

## 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 necesidad, 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<sup>45</sup> (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:

---

<sup>45</sup> 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<sup>46</sup>, 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.

**VIKING**  
Telecom and Security Solutions for the 21st Century!

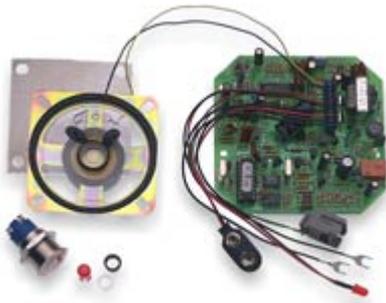


Figura 29: Interfono Viking 1600A sin carcasa.



Figura 30: Interfono montado en carcasa.

**Quantum 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.

<sup>46</sup> 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 *firmwares* (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 en 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 conectarán 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 conectarán 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):

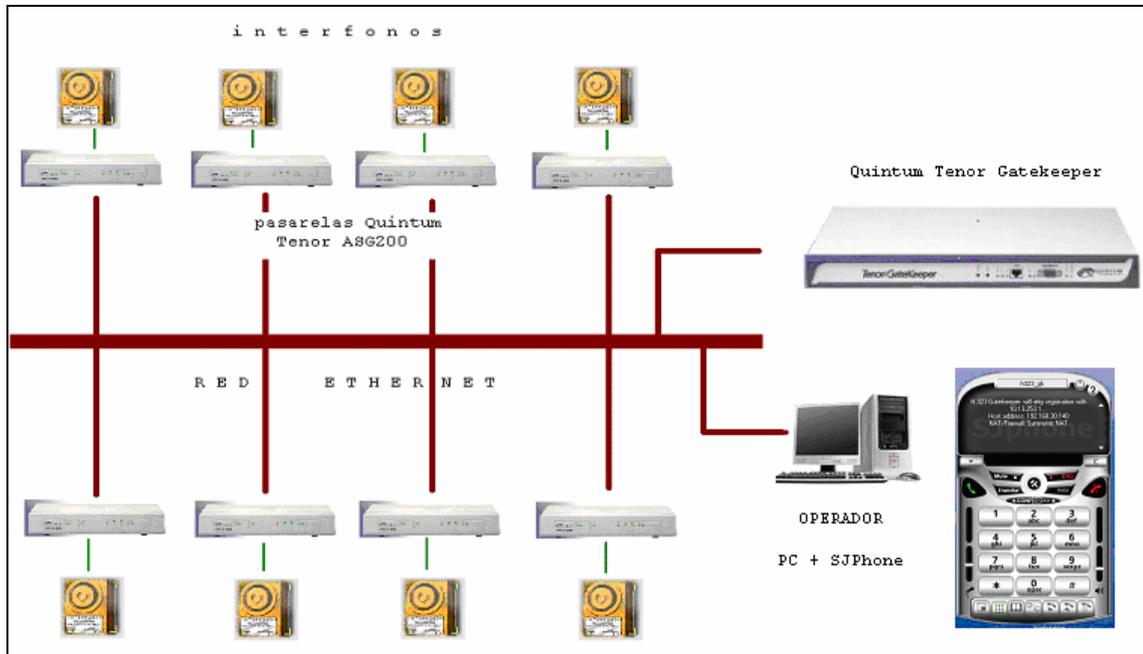


Figura 36: Esquema completo para la Plataforma de Interfonía Barrio de las Letras

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 códecs 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:

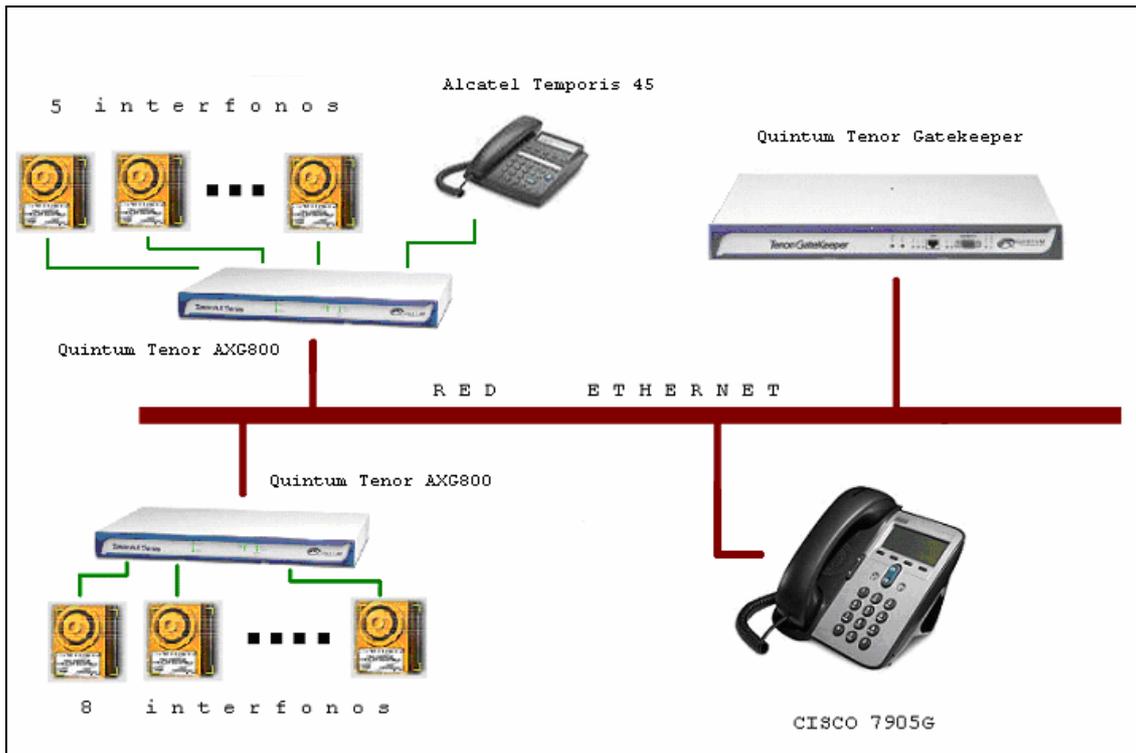


Figura 38: Esquema completo para la Plataforma de Interfonía Estación de Bailén

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:

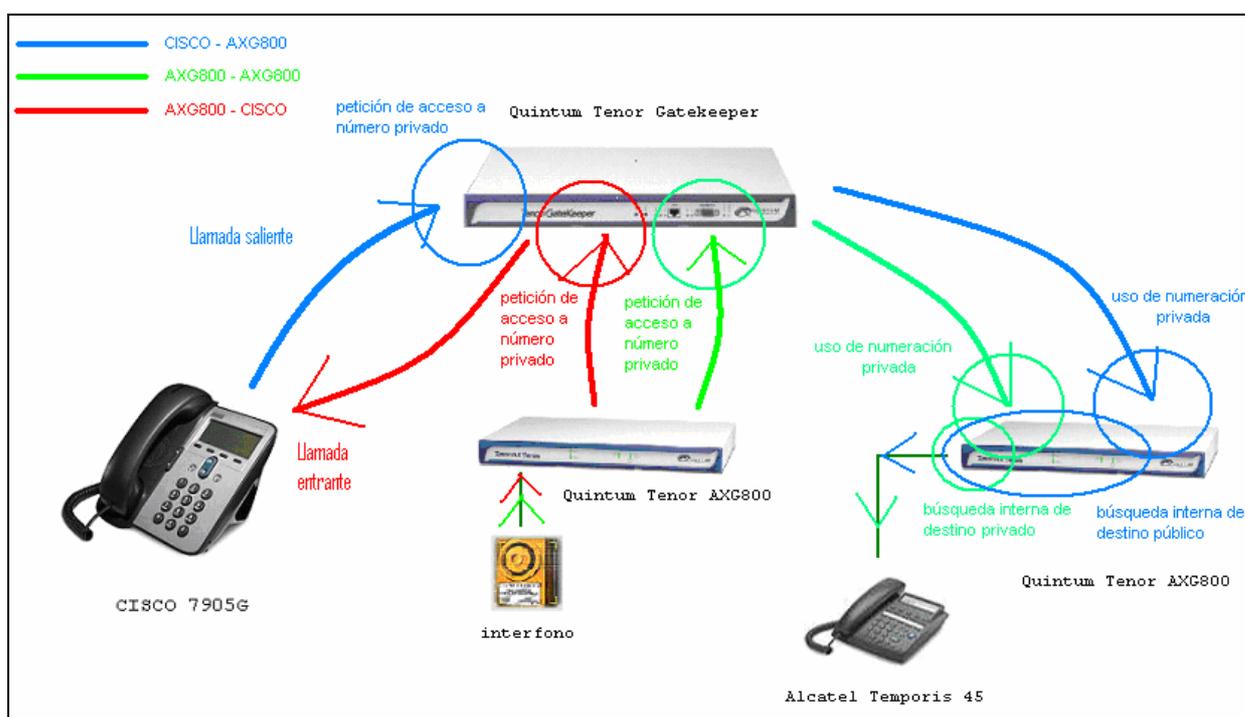


Figura 39: Esquema de comunicaciones y tipos de numeración, Plataforma de Interfonía Estación de Bailén

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	EXPENDEDEDORA-JESU
1008	10.13.108.1 / 8	Bailen1	XATIVA-PILAR
1009	10.13.108.2 / 1	Bailen2	EXPENDEDEDORA-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):

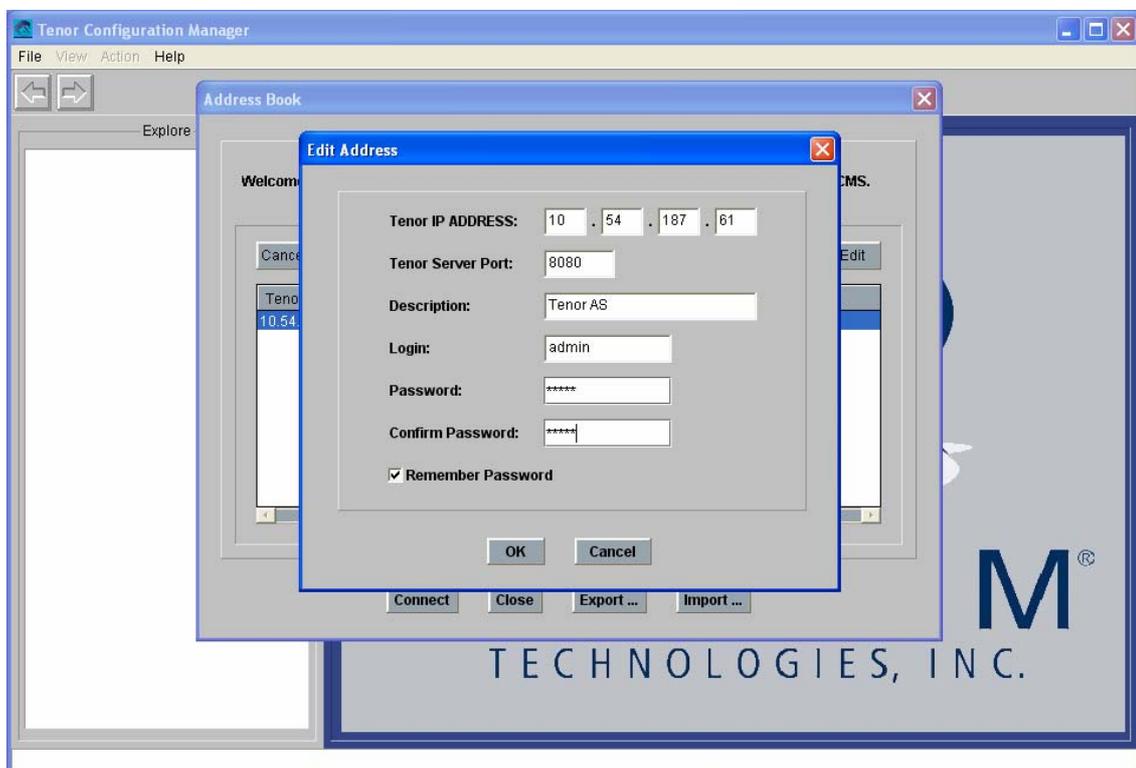


Figura 41: Captura 1 del *Tenor Configuration Manager* para la plataforma del Barrio de las Letras.

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:

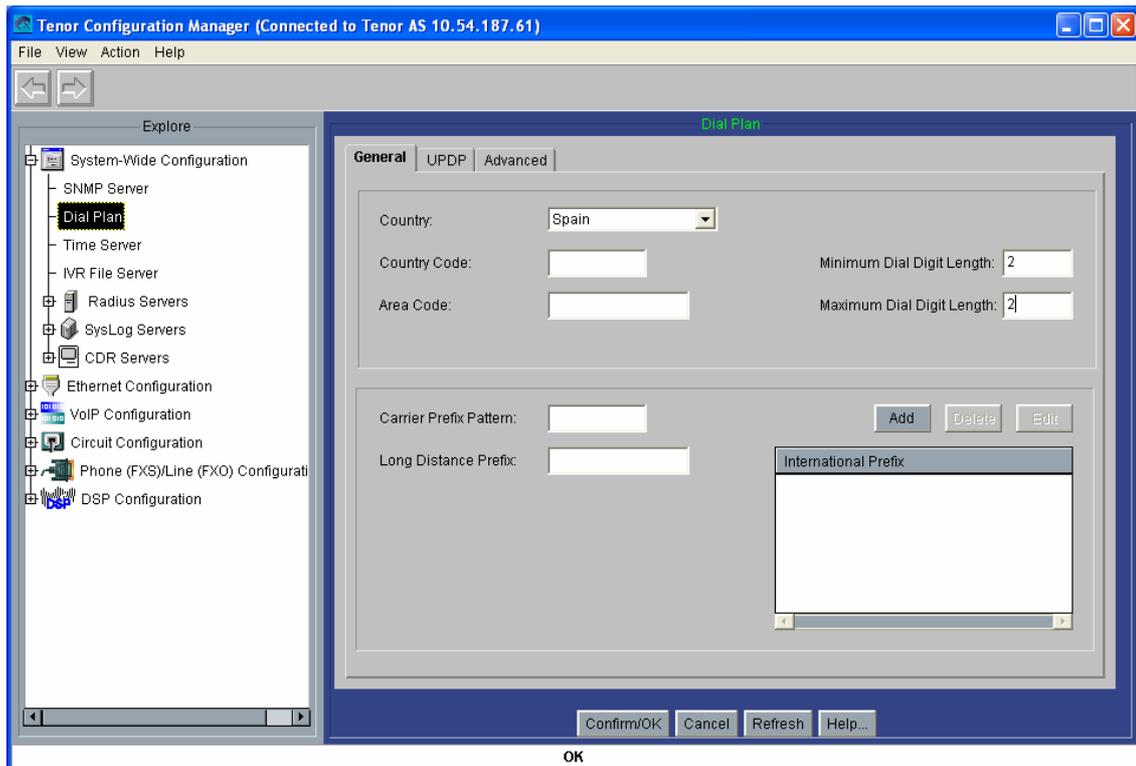


Figura 42: Captura 2 del *Tenor Configuration Manager* para la plataforma del Barrio de las Letras.

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 impediría 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 intrapasarelas. 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):

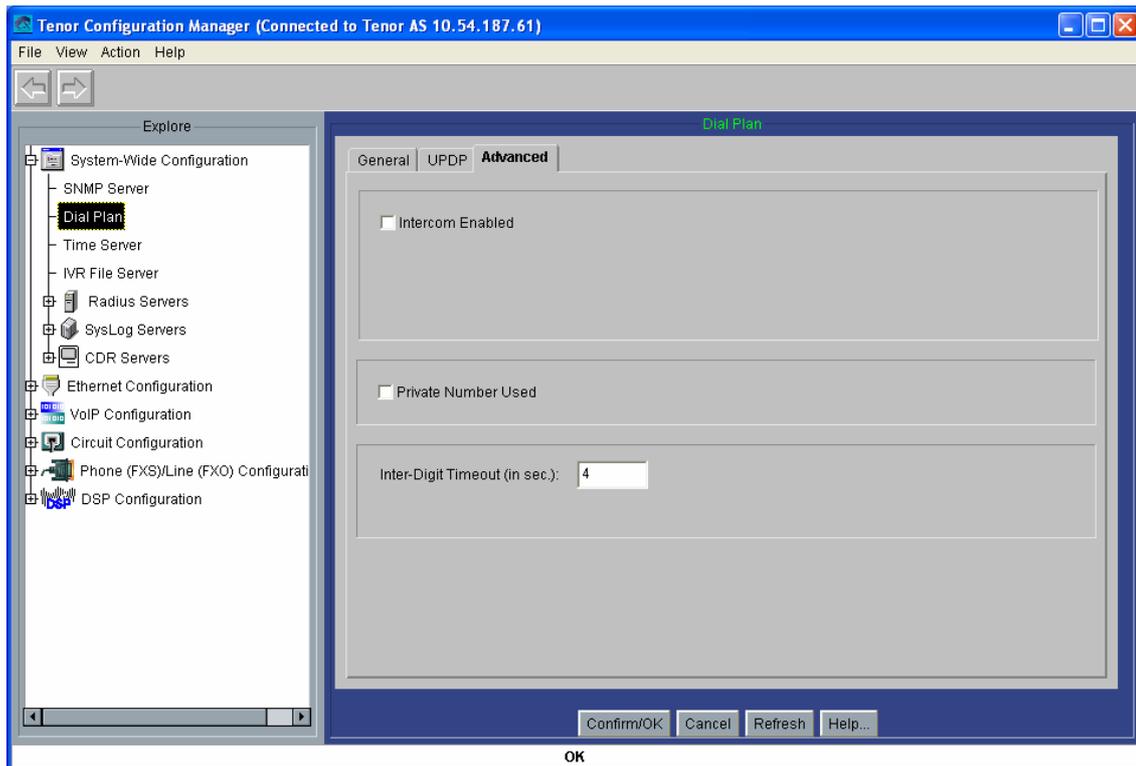


Figura 43: Captura 3 del *Tenor Configuration Manager* para la plataforma del Barrio de las Letras.

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.

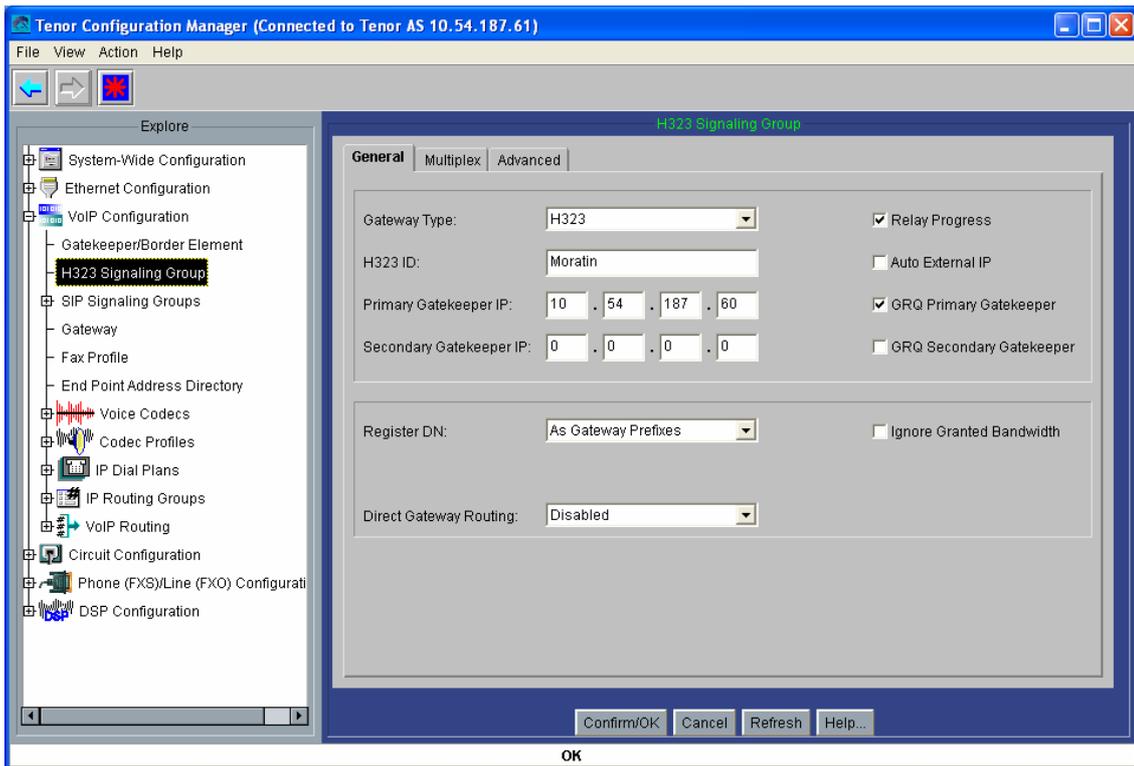


Figura 44: Captura 4 del *Tenor Configuration Manager* para la plataforma del Barrio de las Letras.

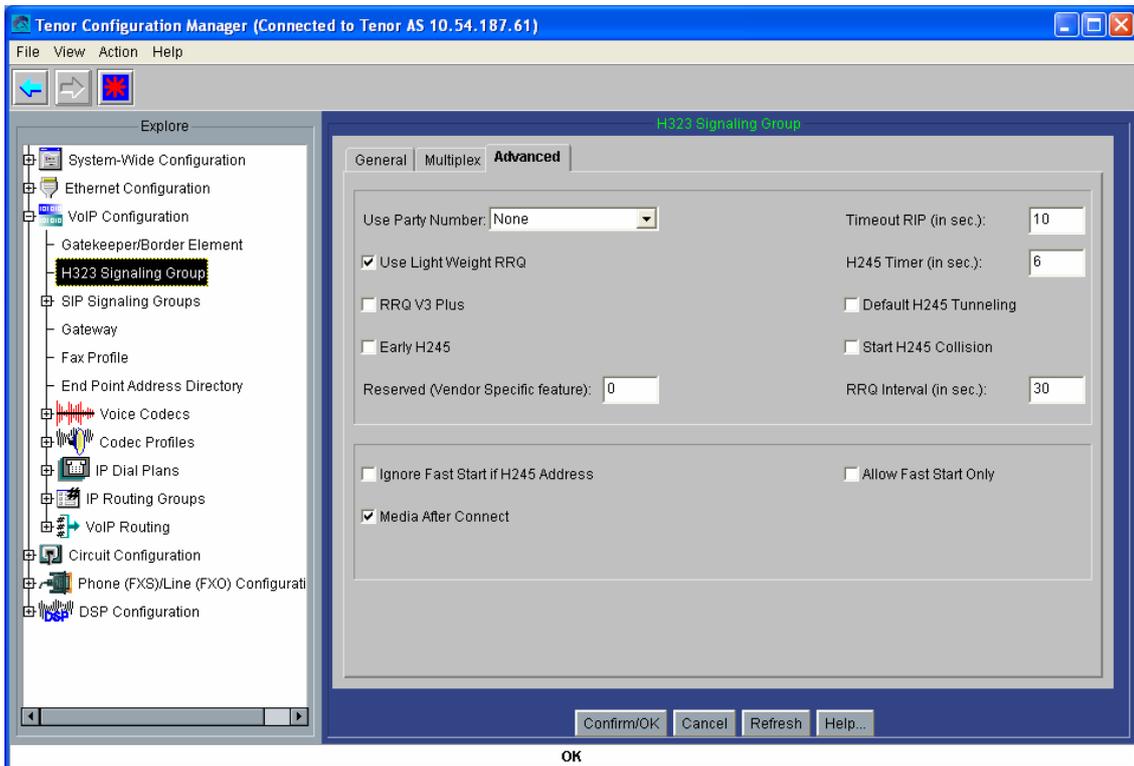


Figura 45: Captura 5 del *Tenor Configuration Manager* para la plataforma del Barrio de las Letras.

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 códec (Codec Profile - default), como se muestra en la figura 47:

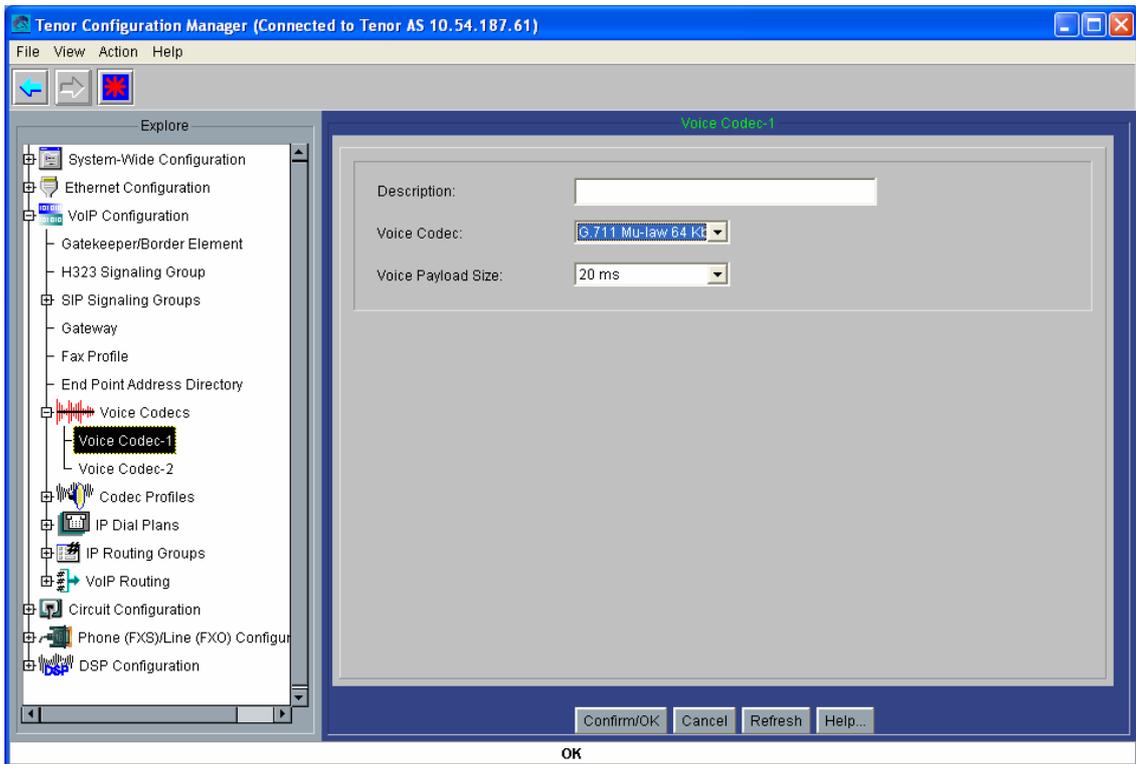


Figura 46: Captura 6 del *Tenor Configuration Manager* para la plataforma del Barrio de las Letras.

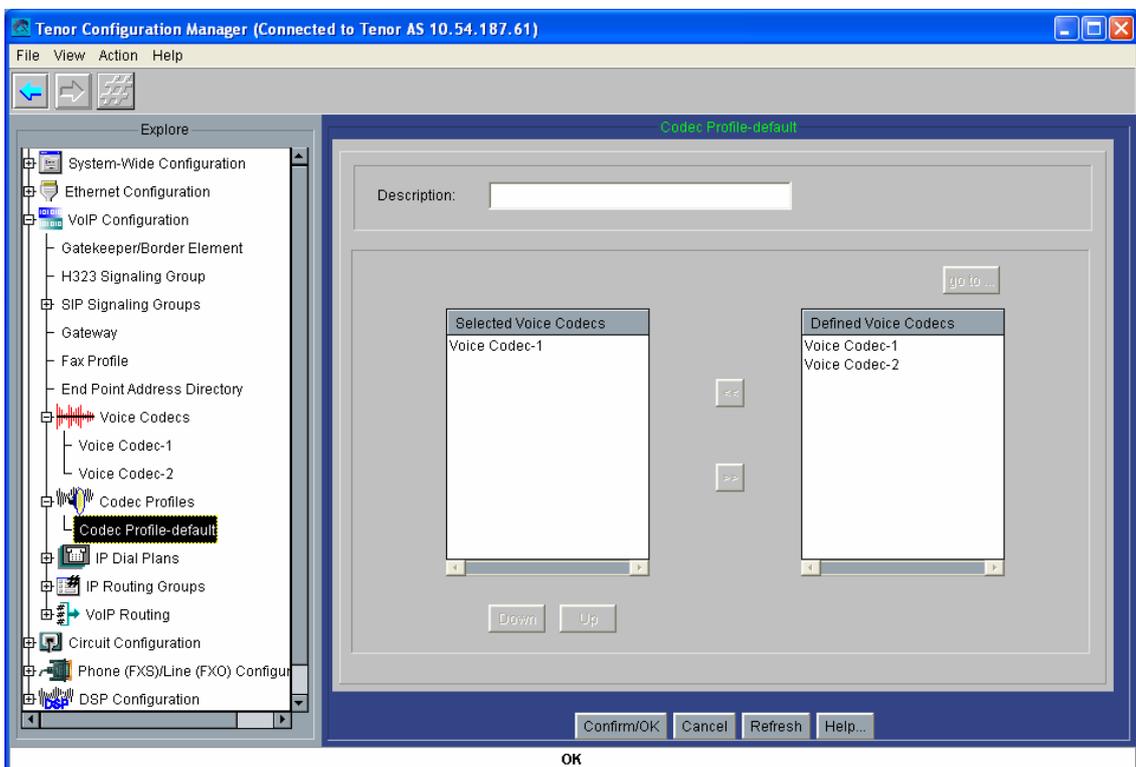


Figura 47: Captura 7 del *Tenor Configuration Manager* para la plataforma del Barrio de las Letras.

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 través de dicho Gatekeeper.

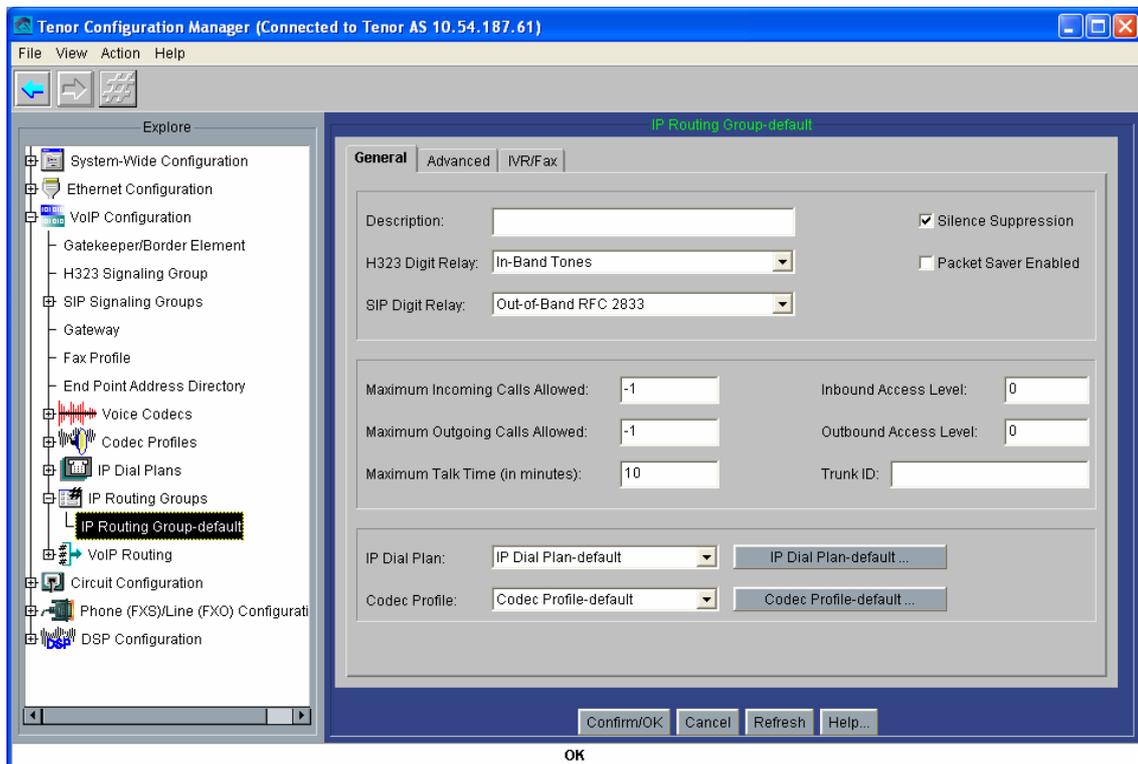


Figura 48: Captura 8 del *Tenor Configuration Manager* para la plataforma del Barrio de las Letras.

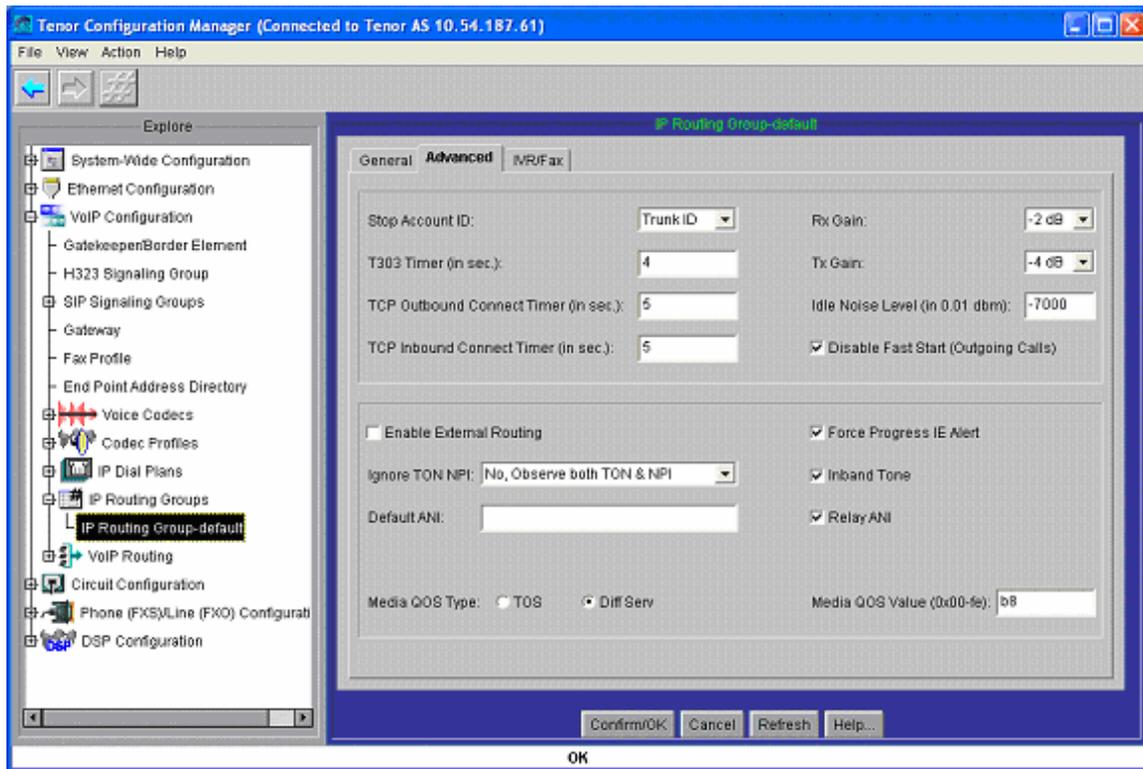


Figura 49: Captura 9 del *Tenor Configuration Manager* para la plataforma del Barrio de las Letras.

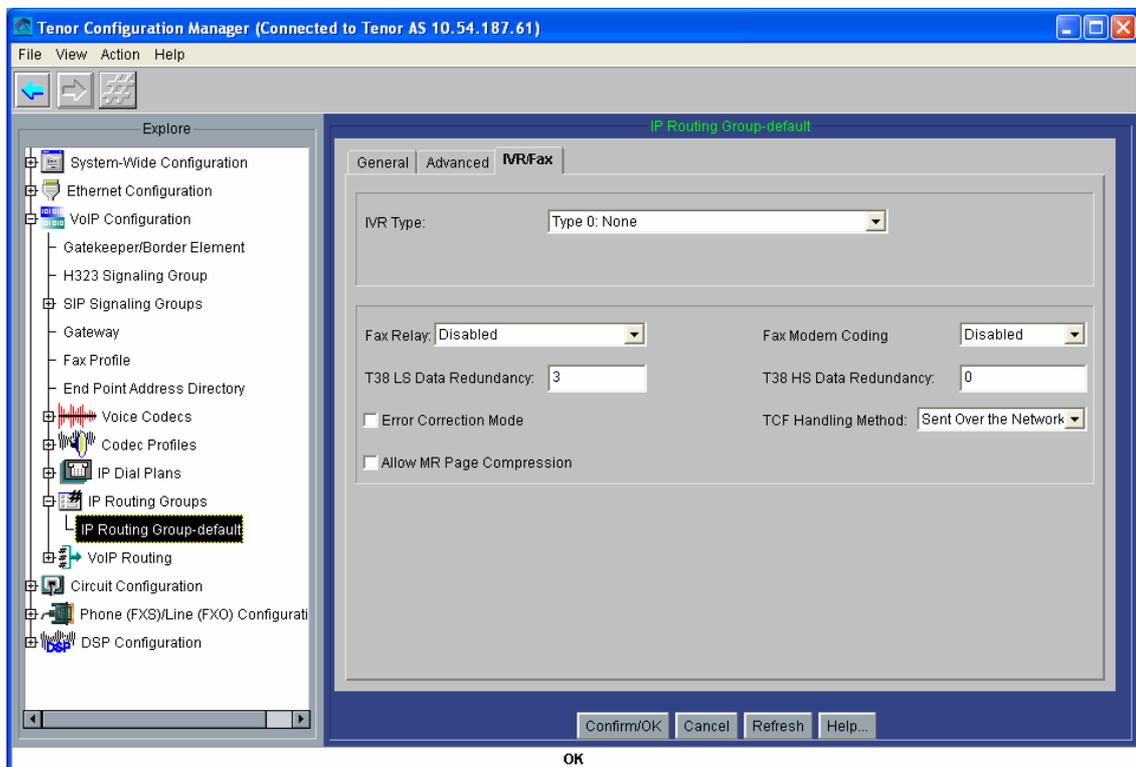


Figura 50: Captura 10 del *Tenor Configuration Manager* para la plataforma del Barrio de las Letras.

A continuación se muestra la configuración de las líneas analógicas: esto se consigue configurando el grupo de señalización CAS (*Channel Associated 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:

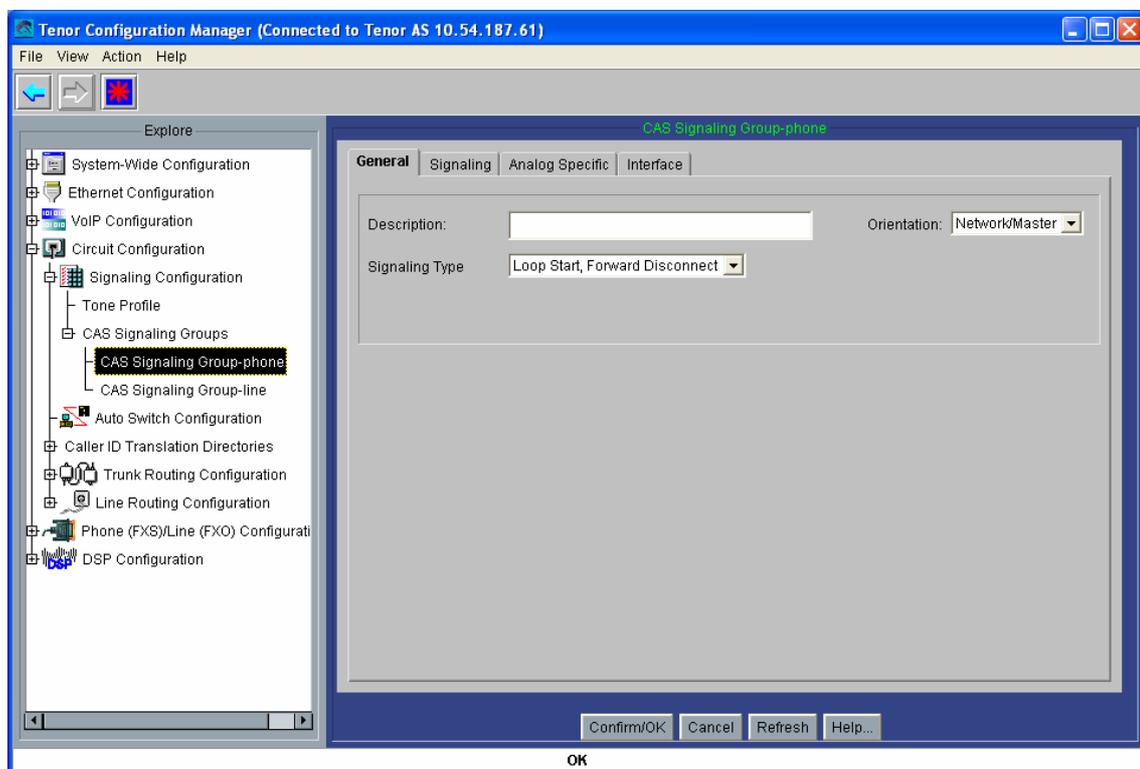


Figura 51: Captura 11 del *Tenor Configuration Manager* para la plataforma del Barrio de las Letras.

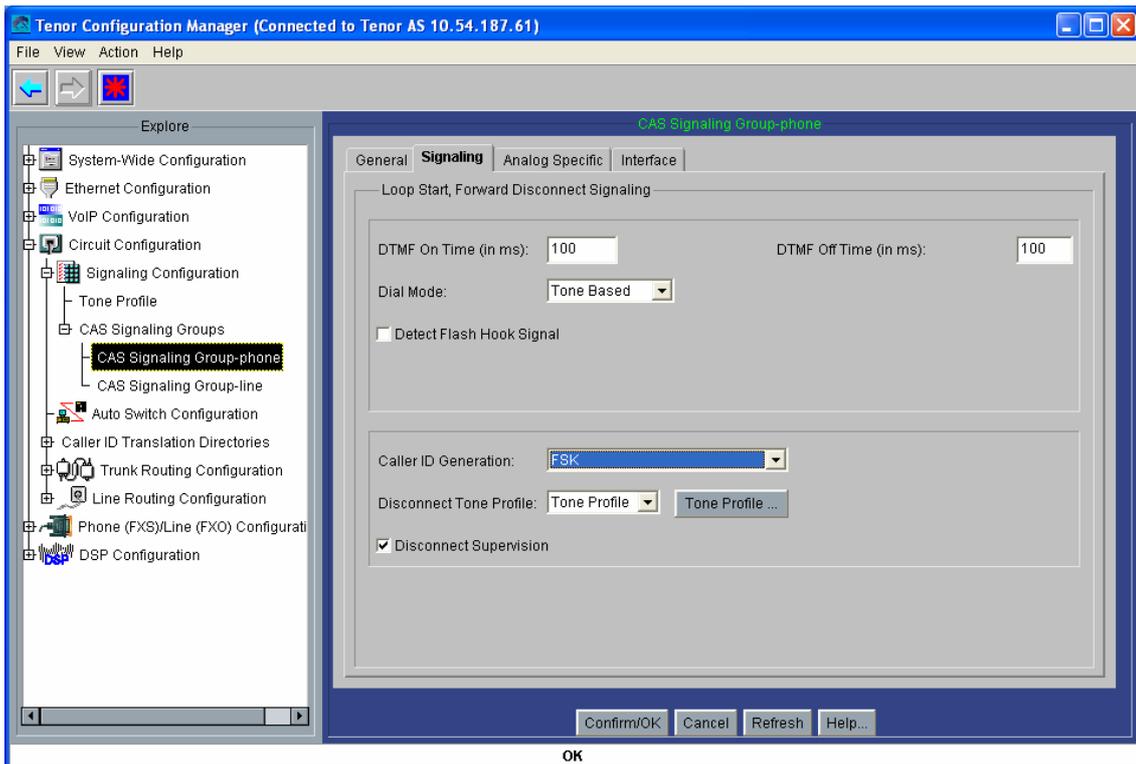


Figura 52: Captura 12 del *Tenor Configuration Manager* para la plataforma del Barrio de las Letras.

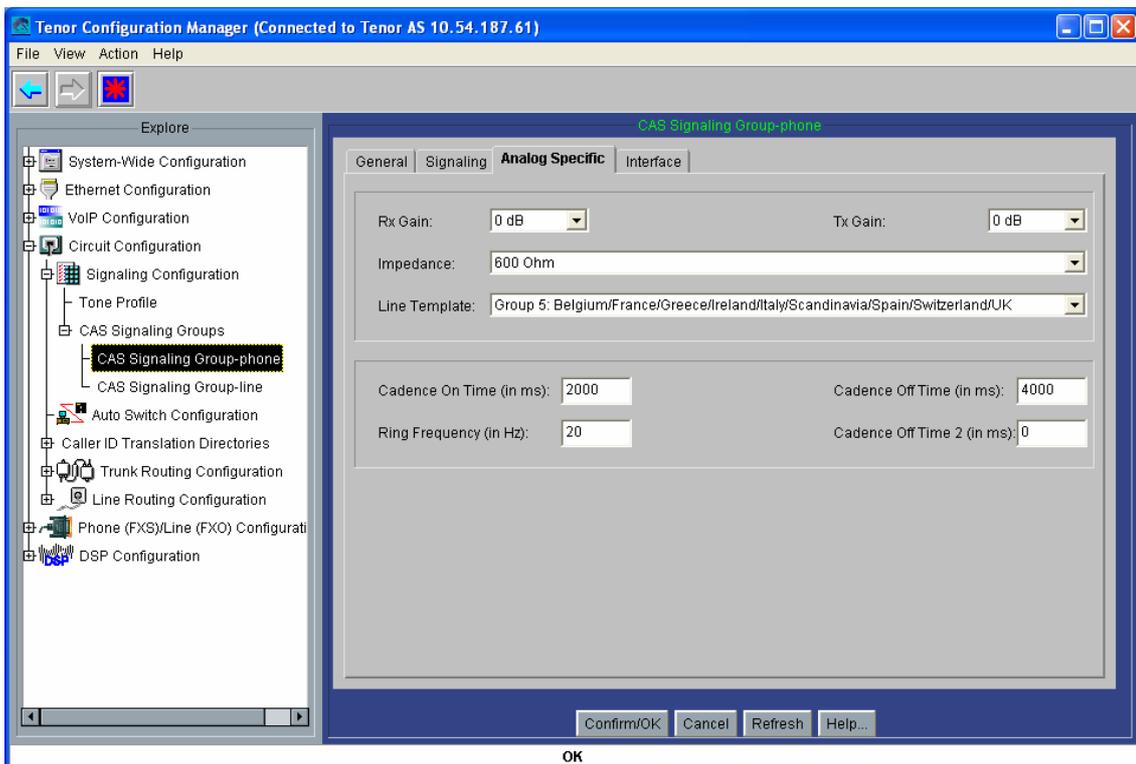


Figura 53: Captura 13 del *Tenor Configuration Manager* para la plataforma del Barrio de las Letras.

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:

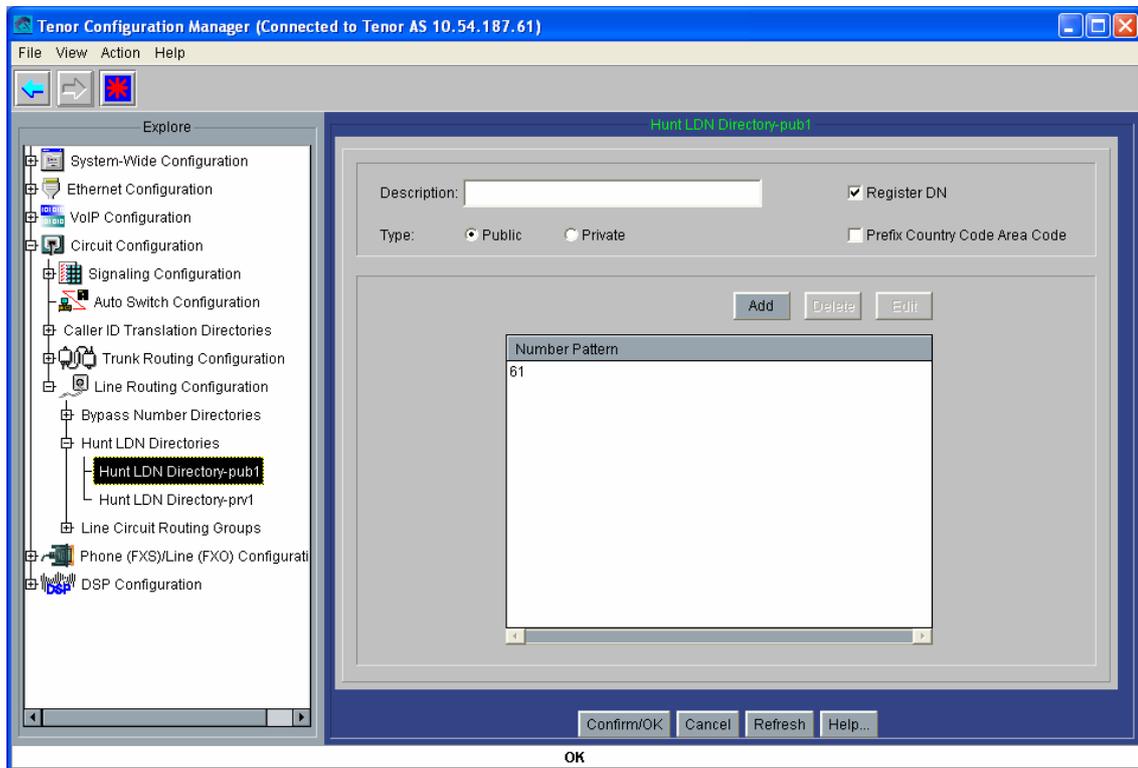


Figura 54: Captura 14 del *Tenor Configuration Manager* para la plataforma del Barrio de las Letras.

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):

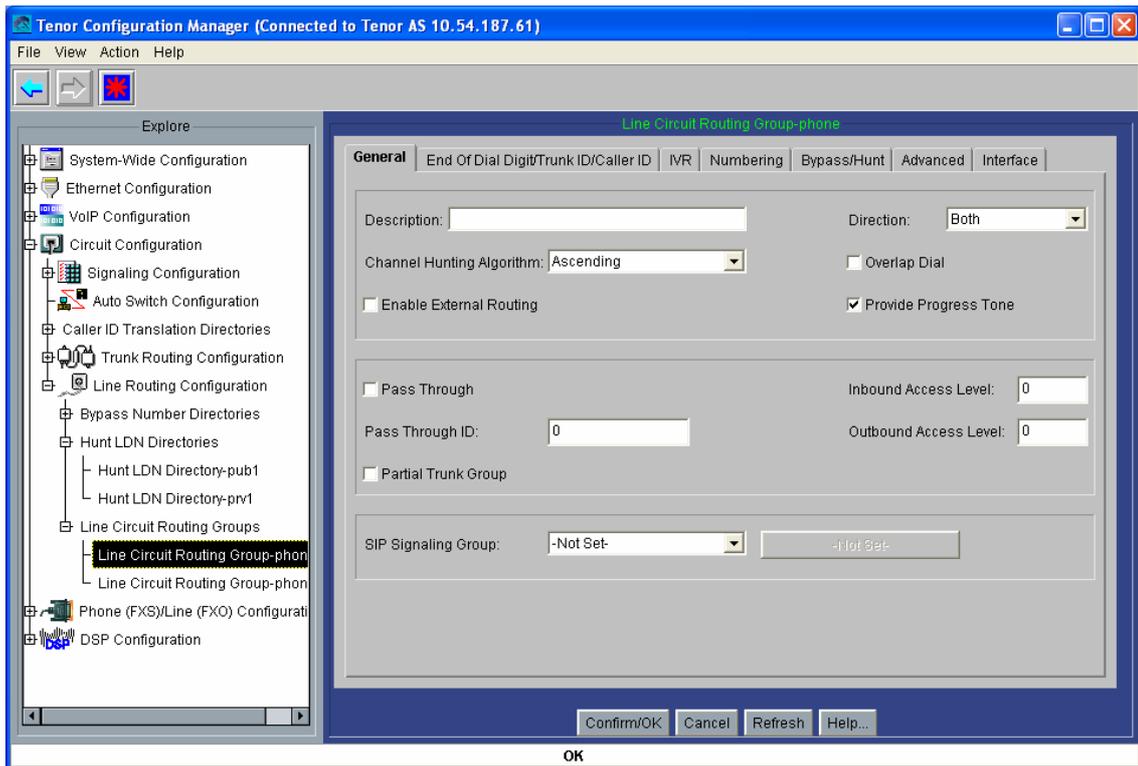


Figura 55: Captura 15 del *Tenor Configuration Manager* para la plataforma del Barrio de las Letras.

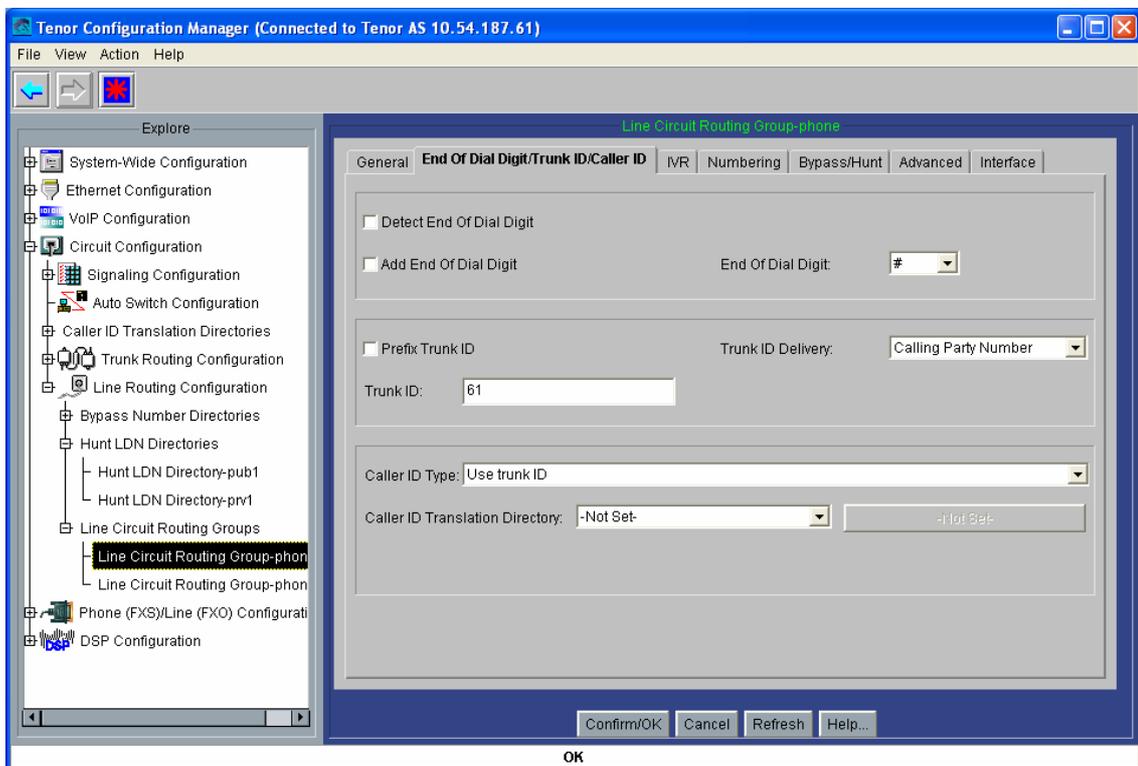


Figura 56: Captura 16 del *Tenor Configuration Manager* para la plataforma del Barrio de las Letras.

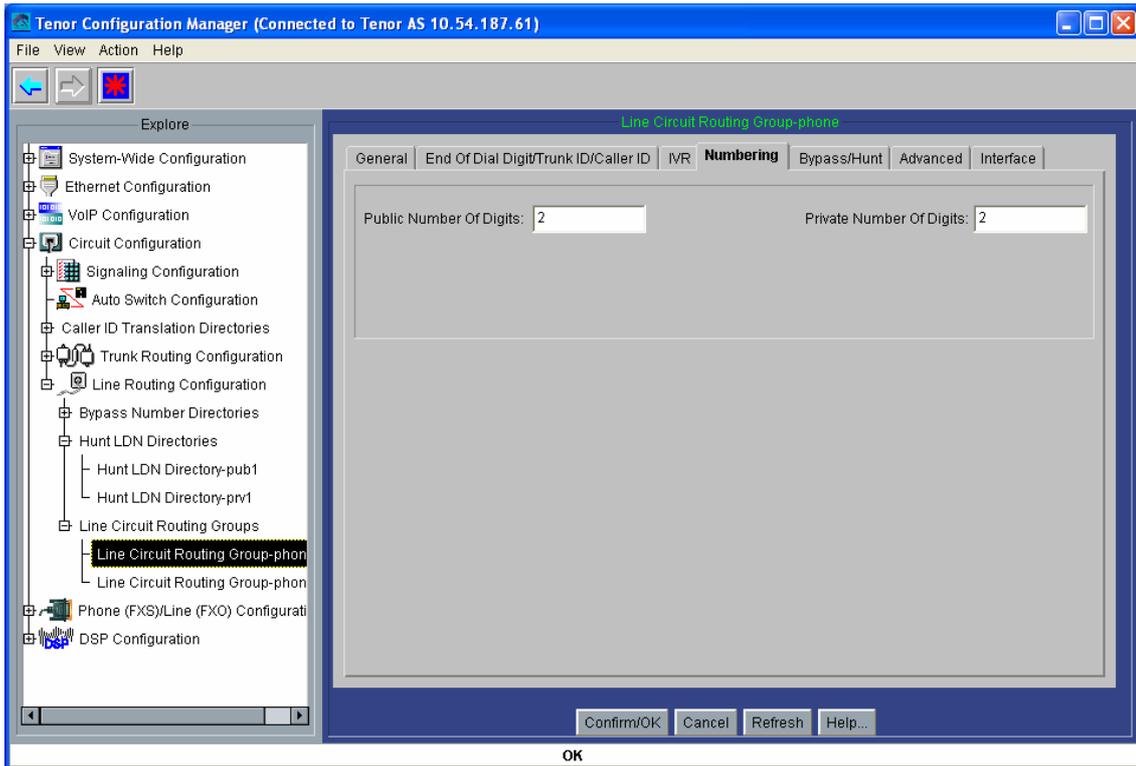


Figura 57: Captura 17 del *Tenor Configuration Manager* para la plataforma del Barrio de las Letras.

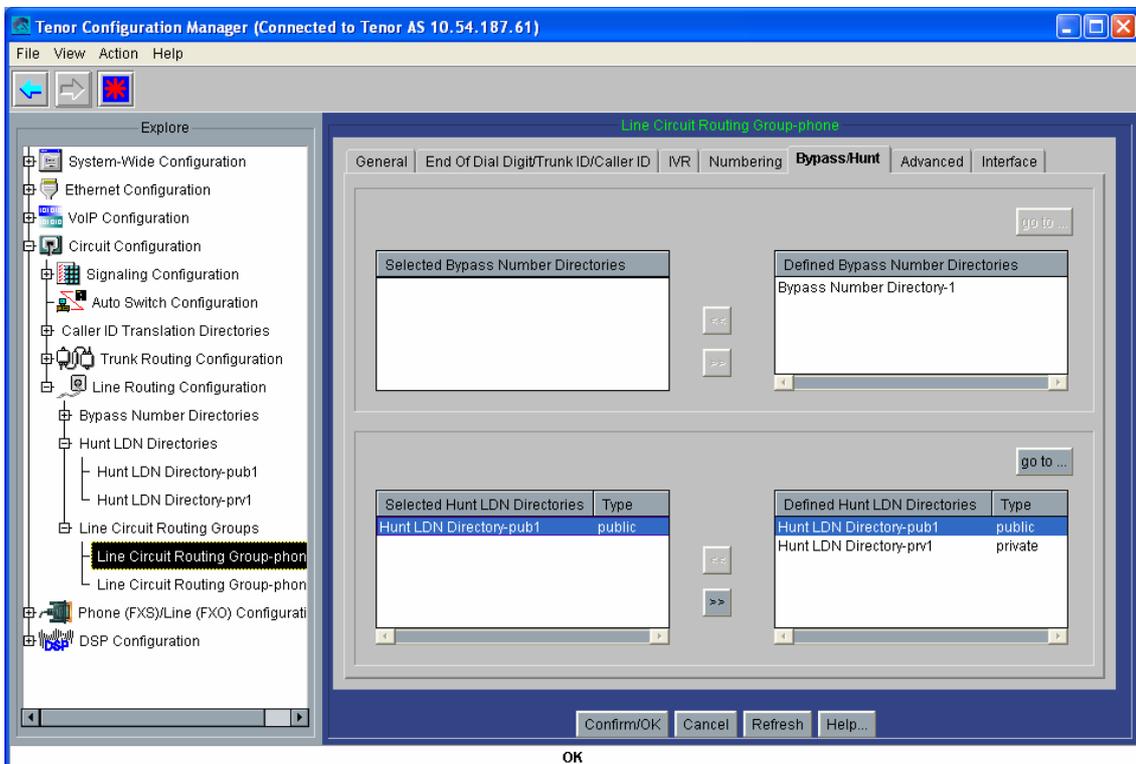


Figura 58: Captura 18 del *Tenor Configuration Manager* para la plataforma del Barrio de las Letras.

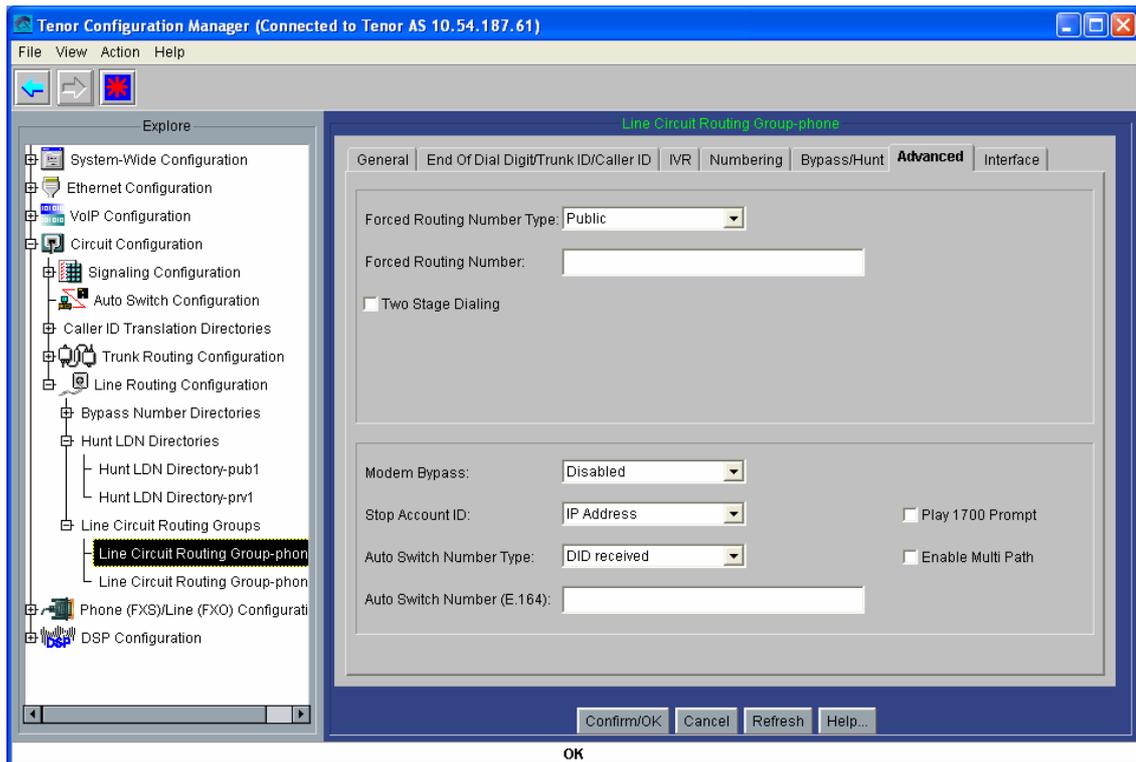


Figura 59: Captura 19 del *Tenor Configuration Manager* para la plataforma del Barrio de las Letras.

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:

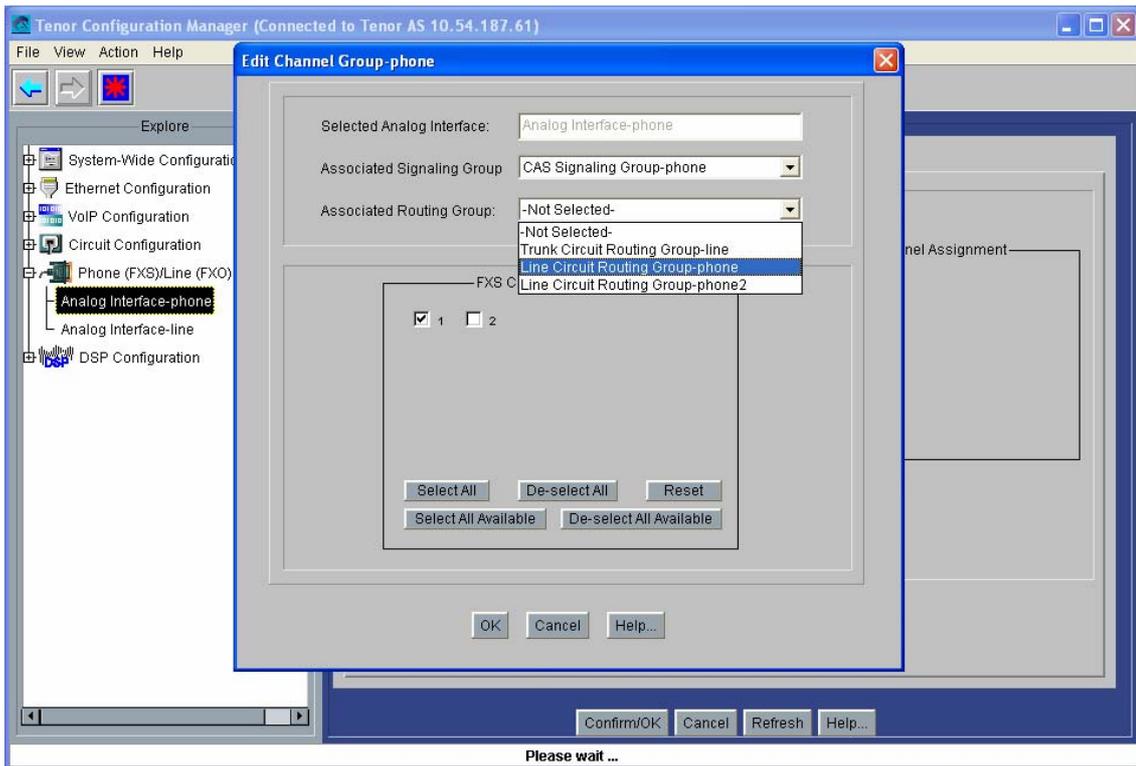


Figura 60: Captura 20 del *Tenor Configuration Manager* para la plataforma del Barrio de las Letras.

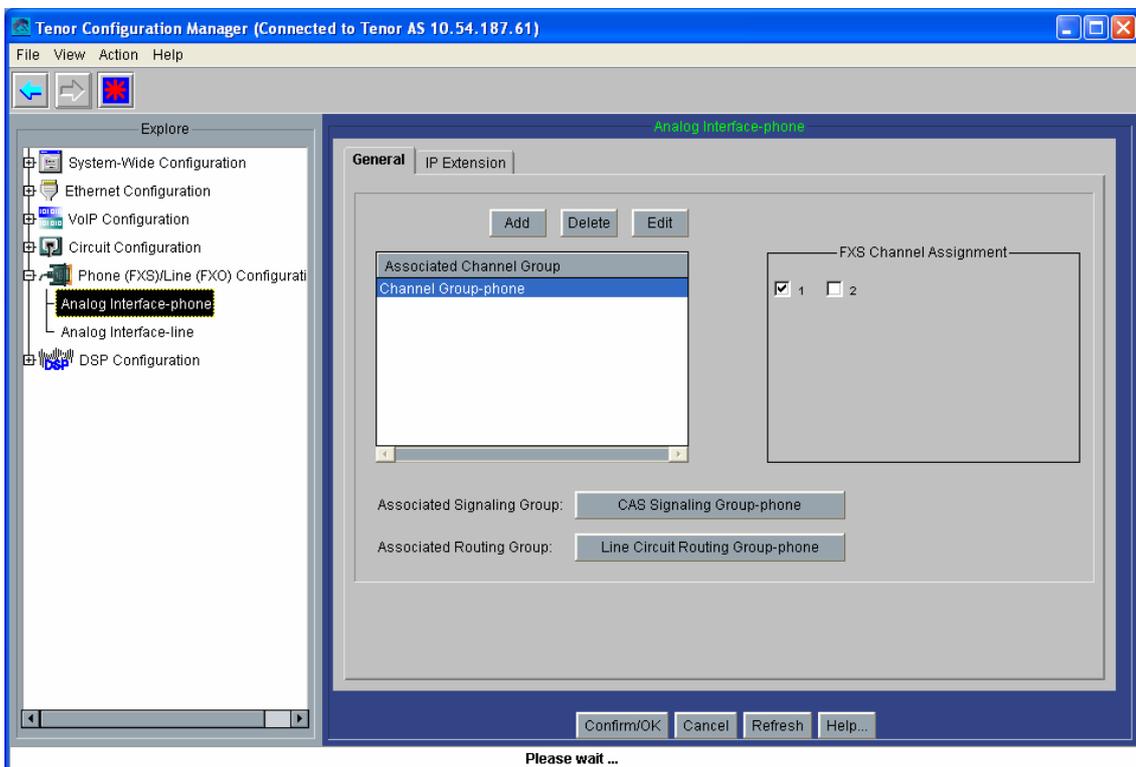


Figura 61: Captura 21 del *Tenor Configuration Manager* para la plataforma del Barrio de las Letras.

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

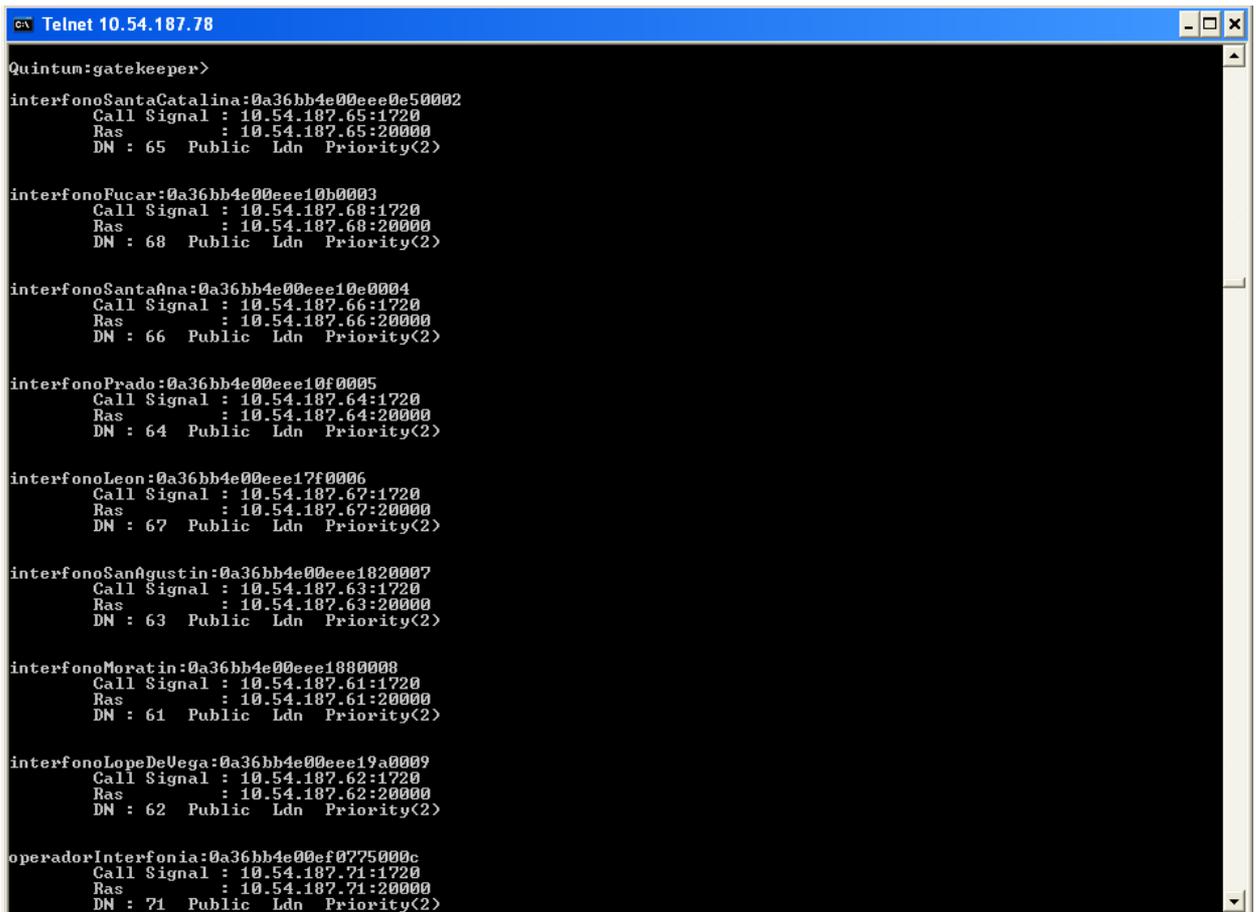
Quintum:gatekeeper> config
config# unit 1
config unit 1# ip 10.54.187.60
config unit 1# name gatekeeper
config unit 1# print
Unit: 1
IP Address = 10.54.187.60
External IP Address = 0.0.0.0
Name = gatekeeper

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):



```

Telnet 10.54.187.78
Quintum:gatekeeper>
interfonoSantaCatalina:0a36bb4e00eee0e50002
  Call Signal : 10.54.187.65:1720
  Ras        : 10.54.187.65:20000
  DN : 65 Public Ldn Priority(2)

interfonoFucar:0a36bb4e00eee10b0003
  Call Signal : 10.54.187.68:1720
  Ras        : 10.54.187.68:20000
  DN : 68 Public Ldn Priority(2)

interfonoSantaAna:0a36bb4e00eee10e0004
  Call Signal : 10.54.187.66:1720
  Ras        : 10.54.187.66:20000
  DN : 66 Public Ldn Priority(2)

interfonoPrado:0a36bb4e00eee10f0005
  Call Signal : 10.54.187.64:1720
  Ras        : 10.54.187.64:20000
  DN : 64 Public Ldn Priority(2)

interfonoLeon:0a36bb4e00eee17f0006
  Call Signal : 10.54.187.67:1720
  Ras        : 10.54.187.67:20000
  DN : 67 Public Ldn Priority(2)

interfonoSanAgustin:0a36bb4e00eee1820007
  Call Signal : 10.54.187.63:1720
  Ras        : 10.54.187.63:20000
  DN : 63 Public Ldn Priority(2)

interfonoMoratin:0a36bb4e00eee1880008
  Call Signal : 10.54.187.61:1720
  Ras        : 10.54.187.61:20000
  DN : 61 Public Ldn Priority(2)

interfonoLopezDeVega:0a36bb4e00eee19a0009
  Call Signal : 10.54.187.62:1720
  Ras        : 10.54.187.62:20000
  DN : 62 Public Ldn Priority(2)

operadorInterfonia:0a36bb4e00ef0775000c
  Call Signal : 10.54.187.71:1720
  Ras        : 10.54.187.71:20000
  DN : 71 Public Ldn Priority(2)

```

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:

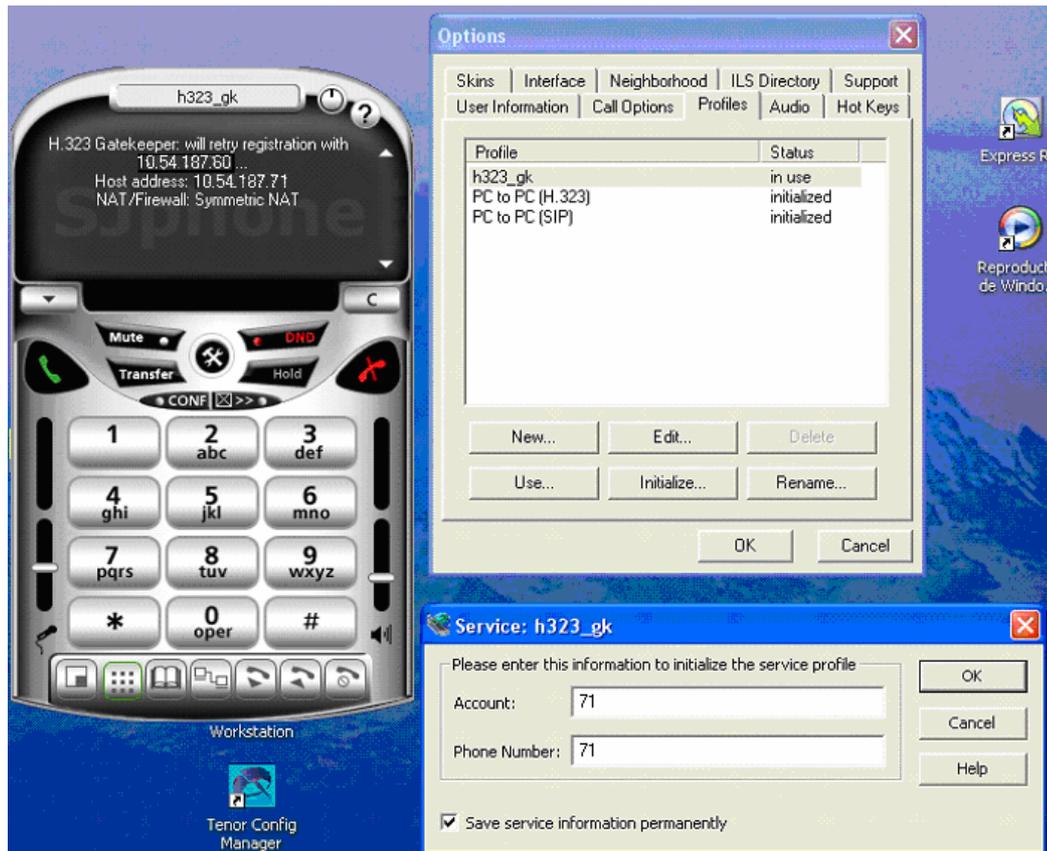


Figura 64: Configuración del número asociado al teléfono software SJPhone.

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):

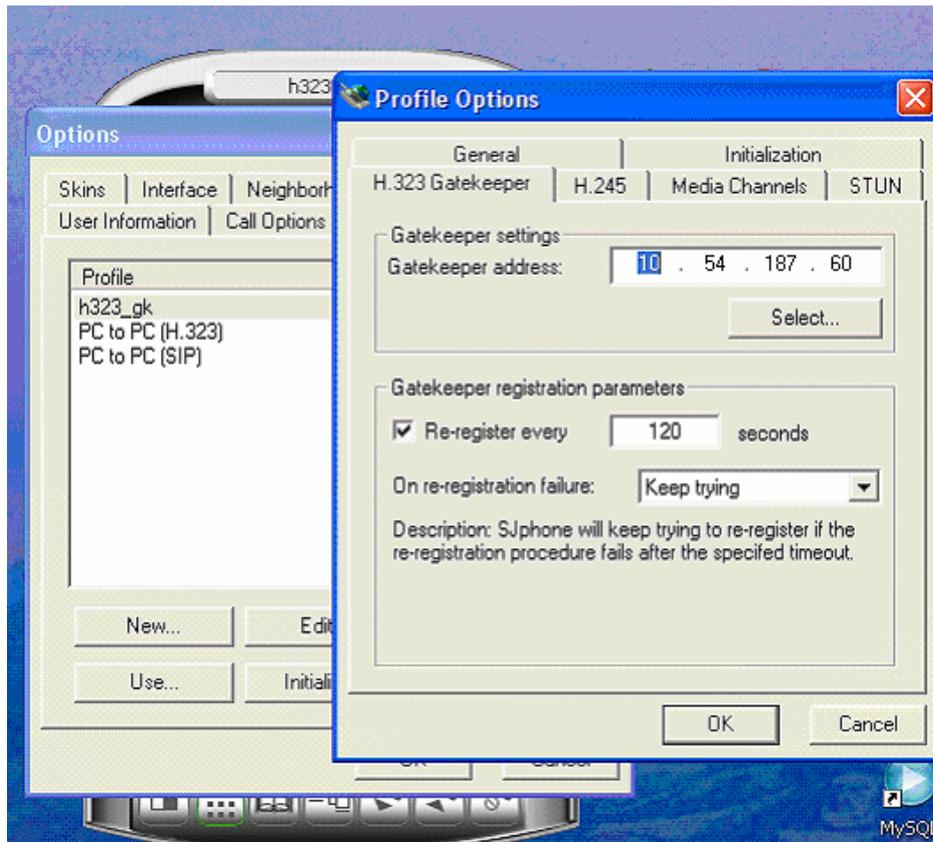


Figura 65: Configuración de parámetros H.323 en el teléfono software SJPhone.

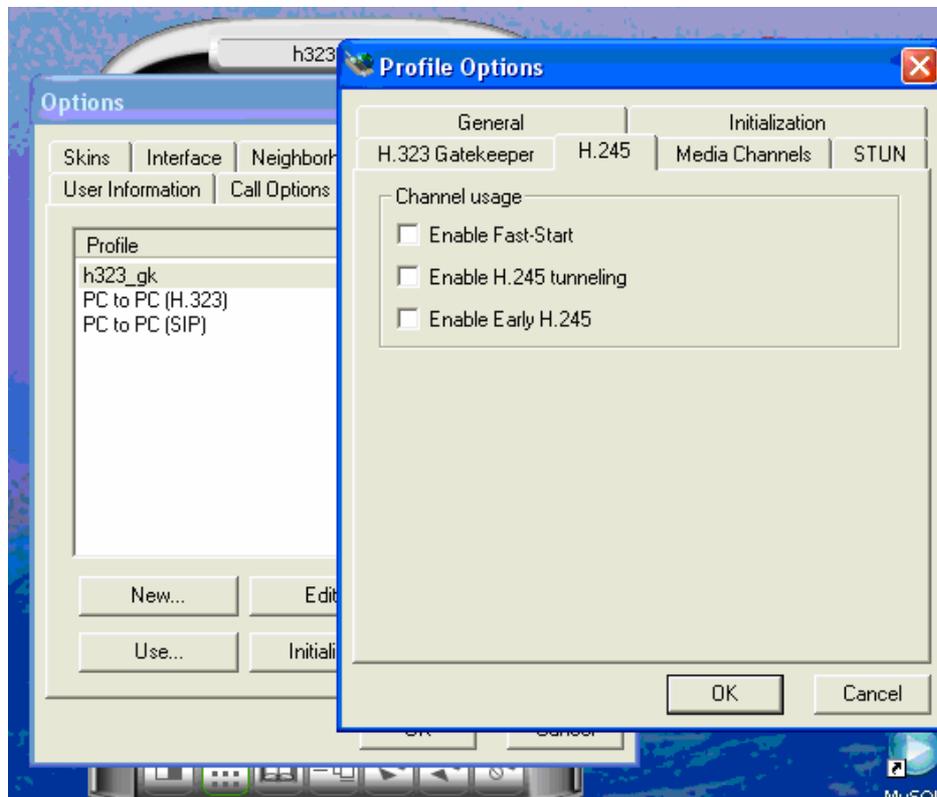


Figura 66: Configuración de parámetros H.245 en el teléfono software SJPhone.

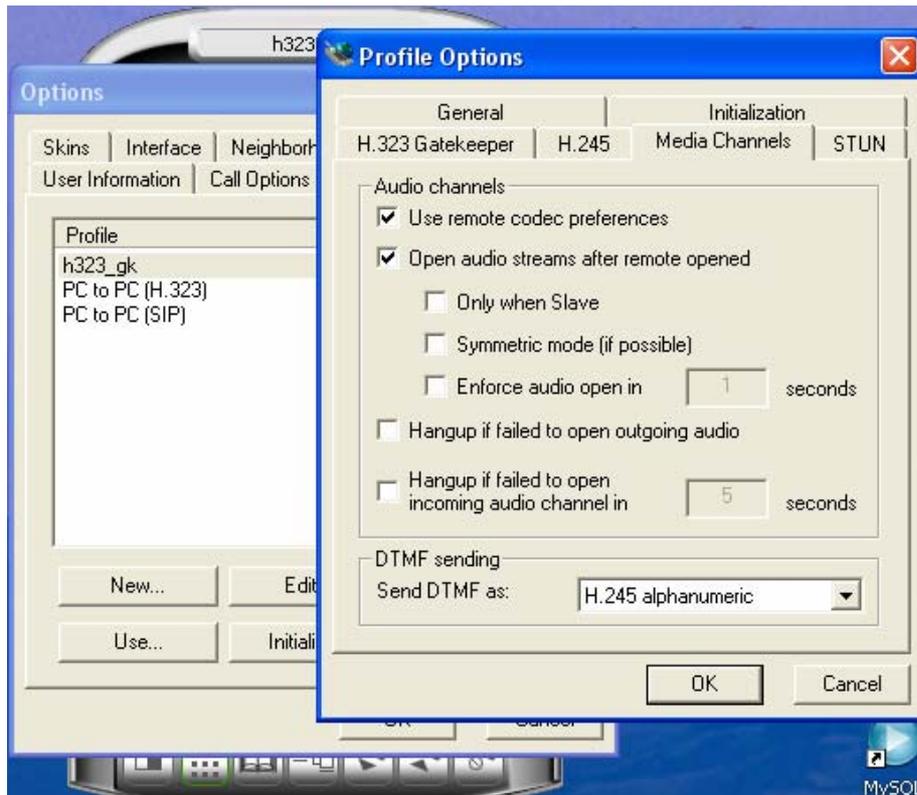


Figura 67: Configuración de parámetros de audio en el teléfono software SJPhone.

### 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 *firmwares* 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):

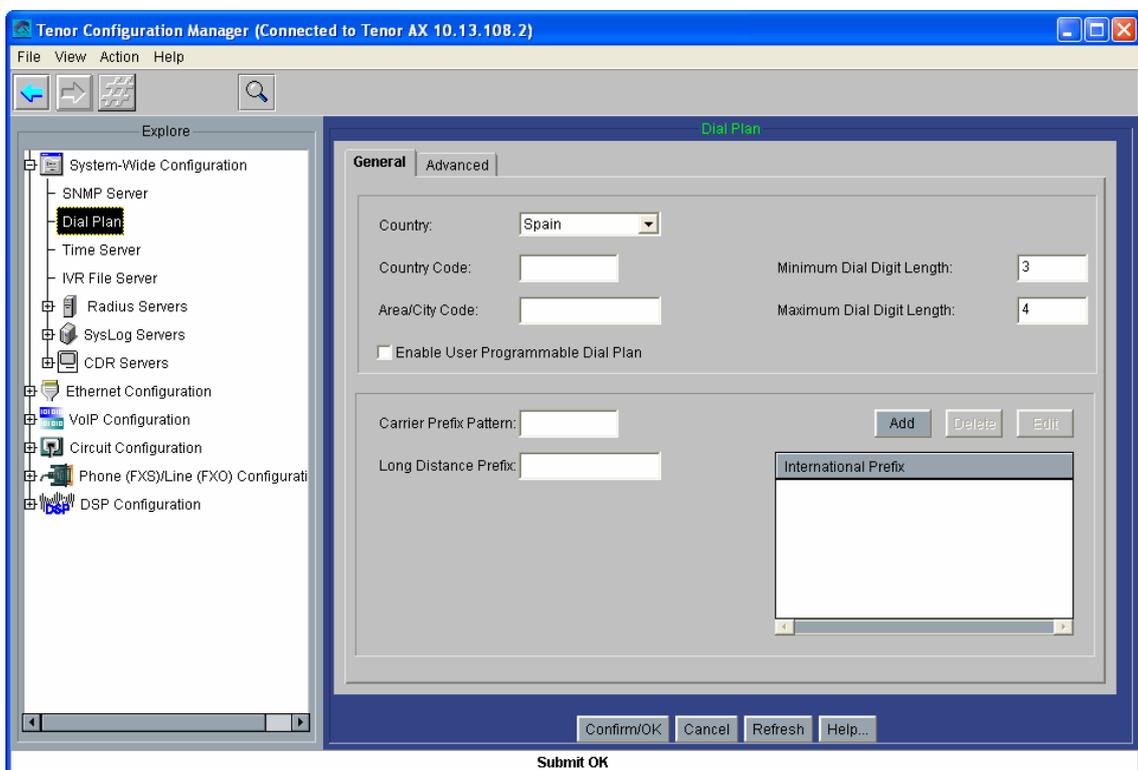


Figura 69: Captura 1 del *Tenor Configuration Manager* para la Plataforma de Interfonía Estación de Bailén.

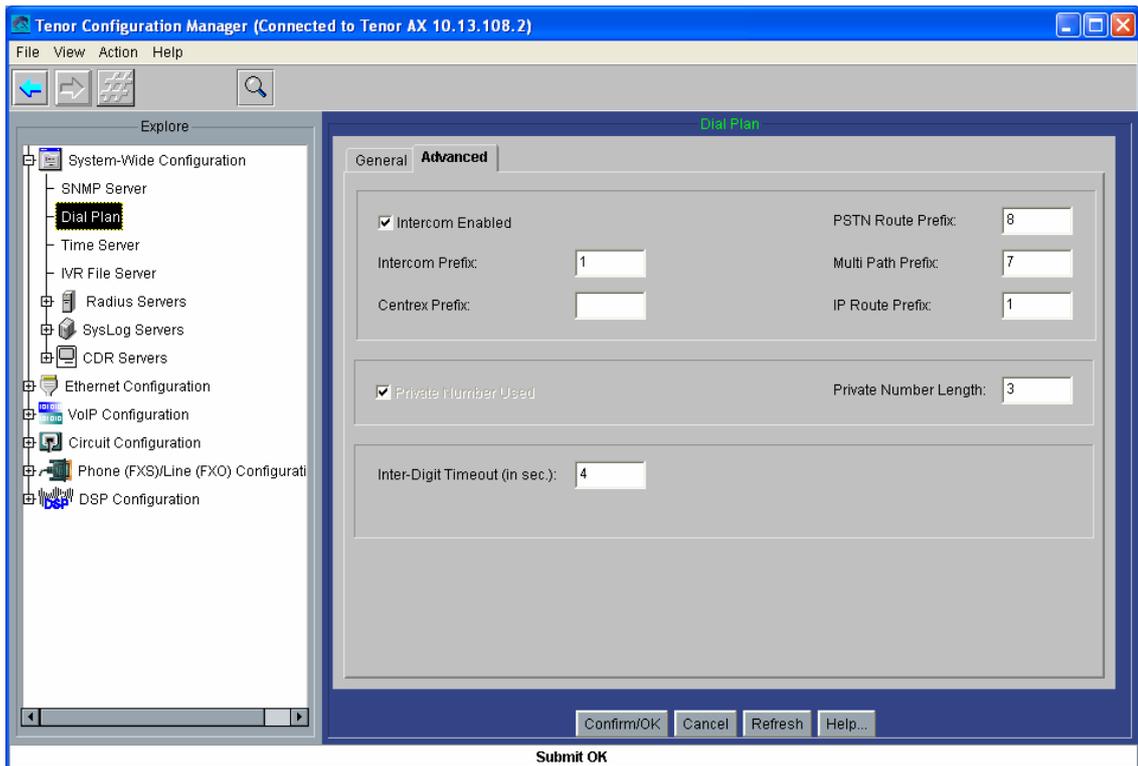


Figura 70: Captura 2 del *Tenor Configuration Manager* para la Plataforma de Interfonía Estación de Bailén.

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:

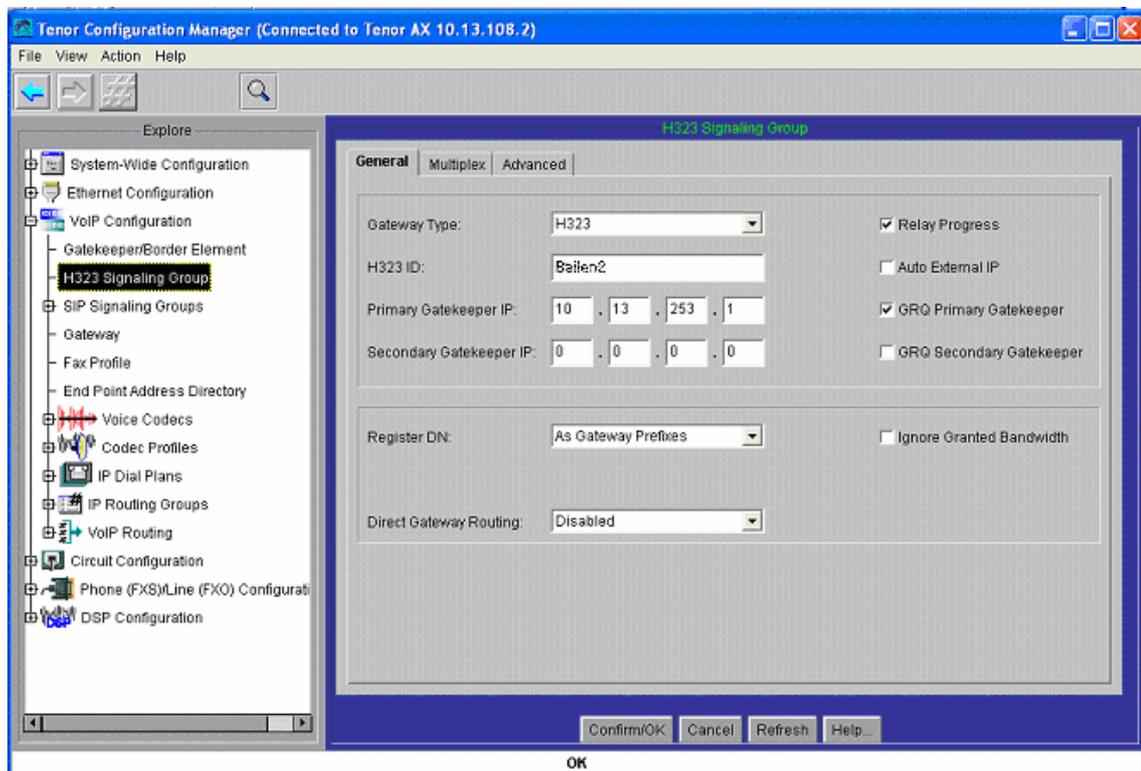


Figura 71: Captura 3 del *Tenor Configuration Manager* para la Plataforma de Interfonía Estación de Bailén.

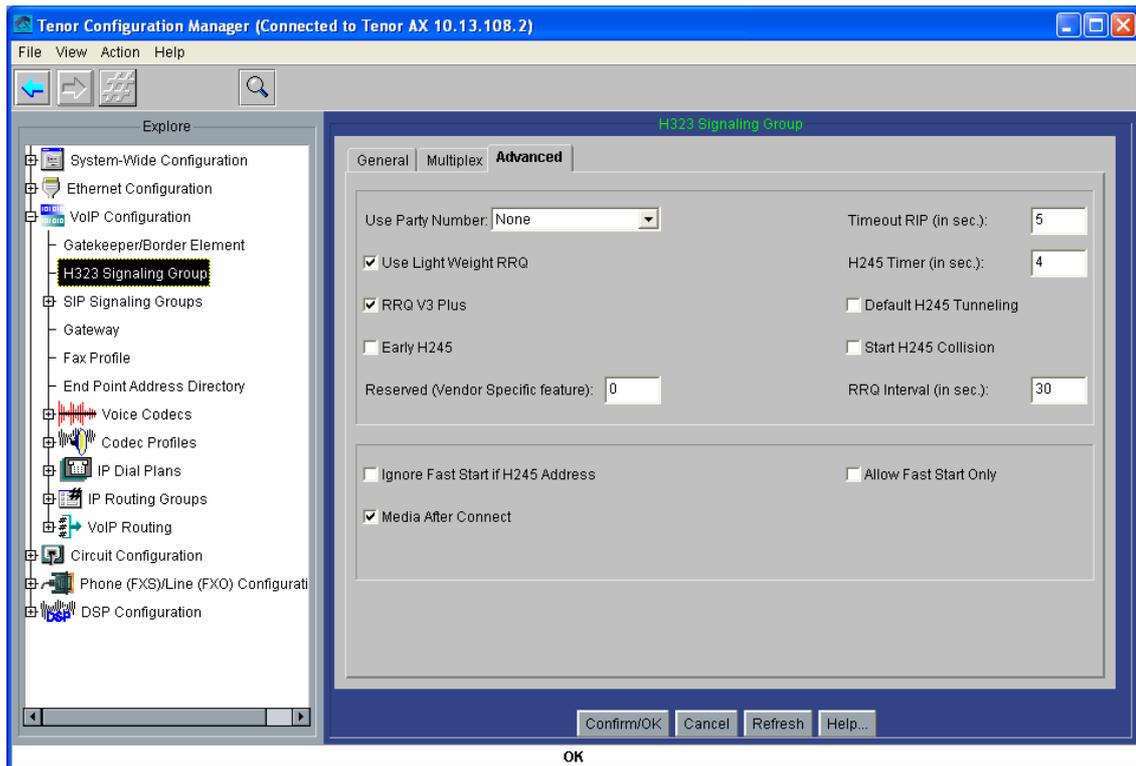


Figura 72: Captura 4 del *Tenor Configuration Manager* para la Plataforma de Interfonía Estación de Bailén.

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:

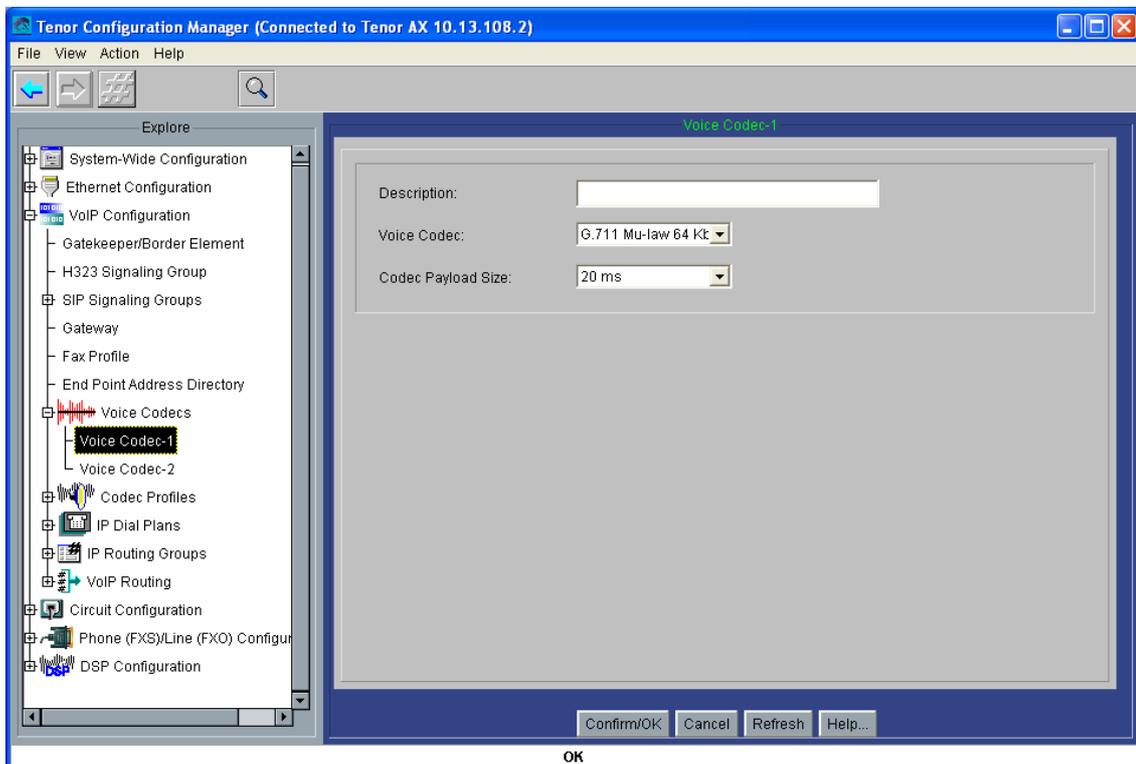


Figura 73: Captura 5 del *Tenor Configuration Manager* para la Plataforma de Interfonía Estación de Bailén.

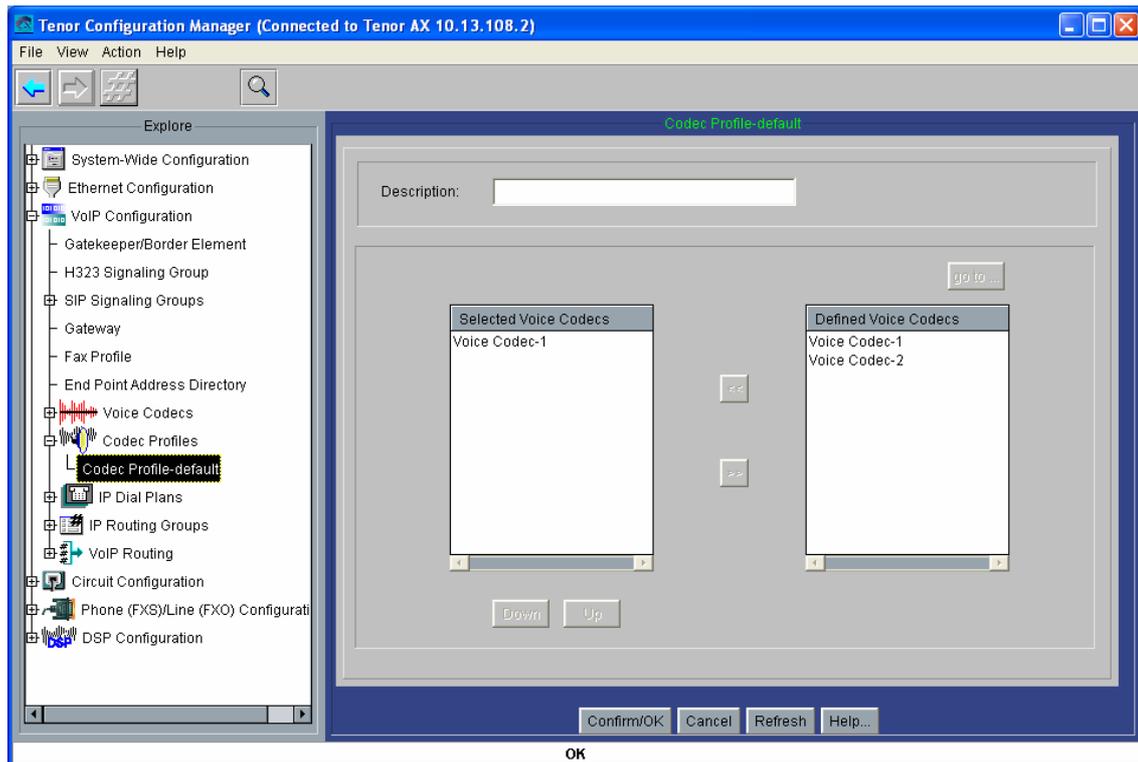


Figura 74: Captura 6 del *Tenor Configuration Manager* para la Plataforma de Interfonía Estación de Bailén.

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 señala 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):

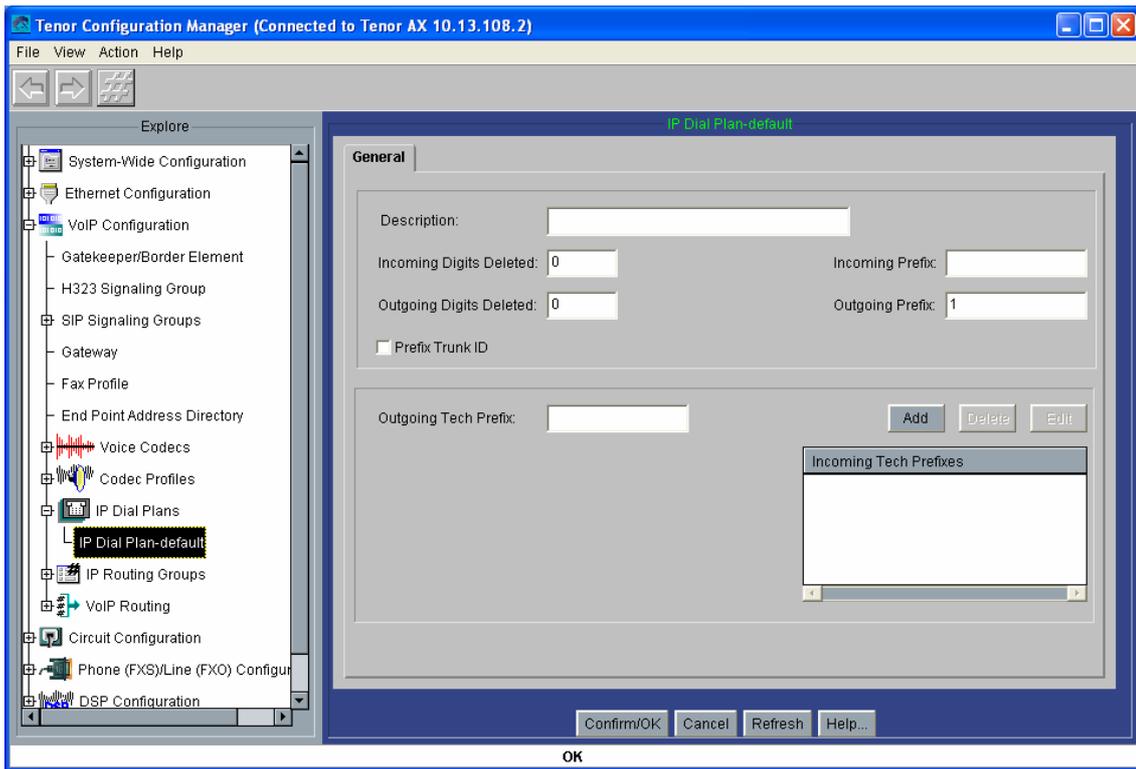


Figura 75: Captura 7 del *Tenor Configuration Manager* para la Plataforma de Interfonía Estación de Bailén.

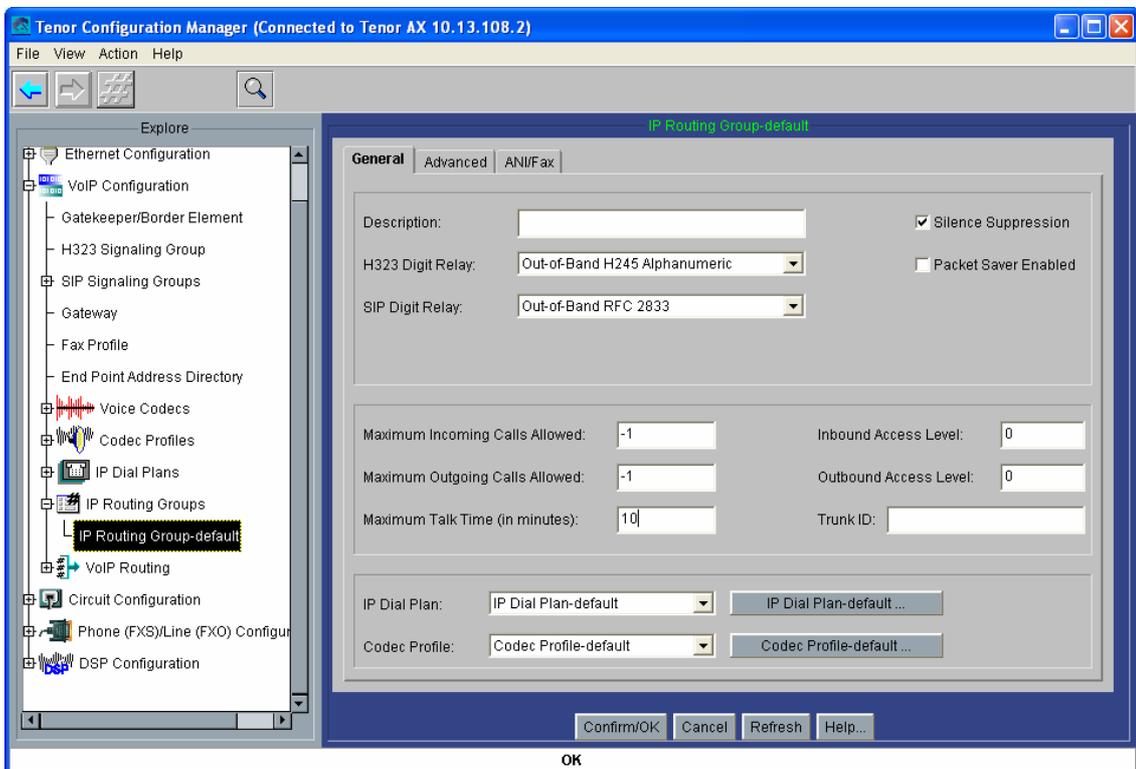


Figura 76: Captura 8 del *Tenor Configuration Manager* para la Plataforma de Interfonía Estación de Bailén.

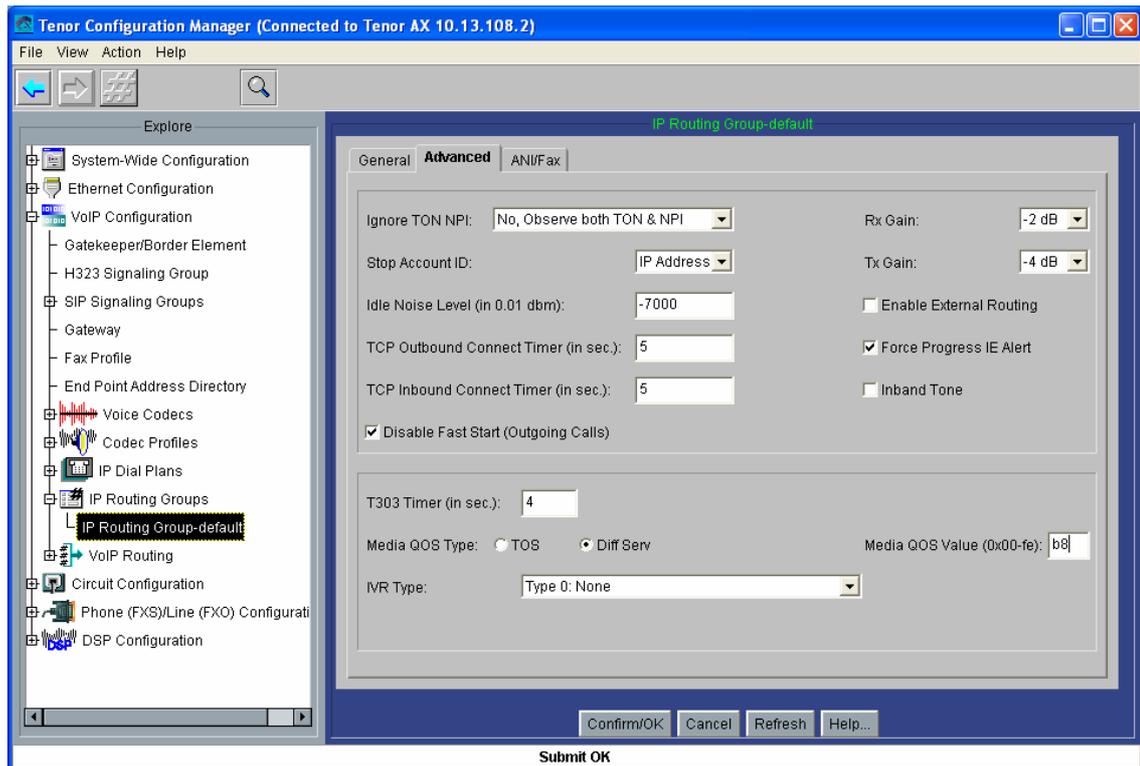


Figura 77: Captura 9 del *Tenor Configuration Manager* para la Plataforma de Interfonía Estación de Bailén.

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<sup>47</sup> 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  $\Omega$  (parámetro *Impedance*) (todo esto, para la correcta comunicación analógica con los interfonos), en la figura 80:

<sup>47</sup> FSK: *Frequency 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.

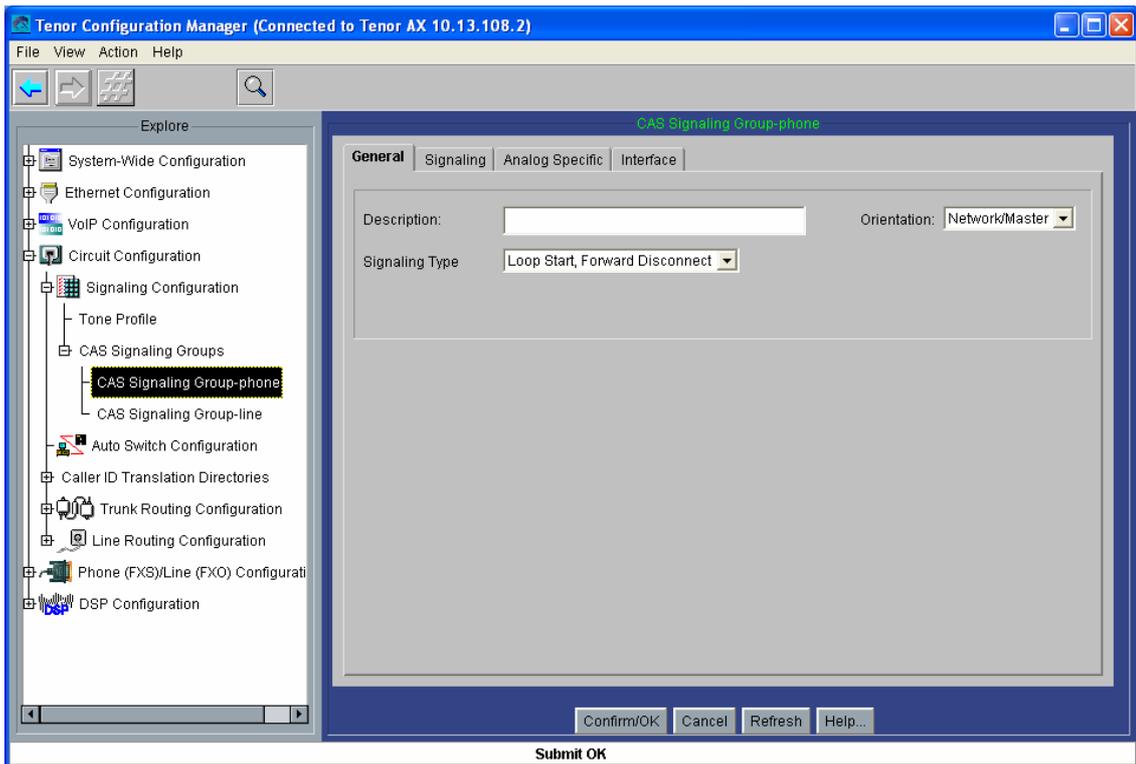


Figura 78: Captura 10 del *Tenor Configuration Manager* para la Plataforma de Interfonía Estación de Bailén.

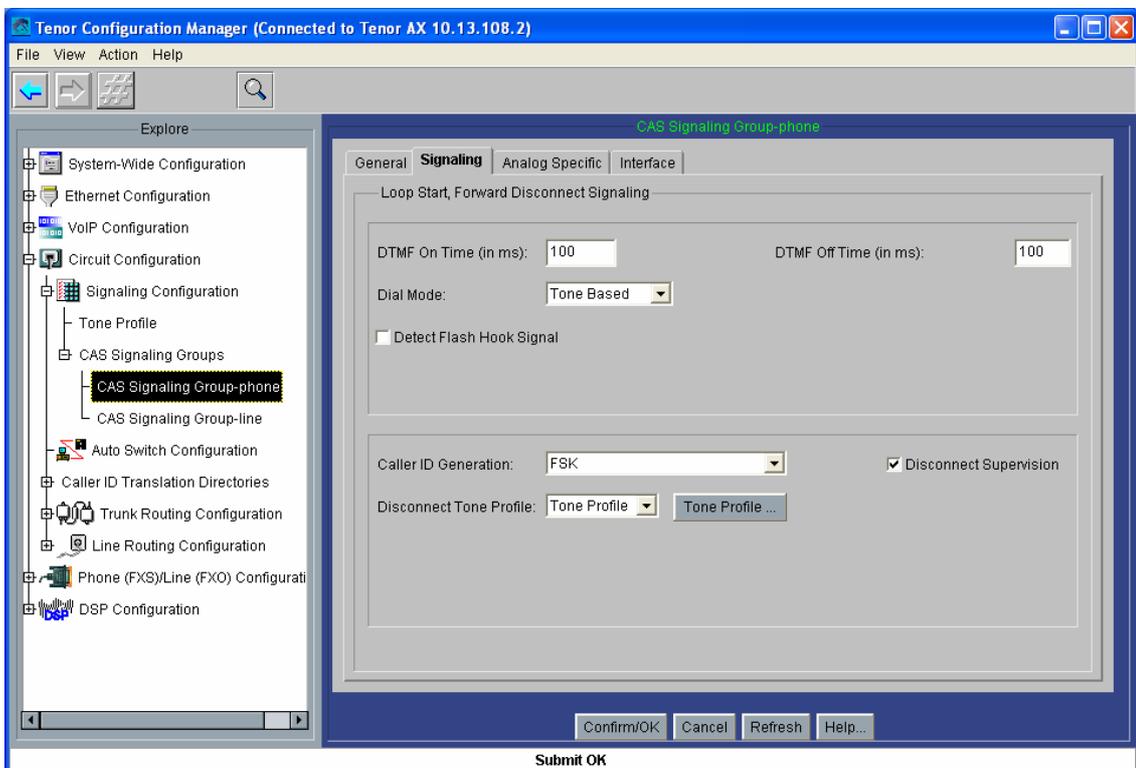


Figura 79: Captura 11 del *Tenor Configuration Manager* para la Plataforma de Interfonía Estación de Bailén.

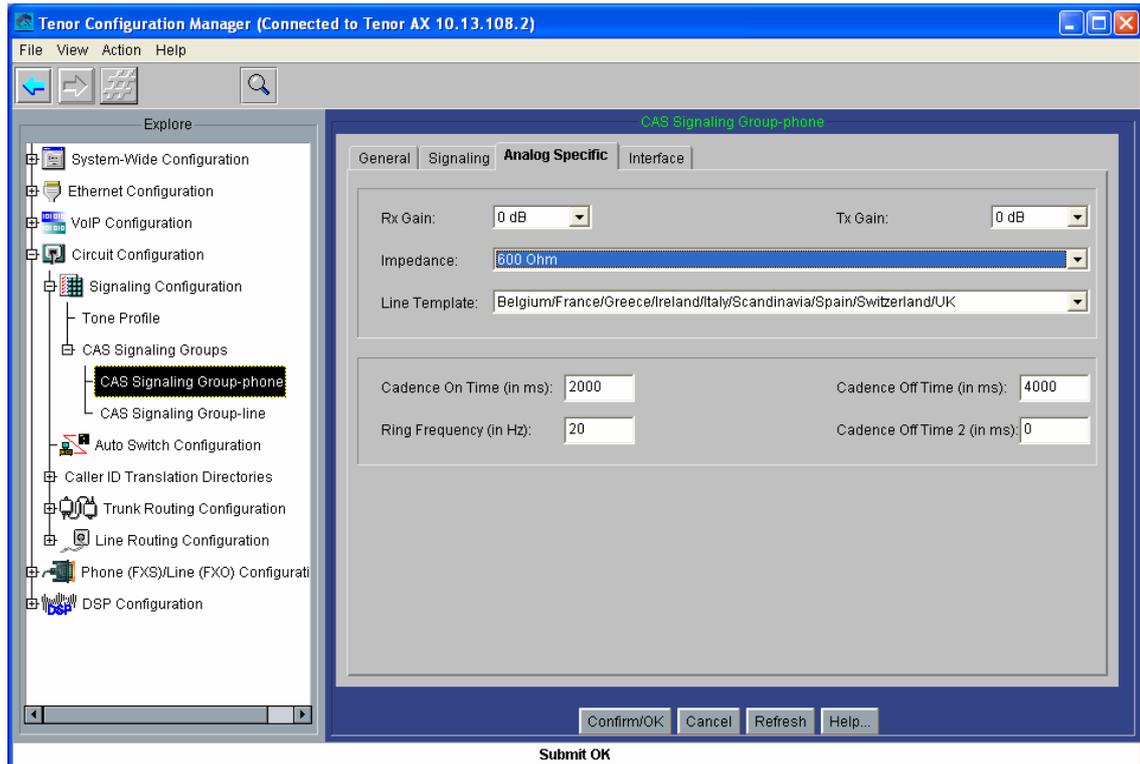


Figura 80: Captura 12 del *Tenor Configuration Manager* para la Plataforma de Interfonía Estación de Bailén.

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):

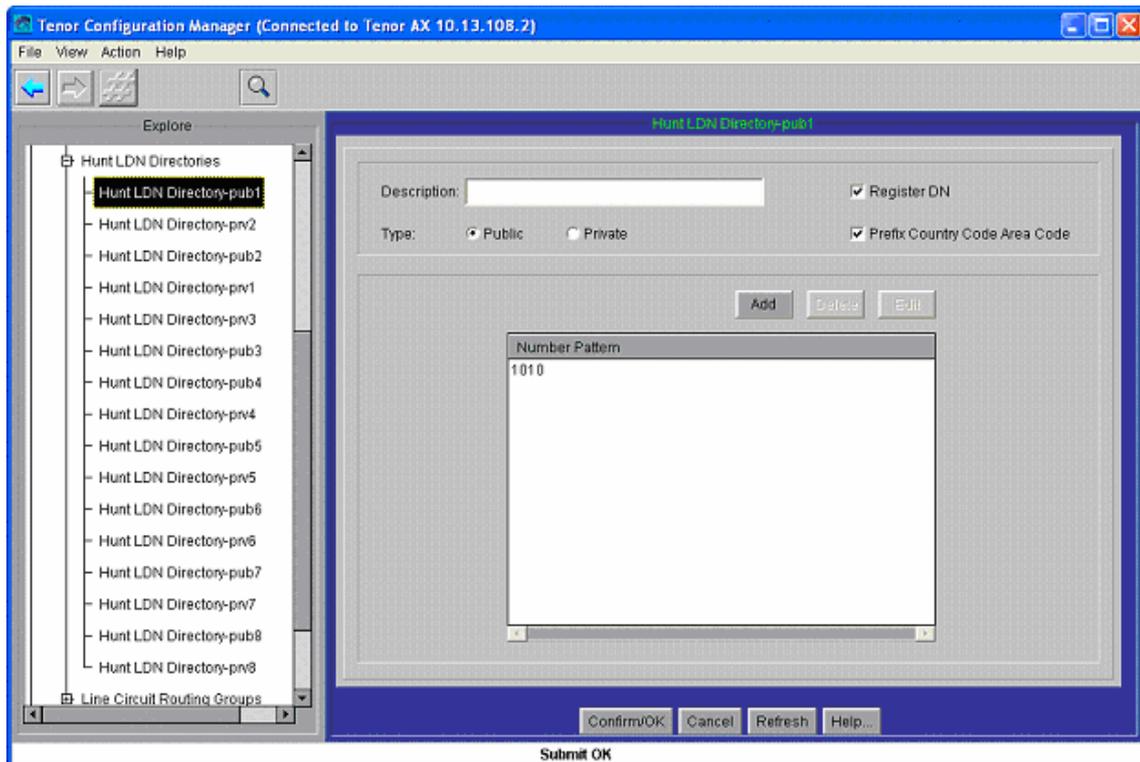


Figura 81: Captura 13 del *Tenor Configuration Manager* para la Plataforma de Interfonía Estación de Bailén.

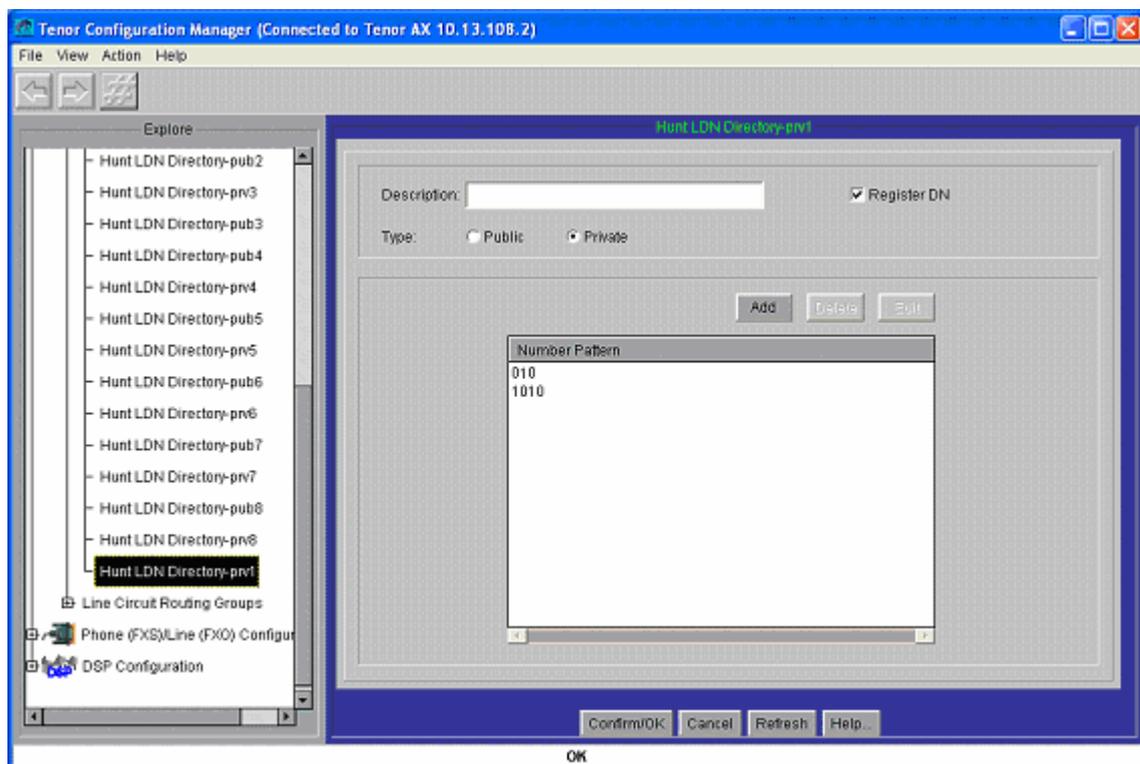


Figura 82: Captura 14 del *Tenor Configuration Manager* para la Plataforma de Interfonía Estación de Bailén.

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):

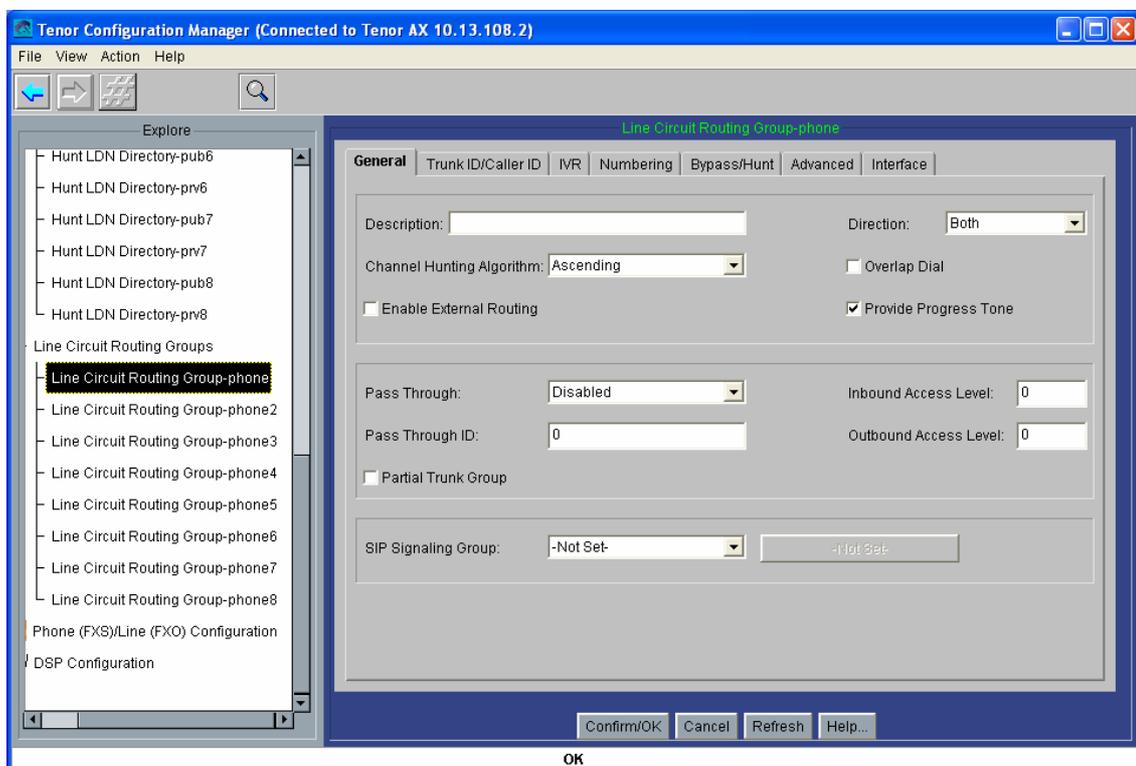


Figura 83: Captura 15 del *Tenor Configuration Manager* para la Plataforma de Interfonía Estación de Bailén.

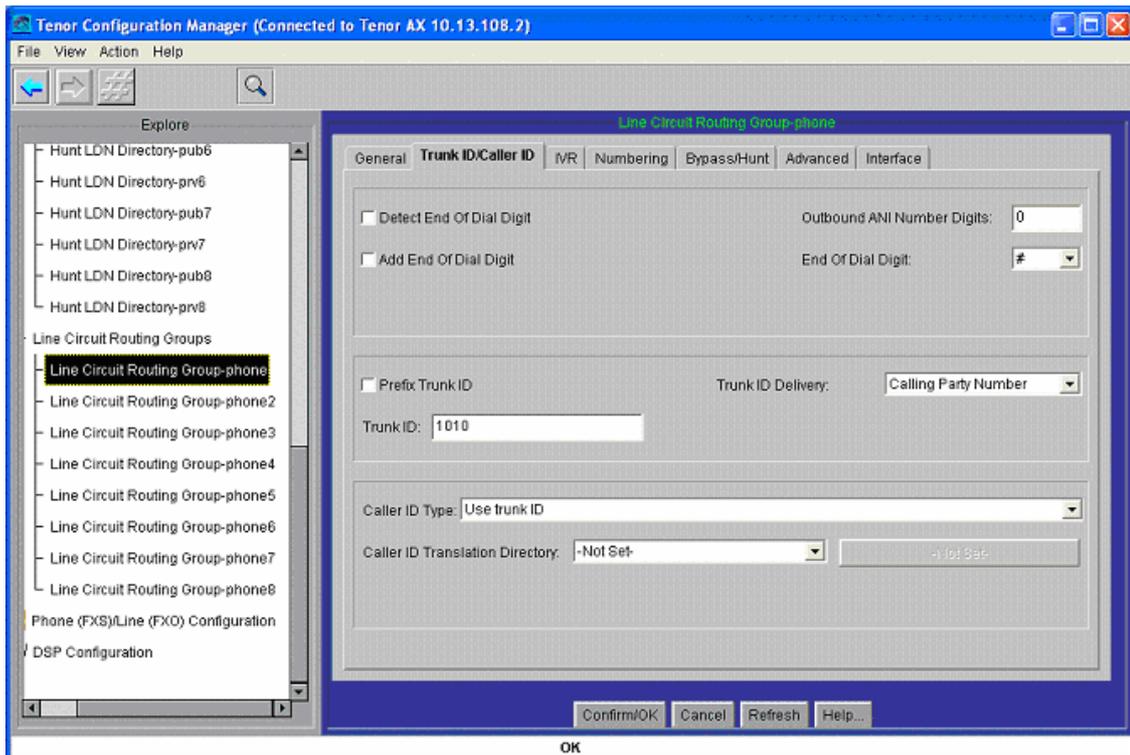


Figura 84: Captura 16 del *Tenor Configuration Manager* para la Plataforma de Interfonía Estación de Bailén.

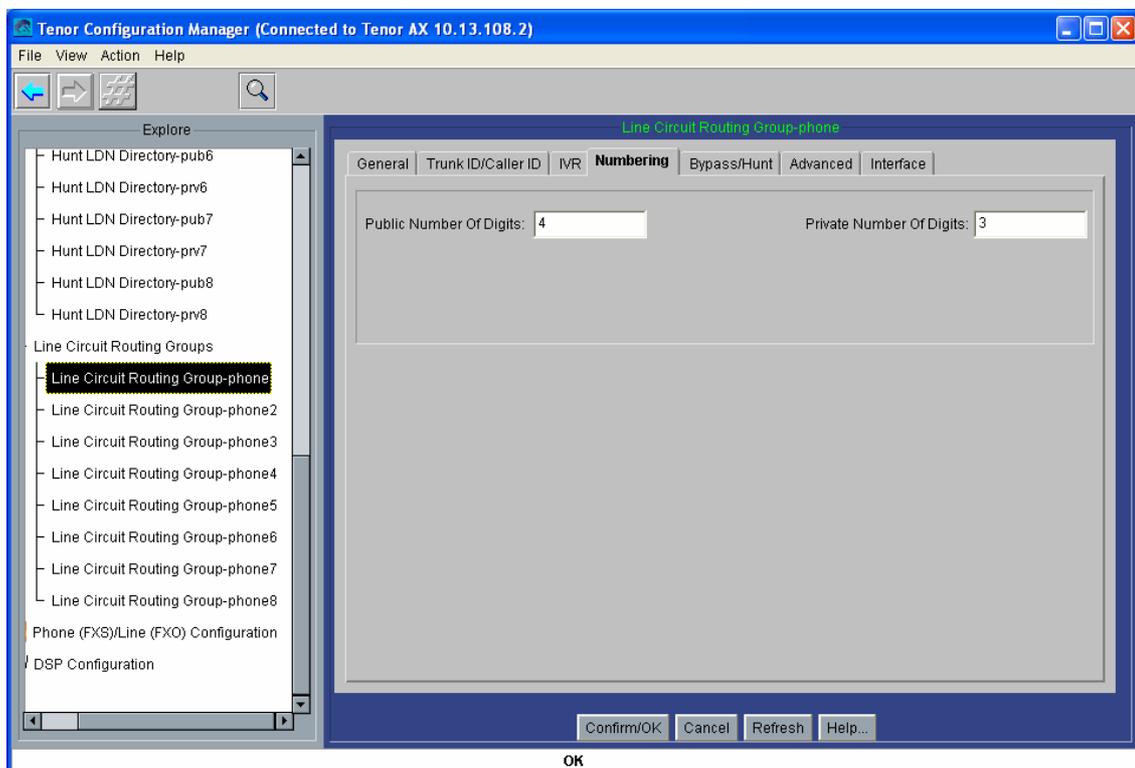


Figura 85: Captura 17 del *Tenor Configuration Manager* para la Plataforma de Interfonía Estación de Bailén.

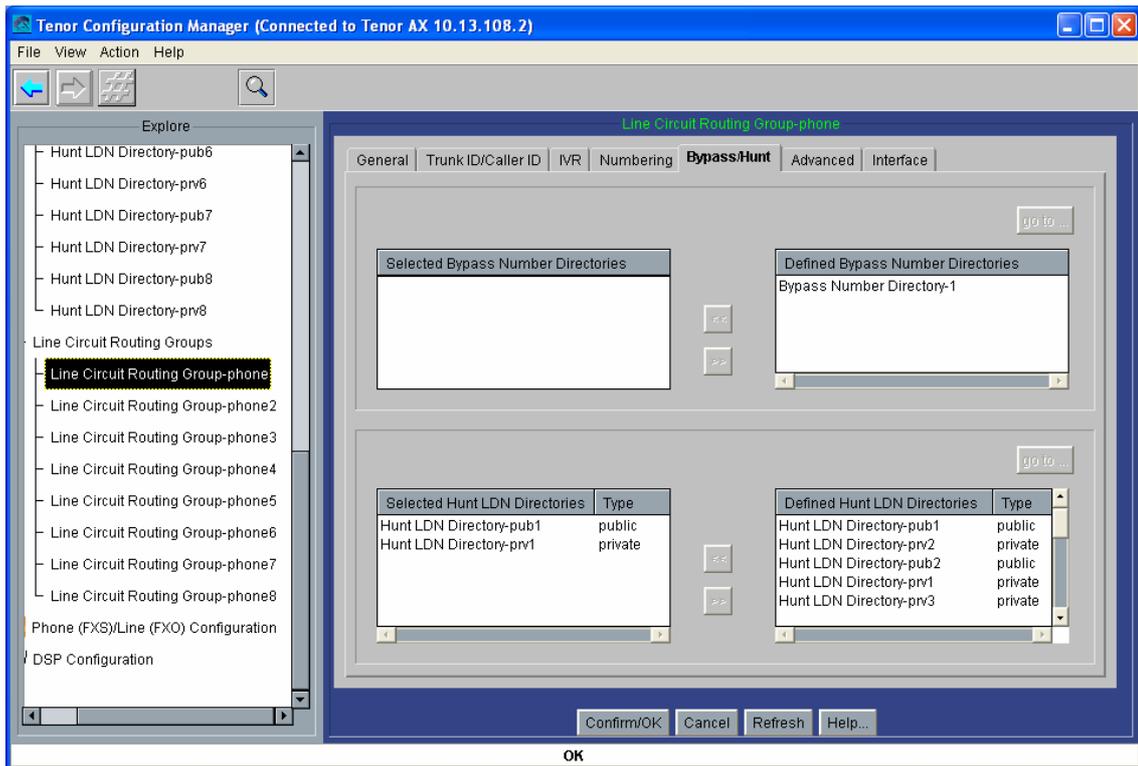


Figura 86: Captura 18 del *Tenor Configuration Manager* para la Plataforma de Interfonía Estación de Bailén.

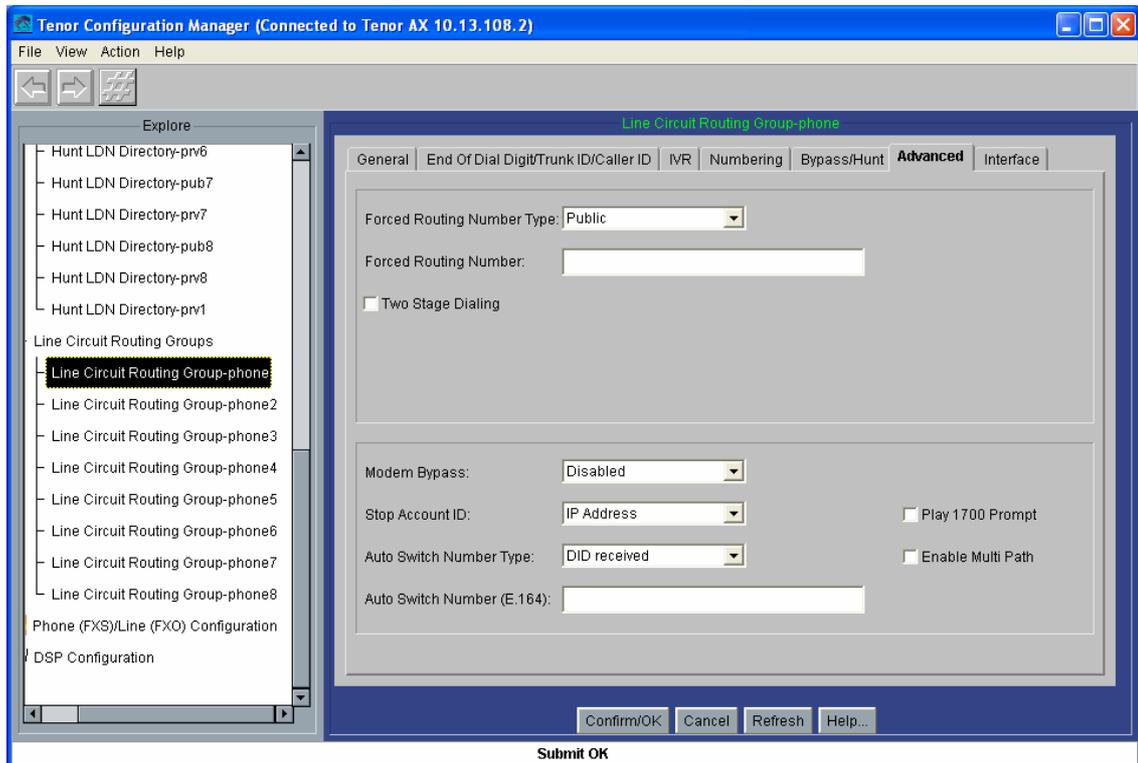


Figura 87: Captura 19 del *Tenor Configuration Manager* para la Plataforma de Interfonía Estación de Bailén.

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):

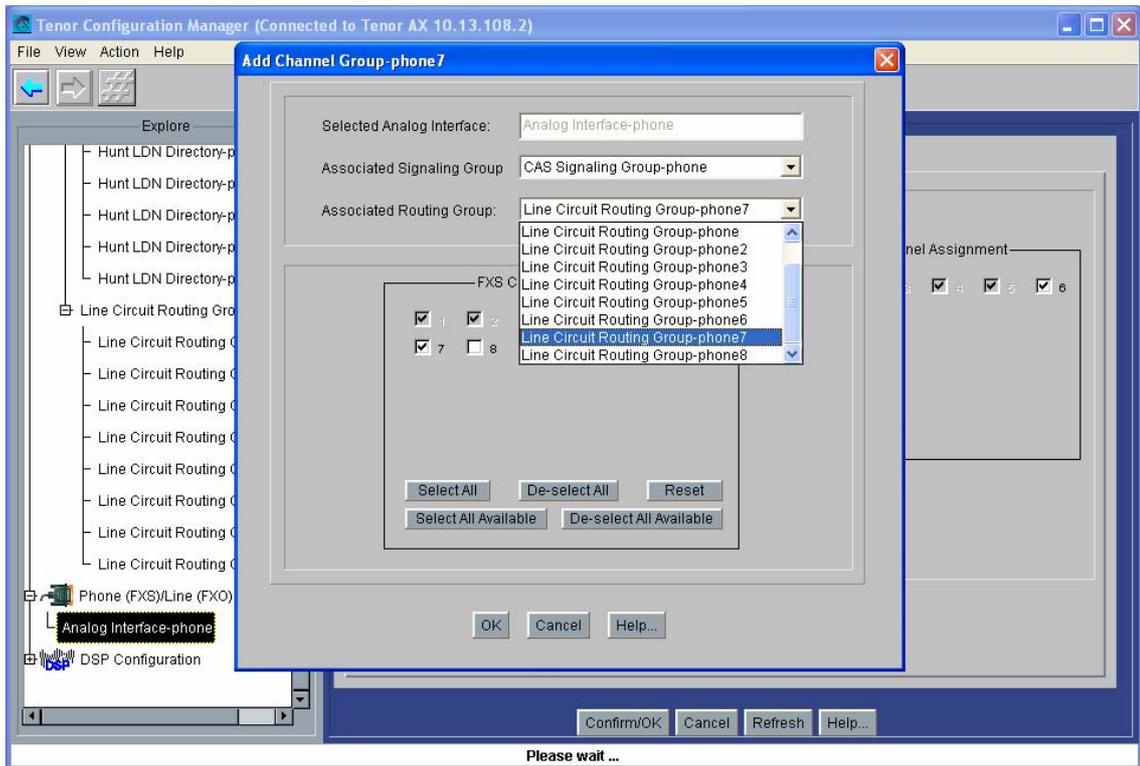


Figura 88: Captura 20 del *Tenor Configuration Manager* para la Plataforma de Interfonía Estación de Bailén.

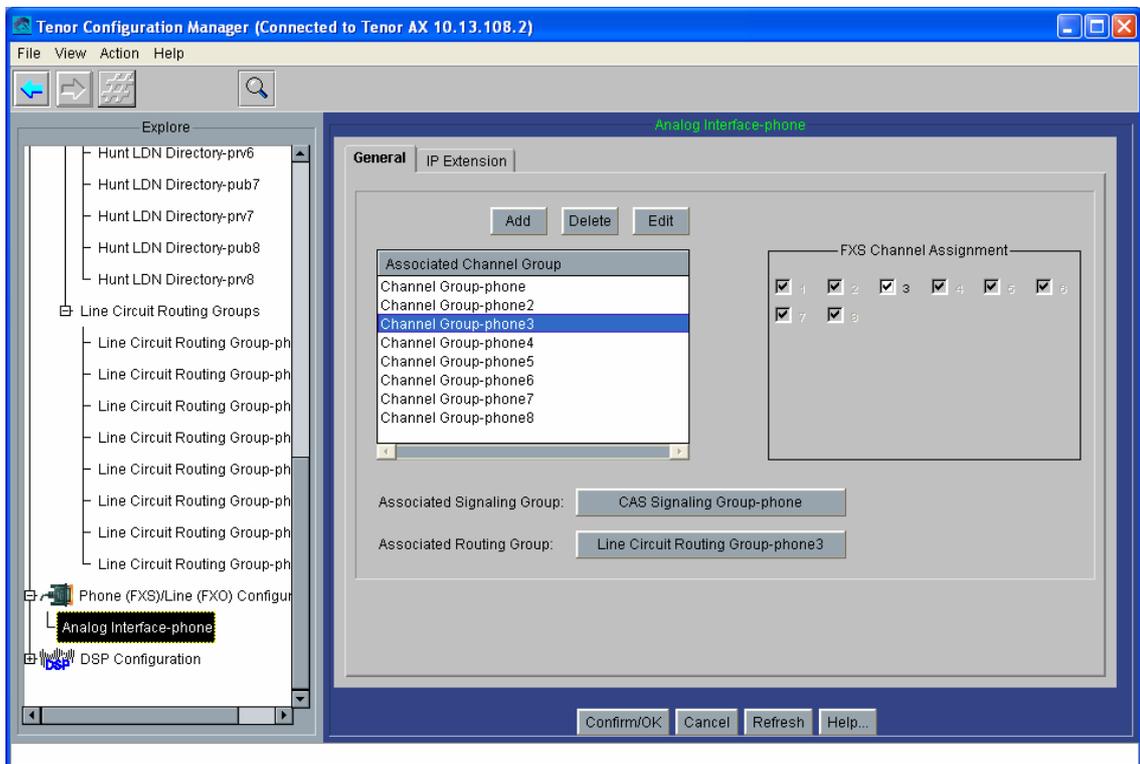


Figura 89: Captura 21 del *Tenor Configuration Manager* para la Plataforma de Interfonía Estación de Bailén.

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 `ldxxxxxxxxxxxxxx`, donde `xxxxxxxxxxxxxx` 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 transmitir 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:0001010000000000000010000000000000
# 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

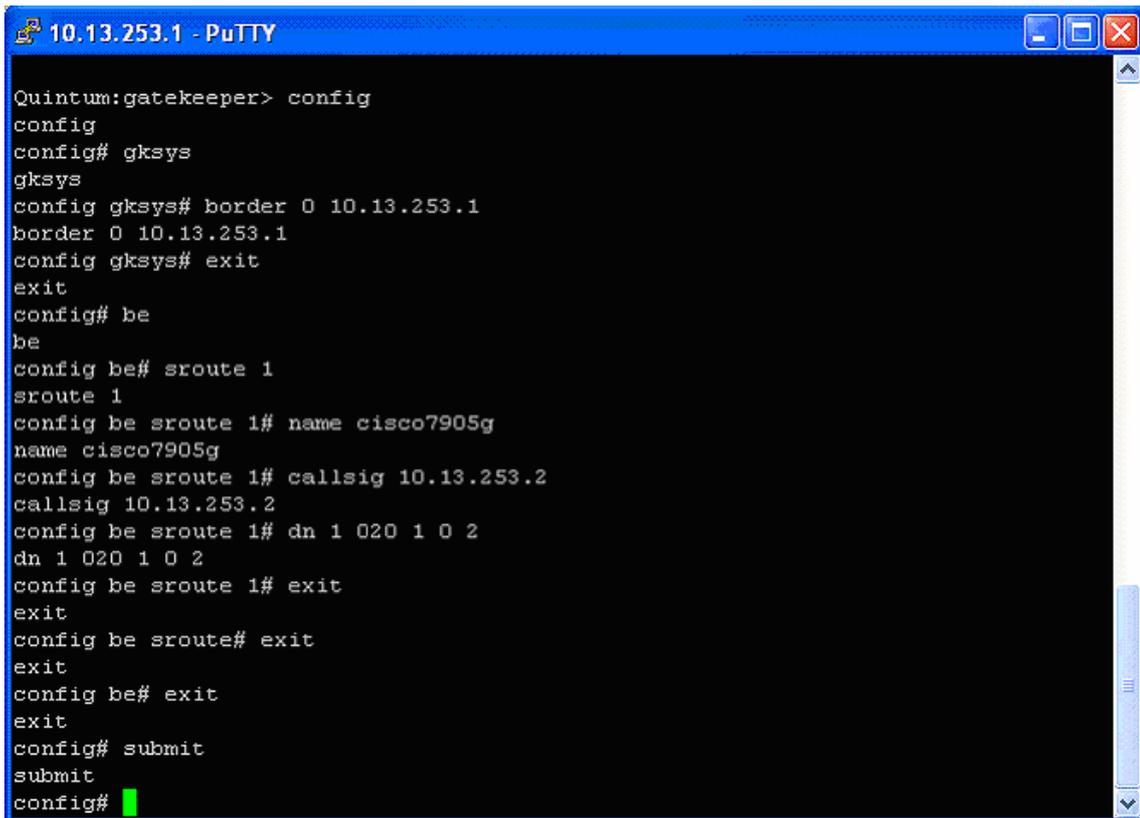
continuación, se le añade el número al que va a asociarse en el *border element* esa IP: comando `dn index dn# type route priority`, donde:

- `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:



```
10.13.253.1 - PuTTY
Quintum:gatekeeper> config
config
config# gksys
gksys
config gksys# border 0 10.13.253.1
border 0 10.13.253.1
config gksys# exit
exit
config# be
be
config be# sroute 1
sroute 1
config be sroute 1# name cisco7905g
name cisco7905g
config be sroute 1# callsig 10.13.253.2
callsig 10.13.253.2
config be sroute 1# dn 1 020 1 0 2
dn 1 020 1 0 2
config be sroute 1# exit
exit
config be sroute# exit
exit
config be# exit
exit
config# submit
submit
config#
```

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 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 encontrarse 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<sup>48</sup>, los *call flow* IVR<sup>49</sup> 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:

---

<sup>48</sup> RADIUS: *Remote Access Dial In Use Server*, protocolo de Autorización, Autenticación y *Accounting* para aplicaciones de acceso a una red.

<sup>49</sup> 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.

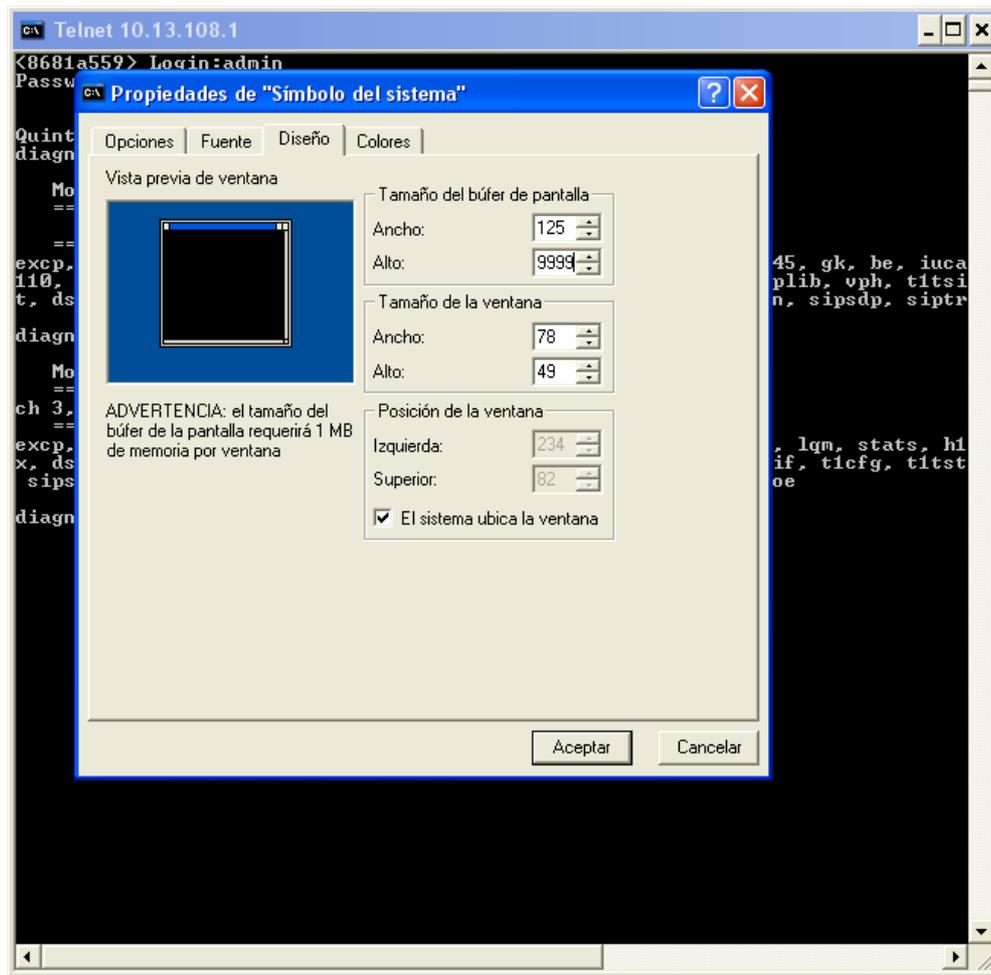


Figura 95: Ampliación de la ventana de comandos MSDOS en Windows XP.

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
ll        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
tltsi     DS1 boards TSI log
tlisr     DS1 boards ISR log
tlcc      DS1 boards Call Control log
tlfrmr    DS1 boards framer log
tll2      DS1 boards Layer 2 ISDN signaling log
tllif     DS1 boards Inter signaling Layers log
tlcfg     DS1 boards configuration log
tltst     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 1[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 11 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:

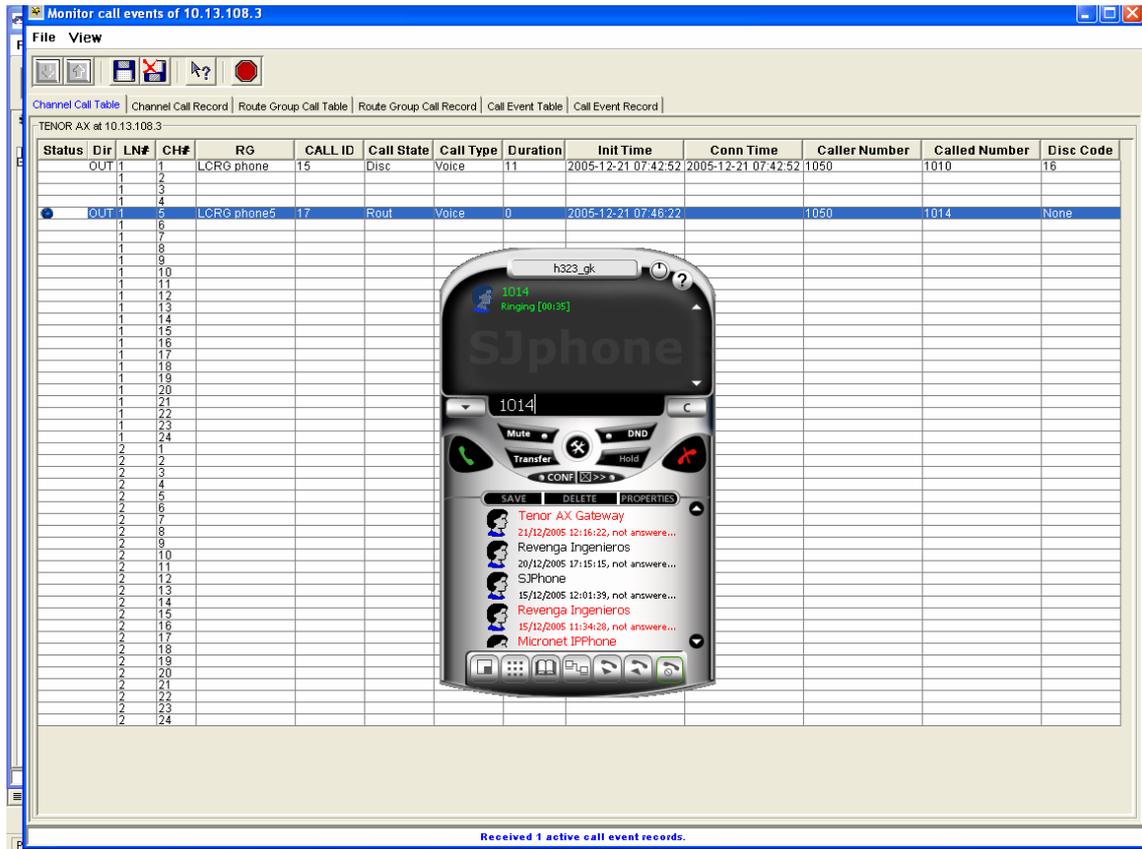


Figura 98: Comportamiento del *Tenor Monitor* mientras se efectúa una llamada contra un Quintum Tenor.

Puede monitorizar CDR<sup>50</sup>, llamadas activas, y alarmas, en tiempo real, y generando *logs* (figura 99):

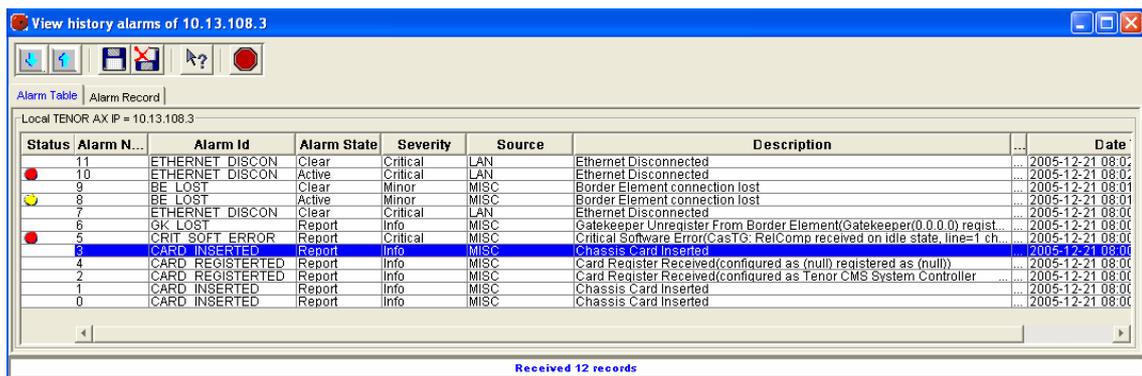


Figura 99: Muestra del histórico de alarmas de los Quintum Tenor, monitorizados por el *Tenor Monitor*.

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

<sup>50</sup> CDR: *Call Detail Record*, registro de detalle de llamadas.

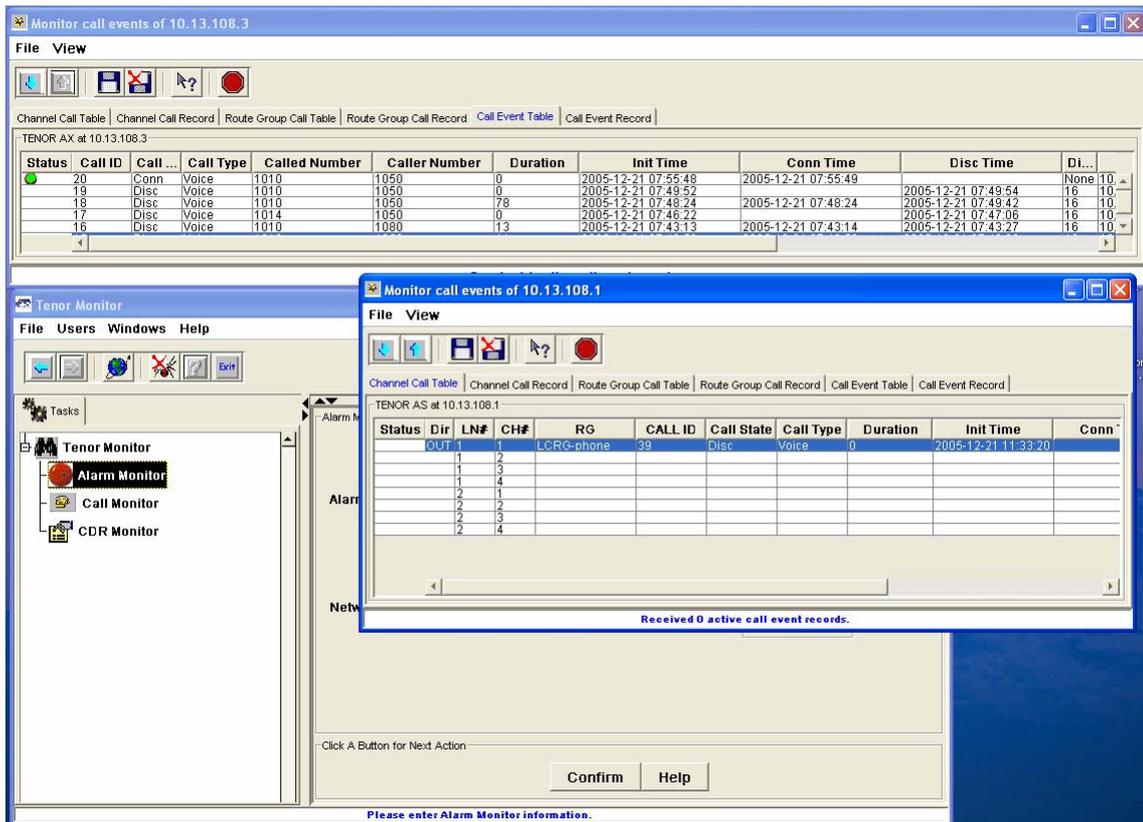


Figura 100: Actividad de las llamadas entre los equipos Quintum Tenor desde el *Tenor Monitor*.

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<sup>51</sup> 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<sup>52</sup>, 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 Quintum 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.

<sup>51</sup> NAT: *Network Address Translation*, traducción de direcciones de red, para transformar direcciones IP públicas en privadas.

<sup>52</sup> 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 11`; máximo con `ev 13`.

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:

```

C:\Documents and Settings\Ramon Montoya\Mis documentos\cisco 7905g\prserv.exe
h245.c 1402 : 0
TSAPI0 <0xa0dfd03 49242>
UNSUPPORTED RxOLC codec 17
UNSUPPORTED : dataType in HandleFastStartPDU
UNSUPPORTED RxOLC codec 0
UNSUPPORTED : dataType in HandleFastStartPDU
UNSUPPORTED RxOLC codec 0
UNSUPPORTED : dataType in HandleFastStartPDU
index = 2, maxFrmCnt = 20
G711/G729: 20 fpp
<pref setmode inmode> = 15 3 3
rnt req Fstart
Setup routed to 0
Caller <addr name> <1050>, Ordenador Ramon
>> callingpartynumber info: 0x60 0x0 0
Q931<-0>:Proceeding
Build FastStart Response
H245<-0>:LcseOpen
Tx=G711 <3> 20 fpp
H245->0:LcseOpenAck
RTP<-0>:<0xa0dfd03 49242>
I0]Enable encoder 0
RTP Tx[I0]:SSRC_ID = 9f82135e
RTP Tx Init: 0, 0
fstart.c 400 : 0x0
OpenRtpRxPort<0,0x0,16384>:9
RTP Rx Init: 0, 0
RTP->0:<0xa0dfd0f 16384>
CESE/MSDSE start:<0 0 0 0>
Q931<-0>:H245/Facility
capSize = 3
Q931<-0>:H245/Facility
GK<-0>: ARQ: 0
Q931->0:Facility
H245 in Q931msg
H245->0:Cese
RemoteAudioCap <4 17>
RemoteAudioCap <4 0>
RemoteAudioCap <4 0>
RemoteAudioCap <4 3>
Q931<-0>:H245/Facility
GK->0: ACF:0:direct call
CallRasCallBack: 1 33e1917 33e1a65 33e3c8a
SCC<-Alerting <Ordenador Ramon <null>>
SCC-><0 0> <cmd 3>
*** AS:0 ***
Q931->0:Facility
H245 in Q931msg
H245->0:MSD: <rn tt> = <0x7d04 50>
Q931<-0>:H245/Facility
Build FastStart Response
Q931<-0>:Alerting
Q931->0:Facility
H245 in Q931msg
H245->0:CeseAck
Q931->0:Facility
H245 in Q931msg
H245->0:MsdAck
2:00;2.0,0.0.

```

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 direccionamiento: 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<sup>53</sup> 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 interesantes 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.

---

<sup>53</sup> 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<sup>54</sup> 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.

<sup>54</sup> 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 interoperabilidad, 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<sup>55</sup>) 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.

---

<sup>55</sup> MicroPYME: Empresa con menos de 10 trabajadores.