Sistema de Voz sobre IP en una Red de Infraestructura Mesh para Gestión de Emergencias

Autor: Diana Lorena Mayo Murillo

Director 1: Manuel Esteve Domingo

Fecha de comienzo: 02/2013

Lugar de trabajo: Departamento de Comunicaciones

Objetivos

- Documentación de sistemas de telefonía IP.
- Implementación y establecimiento de un sistema de comunicación de VoIP sobre una red Mesh de uso táctico (para emergencias).
- Verificar que parámetros de red son recomendables para que se haga efectiva la comunicación.
- Establecer una comunicación de voz sobre una red de infraestructura Mesh configurando una central telefónica.
- Establecer una comunicación desde los terminales con el puesto de mando y control a través de VoIP.
- Determinar los parámetros de calidad de servicios que ofrece VoIP en la red Mesh.

Metodología

- Análisis de los sistemas de telefonía IP basados en Linux y Asterisk.
- Identificación de las principales características, aplicaciones y ventajas de VoIP en la telefonía.
- Acotación del problema y definición de objetivos a cumplir
- Esquema procedimiento a realizar
- Análisis de resultados. Revisiones, correcciones y ajustes.
- Realización de pruebas iniciales.
- Medición más precisa del comportamiento de la red.
- Análisis de resultados
- Documentación.

Desarrollos teóricos realizados

Se ha investigado sobre las características tanto a niveles LAN como de WAN que deben tener los elementos relevantes que hacen parten de este sistema de comunicación de VoIP y cuál podría ser la más conveniente, ligera y operativa, que se pueda implementar en paralelo con cualquier sistema de mando y control existente. Se instruyó de cada uno de los manuales de las antenas de la red Mesh para un correcto funcionamiento. Por otro parte se buscaron y se compararon varios software para los componentes de la red los cuales deberían ser compatibles y así no causar ningún tipo de problemas en la comunicación. Además se realizó un estudio de los parámetros de calidad de servicio que se deberían de tener en cuenta y los mecanismos para medir la calidad de VoIP.

Desarrollo de prototipos y trabajo de laboratorio

Se instalaron diferentes servidores Asterisk y se examinaron nuevas alternativas, así se llegó a que la mejor opción para este sistema es una central PBX virtual (máquina virtual) basado en Elastix. Se realizó el montaje de la red Mesh, con las antenas (JR-BreadCrumb), se analiza el comportamiento y características de la red por medio del software del fabricante Rajant y se ingresan los paramentos necesarios para que haya conectividad. Se hizo las respectivas configuraciones para los clientes VoIP en el servidor y luego para los otros componentes de la red (Ordenadores, PDA, Móviles, Portátiles) teniendo en cuenta el sistema operativo de cada uno, se experimentaron diversas configuraciones, parámetros de red, software telefónico (softphone) con el fin de alcanzar conectividad entre todos. Luego para él análisis de calidad de servicio se evaluó la red con programas de capturas de datos (sniffer) y se instalaron programas para aumentar el tráfico en red y observar el su rendimiento.

Resultados

Al terminar la tesina se han logrado los objetivos propuestos desde el principio, se obtuvo una comunicación VoIP entre varios clientes que se encuentran localizados en una red Mesh, cumpliendo parámetros técnicos de calidad de servicio. Además gracias a las medidas tomadas de QoS se tiene un análisis que permite tener una idea más clara del comportamiento de la red.

Líneas futuras

- Integración del sistema de VoIP sobre red Mesh desarrollado y evaluado dentro del proyecto de investigación "Entrenamiento C4ISR multimedia para gestión de emergencias, basado en la interconexión del mundo real y mundos virtuales"

El aspecto clave del proyecto es la integración entre el mundo real y el mundo virtual; para el intercambio de información de los dos mundos se sigue el estándar ISO/IEC 23005 MPEG-V. El proyecto se integra a un sistema de mando control C4ISR en donde se va a gestionar y controlar los terminales y la comunicación de VoIP. La idea es que al momento de establecer una comunicación de voz sea transparente para el usuario, independientemente donde este el origen y el destino, ya sea en el mundo virtual o en el mundo real.

Publicaciones

De momento no hay publicación alguna

Abstract

In the present project was expressing every step that was made for the creation of a VoIP communication in Wireless Mesh network, describing installation and configuration of an Elastix PBX in a virtual machine, deploying a Mesh network, Elastix server configuration of each VoIP client with their respective characteristics. The main objective is to establish communication among all clients VoIP, therefore ensures connectivity among all terminals in and out of the Mesh network, changes were made to this network parameters, various tests of connectivity changes topology, among others. When communication is established, we conducted a study of the captured packets in different tests, considering parameters such as latency (delay), jitter and bandwidth, with this result is an analysis that is suitable for a good performance in the network.

Autor: Mayo Murillo, Diana Lorena email: diamamu@teleco.upv.es
Director: Esteve Domingo, Manuel email: mesteve@dcom.upv.es
Fecha de entrega: 15-07-13

INDICE

I. INTRODUCCION

Hoy día hay un gran interés en la aplicación de redes inalámbricas Mesh debido a que son redes que permiten una fácil conexión, requieren poco mantenimiento y tienen un despliegue a un bajo costo. El Departamento de Comunicaciones de ésta universidad ha utilizado esta tecnología en los que han implementado varios proyectos de Sistemas de Tiempo Real. Este proyecto se realiza como un Sistema de Emergencia en campo y también para estar operativo en paralelo con otro sistema de mando y control que lo requiera.

Se requiere un sistema de comunicación voz sobre IP el cual aproveche la red que ya se ha implementado en distintas ocasiones, pero al momento de implementar este sistema se realizará distintos cambios en la topología y en los parámetros red. Un sistema de VoIP debe ser gestionado y controlado por una central telefónica sin importar que este dentro o la fuera de la red en cuestión, pero se necesita obligatoriamente su supervisión. Esta central es un servidor Asterisk de código abierto basado en Linux. Asterisk es programa de software libre (bajo licencia GPL) que proporciona funcionalidades de una central telefónica (PBX), una central telefónica privada es un dispositivo que permite conectar sus terminales, logrando que todas las llamadas internas de una misma red o empresa sean conmutadas directamente sin necesidad de salir a la red pública de telefonía.

Desde hace varios años se están utilizando algunas distribuciones basadas en Asterisk, tienen las mismas características que Asterisk pero ya vienen configurados completamente. Se optó por un software aplicativo llamado Elastix que integra las mejores herramientas disponibles de una PBX en una interfaz simple y fácil de utilizar. Con esta distribución de Asterisk y sus características, se pueden llegar a cumplir los objetivos propuestos desde el principio de proyecto, como es el establecimiento de la comunicación de voz en una red IP.

En un sistema de VoIP los clientes desean tener una conversación aceptable en la que no se aprecie ningún tipo de interferencia, el tráfico de voz normalmente es afectado en cualquier red de datos, ocasionando degradación que son causadas por el jitter, perdidas de paquetes, entre otros. En otras palabras el usuario espera ver satisfecha sus expectativas de calidad de servicio, ésta calidad se refiere a la medida del rendimiento de la red desde el punto de vista técnico, y a la posibilidad de ser gestionada para cumplir con las prestaciones necesarias [2].

Por ende después de haber alcanzado el principal objetivo se realizan distintas pruebas para tener una idea del comportamiento del tráfico de voz en la red. En estas pruebas se observan y se miden los parámetros de calidad de servicio para plantear soluciones y mejorar el rendimiento. Se toman medidas y se realiza cambios en la configuración del PBX.

Por último se realizan pruebas finales, ya que la calidad de servicio no solo depende solo del tráfico que se esté transmitiendo, también depende de otros factores como el nivel de señal en red, la distancia entre los AP, interferencias, numero de saltos, entre otros factores que se explicaran a medida en que avance el documento[7].

II. ESTADO DEL ARTE

II.1 SISTEMAS DE INFORMACION PARA MANDO Y CONTROL

El Departamento de Defensa de los Estados Unidos (DoD) lo define como "El ejercicio de la autoridad y de la dirección del comandante apropiado sobre las fuerzas que tiene asignadas para el cumplimiento de una misión" En general un sistema de información de mando y control es un procedimiento en el que se monitorizar, se controlar y se gestiona un sistema, para tener una visión amplia y acertada de lo que está sucediendo en capo, y con esto poder llegar a cumplir los objetivos propuestos.

En cuanto al mando y control las funciones son ejecutadas por una composición de personal, equipamiento, comunicaciones, instalaciones y procedimientos empleados por un comandante en la planificación, dirección, coordinación y control de fuerzas y recursos para la consecución de una misión. Así, el mando y control se refiere tanto a los procesos como a los sistemas que permiten llevar a cabo una misión [1]. En la siguiente figura (Fig.1) se podrá ver un esquema propuesto de mando y control.

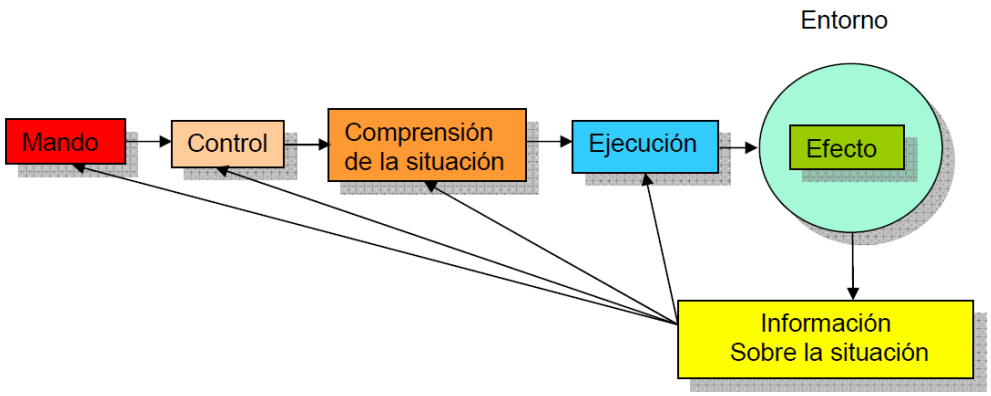


Fig. 1 Modelo de un sistema de mando y control

- **Mando:** definición de la situación inicial y de posibles líneas de evolución futura, intenciones primarias, asignación de responsabilidades, restricciones a la acción (ROEs), asignación de recursos (materiales, personales, información).
- **Control:** seguimiento de la evolución de los planes actuales o futuros, ajustes para mantener el sistema dentro de los márgenes definidos por la función de mando, interpretación de las intenciones de mando.
- **Comprensión de la situación:** percepción compartida de la situación, proyección de la situación al futuro inmediato, toma de decisiones, traducción de las intenciones de mando en objetivos y efectos.
- **Ejecución:** conjunto de acciones e instantes de tiempo en que se llevan a cabo, como resultado de una o más intenciones de mando, pudiendo implicar o no colaboración entre los actores.
- **Efectos:** modificación del entorno físico o cognitivo, como resultado de la ejecución de la intención de mando.
- **Información sobre la situación:** monitorización del entorno físico o cognitivo, y de los efectos de la ejecución.

II.1.2 CALIDAD DEL MANDO Y CONTROL

La calidad del mando y control está determinada por la interrelación de las calidades de las etapas asociadas. Así la calidad del mismo viene determinada por la calidad del mando, la calidad del control, la calidad de la comprensión de la situación (SA) y de la calidad de la ejecución. En la Fig. 2 se observa que el elemento del que dependen todas ellas es el de la calidad de la información para la consecución del objetivo final de todo sistema C2, la efectividad en el desempeño de una misión.

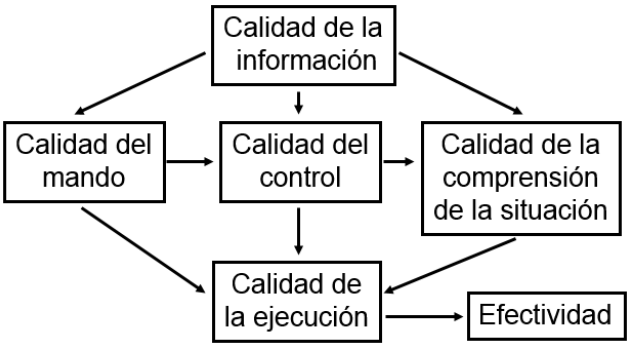


Fig. 2 Calidad del mando y control

La calidad de la información se puede descomponer en sus partes constituyentes: calidad ISR (Intelligence, Surveillance and Reconaissance), calidad en el transporte y calidad en los servicios de información. En el primer caso factores como la calidad de los sensores, los rangos de cobertura de los mismos y las tasas de actualización serán determinantes. En el caso de la calidad del transporte, la calidad de servicio, la conectividad y la interoperabilidad serán básicos. Respecto a la calidad en los servicios de información, la posibilidad de descubrimiento de servicios, la colaboración, la seguridad y la visualización serán los elementos clave [1].

Un concepto fundamental en el que se basa la teoría de los sistemas de mando y control es el de "percepción de la situación" "situational awareness"**.** En un sistema de mando y control, es muy importante conseguir mejorar el situational awareness de las personas a cargo para que puedan dar órdenes y tomar decisiones válidas y oportunas.

Los sistemas C4ISR (Command Control, Computers and Communications Information Surveillance and Reconaissance) engloban un amplio número de arquitecturas y sistemas informáticos y de comunicaciones. Su principal finalidad, tanto en aplicaciones civiles como militares, es la obtener información sobre el estado del teatro de operaciones para entregársela, convenientemente formateada, a las personas al mando de una operación de forma que se construyan una adecuada visión del mismo que les permita tomar las decisiones correctas. Por otra parte, deben servir de plataforma de comunicaciones para transmitir dichas órdenes y cualquier otra información que se estime oportuna [1].

Hoy día las redes de comunicaciones y las tecnologías avanzan, al mismo tiempo lo hacen los sistemas de mando y control en los que se necesita que estos sistemas ofrezcan nuevas soluciones y técnicas adaptativas para poder acoplarse a éste nivel tecnológico.

Los sistemas de mando y control se han implementado sobre varias tecnologías inalámbricas para gestión de emergencias, estas tecnologías dependen de las características del sistema (topología, trafico, ancho de banda, entre otros) y su jerarquía de red (red personal, red combate, red táctica, etc.) así mismo se elige cual tecnología es la más apropiada. Tecnologías como WLAN (802.11), Bluetooth, redes Mesh, WiMAXmóvil (IEEE 802.16e), ZigBee (802.14) [ZIG], comunicaciones satelitales, Ultra Wide Band (UWB) [ISO26907] [1]. La integración de todas estas tecnologías en un sistema C4ISR, es completamente transparente para el usuario y fácilmente conmutable.

Estos sistemas de mando y control tienen la peculiaridad de ser prácticos y flexibles en el contexto que pueden ser complementados con otras tecnologías y servicios logrando ofrecer más prestaciones, cubriendo así una amplia gama de necesidades. Sin olvidar, que hay que tener en cuenta el ancho de banda que se dispone, para desplegar nuevos servicios, ya que se tendría que permitir un flujo de datos mínimo o replantear la arquitectura de red y ampliar su cobertura, para no interferir en el funcionamiento de las otras unidades ya establecidas .

II.2 RED INALAMBRICA MESH (WMN)

La palabra Mesh viene del inglés, que en castellano es malla. Se les denomina Mesh porque los nodos que pertenecen la red forman una malla que permite la comunicación entre todos los elementos de la red. Estas redes son una combinación de dos topologías inalámbricas, por ello se dice que son una variante del WiFi tradicional (topología infraestructura) y una extensión de las redes Ad-Hoc (topología peer-to-peer). Los nodos Mesh se encargan del establecimiento y mantenimiento de la conexión de la red automáticamente, es decir, se auto organiza y se auto configuran dinámicamente creando una red ad hoc.

Las Redes Inalámbricas Mesh se han convertido en un avance en la tecnología inalámbrica para numerosas aplicaciones como redes domésticas de banda ancha, redes de una comunidad de vecinos, redes empresariales, redes públicas o redes en lugares donde es muy difícil y costosa la implantación de una red cableada. Cuantos más nodos haya instalados en la red, mejor va ser la conectividad y el servicio que podrán disfrutar todos los usuarios [3]. Gracias a sus características, esta tecnología se ha establecido en distintas compañías como: en varias universidades, proyectos comunitarios, empresas, laboratorios de investigación, entre otros.

En una red inalámbrica mallada hay dos tipos de nodos:

Enrutadores Mesh: Los enrutadores Mesh son equipos que cumplen con el trabajo de un Access Point (AP) convencional, formando una malla de AP fijos la cual se llama Red de Infraestructura. Estos equipos pueden trabajar con varias tecnologías de transmisión, por ejemplo con la IEEE 802.11. Estos tienen doble función el de proporcionar acceso a la red a los clientes y el de hacer una comunicación multi-hop entre ellos para el correcto direccionamiento y entrega de datos.

Clientes Mesh: Los clientes Mesh son dispositivos móviles que tienen la capacidad de conectarse inalámbricamente a una red u otro dispositivo como por ejemplo laptops, celulares, PDA, palms, entre otros.

Son los terminales, los cuales se les va a poner a disposición todos los servicios que tiene la red Mesh. Además, estos equipos pueden formar una red Ad-Hoc entre ellos, creando una red hibrida con los Mesh routers. En la figura 3 puede verse la topología de una red Mesh.

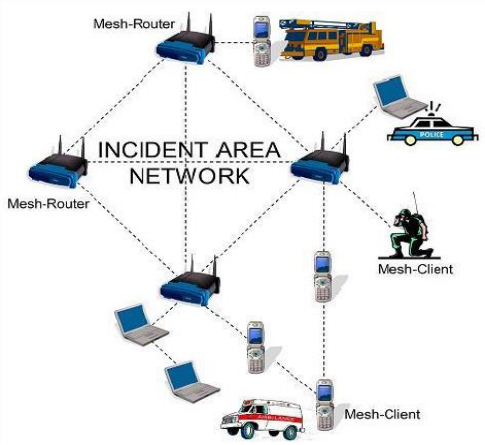


Fig. 3 Esquema de una Red Inalámbrica Mesh

II.2.1 CARACTERISTICAS

Las redes Mesh presentan las siguientes características:

- **Redundancia:** Los nodos que están conectados a la red entre sí, se conectan por varios caminos, esto hace que la red tenga otras rutas redundantes para si un nodo no funcione.
- **Fácil despliegue:** Al ser auto configurable permite dar soluciones de conectividad en cuestiones de emergencias (temblores, inundaciones, etc).
- Son **auto-regenerables, auto-configurables,** permiten la auto-reparación de rutas, por trabajar con protocolos de última generación Mesh, permiten descubrir nuevos nodos admitiéndolos en la comunidad ya existente y regenerando nuevas tablas de encaminamiento.
- **Son robustas**, por el tipo de enrutamiento que se aplica se obtiene una gran estabilidad en cuanto a condiciones variables o en alguna falla de un nodo en particular.
- **Ahorran energía,** para energizar cada nodo de la red mallada no solo se puede usar energía eléctrica sino también energía solar, eólica, hidráulica, celdas de combustible entre otras.
- Su topología permite que sean **útiles en entornos urbanos y rurales,** en los Estados Unidos y en parte de Europa las WMN has sido propuestas para soluciones en entornos urbanos y municipales. Sin embargo, estas redes también son una buena solución para problemas de conectividad en entornos rurales o lejanos.
- **Mayor capacidad a bajo coste**, hay estudios que han demostrado que la capacidad de una red inalámbrica puede ser mejorada mediante la utilización de repetidores, existiendo un compromiso entre distancia e interferencia entre nodos.[3]

II.2.2 ESTANDARES

Los principales grupos de estandarización definen estándares de WMN, los cuales se encargan de proporcionar y facilitar la comunicación y la interoperabilidad entre dispositivos de diferentes fabricantes y de las redes de comunicación emergentes y las ya existentes. La familia del IEEE 802.11, son normas para comunicaciones one-hop (de un solo salto), por lo que no son apropiadas para ser aplicadas en redes de múltiples saltos, múltiples canales de transmisión y de múltiples radios. Para las redes Mesh se siguen los siguientes estándares.

II.2.2.1. IEEE 802.11s

Los equipos que trabajan con el estándar 802.11s, que tienen funcionalidades para trabajar en una red mallada, se denominan Mesh Point (MP). El estándar involucra otros equipos como los Mesh Access Point (MAP) que son puntos de accesos y los Mesh Portal Point (MPP) interconectan las redes Mesh [3].

El estándar 802.11s tiene dos procesos importantes y necesarios para el funcionamiento de una red mallada: primero es la asociación de un equipo terminal con un MAP y la segunda es la asociación de un MAP con un nodo vecino.

La función principal de este estándar es el de aprender de la topología de la red mallada, del ruteo y forwarding, descubrir topologías y realizar las asociaciones entre nodos, seguridad de la red, configuración y monitoreo. Cabe mencionar que existen otros estándares pertenecientes al grupo IEEE 802.11 como el 802.11a, 802.11b, 802.11g y 802.11n, que aplicándolos de una manera idónea pueden también trabajar en una red mallada, dando los mismos servicios y aplicaciones como los estándares exclusivos para WMN[3].

II.2.2.2 ESTANDAR IEEE 802.16 MODO MESH

El estándar IEEE 802.16-2004 soporta la creación de redes Mesh. La simulación de sistemas de comunicación permite su optimización, sobre todo para la mejora de los parámetros de desempeño [4].

Para estas redes se necesitan 2 algoritmos de planificación: *Planificación distribuida*: Todas las estaciones (BS y SS) coordinan sus transmisiones en su vecindario extendido (hasta dos saltos). Todas las estaciones en la red emplean el mismo canal para transmitir la información de planificación en un formato específico. Cuando existe una Mesh BS ésta actúa como responsable de enviar el Network Descriptor con la información necesaria de la red. Los nodos deben transmitir el MSH-DSCH (mensaje que se transmite para informar a los nodos vencinos del scheduler de la estación de transmisión) de la misma forma como coordinan los mensajes MSH-NCFG (provee un nivel básico de comunicación entre todos los nodos, ya sean BS o SS (subscriber) transmiten este mensaje en la red Mesh). Los nodos establecen los requerimientos de BW de una forma directa entre dos nodos sin la participación de una BS. Las Peticiones/Concesiones se transmiten a los vecinos para que todos conozcan el algoritmo de planificación y eviten colisiones. *Planificación Centralizada*: Las conexiones y la topología de red son las mismas que en distribuido, pero el scheduler de transmisión es definido por una estación BS. La BS determina la asignación de recursos que depende de las solicitudes de las SS. El scheduling centralizado asegura comunicaciones libres de colisiones y trabaja de la siguiente forma: el control lo realiza la

Mesh BS por medio de mensajes del tipo MSH-CSCH (lo envía una Mesh BS y también se emplea para para realizar peticiones de ancho de banda al Mesh BS) y MSH-CSCF (es empleado para realizar la configuración necesaria de los nodos Mesh). Los primeros se encargan de la coordinación de las estaciones y el segundo de la configuración.

Los nodos se agregan a un árbol de enrutamiento, en el cual la Mesh BS corresponde a la raíz y se organizan por medio de su distancia en saltos hasta la base. En las peticiones los nodos más lejanos transmiten primero en orden de aparición en este árbol. En las concesiones, se transmite en orden creciente de distancia al Mesh BS, pero dentro de cada nivel en el orden de aparición en el árbol de enrutamiento [4].

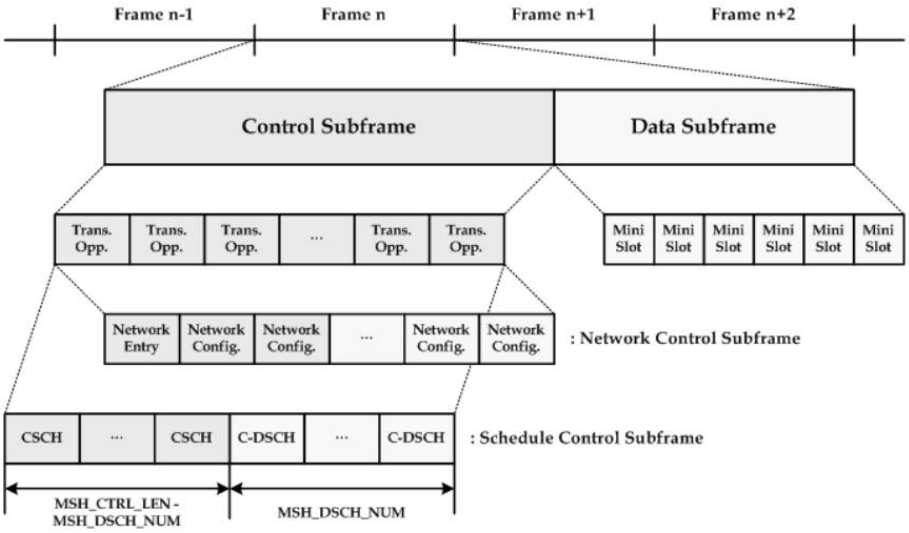


Fig.4 Estructura de la trama IEEE 802.16 modo Mesh

II.2.5 ARQUITECTURA DE RED

Existen varias arquitecturas de red:

- ***Arquitectura plana***: En esta arquitectura todos los nodos están al mismo nivel. Los nodos de los clientes inalámbricos coordinan entre sí para proporcionar enrutamiento, configuración de la red, provisión de servicios, y algún otro tipo de solicitud. Esta arquitectura es la más parecida a una red Ad Hoc y es el caso más simple entre los tres tipos de arquitecturas red Mesh Inalámbricas (WMNs). La principal ventaja de esta arquitectura es su sencillez, y sus desventajas incluyen la falta de escalabilidad y limitaciones de recursos. Los principales problemas a resolver en este diseño son: esquema de direccionamiento, enrutamiento, servicios. En una red plana, el direccionamiento es uno de los problemas que llegan a impedir la estabilidad.

- ***Arquitectura jerárquica:*** En una arquitectura jerárquica, la red tiene múltiples niveles jerárquicos en la que los nodos del cliente forma el nivel más bajo dentro de la arquitectura. Estos nodos del cliente pueden comunicarse con la red que está formada por routers. En la mayoría de los casos, los nodos WMNs se dedican a forman un backbone de una red troncal WMNs. Esto significa que los nodos que forman el backbone no pueden originar o terminar el tráfico de datos como los nodos del cliente. La responsabilidad de auto-organizar

y mantener la red troncal está a cargo de los routers WMNs, algunos de los cuales pueden tener interfaz externa a Internet y a estos nodos se les llama nodos pasarela.

- ***Arquitectura híbrida:*** Este es un caso especial de redes jerárquicas WMNs, donde la red WMNs utiliza otras redes inalámbricas para la comunicación. Por ejemplo, el uso de otras infraestructuras tales como las redes celulares, redes WiMAX, o las redes satelitales. Estas redes híbridas WMNs pueden utilizar múltiples tecnologías tanto para la implementación del backbone como para los terminales. Dado que el crecimiento de WMNs depende en gran medida de cómo trabaja con otras soluciones de red inalámbrica, esta arquitectura se convierte en muy importante en el desarrollo de redes WMNs.

II.3 VOZ SOBRE IP

VoIP es el acrónimo de "Voice Over Internet Protocol", es un estándar de la ITU (Internacional Telecommunications Union), creado en 1996 que tal y como el término dice, hace referencia a la emisión de voz en paquetes IP sobre redes de datos como puede ser Internet. El concepto de Telefonía IP es un sinónimo de VoIP, es la implementación y utilización de VoIP [5] [6].

La telefonía IP conjuga dos partes importantes en la transmisión tanto de voz como de datos. Se trata de transportar la voz que después se convierte en datos entre 2 puntos remotos. Esto posibilitaría utilizar las redes de datos para efectuar las llamadas telefónicas y desarrollar una red convergente que se encargue de cursar todo tipo de información o de tráfico.

VoIP es una tecnología y no un servicio que permite encapsular la voz en paquetes para poder ser transportados sobre redes de datos sin necesidad de disponer de la red pública (PSTN) la cual se utilizó antes para la transmisión de señales de voz. A diferencia de la Red Telefónica Publica Conmutada que utiliza conmutación de circuitos, la telefonía IP envía múltiples conversaciones a través del mismo canal (circuito virtual) codificadas en paquetes y en flujos independientes. Cuando se produce un silencio en una conversación, los paquetes de datos de otras conversaciones pueden ser transmitidos por la red, lo que implica un uso más eficiente de la misma.

Las alternativas tecnológicas de VoIP se pueden dividir en dos grandes grupos: tecnologías cerradas-propietarias por ejemplo como el conocido Skype o el Cisco Skinny (SCCP), entre otros y sistemas abiertos nos encontramos con los estándares abiertos basados en SIP, H.323 o IAX [6].

II.3.2 COMPONENETES DE UNA RED VOIP

Dentro de la estructura básica de una red VoIP hay que diferenciar tres elementos fundamentales:

- Terminales: Son los dispositivos que utilizarán los usuarios para comunicarse. Implementados tanto en hardware como en software realizan las funciones de los teléfonos tradicionales [5].

- Gateways: De forma transparente se encargan de conectar las redes VoIP con las redes de telefonía tradicional. Podemos considerar al Gateway como una caja que por un lado tiene un interface LAN y por el otro dispone de uno o varias interfaces como POST, T1/E1, ISDN, E&M trunks [6].
- Servidor: Proporciona el manejo y las funciones administrativas para soportar el enrutamiento de llamadas a través de la red IP.
- Red IP: Suministra la conectividad entre los terminales, esta puede ser una red IP privada, una Intranet o el propio Internet.

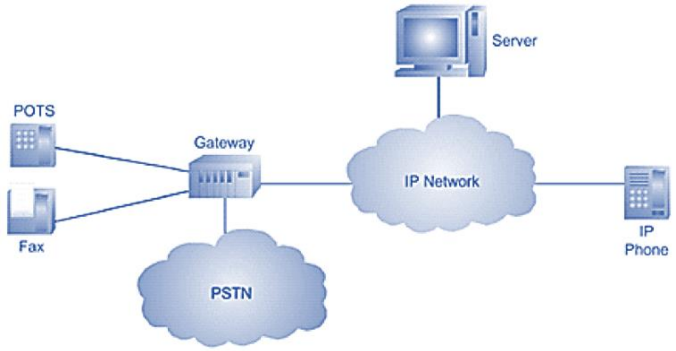


Fig.5 Componentes de una red VoIP

II.3.3 *ARQUITECTURA DE LA TECNOLOGÍA VOIP*

VoIP tiene la ventaja de crear redes empleando dos tipos de arquitecturas la centralizada y la distribuida, permitiendo a las compañías construir redes caracterizadas por una administración simplificada e innovación de Endpoints (teléfonos) dependiendo del protocolo usado.

II.3.3.1 CENTRALIZADA

Esta arquitectura ha estado asociada con los protocolos MGCP (IETF 2705) y MEGACO (IETF RFC 2885 y recomendación ITU H.248), los cuales fueron diseñados para un dispositivo centralizado llamado controlador Media Gateway, que maneja la lógica de conmutación y control de llamadas. VoIP apoya este modelo ya que concentra la administración y control de llamadas.

II.3.3.2 DISTRIBUIDA

Esta arquitectura está asociada con los protocolos H.323 y SIP, los cuales permiten que la inteligencia de la red sea distribuida entre dispositivos de control de llamadas y Endpoints. La inteligencia en esta instancia se refiere a establecer la comunicación, características de llamadas, enrutamiento, provisión, facturación entre otros. Los Endpoints pueden ser Gateways VoIP, teléfonos IP, servidores media. Los dispositivos de control de llamadas son llamados Gatekeepers en una red H.323, y servidores Proxy o Redirect en una red SIP. La tecnología VoIP apoya este modelo por su flexibilidad.

II.3.4 *PAQUETIZACION DE LA VOZ Y CUESTIONES DE ANCHO DE BANDA*

Los paquetes que llevan la voz se transportan sobre la siguiente estructura: Carga útil o “Payload” (muestra de voz), RTP, UDP, IP, Nivel Físico (ATM, Ethernet u otro). Supongamos que queremos enviar por la red IP una

comunicación, con codificación G.711 se genera una muestra cada 125 microsegundos, gracias al periodo de paquetización o "sampling rate" para generar un paquete de voz IP, se espera hasta acumular una cantidad importante, por ejemplo un periodo típico de paquetización es de 20 milisegundos, entonces:

1 muestra vocal ------- 125 µs
X muestras vocales ------- 20 ms X = 20 / 0,125 = 160 muestras vocales

Con esto el "paquete" de voz se compone de:

Carga útil = 160 muestras de voz (160 bytes)
Encabezado del protocolo RTP = 12 bytes
Encabezado del protocolo UDP = 8 bytes
Encabezado del protocolo IP = 20 bytes
Encabezado de Ethernet II + secuencia FCS = 18 bytes
Tamaño total del paquete = 218 bytes

Luego la tasa de paquete es 50 paquetes/s de 218 bytes, traducido esto en ancho de banda: 50 paquetes x 218 bytes x 8 = **87.200 bits/s.** Este resultado es debido al "overhead" introducido por los encabezados de los protocolos de transporte, el ancho de banda requerido a la salida es mayor que el de entrada [8]. Hay que señalar que es una tasa alta para muchos sistemas de comunicaciones que se utilizan hoy, como por ejemplo los que se basan en radio de HF y VHF.

En las funciones básicas al realizar una llamada telefónica por IP está digitalizar nuestra voz en señales PCM (Pulse Code Modulation) por medio de un códec como en el ejercicio anterior G.711, que funciona como codificador/decodificador, luego se comprime y se envía en paquetes de datos IP por la red. Cuando alcanzan su destino, son ensamblados de nuevo, descomprimidos y convertidos en la señal de voz original.

II.3.5 CALIDAD DE SERVICIO

La calidad de servicio es el rendimiento de extremo a extremo de los servicios de transmisión tal y como los pueda percibir el usuario. Los factores que afectan a la calidad se encuentran son:

- La calidad de la voz extremo a extremo: Las pérdidas de paquetes en la red. No todos los paquetes llegan al destino y se ve afectada la interactividad en la conversación, y por tanto a la QoS [6].
- Requerimientos de ancho de banda: la velocidad de transmisión de la infraestructura de red y su topología física, requieren manejo de las capacidades de la red que permita el control del tráfico, protocolos de tiempo real y un adecuado ancho de banda durante el tiempo que tome la realización de la llamada
- Latencia o retardo: Saber cuáles pueden ser las posibles causas que lo produce ya que sabiendo cuales estos factores, se pueden tomar medidas para mantener la red en buen estado.
- Jitter: Se debe a la variación del retardo en toda la conexión y a las colas de buffer cuando llega al destino.

- Eco**:** El eco se define como una reflexión retardada de la señal acústica original, es especialmente molesto cuanto mayor es el retardo éste se convierte en un problema en VoIP.

Las redes IP son redes del tipo best-effort y por tanto no ofrecen garantía de calidad de servicio, pero las aplicaciones de telefonía IP si necesitan garantizar calidad de servicio en términos de demora, jitter y pérdida de paquetes. En otras palabras no hay garantía absoluta en el tiempo que tardan en llegar los paquetes al otro extremo de la comunicación así se utilicen técnicas de priorización. Estos problemas de calidad de servicio y dependencia de la red de datos suponen uno de los principales problemas para la difusión total de la telefonía por IP.

II.3.6 VENTAJAS Y DESVENTAJAS

II.3.6.1 VENTAJAS

- Esta tecnología tiene como principal objetivo la disminución en el pago de la telefonía, es evidente que para un proveedor de servicio de telefonía y datos, obtiene beneficios ya que con una sola línea puede ofrecer más servicios y ahorro de gastos tanto de infraestructura como de mantenimiento, pues una llamada telefónica requiere una gran red de centralitas conectadas entre sí con cableado, fibra óptica, satélites de telecomunicación o cualquier otro medio, que equivale a una enorme inversión para crear y mantener estas infraestructuras [6].
- Las llamadas entre usuarios VoIP entre cualquier operador son gratis en comparación una llamada de VoIP a PSTN que normalmente cuestan al usuario VoIP.
- El desarrollo de diferentes tipos de códec para VoIP (alaw, ulaw, GSM, G729, G.723, etc.) ha permitido que la voz se codifique en paquetes de datos cada vez de menor tamaño. Esto trae como consecuencia que las comunicaciones de voz sobre IP requieran anchos de bandas reducidos, junto al avance de distintas tecnologías de banda ancha este tipo de comunicaciones se hacen muy populares.
- Con VoIP se pueden realizar llamadas desde cualquier lado que exista conectividad a internet. Dado que los teléfonos IP transmiten su información a través de internet estos pueden ser administrados por su proveedor desde cualquier lugar donde exista una conexión.

II.3.6.2 DESVENTAJAS

- Carece de calidad de transmisión garantizada debido a que los datos viajan en paquetes, los cuales pueden verse afectados por problemas de alta latencia o perdidas de paquetes que ocasionan inestabilidad de las conexiones y que los paquetes tarden en llegar de un extremo a otro.
- Se precisa controlar el uso de la red mientras se utiliza VoIP, para mejorar su eficiencia.
- En los casos en que se utilice un softphone la calidad de la comunicación VOIP se puede ver afectada por el PC, cuando se realiza una llamada y luego se abre un programa que utiliza el 100% de la capacidad de nuestro CPU, la calidad de la comunicación VoIP se puede ver comprometida por el procesador de la PC
- La red IP no garantiza calidad de servicio, al menos en IPv4 [6].

II.3.7 SEGURIDAD

La tecnología de VoIP al igual que otras tecnologías populares se ha convertido en un blanco perfecto para las brechas de seguridad, los ataques y las vulnerabilidades del sistema. Los dispositivos de la red, los servidores, sus sistemas operativos, los protocolos con los que trabajan y prácticamente todo elemento que integre la infraestructura VoIP es susceptible de sufrir un ataque. Esta tecnología ha de apoyarse necesariamente en muchas otras capas y protocolos ya existentes de las redes de datos, por lo tanto la telefonía IP hereda ciertos problemas de las capas y protocolos ya existentes, siendo algunas de las amenazas más importantes de VoIP problemas clásicos de seguridad que afectan al mundo de las redes de datos. Algunas de estas amenazas son: Accesos desautorizados y fraudes, Ataques de denegación de servicio, Ataques a los dispositivos, Vulnerabilidades de la red subyacente, Enumeración y descubrimiento, Ataques a nivel de aplicación [5].

El hecho de que la voz esté en un medio compartido que comunica servicios y/o recursos, base del diseño del protocolo IP que no está diseñado para brindar seguridad por sí misma, resulta difícil brindar confidencialidad, integridad, autenticidad y disponibilidad.

El sistema de seguridad debe contemplar políticas de autenticación e integridad de la fuente de señalización, pues si algún intruso la manipula puede controlar el sistema telefónico e intervenir en la conversación de los usuarios, modificando o fabricando información "falsa" a un usuario o todos los usuarios, además de que manipula las funcionalidades operacionales-administrativas brindadas por el sistema de VoIP, presentándose la posibilidad de ataques informáticos al servicio de telefonía IP.

El cifrado es quizás una de las principales y más necesarias medidas que se deben adoptar en una infraestructura VoIP. El uso de TLS/SSL para establecer canales de comunicación seguros resolviendo la mayoría de problemas de eavesdroping, manipulación y reproducción de los mensajes que se intercambian. La comunicación de los datos puede ser segura incorporando algún tipo de cifrado. Los teléfonos VoIP pueden cifrar el audio con el protocolo SRTP. Secure RTP es una réplica del RTP pero ofrece confidencialidad, autenticación de mensajes y protección evitando los ataques de interceptación e inserción de audio entre otros. SRTP es ideal para proveer telefonía IP ya que utiliza una compresión de las cabeceras la cual no afecta prácticamente a las QoS [5].

Al utilizar esta tecnología con redes inalámbricas o WiFi que, por su naturaleza, son inseguras pues el medio compartido es el aire, en el cual se accede libremente y cualquiera con un sniffer puede escuchar dicho tráfico, reensamblarlo e interpretarlo; algunos son Kismet, Ethereal, Wireshark o el propio CAIN, por lo cual es más fácil tener injerencia en esta tecnología, de tal forma que el sistema de seguridad VoIP debe incluir políticas de configuración segura en los equipos inalámbricos, los cuales son independientes al propio sistema de VoIP.

Ayuda también separar la voz y los datos en diferentes redes lógicas formando VLAN (Virtual Local Area Network). De esta manera se segmenta la red y se escogen algunas subredes o direcciones IPs con reglas propias para voz y otras para datos, así de esta forma, no se escucha lo que pasa en la parte de voz, además de que se configuran reglas que impiden que alguien ajeno a la red de voz pueda colocar un sniffer, como lo es la

autenticación de MAC o portales de seguridad, donde si no se cuenta con un login y password no se puede acceder a la red, colocando al intruso en cuarentena.

En WiFi existen distintos métodos de cifrado, pero WPA2 Enterprise (Wired Equivalent Privacy-802.11i) es el más seguro, siendo el estándar de seguridad en WiFi que integra confidencialidad, integridad y autenticación del servicio, ya que sólo da acceso a la red inalámbrica si cuenta el usuario con su login y password, usando como algoritmo de cifrado AES 128, de esta manera se protegerá la información que corre por la red inalámbrica de manera rápida y efectiva.

II.3.8 SIP

SIP (Session Initiation Protocol) se encuentra definido en el RFC 3261, es un protocolo de señalización a nivel de aplicaciones para el establecimiento y gestión de sesiones con múltiples participantes. Define el proceso de llamadas telefónicas, video conferencias y otras conexiones multimedia sobre Internet. Es ampliamente soportado y no tiene dependencia en cuanto a fabricante. Es un modelo atractivo ya que es simple, escalable y cómodo para su uso en paquetización de la voz [6].

SIP puede establecer diferentes tipos de sesiones como conectar dos extremos de llamadas telefónicas ordinarias, de múltiples partes donde todos hablan/escuchan y la multidifusión, estas conexiones pueden ser audio, video o datos. Es importante saber que este protocolo solo maneja la iniciación, modificación y finalización de la sesión. El propósito de SIP es la comunicación entre dispositivos multimedia, y este se logra gracias a los diferentes estándares existentes que son compatibles con SIP. Para el transporte de datos se utiliza el protocolo RTP/RTCP, para negociar las capacidades de los participantes tales como direcciones IP, medio a utilizar, tipo de codificación, etc. se usa el SDP (Session Description Protocol), el cual permite describir el contenido multimedia de la sesión. No hace falta señalar que SIP es un protocolo que funciona tanto sobre UDP como TCP [7].

II.3.8.1 COMPONENTES

SIP realiza tareas que facilitan las comunicaciones multimedia entre clientes y servidor, estas tareas son ejecutadas por 2 elementos el Agente de Usuario (UA) y el Servidor de Redes (UAS). El Agente de Usuario se compone de:

- User Agent Client: Es la parte lógica que genera peticiones y recibes sus respectivas respuestas.
- User Agent Server: Es la entidad que crea las respuestas a las peticiones SIP.

Y el Agente de Red que se clasifica en 4 partes pero pueden estar ubicados en la misma máquina:

- Servidor Proxy SIP: Realiza las funciones intermediador entre le UAC y el UAS. Una vez le llega una petición de inicio de llamada de UAC decide a que servidor debería ser enviada y entonces retransmite la petición, que en algunos casos pude llegar a atravesar varios proxys SIP antes de llegar a su destino.
- Servidor de Redirección: Es un servidor que genera respuestas de redirección a las peticiones que recibe. Este servidor reencamina las peticiones hacia el próximo servidor.

- Servidor de Registro: es un servidor que acepta peticiones de registro de los usuarios y guarda la información de estas peticiones para suministrar un servicio de localización y traducción de direcciones en el dominio que controla.
- Servidor de Localización: Facilita información al Proxy o Redirect sobre la ubicación del destinatario de una llamada [5].

II.3.8.2 MENSAJES SIP

Los mensajes SIP se utilizan para la conexión y control de llamadas. Este protocolo emplea dos tipos de mensajes los de petición (método) y respuesta (código de estado), los mensajes son definidos de la siguiente manera:

- Invite: cuando el usuario cliente desea iniciar una sesión, crea una petición INVITE, la cual es establecida a un servidor, después que este acepte, envía una respuesta en forma de código, bien sea aceptado, rechazado entre otros.
- Re-invite: Permite enviar una nueva petición Invite dentro de una sesión establecida.
- TRYING (100)/RINGING (180): un 100 para indicar que se ha recibido el INVITE y un 180 al detectar timbre.
- 200 OK: Envía este mensaje al usuario que se ha llamado, para indicar que desea establecer sesión.
- ASK: Confirma el inicio de una sesión, indicando el fin del proceso de señalización.
- BYE: Se utiliza para finalizar una sesión entre los usuarios.
- CANCEL: Cuando hay una conexión pendiente se utiliza este método para finalizarla.
- REGISTER: Permite enviar una petición de registro a un servidor especial para tal fin, guardando información del usuario.
- OPTION: Este método permite a un usuario consultar a otro sobre sus capacidades [7].

***II.3.9** ASTERISK*

Asterisk es el más potente, flexible y extenso software de telecomunicaciones disponible para sistemas de VoIP. Está diseñada para conectar cualquier hardware telefónico o cualquier tipo de software de telefonía de manera transparente y consistente. Tradicionalmente, los productos telefónicos son diseñados para ejecutar una tarea específica en una red, sin embargo, las aplicaciones de telefonía comparten gran cantidad de tecnología. Asterisk toma ventaja de esta sinergia para crear un solo entorno de desarrollo que puede ser moldeado a cualquier necesidad que el usuario requiera. Asterisk, además de muchas otras cosas, puede ser usado en aplicaciones como VoIP Gateway (MGCP, SIP, IAX, H.323), Private Branch eXchange (PBX), servidor de voz de respuesta interactiva (IVR), servidor de conferencia, entre otras. Naturalmente esta increíble flexibilidad viene con un precio; Asterisk no es un sistema simple para configurar, pero es una solución práctica, accesible y equilibrada [6].

II.3.10 PBX

Se refiere al dispositivo que actúa como una ramificación de la red primaria pública de teléfonos, por lo que los usuarios de una PBX no están asociados con la central de telefonía pública (RTC), ya que es la misma PBX la que actúa como tal. Es la RTC quien enrute las llamadas a otro destino final mediante líneas troncales. En otras palabras la PBX se encarga de redirigir y gestionar las llamadas entrantes a uno o varios telefónicos de una empresa o red. También ofrece la posibilidad de crear servicios de valor añadido como transferencia de llamadas, pasarela de voz a correo o servicios basados en una respuesta de voz interactiva (IVR), etc.

La ventaja principal de una central telefónica es que la comunicación interna o intercomunicación es rápida y gratuita, además evita conectar todos los teléfonos de una oficina de manera separada a la RTC y requiere poco manteamiento, solo puede tener problemas de capacidad y crecimiento de una empresa [6].

Resumiendo una PBX es una computadora centralizada, en la que le usuario configura los parámetros de las llamadas entrantes y salientes según las necesidad de la red.

II.3.11 ELASTIX

Elastix es una distribución libre de servidor de comunicaciones unificadas que integra en un solo paquete VoIP PBX, fax, mensajería instantánea, correo electrónico, entre otros. Su objetivo de es el de incorporar en una única solución todos los medios y alternativas de comunicación existentes en el ámbito empresarial.

El proyecto Elastix se inició como una interfaz para el reporte de llamadas de Asterisk y fue liberado en Marzo del 2006. Posteriormente el proyecto evolucionó hasta convertirse en una distribución basada en Asterisk [9].

II.3.11.1 Características

Cada día existen nuevas formas de comunicarnos, y la adición de características y funcionalidades debe ser constante. Elastix es capaz de crear un ambiente eficiente en una organización con la suma de múltiples características, y permite integrar otras locaciones para centralizar las comunicaciones de su empresa y llevarlas a niveles globales [9]. Algunas de las características básicas de Elastix incluyen:

- Correo de Voz
- Fax-a-email
- Soporte para softphones
- Interfase de configuración Web
- Sala de conferencias virtuales
- Grabación de llamadas
- Least Cost Routing
- Roaming de extensiones
- Interconexión entre PBXs
- Identificación del llamante

- CRM
- Reportación avanzada
- Entre otras.

II.3.12 SOFTPHONES

Es un software que emula un teléfono en un computador y permite hacer llamadas de VoIP, es decir convierte un PC en un teléfono IP para hacer llamadas a otros softphone de modo gratis en general, o a otros teléfonos convencionales usando un operador de telefonía IP. Generalmente se comunican a través de un entorno de centro de llamadas, para comunicarse desde un directorio de clientes o para recibir llamadas.

Poseen una interfaz intuitiva de fácil comprensión, y también tienen un teclado virtual parecido al de los teléfonos convencionales. Es practico y fácil de utilizar, se puede ejecutar y al mismo tiempo continuar realizando otras tareas en el ordenador. Eso es posible gracias a aplicaciones del tipo click-to-dial o llamada en espera IP.

III. TOPOLOGIA Y HERRAMIENTAS DE HARDWARE Y SOFTWARE DEL SISTEMA

III.1 TOPOLOGÍA

La topología que se diseñó desde el comienzo del proyecto y por la cual se empezó a plantear distintas soluciones se puede ver en la figura 6.

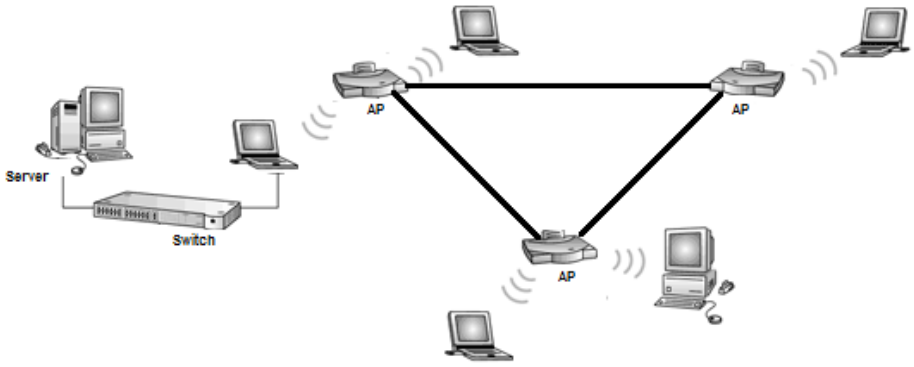


Fig.6 Topología propuesta

Esta topología probada y analizada en el laboratorio, consta de una red LAN que se conecta a la red Inalámbrica Mesh. En la red LAN se encuentra ubicado el PBX o Servidor Elastix el cual administra las llamadas y los clientes VoIP que se encuentran en la red Mesh o fuera de ella, luego este servidor se conecta a un ordenador Windows XP que realiza la tarea de router hacia la red Mesh. La red de infraestructura Mesh que tiene diferentes parámetros a la red LAN, tiene 3 puntos de accesos conectados entre sí, los cuales deben tener una adecuada configuración para obtener buenas prestaciones. Estos AP interconectan todos terminales o los clientes VoIP para que se puedan transmitir el tráfico de voz entre sí. Cada uno de los terminales tiene diferentes características, esto trae como consecuencia que el software de aplicación y programas a implementar en cada

uno, depende de sus propiedades (Sistema operativo, RAM, Procesador, etc.) para que puedan funcionar correctamente.

III.2 HARDWARE

Se han utilizado 6 terminales (4 portátiles y 2 móviles) y 3 puntos de accesos. A continuación veremos las características de cada terminal y AP.

III.2.1 ORDENADORES

Servidor Elastix: Está instalada la versión 2.4, en una máquina virtual de VirtualBox versión 4.1.8, basado en la Versión de Asterisk y distribución de Linux (i386) Versión 2.6.18. Tiene 2 GB de Memoria RAM, 40 GB de disco duro. Todo esto instalado en un ordenador Windows 8, procesador Intel Core i5-3337U de 1.8GHz, RAM 8GB, 1TB de disco duro y con su respectivas tarjetas Wireless y Ethernet para las conexiones de red.

CF-30: Portátil Toughbook, con Sistema Operativo Windows XP Versión 2002 SP3, procesador Intel Core2 Duo @1.60GHz, 0.99 de RAM, 80 GB de disco duro y tarjetas Wireless y Ethernet para las conexiones de red.

CF-19: Portátil Toughbook, con Sistema Operativo Windows XP Versión 2002 SP2, procesador Intel Core2 Duo @1.20GHz, 1.87 de RAM, 50GB de disco duro y tarjetas Wireless y Ethernet para las conexiones de red.

CF-U1: Portátil Toughbook, con Sistema Operativo Windows Vista Profesional, procesador Intel Atom CPU Z530 @1.60GHz, 2.0GB RAM, 60 GB de disco duro y tarjetas Wireless y Ethernet para las conexiones de red.

Fig.7 Portátiles Panasonic Toughbook CF-30 CF-19 CF-U1 (de izquierda a derecha)

III.2.2 MOVILES

PDA DA05M: (Personal Digital Assistant), con Sistema Operativo Windows Mobile 2005, CPU Intel Xscale PXA270 @624 MHz, 128 MB RAM, conectividad WIFI, Bluetooth, GPS.

GALAXY S3: Smartphone de gama alta, con Sistema Operativo Android 4.1.2, procesador 1.4 GHz quad-core ARM Cortex-A9 CP, 1GB de RAM, 16GB de memoria interna, conectividad WIFI, GPS, bluetooth 4.0, NFC entre otros.

Fig.8 Moviles: PDA DA05M Telefono Móvil Galaxy S3

III.2.3 PUNTOS DE ACCESO

Los tres puntos de acceso utilizados son fabricados por Rajan Corporation, es llamado BreadCrumb JR, los cuales utilizan el estándar de red 802.11g para formar una red de inalámbrica mallada auto-configurable, fullduplex, flexible y segura. Comprende una radio 802.11b / g, que opera en la banda de frecuencia de 2,4 GHz. El dispositivo tiene una potencia de entrada en el rango de 10,5 a 25 VCC VDC y proporciona una potencia de salida de 3.3V a 0.5 A. La potencia real que consume puede variar entre 2,5 W a 24 V CC cuando el dispositivo está inactivo y a 4,5 W a 24 V CC cuando el dispositivo está en total funcionamiento. Tiene puerto Ethetnet 10/100 Base-TX Ethernet e interfaz de datos GPS [13].

Radio Card Frequency	Default Channel
900 MHz	5
2.4 GHz	11
4.9 GHz	40
5 GHz	152

Tabla 1. Asignación del canal

El canal por defecto para la radio BreadCrumb JR es 11 (2462 MHz)

Fig. 9 Acces Point Rajant: BreadCrumb_JR

III.3 HERRAMIENTAS DE SOFTWARE

Las herramientas utilizadas fueron las siguientes:

- SIMACOP: Es el acrónimo de SIstema de MAndo y COntrol de Pequeñas unidades, es una herramienta muy rápida de envío de órdenes y reportes (mensajes, alarmas, amenazas y objetos) entre distintas unidades [1].
- BC|Commander: Es un software del fabricante Rajant que se utiliza para el monitoreo de los puntos de acceso (BreadCrumbJR) que conforman una red mallada. También grafica la topología de la red. Este software se ejecuta en cualquier ordenador que se encuentre en la red. La versión de firmware es 10 y esta debe ser igual o mayor que la versión de firmware que se está ejecutando en los BreadCrumbs de la red [13].
- Oracle VM VirtualBox: Es un software de virtualización que permite emular un sistema operativo o varios dentro de un sistema operativo "anfitrión", creando un nuevo espacio virtual en el disco duro de donde se corre el sistema operativo visitante.
- Wireshark: Sniffer y capturador de paquetes el cual permite ver de forma más detallada la estructura de cada paquete que pasa por la red. Comúnmente utilizado como herramienta de auditoria, diagnóstico y de aplicaciones de red.
- Inssider: Ayuda a detectar redes inalámbricas cercanas, muestra la información de las señales descubiertas. Se utilizará para saber el canal que menos se esté utilizando, el más apropiado para un buen funcionamiento

Consola de Windows:

- Ping: Comando o herramienta de diagnóstico para probar si un host o sevidor son alcanzables o tienen conectividad IP, también nos da parámetros de RTT que es el tiempo desde que se envía el paquete hasta llegar al destino.
- Ipconfig: Muestra la información relativa de los parámetros de configuración de IP actual. Se pueden agregar otros comandos para realizar otras funciones como recuperar y establecer parámetros de IP
- Route: Utilizando solo el comando, sirve para observar la tabla de enrutamiento IP.

Línea de Comandos de Asterisk:

- Sip show peers: Veremos una lista de todos los usuarios, y comprobar si están conectados o no. En caso de estar conectados en ese momento, muestra información sobre la dirección IP desde la que se ha iniciado sesión.
- Sip show channel: Muestra una lista de los canales que se están utilizando o estén abierto al establecer una comunicación o al cerrarla.

IV. IMPLEMENTACIÓN

En este apartado se explicará cómo se ha realizado cada uno de los pasos para la elaboración de este proyecto y el detalle de los elementos que se eligieron para hacer parte del sistema de comunicación de VoIP sobre red de infraestructura Mesh.

IV.1 CONFIGURACIÓN DE UN SERVIDOR ASTERISK

Se empezó preparando una distribución Linux "Debian" para posteriormente instalar Asterisk. En esta preparación se utilizó una herramienta de virtualización llamada VitualBox que permite ejecutar cualquier sistema operativo de forma virtual sobre otro sistema operativo. Configurar un servidor Asterisk de forma nativa nos da muchos más control de todo, pero el funcionamiento es prácticamente idéntico al de un servidor Asterisk sobre una máquina virtual, salvo por unas diferencias que no afectan al sistema y topología propuestos, ya que ningún hardware de telefonía está implicado en este esquema.

A medida que se avanzaba y se finalizaba la configuración del servidor, se llegó a la conclusión que un servidor Asterisk, cubre una amplia gama de servicios que no se iban a emplear, ya que nuestro sistema solo necesita transmitir y monitorear comunicaciones de voz. Asterisk proporciona más, como es el de brindar soporte a grandes empresas en donde hay mucho tráfico, más actividades y servicios, a diferencia de esta implementación que se basa en una red privada. Analizando más éste escenario, en un Sistema de Emergencia se necesita practicidad, operatividad y facilidad de configuración de todos los elementos que hacen parten de ese sistema, en este caso el servidor debería cumplir con estas características para que se pueda actuar y resolver cualquier problema lo más rápido posible, pero Asterisk es un software que se caracteriza por ser muy tedioso y complicado a la hora de configurar.

Por estas razones se analizan otras distribuciones que faciliten la instalación de Linux\Asterisk y que puedan ofrecer una interfaz amigable para monitorear y administrar la central PBX. Hoy en día existen muchas, pero las más importantes son Elastix, Tribox y AsteriskNOW. Se eligió Elastix que es un software de código abierto que corre sobre CentOS como sistema operativo y actualmente su versión más estable es Elastix 2.4. Es una distribución que ha experimentado un crecimiento gracias a su cómoda interfaz de administración, facilitando así el manejo a personas que no tienen que ser programadores ni expertos en Linux. Es una forma fácil de configurar un servidor [10].

Se empieza creando una máquina virtual llamada Elastix, en donde se instala la versión 2.4 de la distribución Elastix para 32 bits. Las características de la máquina virtual son las siguientes: 2 GB de memoria RAM y disco duro de 40 GB, en el apartado de red se indica el modo de conexión, en éste caso Bridge Adapter o Adaptador Puente, esto significa que la máquina virtual podrá ser vista en la red local como si fuera un equipo independiente. En el nombre de adaptador, indica si se pretende activar la máquina virtual con el adaptador Ethernet o adaptador de la tarjeta inalámbrica, en éste caso nos interesa que esté en la red LAN Ethernet. En la figura 11, se puede observar las opciones adecuadas para los parámetros de red.

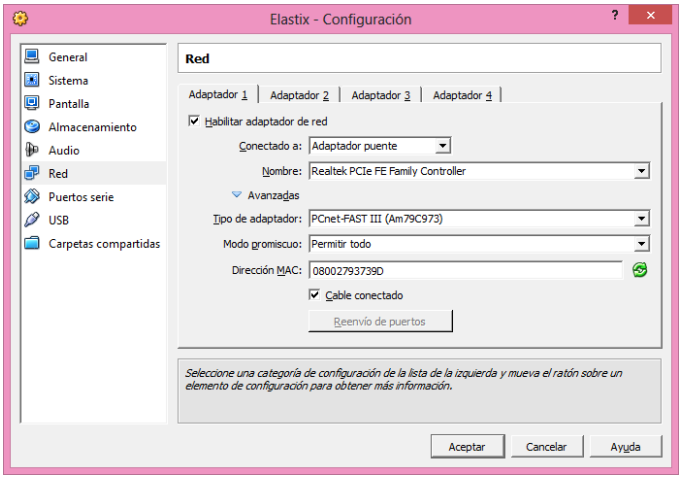


Fig.11 Configuración de red de la Máquina Virtual "Elastix"

Después de varios minutos que se haya terminado el proceso de instalación, se muestra la pantalla de inicio en donde se pide autenticación, siempre entrar como usuario "root" y escribir la respectiva contraseña. En esta pantalla se puede observar la versión del Kernnel 2.6.18 y el Release 348.1.1.el5 y la versión del Centos Relase 5.9 [10].

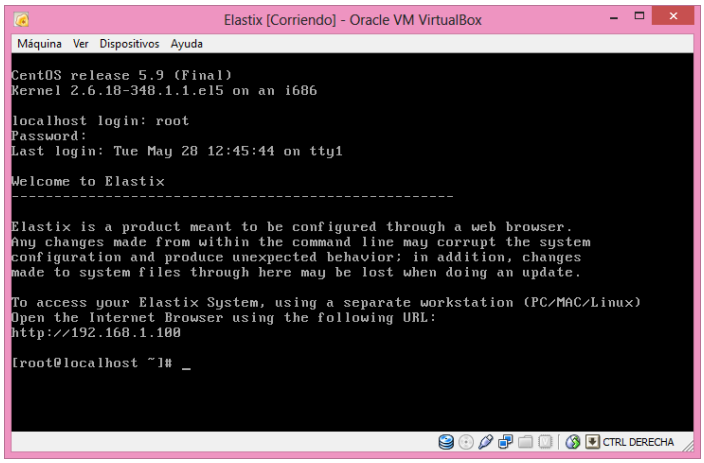


Fig.12 Inicio de la Máquina Virtual "Elastix"

Al escribir el "password" del root en la pantalla de inicio, se puede observar en la figura 12, que indica la dirección IP asignada a la máquina virtual servidor, donde se pueden realizar las respectivas configuraciones del PBX por medio de una interfaz web. Las configuraciones realizadas en servidor se pueden ver en el Anexo 1.

IV.2 CONFIGURACION Y PARAMETROS DE RED

IV.2.1 PARAMETROS INICIALES

IV.2.1.1 RED INALAMBRICA MESH

Como ya se había mencionado en puntos anteriores, la red Mesh consta de 5 terminales los cuales están conectados entre sí por medio de 3 AP inalámbricos BreadCrumb. Cada radio BreadCrumb tiene una dirección

IPv4 en la red de clase A 10.0.0.0 / 8. Este rango de direcciones es asignado durante la fabricación y no puede ser modificado. La dirección se puede asignar por medio de DHCP ya que cada dispositivo BreadCrumb incluye un servidor DHCP incorporado o se puede ingresar de forma estática en cada terminal como se ha hecho en esta implementación [13].

IV.2.1.2 RED LAN

En la red LAN se encuentra los 2 ordenadores conectado por un Switch, la dirección IP asociada a esta red es 192.168.1.0/24, en la que el terminal CF.30 tiene como dirección IP 192.168.1.1/24 y el servidor Elastix tiene la dirección IP 192.168.1.100/24 como ya se ha dicho anteriormente en el punto anterior.

Para implementar un sistema de comunicación de VoIP en la topología propuesta desde un principio, lo primero y más importante que se debe hacer, es resolver el problema de conexión entre todos los componentes que hacen parte de esta comunicación, es decir hay que lograr que todos los equipos sean alcanzables entre sí a nivel IP.

Para esto se hicieron varias pruebas y configuraciones, se modificaron distintos parámetros de host y de red y al final de muchos cambios se logra obtener conectividad absoluta desde cualquier punto de la topología.

IV.2.2 TOPOLOGIA DE RED

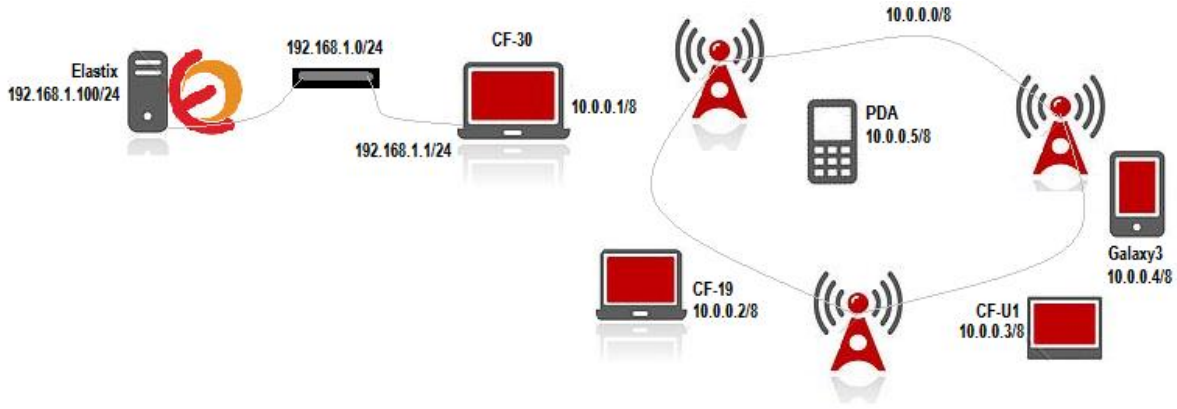


Fig. 13 Estructura de la Topología

Para llegar a esta topología probada en el laboratorio se efectuaron diferentes configuraciones en los ordenadores, se modificaron parámetros de red, se analizó el comportamiento de las 2 redes para observar que características pueden ayudar a resolver y a plantear una solución.

Todos los terminales que están en la red inalámbrica Mesh, exceptuando los móviles, necesitan que se les ingrese una ruta estática permanente hacia la red LAN 192.168.1.0/24, donde se encuentra el servidor VoIP. Al igual que los host que hacen parte de la red LAN (CF-30, Windows 8 y Máquina Virtual "Elastix") también deben tener esta ruta estática permanente para poder alcanzar a nivel IP a los host de la red Mesh. En la figura 13 se puede observar cómo se configuro la ruta estática permanente en la Máquina Virtual. Para añadir una ruta permanente en GNU Linux Centos se edita el fichero con el comando "nano /etc/sysconfig/network-

scripts/route-eth0" y luego se guarda la ruta “to 10.0.0.0/8 vía 192.168.1.1 dev eth0” en el fichero. Las configuraciones de red y de todas las rutas en los ordenadores se pueden ver en el Anexo 2.

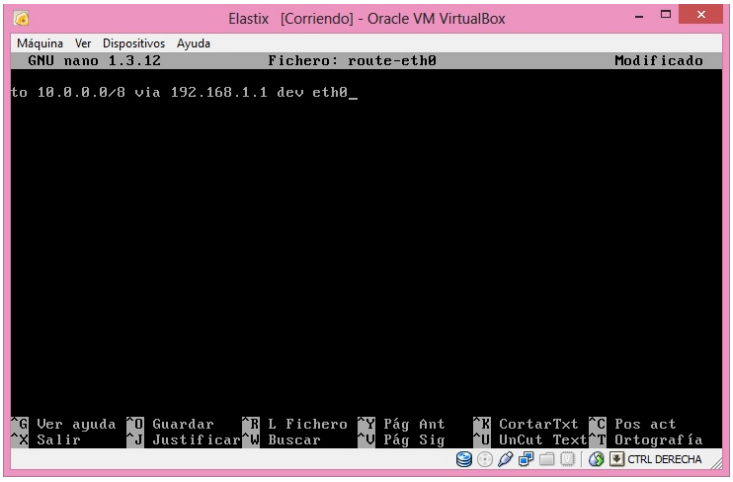


Fig.13 Ruta estática del servidor Elastix.

El portátil CF-30 está ubicado en el medio de las redes, es decir está conectado a la red LAN mediante la tarjeta de red Ethernet y a la red inalámbrica Mesh con la tarjeta inalámbrica. Debido a esto el ordenador tendría que encaminar todo el tráfico que pasa de una red a otra, en otras palabras el ordenador funciona como un router entre las 2 redes. Para que los paquetes puedan traspasar de la red Mesh a la red LAN hay que habilitar el sistema operativo del CF-30 (Windows XP) para que rutee los paquetes; por lo tanto hay que configurar el registro de WindowsXP en modo router como se verá a continuación en la figura 14. Se localiza entre HKEY_LOCAL_MACHINE\SYSTEMCurrentControlSetServices\Tcpip\Parameters\ "IPEnableRouter"

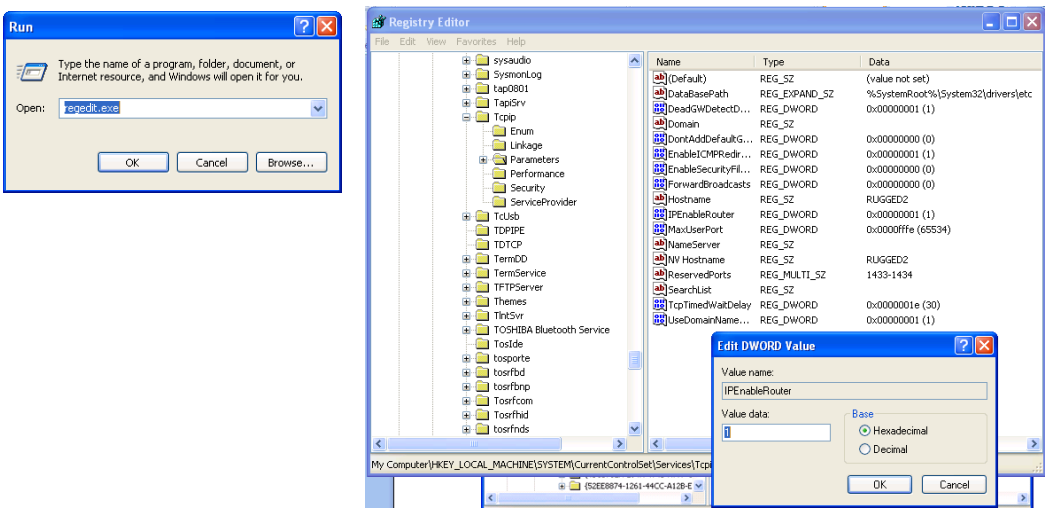


Fig.14 Modo router en Windows XP

Analizando el comportamiento de las redes inalámbricas, estas redes tienen unas características de las cuales se ha sacado provecho para ayudar a resolver y proponer soluciones a los problemas de conectividad de algunos terminales con el Servidor. Se sabe que Wireless funciona independiente de la capa 3 y el que un host se registre en un AP es previo o no previo a utilizar la dirección de Gataway, para que un terminal de la red Mesh se registre a uno de los AP solo tendría que estar asociado a nivel de capa 2, la misma red o SSID y luego sí la dirección

IP y mascara que se ha asignado es válida para esa red. Entonces por lo mismo se prefirió no colocar la dirección IP de la puerta de enlace o Gateway en los equipos, ya que igual se pueden enviar datos. Esta dirección de Gateway serviría para salir de la red hacia otras redes, pero en éste planteamiento no interesa ir a otras redes, por lo mismo no hay necesidad de colocar por ahora esta dirección IP en los parámetros de red de todos los terminales. Se saca provecho a esto pues hay algunos terminales, como los móviles, que no es fácil ingresarles una ruta estática para llegar a la red LAN, para conectarse con el servidor VoIP y poder transmitir el tráfico de voz y control. En la figura 15 se muestra los parámetros de red del móvil Galaxy S3, se observa que la dirección de Gateway es la 10.0.0.1/8 pues es la dirección IP del CF-30 en la red Mesh, el cual sirve para enrutar el tráfico hacia la red LAN, esta dirección es la dirección del siguiente salto para enviar datos a la red 192.168.1.0/24 ya que es la red en la que está ubicado el servidor VoIP. Estos parámetros son los mismo para la PDA solo cambiaría la dirección IP.

Fig.15 Parámetros de red del Galaxy S3

Después de todas las configuraciones anteriores, se realizan pruebas de diagnóstico de red con la herramienta Ping desde cada ordenador hacia todos los dispositivos de la red (Móviles, AP, Ordenadores). Todo esto con el objetivo de alcanzar conectividad desde cada cliente hacia el servidor, por lo tanto se comprobó que los pines hacia el servidor Elastix desde cada cliente de la red Mesh fueran satisfactorios.

IV.3 CLIENTES SIP

Luego de tener conectividad entre todos los dispositivos de la topología, se continúa con la configuración de las extensiones o de cada cliente SIP en el PBX y la instalación de los softphone en cada dispositivo cliente.

IV.3.1 CONFIGURACION DE LAS EXTENSIONES

Se ingresa a la interfaz web del Elastix con la dirección IP que sale en consola, luego utilizando el usuario admin y la respectiva clave accedemos a esta, se verá un listado de todos los módulos disponibles (Voicemail, IVR, Conferencias, entre otros.). Para crear la extensión se ingresa en el Menú "PBX" luego se escoge que tipo de

dispositivo a utilizar (SIP, IAX, ZAP etc.), en este caso se utiliza SIP, luego se crea la nueva extensión y se corresponde a ingresar los datos, basta con rellenar por ahora los siguientes campos: User Extensión, Display Name. Call Waiting, Secret [10].

Ésta acción se repite tantas cuantas extensiones se necesite, en éste caso son 5 clientes SIP con sus respectivos números de extensiones, nombres y claves para autenticarse desde cada terminal SIP hasta el servidor VoIP.

IV.3.2 CONFIGURACIÓN DE TELEFONO SOFTPHONE

Un teléfono softphone nos permitirá utilizar un ordenador a modo de teléfono con la ayuda de micrófono y auriculares. Esto nos va a permitir ahorrar en costes de equipo. Se estudiaron varias opciones de Softphone como: JSphone, Zoiper, Xlite. Al realizar pruebas entre todos los clientes, surgieron problemas como de compatibilidad con sistemas operativos recientes (Windows7), el hardware de algunos dispositivos no soporta las versiones actuales y por último el escaso software que existe hoy día para dispositivos con sistemas operativos antiguos. Por estos motivos se quiso utilizar un Softphone que se pueda instalar en la mayoría de los ordenadores sin ocasionar problemas entre dispositivos (audio en un solo sentido, línea ocupada, etc.), ya sea por incompatibilidad o por otros aspectos.

Al final se instalaron 2 software, el **Zoiper** ya que fue el que tuvo menos inconvenientes con todos los sistemas operativos, y el **JSphone** el cual se utilizó en un solo dispositivo por ser el único software con una versión compatible con Windows Mobile 5.0 (PDA). En el Anexo 3 se explica cómo se configuran los clientes SIP en los softphone.

IV.3.2.1 ZOIPER

Ofrece versiones gratuitas para Windows, MacOS y Linux. Por tanto, no es necesario que el usuario del teléfono tenga instalado un sistema operativo concreto en su puesto de trabajo. Zoiper es un cliente de VoIP muy sencillo y práctico, que permite configurar extensiones tanto con el protocolo SIP como con IAX. Además permite utilizar varias líneas de forma simultánea y seleccionar el códec utilizado entre los más habituales, codificaciones como G.711 (a-law, u-law), GSM, Speed e iLBC (20, 30). Se utilizó G.711 allow.

IV.3.2.2 SJPHONE

Es uno de los softphones SIP opensource que todavía se sigue utilizando mucho, es gratuito, funciona en Windows, Linux, Mac, WindowsMobile y WindowsCE, tiene algunas desventajas como un elevado consumo del procesador de un equipo.

Para que las extensiones funcionen adecuadamente se debe configurar correctamente los teléfonos o softphone en los ordenadores y móviles, con la dirección del servidor, número de extensión, nombre, password del cliente correspondiente al establecido en el PBX. En la siguiente figura 16 se muestra el softphone Zoiper.

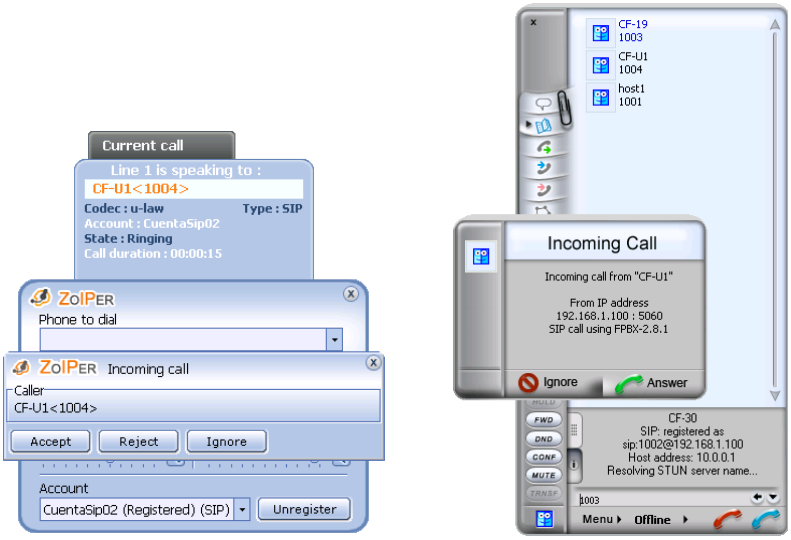


Fig.16 Imagen del Softphone Zoiper

Después de todas las configuraciones en los terminales aparece en cada softphone de los clientes "la cuenta ha sido registrada", con esto se procedió a realizar llamadas de cliente a cliente, obteniendo así comunicación entre todos sin ningún inconveniente en las conversaciones; las llamadas se escuchan bien, sin eco y la movilidad en los clientes no es impedimento para que la comunicación fallara o se distorsionara. Gracias al suficiente ancho de banda que proporciona la red Mesh se puede realizar varias llamadas entre todos los clientes. El ancho de banda mínimo en un solo sentido para cada conversación de VoIP es alrededor de 87.2Kbps y al agregar las cabeceras de otras tecnologías de capas inferiores éste ancho de banda para transmitir una llamada cambiaría [8].

Como se habló en el principio, éste proyecto se va implementar en una red Mesh de uso táctico por lo cual puede estar acompañado con un Sistema de Mando y Control para brindar más prestaciones en la red. Teniendo otros sistemas y operaciones en la red Mesh, se podría ocupar más ancho de banda y las conversaciones podrían verse afectadas por otro tipo de tráfico, esto conlleva a disminuir o evitar que se transmitan paquetes que desperdicien ancha banda el cual puede aprovecharse para mejorar el rendimiento[7].

Como ya se ha explicado en apartados anteriores los clientes utilizan el protocolo SIP para establecer las sesiones y el protocolo RTP para enviar tráfico de voz entre los clientes (Servidores Proxy) [5]. Hasta este punto la topología proporciona comunicación de VoIP, enviando tráfico de control y de voz desde el cliente origen al servidor, y este envía al destino, es decir por cada llamada realizada en la red Mesh se están enviando 4 flujos de voz más los de control y señalización, lo ideal sería, la señalización (SIP) y las conversaciones de voz (RTP) viajan por caminos diferentes y que solo el trafico RTP se envíen entre los usuarios de la red. Con esto se reduciría a 2 flujos de voz por cada llamada realizada.

Para hacer efectivo esto, se realizaron cambios en cada extensión del PBX en los parámetros canreinvite y dtmafmode. Canreinvite a "NO" fuerza a que el servidor Asterisk no permita que los extremos si envíen paquetes RTP entre sí, por lo tanto se cambia a "SI", el parámetro dtmafmodo es el modo en el que se transmiten los tonos DTMF (dual tone multi frequency o tono dual de múltiples frecuencias), es un parámetro que está

tanto en la configuración de las extensiones del PBX como en cada uno de los softphone, éste puede ser RFC2833, INFO, en banda (codificado junto con el audio) y auto, cualquiera de los modos tiene que ser igual en los 2 softphone y en las extensiones que establezcan una comunicación. Con la opción modo RFC2833 los tonos se envían por medio de RTP, por lo que obligaría a enviar los tonos al servidor. Con SIPINFO los tonos son entregados usando SIP, que no es un mecanismo recomendado para la entrega de audio en tiempo real, pero es el que se eligió. Es necesario que los 2 softphone soporten transcoding o que tengan el mismo códec cuando se comuniquen para que se puede realizar una correcta negociación y no tenga que participar el PBX. Otra opción que se podría cambiar sumado con los parámetros anteriores, es el de obligar que solo se utilicen algunos códec configurándolos desde el PBX ingresando estos códec en la opciones allow y disallow [10].

V. ANALISIS DE CALIDAD DE SERVICIO (QoS)

La calidad de servicio se sigue presentado como un requisito indispensable en cualquier tipo de red, pues se necesita mantener un ancho de banda que garantice en este caso, una adecuada comunicación de VoIP evitando que no sea afectada por ningún factor externo. Es por eso que lo recomendable es identificar claramente las causas, efectos directos e indirectos y qué soluciones hay para los elementos que ocasionan que la QoS no llegue a ser óptima. Los factores que más influyen generalmente en VoIP son la latencia y la perdida de paquetes [7].

V.1 PRUEBA DE CALIDAD DE SERVICIO

Para hacer un análisis de los parámetros de calidad de servicio, se realizaron varias pruebas a diferentes distancias con el fin de saber que prestaciones está brindando la red en distintos puntos de la zona. El procedimiento para realizar la prueba fue:

- Instalación de la red Mesh y obtener la conectividad absoluta.
- Configuración de un Servidor NTP para sincronización del reloj en los ordenadores.
- Instalación del software de Mando y Control SIMACOP en los ordenadores para el monitoreo de las unidades o clientes en el campo.
- Realizar llamadas entre las unidades para ensayar la cobertura y la calidad de la comunicación.
- Obtener valores para examinar las prestaciones de la red.

Esta prueba se realizó en la playa de un municipio de la Comunidad Valenciana llamado El Puig, se eligió esta zona ya que se tenía un mapa topográfico de este municipio donde el Laboratorio de sistemas de tiempo real y distribuido ha realizado varias pruebas sin ningún inconveniente.

Con ayuda de la aplicación SIMACOP instalada en los equipos de la prueba, se pudo establecer las distancias de una antena a otra para capturar y analizar los datos, cada unidad o equipo tienen un mismo fichero que se instaló y se cargó para comunicar y distribuir sucesos de la operación entre todos los del equipo. En la siguiente

figura 17 se observa cómo se visualiza el mapa del El Puig desde la versión SIMACOP instalado en la PDA antes de empezar la prueba.

Fig. 17 GESTOP versión SIMACOP para PDA "mapa del Puig"

Gracias a este sistema se pudo compartir la ubicación por cartografía y datos de la operación, pues SIMACOP recoge toda esta información que se envía, la representa en un display o pantalla del terminal (unidades ubicadas en la cartografía) y la envía por la red Mesh al puesto de mando que en este caso está ubicado junto a la antena central [1]. El recorrido se muestra en la figura 18, en donde se mueven 2 antenas respecto a una antena central, de 100 en 100metros se realizaba una llamada hasta llegar a 400 metros, siendo un total de 800 metros de recorridos analizando y obteniendo medidas QoS.

Fig. 18 Mapa de El Puig, recorrido de la prueba

V.1.2 TOPOLOGÍA DE PRUEBA

La topología consta de varios equipos como el CF-30, CF-19, CF-U1, la PDA quienes tienen instalado el GESTOP versión SIMACOP para los equipos, que controla la ubicación en la zona y también en esta topología participan la central PBX y 1 móviles Android. Se puede observar en la figura 19 una topología en la cual hacen parte 6 clientes SIP conectados a una central PBX interna en la red Mesh. Al ser diferente esta topología de campo, de la analizada en el laboratorio, los parámetros de red de los equipos, las configuraciones en la central PBX (extensiones) y en los softphone de cada cliente se modificaron, para lograr conectividad entre todos y el establecimiento de comunicaciones de VoIP entre los clientes SIP, las configuraciones para esta prueba se pueden ver en el Anexo 4. Al igual que la topología de laboratorio se cuenta con los mismos equipos, especificaciones, sistemas operativos, los cuales ayudaron a realizar la prueba y a mantener en constante comunicación con el equipo de trabajo.

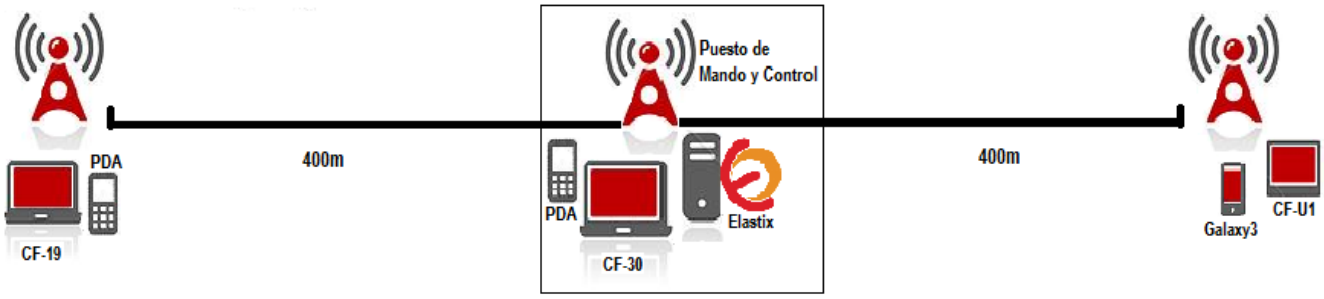


Fig. 19 Topología de prueba de Calidad de Servicio

Se obtuvieron las medidas haciendo pruebas de movilidad para analizar la calidad de servicio de los clientes SIP en movimiento. Consistió en realizar llamadas entre 2 clientes desde los 2 extremos de la red Mesh cada 100 metros de la antena central, cada uno de estos cliente permaneció siempre en cobertura de las antenas, se hizo captura de los paquetes recibidos en el cliente CF-19 utilizando el analizador de paquetes Wireshark. Se utilizó un teléfono móvil Android en el que también se configuró un cliente SIP para mantener en comunicación con el grupo de trabajo.

La comunicación que se estableció desde cada extremo de la red se realizaba por medio de la antena central, es decir, no había una comunicación directa entre estas, por lo que podemos indicar que se realizan 2 saltos para la conexión y el transcurso de la llamada. Al establecer una llamada la antena a la que se está conectado, envía los paquetes a la antena central y luego ésta envía al otro extremo de la red. Este número de saltos y la distancia entre las antenas influyen en los valores de latencia y jitter que se analizaron en la prueba, pero al mismo tiempo brinda información de que parámetros técnicos hay hasta una determinada distancia y hasta cuanto puede la red garantizar una calidad en las comunicaciones de VoIP [2].

La ITU especifica valores máximos y mínimos de ancho de banda, retardo en llamadas VoIP, en donde específica que el ancho de banda mínimo es de 80Kbps, si este es menor podría escucharse mal la voz [11]. El máximo retardo o latencia es de 150ms de extremo a extremo, para valores mayores de retardo la comunicación se vuelve molesta por la pérdida de interactividad, si se pasa de 200ms la comunicación es imposible. El jitter

máximo recomendado en una conversación es de 20ms, entre 20ms y 30ms es aceptable si se incrementa a más de100ms sería imposible la comunicación. Las pérdidas de paquete no deberían superar 3%, según vaya aumentando el porcentaje poco a poco se verá afectada la calidad de la llamada.

En la prueba de movilidad se hizo un recorrido hasta alcanzar la medidas requeridas, los primeros datos se obtuvieron a 100m de la antena central, se capturaron 4688 paquetes RTP en la primera llamada, a 200m se capturaron 4208 paquetes RTP, en 300m 4225 paquetes RTP y a 400m 4118 paquetes RTP. En las siguientes graficas se mostraran 4 graficas por medida de QoS, la primera grafica corresponderá a 100m(a) la segunda a 200m(b) la tercera 300m(c) y la cuarta 400m(d).A continuación se mostraran y se analizaran los resultados de las capturas obtenidas en la prueba de movilidad.

V.1.3 *ANCHO DE BANDA*

En este parámetro se debe tener en cuenta el tamaño de los paquetes de voz, ya que las cabeceras que se añaden a cada paquete transmitido generan un extra a la tasa normal del códec elegido. Si se desea minimizar las cabeceras se enviarían cada paquete de gran tamaño lo cual traería como consecuencia mayor tiempo de empaquetado (generalmente se utiliza de 20ms) [8]. La compresión de voz aumentaría este tiempo de paquetización, por lo que entre más se comprima, mayor es el tiempo de empaquetado y el tamaño del paquete disminuye, es por esto que este tiempo ayuda a determinar el tamaño máximo de cada paquete.

Para estimar el ancho de banda necesario para la prueba de VoIP el tamaño de la carga útil viene estimado por el bloque de entrega del codificador y por el número de bloques que se desea transportar en un paquete (cabeceras) como se explicó en el apartado de paquetización [12]. Para esta prueba se usó el códec G.711 a-Low desde los 2 clientes SIP y con un periodo de empaquetizado de 20ms, el tamaño de la carga útil es de 160 Byte y con un promedio de tasa real de transmisión o ancho de banda requerido de 87,2Kbps (con cabeceras IP/UDP/RTP) en una llamada [8]. En la siguiente gráfica se observa el ancho de banda para las distancia.

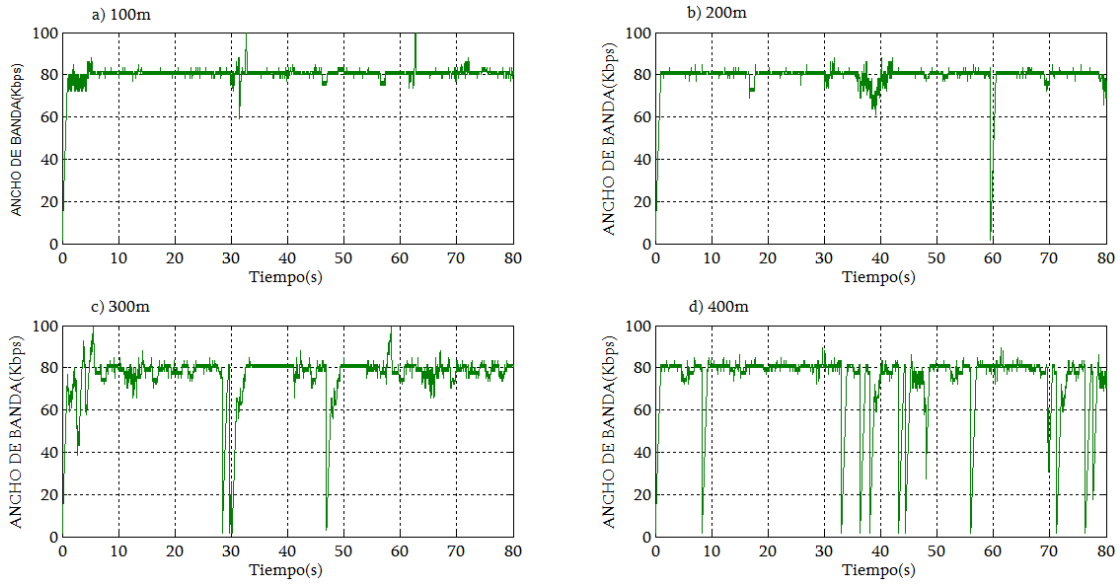


Fig.20 Ancho de banda medido

En la primera grafica representa el ancho de banda a 100m de distancia de una antena a otra, con un promedio de 80.15Kbps, el cual se mantiene un poco constante en el trascurso de la llamada durante 80s. Este promedio está según la UIT en el ancho de banda mínimo permitido para una conversación VoIP, que es de 80Kbps. Las otras distancias de 200m, 300m y 400m se observa como ya no es constante el trafico RTP en las conversaciones, las cuales presentan fluctuaciones de alto rango de ancho de banda. Estos datos se puede ver reflejado en el promedio de estas distancias, pues a 200m se tiene un promedio de 79.04Kbps, a 300m de 76.12Kpbs y a 400m de 73.71Kbps los cuales se encuentran por debajo del ancho de banda mínimo permitido por la UIT [10].

V.1.4 LATENCIA

El retardo o latencia es la diferencia que existe desde el momento en que se transmite una señal, hasta que llegue al receptor. Este retardo en una conversación debe mantenerse por debajo de un nivel para minimizar la perdida de la interactividad entre los clientes. A continuación se muestran en las gráficas las medidas correspondientes para cada distancia.

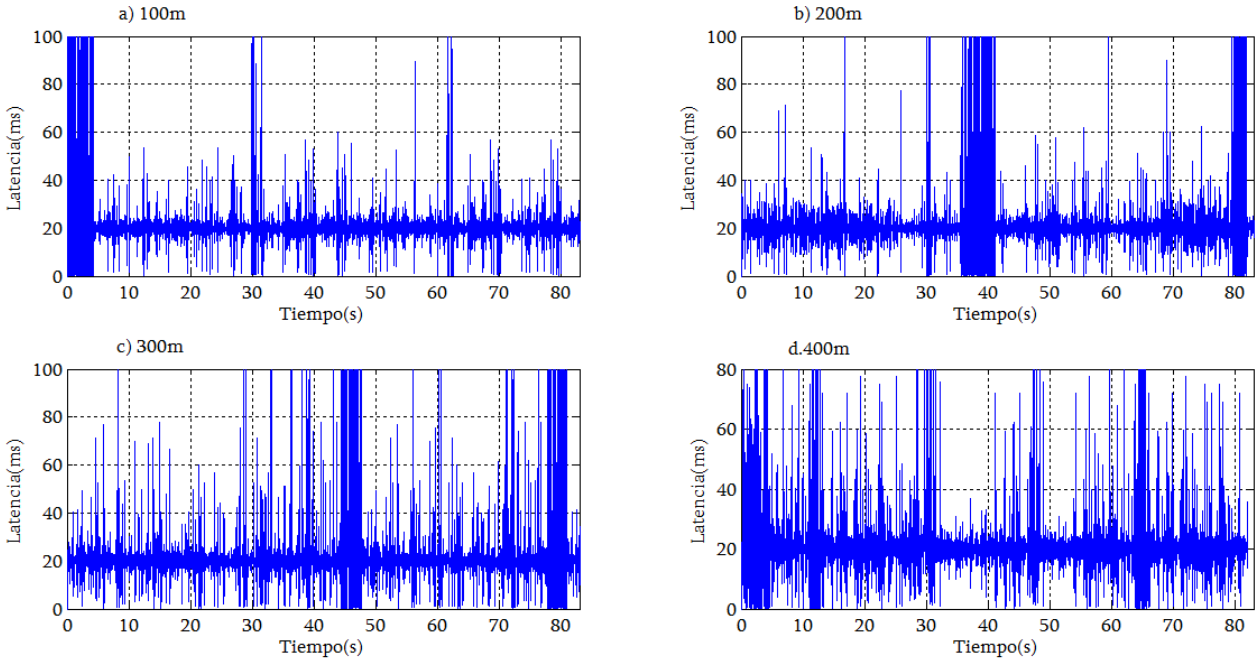


Fig.21 Latencia medida a gran escala

En la figura 21.a se observa que la mayoría valores capturados a 100m de distancia, llegan con un retardo alrededor de 20ms, se valoró como una comunicación clara, fluida y no se percibió ningún tipo de retardo al igual que la figura 21.b en la que se sostuvo también una buena conversación sin ningún tipo retraso, en ésta los valores del retardo aumentan, ya que la mayoría de los paquetes llegan con una latencia alrededor de los 30ms. En la figura 21.c la latencia en muchos de los paquetes se incrementa al doble con respecto a la figura 21.a algunos llegando a valores de los casi 50ms, a diferencia de la figura 21.d en la que cual la conversación se mantiene menos estable con cortes de voz, teniendo más valores de latencia por encima de 40ms. Todos los valores promedios de las gráficas están por debajo del valor máximo de retardo permitido por la ITU para

llamadas VoIP, el cual es de 150 ms, pero evidentemente si hubiera más terminales Mesh estos valores aumentarían [11].

En la figura 22 se observa los picos de retardo que se llegan a alcanzar en cada distancia, al igual de cómo crece la latencia con respecto aumenta la distancia, también se encuentran rangos de elevación desde 20ms hasta casi 1700ms, donde se percibió cortes en la voz durante pocos segundos, el resto de tiempo transcurrió normalmente la llamada. Si estas elevaciones con valores de latencia de más de los 150ms fueran más constante, por ejemplo en la distancia de 400m, lo más probable es que hubiera mucho más pérdidas causando degradación en toda la llamada hasta llegar a no escuchar nada, como ocurrió a 500m.

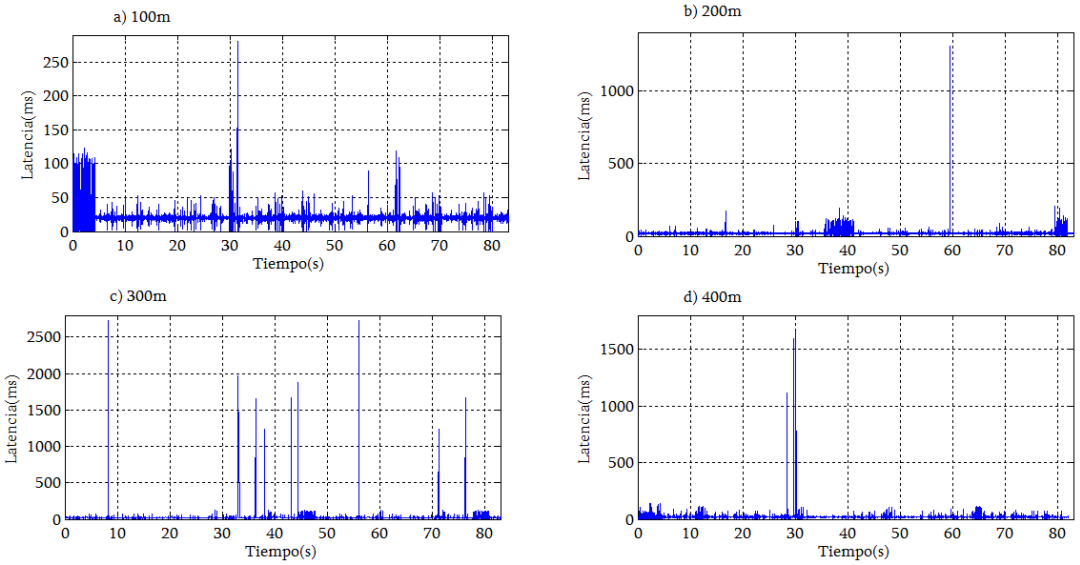


Fig.22 Latencia medida

V.1.4 JITTER

El jitter se puede decir que es la variación de los tiempos de llegada de los paquetes, causados por muchos factores como congestión en la red y por las pérdidas de sincronización ya que los paquetes no llegan a su destino en orden y mucho menos a una velocidad constante, pero el audio tiene que tener una velocidad constante[7]. El jitter entre los puntos iniciales y final de una comunicación debería ser inferior a 100 ms. Si su valor estar por debajo de 100 ms, puede ser compensado de manera apropiada.

En la figura 24.a se muestra como se empieza con un jitter de casi 20ms, pero luego el tiempo de llegada de un paquete con respecto al otro, se estabiliza más en la mayoría de los paquetes ya que se mantienen con un jitter por debajo de los 4ms, en la 24.b se observa que hay más paquetes manteniéndose con valores de 4 y 5 ms, en la 24.c la mayoría de los paquetes sobrepasa los valores de jitter de 5ms, también hay valores de 10ms y picos que llegan por encima de los 25ms. En la 24.d hay más valores con 10ms de jitter con relación a las distancias anteriores y picos más altos que llegan hasta casi 180ms como se puede apreciar en la figura 23.

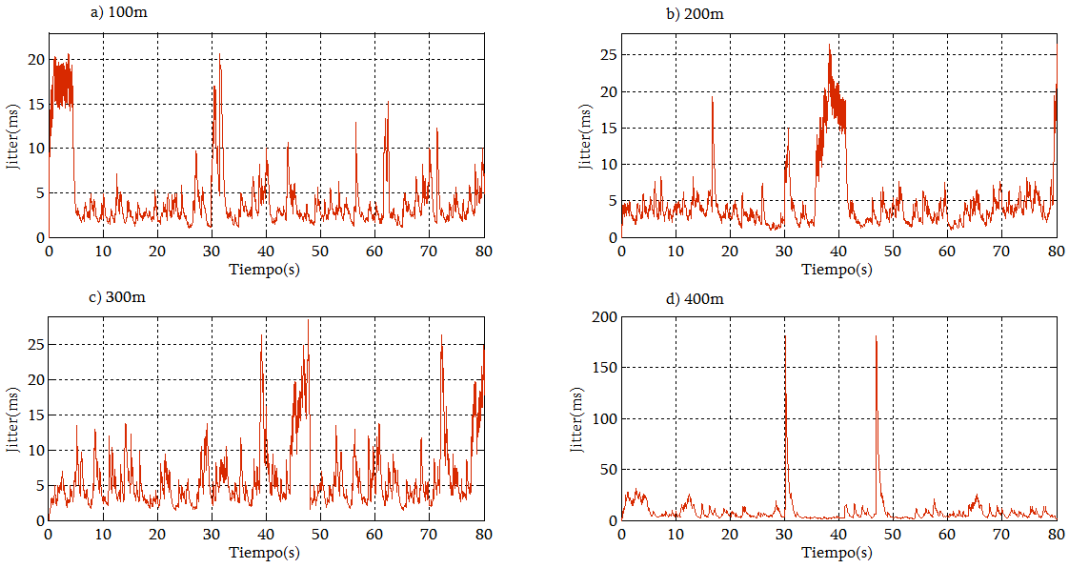


Fig. 23 Jitter medido

El jitter promedio medido para 100m es de 4,23ms, para 200m es de 5ms, para 300m 6,14ms y de 400m 8,56ms. Estos promedios de cada distancia están por debajo del valor máximo recomendado para mantener una excelente comunicación que es de 20ms.

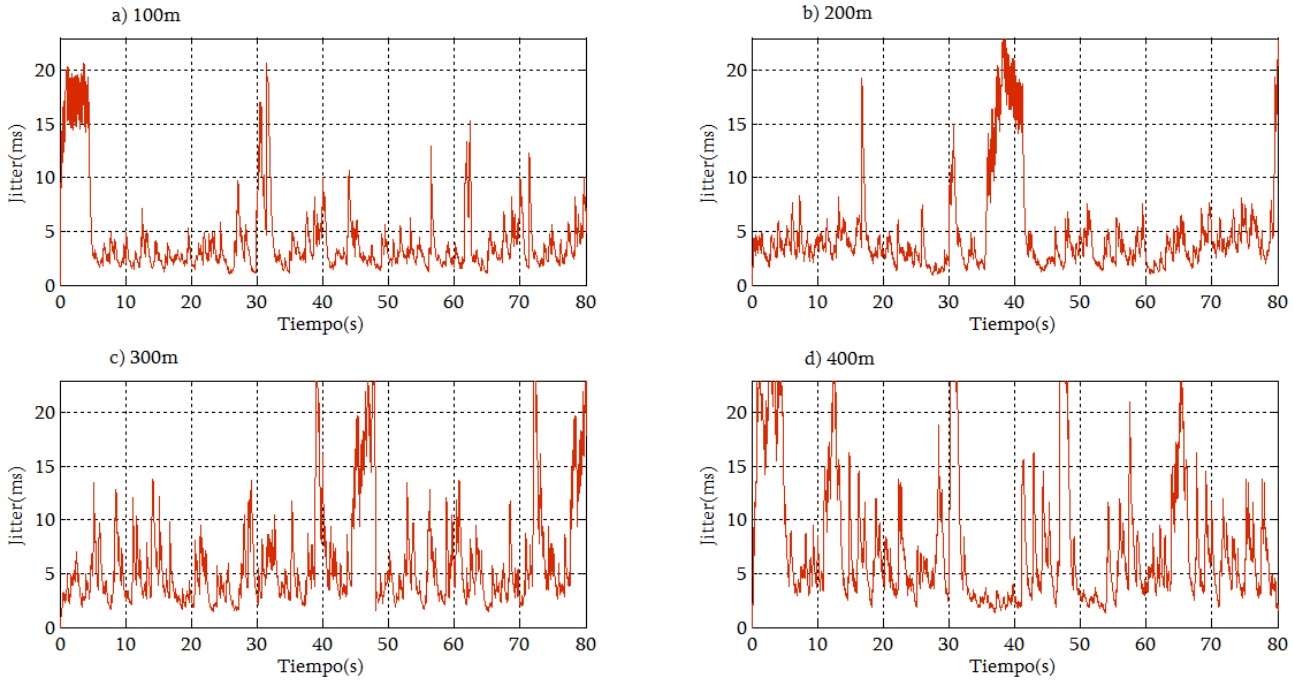


Fig. 24 Jitter medido a gran escala

V.1.5 PÉRDIDAS DE PAQUETES

Las pérdidas de paquetes se deben a muchos factores como son la congestión en la red o por fallos de comunicación, estas pérdidas no solo se refieren a que los paquetes no lleguen al destino, también hace referencia a la llegada de paquetes después de un tiempo determinado lo que ocasiona que el paquete sea inservible y se descarte. El tráfico de VoIP se transporta en paquetes UDP (RTP sobre UDP), el control que se

puede aplicar para estas pérdidas de paquetes se realiza en los extremos de la comunicación [7]. Los códec pueden predecir los paquetes perdidos y reemplazarlos (interpolar y sustituir) así no se percata el usuario de que falta un paquete. Cuando las pérdidas son superiores al 5% los distintos códec no pueden predecir los valores de paquetes perdidos, por lo tanto a falta de paquetes de voz se distorsiona la comunicación y disminuye la calidad de la llamada. En la siguiente figura 25 se observan las pérdidas de paquetes RTP capturadas en cada distancia, se puede apreciar que en las gráficas 25.a y 25.b son los únicos porcentajes de las cuatro capturas, que están en el máximo valor recomendado. En teoría las pérdidas no deberían superar el 3%, pero en las pruebas realizadas en las distancias de 300 y 400m no se contaba con el umbral de ancho de banda requerido para conservar una conectividad estable, produciendo una relación de perdida de paquetes con respecto al aumento de la distancia entre las antenas, sin embargo, a nivel de prueba la conversación tuvo un grado de comunicación básica que garantizó una calidad aceptable de la llamada [11].

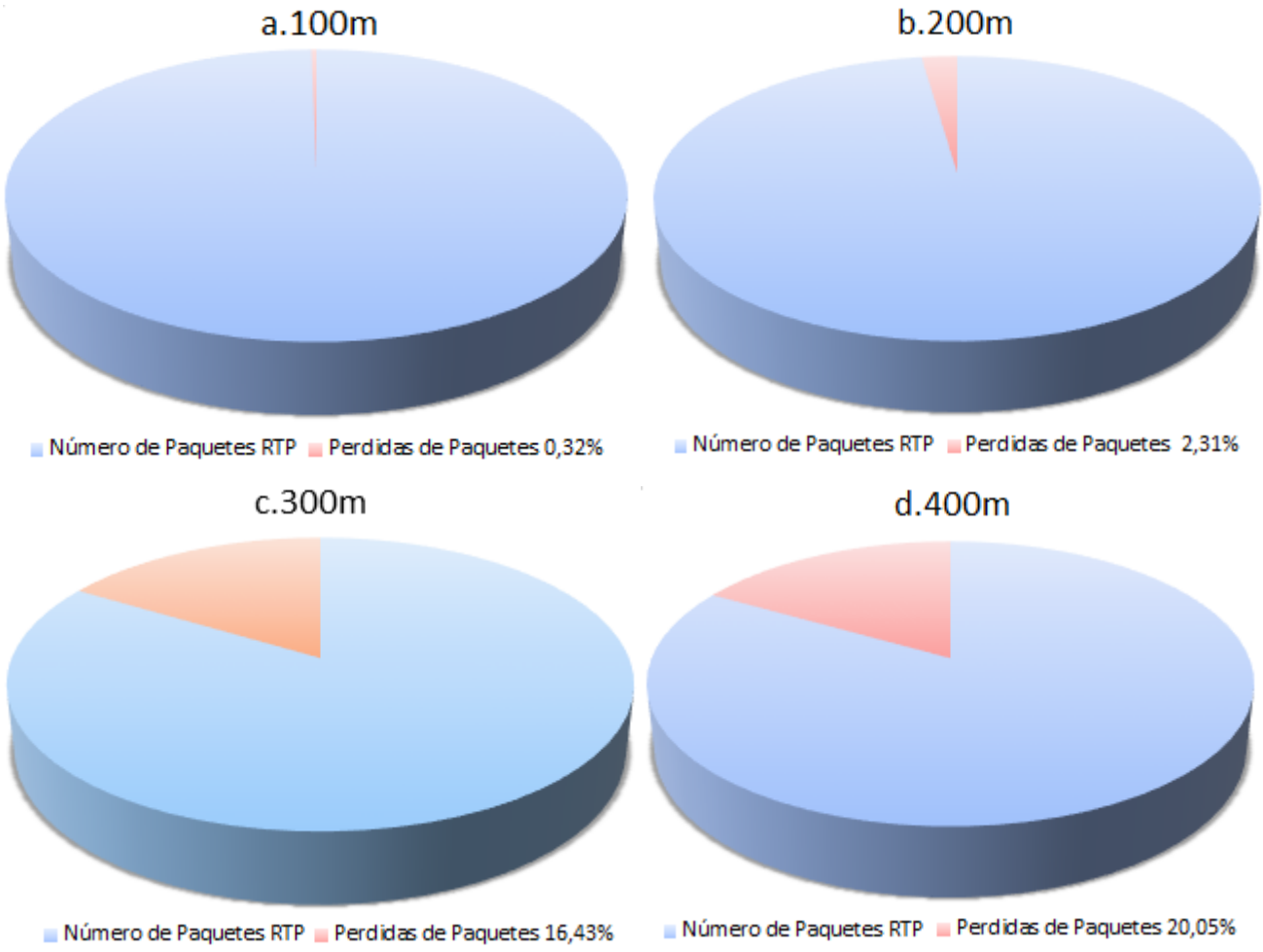


Fig. 25 Pérdidas de Paquetes medida

Todos estos factores que afectan la calidad de las llamadas, pueden reducirse con distintas técnicas y mecanismos, garantizando que el sistema opere y ofrezca el mejor desempeño red y satisfaciendo los requerimientos de los servicio de comunicación, como por ejemplo implementando equipos que permitan soportar el manejo de prioridad de tráfico (Router), reserva de ancho de banda mínimo etc.

También se puede considerar otros tipos de códec para el tráfico de voz, que hagan un uso más efectivo de los recursos disponibles en la red, se podría cambiar por códec libres que usan poco ancho de banda como los son el códec de GSM y el Speex. Otra alternativa es el G.729 que es un códec propietario altamente robusto pero requiere de una licencia para su uso comercial. También se puede considerar otros tipos de códec para el tráfico de voz, que hagan un uso más efectivo de los recursos disponibles en la red, se podría cambiar por códec libres que usan poco ancho de banda como los son el códec de GSM y el Speex. [12].

Los códec están diseñados para enviar las muestras con una frecuencia determinada. Lógicamente, el receptor debe decodificarlas y reproducirlas con la misma frecuencia. Por efecto del jitter es posible que, llegado el momento de reproducir una muestra, no se haya recibido todavía el paquete correspondiente, es por esto que se implementa un almacenamiento temporal (basado en buffer) de paquetes en el receptor llamado "*Jitter Buffer*", que funcionan acumulando varias muestras en una cola, y reproduciéndolas a la frecuencia correspondiente. También ayuda al problema de la llegada de tramas RTP fuera de orden, chequeando los números de secuencia de éstas.

Cuando el tiempo de llegada de los paquetes es desigual, el jitter buffer no alcanza a controlar estos y se pueden perder paquetes, deteriorando la calidad de la voz. Cuando este jitter buffer tiene un valor muy alto, menor será la probabilidad de que se pierdan y se descarten paquetes, pero será mayor el retardo añadido. En servicios interactivos como VoIP no podemos agrandar este buffer, ya que el usuario escucharía la voz con un retardo grande y se percibiría una mala calidad de experiencia en la llamada. Este buffer se puede configurar tanto en el servidor Asterisk como en el softphone de cliente y se recomienda que no supere los 100ms para no degradar la comunicación [7].

VI. AGRADECIMIENTOS

Primero que todo a mi familia por confiar en mí y darme la oportunidad de estudiar en el exterior, a mi director el Dr. Manuel Esteve por permitirme trabajar con él, por su gran apoyo, dedicación y consejos profesionales, a él Dr. Israel Pérez por su dedicación constante y gran aporte en el desarrollo de este trabajo de investigación, a él profesor Juan Ramón Díaz por su tiempo y aporte de conocimientos, a todos los compañeros de Laboratorio de Sistema de Tiempo Real y Distribuido que colaboran con buen ambiente de trabajo y por último no siendo menos a todos mis amigos y personas que han estado a mi lado acompañándome y ayudándome de una manera u otra a sobrellevar todos los inconvenientes que se han presentado en el transcurso del Master.

VII. CONCLUSIONES

Este proyecto se hizo con el objetivo de implementar un sistema de comunicación de VoIP en una red Mesh, en el cual, a través del estudio de sistemas de telefonía IP basados en Linux y Asterisk, el análisis de características y comportamiento de las redes inalámbricas Mesh y la comprobación de resultados válidos, se logró la instalación y funcionamiento de una central PBX de Elastix que establece y controla las llamadas originadas desde clientes de una red Mesh de uso táctico, que emplean diferentes equipos (laptop, ordenadores, móviles, etc.) con distintos sistemas operativos para establecer la comunicación.

Para implementar esta tecnología independientemente para que ámbito se utilice, ya sea para pequeñas hasta grandes empresas, se debe tener una apropiada arquitectura, buenos equipos con sistemas operativos para que el sistema pueda funcionar correctamente y no se presente ningún problema que afecte a la calidad del servicio.

El interés particular del trabajo estuvo en el uso y análisis de la tecnología de VoIP en el entorno de redes Mesh como soporte de comunicaciones de sistemas de información para Mando y Control aplicados a Gestión de Emergencias.

Al analizar las medidas para evaluar la calidad del sistema de VoIP, permitió estimar en éste ámbito de uso, que prestaciones estaba aportando la red y hasta qué punto podría garantizar los parámetros técnicos que puedan mantener una calidad en el flujo de los datos. Los valores de latencia, jitter, ancho de banda y pérdidas, son proporcionales a la distancia que hay entre las antenas y al número de saltos en el momento de establecer una comunicación, debido a la perdida de cobertura e intensidad de señal de las antenas. Es por eso que los valores promedios de ancho de banda, latencia, jitter y perdidas de paquetes son óptimos a una distancia de 100m entre antenas, ya que el sistema es capaz de enviar una mayor cantidad de información a la red, obteniendo mejores resultados en comparación a las otras distancias. En cuanto a las pérdidas de paquetes aparte de no disponer de un buen ancho de banda, puede que el buffer de entrada del dispositivo receptor de VoIP (CF-19) no haya logrado el control de la secuencia de los paquetes para poderlos procesar, lo que puede haber provocado un vacío en los datos y cortes de la señal de voz.

Teniendo en cuenta los datos obtenidos en la prueba se verifica la viabilidad de uso de la tecnología VoIP sobre una red Mesh, pues utilizando solo 3 antenas se obtuvo una calidad aceptable para realizar y mantener una llamada, para un número adecuado de terminales Mesh en la misma red, de hasta 8, separados por unas centenas de metro que sería la dimensión típica en una unidad de intervención de emergencia.

Al implementar este sistema de comunicación en paralelo con otras tecnologías y arquitecturas de datos en un Sistema de Mando y Control se debe saber administrar el tráfico, ya que hay aplicaciones y servicios que devengan un elevado consumo de banda que deterioran las comunicaciones como también puede afectar a los equipos a nivel de aplicación por el alto consumo de recursos estos.

Para el buen funcionamiento del servicio VoIP es necesario reforzar la seguridad, protegiendo y limitando el acceso a la red VoIP y a sus componentes sobre todo desde el exterior, evitando que la red sea vulnerable a

fallos de seguridad y a ataques. Esto se puede lograr habilitando protocolos encriptación (WPA-2) y de cifrado (AES) en los que el canal de señalización también debe de ir completamente cifrado, también es recomendable utilizar VLAN's para priorizar y proteger el tráfico VoIP separándolo en canales lógico de las redes de datos.

VIII. BIBLIOGRAFIA

[1] I. Pérez, *Arquitectura de un sistema C4ISR para pequeñas unidades.* Tesis doctoral, Universidad Politécnica de Valencia, Departamento de Comunicaciones, 2009.

[2] C. Amit, S. Gurpal, Performance Evaluation and Delay Modelling of VoIP Traffic over 802.11 Wireless Mesh Network, International Journal of Computer Applications, Articulo,2011, Vol.21(9), pp.7-13

[3] L.J. Sánchez, 802.11s based Wireless Mesh Network (WMN) test-bed. Final Project, Luleå University of Technology, Dept. of Computer Science and Electrical Engineerin.

[4] J. Sierra, R. Hincapié, R. Bustamante, L. Betancure, Modelo de simulación de la capa MAC IEEE 802.16-2004 para modo Mesh, Vol 4 No 8, Universidad Icesi, 2006.

[5] R. Gutierrez, Serguridad en VoIP "Ataques Amenazas y Riesos" Universidad de Valencia, 2008.

[6] J. M. Cabellero "Implementación de una Red (VoIP) a través de software libre en el desarrollo de una pequeña central telefónica" Tesis, Universidad Autonoma de Yucatan, 2007.

[7] J.Saldaña "Tecnicas de optimización de parámetros de red para la mejora de la comunicación en servicios de tiempo real" Tesis doctoral, Universidad de Zaragoza, Departamento de Ingeniería Electrónica y Comunicaciones, 2011.

[8] Telefónica, Entendiendo la tecnología Voip, contribución técnica, AR.CT.D.0.0014.00, Edición N° 00, Marzo 2002.

[9] J.Saldaña "Tecnicas de optimización de parámetros de red para la mejora de la comunicación en servicios de tiempo real" Tesis doctoral, Universidad de Zaragoza, Departamento de Ingeniería Electrónica y Comunicaciones, 2011

[10] Elastix: Open Source Unified Comunications Server: http://www.elastix.org

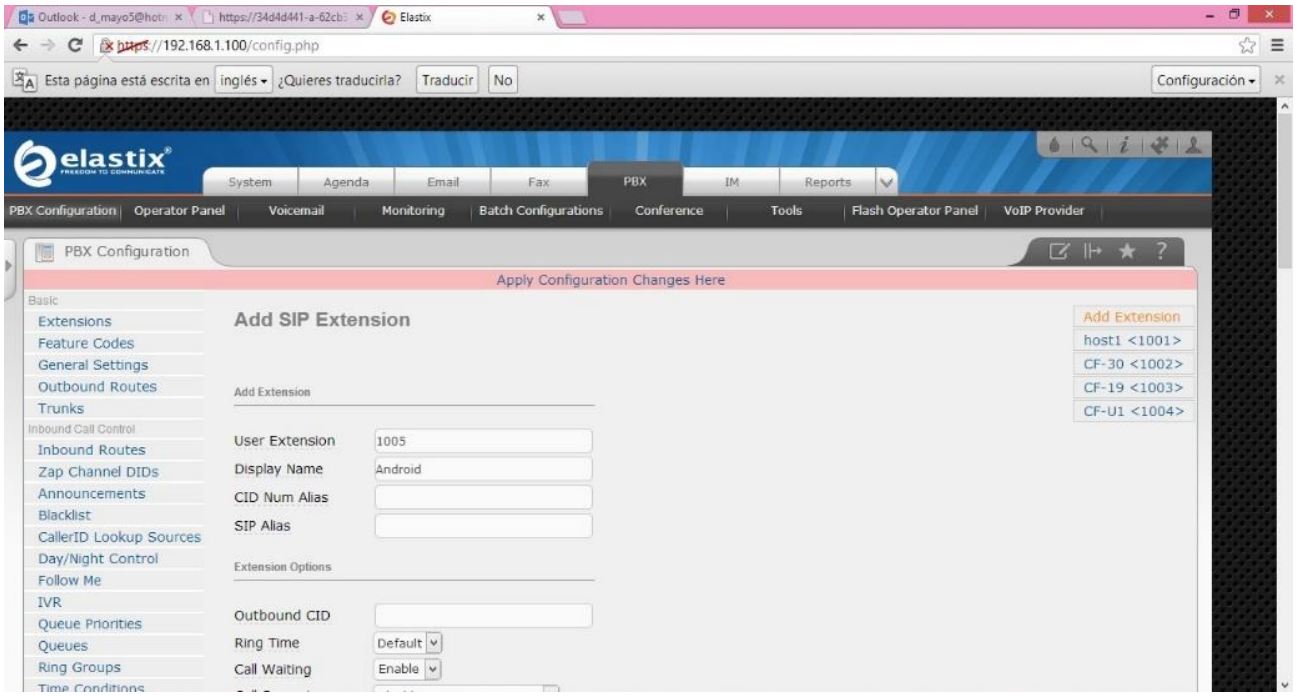
[11] ITU: International Communications Union: http://www.itu.int/ITU-T

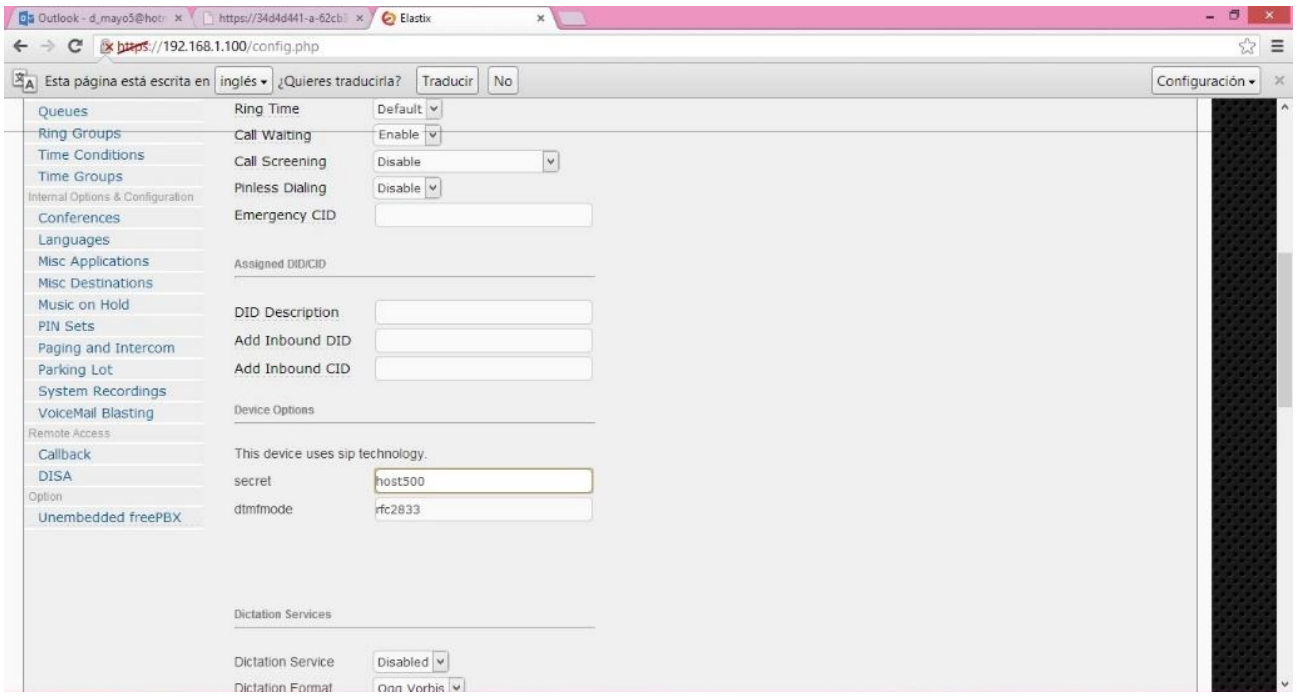
[12] Kim, Kyungtae ; Choi, Young-june ;Lee, Suk-han ; Hanzo, Lajos ; Chung, Min, Young; Lee, Sang-won; Cho, Kwangsu, Performance comparison of various VoIP codecs in wireless environments, Ubiquitous Information Management and Communication: Proceedings of the 5th International Conference, (ICUIMC '11), 2011, pp.1-10

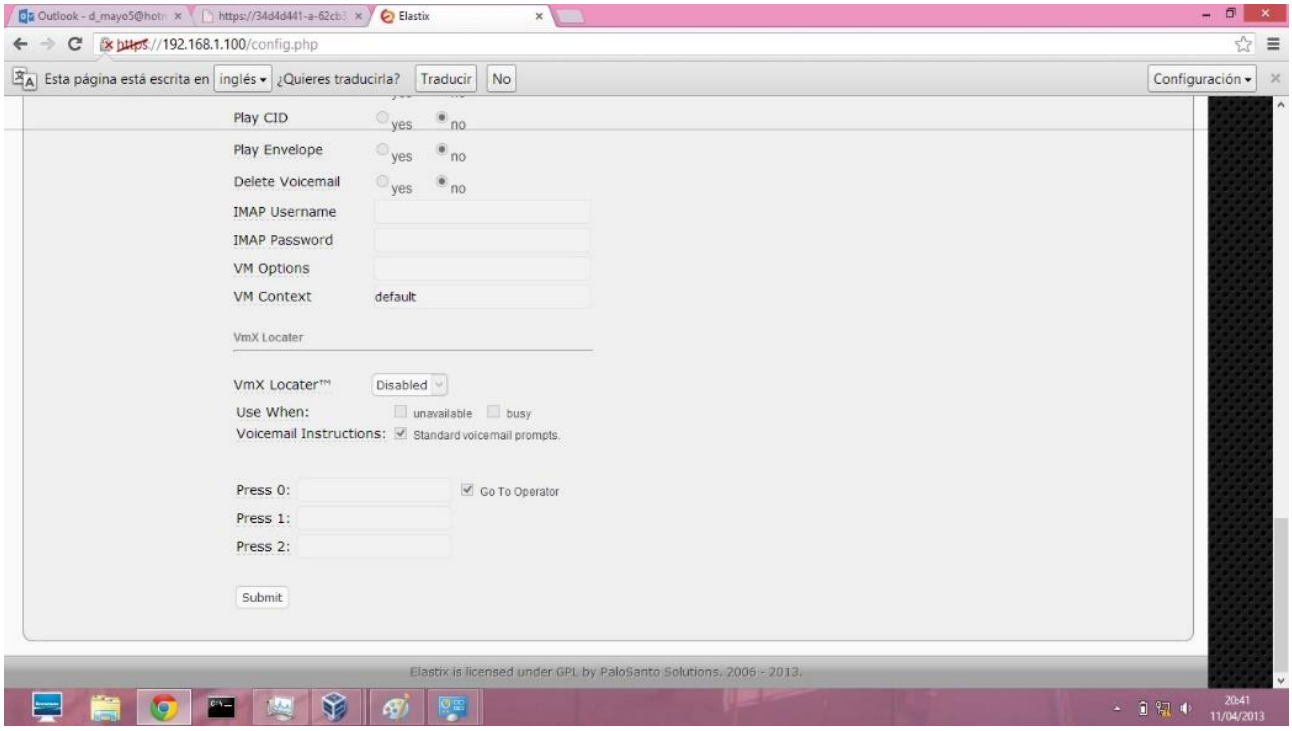
[13] Antenas Mesh: http://www.rajant.com/products/breadcrumb-jr

ANEXO 1. CONFIGURACIONES REALIZADAS EN SERVIDOR

Luego de ingresar la dirección correspondiente al servidor en una ventana, para entrar a la interfaz de administración WEB, en esta se puede empezar a configurar las extensiones desde la pestaña PBX. En la siguiente figuras se mostrará los datos que se ingresan para crear la extensión para la PDA las otras extensiones de los otros equipos que hicieron parte de ésta topología propuesta se expresaran en la tabla 1.







Click en submit y luego en Apply Configuration Changes Here para que se guarden y se carguen los valores en Elastix.

DISPLAY NAME	USER EXTENSION	CALL WAITING	SECRET	DTFMMODE
CF-30	1002	ENABLE	host200	RFC2833
CF-19	1003	ENABLE	host300	RFC2833
CF-U1	1004	ENABLE	host400	RFC2833
ANDROID	1005	ENABLE	host500	RFC2833
PDA	1006	ENABLE	host600	RFC2833

Tabla 1. Datos de configuración de cada las extensión

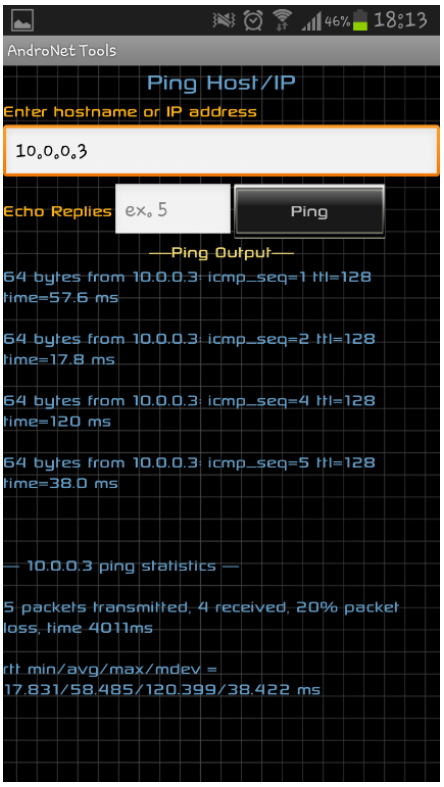
ANEXO 2. CONFIGURACIONES DE RED

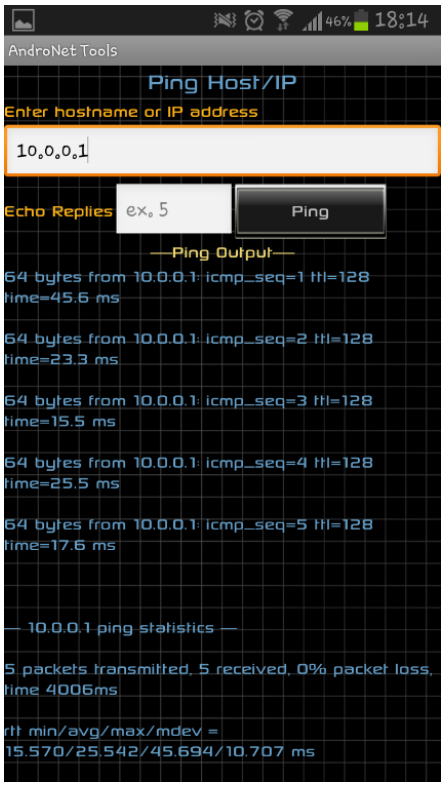
En la tabla número 2 se muestran los parámetros de red y las rutas configuradas desde la línea de comandos de cada equipo.

EQUIPOS	DIRECCION IP	MASCARA	GATEWAY	RUTAS
Lenovo	192.168.1.2	255.255.255.0		route ADD-p 10.0.0.0 MASK 255.0.0.0 192.168.1.1
Maquina Virutal:Elastix	192.168.1.100	255.255.255.0		nano /etc/sysconfig/network-scripts/route-eth0" "to 10.0.0.0/8 vía 192.168.1.1 dev eth0"
CF-30	192.168.1.1	255.255.255.0		Configuración modo Route
	10.0.0.1	255.0.0.0		
CF-19	10.0.0.2	255.0.0.0		route ADD-p 192.168.1.0 MASK 255.255.255.0 10.0.0.1
CF-U1	10.0.0.3	255.0.0.0		route ADD-p 192.168.1.0 MASK 255.255.255.0 10.0.0.1
ANDROID	10.0.0.4	255.0.0.0	10.0.0.1	
PDA	10.0.0.5	255.0.0.0	10.0.0.1	

Tabla 2. Direcciones IP y Rutas configuradas en los equipos

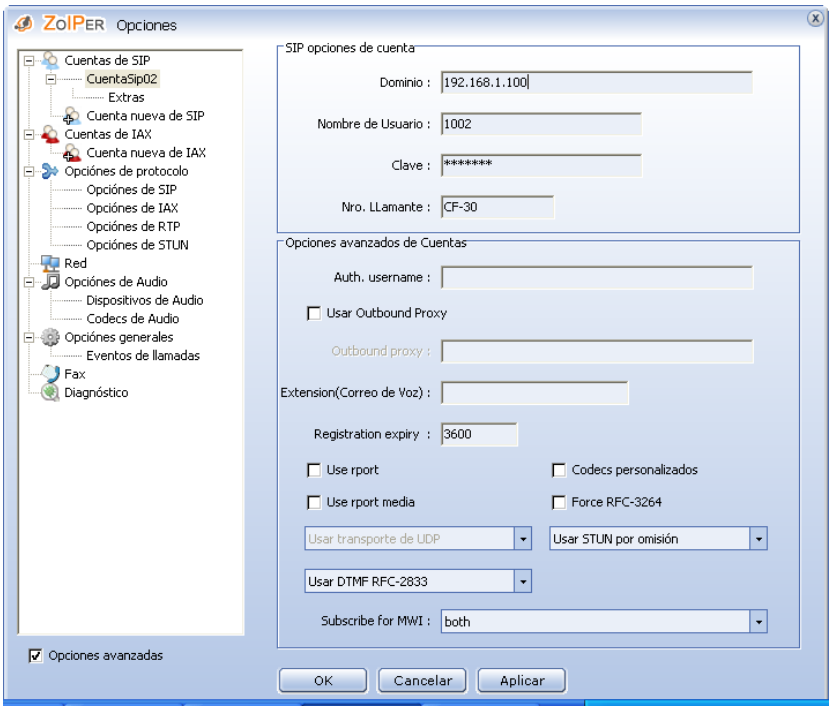
Se comprueba la conectividad con todos los ordenadores desde el móvil Android S3, por medio de una herramienta de diagnóstico de Android llamada AndroNet Tool. Las siguientes figuras muestran los pin a cada terminal.



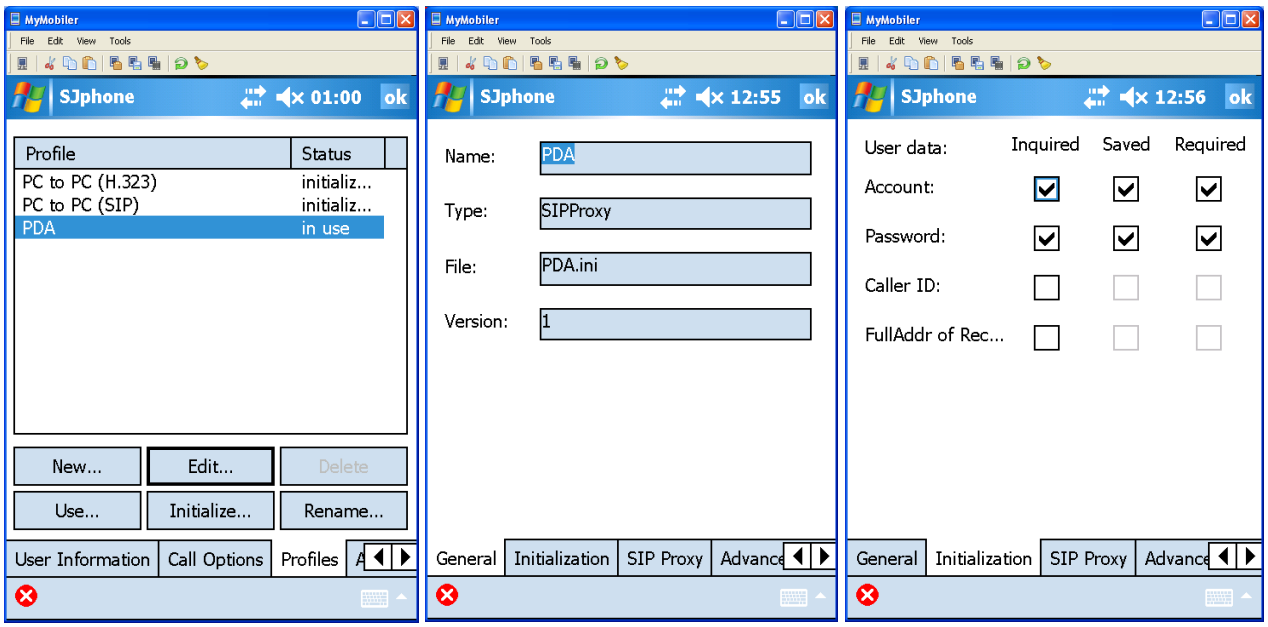


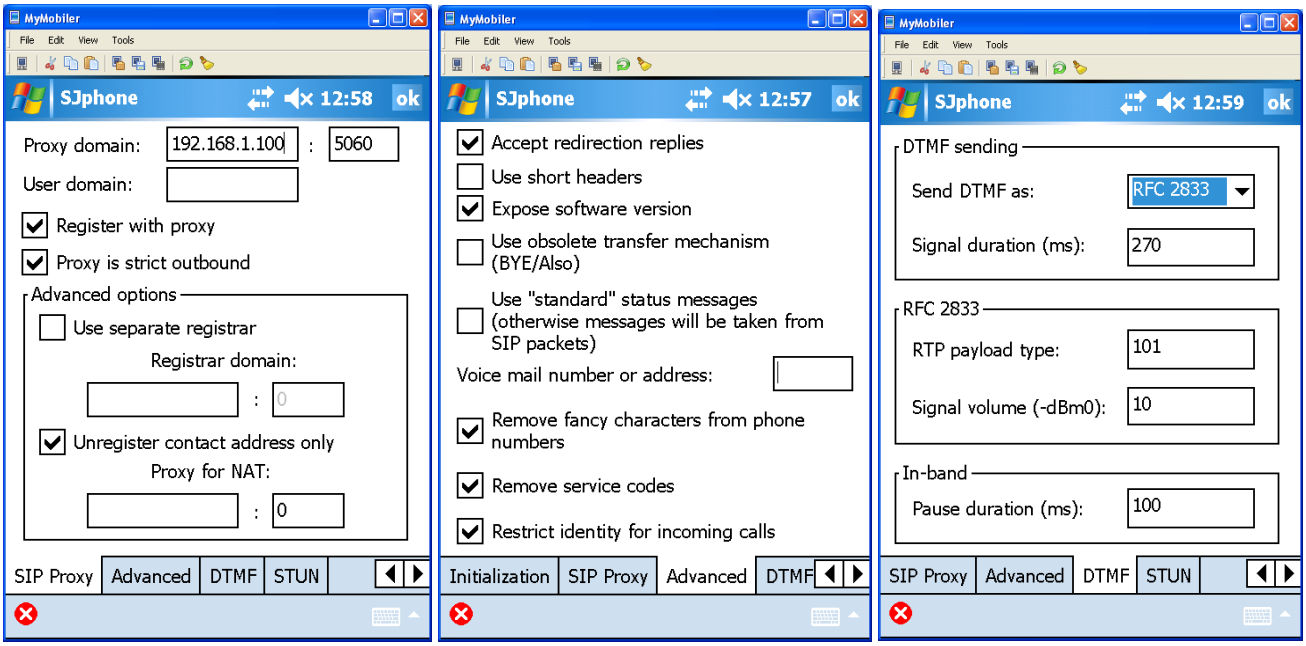
ANEXO 3. CONFIGURACION DE LOS CLIENTES SIP

Después de obtener la conectividad completa desde la red LAN hasta la red Mesh, se prosigue a la configuración de los clientes SIP, en cada uno de los softphone correspondientes. La configuración en el softphone Zoiper se puede apreciar en las siguientes figuras



Todos estos parámetros varían según el cliente que se ha configurado en el PBX, se ingresa la dirección del servidor donde se autenticará y enviará los datos de voz y de control, User Extension (Nombre de Usuario), secret para la extensión (clave) y el Display Name (nombre). La configuración del DTMF (RFC-2833) es recomendable que sea la misma tanto en el servidor como el softphone. La configuración en el softphone SJphone se puede apreciar en las siguientes figuras:





Igual como se ha explicado anteriormente las configuraciones deben de ser las mismas tanto en el cliente como en el servidor, se recomienda no cambiar ninguna otra opción en el SJphone aparte de las señaladas.

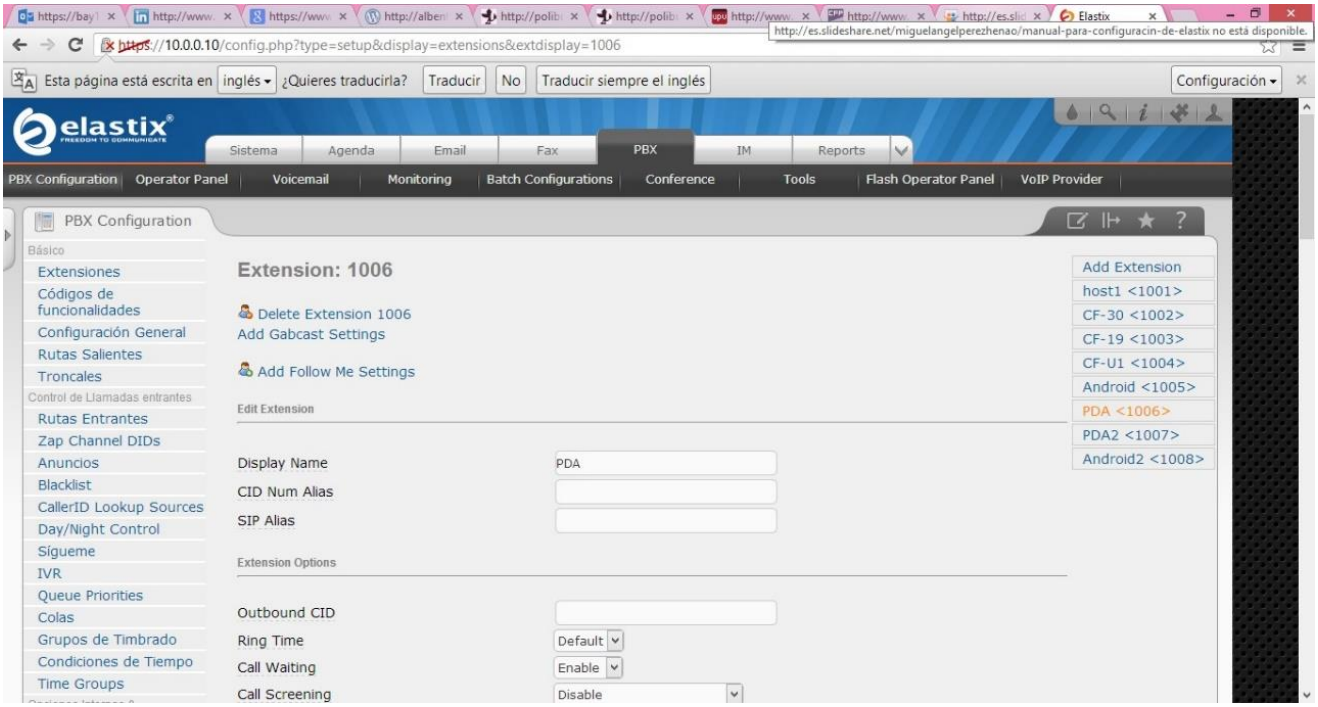
ANEXO 4. CONFIGURACION PARA LA PRUEBA DE CAMPO

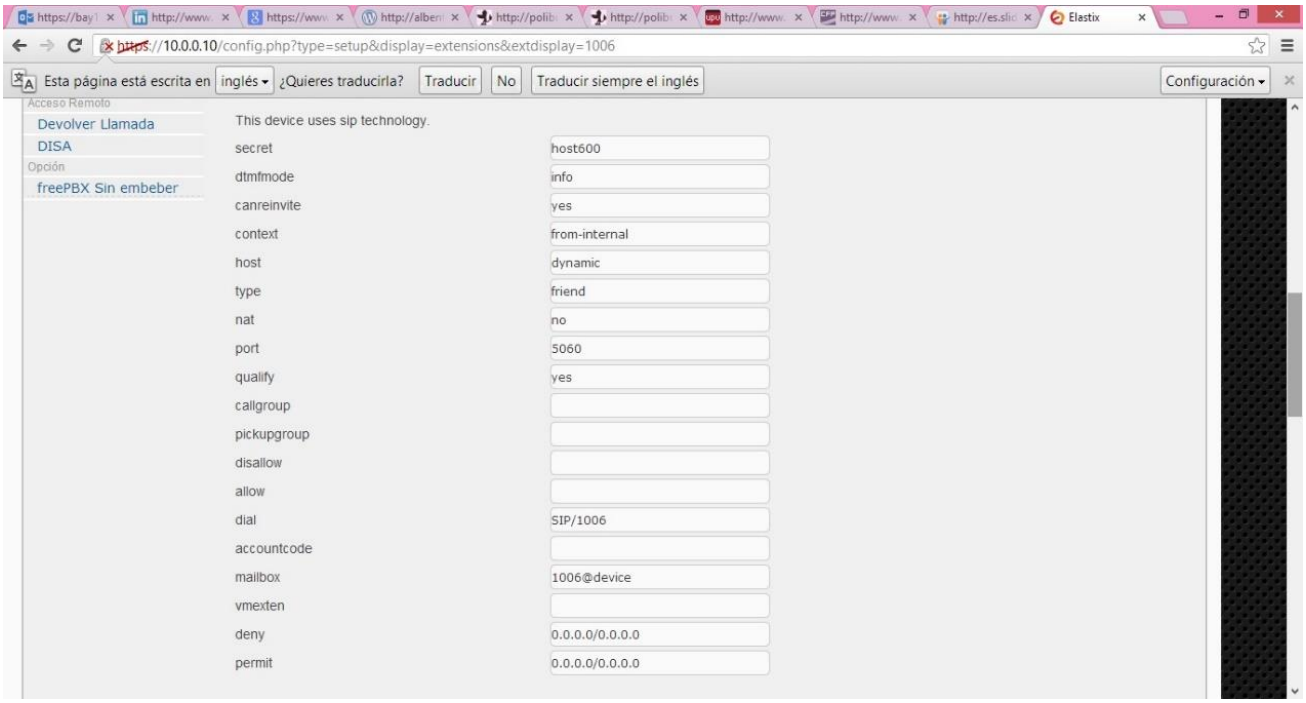
En la tabla 3 se muestran las direcciones IP para la topología de prueba.

EQUIPOS	DIRECCION IP	MASCARA	GATEWAY
Lenovo	10.0.0.9	255.0.0.0	
Maquina Virutal:Elastix	10.0.0.10	255.0.0.0	
CF-19	10.0.0.1	255.0.0.0	
CF-30	10.0.0.2	255.0.0.0	
CF-U1	10.0.0.3	255.0.0.0	
PDA	10.0.0.4	255.0.0.0	10.108.134.1
ANDROID	10.0.0.5	255.0.0.0	10.108.45.1

Tabla 3. Direcciones IP para los Equipos

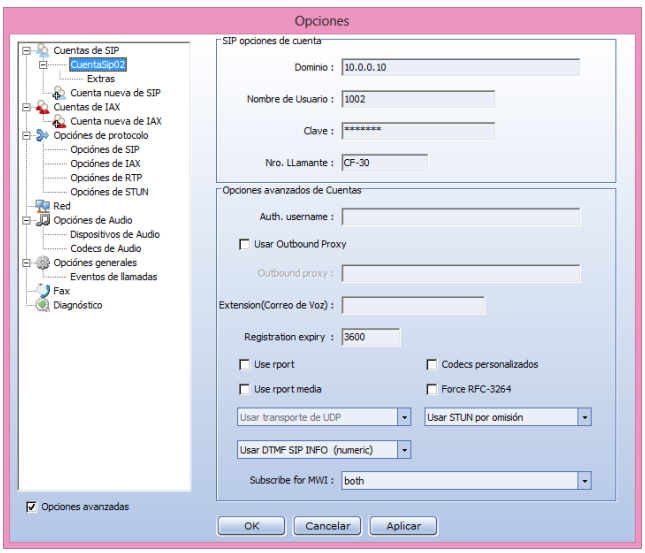
Al tener otra topología el servidor ya hace parte de la red Mesh por lo tanto tiene otra dirección IP, tambíen se cambian algunos parametros en las extensiones, se mostrara a continuación para la extensión de la PDA.

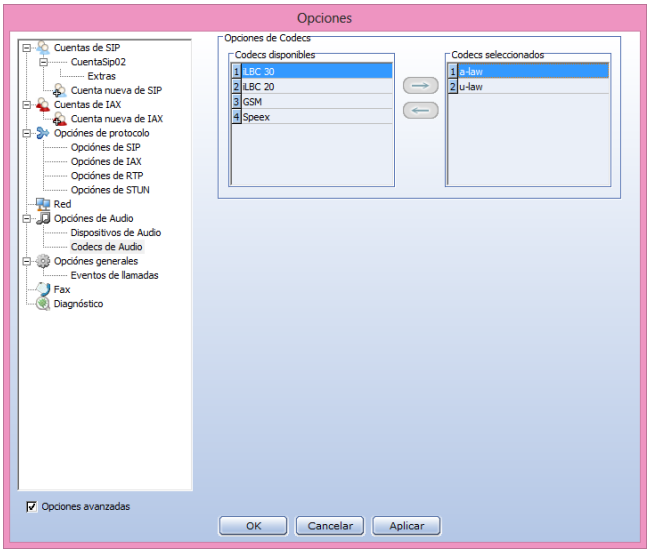




La configuración en el cliente tambien cambia tanto el modo DTMF y los codecs predeterminados en los clientes deben ser los mismos para que el servidor no tenga que hacer transcoding. Se mostrará esta configuración desde el Zoiper y SJphone.

Zoiper





SJphone