VOIP : un exemple en Afrique

Bruno ROGER
ESMT Division Informatique
BP 10.000 DAKAR Liberté (SENEGAL)
bruno.roger@esmt.sn

Oumar Samba BA
ESMT Division Informatique
BP 10.000 DAKAR Liberté (SENEGAL)
Oumarsamba.ba@esmt.sn

Ahmed BOREAU
ESMT Division Informatique
BP 10.000 DAKAR Liberté (SENEGAL)
Ahmed.boreau@esmt.sn

Kader BONGO
ESMT Division Informatique
BP 10.000 DAKAR Liberté (SENEGAL)
Kader.bongo@esmt.sn

Résumé

Le but de ce document est de présenter un cas pratique de mise en oeuvre d'un système de communication de type voix a travers un réseau de type IP. En particulier, après avoir donné quelques définitions nécessaires, nous étudierons dans un premier temps comment établir un réseau local pour la téléphonie, dans un second temps l'interconnexion de plusieurs réseaux de téléphonie, notamment le tunneling, la réservation de bande passante et la qualité de service, puis dans un dernier temps les applications avancées, telles que la sécurité ou le comptage des appels en vue de la taxation. Nous verrons également comment mettre en œuvre un plan de numérotation, avec comme exemple Dakar (numéros 95xxxx) et ses pays membres (préfixes 96xxxx et suivants) en réseau avec RENATER (préfixes 91, 92 et 93) via Internet. La plupart des équipements utilisés sont de type CISCO, mais il faut garder a l'esprit que de nombreux autres produits (notamment des logiciels libres) fonctionnent avec les mêmes configurations et pourraient aussi bien faire l'affaire.

Mots clefs

VOIP, CISCO, H323, SIP, Gateway, Gatekeeper, AAA, …

1 Introduction

Les technologies « intégrées » proposant le transport de plusieurs informations différentes sur un même support sont aujourd'hui très prisées non seulement pour les économies qu'elles permettent de réaliser mais également par la souplesse d'utilisation qu'elles proposent. La Voix sur IP (VOIP) est l'une de ces technologies puisqu'elle permet de transporter la parole sur un réseau de données de type Intranet ou Internet.

1.1 Définitions

Le terme générique VOIP est souvent utilisé dans son sens le plus général pour désigner toutes les solutions permettant le transport de la parole sur un réseau IP. En fait, il faut distinguer :

- la voix sur IP : transport de la parole sur un réseau IP de type privé (Intranet/extranet)
- la voix sur Internet : le transport de la parole via Internet
- la téléphonie sur IP : en plus de la parole, les fonctions téléphoniques (signalisation, fax, multi-appel) sur IP
- la téléphonie sur Internet : propose les services téléphoniques de base via Internet

L'Union Internationale des Télécommunications (UIT-T G114) a fixé la limite entre service téléphonique et transport de la voix à 150ms.

Nom	Délai	Utilisation
Class 1	0 à 150ms	Communications normales
Class 2	150 à 300ms	Bidirectionnel peu interractif
Class 3	300 à 700ms	Semi duplex
Class 4	Plus de 700ms	Radio amateur et militaires

Tableau 1 : *Délai et interactivité (UIT)*

Enfin, de manière historique, on distingue trois types de VOIP (au sens large) :

- la VOIP de PC à PC : lorsque deux utilisateurs d'un LAN ou d'Internet utilisent leurs PC multimédia pour communiquer oralement. Cela nécessite un microphone et des haut-parleurs, ainsi qu'un logiciel approprié (Netmeeting/Gnomemeeting par exemple). Ce type de VOIP n'est en général pas taxé.
- La VOIP de PC à Téléphone ou de Téléphone à PC : elle met en œuvre une passerelle soit au départ de l'appel soit à l'arrivé de l'appel pour faire transiter la communication d'un réseau IP à un réseau téléphonique (RTC). L'appel est taxé uniquement pour la partie RTC, donc pour les appels internationaux plus la proportion du segment IP est grande, plus l'économie réalisée sera intéressante.
- La VOIP de téléphone à téléphone : lorsque le demandeur et le demandé utilisent un poste téléphonique classique, le réseau de transport étant transparent. Elle met en œuvre plusieurs passerelles et la taxation de l'appel dépend de l'opérateur (non taxé dans le cas d'un réseau privé). C'est cette dernière qui réalise le plus l'intégration voix/données.

1.2 Normes et standards

Pour les réseaux de données, on utilise la famille de protocoles TCP/IP, avec notamment :

- Internet Protocol (IP-RFC791) : réalise l'adressage (32 bits) et l'acheminement des paquets d'un nœud à l'autre.
- User Datagram Protocol (UDP-RFC768) : transporte les données utilisateurs de bout en bout sans connections et sans contrôle d'erreurs. Simple et leger il est bien adapté à la VOIP
- Real-Time Transport Protocol (RTP-RFC3550) : au dessus d'UDP, il permet la remise contrôlée des données en temps réel, avec notamment des fonctions de numérotation de séquence ou d'horodatage.

Pour les réseaux téléphoniques, l'Union Internationale des Télécommunications (UIT) a définit tous les standards dans les livres de la série A à Z, en particulier :

- la série D pour les principes Généraux de la tarification (ex : D300R pour les quotes-parts)
- La série E pour l'exploitation générale du réseau (ex : E164 pour la numérotation internationale)
- La série G pour les systèmes et supports de transmission numériques (ex : G703 pour le MIC 2Mb/s)
- La série H pour les systèmes audiovisuels et multimédias (ex : H320 pour la visioconférence sur RNIS)
- La série Q pour la commutation et la signalisation (ex : Q932 pour la signalisation RNIS)
- La série X pour les réseaux de données et systèmes ouverts (ex : X25 ancêtre de Frame Relay)

Pour le codage de la parole, le standard le plus utilisé est le G711 ou Pulse Code Modulation (PCM) qui échantillonne la parole en mots de 8 bits à 8KHz. Le débit résultant est de 64Kb/s et il existe deux variantes : la loi A (Amérique du Nord et Japon) et loi mu (Europe et reste du monde).
D'autres codecs moins gourmands en bande passante sont utilisés pour la VOIP ou pour les applications de téléphonie mobile. Ils exploitent plus finement les caractéristiques de la parole (fréquences) et utilisent la compression pour atteindre des débits allant jusqu'à 5,3 Kb/s.

CODEC	Débit	Score d'écoute (MOS)
G711 (PCM)	64Kb/s	82% (4,1)
G726 (ADPCM)	32Kb/s	77% (3,85)
G728 (LD-CELP)	16Kb/s	72% (3,61)
G729 (CS-ACELP)	8Kb/s	78% (3,92)
G723.1 (MPLQ)	6,3Kb/s	78% (3,9)
G723.1 (ACELP)	5,3Kb/s	73% (3,65)

Tableau 2 : *Codec voix et débits*

Enfin, pour la gestion des appels, il existe trois standards:

- la famille H323 : dérivée de la famille H320 destinée aux applications de visioconférence sur RNIS et comporte plusieurs couches telles que le H225 (pour le contrôle des appels, la mise en paquets et la synchronisation des flux), le H245 (pour l'ouverture et la fermeture des canaux), le H261 (pour le codage de la vidéo à N x 64Kb/s), le H263 (pour le codage de la vidéo à des débits faibles), et les codecs audio (G711, G723, G729).
- Le Session Initiation Protocol (SIP) : à la différence de H323, SIP est à la base étudié pour satisfaire les contraintes d'un réseau de données. Il repose sur une série de primitives d'établissement d'appel (REGISTER, INVITE, ACK, BYE, CANCEL, OPTIONS) et fait très peu appel des serveurs (proxy ou redirecteurs par exemple).
- Le Media Gateway Control Protocol (MGCP) : à l'inverse de H323 et SIP ou le terminal est intelligent et le réseau est simple, MGCP met en œuvre un organe central de gestion des appels et s'appuie sur des terminaux simplifiés à l'extrême. Bien que très utilisé dans l'industrie, MGCP n'est pas reconnu comme un standard officiel.

1.3 La famille H323 (UIT)

1.3.1 Architecture

L'architecture de H.323 s'appuie sur trois familles de protocoles à savoir :

1) les protocoles de communications (RTP, RTCP, …) ;
2) les protocoles de codages audio (G.711,G723.1, G.728,…) et vidéo (H.261 et H.263) ;
3) les protocoles de signalisation (RAS, H.245, Q.931) ;

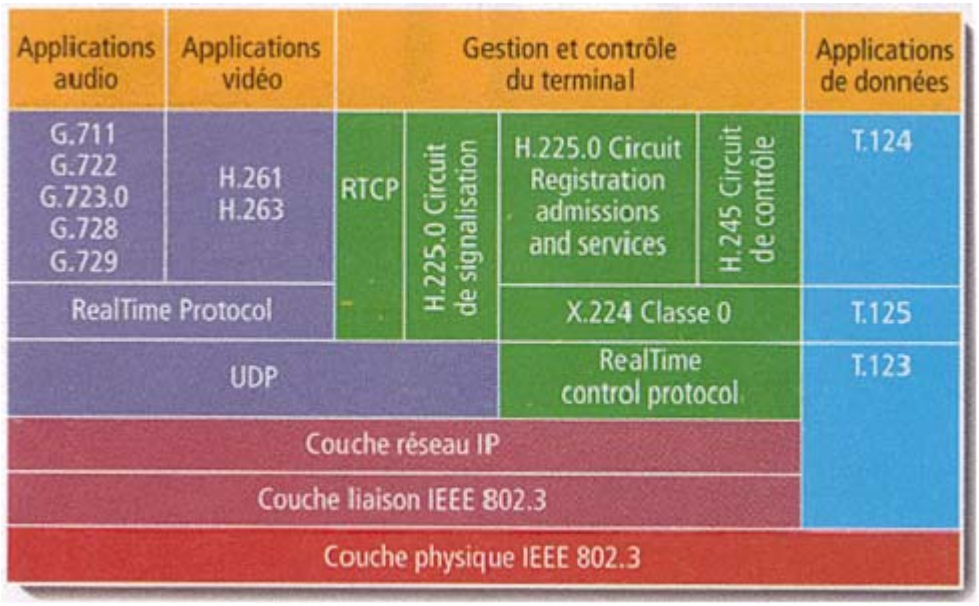

Figure 3 : *La famille de protocoles H323*

1.3.2 Implémentation de H323

Quatre (4) composants permettent l'implémentation du protocole H.323 notamment :

1) **Les équipements d'extrémité ou terminaux H323 (PC+** logiciel Netmeeting) ;
2) **Les gateways,** points d'interconnexion entre les réseaux IP et le RTC, ils assurent les fonctions de codage, de paquetisation ;
3) **Les gatekeepers,** jouant pratiquement le rôle d'un PABX en RTC, assurent le plan d'adressage et l'accès aux ressources (bande de passante par exemple) ;
4) **Et enfin le MCU** assurant les fonctions de multicast.

1.4 Le protocole SIP (IETF-RFC2543)

1.4.1 Architecture

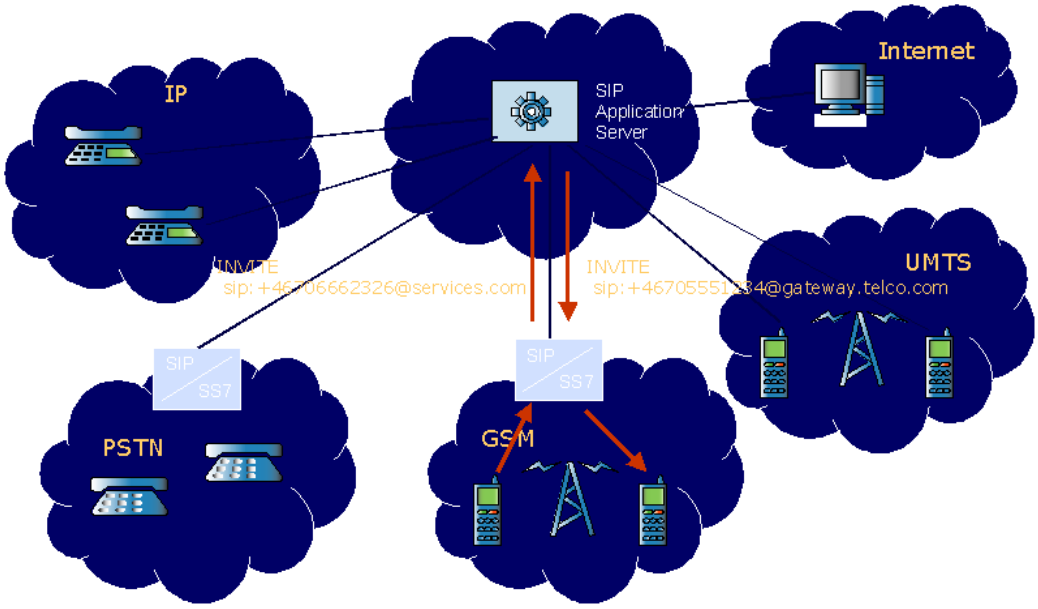

Figure 4 : *Architecture SIP*

1.4.2 Implémentation de SIP

L'implémentation du protocole SIP repose sur les éléments suivants:

1) **Le User Agent Client** constitue l'application d'extrémité (terminal d'abonné) émettant les requêtes ;
2) **Le User Agent Server** reçoit les requêtes (enregistrement, position) du User Agent Client;
3) **Le Location Server, généralement une base de données,** permet de mémoriser les différents utilisateurs (droits, mots de passe, etc.) ainsi que leurs positions actuelles ;
4) **Le Proxy Server** est un serveur auquel est relié le terminal fixe ou mobile. Il permet de relayer les messages vers le ou les terminaux auxquels ceux-ci sont destinés ;
5) **Le Redirect Server** réalise un mapping d'adresses vers une ou plusieurs nouvelles adresses;
6) **Le Gateway** permet de connecter le réseau SIP/IP au réseau commuté.

2 La téléphonie dans un LAN

L'ESMT comporte un réseau local d'une centaine de machines, organisées en topologie d'étoile étendue (à 4 segments principaux). L'un des segments (laboratoires) nous a servi pour mettre en place la VOIP dans notre réseau. Pour ce faire, nous avons utilisé :

- une gateway
- deux téléphones analogiques
- plusieurs PC avec Netmeeting
- un gatekeeper

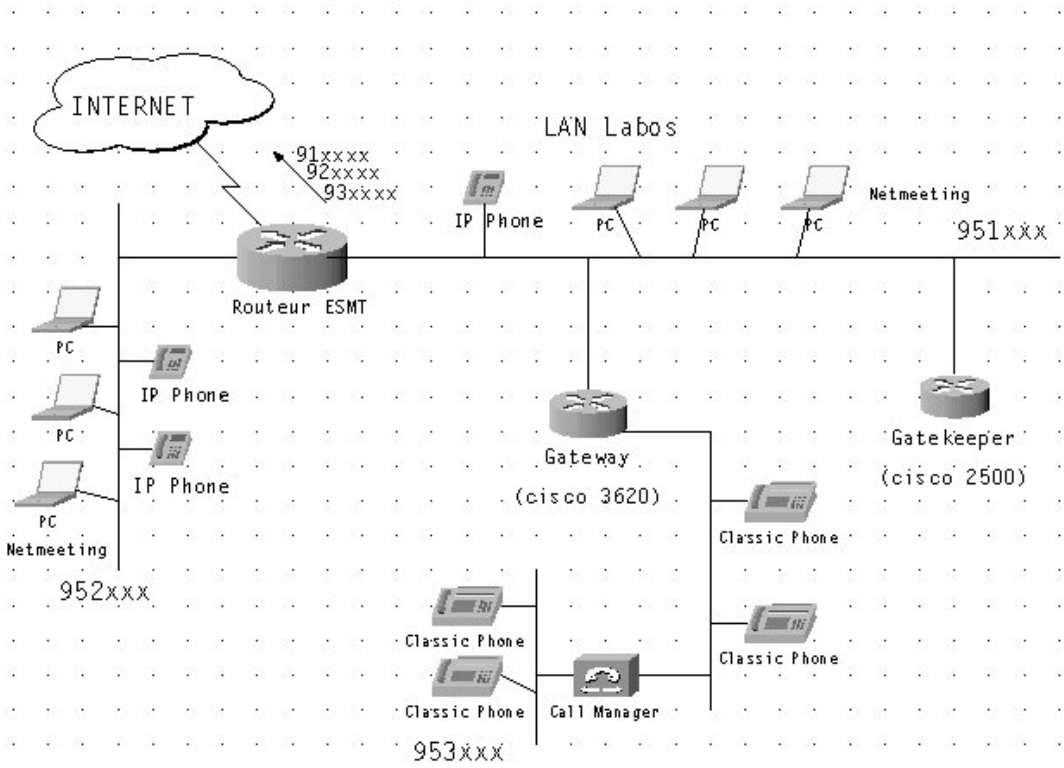

Figure 5 : *Schema du réseau VOIP à l'ESMT*

2.1 La gateway

L'organe vital lorsqu'on met en place un reseau de VOIP est la passerelle entre le reseau IP (caractérisé par son mode de commutation de paquets) et le reseau telephonique (caractérisé par son mode de commutation de circuits).
Pour l'ESMT, nous avons utilisé une gateway à base de routeur CISCO 3620 equipé de 64Mo de RAM et 16Mo de Flash pour stocker l'image IOS correspondant aux fonctions de passerelle VOIP(c3620-is-mz.122-8.T5).
La passerelle est connectée au reseau LAN via une (ou plusieures) interface(s) Fast-Ethernet (ou Ethernet). Les postes analogiques sont directement connectés à la passerelle via une carte FXS placée dans l'un des deux emplacement du module VOIX (le CISCO 3620 comporte deux baies pour des modules, un routeur 3660 à 6 modules pourra connecter un maximum de 20 postes analogiques). Pour plus de postes, on utilise une carte FXO connectée a un PABX traditionnel.

La configuration du routeur est simple :

```
!---- configuration d'une interface LAN ----
Interface FastEthernet0/0
  ip address 213.154.80.154 255.255.255.192
  h323-gateway voip interface
!
!---- Configuration d'un poste analogique tel=951315 ----
dial-peer voice 1 pots
  destination-pattern 951315
  port 1/1/0
!
!---- Configuration d'un autre poste sur une FXS ----
dial-peer voice 2 pots
  destination-pattern 951318
  port 1/1/1
!
```

2.2 Les terminaux

Nous avons vu comment connecter des postes analogiques sur la passerelle à l'aide de cartes FXS. L'avantage de la VOIP est la possibilité d'utiliser aussi des logiciels H323 installés sur des PC. Le plus facile d'accès est sans doute le Netmeeting. La configuration se fait au niveau de chaque poste pour indiquer : le numéro d'appel, l'adresse de la passerelle, éventuellement aussi l'adresse du gatekeeper.

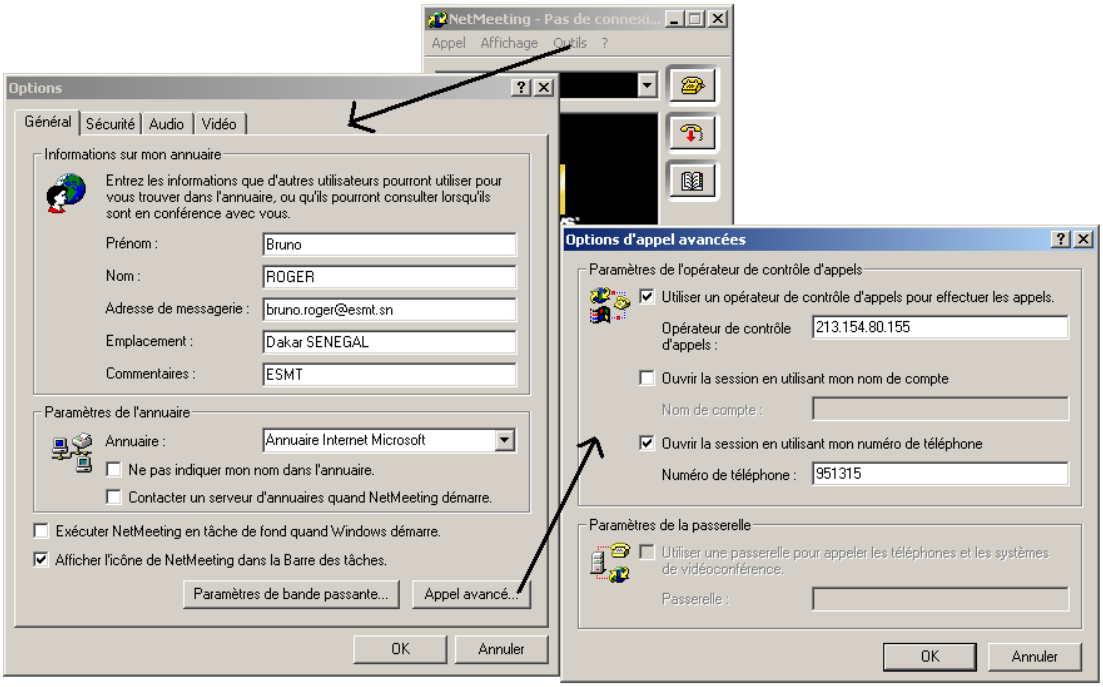

Figure 6 : *Options d'appel de Netmeeting*

A noter que si le gatekeeper n'est pas nécessaire pour appeler à partir d'un poste Netmeeting, il devient indispensable lorsqu'on a aussi besoin de se faire appeler sur son poste Netmeeting.

2.3 Le Gatekeeper

Le rôle du garde barrière est de recenser l'ensemble des terminaux de VOIP et de mettre en place le plan d'acheminement adéquat. Il assure en particulier que deux terminaux n'ont pas le même numéro de téléphone, et met aussi en œuvre des fonctions avancées comme l'accès sécurisé ou le comptage des appels.
Pour l'ESMT, nous avons utilisé un routeur CISCO 25xx avec 16Mo de RAM sans Flash (l'IOS c2500-ix-l.122-10b est chargée par TFTP). Il n'a besoin que d'une seule interface Ethernet (ou FastEthernet) connectée au LAN. Il met en œuvre les protocoles de gestion des appels de la famille H323.

Les éléments de configuration nécessaires sont les suivants :

```
!---- Configuration de l'interface LAN ----
Interface Ethernet0
  Ip address 213.154.80.155 255.255.255.192
!
!---- Configuration du plan d'acheminement 950xxx vers la GWn°1 ----
!---- Attention au nombre de points : 951… = 951+3chiffres
gatekeeper zone local gk-esmt.esmt.sn esmt.sn 213.154.80.155
```

```
 zone prefix gk-esmt.esmt.sn 951… gw-priority 10 gw1-esmt
 gw-type-prefix 1#* default-technology
 no shutdown
!
```

Il faut aussi modifier la configuration de chaque gateway pour lui indiquer de s'enregistrer auprès du Gatekeeper:

```
!---- enregistrement du GW1 aupres du GK ----
Interface FastEthernet0/0
 ip address 213.154.80.154 255.255.255.192
 h323-gateway voip interface
 h323-gateway voip id gk-esmt.esmt.sn ipaddr 213.154.80.155 1718
 h323-gateway voip h323-id gw1-esmt
 h323-gateway voip tech-prefix 1#
!
!---- Le reste ne change pas ----
```

On peut vérifier sur le gatekeeper que la ou les gateways sont bien enregistrées à l'aide de la commande « **show gateway** » et pour connaître tous les terminaux enregistrée (analogiques ou Netmeeting) on peut utiliser la commande « **show gatekeeper endpoint** » toujours sur le gatekeeper.

2.4 Le plan de numérotation

Comme on peut le voir, ne pas utiliser de Gatekeeper revient à peut près à utiliser le routage statique dans un LAN au lieu d'utiliser les protocoles de routages tels que RIP ou OSPF.
Avec un organe central pour gérer le plan d'acheminement, il faut donc planifier correctement le préfixe et le numéro de chacun des postes du réseau.
Pour notre réseau nous utilisons le préfixe 951 suivi de trois chiffres pour les postes (analogiques ou Netmeeting) connectés à la gateway située dans le segment des labos. Si nous avons besoin d'une autre gateway, on utilisera le préfixe 952xxx pour un autre segment de reseau ou pour la connection au PABX. On ajoutera alors dans la configuration du gatekeeper :

```
zone prefix gk-esmt.esmt.sn 952… gw-priority 10 gw2-esmt
```

Pour un réseau privé, un seul gatekeeper suffit, même s'il y a plusieurs gateways. En revanche, s'il faut interconnecter le réseau de VOIP a un autre réseau du même genre, il faudra déclarer le gatekeeper du réseau voisin afin que les deux s'échangent leurs tables d'acheminement. Par exemple, si RENATER utilise le préfixe 94xxxx, on ajoutera alors dans la configuration de notre gatekeeper :

```
zone remote gk-renater.renater.fr renater.fr 157.159.10.10 1719
zone prefix gk-renater.renater.fr 91….
```

Le tableau suivant résume le plan d'acheminement local et extérieur :

Préfixe	Suffixe	Signification	Exemple
95	4 chiffres	ESMT	
951	Numéro de poste à 3 chiffres	Poste IP des labos	951315 ou 95-13-15
952	Numéro de poste à 3 chiffres	Poste sur le PABX	952301 ou 95-23-01
953	Numéro de poste à 3 chiffres	Poste des étudiants	953002 ou 95-30-02
91	3 chiffres	RENATER	91 132
92	4 chiffres	CINES	92 1463
93	3 chiffres	CRIHAN	93 888

Tableau 7 : *plan de numérotation privé*

3 L'interconnexion de réseaux VOIP

3.1 Les problèmes inhérents au transport de la voix sur les réseaux IP

La qualité de la voix comparée à celle de la vidéo est plus exigée par les utilisateurs. En effet la qualité du son, dans notre vie quotidienne ne cesse d'augmenter passant du fm stéréo au hi-fi etc. Tout service doit alors garantir une **intelligibilité** et une **interactivité** acceptable. Pour arriver à ce niveau de qualité il est nécessaire d'analyser les problèmes rencontrés sur le réseau de transport (IP dans notre cas) et sur les équipements terminaux.

Le réseau IP, à la base n'était pas conçu pour les applications temps réels. Transporter la voix sur ces réseaux engendre alors des défauts de transmission que sont principalement le délai, la gigue, les pertes de paquets et l'écho.

Le délai : C'est le temps de transmission d'un bout (de l'émetteur) à l'autre(au récepteur) des paquets transportant la voix. Pour garantir une conversation orale active, ce temps de transit sur le réseau ne doit excéder les 150ms. Il comprend le délai réseau (retard engendré par la propagation sur le support, la commutation et le séjour dans les files d'attente des routeurs, au séjour dans les tampons de compensation de gigue etc.) et des terminaux (temps de numérisation, de codage, de compression, de mise en paquet, de transmission, de décompression, de conversion numérique analogique, etc.)

Délai (de l'émetteur au récepteur)	Difficulté de communication
200ms	28%
450ms	35%
700ms	46%

Tableau 8: *difficulté de communication selon le délai*

La gigue : Cette variation de délai entre le temps de réception prévu et le temps de réception réel du paquet cause une discontinuité dans le flux de données. Elle est importante sur les réseaux qui utilisent UDP protocole de couche transport (cas de la VOIP), la charge des nœuds intermédiaires qui diffèrent selon le chemin suivi par le paquet etc. Elle doit être inférieure à 100ms pour une bonne qualité.

Les pertes de paquets : Fait partie du concept même d'IP et est dû à la destruction volontaire de certains paquets afin d'éviter une congestion, à un TTL nul, à un tampon remplis sur un nœud intermédiaire etc. Le taux de perte doit être inférieur à 20% pour avoir une bonne qualité.

L'écho : dû au tronçon analogique dans la chaîne de transmission des paquets. Il est propre aux communications PC à téléphone, téléphone à pc ou téléphone à téléphone. Il ne doit pas être supérieur à 50ms.

3.2 Quelques solutions envisageables et les protocoles associés

Ces solutions apportent une qualité de service soit sur le réseau IP soit sur les terminaux VOIP. Dans certains cas, il est nécessaire de les combiner.

Ipv6(réseau) : supporte en natif le support de la QoS. Dans son en-tête, le champ « classe de trafic » permet aux applications de marquer les paquets selon le flux. On pourrait ainsi mieux traiter le flux multimédia. Le champ identificateur de flux est un numéro unique indiquant la qualité de service à appliquer à un paquet comme le traitement temps réel accordé au flux multimédia. Il facilite le déploiement des fonctions de qualité de service. Il est adapté aux trafic temps réel de part sa conception.

RTP et RTCP(bout en bout) : se situent au niveau applicatif et permettent respectivement de transporter et de contrôler des flots de données qui ont des propriétés temps-réel sur des réseaux unicast et multicast sans garantir cependant ni les délai ni une fiabilité.

RSVP (réseau) : Il prend en charge la réservation des ressources sur un réseau IP. Combiné à RTP, il permet d'assurer la fiabilité et la QoS. Il « simule » une fonction du réseau X.25 utilisé en téléphonie classique à savoir l'établissement d'un chemin dédié pour le flot de données, ordonne les paquets, réserve les ressources nécessaire avant la transmission du flux multimédia. Cependant il n'est pas déployer sur les grands réseaux par tous les ISP (complexe à gérer selon eux) ce qui réduit son utilisation.

Diffserv (réseau) : Une alternative à RSVP qui exploite les champs ToS (Ipv4) et classe de trafic (Ipv6) pour donner une priorité aux paquets indiqués.

QOSPF (routage) : Apporte une QOS au routage en apportant une amélioration à OSPF. Il se fonde sur la stabilité du chemin.

MPLS (réseau) : Séparation du routage et de la commutation ce qui accélère le traitement des paquets au niveau des routeurs. Il associe les fonctionnalités « intelligentes » du routage aux performances de la commutation.

VPN : Apporte plus de la sécurité que la QoS. Le temps de latence est le principal inconvénient.

Compensation de perte (terminal) : L'interpolation des paquets manquants, la redondance des données, la redondance hybride sont quelques techniques pour améliorer la continuité sonore en compensant au mieux les pertes de paquets.

Choix du codec (terminal) : Le critère d'évaluation est un compromis entre le délai (à réduire au minimum) et l'optimisation de la bande passante. Une classification selon le MOS (Mean Opinion Score) est faite à la figure xxx (Tableau N : *Codec voix et débits*).

Compression (terminal) : Les en-têtes RTP.

Trafic shaping (pas d'élément pour l'instant)

3.3 L'interconnexion de réseau téléphoniques par tunnel ip-ip sur intranet/internet (ipv4/ipv6) avec du cisco

3.3.1 Mise en place d'un tunnel GRE entre deux sites :

```
!--- adresse IP de l'interface GRE Tunnel 0
interface Tunnel0
  ip address @vpn-esmt mask
  tunnel mode ip-ip
  !--- adresses des bouts (local et distant) du tunnel
  tunnel source Loopback0
  tunnel destination @ip-loopback-distant
!
```

3.3.2 Mise en place d'un tunnel Ipv6

```
!--- adresse IP de l'interface GRE Tunnel 0
interface Tunnel1
  ip address @vpn-esmt mask
  tunnel mode ipv6-ip
  !--- adresses des bouts (local et distant) du tunnel
  tunnel source Loopback0
  tunnel destination @ip-loopback-distant
!
```

3.4 La qualité de service

Sur les systèmes cisco, les principaux éléments qui gère la QoS pour la VOIP peuvent être répartis en trois catégories que sont la classification du trafic (Traffic classification and marking), la priorité sur les files d'attente (Queuing) et le (Network provisioning)

3.4.1 RSVP

La configuration du RSVP est la suivante :

```
!---activation du rsvp avec une bande passante
!-- maximum de 512Kbps et 64Kbps par requête
Router(config)# interface serial 0/0
Router(config-if)# ip rsvp bandwidth 512 64
Router(config-if)# fair-queue
Router(config-if)# exit

!--- demande de session rsvp pour chaque peer
!---
Router(config)# dial-peer voice 211 voip
Router(config-dial-peer)# req-qos controlled-load
Router(config)# dial-peer voice 212 voip
Router(config-dial-peer)# req-qos controlled-load
```

3.4.2 La compression des en-têtes RTP

```
!--- active la compression des en-êtes rtp
ip rtp header-compression
ip rtp compression-connections 25
```

3.4.3 DiffServ

Défini par l'IETF dans le RFC-2475 ce procédé est utilisé pour définir des classes de trafic qui seront gérées de manière différents. Ainsi, le trafic sensible au délai (ex : la voix, la vidéo) sera acheminé en priorité, le trafic important (VPN, e-business) sera acheminé sur des liaisons redondantes, et le trafic normal (e-mail, web) sera acheminé là ou il reste de la bande passante disponible.
L'architecture de Diffserv comporte deux élémets importants :

- les nœuds de bordure : ils définissent les classes de trafic et marquent les paquets en conséquence (dans le champ TOS pour IPv4 ou dans l'octer Traffic Class pour IPv6).
- Les nœuds de cœur : ils sont capable de gérer les paquets en fonction de la qualité de service demandée et suivant des règles définies par un administrateur. Chaque classe de trafic possède sa propre file d'attente dans ces nœuds de cœurs et le routage tient compte du type de paquet. Ainsi, non seulement les paquets de voix seront traités en priorité, mais ils pourront éventuellement aussi emprunter un autre chemin que les paquets classiques.

3.4.4 Traffic shaping

En complément des files d'attentes avancées, la mise en place de quotas de bande passante permet également de garantir une certaine qualité de service dans notre réseau voix/données. Ainsi, la technique de traffic shaping consiste à limiter la bande passante allouée à un type de trafic donné (en réalité il suffit de limité la longueur de la file d'attente et de refuser d'acheminer les paquets en trop).
Pour notre réseau VOIP, si la liaison de sortie est de 2Mb/s nous pouvons par exemple définir que le trafic voix dispose d'une réserve de 256Kb/s (environ 6 à 8 communications simultanées) , le trafic vidéo dispose de 1Mb/s, et le reste du trafic (web, e-mail, ftp, etc.) ne doit pas dépasser 512Kb/s (les 256Kb/s restant pour faire 2Mb/s sont laissé pour la signalisation ICMP, les protocoles de routage, et l'encapsulation éventuelle).
Avec cette politique, on peut garantir que la charge du trafic vidéo ou la charge du trafic données n'aura pas d'influence sur le trafic voix. Evidement, pour que cette politique soit complètement efficace, elle doit être garantie d'un bout a l'autre de la chaîne de routage.

4 AAA (Autorisation, Athentication, Accounting)

Dans cette partie , il sera question de la mise en œuvre de la sécurité au sein du réseau VoIP. En effet, l'Authentification est un besoin bien défini aujourd'hui. Mais en parallèle de cette authentification vient s'ajouter l'Autorisation. En fin, la notion d'Accounting peut se rajouter aux deux précédentes . Ce sont les AAA .
Avant de passer à la phase pratique, voyons ce que sont ces trois A.

Les AAA présentent un certain nombre d'avantages :

- Augmentation de la flexibilité et du contrôle d'accès de la configuration
- Evolutivité
- Méthodes d'authentification standardisé : RADIUS, TACACS + et c..
- Plusieurs systèmes de Sauvegarde

Les serveurs d'authentification tels que Cisco Secure Access Control Server proposent ces trois AAA. Ils sont basés sur des protocoles d'authentification tels que TACAS+ ou RADIUS.Il sera question dans cette partie seulement d'authentification basée sur le Protocole RADIUS.

4.1 Authentication (Authentification)

Cela correspond à l'identification de l'utilisateur , que ce soit une personne physique ou un service. Cette identification passe par la présentation de l'identité de l'utilisateur. Cette information est unique à chaque utilisateur et non sécrète. Elle sert de référence dans la base des utilisateurs.
Le contrôle de cette information consiste à vérifier un secret partagé entre l'utilisateur et le serveur. Elle peut être de plusieurs types :

- statique : l'information transmise est alors la même lors d'authentifications successives : mot de passe type UNIX par exemple.
- Dynamique : on passe alors par un challenge entre le serveur et l'utilisateur, ce qui permet d'avoir une information différente à chaque nouvelle authentification : calculette, carte à puce …
- Physique : reconnaissance vocale, empreintes

4.2 Autorization (Autorisation)

C'est le fait de déterminer quels sont les droits de l'utilisateur. Par exemple, après s'être loggé, l'utilisateur peut essayer certaines commandes. L'autorisation détermine si l'utilisateur peut ou non les utiliser. Dans certaines implémentations, l'identification et l'autorisation sont regroupées en une seule étape.

4.3 Accounting (Rapports)

Cela consiste à mesurer les ressources qu'un utilisateur consomme, en terme d'échange réseau, de ressources système,… Cela sert en fait à logger un certain nombre d'informations sur l'utilisateur . Cela permet de connaître à la fois les services demandés par l'utilisateur et la quantité de ressources requises. Ces informations peuvent être souvent utilisées dans les buts de facturation.

4.4 Le protocole RADIUS (Remote Access Dial-In User Service)

Le protocole RADIUS a été créé par Livingston et normalisé par l'IETF (Internet Engineering Task Force) sous la forme de RFC (Request for Comments). Actuellement, il s'agit des RFC 2138 & 2139.

Tous les clients RADIUS communiquent généralement à travers le réseau local sur un serveur unique, ce qui rend la tâche de l'administrateur plus simple. La gestion des utilisateurs et de leurs droits est alors plus facile par rapport à plusieurs serveurs qu'il faudrait mettre à jour simultanément sur le réseau.

Le standard RADIUS est basé sur un ensemble d'attributs relatifs aux utilisateurs. Ils sont stockées dans la base de données RADIUS du serveur. Au cours d'une connexion, un échange d'informations a lieu entre le serveur et le client . Le standard RADIUS propose un certain nombre d'attributs qui doivent être mis en œuvre . Mais beaucoup d'implémentations spécifiques du protocole apportent leur propre jeu d'attributs.

Quelques caractéristiques de RADIUS

Protocole	UDP : port 1645 (1812 normalement)
Chiffrement	Chiffrement du mot de passe
Architecture	Autorisation liée à l'authentification
Emission du profile	Profil global envoyé au NAS lors de la fin de l'authentification
Protocoles supportés	Pas ARA ni de NetBEUI
Challenge/Reponse	Unidirectionnel

4.5 Configuration des AAA au niveau de la Gateway

Pour que le Gateway assure les services d'authentification et accounting, nous devons activer et configurer notre Gateway pour qu'il supporte les services :authentifiaction , autorisation et accounting (AAA). Le service AAA permet au Gateway d'interagir avec un serveur RADIUS pour identifier les utilisateurs (les appels entrants) et assurer les rapports (accounting).

a) Pour configurer les Services RADIUS authentication et accounting, nous procédons comme suit :

```
3600 (config)# aaa new-model
3600 (config)# gw-accounting h323
3600 (config)# aaa authentication login  AhmedBrunoKaderOumar  radius
3600(config)# aaa accounting connection  AhmedBrunoKaderOumar  start-stop radius
3600(config)#radius-server host (@ ip du serveur) auth-port (number)  acct-port  ( number)
3600(config)#radius-server key  esmt
```

b) Configuration de l'authorisation (Authorization)

```
3600 (config)#aaa authorization exec AhmedBrunoKaderOumar group radius if-authenticated
3600 (config)#aaa authorization network AhmedBrunoKaderOumar group radius
```

c) Application aux lignes ou aux interfaces

```
3600 (config)#interface fasethernet 0/0 ou 0/1
3600 (config-if)#login authentication AhmedBrunoKaderOumar
3600 (config-if)#ppp authorization AhmedBrunoKaderOumar
3600 (config-if)#ppp accounting  AhmedBrunoKaderOumar
```

5 Conclusion

Comme on peut le voir en arrivant a la fin de ce document, la mise en place d'un réseau de voix dans un réseau IP existant est tout a fait possible avec quelques équipements minimums. La première étape est d'installer une Gateway dans le LAN et quelques terminaux (analogique, IP phone, ou Netmeeting), puis de mettre en place des tunnels performants pour interconnecter plusieurs réseaux. Pour plus de souplesse, on pourra utiliser un Gatekeeper (un seul suffit pour un système autonome donné) pour gérer le plan de numérotation et pour échanger ce plan avec d'autres gatekeepers dans d'autres réseaux VOIP. Enfin, la sécurité et le comptage des appels peut être mise en place a l'aide d'un serveur proposant les trois AAA (TACACS+ ou RADIUS).
Mais la mise en place d'un réseau de VOIP n'est pas seulement faisable pour le plaisir de la chose, c'est avant tout pour nous une nécessité économique dans la mesure ou les communications internationales (en particulier entre pays Africains très faiblement interconnectés) sont hors de prix. L'utilisation d'Internet pour transporter la voix va diminuer grandement le montant de notre facture téléphonique sans pour autant augmenter celui de notre liaison Internet.

Références

[1] CISCO Systems, BASIC Two Zone Gateway-Gatekeeper Configuration (ID=21063), Janvier 2003.
[2] Technologies des Interconnexions Réseaux, CISCO Press, Aout 2001.
[3] CISCO IOS Security Configuration Guides.
[4] CISCO IOS Multiservice Application Configuration Guide
[5] H323 Compliant Gateway and Gatekeeper Configuration Task List
[6] http://www.highsecu.net
[7] Déploiement d'un réseau VOIP dans un établissement, Guy BISIAUX – Bernard RAPPACCHI, JRES2001