15

La téléphonie et la vidéo sur IP

On entend souvent la conversation suivante entre un sceptique et un convaincu à propos de la téléphonie sur IP :

— Est-ce que ça marche ?

— Oui.

— Mais, est-ce que ça marche *bien* ? Est-ce que la qualité de service est bonne ?

La réponse est : oui, ça marche, et même très bien !

Maintenant que vous avez préparé votre réseau au multimédia, vous pouvez, en effet, mettre en place des solutions de téléphonie et de visioconférence.

Dans ce chapitre, vous apprendrez ainsi :

- à interconnecter des PABX *via* IP ;
- à raccorder un VoIP au réseau téléphonique classique ;
- le fonctionnement des protocoles multimédias.

Les protocoles H.323 de l'ITU-T sont ici expliqués dans le détail, car tous les produits du marché reposent sur cette norme. Mais, à l'avenir, cette dernière pourrait être remplacée par son concurrent SIP (*Session Initiation Protocol* — RFC 2543) promu par l'IETF. Les deux normes pourraient éventuellement cohabiter, SIP se posant en interface applicative, donc de plus haut niveau que H.323.

Présentation des protocoles multimédias

Historiquement le premier, le RTC (réseau téléphonique commuté) est le réseau qu'utilise toujours notre bon vieux téléphone. La version numérique de celui-ci, le RNIS (réseau numérique à intégration de service), est venue s'ajouter par la suite.

L'évolution des technologies a ensuite permis d'envisager d'autres supports pour transporter la voix : ATM, Frame Relay et, aujourd'hui, les réseaux IP (votre intranet et l'Internet). Toujours grâce à l'évolution des technologies, il est ensuite devenu possible d'y ajouter l'image, la vidéo et le partage de données.

Accompagnant le mouvement, les normes H.32x de l'ITU-T (*International Telecommunication Union — Telecommunication Standardization Sector*), sur lesquelles reposent le RTC et le RNIS, ont été adaptées à ces nouveaux supports de transmission et aux nouveaux besoins multimédias. Cette continuité dans la standardisation des protocoles téléphoniques permet ainsi d'assurer une cohabitation et une transition en douceur.

Réseau	Caractéristiques du réseau	Norme ITU-T
RNIS (réseau numérique à intégration de service)	Commutation de circuit Voix numérique	H.320
ATM (*Asynchronous Transfer Mode*)	Commutation de cellules Voix numérique	H.321
Réseaux WAN avec qualité de service	Frame Relay Voix numérique	H.322
Réseau VoIP (*Voice over Internet Protocols*)	Commutation de paquets IP Voix numérique	H.323
RTC (Réseau Téléphonique Commuté)	Commutation de circuit Voix analogique	H.324

Ces normes décrivent un cadre général de fonctionnement et préconisent l'utilisation d'autres normes de l'ITU-T et de l'IETF (*Internet Engineering Task Force*) en fonction du support de transmission (IP, RTC, RNIS, etc.). Elles décrivent les codages audio et vidéo, l'adaptation au support de transmission, la signalisation, etc.

	H.320	H.321	H.322	H.323	H.324
Réseau	RNIS	ATM	WAN QoS	VoIP	RTC
Codec vidéo	H.261 H.263	H.261 H.263	H.261 H.263	H.261 H.263	H.261 H.263
Codec audio	G.711 G.722 G.728	G.711 G.722 G.728	G.711 G.722 G.728	G.711 G.722 G.728 G.723 G.729	G.723
Adaptation	H.221	H.222	H.221	H.225	H.223
Signalisation	H.242 H.230	H.242	H.242 H.230	H.245 H.225	H.245
Conférences multipoints	H.231 H.243	H.231 H.243	H.231 H.243	H.323	
Données	T.120	T.120	T.120	T.120	
Couche de transport	I.400	I.363 AAL	I.400	TCP/IP	Fils

Ainsi, la norme **H.323** décrit un cadre général de fonctionnement pour un terminal multimédia fonctionnant sur IP. Elle implique l'utilisation d'autres normes décrites, cette fois-ci, par des RFC (*Request For Comments*) de l'IETF. Il s'agit notamment de **RTP** (*Real-time Transport Protocol*) qui décrit le format d'un paquet transportant des données (un échantillon sonore, une portion d'un écran vidéo, etc.).

Les composants d'un système H.323

La norme H.323 décrit le fonctionnement et l'interaction de quatre entités :

- un **terminal** qui supporte la voix et, optionnellement la vidéo et les données ;
- une **passerelle** qui permet l'interconnexion avec les autres réseaux H.32x tels que le RTC ;
- un **serveur de conférence**, appelé MCU (*Multipoint Control Units*) ;
- un PABX IP, appelé **gatekeeper**, qui offre le routage, la conversion d'adresses ainsi que la coordination de l'activité de toutes les entités H.323.

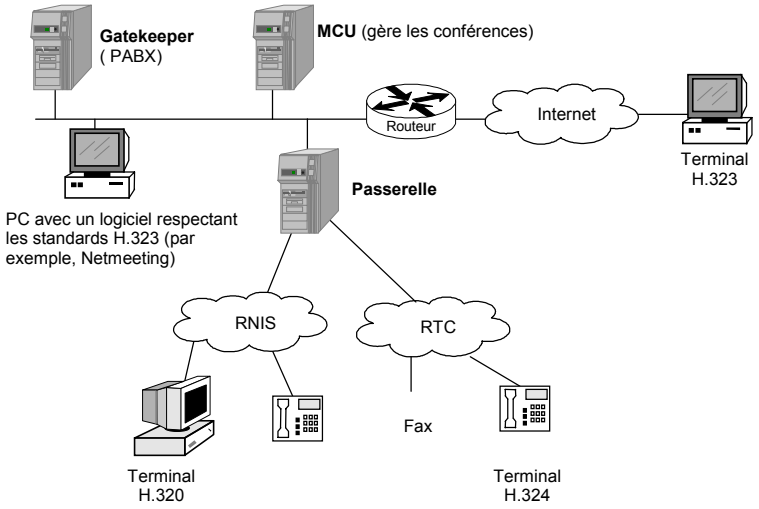


Figure 15-1.
Entités décrites par la norme H.323.

La **passerelle** permet d'interconnecter le réseau téléphonique IP à d'autres réseaux tels que le RTC ou le RNIS. Elle assure la conversion des codecs audio et vidéo, de la signalisation et du support de transmission.

Le **MCU** contrôle l'entrée et la sortie des participants à la conférence, rediffuse le flux entre émetteurs et récepteurs en minimisant le trafic réseau, et assure l'éventuelle conversion de codec (par exemple, si un participant est équipé d'un écran de moins bonne qualité que les autres). Même si son utilisation n'est pas nécessaire lorsque les terminaux disposent des fonctions multicast et de négociation de paramètres, un MCU permet cependant de décharger le terminal de certaines fonctions.

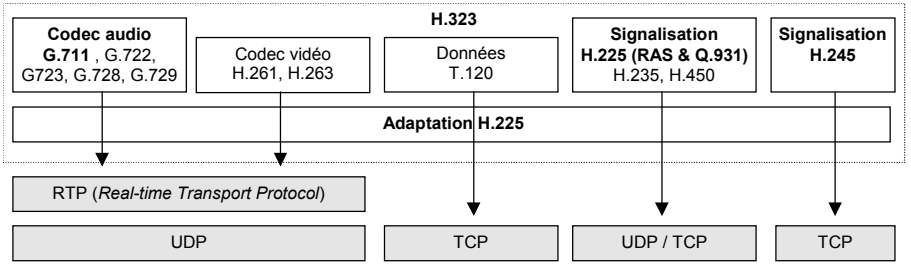
Le **gatekeeper** gère des services pour les entités de sa **zone** de couverture, tels que :

- la gestion des tables de correspondance entre les noms des terminaux (le nom de la personne), un numéro de téléphone E.164, une adresse e-mail et les adresses IP ;
- le contrôle d'admission : autorisation ou non de l'ouverture d'une communication ;
- la gestion de la bande passante sur le réseau, le nombre maximal de conférences, d'utilisateurs, etc. ;
- la localisation des passerelles et des MCU ;
- le routage des appels au sein de la zone et entre les zones.

Le **terminal**, enfin, se présente sous des formes diverses. Il peut prendre l'aspect d'un téléphone classique équipé d'une interface Ethernet dont la prise RJ45 est connectée à un commutateur de notre réseau local. Il peut également être un PC doté d'un logiciel de communication tel que Netmeeting de Microsoft. Le terminal intègre alors l'image, en plus de la voix, ce qui permet aux utilisateurs d'établir des visioconférences directement entre eux. Le PC devient ainsi un terminal multimédia traitant la voix, les données et l'image.

Le schéma suivant précise ce que la norme H.323 couvre (carrés blancs) et les éléments obligatoires (en gras). Les éléments grisés correspondent aux protocoles spécifiés par les RFC sur lesquels s'appuie la norme H.323 pour transporter les informations sur un réseau IP.

Figure 15-2.
Protocoles utilisés par la norme H.323.



La norme H.235 recouvre les fonctions de sécurité (authentification, intégrité des données, chiffrement, etc.). La norme H.450 décrit, quant à elle, les services complémentaires (identification de l'appelant, transfert d'appel, rappel sur occupation, etc.).

Selon ce schéma, un terminal H.323 doit donc comprendre :

- un codec audio (au moins G.711) ;
- optionnellement, un codec vidéo (au moins H.261) ;
- optionnellement, l'échange des données (à la norme T.120) ;
- les protocoles de signalisation RAS, Q.931 et H.245 ;
- une couche H.225 qui assure l'adaptation des protocoles de l'ITU à ceux de l'IETF ;
- les protocoles TCP, IP, UDP et RTP.

Par ailleurs, une entité H.323 comprend deux composants fonctionnels :

- un **MC** (*Multipoint Controler*) pour négocier, *via* H.245, les niveaux de service entre les terminaux et les ressources utilisées au sein d'une conférence (canaux audio et vidéo, adresses multicast, etc.) ;
- optionnellement, un **MP** (*Multipoint Processor*) pour traiter les flux multimédias (mixage, synchronisation de la parole et des images, diffusion, chiffrement, etc.).

En pratique, toutes les entités H.323 intègrent un MC pour participer à des conférences, tandis qu'un MCU intègre les deux composants pour gérer lesdites conférences.

L'établissement d'une communication

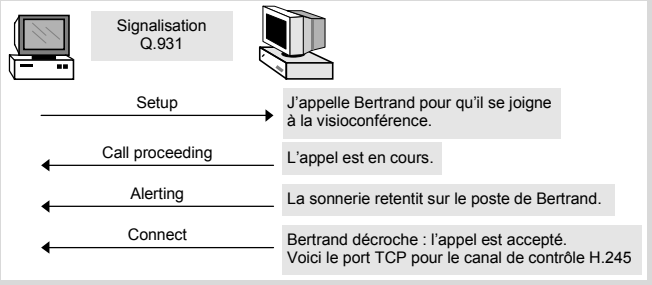
Pour communiquer entre elles, les entités H.323 ouvrent des canaux logiques (sessions TCP, UDP et RTP) soit dédiés à la signalisation, soit dédiés au transport des flux multimédias. On trouve, dans l'ordre :

- un canal de **signalisation RAS** (*Registration, Admission and Status*) qui permet à un terminal de s'enregistrer auprès du gatekeeper de sa zone ;
- un canal de **signalisation d'appel Q.931** (numérotation, sonnerie, etc.) qui permet à un terminal d'en appeler un autre ;
- un canal de **contrôle H.245** qui permet d'échanger les fonctionnalités supportées par les entités (codecs audio et vidéo, T.120) ainsi que d'ouvrir et de fermer les canaux audio, vidéo et données ;
- les canaux audio, vidéo et données.

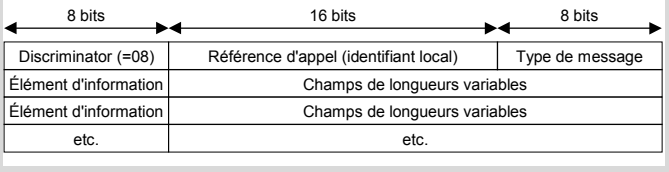
L'utilisation des services d'un gatekeeper, et donc l'ouverture d'un canal RAS, est optionnelle. Les entités H.323 peuvent, en effet, communiquer directement entre elles.

LA SIGNALISATION D'APPEL Q.931

Une entité désirant en appeler une autre doit ouvrir un canal de signalisation d'appel Q.931 (dont l'utilisation au sein de H.323 est décrite par la norme H.225). Il s'agit d'une connexion sur le port TCP 1720 qui véhicule des messages Q.931.



Un message Q.931 comporte un en-tête, suivi d'un certain nombre d'éléments d'information obligatoires ou non. Par exemple, le message " Connect " contient, en plus de l'en-tête, les éléments d'information suivants : " Bearer capability ", " Connect-UUIE ", et optionnellement " Progresss indicator ", " Notification Indicator ", " Facility ", etc.



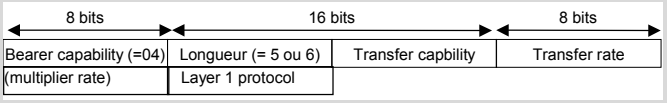
• • •

LA SIGNALISATION D'APPEL Q.931 (SUITE)

La signification des champs de l'en-tête Q.931 est la suivante :

- " Type de message " : 1 = Alerting, 2 = Call proceeding, 5 = Setup, 7 = Connect, etc.
- " Éléments d'information " : 4 = Bearer capability, 204 = numéro de téléphone de l'appelant, 224 = numéro de téléphone à appeler, 130 = temps de transit, etc.

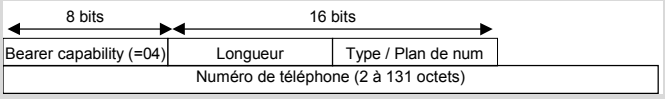
Par exemple, le format de l'élément d'information " Bearer Capability " est le suivant :



La signification des champs est la suivante :

- " Transfer capability " indique les fonctionnalités du terminal (audio, vidéo).
- " Transfer rate " indique le débit (mode paquet ou circuit, de 64 Kbit/s à 1 920 Kbit/s).
- " Multiplier rate " est uniquement présent si le champ précédent indique un débit " multirate ".
- " Layer 1 protocol " : G711 (A-law ou μ-law) ou H.225/H.245 (vidéophone H.323).

Voici un autre exemple montrant le format de l'élément d'information " **Called Number** " :



La signification des champs est la suivante :

- Type de numéro (3 bits) : 1 = international, 2 = national.
- Plan de numérotation (5 bits) : 1 = E.164, 8 = national, 9 = privé.
- Numéro de téléphone : par exemple 1#331836 ou 440553.

L'exemple suivant montre l'élément d'information utilisateur **Connect-UUIE** (*User-to-User Information Element*) pour le message " Connect " décrit selon la syntaxe ASN.1 (qui est utilisée dans toutes les normes de l'ITU-T) :

h323-message-body connect :{

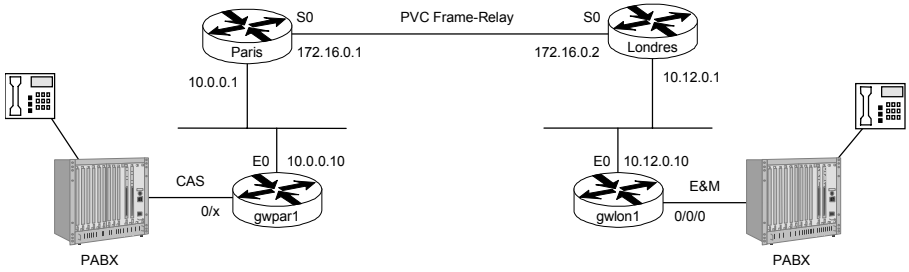
protocolIdentifier	{ 0 0 8 2250 0 3 },
h245Address	ipAddress : { ip '**0A0C0006**'h port 011026 } ,
destinationInfo	{ terminal { }, mc FALSE, undefinedNode FALSE },
conferenceID	5A 1E 55 55 8A B0 CF 72 00 00 00 00 17 00 86 B4,
callIdentifier	CallIdentifier,
h245SecurityMode	H245Security (champ optionnel),
tokens	Sequence of ClearToken (champ optionnel),
cryptoTokens	Sequence of CryptoH323Token (champ optionnel),
fastStart	Sequence of octet string (champ optionnel) }

Interconnecter les PABX *via* IP

Lors de l'introduction d'une nouvelle technologie, la première contrainte est bien souvent de prendre en compte l'existant, en l'occurrence les PABX de l'entreprise.

Dans notre exemple, nous souhaitons profiter de notre réseau WAN pour acheminer les appels internes entre deux sites sur notre réseau privé (on Net), mais également pour passer des appels vers l'extérieur (off Net), de manière à bénéficier des meilleurs coûts (par exemple, Paris-Angleterre en sortant à Londres pour le coût d'un appel local ou national).

Figure 15-3.
Utilisation des passerelles pour interconnecter les PABX via IP.



Nous avons choisi des routeurs Cisco comme passerelles, mais cela aurait pu être des PC équipés de cartes de même nature que celles des routeurs.

La première tâche est de configurer les liaisons entre les passerelles et les PABX, ce qui est réalisé de la manière suivante :

Configuration d'une liaison numérique CAS entre le PABX parisien et la passerelle gwpar1

```
#gwpar1
controler E1 0
 framing crc4
 linecode ami
 mode cas
 voice-group 1 timeslot 1-6 e&m-immediate
voice port 0/1
voice port 0/2
voice port 0/3
...
```

6 canaux sont utilisés

```
#gwlon1
voice-port 0/0/0
signal immediate
 operation 4-wire
 type 2
voice-port 0/0/1
 signal immediate
 operation 4-wire
 type 2
```

Configuration de deux liaisons analogiques E&M entre le PABX londonien et la passerelle gwlon1

Nous n'entrerons pas dans les détails, car ce domaine dépasse le cadre de cet ouvrage. Il faudrait, en effet, expliquer le fonctionnement des signalisations utilisées par les PABX classiques.

L'étape suivante consiste à configurer les liaisons entre les deux passerelles. Il s'agit cette fois de transporter la voix sur IP à l'aide des protocoles H.323.

Les utilisateurs des postes téléphoniques connectés aux PABX manipulent des numéros de téléphone au format E.164 (voir chapitre 10). Il faut donc associer des préfixes (c'est-à-dire la partie située le plus à gauche du numéro de téléphone) à des interfaces PABX d'un côté et à des interfaces IP de l'autre.

Passerelle	Préfixe	Correspondant
gwpar1 port 0/1-3	33	Numéro sur quatre chiffres
gwlon1 port 0/0/0	44	Numéro sur quatre chiffres

Chez Cisco, la connexion PABX est référencée par l'acronyme POTS (*Plain Old Telephone Service*), et la connexion IP est appelée VoIP (*Voice over IP*). Une connexion au sens large est appelée " dial-peer ".

```
# gwpar1
dial-peer voice 33 pots
port 0/1
destination-pattern 33....

dial-peer voice 44 voip
destination pattern 44....
session-target ipv4:10.12.0.10
codec g729r8
```

Tous les numéros d'appels commençant par 33 sont envoyés sur cette interface.

Quatre points indiquent que quatre numéros doivent suivre le préfixe 33.

Tous les numéros d'appel commençant par 44 sont envoyés vers la passerelle de Londres en H.323.

Ce codec utilise 8 kbit/s de bande passante (cf. chapitre 11).

Sur la passerelle de Londres, nous devons disposer d'une configuration symétrique :

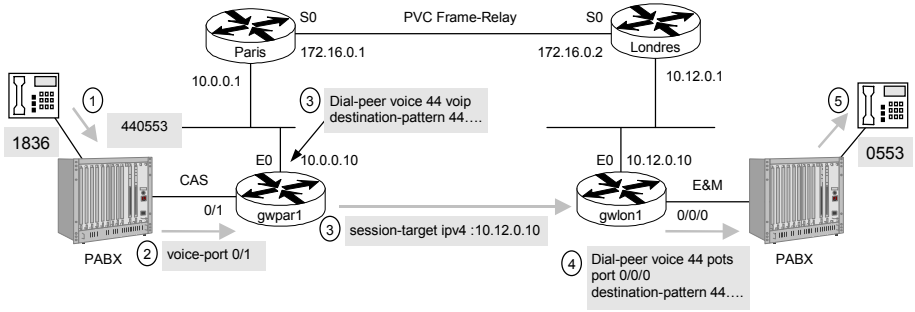
```
# gwlon1
dial-peer voice 44 pots
port 0/0/0
destination-pattern 44....

dial-peer voice 33 voip
destination pattern 33....
session-target ipv4:10.0.0.10
codec g729r8
```

Numéro arbitraire ayant uniquement une signification pour la passerelle locale. Nous avons choisi une notation mnémotechnique.

Active les protocoles H.323

Adresse IP de la passerelle parisienne.

Figure 15-4.
Établissement d'une communication VoIP via des passerelles.



Le correspondant de Paris compose le " 440553 ". Le PABX route ce numéro vers la liaison CAS établie avec la passerelle parisienne. Celle-ci compare le numéro à ses " dial-peer " et constate que le préfixe " 44 " correspond à une connexion H.323. Elle envoie alors la demande de connexion sur IP (signalisation Q.931) à la passerelle londonienne qui compare à son tour le numéro présenté à ses " dial-peer ". Celle-ci constate alors que le préfixe " 44 " correspond à un port physiquement connecté au PABX et y envoie le numéro. Le PABX déclenche la sonnerie du téléphone du correspondant recherché.

Nous souhaitons également acheminer des appels en off Net sans que les utilisateurs français changent leurs habitudes de numérotation : " 00 " pour l'international, " 44 " pour l'Angleterre, suivis de dix chiffres. De même, les utilisateurs anglais numérotent comme suit : " 00 " pour l'international, " 33 " pour la France, suivis de neuf chiffres. Il suffit de configurer autant de " dial-peer " qu'il y a de préfixes :

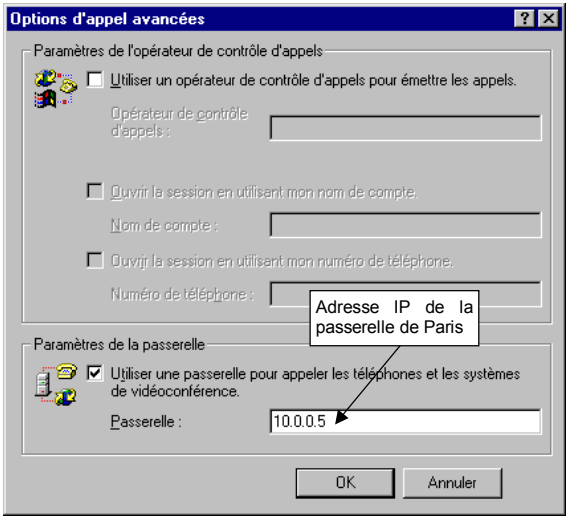
```
# gwpar1
dial-peer voice 0033 pots
port 0/4-6
destination-pattern 0033.........
dial-peer voice 0044 voip
destination pattern 0044..........
session-target ipv4:10.12.0.10
codec g729r8
```

Les neuf points correspondent aux neuf chiffres attendus.

Dix points = dix chiffres.

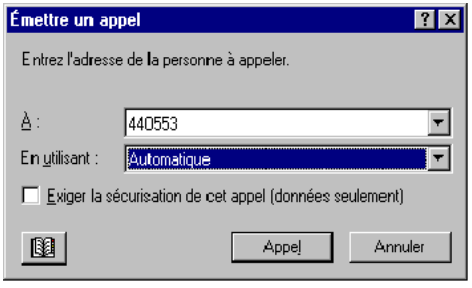
Un PC équipé de Netmeeting peut également profiter des services de nos passerelles pour appeler un correspondant situé sur le RTC classique. Il suffit d'indiquer son adresse IP dans le menu :

" Outil→Option→Appel Avancé ".



Il suffit ensuite de composer le numéro de téléphone de notre correspondant à Londres.

Nous utilisons ici la numérotation abrégée configurée dans nos passerelles.

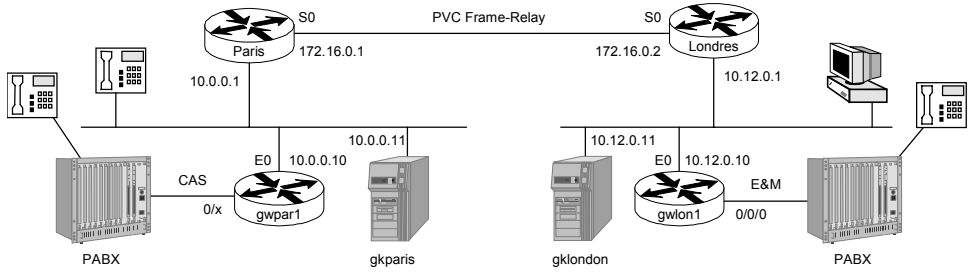


Mettre en place un gatekeeper

La complexité de notre installation augmente avec le nombre de sites à interconnecter. Nous devons de plus supporter des téléphones IP et des PC équipés de logiciels téléphoniques, tels que Netmeeting. Le réseau VoIP prenant de l'importance, nous devons assurer des services plus évolués, tels que le routage automatique, les statistiques ou encore la facturation. Nous devons donc assurer non seulement la reprise de l'existant mais également le développement de la voix tout IP.

La solution est de mettre en place un PABX IP, appelé **gatekeeper** dans la terminologie H.323. Nous choisissons donc d'en installer un par site, de marque Cisco (encore !), et reprenons les deux sites précédents comme exemple.

Figure 15-5.
Utilisation des gatekeepers.



Afin de simplifier les configurations et la vie des utilisateurs, nous choisissons également d'utiliser les services d'un DNS (*Domain Name System*) privé, dont nous avons déjà entrevu l'intérêt au chapitre 3 et dont la mise en œuvre est expliquée au chapitre 17. Le DNS permet de manipuler des noms à la place des adresses IP en assurant la résolution de l'un vers l'autre.

Dès lors, la configuration des gatekeepers est la suivante :

```
#gkparis
gatekeeper
zone local gkparis fr.intranet
zone prefix gklondon 44....
zone prefix gklondon 0044..........
gw-type-prefix 1# default-tech
```

Active H.323, la fonction de gatekeeper et la signalisation RAS.

Le gatekeeper gère les terminaux IP situés dans le domaine DNS indiqué.

Le gatekeeper route les appels préfixés 44 et 0044 vers Londres.

Le préfixe technique, indiqué par la commande " gw-type-prefix " — à ne pas confondre avec le préfixe de numérotation — permet de désigner explicitement les services d'une passerelle, par exemple une passerelle offrant le routage onNet, une autre le routage offNet, le

fax, etc. Par convention, le préfixe technique se termine par un dièse. Dans notre exemple, si aucun préfixe technique n'est indiqué dans le numéro appelé, l'appel sera routé vers la passerelle supportant le préfixe technique 1#.

Le gatekeeper de Londres est configuré de manière symétrique :

```
#gklondon
gatekeeper
zone local gklondon uk.intranet
zone prefix gkparis 33....
zone prefix gkparis 0033..........
gw-type-prefix 1# default-tech
```

Notre DNS privé est configuré avec un sous-domaine par pays, et nous installons un gatekeeper par zone.

Le préfixe technique par défaut est 1#.

Le routage des appels est désormais réalisé entre gatekeepers. Dans chacune des zones, les passerelles doivent par conséquent s'enregistrer auprès de leur gatekeeper de rattachement :

```
#gwpar1
gateway

int e0
h323-gateway voip interface

h323-gateway voip h323-id gwpar1@fr.intranet
h323-gateway voip id gkparis multicast
h323-gateway voip tech-prefix 1#
```

Active H.323 et la signalisation RAS.

Désigne explicitement l'interface Ethernet pour les fonctions H.323.

Nom de la passerelle dans la zone fr.intranet contrôlée par un gatekeeper

Recherche le gatekeeper gkparis à l'aide de la signalisation RAS dans sa version multicast.

À l'aide de ces commandes, la passerelle parisienne numéro 1 va rechercher le gatekeeper appelé " gkparis " et s'y enregistrer avec le préfixe technique 1# sous le nom " gwpar1 " dans la zone " fr.intranet ".

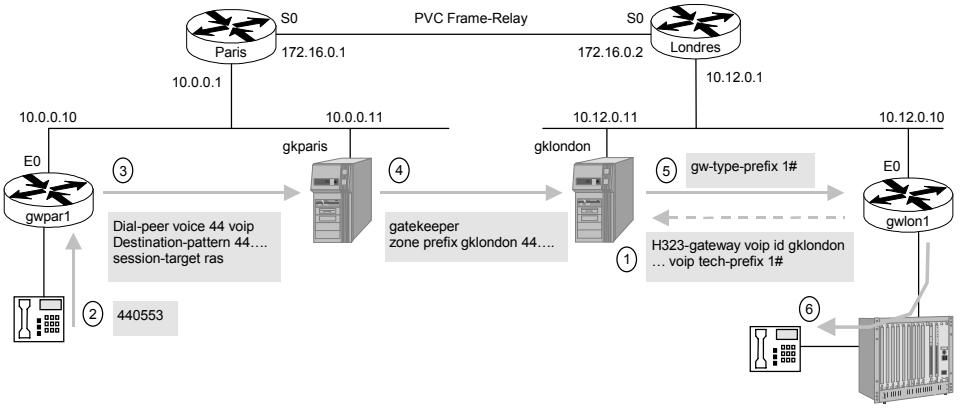
Toujours sur nos passerelles, la configuration des " dial-peer " change légèrement par rapport à une architecture sans gatekeeper :

```
dial-peer voice 44 voip
destination-pattern 44....
tech-prefix 1#
session-target ras
```

Optionnel : ajoute le préfixe 1# au numéro appelé, afin de désigner explicitement un groupe de passerelles.

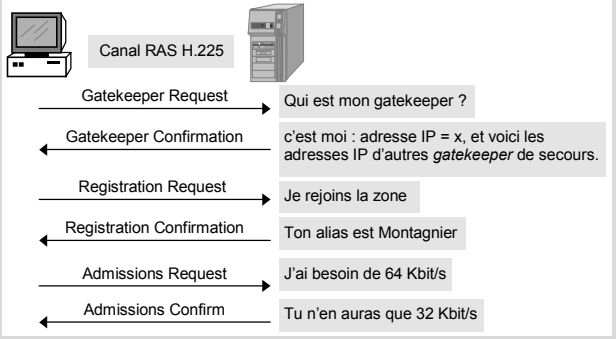
Utilise les services du gatekeeper qui lui donnera l'adresse IP de la passerelle de Londres.

Lorsque ce " dial-peer " sera invoqué, il enverra l'appel au gatekeeper, qui le routera conformément à la configuration précédente.



LE CANAL DE SIGNALISATION RAS (H.225)

La signalisation RAS (*Registration, Admission and Status*) permet à toutes les entités H.323 (un terminal, un MCU ou une passerelle) de communiquer avec un **gatekeeper** afin de bénéficier de ses services.
Les messages de **découverte** sont envoyés dans des paquets UDP, port 1718, soit à destination du gatekeeper s'il est connu (son adresse ayant été configurée manuellement), soit à destination du groupe multicast 224.0.1.41. Si plusieurs gatekeepers répondent, l'entité en choisit un.
L'étape suivante consiste à rejoindre la **zone** contrôlée par un gatekeeper en **s'enregistrant** auprès de ce dernier. Le canal RAS utilise maintenant des paquets UDP unicast, port 1719.



Désormais, l'entité H.323 s'adresse au gatekeeper pour appeler tous ses correspondants en les désignant par leur nom ou leur numéro de téléphone. Le gatekeeper se charge de convertir ce nom en une adresse IP, et de router l'appel :

- soit directement vers le correspondant si celui-ci se trouve dans la même zone ;
- soit vers un autre gatekeeper si le correspondant se trouve dans une autre zone ;
- soit vers une passerelle si le correspondant n'utilise pas un terminal IP (mais un téléphone, par exemple).

• • •

LE CANAL DE SIGNALISATION RAS (H.225 – SUITE)

Plusieurs types de messages peuvent être échangés : Découverte, Enregistrement/annulation, Admission (demande d'autorisation d'utiliser le réseau), Changement de bande passante (demandé par le terminal), Localisation (conversion d'adresses), Statut et Information sur les ressources disponibles (pour les passerelles). Ces types regroupent 18 messages différents.

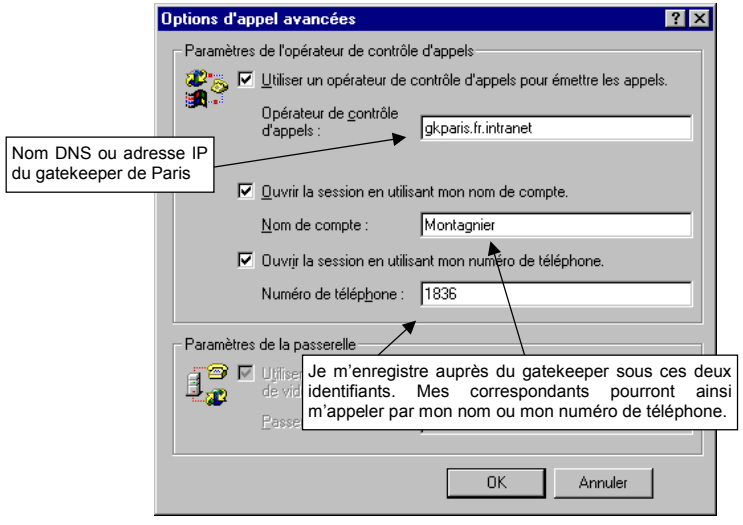
Voici, à titre d'exemple, le format, en syntaxe ASN.1, d'une demande d'enregistrement d'une passerelle auprès d'un gatekeeper :

```
RasMessage ::= registrationRequest : {
requestSeqNum 037001,
protocolIdentifier { 0 0 8 2250 0 3 },
discoveryComplete TRUE,
callSignalAddress { ipAddress : { ip 'A00C00A'h, port 01720 } },
rasAddress { ipAddress : { ip A0 0C 00 0A, port 04520 } },
terminalType { gateway { protocol { voice : { supportedPrefixes { { prefixe 164 :"1#" } } } } } }, mc FALSE, undefinedNode FALSE },
terminalAlias { h323-ID :"gwlon1.fr.intranet" },
gatekeeperIdentifier { "gklondon.fr.intranet" },
endpointVendor { vendor { t35CountryCode 0181, t35Extension 00, manufacturerCode 018 } } }
```

ITU-T, recommandation série H, 225.0, (0), version 3

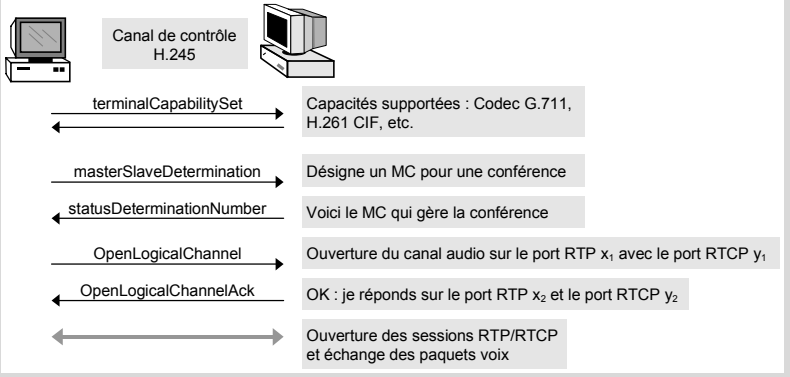
Q.931

Un PC équipé de Netmeeting peut également utiliser les services d'un de nos gatekeepers. Il suffit d'indiquer son adresse IP, ou mieux, son nom DNS, dans le menu " Outil→Option→Appel Avancé ".

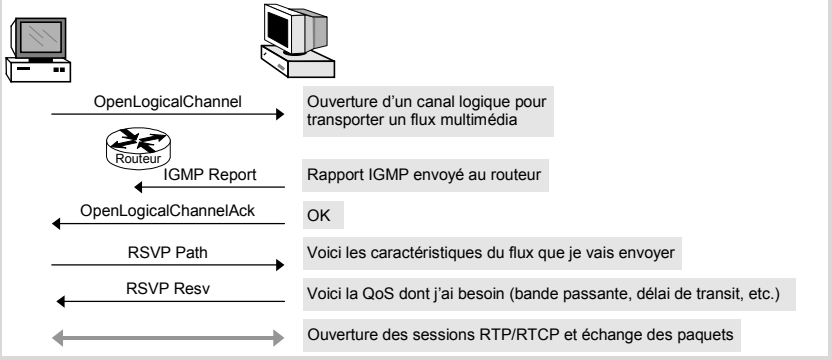


LE CANAL DE CONTRÔLE H.245

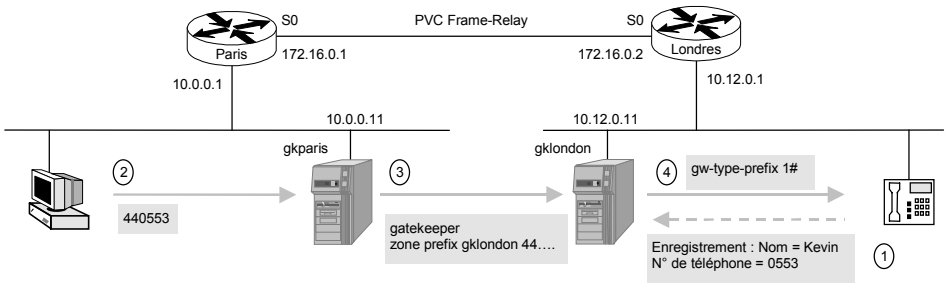
La dernière étape dans l'établissement d'une communication H.323 est l'ouverture du canal de contrôle H.245. Les messages échangés permettent de négocier les fonctions prises en charge par les terminaux (*Terminal Capability*) : choix des codecs audio et vidéo, de la résolution d'image, etc., puis d'affecter dynamiquement les ports UDP supportant les **canaux audio et vidéo**.
Si une conférence à trois ou plus est demandée, la procédure désigne le MC (celui d'un terminal, ou le MCU s'il existe) qui sera responsable de la gérer.



Le canal de contrôle H.245 véhicule ensuite les commandes permettant :
- d'ouvrir et de fermer les canaux audio et vidéo, c'est-à-dire les sessions **RTP** (*Real-time Transport Protocol*) ;
- de gérer les entrées et les sorties dans les conférences ;
- de gérer la **qualité de service**, grâce aux informations données par **RTCP** (*RTP Control Protocol*) et en faisant appel aux services de **RSVP** (*Resource Reservation Protocol*) pour réserver la bande passante nécessaire sur le réseau IP.

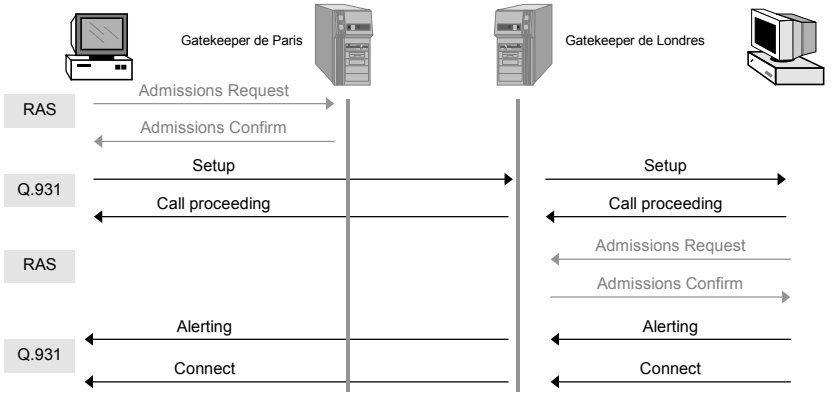


Si cela est nécessaire, un terminal peut demander au gatekeeper l'autorisation de changer de bande passante en lui envoyant un message " Bandwidth Change Request ". S'il obtient l'accord, le canal de contrôle H.245 est fermé entre les deux terminaux, puis un nouveau est ouvert accompagné d'une nouvelle demande RSVP.



Sur chaque site, les terminaux s'enregistrent auprès de leur gatekeeper local (Paris et Londres dans notre cas). Lors d'un appel, le gatekeeper de Paris autorise l'ouverture directe du canal de signalisation d'appel entre le terminal et son correspondant, tandis que le gatekeeper de Londres impose que ce canal passe par lui.

Figure 15-6.
Gestion des appel via des gatekeepers.



Le gatekeeper de Paris peut trouver les informations du correspondant concernant un terminal auprès d'un autre gatekeeper en utilisant le message " *Resource Locator* ". Le gatekeeper de Londres lui renvoie alors son adresse ainsi que le port TCP sur lequel il répond. S'il avait décidé que la communication pouvait être directe, il aurait envoyé l'adresse IP du terminal.

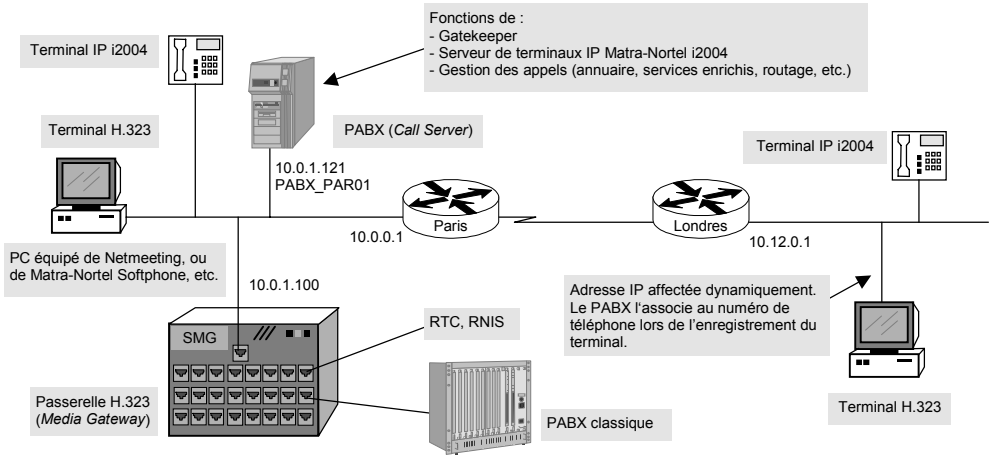
L'appel accepté, les deux entités peuvent ouvrir le canal de contrôle H.245 dans le but de négocier les paramètres du flux multimédia.

La voie vers le tout IP

Nous venons de mettre en place un système qui permet à nos terminaux IP (PC, téléphones IP) de communiquer entre eux (voix et image). Nous utilisons des gatekeepers pour assurer la conversion d'adresses et le routage des appels. Des passerelles sont également mises en place afin d'interconnecter notre réseau au monde téléphonique classique (PABX, RTC, RNIS, DECT, etc.).

Mais, par rapport à la téléphonie classique, il nous manque toute la gamme de services enrichis qu'un PABX peut offrir : plan de numérotation, messagerie vocale, transfert, filtrage, restriction et interception d'appels, etc.

L'aboutissement d'un réseau VoIP est donc la mise en place d'un PABX IP. Deux types d'offres sont proposées sur le marché : celles des constructeurs informatiques (Cisco, Lucent, etc.) et celles des constructeurs de PABX (Alcatel, Matra-Nortel, etc.). Les premiers ont l'avantage de bien connaître le monde IP ; les derniers offrent celui d'une plate-forme existante qu'il suffit de porter sur IP. C'est le cas de Matra-Nortel qui a porté sous Windows sa gamme 6500 fonctionnant à l'origine sous un Unix propriétaire. Le résultat est le produit Succession qui offre le même niveau de fonctionnalité qu'un PABX traditionnel.



Le PABX peut être situé n'importe où sur le réseau. Les sites importants en sont équipés, tandis que les petits sites n'en ont pas besoin, les terminaux dialoguant alors avec le PABX du site principal.

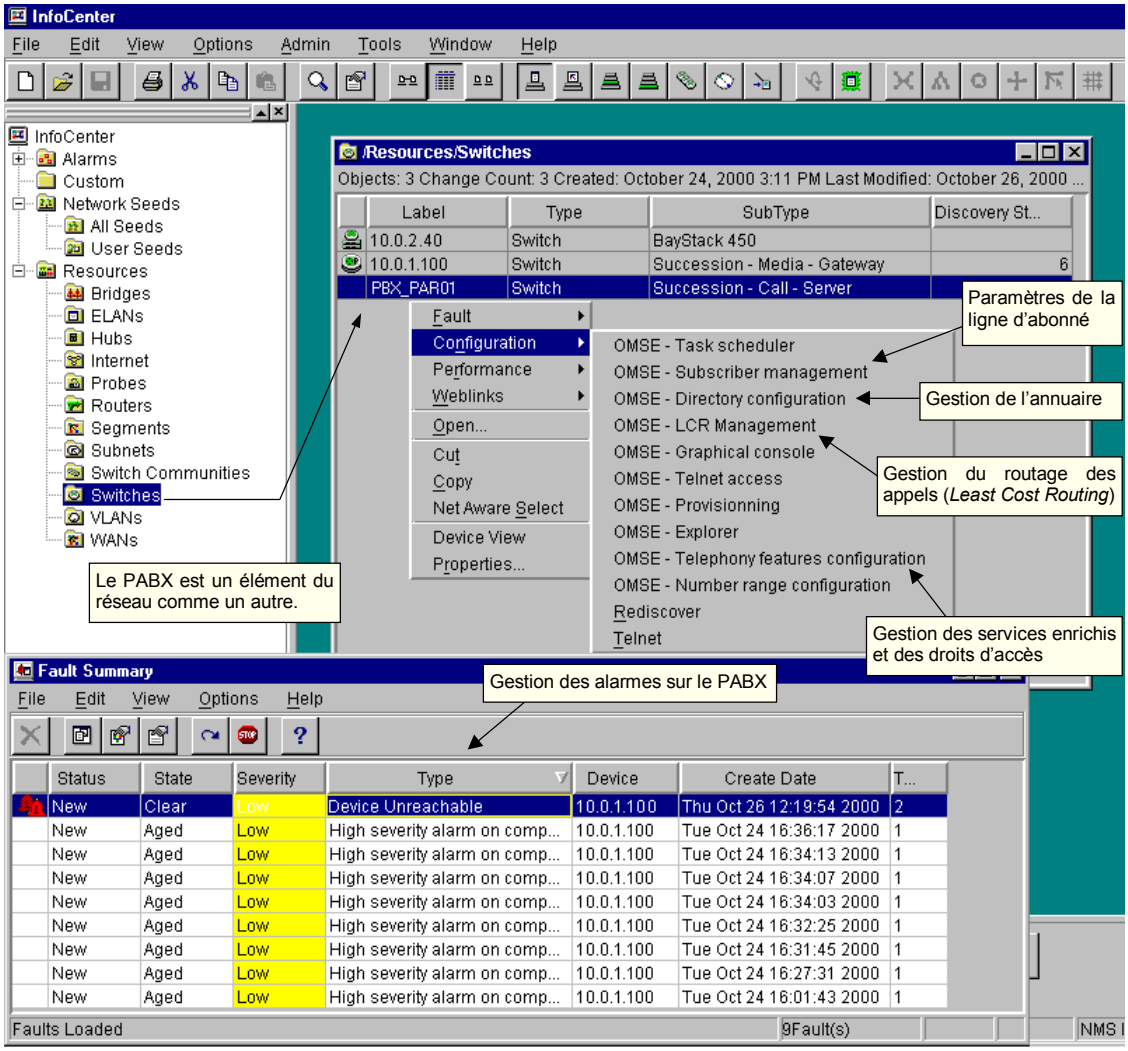
De son côté, la passerelle accueille les terminaux non IP : PABX classiques, téléphones analogiques et numériques Matra-Nortel, bornes DECT, etc. L'accès au monde extérieur (RTC, RNIS) est réalisé soit *via* le PABX traditionnel, soit directement par la passerelle. Cette dernière peut également accueillir les terminaux IP et peut, de ce fait, coupler le terminal VoIP à un poste DECT.

Le PABX accueille les terminaux H.323 natifs ainsi que ceux de Matra-Nortel *via* un protocole propriétaire. Ces derniers se comportent comme des terminaux passifs qui ne font qu'afficher les informations envoyées par le PABX (fonction équivalente à celle d'un serveur de terminaux, tel que MetaFrame).

Configurer le PABX et la passerelle VoIP

Pour configurer tous ces éléments, nous nous retrouvons dans un environnement familier d'une interface graphique sous Windows. Désormais, ces systèmes sont, en effet, considérés comme des services à part entière au même titre que les bases de données, les serveurs de fichiers, la messagerie, etc.

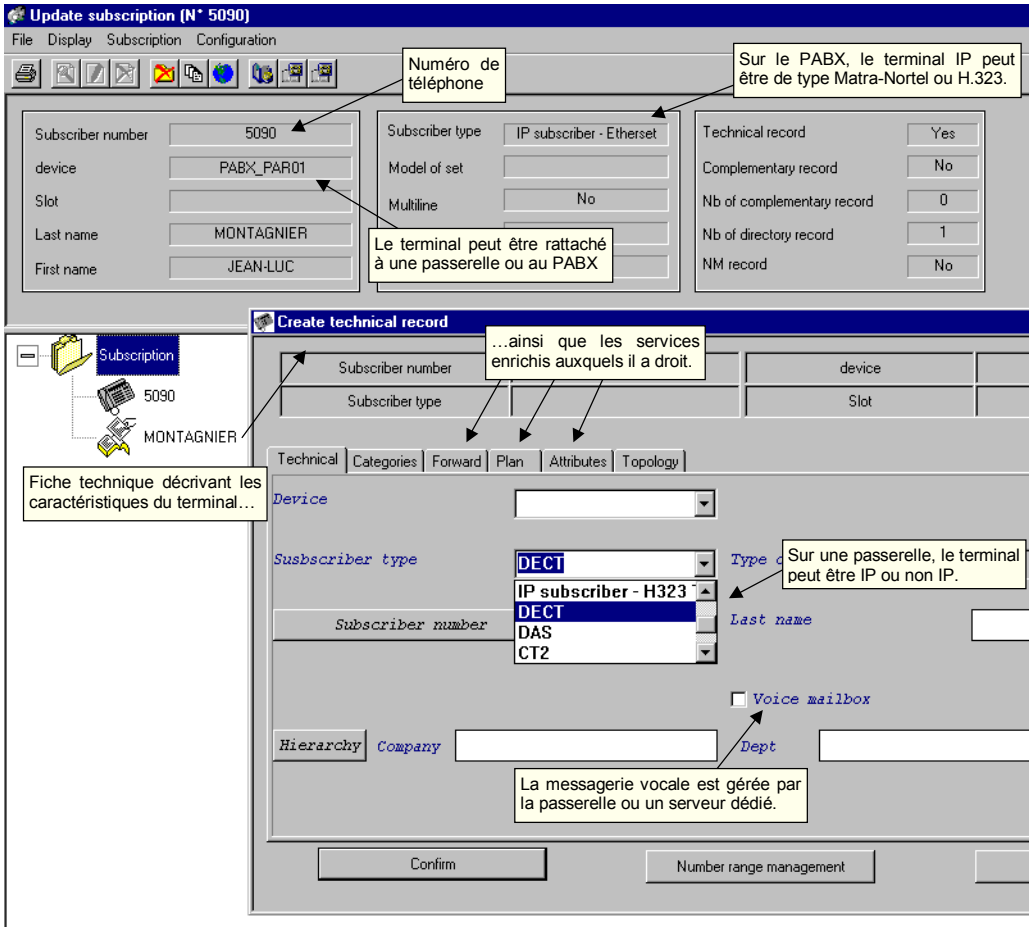
L'écran principal du gestionnaire fourni par Matra-Nortel présente les éléments de notre réseau VoIP : commutateurs du réseau local (ici un *BayStack 450*), passerelles (la *Media Gateway* de Nortel) et PABX (le *Call Server* de Nortel).



Déclarer les terminaux téléphoniques

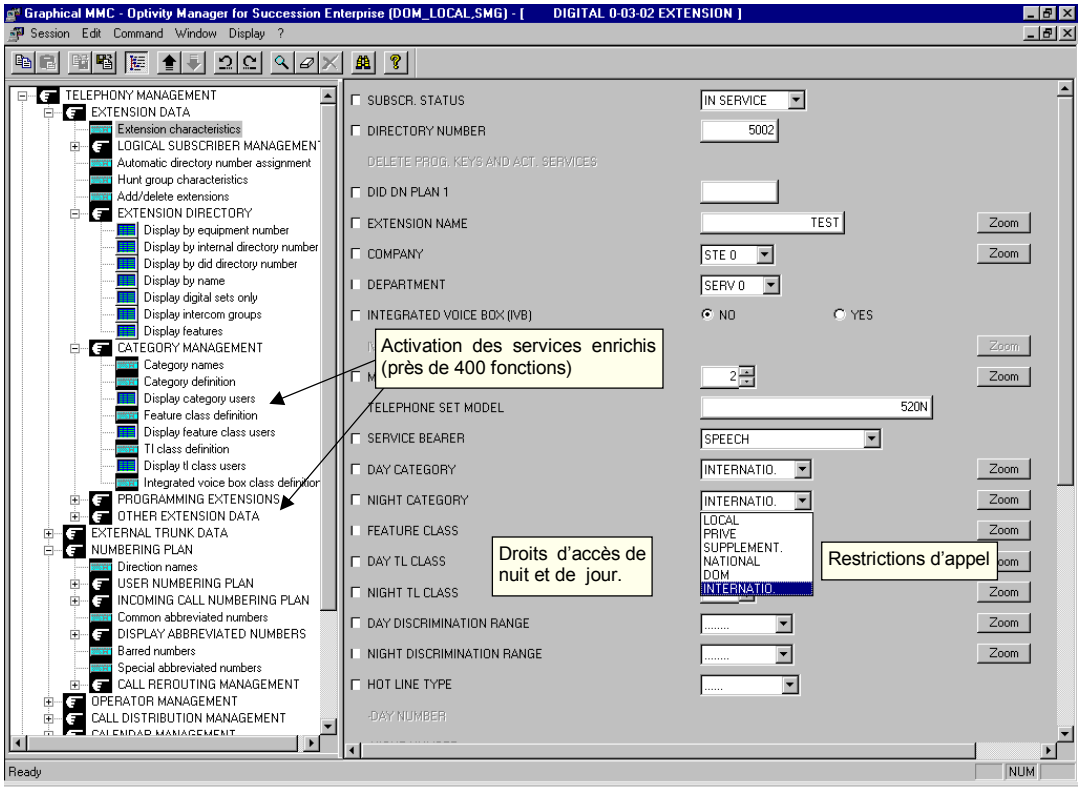
Ensuite, il convient de déclarer les terminaux rattachés à notre PABX : il peut s'agir de téléphones VoIP Matra-Nortel (i2004), de PC équipés de Netmeeting ou encore de téléphones classiques raccordés à une passerelle.

Nous entrons alors dans le monde des téléphonistes : il faut créer un **abonné** auquel on associe une entrée dans l'**annuaire** ainsi qu'une **fiche technique** qui décrit les caractéristiques du poste et les services auxquels l'utilisateur a droit.



Sous l'arborescence *Subscription* (abonnement), nous avons créé l'abonné Montagnier, puis nous lui avons affecté un numéro de téléphone (le 5090) et spécifié le type de terminal qu'il utilise : dans son cas, il s'agit d'un téléphone IP (*IP subscriber – Etherset*). Nous lui avons

ensuite associé une fiche technique décrivant les caractéristiques du terminal (ici, *IP subscriber – H323*) et les services auquel il a droit, par exemple une messagerie vocale (*Voice mailbox*).



Parmi les services enrichis que le PABX peut gérer pour le terminal on trouve :

- l'identification de l'appelant ;
- la restriction d'appel (local, province, étranger, etc.), restrictions horaires ;
- le renvoi, transfert, filtrage ;
- le rappel sur occupation ;
- les numéros programmés (urgence, SVP) ;
- la gestion du second appel : parcage, conférence, va-et-vient ;
- la messagerie vocale ;
- etc.

Assurer la qualité de service

Nous devons également penser à gérer la qualité de service sur l'ensemble de nos routeurs, en activant, par exemple, RSVP et les files d'attente appropriées.

La réservation de la bande passante doit être effectuée à la source des flux VoIP, c'est-à-dire au niveau des passerelles :

```
req-qos guaranteed-delay
```

Demande une garantie sur la bande passante et sur le délai de transit

Ensuite, RSVP doit être activé sur toutes les interfaces de nos routeurs (comme indiqué au chapitre 14) :

45 kbit/s dédiés à RSVP, dont 15 kbit/s par flux (8 kbit/s pour le codec + overhead + signalisation)

```
ip rsvp bandwidth 45 15
fair-queue 64 256 3
```

3 files d'attentes pour RSVP pour 3 communications simultanées

Les débits à réserver dépendent des codecs choisis pour coder la voix (voir chapitre 12). Celui en question est le g729 qui nécessite 8 Kbit/s de bande passante.

Rappelons que les commutateurs sur nos LAN et que les files d'attente WFQ sur les routeurs prennent en compte la priorité des paquets IP. Il est donc intéressant d'affecter une valeur au champ " IP precedence " , ce qui doit être fait à la source des flux VoIP, c'est-à-dire au niveau des passerelles :

```
#gwpar1
dial-peer voice 44 voip
ip precedence 5
```

Priorité 5 = Critical (voir chapitre 13).

Par ailleurs, nos commutateurs doivent assurer la correspondance entre la priorité du paquet IP et celle affectée à la trame Ethernet, ce qui est réalisé comme suit :

```
set qos acl ip politique_voip trust-ipprec
set qos ipprec-dscp-map 0 8 16 24 32 40 48 56
set qos dscp-cos-map 40:6
```

Transporter les flux multimédias

Un terminal H.323 utilise les services de la couche d'adaptation H.225 pour envoyer et recevoir des messages. En plus des signalisations Q.931 et RAS, cette couche réalise l'interface entre la gestion des canaux logiques par le terminal et la gestion des paquets sur un réseau IP. En fonction de leur nature, H.225 sélectionne ainsi le type de paquet dans lequel envoyer les données : TCP, UDP, RTP ou RTCP.

Canal logique	Protocole de transport / Numéro de port
Canal RAS : découverte d'un gatekeeper	UDP 1718 ou adresse multicast 224.0.1.41
Canal RAS : enregistrement auprès d'un gatekeeper	UDP 1719
Canal de signalisation Q.931	TCP 1720
Canal de contrôle H.245	Port TCP alloué dynamiquement par Q.931 (messages *Connect*, *Alerting* et *Call proceeding*)
Sessions RTP/RTCP	Port UDP alloué dynamiquement par H.245 (message *Open Logical Channel*)
T.120	TCP 1503

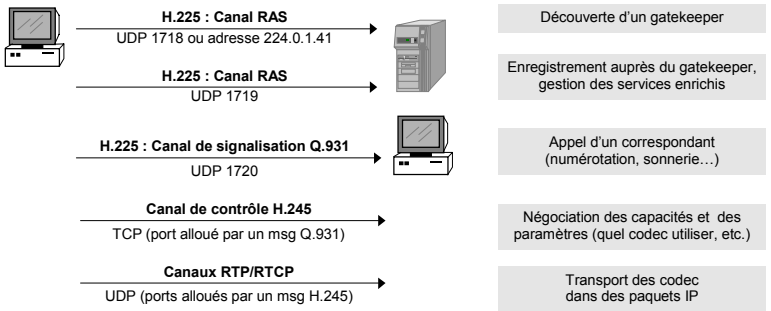


Figure 15-7.
Interaction des protocoles H.323.

Le transport des flux multimédias est donc assuré par H.225 qui reprend les spécifications des RFC suivantes.

RFC	Sujet traité
1889	Spécifications de RTP et de RTCP
1890	Définition des profils pour les conférences audio et vidéo
2032	Transport des codecs vidéo H.261
2190	Transport des codecs vidéo H.263
2198	Transport des codecs audio

Le transport des flux audio et vidéo via *RTP et RTCP*

Une conversation téléphonique génère un flux audio qui est découpé en tranches représentant quelques millisecondes d'un son. De même, une image vidéo est découpée en tranches représentant un groupe de pixels. Une tranche correspond ainsi à un échantillonnage (*sampling*) d'un son ou d'une image vidéo numérisés et donc représentés par des octets (voir chapitre 12).

Ces octets sont placés dans des paquets **RTP** (*Real-time Transport Protocol*). Ce standard ne décrit aucun mécanisme de contrôle ni de récupération d'erreur : il se contente de définir le format des paquets et des données transportés. Ces paquets RTP sont ensuite encapsulés dans des paquets UDP, eux-mêmes transportés dans des paquets IP.

RTP est associé à **RTCP** (*RTP Control Protocol*), également transporté dans des paquets UDP, qui renvoie à l'émetteur un retour sur la qualité de service perçue par les récepteurs d'un flux.

Deux couples de ports UDP (source et destination) sont alloués pour un flux audio ou vidéo : l'un pour RTP, l'autre pour RTCP. Le protocole UDP étant orienté sans connexion, les sessions sont gérées par H.245 qui fait l'association avec ses numéros de canaux logiques.

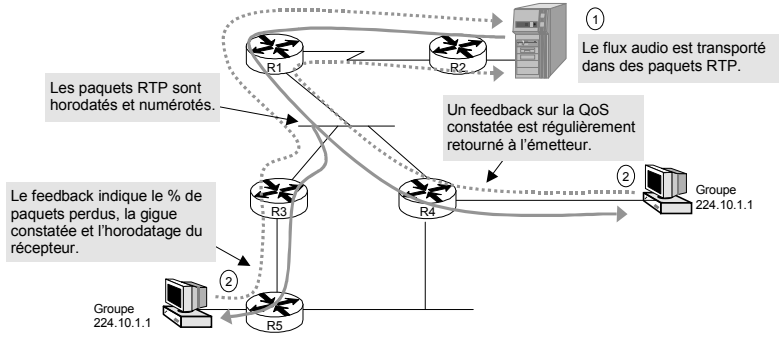


Figure 15-8.
Rôles de RTP et de RTCP.

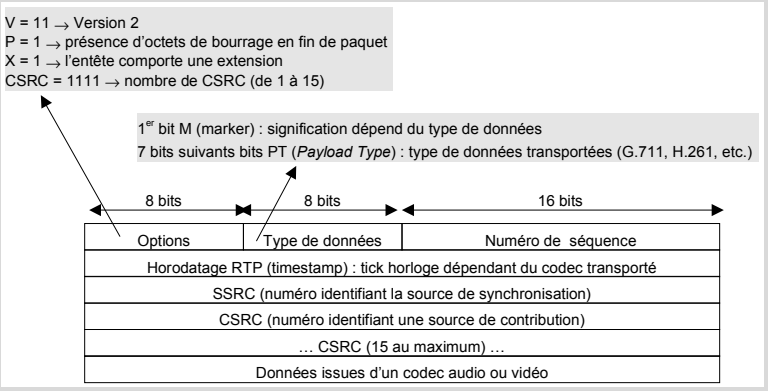
Un flux ne transporte jamais de données mixtes audio et vidéo. Par exemple, pour une visioconférence, les paquets audio et vidéo sont transportés dans deux sessions RTP différentes, chacune étant associée à une session RTCP.

Le codage peut être modifié au cours d'une session pour s'adapter à un changement de la qualité de transmission (débit, erreurs, etc.). L'émetteur peut également modifier la nature du flux au cours d'une session et basculer, par exemple, de la vidéo à l'audio.

LE POINT SUR RTP (RFC 1889 ET 1890)

Le protocole RTP (*Real-time Transport Protocol*) décrit le format des paquets transportant des flux audio ou vidéo.

Utilisant les services de la couche UDP, RTP n'assure pas pour autant un quelconque contrôle de flux, de reprise sur erreur ou même de contrôle d'intégrité du paquet. Son but est simplement de transporter quelques millisecondes de voix ou une portion d'image en y incluant des informations relatives au temps (synchronisation) et permettant d'identifier les émetteurs qui génèrent le signal audio ou vidéo.



Le numéro de port UDP affecté à RTP est alloué aléatoirement par l'application. Il doit simplement être pair. Le numéro suivant (forcément impair) est alors affecté à la session RTCP associée (voir l'encart suivant).

L'**horodatage**, qui dépend de l'horloge de l'émetteur, représente l'instant où le premier octet des données transportées a été échantillonné.

Le champ **SSRC** (*Synchronization Source*) est un numéro unique, généré de manière aléatoire, qui identifie l'émetteur du flux. Un mécanisme permet de gérer les problèmes de collision (deux SSRC identiques).

La RFC prévoit l'utilisation de **mixers** dont le rôle est de mélanger les flux pour n'en faire qu'un qui sera redistribué aux participants d'une conférence audio, par exemple. Il synchronise les flux combinés issus des différentes sources n'utilisant pas le même codage et ne disposant pas de la même source d'horloge ni de la même fréquence d'échantillonnage. Le paquet RTP résultant contient la liste des SSRC qui ont contribué à la formation du flux mélangé (champs **CSRC**, C*ontributing Source*), par exemple, la liste de ceux qui ont parlé en même temps.

Le mixer s'apparente aux fonctions du MCU H.323, mais au niveau RTP, alors que ce dernier assure des fonctions plus évoluées liées à la signalisation. En pratique, un serveur de conférence implémente les fonctions de MCU et de mixer.

La RFC prévoit également l'utilisation de **translators** dont le rôle est de convertir des flux sans les mélanger.
Ce logiciel peut :

- convertir un codec en un autre ;
- convertir un flux multicast en un flux unicast ;
- convertir les ports UDP aléatoires en ports UDP fixes pouvant être filtrés par un firewall ;
- créer un tunnel sécurisé en chiffrant les données ;

Dans ces deux derniers cas, un translator s'utilise par paire.

LE POINT SUR RTCP (RFC 1889 ET 1890)

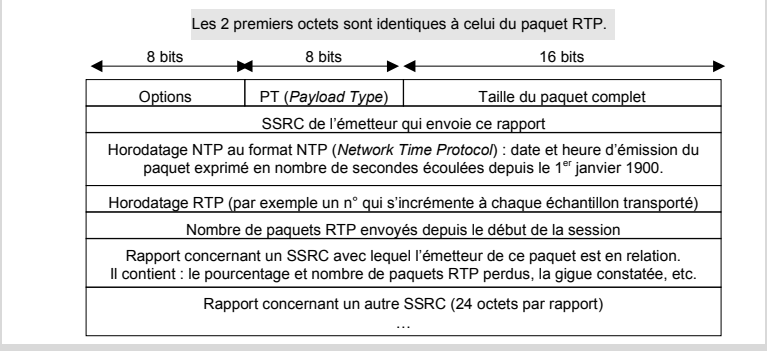
RTCP (*RTP Control Protocol*) décrit le format des informations remontées par le ou les récepteurs d'un flux. Il est utilisé concurremment avec RTP pour remplir trois fonctions :

- fournir un retour sur la qualité de service perçue par les récepteurs ;
- permettre d'identifier tous les participants à la conférence par un nom unique (un nom DNS, tel que machine.laposte.fr). Cela permet de retrouver le participant si le SSRC change en cours de session (suite à une réinitialisation, ou à la détection d'un conflit d'attribution de SSRC) ;
- permettre à chaque participant d'évaluer le nombre total de participants et d'adapter les flux en conséquence (fréquence d'émission des paquets).

Le paquet RTCP contient ainsi des informations relatives à l'**horodatage** des paquets reçus, la **gigue** (*jitter*) constatée par les récepteurs, le nombre de **paquets perdus** par période et en cumulé. Les informations recueillies par les émetteurs et les récepteurs permettent de vérifier que la qualité de service correspond à celle demandée *via* **RSVP**.

Il existe plusieurs types de paquets RTCP : rapport de récepteur (type RR – *Receiver Report*), rapport d'émetteur (type SR – *Sender Report*) si le récepteur est également un émetteur, description de la source (type SDES – *Source Description*), fin d'une participation (BYE) et fonctions spécifiques à une application (type APP), par exemple audio, vidéo, etc.

Ainsi, les rapports RR (PT = 201) et SR (PT = 200) prennent la forme suivante :



Le **rapport SEDS** contient, quant à lui, toutes les informations concernant l'émetteur : nom, adresse e-mail, numéro de téléphone, localisation géographique, nom du logiciel utilisé, etc.

Pour consommer le moins de bande passante possible :

- les différents types de paquets RTCP sont regroupés dans un seul paquet UDP ;
- la périodicité d'émission des paquets RTCP est aléatoire (entre 2 et 5 minutes) ;
- l'envoi des paquets RTCP par tous les participants doit être espacé de 2 à 7 secondes afin d'éviter les *bursts* ;
- le flux RTCP ne doit pas dépasser 5 % de la bande passante utilisée par RTP ;
- un participant ne doit pas générer plus de 20 % du total des flux RTCP.

Optimiser les flux multimédias

Un paquet RTP transporte 2 à 30 ms de voix, ce qui représente 20 à 150 octets selon le codec utilisé. La RFC 2298 montre l'exemple d'un paquet RTP transportant 20 ms de voix échantillonnée à 8 KHz et dont les données utiles ne représentent que 98 octets.

Codec	Données numériques
G.722	8 bits par échantillonnage
G.723	30 ms par trame
G.728	3,1 ms par trame
G.729	10 ms par trame

Afin de réduire l'impact de l'overhead, on pourrait augmenter la taille des données transportées en envoyant plusieurs trames dans un seul paquet. L'inconvénient de cette approche est qu'elle engendre un délai de transit supplémentaire dans une passerelle ou au départ du PC émetteur. Par exemple, au lieu d'attendre 30 ms pour envoyer une trame G.723, on attendra 60 ms pour envoyer deux trames. Résultat : le délai d'attente de la première trame du paquet est allongé de 30 ms, et ce pour une trame sur deux dans le flux.

Les techniques suivantes sont pour cela privilégiées.

Compression des en-têtes

La taille minimale d'un paquet RTP (sans la liste des contributeurs) est de 12 octets, auxquels il faut ajouter 8 octets pour UDP et 20 pour IP, soit 40 octets en tout.

Afin de diminuer cet overhead, les routeurs permettent de compresser ces en-têtes en réduisant leur taille cumulée à 2 ou 5 octets sur les interfaces WAN. Par exemple, les commandes suivantes permettent de compresser les en-têtes de 16 sessions RTP simultanées :

```
int s 0
encapsulation ppp
ip rtp header-compression
ip rtp compression connections 16
```

Le principe repose sur le fait que l'en-tête varie très peu d'un paquet à l'autre : seuls les numéros de séquence et de contrôle d'erreur changent. L'activation de la compression consiste alors à n'envoyer que les données qui ont changé d'un en-tête à l'autre (RTP/UDP/IP), ce qui représente entre 2 et 5 octets la plupart du temps. Cette fonction est surtout efficace pour les liaisons inférieures à 2 Mbit/s.

Utilisation des mixers

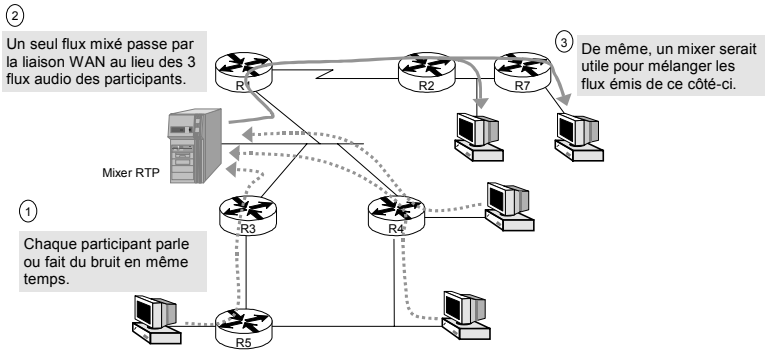
Le son perçu par un participant est la résultante des voix et des bruits émis par les autres. Pourtant, celui-ci reçoit *N* flux audio, provenant des *N* autres participants. Son PC se contente de restituer un son composite.

Afin de diminuer le débit généré par ces flux sur notre réseau, et surtout sur les liaisons WAN limitées en bande passante, il serait intéressant de créer un son composite en amont.

Le **mixer RTP** répond à ce besoin puisqu'il permet de fusionner les différents flux audio en un seul. Rappelons, par ailleurs, qu'un mixer permet également de convertir les codecs audio entre participants ne disposant pas des mêmes équipements.

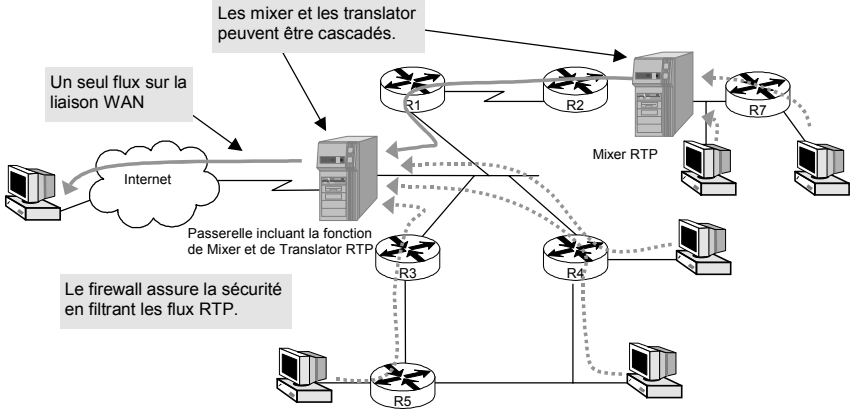
Dans notre réseau, l'installation d'un mixer de chaque côté de la liaison WAN permet de diminuer considérablement les flux générés par une conférence audio. De plus, alors que les participants peuvent envoyer leur flux dans des paquets unicast, le flux envoyé par le mixer pourra utiliser des paquets multicast afin de réduire encore davantage la charge globale du réseau.

Figure 15-9.
Utilisation d'un mixer pour optimiser les flux.



L'intranet est connecté à l'Internet par une liaison (spécialisée, Frame Relay ou autre) dont le débit est souvent limité. Si plusieurs participants à une même conférence sont répartis entre notre intranet et l'Internet, là encore, l'utilisation d'un mixer permet de réduire la charge de la liaison WAN.

Figure 15-10.
Intégration d'un mixer et d'un translator dans un firewall.

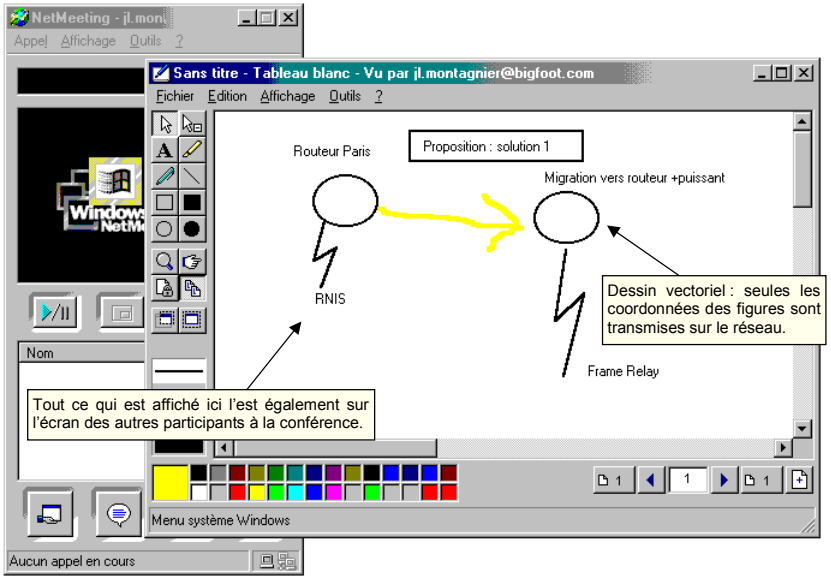


Échanger des données multimédias

Les participants à une visioconférence peuvent vouloir recevoir un document que leur remet l'animateur, par exemple. Le standard T.120 de l'ITU-T offre à ces participants la possibilité d'utiliser quatre applications :

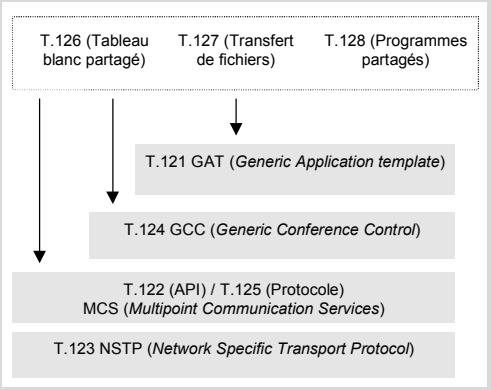
- transfert de fichiers multipoint ;
- partage d'un presse-papiers commun ;
- partage d'un tableau blanc virtuel (*whiteboard sharing*) qui permet à chaque participant de dessiner sur le même schéma ;
- déport écran/clavier pour une prise de contrôle à distance et une démonstration à tous les participants.

On retrouve ici des applications classiques, mais sous la forme du partage par plusieurs utilisateurs.



LES DONNÉES AU SEIN D'UNE CONFÉRENCE MULTIMÉDIA (ITU-T T.120)

La norme T.120 décrit un cadre fonctionnel général permettant à des utilisateurs de **partager des données au sein d'une conférence** *via* des sessions TCP gérées par H.245.



Les protocoles utilisés sont les suivants :

- **GAT** (*Generic Application Template*), norme **T.121**. Définit les interfaces d'accès (API) pour des applications T.120 : entrées et sorties des conférences, négociations des fonctionnalités, etc.
- **MCS** (*Multipoint Communication Service*), normes **T.122** pour l'interface d'accès et **T.125** pour le protocole. Assure la diffusion des données au sein d'une conférence selon trois topologies : en étoile autour d'un gestionnaire central (*top provider*), en cascade autour de plusieurs gestionnaires et d'un *top provider*, ou chaînage (*daisy chain*).
- **NSTP** (*Network Specific Transport Protocol*), norme **T.123**. Assure l'interface entre les applications T.120 et le réseau. Il réalise l'adaptation à différents supports, tels que RNIS et TCP/IP, tout en gérant les erreurs de transmission.
- **GCC** (*Generic Conference Control*), norme **T.124**. Il s'agit du logiciel qui organise la conférence. Il gère la liste des participants, les accepte ou les refuse selon les mots de passe et les droits d'accès, décide à qui passer la main, assure la cohérence des informations échangées (mise à jour en temps réel et simultanément pour tous les participants) et surveille les ressources utilisées par le MCS.

QUATRIÈME PARTIE

Gérer son réseau