6 Session Initiation Protocol (SIP)

L'IETF (Internet Engineering Task Force) a spécifié, dans le stand RFC 2543/RFC 3261, une architecture multimédia sur réseau IP axée le protocole de signalisation SIP (Session Initiation Protocol). Grâce au p cessus de standardisation simple et rapide de l'IETF, les possibilités d'ét dre la fonctionnalité de SIP sont aisées. En contrepartie, le risque de v apparaître des versions différentes du protocole dans les produits du m ché existe. Toutefois, ceci ne devrait pas être un désavantage marqua car les messages SIP, inconnus des anciens équipements, pourront s plement être ignorés.

Le présent chapitre décrit le concept de base de SIP. Il présente s architecture, en relation avec la communication multimédia, et décrit manière détaillée la structure et le fonctionnement du protocole. Il illus également de nombreux cas de signalisation.

6.1 Contexte

Les protocoles de signalisation mis en œuvre dans les réseaux de télécommunications sont généralement conçus et optimisés pour une utilisation spécifique. Leurs caractéristiques respectives sont généralement différentes. La réalisation de communications multimédias, indépendamment du type et du nombre de réseaux à traverser, est rendue possible par des passerelles qui prennent en charge toutes les fonctions de conversion. Des protocoles de signalisation ont été développés, d'une part, pour permettre aux terminaux de dialoguer avec les passerelles et, d'autre part, pour rendre possible l'échange des informations de contrôle entre les extrémités d'une communication.

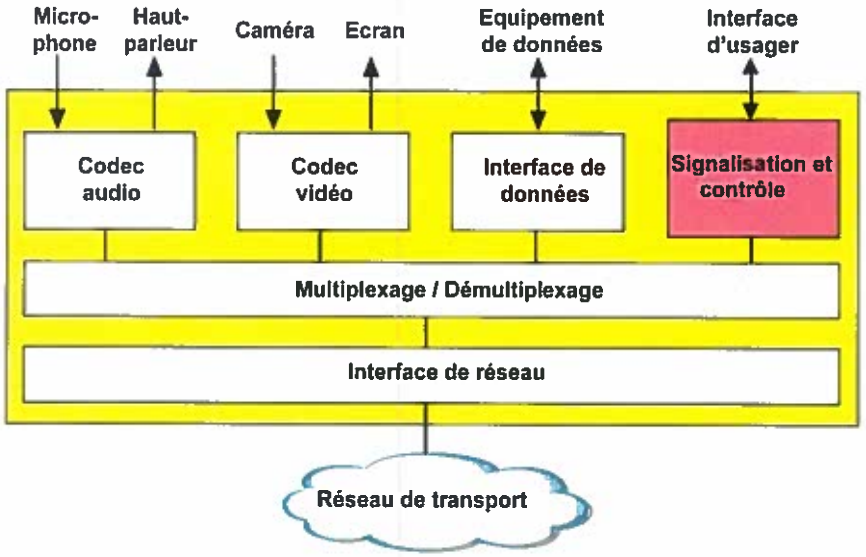

Figure 6-1 : Signalisation et contrôle dans les terminaux multimédias

Un réseau de communication est régi par des caractéristiques opératoires fondamentales. Celles-ci peuvent être classées dans les catégories suivantes :

- L'adressage.
- Le mode d'exploitation.
- Le routage.
- La signalisation.

Les paragraphes suivants présentent une brève description de chacune ces catégories. Il s'agit de mettre en évidence la diversité de protocoles de structures qui vont fixer les contraintes de la réalisation de communi tions multimédias.

6.1.1 Adressage

L'adressage est un concept fondamental dans les réseaux de télécommu cations. Il est destiné à identifier un terminal dans un environnement p lui acheminer l'information.

En fonction de leur structure, les différents types d'adressage peuv contenir des informations multiples, liées à la position géographique l'organisme qui gère le plan ou à l'appartenance à une entité logique (so réseau).

Réseau	Type	Structure	Longueur
ISDN/PSTN	E.164	Géographique	N digits
IP	RFC 791	Logique	32 bits
IPv6	RFC 2373	Logique/géographique	128 bits
LAN	MAC IEEE 802.2	Plate	48 bits

MAC : Medium Access Control
LAN : Local Area Network
RFC : Request For Comment
ISDN : Integrated Services Digital Network
PSTN : Public Switched Telephone Network

Figure 6-2: Types d'adressage

L'éventuelle nature hétérogène des réseaux impliqués dans une communication multimédia va nécessiter la mise en correspondance d'adresses de structures très différentes. Cette conversion est rendue possible par la mise en œuvre de services d'annuaire ad hoc.

La figure 6-2 énumère différents types d'adressage :

- L'adressage selon E.164 est utilisé dans le réseau téléphonique et dans le RNIS. Il est constitué d'un nombre variable de digits et permet d'identifier des zones géographiques (pays, régions).
- L'adressage MAC est l'apanage des réseaux locaux d'entreprises exploitant une méthode de partage du médium (MAC: Medium Access Control). Des plages d'adresses sont distribuées aux constructeurs qui les figent dans leurs équipements. Les adresses ainsi attribuées ne comportent aucune information quant à la localisation géographique ou à l'appartenance logique à un réseau. On parle alors de structure "plate".
- Les adressages IP version 4 et version 6, basés sur 32 respectivement 128 bits, répondent à une structure logique qui permet d'identifier une station parmi un groupe (le sous-réseau) qui partage le même espace d'adressage.

Il existe de nombreux autres types d'adressages. Chacun est, en général, spécifique à un protocole de réseau.

6.1.2 Mode d'exploitation

Le mode d'exploitation a une très grande influence sur les caractéristiques de fonctionnement d'un réseau. Il détermine la manière de signaliser, le mode d'adressage et certaines des propriétés temporelles du trafic qui s'y écoule.

- Un réseau sans connexion, ou "datagramme", fonctionne sur le principe du paquet autonome contenant l'adresse de destination qui est aiguillé par chacun des nœuds du réseau. La base de données, qui contient les routes à utiliser en fonction de l'adresse, s'appelle la table de routage. Elle est sollicitée pour chaque paquet qui doit être acheminé. La fourniture de la qualité de service dans ce genre de structure est problématique, en particulier en raison des temps de transfert variables et de l'impossibilité de garantir la livraison de

l'information en séquence. En revanche, ce mode d'exploitation souple et robuste.

- Les réseaux orientés connexion (à commutations de circuits ou paquets) requièrent la mise en œuvre d'une procédure de sig sation pour établir la connexion (circuit ou circuit virtuel). C'est c cette phase d'établissement qu'intervient l'adressage et le choix d' éventuelle qualité de service. La phase de transfert d'information suivie d'une procédure de signalisation pour fermer les connexi Cette procédure permet de libérer les ressources du réseau qui été mobilisées durant la phase d'appel.

	CONS	CLNS
Type de connexions	Trajet fixe entre source et destination (circuit ou circuit virtuel).	Chaque paquet peut prendre un che différent (datagramme).
Etablissement	Par la signalisation ou par la gestion du réseau.	Pas d'établissement.
Séquentialité de l'information	La séquentialité est assurée.	La séquentialité n'est pas assuré
Utilisation de l'adresse de destination	Uniquement à l'établissement de l'appel.	L'adresse est contenue dans chac paquet.
Exemples	VoIP, ISDN	IP, LAN

CONS : Connection Oriented Network Services
CLNS: Connectionless Network Services

Figure 6-3: Mode d'exploitation des réseaux

L'écoulement du trafic, à priori destiné à des réseaux orientés conne sur des réseaux de type "datagramme" constitue une des difficultés d mise en œuvre de systèmes multimédias sur des environnements IP. ailleurs, l'interconnexion de réseaux, dont les caractéristiques sont différentes, nécessite des passerelles capables d'opérer des adaptat pour chacun des aspects qui divergent entre ces réseaux.

6.1.3 Routage

Le routage est un choix, fait par un nœud du réseau, pour acheminer une unité de données de protocole ou pour établir un circuit. Il est basé sur l'analyse d'une table de routage construite à partir d'échanges d'informations entre les entités de commutations (routage dynamique) ou de tables figées et gérées par la gestion du réseau (routage statique).

Dans les réseaux orientés connexion, la table de routage n'est utilisée que durant la phase d'établissement. Durant la phase de communication, c'est une table de translation qui livre la correspondance entre les identificateurs de connexions.

6.1.4 Signalisation

La signalisation est, de manière générale, la définition d'une syntaxe, d'une sémantique et de procédures permettant un dialogue entre partenaires d'une communication. La signalisation peut être définie dans les catégories suivantes :

- La signalisation usager-réseau constitue le véhicule par lequel un utilisateur transmet les informations de contrôle d'appels et de gestion des connexions à son réseau. Elle peut se résumer à un seul type de paquet dans les réseaux sans connexion, tels que les LANs ou les réseaux IP ou faire l'objet de volumineuses définitions dans le cas des réseaux orientés connexion tels que les réseaux VoIP ou RNIS.
- La signalisation entre les nœuds du réseau permet aux entités actives du réseau d'échanger de multiples informations destinées à la gestion des connexions, à la gestion du réseau, à l'échange de tables de routage, au contrôle de fonctionnement et à la gestion des ressources.
- La signalisation de bout en bout a la particularité d'être totalement ignorée par le réseau. Elle régit les échanges d'information entre deux points terminaux d'une communication selon des définitions généralement propres à l'application. Parmi les fonctions de ces échanges, on peut citer les échanges des caractéristiques des différents flux, le contrôle de la qualité, la détermination des capacités audio et vidéo.

6.2 Le protocole SIP

SIP (Session Initiation Protocol, IETF RFC 2543/RFC 3261) est un pr cole de signalisation simple, flexible et évolutif. Les messages d'établi ment et de libération des sessions voix, audio, vidéo et de données rédigés en format texte.

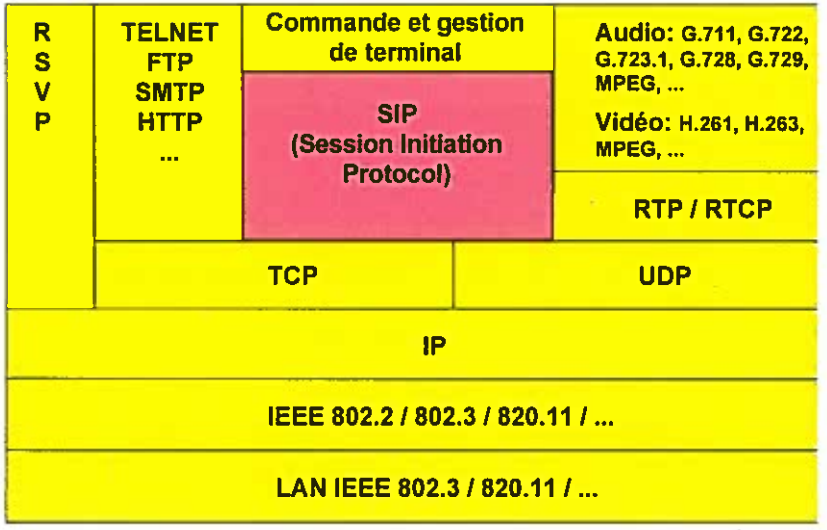

Figure 6-4: Modèle de référence du protocole pour des systèmes multimédias selon SIP

SIP ne sert pas uniquement à la signalisation dans les systèmes de c munication multimédias. Ce protocole permet aussi, par exemple, d'affi des messages e-mail ou des messages d'autres types en attente (mess waiting). Il peut aussi servir à informer l'usager d'événements particulier

Les partenaires de communication d'une session SIP sont en prem ligne des individus, qui peuvent être identifiés de façon univoque par adresse SIP (similaire à l'adresse e-mail) ou par une adresse E.164. Il

aussi s'agir d'ordinateurs ou de machines, qui seront identifiés par une adresse SIP URI (Uniform Resource Identifier).

SIP représente la partie signalisation de l'architecture multimédia définie par l'IETF. Les protocoles utilisés pour le transfert de la parole, des informations audio et vidéo, ou encore des données, sont identiques dans les environnements SIP, H.323, MGCP, ainsi que dans la plupart des environnements propriétaires (p. ex. G.711 sur RTP/UDP). De la sorte, la compatibilité au niveau des flux de médias est assurée.

6.3 Architecture SIP

Dans les systèmes multimédias SIP, deux ou plusieurs agents d'usagers (UA: User Agents) communiquent les uns avec les autres. L'établissement et la libération des connexions, ainsi que la commande des communications, sont pris en charge par des serveurs d'enregistrement, de localisation ou de redirection et par des serveurs proxy. Au besoin, des passerelles (Gateway) assurent l'interconnexion avec les réseaux publics.

Entité:	Description:
User Agents (UA)	Ils émettent et acceptent les requêtes d'établissement des sessions (session requests) et closent les sessions. Ils sont subdivisés en clients d'agents d'usagers (UAC: User Agent Clients), chargés d'établir les connexions et en serveurs d'agents d'usagers (UAS: User Agent Servers), qui acceptent les connexions. Tous deux peuvent libérer les connexions.
Registrar	Il gère les informations des agents d'usagers pour un réseau, respectivement pour un segment de réseau donné. A cette fin, les agents d'usagers doivent s'enregistrer auprès de lui.
Location Server	Il permet au proxy et au serveur de redirection d'obtenir les informations relatives à "l'emplacement" (généralement une adresse IP) d'un usager.
Proxy Server	Chaque serveur proxy contient un client et un serveur. Tous deux travaillent en collaboration afin de recevoir,

	traiter et, au besoin, réacheminer les messages émis les agents d'usagers. Le traitement d'un message signalisation SIP peut également signifier sa modificati Le proxy a la possibilité de traiter ces messages en inte et d'y répondre directement, sans les transmettre à un U respectivement à un autre serveur.
Redirect Server	Le serveur de redirection ne réachemine pas les mes ges de signalisation SIP, contrairement au proxy. Il liv sur demande, l'adresse SIP URI de l'usager requis ou b celle du serveur susceptible de connaître l'adresse de usager.

Tableau 6-1: Blocs fonctionnels de l'environnement SIP

La figure 6-5 illustre l'architecture d'un environnement SIP. En pratique fonctions des trois serveurs (Registrar, Proxy et Redirect Server) sont r sées dans le même équipement.

Entre un réseau VoIP basé sur SIP et le réseau téléphonique ou le R une passerelle assurant la conversion de la signalisation et celle des flu médias est nécessaire. Entre deux réseaux VoIP utilisant des protocole signalisation différents, la conversion des flux de médias n'est pas né saire si la pile de protocoles respecte la structure RTP/UDP conven nelle.

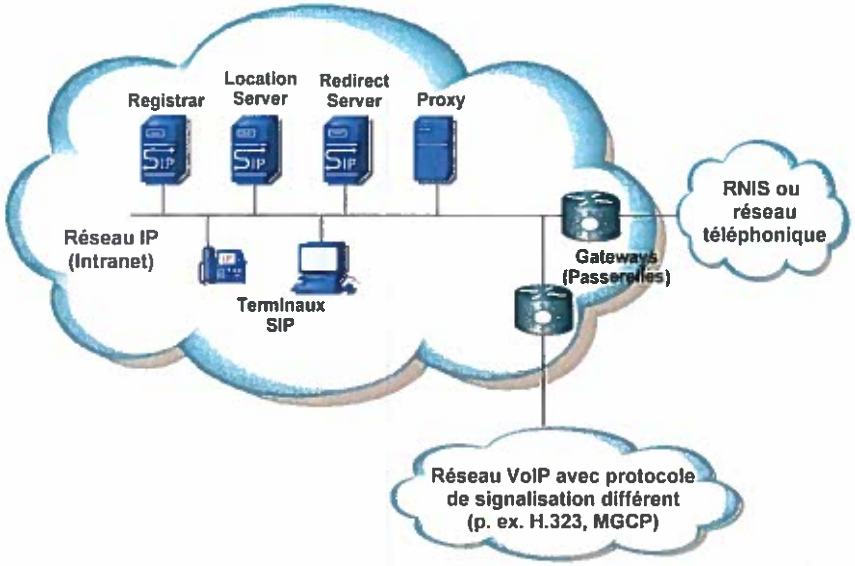

Figure 6-5: Architecture d'un système basé sur SIP

6.4 Messages de signalisation

Les messages (méthodes) de signalisation SIP peuvent être convoyés au moyen de divers protocoles de transport. Toutefois, la faveur est accordée à UDP (User Datagram Protocol), pour s'affranchir de la lourdeur des procédures d'établissement et de libération des connexions usuelles à TCP (Transport Control Protocol).

Le numéro de port 5060 a été standardisé pour le transport de messages SIP, aussi bien sur UDP que sur TCP.

Dans le cas le plus simple, la signalisation SIP est effectuée directement d'agent d'usager (*UA: User Agent*) à agent d'usager. Pour cela, il faut que l'agent qui émet la requête d'établissement connaisse l'adresse SIP du partenaire.

Le protocole SIP comprend des messages de requête et des réponses. La figure 6-6 illustre l'échange des messages entre deux terminaux pour l'établissement, puis la libération d'une communication entre deux téléph IP. Les différentes classes de messages seront décrites en détail dan paragraphes 6.3.1, pour les requêtes, respectivement 6.3.2, pour les ré ses.

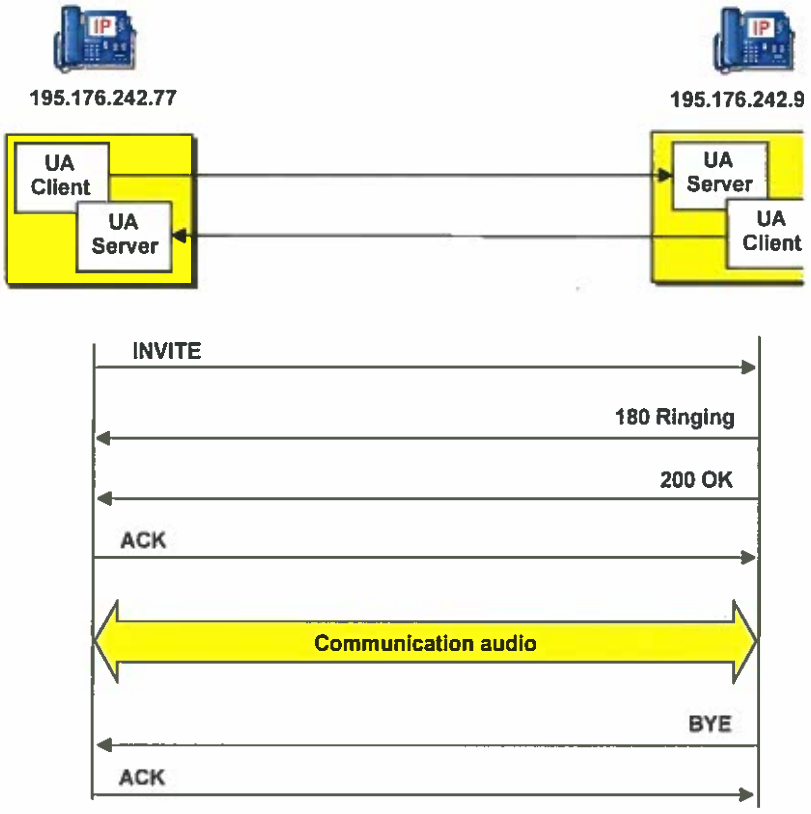

Figure 6-6: Etablissement direct d'une session audio

De nombreux autres cas de signalisation faisant intervenir le serveu redirection, le proxy et des passerelles sont décrits dans le chapitre 6.

6.4.1 Requêtes SIP (méthodes)

Les messages sont formatés conformément à la RFC 822 "Standard for the format of ARPA internet text messages". Le protocole SIP utilise les méthodes listées dans le tableau 6-6 pour invoquer les diverses actions de signalisation. Les 6 premières font partie de la version originale de SIP, spécifiée dans la RFC 2543. Les autres sont décrites dans des documents séparés.

Requête SIP: (méthode)	Description:
INVITE	invite l'usager à établir une session multimédia
ACK	permet d'accuser réception d'un message INVITE
BYE	clôt une session entre deux usagers
CANCEL	clôt une requête
OPTIONS	livre des informations concernant les paramètres de communication possibles
REGISTER	permet à un usager de s'enregistrer auprès d'un serveur d'enregistrement (Registrar)
INFO	permet d'envoyer des messages de signalisation en cours de session
PRACK	sert à envoyer un accusé de réception provisoire (Provisional Response ACKnowledgement, RFC 3262)
SUBSCRIBE	méthode permettant d'abonner un usager à une liste d'événements (RFC 3265).
NOTIFY	permet d'informer un usager d'un événement auquel il est abonné (RFC 3265).
UPDATE	méthode permettant de mettre à jour les paramètres d'une session (RFC 3311)
MESSAGE	permet de transférer de la messagerie instantanée (RFC 3428)
REFER	demande au destinataire de prêter attention à une autre requête contenue dans le message (p.ex. identification d'un service supplémentaire).

Tableau 6-2: Requêtes SIP

Comme illustré dans la figure 6-7, chaque requête SIP renferme la
gnation de la méthode (p. ex. INVITE), un ou plusieurs en-têtes (he
fields), ainsi que le corps du message (payload, body).

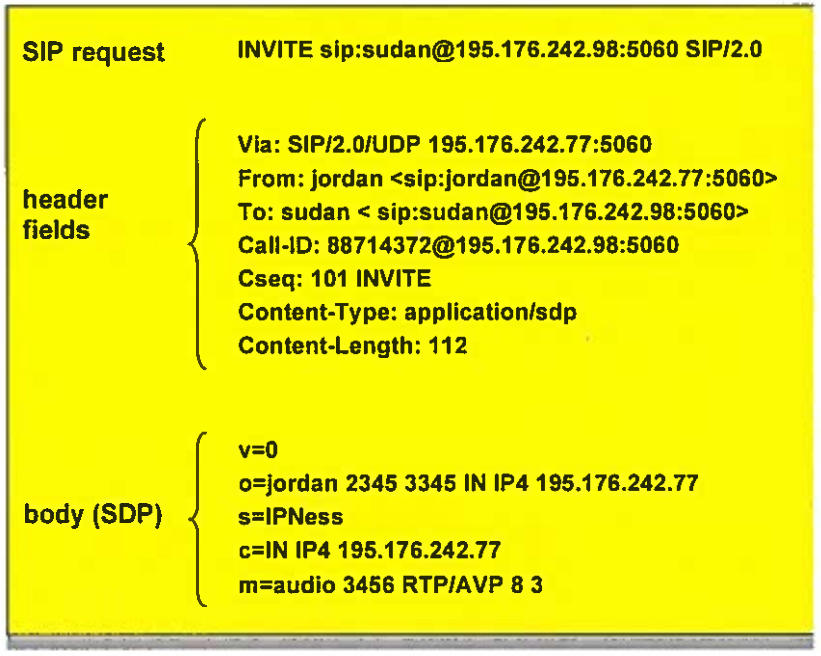

Figure 6-7: Champs d'une requête SIP (request)

- Le champ *Via* contient la liste des serveurs rencontrés sur la route
  la destination. Ainsi, les requêtes peuvent être acheminées s
  même parcours.
- Les champs *To* et *From* contiennent les adresses des usagers ap
  et appelant. Les adresses ont le format d'URL (Unified Resc
  Locators) SIP. Elles ont le même format que les adresses de me
  gerie électronique (e-mail).
- Le champ *Call-ID* contient un identificateur univoque de la f
  session.

- Le champ *Cseq* renferme le numéro de la séquence de commande. La valeur est incrémentée pour chaque nouvelle requête correspondant au même identificateur *Call-ID*. Le comptage ne doit pas obligatoirement débuter à 1 mais la valeur doit toujours représenter un nombre entier.
- Le champ *Content-Type* spécifie selon quel format la session multimédia sera décrite. Actuellement, seul SDP (Session Description Protocol) est utilisé [RFC 2327].
- Le champ *Content-Length* indique combien d'octets sont contenus dans le corps du message.

La description de la session à établir est basée sur le protocole SDP (Session Description Protocol), spécifié dans la RFC 2327. Elle comprend, entre autres, les champs suivants:

- le numéro de version du protocole (*protocol Version*, v=0),
- l'initiateur de la session et son identification univoque (*owner/ creator* and session identifier, o=...),
- la description de la session (*session name*, s=...),
- l'adresse IP vers laquelle les flux informationnels des médias utilisés devront être dirigés (*connection information*, c=...),
- la spécification du flux informationnel, contenant le type de flux: G.723.1, H.261, etc., le protocole de transport et le port à utiliser: RTP 3456, (*media name and transport address*, m=...),
- Les 6 principales méthodes utilisées dans SIP sont décrites plus en détail dans les paragraphes suivants.

```
Captured on 07.10.06 at 08:58:27

---------- ETHER Header ----------
ETHER: Destination: 00-01-02-A1-9D-F4
ETHER: Source: 00-03-6B-C9-7A-06
       :

---------- IP Header ----------
IP: Version = 4
       :
IP: Source address = 160.98.31.160
IP: Destination address = 160.98.30.200

---------- UDP Header ----------
UDP: Source port = 50287
UDP: Destination port = 5060
UDP: Length = 735
UDP: Checksum = 0

---------- SIP Header ----------
SIP: Message Type = Request
SIP: Method = INVITE
SIP: Request URI = sip:sudan@195.176.242.98:5060
SIP: SIP Version = SIP/2.0
SIP: Via = SIP/2.0/UDP 195.176.242.77:5060
SIP: From = jordan <sip:jordan@195.176.242.77:5060
SIP: To = sudan <sip:sudan@195.176.242.98:5060>
SIP: Call-ID = 88714372@195.176.242.77:5060
SIP: Cseq = 101 INVITE
SIP: Content-Type = application/sdp
SIP: Content-Length = 112

---------- SDP Header ----------
SDP: V = 0
SDP: O = jordan 2345 3345 IN IP4 195.176.242.77
SDP: S = IPNess
SDP: C = IN IP4 195.176.242.77
SDP: M = audio 2410 RTP/AVP 0
```

Figure 6-8: Extrait de l'analyse d'un message

Les six méthodes les plus importantes utilisées dans SIP sont décrites bièvement ci-après.

REGISTER

La méthode REGISTER permet à un usager de s'annoncer auprès du serveur d'enregistrement, afin de lui communiquer l'adresse IP et l'URL qui permettront de l'atteindre.

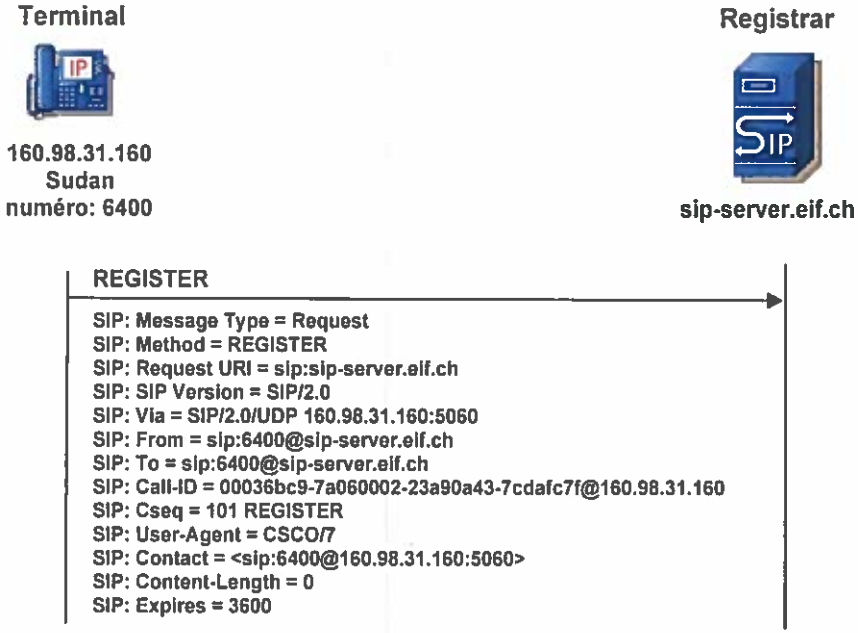

Figure 6-9: Méthode REGISTER

L'enregistrement d'un nouvel usager auprès du serveur SIP local peut se faire, soit en envoyant le message REGISTER à l'adresse multicast "sip.mcast.net" (224.0.1.75), soit en paramétrant l'adresse du serveur d'enregistrement dans le terminal, afin que ce dernier puisse envoyer le message REGISTER directement au serveur concerné.

Un agent d'usager a la possibilité d'établir des appels sortants l'intermédiaire de proxies, sans avoir été au préalable enregistré. contre, pour recevoir des appels entrants de la part des proxies desse le domaine, il doit être enregistré.

La figure 6-9 contient une analyse de protocole du message REGIS Les principaux champs ont déjà été décrits à la figure 6-7. Le mes REGISTER analysé ne contient pas de corps de message (Con Length=0). La valeur *Expires* indique la durée de validité de l'adress champ *Contact*.

INVITE

La méthode INVITE indique qu'un usager est invité à participer à une sion. Le corps de message contient une description de la session co pondante. La méthode INVITE peut être utilisée au début et en cour session.

Utilisée au début de la session, elle permet d'initier le processus d'éta sement d'une connexion audio, vidéo ou multimédia. La méthode IN agit de façon similaire au message SETUP des environnements H.3 RNIS. En cours de communication, cette méthode sert, par exemp transférer un appel vers un autre usager ou à ajouter un participant à conférence.

Dans l'analyse de la figure 6-10, le corps de message, rédigé en SDP, 3 possibilités de codage audio (G.711 loi μ, G.711 loi A et G.729). Le t nal destinataire du message choisira l'algorithme qui lui semble adé pour générer le flux audio en retour.

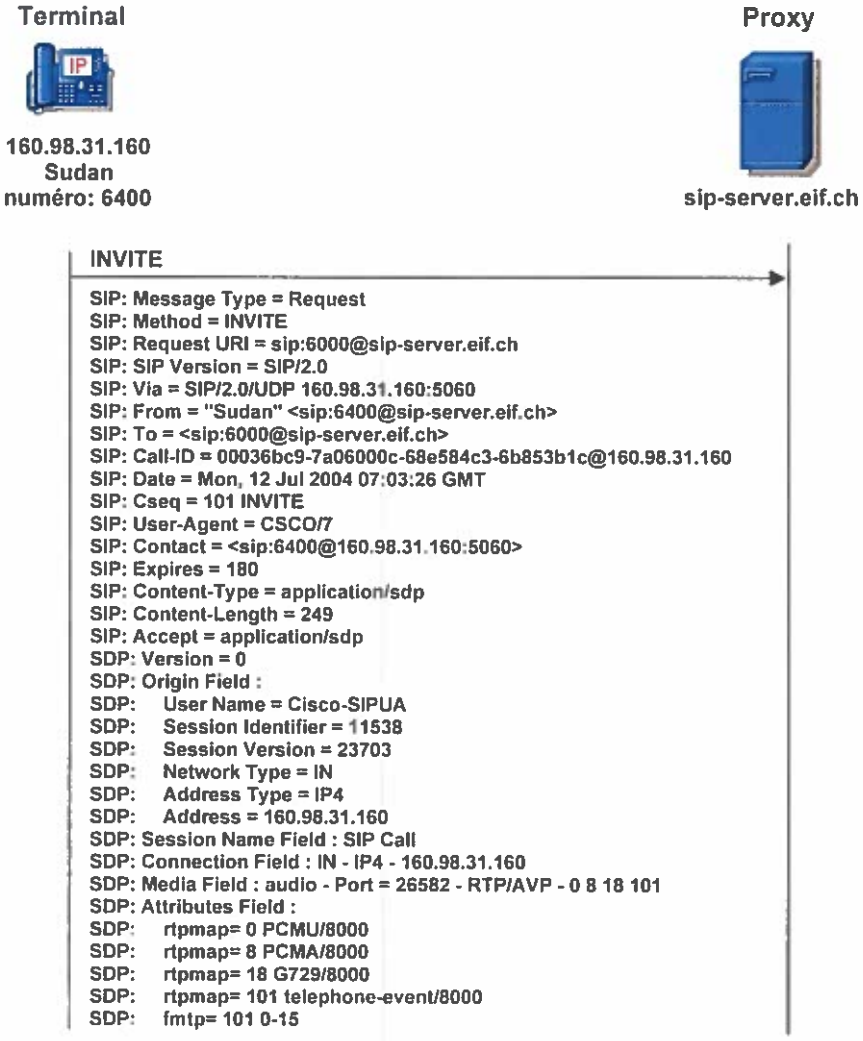

Figure 6-10: Méthode INVITE

ACKnowledge

La méthode ACKnowledge permet à l'usager qui a initié une commu tion, par un message INVITE, d'envoyer la confirmation finale d'étab ment de la session. Ce message confirme la réception des message réponse reçus de l'agent destinataire (p. ex. trying, ringing, OK).

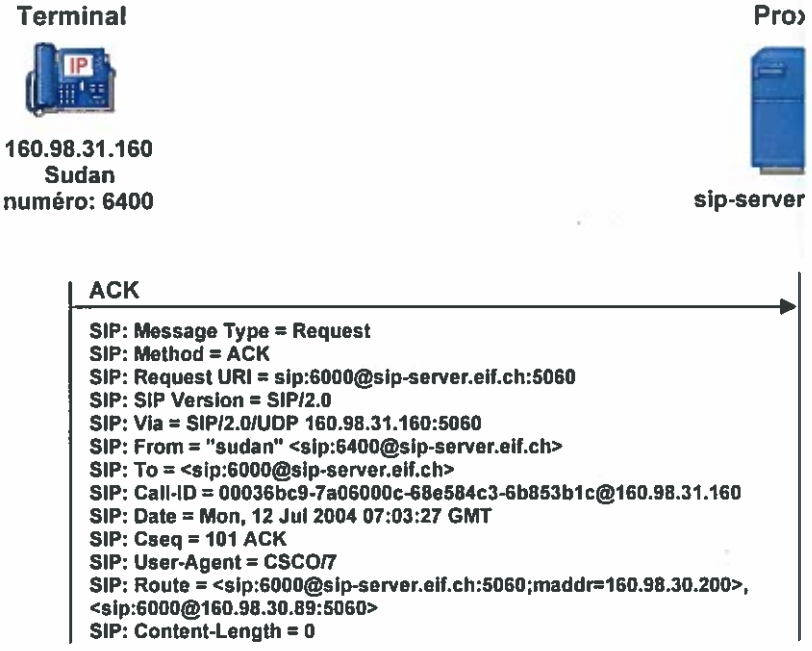

Figure 6-11: Méthode ACKnowledge

La méthode ACK peut contenir un corps de message, avec la descr de session que devra utiliser l'usager appelé. Si le corps de message est vide, l'usager appelé emploie la description de session du mes INVITE.

BYE

Un agent d'usager utilise BYE pour indiquer au serveur qu'il veut terminer la session. La requête BYE est expédiée de manière similaire à INVITE. Elle peut être envoyée par l'appelant ou par l'appelé. Un membre de session devrait normalement envoyer cette requête avant de quitter la session. Le membre recevant le BYE doit immédiatement cesser d'émettre le flux informationnel vers le membre qui s'est annoncé partant.

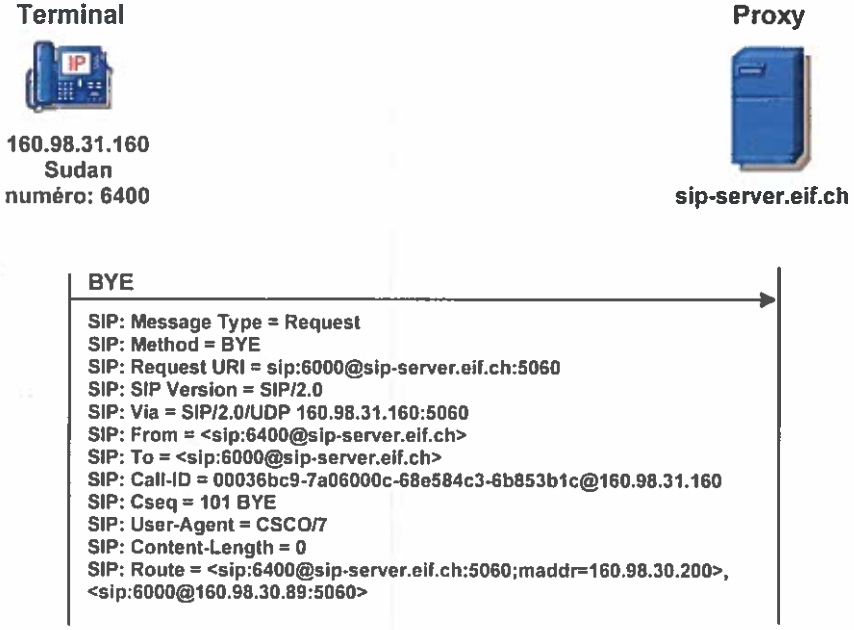

Figure 6-12: Méthode BYE

Si le message INVITE contenait un champ *Contact* dans l'en-tête, le destinataire doit envoyer la requête BYE à cette adresse, plutôt qu'à l'adresse *From*.

CANCEL

La méthode CANCEL annule une requête en cours caractérisée par mêmes valeurs d'en-tête *Call-ID*, *To*, *From* et *Cseq*. Elle n'affecte pas requête achevée. Le proxy qui reçoit un message CANCEL l'achemine toutes les destinations ayant des requêtes en cours. Un agent d'usage a reçu un CANCEL ne doit plus émettre de réponse 2xx pour le mess annulé.

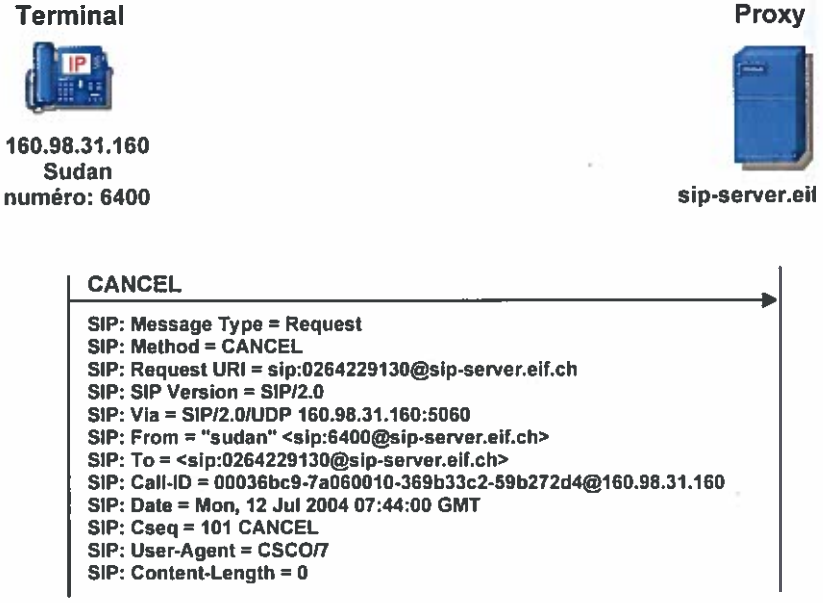

Figure 6-13: Méthode CANCEL

Dans l'analyse de protocole de la figure 6-13, la requête CANCEL l'émission d'une requête INVITE. Le terminal stoppe ainsi l'établisser d'une communication avec un usager RNIS correspondant au numéro 422 91 30.

OPTIONS

La méthode OPTIONS permet de questionner un serveur ou un agent d'usager sur ses capacités.

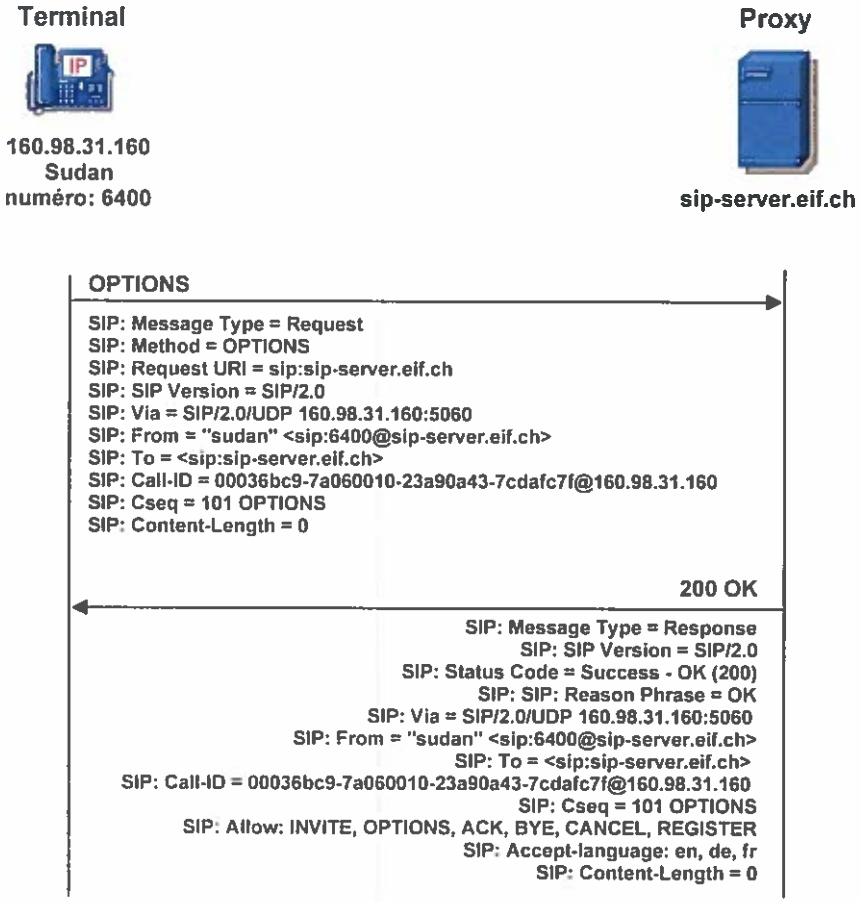

Figure 6-14: Méthode OPTIONS

La réponse sera similaire à celle donnée à une requête INVITE. informera de la possibilité de répondre à un appel (p. ex. réponse classe 4xx ou 6xx pour indiquer l'impossibilité d'accepter un appel). réponse de la classe 2xx peut contenir, dans le champ *Allow*, une liste méthodes supportées.

6.4.2 Réponses SIP

Les réponses SIP ou messages d'état sont identiques à celles du prot HTTP (Hypertext Transfer Protocol). Le tableau 6-7 donne un aperçu classes de réponses. Les réponses elles-mêmes sont décrites dan paragraphes suivants, en conservant la terminologie anglaise de la RF

Classes de réponses:	Exemples:
Informational responses	100 Trying, 180 Ringing, 181 Call is being forwarded
Successful responses	200 Ok, 202 Accepted
Redirection responses	300 Multiple choices, 301 Moved permaner 302 Moved temporarily
Client request failure responses	400 Bad request, 401 Unauthorized, 486 Bu here
Server failure responses	500 Server internal error, 503 Service unavailable
Global failure responses	600 Busy everywhere, 60 Decline

Tableau 6-7: Classes de réponses SIP

Toutes les réponses à une requête donnée contiennent la même v dans les champs *Call-ID*, *CSeq*, *To*, et *From* que la valeur contenue da requête. Ceci permet de mettre en correspondance les réponses ave requêtes.

"Informational responses"

100 Trying: Cette réponse permet d'indiquer qu'une action est en cours de traitement. Elle peut être émise par un agent d'usager ou un serveur proxy. Elle est uniquement utilisée de bond en bond et n'est jamais relayée plus loin. Elle confirme que la requête a été reçue par le serveur et stoppe l'émission des messages INVITE auprès de l'agent d'usager source.

180 Ringing: Cette réponse indique que l'agent d'usager destinataire a été trouvé. Le terminal du destinataire génère ce message pour indiquer qu'il a reçu la requête et qu'il attend que l'on veuille bien "décrocher".

181 Call is Being Forwarded: Cette réponse indique que la requête a été déviée vers un autre destinataire.

182 Queued: Cette réponse informe que l'usager appelé n'est pas atteignable pour le moment. L'appel a été mis en attente plutôt que d'être rejeté.

183 Session Progress: Cette réponse est envoyée par une passerelle lorsqu'elle reçoit du réseau RNIS un message qui contient l'élément *Progress indicator*. L'envoi de cette réponse permet d'indiquer au terminal SIP appelant que de l'information est envoyée dans la bande vocale (p. ex. tonalité).

"Successful responses"

200 OK: Cette réponse informe que la requête a été traitée avec succès.

202 Accepted: Cette réponse informe que la requête a été comprise, mais l'autorisation est en cours ou n'a pas encore été donnée.

"Redirection responses"

300 MultipleChoices: Cette réponse indique que l'adresse a été résolue mais qu'elle conduit vers plusieurs sites. Les adresses de tous les sites sont fournies. L'usager a le choix de l'adresse qu'il va utiliser.

301 MovedPermanently: Cette réponse indique que l'usager n'est plus atteignable à l'adresse requise. Une adresse alternative est jointe dans l'en-tête.

302 Moved Temporarily: Cette réponse informe que l'adresse requis momentanément atteignable à une autre adresse. La nou adresse est indiquée dans le champ *Contact*.

305 Use Proxy: Cette réponse indique que l'usager appelant doit u les services d'un proxy pour entrer en contact avec l'usager appel

380 AlternateService: Cette réponse informe que l'appel a échoué, que d'autres services sont disponibles.

"Client request failure responses"

400 Bad Request: Cette réponse indique que la requête n'a pas pu comprise à cause d'un format illégal.

401 Unauthorized: Cette réponse indique que la requête l'authentification d'utilisateur.

402 Payment Required: Cette réponse indique que l'on exige paie pour que l'appel puisse être traité avec succès.

403 Forbidden: Cette réponse indique que le serveur a reçu et a co la requête, mais ne fournira pas le service.

404 Not Found: Cette réponse indique que le serveur a connaissanc l'utilisateur n'existe pas dans le domaine indiqué.

405 Method Not Allowed: Cette réponse indique que la méthode ut dans la requête n'est pas acceptée. La réponse contient une list méthodes permises.

406 Not Acceptable: Cette réponse indique que la ressource requis uniquement en mesure de produire des réponses qui ont des car ristiques de contenus non acceptables par rapport aux spécifica du champ d'en-tête.

407 Proxy Authentication Required: Cette réponse est semblable à *Unauthorized response*. Cependant, elle indique que le client d'abord s'authentifier auprès du proxy.

408 Request Timeout: Cette réponse indique que le serveur n'a pas é mesure de répondre avant l'expiration du temporisateur.

409 Conflict: Cette réponse indique que la requête n'a pas pu être trai cause d'un conflit avec l'état actuel de la ressource.

410 Gone: Cette réponse indique qu'une ressource n'est plus dispo pour le serveur et qu'aucune adresse de réexpédition n'est connu

411 *Length required:* Cette réponse indique que l'usager refuse d'accepter la requête sans une longueur définie du contenu.

413 *Request Entity Too Large:* Cette réponse indique que le serveur refuse de traiter la requête parce qu'elle est plus grande que ce que le serveur désire offrir ou est capable de traiter.

414 *Request URI Too Long:* Cette réponse indique que le serveur refuse de traiter la requête parce que l'URI est trop long pour pouvoir être interprété par le serveur.

415 *Unsupported Media Type:* Cette réponse indique que le serveur refuse de traiter la requête parce que le format du corps de message ne correspond pas aux possibilités offertes par la destination.

416 *Unsupported URI Scheme:* Cette réponse indique que le serveur ne reconnaît pas le format d'URI.

420 *Bad Extension:* Cette réponse indique que le serveur ne comprend pas l'extension de protocole spécifiée dans l'en-tête de la requête.

421 *Extension Required:* Cette réponse indique que le serveur a besoin de certaines extensions pour traiter la requête.

423 *Interval Too Brief:* Cette réponse indique que le temps d'expiration spécifié dans la requête est trop court.

480 *Temporarily Unavailable:* Cette réponse indique que l'appelé a été contacté, mais est temporairement indisponible.

481 *Call/Transaction Does Not Exist:* Cette réponse indique que le serveur ignore la requête parce qu'il s'agit soit d'un BY, pour lequel il n'y avait aucune ID correspondante, soit d'un CANCEL, pour lequel il n'y avait aucune transaction correspondante.

482 *LoopDetected:* Cette réponse indique que le serveur a reçu une requête qui s'est incluse elle-même dans la même route.

483 *Too Many Hops:* Cette réponse indique que le serveur a reçu une requête qui a exigé plus de bonds que permis par le champ d'en-tête *Max-Forwards*.

484 *Address Incomplete:* Cette réponse indique que le serveur a reçu une requête contenant une adresse incomplète.

485 *Ambiguous:* Cette réponse indique que le serveur a reçu une requête dans laquelle l'adresse de l'usager appelé était ambiguë. Il peut fournir des adresses de remplacement.

486 *Busy Here:* Cette réponse indique que l'on est entré en contact le destinataire, mais que son système est incapable de traiter appels supplémentaires.

487 *Request Terminated:* Cette réponse indique que la requête a terminée par un message *BYE* ou un message *CANCEL*.

488 *Not Acceptable Here:* Cette réponse indique qu'il n'y a pas corres dance des caractéristiques.

491 *Request Pending:* Cette réponse indique qu'une requête est en pens.

493 *Undecipherable:* Cette réponse indique que le contenu n'est déchiffrable.

"Server failure responses"

500 *Server Internal Error:* Cette réponse indique que le serveur passerelle a rencontré une erreur inattendue qui l'a empêché de t la requête.

501 *Not Implemented:* Cette réponse indique que le serveur ou la pa relle n'offre pas les fonctions exigées pour achever la requête.

502 *Bad Gateway:* Cette réponse indique que le serveur ou la passer reçu une réponse invalide d'un serveur en aval.

503 *Service Unavailable:* Cette réponse indique que le serveur passerelle est incapable de traiter la requête en raison d'un prob de maintenance ou d'une surcharge.

504 *Server Time-out:* Cette réponse indique que le serveur ou la pa relle n'a pas reçu de réponse opportune d'un autre serveur (co un serveur de localisation).

505 *Version Not Supported:* Cette réponse indique que le serveur passerelle ne soutient pas la version du protocole de SIP empl dans la requête.

513 *Message Too Large:* Cette réponse indique que la longueur du sage dépasse la longueur maximale acceptée par le serveur.

"Global failure responses"

600 *Busy Everywhere:* Cette réponse indique qu'il y a eu contact avec le destinataire, mais que ce dernier est occupé et ne peut pas prendre d'appel pour l'instant.

603 *Decline:* Cette réponse indique qu'il y a eu contact avec le destinataire, mais que ce dernier ne peut ou ne veut pas participer à la session.

604 *Does Not Exist Anywhere:* Cette réponse indique que le serveur est informé que le destinataire n'existe pas dans le réseau.

606 *Not Acceptable:* Cette réponse indique qu'il y a eu contact avec le destinataire, mais qu'un aspect quelconque de la description de session était inacceptable.

6.5 Exemples de signalisation

6.5.1 Enregistrement d'un terminal SIP

Un enregistrement est opéré lorsqu'un usager doit informer un proxy ou un serveur de redirection de son emplacement. Durant la procédure d'enregistrement, l'usager envoie une requête REGISTER au serveur. Celle-ci inclut l'adresse, voire les adresses auxquelles il peut être atteint.

Les usagers s'enregistrent auprès du serveur avec leurs adresses SIP. Le serveur d'enregistrement fournit cette information au serveur de localisation, à la demande.

Dans l'analyse de la figure 6-15, le terminal s'est enregistré auprès du serveur lorsqu'il a été mis sous tension. La requête REGISTER renferme son numéro de téléphone (no interne 6400), son adresse IP (160.98.30.88), ainsi que le numéro de port UDP à utiliser pour la signalisation (port par défaut: 5060).

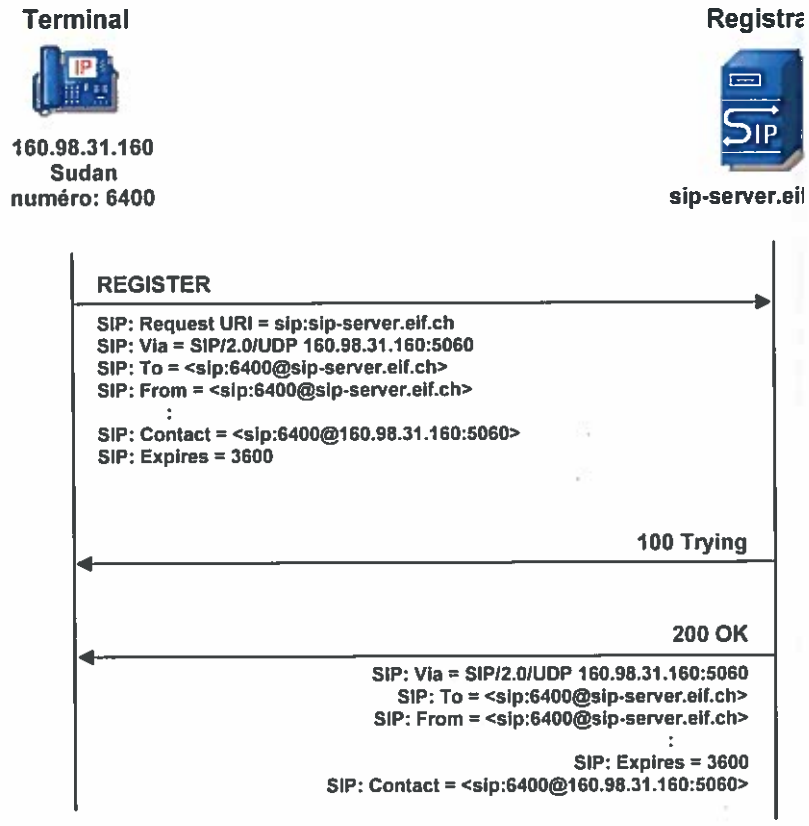

Figure 6-15: Procédure d'enregistrement

6.5.2 Etablissement de session audio entre deux terminaux SIP

Un exemple typique d'établissement de session SIP commence par l' du message INVITE par l'agent d'usager A. Si l'usager A connaît l'ad IP de l'usager B, la session peut être établie directement.

Dans l'exemple de la figure 6-16, l'usager A requiert l'établissement session sur le port UDP 26582, avec un codage audio selon G.711 loi