ESCUELA POLITECNICA DEL EJERCITO

FACULTAD DE INGENIERIA ELECTRONICA

PROYECTO DE GRADO PARA LA OBTENCION DEL TITULO EN INGENIERIA ELECTRONICA

TELEFONIA IP SOBRE REDES INALAMBRICAS WI-FI

CARLOS ALBERTO RAMIREZ TAFUR

QUITO-ECUADOR

2008

CERTIFICACION

Certificamos que el presente Proyecto de Grado “Telefonía IP sobre Redes Inalámbricas WI – FI” fue desarrollado en su totalidad por el señor Carlos Alberto Ramírez Tafur, bajo nuestra dirección, como requerimiento parcial a la obtención del título de INGENIERO ELECTRONICO.

Sangolquí ____ de _____ del 2008

Ing. Román Lara
DIRECTOR DEL PROYECTO

Ing. Fabián Sáenz
CODIRECTOR DEL PROYECTO

AGRADECIMIENTO

Agradezco a Dios por haberme privilegiado con el don de la vida, fortaleciéndome y llenándome día a dia mi espíritu con sabiduría, amor valentía y honestidad que han sido pilares fundamentales en el cumplimiento de mis objetivos.

A mis padres, amigos legales e inigualables, mi más profundo y sincero agradecimiento, ya que con su amor, sacrificio y dedicación me han educado para llegar a ser hombre de bien, así como también por todo el apoyo incondicional que me han brindado en el transcurrir de mi vida.

De manera muy especial mi agradecimiento y reconocimiento profundo a los Ingenieros: Román Lara y Fabián Sáenz, Director y Codirector de mi tesis, quienes con su alto espíritu y forjadores de jóvenes supieron dirigirme en el desarrollo y elaboración de este proyecto.

A la Escuela Superior Politécnica del Ejército, Institución de excelencia, mi agradecimiento por haberme permitido estudiar y ser parte de ella para ser profesional forjador de un nuevo País.

A mis profesores, que me brindaron y compartieron todos sus conocimientos y experiencias de manera sincera y desinteresada a lo largo de mis estudios universitarios.

A todos mis amigos y familiares que en todos los momentos supieron darme su apoyo y comprensión generosamente.

CARLOS ALBERTO RAMIREZ TAFUR

DEDICATORIA

Dedico este Proyecto a Dios Padre Creador del Universo, quien me a dado la oportunidad de ver la luz cada día y llenar de bendiciones mi vida.

En mi vida siempre he tenido el compartimiento de mi Padre José Alberto Ramírez quien ha sido mi guía y protector, para él mi esfuerzo realizado.

Para mi Madre Gladis Tafur Yépez, el amor de mi vida, ofrendo a ella esta labor, sin su ser nada sería lo que ahora soy.

A mi hermano Andrés, quien con su comprensión y amor hizo posible la culminación de esta gran meta.

INDICE

R

S

T

U

V

W

Z

CONTENIDO DEL PROYECTO

CAPÍTULO I:

TECNOLOGIA INALAMBRICA 802.11

1. INTRODUCCIÓN A 802.11

La conectividad inalámbrica es preferiblemente la opción más aceptable, al menos que pretendamos pasar cables por toda nuestra oficina o casa. Esta tendencia se refleja en el tremendo incremento que han sufrido las ventas de equipos de red inalámbricos. El negocio está en auge para los fabricantes de chips y componentes *WLAN*. En un estudio realizado por *Linux Magazine* el escritor *JORG LUTHER* predice que: "Solo en Europa se espera que el beneficio alcance la mágica cifra del billón de dólares en 2007. Esta tendencia también es buena para los consumidores, debido a que el incremento de cantidades significa una rápida caída en los precios de equipos *WLAN."*

Las redes inalámbricas se reparten en dos clases principales subdivididas por la banda de frecuencia. Las primeras tecnologías usaban la banda de 2.4 GHz mientras que las más modernas usan la de 5 GHz . La primera incluye los estándares del Instituto de Ingenieros Eléctricos y Electrónicos 802.11b y es compatible con su sucesor 802.11g.

Por otro lado, tanto 802.11a como 802.11h, que operan en la banda de 5 GHZ, consiguen un rendimiento nominal de 54 Mbps. 802.11h, referida en Estados Unidos como "de compatibilidad en Europa", es la variante Europea del estándar Americano. Sus dos

características más importantes son la selección dinámica y la potencia de transmisión variable, obligatorias para el mercado Europeo según el Instituto Europeo de Estándares de Comunicación (ETSI) con el fin de asegurar que los sistemas tengan una capacidad de transmisión razonable. IEEE 802.11c, especifica métodos para la conmutación inalámbrica, o lo que es lo mismo, métodos para conectar diferentes tipos de redes mediante redes inalámbricas. El 802.11d normalmente se le conoce como el "Método Mundial" y se refiere a las diferencias regionales en tecnologías como a cuantos y cuales son los canales disponibles para usarse en las distintas regiones del mundo. Como usuario sólo necesitamos especificar el país en el que queremos usar la tarjeta *WLAN* y el controlador se ocupa del resto. El protocolo IEEE 802.11e define la calidad del servicio y las extensiones para el flujo de medios para 802.11a/h y g. El objetivo es ajustar las redes de 54 Mbps para aplicaciones multimedia y de voz sobre IP, o lo que es lo mismo, telefonía a través de redes IP e Internet. La red debe soportar valores de transmisión de datos garantizados para servicios individuales o retrasos de propagación mínimos para que sean útiles con multimedia o voz. El protocolo 802.11f describe como se tratan los estándares de las comunicaciones de clientes de móviles fuera de zona entre puntos de acceso.

1.1.1. Historia de 802.11 *o Wi-Fi*

Debido a la gran cantidad de redes LAN, muchos productos aparecieron y existió la necesidad de que tuviera una consistencia en todas las redes. Como ejemplos se pueden mencionar que las redes que se adherían al SNA *(System Network Architecture)* de IBM no podían comunicarse directamente con otras redes que usaran el DNA *(Digital Network Architcture)* de DEC *(Digital Equipement Corporation)*. Es por eso que la Organización Internacional de Estandarización y la IEEE desarrollaron modelos y estándares que luego fueron adoptados internacionalmente con el fin de que todas las redes locales se pudieran comunicar entre sí.

El proyecto que iniciado por el IEEE *(Institute of Electrical and Electronics Engineers)* en Febrero de 1980, de allí su nombre (802). Este proyecto define estándares

para los componentes físicos de una red y están orientados principalmente a las capas físicas y de enlace de datos (Tarjeta de Red y Cableado) del modelo de referencia OSI.

Aunque los estándares IEEE 802 publicados realmente son anteriores a los ISO, ambos estaban en desarrollo aproximadamente al mismo tiempo y compartían información que concluyó con la creación de dos modelos compatibles.

Las especificaciones 802 definen estándares para:

- ✓ Tarjetas de Red
- ✓ Componentes de área global *WAN*.
- ✓ Componentes utilizados para la transmisión (cable, etc.)

Las especificaciones 802 definen la forma en que las tarjetas de red acceden y transfieren datos sobre el medio físico. Estas incluyen conexión, mantenimiento y desconexión de dispositivos de red.

Tabla. 1.1. Resumen de Foros de Estandarización

Organismo	Tecnología básica	Participación Alcatel	Miembros destacados	Estado
DHWG	PC, Elec. Consumo	Si	*Sony, Microsoft*	Pre-Release HNv1 Guidelines Fase 1 2004 fase 2 2006
HomePlug	PLC	No (hasta 2001)	*DS2, Comcast, Conexant*	Certificado disponible
HomePNA	HomePNA	Si (*)	*CopperGate*	Certificado disponible
HomeRF	HomeRF	No	*Intel* lo abandonó	Superado por *WiFi*
OSGI	Software	Si (*)	*Sun, IBM* (>40 memb)	Re. 3 / Compliance program
PLCForum	PLC	Si (*)	*ENEL, Endesa, DS2*	*Lobby regulation*
UPnP	Software	Si	*Microsoft* (más de 680 miembros)	Certificacion Test Toll
Bluetooth	Bluetooth	Si	*Ericson*	Kit de estándares disponible
Bluetooth	Bluetooth	Si	*Ericson*	Kit de estándares disponible
H2GF	Hiperlan 2	Si	*Thomson, Philips*	Estándar completado
WiFi	IEEE802.11	Si	Las organizaciones más relevantes	Incorporación de nuevas familias 802.11, 1H 2005
Zigbee	IEEE802.15.4	No (prevista)	*Motorola*	Estándar cerrado
WiMAX	IEEE802.16	Si	Las organizaciones más relevantes	Estándar cerrado Test Specs 2H2004
UWB A (MBOA)	IEEE802.15.3	No (prevista)	*Intel, Samsung, TI, Philips, (Motorola)*	Cumplimiento regulatorio Prop IEEE802.15.3, 2H04
HAVi	Sw (IEEE1394)	No	Fabr. TV/Video	V1.1, level 2 UI 1.01 Beta
MHP	Software	Si	ETSI DVB Project	Release MHP 1.1 / Test Suite
Jini	Software	Si (Java Comm.)	*Sun Microsystems*	Estándar básico completo

1.1.2. Arquitectura de redes 802.11

El elemento fundamental de la arquitectura de las redes 802.11 es la celda, la cual se puede definir como el área geográfica en el cual una serie de dispositivos se interconectan entre sí por un medio aéreo.

Figura 1.1. Celda fundamental

En general, esta celda estará compuesta por estaciones y un único punto de acceso. Las estaciones son adaptadores que permiten la conversión de información, generalmente encapsulada bajo el protocolo *Ethernet*, existente en terminales o equipos clientes, y su envío y recepción dentro de la celda. El punto de acceso es el elemento que tiene la capacidad de gestionar todo el tráfico de las estaciones y que puede comunicarse con otras celdas o redes. Es a todos los efectos un *bridge* que comunica a nivel 2 (enlace) los equipos, tanto de su celda de cobertura, como a otras redes a las cuales estuviese conectado. A esta configuración se le denomina Grupo de Servicio Básico BSS ("*Basic Service Set*").

El BSS es, por tanto, una entidad independiente que puede tener su vinculación con otros BSS a través del punto de acceso mediante un Sistema de Distribución (DS,

"*Distribution System*"). El DS puede ser interrogado (comunica el BSS con una red externa), cableado (con otros BSS a través de cable como por ejemplo una red *Ethernet* fija convencional), o también inalámbrico, en cuyo caso se denomina Sistema de distribución inalámbrica ("*Wireless Distribution System"*).

Sobre este concepto básico surge una serie de alternativas:

- ✓ **BSS independiente** (**IBSS,** "*Independent Basic Service Set*"). Es una celda inalámbrica en la cual no hay sistema de distribución y, por tanto, no tiene conexión con otras redes.

- ✓ **Modo Ad-hoc**. Es una variante del IBSS en el cual no hay punto de acceso. Las funciones de coordinación son asumidas de forma aleatoria por una de las estaciones presentes. El tráfico de información se lleva a cabo directamente entre los dos equipos implicados, sin tener que recurrir a una jerarquía superior centralizadora, obteniéndose un aprovechamiento máximo del canal de comunicaciones. La cobertura se determina por la distancia máxima entre dos equipos, la cual suele ser apreciablemente inferior a los modos en que hay un punto de acceso. Es un modo de empleo infrecuente por las connotaciones de aislamiento que conlleva aunque puede ser muy útil cuando el tráfico existente se reparte entre todos los equipos presentes.

Figura. 1.2. Ad - Hoc

- ✓ **Modo infraestructura.** El punto de acceso realiza las funciones de coordinación. Todo el tráfico tiene que atravesarlo, por lo que hay una clara pérdida de eficiencia

cuando dos estaciones dentro de un mismo BSS desean comunicarse entre sí (los paquetes de información son enviados una vez al punto de acceso y otra vez al destino). Es una arquitectura apropiada cuando la mayor parte del tráfico se origina o finaliza en las redes exteriores a las cuales está conectado el punto de acceso. La cobertura alcanza una distancia cercana al doble de la distancia máxima entre punto de acceso y estación. Es el modo que se emplea habitualmente para conectar una red inalámbrica con redes de acceso a Internet (ADSL –*"Asymmetrical Digital Subscriber Line"*- , RDSI –*Red Digital de Servicio Integrados*-,..) y redes locales de empresa.

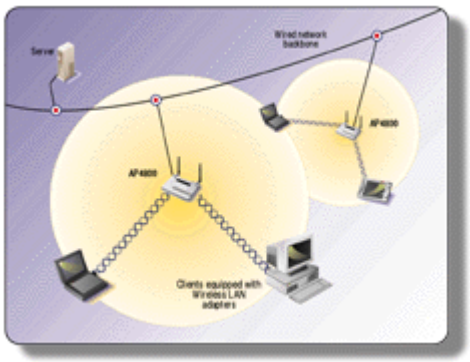

Figura. 1.3. Infraestructura.

- ✓ **BSS extendido** (**ESS,** *"Extended Service Set"*). Es un caso específico del modo infraestructura, representado por un conjunto de BSS asociados mediante un sistema de distribución. Esto permite una serie de prestaciones avanzadas opcionales como el *roaming* entre celdas. Para poder identificar de manera inequívoca a las celdas inalámbricas se les asigna un nombre de red consistente en una cadena con longitud máxima de 32 caracteres denominado "*Service Set Identifier*", SSID. Para poder agregarse a una determinada celda es requisito indispensable que el equipo tenga en su configuración interna el mismo SSID. Si se desea que la estación se conecte a cualquier celda inalámbrica presente, se deberá poner como parámetro "ANY". Inmediatamente el equipo analizará todas las celdas que están presentes y se conectará a una de ellas adoptando su SSID, generalmente con el criterio de la que mayor nivel de señal posea.

Figura. 1.4. BSS Extendido

1.2. Características de los estándares 802.11

La especificación IEEE 802.1X [13] es un estándar de control de acceso desarrollado por el IEEE que permite utilizar diferentes mecanismos de autenticación. Su funcionamiento se basa en el concepto de puerto, visto éste como el punto a través del que se puede acceder a un servicio proporcionado por un dispositivo, que en este caso será el punto de acceso. En principio todos los puertos están desautorizados, excepto el punto de acceso que utiliza para comunicarse con el cliente. Cuando un nuevo usuario entra en su área de cobertura, le pasa al punto de acceso información de autenticación, dependiente del mecanismo utilizado, que éste reenvía al servidor de autenticación. Cuando éste le contesta, si la respuesta es que el cliente puede hacer uso de la red, autoriza un puerto para que lo utilice el cliente. La Figura 1 muestra la estructura general de un sistema IEEE 802.1X.

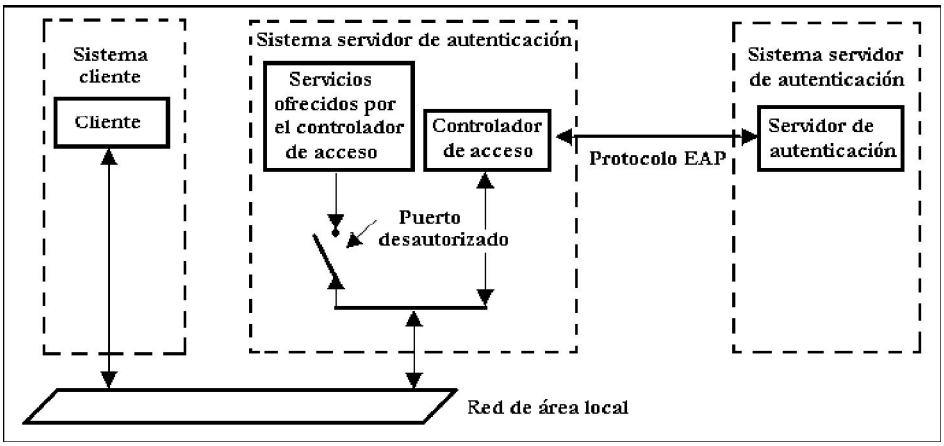

Figura. 1.5. Arquitectura IEEE 802.1X

En esta arquitectura, la información de autenticación se encapsula en el protocolo EAP *(Extensible Authentication Protocol)* [3], un mecanismo genérico de transmisión de datos de autenticación que puede ser materializado en distintos subprotocolos entre los que, por ejemplo, se encuentra EAP-MD5 [22], que basa la autenticación del cliente en el uso de *login y passWord*, o EAP-TLS [1], que se basa en el uso del protocolo TLS [23] y permite autenticación mutua entre los dos extremos. El sistema aquí presentado hará uso de EAP-TLS principalmente por dos motivos: el primero es que, durante la fase de establecimiento de la conexión este protocolo hace uso de certificados X.509 [14] para identificar a las partes, lo cual constituye un mecanismo robusto de autenticación; el segundo es que dicha fase genera una clave compartida por los dos extremos que puede utilizarse para derivar claves para el cifrado de las transmisiones inalámbricas, lo cual es uno de los objetivos de nuestra arquitectura.

Finalmente, los paquetes EAP se transmiten mediante el protocolo EAPOL [12], el cual especifica cómo encapsular los paquetes EAP en una red de área local tanto *Ethernet* como 802.11.

Protocolo de Acceso al medio CSMA/CA y MACA

El algoritmo básico de acceso a este nivel es muy similar al implementado en el estándar IEEE 802.3 y es el llamado CSMA/CA *(Carrier Sense Multiple Access / Collision Advoidance)*. Este algoritmo funciona tal y como se describe a continuación:

1.- Antes de transmitir información, una estación debe testear el medio, o canal inalámbrico, para determinar su estado (libre / ocupado).

2.- Si el medio no esta ocupado por ninguna otra trama la estación ejecuta una espera adicional llamada *espaciado entre tramas* (IFS).

3.- Si durante este intervalo temporal, o bien ya desde el principio, el medio se determina ocupado, entonces la estación debe esperar hasta el final de la transacción actual antes de realizar cualquier acción.

4.- Una vez que finaliza esta espera debido a la ocupación del medio, la estación ejecuta el llamado algoritmo de *Backoff*, según el cual se determina una espera adicional y aleatoria escogida uniformemente en un intervalo llamado ventana de contienda (CW). El algoritmo de *Backoff* nos da un número aleatorio y entero de ranuras temporales *(slot time)* y su función es la de reducir la probabilidad de colisión que es máxima, cuando varias estaciones están esperando que el medio quede libre para transmitir.

5.- Mientras se ejecuta la espera marcada por el algoritmo de *Backoff* se continúa escuchando, de tal manera que si el medio se determina libre durante un tiempo de al menos IFS esta espera va avanzando temporalmente hasta que la estación consume todas las ranura temporales asignadas. En cambio, si el medio no permanece libre durante un tiempo igual o superior a IFS el algoritmo de *Backoff* queda suspendido hasta que se cumpla esta condición.

Cada retransmisión provocará que el valor de CW, que se encontrará entre CWmin y CWmax se duplique hasta llegar al valor máximo. Por otra parte, el valor del *slot time* es 20µseg.

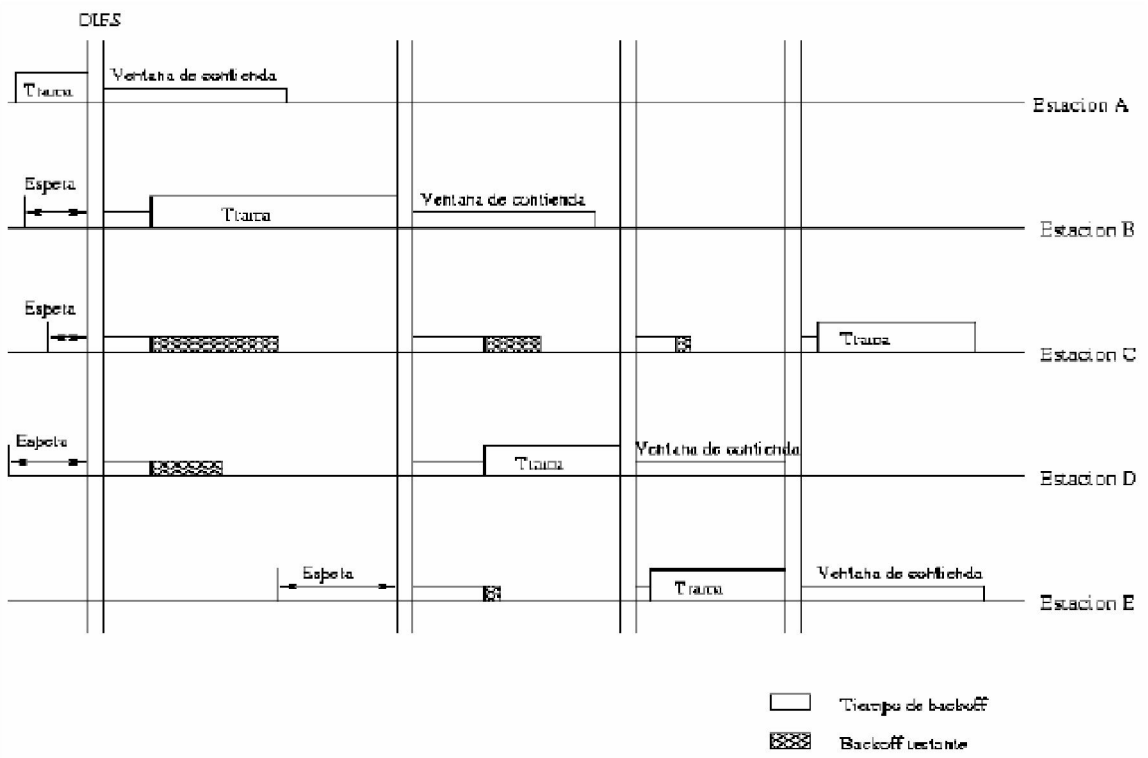

Figura. 1.6 Control de Acceso al Medio

En la figura podemos ver un ejemplo de funcionamiento de acceso CSMA/CA. Sin embargo, CSMA/CA en un entorno inalámbrico y celular, presenta una serie de problemas que intentaremos resolver con alguna modificación. Los dos principales problemas que podemos detectar son:

- Nodos ocultos. Una estación cree que el canal está libre, pero en realidad está ocupado por otro nodo que no oye.

• Nodos expuestos. Una estación cree que el canal está ocupado, pero en realidad está libre pues el nodo al que oye no le interferiría para transmitir a otro destino.

La solución que propone 802.11 es MACA o *MultiAccess Collision Avoidance.* Según este protocolo, antes de transmitir el emisor envía una trama RTS *(Request to Send),* indicando la longitud de datos que quiere enviar. El receptor le contesta con una trama CTS *(Clear to Send),* repitiendo la longitud. Al recibir el CTS, el emisor envía sus datos.

Los nodos seguirán una serie de normas para evitar los nodos ocultos y expuestos:

- Al escuchar un RTS, hay que esperar un tiempo por el CTS
- Al escuchar un CTS, hay que esperar según la longitud

La solución final de 802.11 utiliza MACA con CSMA/CA para enviar los RTS y CTS.

Espaciado entre tramas IFS

El tiempo de intervalo entre tramas se llama IFS. Durante este periodo mínimo, una estación STA estará escuchando el medio antes de transmitir. Se definen cuatro espaciados para dar prioridad de acceso al medio inalámbrico. Veámos los de más cortos a más largos:

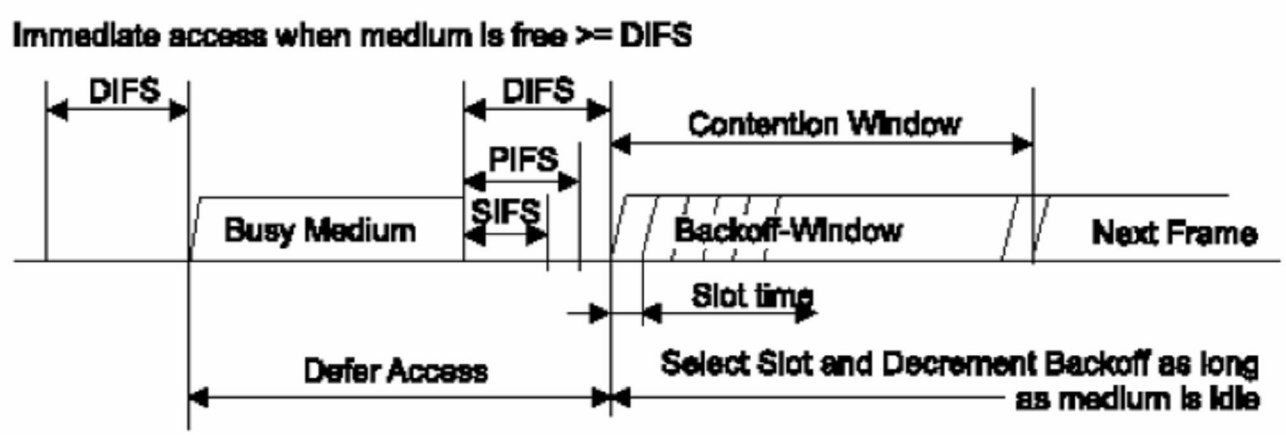

Figura. 1.7. Trama IFS

SIFS (Short IFS). Este es el periodo más corto. Se utiliza fundamentalmente para transmitir los reconocimientos. También es utilizado para transmitir cada uno de los fragmentos de una trama. Por último, es usado por el PC o *Point Control* para enviar testigo a estaciones que quieran transmitir datos síncronos

• PIFS (PCF). Es utilizado por STAs para ganar prioridad de acceso en los periodos libres de contienda. Lo utiliza el PC para ganar la contienda normal, que se produce al esperar DIFS.

• DIFS (DCF). Es el tiempo de espera habitual en las contiendas con mecanismo MACA. Se utiliza pues para el envío de tramas MAC MPDUs y tramas de gestión MMPDUs.

• EIFS (Extended IFS). Controla la espera en los casos en los que se detecta la llegada de una trama errónea. Espera un tiempo suficiente para que le vuelvan a enviar la trama u otra solución.

1.2.1. Estándar 802.11 y 1.3.3.-Estándar 802.11b

Ante la existencia de dispositivos WLAN de diferentes fabricantes, se hizo necesaria la existencia de recomendaciones (contenidas en los estándares), para permitir a los productos de estas firmas, una operación adecuada entre sí y que, además, se cumpliera con un mínimo establecido de calidad y funcionalidades.

Los estándares WLAN principiaron con el estándar 802.11, desarrollado en 1997, por el Instituto de Ingenieros Eléctricos y Electrónicos (IEEE). Estos estándares permiten transmisiones de datos de hasta 2 Mbps, transferencias que han sido mejoradas con el paso del tiempo.

Las extensiones a estas reglas se reconocen con la adición de una letra al estándar original, incluyendo 802.11a y 802.11b. La siguiente tabla contiene las variantes relacionadas al estándar 802.11.

Tabla. 1.2. Los identificadores de canales, frecuencias de canales centrales, y dominios reguladores de cada canal de IEEE 802.11b 22-MHz-de-par-a-par.

Identificador de Canal	Frecuencia en MHz	Dominios Reguladores				
		América (-A)	EMEA (-E)	Israel (-I)	China (-C)	Japón (-J)
1	2412	×	×	—	×	×
2	2417	×	×	—	×	×
3	2422	×	×	×	×	×
4	2427	×	×	×	×	×
5	2432	×	×	×	×	×
6	2437	×	×	×	×	×
7	2442	×	×	×	×	×
8	2447	×	×	×	×	×
9	2452	×	×	×	×	×
10	2457	×	×	—	×	×
11	2462	×	×	—	×	×
12	2467	—	×	—	—	×
13	2472	—	×	—	—	×
14	2484	—	—	—	—	×

Tabla. 1.3. Los identificadores de canales, frecuencias de canales centrales, y dominios reguladores de cada canal de IEEE 802.11a 20-MHz-de-par-a-par.

Identificador de Canal	Frecuencia en MHz	Dominios Reguladores			
		América (-A)	EMEA (-E)	Israel (-I)	Japón (-J)
34	5170	—	×	—	—
36	5180	×	—	×	—
38	5190	—	×	—	—
40	5200	×	—	×	—
42	5210	—	×	—	—
44	5220	×	—	×	—
46	5230	—	×	—	—
48	5240	×	—	×	—
52	5260	×	—	—	×
56	5280	×	—	—	×
60	5300	×	—	—	×
64	5320	×	—	—	×
149	5745	—	—	—	—
153	5765	—	—	—	—
157	5785	—	—	—	—
161	5805	—	—	—	—

1.2.2. Estándar 802.11g

En Junio de 2003, se ratificó un tercer estándar de modulación: 802.11g. Este utiliza la banda de 2.4 Ghz (al igual que el estándar 802.11b) pero opera a una velocidad teórica máxima de 54 Mbit/s, o cerca de 24.7 Mbit/s de velocidad real de transferencia, similar a la del estándar 802.11a. Es compatible con el estándar b y utiliza las mismas frecuencias. Buena parte del proceso de diseño del estándar lo tomó el hacer compatibles los dos estándares. Sin embargo, en redes bajo el estándar g la presencia de nodos bajo el estándar b reduce significativamente la velocidad de transmisión.

Los equipos que trabajan bajo el estándar 802.11g llegaron al mercado muy rápidamente, incluso antes de su ratificación. Esto se debió en parte a que para construir equipos bajo este nuevo estándar se podían adaptar los ya diseñados para el estándar b.

Existen equipos con especificación de potencia de hasta medio vatio, que permite hacer comunicaciones de hasta 50 Km. con antenas parabólicas apropiadas

1.2.3. Estándar 802.11i

Esta dirigido a batir la vulnerabilidad actual en la seguridad para protocolos de autenticación y de codificación. El estándar abarca los protocolos 802.1x, TKIP (Protocolo de Claves Integra – Seguras – Temporales), y AES (Estándar de Encriptación Avanzado).

1.2.4. Resumen estándares

Tabla. 1.4. Resumen Estandares

Standard	Descripción
802.11	Estándar WLAN original. Soporta de 1 a 2 Mbps.
802.11a	Estándar WLAN de alta velocidad en la banda de los 5 GHz. Soporta hasta 54 Mbps.
802.11b	Estándar WLAN para la banda de 2.4 GHz. Soporta 11 Mbps.
802.11e	Está dirigido a los requerimientos de calidad de servicio para todas las interfaces IEEE WLAN de radio.
802.11f	Define la comunicación entre puntos de acceso para facilitar redes WLAN de diferentes proveedores.
802.11g	Establece una técnica de modulación adicional para la banda de los 2.4 GHz. Dirigido a proporcionar velocidades de hasta 54 Mbps.
802.11h	Define la administración del espectro de la banda de los 5 GHz para su uso en Europa y en Asia Pacífico.
802.11i	Está dirigido a abatir la vulnerabilidad actual en la seguridad para protocolos de autenticación y de codificación. El estándar abarca los protocolos 802.1X, TKIP (Protocolo de Llaves Integras – Seguras– Temporales), y AES (Estándar de Encriptación Avanzado).

1.3. "Wi-fi alliance"

Wi-Fi *Alliance* (anteriormente WECA, "*Wireless Ethernet Compatibility Alliance*") es una organización internacional, sin ánimo de lucro, formada en 1999 para certificar la interoperabilidad de productos inalámbricos de redes de área local basados en la especificación del IEEE 802.11. Actualmente la Wi-Fi Alliance tiene más de 200 miembros alrededor del mundo, que representan a un nutrido grupo de relevantes empresas y más de 1.000 productos han recibido la certificación Wi-Fi® desde que el proceso de certificación empezó en Marzo de 2.000. El objetivo de los miembros de la Wi-Fi *Alliance* es enriquecer la experiencia de los usuarios a través de la interoperabilidad de sus productos.

Figura 1.8. Logotipo y etiquetado de certificación de productos de la Wi-Fi Alliance

Organizaciones de este tipo son totalmente imprescindibles para promover una determinada tecnología y lograr que los productos tengan la calidad requerida y la interoperabilidad necesaria

CAPITULO II

VOIP (Voz sobre Internet protocol)

2. EL DESARROLLO DE VOZ SOBRE REDES INALAMBRICAS

"La convergencia de las redes de telecomunicaciones actuales supone encontrar la tecnología que permita hacer convivir en la misma línea la voz y los datos. Esto obliga a establecer un modelo o sistema que permita "empaquetar" la voz para que pueda ser trasmitida junto con los datos. Teniendo en cuenta que Internet es la "red de redes", desarrollar una tecnología de ámbito mundial nos dirige claramente al protocolo IP (Internet Protocol) y a encontrar el método que nos permita transmitir voz a la vez que datos sobre este protocolo. El problema tiene una sencilla solución VOIP *(Voice over Internet Protocol*). Si adicional ha esto, ofrecemos que sea sobre redes inalámbricas, la ventaja será aún mayor, donde se obtendrán grandiosos resultados, entre ellos la disminución de costos."

Margaret Minerva Luna Galindo, Ingeniero de Sistemas egresada de la U.N.EX.PO "Antonio José de Sucre" Vice-rectorado: "Luis Caballero Mejias" en 1998. Actualmente desempeñándose como Ingeniero en la Unidad de Apoyo Tecnológico de CANTV Servicios

2.1. Nivel físico

Todo esto del nivel físico es lo referente a lo topado anteriormente como el tipo de antenas, si se va escoger 802.11 a, b o g, la modulación que interfiere en cada uno de los estándares, etc.

La Capa Física es la que se encarga de las conexiones físicas hacia la red, tanto en lo que se refiere al medio físico, sus características del medio y la forma en la que se transmite la información (codificación de señal, niveles de tensión/intensidad de corriente eléctrica, modulación, tasa binaria, etc.)

Es la encargada de transmitir los bits de información a través del medio utilizado para la transmisión. Se ocupa de las propiedades físicas y características eléctricas de los diversos componentes; de la velocidad de transmisión, si esta es uni o bidireccional (simplex, dúplex o full-duplex). También de aspectos mecánicos de las conexiones y terminales, incluyendo la interpretación de las señales eléctricas/electromagnéticas.

Se encarga de transformar una trama de datos proveniente del nivel de enlace en una señal adecuada al medio físico utilizado en la transmisión. Estos impulsos son electromagnéticos dependiendo de la frecuencia /longitud de onda de la señal. Cuando actúa en modo recepción el trabajo es inverso; se encarga de transformar la señal transmitida en tramas de datos binarios que serán entregados al nivel de enlace.

Sus principales funciones se pueden resumir como:

- Definir el medio o medios físicos por los que va a viajar la comunicación.
- Definir las características materiales (componentes y conectores mecánicos) y eléctricas (niveles de tensión) que se van a usar en la transmisión de los datos por los medios físicos.
- Definir las características funcionales de la interfaz (establecimiento, mantenimiento y liberación del enlace físico).

- Transmitir el flujo de bits a través del medio.
- Manejar las señales eléctricas/electromagnéticas
- Garantizar la conexión (aunque no la fiabilidad de ésta).

2.2. Nivel internet

Puede decirse que esta capa traslada los mensajes hacia/desde la capa física a la capa de red. Especifica como se organizan los datos cuando se transmiten en el medio inalámbrico que es el tema de esta tesis. Esta capa define como son los Frames, las direcciones y las sumas de control de los paquetes *Ethernet*.

Además del direccionamiento local, se ocupa de la detección y control de errores ocurridos en la capa física, del control del acceso a dicha capa y de la integridad de los datos y fiabilidad de la transmisión. En la capa normal de comunicación de Redes TC/P/IP agrupa la información a transmitir en Frames, e incluye a cada uno una suma de control que permitirá al receptor comprobar su integridad. Los datagramas recibidos son comprobados por el receptor. Si algún datagrama se ha corrompido se envía un mensaje de control al remitente solicitando su reenvío, esto no ocurre así en la telefonía IP, debido a que no tiene sentido que se repita la información porque esta seria como repetir una palabra o letra que se dijo anteriormente, simplemente los Frames llegaron al destinatario y se decodificaron y se esta en espera del siguiente paquete a esto se le conoce como UDP que se vera mas adelante.

2.3. Nivel de transporte

Esta capa se ocupa de garantizar la fiabilidad del servicio, describe la calidad y naturaleza del envío de datos. Se define cuando y como debe utilizarse la retransmisión para asegurar su llegada. Para ello divide el mensaje recibido de la capa de sesión en datagramas, los numera correlativamente y los entrega a la capa de red para su envío.

Durante la recepción, si la capa de Red utiliza el protocolo IP, la capa de Transporte es responsable de reordenar los paquetes recibidos fuera de secuencia. También puede funcionar en sentido inverso multiplexando una conexión de transporte entre diversas conexiones de datos. Este permite que los datos provenientes de diversas aplicaciones compartan el mismo flujo hacia la capa de red.

Un ejemplo típico de protocolo usado en esta capa es **TCP** (*"Transport* Control *Protocol"*), que con su homólogo **IP** de la capa de Red, configuran la suite **TCP/IP** utilizada en Internet, aunque existen otros como **UDP** *("Universal Datagram Protocol")* una capa de transporte utilizada para la telefonía IP.

2.3.1. TCP

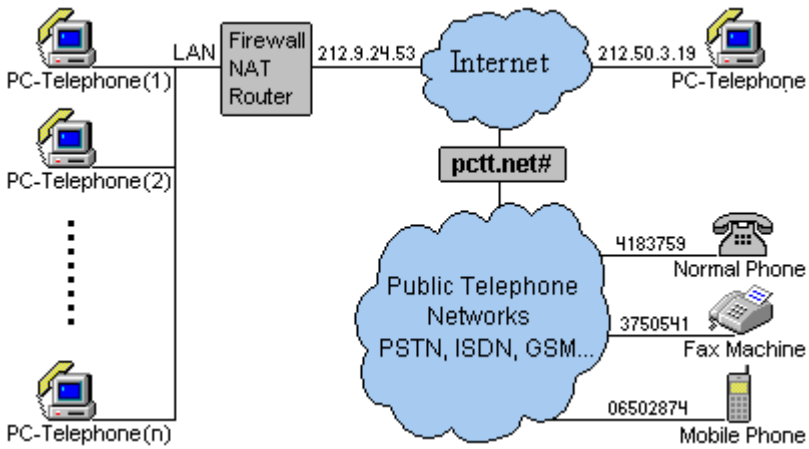

Figura. 2.1. Telefonia Ip Basica

El **Protocolo de Control de Transmisión** (TCP en sus siglas en inglés, *Transmission Control Protocol* que fue creado entre los años 1973 - 1974 por *Vint Cerf* y *Robert Kahn) e*s uno de los protocolos fundamentales. Muchos programas dentro de una red de datos compuesta por computadores pueden usar TCP para crear conexiones entre ellos a través de las cuales envíase un flujo de datos. El protocolo garantiza que los datos serán entregados en su destino sin errores y en el mismo orden en que se transmitieron. También proporciona un mecanismo para distinguir distintas aplicaciones dentro de una misma máquina, a través del concepto de puerto. TCP da soporte a muchas de las aplicaciones.

En el caso de telefonía el protocolo TCP es utilizado para la autentificación de usuarios en los servidores y cuando la comunicación esta detrás de un enrutamiento presenta a la sesión antes del establecimiento de la comunicación.

2.4. Nivel de aplicación

Voz sobre Protocolo de Internet, también llamado **Voz sobre IP**, **VozIP**, **VoIP** (por sus siglas en inglés), o **Telefonía IP**, es el enrutamiento de conversaciones de voz sobre redes basadas en IP, como por ejemplo Internet.

Los Protocolos que son usados para llevar las señales de voz sobre la red IP son comúnmente referidos como protocolos de Voz sobre IP o protocolos IP.

El tráfico de Voz sobre IP puede circular por cualquier red IP, incluyendo aquellas conectadas a Internet, como por ejemplo **redes de área local (LAN)**.

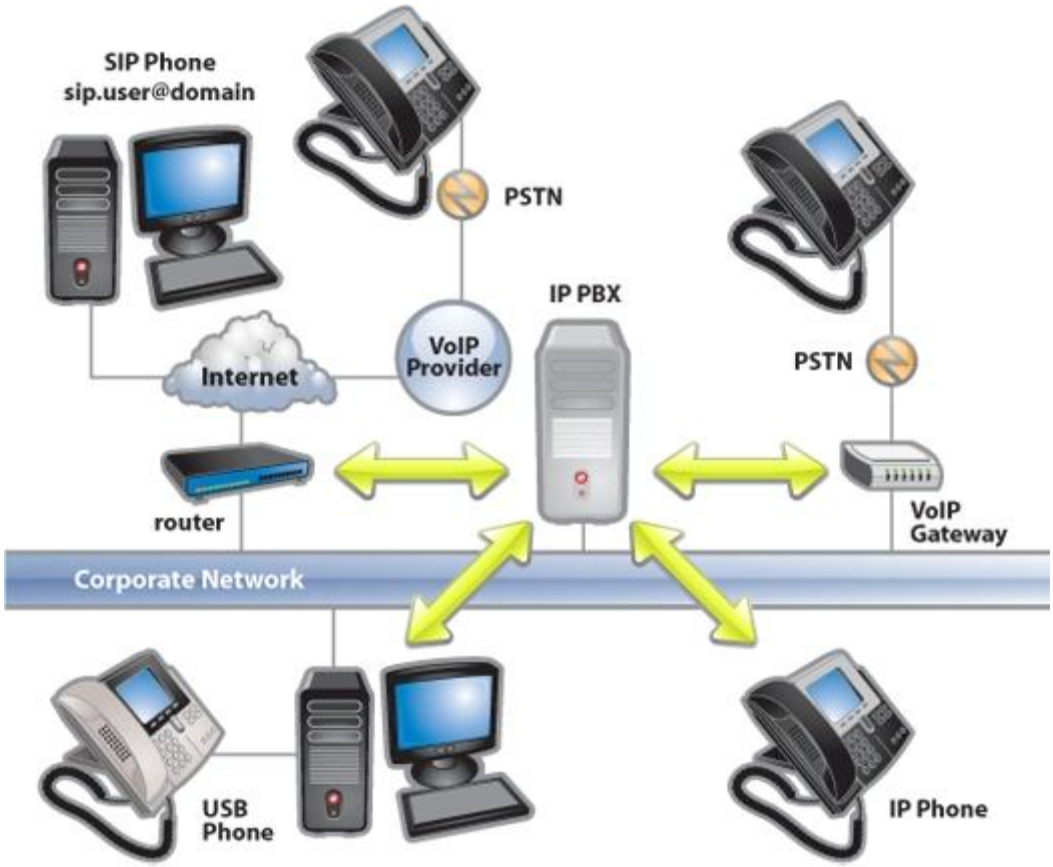

Figura. 2.2. Sistema de Telefonia IP Completo

Parámetros

Este es el principal problema que presenta hoy en día la penetración tanto de VoIP como de todas las aplicaciones de IP. Garantizar la calidad de servicio sobre una red IP, por medio de retardos y ancho de banda, actualmente no es posible; por eso, se presentan diversos problemas en cuanto a garantizar la calidad del servicio.

- *Códecs*:

La voz ha de codificarse para poder ser transmitida por la red IP. Para ello se hace uso de *Códecs* que garanticen la codificación y compresión del audio o del video para su posterior decodificación y descompresión antes de poder generar un sonido o imagen utilizable. Según el *Códec* utilizado en la transmisión, se utilizará más o menos ancho de

banda. La cantidad de ancho de banda suele ser directamente proporcional a la calidad de los datos transmitidos.

Entre los *códecs* utilizados en VoIP encontramos los G.711, G.723.1 y el G.729 (especificados por la ITU-T)

- *Retardo* o *latencia*:

Una vez establecidos los retardos de procesado, retardos de tránsito y el retardo de procesado la conversación se considera aceptable por debajo de los 150 ms.

- *Calidad del servicio*:

La calidad de servicio se está logrando en base a los siguientes criterios:

- ✓ La supresión de silencios, otorga más eficiencia a la hora de realizar una transmisión de voz, ya que se aprovecha mejor el ancho de banda al transmitir menos información.
- ✓ Compresión de cabeceras aplicando los estándares RTP/RTCP.
- ✓ Priorización de los paquetes que requieran menor latencia.
- ✓ La implantación de IPv6 que proporciona mayor espacio de direccionamiento y la posibilidad de *tunneling*.

2.4.1. Protocolo SIP *(Session Initiation Protocol)*

Session Initiation Protocol (**SIP** o **Protocolo de Inicialización de Sesiones**) es un protocolo desarrollado por el *IETF MMUSIC Working Group* con la intención de ser el estándar para la iniciación, modificación y finalización de sesiones interactivas de usuario donde intervienen elementos multimedia como el video, voz, mensajería instantánea, juegos *online* y realidad virtual. SIP fue aceptado como el protocolo de señalización de 3GPP y elemento permanente de la arquitectura IMS (*IP Multimedia Subsystem*). SIP es uno de los protocolos de señalización para voz sobre IP.

Elementos SIP

Los terminales físicos, dispositivos con el aspecto y forma de teléfonos tradicionales, pero que usan SIP y RTP para la comunicación. Algunos de ellos usan numeración electrónica (ENUM) o DUNDi para traducir los números existentes de teléfono a direcciones SIP usando DNS (*Domain Name Server*), así llaman a otros usuarios SIP saltándose la red *VoIp*, con lo que tu proveedor de servicio normalmente actúa de pasarela hacia la red pública conmutada de telefonía para los números de teléfono tradicionales.

SIP requiere *proxy* y elementos de registro para dar un servicio práctico. Aunque dos terminales SIP puedan comunicarse sin intervención de infraestructuras SIP (razón por la que el protocolo se define como punto-a-punto), este enfoque es impracticable para un servicio público. Hay varias implementaciones de *softswitch* que pueden actuar como *proxy* y elementos de registro.

De los RFCs:

> "SIP hace uso de elementos llamados **servidores *Proxy*** para ayudar a enrutar las peticiones hacia la localización actual del usuario, autenticar y autorizar usuarios para darles servicio, posibilitar la implementación de políticas de enrutamiento de llamadas, y aportar capacidades añadidas al usuario."

> "SIP también aporta funciones de registro que permiten al usuario informar de su localización actual a los servidores *Proxy."*

> "Es un concepto importante que la distinción entre los tipos de servidores SIP es lógica y no física."

Protocolo SIP

Los clientes SIP usan el puerto 5060 en TCP (*Transmission Control Protocol*) y UDP (*User Datagram Protocol*) para conectar con los servidores SIP. SIP es usado simplemente para iniciar y terminar llamadas de voz y video. Todas las comunicaciones de voz/video van sobre RTP (*Real-time Transport Protocol*).

Un objetivo de SIP fue aportar un conjunto de las funciones de procesamiento de llamadas y capacidades presentes en la red pública conmutada de telefonía. Así, implementó funciones típicas que permite un teléfono común como son: llamar a un número, provocar que un teléfono suene al ser llamado, escuchar la señal de tono o de ocupado. La implementación y terminología en SIP son diferentes.

SIP también implementa muchas de las más avanzadas características del procesamiento de llamadas de SS7, aunque los dos protocolos son muy diferentes. SS7 es altamente centralizado, caracterizado por una compleja arquitectura central de red y unos terminales tontos (los tradicionales teléfonos de auricular). SIP es un protocolo punto a punto (también llamado p2p). Como tal requiere un núcleo de red sencillo (y altamente escalable) con inteligencia distribuida en los extremos de la red, incluida en los terminales (ya sea mediante *hardware o software)*. Muchas características de SIP son implementadas en los terminales en oposición a las tradicionales características de SS7, que son implementadas en la red.

Aunque existen muchos otros protocolos de señalización para VoIP, SIP se caracteriza porque sus promotores tienen sus raíces en la comunidad IP y no en la industria de las telecomunicaciones. SIP ha sido estandarizado y dirigido principalmente por el IETF.

SIP funciona en colaboración con otros muchos protocolos pero solo interviene en la parte de señalización al establecer la sesión de comunicación. SIP actúa como envoltura al SDP, que describe el contenido multimedia de la sesión, por ejemplo qué puerto IP y *códec* se usarán durante la comunicación, etc. En un uso normal, las sesiones SIP son simplemente flujos de paquetes de RTP (*Real-time Transport Protocol*). RTP es el verdadero portador para el contenido de voz y video.

La primera versión propuesta para estándar (SIP 2.0) fue definida en el RFC 2543. El protocolo aclarado en el RFC 3261, aunque muchas implementaciones están usando todavía versiones en fase de borrador. Hay que fijarse en que el número de versión sigue siendo 2.0.

SIP es similar a HTTP y comparte con él algunos de sus principios de diseño: es legible por humanos y sigue una estructura de petición-respuesta. Los promotores de SIP afirman que es más simple que H.323. Sin embargo, aunque originalmente SIP tenía como objetivo la simplicidad, en su estado actual se ha vuelto tan complejo como H.323. SIP comparte muchos códigos de estado de HTTP, como el familiar '404 no encontrado' (*404 not found*). SIP y H.323 no se limitan a comunicaciones de voz y pueden mediar en cualquier tipo de sesión comunicativa desde voz hasta video o futuras aplicaciones todavía sin realizar.

Metodo_SIP

Las peticiones SIP son caracterizadas por la línea inicial del mensaje, llamada *Request-Line,* que contiene el nombre del método, el identificador del destinatario de la petición *(Request*-URI) y la versión del protocolo SIP. Existen seis métodos básicos SIP (definidos en RFC 254) que describen las peticiones de los clientes:

- ***INVITE***: Permite invitar un usuario o servicio para participar en una sesión o para modificar parámetros en una sesión ya existente.
- **ACK**: Confirma el establecimiento de una sesión.
- ***OPTION****:* Solicita información sobre las capacidades de un servidor.
- ***BYE***: Indica la terminación de una sesión.
- ***CANCEL***: Cancela una petición pendiente.
- ***REGISTER***: Registrar al *User Agent.*

Sin embargo, existen otros métodos adicionales que pueden ser utilizados, publicados en otros RFCs como los métodos INFO, SUBSCRIBER, etc.

A continuación un ejemplo real de mensaje del método *REGISTER*:

Vía: SIP/2.0/UDP
192.168.0.100:5060;rport;branch=z9hG4bK646464100000000b43c52d6c00000d1200000f03
Content-Length: 0
Contact: <sip:20000@192.168.0.100:5060>
Call-ID: ED9A8038-A29D-40AB-95B1-0F5F5E905574@192.168.0.100

CSeq: 36 REGISTER
From: <sip:20000@192.168.0.101>;tag=910033437093
Max-Forwards: 70
To: <sip:20000@192.168.0.101>
User-Agent: SJphone/1.60.289a (SJ Labs)
Authorization: Digest
username="20000",realm="192.168.0.101",nonce="43c52e9d29317c0bf1f885b9aaff1522d93c7692"
,uri="192.168.0.101",response="f69463b8d3efdb87c388efa9be1a1e63"

Respuestas (Códigos de estado) SIP.

Después de la recepción e interpretación del mensaje de solicitud SIP, el receptor del mismo responde con un mensaje. Este mensaje, es similar al anterior, pero difiere en la línea inicial, llamada *Status-Line*, que contiene la versión de SIP, el código de la respuesta *(Status–Code)* y una pequeña descripción *(Reason-Phrase).* El código de la respuesta está compuesto por tres dígitos que permiten clasificar los diferentes tipos existentes. El primer dígito define la clase de la respuesta.

Código Clases
1xx - Mensajes provisionales.
2xx - Respuestas de éxito.
3xx - Respuestas de redirección.
4xx - Respuestas de fallo de método.
5xx - Respuestas de fallos de servidor.
6xx - Respuestas de fallos globales.

A Continuación, se incluye un ejemplo de un código de respuesta.

Internet Protocol, Src Addr: 192.168.0.101 (192.168.0.101), Dst Addr: 192.168.0.100 (192.168.0.100)
User Datagram Protocol, Src Port: 5060 (5060), Dst Port: 5060 (5060)
Session Initiation Protocol
Status-Line: SIP/2.0 200 OK
Status-Code: 200
Resent Packet: False
Vía: SIP/2.0/UDP *192.168.0.100*:5060;rport;branch=z9hG4bK646464100000000b43c52d6c00000d1200000f03
Content-Length: 0
Contact: <sip:20100*@192.168.0.100*:5060>
Call-ID: ED9A8038-A29D-40AB-95B1-0F5F5E905574@100.100.100.16
CSeq: 36 REGISTER
From: <sip:20000*@192.168.0.101*>;tag=910033437093
Max-Forwards: 70
To: <sip:20000*@192.168.0.101*:5060>
Authorization: Digest username="20100",realm="*192.168.0.101*",nonce="43c52e9d29317c0bf1f885b9aaff1522d93c7692",uri="sip:*192.168.0.101*",
response="f69463b8d3efdb87c388efa9be1a1e63"

Errores

A continuación se muestran los errores que se pueden producir en los mensajes SIP de manera más detallada explicando la causa concreta del error.

Como se ha indicado anteriormente corresponde con las respuestas de la clase:

4xx - Respuestas de fallo de método.
5xx - Respuestas de fallos de servidor.
6xx - Respuestas de fallos globales.

Estos errores se corresponden con los mensajes de error Q.931 o DSS1 y suponen el mapeo de los eventos SIP con los códigos de error de la RTC (Red telefonía conmutada)

Tabla. 2.1. Tabla de Errores

Evento SIP	Valor decimal (DSS1)	Valor hexadecimal (DSS1)	Valor transmitido en el canal D	Detalle
400 Bad request	127	7f	Ff	Interworking, unspecified
401 Unauthorized	57	39	b9	Bearer capability not authorized
402 Payment required	21	15	95	Call rejected
403 Forbidden	57	39	b9	Bearer capability not authorized
404 Not found	1	01	81	Unallocated (unassigned) number
405 Method not allowed	127	7f	Ff	Interworking, unspecified
406 Not acceptable	127	7f	Ff	Interworking, unspecified
407 Proxy authentication required	21	15	95	Call rejected

408 Request timeout	102	66	e6	Recover on Expires timeout
409 Conflict	41	29	a9	Temporary failure
410 Gone	1	01	81	Unallocated (unassigned) number
411 Length required	127	7f	Ff	Interworking, unspecified
413 Request entity too long	127	7f	Ff	Interworking, unspecified
414 Request URI (URL) too long	127	7f	Ff	Interworking, unspecified
415 Unsupported media type	79	4f	Cf	Service or option not available
420 Bad extension	127	7f	Ff	Interworking, unspecified
480 Temporarily unavailable	18	12	92	No user response
481 Call leg does not exist	127	7f	Ff	Interworking, unspecified
482 Loop detected	127	7f	Ff	Interworking, unspecified
483 Too many hops	127	7f	Ff	Interworking, unspecified
484 Address incomplete	28	1c	9c	Address incomplete (invalid number format)
485 Address ambiguous	1	01	81	Unallocated (unassigned) number
486 Busy here	17	11	91	User busy
487 Request cancelled	127	7f	Ff	Interworking, unspecified
488 Not acceptable here	127	7f	Ff	Interworking, unspecified
500 Internal server error	41	29	a9	Temporary failure

501 Not implemented	79	4f	Cf	Service or option not implemented
502 Bad gateway	38	26	a6	Network out of order
503 Service unavailable	63	3f	Bf	Service or option unavailable
504 Gateway timeout	102	66	e6	Recover on Expires timeout
505 Version not implemented	127	7f	Ff	Interworking, unspecified
580 Precondition Failed	47	2f	Af	Resource unavailable, unspecified
600 Busy everywhere	17	11	91	User busy
603 Decline	21	15	95	Call rejected
604 Does not exist anywhere	1	01	81	Unallocated (unassigned) number
606 Not acceptable	58	3a	Ba	Bearer capability not presently available

2.4.2. Protocolo SDP *(Session Description Protocol)*

El protocolo SDP *(Session Description Protocol*) RFC 2327 se utiliza para describir sesiones multicast en tiempo real, siendo útil para invitaciones, anuncios, y cualquier otra forma de inicio de sesiones.

La propuesta original de SDP fue diseñada para anunciar información necesaria para los participantes y para aplicaciones de multicast MBONE (*Multicast Backbone).*
Actualmente, su uso está extendido para el anuncio y la negociación de las capacidades de una sesión multimedia en Internet.

Puesto que SDP es un protocolo de descripción, los mensajes SDP se pueden transportar mediante distintos protocolos con SIP, SAP, RTSP, correo electrónico con aplicaciones MIME o protocolos como HTTP. Como el SIP, el SDP utiliza la codificación del texto. Un mensaje del SDP se compone de una serie de líneas, denominados campos, dónde los nombres son abreviados por una sola letra, y está en orden, requerido para simplificar el análisis. El SDP no fue diseñado para ser fácilmente extensible.

La única manera de ampliar o de agregar nuevas capacidades al SDP es definir un nuevo atributo. Sin embargo, los atributos desconocidos pueden ser ignorados.
En la tabla siguiente podemos observar todos los campos:
Tipo Descripción Obligatorio

V Versión del protocolo (obligatorio)
o Identificador (obligatorio)
S Nombre de sesión (obligatorio)
I Información de la sesión (obligatorio)
U URI de la descripción
e Dirección de correo
p Número de teléfono
C Información de conexión
b Ancho de banda
Z Tiempo de corrección
K Clave de encriptación
a Atributos
T Tiempo de sesión(Start y stop) (obligatorio)
R Tiempo de repetición
m Información del protocolo de transporte(media) (obligatorio)

S*ession Description Protocol* Version (v): 0
O*wner/Creator, Session Id* (o): Cisco-SIPUA 26425 12433 IN IP4
192.168.0.100
O*wner Username:* Cisco-SIPUA

S*ession* ID: 26425

S*ession* Version: 12433

O*wner Network Type*: IN

O*wner Address Type:* IP4

O*wner Address*: 192.168.0.100

S*ession Name* (s): SIP Call

C*onnection Information* (c): IN IP4 192.168.0.100

C*onnection Network Type:* IN

C*onnection Address Type:* IP4

C*onnection Address:* 192.168.0.100

T*ime Description, active time* (t): 0 0

S*ession Start Time:* 0

S*ession Stop Time:* 0

Media *Description, name and address* (m): audio 17338 RTP/AVP 0 8 18 101

Media *Type:* audio

Media *Port:* 17338

Media *Proto*: RTP/AVP

Media *Format:* ITU-T G.711 PCMU

Media *Format:* ITU-T G.711 PCMA

Format: ITU-T G.729

Media *Format:* 101

Media *Attribute* (a): rtpmap:0 PCMU/8000

Media *Attribute* (a): rtpmap:8 PCMA/8000

Media *Attribute* (a): rtpmap:18 G729/8000

Media *Attribute* (a): rtpmap:101 *telephone*-event/8000

Media *Attribute* (a): fmtp:101 0-15

2.4.3. Protocolo RTP (*Real-Time TransportPotocol*)

Para encapsular los datos en el pila de TCP/IP se sigue la siguiente estructura:

- ✓ Paquetes de datos VoIP
- ✓ RTP

- ✓ UDP
- ✓ IP
- ✓ Capas I,II

Los paquetes de VoIP se encuentran en el protocolo RTP el cual esta dentro de los paquetes UDP-IP.

VoIP no usa el protocolo de TCP porque es demasiado pesado para las aplicaciones de tiempo real así es que para eso usa la data grama de UDP.

El data grama de UDP no tiene el control sobre la orden de la cual los paquetes son recibidos o de cuanto tiempo toma para llegar ahí. Cualquiera de estos dos puntos son bastante importantes para la calidad (que tan clara se escucha la voz de la otra persona) y la calidad de la conversación (que tan fácil es llevar una conversación), por lo que RTP resuelve este problema permitiendo que el receptor ponga los paquetes en el orden correcto y que no se tarde con los paquetes que hayan perdido el camino o se tarden mucho en ser recibidos.

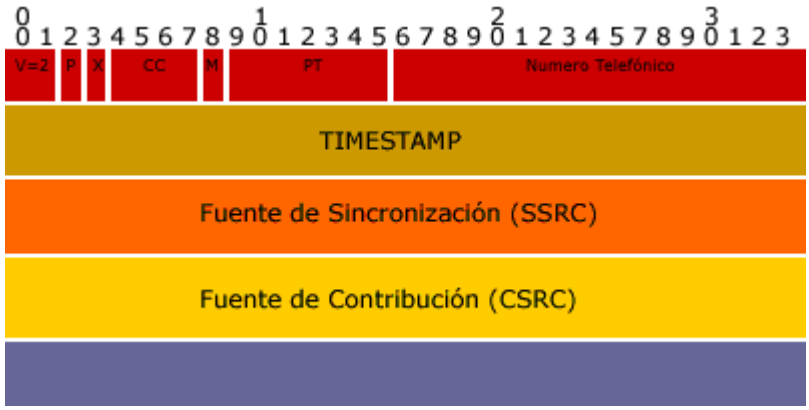

Figura. 2.3. Trama UDP

Donde:

• V indica la versión del RTP que se usa

• P el *BIT* de paridad.

• X indica la presencia de la extensión del encabezado.

• El campo CC es el número de identificadores CSRC que siguen al encabezado. El campo CSRC se usa por ejemplo cuando hay conferencia.

• M indica un *BIT* para Marcar.

2.4.4. Descubrimiento del *proxy out-bound*

En la Red VoIp 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 Controííer* (SBC) cuya dirección IP pública se obtendrá de un servidor DNS.

Para ello se deberán programar en los terminales:

- ✓ SIP *out-bound Proxy*
- ✓ 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-íive*, 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).

2.4.4.1. 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.

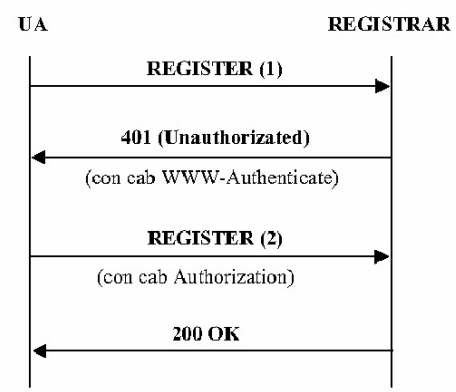

Figura. 2.4. Flujo Registro

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

Tabla. 2.2. Campos Paquete SIP

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

La respuesta 200 Ok

Tabla. 2.5. Ejemplo Campos 200 OK

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.

2.4.5. 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 *pass Word* del usuario viaja codificada.

El procedimiento general de autenticación consiste en lo siguiente (la definición de las cabeceras y parámetros utilizados):

- ✓ 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-*pass Word,* 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 envía 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 *pass Word* 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-lnfo* (o *Proxy-Authentication-lnfo* 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.

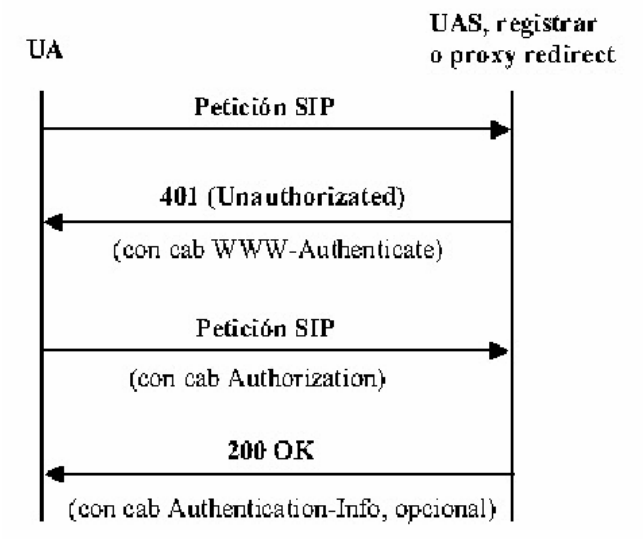

Figura. 2.5. Register-Unauthorizated

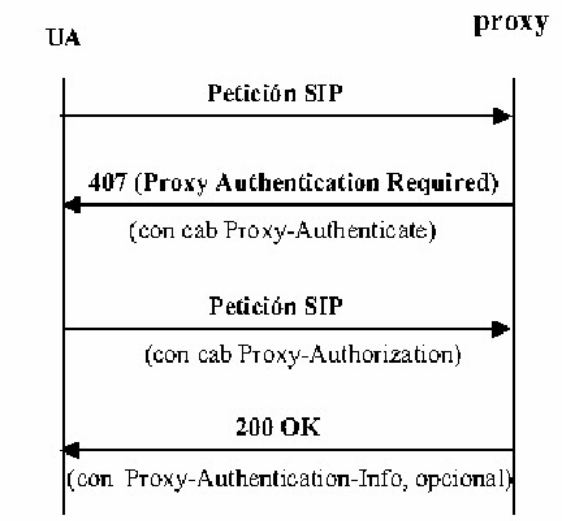

Figura. 2.6. Register-Authentication

2.5. Flujos de llamada en dominio ip

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 pasos:

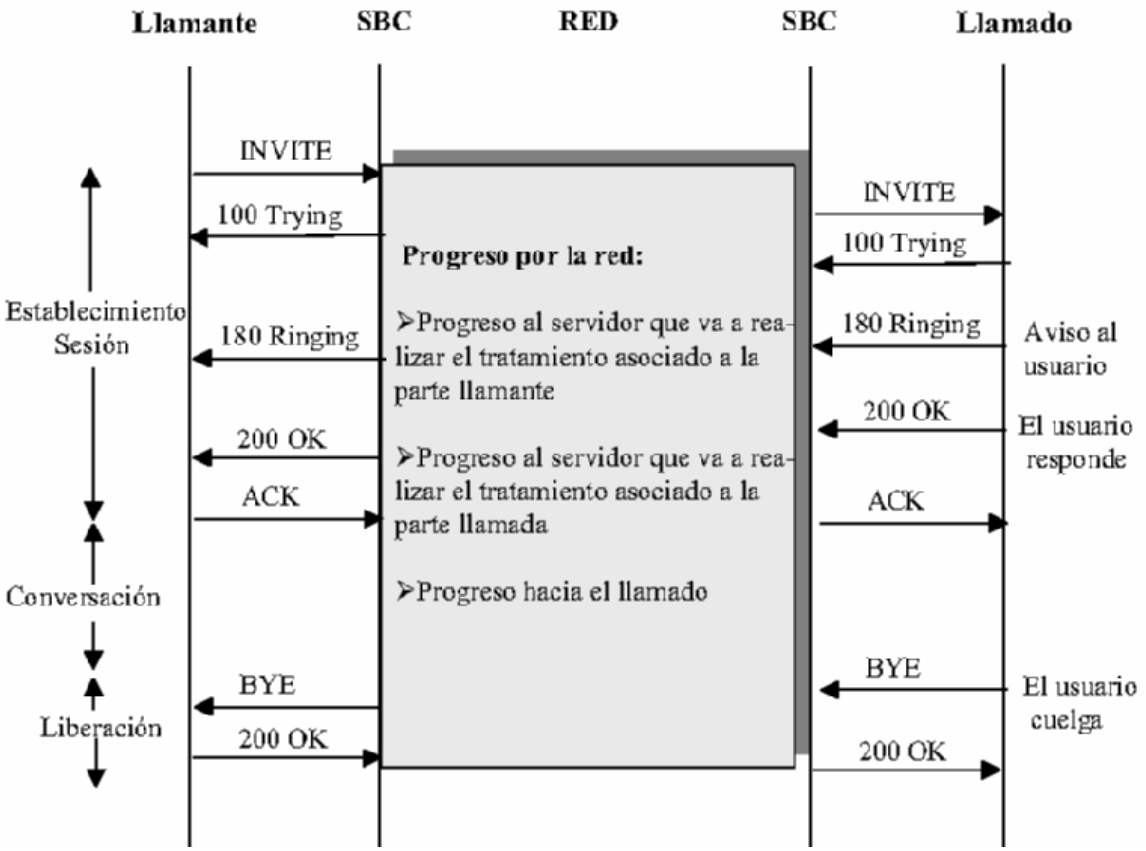

Figura. 2.7. Solicitud de establecimiento de sesión

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 I*NVITE*. 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.

Tabla. 2.4. Campos IP to IP

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

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

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)*.

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"

- ✓ 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".
- ✓ 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 confiabilidad, 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 *Red VoIp)*.

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".

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".

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.

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.

Tabla. 2.7. Campos Ip to IP UA

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

Sesiones infructuosa

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.

La figura refleja una llamada infructuosa notificada al Terminal llamante, mientras que el siguiente gráfico refleja una llamada infructuosa debido al rechazo de la misma realizado desde el Terminal llamado.

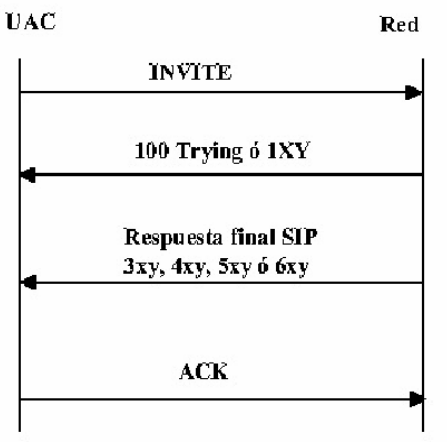

Figura. 2.8. Trying 100

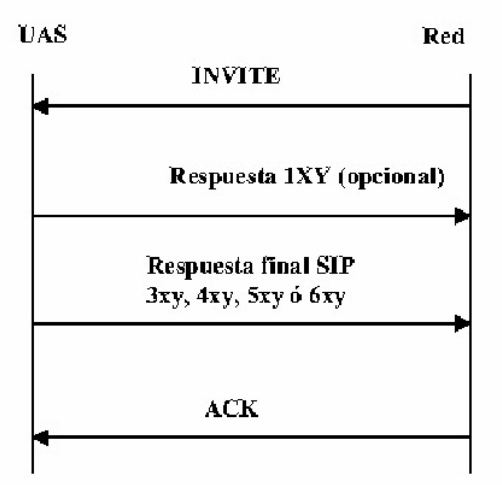

Figura. 2.9. Invite

2.6. Flujos de llamada con dominio ip - pstn

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

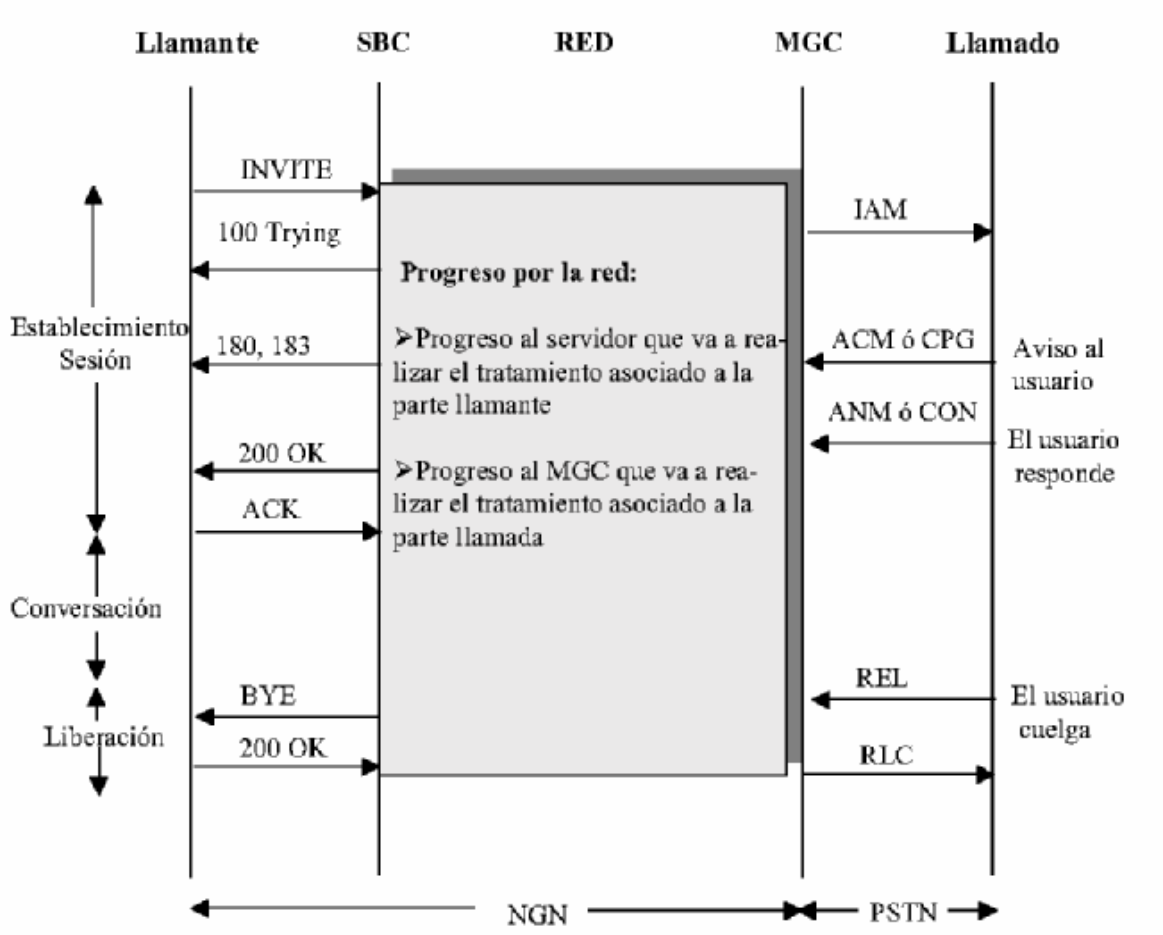

Figura. 2.10. PSTN Sesion

Solicitud de establecimiento de sesión

El establecimiento de la sesión se hace de la misma manera que se indicó en el punto anterior 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.

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 una sesión 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 se resume el citado “mapeo” (para más detalle ver UIT-T Q 191 2.5).

Tabla. 2.6. Campo SDP

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.

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.

Tabla. 2.7. Campos SDP y Sesión

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. 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.

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).

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 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.*

Tabla. 2.8. BYE and CANCEL

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*.

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.

Tabla. 2.9. Errores SIP y Causas

←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"*)

2.6.2. Sesión PSTN-IP

En este punto 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 representa las distintas fases de la llamada y que se describen en los siguientes apartados.

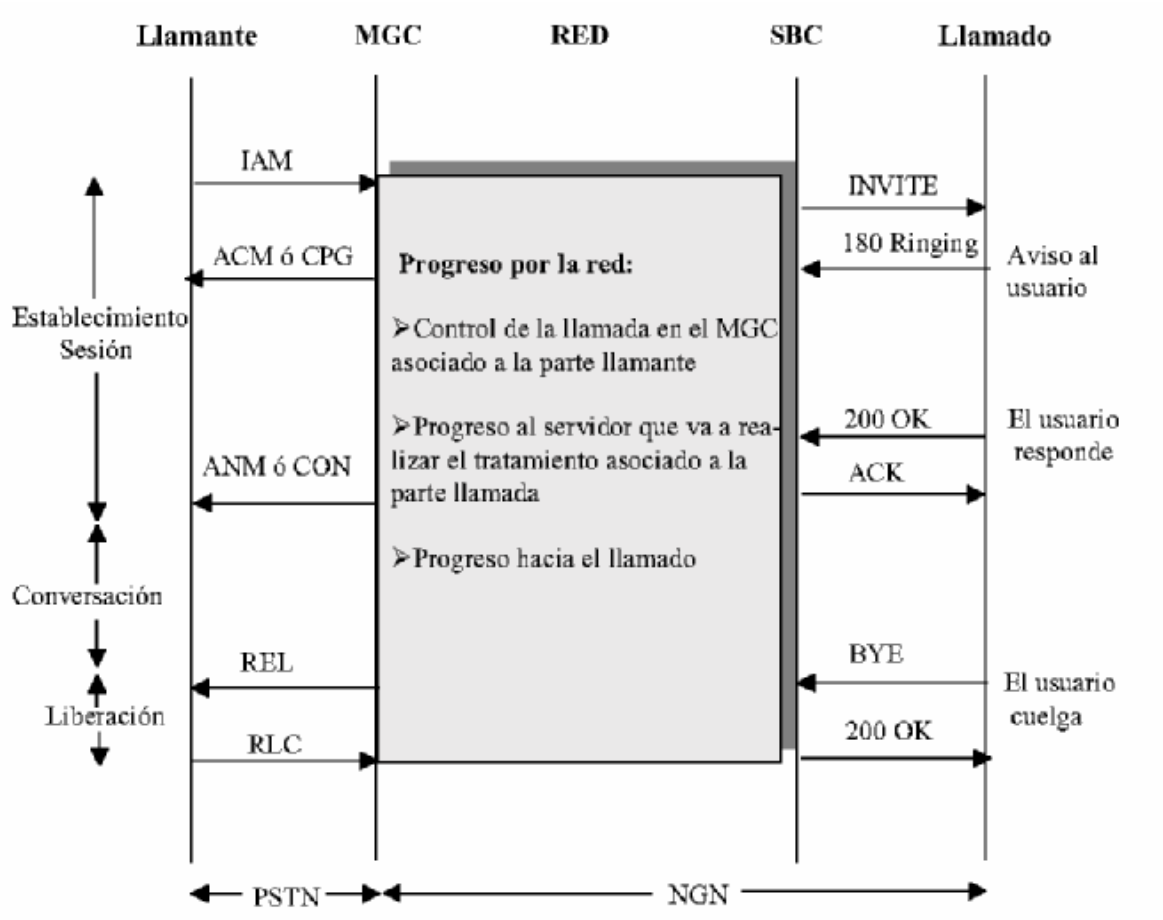

Figura. 2.11. PSTN to IP

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 1AM 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 (para más detalle ver UIT-T Q 1912.5).

Tabla. 2.10. IAM

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).

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 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)*.

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 llamantes y llamado, aunque en estado "anticipado".

  Cuando el MGC recibe esta respuesta:
  - Si incluye el parámetro *tag* en la cabecera *To*, crea el correspondiente diálogo en estado "anticipado".

- ✓ Envía en *PUSI* hacia la red PSTN un mensaje ACM ó CPG. El ACM llevará codificado el parámetro indicador 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.

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".

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.

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

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 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.*

Tabla. 2.11. BYE and CANCEL

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*.

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.*

Tabla. 2.12. Mensajes SIP serie 400/500/600

←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)

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.

2.7. Criterios de apertura de flujos rtp

En las figuras 1 y 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.

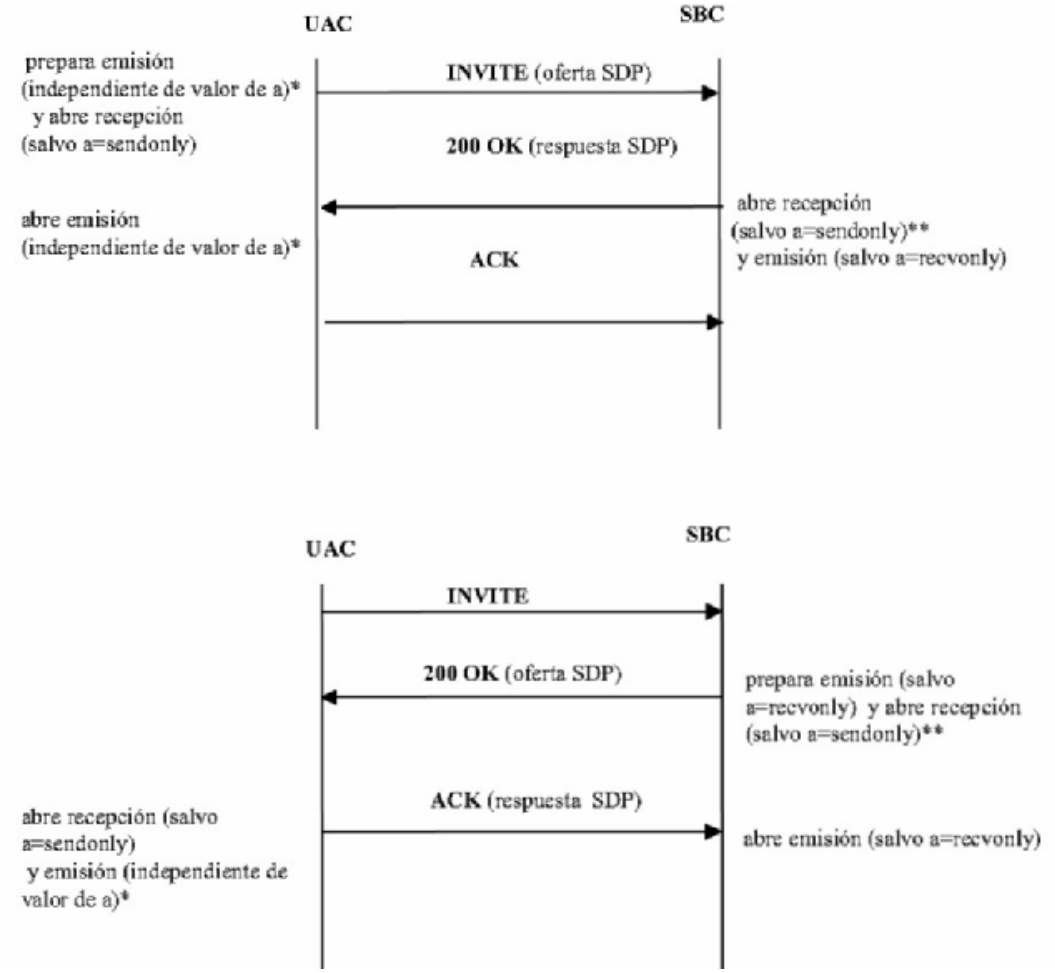

Figura. 2.12. Flujo RTP entre UAC y SBC en sesión IP-IP

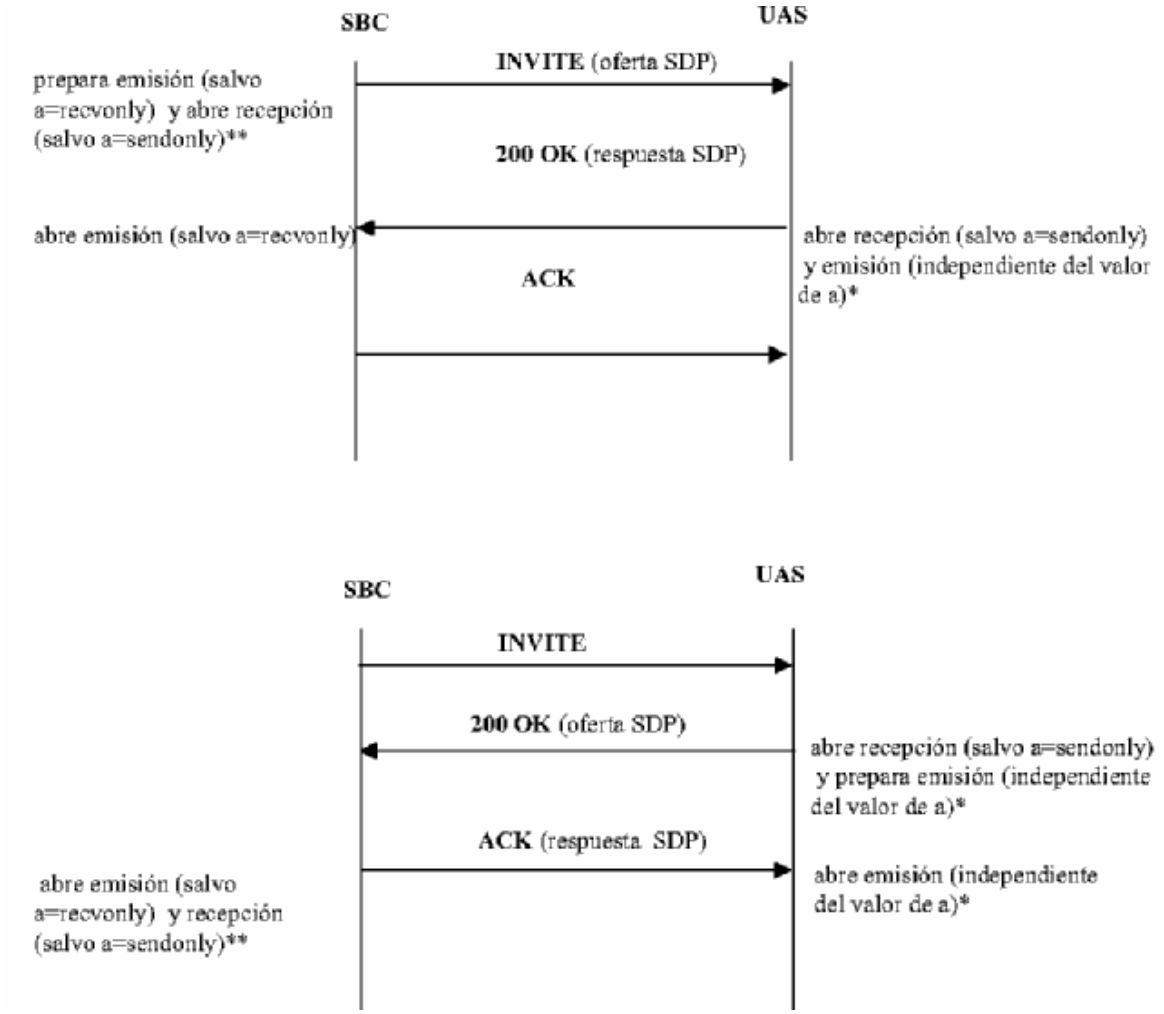

Figura. 2.13. Flujo RTP entre SBC y UAS en sesión IP-IP

En la figura se refleja el criterio de apertura de flujo en un diálogo anticipado con respuesta provisional tipo l8xy. 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.

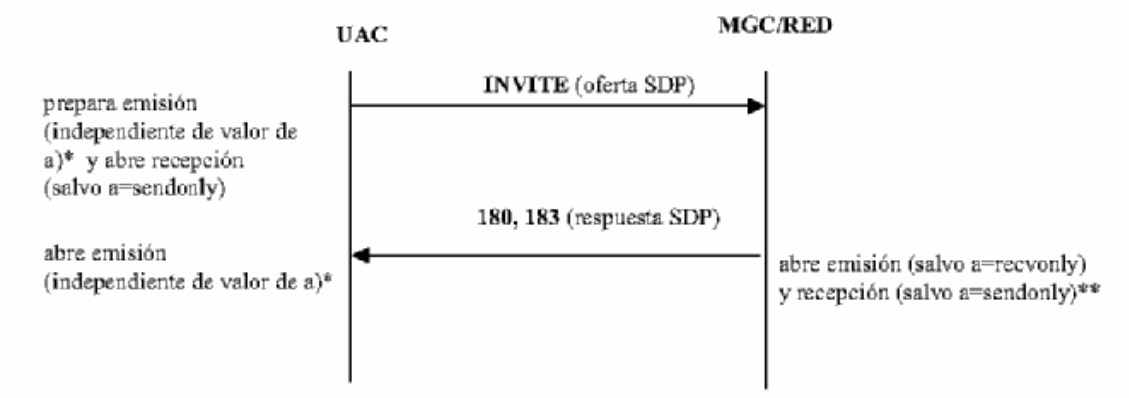

Figura. 2.14. Apertura de flujo RTP en una sesión IP-PSTN.

En las figuras 1 y 2 se refleja el criterio de apertura de flujo RTP ante un cambio de medio en una sesión IP-IP establecida.

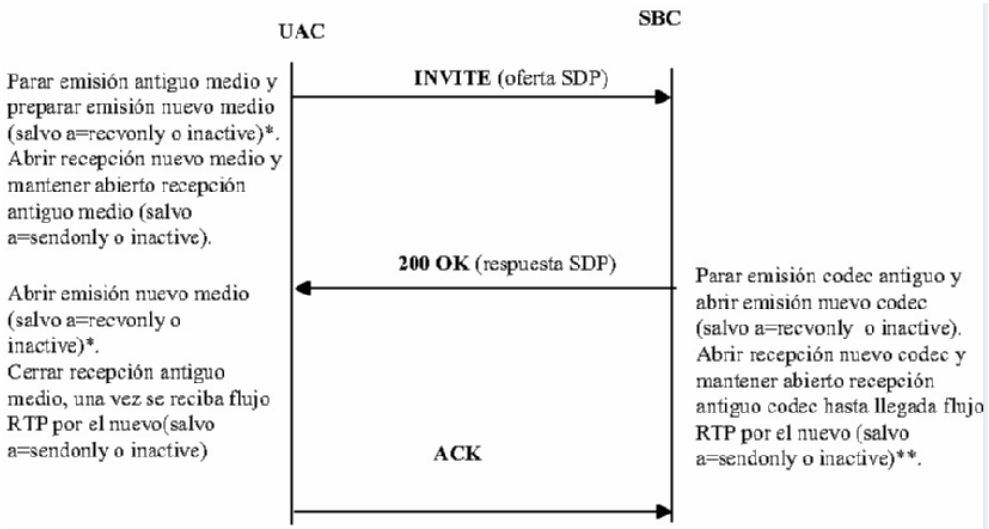

Figura. 2.15. UAC and SBC

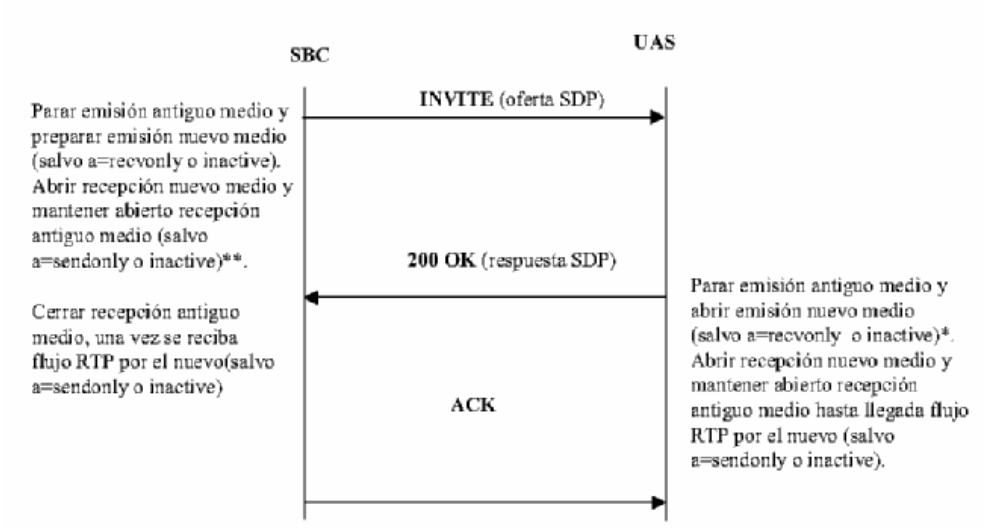

Figura. 2.16. Apertura de flujo en cambio de medio entre SBC y UAS

CAPÍTULO III

SEGURIDAD SOBRE REDES IEEE 802.11

3. MEDIDAS DE SEGURIDAD Y DESCRIPCIÓN MÁS DETALLADA DEL NIVEL FÍSICO Y SUBNIVEL MAC DE 802.11.

Los servicios Lógicos: 802.11 propone dos categorías de servicios empleados en el subnivel MAC:

- Station Service (SS): Son los servicios específicos de las STAs.
- Distribution System Service: Estos servicios se emplean para pasar en cualquier sentido entre DS y BSS.

Los servicios, determinarán distintos tipos de mensajes que fluirán por la red, Independientemente de su categoría, la totalidad de los servicios (y/o mensajes) son:

a. ***Authentication***: A diferencia de una red cableada, en 802.11 no existe una seguridad a nivel físico para prevenir el acceso no autorizado, por lo tanto este estándar ofrece la capacidad de autenticación por medio de este servicio. Si entre dos estaciones no se establece un adecuado nivel de autenticación, la asociación no podrá ser establecida. 802.11 soporta dos metodologías de autenticación:

- *Open System Authentication* (OSA): Cualquier STA puede ser autenticada. *Null Authentication.*
- *Shared Key Authentication*: Este mecanismo requiere la implementación de *Wireless Equivalent Privacy (WEP).*

b. *Deauthentication*: Este servicio es invocado si una *autenticación* debe ser finalizada. Se trata de una notificación, no una solicitud, por lo tanto no puede ser rechazada, y puede ser invocado tanto por una STA (No AP), como por un AP.

c. *Association*: Antes que una STA pueda enviar mensajes vía un AP, la misma deberá encontrarse Asociada a este último. Este servicio permite al DS conectar distintas STA dentro de una *LAN Wireless,* ubicando a cada una de ellas. En cualquier instante de tiempo, una STA solo podrá estar asociada a un único AP. Este servicio es siempre iniciado por una STA no AP, (nunca por un AP).

d. *Deassociation*: Este servicio es invocado si una asociación debe ser finalizada. Se trata de una notificación, no una solicitud, por lo tanto no puede ser rechazada, y puede ser invocado tanto por una STA (No AP), como por un AP.

e. *Reassociation*: Permite cambiar una asociación de un AP a otro, o también cambiar los parámetros de asociación de una STA con el mismo AP.

f. *Distribution:* Este tipo de mensajes se producen al ingresar información a un DS proveniente de un BSS. El encargado de generar estos mensajes será un AP y su objetivo es alcanzar el destino buscado.

g. Integración: Los mensajes que van o vienen dirigidos hacia/desde un portal, harán uso de este servicio.

h. ***Privacy****:* 802.11 al igual que sucede con autenticación (y por las mismas causas) provee la posibilidad de criptografiar el contenido de los mensajes a través de este servicio. Este servicio que es opcional, también se lleva a cabo por *WEP*.

i. ***MSDU delivery***: Responsable de entregar la información al nivel físico. Existe una relación entre asociación y autenticación que provoca los tres "Estados" en los que se puede encontrar una STA en cualquier intervalo de tiempo:

- Estado 1: No autenticado – No asociado.
- Estado 2: Autenticado – No asociado.
- Estado 3: Autenticado – Asociado.

Estos servicios generan distintos tipos de mensajes, los cuales están clasificados en:

a. *Data:*

b. Control:

c. *Management:*

3.1. Como funciona *wep*

Primero debemos distinguir entre: texto plano (P) y texto cifrado (C).

El proceso de reconvertir un texto cifrado en texto plano se denomina descifrado (D). Un algoritmo criptográfico es una función matemática empleada para cifrar y descifrar.

Los algoritmos actuales suelen emplear secuencias de clave (k), para modificar la salida de la función matemática.

En el caso de Criptografiar un texto (o Encriptar {aunque este término no esté aún reconocido por la RAE}), se dice que la función E opera sobre P para producir C y se representa:

Ek (P) = C

El proceso inverso sería: Dk (C) = P

3.1.1. Llaves

La clave se forma a partir de la frase, la cual se ordena en palabras de a 4 *Byte* y se realiza una operación XOR palabra a palabra, dando como resultado una "Semilla" de 32 *bit.*

Esta Semilla es el punto de partida con el cual, la función PRNG a través de 40 iteraciones, creará cuatro claves de 40 *bit*. De estas claves se seleccionará solo una (que estará indicada dentro de la trama).

La STA que inicia esta operación, calcula el CRC de todo el *Payload* y lo agrega al final del mismo, este valor se denomina *Integrity Check Value* (ICV). Otro valor que entra en juego es el IV, que no es más que un contador que oscila entre 0 y 4096 (dentro del mismo se incluirán dos *bits* que identificarán a la clave elegida de las 4 generadas).

Por lo tanto quedan dos bloques:

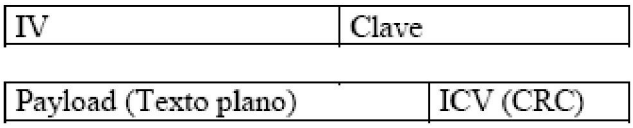

Figura. 3.1. Trama de IV

El IV de 24 *bit*, incluye entonces 2 *bit* que identifican la clave elegida (entre las 4 generadas) y la clave por defecto es de 40 *bits*, formando un bloque de 64 *bits*. Existe

también la posibilidad de trabajar con claves de 128 *bits*, en cuyo caso se mantienen los 24 *bits* de IV y se genera una clave de longitud 104 *bits*, dando el total de 128.

Este bloque es el que conforma la "Semilla" de *WEP (PNRG),* con la cual se genera el flujo de cifrado de bloque realizando nuevamente un XOR con el bloque: Texto plano + ICV.

El algoritmo *WEP*, perteneciente a RSA, no se detalla en este texto. Con esta última operación quedan conformados todos los bloques con los que se armará finalmente la trama que quedará constituida por los siguientes campos:

	24	n >= 1	4
Header	IV (+N° clave)	Payload (Datos >=1)	ICV
← TEXTO PLANO →		← CIFRADO →	

Figura. 3.2. Trama Basica WEP

Se debe tener muy en cuenta aquí que el IV viaja como texto plano, y con cada IV generado (secuencialmente), se crea una nueva semilla y por lo tanto se ingresa a *WEP* con distintos valores clave.

El algoritmo *WEP*, presenta varios puntos vulnerables, en particular si se opera con clave de 64 *bits* (de los cuáles sólo 40 son desconocidos, pues los 24 del IV van en texto plano), pero en este punto cabe mencionar uno de los principales. Si se tiene en cuenta que el IV es secuencial y su valor máximo es 224 (16 millones), el mismo en una red con mediana tasa de tráfico, comenzaría a repetirse en el orden de 5 horas, si se logra obtener valores repetidos del mismo, el espacio de claves se reduce a algoritmos triviales de descifrar.

3.1.2. Encriptación

Lo primero que se hace es calcular el *check zum* del texto que se desea transmitir. Para ello se puede utilizar por ejemplo el CRC-32 del CCITT. A esto se le denomina Valor de Chequeo de Integridad o ICV.

A continuación se selecciona una de las claves y se genera el IV, usando el RC4 para obtener un *keystream* formado por la clave elegida y el IV

El siguiente paso es concatenar el texto a cifrar con el ICV y se realiza una *XOR bit* a *bit* con el *keystream,* obteniendo así el texto cifrado.

Por último se envía el IV, el número de clave seleccionada y el texto cifrado a través del aire.

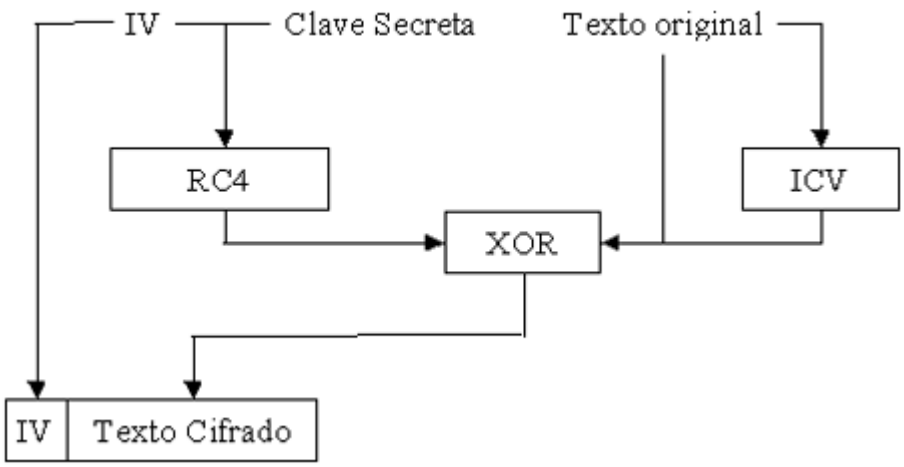

Figura. 3.3. Algoritmo WEP

3.1.3. Desencriptación

Lo primero es utilizar la clave indicada por el número de clave y el IV, ambos valores incluidos en el mensaje recibido, para generar mediante el RC4 el mismo *keystream* que se generó en el proceso de cifrado.

A continuación se realiza la XOR del *keystream* con el texto cifrado contenido en el mensaje recibido, obteniéndose así el texto original junto con el ICV.

Por último, se calcula un nuevo ICV de la misma forma que se hizo en el cifrado y se comprueba con el valor recibido en el mensaje. En caso de que los dos valores coincidan, la transmisión se realizó sin errores.

En la siguiente figura podemos ver estos pasos de forma esquemática.

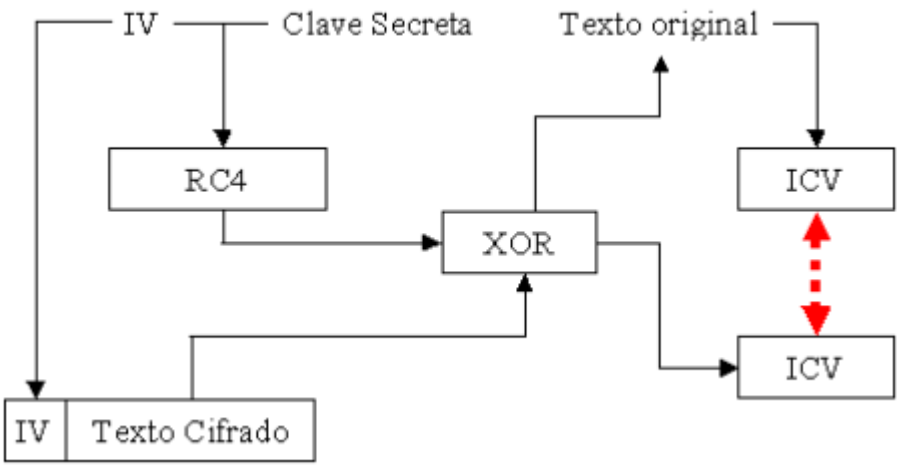

Figura. 3.4. ICV WEP

3.2. Proceso de conexión a una *wlan*

3.2.1. Mecanismos de autenticación

El estándar 802.11 define una serie de mecanismos básicos que tienen como objetivo proporcionar una seguridad equivalente a la de una red tradicional cableada. Para ello buscamos dos objetivos básicos:

• Autentificación: el objetivo es evitar el uso de la red (tanto en la *WLAN* como la *LAN* a la que conecta el AP) por cualquier persona no autorizada. Para ello, el Punto de Acceso solo debe aceptar paquetes de estaciones previamente autentificadas.

• Privacidad: consiste en encriptar las transmisiones a través del canal radio para evitar la captura de la información. Tiene como objetivo proporcionar el mismo nivel de privacidad que en un medio cableado.

• Con estos objetivos en mente se definen los mecanismos básicos de 802.11. Posteriormente se han observado deficiencias en estos mecanismos que los debilitan, y debido a ello se han desarrollado nuevos mecanismos, adicionales o en sustitución de los anteriores, como veremos posteriormente.

3.2.1.1. Open System Autentication

Es el mecanismo de autenticación definido por el estándar 802.11 y consiste en autenticar todas las peticiones que reciben. El principal problema de este mecanismo es que no realiza ninguna comprobación y, además, todas las tramas de gestión son enviadas sin ningún tipo de cifrado, incluso cuando se ha activado *WEP*.

3.2.1.2. Shared Key Autentication

Se trata del primer mecanismo de seguridad implementado, fue diseñado para ofrecer un cierto grado de privacidad, pero no puede compararse con protocolos de redes más seguros tales como IPSec para la creación de Virtual *Private Net Works (VPN).* Comprime y cifra los datos que se envían a través de las ondas de radio. Utiliza una clave secreta, utilizada para el cifrado de los paquetes antes de su retransmisión. El algoritmo utilizado para el cifrado es RC4. Por defecto, *WEP* está deshabilitado.

3.3. La seguridad en las redes 802.11

Las redes inalámbricas requieren nuevos conceptos de seguridad que se obvian en las redes cableadas. Un intruso que busque acceso a una *LAN* cableada se enfrenta irremediablemente con el problema del acceso físico a la misma. El villano necesita conectar su cable al *switch*. En una *WLAN* el problema del intruso se torna etéreo. Le basta permanecer en el área de cobertura que puede ser muy extensa para estar en contacto con la red local. Puede incluso estar en movimiento.

Esta nueva situación obliga a la búsqueda de nuevas soluciones para garantizar la seguridad de los usuarios. Voy a procurar hacer una exposición simple y rápida.

3.3.1. La situación

Como sabemos, la seguridad en redes tipo inalámbricas, es un factor muy importante debido a la naturaleza del medio de transmisión: el aire. Las características de seguridad en la *WLAN* (Red Local Inalámbrica), se basan especialmente en la protección a la comunicación entre el punto de acceso y los clientes inalámbricos, controlan el ingreso a esta red, y protegen al sistema de administración de acceso no autorizado.

Aun a ello, la falta de una recomendación que permitiera la interoperabilidad entre equipos de diferentes productores, contuvo el despliegue masivo de las WLANs. No fue sino hasta mediados de la década pasada que se publicó el estándar que dictaba las especificaciones y criterios que debían aplicarse consistentemente en la fabricación y aprovisionamiento de productos inalámbricos.

Estándares WLAN

Ante la existencia de dispositivos *WLAN* de diferentes fabricantes, se hizo necesaria la existencia de recomendaciones (contenidas en los estándares), para permitir a los productos de estas firmas, una operación adecuada entre sí y que, además, se cumpliera con un mínimo establecido de calidad y funcionalidades.

Los estándares *WLAN* principiaron con el estándar 802.11, desarrollado en 1997, por el Instituto de Ingenieros Eléctricos y Electrónicos (IEEE). Estos estándares permiten transmisiones de datos de hasta 2 Mbps, transferencias que han sido mejoradas con el paso del tiempo.

3.3.2. Las soluciones

Aún cuando las redes inalámbricas son comparables en velocidad y ciertamente más convenientes que los medios de interconexión cableados tradicionales, hay algunas limitaciones a la especificación que merecen una consideración rigurosa. La más importante de estas limitaciones está en la implementación de la seguridad.

Con la emoción de desplegar exitosamente una red 802.11*x*, muchos administradores fallan en poner en práctica aún las precauciones de seguridad más básicas.

Puesto que todas las redes 802.11*x* son hechas usando señales RF de banda alta, los datos transmitidos son fácilmente accesibles a cualquier usuario con un NIC compatible, una herramienta de escaneo de redes inalámbricas tal como ***NetStumbler*** *o* ***Wellenreiter*** y

herramientas comunes de husmeo tales como *dsniff y snort*. Para prevenir tales aberraciones del uso de redes inalámbricas privadas, el estándar 802.11b utiliza el protocolo *Wired Equivalency Privacy (WEP),* el cual está basado en RC4 con encriptación de llaves compartidas de 64- o 128-bit entre nodos o entre el *WAP* y el nodo. Esta llave cifra las transmisiones y descifra los paquetes entrantes de forma transparente y dinámica.

Los administradores fallan a menudo en emplear este esquema de cifrado de llaves compartidas, sin embargo, quizás lo hacen porque se olvidan de hacerlo o elijen no hacerlo debido a la degradación del rendimiento (especialmente en largas distancias). Al habilitar *WEP* en una red inalámbrica se puede reducir significativamente la posibilidad de intercepción de los datos.

Sin embargo, confiar en *WEP,* no es suficiente protección en contra de los usuarios maliciosos bien determinados. Hay utilitarios especializados diseñados específicamente para romper el algoritmo de encriptación RC4 *WEP* protegiendo una red inalámbrica y exponer la llave compartida. ***AirSnort*** *y* ***WEP Crack*** son dos de estas aplicaciones especializadas. Para protegerse contra esto, los administradores deberían acatar políticas estrictas con respecto al uso de los métodos inalámbricos para acceder a información confidencial. Los administradores pueden seleccionar aumentar la seguridad de la conectividad inalámbrica restringiendola solamente a conexiones SSH o VPN, lo que introduce una capa de cifrado adicional por encima de la encriptación *WEP*. Usando esta política, un usuario malicioso fuera de la red que viole el cifrado *WEP* tiene que adicionalmente descifrar la encriptación VPN o SSH, la cual, dependiendo del método de cifrado, puede emplear hasta el triple de la fortaleza con un algoritmo de 168-*bit* DES (3DES) o con algoritmos propietarios de aún mayor fortaleza. Los administradores que aplican tales políticas deberían restringir protocolos de texto plano tales como Telnet o FTP, pues las contraseñas y los datos pueden ser expuestos usando cualquiera de los ataques antes mencionados.

Un método reciente de seguridad y autenticación que ha sido adoptado por los fabricantes de equipos inalámbricos de red es *Wi-fi Protected Access* (WPA). Los administradores pueden configurar WPA en sus redes usando un servidor de autenticación que maneje las llaves para los clientes accediendo a la red inalámbrica. WPA tiene la mejora sobre la encriptación WEP en que utiliza el Protocolo de Integridad de Llaves Temporales o *Temporal Key Integrity Protocol* (TKIP), el cual es un método para utilizar una llave compartida y asociarla con la dirección MAC de la tarjeta inalámbrica de red instalada en el cliente. El valor de la llave compartida y la dirección MAC es procesado posteriormente por un *vector de inicialización* (IV), el cual es utilizado para generar una llave que encripta cada paquete de datos. El IV cambia la llave cada vez que se transmite un paquete, evitando los ataques más comunes a redes inalámbricas.

Sin embargo, WPA usando TKIP se ve como una solución temporal. Las soluciones usando cifrados de llaves más fuertes (tales como AES) están bajo desarrollo y tienen el potencial de mejorar la seguridad de las redes inalámbricas en las empresas

CAPITULO IV

DESPLIEGUE DE REDES DE AREA LOCAL INALAMBRICA

4. Despliegue de redes inalambricas y proyectos técnicos

Desde sus inicios, las tecnologías wireless han tenido un éxito imparable. Su evolución ha sido constante y los estándares actuales ya proporcionan velocidades que permiten trabajar en entornos Ethernet con cierta comodidad.

Quizás este es el motivo por el cual, últimamente el despliegue de los entornos inalámbricos en paralelo con los entornos cableados ha sido espectacular.

Su simplicidad de instalación que basta con poco menos que colocar un punto de acceso wireless pinchado a la red wired y esta ha permitido este despliegue masivo.

Sin embargo, y desde el punto de vista del administrador de red, no deben pasarse por alto muchos efectos colaterales de este despliegue.

El punto más criticado de estos entornos es quizás la facilidad de desencriptación, pero no cabe duda de que hay otras fuentes de problemas.

A modo de ejemplo podemos citar el acceso no controlado a la red, la validación de usuarios y la asignación de direcciones con lo que esto comporta a estos nuevos usuarios.

El presente capitulo intenta abordar cómo debe hacerse un despliegue de una red wireless sobre una red wired, manteniendo la seguridad y controlando los accesos.

A nivel práctico, expondremos también los resultados concretos que han llevado a la creación de un wireless-gateway implementado con IPtables y Linux.

4.1. Metodología para el despliegue de una red 802.11

Las tecnologías wireless están entrando en el mundo de la redes de datos con tanta fuerza como hace anos años irrumpiera la telefonía móvil en el mundo de la voz.

La movilidad en sistemas de voz ya está asumida, y quizás por ello el usuario espera obtener funcionalidades análogas para las nuevas redes de datos inalámbricas.

De todas formas, y pese al paralelismo, la problemática no es la misma. Simplificando el problema, encontramos, al menos dos frentes. Desde el punto de vista del usuario, queremos darle siempre las mismas funcionalidades, con independencia de su ubicación o punto de acceso.

Desde el punto de vista del gestor de red, es necesario un control de los accesos que se están realizando, ya que, en último término, serán accesos conectados directamente a la red cableada.

4.1.1. Planificación radioeléctrica

REGISTRO PARA USO DE FRECUENCIAS – PERSONAS NATURALES O JURIDICAS

Los interesados en instalar y operar sistemas de espectro ensanchado de gran alcance, sean estos PRIVADOS o de EXPLOTACIÓN, en cualquier parte del territorio nacional, deberán presentar los siguientes requisitos:

Información Legal

Solicitud dirigida al Señor Secretario Nacional de Telecomunicaciones, indicando el tipo de Servicio al cual aplica; debe también constar el nombre y la dirección del solicitante (para personas jurídicas, de la compañía y el nombre de su representante legal).

Copia de la cédula de ciudadanía (para personas jurídicas, del representante legal).

Recibo de pago de la contribución del 1/1000 del valor del contrato de los servicios profesionales del ingeniero de telecomunicaciones a cargo del sistema de radiocomunicaciones, que exceda el valor de USD 12 conforme lo determina el Artículo 26 de la Ley de Ejercicio Profesional de la Ingeniería.

Otros documentos que la SENATEL solicite.

Información Técnica

Estudio técnico del sistema elaborado en los formularios disponibles en la página Web del CONATEL, suscrito por un ingeniero en electrónica y telecomunicaciones, con licencia profesional vigente en una de las filiales del Colegio de Ingenieros Eléctricos y Electrónicos del Ecuador (CIEEE) y registrado para tal efecto en la SENATEL.

Copia de la licencia profesional vigente del ingeniero que ha realizado el estudio de ingeniería correspondiente

Para la planificación radioelectrica se debe tomar en cuenta lo siguientes puntos:

a. La capasidad total maxima teniendo en cuenta el ancho de banda por usuario.

b. La capacidad del access tomando en cuenta si es 802.11 a,b,g o n.

c. El trougput efectivo del access para esta aplicacion.

d. Tomar en cuenta el factor de simultaneidad de la conexion de los clientes.

Con estos parametros procedemos a calcular el ancho de banda efectivo para la comunicacion de tantos telefonos o softpones IP.

Ahora tenemos que analizar el espacio en el cual va a cubrir el access, tomando en consideracion que el espacio a cubrir fisicamente tiene que ser menor al de cobertura del access o a su ves realizar el calculo de el numero de access se necesitaran para la total covertura del espacio requerido.

Para determinar la ubicacion mas adecuada de los Putos de aceso lo mas recomendable es un proceso iterativo, mediante el cual se ubican los puntos y se verifican si cumplen todos lo requisitos, en caso negativo se realizara un cambio de posicion hasta que el resultado final sea el esperado, los puntos finales se lo debe ubicar en un plano para su futura certificacion.

Finalmente en una memoria tecnica se tendra en cuenta los siguentes parametros de cada access:

- Denominacion del punto de Aceso.
- Ubicacion segun referencia del Plano.
- Canal Asignado a la trasmision.

- Frecuencia de trabajo.
- Porcentaje del area de interes cubierta.
- Nivel de senal minimo estimado.
- Capacidad media de carga
- Capacidad media de pico.

4.1.2. Emisiones radioeléctricas

Los valores de las emisiones radioelectricas para la frecuencia de 2.4 Ghz en niveles maximos en los puntos de acceso se detallan a continuacion:

Nivel de Referencia (Smax Permitida)	10 W/m2
Potencia por canal	100 mW
Numero de canales Simultaneos	1
Ganancia de las antenas	<= 14 dbi
P.I.R.E.	100 mW
Factor de Reflexion	4
Distancia de Seguridad	6cm
Perdidas en los cables	0.5 db/m

La distancia de seguridad resultante de 6 cm calcualda como:

$$Dmax = sqrt (M . PIRE / 4 pi Smax)$$

quedara cubierta por la ubicación de los Puntos de Acceso proximos al techo y fuera del alcance de los usuarios.

4.1.3. Mecanismos y políticas de seguridad

El despliegue de las redes wireless suele ir asociado a su implantación en la red cableada presentando los siguientes problemas:

• La configuración de los puntos de acceso es sumamente sencilla, muchas veces con cómodas interfaces web. Esto permite que, en el límite, se puede llegar a situaciones en las que cada punto de acceso mantiene su propia política y ésta es sólo responsabilidad de la persona que lo ha configurado.

• El punto de acceso se convierte en un punto potencial de entrada de usuarios no autorizados a la red. No hay un estándar para el control de acceso a través del access-point (y en muchos casos tampoco se soporta esta funcionalidad).

• Es muy difícil desplegar una política común a toda la red wireless. Si la red es multifabricante, no existe una forma trivial de hacerlo (y en ocasiones es imposible). Si es monofabricante, estamos ligados a una marca concreta.

• El despliegue de políticas en función del punto de acceso hace altamente probable que el usuario tenga funcionalidades diferentes según el punto de conexión, cosa que va contra el principio de ‘acceso basado en usuario’.

• La configuración segura más allá de WEP no es estándar, no suele venir activada por defecto y en muchos casos implica que el fabricante sea el mismo para el punto de acceso y la tarjeta del cliente.

Estos problemas no son nuevos, y de hecho ya existen soluciones en el mercado que intentan resolverlos de forma más o menos satisfactoria.

Sin entrar en detalle, las alternativas son:

- Despliegue sin control: simple, pero no es seguro ni escalable ni homogéneo.
- Red monofabricante con control específico.
- Red paralela a la cableada de forma independiente: supone un elevado coste.
- Productos comerciales: como BlueSocket o AirWave, en general con funcionalidades más encaradas a la explotación comercial de hot-spots.

4.1.4. Estructura del proyecto

4.2. Servidores SIP

SIP son las siglas en inglés del Protocolo para Inicio de Sesión, siendo un estándar desarrollado por el la Fuerza de Tarea en Ingeniería de Internet (IETF), identificado como RFC 3261, 2002. SIP es un protocolo de señalización para establecer las llamadas y conferencias en redes IP. El inicio de la sesión, cambio o término de la misma, son independientes del tipo de medio o aplicación que se estará usando en la llamada; una sesión puede incluir varios tipos de datos, incluyendo audio, video y muchos otros formatos. SIP se originó a mediados de los años 90 (aproximadamente al mismo tiempo que el H.323 se presentaba como un estándar) para facilitar la manera en que la gente podía ver una sesión por multidifusión en IP como el lanzamiento del trasbordador espacial en el MBone. El desarrollo de SIP puede tener tanto impacto como el protocolo estándar HTTP, la tecnología que está detrás de las páginas Web y que permite dentro de una simple página el uso de enlaces o vínculos hacia otros textos, audio o video u otras páginas. Mientras que HTTP cumple con esta integración en una página WWW, SIP integra contenido diverso administrando la sesión. SIP se ha reconocido rápidamente como

estándar para comunicaciones integrales y aplicaciones que usan la presencia (Presencia significa la atención que una aplicación da a la ubicación y disponibilidad de un usuario)

SIP fue modelado después de otros protocolos de Internet basados en texto, como SMTP (correo electrónico) y HTTP (páginas Web) y se diseñó para establecer, cambiar y terminar llamadas entre uno o más usuarios en una red IP de manera independiente al contenido de la llamada. Como HTTP, SIP traslada el control de la aplicación al punto terminal, eliminando la necesidad de funciones centrales de conmutación.

4.2.1. Características en Software

Los principales componentes de la arquitectura SIP son:

1. Agente de Usuario SIP

El Agente de Usuario es el software SIP en el punto terminal o estación terminal. Funciona como un cliente cuando hace las peticiones de inicio de sesión, y también actúa como un servidor cuando responde a las peticiones de sesión. Por tanto, la arquitectura básica es de naturaleza cliente/servidor.

El Agente de Usuario es “inteligente”, en el sentido que almacena y administra el estado de la llamada. El Agente de Usuario establece las llamadas usando una dirección parecida a las de correo electrónico, o un número telefónico (E.164). Por ejemplo: SIP:usuario@servidor.universidad.edu. Esto hace que los URL de SIP sean fáciles de asociar con la dirección de correo electrónico del usuario. Los Agentes de Usuario pueden aceptar y recibir llamadas de otros Agentes de Usuario son componentes adicionales SIP. Los siguientes elementos dan funcionalidades y niveles de administración extra al esquema SIP.

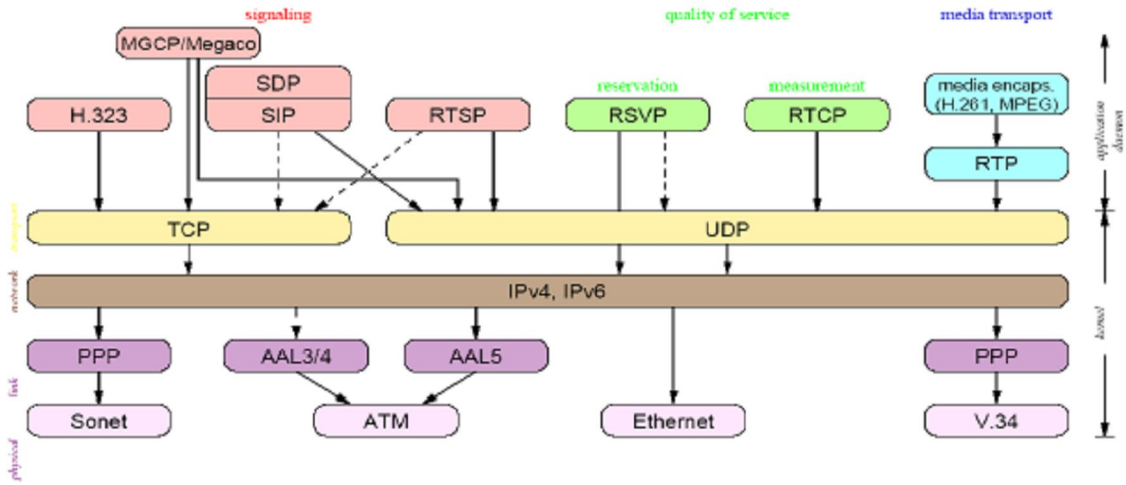

Figura. 4.1.User Agent Flow

a. *Servidor Proxy SIP*

Un tipo de servidor intermedio SIP es el Servidor Proxy SIP. Los Servidores Proxy reenvían peticiones desde el Agente de Usuario hacia el siguiente Servidor SIP, y retienen la información por cuestiones de contabilidad o facturación. Adicionalmente, el Servidor Proxy SIP puede operar en forma constante (como un circuito) o dependiente de la conexión (vía TCP). El Servidor constante SIP puede dirigir las llamadas entrantes hacia diversas extensiones que están activas a la vez y la primera en responder tomará la llamada. Esta capacidad significa que se puede especificar el teléfono SIP en el escritorio, el teléfono móvil SIP y la aplicación de videoconferencia en casa de tipo SIP y todos esos aparatos "sonarían" cuando llegue una llamada que está tratando de localizar al usuario, de tal forma que al contestar en cualquiera de esos medios se inicia la conversación y los otros dispositivos dejan de sonar. Los Servidores Proxy SIP pueden usar varios métodos para intentar resolver la dirección destino solicitada, incluyendo búsquedas en el DNS, en bases de datos o relevando la labor hacia el siguiente Servidor Proxy.

b. *Servidor de Redireccionamiento SIP*

Un segundo tipo de servidor intermedio SIP es el Servidor de Redireccionamiento. El papel de estos servidores es responder a la resolución de nombres y la ubicación del usuario. El Servidor de Redireccionamiento responde a las peticiones de los Agentes de Usuario proporcionando la información acerca de la dirección del servidor requerido, de tal forma que el cliente puede contactar la dirección puntualmente.

2. Registro SIP

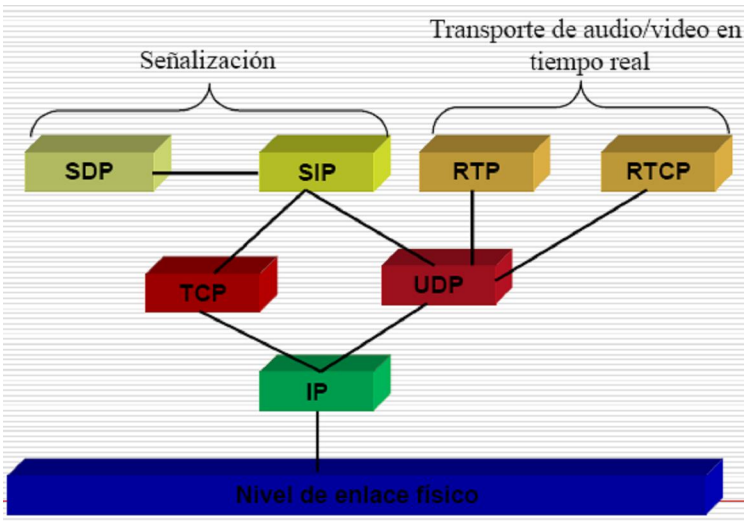

Figura. 4.2.Registro SIP

El Registro SIP da un servicio de información de ubicación; recibe información del Agente de Usuario y la almacena para proporcionarla a otros Agentes de Usuario.

La arquitectura SIP usa el Protocolo para Descripción de Sesión (SDP). SDP fue una herramienta inicial para la conferencia en multidifusión de IP desarrollada para describir sesiones de audio, video y multimedia. De hecho, cualquier tipo MIME (Extensión Multipropósito de Correo en Internet) se puede describir, similar a la facultad

de correo electrónico para interpretar todos los tipos de archivos adjuntos en un mensaje. La descripción de sesión se puede usar para negociar los tipos de medios compatibles.

Como resultado de esta arquitectura, la dirección SIP del usuario remoto siempre es la misma (por ejemplo: *sip:usuario@servidor.universidad.edu*) pero en lugar de estar vinculada a una dirección estática se comporta como una dinámica que refleja la ubicación de usuario actualmente. La combinación de Servidores Proxy y de Redireccionamiento SIP da al protocolo una arquitectura flexible; el usuario puede emplear varios esquemas, simultáneamente, para localizar a los usuarios y es lo que convierte a la arquitectura SIP en algo ideal para la movilidad. Aún cuando es usuario remoto está en un dispositivo móvil, el Servidor Proxy y el de Redireccionamiento pueden reenviar la petición de conexión al lugar en donde se encuentra el usuario. Las sesiones pueden incluir a varios participantes, similar a lo que ocurre en una llamada multipunto H.323. Las comunicaciones dentro de una sesión de grupo pueden ser vía multidifusión o una malla de conexiones unidifusión, o una combinación de ambas.

Otro resultado de la arquitectura SIP es la manera natural en la que se adapta a un ambiente de colaboración ya que permite el uso de varios tipos de datos, aplicaciones, multimedia, etc, con una o más personas.

- Cierto tipo de “reenvío de llamada” permite a los usuarios especificar donde están y las llamadas entrantes serán reenviadas ahí o se puede elegir el reenvío hacia el “correo de voz” o cualquier máquina contestadora
- Los participantes en una llamada pueden controlar el enlace; esto permite que uno o más personas decidan incluir a otro individuo o cancelar una conexión en la llamada.
- Posibilidad de responder a una llamada con un tipo de medio distinto; esto facilita, por ejemplo, que una secuencia de voz entrante sea respondida con una página Web.
- Información de “Presencia” – El Agente de Usuario puede emplearse para indicar dónde está presente el usuario (disponible para tomar la llamada) o ausente (no disponible para tomar la llamada)

4.2.2. Protocolo IAX

Inter-Asterisk eXchange protocol es uno de los protocolos utilizado por Asterisk, un servidor PBX de código abierto patrocinado por Digium. Es utilizado para manejar conexiones VoIP entre servidores Asterisk, y entre servidores y clientes que también utilizan protocolo IAX.

IAX es robusto, lleno de novedades y muy simple en comparación con otros protocolos. Permite manejar una gran cantidad de *códecs* y un gran de número de *streams*, lo que significa que puede ser utilizado para transportar virtualmente cualquier tipo de dato. Esta capacidad lo hace muy útil para realizar videoconferencias o realizar presentaciones remotas.

IAX utiliza un único puerto UDP, generalmente el 4569, para comunicaciones entre puntos finales para señalización y datos. El tráfico de voz es transmitido *in-band*, lo que hace a IAX un protocolo casi transparente a los cortafuegos y realmente eficaz para trabajar dentro de redes internas. En esto se diferencia de SIP, que utiliza una cadena RTP *out-of-band* para entregar la información.

IAX soporta Trunking (red), donde un simple enlace permite enviar datos y señalización por múltiples canales. Cuando se realiza *Trunking*, los datos de múltiples llamadas son manejados en un único conjunto de paquetes, lo que significa que un datagrama IP puede entregar información para más llamadas sin crear latencia adicional.

4.2.3. Diferencias IAX y SIP

Ancho de Banda

IAX utiliza un menor ancho de banda que SIP ya que los mensajes son codificados de forma binaria mientras que en SIP son mensajes de texto**.** Asimismo**,** IAX intenta reducir al máximo la información de las cabeceras de los mensajes reduciendo también el ancho de banda.

NAT

En IAX la señalización y los datos viajan conjuntamente con lo cual se evitan los problemas de NAT que frecuentemente aparecen en SIP. En SIP la señalización y los datos viajan de manera separada y por eso aparecen problemas de NAT en el flujo de audio cuando este flujo debe superar los routers y firewalls. SIP suele necesitar un servidor STUN para estos problemas.

Estandarización y uso

SIP es un protocolo estandarizado por la IETF hace bastante tiempo y que es ampliamente implementado por todos los fabricantes de equipos y software**.** IAX está aun siendo estandarizado y es por ello que no se encuentra en muchos dispositivos existentes en el mercado.

Utilización de puertos

IAX utiliza un solo puerto (4569) para mandar la información de señalización y los datos de todas sus llamadas. Para ello utiliza un mecanismo de multiplexión o "trunking". SIP, sin embargo utiliza un puerto (5060) para señalización y 2 puertos RTP por cada conexión de audio (como mínimo 3 puertos). Por ejemplo para 100 llamadas simultaneas con SIP se usarían 200 puertos (RTP) más el puerto 5060 de señalización. IAX utilizaría sólo un puerto para todo (4569)

Flujo de Audio

En SIP si utilizamos un servidor la señalización de control pasa siempre por el servidor pero la información de audio (flujo RTP) puede viajar extremo a extremo sin tener que pasar necesariamente por el servidor SIP**.** En IAX al viajar la señalización y los datos de forma conjunta todo el tráfico de audio debe pasar obligatoriamente por el servidor IAX**. E**sto produce una aumento en el uso del ancho de banda que deben soportar los servidores IAX sobretodo cuando hay muchas llamadas simulataneas.

Otras Funciones.

IAX es un protocolo pensado para VoIP y transmisión de video y presenta funcionalidades interesantes como la posibilidad de enviar o recibir planes de marcado (dialplans) que resultan muy interesante al usarlo conjuntamente con servidores Asterisk. SIP es un protocolo de proposito general y podría transmitir sin dificultad cualquier información y no sólo audio o video.

4.3. Troncales y centrales

4.3.1. Troncales SIP

Existe una gran variedad de troncales basadas en SIP, pero los pasos de autentificación y acceso son los mismos que el protocolo SIP utiliza, la diferencia radica en que ahora el usuario es el UAS y no el UAC.

4.3.1.1.Descripción ejemplos

Debido a la fácil escalabilidad del protocolo SIP podemos ver algunas formas:

- ✓ Detrás de un Firewall

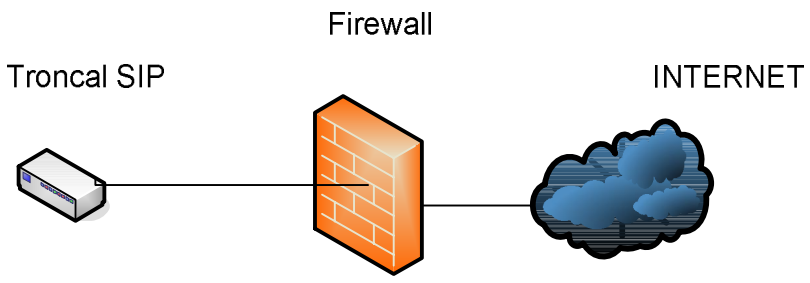

Figura. 4.3. Detras de Firewall

✓ Con IP publica o acceso directo

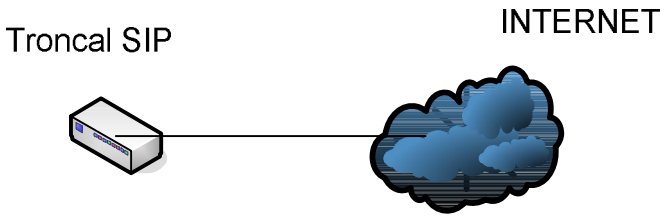

Figura. 4.4. Directo IP

✓ En la misma LAN

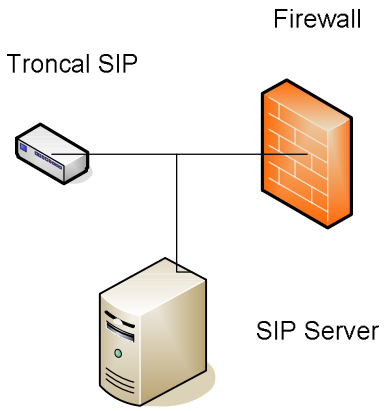

Figura. 4.5. En la misma LAN

4.3.2. Troncales IAX

Al contrario que SIP, IAX no tiene troncales mas que las propias tarjetas Digium detro de las centrales, por lo que si se quiere escalabilidad IAX no es el protocolo recomendado para este punto.

4.3.2.1. Descripción ejemplos

- ✓ En la misma LAN

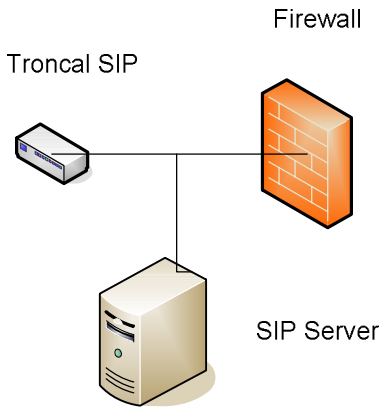

Figura. 4.6. En la misma LAN - IAX

Las aplicaciones a implementar son las siguientes:

Aplicación 1:

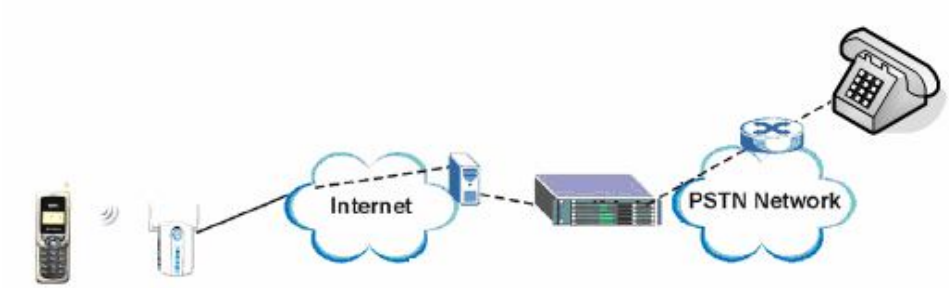

Figura. 4.7. Aplicación 1

La Primera aplicación es la comunicación de un Teléfono Wifi a través de un servidor SIP y luego una conmutación con la red de telefonía fija para una llamada a un teléfono fijo y una grabación de calidad.

Aplicación 2:

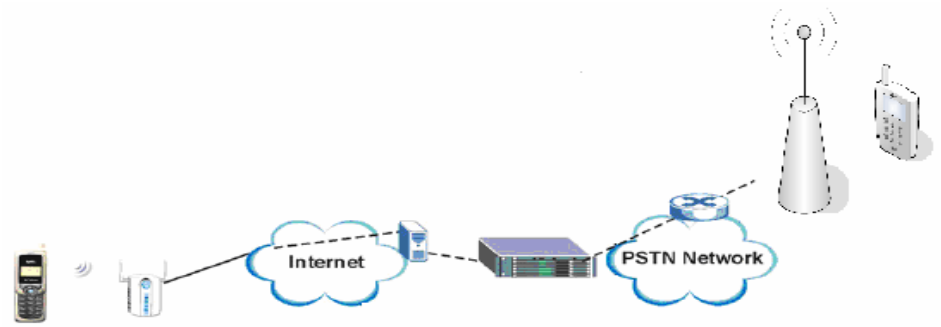

Figura. 4.8. Aplicación 2

La Segunda aplicación es la comunicación de un Teléfono Wifi a través de un servidor SIP y luego una conmutación con la red de telefonía móvil para una llamada a un teléfono celular y una grabación de calidad.

4.3.3. Funcionamiento y verificación de la red

A la hora de hacer el diseño de la solución, los puntos que consideramos fundamentales son los siguientes:

• El usuario debía obtener siempre idéntica funcionalidad, independientemente del punto de acceso que le diera cobertura.

• El dispositivo de acceso no debía requerir ninguna reconfiguración para acceder a la red. Los puntos de acceso se conectan a la red con la configuración “default”.

• Deberiamos permitir el acceso a usuarios “anónimos”, pero en tal caso, con una funcionalidad limitada.

• No haría falta gestionar configuraciones complejas de seguridad ya que ésta se gestionaría a nivel de aplicación o mediante el servidor de aplicacion.

• Debería ser una solución independiente de fabricante.

• La solución debería ser de bajo coste.

En un enfoque global lo que se propone es la activacion por medio de un servidor a los usuarios, es decir la concentracion de todo el trafico proveniente de varios access hacia un servidor central.

En este punto sera el servidor principal el que se encarge de dar las politicas de acceso y privilegios a cada uno de los usuarios conectados, tambien asi definiremos un IPS y un IDS para que nuestro servidor sea mas fuerte y no pueda ser violable.

La implementación concretamente se realizara en sistema linux con herramientas como squid, iptables, y modulos de seguridad como IDS e IPS

La idea central es dotar a la red wireless de un funcionamiento completamente transparente para el usuario, garantizando a la vez el control en el acceso. Este control debía ser lo suficientemente granular como para dar accesos diferenciados a usuarios convenientemente autentificados.

4.4. Configuraciones Telefono Wi-Fi IP, Gateway y Central IP

4.4.1. Configuraciones Wifi phone IP

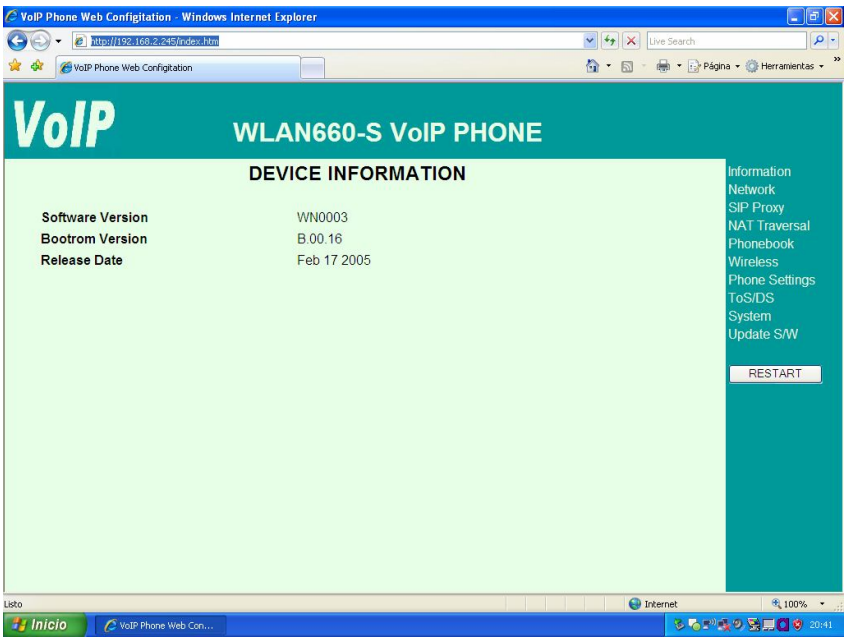

Figura. 4.9. Pagina Wi-Fi Phone - Configuracion

La configuración del Telefono Ip la iremos redactando paso a paso tomando en cuenta los datos del proveedor de servicios. Como podemos ver el acceso a la configuración del Telefono IP la realisamos a traves de cualquier browser de la siguiente manera *http://IP-wifi-phone*.

Figura. 4.10. Pagina Wi-Fi Phone – Configuración de Red

Una ves adentro del telefono procedemos a configurar el modo de acceso según sea el caso de la red Wireless con STATIC o DHCP.

Figura. 4.11. Pagina Wi-Fi Phone – Configuración de SIP PROXY

En la parte SIP PROXY configuramos los parámetros del telefono Wifi-IP como es:

- Sip URI

  Es la cuenta de usuario con la direccion del dominio mas el puerto de comunicación.

- Sip Server Address

  En este espacio configuraremos unicamente el nombre del servidor SIP de registro, obviamente q si el servidor de registro no tiene asignado un nombre se procedera a insertar la IP.

- Sip Server Port

  Se configurara el puerto TCP por el cual se realizara el paso d todas las peticiones propias de comunicación entre UAC y el UAS.

- Registrar Server Addres

  Aquí pondremos exclusivamente la direccion del servidor de registro no el servidor de Acciones.

- Registrar Server Port

  Se configurara el puerto TCP por el cual se realizara el paso de todas las peticiones propias de comunicación entre UAC y el UAS como servidor de Registro.

- Register Expiry Time

  Este es el tiempo en mili segundos en el cual el UAC realisara peticiones al UAS para cumplir el register.

- Registrar Username

  Es el campo en el que se procedera al ingreso del usuario para la conexión con el UAS.

- Registrar Password

  Es el campo en el que se procedera al ingreso del password para la conexión con el UAS.

Figura. 4.12. Pagina Wi-Fi Phone – Configuración NAT

El NAT Traversal se lo configurara en el servidor SIP y no en los SIP PHONE debido a que un usuario generalmente no posee los conocimientos para saber que tipo de esta en la Red, por este sentido lo ponemos deshabilitado.

Figura. 4.13. Pagina Wi-Fi Phone – Configuración Wireless

En el caso de que la red sea encriptada esl SIP- Phone tine la actibilidad de poder ingresar la calve para poder acceder al acceso inalambrico o a su ves podemos escoger entre Modo Infraestructura o Modo Ad-Hoc.

Figura. 4.14. Pagina Wi-Fi Phone – Configuración Telefono

En Phone Settings podemos configurar el codec dependiendo del codec que el UAC soporte. El valor del speaking y del listening depende del usuario inclusive puede ser cambiado manualmente mientras ocurre la conversación.

El DTMF se lo configura como Outband debido a que es un SIP-UAC no asi si es el caso de un IAX-UAC debera configurarse como Inband.

4.4.2. Configuración del Servidor SIP

A continuacion veremos la configuracion del Servidor SIP con las caracteristicas para que las extenciones puedan ser autentificadas desde el Internet.

El siguiente cuadro es donde nosotros especificamos los puertos.

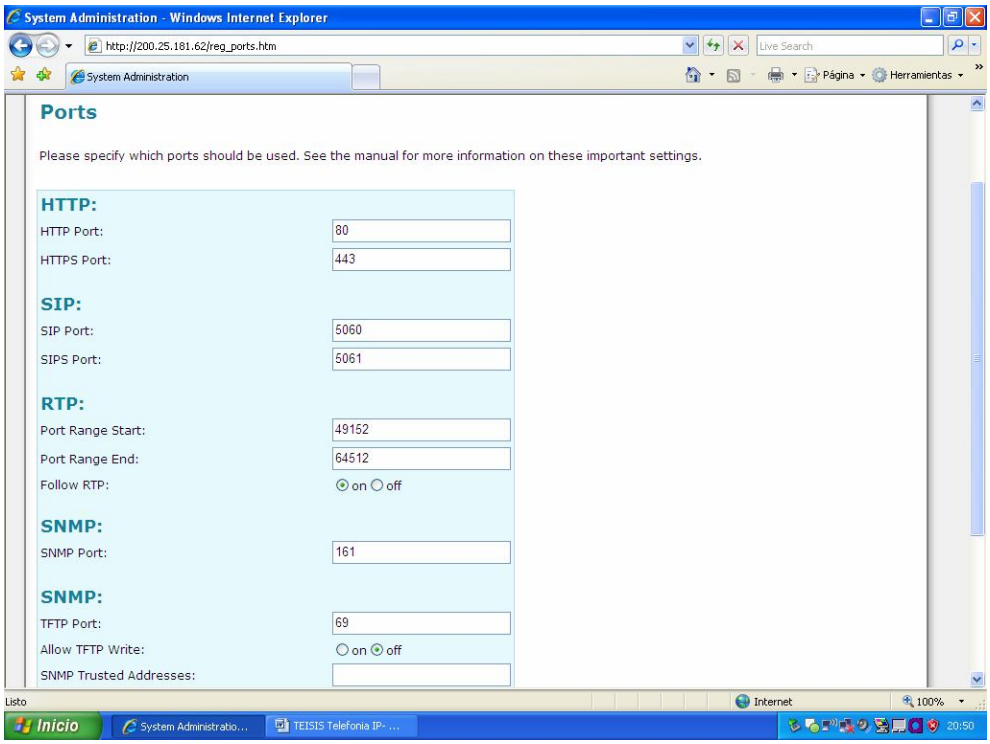

Figura. 4.15. Pagina SIP Server – Configuración Puertos

Una ves configurado los puertos por los cuales se va a realisar la comunicación entraremos a lo que es la configuración de una extencion remota del UAS mediante los siguientes parámetros:

- El primer parámetro es el número de la extencion y el user Agent aplicado a esta extencion mas la contraseña con la que se va a autentificar.
- Luego de esto procedemos a ingresar un Dial Plan en el cual permitiremos los diferentes permisos de marcado para el UAC.
- Adicionalmente configuraremos el Buzon de Mensajes con su respectivo PIN.

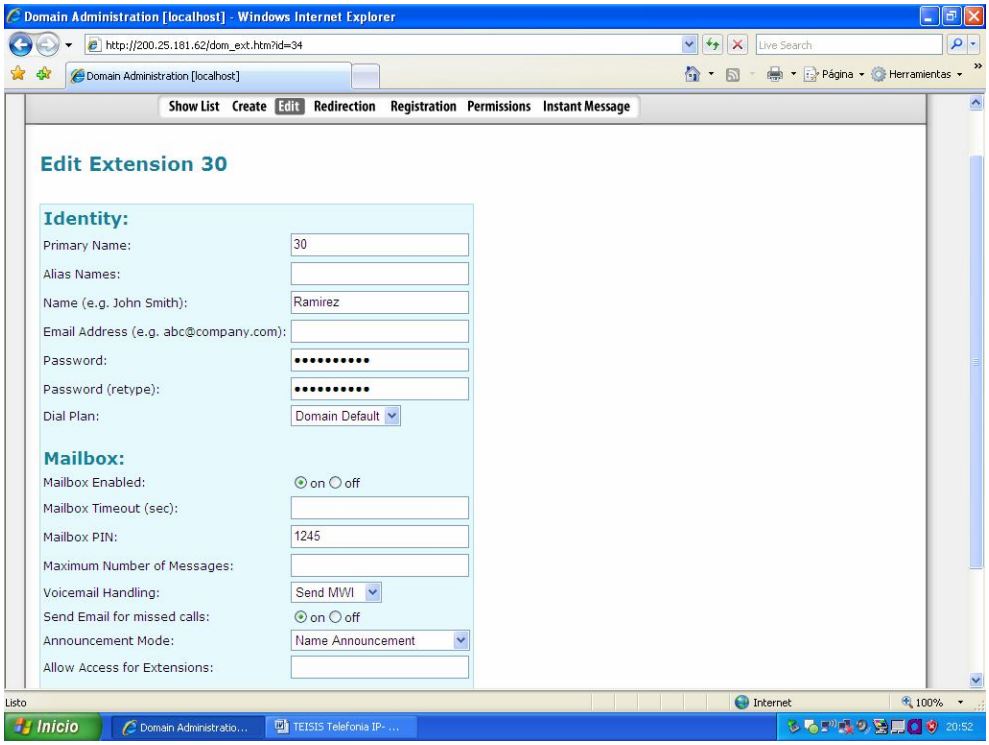

Figura. 4.16. Pagina SIP Server – Configuración Extensión

En el servidor de registro podemos ver como se registra el usuario con un OPTION indicando de que no mas es factible realisar con este usuario, adicionalmnte vmos que esta extencion tiene un doble registro indicando asi que es conmutación de paquetes y no de circuitos.

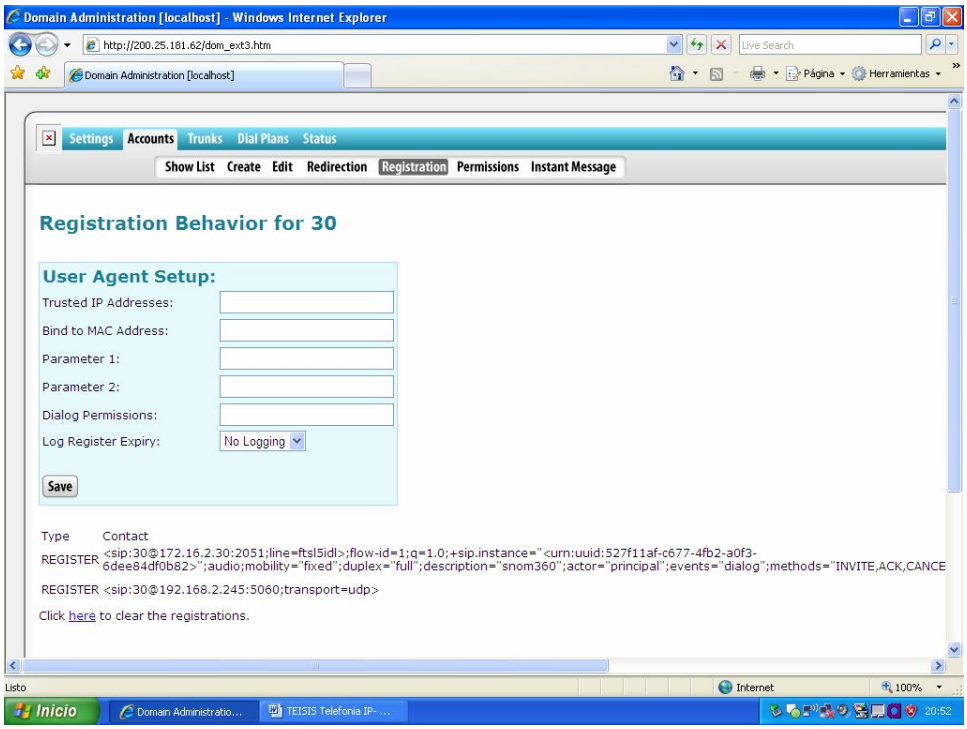

Figura. 4.17. Pagina SIP Server – Configuración Registro

Una ves configurado lo referente al UAC procemos a la coniguracion del Gateway y el UAS para la conmutación con la red PSTN del provedor de telefonia Andinatel.

Primero en el UAS creamos una Troncal por la cual van a salir las llamadas hacia el Gateway en formato SIP.

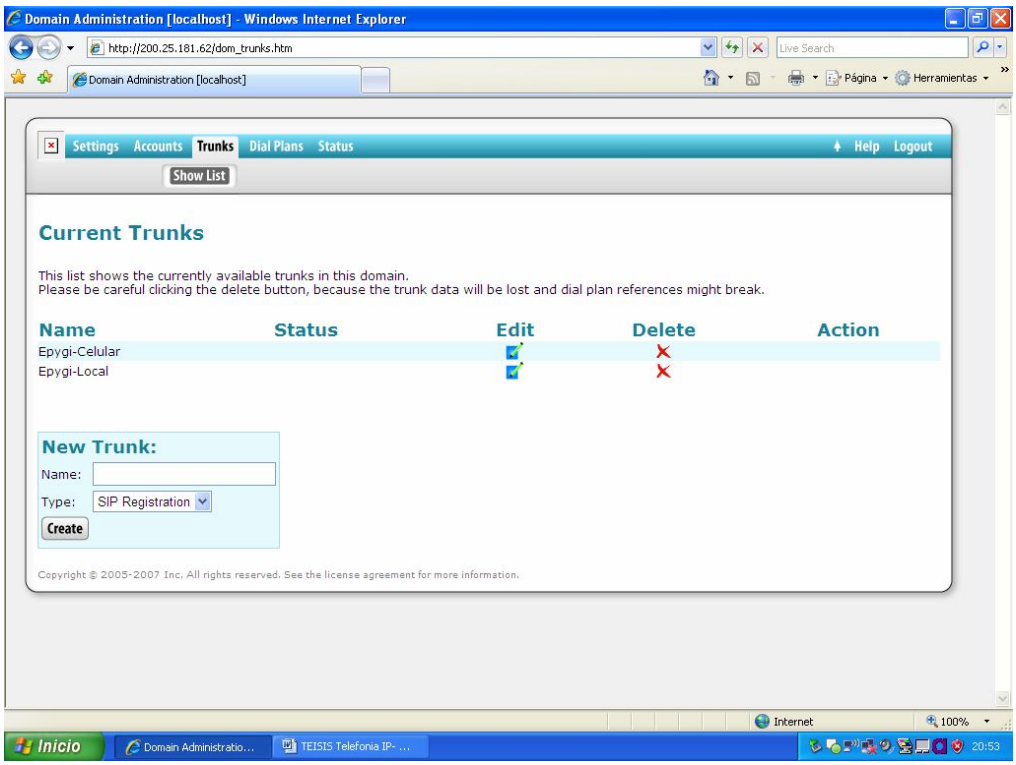

Figura. 4.18. Pagina SIP Server – Configuración Troncales

En la creación de la troncal debemos tomar en cuenta que el paquete va a ser formado por los diferentes dispositivos y configuraciones que se realisaron antes.

En este caso solo vamos a ingresar el medio final de contacto del gateway como es la IP del Gateway o el Dominio asignado para el MGC.

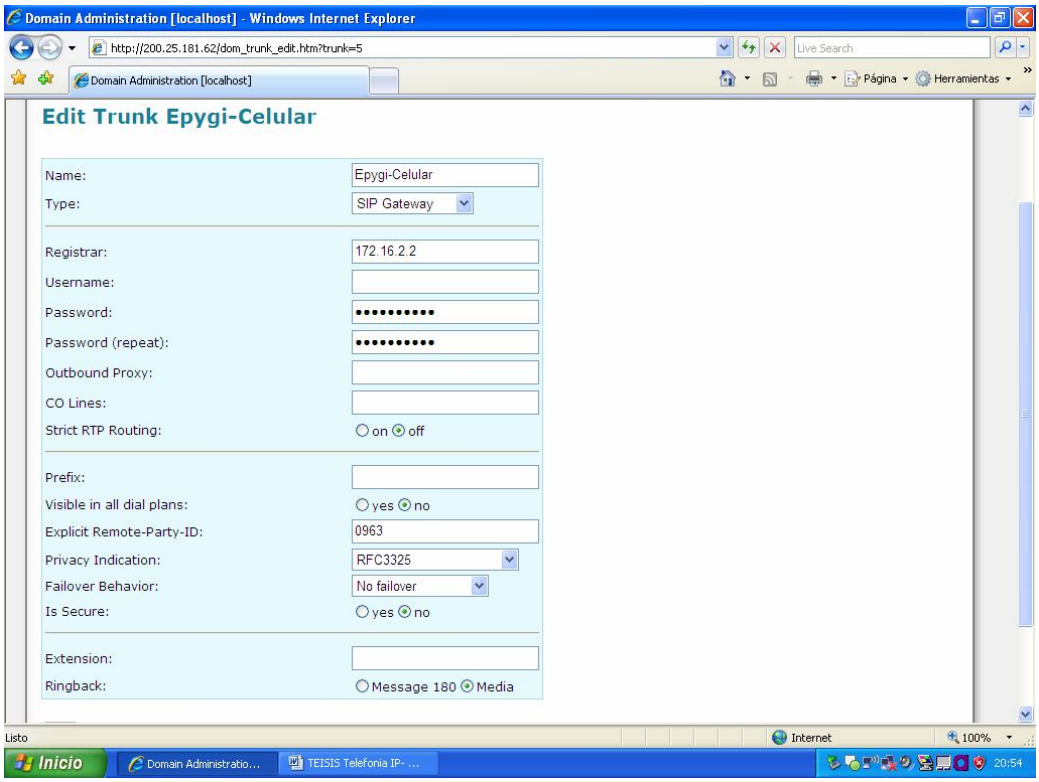

Figura. 4.19. Pagina SIP Server – Configuración Troncal Celular

Rigiendose a la RFC 3325 enviamos un paquete con la cabecera 0963 para indicar que toda llamda que salga por esta troncal sea tratada con proceso 0963 previamente establecido en el gateway.

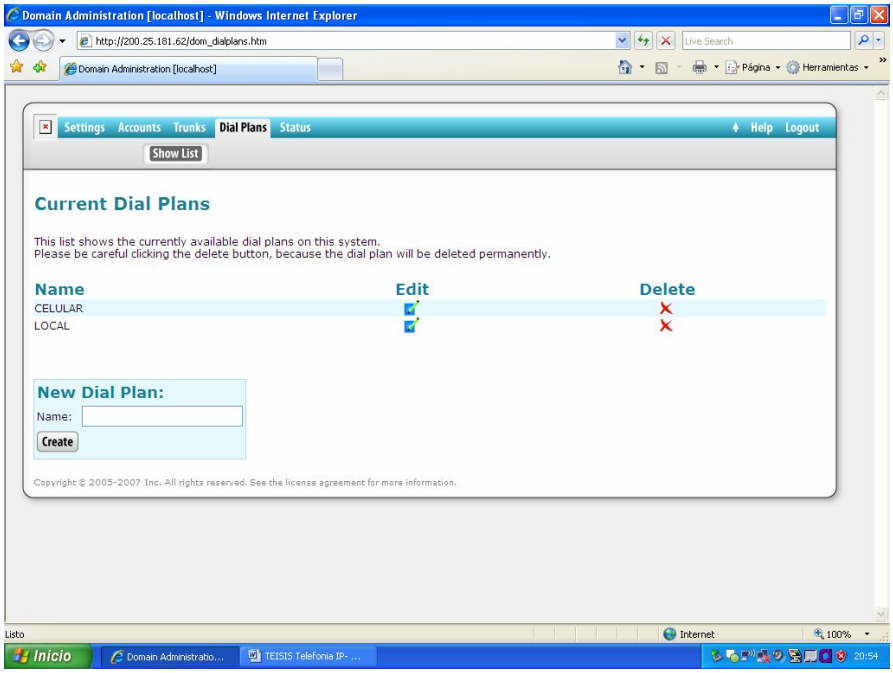

Figura. 4.20. Pagina SIP Server – Configuración Dial Plan

Luego de lo anterior procedemos a configurar los Dial Plan a los cuales van a ser ingresados los UAC.

La forma mas facil de crear las reglas para los Dial Plan es basarse en el sistma de marcado SIP, es decir usuario@dominio.naturalidad. En este caso podemos observar que la regla permite que pase solo los numeros 096 y cualquier otro numero agregado a cualquier dominio.

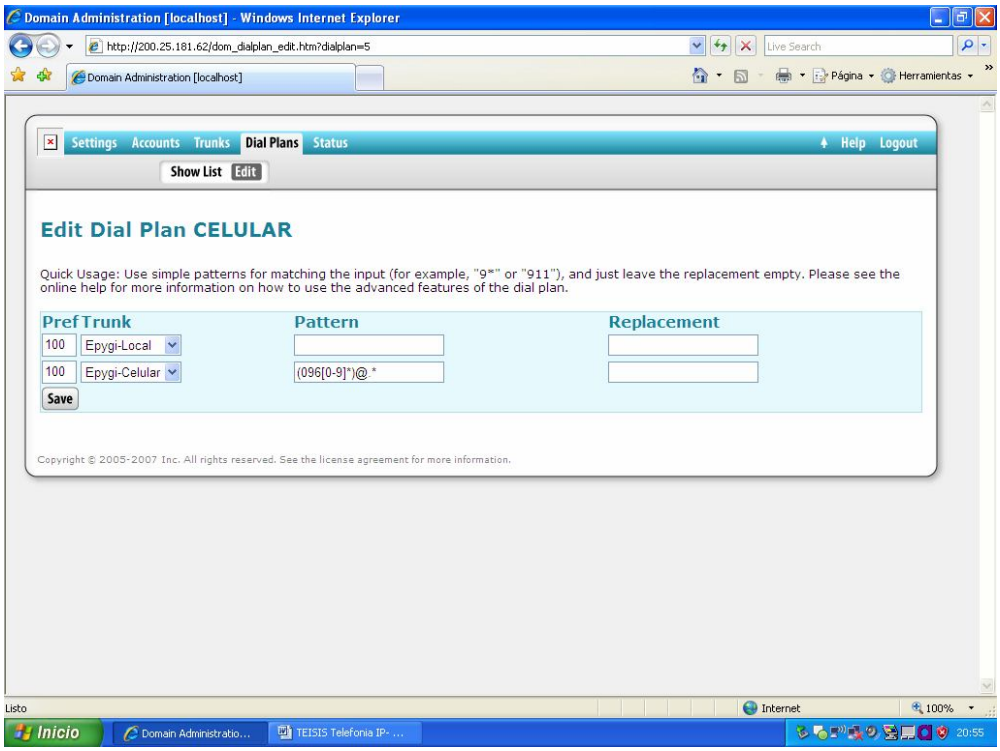

Figura. 4.21. Pagina SIP Server – Configuración Dial Plan CELULAR

Una ves realisado todas las configuraciones anteriores procedemos a chequear los Log SIP para verificar los errores que puedan producir.

A continucion vemos el Log del registro del Wifi Phone en el UAS.

Figura. 4.22. Pagina SIP Server – Log File – Register 1

Figura. 4.23. Pagina SIP Server – Log File – Register 2

A continucion vemos el Log de una llamda desde el Internet hacia el numero 2407560 realizado por el Wi-Fi Phone

LOG 2407560

Logfile

Clear or Reload the log.

[8] 20071028210209: Send Packet 183
[6] 20071028210209: SIP Tr udp:200.69.181.76:5060:
SIP/2.0 183 Session Progress
Via: SIP/2.0/UDP 192.168.2.245:5060;branch=z9hG4bK3d65f2cd8485cf;rport=5060;received=200.69.181.76
From: Carlos <sip:30@200.25.181.62;user=phone>;tag=4BA2394127609C2E2E13
To: <sip:2407560@200.25.181.62;user=phone>;tag=1736886986
Call-ID: 31726-D1B9-1317-32F0-DF63BDDFC232@192.168.2.245
CSeq: 2 INVITE
Contact: <sip:2407560@200.25.181.62:5060;transport=udp>
Supported: 100rel, replaces
Allow-Events: refer
Allow: INVITE, ACK, CANCEL, BYE, REFER, OPTIONS, PRACK, INFO
Accept: application/sdp
User-Agent: Master_Box_IP/1.5.2.7
Content-Type: application/sdp
Content-Length: 204

v=0
o=- 1541178539 1541178539 IN IP4 200.25.181.62
s=-
c=IN IP4 200.25.181.62
t=0 0
m=audio 60166 RTP/AVP 0 101
a=rtpmap:0 pcmu/8000
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-11

```
a=sendrecv
[6] 20071028210210: SIP Rx udp:172.16.2.2:5060:
SIP/2.0 180 Ringing
Via: SIP/2.0/UDP 172.16.2.1:5060;rport=5060;branch=z9hG4bK-94301e08db2bb7f7033668fbcf6475d2
To: <sip:2407560@172.16.2.2;user=phone>;tag=11924723607e0b5daf-4d65-42f8-826a-2a5757896976
From: "Ramirez" <sip:30@172.16.2.2>;tag=1551698757
CSeq: 1 INVITE
Call-ID: 22cf1a18@pbx
Contact: <sip:2407560@172.16.2.2:5060>
Server: Epygi Quadro SIP User Agent/v4.1.7 (QUADRO-FXO)
Content-Length: 0

[6] 20071028210210: SIP Rx udp:172.16.2.2:5060:
SIP/2.0 200 OK
Via: SIP/2.0/UDP 172.16.2.1:5060;rport=5060;branch=z9hG4bK-94301e08db2bb7f7033668fbcf6475d2
To: <sip:2407560@172.16.2.2;user=phone>;tag=11924723607e0b5daf-4d65-42f8-826a-2a5757896976
From: "Ramirez" <sip:30@172.16.2.2>;tag=1551698757
CSeq: 1 INVITE
Call-ID: 22cf1a18@pbx
Allow: INVITE, ACK, CANCEL, BYE, OPTIONS, INFO, SUBSCRIBE, NOTIFY, REFER, MESSAGE, UPDATE
Contact: <sip:2407560@172.16.2.2:5060>
Content-Type: application/sdp
Supported: replaces, norefersub
Server: Epygi Quadro SIP User Agent/v4.1.7 (QUADRO-FXO)
Content-Length: 228

v=0
o=2407560 955 325 IN IP4 172.16.2.2
s=-
c=IN IP4 172.16.2.2
t=0 0
m=audio 6012 RTP/AVP 0 8 2 101
a=rtpmap:0 PCMU/8000
a=rtpmap:8 PCMA/8000
a=rtpmap:2 G726-32/8000
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-15
[8] 20071028210210: Sending RTP to 172.16.2.2:6012
[8] 20071028210210: route_pending_packet -38705: entry=url sip:2407560@172.16.2.2:5060
[8] 20071028210210: route_pending_packet -38705: entry=udp 172.16.2.2 5060
[8] 20071028210210: Send Packet ACK
[6] 20071028210210: SIP Tx udp:172.16.2.2:5060:
ACK sip:2407560@172.16.2.2:5060 SIP/2.0
Via: SIP/2.0/UDP 172.16.2.1:5060;branch=z9hG4bK-1d7934c4a196f0c5efece1ac18b0dd56;rport
From: "Ramirez" <sip:30@172.16.2.2>;tag=1551698757
To: <sip:2407560@172.16.2.2;user=phone>;tag=11924723607e0b5daf-4d65-42f8-826a-2a5757896976
Call-ID: 22cf1a18@pbx
CSeq: 1 ACK
Max-Forwards: 70
Contact: <sip:30@172.16.2.1:5060;transport=udp>
Content-Length: 0

[8] 20071028210210: route_pending_packet -38706: entry=udp 200.69.181.76 5060
[8] 20071028210210: Send Packet 200
[6] 20071028210210: SIP Tx udp:200.69.181.76:5060:
SIP/2.0 200 Ok
Via: SIP/2.0/UDP 192.168.2.245:5060;branch=z9hG4bK3d65f2cd8485cf;rport=5060;received=200.69.181.76
From: Carlos <sip:30@200.25.181.62;user=phone>;tag=4BA2394127609C2E2E13
To: <sip:2407560@200.25.181.62;user=phone>;tag=1736886986
Call-ID: 31726-D1B9-1317-32F0-DF63BDDFC232@192.168.2.245
CSeq: 2 INVITE
Contact: <sip:2407560@200.25.181.62:5060;transport=udp>
Supported: 100rel, replaces
Allow-Events: refer
Allow: INVITE, ACK, CANCEL, BYE, REFER, OPTIONS, PRACK, INFO
Accept: application/sdp
User-Agent: Master_Box_IP/1.5.2.7
Content-Type: application/sdp
Content-Length: 204

v=0
o=- 1541178539 1541178539 IN IP4 200.25.181.62
s=-
c=IN IP4 200.25.181.62
t=0 0
```

```
m=audio 60166 RTP/AVP 0 101
a=rtpmap:0 pcmu/8000
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-11
a=sendrecv
[6] 20071028210210: SIP Rx udp:200.69.181.76:5060:
ACK sip:2407560@200.25.181.62:5060 SIP/2.0
Via: SIP/2.0/UDP 192.168.2.245:5060;branch=z9hG4bK3d65f2cd8485cf
From: Carlos<sip:30@200.25.181.62;user=phone>;tag=4BA2394127609C2E2E13
To: <sip:2407560@200.25.181.62;user=phone>;tag=1736886986
Call-ID: 31726-D1B9-1317-32F0-DF63BDDFC232@192.168.2.245
CSeq: 2 ACK
User-Agent: WLAN660-S VoIP PHONE
Content-Length: 0

[5] 20071028210210: Web Server: File border=0 not found
[8] 20071028210211: Send Packet 401
[6] 20071028210211: SIP Tr udp:200.69.181.76:5060:
SIP/2.0 401 Authentication Required
Via: SIP/2.0/UDP 192.168.2.245:5060;branch=z9hG4bK6aa4949633ec7c;rport=5060;received=200.69.181.76
From: Carlos <sip:30@200.25.181.62;user=phone>;tag=4BA2394127609C2E2E13
To: <sip:2407560@200.25.181.62;user=phone>;tag=1736886986
Call-ID: 31726-D1B9-1317-32F0-DF63BDDFC232@192.168.2.245
CSeq: 1 INVITE
User-Agent: Master_Box_IP/1.5.2.7
WWW-Authenticate: Digest realm="200.25.181.62",nonce="c0c40b3e04dee29be9b9f4fbfadf43a0",
domain="sip:2407560@200.25.181.62:5060",stale=true,algorithm=MD5
Content-Length: 0

[6] 20071028210213: SIP Rx udp:200.69.181.76:5060:
INVITE sip:2407560@200.25.181.62:5060 SIP/2.0
Via: SIP/2.0/UDP 192.168.2.245:5060;branch=z9hG4bK26f1b23c32446c
From: Carlos<sip:30@200.25.181.62;user=phone>;tag=4BA2394127609C2E2E13
To: <sip:2407560@200.25.181.62;user=phone>;tag=1736886986
Call-ID: 31726-D1B9-1317-32F0-DF63BDDFC232@192.168.2.245
CSeq: 3 INVITE
User-Agent: WLAN660-S VoIP PHONE
Session-Expires: 5;refresher=uac
Contact: <sip:30@192.168.2.245:5060;transport=udp>
Content-Type: application/sdp
Content-Length: 207

v=0
o=TelogyUnknown0000 340497 340497 IN IP4 192.168.2.245
s=RTP Audio
c=IN IP4 192.168.2.245
t=0 0
m=audio 2070 RTP/AVP 0 101
a=rtpmap:0 PCMU/8000
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-15
[8] 20071028210213: route_pending_packet -38707: entry=udp 200.69.181.76 5060
[8] 20071028210213: Send Packet 200
[6] 20071028210213: SIP Tx udp:200.69.181.76:5060:
SIP/2.0 200 Ok
Via: SIP/2.0/UDP 192.168.2.245:5060;branch=z9hG4bK26f1b23c32446c;rport=5060;received=200.69.181.76
From: Carlos <sip:30@200.25.181.62;user=phone>;tag=4BA2394127609C2E2E13
To: <sip:2407560@200.25.181.62;user=phone>;tag=1736886986
Call-ID: 31726-D1B9-1317-32F0-DF63BDDFC232@192.168.2.245
CSeq: 3 INVITE
Contact: <sip:2407560@200.25.181.62:5060;transport=udp>
Supported: 100rel, replaces
Allow-Events: refer
Allow: INVITE, ACK, CANCEL, BYE, REFER, OPTIONS, PRACK, INFO
Accept: application/sdp
User-Agent: Master_Box_IP/1.5.2.7
Content-Type: application/sdp
Content-Length: 204

v=0
o=- 1541178539 1541178540 IN IP4 200.25.181.62
s=-
c=IN IP4 200.25.181.62
t=0 0
m=audio 60166 RTP/AVP 0 101
```

```
a=rtpmap:0 pcmu/8000
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-11
a=sendrecv
[6] 20071028210213: SIP Rx udp:200.69.181.76:5060:
ACK sip:2407560@200.25.181.62:5060 SIP/2.0
Via: SIP/2.0/UDP 192.168.2.245:5060;branch=z9hG4bK26f1b23c32446c
From: Carlos<sip:30@200.25.181.62;user=phone>;tag=4BA2394127609C2E2E13
To: <sip:2407560@200.25.181.62;user=phone>;tag=1736886986
Call-ID: 31726-D1B9-1317-32F0-DF63BDDFC232@192.168.2.245
CSeq: 3 ACK
User-Agent: WLAN660-S VoIP PHONE
Content-Length: 0

[8] 20071028210215: Send Packet 401
[6] 20071028210215: SIP Tr udp:200.69.181.76:5060:
SIP/2.0 401 Authentication Required
Via: SIP/2.0/UDP 192.168.2.245:5060;branch=z9hG4bK6aa4949633ec7c;rport=5060;received=200.69.181.76
From: Carlos <sip:30@200.25.181.62;user=phone>;tag=4BA2394127609C2E2E13
To: <sip:2407560@200.25.181.62;user=phone>;tag=1736886986
Call-ID: 31726-D1B9-1317-32F0-DF63BDDFC232@192.168.2.245
CSeq: 1 INVITE
User-Agent: Master_Box_IP/1.5.2.7
WWW-Authenticate: Digest realm="200.25.181.62",nonce="c0c40b3e04dee29be9b9f4fbfadf43a0",
domain="sip:2407560@200.25.181.62:5060",stale=true,algorithm=MD5
Content-Length: 0

[6] 20071028210216: SIP Rx udp:200.69.181.76:5060:
INVITE sip:2407560@200.25.181.62:5060 SIP/2.0
Via: SIP/2.0/UDP 192.168.2.245:5060;branch=z9hG4bK61d9305dcfc341
From: Carlos<sip:30@200.25.181.62;user=phone>;tag=4BA2394127609C2E2E13
To: <sip:2407560@200.25.181.62;user=phone>;tag=1736886986
Call-ID: 31726-D1B9-1317-32F0-DF63BDDFC232@192.168.2.245
CSeq: 4 INVITE
User-Agent: WLAN660-S VoIP PHONE
Session-Expires: 5;refresher=uac
Contact: <sip:30@192.168.2.245:5060;transport=udp>
Content-Type: application/sdp
Content-Length: 207

v=0
o=TelogyUnknown0000 340497 340497 IN IP4 192.168.2.245
s=RTP Audio
c=IN IP4 192.168.2.245
t=0 0
m=audio 2070 RTP/AVP 0 101
a=rtpmap:0 PCMU/8000
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-15
[8] 20071028210216: route_pending_packet -38708: entry=udp 200.69.181.76 5060
[8] 20071028210216: Send Packet 200
[6] 20071028210216: SIP Tx udp:200.69.181.76:5060:
SIP/2.0 200 Ok
Via: SIP/2.0/UDP 192.168.2.245:5060;branch=z9hG4bK61d9305dcfc341;rport=5060;received=200.69.181.76
From: Carlos <sip:30@200.25.181.62;user=phone>;tag=4BA2394127609C2E2E13
To: <sip:2407560@200.25.181.62;user=phone>;tag=1736886986
Call-ID: 31726-D1B9-1317-32F0-DF63BDDFC232@192.168.2.245
CSeq: 4 INVITE
Contact: <sip:2407560@200.25.181.62:5060;transport=udp>
Supported: 100rel, replaces
Allow-Events: refer
Allow: INVITE, ACK, CANCEL, BYE, REFER, OPTIONS, PRACK, INFO
Accept: application/sdp
User-Agent: Master_Box_IP/1.5.2.7
Content-Type: application/sdp
Content-Length: 204

v=0
o=- 1541178539 1541178541 IN IP4 200.25.181.62
s=-
c=IN IP4 200.25.181.62
t=0 0
m=audio 60166 RTP/AVP 0 101
a=rtpmap:0 pcmu/8000
a=rtpmap:101 telephone-event/8000
```

```
a=fmtp:101 0-11
a=sendrecv
[6] 20071028210217: SIP Rx udp:200.69.181.76:5060:
ACK sip:2407560@200.25.181.62:5060 SIP/2.0
Via: SIP/2.0/UDP 192.168.2.245:5060;branch=z9hG4bK61d9305dcfc341
From: Carlos<sip:30@200.25.181.62;user=phone>;tag=4BA2394127609C2E2E13
To: <sip:2407560@200.25.181.62;user=phone>;tag=1736886986
Call-ID: 31726-D1B9-1317-32F0-DF63BDDFC232@192.168.2.245
CSeq: 4 ACK
User-Agent: WLAN660-S VoIP PHONE
Content-Length: 0

[8] 20071028210217: SIP Rx udp:200.69.181.76:5060:
REGISTER sip:200.25.181.62:5060 SIP/2.0
Via: SIP/2.0/UDP 192.168.2.245:5060;branch=z9hG4bK5bd92ba365276d
From: <sip:30@200.25.181.62;user=phone>;tag=DFB9449EE5564AB9E78
To: <sip:30@200.25.181.62;user=phone>
Call-ID: 27920-D1B9-1317-ED28-EB45EA353778@192.168.2.245
CSeq: 89 REGISTER
User-Agent: WLAN660-S VoIP PHONE
Contact: <sip:30@192.168.2.245:5060;transport=udp>
Expires: 3600
Content-Length: 0

[8] 20071028210217: route_pending_packet -38709: entry=udp 200.69.181.76 5060
[8] 20071028210217: Send Packet 200
[8] 20071028210217: SIP Tx udp:200.69.181.76:5060:
SIP/2.0 200 Ok
Via: SIP/2.0/UDP 192.168.2.245:5060;branch=z9hG4bK5bd92ba365276d;rport=5060;received=200.69.181.76
From: <sip:30@200.25.181.62;user=phone>;tag=DFB9449EE5564AB9E78
To: <sip:30@200.25.181.62;user=phone>;tag=1307276926
Call-ID: 27920-D1B9-1317-ED28-EB45EA353778@192.168.2.245
CSeq: 89 REGISTER
Contact: <sip:30@192.168.2.245:5060;transport=udp>;expires=30
Content-Length: 0

[6] 20071028210219: SIP Rx udp:200.69.181.76:5060:
BYE sip:2407560@200.25.181.62:5060 SIP/2.0
Via: SIP/2.0/UDP 192.168.2.245:5060;branch=z9hG4bK24ee1372b8fe1d
From: Carlos<sip:30@200.25.181.62;user=phone>;tag=4BA2394127609C2E2E13
To: <sip:2407560@200.25.181.62;user=phone>;tag=1736886986
Call-ID: 31726-D1B9-1317-32F0-DF63BDDFC232@192.168.2.245
CSeq: 5 BYE
User-Agent: WLAN660-S VoIP PHONE
Content-Length: 0

[8] 20071028210219: route_pending_packet -38710: entry=udp 200.69.181.76 5060
[8] 20071028210219: Send Packet 200
[6] 20071028210219: SIP Tx udp:200.69.181.76:5060:
SIP/2.0 200 Ok
Via: SIP/2.0/UDP 192.168.2.245:5060;branch=z9hG4bK24ee1372b8fe1d;rport=5060;received=200.69.181.76
From: Carlos <sip:30@200.25.181.62;user=phone>;tag=4BA2394127609C2E2E13
To: <sip:2407560@200.25.181.62;user=phone>;tag=1736886986
Call-ID: 31726-D1B9-1317-32F0-DF63BDDFC232@192.168.2.245
CSeq: 5 BYE
Contact: <sip:2407560@200.25.181.62:5060;transport=udp>
User-Agent: Master_Box_IP/1.5.2.7
RTP-RxStat: Dur=11,Pkt=330,Oct=83160
RTP-TxStat: Dur=3,Pkt=524,Oct=90128
Content-Length: 0

[7] 20071028210219: Other Ports: 1
[7] 20071028210219: Call Port: 22cf1a18@pbx#1551698757
[8] 20071028210219: route_pending_packet -38711: entry=url sip:2407560@172.16.2.2:5060
[8] 20071028210219: route_pending_packet -38711: entry=udp 172.16.2.2 5060
[8] 20071028210219: Send Packet BYE
[6] 20071028210219: SIP Tx udp:172.16.2.2:5060:
BYE sip:2407560@172.16.2.2:5060 SIP/2.0
Via: SIP/2.0/UDP 172.16.2.1:5060;branch=z9hG4bK-4ac43b07fe2d4df90b4a7396a8b836d5;rport
From: "Ramirez" <sip:30@172.16.2.2>;tag=1551698757
To: <sip:2407560@172.16.2.2;user=phone>;tag=11924723607e0b5daf-4d65-42f8-826a-2a5757896976
Call-ID: 22cf1a18@pbx
CSeq: 2 BYE
Max-Forwards: 70
Contact: <sip:30@172.16.2.1:5060;transport=udp>
```

```
RTP-RxStat: Dur=11,Pkt=427,Oct=73444
RTP-TxStat: Dur=9,Pkt=391,Oct=67252
Content-Length: 0

[6] 20071028210219: SIP Rx udp:172.16.2.2:5060:
SIP/2.0 200 OK
Via: SIP/2.0/UDP 172.16.2.1:5060;rport=5060;branch=z9hG4bK-4ac43b07fe2d4df90b4a7396a8b836d5
To: <sip:2407560@172.16.2.2;user=phone>;tag=11924723607e0b5daf-4d65-42f8-826a-2a5757896976
From: "Ramirez" <sip:30@172.16.2.2>;tag=1551698757
CSeq: 2 BYE
Call-ID: 22cf1a18@pbx
Server: Epygi Quadro SIP User Agent/v4.1.7 (QUADRO-FXO)
Content-Length: 0

[5] 20071028210219: BYE Response: Terminate 22cf1a18@pbx
[8] 20071028210219: SIP Rx udp:172.16.2.21:5060:
REGISTER sip:172.16.2.1 SIP/2.0
Via: SIP/2.0/UDP 172.16.2.21:5060;branch=z9hG4bK4126216523142331865;rport
From: 21 <sip:21@172.16.2.1>;tag=236647701
To: 21 <sip:21@172.16.2.1>
Call-ID: 1721013724-00112167@172.16.2.21
CSeq: 3242 REGISTER
Contact: <sip:21@172.16.2.21:5060>
Authorization: Digest username="21", realm="172.16.2.1", nonce="69aa43a37370b868b35aa7e9fa8d2b09",
uri="sip:172.16.2.1", response="8c3f26f06233106f5fe2817eef9b9349", algorithm=MD5
max-forwards: 70
expires: 60
user-agent: Voip Phone 1.0
Content-Length: 0

[8] 20071028210219: route_pending_packet -38712: entry=a udp 172.16.2.21 5060
[8] 20071028210219: route_pending_packet -38712: entry=udp 172.16.2.21 5060
[8] 20071028210219: Send Packet 200
[8] 20071028210219: SIP Tx udp:172.16.2.21:5060:
SIP/2.0 200 Ok
Via: SIP/2.0/UDP 172.16.2.21:5060;branch=z9hG4bK4126216523142331865;rport=5060
From: 21 <sip:21@172.16.2.1>;tag=236647701
To: 21 <sip:21@172.16.2.1>;tag=1975676142
Call-ID: 1721013724-00112167@172.16.2.21
CSeq: 3242 REGISTER
Contact: <sip:21@172.16.2.21:5060>;expires=60
Content-Length: 0

[5] 20071028210221: Web Server: File border=0 not found
[8] 20071028210223: Send Packet 401
[6] 20071028210223: SIP Tr udp:200.69.181.76:5060:
SIP/2.0 401 Authentication Required
Via: SIP/2.0/UDP 192.168.2.245:5060;branch=z9hG4bK6aa4949633ec7c;rport=5060;received=200.69.181.76
From: Carlos <sip:30@200.25.181.62;user=phone>;tag=4BA2394127609C2E2E13
To: <sip:2407560@200.25.181.62;user=phone>;tag=1736886986
Call-ID: 31726-D1B9-1317-32F0-DF63BDDFC232@192.168.2.245
CSeq: 1 INVITE
User-Agent: Master_Box_IP/1.5.2.7
WWW-Authenticate: Digest realm="200.25.181.62",nonce="c0c40b3e04dee29be9b9f4fbfadf43a0",
domain="sip:2407560@200.25.181.62:5060",stale=true,algorithm=MD5
Content-Length: 0
```

A continucion vemos el Log de una llamda desde el Internet hacia el numero 096312674 realizado por el Wi-Fi Phone

LOG 096312674

Logfile

Clear or Reload the log.

```
[8] 20071028210643: SIP Rx udp:200.69.181.76:5060:
REGISTER sip:200.25.181.62:5060 SIP/2.0
Via: SIP/2.0/UDP 192.168.2.245:5060;branch=z9hG4bKa95247d1a68fe7
From: <sip:30@200.25.181.62;user=phone>;tag=909AB89F10B8E3C0EE21
To: <sip:30@200.25.181.62;user=phone>
Call-ID: 27920-D1B9-1317-ED28-EB45EA353778@192.168.2.245
CSeq: 107 REGISTER
User-Agent: WLAN660-S VoIP PHONE
Contact: <sip:30@192.168.2.245:5060;transport=udp>
Expires: 3600
Content-Length: 0

[8] 20071028210643: route_pending_packet -38787: entry=udp 200.69.181.76 5060
[8] 20071028210643: Send Packet 200
[8] 20071028210643: SIP Tx udp:200.69.181.76:5060:
SIP/2.0 200 Ok
Via: SIP/2.0/UDP 192.168.2.245:5060;branch=z9hG4bKa95247d1a68fe7;rport=5060;received=200.69.181.76
From: <sip:30@200.25.181.62;user=phone>;tag=909AB89F10B8E3C0EE21
To: <sip:30@200.25.181.62;user=phone>;tag=372734283
Call-ID: 27920-D1B9-1317-ED28-EB45EA353778@192.168.2.245
CSeq: 107 REGISTER
Contact: <sip:30@192.168.2.245:5060;transport=udp>;expires=30
Content-Length: 0

[5] 20071028210644: Web Server: File border=0 not found
[6] 20071028210644: SIP Rx udp:172.16.2.2:5060:
SIP/2.0 180 Ringing
Via: SIP/2.0/UDP 172.16.2.1:5060;rport=5060;branch=z9hG4bK-79b4f86f98912dffddd0158f9ee243b2
To: <sip:096312674@172.16.2.2;user=phone>;tag=119247236055bd522e-8c73-45fb-bed5-a118d3fc0ded
From: "0963" <sip:0963@172.16.2.2>;tag=1894251668
CSeq: 1 INVITE
Call-ID: 2f42bb30@pbx
Contact: <sip:096312674@172.16.2.2:5060>
Server: Epygi Quadro SIP User Agent/v4.1.7 (QUADRO-FXO)
Content-Length: 0

[6] 20071028210644: SIP Rx udp:172.16.2.2:5060:
SIP/2.0 200 OK
Via: SIP/2.0/UDP 172.16.2.1:5060;rport=5060;branch=z9hG4bK-79b4f86f98912dffddd0158f9ee243b2
To: <sip:096312674@172.16.2.2;user=phone>;tag=119247236055bd522e-8c73-45fb-bed5-a118d3fc0ded
From: "0963" <sip:0963@172.16.2.2>;tag=1894251668
CSeq: 1 INVITE
Call-ID: 2f42bb30@pbx
Allow: INVITE, ACK, CANCEL, BYE, OPTIONS, INFO, SUBSCRIBE, NOTIFY, REFER, MESSAGE, UPDATE
Contact: <sip:096312674@172.16.2.2:5060>
Content-Type: application/sdp
Supported: replaces, norefersub
Server: Epygi Quadro SIP User Agent/v4.1.7 (QUADRO-FXO)
Content-Length: 230

v=0
o=096312674 117 659 IN IP4 172.16.2.2
s=-
c=IN IP4 172.16.2.2
t=0 0
m=audio 6014 RTP/AVP 0 8 2 101
a=rtpmap:0 PCMU/8000
a=rtpmap:8 PCMA/8000
a=rtpmap:2 G726-32/8000
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-15
[8] 20071028210644: Sending RTP to 172.16.2.2:6014
[8] 20071028210644: route_pending_packet -38788: entry=url sip:096312674@172.16.2.2:5060
[8] 20071028210644: route_pending_packet -38788: entry=udp 172.16.2.2 5060
[8] 20071028210644: Send Packet ACK
[6] 20071028210644: SIP Tx udp:172.16.2.2:5060:
ACK sip:096312674@172.16.2.2:5060 SIP/2.0
Via: SIP/2.0/UDP 172.16.2.1:5060;branch=z9hG4bK-1748587070b18c583aee4c0c87954660;rport
```

From: "0963" <sip:0963@172.16.2.2>;tag=1894251668
To: <sip:096312674@172.16.2.2;user=phone>;tag=119247236055bd522e-8c73-45fb-bed5-a118d3fc0ded
Call-ID: 2f42bb30@pbx
CSeq: 1 ACK
Max-Forwards: 70
Contact: <sip:0963@172.16.2.1:5060;transport=udp>
P-Preferred-Identity: "Ramirez" <sip:30@172.16.2.2>
Content-Length: 0

[8] 20071028210644: route_pending_packet -38789: entry=udp 200.69.181.76 5060
[8] 20071028210644: Send Packet 200
[6] 20071028210644: SIP Tx udp:200.69.181.76:5060:
SIP/2.0 200 Ok
Via: SIP/2.0/UDP 192.168.2.245:5060;branch=z9hG4bK49645a4224fde6;rport=5060;received=200.69.181.76
From: Carlos <sip:30@200.25.181.62;user=phone>;tag=2DB5241E3BA59572DABF
To: <sip:096312674@200.25.181.62;user=phone>;tag=604857669
Call-ID: 29277-D1B9-1317-6A26-CCE1A47F1DD7@192.168.2.245
CSeq: 2 INVITE
Contact: <sip:096312674@200.25.181.62:5060;transport=udp>
Supported: 100rel, replaces
Allow-Events: refer
Allow: INVITE, ACK, CANCEL, BYE, REFER, OPTIONS, PRACK, INFO
Accept: application/sdp
User-Agent: Master_Box_IP/1.5.2.7
Content-Type: application/sdp
Content-Length: 204

v=0
o=- 1795738459 1795738459 IN IP4 200.25.181.62
s=-
c=IN IP4 200.25.181.62
t=0 0
m=audio 54932 RTP/AVP 0 101
a=rtpmap:0 pcmu/8000
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-11
a=sendrecv
[8] 20071028210644: Send Packet 401
[6] 20071028210644: SIP Tr udp:200.69.181.76:5060:
SIP/2.0 401 Authentication Required
Via: SIP/2.0/UDP 192.168.2.245:5060;branch=z9hG4bK61168421e0e292;rport=5060;received=200.69.181.76
From: Carlos <sip:30@200.25.181.62;user=phone>;tag=2DB5241E3BA59572DABF
To: <sip:096312674@200.25.181.62;user=phone>;tag=604857669
Call-ID: 29277-D1B9-1317-6A26-CCE1A47F1DD7@192.168.2.245
CSeq: 1 INVITE
User-Agent: Master_Box_IP/1.5.2.7
WWW-Authenticate: Digest realm="200.25.181.62",nonce="10836eaa5ab0c7059d0dfc91915c6977",

domain="sip:096312674@200.25.181.62:5060",stale=true,algorithm=MD5
Content-Length: 0

[6] 20071028210644: SIP Rx udp:200.69.181.76:5060:
ACK sip:096312674@200.25.181.62:5060 SIP/2.0
Via: SIP/2.0/UDP 192.168.2.245:5060;branch=z9hG4bK49645a4224fde6
From: Carlos<sip:30@200.25.181.62;user=phone>;tag=2DB5241E3BA59572DABF
To: <sip:096312674@200.25.181.62;user=phone>;tag=604857669
Call-ID: 29277-D1B9-1317-6A26-CCE1A47F1DD7@192.168.2.245
CSeq: 2 ACK
User-Agent: WLAN660-S VoIP PHONE
Content-Length: 0

[6] 20071028210647: SIP Rx udp:200.69.181.76:5060:
INVITE sip:096312674@200.25.181.62:5060 SIP/2.0
Via: SIP/2.0/UDP 192.168.2.245:5060;branch=z9hG4bK82cf5ea4cce0ec
From: Carlos<sip:30@200.25.181.62;user=phone>;tag=2DB5241E3BA59572DABF
To: <sip:096312674@200.25.181.62;user=phone>;tag=604857669
Call-ID: 29277-D1B9-1317-6A26-CCE1A47F1DD7@192.168.2.245
CSeq: 3 INVITE
User-Agent: WLAN660-S VoIP PHONE
Session-Expires: 5;refresher=uac
Contact: <sip:30@192.168.2.245:5060;transport=udp>
Content-Type: application/sdp
Content-Length: 207

v=0

```
o=TelogyUnknown0000 408506 408506 IN IP4 192.168.2.245
s=RTP Audio
c=IN IP4 192.168.2.245
t=0 0
m=audio 2070 RTP/AVP 0 101
a=rtpmap:0 PCMU/8000
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-15
[8] 20071028210647: route_pending_packet -38790: entry=udp 200.69.181.76 5060
[8] 20071028210647: Send Packet 200
[6] 20071028210647: SIP Tx udp:200.69.181.76:5060:
SIP/2.0 200 Ok
Via: SIP/2.0/UDP 192.168.2.245:5060;branch=z9hG4bK82cf5ea4cce0ec;rport=5060;received=200.69.181.76
From: Carlos <sip:30@200.25.181.62;user=phone>;tag=2DB5241E3BA59572DABF
To: <sip:096312674@200.25.181.62;user=phone>;tag=604857669
Call-ID: 29277-D1B9-1317-6A26-CCE1A47F1DD7@192.168.2.245
CSeq: 3 INVITE
Contact: <sip:096312674@200.25.181.62:5060;transport=udp>
Supported: 100rel, replaces
Allow-Events: refer
Allow: INVITE, ACK, CANCEL, BYE, REFER, OPTIONS, PRACK, INFO
Accept: application/sdp
User-Agent: Master_Box_IP/1.5.2.7
Content-Type: application/sdp
Content-Length: 204

v=0
o=- 1795738459 1795738460 IN IP4 200.25.181.62
s=-
c=IN IP4 200.25.181.62
t=0 0
m=audio 54932 RTP/AVP 0 101
a=rtpmap:0 pcmu/8000
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-11
a=sendrecv
[8] 20071028210647: Send Packet 200
[6] 20071028210647: SIP Tr udp:200.69.181.76:5060:
SIP/2.0 200 Ok
Via: SIP/2.0/UDP 192.168.2.245:5060;branch=z9hG4bK82cf5ea4cce0ec;rport=5060;received=200.69.181.76
From: Carlos <sip:30@200.25.181.62;user=phone>;tag=2DB5241E3BA59572DABF
To: <sip:096312674@200.25.181.62;user=phone>;tag=604857669
Call-ID: 29277-D1B9-1317-6A26-CCE1A47F1DD7@192.168.2.245
CSeq: 3 INVITE
Contact: <sip:096312674@200.25.181.62:5060;transport=udp>
Supported: 100rel, replaces
Allow-Events: refer
Allow: INVITE, ACK, CANCEL, BYE, REFER, OPTIONS, PRACK, INFO
Accept: application/sdp
User-Agent: Master_Box_IP/1.5.2.7
Content-Type: application/sdp
Content-Length: 204

v=0
o=- 1795738459 1795738460 IN IP4 200.25.181.62
s=-
c=IN IP4 200.25.181.62
t=0 0
m=audio 54932 RTP/AVP 0 101
a=rtpmap:0 pcmu/8000
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-11
a=sendrecv
[6] 20071028210648: SIP Rx udp:200.69.181.76:5060:
ACK sip:096312674@200.25.181.62:5060 SIP/2.0
Via: SIP/2.0/UDP 192.168.2.245:5060;branch=z9hG4bK82cf5ea4cce0ec
From: Carlos<sip:30@200.25.181.62;user=phone>;tag=2DB5241E3BA59572DABF
To: <sip:096312674@200.25.181.62;user=phone>;tag=604857669
Call-ID: 29277-D1B9-1317-6A26-CCE1A47F1DD7@192.168.2.245
CSeq: 3 ACK
User-Agent: WLAN660-S VoIP PHONE
Content-Length: 0

[8] 20071028210648: Send Packet 401
[6] 20071028210648: SIP Tr udp:200.69.181.76:5060:
```

SIP/2.0 401 Authentication Required
Via: SIP/2.0/UDP 192.168.2.245:5060;branch=z9hG4bK61168421e0e292;rport=5060;received=200.69.181.76
From: Carlos <sip:30@200.25.181.62;user=phone>;tag=2DB5241E3BA59572DABF
To: <sip:096312674@200.25.181.62;user=phone>;tag=604857669
Call-ID: 29277-D1B9-1317-6A26-CCE1A47F1DD7@192.168.2.245
CSeq: 1 INVITE
User-Agent: Master_Box_IP/1.5.2.7
WWW-Authenticate: Digest realm="200.25.181.62",nonce="10836eaa5ab0c7059d0dfc91915c6977",

domain="sip:096312674@200.25.181.62:5060",stale=true,algorithm=MD5
Content-Length: 0

[6] 20071028210650: SIP Rx udp:200.69.181.76:5060:
INVITE sip:096312674@200.25.181.62:5060 SIP/2.0
Via: SIP/2.0/UDP 192.168.2.245:5060;branch=z9hG4bK56af1459156e17
From: Carlos<sip:30@200.25.181.62;user=phone>;tag=2DB5241E3BA59572DABF
To: <sip:096312674@200.25.181.62;user=phone>;tag=604857669
Call-ID: 29277-D1B9-1317-6A26-CCE1A47F1DD7@192.168.2.245
CSeq: 4 INVITE
User-Agent: WLAN660-S VoIP PHONE
Session-Expires: 5;refresher=uac
Contact: <sip:30@192.168.2.245:5060;transport=udp>
Content-Type: application/sdp
Content-Length: 207

v=0
o=TelogyUnknown0000 408506 408506 IN IP4 192.168.2.245
s=RTP Audio
c=IN IP4 192.168.2.245
t=0 0
m=audio 2070 RTP/AVP 0 101
a=rtpmap:0 PCMU/8000
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-15
[8] 20071028210650: route_pending_packet -38791: entry=udp 200.69.181.76 5060
[8] 20071028210650: Send Packet 200
[6] 20071028210650: SIP Tx udp:200.69.181.76:5060:
SIP/2.0 200 Ok
Via: SIP/2.0/UDP 192.168.2.245:5060;branch=z9hG4bK56af1459156e17;rport=5060;received=200.69.181.76
From: Carlos <sip:30@200.25.181.62;user=phone>;tag=2DB5241E3BA59572DABF
To: <sip:096312674@200.25.181.62;user=phone>;tag=604857669
Call-ID: 29277-D1B9-1317-6A26-CCE1A47F1DD7@192.168.2.245
CSeq: 4 INVITE
Contact: <sip:096312674@200.25.181.62:5060;transport=udp>
Supported: 100rel, replaces
Allow-Events: refer
Allow: INVITE, ACK, CANCEL, BYE, REFER, OPTIONS, PRACK, INFO
Accept: application/sdp
User-Agent: Master_Box_IP/1.5.2.7
Content-Type: application/sdp
Content-Length: 204

v=0
o=- 1795738459 1795738461 IN IP4 200.25.181.62
s=-
c=IN IP4 200.25.181.62
t=0 0
m=audio 54932 RTP/AVP 0 101
a=rtpmap:0 pcmu/8000
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-11
a=sendrecv
[6] 20071028210651: SIP Rx udp:200.69.181.76:5060:
ACK sip:096312674@200.25.181.62:5060 SIP/2.0
Via: SIP/2.0/UDP 192.168.2.245:5060;branch=z9hG4bK56af1459156e17
From: Carlos<sip:30@200.25.181.62;user=phone>;tag=2DB5241E3BA59572DABF
To: <sip:096312674@200.25.181.62;user=phone>;tag=604857669
Call-ID: 29277-D1B9-1317-6A26-CCE1A47F1DD7@192.168.2.245
CSeq: 4 ACK
User-Agent: WLAN660-S VoIP PHONE
Content-Length: 0

[6] 20071028210653: SIP Rx udp:200.69.181.76:5060:
INVITE sip:096312674@200.25.181.62:5060 SIP/2.0
Via: SIP/2.0/UDP 192.168.2.245:5060;branch=z9hG4bK3af3894bf5e3a4

From: Carlos<sip:30@200.25.181.62;user=phone>;tag=2DB5241E3BA59572DABF
To: <sip:096312674@200.25.181.62;user=phone>;tag=604857669
Call-ID: 29277-D1B9-1317-6A26-CCE1A47F1DD7@192.168.2.245
CSeq: 5 INVITE
User-Agent: WLAN660-S VoIP PHONE
Session-Expires: 5;refresher=uac
Contact: <sip:30@192.168.2.245:5060;transport=udp>
Content-Type: application/sdp
Content-Length: 207

v=0
o=TelogyUnknown0000 408506 408506 IN IP4 192.168.2.245
s=RTP Audio
c=IN IP4 192.168.2.245
t=0 0
m=audio 2070 RTP/AVP 0 101
a=rtpmap:0 PCMU/8000
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-15
[8] 20071028210653: route_pending_packet -38792: entry=udp 200.69.181.76 5060
[8] 20071028210653: Send Packet 200
[6] 20071028210653: SIP Tx udp:200.69.181.76:5060:
SIP/2.0 200 Ok
Via: SIP/2.0/UDP 192.168.2.245:5060;branch=z9hG4bK3af3894bf5e3a4;rport=5060;received=200.69.181.76
From: Carlos <sip:30@200.25.181.62;user=phone>;tag=2DB5241E3BA59572DABF
To: <sip:096312674@200.25.181.62;user=phone>;tag=604857669
Call-ID: 29277-D1B9-1317-6A26-CCE1A47F1DD7@192.168.2.245
CSeq: 5 INVITE
Contact: <sip:096312674@200.25.181.62:5060;transport=udp>
Supported: 100rel, replaces
Allow-Events: refer
Allow: INVITE, ACK, CANCEL, BYE, REFER, OPTIONS, PRACK, INFO
Accept: application/sdp
User-Agent: Master_Box_IP/1.5.2.7
Content-Type: application/sdp
Content-Length: 204

v=0
o=- 1795738459 1795738462 IN IP4 200.25.181.62
s=-
c=IN IP4 200.25.181.62
t=0 0
m=audio 54932 RTP/AVP 0 101
a=rtpmap:0 pcmu/8000
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-11
a=sendrecv
[6] 20071028210654: SIP Rx udp:200.69.181.76:5060:
ACK sip:096312674@200.25.181.62:5060 SIP/2.0
Via: SIP/2.0/UDP 192.168.2.245:5060;branch=z9hG4bK3af3894bf5e3a4
From: Carlos<sip:30@200.25.181.62;user=phone>;tag=2DB5241E3BA59572DABF
To: <sip:096312674@200.25.181.62;user=phone>;tag=604857669
Call-ID: 29277-D1B9-1317-6A26-CCE1A47F1DD7@192.168.2.245
CSeq: 5 ACK
User-Agent: WLAN660-S VoIP PHONE
Content-Length: 0

[8] 20071028210656: Send Packet 401
[6] 20071028210656: SIP Tr udp:200.69.181.76:5060:
SIP/2.0 401 Authentication Required
Via: SIP/2.0/UDP 192.168.2.245:5060;branch=z9hG4bK61168421e0e292;rport=5060;received=200.69.181.76
From: Carlos <sip:30@200.25.181.62;user=phone>;tag=2DB5241E3BA59572DABF
To: <sip:096312674@200.25.181.62;user=phone>;tag=604857669
Call-ID: 29277-D1B9-1317-6A26-CCE1A47F1DD7@192.168.2.245
CSeq: 1 INVITE
User-Agent: Master_Box_IP/1.5.2.7
WWW-Authenticate: Digest realm="200.25.181.62",nonce="10836eaa5ab0c7059d0dfc91915c6977",

domain="sip:096312674@200.25.181.62:5060",stale=true,algorithm=MD5
Content-Length: 0

[6] 20071028210656: SIP Rx udp:200.69.181.76:5060:
INVITE sip:096312674@200.25.181.62:5060 SIP/2.0
Via: SIP/2.0/UDP 192.168.2.245:5060;branch=z9hG4bKe999c64f6419e2
From: Carlos<sip:30@200.25.181.62;user=phone>;tag=2DB5241E3BA59572DABF

To: <sip:096312674@200.25.181.62;user=phone>;tag=604857669
Call-ID: 29277-D1B9-1317-6A26-CCE1A47F1DD7@192.168.2.245
CSeq: 6 INVITE
User-Agent: WLAN660-S VoIP PHONE
Session-Expires: 5;refresher=uac
Contact: <sip:30@192.168.2.245:5060;transport=udp>
Content-Type: application/sdp
Content-Length: 207

v=0
o=TelogyUnknown0000 408506 408506 IN IP4 192.168.2.245
s=RTP Audio
c=IN IP4 192.168.2.245
t=0 0
m=audio 2070 RTP/AVP 0 101
a=rtpmap:0 PCMU/8000
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-15
[8] 20071028210656: route_pending_packet -38793: entry=udp 200.69.181.76 5060
[8] 20071028210656: Send Packet 200
[6] 20071028210656: SIP Tx udp:200.69.181.76:5060:
SIP/2.0 200 Ok
Via: SIP/2.0/UDP 192.168.2.245:5060;branch=z9hG4bKe999c64f6419e2;rport=5060;received=200.69.181.76
From: Carlos <sip:30@200.25.181.62;user=phone>;tag=2DB5241E3BA59572DABF
To: <sip:096312674@200.25.181.62;user=phone>;tag=604857669
Call-ID: 29277-D1B9-1317-6A26-CCE1A47F1DD7@192.168.2.245
CSeq: 6 INVITE
Contact: <sip:096312674@200.25.181.62:5060;transport=udp>
Supported: 100rel, replaces
Allow-Events: refer
Allow: INVITE, ACK, CANCEL, BYE, REFER, OPTIONS, PRACK, INFO
Accept: application/sdp
User-Agent: Master_Box_IP/1.5.2.7
Content-Type: application/sdp
Content-Length: 204

v=0
o=- 1795738459 1795738463 IN IP4 200.25.181.62
s=-
c=IN IP4 200.25.181.62
t=0 0
m=audio 54932 RTP/AVP 0 101
a=rtpmap:0 pcmu/8000
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-11
a=sendrecv
[8] 20071028210657: Send Packet 200
[6] 20071028210657: SIP Tr udp:200.69.181.76:5060:
SIP/2.0 200 Ok
Via: SIP/2.0/UDP 192.168.2.245:5060;branch=z9hG4bKe999c64f6419e2;rport=5060;received=200.69.181.76
From: Carlos <sip:30@200.25.181.62;user=phone>;tag=2DB5241E3BA59572DABF
To: <sip:096312674@200.25.181.62;user=phone>;tag=604857669
Call-ID: 29277-D1B9-1317-6A26-CCE1A47F1DD7@192.168.2.245
CSeq: 6 INVITE
Contact: <sip:096312674@200.25.181.62:5060;transport=udp>
Supported: 100rel, replaces
Allow-Events: refer
Allow: INVITE, ACK, CANCEL, BYE, REFER, OPTIONS, PRACK, INFO
Accept: application/sdp
User-Agent: Master_Box_IP/1.5.2.7
Content-Type: application/sdp
Content-Length: 204

v=0
o=- 1795738459 1795738463 IN IP4 200.25.181.62
s=-
c=IN IP4 200.25.181.62
t=0 0
m=audio 54932 RTP/AVP 0 101
a=rtpmap:0 pcmu/8000
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-11
a=sendrecv
[6] 20071028210657: SIP Rx udp:200.69.181.76:5060:
ACK sip:096312674@200.25.181.62:5060 SIP/2.0

Via: SIP/2.0/UDP 192.168.2.245:5060;branch=z9hG4bKe999c64f6419e2
From: Carlos<sip:30@200.25.181.62;user=phone>;tag=2DB5241E3BA59572DABF
To: <sip:096312674@200.25.181.62;user=phone>;tag=604857669
Call-ID: 29277-D1B9-1317-6A26-CCE1A47F1DD7@192.168.2.245
CSeq: 6 ACK
User-Agent: WLAN660-S VoIP PHONE
Content-Length: 0

[8] 20071028210659: SIP Rx udp:200.69.181.76:5060:
REGISTER sip:200.25.181.62:5060 SIP/2.0
Via: SIP/2.0/UDP 192.168.2.245:5060;branch=z9hG4bK3fb8ccc0693ff0
From: <sip:30@200.25.181.62;user=phone>;tag=89804A281BC2CFCFED
To: <sip:30@200.25.181.62;user=phone>
Call-ID: 27920-D1B9-1317-ED28-EB45EA353778@192.168.2.245
CSeq: 108 REGISTER
User-Agent: WLAN660-S VoIP PHONE
Contact: <sip:30@192.168.2.245:5060;transport=udp>
Expires: 3600
Content-Length: 0

[8] 20071028210659: route_pending_packet -38794: entry=udp 200.69.181.76 5060
[8] 20071028210659: Send Packet 200
[8] 20071028210659: SIP Tx udp:200.69.181.76:5060:
SIP/2.0 200 Ok
Via: SIP/2.0/UDP 192.168.2.245:5060;branch=z9hG4bK3fb8ccc0693ff0;rport=5060;received=200.69.181.76
From: <sip:30@200.25.181.62;user=phone>;tag=89804A281BC2CFCFED
To: <sip:30@200.25.181.62;user=phone>;tag=532428580
Call-ID: 27920-D1B9-1317-ED28-EB45EA353778@192.168.2.245
CSeq: 108 REGISTER
Contact: <sip:30@192.168.2.245:5060;transport=udp>;expires=30
Content-Length: 0

[6] 20071028210700: SIP Rx udp:200.69.181.76:5060:
INVITE sip:096312674@200.25.181.62:5060 SIP/2.0
Via: SIP/2.0/UDP 192.168.2.245:5060;branch=z9hG4bKc521621dfb204c
From: Carlos<sip:30@200.25.181.62;user=phone>;tag=2DB5241E3BA59572DABF
To: <sip:096312674@200.25.181.62;user=phone>;tag=604857669
Call-ID: 29277-D1B9-1317-6A26-CCE1A47F1DD7@192.168.2.245
CSeq: 7 INVITE
User-Agent: WLAN660-S VoIP PHONE
Session-Expires: 5;refresher=uac
Contact: <sip:30@192.168.2.245:5060;transport=udp>
Content-Type: application/sdp
Content-Length: 207

v=0
o=TelogyUnknown0000 408506 408506 IN IP4 192.168.2.245
s=RTP Audio
c=IN IP4 192.168.2.245
t=0 0
m=audio 2070 RTP/AVP 0 101
a=rtpmap:0 PCMU/8000
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-15
[8] 20071028210700: route_pending_packet -38795: entry=udp 200.69.181.76 5060
[8] 20071028210700: Send Packet 200
[6] 20071028210700: SIP Tx udp:200.69.181.76:5060:
SIP/2.0 200 Ok
Via: SIP/2.0/UDP 192.168.2.245:5060;branch=z9hG4bKc521621dfb204c;rport=5060;received=200.69.181.76
From: Carlos <sip:30@200.25.181.62;user=phone>;tag=2DB5241E3BA59572DABF
To: <sip:096312674@200.25.181.62;user=phone>;tag=604857669
Call-ID: 29277-D1B9-1317-6A26-CCE1A47F1DD7@192.168.2.245
CSeq: 7 INVITE
Contact: <sip:096312674@200.25.181.62:5060;transport=udp>
Supported: 100rel, replaces
Allow-Events: refer
Allow: INVITE, ACK, CANCEL, BYE, REFER, OPTIONS, PRACK, INFO
Accept: application/sdp
User-Agent: Master_Box_IP/1.5.2.7
Content-Type: application/sdp
Content-Length: 204

v=0
o=- 1795738459 1795738464 IN IP4 200.25.181.62
s=-

```
c=IN IP4 200.25.181.62
t=0 0
m=audio 54932 RTP/AVP 0 101
a=rtpmap:0 pcmu/8000
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-11
a=sendrecv
[6] 20071028210700: SIP Rx udp:200.69.181.76:5060:
ACK sip:096312674@200.25.181.62:5060 SIP/2.0
Via: SIP/2.0/UDP 192.168.2.245:5060;branch=z9hG4bKc521621dfb204c
From: Carlos<sip:30@200.25.181.62;user=phone>;tag=2DB5241E3BA59572DABF
To: <sip:096312674@200.25.181.62;user=phone>;tag=604857669
Call-ID: 29277-D1B9-1317-6A26-CCE1A47F1DD7@192.168.2.245
CSeq: 7 ACK
User-Agent: WLAN660-S VoIP PHONE
Content-Length: 0

[6] 20071028210701: SIP Rx udp:200.69.181.76:5060:
BYE sip:096312674@200.25.181.62:5060 SIP/2.0
Via: SIP/2.0/UDP 192.168.2.245:5060;branch=z9hG4bK6bb28c677c1e2c
From: Carlos<sip:30@200.25.181.62;user=phone>;tag=2DB5241E3BA59572DABF
To: <sip:096312674@200.25.181.62;user=phone>;tag=604857669
Call-ID: 29277-D1B9-1317-6A26-CCE1A47F1DD7@192.168.2.245
CSeq: 8 BYE
User-Agent: WLAN660-S VoIP PHONE
Content-Length: 0

[8] 20071028210701: route_pending_packet -38796: entry=udp 200.69.181.76 5060
[8] 20071028210701: Send Packet 200
[6] 20071028210701: SIP Tx udp:200.69.181.76:5060:
SIP/2.0 200 Ok
Via: SIP/2.0/UDP 192.168.2.245:5060;branch=z9hG4bK6bb28c677c1e2c;rport=5060;received=200.69.181.76
From: Carlos <sip:30@200.25.181.62;user=phone>;tag=2DB5241E3BA59572DABF
To: <sip:096312674@200.25.181.62;user=phone>;tag=604857669
Call-ID: 29277-D1B9-1317-6A26-CCE1A47F1DD7@192.168.2.245
CSeq: 8 BYE
Contact: <sip:096312674@200.25.181.62:5060;transport=udp>
User-Agent: Master_Box_IP/1.5.2.7
RTP-RxStat: Dur=20,Pkt=652,Oct=164304
RTP-TxStat: Dur=1,Pkt=992,Oct=170624
Content-Length: 0

[7] 20071028210701: Other Ports: 1
[7] 20071028210701: Call Port: 2f42bb30@pbx#1894251668
[8] 20071028210701: route_pending_packet -38797: entry=url sip:096312674@172.16.2.2:5060
[8] 20071028210701: route_pending_packet -38797: entry=udp 172.16.2.2 5060
[8] 20071028210701: Send Packet BYE
[6] 20071028210701: SIP Tx udp:172.16.2.2:5060:
BYE sip:096312674@172.16.2.2:5060 SIP/2.0
Via: SIP/2.0/UDP 172.16.2.1:5060;branch=z9hG4bK-44e39f307f57035b96df798d01a50ef9;rport
From: "0963" <sip:0963@172.16.2.2>;tag=1894251668
To: <sip:096312674@172.16.2.2;user=phone>;tag=119247236055bd522e-8c73-45fb-bed5-a118d3fc0ded
Call-ID: 2f42bb30@pbx
CSeq: 2 BYE
Max-Forwards: 70
Contact: <sip:0963@172.16.2.1:5060;transport=udp>
RTP-RxStat: Dur=20,Pkt=841,Oct=144652
RTP-TxStat: Dur=17,Pkt=844,Oct=145168
P-Preferred-Identity: "Ramirez" <sip:30@172.16.2.2>
Content-Length: 0

[6] 20071028210701: SIP Rx udp:172.16.2.2:5060:
SIP/2.0 200 OK
Via: SIP/2.0/UDP 172.16.2.1:5060;rport=5060;branch=z9hG4bK-44e39f307f57035b96df798d01a50ef9
To: <sip:096312674@172.16.2.2;user=phone>;tag=119247236055bd522e-8c73-45fb-bed5-a118d3fc0ded
From: "0963" <sip:0963@172.16.2.2>;tag=1894251668
CSeq: 2 BYE
Call-ID: 2f42bb30@pbx
Server: Epygi Quadro SIP User Agent/v4.1.7 (QUADRO-FXO)
Content-Length: 0

[5] 20071028210701: BYE Response: Terminate 2f42bb30@pbx
[6] 20071028210702: SIP Rx udp:200.69.181.76:5060:
BYE sip:096312674@200.25.181.62:5060 SIP/2.0
Via: SIP/2.0/UDP 192.168.2.245:5060;branch=z9hG4bK6bb28c677c1e2c
```

From: Carlos<sip:30@200.25.181.62;user=phone>;tag=2DB5241E3BA59572DABF
To: <sip:096312674@200.25.181.62;user=phone>;tag=604857669
Call-ID: 29277-D1B9-1317-6A26-CCE1A47F1DD7@192.168.2.245
CSeq: 8 BYE
User-Agent: WLAN660-S VoIP PHONE
Content-Length: 0

[6] 20071028210702: SIP Tm udp:200.69.181.76:5060:
SIP/2.0 200 Ok
Via: SIP/2.0/UDP 192.168.2.245:5060;branch=z9hG4bK6bb28c677c1e2c;rport=5060;received=200.69.181.76
From: Carlos <sip:30@200.25.181.62;user=phone>;tag=2DB5241E3BA59572DABF
To: <sip:096312674@200.25.181.62;user=phone>;tag=604857669
Call-ID: 29277-D1B9-1317-6A26-CCE1A47F1DD7@192.168.2.245
CSeq: 8 BYE
Contact: <sip:096312674@200.25.181.62:5060;transport=udp>
User-Agent: Master_Box_IP/1.5.2.7
RTP-RxStat: Dur=20,Pkt=652,Oct=164304
RTP-TxStat: Dur=1,Pkt=992,Oct=170624
Content-Length: 0

[9] 20071028210702: Message repetition, packet dropped
[8] 20071028210706: SIP Rx udp:172.16.2.21:5060:
REGISTER sip:172.16.2.1 SIP/2.0
Via: SIP/2.0/UDP 172.16.2.21:5060;branch=z9hG4bK15761199592460810498;rport
From: 21 <sip:21@172.16.2.1>;tag=236647701
To: 21 <sip:21@172.16.2.1>
Call-ID: 1721013724-00112167@172.16.2.21
CSeq: 3247 REGISTER
Contact: <sip:21@172.16.2.21:5060>
Authorization: Digest username="21", realm="172.16.2.1", nonce="69aa43a37370b868b35aa7e9fa8d2b09",

uri="sip:172.16.2.1", response="8c3f26f06233106f5fe2817eef9b9349", algorithm=MD5
max-forwards: 70
expires: 60
user-agent: Voip Phone 1.0
Content-Length: 0

[8] 20071028210706: route_pending_packet -38798: entry=a udp 172.16.2.21 5060
[8] 20071028210706: route_pending_packet -38798: entry=udp 172.16.2.21 5060
[8] 20071028210706: Send Packet 200
[8] 20071028210706: SIP Tx udp:172.16.2.21:5060:
SIP/2.0 200 Ok
Via: SIP/2.0/UDP 172.16.2.21:5060;branch=z9hG4bK15761199592460810498;rport=5060
From: 21 <sip:21@172.16.2.1>;tag=236647701
To: 21 <sip:21@172.16.2.1>;tag=1052151814
Call-ID: 1721013724-00112167@172.16.2.21
CSeq: 3247 REGISTER
Contact: <sip:21@172.16.2.21:5060>;expires=60
Content-Length: 0

4.4.3. Configuracion Gateway

Al igual que todo los anteriores componentes el Gateway tambien se configura via Web accediendo a la IP o dominio asignado al equipo.

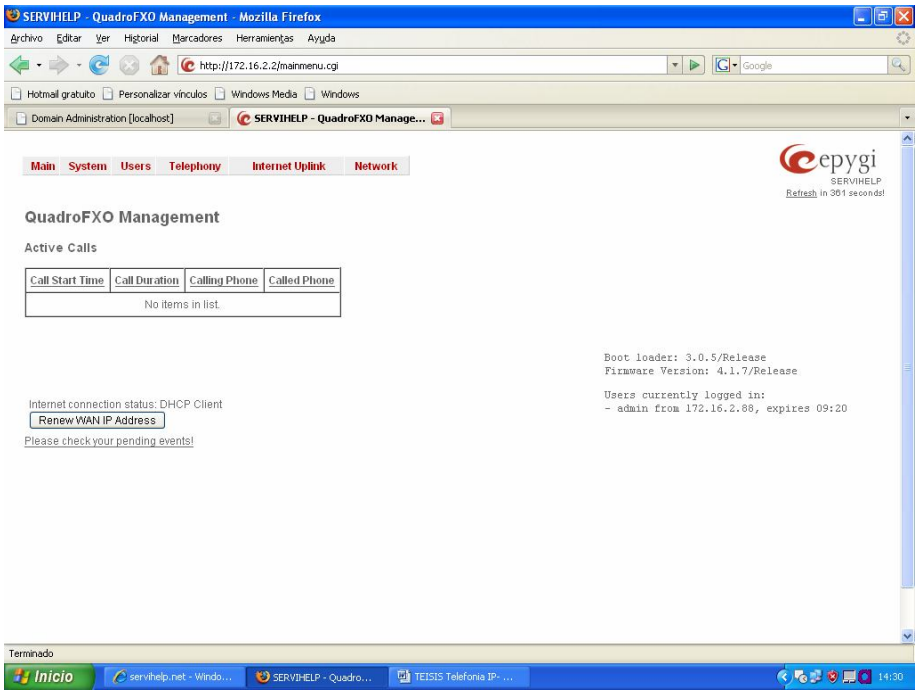

Figura. 4.24. Pagina Gateway

Lo primero que vemos es el Status del Gateway.

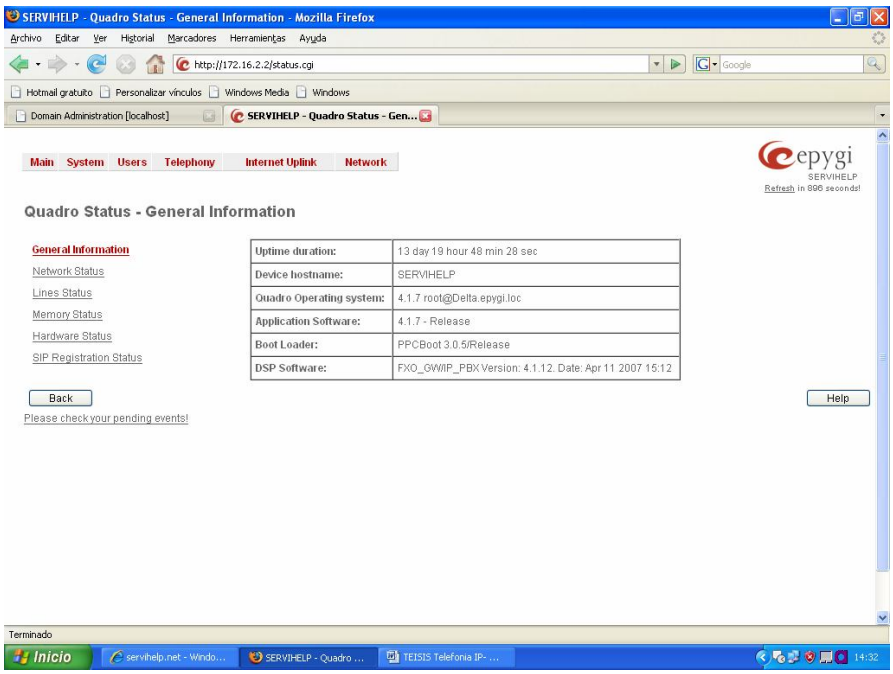

Figura. 4.25. Pagina Gateway - Status

Lo primero a configurar es el Call Routing el cual va a ser el encargado del direccionamiento desde IP hasta la red PSTN.

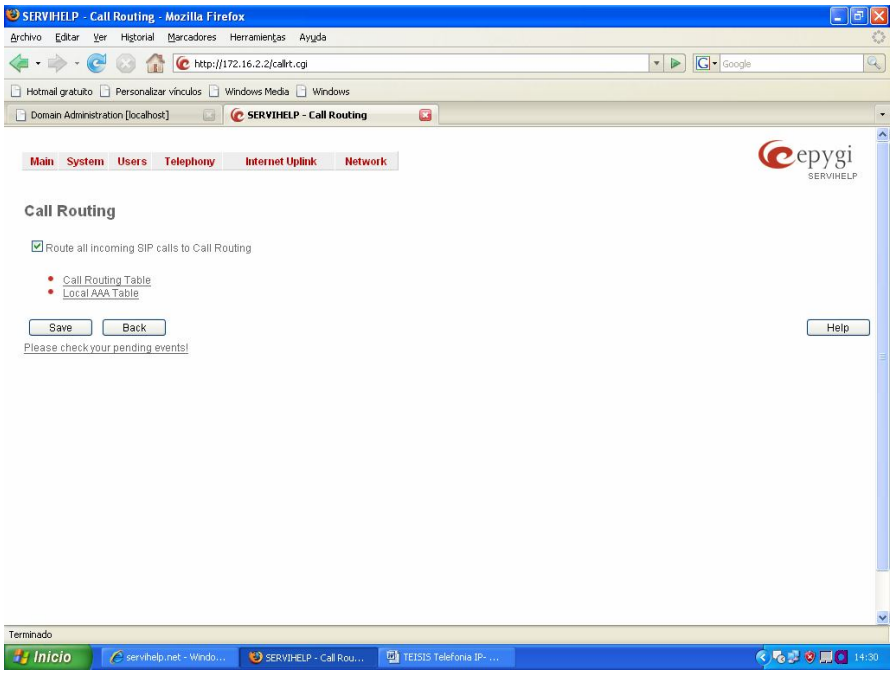

Figura. 4.26. Pagina Gateway – Call Routing

Las reglas de marcado que vemos a continuacion son las qu se aplicaran para todo paquete Sip que apruebe el ingreso, como vemos todo paqute que venga con el 096 ira al puerto FXO numero 6 y asi mismo cualquier otro paquete ira al los puertos FXO 1,2,3.

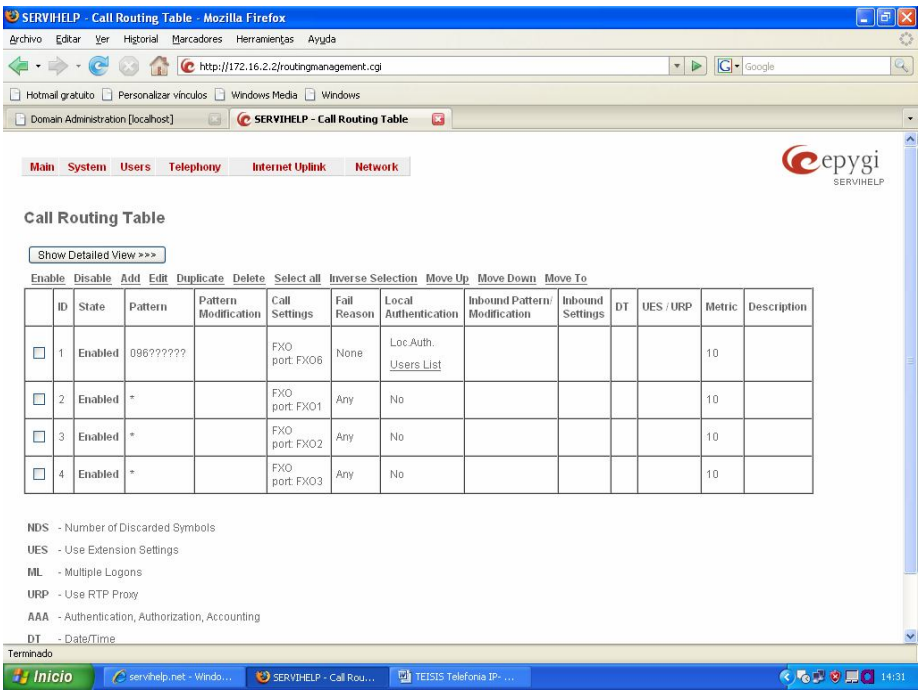

Figura. 4.27. Pagina Gateway – Call Routing Table

A si mismo en el FXO Settings podemos configurar el Incoming de los puertos FXO cuando estos resiban señalización de INVITE por la PUSY o red PSTN.

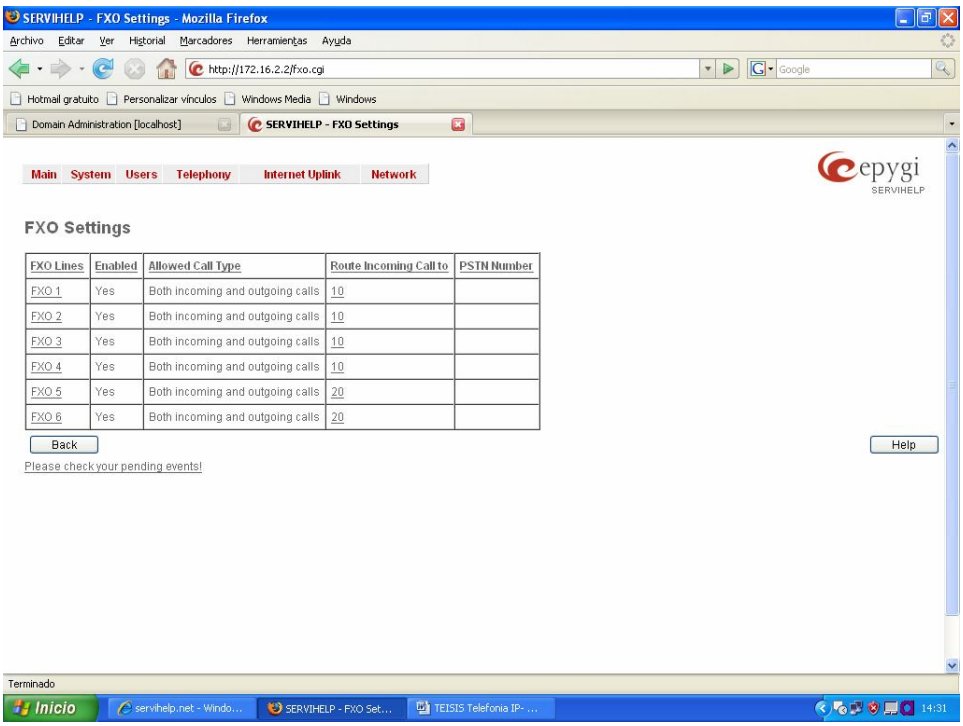

Figura. 4.28. Pagina Gateway – FXO Settings

Asi podemos ver que las primeras lineas timbran al UAC 10 y 20 respectivamente.

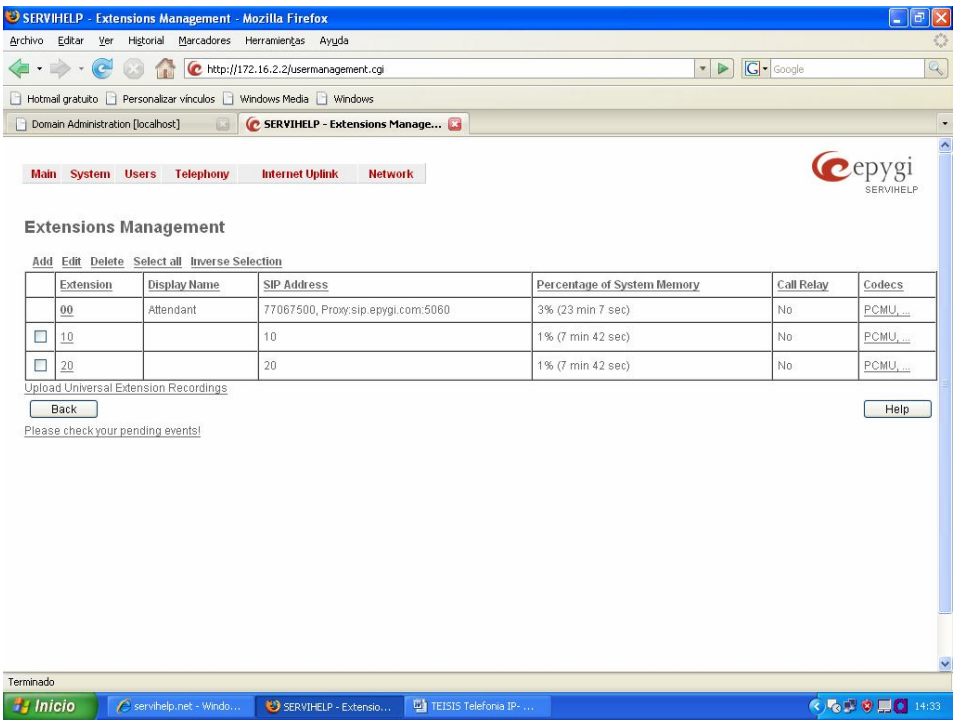

Figura. 4.29. Pagina Gateway – Extensions Managment

Como el gateway esta conectado al internet es susceptible a ataques por lo que el IDS debe estar activo mas el Fierewall, a su ves el NAT en caso de que existan paquetes SIP no nateados.

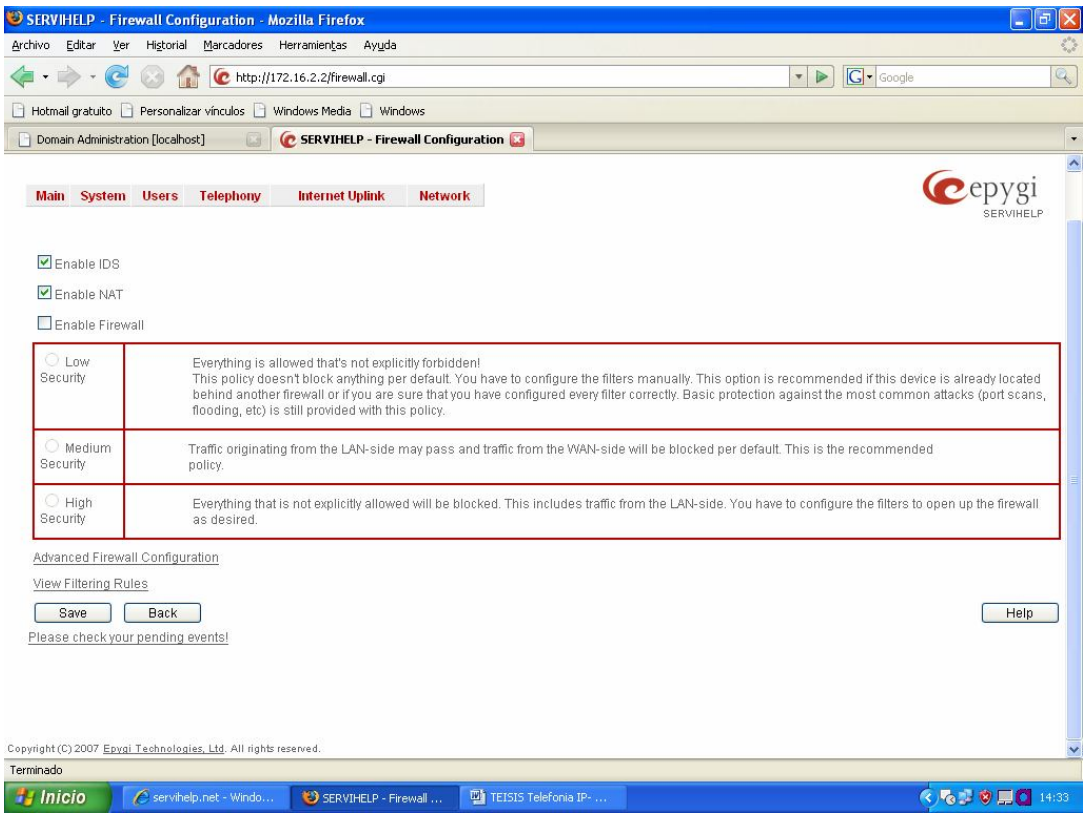

Figura. 4.30. Pagina Gateway – IDS, NAT, Firewall

CONCLUSIONES Y RECOMENDACIONES

Los usuarios van a experimentar varios cambios con una solución IP, el más evidente será el teléfono mismo. Los teléfonos IP son distintos a los teléfonos convencionales porque tienden a tener pantallas grandes a fin de poder manejar algún tipo de navegador de Web simplificado. Dado que el teléfono está conectado a la red de datos, se puede usar para acceder a aplicaciones especiales de Web.

Un cambio todavía más radical puede ser el prescindir por completo del aparato de teléfono y acceder a las funciones de telefonía a través de la computadora, mediante unos audífonos con micrófono y un software especial de telefonía (lo que se llama un “soft phone”).

Uno de los beneficios más importantes de la Telefonia IP es que expertos en temas específicos pueden entrar a la aplicación desde cualquier parte, gracias a lo cual el cliente tiene un acceso directo a las competencias medulares de la empresa de una manera muy eficiente en costos.

Los usuarios de Telefonia IP también se verán afectados de una manera muy positiva por todos los nuevos servicios tales como administración de correo electrónico, interacciones vía Web, las nuevas aplicaciones para teléfonos IP, sistemas de grabación que permiten capturar una llamada completa activándola cuando uno desee, en cualquier momento durante la conversación, la posibilidad de conectar teléfonos con la facilidad de “plug and play”, la posibilidad de instalar sitios remotos a muy bajo costo y muchos más.

REFERENCIAS BIBLIOGRAFICAS

LIBROS:

- GAST MATTHEW S. **Redes wireless 802.11**, Primera Edicion, Anaya Multimedia, Madrid , 1998
- VV.AA. **Hacking wireless**, Segunda Edicion, Anaya Multimedia, Madrid, 1997
- WEBB, WILLIAM. **The future of wireless communications**.
- CISCO, **CCNA1**, Segunda Edicion, Pearson Educacion S.A, Espana, 2004
- CISCO, **CCNA2**, Segunda Edicion, Pearson Educacion S.A, Espana, 2004
- CISCO, **CCNA3**, Tercera Edicion, Pearson Educacion S.A, Espana, 2005
- CISCO, **CCNA4**, Tercera Edicion, Pearson Educacion S.A, Espana, 2005
- BRAMANTE, RICHARD EDWARDS, JAMES MARTIN, **Al Nortel Guide to VPN Routing for Security and VoIP,** Primera Edicion, Wiley.
- KELLY, TIMOTHY V, **VoIP For Dummies,** Primera Edicion, For Dummies.
- **CAMARILLO, GONZALO ROSENBERG, JONATHAN**, SIP Demystified, Segunda Edicion, McGraw-Hill, USA, 2001.
- COLLINS, DANIEL, **Carrier Grade Voice Over IP**, Second Edition, McGraw-Hill, USA, 2002.

PAGINAS WEB:

- REDES INALAMBRICAS, http://es.wikipedia.org/wiki/Comunicaci%C3%B3n_inal%C3%A1mbrica, Redes de comunicacion inalambrica, Referencia historica, Aspectos Tecnicos, Campos Utilizacion.
- FORO VOIP, http://www.zero13wireless.net/foro/, Troncales y linas SIP, Campos SDP y empaqutizacion.
- SIP, H323, IAX, http://www.voipforo.com/, Caracteristicas, arquitecturas y protocolos de tecnologias VoIP y Codecs.
- Software Basado el Windos, http://www.3cx.com

ANEXO 1

BREVE ANALISIS DEL MARCO REGULATORIO

Esta es la resolución del CONATEL para la regulación del uso de frecuencias en el país.

RESOLUCION 538-20-CONATEL-2000

CONSEJO NACIONAL DE TELECOMUNICACIONES
CONATEL
CONSIDERANDO:
Que mediante Ley # 94 del 4 de agosto de 1995, promulgada en el Registro Oficial # 770 del 30 de agosto del mismo año, fue dictada la Ley Reformatoria a la Ley Especial de Telecomunicaciones, mediante la cual crea el Consejo Nacional de Telecomunicaciones CONATEL:

Que el espectro radioeléctrico es un recurso natural limitado y que al no ser utilizado en forma eficiente se desperdicia, en perjuicio del Estado;

Que los sistemas que hacen uso del espectro radioeléctrico en forma eficiente permiten la mejor administración del mismo;

Que los sistemas que utilizan la tecnología de espectro ensanchado *(Spread Spectrum),* utilizan una baja densidad de potencia, que minimiza la posibilidad de interferencia;

Que los sistemas que utilizan esta tecnología pueden coexistir con sistemas de banda angosta, lo que hace posible aumentar la eficiencia de utilización del espectro radioeléctrico;

Que estos sistemas poseen una notable inmunidad a las interferencias que provienen de emisiones similares o de sistemas convencionales haciendo posible la compartición en la misma banda de frecuencia;

Que se hace necesaria la regulación para la operación de sistemas que utilizan esta tecnología; y,

En uso de las atribuciones legales que le confiere el Artículo 10 Título I, Artículo innumerado tercero de la Ley Reformatoria a la Ley Especial de Telecomunicaciones, y en concordancia con el Artículo 41 del Reglamento General a la Ley Especial de Telecomunicaciones Reformada, promulgado según Registro Oficial # 832 del 29 de noviembre de 1995,

RESUELVE:

Expedir la siguiente:

NORMA PARA LA IMPLEMENTACION Y OPERACION DE SISTEMAS DE ESPECTRO ENSANCHADO

DISPOSICIONES GENERALES

NORMA TECNICA

DISPOSICIONES FINALES

DISPOSICIONES GENERALES

Artículo 1: Objetivo. La presente Norma tiene por objeto, regular la instalación y operación de sistemas de radiocomunicaciones que utilizan la técnica de espectro ensanchado *(Spread Spectrum)* en las bandas que determine el Consejo Nacional de Telecomunicaciones, CONATEL.

Artículo 2: Régimen Legal. La implementación y operación de sistemas de espectro ensanchado, se regirá por la Ley Especial de Telecomunicaciones, Ley Reformatoria a la Ley Especial de Telecomunicaciones, Reglamento General a la Ley Especial de Telecomunicaciones Reformada, Reglamento General de Radiocomunicaciones y la presente Norma.

Artículo 3: Definición de Sistema de Espectro Ensanchado. Sistema que utiliza la técnica de codificación, en la cual la señal transmitida es expandida y enviada sobre un rango de frecuencias mayor que el mínimo requerido por la señal de información.

Artículo 4: Términos y Definiciones. Para esta Norma, se utilizarán los términos que tienen las siguientes definiciones.

CONATEL: Consejo Nacional de Telecomunicaciones

Ley Especial: Ley Especial de Telecomunicaciones

Ley Reformatoria: Ley Reformatoria a la Ley Especial de Telecomunicaciones

SNT: Secretaría Nacional de Telecomunicaciones

Secretario: Secretario Nacional de Telecomunicaciones

SUPTEL: Superintendencia de Telecomunicaciones

UIT: Unión Internacional de Telecomunicaciones

Los términos y definiciones para la aplicación de la presente Norma, son los que constan en el Reglamento General a la Ley Especial de Telecomunicaciones Reformada, Reglamento General de Radiocomunicaciones y en el Glosario de Términos de esta

Norma. Lo que no esté definido en dichos reglamentos se sujetará al Glosario de Términos y Definiciones de la UIT.

Artículo 5: Solicitud de Aprobación. Los interesados en instalar y operar sistemas de espectro ensanchado, en cualquier parte del territorio nacional, deberán presentar la solicitud para la aprobación correspondiente, dirigida a la SNT, describiendo la configuración del sistema a operar, el número del certificado de homologación del equipo a utilizar, las características del sistema radiante, las coordenadas geográficas donde se instalarán las estaciones fijas o de base del sistema móvil, localidades a cubrir, y los demás datos consignados en el formulario que para el efecto pondrá a disposición la SNT.

La aprobación de la operación será por un período de 5 años y podrá ser renovado previa solicitud del interesado, dentro de los treinta (30) días anteriores a su vencimiento.

Artículo 6: Registro. El Registro se lo realizará en la SNT previo el pago de los valores establecidos en el artículo 15 de esta Norma.

Artículo 7: Delegación del Secretario. El CONATEL autoriza al Secretario, aprobar la operación de Sistemas de Espectro Ensanchado Privados.

NORMA TECNICA

Artículo 8: Características de los Sistemas de Espectro Ensanchado. Los sistemas de espectro ensanchado son aquellos que se caracterizan por:

Distribución de la energía media de la señal transmitida, dentro de un ancho de banda mucho mayor que el ancho de banda de la información;

La energía de la señal emplea un código seudoaleatorio independiente al de los datos;

Mayor ancho de banda de transmisión, con una densidad espectral de potencia más baja y un mayor rechazo de las señales interferentes de sistemas que operan en la misma banda de frecuencias;

Posibilidad de compartir el espectro de frecuencias con sistemas de banda angosta convencionales, debido a que es posible transmitir una potencia baja en la banda de paso de los receptores de banda angosta;

Permiten rechazar altos niveles de interferencias;

La señal transmitida resultante, con secuencia directa, es una señal de baja densidad de potencia y de banda ancha que se asemeja al ruido. La señal transmitida resultante con salto de frecuencia permanece un corto período de tiempo en cada frecuencia de salto de la banda y no se repite el uso del canal hasta después de un largo período de tiempo;

Permite alta privacidad de la información transmitida;

La codificación de la señal proporciona una capacidad de direccionamiento selectiva, lo cual permite que usuarios que utilizan códigos diferentes puedan transmitir simultáneamente en la misma banda de frecuencias con una interferencia admisible;

Utilización eficaz del espectro, debido a la mayor confiabilidad en la transmisión, en presencia de desvanecimientos selectivos, que los sistemas de banda angosta; y,

Tiene ganancia de procesamiento.

Artículo 9: Clases de Sistemas de Espectro Ensanchado.

a) Espectro Ensanchado por Secuencia Directa *(Direct Sequence)*. Técnica de modulación que mezcla la información de datos digital con una secuencia seudoaleatoria digital de alta velocidad que expande el espectro. Esta señal es mezclada en un modulador con una frecuencia portadora entregando una señal modulada BPSK o QPSK, para obtener una emisión con baja densidad espectral, semejante al ruido.

b) Espectro Ensanchado por Salto de Frecuencia (*Frequency Hopping*). Técnica de ensanchamiento en el cual la frecuencia portadora convencional es desplazada dentro de la banda varias veces por segundo de acuerdo a una lista de canales seudoaleatoria. El tiempo de permanencia en un canal es generalmente menor a 10 milisegundos.

c) Espectro Ensanchado Híbrido. Combinación de las técnicas de estructuración de la señal de espectro ensanchado por secuencia directa y por

Artículo 10: Operación y Configuración de Sistemas de Espectro Ensanchado en las Bandas ICM.

a) Se aprobará la operación de sistemas de radiocomunicaciones que utilicen la técnica de espectro ensanchado, en las bandas de frecuencias ICM indicadas a continuación:

902 – 928
MHz

2.400 – 2.483,5
MHz

5.725 – 5.850
MHz

b) La operación de los sistemas en modo de espectro ensanchado de secuencia directa, salto de frecuencia o híbridos, se aprobará con las siguientes configuraciones:

Sistemas fijos punto a punto;

Sistemas fijos punto – multipunto;

Sistemas móviles;

Sistemas de explotación: cuando la aplicación que se dé a un Sistema de Espectro Ensanchado corresponda a la prestación de un servicio de Telecomunicaciones, se deberá tramitar paralelamente el Titulo Habilitarte requerido de conformidad con la Ley Especial de Telecomunicaciones y su Reglamento General; y,

Las demás configuraciones que el CONATEL defina.

Artículo 11: Bandas de Frecuencias. El CONATEL aprobará la operación en bandas distintas a las indicadas en el Artículo 10 cuando la producción de equipos sea estándar por parte de los fabricantes, y que a su tiempo se describirán en el formulario de solicitud, al que se hace referencia en el Artículo 5. Asimismo, el CONATEL aprobará también las características técnicas de los equipos en bandas distintas a las indicadas.

Artículo 12: Sistemas de Reducido Alcance. Los sistemas que utilicen espectro ensanchado para aplicaciones de transmisión de datos en redes de área local (LAN), telemetría, lectura remota, PBX y teléfonos inalámbricos cuya potencia de salida del transmisor sea menor o igual a 100 mili vatios (Mw.) no requerirán de aprobación expresa. En todo caso, la antena deberá ser omnidireccional con una ganancia máxima de 1 dBi y encontrarse adherida al equipo.

Dentro de los estándares que cumplen con estas especificaciones se encuentran: 802.11 y 802.11b del IEEE, *Bluetooth*, entre otros.

Los equipos que se comercialicen libremente en el país deberán contar con el certificado de homologación otorgado por la SNT, de conformidad con el Artículo 14 de la presente Norma.

Artículo 13: Características de Operación.

a) Categoría de Atribución.

La operación de los sistemas de espectro ensanchado y de los sistemas fijos y móviles convencionales es a título secundario respecto a los sistemas ICM.

Los sistemas punto a punto convencionales aprobados tendrán la misma categoría de atribución que los sistemas de espectro ensanchado aprobados.

b) Potencia Máxima de Salida.

Para los sistemas con salto de frecuencia o secuencia directa que operen en las bandas de 2.400 – 2.483,5 MHz ó 5.725 – 5.850 MHz, la potencia máxima de salida del transmisor autorizado será de 1 vatio.

Para los sistemas con salto de frecuencia que operen en la banda de 902 – 928 MHz la potencia máxima de salida del transmisor será la siguiente:

Sistemas que empleen a lo menos 50 saltos de frecuencias: 1 vatio

Sistemas que empleen entre 25 y 50 saltos de frecuencias: 0,25 vatios

Si la ganancia de la antena direccional empleada en los sistemas fijos punto a punto y punto – multipunto que operan en la banda 2.400 – 2.483,5 MHz es superior a 6 dBi, deberá reducirse la potencia máxima de salida del transmisor, de 1 vatio, en 1dB por cada 3

dB de ganancia de la antena que exceda de los 6 dBi. Los sistemas fijos punto a punto y punto – multipunto que operen en la banda 5.725 – 5.850 MHz podrán utilizar antenas con una ganancia superior a 6 dBi, sin reducir la potencia máxima del transmisor.

Los sistemas que no sean punto a punto y punto – multipunto, y que empleen antenas direccionales con ganancias superiores a 6 dBi, deberán reducir la potencia máxima del transmisor, mencionada en los párrafos anteriores, en el mismo número de dB que sobrepase los 6 dBi de ganancia de la antena.

c) Intensidad de Campo Eléctrico.

La intensidad de campo máxima permitida para las emisiones de los equipos de espectro ensanchado, a que hace referencia esta Norma, deberá cumplir con los siguientes valores para las bandas mencionadas:

Frecuencia Asignada en las bandas (MHz) Intensidad de campo de la frecuencia fundamental (mV/m) Intensidad de campo de las armónicas (mV/m)
902 – 928
50
500
2.400 – 2.483,5
50
500
5.725 – 5.850
50
500

Cuadro # 1

Los límites de intensidad de campo indicados en el Cuadro # 1 serán medidos a 3 metros de distancia de la antena y corresponden al valor medio.

La emisión de radiaciones fuera de la banda, con la excepción de las armónicas, deberá estar atenuada a lo menos 50 dB bajo el nivel de la frecuencia asignada.

d) Anchos de banda de emisión y condiciones de uso de los canales.

Sistemas de Salto de Frecuencia

Los sistemas que empleen salto de frecuencia tendrán sus canales separados como mínimo a 25 kHz, o el ancho de banda a 20 dB del canal de salto, el que sea mayor. Todos los canales serán usados en condiciones de igualdad en base a una lista de frecuencias administrada por una secuencia seudo aleatoria.

Para los sistemas de salto de frecuencia que operan en la banda 902 – 928 MHz, si el ancho de banda a 20 dB del canal de salto de frecuencia es menor a 250 kHz, el sistema usará a lo menos 50 saltos de frecuencias y el promedio de tiempo de ocupación en cualquier frecuencia no podrá ser superior a 0,4 segundos dentro de un período de 20 segundos. Si el ancho de banda a 20 dB del canal de salto de frecuencia es mayor o igual a 250 kHz, el sistema deberá utilizar a lo menos 25 saltos de frecuencias y el promedio de tiempo de ocupación en cualquier frecuencia no deberá ser mayor que 0,4 segundos en un período de 10 segundos. El máximo ancho de banda a 20 dB permitido en un canal de salto es de 500 kHz.

Los sistemas que operen con salto de frecuencia en las bandas de 2.400 – 2.483,5 MHz y 5.725 – 5.850 MHz deberán utilizar a lo menos 75 saltos de frecuencias. El ancho de banda máximo a 20 dB del canal de salto será de 1 MHz. El promedio de tiempo de

ocupación de cualquier frecuencia no deberá ser mayor a 0,4 segundos en un período de 30 segundos.

Sistemas de Secuencia Directa.

Los sistemas de espectro ensanchado que operen con secuencia directa, tendrán un ancho de banda a 6 dB de al menos 500 kHz.

La densidad espectral pico de potencia de salida a la antena no deberá ser superior a 8 dBm en un ancho de 3 kHz durante cualquier intervalo de tiempo de transmisión continua.

e) Ganancia de Procesamiento.

Los sistemas que empleen secuencia directa deberán tener al menos 10 dB de ganancia de procesamiento y los de salto de frecuencia al menos 75 dB.

Los sistemas híbridos que empleen una combinación de salto de frecuencia y secuencia directa deberán tener una ganancia de procesamiento combinada de al menos 17 dB.

Artículo 14: Homologación. Todos los equipos de espectro ensanchado que se utilicen en el país deberán ser homologados por la SNT.

Los equipos, para los fines de homologación, se clasificarán en:

Equipos de reducido alcance

Equipos de gran alcance

a) Equipos de Reducido Alcance.

La homologación de los equipos de reducido alcance se efectuará en base a las características estipuladas en el catálogo técnico del equipo. Estos equipos deberán cumplir con el Artículo 12 de esta Norma. Se considerarán dentro de los estándares que cumplen con los requisitos de los equipos de reducido alcance los siguientes:

- 802.11 y 802.11b del IEEE.

- Parte 15.247 del FCC, con una potencia menor o igual a 100 mW.

- *Bluetooth* versión V.1.

- *BRETS* 300.328 (Especificaciones técnicas de la Comunidad Europea para equipos de transmisión de datos que operen en la banda de 2,4 GHz y usen la técnica de espectro ensanchado).

- ISC RSS210 del Canadá.

- TELEC Radio Regulation de Japón; y, otros que el CONATEL considere pertinentes.

Todos los equipos de reducido alcance deberán tener adherida la antena a la caja de éste y, además, tener una antena con una ganancia máxima de 1 dBi.

b) Equipos de Gran Alcance.

La homologación de los equipos de gran alcance se realizará para todos los equipos que tengan una potencia de salida de 100 mW o superior y que no tengan su antena adherida al equipo, ó que la ganancia de la antena sea superior a 1 dBi. La homologación se realizará en base a una copia del certificado de homologación que recibió el fabricante

del equipo de parte de la FCC de los Estados Unidos, o de alguna Administración de los países de la Comunidad Europea, de Canadá, Japón y otras que considere en el futuro el CONATEL. En todo caso, el equipo deberá cumplir con las características de los sistemas estipuladas en el Artículo 13 de esta Norma.

DISPOSICIONES FINALES

Artículo 15: Derechos para la Operación de Sistemas de Espectro Ensanchado. Quienes obtengan de la SNT la aprobación para la operación de sistemas de espectro ensanchado, excepto para aquellos sistemas que no requieren de aprobación expresa, según lo mencionado en el Artículo 12, deberán cancelar anualmente por anticipado, por concepto de uso del espectro radioeléctrico, durante el período de cinco (5) años, el valor en dólares de los Estados Unidos de América, que resulte de la aplicación de la fórmula que se indica a continuación:

IA (Imposición Anual) = 4 x K x B x NTE (dólares)

B = 12

Para los sistemas punto a punto y punto – multipunto.

B = 0,7 x NA

Para los sistemas móviles. (Se considerará para el cálculo de IA un NTE mínimo de cincuenta (50) estaciones, entre bases y móviles).

B = 39

Para los sistemas de radiolocalización de vehículos (NTE es el número de estaciones de recepción de triangulación, que tendrá un valor mínimo de tres (3) estaciones).

Donde: K = Indice de inflación Anual

NA = Número de áreas de operación

NTE = Es el número de estaciones fijas, bases y móviles y estaciones receptoras de triangulación, de acuerdo al sistema.

Artículo 16: Ejecución.- De la ejecución de la presente Norma encárguese a la SNT.

Artículo 17: Control.- La Superintendencia de Telecomunicaciones realizará el control de los sistemas que utilicen esta tecnología y vigilará porque ellos cumplan con lo dispuesto en la presente Norma y las disposiciones Reglamentarias pertinentes.

Disposición Transitoria

Todos los sistemas que utilizan la tecnología de espectro ensanchado y que se encuentran en operación, deberán proceder a registrarse en la SNT y cumplir con lo dispuesto en esta Norma, en el plazo de 90 días a partir de la fecha de su publicación en el Registro Oficial. Quedan exceptuados del registro sólo los equipos de reducido alcance mencionados en el Artículo 12 de la presente Norma.

Dado en Quito el 31 de octubre del 2000.

Ing. José Pileggi Véliz

PRESIDENTE DEL CONATEL

Dr. Julio Martínez

SECRETARIO DEL CONATEL

ANEXO 2

RESPUESTAS SIP

La definición de las respuestas SIP y el comportamiento de los UA en relación con las mismas se realizan 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.

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.

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.

180 *Ringing*

Esta respuesta se usa para indicar que el *INVITE h*a 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 *Aíert-lnfo.*

181 *CalI 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.

182 *Call queued*

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

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.

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.

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.

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.

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.

300 *Muítipíe 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.

301 *Moved Permanentíy*

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.

302 *Moved Temporariíy*

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.

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.

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.

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.

400 *Bad Request*

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

401 *Unauthorized*

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

402 *Payment Required*

Esta respuesta se mantiene para uso futuro.

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.

404 *NotFound*

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.

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*.

406 *NotAcceptabíe*

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.

407 *Proxy A uthentication Required*

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

408 *Request Timeout*

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

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.

412 *Conditiona! 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.

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.

414 *Request-URI Too Long*

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

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.

416 *Unsupported URI Scheme*

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

420 *Bad Extensión*

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.

421 Extensión *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.

422 *Session Timer Interva! Too Smaíí*

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 Mm-SE.

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

423 *Interva! 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.

429 *Pro vide Referror ldentity*

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.

480 *Temporariíy Unvaiíabíe*

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.

481 *Diaíog/Transaction Does Not Exist*

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

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.

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 *MaxForwards* puesto a 0.

484 *Address Incompíete*

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

485 *Ambiguous*

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

486 *BusyHere*

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.

487 *Request Terminated*

Se enviará como respuesta a un *BYE* o *CANCEL*.

488 *Not Acceptabíe 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.

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.

491 *RequestPending*

Se usa para resolver posibles re-I*NVITEs* simultáneos realizados por ambas partes del diálogo.

493 *Request Undecipherabíe*

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.

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

500 *Server* Interna! 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.

501 *Not 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.

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.

503 *Service Unavailable*

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

504 *Server Time out*

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*.

505 Versión *Not Sup ported*

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

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.

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.

600 *Busy Everywhere*

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

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.

604 *Does 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.

606 *NotAcceptable*

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.

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.

CONTENIDOS EN MÉTODOS Y RESPUESTAS

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.

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.

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.

Alert-lnfo

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.

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.

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 RFC 3265, siendo aplicable lo que en ella figura.

CalI-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 RFC 3261, siendo aplicable lo que en ella figura.

CalI-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.

Contad

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 RFC 3261, 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.*

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 RFC 3261, siendo aplicable lo que en ella figura.

Date

Indica la fecha y hora en que la petición o respuesta se envía por primera vez. Su definición y uso aparece en la RFC 3261, siendo aplicable lo que en ella figura.

Diversión

Se usa en casos de desvíos de llamada para indicar al llamado quién o quienes han realizado desvíos y por qué motivo.

Expires

Proporciona el tiempo relativo tras el cual el mensaje o contenido expira. Su definición y uso aparece en la RFC 3261, siendo aplicable lo que en ella figura.

From

Identifica al usuario que origina la petición. Su definición y uso aparece en la RFC 3261, siendo aplicable lo que en ella figura.

Mm-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 RFC 4028, siendo aplicable lo que en ella figura.

Organization

Se usa para indicar la organización a la que pertenece el que origina el mensaje. Su definición y uso aparece en la RFC 3261, siendo aplicable lo que en ella figura.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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 pérdidas 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.

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.

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.

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.

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.

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.

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.

Vía

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.

CONTENIDOS SÓLO EN RESPUESTAS

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.

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.

Mm-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.

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.

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.

Proxy-Authentication-I nfo

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.

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.

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.

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.

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,* 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.

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.

Unsupported

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

Warning

Se usa para proporcionar información adicional sobre el estado de una respuesta. Su definición y uso aparece en la RFC 3261, siendo aplicable lo que en ella figura.

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 RFC 3261, siendo aplicable lo que en ella figura.

CONTENIDOS SÓLO EN MÉTODOS

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.

Authorization

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

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.

In-Reply-To

Se utiliza en caso de devolución de llamadas perdidas o sesiones no establecidas, y enumera los *CalI-Id* de las llamadas que devuelve la petición en la que va la cabecera. Su definición y uso aparece en la RFC 3261, siendo aplicable lo que en ella figura.

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 RFC 391 1, siendo aplicable lo que en ella figura.

Max-Forwards

Sirve para limitar el número de saltos de un método. Su definición y uso aparece en la RFC 3261, siendo aplicable lo que en ella figura.

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.

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 RFC 3261, siendo aplicable lo que en ella figura.

Proxy-Authorization

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

Proxy-Require

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

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 RFC 3262, siendo aplicable lo que en ella figura.

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 RFC 3515, siendo aplicable lo que en ella figura.

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 RFC 3892, siendo aplicable lo que en ella figura.

Reject-Contact

Forma parte de las extensiones de SIP, que permiten al usuario que envía la petición y 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.

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 RFC 3891, siendo aplicable lo que en ella figura.

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 RFC 3841 siendo aplicable lo que en ella figura.

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.

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 recibida en la respuesta 2XY al *PUBLISH* correspondiente a la publicación inicial. Su definición y uso aparece en la RFC 3903, siendo aplicable lo que en ella figura.

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 RFC 3261, siendo aplicable lo que en ella figura.

Subscription-State

Indica el estado de la suscripción. Su definición y uso aparece en la RFC 3265, siendo aplicable lo que en ella figura.

CAMPOS CABECERA DEL CUERPO DE LOS MENSAJES

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.

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.

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.

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.

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.

Mime Versión

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.

CAMPOS SDP

La definición de campos SDP se realiza en la RFC 2327, siendo 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 un 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.

PROCEDIMIENTOS

En los siguientes puntos 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.

PROCEDIMIENTO DE ENCAMINAMIENTO

Es aplicable lo definido en la RFC3261. No obstante en los terminales conectados a la red VOIP 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 el Terminal envía todas sus peticiones a un *outbound Proxy*, independientemente del valor del *Request*-URI. 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.

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 Red VOIP es el SIP URI.

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

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 Red se soporta sobre un plan de numeración, 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 Red VOIP no deben incluir el número de puerto donde la petición SIP será enviada. Este valor es opcional en la RFC 3261.