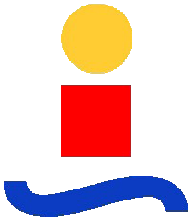
Diseño y Configuración de dos Plataformas de Interfonía H.323

Proyecto Fin de Carrera

Departamento de Ingeniería Sistemas y Automática

Área de Ingeniería Telemática

Universidad de Sevilla



Autor del proyecto:

Ramón Montoya Benito

Tutor del proyecto:

Francisco José Fernández Jiménez

Sevilla, Junio de 2006

Índice:

Agradecimientos

Quisiera inicialmente agradecer a mi tutor Francisco José Fernéndez Jiménez, profesor del Área de Ingeniería Telemática del Departamento de Ingeniería de Sistemas y Automática, por su apoyo y paciencia sin reservas ante tantas dudas que me surgieron durante la elección y redacción del presente proyecto.

También quiero agradecer a Revenga Ingenieros S.A. su amable acogida en el seno empresarial, experiencia que me dio tantos e inestimables conocimientos para afrontar los trabajos del Ingeniero de Telecomunicación. Es sin duda gracias a la confianza depositada en mí, a sus recursos y equipos, y a su calidad emprendedora, como este proyecto ha tenido lugar. En especial, quisiera agradecer a Marcos Reboredo, director del departamento de Desarrollo de Negocio en la empresa, su apoyo y comprensión en los momentos difíciles, y su guía y consejo sobre el oficio. Y también a Merche Albacar, responsable del departamento de Recursos Humanos, por su apoyo y su amistad en el seno de la empresa.

Por último, a mi madre, Ana María Benito Fernández, cuya constante cercanía y amor me ha llenado de fuerzas en todos los momentos de mi vida, y en especial en este capítulo tan importante en el que doy el paso definitivo a mi dedicación laboral.

A todos ellos, gracias, muchas gracias.

Objetivos

En el siguiente documento se expone el proyecto fin de carrera titulado *Diseño y configuración de dos Plataformas de Interfonía H.323*, perteneciente al Área de Ingeniería Telemática del Departamente de Ingeniería de Sistemas y Automática de la Escuela Superior de Ingenieros de la Universidad de Sevilla, y realizado por el alumno Ramón Montoya Benito. El tutor del proyecto ha sido Francisco José Fernández Jiménez, profesor asociado de este centro.

Este proyecto resulta de una beca de colaboración entre la Escuela Superior de Ingenieros de la Universidad de Sevilla y la empresa Revenga Ingenieros S.A. Consecuentemente, algunos planteamientos de partida, decisiones tecnológicas, comentarios y conclusiones, serán referidos en el marco de este entorno empresarial.

Durante el transcurso del período de contratación se llevaron a cabo numerosos trabajos relacionados con la interfonía IP. Entre ellos se ha seleccionado el diseño y la configuración de dos plataformas de interfonía sobre el protocolo H.323, desarrolladas e instaladas por Revenga Ingenieros S.A. durante el otoño del pasado 2005, y actualmente en funcionamiento.

Dichas plataformas se referían a la instalación de plataformas H.323 sobre redes locales, para prestar un servicio de información y atención al público mediante interfonía. Una de ellas presenta características limitadas de ampliabilidad para la plataforma, mientras que en la otra esta ampliabilidad resultaba fundamental. Para ambas plataformas, se trataba de conmutar comunicaciones de interfonía típicamente analógicas a VoIP, aprovechando las redes de datos de los clientes para la transmisión de estas comunicaciones de voz.

El presente proyecto tiene como objetivo fundamental la introducción y aplicación a las tecnologías de VoIP; en concreto a las comunicaciones VoIP basadas en estándares abiertos, que permiten la interoperabilidad de distintos fabricantes, permitiendo la optimización tanto de la funcionalidad como de los costes.

0. Resumen de contenidos

Los siguientes capítulos se estructurarán de la siguiente forma:

- **Introducción**: Tras un breve comentario sobre el significado de las comunicaciones de interfonía, en este capítulo se describirán las tecnologías VoIP con más auge en la actualidad, con especial atención a los protocolos H.323 y SIP. A continuación, se analiza el estado del arte de las tecnologías y servicios VoIP, con especial hincapié en la situación del mercado.

- **El estándar H.323**: Este capítulo estudia en profundidad el protocolo H.323 en el que se basan las plataformas de interfonía. Se divide principalmente en documentación, arquitectura, y protocolos involucrados. Este capítulo pretende darle al lector la oportunidad de conocer este protocolo, presentando para ello un formato general, sencillo y correcto.

- **Desarrollo**: A continuación se dará paso al nudo del proyecto, en el que se introducen los equipos utilizados, se explican los pasos de diseño y la selección de los terminales VoIP para ambas plataformas, y se detalla exhaustivamente la configuración de todos equipos involucrados. También comentaremos algunas herramientas de monitorización y depuración de las plataformas, así como algunos problemas surgidos durante el desarrollo y la puesta en marcha de las plataformas, y sus soluciones. Para finalizar, se presenta una discusión acerca de la ingeniería de integración en la que se basan las plataformas, analizándose las alternativas existentes en el mercado, así como algunas interesantes aplicaciones para el presente proyecto.

- **Presupuesto**: Aquí se incluye el presupuesto de todo el proyecto (de ambas plataformas), así como el diagrama de Gannt y la división en tareas asociados.

- **Conclusiones**: En este apartado se analizan los resultados obtenidos para todo el proyecto. A continuación se proponen algunas ampliaciones para el mismo.

- **Apéndice A: Auditorías de VoIP**: Se incluye, por último, un apéndice en el que se estudian las auditorías de red para VoIP, cruciales para la planificación de proyectos VoIP.

1. Introducción

El presente proyecto contiene el diseño y configuración de dos plataformas de interfonía sobre redes IP[1], ambas instaladas por Revenga Ingenieros S.A. y actualmente en funcionamiento. Una de ellas sustenta el sistema de información disponible al usuario acerca del moderno sistema de control de accesos por videovigilancia instalado en el Barrio de las Letras de Madrid. La otra, el sistema de información y emergencias de la recientemente inaugurada estación de Bailén, en el Metro de Valencia.

Un sistema de interfonía no es sino un sistema de telefonía en el que algunos terminales presentan funcionalidad reducida: los interfonos. En éstos, para generar una llamada bastará con pulsar un simple botón. Así, de cara al público usuario, no será necesario marcar ni conocer ningún número de teléfono o abonado, lo cual es fundamental para que el sistema de comunicación sea cómodo y sencillo: atractivo para su uso en esos escenarios.

Debido a la popularidad del mundo IP, las grandes empresas y conglomerados públicos están desplegando unas redes IP por fibra de una capacidad aún desaprovechada. Esto, sumado a la fiabilidad cada día mayor en las redes de datos, hace que ya actualmente se opte por una conmutación de las comunicaciones de interfonía, tradicionalmente analógica, por vía IP.

Se puede decir que actualmente nos encontramos en la era de la digitalización de las comunicaciones, gracias a la que pueden desarrollarse fácilmente importantes capacidades computacionales sobre estas comunicaciones. El desarrollo de servicios avanzados que aprovechen estas capacidades es fruto de una necesidad de avance no sólo científico y tecnológico, sino también humano.

[1] IP: *Internet Protocol*, protocolo de Internet.

1.1 Introducción tecnológica

1.1.1 Tecnologías de VoIP

La voz sobre IP son las tecnologías que permiten comunicaciones de voz sobre el cada vez más extendido protocolo IP, lo cual, en particular, permite que el servicio de telefonía pueda ofrecerse a través de Internet [1].

Estas tecnologías se basan en múltiples protocolos y servicios, entre los cuales se destacarán los siguientes:

- **COPS**: el *Common Open Policy Service*, RFC[2] 2748 [2], de la IETF[3] [3], describe un modelo cliente-servidor que gestiona políticas de control para protocolos que permitan QoS[4].
- **ENUM**: *Electronic Numbering*, RFC 3761 [4], en el que se describe la traducción de números E.164[5] a esquemas de direccionamiento IP (como son direcciones H.323, SIP o de correo electrónico).
- **IMS**: *IP Multimedia Subsystem* [5], aún en desarrollo, comenzó como parte de la tecnología seleccionada para el diseño de la tercera generación de telefonía móvil desarrollada en el 3GPP[6], pero posteriormente se ha desarrollado como un estándar en sí mismo. Está basado en SIP.
- **MGCP**: *Media Gateway Control Protocol* [6], protocolo de señalización y control para conexiones VoIP.
- **PINT**: *PSTN/Internet Interworking*[7], RFC 2848 [7], protocolo de invocación de servicios de telefonía adicionales, habitualmente usado como una extensión de las capacidades de SIP.
- **SCCP**: *Cisco Skinny Client Control Protocol*, protocolo propietario de Cisco para la comunicación entre los servidores Cisco CallManager y sus teléfonos VoIP.
- **SCTP**: *Stream Control Transmission Protocol*, RFC 3286 [8] de la IETF, es un nuevo protocolo de transporte IP, equivalente a UDP[8] y TCP[9], y que incluye múltiples funciones adicionales para el transporte de telefonía IP.
- **T.37** y **T.38**: de la ITU[10] [9], y en la RFC 3362 [10] su equivalente de la IETF, para la transmisión de fax sobre IP.

---

[2] RFC: *Request for Comments*, documentos base para estándares y publicaciones tecnológicas.
[3] IETF: *Internet Engineering Task Force*, organismo internacional de estandarización.
[4] QoS: *Quality of Service*, calidad de servicio.
[5] La E.164 es una conocida recomendación de la ITU-T para la definición de un plan de numeración internacional.
[6] 3GPP: *3rd Generation Partnership Project*, acuerdo de colaboración para definir los estándares que regulen la tercera generación de teléfonos móviles.
[7] PSTN: *Public Switched Telephonic Network*, red pública de telefonía conmutada.
[8] UDP: *User Datagram Protocol*.
[9] TCP: *Transmission Control Protocol*.
[10] ITU: *International Telecommunications Union*, organismo estandarizador internacional.

- **TRIP**: *Telephony Routing over IP*, RFC 3219 [11], se trata de un protocolo entre servidores interdominio, que publica la alcanzabilidad y las características de los destinos de telefonía asociados a esos dominios, independientemente del protocolo de señalización utilizado.

Sin embargo, y en cuanto a protocolos no propietarios, los más importantes y extendidos protocolos de comunicaciones para VoIP son H.323 y SIP:

- **H.323**, de la ITU, es un conjunto de estándares para la comunicación multimedia sobre redes de paquetes que no proporcionan calidad de servicio (QoS), soportando así conferencias no sólo de audio, sino también de vídeo y de datos [12].

  Entre estos estándares se encuentra H.323 propiamente dicho, el cual describe el uso de las especificaciones H.225.0 y H.245, así como el de otros documentos relacionados con el transporte de servicios de conferencia multimedia basados en paquetes. En la especificación H.225.0 se describen los protocolos de señalización: RAS (*Registration Admission Status*), y el protocolo *Call Signaling* (de señalización de llamada), extraído de la Q.931. Y en la especificación H.245 se describe el protocolo de control multimedia. Estas especificaciones básicas ya se incluyen desde la versión 1.

  En la versión 2, el estándar se amplía con la inclusión de las especificaciones H.235 para seguridad y H.450 para servicios suplementarios, y con la integración de T.120 para comunicaciones de datos. Y en las versiones 3, 4 y 5 se añaden diversos anexos para comunicaciones interdominio, extensibilidad e incluso movilidad.

  Para el transporte, usa RTP[11] (RFC 3550 [13]).

  Además, define una serie de elementos de red que soportan cierta funcionalidad, como son el Gatekeeper, encargado del direccionamiento, y las MCUs, encargadas de habilitar y gestionar multiconferencias.

  Pero la característica clave de la arquitectura H.323 es la definición, en el mismo documento de la especificación, de máquinas de estado explícitas para cada servicio particular.

  Este protocolo es el que soporta actualmente la mayoría de las comunicaciones de VoIP, entre otros motivos por haber sido el primero en desarrollarse.

- **SIP**, RFC 3261, de la IETF, *Session Initiation Protocol*, no es sino un protocolo de la capa de sesión, que sirve para crear, modificar y terminar sesiones entre uno o más participantes [14]. Sus funciones principales son:

  - Localización de recursos/participantes.
  - Invitación a sesiones de servicio.
  - Negociación de parámetros de sesión.

[11] RTP: *Real-Time Transport Protocol*, protocolo de transporte para tiempo real.

Su funcionamiento se parece mucho al de HTTP: es un protocolo modo texto, que funciona en un esquema *request-response*, y que, en su especificación base, comporta un conjunto muy reducido de métodos. La descripción de los contenidos de cada método se consigue mediante el uso del protocolo SDP *Session Description Protocol*, RFC 2327 [15]. Como el contenido de las sesiones es transparente a SIP, podrá describirse cualquier tipo de sesión: desde llamadas de teléfono hasta juegos online o comunicaciones de realidad virtual. Para el transporte se usa típicamente RTP (al igual que H.323).

En definitiva, se trata de un protocolo cuya filosofía principal es la modularidad y generalidad, orientado a Internet, y que ha pasado a formar parte de la 3G móvil bajo el IMS[12]. Sin embargo, esta generalidad ha hecho que sus extensiones, desarrolladas para servir a múltiples aplicaciones de servicio, resulten difíciles de compatibilizar.

1.1.2 Comparación H.323 - SIP

Mucho se ha escrito en lo referente a la bondad de uno u otro protocolo [16]. H.323 presenta una arquitectura cerrada, en la que se define exhaustivamente cada servicio y cada elemento de la red, desde la forma de codificación (ASN.1[13]) hasta las máquinas de estado. Por el contrario, su desarrollo y ampliación resulta difícil y costoso.

SIP, en cambio, presenta una arquitectura modular, fácilmente ampliable, que se adecúa a un formato HTTP[14], adaptándose así directamente a Internet (frente al desarrollo de H.323 más orientado a redes locales, debido en parte a su temprano uso). Bajo esta arquitectura, cada desarrollador puede escoger no sólo su particular forma de ofrecer el servicio sino también de definirlo y de ampliarlo. También permite una fácil integración con cualquier otro servicio de Internet.

Por otro lado, suele caracterizársele a SIP por tener raíces en la comunidad IP, habiendo sido estandarizado y gobernado por el IETF; mientras que a H.323, desarrollado en el seno de la ITU, se le asocia un origen más en el seno de la industria de las telecomunicaciones. A pesar de que las dos organizaciones han participado de alguna forma en la definición de ambos protocolos.

Quizás esta última premisa haya sido la responsable de la aparición de muchos detractores del protocolo H.323; pero sus razones no siempre son suficientes:

- Ante la afirmación de que H.323 es un protocolo anticuado, no puede menos que recordarse que se encuentra en constante revisión y desarrollo.
- Ante la observación de que resulta demasiado complejo, puede afirmarse que H.323 resuelve perfectamente la inclusión de vídeo en las comunicaciones y los esquemas de tarificación de llamadas; que muchas implementaciones del protocolo SIP resultan

[12] IMS: *Internet Multimedia Subsystem*, parte de la 3GP móvil que trata de definir unas redes de telefonía móvil basadas en IP.
[13] ASN.1: *Abstract Syntax Notation* 1, lenguaje de definición de una sintaxis abstracta para la representación de datos de manera independiente de la máquina.
[14] HTTP: *HyperText Transfer Protocol*, lenguaje de transferencia hipertexto para las comunicaciones *World Wide Web*.

tremendamente pesadas, que en efecto el hecho de que la implementación no esté definida hace que en muchos casos éstas no sean estables, o que SIP puede no resultar tan liviano al tener que compartir muchísimos códigos de estado HTTP.

- Ante el comentario de que H.323 ha intentado erróneamente traspasar la arquitectura PSTN a las redes de paquetes, se argumenta que su interoperabilidad con ella es mucho mejor que la que ofrece SIP. Ante la afirmación de que SIP es mucho más flexible y escalable que H.323, responden que SIP es, tan sólo, más simple. Y ambos poseen librerías de código abierto en continuo desarrollo [17].

H.323 define sus extensiones del protocolo en nuevas y complejas versiones (por supuesto, siempre compatibles con las versiones anteriores), que van apareciendo en función de las necesidades de la VoIP con el transcurso del tiempo. Desde luego, para que los nuevos servicios introducidos en las versiones más recientes tengan aplicación en una red H.323 es necesario que todos sus componentes las compartan; pero, debido al refinamiento de las capacidades ofrecidas por las últimas versiones, no es habitual encontrarse con equipos que permitan actualizaciones de *firmware* para las versiones nuevas.

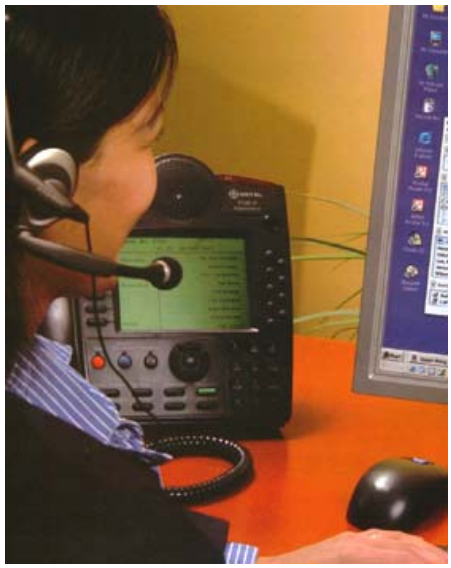
Por otro lado, las extensiones del protocolo en SIP definen nuevas cabeceras, nuevos métodos o nuevos códigos de respuesta [18]. Pero el hecho de que no haya especificación explícita para la definición de servicios suplementarios ha hecho que el IETF, desde diversos grupos de trabajo (*Working Groups*), se haya dedicado a publicar numerosos trabajos:

- Creación de un marco de trabajo para el control de llamada [19].
- Concreción el servicio de transferencia de llamada [20].
- Interoperabilidad con la PSTN (con todo un grupo de trabajo, el PINT) [21]
- Incluso ha propuesto (paralelamente con la ITU, que lo utiliza para H.323 desde su versión 4) la integración con MEGACO para la descripción de arquitecturas de pasarelas.
- Todo esto, además de otros trabajos destinados a aclarar algunas situaciones, como la confiabilidad de respuestas provisionales [22], o la relación entre las preferencias del origen y las capacidades del destino de las sesiones [23].

Las consecuencias son que, en realidad, implementaciones muy completas del protocolo SIP presenten una complejidad similar a la ofrecida en H.323, y que parezca, incluso, que ambos protocolos puedan tender a hacerse muy similares con el paso del tiempo.

Actualmente, la inmensa mayoría de los sistemas VoIP activos y en funcionamiento usan H.323; y, mientras durante un tiempo los productos SIP fueron mucho más económicos que los H.323, debido a la enorme complejidad del protocolo H.323 frente a la simplicidad de SIP a la hora de implementar las características básicas de las comunicaciones de voz, hace poco que los precios comienzan a equipararse, gracias a la especificación de terminal simple de la versión 3 de H.323. Pero, por otro lado, existe una mayor parte de los operadores de VoIP en Internet que, cuando operan con protocolos de código abierto, utilizan SIP. Y también es muy importante el detalle de la inclusión de SIP en el IMS. Actualmente, aún se encuentra el mercado por decidir.

1.2 Estado del arte



1.2.1 Interfonía IP

Hoy en día, la primera respuesta de Google (y fuera de los enlaces patrocinados) ante la entrada “interfonía IP” es el sistema Interfonic de Revenga Ingenieros S.A., para el que se ha desarrollado el presente proyecto.

En efecto, mientras coexisten múltiples posibilidades y opciones en el mercado de la telefonía IP, la interfonía, bastante más restrictiva por el requerimiento de un terminal lo más sencillo posible (el interfono), no se ha desarrollado aún sobre IP, a pesar de sus variadas posibilidades de uso:

- Por ejemplo, con interfonos inteligentes, que permitan la programación interna de la llamada en función de parámetros de red, esta interfonía podría instalarse en entornos residenciales:
- Por ejemplo, teléfonos IP para la tercera edad, que resuelvan una comunicación por ejemplo de emergencia con una o varias personas, en función de la franja horaria o del estado de ocupación de los posibles destinos de la llamada. Esta programación podría ser actualizada por gestores de red que, en este caso, podrían ser los mismos destinatarios de la llamada; por ejemplo, con programación por páginas web.
- Otro ejemplo sería su uso en porteros automáticos por IP que se integrasen con redes telefónicas y que pudieran, en función de la franja horaria, establecer una llamada hacia un teléfono móvil, varias llamadas simultáneas, etc. Y aún podrían sumarse capacidades de vídeo.

De cualquier forma, para todo esto parece fundamental la integración en un estándar internacional. Así la plataforma de interfonía permitiría futuras interoperabilidades, ampliaciones o reducciones, independientes de la empresa con la que se contrata el producto (dejando aparte el soporte técnico imprescindible).

Actualmente sólo existen en el mercado soluciones integrales y propietarias de interfonía IP, orientadas a satisfacer desde comunicaciones directas entre secretarias y jefes hasta grandes conglomerados de servicios (entornos ferroviarios, aeropuertos) [24]. Ejemplos de este tipo

de equipamiento y de sus sistemas de comunicaciones se muestran en las figuras 1 y 2, respectivamente.

Figura 1: Gama de accesorios de interfonía de Digital Acoustics.

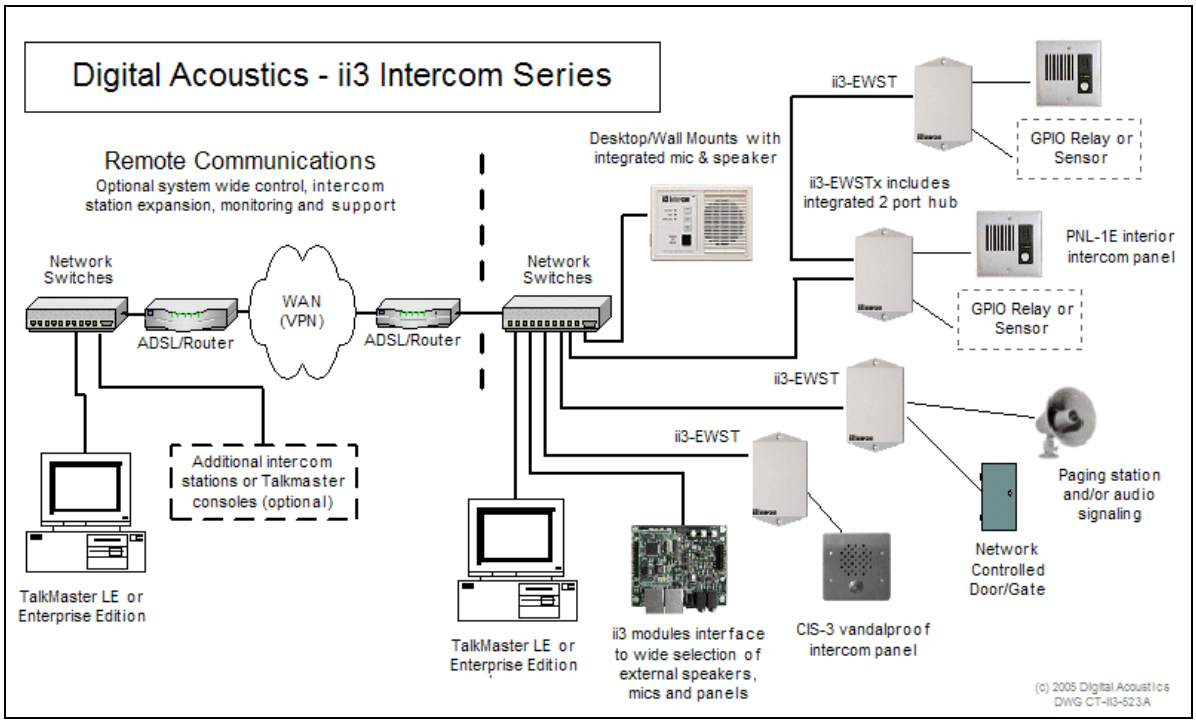


Figura 2: Esquema de comunicaciones de interfonía sobre protocolo propietario de Digital Acoustics.

Mientras, en el marco de la telefonía IP las funcionalidades más impresionantes se encuentran en pleno desarrollo. Para verlas en detalle, elaborando al mismo tiempo algunos esquemas de sus causas o posibles significados a nivel de mercado, se pasará a continuación al estudio del estado del arte de la Voz sobre IP. Este estudio proporcionará un mucho mayor grado de detalle y perspectiva; y, en la medida en que la VoIP engloba a la telefonía IP, también englobará a la interfonía IP.

1.2.2 VoIP

La Voz sobre IP es un concepto que se reduce a la transmisión de voz por redes de datos sobre el protocolo IP. De esta forma pueden, además, atravesar Internet.

La VoIP ha traído consigo dos características que han superado a las redes tradicionales de telefonía: el aumento de la funcionalidad y la reducción de costes.

Pero no sólo eso: también ha aparejado una modificación fundamental en el espectro de mercado de las telecomunicaciones: la transición hacia un modelo de negocio basado en provisión de servicios sobre banda ancha.

1.2.2.1 Aumento de la funcionalidad

El aumento de la funcionalidad, con respecto al servicio ofrecido por el POTS[15] y las GSTN[16], podría parecer quizás aún incipiente, debido a su lenta penetración.
Pero es que, por ejemplo, con **Skype** [25], el servicio VoIP de Internet pionero, *peer-to-peer*, gratuito y ahora además de código abierto [26], se permiten cómodas multiconferencias, además de chat, intercambio de archivos y comunicaciones de vídeo mediante webcam, sin dejar de subrayar la movilidad del usuario hasta allí adonde llegue Internet.

En cuanto a consumibles, en el mercado pueden encontrarse:

- Desde teléfonos IP inalámbricos que funcionan sobre una cuenta Skype [27] o Vonage [28], hasta teléfonos IP de lujoso diseño con pantalla táctil [29] (figura 3).
- Desde mínimas pasarelas de un solo puerto FXS[17] para transformar el teléfono analógico al mundo IP [30], hasta fabricantes de TDMoIP para encapsular TDM[18] en protocolos VoIP [31].
- Y, además, las múltiples opciones de teléfonos software, con o sin vídeo, para PC o PocketPC, en plataformas de desarrollo abiertas o con tecnologías propietarias [32].

[15] POTS: *Public Old Telephony Service*, antiguo servicio público de telefonía.
[16] GSTN: *General Switched Telephone Networks*, entre las que se incluyen tanto las PSTN como las redes privadas analógicas.
[17] FXS: *Foreign eXchange Subscriber*, interfaz analógica dirigida hacia un usuario. Por una FXS debe suministrarse tono de marcado al descolgarse (entonces el circuito analógico queda abierto), voltaje para el tono de llamada, tonos de marcado y de proceso de la llamada (en frecuencias), y corriente para suministrar batería durante la comunicación.
[18] TDM: *Time Division Multiplexing*, forma de multiplexado habitual en redes de circuitos.

Figura 3: El teléfono IP de pantalla táctil i.Picasso 6000.

Por otro lado, una de las corporaciones líder en el desarrollo de soluciones VoIP orientadas a empresa, **Cisco Systems**, ofrece entre sus productos más avanzados el ***Cisco Customer Voice Portal***[19] [33], una aplicación AVVID[20] para las redes propietarias SCCP de Cisco.

Este portal, integrando reconocimiento de voz (ASR[21]) y capacidades TTS[22], constituye una potentísima herramienta para la gestión automatizada de centros de llamadas (*call centers*). Y permite, por ejemplo, pagos de facturas, compra y reserva de productos, o petición de información, sin la participación de operadores humanos, además, por supuesto, de soluciones híbridas en las que la participación de estos operadores resulte necesaria. Todo esto, con unas opciones de seguridad en la red de proceso impresionantes. Un esquema general de la infraestructura CCVP se muestra en la figura 4:

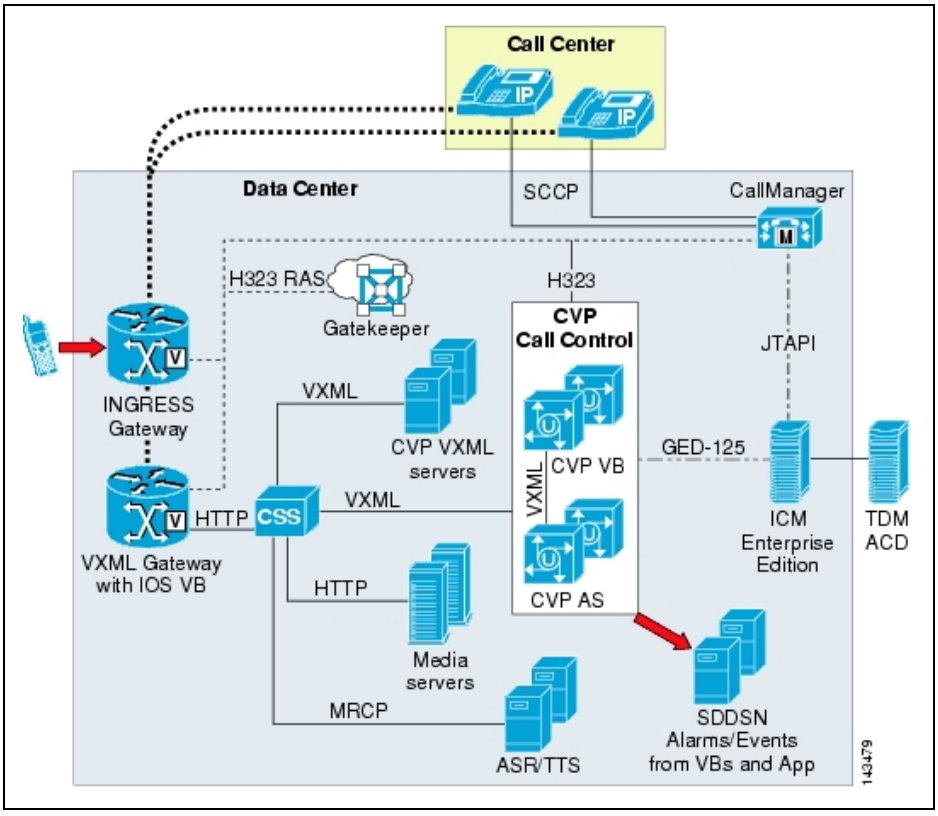


Figura 4: Esquema de aplicación del Cisco Customer Voice Portal (CCVP).

[19] *Cisco Customer Voice Portal*: un portal de voz personalizado, de Cisco.
[20] AVVID: *Architecture for Voice, Video and Integrated Data*, arquitectura par voz, vídeo, y datos integrados.
[21] ASR: *Authomatic Speech Recognition*, reconocimiento de voz automático.
[22] TTS: *Text To Speech*, traducción de textos escritos a voz.

Radicalmente opuestas a la solución Cisco se encuentran las centralitas VoIP de código abierto sobre plataformas libres, como es el caso de la célebre **Asterisk** [34], la cual, junto con su manual de configuración, se adjunta en el CD, en la carpeta `Archivos Adjuntos\Varios\Asterisk`. Esta centralita, aunque aún no ofrece *Authomatic Speech Recognition*, sí que ofrece, entre otras capacidades:

- IVR[23].
- TTS.
- Reproducción de música para llamadas en espera.
- Grabación de conversaciones.

Además, estas centralitas se basan en estándares internacionales (SIP, H.323, MGCP).

Esto permite la ampliación de sus redes de control y gestión mediante el desarrollo de aplicaciones integrables en el sistema, como servidores SNMP, etc; así como la integración con elementos de red compatibles como teléfonos IP, servidores de direccionamiento o pasarelas de los distintos fabricantes que se acojan a los mismos estándares.

Confrontando las dos posibilidades anteriores, una solución propietaria de uno de estos gigantes multinacionales ofrecerá muchas ventajas en cuanto a fiabilidad y soporte técnico, e incluso en cuanto a tiempo de puesta en marcha, aunque el precio resulte tremendamente más elevado. Claro, que este coste habría que añadírselo, en comparación con la solución ofrecida por centralitas libres y gratuitas, en:

- Auditorías de red.
- Integración.
- Pruebas.
- Tolerancia a fallos.
- Mantenimiento.
- Y además, el personal cualificado capaz de llevar todas estas tareas a cabo.

Es posible que, en definitiva, la primera opción resulte óptima para una gran corporación, mientras que la segunda parece más adaptable a entornos PYMEs[24].

Por otro lado, todas las soluciones anteriormente expuestas permiten la integración con las redes de telefonía tradicionales:

- Skype mediante la asignación de un número de teléfono de momento sólo norteamericano.
- Asterisk mediante interfaces FXS y FXO.
- Cisco también con tecnologías TDM.

[23] IVR: *Interactive Voice Response*, respuesta a dígitos marcados mediante grabaciones de voz.
[24] PYME: Pequeña Y Mediana Empresa: hasta 150 trabajadores.

Y es que la PSTN aún funciona bastante mejor que la VoIP, pues, a pesar de que las conexiones analógicas entre el abonado y la central presentan una respuesta ante el ruido que en muchos casos puede distorsionar enormemente la señal, las transmisiones TDM asignan un *slot* de información fijo a cada usuario, en los grandes enlaces telefónicos entre centrales: es decir, que no suceden pérdidas de paquetes [35].

Las redes de paquetes aún no pueden ofrecer esta calidad de servicio *carrier class*[25] por dos motivos:

- El primero, porque se obvian las planificaciones de ancho de banda necesarias para que las comunicaciones en tiempo real sobre estas redes dispongan de holgado rendimiento, (es decir, auditorías de red, que en algunos casos necesitarían ser periódicas, y en otros incluso continuas).
- Y el segundo, porque no se ofrece una QoS, en los equipos de LAN[26] y, sobre todo, en las redes WAN[27], que ya comienza a ser imprescindible para diferenciar tipos de tráfico.

1.2.2.2 Reducción de costes

En este sentido, podría esperarse que los proveedores de servicio en Internet ofrecieran diferentes tarifas por tráfico (BW[28] por ejemplo) en función de la calidad de servicio contratada.

Porque, en efecto, la reducción de costes aparejada a la VoIP proviene del hecho de que las redes de datos no tarifiquen por volumen de datos transmitidos, sino por ancho de banda contratado. En efecto, con el modelo de tarifa plana, todas las llamadas sobre VoIP resultan "gratuitas" una vez se han pagado las cuotas de inscripción en el servicio. Algo totalmente opuesto al modelo de tarificación tradicional PSTN y de telefonía móvil, basado en tiempo de conexión, en el tiempo de ocupación de un circuito. Ahora, de hecho, existen muchos operadores de telefonía VoIP que, con sedes en distintos países, sólo tienen que conmutar las llamadas internacionales por IP a las redes nacionales, ahorrándose unos costes que les permiten ofrecer económicas soluciones de voz con tarjetas de prepago para este mercado de la telefonía internacional.

1.2.2.3 Modificación del modelo de negocio de telefonía

Y es que, por un lado, es posible que se esté desbancando el modelo de negocio tradicional, basado en las redes propietarias de telefonía fija y en la tarificación por tiempo de conexión: este modelo parece sustituirse por el de una tarifa plana de conexión a Internet sobre la que la telefonía se ofrecería como un servicio adicional.

---

[25] *Carrier class*: la clase portadora se refiere a hardware y software usado en redes redes de alta velocidad. Implica transferencias extremadamente fiables, bien testeadas y probadas. También reciben el nombre de *carrier grade*.
[26] LAN: *Local Area Network*, redes de area local.
[27] WAN: *Wide Area Network*, redes de area extensa.
[28] BW: *Band Width*, ancho de banda.

En este sentido, ya existen numerosas empresas intentando consolidarse en este escenario: Skype, VoipBuster, VoipStunt, Gizmo, P4Gphone, DialPad, Sip2Go, Vonage, NetZeroVoice, VoiceEclipse, Skypho, Stanaphone, TotalCall, o Jajah, son sólo algunos ejemplos de proveedores de servicio de VoIP en Internet [36], muchos usando tecnologías propietarias, otros trabajando bajo estándares como SIP. Y la mayoría de ellas, además de ofrecer comunicaciones PC → PC gratuitas, reducen ostensiblemente los costes de las comunicaciones, unidireccionales (es decir, PC → PSTN), a nivel internacional. Incluso ya el nuevo gran gigante de las tecnologías de la información, Google, se ha introducido en el mercado con su sistema VoIP GoogleTalk [37].

No en vano, ya todas las empresas de telecomunicaciones del territorio nacional ofrecen, acompañando a sus ofertas de acceso a Internet, todas las llamadas nacionales entre teléfonos fijos gratuitas. Esto es producto, sencillamente, del aprovechamiento de una pequeña parte del bucle desagregado para tales efectos, por parte de las compañías no propietarias de la red fija. En España, el 72% de las empresas y el 15% de los hogares dispone de conexión a Internet por banda ancha [38]. Los ingresos por telefonía para los operadores de telefonía fija, en lo que respecta a estos usuarios se han reducido a las comunicaciones internacionales (por otro lado mucho más baratas mediante telefonía IP y proveedores de servicio en Internet, como ya se ha comentado), y, sobre todo, a las comunicaciones con la telefonía móvil. Además, los servicios de telecomunicaciones requieren cada día más ancho de banda, y, a pesar de que en España la banda ancha genera muchísimas quejas entre los consumidores [39], nuestro país se sitúa en el onceavo puesto mundial en cuanto a penetración de la banda ancha (figura 5), habiendo experimentado un crecimiento del 48% durante todo el pasado 2005 [40]. En la figura 5, la primera barra representa las conexiones por DSL, y la segunda el resto (en millones de conexiones):

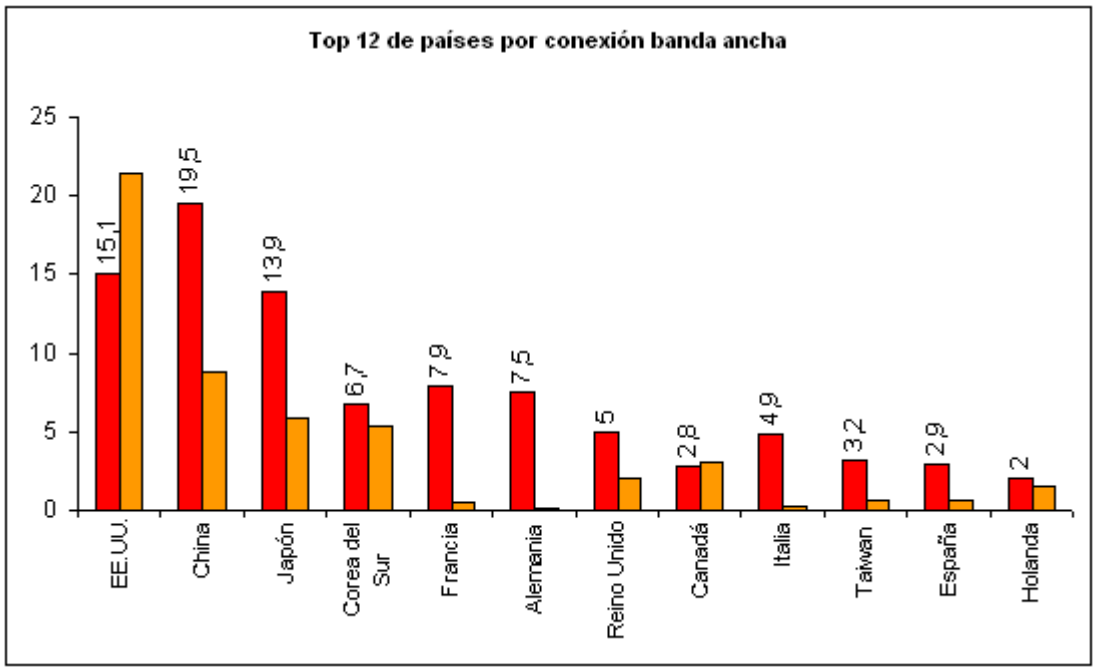


Figura 5: Top 12 de países por conexión a Internet en banda ancha.

Es, por otro lado, la regulación de la VoIP un escollo a salvar para la definición del mercado. Ya se discutía, allá por el año 2004, tanto en el marco internacional como en el nacional [41], y en España aún no se han concluido las actuaciones, entre otras cosas, por la

confrontación con la definición de servicio universal asociada al servicio de telefonía disponible al público. Aunque ya muchos otros países han tomado resoluciones provisionales al respecto [42].

Como consecuencia, aún no resulta fácil recibir una llamada en un PC desde un teléfono de la PSTN. Pero es que ya existen operadores de VoIP internacionales que ofertan llamadas gratuitas hacia teléfonos fijos españoles [43], y que, una vez establecido este marco regulatorio nacional, podrían desplazar a los operadores tradicionales de telefonía fija nacionales, al menos en cierta cuota de mercado [44].

Y tampoco podría dejar de augurarse que, en cuanto se consolide la 3G móvil, esta telefonía podría orientar su modelo de negocio a una definición de acceso de datos móvil basada también en tarifas planas sobre las que, una vez estas tarifas resulten competitivas con el mercado fijo [45], comiencen a usarse aplicaciones de VoIP (sin olvidar el compromiso del UMTS[29] de basar en el estándar SIP su núcleo IMS).

Más allá, ¿se basará la tarificación de la **NGN**[30] (en cuya definición se ofrece QoS independiente de la tecnología de transporte) en múltiples opciones de contrato, cada una orientada a un servicio distinto, o en un *pack* completo y una factura única? En relación con esto, ha de reseñarse la actual tendencia de las grandes multinacionales a fusionarse entre sí, y en cuanto a telecomunicaciones, de ofrecer ***triple play***: televisión, teléfono e Internet, en una única factura [46].

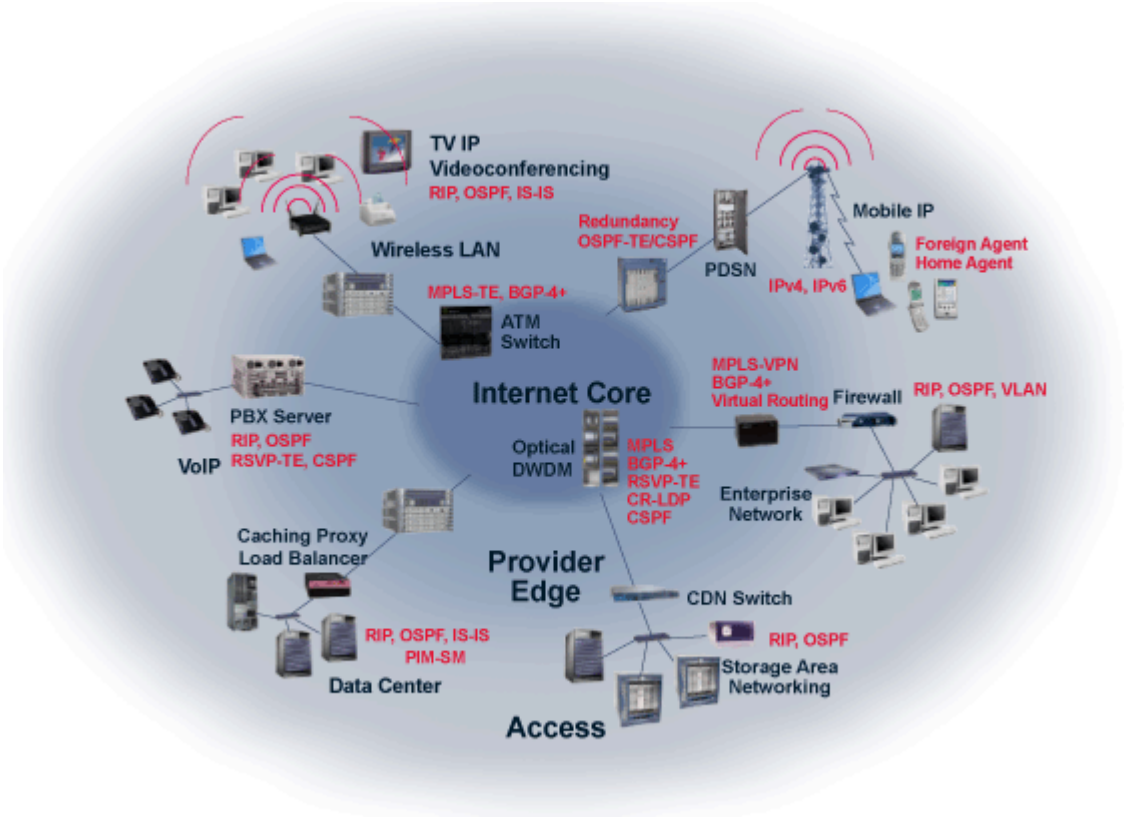


Figura 6: Esquema de la NGN.

[29] UMTS: *Universal Mobile Telecommunications System*, estándar para la definición de la tercera generación de telefonía móvil.
[30] *Next Generation Networks*, las redes futuras.

1.2.2.4 El futuro de la VoIP

En efecto, la VoIP ha significado un enorme avance en las tecnologías de servicios. Y es que la tecnología IP ha superado en intensidad, sobre todo debido al impresionante auge de Internet, a cualquier otra. Pero la VoIP también ha significado un fuerte impulso a otras comunicaciones de datos en tiempo real, como por ejemplo las videoconferencias (que ya se integran en numerosas aplicaciones de telefonía IP).

La televisión interactiva ha comenzado a participar del mercado de las telecomunicaciones: Telefónica ofrece Imagenio [47], que utiliza una conexión telefónica para realimentar la interactividad. Entre los operadores de cable, ONO presentó su nuevo servicio de Vídeo bajo demanda, llamado OJO [48]. Y también hay que resaltar la puesta en funcionamiento, por parte de uno de los proveedores de servicio de banda ancha más importantes de nuestro país, Jazztel, de un proyecto piloto para ofertar televisión a través de ADSL[31] [49]. Todo esto en competencia con la nueva oferta de TDT[32], en el apartado de radiodifusión.
Cada jugador hace su apuesta, pero ¿llegará el momento en el que el *broadcast* se sustituya por el acceso interactivo? Mientras, parece que el mercado de FTTH[33] se consolida en Japón, donde se pueden contemplar velocidades de acceso a Internet de 100Mbps [50].

Pero esto no es todo: aún quedan muchas tecnologías por aparecer, por entrar en juego: como los servicios relacionados con las instalaciones domóticas, de telecontrol vía portal doméstico, con relación a la NGN. Y, un poco más adelante, y en cuanto a tiempo real, la realidad virtual.

Piensen por ejemplo en la definición de un espectro olfativo, con un vector gigante de selección de sustancias olfativas, acompañado a continuación de datos de intensidad para cada una de las sustancias que existan en cada instante de codificación. O en un sistema de codificación de impulsos nerviosos, mediante el cual puedan comunicarse los nervios del sistema humano que se activen, cada uno representando una información de carácter electromagnético y/o químico, en cada instante de tiempo. Imaginen las necesidades de ancho de banda para este tipo de señales.

De cualquier forma, no cabe duda de que la VoIP ha variado el mercado de las telecomunicaciones, quizás marcado por una globalización tan potenciada por Internet, en donde las empresas compiten a un nivel directamente internacional, y en el que muchas empresas se han quedado fuera de juego, a pesar de que la tecnología y el nicho de mercado eran nuevos. Y es que las nuevas tecnologías no pueden dejar de contemplarse desde el punto de vista del mercado, porque en realidad son los usuarios quienes deciden su avance, su utilidad.

Mientras ya se habla de un 13% de todas las comunicaciones de voz, en el mercado residencial de Europa Occidental, para el 2008 [51], ya se pueden advertir de alguna forma las pautas de desarrollo de una tecnología de nueva entrada en un ámbito estrictamente global como es Internet. No cabe duda de que las nuevas tecnologías orientadas al público general requieren de una aceptación por parte de este público, que depende entre otras cosas de la facilidad del uso de estas tecnologías, o en el interés que esta sensación de progreso

[31] ADSL: *Asymmetric Digital Subscriber Line*, línea digital de alta velocidad que se apoya en el par trenzado del bucle de abonado de las redes de telefonía tradicionales.
[32] TDT: Televisión Digital Terrestre.
[33] FTTH: *Fiber To The Home*, fibra hasta el hogar, tecnología de bucle de abonado basada en fibra óptica.

despierta en cada particular entramado cultural. De hecho, y en cuanto a su relación con lo anterior, la entrada de la VoIP depende de dos factores:

- Uno, la familiaridad con el servicio de telefonía, vigente desde finales del siglo XIX, y que se ha mostrado crucial en el espectacular desarrollo de la telefonía móvil.
- Y otro, los accesos de banda ancha, y el uso de los servicios de acceso en Internet.

¿Podría esperarse una analogía entre el comportamiento de esta banda ancha, y de todos los servicios a ella asociados –VoIP, videoconferencias, portales domóticos, TV-, y el *boom* de la telefonía móvil?

La decisión de lo que hace falta y de lo que no, se rompió con la telefonía móvil. Pero, ¿cómo entonces definir un servicio universal? ¿Lo es la televisión, lo es la banda ancha? Y, además, ¿dónde se encuentra la saturación del cliente? ¿Nos estamos saliendo de las necesidades naturales del ser humano, en cuanto a telecomunicaciones?

Nuestro cometido, como creadores de telecomunicaciones, consiste en saldar esas necesidades. Y, también, en crearlas.

2. El estándar H.323

2.1 Documentación y pila de protocolos

El estándar **H.323**, desarrollado por la **ITU-T** desde 1996, es un documento "paraguas" que describe el uso de un conjunto de especificaciones para el transporte de servicios de conferencia multimedia basados en paquetes [52]. La pila de protocolos completa para H.323 se muestra en la figura 7:

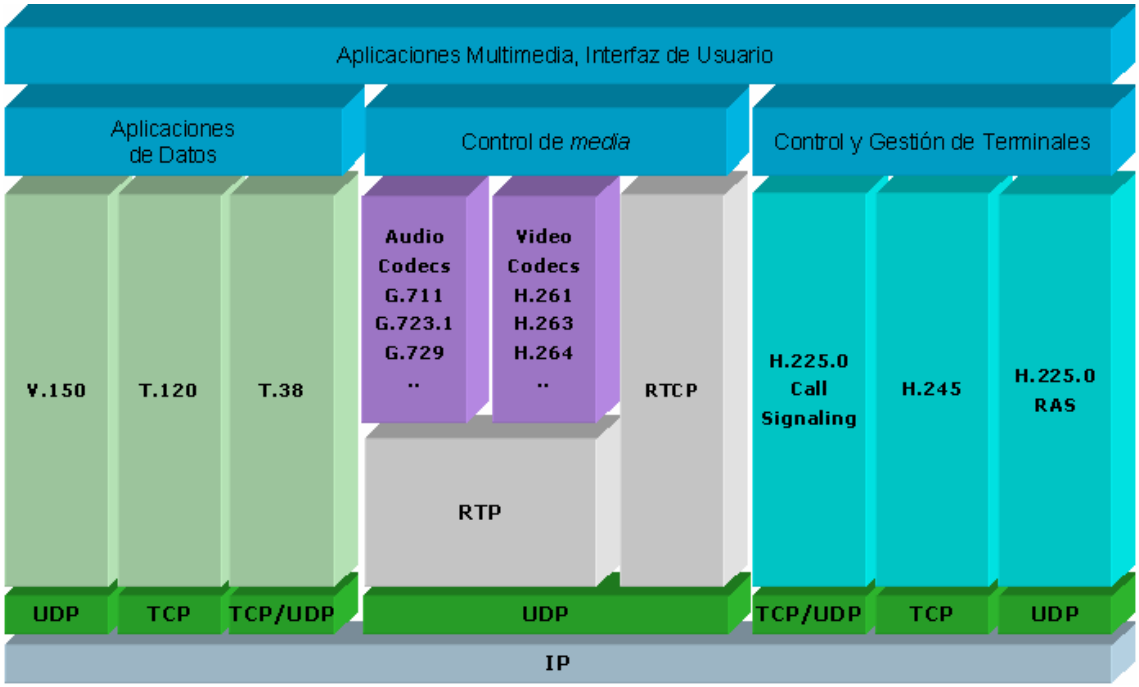


Figura 7: Pila de protocolos H.323.

Los documentos base para la descripción del protocolo H.323, conjuntamente con el estándar H.323 propiamente dicho, son los estándares H.225.0 y H.245:

- **H.225.0** describe el uso de tres protocolos de señalización: RAS (Registro, Admisión, eStado), señalización de llamada Q.931, y el protocolo conocido como Anexo G (o como Anexo G/H.225.0).
- El estándar **H.245** describe un protocolo de control multimedia; es común a los estándares "paraguas" H.310, H.323 y H.324.

Las especificaciones "base" para definir el protocolo de comunicaciones H.323 son, por lo tanto, la especificación H.323 propiamente dicha, la H.225.0 y la H.245.

Por otro lado, se utiliza ASN.1 (*Abstract Syntax Notation* 1) para definir una sintaxis abstracta de representación de los datos de señalización y control, así como las PER[34] que transforman estos datos en un flujo binario. ASN.1 se encuentra disponible en las especificaciones X.680-683, y las PER, en la X.691, de la ITU-T.

Para manejar los flujos de audio y vídeo se utiliza el protocolo de transporte en de datos en tiempo real RTP *Real-Time Transport Protocol*, (así como su apartado de control, RTCP[35]), desarrollado por la IETF.

En cuanto al transporte, H.323 usa comunicaciones fiables para algunas comunicaciones de control (típicamente TCP) y no fiables para el resto de las comunicaciones (especialmente para los flujos de audio y vídeo, RTP/RTCP, y que típicamente se llevarán a cabo con UDP). Igualmente, aunque estas comunicaciones se efectúan típicamente sobre IP, el estándar no refiere ningún protocolo de red específico.

Por último, para la transmisión de audio y de vídeo se utilizan algoritmos de compresión y códecs, siendo obligatorios el soporte de los algoritmos G.711 para audio y H.261 para vídeo (ambos de la ITU-T). Para conferencias de datos se utiliza el estándar T.120, el V.150 para comunicaciones de módem y el T.38 para fax (todos de la ITU), entre otros.

Como documentación adicional, H.323 incluye también los estándares:

- H.235, estándar que describe mecanismos de seguridad en redes basadas en sistemas de control H.245.
- H.248, MEGACO, en donde se describe la comunicación interna de los elementos de las pasarelas entre H.323 y otras redes.
- H.450.x, en donde se describen algunos servicios suplementarios.
- H.460.x, con algunas extensiones de H.323.
- H.501, para gestión de la movilidad y comunicaciones inter/intra dominio.
- H.510, documento en el que se describen el usuario, el terminal y el servicio de movilidad.
- H.530, donde se describen mecanismos de seguridad para H.510.

Además, las *H.323-Series Implementers Guides*, es decir las guías de implementación H.323, se refieren a temas cubiertos inadecuadamente por las recomendaciones, así como correcciones de las mismas. Estas guías se actualizan cada nueve meses aproximadamente y deben ser leídas conjuntamente con las especificaciones.

Y, por último, los anexos y los apéndices. Los anexos son normativos (es decir, que forman parte de la recomendación), mientras que los apéndices sólo son de carácter informativo.
En la figura 8 se enuncian todos los anexos y apéndices de cada una de las especificaciones base de H.323, de cuyos nombres pueden extraerse los apartados cubiertos por cada uno, y

[34] PER: *Packet Encoding Rules*, reglas de codificación de paquetes.
[35] RTCP: *Real-Time Transport Control Protocol*, protocolo de control para el transporte de datos en tiempo real, anejo a RTP y dedicado al control de características de retardo y de *jitter* en las comunicaciones RTP.

que pueden resultar muy útiles cuando se necesite consultar alguna cuestión relacionada con ellos:

Los anexos de la especificación H.323 son:
- Annex A – Mandatory H.245 messages
- Annex B – Procedures for layered video codecs
- Annex C – H.323 on ATM
- Annex D – Fax
- Annex E – UDP for Call Signaling
- Annex F – Simple Endpoint Type (SET)
- Annex G – Text telephony
- Annex I – Error prone channels *(work in progress)*
- Annex J – Secure SET
- Annex K – HTTP-based service control
- Annex L – Stimulus control protocol
- Annex M.x – Tunneling of various protocols within H.323
- Annex N – QoS *(work in progress)*
- Annex O – Use of DNS *(work in progress)*
- Annex P – Modem over IP
- Annex Q – Far-end camera control
- Annex R – Robustness

Los apéndices son:
- Appendix I – Sample MC/terminal communications
- Appendix II – Usage of RSVP
- Appendix III – Gatekeeper based user location
- Appendix IV - Signaling prioritized alternative logical channels in H.245
- Appendix V - Use of E.164 and ISO/IEC 11571 numbering plans

Mientras, para la especificación H.225.0 se especifican los siguientes anexos:
- Annex A – RTP/RTCP (RFC 1889)
- Annex B – RTP profile (RFC 1890)
- Annex C – RTP payload for H.261
- Annex D – RTP payload for H.261A
- Annex E – Video packetization
- Annex F – Audio and multiplexed packetization
- Annex G – Communication between and within Administrative Domains
- Annex H – ASN.1 Syntax
- Annex I – H.263+ packetization
- Y los apéndices:
- Appendix I – RTP/RTCP algorithms (reference to RFC 1889)
- Appendix II – RTP profile (reference to RFC 1890)
- Appendix III – H.261 packetization (reference to RFC 2032)
- Appendix IV – TCP/IP/UDP usage
- Appendix V – ASN.1 usage

Por último, para la especificación H.245, los anexos:
- Annex A – ASN.1 syntax
- Annex B – Semantic definition of messages
- Annex C – Procedures
- Annex D – Object identifier assignments
- Annex E to M – Various “generic capability” definitions, including some codecs

Y los apéndices:
- Appendix I – Overview of ASN.1
- Appendix II – Example of H.245 procedures
- Appendix III – Timers and counters
- Appendix IV – H.245 extension procedure
- Appendix V – Using “replacementFor”
- Appendix VI – Example H.263 capabilities
- Appendix VII – Procedures and template for generic capabilities
- Appendix VIII – List of generic capabilities for H.245 defined in other Recommendations

```
• Appendix IX – Usage of ASN.1 in H.245
```

Figura 8: Lista completa de los Anexos y apéndices de H.323.

Sólo los textos que suponen el núcleo de H.323 suponen más de mil ochocientas páginas. A pesar de que su implementación es directa (gracias a las definiciones ASN.1 y a la estandarización de las máquinas de estado para cada servicio H.323), la revisión de todos y cada uno de los aspectos relacionados con H.323, a la hora de elaborar un producto compatible, resulta muy costosa.

2.2 Grupos de estudio en la ITU-T

El estudio y desarrollo de servicios y sistemas multimedia, por parte de la ITU-T, sigue tomándose lugar en el *Study Group* 16, organizado en cuatro WPs (*Working Parties*). En el contexto de H.323, los más importantes son los WP2 y WP4. La figura 9 muestra una visión general de las Cuestiones más importantes que, en dichos grupos de estudio, se refieren a H.323.

La Cuestión B/16 en el WP4 define un marco de trabajo en el que se establecen las arquitecturas básicas comunes a diferentes sistemas multimedia (H.323, H.320, H.324), intentando identificar las sinergias que puedan existir entre ellos. La Cuestión C/16 identifica y describe servicios y aplicaciones multimedia que funcionen sobre sistemas multimedia. El estándar H.323 y sus protocolos núcleo se estudian en la Cuestión 2/16. Detalles de interoperabilidad se estudian en las cuestiones D/16 y 3/16, incluyéndose la interoperabilidad con la PSTN y entre los diferentes servicios suplementarios.

Muchas otras Cuestiones en el WP2 estudian cómo resolver temas más generales, como QoS, movilidad o seguridad, en los sistemas multimedia. Esto comprende la integración y el uso de los protocolos y métodos ya descritos así como la definición de otros nuevos.

Cuestión	Título	Tareas	Estándares (ejemplos)
Working Party 2: Plataformas Multimedia e Interoperabilidad			
D/16	Interoperabilidad entre Sistemas y Servicios Multimedia	Interoperabilidad de servicios (como los servicios suplementarios), y de sistemas multimedia entre sí y con GSTN; medidas para aumentar la interoperabilidad de las distintas implementaciones.	H.246
F/16	Calidad de Servicio y Rendimiento extremo a extremo en Sistemas Multimedia	Necesidades de QoS en sistemas multimedia; métodos de señalización de QoS; aplicaciones comunes para distintos métodos de señalización; aspectos de rendimiento extremo a extremo según la percepción del usuario.	Contribuciones a estándares de otras Cuestiones
G/16	Seguridad en Sistemas y Servicios Multimedia	Análisis de amenazas de sistemas y servicios multimedia; definición de un marco de trabajo para seguridad; contribuciones a las arquitecturas multimedia para incorporar seguridad.	H.235
1/16	Sistemas Multimedia, Terminales y Conferencias de Datos	Mejoras de las comunicaciones audiovisuales sobre redes fijas y móviles, y RDSI; intercambio de datos; mejoras en el uso de las codificaciones de audio y vídeo.	H.310, H.320, H.321, H.324, T.120

2/16	Multimedia sobre Redes de Paquetes usando sistemas H.323	Protocolos núcleo de H.323, y servicios suplementarios.	H.323, H.225, H.245, H.332
3/16	Infraestructura e Interoperabilidad para Multimedia sobre Sistemas basados en Redes de Paquetes	Pasarelas H.323 e interoperabilidad con la PSTN y con SS7; descomposición de pasarelas; MCUs; gestión de sistemas H.323; H.323 MIB; actualizaciones de la señalización de control.	H.245, H.246, H.248, H.341
4/16	Conferencias de Vídeo y Datos usando servicios de Internet	Arquitectura de protocolos para integración de funciones de conferencia de vídeo y datos, e integración con servicios de Internet; mecanismos de sincronización entre presentaciones audiovisuales y otros servicios; multiconferencias.	Ninguno, por el momento
5/16	Movilidad para Sistemas y Servicios Multimedia	Desarrollo avanzado de movilidad para H.323 y H.324; consideraciones de protocolo; consideraciones sobre terminales y servicios.	H.501, H.510, y contribuciones a estándares de otras Cuestiones
Working Party 4: Marco de trabajo Multimedia			
B/16	Arquitecturas Multimedia	Marco de trabajo común para arquitecturas de proyectos multimedia; consistencia entre sistemas multimedia; elementos de soporte común a protocolos y arquitecturas (como H.245).	Marco de trabajo para arquitecturas multimedia
C/16	Aplicaciones y Servicios Multimedia	Identificación de servicios y aplicaciones multimedia; descripciones de servicios (servicios de distribución, servicios de mensajería, de emergencia, de pago, de comercio electrónico, aplicaciones de telemedicina, etc).	Series F

Figura 9: Algunas de las actividades más importantes relacionadas con H.323 en el ITU-T SG16

2.3 Características fundamentales de H.323

Las características que ofrece este estándar, en cuanto a comunicaciones multimedia, son:

- **Interoperabilidad entre distintos fabricantes**. En realidad, éste es el ánimo de todos los estándares de comunicaciones; sin embargo, precisamente debido a su complejidad, H.323 intenta acotar todas las posibilidades de la comunicación, de las capacidades y de la funcionalidad de cada elemento de la red, incluso las posibles ampliaciones de sí mismo, de forma que en la comunicación exista al menos un conjunto fundamental común a cualquier elemento de la comunicación.
- **Independencia de la red**. La definición de H.323 hace referencia a redes de paquetes que no provean calidad de servicio, pero no especifica ningún protocolo de red en concreto.
- **Independencia de la plataforma y de la aplicación**. Siempre que se cumplan los requisitos y procedimientos descritos en las especificaciones, podrá hacer uso de H.323 cualquier plataforma, hardware o sistema operativo deseado.
- **Soporte para multiconferencias**. Aunque H.323 permite mantener multiconferencias sin el uso de unidades especializadas, las MCUs (*Multipoint Control Units*)

proporcionan una arquitectura más robusta y flexible para el mantenimiento de multiconferencias.

- **Gestión del ancho de banda**. El tráfico de audio y de vídeo resulta costoso en cuanto a recursos de ancho de banda, y podría colapsar la red. H.323 permite la gestión del ancho de banda, pudiendo limitar el número de conexiones H.323 simultáneas, así como especificarles el ancho de banda disponible a aplicaciones y terminales H.323.
- **Soporte para transmisión en multicast**. Multicast es un método de transporte que permite enviar un solo paquete hacia un conjunto de destinos sin replicación (frente a unicast, que utilizaría múltiples transmisiones punto a punto, y a broadcast, que enviaría el paquete a todas los destinos), haciendo un uso mucho más eficiente del ancho de banda.
- **Soporte para el establecimiento de conferencias entre distintas redes multimedia**. H.323 establece mecanismos para unir sistemas basados en comunicaciones LAN con sistemas RDSI[36], así como con las redes PSTN, tanto en audio como en videoconferencias. Esto se consigue gracias a la especificación de un terminal de red encargado de estas interconexiones: las pasarelas o *gateways*.
- **Seguridad**. Mediante H.235, se establecen procedimientos de autenticación, integridad de los paquetes, privacidad (mediante mecanismos de encriptación) y no repudio (es decir, medios de protección contra la afirmación de no haber participado en una conferencia).
- **Establecimiento de llamada rápido (*Fast Call*)**. H.323 también establece mecanismos para que la llamada quede establecida con un mínimo de dos paquetes.
- **Intercambio de requerimiento de calidad de servicio**. Un destino puede especificar una calidad de servicio deseada para sus flujos de audio y vídeo, incluyéndose parámetros RSVP[37] (RFC 2205 [53]).
- **Capacidades para la redundancia de la red**. Mediante servidores de direccionamiento alternativos ("*alternate* Gatekeepers") la red podrá soportar la caída de estos equipos críticos, sin pérdida de comunicación.
- **Descripción genérica de capacidades**. Mediante esta especificación ASN.1, pueden describirse códecs y formatos de audio o vídeo genéricos, sin perturbar las capacidades de comunicación dentro de los estándares más habituales.
- **Gestión del direccionamiento entre dominios administrativos**. Se establecen flexibles mecanismos de escalado para el establecimiento de llamadas entre grandes redes internacionales, mediante la definición, entre los Gatekeepers encargados del direccionamiento de la red, de los llamados elementos de borde o *border elements*.
- **Terminales simples, SET (*Simple Endpoint Type*)**. Como la especificación H.323 puede resultar demasiado extensa para terminales sencillos, la especificación H.341 recoge los mecanismos mínimos para asegurar la comunicación en redes H.323 de terminales con una funcionalidad básica.
- **Servicios suplementarios**. Dentro de los servicios asociados a conferencias, H.323 añade numerosas posibilidades, entre las cuales se destacan:
    - **Transferencia de llamada**: permite que una conferencia establecida entre A y B pase a establecerse entre B y C.

[36] RDSI: Red Digital de Servicios Integrados.
[37] RSVP: *Resource reSerVation Protocol*, protocolo de reserva de resursos.

  - **Desvío de llamada**: ante cierto estado del receptor, la llamada se desvía a otro número antes de establecerse.
  - **Llamada *On Hold***: una llamada puede dejarse inactiva durante un tiempo, para recuperarse la comunicación más tarde, sin necesidad de colgarla ni de establecerla de nuevo.
  - **Conferencia sin consulta**: es el caso, por ejemplo, de una llamada que pasa por una secretaria, y que luego ésta conecta con el destino verdaderamente deseado.
  - **Llamada en espera**: mientras se tiene una llamada activa, un terminal puede recibir una nueva llamada, que se queda como llamada entrante hasta que este terminal decide descolgarla (colgando la anterior llamada, o dejándola *on hold*, por ejemplo).
  - **Identificación del número llamante**.
  - **Establecimiento de prioridades**: posibilidad de establecer prioridades entre las distintas llamadas.
  - **Control de los planes de marcado**: establecimiento, de manera centralizada, de qué números se permiten como destinos rutables, y de cuáles deben ser rechazados de inmediato con sólo ser marcados.

- **Mecanismos de control basados en HTTP**. Mediante el Anexo K/H.323, se permite a los proveedores de servicio mostrar páginas web con contenidos obtenidos desde la red H.323, mediante comunicaciones de control sobre HTTP.
- **Capacidades de gestión de llamadas a crédito**. A partir de la versión 4 se establecen mecanismos para la comunicación de información relativa a llamadas a crédito en el mismo protocolo RAS (como, por ejemplo, mediante tarjetas prepago).
- **Uso de DNS**[38] **para la resolución de direcciones**. En la versión 5 se describen mecanismos para la solución de direcciones mediante servidores DNS a partir de alias de destinos del tipo URL[39].
- **Descripción genérica de servicios suplementarios**. Mediante el *Stimulus Control Protocol* (protocolo de control por estímulos) descrito en el Anexo L/H.323, pueden definirse servicios suplementarios para puntos finales, sin cargo añadido en su software H.323. Para ello, hace uso de un servidor de capacidades o *Feature Server*, que hace de proxy entre este terminal y sus comunicaciones H.323.
- **Robustez**. El Anexo R/H.323 describe mecanismos para asegurar la robustez de las comunicaciones ante errores sencillos en la comunicación.
- **Monitorización de la calidad de servicio**. Con la especificación H.460.9, perteneciente a la versión 5, los Gatekeepers pueden informar de las características de calidad de servicio en tiempo real.
- **Mecanismos para gestión de la movilidad**. Mediante las especificaciones H.501, H.510 y H.530.

Muchas de estas características son opcionales; además, algunos equipos sólo se adaptan a versiones tempranas de la especificación H.323; y otros sencillamente no permiten la configuración de algunos de los servicios H.323 ofrecidos.

[38] DNS: *Domain Name System*, sistema de nombres de dominios.
[39] URL: *Universal Resource Locator*, cadena de caracteres que refiere la dirección de un recurso de Internet.

2.4 Arquitectura de H.323

H.323 define cuatro elementos fundamentales en la arquitectura de red (figura 10):

- Terminales.
- Pasarelas o *gateways*.
- Gatekeepers y *border elements*.
- Y MCUs.

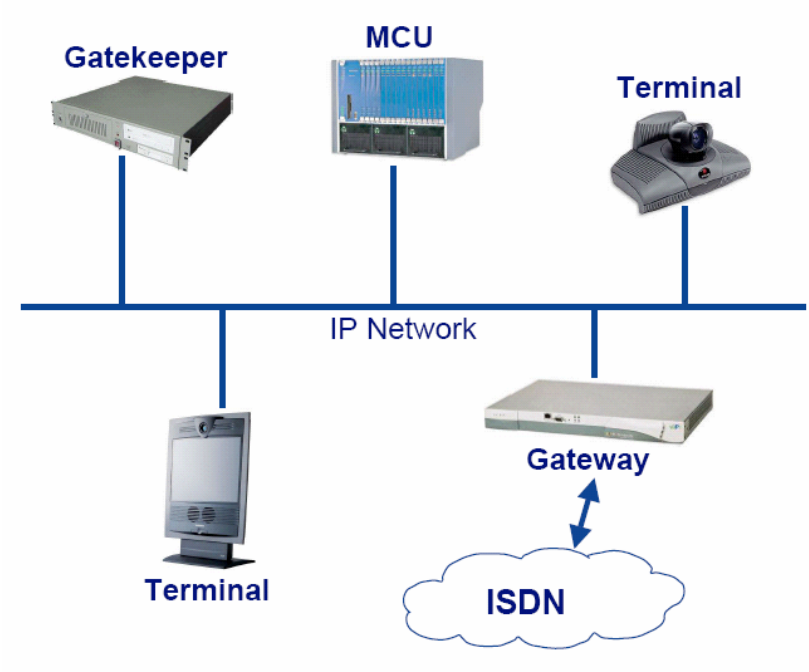


Figura 10: Elementos de una red H.323.

2.4.1 Terminales

Los terminales son puntos finales de la red que permiten comunicaciones bidireccionales en tiempo real. Todo terminal debe permitir comunicaciones de voz, mientras que los vídeos o los datos son opcionales. También debe soportar H.245, que es el protocolo usado para negociar el uso de los canales y las características de los datos. También serán obligatorios otros tres componentes: Q.931 para señalización de llamada, RAS para comunicaciones con un Gatekeeper, y soporte para RTP/RTCP para la secuenciación de paquetes de audio y de vídeo.

Los terminales más habituales que pueden encontrarse son teléfonos, videoteléfonos, dispositivos IVR (*Interactive Voice Response*), sistemas de buzón de voz o teléfonos software.

2.4.2 Pasarelas

Las pasarelas son los elementos de la red H.323 preparados para la interoperabilidad con otras redes. Se distinguen dos elementos en la arquitectura interna de una pasarela:

- El **MGC** (*Media Gateway Controller*), es el encargado de la gestión y traducción de los elementos de la comunicación relativos a la señalización de llamada en ambos extremos (como H.225.0 y SS7, por ejemplo). Controla así la facción de más de alto nivel de las comunicaciones de la pasarela.
- El **MG** (*Media Gateway*), que maneja y traduce los formatos de audio, vídeo o datos sobre las distintas interfaces, controlando la facción de más bajo nivel.

La comunicación entre el MGC y los MGs se lleva a cabo mediante una especificación separada, la H.248, también conocida como MEGACO (*MEdia GAteway COntrol*), y, como resultado de la colaboración entre el IETF y la ITU-T, también disponible en la RFC 3015.

Como ejemplos de pasarelas, las pasarelas analógicas con la PSTN, las pasarelas digitales con RDSI, o incluso pasarelas con otras redes H.323 (*proxys* de red). Entre otras capacidades, las pasarelas con la PSTN deberán poder reconocer señales DTMF[40] y transmitirlas por H.323.

2.4.3 Gatekeepers

Los Gatekeepers son los elementos más importantes de una red H.323, a pesar de que su existencia es opcional. Actúan como punto central para todas las llamadas de su Zona, y proporciona servicios de control de llamadas a todos los puntos finales registrados en él. De esta forma, una Zona es el grupo de terminales, pasarelas y MCUs gestionados por un Gatekeeper.

- El servicio de control de llamadas más importante que realiza un Gatekeeper es la traducción de direcciones, de alias de red (entre los cuales se pueden encontrar números marcados, secuencias de caracteres, direcciones URL o emails), a direcciones de transporte (típicamente, direcciones IP). De esta forma, en una red sin Gatekeepers los terminales tendrían que conocer la dirección de transporte de cada destino de sus comunicaciones. El Gatekeeper también tiene la capacidad de modificar el alias a que se refirió el terminal que inició la llamada.
- Pero también se encarga del control de accesos: si existe un Gatekeeper en la Zona H.323, cada uno de los terminales que deseen comenzar o recibir una llamada deberá solicitar acceso a su Gatekeeper.
- La tercera de sus tareas base es el control del ancho de banda de la red H.323, permitiendo o denegando llamadas en los casos en los que el tráfico supere ciertos límites, previamente configurados. El Gatekeeper dispone de mecanismos para conocer numerosos detalles acerca de cada llamada activa en su Zona. Incluso, si fuera necesario, podría cortar una llamada durante el transcurso de una comunicación.

[40] DTMF: *Dual-Tone Multi-Frecuency*, transmisión de tonos dual, es decir que cada dígito se configura con dos tonos simultáneos.

Por último, el Gatekeeper desempeñará funciones de gestión de Zona, encargándose de:

- Comunicar e intercambiar las tablas de rutas relativas a su Zona con otros Gatekeepers.
- Comunicar estadísticas relativas a la calidad de servicio de los terminales en su Zona en tiempo real
- Distribuir planes de marcado entre estos terminales.

Al resultar un elemento tan imprescindible en las comunicaciones de una red H.323, el estándar dispone potentes capacidades de redundancia para estos elementos: se trata de los *alternate Gatekeepers*, una lista de Gatekeepers alternativos de que dispone cada terminal en caso de caída de su Gatekeeper, para que en ningún momento se carezca de las informaciones de direccionamiento.

Además, los Gatekeepers pueden mantener entre sí varios niveles jerárquicos, mediante los llamados elementos de borde, que permiten la comunicación de informaciones de direccionamiento entre ellos de forma efectiva:

2.4.3.1 Border Elements

Los elementos de borde suponen un nivel más en la jerarquía de direccionamiento H.323, dotando de mayor flexibilidad y potencia a la gestión de rutas. En realidad su funcionamiento es como el de cualquier Gatekeeper, sólo que, además, guardan en su interior la información de tablas de rutas de todos los Gatekeepers dentro de su Dominio Administrativo, participando además de la autorización de llamada entre estos dominios. Un Dominio Administrativo no es, en definitiva, sino un conjunto de Zonas bajo el control de un único elemento de borde.

Por lo demás, el elemento de borde comparte el resto de funciones del Gatekeeper, existiendo, por ejemplo, la posibilidad de definir *alternate Border Elements* en cada Gatekeeper.

2.4.4 MCUs

Las **MCU**s (*Multipoint Control Units*, unidades de control multipunto) soportan la gestión de las multiconferencias. Son elementos opcionales, pero su uso resulta una potente capacidad para administrar y gestionar multiconferencias de forma robusta.

Una MCU se descompone en un **MC** (*Multipoint Controller*, controlador multipunto), y en cero o varios **MP**s (*Multipoint Processors*). El MC gestiona la señalización de las llamadas entre todos los terminales, estableciendo las capacidades para procesado de audio y vídeo entre todos, y determinando qué flujos se establecerán en multicast. Mientras, los MPs mezclarán, conmutarán y procesarán los flujos de datos en tiempo real.

Las multiconferencias pueden establecerse en varias formas, según las necesidades de la red H.323 y de las capacidades de los terminales participantes:

- **Centralizada**: Requieren la existencia de una MCU. Todos los terminales enviarán audio, vídeo, datos y flujos de control a la MCU en formato punto a punto. El MC centralizará la gestión de la multiconferencia, y el MP se encargará del mezclado de audio, la distribución de los datos y la conmutación y mezclado del vídeo, enviando los flujos resultantes a cada uno de los participantes de la multiconferencia, punto a punto o multipunto (sólo para el flujo de vídeo). El MP también permitirá conversiones de formatos (códecs). Se muestra un diagrama de este tipo de multiconferencia, aplicado a comunicaciones de vídeo, en la figura 11.

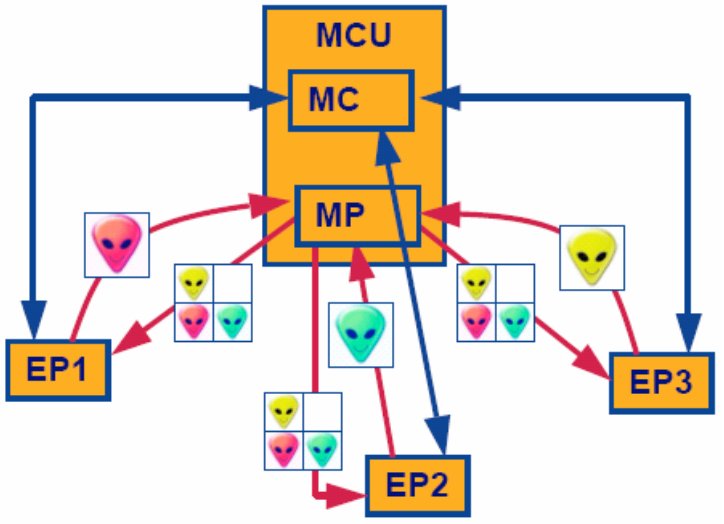


Figura 11: Multiconferencia centralizada. Transmisiones de datos unicast.

- **Descentralizada**: En este caso se podrá hacer uso de la tecnología multicast, mediante la que cada terminal envía los datos al resto de los participantes. Ahora, son cada uno de los terminales los encargados de procesar los múltiples flujos entrantes de audio y de vídeo, mediante funciones internas de MP. Mientras, el MC se encarga aún de la gestión y control de la multiconferencia, comunicándose punto a punto con todos los canales de control de cada participante y llevando a cabo funciones tan interesantes como el control de silla (*chair control*) y la selección de vídeo. La figura 12 muestra un esquema para este tipo de multiconferencias:

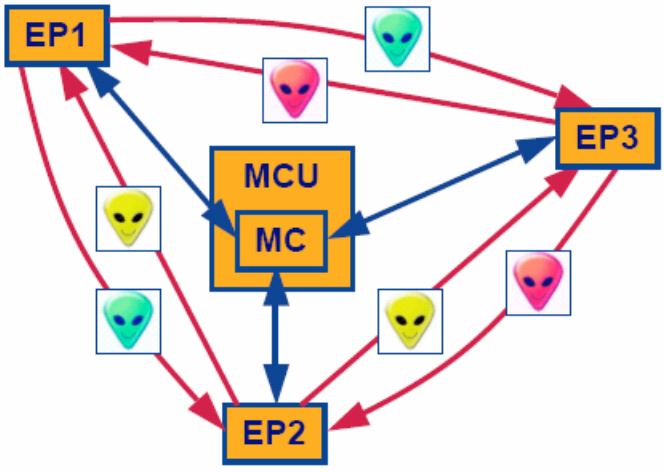


Figura 12: Multiconferencia descentralizada. Transferencia de los datos multicast.

- **Híbrida**: Una multiconferencia híbrida usará una determinada combinación de las capacidades de gestión centralizada y descentralizada. La MCU podría mezclar sólo el audio, dejando el vídeo en formato descentralizado. Por otro lado, en una multiconferencia híbrida también podría haber participantes que mantuvieran una multiconferencia centralizada a la par que otros participantes de la misma multiconferencia sólo utilizaran multicast; el nexo de unión sería la MCU. Así, cada terminal sólo debe preocuparse de la forma de conferencia en que envía y recibe, nunca de la naturaleza mixta de la multiconferencia.

2.5 Protocolos de comunicación H.323

2.5.1 Introducción

Las comunicaciones en H.323 son una combinación de señales de audio, vídeo, datos, y de señalización y control. Las capacidades de audio, señalización de llamada Q.931, control RAS y señalización H.245 son obligatorias en todos los terminales.

Las funciones de control de llamada son el núcleo de un terminal H.323. Estas funciones incluyen señalización para establecimiento de llamada, intercambio de capacidades, señalización de comandos e indicaciones, y mensajes de apertura y descripción del contenido de los canales lógicos. Éstas son las funciones que llevan a cabo los protocolos H.225.0, RAS y H.245:

- La función de señalización **RAS** establece un canal para las comunicaciones entre los terminales y su Gatekeeper, el cual los registra y admite, y además guarda información relativa al estado de cada terminal de su Zona.
- El canal de señalización de llamada se basa en **Q.931**, y sirve para establecer la primera conexión entre dos terminales.
- El canal de control **H.245** es un canal confiable que transporta señales de control que gobiernan las operaciones de la entidad H.323, incluyendo intercambio de capacidades, apertura y cierre de canales lógicos, peticiones de preferencias y mensajes de control de flujo, entre otros comandos e indicaciones. Tras el diálogo H.245 se abren los canales lógicos que transportarán todos los datos multimedia por RTP.

En los siguientes capítulos se estudiarán cada uno de estos protocolos con más detalle.

2.5.2 Usando la notación abstracta ASN.1 para H.323

El lenguaje sintáctico abstracto 1 (*Abstract Syntax Notation* 1) se encarga de la definición de estructuras de datos que, junto con las reglas de codificación de paquetes PER que traducen estos datos a una codificación binaria apta para ser transmitida directamente por el medio de transporte, permiten que el protocolo (situado dentro de estas estructuras de datos, es decir definido mediante las mismas) sea independiente de esta codificación.

De esta forma se consigue que la definición del lenguaje H.323 no necesite de representación binaria, como por ejemplo hace RTP, sino que sólo será necesario definir las estructuras de los paquetes (computacionalmente tratables como objetos o clases), sobre los que a posteriori se aplicaría una función de “encode()” para transmitir, o de “decode()” para la recepción (funciones que se encargarían de traducir a las PER).

En ASN.1 se definen módulos para cada protocolo de H.323. Por otro lado, un módulo podrá adoptar definiciones de otros módulos: para esto, computacionalmente hablando, hará falta usar un compilador ASN.1.

Los módulos ASN.1 son un conjunto de elementos formados por partes, usados para la definición de tipos extensos que, además, permiten la exportación e importación de algunas partes entre sí. La figura 13 muestra la definición de módulo se presenta con los siguientes elementos (tomado directamente de la X.680):

```
   ModuleDefinition ::=
          ModuleIdentifier
          DEFINITIONS
          TagDefault
          ExtensionDefault
          "::="
          BEGIN
          ModuleBody
          END

-- a continuación, pasa a definirse cada una de las partes:
   ModuleIdentifier ::=
          modulereference
          DefinitiveIdentifier

   DefinitiveIdentifier ::=
          "{" DefinitiveObjIdComponentList "}"
          | empty

   DefinitiveObjIdComponentList ::=
          DefinitiveObjIdComponent
          | DefinitiveObjIdComponent DefinitiveObjIdComponentList

   DefinitiveObjIdComponent ::=
          NameForm
          | DefinitiveNumberForm
          | DefinitiveNameAndNumberForm

   DefinitiveNumberForm ::= number

   DefinitiveNameAndNumberForm ::= identifier "(" DefinitiveNumberForm ")"

   TagDefault ::=
          EXPLICIT TAGS
          | IMPLICIT TAGS
          | AUTOMATIC TAGS
          | empty

   ExtensionDefault ::=
          EXTENSIBILITY IMPLIED
          | empty

   ModuleBody ::=
          Exports Imports AssignmentList
          | empty
```

```
Exports ::=
       EXPORTS SymbolsExported ";"
       | EXPORTS ALL ";"
       | empty

SymbolsExported ::=
       SymbolList
       | empty

Imports ::=
       IMPORTS SymbolsImported ";"
       | empty

SymbolsImported ::=
       SymbolsFromModuleList
       | empty

SymbolsFromModuleList ::=
       SymbolsFromModule
       | SymbolsFromModuleList SymbolsFromModule

SymbolsFromModule ::=
SymbolList FROM GlobalModuleReference

GlobalModuleReference ::=
modulereference AssignedIdentifier

AssignedIdentifier ::=
       ObjectIdentifierValue
       | DefinedValue
       | empty

SymbolList ::=
       Symbol
       | SymbolList "," Symbol

Symbol ::=
       Reference
       | ParameterizedReference

Reference ::=
       typereference
       | valuereference
       | objectclassreference
       | objectreference
       | objectsetreference

AssignmentList ::=
       Assignment
       | AssignmentList Assignment

Assignment ::=
       TypeAssignment
       | ValueAssignment
       | XMLValueAssignment
       | ValueSetTypeAssignment
       | ObjectClassAssignment
       | ObjectAssignment
       | ObjectSetAssignment
       | ParameterizedAssignment
```

Figura 13: Definición ASN.1 de módulo H.323.

A continuación, y con el fin de que el lector pueda hacerse una idea del formato de codificación ASN.1 para H.323, se mostrará en la figura 14 una pequeña parte de la

definición del protocolo H.225.0 que se ofrece en el Anexo H/H.225.0 (la descripción completa, sólo para este protocolo, ocupa 36 páginas):

```
   H323-MESSAGES DEFINITIONS AUTOMATIC TAGS ::=
      BEGIN

      IMPORTS
              SIGNED{},
              ENCRYPTED{},
              HASHED{},
              ChallengeString,
              TimeStamp,
              RandomVal,
              Password,
              EncodedPwdCertToken,
              ClearToken,
        CryptoToken,
        AuthenticationMechanism
      FROM H235-SECURITY-MESSAGES
        DataProtocolCapability,
        T38FaxProfile
      FROM MULTIMEDIA-SYSTEM-CONTROL;

   H248PackagesDescriptor ::= OCTET STRING

   H248SignalsDescriptor  ::= OCTET STRING

   H323-UserInformation   ::= SEQUENCE
-- aquí se describe la raíz común para todos los mensajes de
-- señalización de llamada H.225.0 en ASN.1:
   {
      h323-uu-pdu       H323-UU-PDU,
      user-data         SEQUENCE
      {
         protocol-discriminator    INTEGER      (0..255),
         user-information          OCTET STRING (SIZE(1..131)),
         ...
      } OPTIONAL,
      ...
   }

   H323-UU-PDU ::= SEQUENCE
   {
      h323-message-body   CHOICE
      {
         setup                Setup-UUIE,
         callProceeding       CallProceeding-UUIE,
         connect              Connect-UUIE,
         alerting             Alerting-UUIE,
         information          Information-UUIE,
         releaseComplete      ReleaseComplete-UUIE,
         facility             Facility-UUIE,
         ...,
         progress             Progress-UUIE,
         empty                NULL,
         status               Status-UUIE,
         statusInquiry        StatusInquiry-UUIE,
         setupAcknowledge     SetupAcknowledge-UUIE,
         notify               Notify-UUIE
      },
      nonStandardData         NonStandardParameter OPTIONAL,
      ...,
      h4501SupplementaryService    SEQUENCE OF OCTET STRING OPTIONAL,

      h245Tunneling           BOOLEAN,
      h245Control             SEQUENCE OF OCTET STRING OPTIONAL,
      nonStandardControl      SEQUENCE OF NonStandardParameter OPTIONAL,
```

```
      callLinkage             CallLinkage OPTIONAL,
      tunnelledSignallingMessage   SEQUENCE
      {
         tunnelledProtocolID  TunnelledProtocol,
         messageContent       SEQUENCE OF OCTET STRING,
         tunnellingRequired   NULL OPTIONAL,
         nonStandardData      NonStandardParameter OPTIONAL,
         ...
      } OPTIONAL,
      provisionalRespToH245Tunneling    NULL OPTIONAL,
      stimulusControl                   StimulusControl OPTIONAL,
      genericData                       SEQUENCE OF GenericData OPTIONAL
   }
-- a partir de aquí, se siguen describiendo todas las PDUs de cada
-- protocolo H.323:
   ...
-- también se muestran nuevas definiciones de tipos:
   GloballyUniqueID      ::=   OCTET STRING (SIZE(16))
   ConferenceIdentifier  ::=   GloballyUniqueID
   RequestSeqNum         ::=   INTEGER (1..65535)
   GatekeeperIdentifier  ::=   BMPString (SIZE(1..128))
   BandWidth             ::=   INTEGER (0..4294967295)
   CallReferenceValue    ::=   INTEGER (0..65535)
   EndpointIdentifier    ::=   BMPString (SIZE(1..128))
   ProtocolIdentifier    ::=   OBJECT IDENTIFIER
   ...
-- se muestran, para terminar, la referencia al mensaje BRQ (Bandwidth
-- ReQuest):
   BandwidthRequest ::= SEQUENCE --(BRQ)
   {
       requestSeqNum            RequestSeqNum,
       endpointIdentifier       EndpointIdentifier,
       conferenceID             ConferenceIdentifier,
       callReferenceValue       CallReferenceValue,
       callType                 CallType OPTIONAL,
       bandWidth                BandWidth,
       nonStandardData          NonStandardParameter OPTIONAL,
       ...,
       callIdentifier           CallIdentifier,
       GatekeeperIdentifier     GatekeeperIdentifier OPTIONAL,
       tokens                   SEQUENCE OF ClearToken OPTIONAL,
       cryptoTokens             SEQUENCE OF CryptoH323Token OPTIONAL,
       integrityCheckValue      ICV OPTIONAL,
       answeredCall             BOOLEAN,
       callLinkage              CallLinkage OPTIONAL,
       capacity                 CallCapacity OPTIONAL,
       usageInformation         RasUsageInformation OPTIONAL,
       bandwidthDetails         SEQUENCE OF BandwidthDetails OPTIONAL,
       genericData              SEQUENCE OF GenericData OPTIONAL
   }
   ...

   END
```

Figura 14: Definición ASN.1 del protocolo H.225.0 (fragmento).

2.5.3 RAS Registration/Admission/Status

El protocolo RAS (*Registration Admission Status*, es decir registro, admisión y estado) se utiliza para definir las comunicaciones entre cada terminal y su Gatekeeper, en cada Zona.

Es así como el Gatekeeper controla la administración de su Zona, admitiendo o denegando llamadas mediante la resolución de direcciones de red. También hay algunos mensajes RAS destinados a compartir direcciones entre Gatekeepers.

Cada mensaje RAS tiene tres tipos: Request (petición), y sus dos posibles respuestas Reject (rechazo) y Confirm (confirmación). Se abrevian xRQ, xRJ y xCF. También existen las siguientes excepciones:

- Information: ante un mensaje InformationRequest, se responde con un InformationResponse, y éste se confirma o rechaza con mensajes InformationAck o InformationNack.
- ResourceAvailable: tiene sólo las partes Indicate y Confirm (RAI, RAC).
- ServiceControl: tiene sólo las partes Indication y Response.
- Por último, existen mensajes simples: son RequestInProgress (RIP), nonStandardMessage y unknownMessage.

De entre los puertos UDP que la IANA[41] ([54]) ha asignado al estándar H.323, RAS usa el 1719 para transmisiones unicast, y el 1720 para transmisiones multicast, (aunque deben admitirse recepciones unicast en ambos puertos). Por otro lado, los únicos mensajes multicast permitidos son el GRQ (GatekeeperRequest) y el LRQ (LocationRequest).

A continuación, se pasará a estudiar los mensajes RAS más importantes:

- **GRQ**: GatekeeperRequest. Cuando se enciende un terminal (a no ser que éste, raramente, desee establecerse en solitario sin requerir Gatekeeper), tratará de encontrar a su Gatekeeper: esto puede hacerse mediante GRQ en multicast (procedimiento llamado *Gatekeeper discovery*, es decir localización de Gatekeeper); o mediante GRQ en unicast habiéndole suministrado la dirección de transporte de dicho Gatekeeper, típicamente direcciones IP o URL mediante consultas DNS (esta última opción se describe en el Anexo O/H.225.0).

  El contenido ASN.1 del mensaje GRQ se muestra en la figura 15:

```
GatekeeperRequest ::= SEQUENCE
{
    requestSeqNum            RequestSeqNum,
    protocolIdentifier       ProtocolIdentifier,
    nonStandardData          NonStandardParameter OPTIONAL,
    rasAddress               TransportAddress,
    endpointType             EndpointType,
    GatekeeperIdentifier     GatekeeperIdentifier OPTIONAL,
    callServices             QseriesOptions  OPTIONAL,
    endpointAlias            SEQUENCE OF AliasAddress OPTIONAL,
    ...,
    alternateEndpoints       SEQUENCE OF Endpoint OPTIONAL,
    tokens                   SEQUENCE OF ClearToken OPTIONAL,
    cryptoTokens             SEQUENCE OF CryptoH323Token OPTIONAL,
    authenticationCapability SEQUENCE OF AuthenticationMechanism OPTIONAL,
    algorithmOIDs            SEQUENCE OF OBJECT IDENTIFIER OPTIONAL,
    integrity                SEQUENCE OF IntegrityMechanism OPTIONAL,
    integrityCheckValue      ICV OPTIONAL,
    supportsAltGK            NULL OPTIONAL,
    featureSet               FeatureSet OPTIONAL,
```

[41] IANA: *Internet Assigned Numbers Authority*, autoridad de números asignados para Internet.

```
    genericData             SEQUENCE OF GenericData OPTIONAL
}
```

Figura 15: Contenido ASN.1 del mensaje RAS GRQ.

Para rechazar una petición GRQ, el Gatekeeper hace uso del mensaje GRJ, el cual contiene múltiples razones para afirmar su rechazo (como se muestra en la figura 16):

```
GatekeeperReject ::= SEQUENCE
{
    requestSeqNum         RequestSeqNum,
    protocolIdentifier    ProtocolIdentifier,
    nonStandardData       NonStandardParameter OPTIONAL,
    GatekeeperIdentifier  GatekeeperIdentifier  OPTIONAL,
    rejectReason          GatekeeperRejectReason,
    ...,
    altGKInfo             AltGKInfo OPTIONAL,
    tokens                SEQUENCE OF ClearToken OPTIONAL,
    cryptoTokens          SEQUENCE OF CryptoH323Token OPTIONAL,
    integrityCheckValue   ICV OPTIONAL,
    featureSet            FeatureSet OPTIONAL,
    genericData           SEQUENCE OF GenericData OPTIONAL
}
GatekeeperRejectReason ::= CHOICE
{
    resourceUnavailable        NULL,
    terminalExcluded           NULL,
    invalidRevision            NULL,
    undefinedReason            NULL,
    ...,
    securityDenial             NULL,
    genericDataReason          NULL,
    neededFeatureNotSupported  NULL
}
```

Figura 16: Código ASN.1 con las razones de RAS GRJ.

Asimismo, para aceptarla se dispone del mensaje GCF, con una serie de elementos que posteriormente serán utilizados por el terminal durante el transcurso de la llamada (figura 17):

```
GatekeeperConfirm ::= SEQUENCE
{
    requestSeqNum         RequestSeqNum,
    protocolIdentifier    ProtocolIdentifier,
    nonStandardData       NonStandardParameter OPTIONAL,
    GatekeeperIdentifier  GatekeeperIdentifier  OPTIONAL,
    rasAddress            TransportAddress,
    ...,
    alternateGatekeeper   SEQUENCE OF AlternateGK OPTIONAL,
    authenticationMode    AuthenticationMechanism OPTIONAL,
    tokens                SEQUENCE OF ClearToken OPTIONAL,
    cryptoTokens          SEQUENCE OF CryptoH323Token OPTIONAL,
    algorithmOID          OBJECT IDENTIFIER OPTIONAL,
    integrity             SEQUENCE OF IntegrityMechanism OPTIONAL,
    integrityCheckValue   ICV OPTIONAL,
    featureSet            FeatureSet OPTIONAL,
    genericData           SEQUENCE OF GenericData OPTIONAL
}
```

Figura 17: Mensaje RAS GCF, en ASN.1.

Hasta aquí se han mostrado el contenido de estos mensajes ASN.1 con fines exclusivamente didácticos. Todos estos mensajes se encuentran especificados en este formato en el Anexo H/H.225.0.

- **RRQ**: RegistrationRequest. Tras encontrar uno o varios Gatekeepers, el terminal decide registrarse en uno de ellos mediante este mensaje. Que el Gatekeeper le enviase un mensaje de rechazo RRJ significaría que este terminal no recibirá los servicios de este Gatekeeper, (no que le deniegue el uso de la red).

  Si se admite a este terminal en el Gatekeeper, éste le asignará un identificador (*endpoint identifier*), el cual se usará en posteriores comunicaciones entre ellos. El terminal le suministrará asimismo una serie de direcciones alias (*alias addresses*), que luego les servirán a otros terminales para localizar a éste sin necesidad de usar su incómoda dirección de transporte:

  H.323 proporciona una enorme variedad de alias para la descripción del destino deseado en las llamadas:

  - dialedDigits (también llamados números E.164 por representar esta numeración internacional para la PSTN, representada por la ITU-T).
  - h323-ID (cuyo uso sólo tiene sentido en el ámbito entre el Gatekeeper y el terminal).
  - url-ID (para resolución vía DNS).
  - transportID (dirección de transporte).
  - email-ID (cuenta de correo electrónico).
  - partyNumber (refiriéndose tanto a numeración privada como a números E.164).
  - mobileUIM (un número que identifique a un terminal de telefonía móvil de segunda y tercera generación).

  Estos alias, sin embargo, no están diseñados para distinguir a un terminal: sólo para ser traducidos a una dirección de transporte. Además, esta gran variedad puede resultar causa de interoperabilidad entre fabricantes.

  Otra característica de RAS que puede dar lugar a errores es la redundancia en el registro contra el Gatekeeper de cada terminal de su Zona. No puede olvidarse que este elemento de direccionamiento es fundamental para el establecimiento de la conexión porque los terminales H.323 no están preparados para almacenar esta información de direccionamiento. El hecho de que el Gatekeeper pueda rechazar al terminal en los mensajes GRJ y en RRJ resulta crítica ante pérdidas de paquetes o caídas de segmentos de la red.

  En el mensaje de respuesta del Gatekeeper RCF, éste puede indicarle al terminal qué *alias addresses* ha aceptado, de la lista ofrecida por el terminal. También se comunican en el RRQ un tiempo de vida TTL para este registro en el Gatekeeper, y en el RCF éste podrá asignar un TTL menor. Para renovar el estado de registro en el Gatekeeper antes de la expiración de este TTL pueden usarse tramas LW RRQ (*Lightweight* RRQ), es decir tramas faro, que contienen una cantidad de información menor que la usada para los mensajes RRQ.

Por último, en estos mensajes también puede dársele al terminal el permiso necesario para llevar a cabo llamadas dentro de su área sin necesitar de elaborar una petición al Gatekeeper para ello (es decir, sin el uso de los mensajes ARQ/ACF que se comentan a continuación). En efecto, para esto ese terminal necesitará conocer previamente la dirección de transporte del destino. A este terminal se le llamará terminal *pre-granted* (pre-admitido).

- **ARQ**: AdmissionRequest. Tras su registro en el Gatekeeper, el terminal sólo podrá iniciar o aceptar una llamada tras pedirle permiso a su Gatekeeper (a no ser que se trate de un terminal pre-admitido). Es ahora cuando se realiza la traducción del alias a la dirección de transporte del destino.

  El terminal generará y asignará en este instante del proceso de generación de llamada varios identificadores de llamada:

  - Un CRV (callReferenteValue) único para esa llamada, con validez en el enlace (entre el éste y el Gatekeeper).
  - Un CallID de significado globalmente único.
  - Y un CID (conferenceID) que servirá para identificar cada conferencia de forma única, e igual para todos los participantes de esa conferencia. Todos estos identificadores serán utilizados posteriormente en las diversas fases de la llamada y por otros protocolos, como el de señalización de llamada H.225.0.

  Aquí también puede especificar el terminal el ancho de banda deseado de reserva para su comunicación, y bajar esta especificación el Gatekeeper en su respuesta.

- **LRQ**: LocationRequest. Este mensaje puede ser enviado hacia el Gatekeeper por un terminal o por otro Gatekeeper, y sirve para solucionar la dirección IP de un *alias address* desconocido.

  A continuación se presenta, en la figura 18, un diagrama de la participación del protocolo RAS en el establecimiento de una comunicación entre dos terminales situados en dos Zonas distintas (mediante el uso de mensajes LRQ/LCF entre Gatekeepers):

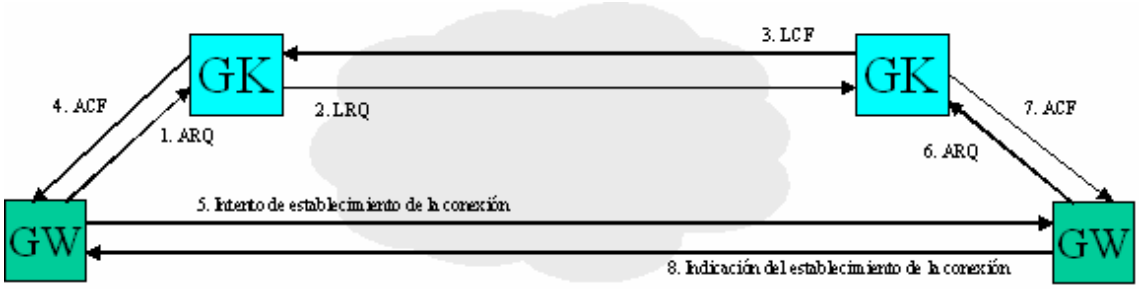


Figura 18: Mensajes RAS en el establecimiento de una llamada H.323.

- **DRQ**: DisengageRequest. Sirve para indicar, sobre el canal RAS, que la llamada se ha completado. Puede ser invocado tanto desde el terminal, como desde el Gatekeeper.

- Por último, los mensajes unknownMessage sirven para responder a mensajes no reconocibles; y los **nonStandardMessages** servirán incluso para que Gatekeepers y terminales se intercambien mensajes no estándares (como sucede, por ejemplo, entre equipos Quintum).

El resto de mensajes RAS que se especifican en el protocolo son: **BRQ** (BandwidthRequest), **IRQ** (InformationRequest), **RAI** (ResourceAvailabilityIndication), **RIP** (RequestInProgress) y **SCI** (ServiceControlIndication).

Se muestra para finalizar en la figura 19 una tabla de temporizadores y reintentos RAS por defecto (algunos equipos permiten su definición, como es el caso de las pasarelas Quintum Tenor):

Mensaje RAS	Temporizador (s)	Número de reintentos
GRQ	5	2
RRQ	3	2
URQ	3	1
ARQ	5	2
BRQ	3	2
IRQ	3	1
IRR	5	2
DRQ	3	2
LRQ	5	2
RAI	3	2
SCI	3	2

Figura 19: Tabla de temporizadores y reintentos RAS.

2.5.4 El Anexo G/H.225.0 para comunicaciones interdominio

El Anexo G de la especificación H.225.0 describe las comunicaciones entre dominios administrativos, es decir, entre los elementos de borde H.323 (o *border elements*). También se habla de esta comunicación en la especificación H.501.

Este Anexo se creó con la intención de resolver comunicaciones entre distintos espacios de direccionamiento, como comunicaciones interLANs que tengan que atravesar Internet.

La diferencia fundamental con la comunicación de mensajes RAS LRG/LCF es que éstos se limitan a solucionar direcciones. El Anexo G, además, permite la propagación de la

información de rutados, la presentación de informes de uso, e incluso la descripción de autorización de accesos.

Los elementos llamados *peer elements* (frente a los *border elements*) son Gatekeepers que utilizan mensajes Anexo G/H.225.0 para la comunicación de informaciones de direccionamiento; es decir, que no establecen comunicaciones interdominio.

La definición de la funcionalidad de cada elemento de la red H.323 que participa de la comunicación de mensajes Anexo G/H.225.0 se especifica en interfaces. La arquitectura resultante se muestra a continuación (figura 20):

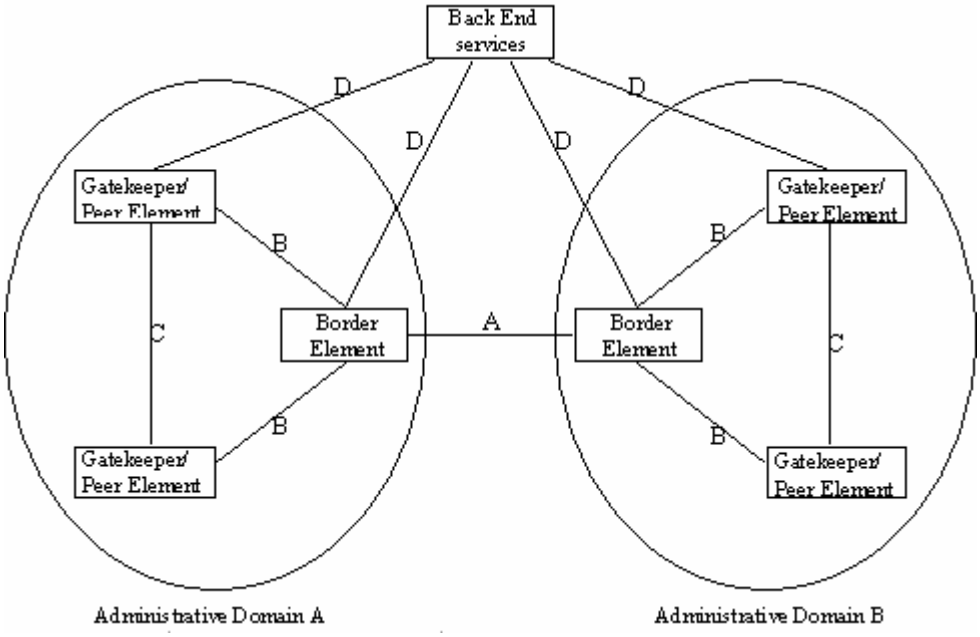


Figura 20: Esquema e Interfaces en comunicaciones Anexo G/H.225.0. La interfaz D está fuera del alcance de la especificación.

Para finalizar, y dado que de sus nombres se puede extraer aproximadamente una definición sobre su comportamiento, se mostrará la lista completa de los mensajes Anexo G/H.225:

- ServiceRequest
- ServiceConfirmation
- ServiceRejection
- ServiceRelease
- DescriptorRequest
- DescriptorConfirmation
- DescriptorRejection
- DescriptorIDRequest
- DescriptorIDConfirmation
- DescriptorIDRejection
- DescriptorUpdate

- DescriptorUpdateAck
- AccessRequest
- AccessConfirmation
- AccessRejection
- RequestInProgress
- NonStandardRequest
- NonStandardConfirmation
- NonStandardRejection
- UnknownMessageResponse
- UsageRequest
- UsageConfirmation
- UsageRejection
- UsageIndication
- UsageIndicationConfirmation
- UsageIndicationRejection
- ValidationRequest
- ValidationConfirmation
- ValidationRejection

2.5.5 Señalización de llamada H.225.0

El protocolo de señalización de llamada H.225.0 se utiliza para establecer llamadas entre dos entidades H.323. Se deriva del protocolo de control de llamada para la RDSI, Q.931, aunque se ha modificado para adaptarse a redes de paquetes. Mediante ASN.1, H.225.0 también se apropia de mensajes Q.932 (que define servicios suplementarios RDSI).

El formato de los mensajes se muestra a continuación, desde un nivel TCP (figura 21):

Figura 21: Formato de los mensajes H.225.0.

El significado de los paquetes involucrados es:

- TPKT: Los cuatro octetos necesarios para separar los mensajes TCP son 0x03, 0x00, HH y LL. HH y LL representan la longitud total del mensaje, incluyendo la misma cabecera TPTK, en *network byte order*.

- Cabecera Q.931: Todos los mensajes tendrán una cabecera Q.931, la cual incluye un octeto discriminador de protocolo (0x08), tres octetos para definir el identificador de llamada CRV (0x02, HH y LL, donde 0x02 representa la longitud del CRV, y HH y LL son los dos octetos del CRV en *network byte order*) y un último octeto con el que se indica el tipo de mensaje.
- IE: Se incluyen varios elementos de información (IEs), que dependerán de cada tipo de mensaje. Los elementos de información IEs transportan información adicional relativa a cada mensaje específico, aunque su uso no tiene por qué ser exclusivo de un tipo específico de mensaje; por ejemplo, un mensaje de Setup contendrá, entre otras cosas, los elementos de información "Calling Party Number" IE, "Called Party Number" IE, "Display" IE, etc. Aunque H.225.0 define qué IEs se corresponden con cada mensaje, la transmisión de algún otro IE no daría como resultado un fallo del protocolo.
- UUIE: *User-User Information Element*, es un elemento de información extremo a extremo. Deberá ser el último elemento del mensaje H.225.0. Se compone de los octetos 0x7E, HH, LL, PD y DATA. 0x7E es el identificador del elemento extremo-extremo entre los demás IEs. HH y LL contienen las longitudes de DATA en *network byte order*, PD es un discriminador de protocolo para ASN.1 (0x05) y DATA contiene el objeto H323-UserInformation codificado PER en ASN.1.

A continuación se muestran la lista de mensajes H.225.0 (ya familiares para los conocedores del protocolo de señalización Q.931, usado también en la RDSI):

- Setup
- Call Proceeding
- Alerting
- Information
- Release Complete
- Facility
- Progress
- Status
- Status Inquiry
- Setup Acknowledge
- Notify
- Connect

El establecimiento de llamada H.225.0 puede resultar tan sencillo como el uso de sólo dos mensajes: Setup y Connect. El resto de los mensajes servirán principalmente para prevenir errores por temporizadores, o para proporcionar anuncios y tonos en banda (o *in-band tones*), es decir, comunicación de tonos en el mismo canal que el propio canal de comunicación de la voz, tonos como el de llamada o el de ocupado; esto se realiza principalmente en el mensaje Progress, mediante el Progress Indicator IE.

Se muestra a continuación (figura 22) un diagrama de establecimiento de llamada en el protocolo de señalización de llamada H.225.0:

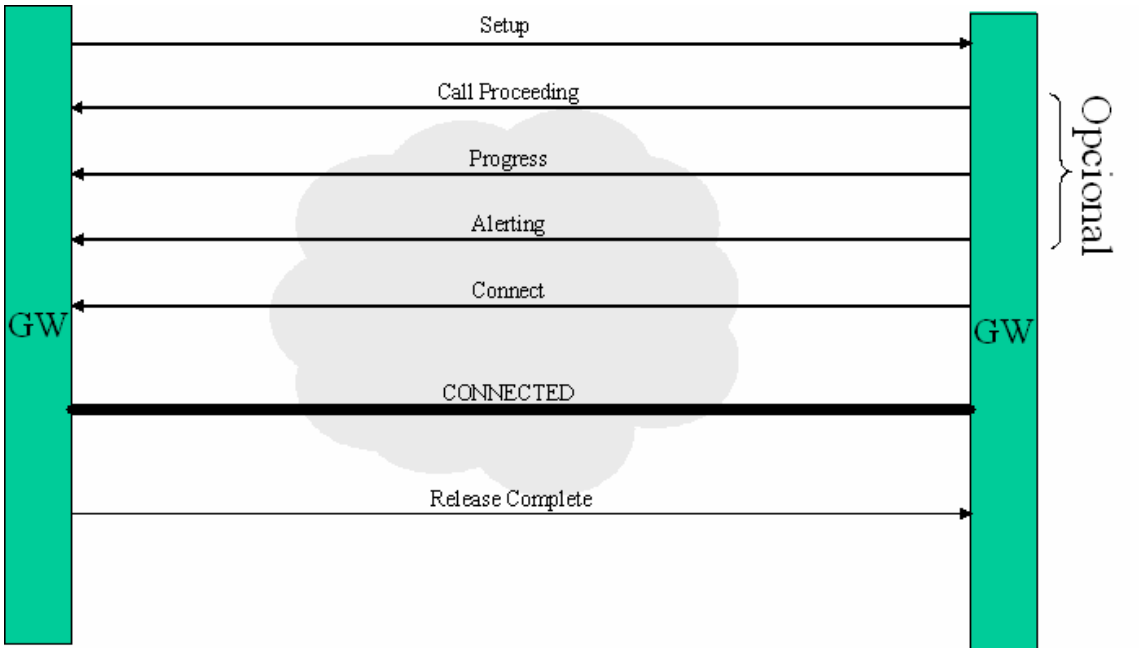


Figura 22: Diagrama de establecimiento de llamada H.225.0

Y, también, las comunicaciones completas de establecimiento de llamada H.225.0, junto con algunos mensajes RAS (figura 23):

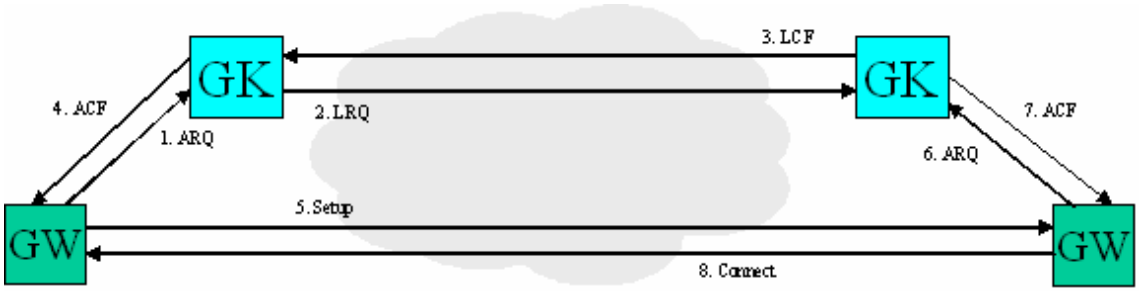


Figura 23: Diagrama de establecimiento de llamada RAS + H.225.0

Las especificaciones H.450 describen una serie de servicios suplementarios para H.323. Entre éstos se incluyen los servicios de transferencia de llamada, llamada en espera, indicación de mensaje en espera, etcétera. Todos estos servicios se transmitirán "tunelizados" en IEs que serán transmitidos en el interior de mensajes H.225.0.

El funcionamiento de H.450 se verá con más profundidad en el capítulo 2.5.8. Se muestra a continuación el funcionamiento del servicio suplementario de redirección simple: en la especificación H.450.2 se define cómo, tras recibir un mensaje de Setup, un mensaje Facility puede indicar un nuevo destino para esa llamada (siempre que se envíe antes del mensaje Connect). Puede verse en la figura 24:

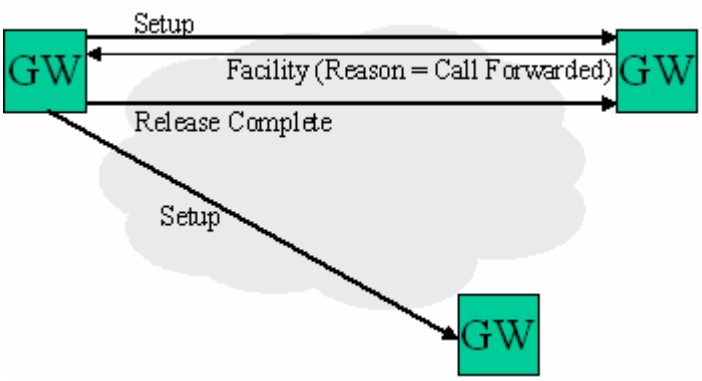


Figura 24: Mensajes involucrados en una transferencia de llamada H.450.2

Es reseñable que muchas de estas facilidades no se encuentran implementadas en todos los fabricantes, y que su uso, en tales casos, puede ocasionar problemas de interoperabilidad.

2.5.6 El canal de control H.245

El H.245 es el protocolo de control de llamada para comunicaciones multimedia que utiliza H.323. Este protocolo es compartido por un cierto número de protocolos H.32x, como el H.324M, usado en conferencias multimedia en redes 3G móviles. Pero H.323 no utiliza todas las características y facilidades que ofrece el estándar H.245; para contemplar cuáles de estos mensajes H.245 son usados por H.323 hay que referirse al Anexo A/H.323.

H.245 es una señalización que debe realizarse en paralelo con H.225.0 y, preferiblemente, antes del mensaje Connect (si no, podrían perderse algunos de los datos transmitidos). H.245 controla la sesión multimedia, encargándose de:

- El intercambio de capacidades de los terminales.
- La determinación del maestro y el esclavo de la comunicación.
- El control y composición de la señalización de canal lógico.

Por canal lógico se entiende un camino (*path*, es decir, una dirección de transporte habilitada, una conexión) para la transmisión de información entre dos terminales. En efecto, este protocolo puede asimilarse a la capa OSI de sesión.

Todos los mensajes H.245 se transportan por un canal especial, llamado el canal de control H.245. La apertura de este canal es, sin embargo, opcional, gracias a la posibilidad de usar el método *Fast Connect*: aunque a menudo este canal supone una conexión TCP separada, puede ser "tunelizado" dentro del canal de señalización de llamada H.225.0, en sus elementos de información IEs. De hecho, cuando se usa UDP para la señalización de llamada, el canal de control H.245 debe obligatoriamente ser "tunelizado". En el capítulo siguiente se estudiará este método en profundidad.

El formato de trama H.245, a nivel TCP, es el mostrado en la figura 25:

Figura 25: Formato de los mensajes H.245

Los significados de los paquetes involucrados son:

- TPKT: Los cuatro objetos necesarios para separar los mensajes TCP, son 0x03, 0x00, HH y LL. HH y LL representan la longitud total del mensaje, incluyendo la misma cabecera TPTK, en *network byte order*.
- H.245 PDU: Los mensajes H.245 son codificados mediante ASN.1 PER, y continúan a la cabecera TPTK. Existe la posibilidad de codificar PDUs H.245 adicionales a continuación de la primera, aunque muchas implementaciones podrían fallar ante esta posibilidad: es, por tanto, recomendable enviar PDUs H.245 separadas por cabeceras TPTK y, al mismo tiempo, prepararse ante la posibilidad de que éstas lleguen de forma continua.

En H.245 se distinguen cuatro tipos distintos de mensajes:

- Request (por ejemplo, masterSlaveDetermination, y terminalCapabilitySet).
- Response (como los mensajes masterSlaveDeterminationAck, y terminalCapabilitySetAck).
- Command (como el mensaje sendTerminalCapabilitySet).
- Indication (caso del mensaje userInput).

Una de las funciones más importantes del canal de control H.245 es permitir el intercambio de capacidades, es decir, la decisión sobre:

- El formato de los datos multimedia, como el tipo de codificación (G.711, G.723, H.261 o T.120).
- El número máximo de muestras de audio por paquete.
- O si se admite soporte para la supresión de silencios.
- Así, los terminales pueden escoger la codificación que mejor se adapta a las necesidades de cada comunicación.

Los primeros mensajes que se envían por el canal H.245 son uno o varios **Terminal Capability Set** (**TCS**), mensaje en el que se describen los códecs y las capacidades multimedia (*Capability Set*) que soporta cada terminal. Cada capacidad (*capability*) se relaciona con un número de las tablas de capacidades descritas en la especificación H.245; todas las posibles capacidades de todos los terminales se encuentran descritos en tablas.

H.323 contiene mecanismos para describir nuevas capacidades (como en el caso de los códecs no descritos a priori en las tablas de la especificación), en los Anexos E al M, de H.245.

En la descripción de las capacidades de cada terminal, hay también que especificar cuáles de estas capacidades pueden soportarse *a la vez*. Así, cada terminal comunicará una serie de descriptores de capacidades, cada uno de los cuales contendrá una serie de entradas de las tablas de capacidades descritas anteriormente; y cada descriptor de capacidades indicará que todos sus contenidos podrán ejecutarse simultáneamente en el terminal.

Otras de las funciones fundamentales de H.245 es la determinación de maestro y esclavo. El maestro de una conferencia punto a punto es el que puede indicar cuándo los canales entran en conflicto (es decir, cuándo el otro terminal intenta abrir un canal incompatible). El esclavo deberá ceder a las indicaciones del maestro y reconfigurar los canales adecuadamente. Otra forma de funcionar en la determinación de maestro y esclavos es, ante multiconferencias, mediante una topología *peer to peer*.

Para la señalización de canal lógico, los canales se abren intercambiando mensajes **openLogicalChannel** (**OLC**); este mensaje contendrá una de las capacidades que anteriormente le comunicó el otro terminal. Cada terminal debe transmitir un OLC; esto permite la comunicación asimétrica en códecs (es decir, que en transmisión se utilice un formato para la codificación de los datos multimedia distinto al usado en recepción). Con cada OLC se asigna un SessionID, es decir un identificador de sesión; por defecto, la sesión 1 se asigna al audio, la 2 a vídeo y la 3 a datos; y futuros SessionIDs serán asignados por el maestro de la comunicación. Para cada SessionID se abre una sesión RTP/RTCP.

El protocolo H.245 completo resulta muy complejo. Presenta en total 53 mensajes H.245 distintos (además de otros 15 que representan mensajes de respuesta). Pero, desde luego, esta parte del protocolo es la que guarda mayor grado de implicación entre los puntos finales, y por esto es necesario que se cubran todos los apartados posibles. Algunos de estos mensajes (que se enumeran para hacer ver algunas de las posibilidades del protocolo) son:

- requestMultiplexEntry.
- roundTripDelayRequest.
- encryptionCommand.
- conferenceCommand.
- flowControlIndication.
- nonStandardParameter.

H.323 especifica que para cerrar el canal de control H.245 el terminal deberá cerrar todos los canales lógicos y esperar los Acks (*acknowledgements*) respectivos. Tras esto, podrá enviar el comando endSession, y esperar asimismo su Ack.

A continuación se muestra un diagrama de llamada H.323 completo, contemplando todos los protocolos involucrados en ella (figura 26):

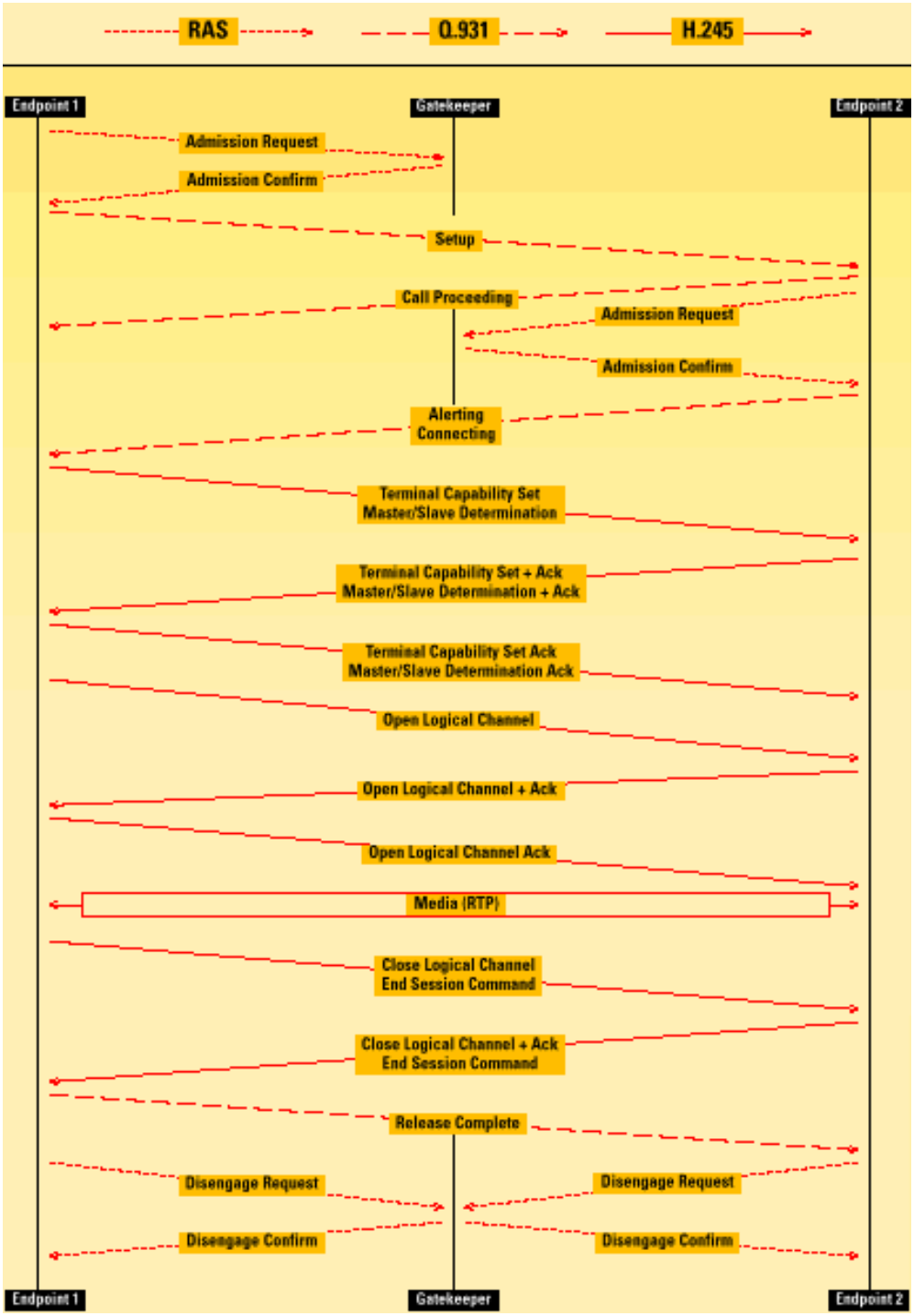


Figura 26: Diagrama completo de llamada H.323

2.5.7 El método Fast Connect

El método *Fast Connect* es un medio que propone H.323 para establecer una llamada con un mínimo de dos paquetes. Así, ni siquiera será necesario abrir un canal de control H.245, permitiéndose que todos los *media* se negocien dentro de este procedimiento rápido.

Para conseguirlo, se "tunelizarán" todos los mensajes OLC H.245 en el mensaje de Setup H.225.0, en uno o varios Fast Connect IEs, representando cada uno de ellos una proposición de canal con el mismo identificador de sesión (1, 2 ó 3, para audio, vídeo o datos respectivamente).

Para aceptar un *Fast Connect* se escoge uno de los OLCs recibidos y se devuelve otro elemento *Fast Connect* en cualquier mensaje dirigido al llamante, (para el caso más rápido, en el interior de un mensaje H.225.0 Connect). Para rechazar el *Fast Connect*, basta con iniciarse procedimientos H.245.

La llamada de dos paquetes requerirá que:

- Ambos elementos involucrados en la llamada estén pre-admitidos por sus Gatekeepers en sus respectivas Zonas.
- El terminal que inicia la llamada conozca la dirección de transporte del destino.
- Que ambos soporten *Fast Connect*.
- Y que los OLCs "tunelizados" en los mensajes Setup y Connect H.225.0 sean aceptados, respectivamente, por cada uno de los elementos.

La versión 4 de H.323 incluye ciertos mecanismos que impiden algunas condiciones de carrera existentes detectadas en versiones anteriores de este *Fast Connect*. Esto supone que en algunos casos prácticos este método no pueda utilizarse, como sucederá con las plataformas de interfonía que se desarrollarán en el siguiente capítulo.

2.5.8 Servicios Suplementarios: H.450

Aunque en el presente Proyecto no va a hacerse uso de ninguno de estos servicios suplementarios H.323, se incluirá a continuación el siguiente estudio sobre H.450 para que el lector pueda conocer la potencialidad y estructuración de la arquitectura H.323 en cuanto a estos servicios, en la medida en que son éstos los que pueden marcar la diferencia de la VoIP con respecto a las redes POTS.

El estándar H.450 posee una arquitectura descentralizada para los servicios suplementarios, y lo más separada posible de la arquitectura de los servicios básicos.

Las entidades H.323 involucradas en estos servicios se comunican directamente mediante señalización H.450, sin requerir del control centralizado de la red, excepto en los casos en los que resulte necesaria alguna capacidad centralizada. En estos casos, se hará uso de un servidor H.323/H.450 de servicios suplementarios, como sucede, por ejemplo, con el servidor de mensajería, o con el servidor distribuidor automático de llamadas.

Además de un control de servicios suplementarios completamente distribuido, H.450 describe también un modelo en el que parte de la funcionalidad H.450 puede llevarse a cabo en *proxies* H.450 entre los terminales. Un *proxy* H.450 podría ser colocado, por ejemplo, en el interior de un Gatekeeper.

Otro de los objetivos más importantes en el diseño de H.450 fue la simplificación de los requerimientos de intercomunicación con las redes conmutadas privadas (QSIG[42]) y públicas (RDSI).

H.450 ha sido diseñado con el objetivo de conseguir un protocolo enormemente flexible, definiendo diversos mecanismos para permitir la interoperabilidad entre fabricantes que presenten distintos grupos de características. Entre estos mecanismos, se encuentra el uso de una arquitectura que separa las máquinas de estado de servicios suplementarios de las máquinas de estado de la llamada básica. Un esquemático de la integración de ambas arquitecturas se muestra en la figura 27:

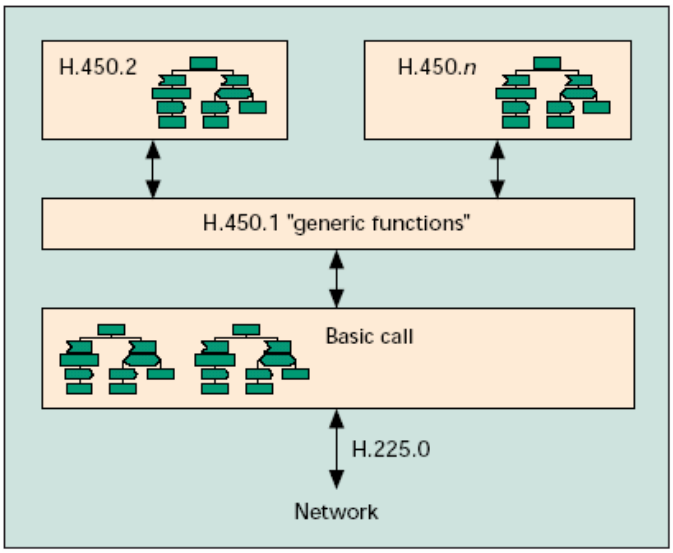


Figura 27: Arquitectura H.323/H.450 en los terminales

El estándar H.450.1 describe servicios genéricos comunes para todos los servicios suplementarios, tanto estándares como específicos de cada fabricante; a estos servicios se les conoce también como funciones genéricas. También describe los comportamientos de cada terminal ante APDUs desconocidas.

Otro estándar que facilita la interoperabilidad entre fabricantes es el H.450.12, que permite el intercambio de las capacidades soportadas por cada terminal. Esto también podría usarse como una reacción por adelantado, como por ejemplo la capacidad de una aplicación para no presentarle al usuario la posibilidad de transferir una llamada si el otro extremo de esa llamada no soportase este servicio suplementario.

Una lista con todos los servicios suplementarios soportados por cada estándar H.450.x es presentado en la figura 28.

[42] QSIG: *Q Signalling*, protocolo para comunicaciones RDSI basado en el estándar Q.931, usado para resolver la señalización entre centralitas digitales.

Estándar	Servicio suplementario	Subfunciones
H.450.1	Funciones genéricas para servicios suplementarios en H.323	
H.450.2	Transferencia de llamada para H.323	Transferencia en un solo paso Transferencia con consulta
H.450.3	Desvío de llamada para H.323	Redirección de llamada incondicional Redirección de llamada cuando ocupado Redirección de llamada cuando no hay respuesta Desvío de llamada
H.450.4	*Call Hold* para H.323	*Call Hold* local *Call Hold* remoto
H.450.5	*Call Park* y *Call Pickup* en H.323	*Park* y *Pickup* dirigidos *Park* y *Pickup* en grupos *Pickup* ante llamadas entrantes.
H.450.6	Llamada en espera para H.323	
H.450.7	Indicación de mensaje en espera para H.323	Sistema de mensajería Reproducción de mensajes en espera
H.450.8	Identificación de nombres para H.323	
H.450.9	Finalización de llamada para H.323	Finalización de llamada cuando ocupado Finalización de llamada cuando no hay respuesta
H.450.10	Ofrecimiento de llamada para H.323	
H.450.11	Intromisión de llamada para H.323	Conexión tipo conferencia Conexión tipo sostenido Monitorización de silencios Liberación de llamada forzada
H.450.12	Información común para H.323	

Figura 28: Lista de servicios suplementarios estandarizados en H.450.

La información de servicio suplementario H.450 es enviada en unidades de datos del protocolo de aplicación (APDUs) “tunelizadas” en cualquier mensaje de control de llamada H.225.0 (mediante IEs específicos, como se vio que sucedía con el método Fast Connect), sin ninguna influencia sobre el estado de la llamada H.225.0.

Entre otra información, las APDUs H.450 contienen referencias a operaciones del Servicio de Operaciones Remotas (ROS, *Remote Operations Service*), las cuales definen la semántica de los servicios suplementarios.

Como sucede con los otros componentes del protocolo H.323, las APDUs H.450 se especifican y codifican usando ASN.1: así, las APDUs H.450 pueden ser extendidas mediante el uso de información específica del fabricante (nonStandardData), en la forma de elementos de información adicionales o incluso la especificación de nuevas operaciones. Ésta es la forma de definir nuevos servicios suplementarios.

El funcionamiento de H.450 es el siguiente: la información H.450 se pasa a la entidad H.450.1. A continuación se identifican los servicios genéricos, y las operaciones del ROS son entonces pasadas a sus respectivas entidades de servicio suplementario. Es también en la entidad de funciones genéricas H.450.1 donde pueden activarse, coordinarse o bloquearse

servicios simultáneos. Cada servicio suplementario se define en una máquina de estado descrita mediante diagramas SDL[43] [55].

Finalmente, una de las ideas básicas de los servicios H.450 es una definición que permita usarlos conjuntamente con la llamada básica, en la forma de bloques constructivos. De esta forma, mediante combinaciones de los bloques básicos, pueden construirse características y servicios más avanzados. Por ejemplo, una consola de atención automática podría construirse a partir de la combinación de los bloques de Llamada básica (con una línea de entrada múltiple y un efectivo control de pulsos DTMF), más *Call Hold*, más Transferencia de llamada, más Mensajería en espera.

2.5.9 El Generic Extensibility Framework

El estándar H.323 permite ampliaciones de protocolo mediante el GEF: El GEF es el *Generic Extensibility Framework* (marco de trabajo genérico para extensibilidad), introducido en la versión 4 de H.323. Se diseñó para suplir la posibilidad de ampliar H.323 con características de interés no necesariamente horizontal (es decir, para casos particulares).

Las capacidades GEF pueden señalizarse como deseadas o como requeridas; si un terminal requiere de específicamente una capacidad GEF que su interlocutor no posee, la llamada no se establecerá.

GEF se basa en el uso de elementos de la comunicación H.323 de tipo genérico, GenericData, tipo de elemento que siempre acaba existiendo de forma opcional en cada protocolo involucrado en H.323. Explica el uso de tablas para definir las características o procedimientos que serán luego necesarios para resolver la comunicación, así como la definición y el uso de elementos genéricos sobre el propio lenguaje ASN.1.

Entre otras cosas, dentro del GEF se han descrito mecanismos para:

- La portabilidad del número en movilidad.
- El establecimiento de prioridades en las llamadas.
- Petición de rutas alternativa.
- Reportes de parámetros para la monitorización de la calidad de servicio.
- Para “tunelizado” de RAS en H.225.0.
- Para atravesar cortafuegos.

El GEF se especifica en la recomendación H.460.x.

[43] SDL: *Specification and Description Language,* Lenguaje de Descripción y Especificación, de la ITU.

2.6 Cinco versiones del estándar H.323

El estándar H.323, en constante desarrollo y adaptación a las necesidades que van surgiendo, ha sufrido hasta ahora 5 revisiones fundamentales (H.245 lleva 9 revisiones). El hecho de que algunos fabricantes hayan elaborado sus productos en base a una documentación que con el paso del tiempo ha ido quedándose obsoleta ha llevado a que numerosas aplicaciones y capacidades de este potente y complejo protocolo no resulten compatibles entre distintos fabricantes, (a pesar de que la especificación se preocupe de que así lo sean). De hecho, una de las primeras cuestiones a la hora de analizar cómo un producto H.323 se adecúa a las necesidades de un determinado proyecto debe ser qué versión del protocolo cumple.
Precisamente por esto, parece imprescindible revisar a continuación, y para finalizar el capítulo teórico, qué han aportado cada una de las versiones a las capacidades estudiadas en los capítulos anteriores.

- Versiones 1 y 2: En estas versiones se establece la base del protocolo H.323. En realidad, la versión 1 por sí sola resulta ya tan anticuada que, a pesar de que cualquier versión H.323 siempre permanece compatible con las anteriores, es preferible obviar la posibilidad de adquirir un producto que sólo se acoja a esta especificación. La versión 2 del protocolo se aprobó en enero de 1998, y contempla:
    - Los mecanismos básicos de H.225.0 (incluyéndose el uso del mensaje Progress de señalización de llamada, o del paquete RIP -*Request In Progress*- y del temporizador Time To Live en el RAS, así como terminales pre-admitidos, paquetes InformationRequest y ResourceAvailability) y H.245.
    - La definición de Gatekeepers alternativos.
    - H.235 (seguridad en cuanto a autenticación, integridad, privacidad y no repudio).
    - El mecanismo *Fast Connect*
    - El "tunelizado" de canales en H.225.0.
    - Algunos servicios suplementarios H.450 (en concreto, la transferencia de llamada especificada en H.450.2 y H.450.3).
    - El uso del identificador de llamada CRV, y de varios alias (en concreto, el H323ID, email, PartyNumber, URL y TransportID).
    - Y la introducción de varios códecs (como el GSM[44]) y de capacidades T.120 (datos) y H.263 (vídeo).

- Versión 3: Aprobada en septiembre de 1999, presenta nuevas características, a saber:
    - Conferencia *out of consultation* (es decir, cuando una llamada pasa por una secretaria antes de ser comunicada con su destino; una especie de transferencia de llamada).

[44] GSM: *Global System for Mobile Communications.*

- Definición la característica CallerID que permite al llamante definir qué información será presentada en el destino y su monitorizado en el Gatekeeper.
- Definición de capacidades genéricas GEF.
- La descripción del Anexo G/H.225.0 para comunicaciones interdominios.
- La definición de SETs Simple Enpoint Types en el Anexo F/H.323 para terminales reducidos.
- Y algunos servicios suplementarios adicionales como llamada en espera y mensajes de indicación de espera.

- Versión 4: Desde noviembre del 2000, la versión 4 de H.323 nos presenta:
  - Una nueva forma de descomponer las pasarelas (*Gateways*) en MG y MGCs, así como la comunicación entre ellos mediante H.248.
  - Mecanismos para la multiplexión de canales de vídeo y audio en un único canal RTP/RTCP.
  - Nuevos y potentes servicios suplementarios, como el Anexo K/H.323 que define mecanismos de control vía HTTP y el Anexo L/H.323 para la comunicación mediante estímulos (como pulsación de teclas o clicks de ratón).
  - Nuevas capacidades para la definición de la identidad llamante y de llamada en espera.
  - Nuevos mecanismos para la definición y uso de tonos y anuncios *in-band.*
  - Mensajes RAS UsageInformation para la generación de estadísticos.
  - Soporte para la gestión del ancho de banda en multiconferencias.
  - Uso de RSVP para gestión de la calidad de servicio.
  - Extensiones del protocolo mediante GEF.
  - Capacidades para la gestión de llamadas a crédito.
  - Una como mejor gestión de cambios de “tunelizado” a status normal para H.245.

- Versión 5: La última versión, hasta la fecha, del protocolo H.323, salió a la luz en julio de 2003. En ella se incluyen los Anexos M hasta el R, así como una extensa revisión del GEF. Entre estas nuevas características cabe destacar:
  - El uso de DNS para resolución de direcciones.
  - Nuevos mecanismos de robustez.
  - Mecanismos para monitorización.
  - Peticiones GEF para rutas alternativas.

El conjunto de todas estas definiciones para procedimientos de comunicaciones multimedia H.323 es tan extenso que, habitualmente, los fabricantes sólo permiten la configuración de algunas de ellas, repartidas entre todas las versiones.

Esto, en general, da lugar a costosas interoperabilidades, que redundan en la reducción progresiva de las capacidades de cada terminal a medida que se amplia el rango de productos de distintos fabricantes empleado para resolver nuestro proyecto de VoIP.

En realidad, esta interoperabilidad es piedra angular en el presente proyecto, como se analizará en el apartado 3.6.

3. Desarrollo

3.1 Introducción

En el presente proyecto se exponen dos plataformas de interfonía que fueron desarrolladas, instaladas y verificadas por Revenga Ingenieros S.A. durante el otoño de 2005.

- La primera de ambas plataformas se requirió para un sistema de información al usuario, instalado en el centro de Madrid (en concreto, en el llamado Barrio de las Letras), para control de accesos de vehículos mediante un sistema de videovigilancia y reconocimiento de matrículas. Acompañando a los equipos de transmisión desde cada cámara situada en los accesos a dicho barrio, se instaló un sistema de interfonía que luego, desde el edificio de control de movilidad del Ayuntamiento de Madrid, se conectaría con un operador encargado de informar al público interesado.

- En el segundo caso se le encargó a Revenga Ingenieros S.A. la instalación de una red de interfonía para información y emergencias en la reciente estación de Bailén, del metro de Valencia, con el propósito, además, de permitir futuras nuevas instalaciones de interfonía en dicho metro. Los interfonos de esta estación tendrían que conectarse con la oficina de expedición de billetes de la misma y con el centro de control del metro de Valencia.

En estas plataformas, las características de la VoIP no se desarrollan en todo su esplendor en cuanto a potencia de operación, monitorización y generación de estadísticos, control y servicios suplementarios. Más bien, son una forma de aprovechar las infraestructuras IP de que disponen ambas entidades, para desplegar, sobre estas potentes redes privadas, una red interna de telefonía (interfonía) sin coste adicional y entre terminales remotos.

En particular, la interfonía IP se consigue como resultado de transformar las comunicaciones desde interfonos analógicos, mediante pasarelas analógicas, al mundo VoIP.

Es muy importante resaltar aquí por qué no ha sido necesario realizar ninguna auditoría de red para ninguna de las dos plataformas. Esta auditoría de red analiza las características de retardo y *jitter* de una red, y resulta crucial para asegurar el buen funcionamiento de las comunicaciones en entornos como por ejemplo redes VoIP destinadas a comunicaciones de empresa, o redes VoIP sobre WAN que precisen atravesar Internet. Las causas de esta decisión son:

- En estos casos, se hará uso de unas redes privadas que no tienen que atravesar ningún cortafuegos, que no presentan de ninguna conexión a Internet ni, por consiguiente, atraviesan ningún operador.
- Las redes trabajan en 100 Mbps como mínimo porque también llevan aparejadas tramos de fibra óptica.
- Se contará con comunicaciones de información en las que sólo habrá dos operadores, es decir, dos llamadas con transporte de datos en tiempo real como máximo.
- Además, los equipos de nivel 2 (switches) involucrados no presentan posibilidades de configuración de la calidad de servicio (como DiffServ), siendo éste uno de los apartados que tratan las auditorías de red.

Puede así resolverse que el estudio y simulación pormenorizada en que consisten las auditorías de red no son necesarios para ninguno de estos proyectos, y que los retardos y el *jitter* no disminuirán la calidad de las comunicaciones.

En el Apéndice A se incluye un pequeño estudio sobre las auditorías de red, analizándose sus características y su necesariedad, y presentando algunas herramientas software para llevar a cabo estas auditorías.

3.2 Empresas y fabricantes

Revenga Ingenieros S.A. [56] es una empresa especializada en soluciones integrales de telecomunicaciones. Entre sus clientes pueden contarse Telefónica de España, Jazztel, RENFE, AENA, Iberdrola o Repsol, entre otros. Asimismo, presenta una amplia gama de productos, tales como sistemas de transmisión y supervisión de fibra óptica (contando con alianzas comerciales con empresas como ACTERNA y Huawei), tarjetas inteligentes y control de accesos (de los que son fabricantes), sistemas de televigilancia y CCTV[45] (tanto analógicos como vía radio o sobre IP), y sistemas de telefonía selectiva, megafonía e interfonía (también fabricantes).

No ha sido sino gracias a una beca de colaboración entre esta empresa y la Universidad de Sevilla que el presente proyecto ha podido llevarse a cabo. Es, por lo tanto, bajo sus necesidades y directrices, como ha sido especificado y desarrollado.

Los interfonos que se usarán en ambas plataformas serán analógicos, conectados a pasarelas IP situadas en entornos seguros (como armarios o salas de equipos). Esta decisión se debe a múltiples razones:

[45] CCTV: *Closed Circuit Television*, circuito cerrado de televisión.

- Distancia: el cable UTP de categoría 5 para comunicaciones en Fast Ethernet de 100 Mbps permite hasta 100 metros de máximo, mientras que el mismo cable UTP usado para la telefonía analógica soporta distancias de hasta 2 y 3 kilómetros.
- Alimentación: si los equipos VoIP no soportan POE[46], en el caso de trasladar estos equipos hasta el lugar de atención al público, sería necesario llevar hasta allí una línea de alimentación, de 220 V o ya transformada, con las consecuentes posibles atenuaciones.
- Robustez: estos interfonos analógicos disponen de una elevada robustez gracias a la presentación en caja de metal, resistente a actos vandálicos, con indicadores de progreso de comunicación, como los populares interfonos amarillos del Metro de Madrid que fabrica Revenga Ingenieros S.A., y ya adaptados a estos interfonos analógicos.

De hecho, hasta el momento no han sido desarrollados interfonos IP bajo el marco de estándares internacionales, los cuales permiten una interoperabilidad fundamental para posibles ampliaciones de la plataforma o para su integración con otros servicios VoIP.

Concretamente, se usarán los interfonos Viking de la serie 1600 (mostrados en las figuras 29 y 30), de **Viking Electronics Inc.** [57], empresa especializada en la fabricación de productos analógicos. El motivo de su elección fue la experiencia que durante muchos años ha mantenido Revenga Ingenieros S.A. en instalaciones de sistemas de interfonía analógicos con estos interfonos Viking. En el CD se adjunta su *datasheet* en la carpeta `Archivos Adjuntos\Viking 1600A`, archivo `Viking 1600a series.pdf`.

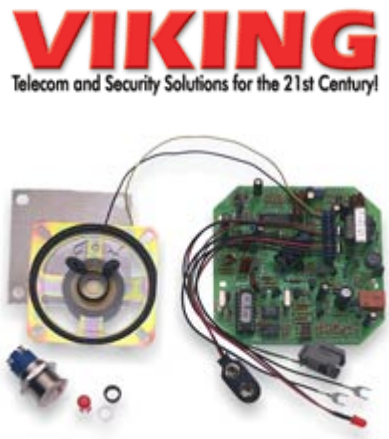


Figura 29: Interfono Viking 1600A sin carcasa.

Figura 30: Interfono montado en carcasa.

Quintum Technologies Inc. [58] es una empresa norteamericana de reciente creación, dedicada a la fabricación de equipos de red para VoIP. Su fuerza comercial se basa en ofrecer la posibilidad de integrar las redes analógicas tradicionales (centralitas PBX de pequeña y mediana empresa) con las comunicaciones VoIP, asegurando así:

- Primero, una transición paulatina de las comunicaciones de voz de empresa al mundo IP.

[46] POE: *Power Over Ethernet*, transmisión de potencia de alimentación sobre uno de los pares reservados del cable ethernet.

- Y segundo, mediante su tecnología *SelectNet*, la fiabilidad de las comunicaciones de voz incluso ante eventos de caída de la red IP, mediante la conmutación automática de todas las llamadas hacia la interfaz analógica tradicional.

De esta forma, sus productos están orientados tanto al mercado de la VoIP empresarial, como a proveedores de servicio de telefonía, prepago por ejemplo, que necesiten puentear la red telefónica tradicional por la red de datos en ciertos segmentos de la comunicación, así como a integradores de VoIP (como en el caso del presente proyecto).

Fue gracias a su familiaridad con las interfaces analógicas y a sus bajos costes en lo respectivo a productos VoIP como Quintum Technologies resultó atractiva a Revenga Ingenieros para la integración de sus sistemas de interfonía analógicos con las comunicaciones IP.

Debido al *partnership* exclusivo de Revenga Ingenieros S.A. con Quintum Technologies Inc. en España y Portugal, para la definición de este proyecto se hará uso expreso de estos equipos: los Quintum Tenor.

Las pasarelas Quintum Tenor soportan los dos estándares internacionales para VoIP líderes del mercado actual, esto es, SIP y H.323. Pero Quintum Technologies aún no ha desarrollado un equipo SIP Proxy/Registrar que soporte el direccionamiento en una red SIP, dejando Quintum Technologies que sea típicamente un proveedor de servicio en Internet el encargado de ofrecer esta capacidad. Esta opción resulta claramente inviable en plataformas de interfonía, las cuales se desarrollan habitualmente sobre una red privada sin conexión con Internet. Quintum Technologies sí ha desarrollado el Quintum Tenor Gatekeeper, equipo que ofrece la misma funcionalidad dentro del estándar H.323. De hecho, la funcionalidad SIP de las pasarelas Quintum Tenor sólo se comercializó a mediados del 2005, es decir que antes sólo contemplaban el protocolo H.323. Y es que no ha sido sino hasta hace poco que SIP ha comenzado a tomar fuerza comercial como protocolo de VoIP.

A esto hay que sumarle la perfecta integración que ofrece H.323 con la PSTN, y que resulta fundamental en la utilización de los interfonos analógicos Viking comentados anteriormente. Finalmente, se concluyó que el presente proyecto debía utilizar el protocolo H.323 para resolver las comunicaciones VoIP. Como desventaja, se asumió que los terminales H.323 resultasen bastante menos económicos que los terminales SIP, en ese momento del mercado.

Por último, también se utilizarán algunos teléfonos VoIP autónomos, concretamente los que se enumeran a continuación:

- Teléfono IP Cisco 7905G: teléfono de coste medio, norteamericano. [59]
- Teléfono SJ Phone: teléfono software. [60]

Sobre el análisis de esta opción de diseño nos remitimos al capítulo 3.6, en el que se discuten esta y otras posibles soluciones a estas redes, desde un punto de vista de costes y de mercado.

3.3 Diseño

Para el diseño de cada plataforma se considerarán los siguientes apartados:

- La elección de los terminales receptores VoIP, que deberían soportar el protocolo H.323 y ser compatibles con los equipos Quintum Tenor, presentando una funcionalidad básica con un coste bajo (menos de 300 €).
- La elección de las pasarelas Quintum Tenor adecuadas en cada caso.
- La especificación de un plan de marcado y del plan de direccionamiento IP.
- Y, específicamente para la VoIP, la determinación del códec de voz y de las funcionalidades H.323 necesarias.

La elección de los terminales involucrados en las plataformas se ha hecho desde el punto de vista de la integración con los equipos Quintum Tenor, y se desarrolló de forma conjunta para ambas plataformas. El resto de los apartados del diseño se especificará en cada una de las plataformas por separado.

3.3.1 Elección de terminales hardware

Los terminales telefónicos VoIP autónomos que se barajaron inicialmente fueron:

- Snom 100 [61]
- SwissVoice IP 10s [62]
- Siptronic ST 102 [63]
- Cisco 7940G [64]
- Telkus Totalfon IP5000 [65]
- Micronet 5100SP [66]
- Cisco 7905G [67]

Estos terminales son los terminales de gama baja de una gran variedad de fabricantes, (algunos de ellos sólo disponían de oferta en gamas bajas). Se adquirieron los tres últimos, sobre todo debido a sus precios. También se adquirió el Cisco 7905G del fabricante Cisco Systems, que resultaba un poco más caro que otros teléfonos de fabricantes poco conocidos, pero que presentaba unas claras expectativas de fiabilidad que, a posteriori, resultaron cruciales.

Figura 31: Teléfono VoIP Micronet 5100SP

Tras largas pruebas en la oficina con los mismos equipos que luego irían destinados a la instalación en campo, los resultados fueron satisfactorios para los tres teléfonos, con la salvedad de un pequeño error del terminal Micronet (figura 31) a la hora de mostrar el tono de llamada: de vez en cuando, lo cambiaba por el tono de ocupado. De cara al usuario, este comportamiento no era aceptable. Este problema se intentó solucionar por todos los medios porque el terminal era atractivo y económico, y salvo este detalle su funcionamiento e interoperabilidad eran muy buenos. Se retocó la configuración de los tonos (vía web y telnet), se trató de consultar al fabricante, se instalaron nuevos *firmware*s (incluso, algunos en los que se definía este comportamiento y se aseguraba que se arreglaba), pero no hubo manera de reducir tal comportamiento. Se incluye en el CD el manual de este teléfono, carpeta `Archivos Adjuntos\Varios\Micronet 5100SP` archivo `SP5100_manual_v3.pdf`.

En la primera instalación del sistema de interfonía, en la sala de máquinas de movilidad del Ayuntamiento de Madrid, el teléfono IP Telkus Totalfon IP5000 ni siquiera respondió correctamente a los Ping. Fue imposible resolver las causas, porque los equipos de vídeo, que precisan de muchísimo más ancho de banda, funcionaban correctamente, al igual que los equipos de conmutación de fibra óptica. Ya se había notado un comportamiento de sus interfaces bastante poco robusto, y cómo una desconexión momentánea podría hacerle perder la comunicación con el Gatekeeper y, por ende, con todo el sistema de interfonía. Al final, se sustituyó por un teléfono software, cuya elección se detalla en el apartado siguiente.

Figura 32: Teléfono VoIP Cisco 7905G

El único terminal que no falló en ningún momento, sencillo, robusto y completo, fue el Cisco 7905 G (figura 32).

Las especificaciones de este teléfono pueden consultarse en el *datasheet* que se incluye en los archivos adjuntos, con el nombre `datasheet.pdf` en la carpeta `Archivos Adjuntos\Cisco 7905G`.

3.3.2 Elección de terminales software

A priori, y para disponer de un cierto margen de diseño, se buscó la interoperabilidad de algún terminal software. Los que se barajaron fueron los siguientes:

- OpenPhone [68]
- Netmeeting [69]
- SJPhone [70]

El análisis de estos tres terminales fue mucho más sencillo que el de equipos hardware, debido a que toda la configuración de red corría a cargo del PC y a las múltiples herramientas de análisis que éste puede soportar. Se escogieron tres opciones: la aplicación nativa para VoIP Windows Netmeeting, para su uso sobre un PC con sistema operativo Windows XP; un desarrollo abierto, el OpenPhone; y el SJPhone que es un desarrollo específico, norteamericano.

- El OpenPhone, teléfono software de código abierto desarrollado por el OpenH323Project, presentó características positivas. Pero en algunos casos, en transferencias de llamada, o frente a errores de protocolo, se cayó, provocando una interrupción de memoria: era inestable.
- El NetMeeting no se registraba correctamente con el Gatekeeper, su funcionamiento fue el más deficiente de los tres. No puede olvidarse que se está utilizando un protocolo realmente complejo. También fue descartado.
- El SJPhone dio un resultado excelente. El análisis de los paquetes mostraba, por ejemplo, que los cortes de comunicación debidos a diversas causas cerraban concienzudamente todos los canales de comunicación H.323, utilizando el protocolo de una forma muy robusta, sin dar lugar a incongruencias. Registros e interoperabilidad con los Quintum correcta, y, pese al coste de su licencia (95 € / unidad), se escogió.

  Este teléfono se adjunta en su versión de prueba en la carpeta `Archivos Adjuntos\SJ Phone`, archivo `SJphone-289a.exe`, así como su datasheet, archivo `sjlabs-von05spring.pdf`, y su manual de uso, en el archivo `SJphone Guide.pdf`.

También se adjunta en la documentación el teléfono OpenPhone, en la carpeta `Archivos Adjuntos\Varios\OpenPhone`. Y algunos programas basados en el OpenH323Project, librerías de código abierto, en la carpeta `Archivos Adjuntos\Varios\Software H.323 de código abierto\OpenH323`.

3.3.3 Elección de terminales analógicos

- Alcatel Temporis 45 [71]
- Famitel Agenda

Estos teléfonos fueron escogidos por poseer una agenda (de 50 números en el caso del Temporis 45, de 200 en el caso del Famitel), y mostrar es un *display* el nombre asociado en la agenda interna con el número llamante. Estos terminales son más económicos que un terminal VoIP y, en algunos casos, su comportamiento es suficiente para resolver las necesidades del sistema (como se verá en la Plataforma de Interfonía Estación de Bailén). El Famitel es un terminal inalámbrico. El teléfono Alcatel Temporis 45 se muestra en la figura 33.

Ambos teléfonos dieron resultados positivos: esto es comprensible, primero por la longevidad de las comunicaciones analógicas, y segundo por su sencillez.

Figura 33: Alcatel Temporis 45

3.3.4 Plataforma Barrio de las Letras

3.3.4.1 Consideraciones iniciales

Esta plataforma formó parte de un proyecto de desarrollado e instalado por Revenga Ingenieros S.A. consistente en un sistema de control de accesos automatizado por lectura de matrículas para el Barrio de las Letras de Madrid. En efecto, se trataba de restringir los

accesos de vehículos a dicho barrio, quedándose únicamente habilitado el acceso a residentes, servicios públicos y vehículos oficiales. La automatización del proceso se realizó mediante la instalación de 16 cámaras, 8 de ellas por infrarrojos, en 8 puntos distintos cubriendo todos los accesos a este barrio. La plataforma de interfonía que aquí se presenta provisiona al sistema de un servicio de información y atención al usuario atendido por un operador.

Para ello, se instalarán 8 interfonos, cada uno de ellos relacionado con los armarios de equipos en los que se encontraban los equipos de digitalización y transmisión de la señal de vídeo tomada desde las 16 cámaras de control (dos para cada armario). Estos equipos de transmisión se conectarían luego a los conmutadores y a la red interna del Ayuntamiento de Madrid, que discurre por canales subterráneos.

Los interfonos, dotados de unas gruesas carcasas metálicas antivandálicas, se conectarían analógicamente a cada pasarela Quintum Tenor situada en dichos armarios, y a través de ella se transformarían a comunicaciones VoIP.

Para la conexión de los interfonos se utilizará la más pequeña pasarela de Quintum, el ASG200, con dos conexiones FXS; es decir, que en cada armario queda una conexión FXS de guarda. En la figura 34 se muestra este dispositivo.

Figura 34: Quintum Tenor ASG200

Estas pasarelas deberán utilizar un Gatekeeper (figura 35), que se situará en la sala de máquinas del centro de control, en el edificio de movilidad del Ayuntamiento de Madrid. En este edificio se encontrará el operador encargado (entre otras tareas) de atender al público que necesite de información sobre el servicio. Éste dispondrá, a tales efectos, de un teléfono VoIP receptor de todas las llamadas de interfonía (aunque también podrá lanzar llamadas contra los interfonos).

Figura 35: Quintum Tenor Gatekeeper

Las especificaciones del Gatekeeper estos equipos, así como sus manuales de configuración y otros documentos informativos, se adjuntan en la carpeta `Archivos Adjuntos\Quintum Technologies\Manuales y documentos Gatekeeper` y `Archivos Adjuntos\Quintum Technologies\Manuales y documentos Pasarelas\ASG200` del CD de documentación.

Como ya se ha comentado, para esta plataforma se quiso utilizar inicialmente un teléfono hardware; pero tras muchos e incomprensibles errores con el Telkus IP5000, y gracias al PC sobre Windows XP de que ya disponía el operador, se acabó por integrar el teléfono software SJPhone.

El diagrama completo queda, por lo tanto, en la forma siguiente (figura 36):

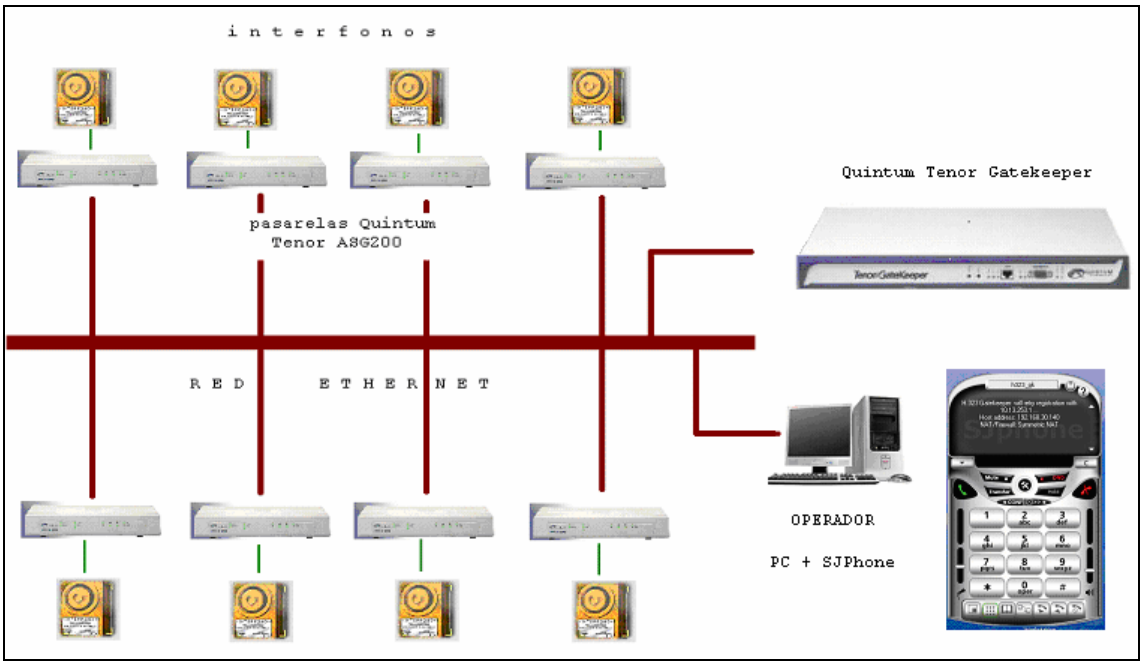


Figura 36: Esquema completo para la Plataforma de Interfonía Barrio de las Letras

En total, se han utilizado:

- 8 Quintum Tenor ASG200, pasarelas de interfonos a VoIP en H.323.
- 1 Quintum Tenor Gatekeeper, H.323.
- 1 SJPhone, teléfono software H.323.
- 8 interfonos Viking 1600A, interfonos analógicos, con soporte metálico reforzado.

3.3.4.2 Planes de marcado y de direccionamiento IP

Todos los equipos tendrán 255.255.192.0 de máscara de subred (a efectos de no colisionar con otros elementos del sistema de control de cámaras), así como el PC del operador.

- Pasarelas:

Localización	Dirección IP	Número de extensión	Número de Serie
Moratín	10.54.187.61	61	A012-103590
Lope de Vega	10.54.187.62	62	A012-10358C
San Agustín	10.54.187.63	63	A012-103594

Prado	10.54.187.64	64	A012-10358E
Santa Catalina	10.54.187.65	65	A012-103598
Santa Ana	10.54.187.66	66	A012-103596
León	10.54.187.67	67	A012-103592
Fúcar	10.54.187.68	68	A012-101F72

- Gatekeeper:

Dirección IP	Modelo	Número de Serie
10.54.187.60	GK20	A006-008767

- PC del operador y SJPhone

H323ID	Dirección IP	Extensión
operadorInterfonia	10.54.187.71	71

3.3.4.3 Códecs y funcionalidades H.323

El códec del sistema de VoIP debe ser permitido por todos los equipos VoIP del sistema. En este caso, se trata de asegurar la correcta comunicación entre las pasarelas Quintum Tenor y el teléfono IP SJPhone.

Ambos dispositivos tienen en común los códec G.711 (banda base) y G.729. Sin embargo, se han observado algunos problemas en la comunicación en el teléfono software con el uso del códec G.729 cuando el PC sobre el que trabaja se encuentra sobrecargado.

Al ser el ancho de banda de la red local lo suficientemente grande, se seleccionará el códec G.711 Mu-law, con muestras de 20 ms: no se practicará compresión de audio.

Por otro lado, también se ha notado que en las pasarelas Quintum Tenor el método *Fast Connect* H.323 puede dar lugar a errores de protocolo, sobre todo contra otros equipos VoIP. Esto es debido probablemente a la existencia de condiciones de carrera, condiciones que se revisan en la versión 4 de H.323 y que no incorporan todos los equipos VoIP utilizados. Por lo tanto, se anularán de la configuración las capacidades de *Fast Connect*, así como los “tunelizados” H.245.

3.3.5 Plataforma Estación de Bailén

3.3.5.1 Consideraciones iniciales

Para esta plataforma se requirió la instalación de 13 interfonos en distintas localizaciones de la reciente estación de Bailén en el metro de Valencia, para proveer a la misma de un servicio de emergencias y de atención al cliente. Estos interfonos deberán conectarse a un puesto de operador situado en la misma estación, y a otro operador situado en el centro de control, que recibirá las llamadas no atendidas en la estación.

La característica fundamental de esta plataforma es que debe prever muy posibles ampliaciones de la red de interfonía.

Para ello se utilizarán dos pasarelas analógicas Quintum Tenor AXG800, de ocho puertos FXS cada una (figura 37). Pueden consultarse sus especificaciones, así como algunos documentos informativos, en la carpeta `Archivos Adjuntos\Quintum Technologies\Manuales y documentos Pasarelas\AXG800` del CD de documentación.

Figura 37: Quintum Tenor AXG800

Utilizando además un Alcatel Temporis 45 para la recepción de llamadas desde el puesto de atención en la misma estación, se dejarán dos puertos FXS de los 16 totales de reserva. Se hará uso también un Gatekeeper, para almacenar la información de direccionamiento de la red H.323, y de un teléfono IP Cisco 7905G, para la recepción de llamadas desde el centro de control.

Esta elección resulta óptima en la medida en que la agenda del Alcatel Temporis 45 es suficiente para contener la identificación de todos los interfonos de la estación de Bailén, pudiendo, mediante dicha agenda, mostrarle al operador la localización del interfono llamante. Mientras, en el centro de control (donde estará el Cisco 7905G), y habilitándose posibles ampliaciones de la red de interfonía, podrían hacer falta más registros; y, sin embargo, a este centro de control no le interesa conocer qué interfono en concreto está llamando, sino, más bien, desde qué estación de toda la red de metro. Esta información se contendrá en el H323ID (identificador de red H.323) de cada pasarela, situada en cada estación, mostrándose en el *display* del teléfono IP (además de la extensión del número llamante).

El diagrama de la plataforma completa se muestra en la figura 38:

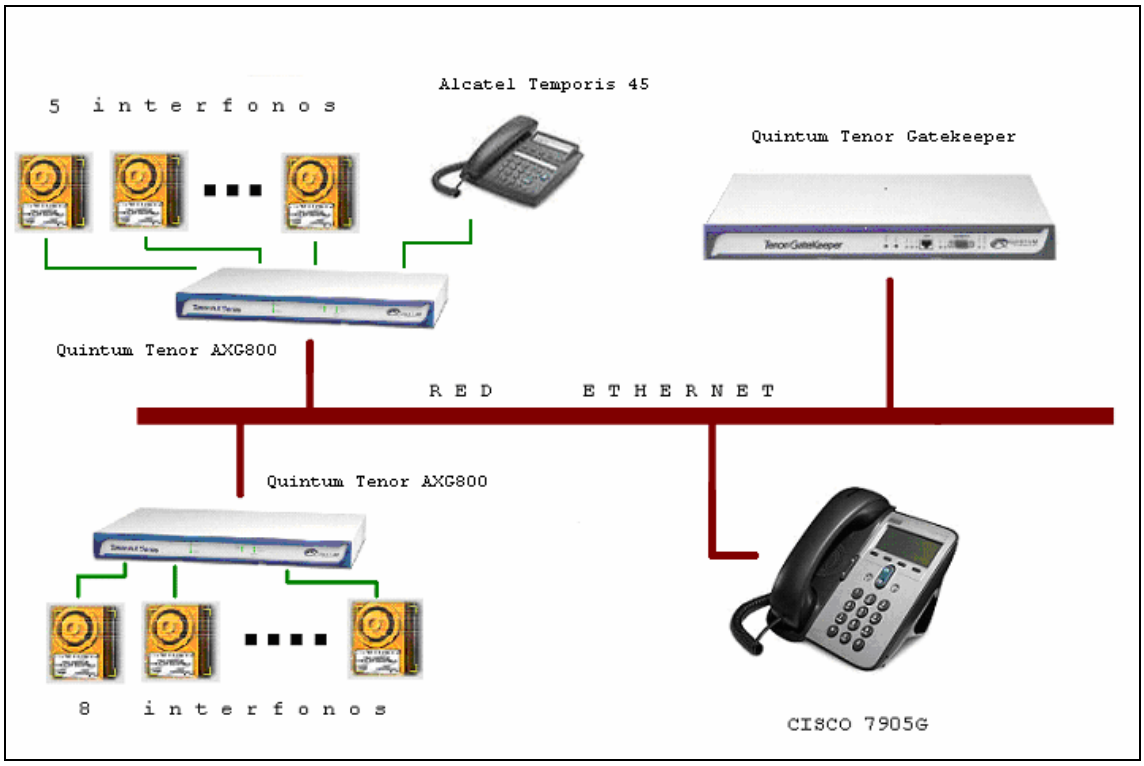


Figura 38: Esquema completo para la Plataforma de Interfonía Estación de Bailén

En total, se utilizarán:

- 2 Quintum Tenor AXG800, pasarela de interfonos a VoIP en H.323.
- 1 Quintum Tenor Gatekeeper, H.323.
- 1 Teléfono IP Cisco 7905G.
- 1 Alcatel Temporis 45, teléfono analógico.
- 13 interfonos Viking 1600A, con soporte metálico reforzado.

3.3.5.2 Elección del plan de marcado

Los equipos Quintum Tenor, usando NonStandardData en las comunicaciones H.323, identifican dos tipos de numeración asociada a comunicaciones VoIP: una pública, destinada a comunicaciones con la PSTN, y otra privada, de carácter interno; esta división puede ocasionar graves problemas de interoperabilidad con equipamientos de otros fabricantes, si no se conocen en profundidad los parámetros Quintum que configuran la numeración en sus equipos y los comportamientos de la red en cada caso.

La numeración pública hace referencia a los rangos numéricos que tengan que acomodarse al formato E.164; hay que recordar que estos equipos están diseñados para permitir la interacción con la extensa red de telefonía norteamericana, que dispone de múltiples operadores, cada uno con unas numeraciones E.164 muy específicas (con prefijos de subred y de selección de portadora). Mientras, la numeración privada se destina a las llamadas que tengan lugar entre los equipos Quintum.

La mayoría de los equipos VoIP se registran en el Quintum Tenor Gatekeeper como números públicos. Sin embargo, la numeración pública presenta algunos problemas incluso en los mismos equipos Quintum, cuando se trata de establecer comunicaciones entre puertos de la misma pasarela. Esto sucede así debido a una separación interna en interfaces analógica y ethernet, cada una con un motor de búsqueda de rutas independiente. En llamadas intra-pasarelas, el motor de rutado interno de la interfaz analógica no identifica los números de tipo público como locales; da paso al siguiente nivel de búsqueda de rutas, por IP, y al final la conmutación no tiene lugar.

Quintum, consciente de estas dificultades, presenta en sus equipos numerosas opciones de configuración relacionadas con el plan de marcado, como se verá a continuación.

Por otro lado, el teléfono IP Cisco 7905G usado también en esta plataforma presenta las siguientes dificultades de interoperabilidad con el equipamiento de Quintum relacionadas con este plan de numeración:

- Para recibir una llamada, se autentica en el Quintum Tenor Gatekeeper como un número de tipo público.
- Mientras, para establecer una llamada, todos los destinos marcados por el Cisco 7905G son considerados (por el Gatekeeper) como destinos de tipo privado. Pero luego, en las pasarelas Quintum Tenor, el número destino marcado por un Cisco 7905G será tratado como de tipo público por el motor interno de rutas analógico de esta pasarela.

Todas las posibilidades de interoperación de la pasarela se muestran en la figura 39: en ella, cada círculo representa una búsqueda interna de rutas relacionada con el tipo de numeración: en rojo se han representado las llamadas desde las pasarelas hasta el Cisco 7905G; en azul, las llamadas desde el Cisco 7905G y las pasarelas; y en verde las llamadas entre pasarelas:

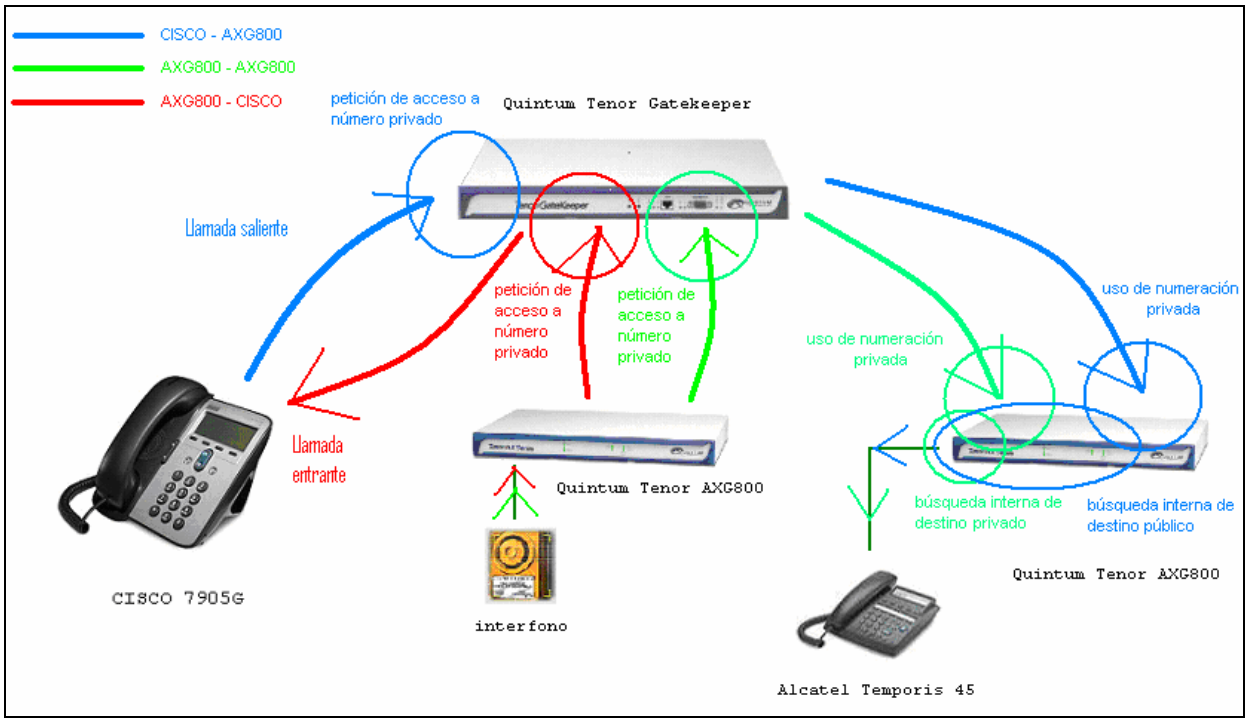


Figura 39: Esquema de comunicaciones y tipos de numeración, Plataforma de Interfonía Estación de Bailén

Ya se introdujo que para permitir las correctas comunicaciones inter-pasarela, necesita hacerse uso de una numeración de tipo privado para las llamadas salientes de las pasarelas Quintum Tenor, o podrían producirse errores. Al mismo tiempo, existirán llamadas que hagan uso internamente de una numeración de tipo público, cuando provengan del Cisco 7905G, (o de cualquier otro terminal VoIP que pueda necesitarse en futuras ampliaciones de la plataforma). Esto quiere decir que hará falta usar ambos tipos de numeración simultáneamente. Para ello, se utiliza el prefijo `Intercom`.

El prefijo `Intercom` es un prefijo numérico que permite el uso conjunto de ambos tipos de numeración, estableciendo las llamadas salientes como de tipo privado para todos los números marcados que comiencen con dicho prefijo. En esta plataforma, este prefijo `Intercom` se establecerá a 1, y todos los números del plan de numeración comenzarán por este número. Para dotar de capacidades de ampliación a la plataforma, se usarán 4 dígitos (mil números en el plan de marcado).

Pero este prefijo es suprimido del número marcado al acceder a la información de direccionamiento, mediante comunicaciones RAS contra el Gatekeeper de la plataforma. Esto quiere decir que en el Gatekeeper todos los números deberán estar registrados tanto con este 1 (para el rutado de llamadas desde equipamiento no Quintum), como sin él (para el rutado de llamadas desde estas pasarelas Quintum), es decir, con 3 y 4 cifras:

- En las pasarelas, bastará con asignarle a cada interfaz esos dos números, (mediante los directorios `HuntLDN`, como se estudiará en el apartado de configuración de las pasarelas).
- Para el Cisco 7905G (así como para todos los terminales que posteriormente necesiten integrarse en la plataforma), hará falta establecer en el Gatekeeper una ruta estática que relacione el número privado de tres cifras con el Cisco 7905G. La forma de hacerlo se detallará en el apartado de configuración del Gatekeeper.

Luego de atravesar el Gatekeeper, las pasarelas permiten reajustar el número destino, mediante los llamados `Outbound Prefix` (prefijos de salida) del plan de marcado IP (*IP Dial Plan*). Estableciendo este prefijo de salida IP a 1, el número de destino volverá a los 4 dígitos, asegurándose la interoperabilidad con otro equipamiento ajeno a estos complicados planes de numeración.

Para clarificar todo esta problemática se analizará a continuación paso a paso el establecimiento de llamada desde un Quintum Tenor hasta el Cisco 7905G, el cual tendrá asignado el número 1020 del plan de numeración:

Cuando un terminal analógico o interfono marca el 1020, primero se suprime el prefijo `Intercom` quedando el número 020 privado. Lo que hace luego la pasarela es buscar ese número entre sus propias extensiones, y si lo encontrase, por tratarse de numeración privada, conmutaría la llamada entre esos dos puertos (sin ni siquiera atravesar el Gatekeeper). En caso contrario, este número pasará a continuación, mediante RAS, al Gatekeeper, en donde una ruta estática asociará este número 020 privado al teléfono Cisco 7905G.

Luego de atravesar el Gatekeeper y de, mediante RAS, recoger la información de rutado IP acerca del destino, el *IP Routing Group*, la pasarela, utilizando el `Outbound Prefix`, transforma el número destino de nuevo a 1020 y tipo privado. Ahora mediante señalización

de llamada H.225.0 en comunicación directa con el destino, el Cisco 7905G recibirá una petición de llamada asociada al número 1020 (sin importarle el tipo de numeración pública o privada).

En fin, en cada pasarela será necesario configurar en las pasarelas, para su registro en el Gatekeeper, asociado a cada extensión FXS:

- Un número privado de 4 cifras, que comience por 1, para saltos inter-pasarelas tras atravesar el Gatekeeper, y para el acceso RAS en el Gatekeeper desde el Cisco 7905G (ver figura 67).
- El mismo número pero con tipo público, para el acceso desde el Cisco 7905G (así como futuros nuevos terminales que sólo usen esta numeración pública) tras atravesar el Gatekeeper.
- Y un número privado de 3 cifras, para saltos intra-pasarelas y para el protocolo RAS en los saltos inter-pasarelas. El número es el mismo pero sin el prefijo 1.

3.3.5.3 Planes de marcado y de direccionamiento IP

Con respecto al plan de direccionamiento IP, todos los elementos IP tienen 255.255.0.0 de máscara de subred, en este caso muy amplia con el objetivo de no entorpecer futuras ampliaciones de la red de interfonía.

Los planes de marcado y de direccionamiento IP quedan en definitiva de la siguiente forma:

- Pasarelas:

Extensión	Dirección IP / Puerto FXS	H323 ID	Nombre asociado en el Alcatel Temporis 45
1001	10.13.108.1 / 1	Bailen1	ANDEN1
1002	10.13.108.1 / 2	Bailen1	ANDEN2
1003	10.13.108.1 / 3	Bailen1	ANDEN3
1004	10.13.108.1 / 4	Bailen1	ANDEN4
1005	10.13.108.1 / 5	Bailen1	CANCELADORA-JES1
1006	10.13.108.1 / 6	Bailen1	CANCELADORA-JES2
1007	10.13.108.1 / 7	Bailen1	EXPENDEDORA-JESU
1008	10.13.108.1 / 8	Bailen1	XATIVA-PILAR
1009	10.13.108.2 / 1	Bailen2	EXPENDEDORA-XATI
1010	10.13.108.2 / 2	Bailen2	PUERTA-XATIVA
1011	10.13.108.2 / 3	Bailen2	VESTIBULO-RENFE
1012	10.13.108.2 / 4	Bailen2	ASCENSOR-RENFE
1013	10.13.108.2 / 5	Bailen2	ASCENSOR-XATIVA
1014	10.13.108.2 / 6	Bailen2	OPERADOR1
1015	10.13.108.2 / 7	Bailen2	por determinar (reserva)
1016	10.13.108.2 / 8	Bailen2	por determinar (reserva)

Los números de serie son A022-00C7E0 para Bailen1 y A022-00C7DE para Bailen2.

En este punto, hay que notar que la elección de los nombres asociados a cada interfono viene dada por el cliente.

- Gatekeeper:

Dirección IP	Máscara de subred	Modelo	Número de Serie
10.13.253.1	255.255.0.0	GK20	A006-002D86

- Cisco 7905G:

Extensión	Dirección IP	H323 ID	Nombre asociado en el Alcatel Temporis 45
1020	10.13.253.2	BailenPuestoMando	PUESTO-MANDO

Tanto el Gatekeeper como el Cisco 7905G se instalarán en el puesto de mando del Metro de Valencia; por eso llevan asociados distinta subred.

3.3.5.4 Códecs y funcionalidades H.323

Para esta plataforma, es fundamental que todos los equipos que, prevista una posible ampliación de la misma, se conecten a ella no sufran ninguna incidencia en su funcionamiento básico.

Al ser de nuevo el ancho de banda de la red local lo suficientemente grande, tampoco en esta ocasión se practicará compresión sobre el audio, usándose de nuevo el códec G.711 Mu-law, con muestras de 20 ms: este códec es obligatorio para cualquier terminal H.323.

Por otro lado, también se anularán de la configuración las capacidades de *Fast Connect*, así como los “tunelizados” H.245, (por los mismos motivos que los expuestos para el diseño de la plataforma de Barrio de las Letras).

3.4 Configuración

3.4.1 Plataforma Barrio de las Letras

A continuación se muestra la configuración de cada uno de los terminales que forman parte de la plataforma.

3.4.1.1 Pasarelas Quintum Tenor ASG200

La versión del *firmware* usada en estas pasarelas es la P102-11-08. Los archivos que contienen esta versión de firmware se pueden encontrar en la documentación adjunta, en la carpeta `Archivos Adjuntos\Quintum Technologies\Version del software AS-AX-GK\AS_AX-P102-11-08\AS`.

La configuración inicial de estas pasarelas se realiza mediante conexión por puerto serie. Con un PC con sistema operativo Windows puede hacerse uso el programa HyperTerminal, con 38400 bps, 8 bits de datos sin paridad, 1 bit de parada, y sin control de flujo. Una vez conectados al Quintum Tenor, con usuario/contraseña admin/admin, escribiendo (la figura 40 muestra lo que aparece en pantalla, con comentarios entre corchetes):

```
Quintum# eth
Quintum-EthernetInterface-SL1DV1EI1# config
config-EthernetInterface-SL1DV1EI1# set sm [y ahora la máscara de subred
deseada] 255.255.192.0
config-EthernetInterface-SL1DV1EI1* set ipa [y la dirección ip del equipo]
10.54.187.61
config-EthernetInterface-SL1DV1EI1* siprd
config-StaticIPRouteDir-1* change 1 g [y ahora la pasarela por defecto:
este parámetro debe pertenecer necesariamente a la subred del equipo,
aunque bien puede no ser utilizado nunca] 10.13.187.254

  StaticIPRoute Table

  index   Destination   NetMask   Gateway         EIAttached    Metric
  -----   -----------   -------   ------------    ------------  ------
  1       0.0.0.0       0.0.0.0   10.54.187.254   EI-SL1DV1EI1  1

config-StaticIPRouteDir-1* submit
config-StaticIPRouteDir-1# main
maintain-StaticIPRouteDir-1# mc
maintain-MasterChassis-1# reset
Are you sure that you want to reset the MasterChassis (Yes/No)? yes
```

Figura 40: Configuración inicial de las pasarelas ASG200 para la plataforma del Barrio de las Letras

Con esto, quedan establecidos los parámetros básicos necesarios para conectarse a la red IP.

A continuación, la configuración de estos equipos debe realizarse mediante el uso de un software java, de un formato claro y visual, suministrado por el fabricante y descargable desde su página web, llamado el *Tenor Configuration Manager*. Todas las referencias de

configuración se harán según este programa, con capturas de pantalla incluidas, así como algunos comentarios sobre sus implicaciones en cuanto al protocolo H.323 o a la interoperabilidad con otros equipos. La mayoría de las opciones de configuración se dejarán por defecto, comentándose sólo algunas de ellas. Este programa sólo se encuentra disponible en inglés. Se adjunta la versión correspondiente al *firmware* utilizado en la carpeta `Archivos Adjuntos\Quintum Technologies\Tenor Configuration Manager` del CD adjunto, en el archivo `CM103-07-02.zip`.

Las configuraciones de cada ASG200 son muy similares entre sí: apenas sí difieren en los parámetros mostrados en las tablas del apartado 3.3.4.2, planes de marcado y de direccionamiento IP: se mostrará la configuración de una de las pasarelas, comentándose también las diferencias que existieran con la configuración del resto de las pasarelas.

Para comenzar, en la pantalla inicial del *Tenor Configuration Manager* arrancado desde un PC conectado a la red local y con la misma máscara de subred, con *Login* admin, *Password* admin, se define a qué equipo desea conectarse (figura 41):

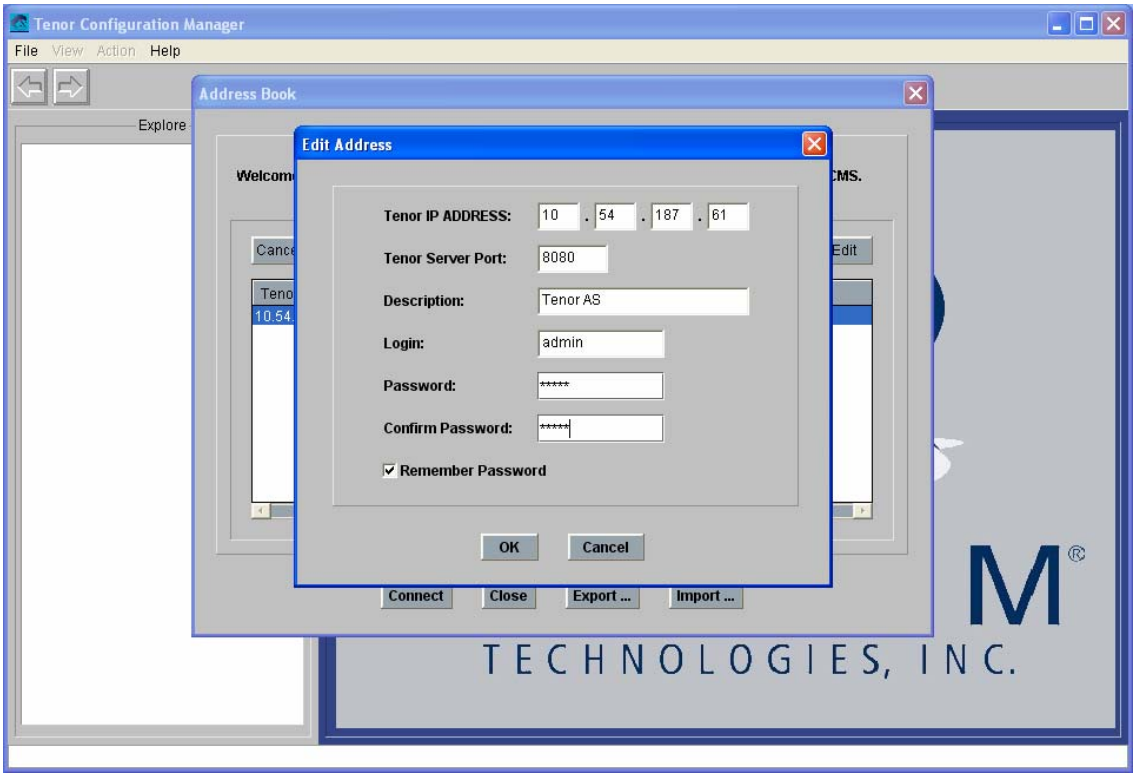


Figura 41: Captura 1 del *Tenor Configuration Manager* para la plataforma del Barrio de las Letras.

A continuación, el software se descarga del equipo una serie de objetos que almacenan la configuración interna. Durante el uso de esta herramienta no se advirtió ningún malfuncionamiento en cuanto a robustez ni a pérdida de información. Es decir, se trata de una herramienta muy fiable.

Lo primero que ha de hacerse es establecer el plan de marcado: hay que anular todos los prefijos públicos (estos prefijos sirven, como ya se comentó, para solventar dificultades de comunicación entre terminales de distintos estados y operadores en los EE.UU.), y limitar la longitud de la numeración a 2 cifras, como se muestra en la figura 42:

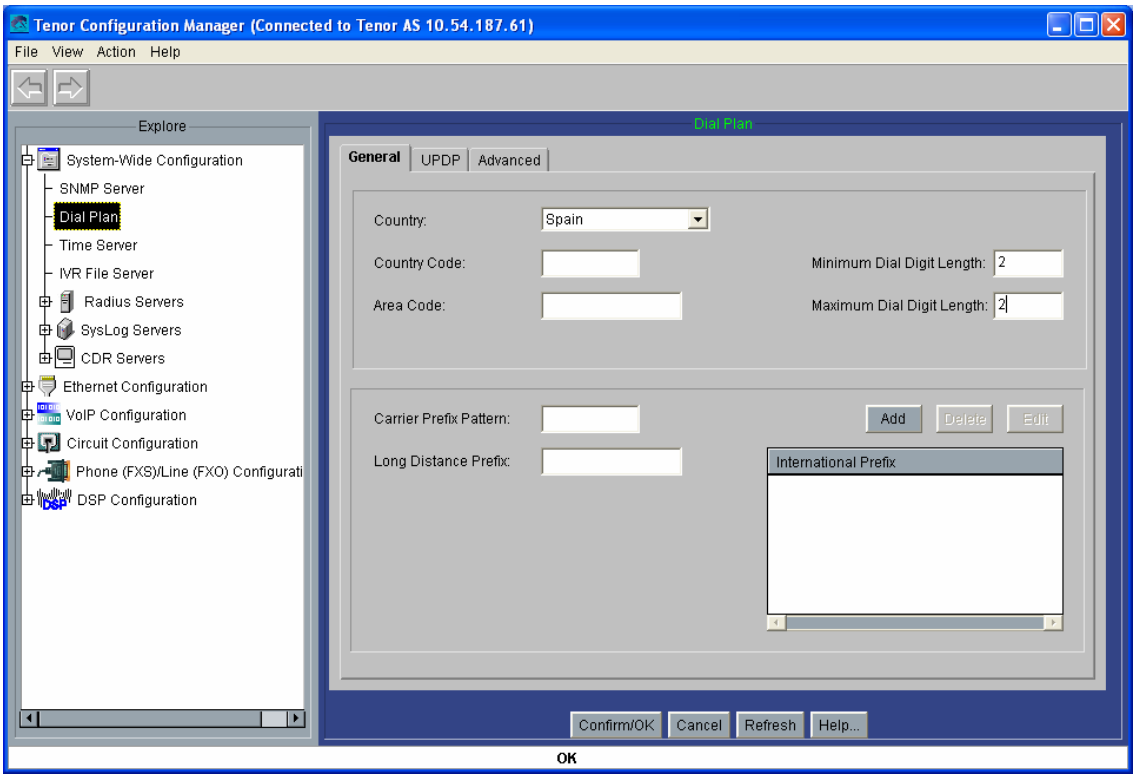


Figura 42: Captura 2 del *Tenor Configuration Manager* para la plataforma del Barrio de las Letras.

A continuación se muestra la configuración del plan de numeración. Como se introdujo anteriormente para la plataforma de la Estación de Bailén, el uso de un plan de numeración privado impidiría la comunicación con el teléfono IP de atención, el SJPhone. Por otro lado, el uso de un plan de tipo público hace imposible las comunicaciones entre puertos de la misma pasarela.

Sin embargo, para esta plataforma en ningún caso se intentarán cursar llamadas intra-pasarelas. Así se ha elegido un plan de numeración de tipo público, con el parámetro `Intercom` (cuyo uso y funcionalidad ya se analizó para el diseño de la Plataforma de Interfonía Estación de Bailén) desactivado (figura 43):

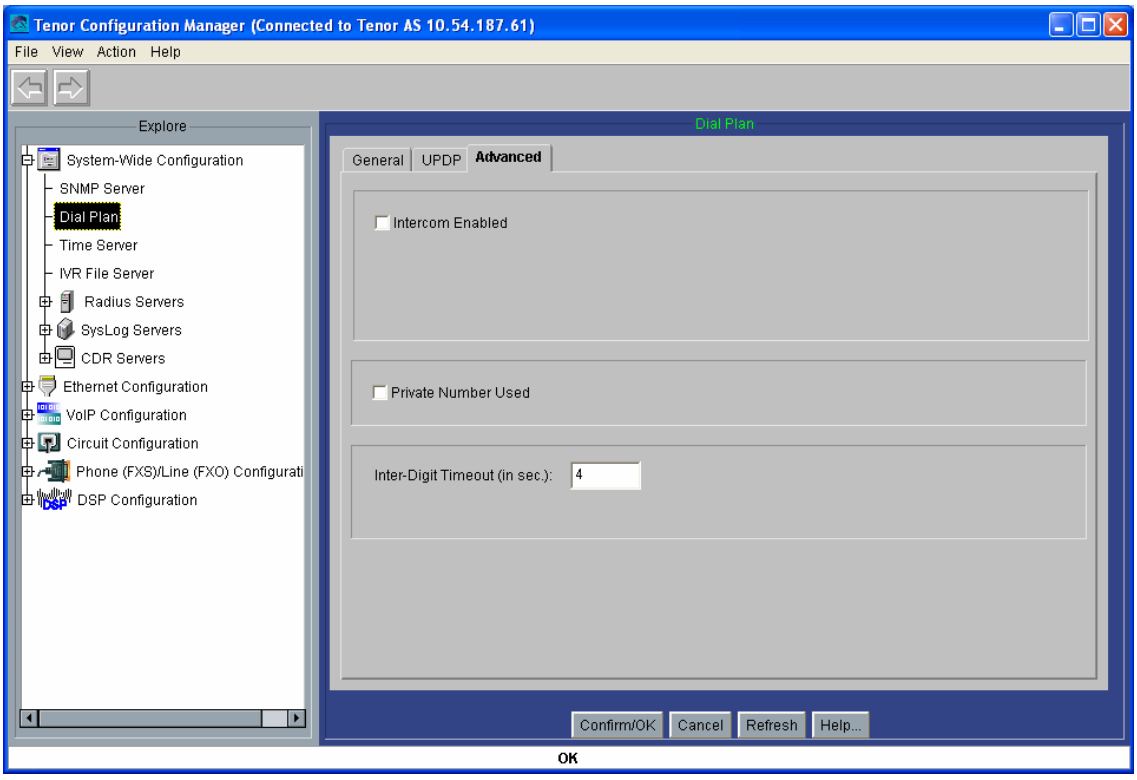


Figura 43: Captura 3 del *Tenor Configuration Manager* para la plataforma del Barrio de las Letras.

En las dos pantallas siguientes (figuras 44 y 45) se establecen los parámetros de configuración VoIP. Se configurará la dirección IP del Gatekeeper: 10.54.187.60. En el `H323ID` se usará la localización de cada una de las pasarelas como mecanismo de identificación en el Gatekeeper: en este caso, interfonoMoratin, y para el resto de pasarelas, interfonoLopeDeVega, interfonoSanAgustin, interfonoPrado, interfonoSantaCatalina, interfonoSantaAna, interfonoLeon, e interfonoFucar, respectivamente. También se anulará *Fast Start* (otra forma de llamar a *Fast Connect*) y el H245 *tunneling* asociado con él, tal como se detalló en el apartado de diseño.

También se configurará el `Lightweight RRQ` (tramas faro con el Gatekeeper) cada 30 segundos, `Timeout RIP` de 10 segundos y `H245 timer` de 6 segundos. Todos estos tiempos son holgados y prevén posibles caídas de la alimentación o sencillamente de algún equipo.

Por otro lado, en el la dirección del *secondary* Gatekeeper, estableciendo la 0.0.0.0, estos equipos se configuran a sí mismos por defecto como *secondary* Gatekeeper: en caso de caída del Gatekeeper primario (lo cual, en principio, anularía el direccionamiento de la plataforma) comenzarían a funcionar 8 Gatekeepers independientes que, mediante mensajes LRQs multicast, podrían restablecer entre sí las tablas de direccionamiento del sistema, permitiéndose así una gran robustez. Mientras se funciona en este estado “secundario”, se comprueba continuamente la viabilidad del *primary* Gatekeeper, para conmutarse al estado normal en cuando éste se levante.

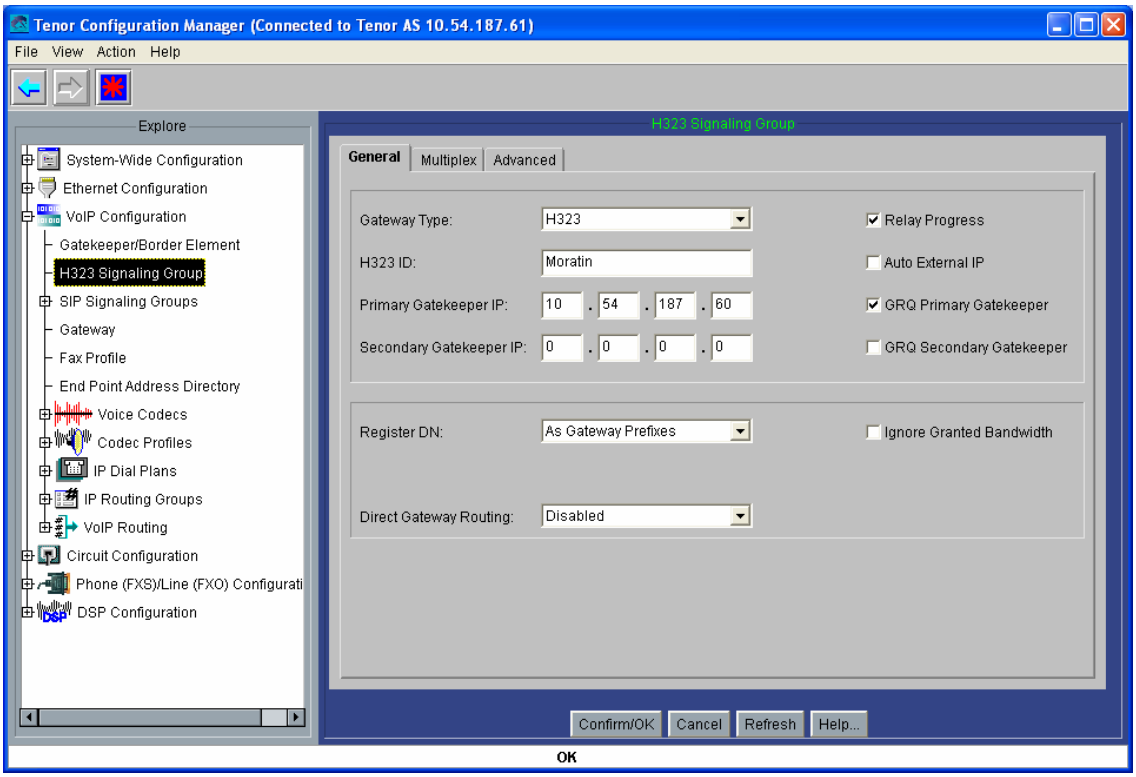


Figura 44: Captura 4 del *Tenor Configuration Manager* para la plataforma del Barrio de las Letras.

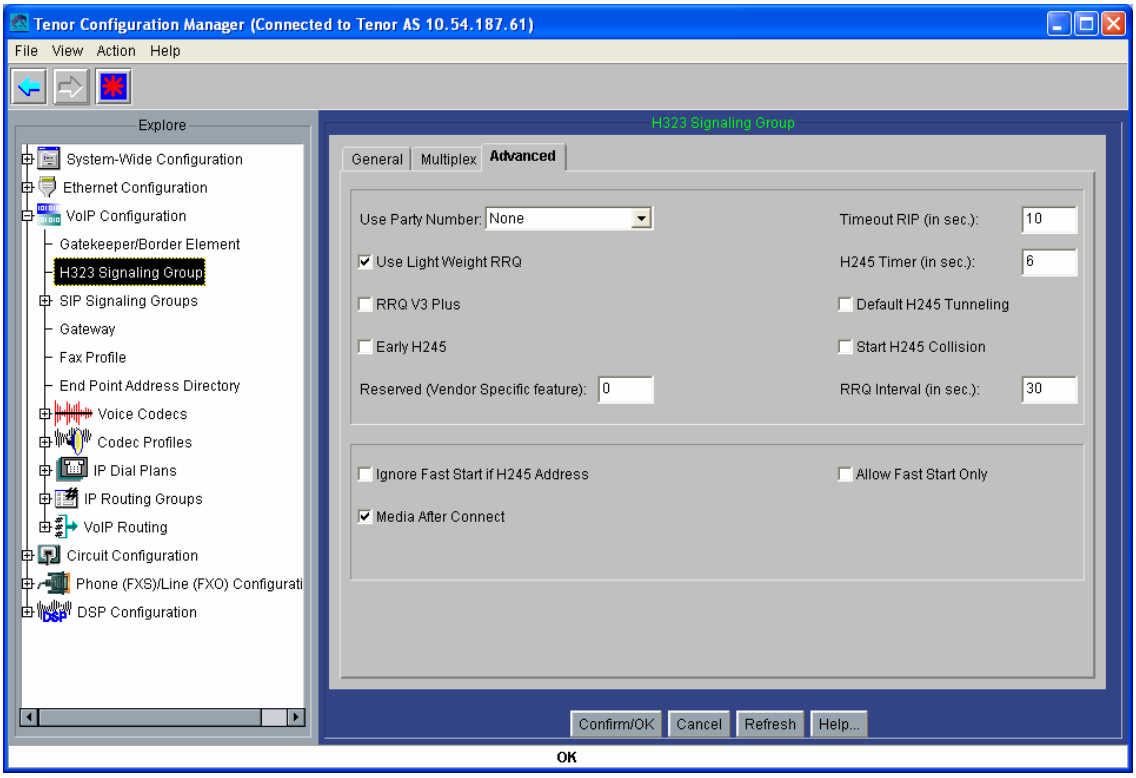


Figura 45: Captura 5 del *Tenor Configuration Manager* para la plataforma del Barrio de las Letras.

A continuación se muestra la configuración de los códecs (figuras 46 y 47): en el apartado `Voice Codec-1` se selecciona el códec G.711 Mu-law, con muestras de 20 ms (figura 46);

a continuación, este códec se introduce en el perfil de códecs (`Codec Profile – default`), como se muestra en la figura 47:

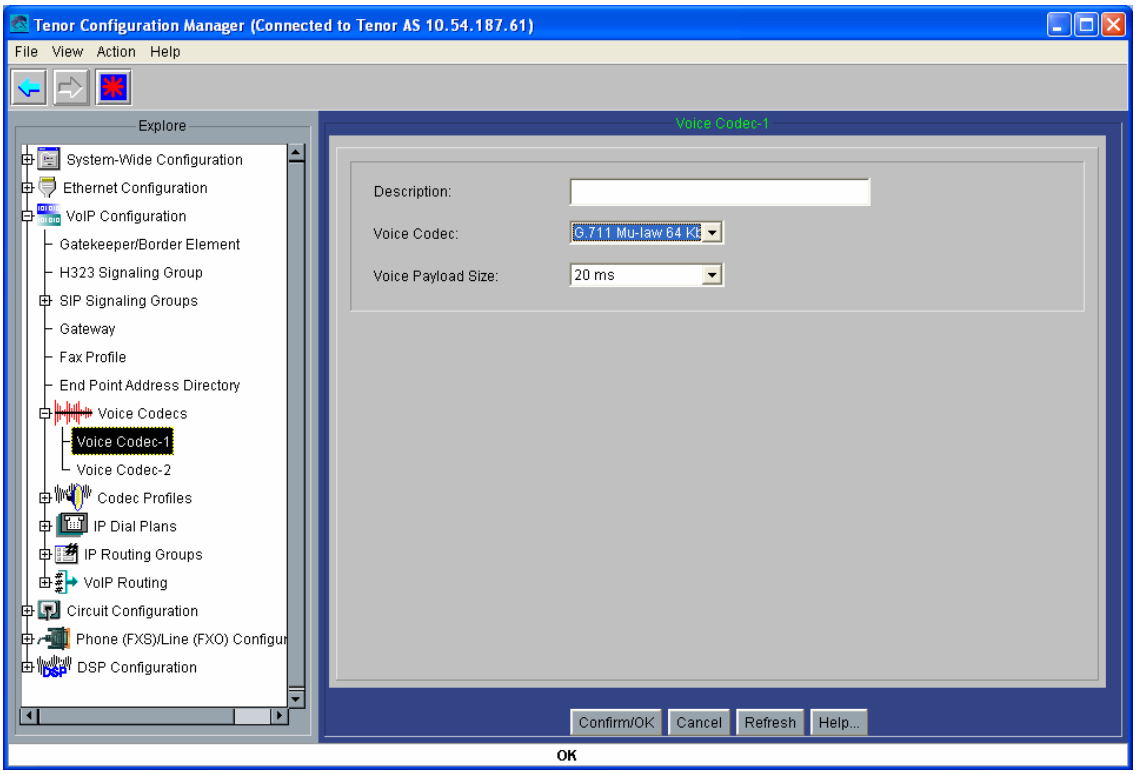


Figura 46: Captura 6 del *Tenor Configuration Manager* para la plataforma del Barrio de las Letras.

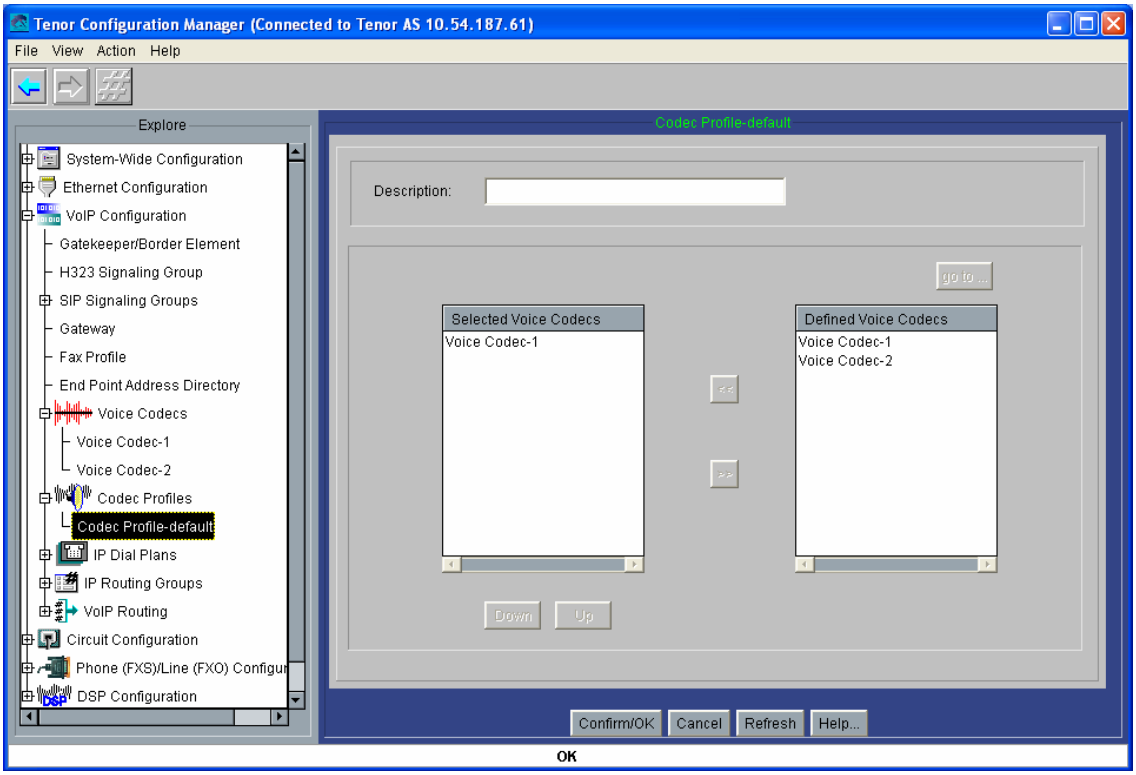


Figura 47: Captura 7 del *Tenor Configuration Manager* para la plataforma del Barrio de las Letras.

A continuación se muestra la configuración del `IP Routing Group` (figuras 48, 49 y 50), que es como un directorio en el que se establecen las características de las rutas IP: Se usarán *timers* TCP de 5 segundos. También se deshabilitará *Fast Start* para llamadas salientes (por el mismo motivo comentado anteriormente) y el uso de llamadas de fax.

También se limitarán todas las llamadas a 10 minutos (`Maximum Talk Time`); esto se hace para evitar cuelgues de la red que dejen las llamadas activas innecesariamente en el Gatekeeper: en algunos casos (en concreto, ante los fallos de comunicación entre los terminales y el Gatekeeper), existe la posibilidad de que se pierdan los paquetes RAS Disengage Request en los que cada terminal avisa al Gatekeeper de la finalización de su llamada. En estos casos, el Gatekeeper sigue esperando este paquete hasta que finaliza un temporizador (que es el que se configura mediante este parámetro). En el trabajo con pasarelas, que disponen de una capacidad de líneas limitada, este comportamiento reiterado podría dejar a esta pasarela, en la configuración interna del Gatekeeper, sin capacidad para aceptar una nueva llamada, rechazándose por RAS cualquier nuevo intento de comunicación contra ella a traves de dicho Gatekeeper.

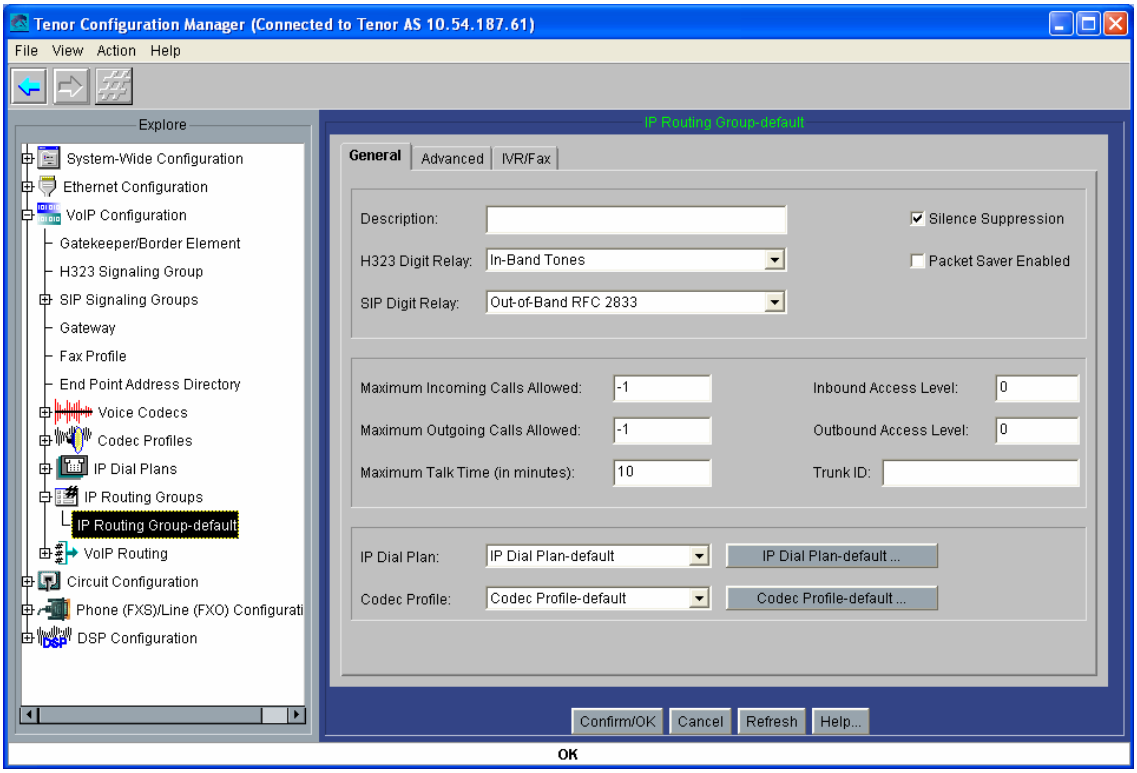


Figura 48: Captura 8 del *Tenor Configuration Manager* para la plataforma del Barrio de las Letras.

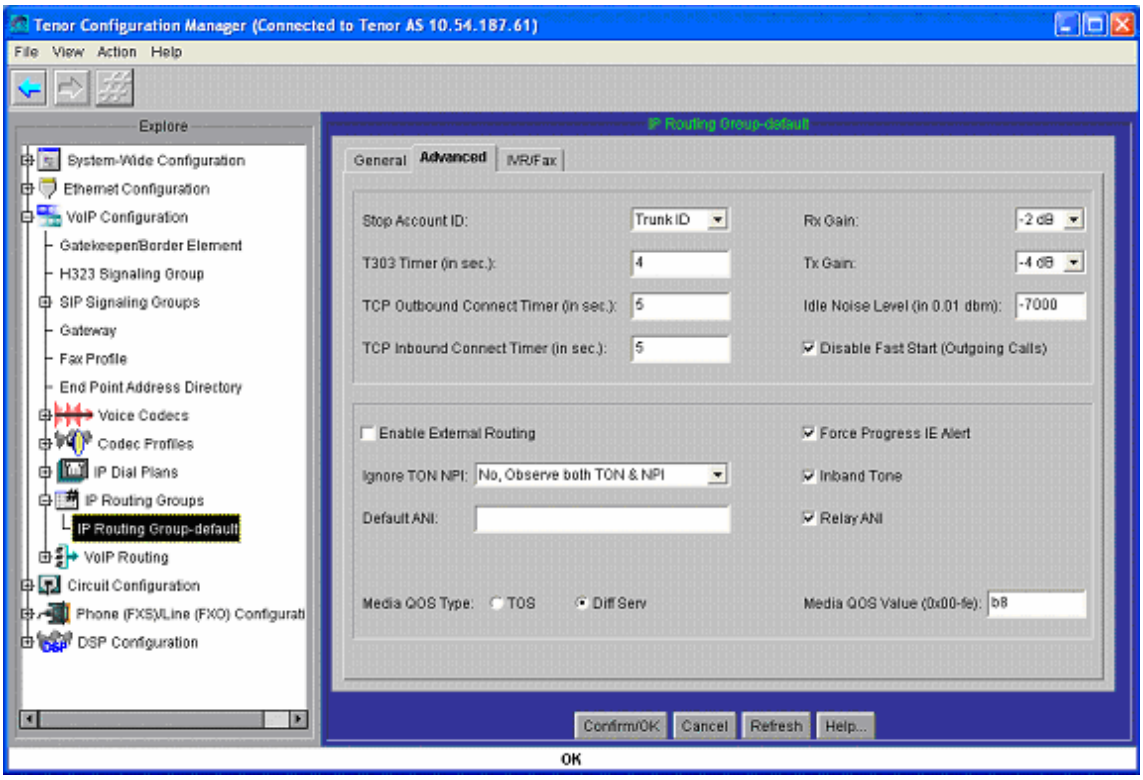


Figura 49: Captura 9 del *Tenor Configuration Manager* para la plataforma del Barrio de las Letras.

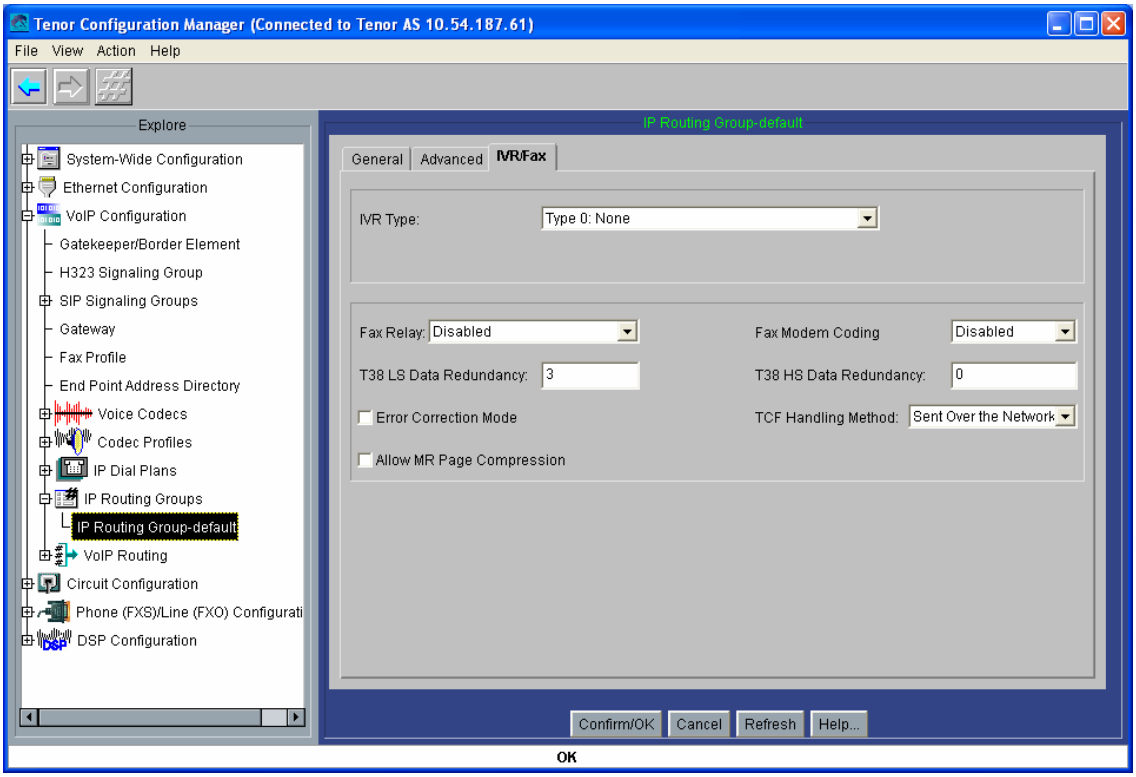


Figura 50: Captura 10 del *Tenor Configuration Manager* para la plataforma del Barrio de las Letras.

A continuación se muestra la configuración de las líneas analógicas: esto se consigue configurando el grupo de señalización CAS (*Channel Asociated Signalling*), que es un directorio de configuración de líneas analógicas (figuras 51, 52 y 53).

Puede configurarse un CAS *Signalling Group* común, o varios; luego, se asociará cada uno a una o a varias líneas (interfaces) analógicas. En este caso, sólo hará falta configurar uno, pues la configuración para ambas interfaces analógicas es idéntica.

En ellos, hay que activar, para conseguir una correcta comunicación entre las pasarelas y los interfonos, los parámetros `Loop Start Forward Disconnect` y `Disconnect Supervision` (con los que se le comunica al interfono el fin de la comunicación), como se muestra en la figura 51; activar el perfil de tonos de desconexión (perfil ya configurado por defecto, en el apartado `Tone Profile` del cual no se mostrará captura de pantalla), en la figura 52; y seleccionar la plantilla 5 (`Line Template`, en la figura 53). El resto de parámetros pueden dejarse con la configuración por defecto:

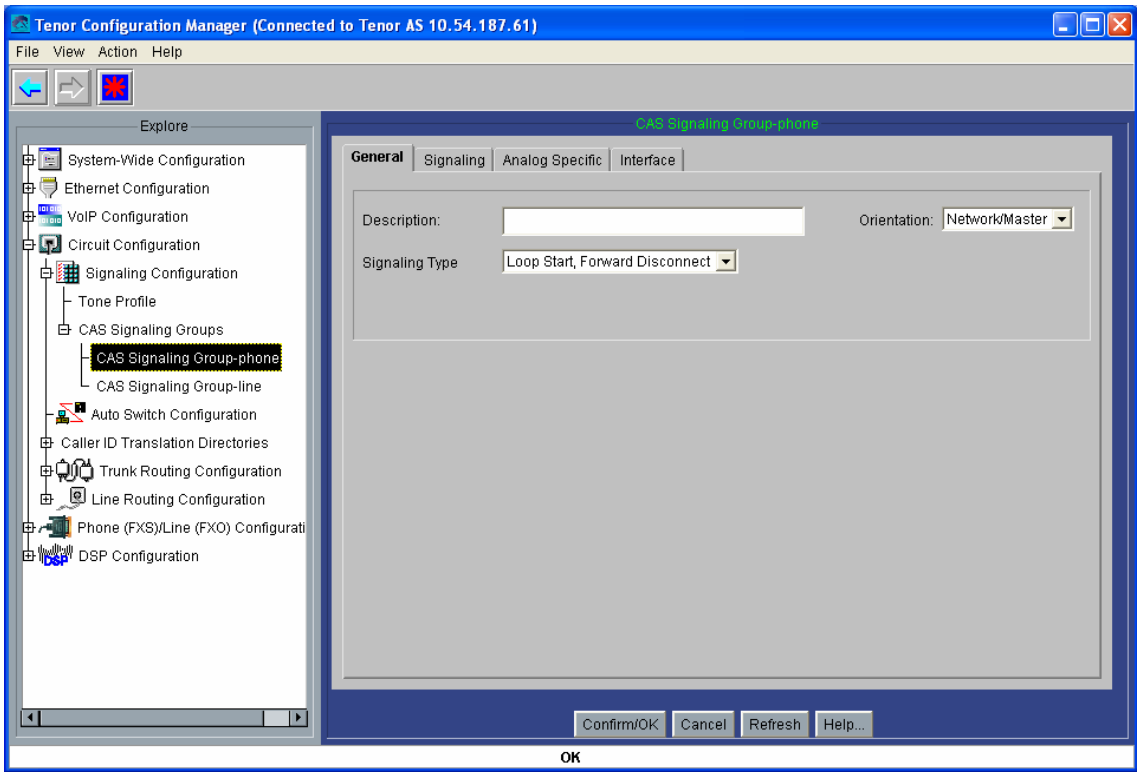


Figura 51: Captura 11 del *Tenor Configuration Manager* para la plataforma del Barrio de las Letras.

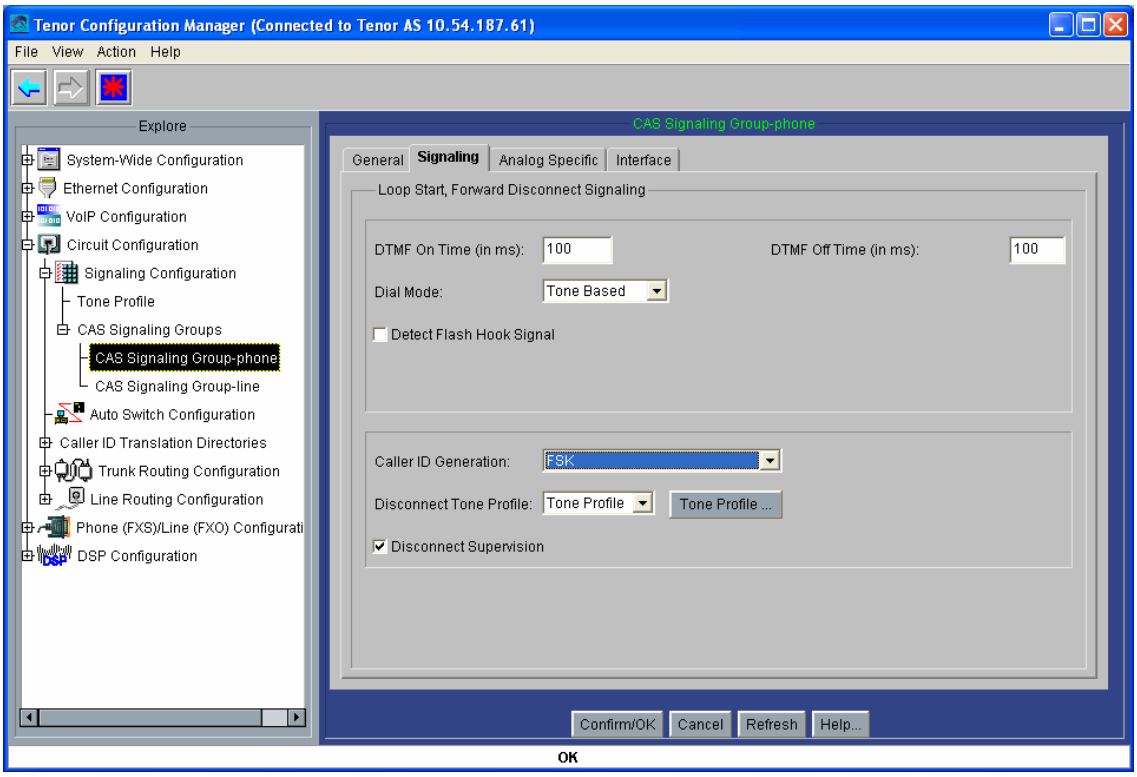


Figura 52: Captura 12 del *Tenor Configuration Manager* para la plataforma del Barrio de las Letras.

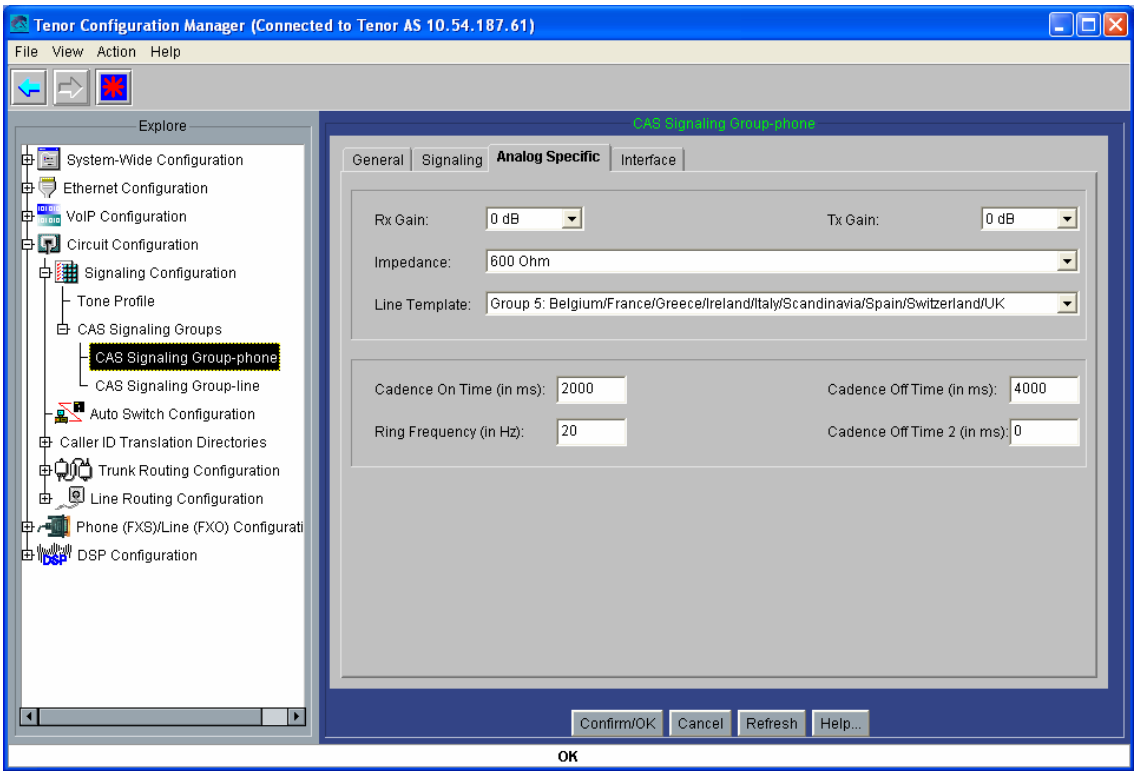


Figura 53: Captura 13 del *Tenor Configuration Manager* para la plataforma del Barrio de las Letras.

A continuación se muestra la configuración de las rutas por circuitos (*Line Routing Configuration*): primero, se creará un HuntLDN (*Hunt Local Directory Number*), es decir un número (o conjunto de números) a ser "cazados" por esta pasarela: se trata de los

números que se registrarán en el Gatekeeper asociados a esta pasarela: el 61 en este caso, el 62, 63, 64, 65, 66, 67 y 68 en las otras pasarelas, como se definió en el plan de numeración. Su configuración se muestra en la figura 54:

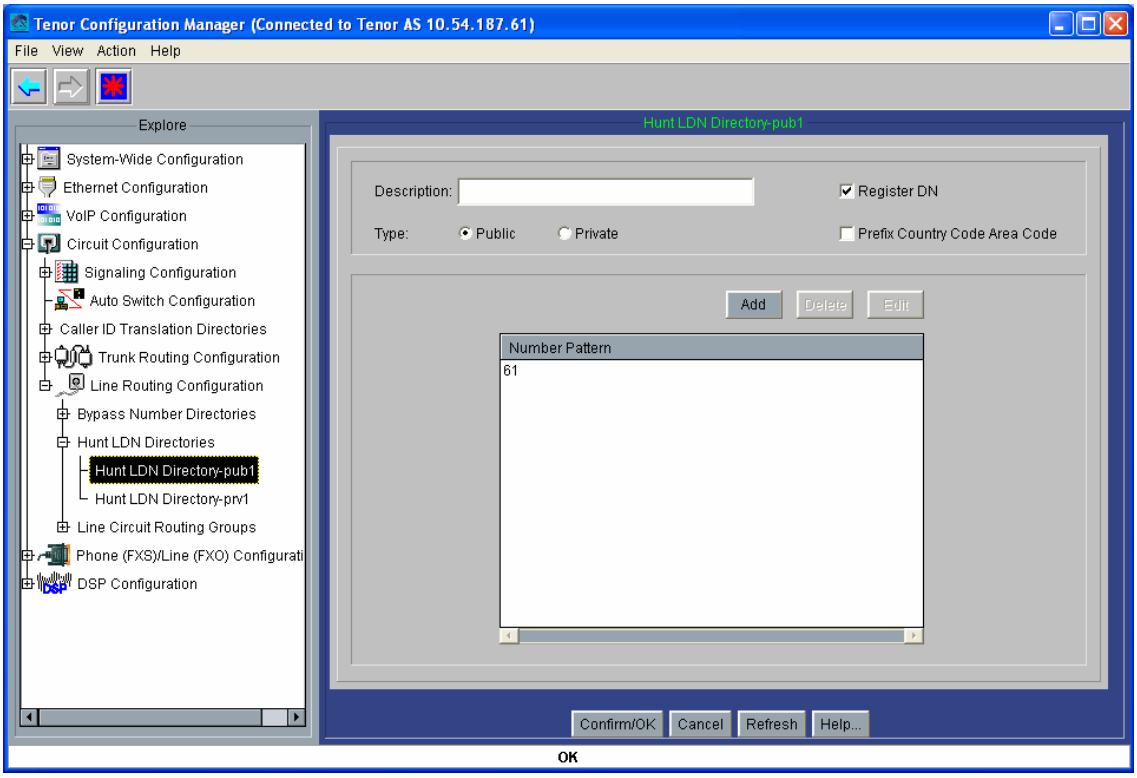


Figura 54: Captura 14 del *Tenor Configuration Manager* para la plataforma del Barrio de las Letras.

Se muestra ahora la configuración del LCRG (`Line Circuit Routing Group`, grupo de rutas por línea y por circuito, en las figuras 55, 56, 57, 58 y 59): al igual que con los CAS *Signalling Groups*, estos LCRG son directorios de configuración que se asociarán a una o varias de las interfaces analógicas de la pasarela. Para su configuración, ha de activarse la transmisión del tono de progreso de llamada para el interfono (`Provide Progress Tone`, figura 55); se establece un `Trunk ID` de 61 (62, 63, 64, 65, 66, 67 y 68 en las otras pasarelas), se activa la opción `caller ID type use trunk ID`, y se selecciona `trunk ID delivery calling party number`, para que el número llamante se corresponda con este *trunk ID* (figura 56). Esto se hará de esta forma para poder enviar la información del número llamante, pues de otra forma la determinación interna del número llamante no funciona correctamente. No se hará uso del dígito de final de marcado (en la misma figura).

Se limitará toda numeración a 2 dígitos para este grupo de líneas y circuitos (figura 57); se seleccionará el HuntLDN público configurado anteriormente para este LCRG (figura 58); y se anulará la opción de `Multi Path` (figura 59):

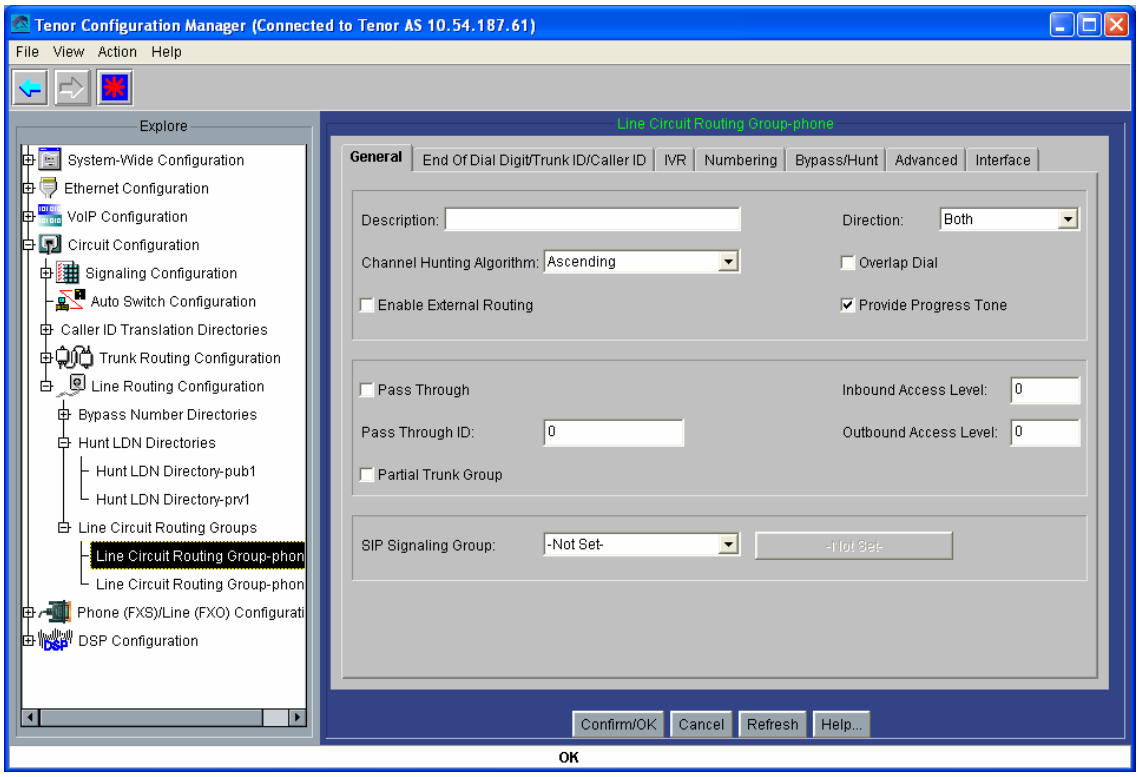


Figura 55: Captura 15 del *Tenor Configuration Manager* para la plataforma del Barrio de las Letras.

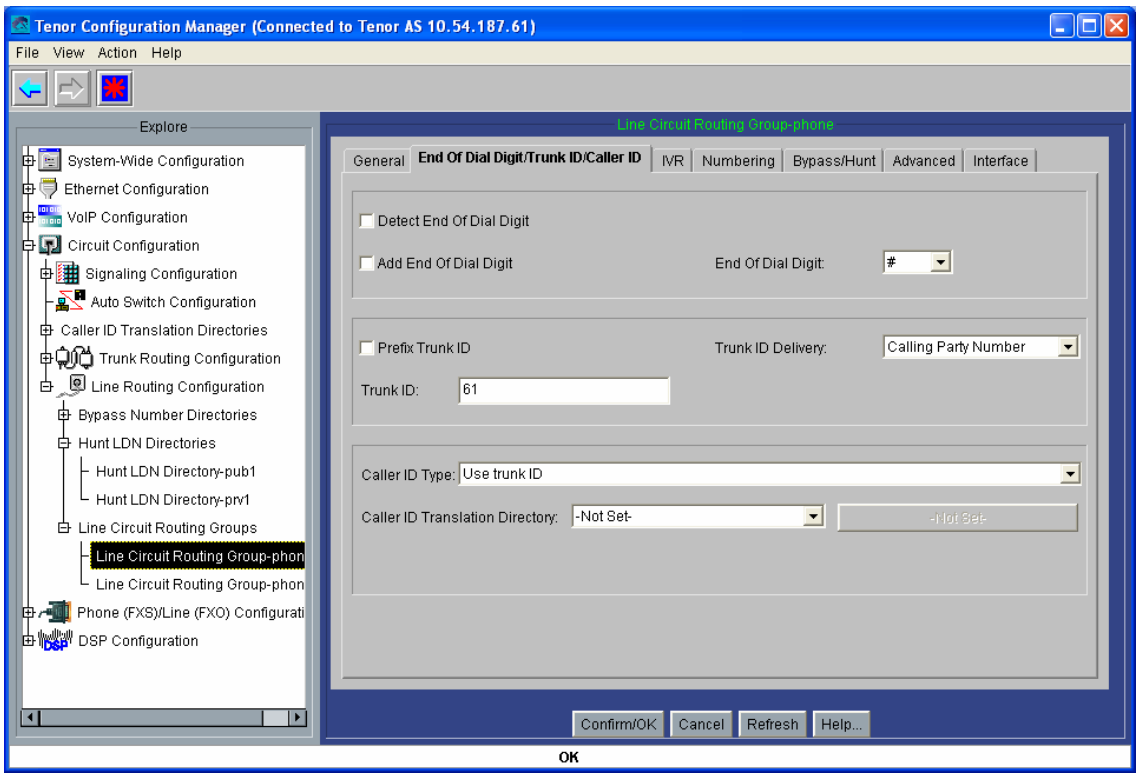


Figura 56: Captura 16 del *Tenor Configuration Manager* para la plataforma del Barrio de las Letras.

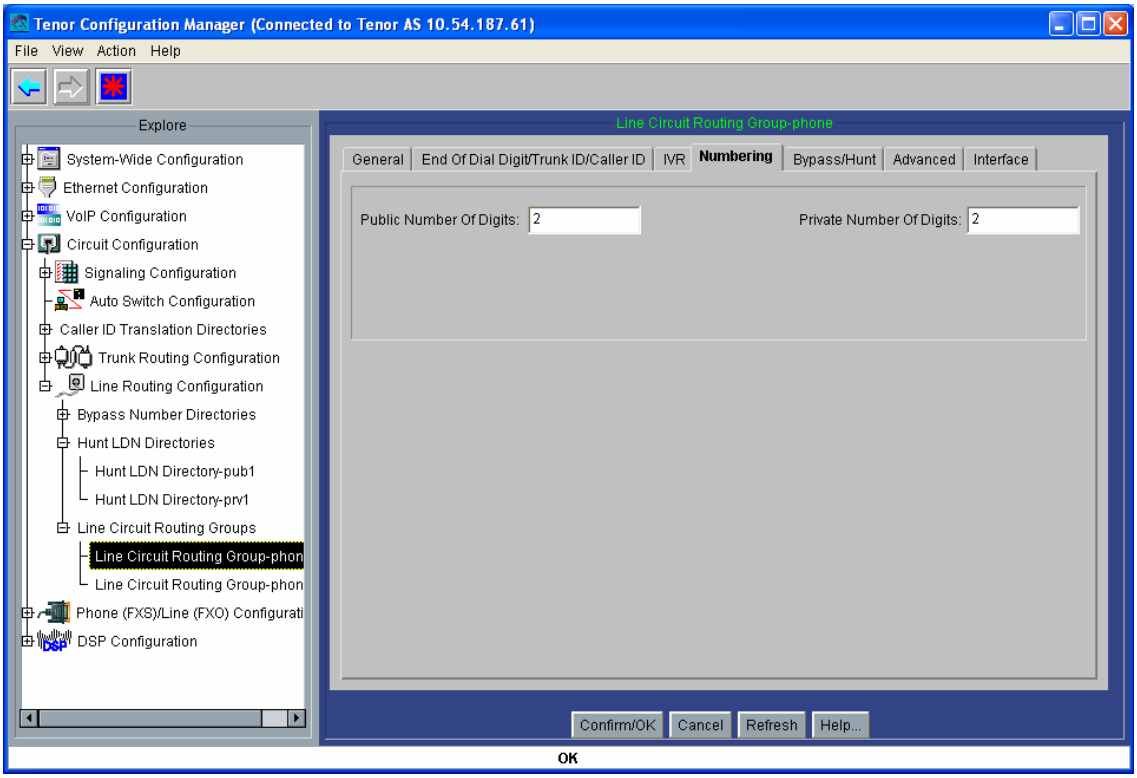


Figura 57: Captura 17 del *Tenor Configuration Manager* para la plataforma del Barrio de las Letras.

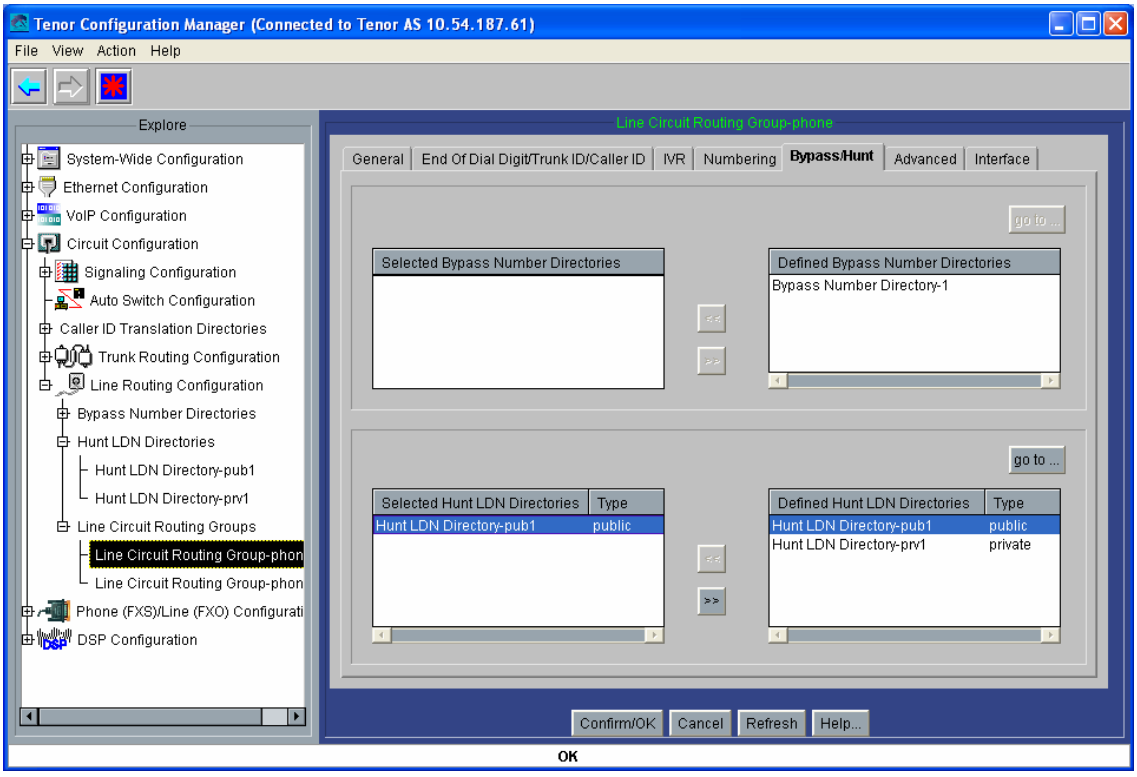


Figura 58: Captura 18 del *Tenor Configuration Manager* para la plataforma del Barrio de las Letras.

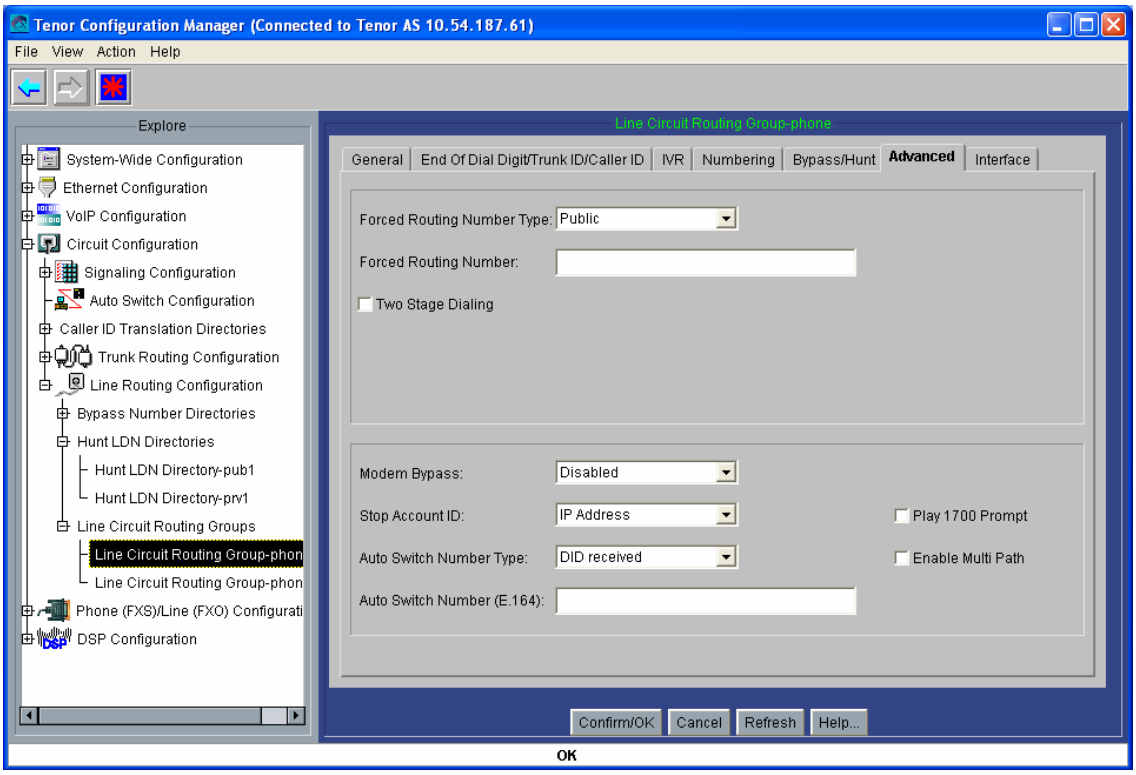


Figura 59: Captura 19 del *Tenor Configuration Manager* para la plataforma del Barrio de las Letras.

Ya sólo falta asociar el anterior LCRG y CASSG a uno de los canales analógicos de la pasarela (figuras 60 y 61): la pasarela tiene dos interfaces FXS, pero una de ellas no hará falta, y se deja deshabilitada. En el caso de que hiciese falta habilitarla, por avería de la primera, podrá hacerse cómodamente conectándose a la pasarela en cuestión mediante el *Tenor Configuration Manager*, desde un PC con acceso a esta subred del Ayuntamiento de Madrid.

Hay que crear un grupo de canales (*Channel Group*), y asociarlo a estos directorios abstractos (figura 60); el resultado se muestra en la figura 61:

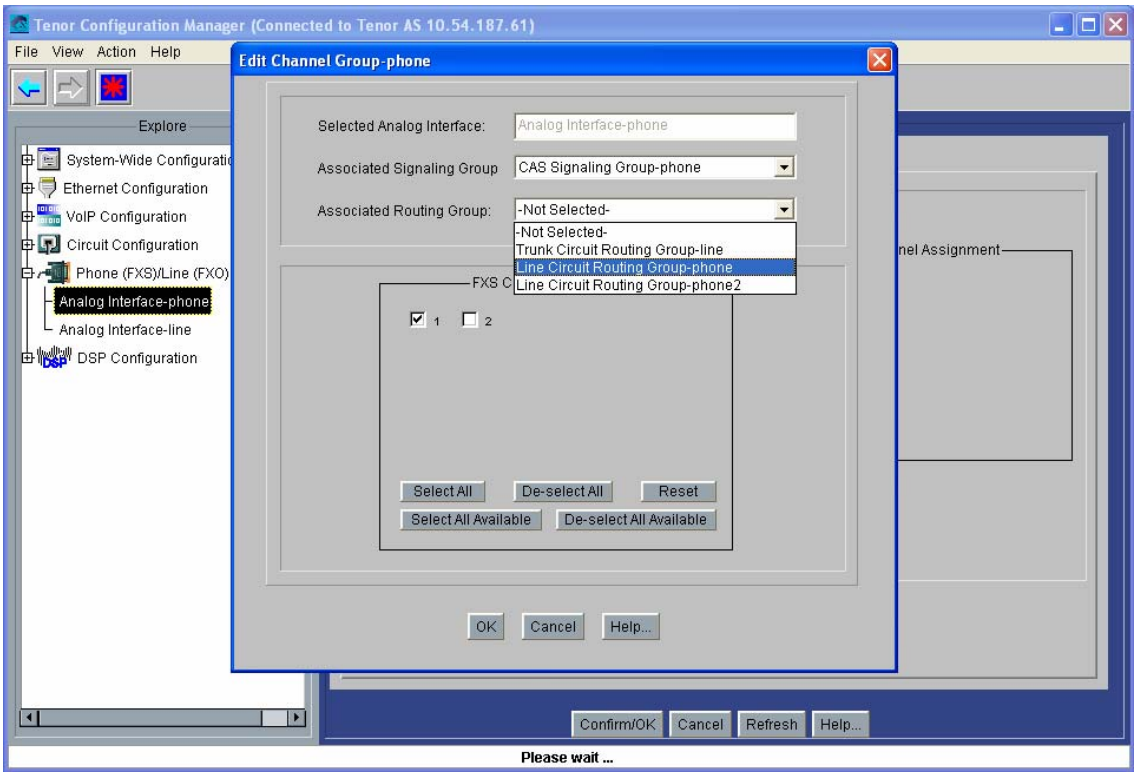


Figura 60: Captura 20 del *Tenor Configuration Manager* para la plataforma del Barrio de las Letras.

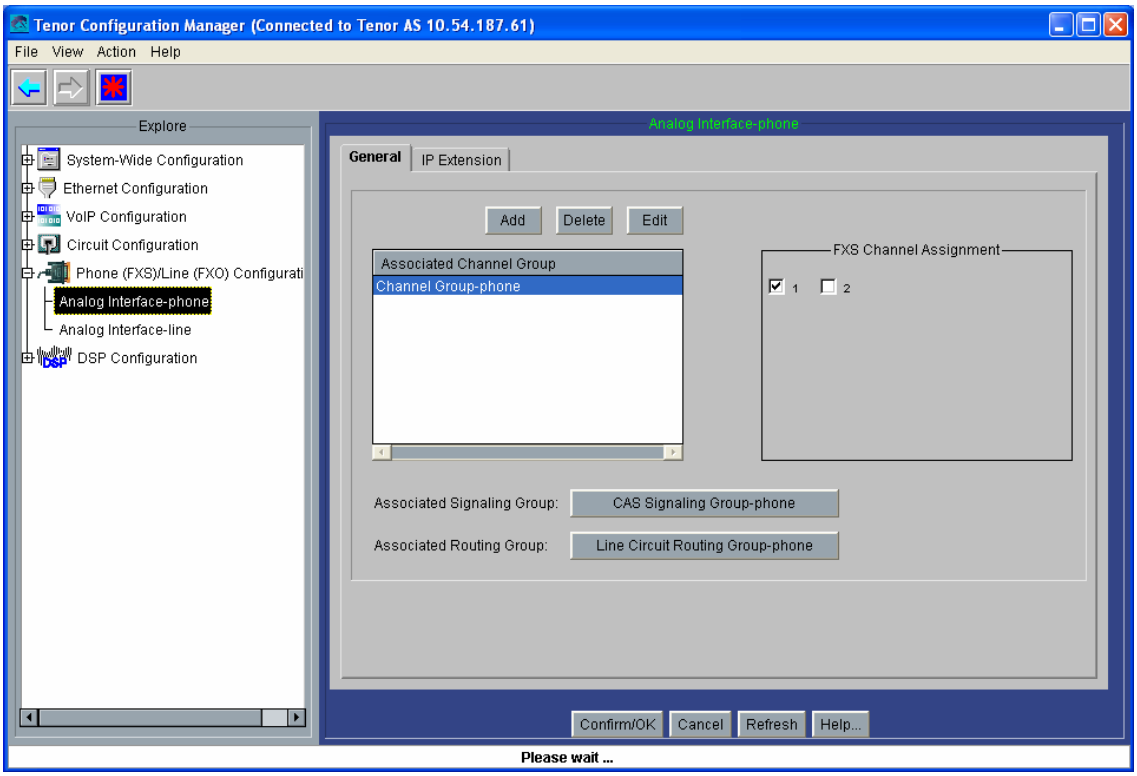


Figura 61: Captura 21 del *Tenor Configuration Manager* para la plataforma del Barrio de las Letras.

Eso es todo. Se guarda la configuración (pulsando sobre el botón que muestra un asterisco rojo sobre fondo azul), y se resetea el equipo (en `Action`).

3.4.1.2 Quintum Tenor Gatekeeper

El Quintum Tenor Gatekeeper fue fabricado en una serie de equipos anterior a la nueva serie de pasarelas Quintum Tenor y no presenta ninguna interfaz visual, sino tan sólo su conexión telnet.

La versión del *firmware* que se usará en esta plataforma será la P4-2-20-40. El archivo que almacena este *firmware* puede encontrarse en la documentación adjunta, carpeta `Archivos Adjuntos\Quintum Technologies\Version del software AS-AX-GK\Gatekeeper-P4-2-20-40`, archivo `tg-sy-p4-2-20-40qt-lec.bin`, así como las instrucciones para su carga en el archivo `Software_Loading_Instructions_10-2001.pdf` de la misma carpeta.

La configuración necesaria para este Gatekeeper no pasa de configurar su IP por cable serie, usando así en todo el resto de los parámetros de configuración (que, por otro lado, tampoco son muchos) los que vienen por defecto. Al igual que antes se hizo con las pasarelas, puede hacerse uso del programa HyperTerminal de Windows en configuración (38400, 8-N-1, None), escribiendo (inicialmente, la contraseña está vacía), como se muestra en la figura 62:

```
Quintum:gatekeeper> Password: Thank you.  Type ? for help

Quintum:gatekeeper> config
config# unit 1
config unit 1# ip 10.54.187.60
config unit 1# name gatekeeper
config unit 1# print
Unit: 1
IP Address = 10.54.187.60
External IP Address = 0.0.0.0
Name = gatekeeper

config unit 1# exit
config unit# exit
config# syslan
config syslan# subnetmask 255.255.192.0
config syslan# print
Subnet Mask = 255.255.192.0
Default Gateway = 0.0.0.0
config syslan# exit
config# submit
config# exit
Quintum:gatekeeper> reset
Are you sure you wish to reset? (y/n) y
```

Figura 62: Configuración inicial del Gatekeeper para la plataforma del Barrio de las Letras

Tras la configuración e instalación del Gatekeeper con el resto de los terminales ASG200, puede hacerse una prueba de conectividad usando el comando `gk ep` en el Gatekeeper, el cual debe dar el siguiente resultado por pantalla (figura 63):

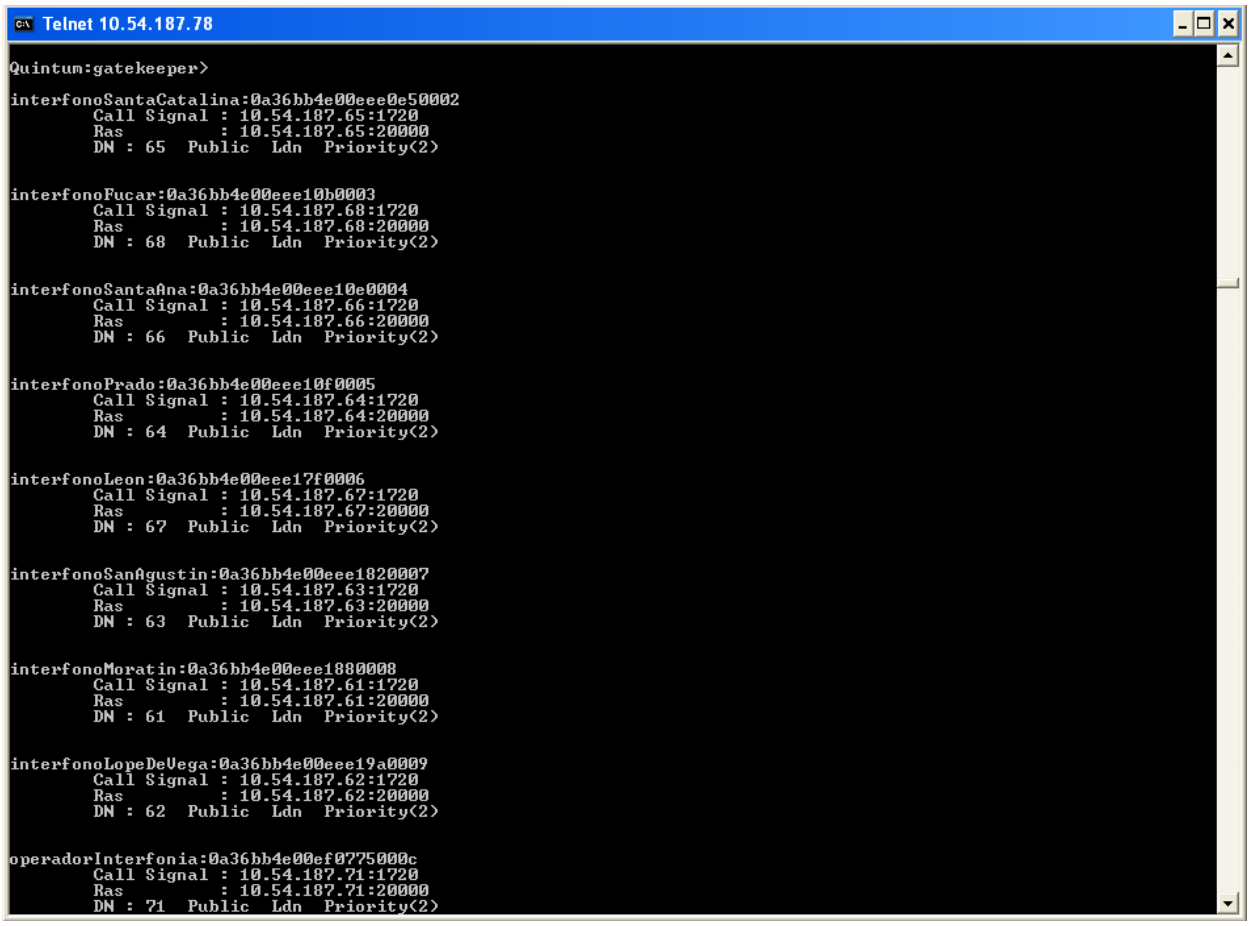


Figura 63: Prueba de conectividad en el Gatekeeper de la plataforma del Barrio de las Letras.

3.4.1.3 SJPhone

Este teléfono es software. Permite los protocolos H.323 y SIP. El único lenguaje disponible es el inglés.

Para la configuración del SJ Phone se utilizan perfiles; en el menú `Options`, ha de hacerse uso apenas sólo de la pestaña `Profiles` (perfiles) desde la cual puede editarse una configuración para cada uso (h323 con o sin Gatekeeper, sip con o sin proxy). Mediante el botón `Initialize...` se configura el número de teléfono a que se asociará este terminal en el Gatekeeper. `Account` y `Phone number` deberán almacenar el mismo valor para la interoperabilidad con el Gatekeeper de Quintum; en él, este número se almacenará como de tipo público. Este proceso se muestra en una captura de pantalla sobre la interfaz de este teléfono en ejecución (figura 64), al igual que se hará con el resto de modificaciones necesarias sobre la configuración por defecto de este teléfono:

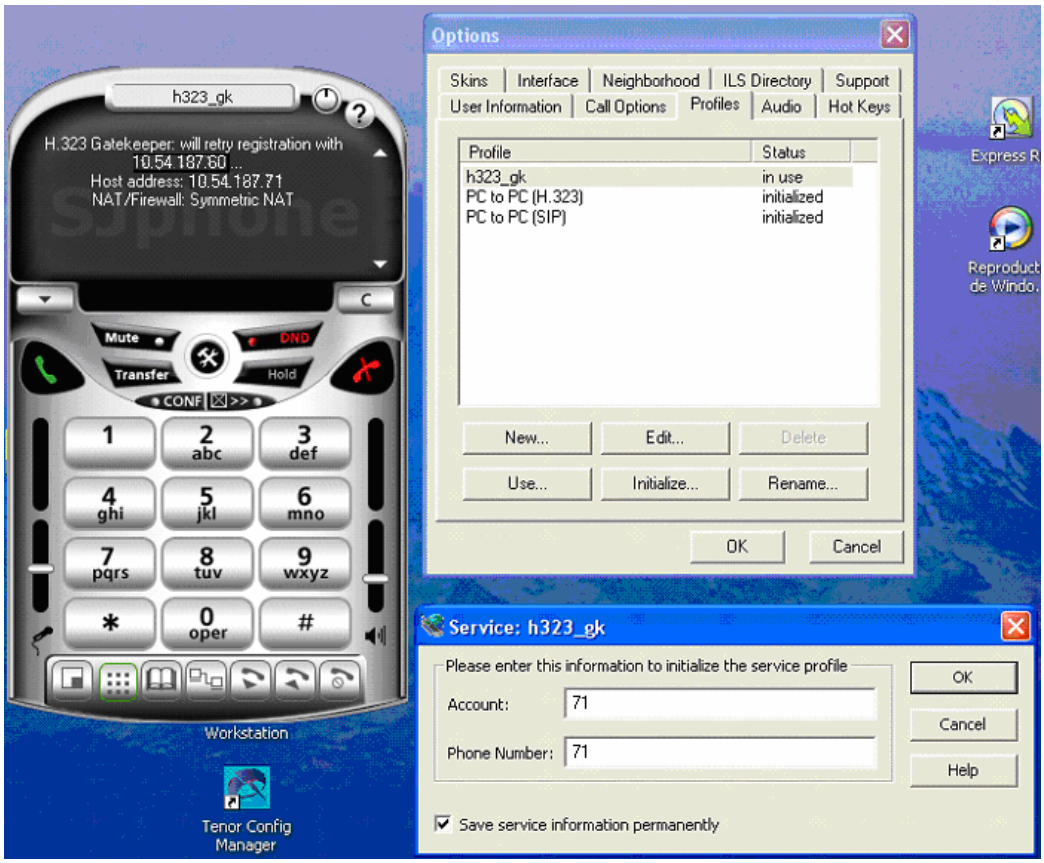


Figura 64: Configuración del número asociado al teléfono software SJPhone.

El resto de parámetros de configuración se editan en el botón `Edit...` En el submenú emergente hará falta modificar la configuración sobre tres pestañas fundamentales:

- `H.323 Gatekeeper` (figura 65): aquí se escribe la dirección IP del Gatekeeper que controlará este terminal. También puede usarse un LightweightRRQ (que funciona perfectamente con los Gatekeepers de Quintum).

- `H.245` (figura 66): En esta sección hay que deshabilitar todas las casillas: `Enable Fast-Start`, `Enable H.245 tunneling`, y `Early H.245`. Se resuelven de esta forma las condiciones de carrera asociadas a Fast Connect comentadas anteriormente.

- `Media Channels` (figura 67): Se habilitarán las casillas `Use remote codec preferences`, y `Open audio streams after remote opened`.

A continuación se muestran las capturas de pantalla que contienen la configuración de este teléfono (figuras 65, 66 y 67):

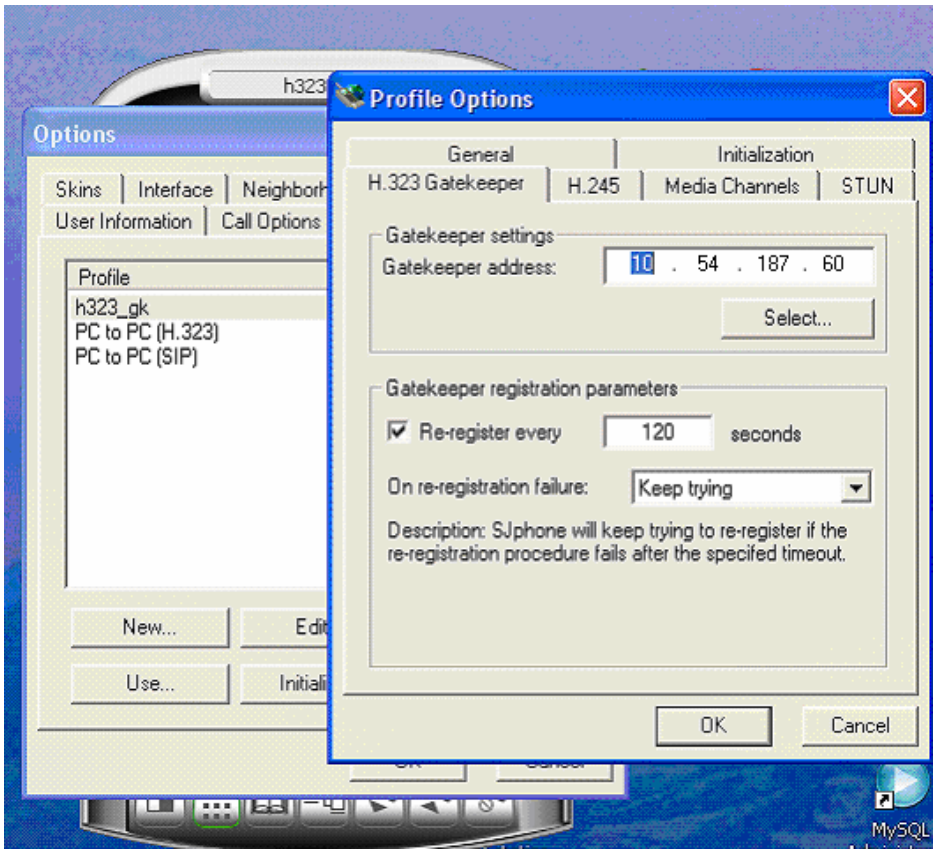


Figura 65: Configuración de parámetros H.323 en el teléfono software SJPhone.

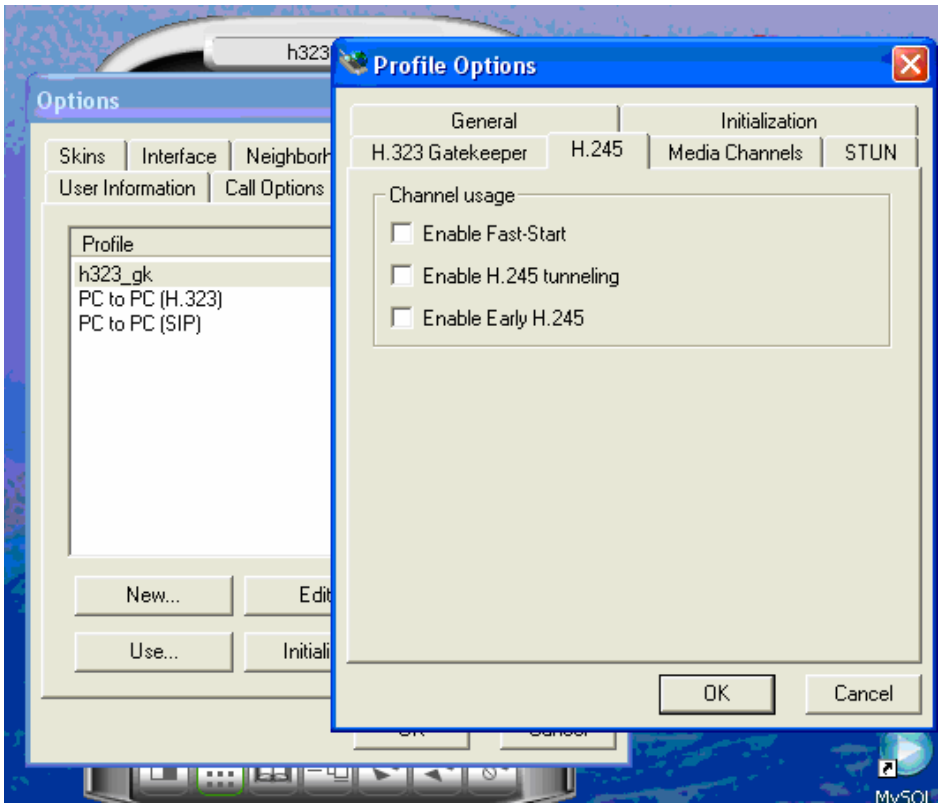


Figura 66: Configuración de parámetros H.245 en el teléfono software SJPhone.

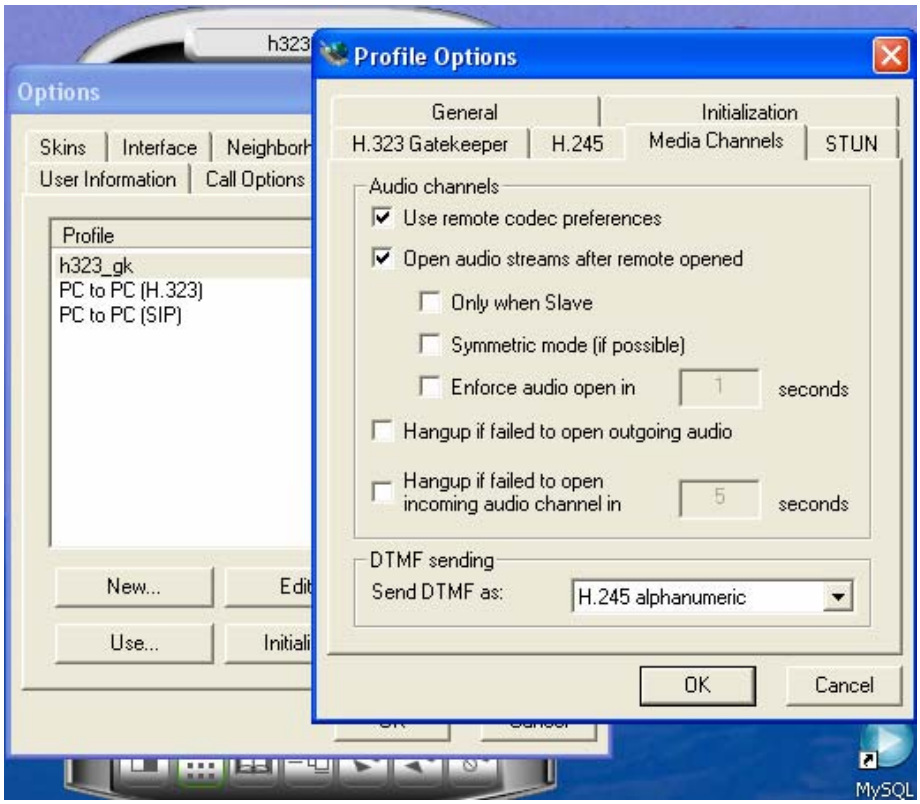


Figura 67: Configuración de parámetros de audio en el teléfono software SJPhone.

3.4.1.4 Interfonos

La configuración de los interfonos analógicos Viking 1600A se realiza mediante transmisión de tonos DTMF en banda durante una comunicación con el mismo interfono. Para esta plataforma, tan sólo ha de programarse en cada uno de ellos el marcado de la extensión destino 71. Al poseer el SJPhone la capacidad de mantener llamadas en espera, no será necesario nada más.

Para ello, hay que efectuar una llamada contra ellos y, una vez conectados, marcar el código de seguridad (por defecto el 845464), y programar el primer número llamado (con la secuencia 71#00).

3.4.2 Plataforma Estación de Bailén

A continuación, se muestra la configuración de cada uno de los terminales implicados en la plataforma.

3.4.2.1 Pasarelas Quintum Tenor AXG800

La versión del *firmware* usada en estas pasarelas es la P102-11-08 (tal y como en las pasarelas ASG200 de la plataforma del Barrio de las Letras). Hay distintos *firmware*s de la misma versión para cada equipo; en realidad, este *firmware* sólo es importante a efectos de uso del *Tenor Configuration Manager* adecuado. Este firmware se incluye en la documentación adjunta, en la carpeta `Archivos Adjuntos\Quintum Technologies\Version del software AS-AX-GK\AS_AX-P102-11-08\AX`.

La configuración inicial de estas pasarelas se realiza, como antes, mediante conexión por puerto serie. Con el HyperTerminal (38400 bps, 8 bits de datos sin paridad, 1 bit de parada, y sin control de flujo), se establecerá una conexión inicial al Quintum Tenor, con usuario/contraseña admin/admin, y escribiendo (se muestra a continuación, en la figura 68, lo que aparece en pantalla, con comentarios entre corchetes):

```
Quintum# eth
Quintum-EthernetInterface-SL1DV1EI1# config
config-EthernetInterface-SL1DV1EI1# set sm [y ahora la máscara de subred
deseada] 255.255.0.0
config-EthernetInterface-SL1DV1EI1* set ipa [y la dirección ip del equipo]
10.13.108.1
config-EthernetInterface-SL1DV1EI1* siprd
config-StaticIPRouteDir-1* change 1 g [y ahora la pasarela por defecto:
este parámetro debe pertenecer necesariamente a la subred del equipo,
aunque bien puede no ser utilizado nunca] 10.13.108.254

  StaticIPRoute Table

  index   Destination   NetMask   Gateway         EIAttached    Metric
  -----   -----------   -------   ------------    ------------  ------
  1       0.0.0.0       0.0.0.0   10.13.108.254   EI-SL1DV1EI1  1

config-StaticIPRouteDir-1* submit
config-StaticIPRouteDir-1# main
maintain-StaticIPRouteDir-1# mc
maintain-MasterChassis-1# reset
Are you sure that you want to reset the MasterChassis (Yes/No)? yes
```

Figura 68: Configuración inicial de las pasarelas AXG800 para la plataforma de la Estación de Bailén

Se establecen así los parámetros básicos necesarios para la conexión con la red IP de estas pasarelas.

A continuación se mostrará la configuración de los equipos, al igual que en la plataforma anterior, mediante capturas de pantalla sobre el *Tenor Configuration Manager*. Sólo se mostrarán las capturas de pantalla realizadas sobre la pasarela 10.13.108.2, comentándose las modificaciones que en concreto tendrían lugar al configurar la otra pasarela que, por lo demás, quedará igual. En este caso, se comentarán los parámetros de configuración con mucha menor profundidad que para la plataforma anterior (pues coinciden en su mayor parte).

Tras entrar en la configuración del equipo (con *Login* admin, *Password* admin), se comenzará por configurar el plan de marcado: sin prefijos públicos (figura 69), con el prefijo `Intercom` a uno, (el resto de los prefijos no tienen importancia en este caso), y longitud de la numeración privada a tres (notar que todo esto sólo tiene relevancia en llamadas salientes), (figura 70):

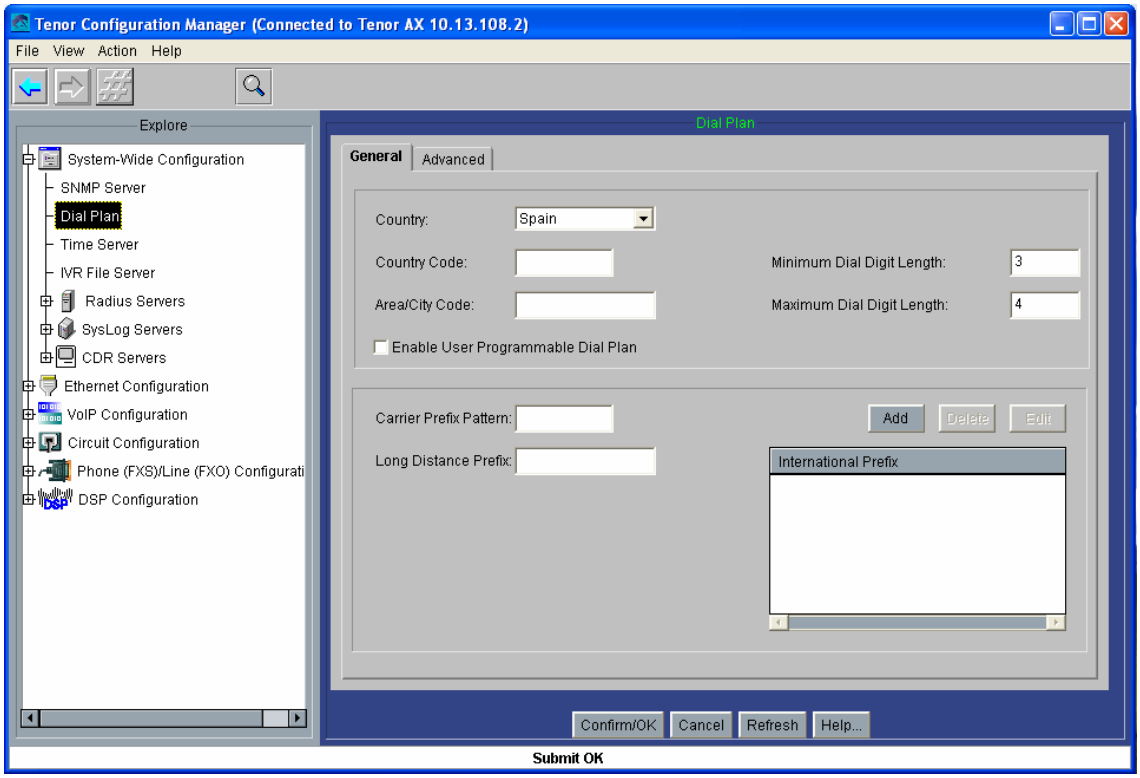


Figura 69: Captura 1 del *Tenor Configuration Manager* para la Plataforma de Interfonía Estación de Bailén.

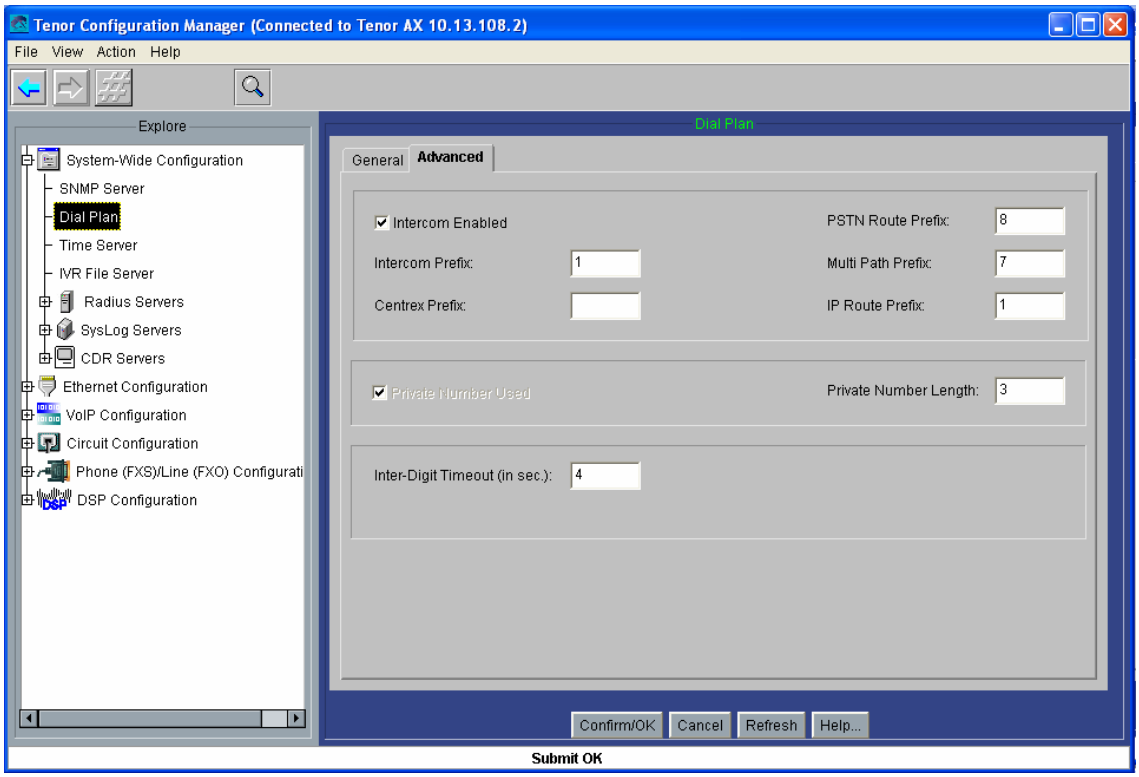


Figura 70: Captura 2 del *Tenor Configuration Manager* para la Plataforma de Interfonía Estación de Bailén.

A continuación se configuran los parámetros H.323 (figuras 71 y 72); para la pasarela 10.13.108.1 debe cambiarse el H323ID por Bailen1:

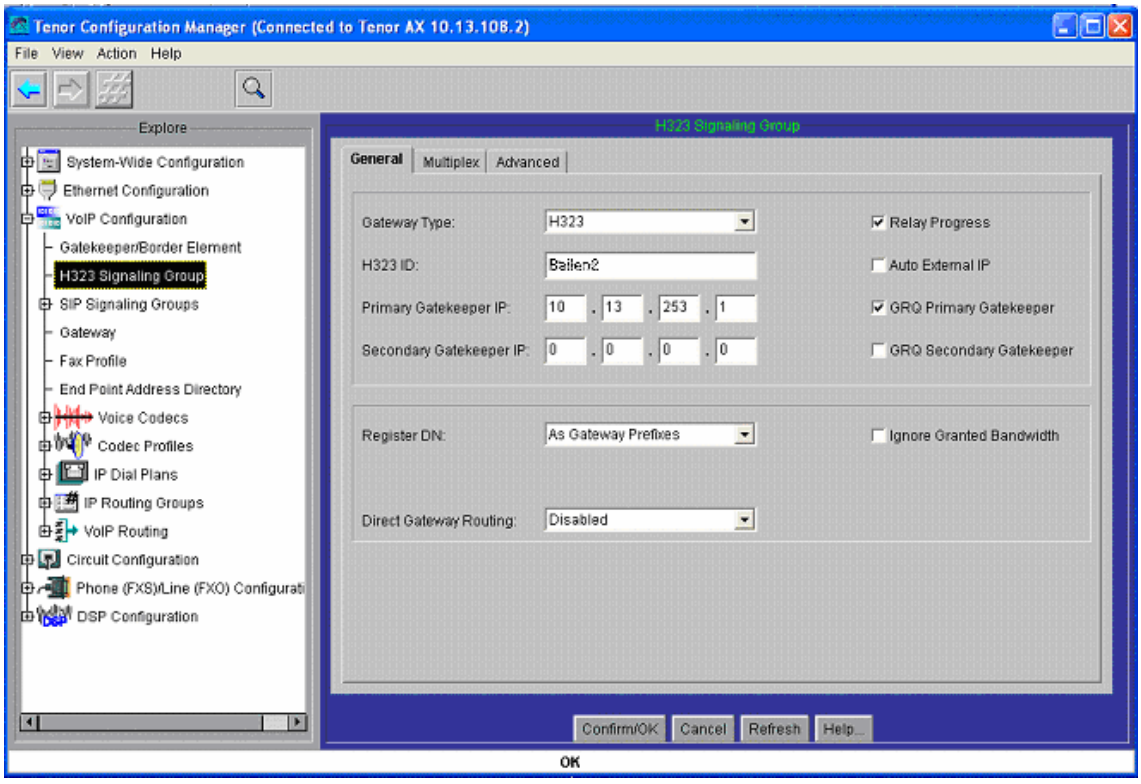


Figura 71: Captura 3 del *Tenor Configuration Manager* para la Plataforma de Interfonía Estación de Bailén.

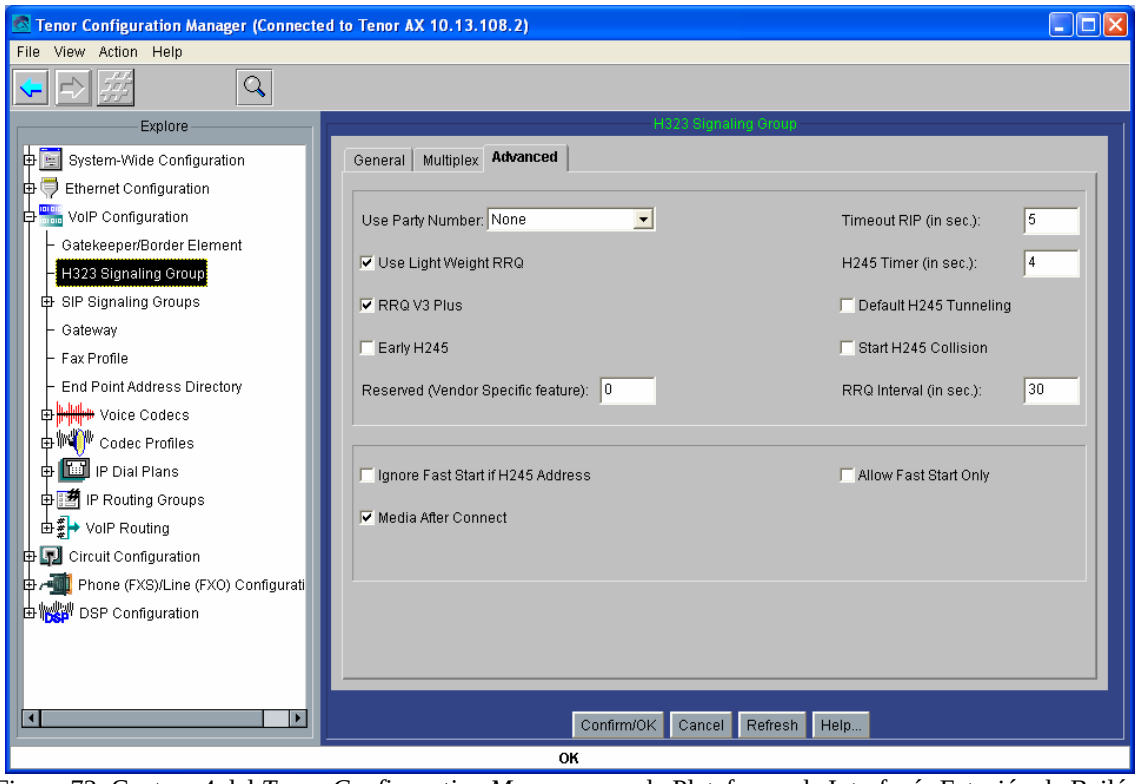


Figura 72: Captura 4 del *Tenor Configuration Manager* para la Plataforma de Interfonía Estación de Bailén.

Se establece a continuación el códec para las pasarelas: El `Voice Codec-1` se establecerá al G.711 Mu-law (figura 73); y se dejará asociado al `Codec Profile` (que luego se asociará al *IP Routing Group*), como se muestra en la figura 74:

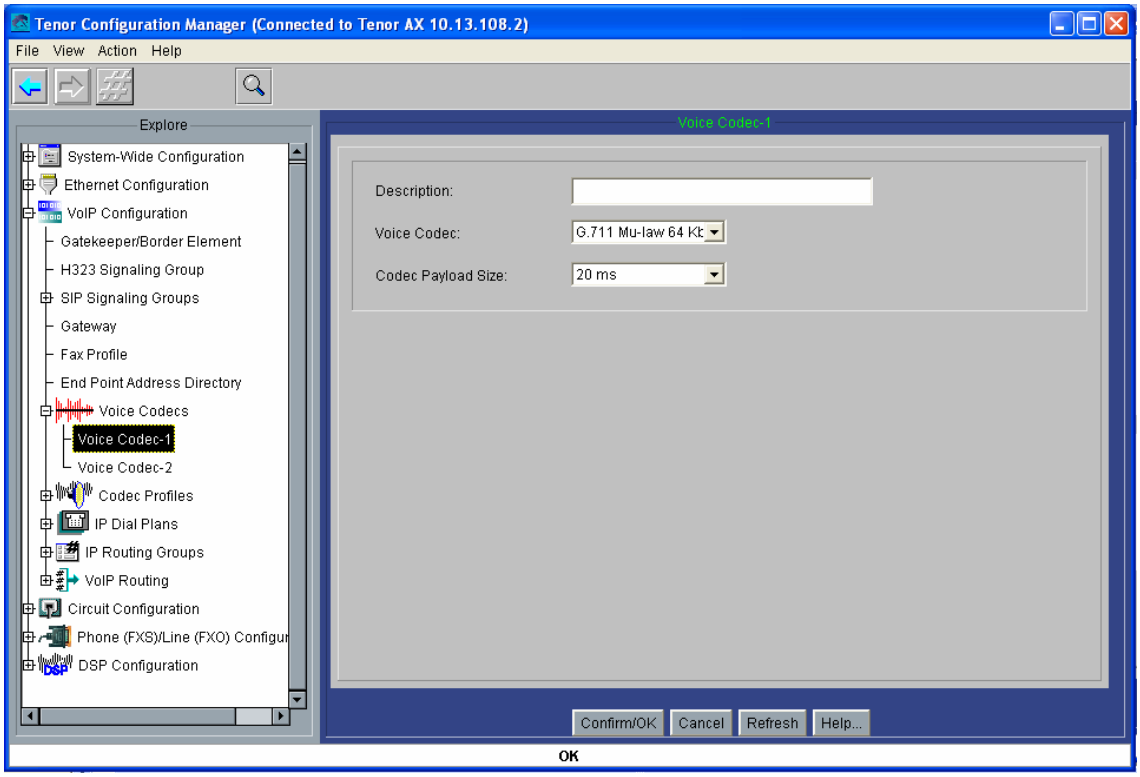


Figura 73: Captura 5 del *Tenor Configuration Manager* para la Plataforma de Interfonía Estación de Bailén.

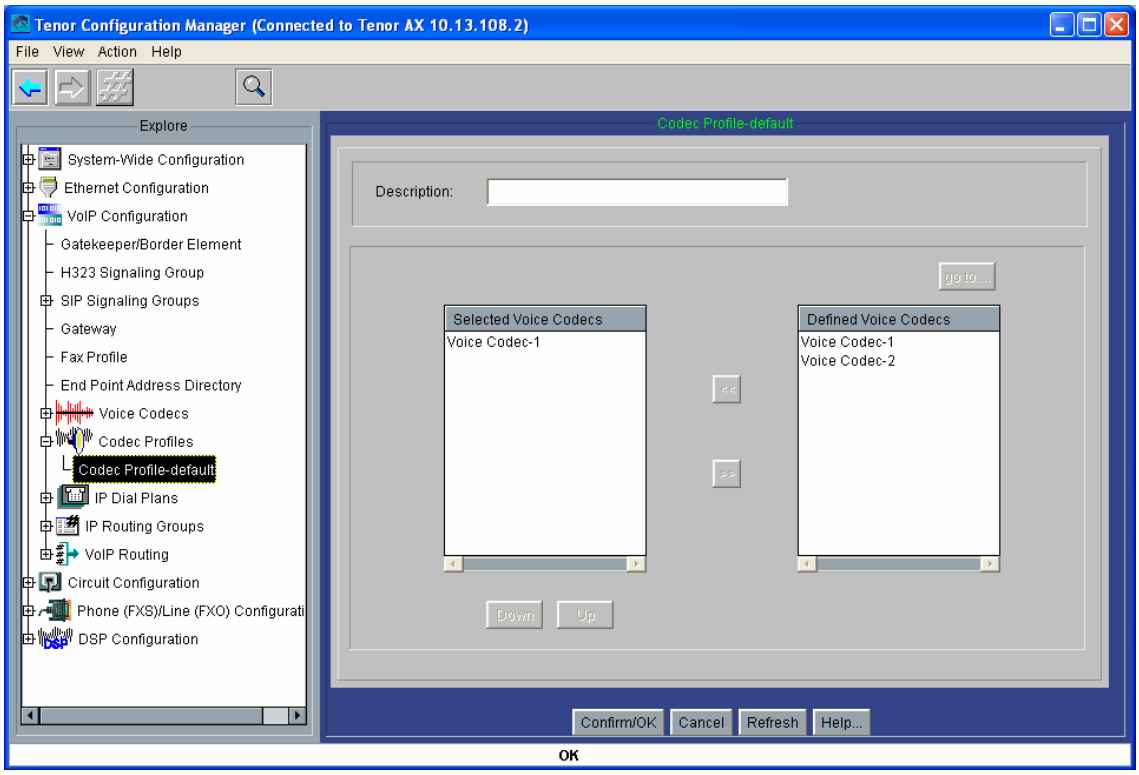


Figura 74: Captura 6 del *Tenor Configuration Manager* para la Plataforma de Interfonía Estación de Bailén.

A continuación se da paso a la configuración los grupos de rutas IP, como se explicó anteriormente poniendo el `Outgoing IP Prefix` a 1 (figura 75). En este apartado también se limitará el tiempo máximo de conversación a 10 minutos (figura 76), y el tiempo de establecimiento TCP a 5 segundos (figura 77).

Otro buen detalle es la deshabilitación el parámetro `Inband Tone` (figura 77), crucial para que los interfonos reciban la información de tonos de ocupado o de llamada recibida (que luego se traducirá a analógico) para su correcta operación. Como se verá más adelante, estos interfonos presentan la capacidad de volver a marcar en el caso de que la llamada no haya tenido éxito. Esta capacidad será usada en la plataforma para conmutar las llamadas de uno a otro operador en el caso de que alguno de ellos no responda o se encuentre ocupado. Si no se habilitase este parámetro, la comunicación con el interfono sería tratada desde la pasarela (no puede olvidarse que es la pasarela quien señaliza al interfono del progreso de la llamada) como una llamada activa desde el mismo inicio de las comunicaciones, transmitiéndose los tonos de llamada o de ocupado sobre un *path* de voz activo (en banda), e impidiendo así su recepción por parte del interfono.

Por último, se deshabilita el *Fast Connect* H.323 (`Disable Fast Start`) para las llamadas salientes (figura 77 también):

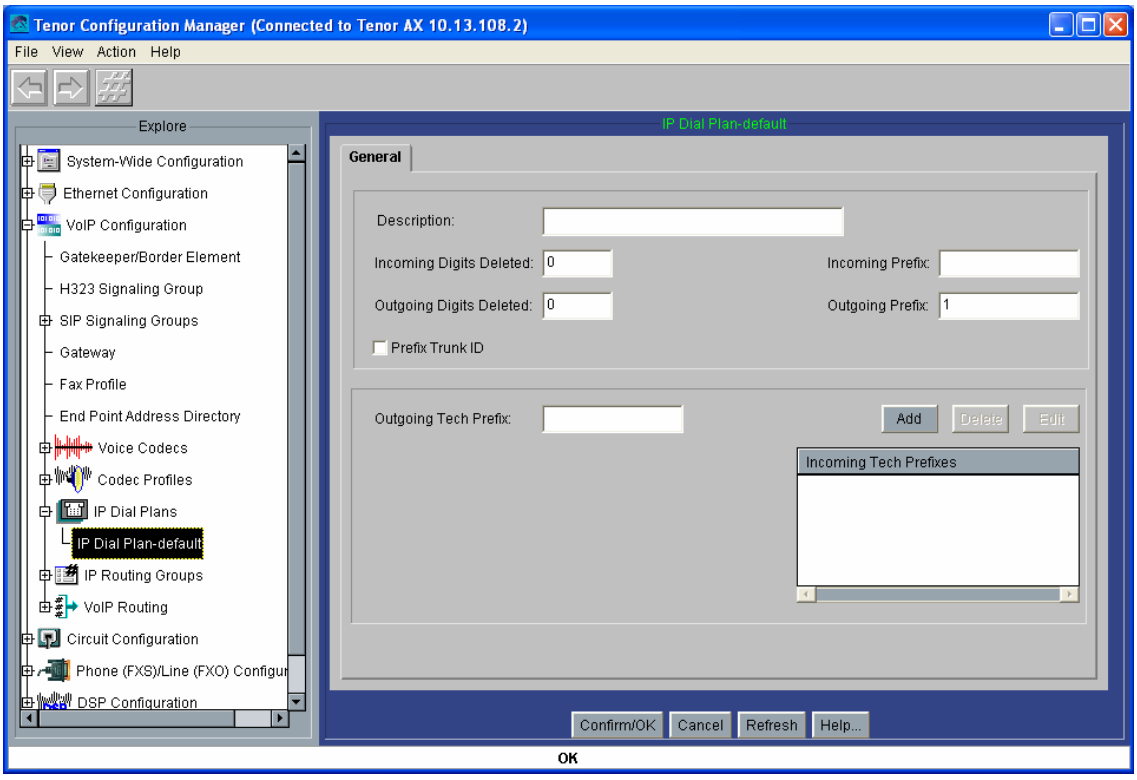


Figura 75: Captura 7 del *Tenor Configuration Manager* para la Plataforma de Interfonía Estación de Bailén.

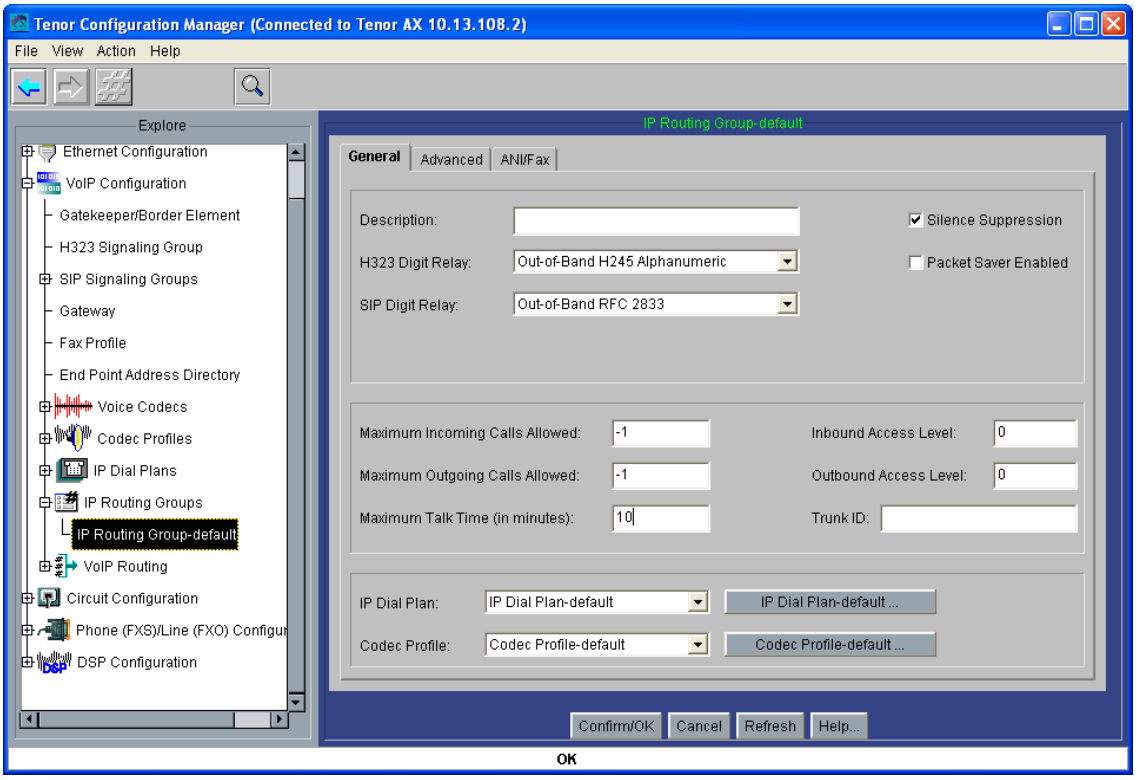


Figura 76: Captura 8 del *Tenor Configuration Manager* para la Plataforma de Interfonía Estación de Bailén.

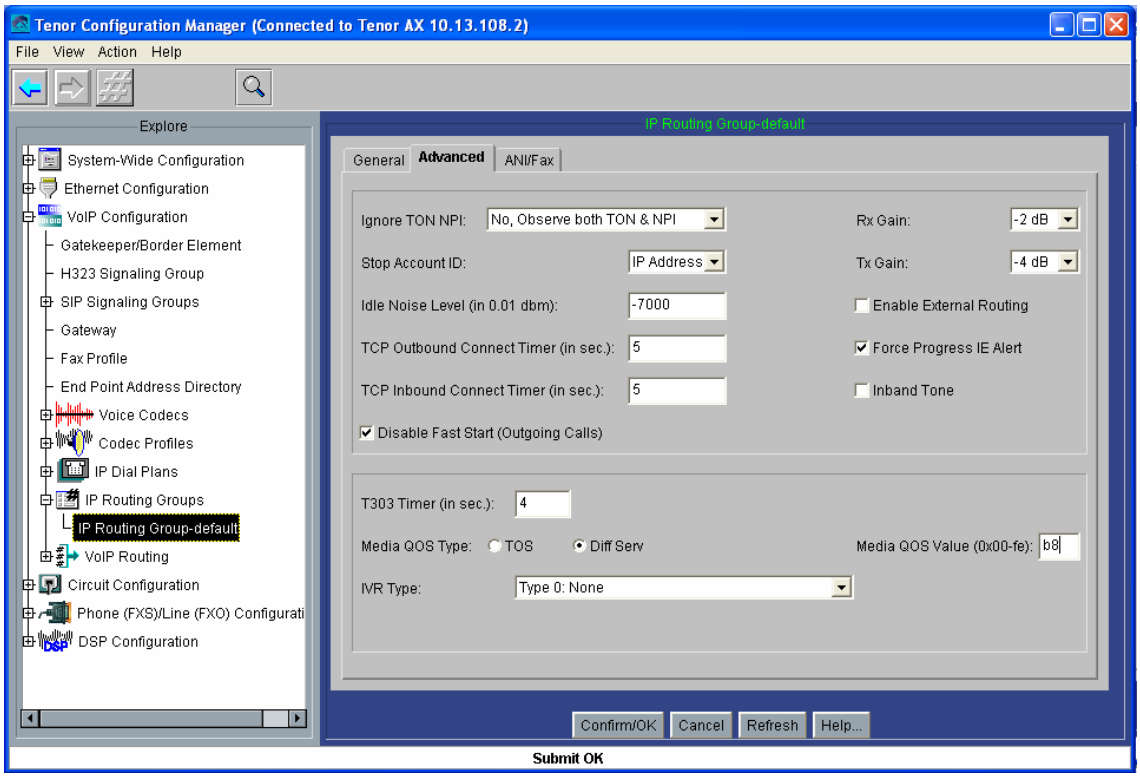


Figura 77: Captura 9 del *Tenor Configuration Manager* para la Plataforma de Interfonía Estación de Bailén.

Se muestra a continuación la configuración de las líneas analógicas con las figuras 78, 79 y 80, de manera similar a la configuración utilizada en la plataforma del Barrio de las Letras: se establece el tipo de señalización (parámetro `Signaling Type`) a `Loop Start Forward Disconnect` (figura 78); también se activa la generación FSK[47] del número llamante (para la recepción de ese número por parte del Alcatel Temporis 45) y se activa la supervisión de la desconexión `Disconnect Supervision` (figura 79); y se selecciona la plantilla de tono de llamada en la zona para España (`Line Template`), con una impedancia estándar de 600 Ω (parámetro `Impedance`) (todo esto, para la correcta comunicación analógica con los interfonos), en la figura 80:

[47] FSK: *Frecuency Shift Keying*, modulación digital por desplazamiento de frecuencia, muy común en para la detección del número llamante en los teléfonos analógicos, en parte debido a su sencillez.

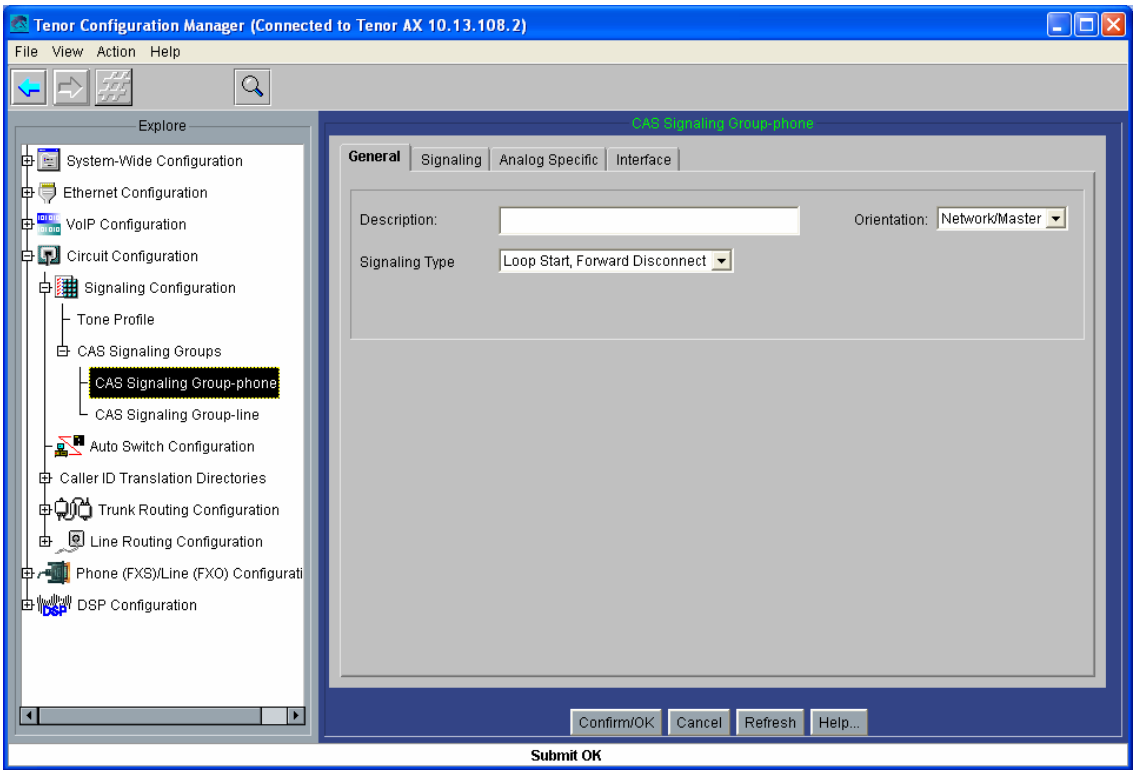


Figura 78: Captura 10 del *Tenor Configuration Manager* para la Plataforma de Interfonía Estación de Bailén.

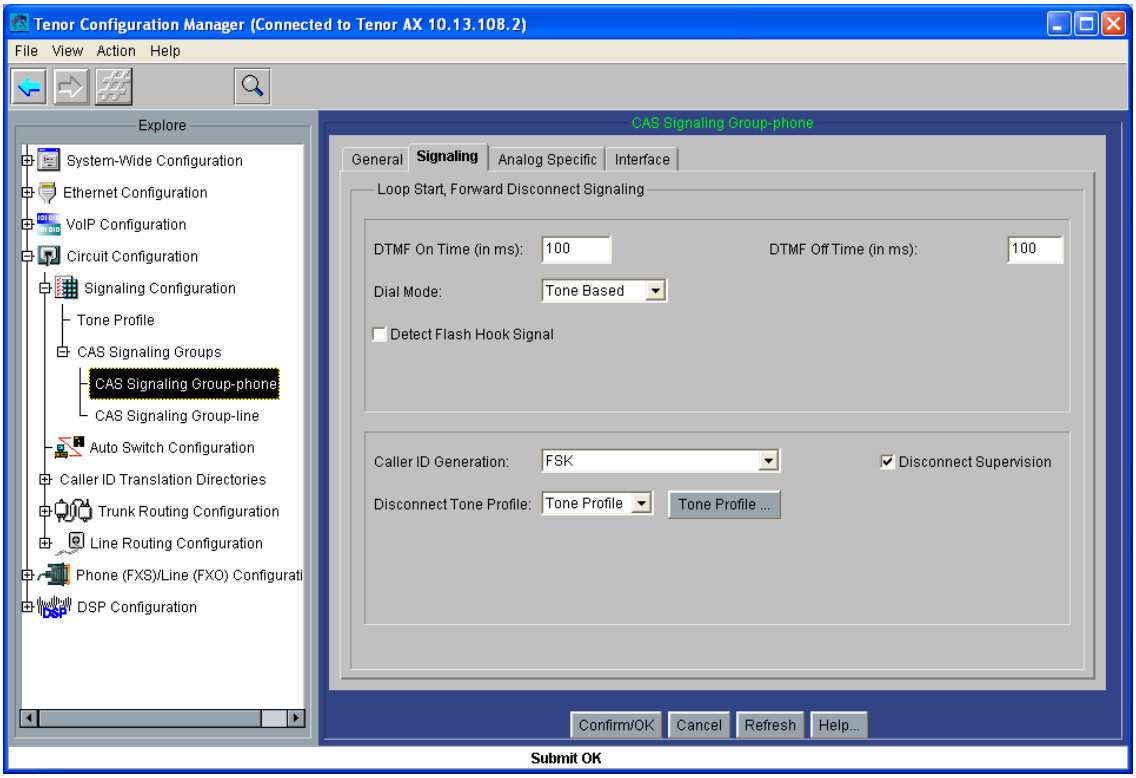


Figura 79: Captura 11 del *Tenor Configuration Manager* para la Plataforma de Interfonía Estación de Bailén.

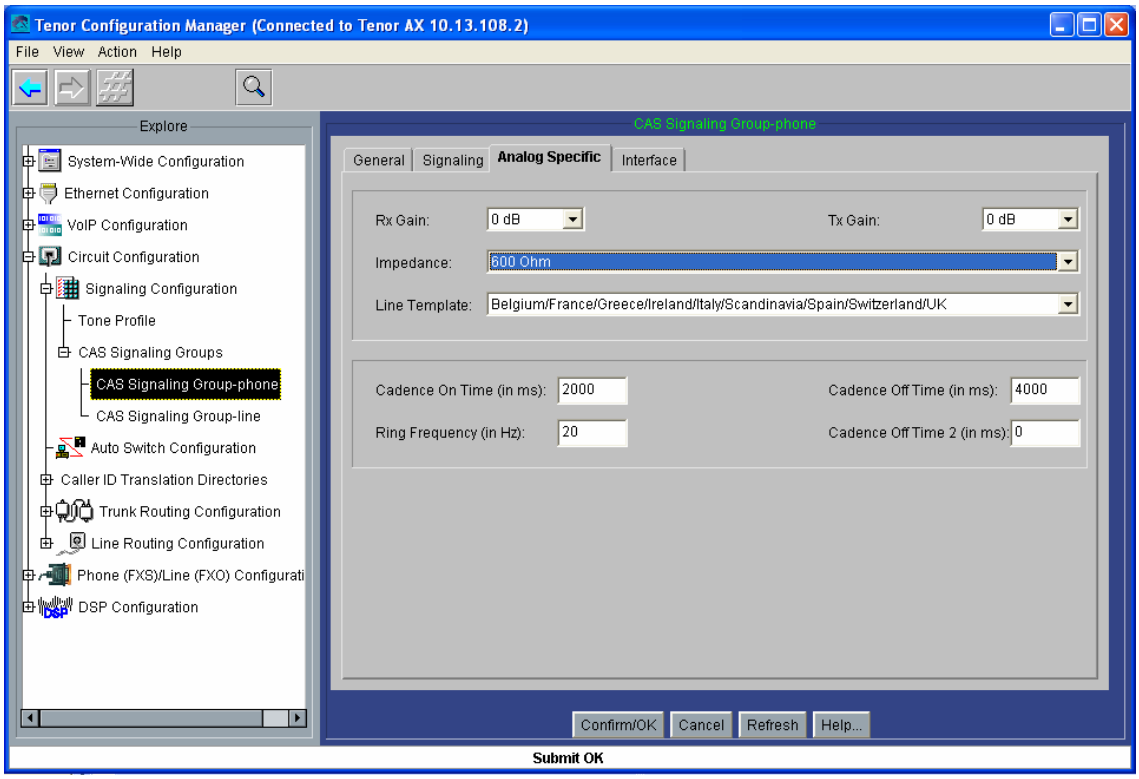


Figura 80: Captura 12 del *Tenor Configuration Manager* para la Plataforma de Interfonía Estación de Bailén.

Se pasa a continuación al establecimiento de los números HuntLDN que cazarán cada uno de los puertos analógicos a los que se conectarán los terminales analógicos: Como se estudió en el apartado de diseño, en el AXG800 1 se han de configurar los números 1000, 1001, 1002, 1003, 1004, 1005, 1006 y 1007 públicos y privados, y los 000, 001, 002, 003, 004, 005, 006 y 007 privados; en el AXG800 2, 1010, 1011, 1012, 1013, 1014, 1015, 1016 y 1017 públicos y privados, y 010, 011, 012, 013, 014, 015, 016 y 017 privados. Estos números se configurarán en grupos en función del tipo de numeración pública o privada, de forma que posteriormente se le asociará cada grupo a una interfaz FXS distinta; por lo tanto, han de crearse 16 grupos (directorios) en total, para que luego se le asocie un grupo público y otro privado a cada interfaz. Los nombres de estos directorios HuntLDN son pub"i" para los públicos y prv"i" para los privados.

A continuación se muestran sólo los dos HuntLDNs correspondientes al puerto 1 de la segunda pasarela, que deberá llevar asociados los números 1010 y 010 privados (figura 82) y 1010 público (figura 81):

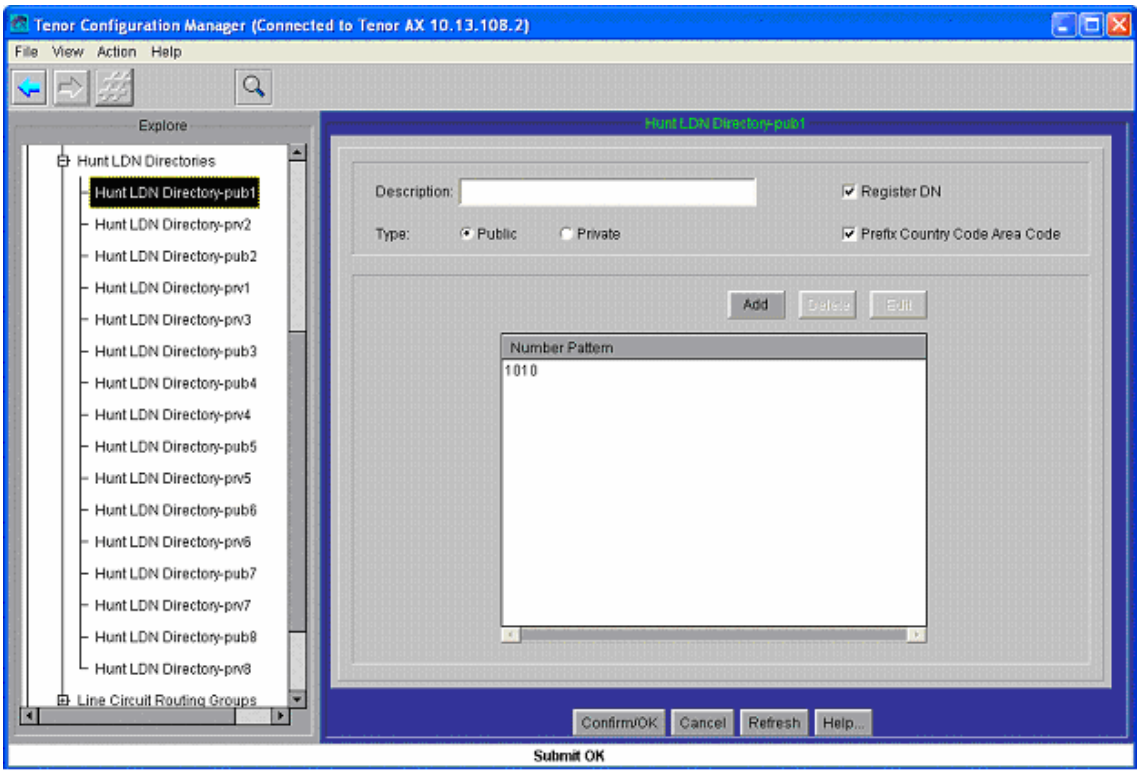


Figura 81: Captura 13 del *Tenor Configuration Manager* para la Plataforma de Interfonía Estación de Bailén.

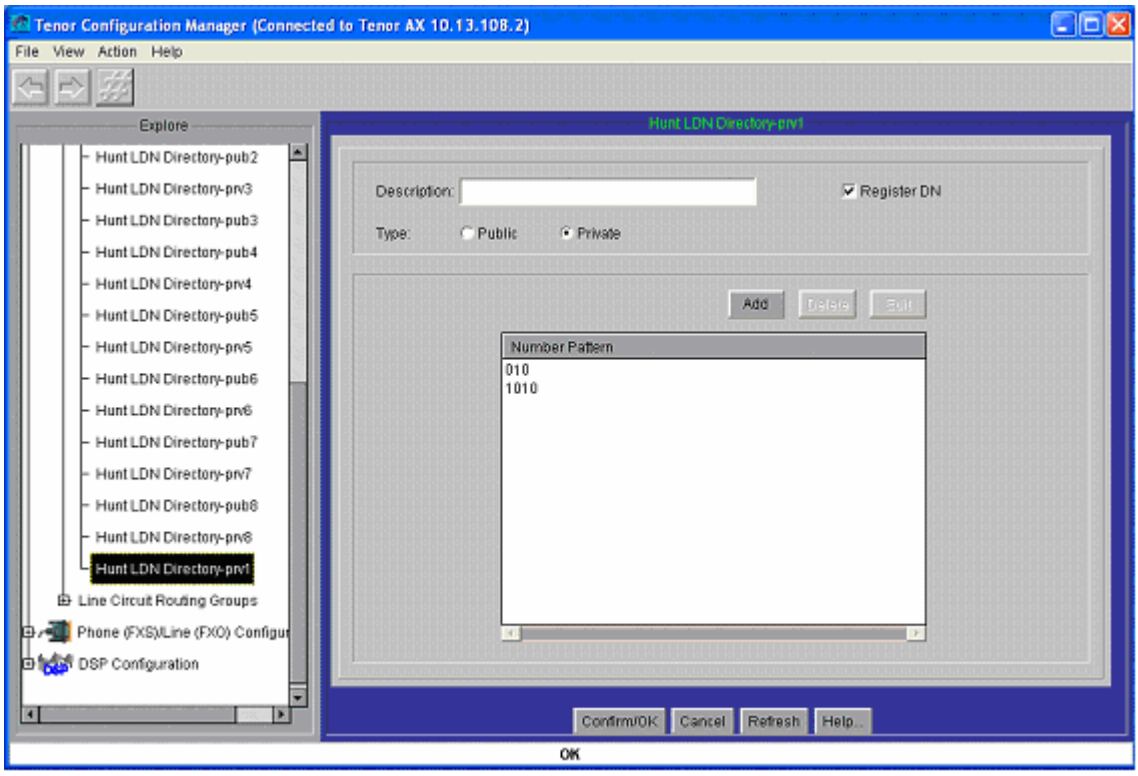


Figura 82: Captura 14 del *Tenor Configuration Manager* para la Plataforma de Interfonía Estación de Bailén.

Ahora hay que configurar los LCRGs (grupos de rutas por circuitos) asociados a cada puerto FXS (analógico): se crearán ocho LCRGs independientes (llamados *Line Circuit Routing*

Group – phone "i"), todos con la misma configuración excepto por el `TrunkID` (que se usará como número llamante) y los HuntLDN (los números asociados a cada puerto) usados: se muestra sólo la configuración del LCRG correspondiente al primer puerto del AXG800 2 (figuras 83-87), teniendo que cambiar los `TrunkID` a 1010, 1011, 1012, 1013, 1014, 1015, 1016 y 1017, en el resto de LCRGs del AXG800 2, y a 1000, 1001, 1002, 1003, 1004, 1005, 1006 y 1007 en cada LCRG del AXG800 1. También se asignan los directorios HuntLDN (prv"i" para los números privados, y pub"i" para los números públicos) a cada *Line Circuit Routing Group – phone* "i" (figura 86), como se explicó anteriormente.

También se selecciona en este apartado el número de cifras asociado a cada tipo de numeración (esto se refiere al número máximo de cifras para llamadas entrantes, en el rutado por circuitos): 4 para público, y 3 para privado (figura 85):

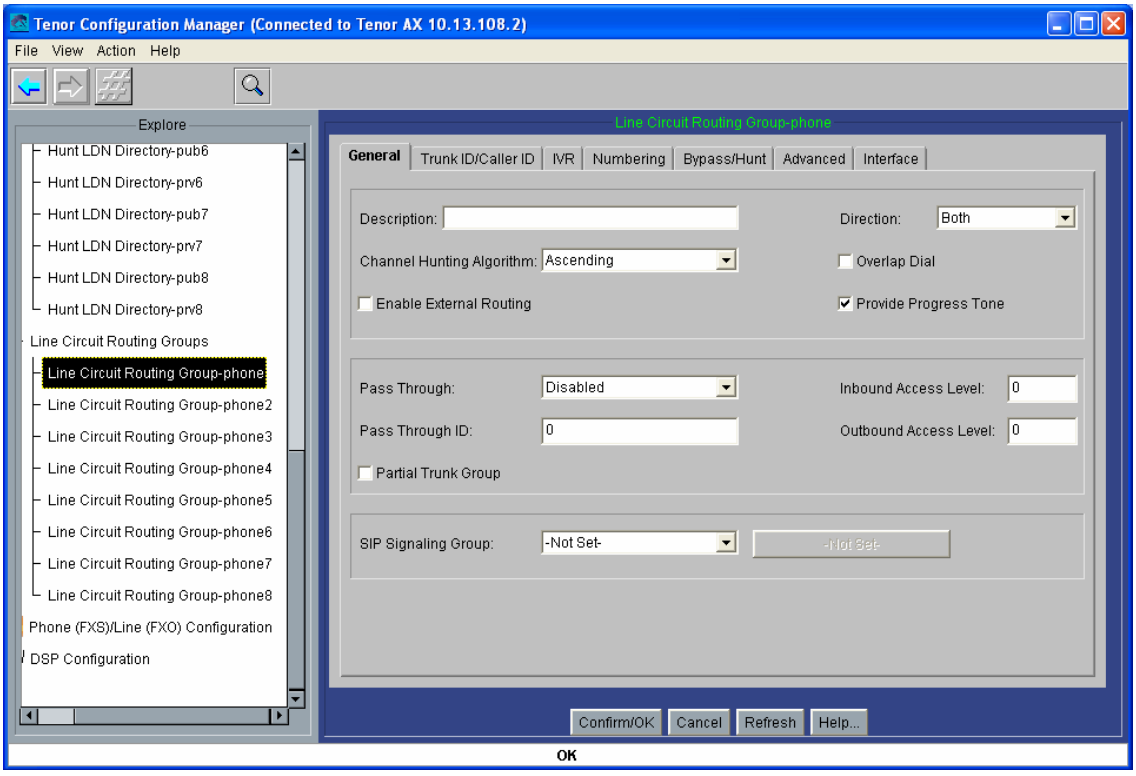


Figura 83: Captura 15 del *Tenor Configuration Manager* para la Plataforma de Interfonía Estación de Bailén.

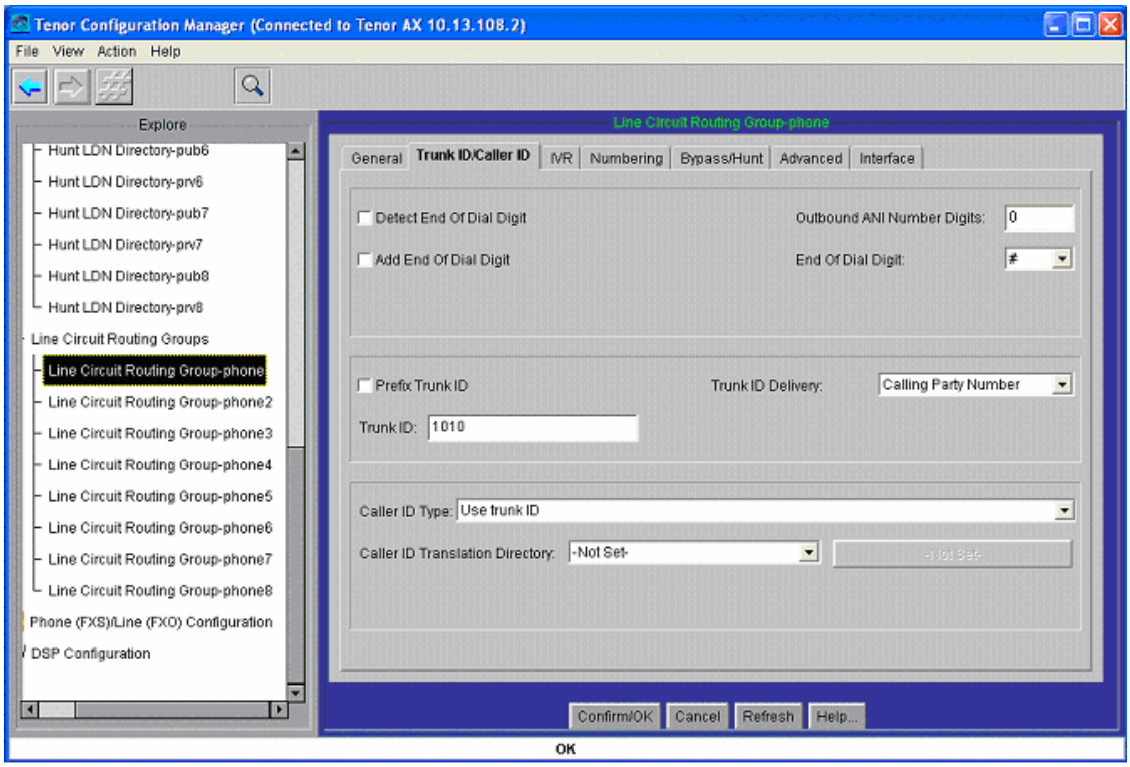


Figura 84: Captura 16 del *Tenor Configuration Manager* para la Plataforma de Interfonía Estación de Bailén.

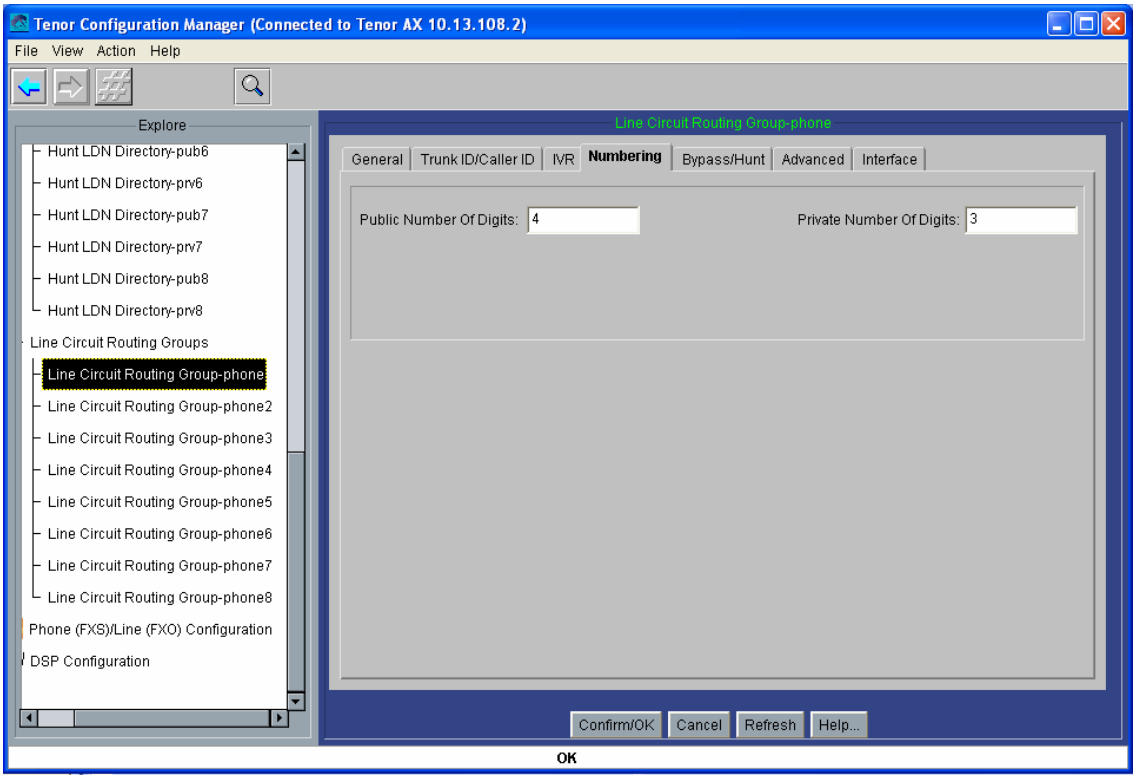


Figura 85: Captura 17 del *Tenor Configuration Manager* para la Plataforma de Interfonía Estación de Bailén.

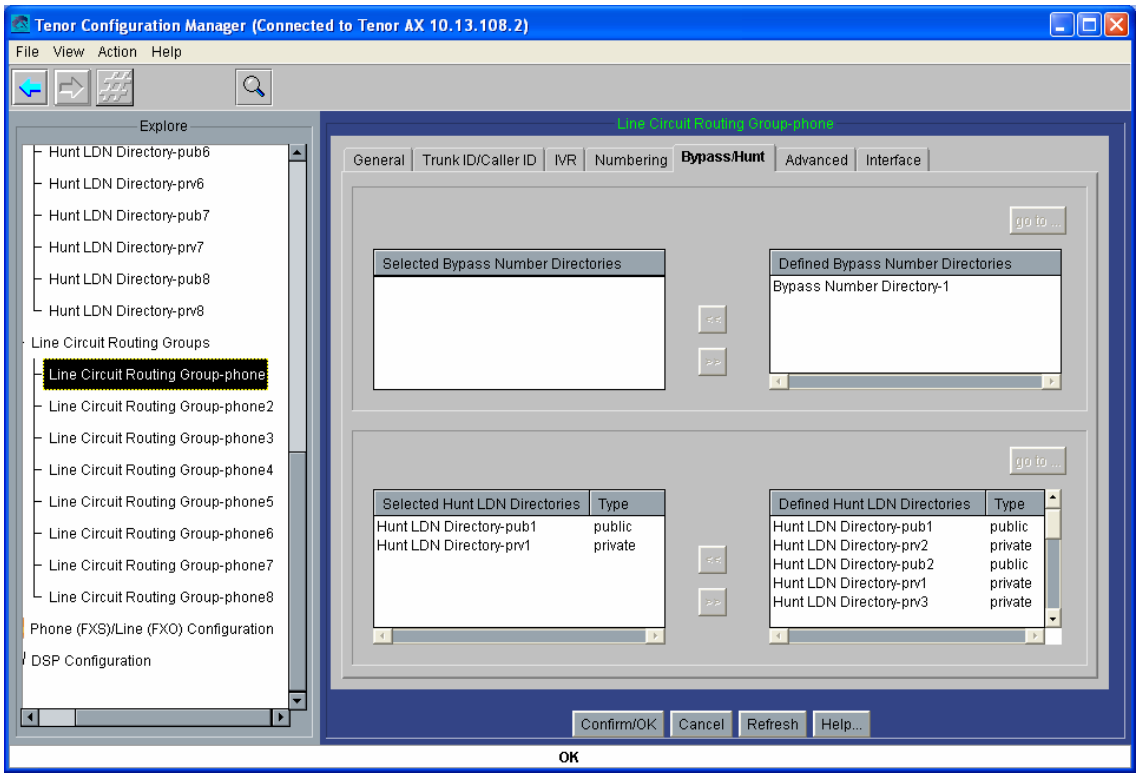


Figura 86: Captura 18 del *Tenor Configuration Manager* para la Plataforma de Interfonía Estación de Bailén.

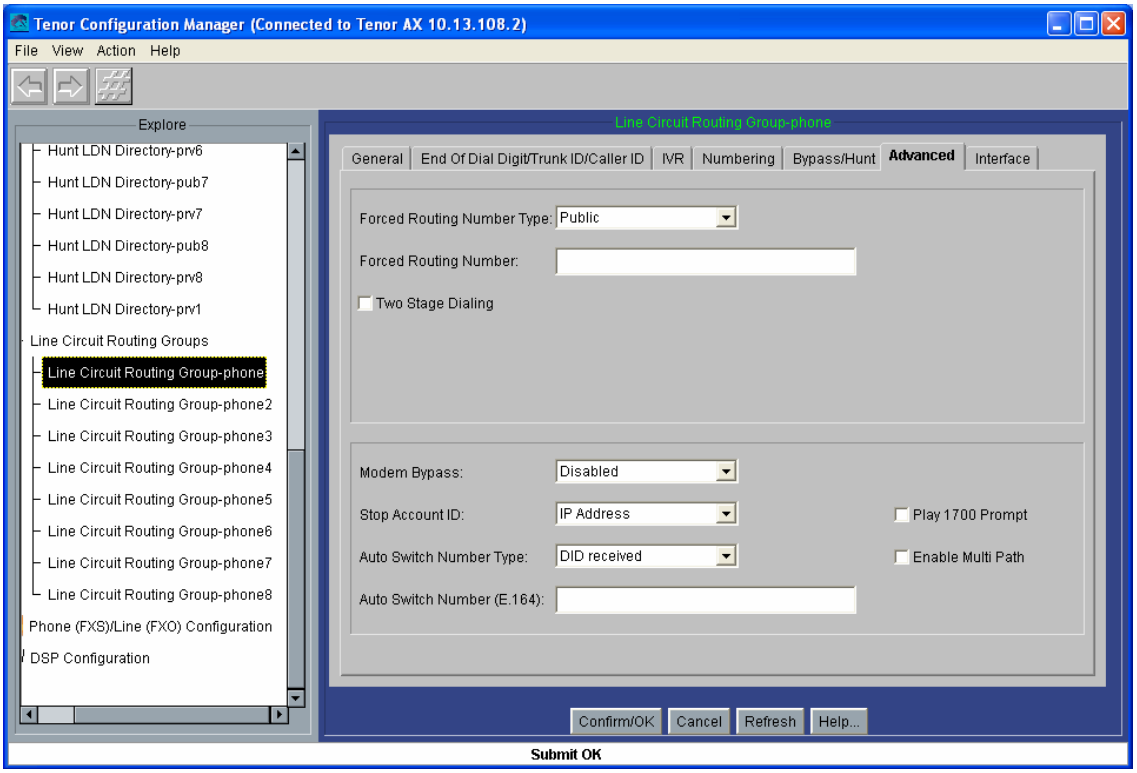


Figura 87: Captura 19 del *Tenor Configuration Manager* para la Plataforma de Interfonía Estación de Bailén.

Para finalizar, se crearán ocho grupos de canales, a cada uno de los cuales se le asocia un canal analógico, el mismo *CAS Signaling Group* y uno de los LCRG creados anteriormente:

a continuación se muestra cómo se crea el grupo 7, y cómo queda el grupo 3, de la pasarela 2 (figuras 88 y 89):

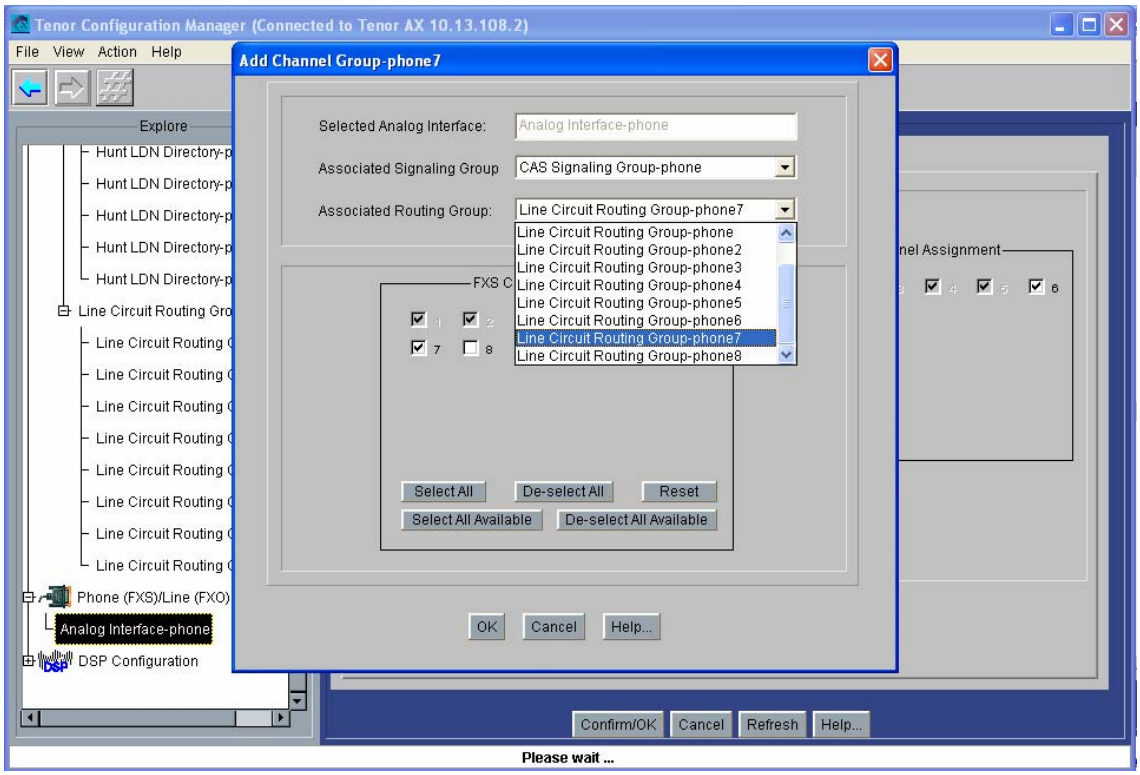


Figura 88: Captura 20 del *Tenor Configuration Manager* para la Plataforma de Interfonía Estación de Bailén.

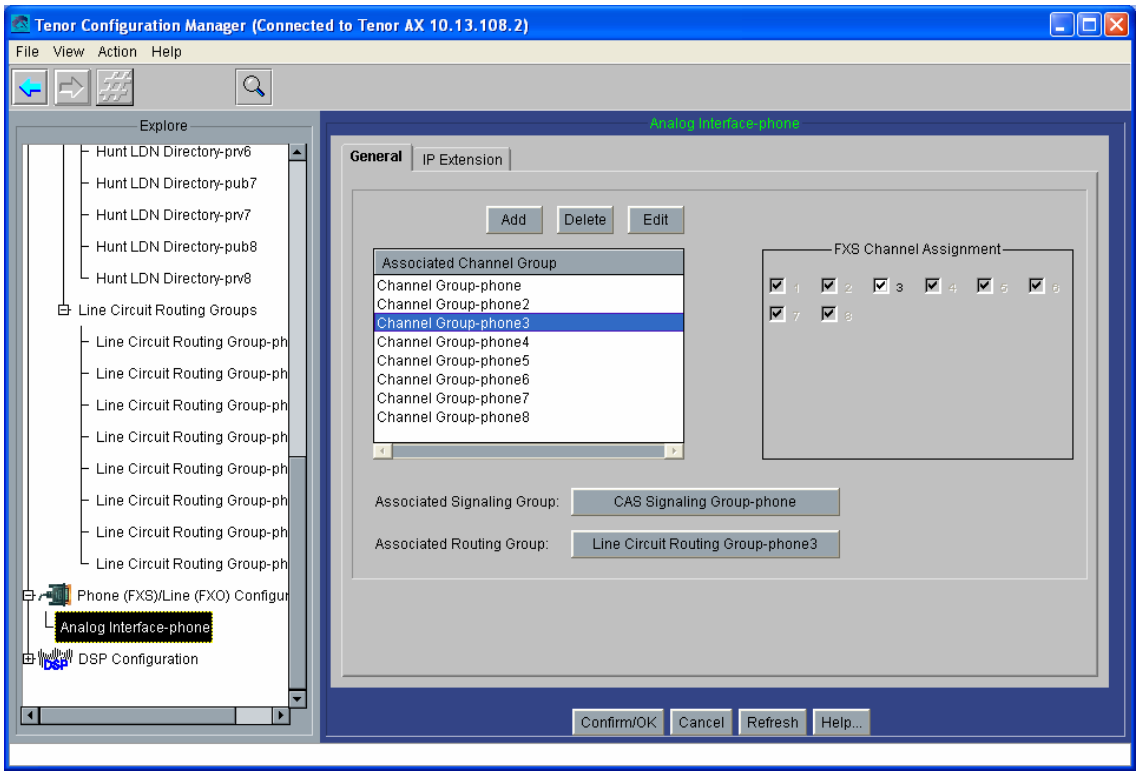


Figura 89: Captura 21 del *Tenor Configuration Manager* para la Plataforma de Interfonía Estación de Bailén.

Al igual que antes, guardar (en el botón con el asterisco en rojo sobre fondo azul), y resetear (en `Action`).

3.4.2.2 Cisco 7905G

Se trata del teléfono VoIP más pequeño de la gama de Cisco Systems que permite H.323. También permite SIP. Entre sus capacidades, se encuentran la posibilidad de uso de SNMP y DHCP y DiffServ, y la posibilidad de especificar de un plan de marcado (para reducir el retardo tras el marcado), además de las típicas posibilidades de un teléfono autónomo VoIP. Permite los códecs G.711 A y Mu, y G.729A. El único lenguaje permitido en la interfaz es el inglés.

La configuración debe cargarse mediante archivos de configuración, personalizados para cada MAC, que se transmiten con un servidor TFTP cada vez que arrancan estos teléfonos. Por cierto, que este teléfono tarda menos de un minuto en arrancar, (reseñable en comparación con el minuto que tardaba el teléfono IP Micronet 5100SP y los casi cinco minutos que requería en teléfono IP Telkus Totalfon IP5000).

Un detalle interesante a remarcar sobre este teléfono es que, al adquirirlo, son necesarios no sólo el terminal, sino también la batería (porque este terminal soporta POE *Power Over Ethernet*, lo cual debe ser suministrado por los switches) y la licencia (que contiene los archivos de configuración del terminal). Esto incrementa ampliamente su coste (en torno a un 50% sobre el precio del terminal aislado).

Para la configuración del Cisco 7905G, es necesario el uso de un servidor TFTP. Para cada protocolo VoIP (SIP o H.323) se precisan archivos de licencia distintos: éstos se cargarán con la configuración cuando sea necesario (es decir, en la migración de un protocolo a otro). Entre los archivos adjuntos se incluye un servidor TFTP, (además de DHCP y NTP): el tftpd32, freeware (carpeta `Archivos Adjuntos\Varios\Servidor DHCP y TFTP`, archivo `tftpd32.280.zip`). También se adjuntan los manuales de este teléfono, en el archivo `7905_H323.pdf` (y `sip_config_7905g.pdf`, para la configuración bajo SIP).

El archivo de configuración se edita en un fichero de texto; luego, la herramienta cfgfmt.exe convertirá, mediante el filtro ptag.dat, este fichero de texto en uno de configuración. El filtro sirve para diferenciar el protocolo que se desea cargar en el teléfono: se dispone de los filtros `h323_ptag.dat`, y el `sip_ptag.dat`, con la misma licencia. El archivo de configuración puede llamarse `ldxxxxxxxxxxxx`, donde `xxxxxxxxxxxx` es la MAC, en hexadecimal, del teléfono IP, o bien `lddefault.cfg`, por defecto. El teléfono, al encenderse, tratará de descargarse primero su `ldxxx…xx`, y si no lo encuentra buscará el fichero `lddefault.cfg`, en el directorio raíz del servidor TFTP. Todos estos ficheros se adjuntan también en la documentación (carpeta `Archivos Adjuntos\Cisco 7905G`).

En el fichero de texto de configuración puede definirse la carga de un nuevo archivo de aplicación (*firmware*): si se cambia de protocolo, al igual que si es la primera vez que se carga la configuración en un teléfono de éstos, es necesario incluir, además de este archivo de configuración, en el directorio del servidor TFTP, el archivo de aplicación. En este caso, para estas plataformas se adquirieron las licencias que se guardan en los archivos

`CP7905010301SIP050608A.sbin` (para SIP) y `CP7905010002H323040927A.sbin` (para H.323). Todos estos archivos y programas se adjuntan en la documentación.
En definitiva, toda la configuración del teléfono se almacenará en el archivo de texto cargado mediante el servidor TFTP. También pueden modificarse algunos parámetros sobre el mismo teléfono, a mano, lo cual resulta muy útil para configurar la IP y el servidor TFTP antes de acceder a los archivos de configuración.

También puede cambiarse la configuración mediante interfaz web (bastante robusta, por cierto); pero, de cualquier forma, para la configuración inicial es necesario el proceso TFTP.

El archivo de texto necesario para usar este teléfono en esta plataforma queda como se muestra a continuación (figura 90):

```
#txt
# la linea anterior es fundamental para que la herramienta cfgfmt.exe
#compile este archivo
# aparte de aquella, las lineas que comienzan por “#” se ignoran: son
comentarios

UIPassword:revenga
# con esto se configura la contrasenia de configuracion

upgradecode:3,0x501,0x0400,0x0100,10.13.253.20,69,0x040927a,
CP7905010002H323040927A.zup
# esta linea es suficiente en caso de upgrade del firmware: en este
#upgrade, usara el servidor TFTP 10.13.253.20, y la licencia
#CP7905010002H323040927A.sbin

dhcp:0
# no se usará servidor DHCP

StaticIp:10.13.253.2
StaticRoute:10.13.253.254
StaticNetMask:255.255.0.0
# parametros IP

GkId:gatekeeper
Gk:10.13.253.1
AltGk:0
AltGkTimeOut:0
GkTimeToLive:300
# parametros de Gatekeeper

Gateway:0
# en el caso de que se desee configurar el telefono como gateway en el
#Gatekeeper

UID:1020
# extension asociada al telefono

LoginID:BailenPuestoMando
# H323ID

UseLoginID:1
# para trasmitir el H323ID en las comunicaciones H.323

RxCodec:2
```

```
TxCodec:2
# seleccion del Mu-Law

AudioMode:0x00230023
# con esto: g711 silence supression, use g711 codec only, dtmf in
#band, y dtmf hookflash deshabilitado, –permitiendo la configuracion
#de los interfonos desde este telefono.

NumTxFrames:2
# cada frame son 10 ms: 20 ms, coincidiendo con los Quintum (codec)

ConnectMode:00010100000000000001000000000000
# con esto, disable fast start, disable h245 tunn, send rrq when
#switch to alt gk, not enable callmanager, disable two-way cut-through
#of voice path before connect, y send ringback tone

Timezone:1
AutMethod:0
NTPIP:0.0.0.0
AltNTPIP:0.0.0.0
DNS1IP:0.0.0.0
DNS2IP:0.0.0.0
# no se usará ni NTP ni DNS

UseTftp:1
# tras la primera carga de configuracion y del firmware, esto puede
#volver a modificarse, impidiendo que el telefono intente conectarse
#al servidor TFTP cada vez que se encienda

EncryptKey:0
NPrintf:0
IPDialPlan:1
DialPlan:....t0
# con este plan de marcado se limita a 4 digitos la numeracion
#utilizada en este telefono, y tras marcar 4 cifras la transmision se
#procesa inmediatamente

RingOnOffTime:2,4,25
DialTone:2,31538,30831,3100,3885,1,0,0,1000
BusyTone:2,30467,28959,1191,1513,0,4000,4000,0
ReorderTone:2,30467,28959,1191,1513,0,2000,2000,0
RingBackTone:2,30831,30467,1943,2111,0,16000,32000,0
CallWaitTone:1,30831,0,5493,0,0,2400,2400,4800
AlertTone:1,30467,0,5970,0,0,480,480,1920
# configuraciones de los tonos

MediaPort:16384
TOS:0xb8
# se establece la posibilidad de usar DiffServ con prioridad 0xb8,
#para el caso de que los switches del sistema lo soporten

SigTimer:0x01418564
OpFlags:0x2
VLANSetting:0x0000002b
TraceFlags:0x00000000
```

Figura 90: Archivo de configuración del Cisco 7905G para la Plataforma de Interfonía Estación de Bailén

3.4.2.3 Quintum Tenor Gatekeeper

La configuración necesaria para este Gatekeeper comienza por configurar su IP por cable serie. Al igual que antes se hizo con las pasarelas, puede utilizarse el programa HyperTerminal de Windows en configuración (38400, 8-N-1, None); se muestra a continuación lo que parece por pantalla (figura 91); inicialmente, la contraseña está vacía:

```
Quintum:gatekeeper> Password: Thank you.  Type ? for help

Quintum:gatekeeper> config
config# unit 1
config unit 1# ip 10.13.253.1
config unit 1# name gatekeeper
config unit 1# print
Unit: 1
IP Address = 10.13.253.1
External IP Address = 0.0.0.0
Name = gatekeeper

config unit 1# exit
config unit# exit
config# syslan
config syslan# subnetmask 255.255.0.0
config syslan# print
Subnet Mask = 255.255.0.0
Default Gateway = 0.0.0.0
config syslan# exit
config# submit
config# exit
Quintum:gatekeeper> reset
Are you sure you wish to reset? (y/n) y
```

Figura 91: Configuración inicial del Gatekeeper para la plataforma de Interfonía Estación de Bailén.

En este caso, además de la configuración básica, hará falta permitir la interoperabilidad con el Cisco 7905G; como se introdujo en análisis del plan de numeración de esta plataforma, en el Gatekeeper este teléfono se registra con el número 1020 (tal y como se asignó en el plan de numeración) de tipo público (esto lo hace visible desde cualquier terminal genérico), pero que las pasarelas Quintum lo buscarán en el Gatekeeper como el 020 privado.

Para asignarle este número al Cisco 7905G en las tablas de numeración internas del Gatekeeper, ha de configurarse primero como *border element* del sistema, para luego establecer una ruta estática que relacione el número 020 privado con la dirección IP del Cisco 7905G. Como se comentó anteriormente, luego, con el parámetro `Outbound IP Prefix` de las pasarelas, este número se transformará en el 1020 cuando la petición de conexión entre en el propio Cisco.

Accediendo al Gatekeeper mediante una sesión de telnet, hay que acceder al submenú `config be`; aquí pueden verse las `sroutes` (*static routes*, rutas estáticas) ya configuradas mediante el comando `print`: éstas están numeradas. Para crear una ruta estática nueva, hay que hacer `sroute index`, y luego asignar la dirección de transporte (puerto TCP por defecto 1720), con `callsig ip#`, (donde `ip#` es la dirección IP del Cisco 7905G). A

continuación, se le añade el número al que va a asociarse en el *border element* esa IP: comando `dn index dn# type route priority`, donde:

- `index` es el número de directory number (dn) configurado en esta ruta estática. En la misma ruta estática se permiten varios dns.
- `dn#` es el número que se desea asociar a la ruta estática.
- El tipo `type` es 0 para establecer el número como público, y 1 para establecerlo como de tipo privado.
- route 0 es para seleccionar ldn *local directory number*, para números de teléfono con conexión en la red; y 1 es para lam, *leaky area number*, para los llamados *hopoffs*, es decir, para números cuya conmutación suponga salir de la red hacia, por ejemplo, la PSTN. En esta plataforma no hay salidas hacia la PSTN.
- `priority 2` es la prioridad normal, usada por defecto en todos los equipos Quintum.

Para activar el Gatekeeper como *border element* hay que entrar en el menú `gksys`, y escribir `border 10.13.253.1` (la dirección IP del *border element* deseado). Luego, en Gatekeepers adicionales, habrá que configurar este mismo *border element* (al que se accederá en el caso de desconocer algún número o dirección, mediante LRQs).

No olvidar hacer `submit` desde el directorio `config` para guardar la información configurada en el equipo.

La configuración completa se muestra en la siguiente captura de pantalla (figura 92), mediante el Telnet del programa Putty:

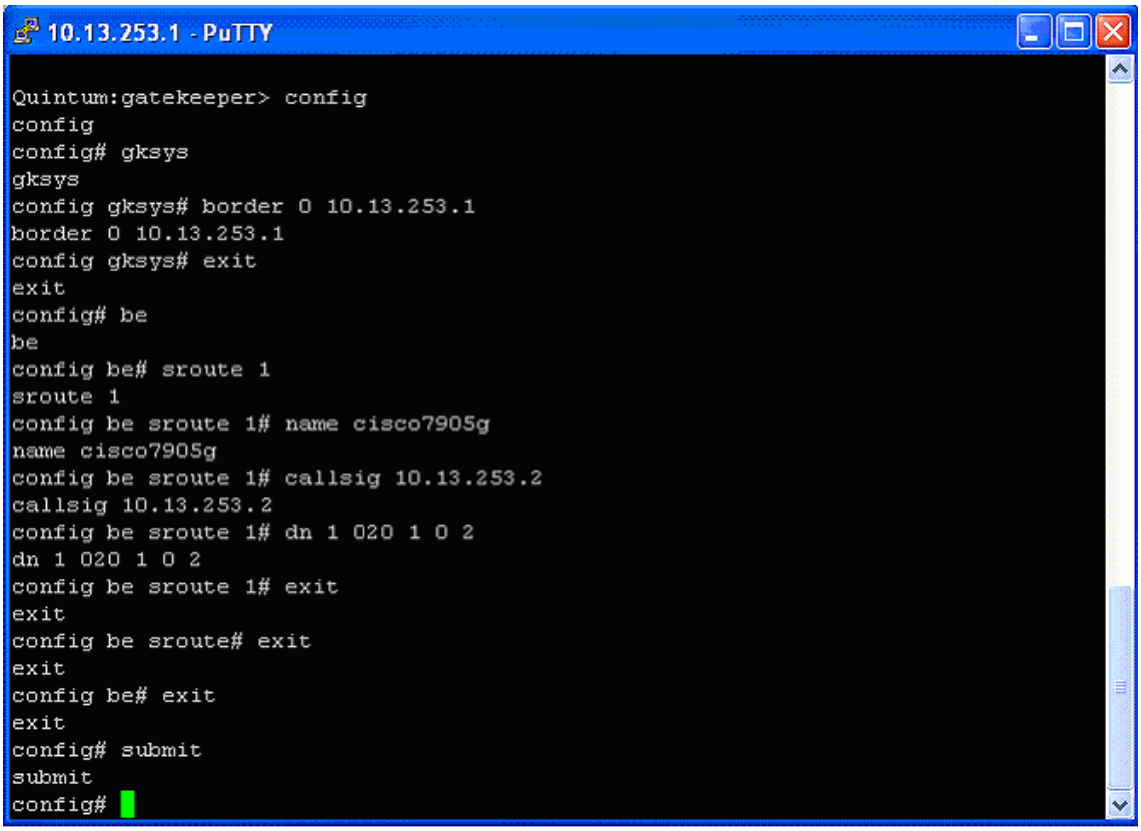
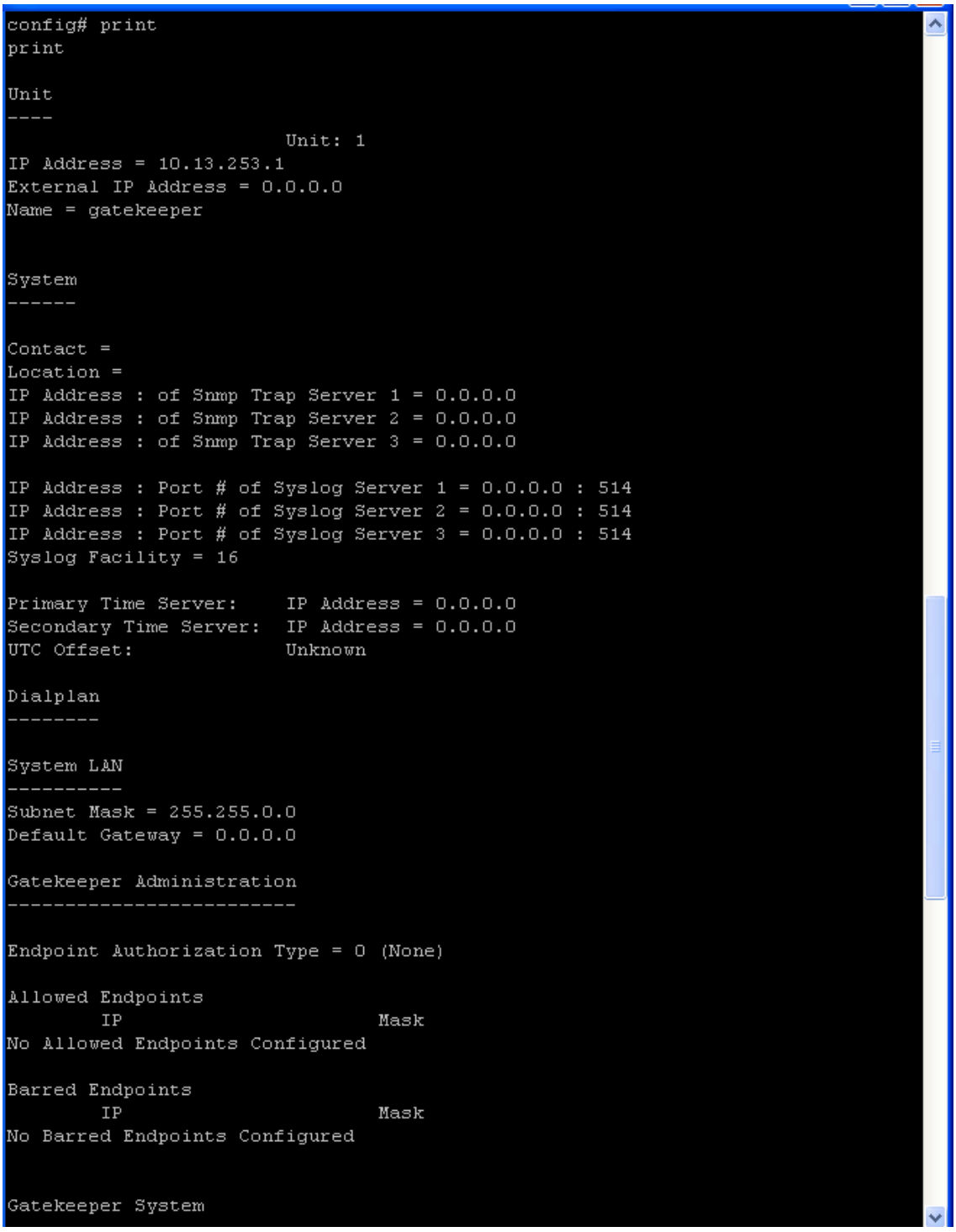


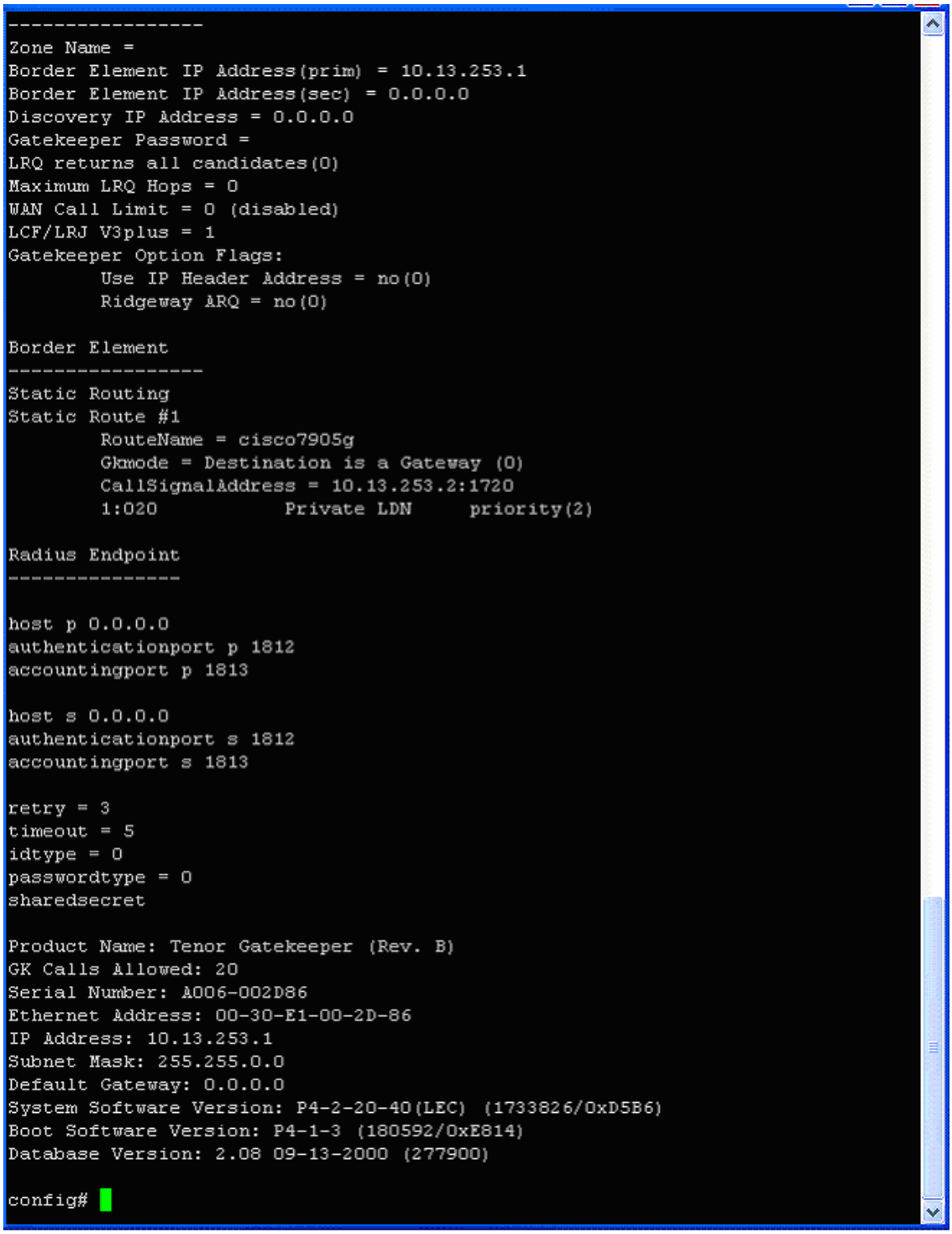
Figura 92: Configuración del Gatekeeper para la Plataforma de Intefonía del Metro de Valencia.

Se puede comprobar toda la configuración interna del Gatekeeper usando el comando `print` desde el menú `config` (en dos capturas de pantalla que se refieren al mismo comando: figuras 93 y 94):



```
config# print
print

Unit
----
                        Unit: 1
IP Address = 10.13.253.1
External IP Address = 0.0.0.0
Name = gatekeeper


System
------

Contact =
Location =
IP Address : of Snmp Trap Server 1 = 0.0.0.0
IP Address : of Snmp Trap Server 2 = 0.0.0.0
IP Address : of Snmp Trap Server 3 = 0.0.0.0

IP Address : Port # of Syslog Server 1 = 0.0.0.0 : 514
IP Address : Port # of Syslog Server 2 = 0.0.0.0 : 514
IP Address : Port # of Syslog Server 3 = 0.0.0.0 : 514
Syslog Facility = 16

Primary Time Server:    IP Address = 0.0.0.0
Secondary Time Server:  IP Address = 0.0.0.0
UTC Offset:             Unknown

Dialplan
--------

System LAN
----------
Subnet Mask = 255.255.0.0
Default Gateway = 0.0.0.0

Gatekeeper Administration
-------------------------

Endpoint Authorization Type = 0 (None)

Allowed Endpoints
        IP                      Mask
No Allowed Endpoints Configured

Barred Endpoints
        IP                      Mask
No Barred Endpoints Configured


Gatekeeper System
```

Figura 93: Captura 1 para mostrar la configuración completa del Gatekeeper en la Plataforma de Interfonía del Metro de Valencia.



```
-----------------
Zone Name =
Border Element IP Address(prim) = 10.13.253.1
Border Element IP Address(sec) = 0.0.0.0
Discovery IP Address = 0.0.0.0
Gatekeeper Password =
LRQ returns all candidates(0)
Maximum LRQ Hops = 0
WAN Call Limit = 0 (disabled)
LCF/LRJ V3plus = 1
Gatekeeper Option Flags:
        Use IP Header Address = no(0)
        Ridgeway ARQ = no(0)

Border Element
------------------
Static Routing
Static Route #1
        RouteName = cisco7905g
        Gkmode = Destination is a Gateway (0)
        CallSignalAddress = 10.13.253.2:1720
        1:020           Private LDN     priority(2)

Radius Endpoint
---------------

host p 0.0.0.0
authenticationport p 1812
accountingport p 1813

host s 0.0.0.0
authenticationport s 1812
accountingport s 1813

retry = 3
timeout = 5
idtype = 0
passwordtype = 0
sharedsecret

Product Name: Tenor Gatekeeper (Rev. B)
GK Calls Allowed: 20
Serial Number: A006-002D86
Ethernet Address: 00-30-E1-00-2D-86
IP Address: 10.13.253.1
Subnet Mask: 255.255.0.0
Default Gateway: 0.0.0.0
System Software Version: P4-2-20-40(LEC) (1733826/0xD5B6)
Boot Software Version: P4-1-3 (180592/0xE814)
Database Version: 2.08 09-13-2000 (277900)

config#
```

Figura 94: Captura 2 para mostrar la configuración completa del Gatekeeper en la Plataforma de Interfonía del Metro de Valencia.

Con respecto a la ampliabilidad de la plataforma, para cada nuevo teléfono VoIP autónomo de numeración estrictamente pública (como por ejemplo el SJPhone), habría que configurar otra ruta estática en el Gatekeeper que haga de *border element* de la plataforma (de forma que si se añaden nuevos Gatekeepers, en éstos sólo hará falta configurarles la existencia de este *border element*, y mediante LRQs toda la información de direccionamiento asociada las rutas estáticas de la plataforma será pasada a los nuevos Gatekeepers).

Esta nueva ruta estática se configurará de forma análoga a la presentada para el teléfono Cisco 7905G: tendrá como destino como destino la IP del nuevo teléfono, y, en este caso, se asociará a dos números de tipo privado: el 1xxx (ya que los números marcados por el Cisco 7905G se consideraban privados en el Quintum Tenor Gatekeeper) y el xxx (para las pasarelas). Por otro lado, se se añaden nuevos Cisco 7905G en la plataforma, a la ruta estática cuya configuración se acaba de mostrar habrá que añadirle también el número 1xxx privado (para la comunicación entre los Cisco 7905G).

3.4.2.4 Interfonos

Al igual que en el anterior proyecto, ha de programarse en cada uno de ellos exactamente lo mismo, a saber: el marcado primero de la extensión destino 1014 (puesto de mando), y segundo de la extensión 1020, en el caso de que la primera comunique o no responda en 4 tonos de señal.

Para ello, hay que efectuar una comunicación analógica contra ellos (también es posible llamarles por VoIP gracias a la transmisión de dígitos DTMF en banda), y entonces marcar el código de seguridad (por defecto el 845464), programar el primer número llamado (con la secuencia 1014#00), y el segundo (secuencia 1020#01), y establecer las opciones de tiempo y marcación (con la secuencia 250421#18, con la cual se configuran 4 tonos de espera antes de saltar al siguiente número, salto al siguiente número si el anterior está ocupado, y otros detalles como 0.2 segundos de retardo de inicio de la comunicación, y 5 minutos de tiempo máximo de comunicación).

3.4.2.5 Alcatel Temporis 45

Para la configuración de este teléfono tan sólo es necesario introducir en su agenda interna la asociación de cada extensión de los interfonos con su localización, con el formato requerido por el cliente. De esta forma, ante la llamada entrante de cada uno de ellos éste podrá identificar su localización desde el puesto de mando.

Para cada registro, hay que pulsar la tecla `menu`, seleccionar con el cursor la opción `agenda`, a continuación teclear el nombre de identificación deseado y volver a pulsar la tecla `menu`, luego el número, y a continuación la tecla `ok`. Se dispone de 20 caracteres como máximo para la definición de cada extensión, pero es suficiente.

3.5 Problemas encontrados y soluciones

Durante el desarrollo de estas plataformas surgieron no pocos problemas. En el presente apartado se dará una orientación de cómo se resolvieron, mediante la monitorización de cada elemento de la plataforma, para comentar a continuación los problemas que resultaron más interesantes o anecdóticos.

3.5.1 Monitorización de cada elemento

Ante un diseño de red de integración, lo más importante es conocer cada paso de la comunicación, en el ámbito del protocolo. Para ello, tras haberse estudiado concienzudamente el mismo, resulta fundamental poder monitorizar el comportamiento de cada elemento de la red, para que, en el caso de que suceda algún comportamiento indeseado, pueda encontrarse la causa.

El examen de las trazas de la comunicación es el método más seguro, en el que puede encontrase el verdadero núcleo del error en la comunicación. En el caso de H.323, se representa en paquetes de protocolo, y será necesario algún programa capaz de descodificarlos. En SIP, las trazas, como todo el protocolo, siguen un formato de texto más legible.

Pero también pueden examinarse los *logs* de comportamiento interno, en el que aparecen las funciones informáticas que ha seguido el proceso; hay que recordar que estos elementos de red se encuentran formados, al final, por una máquina de Von Neumann, con microprocesador y programa internos. Estos casos pueden resultar útiles cuando existen posibilidades de configuración cuyo significado (a pesar de la teoría y a pesar del manual de configuración) acaban por desconocerse absolutamente.

A continuación se mostrarán los elementos de configuración que se han utilizado para los equipos más significativos de las plataformas, así como algunas soluciones rápidas de revisión de parámetros de configuración:

3.5.1.1 Pasarelas Quintum Tenor

El primer elemento de la monitorización es el comando ping. Por él, puede determinarse tanto su conectividad como la fiabilidad de su conexión.

La revisión de los parámetros de conectividad de las pasarelas Quintum Tenor es una tarea laboriosa por la enorme cantidad de detalles que ofrecen:

- Si no hay conectividad con el Gatekeeper, hay que examinar los menús de `H323 Signaling Group`.

- Si ni siquiera se logra iniciar una llamada a pesar de estar registrados en el Gatekeeper, hay que asegurarse de que, si no se usa un servidor RADIUS[48], los *call flow* IVR[49] están desactivados, en los LCRG, TCRG, e IPRG. También, habrá que examinar la configuración correcta del plan de marcado (*Dial Plan*), así como del plan de marcado IP (*IP Dial Plan*).
- Si el destino da tono de llamada pero no se establece la conexión, hay que probar con los parámetros H.245 que se encuentran en la pestaña `Advanced` del menú `H.323 Signalling Group`. También habrá que examinar los *Voice Codecs*, y el *Fast Start* de los *IP Routing Groups*.
- Si no recibe alguna llamada, hay que comprobar detenidamente los HuntLDN asociados a cada canal, (LCRGs, y *Channel Groups*). Para todo esto se utiliza el *Tenor Configuration Manager*.

Pero hay casos en los que la configuración parece ser correcta y el sistema continúa fallando. Una vez revisada toda la configuración, es necesario acudir a una sesión de Telnet y examinar las trazas justo durante la aparición del error.

Como este trazado no se almacena internamente en los Quintum Tenors, una forma sencilla de conservar esta información es en la propia ventana de la sesión de telnet. Para modificar la capacidad del buffer de la ventana MSDOS de Windows, botón derecho sobre la parte superior de la ventana, pestaña `Diseño`, tal como se muestra en la figura 95:

[48] RADIUS: *Remote Access Dial In.Use Server*, protocolo de Autorización, Autenticación y *Accounting* para aplicaciones de acceso a una red.
[49] Los *call flow* IVR (*Interactive Voice Response*) son los esquemas de protocolo RADIUS, que se asocian comúnmente con mensajerías pregrabadas para la interacción con el usuario.

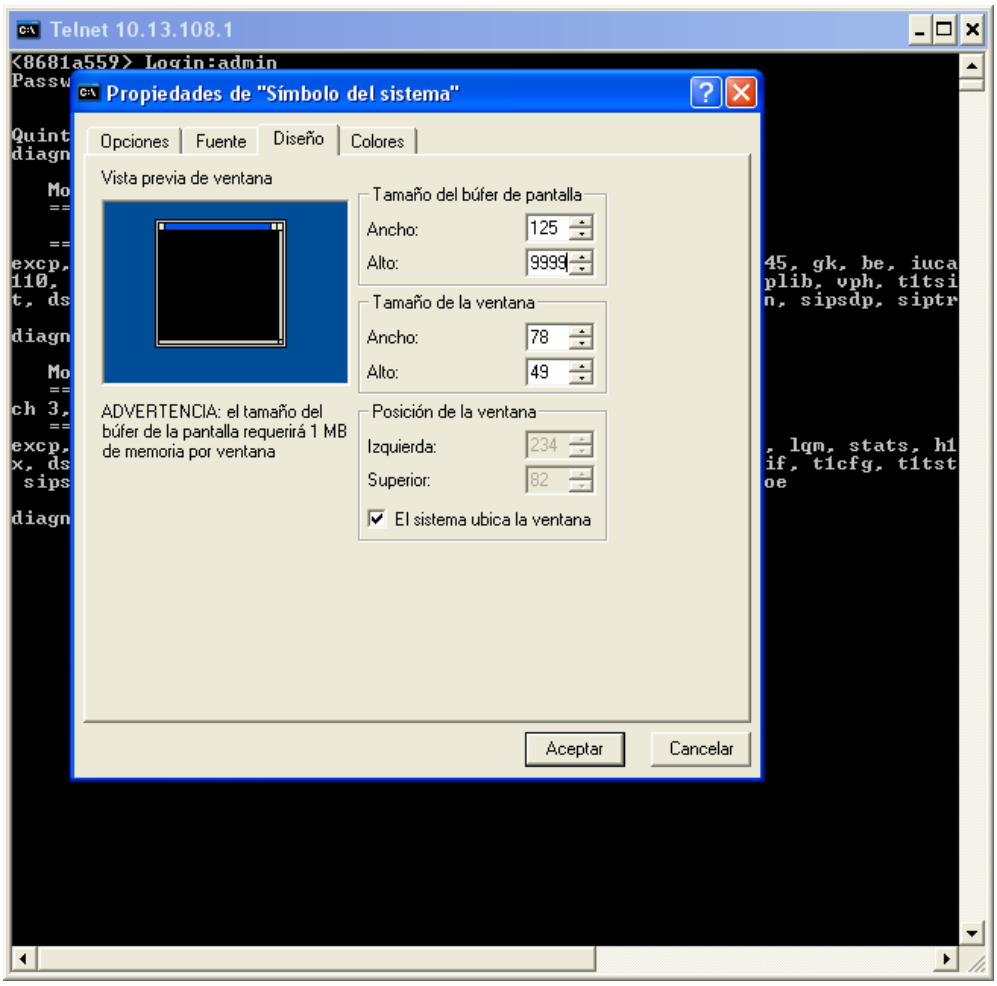


Figura 95: Ampliación de la ventana de comandos MSDOS en Windows XP.

El buffer máximo son 9999 líneas; estos equipos pueden mostrar una cantidad gigantesca de información relacionada con cada llamada: es importante reconocer qué partes del sistema podrían influir en el error. Por ejemplo: sólo el módulo `h323p` suelta 1500 líneas en una llamada de 5 segundos de duración.

A continuación, se muestra una lista con todos los módulos de paquetes de trazas posibles, con el comando `ev names` lanzado desde el menú `diag` (figura 96):

```
Quintum# diag
diagnostic# ev names
-------------------------------------------------------------
Module    Description
-------------------------------------------------------------
excp      Exception
sys       System Library
root      Root/Watchdog/Idle
ab        DS1 boards AB bit signaling on DS0
ch        Call Handler
cas       Telcos Channel Associated Signaling
h323s     H323 Stack
h323p     H323 Protocol
h323q931  H323 Q931
hras      H323 Ras
```

```
h245      H323 H245
gk        Gatekeeper
be        BorderElement
iuca      Iuca MultiUnit
db        Database
isdnhl    High layer ISDN stack
hdlc      HDLC
l1        T1/E1 Layer 1
lqm       Lan Quality Monitor
stats     Statistics from DSPs
h323asn1  H323 ASN1
h110      H.110 CT Bus
pci       PCI Bus Manager
pcievnt   PCI Event/Alarm Logger
pcireg    PCI Registration Server
remlib    Remote Library Process
pri_dec   Primary Rate Interface Msgs Decoder
vphtx     VPH TX
dspstat   DSP Errors/Warnings/Statistics
dsplib    DSP Library on DSP Board
vph       Voice Packet Handler on SysCon board
t1tsi     DS1 boards TSI log
t1isr     DS1 boards ISR log
t1cc      DS1 boards Call Control log
t1frmr    DS1 boards framer log
t1l2      DS1 boards Layer 2 ISDN signaling log
t1lif     DS1 boards Inter signaling Layers log
t1cfg     DS1 boards configuration log
t1tst     DS1 boards testing log
dspdbg    DSP boards debugging log
radius    RADIUS client's logs
ivr       IVR logs
sntp      SNTP client
info      Informative msgs
socket    socket activity log
nms       Network Management System module
sipstk    SIP stack
sipsyn    SIP syntax
sipsdp    SIP sdp events
siptrans  SIP Transections
sipsess   SIP Session events
sipua     SIP user agent events
sproto    SIP protocols all modules event log
pppoe     pppoe  event log

diagnostic#
```

Figura 96: Lista de todos los paquetes de trazas permitidos en las pasarelas Quintum Tenor.

- Para lanzar los eventos, hay que entrar en el menú `diag`, y luego activar cada evento con `ev l[n] [nombre]`, donde `n` es el nivel (*level*) de detalle (a nivel 0 se anula ese módulo, y el máximo es 3). Luego, para visualizar el comportamiento del equipo en tiempo real hay que lanzar el comando `qu`, cuyo resultado se muestra a continuación en la figura 97:

Figura 97: Muestra de los *logs* de los equipos Quintum Tenor mientras reciben una llamada, en este caso, del SJPhone.

- Para reconocer un problema relacionado con incompatibilidades de señal, hay que utilizar el módulo `cas` en las pasarelas analógicas (el `l1` en los digitales), y el módulo `ch`.

- Para examinar la comunicación con el Gatekeeper, hay que hacer uso del módulo `gk`. En errores tras haberse aceptado una llamada en el Gatekeeper, se tendrán que examinar los módulos `hras`, `h245`, `h323s`, y el `h323p` que engloba todos los anteriores. De la misma forma, los módulos SIP específicos.

- Para examinar el comportamiento con el servidor RADIUS, habrá que examinar los módulos `radius` y `ivr`.

- Para errores del sistema, el módulo `excp`, y otros módulos cuyo significado sólo tiene utilidad de cara a los fabricantes (como los que controlan el funcionamiento del bus pci y de los dsp, el examen de las librerías internas).

Por último, Quintum presenta también el *Tenor Monitor*, programa en java sin requerimientos de licencia. Un programa de interfaz sencilla, de funcionalidad sencilla. Debe estar conectado a la red local en la que se sitúen los Tenors a ser monitorizados, y no

admite monitorización de Gatekeepers. La interfaz gráfica de este programa se presenta en las figuras 98, 99 y 100:

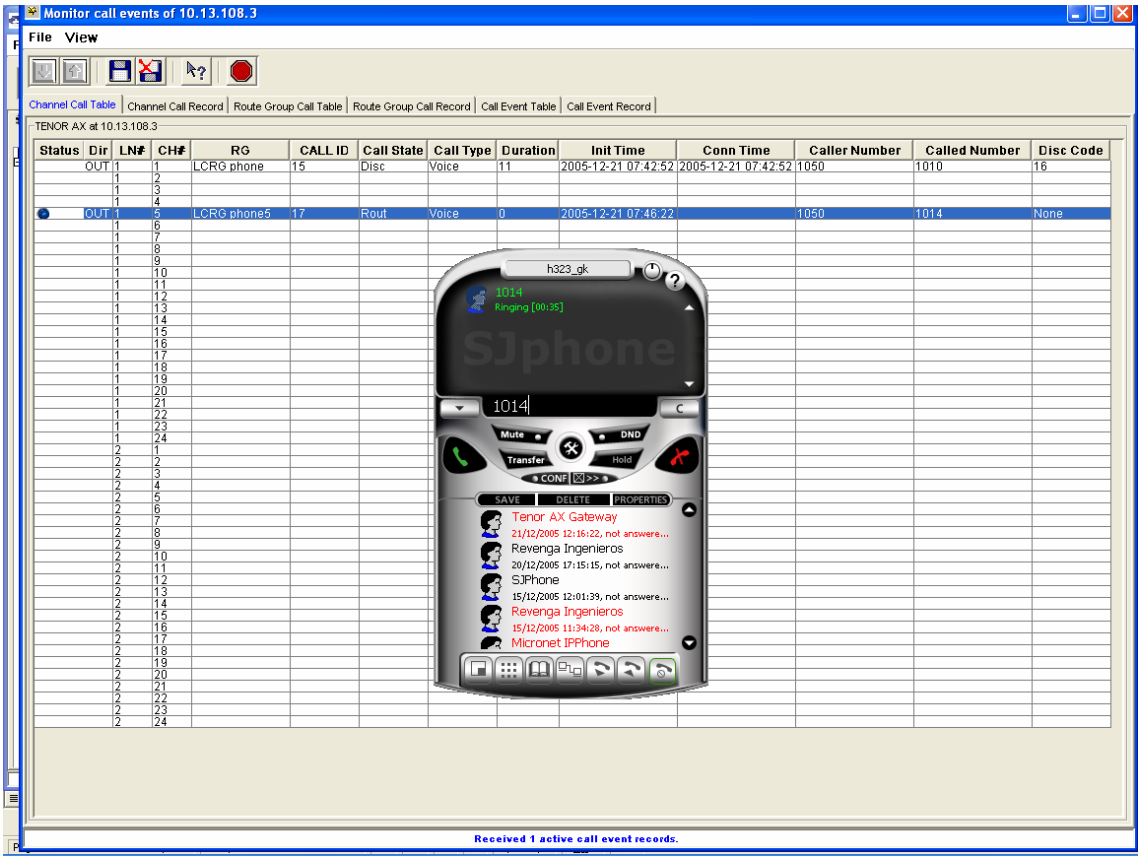


Figura 98: Comportamiento del *Tenor Monitor* mientras se efectúa una llamada contra un Quintum Tenor.

Puede monitorizar CDR[50], llamadas activas, y alarmas, en tiempo real, y generando *logs* (figura 99):

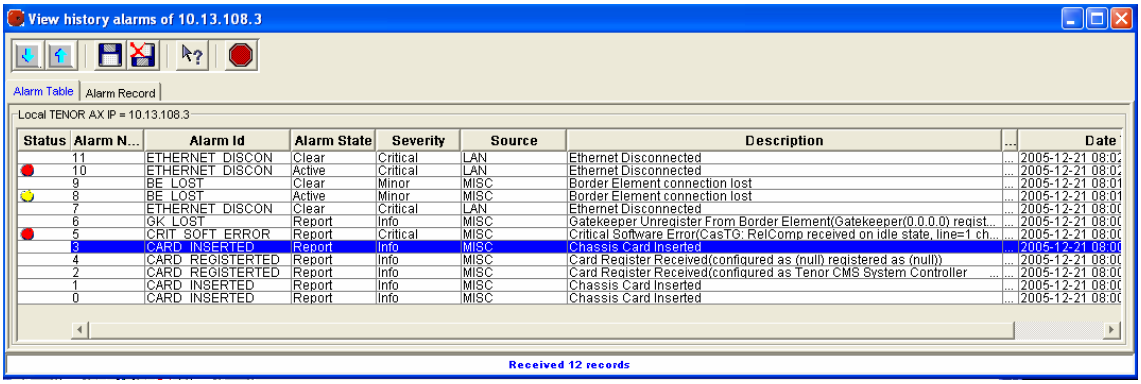


Figura 99: Muestra del histórico de alarmas de los Quintum Tenor, monitorizados por el *Tenor Monitor*.

Puede monitorizar varios Tenors a la vez (figura 100):

[50] CDR: *Call Detail Record*, registro de detalle de llamadas.

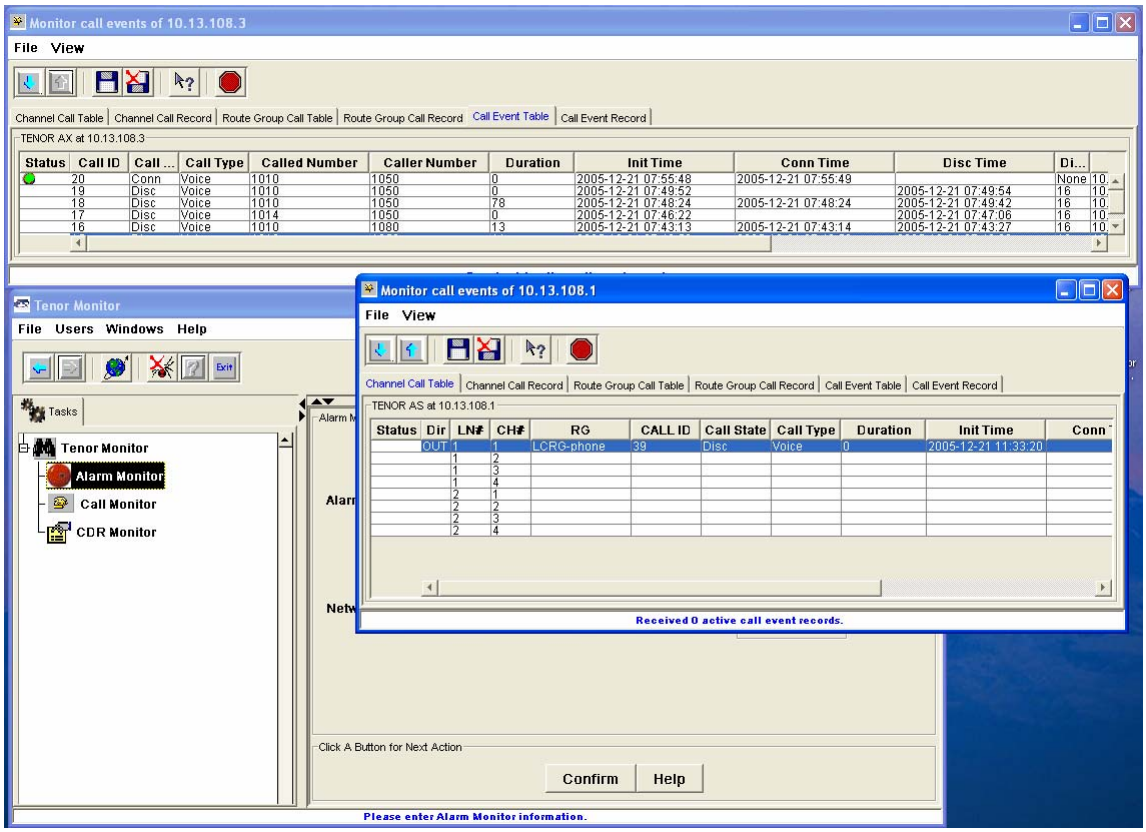


Figura 100: Actividad de las llamadas entre los equipos Quintum Tenor desde el *Tenor Monitor*.

Por último, también se hará referencia al último equipo que Quintum sacó al mercado, llamado *Remote Management Session Server*, un servidor que se dedica exclusivamente a permitir la conexión, a través de diversas cajas NAT[51] y cortafuegos (es decir, accediendo a las redes locales de cada subsistema de VoIP Quintum), contra todos los equipos Quintum Tenor de una corporación. Este equipo está diseñado para permitir el mantenimiento y configuración de grandes redes VoIP con equipos Quintum, mediante conexiones telnet CLI[52], además de conexiones mediante el *Tenor Configuration Manager*.

3.5.1.2 Quintum Tenor Gatekeeper

Como antes, se podrá determinar la actividad de su interfaz de red mediante ping.

El Telnet es el mejor monitor de estos Gatekeeper: el comando qu, aunque no ofrece tanta información como en Quintums Tenor de segunda generación, permite monitorizar módulos de excepciones, telnet y ftp, conexiones RAS, Gatekeeper, *border element* y asn1, así como librerías y base de datos.

[51] NAT: *Network AddressTranslation*, traducción de direcciones de red, para transformar direcciones IP públicas en privadas.
[52] CLI: *Command Line Interface*, interfaz de línea de comandos.

El Gatekeeper apenas presenta opciones de configuración: apenas, la configuración del *border element*, lista de terminales permitidos y rutas estáticas. Además, sólo puede accederse a él mediante telnet (o cable serie).

Para conocer los equipos conectados y admitidos en el Gatekeeper, se usa el comando `gk ep`. Se muestran entonces todos los parámetros configurados en el equipo: LDNs (es decir, números de teléfono asociados a él como extensiones directas), y LAMs (*leaky area numbers*, es decir números de teléfono asociados a él como extensiones de salto, como por ejemplo para salir al exterior).

Y para consultar la rutas estáticas configuradas en el *border element*, hay que usar el comando `print` desde el submenú `config be`.

Finalmente, también permite un *log* de eventos: en telnet, mediante el comando `qu`. Para activar o desactivar los módulos de log se hace `ev + gk`, o `ev – excp`. El nivel de *log* se establece el mismo para todos los módulos: mínimo nivel de detalle con el comando `ev l1`; máximo con `ev l3`.

Se muestra a continuación todos los módulos de *log* permitidos en el Gatekeeper (figura 101):

```
Quintum:gatekeeper> ev s

Event Log Status...
Enabled Modules: excp
Total Evlog memory size=65508
Read_index=148, Write_index=148
Total size used=65508
Event log level=3
===== Event Log Module List =====
excp            Exception
sys             System Library
root            Root/Watchdog/Idle
tn              Telnet
ftp             File Transfer Protocol
hras            H323 Ras
gk              Gatekeeper
be              BorderElement
db              Database
asn1            H323 ASN1
sntp            SNTP
===== Debug Group List =====
h323d           H323 Debug Group
isdnd           ISDN Debug Group
casd            CAS Debug Group
dspd            DSP Debug Group
faxd            FAX Debug Group
Quintum:gatekeeper>
```

Figura 101: Lista de todos los módulos de *log* del Quintum Tenor Gatekeeper.

En este caso, los módulos más útiles son `gk` y `hras`, para ver las comunicaciones de los elementos de su zona con él, y `be` para ver las comunicaciones Anexo G/H.225.0 entre *border elements*.

3.5.1.3 Teléfono IP Cisco 7905G

En la interfaz web del teléfono, en el apartado `Network Statistics` se presentan algunos detalles como el tiempo de conexión, paquetes recibidos y transmitidos, y errores en transmisión y en recepción.

Sin embargo, esta opción resulta un tanto insuficiente, y además no funciona en tiempo real. Este teléfono ofrece entre sus archivos de licencia un pequeño programa MSDOS que recoge gran cantidad de información del teléfono, como los mensajes H.323 que lo atraviesan, la negociación del códec, el resultado de la llamada. Este programa se llama `prserv.exe`, y funciona en tiempo real a través de un puerto configurable. A continuación se mostrará una captura de pantalla con su actividad, en la figura 102, donde se puede apreciar el formato en que se muestra por pantalla la actividad del teléfono durante una llamada, mostrándose información relacionada con los paquetes que pasan y secciones de programa que suceden en el teléfono:

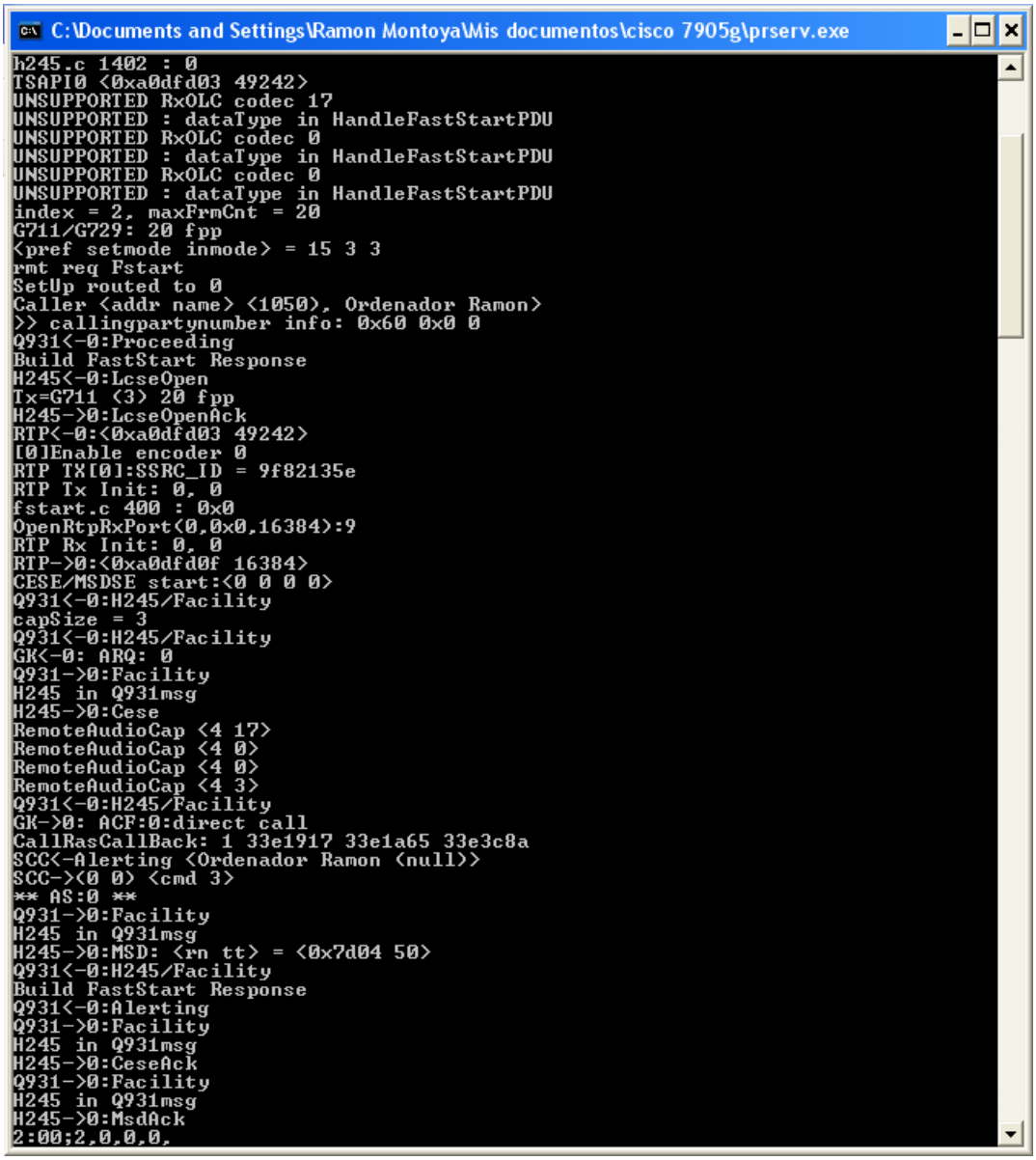


Figura 102: Actividad del programa prserv.exe para monitorizar un Cisco 7905 G.

Automáticamente, toda esta información se almacena en un archivo de texto.

Se revisan a continuación las posibles actuaciones ante problemas de interoperabilidad con este teléfono:

- Ante un problema de comunicación con el Cisco 7905G, lo primero de todo es comprobar los cables: si el teléfono muestra en el *display* el mensaje "*Ethernet Disconnected*", la red se ha caído. A continuación se puede verificar si el Gatekeeper no reconoce al teléfono: esto sucede cuando, al descolgar, el teléfono muestra "*Network Error*". Puede entonces que la IP del teléfono esté mal configurada y caiga fuera de la subred en la que se encuentra el Gatekeeper, o que la dirección del Gatekeeper esté mal configurada en el teléfono.
- Por otro lado, si la llamada se rechaza antes de que el destino dé tono de llamada, entonces puede que exista un problema de direcionamiento: en el caso del uso Gatekeepers Quintum, es necesario registrar el número destino como privado mediante una ruta estática en el *border element* del sistema, y con pasarelas Quintum también es necesario registrar el número de destino como de tipo público (como se analizó en la pasarela Estación de Bailén). También puede haber alguna incompatibilidad por el uso de *Fast Start*: esto se configura en el parámetro `ConnectMode`.
- Si nada de esto sucede, y el teléfono destino hace da tono de llamada pero al descolgar justo la llamada se rechaza, entonces existe una incompatibilidad en los parámetros de voz: en los códecs, en H245 *tunneling*; todo esto se configura en los parámetros `AudioMode` y `ConnectMode` del teléfono.

3.5.1.4 Teléfono IP SJPhone

Este teléfono tampoco admite monitorización; pero, al tratarse de una aplicación software, resulta mucho más sencillo de controlar que cualquier aparato instalado en campo, o independiente de ningún computador.

Se revisan a continuación algunas actuaciones ante problemas de interoperabilidad:

- Ante un problema de conectividad con el Gatekeeper, lo más rápido es hacer uso, con el botón derecho, del comando `Restart` (porque, ante fallos leves de red etc, este teléfono no intenta reconectarse indefinidamente).
- Ante fallos de audio, los códecs se miran en el submenú `Options` pestaña `Audio` botón `compression settings`; también hay que verificar los parámetros del perfil, en las pestañas `H.245` y `Media Channels`. En esta última, se encuentran parámetros como `Use Remote Codec Preferences` (uso de las preferencias de códec del terminal con el que se establece la comunicación), `Open Audio Streams After Remote Opened` (para abrir las conexiones de audio después del remoto), y `Hangup If Failed to Open Outgoing/Incoming Audio` (colgar si hubo algún error en la apertura del audio entrante o saliente).

3.5.1.5 Sniffer de red

Para los casos en los que no fue suficiente otra monitorización, se hizo uso de un sniffer de red (que, entre otras cosas, también sirvió para determinar las IP extraviadas de algunos terminales, debido a sus ARP[53] al conectarse a la alimentación y a la red), el programa *freeware* Ethereal [72], el cual comprende perfectamente el significado y tipo de los paquetes H.323. Este programa se adjunta en el CD, en la carpeta `Archivos Adjuntos\Varios\Ethereal - ethernet sniffer`, archivo `ethereal-setup-0.99.0.exe`.

3.5.2 Problemas concretos

A continuación se muestran algunos de los problemas más intersantes o anecdóticos que surgieron durante el desarrollo de ambas plataformas:

3.5.2.1 Comunicaciones entre las pasarelas y los teléfonos IP

Uno de los problemas más importantes que tuvo que resolverse durante el transcurso de la configuración de los equipos comenzó con una falta de comunicación entre las pasarelas Quintum Tenor y los teléfonos IP, a pesar de que el Gatekeeper registraba perfectamente todos los equipos.

Todo parecía correcto hasta que se notó la división en public – private de los números registrados en el Gatekeeper (división no estrictamente en el marco de H.323 sino debida al uso de parámetros NonStandardData en los paquetes, como ya se ha explicado anteriormente). Por defecto, la numeración de las pasarelas era privada, y la comunicación con los teléfonos IP públicos no tenía lugar.

Así se cambió el tipo de numeración en las pasarelas a público. Todo fue correctamente, hasta que se descubrió un error de comunicaciones en las pasarelas Quintum cuando se trataba de establecer comunicaciones intra-pasarela.

La única posibilidad era un error de configuración a nivel interno, en la propia pasarela. En efecto, las pasarelas están divididas internamente en dos interfaces: una analógica, que asigna rutados a las interfaces FXS, y otra digital, que maneja las rutas H.323. Era posible que, por algún motivo, la interfaz analógica rechazase la comunicación. Examinando los *logs* de la pasarela destino se encontró que la llamada era rechazada porque el número destino no se correspondía con la asignación interna. Se compararon estos *logs* con los generados en la comunicación con teléfonos H.323 no Quintum y pudo apreciarse que las comunicaciones sí funcionaban.

[53] ARP: *Address Resolution Protocol*, protocolo de resolución de direcciones.

Profundizando en los comandos de configuración de las pasarelas (cuya descripción en los manuales no resultaba demasiado esclarecedora), se llegó a los prefijos del plan de marcado y, entre ellos, el prefijo `Intercom`. Éste permitía la comunicación con ambos tipos de numeración: pública (que no funcionaba en las comunicaciones intra-pasarelas y sí en las comunicaciones inter-fabricantes) y privada (destinada a comunicaciones entre equipos Quintum) simultáneamente.

Finalmente, se decidió resolver este paso modificando todo el plan de numeración para adaptarlo al uso del nuevo prefijo y duplicando el plan de numeración (en público y privado) cuando fuese necesario, para posibilitar así la integración con equipos de distintos fabricantes.

3.5.2.2 Comunicaciones entre las pasarelas y los interfonos

Las primeras pruebas que se hicieron con los interfonos fueron satisfactorias: la comunicación era correcta, los niveles de voz eran de calidad (quizás un cierto eco), se permitía la programación gracias a la transmisión de dígitos *in-band* y luego DTMF… hasta el momento en que se probó la programación de salto tras un cierto número de tonos de espera o destinos ocupados. El interfono no parecía enterarse de cuándo la comunicación no podía establecerse: sólo de cuándo acababa.

Se revisaron las frecuencias de operación del interfono en relación con las generadas por la pasarela analógica; la impedancia; todo parecía correcto. La interfaz analógica hacía *forward disconnect*, asegurando la desconexión del interfono… pero el interfono seguía sin enterarse de los tonos de espera o de cuándo los destinos estaban ocupados.

Comenzaron a examinarse los *logs* internos, hasta que se encontraron unas líneas en el *log* que establecían que, antes de comenzar la comunicación, se suprimiese la comunicación analógica local relativa al transcurso de la llamada.

Posteriormente se descubrió que este problema sólo sucedía cuando la comunicación se establecía con destinos remotos (es decir, no con terminales conectados a la misma pasarela). Entonces comenzaron a revisarse los parámetros relacionados con la transmisión de tonos a través de la red. Pero eran los mismos: transmisión DTMF, posibilidad de hacerlo *in-band* o H.245, y algunos parámetros de difícil significado, entre ellos, el parámetro `Inband tones`, activo en la configuración por defecto de las pasarelas.

El manual sólo comentaba algunas diferencias relativas al protocolo usado: entre ellas, el uso de *Fast Connect* y del mensaje H.225.0 Progress. Y, ante el envío de este mensaje (que se realizaba cuando el parámetro `Inband tones` estaba activo), el bucle local conectaba un audio (“*connecting voice path for progress*”), pero no devolvía el tono (“*providing local ring back*”) como sí hacía cuando `Inband tones` estaba desactivado.

A partir de entonces, se determinó desactivar `Inband tones` de todas las pasarelas conectadas a la plataforma de interfonía; sólo entonces los interfonos comenzaron a mostrar el comportamiento deseado.

3.5.2.3 Adquisición del teléfono IP Cisco 7905G

Cuando se adquirió el primer teléfono Cisco 7905G se hizo a través de un distribuidor inglés, que mantenía los mejores precios: 95 libras esterlinas, que con los portes suponían unos 175 €. El teléfono llegó al día siguiente de hacer el pedido, pero lo primero que sucedió fue con que no se pudo enchufarlo a la alimentación, porque este teléfono a priori permitía la posibilidad de trabajar con PoE (*Power over Ethernet*, tecnología que por otra parte soportan prácticamente todos los switches de Cisco Systems), y no traía ningún transformador.

La alimentación necesaria era de 48 V. La empresa disponía de un laboratorio en el que continuamente se fabricaban cables y fuentes con material sobrante de otros proyectos, pero esta era la primera vez que se utilizaba un transformador tan grande.

Para hacer las primeras pruebas con el teléfono pudo hacerse uso de un generador de onda de laboratorio, sumando en serie sus dos generadores de 30 V. Pero entonces se encontró un segundo problema: el teléfono venía cargado por defecto con una licencia de SCCP (el protocolo VoIP propietario de Cisco Systems). Había que adquirir una licencia nueva, para que este teléfono pudiera funcionar bajo H.323 o SIP.

El transformador tuvo un coste de unos 30 €, y la licencia otros 35. El coste del teléfono se incrementó en un 50%. Hay que decir que estos detalles se especificaban en el *datasheet* del teléfono (al final del *datasheet*). Y esto fue sólo por estar acostumbrados a fabricantes de bajo coste: tanto el Micronet como el Telkus venían con su fuente y su *firmware* gratuito y actualizable desde la web.

3.5.2.4 Eco entre el interfono y los teléfonos de atención

Uno de los problemas más graves que se encontraron durante las primeras pruebas SAT[54] en el Metro de Valencia fue que en el puesto de control la comunicación se cortaba. Todo la configuración era correcta pero, a pesar de que la comunicación se establecía durante algún que otro segundo, luego ésta se cortaba.

En fábrica no había sucedido ningún problema parecido. Y, además, este problema sólo sucedía con algunos interfonos, y con otros no. Mientras se ajustaba el eco de las comunicaciones con los primeros, que era bastante grande, pasó un metro (aún no se detenían los metros, sólo pasaban), y la comunicación se cortó. Recordamos entonces el límite de ruido de seguridad que tienen estos interfonos, cuando el nivel de señal supera un cierto número de decibelios.

Tras retocar todas las ganancias posibles en la configuración de las pasarelas (hay posibilidades de configuración de ganancia en IP y en el bucle local), y ver cómo era casi imposible dejar una comunicación con niveles de recepción aceptables, se descubrió que el audio del Alcatel Temporis 45 tenía el volumen de recepción al máximo.

Al bajarlo a un nivel medio todo comenzó a funcionar.

[54] SAT: *Site Acceptance Test* , pruebas tras la instalación

3.5.2.5 Display del Alcatel T45

Tras la instalación de la plataforma en el Metro de Valencia, se recibió el aviso que el operador no recibía la información relativa al número llamante y que, por lo tanto, no sabía a priori desde dónde le estaban llamando.

Al día siguiente se desplazó hasta Valencia un equipo de dos personas entre otras cosas para resolver este problema. El operador ratificó este comportamiento. Se activaron los comandos de trazas en los equipos y se hizo una llamada desde uno de los interfonos al operador. Se rastrearon las trazas exhaustivamente, pero todo parecía correcto. Todo estaba en orden, y además la semana anterior, durante las primeras pruebas, el número había aparecido perfectamente en el *display*. Entonces se probó otra llamada al puesto de control, pero esta vez se pudo comprobar que número aparecía, correctamente, en el *display*, así incluso el nombre, guardado en la agenda, asociado a ese número. Pero, *al descolgar*, esta información se borraba, pasando a mostrar la información relativa al progreso de la llamada.

Es decir, que no había ningún error, y que el operador sólo tenía que fijarse en la información mostrada por el *display antes* de descolgar.

3.6 Discusión

En este capítulo, tras repasar algunas de las dificultades encontradas en este proyecto, se incluye un análisis en profundidad de las ventajas e inconvenientes que presentan las redes de telefonía (en las que se incluyen estas plataformas de interfonía debido a su similar configuración) cuando se plantea un modelo de ingeniería de integración de distintos fabricantes, frente a las soluciones propietarias y los modelos de *renting*.

3.6.1 Comentario sobre los equipos utilizados

En este proyecto se ha llevado a cabo la tarea de aplicar a redes de telefonía sobre LANs unos equipos de VoIP concebidos principalmente para soluciones orientadas a operadores internacionales de telefonía y proveedores de servicio en general.

Esto es lo que sucede con las tecnologías ofrecidas en exclusiva para los equipos Quintum Tenor: la tecnología *SelectNet*, que permite que una llamada que baje de cierta calidad de servicio sobre la red IP pueda conmutarse a una llamada PSTN de forma totalmente automática; y la tecnología *PacketSaver*, que pega paquetes VoIP para aprovechar sus cabeceras, reduciendo un interesante porcentaje de ancho de banda en redes cargadas. Tecnologías claramente orientadas a proveedores de servicio, como también lo es el último equipo que ha sacado Quintum al mercado, el *Remote Management Session Server* [73] dedicado a monitorizar y controlar redes Quintum Tenor, de forma transparente a cortafuegos y a NATs. Por último, también hay que destacar la integración de estos equipos

con servidores RADIUS, típicamente utilizados para autorización de números llamantes y para tarificación, muy útiles en empresas, por ejemplo, de tarjetas de prepago para llamadas internacionales. (Se incluye en la documentación adjunta un servidor CDR desarrollado por Quintum y varios servidores RADIUS, todos software, así como algunas instrucciones sobre autenticación y tarifado, en la carpeta `Archivos Adjuntos\Quintum Technologies\Autenticación y Tarifado`).

En definitiva, quizás la elección que se hizo de partida con estos equipos no haya sido la más acertada, en estos escenarios. Hay que volver a remarcar que esta elección estaba fuera de los objetivos de diseño.

Quizás haya sido en parte debido a esta elección que la dificultad más importante del presente proyecto ha sido la integración de estos equipos con equipos de otros fabricantes, aun en el marco del protocolo H.323, tan minuciosamente diseñado para que esta interacción no dé lugar a errores.

Además, los equipos Quintum Tenor presentan algunas funcionalidades adicionales exclusivas para la comunicación con otros equipos Quintum. Esto no sólo sucede con las anteriormente comentadas tecnologías *SelectNet* y *PacketSaver*, sino también cuando se presentan parámetros específicos para la interacción con equipamiento Nortel o Cisco: esto es lo que sucede con la división del plan de numeración en público o privado, y con el enorme número de prefijos asociados a éste, (y en el manual aparecen reflejados expresamente los nombres de estos fabricantes al explicar la funcionalidad de algunos de estos prefijos). Prefijos que dejan una planificación del plan de numeración en redes integradas sólo practicable por verdaderos “gurús” de estos equipos.

3.6.2 La integración de distintos fabricantes

Desde luego, el comportamiento anteriormente citado de la exclusividad del fabricante es una tarea común entre los fabricantes de hardware de VoIP, que tratan de conservar los clientes mediante pequeñas ventajas que luego podrían convertirse en trabas si se intenta cambiar de marca. Ningún ejemplo mejor que los protocolos propietarios del equipamiento Nortel (que no fabrica equipamiento VoIP bajo estándares internacionales); sin ir más lejos, el teléfono Cisco 7905G, utilizado en la plataforma de interfonía del Metro de Valencia, viene por defecto con el *firmware* para el protocolo propietario SCCP de Cisco Systems, y para utilizar los protocolos SIP o H.323 hace falta adquirir una licencia nueva, exclusiva. Y todos los switches Cisco ofrecen PoE (*Power over Ethernet*), como también lo acepta todo el equipamiento Cisco Systems, (como dicho teléfono IP). Es más rentable asegurar la fidelidad de un cliente que fabricar sistemas de cómoda interoperbilidad, ya que esta interoperabilidad supone la inclusión de otros fabricantes pueden llevarse cuota de mercado.

Tampoco puede olvidarse cómo hubo un par de teléfonos IP cuyo funcionamiento resultó inestable (OpenPhone, teléfono software de código abierto), o no compatible (el Telkus Totalfon IP5000). Y es que a veces un fabricante de bajo coste no es capaz de implementar correctamente un protocolo tan complejo como es H.323. Límite es el caso del teléfono IP Micronet 5100SP, también de bajo coste, el cual, tras mostrar una interoperabilidad impecable (mucho mejor que la encontrada entre los equipos Cisco y Quintum), falló en

pequeños detalles de acabado hardware. Y, en efecto, el estudio y adquisición de estos teléfonos conllevó un gasto adicional en ingeniería.

Pero, de todas formas, el funcionamiento de todo el sistema es perfectamente robusto, los equipos involucrados han demostrado una fiabilidad magnífica, la calidad de la voz es excelente, el resultado es más que satisfactorio. A pesar de todas las dificultades de ingeniería, la integración acaba siendo impecable.

Pero sin ninguna duda, las dos ventajas más importantes de la integración de sistemas de distintos fabricantes son:

- Pueden combinarse productos de distintos costes y características, adaptándolos a las necesidades de cada proyecto.
- El diseño de la red fácilmente queda abierto a futuras ampliaciones, con una interoperabilidad que radica en un protocolo no propietario, sino internacional: H.323.

3.6.3 Proyectos base para redes de telefonía

Se discutirán a continuación las soluciones alternativas a este planteamiento para una red de telefonía VoIP.

Para comenzar, el presente proyecto se refiere al diseño de redes de tamaño más bien pequeño, sobre las que aún no se ha hablado de la posibilidad de conectarse a la PSTN, o de rutar llamadas entre sedes de la misma empresa por IP (redes WAN). Pero estas pequeñas redes no son sino el esquema base sobre el que se basa cualquier red mayor:

- Para solucionar la conexión con la PSTN hay dos opciones: Una, utilizar una pasarela con puertos FXO conectados a las líneas externas o a una centralita analógica. Otra, usar una pasarela con puertos E1/T1 conectada a accesos básicos o primarios RDSI, con un número variable de líneas contratadas con el operador de telefonía, (suprimiendo la antigua centralita analógica). En ambos casos, estas pasarelas actuarían como centralitas.
- Pero esta no es la única forma de conectarse al exterior por IP: también puede usarse un proveedor de servicio de telefonía por Internet, como Cosmovoice [74]. Por ejemplo, sobre SIP sólo habría que dotar al servidor de la empresa con un elemento Proxy/Registrar, y una sola IP daría cabida a múltiples extensiones. Con H.323 habría que retocar la caja NAT (según las recomendaciones H.460.18 y H.460.19) para acabar utilizando uno de los Gatekeepers del sistema como elemento *proxy*, y posteriormente habilitar este Gatekeeper con proveedor del servicio.
- Por otro lado, y adicionalmente a lo anterior, podrían conectarse por IP las sedes de la empresa repartidas por todo el mundo, con sólo conectarse los anteriores Gatekeepers entre sí, mediante el Anexo G/H.225.0 y la definición de *border elements*, habiendo tan sólo que modificar un solo parámetro en la configuración de cada Gatekeeper.

Por último, tampoco pueden olvidarse las enormes posibilidades de ampliación que existen cuando se deja abierto el protocolo y el fabricante: desde sencillos teléfonos IP de código abierto o utilizables, a nivel no comercial, mediante versiones de prueba; hasta potentísimas

centralitas VoIP, como Asterisk, de código abierto (es decir, sin coste adicional alguno), que permiten dotar al sistema de avanzadas capacidades VoIP: conmutación programable y planes de marcado condicionales, mensajerías pregrabadas y atención automática, buzón de voz, colas de espera de llamadas y agentes de atención de llamadas en función de la franja horaria, monitorización de la red, etc.

3.6.4 Comunicaciones VoIP sobre redes WAN

Sin embargo, la enorme dificultad que suponen las comunicaciones VoIP que tengan que atravesar proveedores de servicio radica en que las redes VoIP aún no se han consolidado, y en que los proveedores de servicio de Internet no ofrecen habitualmente conexiones suficientemente fiables a nivel de empresa. Porque las comunicaciones de telefonía de una empresa son vitales en todo momento; la caída de la red de telefonía puede suponer muchos miles de euros en pérdidas. Por eso, ante el planteamiento de desviar las comunicaciones de telefonía por IP, es fundamental llevar a cabo una muy seria auditoría de red, para evaluar las capacidades necesarias para poder soportar holgadamente una hora cargada, quizás renovar los switches para que acepten calidades de servicio, etc.

Sobre las auditorías de VoIP se hablará mucho más extensamente en el Apéndice A.

Tampoco deben soslayarse, cuando las comunicaciones atraviesan Internet, las delicadas precauciones adicionales de seguridad que deben tomarse, no sólo para asegurarnos de la privacidad de nuestras comunicaciones de voz, sino también para protegernos de posibles ataques malintencionados: entre estos se encuentran la usurpación de la identidad del llamante, los ataques de denegación de servicio, el SPIT (*SPam over Internet Telephony*, por ejemplo hacia servidores de buzón de voz), o el acceso no autorizado a los servicios de VoIP.

Algunas soluciones son el uso de cortafuegos con características de VoIP, el encriptado de las comunicaciones, o incluso el uso de herramientas de monitorización de la red VoIP con detección y prevención de intrusos.

3.6.5 Análisis de las alternativas

Frente a este tipo de redes de telefonía, se encuentran las redes de un único fabricante. Avaya, Nortel o Cisco son ejemplos muy importantes.

Las redes “monofabricante” tienen la ventaja de que son mucho menos sensibles a los fallos. En efecto, es muy poco probable que surja un error de protocolo entre equipos de la misma marca, sobre todo si esta marca es la que establece el protocolo (es decir, con protocolos propietarios).

Estas redes disponen de elementos de red que actúan como centralitas IP en las que se han integrado los servicios adicionales más avanzados del momento, cuya característica más importante es que se integran a la perfección con el resto de la red. La robustez de cada solución está garantizada. Por contra, se pierde la capacidad de integración con elementos de red que no pertenezcan a este fabricante. En estas redes, el coste de ingeniería se reduce a

la planificación del volumen de servicio necesario, de cara al operador, y a la auditoría de red asociada.

Las grandes corporaciones prefieren este modelo para sus redes de VoIP. En este caso, la consultoría también puede contratarse al mismo operador.

Pero incluso ya Cisco se ha adelantado, y está preparando en España, junto con Tele 2, ofrecer una solución ya integrada (fabricante más operador) para telefonía VoIP orientada a PYMES, en un modelo de negocio que puede incluir el *renting* [75]. En este caso, el coste de ingeniería se reduce a cero.

3.6.6 Otras aplicaciones para el presente proyecto

Quizás el tamaño de la empresa sea determinante para la elección de una u otra solución de VoIP. Una empresa muy pequeña (microPYME[55]) podría no necesitar más que un tutorial para manejar una cuenta de Skype con conexión al exterior. A una PYME podría interesarle la integración si se le convence de las posibilidades de ampliación, y, sobre todo, si el coste ofrecido es muy inferior al ofertado por competidores como la opción antes comentada de Cisco y Tele 2. Pero el extenso marketing ofrecido desde hace tantos años por estas marcas tan prestigiosas en el mundo de las telecomunicaciones hace que el cliente desconfíe, a priori, de los proyectos de integración. Una gran empresa o multinacional no puede pensar en adquirir un producto que pueda fallar. Este mercado se concentrará claramente en torno a los grandes fabricantes.

Sin embargo, queda un caso de cierto interés: quizás, una empresa (o una institución pública) con efectivos en ingeniería de telecomunicaciones pueda asumir este riesgo, este coste de ingeniería. Entre otras cosas, el servicio técnico se encuentra en casa; y los responsables asumen directamente las garantías de servicio. Y probablemente el coste final resulte muy inferior a una solución contratada externamente.

[55] MicroPYME: Empresa con menos de 10 trabajadores.

4. Presupuesto

4.1 Diagrama de Gannt

Se incluirá a continuación el diagrama de Gannt asociado a ambas plataformas, en tanto en cuanto fueron desarrolladas simultáneamente.

En concreto, las tareas analizadas se corresponden con el trabajo a realizar por un ingeniero en prácticas, nuevo en la empresa, y cuyo cometido es exclusivamente desarrollar ambas plataformas. Todo esto quedará reflejado posteriormente en el presupuesto.

El proyecto se dividió en tres fases:

- **Fase preliminar**: preparación al diseño de las plataformas. Se divide en las siguientes tareas:
    - Acomodación a los recursos de la empresa: Durante esta fase, el ingeniero en prácticas debe conocer la empresa, su composición, los departamentos, y, sobre todo, de qué recursos dispone, a quién puede acudir, qué protocolos existen.
    - Estudio de las tecnologías: Estudio en profundidad del protocolo H.323. Revisión del protocolo SIP, así como otras tecnologías VoIP.
    - Análisis del mercado de la VoIP: Estudio de las posibilidades del mercado VoIP, fabricantes y ofertas en relación al protocolo H.323, características habituales de equipos, equipos de bajo y alto coste, equipos orientados a PYMES y a corporaciones.
    - Estudio de equipos Quintum Tenor: Estudio en profundidad de las opciones de configuración, *firmware*s, interfaces, características, etc de los equipos Quintum Tenor que van a utilizarse en los proyectos de interfonía; uso de los diversos manuales de configuración. Base de estudio en pruebas sobre maqueta.
    - Construcción de la maqueta de interfonía: Esta tarea se desarrolla en paralelo con el estudio de las necesidades de los proyectos requeridos, y consiste en el desarrollo de una maqueta de interfonía a la cual poco a poco van añadiéndose nuevos elementos, probándose, examinando en profundidad su comportamiento, etc.

- **Fase de Diseño**: preparación completa de las plataformas de interfonía, dispuestas para su instalación. Tareas:
    - Selección de terminales: A continuación vuelve a examinarse el mercado de la VoIP para encontrar los terminales más apropiados a los equipos Quintum

Tenor y a las plataformas Barrio de las Letras y Estación Bailén Metro de Valencia: se requieren terminales económicos, compatibles, y acordes a las necesidades.

- Adquisición de terminales: Compra o petición en pruebas de terminales y pruebas de los mismos en la maqueta de interfonía, comprobando interoperabilidad, robustez, funcionamiento; examinando trazas y resolviendo errores.
- Montaje de la maqueta completa: Una vez finalizada la selección de los terminales y su validación, se pasa a montar una maqueta completa, con todos los equipos destinados a la futura instalación, sobre una red cargada (la red interna de la empresa), para cada plataforma.
- Pruebas FAT: *Factory Acceptance Test*, pruebas en fábrica sobre las maquetas completas: durante tres semanas se someterá la maqueta a pruebas como resistencia y robustez temporal, generadores de llamadas, generadores de tráfico masivo, desconexiones de la corriente eléctrica y de la red, y todo tipo de llamadas dentro de la propia maqueta; se medirán niveles de calidad en la forma de retardos, nivel de ruido y ecos, y calificación subjetiva del audio. Y en caso de errores, se subsanarán.

- **Fase de instalación y redacción de informes**: instalación de las plataformas, y resolución de los inconvenientes surgidos en campo. Dos tareas:
  - Instalación y redacción de informes: Los instaladores llevarán los equipos a las salas de máquinas, y los conectarán siguiendo las indicaciones del ingeniero en prácticas.
  - Redacción de informes: Desde aquí hasta el fin de la actividad laboral, el ingeniero en prácticas se dedicará a la elaboración de una documentación en la que se reflejarán todos los pasos de diseño y configuración de los equipos usados en varios documentos internos. Dichos documentos se incluyen en los archivos adjuntos al proyecto, llamados `Cuaderno de configuración de un sistema de interfonía H323 Quintum Tenor.pdf` y `Preguntas de Uso Frecuente para un sistema de interfonía H323 Quintum Tenor.pdf`, en la carpeta `Archivos Adjuntos`.
  - Pruebas SAT: Se realizarán pruebas de conectividad, de calidad del audio y de comunicación. Son pruebas mucho más sencillas que las FAT, orientadas a resolver dificultades que no se habían pensado por sencillas o por depender de las condiciones específicas de los emplazamientos.

Todos estos aspectos pueden observarse concienzudamente en el archivo `Project1.mpp` adjunto, para Microsoft Project, del cual se han obtenido las siguientes gráficas:

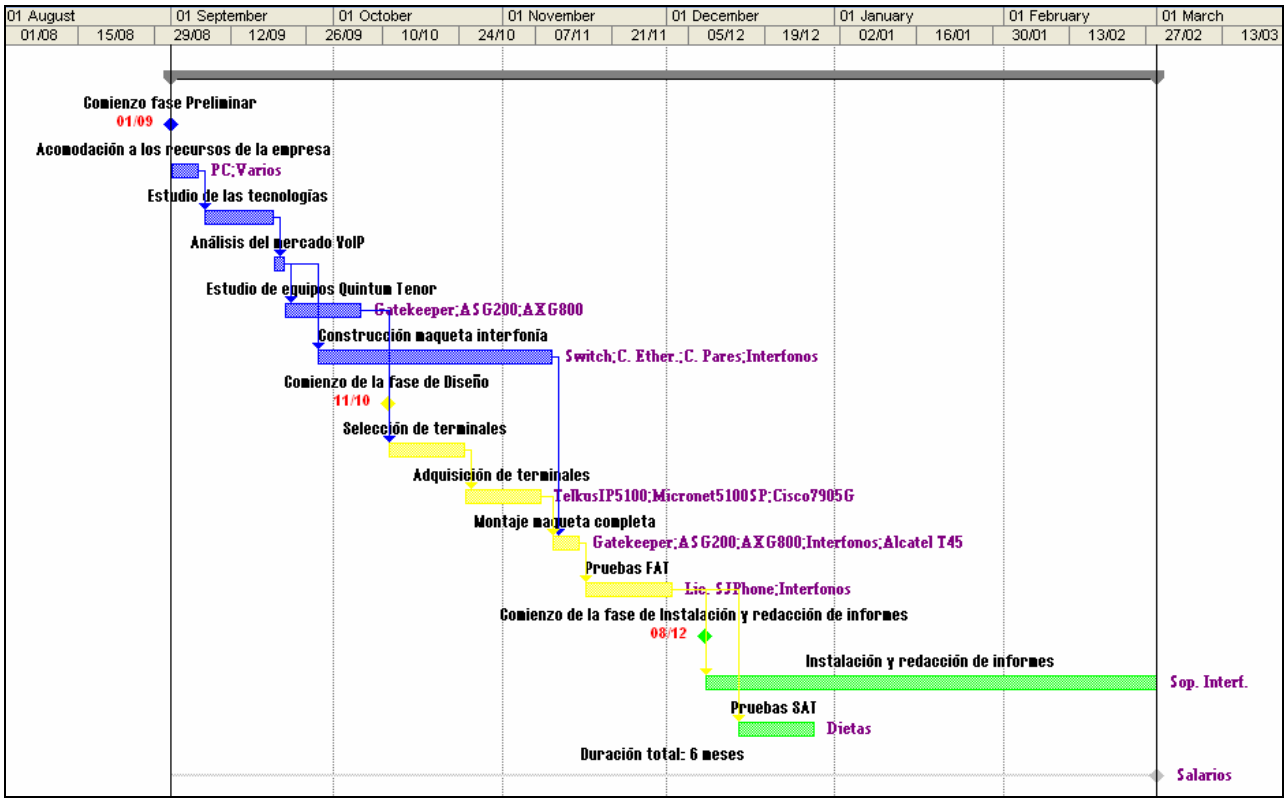


Figura 103: Diagrama de Gannt para el proyecto completo.

Task Usage

Task Name	Duration	Actual Cost	Details	4th Quarter			1st Quarter	
				Sep	Oct	Nov	Dec	Jan	Feb
Plataforma de Interfonía VoIP	**101 days**	**13.250,69 €**	Work	22,49d	22,49d	23,81d	19,84d	23,81d	21,16d
			Cost	2.899,82 €	1.707,41 €	5.660,12 €	1.103,08 €	995,43 €	884,83 €
Comienzo fase Preliminar	0 days	0,00 €	Work						
			Cost						
Acomodación a los recursos de la empresa	2 days	1.059,00 €	Work						
			Cost	1.059,00 €					
Estudio de las tecnologías	7 days	0,00 €	Work						
			Cost	0,00 €					
Análisis del mercado VoIP	2 days	0,00 €	Work						
			Cost	0,00 €					
Estudio de equipos Quintum Tenor	8 days	2.074,64 €	Work						
			Cost	1.296,65 €	777,99 €				
Construcción maqueta interfonía	25 days	188,30 €	Work						
			Cost	15,06 €	128,04 €	45,19 €			
Comienzo de la fase de Diseño	0 days	0,00 €	Work						
			Cost						
Selección de terminales	8 days	0,00 €	Work						
			Cost		0,00 €				
Adquisición de terminales	8 days	544,53 €	Work						
			Cost		272,27 €	272,27 €			
Montaje maqueta completa	2 days	4.519,09 €	Work						
			Cost			4.519,09 €			
Pruebas FAT	10 days	292,60 €	Work						
			Cost			263,34 €	29,26 €		
Comienzo de la fase de Instalación y redacción de informes	0 days	0,00 €	Work						
			Cost						
Instalación y redacción de informes	45 days	1.088,00 €	Work						
			Cost				265,96 €	435,20 €	386,84 €
Pruebas SAT	8 days	341,00 €	Work						
			Cost				341,00 €		
Duración total: 6 meses	101 days	3.143,53 €	Work	22,49d	22,49d	23,81d	19,84d	23,81d	21,16d
			Cost	529,11 €	529,11 €	560,23 €	466,86 €	560,23 €	497,98 €

Figura 104: Tabla de usos de tareas y presupuestos asociados a cada una de ellas.

4.2 Presupuesto

El presupuesto del presente proyecto incluye el valor de alguno de los recursos humanos implicados en el mismo: no se reflejan en él los costes asociados a la selección de personal, ni de asesoramiento parcial del ingeniero en prácticas por parte de otros activos de la empresa.

El cálculo completo lo dejo en la hoja de cálculo `Presupuesto1.xls` adjunta; de ella se ha extraído la siguiente tabla:

	PRESUPUESTO		
	En el presente presupuesto no se incluyen ni la mano de obra asociada a la instalación, ni los costes pre/post dedicación estrictamente becarial.		
	Partida 1.-SALARIOS		
	Salarios correspondientes a la contratación de un becario durante el período de 4 meses (relacionados con el tiempo dedicado a los proyectos presentados).		
Ud.	*Concepto*	*P.Unitario*	*Subtotal*
6	Meses en régimen de prácticas	400,00	2400,00
		Total 1:	2400,00
	Partida 2.-EQUIPAMIENTOS ACCESORIOS		
	Equipos suministrados al becario para la realización de pruebas y estudios, sin relación posterior con la instalación de equipos, y algunos de ellos por tanto reutilizables posteriormente en la empresa.		
Ud.	*Concepto*	*P.Unitario*	*Subtotal*
1	Ordenador personal	1.000,00	1.000,00
2	Cuadernos de anillas	2,00	4,00
3	Bolígrafos	2,50	7,50
20	Cables ethernet de entre 1 y 5 metros	1,00	20,00
15	Cables de pares trenzados de entre 1 y 5 metros	0,50	7,50
2	Teléfonos analógicos sencillos	10,00	20,00
2	Switches de 20 puertos	100,00	200,00
		Total 2:	1259,00
	Partida 3.-EQUIPAMIENTOS INSTALADOS		
	Equipos de prueba que posteriormente fueron usados para su instalación en campo (o bien fueron desechados por malfuncionamiento).		
Ud.	*Concepto*	*P.Unitario*	*Subtotal*
1	Teléfono analógico Alcatel Temporis 45	43,95	43,95
1	Teléfono IP Telkus Totalfon IP5000	137,90	137,90
1	Teléfono IP Micronet 5100 SP	153,20	153,20
1	Teléfono IP Cisco 7905G + fuente alimentación + licencia H.323	235,43	235,43
2	Quintum Tenor Gatekeeper con licencia para 20 puertos simultáneos	639,26	1.278,52
8	Quintum Tenor ASG200	389,95	3.119,60
2	Quintum Tenor AXG800	1.045,43	2.090,86
1	Licencia SJPhone	95,00	95,00
21	Interfonos Viking 1600 A	15,20	319,20

13	Estructuras metálicas de seguridad para instalación en estación	25,00	325,00
8	Estructuras metálicas de seguridad para instalación en calle	95,43	763,44
		Total 3:	8562,10
	Partida 4.-DESPLAZAMIENTOS Y DIETAS		
	Durante la fase de instalación y pruebas SAT, se le dotó al becario de dietas asociadas a desplazamientos y comidas.		
Ud.	*Concepto*	*P.Unitario*	*Subtotal*
8	Menús	8,50	68,00
3	Traslados a Valencia (gasolinas): 350 km x 2 x 0,13 €/km	91,00	273,00
		Total 4:	341,00
	TOTAL PRESUPUESTO		12.562 Euros

5. Conclusiones

Durante este proyecto se han diseñado y configurado dos plataformas de interfonía sobre comunicaciones de VoIP, que además han sido instaladas y verificadas por Revenga Ingenieros S.A. y actualmente se encuentran en funcionamiento.

Además, se ha analizado en profundidad el estado de la VoIP en cuando a mercado y tecnologías, así como sus distintas posibilidades de aplicación. Es importante señalar que nos encontramos actualmente ante la paulatina introducción de la VoIP en las nuevas tecnologías, y que todos estos análisis y estudios, así como las dificultades surgidas ante el equipamiento e integración de las dos plataformas presentadas, muestran la tendencia de la VoIP a corto y a medio plazo.

La ingeniería de integración de sistemas, en el marco de la VoIP, también ha sido analizada en cuanto a que representa la alternativa elegida para la implementación de estos sistemas de interfonía, frente a otros modelos de trabajo más sencillos como son los modelos de *renting* o la selección de un protocolo de comunicaciones propietario y su respectivo fabricante único.

Este proyecto supone el análisis e introducción de un modelo básico para sistemas de VoIP, a partir del cual se presentan las dificultades y características principales inherentes a estas comunicaciones.

A continuación se presentan algunas ampliaciones propuestas sobre este proyecto básico.

5.1 Ampliaciones al presente proyecto

A partir de este proyecto básico de plataformas de interfonía pueden desarrollarse numerosas nuevas aplicaciones de ingeniería, todas ellas relacionadas con la generación de servicios suplementarios que aporten un valor añadido a las redes de interfonía.

5.1.1 Integración con la centralita Asterisk

Este proyecto consistiría en dotar a la red de interfonía/telefonía de un servidor con una centralita Asterisk, centralita de software libre, que soporta H.323 y SIP entre otros, y que presenta funciones tan interesantes como grabación, parking y monitorización de llamadas.

De cara a un cliente de redes de interfonía, es importante conocer el comportamiento de sus empleados, tanto en cuanto a la ocupación de los recursos humanos como en cuanto a la

calidad de su comportamiento laboral. La grabación y monitorización de llamadas puede ser muy útil a este respecto.

Por otro lado, la generación de estadísticos de operación también sería muy interesante. Para ello es necesario tener acceso a todas las llamadas cursadas por la red, aspecto del que se encarga precisamente una centralita.

Por otro lado, las pruebas de robustez deben ser muy potentes, pues la estabilidad del sistema es fundamental en este tipo de redes. Pero, una vez conseguida, podrían suprimirse los Gatekeepers, sustituyéndolos por centralitas Asterisk.

5.1.2 Interfonía para la tercera edad. Interfonía residencial

A partir de la integración con la centralita Asterisk presentada en el apartado anterior, podría asumirse el diseño de una aplicación de interfonía dedicada a la conexión con la PSTN y con las redes móviles, en la que se incluyan capacidades como la aplicación de políticas de conmutación en función del origen, destino, o franja horaria, etc. Así podría construirse un diseño destinado a la operación avanzada de, por ejemplo, porteros automáticos para el acceso residencial, o incluso interfonos especiales para la tercera edad (capaces de comunicarse con el familiar independientemente de su ubicación).

Para estas aplicaciones avanzadas, la parte más importante reside en el diseño de un portal de acceso web de cara al usuario, sobre el cual éste pueda modificar las políticas de conmutación en función de sus intereses. La integración de este portal con el funcionamiento de la centralita debe presentar asimismo un resultado robusto y fiable, con funciones de seguridad. Este proyecto podría significar un interesante avance en ingeniería domótica.

5.1.3 Integración con red Wi-Fi

Otro interesante proyecto de ampliación podría ser, partiendo de una de estas redes de telefonía ya configurada, su integración con una red Wi-Fi, es decir, con puntos de acceso y routers Wi-Fi, midiéndose la calidad de las comunicaciones cuando se atraviesa un espacio con distintas características de pérdida de conectividad e interferencias. A esta red podría añadirse algún terminal H.323 Wi-Fi, y sobre éste medirse zonas de cobertura.

5.1.4 Red WAN de telefonía

El cuarto y último proyecto de ampliación del presente consiste en el diseño de una red de telefonía VoIP WAN que tenga que atravesar Internet para la comunicación entre sedes de una empresa. Para este proyecto es necesaria una auditoría de red, tal como se describe en

el Apéndice A, y muchas consideraciones de seguridad en las comunicaciones. La red podría ser tan grande como se quisiera, y podría destinarse a conectar, por ejemplo, todas las sedes de la Universidad de Sevilla entre sí.

Apéndice A: Auditorías de VoIP

Una auditoría de red evalúa la calidad que tendría un cierto tráfico de VoIP sobre una red de datos.

Antes de desplegar una red VoIP es prácticamente imprescindible realizar una auditoría de red, para analizar las características de los equipos y de las conexiones involucradas en la red sobre la que se pretende desplegar un servicio de telefonía. No se puede olvidar que esta red de telefonía va a circular sobre una red que también tendrá que soportar tráfico de datos.

Una auditoría VoIP partirá de un análisis de la red de datos existente: equipamiento, flujo de datos (topología, picos de tráfico y tráfico medio), y hará una estimación del volumen de tráfico de voz a añadir. A continuación hará una simulación real y análisis del comportamiento del nuevo tráfico de voz, midiendo la calidad de las comunicaciones. Se recomienda simular la red durante dos semanas como mínimo.

A partir de los resultados, se podrán elaborar una serie de recomendaciones con el objeto de adaptar la red a las necesidades de la VoIP.

A.1 Requisitos de la telefonía sobre una red IP

Los requisitos de la telefonía sobre una red IP son:

- **Ancho de banda**: En una red VoIP puede escogerse el códec deseado en función de las características de la red. En una red local donde el ancho de banda no resulte crítico puede usarse G.711, pero cuando se atraviesan segmentos WAN, donde el ancho de banda resulta mucho más costoso, la compresión es fundamental.

  A continuación se muestra una tabla con el consumo de ancho de banda en comunicaciones de voz en función del códec (figura A1):

Codec de Audio	Ancho de Banda comprimido	Ancho de Banda paquetizada	Ancho de Banda en Ethernet
G723	6,3 Kb/s	17 Kb/s	27,2 Kb/s
G729	8 Kb/s	24 Kb/s	28,8 Kb/s
G711	64 Kb/s	74,6 Kb/s	84,7 Kb/s
FAX	4,8 Kb/s	12,8 Kb/s	20,4 Kb/s

Figura A1: Consumo de ancho de banda en comunicaciones de voz en función del códec.

  El ancho de banda también puede reducirse hasta un 30% cuando se utiliza supresión de silencios. Y, en líneas WAN, algunos Routers pueden utilizar compresión de las cabeceras IP (cRTP), reduciéndolas de 40 a 24 bytes.

- **Retardo y Jitter**: Los equipos de red, Routers y cortafuegos, debido a la prioridad del flujo y a los picos de tráfico, pueden perder paquetes de datos, produciendo retardos en la transmisión. El retardo debe ser inferior a 400ms. Además, la variación del retardo (Jitter) da lugar a efectos distorsionantes que también disminuyen la calidad de la comunicación de voz. El Jitter debe ser inferior a 50ms.

  Se muestra a continuación una tabla con los parámetros de calidad debidos al retardo (figura A2):

	Calidad Alta	Calidad Media	Calidad Baja
Pérdida de Paquetes	1 %	3 %	5 %
Retardo	150 ms	400 ms	600 ms
Jitter	20 ms	50 ms	75 ms

Figura A2: Parámetros de calidad en las comunicaciones VoIP en función del retardo y del Jitter.

Por otro lado, y relacionado con el ancho de banda, las redes de datos no deben cargarse a más del 80 % de su capacidad, o las características del retardo aumentarán ostensiblemente.

A.2 Recomendaciones de hardware

Existen una serie de recomendaciones básicas sobre el equipamiento de la red destino que se enumerarán a continuación:

- Los hubs, al replicar todos los paquetes por cada uno de sus puertos, no son nada aconsejables; todos los hubs de la red deberían ser cambiados por switches.
- A su vez, los switches deberán tener capacidades de 100 Mbps en Full Duplex, para que la red no infiera en dificultades asociadas al ancho de banda. Asimismo deberán permitir algún protocolo de calidad de servicio, (como 802.1p/Q o DiffServ), acorde con el protocolo de calidad de servicio permitido en el equipamiento VoIP que vaya a ser utilizado en el despliegue de la red VoIP. Por último, deberán ser capaces de utilizar VLANs[56] para separar el tráfico de telefonía del resto del tráfico, en los casos en que sea posible.
- Las direcciones IP contratadas con el operador deberán ser fijas.
- Por último, los switches, routers, y cortafuegos, deben poder trabajar a “velocidad del cable”, es decir que la velocidad de salida de los paquetes se produzca a la misma velocidad de entrada, y apenas sin retardos de transmisión.

[56] VLAN: *Virtual* LAN, redes de área local virtuales.

A.3 Software para auditorías VoIP

Existen poderosas herramientas comerciales que monitorizan todos los elementos de la red, y que pueden ofrecer estadísticos globales de tráfico y calidad de servicio [76].

Como ejemplo, se introducirán los siguientes programas:

- Clear Sight Analizer [77]
- NetIQ Vivinet Diagnosis [78]
- BrixMon [79]
- Hammer Call Analizer [80]

A.3.1 Clear Sight Analyzer

Con una colocación estratégica (insertando un HUB entre el servidor que lo contenga y los switches principales de la red, o de otra forma, el tráfico no pasará por él), este programa puede reconocer y capturar el tráfico deseado. El esquema necesario se muestra en la figura A3:

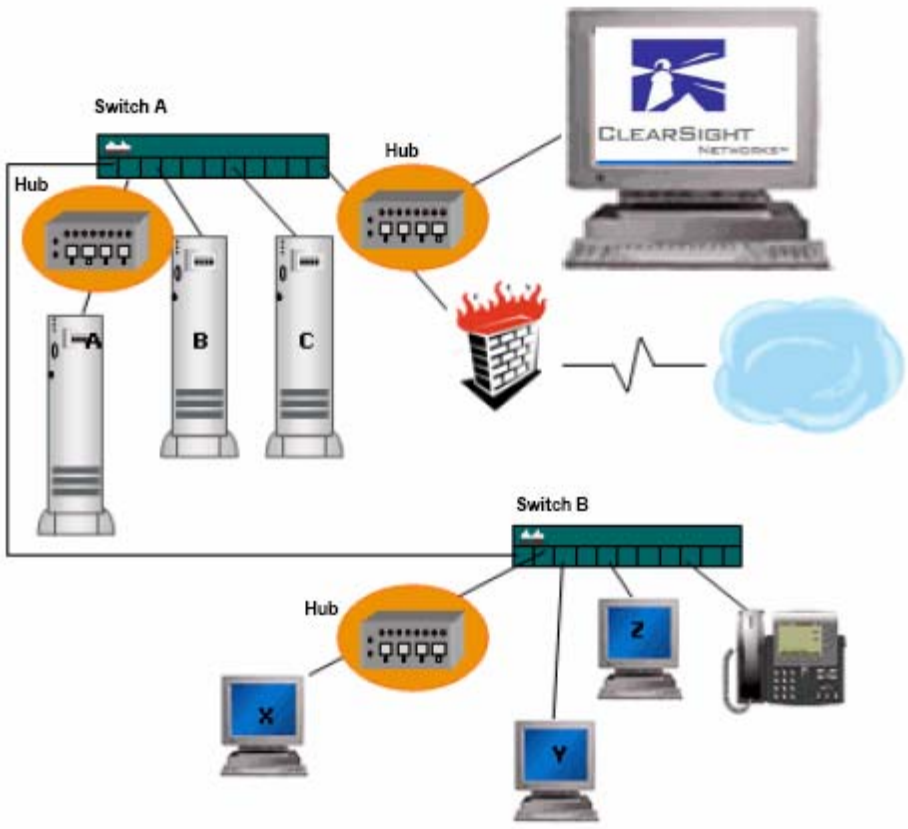


Figura A3: Esquema de funcionamiento para el programa de auditorías VoIP ClearSight.

Este programa, en su versión de prueba, se adjunta en el CD de documentación, en la carpeta `Archivos Adjuntos\Varios\Software Auditorías de red\Clear Sight Analyzer`, archivo `CSA411-Trial.zip`, con su contraseña como el ejecutable

`AnalysisCenter20SP1a-CD-pwd.exe`, así como manuales de uso `ClearSight_GSG.pdf`, `ClearSight_QuickInstall.pdf` y su *datasheet* `ClearSight_Brochure_p1-4.pdf`.

Mientras se mantenía una llamada entre el SJPhone y el Micronet 5100SP se ha tomado una captura de la red (figura A4):

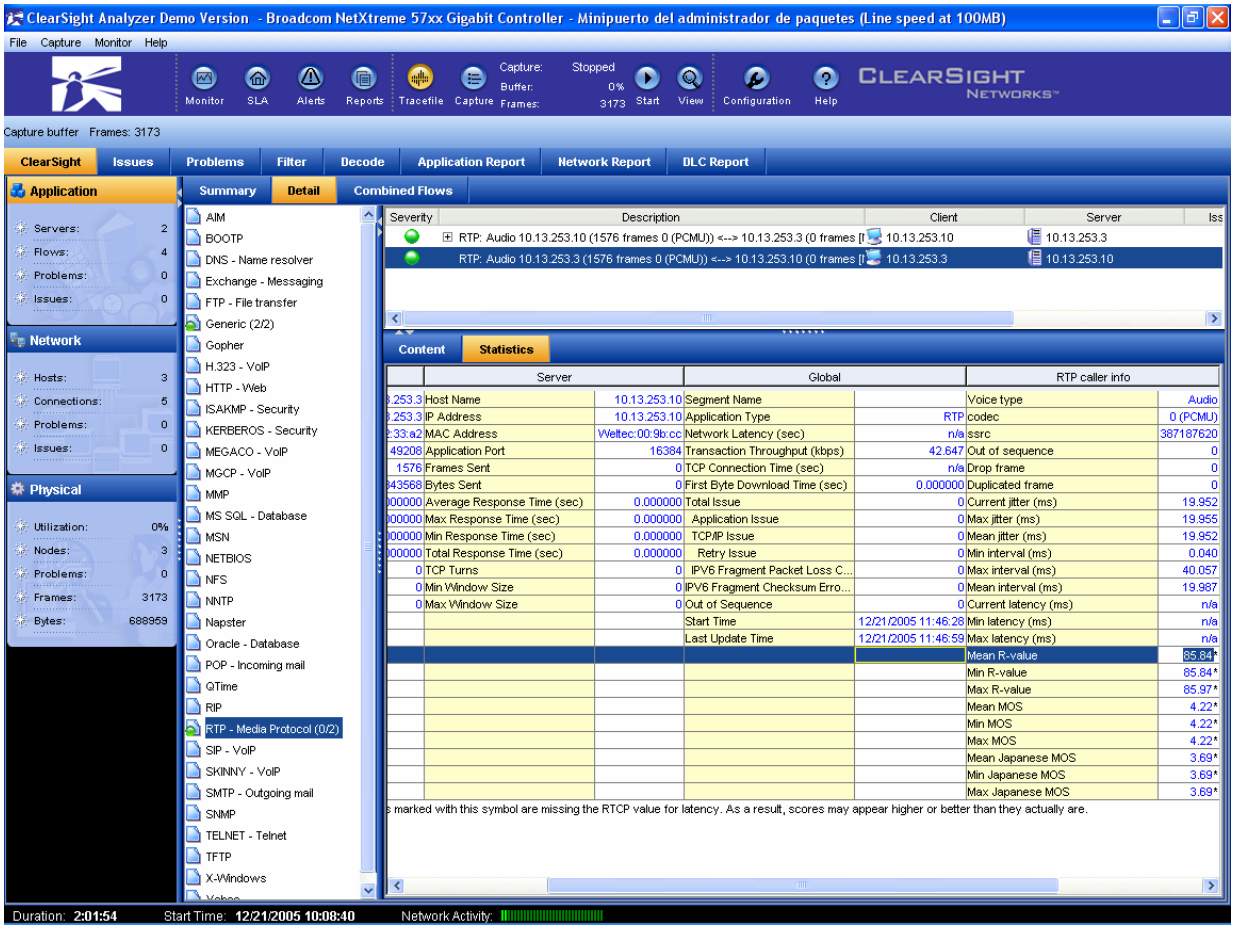


Figura A4: El Programa para auditorías de red ClearSight: pestaña Detalles.

La pantalla mostrada es un programa en versión de *trial* (sólo proporcionan 5 días de prueba) mediante la que se han obtenido, por ejemplo, parámetros como el MOS[57] (de 1 a 5) y el factor R (de 0 a 100), que no representan sino medición de la calidad de una llamada RTP, conforme con la recomendación ITU-T G.107. También muestra jitter y retardos máximo, mínimo y medio, además de diversos detalles adicionales (figura A5):

[57] MOS: *Mean Opinion Score*.

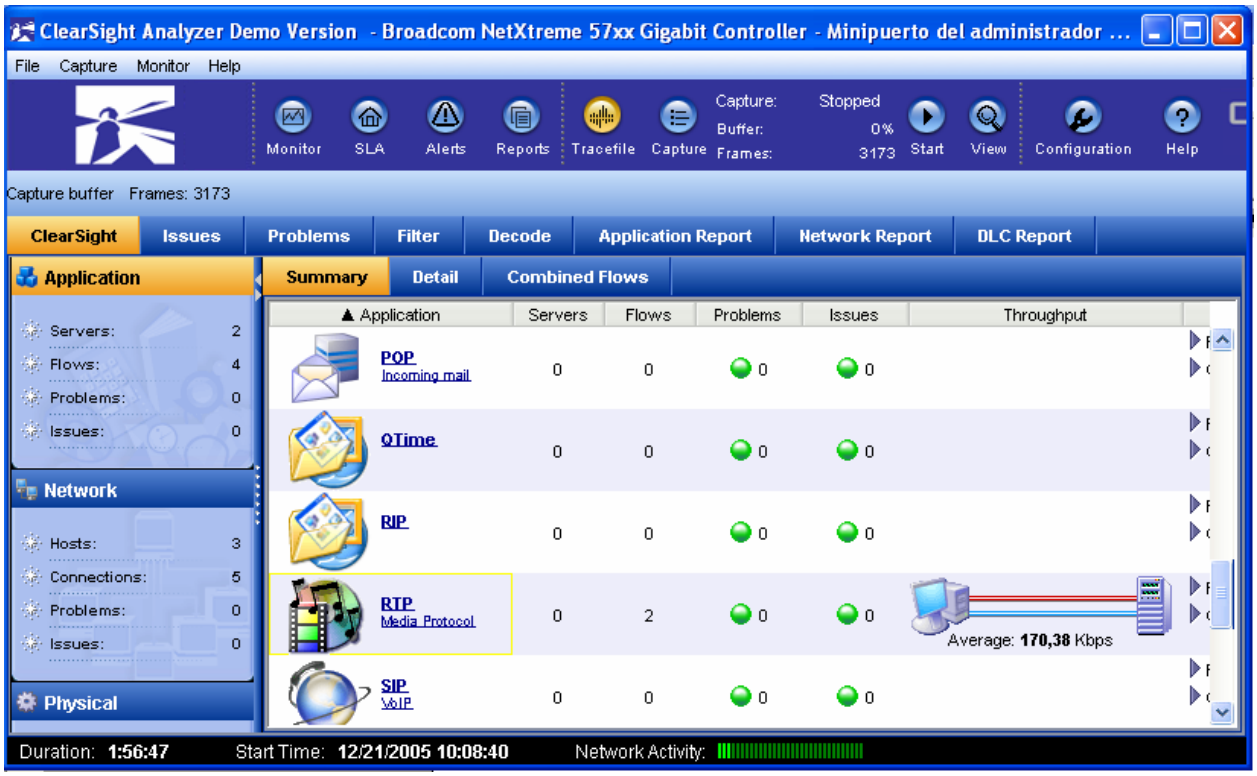


Figura A5: El Programa para auditorías de red ClearSight: pestaña Sumario, monitorización en tiempo real.

En la anterior captura se ha mostrado cómo, con un códec G.711, la llamada alcanza los 85 Kbps ethernet en cada sentido.

A.3.2 NetIQ Vivinet Diagnosis

En realidad, hay que reconocer que la opción de ClearSight, que en el mejor caso necesita de un hub, no siempre es viable. La compañía NetIQ posee, entre otras, la herramienta NetIQ Vivinet Diagnosis, que monitoriza una llamada que falla, analizando el problema en cuanto a congestión de los enlaces o a parámetros de calidad de servicio, y establece un resultado (figura A6).

Una demostración de este programa se incluye en el CD de documentación, en la carpeta `Archivos Adjuntos\Varios\Software Auditorías de red\NetIQ Vivinet software`, archivo `vivinetassessor.exe`, así como el documento relacionado `DS_VivinetAssessor_FEB05pdf.pdf`.

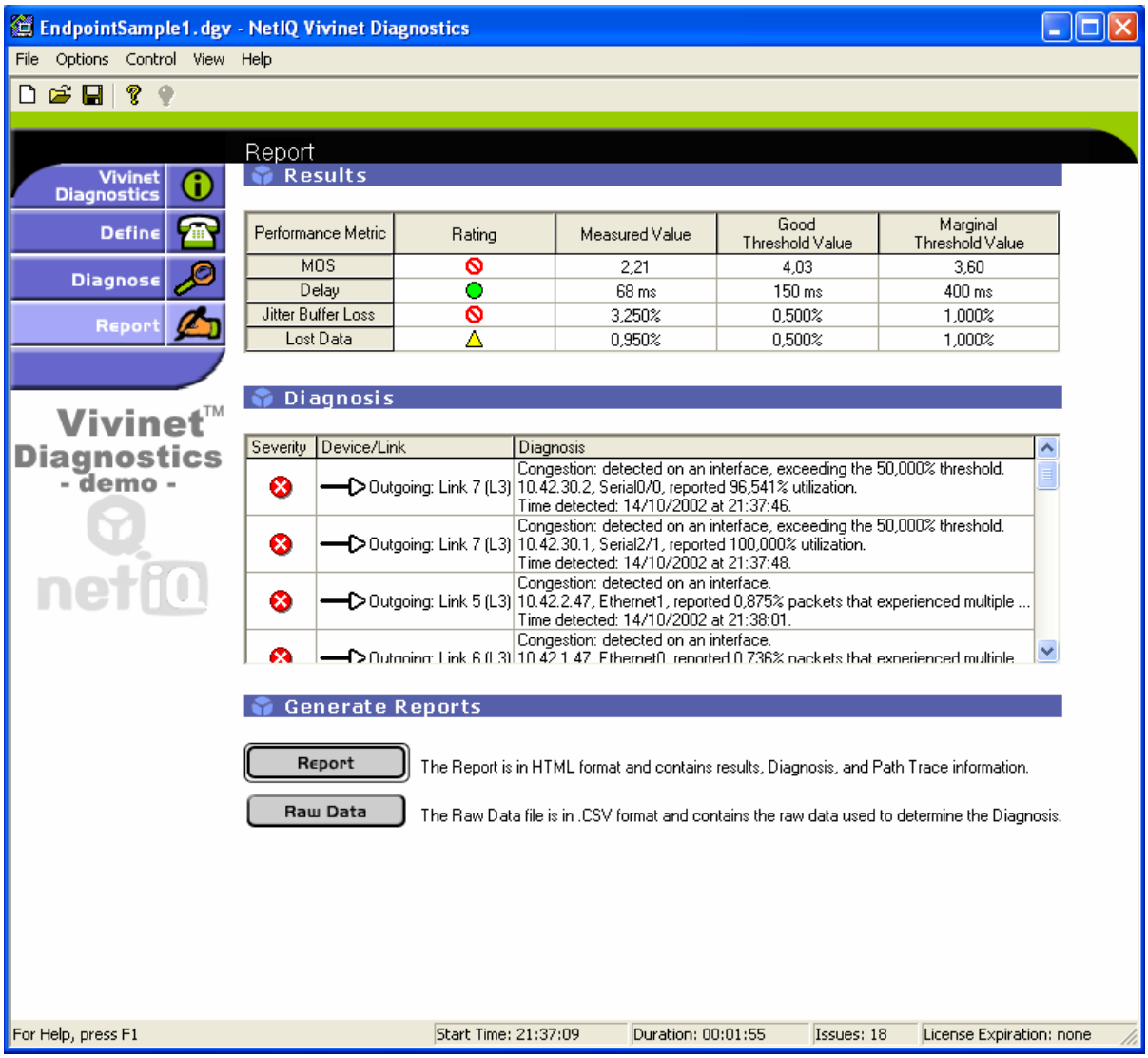


Figura A6: El Programa para auditorías de red de NetIQ Vivinet Diagnostics.

A.3.3 BrixMon

Brixnet se ha especializado en el desarrollo de herramientas para la monitorización y el control de redes VoIP, desde proveedores de servicio hasta nivel de empresa. Entre ellas, el BrixMon monitoriza en tiempo real la calidad de servicio de las llamadas VoIP activas en el sistema (figura A7).

Su datasheet se incluye en el archivo `Brixnet BrixMon DataSheet.pdf` de la carpeta `Archivos Adjuntos\Varios\Software Auditorías de red`, en el CD de documentación.

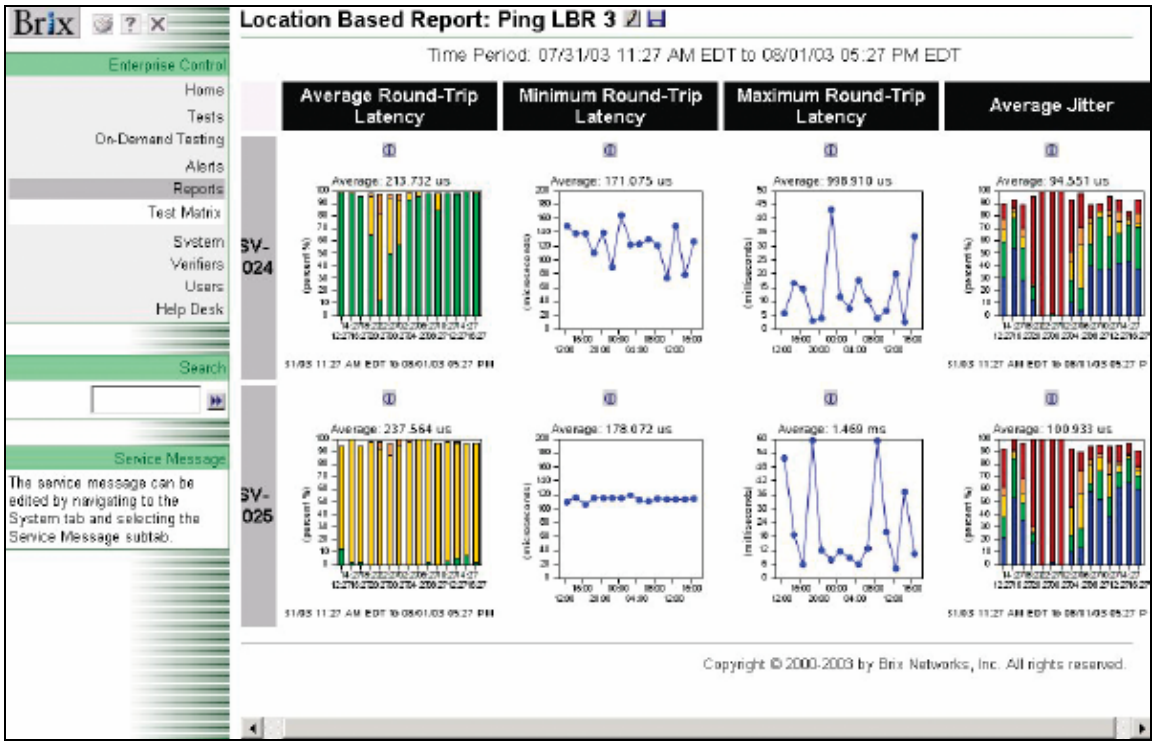


Figura A7: El Programa para auditorías de red Brixmon, de Brixnet.

A.3.4 Hammer Call Analizer

Por último, se introducirá el Hammer Call Analizer [81], de Empirix, optimizado para VoIP. Presenta una interfaz en protocolos muy potente, sobre la cual un experto en protocolos podrá encontrar rápidamente el sentido de un error (figura A8).

Este programa se incluye también en la documentación, en la carpeta `Archivos Adjuntos\Varios\Software Auditorías de red\Empirix Hammer Call Analyzer`, archivo `HammerCAzip.exe`, así como su datasheet `ds_hca.pdf`.

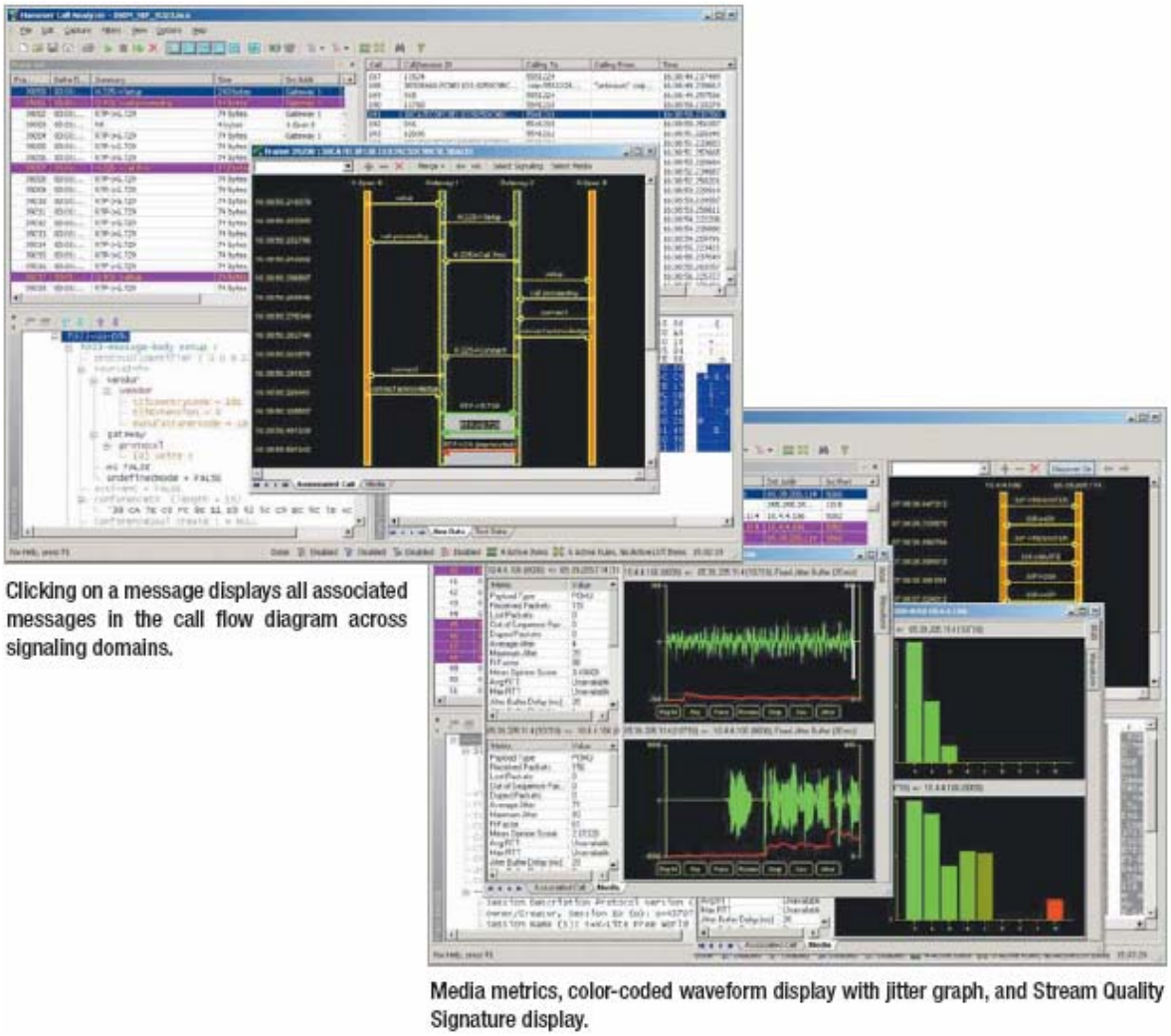


Figura A8: El Programa para auditorías de red Hammer Call Analizer, de Empirix.

Archivos adjuntos

Se presenta a continuación un listado de archivos adjuntos en CD al presente proyecto:

- Directorio raíz:
    - **Contenidos de este CD.pdf**: documento en el que se describen los contenidos del CD adjunto al presente proyecto.
    - **Diseño y Configuración de dos Plataformas de Interfonía H.323.pdf**: el presente documento.
    - **Presupuesto1.xls**: hoja de cálculo que almacena el presupuesto del proyecto completo.
    - **Project1.mpp**: documento Microsoft Project con el diagrama de Gannt del proyecto.
    - <DIR> Archivos Adjuntos.

- Directorio raíz Archivos Adjuntos:
    - **Cuaderno de configuración de un sistema de interfonía H323 Quintum Tenor.pdf** y **Preguntas de Uso Frecuente para un sistema de interfonía H323 Quintum Tenor.pdf**: Archivos redactados para Revenga Ingenieros S.A. en los que se detalla el significado de los parámetros de configuración de las pasarelas Quintum Tenor, y algunas preguntas sobre cómo resolver problemas prácticos.
    - **Presupuesto1.xls**: Hoja de cálculo con el presupuesto del proyecto.
    - **Project1.mpp**: Archivo Microsoft Project con el diagrama de Gannt del proyecto completo.
    - <DIR> Bibliografía: Carpeta con todos los archivos y artículos incluídos en como documentación en la bibliografía.
    - <DIR> Cisco 7905G: Carpeta con todos los archivos de configuración, manuales y *datasheets* relacionados con este teléfono IP.
    - <DIR> Quintum Technologies: Carpeta con los archivos de configuraición, manuales y *datasheets* relacionados con este fabricante y sus equipos Quintum Tenor.
    - <DIR> SJ Phone: Carpeta con el instalador para Windows XP y manuales de este teléfono IP.

- <DIR> Viking 1600A: Carpeta con información relativa a los interfonos Viking.
- <DIR> Varios: Otros programas y documentos.

- <DIR> Documentación:
  - "ITU-T H.323 draft V5(5/2003)", ITU-T, Mayo 2003: archivo **h323V5consented.zip**.
  - "ITU-T H.225.0 draft V5(5/2003)", ITU-T, Mayo 2003: archivo **H.225.0v5-wcm.zip**.
  - "ITU-T H.245 draft V9(10/2002)", ITU-T, Octubre 2002: archivo **H245Version9.zip**.
  - "ITU-T H.450.1 Generic Functional Protocol for the Support of Supplementary Services in H.323", ITU-T, Septiembre 1997: archivo **H4501wht_6.zip**.
  - "ITU-T H.460.1 Guidelines for the Use of the Generic Extensible Framework", ITU-T, Febrero 2002: archivo **H460-1-v7-revOD.zip**.
  - "ITU-T X.680 Information Technology - Abstract Syntax Notation One (ASN-1): Specification of Basic Notation", ITU-T, Julio 2002: archivo **X.680-0207.pdf**.
  - "Service Architectures in H.323 and SIP: A Comparison", J. Glasmann, H. Müller, Munich University of Technology, Diciembre 2004: archivo **h323-sip comparison.pdf**.
  - "Basic Architecture of H.323", C. Schlatter, Switch The Swiss Education and Research Network, Junio 2003: archivo **h323_basics_handout.pdf**.
  - "Overview of H.323", Febrero 2003, Paul E. Jones, Packetizer: archivo **overview_of_h323.ppt**.

- <DIR> Cisco 7905G:
  - **datasheet.pdf**: *datasheet*.
  - **7905_H323.pdf**: manual de configuración H.323.
  - <DIR> Archivos de licencia H323: contiene los archivos de configuración necesarios para la carga del protocolo H.323 en el teléfono IP, en el archivo **CP7905010002H323040927A.zip**.
  - <DIR> Carga de configuración H323: contiene los archivos de licencia necesarios para llevar a cabo la carga de la configuración H.323, así como los archivos de configuración **lddefault.txt** y **lddefault.cfg** (compilado).
  - <DIR> protocolo SIP: los mismos archivos y directorios antes señalados pero para el protocolo SIP.

- <DIR> Quintum Technologies:

- <DIR> Autenticación y tarifado:
  - **Billing_Authentication_Handbook.chm**:se trata de un documento de información sobre la autenticación y el tarifado en equipos Quintum Tenor.
  - <DIR> Servidor CDR desarrollado por Quintum Technologies: contiene un servidor CDR desarrollado por Quintum Technologies con manual, código fuente en C++, y ejecutable para Win32.
  - <DIR> Servidores RADIUS: contiene el documento de la RFC 2865 para el protocolo RADIUS, y varios servidores RADIUS *freeware* con sus respectivos manuales:
    - <DIR> FreeRADIUS: Servidor RADIUS para correr sobre Linux (archivo **freeradius-1.0.1.tar.gz**).
    - <DIR> GnuRadius: Servidor RADIUS desarrollado por GNU, (archivo gnu **radius-1.3.tar.gz**), también sobre Linux.
    - <DIR> ClearBox TACACS_RADIUS: Servidor RADIUS sobre plataformas Windows (archivo **ClearBox TACACS_RADIUS Server for Windows v2.4.zip**).
- <DIR> Manuales y documentos Gatekeeper:
  - **GateKeeper_SpecSheet-0104.pdf**: *datasheet*.
  - **IDsoftware_Version_Analog-Digital_Tenor.pdf**: pequeño documento sobre cómo determinar la versión del software del Quintum Tenor Gatekeeper.
  - **Materials_Guides_gkuserguide.pdf**: manual.
  - **Quintum_Gatekeeper_Architecture.pdf**: documento que especfica el comportamiento de una red Quintum con varios Gatekeepers simultáneos.
  - **Software_Loading_Instructions_10-2001.pdf**: instrucciones para cargar una nueva versión del *firmware*.
- <DIR> Manuales y documentos Pasarelas:
  - **Quintum_Tenor_CLI_Guide_P102-11-00.chm**: manual de configuración.
  - <DIR> ASG200:
    - **d__Materials_Data Sheets_AS Series.pdf**: *datasheet*.
    - **d__Materials_Guides_TenorASuserguide.pdf**: manual.
    - **d__Materials_Quick Start Guides_TenorASquickstart.pdf**: pequeño documento sobre cómo arrancar inicialmente la pasarela.
    - **TenorASuserguide.pdf**: guía de usuario.
  - <DIR> AXG800:
    - **TenorAX-10-04.pdf**: *datasheet*.

- **tenoraxquickstart.pdf**: pequeño documento sobre cómo arrancar inicialmente la pasarela.
- **Tenoraxuserguide.pdf**: manual.

▪ <DIR> Tenor Configuration Manager:

- **CM103-07-02.zip**: instalador para Windows del programa *Tenor Configuration Manager*.

▪ <DIR> Varios: Contiene algunos documentos de información sobre comportamientos y funcionamiento interno Quintum:

- **Tenor_Call_Routing.pdf**: información sobre cómo los Quintum Tenor rutan sus llamadas.
- **Tenor_Interoperability.pdf**: configuraciones para permitir la interoperabilidad con algunos fabricantes.
- **Tenor_MFG_Test_Procedures.pdf**: procedimiento para test de fábrica de equipos Quintum Tenor.
- **Disconnect_Supervision.pdf**: documento sobre el funcionamiento de este apartado de comunicación analógica.
- **Tenor_MFG_Test_SecondGen.pdf**: procedimiento para test de fábrica de equipos Quintum Tenor de segunda generación.

▪ <DIR> Version del software AS-AX-GK: contiene las versiones del *firmware* de estos equipos.

- <DIR> Gatekeeper-P4-2-20-40: *firmware* para el Gatekeeper (archivo **tg-sy-p4-2-20-40qt-lec.bin**) e instrucciones.
- <DIR> AS_AX-P102-11-08: *firmware* para estos equipos.

- <DIR> SJ Phone:
  - **SJphone-289a.exe**: instalador para Windows XP.
  - **sjlabs-von05spring.pdf**: *datasheet*.
  - **SJphone Guide.pdf**: manual.

- <DIR> Viking 1600A:
  - **Viking 1600a series.pdf**: *datasheet*.
  - **Especificaciones de las líneas analógicas.pdf**: documento con especificaciones sobre las características de las líneas de telefonía analógicas.
  - **view_product.php.htm** y <DIR> view_product.php_files: página de Viking con las características de los interfonos de la serie Viking 1600 con algunos enlaces a su página web.

- <DIR> Varios:

- <DIR> Asterisk: centralita Asterisk *freeware* en la versión 1.2.8 y documentos de configuración y uso:
  - **asterisk-1.2.8.tar.gz**: instalador para Linux.
  - **A_B_E_ds.pdf**: datasheet para la centralita Asterisk Business Edition de Digium Systems.
  - **abe_brochure.pdf**: manual para la centralita Asterisk Business Edition de Digium Systems.
  - **abe_quickstart.pdf**: manual de puesta en marcha básico para la centralita Asterisk Business Edition de Digium Systems.
  - **handbook-draft.pdf**: manual para la centralita Asterisk 1.2.
- <DIR> Ethereal - ethernet sniffer: contiene el instalador **ethereal-setup-0.99.0.exe** de este sniffer de red, para Windows.
- <DIR> Micronet 5100SP: contiene el archivo **SP5100_manual_v3.pdf**, manual de este teléfono IP.
- <DIR> OpenPhone: contiene este teléfono software *freeware* para Windows:
  - **openphone.exe**: ejecutable.
  - **OpenH323.dll**, **PWLib.dll** y **PTLib.dll**: librerías para la ejecución.
- <DIR> Servidor DHCP y TFTP: contiene el archivo **tftpd32.280.zip**, para instalar el servidor *freeware* TFTPD32 de DHCP, TFTP y NTP en Windows XP.
- <DIR> Software Auditorías de red: contiene algunos softwares para auditorías de red en sus versiones de prueba, así como diversa información relacionada:
  - **Brixnet BrixMon DataSheet.pdf**: su *datasheet*.
  - **loway QueueMetrics.pdf**: manual del programa QueueMetrics de Loway.
  - <DIR> Clear Sight Analyzer:
    - **CSA411-Trial.zip**: instalador del programa de prueba.
    - **AnalysisCenter20SP1a-CD-pwd.exe**: clave ejecutable para usar el programa de prueba.
    - **ClearSight_Brochure_p1-4.pdf**: *datasheet*.
    - **ClearSight_GSG.pdf**: manual.
    - **ClearSight_QuickInstall.pdf**: manual de instalación rápida.
  - <DIR> Empirix Hammer Call Analyzer:
    - **ds_hca.pdf**: *datasheet*.
    - **HammerCAzip.exe**: instalador del programa de prueba.
  - <DIR> NetIQ Vivinet software:
    - **DS_VivinetAssessor_FEB05pdf.pdf**: documento que habla de las características del programa.

- **AM_Suite_DS.pdf**: documento que habla de la suite de productos NetIQ AppManager Suite.
- **vivinetassessor.exe**: ejecutable con un ejemplo de uso.

- <DIR> Software H.323 de código abierto: se incluyen aquí algunos programas de código abierto para H.323:
  - <DIR> OpenH323: librería de código abierto sobre la que se han desarrollado algunos programas:
    - **callgen323_20030313_win32.zip**: generador de llamadas H.323, para hacer pruebas de robustez.
    - **openh323_20030313_win32.zip**: librería openH323.
    - **openivr_20030313_win32.zip**: servidor IVR sobre openH323.
    - **openphone_20030313_win32.zip**: el teléfono OpenPhone.
    - **pwlib_20030313_win32.zip**: librería openH323.
    - <DIR> fuentes: contiene los códigos fuente de las librerías, en C++.
  - <DIR> GnuGK: Gatekeeper de código abierto y de gran robustez:
    - **gnugk-2.2.3-2.zip**: códigos fuente en C++ (sobre OpenH323).
    - **gnugk-2.2.3-2-win32-x86.zip**: ejecutable para Windows y librerías estables.
    - **Compiling the GNU Gatekeeper.htm** y <DIR> Compiling the GNU Gatekeeper_archivos: instrucciones para el compilado del GnuGK sobre las librerías H.323.
    - **gnugk-manual-2.2.3-2.pdf**: manual.
- <DIR> Vídeos: contiene tres vídeos llevados a cabo en Revenga Ingenieros S.A. para ilustrar el comportamiento de la plataforma de interfonía en pruebas (en formato avi). Los vídeos son **Llamada al exterior desde un SJPhone.avi**, **Maqueta de Interfonía.avi**, y **Llamada a un terminal VoIP desde un teléfono móvil.avi**.

Bibliografía

Esta bibliografía se estructura en la documentación, que contiene los documentos en los que se ha basado expresamente la redacción de la memoria; y en los enlaces de Internet introducidos a lo largo del texto, los cuales contienen referencias informativas sobre algunos comentarios introducidos o documentos de información adicional:

Documentación

Para la redacción del presente proyecto se han consultado los siguientes estándares:

a. "ITU-T H.323 draft V5(5/2003)", ITU-T, Mayo 2003, desde http://ftp3.itu.int/av-arch/avc-site/2001-2004/0305_Gen/h323V5consented.zip .

b. "ITU-T H.225.0 draft V5(5/2003)", ITU-T, Mayo 2003, desde http://ftp3.itu.int/av-arch/avc-site/2001-2004/0305_Gen/H.225.0v5-wcm.zip .

c. "ITU-T H.245 draft V9(10/2002)", ITU-T, Octubre 2002, desde http://www.packetizer.com/voip/h245/Version9/H245Version9.zip .

d. "ITU-T H.450.1 Generic Functional Protocol for the Support of Supplementary Services in H.323", ITU-T, Septiembre 1997, desde http://ftp3.itu.int/av-arch/avc-site/1997-2000/9801_Gen/H4501wht_6.zip .

e. "ITU-T H.460.1 Guidelines for the Use of the Generic Extensible Framework", ITU-T, Febrero 2002, desde http://ftp3.itu.int/av-arch/avc-site/2001-2004/0202_Gen/H460-1-v7-revOD.zip .

f. "ITU-T X.680 Information Technology - Abstract Syntax Notation One (ASN-1): Specification of Basic Notation", ITU-T, Julio 2002, desde http://www.itu.int/ITU-T/studygroups/com17/languages/X.680-0207.pdf .

También se ha consultado los documentos siguientes:

g. "Service Architectures in H.323 and SIP: A Comparison", J. Glasmann, H. Müller, Munich University of Technology, Diciembre 2004, desde http://www.comsoc.org/livepubs/surveys/public/2003/oct/pdf/glasmann.pdf .

h. “Basic Architecture of H.323”, C. Schlatter, Switch The Swiss Education and Research Network, Junio 2003 desde http://www.switch.ch/vconf/ws2003/h323_basics_handout.pdf .

i. “Overview of H.323”, Febrero 2003, Paul E. Jones, Packetizer, desde http://www.packetizer.com/voip/h323/papers/h323_protocol_overview.ppt .

j. “Introduction to ASN.1”, Julio 2005, ASN.1 Information Site, desde http://ASN.1.elibel.tm.fr/en/introduction/index.htm .

k. “A Primer on the H.323 Series Standard”, DataBeam, Marzo de 1998, desde http://www.packetizer.com/voip/h323/papers/primer/ .

l. “H.323 Version 3 Overview”, Packetizer, 2001, desde http://www.packetizer.com/voip/h323/whatsnew_v3.html .

m. “H.323 Version 4 Overview”, Packetizer, 2001, desde http://www.packetizer.com/voip/h323/whatsnew_v4.html .

n. “H.323 Version 5 Overview”, Packetizer, 2003, desde http://www.packetizer.com/voip/h323/whatsnew_v5.html .

Enlaces

[1]: Para acceder a una información muy extensa y continuamente actualizada sobre las tecnologías de VoIP, visitar el portal http://www.voip-info.org/ .

[2]: RFC 2748: http://www.ietf.org/rfc/rfc2748.txt .

[3]: Página principal de la IETF: http://www.ietf.org/overview.html .

[4]: RFC 3761: http://www.ietf.org/rfc/rfc3761.txt .

[5]: Guía IMS y enlaces relacionados: http://www.lightreading.com/document.asp?doc_id=70728 .

[6]: MGCP: http://www.packetizer.com/voip/mgcp/ .

[7]: RFC 2848: http://www.ietf.org/rfc/rfc2848.txt .

[8]: RFC 3286: http://www.ietf.org/rfc/rfc3286.txt .

[9]: http://www.itu.int/rec/T-REC-T.37/en , http://www.itu.int/rec/T-REC-T.38/en .

[10]: RFC 3362: http://www.ietf.org/rfc/rfc3362.txt .

↑

[11]: RFC 3219: http://www.ietf.org/rfc/rfc3219.txt .

↑

[12]: http://www.itu.int/rec/T-REC-H.323/en . También, acerca de H.323, http://www.h323forum.org/ , y http://www.packetizer.com/ .

↑

[13]: RFC 3550: http://www.ietf.org/rfc/rfc3550.txt .

↑

[14]: RFC 3261: http://www.ietf.org/rfc/rfc3261.txt . Sobre SIP, http://www.ietf.org/html.charters/sip-charter.html .

↑

[15]: RFC 2327: http://www.ietf.org/rfc/rfc2327.txt .

↑

[16]: Extensa y muy completa lista de comparativas SIP – H.323: http://www.packetizer.com/voip/h323_vs_sip/ .

↑

[17]: Librerías y proyectos de código abierto SIP y H.323: http://www.voip-info.org/wiki/view/Open+Source+VOIP+Software .

↑

[18]: Por ejemplo, el método UPDATE, en RJ. Rosenberg, “The Session Initiation Protocol (SIP) UPDATE Method” RFC 3311: http://www.ietf.org/rfc/rfc3311.txt .

↑

[19]: B. Campbell, “SIP Call Control - Framework”, IETF Internet Draft, Julio 2001, http://www3.ietf.org/proceedings/02mar/I-D/draft-ietf-sip-cc-framework-00.txt .

↑

[20]: R. Sparks y A. Johnson, “SIP Call Control – Transfer”, IETF Internet Draft, Enero 2002, http://www3.ietf.org/proceedings/02nov/I-D/draft-ietf-sip-cc-transfer-05.txt .

↑

[21]: A. Mankin et al., “Change Process for the Session Initiation Protocol (SIP)”, RFC 3427, http://www.ietf.org/rfc/rfc3427.txt .

↑

[22]: J. Rosenberg y H. Schulzrinne, “Reliability of Provisional Responses in the Session Initiation Protocol (SIP)”, RFC 3262, http://www.ietf.org/rfc/rfc3262.txt .

↑

[23]: J. Rosenberg y H. Schulzrinne, “Session Initiation Protocol (SIP) Caller Preferences and Callee Capabilities”, Agosto 1999, http://www3.ietf.org/proceedings/99jul/I-D/draft-ietf-mmusic-sip-caller-00.txt , y posteriormente J. Rosenberg y H. Schulzrinne “Caller Preferences for the Session Initiation Protocol (SIP)”, RFC 3841, http://www.ietf.org/rfc/rfc3841.txt .

↑

[24]: Interfonía IP propietaria: http://www.ipintercom.com/ , http://www.digac.com/ii3.htm .

↑

[25]: Skype en http://www.skype.com/intl/es/ .

↑

[26]: Código C++ para Skype en http://www.icebrains-soft.com/skype_library_0 .

↑

[27]: Teléfono inalámbrico Linksys CIT-200 para funcionar con Skype: http://www1.linksys.com/international/product.asp?coid=52&ipid=821 .

[28]: El teléfono inalámbrico VTech IP-8100 para Vonage funciona en la banda de 5’8 GHz, prohibida en España; para más información, visitar http://www.vonage.com/corporate/press_reviews.php?PR=2005_08_22_0 .

[29]: El teléfono IP i.Picasso 6000, de Telrad Connegy: http://www.telradusa.com/eng/products.php?actions=show&id=152 .

[30]: ATAs: http://www.voip-info.org/wiki/view/Analog+Telephone+Adapters .

[31]: TDMoIP: http://www.tdmoip.com/ .

[32]: Teléfonos VoIP en general, y entre ellos un excelente listado de teléfonos sotf: http://www.voip-info.org/wiki-VOIP+Phones .

[33]: Cisco Customer Voice Portal Datasheet: http://www.cisco.com/en/US/products/sw/custcosw/ps1006/products_data_sheet09186a0080091b5c.html .

[34]: Portal para la centralita IP Asterisk: http://www.asterisk.org/ ; y una solución ya compilada en CD, disponible para ser instalada sin demasiados conocimientos de Linux, puede encontrarse en http://asteriskathome.sourceforge.net/ .

[35]: Para un desarrollo completo comparando tecnológicamente la telefonía analógica y la VoIP, visitar http://wiki.lug.fi.uba.ar/tiki-read_article.php?articleId=5 .

[36]: Información actualizada de proveedores de servicio en internet en http://almadormida.blogspot.com/2006/01/voip-state-of-art.html , y también en http://www.voip-info.org/wiki/view/VOIP+Service+Providers .

[37]: http://www.google.com/talk/ .

[38]: http://www.lukor.com/webmasters/05051405.htm .

[39]: Artículo explicando algunas causas de las quejas recibidas por la asociación de internautas: http://www.internautas.org/html/3433.html .

[40]: Penetración de la banda ancha en España y en el mundo: http://www2.noticiasdot.com/publicaciones/2005/0905/1009/noticias/internet-numeros/internet-numeros-08.htm ; crecimiento del 48%: http://www.internautas.org/html/3401.html .

[41]: Discusión desde la coalición Voice On the Net (VON) para el marco regulatorio en los USA: http://www.theregister.co.uk/2004/06/03/us_voip_fcc/ . Publicación del GRETEL “El desarrollo de la VoIP y sus implicaciones regulatorias”: http://www.coit.es/foro/pub/ficheros/gretel_cuaderno_voip_9d0c6d72.pdf .

↑

[42]: La regulación VoIP en el marco internacional: http://aui.es/contenidos/aui_bitacora.php3?body=article&id_article=49 .

↑

[43]: Éste es el caso de VoIPBuster: http://www.voipbuster.com/en/index.html .

↑

[44]: http://www.networkingpipeline.com/showArticle.jhtml?articleID=162600046 , y más recientemente, http://www.itworld.com/Net/3303/051219voipcomp/ .

↑

[45]: http://www.umtsforum.net/mostrar_noticias.asp?u_action=display&u_log=1854 .

↑

[46]: Tendencia a la fusión de grandes multinacionales: http://www.time.com/time/europe/magazine/article/0,13005,901060109-1145205,00.html , y artículo sobre la tendencia actual a provisión de todos los servicios posibles en una única factura, *triple play*: http://www.time.com/time/europe/magazine/article/0,13005,901060116-1147112,00.html .

↑

[47]: Imagenio: http://www.telefonicaonline.com/on/es/imagenio/ .

↑

[48]: Vídeo bajo demanda de ONO: http://www.ono.es/default.asp?p=01&o=03&s=20 .

↑

[49]: Jazztel lanza un proyecto piloto de televisión por ADSL: http://www2.noticiasdot.com/publicaciones/2005/0605/2906/noticias/noticias_290605-15.htm .

↑

[50]: Actualidad de la FTTH en Japón: http://www.americasnetwork.com/americasnetwork/article/articleDetail.jsp?id=93689 , http://www.eurotechnology.com/internet/index.html , y también http://www.ispjapan.org/ .

↑

[51]: http://www.vnunet.com/vnunet/news/2126116/voip-rings-death-knell-traditional-telephony .

↑

[52]: Los textos completos de toda la documentación relacionada con H.323 pueden encontrarse en http://www.packetizer.com/voip/h323/standards.html .

↑

[53]: RFC 2205: http://www.ietf.org/rfc/rfc2205.txt .

↑

[54]: Página principal de IANA: http://www.iana.org/ .

↑

[55]: El SDL se describe en la especificación Z.100: http://www.itu.int/ITU-T/studygroups/com10/languages/Z.100_1199.pdf ; también puede consultarse el Forum SDL: http://www.sdl-forum.org/SDL/index.htm .

↑

[56]: Página principal de la empresa Revenga Ingenieros S.A.: http://www.revenga.com/ .

↑

[57]: Página de Viking Electronics Inc: http://www.vikingelectronics.com/index.html . ↑

[58]: Quintum Technologies Inc: http://www.quintum.com/ . ↑

[59]: Información y datasheet del teléfono IP Cisco 7905G, desde la página oficial de Cisco Systems: http://www.cisco.com/en/US/products/hw/phones/ps379/products_data_sheet09186a00800c835a.html . ↑

[60]: Teléfono software SJ Phone, descripción en la página oficial: http://www.sjlabs.com/products.html , y última versión sobre plataformas Win32 en http://www.sjlabs.com/SJphoneWin . ↑

[61]: Referencias del fabricante: http://www.snom.com/snom100_release_notes.html . ↑

[62]: http://www.swissvoice.net/ww/htm_ww/07_products/ds_ip10.html . ↑

[63]: http://www.siptronic.com/assets/s2dmain.html?http://www.siptronic.com/ed0af9955b1250701/ed0af9955b12dde0a.html . ↑

[64]: http://www.cisco.com/en/US/products/hw/phones/ps379/products_data_sheet09186a008008884a.html . ↑

[65]: http://www.telkus.com/esp/productos.asp?id=1 . ↑

[66]: http://www.micronet.com.tw/model_detail.aspx?series_no=12&sno=313 . ↑

[67]: http://www.cisco.com/en/US/products/hw/phones/ps379/products_data_sheet09186a00800c835a.html . ↑

[68]: http://www.openh323.org/. ↑

[69]: http://www.microsoft.com/windows/netmeeting/ . ↑

[70]: http://www.sjlabs.com/index.html. ↑

[71]: Alcatel no ofrece información sobre este teléfono; consultar http://empresas.mundo-r.com/servlet/Satellite?cid=1130497053925&pagename=OpenMarket%2FXcelerate%2FRender&Idioma=es&c=WCR_Seccion . ↑

[72]: Este programa puede descargarse gratuitamente desde http://www.ethereal.com/download.html . ↑

[73]: http://www.quintum.com/enterprise/en_productdetail.html?id=34 . ↑

[74]: http://www.cosmovoice.com/main.php .

↑

[75]: http://www.vnunet.es/Actualidad/Noticias/Canal_distribuci%C3%B3n/Fabricantes/20060330045 .

↑

[76]: Una completa lista de todos ellos puede encontrarse en http://www.voip-info.org/wiki/view/How+To+Debug+and+Troubleshoot+VOIP.

↑

[77]: http://www.clearsightnet.com/products-analyzer.jsp .

↑

[78]: http://www.netiq.com/products/vd/default.asp .

↑

[79]: http://www.brixnet.com/corporate/ .

↑

[80]: http://www.empirix.com/default.asp?action=article&ID=69 .

↑