

## IMPLEMENTACIÓN DE LA PLANTA TELEFÓNICA IP ENTRE EL LABORATORIO DE TELEMÁTICA DE LA FUNDACIÓN UNIVERSIDAD AUTÓNOMA DE COLOMBIA Y EL LABORATORIO ANKLA DE CINTEL

*Implementation of the IP telephone plant between the telematics laboratory of the  
Universidad Autónoma de Colombia Foundation and the ANKLA laboratory of Cintel*

Alvarado Mejía, A.\*; Orozco-Zambrano, L.E.\*\*; González-Bustamante, R.A.\*\*\* y Sánchez-Pacheco, W.F.\*\*\*\*



### RESUMEN

El artículo presenta el desarrollo del proyecto para la implementación de una planta telefónica IP entre el laboratorio de telemática de la Fundación Universidad Autónoma de Colombia y el laboratorio de Cintel. Con referencia a los conceptos de las redes de nueva generación y empleando el protocolo de señalización de comunicación más ampliamente utilizado en la tecnología de voz sobre IP (protocolo de inicio de sesiones (SIP)), se realizó la interconexión a través de una red privada virtual (VPN) y se utilizó una distribución libre de servidor de comunicaciones unificadas (Elastix) compatible entre los dos laboratorios, realizándose un análisis de la *paquetización* de voz sobre IP para garantizar un correcto funcionamiento.

### ABSTRACT

The article expose the implementation of an IP telephone exchange project between the Autonomous University telematics laboratory and Cintel laboratory. Referring to the next generation networks concepts and using the most popular communication protocol in VoIP technology, the session initiation protocol (SIP), We made an interconnection via virtual private network (VPN) and using a free Unified Communications Server distribution (Elastix) supported by both laboratories, an analysis of bundling voice over IP was made too to ensure a proper operation.

**Palabras clave:** IP, NGN, SIP, VoIP, ToIP, VPN, Asterisx, Elastix.

**Key words:** IP, NGN, SIP, VoIP, ToIP, VPN, Asterisx, Elastix.

\* Universidad Autónoma de Colombia. alexander.alvarado@fuac.edu.co

\*\* Universidad Autónoma de Colombia. orozco.luis@fuac.edu.co

\*\*\* Ingeniero Electrónico, M.Sc.

\*\*\*\* Ingeniero Electrónico, M.Sc.

## 1. INTRODUCCIÓN

Uno de los pilares de la sociedad actual y en el que se basa gran parte del desarrollo humano son la internet y las tecnologías que se están desarrollando sobre ésta. Las actuales líneas de desarrollo tecnológico de las telecomunicaciones apuntan hacia las *redes de siguiente generación o red próxima generación (next generation networking (NGN))*. La idea principal que se esconde debajo de este tipo de redes es el transporte de paquetes encapsulados de información a través de Internet con el objetivo de lograr la convergencia tecnológica de los servicios multimedia (voz, datos, video...). Estas redes serán construidas a partir del protocolo IP (Internet Protocol), siendo el término *all-IP* comúnmente utilizado para describir dicha evolución.

El proyecto contempla el uso de los equipos de comunicaciones y telefonía IP (Planta IP bajo Asterisk) del laboratorio de telemática de la Fundación Universidad Autónoma de Colombia (FUAC) para crear una conexión con el laboratorio ANKLA de Cintel ubicado en el Tecno Parque del Sena, constituyéndose así como un proyecto innovador dentro de la FUAC al ser el primero en trabajar con NGN, contribuyendo en abrir una línea de investigación sobre estas redes para su posterior estudio por parte de los estudiantes de la FUAC.

## 2. CONCEPTOS GENERALES

### 2.1. Redes de nueva generación

El concepto de red de próxima generación fue introducido inicialmente por Bellcore. Una red de próxima generación se caracteriza esencialmente por la separación de las funciones de transporte y de control, y por el hecho de que la primera se basa en la tecnología de paquetes. El objetivo de esta arquitectura es construir una red convergente donde la voz y los datos compartan la misma infraestructura de transporte. Otra meta de esta arquitectura es abrir el camino a una nueva generación de servicios.

Una red de próxima generación puede tener las siguientes características técnicas:

- Todos los datos de las aplicaciones son transportados en paquetes/células.
- Tecnología de banda ancha en el acceso.
- Redes multiservicio con capacidad de QoS en la red en el borde.
- Funcionamiento en red óptica en la red núcleo.
- La arquitectura abierta de control distribuido sustituye al conmutador «monolítico» clásico.
- Capa inteligente distribuida que separa la lógica de control del transporte.
- Plataformas y API abiertas para la creación, el aprovisionamiento y la distribución de servicios inteligentes/mejorados.
- «Tecnología web» para la gestión de redes y servicios, incluida la «autogestión» del cliente (gestión basada en la web) (UTI, 2015).

### 2.2. Arquitectura general de una red NGN

La arquitectura general de una NGN está conformada esencialmente por las siguientes capas: aplicación o servicios, control, conectividad y transporte (Redes de Próxima Generación NGN, 2015).

- a) Capa de Gestión: esta capa, esencial para minimizar los costos de explotar una NGN, proporciona las funciones de dirección empresarial, de los servicios y de la red. Permite la provisión, la supervisión, la recuperación y el análisis del desempeño de extremo a extremo necesarios para dirigir la red (Redes de Próxima Generación NGN, 2015).
- b) Capa de Aplicación y Servicios: aquí se ubican los servidores donde residen y se ejecutan las aplicaciones que ofrecen los servicios a los clientes. No se incluyen en esta capa la estandarización de los servicios o aplicaciones, en cambio, se hace referencia a la provisión de funciones, interfaces y API (OSA/Parlay, Jain) estándar para el acceso de las aplicaciones NGN. Este nivel que se ocupa de la conexión lógica con los usuarios y donde se realiza la mayor parte de la gestión de datos (Redes

de Próxima Generación NGN, 2015).

c) Capa de Control: infraestructura intermedia que permite la comunicación entre los niveles de servicio y de transporte. Aquí se coordinan todos los elementos en las otras dos capas. Se encarga de asegurar el interfuncionamiento de la red de transporte con los servicios y las aplicaciones, mediante la interpretación, la generación, la distribución y la traducción de la señalización correspondiente, con protocolos tales como: H.323, SIP, MGCP, Megaco/H.248. La separación del control y la inteligencia de la red de las funciones de transporte es una característica intrínseca al diseño de la NGN (Redes de Próxima Generación NGN, 2015).

d) Conectividad y Transporte: aquí se ubican las tecnologías de red que se encargan de las tareas de conmutación, enrutamiento y transmisión de los paquetes IP. Esta capa suele dividirse en dos subniveles adicionales: capa de acceso y capa de core o tránsito. La capa de acceso comprende la red de banda ancha que da acceso al usuario a la NGN. Este acceso puede ser fijo, móvil, nomádico, entre otros, utilizando múltiples tecnologías (xDSL 802.11(x), 802.16(x), celular, POTS y TDM para permitir la coexistencia con las redes heredadas) y medios de transmisión. La capa de tránsito o de core permite el enrutamiento y conmutación de los paquetes extremo a extremo. Asegura la interconexión de todas las redes de acceso con los otros niveles. También permite el transporte de diferentes tipos de tráfico con variados requerimiento de QoS (calidad de servicio) (Redes de Próxima Generación NGN, 2015).

Cualquier acceso de banda ancha que sirva para hacer llegar al usuario las aplicaciones que éste solicite: la elección de la tecnología, ya sea en cable (fibra o cobre) o sea inalámbrica, es una cuestión de costos y ha de considerar las infraestructuras existentes, la demanda de ancho de banda del usuario y su grado de movilidad (Redes de Próxima Generación NGN,

2015).

### 2.3. Objetivos, beneficios y retos de las redes de próxima generación

El modelo de referencia NGN puede referenciarse a través de las siguientes características:

- Arquitectura de red horizontal basada en una división diáfana de los planos de transporte, control y aplicación
- El plano de transporte estará basado en tecnología de conmutación de paquetes IP/MPLS
- Interfaces abiertos y protocolos estándares
- Migración de las redes actuales a NGN
- Definición, provisión y acceso a los servicios independiente de la tecnología de la red (*Decoupling Access and Services*)
- Soporte de servicios de diferente naturaleza: *real time/non real time, streaming*, servicios multimedia (voz, video, texto)
- Calidad de servicios garantizada extremo a extremo
- Seguridad
- Las funciones de control están separadas de las capacidades de portador, llamada/sesión y aplicación/servicio
- Desacoplamiento de la provisión del servicio del transporte, y se proveen interfaces abiertas
- Soporte de una amplia gama de servicios, aplicaciones y mecanismos basados en construcción de servicios por bloques (incluidos servicios en tiempo real/de flujo continuo en tiempo no real y multimedia).
- Tendrá capacidades de banda ancha con calidad de servicio (QoS) extremo a extremo
- Tendrá interfuncionamiento con redes tradicionales a través de interfaces abiertas
- Movilidad generalizada
- Acceso sin restricciones de los usuarios a diferentes proveedores de servicios
- Diferentes esquemas de identificación
- Características unificadas para el mismo servicio, como es percibida por el usuario
- Convergencia entre servicios fijos y móviles

- Independencia de las funciones relativas al servicio con respecto a las tecnologías subyacentes de transporte.

La visión original a las redes RPG (NGN) está motivada en gran medida por la convergencia de redes de circuitos y redes de paquetes en una única red NGN multiservicios. Se considera que una red NGN aportará una atractiva serie de beneficios para los proveedores de servicios, entre los que se pueden mencionar:

- Invirtiendo en tecnología NGN *evolucionable* pueden congelarse todas las inversiones ya existentes en tecnología.
- Puede utilizarse NGN para sustituir tecnologías anteriores.
- Las instalaciones de voz basadas en paquetes son más económicas que las instalaciones basadas en otras tecnologías, debido a las ventajas de costo propias del protocolo IP.
- NGN ofrece considerables ahorros de operaciones y explotación, ya que pueden integrarse múltiples redes en una única red de multiservicios. Además, las redes de paquetes son más escalables y fáciles de provisionar.
- NGN ofrece nuevas oportunidades de ingresos gracias a su flexibilidad a la hora de desarrollar e implementar nuevos servicios (Redes de Próxima Generación NGN, 2015).

#### 2.4. El protocolo SIP

El Protocolo de Iniciación de Sesión (SIP) es un protocolo de señalización definido por el *Internet Engineering Task Force* (IETF) que permite el establecimiento, la liberación y la modificación de sesiones multimedia (RFC3261). Este protocolo hereda ciertas funcionalidades de los protocolos *Hyper Text Transport Protocol* (http) utilizados para navegar sobre web y *Simple Mail Transport Protocol* (SMTP) utilizados para transmitir mensajes electrónicos (e-mail). SIP se apoya sobre un modelo transaccional cliente/servidor como http. El direccionamiento

utiliza el concepto *Uniform Resource Locator* (URL SIP) parecido a una dirección e-mail. Cada participante en una red SIP es entonces alcanzable vía una dirección, por medio de una URL SIP. Por otra parte, los requerimientos SIP son satisfechos por respuestas identificadas por un código digital. De hecho, la mayor parte de los códigos de respuesta SIP han sido tomados del protocolo http. Por ejemplo, cuando el destinatario no está ubicado, un código de respuesta «404 Not Found» es devuelto. Un requerimiento SIP está constituido de *headers* o encabezamientos, al igual que un mando SMTP. SIP, al igual de SMTP, es un protocolo textual (Dauphin y Geldwerth, 2015).

SIP ha sido extendido con el fin de soportar numerosos servicios, tales como la presencia, la mensajería instantánea (similar al servicio SMS en las redes móviles), la transferencia de llamada, la conferencia, los servicios complementarios de telefonía, entre otras (Dauphin y Geldwerth, 2015).

SIP ha sido elegido por el 3GPP para la arquitectura *IP Multimedia Subsystem* (IMS) como protocolo para el control de sesión y el control de servicio. El reemplazará en el futuro los protocolos ISUP, utilizado para el control de llamada en la Red Telefónica Conmutada, e INAP utilizado para el control de servicio en la arquitectura Red Inteligente.

El protocolo SIP es sólo un protocolo de señalización. Una vez la sesión establecida, los participantes de la sesión intercambian directamente su tráfico audio/video a través del protocolo *Real-Time Transport Protocol* (RTP). SIP no es un protocolo de reserva de recursos, y en consecuencia, no puede asegurar la calidad de servicio. Se trata de un protocolo de control de llamada y no de control del medio (Dauphin y Geldwerth, 2015).

SIP tampoco es un protocolo de transferencia de fichero, tal como http, usado con el fin de transportar grandes volúmenes de datos. Ha sido concebido para transmitir mensajes de señalización cortos con el fin de establecer, mantener y liberar sesiones multime-

dia. Mensajes cortos, no relativos a una llamada pueden sin embargo ser transportados por SIP al estilo de SMS.

## 2.5. Entidades SIP

SIP define dos tipos de entidades: los clientes y los servidores. De manera más precisa, las entidades definidas por SIP son (vease el gráfico 1):

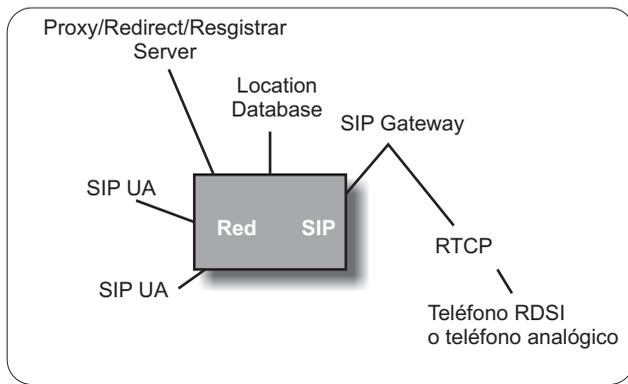


Gráfico 1. Entidades de una red SIP. Fuente: Dauphin y Geldwerth Efort, junio de 2015.

a) Servidor Proxy (Proxy Server): recibe solicitudes de clientes que el mismo trata o encamina hacia otros servidores después de haber eventualmente realizado ciertas modificaciones sobre estas solicitudes.

b) Servidor de Redireccionamiento (Redirect Server): se trata de un servidor que acepta solicitudes SIP, traduce la dirección SIP de destino en una o varias direcciones de red y las devuelve al cliente. De manera contraria al Proxy Server, el Redirect Server no encamina las solicitudes SIP. En el caso de la devolución de una llamada, el Proxy Server tiene la capacidad de traducir el número del destinatario en el mensaje SIP recibido, en un número de reenvío de llamada y encaminar la llamada a este nuevo destino, y eso de manera transparente para el cliente de origen; para el mismo servicio, el Redirect Server devuelve el nuevo número (número de reenvío) al cliente de origen quien se encarga de establecer una llamada hacia este nuevo destino.

c) Agente Usuario (UA): una aplicación sobre un equipo de usuario que emite y recibe solicitudes SIP. Se materializa por un software instalado sobre un User Equipment (UE) : una PC, un teléfono IP o una estación móvil UMTS (Dauphin y Geldwerth, 2015).

d) El Registrador (Registrar): es un servidor que acepta las solicitudes SIP REGISTER. SIP dispone de la función de registro de los usuarios. El usuario indica con un mensaje REGISTER emitido al Registrar, la dirección donde es localizable (dirección IP). El Registrar actualiza entonces una base de datos de localización. El Registrador es una función asociada a un Proxy Server o a un Redirect Server. Un mismo usuario puede registrarse sobre distintas UA SIP, en este caso, la llamada le será entregada sobre el conjunto de estas UA (Dauphin y Geldwerth, 2015).

## 2.6. Métodos y Respuestas SIP

2.6.1. Métodos SIP: el RFC 3261 define seis solicitudes/requerimientos o métodos SIP.

- El método INVITE es usado con el fin de establecer una sesión entre diferentes UA. INVITE corresponde al mensaje ISUP IAM o al mensaje Q.931 SET UP y contiene las informaciones sobre quien genera la llamada y el destinatario, así como sobre el tipo de flujos que serán intercambiados (voz y video) (Dauphin y Geldwerth, 2015).
- Cuando un UA que emitió el método SIP INVITE recibe una respuesta final a la invitación (ejemplo: 200 OK), él confirma la recepción de esta respuesta por medio de un método ACK. Una respuesta del tipo *busy* o *answer* es considerada como final, mientras una respuesta tipo *ringing* significa que el destinatario ha sido avisado: es una respuesta provisoria (Dauphin y Geldwerth, 2015).
- El método BYE permite la liberación de una sesión anteriormente establecida. Corresponde al mensaje RELEASE de los protocolos ISUP y Q.931. Un mensaje BYE puede ser emitido por

- el que genera la llamada o el que la recibe.
- El método REGISTER es usado por una UA con el fin de indicar al Registrar la correspondencia entre su Dirección SIP y su dirección de contacto (ejemplo: dirección IP).
- El método CANCEL es utilizado para pedir el abandono de la llamada en curso, pero no tiene ningún efecto sobre una llamada ya aceptada. De hecho, sólo el método BYE puede terminar una llamada establecida.
- El método OPTIONS es utilizado para interrogar las capacidades y el estado de un User Agent o de un servidor. La respuesta contiene sus capacidades (ejemplo: tipo de media siendo soportado, idioma soportado) o el hecho de que el UA sea indisponible (Dauphin y Geldwerth, 2015).

2.6.2. *Respuestas SIP*: después de haber recibido e interpretado un requerimiento SIP, el destinatario de este requerimiento devuelve una respuesta SIP. Existen seis clases de respuestas:

- Clase 1xx : Información; el requerimiento ha sido recibido y está en curso de tratamiento
- Clase 2xx: Éxito; el requerimiento ha sido recibido, entendido y aceptado.
- Clase 3xx: Re-enrutamiento; la llamada requiere otros procesamientos antes de poder determinar si puede ser realizada.
- Clase 4xx: Error requerimiento cliente; el requerimiento no puede ser interpretado o servido por el servidor. El requerimiento tiene que ser modificado antes de ser reenviado.
- Clase 5xx: Error servidor; el servidor fracasa en el procesamiento de un requerimiento aparentemente válido.
- Clase 6xx: Fracaso global; el requerimiento no puede ser procesado por ningún servidor (Dauphin y Geldwerth, 2015).

#### 4. MÉTODO

En esta sección se muestra la configuración implementada en el laboratorio de antenas de la Fundación

Universidad Autónoma de Colombia, y la configuración ya existente en el laboratorio de Redes Avanzadas ANKLA de CINTEL para la elaboración del proyecto.

En el gráfico 2 se observa el diagrama básico de la interconexión entre la Red NGN ANKLA y el laboratorio de telemática de la Universidad Autónoma de Colombia.

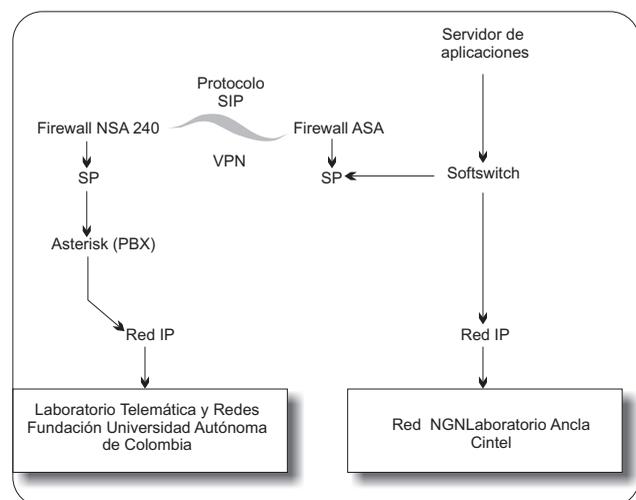


Gráfico 2. Arquitectura básica de interconexión redes NGN.

Para lograr la interconexión de las dos redes entre el laboratorio del Ankla y el laboratorio de la Fundación Universidad Autónoma de Colombia se tuvo en cuenta el uso de un Cortafuegos (Firewall). Un Cortafuego es la parte de un sistema o una red diseñada para bloquear el acceso no autorizado, permitiendo al mismo tiempo comunicaciones autorizadas. Se trata de un dispositivo o conjunto de dispositivos configurados para permitir, limitar, cifrar, descifrar, el tráfico entre los diferentes ámbitos sobre la base de un conjunto de normas y otros criterios. En el gráfico 3 se muestra el diagrama básico de interconexión.

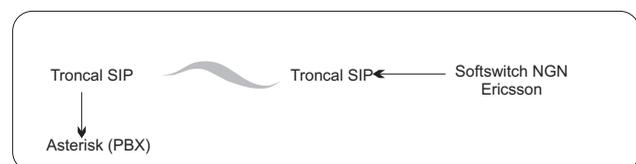


Gráfico 3. Infraestructura básica de Interconexión

### 3. RESULTADOS

En este apartado se documentan las implementaciones realizadas para poder llevar a cabo el proyecto. Principalmente se usó WireShark, un analizador de protocolos utilizado para realizar análisis y solucionar problemas en redes de comunicaciones, para desarrollo de software y protocolos, y como una herramienta didáctica. Cuenta con todas las características estándar de un analizador de protocolos. Se usó para analizar los paquetes de protocolo SIP al implementar la interconexión de los dos laboratorios. El análisis del protocolo SIP se realizó para poder visualizar el encabezado de la señalización SIP y verificar que no hubiera errores en la implementación de la interconexión. Se implementó una solución de VPN para lograr la interconexión entre los dos laboratorios permitiendo cumplir con los objetivos propuestos

#### 3.1. Análisis del protocolo sip

*3.1.1. Análisis del protocolo SIP:* se realizó mediante el analizador de protocolos para poder visualizar el encabezado de la señalización SIP y verificar que no hubiera errores en la implementación de la interconexión.

*3.1.2. Análisis del protocolo sip ankla:* se realizó un análisis de la trama de señalización SIP de la red NGN con arquitectura Softswitch/MGC. En el gráfico 4 se muestra un diagrama de comunicación básica del protocolo SIP de la red NGN de Ankla.

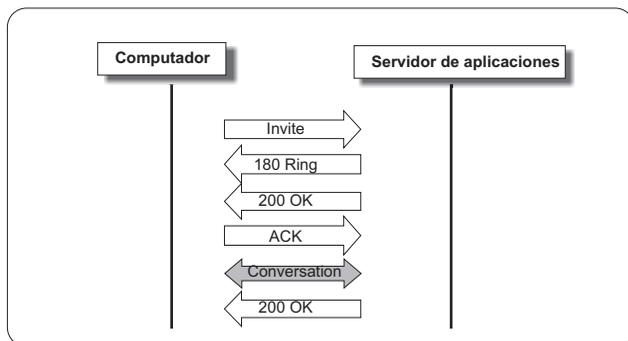


Gráfico 4. Comunicación básica del protocolo SIP de la red NGN ANKLA

*3.1.3. Análisis del protocolo sip de la Fundación Universidad Autónoma de Colombia:* para el análisis del protocolo SIP de la FUAC se utilizó la misma herramienta (analizador de protocolos) permitiendo ver en aspectos generales que el análisis es el mismo ya que se usaron las mismas versiones de Plataforma de comunicaciones unificadas (Elastix).

#### 3.2. Interconexión entre los laboratorios

La interconexión que se realizó entre los laboratorios de telemática y redes de la Fundación Universidad Autónoma de Colombia y el laboratorio ANKLA de Cintel, se hizo por medio de una Red Privada Virtual (VPN).

Ésta es una tecnología de red que permite una extensión segura de la red local (LAN) sobre una red pública o no controlada como Internet. Permite que la computadora en la red envíe y reciba datos sobre redes compartidas o públicas, como si fuera una red privada, con toda la funcionalidad, la seguridad y las políticas de gestión de una red privada. Esto se realiza estableciendo una conexión virtual punto a punto mediante el uso de conexiones dedicadas, cifrado o la combinación de ambos métodos (Quarea, 2014).

Para realizar las pruebas de interconexión se usó una VPN punto a punto que permite el intercambio de toda la señalización SIP además de multimedia.

El servidor VPN, que posee un vínculo permanente a Internet, acepta las conexiones vía Internet provenientes de los sitios y establece el túnel VPN. Los clientes se conectan a Internet utilizando los servicios de su proveedor local de internet, típicamente mediante conexiones de banda ancha. Esto permite eliminar los costosos vínculos punto a punto tradicionales (realizados comúnmente mediante conexiones de cable físicas entre los nodos), sobre todo en las comunicaciones internacionales.

Es más común el siguiente punto, también llamado tecnología de túnel o *tunneling* (Quarea, 2014). A partir de las pruebas obtenidas mediante el desarrollo

de la misma se pudo garantizar la interoperabilidad entre los dos laboratorios, ya que ambos cuentan con una versión de comunicaciones de plataformas unificadas (Elastix) y esto permite que la compatibilidad sea total. Con el analizador de protocolos se puede observar mediante las capturas realizadas en las pruebas las estadísticas en las llamadas que éstas generan, permitiendo ver entre otros aspectos los diferentes mensajes de estado y los errores por ejemplo en la imagen se ve el caso de un error de tipo cliente 405 *Method Not Allowed* (Método no permitido) donde un Softphone se ha configurado de forma errónea, o se recibe una respuesta 401 *Unauthorized* donde se ha configurado de manera errónea la extensión del softphone. De esta manera las estadísticas muestran todos los parámetros que garantizan una correcta conexión entre las centrales.

SIP stats (120 packets) 13 resent packets	
Informational SIP 1xx	
SIP 180 Ringing	6
SIP 100 trying	4
Success SIP 2xx	
SIP 200 OK	29
Redirection SIP 3xx	
Clients errors 4xx	
SIP 401 Unauthorized	4
SIP 405 Method not allowed	18
Server errors 5xx	
Global failures 6xx	
List of request methods	
Invite	7 packets
ACK	7 packets
Options	35 packets
Register	2 packets
Notify	4 packets
Bye	4 packets
Average setup time 11155 ms. Min. 14 ms. Max 21408 ms	

Tabla 1. Estadísticas llamadas SIP

## 6. CONCLUSIONES

Una vez terminado el desarrollo del proyecto de interconexión entre el laboratorio de Telemática de la Fundación Universidad Autónoma de Colombia y la red NGN de CINTEL, se logró establecer la conexión cumpliendo, entre otros, con el objetivo general y los objetivos específicos trazados en el proyecto.

El medio de comunicación utilizado finalmente fue

una VPN mediante el software OpenVPN, software GNU de código abierto basado en Linux; éste permitió crear un túnel de información totalmente cifrado entre el laboratorio de Telemática de la Fundación Universidad Autónoma de Colombia y el laboratorio ANKLA.

Al tener una VPN funcional y segura entre los dos laboratorios, se realizó la conexión SIP entre éstos por medio de la troncal SIP: ésta es una conexión en la que las dos plantas IP pueden intercambiar información mediante el protocolo SIP, y para este caso funciona únicamente sobre la VPN, pues ésta hace que cada laboratorio sea una extensión de red de la otra y los equipos se comuniquen perfectamente.

## REFERENCIAS

- ALZOLA, O. y RAMÍREZ, D. (2008). *Telefonía IP*. Universidad Técnica Federico Santamaría.
- BULLA, B. et al. (2012). *Instalación de un sistema VoIP corporativo basado en Asterisk*. Revista visión electrónica año 6 julio-diciembre de 2012
- CAMBRIDGE UNIVERSITY PRESS (2013). *Cambridge Dictionary Online*. Disponible en: <http://dictionary.cambridge.org>.
- CISCO SYSTEM (2013) *VLANs*. Disponible en: [www.cisco.com](http://www.cisco.com).
- DADAJI S., G. y CHANDAVARKAR, B. R. (s.f). *Security Analysis of Session Initiation Protocol in IPv4 and IPv6 based VoIP network*. Computer Science & Engineering Dept. NITK Surathkal, Mangalore, India.
- DAUPHIN, J. L. y GELDWERTH, R. (2015). *Session Initiation Protocol Simon ZNATY*. Etudes et Formations en Télécommunication. Disponible en: [www.eport.com/media\\_pdf/SIP\\_ESP.pdf](http://www.eport.com/media_pdf/SIP_ESP.pdf).
- DÍAS, M. C. et al. (2014). *Using Asterisk as a Tool for Teaching VoIP for Information Technology Classes*. Telecommunications Symposium (ITS).
- HADI, M. Z. S. (2011). *Network Security*. Disponible en: <http://lecturer.eepis-its.edu/>
- HANIFAN, Y. y BANDUNG, Y. (2010). *Designing VoIP security system for Organizational Network*. School of Electrical Engineering and Informatics, Institut Teknologi Bandung, Bandung, Indonesia.
- IETF (s.f). *Internet Engineering Task Force. RFC 3261*. SIP: Session Initiation Protocol. Disponible en: <http://www.ietf.org/rfc/rfc3261.txt>.
- ITU (2006). *Unión Internacional de Telecomunicaciones – T. Principios para la gestión de redes de próxima generación*. Ginebra: Suiza.

- ITU (s.f.). *International Telecommunication Union*. Committed to connecting the world. [Online]. <http://www.itu.int/en/ITU-T/gsi/ngn/Pages/release1.aspx>
- KLANJŠEK, J. (2010). *An educational multimedia IP telephony platform*. Digital and Information Systems Laboratory Faculty of electrical engineering and computer science, Maribor, Slovenia
- QADEER, M. e IMRAN, A. (2008). *Asterisk Voice Exchange- An alternative to conventional EPBX in Proc. IEEE ICCEE*.
- QUAREA (2014) *Telefonía IP*. Disponible en: [http://www.quarea.com/es/que\\_es\\_telefonia\\_ip](http://www.quarea.com/es/que_es_telefonia_ip).
- RED PRIVADA VIRTUAL (2015). Disponible en: [https://es.wikipedia.org/wiki/Red\\_privada\\_virtual](https://es.wikipedia.org/wiki/Red_privada_virtual).
- REDES DE PRÓXIMA GENERACIÓN NGN (2015). Disponible en: [elendill.wordpress.com/tag/mps/](http://elendill.wordpress.com/tag/mps/)
- RODRÍGUEZ, A. S. (2008). *Metodología de diseño e implementación de soluciones VoIP*. UPC.
- SAI (2014). *Proyecto de implantación de la telefonía IP en los centros educativos*. Disponible en: <http://sai.edu.gva.es/?q=es/node/246>
- SILVA, M. y VIANA, D. (2013). *Variáveis operacionais a serem consideradas no planejamento de disciplinas de projeto para aplicação do PBL nos cursos de engenharia*. In: Proceedings of the 41st COBENGE, Gramado.
- TICAL (2013). *Redes Académicas de VoIP Latinoamericanas frente al desafío de las nuevas tecnologías TICAL*. Cartagena. Colombia. Disponible en: [http://tical\\_2013.redclara.net/doc/Presentaciones/03Aversa\\_Fernando.pdf](http://tical_2013.redclara.net/doc/Presentaciones/03Aversa_Fernando.pdf) Internetworking telephony, IP and ATM networks Veeraraghavan.
- UIT (2015). *Informe esencial sobre telefonía por el protocolo Internet (IP)*. Grupo de Expertos sobre Telefonía IP del UIT-D. UIT (Unión Internacional de Telecomunicaciones). Disponible en: [www.itu.int/dms\\_pub/itu-d/opb/hdb/D-HDB-IPT-2004-R1-PDF-S.pdf](http://www.itu.int/dms_pub/itu-d/opb/hdb/D-HDB-IPT-2004-R1-PDF-S.pdf).
- VSA (2013). *The Voice over IP Security Alliance, security tools*. Disponible en: [www.voipsa.org/Resourcs](http://www.voipsa.org/Resourcs) 2013.
- ZEYAD, A. y SAMAKA, M., (2013). *ePBL: Design and Implementation of a Problem Based Learning Environment*. In: Proceedings of the IEEE Global Engineering Education Conference (EDUCON). Berlín: Germany.