Experiencias de Voz sobre IP en la Universitat de les Illes Balears

Experiences of VoIP at the Universitat de les Illes Balears

A. Pérez, B. Serra y A. Sola

Resumen

Son numerosos los estudios teóricos y de laboratorio que se han desarrollado acerca de Voz sobre IP y Telefonía IP. El proyecto desarrollado por el Centro de Tecnologías de la Información tiene como objetivo realizar un estudio sobre el diseño, instalación y mantenimiento de una red de Voz sobre IP dentro de un entorno en producción.

Los problemas que encontramos en una implementación real son distintos a los que se pueden analizar en un estudio teórico o en un laboratorio con maquetas. El motivo es por una parte los usuarios, distribuidos por nuestra LAN, WAN e Internet, y por la otra los diversos equipos y sistemas que deben interoperar para proveer un buen servicio.

A día de hoy, hace ya un año que tenemos en producción el servicio de Telefonía IP y hemos conseguido una coexistencia totalmente transparente con la telefonía tradicional.

Palabras clave: Voz sobre IP, Telefonía IP, VoIP, convergencia, implementación real.

Summary

There are numerous studies, both theoretical and laboratory, made on Voice over IP (VoIP) and IP Telephony. The project developed by the Center of Information Technologies, has the objective to make a study on the design, installation and maintenance of a production network of VoIP.

The problems encountered in a real implementation are different to those analyzed in a theoretical study or a laboratory model. The reasons for that are on one hand the users, distributed over our LAN, WAN and Internet, and on the other hand the existence of the various systems and pieces of equipment that must interoperate to provide a good service.

As of today, we have had a production IP Telephony system working for over a year, and have achieved a totally transparent coexistence with the traditional telephony system.

Keywords: Voice over IP, Telephony IP, VoIP, convergence, real implementation.

Estudio sobre diseño, instalación y mantenimiento de una red de Voz IP en producción

1.- Introducción

La Voz sobre IP es un concepto sencillo: comunicación audiovisual utilizando la red de datos y el protocolo IP. Pero este concepto sencillo engloba un complejo entramado de protocolos, estándares y desarrollos que han sido objeto de numerosos estudios teóricos y pruebas de laboratorio desde hace ya varios años. Sin embargo, se nos plantean varias cuestiones:

- ¿Es "madura" la tecnología?
- ¿Disponemos de datos acerca de implementaciones reales?
- ¿Qué problemas encontraremos cuando estemos en producción?
- ¿Hay solución para estos problemas?

El Centro de Tecnologías de la Información (CTI), tras realizar un estudio teórico de "Transmisión de Voz sobre Redes de Datos", se propuso analizar las necesidades y los problemas que aparecen al implantar una solución Voz IP y llevar a cabo un estudio sobre un entorno de producción.

Cuando nosotros hablamos de Voz sobre IP realmente hacemos referencia al término de Telefonía sobre IP:

- **Telefonía**: La Telefonía implica una interconexión global. Un usuario, al adquirir un teléfono GSM, no se plantea si podrá realizar o recibir llamadas desde otros operadores o desde la telefonía tradicional. Igualmente debe pasar con la Voz sobre IP.
- **IP:** Cuando hablamos de IP debemos especificar el entorno que abarca. En nuestro caso no hablamos únicamente de un entorno LAN o WAN corporativo, hacemos referencia al entorno de Internet.

A día de hoy, hace ya un año que tenemos implantados equipos de telefonía IP que coexisten de forma transparente con la telefonía tradicional de Centralita (PBX).

Con este artículo queremos compartir las experiencias y conclusiones adquiridas en el diseño, configuración y mantenimiento de nuestra red de Voz IP (Telefonía IP) que tenemos en producción.

2.- Nuestro escenario

2.1.- Ámbito del proyecto

El ámbito geográfico de nuestro proyecto se puede dividir en tres zonas:

- *Internet*: tenemos usuarios desplazados en Phoenix (Arizona), Londres, Ternopil (Ucrania) y Madrid (vía ADSL).
- *RedIRIS*: Madrid, Sevilla y la Universidad de Salamanca disponen de teléfonos IP tanto hardware como software.
- *LAN*: Nuestra LAN formada por varios edificios distribuidos en las Islas de Mallorca, Menorca e Ibiza.

El acceso de nuestra LAN a RedIRIS e Internet Global se realiza mediante un enlace ATM con el nodo central de RedIRIS situado en Madrid.

La LAN de la UIB interconecta a más de 3000 dispositivos Fast-Ethernet. Disponemos de un Campus central situado en Mallorca con doce edificios conectados con el CTI mediante tecnología Gigabit-Ethernet. El acceso a las Extensiones Universitarias de Menorca e Ibiza se realiza mediante enlaces ATM (para datos y voz interconectando las Centralitas). Otros edificios y centros Universitarios, 18 distribuidos por las Islas, acceden al CTI mediante líneas ATM, ADSL o RDSI.

La primera fase del proyecto consistió en la instalación de un radioenlace WLAN (802.11b) entre el CTI y un edificio cercano situado a unos 4 km. Hasta ahora la comunicación telefónica entre la Universidad y dicho edificio era mediante telefonía tradicional a través de un operador telefónico. La instalación de telefonía IP permitiría utilizar el enlace de datos en vez del operador telefónico.

2.2.- Equipos de Voz IP

La solución instalada en producción es H.323v2. En concreto la familia Siemens HiPath 5000 que se compone de elementos puramente IP: Gatekeeper, Gateway y terminales.

El Gatekeeper (HiPath 5500) es un software instalado sobre un servidor. Sus funcionalidades son básicamente las de control de admisión (RAS), traducción de alias a dirección IP, gestión de llamadas (registro y control de privilegios) y servicios de telefonía (buzón de voz, grupos de captura, desvío de llamadas y demás servicios tradicionales).

El Gateway (RG 2500) es un equipo dedicado que ofrece conectividad entre la red IP y la telefonía. En nuestro caso conecta la centralita a la zona IP mediante un puerto Fast-Ethernet y un Primario RDSI. El procesado digital de la señal se realiza mediante 3 DSPs que soportan cada uno 10 canales RDSI.

La centralita es una Ericsson MD110 integrada en el sistema Ibercom, tiene más de 1000 usuarios entre los que se encuentran extensiones GSM corporativas. Para la zona de Voz IP disponemos de líneas externas que son accesibles directamente y de una ruta para extensiones sin acceso directo. En este caso la recepción de llamadas desde la telefonía tradicional se realiza mediante la operadora de centralita.

Los terminales hardware utilizados pertenecen a la familia optiPoint de Siemens, en concreto tres modelos: 300 basic, 300 advance y 400 standard. Los tres modelos soportan H.323, DHCP, SNTP, FTP para actualizaciones y SNMP/HTTP para su gestión. Los modelos 300 disponen de un puerto Ethernet 10Mbps y el modelo 400 dispone de un mini-conmutador de dos puertos 10/100Mbps. Los tres modelos soportan el codec G.711 (64/80Kbps) pero sólo el 300 advance y el 400 soportan el G.723.1 (6.3/22.4Kbps).

Hemos utilizado Adaptadores de Terminal (AP1100) que permiten conectar terminales analógicos a la telefonía IP. Aparte del puerto Ethernet disponen de un puerto FXS para terminales como un FAX, un módem o un teléfono analógico.

Los usuarios que disponen de clientes software utilizan tanto versiones propietarias de Siemens como de libre distribución (NetMeeting y OpenH323). Hemos instalado software sobre distintas plataformas, como Linux, Windows y Windows CE en PDAs, cuyo acceso se realiza mediante Wireless-LAN.

Aparte de la familia de productos Siemens, hemos evaluado una solución de libre distribución como es openH323 y una maqueta de Cisco Systems. Esta maqueta de Cisco estaba formada por un Call Manager, un Gateway con módulos BRI RDSI, FXS y FXO, teléfonos IP hardware y un Switch Catalyst con InLine-Power para los teléfonos. Con esta maqueta, durante un mes, realizamos pruebas con los protocolos H.323 y MGCP en el Gateway y el protocolo SCCP (Skinny) en los teléfonos IP. Utilizamos Básicos RDSI de operador y líneas analógicas FXO de nuestra centralita. Estas pruebas nos han permitido evaluar otros productos y otros protocolos, pero no dejan de ser pruebas de laboratorio.

2.3.- Puesta en marcha

En nuestra LAN hemos instalado terminales hardware y software en el Campus Central, en las Extensiones Universitarias de Menorca e Ibiza y en el mencionado edificio que se encuentra conectado mediante el radioenlace.

En RedIRIS hemos instalado terminales hardware en Madrid, Sevilla y en la Universidad de Salamanca.

Los usuarios que acceden desde Internet utilizan clientes software, excepto algunos usuarios que han utilizado sus teléfonos hardware con líneas ADSL.

Problemas comunes a H.323, SIP y H.248/MGCP

La instalación y configuración del Gatekeeper, Gateway y Centralita se han realizado de tal forma que aseguramos una Interconexión Global, total trasparencia para el usuario y control de privilegios de los usuarios (llamadas locales, nacionales e internacionales).

Hemos llevado a cabo la sustitución de un teléfono tradicional por uno IP sin tener que dar indicaciones al usuario, ya que el plan de marcado es el mismo tanto en la zona de Centralita como en la Zona IP.

3.- Reflexiones y experiencias

Las reflexiones que a continuación desarrollaremos no se limitan a problemas exclusivos de H.323 o de un producto propietario. Los siguientes problemas son comunes para H.323, SIP o H.248/MGCP y para productos tanto propietarios como de libre distribución.

3.1.- Clientes: Hardware *vs.* Software

La gran ventaja de los terminales hardware es que son equipos dedicados. Facilitan a los usuarios utilizar la telefonía IP ya que no suponen ningún impacto, ofrecen gran calidad de audio y reservan todos sus recursos a la telefonía estando registrados permanentemente.

La calidad en el cliente software es limitada aunque superior a la GSM. Influyen factores como la tarjeta de sonido, el micrófono, el altavoz y el procesador. La utilización de handsets conectados a los PCs puede facilitar el uso habitual de los mismos como teléfonos y aumentar la calidad del audio. Otro inconveniente del cliente software es que se ejecuta sobre una máquina que puede tener recursos reservados a otras aplicaciones o simplemente no tener recursos suficientes para dar servicio. Un PC no asegura un registro continuo y además varias aplicaciones acceden concurrentemente a la red.

La gestión es un factor muy importante. Con los terminales hardware tenemos la facilidad de gestión remota vía SNMP o HTTP permitiéndonos realizar cualquier tipo de modificación, e incluso actualizaciones transparentes mediante FTP.

En los clientes software no disponemos de gestión remota, y además existe la complicación de utilizar distintos sistemas operativos y plataformas. Podemos optar por la solución de clientes Proxy, de forma que todos los usuarios accedan a un servidor para disponer de su cliente de voz.

El principal inconveniente de los terminales hardware es su precio, si lo comparamos con las licencias software o con la utilización de software de libre distribución. Aparte, el hecho de ser un equipo dedicado implica la necesidad de una nueva dirección IP y la ocupación de más puntos de red. Una solución para los puntos de red es disponer de terminales con dos puertos Ethernet, lo que facilita la instalación del teléfono entre un PC y su punto de acceso.

Los teléfonos hardware necesitan suministro eléctrico externo o en línea mediante el cable UTP. Deberemos analizar nuestras necesidades teniendo en cuenta si los terminales soportan el estándar (el optiPoint 400 de Siemens soporta 802.3af) y cuántos terminales vamos a alimentar con cada equipo.

La actualización de firmware es un aspecto crítico en los terminales hardware ya que estamos limitados a la voluntad del fabricante. No obstante, teóricamente podremos operar de forma básica si nuestro terminal soporta al menos el estándar.

La falta de servicios añadidos es otro problema para los equipos hardware. Al integrar el teléfono en el PC, es fácil introducir servicios innovadores como la videoconferencia y la mensajería instantánea.

3.2.- Direccionamiento y firewalls

Las direcciones IP y los puertos TCP/UDP se obtienen del cuerpo del mensaje

Los teléfonos IP se comunican mediante direcciones que se obtienen al traducir los alias de los terminales. En el establecimiento y señalización de llamadas, los protocolos H.323, SIP, MGCP o Megaco/H.248 utilizan la información del cuerpo de los mensajes para obtener las direcciones IP y los puertos TCP/UDP de los terminales que intervienen en las llamadas. Esto implica un problema si en nuestra corporación utilizamos NAT y direccionamiento privado y además deseamos conectividad global.

La primera instalación de Voz IP se realizó utilizando direccionamiento privado. Nos supuso un problema el acceso desde el exterior a nuestros usuarios y Gatekeeper.

La primera solución fue plantearnos la utilización de VPNs. De esta forma el usuario desplazado podría acceder a la zona de Voz IP. Esta opción sólo era válida para usuarios con clientes software o para la interconexión de dos redes remotas. No es una solución inmediata porque no es trivial al requerir un estudio de seguridad detallado. A pesar de ello no descartamos esta solución para implantarla a largo plazo.

Otra solución era introducir un Proxy H.323. Es fácil describir la función de un Proxy H.323 pero no es de sencilla implementación. Conocemos soluciones que integran Gatekeeper y Proxy pero en nuestro caso teníamos que operar con el Gatekeeper ya existente. Debemos pensar que al introducir un Proxy agregamos un retardo considerable y además ofrecemos servicio a un número limitado de terminales.

La tercera opción era utilizar NAT H.323. Esto implica que el Router/Firewall que realice NAT debe localizar la dirección IP privada y puertos TCP/UDP en el cuerpo del mensaje. Una vez localizados debe substituirlos por la dirección IP pública o puertos traducidos. Aumentamos así el retardo y ocupamos recursos de un equipo crítico como puede ser el Router/Firewall de una red en producción. Es una solución que descartamos a corto plazo porque, al igual que con las VPNs, es necesario estudiar detalladamente los riesgos que podemos correr.

La solución fue utilizar direcciones públicas para el Gatekeeper y el Gateway, mientras todavía estudiamos las opciones anteriores. De esta forma permitimos el registro desde el exterior y permitimos el acceso desde Internet a cualquier teléfono de Centralita. Los terminales IP que tienen necesidad de comunicación con el exterior también utilizan direcciones IP públicas.

Al comunicarnos con usuarios externos a nuestra LAN aparecen nuevos problemas: los firewalls. Es común encontrar reglas que controlen la utilización de servicios como videoconferencia y telefonía IP por el volumen de tráfico que estos generan. Tuvimos entonces que realizar un estudio de los puertos utilizados y definir nuevas reglas en los firewalls.

Las reglas deben considerar tanto los puertos estándar como los dinámicos utilizados, por ejemplo, para el tráfico RTP/RTCP. Acotar los puertos TCP/UDP de un teléfono IP hardware resultó sencillo al ser un equipo dedicado, pero en los clientes software el rango de puertos es dinámico ya que hay múltiples aplicaciones sobre el mismo equipo utilizando recursos de red.

En el caso de un firewall "packet filtering" deberemos indicar todos los puertos que serán utilizados, ya que la función que realiza es la de simple filtrado de paquetes según reglas. En cambio, si disponemos de un firewall "stateful inspection" se puede simplificar o complicar el problema. Este tipo de firewall es capaz de analizar y mantener las conversaciones, pero también es capaz de identificar protocolos como H.323 o SIP. En este caso no sería necesario definir todos los puertos utilizados dinámicamente ya que el propio firewall los pueden obtener al analizar el cuerpo de los

GDS: Plan de numeración global H.323

mensajes de establecimiento y señalización de llamadas. ¿Qué problema podemos tener? Pues que no tenga bien implementado el protocolo o utilice una versión anterior a la de las conversaciones analizadas (por ejemplo H.323 vs. H.323v2 faststart). En este caso el firewall puede decidir que el tráfico es malicioso y descartarlo.

Cuando hablamos de realizar cambios en los equipos de red y en las políticas de seguridad, debemos tener en cuenta que las redes ajenas en las que queramos tener usuarios no estarán dispuestas a realizar determinadas modificaciones. En nuestro caso hemos contado con la buena colaboración en el entorno de RedIRIS.

3.3.- Calidad de servicio

En nuestro caso no hemos controlado la calidad de servicio ya que todavía no ha sido necesario. Estamos estudiando las modificaciones que vamos a introducir como previsión del aumento de clientes.

Las opciones que tenemos para introducir calidad de servicio son básicamente dos: marcado de tráfico y priorización por identificación.

Al hablar de marcado de tráfico nos referimos a la creación de una VLAN de telefonía IP (802.1Q) y la utilización del campo de prioridad del tag (802.1p). Otra opción de marcado es la de utilizar el campo ToS/DiffServ de la cabecera IP.

Si priorizamos por identificación del terminal lo haremos por dirección MAC, que es útil para priorizar en el radioenlace creando colas, o mediante la dirección IP, para los terminales en la WAN.

Por supuesto aparece un problema: aparte de consumir recursos en nuestros equipos de red, ¿qué hacemos con los clientes Software? Los PCs pertenecen ya a otra VLAN y además generan tráfico que no corresponde a comunicaciones de Voz IP.

4.- Próximos objetivos

Ya tenemos abiertas las próximas líneas de trabajo para el proyecto. Podemos destacar el aumento de seguridad en general, el control de calidad de servicio, la integración de aplicaciones educativas con la Telefonía IP, plantearnos en un futuro pasar de la coexistencia a la substitución total de telefonía tradicional por IP y la integración con el Global Dialing Scheme (GDS).

El GDS es el Plan de Numeración Global para la interconexión de zonas H.323. Define una jerarquía de Gatekeepers asignando prefijos. Los Gatekeepers Munidales disponen del prefijo 00 de los cuales cuelgan los Gatekeepers Nacionales, normalmente gestionados por la Red I+D Nacional. RedIRIS ya dispone del prefijo 34. De los Gatekeepers Nacionales cuelgan los Gatekeepers de las distintas Instituciones.

El GDS ha sido adoptado por varios países europeos y ViDeNet. ViDeNet es una malla de más de 80 zonas H.323 dispersas por todo el mundo con Gatekeepeers institucionales y públicos.

De esta forma cualquier usuario podría ser accesible desde Internet, utilizando un gatekeeper del GDS, mediante su número identificador que puede coincidir con su número telefónico normalizado (p.e. 00-34-971-17xxxx).

5.- Conclusiones

Es el momento de empezar a trabajar, gestionando el cambio sin ser arrastrado por él

Podemos concluir comentando que hemos conseguido una solución de Voz IP con Interconexión Global que coexiste con la telefonía tradicional. Es un sistema totalmente transparente y atractivo para los usuarios. Hemos reducido el gasto de operador telefónico ofreciendo los servicios tradicionales de voz e introduciendo además servicios innovadores. Al integrar la telefonía con los PCs y la red de datos disponemos de una plataforma para desarrollar cualquier idea y proyecto que se nos plantee.

Vemos que conocer el producto a instalar es tan importante como conocer el protocolo, ya que determinadas configuraciones estarán limitadas y condicionadas por las características del Gatekeeper, Gateway, Centralita y por supuesto nuestra red. Tantos equipos interoperando dificulta la localización de problemas y nos implican tener conocimientos de tecnologías como IP y RDSI.

Los productos de Voz IP están en constante cambio. Llegado el momento de realizar una actualización o aplicar algún parche, deberemos analizar las funcionalidades que ganaremos, los problemas que encontraremos y decidir si realmente es necesario.

La gestión de usuarios desplazados en redes ajenas es compleja. Introducir nuevos elementos o realizar modificaciones implica un riesgo difícil de asumir tanto en una red propia como en una red ajena en producción.

Estudiar el entorno en el que se quiera introducir la VoIP es de suma importancia. No es lo mismo interconectar dos centralitas analógicas que querer ofrecer un servicio de telefonía basado únicamente en Voz IP. Hay múltiples soluciones y debemos tener claro nuestro objetivo para cubrir nuestras necesidades.

Finalmente debemos pensar en lo más importante: los usuarios. Como primer objetivo minimizar el impacto y no aturdirlos con servicios innovadores. Primero ofrecer la telefonía básica y estimular el uso de esta tecnología. De nada sirve un proyecto de tal envergadura si al final los usuarios no utilizan el servicio.

Sabemos que la Voz IP es el futuro y es el momento de empezar a trabajar. Hay muchos problemas pero poco a poco los vamos superando.

"Notar enseguida los pequeños cambios ayuda a adaptarse a los cambios más grandes que están por llegar".
"Es mejor gestionar el cambio que ser arrastrado por él".
(Spencer Johnson, M.D.)

Agradecemos la colaboración de Siemens por sus equipos de Voz IP, a Enterasys Networks por sus equipos de red y a Telindus por su apoyo. Ha sido fundamental tanto la participación de RedIRIS Madrid y Sevilla, como la de la Universidad de Salamanca y de todo el equipo del Centre de Tecnologies de la Informació de la Universitat de les Illes Balears.

Antonio Pérez Sánchez
(toni.perez@uib.es)
Bartomeu Serra Cifre
(tomeu.serra@uib.es)
Antonio Sola Venteo
(toni.sola@uib.es)
Centre de Tecnologies de la Informació
Universitat de les Illes Balears