilisés *72*

4.4.3 Architecture logique du réseau *75*

4.4.4 Plan d'adressage utilisé lors de la simulation *76*

4.4.5 Simulation du réseau existant sous GNS3 ..... *78*

4.5 Détermination des points faibles du réseau **84**

4.6 Optimisation des performances réseaux **85**

4.6.1 Solutions proposées face aux différents points faibles détectés *85*

4.6.2 Implémentation des solutions sous GNS3 ..... *90*

4.7 Conclusion **109**

CONCLUSION GENERALE **110**

ANNEXE EXTRAITS DE CONFIGURATIONS **111**

BIBLIOGRAPHIE **116**

FICHE DE RENSEIGNEMENTS **118**

NOTATIONS

1. Minuscules latines

d	Distance entre l'émetteur et le récepteur
n	Nombre de ressources occupées par les trafics réseaux
t_m	Durée moyenne d'occupation de la ressource par chaque demande
v	Valuation d'un graphe
x, y	Couple de sommets x et y formant un arc d'un graphe

2. Majuscules latines

A	Trafic d'un réseau
Ae	Trafic écoulé
D	Délai
E	Unité de trafic nommée Erlang
G	Graphe
$K1, K2, K3, K4, K5$	Pondérations de mesure utilisées par le protocole EIGRP
M	Matrice représentant un graphe
$M1, M2$	Valeurs de métriques calculées par EIGRP
N	Intensité de trafic
P	Perte de paquets
Rx	Représente un routeur de numéro x
S	Ensemble de sommets d'un graphe
T	Période d'observation du trafic
T_A	Temps d'attente
T_P	Temps de propagation
T_T	Durée de transmission
V_p	Vitesse de propagation

3. Abréviations

ACL	Access Control List
ANRE	Agence Nationale de Réalisation de l'E-gouvernance
ARP	Address Resolution Protocol
ATM	Asynchronous Transfer Mode

AVF	Active Virtual Forwarder
AVG	Active Virtual Gateway
BGP	Border Gateway Protocol
BP	Bande Passante
BR	Border Router
CIDR	Classless Inter Domain Routing
CLI	Command-Line Interface
CME	(Cisco Unified) Communication Manager Express
CSU/DSU	Circuit Service Unit/Data Service Unit
CV	Circuit Virtuel
DAAF	Direction des Affaires Administratives et Financières
DEL	Diode Electroluminescent
DG	Direction Générale
DHCP	Dynamic Host Configuration Protocol
DLCI	Data Link Connection Identifier
DMZ	Demilitarized Zone
DNS	Domain Name System
DoD	Department of defense
DoS	Denial Of Service
DPPPP	Direction de la Promotion du Partenariat Public Privé
DRG	Direction du Renforcement de la Gouvernance
DRH	Direction des Ressources Humaines
DSCP	Differentiated Services Code Point
DSI	Direction des Systèmes d'Information
EGP	Exterior Gateway Protocol
EIGRP	Enhanced IGRP
ETCD	Equipement de terminaison de circuit de données
ETTD	Equipement terminal de traitement de données
FAI	Fournisseur d'Accès à Internet
FDDI	Fiber Distributed Data Interface
FTP	File Transfer Protocol

GLBP	Gateway Load Balancing Protocol
GNS3	Graphical Network Simulator 3rd version
HDLC	High-Level Data Link Control
HSRP	Host Standby Routing Protocol
HTTP	HyperText Transfer Protocol
HTTPS	HyperText Transfer Protocol Secure
IANA	Internet Assigned Numbers Authority
ICMP	Internet Control Message Protocol
IDU	In Door Unit
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IGP	Interior Gateway Protocol
IGRP	Interior Gateway Routing Protocol
InARP	Inverse ARP
InterNIC	Internet Network Information Center
IOS	Internetwork Operating System
IP	Internet Protocol
IP SLA	Internet Protocol Service Level Agreement
IPS	Intrusion Prevention System
IPX	Internetwork Packet eXchange
ISO	International Standardization Organization
ISP	Internet Service Provider
KPI	Key Performance Indicator
LAN	Local Area Network
MAC	Medium Access Control
MAN	Metropolitan Area Network
MC	Master Controller
MD5	Message Digest 5
MFB	Ministère des Finances et du Budget
MOS	Mean Opinion Score
MPLS	Multiprotocol Label Switching
MTC	Monitored Traffic Class

MTU	Maximum Transmission Unit
NAT	Network Address Translation
NBNS	NetBIOS Name Service
NIC	Network Interface Card
NM	Network Module
NVRAM	Non Volatile RAM
OER	Optimized Edge Routing
OOP	Out Of Policy
OSI	Open System Interconnection
OSPF	Open Shortest Path First
PAT	Port Address Translation
PBR	Policy Based-Routing
PC	Personal Computer
PDU	Protocol Data Unit
PfR	Performance Routing
QoS	Quality Of Service
RAM	Random Access Memory
RARP	Reverse Address Resolution Protocol
RFC	Requests For Comments
RIP	Routing Information Protocol
RNIS	Réseau Numérique à Intégration de Services
RTP	Real-time Transport Protocol
RTPC	Réseau Téléphonique Public Commuté
RTT	Round Trip Time
SDN	Software-Defined Networking
SIGFP	Système Intégré de Gestion des Finances Publiques
SPOF	Single Point Of Failure
SSH	Secure SHell
TCP	Transmission Control Protocol
TOS	Type Of Service
UDP	User Datagram Protocol
UIT-T	Union Internationale des Télécommunications-Télécommunication

UTP	Unshielded Twisted Pair
VLAN	Virtual LAN
VLSM	Variable Length Subnet Masks
VoIP	Voice over IP
VPN	Virtual Private Network
VRRP	Virtual Router Redundancy Protocol
WAN	World Area Network
WIC	WAN Interface Card
WINS	Windows Internet Naming Service
xDSL	x désigne la famille et DSL Digital Subscriber Line
ZBP-F	Zone Based-Policy Firewall

INTRODUCTION GENERALE

De nos jours, le réseau fait partie intégrale de la vie économique de toute entreprise et les organisations de ces entreprises veulent toujours agrandir leurs affaires. La demande en performances des applications à temps réel augmente. En effet, en plus des partages de ressources (données, applications) et d'autres services traditionnels tels que les échanges de mails, les applications voix telle que VoIP, la téléprésence (pour les réunions à distance) font maintenant partie intégrale des réseaux d'entreprise et leurs performances sont cruciales.

Cependant, la majeure partie de ces entreprises souffre des problèmes de performances réseaux : temps de réponse applicatif détérioré, mauvaise qualité de communication audio, des services interrompus. Dans le but de remédier à ces problèmes, les entreprises ont toujours tendance à augmenter la bande passante. Certes, augmenter la bande passante peut améliorer le débit mais ceci ne permet pas d'améliorer ni les latences ni les pertes de certaines applications. De plus, la fonction des protocoles de routage n'est plus suffisante pour répondre aux besoins des réseaux convergents.

Ce présent mémoire consiste alors à analyser ces problèmes et à étudier les meilleures solutions permettant d'y palier. Un autre objectif de ce mémoire est l'étude d'une technique d'optimisation dénommée Performance Routing (PfR). Elle permet au réseau de faire une décision de routage intelligemment en répondant aux besoins des applications en termes de performances. De plus, cette technologie permet de disposer de manière appropriée les ressources et de réduire les coûts opérationnels que les entreprises doivent encourir.

Notre travail s'intitule « Optimisation de LAN et mise en œuvre de technologie PfR sur WAN d'un réseau d'entreprise » et il est divisé en quatre chapitres. Le premier chapitre est consacré à la description explicite d'un réseau d'entreprise : les notions fondamentales des réseaux informatiques, les topologies des réseaux d'entreprise et leur modèle d'architecture. Dans le deuxième chapitre, nous allons étudier les performances des réseaux d'entreprise : nous allons faire des modélisations mathématiques pour les trafics traversant le réseau ainsi que le routage IP. Nous parlerons aussi de la qualité de service ainsi que des facteurs qui affectent les performances réseaux. Dans le troisième chapitre, nous allons décrire des différentes techniques d'optimisation de réseau dont la solution de Performance Routing. Le dernier chapitre est dédié à l'étude concrète d'un réseau d'entreprise (celui du Ministère des Finances et du Budget) : l'analyse de l'existant, la détermination des points faibles et la proposition des solutions d'optimisation appropriées. La démonstration de l'efficacité de chaque solution est faite sous le simulateur réseau GNS3.

CHAPITRE 1
RESEAU D'ENTREPRISE

1.1 Introduction

Dans ce premier chapitre, nous allons introduire toutes les notions fondamentales pour la compréhension du fonctionnement des réseaux informatiques. Nous parlerons donc de tous les éléments qui entrent en jeu tels que les équipements, les protocoles, les technologies et les normes utilisés.

1.2 Quelques notions

1.2.1 Différents types de réseau

Il existe trois types de réseau suivant les distances entre les communicants :

- les réseaux LAN
- les réseaux MAN
- les réseaux WAN

1.2.1.1 Réseaux LAN (Local Area Network)

Les réseaux locaux couvrent jusqu'à 1km de région : cas dans une salle de classe, dans un bâtiment ou un campus.... Leurs caractéristiques sont les suivants :

- Ils fonctionnent dans une région géographique limitée.
- Ils permettent à de nombreux utilisateurs d'accéder à des médias à haut débit.
- Ils assurent une connectivité continue aux services locaux.
- Ils interconnectent physiquement des unités adjacentes.

1.2.1.2 Réseaux MAN (Metropolitan Area Network)

Ces réseaux connectent un ou plusieurs LAN dans une même région géographique. Ce type de réseau est en émergence du fait du développement des réseaux Wireless. On les trouve souvent en ville, situés dans les endroits publics.

1.2.1.3 Réseaux WAN (World Area Network)

Ce sont des réseaux couvrant une vaste espace, reliant des villes et des pays. Ce type de réseau a été conçu pour relier les réseaux locaux pour faire ainsi circuler les informations rapidement et efficacement entre les entreprises d'un même ou de divers pays. Leurs caractéristiques sont de :

- Couvrir une large région géographique.
- Permettre l'accès par des interfaces séries plus lentes.
- Assurer une connectivité continue et intermittente (irrégulière).
- Relier des unités dispersées à une échelle planétaire.

1.2.2 Equipements réseau

Il existe plusieurs équipements utilisés dans un réseau. [1]

- Le répéteur : c'est un composant actif (il tire l'énergie d'un bloc d'alimentation pour régénérer les signaux réseaux). Il permet de régénérer et de resynchroniser le signal afin de pouvoir étendre la portée des câbles. Il est à un seul port d'entrée et à un seul port de sortie. Il peut être symbolisé comme suit :

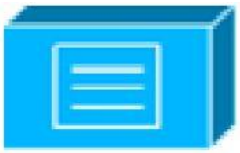


Figure 1.01 : *Symbole d'un répéteur*

- Le concentrateur : c'est un répéteur multi ports. Il reprend le fonctionnement du répéteur en ajoutant une fonctionnalité de connectivité. En effet, il dispose de plusieurs ports permettant d'interconnecter plusieurs équipements réseau. Chaque signal arrivant sur un port est régénéré, resynchronisé et réémis à travers tous les autres ports.

Figure 1.02 : *Concentrateur et son symbole*

Ces deux premiers équipements créent et manipulent des bits. Ils ne reconnaissent aucune information dans les bits, ni les adresses, ni les données. Leur fonction se limite seulement

à déplacer les bits. Ce sont des équipements de la couche 1 (couche physique) du modèle OSI.

- L'émetteur/récepteur : en anglais « Transceiver », convertit un signal en un autre. Il est souvent intégré aux cartes réseau.
- Le pont : Il se définit par son filtrage de trames de couche 2 et par la manière dont celui-ci est vraiment réalisé. Il est conçu pour connecter deux segments LAN : il permet de filtrer le trafic sur un LAN. Comme chaque unité réseau possède une adresse MAC unique sur la carte NIC, le pont effectue le suivi des adresses MAC se trouvant chacun de ses côtés et prend les décisions en fonction de cette liste d'adresses. C'est une unité à un seul port d'entrée et à un seul port de sortie.

Figure 1.03 : *Symbole du pont*

- Le commutateur : il est aussi appelé pont multiport. La différence entre le concentrateur et le commutateur est que ce dernier prend des décisions en fonction des adresses MAC. Il effectue cela en 'commutant' les données uniquement au port auquel le bon hôte est connecté. Il vise à concentrer la connectivité tout en accroissant l'efficacité de la transmission de données.

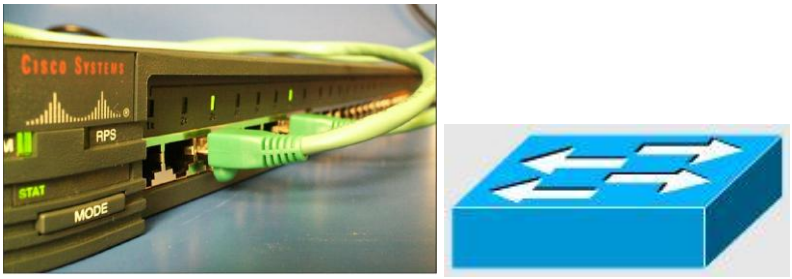


Figure 1.04 : *Commutateur et son symbole*

- Le routeur : c'est un équipement permettant d'interconnecter deux réseaux ou plus en se basant sur les adresses de couche 3 (couche réseau) du modèle OSI. Son rôle consiste à examiner les paquets entrants, à choisir le meilleur chemin pour les transporter sur le réseau et à les commuter ensuite au port de sortie approprié.

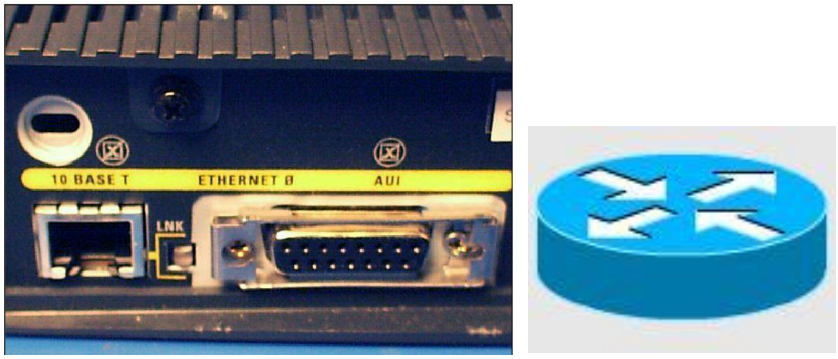


Figure 1.05 : *Routeur et son symbole*

- Les médias : permettent la liaison entre deux équipements et assurent ainsi la transmission des informations (des données) entre eux. Il existe alors plusieurs catégories de médias : les médias de cuivre, les médias optiques et les médias sans fils. [2] [3]

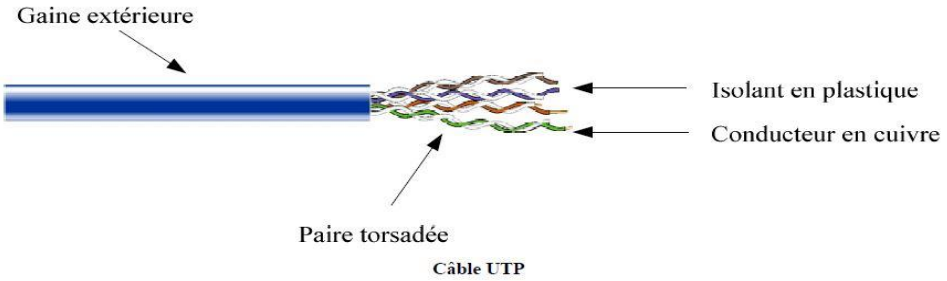


Figure 1.06 : *Câble à paires torsadées non blindées*

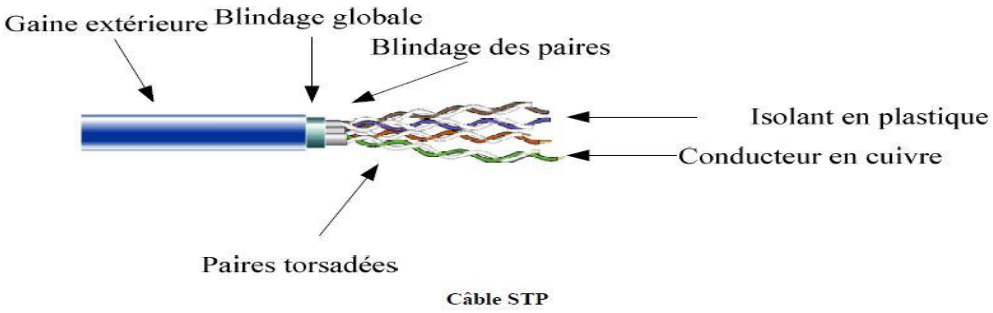


Figure 1.07 : *Câble à paires torsadées blindées*

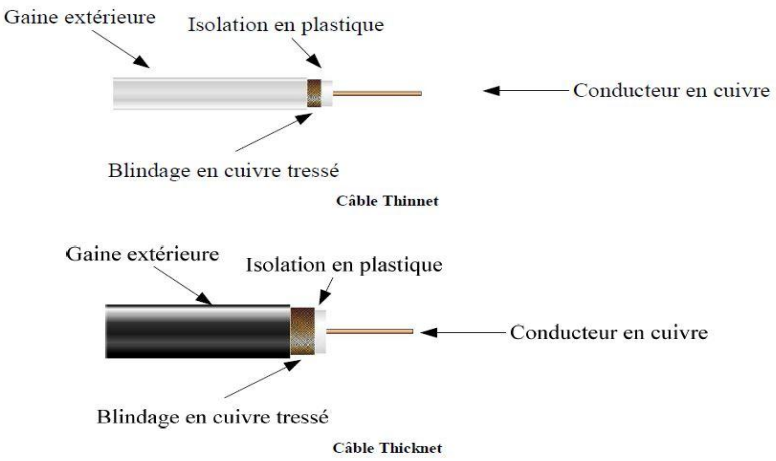


Figure 1.08 : *Câbles coaxiaux*

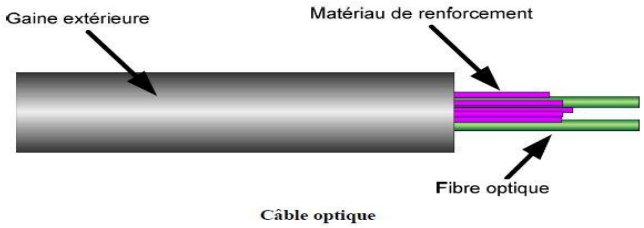


Figure 1.09 : *Câble optique*

Voici quelques exemples de bande passante maximale prise en charge par ces différents médias :

Type de medias	**Bande passante**
Câble coaxial de 50 Ohms (Ethernet 10BASE2 fin, 10BASE5 épais)	10 à 100 Mbps
Paire torsadée non blindée de catégorie 5 (Ethernet 10BASE-T, 100BASE-TX)	10 Mbps
Paire torsadée non blindée renforcée de catégorie 5 (Ethernet 10BASE-T, Fast Ethernet 100BASE-TX et 1000BASE-T)	100 Mbps
Fibre optique multimode (100BASE-FX)	100 Mbps
Fibre optique monomode (100BASE-LX)	1000 Mbps (1Gbps)
Sans fil	11 Mbps

Tableau 1.01: *Bandes passantes offertes par les différents médias*

1.2.3 Modèle de référence OSI

1.2.3.1 Description du modèle

L'OSI (Open System Interconnection) est un système modèle de référence pour interconnecter des systèmes ouverts. Il définit une architecture en couches normalisées adoptées conjointement par l'ISO et l'UIT-T pour les réseaux informatiques, téléinformatiques et télématiques. Cette architecture est constituée de sept couches dont la liaison réelle entre couches adjacentes se fait à partir des «services » ; pour deux systèmes en communication, la relation logique entre les couches se fait à partir des « protocoles ». Ces sept couches sont :

- Couche application
- Couche présentation
- Couche session
- Couche transport
- Couche réseau
- Couche liaison de données
- Couche physique [1] [4]

Le tableau ci-dessous décrit cette architecture :

Couche	**Unité de données**	**Fonctions**	**Equipements utilisés**
7-Application	Donnée	Services réseaux fournis aux processus d'application : synchronisation ; contrôle d'intégrité de données.	hôte
6-Présentation	Donnée	Représentation de données : Lisibilité, format, structure des données (utilisation de format commun).	hôte
5-Session	Donnée	Communication entre les hôtes : Etablissement, gestion et fermeture de sessions entre applications.	hôte

Couche	Unité de données	Fonctions	Equipements utilisés
4-Transport	Segment	Communication de bout en bout : Transport des données, fiabilité du transport ; établissement, maintien et fermeture des circuits virtuels ; détection des pannes et reprise ; contrôle de flux d'informations.	Hôte, nuage (possibilité de se connecter à un autre réseau ou internet en entier)
3-Réseau	Paquet	Adressage et sélection du meilleur chemin : connectivité et sélection du meilleur chemin, domaine de routage	Routeur
2-Liaison de données	Trame	Accès au média : Transfert fiable de données par le média, adressage physique et topologie de réseau, notification des erreurs et contrôle de flux	Pont, commutateur, carte réseau(NIC)
1-Physique	Bits	Transmission binaire : Spécifications électriques et mécaniques pour maintenir la liaison physique des systèmes d'extrémité : fils, connecteurs, tension, débit	Emetteur-récepteur, câble (média réseau), répéteur, concentrateur

Tableau 1.02: *Modèle OSI*

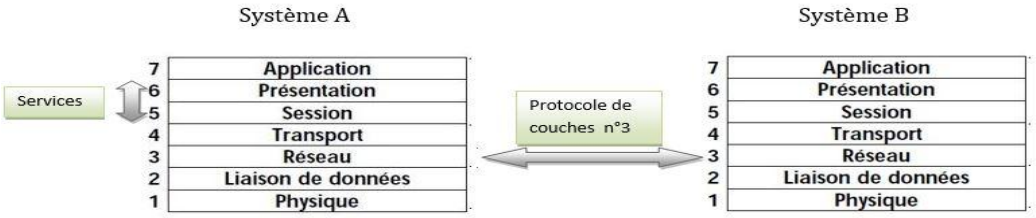


Figure 1.10 : *Liaisons entre deux couches adjacentes et deux couches de même niveau*

1.2.3.2 Encapsulation de données

Au sein d'un réseau, toutes les communications partent d'une source, puis acheminées vers une destination et les informations envoyées sur le réseau sont appelées données ou paquets de données. Si un ordinateur (hôte A) veut envoyer des données à un autre ordinateur (hôte B), les données doivent d'abord être préparées grâce à un processus appelé encapsulation. Ce processus conditionne les données en leur ajoutant des informations relatives au protocole avant de les transmettre dans le réseau. Ainsi, en descendant dans les couches du modèle OSI, les données reçoivent des en-têtes, des en-queues et d'autres informations. Pour comprendre comment se produit l'encapsulation, examinons la manière dont les données traversent les couches. Comme la montre la figure ci-dessous, les données qui sont envoyées par l'ordinateur source traversent la couche application et les autres couches. La présentation et le flux de données échangées subissent des changements au fur et à mesure que les réseaux fournissent leurs services aux utilisateurs.

Les réseaux doivent effectuer les cinq étapes de conversion suivants afin d'encapsuler les données :

a) Construction des données : lorsqu'un utilisateur envoie un message électronique, les caractères alphanumériques qu'il contient sont convertis en données pouvant circuler dans l'inter-réseau.
b) Préparation des données pour le transport de bout en bout : les données sont préparées pour le transport inter-réseau. En utilisant des segments (type de donnée dans la couche transport), la fonction de transport assure que les systèmes hôtes situés à chaque extrémité du système de messagerie peuvent communiquer de façon fiable.
c) Ajout de l'adresse réseau à l'en-tête : les données sont organisées en paquets, ou datagrammes, contenant un en-tête réseau constitué des adresses logiques d'origine et de destination. Ces adresses aident les unités réseau à acheminer les paquets dans le réseau suivant un chemin déterminé.
d) Ajout de l'adresse locale à l'en-tête de liaison : chaque unité réseau doit placer le paquet dans une trame. La trame permet d'établir la connexion avec la prochaine unité réseau directement connectée dans la liaison. Dans l'en-tête de la trame se trouve les adresses physiques de la source et de la destination.
e) Conversion en bits pour la transmission : La trame doit être convertie en une série de un et de zéro (bits) pour la transmission sur le média. Une fonction de synchronisation permet aux unités de distinguer ces bits lorsqu'ils circulent sur le média. Tout au long du trajet suivi dans l'inter-réseau physique, le média peut varier. Ainsi, le message électronique peut

provenir d'un réseau local, traverser le backbone d'un campus, sortir par une liaison WAN pour atteindre sa destination sur un autre LAN éloigné. Les en-têtes et en-queues sont ajoutés au fur et à mesure que les données descendent dans les couches du modèle OSI. [4]

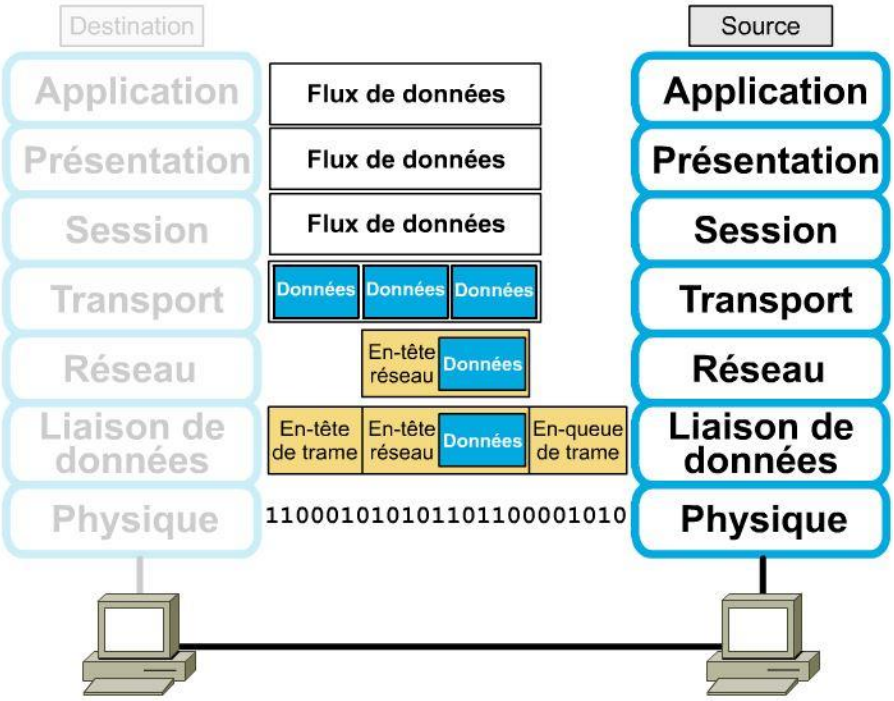


Figure 1.11 : *Encapsulation de données dans l'inter-réseau*

A la réception, des procédures inverses sont effectués aux données en traversant les couches inférieures jusqu'à la couche application, c'est la désencapsulation.

1.2.4 Modèle DoD

Le ministère de la défense (DoD) a développé le modèle de référence TCP/IP dont le but d'avoir un réseau qui résiste à toutes les situations. Ce modèle est inspiré du modèle OSI, il reprend l'approche modulaire (utilisation de modules ou couches) mais il est seulement constitué de quatre couches :

- Couche Application
- Couche Transport
- Couche Internet
- Couche Accès réseau

Depuis lors, ce modèle s'est imposé comme la norme Internet.
Le tableau suivant décrit l'architecture du modèle DoD :

Couche	Unités de données	Fonctions
Application	Donnée	Gestion des protocoles de haut niveau, des questions de présentation, assure le code et le contrôle de dialogue.
Transport	Segment	Fiabilité des communications réseaux ; établissement d'un dialogue entre ordinateur source et ordinateur destination ; contrôle de flux et correction des erreurs.
Internet	Paquet	Identification de meilleur chemin pour l'envoi des paquets sources ; commutation de paquets.
Accès au réseau	Trame - bits	Etablissement de liaison physique pour un paquet physique. Elle comprend les détails dans les couches physiques et liaison de donnée du modèle OSI

Tableau 1.03: *Modèle DoD*

1.2.5 Comparaison entre les deux modèles OSI et TCP/IP

1.2.5.1 Similitudes

- Tous les deux comportent des couches.
- Ils comportent une couche application bien que chacune fournisse des services très différents.
- Les deux comportent des couches réseau et transport comparables.
- Ils supposent l'utilisation de la technologie de commutation de paquets et non de commutation de circuits.

1.2.5.2 Différences

- TCP/IP intègre la couche présentation et la couche session dans sa couche application.
- TCP/IP regroupe les couches physiques et liaison de données OSI au sein d'une seule couche.
- TCP/IP présente moins de couches et semble plus simple.
- Les protocoles TCP/IP constituent la norme sur laquelle s'est développé Internet.

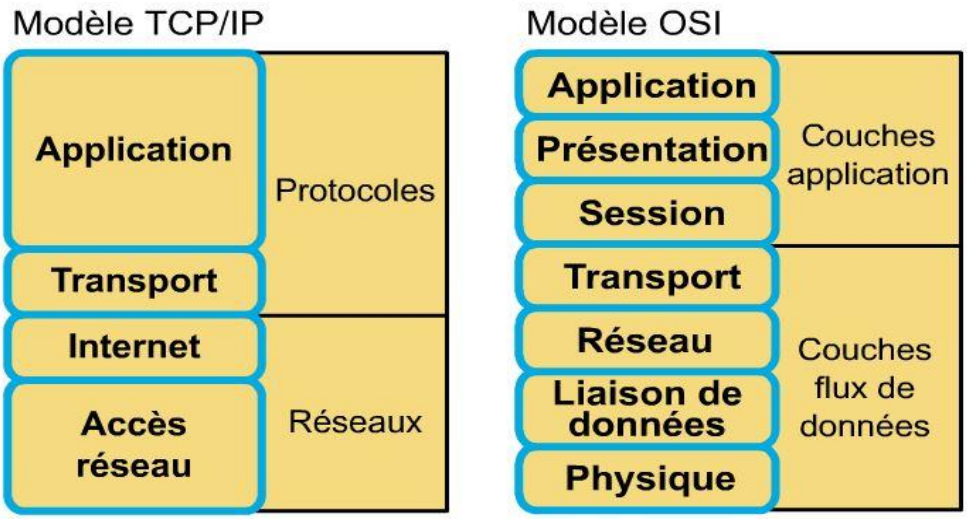


Figure 1.12 : *Comparaison des deux modèles*

1.2.6 Adressage IP

La présence d'une multitude d'équipements terminaux oblige à définir un système d'identification cohérent au sein du réseau pour les différencier : c'est la fonction d'adressage. [5]

Dans un réseau TCP/IP, tous les hôtes connectés possèdent des adresses qui peuvent les identifier au sein du réseau et par les autres réseaux. Pour la communication entre des machines du même réseau, elles utilisent leurs adresses MAC qui sont encapsulées dans l'en-tête et l'en-queue de la trame de la couche liaison de données du modèle OSI. Cette adresse MAC est une adresse physique ; elle est composée de 48 bits et représentée par des nombres hexadécimaux. L'adresse MAC unique de chaque machine se trouve sur sa carte réseau.

Tandis que pour faire communiquer deux machines appartenant à deux différents réseaux, on a besoin des adresses IP. C'est une adresse souvent dite logique ; c'est un identifiant unique attribué à chaque interface et associé à une machine (ordinateur, routeur,…). Cette adresse se trouve dans l'en-tête des paquets échangés.

Une adresse IP est composée de 32 bits représentés par 4 octets séparés par des points et notés en décimal.

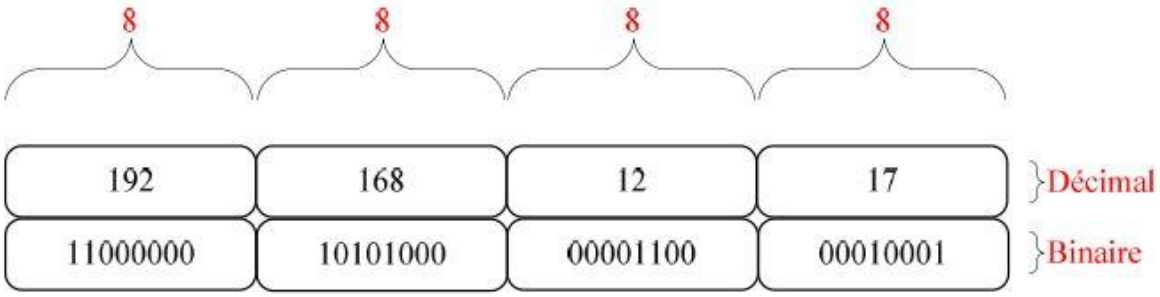


Figure 1.13 : *Exemple d'adresse IP*

Une adresse IP est décomposée en deux parties [6]:

- Une partie qui identifie le réseau dans lequel se trouve l'hôte ; c'est le netID
- Une partie qui identifie le numéro de l'hôte dans le réseau ; c'est le hostID

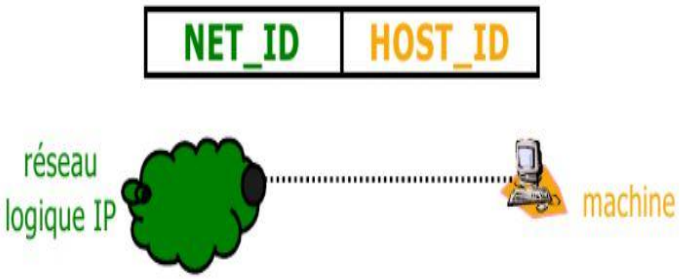


Figure 1.14 : *Les deux parties d'une adresse IP*

Seules les machines appartenant à un même réseau peuvent se communiquer directement, c'est-à-dire ayant le même netID. Dans le cas contraire, elles pourront le faire à partir d'une passerelle qui est souvent un routeur.

Il existe deux versions de l'adresse IP :

- L'IPv4 qui utilise les adresses codées en 32bits comme précédemment permet d'adresser 2^{32} machines soit 4 294 967 296 adresses possibles. Actuellement, cette version n'arrive plus à répondre à l'énorme croissance des hôtes au sein des différents réseaux mais elle reste la plus utilisée.
- L'IPv6 permet de coder les adresses IP en 128 bits sous forme de 8 nombres hexadécimaux séparés de « : ». L'IPv6 permet alors d'adresser 2^{128} machines, c'est une version qui commence à faire son essor pour résoudre le déficit de l'IPv4 et assurer les futurs besoins des nouveaux réseaux.

1.2.6.1 Adresses IP avec classes

On distingue deux types de réseaux qu'on peut adresser en IP [6]:

- Le réseau public Internet où chaque équipement connecté possède une adresse unique et enregistrée au niveau mondial.
- Les réseaux privés dans lesquels le choix des adresses de chaque réseau est libre et que les adresses ne sont uniques que dans ce réseau.

Les adresses IP avec classes concernent les adresses privées. Il existe cinq classes d'adresses IP qui sont attribuées par l'organisme InterNIC (Internet Network Information Center), aujourd'hui remplacé par l'IANA (Internet Assigned Numbers Authority). Ces classes d'adresses se diffèrent par les bits de poids fort qui les composent (ce sont les premiers bits de l'octet le plus à gauche de l'adresse). Pour ne pas confondre les adresses publiques des privées, ces dernières sont résumées avec les plages correspondantes dans le tableau suivant :

Classe	**Plage**	
A	0.0.0.0	127.255.255.255
B	128.0.0.0	191.255.255.255
C	192.0.0.0	223.255.255.255
D	224.0.0.0	239.255.255.255
E	240.0.0.0	247.255.255.255

Tableau 1.04: *Les différentes classes d'adresse IP*

1.2.6.2 Sous-réseaux et masque de sous-réseau

Afin d'améliorer la capacité et mieux gérer le trafic, maîtriser l'adressage au sein du réseau et assurer sa sécurité, il est possible de subdiviser les grands réseaux en plusieurs segments ou sous-réseaux de petites tailles.

Le principe de création des sous-réseaux est le suivant : emprunter des bits à la partie hôte de l'adresse IP; la partie hôte originale est alors divisée en deux pour avoir le champ de sous-réseau (subnetID) et la nouvelle partie machine (hôte). Le nombre minimal de bits à emprunter est deux et le nombre maximal est le nombre restant en laissant 2 bits à la partie hôte.

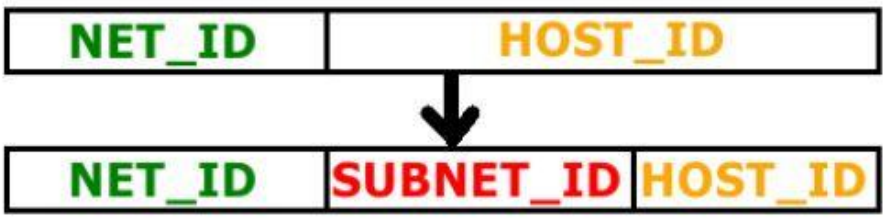


Figure 1.15 : *Création de sous-réseaux*

De la même façon que pour un réseau entier, le découpage en sous-réseaux nécessite l'utilisation de masques de sous-réseaux. Le masque de sous réseau englobe alors la partie netID initiale et la partie subnetID. [7]

1.2.6.3 Adresses IP sans classe – CIDR et VLSM

On sait que pour pouvoir accéder à Internet, un équipement d'une entreprise a besoin d'une adresse publique, les adresses privées, quant à elles, sont affectées aux autres machines afin de pouvoir se communiquer de façon interne. Les adresses publiques sont attribuées par un FAI (Fournisseur d'Accès Internet).

Pour résoudre la pénurie en adresses publiques due à l'évolution exponentielle de l'Internet et au découpage fixe de l'espace d'adressage d'IPv4 (notion de classe), à part l'élaboration de la nouvelle version IPv6 des adresses IP, on utilise l'adressage sans classe (classless) qui permet d'envoyer le masque de sous-réseau utilisé sur les autres équipements afin de créer des sous-réseaux de tailles différentes.

Le CIDR (Classless Inter Domain Routing) et le VLSM (Variable Length Subnet Masks) sont deux procédures différentes mais complémentaires de l'adressage classless. Le VLSM permet de résoudre le problème de gaspillage d'adresses au sein d'une entreprise à partir des masques de sous-réseaux de tailles variables ; le CIDR permet de réduire les nombreuses entrées des tables de routage (qu'on va expliquer ultérieurement), dues aux différents sous-réseaux à gérer, en utilisant des agrégations des routes.

Le principe d'agrégation de routes se fait en conservant la partie réseau en commun de toutes les adresses des sous-réseaux à combiner et en remplaçant par 0 les bits restants ; on obtient ainsi l'adresse agrégée et le nouveau masque de sous-réseau à utiliser dans la table de routage. C'est la notion de résumé de routes ou supernetting.

Le VLSM quant à lui permet de subdiviser une adresse déjà divisée en sous réseaux. Il repose aussi sur le principe d'agrégation. En général, on décompose alors l'adresse de classe C en plusieurs sous-

réseaux de tailles variables : de grands sous-réseaux pour les LAN et de très petits pour les liaisons WAN.

1.2.7 Différents protocoles utilisés

1.2.7.1 ARP, RARP, ARP-Inverse

- ARP (Address Resolution Protocol) est un protocole de la couche réseau qui permet à une station IP de connaître l'adresse physique (adresse MAC ou autre) d'une autre station en sachant son adresse IP. La correspondance entre adresse IP et adresse physique se résume dans une table appelée table ARP stockée dans chaque station. [8]
- RARP (Reverse Address Resolution Protocol) est un protocole de niveau 3 aussi et détermine l'adresse IP d'une station à partir de son adresse MAC et auprès d'un serveur d'adresses. [8]
- InARP (Inverse ARP) est un protocole du réseau de transport Frame Relay ou ATM. C'est le mécanisme inverse d'ARP : il permet à un routeur de connaître l'adresse IP d'un autre routeur se trouvant à l'autre bout d'un circuit virtuel.

1.2.7.2 DHCP (Dynamic Host Configuration Protocol)

DHCP est un protocole qui fonctionne en mode client-serveur. Il sert à configurer dynamiquement les clients au niveau de la couche 3 comme l'attribution d'adresse IP. L'utilisation de ce protocole offre un gain de temps extrêmement précieux aux administrateurs réseau pour l'adressage des ordinateurs de bureau clients. Il faut noter que les équipements tels que les routeurs, les commutateurs et les serveurs sont attribués d'adresses IP statiques.

Le protocole DHCP s'appuie sur le protocole de transport UDP (User Datagram Protocol) et fonctionne sur un principe de location ou de bail. Le client envoie des messages au serveur sur le port 67 ; le serveur répond le client au port 68.

DHCP offre jusqu'à une trentaine de paramètres de configuration dont les principaux sont l'attribution d'adresse IP, le masque de sous-réseau, l'adresse IP passerelle par défaut, l'adresse IP de serveur DNS. Il assure ainsi la configuration automatique des paramètres IP d'une station: attribution automatique d'adresse IP et d'un masque de sous réseau. Il configure aussi l'adresse de passerelle par défaut, des serveurs DNS, des serveurs de noms NBNS ou serveurs WINS (Windows Internet Naming Service pour les réseaux de la société Microsoft).

Son fonctionnement est décrit par la figure suivante :

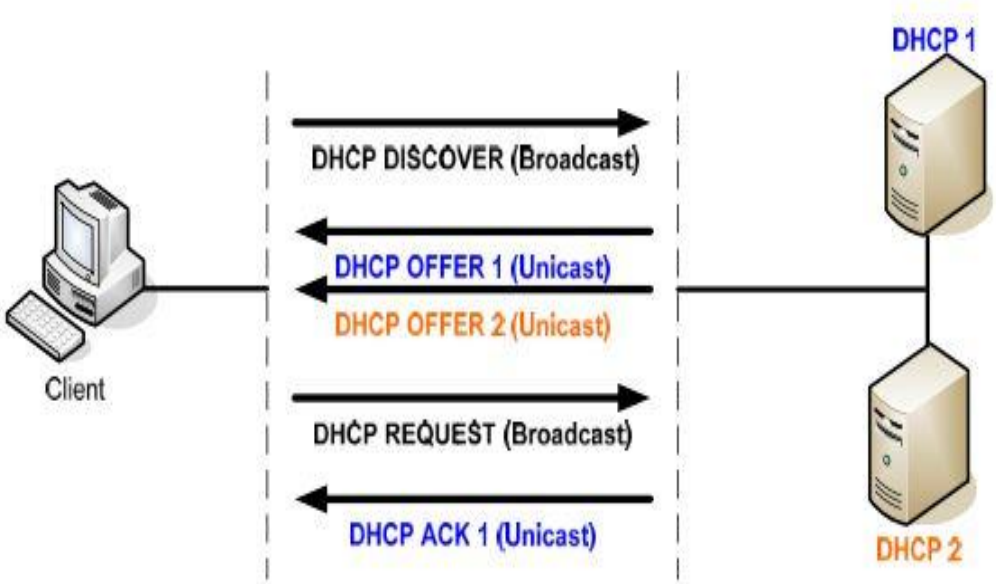


Figure 1.16 : *Fonctionnement de DHCP*

1.2.7.3 DNS (Domain Name System)

Pour une entreprise, il est difficile de retenir l'adresse IP d'un site car elle n'a aucun rapport apparent avec le contenu du site. Le protocole DNS permet alors d'associer des noms en langage courant aux adresses numériques. Pour ce faire, il y a mise en place d'un système de gestion de noms appelé Domain Name System ou Système de nom de domaine. Ce système consiste en une hiérarchie de noms permettant de garantir l'unicité d'un nom dans une structure arborescente.

On appelle FQDN (Full Qualified Domain) l'adresse qui permet de repérer de façon unique une machine. C'est l'ensemble d'un nom d'hôte, d'un point, et du nom de domaine. Le nom de domaine comporte deux composantes : le premier est le nom correspondant au nom de l'organisation ou de l'entreprise et le second est la classification de domaine (.fr, .com, .edu,… selon l'activité de l'entreprise). Le nom d'hôte est unique dans le domaine considéré, www est un exemple pour le serveur web.

Chaque ordinateur doit être configuré avec l'adresse d'une machine capable de transformer n'importe quel nom en une adresse IP. Cette machine est appelée Domain Name Server ou Serveur de nom de domaine.

1.2.7.4 ICMP (Internet Control Message Protocol)

ICMP est un protocole qui fonctionne au niveau de la couche 3. Il offre des fonctions de messagerie et de contrôle pour IP lors de la transmission de paquets. Les messages du protocole ICMP peuvent être des messages d'erreurs ou des messages de contrôle. Il faut noter qu'ICMP ne signale l'état du paquet transmis qu'à l'équipement d'origine. Il ne corrige pas les erreurs, il sert juste à en faire part. [9]

L'utilisation principale de ce protocole est dans la commande *ping* qui permet de tester l'accessibilité et la disponibilité d'une destination et aussi de reporter les erreurs: après une demande echo, une réponse echo confirme l'accessibilité ou non de la destination.

Après une commande ping effectuée, on obtient des informations telles que: le temps mis par le paquet pour atteindre une adresse, le problème de routage rencontré pour atteindre un hôte.

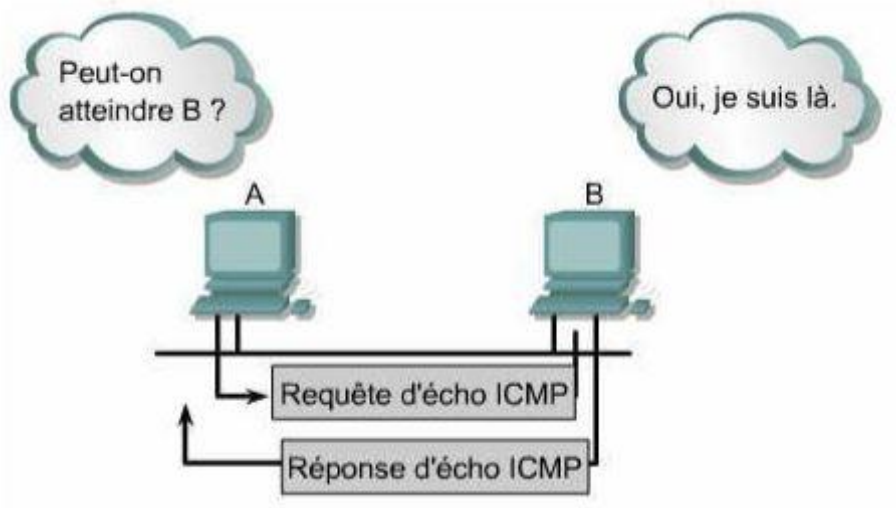


Figure 1.17 : *Echo Request/Reply ICMP lors d'un ping*

1.2.7.5 TCP (Transmission Control Protocol) et UDP (User Datagram Protocol)

Ces deux protocoles sont utilisés dans la couche transport. Cette couche ajoute au mécanisme d'envoi d'informations de l'émetteur au destinataire la notion de « qualité de service », à savoir la garantie d'un acheminement fiable des informations au travers du réseau.

TCP est un protocole orienté connexion, c'est-à-dire qu'il associe au transport des informations la notion de qualité en offrant les services suivants :

- Fiabilité
- Division des messages sortants en segments

- Réassemblage des messages au niveau du destinataire
- Renvoi de toute donnée non reçue

UDP est, lui, un protocole non orienté connexion, c'est-à-dire qu'il n'offre pas de fonction de contrôle du bon acheminement :

- Aucune vérification logicielle de la livraison des messages
- Pas de réassemblage des messages entrants
- Pas d'accusé de réception
- Aucun contrôle de flux

Cependant, UDP offre l'avantage de nécessiter moins de bande passante que TCP. Il peut donc être intéressant d'utiliser ce protocole pour l'envoi de messages ne nécessitant pas de contrôle de qualité.

Afin que plusieurs communications puissent circuler en même temps, TCP et UDP utilisent des numéros de ports. Des conventions ont été établies pour des applications, en voici quelques exemples:

Protocoles	**N° de port**	**Description**
FTP (data)	20	File Transfer (données par défaut)
FTP	21	File Transfer (Contrôle)
SSH	22	Secure Shell
Telnet	23	Telnet
SMTP	25	Simple Mail Transfer
DNS	53	Domain Name System
http	80	World Wide Web HTTP (HyperText Transfer Protocol)
POP3	110	Post Office Protocol – Version 3
HTTPS	443	Protocole HTTP sécurisé (SSL)

Tableau 1.05: *Ports utilisés pour des exemples d'applications*

Le service orienté connexion de TCP comportent 3 points importants :

- Un chemin unique entre les unités d'origine et de destination est déterminé

- Les données sont transmises de manière séquentielle et arrivent à destination dans l'ordre
- La connexion est fermée lorsqu'elle n'est plus nécessaire

Il existe également des méthodes garantissant la fiabilité :

- *La technique Positive Acknowledgement Retransmission* ou PAR qui consiste à envoyer un paquet, démarrer un compteur puis attendre un accusé de réception avant d'envoyer le suivant. Si le compteur arrive à expiration avant l'arrivée de l'accusé, les informations sont alors retransmises plus lentement et un nouveau compteur est déclenché. Cependant, cette technique est consommatrice de bande passante, c'est alors qu'intervient le mécanisme de fenêtrage.
- *Le fenêtrage* qui est un mécanisme dans lequel le récepteur envoi un accusé de réception après avoir reçu un certain nombre de données. Si le destinataire n'envoie pas d'accusé, cela signifie pour l'émetteur que les informations ne sont pas parvenues correctement et dans ce cas sont retransmises. La taille de la fenêtre détermine la quantité de données que l'on peut transmettre avant de recevoir un accusé de réception. TCP utilise un système d'accusé de réception prévisionnel, ce qui signifie que le numéro d'accusé renvoyé indique la prochaine séquence attendue

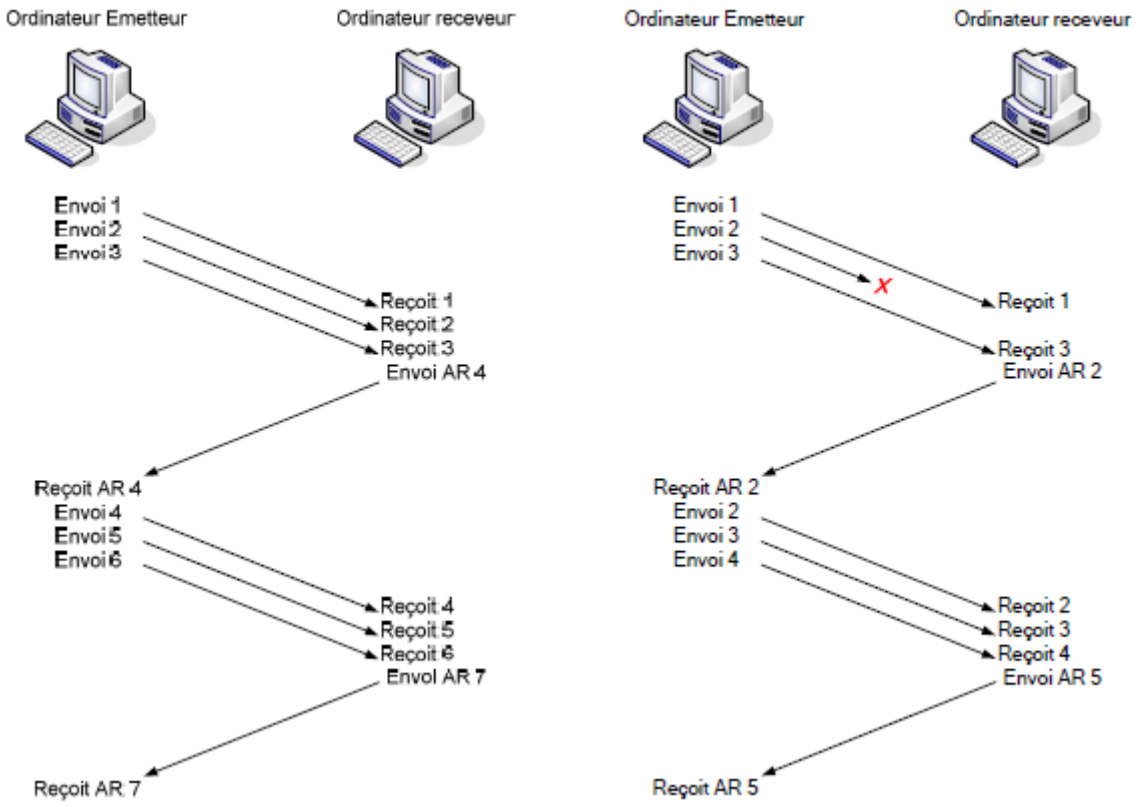


Figure 1.18 : *Transmission sans perte puis avec perte de paquet*

1.3 Les entreprises monosites

Le réseau d'une entreprise monosite est constitué d'un ensemble de réseaux Ethernet commutés de sorte à avoir une duplication des chemins vers les routeurs centraux. Ces derniers redistribuent les paquets vers la périphérie ou envoient les paquets vers l'extérieur de l'entreprise par l'intermédiaire d'un pare-feu. L'extérieur de l'entreprise ici peut être l'Internet. Aujourd'hui, un réseau d'entreprise est essentiellement bâti sur une technologie Ethernet, associée à des réseaux VLAN pour sécuriser et isoler les sous-réseaux.

De plus en plus, les réseaux employés dans l'entreprise sont des réseaux commutés et non plus partagés. La raison de cette mutation tient à l'intégration de la téléphonie, qui nécessite une qualité de service qu'il est impossible de garantir dans les réseaux partagés.

Par ailleurs, on y trouve aussi la composante radio en particulier le wifi. En effet, des équipements terminaux (laptop, tablette, smartphone…) de plus en plus nombreux se connectent directement par radio sur des contrôleurs qui peuvent être eux-mêmes des commutateurs Ethernet ou être connectés sur un commutateur Ethernet. [10]

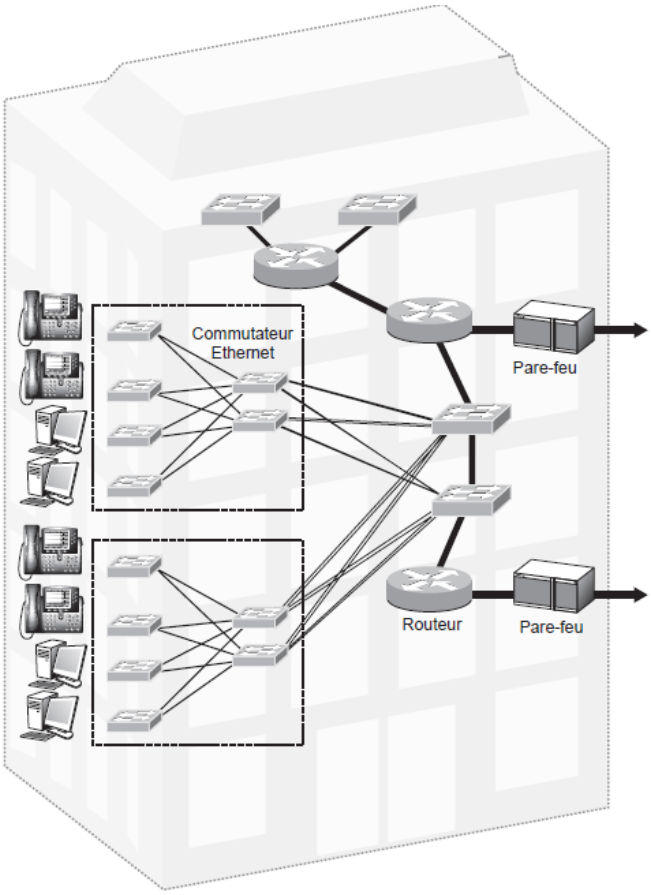


Figure 1.19 : *Exemple de réseau d'entreprise monosite*

1.4 Les entreprises multi-sites

Les réseaux d'entreprise multi-sites sont globalement formés de deux parties importantes, le réseau à l'intérieur de chaque site et le réseau permettant de relier les sites entre eux. Le réseau à l'intérieur de chaque site peut être vu comme un réseau monosite (LAN).

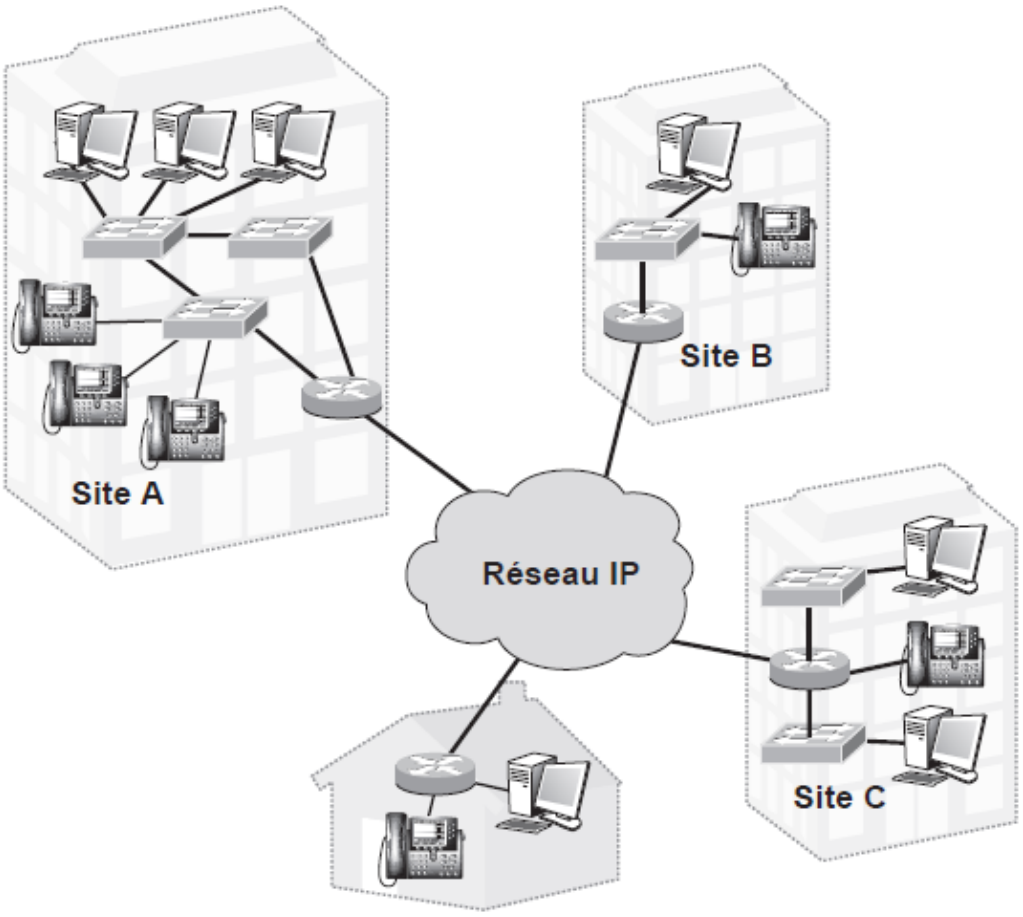


Figure 1.20 : *Exemple d'entreprise multi-sites*

En prenant l'exemple de cette figure, l'entreprise comporte trois sites, plus le domicile d'un télétravailleur. Ces derniers sont reliés entre eux par le réseau IP qui lui est offert par l'opérateur télécom.

Ainsi, quand on parle de réseau multi-site on revient à parler de réseau étendu (WAN). [11]

Pour interconnecter les différents sites, l'opérateur propose aux entreprises des différentes technologies WAN, dénommées réseaux de transport, résumées ci-dessous et dont le choix parmi ces dernières se fera en fonction des besoins de l'entreprise en question, de l'offre du marché et du coût.

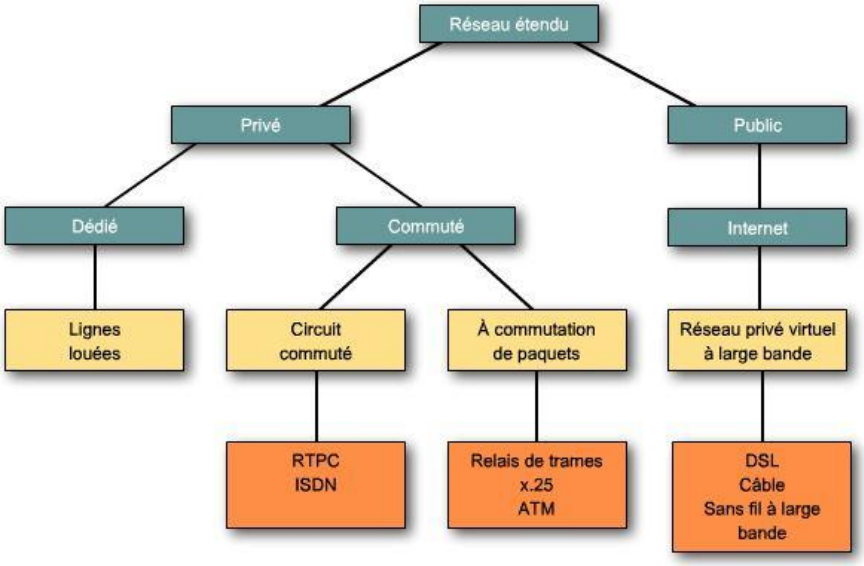


Figure 1.21 : *Les technologies WAN*

1.4.1 Commutation de circuits

C'est une commutation physique qui consiste à mettre bout à bout des tronçons de lignes de transmissions pour relier deux correspondants distants. C'est la commutation utilisée dans les réseaux téléphoniques.

Elle établit de façon dynamique une connexion virtuelle dédiée pour la voix ou les données et elle est effectuée dans les centraux téléphoniques. La liaison se fait de manière non permanente mais assure une bande passante maximale pendant la durée de la communication.

Le RTPC (Réseau Téléphonique Public Commuté) et le RNIS (Réseau Numérique à Intégration de Services) sont des exemples de commutation de circuits.

1.4.2 Commutation de paquets

C'est une commutation logique qui consiste à découper l'information initiale en plusieurs parties appelées paquets. Ces paquets vont ensuite transiter dans le réseau en empruntant des différents chemins selon la disponibilité des nœuds du réseau. Ces paquets sont libellés afin que le récepteur puisse les restituer. La taille des paquets dépend de la capacité d'acheminement des nœuds, cette capacité est appelée MTU (Maximum Transmission Unit) ou Unité de transfert maximal. C'est donc la taille maximale d'un paquet pouvant être transmis en une seule fois sur une interface. La bande passante est partagée entre les différents trafics de façon permanente.

Le Frame Relay ou relais de trame et le X.25 sont des exemples de ce type de commutation. [12] [13]

1.4.3 Commutation de cellules

C'est une commutation de paquets particulière. Le principe est le même que celui de la commutation de paquets, elle se diffère seulement de la taille de paquets qui reste fixe et porte le nom de cellules. L'ATM (Asynchronous Transfer Mode) est l'exemple de cette commutation. Dans le réseau ATM, la taille des cellules est de 53 octets permettant ainsi d'avoir des débits élevés.

1.4.4 Services dédiés

Ce type de service offre un lien physique dédié entre chaque source et destination. Le nombre de liens augmente donc en fonction du nombre d'utilisateurs à interconnecter. Les fournisseurs de services offrent ainsi à ses clients des lignes louées appelées aussi lignes spécialisées. On peut citer des exemples tels que les technologies xDSL (x désigne la famille et DSL Digital Subscriber Line), T1, T3, E1 et E3.

Notons qu'il existe aussi d'autres services qui font intervenir les systèmes satellites, le modem câble et le sans fil qui servent surtout à la connexion à Internet.

1.5 Conclusion

Dans ce premier chapitre, nous nous sommes familiarisés avec le monde du réseau d'entreprise en commençant par les notions de bases d'un réseau IP telles que les différents types de réseaux existants, les équipements réseaux utilisés, la notion d'adressage IP, les protocoles les plus utilisés. Nous avons aussi parlé des entreprises monosites et multi-sites ainsi que l'architecture interne d'un réseau d'entreprise afin de mieux comprendre son fonctionnement.

Dans le chapitre suivant, nous allons nous intéresser aux performances d'un réseau d'entreprise afin de l'évaluer et de l'analyser plus en profondeur.

CHAPITRE 2
PERFORMANCES DES RESEAUX D'ENTREPRISE

2.1 Introduction

La notion de performance est toujours liée à la qualité de service. Celle-ci est relative à la perception qu'a l'usager de la réponse du réseau à sa demande. Il ne faut jamais perdre de vue cette finalité, car c'est elle qui guide l'efficacité économique, et non pas la performance pour la performance. [14]
Cependant, l'atteinte de cet objectif ne peut être que complexe compte tenu à la fois de la diversité des requêtes, de la diversité des équipements mis en jeux et de la complexité des réseaux utilisés.
La qualité de service vue de l'usager sera en fait le résultat d'un ensemble cohérent de performances de tous les éléments de réseaux.
Pour pouvoir évaluer les performances du réseau, il faut connaitre plusieurs notions fondamentales. C'est l'essence même de ce chapitre.

2.2 Concepts de trafics

2.2.1 Définitions

- Le trafic d'un réseau correspond au volume d'informations transportées ou traitées par ce réseau. Il pourra s'agir de données relatives aux échanges d'informations entre usagers (voix, images, e-mails, fichiers...), mais aussi des données relatives aux échanges d'informations entre machines de commande du réseau (données de signalisation dans un réseau de circuits, informations de routage dans un réseau IP, données d'exploitation…). Plus les échanges entre usagers ou machines sont fréquents et de longues durées, plus les ressources nécessaires à l'écoulement de ce trafic seront importantes.
- On appelle intensité de trafic le nombre moyen N de communications en cours simultanément. Elle est exprimée en Erlang, notée E. La loi d'Erlang (dans le cas d'arrivées « poissoniennes » des trafics) est traduite par la définition suivante : *un ensemble de ressources identiques est dit écouler, à un instant donné, un trafic de N erlangs lorsque N de ses unités sont occupées.*
  Ainsi, soit A, le trafic en erlangs et, si on désigne par n(t) le nombre de ressources occupées, on a pour une période d'observation T :

$$A = \frac{1}{T}\int_0^T n(t)dt \qquad (2.01)$$

Plus concrètement, si on suppose un nombre de ressources suffisant pour écouler toutes les demandes présentées, et qu'on appelle λ le nombre moyen, constant, de demandes par unité de temps, et t_m la durée moyenne d'occupation de la ressource par chaque demande, on a :

$$A = \lambda \mathrm{t_m} \qquad (2.02)$$

A ces formules suit la formule de perte d'Erlang qui donne la probabilité de rejet (B) d'une nouvelle demande, du fait de manque de ressources, pour un trafic A offert à N ressources :

$$\mathrm{E(N,A)} = \mathrm{B} = \frac{\frac{\mathrm{A^N}}{N!}}{\sum_{j=0}^{N}\frac{A^j}{j!}} \qquad (2.03)$$

Le trafic écoulé est A_e :

$$A_e = A(1-B) \qquad (2.04)$$

Cette formule exprime donc aussi la capacité du système considéré à écouler le trafic qui lui est offert.

2.2.2 Trafic offert, trafic écoulé

Notre étude de performance est basée sur une distinction fondamentale entre la notion de trafic offert et la notion de trafic écoulé. En effet, le but d'un réseau est d'écouler si possible la totalité du trafic offert, et ce dans les meilleures conditions possibles (délai de réponse, délai de transmission très faibles par exemple). En réalité, il ne sera pas toujours possible d'accepter toutes les demandes. Dans certaines conditions de charges anormalement trop élevées (à l'occasion d'une catastrophe par exemple) ou surcharge, les systèmes devront rejeter les demandes, ne serait-ce que pour se protéger. Mais aussi, sans atteindre ces situations extrêmes, il va de soi qu'à cause de la nature aléatoire du trafic offert (le niveau de la demande varie aléatoirement) et du souci d'optimisation des ressources, il existera toujours une probabilité non nulle d'un manque de ressources et donc de rejet de la demande. Le trafic écoulé sera donc généralement différent du trafic offert.

2.2.3 Profil de charge, charge A et charge B

Au cours d'une journée, les demandes peuvent disparaître à certains moments puis réapparaître, avec d'ailleurs des niveaux de charge différents (par exemple le trafic d'usagers professionnels dans la journée et d'usagers résidentiels le soir...). On parlera d'heures chargées et d'heures creuses qui peuvent ne pas être les mêmes pour différents réseaux et même pour différentes parties d'un même réseau (fuseaux horaires différents, types de services supportés différents). On parlera de profil de charge pour un réseau ou une partie d'un réseau.

Le réseau doit donc répondre correctement à ces différentes sollicitations. C'est à cet effet que l'on distingue le niveau de charge A et le niveau de charge B.

Le niveau de charge A correspond aux situations les plus fréquentes et la qualité de service perçue par l'usager doit être la meilleure. La situation de charge B correspond quant à elle à des situations rares mais cependant prévisibles pour lesquelles la qualité de service peut être moins bonne tout en restant acceptable par l'usager.

2.3 Qualité de service

2.3.1 Définition

La QoS (Quality of Service) ou Qualité de service est définie dans la recommandation E-800 de l'UIT par un effet global produit par la qualité de fonctionnement d'un service qui détermine le degré de satisfaction de l'usager d'un service.

La QoS désigne donc la capacité d'un réseau à fournir un service dans une condition satisfaisante. C'est un concept de gestion qui permet de garantir de bonnes performances aux applications critiques et qui a pour but d'optimiser les ressources d'un réseau.

2.3.2 QoS en réseau d'entreprise

Un réseau d'entreprise, est partagé par plusieurs applications en même temps. La QoS intervient alors pour que ces applications puissent cohabiter au sein du réseau et fonctionner de manière optimale.

Une autre définition énonce aussi que la qualité de service désigne la capacité d'un réseau à fournir un service préférentiel au trafic réseau sélectionné. L'objectif premier de la QoS est de fournir une priorité, y compris une bande passante dédiée, un contrôle de la gigue et de la latence, ainsi qu'une réduction de la perte de paquets. [15]

Les utilisateurs perçoivent la qualité de service en fonction de deux critères :

- la vitesse à laquelle le réseau réagit à leurs requêtes ;
- la disponibilité des applications qu'ils souhaitent utiliser.

Dans un réseau sans QoS, tous les paquets reçoivent le même traitement et les applications temps réel s'en ressentent. En effet, certaines applications sont extrêmement sensibles aux besoins en matière de bande passante, aux retards de paquets, à la gigue du réseau et à la perte éventuelle de paquets, notamment la téléphonie sur IP en temps réel et la lecture vidéo en continu.

La QoS ne crée pas réellement plus de bande passante. Elle définit plutôt les priorités d'utilisation de la bande passante pour la prise en charge des applications, telles que la téléphonie sur IP, qui en ont le plus besoin.

Un des mécanismes le plus connu de la stratégie de QoS est la mise en file d'attente.

Pour ce faire, il faut classer les paquets puis leur fournir une priorité de QoS. Pour la mise en files d'attente par priorité, on distingue alors des priorités de trafic élevées, moyennes, normales et basses. Ainsi, le trafic (tel que le trafic vocal) situé dans les files d'attente prioritaires est envoyé avant le trafic de moindre priorité. [15]

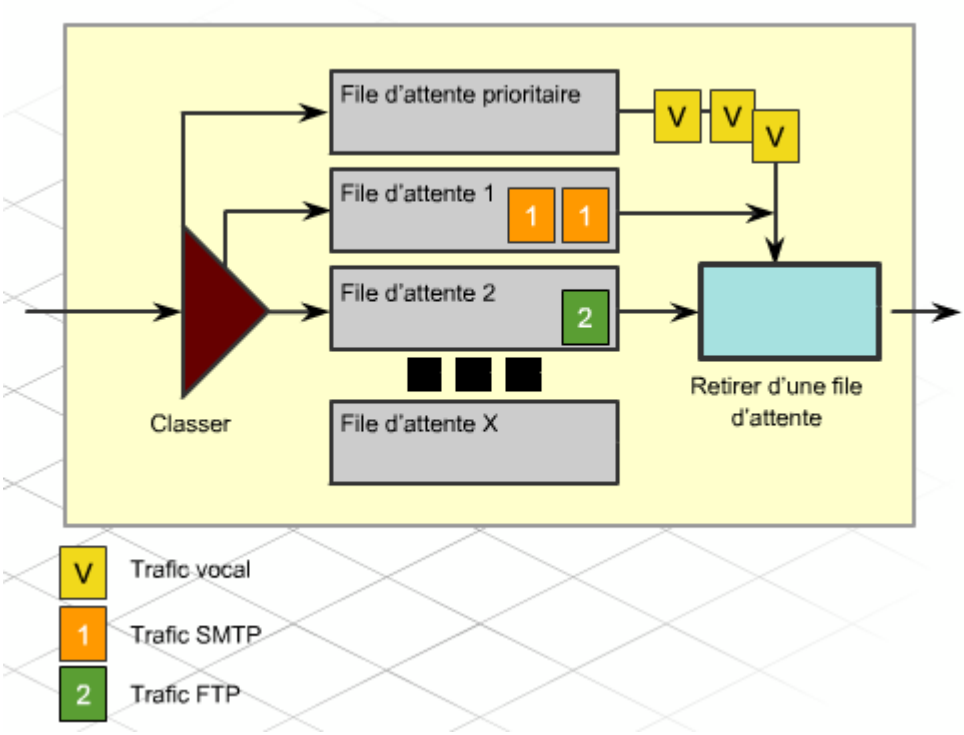


Figure 2.01 : *Exemple de mécanisme de files d'attente*

2.4 Indicateurs de performances KPI

Les KPI, pour Key Performance Indicators, ou indicateurs clés de performance, sont utilisés pour déterminer les facteurs pris en compte pour évaluer l'efficacité d'un réseau. Ces indicateurs permettent donc de mesurer l'efficacité de certains paramètres et servent pour le diagnostic et la supervision de réseau.

Il existe plusieurs indicateurs de performances pour le réseau d'entreprise, dont les cinq majeurs sont la bande passante, la latence, la gigue, le débit et la perte de paquets. [16]

2.4.1 La bande passante

La bande passante est le volume maximal de données pouvant transiter sur un chemin de communication au cours d'une période donnée. Elle est exprimée en bits/s (Kbits/s, Mbits/s).

Cette valeur reste cependant théorique à cause de différents facteurs (les unités d'interconnexions de réseaux ; les autres utilisateurs utilisant le réseau, leur nombre, leurs ordinateurs, le type de données transmises…)

2.4.2 La latence du réseau (Latency)

C'est le temps nécessaire pour véhiculer un paquet au travers d'un réseau (entre l'émission et la réception).

La latence peut être mesurée de plusieurs façons : aller- retour (ou Round Trip Time RTT), unilatérale (One way). Elle est exprimée en seconde (s, ms, µs, …).

La latence est impactée par tout élément dans la chaîne utilisée pour transporter les données : station cliente, liens WAN, routeurs, réseau local LAN, serveurs ; et pour les très grands réseaux, elle est limitée par la vitesse de la lumière.

$$\text{Latence} = T_T + T_P + T_A \tag{2.05}$$

Avec T_T la durée de transmission

T_P le temps de propagation

T_A le temps d'attente

- Durée de transmission : c'est le temps nécessaire pour transmettre les données (les envoyer sur le réseau)

$$T_T = \frac{TailleMessage}{Débit} \tag{2.06}$$

- Temps de propagation : c'est le temps nécessaire pour que les données aillent de l'émetteur au récepteur

$$T_P = \frac{d}{V_P} \tag{2.07}$$

Avec d la distance entre l'émetteur et le récepteur et V_P la vitesse de propagation

- Temps d'attente : c'est le temps "perdu" par le système de communication (notamment à cause de l'occupation des ressources)
- Latence de base : c'est un délai incompressible correspondant au temps écoulé avant de recevoir le premier bit d'un message

$$\text{Latence de Base} = T_P + T_A \tag{2.08}$$

On peut aussi la mesurer à l'aide de la commande ping.

2.4.3 La gigue (Jitter)

C'est la variation de la latence. Les paquets arrivent de manière irrégulière en fonction du trafic réseau. Elle est donc déterminante dans le cas des services en temps réel tels que la VoIP, plus la gigue augmente plus la conversation devient hachée.

2.4.4 Le débit réseau (Throughput)

C'est la quantité de données réellement envoyées et reçues par unité de temps. Il définit le taux de transfert des données obtenu en combinant les effets de bande passante et de latence.
Pour simplifier, disons que la bande passante est ce que nous payons et le débit est ce dont nous disposons réellement. Il est exprimé en bits/s (Kbits/s, Mbits/s…).

2.4.5 La perte de paquets

Il s'agit du nombre de paquets perdus par rapport à 100 paquets émis par un hôte sur le réseau. Elle correspond donc au taux de perte qui oblige à la retransmission des données affectant considérablement la qualité du lien réseau.

Par ailleurs, il existe d'autres facteurs qui peuvent affecter les performances du réseau :

- Utilisation : L'utilisation est le pourcentage de durée occupé par le câble et comprend une retransmission réussie en échec de la trame (collisions et erreurs). Le terme câble occupé

peut également être utilisé. En règle générale, la durée d'inactivité et l'utilisation donnent 100 %

- Instabilité : L'instabilité correspond aux retards variables sur un réseau.
- Jabotage : Le jabotage est un flux continu de données aléatoires transmises sur un réseau en raison d'un dysfonctionnement.
- Goulot d'étranglement : Un goulot d'étranglement est un retard survenant lorsqu'une partie d'un réseau est plus lente que les autres et entrave donc le débit général.
- Collisions : Les collisions sont des trames dont l'envoi a échoué sur un support partagé car les expéditeurs ont tenté d'envoyer plusieurs trames simultanément.

2.4.6 Valeurs des indicateurs de performances

Le tableau suivant donne les valeurs à respecter pour considérer un réseau de qualité :

Réseau	**Perte de paquets**	**Latence**	**Gigue**
Sur un réseau local	< 0.5 %	< 10 ms	< 5 ms
Sur un réseau WAN	< 1 %	< 40 ms	< 10 ms
Internet ou VPN sur Internet	< 2 %	< 100 ms	< 30 ms

Tableau 2.01: *Valeurs des indicateurs de performance*

2.5 Impact du routage IP sur la performance réseau

Le routage IP constitue l'un des aspects fondamentaux d'un réseau. En effet, pour assurer la fiabilité de la communication grâce à ses multiples interconnexions, le réseau nécessite des capacités de routage dynamique pour contourner les pannes et les encombrements. Ainsi, il influe considérablement au bon fonctionnement du réseau.

Dans cette partie, nous allons étudier les différents algorithmes utilisés par les protocoles de routage permettant de déterminer le plus court chemin lors de la commutation des paquets vers la destination.

2.5.1 Concepts de graphes valués

Un graphe (orienté ou non) G = (S, A) est valué si il est muni d'une application v qui sera appelée valuation :

$$\begin{aligned} v : A &\rightarrow R \\ (x, y) &\rightarrow v\,(x, y) \end{aligned} \qquad (2.09)$$

On peut étendre la valuation en une fonction $S \times S \rightarrow R \cup \{+\infty\}$ en posant $v(x, y) = +\infty$ si $(x, y) \notin A$.

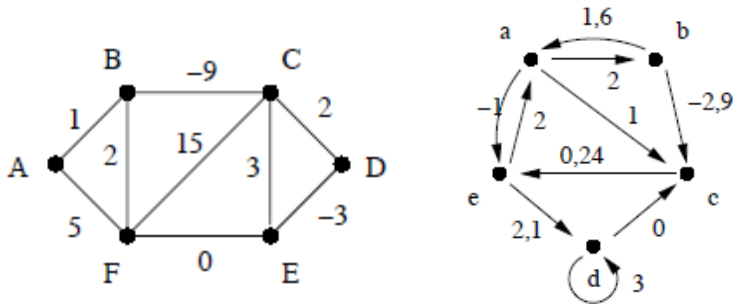
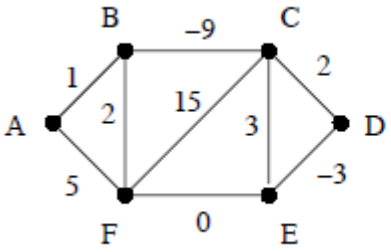


Figure 2.02 : *Exemples de graphes non orienté et orienté valués*

On peut représenter un graphe valué par une matrice carrée, dont les coefficients correspondent à la valuation des arcs.

Soit G = (S, A, v) un graphe valué dont on a numéroté les sommets de 1 à n. La matrice de valuation de G est la matrice carrée $M = (m_{ij})$, de taille $n \times n$, définie par :

$$m_{ij} = \begin{cases} v(I, j) & \text{si } (I, j) \in A \\ +\infty & \text{sinon} \end{cases} \qquad (2.10)$$



$$\begin{pmatrix} \infty & 1 & \infty & \infty & \infty & 5 \\ 1 & \infty & -9 & \infty & \infty & 2 \\ \infty & -9 & \infty & 2 & 3 & 15 \\ \infty & \infty & 2 & \infty & -3 & \infty \\ \infty & \infty & 3 & -3 & \infty & 0 \\ 5 & 2 & 15 & \infty & 0 & \infty \end{pmatrix}$$

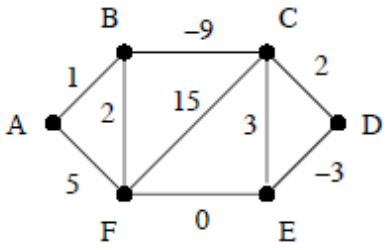
Figure 2.03 : *Exemple de représentation matricielle*

2.5.1.1 Valuation d'un chemin

Soit G = (S, A, v) un graphe valué. La valuation ou longueur d'un chemin (ou d'une chaîne) est la somme des valuations de chacun des arcs qui le composent.

La valuation d'un chemin ne comportant pas d'arcs est égale à 0. [17]

Prenons alors un exemple.



La valuation de la chaîne (A, F, C, E, D) est 5 + 15 + 3 – 3 = 20

2.5.1.2 Distance et plus court chemin

Soit G = (S, A, v) un graphe valué et soient x, y deux sommets de G.

- On appelle distance de x à y notée d(x, y) le minimum des valuations des chemins ou chaînes allant de x à y.
- On appelle plus court chemin ou plus courte chaîne de x à y tout chemin ou chaîne dont la valuation est égale à d(x, y).

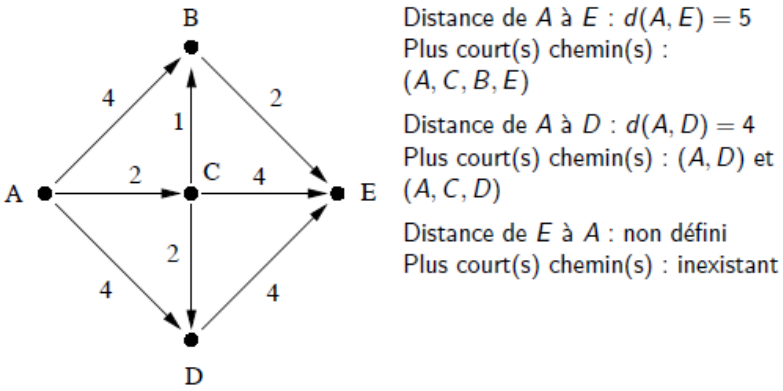


Figure 2.04 : *Exemple illustrant la distance et le plus court chemin*

Ces notions nous amènent alors à modéliser le routage dans les réseaux de télécommunication comme des recherches de plus courts chemins dans des graphes valués.

Nous avons les correspondances suivantes :

Graphe	Réseau de communication
Sommets	Routeurs
Arcs	Lignes de communication
Longueurs	Délais

Tableau 2.02: *Correspondance entre graphe et réseau*

On étudiera principalement donc des algorithmes qui résolvent le problème suivant : étant donné un sommet x, déterminer pour chaque sommet y la distance et un plus court chemin de x à y.

2.5.1.3 Circuit absorbant

Un circuit absorbant est un circuit de valuation négative. Si un graphe possède un circuit absorbant, alors il n'existe pas de plus courts chemins entre certains de ces sommets.
On définit de la même manière un cycle absorbant dans un graphe non orienté. Le théorème reste vrai en remplaçant chemin par chaine.
Pour la suite, on considère donc que le graphe ne possède pas de circuits absorbants.

2.5.1.4 Principe des algorithmes dans le cas général

Etant données un graphe valué G = (S, A, v) et un sommet x_0, on veut déterminer, pour chaque sommet s, la distance et un plus court chemin de x_0 à s.
Les algorithmes de recherche de distance et de plus court chemin dans un graphe valué fonctionnent de la façon suivante :

- On calcule les distances d (x_0, s) par approximations successives. A un stade donné de l'algorithme on dispose d'estimations d(s) (éventuellement égales à $+\infty$) pour ces distances, et de la donnée d'un prédécesseur P(s) pour les plus courts chemins.
- A chaque étape, on considère un sommet x et un successeur y de x. On compare la valeur d(y) à celle que l'on obtiendrait en passant par x, c'est-à-dire d(x) + v(x, y).
- Si cette deuxième valeur est plus petite que d(y), on remplace l'estimation d(y) par : d(x) + v(x, y) et le père P(y) par x. [17]

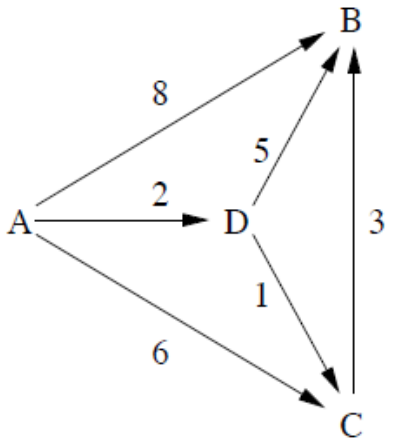
2.5.2 Algorithme de Bellman-Ford

On applique le principe précédent en explorant systématiquement tous les sommets et tous leurs successeurs. On s'arrête quand les valeurs des distances sont stabilisées.

Initialisation :
$d(x_0) = 0,\ P(x_0) = nul$
pour tout $s \in S,\ s \neq x_0$ **répéter**
    $d(s) = +\infty,\ P(s) = nul$
$fin = FAUX$

tant que $fin = FAUX$ **répéter**
    $fin \leftarrow VRAI$
    pour tout $x \in S$ **répéter**
        pour tout $y \in G(x)$ **répéter**
            si $d(x) + v(x, y) < d(y)$ **alors**
                $d(y) \leftarrow d(x) + v(x, y)$ (màj distance)
                $P(y) \leftarrow x$ (màj père)
                $fin \leftarrow FAUX$ (pas encore stabilisé)
fin tant que

Figure 2.05 : *Algorithme de Bellman-Ford*



Itération	$d(A)$	$d(B)$	$d(C)$	$d(D)$	$P(A)$	$P(B)$	$P(C)$	$P(D$
Initialisation	0	$+\infty$	$+\infty$	$+\infty$	nul	nul	nul	nul
1	0	7	3	2	nul	D	D	A
2	0	6	3	2	nul	C	D	A
3	0	6	3	2	nul	C	D	A

Figure 2.06 : *Exemple d'application de l'algorithme de Bellman-Ford*

L'algorithme se termine (les valeurs se stabilisent) après, au plus, n passages dans la boucle principale avec n étant le nombre de sommets du graphe

Les valeurs d(s) obtenues à la fin de l'algorithme sont bien les distances de x_0 aux sommets s. Pour trouver un plus court chemin entre x_0 et s, on se sert du tableau des pères. On construit le chemin à partir de la fin : on part de s, le tableau des pères donne son prédécesseur p le long d'un plus court chemin, et on recommence avec p.

En considérant l'exemple précédent on a :

$P(A)$	$P(B)$	$P(C)$	$P(D)$
nul	C	D	A

Un plus court chemin de A à B est
A→D→C→B

2.5.3 Algorithme de Dijkstra

L'algorithme de Dijkstra est un autre algorithme de recherche de distance et de plus court chemin. Il est plus efficace que Bellman-Ford, mais ne fonctionne que dans le cas où toutes les valuations des arcs sont positives.

Son principe est le suivant :

- On construit petit à petit, à partir de $\{x_0\}$, un ensemble M de sommets marqués. Pour tout sommet marqué s, l'estimation d(s) est égale à la distance d (x_0, s).
- A chaque étape, on sélectionne le sommet non marqué x dont la distance estimée d(x) est la plus petite parmi tous les sommets non marqué.
- On marque alors x (on rajoute x à M), puis on met à jour à partir de x les distances estimées des successeurs non marqués de x.
- On recommence, jusqu'à épuisement des sommets non marqués.

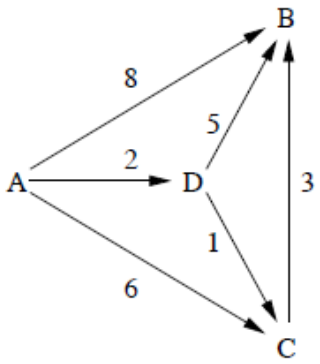
L'algorithme de Dijkstra est plus performant que Bellman-Ford : il est donc à privilégier systématiquement.

Par contre on ne peut pas l'appliquer dès qu'on a des valuations négatives (ou assimilées)

Initialisation
$d(x_0) = 0$, $P(x_0) = nul$
aucun sommet n'est marqué
$min\_dist\_M = 0$ (minimum des distances estimées des sommets non marqués)
pour tout $s \in S$, $s \neq x_0$ **répéter**
    $d(s) = +\infty$, $P(s) = nul$

répéter
    chercher x non marqué tel que $d(x) = min\_dist\_M$
    marquer x
    pour tout $y \in G(x)$, y non marqué **répéter**
        si $d(x) + v(x,y) < d(y)$ **alors**
            $d(y) \leftarrow d(x) + v(x,y)$ (màj distance)
            $P(y) \leftarrow x$ (màj père)
    $min\_dist\_M = \min\{d(s),\ s \notin M\}$
jusqu'à ce que $min\_dist\_M = +\infty$

Figure 2.07 : *Algorithme de Dijkstra*



M	$d(A)$	$d(B)$	$d(C)$	$d(D)$	$P(A)$	$P(B)$	$P(C)$	$P(D$
$\emptyset$	0	$+\infty$	$+\infty$	$+\infty$	nul	nul	nul	nul
$\{A\}$		8	6	2		A	A	A
$\{A, D\}$		7	3			D	D	
$\{A, D, C\}$		6				C		
$\{A, D, C, B\}$	0	6	3	2	nul	C	D	A

Figure 2.08 : *Exemple d'application de l'algorithme de Dijkstra*

Quand on connaît les distances de x_0 à s pour tout sommet s, on peut déterminer (tous) les plus courts chemins de x_0 à s pour tout sommet s. Si on dispose du tableau des pères, il est facile de trouver un plus court chemin :

s	A	B	C	D
$d(A, s)$	0	6	3	2

Un plus court chemin de A à B est :
$A \rightarrow D \rightarrow C \rightarrow$B

2.5.4 Les protocoles de routage dynamique

Bien que l'idée d'une route statique est séduisante par sa facilité de mise en œuvre, elle est devient fastidieuse pour l'administrateur réseau pour l'organisation de grands réseaux où le nombre de routeurs est considérable.

La présence de plusieurs routes possibles pour rejoindre une destination implique de facto l'usage d'un protocole de routage dynamique et l'existence de ces plusieurs routes est une nécessité pour assurer la redondance du service, voire même l'équilibrage du trafic sur plusieurs liens.

Les protocoles de routage permettent donc aux routeurs de gérer et de mettre à jour automatiquement leurs tables de routage. [18]

Si plusieurs chemins existent pour atteindre une destination précise, ils choisissent le plus optimal tout en mettant en réserve un autre meilleur chemin en cas d'indisponibilité du premier.

Il existe deux familles de protocoles de routage dynamique :

- L'IGP ou Interior Gateway Protocol
- L'EGP ou Exterior Gateway Protocol

L'IGP permet d'acheminer les données à l'intérieur d'un système autonome tandis que l'EGP permet de router les données entre différents systèmes autonomes contrôlés par des administrateurs différents. Un système autonome est un ensemble de réseaux gérés par un administrateur commun et qui suit les même règles de routage, c'est-à-dire qu'il y a partage d'une stratégie de routage commune.

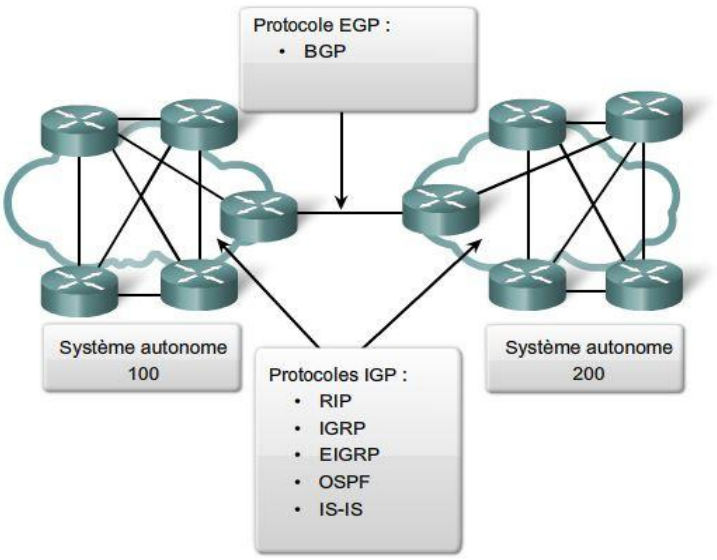


Figure 2.09 : *IGP et EGP*

Les protocoles de routage intérieurs IGP sont classés, selon l'algorithme utilisé, en protocole à vecteur de distance et en protocole à état de lien (ou à état de liaison).

2.5.4.1 Algorithme à vecteur de distances

Les algorithmes de routage à vecteur de distances se basent sur l'algorithme de Bellman-Ford. Ils conduisent les routeurs à transmettre à leurs voisins réseaux immédiats une copie de leur table de routage. Ces tables se modifient au fur et à mesure de leur propagation car chaque route est associée à une métrique qui croît par défaut d'une unité au passage de chaque routeur. La mise à jour se fait donc de manière périodique.

Le terme vecteur de distances est employé parce que la propagation des routes s'effectue sous la forme de vecteurs : " Pour atteindre telle destination, il faut passer par ce routeur et la métrique associée vaut cette valeur " ; donc une direction et une métrique, d'où l'analogie avec un vecteur.

Le choix de la meilleure route est établi par chaque routeur en considérant la valeur minimale de cette métrique pour toutes les routes qui aboutissent à la même destination. Seule la meilleure route est propagée, les autres sont oubliées. Pour ces considérations on dit que le calcul de la route est distribué et par conséquence chaque routeur n'a pas la connaissance de la topologie globale du réseau : il n'en connait qu'une version interprétée par ses voisins.

Les protocoles à vecteur de distance sont les protocoles RIP, IGRP, EIGRP

- RIP

  La métrique utilisée pour déterminer le meilleur chemin est le nombre de sauts, c'est-à-dire le nombre de routeurs que le paquet doit traverser avant d'arriver à la destination finale. Le nombre de sauts maximal avant que le paquet soit éliminer est 15. Les mises à jour de routage se font tous les 30 secondes. Il existe deux versions de RIP : le RIPv1 et RIPv2.

RIPv1	**RIPv2**
Facile à configurer	
Utilisation de protocole de routage par classe (classful)	Utilisation de protocole de routage CIDR (classless)
Les mises à jour se font par broadcast	Les mises à jour se font par multicast sur 224.0.0.9
Aucune information sur les sous-réseaux dans la mise à jour	Masques de sous-réseaux envoyés avec la mise à jour

RIPv1	RIPv2
Aucune authentification	Authentification des voisins dans les mises à jour
Utilisation d'un même masque de sous-réseau	Support du VLSM

Tableau 2.03: *RIPv1 et RIPv2*

Malgré ses avantages, RIP présente un temps de convergence lent et l'utilisation du nombre de sauts comme métrique n'est pas très efficace pour choisir le meilleur chemin ; de plus ce nombre de sauts est limité à 15.

- IGRP et EIGRP

  L'IGRP (Interior Gateway Routing Protocol) et EIGRP (Enhanced IGRP) sont des protocoles de routage à vecteur de distance développés par Cisco. EIGRP est une version améliorée d'IGRP mais les deux protocoles sont compatibles.

	IGRP	EIGRP
Classe de Protocole	A vecteur de distance	A vecteur de distance mais à état de lien lors de la mise à jour
Nombre maximum de sauts	255	224
Métriques utilisées	Bande passante, fiabilité, délai, charge ; 24bits	Métriques composites ; 32 bits
Mise à jour	Toutes les 90s de façon multicast	Lors modification du réseau de façon multicast
Distance administrative	100	90
Bande passante	Consommation de la bande passante	Moins de bande passante utilisée
Spécificités		Support du CIDR et VLSM
		Découverte des voisins

Tableau 2.04: *IGRP et EIGRP*

2.5.4.2 Algorithme à états de liens

Les algorithmes à états de liens bâtissent les tables de routages différemment. Chaque routeur est responsable de la reconnaissance de tous ses voisins, plus ou moins lointains, à qui il envoie une liste complète des noms et des coûts (en termes de bande passante, par défaut) contenu dans une base de données à sa charge et qui représente l'intégralité de tous les routeurs du nuage avec lesquels il doit travailler.

Chaque routeur a donc une connaissance exhaustive de la topologie du " nuage " dans lequel il se situe et c'est à partir de cette représentation qu'il calcule ses routes à l'aide d'un algorithme connu de recherche du plus court chemin dans un graphe : celui de Dijkstra. Sa réponse est plus rapide car la mise à jour se fait seulement en cas de modification du réseau.

- OSPF (Open Shortest Path First)

  Le protocole de routage à états liens le plus répandu est l'OSPF ou Open Shortest Path First. Il permet la connaissance exacte de la topologie du réseau avec découverte des voisins. La métrique utilisée pour la sélection de la meilleure route est la bande passante des liaisons. Plus la bande passante est grande plus le chemin est optimal. La mise à jour de routage ne se fait qu'à chaque modification topologique du réseau à partir d'une adresse multicast diminuant ainsi l'utilisation de la bande passante. C'est aussi un protocole de routage classless supportant le VLSM dont le domaine est dépourvu de boucle de routage.

- Valeur des états de liens

  Le coût des liens, nommé également la métrique, agit directement sur le choix d'une route plutôt qu'une autre. Le constructeur Cisco préconise une formule qui est reprise partout :

$$cost = \frac{100000000}{bande\ passante\ en\ bits/s} \tag{2.11}$$

Média	**Coût**
Liaison série 56 Kbits/s	1785
T1 (série 1544 Kbits/s)	64
E1 (série 2048 Kbits/s)	48
Token Ring 4 Mbits/s	25
Ethernet 10 Mbits/s	10
Token Ring 16 Mbits/s	6
Ethernet 100 Mbits/s	1

Tableau 2.05: *Valeur du coût pour des débits connus*

2.6 Conclusion

Ce chapitre nous a permis d'étudier en profondeur les aspects d'un réseau d'entreprise pouvant nous amener à évaluer sa performance. Parmi ces aspects sont les concepts de trafics afin de les caractériser ; la notion de qualité de service QoS pour atteindre les exigences requises pour les différents services ; les indicateurs de performance ainsi que les facteurs pouvant affecter l'état du réseau ; les algorithmes utilisés par les protocoles de routages dynamique nous permettant de comprendre mieux leur fonctionnement au sein du réseau.

Dans le chapitre suivant, nous allons nous intéresser aux techniques d'optimisation d'un réseau d'entreprise afin d'augmenter au mieux sa capacité et sa performance.

CHAPITRE 3
TECHNIQUES D'OPTIMISATION DES RESEAUX INFORMATIQUES

3.1 Introduction

Dans ce chapitre, nous allons définir les besoins en termes de réseau puis définir les techniques d'optimisation qui permettent de satisfaire ces besoins tout en apportant des solutions aux divers problèmes affectant les performances d'un réseau d'entreprise. A chaque technique d'optimisation, nous allons voir les avantages qu'elle apporte.

3.2 Besoins en réseau

Après examen et analyse des exigences attendues par les réseaux d'entreprise, voici les principaux points nécessaires à prendre en compte :

- Extensibilité : qui permet au réseau d'accueillir de nouveaux groupes d'utilisateurs, de sites distants, et de prendre en charge de nouvelles applications sans affecter le niveau de service fourni aux utilisateurs existants.
- Disponibilité : le réseau doit être disponible à tout moment avec des performances stables et fiables même en cas de panne d'équipements ou de problème de liaisons.
- Sécurité : la conception de réseau doit inclure à l'avance sa sécurisation en assurant la planification de l'emplacement des dispositifs de sécurité, des filtres et des pare-feu pour la protection des ressources du réseau.
- Facilité de gestion : le personnel en charge du réseau doit être capable de le gérer pour son bon fonctionnement. [15]

Le réseau doit permettre, à tout moment, à l'entreprise d'accomplir sans problèmes ses fonctions et de satisfaire ses employés et ses clients via les différents services offerts. Ses performances doivent toujours répondre à leurs attentes.

3.3 Réseaux locaux virtuels ou VLAN

3.3.1 Domaine de diffusion

Un domaine de diffusion est une zone logique d'un réseau informatique dans lequel tous les hôtes reçoivent tout paquet en broadcast émis par l'un d'entre eux.

Comme un switch répète sur tous ses autres ports tout paquet broadcast qu'il reçoit d'un de ses ports, les hôtes interconnectés par un ou des switches appartiennent au même domaine de diffusion.

Plus le nombre de commutateurs connectés augmente, plus le domaine de diffusion augmente aussi. Les broadcasts sont utiles et essentiels pour le bon fonctionnement d'un réseau, mais dans un réseau de switches trop grand, les paquets en diffusion deviennent trop nombreux et ralentissent le réseau.

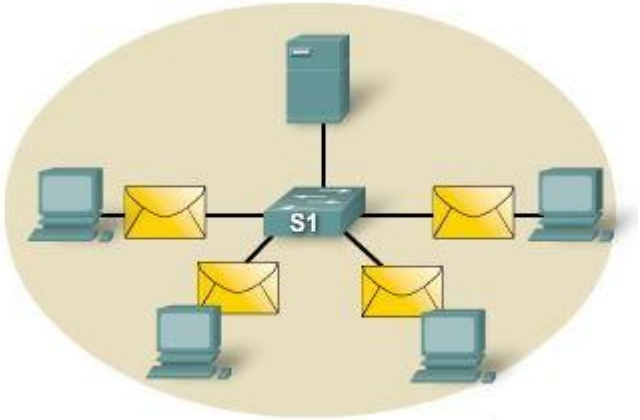


Figure 3.01 : *Domaine de diffusion*

C'est pourquoi on divise les grands réseaux en des réseaux plus petits, possédant chacun son propre domaine de diffusion. Les routeurs sont utilisés pour segmenter les domaines de collision et de diffusion. En effet, un routeur ne permet pas à un paquet en broadcast de passer d'un réseau à un autre.

Cependant, l'utilisation d'un routeur pour interconnecter des sous-réseaux présente lui aussi quelques inconvénients :

- Une augmentation de la lenteur des communications entre les sous-réseaux : là où le commutateur se contentait d'aiguiller la trame, le routeur doit traiter l'en-tête du paquet contenu dans la trame.
- Une gestion plus compliquée des adresses IP, à cause du découpage en plusieurs domaines DHCP, chacun ayant son propre serveur DHCP.
- Une flexibilité réduite : le découpage en sous-réseaux se fait en général sur un critère de proximité physique, qui ne correspond pas toujours aux découpages organisationnels et donc aux besoins de filtrage d'accès.

C'est là que la solution de réseaux locaux virtuels intervient afin de pallier ces problèmes.

3.3.2 Principe du VLAN

Un réseau local virtuel est un sous-réseau IP logique distinct. Les réseaux locaux virtuels permettent à plusieurs réseaux et sous-réseaux IP de coexister sur le même réseau commuté. Les ordinateurs appartenant à différents VLAN se trouvent donc sur différents sous-réseaux tout en partageant la même infrastructure.
Un broadcast envoyé par une machine d'un VLAN sera diffusé uniquement vers toutes les autres machines du même VLAN. [19] [20]

3.3.3 Avantages offerts par les VLANs

L'implémentation de la technologie VLAN permet à un réseau d'assurer une prise en charge plus souple des objectifs de l'entreprise. Les principaux avantages des VLAN sont les suivants :

- Sécurité : les groupes contenant des données sensibles sont séparés du reste du réseau, ce qui diminue les risques de violation de confidentialité.
- Réduction des coûts : des économies sont réalisées grâce à une diminution des mises à niveau onéreuses du réseau et à l'utilisation plus efficace de la bande passante et des liaisons ascendantes existantes.
- Meilleures performances : le fait de diviser des réseaux linéaires de couche 2 en plusieurs groupes de travail logiques (domaines de diffusion) réduit la quantité de trafic inutile sur le réseau et augmente les performances.
- Atténuation des tempêtes de diffusion : le fait de diviser un réseau en plusieurs réseaux VLAN réduit le nombre de périphériques susceptibles de participer à une tempête de diffusion. En effet, la segmentation d'un réseau LAN empêche une tempête de diffusion de se propager dans tout le réseau. Chaque VLAN correspond à un domaine de diffusion.
- Efficacité accrue du personnel informatique : les VLAN facilitent la gestion du réseau, car les utilisateurs ayant des besoins réseau similaires partagent le même VLAN. Lorsque vous configurez un nouveau commutateur, toutes les stratégies et procédures déjà configurées pour le VLAN correspondant sont implémentées lorsque les ports sont affectés. Le personnel informatique peut aussi identifier facilement la fonction d'un VLAN en lui donnant un nom approprié.
- Gestion simplifiée de projets ou d'applications : les VLAN rassemblent des utilisateurs et des périphériques réseau pour prendre en charge des impératifs commerciaux ou géographiques. La séparation des fonctions facilite la gestion d'un projet ou l'utilisation

d’une application spécialisée. Il est également plus facile de déterminer la portée des effets de la mise à niveau des services réseau.

3.4 Modèle de conception hiérarchique

Il existe deux structures de modèles de réseau : le modèle hiérarchique et le modèle maillé. [15]

Dans une structure maillée, la topologie du réseau est linéaire. Tous les routeurs remplissent essentiellement les mêmes fonctions et il n’existe généralement pas de définition précise des fonctions exécutées par chaque routeur. L’expansion du réseau s’effectue par hasard et de façon arbitraire.

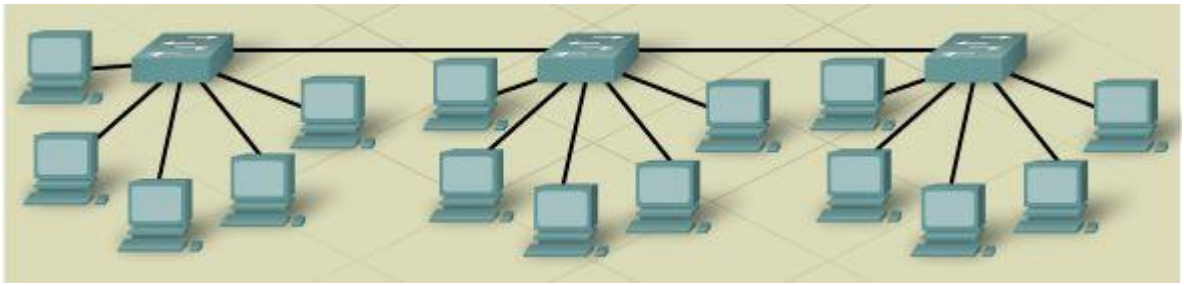


Figure 3.02 : *Réseau maillé*

Dans la structure hiérarchique, on regroupe les périphériques en un certain nombre de réseaux distincts qui sont organisés en couches. Une ou plusieurs fonctions précises sont associées à chaque couche. Le modèle de conception hiérarchique possède trois couches de base :

- Couche Cœur du réseau
- Couche de Distribution
- Couche d’Accès

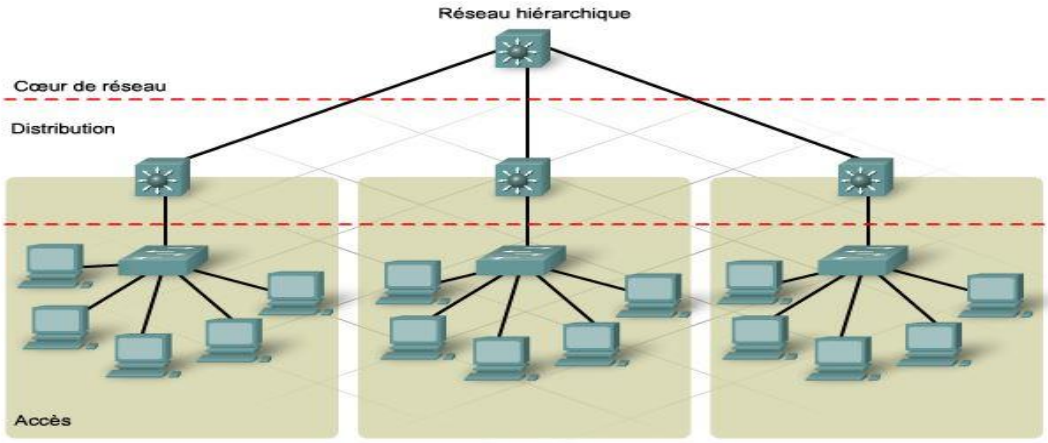


Figure 3.03 : *Réseau hiérarchique*

Cette architecture hiérarchique offre au réseau les avantages suivants :

- Evolutivité : possibilité d'une forte croissance du réseau sans effet négatif sur le contrôle et la facilité de gestion. En effet, les fonctionnalités sont localisées et il est plus facile de détecter les problèmes éventuels.
- Facilité de mis en œuvre : celle-ci est due à l'attribution des fonctionnalités précises à chaque couche.
- La facilité de dépannage : on peut isoler les problèmes qui peuvent survenir au réseau puisque ce dernier est modulaire ; il est aussi facile de segmenter temporairement le réseau pour réduire l'étendue du problème.
- La prévisibilité : on peut comprendre et prévoir le comportement d'un réseau utilisant des couches fonctionnelles ; la planification de la capacité de croissance du réseau et la modélisation de ses performances peuvent être simplifiées.
- La prise en charge des protocoles : l'organisation logique de l'infrastructure sous-jacente sur le réseau permet la facilité de combiner les applications et les protocoles actuels et futurs.
- La facilité de gestion

3.4.1 Couche d'accès

Cette couche est habituellement un LAN ou un groupe de LAN, de type Ethernet ou Token Ring, qui assure aux utilisateurs un accès de première ligne aux services réseau. C'est au niveau de cette couche que la plupart des hôtes, tels que tous les serveurs et les stations de travail des utilisateurs, sont reliés au réseau. Les services et les périphériques de cette couche sont situés dans chaque bâtiment de campus, dans chaque site distant et à la périphérie du réseau d'entreprise.

La topologie de la couche d'accès peut être en étoile ou à maillage globale. Elle utilise la technologie de commutation de couche 2. L'accès peut se faire à partir d'une infrastructure câblée permanente ou de points d'accès sans fil.

L'emplacement physique des équipements représente alors l'une des plus grandes préoccupations lors de la conception d'une couche d'accès.

3.4.2 Couche de distribution

La couche de distribution est une frontière de routage entre la couche d'accès et la couche cœur de réseau ; c'est aussi le point de connexion entre les sites distants et la couche cœur de réseau. Elle assure le filtrage (ACL ou Access Control List), la gestion de flux de trafic et le routage des VLAN ; elle permet aussi d'isoler la couche cœur de réseau par rapport aux pannes ou aux interruptions de service au niveau de la couche d'accès.

La couche de distribution est créée à partir des périphériques de couche 3 tels que les routeurs ou les commutateurs multicouches. Ces périphériques gèrent les files d'attente et la hiérarchisation du trafic avant la transmission vers la couche cœur. Ils présentent aussi des liaisons agrégées et redondantes pouvant être configurées pour un équilibrage de charge, augmentant ainsi la bande passante disponible pour les applications. Cette couche est câblée selon une topologie à maillage partielle tout comme la couche cœur de réseau.

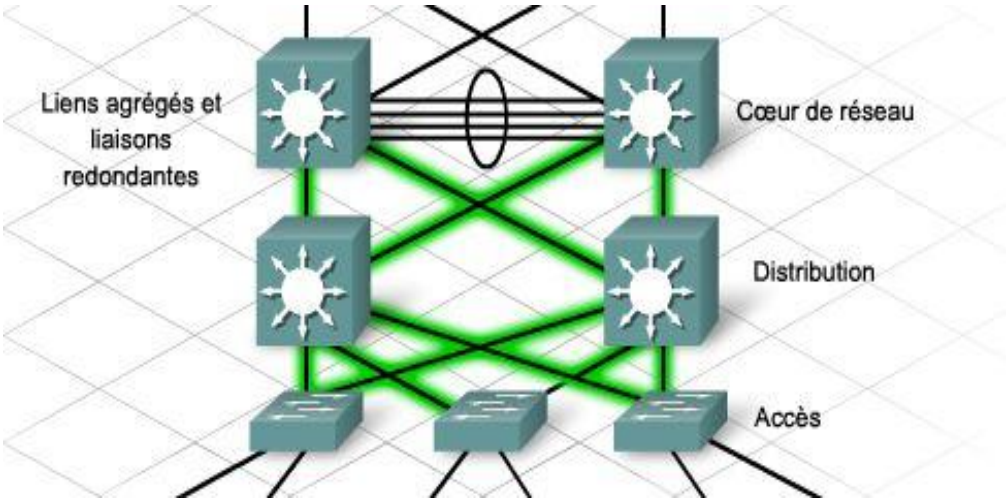


Figure 3.04 : *Topologie à maillage partielle*

3.4.3 Couche cœur

La couche cœur de réseau appelée aussi réseau fédérateur relie les périphériques de la couche distribution. Les routeurs et les commutateurs de cette couche offrent une connectivité haute vitesse. Elle contient une ou plusieurs liaisons vers les périphériques de la périphérie du réseau pour la prise

en charge de l'accès à Internet, aux réseaux privés virtuels (VPN), à l'extranet et aux réseaux étendus (WAN). Ainsi, on conçoit la couche cœur de réseau afin de transférer efficacement et rapidement des données entre deux sections de réseau ; faciliter la croissance du réseau et sa gestion. Toutefois, elle ne s'occupe pas du filtrage ou de la sécurité et une défaillance au niveau de cette couche entraine un problème de grande échelle au niveau du réseau global.

Les technologies utilisées au niveau de cette couche sont les routeurs ou commutateurs multicouches, la redondance pour la continuité de service en cas de panne, les liaisons de haute vitesse, les protocoles de routage tels qu'EIGRP et OSPF ayant des fonctionnalités importantes telles qu'une convergence rapide et le partage de charge.

3.5 Impacts de l'adressage sur la performance réseau

L'allocation d'adresses IP prend une place importante dans la prise en charge du réseau car elle permet :

- D'éviter les doublons d'adresses ;
- De fournir et contrôler l'accès ;
- De veiller à la sécurité et aux performances ;
- De prendre en charge une conception modulaire ;
- De prendre en charge une solution extensible utilisant l'agrégation de routes.

Il faut donc adopter un schéma d'adressage hiérarchique bien planifié afin d'assurer l'extensibilité du réseau (contrairement à l'adressage linéaire), de faciliter l'exécution du résumé de routage et de réduire le traitement du protocole de routage.

Le résumé de routage également connu sous le nom d'agrégation de routes s'agit du processus d'annonce d'un ensemble contigu d'adresses en tant qu'entrée unique avec un masque de sous-réseau ou un préfixe plus court et moins spécifique.

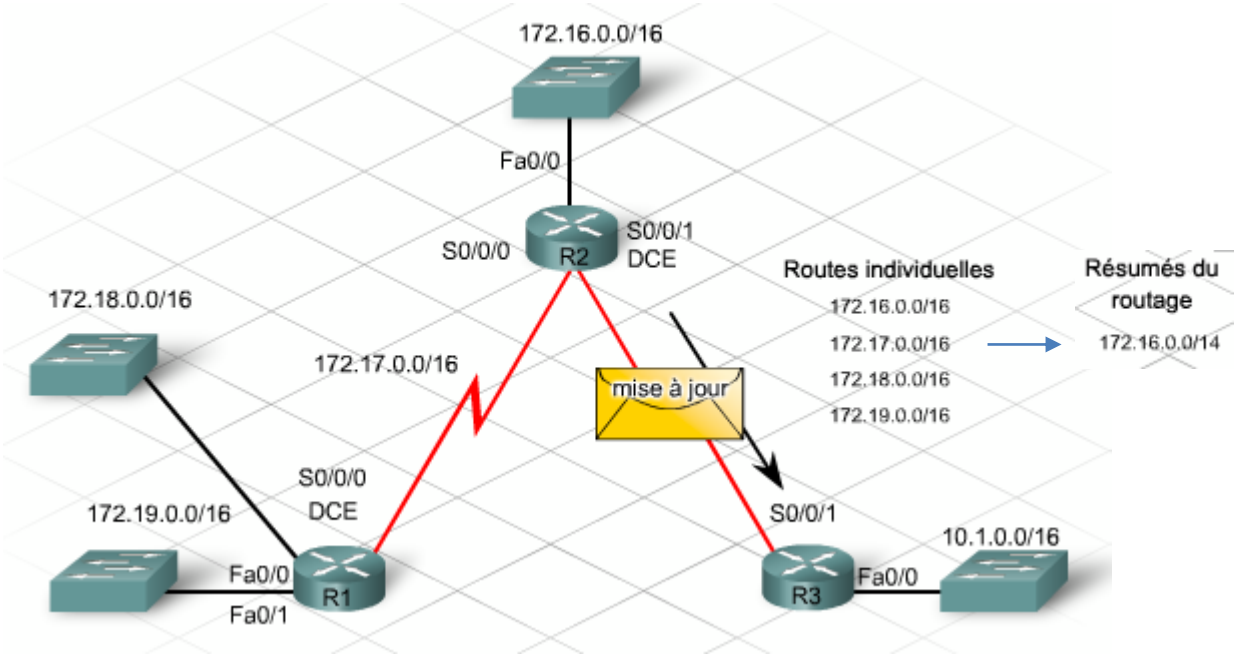


Figure 3.05 : *Exemple de résumé de routage*

Ce type de résumé permet de réduire le nombre d'entrées des mises à jour de routage et des tables de routage locales, ce qui accélère les recherches dans les tables de routage et réduit la quantité de bande passante utilisée lors des mises à jour de routage.

Une bonne planification de l'adressage IP consiste aussi à l'utilisation de la technique VLSM ou Masquage de sous-réseau de longueur variable. En effet, elle assure un meilleur usage de l'espace d'adressage IP. Elle permet également aux routeurs de résumer les routes par une route hors classes IP standard.

Lorsque la technique VLSM est utilisée dans un schéma d'adressage IP, on doit avoir recours à un protocole de routage prenant en charge le routage CIDR ou Routage inter-domaine sans classe. Les protocoles de routage sans classe envoient la longueur du préfixe avec les informations concernant la route dans les mises à jour de routage permettant aux routeurs de déterminer la partie réseau de l'adresse IP sans utiliser les masques par défaut.

L'utilisation de toutes ces techniques permet en d'autres termes d'améliorer la latence du réseau car elles réduisent les temps de traitements effectués au niveau du routeur.

3.6 Cisco Performance Routing

3.6.1 Problématique et objectif

Dans le domaine des réseaux d'entreprises, la tâche traditionnelle du routage était, et est toujours de fournir un accès entre des réseaux IP distants. Dans le monde d'aujourd'hui où le réseau n'est plus seulement un service de transfert de fichier, cette approche traditionnelle de routage ne semble plus être suffisante.

Comme le réseau est désormais convergent c'est-à-dire intégrant les données, la voix, la vidéo et autres services en temps réel, de nouvelles exigences sont requises dans le but de ne plus voir les trafics de données en de simples paquets allant d'une source vers une destination.

En effet, les protocoles de routage que nous avons vus dans le chapitre précédent utilisent des métriques afin de déterminer le chemin le plus court que les paquets doivent emprunter pour arriver à destination.

Cependant, les plus courts chemins définis par ces métriques ne sont pas toujours les meilleurs chemins qui assurent les qualités de services requises par les diverses applications. En d'autres termes, les protocoles de routages ne prennent pas en compte ni l'état du réseau ni les exigences en performances des paquets à acheminer.

Pour démontrer ceci, prenons alors le protocole EIGRP. [21]

Pour sélectionner le chemin préféré vers un réseau, EIGRP utilise les valeurs suivantes dans sa mesure composite : la bande passante, le délai, la fiabilité et la charge.

La formule de mesure composite utilisée par EIGRP est donnée par :

$$\text{Mesure} = 256 \times \left[\text{K1} \times \text{Bande Passante} + \frac{(\text{K2} \times \text{Bande Passante})}{(256 - Ch\arg e)} + (\text{K3} \times \text{Délai}) \right] \times \left[\frac{K5}{Fiabilité + K4} \right] \quad (3.01)$$

Avec K1 à K5 sont connus sous le nom de pondérations de mesure. Par défaut, K1 et K3 ont pour valeur 1, et K2, K4 et K5 ont pour valeur 0. Le résultat est donc que seules les valeurs de bande passante et de délai sont utilisées dans le calcul de la mesure composite par défaut. Ainsi la formule de mesure par défaut est donnée par :

$$\text{Mesure} = 256 \times [\text{K1} \times \text{Bande Passante} + \text{K3} \times \text{Délai}] \quad (3.02)$$

En remplaçant la valeur de K1 et K3, de Bande Passante et Délai on obtient la formule finale :

$$\text{Mesure} = 256 \times \left[\frac{10^7}{\min(BP)} + \sum \frac{Délais}{10} \right] \quad (3.03)$$

Où min (BP) correspond à la plus petite bande passante de liaison entre les hôtes source et destination et Σ Délais correspond à la somme des valeurs de délais de chaque interface de sortie de la route jusqu'à la destination. 10^7 correspond à une valeur de référence de bande passante.
Sur les routeurs, la bande passante est exprimée en Kbits (kilobits). La plupart des interfaces séries utilisent la valeur de bande passante par défaut de 1 544 Kbits ou 1 544 000 bits/s (1 544 Mbits/s). Il s'agit de la bande passante d'une connexion T1 ; les interfaces Ethernet sont de 10000Kbits et les interfaces FastEthernet de 100000 Kbits. La valeur de bande passante peut refléter ou non la bande passante physique réelle de l'interface. La modification de la valeur de bande passante ne change pas la bande passante réelle de la liaison.
La mesure de délai est une valeur statique déterminée à partir du type de liaison à laquelle l'interface est connectée et elle s'exprime en microsecondes. Le tableau suivant présente les valeurs de délai par défaut pour diverses interfaces.

Support	**Délai**
ATM 100 Mbits	100 µs
FastEthernet	100 µs
FDDI	100 µs
Token Ring 16 Mbits	630 µs
Ethernet	1000 µs
T1 (interface série par défaut)	20000 µs
512 Kbits	20000 µs
56 Kbits	20000 µs

Tableau 3.01: *Valeurs par défaut des délais des diverses interfaces*

Montrons alors que le protocole EIGRP ne prend pas en compte l'état du réseau et des liaisons dans son calcul du meilleur chemin. Prenons la topologie de réseau suivante :

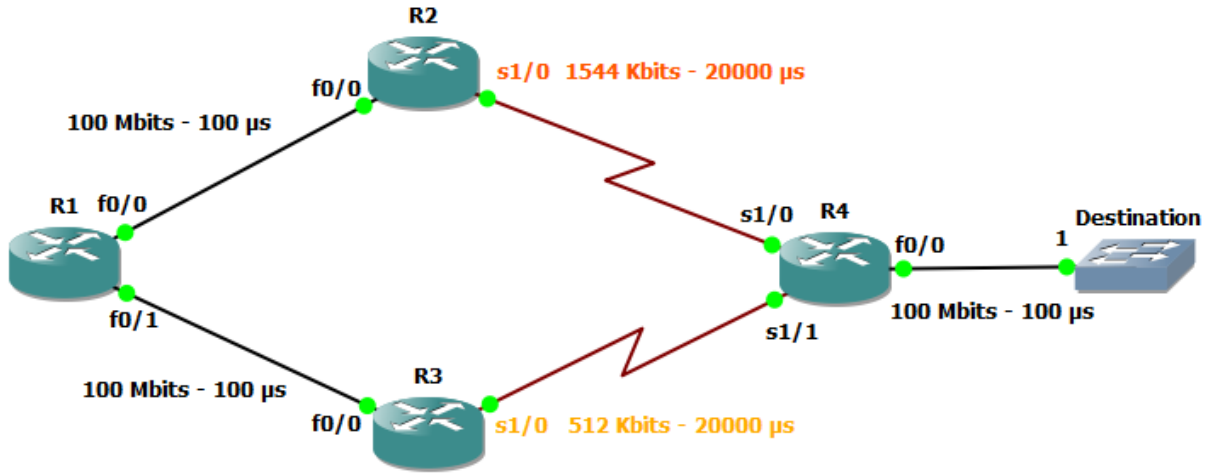


Figure 3.06 : *Topologie pour la démonstration*

Pour arriver à la destination depuis R1, le paquet peut emprunter le chemin soit vers R2 soit vers R3.

Empruntant R2, la métrique calculée par EIGRP est $M1 = 256 \times \left[\frac{10^7}{1544} + \sum \frac{100 + 20000 + 100}{10} \right]$

On obtient après arrondissement, M1=256 x (6476+2020) = 2174976.

Empruntant R3, la métrique calculée par EIGRP est $M2 = 256 \times \left[\frac{10^7}{512} + \sum \frac{100 + 20000 + 100}{10} \right]$

On obtient après arrondissement, M2=256 x (19531+2020) = 5517056.

Ainsi, EIGRP va choisir la plus petite valeur c'est-à-dire le chemin vers R2 pour aller à destination.

Cependant, supposons maintenant qu'à un moment donné l'interface série de R2 subit une latence de 30 ms. La valeur précédemment devient : $M1 = 256 \times \left[\frac{10^7}{1544} + \sum \frac{100 + 32000 + 100}{10} \right]$,

M1 = 2482176. Malgré le changement, EIGRP continue à choisir le chemin vers R2 pour aller à la destination. Or du point de vue de délai, c'est le chemin vers R3 (avec un délai de 20.2 ms) qui est le meilleur, pour une application telle que les sessions TELNET qui sont sensibles à la latence.

Ainsi, EIGRP n'arrive pas à prendre en compte les métriques de performance des applications lors de la sélection du meilleur chemin.

De nos jours, une profonde visibilité des communications de données est ainsi nécessaire : il faut distinguer les différents services l'un de l'autre. Une fois que cette visibilité est établie, le protocole de routage peut lire l'information et les différentes classes d'applications peuvent être traitées de

manières différentes en termes de qualité de service suivant leurs priorités; ce qui amène donc à les router sur des chemins différents.

L'ajout d'information sur les paramètres de qualité de service donne de l'avantage sur les décisions de routage.

Notre objectif est alors de fournir des décisions de routage basées dynamiquement sur le changement des paramètres de QoS au sein du réseau d'entreprise. Nous proposons ainsi la solution de Cisco Performance Routing en démontrant ses possibilités et ses capacités d'optimisation.

3.6.2 Généralité sur PfR

Cisco Performance Routing (PfR) précédemment connu sous le nom d'Optimized Edge Routing ou OER est la dernière technologie promue par Cisco qui peut travailler avec les routeurs existants et les protocoles de routage. Il fait des décisions intelligentes en insérant des routes dans la table de routage pour optimiser la performance du réseau. Ceci est fait pour satisfaire les exigences des applications des utilisateurs. [22]

Cisco PfR complète donc les techniques classiques de routage en ajoutant de l'intelligence pour sélectionner les meilleurs chemins possédant les exigences en performance des applications.

Pour opérer, PfR effectue deux mesures : il utilise Cisco IOS IP SLA (Internet Protocol Service Level Agreement) pour un monitoring actif et Cisco IOS NetFlow pour un monitoring passif. Cependant, aucune connaissance ni expérience préalable de IP SLA ou NetFlow n'est nécessaire car ils sont automatiquement pris en compte par PfR sans aucune configuration manuelle.

Cisco PfR selecte un chemin d'entrée ou de sortie en se basant sur les paramètres qui affectent la performance de l'application tels que l'accessibilité (« reachability »), la latence, le coût, la gigue et le MOS (Mean Opinion Score) ou Note d'opinion moyenne. Il peut réduire les coûts du réseau en facilitant un équilibrage de charge plus efficace et en améliorant la performance d'application sans moderniser les technologies WAN.

Comme vue d'ensemble, PfR est un IOS Cisco intégré qui permet de contrôler les flux de trafic IP et puis de définir des politiques et des règles basés sur la classe de performance du trafic, sur la distribution de charge des liaisons, sur la bande passante des liaisons, sur le type de trafic. PfR permet des systèmes de monitoring actif et passif, une détection dynamique de panne et une correction automatique de chemin.

3.6.2.1 NetFlow

NetFlow est une fonctionnalité des appareils Cisco permettant d'analyser les flux Ipv4 ou Ipv6 traversant l'appareil par les ports configurés pour recueillir les statistiques NetFlow. [23]

Un flux est une séquence unidirectionnelle de paquets partageant des attributs communs tels qu'une adresse IP Source, une adresse IP de destination, la version du protocole IP (v4 ou v6), un port source (UDP ou TCP) et un port destination (UDP ou TCP) ; le TOS (Type Of Service) est aussi nécessaire. Ces flux, une fois analysés par l'appareil Cisco, sont envoyés à un Collecteur NetFlow qui se charge de stocker les flux et peut se faire requêter par l'administrateur réseau afin d'analyser le trafic passant par les interfaces de l'appareil configuré.

NetFlow permet donc dans un cas pratique de déterminer le plus gros consommateur de bande passante sur un réseau local, ou encore le type d'application le plus utilisé. Tout cela permet à l'administrateur réseaux de mieux dimensionner le réseau ainsi que d'appliquer des règles de QoS pour prioriser certaines applications, ou encore mieux de prévenir les éventuels dysfonctionnements du réseau.

3.6.2.2 IP SLA (Internet Protocol Service Level Agreement)

IP SLA est un procédé inventé par Cisco qui permet de générer du trafic entre différents équipements du réseau tels que les routeurs ou les switches et c'est ce trafic qui sera analysé afin de fournir les résultats demandés. [24]
IP SLA est utilisé pour analyser les performances d'un réseau. En effet, Dans un réseau d'entreprise la qualité d'un bout à l'autre doit pouvoir être qualifiée selon des critères précis. C'est ce qu'on appelle SLA (Service Level Agreement).
Il faut au moins un équipement Cisco (un routeur pour la plupart du temps) qui joue le rôle de « probe » ou « master » et au moins un élément du réseau qui sera le « responder » ou « esclave ». C'est le maitre qui va générer le trafic entre lui et les différents esclaves.

3.6.3 Déploiement de PfR

PfR est configuré sur des routeurs Cisco utilisant une interface de ligne de commande (CLI).
L'architecture de PfR est constituée de deux composants :

- le routeur contrôleur appelé Master Controller (MC)

- le routeur de frontière appelé Border Router (BR)

Le déploiement de PfR nécessite un MC et un ou plusieurs BR(s).

La communication entre le MC et le BR est protégée par une chaîne de clé authentique (key-chain authentication).

Selon le choix, le MC peut être configuré sur un routeur dédié ou avec le même routeur de BR.

Le réseau géré par PfR doit avoir au moins deux interfaces de sorties qui peuvent supporter les trafics externes, ils sont configurés comme des interfaces externes. Ces interfaces doivent se connecter à un FAI (Fournisseur d'Accès à Internet) ou à une liaison WAN (Frame Relay, ATM, MPLS). Le routeur doit aussi avoir une interface (accessible par le réseau interne) qui peut être configurée comme une interface interne pour le monitoring passif. Les interfaces servant à la communication entre le MC et le BR constituent les interfaces locales. Une seule interface doit être configurée en tant qu'interface locale sur chaque BR.

Il y a donc trois configurations d'interface nécessaires pour déployer PfR :

- Les interfaces externes
- Les interfaces internes
- Les interfaces locales

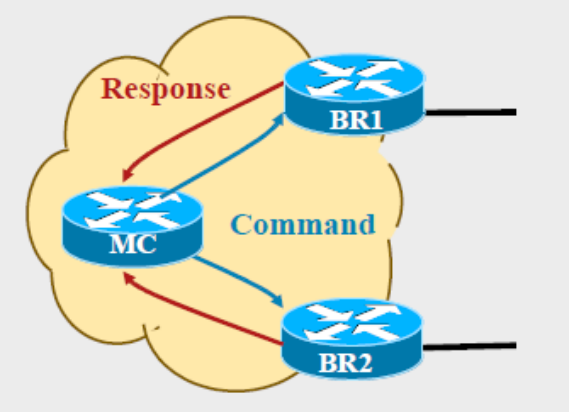


Figure 3.07 : *Architecture PfR reliant le MC et le BR*

3.6.3.2 Le Master Controller (MC)

Le MC est le cerveau intelligent qui gère PfR. C'est un unique routeur qui agit en tant que processeur central et base de données pour le système PfR. Lorsqu'il n'est pas déployé sur le même routeur que BR, il n'a aucune idée sur l'information de routage contenue dans BR. Il ne nécessite pas de protocole de routage.

Il maintient la communication et authentifie les sessions avec les BR.

Il a pour rôle de recueillir les informations issues des BR pour déterminer quelles classes de trafic sont en accord avec la politique de performance et d'ordonner les BR à assurer que ces classes de trafic sont dans les conditions de la politique en utilisant l'injection de route ou l'injection dynamique de PBR (Policy-Based Routing).

3.6.3.3 Le Border Router (BR)

Le routeur BR se trouve sur le routeur de périphérie du réseau avec une ou plusieurs liaisons avec un FAI ou d'autres réseaux. Le BR utilise le NetFlow pour recueillir passivement le débit et l'information sur la performance TCP. Le BR produit aussi tous les IP SLA pour un monitoring explicite des performances.

Le BR est le lieu où les politiques de décisions et les changements de routage dans le réseau sont renforcés.

Il participe au contrôle de préfixe et à l'optimisation de route en rapportant le préfixe et en envoyant les mesures de liaisons au MC, il accomplit ensuite l'application des politiques de changement sous l'ordre du MC. Il assure les politiques de changements en injectant une route choisie pour modifier le routage dans le réseau.

3.6.4 Cycle des opérations de PfR

Pour comprendre le fonctionnement de PfR dans un réseau, il est nécessaire de comprendre ses phases d'opérations. [22]

La boucle de performance de PfR est constituée de cinq phases :

- Phase d'apprentissage
- Phase de mesure
- Phase d'application de la politique
- Phase du contrôle ou renforcement
- Phase de vérification.

Après la phase de vérification, on revient à la phase d'apprentissage pour mettre à jour les classes des trafics et le processus continue ainsi de suite.

Pour faire ce cycle, PfR utilise le protocole TCP qui travaille entre le MC et le BR agissant comme en mode client-serveur pour échanger les messages et les ordres du MC.

Le diagramme qui suit montre les cinq phases de PfR.

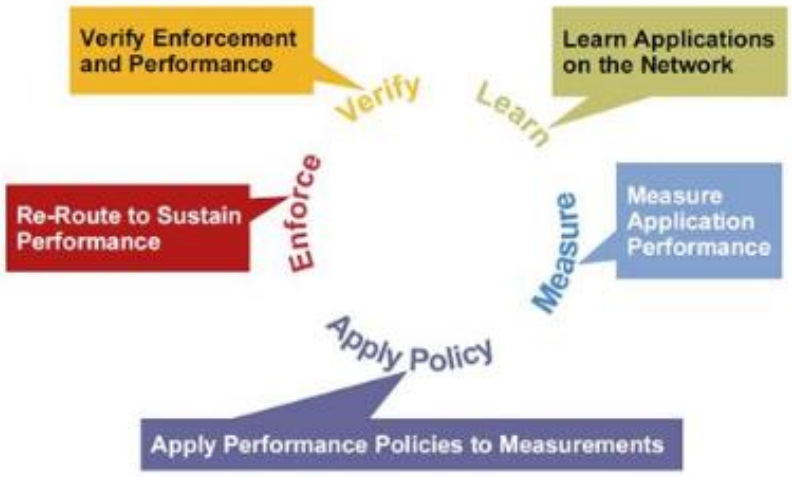


Figure 3.08 : *Les cinq phases de PfR*

3.6.4.1 Phase d'apprentissage

Pour une moyenne à grande entreprise, il existe des centaines de chemins sur lesquels on tente de router un trafic. Parmi les différents trafics arrivant sur le routeur, il faut choisir lesquels doivent être priorisés par rapport à d'autres. En effet, Cisco PfR permet d'appliquer un contrôle avancé de routage pour identifier les préfixes ou les classes de trafics intéressants. Une classe de trafic peut être définie comme une combinaison de préfixe, de protocole, de numéros de port et de valeur DSCP (Differentiated Services Code Point) pour identifier une application précise telle que la voix, par exemple. C'est là qu'intervient la phase d'apprentissage.

Pour ce faire, il existe deux moyens qui sont l'apprentissage automatique et l'apprentissage manuel.

a) Apprentissage automatique

Le routeur détermine le trafic ayant besoin d'une optimisation de routage en étudiant tous les flux qui le traversent et en sélectionnant ceux qui ont une latence (Delay) élevée ou un débit élevé. Le MC dresse alors une liste de tous les flux appris par ordre de latence ou de débit élevé.

b) Apprentissage manuel

Il peut être utilisé seul ou en complément avec l'apprentissage automatique.

Il consiste à configurer manuellement les classes des trafics pour leur donner le meilleur chemin. Pour ce faire, il faut créer une liste d'adresses pour définir le préfixe à considérer ou une ACL pour identifier une application à optimiser. Cette liste doit ensuite être reliée à ce qu'on appelle « PfR-map » qui est configurée avec un numéro de séquence. Le PfR-map qui présente un numéro de

séquence le plus faible sera considéré en premier. Pour chaque numéro de séquence, une seule correspondance avec une liste doit être faite.

3.6.4.2 Phase de mesure

Après avoir déterminé les classes de trafic ayant besoin de routage performant, PfR mesure les métriques de performances individuelles de ces classes de trafic. PfR mesure aussi l'utilisation des liaisons. On distingue alors deux mécanismes : le monitoring passif et le monitoring actif.
On peut utiliser l'un des deux ou les deux en même temps pour accomplir la tâche de mesure.
Le monitoring est l'opération qui consiste à mesurer les métriques de performance à des intervalles de temps périodiques.

- Le monitoring passif est le fait de mesurer les métriques de performances des flux de trafic pendant que ces derniers traversent le routeur. Il utilise la fonctionnalité de NetFlow.

La mesure passive des métriques comprend :

- La latence ou délai : PfR mesure la latence moyenne des flux TCP (Transmission Control Protocol) pour un préfixe donné ou une classe de trafic donnée. Cette latence est la mesure du temps de réponse d'aller-retour RTT (Round-Trip response Time) entre la transmission d'un message de synchronisation TCP et le reçu d'un accusé de réception TCP.
- La perte de paquets : PfR mesure la perte de paquets en déterminant les numéros de séquence TCP pour chaque flux TCP ; il détermine le plus grand numéro de séquence. S'il reçoit un paquet ayant un petit numéro de séquence, PfR incrémente le compteur de perte de paquets.
- L'accessibilité : PfR mesure cette accessibilité en comptant les messages de synchronisation TCP envoyés à plusieurs reprises sans recevoir d'accusé de réception TCP.
- Le débit : PfR mesure le débit en mesurant le nombre total d'octets et de paquets pour chaque classe intéressante de trafic ou pour chaque préfixe pendant un intervalle de temps donné.

- Le monitoring actif consiste à générer du trafic synthétique en utilisant IP SLA pour émuler la classe de trafic à mesurer. On mesure ce trafic synthétique au lieu de la véritable classe de trafic. Les résultats de mesure obtenus sont appliqués pour donner le routage performant à la classe de trafic correspondante. [22]

La mesure active des métriques comprend :

- La latence : PfR mesure la latence moyenne des flux TCP, UDP (User Datagram Protocol) et ICMP (Internet Control Message Protocol) pour une classe de trafic donnée ou un préfixe donné.
- L'accessibilité : PfR mesure cette accessibilité en comptant les messages de synchronisation TCP envoyés à plusieurs reprises sans recevoir d'accusé de réception TCP.
- La gigue (Jitter) : PfR mesure la gigue en envoyant des paquets multiples à une adresse cible et à un numéro de port spécifique cible puis en mesurant l'intervalle de retard entre les arrivées des paquets à la destination.
- Le MOS (Mean Opinion Score) : c'est une méthode standard pour mesurer la qualité de la voix. Les notes peuvent aller de 0 (représentant une très mauvaise qualité) à 5 (représentant la qualité excellente de la voix, comparable à la version originale). PfR mesure le MOS en utilisant IP SLA.

Ces deux mécanismes peuvent être appliqués aux classes de trafic. La phase de monitoring passif peut détecter que la performance de la classe de trafic n'est pas conforme à la politique de PfR et le monitoring actif peut être appliqué à cette classe pour trouver le meilleur chemin alternatif si disponible. [25]

PfR mesure non seulement les classes de trafic mais aussi l'état des liaisons.

La mesure de l'utilisation de liaison (liaison à un WAN) se fait automatiquement après la configuration d'une interface externe sur BR.

Par défaut, les BR reportent l'utilisation de liaison au MC toutes les 20 secondes. Si l'utilisation de la liaison en entrée ou en sortie est au-dessus du seuil (par défaut de 75%) alors la liaison en entrée ou en sortie est en OOP et PfR commence les mesures pour trouver une liaison alternative pour la classe de trafic considérée. Ce seuil peut être manuellement configuré par une valeur en kbps ou en pourcentage (%).

Un rang d'utilisation peut aussi être donné pour faire un équilibrage de charge entre les liaisons de sortie.

a) Les différents états des classes de trafic

Avant toute mesure, PfR détermine l'état de ces trafics ou de la liaison car dans un certain état le PfR ne lance pas la phase de mesure.

On distingue les différents états suivants :

- état « Default » : une classe de trafic est dans cet état lorsqu'elle vient d'être listée parmi les préfixes à considérer appelée MTC (Monitored Traffic Class) ou lorsqu'elle n'est pas sous le contrôle de PfR. Une classe entre ou sort de cet état selon les mesures de performance et la configuration de la politique.
- état « Choose exit » : c'est un état temporaire pendant lequel PfR compare l'état courant de la classe de trafic avec les paramètres de politiques pour trouver la meilleure sortie pour elle. La classe restera dans cet état jusqu'à ce qu'elle soit déplacée à une nouvelle sortie.
- état « Holddown » : une classe de trafic est placée dans cet état lorsque le MC demande au BR de faire des mesures en utilisant des sondes. Les mesures sont collectées par le BR pendant un temps (« Holddown timer ») puis les transmettent au MC afin de vérifier la sortie de la classe de trafic. Si cette dernière est inaccessible, la classe de trafic revient à l'état «Choose exit ».
- état « In Policy » : lorsque les mesures de performances ont été comparées avec les politiques définies ou les politiques par défaut et qu'une sortie a été choisie, le trafic entre dans cet état. Autrement dit, ce trafic emprunte le chemin qui répond au critère des politiques définies. Ainsi, aucune autre action n'est faite par le MC à moins que le temps périodique de mesure expire ou qu'un évènement OOP est déclenché. Dans ce cas, le trafic revient à l'état « Choose exit ».
- état « Out Of Policy ou OOP » : une classe de trafic est en état de OOP lorsqu'aucune sortie ne correspond aux politiques définies. Si toutes les sorties sont en OOP, le MC choisit la sortie la plus satisfaisante disponible.

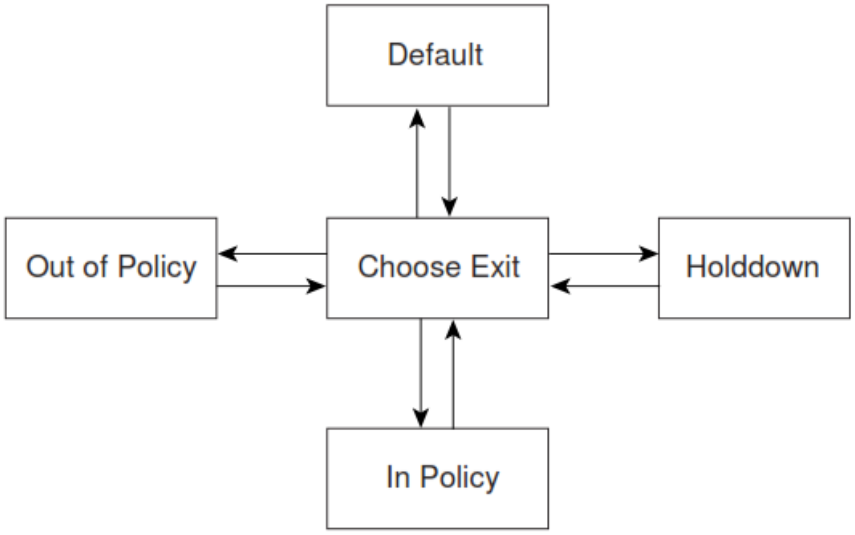


Figure 3.09 : *Transition entre les différents états du trafic*

b) Les sondes actives utilisées par le monitoring actif

Nous avons vu que PfR utilise IP SLA pour le monitoring actif afin d'analyser les niveaux de service des applications IP. Pour ce faire, PfR utilise différents types de sondes actives selon les informations qu'on veut obtenir sur l'état du réseau. Il y a :

- ICMP echo : un ping est envoyé à une adresse cible ; cette sonde est utilisée par défaut par PfR et ne nécessite aucune configuration sur l'équipement cible. On obtient comme résultat le délai à double sens (RTT ou Round Trip Time) vers la cible.
- Jitter : une sonde gigue est envoyée à une adresse cible et un numéro de port cible. La cible doit être configurée en tant que « responder » pour assurer le mécanisme de l'IP SLA. Cette sonde est surtout utilisée pour mesurer les niveaux de service des applications telles que la voix. En effet, elle permet d'obtenir en plus du RTT, la valeur de la gigue entre le maître et l'esclave IP SLA, la perte des paquets et la valeur du MOS qualifiant la voix.
- TCP connect : une connexion TCP est établie avec l'adresse cible avec un numéro de port différent de l'usuel port 23. La cible doit aussi être configurée en tant que « responder ». Cette sonde mesure le temps de réponse pour effectuer une connexion TCP à un port choisi sur un équipement.
- UDP echo : une sonde UDP est envoyée à l'adresse cible. Le mode « responder » doit aussi être actif sur cette cible. Cette sonde permet de mesurer le temps de réponse de bout en bout entre le master et la cible.

Lors de l'activation d'une sonde, on doit spécifier la fréquence de répétition de l'opération. Cette fréquence est égale à 60s par défaut mais peut être diminuée pour une meilleure approximation des états du réseau.

3.6.4.3 Phase d'application de la politique

Après avoir collecté les métriques de la classe de trafic à optimiser, PfR compare les résultats avec une série de seuils (faible et élevé) configurés comme politique pour chaque métrique. Quand une métrique, et par conséquent une politique, dépasse les limites, on a un évènement appelé Out-Of-Policy (OOP). Les résultats sont comparés sur une base relative, une déviation par rapport à une moyenne observée ou par rapport à un seuil, par rapport à la valeur qui manque ou qui excède les limites ou la combinaison des deux.

Ainsi, cette phase consiste à comparer les métriques de performance mesurées avec des seuils connus ou configurés pour déterminer si le trafic correspond à un niveau spécifique de service ou si

une quelconque action est requise. Si la métrique n'est pas conforme au seuil, une décision est prise par PfR pour déplacer la classe de trafic ou l'envoyer dans un autre état.
Une politique PfR est une règle qui définit un objectif et contient les attributs suivants :

- le but ou Scope
- l'action
- la condition ou Triggering event

Si par exemple on vaut configurer une politique qui permet de maintenir une latence inférieure ou égale à 100ms pour des paquets envoyés à une classe de trafic spécifique : le scope est le fait d'envoyer les trafics à une classe spécifique ; l'action est le changement potentiel de la table de routage et le « triggering event » est la détection d'une latence mesurée étant supérieure à 100ms.
Il y a deux types de politiques définies dans PfR : les politiques de classe de trafic et les politiques de liens. Les politiques de classe de trafic sont définies pour les préfixes et les applications. Les politiques de liens sont définies pour les liens entrant ou sortant à la périphérie du réseau. Ces deux types de politiques définissent le critère pour déterminer un évènement OOP. Les politiques sont appliquées, ensuite, soit sur une base globale dans laquelle une série de politiques est appliquée pour toutes les classes de trafic, soit sur une base ciblée dans laquelle une série de politiques est appliquée sur une liste sélectionnée (filtrée) de classes de trafic.

3.6.4.4 Phase de renforcement

Dans cette phase, appelée aussi phase de contrôle, le trafic est contrôlé pour améliorer la performance du réseau. Dans les trois premières phases, PfR a opéré par défaut dans le mode observateur c'est-à-dire avec une simple coordination des informations de performance par MC depuis BR puis une prise de décision de politique. Dans la phase de contrôle, PfR entre dans le mode de contrôle proprement dit, ce qui signifie qu'en plus de ces tâches, MC commande les BR de modifier le routage afin d'implémenter les décisions de politiques.
La technique utilisée pour le contrôle de trafic dépend de la classe de celui-ci. Pour les classes de trafic définies seulement par un préfixe, le préfixe sur l'information d'accessibilité utilisé en routage traditionnelle peut être manipulé. Les protocoles tels que BGP, RIP ou EIGRP sont utilisés pour ajouter ou enlever le préfixe sur l'accessibilité en introduisant ou en supprimant une route avec le coût des métriques appropriés.
Pour les classes de trafic définies par une application dans laquelle un préfixe et un paquet avec un critère associé sont spécifiés, PfR ne peut pas utiliser les protocoles de routages traditionnels car ces

derniers s'appuient seulement sur le préfixe d'accessibilité. Le contrôle devient alors à la charge du routeur et non plus du réseau. Ce contrôle spécifique du routeur est implémenté par PfR en utilisant la fonctionnalité de PBR (Policy-Based Routing).

Le PBR traduit par le routage basé sur une stratégie, fournit un outil pour transmettre et router des paquets de données selon des politiques définies ignorant ainsi les décisions de protocole de routage. Le PBR inclut un mécanisme d'application sélectif des stratégies basé sur la liste d'accès, la taille de paquet ou d'autres critères. Les mesures prises peuvent inclure le paramétrage de la priorité et le routage de paquets sur des routes définies par l'administrateur. [26]

3.6.4.5 Phase de vérification

La dernière phase de vérification consiste à vérifier si les actions de contrôle ont fait des changements sur le flux de trafic et si la performance de la classe de trafic ou celle de la liaison de sortie transite dans l'état « In Policy ».

En effet, comme il est dit précédemment, pendant la phase de renforcement, si une classe de trafic est OOP alors PfR introduit des contrôles pour influer ou optimiser le flux de trafic pour cette classe. Une route statique ou une route BGP est un exemple de contrôle introduit par PfR dans le réseau.

Après ces contrôles, PfR vérifie que le trafic optimisé a traversé les liens préférés entrant ou sortant à la frontière du réseau. Si la classe du trafic reste OOP, PfR enlèvera les contrôles introduits pour optimiser ce trafic et il revient à la première phase du cycle.

3.6.5 Topologie typique du réseau d'entreprise

La figure suivante montre la topologie typique des réseaux d'entreprise utilisant PfR, celle du réseau d'entreprise fournisseur de données (Content Provider).

Le réseau d'entreprise dispose de trois interfaces de sortie, utilisés pour délivrer les données au réseau d'accès du client. L'entreprise Content Provider possède un différent contrat de niveau de services (SLA) avec de différent fournisseur d'accès Internet (ISP) pour chaque liaison de sortie. Le réseau d'accès du client dispose de deux routeurs de périphérie connectés à Internet. Le trafic est transporté entre le réseau d'entreprise et celui du client à travers six réseaux fournisseurs de service.

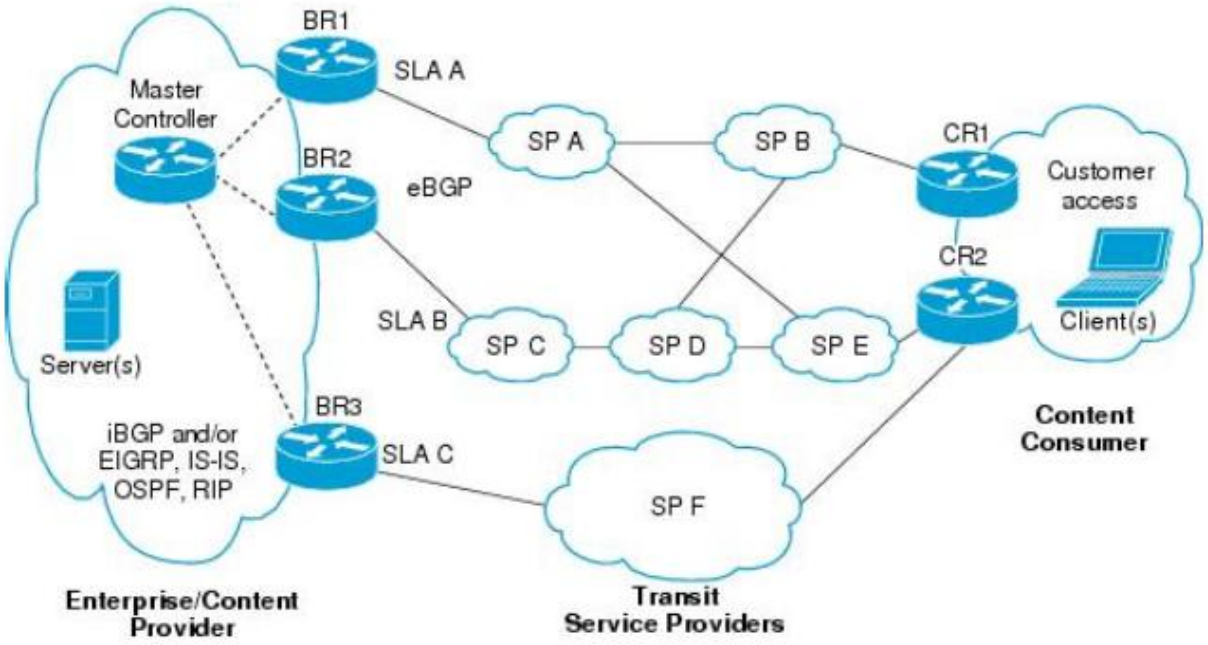


Figure 3.10 : *Topologie typique du réseau*

PfR surveille et contrôle les trafics sortants sur les trois routeurs BR. Il mesure le temps de réponse des paquets et la disponibilité du chemin depuis les interfaces de sortie sur BR1, BR2 et BR3. Les changements de la performance des liaisons de sortie sur les BR sont détectés sur des bases de préfixes. Si la performance d'un préfixe tombe au-dessous des paramètres définis, le routage est localement modifié dans le réseau d'entreprise pour optimiser la performance et pour router malgré des pannes qui se produisent à l'extérieur du réseau. Par exemple, un disfonctionnement d'une interface ou une mauvaise configuration dans le réseau SP D vont produire un trafic qui va atteindre BR2. L'interface de sortie de celui-ci sera donc en congestion ou n'arrive plus à accéder le réseau d'accès du client. Les mécanismes de routage traditionnel ne permettent pas d'anticiper ni de résoudre ces types de problèmes sans l'intervention d'un opérateur réseau, contrairement à PfR qui peut détecter les conditions de pannes et modifie automatiquement le routage à l'intérieur du réseau en compensation.

3.6.6 Clients de la technologie PfR

Les entreprises présentant les caractéristiques suivantes peuvent utiliser la solution PfR :

- Les grandes, moyennes et petites entreprises ayant des missions utilisant Internet nécessitant des exigences de performances en temps réel.
- Les entreprises avec des multiples réseaux WAN pour des besoins en disponibilité.

- Les entreprises avec des sites distants ayant un réseau de transport WAN primaire et un autre pour le backup.
- Les télétravailleurs utilisant des connexions Internet

3.7 Conclusion

En tenant compte des besoins actuels des entreprises en termes de performances des différents services (données, voix, vidéo…) offerts par leurs réseaux, nous avons constaté que les protocoles de routage traditionnels ne sont plus efficaces ni suffisants pour assurer les qualités de service de ces applications et n'arrivent pas non plus à résoudre des problèmes fréquents tels que la congestion, des pannes douces des équipements…. Nous avons ensuite vu les possibilités d'optimisation offertes par la solution Performance Routing (PfR) : il fournit des décisions de routage basées dynamiquement sur le changement des paramètres de qualité de service au sein du réseau d'entreprise, il détecte les conditions de pannes et permet une distribution de charge plus efficace sur les diverses liaisons WAN.

CHAPITRE 4
SIMULATION

4.1 Introduction

La partie simulation pour la concrétisation de ce travail a été basée sur l'étude du réseau du Ministère des Finances et du Budget où j'ai effectué mon projet de recherche.
Avant d'entrer dans le vif du sujet, une présentation générale du Ministère des Finances et du Budget sera abordée. Nous allons ensuite décrire les différentes étapes effectuées lors de l'élaboration du travail d'analyse du réseau et les résultats sont illustrés par des simulations.

4.2 Présentation du Ministère des Finances et du Budget

4.2.1 Missions du Ministère des Finances et du Budget

Dans le cadre de la Politique Générale de l'Etat, le Ministre des Finances et du Budget (MFB):

- élabore et met en œuvre la politique financière, fiscale et budgétaire de l'Etat comprenant :
  - l'élaboration des projets de Lois de Finances ;
  - le contrôle et la synthèse de l'exécution des Lois de Finances ;
  - les travaux d'assiette, de contrôle et de recouvrement des ressources fiscales et douanières ;
  - la gestion et le contrôle du patrimoine de l'Etat et des collectivités locales ;
  - la gestion de la trésorerie et des dettes intérieure et extérieure de l'Etat ;
  - la coordination de la Politique du Gouvernement en matière de micro finance
- partage avec d'autres entités le pilotage de l'économie et la maîtrise des grands équilibres économiques, financiers et monétaires qui consistent en l'établissement, le suivi et le perfectionnement du tableau de bord et la conduite des travaux et d'analyses susceptibles d'éclairer les choix et décisions du Gouvernement en matière budgétaire et financière ;
- assure la gestion et le suivi-évaluation des aides extérieures et contribue à l'harmonisation de la coopération avec les bailleurs de fonds ;
- assure la tutelle des institutions financières et des établissements publics ;
- contribue activement au bon déroulement de l'évolution de l'environnement institutionnel Malagasy dans le cadre de la décentralisation et de la déconcentration, de la régulation de l'environnement comptable de l'ensemble des secteurs économiques

4.2.2 Structure générale du MFB

L'organisation générale du Ministère des Finances et du Budget est fixée comme suit :

- Le Cabinet du Ministère ;
- Le Secrétariat Général ;
- La Direction Générale de l'Audit Interne placé sous l'autorité directe du Ministre ;
- La Direction Générale du Contrôle Financier placée sous la tutelle et le contrôle technique du Ministre ;
- L'Autorité de Régulation des Marchés Publics placée sous la tutelle et le contrôle technique du Ministre ;
- La Cellule de Coordination des Projets de Relance Economique et d'Actions Sociales.

Les directions au sein du siège du Secrétariat Général sont :

- Bureau d'Appui au Secrétaire Général
- Direction des Ressources Humaines et de l'Appui
- Direction des Affaires Administratives et Financières
- Direction des Systèmes d'Information
- Direction du Renforcement de la Gouvernance
- Direction de la Promotion du Partenariat Public Privé
- Service Communication

La figure suivante montre un extrait de l'organigramme du Ministère des Finances et du budget :

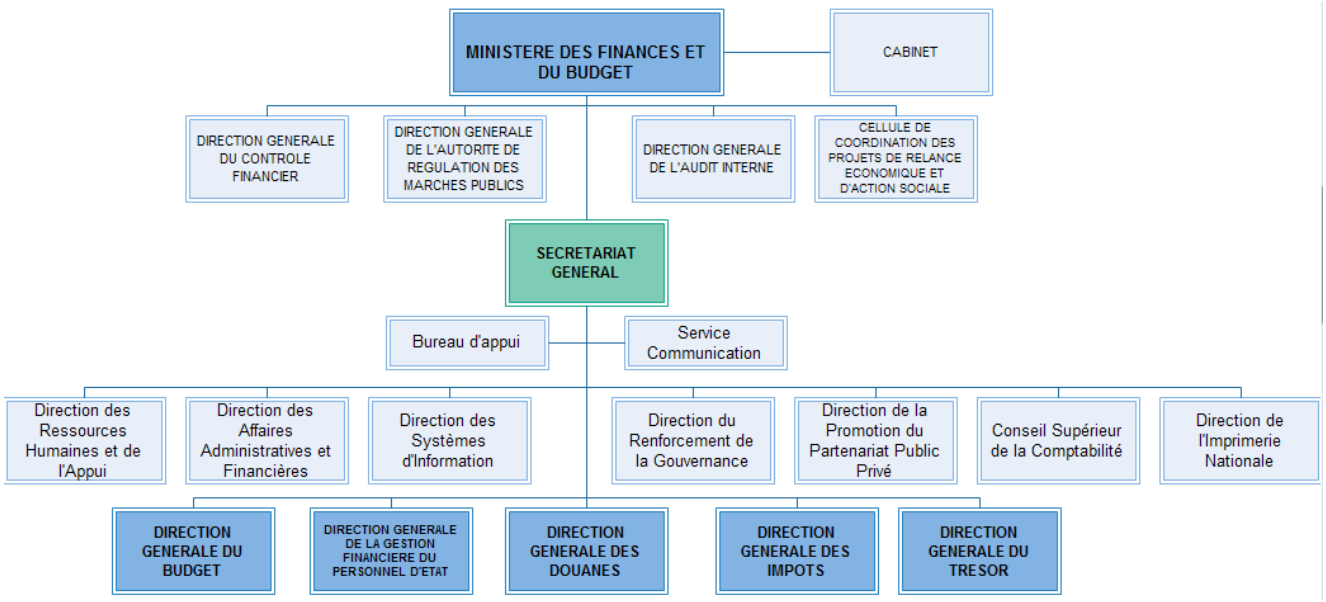


Figure 4.01 : *Extrait de l'organigramme du MFB*

4.2.3 Direction des Systèmes d'Information

Cette direction se trouve sous la responsabilité de Monsieur RANDRIARIJAONA Lucien Elino.
Conformément aux dispositions du Décret N° 2014-1102 du 22 Juillet 2014 fixant les attributions du Ministre des Finances et du Budget ainsi que l'organisation générale de son Ministère, la Direction des Systèmes d'Information est chargée d'une manière générale de la gouvernance et de la gestion du système d'information du Ministère des Finances et du Budget.
A ce titre, elle est chargée de :

- proposer et mettre en œuvre la stratégie d'information du Ministère ;
- assurer la conception, le développement et la mise en œuvre du système d'information du Ministère ;
- proposer et mettre en œuvre la Politique Générale des acquisitions et de maintenance des infrastructures informatiques ;
- proposer et mettre en œuvre la stratégie de sécurité des infrastructures informatiques ;
- former et assister les utilisateurs du système d'information du ministère afin d'assurer la continuité et la fluidité de la circulation des informations ;
- assurer la mission de veille technologique et organiser le système, le réseau et la sécurité de l'information.

La Direction du Système d'Information dispose de :

- un Service de la Veille Technologique, de la Formation et de l'Assistance ;
- un Service de la Conception et du Développement du Système d'Information ;
- un Service de la Maintenance des Infrastructures ;
- un Service du Réseau, du Système et de la Base de Données.

Mon projet de recherche s'est déroulé au sein du Service du Réseau, du Système et de la Base de Données.

4.2.4 Objectifs du projet au sein du MFB

Mon projet au sein du MFB a pour objectif général de déterminer les solutions d'optimisation de son réseau global.
De manière détaillée, nous allons donc mettre à niveau le réseau local du Siège du MFB et optimiser tous les aspects critiques au niveau du WAN.
Le résultat attendu est donc de mettre en œuvre un niveau de performance élevé du réseau satisfaisant toutes les différentes attentes des applications réseaux et des utilisateurs.

Pour atteindre ces objectifs, le déroulement du projet se présente par les étapes suivantes:

- prendre en charge et analyser le réseau actuel du MFB : recenser les différents équipements, étudier les différentes tâches effectuées par ces équipements, fournir une architecture logique du réseau global.
- déterminer les points faibles du réseau entraînant la dégradation des performances du réseau à partir des résultats d'analyses effectuées.
- mettre en œuvre les solutions d'optimisations adéquates aux différents problèmes détectés: fournir une nouvelle architecture du réseau, illustrer toutes les techniques utilisées sous le simulateur réseau GNS3.

4.3 Présentation de l'outil de simulation : GNS3

GNS3 ou Graphical Network Simulator 3rd version est un logiciel libre (« open source ») qui permet d'émuler des routeurs Cisco, des firewalls, des modules de switching de la même façon, par exemple, que VMware permet d'émuler Windows ou Linux.

A partir de GNS3, on peut construire sa propre architecture comme « en réel », et simuler de simples architectures aux plus complexes.

Sa différence avec les autres simulateurs tels que Packet Tracer se repose sur le fait que GNS3 émule un IOS Cisco que l'on fournit et cet IOS se comporte exactement comme s'il tournait sous une plateforme matérielle Cisco. Packet tracer, lui, est un logiciel qui prend quelque commande Cisco et qui répond en conséquence de ce que le programmeur a choisi ; on a donc un fonctionnement approximatif, et on ne pourra pas tester par exemple les nouvelles fonctionnalités d'un IOS.

Ainsi, GNS3 utilise des véritables IOS de Cisco dans un environnement virtuel à travers un ordinateur.

GNS3 est particulièrement intéressant pour :

- l'entrainement, la pédagogie et la familiarisation avec les produits et les technologies de Cisco System,
- tester les fonctionnalités d'un IOS,
- la vérification rapide de configuration à déployer plus tard dans un environnement de production.

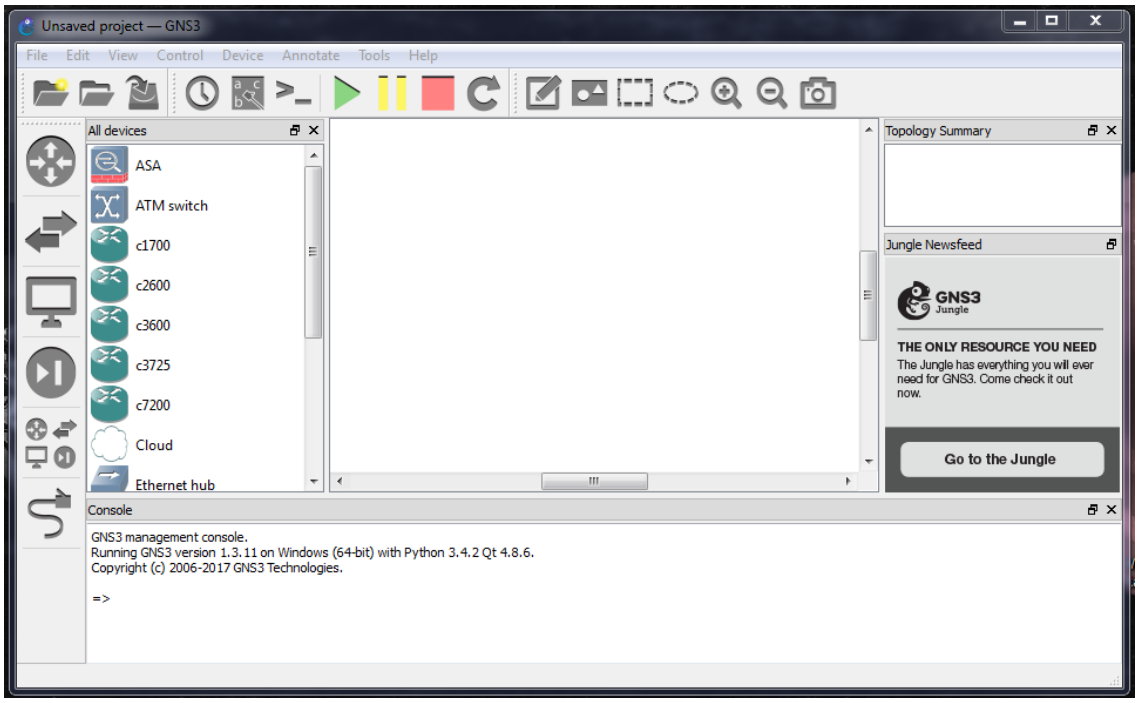


Figure 4.02 : *Interface graphique de GNS3*

4.4 Prise en charge du réseau existant de MFB

4.4.1 Description générale du réseau

Le réseau du Ministère des Finances et du Budget (MFB) trouve son siège dans la ville d'Antananarivo et est constitué par des bureaux intra-villes ainsi que des bureaux dans toutes les régions de Madagascar. Le siège se trouve aussi en réseau avec toutes les autres directions générales qui lui sont rattachées.

Ainsi le réseau MFB est de type multi-site utilisant les technologies LAN et WAN.

Le réseau du siège est un LAN commuté bâti sur une technologie Ethernet, associée à des réseaux VLA. Il est relié avec les bureaux intra-villes ainsi que les autres directions générales (pour former l'Intranet de l'Etat) par réseau WiMax (fourni par l'ANRE ou Agence Nationale de Réalisation de l'E-gouvernance). La liaison entre le siège et toutes les régions se fait par des lignes virtuelles de Frame Relay (fournie par TELMA). Cependant il existe aussi une liaison VPN pour assurer la continuité de travail à domicile des employés du ministère. Le réseau dispose aussi d'un accès à l'Internet (aussi fourni par TELMA).

Les bureaux se trouvant dans chaque région sont interconnectés entre eux par WiMax.

Ainsi les technologies réseaux utilisées sont :

- VLAN

- WAN : Frame Relay
- WiMax
- VPN et Internet

4.4.2 Caractéristiques des différents équipements utilisés

Les équipements réseau utilisés sont :

- Des commutateurs ou switch
- Des routeurs

Les équipements terminaux sont :

- Des serveurs (serveurs de bases de données, serveurs d'application, serveur Web, serveur Mail)
- Des ordinateurs de bureau
- Des ordinateurs portables
- Des imprimantes

4.4.2.1 Les commutateurs ou switch

Nomenclature	**Fonction**	**Modèle**	**Caractéristiques**
SW_Access	Assure l'accès des machines au réseau	Cisco Catalyst 2960	Dédié Ethernet 10/100/1000 Mbits/s, ayant une fonctionnalité de QoS, de 12 à 48 ports
SW_Peripherie	Assure l'accès des routeurs au réseau	Cisco Catalyst 3750	12 ports Gigabit Ethernet SFP (Small Form-factor Pluggable), utilisé comme Switch de la couche 2
SW_Server	Assure l'accès aux serveurs	Cisco Catalyst 2960-S	Connectivité de 1 et 10 Gbits/s, empilable (Cisco FlexStack), Connectivité de bureau Ethernet Gigabit à 24 ou 48 ports, Support de PoE+
		Cisco Catalyst 2960-X	24 ou 48 ports Gigabit Ethernet, FlexStack-Plus pour empiler jusqu'à 8 commutateurs, Support de PoE+
SW_Core	Assure les fonctions des couches cœur et de distribution, Assure le filtrage, le routage inter-VLAN et le routage de niveau 3	Cisco Catalyst 3750 12-S	12 ports Gigabit Ethernet SFP (Small Form-factor Pluggable), Switch Multicouche, avec Cisco StackWise (pour empiler jusqu'à 9 commutateurs)

Tableau 4.01: *Caractéristiques des switches*

4.4.2.2 Les routeurs

Nomenclature	Fonction	Modèle	Caractéristiques
Routeur_VPN	Assure la liaison VPN	Cisco 3825	Support jusqu'à 4 types de module réseau, 4 emplacements pour carte WIC, 2 ports fixes Gigabit Ethernet (10 /100/1000), 2 ports USB, 1 port console, 1 port auxiliaire, intégration des services de téléphonie d'entreprise, des services de routages multi-protocoles, des services de sécurité d'entreprise, VPN intégré (accélération de cryptage des VPN)
Routeur_Internet	Assure la connexion à Internet	Cisco 3945	3 ports LAN (10/100/1000), 3 ports RJ-45, 4 slots WIC, 2 slots USB, 1 port console, 1 port auxiliaire, Sécurité réseau intégré (par intégration à un réseau Cisco SDN), intégration des services sans fil et de mobilité, Commutation LAN intégrée
Routeur_Région	Assure la liaison avec les régions	Cisco 1841	2 ports Ethernet embarqués 10/100, 2 emplacements modulaires pour l'accès au réseau WAN avec support de plus de 30 cartes interfaces, 1 port console, 1 port auxiliaire, avec une option de prévention d'intrusion (IPS), pare-feu à inspection d'état, renforcement de performance VPN (Cisco Easy VPN), support de VLAN
Routeur_ACL	Assure la sécurité : IPS, ACL	Cisco 3945	3 ports LAN (10/100/1000), 3 ports RJ-45, 4 slots WIC, 2 slots USB, 1 port console, 1 port auxiliaire, Sécurité réseau intégré (par intégration à un réseau Cisco SDN), intégration des services sans fil et de mobilité, Commutation LAN intégrée
Routeur_Intranet	Assure la liaison avec l'Intranet de l'Etat	Routeur logique	Connecté à un IDU et une antenne WiMax
Routeur_Intraville	Assure la liaison avec les bureaux de la région Analamanga	Routeur logique	Connecté à un IDU et une antenne WiMax
Routeur_Proxy	Assure la connexion à Internet	Routeur logique (nombre=5)	De type Proxy, utilisant PfSense et RedHat

Tableau 4.02: *Caractéristiques des routeurs*

4.4.2.3 Autres équipements

Description	Modèle	Caractéristiques
Transceiver SFP	GLC-SX-MM ou 1000BASE-SX SFP	Pour fibre optique multimode de plus de 550m
	GLC-T ou 1000BASE-T SFP	Pour câble UTP (10/100/1000) de plus de 100m
Antenne WiMax	Alvarion BreezeMAX µBST	Antenne omnidirectionnelle, Puissance d'émission à -2dBW, gain d'antenne de 10 dBi

Tableau 4.03: *Autres équipements*

4.4.2.4 Câbles

Description	Type	Bande passante
Liaison entre hôte et switch d'accès	Câble Cuivre à Paire Torsadée non blindée UTP	100 Mbps
Liaison avec le Switch Core	Câble optique	1Go par fibre

Tableau 4.04: *Câbles utilisés*

4.4.3 Architecture logique du réseau

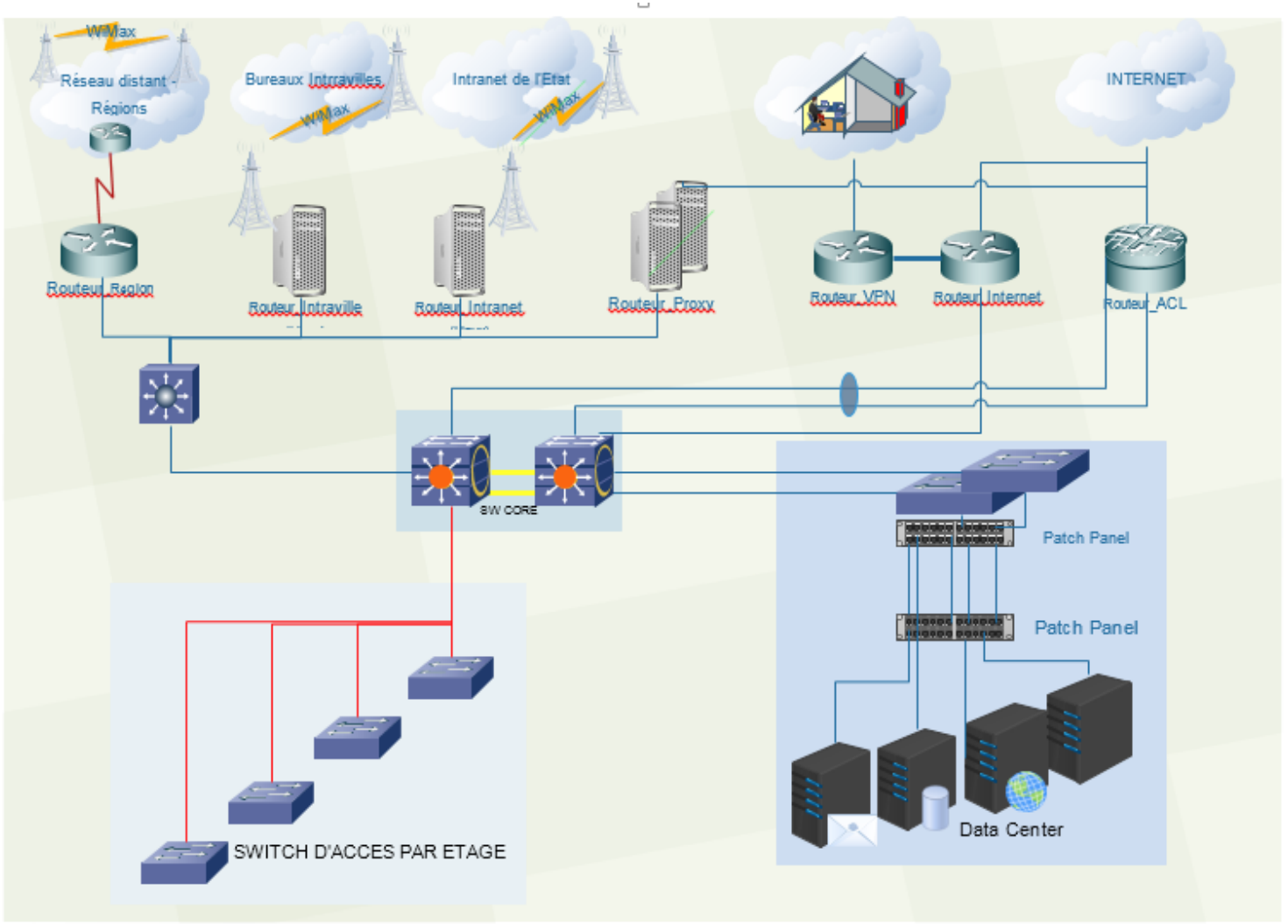


Figure 4.03 : *Architecture logique du réseau*

4.4.4 Plan d'adressage utilisé lors de la simulation

Voici les adresses réseau utilisés pour chaque zone de l'architecture :

- Réseau dans les régions : 20.20.0.0 /16
- Réseau Intranet : 20.21.0.0 /16
- Réseau LAN du siège : 30.30.0.0 /16
- Data Center : 40.40.40.0 /24
- Peer to Peer : 172.16.5.0 /24

La technique de VLSM est utilisée pour l'adressage. Il est à savoir alors que chaque région compte au maximum 100 hôtes ce qui donne alors un nouveau masque réseau de 20.20.0.0 /25 pour avoir 126 adresses utilisables ; chaque direction générale compte jusqu'à 64 hôtes au maximum ce qui donne 20.21.0.0 /26 ; de même, le LAN du siège est divisé en VLAN repartis par direction comptant chacune pas plus de 64 hôtes ce qui donne 30.30.0.0 /26, les routeurs du Siège appartiennent aussi à un VLAN que l'on nommera Périphérie ; les serveurs sont adressés sur l'adresse réseau 40.40.40.0 /24 ; pour chaque liaison Peer to Peer on a 172.16.5.0 /30 pour avoir les deux adresses requises.
Les tableaux suivants donnent le plan d'adressage du réseau.

Région	Adresse réseau	Plage d'adresse	Broadcast
1	20.20.1.0 /25	20.20.1.1 – 20.20.1.126	20.20.1.127
2	20.20.1.128 /25	20.20.1.129 – 20.20.1.254	20.20.1.255
3	20.20.2.0 /25	20.20.2.1 – 20.20.2.126	20.20.2.127
4	20.20.2.128 /25	20.20.2.129 – 20.20.3.254	20.20.2.255
…	…	…	…
25	20.20.13.0 /25	20.20.13.1 – 20.20.13.126	20.20.13.127

Tableau 4.05: *Plan d'adressage des réseaux des régions*

DG	Adresse réseau	Plage d'adresse	Broadcast
1	20.21.1.0 /26	20.21.1.1 – 20.21.1.62	20.21.1.63
2	20.21.1.64 /26	20.21.1.65 – 20.21.1.126	20.21.1.127
3	20.21.1.128 /26	20.21.1.129 – 20.21.1.190	20.21.1.191
4	20.21.1.192 /26	20.21.1.193 – 20.21.1.254	20.21.1.255
5	20.21.2.0 /26	20.21.2.1 – 20.21.2.62	20.21.2.63
…	…	…	…

Tableau 4.06: *Plan d'adressage au niveau de l'Intranet de l'Etat*

VLAN ID	Nom VLAN	Adresse réseau	Plage d'adresse	Broadcast
VLAN 10	Bureau d'appui SG	30.30.1.0 /26	30.30.1.1 – 30.30.1.62	30.30.1.63
VLAN 164	DRH	30.30.1.64 /26	30.30.1.65 – 30.30.1.126	30.30.1.127
VLAN 128	DAAF	30.30.1.128 /26	30.30.1.129 – 30.30.1.190	30.30.1.191
VLAN 192	DSI	30.30.1.192 /26	30.30.1.193 – 30.30.1.254	30.30.1.255
VLAN 20	DRG	30.30.2.0 /26	30.30.2.1 – 30.30.2.62	30.30.2.63
VLAN 264	DPPPP	30.30.2.64 /26	30.30.2.65 – 30.30.2.126	30.30.2.127
VLAN 228	Service Com	30.30.2.128 /26	30.30.2.129 – 30.30.2.190	30.30.2.191
VLAN 292	Cabinet Ministère	30.30.2.192 /26	30.30.2.193 – 30.30.2.254	30.30.2.255
VLAN 30	Audit Internet	30.30.3.0 /26	30.30.3.1 – 30.30.3.62	30.30.3.63
VLAN 364	Contrôle Financier	30.30.3.64 /26	30.30.3.65 – 30.30.3.126	30.30.3.127
VLAN 328	ARMP	30.30.3.128 /26	30.30.3.129 – 30.30.3.190	30.30.3.191
VLAN 392	Coordination Projet	30.30.3.192 /26	30.30.3.193 – 30.30.3.254	30.30.3.255
VLAN 40	Périphérie	30.30.4.0 /26	30.30.4.1 – 30.30.4.62	30.30.4.63

Tableau 4.07: *Plan d'adressage des VLANs au sein du Siège*

VLAN ID	Nom VLAN	Adresse réseau	Plage d'adresse	Broadcast
VLAN 400	Data Center	40.40.40.0 /24	40.40.40.1-40.40.40.254	40.40.40.255

Tableau 4.08: *Plan d'adressage dans le Data Center du Siège*

4.4.5 Simulation du réseau existant sous GNS3

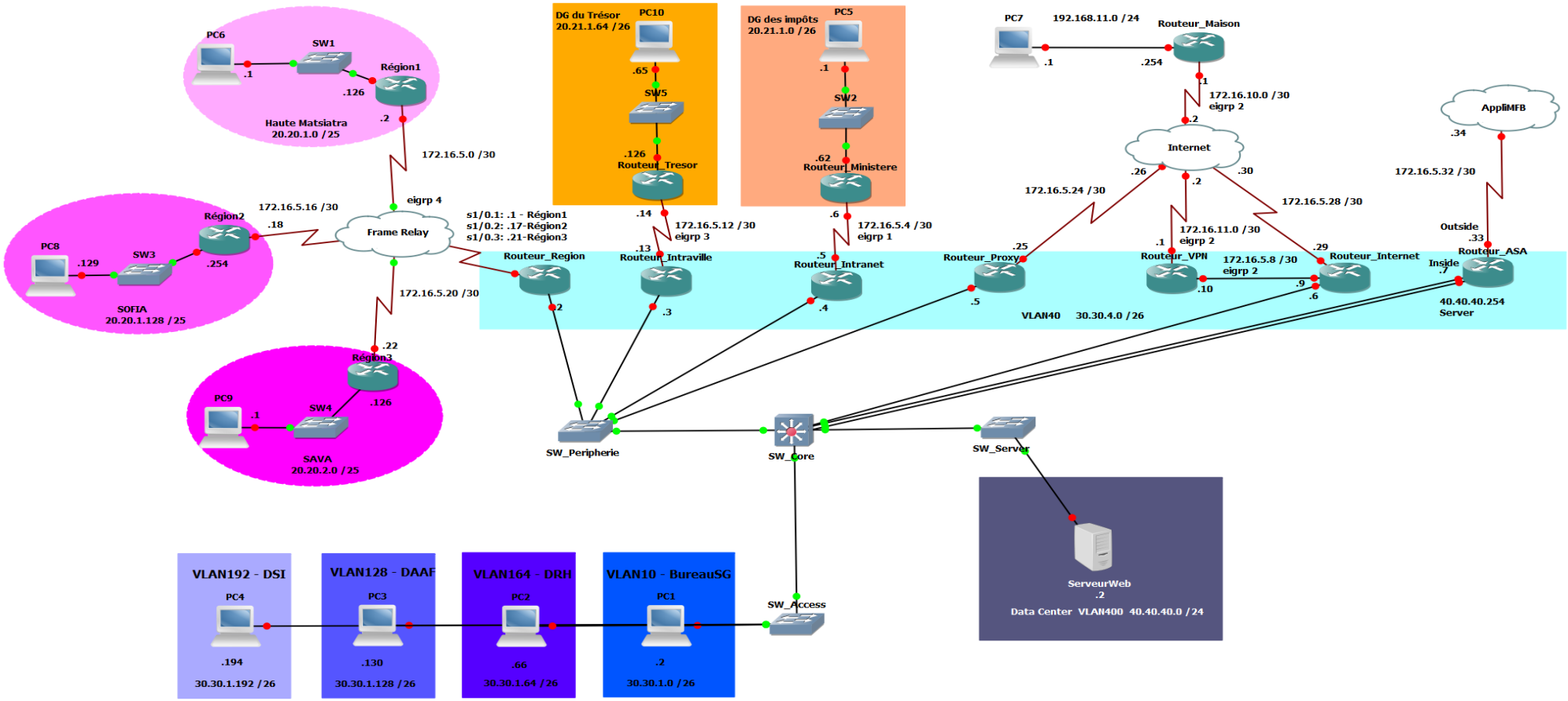


Figure 4.04 : *Topologie du réseau sous GNS3*

Le tableau suivant montre l'adressage des routeurs et du serveur Web.

Périphérique	Interface	Adresse IP	Masque
Routeur_Région	FastEthernet 0/0	30.30.4.2	/26
	Serial 1/0.1	172.16.5.1	/30
	Serial 1/0.2	172.16.5.17	/30
	Serial 1/0.3	172.16.5.21	/30
Région1	FastEthernet 0/0	20.20.1.126	/25
	Serial 1/0.1	172.16.5.2	/30
Région2	FastEthernet 0/0	20.20.1.254	/25
	Serial 1/0.1	172.16.5.18	/30
Région3	FastEthernet 0/0	20.20.2.126	/25
	Serial 1/0.1	172.16.5.22	/30
SW_Core	Interface vlan 400	40.40.40.1	/24
	Interface vlan 10	30.30.1.1	/26
	Interface vlan 164	30.30.1.65	/26
	Interface vlan 128	30.30.1.129	/26
	Interface vlan 192	30.30.1.193	/26
	Interface vlan 40	30.30.4.1	/26
Routeur_Intraville	FastEthernet 0/0	30.30.4.3	/26
	Serial 1/0	172.16.5.13	/30
Routeur_Intranet	FastEthernet 0/0	30.30.4.4	/26
	Serial 1/0	172.16.5.5	/30
Routeur_Ministere	FastEthernet 0/0	20.21.1.62	/26
	Serial 1/0	172.16.5.6	/30
Routeur_Proxy	FastEthernet 0/0	30.30.4.5	/26
	Serial 1/0	172.16.5.25	/30
Routeur_VPN	FastEthernet 0/0	172.16.5.10	/30
	Serial 1/0	172.16.11.1	/30
Routeur_Internet	FastEthernet 0/0	30.30.4.6	/26
	FastEthernet 1/0	172.16.5.9	/30
	Serial 2/0	172.16.5.29	/30

Périphérique	Interface	Adresse IP	Masque
Routeur_ACL	Serial 2/0	172.16.5.33	/30
	FastEthernet 0/1	30.30.4.7	/26
	FastEthernet 1/0	40.40.40.254	/24
Routeur_Maison	FastEthernet 0/0	192.168.11.254	/24
	Serial 1/0	172.16.10.1	/30
Routeur_Trésor	FastEthernet 0/0	20.21.1.126	/26
	Serial 1/0	172.16.5.14	/30
Serveur Web	FastEthernet 0/0	40.40.40.2	/24

Tableau 4.09: *Tableau d'adressage des équipements*

Les configurations du réseau existant sont les suivantes :

- Le réseau dispose aussi d'une zone démilitarisée (DMZ) pour les ressources partagées telles que le serveur d'application (SIGFP) accessible par les autres ministères (Intranet de l'Etat) et via Internet. Le DMZ est ici représenté par le VLAN DataCenter. Une politique de sécurité est définie sur le Routeur_ACL pour la restriction des accès des utilisateurs externes.
- Les différents réseaux locaux virtuels sont indépendants entre eux : utilisation de contrôle de liste d'accès (ACL).
- Le protocole de routage utilisé est EIGRP.
- Le commutateur cœur SW_CORE assure le routage inter-VLAN ainsi que le routage de niveau 3 (EIGRP).
- L'interconnexion avec les routeurs des régions se fait avec des sous-interfaces Frame Relay point-à-point afin que chaque connexion soit son propre sous-réseau.

4.4.5.1 Vérification des configurations pour les VLANs

PC1 (30.30.1.2), PC2 (30.30.1.66), PC3 (30.30.1.130) et PC4 (30.30.1.194) représentent respectivement un hôte du VLAN10, VLAN164, VLAN128 et VLAN192.

La figure (4.05) suivante montre que la communication entre ces VLANs n'est pas autorisée due à l'implémentation d'un contrôle d'accès au niveau de chaque interface VLAN.

Le message ICMP informe que la destination est inaccessible (type : 3) et que la communication est administrativement interdite.

```
PC1> ping 30.30.1.66
*30.30.1.1 icmp_seq=1 ttl=255 time=31.200 ms (ICMP type:3, code:13, Communication administratively prohibited)
30.30.1.66 icmp_seq=2 timeout
*30.30.1.1 icmp_seq=3 ttl=255 time=15.600 ms (ICMP type:3, code:13, Communication administratively prohibited)
30.30.1.66 icmp_seq=4 timeout
*30.30.1.1 icmp_seq=5 ttl=255 time=468.000 ms (ICMP type:3, code:13, Communication administratively prohibited
)

PC1> ping 30.30.1.130
*30.30.1.1 icmp_seq=1 ttl=255 time=249.600 ms (ICMP type:3, code:13, Communication administratively prohibited
)
30.30.1.130 icmp_seq=2 timeout
*30.30.1.1 icmp_seq=3 ttl=255 time=15.600 ms (ICMP type:3, code:13, Communication administratively prohibited)
30.30.1.130 icmp_seq=4 timeout
*30.30.1.1 icmp_seq=5 ttl=255 time=15.600 ms (ICMP type:3, code:13, Communication administratively prohibited)

PC1> ping 30.30.1.194
*30.30.1.1 icmp_seq=1 ttl=255 time=15.600 ms (ICMP type:3, code:13, Communication administratively prohibited)
30.30.1.194 icmp_seq=2 timeout
*30.30.1.1 icmp_seq=3 ttl=255 time=374.401 ms (ICMP type:3, code:13, Communication administratively prohibited)
30.30.1.194 icmp_seq=4 timeout
*30.30.1.1 icmp_seq=5 ttl=255 time=15.600 ms (ICMP type:3, code:13, Communication administratively prohibited)
```

Figure 4.05 : *Communication refusée entre VLANs*

4.4.5.2 Vérification du mappage de Frame Relay

```
Routeur_Region#sh frame-relay map
Serial1/0.1 (up): ip 172.16.5.2 dlci 102(0x66,0x1860), dynamic,
              broadcast,, status defined, active
Serial1/0.2 (up): ip 172.16.5.18 dlci 103(0x67,0x1870), dynamic,
              broadcast,, status defined, active
Serial1/0.3 (up): ip 172.16.5.22 dlci 104(0x68,0x1880), dynamic,
              broadcast,, status defined, active
Routeur_Region#
```

Figure 4.06 : *Mappage de Frame Relay*

La commande “show frame-relay map” permet d’afficher les configurations des différents circuits virtuels entre le routeur du Siège avec ceux des régions : la correspondance entre le DLCI correspondant à chaque sous-interface et l’adresse IP du routeur distant de chaque région.

On a :

- Serial1/0.1 DLCI 102 connecté avec la Région1 172.16.5.2
- Serial1/0.1 DLCI 103 connecté avec la Région2 172.16.5.18
- Serial1/0.1 DLCI 104 connecté avec la Région3 172.16.5.22

4.4.5.3 Vérification des accès au serveur Web

```
PC1> ping 40.40.40.2
84 bytes from 40.40.40.2 icmp_seq=1 ttl=254 time=62.400 ms
84 bytes from 40.40.40.2 icmp_seq=2 ttl=254 time=343.200 ms
84 bytes from 40.40.40.2 icmp_seq=3 ttl=254 time=46.800 ms
84 bytes from 40.40.40.2 icmp_seq=4 ttl=254 time=46.800 ms
84 bytes from 40.40.40.2 icmp_seq=5 ttl=254 time=46.800 ms
```

Figure 4.07 : *Accès VLAN10- ServeurWeb*

```
PC6> ping 40.40.40.2
84 bytes from 40.40.40.2 icmp_seq=1 ttl=252 time=93.600 ms
84 bytes from 40.40.40.2 icmp_seq=2 ttl=252 time=343.200 ms
84 bytes from 40.40.40.2 icmp_seq=3 ttl=252 time=93.600 ms
84 bytes from 40.40.40.2 icmp_seq=4 ttl=252 time=78.000 ms
84 bytes from 40.40.40.2 icmp_seq=5 ttl=252 time=93.600 ms
```

Figure 4.08 : *Accès Région1-ServeurWeb*

```
PC10> ping 40.40.40.2
84 bytes from 40.40.40.2 icmp_seq=1 ttl=252 time=546.001 ms
84 bytes from 40.40.40.2 icmp_seq=2 ttl=252 time=109.200 ms
84 bytes from 40.40.40.2 icmp_seq=3 ttl=252 time=109.200 ms
84 bytes from 40.40.40.2 icmp_seq=4 ttl=252 time=109.200 ms
84 bytes from 40.40.40.2 icmp_seq=5 ttl=252 time=109.200 ms
```

Figure 4.09 : *Accès Trésor-ServeurWeb*

```
PC5> ping 40.40.40.2
84 bytes from 40.40.40.2 icmp_seq=1 ttl=252 time=78.000 ms
84 bytes from 40.40.40.2 icmp_seq=2 ttl=252 time=109.200 ms
84 bytes from 40.40.40.2 icmp_seq=3 ttl=252 time=109.200 ms
84 bytes from 40.40.40.2 icmp_seq=4 ttl=252 time=78.000 ms
84 bytes from 40.40.40.2 icmp_seq=5 ttl=252 time=499.201 ms
```

Figure 4.10 : *Accès Impôt-ServeurWeb*

```
PC7> ping 40.40.40.2
84 bytes from 40.40.40.2 icmp_seq=1 ttl=251 time=436.801 ms
84 bytes from 40.40.40.2 icmp_seq=2 ttl=251 time=93.600 ms
84 bytes from 40.40.40.2 icmp_seq=3 ttl=251 time=93.600 ms
84 bytes from 40.40.40.2 icmp_seq=4 ttl=251 time=93.600 ms
84 bytes from 40.40.40.2 icmp_seq=5 ttl=251 time=124.800 ms
```

Figure 4.11 : *Accès Maison-ServeurWeb*

4.4.5.4 Vérification de la configuration VPN

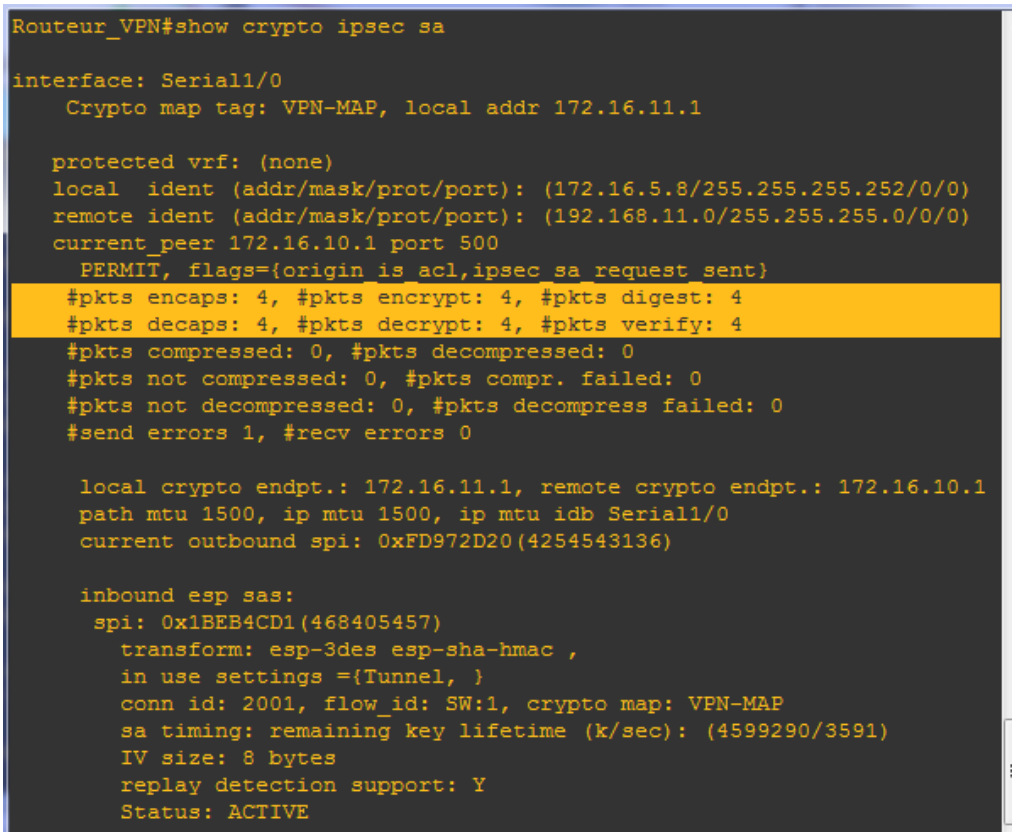


Figure 4.12 : *Résultat après configuration VPN*

On constate qu'après la configuration VPN et après avoir effectué un ping vers le routeur de la maison, la commande « show crypto ipsec sa » informe que le nombre de paquets encryptés a augmenté pour montrer son bon fonctionnement.

4.4.5.5 Vérification de la politique de sécurité au niveau du Routeur_ACL

Un système de pare-feu utilisant ZBP-F (Zone Based-Policy Firewall) a été implémenté au niveau du Routeur_ACL afin de protéger le réseau interne contre toute attaque ou intrusion malveillante. [27]

Trois zones sont alors définies :

- Zone interne : 30.30.0.0 255.255.252.0
- Zone DMZ : 40.40.40.0 255.255.255.0
- Zone Internet : 172.16.5.32 255.255.255.252

Voici les règles établies entre les zones pour la configuration du ZBP-F :

- Les hôtes de la zone interne peuvent accéder à DMZ sur HTTP, FTP, POP, à Internet sur http et HTTPS et ICMP.
- Les hôtes de DMZ ne peuvent accéder à aucune autre zone
- Les hôtes depuis Internet peuvent accéder à DMZ sur HTTP seulement et ils n'ont pas accès à la zone Interne

```
Routeur_ASA#sh policy-map type inspect
  Policy Map type inspect interne-DMZ-policy
    Class interne-DMZ-cmap
      Inspect
    Class class-default

  Policy Map type inspect internet-DMZ-policy
    Class http-acl-cmap
      Inspect
    Class class-default

  Policy Map type inspect interne-internet-policy
    Class interne-internet-cmap
      Inspect
    Class class-default

Routeur_ASA#sh class-map type inspect
 Class Map type inspect match-any interne-DMZ-cmap (id 1)
   Match protocol http
   Match protocol icmp
   Match protocol ftp

 Class Map type inspect match-any http-cmap (id 2)
   Match protocol http

 Class Map type inspect match-all http-acl-cmap (id 3)
   Match access-group  110
   Match class-map http-cmap

 Class Map type inspect match-any interne-internet-cmap (id 4)
   Match protocol http
   Match protocol https
   Match protocol icmp
```

Figure 4.13 : *Politiques établies pour les différentes zones*

4.5 Détermination des points faibles du réseau

L'analyse de l'état du réseau existant nous permet de considérer les points faibles suivants :

- L'architecture ne répond pas aux critères de normalisation et de performance: elle ne dispose pas des trois couches cœur, distribution, accès du modèle hiérarchique. Bien que fonctionnelle, cette architecture actuelle peut vite rencontrer des problèmes au niveau de l'extensibilité, de la gestion mais surtout au niveau des performances du réseau.

- Le commutateur SW_Core constitue un point unique de défaillance ou SPOF (Single Point Of Failure) ; en effet, le fonctionnement du réseau et du reste des équipements dépendent de cet élément et dont la panne va entraîner l'arrêt du système complet.
- Le commutateur SW_CORE exécute trop de tâches pour lui seul : le filtrage de paquet avec des ACL, le routage inter-VLAN, le routage de niveau 3 utilisant le protocole de routage.
  Un inconvénient de l'ACL est le fait que pour chaque paquet, le routeur doit vérifier séquentiellement la correspondance de celui-ci avec les critères définis. Ce traitement peut s'avérer long suivant le nombre de conditions établies.
  De même, l'opération de routage prend également un certain temps lors de la consultation de la table de routage pour chaque paquet reçu. Un temps de réponse élevé au niveau du commutateur peut entraîner des pertes de paquets.
  Ainsi, effectuées par un seul équipement, ces différentes tâches affectent la performance du réseau en termes de latence et de fiabilité. En effet on peut démontrer ceci par la formule du délai de la formule (2.05) donnée par :

$$\text{Latence} = T_T + T_P + T_A$$

  Avec T_T la durée de transmission, T_P la durée de propagation et T_T le temps d'attente.
  Comme le temps d'attente T_T correspond au temps "perdu" par le système de communication notamment à cause de l'occupation des ressources; plus les tâches effectuées par le commutateur SW_CORE sont nombreuses plus ce temps d'attente T_A augmente entraînant ainsi une latence élevée du réseau.
- Il n'y a pas de système de redondance de liaisons et d'équipements pour assurer la haute disponibilité du réseau.

4.6 Optimisation des performances réseaux

4.6.1 Solutions proposées face aux différents points faibles détectés

4.6.1.1 Mise en place de l'architecture hiérarchique du réseau

La première modification consiste à mettre en place les trois couches : couche cœur, couche de distribution et couche d'accès, au sein du réseau pour assurer sa facilité de mis en œuvre, sa facilité de dépannage, la prévisibilité de son comportement, son extensibilité et sa facilité de gestion.
Cette architecture va permettre aussi de bien répartir les tâches au niveau de chaque couche pour améliorer les temps de réponse du système. Rappelons, ici, les fonctions des trois couches :

- Couche d'accès : fournir aux utilisateurs un accès de première ligne aux services réseau (structures de création de noms, architecture de réseau local virtuel).
- Couche de distribution : filtrage et gestion des flux de trafic , mise en application des stratégies de contrôle d'accès, résumé des routes avant notification à la couche cœur de réseau, isolation de la couche cœur de réseau par rapport aux pannes ou interruptions de service de la couche d'accès, routage entre les réseaux locaux virtuels de la couche d'accès.
- Couche Cœur : fournir une connectivité haute vitesse, les transferts de données entre une section du réseau et une autre sont donc efficaces et très rapides.

4.6.1.2 Mise en place d'une stratégie de redondance et d'équilibrage de charge au sein du réseau

Associée à l'architecture hiérarchique, la redondance physique des éléments actifs du réseau permet de mettre en place des principes de hautes disponibilités au sein d'un système d'information. L'utilisation de protocoles permettant de gérer automatiquement les transitions, les répartitions de la charge ainsi que la tolérance de panne est alors nécessaire.

Il existe trois protocoles de redondance de niveau 3 :

- HSRP (Host Standby Routing Protocol) : c'est un protocole propriétaire aux équipements Cisco, dit protocole de « continuité de service ». HSRP sert à augmenter la tolérance de panne sur le réseau en créant un routeur virtuel à partir de deux (ou plus) routeurs physiques : un "actif" et l'autre (ou les autres) "en attente" (ou "standby") en fonction des priorités accordées à chacun de ces routeurs. [28]
- VRRP (Virtual Router Redundancy Protocol) : c'est un protocole standard défini dans la RFC 5789. VRRP est, à l'instar de HSRP, également un protocole qui fournit une solution de continuité de service principalement pour la redondance de passerelles par défaut. Il présente l'avantage d'être compatible aux routeurs non Cisco. [28] [29]
- GLBP (Gateway Load Balancing Protocol) : c'est est un protocole propriétaire Cisco qui permet de faire la redondance ainsi que la répartition de charge sur plusieurs routeurs utilisant une seule adresse IP virtuelle et plusieurs adresses MAC virtuelles. [30]

Comme les équipements utilisés sont tous propriétaires Cisco et pour une utilisation optimale des ressources, il est donc convenable d'utiliser le protocole GLBP dans notre nouvelle architecture.

Abordons brièvement son principe de fonctionnement.

GLBP reprend les concepts de base de HSRP et VRRP. Contrairement à ces 2 protocoles, tous les routeurs du groupe GLBP participent activement au routage alors que dans VRRP ou HSRP, il n'y

qu'un seul routeur qui est en mode actif, tandis que les autres patientent. Plus concrètement, à l'intérieur du groupe GLBP, le routeur ayant la plus haute priorité ou la plus haute adresse IP du groupe prendra le statut de « AVG » (Active Virtual Gateway). Ce routeur va intercepter toutes les requêtes ARP effectuées par les clients pour avoir l'adresse MAC de la passerelle par défaut, et grâce à l'algorithme d'équilibrage de charge préalablement configuré, il va renvoyer l'adresse MAC virtuelle d'un des routeurs du groupe GLBP. C'est d'ailleurs le Routeur AVG qui va assigner les adresses MAC virtuelles aux routeurs du groupe, ces derniers ont le statut « AVF » (Active Virtual Forwarder). Un maximum de 4 adresses MAC virtuelles est défini par groupe, les autres routeurs ont des rôles de backup en cas de défaillance des AVF.

Les routeurs communiquent entre eux par multicast (224.0.0.102) en s'échangeant des messages HELLO. Si l'un d'eux manque à l'appel il disparaît de la rotation au niveau des réponses ARP et si c'est l'AVG qui disparaît, c'est le meilleur AVF qui prendra sa place

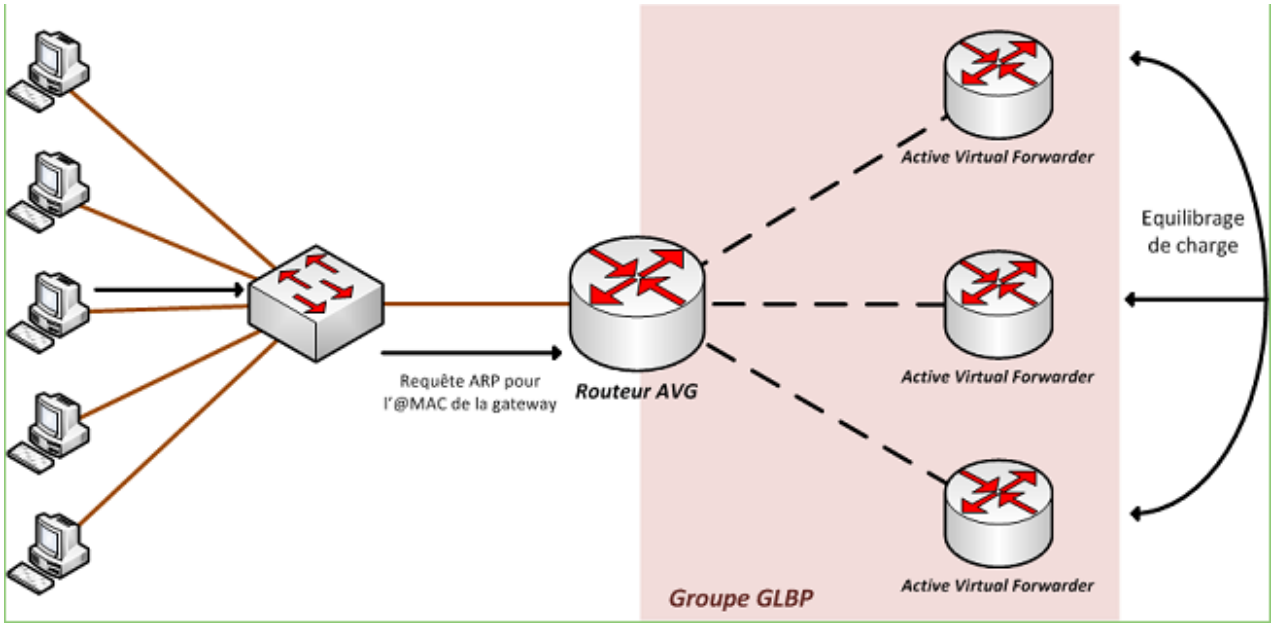


Figure 4.14 : *Fonctionnement du GLBP*

GLBP propose trois modes d'équilibrage de charge :

- Round Robin (le mode par défaut) : pour chaque requête ARP, on renvoie l'adresse Mac virtuelle immédiatement disponible. En d'autres termes, la réponse ARP se fait par tour entre les routeurs du groupe.
- Weighted : le poids de chaque interface du groupe GLBP définit la proportion de trafic à envoyer sur chaque routeur.

- Host-dependent : chaque client générant une requête ARP recevra toujours la même adresse Mac virtuelle.

Pour renforcer la partage de charges au niveau de tous les équipements redondants afin d'améliorer les temps de réponse et d'éviter des goulots d'étranglement, nous avons utilisé le protocole de routage EIGRP pour équilibrer les charges. Le mode d'équilibrage utilisé est l'équilibrage par paquet.

4.6.1.3 Optimisation au niveau WAN

a) Mise en place de la solution PfR au niveau du Routeur_Région

La Direction du Système d'information a un projet de mise à niveau du réseau de MFB en implémentant un système de Backup au niveau des liaisons WAN. Ceci nous permet alors d'adopter la solution de Cisco Performance Routing PfR au niveau du Routeur_Région afin d'optimiser les performances des trafics qui y circulent. De plus, on dispose également d'un routeur 3945 qui peut remplacer le Routeur_Région actuel (un routeur 1841) pour supporter cette technologie PfR.

Pour démontrer les fonctionnalités et les possibilités offertes par PfR, nous allons illustrer deux scénarios. Le premier scénario consiste à démontrer la capacité de PfR à prendre en compte l'état des liaisons de sortie afin qu'un équilibrage de charge puisse être effectué en fonction de leur utilisation ; en effet, sans PfR, un partage de charge peut se faire mais ceci ne prenant pas en compte de l'utilisation réelle des liaisons. Le second consiste à identifier les trafics Telnet et voix et de les contrôler dans le but de les optimiser. Nous avons choisi le trafic voix car c'est l'une des applications qui est extrêmement sensible aux besoins en matière de retard de paquets, de la gigue et qui nécessite les meilleurs traitements pour satisfaire la qualité de service.

Dans chaque scénario, nous allons utiliser des différentes architectures PfR : dans le premier cas, nous allons mettre en place un routeur MC avec deux routeurs BR ; dans le second, le MC et le BR vont être implantés dans le même routeur.

b) Sécurisation du protocole EIGRP

Une deuxième optimisation au niveau du WAN est la sécurisation des protocoles EIGRP afin que seuls les routeurs configurés avec la clé de chiffrement puissent effectuer des échanges de mises à jour de routage. En effet, sans authentification configurée, si une personne non autorisée introduit un autre routeur présentant des informations concernant la route différentes ou conflictuelles sur le réseau, les tables de routage sur les routeurs légitimes peuvent se corrompre et entraîner une attaque DoS. Pour ce faire, le protocole EIGRP prend en charge l'authentification des protocoles de routage

à l'aide du MD5 (Message Digest 5) et toutes les interfaces dans lesquelles le protocole EIGRP est activé doivent être configurées pour prendre en charge cette authentification.
Ceci est donc fait dans le but de réduire les vulnérabilités du réseau face aux éventuelles attaques externes du siège et de renforcer les politiques de sécurité déjà en place.

4.6.2 Implémentation des solutions sous GNS3

4.6.2.1 Nouvelle topologie du réseau

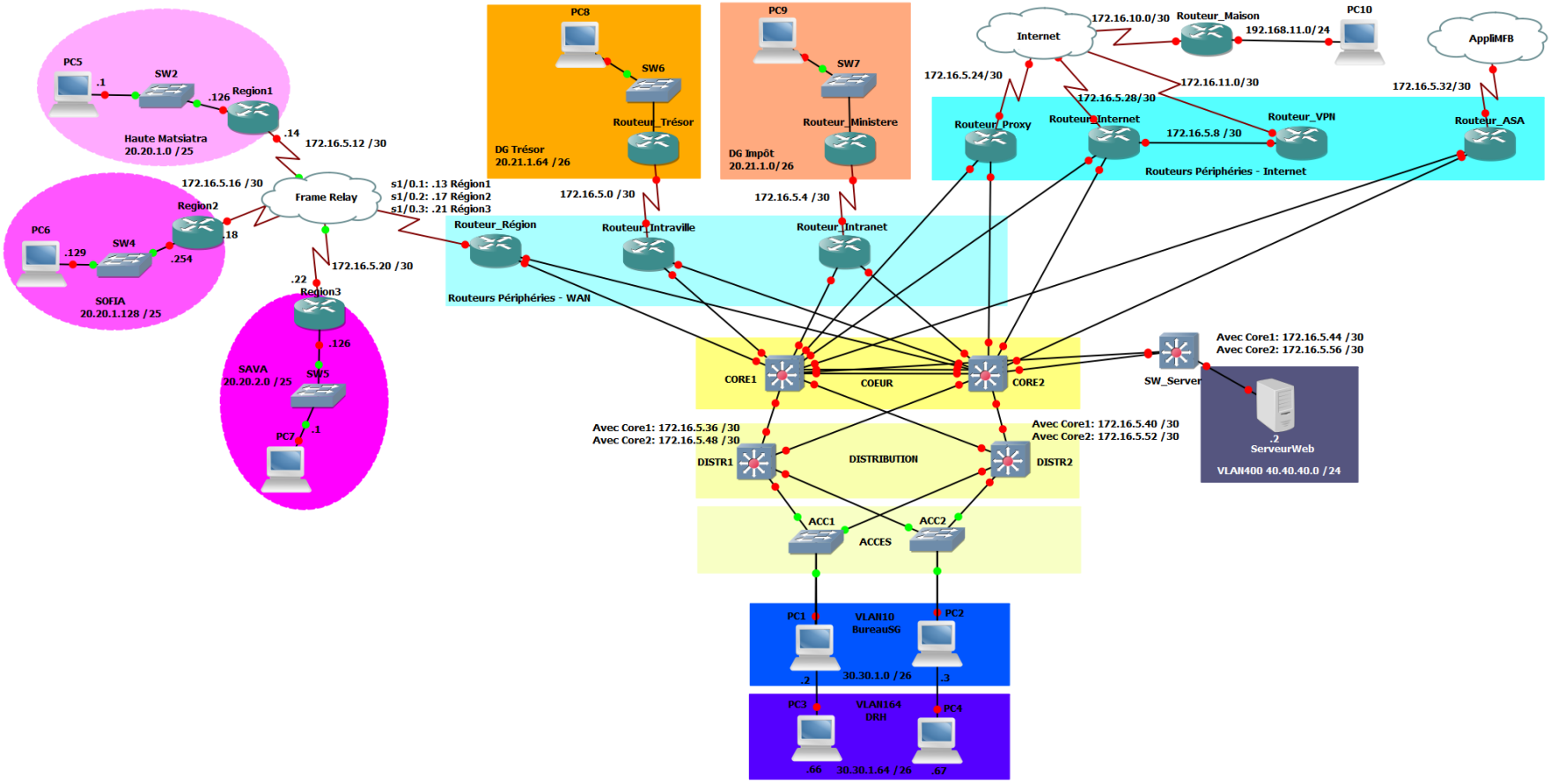


Figure 4.15 : *Nouvelle topologie du réseau*

Cette nouvelle topologie propose l'architecture à trois couches (couche d'accès, couche de distribution et couche Cœur) associée à une stratégie de redondance de liaisons et d'équipements.

4.6.2.2 Vérification de la stratégie de redondance et d'équilibrage de charge au sein du réseau

La figure (4.16) représente l'architecture hiérarchique du réseau associée à une stratégie de redondance des équipements et des liaisons.

Nous avons mis en place le protocole GLBP au niveau de la couche de Distribution, plus précisément au niveau des interfaces VLAN des commutateurs de distribution.

Les routeurs DISTR1 et DISTR2 appartiennent donc au groupe « glbp 1 » pour le VLAN 10 et au groupe « glbp 2 » pour le VLAN 164 ; nous avons désigné DISTR1 comme AVG (Active Virtual Gateway) en lui attribuant la priorité la plus élevée 255 (la valeur par défaut étant 100) et DISTR2 comme AVF (Active Virtual Forward). DISTR1 va donc se charger de répondre aux requêtes ARP pour l'adresse IP virtuelle et de fournir, avec la sienne, l'adresse MAC de DISTR2 pour l'équilibrage de charge. Les adresses IP virtuelles sont respectivement 30.30.1.1 et 30.30.1.65 pour les VLAN 10 et VLAN 164. Le mode d'équilibrage de charge utilisé est le mode « Round Robin ».

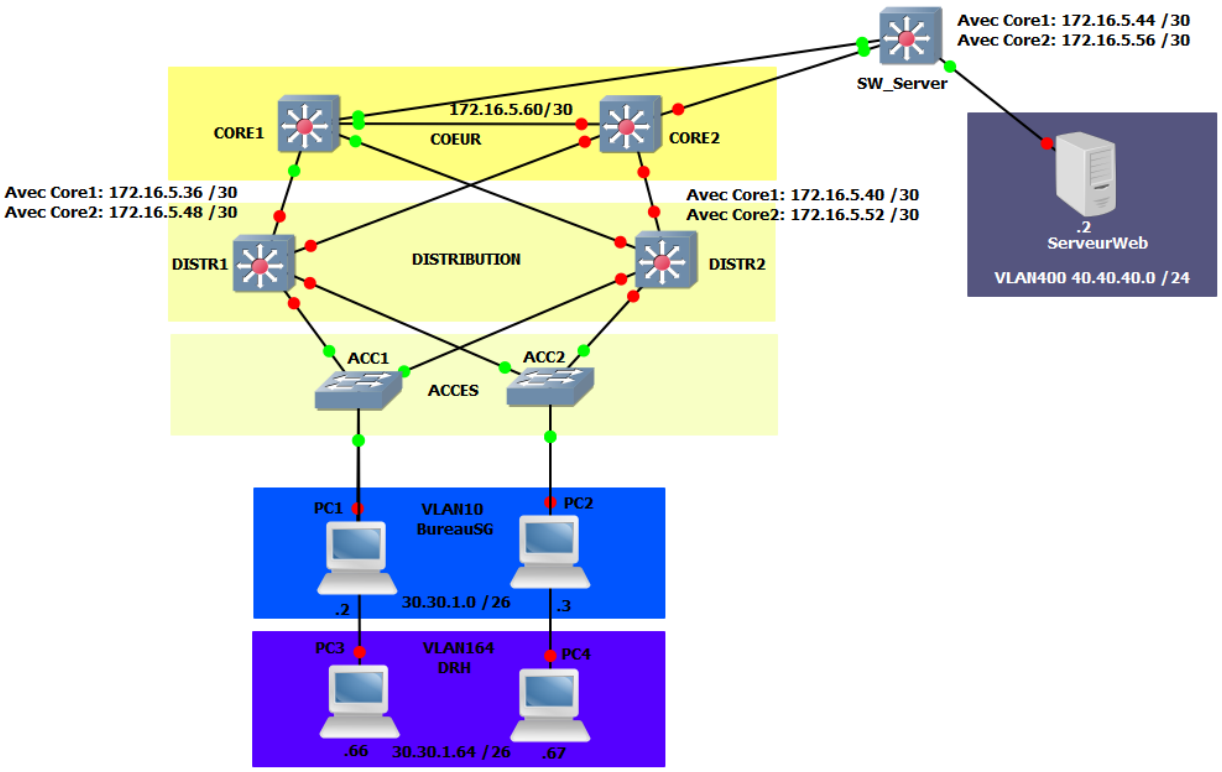


Figure 4.16 : *Architecture hiérarchique du réseau*

La commande « show glbp » permet de vérifier notre configuration.

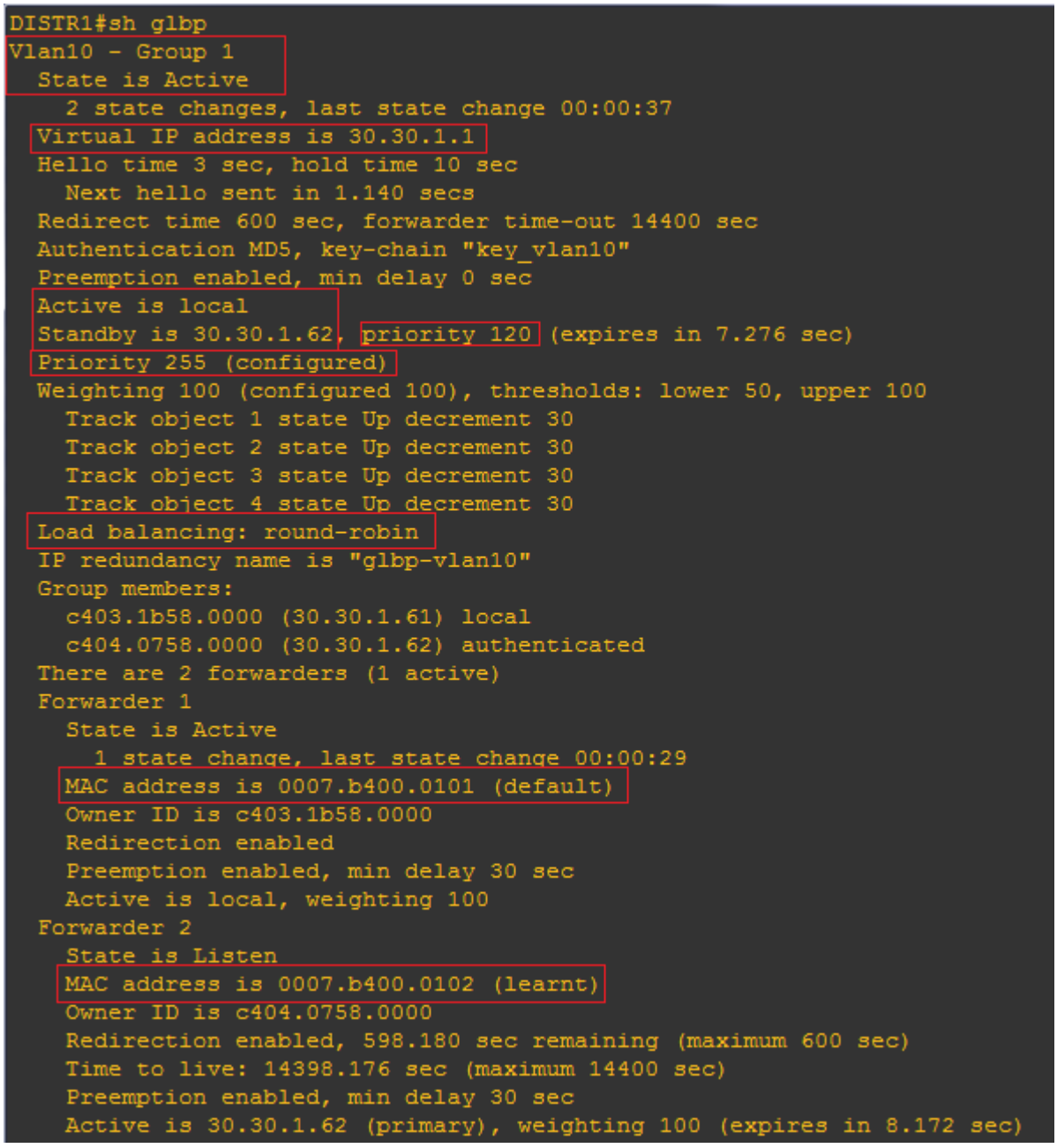


Figure 4.17 : *Vérification de configuration de GLBP sur DISTR1 pour le VLAN 10*

Cette figure (4.17) nous renseigne donc que DISTR1 prend le rôle d'AVG (« State is Active » et « Active is local ») avec une priorité 255, et que DISTR2 est l'AVF (« Standby is 30.30.1.62 », cette adresse étant l'adresse IP réelle de l'interface VLAN 10 de DISTR2) avec une priorité 120 ; l'adresse IP virtuelle du groupe GLBP 1 est 30.30.1.1 pour le VLAN 10 ; le mode d'équilibrage de charge est le Round Robin (« Load-balancing : round-robin ») ; les adresses mac virtuelles de DISTR1 et DISTR2 sont respectivement 0007.b400.0101 (« default »), 0007.b400.0102 (« learnt »).

On obtient la même configuration pour le VLAN 164 mais avec une adresse IP virtuelle 30.30.1.65 pour le groupe GLBP 2 et les adresses mac virtuelles sont respectivement 0007.b400.0201 (« default »), 0007.b400.0202 (« learnt »).

```
Vlan164 - Group 2
  State is Active
    2 state changes, last state change 00:00:41
  Virtual IP address is 30.30.1.65
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 0.588 secs
  Redirect time 600 sec, forwarder time-out 14400 sec
  Authentication MD5, key-chain "key_vlan164"
  Preemption enabled, min delay 0 sec
  Active is local
  Standby is 30.30.1.126, priority 120 (expires in 9.672 sec)
  Priority 255 (configured)
  Weighting 100 (default 100), thresholds: lower 1, upper 100
  Load balancing: round-robin
  IP redundancy name is "glbp-vlan164"
  Group members:
    c403.1b58.0000 (30.30.1.125) local
    c404.0758.0000 (30.30.1.126) authenticated
  There are 2 forwarders (1 active)
  Forwarder 1
    State is Active
      1 state change, last state change 00:00:33
    MAC address is 0007.b400.0201 (default)
    Owner ID is c403.1b58.0000
    Redirection enabled
    Preemption enabled, min delay 30 sec
    Active is local, weighting 100
  Forwarder 2
    State is Listen
    MAC address is 0007.b400.0202 (learnt)
    Owner ID is c404.0758.0000
    Redirection enabled, 597.992 sec remaining (maximum 600 sec)
    Time to live: 14397.988 sec (maximum 14400 sec)
    Preemption enabled, min delay 30 sec
    Active is 30.30.1.126 (primary), weighting 100 (expires in 7.984 sec)
```

Figure 4.18 : *Vérification de configuration de GLBP sur DISTR1 pour le VLAN 164*

Vérifions maintenant le partage de charge entre DISTR1 et DISTR2 en utilisant le mode Round Robin. Pour cela, nous avons fait deux « ping » successifs venant des 2 hôtes (PC1 et PC2) du VLAN10 et la table ARP de ces 2 hôtes vont nous renseigner des routeurs qui ont pris en charge les réponses de leurs requêtes.

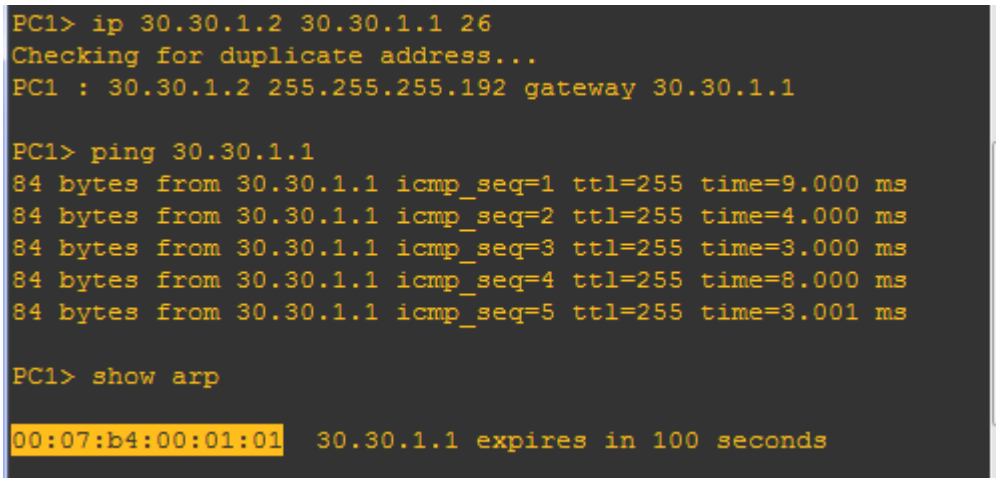


Figure 4.19 : *Vérification du partage de charge sur PC1*

Cette figure (4.19) montre que la réponse ARP provient de 00 :07 :b4 :00 :01 :01 qui représente l'adresse mac de DISTR1.

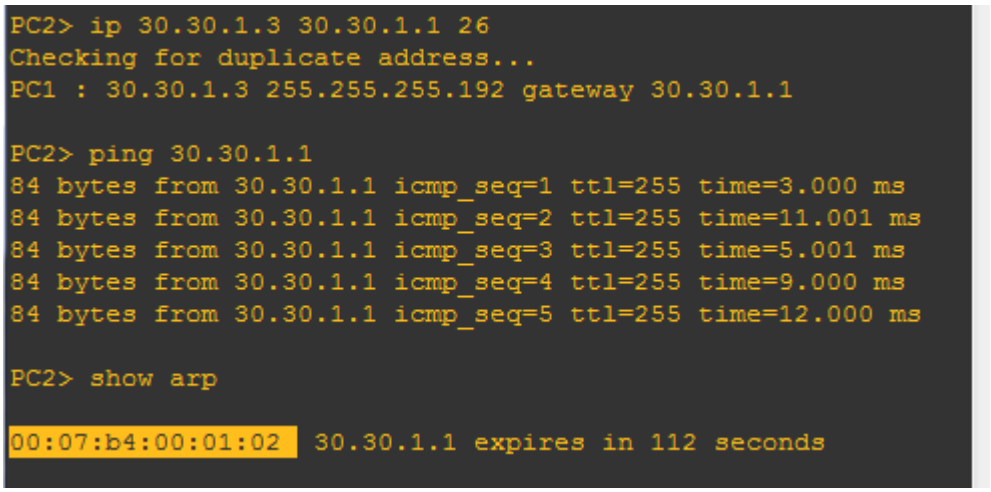


Figure 4.20 : *Vérification du partage de charge sur PC2*

Cette figure (4.20) montre que la réponse ARP provient de 00 :07 :b4 :00 :01 :02 qui représente l'adresse mac de DISTR2.

Ainsi, l'équilibrage de charge entre DISTR1 et DISTR2 est bien effectué en mode Round Robin.

Vérifions ensuite l'équilibrage de charge effectué par le protocole EIGRP en capturant, sous « Wireshark », le trafic sortant de DISTR1 vers les commutateurs CORE1 et CORE2 lors d'un ping vers le serveur web 40.40.40.2. L'équilibrage par paquet est activé en utilisant la commande « ip load-sharing per-packet » sous la configuration des interfaces concernées.

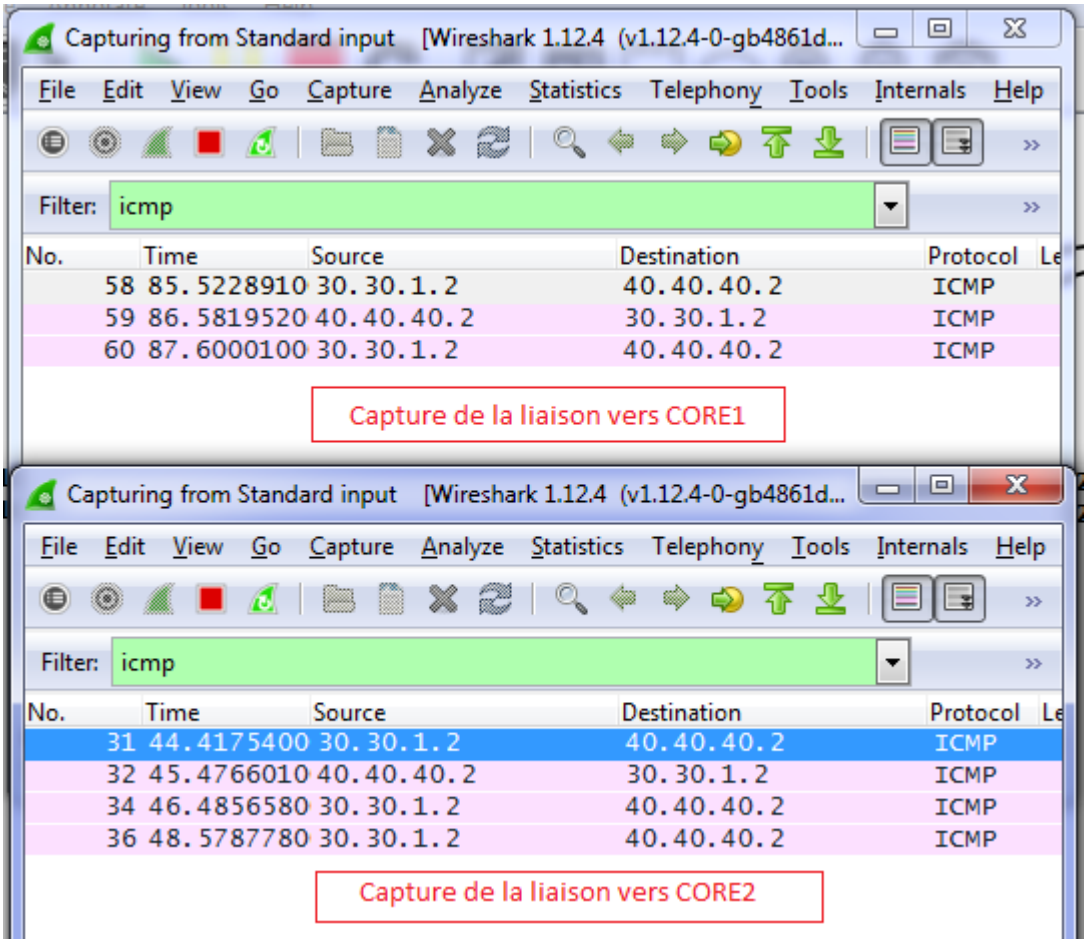


Figure 4.21 : *Capture du trafic sur les liaisons redondantes de DISTR1*

Ainsi, l'équilibrage de charge se fait également au niveau des liaisons redondantes du réseau.

4.6.2.3 Mise en place et vérification de la solution de PfR

a) Scénario 1 : Equilibrage de charge en fonction de l'utilisation de la liaison primaire

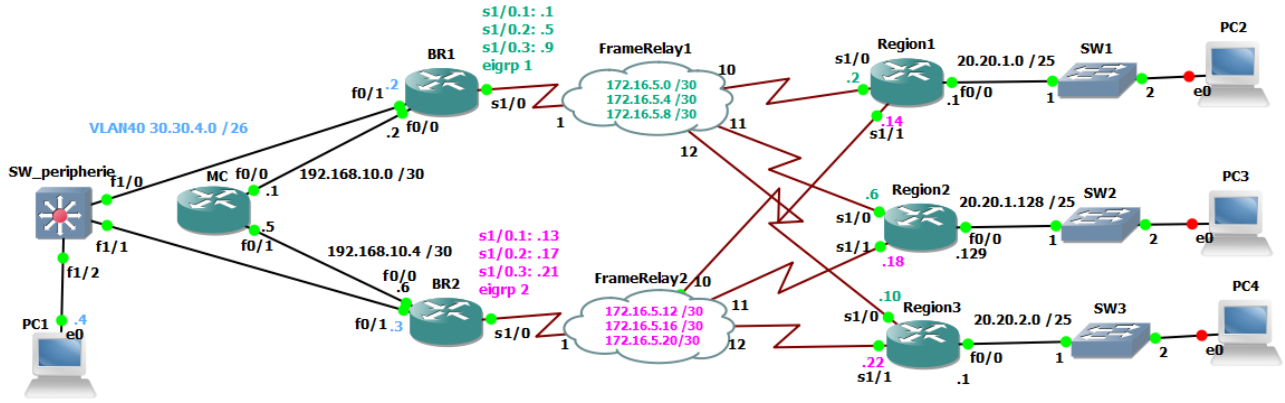


Figure 4.22 : *Topologie étudiée*

Il est à noter que sous des routeurs avec des anciennes versions IOS, le PfR est aussi connu sous le nom d'OER faisant référence à Optimized Edge Routing. Ainsi, il est configuré avec le terme « oer » au lieu de « pfr ». L'IOS du routeur (routeur 7200) disponible sous GNS3 qu'on a utilisé est de version 15.0(1) M et supporte encore OER.

L'architecture de PfR de la figure (4.22) est constituée d'un routeur MC (Master Controller) et de deux routeurs BR (Border Router) qui relient le réseau du Siège avec ceux des régions par deux réseaux WAN qui sont des Frame-Relay dans notre cas.

La liaison principale de 256 Kbits/s est celle utilisant Frame Relay 1 et le backup de 64 Kbits/s est le Frame Relay 2.

Pour chaque BR les interfaces externes sont les sous-interfaces séries Serial 1/0.1, Serial 1/0.2 et Serial 1/0.3 ; l'interface interne est l'interface FastEthernet 0/1 et l'interface locale connectée au MC est l'interface FastEthernet 0/0.

La commande « show oer master border detail » sous MC permet de vérifier ces configurations.

```
MC#show oer master border detail
Border          Status   UP/DOWN            AuthFail  Version
192.168.10.6    ACTIVE   UP       00:00:06          0  3.0
 Se1/0.3        EXTERNAL UP
 Se1/0.2        EXTERNAL UP
 Se1/0.1        EXTERNAL UP
 Fa0/1          INTERNAL UP

 External            Capacity      Max BW   BW Used    Load Status          Exit Id
 Interface             (kbps)      (kbps)    (kbps)    (%)
 ---------           --------      ------   -------  ------- ------          -------
 Se1/0.3         Tx        64          50         0        0 UP                    6
                 Rx                    64         0        0
 Se1/0.2         Tx        64          50         0        0 UP                    5
                 Rx                    64         0        0
 Se1/0.1         Tx        64          50         0        0 UP                    4
                 Rx                    64         0        0
------------------------------------------------------------------------------------
---
Border          Status   UP/DOWN            AuthFail  Version
192.168.10.2    ACTIVE   UP       00:00:09          0  3.0
 Se1/0.3        EXTERNAL UP
 Se1/0.2        EXTERNAL UP
 Se1/0.1        EXTERNAL UP
 Fa0/1          INTERNAL UP

 External            Capacity      Max BW   BW Used    Load Status          Exit Id
 Interface             (kbps)      (kbps)    (kbps)    (%)
 ---------           --------      ------   -------  ------- ------          -------
 Se1/0.3         Tx       256           5         0        0 UP                    3
                 Rx                   256         0        0
 Se1/0.2         Tx       256           5         0        0 UP                    2
                 Rx                   256         0        0
 Se1/0.1         Tx       256           5         0        0 UP                    1
                 Rx                   256         0        0
```

Figure 4.23 : *Détails des Border Router*

Notre attente dans ce scénario est le changement automatique de route vers le backup lorsque l'utilisation de la liaison primaire atteint un seuil (75% par défaut), ici on l'a défini à 5% pour une réaction rapide de notre système.

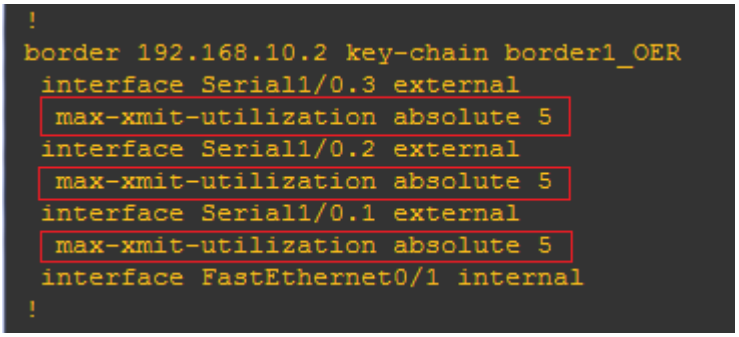


Figure 4.24 : *Seuil d'utilisation des liaisons externes*

Pour ce faire, nous avons configuré les cinq phases de PfR. La phase d'apprentissage doit d'abord être activée, dans notre cas nous avons choisi l'apprentissage automatique des préfixes par ordre de débit et délai élevé car on veut prendre en compte de tous les trafics. On peut vérifier cette configuration par la commande « show oer master ».

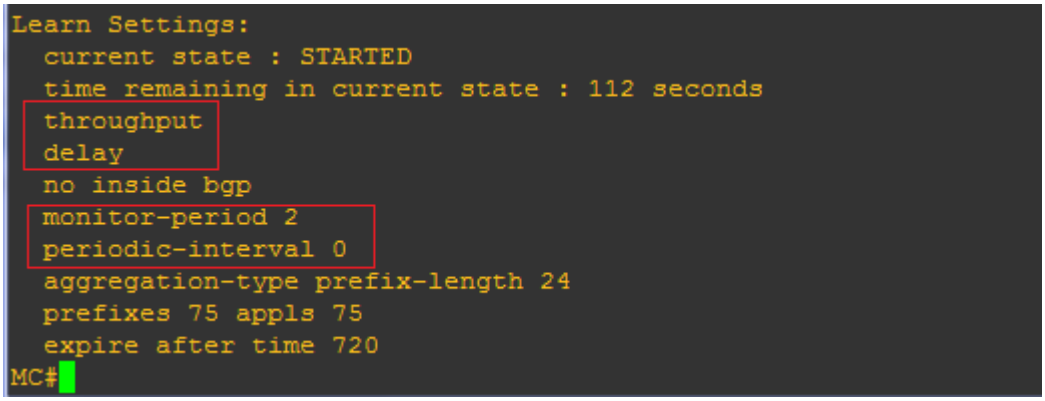


Figure 4.25 : *Paramètres d'apprentissage*

La valeur de monitor-period indique le temps durant lequel MC va effectuer l'apprentissage (ici 2 minutes) et la valeur de periodic-interval indique l'intervalle de temps entre chaque apprentissage (ici, elle sera fera donc en continu). La figure (4.26) suivante indique que la phase d'apprentissage a commencé.

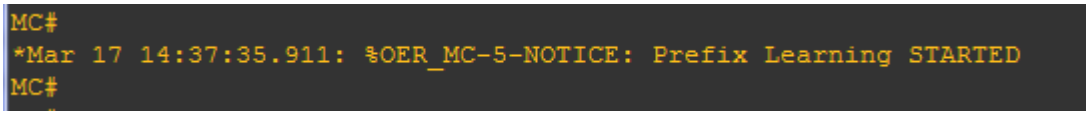


Figure 4.26 : *Début de la phase d'apprentissage*

Pour effectuer le partage de charge, un seuil sur la différence entre l'utilisation des deux liaisons externes est aussi spécifié (ici fixé à 2% pour une réaction rapide).

Pour la phase de mesure, nous avons utilisé le monitoring passif et actif ensemble (défini par « mode monitor both ») pour obtenir plus de précision. La politique sur la différence d'utilisation de liaison (« range ») sera analysée en priorité 1, suivie ensuite de la politique d'utilisation de liaison. La priorisation d'une politique par rapport à une autre est définie par la commande « resolve » suivi de la valeur de la priorité « priority X », avec X la valeur de la priorité. La phase de contrôle est activée par la commande « mode route control » et « mode select best-exit ».

La configuration des phases de mesure, d'application de politique et celle de contrôle est aussi indiquée par la commande show oer master.

```
Global Settings:
  max-range-utilization percent 2 recv 20
  mode route metric bgp local-pref 5000
  mode route metric static tag 5000
  trace probe delay 1000
  logging
  exit holddown time 60 secs, time remaining 0

Default Policy Settings:
  backoff 300 3000 300
  delay relative 50
  holddown 300
  periodic 0
  probe frequency 56
  number of jitter probe packets 100
  mode route control
  mode monitor both
  mode select-exit best
  loss relative 10
  jitter threshold 20
  mos threshold 3.60 percent 30
  unreachable relative 50
  resolve range priority 1 variance 0
  resolve utilization priority 2 variance 15
  resolve delay priority 3 variance 20
```

Figure 4.27 : *Phase de mesure, phase d'application de politique, phase de contrôle*

Toutes les configurations sont alors bien en place. Testons maintenant le comportement de notre système lorsque l'utilisation de la liaison principale atteint ses limites. Pour ce faire, nous allons générer des trafics ICMP en faisant des ping depuis le commutateur SW_peripherie vers le routeur Région2, la taille des paquets sera 1400 octets, le ping sera répété 10000 fois et en continu. Ceci est dans le but que l'interface Serial 1/0.2 va dépasser le seuil d'utilisation et de faire apparaitre un évènement OOP sur le critère « range » définissant la différence entre l'utilisation des deux liaisons.

La commande sous SW_peripherie sera alors : « ping 20.20.1.129 size 1400 repeat 10000 timeout 0 ». Ensuite, nous allons aussi envoyer des ping depuis PC1 du Siège vers le routeur Région2. Les trafics doivent alors être routés sur la seconde liaison de backup.

La figure (4.28) suivante montre ce qui se passe au niveau du MC lorsqu'il a détecté l'évènement OOP :

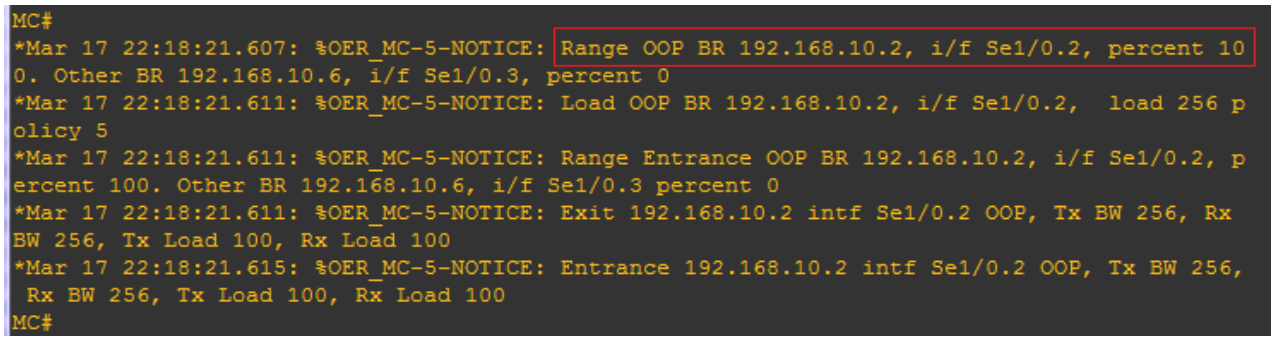


Figure 4.28 : *Evènement OOP du « range » au niveau de Se1/0.2 de BR1*

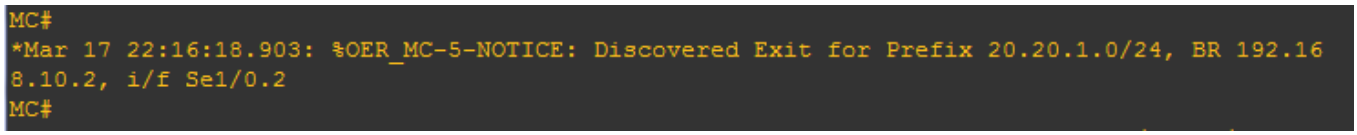


Figure 4.29 : *Découverte de sortie pour le préfixe 20.20.1.0/24*

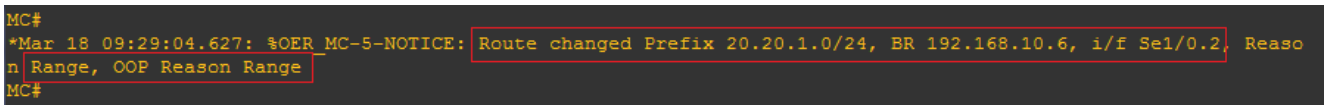


Figure 4.30 : *Découverte de sortie et changement de route pour le préfixe 20.20.1.0/24*

La figure (4.29) signifie que le MC a trouvé une meilleure sortie pour le préfixe 20.20.1.0/24 (à destination de la Région2). La figure (4.30) montre que MC a changé le routage de ce préfixe vers BR2 (192.168.10.6) sur l'interface Se1/0.2.On voit aussi que la raison du changement de route par PfR est le « range » dont on a donné la priorité élevée.

Dans la table de routage du commutateur SW_peripherie, PfR a inséré une route vers BR2 pour le préfixe 20.20.1.0/24 comme le montre la figure (4.31).

```
     20.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
D       20.20.1.0/24 [90/40517120] via 30.30.4.3, 00:19:23, Vlan40
D       20.0.0.0/8 [90/10516992] via 30.30.4.2, 00:19:23, Vlan40
     172.16.0.0/30 is subnetted, 6 subnets
D       172.16.5.16 [90/40514560] via 30.30.4.3, 00:19:23, Vlan40
D       172.16.5.20 [90/40514560] via 30.30.4.3, 00:19:23, Vlan40
D       172.16.5.8 [90/10514432] via 30.30.4.2, 00:19:23, Vlan40
D       172.16.5.12 [90/40514560] via 30.30.4.3, 00:19:23, Vlan40
D       172.16.5.0 [90/10514432] via 30.30.4.2, 00:19:26, Vlan40
D       172.16.5.4 [90/10514432] via 30.30.4.2, 00:19:26, Vlan40
     30.0.0.0/26 is subnetted, 1 subnets
C       30.30.4.0 is directly connected, Vlan40
SW_peripherie#
```

Figure 4.31 : *Insertion d'une route vers BR2 dans la table de routage de SW_Peripherie*

Sous MC, on retrouve les préfixes contrôlés avec le BR courant qui prend la charge de leur sortie ainsi que le protocole utilisé (EIGRP). On utilise pour cela la commande « show oer master prefix ». La figure (4.32) montre notre préfixe 20.20.1.0/24 contrôlé par PfR qui se trouve en état « In Policy » et qui est pris en charge par le BR2.

```
MC#show oer master prefix
OER Prefix Statistics:
 Pas - Passive, Act - Active, S - Short term, L - Long term, Dly - Delay (ms),
 P - Percentage below threshold, Jit - Jitter (ms),
 MOS - Mean Opinion Score
 Los - Packet Loss (packets-per-million), Un - Unreachable (flows-per-million),
 E - Egress, I - Ingress, Bw - Bandwidth (kbps), N - Not applicable
 U - unknown, * - uncontrolled, + - control more specific, @ - active probe all
 # - Prefix monitor mode is Special, & - Blackholed Prefix
 % - Force Next-Hop, ^ - Prefix is denied

Prefix                  State      Time Curr BR         CurrI/F         Protocol
                      PasSDly  PasLDly   PasSUn   PasLUn  PasSLos  PasLLos
                      ActSDly  ActLDly   ActSUn   ActLUn      EBw      IBw
                      ActSJit  ActPMOS  ActSLos  ActLLos
------------------------------------------------------------------------------------
20.20.1.0/24            INPOLICY        0 192.168.10.6     Se1/0.2         EIGRP
                              U         U         0         0         0         0
                              U         U         0         0         1         1
                              N         N
MC#
```

Figure 4.32 : *Préfixe contrôlé par PfR*

On peut aussi vérifier ce partage de charge entre les deux liaisons en faisant des captures de paquets sous Wireshark comme on voit sur la figure (4.33).

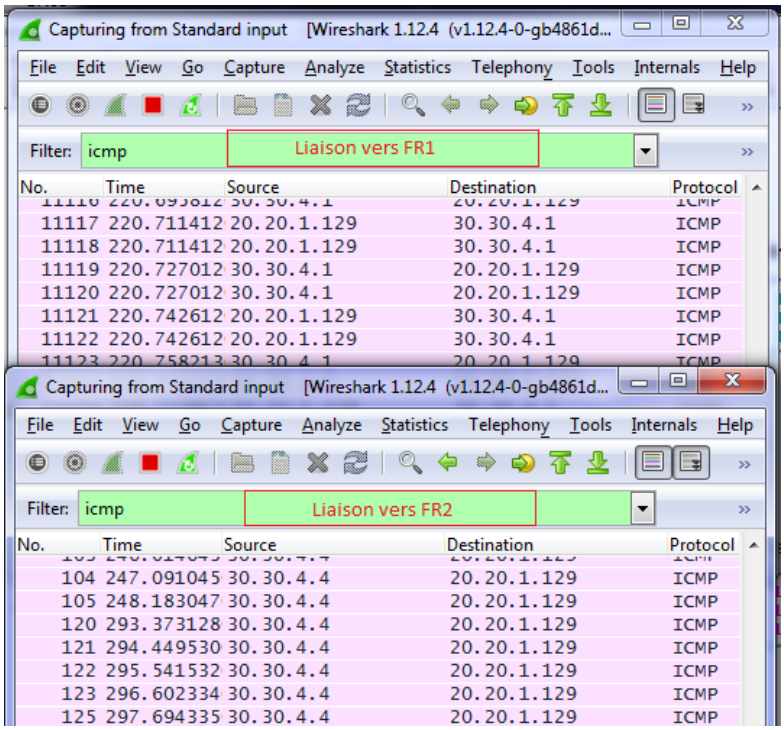


Figure 4.33 : *Capture des paquets sur les liaisons Frame Relay*

b) Scénario 2 : Contrôle du trafic Telnet et optimisation du trafic voix

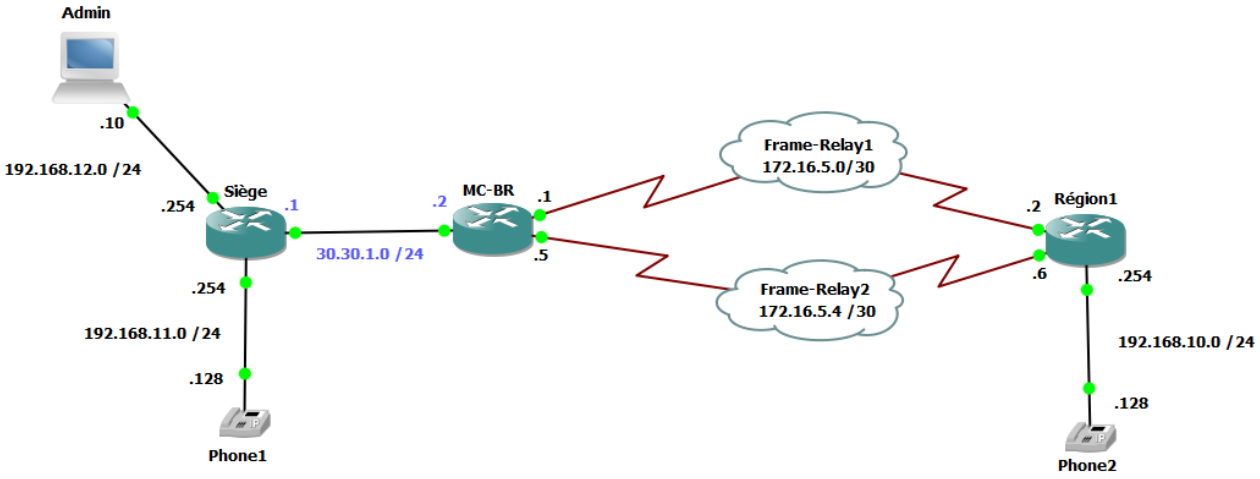


Figure 4.34 : *Topologie du réseau étudié*

Le MC et le BR opèrent sur le même routeur. L'hôte Admin va nous permettre de générer le trafic Telnet. Pour simuler le trafic voix, nous avons mis en place la technologie de VoIP entre le routeur Siège et le routeur Région 1. Pour cela, deux softphones IP ont été installés sous des machines virtuelles.

Les deux routeurs Siège et Région jouent en même temps le rôle de serveurs (contrôleurs d'appel) pour gérer les appels et contrôler la communication et la transmission de la voix.
Le softphone utilisé est le Cisco IP Communicator, les machines virtuelles sont sous Windows XP et le contrôleur d'appel utilisé est le Cisco Unified Communication Manager Express (CME).
Avant d'entrer dans l'optimisation de la voix, nous allons d'abord voir les paramètres affectant sa QoS qui sont le délai de transit, la gigue et la perte de paquets. [31]

- Le délai de transit est le temps moyen que va mettre un paquet IP contenant un échantillon de voix pour traverser l'infrastructure entre deux interlocuteurs. On a :

$$\text{Délai} = D_E + D_P + D_T + D_B \qquad (4.01)$$

Avec D_E le délai d'échantillonnage correspondant à la durée de numérisation de la voix à l'émission puis de conversion en signal voix à la réception, ce temps dépend du type de codec choisi ; D_P le délai de propagation correspondant à la durée de transmission en ligne des données numérisées ; D_T le délai de transport correspondant à la durée passée à traverser les routeurs, les commutateurs et les autres composants du réseau et de l'infrastructure de téléphonie IP ; D_B le délai de Buffers correspondant au retard introduit à la réception en vue de lisser la variation de temps de transit, et donc de réduire la gigue.

- La gigue est la variation du temps de transit, elle est la conséquence du fait que tous les paquets contenant des échantillons de voix ne vont pas traverser le réseau à la même vitesse. Elle peut être de l'ordre de quelques millisecondes à des dizaines de millisecondes.
- La perte de paquets peut être causée par des congestions sur le réseau. Une perte de données régulière mais faible est moins gênante en voix sur IP que des pics de perte de paquets espacés mais élevés. En effet l'écoute humaine s'habituera à une qualité moyenne mais constante et en revanche supportera peu de soudaines dégradations de la QoS.

Le tableau suivant présente les valeurs seuils de ces paramètres critiques et les conséquences constatées pour le niveau de service de VoIP :

Niveau de service	Bon	Moyen	Mauvais
Délai de transit	D < 150 ms	150 ms < D < 400 ms	400 ms < D
Gigue	G < 20 ms	20 ms < G < 50 ms	50 ms < D
Perte de paquets	P < 1%	1% < P < 3%	3% < P

Tableau 4.10: *Valeurs seuils des métriques de performance de la VoIP*

Pour identifier le trafic voix pour notre optimisation, il faut savoir ses caractéristiques.

La transmission de la voix par paquets s'appuie sur le protocole RTP (Real-time Transport Protocol). Ce dernier permet de transmettre sur IP les paquets de voix en reconstituant les informations même si la couche de transport change l'ordre des paquets. Il utilise pour cela des numéros de séquence et s'appuie sur UDP. De plus, en tant qu'application en temps réel les paquets de voix doivent être traités au même débit à mesure de leur envoi ; il n'y a pas de temps pour retransmettre les paquets contenant des erreurs. Par conséquent, la voix sur IP se sert au mieux d'UDP comme d'un protocole de transport, contrairement aux données de transferts qui utilisent les fonctions de contrôle des erreurs et de retransmission de TCP pour résister aux retards et aux pertes de paquets.

Ces différentes notions acquises, passons maintenant à notre second scénario qui est décrit par les points suivants :

- Identifier le trafic Telnet envoyé par l'hôte Admin et le trafic voix entre les deux softphones.
- Le trafic Telnet doit toujours emprunter la liaison de backup utilisant le Frame-Relay2
- Le trafic voix doit emprunter la meilleure liaison qui présentera un délai inférieur à 300 ms et/ou une gigue inférieure à 20 ms pour avoir une bonne qualité. Lorsque le délai sur la route primaire dépasse l'un de ces deux critères de performances, PfR va se charger de router la voix vers la liaison de Backup qui est en accord avec les critères.

Pour prendre le contrôle de ces deux applications, PfR utilise le mécanisme du PBR (Policy-Based Routing) qui va prendre des décisions de routage suivant des stratégies et ignore celles du routage traditionnel mis en place. [26]

Une application est caractérisée par le protocole qu'il utilise, un numéro de port, une adresse source ou de destination. Ainsi, le trafic Telnet est identifié par le protocole de transport TCP au port 23 et le trafic voix par le protocole UDP utilisant les ports entre 16384 et 32767 (intervalle par défaut pour les numéros de port utilisés en VoIP)

Pour mesurer les états du réseau et des liaisons, nous avons utilisé la sonde active « Jitter » entre le MC et le routeur Région1 dans le monitoring actif. Efficace pour la mesure de la qualité de voix, la mesure par cette sonde permet d'obtenir les valeurs du délai, de la gigue, de la perte de paquets et le score MOS allant à la destination de la Région1. On pourra ainsi observer la réaction de notre système régi par PfR à chaque variation de ces valeurs.

Vérifions d'abord les configurations de MC et BR sur le même routeur :

```
MC-BR#show oer master border detail
Border           Status   UP/DOWN             AuthFail  Version
10.10.10.1       ACTIVE   UP       00:04:37          0  2.1
 Se1/1.1         EXTERNAL UP
 Se1/0.1         EXTERNAL UP
 Fa0/0           INTERNAL UP

 External            Capacity      Max BW   BW Used    Load Status          Exit Id
 Interface            (kbps)       (kbps)    (kbps)    (%)
 ---------           --------      ------   ------- ------- ------           ------
 Se1/1.1         Tx       256         192         0       0 UP                    2
                 Rx                   256         0       0
 Se1/0.1         Tx      1544        1158         0       0 UP                    1
                 Rx                  1544         0       0
MC-BR#
```

Figure 4.35 : *Détails du Border Router*

Les interfaces externes sont les interfaces série Serial1/0.1 et Serial1/1.1 ; l'interface interne est l'interface FastEthernet0/0 et l'interface locale pour la communication entre MC et BR est l'interface Loopback0 d'adresse IP 10.10.10.1. La liaison primaire de 1544 Kbits/s est l'interface S1/0.1 et le backup de 256 Kbits/s est l'interface S1/1.1.

Les figures (4.36) et (4.37) présentent les politiques utilisées pour le contrôle de nos trafics, la politique pour la voix a une priorité de 10 et sera traitée en premier, tandis que celle de Telnet a une priorité égale à 20. Chaque trafic est respectivement identifié par les listes de contrôle d'accès étendus nommés VOICE_ACCESS_LIST et TELNET.

```
oer-map TARGET_MAP 10
  sequence no. 8444249301975040, provider id 1, provider priority 30
    host priority 0, policy priority 10, Session id 0
  match ip access-lists: VOICE_ACCESS_LIST
  backoff 180 360 180
 *delay threshold 300
  holddown 300
  periodic 0
 *probe frequency 5
  mode route control
  mode monitor both
 *mode select-exit best
  loss relative 10
 *jitter threshold 20
 *mos threshold 4.00 percent 30
  unreachable relative 50
  next-hop not set
  forwarding interface not set
 *resolve jitter priority 1 variance 10
 *resolve delay priority 2 variance 15
 *resolve mos priority 3 variance 15
 *resolve utilization priority 12 variance 20

  Forced Assigned Target List:
   active-probe jitter 192.168.10.254 target-port 1025 codec g729a
```

Figure 4.36 : *Politique appliquée à la voix*

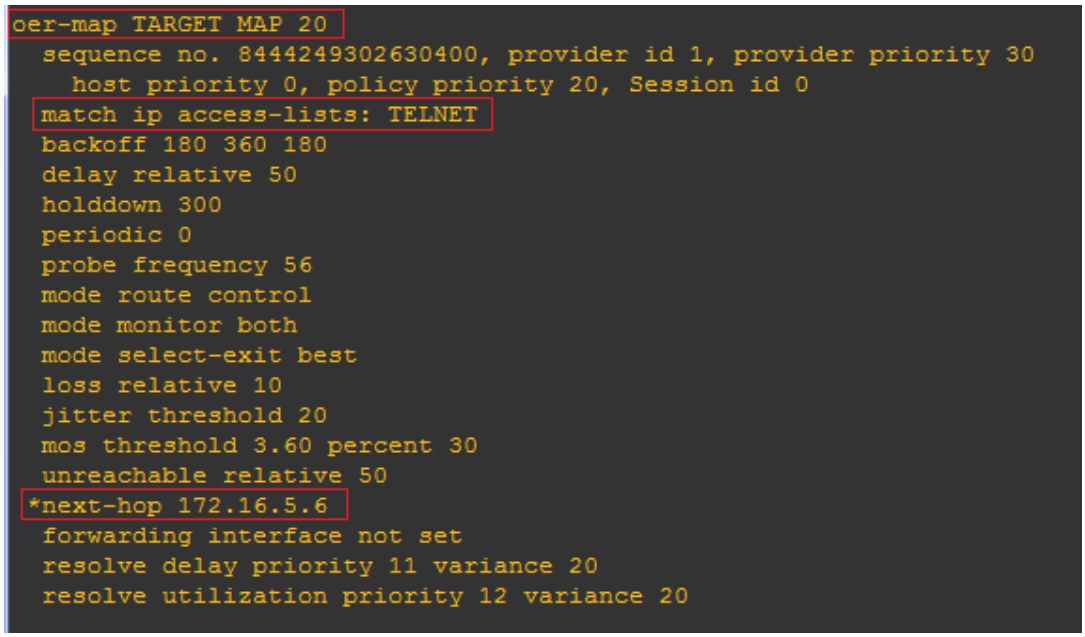


Figure 4.37 : *Politique appliqué au trafic Telnet*

La politique permettant de router le trafic Telnet vers la liaison Backup est le fait d'assigner le prochain saut (routeur) à emprunter à l'adresse 172.16.5.6

La figure (4.38) montre le résultat initial de la mesure de la sonde active Jitter sur les deux liaisons :

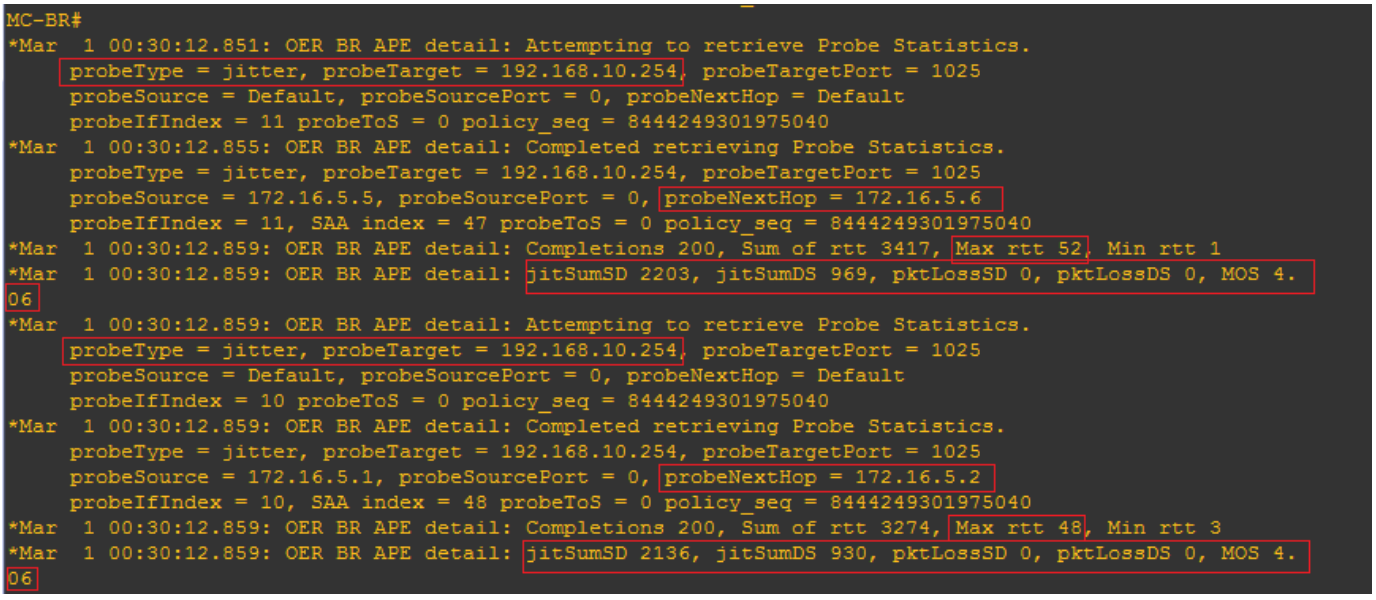


Figure 4.38 : *Mesure par la sonde active Jitter*

Ces mesures nous montrent alors que la liaison primaire sur l'interface S1/0.1 présente un délai RTT de 48ms, une gigue (source-destination) de 10.68 ms (2136/200ms) et une gigue (destination-source) de 4.65ms (930/200 ms), aucune perte de paquets et un score MOS 4.06 tandis que le Backup

dur l'interface S1/1.1 présente un délai RTT de 52 ms, une gigue (source-destination) de 11 ms (2203/200ms) et une gigue (destination-source) de 4.85ms (969/200 ms), aucune perte et un score MOS de 4.06. Notre politique a défini que la gigue prend la priorité par rapport aux autres critères, ainsi le trafic va être routé vers la liaison primaire.

```
*Mar  1 00:30:16.087: %OER_MC-5-NOTICE: Route changed Appl Prefix 172.16.5.0/29 defa 17 [1, 65535] [16
384, 32767], BR 10.10.10.1, i/f Se1/0.1, Reason Jitter, OOP Reason Timer Expired
MC-BR#
```

Figure 4.39 : *Interface S1/0.1 empruntée pour la voix par politique de gigue*

Nos deux applications contrôlées par PfR sont trouvés par la commande « show oer master appl » :

```
R1#sh oer master appl
OER Prefix Statistics:
 Pas - Passive, Act - Active, S - Short term, L - Long term, Dly - Delay (ms),
 P - Percentage below threshold, Jit - Jitter (ms),
 MOS - Mean Opinion Score
 Los - Packet Loss (packets-per-million), Un - Unreachable (flows-per-million),
 E - Egress, I - Ingress, Bw - Bandwidth (kbps), N - Not applicable
 U - unknown, * - uncontrolled, + - control more specific, @ - active probe all
 # - Prefix monitor mode is Special, & - Blackholed Prefix
 % - Force Next-Hop, ^ - Prefix is denied

Prefix                Prot Port [src][dst]/ApplId        DSCP Source Prefix
                         State     Time Curr BR         CurrI/F         Protocol
                       PasSDly  PasLDly   PasSUn   PasLUn  PasSLos  PasLLos
                       ActSDly  ActLDly   ActSUn   ActLUn      EBw      IBw
                       ActSJit  ActPMOS
------------------------------------------------------------------------------
0.0.0.0/0%             tcp [1, 65535] [23, 23]           defa 192.168.11.0/24
                      INPOLICY*        0 10.10.10.1       Se1/1.1         PBR
172.16.5.0/29          udp [1, 65535] [16384, 32767]     defa 0.0.0.0/0
                      INPOLICY         0 10.10.10.1       Se1/0.1         PBR
                             U         U        0        0        0        0
                             U         U        0        0        8        8
                             0         U
```

Figure 4.40 : *Les applications voix et Telnet contrôlées par PfR*

Dans cette figure (4.40), on vérifie bien que Telnet prend bien le chemin (Backup) empruntant l'interface S1/1.1 et la voix prend le celui empruntant l'interface S1/0.1. On vérifie aussi que le routage de ces trafics est bien pris en charge par PBR.

Maintenant, nous allons simuler un retard dans la liaison primaire afin que le routage soit redirigé vers la liaison de Backup. Pour ce faire, nous avons effectué un lissage ou une mise en forme de trafic (Traffic shaping) sur l'interface S1/0.1 afin de retarder la transmission. La figure (4.41) nous montre alors le résultat des mesures effectuées par la sonde Jitter :

```
MC-BR#
*Mar  1 01:39:49.975: OER BR APE detail: Attempting to retrieve Probe Statistics.
     probeType = jitter, probeTarget = 192.168.10.254, probeTargetPort = 1025
     probeSource = Default, probeSourcePort = 0, probeNextHop = Default
     probeIfIndex = 11 probeToS = 0 policy_seq = 8444249301975040
*Mar  1 01:39:49.979: OER BR APE detail: Completed retrieving Probe Statistics.
     probeType = jitter, probeTarget = 192.168.10.254, probeTargetPort = 1025
     probeSource = 172.16.5.5, probeSourcePort = 0, probeNextHop = 172.16.5.6
     probeIfIndex = 11, SAA index = 157 probeToS = 0 policy_seq = 8444249301975040
*Mar  1 01:39:49.983: OER BR APE detail: Completions 200, Sum of rtt 2418, Max rtt 28, Min rtt 3
*Mar  1 01:39:49.983: OER BR APE detail: jitSumSD 1176, jitSumDS 1039, pktLossSD 0, pktLossDS 0, MOS 4.06
*Mar  1 01:39:49.983: OER BR APE detail: Attempting to retrieve Probe Statistics.
     probeType = jitter, probeTarget = 192.168.10.254, probeTargetPort = 1025
     probeSource = Default, probeSourcePort = 0, probeNextHop = Default
     probeIfIndex = 10 probeToS = 0 policy_seq = 8444249301975040
*Mar  1 01:39:49.983: OER BR APE detail: Completed retrieving Probe Statistics.
     probeType = jitter, probeTarget = 192.168.10.254, probeTargetPort = 1025
     probeSource = 172.16.5.1, probeSourcePort = 0, probeNextHop = 172.16.5.2
     probeIfIndex = 10, SAA index = 158 probeToS = 0 policy_seq = 8444249301975040
*Mar  1 01:39:49.983: OER BR APE detail: Completions 13, Sum of rtt 18424, Max rtt 2472, Min rtt 491
*Mar  1 01:39:49.983: OER BR APE detail: jitSumSD 3652, jitSumDS 75, pktLossSD 55, pktLossDS 0, MOS 1.00
MC-BR#
```

Figure 4.41 : *Mesures de la Jitter après simulation de problème*

Cette figure nous montre que la liaison passant par l'interface S1/0.1 présente de très mauvais métriques de performances pour assurer la qualité de la voix car le délai RTT devient 2472 ms, la gigue maximale est de 18.26 ms (3652/200 ms) proche du seuil à 20 ms, une perte de paquets de 55% et un score MOS à 1 ; contrairement à celle passant par l'interface S1/1.1 qui présente une faible délai (28 ms), une gigue de 5.88 ms, aucune perte de paquet et un meilleur score MOS (4.06). Toutes ces raisons réunies amènent alors le PfR à choisir la route idéale pour la voix vers la liaison de Backup.

En revérifiant la commande show oer master appl, nous retrouvons que la voix est désormais routée vers l'interface Serial1/1.1.

```
MC-BR#sh oer master appl
OER Prefix Statistics:
 Pas - Passive, Act - Active, S - Short term, L - Long term, Dly - Delay (ms),
 P - Percentage below threshold, Jit - Jitter (ms),
 MOS - Mean Opinion Score
 Los - Packet Loss (packets-per-million), Un - Unreachable (flows-per-million),
 E - Egress, I - Ingress, Bw - Bandwidth (kbps), N - Not applicable
 U - unknown, * - uncontrolled, + - control more specific, @ - active probe all
 # - Prefix monitor mode is Special, & - Blackholed Prefix
 % - Force Next-Hop, ^ - Prefix is denied

Prefix               Prot Port [src][dst]/ApplId        DSCP Source Prefix
                        State     Time Curr BR         CurrI/F         Protocol
                      PasSDly  PasLDly   PasSUn   PasLUn  PasSLos  PasLLos
                      ActSDly  ActLDly   ActSUn   ActLUn      EBw      IBw
                      ActSJit  ActPMOS
------------------------------------------------------------------------------
0.0.0.0/0%            tcp [1, 65535] [23, 23]           defa 192.168.11.0/24
                     INPOLICY*        0 10.10.10.1      Se1/1.1         PBR
172.16.5.0/29         udp [1, 65535] [16384, 32767]     defa 0.0.0.0/0
                     INPOLICY         0 10.10.10.1      Se1/1.1         PBR
                            U         U        0        0       0        0
                            U         U        0        0      21       21
                            0         U
MC-BR#
```

Figure 4.42 : *Changement de route pour la voix*

Nous pouvons aussi vérifier le contrôle de routage par PBR du trafic Telnet en faisant des captures de paquets sous Wireshark après avoir ouvert une session Telnet depuis l'hôte Admin vers le routeur Région 172.16.5.2 comme le montre la figure (4.43).

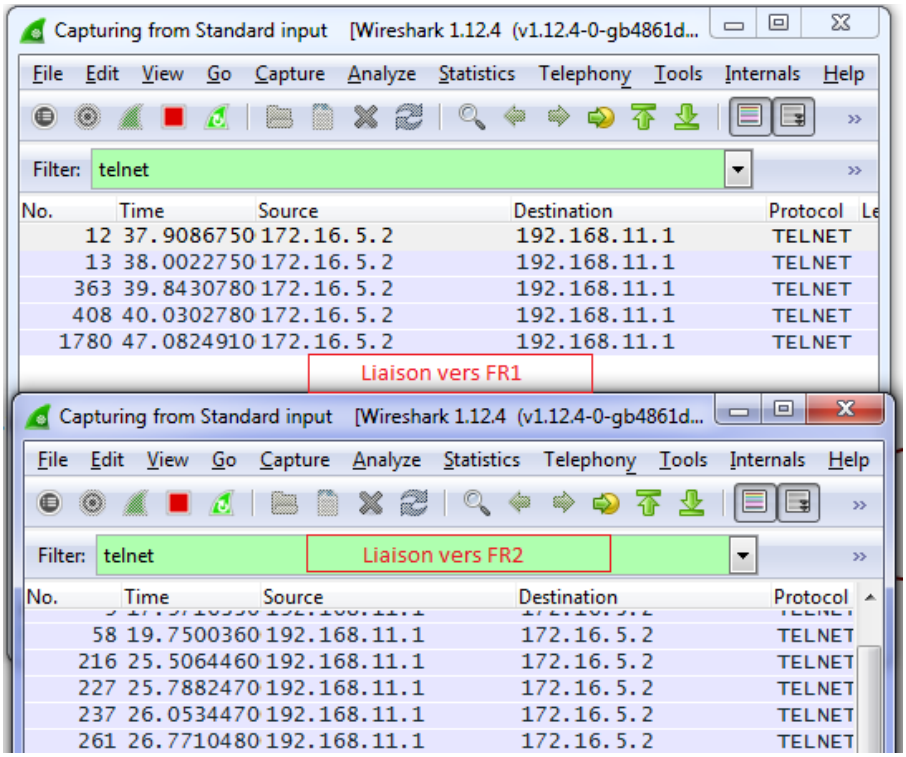


Figure 4.43 : *Capture du trafic Telnet sous Wireshark*

4.6.2.4 Vérification de la sécurisation de EIGRP

Nous avons mis en place la sécurisation d'EIGRP au niveau des routeurs de périphérie en liaison avec les WAN, c'est-à-dire sur les routeurs Régions et le routeur de périphérie du Siège.
La commande « debug eigrp packets » permet de vérifier que seuls les paquets Hello et les mises à jours venant des routeurs possédant la clé de chiffrement sont acceptés et les autres sont ignorés.
Les figures (4.44) et (4.45) affichent les informations données par cette commande.

```
BR1#
*Mar 16 13:07:46.247: EIGRP: received packet with MD5 authentication, key id = 1
*Mar 16 13:07:46.247: EIGRP: Received HELLO on Serial1/0.1 nbr 172.16.5.2
```

Figure 4.44 : *Paquets acceptés avec authentification*

```
*Mar  1 00:50:33.743: EIGRP: Serial1/2: ignored packet from 3.3.3.1, opcode = 5 (missing authentication)
Region3#no debug eigrp packets
EIGRP Packets debugging is off
Region3#
```

Figure 4.45 : *Rejet des paquets venant d'autre routeur*

La figure (4.46) suivante représente un aperçu de l'interface du softphone Cisco IP Communicator durant un appel.

Figure 4.46 : *Aperçu de l'interface de Cisco IP Communicator*

4.7 Conclusion

Dans ce dernier chapitre, nous avons étudié et analysé le réseau actuel du Ministère des Finances et du Budget afin de déterminer les points faibles affectant ses performances, les possibilités à considérer et ainsi proposer des solutions d'optimisation adéquates. La première optimisation concerne la mise à niveau de l'architecture du LAN du Siège et la mise en place de la stratégie de redondance et d'équilibrage de charge pour une meilleure utilisation des ressources, une rapidité et une fiabilité de toute communication. Au niveau du WAN, nous avons proposé la mise en œuvre de PfR (Performance Routing) afin d'optimiser le routage au niveau du routeur de périphérie suivant les applications et l'état des liaisons. La sécurisation du protocole EIGRP a aussi été faite pour minimiser la vulnérabilité du réseau face aux éventuelles attaques (attaque par déni de service ou DoS par exemple).

Nous avons ensuite illustré la mise en place de ces techniques d'optimisation sous le logiciel de simulation GNS3 afin de démontrer leurs efficacités.

CONCLUSION GENERALE

Les performances des réseaux d'entreprises sont d'une importance cruciale. En effet, la fiabilité et la performance du réseau doivent être à la hauteur des enjeux et des besoins de l'entreprise qu'il doit satisfaire.

Nous avons vu les différents indicateurs de performance d'un réseau tels que la latence, la gigue, la perte des paquets, la bande passante qui permettent de définir la qualité de service (QoS) par le réseau.

Afin de satisfaire les attentes des utilisateurs sur l'utilisation du réseau, surdimensionner ce dernier n'est pas toujours la meilleure solution. En effet, à partir d'un cas concret du réseau de MFB, nous avons pu analyser tous les aspects pouvant affecter la performance du réseau actuel et dans le futur. Des améliorations telles que la répartition des différentes tâches sur différents équipements, l'utilisation de protocoles et de techniques pour assurer une meilleure utilisation des ressources ont été identifiées. Ces dernières nous ont amenés à faire une mise à niveau de l'architecture du réseau et une mise en place de la stratégie de redondance et de partage de charge sur différents équipements et liaisons.

Nous avons aussi démontré que la technologie de Performance Routing permet d'optimiser de manière considérable les performances du réseau du fait qu'à partir des bandes passantes existantes du réseau, il peut assurer la qualité de service attendue par les applications critiques telles que la voix. Les mesures passives et actives exécutées par PfR permettent d'exploiter de façon optimale les ressources du réseau.

Un autre aspect bien que minime mais important est le fait de sécuriser le protocole EIGRP afin de diminuer les risques d'attaques au niveau des routeurs de périphérie effectuant le routage.

Les solutions offertes dans ce mémoire permettent donc à toute entreprise disposant des mêmes aspects d'adopter un modèle d'optimisation efficace aux niveaux LAN et WAN.

En termes de perspective, notre étude sur le PfR nous amène à une autre technologie qui est le IWAN ou WAN Intelligent de Cisco qui consiste à déployer une solution de transport WAN avec un contrôle intelligent des chemins de réseau, une optimisation des applications et des communications cryptées et sécurisées en succursales tout en réduisant les coûts d'exploitation du WAN. Il est basé sur l'utilisation des services Internet comme réseau de transport.

ANNEXE

EXTRAITS DE CONFIGURATIONS

A1.1 Configuration de GLBP

A1.1.1 Configuration de la virtualisation de la passerelle VLAN10

- *Sur commutateur Distr1*

```
configure terminal
interface vlan 10
ip address 30.30.1.61 255.255.255.192 //assigner une adresse IP réelle
exit
glbp 1 ip 30.30.1.1
glbp 1 priority 255
glbp 1 preempt
glbp 1 name glbp-vlan10
glbp 1 load-balancing round-robin
exit
//configuration du tracking en cas de défaillance des autres interfaces
track 1 interface f0/0 line-protocol
exit
track 2 interface f0/0 ip routing
exit
track 3 interface f0/1 line-protocol
exit
track 4 interface f0/1 ip routing
exit
interface vlan 10
glbp 1 weighting 100 lower 50
glbp 1 weighting track 1 decrement 30
glbp 1 weighting track 2 decrement 30
glbp 1 weighting track 3 decrement 30
glbp 1 weighting track 4 decrement 30
//Authentification glbp
configure terminal
service password-encryption
key chain key_vlan10
key 0
key-string 0 key10
exit
interface vlan 10
glbp 1 authentication md5 key-chain key_vlan10
```

- *Sur le commutateur Distr2*

```
configure terminal
interface vlan 10
ip address 30.30.1.62 255.255.255.192 //assigner une adresse IP réelle
//config GLBP
glbp 1 ip 30.30.1.1
glbp 1 priority 120
glbp 1 preempt
glbp 1 name glbp-vlan10
glbp 1 load-balancing round-robin
```

```
exit
//configuration de tracking en cas de défaillance des autres interfaces
track 1 interface f0/0 line-protocol
exit
track 2 interface f0/0 ip routing
exit
track 3 interface f0/1 line-protocol
exit
track 4 interface f0/1 ip routing
exit
interface vlan 10
glbp 1 weighting 100 lower 50
glbp 1 weighting track 1 decrement 30
glbp 1 weighting track 2 decrement 30
glbp 1 weighting track 3 decrement 30
glbp 1 weighting track 4 decrement 30
exit
//Authentification glbp
configure terminal
service password-encryption
key chain key_vlan10
key 0
key-string 0 key10
exit
interface vlan 10
glbp 1 authentication md5 key-chain key_vlan10
```

A1.1.2 Configuration de la virtualisation de la passerelle VLAN164

- *Sur commutateur Distr1*

```
configure terminal
interface vlan 164
ip address 30.30.1.125 255.255.255.192 //assigner une adresse IP réelle
//config GLBP
glbp 2 ip 30.30.1.65
glbp 2 priority 255
glbp 2 preempt
glbp 2 name glbp-vlan164
glbp 2 load-balancing round-robin
exit
//configuration de tracking en cas de défaillance des autres interfaces
configure terminal
interface vlan 164
glbp 2 weighting 100 lower 50
glbp 2 weighting track 1 decrement 30
glbp 2 weighting track 2 decrement 30
glbp 2 weighting track 3 decrement 30
glbp 2 weighting track 4 decrement 30
exit
//Authentification glbp
configure terminal
service password-encryption
key chain key_vlan164
```

```
key 1
key-string 0 key164
interface vlan 164
glbp 2 authentication md5 key-chain key_vlan164
```

- *Sur le commutateur Distr2*

```
conf t
interface vlan 164
ip address 30.30.1.126 255.255.255.192 //assigner une adresse IP réelle
//config GLBP
glbp 2 ip 30.30.1.65
glbp 2 priority 120
glbp 2 preempt
glbp 2 name glbp-vlan164
glbp 2 load-balancing round-robin
exit
//configuration du tracking en cas de défaillance des autres interfaces
Configure terminal
interface vlan 164
glbp 2 weighting 100 lower 50
glbp 2 weighting track 1 decrement 30
glbp 2 weighting track 2 decrement 30
glbp 2 weighting track 3 decrement 30
glbp 2 weighting track 4 decrement 30
exit
//Authentification glbp
configure terminal
service password-encryption
key chain key_vlan164
key 1
key-string 0 key164
interface vlan 164
glbp 2 authentication md5 key-chain key_vlan164
```

A1.2 Configuration de PfR

A1.2.1 Configuration VoIP

- *Configurations du routeur Siège*

```
configure terminal
telephony-service
system message Softphone1
max-dn 10
max-ephone 10
ip source-address 192.168.11.254 port 2000
exit
ephone-dn 1
number 1001
name Steffy
label Steffy
description Bureau
exit
```

```
ephone 1
mac-address 000C.293B.59AE
button 1 :1
exit
dial-peer voice 1 voip
session target ipv4 :172.16.5.2
destination-pattern 2...
exit
dial-peer voice 2 voip
session target ipv4 :172.16.5.6
destination-pattern 2...
end
```

- *Configuration du routeur Région1*

```
configure terminal
telephony-service
system message Softphone2
max-dn 10
max-ephone 10
ip source-address 192.168.10.254 port 2000
exit
ephone-dn 1
number 2001
name Ambinina
label Ambinina
description Bureau
exit
ephone 1
mac-address 000C.297B.2B07
button 1 :1
exit
dial-peer voice 1 voip
session target ipv4 : 30.30.1.1
destination-pattern 1...
end
```

A1.2.2 Configurations de base du routeur MC-BR

```
Configuration terminal
interface f0/0  //interface interne
ip address 30.30.1.2 255.255.255.0
no shutdown
exit
interface s1/0
encapsulation frame-relay
no shutdown
load-interval 30
exit
interface s1/0.1 point-to-point  //interface externe
ip address 172.16.5.1 255.255.255.252
no shutdown
frame-relay interface-dlci 102
exit
int s1/1
```

```
encapsulation frame-relay
no shutdown
load-interval 30
exit
interface s1/1.1 point-to-point  //interface externe backup
ip address 172.16.5.5 255.255.255.252
no shutdown
bandwidth 256
frame-relay interface-dlci 103
exit
interface Loopback0  //interface locale
ip address 10.10.10.1 255.255.255.255
no shutdown
```

A1.2.3 Configurations des paramètres et configurations des phases de PfR

- *Paramètres de base de PfR*

```
configure terminal
key chain OER
key 1
key-string OER_BR
exit
oer border //active le BR
local Loopback0
master 10.10.10.1 key-chain OER
exit
oer master //active le MC
border 10.10.10.1 key-chain OER
interface f0/0 internal
interface Serial1/0.1 external
interface Serial1/1.1 external
exit
```

- *Configuration des phases de PfR sur MC*

```
configure terminal
oer master
logging
learn
aggregation-type prefix-length 24
throughput
monitor-period 2
periodic-interval 0
prefixes 150
exit
backoff 180 360
mode monitor both
mode select-exit best
mode route control
// Activation IP SLA sur le routeur Région1
Configure terminal
Région1(config)# ip sla monitor responder
```

BIBLIOGRAPHIE

[1] D. Tilloy, *« Introduction aux réseaux TCP/IP »*, Support de cours, Institut Universitaire de Technologie d'Amiens, A.U : 1998-1999

[2] J. L. Montagnier, *« Construire son réseau d'entreprise »*, Eyrolles : Paris, 2001

[3] E. Robin, L. Boudin, G. Tourres, *« Essentiel CCNA 1»*, Laboratoire SUPINFO des Technologies Cisco, 2005

[4] Cisco Networking Academy, *« CCNA 2.1.2 »*, Cisco Systems : USA, 2000

[5] D. Dromard, D. Seret, « *Architecture des réseaux* », Pearson Education : France, 2009

[6] T. Vaira, « *Cours Réseaux – Adressage IP »*, BTS IRIS, 2012

[7] E. Robin, L. Boudin, G. Tourres, *« Essentiel CCNA 3»*, Laboratoire SUPINFO des Technologies Cisco, 2005

[8] G. Pujolle, « *Cours Réseaux et Télécoms»*, Eyrolles 3è Edition : Paris, 2008

[9] E. Robin, L. Boudin, G. Tourres, *« Essentiel CCNA 2»*, Laboratoire SUPINFO des Technologies Cisco, 2005

[10] G.Pujolle, *« Les réseaux »*, Eyrolles : Paris, Edition 2008

[11] E. Robin, L. Boudin, G. Tourres, M. Vernerie, *« Essentiel CCNA 4»*, Laboratoire SUPINFO des Technologies Cisco, 2005

[12] J. L. Montagnier, *« Réseau d'entreprise par la pratique »*, Eyrolles : Paris, 2004

[13] G. Pujolle, *« Les réseaux, Annexes »*, Eyrolles : Paris, Edition 2011

[14] G. Fiche, G. Hébuterne, *« Trafic et performances des réseaux de télécoms »*, Hermes Science Publications, 2003

[15] Cisco Networking Academy, « CCNA Discovery 4.0 », Cisco Systems : USA, 2007-2008

[16] L.Peterson, B. S. Davie, *« Computer Networking, a system approach »*, 3è Edition, 2003

[17] G. Montcouquiol, *« Théorie des graphes »*, Support de cours, IUT Orsay, AU : 2006-2007

[18] Cisco Networking Academy, « *CCNA Exploration 4.0 , Protocoles et Concepts de routage*», Cisco Systems : USA, 2007-2008

[19] Cisco Networking Academy, « *CCNA Exploration 4.0, Commutation de réseau local et réseau local sans fil»*, Cisco Systems : USA, 2007-2008

[20] J. F. Rasolomanana, *« Commutation et routage IP »*, Cours M2-TCO, Dép. TCO-E.S.P.A., A.U : 2015-2016

[21] Cisco, *« CCNA Exploration –Protocoles et Concepts de routage »*, CCNA 2 Chapitre 9, Cisco System : USA, 2004

[22] Cisco, *« Performance Routing Configuration Guide, Cisco IOS Release 15M&T* », Cisco System : USA, 2013

[23] T. Viaud, *« Découverte de NetFlow et Configuration »*, Article Etudiants SUPINFO International University, Octobre 2015

[24] Cisco, *« Cisco IOS IP SLAs Overview* », Cisco System, 2010

[25] Cisco, *« Optimized Edge Routing Configuration Guide, Cisco IOS Release 12.4T* », Cisco System: USA, 2012

[26] S.Wilkins, *« Policy Based Routing (PBR) Fundamentals»*, https://www.pluralsight.com/blog/it-ops/pbr-policy-based-routing, Août 2010

[27] Cisco, *« Security Configuration : Zone-Based Policy Firewall, Cisco Release 15M&T»*, Cisco System, 2013

[28] C. D. Stefano,S. Wong, *« Les protocoles de redondance HSRP, VRRP et CARP »*, https://wapiti.telecom-lille.fr/commun/ens/peda/options/st/rio/pub/exposes/exposesrio2006-ttnfa2007/DiStefano-Wong/, 2006

[29] S. D. Jongh, « *VRRP: Virtual Router Redundancy Protocol* », https://www.ciscomadesimple.be › Certifications › CCNA - ICND2, Mai 2013

[30] N. Salmon, *« Redondance de routeur avec GLBP »*, http://idum.fr/spip.php?article230, Juin 2012

[31] W. C. Hardy, « *VoIP Service Quality*», McGraw-Hill Networking, 2003

FICHE DE RENSEIGNEMENTS

Nom : RANDRIANANDRASANA

Prénoms : Ando Steffy

Adresse: Lot III K 37 Anjezika 2 Andavamamba Antananarivo

Email : andoste13@gmail.com

Téléphone : 032 75 997 76

Titre du mémoire :

« OPTIMISATION DE LAN ET MISE EN OEUVRE DE TECHNOLOGIE PFR SUR WAN D'UN RESEAU D'ENTREPRISE : CAS DU MINISTERE DES FINANCES ET DU BUDGET »

Nombres de pages : 118

Nombres de tableaux : 21

Nombre de figures : 86

Directeur de mémoire :

Nom : RANDRIARIJAONA

Prénoms : Lucien Elino

Grade : Assistant d'Enseignement et de Recherche

Email : elrandria@yahoo.com

Téléphone : 032 04 747 95

RESUME

Le principal but d'un réseau est d'écouler si possible la totalité du trafic offert, et ce dans les meilleures conditions possibles. L'étude de l'état du réseau permet de déterminer ses caractéristiques et d'en déduire les aspects affectant ses performances. A partir de ces analyses, nous pouvons établir les solutions d'optimisation adéquates. Des techniques de redondances combinées à une utilisation optimale des ressources nous permettent d'acquérir notre objectif. Au niveau du WAN, la solution PfR (Performance Routing) utilisant ces deux techniques a été étudiée pour avoir des performances considérables sans supplément des coûts de mise à niveau du réseau. Le principe de cette solution se résume par le routage dynamique au niveau des routeurs de périphérie en fonction des besoins en performances des trafics et applications du réseau.

Mots clés : Réseau d'entreprise, performance, redondance, optimisation, PfR

ABSTRACT

The main goal of a network is to flow the whole of traffic within the best possible conditions. Studying the state of the network let us identify its characteristics and evolve aspects that affect its performances. By these analysis, we can establish the appropriate optimization solutions. Redundancy technics combined with optimal use of resources allow us to achieve our aim. Over the WAN, the PfR (Performance Routing) solution applying these technics is learnt to get significant performances without extra costs of network optimization. The element of this solution is summarized by dynamic routing over the edge routers depending on network traffics and applications performances needed.

Key words: Enterprise network, performance, redundancy, optimization, PfR