

UIT-T

SECTEUR DE LA NORMALISATION
DES TÉLÉCOMMUNICATIONS
DE L'UIT

Q.3402

(02/2008)

SÉRIE Q: COMMUTATION ET SIGNALISATION

Spécifications et protocoles de signalisation pour les réseaux de prochaine génération – Protocoles de commande de service et de session

Profil de signalisation au niveau de l'interface utilisateur-réseau dans les réseaux de prochaine génération (ensemble 1 de protocoles)

Recommandation UIT-T Q.3402

RECOMMANDATIONS UIT-T DE LA SÉRIE Q
COMMUTATION ET SIGNALISATION

SIGNALISATION DANS LE SERVICE MANUEL INTERNATIONAL	Q.1–Q.3
EXPLOITATION INTERNATIONALE AUTOMATIQUE ET SEMI-AUTOMATIQUE	Q.4–Q.59
FONCTIONS ET FLUX D'INFORMATION DES SERVICES DU RNIS	Q.60–Q.99
CLAUSES APPLICABLES AUX SYSTÈMES NORMALISÉS DE L'UIT-T	Q.100–Q.119
SPÉCIFICATIONS DES SYSTÈMES DE SIGNALISATION N° 4, 5, 6, R1 ET R2	Q.120–Q.499
COMMUTATEURS NUMÉRIQUES	Q.500–Q.599
INTERFONCTIONNEMENT DES SYSTÈMES DE SIGNALISATION	Q.600–Q.699
SPÉCIFICATIONS DU SYSTÈME DE SIGNALISATION N° 7	Q.700–Q.799
INTERFACE Q3	Q.800–Q.849
SYSTÈME DE SIGNALISATION D'ABONNÉ NUMÉRIQUE N° 1	Q.850–Q.999
RÉSEAUX MOBILES TERRESTRES PUBLICS	Q.1000–Q.1099
INTERFONCTIONNEMENT AVEC LES SYSTÈMES MOBILES À SATELLITES	Q.1100–Q.1199
RÉSEAU INTELLIGENT	Q.1200–Q.1699
PRESCRIPTIONS ET PROTOCOLES DE SIGNALISATION POUR LES IMT-2000	Q.1700–Q.1799
SPÉCIFICATIONS DE LA SIGNALISATION RELATIVE À LA COMMANDE D'APPEL INDÉPENDANTE DU SUPPORT	Q.1900–Q.1999
RNIS À LARGE BANDE	Q.2000–Q.2999
SPÉCIFICATIONS ET PROTOCOLES DE SIGNALISATION POUR LES RÉSEAUX DE PROCHAINE GÉNÉRATION	Q.3000–Q.3999
Généralités	Q.3000–Q.3029
Architecture fonctionnelle de signalisation et de commande de réseau	Q.3030–Q.3099
Organisation des données de réseau dans les réseaux de prochaine génération	Q.3100–Q.3129
Signalisation de commande de support	Q.3130–Q.3179
Spécifications et protocoles de signalisation et de commande pour le rattachement aux environnements des réseaux de prochaine génération	Q.3200–Q.3249
Protocoles de commande des ressources	Q.3300–Q.3369
Protocoles de commande de service et de session	Q.3400–Q.3499
Protocoles de commande de service et de session – Services complémentaires	Q.3600–Q.3649
Applications des réseaux de prochaine génération	Q.3700–Q.3849
Tests applicables aux réseaux de prochaine génération	Q.3900–Q.3999

Pour plus de détails, voir la Liste des Recommandations de l'UIT-T.

Recommandation UIT-T Q.3402

Profil de signalisation au niveau de l'interface utilisateur-réseau dans les réseaux de prochaine génération (ensemble 1 de protocoles)

Résumé

La Recommandation UIT-T Q.3402 définit, pour les réseaux de prochaine génération (NGN, *next generation network*), le profil de signalisation au niveau de l'interface utilisateur-réseau (UNI, *user-to-network interface*) à employer entre utilisateurs et réseaux utilisant l'ensemble 1 de protocoles, dans le cas de services de téléphonie, de services vidéos et de services de données.

Historique

Edition	Recommandation	Approbation	Commission d'études	ID unique*
1.0	ITU-T Q.3402	2008-02-29	11	11.1002/1000/9344

Mots clés

Réseau de prochaine génération (NGN), profil, protocole de description de session (SDP), signalisation, protocole d'ouverture de session (SIP).

* Pour accéder à la Recommandation, reporter cet URL <http://handle.itu.int/> dans votre navigateur Web, suivi de l'identifiant unique, par exemple <http://handle.itu.int/11.1002/1000/11830-en>.

AVANT-PROPOS

L'Union internationale des télécommunications (UIT) est une institution spécialisée des Nations Unies dans le domaine des télécommunications et des technologies de l'information et de la communication (ICT). Le Secteur de la normalisation des télécommunications (UIT-T) est un organe permanent de l'UIT. Il est chargé de l'étude des questions techniques, d'exploitation et de tarification, et émet à ce sujet des Recommandations en vue de la normalisation des télécommunications à l'échelle mondiale.

L'Assemblée mondiale de normalisation des télécommunications (AMNT), qui se réunit tous les quatre ans, détermine les thèmes d'étude à traiter par les Commissions d'études de l'UIT-T, lesquelles élaborent en retour des Recommandations sur ces thèmes.

L'approbation des Recommandations par les Membres de l'UIT-T s'effectue selon la procédure définie dans la Résolution 1 de l'AMNT.

Dans certains secteurs des technologies de l'information qui correspondent à la sphère de compétence de l'UIT-T, les normes nécessaires se préparent en collaboration avec l'ISO et la CEI.

NOTE

Dans la présente Recommandation, l'expression "Administration" est utilisée pour désigner de façon abrégée aussi bien une administration de télécommunications qu'une exploitation reconnue.

Le respect de cette Recommandation se fait à titre volontaire. Cependant, il se peut que la Recommandation contienne certaines dispositions obligatoires (pour assurer, par exemple, l'interopérabilité et l'applicabilité) et considère que la Recommandation est respectée lorsque toutes ces dispositions sont observées. Le futur d'obligation et les autres moyens d'expression de l'obligation comme le verbe "devoir" ainsi que leurs formes négatives servent à énoncer des prescriptions. L'utilisation de ces formes ne signifie pas qu'il est obligatoire de respecter la Recommandation.

DROITS DE PROPRIÉTÉ INTELLECTUELLE

L'UIT attire l'attention sur la possibilité que l'application ou la mise en œuvre de la présente Recommandation puisse donner lieu à l'utilisation d'un droit de propriété intellectuelle. L'UIT ne prend pas position en ce qui concerne l'existence, la validité ou l'applicabilité des droits de propriété intellectuelle, qu'ils soient revendiqués par un membre de l'UIT ou par une tierce partie étrangère à la procédure d'élaboration des Recommandations.

A la date d'approbation de la présente Recommandation, l'UIT n'avait pas été avisée de l'existence d'une propriété intellectuelle protégée par des brevets à acquérir pour mettre en œuvre la présente Recommandation. Toutefois, comme il ne s'agit peut-être pas de renseignements les plus récents, il est vivement recommandé aux développeurs de consulter la base de données des brevets du TSB sous <http://www.itu.int/ITU-T/ipr/>.

© UIT 2015

Tous droits réservés. Aucune partie de cette publication ne peut être reproduite, par quelque procédé que ce soit, sans l'accord écrit préalable de l'UIT.

TABLE DES MATIÈRES

	Page
1	Domaine d'application 1
2	Références..... 1
2.1	Références de l'UIT et de l'ISO/CEI..... 1
2.2	Références de l'IETF 2
2.3	Références de l'ETSI 6
2.4	Autres références 6
3	Définitions 6
4	Abréviations..... 7
5	Modèle de référence 8
6	Hypothèses..... 10
7	Mise à disposition des médias au cours d'une session SIP 11
7.1	Considérations relatives aux paquets médias 11
8	Codec 11
8.1	Liste de codecs 11
8.2	Taille de mise en paquets 12
9	Routage et adressage..... 13
10	Profil de signalisation applicable au niveau service 13
10.1	Normes RFC (<i>requests for comments</i> , demandes d'observations) à prendre en charge 13
10.2	Profils SIP..... 18
10.3	Profil SDP..... 38
11	Profil applicable au niveau transport 39
11.1	Spécifications à prendre en charge 39
11.2	Traitement multifréquence bitonalité 41
12	Transport de signalisation de commande d'appel 41
13	Version du protocole IP 41
14	Considérations d'ordre sécuritaire..... 41
	Appendice I – Exemples de flux d'appel..... 42
I.1	Scénario de réussite de l'établissement de session SIP..... 42
I.2	Scénario d'échec de l'établissement de session SIP..... 43
I.3	Echec par non-réponse à l'annulation d'un appel..... 44
I.4	Echec de l'établissement d'un appel..... 45
	Bibliographie..... 46

Recommandation UIT-T Q.3402

Profil de signalisation au niveau de l'interface utilisateur-réseau dans les réseaux de prochaine génération (ensemble 1 de protocoles)

1 Domaine d'application

La présente Recommandation spécifie un profil applicable au niveau service, c'est-à-dire les informations échangées au niveau de l'interface, dans le cadre des protocoles SIP/SDP, entre un utilisateur et un réseau. Elle spécifie également un profil applicable au niveau transport, reposant par exemple sur le protocole de transport en temps réel (RTP).

La présente Recommandation, fondée sur l'ensemble 1 de protocoles du profil UNI NGN, s'applique au multimédia (téléphonie, vidéo et données), notamment à la téléphonie IP (VoIP), à la téléphonie multimédia, à la numérotation multifréquence bitonalité (DTMF), à la télécopie T.38, ainsi qu'aux tonalités de retour d'appel et d'appel et aux annonces multimédias.

La présente Recommandation englobe tous les types de terminaux, par exemple, une passerelle résidentielle SIP, un téléphone SIP ou un commutateur privé (PBX) IP SIP. En conséquence, les interfaces UNI suivantes sont définies:

- L'interface de raccordement d'une passerelle résidentielle SIP à un fournisseur de services, permettant de relier les terminaux RTPC/RNIS ou les téléphones IP à une passerelle résidentielle.
- L'interface de raccordement d'un téléphone SIP à un fournisseur de services, ce téléphone SIP pouvant être un téléphone logiciel ou un téléphone matériel, mis en oeuvre conformément aux spécifications SIP applicables au sous-système multimédia IP (IMS, *IP multimedia subsystem*).
- L'interface de raccordement d'un commutateur PBX IP SIP à un fournisseur de services, ce commutateur PBX pouvant être un intermédiaire ou un agent d'utilisateur de boucle locale (B2BUA).

2 Références

La présente Recommandation se réfère à certaines dispositions des Recommandations UIT-T et textes suivants qui, de ce fait, en sont partie intégrante. Les versions indiquées étaient en vigueur au moment de la publication de la présente Recommandation. Toute Recommandation ou tout texte étant sujet à révision, les utilisateurs de la présente Recommandation sont invités à se reporter, si possible, aux versions les plus récentes des références normatives suivantes. La liste des Recommandations de l'UIT-T en vigueur est régulièrement publiée. La référence à un document figurant dans la présente Recommandation ne donne pas à ce document, en tant que tel, le statut d'une Recommandation.

2.1 Références de l'UIT et de l'ISO/CEI

- [UIT-T G.711] Recommandation UIT-T G.711 (1988), *Modulation par impulsions et codage (MIC) des fréquences vocales.*
- [UIT-T G.722] Recommandation UIT-T G.722 (1988), *Codage audiofréquence à 7 kHz à un débit inférieur ou égal à 64 kbit/s.*
- [UIT-T G.722.1] Recommandation UIT-T G.722.1 (2005), *Codage à faible complexité aux débits de 24 et 32 kbit/s pour utilisation en mains-libres sur les systèmes à faible perte de trames.*
- [UIT-T G.722.2] Recommandation UIT-T G.722.2 (2003), *Codage vocal à large bande à 16 kbit/s environ par codage adaptatif multidébit à large bande (AMR-WB).*

- [UIT-T G.726] Recommandation UIT-T G.726 (1990), *Modulation par impulsions et codage différentiel adaptatif (MICDA) à 40, 32, 24, 16 kbit/s.*
- [UIT-T G.729] Recommandation UIT-T G.729 (2007), *Codage de la parole à 8 kbit/s par prédiction linéaire avec excitation par séquences codées à structure algébrique conjuguée.*
- [UIT-T G.729.1] Recommandation UIT-T G.729.1 (2006), *Codeur intégré à débit variable basé sur le vocodeur G.729: Codeur à flux binaire modulable à large bande à 8-32 kbit/s interopérable avec le codeur G.729.*
- [UIT-T H.263] Recommandation UIT-T H.263 (2005), *Codage vidéo pour communications à faible débit.*
- [UIT-T H.264] Recommandation UIT-T H.264 (2005), *Codage vidéo évolué pour les services audiovisuels génériques.*
- [UIT-T T.38] Recommandation UIT-T T.38 (2007), *Procédures de communication de télécopie du Groupe 3 en temps réel sur les réseaux à protocole Internet.*
- [UIT-T T.140] Recommandation UIT-T T.140 (1998), *Protocole de conversation en mode texte pour application multimédia.*
- [UIT-T Y.2012] Recommandation UIT-T Y.2012 (2006), *Prescriptions et architecture fonctionnelles du réseau de prochaine génération version 1.*
- [ISO/CEI 14496-2] ISO/CEI 14496-2:2004, *Technologies de l'information – Codage des objets audiovisuels – Partie 2: Codage visuel.*
- [ISO/CEI 14496-3] ISO/CEI 14496-3:2005, *Technologies de l'information – Codage des objets audiovisuels – Partie 3: Codage audio.*

2.2 Références de l'IETF

2.2.1 Spécifications de signalisation applicables au niveau service

- [IETF RFC 2046] IETF RFC 2046 (1996), *Multipurpose Internet Mail Extensions (MIME) Part Two: Media Types.*
- [IETF RFC 2327] IETF RFC 2327 (1998), *SDP: Session Description Protocol.*
- [IETF RFC 2617] IETF RFC 2617 (1999), *HTTP Authentication: Basic and Digest Access Authentication.*
- [IETF RFC 2976] IETF RFC 2976 (2000), *The SIP INFO Method.*
- [IETF RFC 3261] IETF RFC 3261 (2002), *SIP: Session Initiation Protocol.*
- [IETF RFC 3262] IETF RFC 3262 (2002), *Reliability of Provisional Responses in the Session Initiation Protocol (SIP).*
- [IETF RFC 3263] IETF RFC 3263 (2002), *Session Initiation Protocol (SIP): Locating SIP Servers.*
- [IETF RFC 3264] IETF RFC 3264 (2002), *An Offer/Answer Model with the Session Description Protocol (SDP).*
- [IETF RFC 3265] IETF RFC 3265 (2002), *Session Initiation Protocol (SIP)-Specific Event Notification.*
- [IETF RFC 3310] IETF RFC 3310 (2002), *Hypertext Transfer Protocol (HTTP) Digest Authentication Using Authentication and Key Agreement (AKA).*

- [IETF RFC 3311] IETF RFC 3311 (2002), *The Session Initiation Protocol (SIP) UPDATE Method.*
- [IETF RFC 3312] IETF RFC 3312 (2002), *Integration of Resource Management and Session Initiation Protocol (SIP).*
- [IETF RFC 3313] IETF RFC 3313 (2003), *Private Session Initiation Protocol (SIP) Extensions for Media Authorization.*
- [IETF RFC 3320] IETF RFC 3320 (2003), *Signaling Compression (SigComp).*
- [IETF RFC 3323] IETF RFC 3323 (2002), *A Privacy Mechanism for the Session Initiation Protocol (SIP).*
- [IETF RFC 3324] IETF RFC 3324 (2002), *Short Term Requirements for Network Asserted Identity.*
- [IETF RFC 3325] IETF RFC 3325 (2002), *Private Extensions to the Session Initiation Protocol (SIP) for Asserted Identity within Trusted Networks.*
- [IETF RFC 3326] IETF RFC 3326 (2002), *The Reason Header Field for the Session Initiation Protocol (SIP).*
- [IETF RFC 3327] IETF RFC 3327 (2002), *Session Initiation Protocol (SIP) Extension Header Field for Registering Non-Adjacent Contacts.*
- [IETF RFC 3329] IETF RFC 3329 (2003), *Security Mechanism Agreement for the Session Initiation Protocol (SIP).*
- [IETF RFC 3388] IETF RFC 3388 (2002), *Grouping of Media Lines in the Session Description Protocol (SDP).*
- [IETF RFC 3420] IETF RFC 3420 (2002), *Internet Media Type message/sipfrag.*
- [IETF RFC 3428] IETF RFC 3428 (2002), *Session Initiation Protocol (SIP) Extension for Instant Messaging.*
- [IETF RFC 3455] IETF RFC 3455 (2003), *Private Header (P-Header) Extensions to the Session Initiation Protocol (SIP) for the 3rd-Generation Partnership Project (3GPP).*
- [IETF RFC 3485] IETF RFC 3485 (2003), *The Session Initiation Protocol (SIP) and Session Description Protocol (SDP) Static Dictionary for Signaling Compression (SigComp).*
- [IETF RFC 3486] IETF RFC 3486 (2003), *Compressing the Session Initiation Protocol (SIP).*
- [IETF RFC 3515] IETF RFC 3515 (2003), *The Session Initiation Protocol (SIP) Refer Method.*
- [IETF RFC 3524] IETF RFC 3524 (2003), *Mapping of Media Streams to Resource Reservation Flows.*
- [IETF RFC 3556] IETF RFC 3556 (2003), *Session Description Protocol (SDP) Bandwidth Modifiers for RTP Control Protocol (RTCP) Bandwidth.*
- [IETF RFC 3581] IETF RFC 3581 (2003), *An Extension to the Session Initiation Protocol (SIP) for Symmetric Response Routing.*
- [IETF RFC 3608] IETF RFC 3608 (2003), *Session Initiation Protocol (SIP) Extension Header Field for Service Route Discovery During Registration.*
- [IETF RFC 3680] IETF RFC 3680 (2004), *A Session Initiation Protocol (SIP) Event Package for Registrations.*

- [IETF RFC 3725] IETF RFC 3725 (2004), *Best Current Practices for Third Party Call Control (3pcc) in the Session Initiation Protocol (SIP)*.
- [IETF RFC 3824] IETF RFC 3824 (2004), *Using E.164 numbers with the Session Initiation Protocol (SIP)*.
- [IETF RFC 3840] IETF RFC 3840 (2004), *Indicating User Agent Capabilities in the Session Initiation Protocol (SIP)*.
- [IETF RFC 3841] IETF RFC 3841 (2004), *Caller Preferences for the Session Initiation Protocol (SIP)*.
- [IETF RFC 3842] IETF RFC 3842 (2004), *A Message Summary and Message Waiting Indication Event Package for the Session Initiation Protocol (SIP)*.
- [IETF RFC 3853] IETF RFC 3853 (2004), *S/MIME Advanced Encryption Standard (AES) Requirement for the Session Initiation Protocol (SIP)*.
- [IETF RFC 3856] IETF RFC 3856 (2004), *A Presence Event Package for the Session Initiation Protocol (SIP)*.
- [IETF RFC 3857] IETF RFC 3857 (2004), *A Watcher Information Event Template-Package for the Session Initiation Protocol (SIP)*.
- [IETF RFC 3858] IETF RFC 3858 (2004), *An Extensible Markup Language (XML) Based Format for Watcher Information*.
- [IETF RFC 3859] IETF RFC 3859 (2004), *Common Profile for Presence (CPP)*.
- [IETF RFC 3860] IETF RFC 3860 (2004), *Common Profile for Instant Messaging (CPIM)*.
- [IETF RFC 3861] IETF RFC 3861 (2004), *Address Resolution for Instant Messaging and Presence*.
- [IETF RFC 3862] IETF RFC 3862 (2004), *Common Presence and Instant Messaging (CPIM): Message Format*.
- [IETF RFC 3863] IETF RFC 3863 (2004), *Presence Information Data Format (PIDF)*.
- [IETF RFC 3891] IETF RFC 3891 (2004), *The Session Initiation Protocol (SIP) Replaces Header*.
- [IETF RFC 3892] IETF RFC 3892 (2004), *The Session Initiation Protocol (SIP) Referred-By Mechanism*.
- [IETF RFC 3903] IETF RFC 3903 (2004), *Session Initiation Protocol (SIP) Extension for Event State Publication*.
- [IETF RFC 3911] IETF RFC 3911 (2004), *The Session Initiation Protocol (SIP) Join Header*.
- [IETF RFC 3959] IETF RFC 3959 (2004), *The Early Session Disposition Type for the Session Initiation Protocol (SIP)*.
- [IETF RFC 3960] IETF RFC 3960 (2004), *Early Media and Ringing Tone Generation in the Session Initiation Protocol (SIP)*.
- [IETF RFC 3966] IETF RFC 3966 (2004), *The tel URI for Telephone Numbers*.
- [IETF RFC 3994] IETF RFC 3994 (2005), *Indication of Message Composition for Instant Messaging*.
- [IETF RFC 4028] IETF RFC 4028 (2005), *Session Timers in the Session Initiation Protocol (SIP)*.

- [IETF RFC 4032] IETF RFC 4032 (2005), *Update to the Session Initiation Protocol (SIP) Preconditions Framework.*
- [IETF RFC 4145] IETF RFC 4145 (2005), *TCP-Based Media Transport in the Session Description Protocol (SDP).*
- [IETF RFC 4168] IETF RFC 4168 (2005), *The Stream Control Transmission Protocol (SCTP) as a Transport for the Session Initiation Protocol (SIP).*
- [IETF RFC 4235] IETF RFC 4235 (2005), *An INVITE-Initiated Dialog Event Package for the Session Initiation Protocol (SIP).*
- [IETF RFC 4244] IETF RFC 4244 (2005), *An Extension to the Session Initiation Protocol (SIP) for Request History Information.*
- [IETF RFC 4320] IETF RFC 4320 (2006), *Actions Addressing Identified Issues with the Session Initiation Protocol's (SIP) Non-INVITE Transaction.*
- [IETF RFC 4412] IETF RFC 4412 (2006), *Communications Resource Priority for the Session Initiation Protocol (SIP).*
- [IETF RFC 4458] IETF RFC 4458 (2006), *Session Initiation Protocol (SIP) URIs for Applications such as Voicemail and Interactive Voice Response (IVR).*
- [IETF RFC 4480] IETF RFC 4480 (2006), *RPID: Rich Presence Extensions to the Presence Information Data Format (PIDF).*
- [IETF RFC 4483] IETF RFC 4483 (2006), *A Mechanism for Content Indirection in Session Initiation Protocol (SIP) Messages.*
- [IETF RFC 4566] IETF RFC 4566 (2006), *SDP: Session Description Protocol.*
- [IETF RFC 4575] IETF RFC 4575 (2006), *A Session Initiation Protocol (SIP) Event Package for Conference State.*
- [IETF RFC 4579] IETF RFC 4579 (2006), *Session Initiation Protocol (SIP) Call Control – Conferencing for User Agents.*
- [IETF RFC 4583] IETF RFC 4583 (2006), *Session Description Protocol (SDP) Format for Binary Floor Control Protocol (BFCP) Streams.*
- [IETF RFC 4662] IETF RFC 4662 (2006), *A Session Initiation Protocol (SIP) Event Notification Extension for Resource Lists.*
- [IETF RFC 4715] IETF RFC 4715 (2006), *The Integrated Services Digital Network (ISDN) Subaddress Encoding Type for tel URI.*
- [IETF RFC 4730] IETF RFC 4730 (2006), *A Session Initiation Protocol (SIP) Event Package for Key Press Stimulus (KPML).*
- [IETF RFC 5031] IETF RFC 5031 (2008), *A Uniform Resource Name (URN) for Emergency and Other Well-Known Services.*
- [IETF RFC 5049] IETF RFC 5049 (2007), *Applying Signaling Compression (SigComp) to the Session Initiation Protocol (SIP).*
- [IETF RFC 5079] IETF RFC 5079 (2007), *Rejecting Anonymous Requests in the Session Initiation Protocol (SIP).*

2.2.2 Spécifications applicables au niveau transport

- [IETF RFC 3016] IETF RFC 3016 (2000), *RTP Payload Format for MPEG-4 Audio/Visual Streams.*

- [IETF RFC 3047] IETF RFC 3047 (2001), *RTP Payload Format for UIT-T Recommendation G.722.1*.
- [IETF RFC 3267] IETF RFC 3267 (2002), *Real-Time Transport Protocol (RTP) Payload Format and File Storage Format for the Adaptive Multi-Rate (AMR) and Adaptive Multi-Rate Wideband (AMR-WB) Audio Codecs*.
- [IETF RFC 3389] IETF RFC 3389 (2002), *Real-time Transport Protocol (RTP) Payload for Comfort Noise (CN)*.
- [IETF RFC 3550] IETF RFC 3550 (2003), *RTP: A Transport Protocol for Real-Time Applications*.
- [IETF RFC 3551] IETF RFC 3551 (2003), *RTP Profile for Audio and Video Conferences with Minimal Control*.
- [IETF RFC 3558] IETF RFC 3558 (2003), *RTP Payload Format for Enhanced Variable Rate Codecs (EVRC) and Selectable Mode Vocoders (SMV)*.
- [IETF RFC 3611] IETF RFC 3611 (2003), *RTP Control Protocol Extended Reports (RTCP XR)*.
- [IETF RFC 3711] IETF RFC 3711 (2004), *The Secure Real-time Transport Protocol (SRTP)*.
- [IETF RFC 3984] IETF RFC 3984 (2005), *RTP Payload Format for H.264 Video*.
- [IETF RFC 4103] IETF RFC 4103 (2005), *RTP Payload for Text Conversation*.
- [IETF RFC 4348] IETF RFC 4348 (2006), *Real-Time Transport Protocol (RTP) Payload Format for the Variable-Rate Multimode Wideband (VMR-WB) Audio Codec*.
- [IETF RFC 4629] IETF RFC 4629 (2007), *RTP Payload Format for UIT-T Rec. H.263 Video*.
- [IETF RFC 4733] IETF RFC 4733 (2006), *RTP Payload for DTMF Digits, Telephony Tones, and Telephony Signals*.
- [IETF RFC 4749] IETF RFC 4749 (2006), *RTP Payload Format for the G.729.1 Audio Codec*.

2.3 Références de l'ETSI

- [ETSI EN 301 703] ETSI EN 301 703 V7.0.2 (1999-12), *Digital cellular telecommunications system (Phase 2+) (GSM); Adaptive Multi-Rate (AMR); Speech processing functions; General description (GSM 06.71 version 7.0.2 Release 1998)*.

2.4 Autres références

- [TIA-127-A] TIA-127-A (2004), *Enhanced Variable Rate Codec Speech Service Option 3 for Wideband Spread Spectrum Digital Systems*.
- [TIA-1016-A] TIA-1016-A (2006), *Source-Controlled Variable-Rate Multimode Wideband Speech Codec (VMR-WB), Service Options 62 and 63 for Spread Spectrum Systems*.

3 Définitions

S'agissant de la terminologie qui concerne les protocoles SIP et SDP, il est renvoyé aux références [IETF RFC 3261], [IETF RFC 3264], [IETF RFC 2327] et [IETF RFC 4566]. Pour ce qui est de la terminologie propre aux réseaux NGN, il est renvoyé à la référence [UIT-T Y.2012]. Les autres termes employés dans la présente Recommandation sont définis ci-après:

3.1 fonction d'utilisateur final (EUF): fonction assurée par l'équipement d'utilisateur final de type ancien ou NGN ainsi que par les réseaux d'abonné. L'équipement d'utilisateur final peut être fixe

ou mobile. Les interfaces au niveau de l'utilisateur final, par le biais desquelles la fonction EUF est reliée au réseau NGN, sont des interfaces tant physiques que fonctionnelles (de commande).

3.2 liste de codecs recommandés: liste contenant les codecs que le réseau doit communiquer à l'utilisateur, dans les messages SIP/SDP échangés par le biais de l'interface UNI.

NOTE – La liste de codecs recommandés a pour seul objet d'indiquer les codecs qu'un réseau recommande d'utiliser au niveau de l'interface UNI. Elle ne recommande nullement aux terminaux d'employer tous les codecs figurant sur la liste.

3.3 fonctions de commande de service (SCF): fonctions qui établissent, surveillent, prennent en charge et libèrent les sessions multimédias, et qui gèrent les échanges de service de l'utilisateur.

3.4 agent d'utilisateur de boucle locale (B2BUA) SIP: agent issu de la concaténation d'un client d'agent d'utilisateur (UAC) SIP et d'un serveur d'agent d'utilisateur (UAS) SIP.

NOTE – Dans la référence [IETF RFC 3261], l'IETF définit l'agent B2BUA comme "une entité logique qui reçoit une demande et la traite comme le ferait un serveur d'agent d'utilisateur (UAS). Afin de déterminer comment y répondre, il assure le rôle de client d'agent d'utilisateur (UAC) et fait des demandes. Contrairement au serveur relais, il poursuit le dialogue et participe, pour toutes les demandes formulées, aux dialogues qu'il a établis. Puisqu'il est issu d'une concaténation d'un client UAC et d'un serveur UAS, son comportement ne nécessite aucune définition particulière" (les comportements du client UAC et du serveur UAS sont définis dans la référence [IETF RFC 3261]). Un agent B2BUA reformule un message avant de l'envoyer en tant que nouvelle demande.

4 Abréviations

La présente Recommandation utilise les abréviations suivantes:

3GPP	projet de partenariat de troisième génération (<i>3rd generation partnership project</i>)
AKA	authentification et concordance de clés (<i>authentication and key agreement</i>)
AMR	(codec) adaptatif multidébit (<i>adaptive multirate (codec)</i>)
AMR-NB	codec AMR bande étroite (<i>AMR narrowband</i>)
AMR-WB	codec AMR large bande (<i>AMR wideband</i>)
B2BUA	agent d'utilisateur de boucle locale (<i>back-to-back user agent</i>)
CSC-FE	entité fonctionnelle de commande de session d'appel (<i>call session control functional entity</i>)
CSMA/CD	accès multiple à repérage de porteuse avec détection de collision (<i>carrier sense multiple access with collision detection</i>)
DTMF	multifréquence bitonalité (<i>dual-tone multifrequency</i>)
EUF	fonctions d'utilisateur final (<i>end-user functions</i>)
EVRC	codec amélioré à débit variable (<i>enhanced variable rate codec</i>)
FQDN	nom de domaine complet (<i>fully qualified domain name</i>)
GRUU	identificateur URI d'agent d'utilisateur, susceptible d'être acheminé à l'échelle mondiale (<i>globally routable user agent URIs</i>)
HTTP	protocole de transfert hypertexte (<i>hypertext transfer protocol</i>)
IBC-FE	entité fonctionnelle de commande de passerelle périphérique d'interconnexion (<i>interconnection border gateway control functional entity</i>)
ICMP	protocole de messagerie de commande Internet (<i>Internet control message protocol</i>)
IP PBX	commutateur privé IP (<i>IP private branch exchange</i>)

ISUP	sous-système utilisateur du RNIS (<i>ISDN user part</i>)
IVR	réponse vocale interactive (<i>interactive voice response</i>)
KPML	invite à appuyer sur une touche (<i>key press stimulus</i>)
MIME	extensions multifonctions du courrier Internet (<i>multi-purpose Internet mail extensions</i>)
MPEG	groupe d'experts chargé des images animées (<i>moving picture experts group</i>)
NAT	traduction d'adresse réseau (<i>network address translation</i>)
NGN	réseau de prochaine génération (<i>next generation network</i>)
NGN-TE	équipement terminal NGN (<i>NGN terminal equipment</i>)
QoS	qualité de service (<i>quality of service</i>)
RGW	passerelle résidentielle (<i>residential gateway</i>)
RNIS	réseau numérique à intégration des services
RTCP	protocole de commande RTP (<i>RTP control protocol</i>)
RTCP XR	rapports étendus dans le cadre du protocole RTCP (<i>RTCP extended reports</i>)
RTP	protocole de transport en temps réel (<i>real-time transport protocol</i>)
RTPC	réseau téléphonique public commuté
SCF	fonctions de commande de service (<i>service control functions</i>)
SCTP	protocole de transmission de commande de flux (<i>stream control transmission protocol</i>)
SDP	protocole de description de session (<i>session description protocol</i>)
SIP	protocole d'ouverture de session (<i>session initiation protocol</i>)
SIPS	protocole d'ouverture de session sécurisée (<i>session initiation protocol secure</i>)
SMV	codeurs vocaux multimodes (<i>selectable mode vocoders</i>)
SRTP	protocole de transport sécurisé en temps réel (<i>secure real-time transport protocol</i>)
TCP	protocole de commande de transmission (<i>transmission control protocol</i>)
TLS	sécurité de la couche transport (<i>transport layer security</i>)
UA	agent d'utilisateur (<i>user agent</i>)
UAC	client d'agent d'utilisateur (<i>user agent client</i>)
UAS	serveur d'agent d'utilisateur (<i>user agent server</i>)
UDP	protocole applicable aux datagrammes d'utilisateur (<i>user datagram protocol</i>)
UNI	interface utilisateur-réseau (<i>user-to-network interface</i>)
URI	identificateur universel de ressource (<i>universal resource identifier</i>)
VMR-WB	codec multimode large bande à débit variable (<i>variable-rate multi-mode wideband</i>)
VoIP	téléphonie IP (<i>voice over IP</i>)

5 Modèle de référence

La Figure 1 illustre l'interface UNI, sur laquelle porte la présente Recommandation, dans l'architecture NGN définie dans la référence [UIT-T Y.2012].

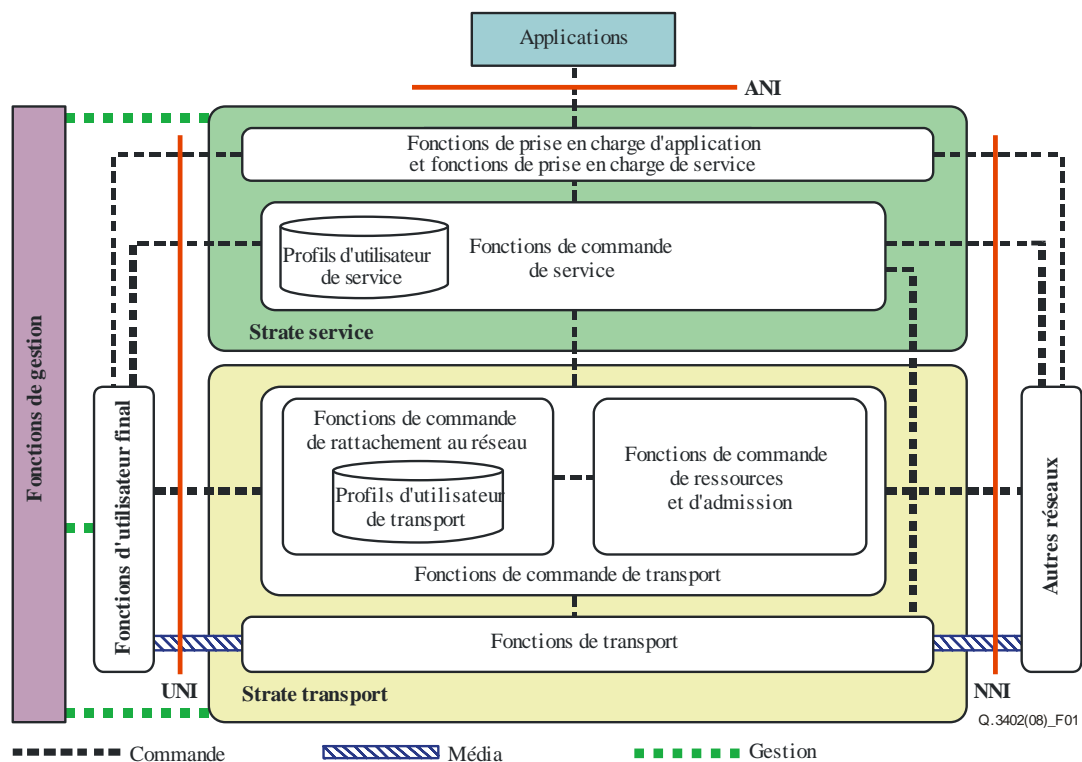


Figure 1 – L'interface UNI, sur laquelle porte la présente Recommandation, dans l'architecture NGN

Les Figures 2, 3 et 4 illustrent les scénarios possibles applicables aux types de terminaux qui assurent les fonctions EUF.

La Figure 2 représente le scénario applicable aux terminaux RTPC/RNIS et aux téléphones IP, reliés à un fournisseur de services par l'intermédiaire d'une passerelle résidentielle SIP.

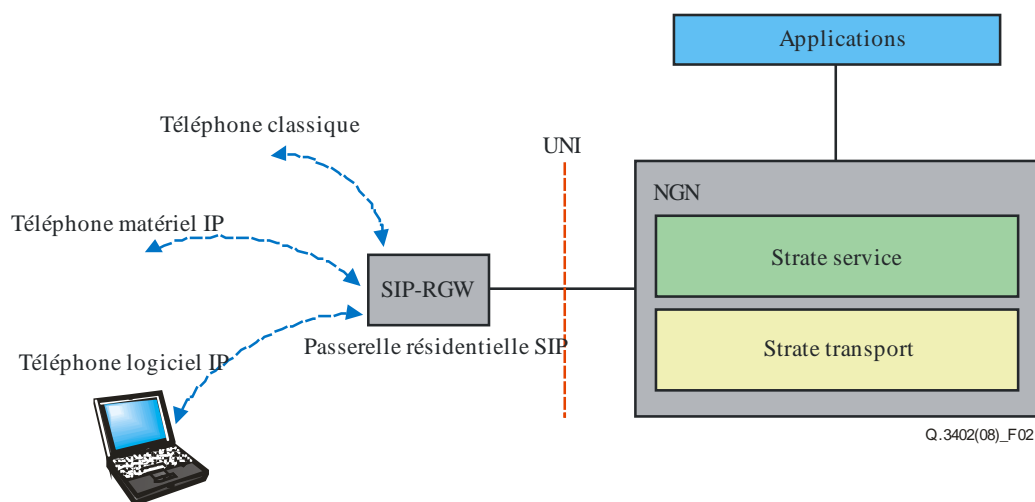


Figure 2 – Scénario faisant intervenir une passerelle résidentielle SIP

La Figure 3 représente le scénario applicable aux téléphones SIP, qui font partie d'un sous-système IMS et sont directement reliés à un fournisseur de services.

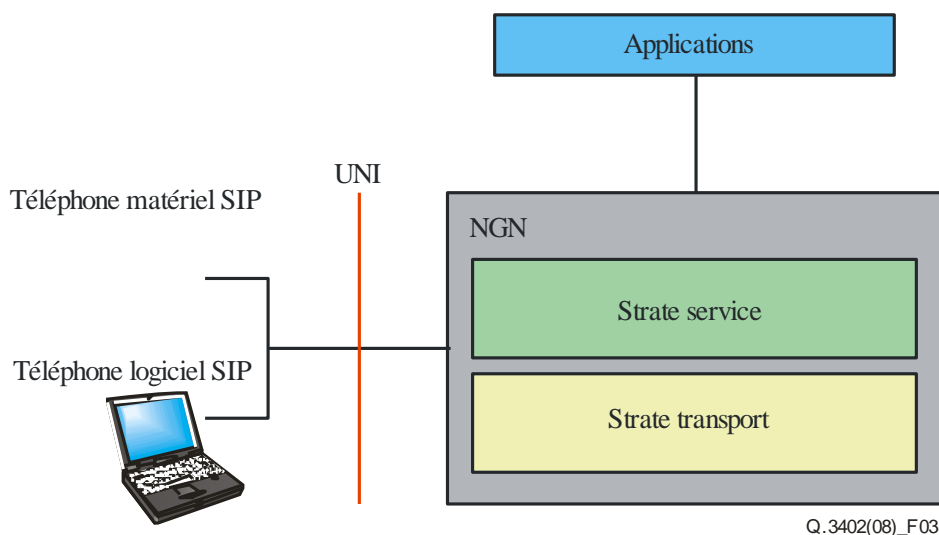


Figure 3 – Scénario applicable aux téléphones SIP qui font partie d'un sous-système IMS

La Figure 4 représente le scénario applicable aux téléphones SIP reliés à un fournisseur de services par l'intermédiaire d'un commutateur PBX IP SIP.

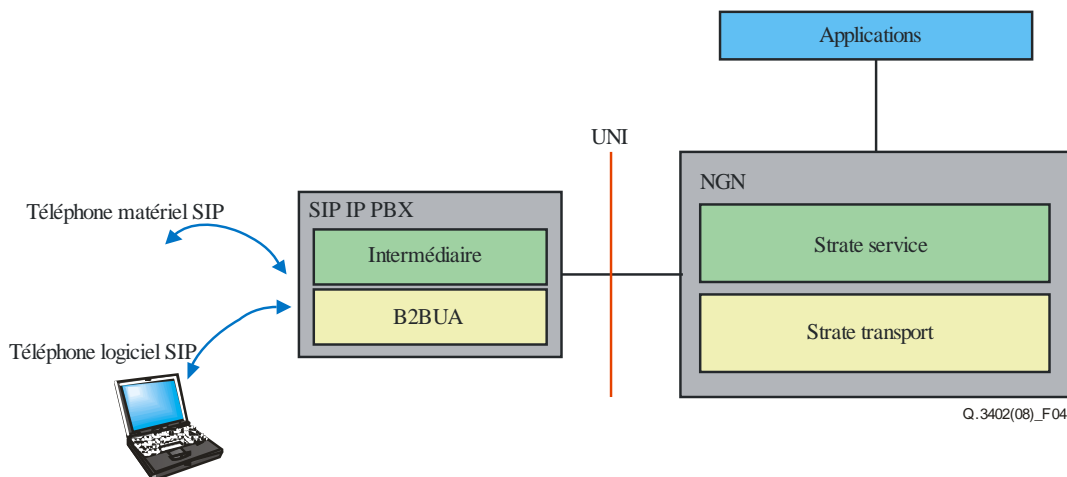


Figure 4 – Scénario faisant intervenir un commutateur PBX IP SIP

6 Hypothèses

La présente Recommandation est fondée sur les hypothèses suivantes:

- 1) Les protocoles SIP/SDP sont employés pour la commande de la session.
- 2) Les protocoles RTP ou SRTP sont employés pour le transport téléphonique et vidéo, mais d'autres protocoles de transport peuvent être employés pour les applications qui concernent les données.

7 Mise à disposition des médias au cours d'une session SIP

7.1 Considérations relatives aux paquets médias

Au cours de chacune des sessions établies par le biais de l'interface UNI au moyen du protocole SIP, il sera procédé comme suit:

- a) La fonction EUF côté origine:
 - doit envoyer en direction du réseau les paquets médias provenant de l'entité d'origine, après avoir reçu une réponse SDP finale, contenue dans une réponse 2xx SIP à l'INVITE d'un dialogue normal;
 - peut envoyer en direction du réseau les paquets médias provenant de l'entité d'origine, dès réception de la première réponse SDP contenue dans une réponse 1xx SIP à l'INVITE après l'établissement d'un dialogue initial. Un réseau peut choisir, selon sa politique, de ne pas transmettre les paquets médias provenant de l'entité d'origine avant que l'offre/la demande SDP finale n'ait été faite, afin d'éviter le vol de service dans les cas où la facturation est fonction de l'utilisation;
 - doit être prête à recevoir par l'intermédiaire du réseau les paquets médias provenant de l'entité de terminaison, après avoir envoyé l'INVITE avec une offre SDP.
- b) La fonction EUF côté terminaison:
 - doit envoyer en direction du réseau les paquets médias provenant de l'entité de terminaison, après avoir reçu une réponse 2xx SIP à la demande INVITE avec l'offre SDP;
 - doit être prête à recevoir par l'intermédiaire du réseau les paquets médias provenant de l'entité d'origine, après avoir envoyé une réponse 2xx SIP à l'INVITE.
- c) Conformément à la référence [IETF RFC 3261], dès l'achèvement d'un dialogue SIP, le flux de paquets médias doit être arrêté.
- d) L'absence de paquets médias au niveau de l'interface UNI pendant un certain intervalle de temps dans l'une ou l'autre direction ne doit pas être considérée par une fonction EUF ou par le réseau comme un motif suffisant pour clore la session SIP. Mais lorsque, conformément à la négociation SIP, les flux de média sont en activité, ce fait de ne plus avoir de paquets médias au niveau de l'interface UNI pendant une certaine durée peut être un motif de clôture de la session SIP.

NOTE – Le fait qu'il n'y ait pas de paquets médias au niveau de l'interface UNI pendant une certaine durée ne peut être un motif de clôture de la session SIP que s'il est sûr que cette absence de paquets est due à une défaillance.

7.2 Adjonction ou suppression d'un flux de média

Toute session média établie par le biais de l'interface UNI au moyen du protocole SIP débute, dans le cas d'un type de média (par exemple, la téléphonie) ou de plusieurs types de flux de média (par exemple, la téléphonie et la vidéo), par un échange d'offres et de demandes SDP entre les entités d'origine et de terminaison. L'adjonction de plusieurs types de flux de média ou la suppression de certains d'entre eux est possible au cours de la communication.

8 Codec

8.1 Liste de codecs

Il incombe aux entités à la périphérie du réseau NGN (par exemple, l'équipement terminal NGN) et aux équipements de réseau émettant ou recevant des flux de média IP de négocier afin de choisir un codec commun pour chacune des sessions médias "de bout en bout". Le réseau NGN doit donc

admettre la négociation de bout en bout d'un codec qui figure sur la liste des codecs recommandés par lui. Il peut aussi, selon sa politique, admettre un codec ne faisant pas partie de ladite liste.

NOTE 1 – La présente Recommandation ne prévoit aucune procédure pour l'interface UNI, dans le cas où la négociation d'un codec commun échouerait.

NOTE 2 – Afin de renforcer l'interopérabilité, de limiter le nombre de transcodages sur les connexions de réseau et d'améliorer éventuellement la gestion des ressources de réseau, il est souhaitable que le réseau NGN recommande aux utilisateurs l'emploi de la liste des codecs recommandés. Une invite à l'emploi d'un ou de plusieurs codecs parmi ceux de ladite liste figure dans les messages SIP/SDP échangés par le biais de l'interface UNI.

Le traitement des messages, qui comportent des codecs ne figurant pas sur la liste des codecs recommandés ou qui ne comportent aucun des codecs de cette liste, dépend de la politique du réseau, à savoir, certains réseaux peuvent admettre l'emploi de codecs ne figurant pas sur ladite liste tandis que d'autres peuvent rejeter de tels messages.

La recommandation de l'emploi d'une liste de codecs recommandés n'impose pas directement les codecs devant être utilisés dans le réseau à des fins de transcodage, et ne signifie pas non plus que les terminaux doivent prendre en charge tous les codecs de ladite liste. Donc, même si une offre SIP/SDP fait appel à ladite liste, la réussite de la négociation d'un codec n'est pas garantie.

NOTE 3 – Lorsque les codecs à prendre en charge au niveau de l'interface UNI sont limités, en raison de la politique du réseau, une recommandation comme dans la Note 2 est souhaitable. Lorsqu'une telle recommandation ne peut être faite, la liste de codecs recommandés doit comporter la loi A/ μ G.711 [UIT-T G.711].

NOTE 4 – Dans le cas de la communication téléphonique, la liste de codecs recommandés doit comporter la loi A/ μ G.711. Tandis que tout autre codec figurant sur ladite liste peut être employé, en fonction de la politique du réseau, il est conseillé que la liste contienne les codecs AMR NB [ETSI EN 301 703], EVRC [TIA-127-A], [UIT-T G.729], y compris l'Annexe A, [UIT-T G.722.1], [UIT-T G.726], et le codec audio MPEG-4 [ISO/CEI 14496-3]. Si l'on veut fournir un service téléphonique de qualité supérieure, il est fortement conseillé que la liste contienne un codec large bande tel que les codecs AMR WB [UIT-T G.722.2], VMR-WB [TIA-1016-A], [UIT-T G.722], ou [UIT-T G.729.1]. Si l'on veut prendre en charge les malentendants, il est conseillé d'insérer le codec [UIT-T T.140] dans la liste de codecs. Si l'interconnexion se fait sur un réseau RTPC/RNIS existant, il est conseillé que le codec [UIT-T T.140] soit remplacé par la loi A/ μ [UIT-T G.711]. Dans le cas de la communication vidéo, il est conseillé que la liste de codecs recommandés contienne les codecs [UIT-T H.263], [UIT-T H.264], et le codec visuel MPEG-4 [ISO/CEI 14496-2]. S'agissant de la communication de données, il est conseillé que le réseau indique à l'utilisateur les applications pour les données, qui ont sa préférence.

NOTE 5 – Dans le cas de sessions individuelles, un élément de signalisation d'appel, tel qu'une entité CSC-FE, un serveur d'application ou une entité IBC-FE, informé de la négociation de bout en bout d'un codec, peut déterminer si le transcodage entre les extrémités est nécessaire et peut l'entamer.

NOTE 6 – Bien que le transcodage doit être évité dans la mesure du possible, le réseau peut le prendre en charge en vue d'accroître les chances d'établissement d'une session (par exemple, lorsque les codecs pris en charge par les extrémités font partie de la liste de codecs recommandés mais qu'aucun codec commun ne peut être trouvé). Toutefois, une recommandation de l'emploi d'une telle liste n'implique pas que le réseau doive prendre en charge le transcodage entre l'un des codecs de la liste et tout autre codec, ou entre deux codecs de la liste.

8.2 Taille de mise en paquets

Lorsque la taille de mise en paquets n'est pas choisie dans le cadre d'une négociation de codec entre terminaux et/ou entre éléments de réseau ou n'est pas recommandée par la politique du réseau, il conviendrait d'utiliser des échantillons de 10 ms pour la mise en paquets de données vocales à codage UIT-T G.711. Il s'agit de la valeur optimale recommandée qui permette d'aboutir à un équilibre entre le temps de propagation de bout en bout et celui de l'utilisation du réseau. Il est admis qu'en raison de contraintes éventuelles du réseau, la politique de celui-ci peut consister à recommander une valeur plus élevée, à savoir une valeur de 20 ms. Il est aussi admis que, dans la politique, une limite

supérieure pour la taille de mise en paquets devrait être prévue, qui ne dépasse pas 60 ms, par exemple.

NOTE – Lorsque la taille de mise en paquets est choisie dans le cadre d'une négociation de codec entre terminaux et/ou entre éléments de réseau, la présente Recommandation n'impose rien quant à la valeur qui doit être choisie.

9 Routage et adressage

Le Tableau 1 décrit les formats des identificateurs URI qui sont pris en charge au niveau de l'interface UNI.

D'autres formats peuvent être pris en charge.

Tableau 1 – Formats des identificateurs URI

Identificateur URI SIP	sip:userinfo@hostport;uri-parameters (Note)
	Description: "userinfo", "hostport" et "uri-parameters" sont fondés sur le § 25 de la référence [IETF RFC 3261]. "userinfo" contient le numéro E.164 international ou le numéro local
	Référence: [IETF RFC 3261] et [IETF RFC 3966]
Identificateur URI téléphonique	tel:telephone-subscriber
	Description: telephone-subscriber est le numéro E.164 international ou le numéro local
	Référence: [IETF RFC 3966]
NOTE – "hostport" contient un nom de domaine ou une adresse IP. "hostport" peut aussi contenir un numéro de port.	

Dans la procédure REGISTER, l'identificateur URI SIP dans l'identificateur Request-URI ne doit pas contenir "userinfo" avec "@", comme spécifié dans la référence [IETF RFC 3261].

10 Profil de signalisation applicable au niveau service

10.1 Normes RFC (*requests for comments*, demandes d'observations) à prendre en charge

Tableau 2 – Notations O/F/C au niveau de l'interface UNI

Code	Description du code	Signification
O	Obligatoire	L'interface UNI doit être conforme aux normes RFC énumérées. Pour plus de détails sur l'application d'une norme RFC obligatoire particulière, voir le paragraphe pertinent au bas du Tableau.
F	Facultatif	L'interface UNI peut être conforme aux normes RFC énumérées.
C	Conditionnel	L'interface UNI doit être conditionnellement conforme aux normes RFC énumérées, selon le contexte. Concernant le contexte pour l'application d'une norme RFC obligatoire particulière, voir le paragraphe pertinent au bas du Tableau.

Tableau 3 – Normes RFC à prendre en charge au niveau de l'interface UNI

Catégorie	Norme RFC	Titre	Fonctions EUF	Fonctions SCF
Identité et confidentialité	RFC 3323	"A Privacy Mechanism for the Session Initiation Protocol (SIP)"	O (Note 1)	O
	RFC 3324	"Short Term Requirements for Network Asserted Identity"	O (Note 1)	O
	RFC 3325	"Private Extensions to the Session Initiation Protocol (SIP) for Asserted Identity within Trusted Networks"	O (Note 1)	O
Identificateur URI	RFC 3966	"The tel URI for Telephone Numbers"	O (Note 2)	O (Note 2)
	RFC 4715	"The Integrated Services Digital Network (ISDN) Subaddress Encoding Type for tel URI"	F	F
	RFC 3824	"Using E.164 numbers with the Session Initiation Protocol (SIP)"	C1	C1
	RFC 4458	"Session Initiation Protocol (SIP) URIs for Applications such as Voicemail and Interactive Voice Response (IVR)"	C2	C2
	RFC 5031	"A Uniform Resource Name (URN) for Emergency and Other Well-Known Services"	F	F
Protocole SIP et extension	RFC 3261	"SIP: Session Initiation Protocol"	O	O
	RFC 3262	"Reliability of Provisional Responses in Session Initiation Protocol (SIP)"	C3	O
	RFC 3263	"Session Initiation Protocol (SIP): Locating SIP Servers"	C4	C4
	RFC 3264	"An Offer/Answer Model with Session Description Protocol (SDP)"	O	O
	RFC 3265	"Session Initiation Protocol (SIP)-Specific Event Notification"	C5	C5
	RFC 3310	"Hypertext Transfer Protocol (HTTP) Digest Authentication Using Authentication and Key Agreement (AKA)"	C6	C6
	RFC 3311	"The Session Initiation Protocol (SIP) UPDATE Method"	O (Note 3)	O (Note 3)
	RFC 3312	"Integration of Resource Management and Session Initiation Protocol (SIP)"	F	F
	RFC 3326	"The Reason Header Field for the Session Initiation Protocol (SIP)"	F	F
	RFC 3327	"Session Initiation Protocol (SIP) Extension Header Field for Registering Non-Adjacent Contacts"	F	F
	RFC 3313	"Private Session Initiation Protocol (SIP) Extensions for Media Authorization"	F	F
	RFC 3320	"Signaling Compression (SigComp)"	F	F
	RFC 3515	"The Session Initiation Protocol (SIP) Refer Method"	C7	C7

Tableau 3 – Normes RFC à prendre en charge au niveau de l'interface UNI

Catégorie	Norme RFC	Titre	Fonctions EUF	Fonctions SCF
Protocole SIP et extension	RFC 3581	"An Extension to the Session Initiation Protocol (SIP) for Symmetric Response Routing"	C8	C8
	RFC 3891	"The Session Initiation Protocol (SIP) "Replaces" Header"	C7	C7
	RFC 3892	"The Session Initiation Protocol (SIP) Referred-By Mechanism"	C7	C7
	RFC 4244	"An Extension to the Session Initiation Protocol for Request History Information"	C9 (Note 4)	C9 (Note 4)
	RFC 3959	"The Early Session Disposition Type for the Session Initiation Protocol (SIP)"	F	F
	RFC 3960	"Early Media and Ringing Tone Generation in the Session Initiation Protocol"	C10	C10
	RFC 3842	"A Message Summary and Message Waiting Indication Event Package for the Session Initiation Protocol (SIP)"	C11	C11
	RFC 4028	"Session Timers in the Session Initiation Protocol (SIP)"	O	O
	RFC 3725	"Best Current Practices for Third Party Call Control (3pcc) in the Session Initiation Protocol (SIP)"	F	F
	RFC 4730	"A Session Initiation Protocol (SIP) Event Package for Key Press Stimulus (KPML)"	F	F
	RFC 2617	"HTTP Authentication: Basic and Digest Access Authentication"	F (Note 5)	F (Note 5)
	RFC 2976	"The SIP INFO method"	F	F
	RFC 3911	"The Session Initiation Protocol (SIP) "Join" Header"	F	F
	RFC 3840	"Indicating User Agent Capabilities in the Session Initiation Protocol (SIP)"	F	F
	RFC 3841	"Caller Preferences for the Session Initiation Protocol (SIP)"	F	F
	RFC 3608	"Session Initiation Protocol (SIP) Extension Header Field for Service Route Discovery During Registration"	F	F
	RFC 3680	"A Session Initiation Protocol (SIP) Event Package for Registrations"	F	F
	RFC 3329	"Security Mechanism Agreement for the Session Initiation Protocol (SIP)"	F	F
	RFC 3455	"Private Header (P-Header) Extensions to the Session Initiation Protocol (SIP) for the 3rd-Generation Partnership Project (3GPP)"	F	F
	RFC 3485	"The Session Initiation Protocol (SIP) and Session Description Protocol (SDP) Static Dictionary for Signaling Compression (SigComp)"	F	F

Tableau 3 – Normes RFC à prendre en charge au niveau de l'interface UNI

Catégorie	Norme RFC	Titre	Fonctions EUF	Fonctions SCF
Protocole SIP et extension	RFC 3486	"Compressing the Session Initiation Protocol (SIP)"	F	F
	RFC 3853	S/MIME AES Requirement for SIP	F	F
	RFC 4320	"Actions Addressing Identified Issues with the Session Initiation Protocol's (SIP) non-INVITE Transaction"	F (Note 6)	F (Note 6)
	RFC 4412	"Communications Resource Priority for the Session Initiation Protocol (SIP)"	F	F
	RFC 4483	"A Mechanism for Content Indirection in Session Initiation Protocol (SIP) Messages"	F	F
	RFC 4032	"Update to the Session Initiation Protocol (SIP) Preconditions Framework"	F	F
	RFC 4235	"An INVITE-Initiated Dialog Event Package for the Session Initiation Protocol (SIP)"	F	F
	RFC 4168	"The Stream Control Transmission Protocol (SCTP) as a Transport for the Session Initiation Protocol (SIP)"	F	F
	RFC 5079	"Rejecting Anonymous Requests in the Session Initiation Protocol (SIP)"	F	F
	RFC 5049	"Applying Signaling Compression (SigComp) to the Session Initiation Protocol (SIP)"	F	F
Description de média	RFC 2046	"Multipurpose Internet Mail Extensions (MIME) Part Two: Media Types"	F	F
	RFC 3388	"Grouping of Media Lines in the Session Description Protocol"	F	F
	RFC 3420	"Internet Media Type message/sipfrag"	F	F
	RFC 3524	"Mapping of Media Streams to Resource Reservation Flows"	F	F
	RFC 3556	"Session Description Protocol (SDP) Bandwidth Modifiers for RTP Control Protocol (RTCP) Bandwidth"	F	F
	RFC 4145	"TCP-Based Media Transport in the Session Description Protocol (SDP)"	F	F
	RFC 4566	"SDP: Session Description Protocol"	O (Note 7)	O (Note 7)
	RFC 4583	"Session Description Protocol (SDP) Format for Binary Floor Control Protocol (BFCP) Streams"	F	F
Conférence	RFC 4575	"A Session Initiation Protocol (SIP) Event Package for Conference State"	C12	C12
	RFC 4579	"Session Initiation Protocol (SIP) Call Control – Conferencing for User Agents"	C13	C13
Messagerie instantanée	RFC 3428	"Session Initiation Protocol (SIP) Extension for Instant Messaging"	C14	C14
	RFC 3860	"Common Profile for Instant Messaging (CPIM)"	F	F
	RFC 3861	"Address Resolution for Instant Messaging and Presence"	F	F
	RFC 3862	"Common Presence and Instant Messaging (CPIM): Message Format"	F	F

Tableau 3 – Normes RFC à prendre en charge au niveau de l'interface UNI

Catégorie	Norme RFC	Titre	Fonctions EUF	Fonctions SCF
	RFC 3994	"Indication of Message Composition for Instant Messaging"	F	F
Présence	RFC 3903	"Session Initiation Protocol (SIP) Extension for Event State Publication"	C15	C15
	RFC 3856	"A Presence Event Package for the Session Initiation Protocol (SIP)"	C15	C15
	RFC 3857	"A Watcher Information Event Template-Package for the Session Initiation Protocol (SIP)"	F	F
	RFC 3858	"An Extensible Markup Language (XML) Based Format for Watcher Information"	F	F
	RFC 3859	"Common Profile for Presence (CPP)"	F	F
	RFC 3863	"Presence Information Data Format"	F	F
	RFC 4480	"RPID: Rich Presence Extensions to the Presence Information Data Format (PIDF)"	F	F
	RFC 4662	"A Session Initiation Protocol (SIP) Event Notification Extension for Resource Lists"	F	F
<p>C1: La norme [IETF RFC 3824] est conditionnellement obligatoire lorsqu'elle est employée comme directive à caractère conditionnellement obligatoire lors du formatage de l'identificateur URI SIP avec ENUM.</p> <p>C2: La norme [IETF RFC 4458] est conditionnellement obligatoire lorsqu'un nouvel adressage est requis.</p> <p>C3: La norme [IETF RFC 3262] est conditionnellement obligatoire lorsqu'une réponse provisoire fiable est requise.</p> <p>C4: La norme [IETF RFC 3263] peut ne pas être nécessaire dans des réseaux bien administrés et équipés de dispositifs configurés ou si l'adresse d'un intermédiaire extérieur est reçue au cours du rattachement au réseau, mais elle est conditionnellement obligatoire dans les autres cas.</p> <p>C5: La norme [IETF RFC 3265] est conditionnellement obligatoire lorsque la notification d'un événement, tel que l'indication d'attente de message, est requise.</p> <p>C6: La norme [IETF RFC 3310] est conditionnellement obligatoire pour l'équipement d'utilisateur mobile. Elle est toutefois facultative pour les terminaux de ligne fixe.</p> <p>C7: Les normes [IETF RFC 3515], [IETF RFC 3891] et [IETF RFC 3892] sont conditionnellement obligatoires lorsque la transmission des demandes est requise.</p> <p>C8: La norme [IETF RFC 3581] est conditionnellement obligatoire lorsqu'elle est employée pour le passage par le dispositif de traduction NAT.</p> <p>C9: La norme [IETF RFC 4244] est conditionnellement obligatoire lorsqu'une déviation d'appel est requise et que des informations concernant celle-ci sont transférées par le biais de l'interface UNI.</p> <p>C10: Le § 3 de la norme [IETF RFC 3960] est conditionnellement obligatoire lorsqu'il est employé comme directive à caractère obligatoire lors de l'émission et de la réception des annonces, sauf dans les cas où l'en-tête de média préalable P est pris en charge.</p> <p>C11: La norme [IETF RFC 3842] est conditionnellement obligatoire lorsqu'une indication de messagerie, telle que le nombre de messages vocaux, est requise.</p> <p>C12: La norme [IETF RFC 4575] est conditionnellement obligatoire lorsque la conférence est requise.</p> <p>C13: La norme [IETF RFC 4579] est conditionnellement obligatoire pour la conférence, afin que soient données des précisions quant à la manière de prendre en charge les normes RFC qui s'appliquent dans ce cas.</p> <p>C14: La norme [IETF RFC 3428] est conditionnellement obligatoire lorsque la messagerie instantanée est requise.</p> <p>C15: Les normes [IETF RFC 3903] et [IETF RFC 3856] sont conditionnellement obligatoires lorsque la présence est requise.</p>				

Tableau 3 – Normes RFC à prendre en charge au niveau de l'interface UNI

Catégorie	Norme RFC	Titre	Fonctions EUF	Fonctions SCF
<p>NOTE 1 – L'application des normes [IETF RFC 3323], [IETF RFC 3324] et [IETF RFC 3325] est facultative dans le cas de réseaux d'entreprise.</p> <p>NOTE 2 – Même si seul l'identificateur URI SIP est pris en charge, la norme [IETF RFC 3966] est obligatoire pour le champ userinfo, fondé sur la référence [b-UIT-T E.164], dans l'identificateur URI SIP.</p> <p>NOTE 3 – Les fonctions EUF et SCF doivent prendre en charge l'ensemble des dispositions obligatoires de la norme [IETF RFC 3311]. Afin de mettre à jour les paramètres avant que l'INVITE initiale ne soit achevée, il faut appliquer une procédure UPDATE. Afin de mettre à jour les paramètres après l'achèvement de l'INVITE initiale, il faut réitérer l'INVITE ou appliquer une procédure UPDATE. L'emploi de la procédure UPDATE est subordonné à l'indication par l'utilisateur de son accord dans le champ d'en-tête Allow.</p> <p>Si le but est de restreindre l'acceptation ou le rejet d'une nouvelle offre par l'utilisateur à l'autre extrémité, une procédure UPDATE devrait être employée.</p> <p>Si le but est de laisser à l'utilisateur à l'autre extrémité la possibilité d'accepter ou de rejeter une nouvelle offre, une nouvelle INVITE devrait être employée.</p> <p>Si l'autre extrémité ne prend pas en charge la procédure UPDATE, une nouvelle INVITE doit être employée.</p> <p>NOTE 4 – La référence [IETF RFC 4458] est appliquée dans certaines mises en oeuvre SIP anciennes en remplacement de la référence [IETF RFC 4244].</p> <p>NOTE 5 – Le système d'authentification BASIC ne doit pas être employé.</p> <p>NOTE 6 – Il est recommandé que cette référence [IETF RFC 4320] soit appliquée au traitement des transactions sans INVITE.</p> <p>NOTE 7 – Si une quelconque spécification ne figurant que dans la référence [IETF RFC 2327] est employée, par exemple m=data, cette référence [IETF RFC 2327] doit être prise en charge.</p>				

10.2 Profils SIP

10.2.1 Profil SIP fondé sur la norme RFC 3261

Le présent paragraphe définit un profil SIP applicable aux fonctions EUF et SCF au niveau de l'interface UNI. Sa structure et la numérotation de ses paragraphes font écho à celles de la référence [IETF RFC 3261]. Les sous-paragraphes sont ici numérotés de telle manière que le quatrième chiffre (par exemple, x dans 10.2.1.x) corresponde au numéro de paragraphe de la référence [IETF RFC 3261], tandis que le titre du sous-paragraphe correspond au titre dudit paragraphe de la référence [IETF RFC 3261].

Le présent paragraphe définit l'ensemble d'améliorations et de restrictions apportées à une mise en oeuvre SIP normalisée, reposant sur la référence [IETF RFC 3261].

Sauf indication contraire dans la présente Recommandation, les fonctions EUF et SCF doivent assumer leurs tâches en conformité avec la référence [IETF RFC 3261].

10.2.1.1 Introduction

Le § 1 de la référence [IETF RFC 3261] est mentionné à titre informatif.

10.2.1.2 Aperçu de la fonctionnalité SIP

Le § 2 de la référence [IETF RFC 3261] est mentionné à titre informatif.

10.2.1.3 Terminologie

Le § 3 de la référence [IETF RFC 3261] est mentionné à titre informatif.

10.2.1.4 Aperçu de l'exploitation

Le § 4 de la référence [IETF RFC 3261] est mentionné à titre informatif.

10.2.1.5 Structure du protocole

La structure du protocole est décrite au § 5 de la référence [IETF RFC 3261], qui est mentionné à titre informatif.

10.2.1.6 Définitions

Le § 6 de la référence [IETF RFC 3261] définit les termes qui ont une signification particulière dans le cadre du protocole SIP. Des définitions supplémentaires sont données dans le § 3 de la présente Recommandation.

Il convient de souligner que le terme "client" dans le présent sous-paragraphe concerne tant les clients d'agent d'utilisateur que les intermédiaires.

10.2.1.7 Messages SIP

Les fonctions EUF et SCF doivent définir le profil SIP conformément au § 7 de la référence [IETF RFC 3261], sauf indication contraire dans le présent sous-paragraphe.

10.2.1.7.1 Demandes

Les fonctions EUF et SCF doivent définir le profil SIP conformément au § 7.1 de la référence [IETF RFC 3261], sauf indication contraire dans le présent sous-paragraphe.

Les fonctions EUF et SCF doivent se charger des procédures INVITE, ACK, CANCEL et BYE. La fonction SCF doit se charger des procédures UPDATE et PRACK, tandis que la fonction EUF doit se charger de la procédure UPDATE, ainsi que de la procédure PRACK, au cas où une réponse provisoire fiable est requise. La fonction EUF doit se charger de l'envoi de la demande REGISTER, tandis que la fonction SCF doit se charger de la réception de cette demande REGISTER. La procédure OPTIONS peut être prise en charge.

L'identificateur Request-URI doit être un identificateur URI SIP, comme défini dans la référence [IETF RFC 3261], ou un identificateur URI téléphonique, comme défini dans la référence [IETF RFC 3966]. Le format URI SIPS peut être pris en charge.

L'identificateur Request-URI dans une INVITE initiale lors d'un appel téléphonique ordinaire¹ doit identifier l'entité appelée, soit en employant un identificateur URI téléphonique, soit en employant la syntaxe d'abonné téléphonique (c'est-à-dire le numéro de téléphone composé) dans un identificateur URI SIP. Lorsque l'identificateur Request-URI est un identificateur URI SIP, la partie serveur de l'identificateur Request-URI doit identifier la fonction SCF ou l'entité à laquelle le message est adressé.

L'identificateur Request-URI doit, dans le cas d'autres demandes associées à un appel téléphonique ordinaire, identifier le serveur ciblé au moyen de son adresse IP ou de son nom FDQN, comme mentionné dans l'en-tête Contact.

La partie serveur de l'identificateur Request-URI concorde habituellement avec l'un des noms du serveur de réception. Toutefois, si l'identificateur Request-URI d'une INVITE reçue ne concorde pas, le serveur devrait transmettre la demande à une autre entité en employant les informations de traduction sauvegardées ou les informations préconfigurées selon la politique.

NOTE – L'identificateur Request-URI dans une demande REGISTER ne doit pas contenir "userinfo" avec "@", comme spécifié dans la référence [IETF RFC 3261].

10.2.1.7.2 Réponses

Les fonctions EUF et SCF doivent définir le profil SIP conformément au § 7.2 de la référence [IETF RFC 3261].

¹ Cela inclut les INVITE résultant d'un transfert.

10.2.1.7.3 Champs d'en-tête

Les fonctions EUF et SCF doivent définir le profil SIP conformément au § 7.3 de la référence [IETF RFC 3261].

10.2.1.7.4 Corps de message

Les fonctions EUF et SCF doivent définir le profil SIP conformément au § 7.4 de la référence [IETF RFC 3261], sauf indication contraire dans le présent sous-paragraphe.

10.2.1.7.4.1 Types de corps de message

Les fonctions EUF et SCF doivent définir le profil SIP conformément au § 7.4.1 de la référence [IETF RFC 3261], sauf indication contraire dans le présent sous-paragraphe.

Les fonctions EUF et SCF doivent définir le profil SIP de manière que le type de corps de message "application/sdp" soit pris en charge. D'autres types de corps de message peuvent par ailleurs être pris en charge.

Le type de corps de message "application/sdp" doit être pris en charge par les procédures INVITE et UPDATE, ainsi que par toute réponse de non-défaillance à ces procédures. Il doit aussi être pris en charge par la procédure PRACK, ainsi que par toute réponse de non-défaillance à cette procédure, afin que soit assuré l'interfonctionnement avec les réseaux H.323 et la fourniture des services utilisant la commande d'appel par un tiers.

Le type de corps de message "application/sdp" peut être pris en charge par des réponses de défaillance, telles que la réponse 488 (Not Acceptable Here), faite aux procédures susmentionnées.

10.2.1.7.4.2 Longueur de corps de message

Les fonctions EUF et SCF doivent définir le profil SIP conformément au § 7.4.2 de la référence [IETF RFC 3261].

10.2.1.7.5 Mise en trame de messages SIP

Les fonctions EUF et SCF doivent définir le profil SIP conformément au § 7.5 de la référence [IETF RFC 3261].

10.2.1.8 Comportement général de l'agent d'utilisateur

Le présent sous-paragraphe et ses sous-paragraphe ne s'appliquent que si la fonction EUF assure le rôle d'agent d'utilisateur, à savoir un client UAC ou un serveur UAS, et si la fonction SCF assure aussi le rôle d'agent d'utilisateur, à savoir un agent B2BUA ou un serveur de réacheminement.

Le comportement des fonctions EUF et SCF doit être conforme au § 8 de la référence [IETF RFC 3261], sauf indication contraire dans le présent sous-paragraphe.

La prise en charge, pour un seul appel, de multiples flux de média simultanés est facultative.

Il convient de noter que le comportement défini dans le présent sous-paragraphe ne s'applique qu'aux demandes et aux réponses qui se font en dehors d'un dialogue. Le comportement dans le cadre d'un dialogue est défini dans le § 10.2.1.12.

10.2.1.8.1 Comportement du client d'agent d'utilisateur

Le comportement des fonctions EUF et SCF doit être conforme au § 8.1 de la référence [IETF RFC 3261], sauf indication contraire dans le présent sous-paragraphe. 10.2.1.8.1.1 Formulation de la demande.

10.2.1.8.1.1 Formulation de la demande

Le comportement des fonctions EUF et SCF doit être conforme au § 8.1.1 de la référence [IETF RFC 3261], sauf indication contraire dans le présent sous-paragraphe.

L'identificateur Request-URI dans la demande contient l'adresse de l'entité appelée. Il s'agit habituellement d'un numéro de téléphone, mais il peut aussi s'agir d'un identificateur URI SIP général. Les champs From et To dans la demande peuvent contenir des chaînes aléatoires qui assurent la confidentialité de l'initiateur de la session.

Voir le § 10.2.1.20 pour plus de détails sur l'emploi des diverses valeurs du champ d'en-tête.

10.2.1.8.1.2 Envoi de la demande

Le comportement des fonctions EUF et SCF doit être conforme au § 8.1.2 de la référence [IETF RFC 3261].

10.2.1.8.1.3 Traitement des réponses

Le comportement des fonctions EUF et SCF doit être conforme au § 8.1.3 de la référence [IETF RFC 3261], sauf indication contraire dans le présent sous-paragraphe.

Si une autorisation SIP est requise, les fonctions EUF et SCF doivent appliquer les procédures d'autorisation SIP employant la réponse 401 (Unauthorized), conformément au § 8.1.3.5 de la référence [IETF RFC 3261].

L'application des procédures d'autorisation SIP où est employée la réponse 407 (Proxy Authentication Required) est facultative. Si elle se fait, elle doit être conforme au § 8.1.3.5 de la référence [IETF RFC 3261].

L'application des procédures de nouvelle tentative SIP, à la réception de la réponse 420 (Bad Extension), est facultative. Si elle se fait, elle doit être conforme au § 8.1.3.5 de la référence [IETF RFC 3261].

10.2.1.8.2 Comportement du serveur d'agent d'utilisateur

Le comportement des fonctions EUF et SCF doit être conforme au § 8.2 de la référence [IETF RFC 3261].

10.2.1.8.3 Serveurs de réacheminement

Le comportement des fonctions EUF et SCF doit être conforme au § 8.3 de la référence [IETF RFC 3261], sauf indication contraire dans le présent sous-paragraphe.

La fonction SCF n'est pas tenue d'assurer le rôle de serveur de réacheminement. Elle peut toutefois le faire et invoquer des réacheminements pour un nombre limité de demandes INVITE. La limitation du nombre de réacheminements permet de limiter le trafic de signalisation SIP au niveau de l'interface UNI et la complexité du traitement associée aux réacheminements. L'en-tête Max-Forwards (voir le § 10.2.1.20), qui est obligatoire dans toutes les demandes SIP, sert à limiter le nombre de bonds qu'une demande peut effectuer avant d'arriver à destination. Si la fonction de réacheminement est prise en charge, la fonction SCF doit être conforme au § 8.3 de la référence [IETF RFC 3261].

Les codes de réponse 3xx peuvent être pris en charge au niveau de l'interface UNI, selon la politique de réseau ou l'option d'un abonnement, pour assurer les réacheminements dans le réseau ou dans un réseau situé en aval, où est reçu le message INVITE.

10.2.1.9 Annulation d'une demande

Dans le présent sous-paragraphe et dans ses sous-paragrapes, le traitement propre à un intermédiaire ne s'applique que si la fonction SCF assure le rôle d'intermédiaire SIP. Le traitement propre à un agent d'utilisateur ne s'applique que si la fonction EUF assure le rôle d'agent d'utilisateur, à savoir un client UAC ou un serveur UAS, et si la fonction SCF assure le rôle d'agent d'utilisateur, à savoir un agent B2BUA ou un serveur de réacheminement. Finalement, le traitement propre à une unité d'enregistrement ne s'applique que si la fonction SCF assure le rôle d'unité d'enregistrement.

Le comportement des fonctions EUF et SCF doit être conforme au § 9 de la référence [IETF RFC 3261].

10.2.1.10 Enregistrements

Dans le présent sous-paragraphe et dans ses sous-paragrapes, le traitement propre à un intermédiaire ne s'applique que si la fonction SCF assure le rôle d'intermédiaire SIP. Le traitement propre à un agent d'utilisateur ne s'applique que si la fonction EUF assure le rôle d'agent d'utilisateur, à savoir un client UAC ou un serveur UAS, et si la fonction SCF assure le rôle d'agent d'utilisateur, à savoir un agent B2BUA ou un serveur de réacheminement. Finalement, le traitement propre à une unité d'enregistrement ne s'applique que si la fonction SCF assure le rôle d'unité d'enregistrement.

Le comportement des fonctions EUF et SCF doit être conforme au § 10 de la référence [IETF RFC 3261].

10.2.1.11 Interrogations concernant les capacités

Dans le présent sous-paragraphe et dans ses sous-paragrapes, le traitement propre à un intermédiaire ne s'applique que si la fonction SCF assure le rôle d'intermédiaire SIP. Le traitement propre à un agent d'utilisateur ne s'applique que si la fonction EUF assure le rôle d'agent d'utilisateur, à savoir un client UAC ou un serveur UAS, et si la fonction SCF assure le rôle d'agent d'utilisateur, à savoir un agent B2BUA ou un serveur de réacheminement. Finalement, le traitement propre à une unité d'enregistrement ne s'applique que si la fonction SCF assure le rôle d'unité d'enregistrement.

La prise en charge des interrogations concernant les capacités est facultative. Si elle est assurée, elle doit être conforme au § 11 de la référence [IETF RFC 3261].

10.2.1.12 Dialogues

Le présent sous-paragraphe et ses sous-paragrapes ne s'appliquent que si la fonction EUF assure le rôle d'agent d'utilisateur, à savoir un client UAC ou un serveur UAS, et uniquement si la fonction SCF assure le rôle d'agent d'utilisateur, à savoir un agent B2BUA ou un serveur de réacheminement.

Le comportement des fonctions EUF et SCF doit être conforme au § 12 de la référence [IETF RFC 3261], sauf indication contraire dans le présent sous-paragraphe.

10.2.1.12.1 Etablissement d'un dialogue

La prise en charge des identificateurs URI SIPS est facultative. Si elle est assurée, elle doit être conforme au § 12.1 de la référence [IETF RFC 3261].

10.2.1.12.2 Demandes dans le cadre d'un dialogue

La prise en charge des identificateurs URI SIPS est facultative. Si elle est assurée, elle doit être conforme au § 12.2 de la référence [IETF RFC 3261].

10.2.1.12.3 Achèvement d'un dialogue

Le comportement des fonctions EUF et SCF doit être conforme au § 12.3 de la référence [IETF RFC 3261].

10.2.1.13 Ouverture d'une session

Le présent sous-paragraphe et ses sous-paragrapes ne s'appliquent que si la fonction EUF assure le rôle d'agent d'utilisateur, à savoir un client UAC ou un serveur UAS, et si la fonction SCF assure le rôle d'agent d'utilisateur, à savoir un agent B2BUA ou un serveur de réacheminement.

Le comportement des fonctions EUF et SCF doit être conforme au § 13 de la référence [IETF RFC 3261], sauf indication contraire dans le présent sous-paragraphe.

Dans la mesure du possible, la fonction EUF côté envoi doit incorporer un type de corps de message "application/sdp" avec l'INVITE initiale.

La prise en charge de l'INVITE initiale sans offre SDP est recommandée afin que soit assuré l'interfonctionnement avec les réseaux H.323 et la fourniture des services utilisant la commande d'appel par un tiers.

Afin de procéder au choix du codec:

- Lorsque l'INVITE initiale contient une offre SDP, une réponse SDP peut être incorporée soit dans la réponse fiable provisoire de non-défaillance à l'INVITE (par exemple, 183-Session-Progress envoyé de manière fiable), soit dans la réponse finale de non-défaillance à l'INVITE (par exemple, 2xx), et, si elle n'est pas incorporée dans la réponse fiable provisoire de non-défaillance, elle doit l'être dans la réponse finale de non-défaillance. Lorsque la réponse finale de non-défaillance contient une réponse SDP, celle-ci peut être incorporée dans la réponse non fiable provisoire de non-défaillance à l'INVITE.
- Lorsque l'INVITE initiale ne contient pas d'offre SDP, l'offre SDP initiale doit être incorporée dans la première réponse fiable provisoire de non-défaillance à l'INVITE, à savoir la première réponse 18x envoyée de manière fiable (par exemple, 180-Ringing envoyé de manière fiable), lorsqu'elle existe, ou, lorsqu'elle n'existe pas, dans la réponse finale de non-défaillance à l'INVITE (par exemple, 2xx). Lorsque l'offre SDP initiale est contenue dans une réponse fiable provisoire, la réponse SDP doit être incorporée dans le message PRACK accusant réception de cette réponse. Lorsque l'offre initiale SDP est contenue dans la réponse finale de non-défaillance à l'INVITE (par exemple, 2xx), la réponse SDP doit être incorporée dans le message ACK accusant réception de cette réponse.

10.2.1.14 Modification d'une session établie

Le présent sous-paragraphe et ses sous-paragraphe ne s'appliquent que si la fonction EUF assure le rôle d'agent d'utilisateur, à savoir un client UAC ou un serveur UAS, et uniquement si la fonction SCF assure le rôle d'agent d'utilisateur, à savoir un agent B2BUA ou un serveur de réacheminement.

Le comportement des fonctions EUF et SCF doit être conforme au § 14 de la référence [IETF RFC 3261], sauf indication contraire dans le présent sous-paragraphe.

Lors de la formulation d'une réponse SDP à une offre SDP nouvellement reçue, contenue dans une demande INVITE réitérée ou dans une procédure UPDATE, ni la fonction SCF qui commande le plan de transfert, ni la fonction EUF ne doivent altérer l'adresse IP ou le numéro de port d'écoute qui ont été négociés au cours de la négociation SDP initiale pour un flux de média donné.

10.2.1.15 Clôture d'une session

Le présent sous-paragraphe et ses sous-paragraphe ne s'appliquent que si la fonction EUF assure le rôle d'agent d'utilisateur, à savoir un client UAC ou un serveur UAS, et uniquement si la fonction SCF assure le rôle d'agent d'utilisateur, à savoir un agent B2BUA ou un serveur de réacheminement.

Le comportement des fonctions EUF et SCF doit être conforme au § 15 de la référence [IETF RFC 3261].

10.2.1.16 Comportement de l'intermédiaire

Le présent sous-paragraphe et ses sous-paragraphe ne s'appliquent que si la fonction SCF assure le rôle d'intermédiaire SIP.

Le comportement de la fonction SCF doit être conforme au § 16 de la référence [IETF RFC 3261], sauf indication contraire dans le présent sous-paragraphe.

La prise en charge, pour un seul appel, de multiples flux de média simultanés est facultative.

10.2.1.17 Transactions

Dans le présent sous-paragraphe et dans ses sous-paragraphe, le traitement propre à un intermédiaire ne s'applique que si la fonction SCF assure le rôle d'intermédiaire SIP. Le traitement propre à un agent

d'utilisateur ne s'applique que si la fonction EUF assure le rôle d'agent d'utilisateur, à savoir un client UAC ou un serveur UAS, et si la fonction SCF assure le rôle d'agent d'utilisateur, à savoir un agent B2BUA ou un serveur de réacheminement. Finalement, le traitement propre à une unité d'enregistrement ne s'applique que si la fonction SCF assure le rôle d'unité d'enregistrement.

Le comportement des fonctions EUF et SCF doit être conforme au § 17 de la référence [IETF RFC 3261], sauf indication contraire dans le présent sous-paragraphe.

Les fonctions EUF et SCF peuvent renvoyer le code d'erreur 486 (Busy Here) en réponse à une demande INVITE pour un utilisateur, lorsqu'un dialogue concernant celui-ci est déjà établi et que la nouvelle INVITE n'est pas faite dans le cadre de ce dialogue.

10.2.1.18 Transport

Le comportement des fonctions EUF et SCF doit être conforme au § 18 de la référence [IETF RFC 3261]. Toutefois, en cas de conflit, le § 12 prévaut sur le § 18.

10.2.1.19 Composants de message communs

Les fonctions EUF et SCF doivent définir le profil SIP conformément au § 19 de la référence [IETF RFC 3261], sauf indication contraire dans le présent sous-paragraphe.

La prise en charge de l'identificateur URI SIPS est facultative. Si elle est assurée, elle doit être conforme au § 19.1.1 de la référence [IETF RFC 3261].

10.2.1.20 Champs d'en-tête

Les fonctions EUF et SCF doivent définir le profil SIP conformément au § 20 de la référence [IETF RFC 3261], sauf indication contraire dans le présent sous-paragraphe.

Ci-après sont énumérés les en-têtes SIP définis dans la référence [IETF RFC 3261] et sont indiquées les spécifications qui permettent leur prise en charge dans les fonctions EUF et SCF.

10.2.1.20.1 Accept

La prise en charge de l'en-tête Accept est facultative. Si elle est assurée, elle doit être conforme au § 20.1 de la référence [IETF RFC 3261].

10.2.1.20.2 Accept-Encoding

La prise en charge de l'en-tête Accept-Encoding est facultative. Si elle est assurée, elle doit être conforme au § 20.2 de la référence [IETF RFC 3261], sauf indication contraire ci-après.

L'en-tête Accept-Encoding peut être employé par les fonctions EUF et SCF. Le codage "identity" doit être pris en charge. D'autres codages peuvent également être pris en charge.

10.2.1.20.3 Accept-Language

La prise en charge de l'en-tête Accept-Language est facultative. Si elle est assurée, elle doit être conforme au § 20.3 de la référence [IETF RFC 3261].

10.2.1.20.4 Alert-Info

La prise en charge de l'en-tête Alert-Info est facultative. Si elle est assurée, elle doit être conforme au § 20.4 de la référence [IETF RFC 3261].

Il convient de noter que toute action sur l'en-tête Alert-Info comporte des risques en matière de sécurité, comme décrit audit § 20.4 de la référence [IETF RFC 3261].

10.2.1.20.5 Allow

La prise en charge de l'en-tête Allow doit être conforme au § 20.5 de la référence [IETF RFC 3261], sauf indication contraire ci-après.

L'en-tête Allow doit figurer dans l'INVITE initiale et dans la réponse 2xx à cette INVITE initiale.

L'en-tête doit énumérer toutes les procédures prises en charge, par exemple, INVITE, ACK, CANCEL, BYE, UPDATE et PRACK.

Les fonctions EUF et SCF doivent néanmoins être prêtes à recevoir des messages sans en-tête Allow. Elles doivent continuer à se charger de la commande d'appel, même si l'en-tête Allow ne figure ni dans l'INVITE initiale ni dans la réponse 2xx à cette INVITE initiale.

10.2.1.20.6 Authentication-Info

La prise en charge de l'en-tête Authentication-Info est facultative. Si elle est assurée, elle doit être conforme au § 20.6 de la référence [IETF RFC 3261].

10.2.1.20.7 Authorization

Si une autorisation SIP est requise, la fonction EUF doit se charger de l'envoi de l'en-tête Authorization tandis que la fonction SCF doit se charger de la réception de cet en-tête Authorization, conformément au § 20.7 de la référence [IETF RFC 3261]. La prise en charge tant de l'envoi que de la réception de l'en-tête Authorization par la fonction EUF, et la prise en charge de l'envoi de cet en-tête Authorization par la fonction SCF sont facultatives. Si elles sont assurées, elles doivent être conformes audit § 20.7 de la référence [IETF RFC 3261].

10.2.1.20.8 Call-ID

La prise en charge de l'en-tête Call-ID doit être conforme au § 20.8 de la référence [IETF RFC 3261], sauf indication contraire ci-après.

L'en-tête Call-ID doit être unique à l'échelle mondiale, comme décrit au § 8.1.1.4 de la référence [IETF RFC 3261], et doit comporter une suite de valeurs aléatoires suffisamment longue (celle de l'étiquette de l'en-tête From de la demande pouvant même être réutilisée) plutôt que l'adresse IP ou le nom du serveur ajouté à la fin de l'en-tête Call-ID, pour des raisons de protection de la confidentialité, comme décrit au § 4.1 de la référence [IETF RFC 3323]. Lorsque la confidentialité est requise par l'initiateur de la session, sa fonction EUF doit employer un en-tête Call-ID qui assure la confidentialité.

10.2.1.20.9 Call-Info

La prise en charge de l'en-tête Call-Info est facultative. Si elle est assurée, elle doit être conforme au § 20.9 de la référence [IETF RFC 3261].

Il convient de noter que toute action sur l'en-tête Call-Info comporte des risques en matière de sécurité, comme décrit audit § 20.9 de la référence [IETF RFC 3261].

10.2.1.20.10 Contact

La prise en charge de l'en-tête Contact doit être conforme au § 20.10 de la référence [IETF RFC 3261], sauf indication contraire ci-après.

Les fonctions EUF et SCF doivent définir le profil SIP de manière telle qu'un identificateur URI SIP puisse être inséré dans l'en-tête Contact d'une demande INVITE, d'une réponse fiable provisoire ou d'une réponse 2xx à une demande INVITE. La prise en charge de tout autre type d'identificateur URI est facultative.

Lorsque l'utilisateur exige la confidentialité, l'en-tête Contact ne doit pas contenir de nom de domaine. Il vaut mieux, dans ce cas, utiliser la forme d'adresse IP. Il convient de noter que, dans les systèmes à multiples interfaces de réseau, l'emploi d'une (unique) forme d'adresse IP peut diminuer la fiabilité du système dans son ensemble. Si de multiples interfaces existent et que la fiabilité est un point sensible, ne pas faire appel à la forme d'adresse IP est sans doute un bon compromis.

Les fonctions EUF et SCF doivent définir le profil SIP de manière telle qu'un identificateur URI SIP ou un identificateur URI téléphonique valable puisse être inséré dans l'en-tête Contact d'une réponse 3xx à une demande INVITE. Si la nouvelle destination est un numéro de téléphone, l'en-tête doit contenir un identificateur URI SIP ou un identificateur URI téléphonique avec le numéro de la nouvelle destination, comme décrit au § 10.2.1.7.1. La prise en charge de tout autre type d'identificateur URI est facultative.

10.2.1.20.11 Content-Disposition

La prise en charge de l'en-tête Content-Disposition est facultative. Si elle est assurée, elle doit être conforme au § 20.11 de la référence [IETF RFC 3261], sauf indication contraire ci-après.

L'en-tête Content-Disposition peut être employé par les fonctions EUF et SCF. La valeur "session" doit être prise en charge. D'autres valeurs peuvent également être prises en charge.

Si un média préalable est fourni par le type de serveur d'application défini dans la référence [IETF RFC 3959], l'en-tête Content-Disposition doit contenir la valeur "early-session" spécifiée dans ladite référence.

Il convient de noter que la valeur par défaut pour le type de corps de message "application/sdp" est "session", alors que la valeur par défaut pour tous les autres types de corps de message (par exemple, "message/sipfrag") est "render". Si la valeur par défaut n'est pas souhaitée, l'en-tête Content-Disposition doit être incorporé.

10.2.1.20.12 Content-Encoding

La prise en charge de l'en-tête Content-Encoding est facultative. Si elle est assurée, elle doit être conforme au § 20.12 de la référence [IETF RFC 3261], sauf indication contraire ci-après.

L'en-tête Content-Encoding peut être employé par les fonctions EUF et SCF. Le codage "identity" doit être pris en charge. D'autres codages peuvent également être pris en charge.

10.2.1.20.13 Content-Language

La prise en charge de l'en-tête Content-Language est facultative. Si elle est assurée, elle doit être conforme au § 20.13 de la référence [IETF RFC 3261].

10.2.1.20.14 Content-Length

L'en-tête Content-Length doit être pris en charge conformément au § 20.14 de la référence [IETF RFC 3261].

10.2.1.20.15 Content-Type

L'en-tête Content-Type doit être pris en charge conformément au § 20.15 de la référence [IETF RFC 3261], sauf indication contraire ci-après.

La valeur "application/sdp" doit être prise en charge. D'autres valeurs peuvent également être prises en charge.

Si un média préalable est fourni par le type de serveur d'application, défini dans la référence [IETF RFC 3261], le type de contenu "multipart/mixed" doit être pris en charge conformément à la référence [IETF RFC 2046], afin que soient précisés les types différents de session (par exemple, session normale ou session préalable). Chacun des types de contenu est spécifié au moyen de l'étiquette "boundary", insérée dans cet en-tête.

10.2.1.20.16 CSeq

L'en-tête CSeq doit être pris en charge conformément au § 20.16 de la référence [IETF RFC 3261].

10.2.1.20.17 Date

La prise en charge de l'en-tête Date est facultative. Si elle est assurée, elle doit être conforme au § 20.17 de la référence [IETF RFC 3261].

10.2.1.20.18 Error-Info

La prise en charge de l'en-tête Error-Info est facultative. Si elle est assurée, elle doit être conforme au § 20.18 de la référence [IETF RFC 3261].

Il convient de noter que toute action sur l'en-tête Error-Info comporte des risques en matière de sécurité, comme décrit au § 20.18 de la référence [IETF RFC 3261].

10.2.1.20.19 Expires

La prise en charge de l'en-tête Expires est facultative. Si elle est assurée, elle doit être conforme au § 20.19 de la référence [IETF RFC 3261].

10.2.1.20.20 From

L'en-tête From doit être pris en charge conformément au § 20.20 de la référence [IETF RFC 3261], sauf indication contraire ci-après.

Afin d'assurer la confidentialité de l'utilisateur, la fonction SCF limite les contenus admissibles de l'en-tête From.

Lorsque l'initiateur de la session exige la confidentialité, la fonction EUF doit produire un en-tête From selon les règles suivantes:

- Le nom display-name peut être "Anonymous".
- La partie userinfo de la spécification addr-spec doit contenir l'identificateur "anonymous".
- La spécification addr-spec doit contenir le nom de serveur "anonymous.invalid", qui ne permet pas l'identification.

10.2.1.20.21 In-Reply-To

La prise en charge de l'en-tête In-Reply-To est facultative. Si elle est assurée, elle doit être conforme au § 20.21 de la référence [IETF RFC 3261].

10.2.1.20.22 Max-Forwards

La prise en charge de la réception de l'en-tête Max-Forwards par la fonction EUF est facultative. Si elle est assurée, elle doit être conforme au § 20.22 de la référence [IETF RFC 3261]. La fonction EUF doit se charger de l'envoi de l'en-tête Max-Forwards conformément audit § 20.22 de la référence [IETF RFC 3261].

La fonction SCF doit prendre en charge l'en-tête Max-Forwards conformément audit § 20.22 de la référence [IETF RFC 3261], sauf indication contraire ci-après.

Lorsqu'un agent B2BUA, au niveau d'une fonction SCF, transmet une demande, il emploie une valeur pour l'en-tête Max-Forwards qui est égale à la valeur Max-Forwards entrante moins un.

10.2.1.20.23 Min-Expires

La fonction EUF doit se charger de la réception de l'en-tête Min-Expires et la fonction SCF doit se charger de l'envoi de cet en-tête Min-Expires conformément au § 20.23 de la référence [IETF RFC 3261]. La prise en charge de l'en-tête Min-Expires dans le sens qui va de la fonction EUF à la fonction SCF est sans objet.

10.2.1.20.24 MIME-Version

La prise en charge de l'en-tête MIME-Version est facultative. Si elle est assurée, elle doit être conforme au § 20.24 de la référence [IETF RFC 3261], sauf indication contraire ci-après.

La valeur "1.0" pour la version doit être prise en charge. D'autres valeurs peuvent également être prises en charge.

10.2.1.20.25 Organization

La prise en charge de l'en-tête Organization est facultative. Si elle est assurée, elle doit être conforme au § 20.25 de la référence [IETF RFC 3261].

10.2.1.20.26 Priority

La prise en charge de l'en-tête Priority est facultative. Si elle est assurée, elle doit être conforme au § 20.26 de la référence [IETF RFC 3261].

Il convient de noter que l'action par des entités sur cet en-tête peut avoir des répercussions d'ordre sécuritaire.

10.2.1.20.27 Proxy-Authenticate

La prise en charge de la réception de l'en-tête Proxy-Authenticate par la fonction EUF et la prise en charge de l'envoi de cet en-tête Proxy-Authenticate par la fonction SCF sont facultatives. Si elles sont assurées, elles doivent être conformes au § 20.27 de la référence [IETF RFC 3261]. La prise en charge de l'en-tête Proxy-Authenticate dans le sens qui va de la fonction EUF à la fonction SCF est sans objet.

10.2.1.20.28 Proxy-Authorization

La prise en charge de l'envoi de l'en-tête Proxy-Authorization par la fonction EUF et la prise en charge de la réception de cet en-tête Proxy-Authorization par la fonction SCF sont facultatives. Si elles sont assurées, elles doivent être conformes au § 20.28 de la référence [IETF RFC 3261]. La prise en charge de l'en-tête Proxy-Authorization dans le sens qui va de la fonction SCF à la fonction EUF est sans objet.

10.2.1.20.29 Proxy-Require

La fonction SCF doit se charger de la réception de l'en-tête Proxy-Require. La prise en charge tant de l'envoi que de la réception de l'en-tête Proxy-Require par la fonction EUF et la prise en charge de l'envoi de cet en-tête Proxy-Require par la fonction SCF sont facultatives. Si elles sont assurées, elles doivent être conformes au § 20.29 de la référence [IETF RFC 3261], sauf indication contraire ci-après.

L'étiquette d'option "privacy" doit être prise en charge conformément à la référence [IETF RFC 3323]. D'autres étiquettes d'option peuvent également être prises en charge.

10.2.1.20.30 Record-Route

L'en-tête Record-Route doit être pris en charge conformément au § 20.30 de la référence [IETF RFC 3261].

10.2.1.20.31 Reply-To

La prise en charge de l'en-tête Reply-To est facultative. Si elle est assurée, elle doit être conforme au § 20.31 de la référence [IETF RFC 3261].

10.2.1.20.32 Require

L'en-tête Require doit être pris en charge conformément au § 20.32 de la référence [IETF RFC 3261], sauf indication contraire ci-après.

L'étiquette d'option "timer" doit être prise en charge par les fonctions EUF et SCF conformément à la référence [IETF RFC 4028]. L'étiquette d'option "100rel" doit être prise en charge par la fonction EUF, si une réponse provisoire fiable est requise, et doit être prise en charge par la fonction SCF

conformément à la référence [IETF RFC 3262]. D'autres étiquettes d'option peuvent également être prises en charge.

Si un média préalable est fourni par le type de serveur d'application défini dans la référence [IETF RFC 3959], et que le client UAC s'attend à ce que le serveur UAS prenne en charge la procédure de demande de média préalable, l'en-tête Require doit contenir la valeur "early-session" spécifiée dans ladite référence.

10.2.1.20.33 Retry-After

La prise en charge de l'en-tête Retry-After est facultative. Si elle est assurée, elle doit être conforme au § 20.33 de la référence [IETF RFC 3261], sauf indication contraire ci-après.

Après soumission de la demande REGISTER, une fonction EUF peut recevoir une réponse d'erreur avec un en-tête Retry-After. Dans ce cas, il est recommandé de renvoyer la demande au terme du temps spécifié dans l'en-tête Retry-After.

10.2.1.20.34 Route

La fonction EUF doit se charger de l'envoi de l'en-tête Route et la fonction SCF doit se charger de la réception de cet en-tête Route conformément au § 20.34 de la référence [IETF RFC 3261].

La prise en charge de l'en-tête Route dans le sens qui va de la fonction SCF à la fonction EUF est sans objet.

10.2.1.20.35 Server

La prise en charge de l'en-tête Server est facultative. Si elle est assurée, elle doit être conforme au § 20.35 de la référence [IETF RFC 3261].

10.2.1.20.36 Subject

La prise en charge de l'en-tête Subject est facultative. Si elle est assurée, elle doit être conforme au § 20.36 de la référence [IETF RFC 3261].

10.2.1.20.37 Supported

L'en-tête Supported doit être pris en charge conformément au § 20.37 de la référence [IETF RFC 3261], sauf indication contraire ci-après.

L'étiquette d'option "timer" doit être prise en charge conformément à la référence [IETF RFC 4028]. L'étiquette d'option "100rel" doit être prise en charge par la fonction EUF, si une réponse provisoire fiable est requise, et doit être prise en charge par la fonction SCF conformément à la référence [IETF RFC 3262]. D'autres étiquettes d'option peuvent également être prises en charge.

Si un média préalable est fourni par le type de serveur d'application, défini dans la référence [IETF RFC 3959], l'en-tête Supported doit contenir la valeur "early-session" spécifiée dans ladite référence.

10.2.1.20.38 Timestamp

La prise en charge de l'en-tête Timestamp est facultative. Si elle est assurée, elle doit être conforme au § 20.38 de la référence [IETF RFC 3261], sauf indication contraire ci-après.

Les fonctions EUF et SCF peuvent envoyer l'en-tête Timestamp dans les demandes. En cas de réception, cet en-tête doit être exploité comme décrit audit § 20.38 de la référence [IETF RFC 3261].

10.2.1.20.39 To

L'en-tête To doit être pris en charge conformément au § 20.39 de la référence [IETF RFC 3261], sauf indication contraire ci-après.

Afin d'assurer la confidentialité de l'utilisateur, les fonctions EUF et SCF peuvent limiter les contenus admissibles de l'en-tête To. Habituellement, l'en-tête To indique les chiffres composés dans l'identificateur URI SIP ou l'identificateur URI téléphonique. Cette information, dont la portée s'étend d'un bout à l'autre, peut donner des informations sur l'emplacement de l'appelant, par exemple, une entreprise, et indiquer si l'appel est local, interurbain ou international.

Lorsque l'appelant exige la confidentialité, les fonctions EUF et SCF peuvent produire un en-tête To selon les règles suivantes:

- Le nom display-name ne doit pas y figurer".
- Si un numéro de téléphone international est employé, la partie userinfo de la spécification addr-spec doit comporter un numéro E.164 complet comprenant l'indicatif du pays.
- La partie serveur de la spécification addr-spec doit contenir le nom de serveur "anonymous.invalid", qui ne permet pas l'identification.

Si l'anonymat n'est pas exigé par l'appelant et que l'utilisateur a composé un numéro de téléphone, l'en-tête To doit comporter un identificateur URI SIP ou un identificateur URI téléphonique contenant les chiffres composés.

10.2.1.20.40 Unsupported

L'en-tête Unsupported doit être pris en charge conformément au § 20.40 de la référence [IETF RFC 3261].

10.2.1.20.41 User-Agent

La prise en charge de l'en-tête User-Agent est facultative. Si elle est assurée, elle doit être conforme au § 20.41 de la référence [IETF RFC 3261].

10.2.1.20.42 Via

L'en-tête Via doit être pris en charge conformément au § 20.42 de la référence [IETF RFC 3261].

10.2.1.20.43 Warning

La prise en charge de l'en-tête Warning est facultative. Si elle est assurée, elle doit être conforme au § 20.43 de la référence [IETF RFC 3261].

10.2.1.20.44 WWW-Authenticate

Si une autorisation SIP est requise, la fonction EUF doit se charger de la réception de l'en-tête WWW-Authenticate et la fonction SCF doit se charger de l'envoi de cet en-tête WWW-Authenticate conformément au § 20.44 de la référence [IETF RFC 3261].

La prise en charge de l'envoi de l'en-tête WWW-Authenticate par la fonction EUF et la prise en charge de la réception de cet en-tête WWW-Authenticate par la fonction SCF sont facultatives. Si elles sont assurées, elles doivent être conformes audit § 20.44 de la référence [IETF RFC 3261].

10.2.1.21 Codes de réponse

Les fonctions EUF et SCF doivent définir le profil SIP conformément au § 21 de la référence [IETF RFC 3261].

10.2.1.22 Emploi de l'authentification HTTP

La prise en charge de l'authentification HTTP est facultative. Si elle est assurée, elle doit être conforme au § 22 de la référence [IETF RFC 3261].

10.2.1.23 Extensions S/MIME

La prise en charge des extensions S/MIME est facultative. Si elle est assurée, elle doit être conforme au § 23 de la référence [IETF RFC 3261].

10.2.1.24 Exemples

Le § 24 de la référence [IETF RFC 3261] est mentionné à titre informatif.

10.2.1.25 Forme de Backus-Naur (BNF) augmentée pour le protocole SIP

Les fonctions EUF et SCF doivent définir le profil SIP conformément au § 25 de la référence [IETF RFC 3261].

10.2.2 Profil SIP applicable aux extensions de la référence [IETF RFC 3261]

Le présent paragraphe définit les extensions des procédures, des en-têtes et des codes de réponse, spécifiées dans les normes RFC, autres que la référence [IETF RFC 3261], qui doivent obligatoirement être prises en charge et qui sont énumérées au § 10.1. Si la prise en charge d'une norme RFC est facultative, les procédures, les en-têtes et les codes de réponse spécifiés dans cette norme RFC sont aussi facultatifs, et le présent paragraphe ne les décrit pas individuellement.

10.2.2.1 Extensions des procédures

La fonction SCF doit se charger des procédures UPDATE et PRACK, tandis que la fonction EUF doit se charger de la procédure UPDATE, ainsi que de la procédure PRACK au cas où une réponse provisoire fiable est requise.

10.2.2.1.1 UPDATE

Les fonctions EUF et SCF doivent se charger de la procédure UPDATE conformément à la référence [IETF RFC 3311].

La procédure UPDATE doit être employée pour mettre à jour les paramètres de session avant que l'INVITE initiale ne soit achevée.

Après achèvement de l'INVITE initiale, une réitération de l'INVITE ou une procédure UPDATE peut être employée. Il est recommandé d'employer la réitération de l'INVITE pour mettre à jour les paramètres de session. En particulier, pendant la communication, l'ajout de nouveaux médias à une session média établie précédemment ou la suppression d'un média doivent se faire au moyen de la réitération de l'INVITE plutôt que de la procédure UPDATE, avec la description des nouveaux médias contenant les profils SDP modifiés conformément à la procédure d'offre/de demande SDP.

10.2.2.1.2 PRACK

La fonction SCF doit se charger de la procédure PRACK conformément à la référence [IETF RFC 3262].

Si une réponse provisoire fiable est requise, la fonction EUF doit se charger de la procédure PRACK conformément à la référence [IETF RFC 3262]. Si la fonction EUF côté envoi émet une demande initiale qui contient l'en-tête "Require" avec l'étiquette d'option "100rel" afin de garantir la fiabilité de la réponse provisoire, la fonction EUF côté réception doit insérer l'en-tête "Require" avec l'étiquette d'option "100rel" dans la réponse provisoire. Si la réponse provisoire SIP, autre que 100, contient un en-tête "Require" avec l'étiquette d'option "100rel", la fonction EUF côté envoi doit renvoyer une demande PRACK conformément à ladite référence [IETF RFC 3262]. Si la fonction EUF côté envoi émet une demande initiale qui contient l'en-tête "Supported" avec l'étiquette d'option "100rel", la fonction EUF côté réception peut envoyer de manière fiable toute réponse provisoire à l'INVITE, autre que 100. Lorsqu'une réponse provisoire SIP, autre que 100, contient une étiquette d'option "early-session" ou "precondition" dans l'en-tête "Require", elle doit contenir l'étiquette "100rel" dans le champ d'en-tête Supported.

10.2.2.2 Extensions des en-têtes

10.2.2.2.1 Min-SE

L'en-tête Min-SE indique la valeur minimale de l'intervalle entre les sessions, exprimé en delta-secondes.

La prise en charge de l'envoi de l'en-tête Min-SE par la fonction EUF est facultative. Si elle est assurée, elle doit être conforme à la référence [IETF RFC 4028]. La fonction EUF doit se charger de la réception de l'en-tête Min-SE conformément à ladite référence [IETF RFC 4028].

La fonction SCF doit prendre en charge l'en-tête Min-SE conformément à ladite référence [IETF RFC 4028].

10.2.2.2.2 P-Asserted-Identity

Le champ d'en-tête P-Asserted-Identity est utilisé entre des entités SIP de confiance, pour transmettre l'identité de l'expéditeur d'un message SIP, telle qu'elle a été vérifiée par une authentification.

La fonction EUF doit se charger de la réception de l'en-tête P-Asserted-Identity et la fonction SCF doit se charger de l'envoi de cet en-tête P-Asserted-Identity conformément à la référence [IETF RFC 3325]. La prise en charge de l'en-tête P-Asserted-Identity dans le sens qui va de la fonction EUF à la fonction SCF est sans objet.

10.2.2.2.3 P-Preferred-Identity

Le champ d'en-tête P-Preferred-Identity est employé pour transmettre, entre un agent d'utilisateur et un intermédiaire de confiance, l'identité que l'expéditeur du message SIP souhaite utiliser pour la valeur du champ P-Asserted-Identity, à insérer par l'élément de confiance.

La prise en charge de l'envoi de l'en-tête P-Preferred-Identity par la fonction EUF est facultative. Si elle est assurée, elle doit être conforme à la référence [IETF RFC 3325]. La fonction SCF doit se charger de la réception de l'en-tête P-Preferred-Identity conformément à ladite référence [IETF RFC 3325]. La prise en charge de l'en-tête P-Preferred-Identity dans le sens qui va de la fonction SCF à la fonction EUF est sans objet.

10.2.2.2.4 Privacy

L'en-tête Privacy permet à un agent d'utilisateur de demander un certain degré de confidentialité pour un message.

La fonction EUF doit se charger de la réception de l'en-tête Privacy et la fonction SCF doit se charger tant de l'envoi que de la réception de l'en-tête Privacy. La prise en charge de l'envoi de l'en-tête Privacy par la fonction EUF est facultative.

Si la prise en charge est assurée, elle doit être conforme à la référence [IETF RFC 3323], sauf indication contraire ci-après.

L'option de confidentialité "id" doit être prise en charge. Mais d'autres options de confidentialité peuvent également être prises en charge, selon la politique de réseau ou l'option de l'abonnement.

10.2.2.2.5 RACK

L'en-tête RACK est envoyé dans une demande PRACK afin d'assurer la fiabilité des réponses provisoires.

L'en-tête RACK doit être pris en charge par la fonction EUF, si une réponse provisoire fiable est requise, conformément à la référence [IETF RFC 3262], et doit être pris en charge par la fonction SCF conformément à ladite référence [IETF RFC 3262].

10.2.2.2.6 RSeq

L'en-tête RSeq est employé dans les réponses provisoires afin de les transmettre de manière fiable.

L'en-tête RSeq doit être pris en charge par la fonction EUF, si une réponse provisoire fiable est requise, conformément à la référence [IETF RFC 3262], et par la fonction SCF conformément à ladite référence [IETF RFC 3262].

10.2.2.2.7 Session-Expires

Le champ d'en-tête Session-Expires transmet, pour une session SIP, l'intervalle entre les sessions.

L'en-tête Session-Expires doit être pris en charge conformément à la référence [IETF RFC 4028].

10.2.2.3 Extensions des codes de réponse

10.2.2.3.1 Code 422 (Session Interval Too Small)

La prise en charge de l'envoi du code 422 (intervalle entre sessions trop court) par la fonction EUF est facultative. Si elle est assurée, elle doit être conforme à la référence [IETF RFC 4028]. La fonction EUF doit se charger de la réception du code 422 (Session Interval Too Small) conformément à ladite référence [IETF RFC 4028].

La fonction SCF doit prendre en charge le code 422 (Session Interval Too Small) conformément à ladite référence [IETF RFC 4028].

10.2.3 Synthèse des procédures et des en-têtes SIP

La prise en charge des procédures et des en-têtes SIP suivants est obligatoire, facultative ou sans objet, comme spécifié dans les Tableaux 4, 5, 6 et 7. La prise en charge de la transmission ou de la réception d'une procédure ou d'un en-tête SIP donné signifie que la procédure et l'en-tête doit traverser l'interface UNI de manière fiable et ne signifie pas que l'en-tête doive toujours figurer dans les messages SIP concernés au niveau de l'interface UNI.

NOTE – Pour des informations sur la prise en charge des réponses, voir la référence [IETF RFC 3261].

Tableau 4 – Procédures [IETF RFC 3261]

Procédure	EUF→SCF		SCF→EUF		Référence
	EUF Send	SCF Recv	SCF Send	EUF Recv	
ACK	O	O	O	O	Voir le § 10.2.1.7.1
BYE	O	O	O	O	Voir le § 10.2.1.7.1
CANCEL	O	O	O	O	Voir le § 10.2.1.7.1
INVITE	O	O	O	O	Voir le § 10.2.1.7.1
OPTIONS	F	F	F	F	Voir le § 10.2.1.7.1
REGISTER	O	O	s.o.	s.o.	Voir le § 10.2.1.7.1

Tableau 5 – Extensions des procédures

Procédure	EUF→SCF		SCF→EUF		Référence	Norme RFC
	EUF Send	SCF Recv	SCF Send	EUF Recv		
PRACK	C	O	O	C	Voir le § 10.2.1.7.1	RFC 3262
UPDATE	O	O	O	O	Voir le § 10.2.1.7.1	RFC 3311

C: La procédure est conditionnellement obligatoire lorsqu'une réponse provisoire fiable est requise.

Tableau 6 – En-têtes [IETF RFC 3261]

En-tête	EUF→SCF		SCF→EUF		Référence
	EUF Send	SCF Recv	SCF Send	EUF Recv	
Accept	F	F	F	F	Voir le § 10.2.1.20.1
Accept-Encoding	F	F	F	F	Voir le § 10.2.1.20.2
Accept-Language	F	F	F	F	Voir le § 10.2.1.20.3
Alert-Info	F	F	F	F	Voir le § 10.2.1.20.4
Allow	O	O	O	O	Voir le § 10.2.1.20.5
Authentication-Info	F	F	F	F	Voir le § 10.2.1.20.6
Authorization	C	C	F	F	Voir le § 10.2.1.20.7
Call-ID	O	O	O	O	Voir le § 10.2.1.20.8
Call-Info	F	F	F	F	Voir le § 10.2.1.20.9
Contact	O	O	O	O	Voir le § 10.2.1.20.10
Content-Disposition	F	F	F	F	Voir le § 10.2.1.20.11
Content-Encoding	F	F	F	F	Voir le § 10.2.1.20.12
Content-Language	F	F	F	F	Voir le § 10.2.1.20.13
Content-Length	O	O	O	O	Voir le § 10.2.1.20.14
Content-Type	O	O	O	O	Voir le § 10.2.1.20.15
CSeq	O	O	O	O	Voir le § 10.2.1.20.16
Date	F	F	F	F	Voir le § 10.2.1.20.17
Error-Info	F	F	F	F	Voir le § 10.2.1.20.18
Expires	F	F	F	F	Voir le § 10.2.1.20.19
From	O	O	O	O	Voir le § 10.2.1.20.20
In-Reply-To	F	F	F	F	Voir le § 10.2.1.20.21
Max-Forwards	O	O	O	F	Voir le § 10.2.1.20.22
Min-Expires	s.o.	s.o.	O	O	Voir le § 10.2.1.20.23
MIME-Version	F	F	F	F	Voir le § 10.2.1.20.24
Organization	F	F	F	F	Voir le § 10.2.1.20.25
Priority	F	F	F	F	Voir le § 10.2.1.20.26
Proxy-Authenticate	s.o.	s.o.	F	F	Voir le § 10.2.1.20.27
Proxy-Authorization	F	F	s.o.	s.o.	Voir le § 10.2.1.20.28
Proxy-Require	F	O	F	F	Voir le § 10.2.1.20.29
Record-Route	O	O	O	O	Voir le § 10.2.1.20.30
Reply-To	F	F	F	F	Voir le § 10.2.1.20.31
Require	O	O	O	O	Voir le § 10.2.1.20.32
Retry-After	F	F	F	F	Voir le § 10.2.1.20.33
Route	O	O	s.o.	s.o.	Voir le § 10.2.1.20.34
Server	F	F	F	F	Voir le § 10.2.1.20.35
Subject	F	F	F	F	Voir le § 10.2.1.20.36

Tableau 6 – En-têtes [IETF RFC 3261]

En-tête	EUF→SCF		SCF→EUF		Référence
	EUF Send	SCF Recv	SCF Send	EUF Recv	
Supported	O	O	O	O	Voir le § 10.2.1.20.37
Timestamp	F	F	F	F	Voir le § 10.2.1.20.38
To	O	O	O	O	Voir le § 10.2.1.20.39
Unsupported	O	O	O	O	Voir le § 10.2.1.20.40
User-Agent	F	F	F	F	Voir le § 10.2.1.20.41
Via	O	O	O	O	Voir le § 10.2.1.20.42
Warning	F	F	F	F	Voir le § 10.2.1.20.43
WWW-Authenticate	F	F	C	C	Voir le § 10.2.1.20.44
C: L'en-tête est conditionnellement obligatoire lorsque l'autorisation SIP est requise.					

Tableau 7 – Extensions des en-têtes

En-tête	EUF→SCF		SCF→EUF		Référence	Norme RFC
	EUF Send	SCF Recv	SCF Send	EUF Recv		
Min-SE	F	O	O	O	Voir le § 10.2.2.2.1	RFC 4028
P-Asserted-Identity	s.o.	s.o.	O	O	Voir le § 10.2.2.2.2	RFC 3325
P-Preferred-Identity	F	O	s.o.	s.o.	Voir le § 10.2.2.2.3	RFC 3325
Privacy	F	O	O	O	Voir le § 10.2.2.2.4	RFC 3323
RAck	C	O	O	C	Voir le § 10.2.2.2.5	RFC 3262
RSeq	C	O	O	C	Voir le § 10.2.2.2.6	RFC 3262
Session-Expires	O	O	O	O	Voir le § 10.2.2.2.7	RFC 4028
C: L'en-tête est conditionnellement obligatoire lorsque l'autorisation SIP est requise.						

Dans les tableaux ci-dessus, les codes O, F, C et s.o. ont la signification suivante:

Tableau 8 – Détails des codes dans les Tableaux 4, 5, 6, et 7

Code	Nom de code	EUF→SCF		SCF→EUF	
		EUF Send	SCF Recv	SCF Send	EUF Recv
O	Obligatoire	<p>La capacité doit être prise en charge.</p> <p>La fonction EUF doit être en mesure d'assurer l'envoi sur demande.</p>	<p>La capacité doit être prise en charge.</p> <p>La prise en charge de la réception d'un message ou d'un en-tête SIP par la fonction SCF au niveau de l'interface UNI signifie que, s'il provient de l'interface UNI, ce message ou cet en-tête doit être traité comme prévu. Cela n'implique pas que les éléments du réseau desservi ou que l'équipement d'utilisateur relié à ce réseau doivent prendre en charge ce message ou cet en-tête.</p> <p>Le traitement ne doit pas être poursuivi si les informations nécessaires ne sont pas disponibles (une procédure appropriée de déconnexion/libération doit être exécutée).</p> <p>Toutefois, lorsqu'une valeur par défaut a été choisie, le traitement est effectué avec cette valeur.</p>	<p>La capacité doit être prise en charge.</p> <p>La prise en charge de l'envoi d'un message ou d'un en-tête SIP par la fonction SCF au niveau de l'interface UNI signifie que, s'il provient du réseau desservi, ce message ou cet en-tête doit être traité au niveau de l'interface UNI. Cela n'implique pas que les éléments du réseau desservi ou que l'équipement d'utilisateur relié à ce réseau doivent prendre en charge ce message ou cet en-tête.</p>	<p>La capacité doit être prise en charge.</p> <p>Le traitement ne doit pas être poursuivi si les informations nécessaires ne sont pas disponibles (une procédure appropriée de déconnexion/libération doit être exécutée).</p> <p>Toutefois, lorsqu'une valeur par défaut a été choisie, le traitement est effectué avec cette valeur.</p>

Tableau 8 – Détails des codes dans les Tableaux 4, 5, 6, et 7

Code	Nom de code	EUF→SCF		SCF→EUF	
		EUF Send	SCF Recv	SCF Send	EUF Recv
F	Facultatif	La capacité peut être prise en charge par la fonction EUF au niveau de l'interface UNI ou ne pas l'être. Il s'agit d'un choix de mise en oeuvre.	La capacité peut être prise en charge par la fonction SCF au niveau de l'interface UNI ou ne pas l'être. Il s'agit d'un choix de mise en oeuvre. Dans la mesure du possible, le traitement auquel s'attend la fonction EUF côté envoi doit être effectué. Lorsque le traitement auquel s'attend la fonction EUF ne peut être effectué, il ne doit pas être tenu compte du contenu reçu, et le traitement doit être poursuivi.	La capacité peut être prise en charge ou ne pas l'être par la fonction SCF au niveau de l'interface UNI. Il s'agit d'un choix de mise en oeuvre.	Comme pour la fonction EUF côté envoi. Dans la mesure du possible, le traitement auquel s'attend la fonction SCF côté envoi doit être effectué. Lorsque le traitement auquel s'attend la fonction SCF côté envoi ne peut être effectué, il ne doit pas être tenu compte du contenu reçu, et le traitement doit être poursuivi.
C <entier>	Conditionnel	La prescription en matière de capacité ("O", "F") dépend de la prise en charge d'autres éléments facultatifs ou conditionnels. L'indice <entier> est l'identificateur de l'expression conditionnelle.	Comme pour la fonction EUF côté envoi.	Comme pour la fonction EUF côté envoi.	Comme pour la fonction EUF côté envoi.
s.o.	sans objet	Il est impossible d'employer la capacité. Aucune réponse dans la colonne de prise en charge n'est requise.	Comme pour la fonction EUF côté envoi.	Comme pour la fonction EUF côté envoi.	Comme pour la fonction EUF côté envoi.

10.3 Profil SDP

10.3.1 Emploi du profil SDP

Le présent paragraphe définit un profil SDP applicable aux fonctions EUF et SCF. Il définit aussi un ensemble d'améliorations et de restrictions apportées à une mise en oeuvre SDP normalisée, qui reposent sur les références [IETF RFC 2327] et [IETF RFC 4566]. Dans le Tableau 9, les codes O, F et C ont la même signification que dans le Tableau 8.

Tableau 9 – Emploi du profil SDP

Élément	EUF→SCF		SCF→EUF	
	EUF Send	SCF Recv	SCF Send	EUF Recv
Description de session				
v = (version de protocole)	O	O	O	O
o = (propriétaire/créateur et identificateur de session)	O	O	O	O
s = (nom de session)	O	O	O	O
i = (informations sur la session)	F	O	F	O
u = (identificateur URI de description)	F	F	F	F
e = (adresse de courrier électronique)	F	F	F	F
p = (numéro de téléphone)	F	F	F	F
c = (informations sur la connexion)	C1	O	C1	O
b = (informations sur la largeur de bande)	F	O	F	O
Description temporelle (un ou plusieurs par description)				
t = (durée d'activité de la session)	O	O	O	O
r = (zéro, une ou plusieurs répétitions)	F	F	F	F
Description au niveau session (suite)				
z = (réglages de fuseau horaire)	F	F	F	F
k = (clé de chiffrement)	F	F	F	F
a = (zéro, une ou plusieurs rubriques attribut de session)	F	O	F	O
Description de média (zéro, un ou plusieurs par description)				
m = (nom de média et destination de transport)	C2	O	C2	O
i = (titre de média)	F	F	F	F
c = (informations sur la connexion)	C1, C2	O	C1, C2	O
b = (informations sur la largeur de bande)	F	O	F	O
k = (clé de chiffrement)	F	F	F	F
a = (zéro, une ou plusieurs rubriques attribut de média) (Note)	F	O	F	O

C1: Au moins une des rubriques 'c' figurant dans les descriptions de session et de média doit être remplie.

C2: Dans le cas de la description de média, les deux rubriques 'm' et 'c' doivent être remplies.

NOTE – Dans le cas d'une session vidéo, la description de la session devrait être incorporée dans le champ 'fmp' à la rubrique 'a' du profil SDP, comme spécifié dans les références [b-IETF RFC 2429] et [IETF RFC 4629], ainsi que dans les normes RFC, qui définissent le format propre au codec. La fréquence des images peut être incorporée dans le champ 'framerate' à la rubrique 'a'. Si elle l'est, la valeur de ce champ 'framerate' doit être la même que la fréquence d'images incorporée dans le champ 'fmp'.

NOTE – Dans le Tableau 9, le statut des mises en oeuvre est celui qui est spécifié dans le Tableau 8. Par exemple, même si la rubrique 'c' figure dans la description de média, cela ne veut pas dire que toutes les descriptions de média dans un message SIP/SDP donné contiennent cette rubrique 'c'. Lorsque la rubrique 'c' figure dans la description de session, cette rubrique 'c' peut ne pas être contenue dans la description de média.

Si une session média au niveau de l'interface UNI emploie la vidéo, le type de média "video" doit être pris en charge. Les paramètres de description de média spécifiés dans le Tableau 9 (par exemple, le codec de média, ses attributs et ses valeurs) sont échangés dans un message SIP/SDP en vue de l'établissement d'une connexion vidéo.

10.3.2 Capacités de négociation

Lors de l'envoi d'une réponse SDP, pour chaque type de média accepté (indiqué par la rubrique "m="), la fonction EUF côté réponse ne doit choisir, parmi les formats de média proposés dans l'offre SDP reçue, que le premier format de média pris en charge. Cela est différent de ce qui se passe pour le format de média "telephone-event", qui est incorporé dans la réponse SDP s'il est employé.

11 Profil applicable au niveau transport

11.1 Spécifications à prendre en charge

Dans le Tableau 10, les codes O et F ont la même signification que celle qui est définie au § 10.1.

Tableau 10 – Spécifications applicables au niveau transport à prendre en charge

Spécification	Titre	Fonction EUF	Fonction SCF
[IETF RFC 3016]	"RTP Payload Format for MPEG-4 Audio/Visual Streams"	F	F
[IETF RFC 3047]	"RTP Payload Format for UIT-T Recommendation G.722.1"	F	F
[IETF RFC 3267]	"Real-time Transport Protocol (RTP) Payload Format and File Storage Format for the Adaptive Multi-Rate (AMR) and Adaptive Multi-Rate Wideband (AMR-WB) Audio Codecs"	F	F
[IETF RFC 3389]	"RTP Payload for Comfort Noise"	F (Note 1)	F (Note 1)
[IETF RFC 3550]	"RTP: A Transport Protocol for Real-Time Applications"	O	O
[IETF RFC 3551]	"RTP Profile for Audio and Video Conferences with Minimal Control"	O	O
[IETF RFC 3558]	"RTP Payload Format for Enhanced Variable Rate Codecs (EVRC) and Selectable Mode Vocoders (SMV)"	F	F
[IETF RFC 3611]	"RTP Control Protocol Extended Reports (RTCP XR)"	F	F
[IETF RFC 3711]	"The Secure Real-time Transport Protocol (SRTP)"	F	F
[IETF RFC 3984]	"RTP Payload Format for H.264 Video"	F	F
[IETF RFC 4103]	"RTP Payload for Text Conversation"	F	F
[IETF RFC 4348]	"Real-Time Transport Protocol (RTP) Payload Format for the Variable-Rate	F	F

Tableau 10 – Spécifications applicables au niveau transport à prendre en charge

Spécification	Titre	Fonction EUF	Fonction SCF
	Multimode Wideband (VMR-WB) Audio Codec"		
[IETF RFC 4629]	"RTP Payload Format for UIT-T Rec. H.263 Video"	F	F
[IETF RFC 4733]	"RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals"	O (Note 2)	O (Note 2)
[IETF RFC 4749]	"RTP Payload Format for the G.729.1 Audio Codec"	F	F
[UIT-T T.38]	" Procédures de communication de télécopie du Groupe 3 en temps réel sur les réseaux à protocole Internet"	F	F
<p>NOTE 1 – Pour emploi avec des codecs tels que ceux des références [UIT-T G.711] et [UIT-T G.726], qui ne prennent pas eux-mêmes intrinsèquement en charge le bruit de confort.</p> <p>NOTE 2 – Lorsque la référence [UIT-T G.711] est employée, la référence [IETF RFC 4733] n'est pas obligatoire.</p>			

Dans la liste suivante sont indiqués des exemples types de protocoles qui décrivent les couches inférieures à celles qui sont décrites dans les protocoles du Tableau 10. D'autres protocoles peuvent être pris en charge pour les couches inférieures.

- [b-IETF RFC 768] (08/1980): User Datagram Protocol.
- [b-IETF RFC 791] (09/1981): Internet Protocol.
- [b-IETF RFC 792] (09/1981): Internet Control Message Protocol.
- [b-IETF RFC 793] (09/1981): Transmission Control Protocol.
- [b-IETF RFC 826] (11/1982): An Ethernet Address Resolution Protocol – or Converting Network Protocol Addresses to 48.bit Ethernet Address for Transmission on Ethernet Hardware.
- [b-IETF RFC 2460] (12/1998): Internet Protocol, Version 6 (IPv6) Specification.
- [b-IETF RFC 2461] (12/1998): Neighbor Discovery for IP Version 6 (IPv6).
- [b-IETF RFC 2463] (12/1998): Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification.
- [b-IEEE 802.3] (12/2005): Information technology – Telecommunications and information exchange between systems – Local and metropolitan area networks – Specific requirements – Part 3: Carrier sense multiple access with collision detection (CSMA/CD) access method and physical layer specifications.
- [b-ISO/CEI 8877] (12/1992): Technologies de l'information. Télécommunications et échange d'informations entre systèmes. Connecteur d'interface et affectation des contacts pour l'interface d'accès de base au RNIS situé aux points de référence S et T.

11.2 Traitement multifréquence bitonalité

Les fonctions EUF et SCF qui assurent le rôle d'agent d'utilisateur doivent prendre en charge une partie déterminée de la référence [IETF RFC 4733] afin d'acheminer les événements DTMF. Lorsque la référence [UIT-T G.711] est employée, cette référence [IETF RFC 4733] peut ne pas être obligatoire.

Il existe des prescriptions propres aux équipements qui fonctionnent selon un protocole RTP audio d'un côté et selon un protocole non-RTP audio de l'autre. Ces équipements doivent être en mesure de détecter les données utiles conformes à la référence [IETF RFC 4733] provenant du côté RTP et de produire des tonalités audio DTMF du côté non-RTP.

Réciproquement, ils doivent détecter les tonalités audio DTMF provenant du côté non-RTP et produire des données utiles conformes à la référence [IETF RFC 4733] du côté RTP tout en supprimant les tonalités DTMF des tonalités audio dans la bande.

12 Transport de signalisation de commande d'appel

L'interface UNI doit utiliser, en tant que transport par défaut, le transport SIP fondé sur le protocole UDP. Le transport SIP fondé sur les protocoles TCP ou SCTP peut être utilisé, par exemple pour de longs messages. Le transport SIP TLS peut être employé pour des motifs de sécurité.

13 Version du protocole IP

Le réseau doit prendre en charge la version IPv4. Il peut en outre prendre en charge la version IPv6.

La fonction EUF doit prendre en charge la version IPv4 et peut, en outre, prendre en charge la version IPv6. Toutefois, si elle n'est pas supposée se connecter à un réseau qui prend uniquement la version IPv4 en charge, elle peut ne prendre en charge que la version IPv6.

14 Considérations d'ordre sécuritaire

La signalisation doit être sécurisée et le média peut être sécurisé.

Appendice I

Exemples de flux d'appel

(Cet appendice ne fait pas partie intégrante de la présente Recommandation)

Les flux d'informations décrits dans le présent appendice sont des exemples d'établissement et de libération, par le biais de l'interface UNI, d'une session média entre un agent d'utilisateur côté origine et un agent d'utilisateur côté terminaison. Les scénarios dans le présent appendice sont fondés sur des cas où les agents d'utilisateur, reliés par des exploitants différents, s'échangent des messages SIP afin d'établir des sessions médias.

Le présent appendice comporte, à titre d'exemple, des scénarios, dans le cadre des services conversationnels de base, de réussite ou d'échec d'établissement et de libération d'appel entre deux agents d'utilisateur. Il convient de noter que ces scénarios ne décrivent pas les procédures d'appel entre les réseaux des exploitants, qui sont exécutées au niveau de l'interface réseau-réseau (NNI).

I.1 Scénario de réussite de l'établissement de session SIP

Le présent paragraphe décrit les flux d'informations dans le cas d'un scénario de réussite d'un service de base entre un agent d'utilisateur 1 (UA1) et un agent d'utilisateur 2 (UA2), ces deux agents étant reliés à des réseaux d'exploitants différents. La Figure I.1 contient un exemple de scénario d'un service en trois parties: l'établissement initial de l'appel, l'établissement du rappel au moyen de l'INVITE réitérée et la libération de l'appel.

Comme indiqué dans la partie 1 de la Figure I.1, l'UA1 envoie à l'UA2 un message INVITE contenant dans le protocole SDP la description des paramètres de session. Selon le type de média (à savoir, audio, vidéo, etc.) à employer au cours de la session, des paramètres et des valeurs de média particuliers doivent être négociés entre les agents d'utilisateur. A l'issue de l'échange des messages ACK, la communication sera établie entre l'UA1 et l'UA2.

La partie 2 de la Figure I.1 décrit les flux d'informations pour l'établissement du rappel au moyen de l'INVITE réitérée après l'établissement d'une session média entre les deux agents d'utilisateur. Dans cet exemple, l'agent d'utilisateur côté terminaison (à savoir, l'UA2) envoie à l'agent d'utilisateur côté origine (à savoir, l'UA1) un message INVITE contenant dans le protocole SDP une nouvelle description de session afin de ré-établir une session média. Une telle procédure permet d'ajouter de nouveaux types de média ou de supprimer certains types de média d'une session établie précédemment, telle que celle dont il est question dans la partie 1.

Finalement, l'UA1 envoie un message BYE à l'UA2 pour libérer la session dès la fin de la conversation, comme indiqué dans la partie 3 de la Figure I.1. Dans cet exemple, lorsque l'UA2 envoie un message de réponse 200 à l'UA1, la session sera close.

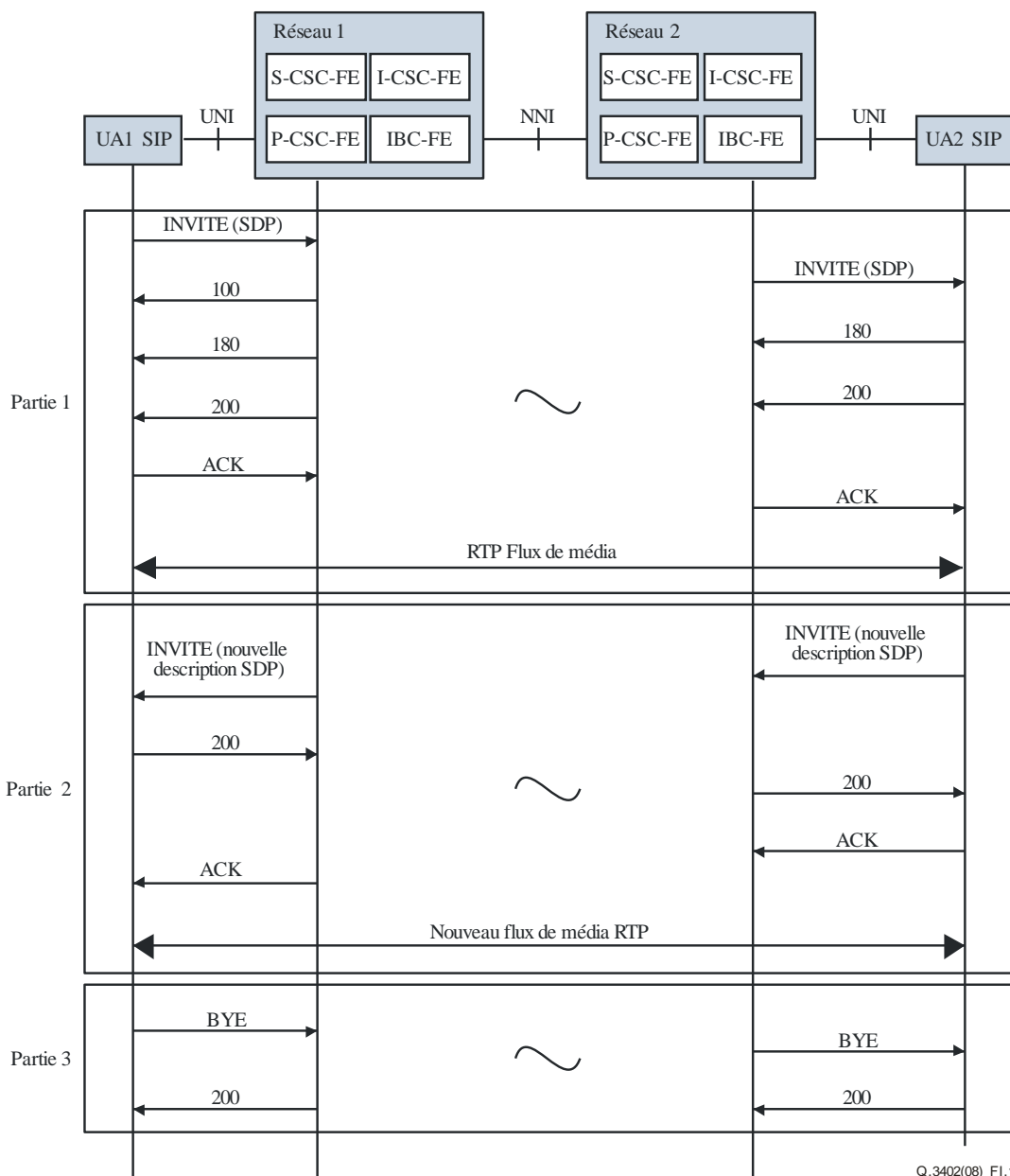


Figure I.1 – Scénario de réussite de l'établissement de session SIP

I.2 Scénario d'échec de l'établissement de session SIP

Le présent paragraphe décrit les flux d'informations dans le cas d'un scénario d'échec d'un service de base entre un agent d'utilisateur 1 (UA1) et un agent d'utilisateur 2 (UA2), ces deux agents étant reliés à des réseaux d'exploitants différents.

La Figure I.2 contient quelques exemples particuliers d'échec d'un service: l'échec dû à l'occupation et l'échec dû à la non-réponse.

Comme indiqué dans la partie 1 de la Figure I.2, l'agent d'utilisateur côté terminaison (à savoir, l'UA2) est occupé lorsqu'il reçoit un message INVITE provenant de l'agent d'utilisateur côté origine (à savoir, l'UA1). En conséquence, il renvoie un message de réponse 486 à l'UA1 et aucune session média n'est donc établie entre eux.

La partie 2 de la Figure I.2 décrit les flux d'informations dans le cas de l'échec de l'établissement d'un appel parce que l'UA2 ne répond pas à la réception d'un message INVITE provenant de l'UA1. Il convient de noter que le message INVITE initial sera réémis six fois supplémentaires à destination de l'UA2. Après quoi, l'UA1 reçoit un message de réponse 408 en provenance du réseau.

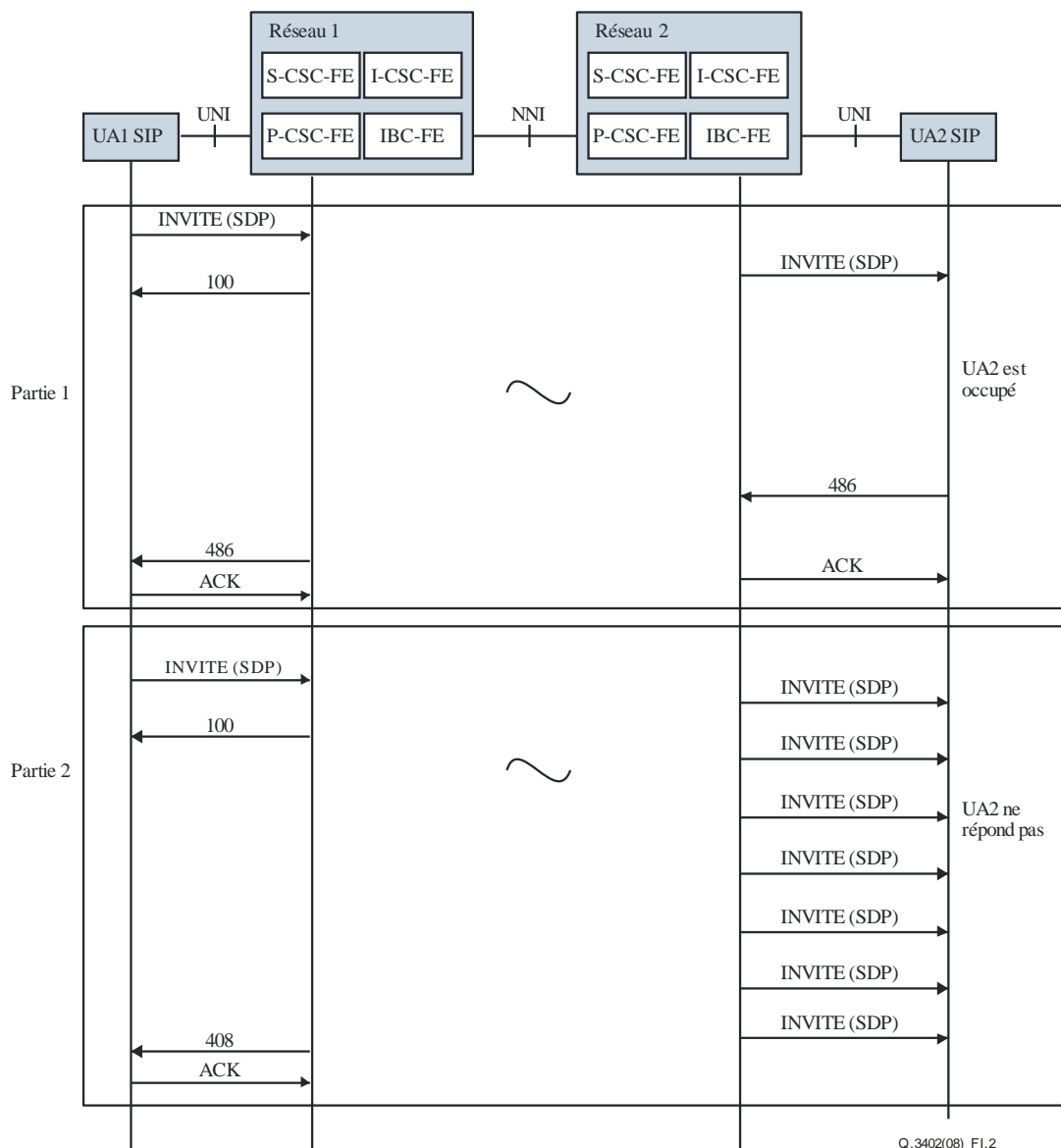


Figure I.2 – Scénario d'échec de l'établissement de session SIP

I.3 Echec par non-réponse à l'annulation d'un appel

La Figure I.3 contient un exemple d'échec d'un service entre un UA1 et un UA2 SIP, ces deux agents étant reliés à des réseaux d'exploitants différents. L'UA1 envoie un message INVITE pour établir un appel avec l'UA2. Mais il abandonne l'appel après avoir reçu une réponse 180 en provenance de l'UA2. Pour annuler l'appel, l'UA1 envoie un message CANCEL, auquel l'UA2 ne répond pas. Ce cas peut se produire lorsque l'UA2 a brusquement subi une coupure d'alimentation ou a été déconnecté du réseau.

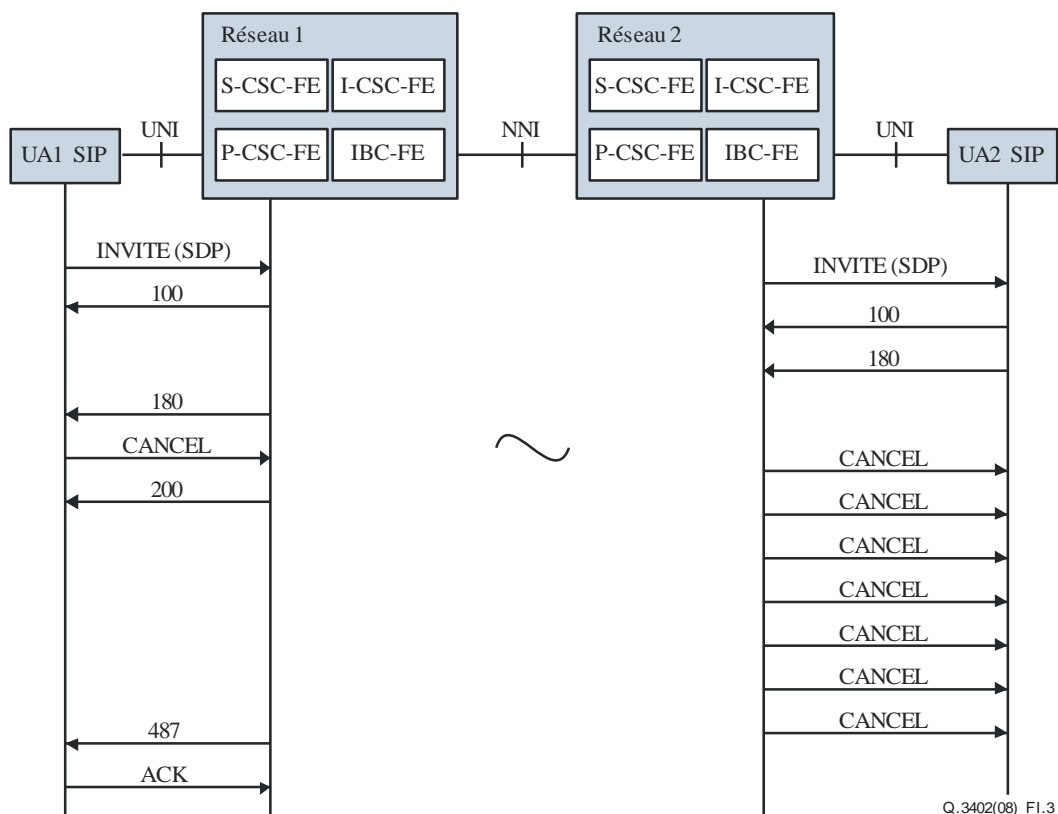


Figure I.3 – Echec par non-réponse à l'annulation d'un appel

I.4 Echec de l'établissement d'un appel

La Figure I.4 contient un exemple d'échec d'un service entre un UA1 et un UA2 SIP, ces deux agents étant reliés à des réseaux d'exploitants différents. L'UA1 envoie un message INVITE pour établir un appel avec l'UA2. L'entité appelée a pu être contactée, mais l'UA2 a rejeté l'appel en envoyant un message de réponse 4xx (Client-Error). Ce cas peut se produire lorsque l'UA2 a identifié l'entité appelante et a décidé de ne pas participer.

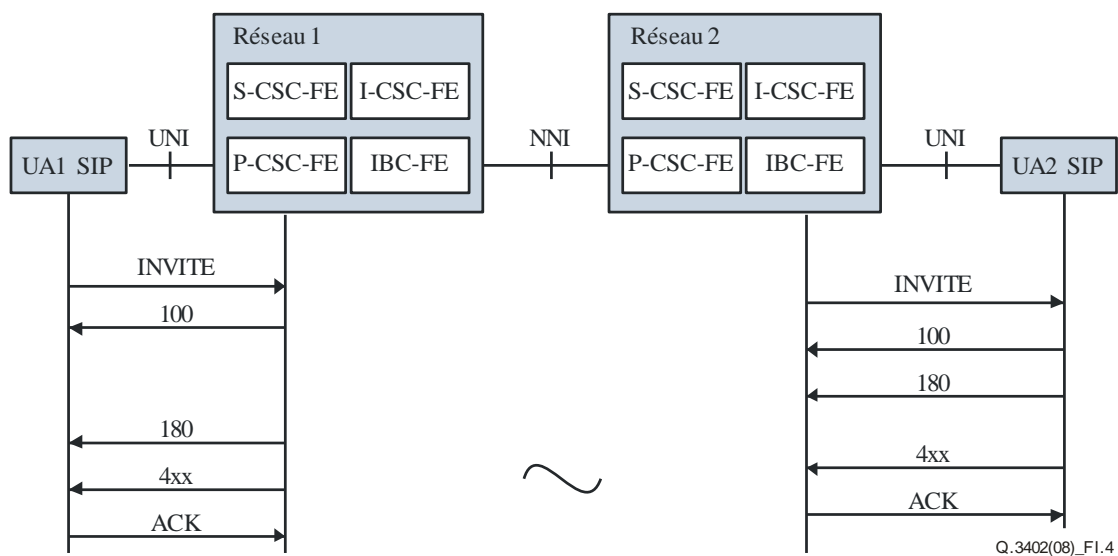


Figure I.4 – Echec de l'établissement d'un appel

Bibliographie

- [b-UIT-T E.164] Recommandation UIT-T E.164 (2005), *Plan de numérotage des télécommunications publiques internationales*.
- [b-3GPP TS 24.229] 3GPP TS 24.229 (2007), *3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; IP multimedia call control protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP); Stage 3*.
- [b-ETSI ES 282 007] ETSI ES 282 007 (2006), *Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); IP Multimedia Subsystem (IMS); Functional architecture*.
- [b-ETSI ES 283 003] ETSI ES 283 003 (2007), *Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); IP Multimedia Call Control Protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP) Stage 3 [3GPP TS 24.229 (Release 7), modified]*.
- [b-ETSI TS 182 006] ETSI TS 182 006 (2006), *Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); IP Multimedia Subsystem (IMS); Stage 2 description (3GPP TS 23.228 v7.2.0, modified)*.
- [b-IEEE 802.3] IEEE 802.3-2005, *Information technology – Telecommunications and information exchange between systems – Local and metropolitan area networks – Specific requirements – Part 3: Carrier sense multiple access with collision detection (CSMA/CD) access method and physical layer specifications*.
- [b-IETF RFC 768] IETF RFC 768 (1980), *User Datagram Protocol*.
- [b-IETF RFC 791] IETF RFC 791 (1981), *Internet Protocol*.
- [b-IETF RFC 792] IETF RFC 792 (1981), *Internet Control Message Protocol*.
- [b-IETF RFC 793] IETF RFC 793 (1981), *Transmission Control Protocol*.
- [b-IETF RFC 826] IETF RFC 826 (1982), *An Ethernet Address Resolution Protocol – or Converting Network Protocol Addresses to 48.bit Ethernet Address for Transmission on Ethernet Hardware*.
- [b-IETF RFC 2429] IETF RFC 2429 (1998), *RTP Payload Format for the 1998 version of UIT-T Rec. H.263 Video (H.263+)*.
- [b-IETF RFC 2460] IETF RFC 2460 (1998), *Internet Protocol, Version 6 (IPv6) Specification*.
- [b-IETF RFC 2461] IETF RFC 2461 (1998), *Neighbor discovery for IP version 6 (IPv6)*.
- [b-IETF RFC 2463] IETF RFC 2463 (1998), *Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification*.
- [b-ISO/CEI 8877] ISO/CEI 8877:1992, *Technologies de l'information. Télécommunications et échange d'informations entre systèmes. Connecteur d'interface et affectation des contacts pour l'interface d'accès de base au RNIS situé aux points de référence S et T*.

SÉRIES DES RECOMMANDATIONS UIT-T

Série A	Organisation du travail de l'UIT-T
Série D	Principes généraux de tarification
Série E	Exploitation générale du réseau, service téléphonique, exploitation des services et facteurs humains
Série F	Services de télécommunication non téléphoniques
Série G	Systèmes et supports de transmission, systèmes et réseaux numériques
Série H	Systèmes audiovisuels et multimédias
Série I	Réseau numérique à intégration de services
Série J	Réseaux câblés et transmission des signaux radiophoniques, télévisuels et autres signaux multimédias
Série K	Protection contre les perturbations
Série L	Construction, installation et protection des câbles et autres éléments des installations extérieures
Série M	Gestion des télécommunications y compris le RGT et maintenance des réseaux
Série N	Maintenance: circuits internationaux de transmission radiophonique et télévisuelle
Série O	Spécifications des appareils de mesure
Série P	Terminaux et méthodes d'évaluation subjectives et objectives
Série Q	Commutation et signalisation
Série R	Transmission télégraphique
Série S	Equipements terminaux de télégraphie
Série T	Terminaux des services télématiques
Série U	Commutation télégraphique
Série V	Communications de données sur le réseau téléphonique
Série X	Réseaux de données, communication entre systèmes ouverts et sécurité
Série Y	Infrastructure mondiale de l'information, protocole Internet et réseaux de prochaine génération
Série Z	Langages et aspects généraux logiciels des systèmes de télécommunication