ÍNDICE

LISTA DE CUADROS

LISTA DE FIGURAS

CAPÍTULO I

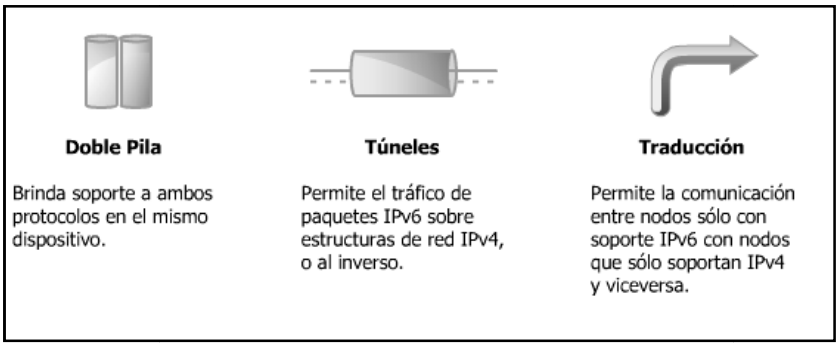
1. INTRODUCCIÓN

1.1. Antecedentes

El crecimiento acelerado de Internet y el agotamiento inminente del espacio de direcciones IPv4 ha hecho necesario a algunas organizaciones, utilizar varias alternativas que puedan sostener este avance imparable e implacable , una de estas son los traductores de direcciones de red NAT, (Network Address Translator) para asignar múltiples direcciones privadas a una única dirección IP pública. Aunque los NAT impulsan la reutilización del espacio de direcciones privadas, no admiten la seguridad de nivel de red basada en estándares o la asignación correcta de todos los protocolos de nivel superior y pueden crear problemas al enlazar dos organizaciones que utilizan el espacio de direcciones privadas. El Protocolo IPv6 es una versión del protocolo Internet Protocol (IP) y está destinado a reemplazar a IPv4, definido en el RFC 2460 esta nueva versión del Protocolo de Internet fue Diseñado por Steve Deering de Xerox PARC y Craig Mudge.

Uno de los aspectos primordiales de este nuevo estándar, a más de mecanismos de seguridad incorporados, es el soporte de Calidad del Servicio (QoS), lo que abre las puertas a nuevas tecnologías para soportar ingeniería de Tráfico, y una de las aplicaciones tiene mayor demanda es la VoIP. Aunque las ventajas sobre Ipv4 son muchas, sin embargo la implementación del nuevo protocolo se la ha ido haciendo de una manera prudente, coexistiendo con el “viejo” protocolo, a través de mecanismos de transición bien definidos como Doble Pila, Túneles o Traducción .

Figura 1. Túneles de transición



Fuente:blogs.salleurl.edu

Cada una de estas técnicas muestra una característica específica y puede ser utilizada individualmente o en conjunto, para atender las necesidades de cada situación, ya sea para realizar una migración a IPv6 paso a paso comenzando con un único host o una subred, o incluso toda una red corporativa.[1]

1.2. Justificación

Si bien, IPv6 no resuelve ni remedia todos los problemas que afectan a IPv4, sin embargo ayuda a menguar muchos de sus efectos. IPv6 es primordial para la innovación y desarrollo de nuevas e inimaginables aplicaciones y servicios de las redes actuales y futuras.

De tal forma que se considera a IPv6 como una parte clave en: comunicaciones ubicuas, servicios multimedia de VoIP, redes sociales (P2P) y redes de sensores, por mencionar algunas. Todo gracias a las ventajas competitivas y de eficiencia que ofrece IPv6 respecto a IPv4.

Dentro de las soluciones al problema propuesto se desarrolló un ambiente de simulación de una red empresarial, en el que se implemente trafico de VoIP

[1] Análisis del protocolo IPv6 su Evolución y Aplicabilidad – Duque Vallejo

empleando Calidad de servicio (QoS), para una red local corporativa en ambiente de Software libre (Linux), utilizando IPv6, Utilizando políticas de Calidad de servicio, de servicios diferenciados. Con el objetivo de minimizar la latencia de los paquetes deseados, maximizar la salida de estos paquetes y por el contrario, parar la salida de tráfico, por ejemplo, P2P, y garantizar el paso del tráfico RTP.

1.3. Objetivos

1.3.1. General

Analizar la aplicación de QoS sobre IPv6 para mejorar la transmisión de VoIP en una LAN corporativa.

1.3.2. Específicos

- Analizar la transmisión de VoIP sobre IPv6 en una red local corporativa.
- Analizar y comparar las versiones de protocolos de internet (IP) existentes para la transmisión de VoIP.
- Proponer una alternativa de QoS bajo IPv6, para mejorar la transmisión de VoIP
- Desarrollar un ambiente de simulación de una red, en el que se implemente VoIP; empleando Calidad de servicio (QoS) bajo Linux, para una red local corporativa.

1.4. Hipótesis

La aplicación de QoS sobre IPv6 permitirá mejorar la transmisión de VoIP en una LAN corporativa.

CAPÍTULO II

2. REVISIÓN DE LA LITERATURA

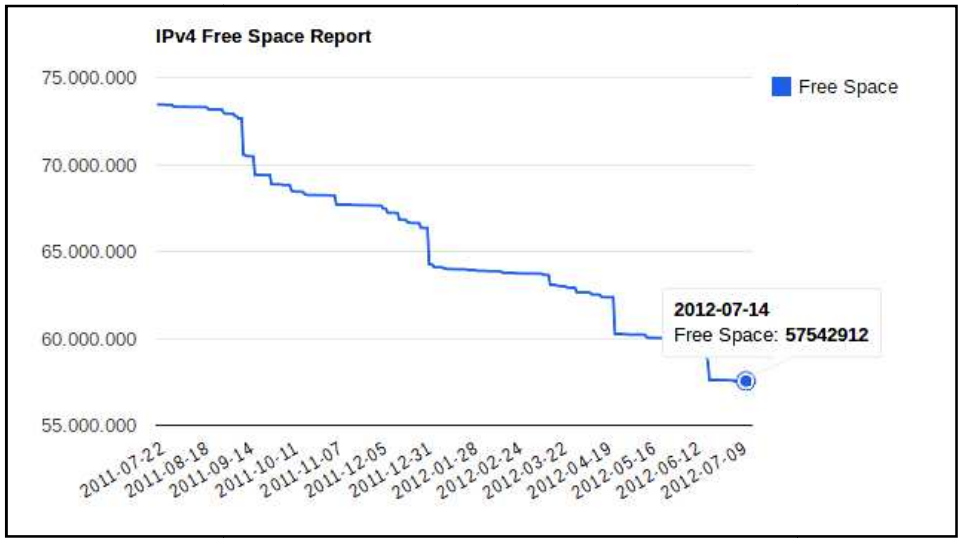
2.1 El protocolo IPv6

El Protocolo de Internet versión 6, mejor conocido como IPv6, es la versión más reciente de este protocolo y el sucesor de IPv4, la versión anterior, la cual no había sobrellevado cambios importantes desde 1981 cuando se dio a conocer por primera vez. Antes de acoger este nombre, el protocolo IPv6 fue llamado IPng (Internet Protocol next generation), y hasta la fecha existen personas que lo siguen llamando de esta manera. Al mirar el salto desde IPv4 hasta IPv6 (omitiendo la opción que parecería ser más lógica, IPv5) surge la duda en cuanto a por qué no se utilizó IPv5 como el nombre para el protocolo sucesor. La respuesta es muy simple: IPv5 nunca fue considerado para ser la nueva versión del protocolo. El nombre IPv5 fue asignado a un protocolo experimental, cuyo objetivo era el de la transmisión de datos en tiempo real. Este protocolo fue conocido originalmente como ST-2 (Stream Protocol Version 2), pero su función fue reemplazada eventualmente por RSVP (Resource Reservation Setup Protocol). Incluso, a raíz de este suceso, se han hecho peticiones para que en un futuro las versiones aumenten en números pares.

El motivo básico por el que surge, en el seno del IETF (Internet Engineering Task Force), la necesidad de crear un nuevo protocolo, fue la evidencia de la falta de direcciones, ya que IPv4 tiene un espacio de direcciones de 32 bits, es decir, 2 exp 32 (4.294.967.296). En cambio, IPv6 ofrece un espacio de 2 exp 128

(340.282.366.920.938.463.463.374.607.431.768.211.456).[2]

Figura 2. Reporte Lacnic: IPv4 Addresses Available for allocation (Reserve last /10):



Fuente:http://lacnic.net/sp/registro/espacio-disponible-IPv4.html

2.2. Tipos de direcciones IPv6.

Existen tres tipos de direcciones IPv6.

Direcciones Unicast (uno a uno). Asemeja una interfaz de red única. Un paquete enviado a una dirección Unicast es entregado sólo a la interfaz identificada con dicha dirección. Es el paralelo a las direcciones IPv4 actuales, y tenemos las siguientes:

- globales
- enlace-local
- local-de-sitio (desaprobada)
- Unique Local (ULA)
- Compatible-IPv4 (desaprobada)

[2] IP Version 6 Working Group IETF

- Mapeada-IPv4

Direcciones multicast: (uno-a-muchas) Una dirección multicast se asigna a un grupo de hosts que reciben todos los paquetes destinados a dicha IP multicast. Las direcciones multicast tienen los primeros ocho bits en 1. Los últimos cuatro bits del segundo octeto identifican el alcance de la dirección. Los últimos 112 bits se usan para identificar cada grupo multicast.

Direcciones anycast: (uno-a-la-mas-cercana) Una dirección anycast se asigna a un grupo de interfaces que normalmente pertenecen a diferentes hosts. Un paquete enviado a una dirección anycast se envía a sólo una de las interfaces miembros del grupo, normalmente la más cercana.

Reservadas: Grupo de direcciones reservadas

Direcciones Unicast Especiales

Dirección no especificada. Es utilizada temporalmente cuando no se ha asignado una dirección: 0:0:0:0:0:0:0:0 (::/128), definido en el RFC5156[3]

Dirección de loopback, para el "auto-envío" de paquetes: 0:0:0:0:0:0:0:1 (::1/128)

Prefijo de documentación: 2001:0db8::/32 definido en el RFC 3849

Cabe señalar que las direcciones Unicast y Milticast ya existían en el protocolo IPv4.[4]

[3]Leandro Di Tommaso — Maximiliano García Rodríguez
[4]6deploy (Consulintel)

2.3. Abreviaciones del Protocolo IPv6

Representación Textual. La representación de las direcciones IPv6 conlleva las siguientes normas generales:

- 8 Grupos de 16 bits separados por ":"

- Notación hexadecimal de cada nibble (4 bits)

- Se pueden eliminar los ceros a la izquierda dentro de cada grupo

- Se pueden sustituir uno o más grupos "todo ceros" por "::". (Esto se puede hacer solo una vez)

Ejemplos

2001:0db8:3003:0001:0000:0000:6543:0ffe

Nos queda: 2001:db8:3003:1::6543:ffe

2.4. Prefijos de los Tipos de Direcciones

Figura 3. Tipos de direcciones IPv6

Tipo de Dirección	Prefijo Binario	Notación IPv6
Unspecified	00...0 (128 bits)	::/128
Loopback	00...1 (128 bits)	::1/128
Multicast	1111 1111	FF00::/8
Link-Local Unicast	1111 1110 10	FE80::/10
ULA	1111 110	FC00::/7
Global Unicast	(everything else)	
IPv4-mapped	00...0:1111...1111:IPv4	::FFFF:IPv4/128
Ipv4-compatible (desaprobada)	00...0 (96 bits)	::IPv4/128
Site-Local Unicast (desaprobada)	1111 1110 11	FEC0::/10

Fuente: WALC2011 Track 2: Despliegue de IPv6 Alvaro Vives (alvaro.vives@consulintel.es)

2.4.1. Prefijos Globales Unicast

El prefijo 2000::/3 se esta usando para las asignaciones de direcciones Globales Unicast, todos los demás prefijos están reservados.

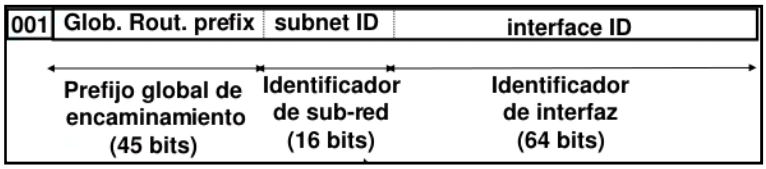
Figura 4 Prefijos Globales Unicast

Tipo de Dirección	Prefijo Binario
IPv4-compatible	0000...0 (96 zero bits) (desaprobada)
IPv4-mapped	00...0FFFF (80 zero+ 16 one bits)
Global unicast	001
ULA	1111 110x (1= Asignado localmente) (0=Asignado centralmente)

Fuente: WALC2011 Track 2: Despliegue de IPv6 Alvaro Vives (alvaro.vives@consulintel.es)

2.4.2. Dirección Global Unicast

Figura 5 Dirección Global Unicast



Fuente: WALC2011 Track 2: Despliegue de IPv6 Alvaro Vives (alvaro.vives@consulintel.es)

El prefijo de encaminamiento global es un valor asignado a un zona (site), es decir, a un conjunto de sub-redes/links. Se ha diseñado para ser estructurado jerárquicamente por los RIRs e ISPs

El ID de sub-red es un identificador de una subred dentro de un site. Se ha diseñado para ser estructurado jerárquicamente por el administrador del site

El identificador de interfaz se construye normalmente según el formato EUI-64

2.4.3. Dirección Global Unicast para Servicios de Producción

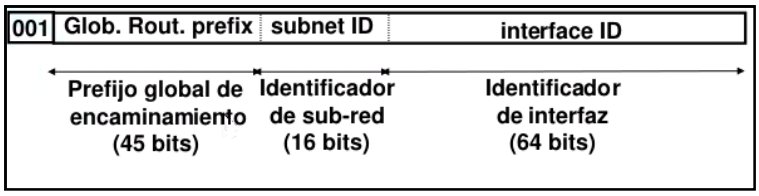
Los ISPs normalmente toman prefijos /32

Las direcciones IPv6 de producción empiezan por 2001, 2003, 2400, 2800, etc.

Hasta /48 se estructura jerárquicamente por el ISP según el uso interno

Desde /48 hasta /128 se delega a los usuarios.

Figura 6. Dirección Global de Unicast



Fuente: WALC2011 Track 2: Despliegue de IPv6 Alvaro Vives (alvaro.vives@consulintel.es)

2.4.4. Recomendaciones para la delegación de direcciones

- /48 caso general, excepto para abonados grandes

- /64 si se sabe que una y solo una única red es necesaria

- /128 si es absolutamente seguro que se va a conectar uno y solo un dispositivo

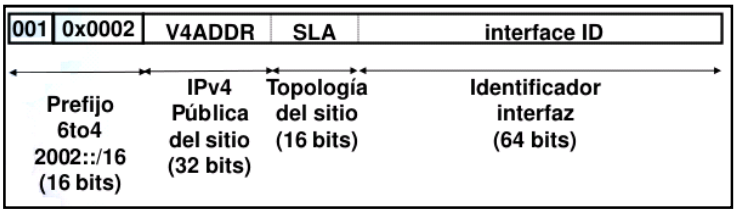
2.4.5. Direcciones 6to4

Conexiones hacia dominios IPv6 a través de IPv4

Prefijo asignado 2002::/16

Para asignarlos a los sitios 2002:IPV4ADDR::/48

Figura 7 Conexiones hacia dominios IPv6

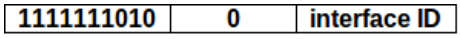


Fuente: WALC2011 Track 2: Despliegue de IPv6 Alvaro Vives (alvaro.vives@consulintel.es)

2.4.6. Direcciones Link-Local y Site-Local

Las direcciones link-local se usan durante la autoconfiguración de los dispositivos y cuando no existen encaminadores (FE80::/10)

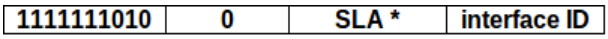
Figura 8. LinkLocal



Fuente: WALC2011 Track 2: Despliegue de IPv6 Alvaro Vives (alvaro.vives@consulintel.es)

Las direcciones site-local se usan para tener independencia del ISP y facilitar su cambio. Pueden usarse junto a direcciones globales o en exclusiva si no hay conectividad global (FEC0::/10) .

Figura 9. Site Local



Fuente: WALC2011 Track 2: Despliegue de IPv6 Alvaro Vives (alvaro.vives@consulintel.es)

2.4.7. Dirección Anycast

Es un identificador de un conjunto de interfaces (normalmente en diferentes nodos).

Un paquete enviado a una dirección anycast se entregará a una de las interfaces identificadas por esa dirección (la más cercana desde el punto de vista de los protocolos de encaminamiento)

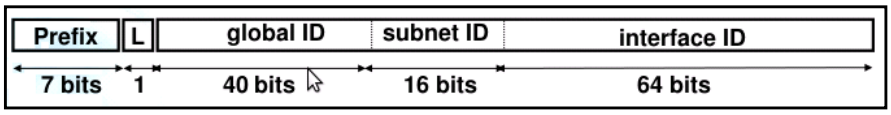
Se obtienen del espacio de direcciones unicast (de cualquier ámbito) y son sintácticamente indistiguinguibles de las direcciones unicast.

Las direcciones anycast reservadas se definen en el RFC2526.

2.4.8. Direcciones IPv6 Unique Local

IPv6 ULA (Unique Local Address)

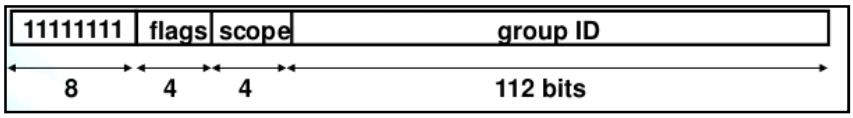
Figura 10 Dirección ULA.



Fuente: WALC2011 Track 2: Despliegue de IPv6 Alvaro Vives (alvaro.vives@consulintel.es)

2.4.9. Direcciones Multicast

Figura 11. Multicast.



Fuente: WALC2011 Track 2: Despliegue de IPv6 Alvaro Vives (alvaro.vives@consulintel.es)

Flags: 0RPT: El flag de más peso está reservado y debe inicializarse a 0

– T: Asignación Transitoria, o no

– P: Asignación basada, o no, en un prefijo de red

– R: Dirección de un Rendezvous Point incrustada, o no

Scope:

1 - Interface-Local

2 - link-local

4 - admin-local

5 - site-local

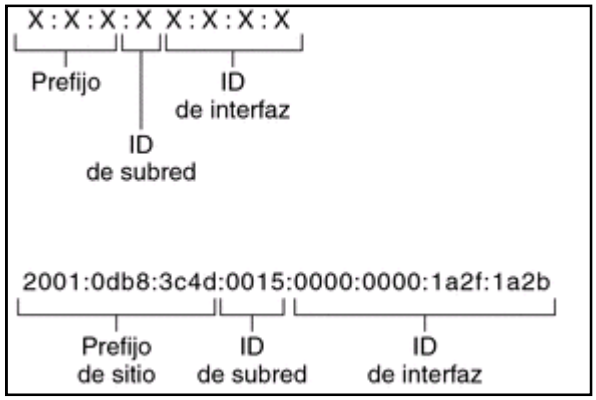
8 - organization-local

E – global.

2.5. Características del protocolo IPv6.

En el protocolo IPv6, una dirección a diferencia de IPv4 (32 bits), tiene un tamaño de 128 bits y se compone de ocho campos de 16 bits, cada uno de ellos unido por dos puntos. Cada campo debe contener un número hexadecimal, como lo indica la figura:

Figura 12. Características de IPv6.



Fuente:Alvaro Vives Consulintel Walc 2011

Los tres campos que están más a la izquierda (48 bits) contienen el prefijo de sitio. El prefijo describe la topología pública que el ISP o el RIR (Regional Internet Registry, Registro Regional de Internet) suelen asignar al sitio.

El campo siguiente lo ocupa el ID de subred de 16 bits que usted (u otro administrador) asigna al sitio. El ID de subred describe la topología privada, denominada también topología del sitio, porque es interna del sitio.

Los cuatro campos situados más a la derecha (64 bits) contienen el ID de interfaz, también denominado token. El ID de interfaz se configura automáticamente desde la dirección MAC de interfaz o manualmente en formato EUI-64.[5]

Hasta hace algunos años, el IPv4 había resultado ser un protocolo completo y de fácil implementación. El problema es que no se anticiparon algunas situaciones que eventualmente se convertirían en limitantes para la utilización del mismo.

IPv6 presenta ciertas características que contrastan con la versión 4 de este protocolo. Estas características se listan a continuación:

• Mayor espacio para direccionamiento.

• Simplificación de la cabecera.

• Cabeceras de extensión.

• Mejor soporte para calidad de servicio.

• Mayor seguridad en el protocolo.

• Direccionamiento jerárquico y enrutamiento eficientes.

2.5.1. Mayor espacio para el direccionamiento

En el protocolo IPv6 se incrementó el tamaño de las direcciones IP de 32 bits a 128 bits. El propósito de utilizar 128 bits no es exclusivamente para aumentar la cantidad de direcciones IP, ya que aunque 128 bits pueden representar hasta 3.4x1038 posibles direcciones, el espacio para direccionamiento en IPv6 ha sido diseñado para soportar múltiples niveles de direccionamiento jerárquico (niveles tales como el diseño de subredes).

[5]http://docs.oracle.com/cd/E19957-01/820-2981/6nei0r0ue/index.html#ipv6-overview-fig-2

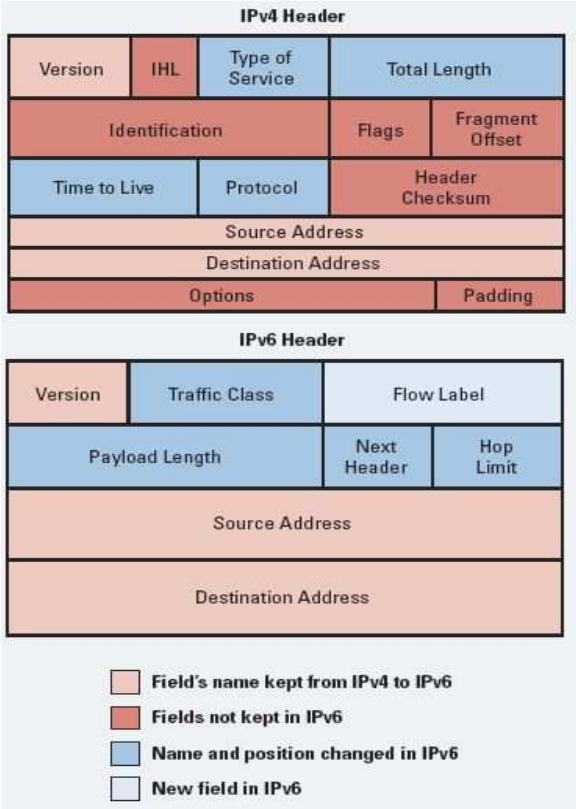
Por el momento solo hay una pequeña cantidad de estas direcciones asignadas, lo que indica que existe un gran número de direcciones disponibles para ser utilizadas en un futuro.

2.5.2. Simplificación de la cabecera

La cabecera IPv6 fue diferenciada para contraer el tiempo que tardaban los enrutadores en procesarla. Esto se logró descartando algunos campos obsoletos y moviendo los campos opcionales y los que no se consideraban indispensables a las cabeceras de extensión, las cuales se colocan después de la cabecera IPv6.[6]

Cuadro Comparativo con respecto a IPv4

Figura 13. Encabezado IPv4 – IPv6.



Fuente: http://notannuevo.blogspot.com/2011/02/la-reserva-de-numeros-ip-necesarios.html

[6]http://www.hola-mundo.net/index.php?/gallery/image/77-cabecera-IPv4/

El motivo fundamental por el que los campos son eliminados, es la innecesaria redundancia. En IPv4 estamos facilitando la misma información de varias formas. Un caso muy evidente es el checksum o verificación de la integridad de la cabecera: Otros mecanismos de encapsulado ya realizan esta función (IEEE 802 MAC, framing PPP, capa de adaptación ATM, etc.).

El caso del campo de “Desplazamiento de Fragmentación”, es ligeramente diferente, dado que el mecanismo por el que se realiza la fragmentación de los paquetes es totalmente modificado en IPv6, lo que implica la total “inutilidad” de este campo. En IPv6 los encaminadores no fragmentan los paquetes, sino que de ser precisa, dicha fragmentación/desfragmentación se produce extremo a extremo.

Algunos de los campos son renombrados:

Longitud total .- Longitud de carga útil (payload length), que en definitiva, es la longitud de los propios datos, y puede ser de hasta 65.536 bytes. Tiene una longitud de 16 bits (2 bytes).

Protocolo.- Siguiente cabecera (next header), dado que en lugar de usar cabeceras de longitud variables se emplean sucesivas cabeceras encadenadas, de ahí que desaparezca el campo de opciones. En muchos casos ni siquiera es procesado por los encaminadores, sino tan sólo extremo a extremo. Tiene una longitud de 8 bits (1 byte).

Tiempo de vida .- Límite de saltos (Hop Limit). Tiene una longitud de 8 bits (1 byte).

Los nuevos campos son:

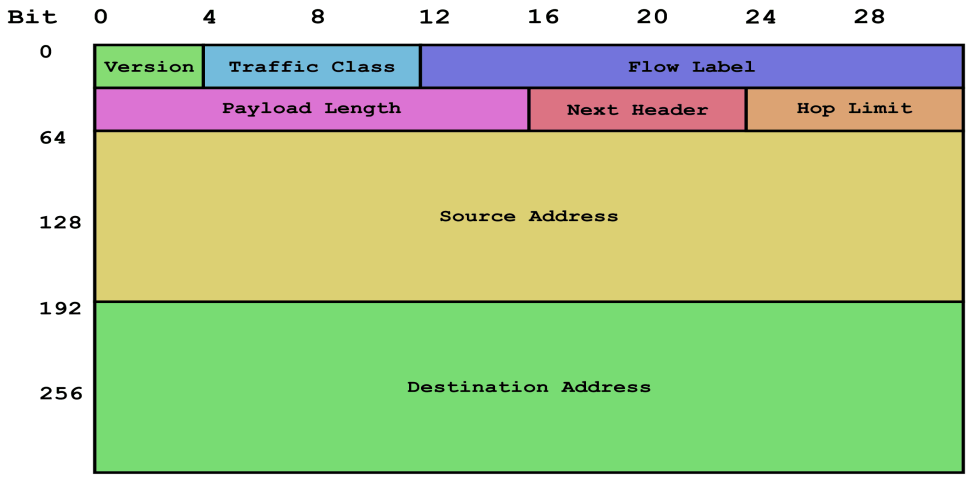
Clase de Tráfico (Traffic Class), también denominado Prioridad (Priority), o simplemente Clase (Class). Podría ser más o menos equivalente a TOS en IPv4. Tiene una longitud de 8 bits (1 byte).

Etiqueta de Flujo (Flow Label), para permitir tráficos con requisitos de tiempo real. Tiene una longitud de 20 bits.

Estos dos campos, como se puede suponer, son los que nos permiten una de las características fundamentales e intrínsecas de IPv6: Calidad de Servicio (QoS), Clase de Servicio (CoS), y en definitiva un poderoso mecanismo de control de flujo, de asignación de prioridades diferenciadas según los tipos de servicios.

Por tanto, en el caso de un paquete IPv6, la cabecera tendría el siguiente formato:

Figura 14. Cabecera IPv6



Fuente: Jordi Palet Martínez (jordi@consulintel.es)

El campo de versión, que es igual a 6, lógicamente, tiene una longitud de 4 bits.
La longitud de esta cabecera es de 40 bytes, el doble que en el caso de IPv4, pero con muchas ventajas, al haberse eliminado campos redundantes.

Además, como ya hemos mencionado, la longitud fija de la cabecera, implica una mayor facilidad para su procesado en routers y conmutadores, incluso mediante hardware, lo que implica unas mayores prestaciones.

A este fin coadyuva, como hemos indicado anteriormente, el hecho de que los campos están alineados a 64 bits, lo que permite que las nuevas generaciones de procesadores y microcontroladores, de 64 bits, puedan procesar mucho más eficazmente la cabecera IPv6.

El valor del campo “siguiente cabecera”, indica cual es la siguiente cabecera y así sucesivamente. Las sucesivas cabeceras, no son examinadas en cada nodo de la ruta, sino sólo en el nodo o nodos destino finales. Hay una única excepción a esta regla: cuando el valor de este campo es cero, lo que indica opción de examinado y proceso “salto a salto” (hop-by-hop). Así tenemos, por citar algunos ejemplos, cabeceras con

información de encaminado, fragmentación, opciones de destino, autenticación, encriptación, etc., que en cualquier caso, han de ser procesadas en el orden riguroso en que aparecen en el paquete.

2.5.3. Mejor soporte para calidad de servicio

Se agregó la capacidad de etiquetar paquetes que pertenezcan a un mismo tipo de tráfico, para los cuales el emisor haya solicitado un manejo especial, como el envío de datos “en tiempo real”.

2.5.4. Direccionamiento jerárquico y enrutamiento eficientes

Las direcciones IPv6 globales utilizadas en la porción IPv6 del Internet fueron diseñadas para crear una infraestructura de enrutamiento eficiente y jerárquica, basada en la existencia de diferentes proveedores de servicio de Internet , cada uno con diferentes características.

Debido a estas características, en la parte IPv6 del Internet los enrutadores pertenecientes al backbone manejan tablas de enrutamiento mucho más pequeñas.

2.5.5. La seguridad en el protocolo IP

Debido al carácter científico que en un inicio tuvo INTERNET, la seguridad no fue avistada históricamente en ninguna de las capas que constituyen la estructura TCP/IP. Con el apogeo de las tecnologías de la información y el aumento de personas y empresas conectadas a INTERNET, la necesidad de seguridad se fue convirtiendo en una necesidad. Además la difusión de noticias sobre personas sin escrúpulos dedicadas a la piratería en INTERNET, creó un gran disgusto social debido a la sensación de inseguridad por los ataques que sufrían tanto las empresas (bancos, universidades e incluso instituciones como la NASA) como los usuarios (utilización ilícita de números de tarjetas de crédito...). La tardía reacción de las instituciones encargadas de la creación y modificación de los protocolos de INTERNET, propició la

aparición de diferentes soluciones comerciales (SSL, SET...) para que los usuarios pudieran disfrutar de una seguridad que INTERNET no proporcionaba.

Aprovechando la necesidad de adaptar los diferentes protocolos al incremento de INTERNET, se optó por encuadrar una serie de especificaciones para garantizar la seguridad como parte implícita de las nuevas especificaciones de los protocolos. Estas especificaciones se conocen como IP Security o IPSec.

Las especificaciones IPSec han sido precisadas para trabajar en la capa inferior de la pila (Stack) de protocolos TCP/IP, funcionando por lo tanto en el nivel de datagrama y siendo independientes del resto de protocolos de capas superiores (TCP, UDP...). La seguridad en IPSec se facilita mediante dos aspectos de seguridad (Security Payload):

- Cabecera de autenticación (Authentication Header, AH). Esta cabecera es la encargada de proporcionar autenticidad a los datos (datagramas) que se reciben en dos aspectos:

• Los datagramas provienen del origen especificado. Se garantiza la autenticidad del origen de los datos (no pueden ser repudiados).

• Los datagramas (y por tanto los datos que contienen) no han sido modificados.

- Cifrado de seguridad (Encrypted Security Payload, ESP). De esta forma se garantiza que tan sólo el destinatario legítimo del datagrama (datos) pueda descifrar el contenido del datagrama.

La autenticidad y el cifrado de datos (o datagramas) requiere que tanto el emisor como el receptor conlleven una clave, un algoritmo de cifrado/descifrado y una serie de parámetros (como el tiempo de validez de la clave) que diferencian una comunicación segura de otra. Estos parámetros conforman la asociación de seguridad (Security Association, SA) que permite unir la autenticidad y la seguridad en IPSec.

En un computador con múltiples conexiones (consultar el mail mientras se baja un fichero por FTP y se consulta el saldo bancario...) podemos tener varias asociaciones de seguridad (como mucho una por conexión). Para poder diferenciar entre ellas utilizaremos un índice de parámetros de seguridad (Security Parameter Index, SPI)

que nos permitirá al recibir un datagrama saber a que asociación de seguridad hace referencia, y de esta forma poder autenticarlo y/o descifrarlo.

Al comenzar una comunicación que use los servicios IPSec con un único destino (direcciones unicast) este nos debe comunicar a que índice de parámetros de seguridad (SPI) debemos hacer referencia. Análogamente en una comunicación con varios destinos (direcciones multicast o anycast) todos los destinatarios deben compartir el mismo número de índice (SPI).

2.5.6. Movilidad IPv6

Conceptos de movilidad

- Home Agent: Servidor en la “Home Network” (HN).

- Foreing Agent: Servidor en la red visitada.

- Mobile Node: Nodo en movimiento.

- Correspondent Node: Nodo con el que comunica el MN.

- Home Address: Dirección obtenida en la HN.

- Care of Address: Dirección obtenida en la red visitada y que representa al Mobile Node. Es una dirección que está dentro del Foreing Agent, en una interfaz virtual (CoA).

Un Nodo en movimiento tiene una o más direcciones de origen relativamente estables; asociadas con el nombre del host a través de DNS, cuando descubre que se encuentra en una subred diferente (cuando no está en su subred de origen), adquiere una dirección diferente

• Registra la “care-of-address” obtenida con su Home Agent

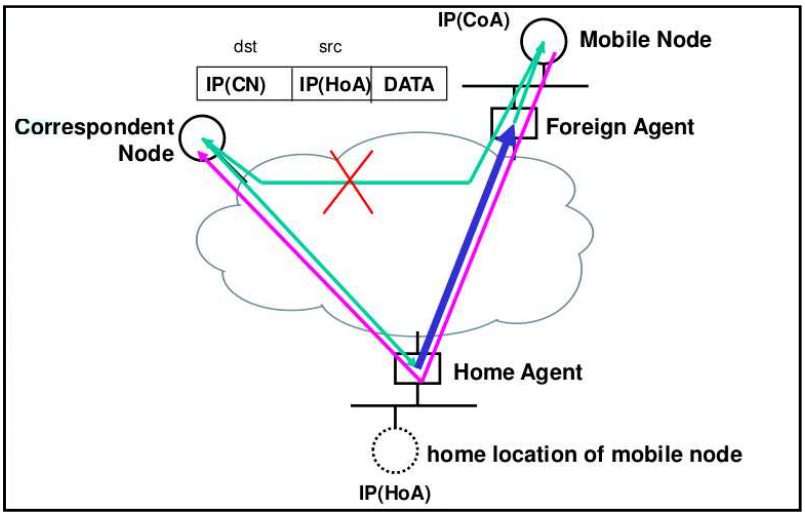
• Los paquetes enviados a la “home address” del Nodo en movimiento, son interceptados por el Home Agent y reenviados al Foreing Agent, utilizando encapsulación.

• Los paquetes enviados por el Mobile Node se entregan de dos maneras alternativas:

– Los envía al Foreing Agent y este los renvía con la “home address”. Problemas si se implementa “ingress-filtering” en el ISP.

– Crea un túnel con el Home Agent y se los reenvía.

Figura 15. Movilidad IPv6



Fuente: WALC2011 Track 2: Despliegue de IPv6 Alvaro Vives (alvaro.vives@consulintel.es)

IPv6 posee dos características importantes que ayudan enormemente en el diseño de una solución de movilidad

– Descubrimiento de Vecinos (ND. *Neighbor Discovery*)

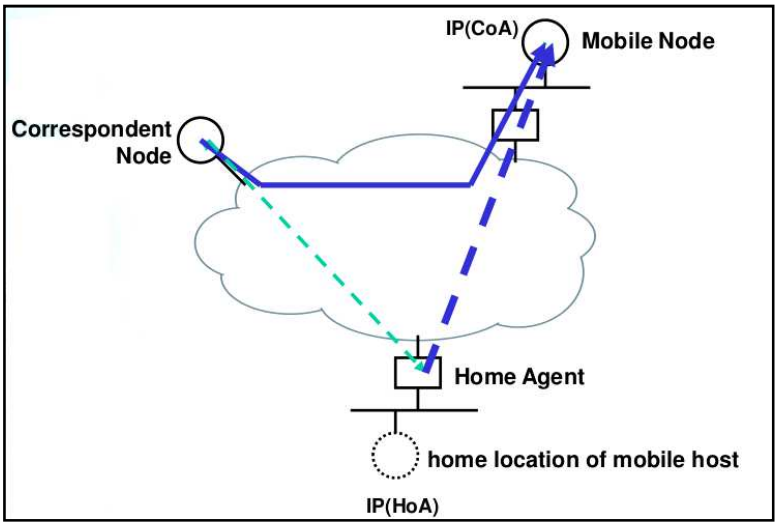
– Auto-configuración

– Se emplean para

Mobile Prefix Discovery: Similar a los RS y RA

Dynamic Home Agent Address Discovery. Puede haber más de un Home Agent

Figura 16. Movilidad IpNg



Fuente: WALC2011 Track 2: Despliegue de IPv6 Alvaro Vives (alvaro.vives@consulintel.es)

2.6. Multicast

Una dirección multicast en el protocolo IPv6 es un identificador para un conjunto de interfaces, (Típicamente en diferentes nodos). Una interfaz puede pertenecer a varios grupos multicast[7].

2.6.1. Conceptos Multicast

2.6.1.1.Multicast Distribution Tree (MDT)

– Es el camino de distribución multicast que se usa para entregar información multicast en las redes que tienen participante multicast.

– Tiene forma de árbol con el fin de evitar bucles multicast cerrados en la red

– La raíz del MDT es la fuente del grupo multicast.

[7]http://es.wikipedia.org/wiki/IP_Multicast

2.6.1.2.Shortest Path Tree (SPT)

– Es el MDT que tiene la fuente del grupo multicast como raíz y a los

participantes multicast como hojas del árbol

– Se representa como (S,G).

2.6.1.3.Shared Tree (ST)

– Es el MDT resultante de tener una única raíz, denominada “Rendezvous Point” cuando hay más de una fuente para el mismo grupo multicast.

2.6.2.Funcionamiento de Multicast

- El nodo se une/abandona un grupo multicast.
- No hay ninguna restricción acerca del número de grupos o del número de miembros por grupo.
- Enviar paquetes al grupo no significa que se pertenezca a él.
- La dirección de destino es una dirección multicast que representa a todo el grupo multicast.
- Los servicios multicast no están orientados a conexión por lo que no se puede emplear TCP.

2.6.3. Direcciones Multicast

• IPv4

– Broadcast

• Limitado: 255.255.255.255

• Dirigido: <network>11..1

– Multicast

• Clase D:

224.0.0.0 - 239.255.255.255

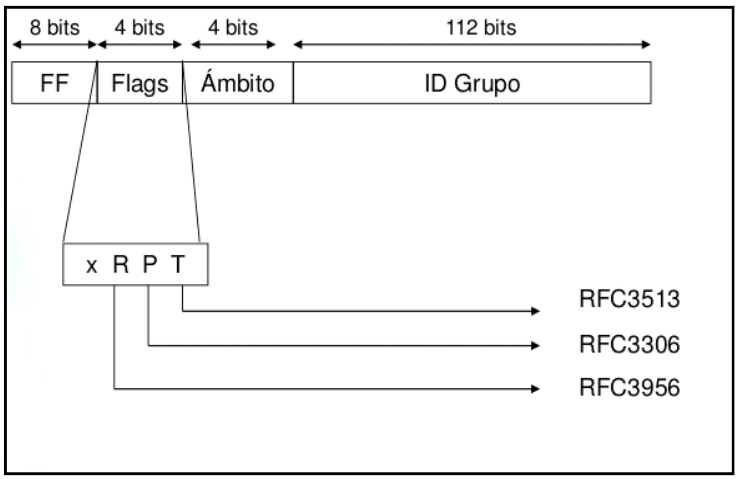
• IPv6

– Multicast

• FF....

2.6.3.1. Direcciones Multicast IPv6

Figura 17. Direcciones Multicast IPv6



Fuente: WALC2011 Track 2: Despliegue de IPv6 Alvaro Vives (alvaro.vives@consulintel.es)

• Node-Local Scope

FF01::1 Todos los nodos de la red

FF01::2 Todos los encaminadores de la red

• Link-Local Scope

FF02::1 Todos los nodos de la red

FF02::2 Todos los encaminadores de la red

FF02::4 Encaminadores DVMRP

FF02::5 Encaminadores OSPFIGP

FF02::6 Encaminadores designados OSPFIGP

FF02::9 Encaminadores RIP

FF02::B Mobile-Agents

FF02::D Todos los encaminadores PIM

FF02::1:2 Todos los DHCP-agents

FF02::1:FFXX:XXXX Solicited-Node Address

• Site-Local Scope

FF05::2 Todos los encaminadores

FF05::1:3 Todos los DHCP-servers

FF05::1:4 Todos los DHCP-relays

• Variable Scope Multicast Addresses

– FF0X::101 Network Time Protocol (NTP)

– FF0X::129 Gatekeeper

– FF0X::2:0000-FF0X::2:7FFD Multimedia Conference Calls

– FF0X::2:7FFE SAPv1 Announcements

– FF0X::2:8000-FF0X::2:FFFF SAP Dynamic Assignments

Direcciones Multicast Importantes

• FF01::1, FF02::1 Todos los nodos

• FF01::2, FF02::2, FF05::2 Todos los encaminadores

• Dirección (SN) multicast a partir de la unicast

– Si la dirección acaba en “XY:ZTUV”

– La SN es: FF02::1:FFXY:ZTUV

• Cada nodo IPv6 debe unir la dirección SN a todas sus direcciones unicast y anycast.

2.7. Mecanismos de Transición

Las técnicas que facilitan y en un futuro permitirán la transición de Internet de su infraestructura IPv4 al sistema de direccionamiento de nueva generación IPv6. Se las denomina como Mecanismos de transición. [8]

IPv6 se ha diseñado para facilitar la transición y la coexistencia con IPv4, es decir que no existe un día especificado para que se realice un "Apagón de IPv4", por así llamarlo., sino que es probable que coexistirán durante décadas.

Concretamente, hay procedimientos que permitirán a hosts conectados únicamente a IPv4 ó IPv6 acceder a recursos sólo disponibles utilizando el otro protocolo. Así tenemos:

Se han identificado técnicas, agrupadas básicamente dentro de tres categorías:[9]

1) Doble-pila, para permitir la coexistencia de IPv4 e IPv6 en el mismo dispositivo y redes.

2) Técnicas de túneles, encapsulando los paquetes IPv6 dentro de paquetes IPv4. Es la más común.

3) Técnicas de traducción, para permitir la comunicación entre dispositivos que son sólo IPv6 y aquellos que son sólo IPv4.

Todos estos mecanismos están siendo utilizados en la actualidad.

2.7.1. Doble Pila

Al incorporar IPv6 a un sistema, no se excluye la pila IPv4; es la misma aproximación multiprotocolo que ha sido utilizada anteriormente y por tanto es bien conocida (AppleTalk, IPX, etc.)

En la actualidad, IPv6 está incluido en todos los Sistemas Operativos modernos, lo que evita costes adicionales

[8]Despliegue de IPv6Día -4 Alvaro Vives

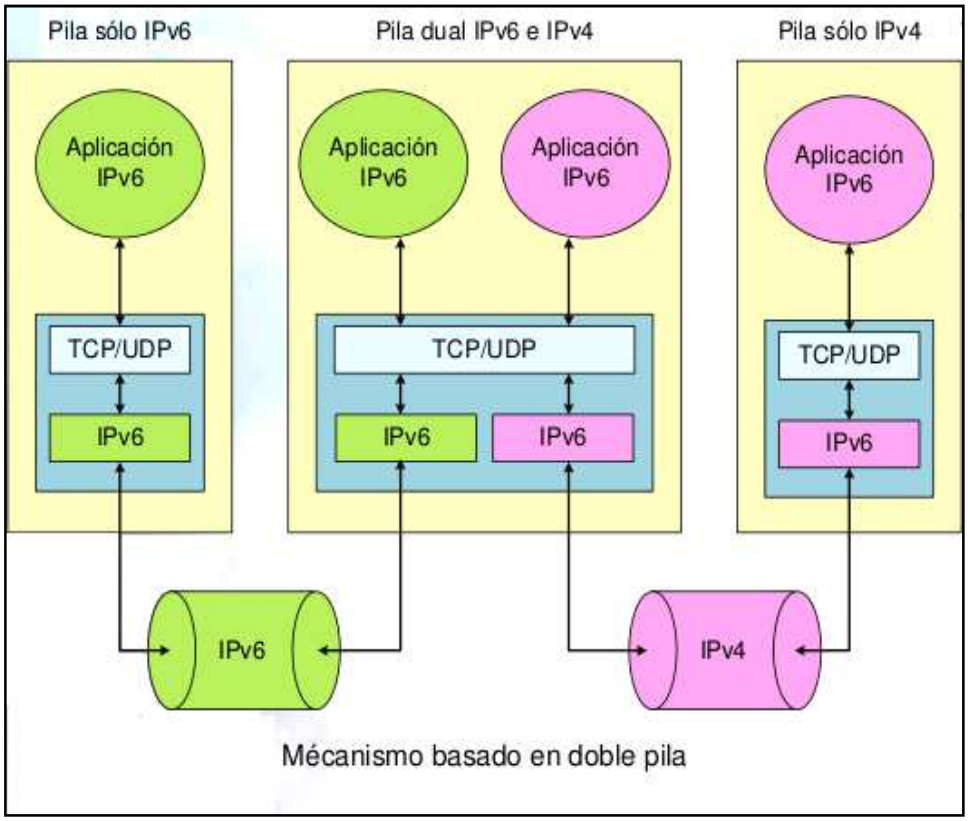
[9]http://es.wikipedia.org/wiki/Mecanismos_de_transici%C3%B3n_IPv6

Las aplicaciones (o librerías) eligen la versión de IP a utilizar, en función de la respuesta DNS, si el destino tiene un registro AAAA, utilizan IPv6, en caso contrario IPv4

La respuesta pende del paquete que inició la transferencia

Esto permite la coexistencia indefinida de IPv4 e IPv6, y la actualización gradual a IPv6, aplicación por aplicación.

Figura 18. Doble Pila



Fuente: Jordi Palet Martínez (jordi@consulintel.es)

2.7.2. Túneles

La función elemental es la de Encapsular paquetes IPv6 en paquetes IPv4 para proporcionar conectividad IPv6 en redes que solo tiene soporte IPv4.

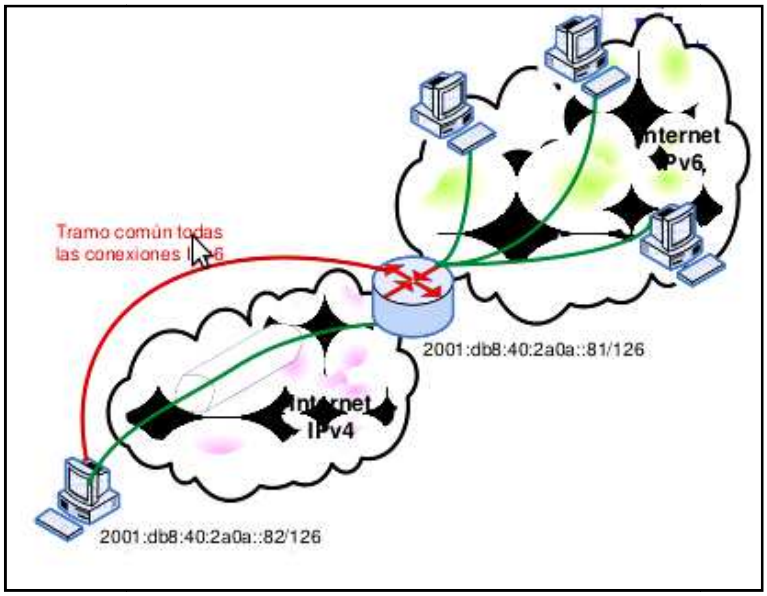
2.7.2.1. Túneles 6in4

Encapsula de manera directa el paquete IPv6 dentro de un paquete IPv4.

El túnel se considera como un enlace punto-a-punto y desde el punto de vista de IPv6 tiene solo un salto IPv6 aunque existan varios IPv4 en la que las direcciones IPv6 de ambos extremos del túnel son del mismo prefijo.

Todas las conexiones IPv6 del nodo final siempre pasan por el router que está en el extremo final del túnel.

Figura 19. Túnel 6in4



Fuente: Jordi Palet Martínez (jordi@consulintel.es)

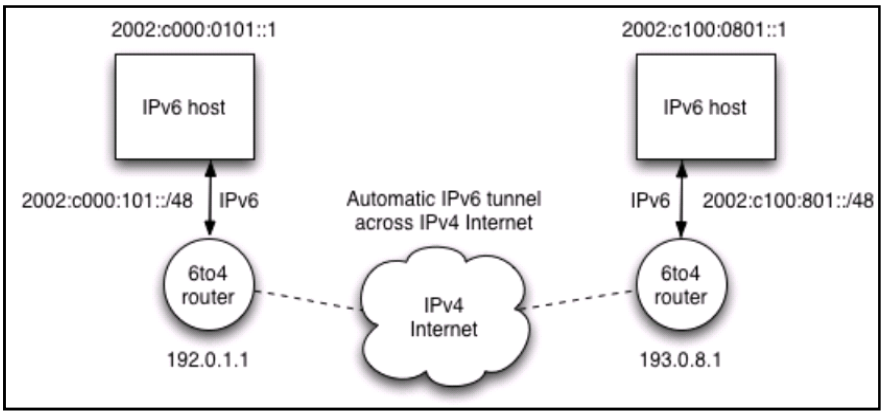
2.7.2.2. Túneles 6to4

Un Túnel 6to4 es un tunnel broker que permite envíar paquetes IPv6 sobre redes IPv4 obviando la necesidad de configurar túneles manualmente. Fue diseñado para permitir conectividad IPv6 sin la cooperación de los proveedores de internet. Este sistema puede funcionar en un router, proveyendo conectividad a toda una red, o en una máquina en particular. En ambos casos se necesita una dirección IP pública. La clave del sistema consiste en la asignación de direcciones IPv6 que contienen embebida la dirección IPv4 pública del router. Estas direcciones tienen todas el prefijo 2002::/16. De esta manera, cuando es necesario convertir un paquete IPv6 para que atraviese la

red IPv4, el router sabe la dirección a la que debe estar dirigido el paquete IPv4 generado.

Los routers que proporcionan conectividad a la red nativa en IPv6 mediante túneles 6to4 reciben el nombre de relay routers. Este elemento es el que proporciona la red del grupo de Comunicaciones de Banda Ancha para que pueda experimentar la posibilidad de conectarse a la Internet IPv6 aunque su operador no le ofrezca aún este servicio.[10]

Figura 20. Túnel 6to4



Fuente: Lacnic (Registro de Direcciones de Internet para América Latina y el Caribe)

2.7.2.3. Túneles 6RD

Este mecanismo facilita el despliegue de IPv6 dentro de la infraestructura del ISP.• Intenta corregir los problemas que se presentan en 6to4, realizando los siguientes cambios:

Se reemplaza el prefijo 2002::/16 por un prefijo que es asignado al ISP por parte de un RIR.

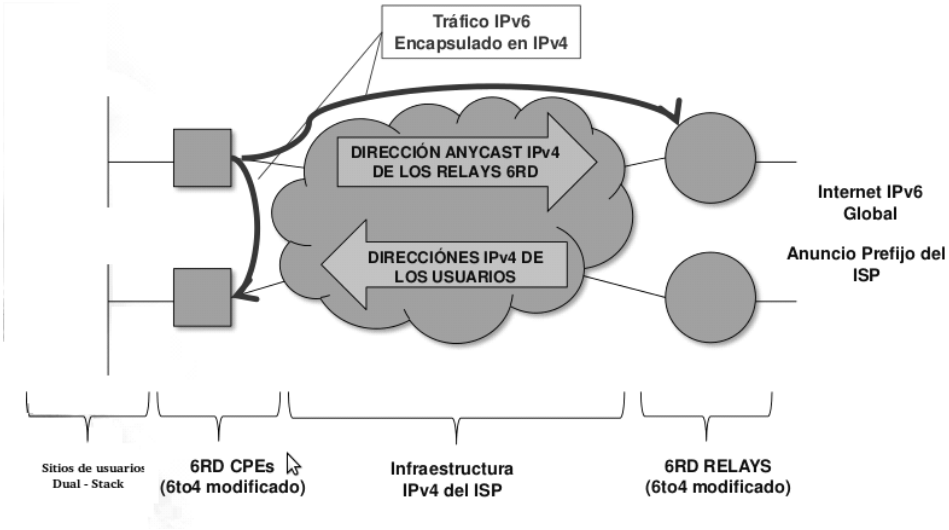
Se reemplaza la dirección anycast 192.88.99.1 por otra dirección escogida por el ISP.

El ISP despliega uno o varios Gateway 6RD (Relay 6to4) dentro de la infraestructura del ISP.

[10]http://ipv6.ccaba.upc.edu/broker.php

El ISP actualiza o provee un Home Gateway 6RD (Router 6to4).

Figura 21. Túnel 6RD



Fuente: Lacnic (Registro de Direcciones de Internet para América Latina y el Caribe)

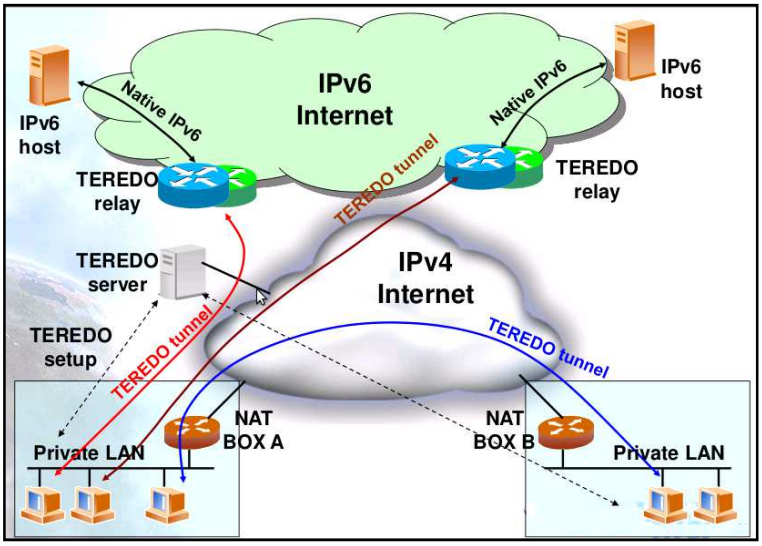
2.7.3. Teredo

Teredo es una tecnología de transición que brinda conectividad IPv6 a hosts que soportan IPv6 pero que se encuentran conectados a Internet mediante una red IPv4. Comparado con otros protocolos similares, la característica que lo distingue es que es capaz de realizar su función incluso detrás de dispositivos NAT, como los routers domésticos.

Teredo maniobra usando un protocolo de túneles independiente de la plataforma diseñado para proporcionar conectividad IPv6 encapsulando los datagramas IPv6 dentro de datagramas UDP IPv4. Estos datagramas pueden ser encaminados en Internet IPv4 y a través de dispositivos NAT. Otros nodos Teredo, también llamados Teredo relays, que tienen acceso a la red IPv6, reciben los paquetes, los desencapsulan y los encaminan.[11]

[11]http://es.wikipedia.org/wiki/Teredo

Figura 22. Teredo



Fuente: Lacnic (Registro de Direcciones de Internet para América Latina y el Caribe)

2.7.4. Softwires

Protocolo que está siendo contendido en el grupo de trabajo Softwire del IETF. Presenta las siguientes características:

1. Mecanismo de transición “universal” basado en la creación de túneles

- IPv6-en-IPv4, IPv6-en-IPv6, IPv4-en-IPv6, IPv4-en-IPv4

- Permite atravesar NATs en las redes de acceso

- Proporciona delegación de prefijos IPv6 (/48, /64, etc.)

- Autenticación de usuario para la creación de túneles mediante la interacción con infraestructura AAA

- Posibilidad de túneles seguros

- Baja sobrecarga en el transporte de paquetes IPv6 en los túneles

- Fácil inclusión en dispositivos portátiles con escasos recursos hardware

2. Softwires posibilitará la provisión de conectividad IPv6 en dispositivos como routers ADSL, teléfonos móviles, PDAs, etc. cuando no exista conectividad IPv6 nativa en el acceso

3. Posibilita la provisión de conectividad IPv4 en dispositivos que solo tienen conectividad IPv6 nativa.

2.7.5. DS-Lite

Este mecanismo procura solucionar el problema del agotamiento de IPv4, comparte (las mismas) direcciones IPv4 entre usuarios combinando Tuneling y Nat.

Para este mecanismo de transición, no hay necesidad de varios niveles de NAT.

Tenemos dos elementos principales a destacar:

– DS-Lite Basic Bridging BroadBand (B4)

– DS-Lite Address Family Transition Router (AFTR) (También llamado CGN (Carrier Grade NAT) o LSN (Large Scale NAT)).

2.7.6. Traducción

Se puede utilizar traducción de protocolos IPv6-IPv4 para:

– Nuevos tipos de dispositivos Internet (como teléfonos celulares, coches, dispositivos de consumo).

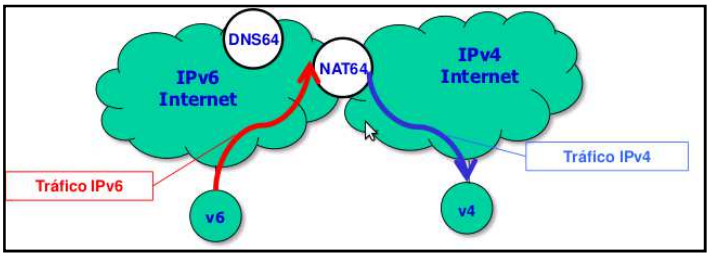
• Es una extensión a las técnicas de NAT, convirtiendo no sólo direcciones sino también la cabecera

– Los nodos IPv6 detrás de un traductor tienen la funcionalidad de IPv6 completa cuando hablan con otro nodo IPv6.

– Obtienen la funcionalidad habitual (degradada) de NAT cuando se comunican con dispositivos IPv4.

–Los métodos usados para mejorar el rendimiento de NAT (p.e. RISP) también se pueden usar para mejorar la rendimiento de la traducción IPv6-IPv4.

Figura 23. Nat 64



Fuente: Lacnic (Registro de Direcciones de Internet para América Latina y el Caribe)

Tabla 1, Resumen Mecanismos de transición.

CUADRO DE RESUMEN DE MECANISMOS DE TRANSICIÓN

MECANISMO	ACTIVIDAD	EJEMPLO
1) Doble-pila	Permite la coexistencia de IPv4 e IPv6 en el mismo dispositivo y redes.	Dual Stack
2) Técnicas de túneles, encapsulando los paquetes IPv6 dentro de paquetes IPv4. Es la más común.	Encapsula los paquetes IPv6 dentro de paquetes IPv4. Es la más común.	Túneles 6in4, Túneles 6to4, Túneles 6RD, Teredo, , Softwires, DS-Lite
3) Técnicas de traducción, para permitir la comunicación entre dispositivos que son sólo IPv6 y aquellos que son sólo IPv4.	Permite la comunicación entre dispositivos que son sólo IPv6 y aquellos que son sólo IPv4.	DNS64, NAT64

Fuente : Proaño Alulema Ricardo

2.8. QoS (Quality of Service o Calidad de Servicio)

Es un conjunto de protocolos y tecnologías que garantizan la entrega de datos a través de la red en un momento determinado. Así, nos aseguramos que las aplicaciones que requieran un tiempo de latencia bajo o un mayor consumo de ancho de banda, realmente dispongan de los recursos suficientes cuando los soliciten. Por ello, uno de las principales metas de QoS es la priorización. Esto es, el dar más relevancia a unas conexiones frente a otras.

Algunos de los beneficios que podemos obtener al implantar QoS en nuestro sistema son:

● Control sobre los recursos: podemos limitar el ancho de banda consumido por transferencias de FTP y dar más prioridad a un servidor de bases de datos al que acceden múltiples clientes.

● Uso más eficiente de los recursos de red: al poder establecer prioridades dependiendo del tipo de servicio, umbrales de tasas de transferencia.

● Menor latencia: en aplicaciones de tráfico interactivo como SSH, telnet... que requieren un tiempo de respuesta corto.

Existen varias estrategias y técnicas para llevar a cabo la aplicación de QoS, tanto software como Hardware, comerciales y de código abierto (libres). En este documento se realizará la implantación práctica de un sistema QoS sencillo bajo un entorno Debian GNU/Linux. El propósito es proveer un acercamiento práctico al manejo de las disciplinas de cola bajo Linux que permiten ordenar el tráfico de red.

Para proceder a la implantación práctica de un sistema QoS para gestionar el ancho de banda, hay que comprender cual es el camino que recorre un paquete desde que “entra” o se genera en nuestra máquina Linux (que hará las veces de router) hasta que sale a Internet u otra red; así como las diferentes disciplinas de cola también conocidas como qdiscs (Queue Disciplines) que clasifican los paquetes.[12]

Para entenderlo de mejor manera tenemos:

Calidad: Entrega fiable de datos

1. Pérdida de datos
2. Latencia
3. “Jittering”
4. Ancho de banda

[12]Bruno Herrero (mines) Última revisión: Octubre 2006

Servicio

Cualquier cosa ofrecida al usuario

1. Comunicaciones
2. Transporte
3. Aplicaciones

Existen dos arquitecturas básicas desarrolladas en IETF que son:

“Integrated Service” (int-serv)

– “Ajuste fino” (por-flujo), especificaciones cuantitativas (p.ej., x bits por segundo), usa señalización RSVP

“Differentiated Service” (diff-serv)

– “Ajuste basto” (por-clase), especificaciones cualitativas (p.ej., mayor prioridad), no hay señalización explícita.

2.8.1. Soporte QoS en IPv6

2.8.1.1.Soporte IPv6 para Int-Serv

Campo Flow Label de 20 bits para identificar flujos específicos que necesitan un tratamiento especial de QoS.

– Cada fuente especifica su propio valor de Flow Label; los encaminadores usan la Dirección Origen + Flow Label para identificar los distintos flujos

– El valor 0 en el Flow Label se usa cuando no se requiere una QoS especial, lo cual es el caso más común de momento

– Esta parte de IPv6 no está estandarizada aún y puede cambiar su semántica en el futuro.

2.8.1.2 Soporte IPv6 para Diff-Serv

Campo Traffic Class de 8 bits para identificar clases de paquetes específicas que necesitan un tratamiento especial de QoS

– Tiene el mismo significado que la definición nueva del octeto Type-of-Service en IPv4

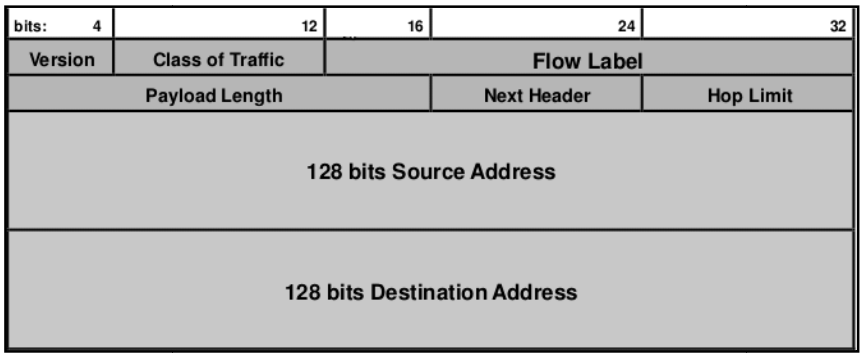
– Puede ser inicializada por un nodo o un encaminador en la ruta hacia el destino. También puede ser rescrito por cualquier encaminador en la ruta hacia el destino.

– El valor 0 en el campo Traffic Class se usa para especificar que no es necesario un tratamiento especial de QoS, lo cual es lo más común en la actualidad

2.8.1.3. IPv6 Flow Label

El campo “Flow Label” de 20 bits habilita la clasificación eficiente de flujos IPv6 basados solo en los campos principales de la cabecera IPv6 que tienen posiciones fijas.

Figura 24. IPv6 FlowLabel



Fuente: Jordi Palet Martínez (jordi@consulintel.es)

2.9. QoS sobre VoIP

El apogeo de la telefonía IP es algo indudable y la principal razón es el reaprovechamiento de los recursos y la disminución en el coste de llamadas a través de Internet.

Sin embargo, si de algo padece todavía la VoIP es de la calidad de los sistemas telefónicos tradicionales. Los problemas de esta calidad son muchos veces inherentes a la utilización de la red (Internet y su velocidad y ancho de banda) y podrán irse

solventando en el futuro. Mientras tanto, cuanto mejor conozcamos los problemas que se producen y sus posibles soluciones mayor calidad disfrutaremos.

Los principales problemas en cuanto a la calidad del servicio (QoS) de una una red de VoIP, son la Latencia, el Jitter la pérdida de paquetes y el Eco. En VoIP estos problemas pueden ser resueltos mediante diversas técnicas que se explican en los siguientes apartados.

Los problemas de la calidad del servicio en VoIP vienen derivados de dos factores principalmente:

a) Internet es un sistema basado en conmutación de paquetes y por tanto la información no viaja siempre por el mismo camino. Esto produce efectos como la pérdida de paquetes o el jitter.

b) Las comunicaciones VoIP son en tiempo real lo que produce que efectos como la pérdida de paquetes y el retardo o latencia sean muy molestos y perjudiciales y deban ser evitados.

CAPÍTULO III

3. MATERIALES Y MÉTODOS

3.1. Introducción

El presente manual es un análisis del comportamiento del tráfico de VoIP, dentro de una red con protocolo IPv6 nativo, comparado con el comportamiento del mismo en una red con IPv4, para asegurar en la medida de lo posible que se garantice un correcto funcionamiento de la llamada, se aplicarán parámetros de Calidad de Servicio, que permitan diferenciar los paquetes de voz en relación a los datos.

3.2. Objetivo de la Metodología.

El objetivo de esta metodología es la de poder analizar en qué medida la aplicación de Calidad de Servicio en una Llamada mediante el Protocolo SIP, podrán asegurar una comunicación adecuada.

La investigación a realizarse es cuasi-experimental ya que los contenidos a ser enviados en el ambiente de pruebas no serán tomados al azar, sino que se los tendrá definidos antes de realizar dicho ambiente.

3.3. Métodos, Técnicas e Instrumentos

3.3.1. Métodos

Para este proyecto se utilizaron los siguientes métodos de investigación.

Método Científico: Se utilizó este método ya que se analizaron ciertos rasgos de los protocolos propuestos para las tecnologías de VoIP, además las ideas, conceptos, y teorías expuestas en este proyecto de tesis son verificables como válidas, las mismas

que sirvieron para recopilar la información necesaria con el objetivo de encontrar la tecnología adecuada que se aplicó en el ambiente de pruebas construído.

Método Inductivo. Debido a que al observar el funcionamiento de los protocolos de VoIP, en diversos escenarios, se va a llegar a una conclusión que permita identificar las diferencias y mejoras de VoIP sobre IPv6, aplicando Calidad de Servicio, sobre la transmisión de VoIP en escenarios que no posean esta última característica.

Al estudiar en forma en el ambiente de pruebas las diferentes tecnologías y mecanismos de transición se trató de encontrar una tecnología que contenga las mejores características para la transferencia de VOIP.

3.3.2. Técnicas

Además se utilizaron las técnicas, que se indican a continuación:

- Observación
- Recopilación de información.
- Análisis
- Pruebas

3.3.3. Validación de instrumentos

Instrumentos de Medición. Según lo destaca Herrera (1998, p.16). Un instrumento de medida es la técnica o conjunto de técnicas que permiten la asignación numérica a las magnitudes de la propiedad o atributo ya sea por compara-ción con las unidades de medida o para provocar y cuantificar las manifestaciones del atributo cuando éste

es medible sólo de manera indirecta. Un instrumento debe satisfacer tres exigencias básicas:[13]

1. Detectar 'la señal' sin interferencia y, en especial, sin intervención del operador. La operación de medida es la interacción objeto de medida-instrumento, por tanto el interés no es ya el objeto de medida sino el complejo objeto-instrumento.

2. No provocar reacción en el objeto de medida o, de ser así, tal reacción debe ser calculable.

3. Basarse en supuestos determinados sobre la relación entre la propiedad y el efecto observado.

Actualmente existen tres teorías bien delineadas para la validación de instrumentos y estas son: Teoría de Respuesta al Ítem (ver Hambleton, Swaminathan y Rogers, 1991; Muñiz, 1997), Teoría dela Generazabilidad (ver Cronbach, Gleser, Nanda y Rajaratnam, 1972; Shavelson y Webb, 1991), y Teoría Clásica de los Test (Brown, 1980; Nunally, 1987; Thorndike, 1989). La última de estas tres teorías es la que sustenta la mayor parte de los instrumentos de medición existentes, por tal motivo será la expuesta en este documento.

Teniendo en cuenta que lo deseable de un instrumento de medición es que permita realizar mediciones consistentes y precisas, los errores afectan las propiedades las propiedades o variables (Confiabilidad y Validez). A continuación se exponen los aspectos conceptuales de cada una de ellas así como los principales procedimientos para estimarlas y por ende identificar la calidad del instrumento usado en el proceso de medición (Hogan, 2004).

Confiabilidad. Se define como la cantidad de la varianza presente en los resultados de la medición que se debe a diferencias reales en la magnitud de atributo medido, o en otras palabras, es la proporción de varianza observada que es varianza verdadera.

13

Documento elaborado por Juan Carlos Espinosa Méndez miembro del Equipo Interdisciplinario de la Universidad Nacional de Colombia, coordinado por José Ignacio Ruíz, para la Subdirección de Evaluación y Tratamiento del INPEC en el marco del Convenio Interadministrativo de Cooperación Académico-Científico No. 29 de 2008

Existen diferentes procedimientos para estimar la confiabilidad de un instrumento de medición, los más populares son estabilidad, equivalencia y consistencia interna.

Validez Según Hogan (2004) indica que los criterios de aplicación y calificación claros y exactos al igual que altos niveles confiabilidad son deseables en un instrumento, pero que lo más importante es la validez.[14]

En ese sentido, la validez es la proporción de varianza observada que es producida por diferencias individuales reales en el atributo que se pretende medir.

Teniendo en cuenta los aspectos antes mencionados, las herramientas que se han escogido para esta delicada tarea dentro del presente proyecto de investigación son Wireshark y Network Miner, así como también Mausezahn para generar tráfico, ya que cumplen a cabalidad los puntos citados en el inicio de este inciso.

Wireshark y NetworkMiner en el caso de sniffers y Mausezahn como generador de tráfico, a pesar de ser programas gratuitos (GPL) son muy difundidos entre profesionales, estudiantes y maestros que de una u otra forma requieren de un análisis de tráfico de datos confiable y completamente seguros, no se los detalla porque la lista sería interminable; así como también el someter a una red a las más altas exigencias con el objeto de probar el rendimiento de soluciones que puedan resolver problemas cotidianos que día a día se presentan en las transmisiones de datos.

Existen otras herramientas como Snort, OSSIM así como multitud de IDS/IPS permiten alertar sobre algunos de los problemas y ataques expuestos en una red. No obstante, cuando se necesita analizar tráfico en profundidad o hay que auditar un entorno en el que el tiempo prima, dichas herramientas suelen carecer de la flexibilidad que nos ofrece un analizador de protocolos como Wireshark o Network Miner.[15]

[14] Validación de Instrumentos: http://extension.upbbga.edu.co/inpec2009/Estudiosprimeraparte/VYEInstrumentos.pdf
[15] INTECO-CERT Febrero 2011

3.3.3.1. Wireshark.

Se utilizó Wireshark ya que es utilizado por muchas empresas, universidades, institutos. El programa posee la ventaja de ser gratuito y de código abierto desarrollado por un equipo internacional de desarrolladores de redes.[16]

3.3.3.2. NetworkMiner.

Es una herramienta forense de análisis de redes para Windows (posible emulación en GNU/Linux con Wine). El propósito de NetworkMiner es recolectar información (como evidencia forense) sobre los hosts de la red en vez de recoger información concerniente al tráfico de la red. Puede ser usado como esnifer pasivo/herramienta de captura de paquetes con el objetivo de detectar detalles específicos del host como sistemas operativo, hostname, sesiones, etc. sin generar ningún tráfico en la red.

Para la identificación del sistema operativo se basa en paquetes TCP SYN y SYN+ACK haciendo uso de la base de datos de p0f y Ettercap. También puede realizar fingerprinting del S.O por medio de paquetes DHCP (generalmente paquetes broadcast) apóyandose en la base de datos de Satori.

3.3.3.3. Generador de tráfico

Mausezahn (en alemán "dientes de ratón") es un generador de tráfico escrito en C para Linux, muy versátil y rápido, que nos permitirá generar y enviar prácticamente todos los paquetes posibles (e imposibles) con una sintaxis bastante sencilla.

Aunque es relativamente nuevo, se utilizó este generador de tráfico ya que es muy utilizado para probar VoIP o redes multicast, aunque también puede usarse en auditorías de seguridad para chequear si los sistemas están suficientemente fortificados o, en mi caso, como otra interesante herramienta para comprobar los IDS, SIEM y demás elementos de seguridad perimetral.

[16] http://www.mipaginapersonal.movistar.es/web3/alypso/PracticaWireshark.pdf

Al tratarse de Voz sobre IP se trata de generar tráfico IP desde una terminal virtualizada con Ubuntu con el siguiente comando:

#sudo mz –c 0 –t ip –p 1024 –B ip destino –d 2m

Al enviar tráfico tanto IPv4 como IPv6 hacia un terminal con Windows 7 se obtiene lo que se indica en el ***Anexo 6.***

3.4. Implementación del entorno de Pruebas

Para la realización del presente proyecto, se utilizaron conjuntamente elementos de software y hardware, que permitieron la implementación exitosa del entorno de pruebas, que brinda una calidad aceptable en las transmisiones de VoIP. Sumado esto, se utilizaron aplicaciones de software libre, que permitieron minimizar costos y además otorgaron flexibilidad en el proceso de configuración y actualización del sistema en general.

3.4.1. Requerimientos de software y hardware para el entorno de pruebas.

A continuación se presenta un listado de los elementos de software y hardware utilizados en el presente escenario de pruebas.

Hardware

- 2 Equipos de cómputo PCs (Servidores asterisk)
- 2 Equipos de cómputo PCs (Routers, servicios XAAMP, QoS)
- 1 Switch
- 1 Hub (Para monitoreo de red)
- 1 regulador de energía
- Cable UTP
- Conectores RJ45

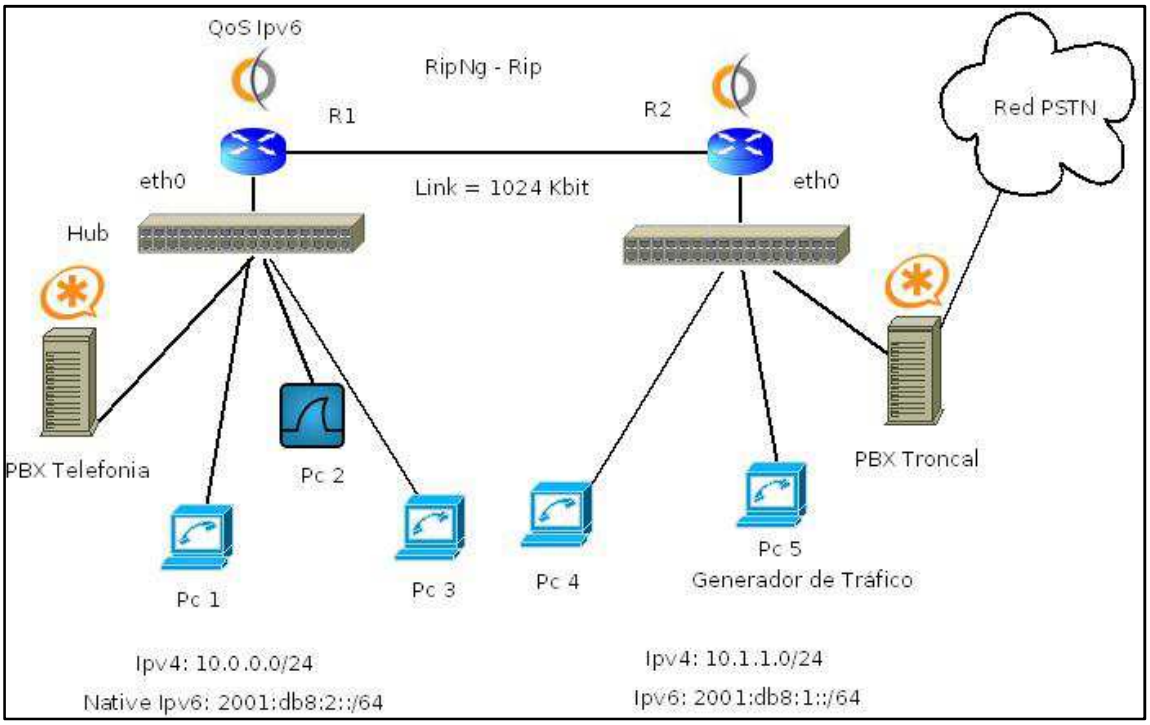
- Cable telefónico
- Conectores RJ11
- Dos pares de dispositivos de E/S (Micrófonos, auriculares)
- Softphones (Laptops)
- Tarjeta TDM Digium FXO, FXS

Software

- Sistema operativo Linux distribución CentOs 5.6
- Software para VoIP Asterisk 1.8
- Software de monitoreo y tráfico “wireshark”
- Software para cliente SIP Linphone – SIP Comunicator (jitsi)
- Driver Dahdi-complete 2.0
- Software de Ruteo Vyatta
- Generador de tráfico basado en C “Mausezahn”

Direccionamiento del Entorno de Pruebas

Figura 25. Escenario General



Fuente: Proaño Ricardo Xavier

Red Telefonía

Tabla 2. Direccionamiento de la Red Telefonia

	IPv4	**IPv6**
R1	10.0.0.1 /24	2001:db8:2::1 /64
PBX Telefonia	10.0.0.4 /24	2001:db8:2::4 /64
Pc1	10.0.0.65 /24	2001:db8:2::100 /64
Pc2 (Wireshark)	10.0.0.66 /24	2001:db8:2::98 /64
Pc3 /Virtualizado)	10.0.0.34 /24	2001:db8:2::34 /64

Fuente: Proaño Ricardo Xavier

Red Troncal

Tabla 3. Direccionamiento de la Red Troncal

	IPv4	IPv6
R2	10.1.1.1 /24	2001:db8:1::1 /64
PBX Troncal	10.1.1.4 /24	2001:db8:1::4 /64
Pc4	10.1.1.25 /24	2001:db8:1::100 /64
Pc5 (Virtualizado)	10.1.1.7 /24	2001:db8:1::67 /64

Fuente: Proaño Ricardo Xavier

3.4.1.1. Configuración del Sistema Base

Para la configuración de los servidores de VoIP se escogió el Sistema Operativo CentOs 5.6, ya que es una distribución de Linux basada en fuentes disponibles de Red Hat Enterprise y cada versión es mantenida durante siete años a través de actualizaciones de seguridad. Es un sistema operativo muy utilizado en entornos de computación cuyo uso es destinado a la utilización de servidores de multiples usos.

3.4.1.2. Asterisk 1.8

Se eligió usar Asterisk ya que es una herramienta líder a nivel mundial ello que correspondiente a servicios de telefonía IP utilizando software libre, brindando la flexibilidad que no existe al usar un software propietario.

Es una aplicación de Open Source basada en GPL que fue desarrollada en 1999 por Mark Spencer de la empresa Digium, nos permite configurar una central

telefónica privada para establecer comunicaciones en tiempo real, a través de la implementación de protocolos estándares que la tecnología VoIP nos ofrece.

Entre sus principales ventajas tenemos su versatilidad y flexibilidad para adaptarse a las necesidades de cualquier organización, permitiendo la instalación y configuración de varios tipos de servicios.

En la actualidad existen varias implementaciones llamadas “tres en uno” como Trixbox, Asterisk Now y Elastix, que son de distribución libre e integran el Sistema Operativo CentOs, Asterisk y un administardor web de la Central telefónica.

Asterisk tiene soporte para muchos teléfonos IP y softphones, actuando como pasarela de conexión hacia a PSTN. Esto se logra utilizando tarjetas con interface FXO, diseñada para conectar líneas analógicas desde la PSTN; y una interfaz FXS, que permiten conectar un teléfono analógico para así convertirlo en un teléfono IP.

3.4.1.3. Dispositivos y software utilizado en clientes VoIP

Un softphone es la aplicación informática que forma parte de un entorno VoIP, y puede estar basada en protocolos estándares y propietarios. Los softphones son herramientas que tienen funciones tales como: conferencias entre dos o más líneas, grabación de llamadas, agendas de contactos, registros de llamadas, etc.

Para la realización de las pruebas se utilizó el softphone Linphone 3.5.2, que es de licencia libre, que tiene la finalidad de simular un teléfono convencional por computadora, y permite establecer llamadas mediante el protocolo SIP a otros softphones o teléfonos IP, registrados en nuestro servidor.

3.4.1.4. Vyatta

Se escogió Vyatta por ser un open flexible router (OFR) 1.0 que puede ser utilizado en lugar del equipamiento de Routing comercial tanto en pequeñas empresas como en organizaciones con miles de usuarios.[17]

Tabla 4. Comparación de servicios soportados por algunas distribuciones

Distribución	Servicios	Puntos
Smoothwall	Router/ firewall distribution with a web interface and light terminal	2
Vyatta	Multiple SSID/VLAN/WLAN/QOS/LIVE CD/Clase c router, firewall,VPN,IPv6, servicios LAN avanzado/vFirewwall /vRouter/network virtualization functionaly /routing dinámico/router/firewall/QoS/Wifi/Multiple SSID/Radius/Autentication /Zeroshell/VLAN/bridging/WAN/Load balancing	21
Zentyal	Router /Firewall and small officce server	2
Zeroshell	Router/Firewall/QoS/Wifi/Multiple SSID/RADIUS Autentication/Zeroshell/Vlan/bridging/Wan/Load balancing	10

Fuente: Martinez, Mendieta, Landino

En razón a su mayor robustez como se vé en la *Tabla 4*, se utilizó Vyatta para el desarrollo del proyecto.

Ya es muy popular la telefonía IP en Open-source con Asterisk, y toda la libertad de creación que proporciona una herramienta de Software Libre. Pues bien, así como Asterisk está liderando y enfrentándose a equipos propietarios como CISCO, NORTEL o AVAYA, al mismo paso que se abre campo como una solución optima

[17]Implementación y configuración de un enrutador para la interconexión de la red de tecnología avanzada RITA-UD con la red metropolitana rumbo mediante software libre y el modelo TMN de la UIT-T
Carlos Andres Martínez / Fabio Antonio González Mendieta / Dora Andrea Antolínez Ladino

para redes de comunicación de voz, existe otra solución Open-source que se está abriendo camino en las redes de comunicación de datos y esta es Vyatta, y está buscando directa competencia con CISCO. Vyatta es basado en Linux, preparado especialmente para realizar funciones de ruteo, vpn, firewall e incluso para trabajar como maquina virtual. Vyatta está hecho para trabajar en hardware x86 (Computadores Personales) y siendo así tiene mayor capacidad de procesamiento que los procesadores de los routers CISCO en los cuales corre el IOS CISCO. La alternativa de poder usar Software que no sea propietario sobre Hardware que podemos adquirir con mucha facilidad como computadoras de medio uso, hace que se reduzcan costos en la implementación, por otra parte la línea de comandos es diferente a la de un Linux y a la del IOS de CISCO, es más como un hibrido de estas dos, también cuenta con una interface web para administración.

Para nuestros escenarios se utilizó el protocolo de Ruteo RIP (Protocolo de Información de Enrutamiento) para IPv4, y RIPNG (Protocolo de Información de Enrutamiento Nueva Generación) para IPv6. El mismo que se considera como una excelente alternativa en los entornos de redes por la gran flexibilidad que presenta en su sencillez y eficacia, un estudio realizado por Octavio Salcedo Parra en su "Análisis y Evaluación del Routing Information Protocol RIP"[18], presenta sus ventajas, mismas que son por demás útiles a la hora de implementar el presente proyecto.

Las Políticas de QoS utilizadas fueron:

Traffic-Shaper basadas en el algoritmo Token Bucket Shaping para la selección del tráfico RTP

Rate Control (control de índice o tasa) para establecer el límite de ancho de banda, este es un algoritmo de planificación. Provee colas basadas en el algoritmo de Token Bucket Filter. Este algoritmo solamente pasa paquetes que llegan a una velocidad o tasa que no excede la tasa administrativamente fijada. Es posible, sin embargo, sobrepasar esta tasa para ráfagas cortas de tráfico.

[18]Salcedo Parra, Octavio J.Hernández, Cesar; Manta C., Hector C.. "*Analisis y evaluación del routing information protocol RIP*". Tecnura27 (2010)

3.5. Archivos principales de configuración

3.5.1. Configuración de servidor CenTOs 5.6

Archivo: /etc/host.conf

. order host, bind
. multi on

Archivo: /etc/hosts

::1
2001:db8:2::4 telefonia.com

Archivo: /etc/sysconfig/network

.networking=yes
.networking_IPv6 = yes
.hostname=telefonia.com
.IPv6forwarding = yes

Archivo /etc/resolv.conf

.nameserver telefonia.com
.dns1= 2001:db8:2::4
.dns2= 2001:db8:2::5

Para permitir el tráfico VoIP entre los servidores y que estos puedan registrar las direcciones SIP, se deben abrir los puertos de iptables y de ip6tables, que son los archivos que definen las reglas de firewall.

-A RH-Firewall-1-INPUT –p udp –m udp – - dport 5060 –j ACCEPT

-A RH-Firewall-1-INPUT –p udp –m udp – - dport 4569 –j ACCEPT

-A RH-Firewall-1-INPUT –p tcp - –dport 5038 –j ACCEPT

3.5.2. Instalación y configuración de Asterisk

Antes de instalar Asterisk en nuestro servidor, es necesario verificar que la versión y las fuentes del kernel estén instaladas y actualizadas para evitar errores de compilación e instalación de este software.

Para verificar la versión del kernel digitamos el comando : *uname –r*

Para instalar y actualizar las fuentes del kernel y sus cabeceras se ejecuta el comando:

 # yum install kernel kernel-devel kernel-headers

Para una actualización total de los repositorios se utiliza el comando:

#yum update

La instalación de librerías necesarias para la compilación de las fuentes de Asterisk se realiza con el comando:

#yum install gcc ncurses ncurses-devel make gcc-c++ libtermcap libtermcap-devel zlib zlib-devel libtool bison bison-devel openssl-devel bzip2 bzip2-devel wget newt newt-devel libxml2 libxml2-devel

Creación del Directorio de asterisk

Cd /usr/scr

ns:~# cd /usr/src/

ns:~# wget -c http://downloads.digium.com/pub/telephony/dahdi-linux-complete/dahdi-linux-complete-2.6.0+2.0.0.tar.gz

ns:~# tar xvzf dahdi-linux-complete-2.6.0+2.6.0.tar.gz

ns:~# cd dahdi-linux-complete-2.6.0+2.6.0

ns:~# make

ns:~# make install

ns:~# make config

ns:~# dahdi_cfg –v

Archivos de configuración de Asterisk

La configuración de Asterisk es la misma tanto en la Troncal como en la que se encuentra en el edificio matriz.

Ver Anexo 1. Configuración de Archivos principales de Asterisk

Visualización de canales Dahdi mediante el comando:

*Troncal*CLI> dahdi show channels*

Figura 26. Canales FxO – FxS de la tarjeta Digium

Chan	Extension	Context	Language	MOH Interpret	Blocked	State
pseudo		default	default			In Service
1		from-pstn	default			In Service
2		from-pstn	default			In Service
3		from-pstn	default			In Service
4		from-pstn	default			In Service

Fuente: Proaño Ricardo Xavier

3.5.3. Configuración de Routers

Dentro de las herramientas de QoS implementadas, y al desarrollarlas en ambiente de Software Libre, se utilizaron políticas de tráfico saliente: Traffic Shaper y Rate Control, del software de ruteo Vyatta (Linux BSD).

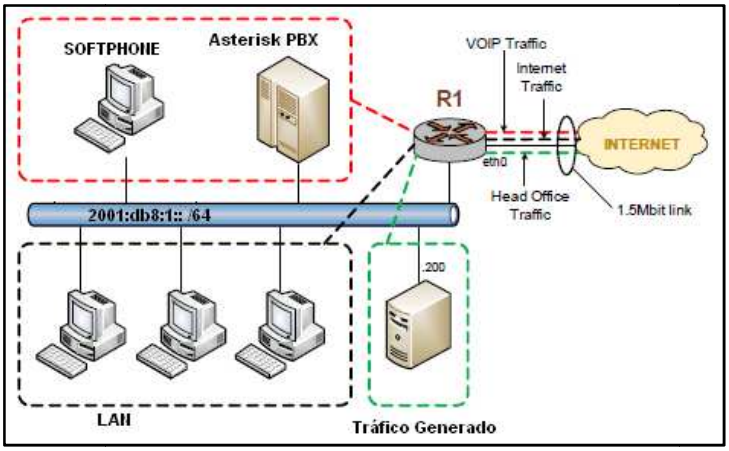
Traffic-shaper (moldeador de tráfico) este algoritmo provee colas basadas en Token Bucket el mismo que es muy similar a round-robin pero no es tan estricto ya que permite que los recursos no usados por una clase de tráfico sean tomados por otra que los necesita. El algoritmo de Shaper al igual que round-robin limita el uso del ancho de banda por clases pero realoja y distribuye el ancho de banda sobrante.

El mecanismo de la política de tráfico Rate-Control (control de índice o tasa) es un algoritmo de planificación. Provee colas basadas en el algoritmo de Token Bucket Filter. Este algoritmo solamente pasa paquetes que llegan a una velocidad o tasa que

no excede la tasa administrativamente fijada. Es posible, sin embargo, sobrepasar esta tasa para ráfagas cortas de tráfico. Se utilizó este algoritmo para simular un enlace de 1024 Kbps , tanto de subida como de bajada.

En el siguiente gráfico podemos observar un ejemplo de Traffic Shaper, operando de la siguiente manera: Las líneas de color Rojo representan el tráfico VoIP, las líneas de color Verde el tráfico de saturación y las líneas de color Negro el tráfico de internet (WAN).

Figura 27. Ejemplo de Traffic Shaper



Fuente: Proaño Ricardo Xavier

Ver Anexo 2. Configuración de Routers Vyatta

Ver Anexo 3. Configuración de cancelador de eco por hardware

3.6. Operacionalización Conceptual

Tabla 5 Operacionalización Conceptual

VARIABLE	TIPO	DEFINICION
La aplicación de QoS sobre IPv6	INDEPENDIENTE	Es nueva versión del protocolo de redes de datos en los que Internet esta basado. El IETF (Internet Engineering Task Force) QoS o Calidad de Servicio (Quality of Service, en inglés) son las tecnologías que garantizan la transmisión de cierta cantidad de información en un tiempo dado (throughput)
transmisión de VoIP	DEPENDIENTE	VoIP. Grupo de recursos que hacen posible que la señal de voz viaje a través de internet empleando un protocolo IP

Fuente: Proaño Ricardo Xavier

3.7. Operacionalización Metodológica

Tabla 6. Operacionalización Metodológica

VARIABLE	INDICADORES	TECNICA	INSTRUMENTOS
La aplicación de QoS sobre IPv6	Ancho de banda Políticas de QoS	Pruebas Configuración Razonamiento Intuición	Recopilación de Información Wireshark, NetwokMiner
transmisión de (VoIP)	Ancho de Banda Paquetes perdidos Latencia Jitter	Pruebas Configuración Comparación Razonamiento Intuición	Sniffer (Wireshark, NetworkMiner)

Fuente: Proaño Ricardo Xavier

3.8. Datos de Prueba

Se establecieron seis escenarios de pruebas para la obtención de los datos en base a los siguientes requerimientos que no deben faltar en una red de datos según la norma ETSI TS 123 107 V7.1.0 (2007-10), y que se describen en la *Tabla 7*

Tabla 7. Parámetros de calidad en un canal de banda ancha fija

Parámetros de Calidad en la banda ancha fija	
Magnitud	**Criterio**
Disponibilidad	Mayor o igual a 99% (equivalente a 7,2h de interrupción o menos cada mes)
Flujo/Velocidad Media	Media mayor que 60% del flujo/velocidad máxima contratada
Flujo/Velocidad Instantánea	Valor instantáneo mínimo de 20% del flujo/velocidad máxima contratada
Pérdida de Paquetes	Perdida máxima del 2% del volumen de dados enviados
Latencia unidireccional	Valor máximo de 40 milisegundos
Latencia Ida y Vuelta (RTT)	Valor máximo de 80 milisegundos
Jitter	**Variación máxima de 50 milisegundos**
Tiempo para establecimiento de conectividad IP	Tiempo máximo de 1 minuto
Número de intentos para establecer la conectividad IP	Máximo de 2 intentos
DNS - tiempo de respuesta del servidor recursivo	Máximo de 80 milisegundos
DNS - obediencia al campo TTL	El Servidor recursivo debe obedecer al campo TTL
DNS - respuesta a una consulta a una dirección inexistente	El Servidor recursivo debe responder que la dirección no existe
DNS - posibilidad de consulta al servidor autoritativo	El cliente debe recibir una respuesta a la consulta
DNS - posibilidad de consulta al servidor autoritativo	En el log del servidor autoritativo debe poderse verificar que hubo consulta del cliente, permitiendo comprobar que no existe un proxy DNS transparente en la red
Tempo de Instalación del servicio	7 (siete) días
Ancho de banda en un canal de voz	32 Kbps
Tempo de cancelación del servicio	Período máximo de 30 días.

Fuente: Anatel, CGI.Br e Inmetro analisam qualidade da banda larga fixa, 11 de mayo de 2010

De donde se resaltan los Indicadores presentados en la Variable Dependiente.

Tabla 8. Indicadores de la variable dependiente

Pérdida de Paquetes	Perdida máxima del 2% del volumen de dados enviados
Media de Latencia unidireccional y RTT	Valor máximo de 60 milisegundos
Jitter	**Variación máxima de 50 milisegundos**
Ancho de banda en un canal de voz	**32 Kbps para un canal de ida o vuelta**

Fuente: Proaño Ricardo Xavier

Se tomará un valor promedio en el caso del Jitter de 60 milisegundos

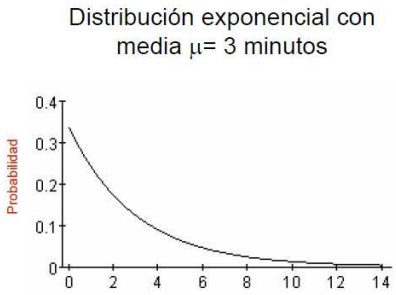
En el caso de la **duración de la llamada**, para el caso de telefonía vocal, según ATEL ASESORES C.A y su obra "Tráfico en Redes de Telecomunicaciones "elaborado por . Diógenes Marcanose[19], se considera que tiene un comportamiento como el de una distribución exponencial negativa.

La distribución exponencial. Interpretación: la cantidad de llamadas de duración x viene dada por:

$$P(X = x) = \frac{1}{\mu} e^{-x/\mu}$$

La probabilidad de que la duración de las llamadas sea x, viene dada por P(X=x).

La media y la varianza son iguales a μ = 3 minutos



Por lo cual el tiempo de llamadas para las pruebas realizadas fue de tres minutos.

[19] *ATEL ASESORES C.A IMS Prof. Diógenes Marcano. Fundamentos de IMS*

El direccionamiento en el caso de IPv6 se escogió el prefijo 2001, por tratarse de un rango establecido únicamente para documentación, y una máscara /64.[20]

3.9. Tamaño de la muestra y número de repeticiones en el diseño experimental.

El número de réplicas (repetición de un experimento), que en otro contexto puede referirse a la repetición o duplicación de un experimento para confirmar o verificar los resultados. En el presente proyecto, este concepto tiene dos propiedades importantes.
En primer lugar, permitió obtener una estimación del error experimental, la misma que se convirtió en la unidad básica para determinar si las diferencias observadas en los datos fueron estadísticamente significativas.
El número de repeticiones del experimento o el número de llamadas realizadas, se determinó por la cantidad promedio de llamadas obtenidas en el rango de una hora pico que se expresa en el artículo Fundamentos de IMS de Diógenes Marcano, el mismo que ha servido para determinar otro parámetro importante de los escenarios planteados como es el ancho de banda promedio de una empresa (PYME), los datos obtenidos se resumen en la siguiente tabla.

Tabla 9. Número de llamadas recibidas en hora pico(10:00-11:00)

Parámetro	Cuantificador
Número de llamadas en una hora pico	180
Canal de datos de un cliente corporativo promedio	1024 Kbps compartición 1:1
Hora Pico	10:00 a 11:00

Fuente : Proaño Ricardo Xavier.

El Cálculo del tráfico promedio A (Earlang) se lo ha realizado en base a dos factores importantes:

1.- La tasa de llegada de sesiones de comunicaciones Q [sesiones/s,sesión/min, sesión/hr]

2.- La duración promedio de cada sesión μ [seg o min]

[20]IPv6 para todos, guía de uso y aplicación para diversos entornos, pág 101

$A = \mu * Q$[21]

De donde se obtiene los siguientes resultados:

A = 180 llamadas en hora pico * 3 minutos (valor de llamada promedio validado anteriormente)

A= 3 llamadas por minuto * 3 minutos

A = 9

El número de repeticiones será de 9 y lo haremos en base a este resultado para cada escenario.

El software utilizado para la comunicación entre terminales fue Jitsi y Linphone, herramientas de software libre que poseen algunas configuraciones que permiten inclusive dotar de más seguridad a la comunicación de VoIP. Mismas que se utilizaron al no poder contar con teléfonos IP por su elevado costo.

Cabe señalar que las muestras tomadas corresponden a terminales que recibieron el ataque de desbordamiento de tráfico IP con el generador de tráfico Mausezahn, escrito en C para Linux, muy versátil y rápido, que permitirá generar y enviar prácticamente todos los paquetes posibles (e imposibles) con una sintaxis bastante sencilla. Se satura la red, siendo ésta de un ancho de banda de 1024 Mbps tanto de subida como de bajada***. (Anexo 6)***

Para las pruebas se establecieron los siguientes escenarios:

- Escenario 1. IPv4 sin QoS en la Red de Área Local (LAN)
- Escenario 2. IPv4 sin QoS desde la red de telefonía pública (PSTN)
- Escenario 3. IPv6 sin QoS en la Red de Área Local (LAN)
- Escenario 4. IPv6 sin QoS desde la red de telefonía pública (PSTN)
- Escenario 5. IPv6con QoS en la Red de Area Local (LAN)

[21]ATEL ASESORES C.A IMS Prof. Diógenes Marcano. Fundamentos de IMS

- Escenario 6. IPv6 con QoS desde la red de telefonía pública (PSTN)

Se usaron códec tipo G711 para audio en los servicios VoIP.

CAPÍTULO IV

4. RESULTADOS Y DISCUSIÓN

A continuación se detallan los resúmenes de cada una de las llamadas realizadas en los escenarios de pruebas, en base a los indicadores de la variable Dependiente.

Los datos obtenidos en cada Escenario, se detallan en el ***(Anexo 5)***

Escenario 1. IPv4 sin QoS en la Red de Área Local (LAN)

Se realizaron nueve llamadas con una duración promedio de 3 minutos (el mismo que se toma a partir de la saturación de la red), en el que se genera tráfico Tcp con el software Mausezahnn, utilizando el protocolo **IPv4 sin QoS en la Red de Área Local (LAN),** los datos recopilados se obtuvieron con el analizador de tráfico Wireshark y corroborados con NetworkMiner **(Anexo 5).**

En la siguiente tabla, se detallan los Parámetros del escenario, en base al direccionamiento descrito en las *Tabla 2* y *Tabla 3*:

Tabla 10. Direccionamiento Escenario 1

ORIGEN	DESTINO
Pc4 (Inicia Llamada)	Pc1(Recibe Llamada)
Pc4 (Genera Tráfico FTP)	Pc1 (Recibe Tráfico FTP)
Pc5 (Genera Tráfico IP)	Pc1(Recibe Tráfico IP)
Pc2 (Analiza el tráfico de la red)	

Fuente: Proaño Ricardo Xavier

A continuación se muestran los datos obtenidos en el Pc1

Resumen de la Llamada No 1.

Tabla 11. Resumen de la Llamada No 1 . Escenario 1

Ancho de Banda Kbps	Paquetes esperados	Paquetes Perdidos	Porcentaje de paquetes perdidos %	Latencia (ms)	Jitter (ms)
12	6223	2275	21	245	130

Fuente: Proaño Ricardo Xavier

Resumen de la Llamada No 2.

Tabla 12. Resumen de la Llamada No 2 . Escenario 1

Ancho de Banda Kbps	Paquetes esperados	Paquetes Perdidos	Porcentaje de paquetes perdidos %	Latencia (ms)	Jitter (ms)
13	6223	1367	22	123	135

Fuente: Proaño Ricardo Xavier

Resumen de la Llamada No 3.

Tabla 13. Resumen de la Llamada No 3 . Escenario 1

Ancho de Banda Kbps	Paquetes esperados	Paquetes Perdidos	Porcentaje de paquetes perdidos%	Latencia (ms)	Jitter (ms)
16	6850	2084	30,4	126	133

Fuente: Proaño Ricardo Xavier

Resumen de la Llamada No 4

Tabla 14. Resumen de la Llamada No 4 . Escenario 1

Ancho de Banda Kbps	Paquetes esperados	Paquetes Perdidos	Porcentaje de paquetes perdidos %	Latencia (ms)	Jitter (ms)
15	6131	1380	22,5	116	145

Fuente: Proaño Ricardo Xavier

Resumen de la Llamada No 5

Tabla 15. Resumen de la Llamada No 5 . Escenario 1

Ancho de Banda Kbps	Paquetes esperados	Paquetes Perdidos	Porcentaje de paquetes perdidos %	Latencia (ms)	Jitter (ms)
17	6306	1531	24,3	166	140

Fuente: Proaño Ricardo Xavier

Resumen de la Llamada No 6

Tabla 16. Resumen de la Llamada No 6 . Escenario 1

Ancho de Banda Kbps	Paquetes esperados	Paquetes Perdidos	Porcentaje de paquetes perdidos%	Latencia (ms)	Jitter (ms)
12	6855	1561	22,8	115	123

Fuente: Proaño Ricardo Xavier

Resumen de la Llamada No 7

Tabla 17. Resumen de la Llamada No 7 . Escenario 1

Ancho de Banda Kbps	Paquetes esperados	Paquetes Perdidos	Porcentaje de paquetes perdidos %	Latencia (ms)	Jitter (ms)
15	6213	1630	26,2	88	131

Fuente: Proaño Ricardo Xavier

Resumen de la Llamada No 8

Tabla 18. Resumen de la Llamada No 8 . Escenario 1

Ancho de Banda Kbps	Paquetes esperados	Paquetes Perdidos	Porcentaje de paquetes perdidos %	Latencia (ms)	Jitter (ms)
16	6412	2065	32,2	149	127

Fuente: Proaño Ricardo Xavier

Resumen de la Llamada No 9

Tabla 19. Resumen de la Llamada No 9 . Escenario 1

Ancho de Banda Kbps	Paquetes esperados	Paquetes Perdidos	Porcentaje de paquetes perdidos %	Latencia (ms)	Jitter (ms)
14	6523	1912	29,3	82	197

Fuente: Proaño Ricardo Xavier

Escenario 2. IPv4 sin QoS desde la red de telefonía pública (PSTN).

Nueve Llamadas con una duración promedio de 3 minutos (el mismo que se toma a partir de la saturación de la red) , en el que se genera tráfico Tcp con el software Mausezahnn, con el fin de saturar la red además utilizando el protocolo ***IPv4 sin QoS en donde se establece comunicación con la red de telefonía pública (PSTN)***, desde el número 032856753hacia el 032854193 de la ciudad de Ambato; los datos recopilados se obtuvieron con el analizador de tráfico Wireshark y corroborados con NetworkMiner.

En la siguiente tabla, se detallan los Parámetros del escenario, en base al direccionamiento descrito en las Tabla 2 y Tabla 3:

Tabla 20. Direccionamiento Escenario 2.

ORIGEN	DESTINO
Pc4 (Inicia Llamada)	Pc1(Recibe Llamada)
Pc4 (Genera Tráfico FTP)	Pc1 (Recibe Tráfico FTP)
Pc5 (Genera Tráfico IP)	Pc1(Recibe Tráfico IP)
Pc2 (Analiza el tráfico de la red)	

Fuente Proaño Ricardo Xavier

A continuación se muestran los datos obtenidos en el Pc1

Resumen de la Llamada No 1

Tabla 21. Resumen de la Llamada No 1 . Escenario 2

Ancho de Banda Kbps	Paquetes esperados	Paquetes Perdidos	Porcentaje de paquetes perdidos %	Latencia (ms)	Jitter (ms)
15	6673	1987	29,8	95	103

Fuente: Proaño Ricardo Xavier

Resumen de la Llamada No 2

Tabla 22. Resumen de la Llamada No 2 . Escenario 2

Ancho de Banda Kbps	Paquetes esperados	Paquetes Perdidos	Porcentaje de paquetes perdidos %	Latencia (ms)	Jitter (ms)
17	5873	1238	21,1	93	99

Fuente: Proaño Ricardo Xavier

Resumen de la Llamada No 3

Tabla 23. Resumen de la Llamada No 3 . Escenario 2

Ancho de Banda Kbps	Paquetes esperados	Paquetes Perdidos	Porcentaje de paquetes perdidos %	Latencia (ms)	Jitter (ms)
15	5678	1512	26,6	95	93

Fuente: Proaño Ricardo Xavier

Resumen de la Llamada No 4

Tabla 24. Resumen de la Llamada No 4 . Escenario 2

Ancho de Banda Kbps	Paquetes esperados	Paquetes Perdidos	Porcentaje de paquetes perdidos %	Latencia (ms)	Jitter (ms)
16	5345	1423	26,6	84	98

Fuente: Proaño Ricardo Xavier

Resumen de la Llamada No 5

Tabla 25. Resumen de la Llamada No 5 . Escenario 2

Ancho de Banda Kbps	Paquetes esperados	Paquetes Perdidos	Porcentaje de paquetes perdidos %	Latencia (ms)	Jitter (ms)
15	6678	1213	18,2	75	71

Fuente: Proaño Ricardo Xavier

Resumen de la Llamada No 6

Tabla 26. Resumen de la Llamada No 6 . Escenario 2

Ancho de Banda Kbps	Paquetes esperados	Paquetes Perdidos	Porcentaje de paquetes perdidos %	Latencia (ms)	Jitter (ms)
14	5876	1523	25,9	55	87

Fuente: Proaño Ricardo Xavier

Resumen de la Llamada No 7

Tabla 27. Resumen de la Llamada No 7 . Escenario 2

Ancho de Banda Kbps	Paquetes esperados	Paquetes Perdidos	Porcentaje de paquetes perdidos %	Latencia (ms)	Jitter (ms)
14	5812	1598	27,5	56	86

Fuente: Proaño Ricardo Xavier

Resumen de la Llamada No 8

Tabla 28. Resumen de la Llamada No 8 . Escenario 2

Ancho de Banda Kbps	Paquetes esperados	Paquetes Perdidos	Porcentaje de paquetes perdidos %	Latencia (ms)	Jitter (ms)
16	6376	1954	30,6	98	96

Fuente: Proaño Ricardo Xavier

Resumen de la Llamada No 9

Tabla 29. Resumen de la Llamada No 9 . Escenario 2

Ancho de Banda Kbps	Paquetes esperados	Paquetes Perdidos	Porcentaje de paquetes perdidos %	Latencia (ms)	Jitter (ms)
17	6276	1745	27,8	52	99

Fuente: Proaño Ricardo Xavier

Escenario 3. IPv6 sin QoS en la Red de Área Local (LAN).

Nueve Llamadas con una duración promedio de 3 minutos (el mismo que se toma a partir de la saturación de la red), en el que se genera tráfico Tcp con el software Mausezahnn, utilizando el protocolo ***IPv6 sin QoS en donde se establece comunicación con la Red de Área Local (LAN)***; los datos recopilados se obtuvieron con el analizador de tráfico Wireshark y corroborados con NetworkMiner.

En la siguiente tabla, se detallan los Parámetros del escenario, en base al direccionamiento descrito en las Tabla 2 y Tabla 3:

Tabla 30. Direccionamiento Escenario 3.

ORIGEN	DESTINO
Pc4 (Inicia Llamada)	Pc1(Recibe Llamada)
Pc4 (Genera Tráfico FTP)	Pc1 (Recibe Tráfico FTP)
Pc5 (Genera Tráfico IP)	Pc1(Recibe Tráfico IP)
Pc2 (Analiza el tráfico de la red)	

Fuente: Proaño Ricardo Xavier

A continuación se muestran los datos obtenidos en el Pc1

Resumen de la Llamada No 1

Tabla 31. Resumen de la Llamada No 1 . Escenario 3

Ancho de Banda Kbps	Paquetes esperados	Paquetes Perdidos	Porcentaje de paquetes perdidos %	Latencia (ms)	Jitter (ms)
15	6119	872	14,3	65	64

Fuente: Proaño Ricardo Xavier

Resumen de la Llamada No 2

Tabla 32. Resumen de la Llamada No 2 . Escenario 3

Ancho de Banda Kbps	Paquetes esperados	Paquetes Perdidos	Porcentaje de paquetes perdidos %	Latencia (ms)	Jitter (ms)
15	6345	1283	20,2	68	64

Fuente: Proaño Ricardo Xavier

Resumen de la Llamada No 3

Tabla 33. Resumen de la Llamada No 3 . Escenario 3

Ancho de Banda Kbps	Paquetes esperados	Paquetes Perdidos	Porcentaje de paquetes perdidos %	Latencia (ms)	Jitter (ms)
15	7523	1190	15,8	76	86

Fuente: Proaño Ricardo Xavier

Resumen de la Llamada No 4

Tabla 34. Resumen de la Llamada No 4 . Escenario 3

Ancho de Banda Kbps	Paquetes esperados	Paquetes Perdidos	Porcentaje de paquetes perdidos %	Latencia (ms)	Jitter (ms)
16	6925	2198	31,7	73	76

Fuente: Proaño Ricardo Xavier

Resumen de la Llamada No 5

Tabla 35. Resumen de la Llamada No 5 . Escenario 3

Ancho de Banda Kbps	Paquetes esperados	Paquetes Perdidos	Porcentaje de paquetes perdidos %	Latencia (ms)	Jitter (ms)
15	7292	1845	14	74	75

Fuente: Proaño Ricardo Xavier

Resumen de la Llamada No 6

Tabla 36. Resumen de la Llamada No 6 . Escenario 3

Ancho de Banda Kbps	Paquetes esperados	Paquetes Perdidos	Porcentaje de paquetes perdidos %	Latencia (ms)	Jitter (ms)
14	7187	1976	27,5	76	77

Fuente: Proaño Ricardo Xavier

Resumen de la Llamada No 7

Tabla 37. Resumen de la Llamada No 7 . Escenario 3

Ancho de Banda Kbps	Paquetes esperados	Paquetes Perdidos	Porcentaje de paquetes perdidos %	Latencia (ms)	Jitter (ms)
19	7491	1834	24,6	75	77

Fuente: Proaño Ricardo Xavier

Resumen de la Llamada No 8

Tabla 38. Resumen de la Llamada No 8 . Escenario 3

Ancho de Banda Kbps	Paquetes esperados	Paquetes Perdidos	Porcentaje de paquetes perdidos %	Latencia (ms)	Jitter (ms)
18	6985	1193	17,1	76	78

Fuente: Proaño Ricardo Xavier

Resumen de la Llamada No 9

Tabla 39. Resumen de la Llamada No 9 . Escenario 3

Ancho de Banda Kbps	Paquetes esperados	Paquetes Perdidos	Porcentaje de paquetes perdidos %	Latencia (ms)	Jitter (ms)
16	7019	1392	19,8	75	79

Fuente: Proaño Ricardo Xavier

Escenario 4. IPv6 sin QoS desde la red de telefonía pública (PSTN)

Nueve Llamadas con una duración promedio de 3 minutos (el mismo que se toma a partir de la saturación de la red) , en el que se genera tráfico Tcp con el software Mausezahnn, con el fin de saturar la red además utilizando el protocolo ***IPv4 sin QoS en donde se establece comunicación con la red de telefonía pública (PSTN)***, Desde el número 032856753hacia el 032854193 de la ciudad de Ambato; los datos recopilados se obtuvieron con el analizador de tráfico Wireshark y corroborados con NetworkMiner.

En la siguiente tabla, se detallan los Parámetros del escenario, en base al direccionamiento descrito en las Tabla 2 y Tabla 3:

Tabla 40. Direccionamiento Escenario 4.

ORIGEN	DESTINO
Pc4 (Inicia Llamada)	Pc1(Recibe Llamada)
Pc4 (Genera Tráfico FTP)	Pc1 (Recibe Tráfico FTP)
Pc5 (Genera Tráfico IP)	Pc1(Recibe Tráfico IP)
Pc2 (Analiza el tráfico de la red)	

Fuente : Proaño Ricardo Xavier

A continuación se muestran los datos obtenidos en el Pc1

Resumen de la Llamada No 1

Tabla 41. Resumen de la Llamada No 1 . Escenario 4

Ancho de Banda Kbps	Paquetes esperados	Paquetes Perdidos	Porcentaje de paquetes perdidos %	Latencia (ms)	Jitter (ms)
16	6676	1009	15,1	86	84

Fuente: Proaño Ricardo Xavier

Resumen de la Llamada No 2

Tabla 42. Resumen de la Llamada No 2 . Escenario 4

Ancho de Banda Kbps	Paquetes esperados	Paquetes Perdidos	Porcentaje de paquetes perdidos %	Latencia (ms)	Jitter (ms)
19	6923	1216	17,6	94	86

Fuente: Proaño Ricardo Xavier

Resumen de la Llamada No 3

Tabla 43. Resumen de la Llamada No 3 . Escenario 4

Ancho de Banda Kbps	Paquetes esperados	Paquetes Perdidos	Porcentaje de paquetes perdidos %	Latencia (ms)	Jitter (ms)
22	6986	1023	14,6	80	98

Fuente: Proaño Ricardo Xavier

Resumen de la Llamada No 4

Tabla 44. Resumen de la Llamada No 4 . Escenario 4

Ancho de Banda Kbps	Paquetes esperados	Paquetes Perdidos	Porcentaje de paquetes perdidos %	Latencia (ms)	Jitter (ms)
21	6534	1812	27,7	66	98

Fuente: Proaño Ricardo Xavier

Resumen de la Llamada No 5

Tabla 45. Resumen de la Llamada No 5 . Escenario 4

Ancho de Banda Kbps	Paquetes esperados	Paquetes Perdidos	Porcentaje de paquetes perdidos %	Latencia (ms)	Jitter (ms)
16	6022	1276	21,2	62	73

Fuente: Proaño Ricardo Xavier

Resumen de la Llamada No 6

Tabla 46. Resumen de la Llamada No 6 . Escenario 4

Ancho de Banda Kbps	Paquetes esperados	Paquetes Perdidos	Porcentaje de paquetes perdidos %	Latencia (ms)	Jitter (ms)
22	6043	1297	21,5	65	83

Fuente: Proaño Ricardo Xavier

Resumen de la Llamada No 7

Tabla 47. Resumen de la Llamada No 7 . Escenario 4

Ancho de Banda Kbps	Paquetes esperados	Paquetes Perdidos	Porcentaje de paquetes perdidos %	Latencia (ms)	Jitter (ms)
21	6056	1290	21,3	72	95

Fuente: Proaño Ricardo Xavier

Resumen de la Llamada No 8

Tabla 48. Resumen de la Llamada No 8 . Escenario 4

Ancho de Banda Kbps	Paquetes esperados	Paquetes Perdidos	Porcentaje de paquetes perdidos %	Latencia (ms)	Jitter (ms)
20	6699	1645	24,6	61	87

Fuente: Proaño Ricardo Xavier

Resumen de la Llamada No 9

Tabla 49. Resumen de la Llamada No 9 . Escenario 4

Ancho de Banda Kbps	Paquetes esperados	Paquetes Perdidos	Porcentaje de paquetes perdidos %	Latencia (ms)	Jitter (ms)
21	6919	1734	25,1	55	94

Fuente: Proaño Ricardo Xavier

Escenario 5. IPv6 con QoS en la Red de Area Local (LAN)

Nueve Llamadas con una duración promedio de 3 minutos (el mismo que se toma a partir de la saturación de la red) , en el que se genera tráfico Tcp con el software

Mausezahnn con el fin de saturar la red, utilizando el protocolo **IPv6 Con QoS en donde se establece comunicación en la Red de Area Local (LAN)**

Los datos recopilados se obtuvieron con el analizador de tráfico Wireshark y corroborados con NetworkMiner.

En la siguiente tabla, se detallan los Parámetros del escenario, en base al direccionamiento descrito en las Tabla 2 y Tabla 3:

Tabla 50. Direccionamiento Escenario 5.

ORIGEN	DESTINO
Pc4 (Inicia Llamada)	Pc1(Recibe Llamada)
Pc4 (Genera Tráfico FTP)	Pc1 (Recibe Tráfico FTP)
Pc5 (Genera Tráfico IP)	Pc1(Recibe Tráfico IP)
Pc2 (Analiza el tráfico de la red)	

Fuente: Proaño Ricardo Xavier

A continuación se muestran los datos obtenidos en el Pc1

Resumen de la Llamada No 1

Tabla 51. Resumen de la Lamada No 1 . Escenario 5

Ancho de Banda Kbps	Paquetes esperados	Paquetes Perdidos	Porcentaje de paquetes perdidos %	Latencia (ms)	Jitter (ms)
38	5823	12	0,2	21	22

Fuente: Proaño Ricardo Xavier

Resumen de la Llamada No 2

Tabla 52. Resumen de la Llamada No 2 . Escenario 5

Ancho de Banda Kbps	Paquetes esperados	Paquetes Perdidos	Porcentaje de paquetes perdidos %	Latencia (ms)	Jitter (ms)
37	7276	24	0,3	22	23

Fuente: Proaño Ricardo Xavier

Resumen de la Llamada No 3

Tabla 53. Resumen de la Llamada No 3 . Escenario 5

Ancho de Banda Kbps	Paquetes esperados	Paquetes Perdidos	Porcentaje de paquetes perdidos %	Latencia (ms)	Jitter (ms)
38	5942	14	0,2	27	23

Fuente: Proaño Ricardo Xavier

Resumen de la Llamada No 4

Tabla 54. Resumen de la Llamada No 4 . Escenario 5

Ancho de Banda Kbps	Paquetes esperados	Paquetes Perdidos	Porcentaje de paquetes perdidos %	Latencia (ms)	Jitter (ms)
37	6921	18	0,3	22	22

Fuente: Proaño Ricardo Xavier

Resumen de la Llamada No 5

Tabla 55. Resumen de la Llamada No 5 . Escenario 5

Ancho de Banda Kbps	Paquetes esperados	Paquetes Perdidos	Porcentaje de paquetes perdidos %	Latencia (ms)	Jitter (ms)
37	6876	19	0,3	24	24

Fuente: Proaño Ricardo Xavier

Resumen de la Llamada No 6

Tabla 56. Resumen de la Llamada No 6 . Escenario 5

Ancho de Banda Kbps	Paquetes esperados	Paquetes Perdidos	Porcentaje de paquetes perdidos %	Latencia (ms)	Jitter (ms)
39	6923	23	0,3	24	24

Fuente: Proaño Ricardo Xavier

Resumen de la Llamada No 7

Tabla 57. Resumen de la Llamada No 7 . Escenario 5

Ancho de Banda Kbps	Paquetes esperados	Paquetes Perdidos	Porcentaje de paquetes perdidos %	Latencia (ms)	Jitter (ms)
38	5912	12	0,2	22	23

Fuente: Proaño Ricardo Xavier

Resumen de la Llamada No 8

Tabla 58. Resumen de la Llamada No 8 . Escenario 5

Ancho de Banda Kbps	Paquetes esperados	Paquetes Perdidos	Porcentaje de paquetes perdidos %	Latencia (ms)	Jitter (ms)
39	5914	11	0,2	23	23

Fuente: Proaño Ricardo Xavier

Resumen de la Llamada No 9

Tabla 59. Resumen de la Llamada No 9 . Escenario 5

Ancho de Banda Kbps	Paquetes esperados	Paquetes Perdidos	Porcentaje de paquetes perdidos %	Latencia (ms)	Jitter (ms)
38	5376	19	0,4	24	21

Fuente: Proaño Ricardo Xavier

Escenario 6. IPv6 con QoS desde la red de telefonía pública (PSTN)

Nueve Llamadas con una duración promedio de 3 minutos (el mismo que se toma a partir de la saturación de la red) , en el que se genera tráfico Tcp con el software Mausezahnn, con el fin de saturar la red además utilizando el protocolo ***IPv4 con QoS en donde se establece comunicación con la red de telefonía pública (PSTN)***, Desde el número 032856753hacia el 032854193 de la ciudad de Ambato; los datos recopilados se obtuvieron con el analizador de tráfico Wireshark y corroborados con NetworkMiner.

En la siguiente tabla, se detallan los Parámetros del escenario, en base al direccionamiento descrito en las Tabla 2 y Tabla 3:

Tabla 60. Direccionamiento Escenario 6.

ORIGEN	DESTINO
Pc4 (Inicia Llamada)	Pc1(Recibe Llamada)
Pc4 (Genera Tráfico FTP)	Pc1 (Recibe Tráfico FTP)
Pc5 (Genera Tráfico IP)	Pc1(Recibe Tráfico IP)
Pc2 (Analiza el tráfico de la red)	

Fuente: Proaño Ricardo Xavier

A continuación se muestran los datos obtenidos en el Pc1

Resumen de la Llamada No 1

Tabla 61. Resumen de la Llamada No 1 . Escenario 6

Ancho de Banda Kbps	Paquetes esperados	Paquetes Perdidos	Porcentaje de paquetes perdidos %	Latencia (ms)	Jitter (ms)
37	6309	24	0,4	21	22

Fuente : Proaño Ricardo Xavier

Resumen de la Llamada No 2

Tabla 62. Resumen de la Llamada No 2 . Escenario 6

Ancho de Banda Kbps	Paquetes esperados	Paquetes Perdidos	Porcentaje de paquetes perdidos %	Latencia (ms)	Jitter (ms)
38	6986	37	0,5	24	23

Fuente : Proaño Ricardo Xavier

Resumen de la Llamada No 3

Tabla 63. Resumen de la Llamada No 3 . Escenario 6

Ancho de Banda Kbps	Paquetes esperados	Paquetes Perdidos	Porcentaje de paquetes perdidos %	Latencia (ms)	Jitter (ms)
37	7418	22	0,3	22	23

Fuente : Proaño Ricardo Xavier

Resumen de la Llamada No 4

Tabla 64. Resumen de la Llamada No 4 . Escenario 6

Ancho de Banda Kbps	Paquetes esperados	Paquetes Perdidos	Porcentaje de paquetes perdidos %	Latencia (ms)	Jitter (ms)
37	6498	16	0,2	21	22

Fuente : Proaño Ricardo Xavier

Resumen de la Llamada No 5

Tabla 65. Resumen de la Llamada No 5 . Escenario 6

Ancho de Banda Kbps	Paquetes esperados	Paquetes Perdidos	Porcentaje de paquetes perdidos %	Latencia (ms)	Jitter (ms)
39	6308	27	0,4	22	23

Fuente : Proaño Ricardo Xavier

Resumen de la Llamada No 6

Tabla 66. Resumen de la Llamada No 6 . Escenario 6

Ancho de Banda Kbps	Paquetes esperados	Paquetes Perdidos	Porcentaje de paquetes perdidos %	Latencia (ms)	Jitter (ms)
38	5398	14	0,3	24	25

Fuente : Proaño Ricardo Xavier

Resumen de la Llamada No 7

Tabla 67. Resumen de la Llamada No 7 . Escenario 6

Ancho de Banda Kbps	Paquetes esperados	Paquetes Perdidos	Porcentaje de paquetes perdidos %	Latencia (ms)	Jitter (ms)
37	6267	29	0,5	21	21

Fuente : Proaño Ricardo Xavier

Resumen de la Llamada No 8

Tabla 68. Resumen de la Llamada No 8 . Escenario 6

Ancho de Banda Kbps	Paquetes esperados	Paquetes Perdidos	Porcentaje de paquetes perdidos %	Latencia (ms)	Jitter (ms)
38	5209	6	0,1	22	21

Fuente : Proaño Ricardo Xavier

Resumen de la Llamada No 9

Tabla 69. Resumen de la Llamada No 9 . Escenario 6

Ancho de Banda Kbps	Paquetes esperados	Paquetes Perdidos	Porcentaje de paquetes perdidos %	Latencia (ms)	Jitter (ms)
39	6876	12	0,2	22	23

Fuente : Proaño Ricardo Xavier

4.1. Tabla de los ambientes de prueba

4.1.1. Resumen Escenario 1 IPv4 sin QoS en la Red de Area Local (LAN)

Tabla 70. Resumen Escenario 1

# Llamada	Ancho de Banda Kbps	Paquetes esperados	Paquetes Perdidos	Porcentaje de paquetes perdidos %	Latencia (ms)	Jitter (ms)
1	12	6223	2275	21	245	130
2	13	6223	1367	22	123	135
3	16	6850	2084	30,4	126	133
4	15	6131	1380	22,5	116	145
5	17	6306	1531	24,3	166	140
6	12	6855	1561	22,8	115	123
7	15	6213	1630	26,2	88	131
8	16	6412	2065	32,2	149	127
9	14	6523	1912	29,3	82	197

Fuente : Proaño Ricardo Xavier

4.1.2. Resumen Escenario 2 IPv4 sin QoS desde la red de telefonía pública (PSTN)

Tabla 71. Resumen Escenario 2

# Llamada	Ancho de Banda Kbps	Paquetes esperados	Paquetes Perdidos	Porcentaje de paquetes perdidos %	Latencia (ms)	Jitter (ms)
1	15	6673	1987	29,8	95	103
2	17	5873	1238	21,1	93	99
3	15	5678	1512	26,6	95	93
4	16	5345	1423	26,6	84	98
5	15	6678	1213	18,2	75	71
6	14	5876	1523	25,9	55	87
7	14	5812	1598	27,5	56	86
8	16	6376	1954	30,6	98	96
9	17	6276	1745	27,8	52	99

Fuente : Proaño Ricardo Xavier

4.1.3. Resumen Escenario 3 IPv6 sin QoS en la Red de Área Local (LAN)

Tabla 72. Resumen Escenario 3

# Llamada	Ancho de Banda Kbps	Paquetes esperados	Paquetes Perdidos	Porcentaje de paquetes perdidos %	Latencia (ms)	Jitter (ms)
1	15	6119	872	14,3	65	64
2	15	6345	1283	20,2	68	64
3	15	7523	1190	15,8	76	86
4	16	6925	2198	31,7	73	76
5	15	7292	1845	14	74	75
6	14	7187	1976	27,5	76	77
7	19	7491	1834	24,6	75	77
8	18	6985	1193	17,1	76	78
9	16	7019	1392	19,8	75	79

Fuente : Proaño Ricardo Xavier

4.1.4. Resumen Escenario 4 IPv6 sin QoS desde la red de telefonía pública (PSTN)

Tabla 73. Resumen Escenario 4

# Llamada	Ancho de Banda Kbps	Paquetes esperados	Paquetes Perdidos	Porcentaje de paquetes perdidos %	Latencia (ms)	Jitter (ms)
1	16	6676	1009	15,1	86	84
2	19	6923	1216	17,6	94	86
3	22	6986	1023	14,6	80	98
4	21	6534	1812	27,7	66	98
5	16	6022	1276	21,2	62	73
6	22	6043	1297	21,5	65	83
7	21	6056	1290	21,3	72	95
8	20	6699	1645	24,6	61	87
9	21	6919	1734	25,1	55	94

Fuente : Proaño Ricardo Xavier

4.1.5. Resumen Escenario 5 IPv6 con QoS en la Red de Area Local (LAN)

Tabla 74. Resumen Escenario 5

# Llamada	Ancho de Banda Kbps	Paquetes esperados	Paquetes Perdidos	Porcentaje de paquetes perdidos %	Latencia (ms)	Jitter (ms)
1	38	5823	12	0,2	21	22
2	37	7276	24	0,3	22	23
3	38	5942	14	0,2	27	23
4	37	6921	18	0,3	22	22
5	37	6876	19	0,3	24	24
6	39	6923	23	0,3	24	24
7	38	5912	12	0,2	22	23
8	39	5914	11	0,2	23	23
9	38	5376	19	0,4	24	21

Fuente : Proaño Ricardo Xavier

4.1.6. Resumen Escenario 6 IPv6 con QoS desde la red de telefonía pública (PSTN)

Tabla 75. Resumen Escenario 6

# Llamada	Ancho de Banda Kbps	Paquetes esperados	Paquetes Perdidos	Porcentaje de paquetes perdidos %	Latencia (ms)	Jitter (ms)
1	37	6309	24	0,4	21	22
2	38	6986	37	0,5	24	23
3	37	7418	22	0,3	22	23
4	37	6498	16	0,2	21	22
5	39	6308	27	0,4	22	23
6	38	5398	14	0,3	24	25
7	37	6267	29	0,5	21	21
8	38	5209	6	0,1	22	21
9	39	6876	12	0,2	22	23

Fuente : Proaño Ricardo Xavier

4.2. Resumen de Indicadores de la Variable Dependiente

En base a los datos recopilados, podemos obtener las siguientes tablas comparativas entre los seis escenarios propuestos:

4.2.1 Ancho de Banda

Tabla 76 Comparación del indicador Ancho de banda entre los escenarios

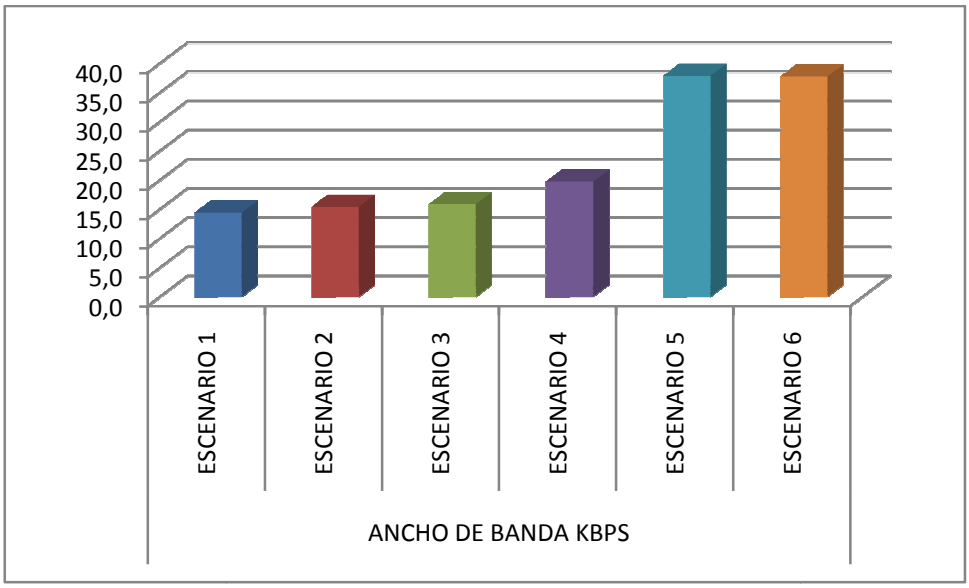
Tabla 76. Variable Ancho de Banda

ANCHO DE BANDA KBPS					
ESCENARIO 1	**ESCENARIO 2**	**ESCENARIO 3**	**ESCENARIO 4**	**ESCENARIO 5**	**ESCENARIO 6**
12	15	15	16	38	37
13	17	15	19	37	38
16	15	15	22	38	37
15	16	16	21	37	37
17	15	15	16	37	39
12	14	14	22	39	38
15	14	19	21	38	37
16	16	18	20	39	38
14	17	16	21	38	39
14,4	**15,4**	**15,9**	**19,8**	**37,9**	**37,8**

Fuente : Proaño Ricardo Xavier

Comparación del indicador Ancho de banda entre los escenarios.

Figura 28 : Comparación de indicador Ancho de Banda



Fuente : Proaño Ricardo Xavier

Según el apartado “Datos de prueba” en el que requiere mínimo 32 Kbps de Ancho de banda para un canal de voz, vemos una clara ventaja de los escenarios 5 y 6 con respecto a 1,2,3,4.

4.2.2. Paquetes perdidos

Tabla 77 Comparación de Porcentaje de pérdida de paquetes %s entre los escenarios

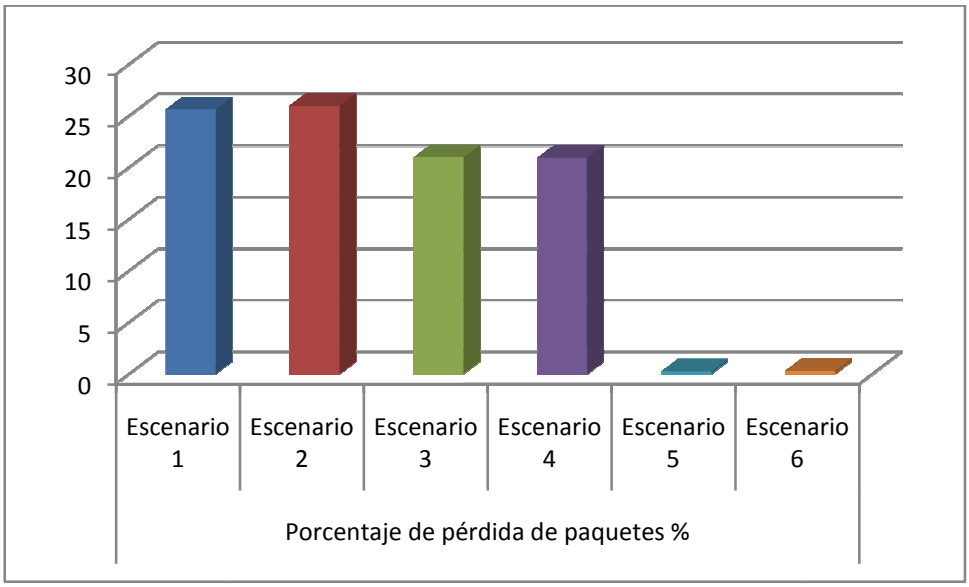
Tabla 77. Porcentaje de paquetes perdidos

Porcentaje de pérdida de paquetes %					
Escenario 1	**Escenario 2**	**Escenario 3**	**Escenario 4**	**Escenario 5**	**Escenario 6**
21	29,8	14,3	15,1	0,2	0,4
22	21,1	20,2	17,6	0,3	0,5
30,4	26,6	15,8	14,6	0,2	0,3
22,5	26,6	31,7	27,7	0,3	0,2
24,3	18,2	14	21,2	0,3	0,4
22,8	25,9	27,5	21,5	0,3	0,3
26,2	27,5	24,6	21,3	0,2	0,5
32,2	30,6	17,1	24,6	0,2	0,1
29,3	27,8	19,8	25,1	0,4	0,2
26	**26**	**21**	**21**	**0,3**	**0,3**

Fuente : Proaño Ricardo Xavier

Es en base a esta última tabla que obtendremos las bases de comparación ya que en lo citado anteriormente, una comunicación óptima requiere máximo un 2% de paquetes perdidos. Además el indicador se refiere al porcentaje de paquetes perdidos entre los diferentes escenarios.

Figura 29.Comparación Indicador Porcentaje de Pérdida de Paquetes



Fuente : Proaño Ricardo Xavier

Los resultados muestran un resultado favorable para los escenarios en dónde se aplicó Calidad de Servicio (QoS).

4.2.3. Latencia (Valor máximo según las normas ETSI TS 123 107 V7.1.0 - 60 milisegundos)

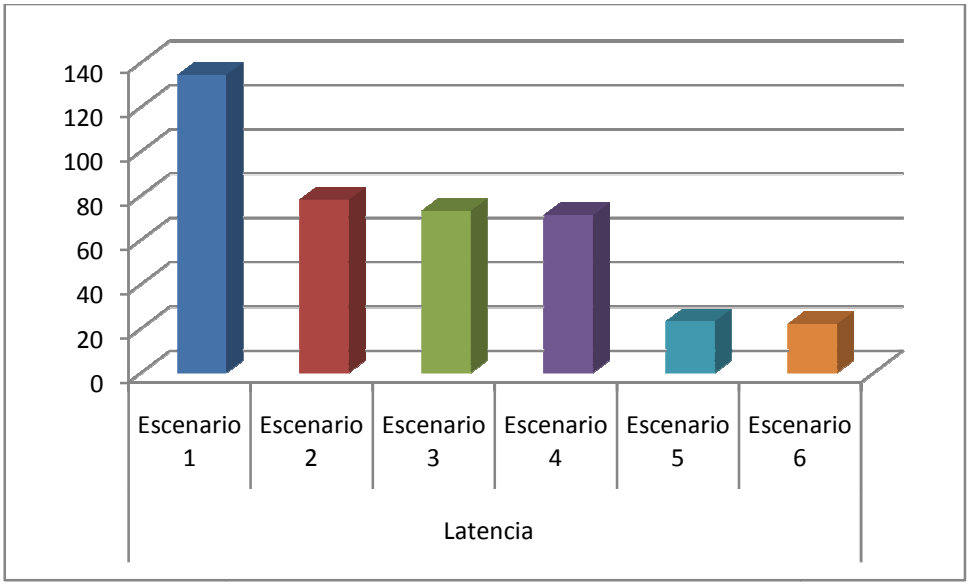
Tabla 78. Latencia

Latencia					
Escenario 1	**Escenario 2**	**Escenario 3**	**Escenario 4**	**Escenario 5**	**Escenario 6**
245	95	65	86	21	21
123	93	68	94	22	24
126	95	76	80	27	22
116	84	73	66	22	21
166	75	74	62	24	22
115	55	76	65	24	24
88	56	75	72	22	21
149	98	76	61	23	22
82	52	75	55	24	22
134	**78**	**73**	**71**	**23**	**22**

Fuente : Proaño Ricardo Xavier

Comparación de Latencia entre los diferentes escenarios

Figura 30. Comparación de Indicador Latencia



Fuente : Proaño Ricardo Xavier

Se aprecia una notable mejoría para la comunicación en los escenarios 5 y 6 donde se aplicó Calidad de Servicio QoS.

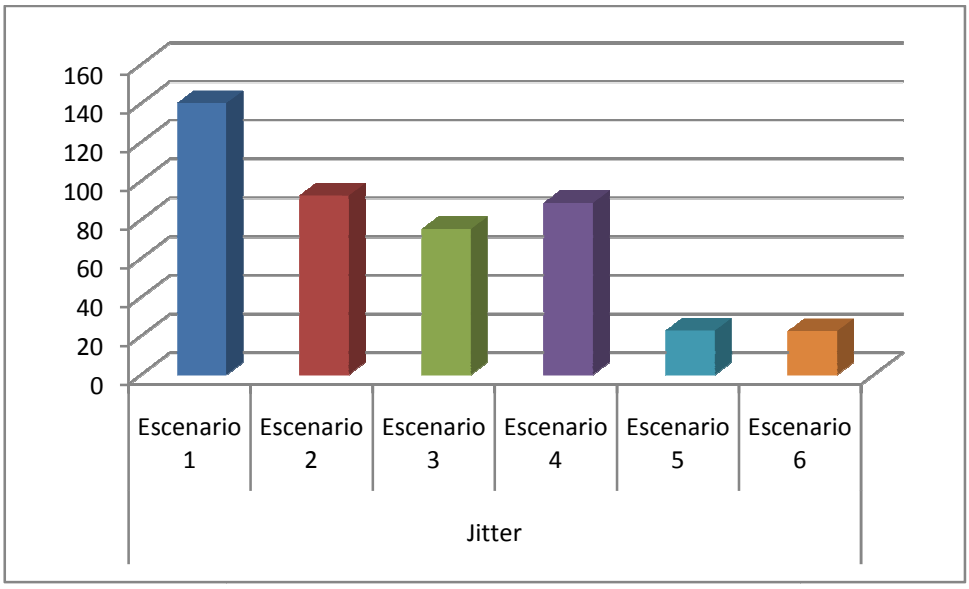
4.2.4. Jitter (Valor requerido según las normas ETSI TS 123 107 V7.1.0 - 50 milisegundos)

Tabla 79. Jitter

Jitter					
Escenario 1	**Escenario 2**	**Escenario 3**	**Escenario 4**	**Escenario 5**	**Escenario 6**
130	103	64	84	22	22
135	99	64	86	23	23
133	93	86	98	23	23
145	98	76	98	22	22
140	71	75	73	24	23
123	87	77	83	24	25
131	86	77	95	23	21
127	96	78	87	23	21
197	99	79	94	21	23
140	**92**	**75**	**89**	**23**	**23**

Fuente : Proaño Ricardo Xavier

Figura 31. Comparación de Indicador Jitter



Fuente : Proaño Ricardo Xavier

Al igual que en los casos anteriores, se observa una pronunciada mejoría de la comunicación en los escenarios 5 y 6 que fue donde se aplicó Calidad de Servicio QoS.

Es muy importante indicar que al tratarse de datos de diferente naturaleza, y al obtener datos que una vez ingresados en una tabla de contingencia general, se dispersan de manera muy pronunciada, se procedió a clasificarlos en una escala de Likert, construida en base a una serie de ítems codificados que actúan como reactivos; estos ítems permiten determinar la intensidad y la dirección, positiva o negativa, de cada indicador.

De acuerdo a cada indicador de la variable dependiente se detalla la escala utilizada en el presente proyecto y con base en la *Tabla 8* en donde se indican los valores Óptimos de cada indicador según normas estandarizadas:

Tabla 80. Escala de Likert de los indicadores de la variable dependiente

TRANSMISIÓN DE VoIP	
INDICADOR	**VALOR ASIGNADO**
MUY BUENA	4
BUENA	3
MALA	2
MUY MALA	1

Fuente: Proaño Ricardo Xavier

Valores asignados según la escala de Likert para el indicador Ancho de banda.

Tabla 81. Escala de Likert para Ancho de Banda

	ANCHO DE BANDA				
	MUY BUENO (4)	**BUENO (3)**	**MALO (2)**	**MUY MALO (1)**	**VALOR**
ESCENARIO 1				x	1
ESCENARIO 2				x	1
ESCENARIO 3				x	1
ESCENARIO 4				x	1
ESCENARIO 5	x				4
ESCENARIO 6	x				4

Fuente: Proaño Alulema Ricardo

CONDICIÓN

MUY BUENO > 35 Kbps

BUENO 30 - 35 Kbps

MALO 25 -29 Kbps

MUY MALO < 25 Kbps

Valores asignados según la escala de Likert para el indicador % Paquetes Perdidos.

Tabla 82. Escala de Likert para % Paquetes Perdidos

% DE PAQUETES PERDIDOS

	MUY BUENO (4)	BUENO (3)	MALO (2)	MUY MALO (1)	VALOR
ESCENARIO 1				x	1
ESCENARIO 2				x	1
ESCENARIO 3				x	1
ESCENARIO 4				x	1
ESCENARIO 5	x				4
ESCENARIO 6	x				4

Fuente: Proaño Ricardo Xavier

CONDICIÓN

MUY BUENO < 1%

BUENO 1 - 2 %

MALO 3 - 5 %

MUY MALO > 5 %

Valores asignados según la escala de Likert para el indicador Latencia.

Tabla 83. Escala de Likert para Latencia

	LATENCIA				
	MUY BUENO (4)	**BUENO (3)**	**MALO (2)**	**MUY MALO (1)**	**VALOR**
ESCENARIO 1				x	1
ESCENARIO 2				x	1
ESCENARIO 3				x	1
ESCENARIO 4				x	1
ESCENARIO 5	x				4
ESCENARIO 6	x				4

Fuente: Proaño Ricardo Xavier

CONDICIÓN

MUY BUENO	< 45 ms
BUENO	45 -50 ms
MALO	51 -55 ms
MUY MALO	> 55 ms

Valores asignados según la escala de Likert para el indicador Jitter.

Tabla 84. Escala de Likert para Jitter

	JITTER				
	MUY BUENO (4)	**BUENO (3)**	**MALO (2)**	**MUY MALO (1)**	**VALOR**
ESCENARIO 1				x	1
ESCENARIO 2				x	1
ESCENARIO 3				x	1
ESCENARIO 4				x	1
ESCENARIO 5	x				4
ESCENARIO 6	x				4

Fuente : Proaño Ricardo Xavier

CONDICIÓN	
MUY BUENO	< 55 ms
BUENO	55 -60 ms
MALO	61 -65 ms
MUY MALO	> 65 ms

4.3. Comprobación de la Hipótesis de la Investigación realizada

4.3.1 Planteamiento de las Hipótesis

Para la comprobación de la hipótesis se utilizó Chi cuadrado, ya que dentro de las pruebas no paramétricas, ha tomado mucha popularidad entre los investigadores, así varios de ellos coinciden en el uso o propósito fundamental de esta prueba. Y para su validación dentro de este proyecto nos basaremos en el juicio emitido por varios expertos. Así, Levin Jack PhD. señala: "La prueba de significancia no paramétrica más popular en la investigación social se conoce como Chi cuadrada (X^2). Como veremos, la prueba se usa para hacer comparaciones entre dos o más muestras".[22]

Por su parte, W. Emory dice: "Probablemente la más ampliamente usada prueba no paramétrica de significancia es la prueba chi cuadrada".[23]

Igualmente Manheim y Rich (Investigadores Sociales) al referirse a medidas de asociación y significancia para variables nominales expresan: "El test de significancia estadística para variables nominales es X^2 (chi cuadrada).[24]

Esta prueba es particularmente utilizada en pruebas que envuelven data nominal aunque también puede ser utilizada para escalas superiores. Típicamente es utilizada

[22] Fundamentos de Estadística en la Investigación Social. Editorial HARLA, México, 1979. Pag. 170.
[23] EMORY C., William. Business Research Methods. Editorial Richard Irwin, Inc. Illinois, U.S.A., 1985. Pag. 360.
[24] MANHEIM, Jarol B y RICH, Richard C. Empirical Political Analysis. Research Methods in Political Science. 3ra. Edición, Longman Publishing Group, New York, 1991, pag. 269.

en casos donde los eventos, persona u objetos son agrupados en dos o más categorías nominales, tales como: "si-no", "a favor, en contra, indeciso", o clases A, B, C, D.

Al usar esta técnica estadística se puede probar significantes diferencias entre la distribución observada de la data entre categorías y la distribución esperada basada sobre la hipótesis nula. En otras palabras, "la prueba de significancia Chi cuadrada tiene que ver esencialmente con la distinción entre las frecuencias esperadas y las frecuencias obtenidas u observadas. Las frecuencias esperadas (Fe) se refieren a los términos de la hipótesis nula, de acuerdo con la cual se espera que la frecuencia relativa (o proporción) sea la misma de un grupo a otro. En contraste, la frecuencia obtenida (Fo) se refiere a los resultados que obtenemos realmente al realizar un estudio, y por lo tanto puede variar o no de un grupo a otro. Sólo si las diferencias entre las frecuencias esperadas y obtenidas es lo suficientemente grande, rechazamos la hipótesis nula y decidimos que existe una diferencia poblacional verdadera".

Según lo expuesto por estos autores, se señala que Chi cuadrada, representada por la letra griega X elevada al cuadrado, es una prueba estadística clasificada como no paramétrica, utilizada en la evaluación de hipótesis y que sirve como test o prueba de significancia.

Para el presente proyecto se define la siguiente Hipótesis:

Ho: La Aplicación de QoS sobre IPv6 no mejora la transmisión de VoIP.

Hi: La Aplicación de QoS sobre IPv6 mejora la transmisión de VoIP.

4.3.2. Nivel de significancia

El nivel de significancia con el que se trabajó es de 0,05. El mismo que es utilizado por la gran mayoría de los investigadores.

Alfa (α): este valor hace referencia al nivel de confianza que deseamos que tengan los cálculos de la prueba; es decir, si queremos tener un nivel de confianza del 95%, el

valor de alfa debe ser del 0.05, lo cual corresponde al complemento porcentual de la confianza.

Grados de Libertad (k): Es un estimador del número de categorías independientes en la prueba de independencia o experimento estadístico. Se encuentran mediante la fórmula n-r, donde n=número de sujetos y r es el número de grupos estadísticamente dependientes.

El grado de libertad es igual a la multiplicación del número de las filas menos uno por el numero de las columnas menos uno así:

Simbología:

gl = Grados de libertad
nf = Número de filas de la tabla
nc = Número de columnas de la tabla
α = Nivel de significancia
x^2_α = CHI crítico

Cálculo:

gl = (nf-1)(nc-1)

gl = (2-1)(6-1)

gl = (1)(5)

gl = 5

$x^2\alpha = critico = 11{,}07$

Estadístico de prueba

$$x^2c = \sum \frac{(O-E)^2}{E}$$

4.3.3. Criterio

Para la comprobación de la Hipótesis nos basamos en el siguiente criterio:

Si $X^2_c \geq X^2_\alpha$ => Se rechaza Ho y se acepta Hi

4.4 Matriz de Contingencia Valores Observados

Tabla 85. Tabla de contingencia de valores observados

		Indicador	Escenario 1 IPv4 sin QoS, en la red LAN	Escenario 2 IPv4 sin QoS desde la red PSTN	Escenario 3 IPv6 sin QoS en la red LAN	Escenario 4 IPv6 sin QoS desde la red PSTN	Escenario 5 IPv6 con QoS en la red LAN	Escenario 6 IPv6 con QoS desde la red PSTN
La Aplicación de QoS mejora la transmisión de VoIP	Hi	**Ancho de banda Kbps**	0	0	0	0	4	4
		% Paquetes perdidos	0	0	0	0	4	4
		Latencia (ms)	0	0	0	0	4	4
		Jitter (ms)	0	0	0	0	4	4
La Aplicación de QoS mejora la transmisión de VoIP	Ho	**Ancho de banda Kbps**	1	1	1	1	0	0
		% Paquetes perdidos	1	1	1	1	0	0
		Latencia (ms)	1	1	1	1	0	0
		Jitter (ms)	1	1	1	1	0	0

Fuente: Proaño Ricardo Xavier

4.5 Matriz de Contingencia Valores Observados promediada.

Tabla 86. Tabla promediada de valores observados

		Escenario 1 IPv4 sin QoS, en la red LAN	Escenario 2 IPv4 sin QoS desde la red PSTN	Escenario 3 IPv6 sin QoS en la red LAN	Escenario 4 IPv6 sin QoS desde la red PSTN	Escenario 5 IPv6 con QoS en la red LAN	Escenario 6 IPv6 con QoS desde la red PSTN	∑
La Aplicación de QoS mejora la transmisión de VoIP	Hi	0	0	0	0	4	4	8
La Aplicación de QoS mejora la transmisión de VoIP	Ho	1	1	1	1	0	0	4
		1	1	1	1	4	4	12

Fuente: Proaño Ricardo Xavier

Tabla de Valores Observados y valores Esperados.

Tabla 87. Valores Observados - Esperados

			Escenario 1 IPv4 sin QoS, en la red LAN	Escenario 2 IPv4 sin QoS desde la red PSTN	Escenario 3 IPv6 sin QoS en la red LAN	Escenario 4 IPv6 sin QoS desde la red PSTN	Escenario 5 IPv6 con QoS en la red LAN	Escenario 6 IPv6 con QoS desde la red PSTN	∑
La Aplicación de QoS mejora la transmisión de VoIP	Hi	(O-E)^2/E	0,7	0,7	0,7	0,7	0,7	0,7	4,0
La Aplicación de QoS mejora la transmisión de VoIP	Ho	(O-E)^2/E	1,3	1,3	1,3	1,3	1,3	1,3	8,0
									12,0

Fuente: Proaño Ricardo Xavier

4.5 Decisión

De acuerdo a la tabla estadística IV.11 de distribución de chi-cuadrado, con un nivel de significancia 5%, con un grado de libertad de gl = 5, genera un valor tabulado de$x^2\alpha$= 11,07.

Tabla 88. Tabla Chicuadrado

DISTRIBUCION DE χ^2

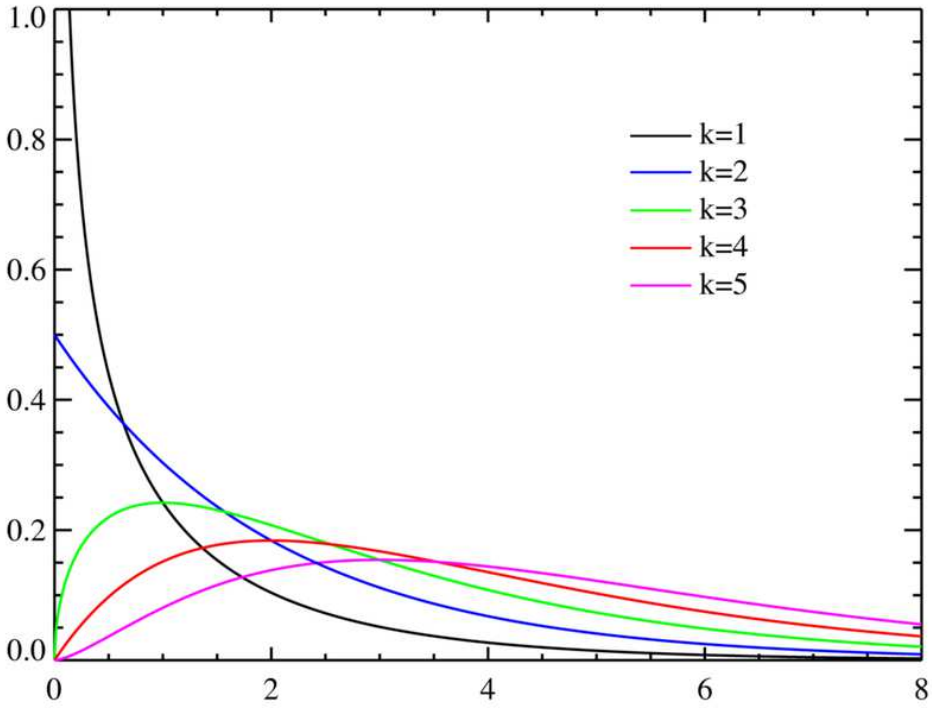
Grados de libertad	Probabilidad										
	0,95	0,90	0,80	0,70	0,50	0,30	0,20	0,10	0,05	0,01	0,001
1	0,004	0,02	0,06	0,15	0,46	1,07	1,64	2,71	3,84	6,64	10,83
2	0,10	0,21	0,45	0,71	1,39	2,41	3,22	4,60	5,99	9,21	13,82
3	0,35	0,58	1,01	1,42	2,37	3,66	4,64	6,25	7,82	11,34	16,27
4	0,71	1,06	1,65	2,20	3,36	4,88	5,99	7,78	9,49	13,28	18,47
5	1,14	1,61	2,34	3,00	4,35	6,06	7,29	9,24	11,07	15,09	20,52
6	1,63	2,20	3,07	3,83	5,35	7,23	8,56	10,64	12,59	16,81	22,46
7	2,17	2,83	3,82	4,67	6,35	8,38	9,80	12,02	14,07	18,48	24,32
8	2,73	3,49	4,59	5.53	7,34	9,52	11,03	13,36	15,51	20,09	26,12
9	3,32	4,17	5,38	6,39	8,34	10,66	12,24	14,68	16,92	21,67	27,88
10	3,94	4,86	6,18	7,27	9,34	11,78	13,44	15,99	18,31	23,21	29,59
	No significativo								Significativo		

Fuente: García José Manuel

Condición: $X^2_c \geq X^2_\alpha$ => Se rechaza Ho y se acepta Hi

12 ≥ 11,07 => Cumple con la condición

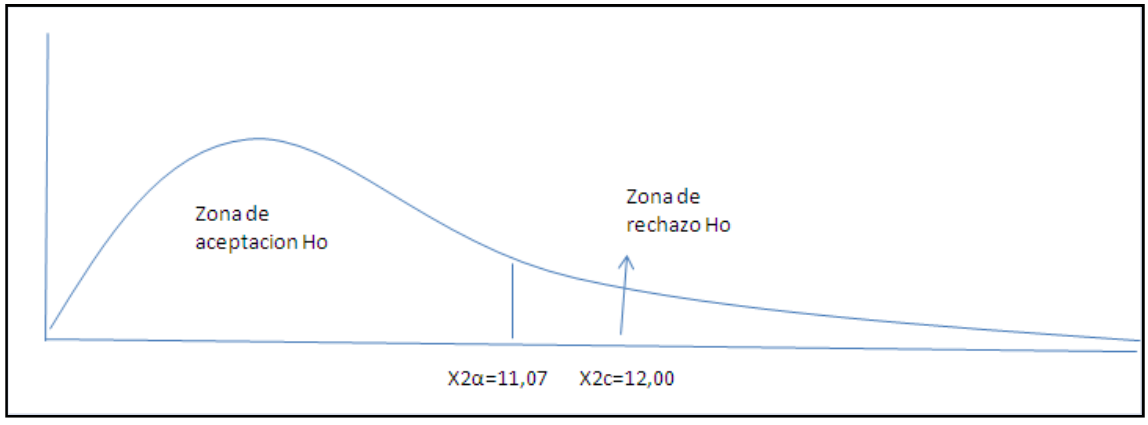
Para la demostración gráfica, los límites de la región de rechazo están definidas por los grados de libertad (gl), que se los representa así:



Fuente: http://commons.wikimedia.org/wiki/File:Chi-square_distributionPDF.png

Los valores de *k* corresponden a los grados de libertad que para x^2 son gl=5. En la siguiente figura se representa el valor tabulado $x^2\alpha$ y el valor calculado x^2c.

Tabla 89. Rechazo de Ho



Fuente:Proaño Ricardo Xavier

Como X^2_c =12es mayor X^2_α = 11,07, por lo tanto se rechaza la hipótesis nula Ho y se acepta la hipótesis de investigación Hi que dice:“La Aplicación de QoS sobre IPv6 mejora la transmisión de VoIP”

Conclusiones

- El presente Proyecto de Investigación se realizó bajo la consola de Asterisk, sobre el Sistema base CentOS 5.6, logrando comprobar que efectivamente se pueden manejar soluciones VoIP con soporte nativo y enteramente compatible con IPv6, permitiendo un significativo ahorro en costos de derechos de uso.
- El presente proyecto evidenció las ventajas competitivas que ofrece IPv6 respecto a IPv4, a través de la comparación de cada indicador de la variable dependiente, así tenemos que el Ancho de Banda con IPv4 y sin QoS, alcanza un 46 % de su valor óptimo, el mismo indicador con IPv6 sin QoS, 56 % y con IPv6 pero aplicando QoS, alcanza valores que rondan el 100 % del valor óptimo. Para el indicador Paquetes Perdidos, en el caso de IPv4 sin QoS, se obtiene un 26 %, IPv6 sin QoS 21 % eIPv6 con QoS, 0,3%. En los indicadores Latencia y Jitter se obtuvo un comportamiento con esta misma tendencia, es decir en ambientes de IPv4 se pudieron observar valores más lejanos al óptimo recomendado que en situaciones donde se aplicó IPv6 y más aún IPv6 con QoS.

- Con los resultados obtenidos al implementar el mecanismo de la política de tráfico traffic-shaper que provee colas basadas en el algoritmo Token Bucket Shaping permite que los recursos no usados por una clase de tráfico sean tomados por otra que los necesita. El algoritmo de shaper limita el uso del ancho de banda por clases pero realoja y distribuye el ancho de banda sobrante que permite asegurar una transmisión de VoIP estable y permanente.
- El presente proyecto de investigación ha demostrado que existen soluciones robustas y completamente libres, que permiten implementar escenarios complejos en los que se puede incluir Ruteo, QoS, y VoIP, sin ningún coste por el uso de licencias.
- El valor calculado del análisis estadístico Chi cuadrado, $X2c = 12$ el mismo que es mayor al valor tabulado $X2\alpha = 11,07$, por lo tanto se comprueba la Hipótesis planteada: “La Aplicación de QoS sobre IPv6 mejora la transmisión de VoIP”.

Recomendaciones.

- Con el fin de asegurar la transmisión de VoIP, los softphones utilizados, pueden configurarse con el protocolo ZRTP, lo que conlleva a que nuestra comunicación viaje con datos encriptados.
- Se recomienda seguir investigando en el tema presentado en esta tesis, sobre todo profundizar en el tema de la seguridad en la transmisión VoIP.
- El personal encargado de la gestión de la red en la que se implemente este servicio, debe conocer el manejo del Sistema Operativo Linux, tener conocimientos sólidos de redes TCP/IP y de los servicios planteados, para que el sistema funcione a su máxima capacidad y para que se puedan gestionar exitosamente cambios en su configuración.

BIBLIOGRAFÍA

1.-**ADASME**, A., Implementación de una Central PBX con soporte de H323 y SIP,utilizando Asterisk y GNU Gatekeeper., Santiago - Chile., Universidad de Chile., 2009., P.p. 13-21.

2.- **BARRIOS**, J.,Implementación de Servidores con GNU/Linux., México-México.,UNAM.,2007., P.p. 110-484.

3.-**EMORY**W., Business Research Methods. Illinois - U.S.A., Editorial Richard Irwin., 1985., P.p. 360.

4.- **ESPINOZA**, J., Validación y Estandarización de Instrumentos., Bogotá - Colombia., Subdirección de Evaluación y Tratamiento del INPEC., 2008., P.p. 5.

5.-**FERNÁNDEZ** M., Implementación de IPv6, QoS e IPSec con Linux., Madrid - España., 2003., P.p. 16-29.

6.-**PALET** J., IPv6 para todos., Buenos Aires - Argentina., Internet Society.,2009., P.p.40-119.

7.- **INSTALACIÓN DE ASTERISK**

http://www.sinologic.net/proyectos/voip2day2010/

20012-06-25

8.- **QoS PARA VoIP**

http://www.improvisa.com/28-08-2009/qos-para-VoIP-con-hfsc/

2012-04-30

9.- **QoS EN UNA RED DE VoIP**

http://www.sinologic.net/2007-05/configurar-qos-en-una-red-de-voip/

2012-05-25

ANEXOS

Anexo 1.

Archivos de Configuración de Asterisk

/etc/dahdi/system.conf (Sistema de configuración de los controladores dahdi)

```
fxsks=1
echocanceller=mg2,1
fxsks=2
echocanceller=mg2,2
fxsks=3
echocanceller=mg2,3
fxsks=4
echocanceller=mg2,4
# Global data
loadzone        = us
defaultzone     = us
```

/etc/asterisk/chan_dahdi.conf

```
#include dahdi-channels.conf
```

/etc/asterisk/dahdi_channels.conf (Canales Fxo-Fxs)

```
; Span 1: WCTDM/0 "Wildcard TDM410P" (MASTER)
;;; line="1 WCTDM/0/0 FXSKS  (EC: MG2 - INACTIVE)"
signalling=fxs_ks
callerid=asreceived
group=0
context=from-pstn
channel => 1
callerid=
group=
context=default

;;; line="2 WCTDM/0/1 FXSKS  (EC: MG2 - INACTIVE)"
signalling=fxs_ks
callerid=asreceived
group=0
context=from-pstn
channel => 2
callerid=
group=
```

context=default
;;; line="3 WCTDM/0/2 FXSKS (EC: MG2 - INACTIVE)"
signalling=fxs_ks
callerid=asreceived
group=0
context=from-pstn
channel => 3
callerid=
group=
context=default

;;; line="4 WCTDM/0/3 FXSKS (EC: MG2 - INACTIVE)"
signalling=fxs_ks
callerid=asreceived
group=0
context=from-pstn
channel => 4
callerid=
group=
context=default

/etc/asterisk/sip.conf. (Archivo principal de configuración de asterisk), por tratarse de un entorno de pruebas, se escogieron nombres muy simples para las extensiones, sin embargo es totalmente transparente para el usuario, ya que cada extensión representa un departamento de la empresa)

[general]
#bindport=5060
udpbindaddr=[2001:db8:2::4]:5060
videosupport=yes
disallow=all
allow=alaw
allow=ilbc
allow=gsm
allow=h261
allow=h263
allow=ulaw
allow=h264
allow=g722
allow=g726
allow=h263p
;Troncalización
register =
telefonia:welcome@[2001:db8:1::4]/troncal ; para

el otro extremo será:
register =troncal:welcome@[2001:db8:2::4]/telefonia

[pepe]
secret=pepin
callerid="pepe perez"<1001>
type=friend
context=internos
host=dynamic
qualify=yes
allow=ulaw
mailbox=1001@default
[juan]
secret=juanin
callerid="juan proanio"<1002>
type=friend
context=internos
host=dynamic
qualify=yes
allow=ulaw
mailbox=1002@default

[pedro]
secret=pedrin
callerid="pedro pacheco"<1003>
type=friend
context=internos
host=dynamic
qualify=yes
allow=ulaw
mailbox=1003@default
[secretaria]
secret=secretaria
callerid="Secretaria"<1004>
type=friend
context=internos
host=dynamic
qualify=yes
allow=ulaw
mailbox=1004@default
[troncal]
type=friend
secret=welcome
context=internos
qualify=yes
host=dynamic
#insecure=invite
disallow=all

allow=gsm
allow=ulaw
allow=alaw
videosupport=yes
allow=h264
allow=h263p
#allow=g722
#allow=g726
#allow=ilbc
rtptimeout=60

extensions.conf (Archivo donde se configuran todas las extensiones de asterisk)

[internos]
exten => 1001,1,Dial(SIP/pepe,10)
exten => 1001,2,Voicemail(1001,u)
exten => 1001,3,Hangup()
exten => 1001,102,Voicemail(1001,b)
exten => 1001,103,Hangup()

exten => 1002,1,Dial(SIP/juan,10)
exten => 1002,2,Voicemail(1002,u)
exten => 1002,3,Hangup()
exten => 1002,102,Voicemail(1002,b)
exten => 1002,103,Hangup()

exten => 1003,1,Dial(SIP/pedro,10)
exten => 1003,2,Voicemail(1003,u)
exten => 1003,3,Hangup()
exten => 1003,102,Voicemail(1003,b)
exten => 1003,103,Hangup()

exten => 1004,1,Dial(SIP/secretaria,10)
exten => 1004,2,Voicemail(1004,u)
exten => 1004,3,Hangup()
exten => 1004,102,Voicemail(1004,b)
exten => 1004,103,Hangup()
#Enlace al Voice mail
exten => 81001,1,VoiceMailMain(1001,s)
exten => 81001,2,Hangup()
exten => 81002,1,VoiceMailMain(1002,s)
exten => 81002,2,Hangup()
exten => 81003,1,VoiceMailMain(1003,s)
exten => 81003,2,Hangup()
exten => 81004,1,VoiceMailMain(1004,s)

exten => 81004,2,Hangup()
#Acceso a la cuenta
*exten => *86,1,VoiceMailMain*
*exten => *86,2,Hangup()*

include => aplicaciones
exten =>
_2XXX,1,Dial(SIP/${EXTEN}@troncal,10)
exten => _2XXX,n,Hangup()

[directorio]
exten => 8,1,Directory(default,internos,f)
exten => 9,1,Directory(default,internos)

[aplicaciones]
exten => 9999,1,Answer()
exten => 9999,n,Playback(hello-world)
exten => 9999,n,Hangup()
;Grabacion de mensaje de bienvenida
exten => 9991,1,Answer()
exten => 9991,n,Wait(0.5)
exten => 9991,n,Record(bienvenida.gsm)
exten => 9991,n,Wait(0.5)
exten => 9991,n,Playback(bienvenida)
exten => 9991,n,Hangup()

exten => 9000,1,Goto(ivr,s,1)

; Configuración del IVR
[ivr]
exten => s,1,Answer()
exten => s,n,Wait(0.5)
exten => s,n,Background(bienvenida)
exten => s,n,WaitExten(5)

exten => 1,1,Goto(internos,1001,1)
exten => 2,1,Goto(internos,1002,1)
exten => 3,1,Goto(internos,1003,1)
exten => 4,1,Goto(internos,1004,1)
exten => 5,1,Goto(internos,2001,1) ; hacia la Troncal
*exten => *,1,Goto(s,1)*

exten => t,1,Playback(en/goodbye)
exten => t,n,Hangup()
exten => i,1,Playback(en/pbx-invalid)
exten => i,n,Goto(s,1)

voicemail.conf (Archivo que corresponde al buzón de voz)

[general]
#format=wav49|gsm|wav
[default]
1001 => 4242,pepe
1002 => 4242,juan
1003 => 4242,pedro
1004 => 4242,secretaria

Anexo 2

Configuración de Routers Vyatta

Interfaces de Troncal

```
ethernet eth0 {
    address 10.1.1.1/24
    address
2001:db8:1::1/64
    duplex auto
    hw-id
00:08:a1:84:45:35
    smp_affinity auto
    speed auto
    traffic-policy {
    }
}
ethernet eth1 {
    address 192.168.40.1/24
    duplex auto
    hw-id 00:d0:09:f8:cc:b2
    smp_affinity auto
    speed auto
    traffic-policy {
out QOSTRONCAL
    }
}
loopback lo {
}
```

Configuración de Túnel SIT

```
tunnel tun0 {
 address
2001:db8:3::2/64
    encapsulation sit
    local-ip 192.168.40.1
    multicast disable
    remote-ip
192.168.40.2
```

QoS en Router “Troncal”

```
rate-control LIMITAR {
    bandwidth 1024kbit
    burst 15k
    description "Limirat 1024"
```

```
    latency 50ms
  }
  shaper QOSTRONCAL {
    bandwidth 1024Kbit
    class 10 {
      bandwidth 90%
      burst 15k
      ceiling 100%
      description RTP
      match VOIP-RTP {
IPv6 {
          dscp 46
        }
      }
      queue-type fair-queue
    }
    class 20 {
      bandwidth 5%
      burst 15k
      ceiling 100%
      description SIP
      match VOIP-SIP {
IPv6 {
          dscp 26
        }
      }
      queue-type fair-queue
    }
    default {
      bandwidth 5%
      burst 15k
      ceiling 100%
queue-type fair-queue
    }
description "Politicas de Calidad de servicio"
}
```

Router Central

```
      Interfaces
      ethernet eth1 {
        address 192.168.40.2/24
        duplex auto
        hw-id 00:19:21:eb:8f:b2
        smp_affinity auto
        speed auto
        traffic-policy {
          out QoS
        }
```

```
        }
        ethernet eth2 {
            address 10.0.0.1/24
            address
        2001:db8:2::1/64
            duplex auto
            hw-id 00:08:54:47:6a:f9
            smp_affinity auto
            speed auto
            traffic-policy {
        }
        }
        loopback lo {
        }
```

#Configuración de QOS en Router Central

```
rate-control LIMITAR {
    bandwidth 1024kbit
    burst 15k
    description "Limitar 1024"
    latency 50ms
}
shaper QoS {
    bandwidth 1024kbit
    class 10 {
        bandwidth 90%
        burst 15k
        ceiling 100%
        description RTP
        match VOIP-RTP {
IPv6 {
            dscp 46
        }
        }
        queue-type fair-queue
    }
    class 20 {
        bandwidth 5%
        burst 15k
 ceiling 100%
        description SIP
        match VOIP-SIP {
IPv6 {
            dscp 26
        }
        }
        queue-type fair-queue
    }
```

```
    default {
        bandwidth 5%
        burst 15k
        ceiling 100%
queue-type fair-queue
}
    description "Politicas de Calidad de
servicio"
 }
```

Anexo 3

Configuración de Cancelador de eco por hardware

Cancelador de eco por hardware

/etc/dahdi/system.conf
 # Span 1: WCTDM/0 "Wildcard TDM410P"
(MASTER)
fxsks=1
echocanceller=mg2,1
fxsks=2
echocanceller=mg2,2
fxsks=3
echocanceller=mg2,3
fxsks=4
echocanceller=mg2,4

Anexo 4

Acontinuación se muestran los datos obtenidos con el sniffer Wireshark***(Anexo 5).*** Para obtener las diferentes tablas de resúmenes, se obtuvieron los promedios de los campos Delta (Latencia), Jitter, IP BW(Ancho de banda); de cada una de las tablas con el objetivo de obtener el Gran Total, el mismo que servirá para determinar la validez o no de la Tésis planteada.

Transmisión de VoIP sin QoS sobre IPv4

Delta (ms)	Jitter (ms)	IP BW (kbps)	Status
379,3	174,5	7,2	Wrong sequence nr.
897,4	202,5	4,0	Wrong sequence nr.
568,0	215,7	4,0	Wrong sequence nr.
1526,6	269,2	2,4	Wrong sequence nr.
765,7	279,3	4,0	Wrong sequence nr.
156,0	268,2	5,6	Wrong sequence nr.
661,2	276,8	5,6	Wrong sequence nr.
73,2	261,9	7,2	[Ok]
1182,3	286,0	2,4	Wrong sequence nr.
629,9	286,6	4,0	Wrong sequence nr.
535,2	283,7	4,0	Wrong sequence nr.
1671,7	308,3	2,4	Wrong sequence nr.
423,5	297,1	4,0	Wrong sequence nr.
43,4	281,6	5,6	[Ok]
179,5	266,0	7,2	Wrong sequence nr.
689,0	254,0	7,2	Wrong sequence nr.
62,9	243,7	8,8	Wrong sequence nr.
139,9	232,9	10,4	Wrong sequence nr.
612,5	223,2	7,2	Wrong sequence nr.
113,5	213,0	8,8	Wrong sequence nr.
588,2	218,0	5,6	Wrong sequence nr.
757,4	227,0	4,0	Wrong sequence nr.
329,5	220,0	4,0	Wrong sequence nr.
214,8	211,3	5,6	Wrong sequence nr.
669,3	221,5	5,6	Wrong sequence nr.
952,8	227,5	4,0	Wrong sequence nr.
650,3	224,3	4,0	Wrong sequence nr.
387,3	214,8	5,6	Wrong sequence nr.

262,7	204,4	5,6	Wrong sequence nr.
279,8	199,4	7,2	Wrong sequence nr.
305,0	188,9	7,2	Wrong sequence nr.
144,7	178,9	8,8	Wrong sequence nr.
64,2	170,7	10,4	Wrong sequence nr.
209,0	168,5	10,4	Wrong sequence nr.
654,4	171,7	8,8	Wrong sequence nr.
354,4	167,0	5,6	Wrong sequence nr.
278,2	164,3	5,6	Wrong sequence nr.
7675,7	557,8	2,4	Wrong sequence nr.
125,2	526,1	4,0	Wrong sequence nr.
154,2	499,3	5,6	Wrong sequence nr.
943,7	477,4	4,0	Wrong sequence nr.
149,1	452,8	4,0	Wrong sequence nr.
615,3	442,0	5,6	Wrong sequence nr.
175,0	416,9	7,2	Wrong sequence nr.
574,4	404,6	5,6	Wrong sequence nr.
64,5	381,2	7,2	[Ok]
953,6	374,8	5,6	Wrong sequence nr.
6377,6	726,5	2,4	Wrong sequence nr.
521,4	691,5	4,0	Wrong sequence nr.
1065,4	685,2	2,4	Wrong sequence nr.
905,8	674,4	4,0	Wrong sequence nr.
186,7	635,5	4,0	Wrong sequence nr.
43,4	598,8	5,6	[Ok]
368,8	573,5	7,2	Wrong sequence nr.
101,4	542,0	8,8	Wrong sequence nr.
87,4	510,9	10,4	Wrong sequence nr.
609,3	498,7	10,4	Wrong sequence nr.
1424,7	501,9	2,4	Wrong sequence nr.
3582,1	593,5	2,4	Wrong sequence nr.
501,3	569,3	4,0	Wrong sequence nr.
5981,7	786,6	2,4	Wrong sequence nr.
347,5	744,5	4,0	Wrong sequence nr.
937,5	713,2	4,0	Wrong sequence nr.
249,8	670,8	4,0	Wrong sequence nr.
1066,3	657,1	2,4	Wrong sequence nr.
196,8	622,4	4,0	Wrong sequence nr.
429,6	597,0	5,6	Wrong sequence nr.
395,8	566,0	7,2	Wrong sequence nr.
160,9	533,8	7,2	Wrong sequence nr.
347,6	503,7	7,2	Wrong sequence nr.
43,5	475,3	8,8	[Ok]

330,6	448,1	8,8	Wrong sequence nr.
300,7	423,0	10,4	Wrong sequence nr.
5990,2	715,0	2,4	Wrong sequence nr.
1012,0	687,7	4,0	Wrong sequence nr.
1841,2	695,1	2,4	Wrong sequence nr.
517,0	669,3	4,0	Wrong sequence nr.
744,3	643,1	4,0	Wrong sequence nr.
385,7	611,1	4,0	Wrong sequence nr.
656,1	586,7	5,6	Wrong sequence nr.
1684,7	591,9	2,4	Wrong sequence nr.
234,4	558,7	4,0	Wrong sequence nr.
178,5	527,7	5,6	Wrong sequence nr.
1009,1	511,9	4,0	Wrong sequence nr.
1841,5	529,1	2,4	Wrong sequence nr.
161,0	501,4	4,0	Wrong sequence nr.
74,1	472,5	5,6	[Ok]
53,0	445,4	7,2	[Ok]
667,7	435,9	8,8	Wrong sequence nr.
480,3	425,3	4,0	Wrong sequence nr.
1709,4	435,9	2,4	Wrong sequence nr.
64,3	411,6	4,0	Wrong sequence nr.
236,2	393,5	5,6	Wrong sequence nr.
1026,6	408,4	4,0	Wrong sequence nr.
2985,8	507,3	2,4	Wrong sequence nr.
281,9	479,8	4,0	Wrong sequence nr.
177,5	455,0	5,6	Wrong sequence nr.
1050,6	451,3	2,4	Wrong sequence nr.
317,9	429,5	4,0	Wrong sequence nr.
501,0	408,1	5,6	Wrong sequence nr.
298,1	389,0	7,2	Wrong sequence nr.
157,2	369,9	7,2	Wrong sequence nr.
102,0	348,6	8,8	Wrong sequence nr.
555,9	348,2	8,8	Wrong sequence nr.
43,2	329,4	10,4	[Ok]
1581,2	360,5	2,4	Wrong sequence nr.
704,8	361,1	4,0	Wrong sequence nr.
366,5	345,5	5,6	Wrong sequence nr.
669,5	339,9	5,6	Wrong sequence nr.
139,6	322,7	5,6	Wrong sequence nr.
274,9	307,5	7,2	Wrong sequence nr.
1517,6	326,0	2,4	Wrong sequence nr.
83,8	308,7	4,0	[Ok]
650,9	301,7	5,6	Wrong sequence nr.

289,5	291,2	7,2	Wrong sequence nr.
385,6	285,0	5,6	Wrong sequence nr.
917,9	288,6	4,0	Wrong sequence nr.
43,2	273,6	5,6	[Ok]
849,3	283,7	5,6	Wrong sequence nr.
43,2	269,0	7,2	[Ok]
588,8	270,5	5,6	Wrong sequence nr.
479,8	268,9	7,2	Wrong sequence nr.
533,7	268,3	5,6	Wrong sequence nr.
63,8	253,4	7,2	[Ok]
339,6	245,4	7,2	Wrong sequence nr.
699,4	246,6	7,2	Wrong sequence nr.
194,8	238,7	5,6	Wrong sequence nr.
347,1	237,0	5,6	Wrong sequence nr.
2578,5	314,9	2,4	Wrong sequence nr.
236,5	301,6	4,0	Wrong sequence nr.
232,5	288,9	5,6	Wrong sequence nr.
952,7	297,0	4,0	Wrong sequence nr.
45,3	281,3	5,6	[Ok]
385,3	275,6	5,6	Wrong sequence nr.
73,0	260,8	7,2	[Ok]
1322,1	287,5	2,4	Wrong sequence nr.
64,1	272,5	4,0	Wrong sequence nr.
43,4	258,5	5,6	[Ok]
1087,2	269,4	2,4	Wrong sequence nr.
143,0	256,8	4,0	Wrong sequence nr.
836,2	267,1	5,6	Wrong sequence nr.
970,5	270,1	4,0	Wrong sequence nr.
538,0	269,7	4,0	Wrong sequence nr.
2873,1	359,0	2,4	Wrong sequence nr.
306,9	351,1	4,0	Wrong sequence nr.
171,0	337,7	5,6	[Ok]
464,2	325,9	7,2	Wrong sequence nr.
212,1	310,4	8,8	Wrong sequence nr.
1142,1	326,4	2,4	Wrong sequence nr.
210,6	313,3	4,0	Wrong sequence nr.
68,9	297,6	5,6	Wrong sequence nr.
822,5	294,5	7,2	Wrong sequence nr.
163,8	284,2	7,2	[Ok]
113,8	268,8	8,8	Wrong sequence nr.
236,6	257,1	7,2	Wrong sequence nr.
99,7	243,1	8,8	Wrong sequence nr.
43,2	230,9	10,4	[Ok]

519,6	233,0	12,0	Wrong sequence nr.
274,0	228,4	10,4	Wrong sequence nr.
611,6	233,9	5,6	Wrong sequence nr.
218,3	229,6	7,2	Wrong sequence nr.
2976,7	347,8	2,4	Wrong sequence nr.
346,5	331,4	4,0	Wrong sequence nr.
43,2	313,7	5,6	[Ok]
933,4	314,1	5,6	Wrong sequence nr.
555,8	302,0	4,0	Wrong sequence nr.
367,7	295,2	5,6	Wrong sequence nr.
2464,8	374,9	2,4	Wrong sequence nr.
102,3	354,4	4,0	Wrong sequence nr.
196,2	339,9	5,6	Wrong sequence nr.
559,4	333,9	7,2	Wrong sequence nr.
2575,8	370,6	2,4	Wrong sequence nr.
196,7	354,6	4,0	Wrong sequence nr.
252,4	338,6	5,6	Wrong sequence nr.
102,6	319,2	7,2	Wrong sequence nr.
877,1	318,2	5,6	Wrong sequence nr.
139,9	301,1	7,2	Wrong sequence nr.
83,1	285,3	7,2	[Ok]
177,0	270,2	7,2	Wrong sequence nr.
1029,0	296,7	4,0	Wrong sequence nr.
536,5	294,5	4,0	Wrong sequence nr.
103,1	280,4	5,6	[Ok]
109,3	267,5	7,2	[Ok]
173,5	253,2	8,8	Wrong sequence nr.
253,4	239,8	10,4	Wrong sequence nr.
494,2	233,5	10,4	Wrong sequence nr.
101,9	221,9	12,0	Wrong sequence nr.
161,1	209,9	10,4	Wrong sequence nr.
232,2	199,3	8,8	Wrong sequence nr.
63,8	188,6	10,4	[Ok]
2976,7	280,7	2,4	Wrong sequence nr.
1483,6	310,0	2,4	Wrong sequence nr.
309,1	296,5	4,0	Wrong sequence nr.
498,9	287,0	5,6	Wrong sequence nr.
1200,9	301,9	2,4	Wrong sequence nr.
119,0	286,4	4,0	Wrong sequence nr.
1463,2	325,3	2,4	Wrong sequence nr.
959,9	345,3	4,0	Wrong sequence nr.
927,2	365,7	4,0	Wrong sequence nr.
404,6	359,7	4,0	Wrong sequence nr.

43,4	340,3	5,6	[Ok]
1109,5	364,9	2,4	Wrong sequence nr.
175,2	347,1	4,0	Wrong sequence nr.
327,5	337,5	5,6	Wrong sequence nr.
404,4	329,5	7,2	Wrong sequence nr.
6419,1	619,2	2,4	Wrong sequence nr.
954,9	623,0	4,0	Wrong sequence nr.
1162,6	632,1	2,4	Wrong sequence nr.
136,0	597,6	4,0	Wrong sequence nr.
1899,5	618,1	2,4	Wrong sequence nr.
422,5	590,0	4,0	Wrong sequence nr.
993,1	588,0	4,0	Wrong sequence nr.
43,2	554,3	5,6	[Ok]
632,8	532,0	5,6	Wrong sequence nr.
479,3	514,0	4,0	Wrong sequence nr.
43,2	485,0	5,6	[Ok]
1937,7	508,6	2,4	Wrong sequence nr.
43,4	479,8	4,0	[Ok]
652,1	468,4	5,6	Wrong sequence nr.
3280,7	523,3	2,4	Wrong sequence nr.
3426,0	560,0	2,4	Wrong sequence nr.
43,2	528,1	4,0	[Ok]
1843,4	535,6	2,4	Wrong sequence nr.
1306,3	545,3	2,4	Wrong sequence nr.
43,2	514,3	4,0	[Ok]
872,7	507,0	5,6	Wrong sequence nr.
4711,1	655,1	2,4	Wrong sequence nr.
139,0	618,2	4,0	Wrong sequence nr.
4414,5	777,0	2,4	Wrong sequence nr.
517,4	746,2	4,0	Wrong sequence nr.
123,8	703,8	5,6	Wrong sequence nr.
1252,8	697,2	2,4	Wrong sequence nr.
1375,5	713,7	2,4	Wrong sequence nr.
136,0	671,7	4,0	Wrong sequence nr.
1310,1	675,7	2,4	Wrong sequence nr.
1769,3	711,9	2,4	Wrong sequence nr.
743,6	696,7	4,0	Wrong sequence nr.
439,9	674,7	4,0	Wrong sequence nr.
1501,3	681,7	2,4	Wrong sequence nr.
234,3	644,1	4,0	Wrong sequence nr.
518,1	612,8	5,6	Wrong sequence nr.
184,7	581,4	7,2	Wrong sequence nr.
926,7	577,0	4,0	Wrong sequence nr.

801,8	565,2	4,0	Wrong sequence nr.
311,7	533,4	4,0	Wrong sequence nr.
591,8	516,1	5,6	Wrong sequence nr.
139,7	487,1	7,2	Wrong sequence nr.
63,9	458,5	8,8	[Ok]
281,4	437,8	8,8	Wrong sequence nr.
2268,4	485,0	2,4	Wrong sequence nr.
139,0	457,5	4,0	Wrong sequence nr.
291,0	438,7	5,6	Wrong sequence nr.
404,4	428,1	7,2	Wrong sequence nr.
783,0	431,9	4,0	Wrong sequence nr.
766,1	441,8	4,0	Wrong sequence nr.
801,5	442,1	4,0	Wrong sequence nr.
3069,5	524,2	2,4	Wrong sequence nr.
179,5	496,7	4,0	Wrong sequence nr.
404,1	473,8	5,6	Wrong sequence nr.
100,0	449,9	7,2	Wrong sequence nr.
139,4	428,3	8,8	[Ok]
574,1	421,5	7,2	Wrong sequence nr.
65,1	399,3	8,8	Wrong sequence nr.
347,4	380,2	8,8	Wrong sequence nr.
1444,7	390,8	2,4	Wrong sequence nr.

Transmisión de VoIP sin QoS sobre IPv6

Delta (ms)	Jitter (ms)	IP BW (kbps)	Status
392,3	244,2	7,5	Wrong sequence nr.
910,3	272,2	4,3	Wrong sequence nr.
580,9	285,3	4,3	Wrong sequence nr.
1539,5	338,9	2,7	Wrong sequence nr.
778,6	349,0	4,3	Wrong sequence nr.
168,9	337,9	5,9	Wrong sequence nr.
674,1	346,5	5,9	Wrong sequence nr.
86,1	331,6	7,5	[Ok]
1195,2	355,7	2,7	Wrong sequence nr.
642,8	356,3	4,3	Wrong sequence nr.
548,1	353,4	4,3	Wrong sequence nr.
1684,6	378,0	2,7	Wrong sequence nr.
436,4	366,8	4,3	Wrong sequence nr.
56,3	351,2	5,9	[Ok]

192,4	335,6	7,5	Wrong sequence nr.
701,9	323,7	7,5	Wrong sequence nr.
75,8	313,3	9,1	Wrong sequence nr.
152,8	302,6	10,7	Wrong sequence nr.
625,4	292,9	7,5	Wrong sequence nr.
126,4	282,6	9,1	Wrong sequence nr.
601,1	287,7	5,9	Wrong sequence nr.
770,3	296,7	4,3	Wrong sequence nr.
342,4	289,7	4,3	Wrong sequence nr.
227,7	281,0	5,9	Wrong sequence nr.
682,2	291,2	5,9	Wrong sequence nr.
965,7	297,2	4,3	Wrong sequence nr.
663,2	294,0	4,3	Wrong sequence nr.
400,2	284,5	5,9	Wrong sequence nr.
275,6	274,1	5,9	Wrong sequence nr.
292,7	269,1	7,5	Wrong sequence nr.
317,9	258,5	7,5	Wrong sequence nr.
157,6	248,6	9,1	Wrong sequence nr.
77,1	240,4	10,7	Wrong sequence nr.
221,9	238,1	10,7	Wrong sequence nr.
667,3	241,3	9,1	Wrong sequence nr.
367,3	236,7	5,9	Wrong sequence nr.
291,1	234,0	5,9	Wrong sequence nr.
7688,6	627,5	2,7	Wrong sequence nr.
138,1	595,8	4,3	Wrong sequence nr.
167,1	569,0	5,9	Wrong sequence nr.
956,6	547,1	4,3	Wrong sequence nr.
162,0	522,4	4,3	Wrong sequence nr.
628,2	511,7	5,9	Wrong sequence nr.
187,9	486,6	7,5	Wrong sequence nr.
587,4	474,2	5,9	Wrong sequence nr.
77,5	450,8	7,5	[Ok]
966,5	444,4	5,9	Wrong sequence nr.
6390,5	796,2	2,7	Wrong sequence nr.
534,3	761,2	4,3	Wrong sequence nr.
1078,3	754,9	2,7	Wrong sequence nr.
918,7	744,0	4,3	Wrong sequence nr.
199,6	705,1	4,3	Wrong sequence nr.
56,3	668,4	5,9	[Ok]
381,7	643,1	7,5	Wrong sequence nr.
114,4	611,7	9,1	Wrong sequence nr.
100,4	580,6	10,7	Wrong sequence nr.
622,2	568,3	10,7	Wrong sequence nr.

1437,6	571,5	2,7	Wrong sequence nr.
3595,0	663,1	2,7	Wrong sequence nr.
514,3	639,0	4,3	Wrong sequence nr.
5994,6	856,3	2,7	Wrong sequence nr.
360,4	814,2	4,3	Wrong sequence nr.
950,4	782,8	4,3	Wrong sequence nr.
262,7	740,5	4,3	Wrong sequence nr.
1079,3	726,8	2,7	Wrong sequence nr.
209,7	692,1	4,3	Wrong sequence nr.
442,6	666,6	5,9	Wrong sequence nr.
408,7	635,6	7,5	Wrong sequence nr.
173,8	603,4	7,5	Wrong sequence nr.
360,5	573,4	7,5	Wrong sequence nr.
56,4	544,9	9,1	[Ok]
343,5	517,8	9,1	Wrong sequence nr.
313,6	492,7	10,7	Wrong sequence nr.
6003,2	784,7	2,7	Wrong sequence nr.
1024,9	757,3	4,3	Wrong sequence nr.
1854,1	764,8	2,7	Wrong sequence nr.
529,9	739,0	4,3	Wrong sequence nr.
757,2	712,7	4,3	Wrong sequence nr.
398,6	680,7	4,3	Wrong sequence nr.
669,0	656,4	5,9	Wrong sequence nr.
1697,6	661,6	2,7	Wrong sequence nr.
247,3	628,3	4,3	Wrong sequence nr.
191,4	597,4	5,9	Wrong sequence nr.
1022,0	581,6	4,3	Wrong sequence nr.
1854,4	598,8	2,7	Wrong sequence nr.
173,9	571,1	4,3	Wrong sequence nr.
87,0	542,2	5,9	[Ok]
65,9	515,1	7,5	[Ok]
680,6	505,6	9,1	Wrong sequence nr.
493,2	494,9	4,3	Wrong sequence nr.
1722,3	505,5	2,7	Wrong sequence nr.
77,2	481,2	4,3	Wrong sequence nr.
249,1	463,1	5,9	Wrong sequence nr.
1039,5	478,0	4,3	Wrong sequence nr.
2998,7	576,9	2,7	Wrong sequence nr.
294,8	549,4	4,3	Wrong sequence nr.
190,4	524,6	5,9	Wrong sequence nr.
1063,6	520,9	2,7	Wrong sequence nr.
330,8	499,2	4,3	Wrong sequence nr.
513,9	477,7	5,9	Wrong sequence nr.

311,0	458,7	7,5	Wrong sequence nr.
170,1	439,5	7,5	Wrong sequence nr.
115,0	418,3	9,1	Wrong sequence nr.
568,8	417,8	9,1	Wrong sequence nr.
56,1	399,1	10,7	[Ok]
1594,1	430,2	2,7	Wrong sequence nr.
717,7	430,8	4,3	Wrong sequence nr.
379,4	415,2	5,9	Wrong sequence nr.
682,4	409,5	5,9	Wrong sequence nr.
152,6	392,3	5,9	Wrong sequence nr.
287,8	377,2	7,5	Wrong sequence nr.
1530,5	395,6	2,7	Wrong sequence nr.
96,7	378,3	4,3	[Ok]
663,8	371,3	5,9	Wrong sequence nr.
302,4	360,9	7,5	Wrong sequence nr.
398,5	354,6	5,9	Wrong sequence nr.
930,8	358,3	4,3	Wrong sequence nr.
56,1	343,3	5,9	[Ok]
862,2	353,3	5,9	Wrong sequence nr.
56,1	338,6	7,5	[Ok]
601,7	340,2	5,9	Wrong sequence nr.
492,7	338,6	7,5	Wrong sequence nr.
546,6	338,0	5,9	Wrong sequence nr.
76,7	323,0	7,5	[Ok]
352,5	315,0	7,5	Wrong sequence nr.
712,3	316,2	7,5	Wrong sequence nr.
207,8	308,3	5,9	Wrong sequence nr.
360,0	306,7	5,9	Wrong sequence nr.
2591,4	384,6	2,7	Wrong sequence nr.
249,4	371,3	4,3	Wrong sequence nr.
245,4	358,6	5,9	Wrong sequence nr.
965,7	366,6	4,3	Wrong sequence nr.
58,2	351,0	5,9	[Ok]
398,2	345,3	5,9	Wrong sequence nr.
85,9	330,5	7,5	[Ok]
1335,1	357,1	2,7	Wrong sequence nr.
77,0	342,1	4,3	Wrong sequence nr.
56,3	328,1	5,9	[Ok]
1100,1	339,0	2,7	Wrong sequence nr.
155,9	326,5	4,3	Wrong sequence nr.
849,2	336,7	5,9	Wrong sequence nr.
983,4	339,8	4,3	Wrong sequence nr.
550,9	339,4	4,3	Wrong sequence nr.

2886,0	428,7	2,7	Wrong sequence nr.
319,8	420,7	4,3	Wrong sequence nr.
183,9	407,3	5,9	[Ok]
477,1	395,6	7,5	Wrong sequence nr.
225,0	380,0	9,1	Wrong sequence nr.
1155,0	396,1	2,7	Wrong sequence nr.
223,5	382,9	4,3	Wrong sequence nr.
81,8	367,3	5,9	Wrong sequence nr.
835,4	364,2	7,5	Wrong sequence nr.
176,7	353,8	7,5	[Ok]
126,7	338,5	9,1	Wrong sequence nr.
249,5	326,8	7,5	Wrong sequence nr.
112,6	312,7	9,1	Wrong sequence nr.
56,1	300,6	10,7	[Ok]
532,5	302,7	12,3	Wrong sequence nr.
286,9	298,1	10,7	Wrong sequence nr.
624,5	303,6	5,9	Wrong sequence nr.
231,2	299,2	7,5	Wrong sequence nr.
2989,6	417,5	2,7	Wrong sequence nr.
359,4	401,1	4,3	Wrong sequence nr.
56,1	383,4	5,9	[Ok]
946,3	383,7	5,9	Wrong sequence nr.
568,7	371,7	4,3	Wrong sequence nr.
380,6	364,8	5,9	Wrong sequence nr.
2477,7	444,5	2,7	Wrong sequence nr.
115,3	424,1	4,3	Wrong sequence nr.
209,1	409,5	5,9	Wrong sequence nr.
572,3	403,6	7,5	Wrong sequence nr.
152,6	556,8	7,5	Wrong sequence nr.
76,8	528,2	9,1	[Ok]
294,3	507,4	9,1	Wrong sequence nr.
2281,3	554,7	2,7	Wrong sequence nr.
151,9	527,1	4,3	Wrong sequence nr.
303,9	508,3	5,9	Wrong sequence nr.
417,3	497,8	7,5	Wrong sequence nr.
795,9	501,5	4,3	Wrong sequence nr.
779,0	511,5	4,3	Wrong sequence nr.
814,4	511,8	4,3	Wrong sequence nr.
3082,4	593,9	2,7	Wrong sequence nr.
192,4	566,4	4,3	Wrong sequence nr.
417,0	543,4	5,9	Wrong sequence nr.
112,9	519,6	7,5	Wrong sequence nr.
152,3	498,0	9,1	[Ok]

587,1	491,2	7,5	Wrong sequence nr.
115,5	388,9	7,5	Wrong sequence nr.
890,0	387,9	5,9	Wrong sequence nr.
152,8	370,8	7,5	Wrong sequence nr.
96,0	355,0	7,5	[Ok]
189,9	339,8	7,5	Wrong sequence nr.
1041,9	366,3	4,3	Wrong sequence nr.
549,5	364,2	4,3	Wrong sequence nr.
116,0	350,0	5,9	[Ok]
122,2	337,2	7,5	[Ok]
186,4	322,8	9,1	Wrong sequence nr.
266,4	309,4	10,7	Wrong sequence nr.
507,1	303,2	10,7	Wrong sequence nr.
114,8	291,5	12,3	Wrong sequence nr.
174,0	279,6	10,7	Wrong sequence nr.
245,2	268,9	9,1	Wrong sequence nr.
76,7	258,3	10,7	[Ok]
2989,6	350,4	2,7	Wrong sequence nr.
1496,5	379,6	2,7	Wrong sequence nr.
322,0	366,2	4,3	Wrong sequence nr.
511,8	356,6	5,9	Wrong sequence nr.
1213,8	371,6	2,7	Wrong sequence nr.
131,9	356,0	4,3	Wrong sequence nr.
1476,1	394,9	2,7	Wrong sequence nr.
972,8	414,9	4,3	Wrong sequence nr.
940,1	435,4	4,3	Wrong sequence nr.
417,5	429,4	4,3	Wrong sequence nr.
56,3	409,9	5,9	[Ok]
1122,4	434,6	2,7	Wrong sequence nr.
188,1	416,8	4,3	Wrong sequence nr.
340,5	407,2	5,9	Wrong sequence nr.
417,3	399,2	7,5	Wrong sequence nr.
6432,0	688,9	2,7	Wrong sequence nr.
967,8	692,7	4,3	Wrong sequence nr.
1175,5	701,7	2,7	Wrong sequence nr.
148,9	667,3	4,3	Wrong sequence nr.
1912,4	687,8	2,7	Wrong sequence nr.
435,4	659,6	4,3	Wrong sequence nr.
1006,0	657,6	4,3	Wrong sequence nr.
56,1	623,9	5,9	[Ok]
645,7	601,7	5,9	Wrong sequence nr.
492,3	583,7	4,3	Wrong sequence nr.
56,1	554,6	5,9	[Ok]

1950,6	578,2	2,7	Wrong sequence nr.
56,3	549,5	4,3	[Ok]
665,0	538,1	5,9	Wrong sequence nr.
3293,6	592,9	2,7	Wrong sequence nr.
3438,9	629,7	2,7	Wrong sequence nr.
56,1	597,7	4,3	[Ok]
1856,3	605,3	2,7	Wrong sequence nr.
1319,2	615,0	2,7	Wrong sequence nr.
56,1	584,0	4,3	[Ok]
885,6	576,7	5,9	Wrong sequence nr.
4724,0	724,8	2,7	Wrong sequence nr.
151,9	687,8	4,3	Wrong sequence nr.
4427,4	846,7	2,7	Wrong sequence nr.
530,3	815,8	4,3	Wrong sequence nr.
136,7	773,5	5,9	Wrong sequence nr.
1265,7	766,9	2,7	Wrong sequence nr.
1388,4	783,4	2,7	Wrong sequence nr.
148,9	741,3	4,3	Wrong sequence nr.
1323,0	745,3	2,7	Wrong sequence nr.
1782,2	781,5	2,7	Wrong sequence nr.
756,5	766,3	4,3	Wrong sequence nr.
452,8	744,4	4,3	Wrong sequence nr.
1514,2	751,4	2,7	Wrong sequence nr.
247,2	713,7	4,3	Wrong sequence nr.
531,0	682,4	5,9	Wrong sequence nr.
197,6	651,0	7,5	Wrong sequence nr.
939,7	646,7	4,3	Wrong sequence nr.
814,7	634,8	4,3	Wrong sequence nr.
324,6	603,1	4,3	Wrong sequence nr.
78,0	469,0	9,1	Wrong sequence nr.
360,3	449,8	9,1	Wrong sequence nr.
2588,7	440,3	2,7	Wrong sequence nr.
209,7	424,3	4,3	Wrong sequence nr.
265,3	408,2	5,9	Wrong sequence nr.
604,7	585,8	5,9	Wrong sequence nr.

Transmisión de VoIP con QoS sobre IPv6

Delta (ms)	Jitter (ms)	IP BW (kbps)	Status
19,1	5,0	4,2	[Ok]
19,3	5,1	4,9	[Ok]

19,4	14,9	5,7	[Ok]
19,9	15,4	6,4	[Ok]
20,1	14,7	7,2	[Ok]
20,5	15,2	7,9	[Ok]
20,6	15,7	8,7	[Ok]
20,6	16,2	9,4	[Ok]
20,7	16,6	10,1	[Ok]
20,8	17,1	10,9	[Ok]
20,9	17,5	11,6	[Ok]
20,9	17,8	12,4	[Ok]
20,9	17,1	13,1	[Ok]
21,0	17,5	13,9	[Ok]
21,0	18,2	14,6	[Ok]
21,4	18,5	15,3	[Ok]
21,5	19,0	16,1	[Ok]
21,6	19,3	16,8	[Ok]
21,7	19,1	17,6	[Ok]
21,8	19,4	18,3	[Ok]
21,8	19,9	19,1	[Ok]
21,9	20,1	19,8	[Ok]
21,9	20,6	20,6	[Ok]
21,9	20,7	21,3	[Ok]
22,0	20,5	22,0	[Ok]
22,0	20,6	22,8	[Ok]
22,1	20,9	23,5	[Ok]
22,4	21,0	24,3	[Ok]
22,5	20,8	25,0	[Ok]
22,5	20,9	25,8	[Ok]
22,5	21,4	26,5	[Ok]
22,5	21,5	27,3	[Ok]
22,6	21,9	28,0	[Ok]
22,6	22,0	28,7	[Ok]
22,7	20,9	29,5	[Ok]
22,7	21,0	30,2	[Ok]
22,7	21,8	31,0	[Ok]
22,7	21,9	31,7	[Ok]
22,7	21,8	32,5	[Ok]
22,7	21,9	33,2	[Ok]
22,8	21,6	33,9	[Ok]
22,8	21,7	34,7	[Ok]
22,8	22,0	35,4	[Ok]
22,8	22,1	36,2	[Ok]
22,8	22,4	36,9	[Ok]

22,8	22,5	37,7	[Ok]
22,8	24,8	38,4	[Ok]
22,9	24,7	39,2	[Ok]
22,9	24,5	39,9	[Ok]
22,9	24,4	40,6	[Ok]
22,9	24,6	39,3	[Ok]
22,9	24,5	40,1	[Ok]
22,9	24,7	40,1	[Ok]
22,9	24,6	40,8	[Ok]
22,9	24,1	41,5	[Ok]
22,9	24,0	42,3	[Ok]
22,9	24,3	43,0	[Ok]
23,0	24,2	43,8	[Ok]
23,0	24,3	44,5	[Ok]
23,0	24,2	45,3	[Ok]
23,0	23,8	44,5	[Ok]
23,0	23,8	45,3	[Ok]
23,0	23,9	38,6	[Ok]
23,0	23,7	39,3	[Ok]
23,0	24,0	38,6	[Ok]
23,0	24,0	39,3	[Ok]
23,0	22,7	40,1	[Ok]
23,1	22,8	40,8	[Ok]
23,1	23,0	40,1	[Ok]
23,1	23,0	40,8	[Ok]
23,1	23,4	40,1	[Ok]
23,1	23,4	40,8	[Ok]
23,1	23,4	40,1	[Ok]
23,1	23,4	40,8	[Ok]
23,1	23,0	40,1	[Ok]
23,1	23,0	40,8	[Ok]
23,1	23,5	40,1	[Ok]
23,2	23,5	40,8	[Ok]
23,2	26,2	38,6	[Ok]
23,2	26,0	39,3	[Ok]
23,2	25,9	40,1	[Ok]
23,2	25,7	40,8	[Ok]
23,2	25,4	40,1	[Ok]
23,2	25,3	40,8	[Ok]
23,2	25,4	38,6	[Ok]
23,2	25,2	39,3	[Ok]
23,2	24,9	38,6	[Ok]
23,2	24,8	39,3	[Ok]

23,2	24,8	38,6	[Ok]
23,2	24,7	39,3	[Ok]
23,2	24,2	38,6	[Ok]
23,2	24,1	39,3	[Ok]
23,2	24,3	38,6	[Ok]
23,2	24,2	39,3	[Ok]
23,2	24,5	38,6	[Ok]
23,2	24,5	39,3	[Ok]
23,2	24,4	40,1	[Ok]
23,2	24,4	40,8	[Ok]
23,2	23,9	38,6	[Ok]
23,2	23,8	39,3	[Ok]
23,2	23,5	40,1	[Ok]
23,2	23,5	40,8	[Ok]
23,2	23,6	40,1	[Ok]
23,2	23,6	40,8	[Ok]
23,3	23,2	40,1	[Ok]
23,3	23,2	40,8	[Ok]
23,3	23,5	40,1	[Ok]
23,3	23,5	40,8	[Ok]
23,3	23,6	40,1	[Ok]
23,3	23,6	40,8	[Ok]
23,3	23,2	40,1	[Ok]
23,3	23,2	40,8	[Ok]
23,3	25,1	38,6	[Ok]
23,3	25,0	39,3	[Ok]
23,3	23,8	40,1	[Ok]
23,3	23,8	40,8	[Ok]
23,3	23,6	38,6	[Ok]
23,3	23,6	39,3	[Ok]
23,3	23,5	38,6	[Ok]
23,3	23,4	39,3	[Ok]
23,3	23,7	38,6	[Ok]
23,3	23,7	39,3	[Ok]
23,3	23,8	38,6	[Ok]
23,3	23,7	39,3	[Ok]
23,3	23,4	38,6	[Ok]
23,3	23,3	39,3	[Ok]
23,3	23,6	38,6	[Ok]
23,3	23,6	39,3	[Ok]
23,3	23,9	40,1	[Ok]
23,3	23,9	40,8	[Ok]
23,3	22,6	41,5	[Ok]

23,3	22,7	42,3	[Ok]
23,4	23,1	40,1	[Ok]
23,4	23,1	40,8	[Ok]
23,4	23,2	40,1	[Ok]
23,4	23,2	40,8	[Ok]
23,4	23,2	40,1	[Ok]
23,4	23,2	40,8	[Ok]
23,4	23,3	40,1	[Ok]
23,4	23,3	40,8	[Ok]
23,4	22,9	40,1	[Ok]
23,4	22,9	40,8	[Ok]
23,4	23,2	40,1	[Ok]
23,4	23,2	40,8	[Ok]
23,4	25,6	38,6	[Ok]
23,4	25,5	39,3	[Ok]
23,4	25,4	40,1	[Ok]
23,4	25,2	40,8	[Ok]
23,4	25,4	38,6	[Ok]
23,5	25,3	39,3	[Ok]
23,5	25,3	38,6	[Ok]
23,5	25,2	39,3	[Ok]
23,5	24,7	40,1	[Ok]
23,5	24,6	40,8	[Ok]
23,5	24,8	38,6	[Ok]
23,5	24,7	39,3	[Ok]
23,5	24,9	38,6	[Ok]
23,5	24,8	39,3	[Ok]
23,5	24,2	40,1	[Ok]
23,5	24,2	40,8	[Ok]
23,5	24,6	38,6	[Ok]
23,5	24,5	39,3	[Ok]
23,5	23,8	40,1	[Ok]
23,5	23,8	40,8	[Ok]
23,5	23,4	40,1	[Ok]
23,5	23,4	40,8	[Ok]
23,5	23,7	40,1	[Ok]
23,5	23,6	40,8	[Ok]
23,5	23,8	38,6	[Ok]
23,5	23,7	39,3	[Ok]
23,5	23,3	40,1	[Ok]
23,5	23,3	40,8	[Ok]
23,5	23,5	40,1	[Ok]
23,5	23,3	40,8	[Ok]

23,5	23,5	38,6	[Ok]
23,5	23,5	39,3	[Ok]
23,5	23,1	40,1	[Ok]
23,6	23,1	40,8	[Ok]
23,6	23,5	40,1	[Ok]
23,6	23,4	40,8	[Ok]
23,6	23,0	38,6	[Ok]
23,6	23,0	39,3	[Ok]
23,6	23,3	38,6	[Ok]
23,6	23,3	39,3	[Ok]
23,6	23,5	38,6	[Ok]
23,6	23,5	39,3	[Ok]
23,6	26,3	37,1	[Ok]
23,6	26,1	37,8	[Ok]
23,6	25,9	38,6	[Ok]
23,6	25,8	39,3	[Ok]
23,6	25,4	38,6	[Ok]
23,6	25,3	39,3	[Ok]
23,6	24,7	38,6	[Ok]
23,6	24,7	39,3	[Ok]
23,6	24,1	40,1	[Ok]
23,6	24,1	40,8	[Ok]
23,6	24,3	41,5	[Ok]
23,6	24,2	42,3	[Ok]
23,6	24,4	40,1	[Ok]
23,6	24,3	40,8	[Ok]
23,6	23,8	40,1	[Ok]
23,6	23,8	40,8	[Ok]
23,6	24,2	38,6	[Ok]
23,6	24,1	39,3	[Ok]
23,6	24,9	38,6	[Ok]
23,6	24,7	39,3	[Ok]
23,6	23,9	40,1	[Ok]
23,6	23,9	40,8	[Ok]
23,6	23,6	40,1	[Ok]
23,6	23,5	40,8	[Ok]
23,6	23,8	40,1	[Ok]
23,6	23,7	40,8	[Ok]
23,6	23,3	40,1	[Ok]
23,6	23,3	40,8	[Ok]
23,6	23,8	38,6	[Ok]
23,6	23,8	39,3	[Ok]
23,7	23,3	38,6	[Ok]

23,7	23,3	39,3	[Ok]
23,7	23,5	38,6	[Ok]
23,7	23,5	39,3	[Ok]
23,7	24,9	38,6	[Ok]
23,7	24,8	39,3	[Ok]
23,7	23,7	38,6	[Ok]
23,7	23,7	39,3	[Ok]
23,7	23,3	38,6	[Ok]
23,7	23,3	39,3	[Ok]
23,7	22,9	39,3	[Ok]
23,7	22,9	39,3	[Ok]
23,7	22,5	40,1	[Ok]
23,7	22,6	40,8	[Ok]
23,7	22,8	40,1	[Ok]
23,7	22,8	40,8	[Ok]
23,7	23,3	38,6	[Ok]
23,7	23,3	39,3	[Ok]
23,7	22,9	40,1	[Ok]
23,7	22,9	40,8	[Ok]
23,7	23,2	40,1	[Ok]
23,7	23,2	40,8	[Ok]
23,7	22,8	41,5	[Ok]
23,7	22,8	42,3	[Ok]
23,7	23,6	40,1	[Ok]
23,7	23,5	40,1	[Ok]
23,7	23,3	38,6	[Ok]
23,7	23,3	39,3	[Ok]
23,8	23,6	38,6	[Ok]
23,8	23,5	39,3	[Ok]
23,8	23,2	38,6	[Ok]
23,8	23,2	39,3	[Ok]
23,8	23,0	38,6	[Ok]
23,8	23,0	39,3	[Ok]
23,8	23,3	38,6	[Ok]
23,8	23,3	39,3	[Ok]
23,8	26,3	38,6	[Ok]
23,8	26,1	39,3	[Ok]
23,8	25,9	40,1	[Ok]
23,8	25,8	40,8	[Ok]
23,8	25,2	38,6	[Ok]
23,8	25,0	39,3	[Ok]
23,8	23,9	40,1	[Ok]
23,8	23,8	40,8	[Ok]

23,8	24,1	40,1	[Ok]
23,8	23,9	40,8	[Ok]
23,9	24,0	38,6	[Ok]
23,9	23,9	39,3	[Ok]
23,9	23,5	40,1	[Ok]
23,9	23,4	40,8	[Ok]
23,9	23,6	40,1	[Ok]
23,9	23,6	40,8	[Ok]
23,9	23,8	40,1	[Ok]
23,9	23,7	40,8	[Ok]
23,9	23,9	40,1	[Ok]
23,9	23,9	40,8	[Ok]
23,9	23,5	40,1	[Ok]
23,9	23,5	40,8	[Ok]
23,9	23,7	40,1	[Ok]
23,9	23,7	40,8	[Ok]
23,9	23,2	40,1	[Ok]
23,9	23,2	40,8	[Ok]
24,0	24,7	38,6	[Ok]
24,0	24,6	39,3	[Ok]
24,0	23,5	38,6	[Ok]
24,0	23,5	39,3	[Ok]
24,0	23,7	38,6	[Ok]
24,1	23,7	39,3	[Ok]
24,1	25,8	37,1	[Ok]
24,1	25,6	37,8	[Ok]
24,1	24,8	38,6	[Ok]
24,1	24,7	39,3	[Ok]
24,1	24,5	38,6	[Ok]
24,1	24,5	39,3	[Ok]
24,1	23,2	40,1	[Ok]
24,2	23,2	40,8	[Ok]
24,2	23,4	40,1	[Ok]
24,2	23,4	40,8	[Ok]
24,2	23,6	40,1	[Ok]
24,2	23,6	40,8	[Ok]
24,2	23,8	40,1	[Ok]
24,2	23,7	40,8	[Ok]
24,2	23,4	40,1	[Ok]
24,2	23,3	40,8	[Ok]
24,2	23,6	40,1	[Ok]
24,2	23,6	40,8	[Ok]
24,3	23,2	40,1	[Ok]

24,3	23,2	40,8	[Ok]
24,3	23,6	41,5	[Ok]
24,3	23,6	42,3	[Ok]
24,3	23,6	40,1	[Ok]
24,3	23,6	40,8	[Ok]
24,4	23,7	38,6	[Ok]
24,4	23,6	39,3	[Ok]
24,4	23,2	38,6	[Ok]
24,4	23,2	39,3	[Ok]
24,4	23,6	38,6	[Ok]
24,5	23,6	39,3	[Ok]
24,5	23,9	38,6	[Ok]
24,5	23,7	39,3	[Ok]
24,5	26,3	37,1	[Ok]
24,5	26,1	37,8	[Ok]
24,5	25,9	38,6	[Ok]
24,5	25,7	39,3	[Ok]
24,5	25,0	40,1	[Ok]
24,5	24,9	40,8	[Ok]
24,5	24,5	40,1	[Ok]
24,6	24,4	40,8	[Ok]
24,6	24,5	40,1	[Ok]
24,6	24,5	40,8	[Ok]
24,6	24,0	40,1	[Ok]
24,6	23,9	40,8	[Ok]
24,6	24,2	40,1	[Ok]
24,6	24,1	40,8	[Ok]
24,6	24,2	40,1	[Ok]
24,7	24,1	40,8	[Ok]
24,7	23,7	40,1	[Ok]
24,7	23,6	40,8	[Ok]
24,7	23,8	40,1	[Ok]
24,7	23,6	40,8	[Ok]
24,7	23,7	40,1	[Ok]
24,7	23,6	40,8	[Ok]
24,7	23,2	40,1	[Ok]
24,7	23,2	40,8	[Ok]
24,7	23,7	38,6	[Ok]
24,7	23,7	39,3	[Ok]
24,8	23,7	38,6	[Ok]
24,8	23,7	39,3	[Ok]
24,8	23,3	38,6	[Ok]
24,8	23,3	39,3	[Ok]

24,8	23,6	38,6	[Ok]
24,8	23,6	39,3	[Ok]
24,8	23,7	38,6	[Ok]
24,9	23,7	39,3	[Ok]
24,9	24,6	38,6	[Ok]
24,9	24,5	39,3	[Ok]
24,9	23,6	38,6	[Ok]
24,9	23,6	39,3	[Ok]
25,0	22,7	40,1	[Ok]
25,0	22,7	40,8	[Ok]
25,1	23,1	40,1	[Ok]
25,1	23,1	40,8	[Ok]
25,2	22,7	40,1	[Ok]
25,2	22,8	40,8	[Ok]
25,2	24,5	38,6	[Ok]
25,2	24,4	39,3	[Ok]
25,3	23,1	40,1	[Ok]
25,3	23,1	40,8	[Ok]
25,3	22,7	40,1	[Ok]
25,3	22,8	40,8	[Ok]
25,3	23,1	40,1	[Ok]
25,4	23,1	40,8	[Ok]
25,4	23,3	41,5	[Ok]
25,4	23,3	42,3	[Ok]
25,4	23,0	40,1	[Ok]
25,4	23,0	40,8	[Ok]
25,5	23,4	38,6	[Ok]
25,6	23,4	39,3	[Ok]
25,6	22,9	40,1	[Ok]
25,7	22,9	40,8	[Ok]
25,8	23,6	38,6	[Ok]
25,8	23,6	39,3	[Ok]
25,8	23,3	38,6	[Ok]
25,8	23,3	39,3	[Ok]
25,9	23,5	38,6	[Ok]
25,9	23,5	39,3	[Ok]
25,9	23,4	38,6	[Ok]
26,0	23,4	39,3	[Ok]
26,1	23,6	38,6	[Ok]
26,1	23,6	39,3	[Ok]
26,2	22,5	40,1	[Ok]
26,3	22,5	40,8	[Ok]
26,3	22,9	38,6	[Ok]

26,6	22,9	39,3	[Ok]
26,9	23,3	40,1	[Ok]
27,1	23,2	40,8	[Ok]
27,4	25,8	37,1	[Ok]

ANEXO 5

Captura de Tráfico

Para encapsular los datos en la pila de TCP/IP se sigue la siguiente estructura:

Paquetes de datos VoIP

RTP

UDP

IP

Capas I,II

Los paquetes de VoIP se encuentran en el protocolo RTP el cual está dentro de los paquetes UDP-IP.

1) VoIP no usa el protocolo de TCP porque es demasiado pesado para las aplicaciones de tiempo real así es que para eso usa el datagrama de UDP.

2) El datagrama de UDP no tiene el control sobre la orden de la cual los paquetes son recibidos o de cuánto tiempo toma para llegar ahí. Cualquiera de estos dos puntos son bastante importantes para la calidad (que tan clara se escucha la voz de la otra persona) y la calidad de la conversación (que tan fácil es llevar una conversación), por lo que RTP resuelve este problema permitiendo que el receptor ponga los paquetes en el orden correcto y que no se tarde con los paquetes que hayan perdido el camino o se tarden mucho en ser recibidos.

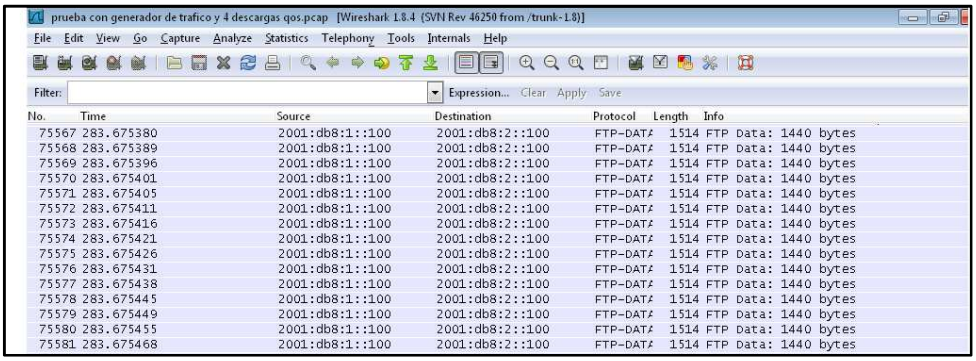
Para la ilustración de la captura de tráfico en una llamada, se escogió al azar una llamada y se ha priorizado una que contiene QoS, aunque el procedimiento bien puede aplicarse a cualquiera de los escenarios planteados, aquí se explica cómo se obtienen los datos con los que obtendremos la información que necesita ser procesada con el fin de comprobar la hipótesis planteada.

Primero se establece la llamada entre dos softphones con el software Jitsi:

Origen	Destino
2001:db8:2::100	2001:db8:1::100

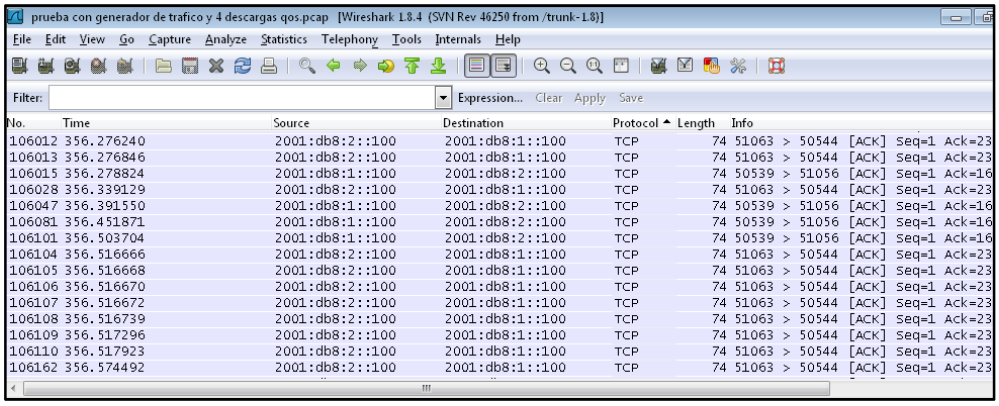
Luego se inunda la red con tráfico IP, FTP ***(Anexo 6)***

El sniffer Wireshark nos presenta la siguiente información:



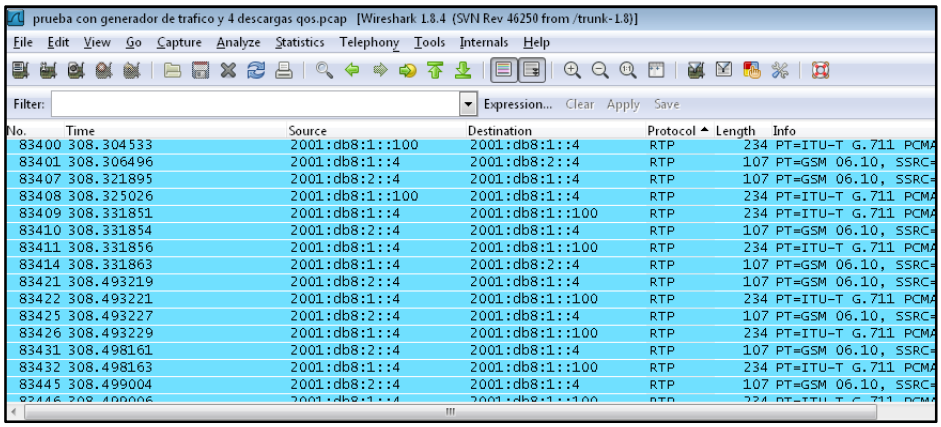
Ejemplo de captura de tráfico Ftp

Podemos observar el tráfico que se ha generado y que se ha capturado con Wireshark



Tráfico TCP generado

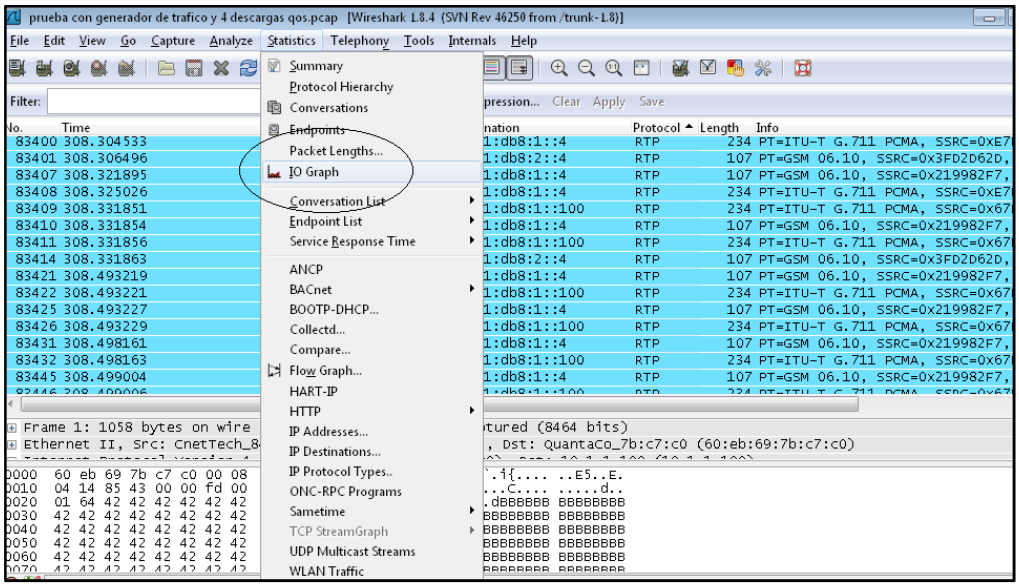
En la siguiente figura notamos el tráfico RTP que se ha generado



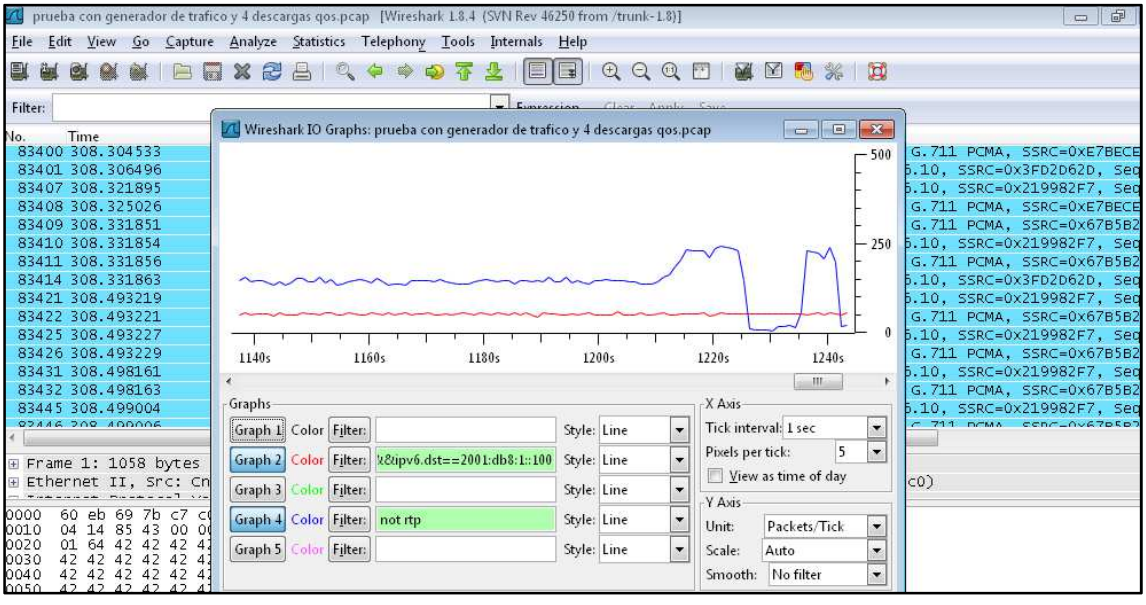
Tráfico RTP

Es importante señalar que la Ip de origen no se observa, esto sucede que al estar en otro extremo de la red, el sniffer únicamente observa el servidor SIP, troncalizado “2001:db8:2::4”, que lo toma como generador del tráfico RTP.

Procedemos ahora a realizar el análisis del comportamiento del tráfico generado en nuestra red.



Una de las fortalezas de Wireshark, es su gran versatilidad para obtener el tipo de información que necesitamos de un segmento de red, así podemos observar gráficamente el comportamiento de la red en diferentes circunstancias.



Análisis de tráfico aplicando QoS

Al aplicar filtrados de tráfico, podemos apreciar al tráfico RTP de color Rojo, el mismo que no decae al momento de saturar la red, el tráfico que no es RTP, lo podemos ver en color azul (es todo el tráfico restante).

Los comandos que se utilizaron para este análisis son:

Filter:

- RTP && pv6.dst = = 2001:db8:1::100

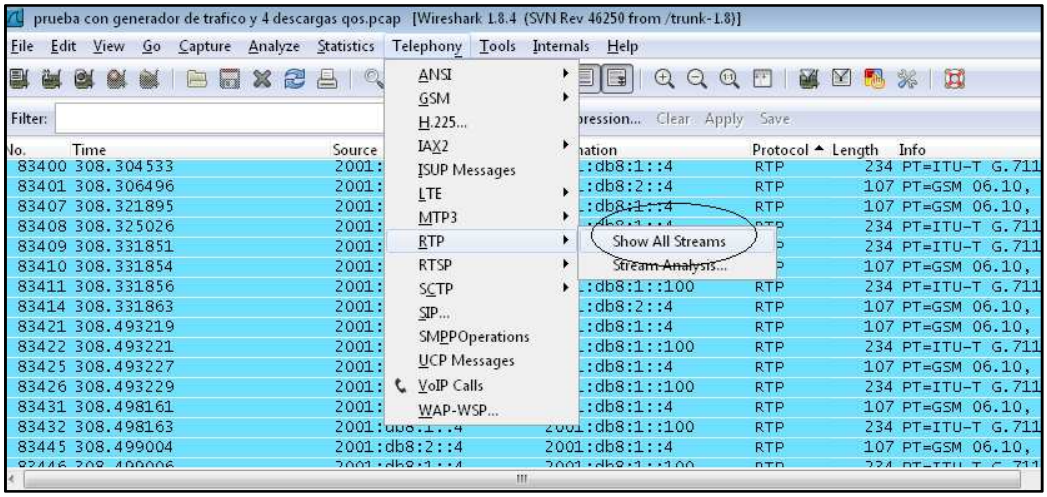
Esto quiere decir que deseamos generar un gráfico que muestre el tráfico RTP generado hacia la ip 2001:db8:1::100 con una línea de color rojo.

- NOT RTP

Para observar el resto de tráfico mostrado con la línea de color azul, en este caso inferimos que se ha aplicado QoS, por lo que llamada se ha mantenido y no ha decaído.

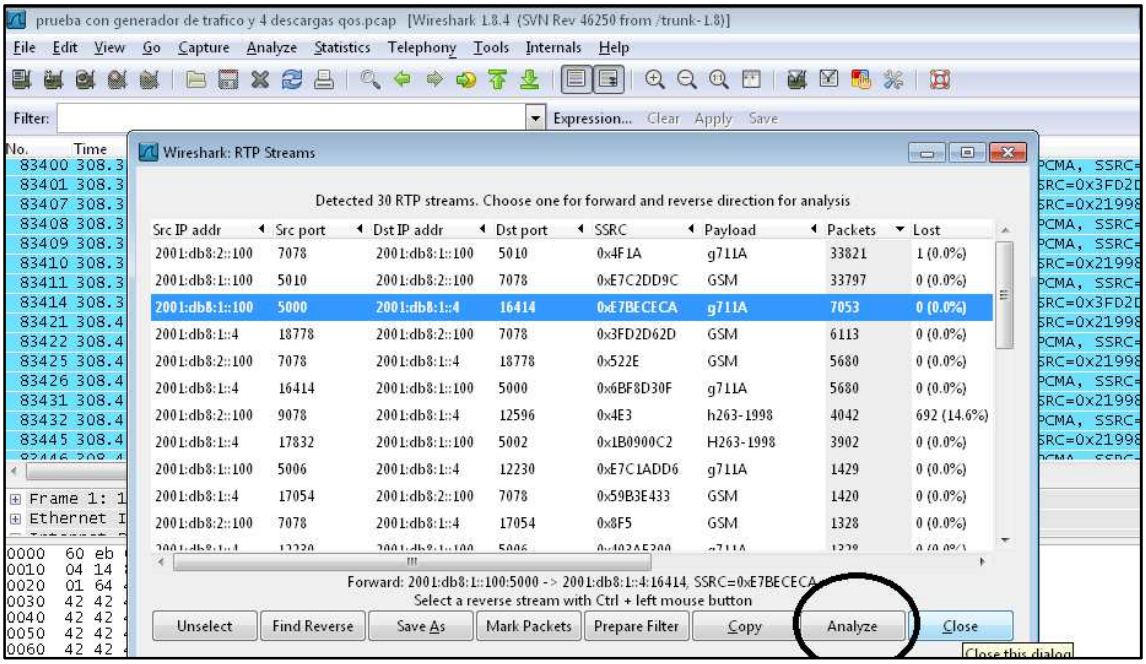
Luego procedemos a obtener los RTP Streams, que son las estadísticas de las cuales obtendremos la información respecto a las variables independientes de nuestra investigación.

Como podemos apreciar en la siguiente figura, escogemos la opción Telephony- RTP-Show All Streams.

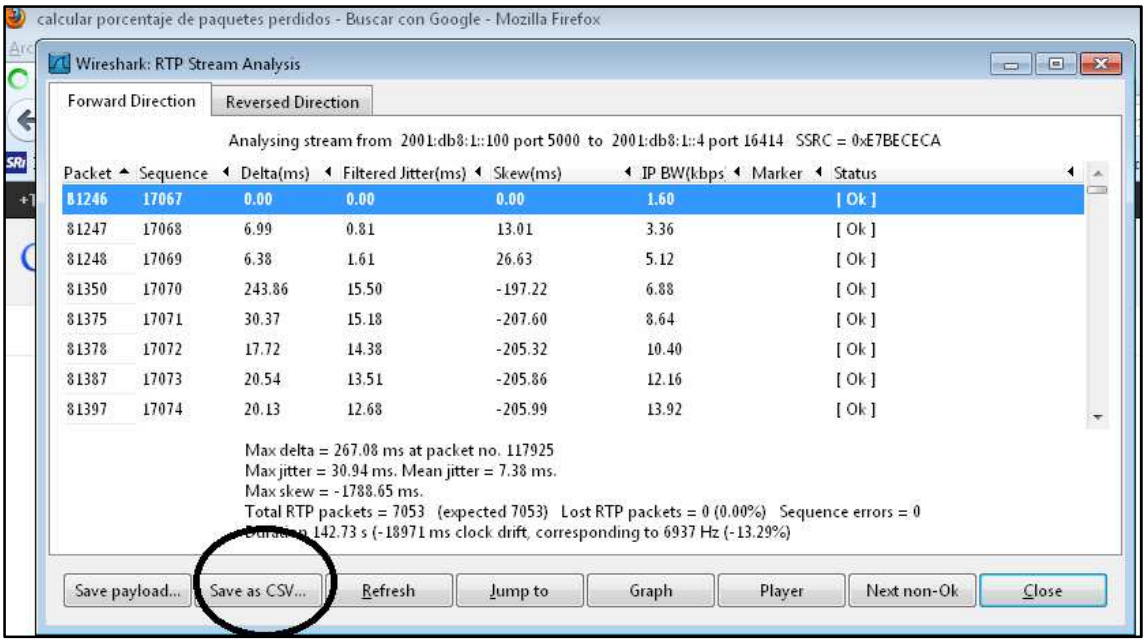


Obtención de los streams

Luego se presenta un listado con más detallado con todo el tráfico RTP y los parámetros que se necesitan para establecer una buena comunicación:



Una vez que seleccionamos el stream deseado, teniendo en cuenta las Ips origen y destino, procedemos a dar click en el botón *Analize*. Lo que nos indica la siguiente figura:



Aquí se detallan los campos que nos van a servir para el presente proyecto, los cuales son:

Los datos recibidos corresponden al resumen obtenido con el sniffer, tomando en cuenta los siguientes campos:

TOTAL RTP packets (Total de paquetes RTP que envía la máquina Origen)= *n*

Expected *n (Total de paquetes RTP que espera la máquina destino)*

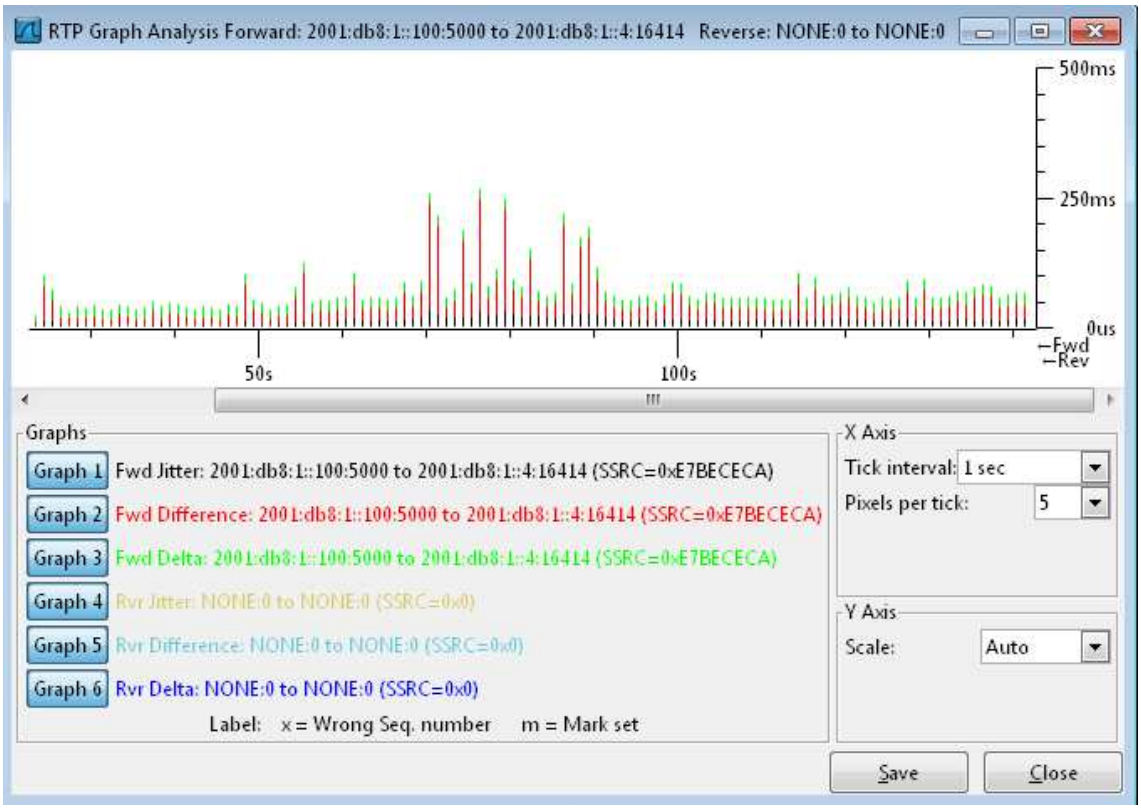
Lost RTP packets = *n* (Total de paquetes RTP perdidos)

Donde *n* corresponde al número de paquetes.

La diferencia entre "*Expected n" de "TOTAL RTP packets*", nos señala el valor "*Lost RTP packets*"

Los datos del *ancho de banda (IP BW), Latencia (Delta) y jitter (Filtered Jitter)*, son un promedio del total de datos recibidos, los cuales se los puede observar generando un archivo CSV como lo indica la figura, la tabla generada se puede observar en el ***Anexo 4.***

También podemos generar un reporta gráfico del Jitter y Latencia así:



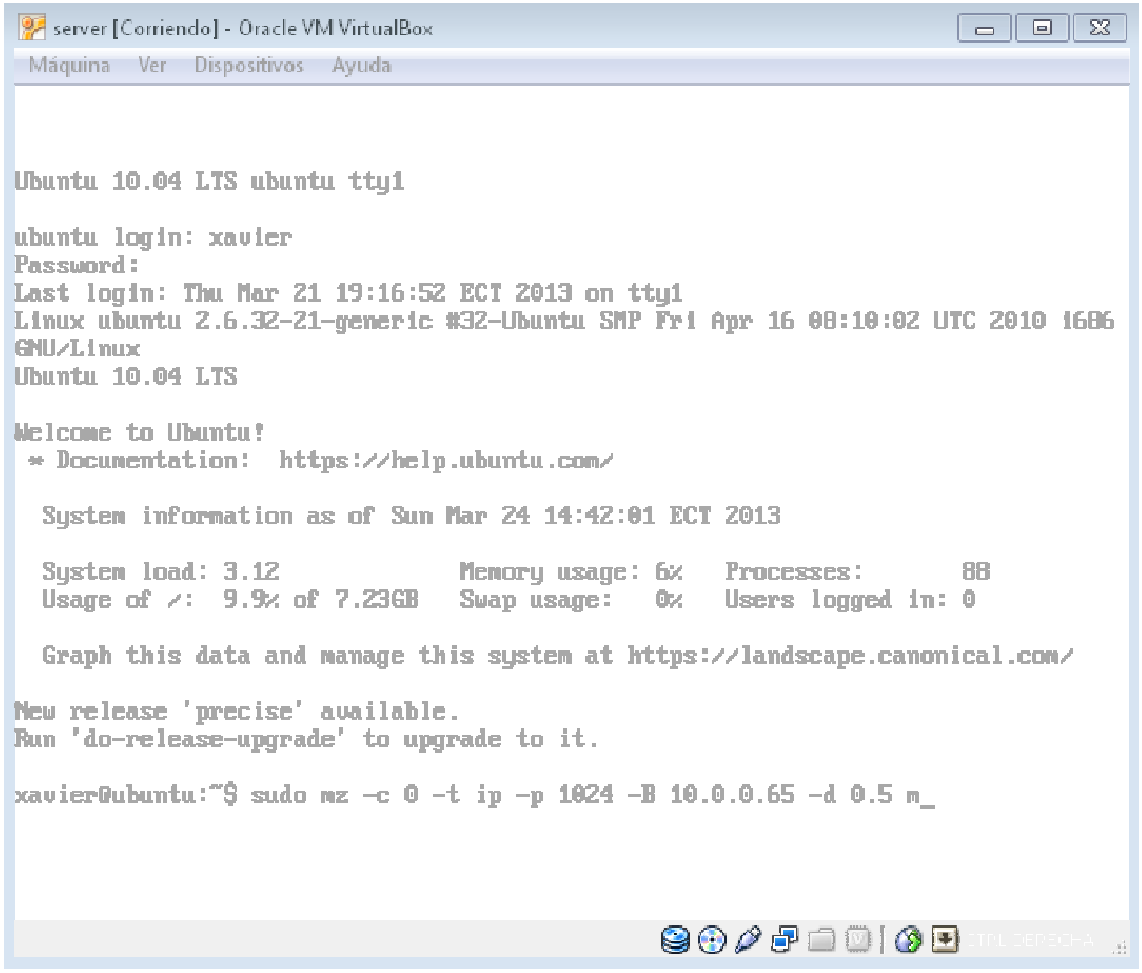
Esto nos da una idea general de cómo está transmitiéndose la llamada.

ANEXO 6

Para la generación de tráfico, utilizamos máquinas virtuales que corresponden a las Pc3 y Pc5 de las Tabla 2 y Tabla 3. Las mismas que contienen la distribución Ubuntu Server, con el software *mausezahn* previamente instalado, desde donde ejecutamos el siguiente comando:

sudo mz –c 0 –t ip –p 1024 –B ip destino –d 0.5m

sudo mz –c 0 –t IPv6 –p 1024 –B ip destino –d 0.5m



-c (Envía los tiempos de conteo de paquetes: 1 default, 0 infinite)

-t (Creador del paquete)

Ip - IPv6 (Versión del protocolo)

-p (enviar paquetes de una longitud específica)

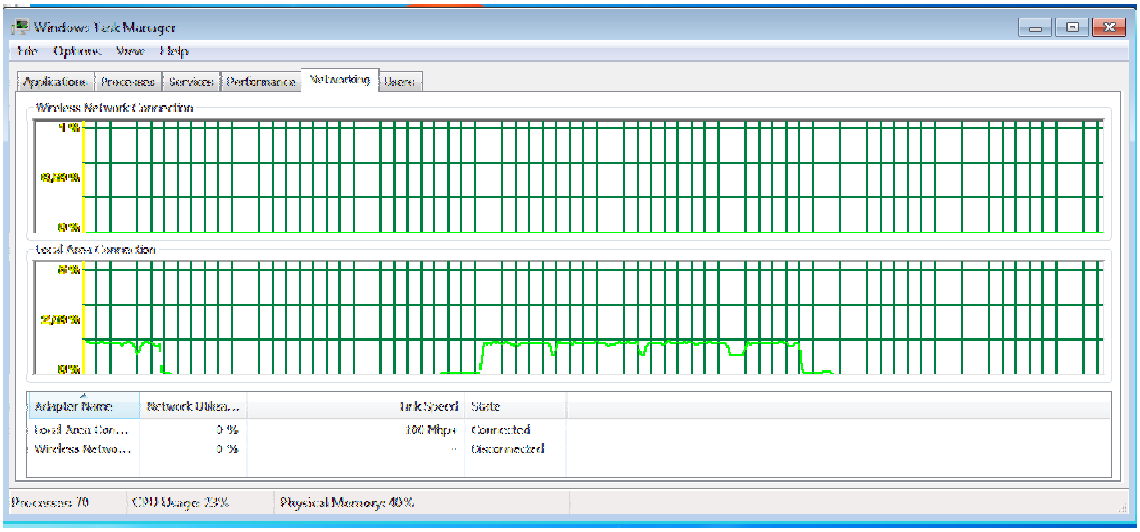
-B (Usar una dirección ip específica)

-d (Retardo entre las transmisiones)

El objetivo es el de inundar la red con tráfico IP y de esa manera probar el QoS Aplicado.

Los datos obtenidos del tráfico generado lo tenemos en la tabla siguiente:

CAPACIDAD TOTAL DE LOS INTERFACES	PORCENTAJE DE LA NIC UTILIZADO
10 MB	12 %
100 MB	1,2 %

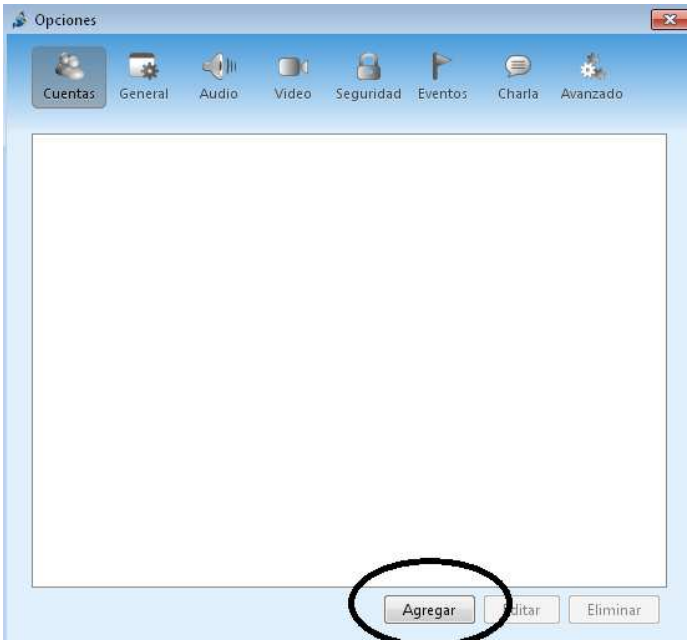


Prueba de tráfico obtenida con administrador de tareas de Windows 7en la máquina Pc1 del esquema general

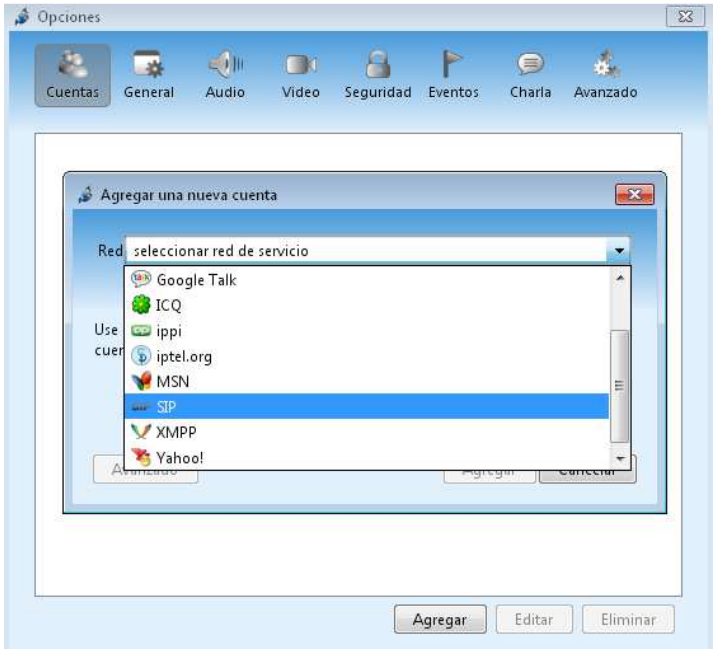
ANEXO 7

Configuración de Softphone Jitsi

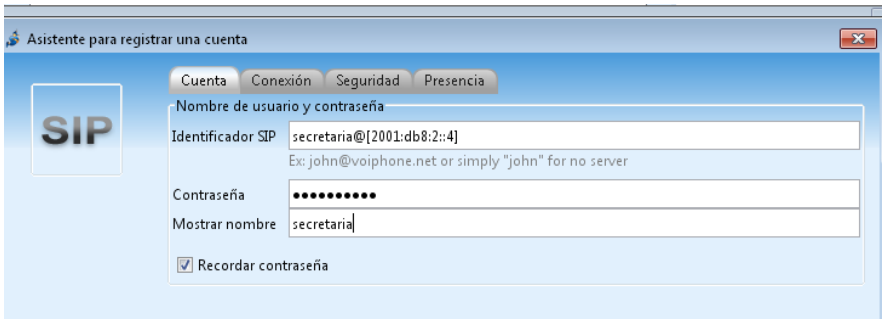
El primer paso consiste en crear una cuenta, previamente configurada en Asterisk



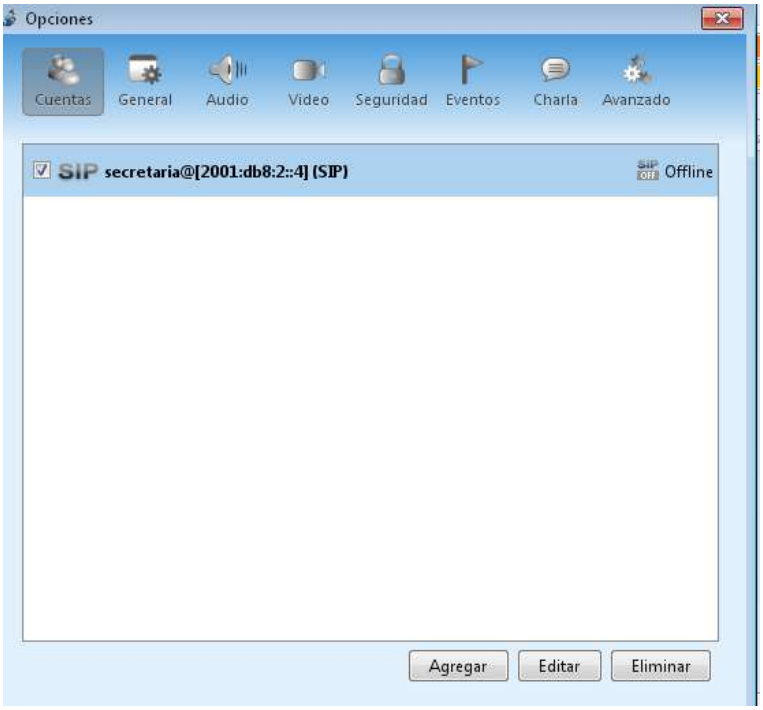
El protocolo de señalización SIP, se configura como se aprecia en la siguiente figura:



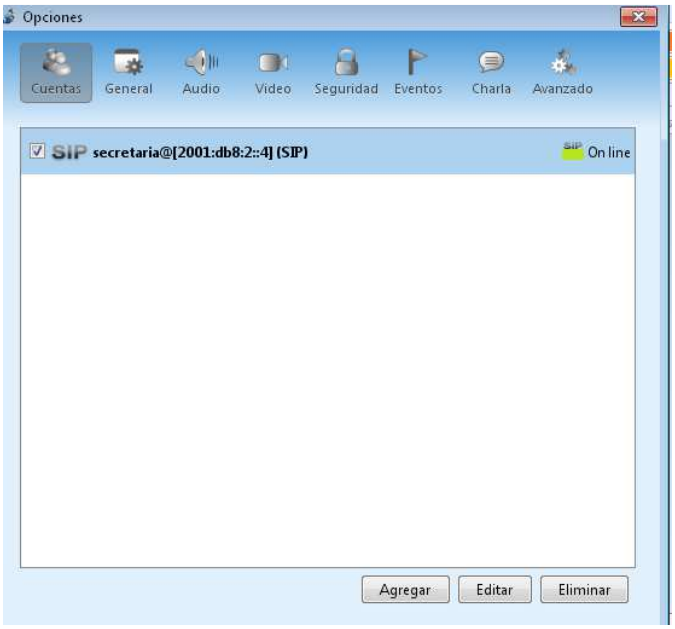
Los datos que introducimos a continuación son: el identificador SIP, que es la extensión creada en la centralita con su respectiva clave.



Si la información no se ingresa correctamente, no se registrará en Asterisk, como podemos apreciarlo en la siguiente figura:



Si todo se ha configurado correctamente se obtiene:



Y el softphone está listo para enviar y recibir llamadas. En el caso de la siguiente figura, se muestra un ejemplo de la creación de la cuenta “Secretaria”