INTERFAZ de TELEFÓNICA DE ESPAÑA, S.A.U.

ITE-BA-009

Versión 1ª

Noviembre-2005

Características Técnicas de las Interfaces de TELEFONICA DE ESPAÑA, S.A.U.

Interfaz para la conexión de terminales a los servicios de voz sobre IP

Interfaz para la conexión de terminales a los servicios de voz sobre IP

ÍNDICE

PREAMBULO

La presente información se facilita en cumplimiento de lo dispuesto en los artículos 7 a 9 del Reglamento que establece el procedimiento para la evaluación de la conformidad de los aparatos de telecomunicaciones, aprobado por el Real Decreto 1890/2000, de 20 de noviembre, y con la finalidad y alcance establecidos en dicho Reglamento. Este Real Decreto corresponde a la trasposición al ordenamiento jurídico español de la Directiva 1999/5/CE y por tanto la documentación técnica aquí facilitada cubre asimismo lo dispuesto en el artículo 4.2 de dicha Directiva.

La información publicada por Telefónica de España, S.A.U. es copia del documento notificado por esta misma a la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información del Ministerio de Industria, Turismo y Comercio. Cualquier desviación involuntaria entre la información publicada y la notificada será corregida tan pronto como sea detectada.

Telefónica de España, S.A.U. no se hace responsable de las manipulaciones realizadas por terceros, cualquiera que sea el medio utilizado.

Telefónica de España, S.A.U. se reserva el derecho de actualización de los requisitos y de su alineación con la normativa nacional o internacional de acuerdo con los procedimientos establecidos para ello.

1. OBJETO Y CAMPO DE APLICACIÓN

El presente documento describe las características que la red presenta a los terminales para el acceso a los servicios de voz sobre IP soportados sobre la arquitectura de nueva generación NGN de Telefónica de España S.A.U.

2. REFERENCIAS

IETF

[1] *RFC 768 User Datagram Protocol, 1980*

[2] *RFC 793 Transmision Control protocol, 1981*

[3] *RFC 1123 Requrements for Internet Hosts, 1989*

[4] *RFC 1305: Network Time Protocol (version 3): Specification, Implementation and Analysis, 1992*

[5] *RFC 2045: Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet Message Bodies, 1996*

[6] *RFC 2246 The TLS Protocol Version 1.0, 1999*

[7] *RFC 2327: SDP: Session Description Protocol, April, 1998*

[8] *RFC 2030: Simple Network Time Protocol (SNTP) Version4 for IPv4 and IPv6 and OSI,. Octubre 1996*

[9] *RFC 2543: SIP: Session Initiation Protocol, March 1999*

[10] *RFC 2616: Hypertext Transfer Protocol-HTTP/1.1, 1999*

[11] *RFC 2617: HTTP Authentication: Basic and Digest Access Authentication, Junio 1999*

[12] *RFC 2833: RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals, Mayo 2000*

[13] *RFC 2976: The SIP INFO Method, October 2000*

[14] *RFC 3261: SIP: Session Initiation Protocol, June 2002*

[15] *RFC 3262: Reliability of Provisional Responses in SIP, June 2002*

[16] *RFC 3263: Session Initiation Protocol (SIP): Locating SIP Servers, Junio 2002*

[17] *RFC 3264: An Offer/Answer Model with the Session Description Protocol, June 2002*

[18] *RFC 3265: Session Initiation Protocol (SIP)-Specific Event Notification, June 2002*

[19] *RFC 3311: The Session Initiation Protocol (SIP) UPDATE Method, September 2002*

[20] *RFC 3323: A Privacy Mechanism for the Session Initiation Protocol (SIP), November 2002*

[21] *RFC 3325: Private Extensions to the Session Initiation Protocol (SIP) for Asserted Identity within Trusted Networks, November 2002*

[22] *RFC 3326: The Reason Header Field for the Session Initiaition Protocol (SIP), Dicembre 2002*

[23] *RFC 3327: Session Initiation Protocol (SIP) Extension Header Field for Registering Non-Adjacent Contacts, Dicembre 2002*

[24] *RFC 3420. Internet Media Type message/sipfrag, 2003*

[25] *RFC 3428: Session Initiation Protocol (SIP) Extension for Instant Messaging, December 2002*

[26] *RFC 3455: Private Header (P-Header) Extensions to the Session Initiation Protocol (SIP) for the 3rd-Generation Partnership Project (3GPP), Enero 2003*

[2] *RFC 3486: Compressing the Session Initiation Protocol (SIP), Febrero 2003*

[28] *RFC 3515: The Session Initiation Protocol (SIP) Refer Method, April, 2003*

[29] *RFC 3550: RTP: A Transport Protocol for Real-Time Applications, 2003*

[30] *RFC 3551: RTP Profile for Audio and Video Conferences with Minimal Control, 2003*

[31] *RFC 3581: An Extension to the Session Initiation Protocol (SIP) for Symetric Response Routing, Agosto 2003*

[32] *RFC 3608: Session Initiation Protocol (SIP) Extension Header Field for Service Route Discovery During Registration, Octubre 2003*

[33] *RFC 3840: Indicating User Agent Capabilities in the Session Initiation Protocol (SIP), Agosto 2004*

[34] *RFC 3841: Caller Preferences for the Session Initiation Protocol (SIP), Agosto 2004*

[35] *RFC 3842: A Message Waiting Indication Event Package for the Session Initiation Protocol (SIP), Agosto 2004*

[36] *RFC 3863: Presence Information Data Format, Agosto 2004*

[37] *RFC 3891: The Session Initiation Protocol (SIP) "Replaces" Header, Septiembre 2004*

[38] *RFC 3892: The Session Initiation Protocol (SIP) Referred-By Mechanism, Septiembre 2004*

[39] *RFC 3903: The Session Initiation Protocol (SIP) Extension for Event State Publication, Octubre 2004*

[40] *RFC 3911: The Session Initiation Protocol (SIP) "Join" Header, Octubre 2004*

[41] *RFC 3959: The Early Session Disposition Type for the Session Initiation Protocol (SIP), Diciembre 2004*

[42] *RFC 3966: The tel URI for Telephone Numbers, December, 2004*

[43] *RFC 4028: Session Timers in the Session Initiation Protocol (SIP), Septiembre 2004*

[44] *draft-levy-sip-diversion-08.txt Diversion Indication in SIP, Agosto 2004*

UIT-T

[45] Q.1912.5. Interfuncionamiento entre el protocolo de iniciación de sesión y el protocolo de control de llamada independiente del portador o el protocolo de parte de usuario RDSI (PU-RDSI),Marzo 2004.

3. PILA DE PROTOCOLOS INTERNET MULTIMEDIA

En la figura 3.1 se representa la pila de protocolos Internet Multimedia constituida por cuatro niveles: nivel físico, nivel Internet, nivel de transporte y nivel de aplicación.

En los puntos que siguen a continuación se hace una breve descripción de cada uno de ellos.

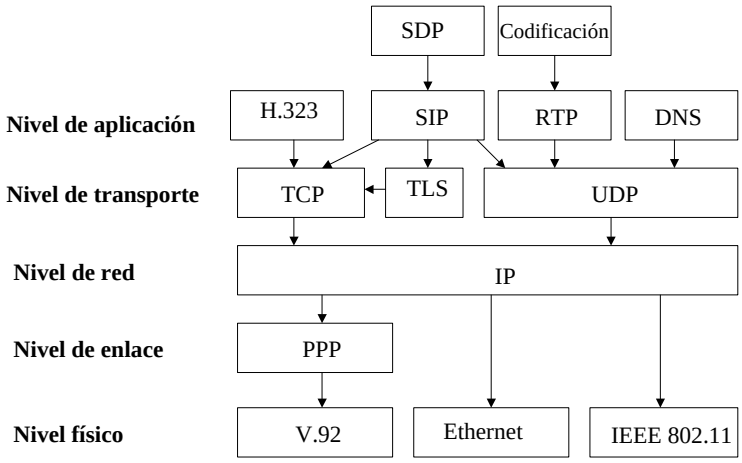


Figura 3.1 Pila de protocolos Internet multimedia

3.1 NIVEL FÍSICO

En este nivel estarían los protocolos empleados en la interfaz física, tales como Ethernet (IEEE 802.2, 802.3), interfaz inalámbrico (IEEE 802.11), línea digital ADSL.

3.2 NIVEL INTERNET

Este nivel lo constituye el protocolo IP (Internet Protocol) encargado de enrutar un paquete a través de la red a partir de la dirección IP de destino. Se trata de un protocolo no orientado a la conexión, en donde cada paquete se enruta de forma independiente a partir de la información contenida en la cabecera del mismo. En el protocolo IP los paquetes no son reconocidos, simplemente se aplica una detección de errores en la cabecera mediante la aplicación de códigos correctores de errores. Sin embargo no se detectan errores en la información transmitida dentro el paquete.

El protocolo ha ido evolucionanado a través de diferentes versiones que van mejorando aspectos como por ejemplo el aumento de la capacidad de direccionamiento IP (el espacio de direccionamiento en IPv4 era de 32 bits mientras que en IPv6 es de 128 bits).

3.3 NIVEL DE TRANSPORTE

Este nivel usa un número de puerto de dos octetos que identifican el protocolo de nivel de aplicación al que hay que entregar el paquete o segmento. Existen números dedicados a determinados protocolos. Éste es el caso, por ejemplo, del protocolo HTTP al que se le asigna el puerto 80 y el protocolo SIP al que se le asigna el 5060 ó 5061. Sin embargo existe también la posibilidad de asignar a un protocolo de forma dinámica un número de puerto dentro del rango habilitado para ello (49152 a 65535).

En el caso que nos ocupa del servicio de Voz sobre IP, se ha asignado el puerto 5070 al protocolo SIP que soporta este servicio en la interfaz terminal-red.

Básicamente hay tres protocolos de nivel de transporte: TCP (Transmisión Control Protocol), TLS (Transmission Layer Security) y UDP (User Datagram Protocol).

3.3.1 TCP

Proporciona un transporte fiable orientado a la conexión sobre IP. TCP usa números de secuencia y reconocimientos positivos para asegurar que cada bloque de datos, llamado segmento, ha sido recibido. Los segmentos perdidos se retransmiten hasta que se reciban correctamente. La figura 3.3.1.1 refleja el intercambio de mensajes para establecer y liberar una conexión TCP. Dicho protocolo viene descrito en la RFC 793 “Transmisión Control Protocol”.

Como se puede ver en dicha figura, la conexión TCP entre cliente y servidor se abre con el mensaje SYN, el cual contiene el número de secuencia inicial que el cliente TCP usará durante la conexión. El servidor TCP responde con un mensaje SYN que contiene su propio número de secuencia inicial y un número de reconocimiento que indica que ha sido recibido el SYN del cliente. El cliente TCP completa con un ACK o un paquete DATA con el flag AK puesto al número de secuencia del servidor. Ahora que la conexión está abierta tanto el cliente como el servidor pueden enviar paquetes DATA llamados segmentos.

Cada vez que un emisor envía un segmento abre un temporizador de forma que si se pierde éste en transmisión el temporizador expirará. En ese caso el emisor volverá a enviar el segmento hasta que reciba su reconocimiento. El mensaje FIN cierra la conexión TCP.

El protocolo TCP también incorpora mecanismos de control de flujo, limitando el número máximo de segmentos que pueden ser enviados pendientes de reconocimiento.

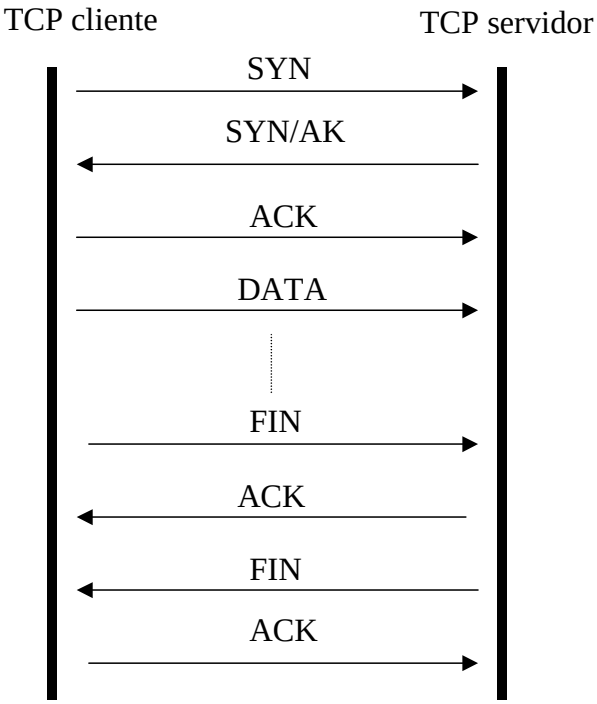


Fig.3.3.1.1 Apertura y cierre de una conexión TCP

3.3.2 UDP

Proporciona un transporte no fiable a través de Internet. No realiza el reconocimiento de los paquetes. Efectúa detección de errores mediante códigos correctores de error, siendo la responsabilidad de los protocolos de nivel superior el detectar la pérdida de los paquetes y el iniciar si se desea la retransmisión de los mismos.

Está definido en la RFC 768 “User Data Protocol”.

3.3.3 TLS

Se basa en el protocolo SSL (Secure Sockets Layer) y usa TCP para transporte. Está definido en la RFC 2246 “The TLS Protocol Versión 1.0”.

Tiene dos niveles: protocolo TLS de transporte y Protocolo TLS *handshake*. El primero se usa para proporcionar un mecanismo de transporte privado y fiable. Los datos enviados que usan TLS de transporte se encriptan. El segundo protocolo se usa para establecer la conexión, negociar las claves de cifrado a usar en el protocolo TLS de transporte y proporcionar autenticación.

3.4 NIVEL DE APLICACIÓN

3.4.1 Protocolo SIP (*Session Initiation Protocol*)

El protocolo SIP (Session Initiation Protocol) permite establecer sesiones multimedia entre puntos extremos, denominados Agentes de usuario. Las principales funciones de señalización del protocolo son las siguientes:

- Localización de un agente de usuario.
- Contacto con un agente de usuario para indicar la voluntad de establecer una sesión.
- Intercambio de información del medio sobre el que se va a establecer la sesión.
- Modificación del medio existente en las sesiones.
- Liberación de medios empleados en las sesiones.

Además, permite la petición y entrega de información de presencia , así como sesiones de mensajería instantánea.

Asimismo el protocolo SIP soporta mecanismos de fiabilidad que permiten el uso de protocolos de transporte no fiables tales como el protocolo UDP. Cuando SIP usa protocolos fiables como TCP o TLS estos mecanismos no se usan ya que son asumidos por los citados protocolos.

Por otro lado, un Agente de presencia en SIP es un dispositivo capaz de recibir peticiones de suscripción a la notificación de eventos y de generar las correspondientes notificaciones de estado de dichos eventos.

SIP no proporciona servicios, sino primitivas que pueden ser usadas para implementar diferentes servicios.

SIP trabaja tanto sobre protocolo IP v4 como la v6.

Un servidor SIP es un elemento de red que recibe y atiende peticiones SIP, devolviendo las correspondientes respuestas. Un servidor SIP puede ser por ejemplo un *Proxy* o un Agente de usuario.

El cliente SIP es aquel elemento de red que origina las peticiones y recibe las correspondientes respuestas. Un cliente SIP puede ser por ejemplo un Agente de usuario o un *Proxy*. Un servidor *Proxy* es una entidad intermedia que genera peticiones en nombre de otros clientes. Se encarga fundamentalmente del enrutamiento, es decir su trabajo es asegurar que el envío de las peticiones se acerca al usuario objetivo. Un servidor *Redirect* es un servidor agente de usuario que genera respuestas 3XY (ver punto 5.3) a las peticiones que recibe, dirigiendo al cliente a un contacto elegido entre un conjunto de direcciones URI alternativas.

El protocolo SIP es un protocolo basado en texto y está constituido por mensajes. Los mensajes pueden ser una petición (*Request*) de un cliente a un servidor o una respuesta (*Response*) de un servidor a un cliente. Ambos tipos de mensajes constan de una línea de texto inicial, uno o más campos cabecera, una línea vacía que indica el final de los campos cabecera y opcionalmente un cuerpo del mensaje.

En la línea inicial del mensaje SIP se distingue si se trata de una petición (*Request-Line*) o de una respuesta (*Status-Line*).

3.4.1.1 Peticiones (*Request*)

En la línea inicial de los mensajes de petición (*Request-Line*), se identifican: el método , el *Request-URI* y la versión SIP.

Los **Métodos** son considerados como los "verbos" del protocolo y se definieron inicialmente seis métodos en la RFC 3261: REGISTER para registrar la información de contacto, INVITE, ACK, CANCEL para el establecimiento de sesiones, BYE para la liberación de éstas y OPTIONS para interrogar al Agente de usuario o Servidor sobre sus capacidades, este último permite que puedan utilizarse métodos adicionales definidos como extensiones del protocolo SIP. Posteriormente se ha ampliado el número de éstos, definiéndose en RFCs separados: REFER, SUBSCRIBE, NOTIFY, MESSAGE, UPDATE, INFO, PRACK y PUBLISH.

La ***Request-URI*** es la dirección del usuario o servicio a la que se quiere dirigir la petición.

La **versión SIP** indica la versión del protocolo que se está usando.

A continuación se pone un ejemplo de un mensaje de petición (INVITE) en el que se marcan las partes básicas que integran éste:

```
INVITE sip:917240010@telefonica.net;user=phone SIP/2.0      (Request Line)
```

```
Via: SIP/2.0/UDP telefonica.net:500;branch=z9hG4bK1d32hr4
Max-Forwards:70
To: <sip:917240010@telefonica.net;user=phone>;tag=a53e42
From: "Pepe" <sip:917240000@telefonica.net>;tag=76341
Call-ID: 12-45-A5-46-F5@telefonica.net
CSeq: 1 INVITE
Subject: Horario de trenes
Contact: sip:<917240000@telefonica.net>
Content-Type: application/sdp
Content-Length: 151                                    (campos cabecera)
```

```
v=0
o=pepe 2890842326 2890844532 IN PI4 telefonica.net
s=Phone Call
c=IN PI4 136.2.7.3
m=audio 9999 RTP/AVP 0
a=rtpmap:0 PCMU/8000
t=0 0                                                  (cuerpo del mensaje)
```

3.4.1.2 Respuestas

En la línea inicial de los mensajes de respuesta (*Status-Line*), se identifican: versión SIP, código numérico de estado y su texto asociado.

El código numérico es un entero de 3 dígitos que identifica el significado de la respuesta. Las respuestas se clasifican en seis clases, identificadas cada una de ellas por el primer dígito de dicho código:

1XY: informativa.

2XY: aceptación.

3XY: redirección.

4XY: error de cliente.

5XY: error de servidor.

6XY: error global.

Las respuestas 1XY son respuestas denominadas provisionales, mientras que al resto de respuestas se las denomina respuestas finales.

A continuación se pone un ejemplo de un mensaje de respuesta (180 Ringing) en el que se marcan las partes básicas que integran ésta:

```
SIP/2.0 180 Ringing                                          (status-Line)
```

```
Via: SIP/2.0/UDP lab.high-voltage.org:5060;branch=z9hG4bKfw19b
;received=100.101.102.103
To: <917240010@telefonica.net;user=phone>;tag=a53e42
From: "Pepe" <sip:917240000@telefonica.net>;tag=76341
Call-ID: 12-45-A5-46-F5@telefonica.net
CSeq: 1 INVITE
Contact: <sip:917240000@telefonica.net >
Content-Length: 0                                          (campos cabecera)
```

3.4.1.3 Transacción, Diálogo y Sesión

El protocolo SIP es un protocolo transaccional. Una transacción SIP se produce entre un cliente y un servidor y comprende todos los mensajes desde la primera petición del cliente al servidor hasta que el cliente recibe una respuesta final del servidor.

Un diálogo SIP es una relación entre agentes de usuario que persiste durante un tiempo. El diálogo facilita el intercambio de mensajes y el adecuado enrutamiento de las peticiones entre dichos agentes. El diálogo representa el contexto en el cual son interpretados los mensajes SIP.

Un diálogo se identifica en cada agente de usuario por una identidad de diálogo constituida por los valores de las cabeceras *Call Id* (ver punto 6.1.7), parámetro *tag* de la cabecera *To* (ver punto 6.1.31) y parámetro *tag* de la cabecera *From* (ver punto 6.1.14). Los valores de la cabecera *Call Id* y del *tag* de la *From* se establecen en la petición que crea el diálogo y el valor *tag* del *To* se establece en la respuesta a dicha petición. La identidad de diálogo es diferente para cada agente de usuario involucrado en el mismo.

Un diálogo puede ser anticipado si se crea con una respuesta provisional y confirmado si se crea con una respuesta final 2XY. Cualquier diálogo anticipado termina si se recibe una respuesta diferente de 2XY o si no se recibe respuesta final.

Una sesión en SIP está constituida por un conjunto de emisores y receptores multimedia y los correspondientes flujos de tráfico entre éstos. Una sesión queda establecida en SIP al completarse el intercambio oferta y respuesta contenidas en los cuerpos SDP de los mensajes SIP que constituyen un diálogo. Si el diálogo es anticipado se trataría de una sesión anticipada y si el diálogo es confirmado sería un asesión confirmada. Las caracterísicas de una sesión se pueden modificar en el transcurso de la misma.

3.4.2 Protocolo SDP (*Session Description Protocol*)

El protocolo SDP (*Session Description Protocol*) está definido en la RFC 2327 “SDP:Session Description Protocol”. Se trata de un lenguaje para la descripción del medio de comunicación, es decir, es mas la definición de una sintaxis que un protocolo.

El SDP contiene la siguiente información sobre el medio empleado en la sesión:

- Dirección IP
- Número de puerto (usado por el protocolo de transporte UDP o TCP).
- Tipo de medio (audio, video, etc.)
- Esquema de codificación del medio (PCM ley A, MPEG II video, etc.).

Adicionalmente el SDP incluye también:

- Sujeto de la sesión.
- Hora de inicio y fin.
- Información de contacto relacionada con la sesión.

Igual que SIP, SDP utiliza codificación basada en texto. Un mensaje SDP está compuesto de un conjunto de líneas llamadas campos, cuyos nombres están abreviados a una sóla letra y se colocan siguiendo un orden establecido para facilitar su análisis. El SDP no es fácilmente extensible. La única manera de añadir nuevas capacidades a SDP es definiendo nuevos atributos. Los atributos son valores asignados al campo atributo (campo a) que es un campo opcional que se utiliza para proporcionar mayor información relacionado con el medio.

El protocolo SIP usa los campos de conexión, medio y atributos (ver la definición de estos campos en la RFC 2327) para establecer sesiones entre agentes de usuario. Dado que el tipo de medio y codec que se usa en una determinada sesión son parte de la negociación de la conexión, SIP podrá usar SDP para especificar múltiples alternativas de tipos de medio y aceptar o rechazar algunos de ellos.

3.4.3 Protocolo RTP (*Real-Time Transport Potocol*)

El protocolo RTP (*Real-Time Transport Protocol*) permite el transporte de paquetes de información en tiempo real, tales como voz y video, sobre una red IP. RTP está definido en la RFC 3550.

RTP no proporciona calidad de servicio sobre la red, es decir los paquetes son tratados de la misma manera que el resto de paquetes que se transmiten por la red IP. Sin embargo, RTP detecta las siguientes situaciones:

- Pérdida de paquetes.
- Retardo variable en el transporte (“jitter”).
- Llegada de paquetes fuera de secuencia.
- Enrutamiento asimétrico.

RTP soporta cifrado del medio.

Conforme a la pila de protocolos de la Figura 3.1, RTP es un protocolo del nivel de aplicación que usa UDP para transporte sobre IP. Usa una cabecera orientada a bit (compuesta por 12 octetos) igual que UDP e IP.

La pérdida de paquetes se determina analizando el campo Número de secuencia de la cabecera y observando que se ha producido un salto en la secuencia. No obstante, la solución del problema se delega a los codec.

El retardo variable o "jitter" se puede corregir analizando el campo *"Timestamp*" de la cabecera.

En la RFC 3550 también se define el protocolo RTCP (*RTP Control Protocol*) que permite a los participantes en una sesión RTP intercambiar informes, estadísticas e información relacionadas con las identidad de los participantes. Por ejemplo: número de paquetes enviados y recibidos, número de paquetes perdidos, "jitter" de los paquetes e informaciones relativas a la identidad de los participantes , tales como dirección de correo electrónico, número de teléfono, etc.

En una sesión multimedia establecida con SIP la información necesaria para la selección de los codecs y el envío de los paquetes RTP a la localización correcta se transporta en el cuerpo del mensaje SDP. En algunos escenarios, es deseable cambiar los codecs durante una sesión RTP. En general este cambio de codecs en medio de la sesión requiere intercambio de señalización SIP entre los Agentes de usuario (mensaje re-INVITE) ya que la sesión puede fallar si uno de los dos lados no soporta el nuevo codec. El mensaje re-INVITE de SIP permite que falle el cambio del codec en medio de la sesión sin provocar fallo en la sesión establecida.

3.4.3.1 Perfiles Audio Video

El uso de perfiles permite a RTP ser un protocolo de un amplio número de medios de transporte.

La lista de perfiles audio video se relaciona en la RFC 3551. El perfil de los codecs propuestos en un mensaje INVITE SIP se incluye en el cuerpo SDP como valores del campo atributo **a=rtpmap** (lista de atributos del medio). El número de puerto RTP incluido en dicho atributo será siempre par.

Si un codec no es aceptado por el destino, éste se rechaza poniendo a 0 el puerto incluido en el campo de información del medio en la respuesta SDP

4. MÉTODOS DEL PROTOCOLO SIP

4.1 INVITE

El método INVITE se usa para establecer sesiones entre agentes de usuario. Es similar al *Setup* de RDSI y al IAM de la PUSI usados en telefonía.

La definición de este método y el comportamiento de los UA en relación con el mismo se realiza en la RFC 3261, siendo de obligado cumplimiento lo que en ella aparece.

Para mayor detalle sobre el establecimiento de sesión, del modelo de oferta-respuesta que se aplica y de la negociación de medios entre participantes, ver la RFC 3264 y el punto 8.

Se pueden cambiar las características de una sesión establecida o refrescarla (incluyendo o no cambios en los parámetros de temporización) mediante el envío de un nuevo INVITE, denominado re-INVITE.

El re-INVITE es como un INVITE inicial, al que se le aplica las mismas normas del modelo oferta-respuesta y el mismo tratamiento de este último, con las particularidades expresadas en la RFC 3261

4.2 REGISTER

Un agente de usuario utiliza el método REGISTER para notificar a la plataforma de red SIP su dirección IP de contacto actual y la dirección URI a la que van a llegar las peticiones que deben ser enrutadas a dicho contacto. Este método añade, borra y consulta las asociaciones que en el procedimiento de registro se establecen entre una dirección que identifica al usuario y una o varias direcciones de contacto, a partir de las cuales, los servidores *proxy* o *redirect*, son capaces de encaminar las peticiones SIP a dicho usuario (más detalles sobre el procedimiento de registro en el punto 8.4).

La definición de este método y el comportamiento de los UA en relación con el mismo se realiza en la RFC 3261, siendo de obligado cumplimiento lo que en ella aparece.

4.3 BYE

El método BYE se usa para terminar una sesión establecida o un intento de sesión. Es similar al mensaje de Liberación empleado en telefonía.

La definición de este método y el comportamiento de los UA en relación con el mismo se realiza en la RFC 3261, siendo de obligado cumplimiento lo que en ella aparece

4.4 ACK

El método ACK se usa como reconocimiento a las respuestas finales (2XY, 3XY, 4XY, 5XY ó 6XY) a la petición INVITE.

La definición de este método y el comportamiento de los UA en relación con el mismo se realiza en la RFC 3261, siendo de obligado cumplimiento lo que en ella aparece

4.5 CANCEL

Se usa para cancelar una petición previamente enviada, para la que se ha recibido una respuesta provisional (1XY) pero no una respuesta final.

La definición de este método y el comportamiento de los UA en relación con el mismo se realiza en la RFC3261, siendo de obligado cumplimiento lo que en ella aparece.

4.6 OPTIONS

Permite a un agente de usuario interrogar a otro o a un servidor *proxy* sobre sus capacidades (métodos soportados, tipos de contenidos, extensiones, codecs, etc).

La definición de este método y el comportamiento de los UA en relación con el mismo se realiza en la RFC 3261, siendo de obligado cumplimiento lo que en ella aparece.

4.7 SUBSCRIBE

El método SUBSCRIBE es usado por un agente de usuario cliente (UAC) a fin de establecer una suscripción o solicitud para que el UAS envíe información sobre un evento en particular (contenida en el método NOTIFY descrito en el punto 4.8), en el contexto de un diálogo ya existente o que se establece mediante este procedimiento.

La definición de este método y el comportamiento de los UA en relación con el mismo se realiza en la RFC 3265, siendo de obligado cumplimiento lo que en ella aparece. La lista de los paquetes y plantillas de eventos a los que puede suscribirse un UA están registrados en IANA (Internet Assigned Numbers Authority).

4.8 NOTIFY

Este método lo utiliza un UA para informar de los cambios en el estado de un evento para el que existe alguna suscripción. Normalmente estas suscripciones se crean mediante el procedimiento de envío de un método SUBSCRIBE, sin embargo también puede estar implícita en otras peticiones SIP no SUBSCRIBE (por ejemplo el método REFER establece una suscripción implícita).

La definición de este método y el comportamiento de los UA en relación con el mismo se realiza en la RFC 3265, siendo de obligado cumplimiento lo que en ella aparece.

En el caso particular de suscripción realizada para obtener la indicación de mensajes pendientes en un buzón, el formato del cuerpo de mensaje de NOTIFY se define en la RFC 3842.

4.9 REFER

El método REFER lo usa un agente de usuario para solicitar a otro el acceso a un recurso URI o URL. Este método indica al receptor (identificado por el *Request-URI*) que debería contactar con una tercera parte, usando la información de contacto suministrada en la solicitud. Cada REFER enviado crea una suscripción separada.

La definición de este método y el comportamiento de los UA en relación con el mismo se realiza en la RFC 3515, siendo de obligado cumplimiento lo que en ella aparece.

4.10 MESSAGE

Se usa para transportar mensajes instantáneos (en tiempo real) mediante SIP, normalmente son mensajes cortos cuyo intercambio es lo bastante rápido como para que los participantes mantengan una conversación interactiva.

La definición de este método y el comportamiento de los UA en relación con el mismo se realiza en la RFC 3428, siendo de obligado cumplimiento lo que en ella aparece.

Conviene destacar que el método MESSAGE no es el único procedimiento para establecer sesiones de mensajería instantánea. Una sesión de este tipo se puede realizar de manera análoga a como se establecería una sesión multimedia en SIP; es decir, usando un INVITE con un cuerpo de mensaje SDP que describiera las características de la sesión entre los dos usuarios.

4.11 INFO

Lo usa un agente de usuario para enviar información de señalización de la llamada a otro usuario con el que se ha establecido una sesión. Es distinto del re-INVITE, puesto que no puede cambiar las características de la sesión SIP.

La definición de este método y el comportamiento de los UA en relación con el mismo se realiza en la RFC 2976, siendo de obligado cumplimiento lo que en ella aparece.

Aplicaciones potenciales del INFO pueden ser, por ejemplo, el envío de dígitos DTMF durante una sesión SIP, o el transporte de mensajes de señalización hacia la PSTN durante la llamada, a través de señalización usuario-usuario PUSI.

4.12 PRACK

Se utiliza para aceptar una respuesta provisional que se ha transmitido de manera fiable (excepto la 100 que nunca se transmite de este modo).

La definición de este método y el comportamiento de los UA en relación con el mismo se realiza en la RFC 3262, siendo de obligado cumplimiento lo que en ella aparece.

4.13 UPDATE

Sirve para cambiar las características de una sesión establecida o refrescarla (incluyendo o no cambios en los parámetros de temporización).

Al UPDATE se le aplican las mismas reglas de tratamiento y del modelo de oferta-respuesta de un re-INVITE recogidas en la RFC3261 con las particularidades expresadas en la RFC 3311.

4.14 PUBLISH

Es un método para la publicación de estado de eventos. Es similar al método REGISTER en el sentido de que permite crear, modificar y borrar el estado en otra entidad que gestiona dicho estado en nombre del usuario, denominado Compositor del estado de los eventos (ESC). Al agente de usuario de cliente que envía un PUBLISH se le denomina Agente de publicación de eventos (EPA).

La definición de este método y el comportamiento de los UA en relación con el mismo se realiza en la RFC 3903, siendo de obligado cumplimiento lo que en ella aparece.

5. RESPUESTAS SIP

La definición de las respuestas SIP y el comportamiento de los UA en relación con las mismas se realiza en la RFC 3261, siendo de obligado cumplimiento lo que en ella aparece.

A continuación se describen brevemente las diferentes respuestas, clasificadas según la citada RFC.

Asimismo figuran ciertas respuestas que no aparecen en la RFC 3261, indicándose para ellas la RFC en que se definen y sus características principales.

5.1 INFORMATIVAS

La clase de respuesta informativa tipo 1XY se emplea para indicar progreso de llamada, evitando las retransmisiones de las peticiones.

Cualquier respuesta informativa puede enviarse desde el UAS previamente a una respuesta de cualquiera del resto de las clases.

Las respuestas informativas son opcionales, es decir un UAS puede enviar una respuesta final sin tener que haber enviado previamente una respuesta provisional.

Mientras las respuestas finales a un INVITE tienen que recibir un ACK para confirmar su recepción, las respuestas provisionales no tienen que ser reconocidas, excepto cuando se usa el método PRACK de transmisión fiable para las respuestas provisionales.

En los puntos que siguen a continuación se detallan las diferentes respuestas informativas definidas en SIP.

5.1.1 100 *Trying*

Indica únicamente que algún tipo de acción no especificada se está llevando a cabo para procesar la llamada, sin indicar si el usuario ha sido localizado.

5.1.2 180 *Ringing*

Esta respuesta se usa para indicar que el INVITE ha sido recibido por el agente de usuario y que se le está dando señal de llamada. Es una respuesta importante en el interfuncionamiento con el protocolo PUSI o con el protocolo canal D, mapeándose en el primer caso en el mensaje de dirección completa (ACM) o en el mensaje de progreso para el segundo caso.

A partir de esta respuesta el UAC generará su propio tono de llamada salvo que se reciba el campo cabecera *Alert-Info* (ver 6.1.4).

5.1.3 181 C*all is being forwarded*

Esta respuesta se usa para indicar que la llamada está siendo desviada a otro terminal. Se envía cuando esta información puede ser utilizada por el llamante.

5.1.4 182 C*all queued*

Esta respuesta se utiliza para indicar que el INVITE se ha recibido y que se procesará en una cola.

5.1.5 183 *Session Progress*

La respuesta 183 *Session Progress* se utiliza para transportar información del progreso de la llamada que no está clasificada de otra manera. Dicha información puede estar presente en el texto asociado a la respuesta, en los campos cabecera, en el cuerpo del mensaje o en el flujo de información del medio.

Cuando un UAC reciba una respuesta 183, el terminal no generará tono local, tanto si lleva cuerpo SDP como si no.

5.2 ACEPTACIÓN

Esta clase de respuestas indica que la petición ha sido aceptada.

En los puntos que siguen a continuación se detallan las diferentes respuestas de aceptación definidas en SIP.

5.2.1 200 OK

Esta respuesta tiene dos usos en SIP. El primero para aceptar una invitación de sesión (INVITE), en cuyo caso contendrá un cuerpo de mensaje con las propiedades del medio del UAS (parte llamada). El segundo como respuesta a otras peticiones, indicando que la petición se ha recibido con éxito.

Esta respuesta detiene posteriores retransmisiones de la petición.

5.2.2 202 *Accepted*

Esta respuesta indica que el UAS ha recibido y comprendido la petición, pero que la petición puede no haber sido autorizada o procesada por el servidor. Se define en la RFC 3265, siendo de obligado cumplimiento lo que en ella aparece.

5.3 REDIRECCIÓN

La clase de respuesta de redirección es enviada por un servidor SIP que actúa como servidor *redirect*, dirigiendo al cliente a un contacto elegido entre un conjunto de direcciones URI alternativas. Asimismo, un UAS puede enviar una respuesta de esta clase en el caso de que estén implementados los servicios de desvío de llamada.

5.3.1 300 *Multiple Choices*

Esta respuesta de redirección contiene múltiples direcciones de contacto (campos *Contact*), las cuales indican que el servicio de localización ha devuelto diferentes localizaciones posibles para el Request-URI de la petición SIP.

5.3.2 301 *Moved Permanently*

Esta respuesta contiene un campo cabecera *Contact* que indica la nueva dirección URI de la parte llamada. El cliente que realiza la petición deberá actualizar su lista de direcciones con la nueva dirección para tenerla en cuenta en las siguientes peticiones.

5.3.3 302 *Moved Temporarily*

La dirección URI incluida en esta respuesta tiene una validez temporal, por el tiempo indicado en la cabecera *Expires* o en el parámetro *expires* del campo *Contact* y por tanto dicha dirección puede ser guardada en el proxy o UAS para posteriores transacciones durante el tiempo indicado en dicho parámetro o campo. En caso de que no se indique explícitamente la duración de la validez de la citada dirección, ésta sólo será válida por una vez y por tanto no debe ser guardada.

5.3.4 305 *Use Proxy*

Esta respuesta contiene la dirección URI que apunta a un servidor *proxy* que tiene información autorizada sobre la parte llamante. Es decir, al recurso requerido debe accederse a través del servidor *proxy*. La dirección del *proxy* vendrá en el campo *Contact* de la respuesta y será a la que el cliente dirigirá de nuevo la petición.

5.3.5 380 *Alternative service*

Se produce en situaciones en las que no se ha podido completar la llamada pero existen servicios alternativos, como por ejemplo el desvío a un buzón de voz. Esta respuesta devuelve una dirección URI en función del tipo de servicio activado por la parte llamada.

5.4 ERROR DEBIDO AL CLIENTE

Esta clase de respuesta es usada por un servidor o UAS para indicar que la petición no puede ser formulada tal y como se ha remitido. El tipo de respuesta o la presencia de determinados campos cabecera, indicarán al UAC la naturaleza del error y cómo debe ser formulada de nuevo la petición.

5.4.1 400 *Bad Request*

Esta respuesta indica que la petición no la ha entendido el servidor por error de sintaxis.

5.4.2 401 *Unauthorized*

Esta respuesta indica que la petición requiere llevar a cabo el procedimiento de autenticación.

5.4.3 402 *Payment Required*

Esta respuesta se mantiene para uso futuro.

5.4.4 403 *Forbidden*

Esta respuesta se utiliza para denegar una petición sin dar opción al llamante. En este caso el servidor ha entendido la petición y está correctamente formulada pero no atenderá la petición.

5.4.5 404 *Not Found*

Esta respuesta se proporciona cuando el servidor tiene seguridad de que el usuario identificado por la dirección URI no existe en el dominio especificado en el *Request–URI*. También se envía si el dominio no es ninguno de los dominios manejados por el receptor de la petición.

5.4.6 405 *Method Not Allowed*

En este caso el Método especificado en el *Request-Line* ha sido comprendido correctamente por el servidor o agente de usuario pero no está permitido su uso para la dirección identificada en el *Request-URI*.

5.4.7 406 *Not Acceptable*

El recurso identificado por la petición es únicamente capaz de responder con características de contenido no aceptables según el campo cabecera *Accept* incluido en la petición.

5.4.8 407 *Proxy Authentication Required*

Esta respuesta se envía desde un *proxy* para indicar al UAC que debe primero autenticarse antes de que la petición pueda ser procesada.

5.4.9 408 *Request Timeout*

Se enviará cuando el servidor de la petición no genere una respuesta a dicha petición en el tiempo adecuado.

5.4.10 410 *Gone*

Es similar a la respuesta 404 pero proporciona la pista de que el usuario requerido no estará disponible en su posición en el futuro. El servidor utilizará esta respuesta cuando tenga seguridad de que se trata de una condición permanente, en caso de que no exista tal seguridad deberá emplear la respuesta 404.

5.4.11 412 *Conditional Request Failed*

La utiliza el ESC (compositor del estado de eventos) si en una petición PUBLISH de refresco, modificación o borrado, el estado de evento al que se refiere ha expirado. Se define en la RFC 3903, siendo de obligado cumplimiento lo que en ella aparece.

5.4.12 413 *Request Entity Too Large*

Será utilizado por un servidor para rechazar una petición recibida con un cuerpo de mensaje más largo de lo que es capaz de procesar.

5.4.13 414 *Request-URI Too Long*

Esta respuesta indica que el Request URI de la petición es demasiado largo y no puede ser procesado correctamente.

5.4.14 415 *Unsupported Media Type*

Esta respuesta es enviada desde un Agente de usuario para indicar que el tipo de medio contenido en la petición no se soporta.

5.4.15 416 *Unsupported URI Scheme*

Se emplea cuando un UAC usa un esquema URI en un Request-URI que el UAS no entiende.

5.4.16 420 *Bad Extension*

Esta respuesta indica que la extensión especificada en el campo cabecera *Require* no se soporta en el agente de usuario o *proxy*, según se trate.

5.4.17 421 *Extension required*

Esta respuesta indica que un servidor necesita una extensión que no está presente en el campo cabecera *Supported* de una petición para el correcto procesamiento de la misma.

5.4.18 422 *Session Timer Interval Too Small*

Se usa para rechazar una petición que contiene un campo cabecera *Session-Expires* con un intervalo de tiempo demasiado corto. El intervalo de tiempo mínimo permitido es el indicado en el campo cabecera *Min-SE*.

Se define en la RFC 4028, siendo de obligado cumplimiento lo que en ella aparece.

5.4.19 423 *Interval Too Brief*

La usa un servidor de registro (registrar) para rechazar una petición debido a que el tiempo en el que expira uno o más contactos (*Contact*) es demasiado corto.

5.4.20 429 *Provide Referror Identity*

Se usa para pedir que un campo cabecera *Referred-By* sea reenviado con seguridad.

Se define en la RFC 3892, siendo de obligado cumplimiento lo que en ella aparece.

5.4.21 480 *Temporarily Unvailable*

Sirve para indicar que la petición ha alcanzado el destino correcto pero la parte llamada no está disponible por alguna razón (por ejemplo tiene activado el servicio “no molesten”). El texto asociado dará información más detallada de la causa por la que no está disponible.

5.4.22 481 *Dialog/Transaction Does Not Exist*

Indica que el UAS ha recibido una petición para la cual no encuentra un transacción o diálogo existente.

5.4.23 482 *Loop Detected*

Indica que la petición ha entrado en un bucle ya que ha sido devuelta a un *proxy* que previamente transfirió la petición.

5.4.24 483 *Too Many Hops*

Indica que la petición ha sido desviada un número de veces que supera el máximo permitido. El servidor que manda esta respuesta ha recibido en la petición el campo cabecera *Max-Forwards* puesto a 0.

5.4.25 484 *Address Incomplete*

Indica que el servidor ha recibido en el Request-URI de la petición una dirección incompleta. Esta respuesta permite el empleo de marcación solapada.

5.4.26 485 *Ambiguous*

Indica que el Request-URI de la petición es ambiguo y debe clarificarse para poder ser procesado.

5.4.27 486 *Busy Here*

Se usa para indicar que, aunque se ha alcanzado correctamente a la parte llamada, el agente de usuario no puede aceptar la llamada en la posición cuya dirección se identifica en el *Request-URI*.

5.4.28 487 *Request Terminated*

Se enviará como respuesta a un BYE o CANCEL.

5.4.29 488 *Not Acceptable Here*

Indica que el agente de usuario fue contactado correctamente pero que algunos aspectos de la descripción de la sesión, tales como el medio requerido, el ancho de banda o el esquema de direccionamiento no son aceptables.

5.4.30 489 *Bad Event*

Se usa para rechazar una petición de suscripción o de notificación que contiene un paquete de evento (cabecera *Event*) desconocido o no soportado por el UAS. También se usará para rechazar peticiones de suscripción que no especifican un paquete de evento en la cabecera *Event*.

Se define en la RFC 3265, siendo de obligado cumplimiento lo que en ella aparece.

5.4.31 491 *Request Pending*

Se usa para resolver posibles re-INVITEs simultáneos realizados por ambas partes del diálogo.

5.4.32 493 *Request Undecipherable*

Esta respuesta es usada por el UAS cuando no puede descifrar el cuerpo de mensaje S/MIME al no disponer éste de la clave pública.

5.5 ERROR DEBIDO A FALLO EN EL SERVIDOR

Esta clase de respuestas se usará para indicar que la petición no se puede procesar debido a un fallo en el propio servidor. La petición podrá ser reintentada para otras direcciones

5.5.1 500 *Server Internal Error*

Esta respuesta se envía cuando el servidor se ha encontrado con un fallo inesperado que no le permite procesar la petición. Se trata de fallos temporales, por tanto, el cliente puede hacer un nuevo intento transcurridos unos segundos.

5.5.2 501 N*ot implemented*

Indica que el servidor no es capaz de procesar la petición. Es una respuesta apropiada cuando el UAS no reconoce el Método requerido. La diferencia con la respuesta 405 es que en esta última el servidor sí reconoce el método pero no es soportado o no está permitido.

5.5.3 502 *Bad Gateway*

Esta respuesta se envía desde un *proxy* que está actuando como *gateway* de otra red e indica que existe algún problema en la otra red que impide procesar la petición.

5.5.4 503 *Service Unavailable*

Indica que el servicio requerido está temporalmente indisponible por congestión o actuaciones de mantenimiento del servidor.

5.5.5 504 *Server Timeout*

Esta respuesta indica que la petición ha fallado debido a un vencimiento de la temporización que se ha producido en el servidor o en la otra red con la que se interconecta el *gateway*.

5.5.6 505 *Version Not Supported*

Esta respuesta indica que el servidor ha rechazado la petición debido a la versión SIP empleada en la petición.

5.5.7 513 *Message Too large*

Esta respuesta es usada por el UAS para indicar que el tamaño de la petición es demasiado grande para ser procesado.

5.6 ERROR GLOBAL

Esta clase de respuesta indica que el servidor sabe que la petición fallará allá donde se intente. Como consecuencia, no debería reintentarse a otras direcciones.

5.6.1 600 *Busy Everywhere*

Esta respuesta es la versión definitiva de la respuesta 486, es decir, tiene le mismo significado pero referido no sólo a una dirección sino a cualquier posible dirección del usuario identificado en el *Request-URI*.

5.6.2 603 *Decline*

Es una respuesta similar a la 600 pero sin dar información del estado de la llamada, simplemente indica que no acepta la llamada, bien porque no quiere o porque no puede.

5.6.3 604 D*oes Not Exist Anywhere*

Esta respuesta es similar a la 404 pero el servidor tiene información autorizada para indicar que el usuario identificado no puede ser localizado en ninguna dirección.

5.6.4 606 *Not Acceptable*

Esta respuesta se podrá usar para implementar alguna capacidad de negociación de sesión en SIP. Sirve para indicar que algún aspecto de la sesión requerida no es aceptable por el UAS (medio requerido, ancho de banda, estructura de direccionamiento, etc.) y en consecuencia, no se puede establecer la citada sesión.

6. CAMPOS CABECERA SIP

En los siguientes apartados se indica la relación de campos cabecera que se consideran, clasificados en cuatro grupos según puedan aparecer en métodos y respuestas, sólo en respuestas, sólo en métodos o se relacionen con el cuerpo del mensaje. En cada uno aparece una descripción general de su utilización y la referencia en que se encuentra definido.

Las particularidades que Telefónica pueda presentar respecto a dicha definición figuran en el punto correspondiente a la descripción de procedimientos.

A continuación se ofrece la lista de todos ellos por orden alfabético y para cada uno su apartado correspondiente.

Accept	6.1.1	P-Charging-Vector	6.1.20
Accept-Contact	6.3.1	P-Preferred-Identity	6.1.21
Accept-Encoding	6.1.2	Priority	6.3.8
Accept-Language	6.1.3	Privacy	6.1.23
Alert-Info	6.1.4	Proxy-Authenticate	6.2.5
Allow	6.1.5	Proxy-Authentication-Info	6.2.6
Allow-Events	6.1.6	Proxy-Authorization	6.3.9
Authentication-Info	6.2.1	Proxy-Require	6.3.10
Authorization	6.3.2	Rack	6.3.11
Call-Id	6.1.7	Reason	6.1.24
Call-Info	6.1.8	Record-Route	6.1.25
Contact	6.1.9	Referred-By	6.3.13
Content-Disposition	6.4.1	Refer-To	6.3.12
Content-Encoding	6.4.2	Reject-Contact	6.3.14
Content-Language	6.4.3	Replaces	6.3.15
Content-Length	6.4.4	Reply-To	6.1.26
Content-Type	6.4.5	Request-Disposition	6.3.16
Cseq	6.1.10	Require	6.1.27
Date	6.1.11	Retry-After	6.2.7
Diversion	6.1.12	Route	6.3.17
Error-Info	6.2.2	Rseq	6.2.8
Event	6.3.3	Server	6.2.9
Expires	6.1.13	Service-Route	6.2.10
From	6.1.14	Session-Expires	6.1.28
In-Reply-To	6.3.4	SIP-Etag	6.2.11
Join	6.3.5	SIP-If-Match	6.3.18
Max-Forwards	6.3.6	Subject	6.3.19
Mime Version	6.4.6	Subscription-State	6.3.20
Min-Expires	6.2.3	Supported	6.1.29
Min-SE	6.1.15	Timestamp	6.1.30
Organization	6.1.16	To	6.1.31
P-Access-Network-Info	6.1.17	Unsupported	6.2.12
P-Asserted-Identity	6.1.18	User-Agent	6.1.32
P-Associated-URI	6.2.4	Via	6.1.33
Path	6.1.22	Warning	6.2.13
P-Called-Party-ID	6.3.7	WWW-Authenticate	6.2.14
P-Charging-Function-Addresses	6.1.19		

6.1 CONTENIDOS EN MÉTODOS Y RESPUESTAS

6.1.1 Accept

Esta cabecera se usa para indicar tipos de medios aceptables para los cuerpos de mensaje, por parte del cliente (si se envía en una petición) o del servidor (si se envía en una respuesta). Su definición y uso aparece en la RFC3261, siendo aplicable lo que en ella figura. Los distintos valores de tipo/subtipo de medios están registrados en IANA.

6.1.2 Accept-Encoding

Es similar a la cabecera Accept pero referida a los esquemas de codificación aceptables para el cuerpo de mensaje. Su definición y uso aparece en la RFC3261, siendo aplicable lo que en ella figura. Los distintos esquemas de codificación están registrados en IANA.

6.1.3 Accept-Language

Se usa en las peticiones para indicar los lenguajes preferidos para frases, descripción de sesiones o estado de respuestas, que se incluyan como cuerpo de mensaje en la respuesta. Su definición y uso aparece en la RFC3261, siendo aplicable lo que en ella figura.

6.1.4 Alert-Info

Esta cabecera se usa para proporcionar un servicio de “tono distintivo”. Su definición y uso aparece en la RFC3261, siendo aplicable lo que en ella figura.

6.1.5 Allow

Proporciona una lista con el conjunto de métodos soportados por el UA que genera el mensaje. Su definición y uso aparece en la RFC3261, siendo aplicable lo que en ella figura.

6.1.6 Allow-Events

Incluye la lista de los paquetes de eventos que soporta el UAC (si se envía en una petición) o el UAS (si aparece en una respuesta). Su definición y uso aparece en la RFC3265, siendo aplicable lo que en ella figura.

6.1.7 Call-Id

Actúa como identificador de una petición o de su pertenencia a un diálogo. La respuesta copia el valor de la petición. Su definición y uso aparece en la RFC3261, siendo aplicable lo que en ella figura.

6.1.8 Call-Info

Proporciona información adicional sobre llamante o llamado, dependiendo de si se encuentra en una petición o una respuesta. Su definición y uso aparece en la RFC3261, siendo aplicable lo que en ella figura.

6.1.9 Contact

Proporciona uno o varios URI para identificar y facilitar el acceso o contacto con el recurso origen o destino de la petición (dependiendo de si aparece en un método o en una respuesta). Su definición y uso aparece en la RFC3261, siendo aplicable lo que en ella figura.

Además puede incluir parámetros, definidos en la RFC 3840, que describen determinados rasgos o características (feature tags) que describen capacidades del dispositivo identificado por el URI-Contact.

6.1.10 Cseq

Sirve para ordenar las transacciones dentro de un diálogo, proporcionar un medio de identificarlas unívocamente y diferenciar entre métodos nuevos y retransmitidos. Su definición y uso aparece en la RFC3261, siendo aplicable lo que en ella figura.

6.1.11 Date

Indica la fecha y hora en que la petición o respuesta se envía por primera vez. Su definición y uso aparece en la RFC3261, siendo aplicable lo que en ella figura.

6.1.12 Diversion

Se usa en casos de desvíos de llamada para indicar al llamado quién o quienes han realizado desvíos y por qué motivo. Su definición y uso aparece en draft-levy-sip-diversion-08.txt, siendo aplicable lo que allí figura.

6.1.13 Expires

Proporciona el tiempo relativo tras el cual el mensaje o contenido expira. Su definición y uso aparece en la RFC3261, siendo aplicable lo que en ella figura.

6.1.14 From

Identifica al usuario que origina la petición. Su definición y uso aparece en la RFC3261, siendo aplicable lo que en ella figura.

6.1.15 Min-SE

Indica el valor mínimo, en segundos, que puede darse al intervalo de tiempo de expiración de la sesión. Su definición y uso aparece en la RFC4028, siendo aplicable lo que en ella figura.

6.1.16 Organization

Se usa para indicar la organización a la que pertenece el que origina el mensaje. Su definición y uso aparece en la RFC3261, siendo aplicable lo que en ella figura.

6.1.17 P-Access-Network-Info

Esta cabecera contiene información sobre la red de acceso que el UA está utilizando. Forma parte de las extensiones de SIP definidas en la RFC 3455 y denominadas cabeceras privadas, siendo aplicable lo que en ella figura.

6.1.18 P-Asserted-Identity

Transporta entre proxies de un dominio seguro la identidad de un usuario certificada mediante un proceso de autenticación. Forma parte de las extensiones de SIP definidas en la RFC 3325 y denominadas cabeceras privadas, siendo aplicable lo que en ella figura.

6.1.19 P-Charging-Function-Addresses

Esta cabecera contiene los nombres de los host o las direcciones IP de los nodos que reciben la información de facturación. Forma parte de las extensiones de SIP definidas en la RFC 3455 y denominadas cabeceras privadas, siendo aplicable lo que en ella figura.

6.1.20 P-Charging-Vector

Proporciona información para poder correlacionar los registros de tarificación generados por cada una de las entidades de red involucradas en una misma sesión. Forma parte de las extensiones de SIP definidas en la RFC 3455 y denominadas cabeceras privadas, siendo aplicable lo que en ella figura.

El Agente de usuario no requiere entender esta cabecera.

6.1.21 P-Preferred-Identity

La usa un UA para comunicar a un proxy seguro qué identidad prefiere que use en la cabecera P-Asserted-Identity cuando la inserte, del conjunto de identidades asociadas al UA. Forma parte de las extensiones de SIP definidas en la RFC 3325 y denominadas cabeceras privadas, siendo aplicable lo que en ella figura.

6.1.22 Path

Proporciona una relación de *proxies* que la petición REGISTER recorre entre el UAC (origen) y el registrar (destino). Su definición y uso aparece en la RFC3327, siendo aplicable lo que en ella figura.

6.1.23 Privacy

Esta cabecera se utiliza para ocultar información de usuario a efectos de mantener su privacidad, cuando esta actuación debe llevarla a cabo un elemento intermedio de la red (proxy), dado que, en general, se trata de información que el usuario no puede ocultar por sí mismo (por ejemplo por ser utilizada para encaminar las peticiones o respuestas). Su definición y uso aparece en la RFC3323, siendo aplicable lo que en ella figura. Además para el valor: “id”, aplica lo definido en la RFC3325.

6.1.24 Reason

Indica la razón por la que la sesión o llamada termina. Su definición y uso aparece en la RFC3326, siendo aplicable lo que en ella figura.

6.1.25 Record-Route

Se usa para forzar el enrutamiento a través de un proxy para todas las peticiones enviadas dentro del diálogo que se establezca entre dos agentes de usuario (en ambos sentidos). Su definición y uso aparece en la RFC3261, siendo aplicable lo que en ella figura.

6.1.26 Reply-To

Se usa para indicar el SIP o SIPS URI que debería usarse en contestaciones a esa petición (por ejemplo, casos de devolución de llamadas perdidas o sesiones no establecidas) y que puede ser distinto del contenido en la cabecera From. Su definición y uso aparece en la RFC3261, siendo aplicable lo que en ella figura.

6.1.27 Require

Se usa para enumerar las características y extensiones que un UAC necesita que soporte un UAS para procesar la petición. Su definición y uso aparece en la RFC3261, siendo aplicable lo que en ella figura.

6.1.28 Session-Expires

Se usa para indicar el tiempo de expiración de la sesión en segundos. Su definición y uso aparece en la RFC4028, siendo aplicable lo que en ella figura.

6.1.29 Supported

Enumera todas las extensiones soportadas por el UAC o UAS. Su definición y uso aparece en la RFC3261, siendo aplicable lo que en ella figura.

6.1.30 Timestamp

Indica el tiempo exacto en que el UAC envía la petición al UAS. Su definición y uso aparece en la RFC3261, siendo aplicable lo que en ella figura.

6.1.31 To

Indica el receptor "lógico" de la petición o la dirección pública del usuario o recurso destino de esa petición, que puede ser o no el último receptor de la misma. Su definición y uso aparece en la RFC3261, siendo aplicable lo que en ella figura.

6.1.32 User-Agent

Contiene información sobre el UA que origina la petición (información sobre el fabricante, versión software o comentarios). Su definición y uso aparece en la RFC3261, siendo aplicable lo que en ella figura.

6.1.33 Via

Indica el transporte usado para la transacción e identifica la localización donde la respuesta al método va a ser enviada. Su definición y uso aparece en la RFC3261, siendo aplicable lo que en ella figura. Además de los definidos en esta RFC, puede llevar los parámetros: "comp", tal como se define en la RFC3486 y "rport", tal como se define en la RFC3581.

6.2 CONTENIDOS SÓLO EN RESPUESTAS

6.2.1 Authentication-Info

Un servidor puede incluir esta cabecera en una respuesta 2XY generada para una petición que se ha autenticado satisfactoriamente. En ella figura información adicional útil para futuras autenticaciones. Su definición y uso aparece en la RFC3261, siendo aplicable lo que en ella figura.

6.2.2 Error-Info

Proporciona un puntero hacia una dirección URI que aporte información adicional sobre el estado de error de la respuesta. Su definición y uso aparece en la RFC3261, siendo aplicable lo que en ella figura.

6.2.3 Min-Expires

Comunica el mínimo intervalo de refresco en registros, suscripciones, publicaciones para elementos manejados por el servidor. Su definición y uso aparece en la RFC3261, siendo aplicable lo que en ella figura.

6.2.4 P-Associated-URI

Indica un conjunto de URI's relacionadas con una dirección registrada (address of record). Forma parte de las extensiones de SIP definidas en la RFC 3455 y denominadas cabeceras privadas, siendo aplicable lo que en ella figura.

6.2.5 Proxy-Authenticate

Esta cabecera incluye información para que el cliente pueda enviar de nuevo la petición con una acreditación correcta, en caso de que la autenticación la realice un proxy. Su definición y uso aparece en la RFC3261, siendo aplicable lo que en ella figura.

6.2.6 Proxy-Authentication-Info

Su sintaxis y significado son análogos a los indicados para la cabecera *Authentication-Info.* Su definición y uso aparece en la RFC2617, siendo aplicable lo que en ella figura.

6.2.7 Retry-After

Indica cuando un recurso o servicio puede estar disponible de nuevo. Su definición y uso aparece en la RFC3261, siendo aplicable lo que en ella figura.

6.2.8 Rseq

Se utiliza para indicar la secuencia de todas las respuestas provisionales fiables enviadas para una petición. Su definición y uso aparece en la RFC3262, siendo aplicable lo que en ella figura.

6.2.9 Server

Contiene información acerca del software usado por el UAS para manejar la petición. Su definición y uso aparece en la RFC3261, siendo aplicable lo que en ella figura.

6.2.10 Service-Route

La incluye un *registrar* en la respuesta 200 OK al método REGISTER indicando una secuencia de *proxies*. Dicha secuencia es la que seguirán las peticiones iniciales originadas

en el UAC cuya dirección está registrada. Para ello, el UAC construiría una cabecera Route (ver 6.3.17), en futuras peticiones, con el valor de la cabecera Service-Route recibida. Su definición y uso aparece en la RFC3608, siendo aplicable lo que en ella figura.

6.2.11 SIP-Etag

Esta cabecera es obligatoria en la respuesta 2xy enviada para la petición PUBLISH por el ESC (compositor del estado de los eventos). La genera este último y contiene un identificador asociado al evento publicado (*entity-tag*). Su definición y uso aparece en la RFC3903, siendo aplicable lo que en ella figura.

6.2.12 Unsupported

Lista las características no soportadas por el UAS. Su definición y uso aparece en la RFC3261, siendo aplicable lo que en ella figura.

6.2.13 Warning

Se usa para proporcionar información adicional sobre el estado de una respuesta. Su definición y uso aparece en la RFC3261, siendo aplicable lo que en ella figura.

6.2.14 WWW-Authenticate

Esta cabecera incluye información para que el cliente pueda enviar de nuevo la petición con una acreditación correcta, en caso de que la autenticación la realice un UA o un *registrar*. Su definición y uso aparece en la RFC3261, siendo aplicable lo que en ella figura.

6.3 CONTENIDOS SÓLO EN MÉTODOS

6.3.1 Accept-Contact

Forma parte de las extensiones de SIP, que permiten al usuario que envía la petición establecer preferencias que controlan de algún modo el proceso de la misma por parte de los proxy. En concreto, indica un conjunto de rasgos o características correspondiente al UAS que se quiere alcanzar. Su definición y uso aparece en la RFC3841 siendo aplicable lo que en ella figura.

6.3.2 Authorization

Esta cabecera contiene la acreditación del cliente (incluyendo usuario y password) a efectos de autenticación. Su definición y uso aparece en la RFC3261, siendo aplicable lo que en ella figura.

6.3.3 Event

Indica qué paquete de eventos está utilizando la petición. Su definición y uso aparece en la RFC3265, siendo aplicable lo que en ella figura.

6.3.4 In-Reply-To

Se utiliza en caso de devolución de llamadas perdidas o sesiones no establecidas, y enumera los Call-Id de las llamadas quie devuelve la petición en la que va la cabecera. Su definición y uso aparece en la RFC3261, siendo aplicable lo que en ella figura.

6.3.5 Join

Esta cabecera se usa en un INVITE que solicita la incorporación de un nuevo participante a un diálogo (sesión) existente. Su definición y uso aparece en la RFC3911, siendo aplicable lo que en ella figura.

6.3.6 Max-Forwards

Sirve para limitar el número de saltos de un método. Su definición y uso aparece en la RFC3261, siendo aplicable lo que en ella figura.

6.3.7 P-Called-Party-ID

Esta cabecera la inserta un proxy con el valor de la dirección lógica de un usuario registrada (address of record) presente en un Request-URI, antes de sustituir este último con la dirección que va a utilizar para encaminar la petición al usuario (por ejemplo la de contacto registrada). De este modo, se asegura que el destino reciba la dirección lógica correspondiente a la petición. Forma parte de las extensiones de SIP definidas en la RFC 3455 y denominadas cabeceras privadas, siendo aplicable lo que en ella figura.

6.3.8 Priority

Indica la urgencia de la petición tal como la percibe el cliente, describiendo la prioridad que la petición debería tener para el usuario o su agente. Su definición y uso aparece en la RFC3261, siendo aplicable lo que en ella figura.

6.3.9 Proxy-Authorization

Esta cabecera contiene la acreditación del cliente (incluyendo usuario y password) a efectos de autenticación. Su definición y uso aparece en la RFC3261, siendo aplicable lo que en ella figura.

6.3.10 Proxy-Require

Se usa para indicar las características que un UA necesita que soporte el *proxy*. Su definición y uso aparece en la RFC3261.

6.3.11 Rack

Se envía en un método PRACK para soportar la fiabilidad de las respuestas provisionales y sirve para poder relacionar dicho método con la respuesta que acepta. Su definición y uso aparece en la RFC3262, siendo aplicable lo que en ella figura.

6.3.12 Refer-To

Solo aparece en el método REFER como cabecera obligatoria. Indica el recurso que está siendo referenciado en el método REFER, y por tanto con el que el receptor debería contactar. Su definición y uso aparece en la RFC3515, siendo aplicable lo que en ella figura.

6.3.13 Referred-By

Referred-by contiene información sobre el emisor del REFER, que debe llegar al receptor de la nueva petición generada como resultado del proceso del REFER. Su definición y uso aparece en la RFC3892, siendo aplicable lo que en ella figura.

6.3.14 Reject-Contact

Forma parte de las extensiones de SIP, que permiten al usuario que envía la petición establecer preferencias que controlan de algún modo el proceso de la misma por parte de los proxy. En concreto, permite al UAC especificar al proxy que no contacte con un URI cuyas características, indicadas explícitamente en la cabecera “Contact”, concuerden con cualquiera de los valores de este campo cabecera. Su definición y uso aparece en la RFC3841 siendo aplicable lo que en ella figura.

6.3.15 Replaces

Se utiliza para reemplazar a un participante por otro en un diálogo existente. Contiene la información necesaria para poder identificar dicho diálogo (*Call-id*, *Tag* del To y del From). Su definición y uso aparece en la RFC3891, siendo aplicable lo que en ella figura.

6.3.16 Request-Disposition

Forma parte de las extensiones de SIP, que permiten al usuario que envía la petición establecer preferencias que controlan de algún modo el proceso de la misma por parte de los proxy. En concreto, proporciona una lista de directivas que el *proxy* debería cumplir. Su definición y uso aparece en la RFC3841 siendo aplicable lo que en ella figura.

6.3.17 Route

Se usa para proporcionar información de encaminamiento y consta de una lista de URI's a las que, en general, se progresará la petición hasta alcanzar el destino. Su definición y uso aparece en la RFC3261, siendo aplicable lo que en ella figura.

6.3.18 SIP-If-Match

Solo aparece en el método PUBLISH. La introduce el UA de cliente que envía dicho método, como actualización de una publicación realizada con anterioridad. Su valor debe coincidir con el del identificador (entity-tag) de la cabecera SIP-Etag (ver 6.2.11) recibida en la respuesta 2XY al PUBLISH correspondiente a la publicación inicial. Su definición y uso aparece en la RFC3903, siendo aplicable lo que en ella figura.

6.3.19 Subject

Indica el asunto de la sesión, permitiendo filtrados sin tener que analizar la descripción de sesión. Puede presentarse al usuario para que decida si acepta o no la sesión. Su definición y uso aparece en la RFC3261, siendo aplicable lo que en ella figura.

6.3.20 Subscription-State

Indica el estado de la suscripción. Su definición y uso aparece en la RFC3265, siendo aplicable lo que en ella figura.

6.4 CAMPOS CABECERA DEL CUERPO DE LOS MENSAJES

6.4.1 Content-Disposition

Indica como debe un UA interpretar el cuerpo del mensaje. Su definición y uso aparece en la RFC3261, siendo aplicable lo que en ella figura. Además de los valores allí indicados, puede utilizar el valor: "early-session" tal como se define en la RFC3959.

6.4.2 Content-Encoding

Indica que se ha aplicado una codificación al cuerpo de mensaje, y por tanto deben utilizarse decodificadores para obtener el tipo de medio referenciado en la cabecera Content-Type. Su definición y uso aparece en la RFC3261, siendo aplicable lo que en ella figura. Los esquemas de codificación están registrados en IANA.

6.4.3 Content-Language

Se usa para indicar el lenguaje del cuerpo del mensaje. Su definición y uso aparece en la RFC3261, siendo aplicable lo que en ella figura. Sus posibles valores están registrados en IANA.

6.4.4 Content-Length

Indica el número de octetos del cuerpo del mensaje (incluidos los CRLF de fin de línea). No se incluyen en este cómputo los CRLF que separan los campos cabecera y el cuerpo de mensaje. Su definición y uso aparece en la RFC3261, siendo aplicable lo que en ella figura.

6.4.5 Content-Type

Indica el tipo de medio del cuerpo de mensaje (tipo/subtipo). Su definición y uso aparece en la RFC3261, siendo aplicable lo que en ella figura. Los distintos valores de tipos y subtipos están registrados en IANA.

6.4.6 Mime Version

Proporciona la versión del protocolo MIME (definido en RFC 2045) utilizada en el cuerpo de mensaje. Su definición y uso aparece en la RFC3261, siendo aplicable lo que en ella figura.

7. CAMPOS SDP

La definición de campos SDP se realiza en la RFC 2327, sendo de obligado cumplimiento lo que en ella aparece.

El SDP en SIP se empleará conforme al modelo oferta-respuesta definido en la RFC 3264, siendo asimismo de obligado cumplimiento lo que en ella aparece.

En el citado modelo un participante de una sesión genera una mensaje SDP que constituye una oferta compuesta por un conjunto de medios y codecs que el oferente desea usar, junto con las direcciones IP y puertos por los que quiere recibir los flujos de información. Esta oferta es trasladada al otro participante, el cual responderá con un mensaje SDP en relación con la oferta propuesta. La respuesta indica para cada uno de los medios contemplados en la oferta cuáles son aceptados y cuáles no, junto con los codecs que serán usados y las direcciones IP y puertos por los que quiere recibir los flujos de información.

El SIP usa el mecanismo de oferta-respuesta SDP con el propósito de establecer sesiones entre agentes de usuario.

El criterio de apertura de flujo RTP utilizado en la NGN de Telefónica se detalla en el punto 8.8.

8. PROCEDIMIENTOS BÁSICOS

En los siguientes apartados se describen los procedimientos básicos soportados en SIP. En cada uno de ellos se hace bien una descripción general del procedimiento conforme a las RFCs que aplican al mismo o bien una referencia explícita a las mismas, así como las singularidades que con respecto a éste presenta por el momento la red NGN de Telefónica de España.

8.1 PROCEDIMIENTO DE ENCAMINAMIENTO

Es aplicable el definido en la RFC3261. No obstante en los terminales conectados a la NGN actualmente se utiliza solo una de las posibilidades admitidas, según la cual la política local del terminal puede especificar un conjunto de destinos alternativos a lo indicado en el Request-URI o Route.

En concreto en la solución NGN de Telefónica, el terminal envía todas sus peticiones a un *outbound proxy*, independientemente del valor del Request-URI, tal y como se indica en el punto 8.3. No obstante, el terminal debe ser configurable para que en el momento en que se decida pueda encaminar las peticiones dentro de diálogo conforme a la dirección incluida en el Request URI.

8.2 ESQUEMAS DE NUMERACIÓN SIP

Aunque SIP soporta diferentes esquemas de numeración URI tales como sip (SIP URI), sips (Secure SIP URI), tel (Telephone URI, conforme a RFC 3966) y pres (Presence URI), el esquema de numeración con el que se garantiza en estos momentos el funcionamiento en la NGN de Telefónica de España es el SIP URI.

Dado que el protocolo de Transporte empleado actualmente en dicha NGN es UDP no se soportará por el momento el esquema de numeración SIPS URI.

8.2.1 Componentes SIP URI

Es aplicable el formato, componentes y parámetros tal como se definen en la RFC3261. Además puede utilizarse el parámetro “comp” definido en la RFC3486.

Dado que el servicio de voz sobre IP en la NGN se soporta sobre el Plan de Numeración de Telefónica, los números marcados en el terminal se deberán transformar hacia la red en una dirección SIP URI en el que el campo *user* contendrá el número de teléfono y el parámetro *user* será igual a *phone*.

Como particularidad, los terminales conectados a la NGN no deben incluir el número de puerto donde la petición SIP será enviada. Este valor es opcional en la RFC 3261 y la NGN de Telefónica no lo requiere.

8.3 DESCUBRIMIENTO DEL *PROXY OUT-BOUND*

En la solución NGN de Telefónica el punto de contacto del terminal con la red será único. Dicho punto, con el que se establecerán tanto los flujos de señalización SIP como los flujos RTP, estará implementado en el *Session Border Controller* (SBC) cuya dirección IP pública se obtendrá de un servidor DNS.

Para ello se deberán programar en los terminales:

- SIP out-bound Proxy: sbc.ngn.rima-tde.net
- DNS IP address. Se almacenarán dos direcciones: DNS primario y DNS secundario. En caso de fallo del DNS primario se accederá al DNS secundario. La consulta DNS se realizará conforme a lo requerido en la RFC 3263, teniendo en cuenta que mientras se utilice el protocolo de transporte UDP y el puerto configurado no es necesario llevar a cabo la consulta NAPTR ni la consulta SRV, únicamente se realizará una consulta tipo A. En el caso de que la respuesta DNS incluya el campo *time-to-live*, el terminal deberá ser capaz de almacenar la respuesta DNS durante el tiempo indicado en el citado campo.

Los terminales deben soportar señalización simétrica, es decir, recibir y enviar mensajes SIP desde el mismo puerto UDP, y también flujo de medios simétrico (recibir y enviar flujo RTP desde el mismo puerto UDP).

8.4 PROCEDIMIENTO DE REGISTRO

Permite a un UA solicitar la creación en un dominio de una asociación entre la dirección lógica o pública que identifica al usuario (la dirección que se registra o “address of record”) y una o más direcciones de contacto adecuadas para encaminar las peticiones con destino a dicho usuario.

8.4.1 Descripción

Este procedimiento se realiza mediante el envío, por parte de un UAC de un método REGISTER, en el que figura, en determinados campos cabecera (ver 8.4.2) el dominio en el que debe realizarse el registro, la dirección que debe registrarse, y las direcciones de contacto.

El destino de esta petición es un elemento particular SIP llamado registrar que, en general, se encarga de:

- Incluir la dirección lógica o pública del usuario que se registra, en el servicio de localización al que pueden consultar los servidores proxy o de redirección del correspondiente dominio, asociándola a una o más direcciones a las que dichos elementos deben progresar las peticiones con ese destino.
- Mantener y actualizar la información y estado de todos los registros realizados.

En particular, para cada petición REGISTER recibida, el registrar:

- Solicita, antes de la realización del registro o actualización, la autenticación del usuario que va a registrarse siguiendo el procedimiento indicado en el punto 8.5, si la petición recibida no lleva una acreditación correcta.
- Determina si la petición corresponde a:
  - Un registro inicial, en cuyo caso la dirección de la cabecera To no está registrada. El registrar, si todo es correcto, va a crear un nuevo registro para esa dirección asociándola a las direcciones de contacto indicadas en la cabecera Contact. Lo normal es que este tipo de REGISTER se envíe cuando se enciende el terminal, o en caso de reinicio.
  - Una actualización de registro, en cuyo caso la dirección está ya registrada y la petición lleva cabecera Contact con valor distinto de "*". El registrar, si todo es correcto, va a actualizar, según el contenido de la cabecera Contact, las asociaciones correspondientes que ya existan. Las asociaciones nuevas presentes en la cabecera Contact se añadirán si el procedimiento se realiza con éxito. Lo normal es que el UAC envíe una actualización o refresco antes de que concluya el intervalo de validez de una o más asociaciones para evitar que se borren, o para variar la lista de contactos. Si quiere eliminar uno concreto, pondrá al valor 0 su correspondiente parámetro "expires".
  - Un borrado de registro, en cuyo caso la dirección está ya registrada y la petición lleva cabecera Contact con valor "*" y parámetro "expires"=0. El registrar borrará el registro creado para la dirección del To. Hay que tener en cuenta que, aunque no haya petición explícita de borrado, el registrar borrará el registro si vence el periodo de validez de todas las asociaciones.
  - Una consulta de registro, en cuyo caso, se recibe una petición REGISTER sin cabecera Contact. El registrar informará al UAC incluyendo las asociaciones existentes en la cabecera Contact de la respuesta 200 OK enviada.

  Se recomienda que, en caso de actualización, consulta o borrado de registro, el método REGISTER utilice el Call-Id del registro inicial, si bien se debe incrementar el Cseq en cada REGISTER, para que el registrar pueda realizar las actualizaciones siguiendo la secuencia correcta.
- Determina el tiempo de validez de cada asociación. Para cada dirección de contacto, en general, toma el tiempo del parámetro "expires" recibido en el Contact como intervalo de validez. Si no está presente, toma el de la cabecera Expires, y si tampoco figura, elige un intervalo según su propia configuración. No obstante, puede elegir un intervalo temporal menor que el indicado en los "expires" de la petición recibida.
- Si para un contacto, se supera el intervalo de validez sin recibir un REGISTER de refresco en cuya cabecera Contact esté incluido, el registrar borra su asociación con la dirección registrada. Si dicha dirección se queda sin ninguna asociación, se elimina su entrada en el servicio de localización y se considera no registrada.
- Genera la respuesta para el REGISTER recibido:
  - Si todo es correcto, responde con una 200 OK que:

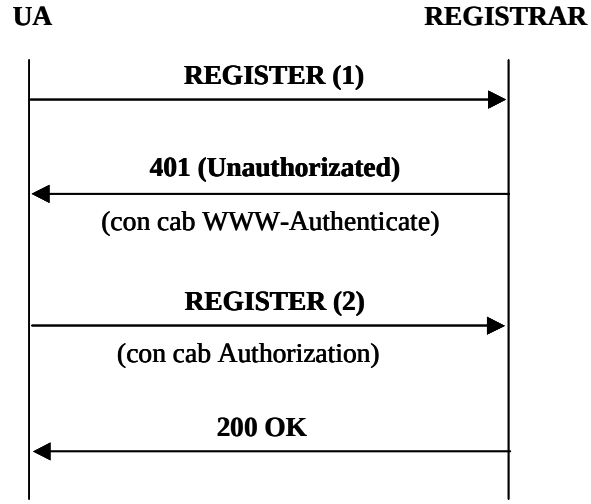
- Incluye una cabecera Contact con la lista de contactos (cero o más) que quedan asociados a la dirección registrada, indicando para cada uno de ellos el intervalo de validez en un parámetro “expires”.
- Opcionalmente puede incluir una cabecera Service-Route indicando la secuencia de proxies que conviene sigan las peticiones iniciales originadas por el UAC.
- Opcionalmente puede incluir una cabecera: Authentication-Info (ver 8.5).
- No incluye ninguna cabecera Record-Route, aunque la lleve el REGISTER recibido.

▪ En caso de error relativo al procedimiento de registro, pueden enviarse las siguientes respuestas:

- 400 Bad Request. Si el Contact lleva valor “*” con parámetro “expires” distinto de cero, o incluye el valor “*” y alguno más.
- 401 Unauthorized. Si la petición no lleva una acreditación correcta y se admite que se reenvíe (ver 8.5).
- 403 Forbidden. Si la petición no lleva acreditación válida, pero ya no debe reenviarse (ver 8.5).
- 404 Not Found. Si la dirección que quiere registrarse no es válida para el dominio indicado en el Request-URI.
- 423 Interval Too Brief. Si, en el REGISTER, el tiempo de expiración para uno o más contactos es demasiado corto.
- 500 Server Internal Error. Si no puede realizarse el procedimiento por un fallo interno del registrar, o la petición se ha enviado a un puerto distinto del esperado.

8.4.2 Flujo de señalización

La siguiente figura resume el flujo de señalización para un procedimiento de registro válido, considerando que con el REGISTER no llega una acreditación correcta y debe ser reenviado (lo normal en un registro inicial). Si la petición ya lleva acreditación y el registrar la admite, envía 200 OK si todo es correcto, sin previa 401, ni reenvío del REGISTER. Este último escenario es el normal en modificación o consultas de registros ya existentes.



(1) REGISTER sin acreditación (2) REGISTER con acreditación

A continuación se detallan los campos cabecera obligatorios y los opcionales más significativos que llevaría el REGISTER (2) enviado por el terminal (incluyendo acreditación).

Cabecera	Valor
Request-URI	Obligatorio. Nombre de dominio en el que se registra
To	Obligatorio. Identidad pública del usuario que se registra. Será una dirección SIP URI
From	Obligatorio. Normalmente la misma identidad pública que en To
Call-Id	Obligatorio. Nuevo valor en registro inicial, manteniéndose en sucesivos registros.
Via	Obligatorio. Dirección a la que debe enviarse la respuesta
Max-Forwards	Obligatorio. Número de saltos permitidos para la petición
Cseq	Obligatorio. Número de secuencia que se incrementa con cada REGISTER enviado
Route	Opcional. Route-set preexistente que tenga configurado el terminal (dirección del out-bound proxy).
Contact	Con las direcciones de contacto que quedarán asociadas a la dirección pública en el registro. Obligatorio en registros iniciales, actualizaciones y borrado de registros. Puede incluir

	el parámetro “expires”.
Authorization	Obligatorio. Lleva la acreditación del usuario.
Expires	Opcional. Valor de expiración aplicable a los contactos que no lleven el parámetro “expires”.

La respuesta 200 OK generada llevaría:

Cabecera	Valor
To	Obligatorio. El de la petición recibida correspondiente.
From	Obligatorio. El de la petición recibida correspondiente.
Call-Id	Obligatorio. El de la petición recibida correspondiente.
Via	Obligatorio. El de la petición recibida correspondiente.
Cseq	Obligatorio. El de la petición recibida correspondiente.
Authentication-Info	Opcional. Indicando información útil para nuevas autenticaciones.
Service-Route	Opcional. Direcciones que puede usar el UAC para encaminar peticiones, configurando con ellas una cabecera Route.
Contact	Obligatorio. Con las direcciones de contacto que en ese momento están asociadas a la dirección pública registrada No incluirá ninguna si el registro ha sido borrado. Cada dirección incluida lleva el parámetro “expires” indicando el tiempo de validez de la asociación correspondiente.

8.4.3 Consideraciones adicionales propias de la red NGN de Telefónica

En la solución NGN de Telefónica, el único punto de acceso de cada terminal a la red (outbound proxy) incorpora la funcionalidad “Hosted Nat Transversal” que permite que los equipos de usuario con funcionalidad de NAT/Firewall puedan atravesarse sin necesidad de realizar ninguna actualización software o hardware en casa del cliente. Esta funcionalidad, además de que el terminal soporte flujo RTP y señalización simétrica, tal y como se indicó en el punto 8.3, implica varias actuaciones, por parte del equipo que la soporta (SBC, Session Border Controller), que afectan al procedimiento de registro y se indican a continuación:

- Todos los mensajes de señalización SIP con destino el terminal deben llegar previamente al SBC encargado de realizar la función de “Hosted NAT Transversal” para dicho terminal. Para garantizar ésto, el SBC cambiará la dirección URI recibida como contacto en la petición REGISTER que reciba del terminal, por la suya propia, de modo que la dirección pública del usuario quede asociada en el registro con la dirección del SBC, a la que por

tanto llegarán todas las peticiones dirigidas al usuario. Este cambio se realiza de forma transparente para el terminal, que recibe en la correspondiente respuesta 200 OK el contacto que él incluyó.

La funcionalidad necesita que se mantengan abiertos los puertos del router de cliente. Como casi todos ellos se cierran aproximadamente tras 1 minuto de inactividad, el out-bound proxy va a forzar al terminal a enviar una actualización de registro en un intervalo que garantice la operativa del puerto. Para ello, modificará la respuesta 200 OK que envía el registrar a cada petición REGISTER del terminal, acortando el tiempo de expiración de cada contacto registrado. De los REGISTER que tan solo refresquen el intervalo de expiración, el SBC progresará hasta el registrar solo aquellos necesarios en función del intervalo impuesto por el registrar.

En la respuesta 200 OK al REGISTER no llegará al terminal la cabecera Service-Route. No obstante, en el supuesto de que en algún caso la llevara, el terminal deberá ignorarla y encaminar todas las peticiones conforme al procedimiento expresado en el punto 8.3.

Cada petición REGISTER llevará asociado un sólo contacto de manera que si se quiere asociar a un mismo usuario varios contactos se enviarán varias peticiones REGISTER, una por cada contacto.

8.5 AUTENTICACIÓN

Se utiliza un mecanismo de desafío-respuesta (chanllenge-response), basado en uno de los esquemas de autenticación (*Digest* y *Basic*) definidos en HTTP (RFC 2617). En concreto, en SIP se utiliza el esquema *Digest*, pues presenta sobre el esquema *Basic* la ventaja de que la password del usuario viaja codificada.

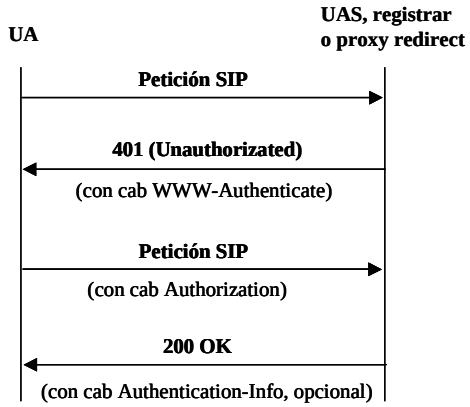
El procedimiento general de autenticación consiste en lo siguiente (la definición de las cabeceras y parámetros utilizados figura, respectivamente en los puntos 6 y 8.5.1):

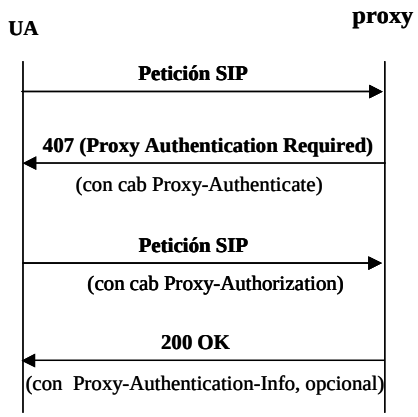
- Si un registrar, UAS o proxy recibe una petición, para la que necesita disponer de autenticación, analiza la acreditación o credenciales incluidas en la misma. Si no las lleva o son incorrectas, envía al UAC una respuesta indicando que debe reenviar la petición con una acreditación correcta (en esto consiste el “challenge”).
- Esta respuesta será distinta según el tipo de elemento SIP que solicite la autenticación, como se indica a continuación, pero en cualquier caso, indicará el esquema de autenticación utilizado (en este caso “Digest”), y llevará información suficiente para que el UAC pueda proporcionar la acreditación adecuada. Dicha información incluye el espacio de protección (parámetro “realm”) dentro del cual podrá utilizarse esa acreditación con el correspondiente usuario-password, y un valor generado por el servidor que se utiliza para validar la acreditación (parámetro “nonce”).

- Si el servidor que solicita la autenticación es un registrar, un *proxy redirect* o un UAS, la respuesta es la 401 (Unauthorizated). Incluye obligatoriamente la cabecera WWW-Authenticate.
- Si el servidor que solicita la autenticación es un proxy la respuesta es la 407 (*Proxy Authentication Required*). Incluye obligatoriamente la cabecera *Proxy-Authenticate*.

- Como respuesta al "challenge", el UAC envia de nuevo la petición, incrementando el valor de la cabecera Cseq, e incluyendo la acreditación en una cabecera: *Authorization* si la respuesta recibida fue la 401, o *Proxy-Authorization* si la respuesta recibida fue la 407. Estas cabeceras incluyen, en el parámetro "response" la identidad privada del usuario y password codificados.
- El servidor analiza el contenido de la cabecera *Authorization* o *proxy-Authorization* verificando la validez de la acreditación. Si todo es correcto envía una respuesta 200 OK, que puede incluir la cabecera *Authentication-Info* (o *Proxy-Authentication-Info* si la autenticación la realiza un proxy) , indicando información útil para nuevas autenticaciones, como el nonce que debe usarse (parámetro "nextnonce").

La siguiente figura representa el procedimiento descrito.





Consideraciones adicionales

- Puede enviarse una respuesta 401/407 forzando la autenticación de cualquier petición que no sea CANCEL o ACK. La primera porque no puede reenviarse, y la segunda porque es una petición para la que no se recibe respuesta y que siempre llevará las cabeceras Authorization o Proxy-Authorization del INVITE correspondiente.
- El UAC puede enviar, en las peticiones que genere, la cabecera Authorization o Proxy-Authorization, aunque no haya recibido la respuesta 401 o 407.
- El UAC puede necesitar la intervención del usuario para obtener su nombre y password para un determinado "realm" (se presentaría al usuario), y así poder elaborar la acreditación. Una vez obtenida esta información debería almacenarla asociada con el "realm" pudiendo así reutilizarla en otras peticiones.
- Si el UAC no tiene almacenada la información de acreditación, y no consigue obtener el nombre y password del usuario, puede intentar elaborar la acreditación con nombre de usuario: "anonymous" y password: " ".
- Un UAC que representa a muchos usuarios, como por ejemplo un gateway PSTN, puede tener un único nombre y password para todos ellos.
- Si la acreditación proporcionada en la cabecera Authorization o Proxy-Authorization no es correcta, el servidor puede enviar la respuesta 401/407, que forzará al UAC a reenviar la petición con una acreditación distinta a la rechazada, o una respuesta 403 (Forbidden), en cuyo caso el UAC no reenviará la petición.

8.5.1 Parámetros

Se especifican en la RFC 2617. A continuación se indican sus detalles más relevantes o las diferencias particulares de SIP.

"username": Es el nombre del usuario .

"realm": Define el espacio de protección. Es una cadena de caracteres que se presenta al usuario, de modo que sepa que usuario y password utilizar. Debería contener al menos el nombre del host que solicita la autenticación y podría adicionalmente indicar el conjunto de usuarios que tendrían acceso al mismo.

"domain": Una lista entrecomillada de URI's, separadas por espacios, que definen el dominio de protección en el que un cliente puede utilizar la misma información de autenticación. Si no aparece o está vacío, se asume que es el cubierto por el servidor que realiza la autenticación y que aparece en el "realm".

No se utiliza en las cabeceras proxy-Autenticate para las cuales el espacio de protección es el del proxy. Si aparece en este caso debe ignorarse.

"nonce": Es una cadena de caracteres generada por el servidor que realiza la autenticación y que debería ser única para cada respuesta 401/407 enviada. Se recomienda que la cadena esté en base64 o en hexadecimal. Su contenido es dependiente de la implementación. No se presenta al usuario.

"nextnonce": Indica el valor que el servidor quiere que use el cliente para las futuras respuestas a una solicitud de autenticación. Aparece en la cabecera Authentication-Info.

"opaque" : Es una cadena de caracteres especificada por el servidor, que debería ser devuelta por el cliente sin cambios en la cabecera "Authorization" de las siguientes peticiones con URI´s pertenecientes al mismo espacio de protección. Se recomienda que esté en base64 o hexadecimal.

"stale": Indica que la petición anterior del cliente ha sido rechazada debido a que el valor del nonce incluido ha caducado. Si "stale" tiene valor:TRUE, el cliente puede simplemente reenviar la petición con una nueva respuesta, sin variar el usuario ni la pasword, pues con dicho valor se indica que el "digest" es válido (salvo el "nonce"). Si se rechaza la autenticación y no se envía este parámetro o se envía con valor: FALSE, el rechazo se debe a que el usuario y/o password son inválidos y debe obtenerse nuevos valores para ellos.

"digest-uri": Es el URI del Request-URI (entre comillas), duplicado aquí puesto que algún proxy podría cambiar este valor al transitar la petición.

"response": Una cadena de 32 caracteres hexadecimales que incluye el nombre de usuario y la password codificados según los esquemas correspondientes al mecanismo "digest", junto a los valores del método correspondiente y de al menos los parámetros nonce y digest-uri. Los detalles acerca de la construcción de este parámetro aparecen en los puntos 3.2.2.1-3.2.2.5 de la RFC 2617.

"rspauth": Se construye como el parámetro "response", pero sin incluir el método, y proporciona autenticación mutua. Solo se utiliza en una cabecera Authentication-Info o Proxy-Authentication-Info.

"algorithm": Es una cadena de caracteres que indica el algoritmo utilizado para realizar la codificación aplicada al mecanismo "digest". Este valor debe corresponder al proporcionado por el servidor que autentica en la cabecera WWW-Authenticate. En la actualidad están definidos los valores MD5 y MD5-ess. Por defecto se asume MD5.

"qop": Indica la "protección de calidad" aplicada. Es opcional por compatibilidad con la RFC 2543. No obstante todos los servidores SIP que cumplan la RFC3261 deben incluirlo en las cabeceras generadas para solicitar la autenticación, y si un cliente recibe una de estas cabeceras con el parámetro "qop", la correspondiente cabecera que genere incluyendo su acreditación, lo llevará obligatoriamente y con el mismo valor.

Sus valores posibles por el momento son: "auth" (autenticación) o "auth-int"(autenticación con integridad de protección). Su presencia y valor afecta a la construcción del parámetro "response" o "rspauth", en cuanto a si se incluyen en él más o menos valores, pues si está presente, se incluye su propio valor, el del "cnonce" y "nonce-count". Con el valor: "auth-int" se incluye además el cuerpo de mensaje de la petición o respuesta en la codificación, obteniendo así cierta protección de integridad para el mismo.

"cnonce": Solo se envía si figura el parámetro "qop", siendo en este caso un parámetro obligatorio. Consta de una cadena de caracteres opaca para el usuario, que genera el cliente (el que se está autenticando) y es usada tanto por dicho cliente como por el servidor para evitar ataques y para proporcionar mutua autenticación y alguna protección de integridad al mensaje.

"nc" (nonce-count): Solo se envía si figura el parámetro "qop", siendo en este caso un parámetro obligatorio. Es el contador hexadecimal del número de peticiones que el cliente ha enviado con el valor de "nonce" que figura en la petición actual (se cuenta también esta última).

Se permite la inclusión de futuras extensiones o parámetros. Cualquier directiva no reconocida, será ignorada.

8.5.2 Restricciones actuales en NGN de Telefónica

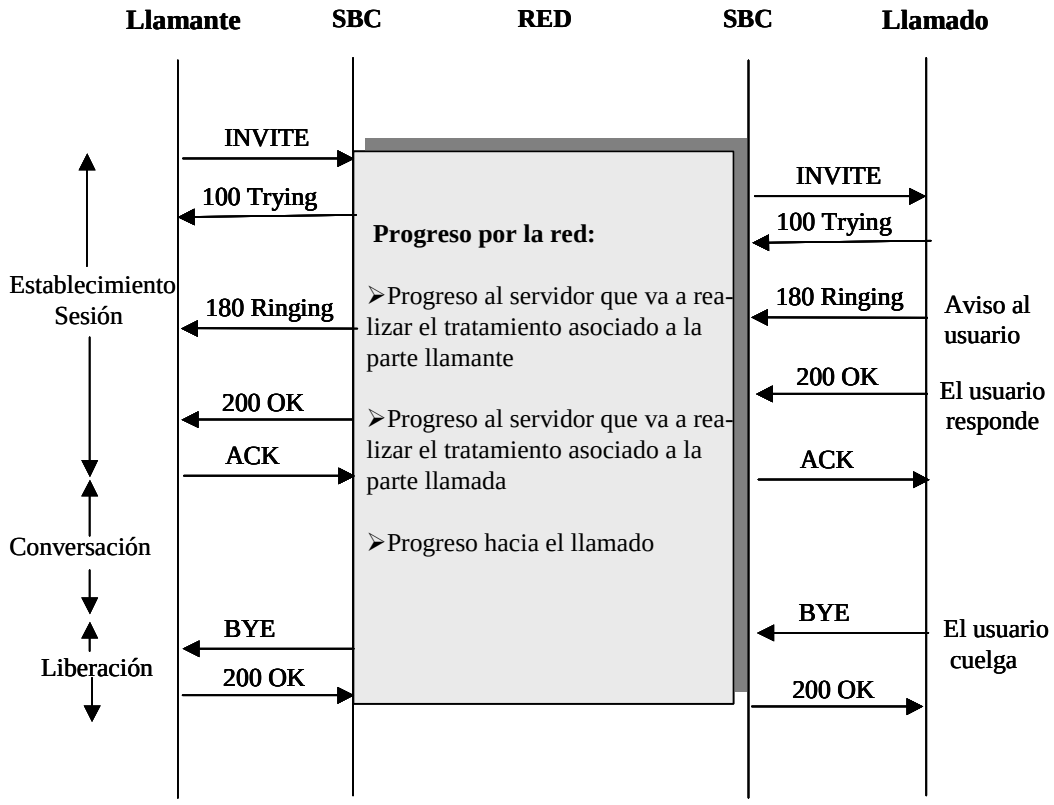
- La plataforma que autentica distingue entre mayúsculas y minúsculas en el "realm".
- Como valores de "qop", la plataforma solo envía, por el momento el valor "auth". Como valor de "algorithm" solo el valor MD5.
- Hay que señalar que de acuerdo con la RFC 2617, los terminales deben soportar la reutilización del "nonce" y la cabecera *Authentication Info* con "nextnonce".

8.6 FLUJOS DE LLAMADA EN DOMINIO IP

8.6.1 Sesión IP-IP

A continuación se muestra el procedimiento correspondiente a una llamada telefónica entre dos terminales IP cursada a través de una red VoIP.

La figura adjunta representa las distintas fases de la llamada y que se describen en los siguientes apartados.



8.6.1.1 Solicitud de establecimiento de sesión

Cuando el usuario llamante indica la dirección del destino al que quiere llamar (por ejemplo marcando su número), su UA solicita el establecimiento de una sesión que permita el intercambio de flujos RTP con ese destino. Para ello envía una petición INVITE que generalmente incluirá un cuerpo de mensaje tipo SDP (descripción de sesión), indicando la oferta de medios por parte del llamante para cursar los flujos RTP asociados a la comunicación con el llamado.

En la tabla adjunta figura el contenido de este INVITE. Aunque puede llevar más cabeceras opcionales, se indican las obligatorias y las más comunes o recomendables. El Request-URI lleva la identidad pública del usuario llamado.

Campos	Valor
To	Obligatorio. Identidad pública del usuario llamado
From	Obligatorio. Identidad pública del usuario llamante
Call-Id	Obligatorio. Identificador de llamada
Via	Obligatorio. Dirección a la que debe enviarse la respuesta

Max-Forwards	Obligatorio. Número de saltos permitidos para la petición
Cseq	Obligatorio. Número de secuencia
Contact	Obligatorio. Con la dirección de contacto para el llamante.
Content-Type	Obligatorio si se incluye cuerpo de mensaje, indicando el tipo de medio. En caso de descripción de sesión su valor es: application/sdp
Content-Length	Solo obligatorio si el protocolo de acceso en TCP. Nº de octetos del cuerpo de mensaje
Allow	Recomendable. Indica los métodos que pueden usarse en el diálogo que va a establecerse.
Session-Expires	Recomendable (ver consideraciones punto 8.6.2).
Supported	Obligatorio. Indica las extensiones que soporta el UA llamante (ver consideraciones punto 8.6.2).
Route	Si se incluye, la petición se encamina a su dirección superior. El terminal lo cofiguraría a partir del preexistente route-set o de la información de un Service-Route recibido en el proceso de registro
Privacy	Opcional. Se puede usar para ocultar la identidad del usuario (CLIR). Para ello se deberá configurar con los valores *user*, *id* y *critical*.

Una vez configurada, la petición se envía siguiendo los criterios definidos en el apartado correspondiente al encaminamiento SIP. Los terminales de Telefónica van a enviarla siempre al outbound proxy con funcionalidad SBC.

8.6.1.2 Progreso de la solicitud

El SBC envía a la red el INVITE recibido para que progrese la solicitud de establecimiento de sesión hasta el terminal llamado.

Cada elemento SIP, al recibir un INVITE, envía inmediatamente hacia el anterior una respuesta provisional 100-Trying, a fin de indicar la recepción de la petición y detener así sus retransmisiones. Después realiza para la petición INVITE el análisis y tratamiento adecuados y la dirige hacia el siguiente elemento.

La solicitud progresa por la red hacia los elementos encargados de realizar el control de la llamada, tanto para la parte llamante como para la parte llamada, en función de los respectivos perfiles de usuario configurados en la red.

En caso de que el llamado tenga registradas varias direcciones de contacto, el servidor que obtenga sus datos de registro, realizará un envío múltiple de la solicitud INVITE hacia todos ellos (forking).

8.6.1.3 Aviso al llamado

La solicitud de establecimiento llega al terminal llamado a través de su correspondiente SBC. Si todo es correcto, el terminal avisa al usuario proporcionando una corriente de llamada, localmente o tratando la cabecera "Alert-Info" si estuviera presente. Entonces envía hacia atrás una respuesta provisional: 180 Ringing, que podría incluir opcionalmente:

- Un parámetro tag en la cabecera To, a fin de establecer el diálogo entre terminales llamante y llamado, aunque en estado "anticipado" (ver detalles en 8.6.1.4.1).
- Un cuerpo de mensaje SDP con la respuesta a la oferta recibida en el INVITE. En este caso, el llamado realiza la apertura de flujos RTP correspondiente a la oferta-respuesta negociada.

Cuando el terminal llamante recibe esta respuesta:

- Si incluye el parámetro tag en la cabecera To, crea el correspondiente diálogo en estado "anticipado" (ver 8.6.1.4.1).
- Si incluye un cuerpo de mensaje SDP, realiza la apertura de flujos RTP correspondiente a la oferta-respuesta negociada.
- Si no incluye cuerpo de mensaje SDP, proporciona al llamante el tono de llamada, localmente o tratando la cabecera "Alert-Info" si estuviera presente.

El que la respuesta provisional lleve cuerpo de mensaje con descripción de sesión no es lo habitual, y solo tiene sentido si puede realizarse la apertura de flujo RTP antes del envío de la respuesta final.

Lo anterior sucede si el INVITE se recibe con una oferta de sesión a la que la respuesta provisional contesta o, en caso contrario, si la respuesta provisional lleva una oferta y se transmite con fiabilidad, lo que obliga a que se conteste inmediatamente con un PRACK, que debe llevar la respuesta a la oferta.

La apertura de flujo RTP antes de la respuesta 200 OK puede ser útil en caso de que el llamante reciba una locución sin descolgado o reciba un tono de llamada desde el terminal llamado (aunque este procedimiento no se aplica actualmente en la NGN de Telefónica).

En caso de haberse realizado un envío múltiple de la solicitud de sesión (forking), el llamante puede recibir varias respuestas 180 Ringing procedentes de distintos puntos. Su tratamiento será para cada una de ellas el que se ha indicado, pudiendo generarse varios diálogos "anticipados".

8.6.1.4 Respuesta del llamado

Se produce cuando el llamado descuelga.

El terminal envía una respuesta 200 OK, que obligatoriamente llevará el parámetro tag en la cabecera To, quedando establecido de este modo el diálogo entre llamante y llamado, ya en estado "confirmado". En el apartado 8.6.1.4.1 se describe la creación del diálogo.

Además la 200 OK incluye obligatoriamente un cuerpo de mensaje SDP con la respuesta a la oferta recibida en el INVITE, o, en caso de recepción de INVITE sin SDP, la oferta por parte

del llamado en cuanto a medios disponibles para la sesión. Si ya se ha enviado una respuesta 180 Ringing con cuerpo de mensaje SDP, ese mismo cuerpo se incluirá en la respuesta 200 OK.

Cuando se produce el envío y recepción de la respuesta 200 OK a un INVITE portador de una oferta de sesión, se considera realizada la negociación y apertura de medios, y por tanto establecida la sesión.

En el caso de que se haya realizado un envío múltiple de la solicitud de establecimiento de sesión (forking), pueden llegar al llamante respuestas 200 OK desde distintos puntos (con diferente tag en el To), estableciéndose, para cada una de ellas, un diálogo distinto en el UAC (aunque todos ellos correspondan a la misma llamada), que aplicará a cada uno el tratamiento que se indica en el apartado 8.6.1.4.1.

El terminal considera completa la transacción correspondiente al INVITE inicial tras un intervalo de tiempo establecido a partir de la primera respuesta 200 OK recibida. Finalizado el mismo, elimina cualquier diálogo relacionado con este INVITE que no esté confirmado (es decir para el que no se haya recibido una respuesta final).

En la tabla adjunta figura el contenido de la respuesta 200 OK. Aunque puede llevar más cabeceras opcionales, se indican las obligatorias y las más comunes o recomendables.

Campos	Valor
To	Obligatorio. El de la petición, pero con Tag obligatorio
From	Obligatorio. El de la petición recibida.
Call-Id	Obligatorio. El de la petición recibida.
Via	Obligatorio. El de la petición recibida, manteniendo el orden.
Cseq	Obligatorio. El de la petición recibida.
Contact	Obligatorio. Con la dirección de contacto para el llamado.
Record-Route	Obligatorio si está en la petición recibida. Se copia manteniendo el orden.
Content-Type	Obligatorio pues se incluye cuerpo de mensaje, indicando el tipo de medio. En caso de descripción de sesión su valor es: application/sdp
Content-Length	Solo obligatorio si el protocolo de acceso en TCP. Nº de octetos del cuerpo de mensaje
Allow	Recomendable. Indica los métodos que pueden usarse en el diálogo que va a establecerse.
Session-Expires	Recomendable (ver consideraciones punto 8.6.2).
Supported	Obligatorio (ver consideraciones punto 8.6.2). Indica las extensiones que soporta el UA llamado

8.6.1.4.1 Establecimiento de diálogo

La creación del diálogo correspondiente a una llamada, está asociada al envío o recepción de la primera respuesta (no 100-Trying), con parámetro tag en la cabecera To, al INVITE inicial. El UA llamado crea el diálogo al enviar dicha respuesta y el UA llamante al recibirla.

Consiste en el almacenamiento en ambos UA, de determinada información obtenida a partir de la petición inicial recibida (UA llamado) y de la primera respuesta recibida con parámetro tag en la cabecera To (UA llamante). Esta información sirve para el envío de las siguientes peticiones dentro de la misma sesión (configuración de sus cabeceras, control de secuencia, etc).

En concreto la información que se guarda es:

- Call-Id+tag del From+tag del To. Con ella se crea el "Identificador del diálogo". A cualquier nueva petición que se envíe dentro ese diálogo le corresponde el mismo identificador, es decir todas llevan el mismo Call-Id y los mismos tag en cabeceras From y To.
- URI del From. Con ella el UA llamado crea la URI-remota, que incluye en la cabecera To de las nuevas peticiones que envíe. El UA llamante crea la URI-local, que incluye en la cabecera From de las nuevas peticiones que envíe.
- URI del To. Con ella el UA llamado crea la URI-local, que incluye en la cabecera From de las nuevas peticiones que envíe. El UA llamante crea la URI-remota, que incluye en la cabecera From de las nuevas peticiones que envíe.
- Cseq. Sirve para crear los números de secuencia locales o remotos. Los primeros se usan para construir el Cseq de las siguientes peticiones que se envíen dentro del diálogo (se incrementa en 1 la secuencia local, excepto en los casos de envío de ACK, PRACK y CANCEL). Los segundos para comprobar que las peticiones dentro del diálogo se reciben en secuencia.

  El llamado crea la secuencia remota con el Cseq del INVITE inicial recibido y la actualiza con el de cada nueva petición recibida. La secuencia local, al constituir el diálogo, está vacía y luego se actualiza con el Cseq de cada nueva petición enviada dentro del diálogo.

  En el llamante se crea la secuencia local con el Cseq del INVITE inicial enviado, y se actualiza con los de las siguientes peticiones que envía dentro del diálogo. La secuencia remota está vacía al construir el diálogo, y luego se actualiza con el Cseq de cada nueva petición recibida dentro del diálogo.
- Record-Route. Con ella se crea el route-set que sirve para construir la cabecera Route de las siguientes peticiones dentro del diálogo. El UA llamado lo crea con el Record-Route recibido en el INVITE inicial y que copia en la respuesta enviada. El llamante lo crea con el Record–Route de la respuesta recibida, pero invirtiendo su orden. Si no se recibe cabecera Record-Route, el route-set queda vacío, y no se envía cabecera Route en las siguientes peticiones.
- Contact. Con esta información se configura el destino remoto (remote-target) que, en general, se incluye en el Request-URI de las nuevas peticiones enviadas dentro del diálogo. El UA llamado utiliza el Contact del INVITE inicial recibido, enviando su propia

dirección de contacto en la respuesta. El UA llamante utiliza el Contact recibido en dicha respuesta.

Tanto si la respuesta que configura el diálogo es provisional, como si es 200 OK, se guarda la misma información, aunque el estado de diálogo asociado es distinto: “anticipado” en el primer caso y “confirmado” en el segundo.

Cuando se envía o recibe una respuesta 200 OK, y ya existe para la llamada un diálogo anticipado, se sustituye la información de route-set almacenada con la correspondiente al Record-Route de la respuesta 200 OK (es por compatibilidad con RFC anteriores a la 3261, en las que las respuestas provisionales no llevaban la cabecera Record-Route).

Además de la petición INVITE, en SIP se pueden crear también diálogos con las peticiones SUBSCRIBE y REFER.

Asociado a un diálogo existente se pueden realizar las peticiones INVITE, UPDATE, OPTIONS, NOTIFY, SUBSCRIBE, MESSAGE, REFER, INFO, PUBLISH, CANCEL y BYE.

Las peticiones OPTIONS, MESSAGE, PUBLISH y CANCEL pueden ir fuera de diálogo y la petición REGISTER va siempre fuera de diálogo y además no lo crea.

8.6.1.5 Aceptación

Cuando el UA llamante recibe la respuesta 200 OK, envía una petición ACK al otro extremo que finaliza la retransmisión de dicha respuesta, pues ya está seguro de que se ha recibido. El envío y recepción del ACK provoca que los extremos terminen la transacción asociada al INVITE. En caso de recibir varias respuestas 200 OK para el mismo INVITE, como resultado de que se haya realizado un envío múltiple (forking), se mandará un ACK para cada una de ellas.

Este ACK es una petición que se envía dentro del diálogo establecido, y sus cabeceras se ajustan a las normas indicadas para este caso, excepto que, en el Cseq, utiliza el mismo número de secuencia que el INVITE al que corresponde, aunque el método indica ACK.

Si el INVITE no llevó oferta SDP, entonces la llevará la respuesta 200 OK, y el ACK llevará la respuesta a dicha oferta. En este caso, la sesión queda establecida con el envío y recepción del ACK.

Si la oferta no es aceptable, enviará asimismo el ACK con una respuesta válida, indicando que se rechazan todos los medios, e inmediatamente un mensaje BYE que terminará el intento de sesión.

8.6.1.6 Liberación de una sesión

Cuando, tras el establecimiento de sesión, el llamante o llamado cuelga, se produce la liberación de la misma. El UA correspondiente envía para ello una petición BYE, que se construye como cualquier otra dentro de diálogo y supone la finalización de la sesión (es decir se detiene el envío o recepción de flujo RTP).

Asimismo, se termina el diálogo correspondiente salvo que haya alguna otra aplicación asociada al mismo (por ejemplo una suscripción para un evento). Por tanto, en general y, en concreto, en el escenario de llamada básica, el BYE termina tanto la sesión como el diálogo.

Se dan las siguientes diferencias en función de que el usuario que cuelgue sea el llamante o el llamado:

- El llamante, solo envía BYE cuando se ha establecido ya un diálogo, ya sea anticipado o confirmado (debe liberar con CANCEL antes de que esté constituido el diálogo). Aunque se recomienda que antes de recibir una respuesta 200 OK, y por tanto con diálogo anticipado, utilice CANCEL para liberar la sesión o intento.

  En diálogos confirmados solo libera con BYE. En caso de que para la misma llamada haya varios diálogos confirmados (cuando se ha hecho un envío múltiple), se enviará un BYE para cada uno.

- El llamado no envía BYE para terminar la sesión a menos que haya recibido ya el ACK, o bien haya vencido la temporización asociada a la transacción INVITE sin recibir ACK, incluso aunque el usuario haya colgado antes.

8.6.1.7 Modificación o refresco de una sesión

Un UA llamante o llamado puede realizar cambios en los parámetros de una sesión establecida, incluyendo una nueva oferta SDP (tanto lo que cambia como lo que no) en una petición: INVITE (en este caso se llama re-INVITE, puesto que se envía dentro de diálogo) o UPDATE, enviadas ambas siempre dentro de un diálogo. El otro extremo responderá, en caso de aceptar el cambio, con una 200 OK, que incluirá la respuesta SDP a la oferta realizada (si no acepta la oferta envía el mensaje de error adecuado y la sesión permanece como antes).

Tanto UPDATE como re-INVITE pueden modificar la sesión negociada y/o el contenido del "destino remoto" en el diálogo correspondiente (el receptor cambia la dirección URI de este contenido por la de la cabecera "Contact" de la petición, si son distintas).

El uso de una u otra petición depende del momento en que se realice la modificación:

- Si no se ha recibido la respuesta 200 OK al INVITE inicial, se envía UPDATE. Esta petición se contesta con la 200 OK inmediatamente. Si se modifica la sesión, el UPDATE lleva una oferta SDP y el 200 OK su respuesta aceptándola.

- Si se ha recibido la respuesta 200 OK al INVITE inicial, puede utilizarse tanto UPDATE como re-INVITE, pero se recomienda el uso de esta última, pues proporciona la opción de avisar al usuario antes de responder a la petición con 200 OK.

  Si se usa re-INVITE es aplicable el modelo de oferta-respuesta SDP indicado para el INVITE inicial, de modo que aunque el re-INVITE no lleve una oferta para cambiar la sesión, ésta puede incluirse la respuesta 200 OK, y la aceptación se incluiría en el ACK correspondiente.

Puede acudirse a más detalles sobre la modificación de sesión en los puntos anteriores que describen los métodos INVITE (ver punto 4.1) o UPDATE (ver punto 4.13), y en el que describe el modelo oferta-respuesta (ver punto 7).

Si se aplica a la sesión un procedimiento de temporización según la RFC 4028, se enviarán las peticiones de refresco a lo largo de la misma (el UAC o el UAS según la negociación realizada en dicho procedimiento). Estas peticiones en la Plataforma NGN serán por el momento re-INVITE y no UPDATE.

8.6.1.8 Sesiones infructuosas

De acuerdo con el procedimiento de establecimiento de sesión indicado en los apartados anteriores se pueden dar situaciones de error en las que se rechaza la llamada. Este rechazo puede realizarse desde el lado llamado o directamente se puede ordenar desde la Red NGN.

La figura 8.6.1.8.1 refleja una llamada infructuosa notificada al terminal llamante, mientras que la figura 8.6.1.8.2 refleja una llamada infructuosa debido al rechazo de la misma realizado desde el terminal llamado.

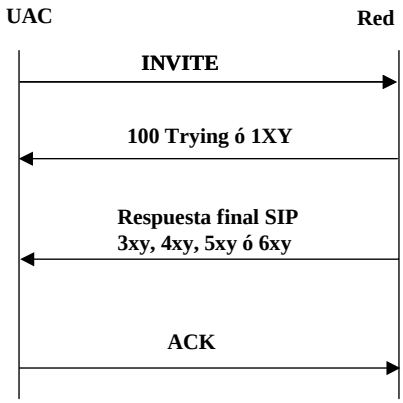


Figura 8.6.1.8.1

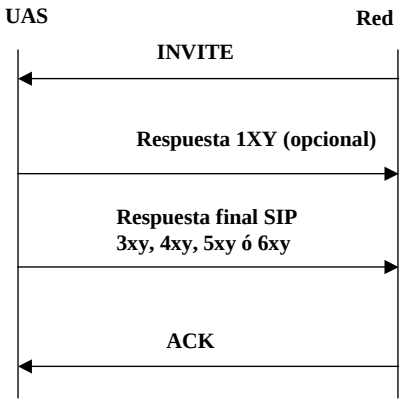


Figura 8.6.1.8.2

Las respuestas finales de las sesiones infructuosas pueden ser cualquiera de las definidas en los apartados 5.3, 5.4, 5,5 y 5.6 de este documento.

8.6.2 Consideraciones adicionales propias de la red NGN de Telefónica

Según se puede observar en la figura 8.6.1.1, el intercambio de señalización SIP para el establecimiento de sesiones IP-IP se realiza siempre entre el terminal y el SBC, tanto en llamadas originadas como terminadas. La respuesta 200 OK al INVITE llevará el parámetro *received* con la dirección IP pública del router, desde la que el SBC ha recibido la petición, en el campo cabecera Via.

Del mismo modo, el modelo oferta/respuesta SDP se efectúa entre el terminal y el SBC, abriendo los flujos RTP entre los puertos y medios negociados por ambos. Esto es válido tanto para el lado llamante como para el lado llamado. Los mensajes SIP y el flujo RTP progresan por la red entre los SBCs lado llamante y llamado.

La interfaz terminal-red utilizará para transporte el protocolo UDP.

El envío de tonos DTMF en la interfaz terminal-red se podrá realizar en RTP tanto en banda como fuera de banda. Para este último caso se deberá cumplir la RFC 2833. Desde la red se podrá configurar el terminal para que use cualquiera de los dos métodos.

El terminal debe soportar el procedimiento de temporización de sesión definido en la RFC 4028. Es decir, debe incluir en las peticiones INVITE y UPDATE la cabecera *Supported* con valor *Timer*. Los valores utilizados para temporizar, correspondientes a las cabeceras Session-Expires y MIN-SE, deben fijarse a criterio de la red por lo que ambas cabeceras serán teleconfigurables en los terminales, debiendo admitir valores MIN-SE iguales o mayores a 90s.

En el caso de envío múltiple (forking) cuando se recibe en la Plataforma NGN el primer 200 OK correspondiente a uno de los INVITE enviados, se envía desde ésta peticiones CANCEL para el resto de los INVITE enviados, con el fin de que se establezca una única sesión (con el primer destino que contesta). Sin embargo, lo anterior no garantiza que al terminal le llegue un único 200 OK. En caso de que tras el primer 200 OK recibido lleguen 200 OK procedentes de otros puntos, enviará a cada uno un BYE tras la correspondiente aceptación con ACK.

El SBC para evitar que lleguen al terminal direcciones propias de la red NGN, no va a progresar hacia él la cabecera *Service-route* que reciba en la respuesta 200 OK a un REGISTER. Por tanto, el terminal utilizará, como valor de cabecera *Route* (si la incluyera) de una petición inicial, el preexistente *route-set* que debe ser la dirección del outbound proxy.

La restricción de la presentación de la identidad de la línea llamane (CLIR) se podrá realizar anteponiendo al número marcado el código 067 o haciendo uso de la cabecera *Privacy* con los valores indicados en la tabla del punto 8.6.1.1. El terminal llamado recibirá en la cabecera From el *display name* “Anónimo”. Nunca recibirá la cabecera *P-Asserted-Identity* ya que los proxies de la red consideran que el terminal pertenece al dominio no seguro y borra dicha cabecera antes de entregar la petición.

Las respuestas 18xy se deberán generar en los terminales sin SDP. Únicamente la Plataforma podrá enviar respuestas 18xy con SDP (envío de locuciones sin respuesta).

Los cambios de medio en una sesión establecida se realizarán con INVITE preferiblemente.

Las peticiones INVITE que genera el terminal siempre llevarán cuerpo SDP. Lo anterior garantiza que se realiza la correcta tarificación a partir del 200 OK, dado que en ese momento se establece la sesión.

8.7 FLUJOS DE LLAMADA CON INTERFUNCIONAMIENTO DOMINIO IP-PSTN

8.7.1 Sesión IP-PSTN

A continuación se muestra el procedimiento correspondiente a una llamada telefónica con origen en un terminal IP que accede a través de una red VoIP y cuyo destino es un terminal de la PSTN. En este escenario es necesario llevar a cabo el interfuncionamiento SIP-PUSI definido en la recomendación Q.1912.5 de la UIT-T.

La figura 8.7.1.1 representa las distintas fases de la llamada y que se describen en los siguientes apartados.

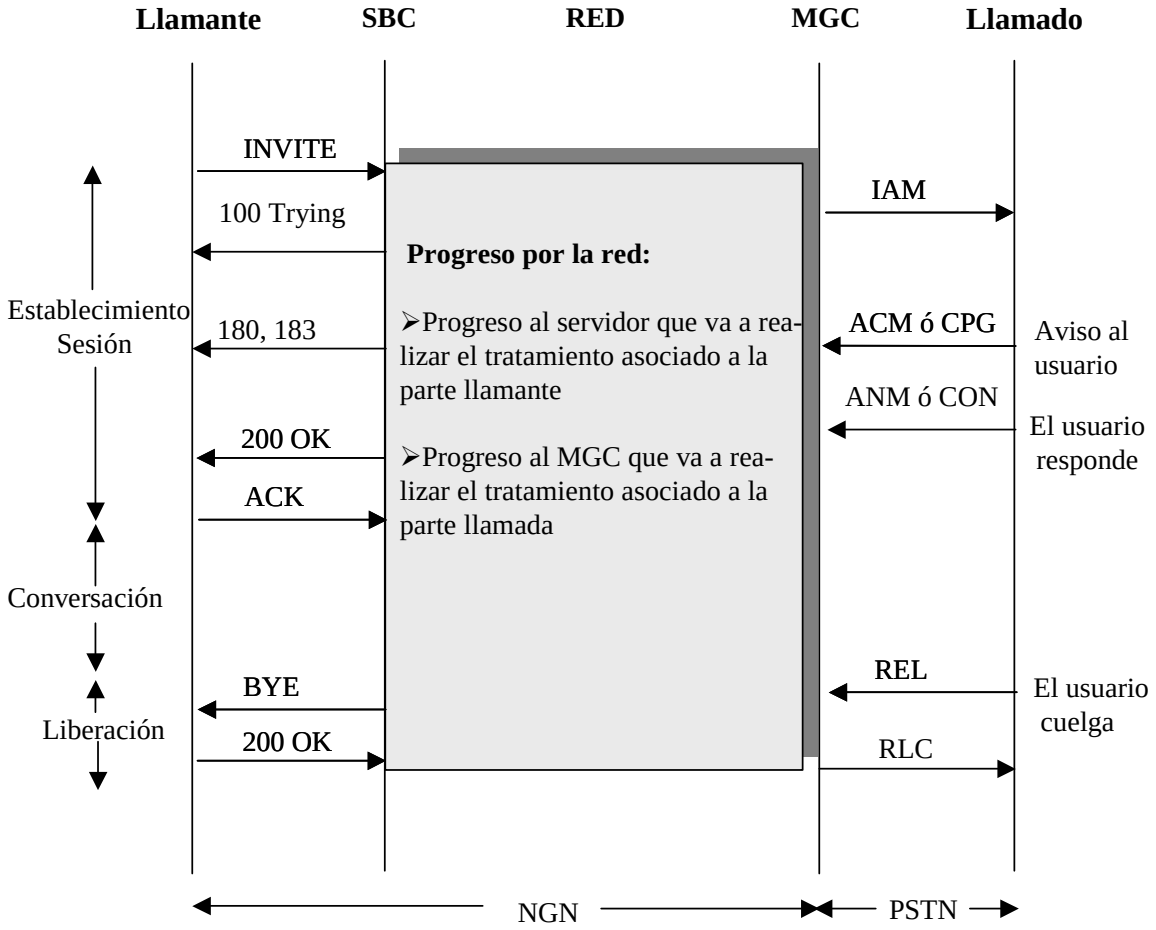


Figura 8.7.1.1

8.7.1.1 Solicitud de establecimiento de sesión

El establecimiento de la sesión se hace de la misma manera que se indicó en el apartado 8.6.1.1 para la sesión IP-IP. Es decir, se envía una petición INVITE que generalmente incluirá un cuerpo de mensaje tipo SDP (descripción de sesión), indicando la oferta de medios por parte del llamante para cursar los flujos RTP asociados a la comunicación con el llamado. El contenido del INVITE y su encaminamiento hacia el outbound proxy será también el mismo que el indicado en dicho apartado.

8.7.1.2 Progreso de la solicitud

El SBC envía a la red el INVITE recibido para que progrese la solicitud de establecimiento de sesión hasta el terminal llamado.

De la misma manera que se hacía en un asesión IP-IP, cada elemento SIP, al recibir un INVITE, envía inmediatamente hacia el anterior una respuesta provisional 100-Trying, a fin de

indicar la recepción de la petición y detener así sus retransmisiones. Después realiza para la petición INVITE el análisis y tratamiento adecuados y la dirige hacia el siguiente elemento.

La solicitud progresa por la red hacia los elementos encargados de realizar el control de la llamada, que comprueban que el terminal llamado no pertenece a la red NGN y como consecuencia la llamada se remite hacia la PSTN. El elemento de la red encargado de realizar el interfuncionamiento SIP-PUSI necesario es el *Media Gateway Controller* (MGC). Dicho interfuncionamiento se realizará conforme a lo expresado en la recomendación Q.1912.5 de la UIT-T, destacándose en este documento los aspectos más relevantes contenidos en la misma.

En el citado interfuncionamiento se "mapeará" la petición INVITE al mensaje IAM de la PUSI. En la tabla 8.8.1.2.1 se resume el citado "mapeo" (para más detalle ver UIT-T Q 1912.5).

INVITE	**IAM**
userinfo del Request-URI (sip: URI con user=phone)	Número de la Parte llamada
	Categoría de la Parte llamante. Valor por defecto = Abonado regular
Cuerpo SDP	Medio de Transmisión Requerido. Derivado del cuerpo SDP (ver UIT-T Q1912.5)
	Información de Servicio de Usuario. Derivado del cuerpo SDP (ver UIT-T Q1912.5)
P-Asserted-Identity	Número de la Parte Llamante. Si está presente la cabecera P-Asserted-Identity. Si no está presente, la red puede proporcionar un número llamante por defecto.
Privacy.	Indicador de presentación restringida (nº llamante). Ausencia de Privacy= permitida; *none*= permitida; *header, user, id*= restringida
From.	Número Genérico (si éste se soporta en PUSI). La red puede omitirlo si no se envía el Número de la Parte llamante en PUSI.

8.7.1.3 Aviso al llamado

En el procedimiento de aviso al llamado la PSTN envía hacia atrás en PUSI el mensaje de dirección completa (ACM) o el mensaje de progresión de la llamada (CPG). Por tanto el MGC deberá realizar el correspondiente "mapeo" de señalización reflejado en la Q. 1912.5 UIT-T. En los siguientes cuadros se resume éste.

ACM	Mensaje SIP
Parámetro Indicadores de Llamada hacia atrás	
Estado “libre”	180 Ringing con SDP
Estado diferente de “libre”	183 session Progress con SDP

CPG	Mensaje SIP
Parámetro Información de evento	
Evento “aviso”	180 Ringing con SDP
Evento distinto de “aviso”	183 session Progress con SDP

EL terminal llamante al recibir las respuestas 180 ó 183 con SDP debe realizar la apertura de flujo RTP (ver apartado 8.8). En cualquier caso si recibiera una respuesta 180 sin SDP debería suministrar localmente el tono de llamada, mientras que si recibiera una respuesta 183 sin SDP no debería suministrarlo.

8.7.1.4 Respuesta del llamado

Se produce cuando el llamado descuelga. La PSTN envía hacia atrás el mensaje PUSI de Conexión (CON) o de respuesta (ANM). En ambos casos el MGC “mapea” el mensaje a un 200 OK en el lado SIP.

El terminal llamante no debe abrir flujo RTP al recibir la respuesta 200 OK puesto que ya fue abierto con la respuesta provisional 180 ó 183 (salvo que se hubieran recibido sin SDP, en cuyo caso sí debe hacerlo).

8.7.1.5 Liberación de una sesión

La liberación de la sesión se produce bien porque se genera un mensaje BYE o CANCEL desde el lado SIP (lado llamante) o bien porque se genera un un mensaje de liberación (REL) desde el lado PSTN (lado llamado).

En el primer caso si en los mensajes BYE o CANCEL se incluye el campo cabecera *Reason* con causa valor Q.850, ésta se hará corresponder con el campo valor de causa PUSI en el mensaje REL. En el siguiente cuadro se muestra la codificación del valor de causa en el mensaje REL, si ésta no está disponible en el campo cabecera *Reason*.

Mensaje SIP	REL (Indicadores de Causa)
BYE	Valor de causa 16 (liberación normal)
CANCEL	Valor de causa 31 (normal, no especificado)

En el segundo caso, al recibirse de la PSTN un mensaje REL, el MGC devuelve un mensaje RLC y envía hacia el lado SIP un mensaje BYE.

8.7.1.6 Sesiones infructuosas

Cuando se recibe un mensaje REL de la PSTN antes de que se reciban los mensajes ANM o CON, el MGC enviará hacia el lado SIP el correspondiente código de estado SIP en la respuesta final. En el siguiente cuadro se muestra la correspondencia entre el valor de causa PUSI y el código de estado SIP. En el caso particular de respuestas 5XY se podrá añadir opcionalmente la cabecera *Reason* con el valor de causa Q.850 correspondiente.

←Mensaje SIP	**← REL** **Parámetro Indicadores de Causa**
404 No encontrado	Valor de causa N.º 1 ["*número no atribuido (no asignado)*"]
500 Error interno del servidor	Valor de causa N.º 2 ("*no hay ruta hacia la red*")
500 Error interno del servidor	Valor de causa N.º 3 ("*no hay ruta hacia el destino*")
500 Error interno del servidor	Valor de causa N.º 4 ("*enviar tono especial de información*")
404 No encontrado	Valor de causa N.º 5 ("*prefijo interurbano marcado erróneamente*")
500 Error interno del servidor (únicamente SIP-I)	Valor de causa N.º 8 ("*Precedencia*")
500 Error interno del servidor (únicamente SIP-I)	Valor de causa N.º 9 ("*Precedencia-circuito reservado para reutilización*")
486 Ocupado aquí	Valor de causa N.º 17 ("*usuario ocupado*")
480 Temporalmente no disponible	Valor de causa N.º 18 ("*no hay respuesta del usuario*")
480 Temporalmente no disponible	Valor de causa N.º 19 (no hay respuesta del usuario "*usuario avisado*")
480 Temporalmente no disponible	Valor de causa N.º 20 ("*abonado ausente*")
480 Temporalmente no disponible	Valor de causa N.º 21 ("*llamada rechazada*")
410 Baja	Valor de causa N.º 22 ("*número cambiado*")
No hay correspondencia	Valor de causa N.º 23 ("*redireccionamiento a nuevo destino*")

←Mensaje SIP	← REL Parámetro Indicadores de Causa
480 Temporalmente no disponible	Valor de causa N.º 25 ("*error de encaminamiento de central*")
502 Pasarela errónea	Valor de causa N.º 27 ("*destino fuera de servicio*")
484 Dirección incompleta	Valor de causa N.º 28 ["*formato de número no válido (dirección incompleta*")]
500 Error interno del servidor	Valor de causa N.º 29 ("*facilidad rechazada*")
480 Temporalmente no disponible	Valor de causa N.º 31 ("*normal, no especificado*") (Clase por defecto)
486 Ocupado aquí, si el indicador de diagnóstico incluye el indicador CCBS = "*CCBS posible*") cualquier otro caso, 480 Temporalmente no disponible	Valor de causa de la clase 010 (recurso indisponible, Valor de causa N.º 34)
500 Error interno del servidor	Valor de causa de la clase 010 (recurso no disponible, Valor de causa N.º 38-47) (47 es la clase por defecto)
500 Error interno del servidor	Valor de causa N.º 50 ("*facilidad solicitada no abonada*")
500 Error interno del servidor (únicamente SIP-I)	Valor de causa N.º 55 ("*prohibición de llamadas entrantes dentro de un grupo cerrado de usuarios*")
500 Error interno del servidor	Causa valor N.º 57 ("*capacidad portadora no autorizada*")
500 Error interno del servidor	Causa valor N.º 58 ("*capacidad portadora no disponible actualmente*")
500 Error interno del servidor	Valor de causa N.º 63 ("*servicio u opción no disponible, no especificado*") (clase por defecto)
500 Error interno del servidor	Valor de causa de la clase 100 (servicio u opción no implementado, Valor de causa N.º 65-79) (79 es la clase por defecto)
500 Error interno del servidor (únicamente SIP-I)	Valor de causa N.º 87 ("*el usuario no es miembro del grupo cerrado de usuarios*")
500 Error interno del servidor	Valor de causa N.º 88 ("*destino incompatible*")
500 Error interno del servidor (únicamente SIP-I)	Valor de causa N.º 90 ("*grupo cerrado de usuarios inexistente*")
404 No encontrado	Valor de causa N.º 91 ("*selección de red de tránsito no válida*")

←Mensaje SIP	← REL Parámetro Indicadores de Causa
500 Error interno del servidor	Valor de causa N.º 95 ("*mensaje no válido, no especificado*") (clase por defecto)
500 Error interno del servidor	Valor de causa N.º 97 ("*tipo de mensaje inexistente o no implementado*")
500 Error interno del servidor	Valor de causa N.º 99 ("*elemento/parámetro de información inexistente o no implementado*")
480 Temporalmente no disponible	Valor de causa N.º 102 ("*recuperación tras la expiración del plazo del temporización*")
500 Error interno del servidor	Valor de causa N.º 103 ("*parámetro inexistente o no implementado, transferido*")
500 Error interno del servidor	Valor de causa N.º 110 ("*mensaje con parámetro no reconocido descartado*")
500 Error interno del servidor	Valor de causa N.º 111 ("*error de protocolo, no especificado*") (clase por defecto)
480 Temporalmente no disponible	Valor de causa N.º 127 ("*interfuncionamiento, no especificado*") (clase por defecto)

Cuando se cancela una sesión antes de la respuesta 200 OK, el llamante libera con un CANCEL que se mapeará en PUSI a un REL, con las consideraciones efectuadas para el CANCEL en el punto 8.7.1.5.

8.7.2 Sesión PSTN-IP

En este apartado se muestra el procedimiento correspondiente a una llamada telefónica con origen en un terminal de la PSTN y cuyo destino es un terminal SIP perteneciente a la NGN. En este escenario es necesario llevar a cabo el interfuncionamiento PUSI-SIP definido en la recomendación Q.1912.5 de la UIT-T.

La figura 8.7.2.1 representa las distintas fases de la llamada y que se describen en los siguientes apartados.

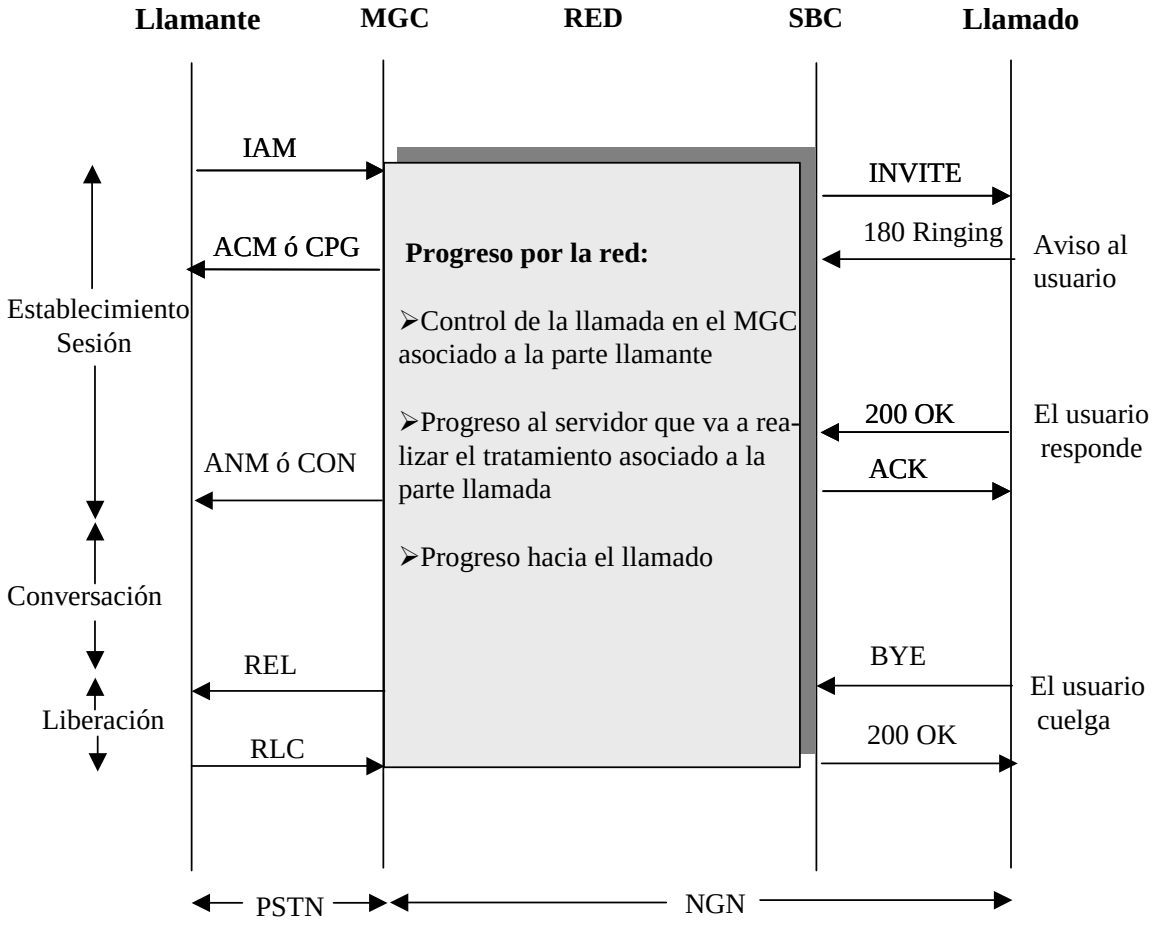


Figura 8.7.2.1

8.7.2.1 Solicitud de establecimiento de sesión

En este escenario la sesión se inicia en la PSTN, progresando la solicitud a través de ésta mediante el envío del mensaje IAM de la PUSI. El MGC al recibir dicho mensaje realiza el "mapeo" de éste a un INVITE que generalmente incluirá un cuerpo de mensaje tipo SDP (descripción de sesión), indicando la oferta de medios por parte del llamante para cursar los flujos RTP asociados a la comunicación con el llamado.

El citado "mapeo" se refleja en la tabla 8.7.2.1.1 (para más detalle ver UIT-T Q 1912.5).

IAM	INVITE
Número de la Parte llamada	Request-URI. Se obtiene el addr-spec (sip: URI con user=phone)

	To. Se obtiene el addr-spec (sip: URI con user=phone)
Categoría de la Parte llamante. Valor por defecto = Abonado regular	No proporciona información el mensaje INVITE
Número de la Parte Llamante	P-Asserted-Identity
	From. Si no se recibe el parámetro número genérico
Indicador de presentación restringida (nº llamante).	Ausencia de Privacy= permitida; Privacy con valores *none*= permitida; *header, user, id*= restringida
Número Genérico (si éste se soporta en PUSI)	From.
Medio de Transmisión Requerido e Información de Servicio de Usuario	Cuerpo SDP derivado de ambos parámetros (ver UIT-T Q1912.5).

8.7.2.2 Progreso de la solicitud

El INVITE progresa por los elementos de la red NGN hasta alcanzar el SBC asociado al terminal llamado. El avance hacia el usuario llamado sólo es posible si el usuario llamado está registrado en la red.

El contenido del INVITE será el mismo que el definido en el apartado 8.6.1.1 para la sesión IP-IP.

En caso de que el llamado tenga registradas varias direcciones de contacto, el servidor que obtenga sus datos de registro, realizará un envío múltiple de la solicitud INVITE hacia todos ellos (forking).

8.7.2.3 Aviso al llamado

La solicitud de establecimiento llega al terminal llamado a través de su correspondiente SBC. Si todo es correcto, el terminal avisa al usuario proporcionando una corriente de llamada, localmente o tratando la cabecera “Alert-Info” si estuviera presente. Entonces envía hacia atrás una respuesta provisional: 180 Ringing, que podría incluir opcionalmente:

- Un parámetro tag en la cabecera To, a fin de establecer el diálogo entre terminales llamante y llamado, aunque en estado “anticipado” (ver detalles en 8.6.1.4.1).

Cuando el MGC recibe esta respuesta:

- Si incluye el parámetro tag en la cabecera To, crea el correspondiente diálogo en estado “anticipado” (ver 8.6.1.4.1).

- Envía en PUSI hacia la red PSTN un mensaje ACM ó CPG. El ACM llevará codificado el parámetro indicadores de llamada hacia atrás con estado "libre" y el CPG llevará codificado el parámetro información de evento con el evento "aviso".

En caso de haberse realizado un envío múltiple de la solicitud de sesión (forking), el MGC puede recibir varias respuestas 180 Ringing procedentes de distintos puntos. En caso de producirse dicha situación, el MGC mapeará en PUSI al mensaje ACM ó CPG únicamente la primera respuesta.

8.7.2.4 Respuesta del llamado

Se produce cuando el llamado descuelga.

El terminal envía una respuesta 200 OK, que obligatoriamente llevará el parámetro tag en la cabecera To, quedando establecido de este modo el diálogo entre llamante y llamado, ya en estado "confirmado". En el apartado 8.6.1.4.1 se describe la creación del diálogo.

Además la 200 OK incluye obligatoriamente un cuerpo de mensaje SDP con la respuesta a la oferta recibida en el INVITE, o, en caso de recepción de INVITE sin SDP, la oferta por parte del llamado en cuanto a medios disponibles para la sesión.

Cuando se produce el envío y recepción de la respuesta 200 OK a un INVITE portador de una oferta de sesión, se considera realizada la negociación y apertura de medios, y por tanto establecida la sesión.

El MGC considera completa la transacción correspondiente al INVITE inicial tras un intervalo de tiempo establecido a partir de la primera respuesta 200 OK recibida. Finalizado el mismo, elimina cualquier diálogo relacionado con este INVITE que no esté confirmado (es decir para el que no se haya recibido una respuesta final). Asimismo, en caso de *forking* envía BYE (que no se mapea hacia PSTN) tras el ACK para liberar cualquier sesión correspondiente a un diálogo confirmado con respuesta 200 OK recibida después de la primera. De este modo sólo se establecerá la sesión entre el terminal PSTN y el primer terminal IP que responde satisfactoriamente.

En contenido de la respuesta 200 OK es el mismo que el definido en el apartado 8.7.1.4.

El MGC "mapea" la respuesta 200 OK hacia la PSTN en el mensaje PUSI de Conexión (CON) o de respuesta (ANM).

8.7.2.5 Liberación de una sesión

La liberación de la sesión se produce bien porque se genera un mensaje BYE o CANCEL desde el lado SIP (lado llamado) o bien porque se genera un un mensaje de liberación (REL) desde el lado PSTN (lado llamante).

En el primer caso si en los mensajes BYE o CANCEL se incluye el campo cabecera *Reason* con causa valor Q.850, ésta se hará corresponder con el campo valor de causa PUSI en el mensaje REL. En el siguiente cuadro se muestra la codificación del valor de causa en el mensaje REL, si ésta no está disponible en el campo cabecera *Reason*.

Mensaje SIP	REL (Indicadores de Causa)
BYE	Valor de causa 16 (liberación normal)
CANCEL	Valor de causa 31 (normal, no especificado)

En el segundo caso, al recibirse de la PSTN un mensaje REL, el MGC devuelve un mensaje RLC y envía hacia el lado SIP un mensaje BYE.

8.7.2.6 Sesiones infructuosas

En los intentos de establecimiento de sesiones en los que se genera en el lado SIP una respuesta 4XY, 5XY y 6XY al mensaje INVITE el MGC envía hacia la PSTN en PUSI el mensaje REL. La correspondencia entre las posibles respuestas y el valor de la causa de liberación PUSI se refleja en el siguiente cuadro, salvo que esté presente la cabecera Reason en las respuestas SIP, en cuyo caso se hará corresponder el valor de causa del mensaje REL con el valor de causa de la cabecera Reason.

←REL (Valor de Causa)	←Mensaje SIP 4XX/5XX/6XX	Observaciones
127 Interfuncionamiento	400 Solicitud errónea	
127 Interfuncionamiento	401 No autorizado	(Nota 1)
127 Interfuncionamiento	402 Pago requerido	
127 Interfuncionamiento	403 Prohibido	
1 Número no asignado	404 No encontrado	
127 Interfuncionamiento	405 Método no permitido	
127 Interfuncionamiento	406 No aceptable	
127 Interfuncionamiento	407 Autenticación del apoderado requerida	(Nota 1)
127 Interfuncionamiento	408 Solicitud de expiración del temporizador	
22 Número cambiado (sin diagnóstico)	410 Baja	
127 Interfuncionamiento	413 Petición de entidad demasiado larga	(Nota 1)
127 Interfuncionamiento	414 Request-uri demasiado largo	(Nota 1)
127 Interfuncionamiento	415 Tipo de medios no soportado	(Nota 1)
127 Interfuncionamiento	416 Esquema URI no soportado	(Nota 1)
127 Interfuncionamiento	420 Extensión errónea	(Nota 1)
127 Interfuncionamiento	421 Extensión requerida	(Nota 1)

←REL (Valor de Causa)	←Mensaje SIP 4XX/5XX/6XX	Observaciones
127 Interfuncionamiento	423 Intervalo demasiado breve	
20 Abonado ausente	480 Temporalmente no disponible	
127 Interfuncionamiento	481 La llamada/transacción no existe	
127 Interfuncionamiento	482 Bucle detectado	
127 Interfuncionamiento	483 Demasiados saltos	
28 Formato de número no válido	484 Dirección incompleta	(Nota 1)
127 Interfuncionamiento	485 Ambiguo	
17 Usuario ocupado	486 Ocupado aquí	
127 Interfuncionamiento o no hay correspondencia (Nota 3)	487 Petición terminada	(Nota 2)
127 Interfuncionamiento	488 No aceptable aquí	
No hay correspondencia	491 Petición pendiente	(Nota 2)
127 Interfuncionamiento	493 Indescifrable	
127 Interfuncionamiento	500 Error interno del servidor	
127 Interfuncionamiento	501 No implementado	
127 Interfuncionamiento	502 Pasarela errónea	
127 Interfuncionamiento	503 Servicio no disponible	(Nota 1)
127 Interfuncionamiento	504 Expiración del temporizador del servidor	
127 Interfuncionamiento	505 Versión no soportada	(Nota 1)
127 Interfuncionamiento	513 Mensaje demasiado amplio	(Nota 1)
127 Interfuncionamiento	580 Fallo de condición previa	(Nota 1)
17 Usuario ocupado	600 Ocupado en todas partes	
21 Llamada rechazada	603 Declive	
1 Número no asignado	604 No existe	
127 Interfuncionamiento	606 No aceptable	

NOTA 1 – Esta respuesta puede tratarse en su integridad en el lado SIP. En tal caso, no interviene en el interfuncionamiento

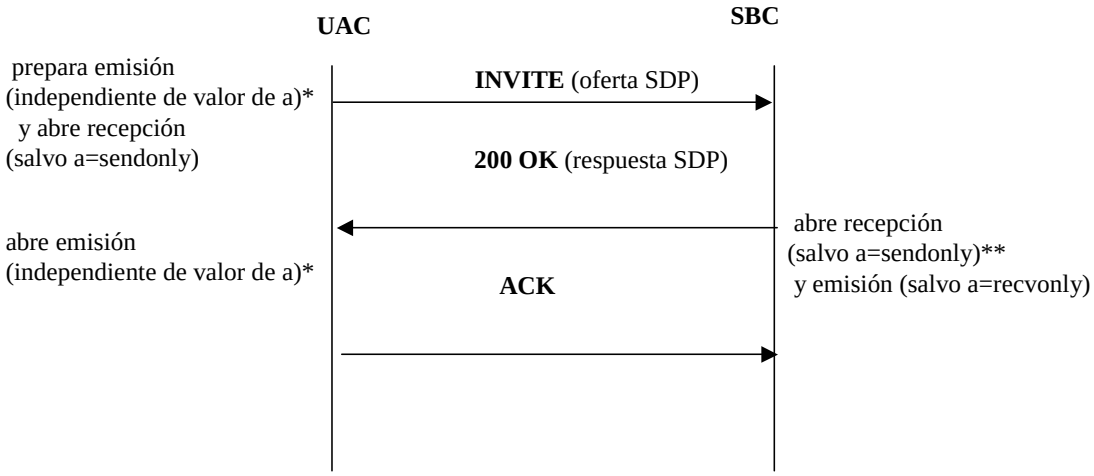
NOTA 2 – Esta respuesta no termina un diálogo SIP, sólo una transacción específica dentro de él.

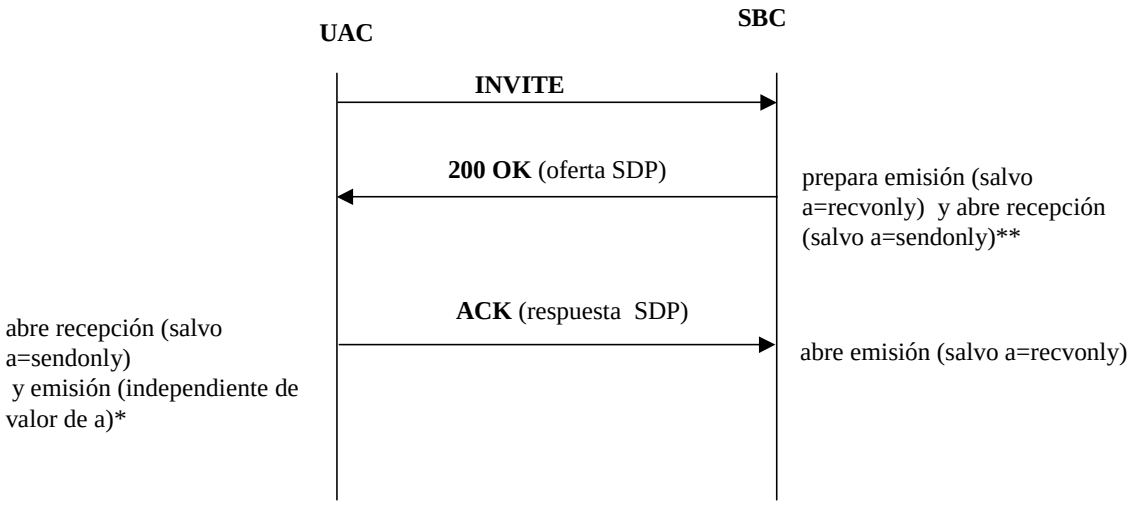
NOTA 3 – No hay correspondencia si el MGC ya ha enviado una petición CANCEL para el mensaje INVITE.

En el caso de que se libere desde la PSTN antes de la respuesta del llamado, el MGC enviará un CANCEL que opcionalmente podría llevar la cabecera Reason con causa valor Q.850.

8.8 CRITERIOS DE APERTURA DE FLUJOS RTP

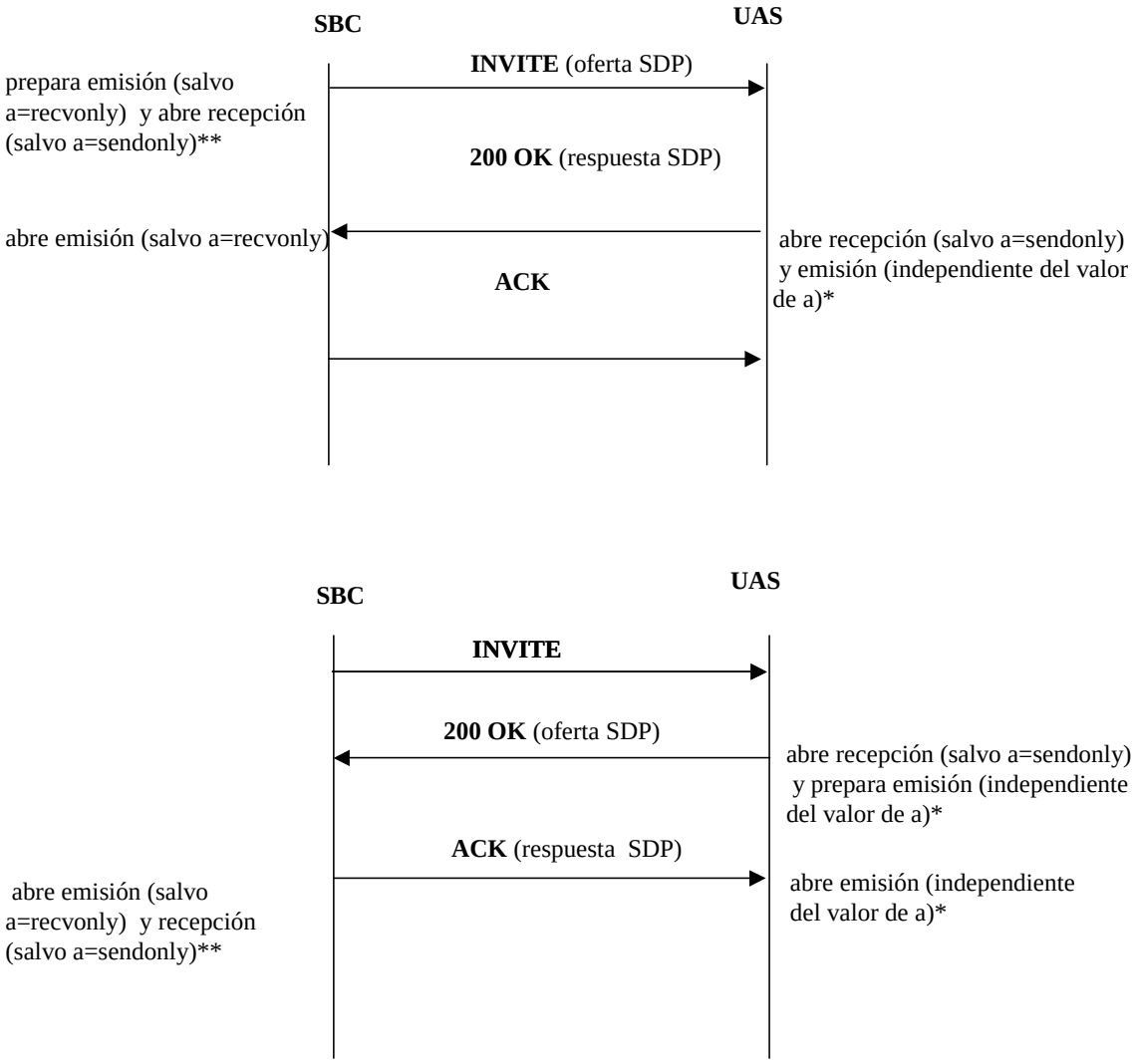
En las figura 8.9.1 y 8.9.2 se resumen los criterios de apertura de flujo RTP en cada lado de una sesión IP-IP cuando el INVITE lleva cuerpo SDP y cuando el INVITE no lo lleva.





(*) Permite la asignación de un puerto en el router accesible desde el SBC
(**) Si a=sendonly abre la recepción con el UAC para determinar su puerto RTP pero cierra la recepción hacia el UAS.

Figura 8.9.1. Flujo RTP entre UAC y SBC en sesión IP-IP



(*) Permite la asignación de un puerto en el router accesible desde el SBC
(**) Si a=sendonly abre la recepción con el UAS para determinar su puerto RTP pero cierra la recepción hacia el UAC.

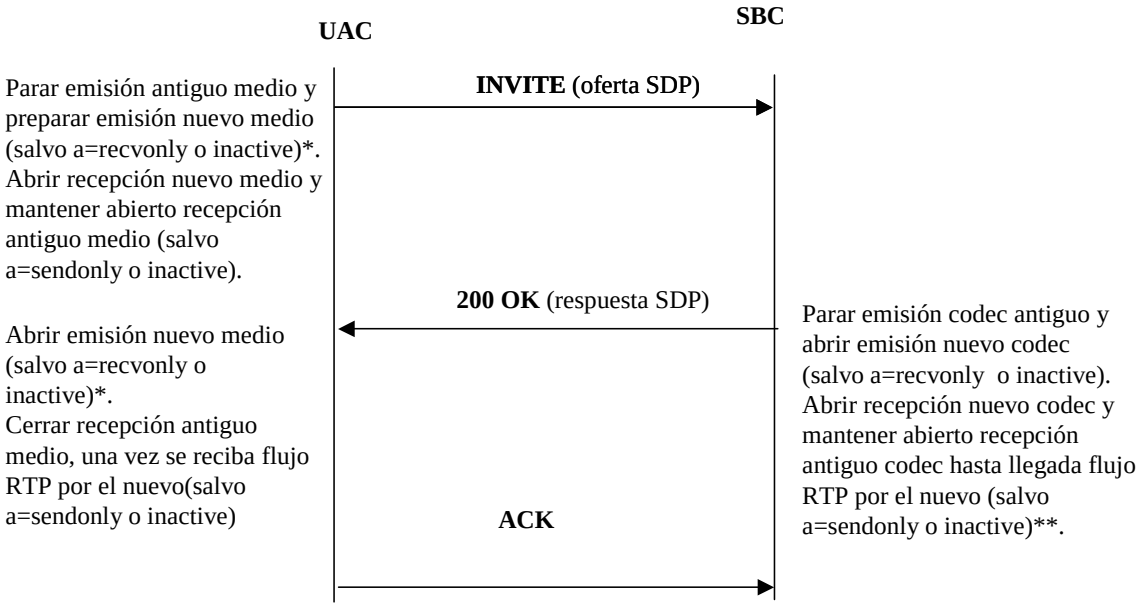
Figura 8.9.2. Flujo RTP entre SBC y UAS en sesión IP-IP

En la figura 8.9.3 se refleja el criterio de apertura de flujo en un diálogo anticipado con respuesta provisional tipo 18xy. Este tipo de escenario se podrá presentar en sesiones con origen IP y destino la PSTN o en sesiones IP en las que la red proporciona locuciones informativas sin señal de descolgado.

(*) Permite la asignación de un puerto en el router accesible desde el SBC
(**) Si a=sendonly abre la recepción con el UAS para determinar su puerto RTP pero cierra la recepción hacia la red.

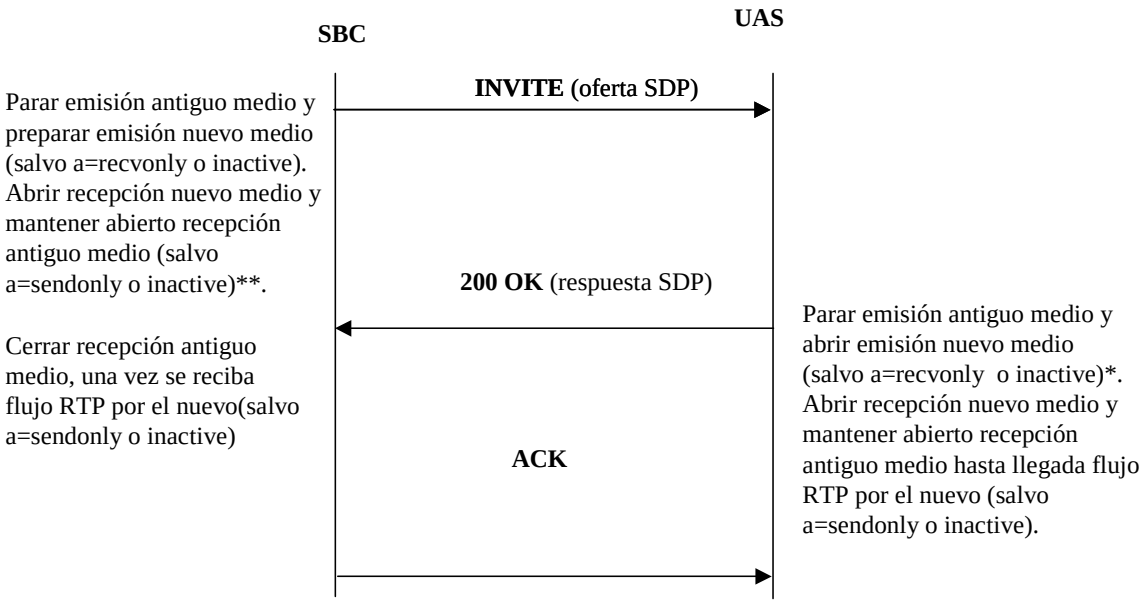
Figura 8.9.3. Apertura de flujo RTP en una sesión IP-PSTN.

En las figuras 8.9.4 y 8.9.5 se refleja el criterio de apertura de flujo RTP ante un cambio de medio en una sesión IP-IP establecida.



(*) Si se utiliza un nuevo puerto abre la emisión independiente del valor de a.
(**) Si se utiliza un nuevo puerto aunque a=sendonly abre la recepción con el UAC para determinar su puerto RTP pero cierra la recepción hacia el UAS.

Figura 8.9.4. Apertura de flujo en cambio de medio entre UAC y SBC



(*) Si se utiliza un nuevo puerto abre la emisión independiente del valor de a.
(**) Si se utiliza un nuevo puerto aunque a=sendonly abre la recepción con el UAS para determinar su puerto RTP pero cierra la recepción hacia el UAC.

Figura 8.9.5. Apertura de flujo en cambio de medio entre SBC y UAS

9. PROCEDIMIENTOS DE TELECONFIGURACIÓN DE TERMINALES

9.1 CARGA DE CONFIGURACIÓN

Para poder integrar la provisión de abonados y la configuración del terminal en la plataforma es necesario que el terminal soporte:

- Acceso ficheros TFTP/FTP para configurar los fichero del terminal
- Ficheros de configuración del terminal en formato anidado o formato sistema/individual
- Soporte de provision de los siguientes tipos de campos en los ficheros de configuración mostrados en la siguiente tabla

	Parámetros	**Formato**
Datos de Red	IP Addr	Dirección IP
	IPSubMask	Dirección IP
	IPDefGW	Dirección IP
	DNSserverIP1 (primario)	Dirección IP
	DNSserverIP2 (secundario)	Dirección IP
	NTPserverIP	Dirección IP o dominio
	TimeZone	Formato Time Zone (GMT +x)
	DayLight	Booleano (0= no habilitado, 1=no habilitado)
	IPType	Entero (0=estático, 1=DHCP)
Autoprovisión	EnableFTP	Booleano (0= no habilitado, 1= habilitado)
	FTPserver	Dirección IP
	FTPLogin	Cadena de caracteres
	FTPPassword	Cadena de caracteres
	EnableTFTP	Booleano (0= no habilitado, 1= habilitado)
	TFTPserver	Dirección IP
Datos SIP	SIPPort	Entero
	RegistrarServerIP	Dominio
	RegistrarPort	Entero
	OutboundProxyIP	Dirección IP o nombre de host
	OutboundProxyIPPort	Entero
	MInSessionTimer	Entero
	SessionTimer	Entero
	MaxSessionTimer	Entero
	SessionRefresher	Entero (0=ninguno, 1=UAC, 2=UAS)
	UDP/TCP	Entero (0=UDP, 1=TCP)
Usuario SIP	ACCSIPuser01 (identidad pública)	Cadena de caracteres
	ACCAuthUN01 (identidad privada)	Cadena de caracteres
	ACCAuthPW01 (contraseña)	Cadena de caracteres
	ACCDisplay01 (nombre de presentación)	Cadena de caracteres
	Número de Teléfono	E.164
Otros Datos	DTMF	Entero (0=fuera banda, 1=en banda, 2=SIP)

Una vez cambiado el archivo de configuración de un terminal para forzar que se cargue el fichero actualizado es necesario hacer un *reboot* normalmente.

9.2 SINCRONIZACIÓN DE FECHA Y HORA EN TERMINALES

La sincronización horaria de los terminales se efectuará mediante protocolo SNTP (Simple Network Time Protocol, conforme a la RFC 2030) desde un servidor NTP encargado de proporcionar dicho sincronismo. El modelo que empleará el citado servidor será el de *pooling* de clientes. El servidor NTP mandará información de sincronismo sólo bajo demanda de los clientes NTP.

El terminal deberá tener configurado este servidor.

10. GLOSARIO DE TÉRMINOS

ACM	Address Complete Message (Mensaje de dirección completa)
ADSL	Asymmetric Digital Subscribe Line
ANM	Answer Message (Mensaje de respuesta)
AVP	Audio Video Profile
CLID	Calling Line IDentification
CLIR	Calling Line Identification Restriction
CON	Connect Message (Mensaje de Conexión)
CPG	Call Progress (Mensaje de progreso)
DNS	Domain Name System
DTMF	Dual Tone Multifrecuency
EPA	Agente de Publicación de Eventos
ESC	Compositor del Estado de Eventos
FQDN	Fully Qualified Domain Name
FTP	File Transfer Protocol
GMT	Greenwich Mean Time
HTTP	Hypertext Transfer Protocol
IAM	Initial Address Message (Mensaje Inicial de Dirección)
IANA	Internet Assigned Numbers Authority
IETF	Internet Engineering Task force

IP	Internet Protocol
ISP	Internet Service Provider
ITU-T	Unión Internacional de Telecomunicaciones (Sector de Normalización de las Telecomunicaciones)
MGC	Media Gateway Controller
MIME	Multipart Internet Mail Extensions
NAT	Network Address Translator
NGN	Next Generation Network
NTP	Network Time Protocol
PA	Presence Agent
PCM	Pulse Code Modulation
PIDF	Presence Information Data Format
PSTN	Public Switched Telephone Network
PUSI	Parte de Usuario de Servicios Integrados
REL	Release Message (Mensaje de liberación)
RFC	Request For Comments
RLC	Release Complete (Liberación Completa)
RTC	Red Telefónica Conmutada
RTCP	RTP Control Protocol
RTP	Real-Time Transport Protocol
SBC	Session Border Controller
SCTP	Stream Control Transmission Protocol
SDP	Session Description Protocol
SIP	Session Initiation Protocol
SIPs	Secure Session Initiation Protocol
SIP-I	SIP con PUSI encapsulada
S/MIME	Securing Multipart Internet Mail Extensions
TCP	Transmission Control Protocol
TLS	Transpot Layer Security
TFTP	Trivial File Transfer Protocol
UA	User Agent (Agente de Usuario)
UAC	User Agent Client (Agente de Usuario Cliente)

UAS	User Agent Server (Agente de Usuario Servidor)
UDP	User Datagram Protocol
URI	Uniform Resource Identifier
URL	Uniform Resource Locator