

TABLE DES MATIERES

REMERCIEMENTS.....	i
TABLE DES MATIERES	ii
NOTATIONS.....	vi
ABREVIATIONS	vii
INTRODUCTION.....	1
CHAPITRE 1 RESEAUX TCP/IP	2
1.1 Introduction à TCP/IP	2
1.1.1 Généralités	2
1.1.2 Principe des couches et des protocoles	2
1.1.3 Mécanismes d'encapsulation.....	4
1.2 Le protocole Internet version 4 ou IPv4.....	4
1.2.1 Description du protocole IP	5
1.2.2 Principe d'adressage des machines.....	5
1.2.2.1 Structure d'adresse IP	5
1.2.3 Transport et format de datagramme IP	6
1.2.3.1 Datagramme IP.....	6
1.2.3.2 Routage des datagrammes sur Internet.....	9
1.2.3.3 Détermination des distances des chemins de réseau à l'aide de métriques.....	13
1.3 Les protocoles de la couche « Transport »	14
1.3.1 Le protocole TCP.....	14
1.3.2 Le protocole UDP.....	15
1.3.3 Comparaison des protocoles TCP et UDP	16
1.4 Conclusion	17
CHAPITRE 2 LA VOIX SUR IP	18
2.1 Présentation de la voix sur IP (VoIP)	18
2.1.1 Introduction à la VoIP.....	18
2.1.1.1 Contexte technologique de la VoIP.....	19
2.1.1.2 Traitement et transmission de la voix en mode paquet.....	19
2.1.2 Les codages de la VoIP	20

2.1.2.1	<i>Introduction</i>	20
2.1.2.2	<i>Les différents types de codecs utilisés en VoIP</i>	21
2.1.2.3	<i>Le MOS</i>	23
2.2	<i>Normes et protocoles de la VoIP</i>	24
2.2.1	<i>Le protocole H.323</i>	24
2.2.1.1	<i>Introduction</i>	24
2.2.1.2	<i>Fonctionnement</i>	25
2.2.1.3	<i>Architecture H.323</i>	25
2.2.1.4	<i>Les protocoles secondaires de H.323</i>	27
2.2.1.5	<i>Phases d'appel de H.323</i>	28
2.2.1.6	<i>H.323 dans le modèle OSI</i>	29
2.2.2	<i>Protocole SIP</i>	30
2.2.2.1	<i>Introduction</i>	30
2.2.2.2	<i>Fonctionnement</i>	31
2.2.2.3	<i>Les clients et les serveurs de SIP</i>	31
2.2.2.4	<i>Comparaison de SIP avec H.323</i>	32
2.2.2.5	<i>Conclusion</i>	34
2.2.3	<i>Protocole MGCP</i>	34
2.2.4	<i>Protocoles RTP et RTCP</i>	34
2.2.4.1	<i>Protocole RTP</i>	34
2.2.4.2	<i>Utilisation de RTP</i>	35
2.2.4.3	<i>Protocole RTCP</i>	36
2.3	<i>Problèmes de la VoIP et qualité de service</i>	38
2.3.1	<i>Les paramètres de la VoIP</i>	38
2.3.1.1	<i>La latence</i>	40
2.3.1.2	<i>La gigue</i>	42
2.3.1.3	<i>La Perte et le déséquenceement de paquets</i>	43
2.3.1.4	<i>L'écho</i>	44
2.3.2	<i>Mécanismes de QoS</i>	45
2.3.2.1	<i>Mécanisme IntServ</i>	45
2.3.2.2	<i>Mécanisme Diffserv</i>	46

2.3.2.3 MPLS	47
CHAPITRE 3 LA TELEPHONIE SUR IP	49
3.1 Définition	49
3.1.1 Caractéristique de la ToIP	50
3.1.2 Les équipements de la ToIP	51
3.1.2.1 Les terminaux téléphoniques.....	51
3.1.2.2 Le « gatekeeper »	52
3.1.2.3 Le « voice gateway »	52
3.1.2.4 Les équipements complémentaires	52
3.1.3 Avantages de la ToIP	53
3.1.3.1 Convergence.....	53
3.1.3.2 Optimisation des ressources	54
3.1.3.3 Coût de transport quasiment nul.....	54
3.1.3.4 Services exclusifs	54
3.1.3.5 Disparition des commutateurs locaux.....	55
3.1.4 Architecture de ToIP	55
3.1.4.1 De poste informatique à poste informatique.....	56
3.1.4.2 De Poste informatique à téléphone (ou vice-versa)	56
3.1.4.3 De téléphone à téléphone.....	57
3.1.5 Sécurisation	58
3.1.6 Différence entre VoIP et ToIP	60
3.1.7 ToIP et NGN.....	61
3.1.7.1 Objectif.....	61
3.1.7.2 NGN et la téléphonie IP.....	61
3.2 Conclusion	63
CHAPITRE 4 PLANIFICATION DES LIENS VoIP	64
4.1 Introduction	64
4.2 Dimensionnement d'un réseau offrant le service de la voix	64
4.2.1 Modèle de trafic.....	65
4.2.2 Lois d'Erlang.....	65
4.2.3 Débit d'accès.....	66

4.2.3.1	Débit par appel.....	66
4.2.3.2	calcul du nombre de circuits.....	70
4.2.4	Estimation du trafic entre les Edge Router	71
4.2.5	Calcul des capacités	72
4.2.5.1	Capacité du plus court chemin entre deux sites.....	72
4.2.5.2	Algorithme de DIJKSTRA.....	72
4.2.5.3	Capacité des liens individuels.....	74
4.3	Dimensionnement pour un réseau offrant le service data.....	74
4.3.1	Exemple de type de contrat	75
4.3.2	Principe de distribution de charge.....	75
4.3.3	Capacité du plus court chemin pour le trafic data.....	76
4.3.4	Capacité des liens individuels pour le trafic data.....	76
4.3.5	Capacité des liens supportant le trafic voix et data.....	76
4.4	Conclusion	77
CHAPITRE 5 SIMULATION AVEC LE LANGAGE JAVA		78
5.1	Introduction.....	78
5.2	Topologie à simuler.....	78
5.2.1	Modèles utilisés.....	79
5.2.2	Organigramme de la simulation	79
5.3	Présentation du logiciel	80
5.3.1	Informations sur chaque site.....	80
5.3.2	Calcul du débit d'accès au niveau de chaque site.....	80
5.3.3	Capacité voix	87
5.3.4	Calcul de la capacité totale du lien	88
5.4	Conclusion.....	91
CONCLUSION.....		92
ANNEXES.....		93
BIBLIOGRAPHIE		102

NOTATIONS

1. Minuscules latines

ms	Milliseconde
n	nombre de ressources disponibles

2. Majuscules latines

C_{kd}	Capacité du lien individuel k
C_{kv}	capacité du lien individuel pour le trafic voix
D_{downi}	Débit des liens descendant au niveau de chaque site
$Débit_{apl}$	Débit par appel en Kbit
D_{sig}	Débit de signalisation
D_{upi}	Débit du lien montant au niveau de chaque site
Gbps	Gigabit par seconde
GHz	Gigahertz
Kbps	Kilobit par seconde
Mbps	Mégabit par seconde
$P_k(t)$	Probabilité d'observation de k à l'instant t
P_n	Probabilité de blocage
T_{ijv}	Trafic entre les sites i et j
T_{tra}	Matrice de Trafic

3. Minuscule grecque

λ	taux d'arrivée
-----------	----------------

ABBREVIATIONS

ADSL	Asymmetric Digital Subscriber Line
ARP	Address Resolution Protocol
ARPANET	Advanced Research Projects Agency Network
ATM	Asynchronous Transfer Mode
BGP	Border Gateway Protocol
CELP	Code Excited Linear Prediction
CODEC	Codeur Décodeur
CS-ACELP	Conjugate Structure Algebraic Code Excited Linear Prediction
DHCP	Dynamic Host Configuration Protocol
Diffserv	Differentiate Service
DNS	Domain Name Service
DoD	Department Of Defense
DOS	Deny Of Service
DRARP	Dynamic Reserve Address Resolution Protocol
DSCP	Differentiated Service Code Point
DSL	Digital Subscriber Line
DSP	Digital System Processing
EGP	Exterior Gateway Protocol
EIGRP	Enhanced Interior Gateway Routing Protocol
EoIP	Everything over Internet Protocol
ESP	Encapsulating Security Payload
ETSI	European Telecommunication Standards Institute
FTP	File transfer Protocol
GLP	Gateway Location Protocol

GSM	Global System for Mobile Communications
HDLC	High level Data Link Control
HTTP	HyperText transfer Protocol
ICMP	Internet Control Message Protocol
IDRP	InterDomain Routing Protocol
IETF	Internet Engineering Task Force
IGP	Interior Gateway Protocol
IGMP	Internet Group Membership Protocol
IGRP	Interior Gateway Router Protocol
ILS	Internet Locator Server
INTERNET	Interconnected network
IntServ	Integrated Services
IP	Internet Protocol
IPBX	IP Private Branch eXchange
Ipssec	IP Security
IRTF	Internet Research Task Force
IS-IS	Intermediate System to Intermediate System
ISO	International Standard Organization
ISDN	Integrated Services Digital Networks
ISP	Internet Service Provider
ITU	International Telecommunication Union
IVR	Interactive Voice Response
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
LD-CELP	Low-Delay CELP

LLC	Logical Link Control
LS	Location server
MAC	Media Access Control
MAN	Metropolitan Area Network
MCU	Multipoint Control Unit
MEGACO	Media Gateway Controller
MGCP	Media Gateway Control Protocol
MIC	Modulation par Impulsion et Codage
MMUSIC	Multiparty Multimedia Session Protocol
MOS	Mean Opinion Score
MPLS	Multi Protocol Label Switching
MP-MLQ	Multi Pulse –Maximum Linklihood Quantization
MTU	Maximum Transfer Unit
NFS	Network File System
NGN	Next Generation Network
NIC	Network Information Center
OMERT	Office Malgache d’Etudes et de Régulation des Télécommunications
OSI	Open System Interconnexion
OSPF	Open Shortest Path First
PABX	Private Automatic Branch eXchange
PAPS	Premier Arrivé Premier Servi
PBX	Private Branch eXchange
PC	Personal Computer
PCM	Pulse Code Modulation
PDU	Protocol Data Unit

PGPS	Packet Generalized Processor Sharing
POP	Post Office Protocol (Point Of Presence)
PPP	Point to Point Protocol
PS	Proxy Server
PSTN	Public Switched Telephone Network
QoS	Quality of Service
QSIG	Q-Signaling
RARP	Reverse Address Resolution Protocol
RAS	Registration Admission and Status
RED	Random Early Detection
RFC	Request For Comments
RIP	Routing Information Protocol
RNIS	Réseau Numérique à Intégration de Service
RS	Redirect Server
RSVP	Resource reSerVation Protocol
RTC	Réseau Téléphonique Commuté
RTCP	Real-Time Transport Control Protocol
RTP	Real-Time Transport Protocol
SIP	Session Initiation Protocol
SPIT	SPam over IP Telephony
SRTP	Secure Real-time Transport Protocol
TCP	Transport Control Protocol
TCP/IP	Transport Control Protocol/Internet Protocol
TLS	Transport Layer Security
TTL	Time To Live

ToIP	Telephony over Internet Protocol
ToS	Type of Service
UA	User Agent
UAC	User Agent Client
UAS	User Agent Server
UDP	User Datagram Protocol
UIT-T	Union Internationale des Télécommunications - Branche de standardisation des Télécommunications
UMTS	Universal Mobile Telecommunication System
VLAN	Virtual Local Network
VoIP	Voice over Internet Protocol
VPN	Virtual Private Network
WAN	Wide Area Network
WAP	Wireless Application Protocol
WFQ	Weighted Fair Queuing
WiFi	Wireless Fidelity
WRED	Weighted Random Early Detection

INTRODUCTION

Jadis réservé au transport des données, IP est désormais utilisé pour le transport de la voix. La Voix sur IP fait référence au transport de la voix sous la forme de paquets IP entre deux points d'un réseau. On est passé alors d'une commutation de circuits à une commutation de paquets. Au lieu de disposer à la fois d'un réseau informatique et d'un réseau téléphonique commuté, l'entreprise peut donc, grâce à la VoIP, tout fusionner sur un même réseau.

Si les techniques de mise en œuvre d'IP permettent théoriquement de transporter la voix avec un bon niveau de qualité, encore faut-il que les choix d'architecture, de dimensionnement et de paramétrage permettent d'atteindre l'un des objectifs visé qui est le partage des ressources d'infrastructures entre les données et la voix. Des choix inadaptés en termes d'ingénierie d'infrastructure et de trafic rendront par conséquent impossible la cohabitation voix/données. C'est pourquoi, dans le cadre de ce mémoire, on effectue la planification des liens VoIP.

Étant donné que la VoIP est basée sur l'IP, il s'avèrera nécessaire de présenter dans le premier chapitre une vue d'ensemble des réseaux TCP/IP avec les principes des protocoles utilisés.

Le second chapitre sera consacré à la technologie de la voix sur IP, où seront abordés une présentation générale de cette technologie, puis les différentes normes et protocoles utilisés. Ensuite, les problèmes de la VoIP et de la qualité de service seront détaillés. Le troisième chapitre concernera la téléphonie sur IP (ToIP) qui est une technologie dérivée de la VoIP.

L'amélioration des performances des réseaux est vue comme un défi d'optimisation composé de deux parties : la gestion de capacité et la gestion du trafic. D'où le quatrième chapitre concernera la gestion de capacité, en d'autres termes du dimensionnement des liens VoIP. Ces liens correspondent à l'interconnexion de différents sites au travers d'un réseau IP.

Le dernier chapitre présentera la simulation de la gestion de capacité évoquée dans le chapitre précédent. Cette simulation a été développée avec le langage JAVA.

Finalement, une conclusion générale résumera le travail effectué et, vu que l'étude du domaine de la voix sur IP est encore très large, elle ouvrira de nouvelles perspectives vers de nouveaux points qui doivent être étudiés ultérieurement.

CHAPITRE 1

RESEAUX TCP/IP

1.1 Introduction à TCP/IP

1.1.1 Généralités

Un réseau est constitué d'un ensemble d'ordinateurs et de périphériques interconnectés par différents liens de communication, capables d'échanger des données en temps réel ou quasi-réel. Chaque élément constituant un réseau est appelé nœud.

L'Internet (Interconnected Network) n'est pas un réseau au sens classique du terme, il n'y a rien qui puisse ressembler à une énorme multinationale qui fournirait des services dans tous les continents. En fait, l'Internet est une connexion anarchique de réseaux appartenant à divers propriétaires et de différents types. Le mode opératoire de l'Internet est très simple, des réseaux sont reliés par des programmes inter-réseaux. Tout hôte de l'Internet est supposé abriter une instance de ce programme. Les applications accèdent en général au programme Internet à travers un programme de transport TCP ou UDP.

Les données qui transitent sur le réseau sont fragmentées en tronçons appelés paquets. Chacun est manipulé individuellement et mentionne les adresses d'origine et de destination. Le paquet est emballé pour traverser le réseau dans lequel il est apparu puis déballé et acheminé par un programme Internet suivant un autre type d'encapsulation. En d'autres termes, à l'intérieur de chaque réseau, les nœuds utilisent la technologie spécifique de leur réseau (Ethernet, X. 25,...). Le logiciel d'interconnexion de la couche réseau encapsule ces spécificités et offre un service commun à tous les applicatifs, faisant apparaître l'ensemble de ces réseaux disparates comme un seul et unique réseau. [1]

1.1.2 Principe des couches et des protocoles

Tous les applicatifs réseaux doivent pouvoir communiquer entre eux, quelque soit l'architecture ou la plate-forme utilisée. Pour cela, les opérations sur les réseaux ont été divisées en plusieurs phases de base, de manière à simplifier le portage des applicatifs sur toutes les plates-formes. C'est ce que l'on appelle le modèle en couche. Un standard a alors été créé, normalisé par l'Open Systems Interconnection Reference Model (modèle de référence

d'interconnexion des systèmes ouverts) sous la référence OSI-RM, utilisant 7 couches distinctes.

Pour réduire la complexité de conception, les réseaux sont organisés en série de couches ou niveaux, chacune étant construite sur la précédente. Le nombre de couches, leur nom et leur fonction varie d'un réseau à un autre. Cependant, dans chaque type de réseau, l'objet de chaque couche est d'offrir certains services aux couches plus hautes, en leur épargnant les détails de la mise en œuvre de ces services.

La couche N d'une machine gère la conversation avec la couche N d'une autre machine. Les règles et conventions pour cette conversation sont connues sous le nom de protocole de la couche N. en réalité, aucune donnée n'est transférée directement d'une couche N d'une machine à la couche N d'une autre machine mais chaque couche passe les données et les contrôles à la couche immédiatement inférieure, jusqu'à la plus basse. Entre chaque paire de couches adjacentes, on trouve une interface. L'interface définit les opérations élémentaires et les services que la couche inférieure offre à la couche supérieure.

TCP/IP est un des langages utilisés dans les réseaux. Le terme TCP/IP n'est pas limité à l'expression Transport Control Protocol/Internet Protocol, il recouvre toute une famille de protocoles comme UDP (User Datagram Protocol), Telnet, FTP (File Transfer Protocol), http (HyperText Transfer Protocol)... [1] [2]

La hiérarchie des couches et protocoles est appelé architecture du réseau représentée par la figure 1.01 :

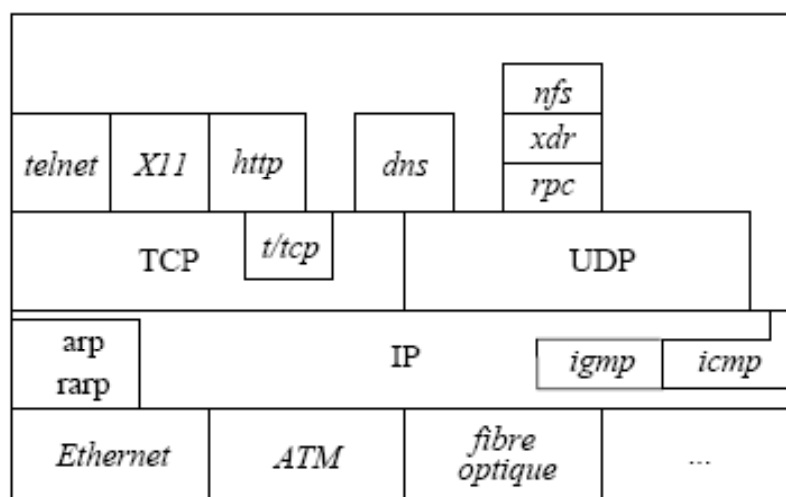


Figure 1.01 : Hiérarchie des protocoles TCP/IP

1.1.3 Mécanismes d'encapsulation

Que ce soit dans le modèle OSI ou dans de modèle TCP/IP, les données utilisateurs sont toujours encapsulées à l'envoi et désencapsulées à partir des trains de bits au niveau de la réception. A chaque passage au niveau d'une couche donnée, il y a ajout relatives aux protocoles utilisées (en-tête/ en-queue) comme enveloppes de ces couches de façon à ce que le contrôle soit plus aisé. Le processus d'encapsulation commence à la couche application et ne se termine qu'à la couche physique. Par contre, la désencapsulation commence à la couche physique et se termine à la couche application afin de resituer les données applicatives envoyées par l'émetteur. Le mécanisme d'encapsulation est représenté par la figure 1.02 : [2]

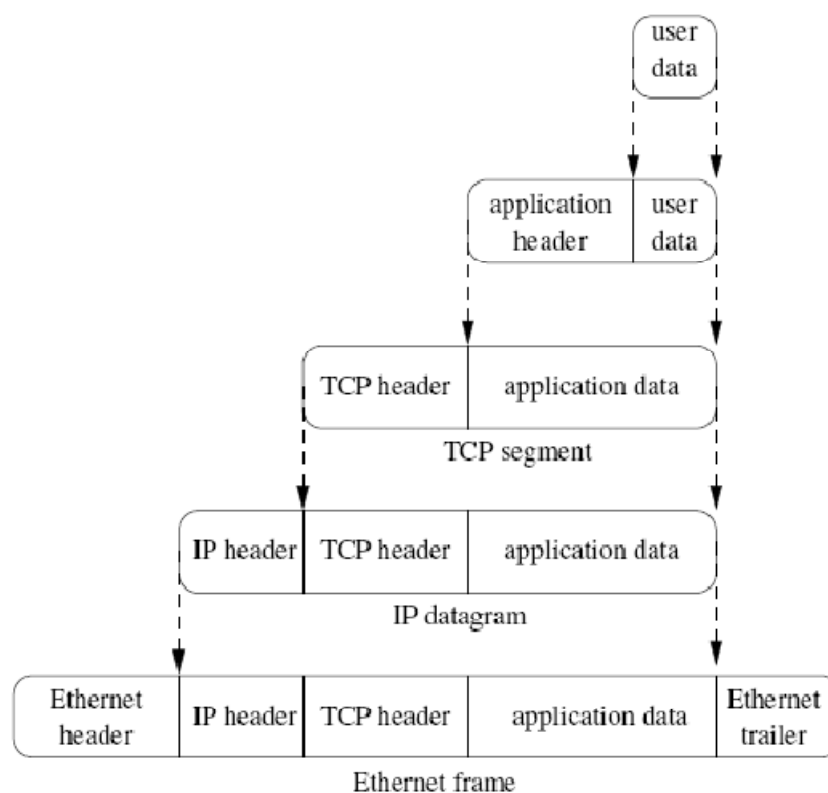


Figure 1.02 : Encapsulation des données

1.2 Le protocole Internet version 4 ou IPv4

La couche Internet, similaire à la couche réseau du modèle OSI, assure le transport des données. Le rôle de cette couche est de trouver le meilleur chemin au sein d'un réseau. Les unités utilisent le système d'adressage de la couche réseau pour déterminer la destination des données durant leur déplacement.

1.2.1 Description du protocole IP

Comme son nom l'indique (Internet Protocol), le protocole IP a pour rôle de router le trafic à travers des réseaux. Il a été conçu pour réaliser l'interconnexion de réseaux informatiques et permettre ainsi les communications entre systèmes. Ce protocole assure la transmission de paquets de données, appelés datagrammes entre ordinateur source et un ordinateur de destination.

Par exemple, les applications qui tournent sur une machine cliente génèrent des messages qui doivent être envoyés sur une autre machine d'un autre réseau. IP reçoit ces messages de la couche transport et les envoie vers sa destination grâce à l'adressage IP.

Le protocole IP multiplexe les protocoles de la couche transport et a la faculté de détruire les paquets ayant transité trop longtemps sur le réseau. Il permet également de fragmenter et de rassembler de nouveau les fragments de données. Cependant, il n'effectue ni contrôle d'erreur, ni contrôle de flux. [2]

Remarque :

Dans le modèle OSI, nous parlons plutôt de paquets au niveau de la couche réseau. En revanche, dans le modèle TCP/IP, l'unité transférée est le datagramme. Cependant, dans la suite de l'ouvrage, nous les mentionnerons indifféremment.

1.2.2 Principe d'adressage des machines

Lorsque nous envoyons des données à travers l'Internet, les données ne sont pas envoyées de manière brute mais elles sont découpées en messages, puis en segments, en datagrammes et enfin en trames. Les datagrammes, outre l'information, sont constitués d'en-tête contenant l'adresse IP de l'expéditeur et celle du destinataire, ainsi qu'un nombre de contrôle déterminé par l'information emballée dans le paquet : ce nombre de contrôles, communément appelé en-tête totale de contrôles ou « checksum », permet au destinataire de savoir si le datagramme IP a été « abîmé » pendant son transport. L'adressage joue donc un rôle très important dans ce processus. [1]

1.2.2.1 Structure d'adresse IP

Une des choses les plus intéressantes du protocole TCP/IP est d'avoir attribué un numéro fixe, comme un numéro de téléphone, à chaque ordinateur connecté sur Internet. Ce numéro est appelé *l'adresse IP*. Dans le cadre de l'IPv4, les adresses sont codées sur 32 bits.

Ainsi, tout ordinateur sur Internet, par exemple un ordinateur particulier connecté à Internet, se voit attribuer une adresse de type a.b.c.d (où a,b,c,d sont des nombres compris entre 0 et 255 donc des blocs de 8 bits), par exemple 202.15.170.1. Dès ce moment, cet ordinateur est le seul au monde à posséder ce numéro, et il y est en principe directement atteignable.

Un rapide calcul montre qu'il y a, en théorie, un maximum de $256^4 = 4'294'967'296$ adresses possibles, ou, en d'autres termes, d'ordinateurs directement connectables, ce qui est plus que suffisant même à l'échelle mondiale. En fait, il y a beaucoup moins d'adresses que ce nombre impressionnant, car de nombreux numéros IP ne sont pas autorisés ou sont utilisés à des fins techniques.

Bien qu'IPv6, la nouvelle génération du protocole IP existe déjà, IPv4 reste largement le plus utilisé étant donnée que la saturation d'adressage ne semble pas encore être un problème majeur. Aussi, dans la suite de l'ouvrage, nous nous référons au protocole IPv4. IPv6 utilise un adressage utilisant huit groupes de quatre lettres hexadécimales séparés par « : ». Les enjeux majeurs de l'IPv6, outre l'extension de l'espace d'adressage sont : un traitement plus rapide grâce à un en-tête plus simplifié, la sécurité, la notion de flux... [1] [2]

1.2.3 Transport et format de datagramme IP

1.2.3.1 Datagramme IP

La structure du datagramme IP sera détaillée dans la figure 1.03:

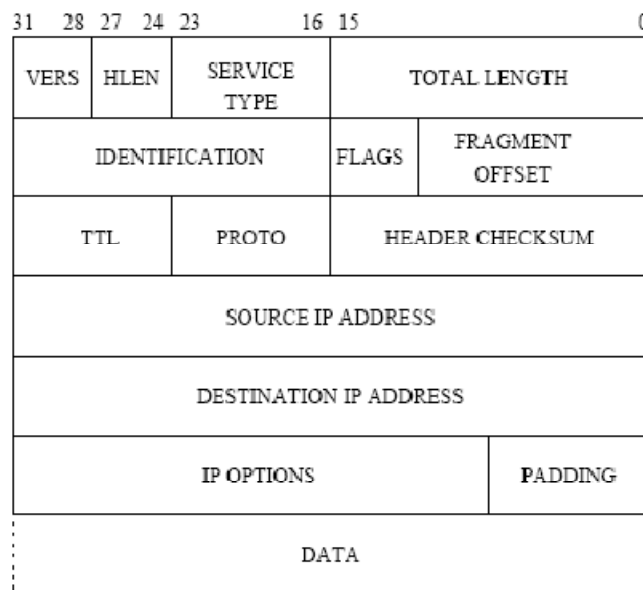


Figure 1.03 : Champs d'un datagramme IP

- Version : 4 bits qui spécifient la version du protocole IP. L'objet de ce champ est la vérification que l'émetteur et le destinataire des datagrammes sont bien en phases avec la même version. Actuellement c'est la version 4 qui est principalement utilisée sur l'Internet, bien que quelques implémentations de la version 6 existent et soient déjà en expérimentation.
- Hdr Len : 4 bits qui donnent la longueur de l'en-tête en mots de 4 octets. La taille standard de cet en-tête fait 5 mots, la taille maximale fait :

$$(2^3 + 2^2 + 2^1 + 2^0) \times 4 = 60 \text{ octets}$$

- Total Length : Donne la taille du datagramme, en-tête plus données. S'il y a fragmentation (voir plus loin) il s'agit également de la taille du fragment (chaque datagramme est indépendant des autres).

La taille des données est donc à calculer par soustraction de la taille de l'en-tête.

16 bits autorisent la valeur 65535. . La limitation vient le plus souvent du support physique (MTU) qui impose une taille plus petite, sauf sur les "hyperchannel".

- TYPE OF SERVICE : 8 bits (4 utiles) qui indiquent au routeur l'attitude à avoir vis à vis de ce datagramme. Suivant les valeurs de ce champ, le routeur peut privilégier un datagramme par rapport à un autre.

Les bits de ce champ sont répartis comme suit :

Bits 0-2 : priorité

Bits 3 : 0 = retard standard, 1 = retard faible.

Bits 4 : 0 = débit standard, 1 = taux d'erreur standard, 1 = taux d'erreur faible

Bit 6-7 : réservé

Priorité	R	D	T	0	0	
0	2	3	4	5	6	7

Figure 1.04 : Le champ Type of Service

- IDENTIFICATION, FLAGS et FRAGMENT OFFSET : Ces mots sont prévus pour contrôler la fragmentation des datagrammes. Les données sont fragmentées car les datagrammes peuvent avoir à traverser des réseaux avec des MTU plus petits que celui du premier support physique employé.

- TTL « Time To Live » (durée de vie) : 8 bits, 255s maximum de temps de vie pour un datagramme sur le net. Prévu à l'origine pour décompter un temps, ce champ n'est qu'un compteur décrémenté d'une unité à chaque passage dans un routeur. Couramment la valeur de départ est 32 ou même 64. Son objet est d'éviter la présence de paquets fantômes circulant indéfiniment.
Si un routeur passe le compteur à zéro avant délivrance du datagramme, un message d'erreur est renvoyé à l'émetteur avec l'indication du routeur. Le paquet en lui-même est perdu.
- PROTOCOL (protocole): 8 bits pour identifier le format et le contenu des données, un peu comme le champ « type » d'une trame Ethernet. Il permet à IP d'adresser les données extraites à l'une ou l'autre des couches de transport.
Dans le cadre de ce cours, nous utiliserons essentiellement ICMP, IGMP, UDP et TCP.
- HEADER CHECKSUM (somme de contrôle d'en-tête): 16 bits pour s'assurer de l'intégrité de l'en-tête. Lors du calcul de ce “ checksum ” ce champ est à 0.
A la réception de chaque paquet, la couche calcule cette valeur, si elle ne correspond pas à celle trouvée dans l'en-tête le datagramme est oublié (« discard ») sans message d'erreur.
- SOURCE ADDRESS (adresse source): Adresse IP de l'émetteur, à l'origine du datagramme.
- DESTINATION ADDRESS (adresse de destination): Adresse IP du destinataire du datagramme.
- IP OPTIONS : 24 bits pour préciser des options de comportement des couches IP traversées et destinataires. Les options les plus courantes concernent :
 - Des problèmes de sécurité
 - Des enregistrements de routes
 - Des enregistrements d'heure
 - Des spécifications de route à suivre
- PADDING Remplissage pour aligner sur 32 bits.

Les données contenues dans les datagrammes sont analysées (et éventuellement modifiées) par les routeurs permettant leur transit. [1] [2]

1.2.3.2 Routage des datagrammes sur Internet

Le routage désigne une technique permettant de déterminer le chemin emprunté par un message ou un paquet de données. C'est une méthode d'acheminement d'informations vers la bonne destination. Le routage s'opère au niveau de la couche 3 du modèle OSI, c'est-à-dire la couche réseau ou couche IP. Ainsi, les couches TCP et UDP restent donc à l'écart du concept de routage.

Comme nous l'avons dit précédemment les données circulent à travers le réseau sous forme de paquets ou datagrammes IP. Afin d'atteindre leur destination, ils traversent maints routeurs. Les routeurs sont des unités d'interconnexions de réseaux qui fonctionnent au niveau de la couche 3 OSI (couche réseau) ou couche Internet du modèle DoD. Ils interconnectent des segments de réseau ou des réseaux entiers. Leur rôle consiste à acheminer les paquets de données entre les réseaux, en fonction des informations de la couche 3. Ils possèdent l'intelligence nécessaire pour déterminer le meilleur chemin de transmission des données sur le réseau. [2]

Le routeur assure trois fonctions principales :

- Permettre la communication entre des machines n'appartenant pas au même réseau.
- Offrir un accès Internet à des utilisateurs d'ordinateurs se trouvant dans un réseau local.
- Filtrer les datagrammes IP pouvant avoir accès à un réseau.

Il existe différents niveaux de routeurs, ceux-ci fonctionnent donc avec des protocoles différents.

- Les routeurs noyaux sont les routeurs principaux car ce sont eux qui relient les différents réseaux.
- Les routeurs externes permettent une liaison des réseaux autonomes entre eux. Ils fonctionnent avec un protocole appelé EGP (Exterior Gateway Protocol) qui évolue petit à petit en gardant la même appellation.
- Les routeurs internes permettent le routage des informations à l'intérieur d'un réseau autonome. Ils s'échangent des informations grâce à de protocoles appelés IGP (Interior Gateway Protocol).

Le système de routage est représenté par la figure 1.05 :

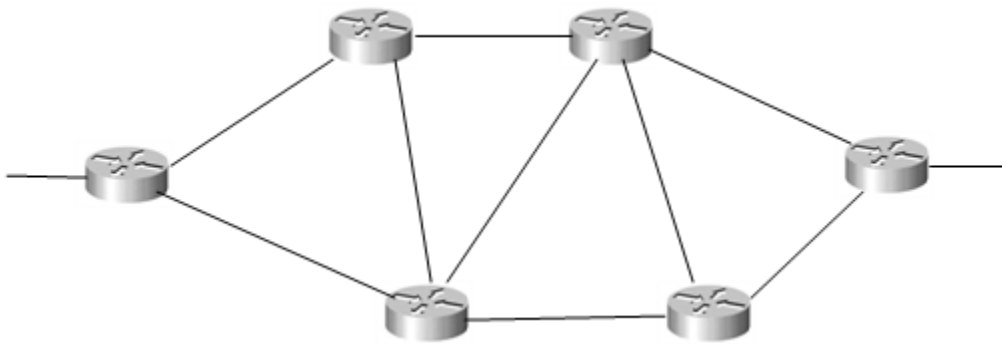


Figure 1.05 : Routage de paquets IP

Les routeurs possèdent des tables de routage (Tableau 1.01) leur permettant de choisir l'interface de sortie d'un datagramme à partir des informations stockées dans cette dernière. Les routeurs prennent également des décisions en fonction de la densité du trafic et du débit des liaisons (bande passante). La sélection du chemin permet à un routeur d'évaluer les chemins disponibles vers une destination donnée et de définir le meilleur chemin pour traiter un datagramme. [2]

Dans le cas où le chemin correspondant figurant dans la table de routage est introuvable, IP supprime le datagramme.

Il existe plusieurs protocoles de routage comme le RIP (Routing Information Protocol), l'OSPF (Open Shortest Path First), l'IGRP (Interior Gateway Router Protocol), le BGP (Border Gateway Protocol), l>IDRP (Inter Domain Routing Protocol), l'IS-IS (Intermediate System to Intermediate System)... [2] [3]

Le tableau 1.01 représente un exemple de table de routage :

Destination réseau	Masque réseau	Adresse passerelle	Adresse Interface
127.0.0.1	255.0.0.0	127.0.0.1	127.0.0.1
192.168.30.0	255.255.255.0	192.168.30.x	192.168.30.x
192.168.30.x	255.255.255.255	127.0.0.1	127.0.0.1
192.168.30.255	255.255.255.255	192.168.30.x	192.168.30.x

Tableau 1.01 : table de routage

Remarque :

Dans un réseau maillé, le routage des paquets nécessite des algorithmes complexes. Un nœud devrait connaître l'état de l'ensemble des autres nœuds avant de décider de la direction dans laquelle envoyer un paquet.

a. Le protocole RIP

- *Définitions:*

La méthode de routage à vecteur de distance détermine la direction (vecteur) et la distance vers n'importe quel lien de l'inter-réseau. Les algorithmes de routage à vecteur de distance transmettent des copies périodiques d'une table de routage d'un routeur à un autre. Ces mises à jour régulières entre les routeurs permettent de communiquer les modifications topologiques.

Le concept de vecteur de distance s'appuie sur un algorithme de calcul du chemin le plus court dans un graphe. Le graphe est celui des routeurs, la longueur du chemin est établie en nombre de sauts (« hop »), ou métrique, entre la source et la destination, c'est à dire en comptant toutes les liaisons. Cette distance est exprimée comme un nombre entier variant entre 1 et 15; la valeur 16 est considérée comme l'infini et indique une mise à l'écart de la route.

RIP est le protocole le plus utilisé pour transférer des informations de routage entre des routeurs situés sur un même réseau. Ce protocole calcule la distance vers une destination donnée. Il permet aux routeurs qui l'utilisent de mettre à jour leurs tables de routage à des intervalles programmables, en général toutes les 30 secondes. Cependant, comme les routeurs établissent sans cesse des connexions avec leurs routeurs voisins, il en résulte une augmentation du trafic réseau. [2]

- *Fonctionnement:*

Le protocole RIP permet aux routeurs de déterminer le chemin d'envoi des données, sur la base du concept de vecteur de distance. Lorsque les données passent par un routeur, elles exécutent un saut. Un chemin comportant quatre sauts indique que les données empruntant ce chemin doivent passer par quatre routeurs avant d'atteindre leur destination.

Chaque routeur émet dans un datagramme portant une adresse IP de broadcast, à fréquence fixe (environ 30 secondes), le contenu de sa table de routage et écoute celle des

autres routeurs pour compléter sa propre table. Ainsi se propagent les tables de routes d'un bout à l'autre du réseau. Pour éviter une « tempête de mises à jours », le délai de 30 secondes est augmenté d'une valeur aléatoire comprise entre 1 et 5 secondes. Si une route n'est pas annoncée au moins une fois en trois minutes, la distance devient « infinie », et la route sera retirée un peu plus tard de la table (elle est propagée avec cette métrique). [2]

b. Le protocole OSPF

Le protocole OSPF (Open Shortest Path First) a été conçu au sein de l'IETF à la fin des années 80. Il utilise plusieurs critères pour sélectionner le meilleur chemin vers une destination. Ces critères incluent des métriques de coût qui tiennent compte notamment de la vitesse d'acheminement du trafic, de la fiabilité et de la sécurité. OSPF est un protocole ouvert, c'est-à-dire qu'il n'a pas de copyright. Il est beaucoup plus complexe que RIP mais ses performances et sa stabilité sont supérieures. Le protocole OSPF utilise une base de données distribuée qui permet de garder en mémoire l'état des liaisons. Ces informations forment une description de la topologie du réseau et de l'état de l'infrastructure. [2]

Son avantage majeur réside dans le fait qu'il y a moins d'informations à faire circuler entre les routeurs, le protocole OSPF n'envoyant pas à ses voisins le nombre de sauts qui les sépare mais l'état de la liaison qui les sépare, ce qui permet d'avoir une meilleure bande passante disponible. Cependant, il est important de noter que l'algorithme utilisé par OSPF pour ses calculs de routes est extrêmement gourmand en ressources processeurs. En effet, plus une zone est importante et plus le nombre de calculs exécutés est conséquent. Les problèmes de performances sont donc accrus. Pour éviter ces problèmes de performances, il existe une solution. En effet, lorsque des modifications interviennent sur le réseau, les routeurs ayant de nombreux voisins ont beaucoup de travail à accomplir. C'est pourquoi il est conseillé de limiter à cinquante le nombre de routeurs par zone. [3]

Remarque :

Lorsqu'un algorithme de routage met à jour une table de routage, son principal objectif est de déterminer les meilleures informations à présenter dans la table. Chaque algorithme de routage interprète à sa façon les meilleures informations qui peuvent être : la bande passante, le délai, la charge (la qualité de trafic sur une ressource réseau), la fiabilité, le nombre de

sauts. Ces informations constituent la métrique de routage ou métrique de coût. En règle générale, plus le nombre est petit, meilleur est le chemin.

c. Le protocole IGRP

Le protocole IGRP (Interior Gateway Router Protocol) a été défini par la société Cisco pour ses routeurs. En effet, alors qu'elle utilisait presque exclusivement à ses débuts le protocole RIP, cette compagnie a été amenée à mettre en place un routage plus performant, l'IGRP, qui n'est autre qu'une version améliorée de RIP. Elle intègre le routage multichemin, la gestion des routes par défaut, la diffusion de l'information toutes les 90 secondes au lieu de toutes les 30 secondes, la détection des bouclages, etc. Ce protocole a lui-même été étendu par une meilleure protection contre les boucles : il s'agit du protocole EIGRP « Extended IGRP ».

[2]

d. Le protocole IS-IS

Le protocole IS-IS (Intermediate System to Intermediate System) a été principalement développé par l'ISO ; il décrit un routage hiérarchique fondé sur la décomposition des réseaux de communication en domaines. Dans un domaine, les différents nœuds indiquent leur état aux routeurs IS-IS afférents. Les communications inter-domaines sont effectuées par un routage vers un point d'accès au domaine, déterminé par les routeurs chargés des communications externes au domaine. [2]

1.2.3.3 Détermination des distances des chemins de réseau à l'aide de métriques

La table de routage est mise à jour dans un intervalle de temps régulier selon les algorithmes utilisés (à chaque 30 s pour RIP). En outre, cette mise à jour est aussi effectuée dès qu'une modification topologique se produit à savoir: pannes des équipements de routage (routeurs ou lignes de transmissions), ajout ou suppression des hôtes ou autres modifications.

Lorsqu'un algorithme de routage met à jour une table de routage, son principal objectif est de déterminer les meilleures informations à présenter dans la table. L'algorithme génère un nombre, appelé « valeur métrique », pour chaque chemin du réseau. [3]

Nous pouvons calculer les métriques en fonction d'une seule caractéristique de chemin ou en combinant plusieurs caractéristiques parmi lesquelles :

- Le débit : le débit d'une liaison, mesuré en bits par seconde (en règle générale, une liaison Ethernet à 10 Mbits/s est préférable à une ligne louée de 64kbits/s).
- Le délai : le temps nécessaire à l'acheminement d'un paquet, pour chaque liaison, de la source à la destination.
- La charge : la quantité de trafic sur une ressource réseau telle qu'un routeur ou une liaison.
- La fiabilité : cette notion indique généralement le taux d'erreurs sur chaque liaison du réseau.
- Le nombre de sauts : le nombre de routeurs par lesquels un paquet doit passer avant d'arriver à destination.
- Le coût : une valeur arbitraire, généralement basée sur la bande passante, une dépense monétaire ou une autre mesure, attribuée à un lien par un administrateur réseau. [4]

1.3 Les protocoles de la couche « Transport »

1.3.1 Le protocole TCP

TCP, acronyme de « Transport Control Protocol », est un protocole défini dans RFC 793 conçu pour être utilisé avec IP. TCP apporte des services élaborés en termes de transmission de données entre des machines raccordés sur un réseau.

Les fonctions principales de TCP sont :

- L'établissement d'une connexion fiable « full duplex ».
- Le formatage des données en segments où chaque segment est numéroté et sa réception est confirmée par le récepteur.
- Le contrôle des erreurs (détection d'erreurs et reprise).
- Le contrôle de flux pour ne pas déborder le récepteur en imposant à l'émetteur une limite lors de la transmission d'un segment.
- Le bon séquençement de segments reçus (en utilisant leur numéro)
- L'acheminement des données normales ou urgentes. [2]

La connexion TCP s'explique par l'établissement d'un chemin entre les points échangeant des informations appelé « circuit virtuel ». On dit depuis un certain temps que TCP fonctionne

en mode « orienté-connexion », c'est-à-dire l'une des applications doit effectuer un appel que l'autre doit accepter avant que la connexion soit établie et que le transfert puisse débuter.

Conceptuellement, cinq éléments doivent être réunis pour établir un circuit virtuel :

- Le protocole
- L'adresse IP de la machine émettrice
- Le port local (le numéro de port de l'application locale)
- L'adresse IP de la machine distante
- Le port distant (le numéro de port de l'application distante) [3]

Ces points réunis, la connexion peut s'établir. Comme la connexion TCP est « full-duplex », les données circulent indépendamment dans un sens et dans l'autre. A chaque envoi de paquets par l'émetteur, le récepteur doit acquitter chaque paquet par un accusé ACK pour s'assurer que les données sont bien reçues.

TCP (tout comme UDP) utilise la notion de port, excepté que TCP utilise la connexion comme abstraction de port. Une connexion est identifiée par une paire de « End points » : Host et Port. [2]

1.3.2 Le protocole UDP

UDP, acronyme de « User Datagram Protocol », est un protocole défini dans la RFC 768. Avec plus de simplicité que TCP, UDP est également conçu pour être utilisé avec IP, UDP permet de fournir une communication par paquets entre deux processus dans un environnement réseau étendu. Le protocole IP lui sert de support de base à la communication.

Les fonctions principales du protocole UDP sont :

- Le transport non fiable en mode non connecté.
- L'envoi d'un message court d'une application vers une autre avec un mécanisme simple.
- Le mécanisme de gestion des ports. [2]

UDP est caractérisé par l'absence d'un accusé de réception au niveau du protocole pour apporter un moyen de contrôle sur l'acheminement de données. L'émission des messages se fait également sans garantie ce qui signifie qu'UDP ne garantit pas la livraison et la vérification de la mise en séquence des datagrammes. L'hypothèse du non fiabilité de la

transmission avec UDP est alors vérifiée. En même temps, le contrôle de flux limitant des données volumineuses reçues par le récepteur n'existe pas avec le protocole UDP. [3]

On utilise UDP pour un transport rapide où la perte occasionnelle des paquets n'est pas critique.

1.3.3 Comparaison des protocoles TCP et UDP

En se référant aux caractéristiques de ces deux protocoles : on peut déduire que contrairement à TCP qui ne tolère aucune erreur en transmettant et en retransmettant plusieurs fois jusqu'à ce qu'ils soient corrects à l'arrivée, les impératifs de la transmission en temps réel rendent UDP plus adapté aux programmes qui présentent les exigences en temps réel (la voix, la vidéo,...). D'autant plus, UDP tolère les erreurs donc il est adapté aux situations où la perte occasionnelle des paquets n'est pas critique. [2]

Exemple : une perte de quelques pixels dans une image est tolérable vue que cela ne soit pas perçue par l'œil humain.

Le tableau 1.02 établit une comparaison des différents modes de gestion des communications suivant que le protocole UDP et TCP soit utilisé ou non pour le transport des données.

UDP	TCP
Service sans connexion : aucune session n'est établie entre les machines.	Service orienté connexion : une session est établie entre les machines.
UDP ne garantit pas la réception des données de livraison ou de séquence (pas d'accusé de réception)	TCP garantit la livraison à l'aide des accusés de réception et la livraison des données en séquence.
UDP tolère les pertes dans la transmission des données.	TCP ne tolère aucune perte dans la transmission des données.
UDP est rapide et présente des exigences de faible délai et peut prendre en charge des communications point à point à multipoint.	TCP est plus lent et présente des exigences de délai plus élevé. Il ne peut prendre en charge que les communications point à point.

Tableau 1.02: Comparaison de TCP et UDP

1.4 Conclusion

On entend souvent qu'avant le déploiement de l'IPv6, la prochaine version du protocole IP, il sera impossible de déployer à grande échelle des applications de voix sur IP à cause de manque d'adresses. Ceci est totalement faux. La sophistication des outils de routage disponibles en IPv4 et l'utilisation combinée de passerelles applicatives de voix sur IP rendent possible l'utilisation d'un ensemble limité d'adresses pour fournir un service à un ensemble potentiellement illimité d'utilisateurs. A cause de la taille plus faible des paquets de données IPv4, la latence sur tels réseaux, particulièrement sur les liens d'accès, sera meilleure que sur un réseau IPv6 équivalent, et l'efficacité du protocole IPv4 pour de tels paquets est également bien meilleure.

Enfin, UDP est plus adapté aux programmes qui présentent des exigences en temps réel (voix sur IP, téléphonie sur IP,...)

CHAPITRE 2

LA VOIX SUR IP

2.1 Présentation de la voix sur IP (VoIP)

2.1.1 Introduction à la VoIP

La voix sur IP constitue actuellement l'évolution la plus importante du domaine des télécommunications. La VoIP correspond à l'ensemble des technologies permettant la transmission d'une conversation sur un réseau de protocole IP. La communication par VoIP est plus flexible et permet de déployer simultanément d'autres services que le transport de la voix, comme par exemple la vidéo ou les données (ce qu'on entend par triple play : voix, données et vidéo). Avec la technologie VoIP, la voix est donc numérisée, compressée et envoyée sous forme de paquets sur un réseau fonctionnant avec le protocole IP. Les données reçues sont décompressées et converties en voix audible.

La VoIP peut être définie comme la possibilité d'effectuer des appels téléphoniques et d'envoyer des fichiers à travers un réseau de données à base du protocole IP à une qualité acceptable et à des prix abordables voire symboliques. On peut ainsi communiquer, par écran interposé, n'importe où dans le monde sans aucune considération financière puisque le prix est toujours celui d'une communication locale. Nous assistons à une révolution au niveau des tarifs qui s'annoncent démesurément bas. [6]

Le but de la VoIP est la convergence voix/données autour d'un protocole unique IPv4 (éventuellement IPv6). En effet, la VoIP se base sur la même architecture que l'Internet et utilise les mêmes infrastructures. En intégrant la voix et les données, la VoIP simplifie l'administration des réseaux car tout est centralisé dans un unique réseau (réseau LAN) et non deux (réseau téléphonique et réseau LAN). Elle procure ainsi des facilités pour le développement d'applications utilisant la voix et les données. Nous pourrions par exemple bénéficier des applications coopératives ; les utilisateurs peuvent dialoguer avec un correspondant, tout en consultant simultanément les mêmes données sur leur ordinateur, grâce aux infrastructures Internet. Le développement actuel des technologies IP devrait faciliter le travail de coopération multimédia. [6]

Ainsi, au contraire de téléphones analogiques filaires RTC dépendant de centraux téléphoniques dédiés, la voix sur IP permet le transport de conversations téléphoniques sur tout réseau numérique acceptant le protocole TCP/IP (Ethernet, PPP,...).

2.1.1.1 Contexte technologique de la VoIP

Si à l'origine le protocole IP a été conçu pour fournir des services de type « best effort », les réseaux IP représentent désormais une part importante des infrastructures de télécommunications et ont vocation à transporter de nombreux services avec leurs contraintes de disponibilité (applications distantes, voix, vidéo, télévision, etc.).

Avant 1996, les solutions de voix sur IP reposaient sur des architectures propriétaires. Ces solutions présentaient des défauts parmi lesquels : la manque d'interopérabilité des équipements, l'impossibilité de raccordement au réseau public (seuls les ordinateurs pouvaient communiquer entre eux), l'absence d'architecture générale pour la connexion de n'importe quel type de terminal, chaque architecture était définie pour deux équipements d'extrémité spécifiques et ne pouvait pas interopérer avec d'autres architectures d'équipements. [5]

2.1.1.2 Traitement et transmission de la voix en mode paquet

Pour acheminer la voix à travers le réseau IP, il faut réduire au maximum le signal vocal en lui apportant le moins de dégradations possibles car le débit nominal de transport de la voix codée MIC (Modulation par Impulsions et Codage) à travers le RTC (Réseau Téléphonique Commuté) est de 64 kbps, alors que celui d'un réseau IP est nettement inférieure à 64 kbps (14.4, 28.8, 56 kbps).

Pour comprendre le traitement complexe de la voix analogique (signaux électriques) en signaux binaires, voici un synoptique explicatif qui est représenté par la figure 2.01:

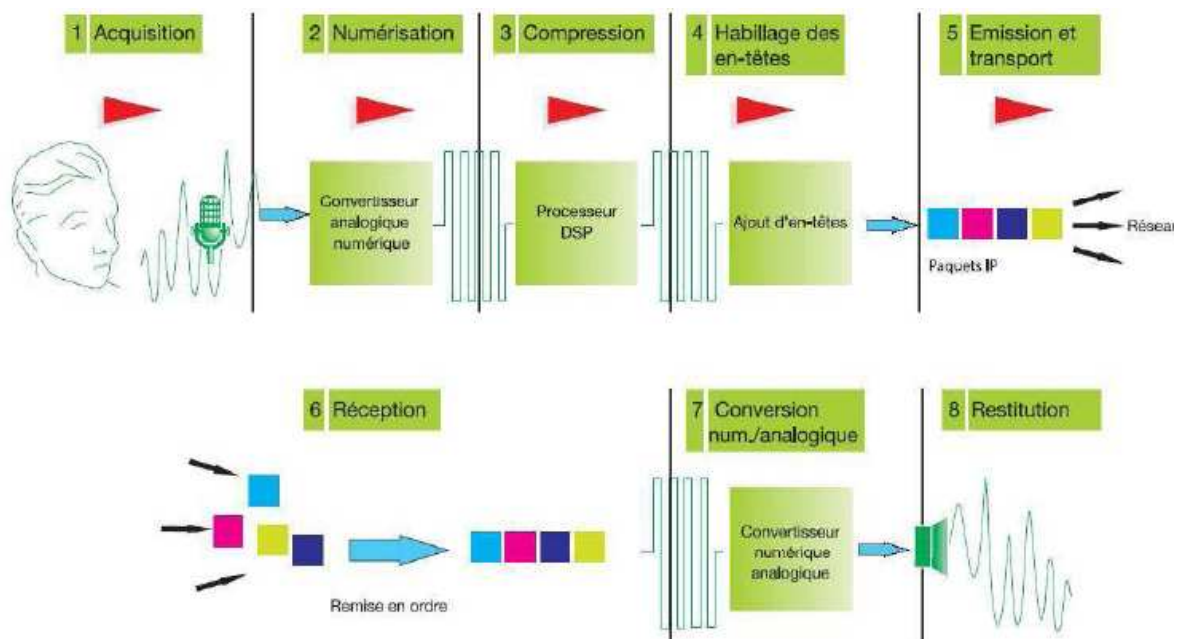


Figure 2.01: *Synoptique de transmission de la voix analogique en mode paquet.*

La bande voix qui est un signal électrique analogique utilisant une bande de fréquence de 300 à 3400 Hz, est d'abord échantillonnée numériquement par un convertisseur et codée sur 8 bits. Par la suite, elle est compressée par des codecs (il s'agit de processeurs DSP : Digital System Processing) selon une certaine norme de compression, variable selon les codecs utilisés, et ensuite on peut éventuellement supprimer les pauses de silences observés lors d'une conversation, pour ensuite ajouter les en-têtes RTP, UDP et enfin IP. Une fois que la voix est transformée en paquets IP, ces petits paquets IP identifiés et numérotés peuvent transiter sur n'importe quel réseau IP (ADSL, Ethernet, Satellite, routeurs, switchs, PC, Wifi, etc...). [6]

A l'arrivée, les paquets transmis sont réassemblés et le signal de données ainsi obtenu est décompressé puis converti en signal analogique pour restitution sonore à l'utilisateur.

2.1.2 Les codages de la VoIP

2.1.2.1 Introduction

Une information à émettre est toujours sous forme d'un signal qui peut être numérique ou analogique. Fondamentalement, un signal est toujours une grandeur physique analogique. La différence consiste dans le type d'information que celui-ci transporte. Un signal

analogique prend des valeurs continues et varie en amplitude, fréquence et phase. Un signal numérique prend une série de valeurs discrètes représentées par un signal élémentaire appelé moment. Les signaux analogiques peuvent être convertis en signaux numériques et inversement par des équipements appelés CODEC (codeur/décodeur).

Pour faire passer la voix dans un réseau IP, il faut tenir compte de certains paramètres. On estime la bande passante de la voix à 4 kHz (400-3400 Hz). Ce qui donne après numérisation une bande passante de 8 kHz et après codage un débit de 64 kbps. Ceci entraîne que si on veut transmettre la voix sur un réseau IP sans mécanisme d'optimisation de la taille il nous faudra une bande passante « continue » de 64 kbps rien que pour la partie : données à transmettre. [5]

Toutefois, ceci est rarement le cas, car à l'aide de mécanisme de codage optimisé grâce aux lois de compression de l'information, on arrive à réduire ce débit nécessaire de plus de 8 fois pour les meilleurs algorithmes de codages.

Le choix d'un codeur est un processus en général très long. Avant de sélectionner un codeur, l'UIT en teste la qualité subjective par le score MOS (Mean Opinion Score) qui est la note moyenne attribuée par un panel d'auditeurs écoutant des séquences enregistrées dans diverses conditions (voix, voix et musique, voix et bruit de fond...) et qui varie de 1 à 5. L'UIT exige aussi une qualité équivalente ou supérieure à la qualité commerciale « toll quality » correspondant à des notes de 3.5 à 4 de MOS. [6]

2.1.2.2 Les différents types de codecs utilisés en VoIP

Le terme codec est construit d'après les mots codeur et décodeur, et fait appel à la compression et décompression des données.

Il s'agit d'un procédé algorithmique permettant, en général, de réduire la taille du fichier original par des facteurs allant de 2 à 100 (voire plus pour certaines applications).

La compression se fait soit avec des algorithmes purement mathématiques de compression de données sans perte d'information ou par des algorithmes prenant en compte les caractéristiques des données à compresser et qui peuvent perdre des informations dites « non pertinentes ». [6]

Afin d'avoir la meilleure qualité possible de la voix après avoir passé au travers d'un codec, on a défini les exigences suivantes :

- Robustesse contre les erreurs binaires : masquage d'erreur nécessaire (utilisation d'outils tels que la protection inégale contre les erreurs);
- Robustesse contre les pertes de paquets : généralement, pas de temps pour demander la retransmission de paquets; dégradation progressive de la qualité vocale en cas de perte (par exemple par la production d'un supplément vocal et d'un bruit de fond).

Les principaux codecs utilisés en VoIP sont résumés dans le tableau 2.01 :

Standards	Méthode de codage	Débits (kbps)	Délais de traitement (ms)
G.711	PCM	64	0.125
G.726	ADPCM	32	0.125
G.728	LPAS, CELP	16	0.625
G.729	LPAS, CS-ACELP	8	15
G.723.1	ACELP, MP-MLQ	6.4/ 5.3	37.5

Tableau 2.01 : Les codecs de la VoIP

Généralement l'utilisateur peut paramétrer son logiciel de VoIP et ainsi le codec qui lui convient. Il est cependant recommandé d'utiliser soit le G.711 soit le G.729 vu qu'ils détiennent les meilleurs scores de MOS.

Remarque :

Le G.723.1 possède deux débits différents car il utilise deux types de compression qui sont le MP-MLQ (6.4 kbit/s) et ACELP (5.3 kbit/s). Mais pour les autres, bien qu'utilisant des méthodes de codage différents, le débit est toujours identique (exemple : G.729).

2.1.2.3 Le MOS

Note d'opinion moyenne (*Mean Opinion Score* ou MOS) est une note donnée à un codec audio pour caractériser la qualité de la restitution sonore. La note peut varier entre 0 (très mauvais) et 5 (excellent, comparable à la version d'origine). Il est défini par l'UIT-T comme la norme « P.800 : Méthodes d'évaluation subjective de la qualité de transmission ». [6]

L'échelle utilisée pour l'évaluation de la qualité de la voix est représentée par le tableau 2.02 :

Qualité de la parole	Score
Excellente	5
Bonne	4
Correcte	3
Pauvre	2
Insuffisante	1

Tableau 2.02 : *Echelle utilisée pour l'évaluation de la qualité de la voix*

Le principe de calcul du MOS est basé sur un sondage d'un échantillon supposé représentatif de la population des utilisateurs. Les personnes constituant l'échantillon sont invitées à écouter un signal (souvent de la voix), puis son équivalent codé-décodé. Après chaque écoute, l'auditeur donne une note sanctionnant la qualité qu'il a perçue. La moyenne des notes fournies par la population constitue le MOS. Le tableau ci-dessous montre les résultats obtenus par quelques codecs courants. [5]

Le tableau 2.03 représente la valeur du score MOS des différents codecs utilisés pour la voix sur IP :

Nom	Débit	Utilisation typique	Score MOS
G.711	64 kbit/s	VoIP, RNIS	4.1
G.729a	8 kbit/s	VoIP	3.9
G.726	32 kbit/s	VoIP, DECT	3.85
G.723	5.3 kbit/s	VoIP	3.6
RPE-LTP	9.6 kbit/s	GSM	3.5

Tableau 2.03: *Score MOS des différents codecs*

2.2 Normes et protocoles de la VoIP

La VoIP met en œuvre des techniques de télécommunications sur un réseau de paquets. Une normalisation de la signalisation est donc bien entendu nécessaire pour garantir l'interopérabilité des appareils. Outre le protocole IP, plusieurs protocoles assurent le bon fonctionnement de la technologie VoIP.

Jusqu'à présent, il existe trois standards ou protocoles qui permettent la mise en place d'un « service » VoIP. Le plus connu est le standard H.323. Ensuite, plus ancien, le MGCP (Media Gateway Control Protocol). Et le plus récent est le SIP. Les plus populaires sont H.323 et le SIP. H.323 est plus difficile à mettre en œuvre par rapport à SIP et que sa description est plus complexe. [3] [6]

2.2.1 Le protocole H.323

2.2.1.1 Introduction

Avec le développement du multimédia sur les réseaux, il est devenu nécessaire de créer des protocoles qui supportent ces nouvelles fonctionnalités, telles que la visioconférence: l'envoi de son et de vidéo avec un souci de données temps réel. Le protocole H.323 est l'un d'eux. Il permet de faire de la visioconférence sur des réseaux IP.

H.323 est un protocole de communication englobant un ensemble de normes utilisées pour l'envoi de données audio et vidéo sur Internet. Il existe depuis 1996 et a été initié par l'ITU (International Communication Union). Concrètement, il est utilisé dans des programmes tels que Microsoft Netmeeting, ou encore dans des équipements tels que les routeurs Cisco. [3]

2.2.1.2 Fonctionnement

Le protocole H.323 est utilisé pour l'interactivité en temps réel, notamment la visioconférence (signalisation, enregistrement, contrôle d'admission, transport et encodage). C'est le leader du marché pour la téléphonie sur IP. Il s'inspire du protocole H.320 qui proposait une solution pour la visioconférence sur un réseau numérique à intégration de service (RNIS ou ISDN en anglais), comme par exemple le service Numéris proposé par France Telecom. Le protocole H.323 est une adaptation de H.320 pour les réseaux IP. A l'heure actuelle, la visioconférence sur liaison RNIS est toujours la technique la plus déployée. Elle existe depuis 1990. Les réseaux utilisés sont à commutation de circuits. Ils permettent ainsi de garantir une Qualité de Service (QoS) aux utilisateurs (pas de risque de coupure du son ou de l'image). Aujourd'hui, c'est encore un avantage indiscutable. Par contre, comme pour le téléphone, la facturation est fonction du débit utilisé, du temps de communication et de la distance entre les appels. [5]

2.2.1.3 Architecture H.323

H.323 définit plusieurs éléments de réseaux :

Les terminaux - Dans un contexte de Voix sur IP, deux types de terminaux H.323 sont Aujourd'hui disponibles. Un poste téléphonique IP raccordés directement au réseau Ethernet de l'entreprise. Un PC multimédia (muni d'une carte son et d'un micro) sur lequel est installé une application compatible H.323. Éventuellement, le terminal peut être doté d'un système de transmission d'images et de données, mais ce n'est pas obligatoire. Cet appareil joue un rôle clé dans VoIP car c'est à partir de lui que seront émises et reçues les conversations des utilisateurs. Le rôle premier du standard H.323 est de permettre les échanges entre les terminaux. [6]

Les passerelles (GW: Gateway) - Elles assurent l'interconnexion entre un réseau IP et le réseau téléphonique, ce dernier pouvant être soit le réseau téléphonique public, soit un PABX d'entreprise. Elles assurent la correspondance de la signalisation et des signaux de contrôle et la cohésion entre les médias. Pour ce faire, elles implémentent les fonctions suivantes de transcodage audio (compression, décompression), de modulation, démodulation (pour les fax), de suppression d'échos, de suppression des silences et de contrôle d'appels. Les passerelles sont le plus souvent basées sur des serveurs informatiques standards (Windows NT, Linux) équipés d'interfaces particuliers pour la téléphonie (interfaces analogiques, accès de base ou accès primaire RNIS, interface E1, etc.) et d'interfaces réseau, par exemple de type Ethernet. La fonctionnalité de passerelle peut toutefois être intégrée directement dans le routeur ainsi que dans les PABX eux-mêmes. [6]

Les portiers (GK: Gatekeeper) - Ils sont des éléments optionnels dans une solution H.323. Ils ont pour rôle de réaliser la traduction d'adresse (numéro de téléphone - adresse IP) et la gestion des autorisations. Cette dernière permet de donner ou non la permission d'effectuer un appel, de limiter la bande passante si besoin et de gérer le trafic sur le LAN. Les "gardes-barrière" permettent également de gérer les téléphones classiques et la signalisation permettant de router les appels afin d'offrir des services supplémentaires. Ils peuvent enfin offrir des services d'annuaires. [6]

Les unités de contrôle multipoint (MCU, Multipoint Control Unit) - Référence au protocole T.120 qui permet aux clients de se connecter aux sessions de conférence de données. Les unités de contrôle multipoint peuvent communiquer entre elles pour échanger des informations de conférence. [6]

L'architecture H.323 est représentée par la figure 2.02 :

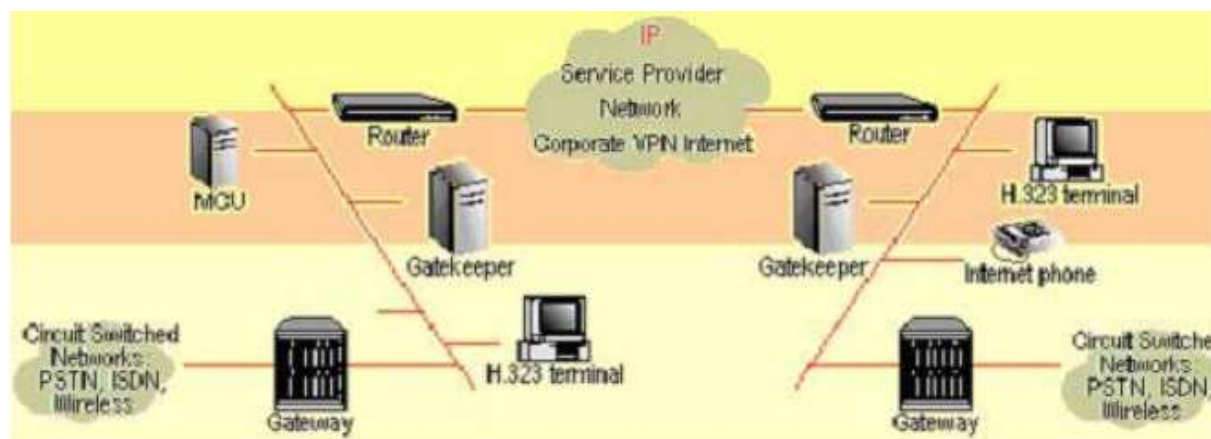


Figure 2.02 : *Architecture H.323*

2.2.1.4 Les protocoles secondaires de H.323

Comme indiqué précédemment, H.323 ressemble davantage à une association de plusieurs protocoles différents et qui peuvent être regroupés en trois catégories : la signalisation, la négociation de codec, et le transport de l'information.

Trois protocoles de signalisation sont spécifiés dans le cadre de H.323 à savoir :

RAS (Registration, Admission and Status) : Ce protocole est utilisé pour communiquer avec un Gatekeeper. Il sert notamment aux équipements terminaux pour découvrir l'existence d'un Gatekeeper et s'enregistrer auprès de ce dernier ainsi que pour les demandes de traduction d'adresses. La signalisation RAS utilise des messages H.225.0 transmis sur un protocole de transport non fiable (UDP, par exemple).

Q.931 : H.323 utilise une version simplifiée de la signalisation RNIS Q.931 pour l'établissement et le contrôle d'appels téléphoniques sur IP. Cette version simplifiée est également spécifiée dans la norme H.225.0.

H.245 : ce protocole est utilisé pour l'échange de capacités entre deux équipements terminaux. Par exemple, il est utilisé par ces derniers pour s'accorder sur le type de codec à activer. Il peut également servir à mesurer le retard aller-retour (Round Trip Delay) d'une communication. [5]

L'établissement d'une communication H.323 diffère selon que le système utilise ou non un Gatekeeper. En mode direct (sans Gatekeeper), le terminal qui établit un appel E.164 assure lui-même la traduction d'adresse, la liaison est établie directement par un échange de

messages H.225 et H.245. En mode Gatekeeper, le terminal appelant interroge, au préalable, le gatekeeper pour traduire et obtenir l'autorisation d'appeler son correspondant (garantie de bande passante pour accepter un nouveau flux). De même, le correspondant n'accepte l'appel qu'après autorisation de son gatekeeper. [6]

2.2.1.5 Phases d'appel de H.323

Une communication H.323 se déroule en cinq phases :

- Établissement d'appel
- Échange de capacité et réservation éventuelle de la bande passante à travers le protocole RSVP (Ressource reSerVation Protocol)
- Établissement de la communication audio-visuelle
- Invocation éventuelle de services en phase d'appel (par exemple, transfert d'appel, changement de bande passante, etc.)
- Libération de l'appel. [4]

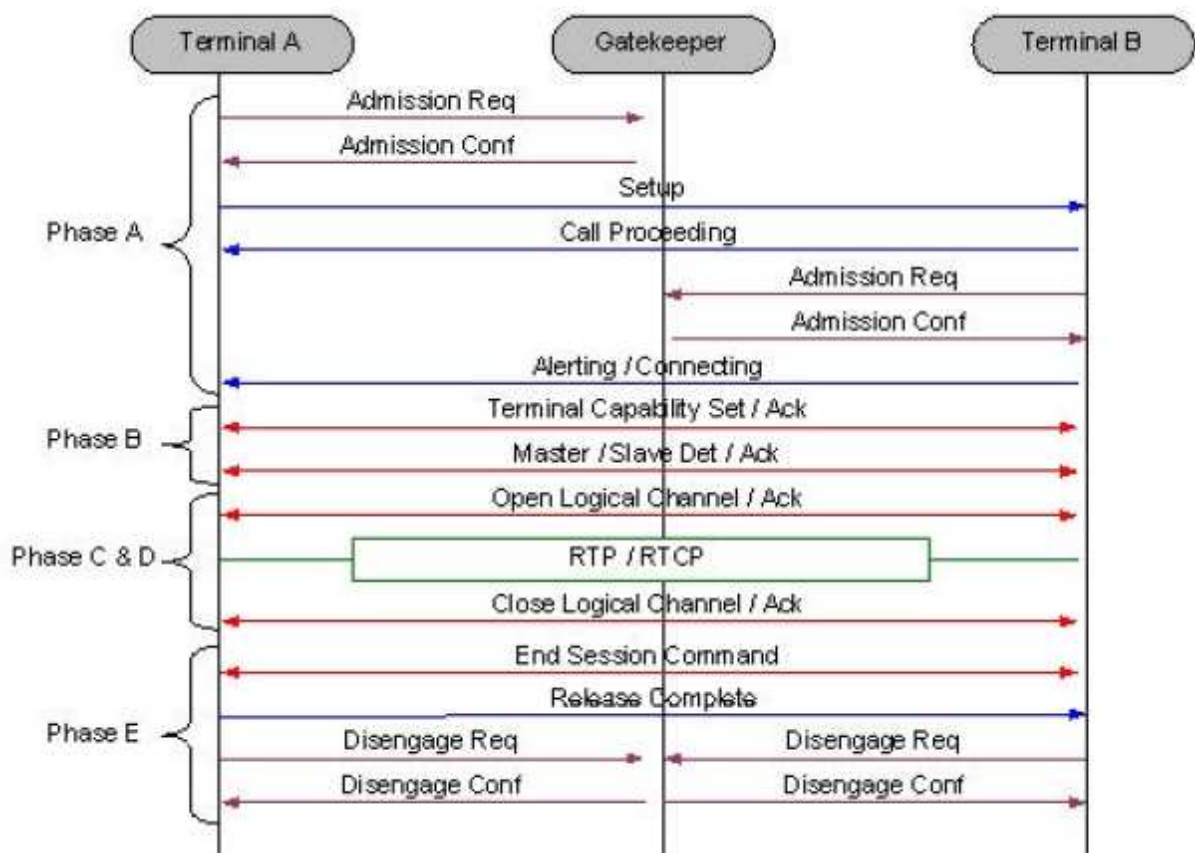


Figure 2.03 : Signalisations d'appel H.323.

2.2.1.6 H.323 dans le modèle OSI

Les différents protocoles sont représentés par la figure 2.04 dans le modèle OSI :

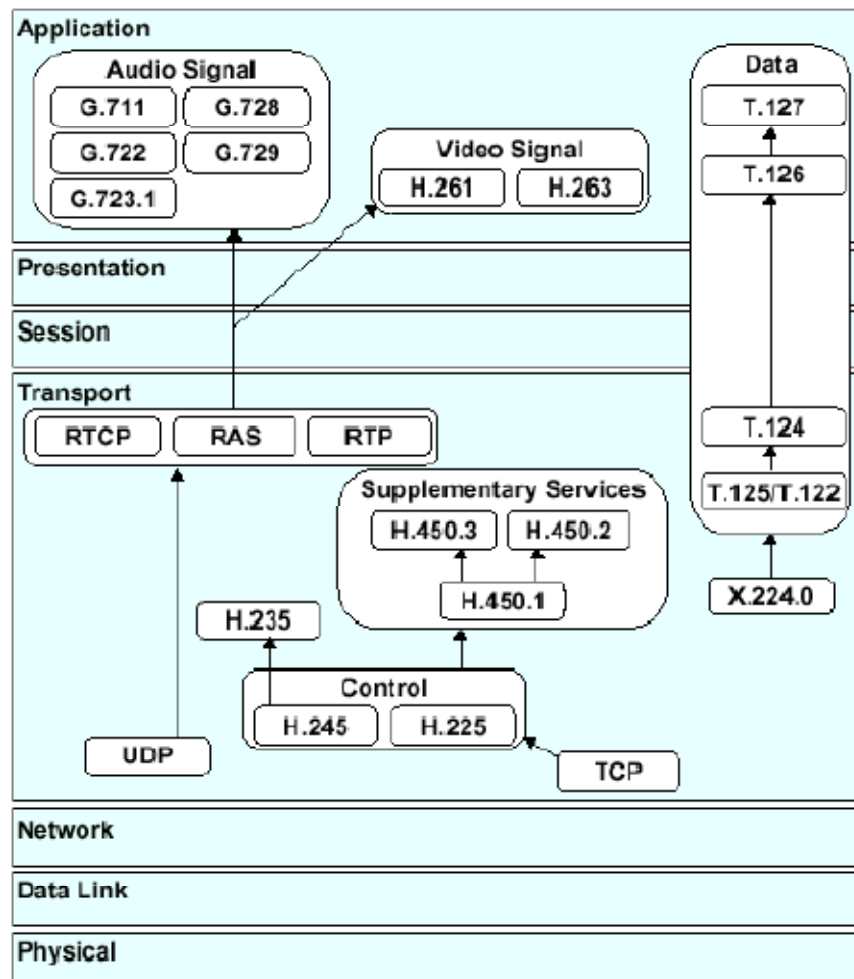


Figure 2.04 : H.323 dans OSI

Cette structure nous fait remarquer que H.323 rassemble de nombreux protocoles représentés dans le tableau 2.04:

Rôle	Normes	Description
Terminal, contrôle et administration	H.225	Signalisation d'appels, paquets des signaux, état et admission au garde-barrière
	H.245	Contrôle (négociation et établissement de sessions)
	RTP	Protocole de transport pour les applications temps réels
	RTCP	Contrôle de flux de données multimédia
	RSVP	Réservation d'une ressource en bande passante
Données	T.120	Contrôle des données
Applications audio/vidéo	G.7xx	Codec audio
Services supplémentaires	H.450	Divers services supplémentaires (attente,...)
Sécurité	H.235	Procédure de sécurité dans l'environnement H.323

Tableau 2.04 : *Les normes de H.323*

2.2.2 Protocole SIP

2.2.2.1 Introduction

Le protocole SIP (Session Initiation Protocol) a été initié par le groupe MMUSIC (Multiparty Multimedia Session Control) et désormais repris et maintenu par le groupe SIP de l'IETF donnant la RFC 3261 rendant obsolète la RFC 2543. SIP est un protocole de signalisation appartenant à la couche application du modèle OSI. Son rôle est d'ouvrir, modifier et libérer les sessions. L'ouverture de ces sessions permet de réaliser de l'audio ou vidéoconférence, de l'enseignement à distance, de la voix (téléphonie) et de la diffusion multimédia sur IP essentiellement. Un utilisateur peut se connecter avec les utilisateurs d'une session déjà ouverte. Pour ouvrir une session, un utilisateur émet une invitation transportant un descripteur de session permettant aux utilisateurs souhaitant communiquer de s'accorder sur la compatibilité de leur média, SIP permet donc de relier des stations mobiles en transmettant ou redirigeant les requêtes vers la position courante de la station appelée. Enfin, SIP possède l'avantage de ne pas être attaché à un médium particulier et est sensé être indépendant du protocole de transport des couches basses. [6]

2.2.2.2 Fonctionnement

SIP intervient aux différentes phases de l'appel :

- Localisation du terminal correspondant,
- Analyse du profil et des ressources du destinataire,
- Négociation du type de média (voix, vidéo, données...) et des paramètres de communication,
- Disponibilité du correspondant, détermine si le poste appelé souhaite communiquer, et autorise l'appelant à le contacter.
- Etablissement et suivi de l'appel, avertit les parties appelant et appelé de la demande d'ouverture de session, gestion du transfert et de la fermeture des appels.
- Gestion de fonctions évoluées : cryptage, retour d'erreurs, ... [5]

2.2.2.3 Les clients et les serveurs de SIP

Dans un système SIP, on trouve deux types de composantes, les users agents (UAS, UAC) et un réseau de serveurs :

- L'UAS (User Agent Server) : représente l'agent de la partie appelée. C'est une application de type serveur qui contacte l'utilisateur lorsqu'une requête SIP est reçue. Et elle renvoie une réponse au nom de l'utilisateur.
- L'UAC (User Agent Client) : représente l'agent de la partie appelante. C'est une application de type client qui initie les requêtes SIP.

a. Les clients SIP

Le protocole SIP fonctionne en mode client/serveur, dans un même terminal client on trouve deux applications : UAC (User Agent Client) qui émet les requêtes et UAS (User Agent Server) qui reçoit les requêtes. Et le terminal fonctionne seulement comme l'un ou l'autre par transaction. Ces deux applications ensemble, forment le UA (User Agent). Un terminal A peut appeler directement un terminal B ou passer par des serveurs. Un client doit avoir un minimum de méthodes afin d'établir la connexion. Les échanges entre un terminal appelant et un terminal appelé se font par l'intermédiaire de requêtes. [5]

b. *Les serveurs SIP*

- Le Proxy Server (PS) : ou serveur de délégation ou encore relais mandataire, auquel est relié un terminal fixe ou mobile. Il a pour fonction de relayer les requêtes. Chaque terminal est relié au PS le plus proche et peut changer de PS. Le PS agit à la fois comme client et serveur. Il peut interpréter et modifier les messages qu'il reçoit avant de les retransmettre. Il y a deux sortes de proxy : les proxys « stateful » et « stateless », la différence est le fait que le proxy « stateful » enregistre la position du destinataire tandis que le proxy « stateless » ne la mémorise pas. Ce qui fait que le proxy « stateful » consulte une seule fois le serveur de localisation par destination jusqu'à ce que la destination soit effacée de sa « table de routage ».
- Le Redirect Server (RS) : il fournit une adresse alternative à laquelle l'appelé peut être joint.
- Le ReGistrar (RG) : c'est un équipement qui permet d'enregistrer les localisations des User Agents. En fait, chaque PS ou RS est généralement relié à un Registrar.)
- Le Location Server (LS) : ce serveur fournit la position courante des utilisateurs dont les communications traversent les RS et les PS). [5]

L'architecture SIP est représentée par la figure 2.05 :

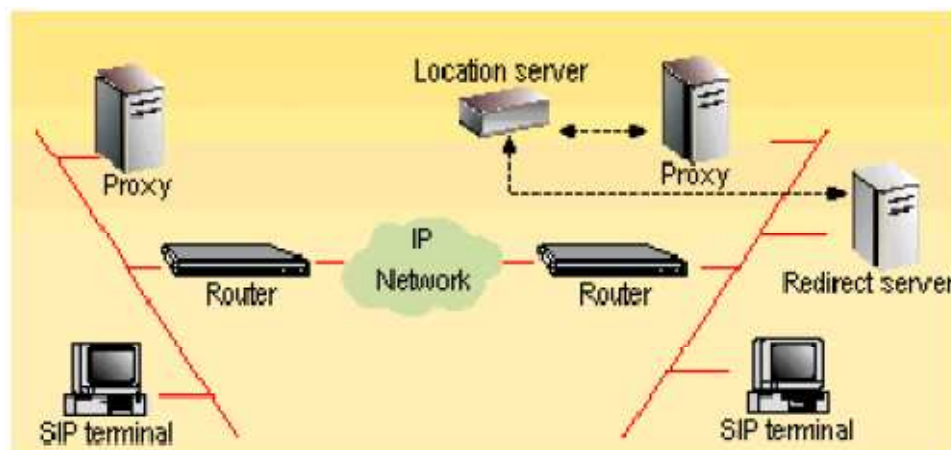


Figure 2.05 : Architecture SIP

2.2.2.4 Comparaison de SIP avec H.323

Les protocoles SIP et H.323 représentent les standards définis jusqu'à présent pour la signalisation à propos de la téléphonie sur Internet. Ils représentent tous deux des approches différentes pour résoudre un même problème. Ils remplissent les mêmes rôles mais suivant

des complexités nettement différentes. SIP est plus évolutif que H.323, il sera bien de se renseigner sur des calculs de performances de chacun d'eux et d'adopter la meilleure solution suivant les besoins. [6]

Le tableau 2.05 représente la comparaison entre SIP et H.323 :

	SIP	H.323
Nombre d'échanges pour établir la connexion	1,5 aller-retour	6 à 7 allers-retours
Maintenance du code protocolaire	Simple par sa nature textuelle à l'exemple de http	Complexe et nécessitant un compilateur
Evolution du protocole	Protocole ouvert à de nouvelles fonctions	Ajout d'extensions propriétaires sans concertation entre vendeurs
Fonction de conférence	Distribuée	Centralisée par l'unité MC
Fonction de téléservices	Oui, par défaut	H.323 v2 + H.450
Détection d'un appel en boucle	Oui	Inexistante sur la version 1 un appel routé sur l'appelant provoque une infinité de requêtes
Signalisation multicast	Oui, par défaut	Non

Tableau 2.05: comparaison entre SIP et H.323

2.2.2.5 Conclusion

La simplicité, la rapidité et la légèreté d'utilisation, tout en étant très complet, du protocole SIP sont autant d'arguments qui pourraient permettre à SIP de convaincre les investisseurs. De plus, ses avancées en matière de sécurité de messages sont un atout important par rapport à ses concurrents.

2.2.3 *Protocole MGCP*

Le protocole MGCP (Media Gateway Control Protocol) est complémentaire à H.323 ou SIP, et traite des problèmes d'interconnexion avec le monde téléphonique. C'est un protocole de contrôle des gateways. Les éléments de contrôle utilisés sont les « Call Agents » ou « Media Gateway Controllers ». Ces éléments :

- Fournissent des signaux d'appels, de contrôle et des processus intelligents aux gateways.
- Envoyent et reçoivent également des commandes des gateways.

Les commandes du « call agent » sont : la configuration des terminaux, les requêtes de modification et la suppression d'une connexion, et aussi, l'audit des terminaux ainsi que l'audit des connexions. Une amélioration de ce protocole s'appelle MEGACO (Media Gateway Controller) développé conjointement par l'UIT et l'IETF. [6]

2.2.4 *Protocoles RTP et RTCP*

2.2.4.1 Protocole RTP

RTP (Real-time Transport Protocol) et son compagnon RTCP (Real-time Transport Control Protocol) permettent respectivement de transporter et de contrôler des flots de données qui ont des propriétés temps-réel.

RTP fournit un transport de bout en bout sur un réseau, c'est à dire entre les utilisateurs, pour les applications transmettant des données en temps réel, tel que de l'audio ou de la vidéo, en unicast et en multicast. RTP ne se préoccupe pas de la réservation de ressources et ne garantit pas la qualité de service des transferts de données en temps réel. Pour cela il est agrémenté d'un protocole de contrôle, le RTCP, qui permet le suivi dans la livraison des données. Il fournit un contrôle minimal et des fonctions d'identification particulièrement utiles dans le

cas de réseaux multicast. RTP et RTCP sont conçus pour être indépendants des réseaux sous-jacents. [2]

Le format de paquets est partagé par deux protocoles :

- Le protocole de transport temps réel pour l'échange de données aux propriétés temps réel. L'entête RTP est composée d'une partie de longueur fixe à laquelle s'ajoutent des champs optionnels.
- Le protocole de contrôle de RTP pour faire circuler les informations sur les participants à une session en cours. RTCP consiste en des options d'entêtes supplémentaires qui peuvent être ignoré sans risque de ne pas recevoir les données. RTCP est utilisé pour le contrôle des pertes, c'est à dire quand il n'y a pas de contrôle explicite déjà utilisé. Les fonctionnalités de RTCP doivent être conjuguées avec un protocole de contrôle sous-jacent.

L'Internet d'aujourd'hui ne supporte pas l'utilisation des services temps réel dès lors qu'il faut traverser des routeurs. De plus, des services gourmand en bande passante, tel que le transfert de vidéos, peut potentiellement dégrader les autres services du réseau. C'est aux programmeurs de prendre toutes les dispositions pour limiter l'usage excessif de bande passante.

Après ces considérations générales sur RTP et RTCP voyons comment ils fonctionnent.

2.2.4.2 Utilisation de RTP

Le but du protocole RTP est de transporter des données qui ont des propriétés temps-réel. Il fournit des services de livraison pour des applications multimédias, ainsi que des moyens pour ces applications de travailler sur les réseaux. Il confie l'assurance de la livraison des paquets aux services de plus bas niveau, n'offre pas de garantie sur la séquence de livraison mais délivre un numéro de séquence qui permet de détecter les paquets manquants, et les paquets hors séquence. Il faut s'assurer que l'on peut compter sur les couches inférieures et notamment que celles-ci délivrent les paquets dans l'ordre d'émission. Les numéros de paquets inclus dans RTP permettent au système final de reconstruire la séquence de paquets de l'expéditeur. RTP est défini pour fonctionner dans les situations caractérisées par des transmissions de type un à un ou de type un à plusieurs. [6]

RTP peut se mettre au dessus d'une panoplie variée de protocole réseaux et de transport

comme IP, ou UDP (mais il transporte habituellement des données en utilisant UDP comme mécanisme de livraison), mais est défini comme étant indépendant des protocoles de transport.

RTP transfère des données mono directionnelle vers éventuellement des destinations multiples si le réseau sous-jacent le permet. On a toutefois la possibilité de transférer des informations de contrôle dans le sens opposé à la transmission RTP. [6]

Lorsqu'une application démarre une session RTP, elle fait appel à deux ports : un port RTP et un second port pour le protocole RTCP, décrit après. Les données multimédias sont transmises en deux sessions; l'une pour le son, l'autre pour la vidéo.

RTP ne fournit pas de mécanisme de transport fiable pour livrer des paquets en séquence. Il n'offre pas non plus de contrôle de flux ou de congestion et dépend de RCTP pour fournir ces services.

Les paquets RTP de données contiennent une durée variant de 0 à 200ms, ce qui est envisageable et raisonnable en ce qui concerne un buffering, la durée moyenne la plus couramment utilisée des paquets est de 20ms. Ces données sont précédées par douze octets qui représentent l'entête RTP. [6]

L'entête RTP est représenté par la figure 2.06 :

V	P	X	CC	M	Payload type	Sequence number
HORODATAGE						
IDENTIFICATEUR DE SOURCE (SSRC)						
IDENTIFICATEUR(S) de CONTRIBUTEUR (CSRC)						

Figure 2.06 : Entête du protocole RTP

2.2.4.3 Protocole RTCP

Maintenant nous allons voir ce qui est transmis par le port RTCP. Le protocole RTCP est basé sur des transmissions périodiques de paquets de contrôle par tous les participants dans la session. Chaque participant envoie de tels paquets à son tour. L'intervalle de temps entre l'envoi des paquets est calculé dynamiquement en rapport au nombre de SSRC différent connecté à une session. [5]

Le RTCP a quatre fonctions :

- La première est de donner une meilleure qualité de distribution des paquets RTP. Ceci, tant en ce qui concerne la connaissance du nombre de paquets perdus, et peut-être les raisons, qu'en ce qui concerne la congestion du réseau. Il permet donc un encodage évolutif utilisant des bandes passantes plus ou moins faibles et de plus ou moins bonne qualité.
- Il transporte le nom canonique (canonical name) CNAME d'un utilisateur. Ce CNAME est un identifiant persistant d'une source, et ceci pour toutes les connections. Il est utile pour retrouver ses partenaires, et que les partenaires le reconnaissent lors d'une reconnexion, alors que le numéro SSRC lui change. Il est aussi utile dans la synchronisation de deux sessions telles qu'une session audio et une session vidéo.
- Chacun peut savoir combien de personnes font partie de la conférence.
- Permet de transporter un minimum de fonctions de contrôle. Cette fonctionnalité est bien sûr optionnelle mais très pratique.

Les paquets RTCP possèdent le même header de base que les paquets RTP de données. Ils sont terminés par 32 bits de liaison qui leur permettent d'être empilé dans un « compound packet » (ou appelé par abus simplement " compound "). Ce dernier contient en tout premier, et s'il y a lieu qu'ils soient présents, 32 bits de données de cryptage. Le cryptage sert de protection des données, c'est l'unique niveau de sécurité proposé par le protocole.

Ensuite un compound débute toujours par un paquet de rapport, même vide. Ce paquet peut être de deux formes, soit un rapport d'émetteur (sender report) SR, soit un rapport de récepteur (receiver report) RR. La partie fixe minimum d'un paquet SR est de 4 octets. Un paquet SR peut contenir des informations de la partie émetteur (sender info) sur 6 mots de 32 bits (48 octets) et ou des informations de la partie récepteur (report block) sur 6 mots de 32 bits (48 octets). [6]

Puis le compound peut contenir un RR additionnel si le nombre de rapport de récepteur est supérieur à trente et un.

Le compound contient aussi un paquet SDES qui contient le CNAME.

Et enfin il peut être inclus un paquet de fin de liaison, le BYE packet (ou encore par abus le " BYE "). Il peut y en avoir plusieurs, mais ils sont toujours placés en fin de compound et indiquent la fin de session pour un participant.

Il existe donc 5 types de paquets RTCP pour transporter des informations de contrôle :

- SR : Sender Report, transmission de statistiques des participants actifs en émission
- RR : Receiver Report, transmission de statistiques des participants passifs
- SDES : Source Description items (CNAME, NAME, EMAIL, PHONE,...)
- BYE : Fin de participation
- APP : fonctions spécifiques à l'application

Les paquets de rapport : Ils permettent de connaître la qualité des liaisons en émission et en réception, et ceci avec une grande précision. Leur placement en tête d'un compound permet de faire la différence entre un flux RTP et un flux RTCP. Le SR diffère du RR par 20 bits d'information venant de l'émetteur placés en tête du paquet. Leur structure étant identique nous allons voir comment est composé un SR grâce à la figure 2.07 :

V	P	RC	Packet type	Length
SSRC de l'EMETTEUR				
SR : INFORMATIONS D'EMISSION (5x32bits)				
RR : INFORMATIONS DE RECEPTION (6x32bits)				

Figure 2.07: *Entête RTCP*

2.3 Problèmes de la VoIP et qualité de service

Il importe donc de sécuriser l'architecture de transport en séparant les trafics voix et data en 2 sous-réseaux (VLAN), de contrôler très rigoureusement l'accès et la liste des postes autorisés. Les équipements contribuant au projet VoIP doivent également être sécurisés : les serveurs doivent être isolés, les pare-feux existants adaptés ou de nouveaux pare-feux dédiés au projet, les mises à jour et correctifs effectués sur les postes IP et serveurs doivent être contrôlés et tracés; sur les réseaux wifi, les communications doivent être cryptées. [9]

2.3.1 Les paramètres de la VoIP

Le protocole IP, comme la majorité des autres technologies de transport de données en mode paquet, a été construit et optimisé pour transporter des fichiers des données, et non pas

la voix ou la vidéo. Il devient donc particulièrement important de savoir contrôler et caractériser la qualité de service d'un réseau IP. [8]

Plusieurs paramètres influent sur la qualité de la voix, comme représentés sur la figure 2.08:

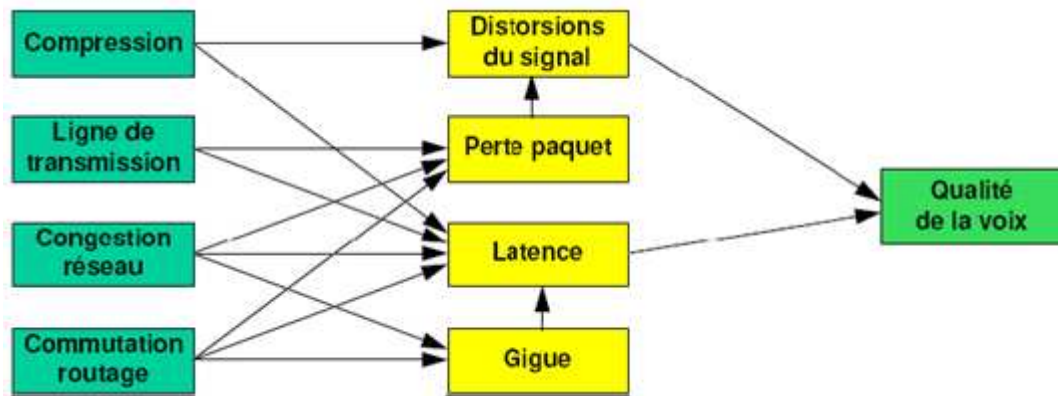


Figure 2.08: Les contraintes de la VoIP

Le traitement de la voix (qualité de codage ou de compression) : influence du codec, du nombre de trames et la redondance.

La clarté : c'est la mesure de fidélité de la voix reçue par rapport à la voix émise, évaluée selon le MOS.

La latence (délai de transmission ou délai de transit) : c'est le temps écoulé entre l'émission de la parole et sa restitution à l'arrivée. Pour permettre un échange interactif, la voix doit être transmise avec des contraintes de délai.

La gigue de phase : c'est la variation du délai de transmission, la gigue doit rester inférieure à 100 ms pour garder une qualité acceptable.

Le phénomène d'écho : l'écho est le délai entre l'émission du signal et la réception de ce même signal réverbéré. Ce phénomène est causé par les composantes électroniques des parties analogiques du système qui renvoient une partie du signal traité. Un écho inférieur à 50ms n'est pas perceptible.

La bande passante : généralement connu du grand public sous l'appellation débit maximum, elle constitue le taux de transfert maximum pouvant être maintenu entre deux points terminaux.

La disponibilité du réseau : c'est le taux moyen d'erreurs d'une liaison.

Les pertes de paquets : le problème de perte de paquets est très lié au problème de la bande passante, ainsi qu'à l'utilisation appropriée d'algorithmes de contrôle de la congestion en bordure et dans le réseau cœur.

Les erreurs d'étiquetage/d'adressage.

2.3.1.1 La latence

La latence désigne le délai de transmission du signal de bout en bout. Plusieurs facteurs influent sur elle : la bande passante disponible, son occupation (trafic), les algorithmes de sécurisation (qui ont tendance à introduire des détails supplémentaires), etc. Trop de latence introduit des blancs dans la conversation qui font perdre son côté naturel. [5]

La maîtrise du délai de transmission est un élément essentiel pour bénéficier d'un véritable mode conversationnel et minimiser la perception d'écho.

Il faut que le temps de transport des données entre l'émetteur et le récepteur soit faible. Or le retard introduit par Internet (de l'ordre de 50 à plus de 500 ms, selon l'état du réseau) est d'un ordre de grandeur nettement plus élevé que celui d'un réseau classique. Un retard est supportable jusqu'à 300 ms, il devrait être inférieur à 150 ms pour une bonne interactivité. [6]

Ce retard est dû à plusieurs facteurs, notamment:

- au temps de traitement dans la compression du signal vocal, plus il est élevé plus le débit obtenu est plus bas;
- à la durée d'un paquet (20 à 40 ms) : pour limiter l'incidence du surdébit, et celui du nombre de paquets par seconde (qui conditionne la charge des routeurs ou commutateurs IP), on regroupe l'information utile dans des paquets assez gros, d'où il résulte un retard pour constituer ces paquets;

- au stockage dans les files d'attente des commutateurs ou routeurs, d'autant plus sensible que le mode de gestion des réseaux IP ne manifeste pas de souci de réduction du nombre de routeurs traversés ;
- au dispositif de correction ou de "camouflage" des paquets manquants, qui nécessite l'attente de blocs de correction ;
- au dispositif de lissage, qui stocke le débit reçu irrégulièrement dans une mémoire tampon, de façon à le restituer de façon continue au décodeur du signal. Le délai est ajusté au délai maximal susceptible de se produire, sans toutefois l'égaliser (on court le risque d'une insuffisance de temps en temps). [6]

Notons que le temps de transport de l'information n'est pas le seul facteur responsable de la durée totale de traitement de la parole. Le temps de codage et la mise en paquet de la voix contribuent aussi de manière importante à ce délai.

Il est important de rappeler que sur les réseaux IP actuels (sans mécanismes de garantie de qualité de service), chaque paquet IP « fait son chemin » indépendamment des paquets qui le précèdent ou le suivent : c'est ce qu'on appelle grossièrement le « Best effort » pour signifier que le réseau ne contrôle rien. Ce fonctionnement est fondamentalement différent de celui du réseau téléphonique où un circuit est établi pendant toute la durée de la communication.

Les chiffres du tableau 2.06 (tirés de la recommandation UIT-T G.114) sont donnés à titre indicatif pour préciser les classes de qualité et d'interactivité en fonction du retard de transmission dans une conversation téléphonique. Ces chiffres concernent le délai total de traitement, et pas uniquement le temps de transmission de l'information sur le réseau.

Classe n°	Délai par sens	Commentaires
1	0 à 150 ms	Acceptable pour la plupart des conversations
2	150 à 300 ms	Acceptable pour des communications faiblement interactives
3	300 à 700 ms	Devient pratiquement une communication half duplex (mode alterné, communication de type militaire)
4	Au-delà de 700 ms	Inutilisable sans une bonne pratique de la conversation half duplex (mode alterné)

Tableau 2.06: *Classes de qualité en fonction du temps de latence*

Un délai par sens de 150 ms correspond à une conversation avec un bond satellite et un délai par sens de 400 ms correspond à deux bonds satellite consécutifs.

En conclusion, on considère généralement que la limite supérieure « acceptable », pour une communication téléphonique, se situe entre 150 et 200 ms par sens de transmission (en considérant à la fois le traitement de la voix et le délai d'acheminement).

Le tableau 2.07 représente l'influence du délai à la qualité vocale :

Délai par sens	Indice de dégradation de la conversation
200 ms	28%
450 ms	35%
700 ms	46%

Tableau 2.07 : *Qualité vocale en fonction du délai*

Ceci montre bien que le délai est très important pour avoir une bonne qualité de la conversation.

2.3.1.2 La gigue

C'est une variation du délai de transmission de l'information. Elle provient de la variation de la charge du réseau (si la taille des files d'attente dans les routeurs augmente, le temps de latence augmente et inversement), éventuellement des routes différentes utilisées (IP

est un mode sans connexion où un flot de datagrammes peut emprunter des chemins différents lors d'un même appel téléphonique). Cette gigue ne doit pas être trop importante. On peut la diminuer en ajoutant des mémoires tampons dans le chemin, mais cela peut engendrer une augmentation du temps de latence.

Le lissage (ou suppression de la gigue) est donc rendu nécessaire par le fait que le retard introduit par les mémoires tampon du réseau n'est pas constant, mais fluctue au gré de la charge des liaisons de transmission, donc des débits instantanés des usagers. Cette fluctuation du retard tend à réduire de manière importante la qualité acoustique, d'où la nécessité d'un lissage. [8]

2.3.1.3 La Perte et le déséquencelement de paquets

La voix supporte bien les pertes de paquets par rapport à d'autres applications. On considère que le taux de pertes doit être inférieur à 20 %. A noter que la retransmission des paquets erronés ou perdus est inutile car elle induirait un temps de latence trop important. Dans un réseau IP, lorsque le débit offert à une liaison excède durablement le débit maximal de cette liaison, la mémoire tampon correspondante élimine un certain nombre de paquets. En revanche, il existe dans les terminaux un mécanisme d'ajustement de la fenêtre aux pertes de paquets constatées. Ce mécanisme ralentit l'émission de paquets en cas d'encombrement du réseau. Il s'agit là d'un mécanisme d'autolimitation mis en jeu par les terminaux. Pour rendre service à l'ensemble de la collectivité des utilisateurs du réseau IP, le terminal restreint le débit de son émission. Le protocole RTP, destiné à véhiculer des signaux en temps réel, ne comporte pas d'ajustement du débit aux conditions d'encombrement rencontrées dans le réseau. Les paquets RTP n'échappent pas à l'éjection en cas d'encombrement. [8]

L'utilisation de redondance pour pallier les pertes de paquets peut prendre la forme d'un code correcteur classique agencé pour faire face à des disparitions de paquets. Il peut prendre la forme d'un "camouflage", dans lequel la portion de signal manquante est remplacée par un signal reconstitué à partir des portions voisines reçues. Une forme plus performante de camouflage consiste à transmettre chaque portion de signal en double, dans deux paquets différents. L'une de ces portions est codée par un procédé plus grossier, mais de débit très réduit. En cas de disparition de la portion de signal normale, la portion grossièrement codée lui est substituée. Le résultat global de ce dispositif est que la qualité

perçue par l'utilisateur demeure acceptable pour des taux de perte de paquets atteignant 10 à 15%, voire plus en fonction du type de codage. [6]

Enfin, connaître le pourcentage de perte de paquets sur une liaison n'est pas suffisant pour déterminer la qualité de la voix que l'on peut espérer, mais cela donne une bonne approximation. En effet, un autre facteur essentiel intervient ; il s'agit du modèle de répartition de cette perte de paquets, qui peut être soit « régulièrement » répartie, soit répartie de manière corrélée, c'est-à-dire avec de pics de perte lors des phases de congestion, suivies de phases moins dégradées en termes de QoS.

Le tableau 2.07 donne un bref aperçu des valeurs acceptables en VoIP.

	Bon	Moyen	Mauvais
Délai de transit	$D < 150 \text{ ms}$	$150 \text{ ms} < D < 400 \text{ ms}$	$D > 400 \text{ ms}$
Gigue déphasé	$G < 20 \text{ ms}$	$20 \text{ ms} < G < 50 \text{ ms}$	$G > 50 \text{ ms}$
Perte de données	$P < 1\%$	$1\% < P < 3\%$	$P > 3\%$

Tableau 2.07 : Seuils de valeurs pour les paramètres critiques

2.3.1.4 L'écho

Ce problème se pose ou non suivant le contexte d'insertion de l'IP dans le réseau général de téléphonie : si l'une au moins des extrémités de la connexion est constituée par une ligne d'abonné téléphonique utilisée en basse fréquence, comme pour une communication téléphonique normale, alors différents équipements pourront induire des phénomènes d'écho (Les passerelles H.323 qui assurent la transmission du signal entre un réseau 4 fils (Ethernet) et un réseau 2 fils (téléphone analogique) par exemple). Il faudra recourir à des fonctions d'annulation d'écho de bonne performance. Il y a un autre cas où l'écho peut se manifester, c'est celui de la téléphonie mains-libres ou de la conférence mains-libres : le couplage a alors lieu de façon acoustique et le temps de transmission élevé rend cet écho particulièrement sensible. Les terminaux de conférence mains-libres doivent donc être dotés d'un bon dispositif d'annulation. [8]

2.3.2 Mécanismes de QoS

La problématique de qualité de la voix sur IP est particulière car la voix attend de son transporteur autre chose que les données. La transmission de données classique (fichiers, messages, transactions ...) ne supporte aucune perte en ligne sous peine de graves conséquences pour l'interprétation et l'utilisation de ces données par l'équipement récepteur, mais elle supporte en revanche une dérive importante en termes de durée d'acheminement. Peu importe qu'un paquet arrive avec 100 ms de retard. Le comportement attendu pour la voix est exactement inverse : 1% ou 2% de perte de données de voix en ligne ne sont pas trop gênants pour la qualité du service de VoIP, mais en revanche une variation fréquente de 100 ms sur le délai de transit est catastrophique et rend le service inutilisable. [2][6]

2.3.2.1 Mécanisme IntServ

a. Présentation de IntServ

IntServ est un modèle d'architecture qui propose de réserver des ressources avant de commencer à les utiliser, de manière à ce que le flux soit constant et répondant toujours aux critères de qualité lors du transfert de données. Le modèle est basé sur la définition de classes de service et la réservation de ressources dans les différents éléments du réseau. Le modèle d'architecture IntServ est décrit dans la RFC 1633. [11]

L'implémentation d'IntServ nécessite quatre composants : un « packet scheduler », un « admission control », un classificateur (« classifier »), et un protocole de réservation de ressources.

- Packet Scheduler (ordonnanceur de paquet) : le packet scheduler contrôle l'acheminement vers la prochaine destination, qui peut être un autre routeur ou un LAN, des différents paquets.
- Le classificateur : afin de pouvoir effectuer un contrôle du trafic, il faut pouvoir identifier chaque paquet entrant et donc pouvoir l'associer à une certaine classe. Le classificateur se base sur le contenu de l'en-tête du paquet et détermine à quelle classe (catégorie de flux) appartient le paquet.
- L'admission control : l'admission control implémente l'algorithme qui détermine si un routeur ou un hôte, est à même de répondre à une nouvelle demande de QoS, sans entraver les demandes qui ont été déjà accordées. Elle est invoquée dans chaque nœud

afin de prendre la décision d'accepter ou de refuser une demande de service temps réel. D'autres tâches, comme l'authentification de ceux qui effectuent des réservations, l'établissement des rapports concernant celui qui a demandé telle réservation, lui sont également confiés.

- Le protocole de réservation : il est nécessaire afin de créer et de maintenir un état décrivant les spécificités d'un flux dans chaque routeur le long du chemin, ainsi que dans les hôtes finaux. Il existe la possibilité de définir plusieurs protocoles de réservation, mais le plus utilisé est RSVP. [11]

b. Fonctionnalités des protocoles de réservations

Il y a quatre fonctions que doit effectuer un protocole de réservation comme RSVP :

- Trouver une route qui permette la réservation de ressources. Cela notamment avec le champ « type-of-service ».
- Trouver une route qui dispose encore de suffisamment de capacité pour de nouveaux flux.
- S'adapter à une route qui devient défaillante : le mécanisme de rafraîchissement d'une réservation, s'effectue à certains intervalles de temps et cela peut provoquer un retard au niveau d'un service temps réel, ainsi, l'application devrait s'adapter à la route autant que possible.
- Ne pas changer une route tant que celle-ci est encore viable. [11]

2.3.2.2 Mécanisme Diffserv

a. Concept de base de Diffserv

Le modèle Diffserv est établi par le RFC 3260. Il consiste à classer le trafic grâce à un code présent dans le paquet IP (le champ Type Of Service de IPv4...). Des traitements différents sont ensuite appliqués aux diverses classes de trafics identifiés par le contenu de ce code. La différenciation des services peut porter sur la priorité des paquets par rapports à d'autres. La base essentielle de ce modèle est donc de remarquer que les informations transportées par les paquets IP sont diverses et que certains types de données ont besoin d'un mode de transmission plus efficace que d'autres. [11]

b. Fonctionnement

Les trames IPv4 contiennent un champ permettant d'identifier son type de contenu et par la même occasion de trouver quels types de privilèges QoS lui appliquer. Dès lors qu'une valeur précise est attribuée à ce champ, on dit que le paquet est coloré.

Le champ ToS (Type of Service) est actuellement représenté par une partie dite DSCP (Differentiated Service Code Point Field). Selon ce type de code, le routeur adopte un comportement de priorisation selon le type de flux ou de mise en attente.

2.3.2.3 MPLS

Dans un réseau mettant en oeuvre MPLS (MultiProtocol Label Switching), tout paquet entrant se voit attribuer un «label» par un routeur de frontière ou «Label Edge Router» (LER). Le premier routeur d'entrée MPLS intitulé «MPLS Ingress Node» est celui qui gère le trafic qui entre dans un réseau MPLS. Il possède à la fois des interfaces IP traditionnelles et des interfaces connectées au réseau MPLS. Pour un routeur donné, les routeurs situés vers la destination sont dits en aval («downstream») alors que les routeurs situés vers la source sont dits en amont («upstream»). En d'autres termes, la source d'information est considérée comme le plus haut point. Le routeur « Ingress » et lui seul, classe les paquets en amont dans des classes de service («Class of Service », CoS) appelées FECs associées à des préfixes d'adresse IP et le protocole transporté, leur ajoute les « labels ». Chaque FEC représente une QoS donnée. Les paquets sont routés le long d'un tunnel dit «Label Switch Path» (LSP) où chaque routeur supportant MPLS, «Label Switch Router» (LSR) prend les décisions de routage en s'appuyant seulement sur la valeur des «labels». A chaque saut, le LSR remplace l'ancien «label» par un autre nouveau qui indique comment router le paquet au prochain saut. Donc les «labels» sont échangés selon le mécanisme de «Label Swapping» et ne sont donc pas routés. [6]

A la sortie du réseau MPLS, le routeur de sortie MPLS intitulé «MPLS Egress Node» retire le «label» aux paquets sortants. Or lorsque le paquet arrive sur le LER, il n'est pas nécessaire pour lui d'avoir toujours le «label» inclus dans le paquet. En effet, il va devoir le dépiler et utiliser les mécanismes de routage qui vont lui permettre de router le paquet vers sa

prochaine destination hors du réseau MPLS. Comme les opérations de routage sont complexes et coûteuses, il est recommandé d'effectuer l'opération de dépilement sur le dernier LSR du LSP (avant-dernier nœud du LSP avant le LER) pour éviter de surcharger le LER inutilement. Le routeur immédiat précédant le routeur LER de sortie jouant ce rôle d'optimisation est dit « Penultimate Node » et cette option de MPLS est dite « Penultimate Hop Mapping».

CHAPITRE 3

LA TELEPHONIE SUR IP (TOIP)

3.1 Définition

Depuis les années quatre-vingt, les éditeurs de logiciels cherchent à utiliser le réseau informatique pour y véhiculer de la voix. Suite à l'apparition de protocoles comme H.323 ou SIP, les constructeurs d'autocommutateurs ont progressivement intégré cette dimension IP à leurs solutions dans une optique de convergence voix-données. Dans un premier temps, cette convergence a pris la forme de cartes optionnelles à intégrer dans les PABX (« *Private Automatic Branch eXchange* ») existants, pour être proposée aujourd'hui de façon native. C'est ce qu'on appelle la Téléphonie sur IP (« *Telephony over IP* » ou ToIP). [7]

La ToIP consiste donc en un ensemble de techniques qui, dans une entreprise ou un organisme, permettent la mise en place des services téléphoniques sur un réseau IP en utilisant la technique de la Voix sur IP (« *Voice over IP* » ou VoIP) pour la transmission de messages vocaux sur des réseaux de données à paquets utilisant le protocole IP. ToIP est de ce fait la première alternative réelle aux réseaux traditionnels de téléphonie qui utilisent une technologie dite de commutation de circuits (*voice switching*) vieille de plus de 100 ans.

La figure 3.01 illustre la convergence des réseaux :

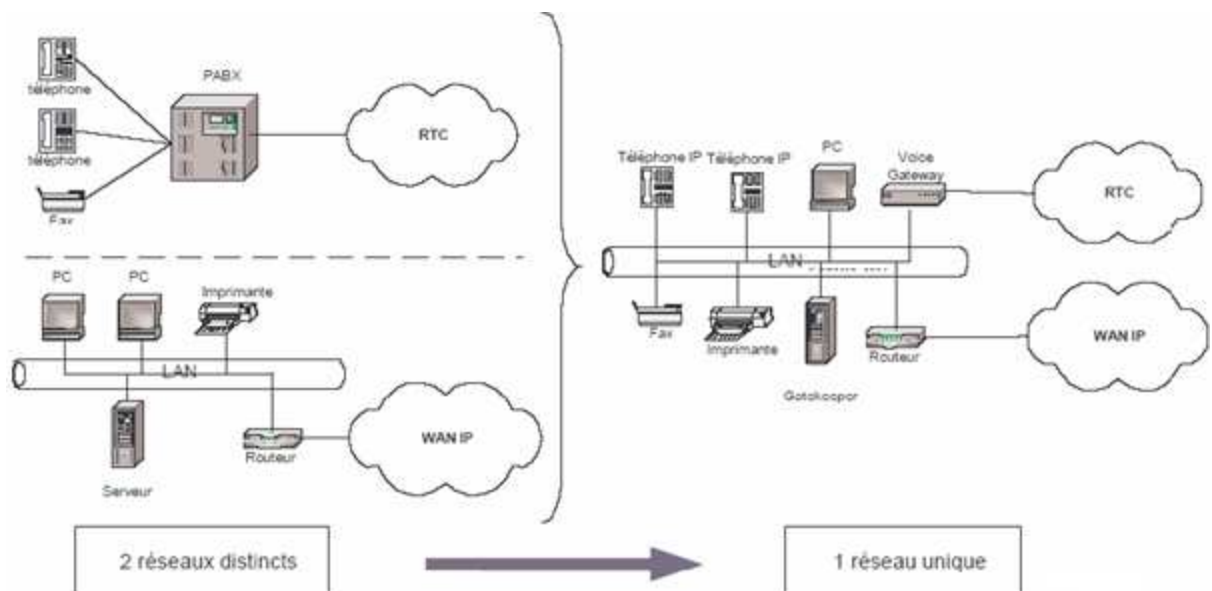


Figure 3.01: Schéma de convergence des réseaux

La téléphonie sur IP est confiée à un réseau géré par une entité unique, une entreprise pour ses besoins internes ou un opérateur télécom. La différence de la ToIP avec la téléphonie traditionnelle, en terme de qualité de service est énorme or, la voix est très sensible à tout retard dans la diffusion du signal. C'est ainsi que nous avons souffert de la mauvaise qualité des appels téléphoniques transmis par satellite car le temps de retour du signal depuis le satellite produisait un écho nuisible à la qualité de la conversation. [7]

3.1.1 Caractéristique de la ToIP

Depuis son invention par A. Graham Bell, le premier téléphone possédait déjà les fonctionnalités de signalisation par les états décroché/raccroché et la composition du numéro d'abonné distant, ainsi que par les facilités d'envoyer les signaux vocaux de la conversation sur le lien bifilaire. La téléphonie est donc composée de deux plans, un plan usager par lequel circulent les échantillons de voix en provenance de l'écouteur du poste téléphonique et le plan contrôle où s'effectuent l'échange de la signalisation pour l'établissement et la terminaison de l'appel. [4]

Avec la numérisation des centraux téléphoniques et l'introduction du réseau numérique à intégration de services, il y a eu séparation du plan de l'utilisateur du plan de contrôle. Les messages de signalisation sont donc commutés dans un commutateur de paquet et les informations de voix sont échangées dans un réseau à commutation de circuit. Avec l'évolution des technologies, on est passé vers une transmission sans fil dans les réseaux mobiles et donc vers un monde plus vulnérable aux attaques et aux fraudes sur les liaisons radios. La notion de signalisation de l'appel et d'échanges des informations de voix existent toujours même en passant à la voix sur IP. [4]

Par ailleurs, toutes les contraintes de la VoIP sont inhérentes à la ToIP et les contraintes et défauts inhérents à IP sont les fondements des difficultés rencontrées par le concept VoIP. Or, le transport de la ToIP ne doit souffrir d'aucun retard de transmission, ni d'altérations, ni de perte de paquets. Due à ces contraintes temporelles, la taille des paquets de voix se limitera entre 10 et 50 octets de données utiles.

De plus, les applications temps réel, c'est à dire la vidéoconférence, Voix sur IP, vidéo temps réel imposent des contraintes temporelles, présentent certaines vulnérabilités au niveau de la transmission des paquets et posent des problèmes de synchronisation temporelle. [4]

La sécurité est donc aussi bien nécessaire aux informations de voix qu'aux informations de signalisation nécessaires à l'établissement de l'appel et aux services, qui transportent des informations critiques comme l'identifiant du numéro appelé et appelant, etc. Or, introduire une nouvelle couche de sécurité, garantissant la confidentialité, l'intégrité et l'authentification, ralentit la transmission des paquets et augmente le délai... [6]

3.1.2 Les équipements de la ToIP

Les principaux équipements d'une communication IP sont : les terminaux téléphoniques IP, le « *gatekeeper* » et la « *voice gateway* ».

3.1.2.1 Les terminaux téléphoniques

a. Le hardphone:

L'« *IP-phone* » ou « *hardphone* » est un terminal téléphonique totalement indépendant de l'équipement informatique, destiné à remplacer l'équipement de téléphonie classique existant et, fonctionnant sur le réseau LAN IP à 10/100 avec une norme soit propriétaire, soit SIP, soit H.323. Il peut y avoir plusieurs codecs (G.711 obligatoire) pour l'audio, et il peut disposer d'un écran monochrome ou couleur, et d'une ou plusieurs touches soit programmables, soit préprogrammées. Il est en général doté d'un hub passif à un seul port pour pouvoir alimenter le PC de l'utilisateur. [7]

b. Le softphone:

Le « *softphone* » est un logiciel qui assure toutes les fonctions téléphoniques et qui utilise la carte son et le micro du PC de l'utilisateur, et aussi la carte Ethernet du PC. Il est géré soit par le Call Manager, soit par le PABX-IP.

c. L'alimentation du hardphone:

Un poste IP (ou « *IP-phone* ») a besoin d'une alimentation :

- soit *locale* : le poste dispose alors d'une alimentation externe DC de 48Volts, ce qui nécessite l'utilisation d'un petit transformateur 220V~/48VDC pouvant être facilement oublié et débranché avec une fausse manipulation ;
- soit *distante* : le poste est alors télé-alimenté :

- o soit par le commutateur Ethernet selon la norme 802.3af d'IEEE Computer Society ;
- o soit par un équipement intermédiaire appelé MID-SPAN, situé entre le switch et le panneau de câblage.

Il est à noter qu'en cas de panne secteur, il n'y a plus de téléphone et aucun appel d'urgences n'est donc possible.

3.1.2.2 Le « gatekeeper »

Le « *gatekeeper* », ou garde-barrière, effectue les translations d'adresses (identifiant H.323 ou SIP et adresse IP du référencement du terminal) et gère la bande passante et les droits d'accès. C'est le point de passage obligé pour tous les équipements de sa zone d'action. Physiquement, un « *gatekeeper* » est un serveur informatique localisé sur le même réseau que les terminaux téléphoniques IP. [7]

3.1.2.3 Le « voice gateway »

Le « *voice gateway* », ou passerelle, est un élément de routage équipé de cartes d'interfaces analogiques et/ou numériques pour s'interconnecter avec soit d'autres PABX, soit des opérateurs de télécommunications locaux, nationaux ou internationaux. Plusieurs passerelles peuvent faire partie d'un seul et même réseau, ou l'on peut également avoir une passerelle par réseau local (LAN). La passerelle peut également assurer l'interface de postes analogiques classiques qui pourront utiliser toutes les ressources du réseau téléphonique IP (appels internes et externes, entrants et sortants). [7]

3.1.2.4 Les équipements complémentaires

D'autres équipements peuvent entrer aussi dans la composition des réseaux de ToIP :

- le *PABX-IP*, c'est lui qui assure la commutation des appels et leurs autorisations, il peut servir aussi de routeur ou de switch dans certains modèles, ainsi que de serveur DHCP. Il peut posséder des interfaces de type analogiques (fax), numériques (postes), numériques (RNIS, QSIG) ou opérateurs (RTC-PSTN ou EURO-RNIS). Il peut se gérer par IP en intranet ou par un logiciel serveur spécialisé que ce soit en interne ou depuis l'extérieur. Il peut s'interconnecter avec d'autres PABX-IP ou PABX non IP de

la même marque (réseau homogène) ou d'autres PABX d'autres marques (réseau hétérogène) ;

- le *serveur de communications*, il gère les autorisations d'appels entre les terminaux IP ou « *softphones* » et les différentes signalisations du réseau. Il peut posséder des interfaces réseaux opérateurs (RTC-PSTN ou RNIS), sinon les appels externes passeront par la passerelle dédiée à cela (*gateway*) ;
- le *MCU* (« *Multipoint Control Unit* ») est un élément optionnel et gère les conférences audio vidéo. [7]

Enfin, outre ces fonctionnalités basiques, les systèmes de ToIP savent proposer des fonctions de péritéléphonie à travers les équipements suivants :

- plate-forme de supervision et d'administration ;
- serveurs de messagerie vocale ;
- standards téléphoniques ;
- serveurs de taxation ;
- serveurs d'enregistrement.

3.1.3 Avantages de la ToIP

La téléphonie n'a jamais été une application simple. Les contraintes temps réel et de synchronisation pèsent lourdement sur sa mise en œuvre, et la téléphonie par paquet ne fait que compliquer le transport.

Cependant, plusieurs raisons expliquent le succès de la téléphonie par paquet, et plus spécifiquement de la téléphonie sur IP :

3.1.3.1 Convergence

Quel que soit le type de données véhiculées, le réseau est unique : les flux de voix, de vidéo, de textes et d'applicatifs transitent sur le même réseau. Les communications deviennent plus riches, et sans avoir besoin de multiplier les canaux de transport. Les utilisateurs peuvent, par exemple, envoyer un compte rendu d'activité en même temps qu'ils téléphonent à leur correspondant. Pour les utilisateurs, la convivialité est accrue. En

entreprise, la productivité est améliorée. Pour les administrateurs, un seul réseau est à administrer, ce qui simplifie grandement la gestion. [6]

3.1.3.2 Optimisation des ressources

Le réseau IP utilisant un transfert de paquets, l'utilisation des ressources est optimisée en comparaison des solutions de type commutation de circuits. Dans le réseau RTC, qui est à commutation de circuits, des ressources sont dédiées pour toute la durée de la communication, qu'elles soient utilisées ou non. Or les très nombreux silences d'une conversation téléphonique rendent le dimensionnement du canal réservé systématiquement trop grand. Pour que la voix supporte simultanément la superposition des deux paroles correspondant aux deux intervenants d'une communication téléphonique (full-duplex), les réseaux RTC doivent allouer pour chaque intervenant des canaux différents, l'un en émission, l'autre en réception. [6]

Dans la pratique, lors d'une conversation téléphonique, une seule personne parle en même temps. Les ressources sont donc globalement gaspillées. C'est pourquoi la réservation effectuée dans les réseaux RTC représente un coût nettement supérieur à celui des réseaux IP.

3.1.3.3 Coût de transport quasiment nul

Grâce à l'intégration de la téléphonie parmi de nombreuses autres applications, le coût du transport devient pratiquement nul. Le réseau permettant d'effectuer le transport est le réseau cœur des opérateurs, celui qui effectue tous les transports de données. Ces opérateurs, qui étaient auparavant obligés de maintenir au moins deux réseaux, celui de téléphonie et celui de données, n'en ont plus qu'un seul à maintenir. L'intégration supplémentaire de la télévision dans le réseau de données fait également chuter les coûts de transport de cette application. [6]

3.1.3.4 Services exclusifs

Certains services sont propres aux réseaux IP. Par exemple, le service de présence, consistant à détecter si un utilisateur est connecté au réseau ou non, ne nécessite aucune réservation de ressources dans un réseau IP, à la différence du réseau RTC. De façon analogue, pour le nomadisme des utilisateurs, il est plus simple de passer, partout dans le monde, par le réseau IP plutôt que par le réseau RTC. [6]

3.1.3.5 Disparition des commutateurs locaux

Liée à la précédente, cette nouvelle donne résulte de la possibilité de gérer les téléphones depuis le réseau de l'opérateur (système Centrex). Des solutions intermédiaires, comme les PBX-IP, permettent de passer petit à petit des circuits numériques aux liaisons paquet IP.

La téléphonie devient ainsi une application du réseau IP comme une autre, si ce n'est qu'elle nécessite une qualité de service particulière. De ce fait, les modems ADSL qui amènent chez l'utilisateur la connectivité IP constituent la porte d'entrée de la téléphonie IP. Le modem l'intègre avec les applications de données (messagerie, transfert de fichiers,...), la télévision, la visiophonie, etc.

Vers Début 2007, cette intégration n'était pas encore finalisée puisque la plupart des postes téléphoniques ne sont pas encore des postes IP capables d'émettre directement des paquets IP. Il faut un point de connexion spécifique sur le modem pour indiquer que le flux est une parole téléphonique. De même, le flux de télévision se distingue des autres applications par un accès spécifique sur le modem. Cependant, dès que les téléphones et les télévisions seront IP, le réseau domestique ne distinguera plus ces applications particulières, et ce sera le modem qui, en filtrant les flux, découvrira les paquets de téléphonie et les paquets de télévision pour les traiter en conséquence. [7]

3.1.4 *Architecture de ToIP*

En offrant la possibilité de faire transiter les communications voix sur des réseaux de données, la ToIP marque la fin d'une cohabitation entre deux réseaux distincts, très différents, du point de vue de la gestion et de la technologie. Ce transfert de l'ensemble des flux sur une infrastructure unique marque les prémices d'une convergence des réseaux multiservices existants (voix, données, vidéo).

Trois grandes familles de ToIP traduisent le taux de convergence des réseaux voix-données :

- la famille « de poste informatique à poste informatique » ;
- la famille « de poste informatique à téléphone » ;
- la famille « de téléphone à téléphone ».

3.1.4.1 De poste informatique à poste informatique

Cela nécessite que les deux interlocuteurs soient équipés informatiquement et dialoguent en utilisant absolument le même logiciel et pour cela évidemment un simple micro et des hauts parleurs. Ce genre de communication est gratuite exception faite du coût du logiciel.

L'intérêt de ce type de communication se trouve dans la Visioconférence, les ordinateurs se connaissent par leurs adresses IP. Or, les adresses IP changeant à chaque connexion, les correspondants doivent se mettre d'accord sur la consultation d'un annuaire pour permettre à l'appelant de connaître l'adresse de l'appelé. [6]

L'architecture de poste informatique à poste informatique est représentée par la figure 3.02 :

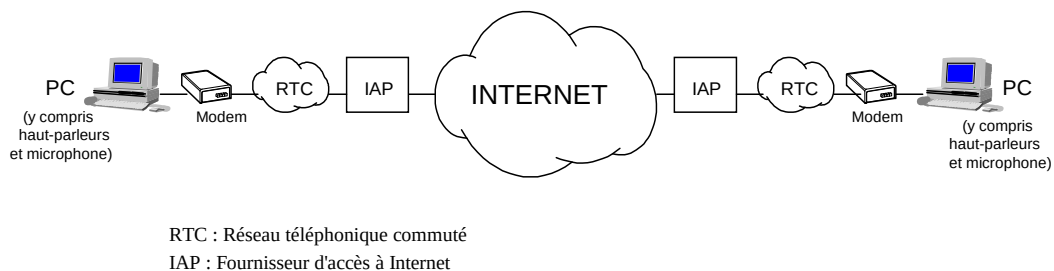


Figure 3.02: *Téléphonie entre postes informatiques*

3.1.4.2 De Poste informatique à téléphone (ou vice-versa)

L'un des correspondants est sur son micro-ordinateur; s'il désire appeler un correspondant sur le poste téléphonique de celui-ci, il doit se connecter sur un service spécial sur Internet, offert par un fournisseur de service (un ISP) ou par son fournisseur d'accès à Internet (son IAP), mais qui doit mettre en œuvre une *gateway* (passerelle) avec le réseau téléphonique. Cela nécessite la mise en œuvre d'une passerelle soit au départ de l'appel soit à l'arrivée pour assurer la traduction entre les éléments spécifiques des deux réseaux (signalisation, codecs, formats de transmission d'information) afin de faire transiter la communication d'un réseau IP à un réseau téléphonique.

Si le correspondant qui appelle est sur son poste téléphonique et qu'il veut joindre un correspondant sur Internet, il devra appeler le numéro spécial d'une passerelle qui gérera l'établissement de la communication avec le réseau Internet et le correspondant sur ce réseau

pourvu, là aussi, qu'il soit disponible (c'est-à-dire connecté). L'appel est taxé uniquement pour la traversée du réseau téléphonique. Ainsi, pour les appels internationaux, plus la proportion du segment IP est grande, plus l'économie réalisée sera importante. L'intérêt de cette famille de communication réside dans le *tout-IP* (ou « *full-IP* ») : la configuration ne se borne pas à l'interconnexion de PBX (« *Private Branch eXchange* »), tous les éléments peuvent se contacter. Le réseau IP doit pouvoir supporter un certain niveau de qualité de service. [6]

L'architecture de poste informatique à téléphone est représentée par la figure 3.03 :

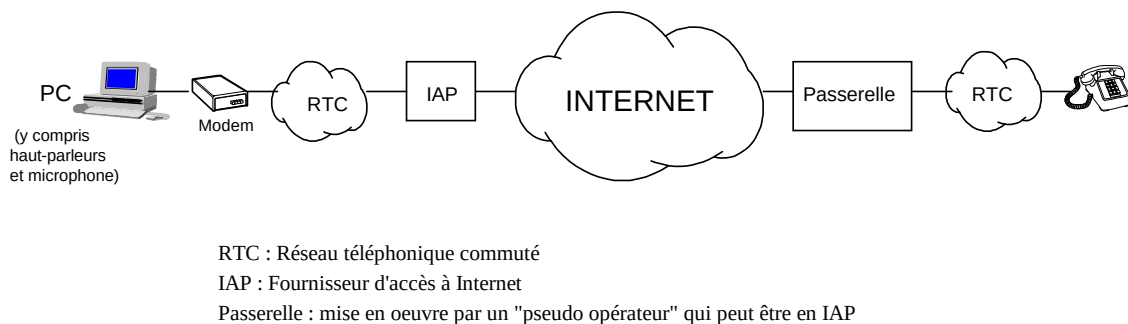


Figure 3.03 : Téléphonie entre poste informatique et téléphone.

Les solutions tout-IP se regroupent en deux types d'architectures :

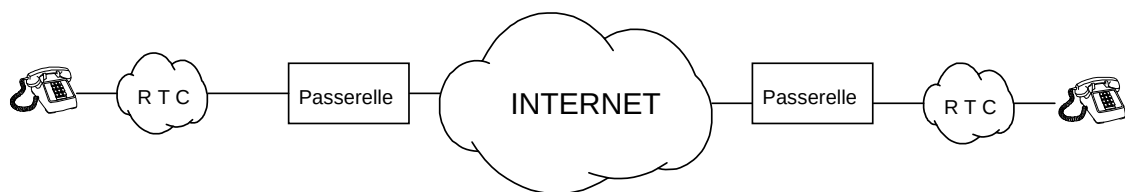
- l'architecture de ToIP *locale*, qui peut s'utiliser pour une nouvelle infrastructure (nouvel immeuble par exemple avec uniquement du câblage catégorie 5 ou 6) ;
- l'architecture de ToIP *distante*, elle, s'utilise en multi-sites tout-IP avec l'aide d'un opérateur adéquat et parfois des serveurs centralisés. L'idée déjà ancienne d'externaliser la fonction remplie par le PBX est placée sous le terme générique de *centrex*. Les centrex IP facilitent la mise en œuvre de fonctions mixant informatique et téléphonie, la première de ces applications mixtes est la messagerie unifiée, les messages vocaux étant traduits en fichiers sonores et envoyés sur des adresses e-mails. [6]

3.1.4.3 De téléphone à téléphone

Lorsque l'appelant et l'appelé sont tous les deux sur téléphone, le réseau de transport devient transparent, cela nécessite la mise en œuvre de plusieurs passerelles qui s'occupent alors de la gestion de la communication, y compris la signalisation avec le réseau

téléphonique et les conversions à l'entrée et à la sortie du réseau IP. Cette architecture est dite *hybride* (circuit / Voix sur IP). Elle est intéressante pour l'interconnexion de PABX : remplacement d'une ligne louée de type RNIS par une architecture réseau assurant une qualité de service, tout en préservant l'architecture téléphonique globale. La tarification dépend de l'opérateur ; s'il s'agit d'un réseau privé, c'est gratuit. Les téléphones classiques (non « IP-phone ») ne peuvent contacter les ordinateurs. [6]

L'architecture de téléphone à téléphone est représentée par la figure 3.04 :



RTC : Réseau téléphonique commuté

Passerelle : mise en oeuvre par un "pseudo opérateur" (par exemple un fournisseur d'accès à Internet) dans ses locaux

Figure 3.04 : *Téléphonie entre postes de téléphones.*

3.1.5 Sécurisation

Selon le Giga Information Group, les sociétés qui font le choix de la téléphonie IP augmentent leurs risques d'être piratées. En effet, alors que la téléphonie traditionnelle constituait un environnement isolé, la téléphonie sur IP, avec une infrastructure commune aux données, engendre bien des interrogations concernant la sécurité. Le serveur de communication et les terminaux IP échangent trois types de flux : le premier permet le téléchargement d'une image, qui apporte le firmware. Le deuxième fournit les informations de configuration, qui personnalisent le poste d'un utilisateur. Le troisième concerne la communication téléphonique. Les trois peuvent comporter des brèches s'ils ne sont pas convenablement sécurisés. [7]

Tous les fournisseurs de solutions de téléphonie sur IP s'accordent à dire qu'il faut absolument isoler les flux de téléphonie des flux concernant les données. Cela implique un environnement Ethernet commuté et non partagé, et la mise en place de réseaux locaux virtuels (ou VLAN) dont un sera dédié à la voix, avec des règles très rigoureuses pour passer d'un VLAN à l'autre. Séparer les flux vocaux des flux de données est de toute façon conseillé pour assurer une meilleure qualité de service.

Pour les utilisateurs distants, la mise en place d'un réseau privé virtuel (ou VPN), généralement basé sur le protocole IPSec, s'impose.

Placés sur un PC, les téléphones IP logiciels (« softphones », comme le logiciel Carrousel par exemple) peuvent être particulièrement vulnérables. D'une part, le poste est exposé à des risques liés à des failles de son système d'exploitation, à des problèmes applicatifs ou à des virus. D'autre part, il est exposé à toute attaque en provenance du réseau de données. C'est pourquoi, il est recommandé de protéger ses réseaux, car les attaques qui affaiblissent les réseaux, pourraient également mettre les téléphones sur IP hors service. [7]

Cependant, des mesures de sécurité inappropriées font risquer à l'entreprise des appels longues distances non contrôlés, des conversations mises sur écoute et enregistrées à l'insu des interlocuteurs, des attaques incapacitantes (« denial of service attacks ») qui utilisent les ports téléphonie comme points d'entrée.

La menace la plus importante est le *déni de service*. En effet, une attaque de déni de service (ou DoS, pour « *Denial of Service* ») prolongée saturera ou fera tomber le PABX-IP. C'est à la fois l'attaque qui a le plus de répercussions et celle qui est la plus facile à réaliser. À cela s'ajoutent les craintes d'utilisation frauduleuse du système, les craintes d'écoute ou d'espionnage. Le type de fraude qui, instinctivement, fait l'objet du plus grand nombre d'investigations de la part des fraudeurs est celui qui comporte un aspect lucratif, comme téléphoner aux frais de l'entreprise. [6]

Les intrusions pourront aussi viser à écouter les communications, enregistrer les numéros appelés, subtiliser des informations (par exemple, un vol d'annuaire), ou encore modifier des informations. Enfin, la passerelle, qui permet de connecter le réseau IP au réseau public RTC, peut être perçue comme une porte d'entrée potentielle et des applications comme les serveurs d'appels ou la téléphonie IP offrent aussi un point d'entrée sur le réseau, semblables à des « *back doors* » et, la trace de pirates entrant par cette porte dérobée pourrait se révéler difficile à suivre. [6]

Autre aspect à examiner, les fonctions d'administration au niveau du gestionnaire d'appels. S'il comporte un serveur Web pour la gestion à distance, il faut y accéder par l'intermédiaire d'un protocole sécurisé tel que HTTPS.

3.1.6 Différence entre VoIP et ToIP

Dans les deux cas, nous parlons d'équipements et de mécanismes permettant de transporter de la voix sur un réseau de données de type IP (*Internet Protocol*).

Dans le cas de la VoIP, on se contente d'interconnecter des PABXs encapsulant la voix numérisée, dans les paquets IP. Ces derniers sont ensuite véhiculés au sein du réseau de données, de manière classique, comme des paquets de données. La voix est simplement « reconstituée » lorsque les paquets arrivent chez le destinataire. Un exemple « parlant » de VoIP se trouve dans le raccordement de 2 sites via une ligne spécialisée qui transporte la voix et les données. La figure 3.05 représente l'infrastructure VoIP :

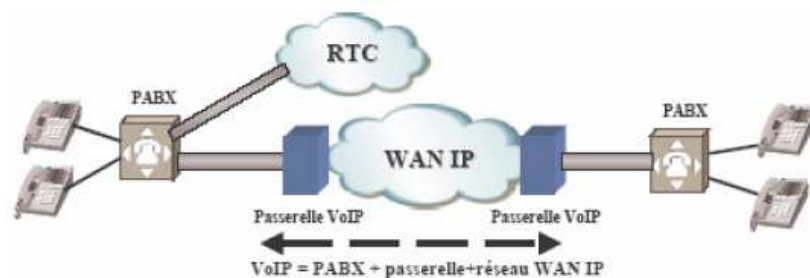


Figure 3.05 : Infrastructure VoIP.

Quant à la ToIP, elle va plus loin que la VoIP en terme de mécanismes et d'équipement, cherchant à apporter aux utilisateurs la qualité de service (qualité de transmission, qualité de voix, disponibilité du service) et les services que ces derniers ont l'habitude de trouver du côté de la téléphonie classique (présentation du numéro, transfert d'appel, conférence, etc.) le tout sans faire appel aux PABXs. La figure 3.06 représente l'infrastructure ToIP :

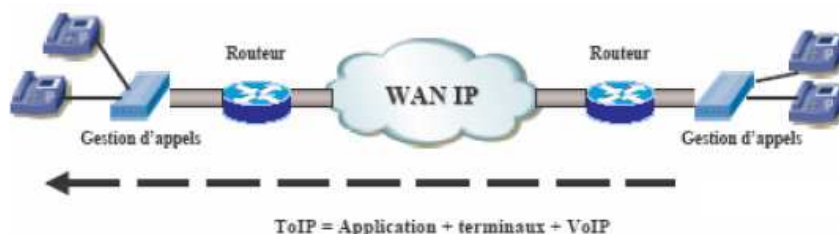


Figure 3.06: Infrastructure ToIP

La VoIP est donc une composante de la ToIP. L'encapsulation de la voix peut être implémentée en deux points différents de l'infrastructure du réseau voix de l'entreprise : [5]

- Limitée au réseau d'interconnexion privé des sites (technologie de transport) et contournant le réseau téléphonique commuté de l'opérateur voix : **la voix sur IP**
- Etendue de bout en bout du réseau de desserte jusqu'aux postes de travail et intégrant des services voix/données aux utilisateurs et aux exploitants : **la téléphonie sur IP**

3.1.7 ToIP et NGN

3.1.7.1 Objectif

La commutation téléphonique évolue. Une nouvelle génération d'architectures de réseaux apparaît, permettant d'offrir de nouveaux services émergents mixant voix et données : les NGN pour les opérateurs, et les réseaux de téléphonie sur IP pour les entreprises. [9]

3.1.7.2 NGN et la téléphonie IP

Les NGN est un réseau de transport en mode paquet permettant la convergence des réseaux Voix/données et fixe/mobile; ces réseaux permettront de fournir des services multimédia accessibles depuis différents réseaux d'accès.

Le protocole Internet (IP) est la base de ce modèle de réseau. Dans les NGN, l'IP peut être l'intégrateur universel des services voix, données et vidéo, aussi bien pour le fixe que pour le mobile. Le transport de tous ces services s'effectue sur un réseau IP commun. Il ne s'agit pas de l'Internet public actuel bien qu'il s'y connectera. On peut envisager aujourd'hui que l'Internet devienne une application ou un des services dont la fourniture est assurée par les NGN en faisant appel à la technologie IP.

Les NGN sont basés sur une évolution progressive vers le « tout-IP » et sont modélisés en couches indépendantes dialoguant via des interfaces ouvertes et normalisées :

- la couche « Accès », qui permet l'accès de l'utilisateur aux services via des supports de transmission et de collecte divers : câble, cuivre, fibre optique, boucle local radio, xDSL, réseaux mobiles.

- La couche « Transport », qui gère l'acheminement du trafic vers sa destination. En bordure du réseau de transport, des « média gateways » et des « signalling gateways » gèrent respectivement la conversion des flux de données et de signalisation aux interfaces avec les autres ensembles réseaux ou les réseaux tiers interconnectés.
- La couche « contrôle », qui se compose de serveurs dits « softswitch » gérant d'une part les mécanismes de contrôle d'appel (pilotage de la couche transport, gestion des adresses), et d'autre part l'accès aux services (profils d'abonnés, accès aux plates-formes de services à valeur ajoutée).
- La couche « services », qui regroupe les plates-formes d'exécution de services et de diffusion de contenus. Elle communique avec la couche contrôle du cœur de réseau via des interfaces ouvertes et normalisées, indépendantes de la nature du réseau d'accès utilisé. Les services et contenus eux-mêmes sont par ailleurs développés avec des langages convergents et unifiés.

Toutefois, la technologie IP offre de multiples autres opportunités de fonctionnalités téléphoniques de nouvelle génération. De plus, l'activation et l'annulation de ces services sont simplifiées par la mise en place d'interfaces Web.

Parmi les services de nouvelle génération disponibles, on retiendra notamment : l'accès universel à son carnet d'adresses personnel unique, l'accès universel au répertoire d'entreprise, l'intégration avec les répertoires mondiaux (par exemple DNS, LDAP, H.350), l'obtention des cours de la bourse, une application Web qui renvoie des informations au format XML, une application intelligence artificielle (une Interactive Voice Response (IVR) ou une Customer Response Application (CRA), comme par exemple une « secrétaire virtuelle »), le répondeur vidéo, la messagerie vidéo, l'enregistrement de la conversation audio/vidéo, la vidéo d'attente, la redirection vers la messagerie électronique, la redirection vers un site Web, la redirection vers n'importe quel poste (IP ou pas), la mobilité de poste locale (logiciel sur PC, téléphone IP fixe ou mobile) au sein de l'entreprise, la mobilité de poste globale (logiciel sur PC, téléphone IP fixe ou mobile) à travers le monde, l'appel vers une conférence (afin d'y participer), le routage intelligent d'un appel (ex : prise en compte de données acquises durant la communication, l'état d'une file d'attente, l'heure actuelle, etc.), la liberté du lieu de prestations de service de helpdesk (par exemple un centre d'appels peut être géographiquement délocalisé tant que l'accès au réseau IP est présent), la maintenance

centralisée d'infrastructures décentralisées, la sélection de la passerelle la plus adéquate, etc.
[9]

3.2 Conclusion

La VoIP ouvre des horizons très riches en facilitant l'ajout d'applications à valeur ajoutée. En voici quelques exemples : la visiophonie, la convergence fixe – sans fil – mobile et le travail coopératif. Les terminaux téléphoniques IP n'en sont qu'à leurs débuts. Ils doivent encore évoluer pour : offrir de nouvelles interfaces utilisateur, des capacités de traitement multimédia, et des fonctionnalités de confort ; converger vers des protocoles standardisés permettant l'interopérabilité en environnement multi-constructeurs.

A l'origine, la voix sur IP était une technologie exclusivement réservée aux opérateurs de télécommunications. Cette technique de transport leur a permis de remplacer des liaisons TRUNK entre les équipements de leurs réseaux PSTN, permanentes et onéreuses, par des connexions dynamiques et moins coûteuses grâce au protocole IP.

Aujourd'hui, grâce à l'avènement de l'accès Internet large bande, l'intérêt pour ces technologies gagne également le public. Le consommateur professionnel ou privé tend à utiliser le réseau Internet comme infrastructure alternative d'accès aux services de téléphonie.

Au-delà d'une réduction substantielle de ses coûts de communication, le consommateur peut ainsi avoir accès à une multitude de services complémentaires ; la vidéo, le chat, le partage de contenus (par exemple les photos) ou d'applications, la messagerie instantanée, la messagerie unifiée (boîte vocale, comptes e-mail, fax, SMS, MMS,..., réunis au sein d'une seule « boîte » accessible de partout), la personnalisation de services (ringtones, déviation, musique/vidéo d'attente,...), l'utilisation mobile (comme pour le GSM) grâce aux technologies d'accès réseau sans fil (WiFi et WiMax)...

CHAPITRE 4

PLANIFICATION DES LIENS VOIP

4.1 Introduction

L'amélioration des performances des réseaux est vue comme un défi d'optimisation composé de deux parties : la gestion de capacité et la gestion du trafic. Logiquement ces deux actions opèrent à différentes portées et à différentes échelles de temps. La gestion de la capacité consiste à faire la planification de la capacité, à contrôler le routage et à gérer les ressources telles que : la capacité des liens.

La planification de la capacité implique la planification des ressources nécessaires dans le réseau à savoir la capacité des liens. Par contre, la gestion du trafic consiste à conditionner le trafic et à gérer les files d'attente.

Lors de la mise en place d'un réseau, on doit tenir compte de certaines données physiques et commerciales ainsi que des besoins des utilisateurs à court et à moyen terme. Le processus de planification doit réserver des ressources pour chaque type de service en tenant compte du trafic généré. [18]

4.2 Dimensionnement d'un réseau offrant le service de la voix

Initialement, l'étude d'un réseau se fait en suivant des procédures successives et qui peuvent être révisées par la suite. Il y a toujours certains éléments auxquels on doit faire attention dans la conception d'un réseau :

- la planification du trafic : cette procédure consiste à déterminer le nombre de clients auxquels le service est destiné ainsi que les différents types de services offerts par le réseau.
- le choix de la topologie du réseau : emplacement des nœuds, classification des nœuds (exemple : choix du nombre de nœuds d'entrée et du nombre de nœuds du cœur dans un réseau VoIP).
- le calcul de la capacité des liens. [13]

Partons d'un scénario particulier formé des hypothèses initiales suivantes :

- Le réseau est composé de n sites notés: $S_1, S_2, S_3, S_4 \dots S_n$
- Chaque site est formé d'un certain nombre d'utilisateurs respectivement $N_1, N_2, N_3, N_4, \dots N_n$

4.2.1 *Modèle de trafic*

On considère que la loi du trafic voix obéit à un processus de poisson. La probabilité d'observer alors k arrivées pendant un intervalle de temps t est donnée par: [16]

$$P_k(t) = \frac{(\lambda t)^k}{k!} e^{-\lambda t} \quad (4.01)$$

λ : étant le taux d'arrivée

On parle alors d'*arrivées poissonniennes*.

La propriété la plus importante du processus de Poisson, peut s'interpréter de la façon suivante : une arrivée poissonnienne signifie que la probabilité pour qu'un client arrive pendant dt est à peu près égale λdt .

La deuxième propriété essentielle du processus de Poisson relie le processus d'arrivée poissonnienne aux variables aléatoires mesurant le temps d'inter-arrivée. Cette propriété s'interprète de la façon suivante : des arrivées poissonniennes signifie que les inter-arrivées sont de types exponentielles.

Les lois d'Erlang qui sont utilisées pour le dimensionnement des réseaux offrant le service de la voix, se basent sur l'hypothèse que les services sont exponentiels et les arrivées sont de type poissonniennes. [13]

4.2.2 *Lois d'Erlang*

Le choix des lois d'Erlang dans plusieurs projets est justifié par le fait qu'elles donnent généralement des résultats raisonnables.

Les formules sont utilisées dans les conditions suivantes :

- le nombre de clients est supérieur au nombre de ressources disponibles pour les servir.
- les demandes des clients sont indépendantes les unes des autres

Dans les réseaux téléphoniques classiques, la loi la plus utilisée est celle d'Erlang B. Pour la voix sur IP, les opérateurs conservent toujours cette formule dans leur procédure de dimensionnement du réseau d'accès. La loi d'Erlang B permet de calculer la probabilité qu'une demande de ressource sera rejetée à raison de ressources non disponibles. La probabilité de blocage sera alors égale à : [13]

$$P_n = \frac{\frac{A^n}{n!}}{\sum_{n=0}^n \frac{A^n}{n!}} = E_1(A, n) \quad (4.02)$$

Où

- n : le nombre de ressources disponibles
- A : le trafic offert
- p_n : la probabilité que les n ressources soient occupés
- E_1 : la première formule d'Erlang qui est fonction de A et n

4.2.3 Débit d'accès

Pour chaque site, on peut calculer le débit d'accès en suivant les étapes suivantes :

- Calcul du débit par appel.
- Calcul du nombre de circuits.

4.2.3.1 Débit par appel

Le débit d'accès peut être calculé en tenant compte des éléments suivant :

- les codecs audio utilisés au niveau de la couche application.
- les différentes encapsulations aux niveaux des différentes couches (transport, réseau).
- les protocoles au niveau de la couche liaison.

a. Les codecs audio

Les codecs les plus utilisés pour la compression/décompression de la voix sur IP sont :

- ✓ G.711 offrant un débit de 64 Kbit/s
- ✓ G.723 offrant un débit de 6.3 et 5.3 Kbit/s

- ✓ G.729 offrant un débit de 8 Kbit/s

Selon le débit généré par le codec et en tenant compte des différentes possibilités des cycles de transmission, on peut obtenir la taille des données audio (data Voice). Ces données audio vont subir des encapsulations au niveau des différentes couches commençant par la couche transport jusqu'à arriver à la couche liaison de données. [6]

b. Les encapsulations au niveau transport et réseau

Les données audio de la couche application sont affectées au niveau de la couche transport d'un en-tête RTP ayant une taille minimale de 12 octets, puis d'un en-tête UDP avec 8 octets enfin la mise en paquet au niveau de la couche réseau ajoute 20 octets pour l'en-tête IP. La figure suivante illustre le principe de la mise en paquet. [11]

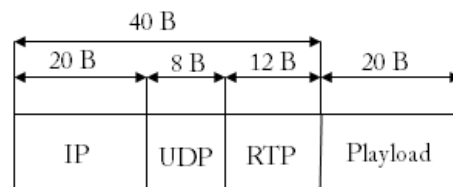


Figure 4.01: Encapsulation RTP/UDP/IP

c. Les protocoles utilisés au niveau de la couche liaison

L'encapsulation doit tenir compte des différents protocoles en niveau de la couche liaison.

- *Ethernet:*

La technologie Ethernet est la technologie la plus répandue dans les réseaux d'entreprises (LAN). La structure de la trame Ethernet est donnée par la figure 4.02 :

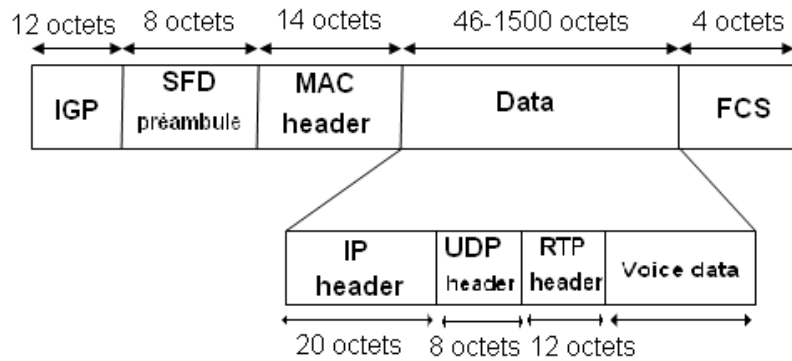


Figure 4.02 : *format de trame Ethernet*

- *HDLC (High Data Link Control):*

Ce protocole permet une liaison point à point ou point multipoint et une transmission synchrone. Il se base également sur le principe de fenêtre coulissante. La taille des données dans la trame HDLC est variable. La structure de la trame en HDLC est représentée par la figure 4.03 :

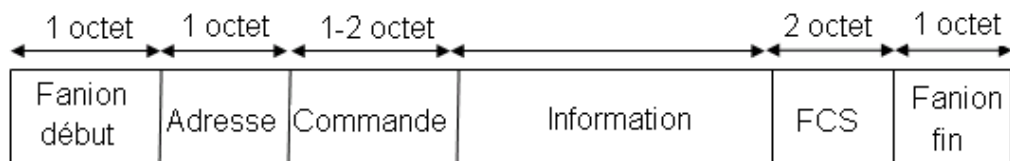


Figure 4.03 : *format de trame HDLC*

- *FR (Frame Relay):*

Ce protocole est utilisé dans les réseaux maillés. Il assure l'établissement de circuit virtuel entre deux usagers. La structure de la trame FR est représentée par la figure 4.04 :

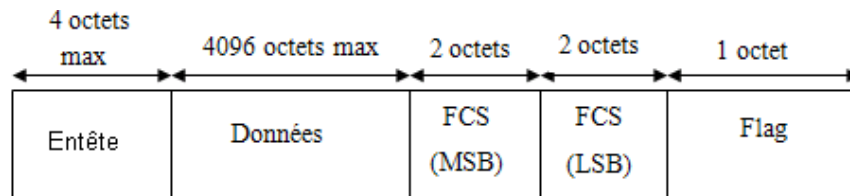


Figure 4.04 : *format de trame Frame Relay*

- *PPP (Point to point Protocol):*

Ce protocole est utilisé pour transporter des paquets entre deux usagers à travers des liens simples. Ces liens fournissent des transmissions simultanées full-duplex. La structure de la trame PPP est représentée par la figure 4.05 :

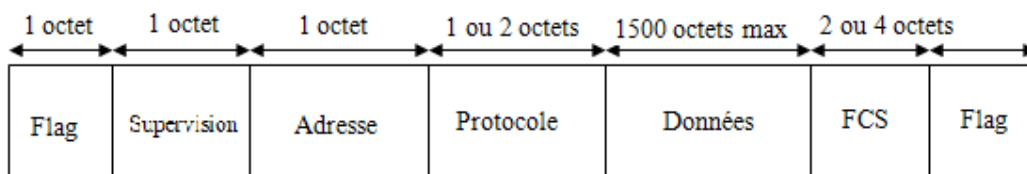


Figure 4.05 : format de trame PPP

- *ATM (Asynchronous Transfert Mode) :*

Ce protocole se base sur la transmission de cellules à l'intérieur d'un circuit virtuel. Son principal intérêt est qu'il permet la réservation de ressources pour un CV (circuit virtuel). Le format de la trame ATM est représenté par la figure 4.06 :

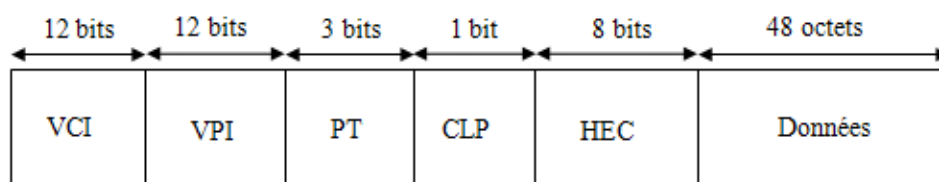


Figure 4.06 : format de trame ATM

La signification des différents champs n'est pas aussi importante que la taille des données qu'ajoute chaque protocole. Le débit généré sur le support physique varie avec la variation des différents paramètres cités ci-dessus.

Pour chaque site, on suppose qu'on a un choix uniforme entre les différents utilisateurs des différents paramètres : codec, cycle de transmission, protocole de couche liaison.

La formule qui permet de calculer le débit par appel est la suivante :

$$\text{débit}_{\text{appel}} = \left[(\text{débit}_{\text{codec}} \cdot \text{cycl}_{\text{trans}}) + \text{entête}_{\text{RTP,UDP,IP}} + \text{entête}_{\text{protocole liaison}} + \text{enquête}_{\text{protocole liaison}} \right] \cdot \frac{8}{\text{cycl}_{\text{trans}}} \quad (4.03)$$

- $Débit_{apl}$: débit par appel en Kbit/s
- $Débit_{codeC}$: débit généré par le codec en Kbit/s
- $cycle_{trans}$: le cycle de transmission de paquet en ms
- $entête_{RTP/UDP/IP}$: la taille l'entête RTP/UDP/IP à ajouter en octets
- $entête_{protocoleliaison}$: la taille de l'entête du protocole de couche liaison en octets
- $enqueue_{protocoleliaison}$: la taille de l'en-queue du protocole de couche liaison en octets

4.2.3.2 calcul du nombre de circuits

L'algorithme de la formule d'Erlang inverse permet de déterminer le nombre de circuits à mettre en œuvre pour supporter un trafic donné avec une probabilité de blocage fixe. [13]

Cet algorithme est représenté par la figure 4.07 :

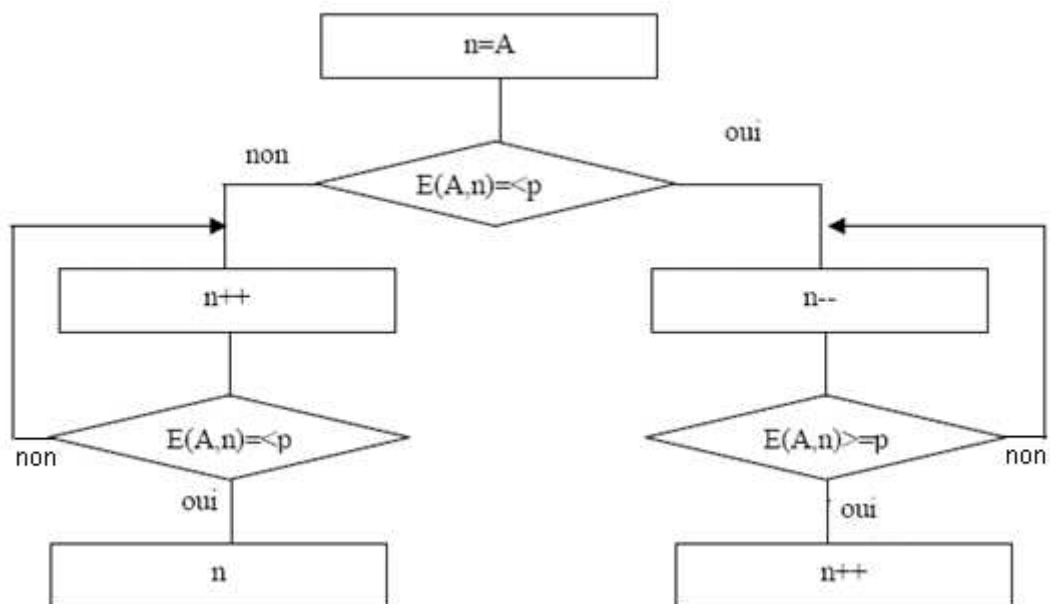


Figure 4.07: l'algorithme d'Erlang inverse

- A : trafic offert
- n : nombre de circuit
- E : formule d'Erlang
- p : probabilité de blocage fixé par l'opérateur

On peut calculer le débit d'accès nécessaire à partir du nombre de circuits et le débit par appel.

$$\mathbf{debit}_{\mathbf{acces}} = \mathbf{débit}_{\mathbf{appel}} \cdot \mathbf{nb}_{\mathbf{circuit}} \quad (4.04)$$

- $\mathbf{debit}_{\mathbf{acces}}$: Bande passante nécessaire
- $\mathbf{débit}_{\mathbf{appel}}$: débit par appel
- $\mathbf{nb}_{\mathbf{circuit}}$: nombre de circuit

4.2.4 Estimation du trafic entre les Edge Router

On peut de cette manière estimer le trafic entre les différents routeurs de la périphérie deux à deux pour construire une matrice de trafic. La distribution du trafic à l'entrée de chaque Edge router se fait selon : [13]

- le nombre d'utilisateurs liés à chaque site.
- le plus court chemin entre deux edge routers.

La matrice de trafic aura alors la forme suivante entre les différents nœuds:

$$T_{\text{trafic}} = \begin{bmatrix} 0 & A_{12} & A_{13} & A_{14} \\ A_{21} & 0 & A_{23} & A_{24} \\ A_{31} & A_{32} & 0 & A_{34} \\ A_{41} & A_{42} & A_{43} & 0 \end{bmatrix}$$

A_{ij} : le trafic généré entre les nœuds d'extrémité i et j

C'est une matrice à diagonale nulle puisqu'on ne tient pas compte de la communication intrasite.

Par exemple :

Le trafic T1 qui entre par le nœud 1 va être distribué selon le pourcentage du nombre d'utilisateurs dans les autres sites. Partons alors des hypothèses suivantes pour le nombre d'utilisateurs au niveau des sites, avec le trafic T1 destinés respectivement aux sites S2, S3 et S4 correspondants :

	S1	S2	S3	S4
N	Nœud source	20	40	10
%T1	Nœud source	28.57% T1	57.14% T1	14.28% T1

Tableau 4.01 : Répartition du trafic entre les sites

4.2.5 Calcul des capacités

4.2.5.1 Capacité du plus court chemin entre deux sites

Dans tous les cas, le trafic suit le plus court chemin pour des raisons de coût et de qualité de service (QoS) puisque le plus court chemin assure généralement un délai faible. [17]

Le chemin le plus court doit supporter la somme des deux trafics étant donné que les artères sont considérées en full-duplex.

Dans le processus de dimensionnement, on doit tenir compte d'un autre facteur à part la qualité de service à savoir la disponibilité du réseau. Pour cela, si le plus court chemin est incapable de véhiculer le trafic entre deux sites donnés, les chemins alternatifs doivent partager ce trafic suivant des coefficients basés sur des métriques de distances croissantes. En d'autre terme, plus le chemin alternatif est court, plus la portion de trafic qu'il supporte sera importante. [17]

4.2.5.2 Algorithme de DIJKSTRA

La métrique utilisée pour calculer le chemin le plus court pour cet algorithme est le coût qui est défini par avance. [13]

Cet algorithme permet le calcul de chemins optimaux d'un sommet à tous les autres :

Soit $G=(X, U)$ le graphe représentant le réseau,

$X= (1,2,..., N)$ l'ensemble des nœuds du graphe,

$U= (1,2,..., M)$ l'ensemble des arcs du graphe,

$V : U \rightarrow R^+$ étendu par pour tout $(i,j) \in X^2-U, v(i,j) = +\infty$

$d(i)$ définit la valeur minimale d'un chemin de 1 à i

v : valuation des arcs du graphe (des liaisons du réseau)

S : sommet du graphe fixé comme source

Tant que $S \neq X$ faire

 début

 choisir $y \in X-S$ avec $d(y)$ minimum

$S := S \cup \{y\}$

 Pour tout $i \in X-S$ faire

$d(i) := \text{MIN}(d(i), d(y) + v(y, i))$;

 fin

L'organigramme suivant résume cet algorithme de DIJKSTRA :

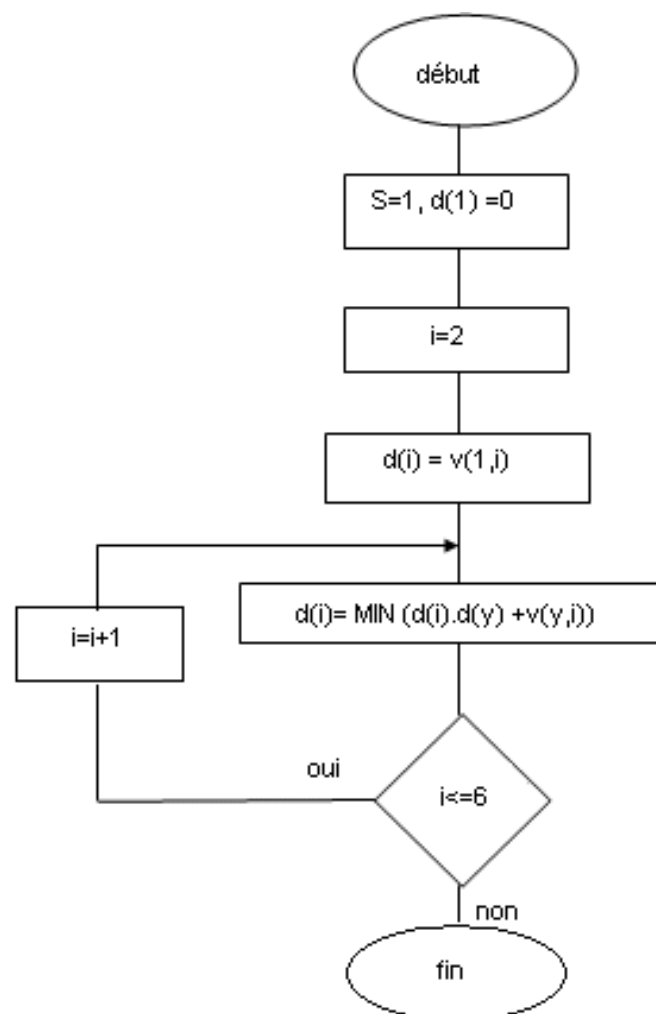


Figure 4.08: *Algorithme de DIJKSTRA*

4.2.5.3 Capacité des liens individuels

Dans ce cas, on doit tenir compte des différents trafics acheminés entre les différents sites. On suppose pour cela qu'il existe des trafics entre les différents sites. Au pire des cas, chaque lien doit être dimensionné de telle façon qu'il supporte la totalité du trafic qui le traverse. [13]

$$C_{kv} = \sum_{i=1}^{n-1} \sum_{j=i+1}^n \alpha_{ijv} T_{ijv} \quad (4.05)$$

C_{kv} : la capacité du lien individuel pour le trafic voix

T_{ijv} : le trafic entre les sites i et j

$$T_{ijv} = T_{ij} + T_{ji} \quad (4.06)$$

α_{ijv} : un coefficient de pondération attribué au chemin supportant le trafic voix entre le site i et le site j.

Etant donné qu'il existe plusieurs chemins entre deux nœuds i et j et étant donné que le plus court chemin doit supporter la totalité du trafic, les autres chemins doivent partager le trafic entre eux selon des coefficients de pondération.

4.3 Dimensionnement pour un réseau offrant le service data

Jusqu'à aujourd'hui, le service data est le service dominant sur le réseau IP bien qu'on cherche à intégrer d'autres services temps réel. Mais, ce service est moins prioritaire puisqu'il n'a pas de contraintes de temps de transmission. Un consensus général existe sur le fait que le trafic data sur IP n'est pas poissonien. Cependant les recherches ne sont pas d'accord sur l'approche qu'on peut adopter pour modéliser le trafic sur Internet. Le modèle BMAP (Batch Markovian Arrival Process) a été exploité pour modéliser le trafic IP. Ce modèle est bien adapté au trafic data où le besoin en débit des utilisateurs est aléatoire. En effet, les flux arrivent parfois en lots, parfois l'activité des utilisateurs est pratiquement nulle. [16]

4.3.1 Exemple de type de contrat

En se basant sur les contrats SLA (Service Level Agreement) entre les opérateurs et les abonnés et en partant d'un cas particulier de deux types de contrats qu'on appelle respectivement SLA1 et SLA2 :

- SLA1 : garantissant un débit montant de 64 Kbit/s et un débit descendant de 128 Kbit/s
- SLA2 : garantissant un débit montant de 128 Kbit/s et un débit descendant de 256 Kbit/s

Chaque site du réseau possède un nombre d'abonnés bien particulier. Pour chaque site, il y a un certain pourcentage d'utilisateurs qui demandent un service de type SLA1 alors que les autres demandent un service de type SLA 2. [10]

Chaque trafic va transiter à travers les nœuds du réseau pour atteindre leur site destinataire.

4.3.2 Principe de distribution de charge

On adopte la même topologie que dans le cas de la voix. Par la suite, on va procéder comme suit :

- On calcule le débit du lien montant au niveau de chaque site selon les différents types de contrats établis entre l'opérateur et les clients suivant un accès ADSL.

$$D_{up i} = N_{1i} * 64 + N_{2i} * 128 \quad (4.07)$$

N_{1i} : représente le nombre d'abonnés du site i ayant un contrat SLA1

N_{2i} : représente le nombre d'abonnés du site j ayant un contrat SLA2

- On calcule le débit des liens descendants selon les conditions imposées par les contrats.

$$D_{down i} = N_{1i} * 128 + N_{2i} * 256 \quad (4.08)$$

4.3.3 Capacité du plus court chemin pour le trafic data

Le trafic dans les deux sens (montant et descendant) va suivre le plus court chemin. Ce dernier va être dimensionné de telle façon qu'il supporte la totalité du trafic afin d'assurer certaines exigences en terme de qualité de service telles que: un délai faible et un coût minimal.

Il est essentiel de prévoir d'autres chemins alternatifs qui vont partager respectivement les trafics upload et download. Cette distribution de charge se fait selon des coefficients de pondération et elle est utile surtout en cas de surcharge au niveau du plus court chemin ou lorsque ce chemin n'est pas fonctionnel. [13]

4.3.4 Capacité des liens individuels pour le trafic data

Dans ce cas, on a suivi le même principe que pour le trafic voix. De façon générale, on suppose que l'accès Internet est possible à partir d'un nœud i:

$$C_{kd} = \sum_{i=1}^{-1} \alpha_{ijd} T_{ijd} \quad (4.09)$$

$$T_{ijv} = T_{ij} + T_{ji} \quad (4.10)$$

C_{kd} : capacité du lien individuel k

α_{ij} : Coefficient de pondération attribué au chemin supportant le trafic data entre le nœud i et j

4.3.5 Capacité des liens supportant le trafic voix et data

Pour les liens qui vont supporter le trafic data et le trafic voix, la capacité du lien doit être capable de supporter les deux trafics en même temps. La capacité totale doit être égale à la somme des deux capacités. Cette capacité a été répartie suivant des coefficients entre le trafic temps réel (voix) et le trafic élastique (données). Pour le trafic data, on n'a pas besoin de calculer le débit de la signalisation pour connaître la capacité des liens. En fait, le débit définit dans le contrat et que l'opérateur doit garantir tient déjà compte de la signalisation. On peut

tenir compte de l'évolution du réseau. Pour cela, on peut ajouter un certain pourcentage à la capacité du réseau. [13]

4.4 Conclusion

L'un des moyens pour dimensionner un réseau est de déterminer les capacités des différents liens au niveau de ce réseau. La détermination de ces capacités doit tenir compte de certains éléments tel que : le trafic généré par appels, le nombre d'appels et surtout la manière avec laquelle sont réparties les différents trafics entre les différents sites. Le passage d'un service voix à un service data, permet de modifier le comportement du réseau et la distribution de charge.

CHAPITRE 5

SIMULATION AVEC LE LANGAGE JAVA

5.1 Introduction

Dans le chapitre précédent, nous avons présenté la méthode utilisée pour le dimensionnement dans les réseaux multiservices. Nous nous sommes intéressés particulièrement au dimensionnement des capacités des liens.

Dans ce chapitre, on se propose d'élaborer un outil logiciel de dimensionnement de ces capacités en intégrant la méthode déjà présentée dans le chapitre précédent. La présentation des différentes fonctionnalités de l'outil sera faite à travers la description de ses interfaces.

5.2 Topologie à simuler

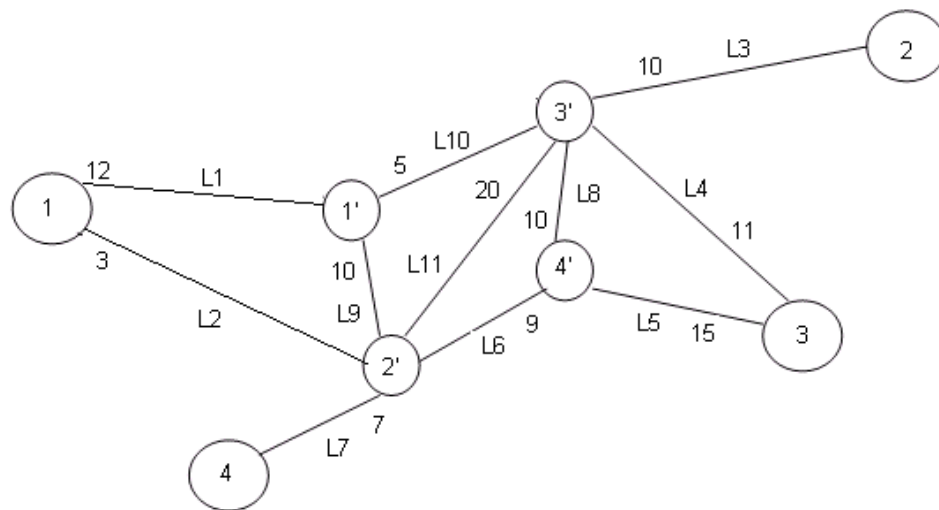


Figure 5.01 : Topologie du réseau à simuler

Le réseau véhiculant les deux types de trafic voix et données est formé comme le montre la figure 5.01 par quatre routeurs, numérotés i ($i=1, 2, 3, 4$), à la périphérie (ER ou edge router) et quatre routeurs, numérotés i' ($i'=1', 2', 3', 4'$) au cœur du réseau (SR ou switching router). Pour des raisons de simplification, on suppose que les Edge Router n'effectuent pas d'opération de commutation des paquets. Les numéros inscrits sur les lignes représentent les métriques des liens associés aux distances. Les L_j représentent les numéros des liens et ceci pour tout i de 1 à 11.

Supposons qu'on s'intéresse aux trafics A_{13} et A_{31} entre les nœuds 1 et 3. Ces trafics suivront le plus court chemin entre ces deux nœuds. Les différentes métriques possibles 28, 53, 27, 33, 34, 29, 43. Donc le plus court chemin sera celui qui passe par les routeurs internes 2'-4' à travers les liens L2, L6, L5. C'est ce chemin qui véhicule la totalité du trafic entre les nœuds 1 et 3. Ce chemin doit être capable de supporter le maximum de la charge entre ces deux nœuds.

5.2.1 Modèles utilisés

La réussite du travail dépend de la stratégie de routage choisie. Un élément qui peut jouer en sa faveur est la gestion de file d'attente. Ainsi, on a choisi une approche de modélisation simple de ce problème, en utilisant le modèle de file d'attente M/M/1. Le calcul de base donc sur l'équation : [16]

$$T_i = \frac{1}{\mu C_i - \lambda_i} \quad (5.01)$$

T_i : temps de réponse du système

μC_i : taux de service en paquet par seconde

λ_i : taux d'arrivée de paquets par seconde

5.2.2 Organigramme de la simulation

L'organigramme suivant résume les différentes étapes suivies pour le dimensionnement des capacités des liens du réseau.

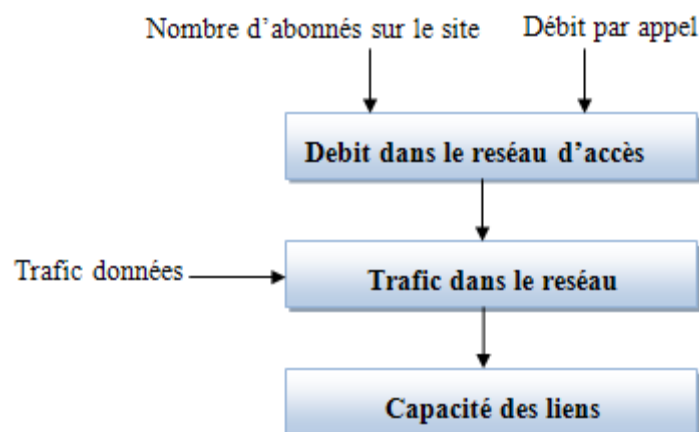


Figure 5.02 : Organigramme de la simulation

5.3 Présentation du logiciel

Le logiciel a été développé avec le langage orienté objet JAVA. Son rôle est de présenter une interface conviviale pour aider au dimensionnement des liens du réseau fournissant le service de voix sur IP. Dans ce paragraphe, nous montrons les résultats de simulation effectuée. La description de l'outil se fera en annexe.

5.3.1 Informations sur chaque site

L'interface *Information site*, représentée par la figure A1.04, en annexe permet de voir les informations relatives à chaque site.

Le tableau 5.01 contient toutes les informations relatives à chaque site du réseau. Ces informations incluent notamment le nombre d'utilisateurs, la probabilité de blocage ainsi que le taux d'utilisateurs souscrits en SLA1 et en SLA2 affectés à chaque site.

Site	Site 1	Site 2	Site 3	Site 4
Nombre d'utilisateurs	50	20	40	10
Probabilité de blocage	0.01	0.01	0.01	0.01
Taux utilisateurs SLA 1	0.2	0.3	0.4	0.25
Taux utilisateurs SLA 2	0.8	0.7	0.6	0.75

Tableau 5.01 : informations sur les sites du réseau

Notons que le choix de la probabilité de blocage est effectué par l'opérateur. Habituellement elle doit être inférieure à 0.01. C'est pourquoi on a choisit la valeur $p_B=0.01$.

5.3.2 Calcul du débit d'accès au niveau de chaque site

La boîte de dialogue *Débit d'accès par site*, représentée par la Figure A1.05 permet de calculer le *débit d'accès* nécessaire pour chaque site.

Le tableau suivant montre les relations entre les différentes variables affichées dans la boîte de dialogue *Débit d'accès par site*.

Variables d'entrée	Variables de sortie 1	Variables de sortie 2
- probabilité de blocage - taux d'arrivée - temps de service	Nombre de circuits	Débit d'accès
- codec - cycle de transmission - protocole de couche de liaison	Débit par appel	

Tableau 5.02 : *paramètres d'entrée et paramètres de sortie de la fenêtre Réseau d'accès*

Voici les débits par appel en Kbit/s obtenus, en fonction du codec, du cycle de transmission et du protocole au niveau de la couche liaison de données d'après la formule (4.03). On va catégoriser les résultats selon le choix du codec :

Codec G.711 :

Protocole liaison de données	Ethernet	HDLC	FR	PPP	ATM
Cycle de transmission (ms)					
10	124.9	100.71	99.15	103.05	99.15
20	94.46	82.35	81.57	83.52	81.57
30	73.89	65.82	65.3	66.6	65.3

Tableau 5.03 : *débit par appel par site pour le codec G.711*

Codec G.726 :

Protocole liaison de données	Ethernet	HDLC	FR	PPP	ATM
Cycle de transmission (ms)					
10	92.93	68.71	67.15	71.05	67.15
20	62.46	50.35	49.57	51.52	49.57
30	52.31	44.23	43.71	45.01	43.71

Tableau 5.04 : *débit par appel par site pour le codec G.726*

Codec G.728 :

Protocole liaison de données	Ethernet	HDLC	FR	PPP	ATM
Cycle de transmission (ms)					
10	76.93	52.71	51.15	55.05	51.15
20	46.46	34.35	33.57	35.52	33.57
30	36.31	28.23	27.71	29.01	27.71

Tableau 5.05 : débit par appel par site pour le codec G.728

On remarque que plus le débit du codec utilisé est faible, plus le débit par appel diminue. Parallèlement, plus la valeur du cycle de transmission choisi augmente, plus le débit par appel diminue.

Le choix du protocole de la couche liaison de données dépend du cadre d'utilisation. L'opérateur doit effectuer une analyse des contraintes entre coût et performance, sans entraver à la qualité de service.

Par ailleurs, afin de trouver la bande passante affectée à chaque site, on doit calculer le nombre de circuits correspondants, en fonction du taux d'arrivée et du temps moyen de service caractérisant chaque site, pour cela on utilise l'algorithme inverse d'Erlang. Voici les résultats obtenus :

Site	Site 1	Site 2	Site 3	Site 4
Nombre d'appel par heure	850	900	1200	910
Durée moyenne de communication en seconde	2400	1800	2700	1900
Trafic offert en Erlang	566,67	450	900	480,28
Nombre de circuits	594	476	929	507

Tableau 5.06 : Nombre de circuits correspondants à chaque site

En utilisant la valeur du débit par appel ainsi que la valeur du nombre de circuits obtenus, on peut calculer le Débit d'accès correspondant à chaque site en se référant à la formule (4.04). Voici les résultats obtenus :

Codec G.711 :

- Site 1:

Protocole liaison de données	Ethernet	HDLC	FR	PPP	ATM
Cycle de transmission (ms)					
10	74220.3	59845.5	58954.5	61271.10	58954.5
20	56118.15	48930.75	48485.25	49643.55	48485.25
30	50084.1	45292.49	44995.5	45767.7	44995.5

Tableau 5.07: Débit d'accès pour le site 1 avec le codec G.711

- Site 2:

Protocole liaison de données	Ethernet	HDLC	FR	PPP	ATM
Cycle de transmission (ms)					
10	59476.2	47957.0	47243.0	49099.4	47243.0
20	44970.1	39210.5	38853.5	39781.70	38853.5
30	40134.73	36294.99	36057.0	36675.79	36057.0

Tableau 5.08: Débit d'accès pour le site 2 avec le codec G.711

- Site 3 :

Protocole liaison de données	Ethernet	HDLC	FR	PPP	ATM
Cycle de transmission (ms)					
10	36675.79	93596.75	92203.25	95826.35	92203.25
20	87767.27	76526.37	75829.625	501.45	75829.625
30	78330.18	70836.24	70371.75	71579.45	70371.75

Tableau 5.09: Débit d'accès pour le site 3 avec le codec G.711

- Site 4 :

<i>Protocole liaison de données</i>	Ethernet	HDLC	FR	PPP	ATM
<i>Cycle de transmission (ms)</i>					
10	63349.65	51080.25	50319.75	52297.05	50319.75
20	47898.82	41764.12	41383.875	42372.525	41383.875
30	42748.54	38658.74	38405.25	39064.35	38405.25

Tableau 5.10: Débit d'accès pour le site 4 avec le codec G.711

Codec G.726 :

- Site 1 :

<i>Protocole liaison de données</i>	Ethernet	HDLC	FR	PPP	ATM
<i>Cycle de transmission (ms)</i>					
10	55212.3	40837.5	39946.5	426.9	39946.5
20	37110.15	29922.75	29477.25	30635.55	29477.25
30	31076.1	26284.5	25987.49	26759.69	25987.49

Tableau 5.11: Débit d'accès pour le site 1 avec le codec G.726

- Site 2 :

<i>Protocole liaison de données</i>	Ethernet	HDLC	FR	PPP	ATM
<i>Cycle de transmission (ms)</i>					
10	44244.20	32725.0	32011.0	33867.39	32011.0
20	29738.10	23978.5	23621.5	24549.7	23621.5
30	24902.733	21063.0	20824.99	21443.8	20824.99

Tableau 5.12: Débit d'accès pour le site 2 avec le codec G.726

- Site 3 :

<i>Protocole liaison de données</i>	Ethernet	HDLC	FR	PPP	ATM
<i>Cycle de transmission (ms)</i>					
10	86350.55	63868.75	62475.25	66098.34	62475.25
20	58039.275	46798.37	46101.625	47913.175	46101.625
30	48602.183	41108.25	40643.74	41851.45	40643.74

Tableau 5.13: Débit d'accès pour le site 3 avec le codec G.726

- Site 4 :

<i>Protocole liaison de données</i>	Ethernet	HDLC	FR	PPP	ATM
<i>Cycle de transmission (ms)</i>					
10	47125.65	34856.25	34095.75	36073.049	34095.75
20	31674.825	25540.125	25159.875	26148.525	25159.875
30	26524.55	22434.75	22181.24	22840.35	22181.24

Tableau 5.14: Débit d'accès pour le site 4 avec le codec G.726

Codec G.728 :

- Site 1 :

<i>Protocole liaison de données</i>	Ethernet	HDLC	FR	PPP	ATM
<i>Cycle de transmission (ms)</i>					
10	45708.3	31333.50	30442.5	32759.1	30442.5
20	27606.15	20418.75	19973.25	21131.55	19973.25
30	21572.1	16780.5	16483.5	17255.7	16483.5

Tableau 5.15: Débit d'accès pour le site 1 avec le codec G.728

- Site 2 :

<i>Protocole liaison de données</i>	Ethernet	HDLC	FR	PPP	ATM
<i>Cycle de transmission (ms)</i>					
10	36628.2	25109.0	24395.0	386.05	24395.0
20	22122.1	16362.5	16005.5	16933.69	16005.5
30	17286.73	13447.0	13209.0	13827.8	13209.0

Tableau 5.16: Débit d'accès pour le site 2 avec le codec G.728

- Site 3 :

<i>Protocole liaison de données</i>	Ethernet	HDLC	FR	PPP	ATM
<i>Cycle de transmission (ms)</i>					
10	71486.55	49004.75	47611.2	51234.35	47611.2
20	43175.275	31934.375	31237.625	33049.17	31237.625
30	33738.1	26244.25	25779.75	26987.45	25779.75

Tableau 5.17: Débit d'accès pour le site 3 avec le codec G.728

- Site 4 :

<i>Protocole liaison de données</i>	Ethernet	HDLC	FR	PPP	ATM
<i>Cycle de transmission (ms)</i>					
10	39013.65	26744.25	25983.75	27961.05	25983.75
20	23562.825	17428.125	17047.875	18036.52	17047.87
30	18412.55	14322.75	14069.25	14728.35	14069.25

Tableau 5.18: Débit d'accès pour le site 4 avec le codec G.728

Les résultats sont influencés par la variation des paramètres d'entrée c'est-à-dire par le trafic, le choix du codec, le cycle de transmission et le protocole de la couche liaison de données.

En effet, l'augmentation de la valeur du débit d'accès est proportionnelle à l'augmentation de celle du débit par appel ainsi que celle du nombre de circuits. Les résultats affichés dans la boîte de dialogue sont : le nombre de circuits, le débit par appel et le débit d'accès

La priorité de l'opérateur est de diminuer le nombre de ressources à mettre en œuvre pour des raisons de coût. Ainsi, il est nécessaire que le débit soit le plus faible possible pour des raisons de surcharge au sein de son réseau.

L'interprétation des résultats de simulation peuvent être résumée comme suit :

- Influence du trafic sur le nombre de circuits : plus le trafic augmente plus le nombre de circuits à réserver augmente.
- Influence du codec sur le débit par appel : plus le débit du codec utilisé est faible plus le débit par appel est faible.
- Influence du cycle de transmission sur le débit par appel : l'augmentation du cycle de transmission permet de diminuer le débit par appel.

L'opérateur doit donc effectuer un choix qui doit tenir compte des contraintes engendrées par chaque paramètre dans les calculs du débit d'accès.

5.3.3 Capacité voix

Le calcul de la capacité voix s'effectue par l'intermédiaire de la boîte de dialogue *Caractéristiques voix* de la figure A1.06.

Le calcul de la capacité des liens nécessite de connaître tous les trafics possibles entre les différents nœuds du réseau. Pour cela, on doit répartir le trafic à l'entrée de chaque nœud. Répartir le trafic entre les différents nœuds se fait selon le nombre d'utilisateurs dans chaque site. Le calcul de la capacité pour la voix est conforme à la formule (4.05).

Selon les nœuds source et destination choisis, la répartition du trafic est présentée dans le tableau 5.19 tel que la représentation en ligne représente la source et celle en colonne la destination :

	Nœud 1	Nœud 2	Nœud 3	Nœud 4
Nœud 1	0	161.9	323.81	80.95
Nœud 2	225.0	0	180.0	45.0
Nœud 3	562.5	225.0	0	112.5
Nœud 4	218.81	87.27	174.54	0

Tableau 5.19 : Matrice de trafic entre les nœuds

Selon les nœuds d'extrémités choisis, on calcule la métrique du plus court chemin en utilisant l'algorithme de DIJKSTRA :

Nœuds d'extrémité	1-2	1-3	1-4	2-3	2-4	3-4
Métrique du plus court chemin	27	10	27	21	32	31

Tableau 5.20 : Matrice de trafic entre les nœuds

On peut calculer la capacité des liens individuels en utilisant la formule (4.06), elle est fonction du choix des nœuds d'extrémités. Pour ce faire, on ne considère que le plus court chemin reliant deux sites. Voici un exemple de calcul pour quelques liens :

Lien	L1	L2	L3	L4	L5
Capacités du lien	10446.3	26927.97	23183.94	8505	32828.61

Tableau 5.21 : Capacité des liens individuels

La capacité des liens voix sont essentiellement fonction des trafics qui circulent entre les différents nœuds du réseau. Ainsi plus le trafic qui traverse un lien est grand plus la capacité à mettre en œuvre doit également être grande.

5.3.4 Calcul de la capacité totale du lien

La boîte de dialogue *Caractéristiques données* de la figure A1.06 permet de calculer la capacité totale des liens.

Le calcul de la capacité totale nécessite d'ajouter au résultat du calcul précédent les trafics data possibles sur chaque lien. Les paramètres d'entrées et de sortie peuvent être résumés dans le tableau suivant :

Paramètres d'entrée	Paramètre de sortie
- Débit upload - Débit download	Débit data au niveau du nœud d'entrée
- Lien - trafic data avec le nœud lié au site d'accès Internet	Capacité du lien (data)
- Capacité du lien (data) - Trafic voix - Débit signalisation	Capacité totale

Tableau 5.22 : *paramètres d'entrée et de sortie pour la boîte de dialogue capacité totale*

On calcule les débits upload et download correspondant à chaque site en utilisant les formules (4.11) et (4.12). Les tableaux suivants représentent respectivement les débits upload et download entre les sites:

- *Débit upload (en Kbit/s):*

	Nœud 1	Nœud 2	Nœud 3	Nœud 4
Nœud 1	0	2432	3712	896
Nœud 2	5504	0	3456	640
Nœud 3	6144	2816	0	1280
Nœud 4	5248	1920	3200	0

Tableau 5.23: *Débit Upload*

- Débit download (en Kbit/s):

	Nœud 1	Nœud 2	Nœud 3	Nœud 4
Nœud 1	0	4864	7424	1795
Nœud 2	11008	0	6912	1280
Nœud 3	12288	5632	0	2560
Nœud 4	11264	4608	7168	0

Tableau 5.24 : Débit download

Pour calculer la capacité du plus court chemin en termes de débit, on ajoute le débit upload au débit download correspondant à chaque site :

Site	Site 1	Site 2	Site 3	Site 4
Capacité du plus court chemin	21123	28800	30720	33408

Tableau 5.25 : Capacité du plus court chemin

On procède de la même manière que pour le calcul de la capacité des liens individuels de la voix pour calculer la capacité des liens pour les données. Pour cela on utilise la formule (4.13).

Lien	L1	L2	L3	L4	L5
Capacités du lien	22309.29	53058.65	92481.9	24855.81	80731.3

Tableau 5.26: Capacité des liens supportant le trafic de données

On remarque que la capacité des liens pour les données est plus importante que celle de la voix. En effet le service de données est le plus dominant sur un réseau IP.

Ainsi en additionnant la capacité des liens individuels pour les deux types de trafic, on obtient la capacité totale des liens.

Lien	L1	L2	L3	L4	L5
Capacité total du lien	22309.29	53058.65	92481.9	24855.81	80731.3

Tableau 5.27: *Capacité totale des liens*

5.4 Conclusion

Dans ce chapitre, on a présenté les fonctionnalités de base de l'outil développé. Ce qu'on peut remarquer c'est que la procédure de dimensionnement des capacités des liens n'est pas une tâche assez simple. En effet, dans des réseaux IP multiservices le comportement des utilisateurs est aléatoire essentiellement pour le trafic de données. Le manque de données fournies par un opérateur rend la procédure encore plus complexe. On a essayé de simplifier quelques détails pour rendre l'opération de dimensionnement faisable sans oublier que peu de recherches ont été faites sur le service VoIP. La simulation était un moyen pour tester certains paramètres de la qualité de service essentiellement le taux de rejet des paquets au niveau du nœud d'accès au réseau.

CONCLUSION

L'application de quelques règles d'ingénierie est un élément essentiel dans le processus de dimensionnement. Mais, faute de données et de statistiques fournies par un opérateur, la tâche de dimensionnement se trouve face à quelques obstacles. Ces statistiques contribuent avec des modèles mathématiques à donner un aspect plus réaliste au processus de dimensionnement. On peut chercher à optimiser la bande passante en prenant la topologie choisie comme une topologie de référence. Le chantier reste encore ouvert à d'autres améliorations au niveau du travail effectué.

Ce travail consiste à dimensionner les capacités des liens au niveau d'un réseau supportant à la fois le trafic voix et données. Il a pour principal objectif le dimensionnement du réseau de voix sur IP. On effectue un dimensionnement afin d'offrir correctement le service de la voix sur IP. Outre le dimensionnement du trafic voix, l'outil permet également de dimensionner le réseau avec l'intégration d'un autre type de trafic qui est le trafic de données. L'objectif principal de ce travail a été de dimensionner les liens du réseau. En fonction des résultats obtenus, l'étude d'une topologie de référence permet de faciliter le choix d'une topologie adéquate pour des études ultérieures.

La qualité des services offerts n'est pas encore satisfaisante dans le cadre de l'utilisation de la VoIP. En effet pour un réseau véhiculant deux types de trafic très différents qui sont le trafic voix et le trafic données, le partage de ressources au sein du réseau n'est pas toujours évident. D'où, cette proposition de méthode d'optimisation du partage de ressources par la planification des liens du réseau.

Par ailleurs, vu que la VoIP est une technologie basée sur Internet Protocol, elle est exposée à plusieurs types de risques. Ainsi, pour compléter ce travail, des solutions de sécurisation de la VoIP devront être étudiées.

ANNEXES

ANNEXE 1 INTERFACE DU LOGICIEL DE SIMULATION

Le logiciel développé avec le langage JAVA comprend six interfaces dont voici respectivement les descriptions :

A1.1 Interface principale

Pour lancer l'application, on clique sur le fichier exécutable « P.L.VoIP » :



Figure A1.01 : *Lancement du fichier exécutable*

L'utilisation de l'outil commence par l'accès à la fenêtre principale qui est présentée par la figure A1.02 :



Figure A1.02 : *Interface d'accueil*

- *Entrer* permet de lancer la simulation proprement dite.
- *Quitter* permet de quitter définitivement l'application. Si on valide ce bouton, une demande de confirmation apparaîtra :

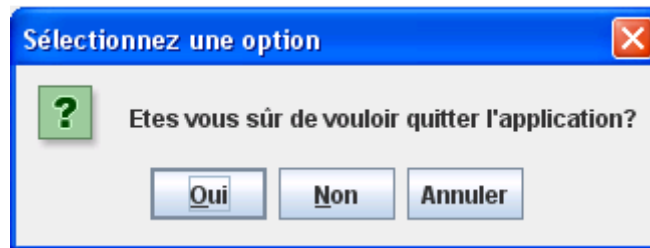


Figure A1.03 : *Message de confirmation*

Notons que pour connaître la fonction des boutons des interfaces de simulation, on déplace le curseur sur les boutons concernés, des info-bulles apparaissent.

A1.2 Informations sur les sites

L'utilisateur peut saisir les informations sur le site choisi grâce à la boîte de dialogue *Information Site*. Le choix du site nous permet d'afficher le nombre d'utilisateurs et de faire entrer la probabilité de blocage et le pourcentage d'utilisateurs ayant respectivement des contrats SLA 1 et SLA 2.

- *Capacité Voix* : ce bouton permet d'accéder à la boîte de dialogue *Caractéristiques Voix*.
- *Capacité data* : ce bouton permet d'accéder à la boîte de dialogue *caractéristiques Data*.
- *Calcul débit d'accès* : ce bouton permet d'accéder à la boîte de dialogue *Bande passante*
- *Accueil* : ce bouton permet de retourner à l'interface d'accueil.

La figure A1.04 représente l'interface qui permet de connaître les différents paramètres affectés à chaque site, ces paramètres sont notamment le nombre d'utilisateurs, la probabilité de blocage, les taux de souscription des abonnés pour les contrats de type SLA1 et SLA2. Dans le cas suivant on a choisi le site 2.

Information site

Information Site

Site **Nombre d'utilisateurs**

site 3 40

Voix

Probabilité de blocage 0.01

Données

SLA1 0.4 %

SLA2 0.6 %

Calcul débit d'accès

Capacité voix

Capacité Données

Accueil

Figure A1.04 : Recueil d'Informations sur le site 3

A1.3 Débit d'accès affecté à chaque site

La fenêtre *Débit d'accès par site* de la figure A1.05 permet de calculer le débit d'accès qui devra être affectée à chaque site en faisant des calculs intermédiaires qui consistent notamment dans le calcul du :

- nombre de circuits,
- débit par appel

Dans cette interface, l'utilisateur doit choisir un site, puis tenir compte de plusieurs paramètres tels:

- le choix du codec,
- le cycle de transmission,
- le protocole au niveau de la couche liaison de données.

Les résultats affichés sont : le débit par appel pour un site donné, le nombre de circuits ainsi que le débit d'accès à mettre en œuvre.

Debit d'accès par site

Paramètres d'entrée

Site	Taux d'arrivée	Durée moyenne de service
site 3	1200	2700 s

Choix paramètres

choix du Codec: ☒ G.711 ☐ G.726 ☐ G.728

Cycle de transmission: 20 ms

Protocole couche liaison de données: Ethernet

Résultats

Débit par appel	94.47	Kbps
Nombre de circuits	929.0	
Débit d'accès	87767.27	kbps

Calculer

Voir la répartition

Accueil

Figure A1.05: calcul du débit d'accès au niveau du site 3

- *Accueil* : ce bouton permet de revenir à l'interface Principale.
- *Calculer* : permet de calculer le débit par appel, le nombre de circuits et le débit d'accès.
- *Voir la répartition* : ce bouton permet d'afficher la boîte de dialogue caractéristiques Voix.

A1.4 Caractéristiques Voix

Dans la figure A1.06, on a pris comme source le nœud 3. Notons que l'on a précisément calculé le débit d'accès au niveau du site 3 dans l'interface précédente. On appuie sur le bouton *Répartir le trafic* pour répartir le trafic à travers les nœuds du réseau.

On choisit le nœud de destination afin de trouver la métrique du plus court chemin. Dans le cas de l'exemple, le destinataire est le nœud 4.

Parmi les liens empruntés par l'information issue de la source vers sa destination, on en choisit un pour voir sa capacité. Dans notre cas, on a sélectionné le lien L5.

Caractéristiques Voix

Répartition du trafic

Répartir le trafic

Source

Noeud source

3

Destination

Noeud 1	562.5	E	Noeud 3	0.0	E
Noeud 2	225.0	E	Noeud 4	112.5	E

Choix des noeuds d'extrémité

Noeuds d'extrémités 3-4

Métrique du plus court chemin 31

Calculer

Capacité des liens

Choix du lien L5

Calculer la capacité

Capacité du lien 32828.61

Caractéristiques données

Précédent

Accueil

Figure A1.06 : exemple de caractéristiques voix

- *Caractéristiques données* permet d'accéder à la boîte de dialogue Caractéristiques données qui permet de voir les caractéristiques du trafic de données et de calculer la capacité totale du lien.
- *Précédent* permet de revenir à l'interface Caractéristiques Voix.
- *Accueil* permet de revenir à l'interface principale.

A1.6 Caractéristiques Données

- *Capacité lien* : ce bouton permet d'afficher la capacité du lien choisi pour le trafic data uniquement.
- *Afficher capacité totale* : ce bouton permet de calculer la capacité du lien choisi en tenant compte du trafic voix, de la signalisation ainsi que du trafic data.

On sélectionne un site, notamment celui avec lequel on a travaillé dans les calculs précédents, afin de déterminer les caractéristiques données et d'en déduire par conséquent la capacité totale du lien. Dans notre cas on a travaillé sur le site 3 et le lien L5.

The screenshot shows a software window titled "caractéristiques Données". It contains three main sections for data entry and calculation:

- Débit**: A section with a "Site" dropdown menu set to "site 3". Below it are two input fields: "Débit total Upload" with the value 4096.0 and "Débit total Download" with the value 8192.0. To the right of these fields is the unit "Kbps" and a "Calcul débit" button.
- Capacité du plus court chemin**: A section with an input field for "Capacité du plus court chemin" containing the value 12288.0 and a "Calcul capacité" button below it.
- Capacité des liens**: A section with a "Choix du lien" dropdown menu set to "L5" and an input field for "Capacité du lien" containing the value 80731.3. To the right is a "calcul capacité lien" button.

At the bottom of the window, there is a "Capacité totale" button next to an input field showing the final result, 113559.91, and a "Terminer" button on the far right.

Figure A1.07 : détermination de la capacité totale des liens

Le résultat final est donc la capacité totale que l'on doit attribuer au lien L5 afin qu'il puisse supporter à la fois le trafic voix et le trafic de données issus du site 3.

ANNEXE 2 Les architectures OSI et TCP/IP

A2.1 Le modèle OSI

A2.1.1 Principe général

Le modèle OSI (Open System Interconnexion) a été développé en 1978 par l'ISO (International Standard Organization) afin que soit défini un standard utilisé dans le développement de système ouvert. Les réseaux s'appuyant sur le modèle OSI parlent le même langage, ils utilisent des méthodes de communication semblables pour échanger des données. Le modèle OSI a sept couches : la couche physique, la couche liaison de données, la couche réseau, la couche transport, la couche session, la couche présentation, et la couche application. [1]



Figure A2.01: *Le modèle OSI*

Les principes ayant conduit aux sept couches sont les suivantes :

- Une couche ne peut être créée que quand un niveau différent d'abstraction est nécessaire.
- Chaque couche doit fournir une fonction bien définie.
- Les fonctions de chaque couche doivent être choisies en pensant à la définition de protocoles normalisés internationaux.
- Les caractéristiques d'une couche doivent être choisies pour qu'elles réduisent les informations transmises entre les couches.

Le nombre de couches doit être suffisamment grand pour éviter la cohabitation dans une même couche de fonctions très différentes et suffisamment petit pour éviter que l'architecture ne devienne difficile à maîtriser. [2]

A2.1.2. Rôles des couches

La couche **physique** s'occupe de la transmission des bits de façon brute sur un circuit de communication. Les bits peuvent être en codés sous forme de 0 ou de 1 ou sous forme analogique. Elle fait intervenir des interfaces mécaniques et électriques sur le média utilisé.

La couche **liaison de données** prend les données de la couche physique et fournit ses services à la couche réseau. Les bits reçus sont groupés en unité logique appelée trame. Les fonctions de contrôle de flux et d'erreurs y sont éventuellement assurées avec un contrôle d'accès au support.

La couche **réseau** gère la connexion entre les différents nœuds du réseau. Il comporte trois fonctions principales : le contrôle de flux, le routage et l'adressage.

La couche **transport** effectue des contrôles supplémentaires à la couche réseau. Elle réalise le découpage des messages en paquets pour la couche réseau. Elle doit également gérer les ressources de communication en gérant un contrôle de flux ou un multiplexage. C'est l'ultime niveau qui s'occupe de l'acheminement de l'information.

Le rôle de la couche **session** est de fournir aux entités de présentation les moyens nécessaires à l'organisation et à la synchronisation de leur dialogue. Elle a pour but d'ouvrir et de fermer des sessions entre les utilisateurs et possède par conséquent des fonctionnalités nécessaires à l'ouverture, à la fermeture et au maintien de la connexion. L'insertion de points de synchronisation est recommandée ; ils permettent, en cas de problèmes, de disposer d'un point précis à partir duquel l'échange pourra redémarrer.

Pour que deux systèmes puissent se comprendre, ils doivent utiliser le même système de représentation des données, et cette tâche est assurée par la couche présentation. Elle se charge donc de la syntaxe des informations, de la représentation des données transférées entre applications. [1]

Quant à la couche **application**, elle fournit les fonctions nécessaires aux applications utilisateurs qui doivent accomplir des tâches de communication. Elle intègre les logiciels qui utilisent les ressources du réseau.

A2.2. Le modèle TCP/IP

Dans les années 70, la défense américaine, DoD (Department Of Defense), devant le foisonnement de machines utilisant des protocoles de communication différents et

incompatibles, décide de définir sa propre architecture. Cette architecture TCP/IP est à la source de l'Internet.

Contrairement au modèle OSI, le modèle TCP/IP ne comporte que quatre couches : la couche accès réseau, la couche Internet, la couche transport et la couche application. Les deux principaux protocoles définis sont : TCP et IP.

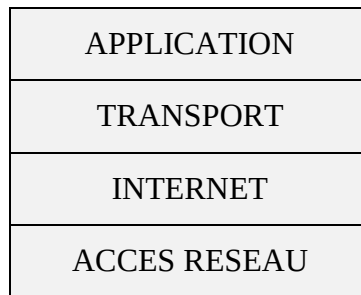


Figure A2.02 : *le modèle TCP/IP*

La couche accès réseau représente la connexion physique avec les câbles, les cartes réseau, les protocoles d'accès au réseau.

La couche Internet doit fournir une adresse logique pour l'interface physique. Cette couche fournit un mappage entre l'adresse physique et l'adresse logique grâce aux protocoles ARP (Address Resolution Protocol) et RARP (Reverse Address Resolution Protocol). Quant à ICMP (Internet Control Message Protocol), il s'occupe des problèmes et diagnostics associés au protocole IP. Cette couche gère également le routage des paquets entre les hôtes.

La couche transport définit la connexion entre deux hôtes. Deux protocoles sont associés à cette couche, le TCP et l'UDP. TCP est responsable du service de transmission fiable avec la fonction de détection et de correction d'erreurs. UDP est quant à lui, un protocole peu fiable, il est spécialement utilisé dans les applications n'exigeant pas la fiabilité de TCP, comme dans les applications temps réel.

La couche application renferme les protocoles d'application fournissant des services à l'utilisateur. Elle interface donc les applications utilisateurs avec la pile de protocole TCP/IP.

[2]

BIBLIOGRAPHIE

- [1] Randriarijaona L.E., « *Réseaux TCP/IP* », Cours I4-TCO, Dép. Tél.-E.S.P.A, A.U. : 2007-2008
- [2] Pujolle G., « *Les réseaux* », Edition Eyrolles : Paris, 2003
- [3] Servin C., « *Réseaux et Télécoms*», Dunod : Paris, 2003
- [4] Andriamiasy Z.V., « *Téléphonie avancée* », Cours I5-TCO, Dép. Tél.-E.S.P.A., A.U. :2008-2009
- [5] Andriamialison T.H., « *La Voix sur IP* », Mémoire de fin d'études en vue d'obtention du diplôme d'Ingénieur, Dép. Tél. –E.S.P.A, A.U. :2000-2001
- [6] Hersent O., Gurle D., Petit J.P., « *La Voix sur IP* », Dunod : Paris 2006
- [7] Sulkin A., « *PBX Systems for IP Telephony* », McGraw-Hill Telecom: USA 2002
- [8] ITU-T, Recommandation Y.1291, « *An architectural framework for support of Quality of Service (QoS) in Packet networks* », juillet 2003
- [9] Cabinet Arcome, « *Etude technique, économique et réglementaire de l'évolution vers les réseaux de nouvelle génération NGN* », Septembre 2002
- [10] Kofman D., « *Synthèse sur l'évolution des réseaux de télécommunications* », ENST, Paris : 2001
- [11] Tanenbaum A., « *Réseaux* », 4^e Edition, Pearson Education, Paris : 2003
- [12] Rakotomalala M.A., « *Réseaux des Télécommunications* », Cours I5-TCO, Dép. Tél.-E.S.P.A., A.U. : 2007-2008
- [13] Ratsiranto A., « *Outils de planification de réseau* », Cours 5^{ème} année, Dép. Tél. E.S.P.A, A.U. : 2008-2009
- [14] Grondran M., Minoux M., « *Graphes et algorithmes* ». Dunod Informatique, 1978
- [15] Cohen J., « *Théorie des graphes et algorithmes* », UIT Bordeaux I, 2002
- [16] Rasamoelina J.N., « *Trafic et file d'attente* », Cours I5-TCO, Dép. Tél.-E.S.P.A., A.U. : 2008-2009
- [17] Rabeherimanana L.I., « *Théorie des graphes* », Cours I5-TCO, Dép. Tél. –E.S.P.A., A.U. : 2008-2009

- [18] Randriamitantsoa P.A., « *Ingénierie des réseaux cellulaires* », Cours I5-TCO, Dép. Tél. -E.S.P.A., A.U : 2008-2009
- [19] Gelenbe E., Pujolle G., « *Introduction aux réseaux de file d'attente* », Edition Eyrolles, Paris : 1990

PAGE DE RENSEIGNEMENTS

Nom : RAMINOSON

Prénoms : Mamintsoa Sitraka



Adresse de l’auteur : Lot AV 452 Ambohijanamasoandro Itaosy
ANTANANARIVO 102
Madagascar
Tél : + 261 (0) 33 14 664 07
E-mail : mamintsoa.sitraka@gmail.com

Titre du mémoire : « PLANIFICATION DES LIENS VOIP »

Nombre de pages : 104

Nombre de figures : 38

Nombre de tableaux : 37

Mots clés : capacité - graphes - Dijkstra - VoIP - trafic - liens - Débit - Bande passante - Nœud

Directeur de mémoire : M. RATSIMBAZAFY Andriamanga
Tél : +261 (0) 34 01 377 97
E-mail : ndriamanga@gmail.com

RESUME

Dans le contexte d'unification du réseau de voix et de données, le marché de la téléphonie est en train d'évoluer vers une convergence voix/données autour d'un protocole unique : IP. Cependant cette technologie est encore loin de satisfaire aux exigences de qualité de service attendues pour la transmission de la voix.

Ce mémoire consiste à effectuer une étude théorique des caractéristiques du réseau en effectuant la simulation d'une topologie de réseau spécifique, en vue d'améliorer la performance du réseau en termes de qualité de service. Ainsi, ce travail propose une étude d'optimisation de partage de ressources au sein d'un réseau IP en effectuant une planification des liens du réseau afin qu'ils puissent supporter le trafic voix et le trafic de données.

ABSTRACT

About unification of the network containing voice and data, the market of the telephony is evolving toward a convergence voice/data around Internet protocol. However this technology is still far from satisfying all the requirements of QoS concerning voice transmission.

The main objective of this work is to do a theoretical survey of the network's features while doing the simulation of a specific network topology, in view to improve it the performance of the network in terms of service quality. Thus, this work proposes a survey of sharing resources optimization within an IP network by making a dimensioning of the network links as well as they would support voice and data traffic.