

ANÁLISIS DE RENDIMIENTO DE LOS PROTOCOLOS DE SEÑALIZACIÓN VOIP SIP E IAX EN UN ENTORNO DE RED DUAL STACK

PERFORMANCE ANALYSIS OF SIP AND IAX VOIP SIGNALING PROTOCOLS IN A DUAL STACK ENVIROMENT NETWORK



AUTOR

FLORENTINO MÉNDEZ GIJÓN
Magister en Ingeniería en
Tecnologías de la Información
*Universidad de la Sierra Juárez
Profesor Investigador
Licenciatura en Informática
fmendez@juppa.unsij.edu.mx
MÉXICO

AUTOR

JOSÉ GUILLERMO VALDEZ BESARES
Magister en Ciencias
Computacionales
*Universidad de la Sierra Juárez
Profesor Investigador
Licenciatura en Informática
jvaldez@juppa.unsij.edu.mx
MÉXICO

AUTOR

DAVID LÓPEZ BAUTISTA
Estudiante Universitario
*Universidad de la Sierra Juárez
Alumno
Licenciatura en Informática
lopez_65b@hotmail.com
MÉXICO

*INSTITUCIÓN

Universidad de la Sierra Juárez
UNSIJ
Campus, Ixtlán de Juárez, Oaxaca
Av. Universidad S/N, Ixtlán de Juárez,
Oaxaca.
jefaturas@juppa.unsij.edu.mx
MÉXICO

INFORMACIÓN DE LA INVESTIGACIÓN O DEL PROYECTO: El presente artículo surge como resultado de la investigación sobre Tecnologías de Información y Comunicaciones que se realiza al interior del cuerpo académico de la Licenciatura en Informática de la Universidad de la Sierra Juárez.

RECEPCIÓN: Julio 4 de 2013

ACEPTACIÓN: Diciembre 2 de 2013

TEMÁTICA: Ingeniería Eléctrica, Electrónica, Telecomunicaciones y Telemática

TIPO DE ARTÍCULO: Artículo de Investigación Científica e Innovación

Forma de citar: Méndez Gijón, F., Valdez Besares, J. G., & López Bautista, D. (2014). Análisis de rendimiento de los protocolos de señalización VOIP SIP e IAX en un entorno de red DUAL STACK. En R, Llamosa Villalba (Ed.). Revista Gerencia Tecnológica Informática, 13(35), 47-61. ISSN 1657-8236.

RESUMEN ANALÍTICO

Las comunicaciones de VoIP basan su funcionamiento a nivel de señalización en tres protocolos estandarizados H.323, SIP e IAX, el enrutamiento de paquetes se logra a través del protocolo IP que en la actualidad existe en dos versiones IPv4 e IPv6, por lo que en este artículo se describe la implementación de los protocolos SIP e IAX en un entorno de red DualStack, con la finalidad de capturar los paquetes y después realizar el análisis de los parámetros que afectan las comunicaciones VoIP y con los resultados obtenidos del análisis de rendimiento y funcionalidad IPsec se pretende demostrar la funcionalidad de los protocolos de señalización VoIP en ambas versiones del protocolo IP.

Finalmente también probar que es posible implementar sistemas de telefonía IP haciendo uso de herramientas de Software Libre como Asterisk, que ya tiene soporte para ambas versiones del protocolo IP y de herramientas de software con iguales características funcionales que los teléfonos fijos, lo que beneficia en el ahorro de costos económicos en Innovación Tecnológica para pequeñas y grandes organizaciones.

Las pruebas se realizaron con dos servidores VoIP con un conjunto de extensiones, dos enlaces troncales y un analizador de tráfico que permite capturar los paquetes VoIP para su posterior análisis, en cada servidor se habilitó una extensión para realizar llamadas entre ellos.

PALABRAS CLAVES: VoIP, IPv6, IPv4, Protocolo, SIP, IAX, RTP, H.323.

ANALYTICAL SUMMARY

VoIP communications base their function at a level of signalization in three standard protocols: H.323, SIP and IAX, and the routing of packets is achieved through the protocol IP that currently exists in two versions IPv4 and IPv6. With respect to this article, the implementation of the protocols SIP and IAX in a range of the Dual Stack network, in order to realize the analysis of the parameters that affect the VoIP communications. The results obtained from the analysis of the performance and IPsec functionality is expected to demonstrate the functionality of the signalization protocols of VoIP in both versions of the protocol IP.

Lastly, it will also be demonstrated that it is possible to implement systems of IP telephony by using the tools of Free Software, like Asterisk that already supports both versions of the protocol IP, besides the fact that there exist software tools with the same functional characteristics of landlines, which benefits small and large organizations in saving on economic costs of Technological Innovation.

Tests were performed with two VoIP servers with a set of extensions, two core links, and a traffic analyzer that make it possible to capture the VoIP packets for their subsequent analysis, on each server extension was enabled to make calls between them.

KEYWORDS: VoIP, IPv6, IPv4, Protocol, SIP, IAX, RTP, H.323.

INTRODUCCIÓN.

En los modelos de la tecnología VoIP, los protocolos estandarizados SIP, IAX, H.323 se encargan de la señalización y a través de RTP y RTCP se realiza la transferencia de media y señalización de control, para lo que se utilizan puertos UDP y TCP que son empaquetados con el protocolo IP que actualmente

opera en dos versiones IPv4 e IPv6, esta característica del protocolo IP permite implementar entornos Dual Stack donde conviven las dos versiones.

En este estudio se lleva a cabo la implementación de los protocolos SIP e IAX en un entorno de red Dual Stack (IPv4 e IPv6) con la finalidad de medir parámetros como: tiempo de transmisión, número de paquetes transmitidos,

Retardo y Jitter generado, ya que son factores que afectan de manera directa la calidad del servicio de voz, así como probar la funcionalidad de IPSec en el cifrado de los paquetes de voz al intentar escuchar las conversaciones realizadas entre dos extensiones, sin embargo no se aborda la implementación de este protocolo de seguridad; en trabajos previos se han realizado pruebas sobre túneles para comparar el rendimiento de IPv6 con respecto a IPv4 sin enfocarse en un servicio en particular, en este trabajo se implementa el servicio de VoIP sin utilizar túneles, haciendo pruebas sobre un entorno operativo común.

En [1, 10, 11, 12], se realizan análisis sobre rutas punto a punto nativas IPv6 y túneles en redes como RIPE y CERNET usando herramientas como Traceroute con MTU Discovery y Ping para medir el Retardo, rendimiento y RTT. En la mayor parte de resultados se observa que las rutas IPv6 tienen un rendimiento inferior con respecto a IPv4, se menciona que puede deberse a la mala configuración y saturación de las rutas o túneles.

En [7] se hace una evaluación sobre dos sistemas operativos clientes configurados con ambas versiones del protocolo IP, para medir de forma empírica la diferencia en el rendimiento relacionado a throughput, Retardo, Jitter y uso de CPU. Se determina que el rendimiento no depende solamente de la versión del protocolo IP y el tipo de tráfico, influye también el sistema operativo empleado.

En [3] desde la perspectiva de un usuario final se implementa una metodología de medición activa para valorar el rendimiento de IPv6 frente a IPv4, se mide el tráfico ICMP y TCP, concluyendo que el throughput de IPv6 es superior al alcanzado con IPv4.

1. FUNDAMENTOS TEÓRICOS.

1.1 DIRECCIONAMIENTO IP.

IP es un protocolo del nivel de red capa 3 del modelo de referencia OSI, o del nivel de capa 2 del modelo TCP/IP. En una comunicación el protocolo IP se encarga del transporte de paquetes desde el origen hasta el destino. Es un protocolo de mejor esfuerzo no orientado a conexión, lo que significa que no garantiza la fiabilidad en la entrega de los paquetes por lo que hace uso de otros protocolos para poder garantizar que todos los paquetes lleguen al destino indicado en su cabecera.

El estándar IPv4 es la primera versión del protocolo IP, fue desarrollado en la década de los 70's, su arquitectura se describe en el RFC 791. Una dirección IPv4 está compuesta por un grupo de 32 bits representados en 4 octetos o bloques de 8 bits de la siguiente

forma: X.X.X.X, donde cada X es un número decimal comprendido entre 0 y 255, que justamente son todos los números decimales representables con 8 bits.

Con el esquema de direccionamiento IPv4 se pueden direccionar teóricamente un máximo de 2^{32} dispositivos de forma simultánea.

En la versión 6 del protocolo IP se incrementa el tamaño de dirección de 32 bits a 128 bits, para dar soporte a mas niveles de direccionamiento jerárquico e incrementar hasta 2^{128} el número de nodos direccionables.

Las direcciones IPv6 son identificadores de 128 bits de longitud divididos en grupos de 16 bits con el formato X:X:X:X:X:X:X, donde cada X es un grupo de 4 dígitos hexadecimales e identifican interfaces de red, para señalar las secciones que identifican a la red y al host se utiliza el formato CIDR (Classless Inter-Domain Routing) en la forma: <dirección>/<prefijo>, donde prefijo es un número en formato decimal.

La arquitectura de direccionamiento IPv6 se define en el RFC 3513 en donde se especifican la representación textual, los tipos de direcciones y las direcciones requeridas por los nodos.

El protocolo IPv6 agrega algunas otras funcionalidades respecto a IPv4, como son encriptación de datos, autoconfiguración, calidad de servicio, enrutamiento jerárquico y seguridad basada en el protocolo IPSec.

1.2 PROTOCOLOS VOIP.

A nivel de capa de transporte el protocolo UDP es el que permite transporte de información en tiempo real, pero debido a que presenta algunos inconvenientes para el transporte de media se complementa con los protocolos conocidos como RTP o protocolos de transporte en tiempo real, tres de estos protocolos RTP, RTCP y RTSP están definidos en los RFC3550, RFC3551 y RFC3711, respectivamente.

A nivel de sesión y para señalización los protocolos H.323, SIP y IAX son estandarizados por la IETF y por la ITU-T, por lo que ésta investigación versará sobre dos de estos protocolos que son los más utilizados: SIP e IAX.

El protocolo SIP es un protocolo de señalización extremo a extremo a nivel de aplicación, lo cual implica que toda la lógica y estado de conexión son almacenados en los dispositivos finales, que le da una gran capacidad de distribución a costo de una sobrecarga en la cabecera de los mensajes, producto de mandar toda la información entre los dispositivos finales. SIP trabaja en la creación, modificación, y finalización de sesiones que incluyen

llamadas telefónicas de Internet, tráfico multimedia, mensajería instantánea, conferencias multimedia y mensajería inmediata, que es transportada dentro de los protocolos RTP/RTCP y SDP con uno o varios participantes, basándose en mensajes de petición y respuesta. Reutiliza muchos conceptos de estándares de protocolos como el protocolo de transferencia de hipertexto HTTP y el protocolo simple de transferencia de correo SMTP.

El protocolo IAX se encuentra en su segunda versión y está definido en el RFC-5456, intenta resolver una serie de problemas e inconvenientes que presenta SIP, permite manejar una gran cantidad de códecs y un gran número de streams que lo hace muy útil para realizar videoconferencias o realizar presentaciones remotas, utiliza un único puerto por default el 4569. El tráfico de voz es transmitido in – band, lo que permite que IAX2 sea un protocolo transparente a los firewalls, hace uso de un mecanismo denominado Trunking que permite enviar varias sesiones en un único flujo de datos, optimizando el uso del canal de comunicaciones, debido a ésta característica se puede utilizar cuando se requieren enlazar dos servidores donde exista un tráfico fuerte de VoIP.

El protocolo IAX, aún no cuenta con el soporte suficiente en la implementación de teléfonos fijos y existen un reducido número de Softphones que lo soportan, por lo que su mayor uso se encuentra en enlazar centrales telefónicas debido a que es un protocolo punto a punto que multiplexa la señalización y flujos múltiples de media en un único puerto UDP entre dos host.

1.3 CODECS VOIP.

Cuando se establece una comunicación de voz entre dos usuarios remotos mediante VoIP, la señal que cada uno emite es analógica, por lo que se requiere digitalizar, comprimir y codificarla antes de ser transmitida por la red IP, para ello se utilizan algoritmos matemáticos implementados en software más comúnmente conocidos como CODECS. Dependiendo del tipo de códec elegido variará también la calidad de la voz, el ancho de banda necesario y la carga computacional.

Algunos de los códecs más utilizados y estandarizados por la ITU son el G.711 y el G.729 en menor grado se encuentran los códecs G.723 y el G.726.

La elección de que códec utilizar depende de las necesidades de cada entorno y está directamente relacionado con el costo computacional, uso de ancho de banda y soporte en los dispositivos finales, ya que estos parámetros influyen también en la calidad de la comunicación VoIP.

1.4 FACTORES NEGATIVOS INHERENTES EN UNA COMUNICACIÓN VOIP.

En una transferencia de paquetes VoIP existen al menos cuatro factores que afectan la calidad de la comunicación que son: el Retardo, Jitter, eco y pérdida de paquetes, mismos que se analizan en este trabajo para comparar la funcionalidad de los protocolos de señalización SIP e IAX en un entorno de red Dual Stack.

El Retardo es causado por distintas fuentes tales como el tipo de códec utilizado, los medios utilizados para transmitir los datos y el entorno de red, según el documento G.114 de la ITU-T el Retardo máximo permisible en una comunicación extremo a extremo en una llamada de voz debe ser menor a 150 ms.

El Jitter se define como la variación del tiempo de llegada de los paquetes causado por diversos factores de la red, para tratar de reducir este fenómeno se implementa un mecanismo denominado buffer – Jitter y su diseño se basa en contar los paquetes que tengan Retardo para crear una relación entre éstos paquetes y el número de paquetes que si fueron procesados correctamente.

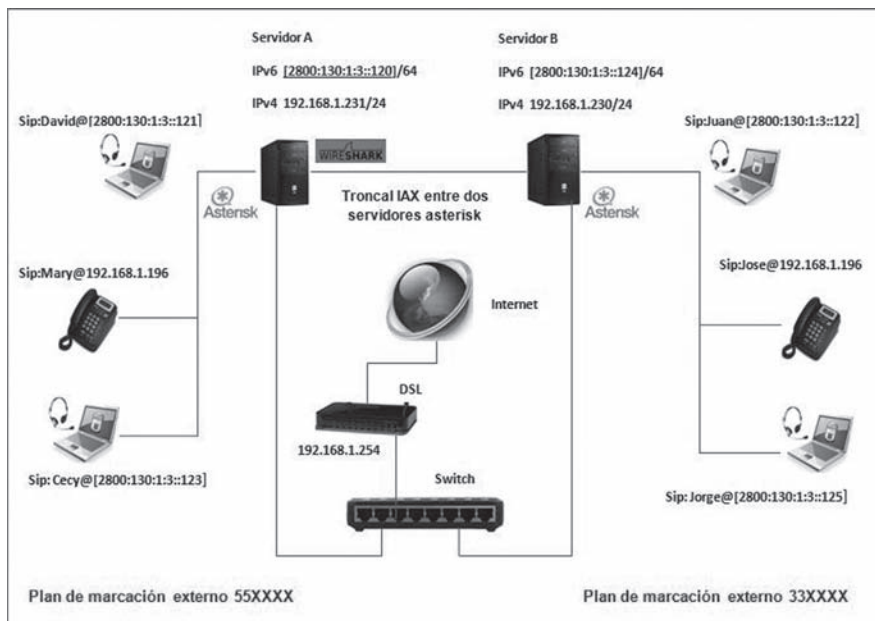
El eco por su parte se origina por la conversión de 2 a 4 hilos de los sistemas telefónicos o por un retorno de señal que se escucha por los altavoces y se transmite de nuevo por el micrófono, para resolver ésta problemática se implementan dispositivos supresores y de cancelación de eco.

2. PRUEBAS.

La implementación se realiza en un entorno de pruebas implementado con Asterisk, instalado en un sistema operativo Linux en la distribución Centos y para el monitoreo de tráfico se utiliza Wireshark, un Sniffer de distribución libre que se utiliza para captura de tráfico, en este caso flujos de paquetes RTP, con la finalidad de poder realizar la comparación de los parámetros que impactan una comunicación VoIP en un entorno de red Dual Stack.

El escenario de pruebas que se implementó se muestra en la figura 1, en el que se simularon dos entidades remotas representados cada una por un servidor Asterisk, que se instalaron sobre dos PC con sistema operativo Centos, y donde cada servidor tiene su grupo de extensiones SIP internas, que permitieron establecer comunicación entre ellos mediante un enlace troncal con el protocolo IAX, utilizando el plan de marcado que se especifica en la figura 2.

FIGURA 1. Entorno de pruebas.



Se realizó la configuración Dual Stack donde se utilizó una red privada clase C para IPv4 y una red de enlace global para IPv6 de la siguiente forma: 192.68.1.0/24 y 2800:130:1:/64 respectivamente, esto con la finalidad de realizar las pruebas de transmisión VoIP en las versiones IPv4 e IPv6 del protocolo IP y poder hacer el análisis de ciertos parámetros como son: uso

de ancho de banda, Jitter y Retardo en un entorno Dual Stack.

El análisis de tráfico se realizó con el software Wireshark que permitió capturar los flujos de tráfico de VoIP, este se implementó en uno de los servidores que fungió como entidad, para facilitar la captura de paquetes.

FIGURA 2. Plan de marcación.

SERVIDOR A	SERVIDOR B
<p>Nombre del contexto</p> <p>[Teléfonos]</p> <p>Incluir contexto para extensiones internas</p> <p>include->llamadas_internas</p> <p>Incluir contexto para extensiones externas</p> <p>include->llamadas_externas</p> <p>Definición del contexto para llamadas internas</p> <p>[llamadas_internas]</p> <p>Llamadas entre extensiones SIP</p> <p>exten->1001,1,Dial(SIP/David,30,tTr)</p> <p>exten->1002,1,Dial(SIP/Mary,30,tTr)</p> <p>Llamadas entre extensiones IAX</p> <p>exten->1003,1,Dial(IAX2/Cecy,30tTr)</p> <p>Definición del contexto para llamadas externas</p> <p>[llamadas_externas]</p> <p>Llamadas externas entre extensiones IAX</p> <p>exten->_55XXXX,1,NoOp(Llamadas al servidor B)</p> <p>exten->_55XXXX,2,Dial(IAX2/asteriskb/\${EXTEN:2},30,tTr)</p> <p>exten->_55XXXX,3,Hangup()</p> <p>Llamadas externas entre extensiones SIP</p> <p>exten->_55XXXX,1,NoOp(Llamadas al servidor B)</p> <p>exten->_55XXXX,2,Dial(SIP/asteriskb/\${EXTEN:2},30,tTr)</p> <p>exten->_55XXXX,3,Hangup()</p>	<p>Nombre del contexto</p> <p>[Teléfonos]</p> <p>Incluir contexto para extensiones internas</p> <p>include->llamadas_internas</p> <p>Incluir contexto para extensiones externas</p> <p>include->llamadas_externas</p> <p>Definición del contexto para llamadas internas</p> <p>[llamadas_internas]</p> <p>Llamadas entre extensiones SIP</p> <p>exten->2001,1,Dial(SIP/Juan,30,tTr)</p> <p>exten->2002,1,Dial(SIP/Jose,30,tTr)</p> <p>Llamadas entre extensiones IAX</p> <p>exten->2003,1,Dial(IAX2/Jorge,30tTr)</p> <p>Definición del contexto para llamadas externas</p> <p>[llamadas_externas]</p> <p>Llamadas externas entre extensiones IAX</p> <p>exten->_33XXXX,1,NoOp(Llamadas al servidor A)</p> <p>exten->_33XXXX,2,Dial(IAX2/asteriska/\${EXTEN:2},30,tTr)</p> <p>exten->_33XXXX,3,Hangup()</p> <p>Llamadas externas entre extensiones SIP</p> <p>exten->_33XXXX,1,NoOp(Llamadas al servidor A)</p> <p>exten->_33XXXX,2,Dial(SIP/asteriska/\${EXTEN:2},30,tTr)</p> <p>exten->_33XXXX,3,Hangup()</p>

2.1 ENLACE TRONCAL IAX.

Un enlace o troncal IAX como se conoce comúnmente, se utiliza para establecer llamadas entre extensiones de diferentes servidores, con el fin de aprovechar al máximo el ancho de banda, puesto que con el protocolo

IAX se utiliza solamente un puerto para enrutar múltiples llamadas de manera simultánea.

En la figura 3 se muestra la configuración del enlace troncal IAX entre las centrales A y B.

FIGURA 3. Configuración del enlace troncal IAX.

SERVIDOR A	SERVIDOR B
<pre>register=>asteriska:1234@192.168.1.230 [asteriskb] type=friend username=asteriska host=dynamic secret=1234 auth=plaintext context=Téfonos deny=0.0.0.0/0.0.0.0 permit=192.168.1.0/255.255.255.0 trunk=yes qualify=yes requirecalltoken=no</pre>	<pre>register=>asteriskb:1234@192.168.1.231 [asteriska] type=friend username=asteriskb host=dynamic secret=1234 auth=plaintext context=Téfonos deny=0.0.0.0/0.0.0.0 permit=192.168.1.0/255.255.255.0 trunk=yes qualify=yes requirecalltoken=no</pre>

2.2 REGITRO DE LAS EXTENSIONES SIP E IAX.

En las figuras 4 y figura 5 se muestra el proceso de registro de las extensiones SIP e IAX en ambas centrales A y B.

FIGURA 4. Extensiones y Troncal IAX registrados en el servidor A.

```
[root@asteriska ~]# asterisk -r
Verbosity is at least 3
asteriska*CLI> sip show peers
Name/username      Host                               Dyn Forcerpor
t ACL Port      Status
David/David        2800:130:1:3::121                 D           5
060      Unmonitored
Mary/Mary          192.168.1.196                     D           5
060      Unmonitored
2 sip peers [Monitored: 0 online, 0 offline Unmonitored: 2 online, 0 offline]
asteriska*CLI> iax2 show registry
Host                dnsmgr Username      Perceived      Refresh State
192.168.1.230:4569 N      asteriska     192.168.1.231:4569 60  Register
red
1 IAX2 registrations.
asteriska*CLI> iax2 show peers
Name/Username      Host                               Mask          Port          Status
Cecy              (null)                            (D) 255.255.255.255 0      Unmonitored
asteriskb/aster   192.168.1.230 (D) 255.255.255.255 4569 (T) OK (3 ms)
2 iax2 peers [1 online, 0 offline, 1 unmonitored]
asteriska*CLI>
```

FIGURA 5. Extensiones y Troncal IAX registrados en el servidor B.

```
[root@asteriskb ~]# asterisk -rvvv
Verbosity is at least 3
-- Remote UNIX connection
asteriskb*CLI> sip show peers
Name/username      Host
t ACL Port      Status
Jose/Jose          192.168.1.196      D      5
061 Unmonitored
Juan/Juan          2800:130:1:3::122 D      5
060 Unmonitored
2 sip peers [Monitored: 0 online, 0 offline Unmonitored: 2 online, 0 offline]
asteriskb*CLI> iax2 show registry
Host      dnsmgr Username Perceived Refresh State
192.168.1.231:4569 N asteriskb 192.168.1.230:4569 60 Registered
1 IAX2 registrations.
asteriskb*CLI> iax2 show peers
Name/Username      Host      Mask      Port      Status
Jorge              192.168.1.240 (D) 255.255.255.255 4569 Unmonitored
asteriska/aster 192.168.1.231 (D) 255.255.255.255 4569 (T) OK (3 ms)
2 iax2 peers [1 online, 0 offline, 1 unmonitored]
asteriskb*CLI> █
```

2.3 CAPTURA DE TRÁFICO VOIP.

El proceso de captura de paquetes RTP con Wireshark se llevó a cabo en un entorno de red Dual Stack, realizando llamadas entre las extensiones SIP registradas en un mismo servidor y haciendo uso del enlace IAX para extensiones registradas en un servidor diferente.

Se realizaron 20 llamadas, de las que 10 fueron utilizando el protocolo IPv4 y 10 llamadas con el protocolo IPv6, obteniendo para ambas la misma cantidad de paquetes capturados.

2.4 LLAMADAS ENTRE EXTENSIONES IPV6.

Primeramente se realizaron llamadas entre extensiones con direccionamiento IPv6 resultando todas las llamadas exitosas, en la figura 6 se muestra la sesión establecida entre dos extensiones IPv6 y en la figura 7 podemos observar algunos parámetros que describen de manera más detallada el flujo RTP de los paquetes VoIP capturados.

FIGURA 6. Sesión establecida entre los clientes SIP mediante IPv6.

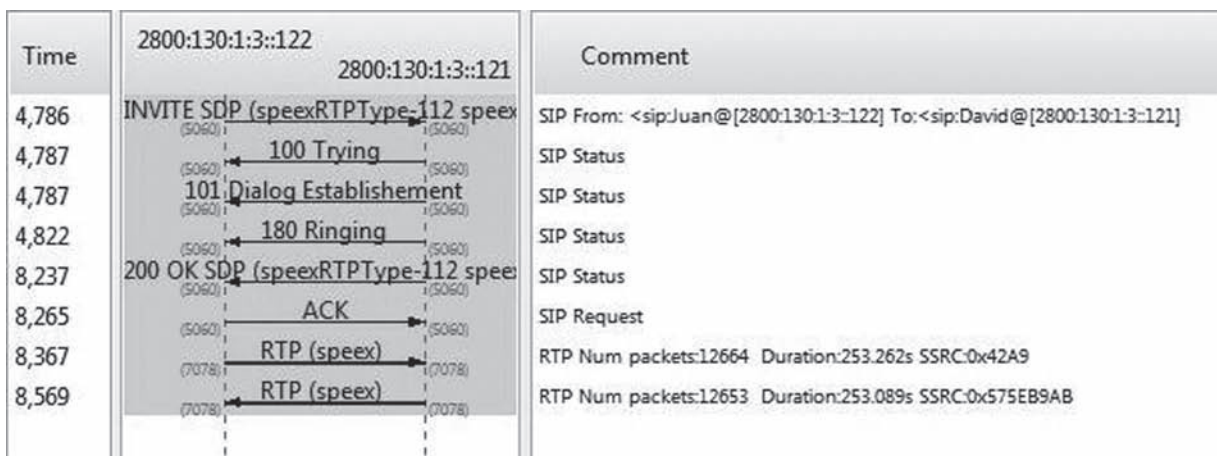


FIGURA 7. Flujo de paquetes RTP en una llamada entre extensiones IPv6.

Analysing stream from 2800:130:1:3::1 port 7078 to 2800:130:1:3::1 port 7078 SSRC = 0x42A9

Packet ^	Sequence ^	Delta(ms) ^	Filtered Jitter(ms) ^	Skew(ms) ^	IP BW(kbps) ^	Marker ^	Status
15	0	0,00	0,00	0,00	0,91		[Ok]
16	1	1,21	1,17	18,79	1,82		[Ok]
17	2	37,61	2,20	1,18	2,74		[Ok]
18	3	0,07	3,31	21,11	3,65		[Ok]
19	4	23,56	3,33	17,55	4,56		[Ok]
20	5	0,06	4,36	37,49	5,47		[Ok]
21	6	55,14	6,29	2,35	6,16		[Ok]

Max delta = 148,06 ms at packet no. 1649
 Max jitter = 30,93 ms. Mean jitter = 20,08 ms.
 Max skew = -119,72 ms.
 Total RTP packets = 12664 (expected 12664) Lost RTP packets = 0 (0,00%) Sequence errors = 0
 Duration 253,26 s (-38 ms clock drift, corresponding to 31995 Hz (-0,01%))

En la figura 7 se puede observar el número de paquetes y la secuencia de estos en la transmisión de voz, también muestra el Jitter máximo que fue de 30.93 ms y Jitter promedio generado durante la llamada, la diferencia máxima entre llegada de un paquete y el siguiente (Max delta) que fue de 148.06 ms, el total de paquetes transmitidos que fue de 12664, el porcentaje de paquetes perdidos de 0%, el estado en cada secuencia (status) que en este caso indica OK en todas las secuencias, lo que significa que todos los paquetes fueron entregados correctamente, puesto que no hubo pérdida de paquetes.

En la figura 8 podemos observar que el Jitter máximo generado entre el intervalo de 216.0s a 217.0s, fue de 30.93ms, posteriormente se mantuvo en un promedio de 20.08 ms.

En la figura 9 podemos observar el Retardo máximo entre la llegada de un paquete y el siguiente que fue de 148.06 ms, se observa también que a partir del segundo 17 este parámetro disminuye de forma considerable, ya que este valor depende de algunos factores inherentes a los dispositivos emisores y receptores y al uso del canal, tales como paquetización, encolamiento, Retardo de propagación, entre otros.

Para graficar el Jitter y Retardo se utilizaron paquetes aleatorios y se grafica el tiempo transcurrido entre la emisión y recepción del paquete (eje X) y el parámetro respectivo (eje Y).

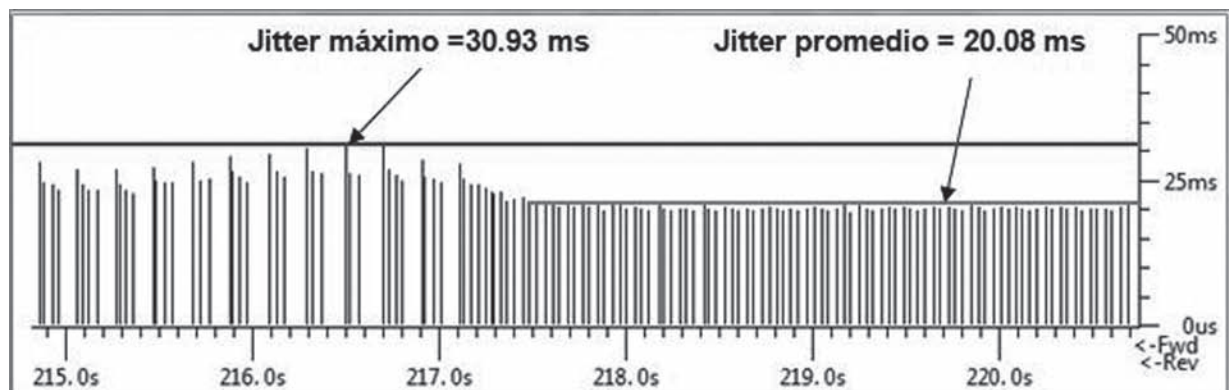
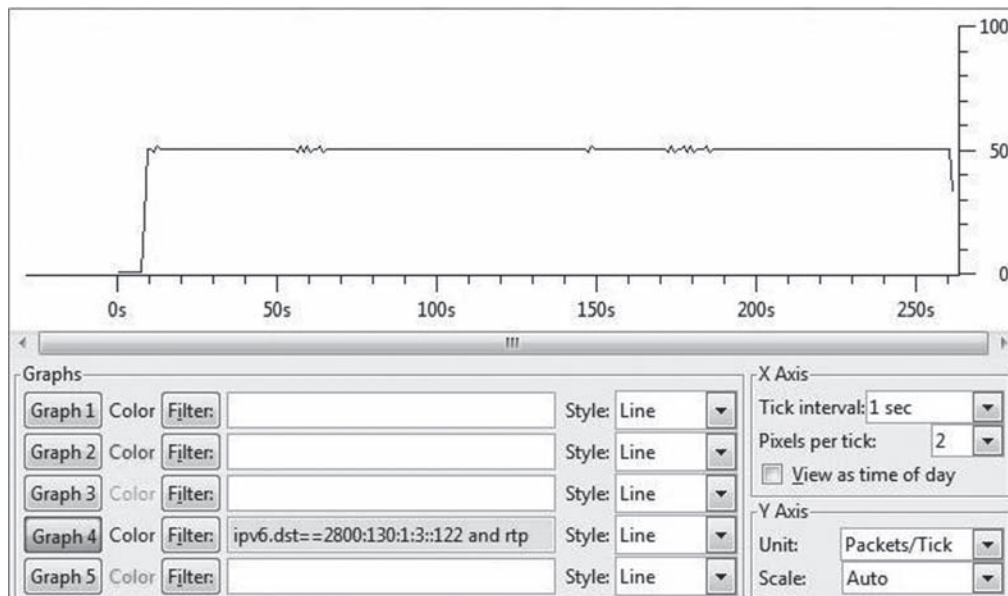
FIGURA 8. Jitter máximo y promedio generado en una llamada entre extensiones IPv.

FIGURA 9. Retardo máximo generado en una llamada entre extensiones IPv6.



En las figuras 10 y 11 se observa de forma gráfica el tráfico RTP generado en ambos clientes relacionando los paquetes entregados con respecto al tiempo y como se observa el tráfico RTP es similar en los dos clientes debido a que en este caso no hubo pérdida de paquetes,

si existiera pérdida de paquetes la variación del flujo RTP entre los clientes estaría en relación al número de paquetes descartados o perdidos por cada terminal al momento de la comunicación.

FIGURA 10. Tráfico RTP generado por el cliente SIP que inicia la llamada.

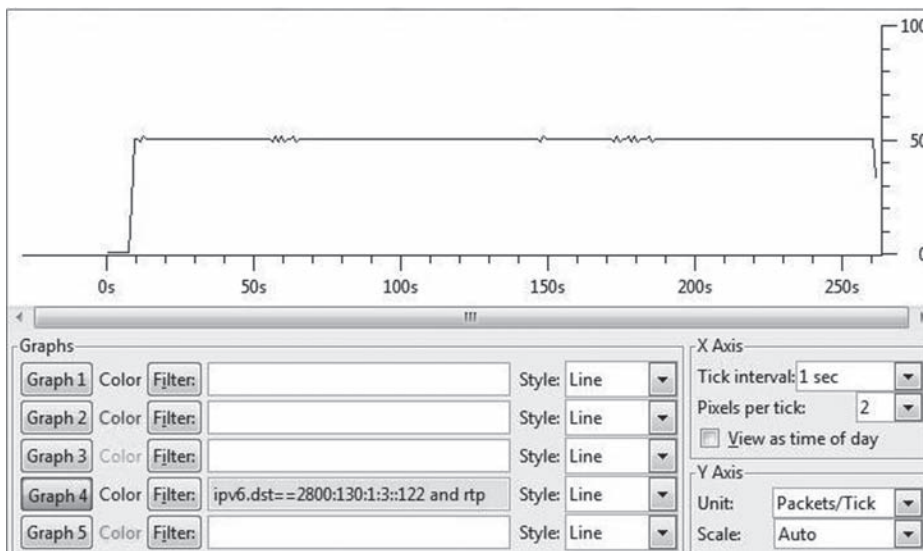
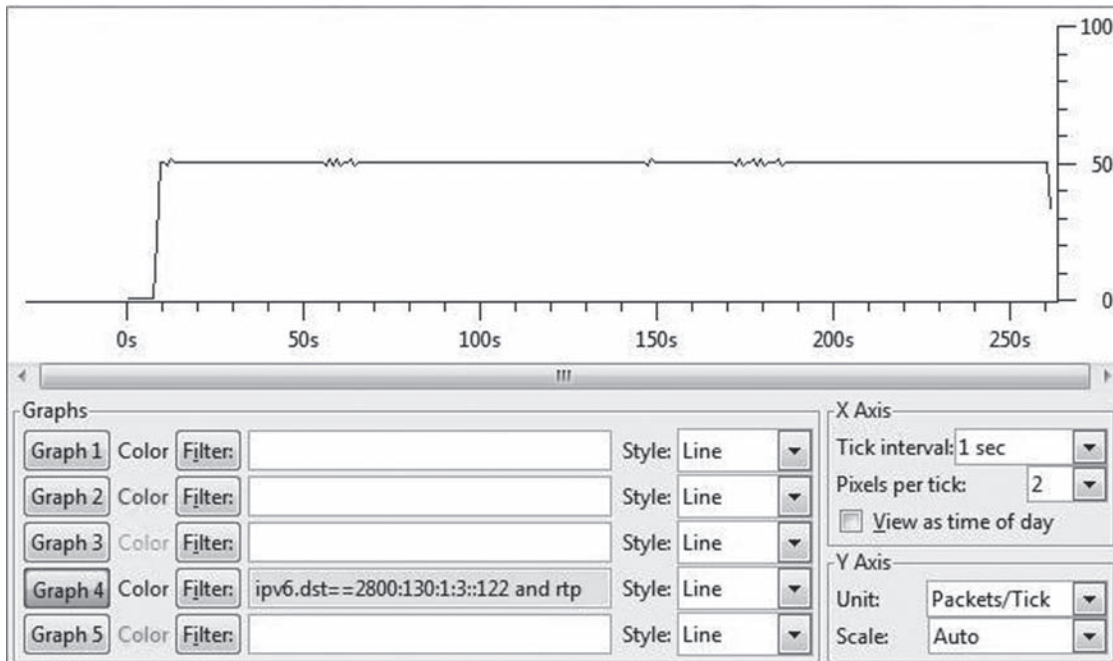


FIGURA 11. Tráfico RTP generado por el cliente SIP que recibe la llamada.



2.5 LLAMADAS ENTRE EXTENSIONES IPV4.

En las llamadas entre extensiones con direccionamiento IPv4 también se obtuvieron resultados satisfactorios. En la figura 12 se muestra la sesión establecida entre dos extensiones IPv4.

En la figura 13 podemos observar el flujo RTP generado en el establecimiento de la llamada, con los mismos parámetros que se describieron en la figura 7.

FIGURA 12. Sesión establecida entre clientes SIP mediante IPv4.

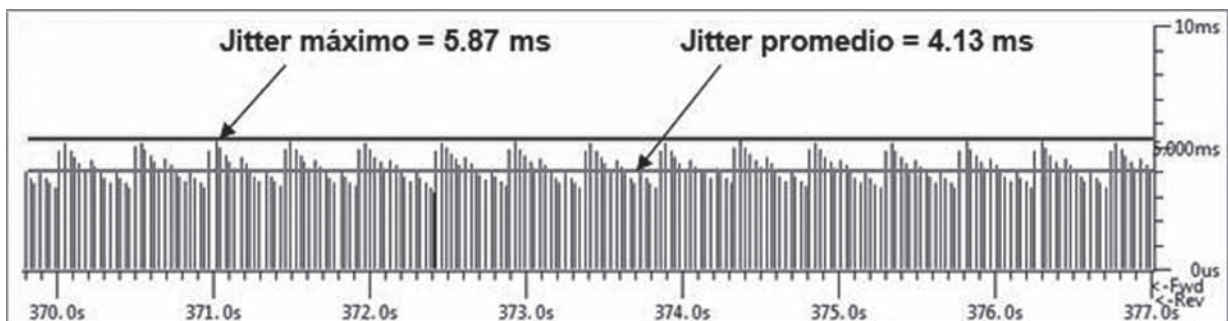
Time	192.168.1.135	192.168.1.196	Comment
2,230	INVITE SDP (speexRTPTType-112 speex		SIP From: "Mary" <sip:Mary@192.168.1.135 To:<sip:Jose@192.168.1.196
2,235	100 Trying		SIP Status
2,240	180 Ringing		SIP Status
4,973	200 OK SDP (g711U NSERTPTType-100		SIP Status
4,985	ACK		SIP Request
5,015	RTP (g711U)		RTP Num packets:12564 Duration:377.066s SSRC:0x32E5C329
5,045	RTP (g711U)		RTP Num packets:12568 Duration:377.009s SSRC:0x45088793

FIGURA 13. Flujo de paquetes RTP en una llamada entre extensiones IPv4.

Forward Direction		Reversed Direction					
Analysing stream from 192.168.1.135 port 7078 to 192.168.1.196 port 16436 SSRC = 0x45088793							
Packet	Sequence	Delta(ms)	Filtered Jitter(ms)	Skew(ms)	IP BW(kbps)	Marker	Status
16	0	0,00	0,00	0,00	2,24		[Ok]
18	1	39,59	0,60	-9,59	4,48		[Ok]
20	2	26,94	0,75	-6,53	6,72		[Ok]
22	3	33,72	0,94	-10,25	8,96		[Ok]
24	4	29,63	0,90	-9,89	11,20		[Ok]
26	5	29,79	0,86	-9,68	13,44		[Ok]
28	6	40,71	1,48	-20,39	15,68		[Ok]
30	7	29,61	1,41	-20,00	17,92		[Ok]
32	8	29,63	1,34	-19,62	20,16		[Ok]
Max delta = 44,62 ms at packet no. 24860 Max jitter = 5,87 ms. Mean jitter = 4,13 ms. Max skew = 50,48 ms. Total RTP packets = 12568 (expected 12568) Lost RTP packets = 0 (0,00%) Sequence errors = 0 Duration 377,01 s (15 ms clock drift, corresponding to 8000 Hz (+0,00%))							

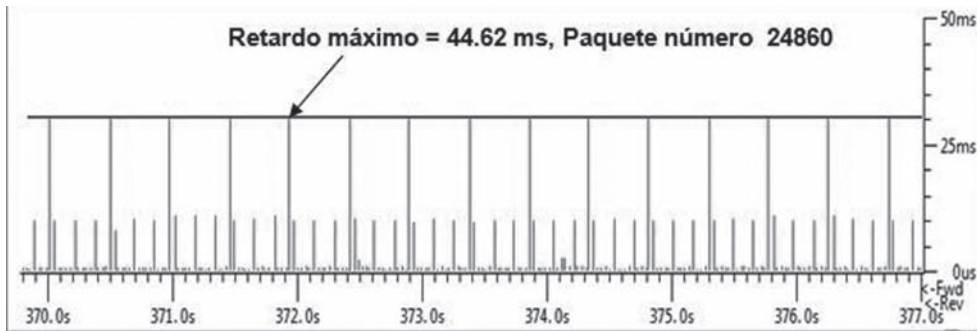
En la figura 14 se muestra el total de paquetes RTP que fue de 12568, el comportamiento del Jitter promedio y Jitter máximo, generado durante una llamada con IPv4 donde se observa que el Jitter máximo no tiene un intervalo definido, ya que fue constate en toda la llamada

con un valor de 5.87 ms, pero sin afectar la calidad de la voz, debido a que el valor es mucho menor en relación al Jitter presentado con IPv6 que fue de 30.93 ms, se observa también un delta máximo de 44.62 ms inferior al observado en la captura con IPv6.

FIGURA 14. Jitter máximo y promedio generado en una llamada entre extensiones IPv4.

En la figura 15 se puede observar que el Retardo máximo entre la llegada de dos paquetes continuos fue de 44.62 ms.

FIGURA 15. Retardo máximo generado en una llamada entre extensiones IPv4.



En las figuras 16 y 17 se observa que el Jitter generado fue constante durante todo el transcurso del tráfico RTP.

FIGURA 16. Tráfico generado por el cliente SIP que inicia la llamada.

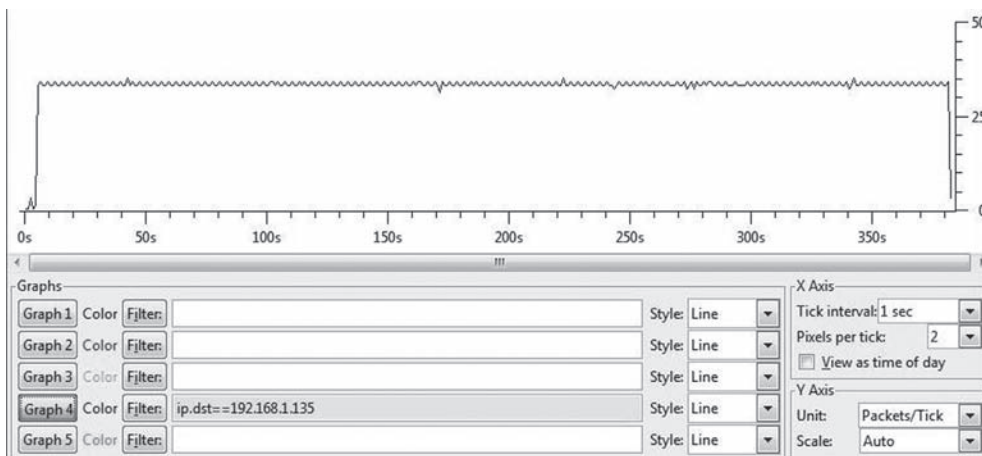
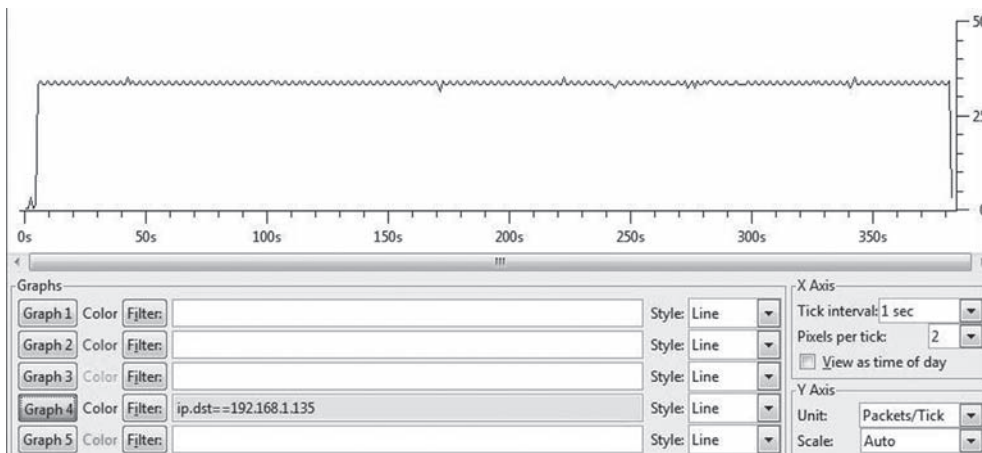


FIGURA 17. Tráfico RTP generado por el cliente SIP que recibe la llamada.



3. ANÁLISIS DE RESULTADOS.

En base a los resultados obtenidos en 10 llamadas, utilizando los protocolos IPv4 e IPv6 se generó la tabla

1, donde se muestra el tiempo en segundos utilizado por cada protocolo para entregar el total de paquetes generados en cada una de las llamadas.

TABLA 1. Resultados en 10 llamadas.

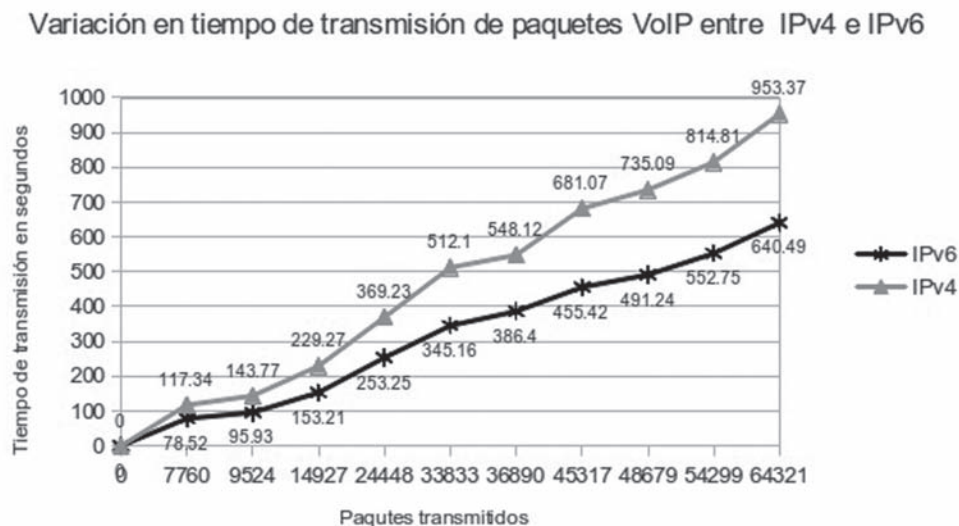
Llamada	N. paquetes	Tiempo de transmisión en segundos IPv6	Tiempo de transmisión en segundos IPv4
1	7760	78.52	117.34
2	9524	95.93	143.77
3	14927	153.21	229.27
4	24448	253.25	369.23
5	33833	345.16	512.1
6	36890	386.4	548.12
7	45317	455.42	681.07
8	48679	491.24	735.09
9	54299	552.75	814.81
10	64321	640.49	953.37
Promedio	33.9998	345.237	510.417

La figura 18 muestra de forma gráfica los datos obtenidos por cada llamada realizada con los protocolos IPv4 e IPv6, donde se puede observar la variación del tiempo total utilizado por IPv4 e IPv6 en la entrega del total de paquetes definidos en las capturas del tráfico RTP.

Considerando los tiempos de transmisión entre IPv4 e IPv6 de la tabla 1, se puede calcular el porcentaje de mejora de IPv6 con respecto a IPv4 y se observa que existe una diferencia de 165.18 ms a favor de IPv6, lo que representa un 32% de mejora, en lo que respecta a número de paquetes por tiempo de transmisión, que impacta que en IPv6 exista un menor Retardo con respecto a IPv4.

En la tabla 2 se tienen el promedio de paquetes enviados por segundo en cada llamada en las dos versiones del protocolo IP y se observa que el promedio de paquetes transmitidos por segundo, utilizando IPv6 es mayor respecto a la cantidad de paquetes transmitidos con IPv4, al graficar estos resultados se obtiene la gráfica de la figura 19.

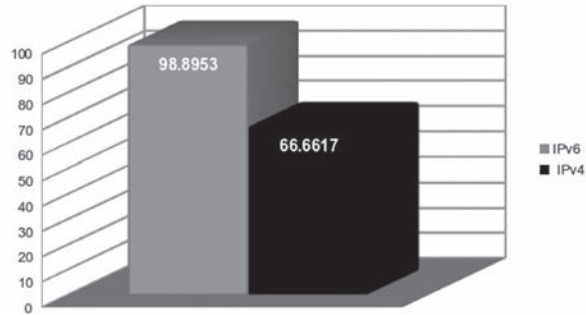
FIGURA 18. Tiempo consumido en la transmisión de paquetes VoIP entre IPv4 e IPv6.



Con respecto al Retardo en las llamadas IPv4 e IPv6 se encuentran por debajo de la recomendación ITU-T G.114 que establece un valor máximo de 150 ms, para poder realizar una llamada de buena calidad.

En cuanto al Jitter promedio generado en las llamadas utilizando los protocolos IPv4 e IPv6, los resultados obtenidos se muestran en la tabla 3 y la gráfica de

estos resultados se muestra en la figura 20, donde observamos que IPv6 presenta un Jitter de 17.51 que es un valor por encima del Jitter presentado con IPv4 que fue de 4.60, sin embargo el Jitter presentado por IPv6 no afectó la calidad del servicio VoIP porque se encuentra dentro del rango de intervalo aceptado por la industria que establecen valores de Jitter menores a 100 ms.

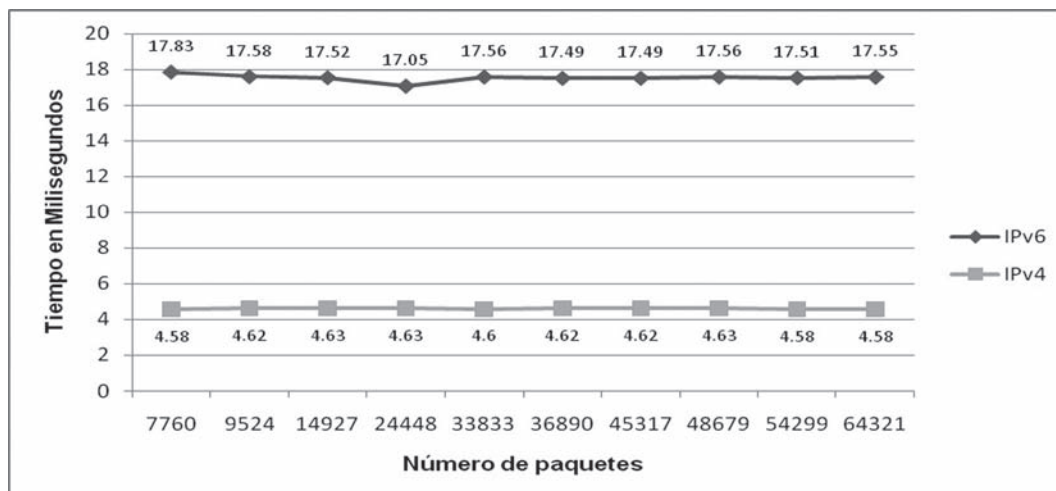
FIGURA 19. Promedio de paquetes VoIP transmitidos con IPv4 e IPv6.**TABLA 2.** Resultados obtenidos en 10 llamadas utilizando IPv4 e IPv6.

Llamada	N. paquetes	Paquetes enviados / seg IPv6	Paquetes enviados / seg IPv4
1	7760	98.093	64.932
2	9524	99.491	65.37
3	14927	96.224	66.568
4	24448	98.307	67.323
5	33833	97.963	67.008
6	36890	100.271	66.568
7	45317	99.379	66.911
8	48679	99.755	66.885
9	54299	99.294	67.85
10	64321	100.176	67.202
Promedio	33.9998	98.8953	66.6617

TABLA 3. Jitter promedio generado en las llamadas VoIP con IPv4 e IPv6.

Llamada	N. de paquetes	Jitter promedio IPv6	Jitter promedio IPv4
1	7760	17.83	4.58
2	9524	17.58	4.62
3	14927	17.52	4.63
4	24448	17.05	4.63
5	33833	17.56	4.6
6	36890	17.49	4.62
7	45317	17.49	4.62
8	48679	17.56	4.63
9	54299	17.51	4.58
10	64321	17.55	4.58
Promedio	33.9998	17.51	4.60

En relación a la seguridad en la transmisión VoIP se observó, que para las llamadas realizadas utilizando direccionamiento IPv6 no fue posible decodificar el audio con el componente que proporciona Wireshark, mientras que para un entorno IPv4 esta misma herramienta permitió decodificar el audio de las llamadas y escuchar la conversación entre dos clientes. Esto se debe a que IPv6 cifra la información desde el protocolo base utilizando IPSec, en IPv4 es posible también implementar este protocolo de seguridad pero a niveles de capas superiores.

FIGURA 20. Jitter generado en la transmisión de paquetes VoIP con IPv4.

4. CONCLUSIONES.

El presente trabajo se realizó teniendo como objetivo principal comprobar de forma práctica la funcionalidad de los protocolos VoIP, SIP e IAX en la transmisión de paquetes de voz en tiempo real sobre un entorno IP Dual Stack, logrando implementar de manera exitosa el protocolo SIP sobre IPv6 e IPv4, en tanto que IAX solo se logró implementar sobre IPv4.

En lo que respecta a los factores inherentes a la transmisión de voz, se observó que en lo referente a uso de ancho de banda y Retardo, la transmisión sobre IPv6 es mejor que sobre IPv4 y en lo que respecta al Jitter, este presenta valores más elevados en IPv6, sin embargo, estos valores de Jitter están dentro del intervalo de valores aceptados por la industria, que recomiendan valores inferiores a los 100 ms, para lograr una llamada de buena calidad, por lo que no genera un problema serio.

Con respecto a la seguridad que ofrece IPv6 no fue posible decodificar el audio de las llamadas utilizando la misma herramienta que proporciona Wireshark que se utilizó de forma exitosa para decodificar el audio de las llamadas sobre IPv4.

Por último es importante mencionar que la mayoría de herramientas que se utilizaron para el desarrollo de este proyecto están basadas en Software Libre, tal es el caso de Asterisk, Cent OS, Liphone y Wireshark, demostrándose que es posible realizar implementaciones VoIP utilizando aplicaciones de Software Libre.

5. REFERENCIAS.

- [1] Cho, K., Luckie, M., & Huffaker, B. (2004). Identifying IPv6 Network Problems in the Dual-Stack World. En SIGCOMM, (Ed.). Network Troubleshooting Workshop del 30 de Agosto al 1 de Septiembre de 2004. (P. 283 – 288) Portland, OR, USA: ACM, ISBN:1-58113-942-X.
- [2] Froehlich, A. (2010). *CCNA Voice Study Guide*. Indianapolis, Indiana: Wiley Publishing.
- [3] Law, Y.N., Lai, M.C., Tan, W.L., & Lau, W.C. (2008). Empirical performance of IPv6 vs. IPv4 under a dual-stack environment. En IEEEEXDL, (Ed.). IEEE International Conference on del 19 al 23 Mayo de 2008 (P. 5924 – 5929). Beijing: IEEE Xplore Digital Library. ISBN: 978-1-4244-2075-9.
- [4] Loshin, P. (2004). *IPv6: theory, protocol, and practice*. San Francisco, CA: Morgan Kaufmann Publishers.
- [5] Meggelen, J.V., Madsen, L., & Smith, J. (2007). *Asterisk: The Future of Telephony*. United States of America: Oreilly.
- [6] Miranda Campos, K.S. (2009). Evaluación de algoritmos de control de Retardo en Voz sobre Internet. Tesis de maestría no publicada. Universidad Autónoma Metropolitana, Ixtapalapa, D.F, México.
- [7] Narayan, S., Shang, P., & Fan, N. (2009). Performance Evaluation of IPv4 and IPv6 on Windows Vista and Linux Ubuntu. En IEEEEXDL, (Ed.). Networks Security, Wireless Communications and Trusted Computing, NSWCTC '09. International Conference on, vol.1 del 25 al 26 Abril de 2009, (P. 653-656). Wuhan, Hubei: IEEE Xplore Digital Library. ISBN:978-1-4244-4223-2.
- [8] Salcedo, O., López, D., & Hernández, C. (2012). Estudio comparativo de la utilización de ancho de banda con los protocolos SIP e IAX. *Revista Tecnura*, 16, 171 – 187.
- [9] Spencer, M., Allison, M., & Rhodes, C. (2003). *The Asterisk Handbook, Version 2*. United States of America: Digium, Inc.
- [10] Wang, Y., Ye, S., & Li, X. (2005). Understanding current IPv6 performance: a measurement study. En IEEEEXDL, (Ed.). Computers and Communications, Proceedings. 10th IEEE Symposium on del 27 al 30 de Junio de 2005. (P. 71 – 76). La Manga del Mar Menor, Cartagena, España: IEEE Xplore Digital Library. ISBN: 0-7695-2373-0.
- [11] Zhou, X., Jacobsson, M., Uijterwaal, H., & Miegheem, P.V. (2008). IPv6 delay and loss performance evolution. *Revista International Journal of Communications Systems*, 21, 643 – 663.
- [12] Zhou, X., & Miegheem, P.V. (2005). Hopcount and E2E Delay: IPv6 versus IPv4. En SBH, (Ed.). 6th International Workshop, PAM 2005 del 31 de Marzo al 1 de Abril 2005. (P. 345 – 348). Boston, MA, USA: Springer-Verlag. ISBN: 978-3-540-31966-5.
- [13] Internet E. T. F. (1981). RFC791, Internet Protocol. Recuperado (2012, Septiembre 20) de <http://tools.ietf.org/html/rfc791>.
- [14] Internet E. T. F. (2003). RFC3513, Internet Protocol Version 6 (IPv6) Addressing Architecture. Recuperado (2012, Septiembre 20) de <http://www.ietf.org/rfc/rfc3513.txt>.

- [15] Internet E. T. F. (2003). RFC 3550, RTP: A Transport Protocol for Real-Time Applications. Recuperado (2012, Octubre 12) de <http://www.ietf.org/rfc/rfc3550.txt?number=3550>.
- [16] Internet E. T. F. (2003). RFC 3551, RTP Profile for Audio and Video Conferences with Minimal Control. Recuperado (2012, Octubre 12) de <http://www.ietf.org/rfc/rfc3550.txt?number=3551>.
- [17] Internet E. T. F. (2003). RFC 3611, RTP Control Protocol Extended Reports (RTCP XR). Recuperado (2012, Octubre 12) de <http://www.ietf.org/rfc/rfc3611.txt?number=3611>.
- [18] Internet E. T. F. (2003). RFC 3711, The Secure Real-time Transport Protocol (SRTP). Recuperado (2012, Octubre 12) de <http://www.ietf.org/rfc/rfc3711.txt>.
- [19] Internet E. T. F. (2010). RFC 5446, IAX: Inter-Asterisk eXchange Version 2. Recuperado (2012, Octubre 12) de <http://tools.ietf.org/html/rfc5446>.