ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

"ANÁLISIS COMPARATIVO DEL PROTOCOLO BGP EN IPV4 E IPV6 PARA LA TRANSMISIÓN DE SERVICIOS WEB DENTRO DE UN ESCENARIO BÁSICO"

GABRIEL FERNANDO LASCANO TACURI

Trabajo de Titulación modalidad Proyectos de Investigación y Desarrollo, presentado ante el Instituto de Postgrado y Educación Continua de la ESPOCH, como requisito parcial para la obtención del grado de Magíster en Interconectividad de Redes

Riobamba – Ecuador

Junio 2016

ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

CERTIFICACIÓN

EL TRIBUNAL DE TRABAJO DE TITULACIÓN CERTIFICA QUE:

El Trabajo de Titulación modalidad Proyectos de Investigación y Desarrollo, titulado: **"ANÁLISIS COMPARATIVO DEL PROTOCOLO BGP EN IPV4 E IPV6 PARA LA TRANSMISIÓN DE SERVICIOS WEB DENTRO DE UN ESCENARIO BÁSICO"**, de responsabilidad del Ing. Gabriel Fernando Lascano Tacuri ha sido prolijamente revisado y se autoriza su presentación.

Tribual de Tesis:

Dr. Galo Patricio Noboa Viñan, Phd
PRESIDENTE _____

Ing. Jorge Ernesto Huilca Palacios, Mgs
TUTOR _____

Ing. Diego Marcelo Reina Haro, Mgs
MIEMBRO _____

Ing. Mentor Javier Sánchez Guerrero, Mgs
MIEMBRO _____

_____
DOCUMENTALISTA SISBIB ESPOCH _____

Riobamba, Junio 2016.

DERECHOS INTELECTUALES

Yo, Gabriel Fernando Lascano Tacuri, soy responsable de las ideas, doctrinas y resultados expuestos en esta Tesis; y el patrimonio intelectual de la Tesis de Grado pertenece a la ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO.

_____

C.I. 1803686482

DECLARACIÓN DE AUTENTICIDAD

Yo, Gabriel Fernando Lascano Tacuri, declaro que el presente Proyecto de Investigación, es de mi autoría y que los resultados del mismo son auténticos y originales. Los textos constantes en el documento que provienen de otra fuente están debidamente citados y referenciados.

Como autor, asumo la responsabilidad legal y académica de los contenidos de este proyecto de investigación de maestría.

Riobamba, 13 de junio de 2016

_____

Gabriel Fernando Lascano Tacuri

C.I. 1803686482

DEDICATORIA

Deseo dedicar la presente investigación a DIOS y a mi VIRGEN DEL CISNE por sus infinitas bendiciones, a mis PADRES y a mi HIJO que son la fuerza que me motiva a levantarme cada día, a toda mi familia por su apoyo constante; y, a los miembros del tribunal por brindarme la confianza y respaldo necesarios no solo como docentes, sino como amigos.

Han sido meses difíciles en los cuales muchas personas señalaron que no podría lograrlo; a ellos de manera especial, les dedico los resultados alcanzados.

Gabriel

AGRADECIMIENTO

Luego de todas las experiencias transcurridas en el desarrollo de esta investigación; y, una vez finalizada la misma, solo me queda dar gracias a DIOS y a mi VIRGEN DEL CISNE por darme vida y su bendición para llegar hasta aquí, a mis PADRES por haber sido el apoyo incondicional todos estos años, a mi HIJO por convertirse en el impulso que me ha llevado a alcanzar metas que creía distantes, a toda mi familia que de una u otra forma se han hecho presentes, a mis amigos miembros del tribunal a quienes expreso mi gratitud infinita y a la Escuela Superior Politécnica de Chimborazo noble institución académica de excelencia que me ha permitido alcanzar una nueva meta profesional.

Gabriel.

ÍNDICE DE ABREVIATURAS

BGP	Boarder Gateway Protocol
IPV4	Internet Protocol Version 4
IPV6	Internet Protocol Version 6
WEB	World Wide Web o Red mundial de información - INERTNET
FTP	File Transfer Protocol
RTP	Real Time Protocol
EGP	External Gateway Protocol
MP-BGP	Multiprotocol Boarder Gateway Protocol
RFC	Request For Comments
iBGP	Internal Boarder Gateway Protocol
TCP	Trasmission Control Protocol
ICANN	Internet Corporation for Assigned Names and Numbers
IETF	Internet Engineering Task Force
ISP	Internet Service Provider
DHCP	Dynamic Host Configuration Protocol
QoS	Quality of Service
VoIP	Voice over Internet Protocol
WALC	Workshop para América Latina y el Caribe
WAN	Wide Area Network
HTTP	Hypertext Transfer Protocol
RIR	Regional Internet Registry
EUI-64	Extended Unique Identifier 64 bits
ID	Identity - Identificador
ULA	Unique Local Address
IEEE	Institute of Electrical and Electronics Engineers
PPP	Point to Point Protocol
ATM	Asynchronous Transfer Mode
ToS	Type of Sevicie
CoS	Class of Service
VLSM	Variable Length Subnet Mask
RIP	Routing Information Protocol
IGRP	Interior Gateway Routing Protocol
CIDR	Classless Inter-Domain Routing
NAT	Network Address Translation

AS / SA	Autonomous System / Sistema Autónomo
RIPE	Réseaux IP Européens
ARIN	American Registry for Internet Numbers
APNIC	Asia Pacific Network Information Centre
PoP	Point of Presence
IANA	Internet Assigned Numbers Authority
ASN	Autonomous System Number
RIP	Routing Information Protocol
OSPF	Open Shortest Path First
RR	Route Reflector
DTP	Data Transfer Protocol
PI	Protocol Interpreter
UDP	User Datagram Protocolo
SSRC	Synchronization Source
CSRC	Content Source
RIPNG	Routing Information Protocol Next Generation
GPL	General Public License
ITU	International Telecommunication Union

ÍNDICE DE TABLAS

ÍNDICE DE GRÁFICOS

ÍNDICE DE FIGURAS

ÍNDICE

RESUMEN

La presente investigación tuvo como objetivo analizar comparativamente el comportamiento del protocolo BGP aplicado sobre los protocolos de Internet IPV4 e IPV6 para determinar que versión muestra un mejor desempeño en la trasmisión de servicios Web FTP y RTP. El protocolo BGP sobre IPV4 e IPV6 ha sido configurado en el mismo ambiente de pruebas, esto ha permitido implementar un escenario DUALSTACK, de esta manera se ha podido realizar las mediciones en las transmisiones de los protocolos FTP y RTP en las mismas condiciones de red, empleando cuatro PCs de escritorio configurados como routers BGP en tres distintos Sistemas Autónomos con un canal de datos limitado, todo esto gracias a recursos de hardware libre; y, de igual forma aplicativos de software libre para poder realizar la generación de tráfico y análisis de los paquetes generados desde cuatro computadores empleados como Hosts de red, recreando de esta manera las condiciones existentes en una red de producción real. Los resultados alcanzados indican que la implementación de BGP sobre IPV6 presenta leves mejoras en relación a su aplicación sobre IPV4, a pesar de no haber utilizado mecanismos que aseguren la calidad de los servicios. Se concluye que BGP mejora la transmisión de información de los protocolos FTP y RTP priorizando la comunicación de los routers dentro y fuera de un sistema autónomo; no obstante, se recomienda seleccionar de manera correcta el escenario y tráfico a ser analizado, debido a la naturaleza distinta cuando se trata de servicios Web.

Palabras claves: <TECNOLOGIA Y CIENCIAS DE LA INGENIERIA>, <INTERCONECTIVIDAD DE REDES>, <PROTOCOLOS DE RED>, <PROTOCOLO DE INTERNET IPV4>, <PROTOCOLO DE INTERNET IPV6>, <FILE TRANSFER PROTOCOL (FTP)>, <REAL TIME PROTOCOL (RTP)>, <BOARDER GATEWAY PROTOCOL (BGP)>

SUMMARY

This research was carried out to comparatively analyze the behavior of BGP protocol implemented on Internet protocols IPV4 and IPV6, to determine which version shows a better performance in the transmission of FTP and RTP Web services. The BGP protocol over IPV4 and IPV6 has been set to the same test environment, this has allowed to implement a DUALSTACK scenario, so it has been possible to perform measurements on transmissions of FTP and RTP protocols on the same network conditions, using four desktop PCs configured as BGP routers in three different Autonomous Systems with limited data channel, all thanks to free hardware resources; and, just as free software applications to perform traffic generation and analysis of packets generated from four computers used as network hosts, thus recreating the conditions in an actual production network. The results obtained indicate that the implementation of BGP on IPV6 presents relation slight improvements in its application on IPV4, dispite not having used mechanism to ensure the quality of services. BGP is concluded that improves the information transmission of protocols FTP and RTP giving priority to communication between routers inside and outside an autonomous system; however, it is recommended to correctly select the scenario and traffic to be analyzed, because of the different nature when it comes to Web services.

Key words: <TECHNOLOGY AND SCIENCE ENGINEERING>, <NETWORKS INTERCONNECTIVITY>, <NETWORK PROTOCOLS>, <INTERNET PROTOCOL IPV4>, <INTERNET PROTOCOL IPV6>, <FILE TRANSFER PROTOCOL (FTP)>, <REAL TIME PROTOCOL (RTP)>, <BOARDER GATEWAY PROTOCOL (BGP)>

CAPÍTULO I

1. INTRODUCCIÓN

1.1 Antecedentes

Los protocolos de ruteo externo son los que se utilizan para interconectar Sistemas Autónomos. En los protocolos de ruteo externo la prioridad radica en buscar rutas óptimas atendiendo únicamente al criterio de minimizar la 'distancia' medida en términos de la métrica elegida para la red.

Hasta 1990 se utilizaba como protocolo de ruteo externo en la Internet el denominado EGP o Exterior Gateway Protocol en inglés. Este protocolo no fue capaz de soportar el crecimiento de la Red y entonces se desarrollo un nuevo protocolo de ruteo externo denominado BGP. Desde entonces se ha producido 4 versiones de BGP, las especificaciones para el protocolo BGP-4 se encuentran en el RFC 1771 (Vanaclocha, s.f., p.2, www.uv.es), que fue socializado en 1995 y actualizada en RFC 4271 en el 2006; no obstante, en este se encuentra contempladas todos los particulares para su funcionamiento en los protocolos IPV4 e IPV6.

Algo de magia es requerida para permitir que un protocolo de ruteo de 21 años, transporte información de ruteo para un protocolo de red de 19 años, misma que debería ser conocida como las Extensiones Multiprotocolo. Esto convierte al BGP-4 regular en BGP Multiprotocolo en inglés Multiprotocol BGP o sus siglas MP-BGP, sin embargo este término es raramente utilizado estos días. Las Extensiones Multiprotocolo, publicadas originalmente como el RFC 2283 en 1998, utilizan algunas codificaciones inteligentes para permitir que BGP-4 transporte un amplio rango de familias de direcciones (Noction Network Intelligence, 2015, http://www.noction.com).

BGP es usado principalmente para conectar dominios de ruteo separados que contienen políticas de ruteo independientes; cada dominio es denominado sistema autónomo, por lo que es ampliamente utilizado para conexiones a proveedores de servicios de INTERNET. El BGP se puede utilizar también dentro de un sistema autónomo, y esta variación es conocida como Internal BGP o iBGP. Multiprotocol BGP es un BGP mejorado que transporta información de enrutamiento para diversas familias de direcciones del protocolo de capa de red, como la familia de direcciones de IPv6 y para rutas de IP Multicast (CISCO, 2014, p.1, http://www.cisco.com).

BGP es un protocolo de transporte fiable. Esto elimina la necesidad de llevar a cabo la fragmentación de actualización explícita, la retransmisión, el reconocimiento, y secuenciación (Vanaclocha, s.f., p.2, www.uv.es).

Resulta indispensable indagar el comportamiento de BGP-4 y las características que ofrece para la interconexión de varios sistemas autónomos mediante el protocolo de red IPV4 e IPV6, se genera así la interrogante: ¿La implementación del protocolo BGP sobre ipv6 podrá mejorar la transmisión de servicios web con respecto al protocolo BGP sobre ipv4, en un escenario básico?

Así se podrán identificar diferencias, ventajas y/o desventajas, que establezcan si se puede mejorar el desempeño de una red en la trasmisión de servicios existentes en INTERNET, sin características que aseguren la calidad de los servicios.

1.2 Justificación

Una de las remarcables cualidades que posee la INTERNET, es su notable escalabilidad hasta llegar a su tamaño actual. No es sorprendente que todo haya cambiado desde los orígenes tempranos de INTERNET con la ARPANET en 1969, sin embargo los actuales protocolos TCP e IP no surgieron sino hasta los últimos años de la década de 1970. Desde ese entonces TCP/IP se ha convertido se ha convertido en el protocolo de red predominante para casi todo tipo de comunicación digital (Beijnum, 2011, p.1).

El protocolo de red original, fue estructurado para un máximo de 4.3 billones de identificadores de terminales o direcciones de red. Este límite fue incrementándose utilizando un mecanismo llamado Traducción de direcciones de red, que permite a varios dominios usar espacios de direcciones privadas que no son publicadas en el INTERNET público valga la redundancia, pero pueden ser traducidas en una dirección IPV4 compartida, pública y enrutable. El espacio de direcciones IPV4 finalmente se agotó en la Corporación de Internet para la Asignación de Nombres y Números o por sus siglas en inglés ICANN; en febrero del 2011, dejando a los registros regionales de INTERNET lidiar con la asignación de sus espacios de red restantes.
IPV6 fue desarrollado a mediados de la década de 1990 y estandarizado por el Grupo de Trabajo de ingeniería de INTERNET por sus siglas en inglés IETF, para proveer 340 billones de billones de billones de direcciones. Su implementación ha sido lenta, pero existen necesidades que han hecho indispensable su utilización: el agotamiento de direcciones IPV4, la demanda constante de direcciones de INTERNET para asignarlas a dispositivos móviles, equipos de red, vehículos y literalmente a decenas de billones de otros dispositivos programables. Esta es la llamada INTERNTE de las cosas (Hagen, 2014, p. xi). Todo esto sin mencionar mejoras como

seguridad, capacidad de transmisión de datos, velocidad, calidad entre otras, que ofrece para nuevas aplicaciones y novedosos servicios en las redes presentes y futuras.

De tal manera, resulta importante la investigación del comportamiento de los protocolos empleados en la interconexión a INTERNET, al ser BGP el protocolo de ruteo más difundido para este propósito, se estudiará su aplicación en IPV4 e IPV6, teniendo como fin determinar su funcionamiento y mejoras existentes en la trasmisión de los servicios web más utilizados, en redes de constante crecimiento y evolución.

Se presentan a continuación una descripción gráfica de los escenarios tentativos para analizar y obtener los resultados de la presente investigación:

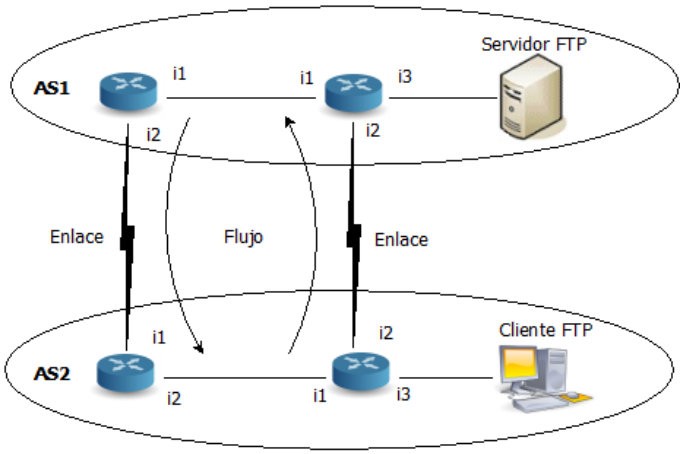


Gráfico 1-1. Escenario BGP Básico con un cliente y un servidor FTP
Realizado por: Gabriel Lascano, 2015

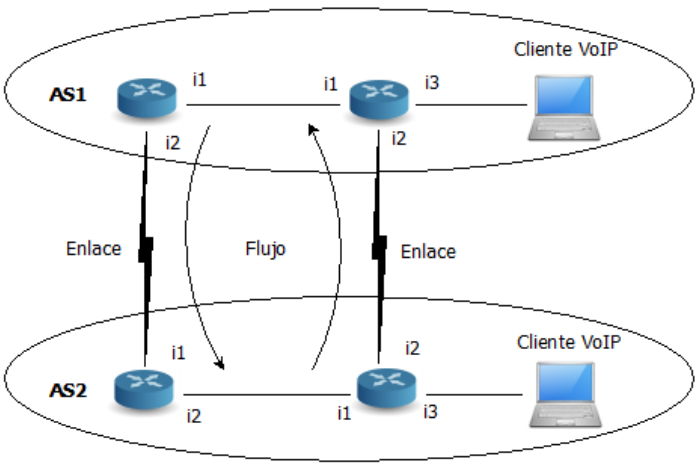


Gráfico 2-1. Escenario BGP Básico con dos dispositivos VoIP
Realizado por: Gabriel Lascano, 2015

Lo que se conseguirá es establecer el comportamiento del protocolo de ruteo BGP aplicado en IPV4 e IPV6, comparando las diferencias en servicios web como RTP y FTP, de tal manera mediante mediciones se establecerán las mejoras entre las dos versiones.

1.3 Objetivos

1.3.1 Objetivo general

Analizar comparativamente el protocolo BGP en IPV4 e IPV6 para la transmisión de servicios web dentro de un escenario básico.

1.3.2. Objetivos específicos

- Analizar el funcionamiento del protocolo BGP IPV4 e IPV6 para la conexión de una red entre sistemas autónomos parte fundamental del INTERNET.
- Comparar los protocolos BGP IPV4 y BGP IPV6 en la trasmisión de servicios FTP y RTP.
- Desarrollar un escenario básico de estudio que permita representar el tráfico de información en INTERNET mediante software libre y que permita la implementación de BGP en IPV4 e IPV6.

1.4 Hipótesis

La comparación del protocolo BGP en IPV4 e IPV6 permite definir que protocolo mejora la transmisión de servicios web en un escenario básico.

CAPÍTULO II

2. REVISIÓN DE LITERATURA

2.1 Transición de ipv4 a ipv6

El lenguaje común del Internet es conocido como Protocolo de Internet IP o Internet Protocol. Cuando un dispositivo, como una computadora o un smartphone, se conecta al Internet a través de un Proveedor de Servicios de Internet ISP en inglés Internet Service Provider, una dirección IP única es asignada a dicho dispositivo. Esta dirección IP permite al dispositivo ser únicamente identificado y subsecuentemente comunicado a Internet.

Cuando el Internet fue construido, los ingenieros asumieron que el protocolo de Internet IPv4, que abarca cerca de 4300 millones de direcciones, sería suficiente para durar por mucho tiempo. No obstante, dado que las direcciones fueron delegadas incrementalmente a usuarios finales, se hizo evidente que el direccionamiento IPv4 no sería capaz de manejar el inmenso crecimiento del Internet para siempre. Para el año 1990, se estimó que 536 millones de direcciones, de los cuales un octavo está disponible para IPv4, ya habían sido asignadas. En los años recientes, el uso de direcciones IPv4 ha aumentado a cerca de 4000 millones. Se espera que la mayoría de los registros regionales de direcciones IP terminen de asignar su espacio de direcciones IPv4 en el año 2011.

IPv6, el sucesor de IPv4, proveerá más de 4000 millones de veces más espacio de direcciones que IPv4. A diferencia de IPv4, en que las direcciones están formadas por 32 bits de información, IPv6 utiliza 128 bits, lo cual efectivamente incrementa el número de direcciones disponibles a aproximadamente 340 billones de billones de billones (3.4 x 10^38) de direcciones, comparadas a las aproximadamente 4300 millones (2^32) de IPv4. El inminente agotamiento de direcciones IPv4 pronto conducirá la migración a IPv6 a una escala global. IPv4 e IPv6 podrán coexistir durante una suave transición. Muchos de los sistemas operativos modernos como Windows 7, Mac OS X y Linux, ahora soportan IPv6. Los dispositivos móviles operados por sistemas operativos como iOS 4.1+, Windows Mobile y Android 2.2, también ya incluyen soporte para IPv6 (IPV6MX, s.f., http://www.ipv6.mx).

2.2 Transición gradual y esencial

Aunque la transición a IPv6 será imperceptible para muchos usuarios, los negocios tienen una causa de atención, especialmente si sus operaciones diarias dependen de Internet. Las redes que usan equipo sin soporte para IPv6, pueden experimentar complicaciones al comunicarse con otros dispositivos operando en IPv6. Por tanto, los administradores de redes deben asegurarse que sus redes actuales sean capaces de soportar IPv6 lo más pronto posible.

Afortunadamente, la transición a IPv6 no sucederá de la noche a la mañana. El proceso gradual a menudo requerirá del soporte de los dos protocolos simultáneamente en sus redes. Esto puede ser difícil, dado que IPv6 e IPv4 utilizan diferentes topologías y necesitan técnicas lógicas para su coexistencia durante la transición. Dos técnicas lógicas populares para la coexistencia son "dual stack" y "tunnelling".

Dual stack implica proveer implementaciones completas de las dos versiones del Protocolo de Internet en el mismo equipo IPv4 e IPv6; y, Tunnelling provee un medio para llevar paquetes IPv6 a través de infraestructuras de ruteo IPv4 no modificadas, pormenores contenidos en el RFC 4213.

Como se puede esperar, la implementación lado a lado de los dos protocolos es un camino seguro para garantizar compatibilidad. Dual stack corre IPv4 e IPv6 paralelamente, permitiendo a los usuarios introducir contenido IPv4 e IPv6 de manera simultánea. Dual stack no requiere mecanismos de tunnelling en redes internas. IPv4 e IPv6 pueden ser utilizados independientemente el uno del otro hasta que IPv4 deje de ser necesario.

Tunneling, algunas veces llamado encapsulación, es la técnica de poner paquetes IPv6 dentro de paquetes IPv4 para que puedan ser llevados a través de infraestructuras IPv4. Simplemente, tunnelling es el ruteo de la información o paquetes IPv6 a través de topologías IPv4. Esto es de alguna manera menos seguro que dual stack porque la información encapsulada no siempre puede ser inspeccionada por firewalls. Este riesgo potencial de seguridad hace del tunnelling un medio temporal hasta que IPv6 sea adoptado completamente (IPV6MX, s.f., http://www.ipv6.mx).

2.3 Ventajas de ipv6

Durante el periodo de coexistencia de IPv4/IPv6, continuarán surgiendo nuevas redes en el mundo. Se espera que los dispositivos conectados a esas redes utilicen direcciones IPv6 por omisión, así, se creará un mayor espacio compatible entre IPv4 e IPv6.

Esto conducirá a la necesidad de migración a IPv6 y eventualmente creará oleadas de adopción del nuevo protocolo con convincentes ganancias financieras y beneficios tanto para gobiernos como para proveedores de servicios. Con el paso del tiempo, las direcciones obsoletas IPv4 serán muy pocas, por lo que será más costoso conseguirlas con los ISP. Contrariamente, las direcciones IPv6 serán menos costosas dada su abundancia. A los usuarios en hogares y pequeños negocios eventualmente les serán asignadas direcciones IPv6 exclusivamente debido a la escasez de direcciones IPv4.

IPv6 le puede ahorrar dinero a aquellos negocios que hacen de IPv6 una prioridad, pero otros beneficios adicionales por la actualización no deben ser menospreciados.

Algunas de las mejoras notables incluyen lo siguiente:

2.3.1 Autoconfiguración

IPv6 provee la opción para auto configuración de red, lo que significa que cualquier dispositivo IPv6 puede ser conectado a la red, encendido y generará exitosamente por sí mismo una dirección IPv6 sin necesidad de dar una entrada estática en un servidor DHCP. Si el dispositivo es conectado a un router IPv6, éste puede genera una dirección local y una global, ofreciendo acceso inmediato a Internet.

2.3.2 Seguridad intrínseca

Otro de los beneficios para IPv6 es la seguridad y la encriptación intrínseca del contenido. A diferencia de IPv4, los paquetes de IPv6 garantizan una seguridad de punta a punta dado que la información contenida en ellos no puede ser fácilmente decodificada por intermedios.

2.3.3 Soporte mejorado de la calidad de servicio (qos)

La adopción de IPv6 también conlleva notables mejoras en la calidad del servicio (QoS). Las aplicaciones que requieren baja latencia, como VoIP, y aplicaciones multimedia que usen streams, pueden marcar sus paquetes con el nivel de prioridad apropiado para ser transferidos a través de una red de área amplia (WAN) con el retraso más bajo posible.

2.3.4 Mejoras de ruteo

Las tablas de ruteo de Internet se han hecho extremadamente complejas a lo largo de Internet. El esquema de asignación de direcciones de red estructurada usada para IPv6 ayuda a reducir la actual carga en la estructura de red de área amplia. Adicionalmente IPv6 incluye un esquema más sensible para soportar ruteo multicasting.

2.3.5 Encabezado de paquete simplificado

El nuevo encabezado de paquete simplificado y estandarizado usado en IPv6 también mejora el ruteo. IPv6 usa un encabezado de longitud fija de 40 bytes, de los cuales solo 8 son de información general. Esta configuración permite a la información ser ruteada más rápidamente. IPv6 además elimina los campos de fragmentación desde el encabezado del paquete para una mayor eficiencia. Los encabezados de extensión aún pueden ser utilizados, pero sólo cuando sea necesario.

2.3.6 Movilidad mejorada

IPv6 provee mejor movilidad para los usuarios que van de una subred a otra. Una conexión a red móvil puede ser mantenida transparentemente ya que cada dispositivo, ya sea smarthphone o tableta, es identificado por su dirección original. Si un dispositivo se conecta a través de una red foránea, su información de ubicación será relevada a un agente de casa. Éste agente intercepta los paquetes hacia el dispositivo para luego enviarlos hacia su ubicación. En conclusión, IPv6 tiene el potencial de hacer que los usuarios usen sus dispositivos en distintas redes de forma transparente (IPV6MX, s.f., http://www.ipv6.mx).

2.3.7 Tipos de direcciones ipv6

Existen tres tipos de direcciones IPv6:

- Direcciones unicast (uno a uno): Identifica una interfaz de red única. Un paquete enviado a una dirección unicast es entregado sólo a la interfaz identificada con dicha dirección. Es el equivalente a las direcciones IPv4 actuales, y tenemos las siguientes:
  - Globales
  - Enlace - local
  - Local - de - sitio (desaprobada)
  - Unique Local (ULA)

- Compatible - IPv4 (desaprobada)
- 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.

Además podemos citar los siguientes particulares:

- 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 (di Tommaso, L. & García , M., s.f.; citados en Proaño Alulema, 2013).
  - 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 han existido desde el protocolo IPv4 (Vives, A., 2011; citado en Proaño Alulema, 2013).

2.3.8 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 (Proaño Alulema, 2013, pp. 22-23).

2.3.9 Prefijos de los tipos de direcciones

Tabla 1-2: 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

Realizado por: Gabriel Lascano
Fuente: Proaño Alulema, R.X. (2013)

2.3.10 Prefijos globales unicast

Tabla 2-2: 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)

Realizado por: Gabriel Lascano
Fuente: Proaño Alulema, R.X. (2013)

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

2.3.11 Dirección global unicast

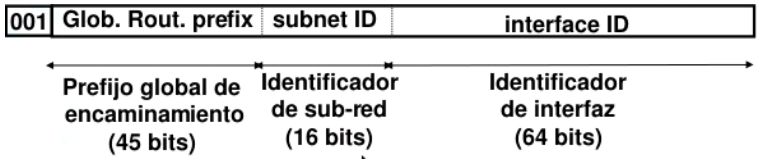


Gráfico 1-2. Dirección Global Unicast
Fuente: Proaño Alulema, R.X. (2013)

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 (Proaño Alulema, 2013, pp. 23-24).

2.3.12 Dirección global unicast para servicios de producción

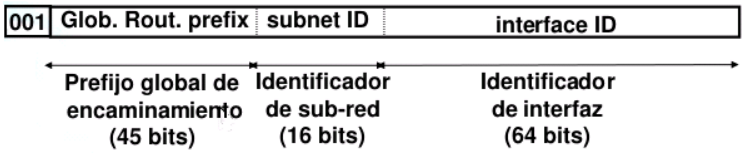


Gráfico 2-2. Dirección Global Unicast Servicios de Producción
Fuente: Proaño Alulema, R.X. (2013)

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.

2.3.13 Recomendaciones para la delegación de direcciones

(Ref RFC3177)

- /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

2.3.14 Direcciones 6to4

Conexiones hacia dominios IPv6 a través de IPv4

Prefijo asignado 2002::/16

Para asignarlos a los sitios 2002:IPV4ADDR::/48 (Proaño Alulema, 2013, pp. 25-26).

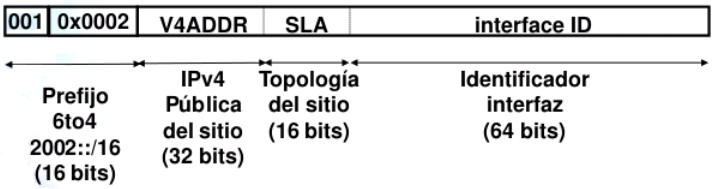


Gráfico 3-2. Conexiones hacia dominios IPv6
Fuente: Proaño Alulema, R.X. (2013)

2.3.15 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

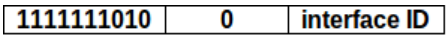


Gráfico 4-2. Link Local
Fuente: Proaño Alulema, R.X. (2013)

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) .

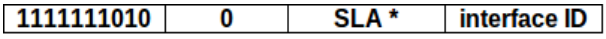


Gráfico 5-2. Site Local
Fuente: Proaño Alulema, R.X. (2013)

2.3.16 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 no distinguibles de las direcciones unicast.

Las direcciones anycast reservadas se definen en el RFC2526 (Proaño Alulema, 2013, pp. 26-27).

2.3.17 Direcciones ipv6 unique local

IPv6 ULA (Unique Local Address)

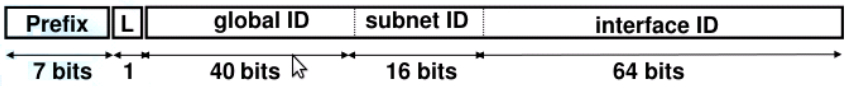


Gráfico 6-2. Dirección ULA
Fuente: Proaño Alulema, R.X. (2013)

2.3.18 Direcciones multicast

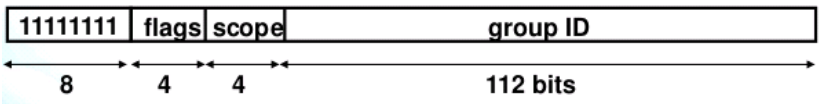


Gráfico 7-2. Multicast
Fuente: Proaño Alulema, R.X. (2013)

- 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:
  - Interface-Local
  - Link-local
  - Admin - local
  - Site - local
  - Organization - local
  - Global

(Proaño Alulema, 2013, pp. 27-28).

2.3.19 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

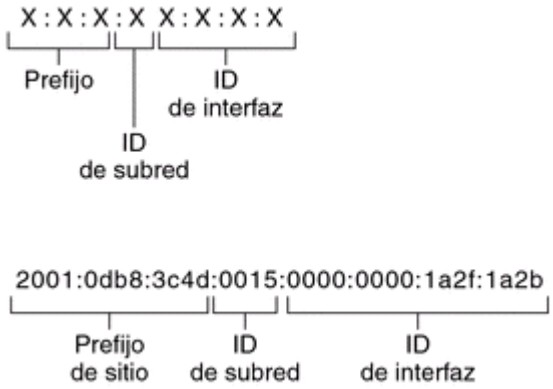


Gráfico 8-2. Características de IPv6
Fuente: Proaño Alulema, R.X. (2013)

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 (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 (Proaño Alulema, 2013, p. 29).

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 (ORACLE, 2010, http://docs.oracle.com; citado en Proaño Alulema, 2013).

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.

2.3.20 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).

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 (Proaño Alulema, 2013, p.29).

2.3.21 Simplificación de la cabecera

La cabecera IPv6 fue modificada para disminuir el tiempo que tardaban los enrutadores en procesarla. Esto se logró eliminando 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 (Domínguez, 2010, http://www.hola-mundo.net; citado en Proaño Alulema, 2013).

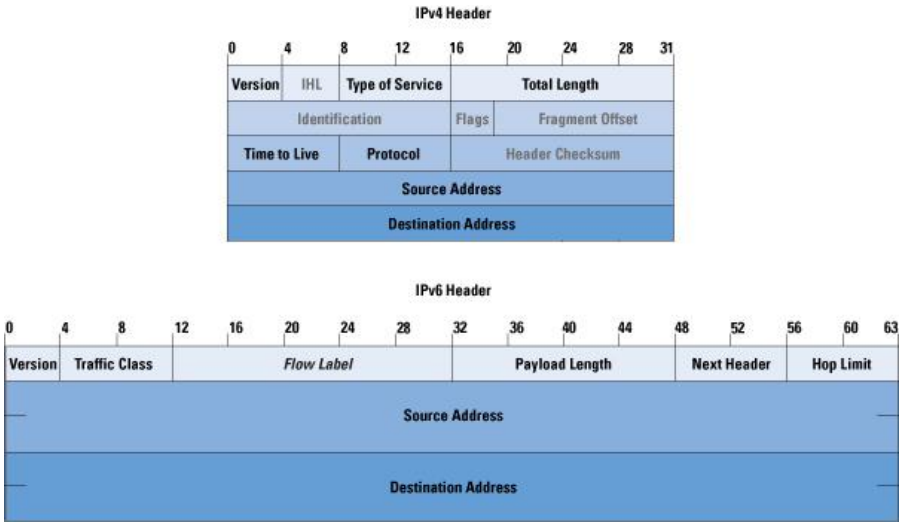


Gráfico 9-2. Encabezado IPv4 – Ipv6.
Fuente: http://notannuevo.blogspot.com/2011/02/la-reserva-de-numeros-ip-necesarios.html

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 ruteadores 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) (Proaño Alulema, 2013, p. 31).

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:

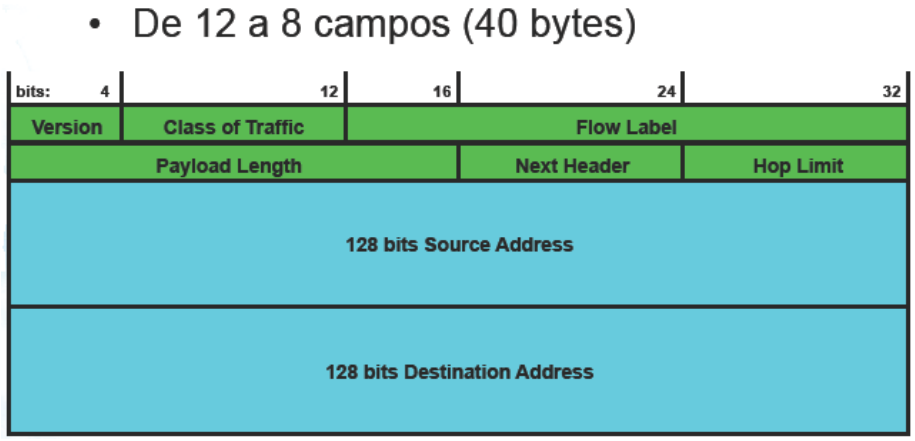


Gráfico 10-2. Formato de la Cabecera IPv6
Fuente: www.spri.eus/euskadinnova/documentos/1535.aspx

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 de destino final. 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 (Proaño Alulema, 2013, pp.32-33).

2.3.22 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".

2.3.23 Direccionamiento jerárquico y enrutamiento eficiente

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 (Proaño Alulema, 2013, p.33).

2.4 Tipos de enrutamiento ipv4

Los protocolos de enrutamiento proporcionan mecanismos distintos para elaborar y mantener las tablas de enrutamiento de los diferentes routers de la red, así como determinar la mejor ruta para llegar a cualquier host remoto. En un mismo router pueden ejecutarse protocolos de enrutamiento independientes, construyendo y actualizando tablas de enrutamiento para distintos protocolos encaminados.

2.4.1 Enrutamiento estático

El principal problema que plantea mantener tablas de enrutamiento estáticas, además de tener que introducir manualmente en los routers toda la información que contienen, es que el router no puede adaptarse por sí solo a los cambios que puedan producirse en la topología de la red. Sin embargo, este método de enrutamiento resulta ventajoso en las siguientes situaciones:

- Un circuito poco fiable que deja de funcionar constantemente. Un protocolo de enrutamiento dinámico podría producir demasiada inestabilidad, mientras que las rutas estáticas no cambian.
- Se puede acceder a una red a través de una conexión de acceso telefónico. Dicha red no puede proporcionar las actualizaciones constantes que requiere un protocolo de enrutamiento dinámico.
- Existe una sola conexión con un solo ISP. En lugar de conocer todas las rutas globales, se utiliza una única ruta estática.
- Un cliente no desea intercambiar información de enrutamiento dinámico.

2.4.2 Enrutamiento predeterminado

Es una ruta estática que se refiere a una conexión de salida o Gateway de "último recurso". El tráfico hacia destinos desconocidos por el router se envía a dicha conexión de salida. Es la forma más fácil de enrutamiento para un dominio conectado a un único punto de salida. Esta ruta se indica como la red de destino **0.0.0.0/0.0.0.0**.

2.4.3 Enrutamiento dinámico

Los protocolos de enrutamiento mantienen tablas de enrutamiento dinámicas por medio de mensajes de actualización del enrutamiento, que contienen información acerca de los cambios sufridos en la red, y que indican al software del router que actualice la tabla de enrutamiento en consecuencia. Intentar utilizar el enrutamiento dinámico sobre situaciones que no lo requieren es una pérdida de ancho de banda, esfuerzo, y en consecuencia de dinero (GuilleSQL, 2008, http://www.guillesql.es).

2.5 Tipos de direccionamiento y otros conceptos ipv4

Para el diseño de arquitectura de cualquier red, es también muy importante conocer y utilizar los siguientes conceptos, con el fin de optimizar y simplificar el direccionamiento y el tamaño de las tablas de enrutamiento. Gracias a la utilización de estas técnicas, los datos reales a principios

de 2000 mostraban que el tamaño de la tabla de enrutamiento era aproximadamente de 76000 rutas.

2.5.1 Direccionamiento con clase

Es también conocido como Direccionamiento IP básico. Siguiendo este modelo de direccionamiento, a una dirección IP únicamente se le puede asignar su máscara predeterminada o máscara natural. Esto supone muy poca flexibilidad, y no es recomendable salvo para redes locales muy pequeñas.

2.5.2 Subnetting

La técnica de subnetting, permite dividir una red en varias subredes más pequeñas que contienen un menor número de hosts. Esto nos permite adquirir, por ejemplo, una red de clase B, y crear subredes para aprovechar este espacio de direcciones entre las distintas oficinas de nuestra empresa. Esto se consigue alterando la máscara natural, de forma que al añadir unos en lugar de ceros, hemos ampliado el número de subredes y disminuido el número de hosts para cada subred.

2.5.3 Máscara de subred de longitud variable (VLSM)

Utilizar protocolos de enrutamiento y dispositivos que soporten VLSM, nos permite poder utilizar diferentes máscaras en los distintos dispositivos de nuestra red, lo cual no es más que una extensión de la técnica de subnetting. Mediante VLSM, podemos dividir una clase C para albergar dos subredes de 50 máquinas cada una, y otra subred con 100 máquinas. Es importante tener en cuenta que RIP1 e IGRP no suportan VLSM.

2.5.4 Supernetting o agregación

La técnica de supernetting o agregación, permite agrupar varias redes en una única superred. Para esto se altera la máscara de red, al igual que se hacía en subnetting, pero en este se sustituyen algunos unos por ceros. El principal beneficio es para las tablas de enrutamiento, disminuyendo drásticamente su tamaño. Un dominio al que se le ha asignado un rango de direcciones tiene la autoridad exclusiva de la agregación de sus direcciones, y debería agregar todo lo que sea posible siempre y cuando no introduzca ambigüedades, lo cual es posible en el caso de redes con interconexiones múltiples a distintos proveedores (GuilleSQL, 2008, http://www.guillesql.es).

2.5.5 Notación cidr

La notación CIDR, permite identificar una dirección IP mediante dicha dirección, seguida de una barra y un número que identifica el número de unos en su máscara. Así, se presenta una forma de notación sencilla y flexible, que actualmente es utilizada en la configuración de gran cantidad de dispositivos de red. Un ejemplo sería: 194.224.27.00/24.

2.5.6 Traducción de dirección de red (NAT)

La tecnología NAT permite a las redes privadas conectarse a Internet sin recurrir a la renumeración de las direcciones IP. El router NAT se coloca en la frontera de un dominio, de forma que cuando un equipo de la red privada se desea comunicar con otro en Internet, el router NAT envía los paquetes a Internet con la dirección pública del router, y cuando le responden reenvía los paquetes al host de origen. Para realizar esto, basta con relacionar los sockets abiertos desde el equipo NAT a los equipos de la red privada, con los sockets abiertos desde el equipo NAT a los equipos de Internet, así como modificar las cabeceras de los paquetes reenviados.

2.5.7 Convergencia

La convergencia se refiere al tiempo que tardan todos los routers de la red en actualizarse en relación con los cambios que se han sufrido en la topología de la red.

Todas las interfaces operativas conectadas al router se sitúan en la tabla de enrutamiento. Por ello, si sólo hay un router en la red, éste tiene información sobre todas las redes o subredes diferentes y no hay necesidad de configurar un enrutamiento estático o dinámico (GuilleSQL, 2008, http://www.guillesql.es).

2.6 Sistemas autónomos

Un Sistema Autónomo (AS por sus siglas en Ingles) es un conjunto de redes, o de routers, que tienen una única política de enrutamiento y que se ejecuta bajo una administración común, utilizando habitualmente un único IGP. Para el mundo exterior, el SA es visto como una única entidad. Cada SA tiene un número identificador de 16 bits, que se le asigna mediante un Registro de Internet (como RIPE, ARIN, o APNIC), o un proveedor de servicios en el caso de los SA privados. Así, conseguimos dividir el mundo en distintas administraciones, con la capacidad de tener una gran red dividida en redes más pequeñas y manipulables. En un Point of

Presence o PoP (comúnmente son interfaces entre ISPs) dónde se juntan varios SA, cada uno de estos utilizará un router de gama alta que llamaremos router fronterizo, cuya función principal es intercambiar tráfico e información de rutas con los distintos routers fronterizos del PoP. Así, un concepto importante de comprender es el tráfico de tránsito, que no es más que todo tráfico que entra en un SA con un origen y destino distinto al SA local.

En Internet, la IANA es la organización que gestiona las direcciones IP y números de AS, teniendo en cuenta que cada Sistema Autónomo se identifica por un número inequívoco que no puede ser superior a 65535, teniendo en cuenta que la colección 65412-65535 son SA privados para ser utilizados entre los proveedores y los clientes. Así, podemos ponernos en contacto con RIPE, ARIN o APNIC para solicitar rangos de direcciones IP o números de AS.

2.6.1 SA de conexión única, sin tránsito

Se considera que un SA es de conexión única cuando alcanza las redes exteriores a través de un único punto de salida. En este caso disponemos de varios métodos por los cuales el ISP puede aprender y publicar las rutas del cliente.

- Una posibilidad para el proveedor es enumerar las subredes del cliente como entradas estáticas en su router y publicarlas a Internet a través de BGP.
- Alternativamente, se puede emplear un IGP entre el cliente y el proveedor, para que el cliente publique sus rutas.
- El tercer método es utilizar BGP entre el cliente y el proveedor. En este caso, el cliente podrá registrar su propio número SA, o bien utilizar un número de SA privado si el proveedor tiene soporte para ello.

2.6.2 SA de múltiples conexiones, sin tránsito

Un SA puede tener múltiples conexiones hacia un proveedor o hacia varios proveedores, sin permitir el paso de tráfico de tránsito a través de él. Para ello, el SA sólo publicará sus propias rutas y no propagará las rutas que haya aprendido de otros SA. Los SA sin tránsito y con múltiples conexiones no necesitan realmente ejecutar BGP con sus proveedores, aunque es recomendable y la mayor parte de las veces es requerido por el proveedor.

2.6.3 SA de múltiples conexiones, con tránsito

Esto es un SA con más de una conexión con el exterior, y que puede ser utilizado para el tráfico de tránsito por otros SA. Para ello, un SA de tránsito publicará las rutas que haya aprendido de

otros SA, como medio para abrirse al tráfico que no le pertenezca. Es muy aconsejable (y en la mayoría de los casos requerido) que los SA de tránsito de múltiples conexiones utilicen BGP-4 para sus conexiones a otros SA, mientras que los routers internos pueden ejecutar enrutamiento predeterminado hacia los routers BGP (GuilleSQL, 2008, http://www.guillesql.es).

2.7 Número de Sistemas Autónomos

- El número de sistemas autónomos esta divido en dos rangos:
  - 0 – 65535: rango original de 16 bits
  - 6536 – 4294967295: rango de 32 bits, publicado en la RFC 4893

- Su uso está dispuesto de la siguiente manera:
  - 0 and 65535 (reservado)
  - 1-64495 (para Internet publica)
  - 64496-64511 (para documentación - RFC5398)
  - 64512-65534 (sólo para uso privado)
  - 23456 (representar 32 bits en 16 bits)
  - 65536-65551 (documentación - RFC5398)
  - 65552-4294967295 (para Internet pública)

La representación de 32 bits se especifica en RFC 5396, define “asplain” (formato tradicional) como notación estándar. Los Registros Regionales de Internet por sus siglas en inglés RIRs, asignan los ASNs, que también están disponibles a través los ISP que son miembros de los RIRs.

Actualmente se han distribuido hasta 58367 ASNs de 16 bits a los RIRs para asignación, cerca de 37500 son visibles en Internet Cada RIR ha recibido un bloque de ASNs de 32 bits; de 1400 asignaciones, cerca de 1100 están visibles en Internet (WALC Workshop - Enrutamiento Avanzado, 2011, https://nsrc.org).

2.8 Clasificación y evolución de los protocolos de enrutamiento

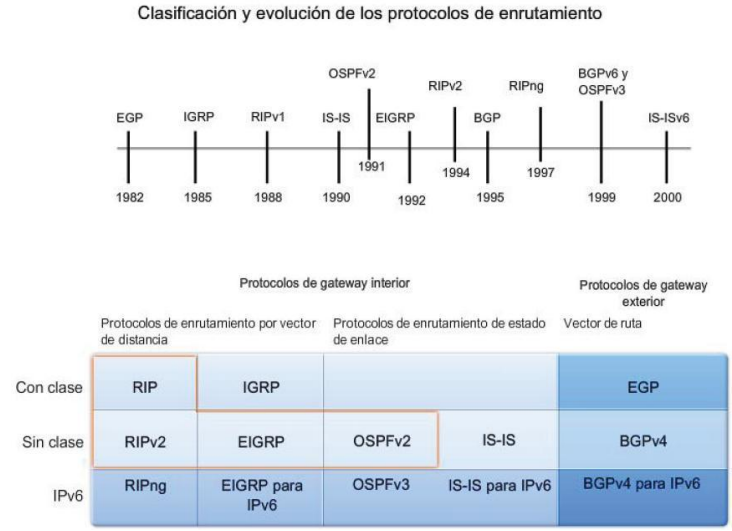


Gráfico 11-2. Clasificación y Evolución de los protocolos de enrutamiento

Fuente: http://networkeando.blogspot.com/2008/11/evolucin-de-los-protocolos-de.html

Los protocolos de enrutamiento dinámico se han usado en redes desde comienzos de la década de los ochenta. La primera versión de RIP se lanzó en 1982, pero algunos de los algoritmos básicos dentro del protocolo ya se usaban en ARPANET en 1969. Debido a la evolución de las redes y a su complejidad cada vez mayor, han surgido nuevos protocolos de enrutamiento. La figura muestra la clasificación de los protocolos de enrutamiento.

Uno de los primeros protocolos de enrutamiento fue el Routing Information Protocol (RIP). RIP ha evolucionado a una nueva versión, el RIPv2. Sin embargo, la versión más nueva de RIP aún no escala a implementaciones de red más extensas.

Para abordar las necesidades de redes más amplias, se desarrollaron dos protocolos de enrutamiento avanzados:

- Open Shortest Path First (OSPF) e Intermediate SystemtoIntermediate System (ISIS).
- Cisco desarrolló el Interior Gateway Routing Protocol (IGRP) y el Enhanced IGRP (EIGRP), que también escala bien en implementaciones de redes más grandes.

Asimismo, surgió la necesidad de interconectar diferentes internetworks y proveer el enrutamiento entre ellas. El protocolo Border Gateway Routing (BGP) ahora se usa entre ISP y entre ISP y sus clientes privados más grandes para intercambiar información de enrutamiento. Con la llegada de numerosos dispositivos para consumidores que usan IP, el espacio de direccionamiento IPv4 está prácticamente agotado. Por tal motivo, ha surgido el IPv6. A fin de

sostener la comunicación basada en IPv6, se han desarrollado versiones más nuevas de los protocolos de enrutamiento IP los cuales se ven en el gráfico 11-2 (Velazquez, 2008, http://networkeando.blogspot.com).

A continuación se muestra una tabla de resumen con las principales características de los protocolos de ruteo más utilizados:

Tabla 3-2: Características de los Protocolos de Ruteo

	RIP-1	**RIP-2**	**IGRP**	**EIGRP**	**OSPF**	**BGP**
¿Soporta VLSM?	NO	SI	NO	SI	SI	SI
Velocidad Convergencia	Lenta	Media	Media	Rápida	Rápida	Rápida
Tecnología	Vector	Vector	Vector	Mixto	Enlace	Vector
Número max. Saltos	15	15	255	255	65535	
Seguridad		MD5		MD5	MD5	
Selección de Ruta	Saltos	Saltos	Varias Métricas	Varias Métricas	Ancho Banda	
Compatibilidad	Universal	Universal	Cisco	Cisco	Universal	Universal
Tipo	IGP	IGP	IGP	IGP	IGP	EGP
¿Proceso / ASN?	NO	NO	PROCESO	PROCESO	PROCESO	ASN
¿Depende de Topología?	NO	NO	NO	NO	SI	NO

Realizado por: Gabriel Lascano
Fuente: http://www.guillesql.es

2.8.1 Protocolos interiores (IGP)

Se encargan del enrutamiento de paquetes dentro de un dominio de enrutamiento o sistema autónomo. Los IGP, como RIP o IGRP, se configuran en cada uno de los routers incluidos en el dominio:

- **Routing Information Protocol (RIP):** RIP es un protocolo universal de enrutamiento por vector de distancia que utiliza el número de saltos como único sistema métrico. Un salto es el paso de los paquetes de una red a otra. Si existen dos rutas posibles para alcanzar el mismo destino, RIP elegirá la ruta que presente un menor número de saltos. RIP no tiene en cuenta la velocidad ni la fiabilidad de las líneas a la hora de seleccionar la mejor ruta. RIP envía un mensaje de actualización del enrutamiento cada 30 segundos (tiempo predeterminado en routers Cisco), en el que se incluye toda la tabla de enrutamiento del router, utilizando el protocolo UDP para el envío de los avisos. RIP-1 está limitado a un número máximo de saltos de 15, no

soporta VLSM y CIDR, y no soporta actualizaciones desencadenadas. RIP-1 puede realizar equilibrado de la carga en un máximo de seis rutas de igual coste. RIP-2 es un protocolo sin clase que admite CIDR, VLSM, resumen de rutas y seguridad mediante texto simple y autenticación MD5. RIP publica sus rutas sólo a los routers vecinos.

- **Open Short Path First (OSPF):** OSPF es un protocolo universal basado en el algoritmo de estado de enlace, desarrollado por el IETF para sustituir a RIP. Básicamente, OSPF utiliza un algoritmo que le permite calcular la distancia más corta entre la fuente y el destino al determinar la ruta para un grupo específico de paquetes. OSPF soporta VLSM, ofrece convergencia rápida, autenticación de origen de ruta, y publicación de ruta mediante multidifusión. OSPF publica sus rutas a todos los routers de la misma área. En la RFC 2328 se describe el concepto y operatividad del estado de enlace en OSPF, mientras que la implementación de OSPF versión 2 se muestra en la RFC 1583. OSPF toma las decisiones en función del corte de la ruta, disponiendo de una métrica máxima de 65535. OSPF funciona dividiendo una intranet o un sistema autónomo en unidades jerárquicas de menor tamaño. Cada una de estas áreas se enlaza con un área backbone mediante un router fronterizo. Así, todos los paquetes direccionados desde un área a otra diferente, atraviesan el área backbone. OSPF envía Publicaciones del Estado de Enlace (Link-State Advertisement – LSA) a todos los routers pertenecientes a la misma área jerárquica mediante multidifusión IP. Los routers vecinos intercambian mensajes Hello para determinar qué otros routers existen en una determinada interfaz y sirven como mensajes de actividad que indican la accesibilidad de dichos routers. Cuando se detecta un router vecino, se intercambia información de topología OSPF. La información de la LSA se transporta en paquetes mediante la capa de transporte OSPF (con acuse de recibo) para garantizar que la información se distribuye adecuadamente. Para la configuración de OSPF se requiere un número de proceso, ya que se pueden ejecutar distintos procesos OSPF en el mismo routers. Los administradores acostumbran usar un número de SA como número de proceso.

- **Interior Gateway Protocol (IGRP):** IGRP fue diseñado por Cisco a mediados de los ochenta, para corregir algunos de los defectos de RIP y para proporcionar un mejor soporte para redes grandes con enlaces de diferentes anchos de banda, siendo un protocolo propietario de Cisco. IGRP es un protocolo de enrutamiento por vector de distancia capaz de utilizar hasta 5 métricas distintas (ancho de banda K1, retraso K3, carga, fiabilidad, MTU), utilizándose por defecto únicamente el ancho de banda y el retraso. Estas métrica pueden referirse al ancho de banda, a la carga (cantidad de tráfico que ya gestiona un determinado router) y al coste de la comunicación (los paquetes se envían por la ruta más barata). Para la configuración de OSPF se requiere un número de proceso, ya que se pueden ejecutar distintos procesos OSPF en el mismo routers. Los administradores acostumbran usar un número de SA como número de proceso.

IGRP envía mensajes de actualización del enrutamiento a intervalos de tiempo mayores que RIP, utiliza un formato más eficiente, y soporta actualizaciones desencadenadas. IGRP posee un número máximo predeterminado de 100 saltos, que puede ser configurado hasta 255 saltos, por lo que puede implementarse en grandes interconexiones donde RIP resultaría del todo ineficiente. IGRP puede mantener hasta un máximo de seis rutas paralelas de coste diferente; Por ejemplo, si una ruta es tres veces mejor que otra, se utilizará con una frecuencia tres veces mayor. IGRP no soporta VLSM. IGRP publica sus rutas sólo a los routers vecinos.

- **Enhaced IGRP – EIGRP:** Basado en IGRP y como mejora de este, es un protocolo híbrido que pretende ofrecer las ventajas de los protocolos por vector de distancia y las ventajas de los protocolos de estado de enlace. EIGRP soporta VLSM y soporta una convergencia muy rápida. EIGRP publica sus rutas sólo a los routers vecinos. Para la configuración de OSPF se requiere un número de proceso, ya que se pueden ejecutar distintos procesos OSPF en el mismo routers. Los administradores acostumbran usar un número de SA como número de proceso.

2.8.2 Protocolos exteriores (EGP)

Los protocolos de enrutamiento exterior fueron creados para controlar la expansión de las tablas de enrutamiento y para proporcionar una vista más estructurada de Internet mediante la división de dominios de enrutamiento en administraciones separadas, llamadas Sistemas Autónomos (SA), los cuales tienen cada uno sus propias políticas de enrutamiento. Durante los primeros días de Internet, se utilizaba el protocolo EGP (no confundirlo con los protocolos de enrutamiento exterior en general). NSFNET utilizaba EGP para intercambiar información de accesibilidad entre el backbone y las redes regionales. Actualmente, BGP-4 es el estándar de hecho para el enrutamiento entre dominios en Internet (GuilleSQL, 2008, http://www.guillesql.es).

2.8.2.1 BGP

Border Gateway Protocol (BGP). Es un protocolo de enrutamiento por vector de distancia usado comúnmente para enrutar paquetes entre dominios, estándar en Internet. BGP gestiona el enrutamiento entre dos o más routers que sirven como routers fronterizos para determinados Sistemas Autónomos. BGP versión 4 (BGP-4), es el protocolo de enrutamiento entre dominios elegido en Internet, en parte porque administra eficientemente la agregación y la propagación de rutas entre dominios. Aunque BGP-4 es un protocolo de enrutamiento exterior, también puede utilizarse dentro de un SA como un conducto para intercambiar actualizaciones BGP. Las conexiones BGP dentro de un SA son denominadas BGP interno (IBGP), mientras que las conexiones BGP entre routers fronterizos (distintos SA) son denominadas BGP externo

(EBGP). BGP-1, 2 y 3 están obsoletos. Para la configuración de OSPF se requiere un número de Sistema Autónomo, ya que se pueden ejecutar distintos procesos OSPF en el mismo routers. BGP se especifica en las RFC 1163, 1267 y 1771, que definen las versiones 2, 3 y 4 de BGP, respectivamente (GuilleSQL, 2008, http://www.guillesql.es).

BGP es más antiguo que IPV6. Aún cuando la versión BGP-4, se sigue utilizando hoy en día, esta precede a IPV6: la primera revisión RFC de BGP-4 (RFC1654) fue publicada en julio de 1994, mientras la RFC1883; la primera revisión de IPV6, no fue publicada hasta diciembre de 1995. A diferencia de protocolos como RIP y OSPF, los cuales tienen versiones separadas para IPV4 e IPV6, hay un solo BGP: BGP-4 maneja los protocolos IPV4 e IPV6 (así como VPNs, MPLS y más) (Noction Network Intelligence, 2015, http://www.noction.com).

2.8.2.2 IBGP

IBGP o también conocido como BGP Interno, permite establecer la comunicación interna entre los routers que se encuentras dentro de un Sistema Autónomo.

Cada router pasarela establece una sesión I-BGP con el resto de pasarelas del mismo AS. Aunque no exista conectividad física directamente, la sesión I-BGP se puede establecer a través de un camino indirecto gracias al resto de routers del AS, los cuales utilizan un protocolo IGP para el encaminamiento.

Las pasarelas de un mismo AS no establecerán sesiones I-BGP mediante direcciones físicas, sino mediante direcciones de bucle o loopback (neighbor {ip address | peer-group} update-source loopback0). El uso de direcciones loopback permite la conexión a una sola dirección virtual de un router que cuenta con varias interfaces y direcciones físicas, de manera que dicha conexión sea independiente a los fallos de una interfaz física. El protocolo IGP correspondiente es el encargado de indicar a una pasarela cómo alcanzar la dirección virtual del otro extremo.

Un aspecto a tener en cuenta en el caso de que un router anuncie vía IBGP información de rutas aprendidas vía EBGP es que el atributo NEXT-HOP de cada ruta se mantiene. De este modo, surgirá un problema si una ruta proviene de un router externo al AS, ya que el router interno que aprende dicha ruta mediante IBGP no sabrá cómo llegar al router externo. Por ello, en los routers frontera que se encargan de intercambiar información de encaminamiento con otros routers de otros AS se utiliza el comando neighbor @IP_vecino_IBGP next-hop-slf. Con este comando se obliga a que todos los anuncios que dicho router hace vía IBGP tengan como NEXT_HOP su propia dirección y no la del router del AS externo.

Para que dentro de un AS todos los routers BGP conozcan todas las redes propagadas vía IBGP, es necesario que el AS se encuentre totalmente mallado (fully meshed), es decir, que se establezcan sesiones IBGP entre todos los routers BGP. En consecuencia, para *n* routers se necesitarán n(n-1)/2 sesiones I-BGP, lo cual puede resultar inviable en un AS con un número considerable de routers. Por ello, para hacer escalable el protocolo I-BGP y reducir el número de sesiones I-BGP dentro de un sistema autónomo se utilizan dos técnicas: BGP Confederations y Route Reflectors.

2.8.2.2.1 Confederations

Dentro de un AS es posible definir AS internos denominados confederaciones, los cuales se comportan como un solo AS general de cara al exterior. La finalidad de una confederación BGP es reducir el mallado I-BGP dentro de un AS. Para ello, se define la confederación como el conjunto de redes y routers del AS principal, el cual se divide en diversos AS. De este modo, en el interior de cada AS interno se utilizará un mallado total (*fully meshed*) entre sus routers de borde y cada AS se conectará con el resto de AS dentro de la confederación.

Aunque los routers de borde de AS diferentes dentro de la confederación intercambian información de encaminamiento mediante sesiones E-BGP, dicha información se intercambia como si se tratase de sesiones I-BGP, es decir, que se preservan atributos como NEXT_HOP, METRIC y LOCAL_PREF. Además, desde el punto de vista de los AS externos a la confederación, el grupo de AS de la confederación se ven como un solo AS.

2.8.2.2.2 Router Reflectors

Una regla a cumplir por los routers BGP para evitar bucles es que no deben anunciar una ruta a un vecino I-BGP si dicha ruta la prendió de otro vecino mediante I-BGP. Por esto, en un AS se debe cumplir que cada router de borde debe tener establecida una sesión I-BGP con el resto de routers de borde de su mismo AS.

Como excepción a la regla anterior, un router con la propiedad de Route Reflector puede anunciar una ruta aprendida por I-BGP a otro vecino I-BGP, lo cual permite reducir considerablemente el número de sesiones I-BGP en un AS. La siguiente opción del comando neighbor convierte a un router en Route Reflector y la IP del vecino indicado corresponde al cliente de dicho Route Reflector: neighbor IP_vecino route-reflector-client.

La combinación de un RR y sus clientes se denomina cluster. El resto de vecinos I-BGP no indicados con el comando anterior en la configuración del RR son considerados como no clientes, por lo que el RR no les anunciará mediante I-BGP las rutas aprendidas de los clientes I-BGP (aunque sí podría hacerlo mediante IGP).

El despliegue de los route reflectors se lleva a cabo dividiendo el backbone en varios grupos (clúster), de manera que cada grupo disponga de un RR al menos (o de múltiples para redundancia) y múltiples clientes. Los RR establecen una malla completa I-BGP entre ellos y pueden ser configurados de forma jerárquica, de forma que en un cluster se pueden tener RRs clientes de otros RRs de un nivel superior (bibing.es.us, s.f., http://bibing.us.es).

2.8.2.3 EBGP

EBGP o también conocido como BGP Externo, permite establecer la comunicación interna entre los routers que se encuentran en distintos Sistemas Autónomos.

EBGP envía información de routing entre Sistemas Autónomos. Los routers EBGP sí tienen que estar físicamente conectados (trajano.us.es)

EBGP se usa para:

- Intercambiar prefijos con otros Sistemas Autónomos
- Implementar políticas (reglas) de enrutamiento

Entre pares BGP en diferentes Sistemas Autónomos:

- Deben estar directamente conectados
- Nunca se debe correr un protocolo interno (IGP) entre pares eBGP (WALC Workshop - Enrutamiento Avanzado, 2011, https://nsrc.org).

2.9 Protocolo ftp

El protocolo FTP o Protocolo de transferencia de archivos es, como su nombre lo indica, un protocolo para transferir archivos. La implementación del FTP se remonta a 1971 cuando se desarrolló un sistema de transferencia de archivos; descrito en RFC141 entre equipos del Instituto Tecnológico de Massachusetts. Desde entonces, diversos documentos de RFC han mejorado el protocolo básico, pero las innovaciones más importantes se llevaron a cabo en julio de 1973. Actualmente, el protocolo FTP está definido por RFC 959, Protocolo de transferencia de archivos (FTP) - Especificaciones.

2.9.1 La función del protocolo ftp

El protocolo FTP define la manera en que los datos deben ser transferidos a través de una red TCP/IP.

El objetivo del protocolo FTP es:

- permitir que equipos remotos puedan compartir archivos
- permitir la independencia entre los sistemas de archivo del equipo del cliente y del equipo del servidor
- permitir una transferencia de datos eficaz

2.9.2 El modelo ftp

El protocolo FTP está incluido dentro del modelo cliente-servidor, es decir, un equipo envía órdenes (el cliente) y el otro espera solicitudes para llevar a cabo acciones (el servidor).

Durante una conexión FTP, se encuentran abiertos dos canales de transmisión:

- Un canal de comandos (canal de control).
- Un canal de datos.

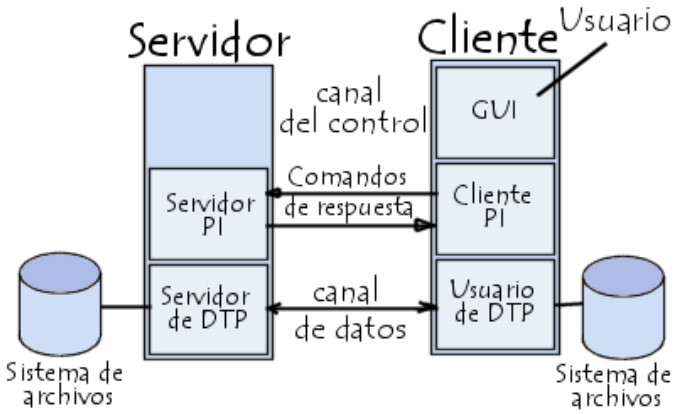


Gráfico 12-2. Modelo FTP
Fuente: http://es.ccm.net/contents/263-protocolo-ftp-protocolo-de-transferencia-de-archivos

Por lo tanto, el cliente y el servidor cuentan con dos procesos que permiten la administración de estos dos tipos de información:

- **DTP** (Proceso de transferencia de datos) es el proceso encargado de establecer la conexión y de administrar el canal de datos. El DTP del lado del servidor se denomina SERVIDOR DE DTP y el DTP del lado del cliente se denomina USUARIO DE DTP.
- **PI** (Intérprete de protocolo) interpreta el protocolo y permite que el DTP pueda ser controlado mediante los comandos recibidos a través del canal de control. Esto es diferente en el cliente y el servidor:

- El SERVIDOR PI es responsable de escuchar los comandos que provienen de un USUARIO PI a través del canal de control en un puerto de datos, de establecer la conexión para el canal de control, de recibir los comandos FTP del USUARIO PI a través de éste, de responderles y de ejecutar el SERVIDOR DE DTP.
- El USUARIO PI es responsable de establecer la conexión con el servidor FTP, de enviar los comandos FTP, de recibir respuestas del SERVIDOR PI y de controlar al USUARIO DE DTP, si fuera necesario.

Cuando un cliente FTP se conecta con un servidor FTP, el USUARIO PI inicia la conexión con el servidor de acuerdo con el protocolo Telnet. El cliente envía comandos FTP al servidor, el servidor los interpreta, ejecuta su DTP y después envía una respuesta estándar. Una vez que se establece la conexión, el servidor PI proporciona el puerto por el cual se enviarán los datos al Cliente DTP. El cliente DTP escucha el puerto especificado para los datos provenientes del servidor. Es importante tener en cuenta que, debido a que los puertos de control y de datos son canales separados, es posible enviar comandos desde un equipo y recibir datos en otro. Entonces, por ejemplo, es posible transferir datos entre dos servidores FTP mediante el paso indirecto por un cliente para enviar instrucciones de control y la transferencia de información entre dos procesos del servidor conectados en el puerto correcto.

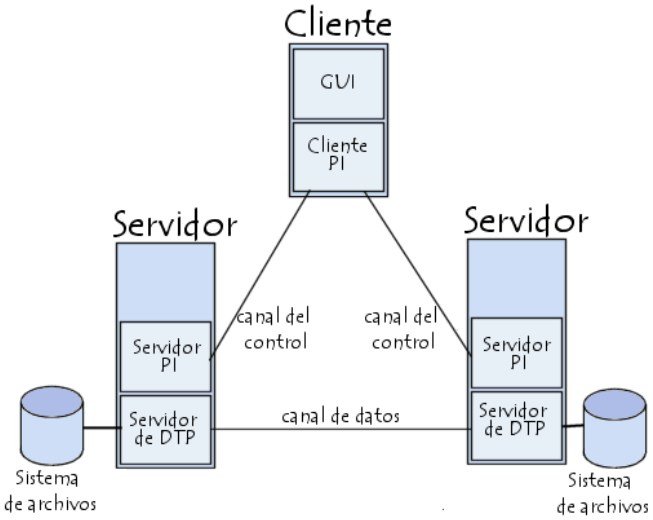


Gráfico 13-2. FTP Funcionamiento de canales de Control
Fuente: http://es.ccm.net/contents/263-protocolo-ftp-protocolo-de-transferencia-de-archivos

En esta configuración, el protocolo indica que los canales de control deben permanecer abiertos durante la transferencia de datos. De este modo, un servidor puede detener una transmisión si el canal de control es interrumpido durante la transmisión (CCM, 2015, http://es.ccm.net).

2.10 Protocolo rtp

El objetivo de RTP o Protocolo en Tiempo Real es brindar un medio uniforme de transmisión sobre IP de datos que estén sujetos a las limitaciones de tiempo real (audio, video, etc.). La función principal de RTP es implementar los números de secuencia de paquetes IP para rearmar la información de voz o de video, incluso cuando la red subyacente cambie el orden de los paquetes.

De manera más general, RTP permite:

- identificar el tipo de información transmitida;
- agregarle marcadores temporales y números de secuencia a la información transmitida;
- controlar la llegada de los paquetes a destino.

Además, los paquetes de difusión múltiple pueden utilizar RTP para enrutar conversaciones a múltiples destinatarios.

2.10.1 Uso de rtp

RTP permite la administración de flujos multimedia (voz, video) sobre IP. RTP funciona sobre el protocolo UDP. El encabezado RTP lleva información de sincronización y numeración. La codificación de datos dependerá del tipo de compresión. El documento RFC3550 especifica el protocolo RTP. Sin embargo, la adaptación de un método de compresión a RTP se describe en un documento RFC específico, por ejemplo H261 en RTP se describe en RFC2032. Se utiliza un canal RTP por tipo de flujo: uno para audio, uno para video. El campo SSRC se utiliza para la sincronización. RTP ofrece un servicio extremo a extremo. Agrega un encabezado que brinda información de tiempo, necesaria para la sincronización de flujo en tiempo real de sonido y video. RTP permite transportar bloques de datos que cuentan con propiedades de tiempo real. El protocolo RTP se encuentra en un nivel de aplicación y utiliza los protocolos de transporte subyacentes TCP o UDP. El uso de RTP generalmente se lleva a cabo por encima de UDP. RTP utiliza tanto el método de difusión individual punto a punto, como el método de difusión múltiple o multipunto.

2.10.2 Formato de los encabezados y su contenido

El encabezado RTP lleva la siguiente información:

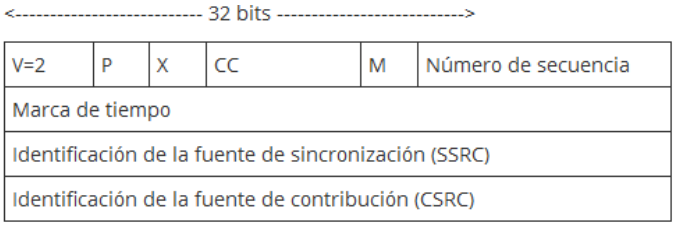


Gráfico 14-2. Encabezado del protocolo RTP
Fuente: http://es.ccm.net/contents/278-protocolos-rtp-rtcp

A continuación se indican los significados de los diferentes campos de encabezados:

- **campo de versión V**: 2 bits de longitud. Indica la versión del protocolo (V=2);
- **campo de relleno P**: 1 bit. Si P es igual a 1, el paquete contiene bytes adicionales para rellenar y finalizar el último paquete;
- **campo de extensión X**: 1 bit. Si X = 1, el encabezado está seguido de un paquete de extensión;
- **campo de conteo CRSC CC**: 4 bits. Contiene el número de CRSC que le sigue al encabezado;
- **campo de marcador M**: 1 bit. Un perfil de aplicación define su interpretación;
- **campo de tipo de carga útil PT**: 7 bits. Este campo identifica el tipo de carga útil (audio, video, imagen, texto, html, etc.);
- **campo Número de secuencia**: 16 bits. Su valor inicial es aleatorio y aumenta de a 1 por cada paquete enviado. Puede utilizarse para detectar paquetes perdidos;
- **campo Marca de tiempo**: 32 bits. Refleja el instante de muestreo del primer byte del paquete RTP. Este instante debe obtenerse a partir de un reloj que aumenta de manera monótona y lineal para permitir la sincronización y el cálculo de la variación de retardo en el destino;
- **campo SSRC**: 32 bits. Identifica de manera única la fuente. La aplicación elige su valor de manera aleatoria. SSRC identifica la fuente de sincronización (simplemente llamada "la fuente"). Este identificador se elige de manera aleatoria con la intención de que sea único entre todas las fuentes de la misma sesión. La lista de CSRC identifica las fuentes (SSRC) que han ayudado a obtener los datos contenidos en el paquete que contiene estos identificadores. La cantidad de identificadores se proporciona en el campo CC;
- **campo CSRC**: 32 bits. Identifica las fuentes contribuyentes (CCM, 2015, http://es.ccm.net).

CAPÍTULO III

3. MATERIALES Y MÉTODOS

3.1 Introducción

La investigación consiste en realizar un análisis comparativo del comportamiento del protocolo de ruteo BGP aplicado en el protocolo de Internet IPV4 e IPV6; dentro de un ambiente de pruebas, que a través de un escenario básico permita observar el comportamiento de cada uno de los protocolos en la trasmisión de servicios web. Debe indicarse que ha sido utilizado el mismo escenario básico para las configuraciones de IPV4 e IPV6, de esta manera se puede establecer una comparación fiable de su comportamiento al emplear las mismas condiciones para su funcionamiento.

Se utilizarán parámetros que permiten diferenciar la eficiencia de los protocolos y mediante su comparación poder establecer las diferencias y ventajas en la implementación de cada uno.

3.2 Objetivo de la metodología

El objetivo de la metodología es determinar el comportamiento del protocolo de ruteo BGP, aplicado sobre el protocolo de comunicación IP en sus versiones 4 y 6, para poder determinar cuál de las dos versiones permite una mejor funcionalidad y eficiencia en la trasmisión de servicios web.

Se considera que la presente investigación es experimental primordialmente ya que se observará el comportamiento en la trasmisión de servicios web sobre cada versión del protocolo IP, sin embargo se han preestablecido ya los servicios RTP y FTP, que serán utilizados para las pruebas, de esta manera se aspira obtener los resultados necesarios que concluyan la investigación.

Por otra parte debido a la naturaleza del proyecto, también se considera que es una investigación descriptiva y se dependerá de pruebas de laboratorio en el escenario básico a ser implementado; y, se utilizará el conocimiento para llevar a cabo el análisis comparativo de los protocolos propuestos.

3.3 Métodos técnicas e instrumentos

3.3.1 Métodos

Para la investigación, se han considerado los siguientes métodos:

3.3.1.1 Método experimental y de observación

Se han empleado estos métodos al estudiar, comparar y determinar el resultado final de valores obtenidos en el ambiente de pruebas, a través de la observación de los indicadores de comparación de los protocolos en cada uno de los casos.

3.3.1.2 Método inductivo

A partir de las pruebas realizadas en el escenario básico, se han obtenido los valores de las variables medibles, de esta forma al compararlas se llegará a una conclusión concreta que permita determinar si la aplicación del protocolo BGP resulta más eficiente sobre IPV4 o IPV6, para la transmisión de servicio web en redes como Internet.

3.3.1.3 Método de análisis

Para poder llegar a la comprobación de la hipótesis que concluya la investigación, se analizarán detenidamente las interacciones presentes en cada caso.

3.3.2 Técnicas

A continuación se indican las técnicas principalmente utilizadas:

- Experimentación
- Observación
- Intuición
- Razonamiento
- Recopilación de información
- Análisis
- Pruebas

3.3.3 Validación de instrumentos

Para la presente investigación resulta imprescindible crear un parámetro de justificación sobre los instrumentos de medición que serán utilizados para las comprobaciones requeridas. De esta manera se podrá establecer el por qué y cómo se han evaluado los escenarios y datos obtenidos.

3.3.3.1 Instrumentos de medición

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 comparación 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:

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.

El cumplimiento de estos requisitos exige apoyo teórico sobre la propiedad que se mide (Herrera, 1998; citado en Proaño Alulema, 2013).

Existen varios criterios para la validación de instrumentos utilizados en la obtención de resultados de una investigación, sin embargo debido a la naturaleza del proyecto se ha escogido la Teoría Clásica de los Test de la cual se han desarrollado posteriormente teorías como la Teoría de Respuestas por Item.

La Teoría Clásica de los Test se denomina al conjunto de principios teóricos y métodos cuantitativos derivados de ellos, que fundamentan la construcción, aplicación, validación e interpretación de distintos tipos de tests y que permiten derivar escalas estandarizadas aplicables a una población (Hambleton, 1996; ciatdo en Proaño Alulema 2013). Los principios en que se basa son relativamente simples y se aplican tanto a las pruebas de desempeño, como a las de aptitud (Camacho, s.f.; citado en Proaño Alulema, 2013).

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 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; citado en Proaño Alulema, 2013).

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.

Existen diferentes procedimientos para estimar la confiabilidad de un instrumento de medición, los más populares son estabilidad, equivalencia y consistencia interna (Proaño Alulema, 2013, p.56).

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 (Hogan, 2004; citado en Proaño Alulema, 2013).

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 (Validación y Estandarización de Instrumentos, s.f.; citado en Proaño Alulema, 2013).

De acuerdo a lo citado anteriormente se ha optado como instrumento de medición al aplicativo de monitoreo de tráfico de red Wireshark; no obstante, de igual manera se han utilizado capturas de datos mediante la observación del investigador en el escenario básico planteado para el presente proyecto con un aplicativo de medición de uso de ancho de banda denominado DU-Meter, así como el monitoreo de las funciones de red mediante el Administrador de tareas de Windows, en los host que realizan las interacciones para la transmisión de datos. De la misma manera se ha utilizado Mausezahn con el fin de generar tráfico en el escenario planteado para poder simular las interferencias existentes en redes reales. Los mencionados instrumentos se ajustan a las necesidades de la investigación debido al tipo de análisis a ser realizado y cuentan con licencias GPL; excepto en el caso de DU-Meter al ser un software licenciado, por lo que en su mayoría son gratuitos y ampliamente utilizados en el ámbito académico y profesional.

3.3.3.2 Wireshark

Figura 1-3. Logo Wireshark
Fuente: https://www.wireshark.org/

Wireshark es un analizador de protocolos open – source diseñado por Gerald Combs y que actualmente está disponible para plataformas Windows y Unix. Conocido originalmente como

Ethereal, su principal objetivo es el análisis de tráfico además de ser una excelente aplicación didáctica para el estudio de las comunicaciones y para la resolución de problemas de red.

Wireshark implementa una amplia gama de filtros que facilitan la definición de criterios de búsqueda para los más de 1100 protocolos soportados actualmente hasta la versión 1.4.3; y todo ello por medio de una interfaz sencilla e intuitiva que permite desglosar por capas cada uno de los paquetes capturados.

Gracias a que Wireshark "entiende" la estructura de los protocolos, podemos visualizar los campos de cada una de las cabeceras y capas que componen los paquetes monitorizados, proporcionando un gran abanico de posibilidades al administrador de redes a la hora de abordar ciertas tareas en el análisis de tráfico.

De forma similar a Tcpdump, Wireshark incluye una versión en línea de comandos, denominada Tshark. Pueden existir situaciones en las que Wireshark no sea capaz de interpretar ciertos protocolos debido a la falta de documentación o estandarización de los mismos, en cuyo caso la ingeniería inversa será la mejor forma de abordar la situación.

Otras herramientas como Snort, OSSIM así como multitud de IDS/IPS permiten alertar sobre algunos de los problemas y ataques comunes en redes existentes hoy en día. 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 (Merino, 2011, https://www.incibe.es).

Ver Anexo A Captura de Tráfico con Wireshark

3.3.3.3 DU Meter

Figura 2-3. Logo DU Meter
Fuente: http://www.hageltech.com

Du Meter es un monitor de uso de Internet que puede ser instalado en un computador. Muestra gráficos en tiempo real y puede crear reportes y alertas basados en las cargas y descargas hechas desde el equipo (Ltd., 2016, http://www.hageltech.com).

A pesar de ser una aplicación licenciada, su versión de prueba permite disponer de todas sus características. Es de fácil instalación y presenta una pequeña pantalla flotante e interactiva que permite ir viendo el uso real de ancho de banda del medio utilizado por el computador. Permite generar gráficos a partir de la información obtenía, programar cronómetros de medición, realizar pantallas comparativas de acuerdo al tipo de tráfico que es enviado a través de la red entre otras características.

Ha sido empleado para comprobar e incluso realizar mediciones en el presente proyecto, permitiendo comprobar los resultados obtenidos con el analizador de tráfico seleccionado. Además Se ha podido ir monitoreando en tiempo real el comportamiento del ancho de banda del medio en cada unos de los gráficos y tablas disponibles, facilitando evidenciar el comportamiento real del medio en cada una de las pruebas realizadas.

Ver Anexo B Medición de ancho de banda con DUMeter

3.3.3.4 FileZilla Server

Figura 3-3. Logo FileZilla Server
Fuente: https://filezilla-project.org

Aplicativo de software libre que permite la transmisión de archivos mediante la estructura cliente - servidor. Muy sencillo de utilizar, permite la creación de una carpeta o repositorio en donde se ingresan los archivos que estarán disponibles en el servidor. Puede accederse desde cualquier explorador digitando directamente la dirección IP del dispositivo en donde fue instalado o a su vez se puede instalar la versión cliente para una interacción por medio de la interfaz del aplicativo.

Debe configurarse una contraseña de acceso al servidor para iniciar la comunicación y se debe especificar un número de servidor y puerto para su funcionamiento por defecto se encuentran estos parámetros como 127.0.0.0 (local) y 14147 respectivamente.

3.3.3.5 Generador de Tráfico Mausezahn

Figura 4-3. Logo Mausezahn
Fuente: http://www.perihel.at/sec/mz/

Mausezahn que en alemán significa "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 este proyecto, como una valiosa herramienta para simular el ruido o interferencia que se presenta en las redes debido al funcionamiento de los dispositivos que conviven en la misma, los que afectan el rendimiento del medio.

Lo que se pretende es generar tráfico IP desde una terminal con Ubuntu ubicada en uno de los extremos del escenario, con el siguiente comando:

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

(Proaño Alulema, 2013, p.58).

Ver Anexo C Generación de Tráfico Ip con Mausezahn

3.4 Implementación del entorno de pruebas

En el presente proyecto se ha procurado desarrollar un entorno de pruebas acorde a las necesidades de transmisión de los servicios web escogidos, permitiendo principalmente la simulación de una red de área extensa o WAN por sus siglas en inglés, en las que es utilizado ampliamente el protocolo BGP, tratando de mantener un ambiente cercano a lo existente en redes como el INTERNET.

Es así que el escenario propuesto contempla la implementación de dos sistemas autónomos, cada uno posee dos routers que realizan el ruteo interno y entre cada sistema autónomo;

finalmente, uno de los routers de cada sistema cuenta con dos interfaces que permiten configurar el ruteo externo a los host o computadores de los extremos que tienen la función de llevar a cabo las interacciones en la trasmisión de servicios web, a través de los protocolos seleccionados. Posteriormente se presentará gráficamente la distribución de los equipos.

Adicionalmente, se ha utilizado recursos de software libre que han facilitado la implementación correcta del protocolo BGP y su medición fiable, lo que ha permitido reducir los costos en comparación de la utilización de hardware y software licenciados.

Se debe señalar que por al trabajar con hardware alternativo y software libre, en lugar de equipos de marca o licenciados, se empleó un hub para la comunicación del sistema autónomo principal es decir para la interconexión entre los cuatro routers empelados, esto facilita la medición del tráfico existente en la red propuesta, permitiendo que los computadores responsables del monitoreo puedan escuchar todo el tránsito existente. Algo similar ocurre con el equipo generador de tráfico, el cual se encuentra conectado directamente al hub, con el objeto de inyectar tráfico para simular la interferencia y saturación del medio debido a la trasmisión de datos entre dispositivos en una red de producción.

3.4.1 Tráfico seleccionado

Se debe indicar el tipo de tráfico existente en la actualidad en INTERNET, al ser el tipo de red en la que principalmente se aplica el protocolo de ruteo avanzado BGP, sobre los protocolos IPv4 e IPv6; los cuales a pesar de denominarse protocolos de INTERNET, son esenciales para el funcionamiento de cualquier tipo de red de computadores y hoy en día dispositivos móviles.

Como se puede evidenciar en nuestras actividades diarias, siempre recurrimos en busca de descargas de programas, aplicativos, documentos, archivos de varios tipos desde INTERNET, se podría decir que es el principal uso para la red de redes, facilitándonos la obtención de contenidos. En base a lo expuesto, para llevar a cabo dicha actividad, es empleado el protocolo FTP, que permite la transmisión de archivos desde servidores localizados alrededor del mundo entero.

Por otra parte hoy en día, se han difundido las aplicaciones de telefonía y video conferencia a través de INTERNET, varias páginas de redes sociales ofrecen esta posibilidad, facilitándonos la comunicación con lugares de todo el mundo. Este tipo de protocolo se denomina protocolo en tiempo real o RTP, el cual permite el funcionamiento de aplicaciones de este tipo.

Finalmente, encontramos el protocolo más utilizado en la web HTTP o Hypertex Transfer Protocol, el cual ha estado presente desde los inicios de la INTERNET, al ser un protocolo orientado a transacciones y que sigue el esquema petición – respuesta entre un equipo cliente y un servidor. Permite casi todas las transacciones realizadas en páginas web, sin embargo la cantidad de datos transmitidos en el escenario escogido no facilita el propósito comparativo de la presente investigación.

Para este estudio, nos centraremos en el tráfico FTP y RTP existente, debido a la gran cantidad que se genera de estos, lo que facilitará la obtención de datos y su correspondiente comprobación.

3.4.2 Escenario básico de red

Resulta necesario establecer un escenario que permitan la demostración correcta del proyecto, existen varios conceptos sobre el diseño de escenarios de pruebas en redes; no obstante, se puede decir que un escenario básico de red comprende una estructura simple en la que existe una única red con un router de salida a Internet y una única red interna (GIGAS, 2011, https://gigas.com).

Por lo expuesto el escenario básico consiste en una única red que simula la configuración interna de BGP o IBGP en los sistemas autónomos planteados y que a los extremos ubica los routers de salida para configuración de BGP externo o EBGP. Dicha red ha sido interconectada a través de un Hub que permite la comunicación de los routers empleados. De igual manera se han utilizado clientes de red conectados a los routers extremos todo esto en conjunto, permite la transmisión de paquetes y su medición, en la red simulada.

3.4.3 Recursos de software y hardware utilizados

Se detalla un listado de los recursos de Software y hardware utilizados para la implementación del entorno de pruebas desarrollado:

Requerimientos de Hardware:

- 4 PCs de escritorio como routers VYATTA
- 1 PC de escritorio para la captura y análisis de tráfico con WIRESHARK
- 1 Hub para permitir el monitoreo de red
- 1 regulador de energía
- 2 corta picos

- 8 Patchs cords elaborados de Cable UTP categoría 6 (6 configurados para una conexión directa y 2 para una conexión cruzada)
- Conectores RJ45
- 3 Laptops, 2 que servirán como Softphones y 1 que permitirá la inyección de tráfico en la red simulada.

Requerimientos de Software:

- Sistema operativo Linux distribución Ubuntu 15.10
- Sistema operativo Windows 7 Ultimate service pack 1
- Sistema operativo Windows XP service pack 3
- Software de monitoreo y tráfico WIRESHARK
- Software para cliente SIP LINPHONE
- Software de Ruteo LINUX VYATTA
- Generador de tráfico basado en C MAUSEZAHN
- Software servidor FTP FILEZILA SERVER 0.9.53 Beta
- Software de monitoreo estadístico de ancho de banda DU-Meter

Diagrama sobre el direccionamiento utilizado en el escenario propuesto:

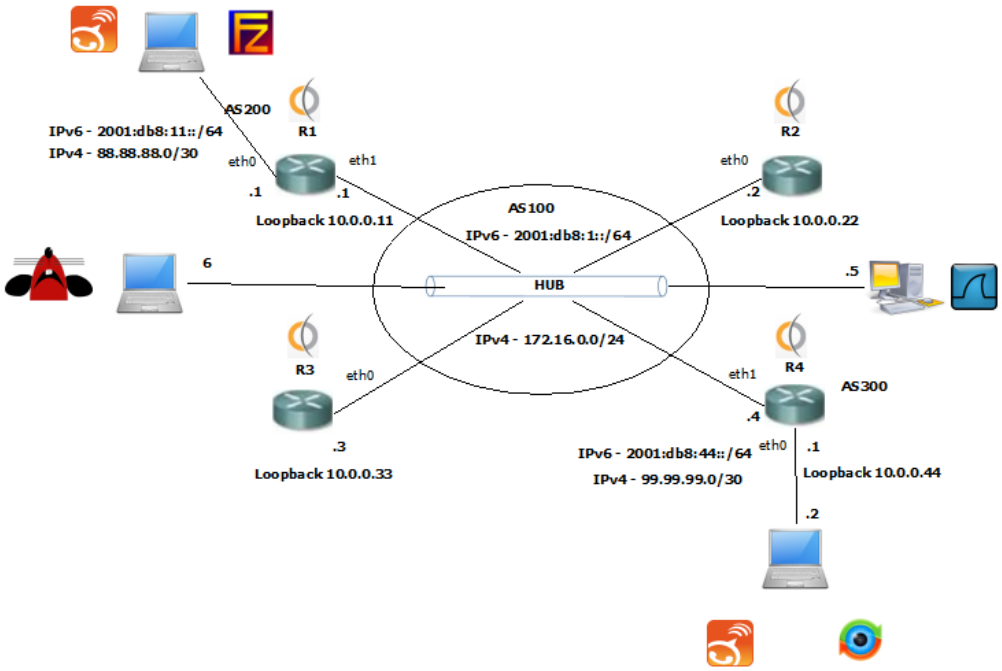


Gráfico 1-3. Diagrama del escenario de Pruebas utilizado
Fuente: Gabriel Lascano

A continuación se detalla el direccionamiento utilizado para cada uno de los dispositivos:

Tabla 1-3: Direccionamiento de Red utilizado en el Escenario

Dispositivo / Interfaz	IPv4	IPv6
R1 eth0	88.88.88.1/30	2001:db8:11::1/64
R1 eth1	172.16.0.1/24	2001:db8:1::1/64
R2 eth0	172.16.0.2/24	2001:db8:1::2/64
R3 eth0	172.16.0.3/24	2001:db8:1::3/64
R4 eth1	172.16.0.4/24	2001:db8:1::4/64
R4 eth0	99.99.99.1/30	2001:db8:44::1/64

Realizado por: Gabriel Lascano

El direccionamiento de los PCs utilizados como host de telefonía, servidor FTP, monitoreo de red y generador de tráfico es el siguiente:

Tabla 2-3: Direccionamiento de Red utilizado en el Escenario

Recurso Instalado	IPv4	IPv6
Filezila Sever / Linphone	99.99.99.2/30	2001:db8:44::2/64
Wireshark	172.16.0.5/24	****
Linphone / DU - Meter	88.88.88.2/30	2001:db8:11::2/64
Mausezahn	172.16.0.6/30	2001:db8:1::6/64

Realizado por: Gabriel Lascano

Se debe indicar que el PC utilizado para el monitoreo de red mediante WIRESHARK, dispone únicamente de dirección IPv4, debido a que puede escuchar todo el tráfico generado en la red aun IPv6; además, gracias a la utilización de un HUB ha sido posible realizar las mediciones de todo el tráfico existente sin necesidad de ningún otro tipo de configuración como en equipos CISCO, en los que para realizar esta tarea es indispensable habilitar los puertos en modo promiscuo mediante configuración y de esta manera poder escuchar todo el tráfico existente.

Ver Anexo D Capturas del escenario de pruebas

3.5 Configuración del Sistema

3.5.1 Linux vyatta 6.5

Figura 5-3. Logo Vyatta
Fuente: http://distrowatch.com/?newsid=07572

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 (Martínez et. al, 2011; citado en Proaño Alulema, 2013).

Tabla 3-3: Cuadro comparativo software de ruteo

Distribución	Servicios	Puntos
Smoothwall	Distribución Router / Firewall con una interface web y terminal liviana	2
Vyatta	Router calse C Mútiple SSID/VLAN/WLAN/QoS/LIVE CD, firewall, VPN, ipv6, servicios lan avanzados/vFirewall/funcionalidad de virtualización de red vRouter/routing dinámico/router/firewall/QoS/Wi-Fi/Autenticación Múltiple SSID-RADIUS/Zeroshell/VLAN/bridging/WAN/balanceo de carga	21
Zentyal (formely eBox Platform)	Router / Firewall y pequeño servidor de oficina	
Zeroshell	Router/firewall/QoS/Wi-Fi/Autenticación Múltiple SSID - RADIUS/Zeroshell/VLAN/bridging/WAN/balanceo de carga	10

Realizado por: Gabriel Lascano
Fuente: http://revistas.udistrital.edu.co/ojs/index.php/REDES/article/view/7174/8831

Gracias a las características ofrecidas por esta distribución de LINUX diseñado como un sistema operativo para ruteo, fue seleccionado VYATTA para el desarrollo del proyecto.

VYATTA está preparado especialmente para realizar funciones de ruteo, vpn, firewall e incluso para trabajar como maquina virtual. Está hecho para trabajar en hardware x86 o PCs y siendo así tiene mayor capacidad de procesamiento que los procesadores de los routers CISCO que poseen su propio sistema operativo denominado IOS. 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, se podría decir que resulta un hibrido de estos dos sistemas operativos y también cuenta con una interface web para administración que podría ser adquirida (Proaño Alulema, 2013, p.64).

Sin embargo en los últimos años a partir del 2013, se ha dejado de desarrollar esta distribución de LINUX dejando de ser gratuito, pasando a desarrollar sistemas operativos que pueden ser comprados o incluso equipos desarrollados para ruteo en los cuales se encuentra instalado ya este software de ruteo. A pesar de que resulta una gran alternativa en el mercado por las características que este sistema posee, se ha tornado difícil poder conseguir versiones gratuitas o anteriores para el desarrollo de investigaciones experimentales como la presente.

A pesar de haberse desarrollado un escenario Dual Stack debido a que BGP fue aplicado sobre los dos protocolos IP y conviven en funcionamiento en el mismo ambiente, se debe indicar que para el ruteo interno o IBGP en IPV4 se ha utilizado OSPF y para IPv6 fue utilizado RIPNG necesarios para realizar dicha labor en BGP. Como BGP necesita un mecanismo de ruteo interno para los routers que se encuentran en un mismo sistema autónomo, resulta indistinto si se aplica el mismo protocolo de ruteo interno sobre las versiones del protocolo IP, por esta razón se ha realizado la experimentación indicada con dos protocolos distintos para el ruteo interno.

3.5.2 Software de clientes voip

Figura 6-3. Logo Linphone
Fuente: http://www.linphone.org

Para la implementación de telefonía IP se ha instalado el software LINPHONE en su versión 3.5.8, en computadores portátiles para facilitar la experimentación realizada. El software implementado es un softphone y es una aplicación informática que forma parte de un entorno VoIP, 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, video conferencia entre otras características (Proaño Alulema, 2013, p.62).

Ver Anexo E Funcionamiento de Linphone

3.5.3 Configuración de routers

Se han utilizado 4 PCs que funcionan como routers configurados para el protocolo BGP sobre las versiones de IPv4 e IPv6. Internamente se ha establecido una sesión de BGP interno o IBGP necesario para la comunicación de los equipos de ruteo dentro del sistema autónomo planteado anteriormente. Los routers R1 y R4 que se encuentran a los extremos en el escenario planteado, realizan el proceso de ruteo externo de BGP o EBGP para la comunicación a los host que funcionan como servidor FTP y clientes de telefonía IP.

Para poder simular un ambiente lo más cercano a la realidad existente en una red como la planteada y que ha permitido experimentar con BGP, se ha optado por interactuar con los

sistemas autónomos de los extremos AS200 y AS300, configurando en los Routers 1 y 4 una característica del software de ruteo VYATTA, utilizada como método para garantizar la Calidad de Servicios o QoS; Traffic Shaper, para poder limitar el ancho de banda (10 Mbps) a las condiciones existentes en una red local que se encontraría en los sistemas autónomos indicados, de esta manera se procura disponer de las características disponibles dentro de una red de comunicaciones entre sistemas de diferente naturaleza como en el caso de Internet, todo esto en el caso de telefonía IP.

Se han escogido los protocolos de ruteo en el caso de IPv4 OSPF y para IPv6 RIPNG, mismos que se encuentran configurados en los cuatro routers y que permiten el encaminamiento interno de la red en el segmento de Sistema Autónomo AS100. Externamente se han configurado dos sistemas autónomos adicionales AS200 y AS300, en los routers 1 y 4 respectivamente, de esta manera se cumple con todo lo requerido por BGP para poder realizar el ruteo de extremo a extremo en el ambiente establecido para las pruebas de la investigación

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.

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 (Proaño Alulema, 2013, p.68).

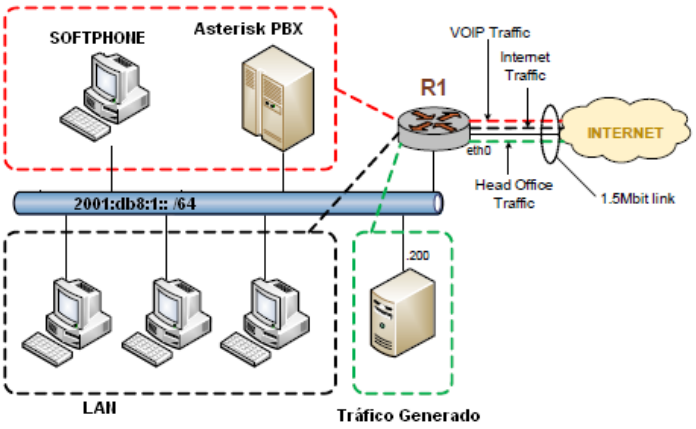


Gráfico 2-3. Funcionamiento de Traffic Shaper
Fuente: Copyright © 2005–2012 por Vyatta, Inc.

Ver Anexo F Configuración de Routers Vyatta

3.6 Planteamiento de la hipótesis

La comparación del protocolo BGP en IPV4 e IPV6 permite definir que protocolo mejora la transmisión de servicios web en un escenario básico.

3.7. Determinación de las variables

Según el planteamiento de la Hipótesis se han identificado dos variables:

3.7.1 Variable independiente

La comparación del protocolo BGP en IPV4 e IPv6.

3.7.2 Variable dependiente

Transmisión de servicios web.

3.8 Operacionalización conceptual

Tabla 4-3: Operacionalización Conceptual de las variables

VARIABLE	TIPO	DEFINICIÓN
La comparación del protocolo BGP en ipv4 e ipv6	INDEPENDIENTE	BGP, protocolo de ruteo externo que permite la interconexión de varios sistemas autónomos, a través de los protocolos de red IPV4 e IPV6, presentes en las redes actuales y futuras por la evolución de las comunicaciones.
Trasmisión de servicios web	DEPENDIENTE	Servicios trasmitidos en redes como la INTERNET, que es la red de redes cuyo pilar fundamental de interconexión es el protocolo de ruteo BGP.

Realizado por: Gabriel Lascano

3.9 Operacionalización metodológica

Tabla 5-3: Operacionalización Metodológica de las Variables

HIPÓTESIS	VARIABLE	INDICADOR	TÉCNICA	INSTRUMENTO
La comparación del protocolo BGP en IPV4 e IPV6 permite definir que protocolo mejora la transmisión de servicios web en un escenario básico.	La comparación del protocolo BGP EN IPV4 E IPV6	* Ancho de banda	Pruebas	Software libre de monitoreo de redes
		* Decisiones de Enrutamiento		
		* Retardo		
	Trasmisión de Servicios Web	* Ancho de Banda	Pruebas	Software libre de monitoreo de redes
		* Paquetes perdidos		
		* Latencia		

Realizado por: Gabriel Lascano

3.10 Datos de prueba

Para la experimentación se han desarrollado cuatro escenarios de pruebas para la obtención de los datos. Debido al tráfico a ser medido se han debido tomar medidas referenciales para cada caso. Resulta indispensable considerar que existen parámetros únicos para el tipo de datos a ser transmitidos de acuerdo a las aplicaciones utilizadas, de esta manera las consideraciones que se establezcan para aplicaciones en tiempo real como VoIP no pueden ser siempre las mismas para en el caso de aplicaciones de transferencia de archivos como FTP.

Por lo expuesto se han considerado los siguientes requerimientos que aseguran la calidad de banda ancha fija con énfasis en canales de voz (Anatel et al., 2010, http://www.anatel.gov.br; citado en Proaño Alulema, 2013):

Tabla 6-3: Parámetros mínimos 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.

Realizado por: Gabriel Lascano
Fuente: Recuperado de http://www.anatel.gov.br

De lo indicado anteriormente, se puede tener una idea de los Indicadores presentados en la Variable Dependiente cuando se aplica calidad de servicio como lo indica Proaño Alulema (2013, pp.71-72), todo esto como ligera referencia ya que no se han utilizado métodos que permitan asegurar la misma en la presenta investigación:

Tabla 7-3: Tabla Referencial de valores de las variables dependientes

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

Realizado por: Gabriel Lascano
Fuente: Recuperado de http://www.anatel.gov.br

Para el cálculo de duración de la llamada, se considera que tiene un comportamiento como el de una distribución exponencial negativa.

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

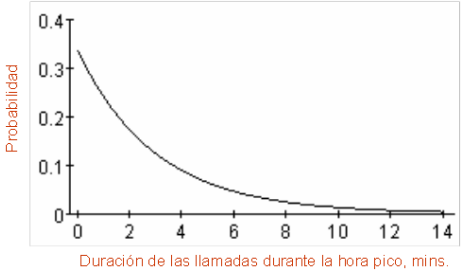


Gráfico 3-3-. Distribución exponencial con media $\mu = 3$ minutos
Fuente: atel.asesores@cantv.net

Por lo cual el tiempo de llamadas para las pruebas realizadas fue de tres minutos (ATEL ASESORES C.A., s.f., http://departamento.pucp.edu.pe; citado en Proaño Alulema, 2013).

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 (Cicileo, 2009, https://nic.ar; citado en Proaño Alulema, 2013).

Se debe indicar que para el análisis de los datos de prueba de la trasmisión de FTP, se utilizarán netamente las comparaciones realizadas de la información obtenida del análisis de tráfico de WIRESHARK y que lo indicado anteriormente establece el tiempo requerido únicamente en el análisis de VoIP. A pesar de no tratarse de una red exclusiva de telecomunicaciones en la que se pueden estimar horarios picos de utilización, los recursos de software anteriormente citados han servido para poder establecer una comparación válida dentro del escenario propuesto, procurando siempre un ambiente lo más real posible al simular un medio ocupado constantemente; no obstante, se debe indicar que el promedio de duración de llamadas señalado a sido estimado para el tráfico de VoIP.

El cálculo del tráfico depende de 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 [s o min]
   Esto se aplica por igual para llamadas de voz o para aplicaciones de datos.

Si Q se expresa en sesión/min y μ en min, el tráfico promedio en erlang viene dado por:

$$A = \mu * Q$$

Si Q se expresa en sesión/hr y μ en segundos entonces el tráfico es

$$A = \frac{\mu * Q}{3600}$$

Por ejemplo: Si en una red llegan 10 llamadas por mín. y cada una dura en promedio 3 min, entonces el tráfico promedio ofrecido a la red es de 30 Erlang (ATEL ASESORES C.A., s.f., http://departamento.pucp.edu.pe; citado en Proaño Alulema, 2013).

Por lo indicado, se ha considerado que el promedio de repeticiones a realizarse en los escenarios de telefonía IP por protocolo será de 10 llamadas de tres minutos para realizar interacciones de 30 minutos en cada caso; y, asumiendo que al mismo tiempo existen varios equipos de telefonía funcionando en la misma red al mismo tiempo en el que se realizan las interacciones entre los host que trabajan con el softphone indicado. Se considera que la red está constantemente intervenida por tráfico ip gracias al generador de tráfico, de esta manera se simula las condiciones de saturación de red en un horario pico.

En la trasmisión de FTP, se ha considerado una ocupación similar del medio, aproximadamente 30 minutos de transmisión, es así que se han escogido archivos de distinto tamaño aleatoriamente que permitan realizar la medición en el tiempo indicado. La comparación de las variables como fue citado, se ha realizado directamente entre los escenarios y archivos utilizados para poder establecer una diferencia mediante el comportamiento de cada protocolo IP. Como principal consideración se ha tomado el porcentaje de mejora en las transmisiones realizadas de una versión con respecto a la otra, es decir se han obtenido los resultados de la aplicación de BGP sobre IPV4 como punto de partida y se ha comparado directamente con su aplicación sobre IPV6, determinado de esta forma su mejora en caso de existirlo.

3.11 Tamaño de la muestra

Al tratarse de una simulación de una red como Internet, resulta difícil establecer el número máximo de transmisiones de servicios web día a día debido a la magnitud de la información enviada y recibida a través de dicha red. No obstante, para la investigación se han establecido los siguientes parámetros de donde se obtendrán los datos necesarios:

- Número de repeticiones de llamadas a realizarse por escenario: 10 llamadas justificadas anteriormente.
- Número de Trasferencias de archivos a través del protocolo FTP: se transferirán 3 archivos de diferentes tamaños de hasta 1 GB, definido como el peso máximo de un archivo descargado a través de la red propuesta (Carrodeguas, 2010, https://norfipc.com).

Para la experimentación se contará con los siguientes escenarios de prueba en el mismo ambiente:

- Escenario 1: Aplicación de BGP sobre IPv4 para la transmisión de RTP
- Escenario 2: Aplicación de BGP sobre IPv6 para la transmisión de RTP
- Escenario 3: Aplicación de BGP sobre IPv4 para la transmisión de FTP
- Escenario 4: Aplicación de BGP sobre IPv6 para la transmisión de FTP

CAPÍTULO IV

4. ANÁLISIS DE RESULTADOS Y DISCUSIÓN

Se detallan los resultados obtenidos de cada escenario en la transmisión de los servicios web RTP y FTP, especificando el detalle de las llamadas realizadas y las transferencias de archivos escogidos para cada uno de los casos. Todo a partido de la observación del comportamiento de cada uno de los protocolos dentro del escenario de prueba, concluyendo directamente de la experimentación y análisis.

Escenario 1: Aplicación de BGP sobre IPv4 para la transmisión de RTP

Se realizan diez llamadas con una duración individual de tres minutos en este escenario, se genera tráfico TCP en el medio con MAUSEZAHN, probando la aplicación del protocolo de ruteo BGP sobre el protocolo IPv4. Los datos obtenidos son los siguientes:

Se detallan a continuación las interacciones entre los equipos de origen y destino:

Tabla 1-4: Interacciones realizadas en el Escenario 1

Host de Origen	Host de Destino
PC1 inicia la llamada	PC2 recibe la llamada
PC1 genera tráfico RTP	PC2 recibe tráfico RTP
PC4 genera tráfico IP	PC2 recibe tráfico IP
PC3 analiza el tráfico de red	

Realizado por: Gabriel Lascano

Los datos obtenidos son los siguientes:

Resumen de la Llamada No 1.

Tabla 2-4: Resumen de la Llamada No 1. Escenario 1

LLAMADA No.	ANCHO DE BANDA Kbps	PAQUETES ESPERADOS	PAQUETES PERDIDOS	PORCENTAJE DE PAQUETES PERDIDOS	LATENCIA
1	28,41	4932	170	3,46	49,67

Realizado por: Gabriel Lascano

Resumen de la Llamada No 2.

Tabla 3-4: Resumen de la Llamada No 2. Escenario 1

LLAMADA No.	ANCHO DE BANDA Kbps	PAQUETES ESPERADOS	PAQUETES PERDIDOS	PORCENTAJE DE PAQUETES PERDIDOS	LATENCIA
2	29,2	9088	275	3,03	49,61

Realizado por: Gabriel Lascano

Resumen de la Llamada No 3.

Tabla 4-4: Resumen de la Llamada No 3. Escenario 1

LLAMADA No.	ANCHO DE BANDA Kbps	PAQUETES ESPERADOS	PAQUETES PERDIDOS	PORCENTAJE DE PAQUETES PERDIDOS	LATENCIA
3	27,73	5313	204	3,85	53,32

Realizado por: Gabriel Lascano

Resumen de la Llamada No 4.

Tabla 5-4: Resumen de la Llamada No 4. Escenario 1

LLAMADA No.	ANCHO DE BANDA Kbps	PAQUETES ESPERADOS	PAQUETES PERDIDOS	PORCENTAJE DE PAQUETES PERDIDOS	LATENCIA
4	24,41	4793	166	3,34	51,49

Realizado por: Gabriel Lascano

Resumen de la Llamada No 5.

Tabla 6-4: Resumen de la Llamada No 5. Escenario 1

LLAMADA No.	ANCHO DE BANDA Kbps	PAQUETES ESPERADOS	PAQUETES PERDIDOS	PORCENTAJE DE PAQUETES PERDIDOS	LATENCIA
5	30,23	9470	364	3,85	50,67

Realizado por: Gabriel Lascano

Resumen de la Llamada No 6.

Tabla 7-4: Resumen de la Llamada No 6. Escenario 1

LLAMADA No.	ANCHO DE BANDA Kbps	PAQUETES ESPERADOS	PAQUETES PERDIDOS	PORCENTAJE DE PAQUETES PERDIDOS	LATENCIA
6	31,81	3986	131	3,3	55,16

Realizado por: Gabriel Lascano

Resumen de la Llamada No 7.

Tabla 8-4: Resumen de la Llamada No 7. Escenario 1

LLAMADA No.	ANCHO DE BANDA Kbps	PAQUETES ESPERADOS	PAQUETES PERDIDOS	PORCENTAJE DE PAQUETES PERDIDOS	LATENCIA
7	31,05	5597	188	3,36	53,23

Realizado por: Gabriel Lascano

Resumen de la Llamada No 8.

Tabla 9-4: Resumen de la Llamada No 8. Escenario 1

LLAMADA No.	ANCHO DE BANDA Kbps	PAQUETES ESPERADOS	PAQUETES PERDIDOS	PORCENTAJE DE PAQUETES PERDIDOS	LATENCIA
8	29,31	4413	153	3,48	51,65

Realizado por: Gabriel Lascano

Resumen de la Llamada No 9.

Tabla 10-4: Resumen de la Llamada No 9. Escenario 1

LLAMADA No.	ANCHO DE BANDA Kbps	PAQUETES ESPERADOS	PAQUETES PERDIDOS	PORCENTAJE DE PAQUETES PERDIDOS	LATENCIA
9	30,45	3614	125	3,47	50,29

Realizado por: Gabriel Lascano

Resumen de la Llamada No 10.

Tabla 11-4: Resumen de la Llamada No 10. Escenario 1

LLAMADA No.	ANCHO DE BANDA Kbps	PAQUETES ESPERADOS	PAQUETES PERDIDOS	PORCENTAJE DE PAQUETES PERDIDOS	LATENCIA
10	31,21	5889	194	3,31	52,7

Realizado por: Gabriel Lascano

Escenario2: Aplicación de BGP sobre IPv6 para la transmisión de RTP

Se realizan diez llamadas con una duración individual de tres minutos en este escenario, se genera tráfico TCP en el medio con MAUSEZAHN, probando la aplicación del protocolo de ruteo BGP sobre el protocolo IPv6. Los datos obtenidos son los siguientes:

Se detallan a continuación las interacciones entre los equipos de origen y destino:

Tabla 12-4: Interacciones realizadas en el Escenario 2

Host de Origen	Host de Destino
PC1 inicia la llamada	PC2 recibe la llamada
PC1 genera tráfico RTP	PC2 recibe tráfico RTP
PC4 genera tráfico IP	PC2 recibe tráfico IP
PC3 analiza el tráfico de red	

Realizado por: Gabriel Lascano

Los datos obtenidos son los siguientes:

Resumen de la Llamada No 1.

Tabla 13-4: Resumen de la Llamada No 1. Escenario 2

LLAMADA No.	ANCHO DE BANDA Kbps	PAQUETES ESPERADOS	PAQUETES PERDIDOS	PORCENTAJE DE PAQUETES PERDIDOS	LATENCIA
1	34,87	9049	171	1,9	45,2

Realizado por: Gabriel Lascano

Resumen de la Llamada No 2.

Tabla 14-4: Resumen de la Llamada No 2. Escenario 2

LLAMADA No.	ANCHO DE BANDA Kbps	PAQUETES ESPERADOS	PAQUETES PERDIDOS	PORCENTAJE DE PAQUETES PERDIDOS	LATENCIA
2	33,68	5408	107	1,98	44,24

Realizado por: Gabriel Lascano

Resumen de la Llamada No 3.

Tabla 15-4: Resumen de la Llamada No 3. Escenario 2

LLAMADA No.	ANCHO DE BANDA Kbps	PAQUETES ESPERADOS	PAQUETES PERDIDOS	PORCENTAJE DE PAQUETES PERDIDOS	LATENCIA
3	32,78	4167	90	2,06	47,09

Realizado por: Gabriel Lascano

Resumen de la Llamada No 4.

Tabla 16-4: Resumen de la Llamada No 4. Escenario 2

LLAMADA No.	ANCHO DE BANDA Kbps	PAQUETES ESPERADOS	PAQUETES PERDIDOS	PORCENTAJE DE PAQUETES PERDIDOS	LATENCIA
4	34,96	9044	193	2,04	44,46

Realizado por: Gabriel Lascano

Resumen de la Llamada No 5.

Tabla 17-4: Resumen de la Llamada No 5. Escenario 2

LLAMADA No.	ANCHO DE BANDA Kbps	PAQUETES ESPERADOS	PAQUETES PERDIDOS	PORCENTAJE DE PAQUETES PERDIDOS	LATENCIA
5	36,98	7587	160	1,95	46,7

Realizado por: Gabriel Lascano

Resumen de la Llamada No 6.

Tabla 18-4: Resumen de la Llamada No 6. Escenario 2

LLAMADA No.	ANCHO DE BANDA Kbps	PAQUETES ESPERADOS	PAQUETES PERDIDOS	PORCENTAJE DE PAQUETES PERDIDOS	LATENCIA
6	35,91	8230	172	2,1	47,45

Realizado por: Gabriel Lascano

Resumen de la Llamada No 7.

Tabla 19-4: Resumen de la Llamada No 7. Escenario 2

LLAMADA No.	ANCHO DE BANDA Kbps	PAQUETES ESPERADOS	PAQUETES PERDIDOS	PORCENTAJE DE PAQUETES PERDIDOS	LATENCIA
7	33,37	6350	130	2,02	41,62

Realizado por: Gabriel Lascano

Resumen de la Llamada No 8.

Tabla 20-4: Resumen de la Llamada No 8. Escenario 2

LLAMADA No.	ANCHO DE BANDA Kbps	PAQUETES ESPERADOS	PAQUETES PERDIDOS	PORCENTAJE DE PAQUETES PERDIDOS	LATENCIA
8	34,85	9032	180	2	48,57

Realizado por: Gabriel Lascano

Resumen de la Llamada No 9.

Tabla 21-4: Resumen de la Llamada No 9. Escenario 2

LLAMADA No.	ANCHO DE BANDA Kbps	PAQUETES ESPERADOS	PAQUETES PERDIDOS	PORCENTAJE DE PAQUETES PERDIDOS	LATENCIA
9	32,65	5968	119	2	49,98

Realizado por: Gabriel Lascano

Resumen de la Llamada No 10.

Tabla 22-4: Resumen de la Llamada No 10. Escenario 2

LLAMADA No.	ANCHO DE BANDA Kbps	PAQUETES ESPERADOS	PAQUETES PERDIDOS	PORCENTAJE DE PAQUETES PERDIDOS	LATENCIA
10	35,75	7308	138	1,89	46,03

Realizado por: Gabriel Lascano

Escenario 3: Aplicación de BGP sobre IPv4 para la transmisión de FTP

Se realizan tres transferencias de archivos diferentes de tamaños 1,14 GB, 632 MB y 18.7 MB, se genera tráfico TCP en el medio con MAUSEZAHN, probando la aplicación del protocolo de ruteo BGP sobre el protocolo IPv4. Los datos obtenidos son los siguientes:

Se detallan a continuación las interacciones entre los equipos de origen y destino:

Tabla 23-4: Interacciones realizadas en el Escenario 3

Host de Origen	Host de Destino
PC2 inicia descarga	PC1 inicia envío
PC2 genera tráfico FTP	PC1 recibe tráfico FTP
PC4 genera tráfico IP	PC2 recibe tráfico IP
PC3 analiza el tráfico de red	

Realizado por: Gabriel Lascano

Los datos obtenidos son los siguientes:

Descarga del archivo de 1,14 GB:

Tabla 24-4: Resumen de la transferencia de archivo de 1,14 GB. Escenario 3

No.	ANCHO DE BANDA Kbps	PAQUETES ESPERADOS	PAQUETES PERDIDOS	PORCENTAJE DE PAQUETES PERDIDOS	LATENCIA
1	270	844118	26930	3,1903	52,79

Realizado por: **Gabriel Lascano**

Descarga del archivo de 632 MB:

Tabla 25-4: Resumen de la transferencia de archivo de 632 MB. Escenario 3

No.	ANCHO DE BANDA Kbps	PAQUETES ESPERADOS	PAQUETES PERDIDOS	PORCENTAJE DE PAQUETES PERDIDOS	LATENCIA
2	250	457496	13757	3,007	49,998

Realizado por: **Gabriel Lascano**

Descarga del archivo de 18,7 MB:

Tabla 26-4: Resumen de la transferencia de archivo de 18,7 MB. Escenario 3

No.	ANCHO DE BANDA Kbps	PAQUETES ESPERADOS	PAQUETES PERDIDOS	PORCENTAJE DE PAQUETES PERDIDOS	LATENCIA
3	200	13561	410	3,0233	50,732

Realizado por: **Gabriel Lascano**

Escenario 4: Aplicación de BGP sobre IPv6 para la transmisión de FTP

Se realizan tres transferencias de archivos diferentes de tamaños 1,14 GB, 632 MB y 18.7 MB, se genera tráfico TCP en el medio con MAUSEZAHN, probando la aplicación del protocolo de ruteo BGP sobre el protocolo IPv6. Los datos obtenidos son los siguientes:

Se detallan a continuación las interacciones entre los equipos de origen y destino:

Tabla 27-4: Interacciones realizadas en el Escenario 4

Host de Origen	Host de Destino
PC2 inicia descarga	PC1 inicia envío
PC2 genera tráfico FTP	PC1 recibe tráfico FTP
PC2 genera tráfico IP	PC1 recibe tráfico IP
PC3 analiza el tráfico de red	

Realizado por: Gabriel Lascano

Los datos obtenidos son los siguientes:

Descarga del archivo de 1,14 GB:

Tabla 28-4: Resumen de la transferencia de archivo de 1,14 GB. Escenario 4

No.	ANCHO DE BANDA Kbps	PAQUETES ESPERADOS	PAQUETES PERDIDOS	PORCENTAJE DE PAQUETES PERDIDOS	LATENCIA
1	520	853853	11031	1,2919	50,005

Realizado por: **Gabriel Lascano**

Descarga del archivo de 632 MB:

Tabla 29-4: Resumen de la transferencia de archivo de 632 MB. Escenario 4

No.	ANCHO DE BANDA Kbps	PAQUETES ESPERADOS	PAQUETES PERDIDOS	PORCENTAJE DE PAQUETES PERDIDOS	LATENCIA
2	460	461266	5633	1,2212	48,97

Realizado por: **Gabriel Lascano**

Descarga del archivo de 18,7 MB:

Tabla 30-4: Resumen de la transferencia de archivo de 18,7 MB. Escenario 4

No.	ANCHO DE BANDA Kbps	PAQUETES ESPERADOS	PAQUETES PERDIDOS	PORCENTAJE DE PAQUETES PERDIDOS	LATENCIA
3	430	13704	157	1,1456	46,96

Realizado por: **Gabriel Lascano**

4.1 Resultados Totales de los Escenarios de Prueba

4.1.1 Resumen del Escenario 1, Aplicación de BGP sobre ipv4 para la transmisión de RTP

Tabla 31-4: Indicadores observados en el Escenario 1

LLAMADA No.	ANCHO DE BANDA Kbps	PAQUETES ESPERADOS	PAQUETES PERDIDOS	PORCENTAJE DE PAQUETES PERDIDOS	LATENCIA
1	28,41	4932	170	3,46	49,67
2	29,2	9088	275	3,03	49,61
3	27,73	5313	204	3,85	53,32
4	24,41	4793	166	3,34	51,49
5	30,23	9470	364	3,85	50,67
6	31,81	3986	131	3,3	55,16
7	31,05	5597	188	3,36	53,23
8	29,31	4413	153	3,48	51,65
9	30,45	3614	125	3,47	50,29
10	31,21	5889	194	3,31	52,7

Realizado por: Gabriel Lascano

4.1.2 Resumen del Escenario2, Aplicación de BGP sobre ipv6 para la transmisión de RTP

Tabla 32-4: Indicadores observados en el Escenario 2

LLAMADA No.	ANCHO DE BANDA Kbps	PAQUETES ESPERADOS	PAQUETES PERDIDOS	PORCENTAJE DE PAQUETES PERDIDOS	LATENCIA
1	34,87	9049	171	1,9	45,2
2	33,68	5408	107	1,98	44,24
3	32,78	4167	90	2,06	47,09
4	34,96	9044	193	2,04	44,46
5	36,98	7587	160	1,95	46,7
6	35,91	8230	172	2,1	47,45

7	33,37	6350	130	2,02	41,62
8	34,85	9032	180	2	48,57
9	32,65	5968	119	2	49,98
10	35,75	7308	138	1,89	46,03

Realizado por: Gabriel Lascano

4.1.3 Resumen del Escenario 3, Aplicación de BGP sobre ipv4 para la transmisión de FTP

Tabla 33-4: Indicadores observados en el Escenario 3

No.	ANCHO DE BANDA Kbps	PAQUETES ESPERADOS	PAQUETES PERDIDOS	PORCENTAJE DE PAQUETES PERDIDOS	LATENCIA
1	270	844118	26930	3,1903	52,79
2	250	457496	13757	3,007	49,998
3	200	13561	410	3,0233	50,732

Realizado por: **Gabriel Lascano**

4.1.4 Resumen del Escenario 4, Aplicación de BGP sobre ipv6 para la transmisión de FTP

Tabla 34-4: Indicadores observados en el Escenario 4

No.	ANCHO DE BANDA Kbps	PAQUETES ESPERADOS	PAQUETES PERDIDOS	PORCENTAJE DE PAQUETES PERDIDOS	LATENCIA
1	520	853853	11031	1,2919	50,005
2	460	461266	5633	1,2212	48,97
3	430	13704	157	1,1456	46,96

Realizado por: **Gabriel Lascano**

4.2 Resumen de los indicadores de la Variable dependiente

De acuerdo a la información obtenida, se han podido generar los siguientes cuadros:

4.2.1 Indicador ancho de banda

ANCHO DE BANDA EN RTP

Tabla 35-4: Resumen Ancho de Banda Escenarios 1 y 2

ESCENARIO 1	ESCENARIO 2
28,41	34,87
29,2	33,68
27,73	32,78
24,41	34,96

30,23	36,98
31,81	35,91
31,05	33,37
29,31	34,85
30,45	32,65
31,21	35,75
29,381	**34,58**

Realizado por: Gabriel Lascano

De la comparación directa entre los valores observados se tiene una diferencia de 5,27 considerando el valor obtenido 29,381 del Escenario 1 como el 100% y la diferencia como el valor de comparación, se tendría una mejora del 17,98% en el Escenario 2.

Comparación del Ancho de Banda en trasmisión de RTP:

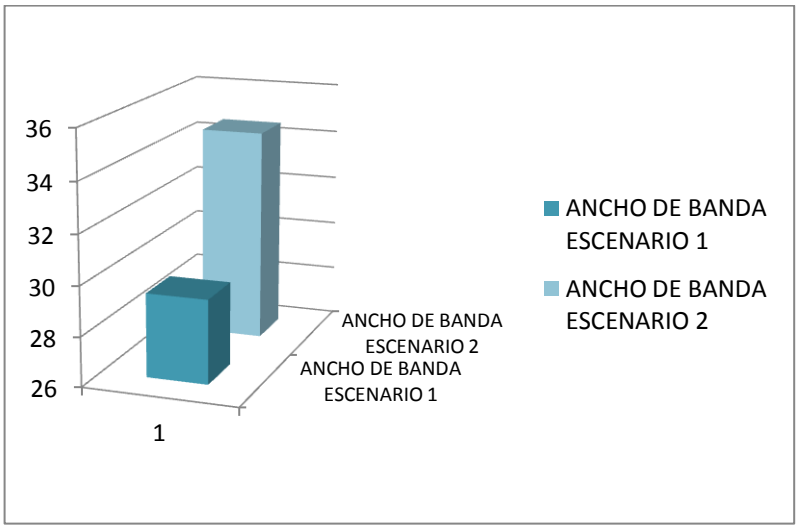


Gráfico 1-4. Comparación Ancho de Banda en Transmisión de RTP
Fuente: Gabriel Lascano

ANCHO DE BANDA EN FTP

Tabla 36-4: Resumen Ancho de Banda Escenarios 3 y 4

ESCENARIO 3	ESCENARIO 4
270	520
250	460
200	430
240	**470**

Realizado por: **Gabriel Lascano**

De la comparación directa entre los valores observados se tiene una diferencia de 230 considerando el valor obtenido 240 del Escenario 3 como el 100% y la diferencia como el valor de comparación se tendría una mejora del 95,83% en el Escenario 4.

Comparación del Ancho de Banda en trasmisión de FTP:

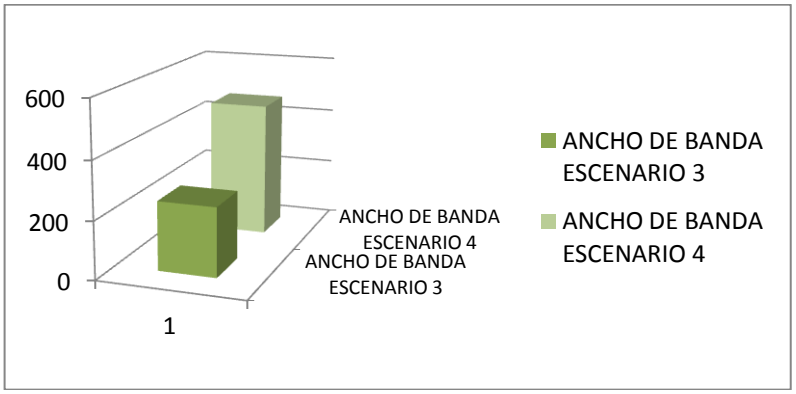


Gráfico 2-4. Comparación Ancho de Banda en Transmisión de FTP

Fuente: Gabriel Lascano

Por lo mostrado en los gráficos, se puede evidenciar que el Escenario No.2 tiene un mejor uso del ancho de banda en relación al Escenario No. 1 en lo que corresponde a RTP. Por otra parte el Escenario No.4 tiene una mejor utilización del ancho de banda del medio en relación al Escenario No. 3 en cuanto a transmisión de paquetes FTP.

4.2.2 Indicador porcentaje de paquetes perdidos

PAQUETES PERDIDOS EN RTP

Tabla 37-4: Resumen Paquetes Perdidos en Escenarios 1 y 2

ESCENARIO 1	ESCENARIO 2
3,46	1,9
3,03	1,98
3,85	2,06
3,34	2,04
3,85	1,95
3,3	2,1
3,36	2,02
3,48	2
3,47	2
3,31	1,89
3,445	**1,994**

Realizado por: Gabriel Lascano

De la comparación directa entre los valores observados se tiene una diferencia de 1,451 considerando el valor obtenido 1,994 del Escenario 2 como el 100% y la diferencia como el valor de comparación se tendría una mejora del 72,76% en el Escenario 2. Debe considerarse que aquí se procura reducir el porcentaje de paquetes perdidos. A continuación se muesta la comparación gráfica de Paquetes Perdidos en trasmisión de RTP:

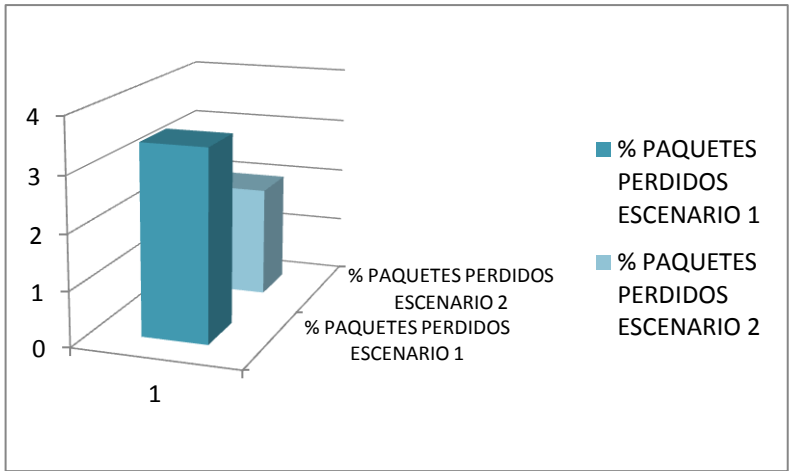


Gráfico 3-4. Comparación Paquetes Perdidos en Trasmisión de RTP

Fuente: Gabriel Lascano

PAQUETES PERDIDOS EN FTP

Tabla 38-4: Resumen Paquetes Perdidos en Escenarios 3 y 4

ESCENARIO 3	ESCENARIO 4
3,1903	1,2919
3,007	1,2212
3,0233	1,1456
3,073533333	**1,219566667**

Realizado por: **Gabriel Lascano**

De la comparación directa entre los valores observados se tiene una diferencia de 1,854 considerando el valor obtenido 1,219 del Escenario 4 como el 100% y la diferencia como el parámetro de comparación, se tendría una mejora del 152,09% en el Escenario 4. Debe considerarse que aquí se procura reducir el porcentaje de paquetes perdidos. A continuación se muesta la comparación gráfica de Paquetes Perdidos en trasmisión de FTP:

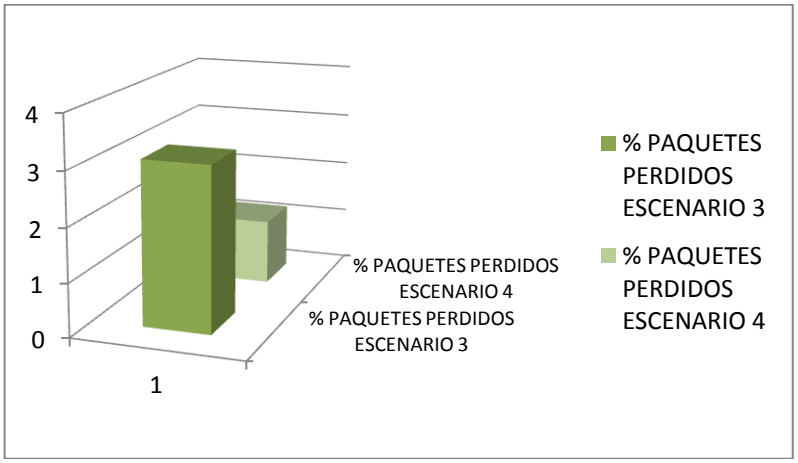


Gráfico 4-4. Comparación Paquetes Perdidos en Trasmisión de FTP

Fuente: Gabriel Lascano

En el gráfico, se puede evidenciar que el Escenario No.2 tiene menor pérdida de paquetes en relación al Escenario No. 1 en lo que corresponde a RTP. De la misma manera el Escenario No.4 tiene una menor pérdida de paquetes en relación al Escenario No. 3 en cuanto a transmisión de paquetes FTP.

4.2.3 Indicador latencia

LATENCIA EN RTP

Tabla 39-4: Resumen Latencia en Escenarios 1 y 2

ESCENARIO 1	ESCENARIO 2
49,67	45,2
49,61	44,24
53,32	47,09
51,49	44,46
50,67	46,7
55,16	47,45
53,23	41,62
51,65	48,57
50,29	49,98
52,7	46,03
51,779	**46,134**

Realizado por: Gabriel Lascano

De la comparación directa entre los valores observados se tiene una diferencia de 5,645 considerando el valor obtenido 46,134 del Escenario 2 como el 100% y la diferencia como el parámetro de comparación, se tendría una mejora del 10,90% en el Escenario 2. Debe considerarse que aquí se procura reducir la Latencia existente. A continuación se muesta la comparación gráfica de Paquetes Perdidos en trasmisión de RTP:

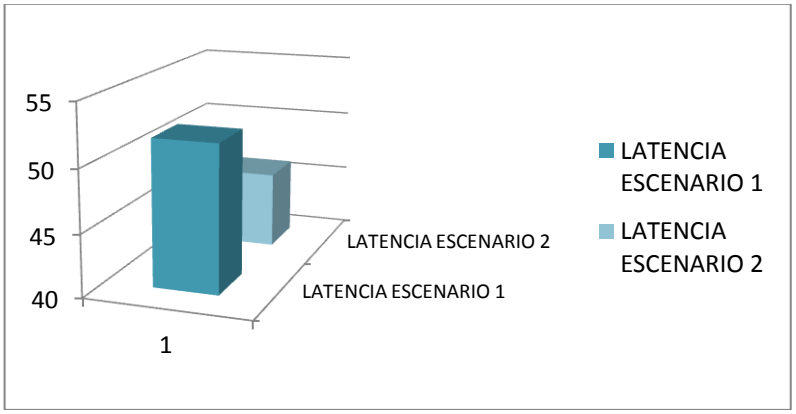


Gráfico 5-4. Comparación Latencia en Trasmisión de RTP
Fuente: Gabriel Lascano

LATENCIA EN FTP

Tabla 40-4: Resumen Latencia en Escenarios 3 y 4

ESCENARIO 3	ESCENARIO 4
52,79	50,005
49,998	48,97
50,732	46,96
51,17333333	**48,645**

Realizado por: **Gabriel Lascano**

De la comparación directa entre los valores observados se tiene una diferencia de 2,528 considerando el valor obtenido 48,645 del Escenario 2 como el 100% y la diferencia como el parámetro de comparación, se tendría una mejora del 5,19% en el Escenario 2. Debe considerarse que aquí se procura reducir la Latencia existente. A continuación se muesta la comparación gráfica de Paquetes Perdidos en trasmisión de FTP:

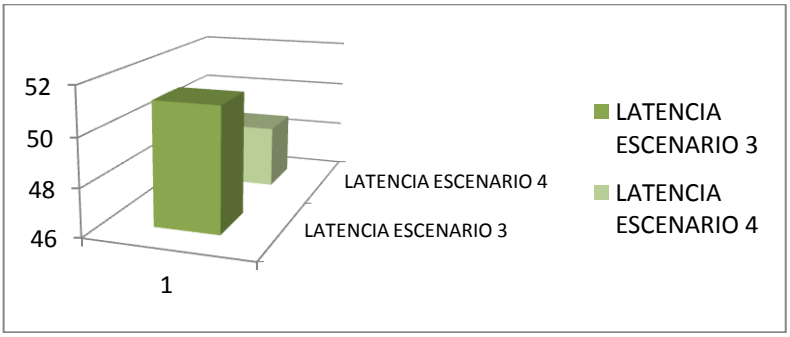


Gráfico 6-4. Comparación Latencia en Trasmisión de FTP
Fuente: Gabriel Lascano

En el gráfico, se puede evidenciar que el Escenario No.2 tiene menor latencia en relación al Escenario No. 1 en lo que corresponde a RTP. De la misma manera el Escenario No.4 tiene un menor retardo comparado con el Escenario No. 3 en cuanto a transmisión de paquetes FTP.

Se debe resaltar que al tratarse de datos de diferente tipo, se han debido comparar por separado con el fin de establecer las diferencias para cada transmisión. De esta manera se ha logrado notar que el único indicador que puede ser comparado entre los cuatro escenarios es el porcentaje de paquetes perdidos que ha mantenido un porcentaje sin mayores fluctuaciones entre cada trasmisión. No obstante, al observar la naturaleza de los datos empleados se ha procedido a observar las consideraciones establecidas en la norma ETSI TS 123 107 V7.1.0 (2007-10) con parámetros mínimos para redes de banda ancha fija como se indica en la Tabla 7.3, sin embargo no se han podido aplicar las mismas para el indicador ancho de banda en FTP para lo cual se tomarán en cuenta otros aspectos que se indican más adelante. Al no utilizar políticas de calidad de servicios que diferencian a las versiones de IPV4 e IPV6, se ha presentado la necesidad de considerar referencialmente cualquier parámetro para poder medir el

desempeño de red. Como el propósito es comparar el comportamiento en la trasmisión de datos en los protocolos seleccionados y poder analizarlos comparativamente uno con respecto al otro, se han definido la siguiente escala de Likert, contemplando la mejor utilización del medio en una red como la del escenario básico de pruebas.

Tabla 41-4: Escala de Likert de los indicadores de la variable dependiente

TRANSMISIÓN DE SERVICIOS WEB	
INDICADOR	**VALOR ASIGNADO**
MUY BUENO	4
BUENO	3
MALO	2
MUY MALO	1

Realizado por: Gabriel Lascano

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

Tabla 42-4: Escala de Likert para Ancho de Banda

VALORES / ESCENARIO	MUY BUENO (4)	BUENO (3)	MALO (2)	MUY MALO (1)	VALOR
1			x		2
2		x			3
3			x		2
4		x			3

Realizado por: Gabriel Lascano

CONDICIÓN PARA RTP

MUY BUENO	> 35 Kbps
BUENO	30 - 35 Kbps
MALO	25 -29 Kbps
MUY MALO	< 25 Kbps

CONDICIÓN PARA FTP

Como ya fue indicado, para el desarrollo del escenario de pruebas se le dio forma al canal de datos reduciéndolo a 10 Mbps configurando mediante Traffic Shaper las condiciones existentes en una red LAN como las consideradas en los sistemas autónomos de los extremos; además, se dividió el ancho de banda en 50% como canal de voz y 50% como canal de datos, lo que significa que para el caso de paquetes FTP en la transmisión de archivos a través de la red se tiene disponible un canal de 5 Mbps, todo esto con el fin de facilitar las comprobaciones.

Según Pinedo (2008, p.54), el ancho de banda disminuye al disminuir el tamaño de los paquetes, puesto que se pierde eficiencia al incrementarse el número de bytes de cabecera por datos enviados. En su investigación en la que además se citan estándares como ITU-T Rec.1540 e ITU-T Rec.1541 que contienen varias consideraciones y recomendaciones sobre el protocolo de Internet y redes de próxima generación, se cita que la ocupación de un canal de datos depende del tamaño de los archivos a ser transferidos y del ancho de banda disponible en el mismo.

De esta manera se ha utilizado la siguiente escala debido a la naturaleza distinta de los paquetes con relación a RTP, considerando los 5 Mbps disponibles según lo explicado en el párrafo anterior, así se considera que mientras más cercana sea la ocupación al ancho de banda disponible, mucho mejor será el protocolo de Internet empleado para la configuración de BGP:

MUY BUENO	> 4 Mbps
BUENO	3 - 4 Mbps
MALO	1 - 2 Mbps
MUY MALO	< 1 Mbps

Como los valores resultantes de la experimentación se encuentran en Kbps se debe proceder a la siguiente conversión de unidades para esta comparación: 1 Mbps = 125 Kbps. De esta manera los valores obtenidos son:

- En el escenario 3 los 240 Kbps promedio equivalen a 1,92 Mbps
- En el escenario 4 los 470 Kbps promedio equivalen a 3,76 Mbps

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

Tabla 43-4: Escala de Likert para Porcentaje de paquetes perdidos

VALORES / ESCENARIO	MUY BUENO (4)	BUENO (3)	MALO (2)	MUY MALO (1)	VALOR
1			x		2
2		x			3
3			x		2
4		x			3

Realizado por: Gabriel Lascano

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 44-4: Escala de Likert para Latencia

VALORES / ESCENARIO	MUY BUENO (4)	BUENO (3)	MALO (2)	MUY MALO (1)	VALOR
1			x		2
2		x			3
3			x		2
4		x			3

Realizado por: Gabriel Lascano

CONDICIÓN

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

4.3 Comprobación de la hipótesis de la investigación

Con el objetivo de realizar la demostración de la investigación se ha empleado la prueba de Chi cuadrado, que como veremos a continuación es una prueba no paramétrica común mente adoptada para comprobar los resultados de una investigación en todo campo lo que le ha permitido tomar mucha popularidad entre diversidad de investigadores, a continuación citamos varios conceptos que nos ampliarán la percepción sobre esta prueba, validando la importancia de su uso o propósito fundamental:

De acuerpo a Jack Levin, 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 (Levin, 1979, p.170; citado en Becerra, s.f.).

"Probablemente la más ampliamente usada prueba no paramétrica de significancia es la prueba chi cuadrada" (Emory, 1985, p.362; citado en Becerra, s.f.).
El test de significancia estadística para variables nominales es X^2 chi cuadrada (Manhein, 1991, p.269; citado en Becerra, s.f.).

Esta prueba es particularmente utilizada en pruebas que envuelven data nominal aunque también puede ser utilizada para escalas superiores. Típicamente es utilizada 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 (Becerra, s.f., http://rigobertobecerra.tripod.com).

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" (Levin, 1979, p.171; citado en Becerra, s.f.).

Por todos los criterios expuestos en relación a la importancia de la prueba escogida, se puede considerar que Chi cuadrada; representada por la letra griega X elevada al cuadrado, es una prueba estadística considerada como no paramétrica, utilizada en la evaluación de hipótesis y que se encasilla como un test o prueba de significancia. De esta manera ha sido seleccionada para la comprobación de la presente investigación.

En el presente proyecto se han define la siguiente Hipótesis a comprobar:

Ho: La Implementación de BGP sobre IPv4 mejora la transmisión de servicios web.
Hi: La Implementación de BGP sobre IPv6 mejora la transmisión de servicios web.

4.3.1. Nivel de significancia

Se ha trabajado con un nivel de significancia de 0,05. Este es valor es ampliamente utilizado por la mayoría de investigadores a nivel mundial para la comprobar de hipótesis y por consiguiente la demostración de los resultados en cada una de sus investigaciones.

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)(4-1)

gl = (1)(3)

gl = 3

$x^2\alpha = critico = 7{,}82$

En la Tabla 50-4, se pueden observar la tabla con los valores críticos de chi cuadrada

Estadístico de prueba

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

4.3.2. 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 de valores observados

Tabla 45-4: Matriz de Contingencia de Valores Observados

			ESCENARIO 1	ESCENARIO 2	ESCENARIO 3	ESCENARIO 4
La Implementación de BGP sobre IPv6 mejora la transmisión de servicios web	**Hi**	**ANCHO DE BANDA**	0	3	0	3
		% PAQUETES PERDIDOS	0	3	0	3
		LATENCIA	0	3	0	3
La Implementación de BGP sobre IPv4 mejora la transmisión de servicios web	**Ho**	**ANCHO DE BANDA**	2	0	2	0
		% PAQUETES PERDIDOS	2	0	2	0
		LATENCIA	2	0	2	0

Realizado por: Gabriel Lascano

4.5 Matriz de contingencia de valores observados promediada

Tabla 46-4: Matriz de Contingencia de Valores Observados Promediada

		ESCENARIO 1	ESCENARIO 2	ESCENARIO 3	ESCENARIO 4	Σ
La Implementación de BGP sobre IPv6 mejora la transmisión de servicios web	**Hi**	0	3	0	3	6
La Implementación de BGP sobre IPv4 mejora la transmisión de servicios web	**Ho**	2	0	2	0	4
		2	3	2	3	10

Realizado por: Gabriel Lascano

4.6 Matriz de valores esperados

Tabla 47-4: Matriz de Valores Esperados

		ESCENARIO 1	ESCENARIO 2	ESCENARIO 3	ESCENARIO 4	Σ en %
La Implementación de BGP sobre IPv6 mejora la transmisión de servicios web	**Hi**	1,2	1,8	1,2	1,8	0,6
La Implementación de BGP sobre IPv4 mejora la transmisión de servicios web	**Ho**	0,8	1,2	0,8	1,2	0,4

Realizado por: Gabriel Lascano

4.7 Matriz diferencia entre valores esperados y observados

Tabla 48-4: Diferencia entre Valores Esperados y Observados

		ESCENARIO 1	ESCENARIO 2	ESCENARIO 3	ESCENARIO 4
La Implementación de BGP sobre IPv6 mejora la transmisión de servicios web	**Hi**	-1,2	1,2	-1,2	1,2
La Implementación de BGP sobre IPv4 mejora la transmisión de servicios web	**Ho**	1,2	-1,2	1,2	-1,2

Realizado por: Gabriel Lascano

4.8 Cálculo de valor de X^2

Tabla 49-4: Cálculo de Chi cuadrado

			ESCENARIO 1	ESCENARIO 2	ESCENARIO 3	ESCENARIO 4	Σ
La Implementación de BGP sobre IPv6 mejora la transmisión de servicios web	**Hi**	**(O-E)^2/E**	1,2	0,8	1,2	0,8	4
La Implementación de BGP sobre IPv4 mejora la transmisión de servicios web	**Ho**	**(O-E)^2/E**	1,8	1,2	1,8	1,2	6
						X^2	10

Realizado por: Gabriel Lascano

4.9 Decisión

De acuerdo a la tabla estadística de distribución de chi-cuadrado, con un nivel de significancia 5%, con un grado de libertad de gl = 3, genera un valor tabulado de X_α^2= 7,82 o Chi crítico.

Tabla 50-4: Valores Críticos de la Distribución de Chi Cuadrada

	0,001	0,01	0,01	0,02	0,03	0,03	0,04	0,05	0,10	0,15	0,20	0,25	0,30	0,35	0,40	
G.D.L	**SIGNIFICATIVO**								**NO SIGNIFICATIVO**							**G.D.L**
1	10,8274	9,1404	7,8794	6,6349	5,0239	3,8415	2,7055	2,0722	1,6424	1,3233	1,0742	0,8735	0,7083	0,5707	0,4549	**1**
2	13,815	11,983	10,597	9,2104	7,3778	5,9915	4,6052	3,7942	3,2189	2,7726	2,4079	2,0996	1,8326	1,597	1,3863	**2**
3	16,266	12,838	11,345	9,837	9,348	8,947	8,311	7,815	6,251	5,317	4,642	4,108	3,665	3,283	2,946	**3**
4	18,467	14,86	13,277	11,668	11,143	10,712	10,026	9,488	7,779	6,745	5,989	5,385	4,878	4,438	4,045	**4**
5	20,515	16,75	15,086	13,388	12,833	12,375	11,644	11,07	9,236	8,115	7,289	6,626	6,064	5,573	5,132	**5**
6	22,458	18,548	16,812	15,033	14,449	13,968	13,198	12,592	10,645	9,446	8,558	7,841	7,231	6,695	6,211	**6**
7	24,322	20,278	18,475	16,622	16,013	15,509	14,703	14,067	12,017	10,748	9,803	9,037	8,383	7,806	7,283	**7**
8	26,124	21,955	20,09	18,168	17,535	17,01	16,171	15,507	13,362	12,027	11,03	10,219	9,524	8,909	8,351	**8**
9	27,877	23,589	21,666	19,679	19,023	18,48	17,608	16,919	14,684	13,288	12,242	11,389	10,656	10,006	9,414	**9**
10	29,588	25,188	23,209	21,161	20,483	19,922	19,021	18,307	15,987	14,534	13,442	12,549	11,781	11,097	10,473	**10**
11	31,264	26,757	24,725	22,618	21,92	21,342	20,412	19,675	17,275	15,767	14,631	13,701	12,899	12,184	11,53	**11**
12	32,909	28,3	26,217	24,054	23,337	22,742	21,785	21,026	18,549	16,989	15,812	14,845	14,011	13,266	12,584	**12**
13	34,528	29,819	27,688	25,472	24,736	24,125	23,142	22,362	19,812	18,202	16,985	15,984	15,119	14,345	13,636	**13**
14	36,123	31,319	29,141	26,873	26,119	25,493	24,485	23,685	21,064	19,406	18,151	17,117	16,222	15,421	14,685	**14**
15	7,697	32,801	30,578	28,259	27,488	26,848	25,816	24,996	22,307	20,603	19,311	18,245	17,322	16,494	15,733	**15**

Realizado por: Gabriel Lascano
Fuente: http://www.mat.uda.cl/hsalinas/cursos/2010/eyp2/Tabla%20Chi-Cuadrado.pdf

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

$10 \geq 7.82$ => Cumple con la condición

Como X^2_c =10 es mayor X^2_α = 7,82 por lo tanto se rechaza la hipótesis nula Ho y se acepta la hipótesis de investigación Hi que dice:

"La Implementación de BGP sobre IPv6 mejora la transmisión de servicios web"

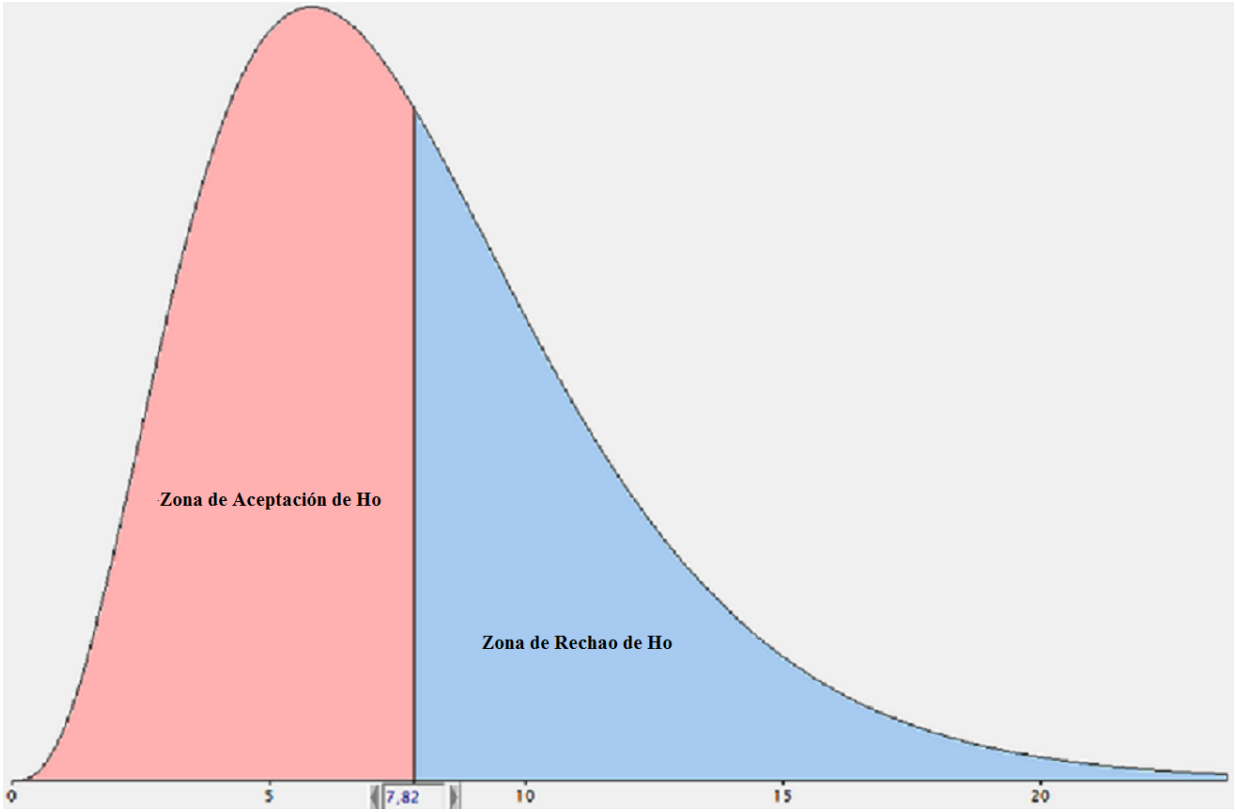


Gráfico 7-4. Comprobación Gráfica de Hipótesis
Fuente: Gabriel Lascano

CONCLUSIONES

- Del presente proyecto se concluye que, al aplicar el protocolo BGP sobre IPv6 se observa mejoras en la transmisión de datos con respecto a IPv4, utilizando una configuración que no contempla las nuevas características que ofrece la calidad de servicios. Se destaca de la comparación directa entre los indicadores, el ancho de banda que mejoró en un 17% en RTP y casi 95% en FTP, porcentaje de paquetes perdidos que se redujo 72% en RTP y hasta 152% en FTP y la una disminución de la latencia con 10 % en RTP y hasta el 5% FTP, a pesar de que las mejoras no fueron tan significativas en todos los escenarios e indicadores.
- BGP escoge el mejor camino para la comunicación, procurando limitar los retardos o pérdidas en las transmisiones en redes como INTERNET, se orienta a la disponibilidad del medio de transmisión de los equipos de ruteo proveyendo la mejor ruta para la comunicación entre los equipos de un mismo sistema autónomo y fuera de este.
- En cuanto a la transferencia de información de los protocolos RTP o FTP, indistintamente de la versión del protocolo IP utilizada, BGP prioriza la comunicación constante de los routers dentro de un sistema autónomo y fuera del mismo a pesar de configuraciones o arquitecturas distintas.
- BGP requiere de un mecanismo de ruteo dentro de los sistemas autónomos. IBGP o BGP interno, hace uso de un protocolo de ruteo interior para poder establecer comunicación entre los routers de un mismo sistema autónomo. De esta manera se aplicó OSPF en IPv4 y RIPNG en IPv6.
- Se ha concluido por que BGP es uno de los protocolos más utilizados para encaminar dominio administrativos distantes, sin embargo se debe recalcar que por sí mismo no tiene en cuenta aspectos importantes como retardo en los enlaces, manejo adecuado del ancho de banda y congestión en la red, algo que fue más notorio cuando fue aplicado sobre la versión del protocolo IPv4. Para su configuración, BGP hace uso de las direcciones de loopback de los routers que intervienen en el sistema.
- BGP se centra principalmente en la comunicación entre routers a través de criterios de asociación y actualización de rutas, de esta manera se encarga de mantener los caminos de comunicación actualizados entre routers de un mismo sistema (pares) así como en los routers de comunicación externa al AS, facilitando la interconexión de redes privadas y públicas de diferente naturaleza como INTERNET.
- Finalmente se puede indicar que existen alternativas a los equipos propietarios, normalmente utilizados para este tipo de comunicaciones y redes; y, a pesar de no ofrecer equipos industrializados de producción continua, prestan una nueva alternativa para la utilización de

protocolos avanzados de ruteo. A pesar de lo indicado siempre va a existir la limitación de hardware al no contar con equipo especialmente diseñado para este propósito.

RECOMENDACIONES

- Al trabajar con software libre y equipos ensamblados, se debe tomar en cuenta el estado físico de los mimos y la disponibilidad de información para su configuración. En la actualidad resulta complicado la utilización de VYATTA por su reciente comercialización, lo que dificulta obtener información adecuada e incluso el sistema operativo mismo para su descarga.
- El software utilizado para la investigación, facilita la implementación de BGP, sin embargo la configuración en el protocolo de transporte IPv6 resulta retadora al momento de escoger el funcionamiento y modo de comunicación de los equipos utilizados.
- Se recomienda planificar correctamente la red a implementarse, definir correctamente su distribución y dispositivos necesarios para su correcto funcionamiento.
- Dependiendo de las interferencias o ruido presente a la red debido a la naturaleza del tráfico empleado en la experimentación, se puso de manifiesto la necesidad de políticas de QoS que garanticen una mejor transmisión de acuerdo a los servicios utilizados.
- Para poder llevar a cabo una medición más precisa en la transmisión, se recomienda implementar mecanismos que garanticen la calidad de la comunicación.
- Se recomienda escoger el tráfico correcto para las mediciones así como los atributos a ser medidos (ancho de banda, retardo, latencia, trasferencia de paquetes), ya que puede encontrarse que los datos a ser medidos no facilitan la demostración al no mostrar diferencias o incluso a tender a valores nulos.
- Se recomienda continuar la Investigación del protocolo de ruteo avanzado BPG y sus aplicaciones para comunicación de redes de distintos orígenes como en el caso de INTERNET.

BIBLIOGRAFÍA

1. **Anatel, CGI.Br e Inmetro.** (11 de 5 de 2010). *Analisam qualidade da banda larga fixa*. Recuperado el 10 de 8 de 2015, de http://www.anatel.gov.br/Portal/exibirPortalNoticias.do?acao=carregaNoticia&codigo=20294
2. **ATEL ASESORES C.A.** (s.f.). *http://departamento.pucp.edu.pe.* Recuperado el 21 de 12 de 2015, de http://departamento.pucp.edu.pe/ingenieria/images/documentos/seccion_telecomunicaciones/Capitulo%205%20Modelos%20de%20Trafico.pdf
3. **Becerra, R.** (s.f.). *Propósito Fundamental de los Test Chi Cuadrado*. Recuperado el 19 de 11 de 2015, de http://rigobertobecerra.tripod.com/chicuadrado.htm
4. **Beijnum, I. v.** (2011). *BPG - Building Reliable Networks with the Borther Gateway Protocol.* (J. Sumser, Ed., & G. Lascano, Trad.) Sebastopol, C.A.: O'Reilly.
5. **bibing.es.us.** (s.f.). *http://bilbing.es.us.* Recuperado el 16 de 12 de 2015, de http://bibing.us.es/proyectos/abreproy/11359/descargar_fichero/BGP%252F6.+I-BGP.pdf
6. **Camacho, J. E.** (s.f.). *www.uv.mx.* Recuperado el 20 de 12 de 2015, de De la Teoría Clásica de los Tests a los Tests Adaptativos Computarizados: Una revisión: http://www.uv.mx/jdiaz/ItemResTheory.htm
7. **Carrodeguas, N.** (2010). *norfiPC*. Recuperado el 14 de 8 de 2015, de https://norfipc.com/redes/velocidad-conexion-internet.html
8. **CCM.** (11 de 2015). *Protocolo FTP*. Recuperado el 20 de 12 de 2015, de es.ccm.net: http://es.ccm.net/contents/263-protocolo-ftp-protocolo-de-transferencia-de-archivos
9. **CCM.** (12 de 2015). *Protocolo RTP*. Recuperado el 20 de 12 de 2015, de es.ccm.net: http://es.ccm.net/contents/278-protocolos-rtp-rtcp
10. **Cicileo, e. o.** (2009). *https://nic.ar.* Recuperado el 21 de 12 de 2015, de https://nic.ar/static/files/ipv6paratodos.pdf
11. **CISCO.** (25 de 12 de 2014). *Multiprotocol BGP para el ejemplo de configuración del IPv6.* Recuperado el 10 de 07 de 2015, de http://www.cisco.com/cisco/web/support/LA/109/1099/1099522_ipv6-bgp-00.pdf
12. **Dominguez, A.** (2010). *Hola Mundo*. Recuperado el 16 de 12 de 2015, de http://www.hola-mundo.net/index.php?/gallery/image/77-cabecera-ipv4/
13. **Emory, W.** (1985). *Business Research Methods.* Illinois, USA: Richard Irwin, Inc.
14. **GIGAS.** (2011). *VPN FICHA TÉCNICA*. Recuperado el 21 de 12 de 2015, de https://gigas.com/static/documents/vpn.pdf

15. ***GuilleSQL.*** (17 de 03 de 2008). Recuperado el 15 de 07 de 2015, de Cap2. Protocolos de Enrutamiento: http://www.guillesql.es/Articulos/Manual_Cisco_CCNA_Protocolos_Enrutamiento.aspx
16. **Hagen, S.** (2014). *IPV6 Essentials - Integrating IPV6 into your IPV4 Network.* (M. &. Loukides, Ed., & G. Lascano, Trad.) Sebastopol, C.A.: O'Reilly.
17. **Hambleton, J. M.** (12 de 1996). *Papeles del Psicólogo.* Recuperado el 20 de 12 de 2015, de http://www.papelesdelpsicologo.es/vernumero.asp?id=737
18. **Herrera, A. N.** (02 de 1998). *DocSlide.* Recuperado el 11 de 12 de 2015, de http://documents.tips/documents/herrera-a-1998-notas-de-psicometria-1-2-historia-de-psicometria-y-teoria.html
19. **Hogan, T. P.** (2004). *Pruebas psicológicas una introducción práctica*. Mexico D.F.: Manual Moderno.
20. **IPV6MX.** (s.f.). *¿Estás listo para Ipv6?* Recuperado el 11 de 06 de 2015, de http://www.ipv6.mx/index.php/informacion/noticias/1-latest-news/93-estas-listo-para-ipv6
21. **Levin, J.** (1979). *Funadamentos de Estadística en la Investigación Social.* México: Harla.
22. **Ltd., H. T.** (2016). *DU Meter 7: How to monitor your internet usage*. Recuperado el 22 de 02 de 2016, de Hagel Technologies Ltd: http://www.hageltech.com/dumeter/about
23. **Manhein, J.** (1991). *Empirical Political Analysis. Research Methods in Political Science.* New York, USA: Longman.
24. **Martínez/González/Antolínez.** (15 de 11 de 2011). *Redes de Ingeniería*. Recuperado el 21 de 12 de 2015, de http://revistas.udistrital.edu.co/ojs/index.php/REDES/article/view/7174/8831
25. **Merino, B.** (02 de 2011). *www.incibe.es.* Recuperado el 21 de 12 de 2015, de https://www.incibe.es/extfrontinteco/img/File/intecocert/EstudiosInformes/cert_inf_seguridad_analisis_trafico_wireshark.pdf
26. ***Multiprotocol BGP para el ejemplo de configuración del IPv6.*** (s.f.). Recuperado el 10 de 07 de 2015, de www.cisco.com: http://www.cisco.com/cisco/web/support/LA/109/1099/1099522_ipv6-bgp-00.pdf
27. **Noction Network Intelligence.** (6 de 2 de 2015). *IPV4 BGP vs IPV6 BGP (G. Lascano, Trad.)*. Recuperado el 10 de 07 de 2015, de http://www.noction.com/blog/ipv4_bgp_vs_ipv6_bgp
28. **ORACLE.** (2010). *Guía de administración del sistema: servicios IP*. Recuperado el 16 de 12 de 2015, de http://docs.oracle.com/cd/E19957-01/820-2981/6nei0r0ue/index.html#ipv6-overview-fig-2
29. **Proaño Alulema, R. X.** (2013). Análisis de la aplicación de QoS sobre IPv6 en la transmisión de VoIP en una LAN corporativa (Tesis de Postgrado). ESPOCH, Riobamba, Chimborazo, Ecuador.
30. **trajano.us.es.** (s.f.). Recuperado el 16 de 12 de 2015, de http://trajano.us.es/~rafa/REDES/apuntes/T5-Introduccion_BGP.pdf

31. **UNT - Facultad Regional Mendoza.** (s.f.). *Valores críticos de la distribución de Chi Cuadrada [Tabla]*. Recuperado el 12 de 12 de 2015, de http://departamento.pucp.edu.pe: http://www.mat.uda.cl/hsalinas/cursos/2010/eyp2/Tabla%20Chi-Cuadrado.pdf
32. ***Validación y Estadarización de Instrumentos.*** (s.f.). Recuperado el 20 de 12 de 2015, de http://extension.upbbga.edu.co/inpec2009/Estudiosprimeraparte/VYEInstrumentos.pdf
33. **Vanaclocha, B.** (s.f.). *PROTOCOLOS DE ROUTING EXTERNO : BGP (BORDER GATEWAY PROTOCOL).* Recuperado el 10 de 05 de 2015, de www.uv.es/~montanan/redes/trabajos/BGP.doc
34. **Velazquez, R.** (25 de 11 de 2008). *Networkeando: Evolución de los protocolos de enrutamiento dinámico*. Recuperado el 12 de 8 de 2015, de http://networkeando.blogspot.com/2008/11/evolucin-de-los-protocolos-de.html
35. **WALC Workshop - Enrutamiento Avanzado.** (13 de 10 de 2011). Recuperado el 20 de 05 de 2015, de https://nsrc.org/workshops/2011/walc/routing/raw-attachment/wiki/Agenda/Intro_BGP.pdf

ANEXOS

Anexo A. CAPTURA DE TRÁFICO CON WIRESHARK

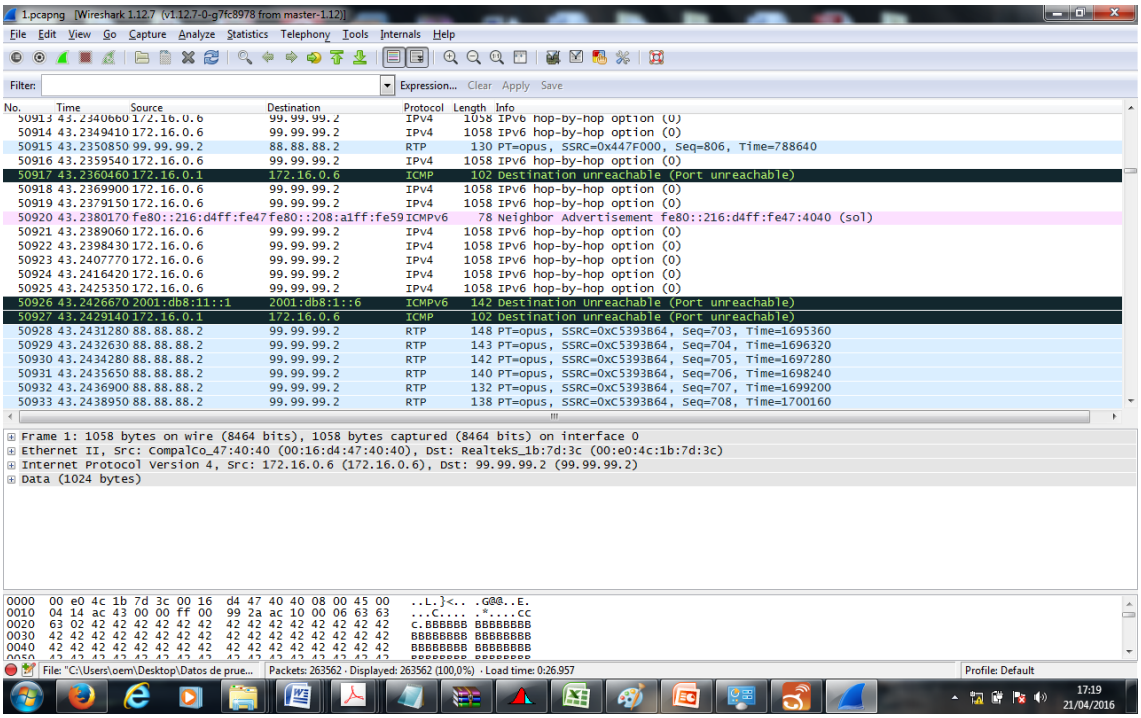
La captura de tráfico como ya se ha especificado ha sido de todos los paquetes transmitidos por los protocolos RTP y FTP, a través del mismo escenario planteado para todos los caso de análisis. Es así que se ha procedido a iniciar la generación de tráfico desde MAUSEZAHN instalado en PC6 (computador portátil) conectado directamente al HUB que permite la interconexión de sistema. De la misma manera conectado directamente al HUB se encuentra el PC5 que captura el tráfico que atraviesa la red gracias a WIRESHARK, conectado de esta manera para que pueda escuchar todos los datos transmitidos en la red. Las interacciones entre los host para la transmisión de datos PC88 y PC99 (computadores portátiles), se encuentran conectados a las interfaces ethernet de R1 y R4 respectivamente los cuales poseen dos interfaces físicas. Todos los routers se encuentran directamente conectados por medio físico al HUB. Antes de iniciar cada transmisión se ha ejecutado la captura de paquetes.

Para el análisis de RTP se debe considerar que, el mencionado no realiza un control de los paquetes transmitidos por lo cual no utiliza el protocolo TCP, al ser un protocolo para aplicaciones en tiempo real necesita mayora rapidez en la transmisión y no se centra en la pérdida de paquetes. Es por eso que utiliza el datagrama UDP que no realiza un control del orden de los paquetes enviados o del tiempo en el que estos se demoran en llegar al destino, dejando así que el receptor decida el orden correcto en el que se ordenan los paquetes al llegar. Esto asegura que la calidad de las aplicaciones de este tipo no experimenten problemas comunes como el retardo o interferencia.

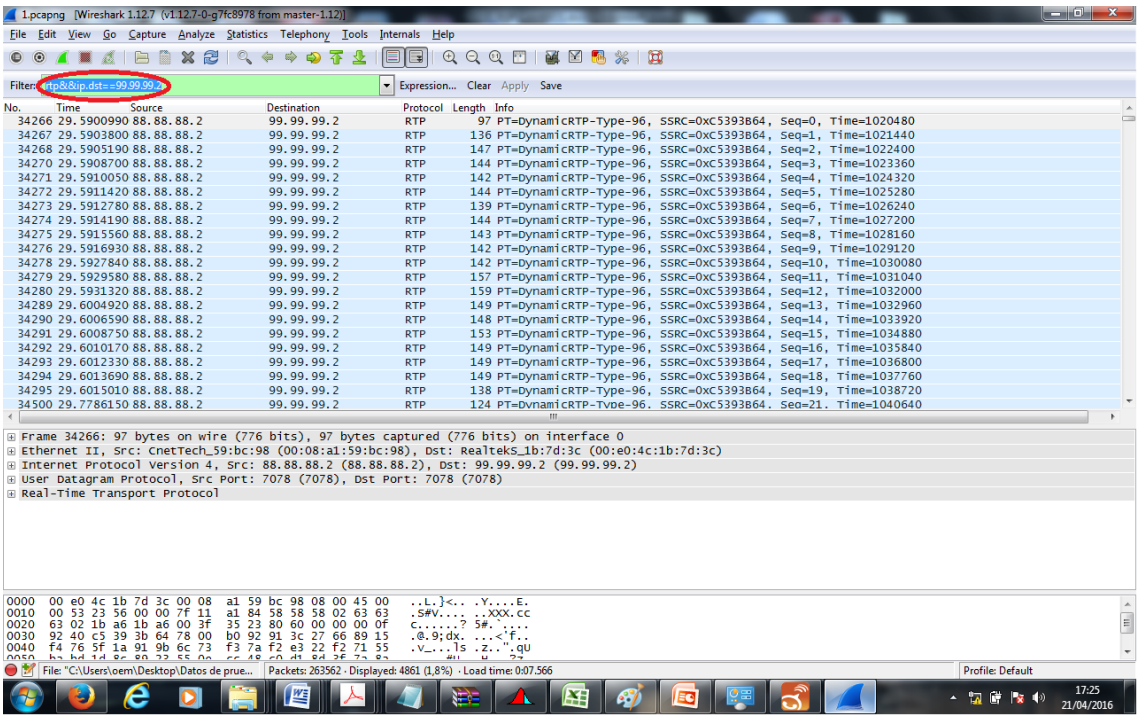
Por el contrario el protocolo de transmisión de archivos FTP, se focaliza en la transmisión eficaz de los paquetes enviados a través de una red TCP/IP. Al utilizar mecanismos de control resulta más viable en la entrega recepción de datos a través de una red. Como se explicó anteriormente el modelo FTP está relacionado con el modelo cliente servidor, facilitando la transmisión de archivos entre los equipos.

A continuación se detallan las capturas y los análisis realizados para RTP:

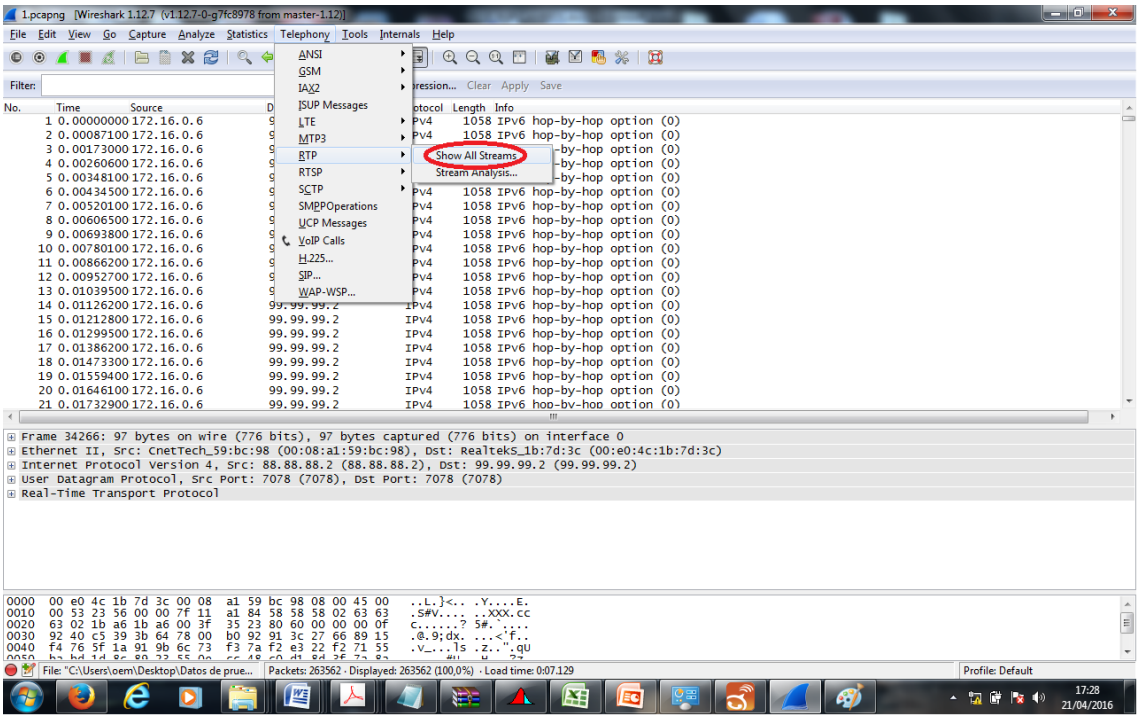
Todas las interacciones han sido realizadas en el mismo sentido la llamada se realiza desde el host conectado a R1 con la dirección 88.88.88.2 al host conectado a R4 con dirección 99.99.99.2. Se presenta las transmisiones más significativas para IPv4 e IPv6:



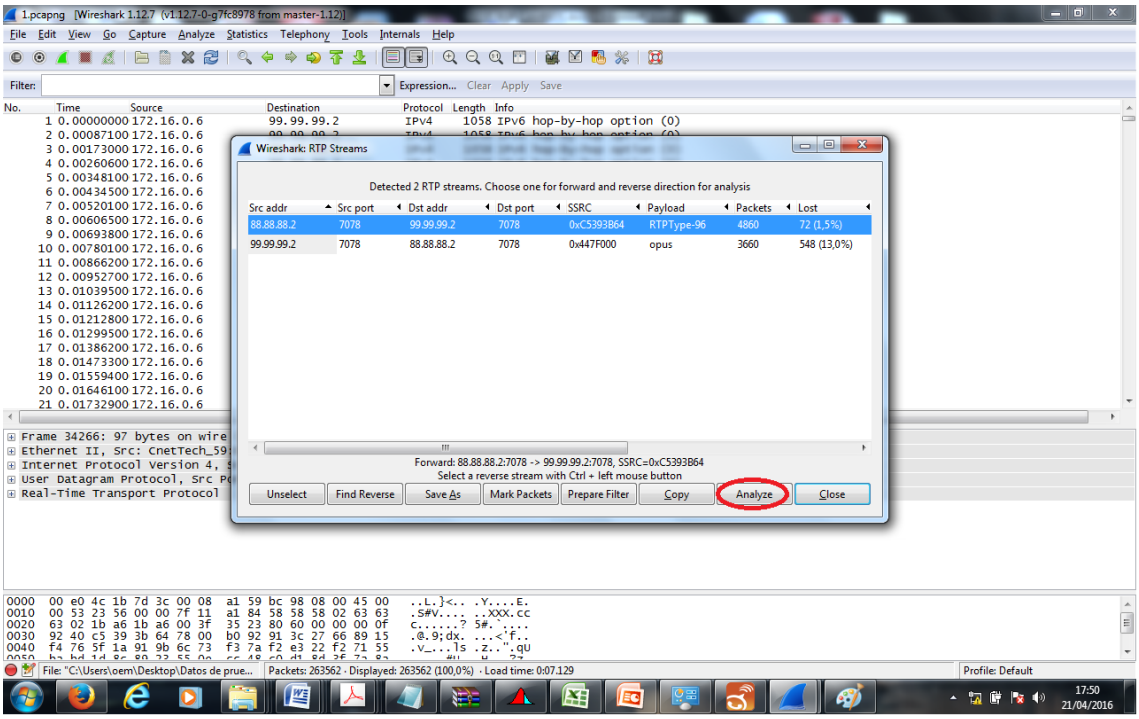
Como se puede ver en la figura, se registra el tráfico que atraviesa la red junto a los paquetes RTP. Se pueden utilizar filtros para poder seleccionar el tráfico requerido y diferenciarlo para su análisis. A continuación se muestra la captura obtenida mediante le filtro rtp&&ip.dst==99.99.99.2, que permite seleccionar todo el tráfico RTP que llega a la ip de destino 99.99.99.2. Para el caso de IPv6 se puede aplicar el filtro rtp&&ipv6.dst==2001:db8:44::2.



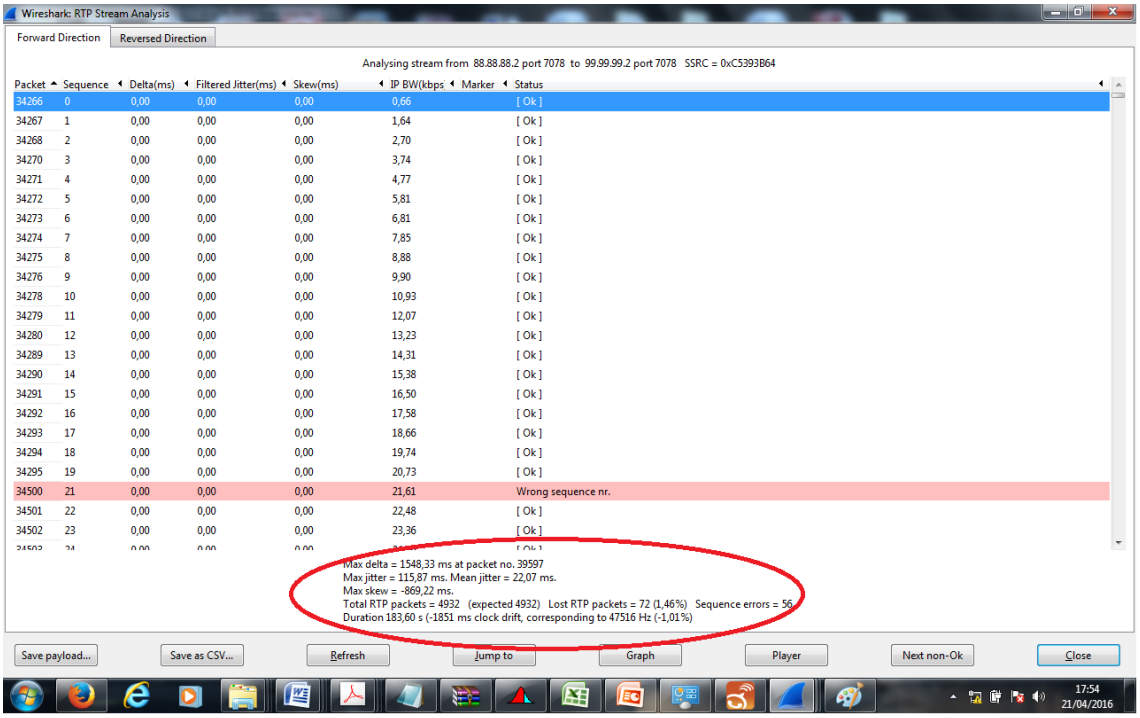
Para poder realizar el análisis del proyecto se ha procedido a utilizar una opción muy útil disponible en el analizador de tráfico accediendo por el menú TELEPHONY => RTP => SHOW ALL STREAMS.



Al seleccionar esta opción podemos acceder a la visualización de todo el tráfico RTP capturado.



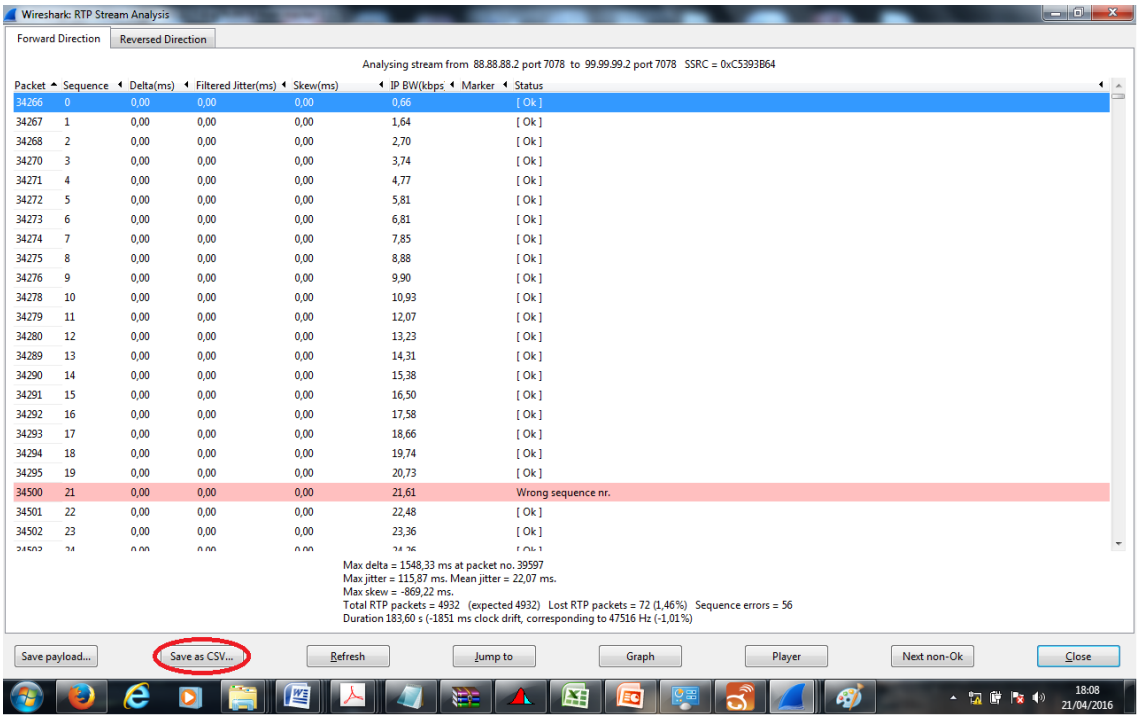
Seguidamente se procede a seleccionar el sentido del tráfico deseado para nuestro caso de 88.88.88.2 a 99.99.99.2 y presionamos el botón ANALYZE para poder ver el análisis de los paquetes para ese sentido de la transmisión del protocolo RTP como se muestra a continuación:



En la parte inferior podemos ver el resumen de lo más representativo de la captura de realizada para RTP en el sentido seleccionado, así:

Max delta = 1548,33 ms at packet no. 39597
Max jitter = 115,87 ms. Mean jitter = 22,07 ms.
Max skew = -869,22 ms.
Total RTP packets = 4932 (expected 4932) Lost RTP packets = 72 (1,46%) Sequence errors = 56
Duration 183,60 s (-1851 ms clock drift, corresponding to 47516 Hz (-1,01%)

Se puede observar los valores máximos de los indicadores principales a ser observados en el proyecto: Latencia máxima (Max delta), porcentaje de paquetes perdidos (Lost RTP packets) y el ancho de banda (IP BW) que puede ser calculado del promedio registrado durante el envío de todos los paquetes, para lo cual debemos proceder a exportar los datos de la captura a un archivo con extensión *.csv mediante el botón SAVE AS CSV, valores que pueden ser promediados en una hoja de cálculo.



Se muestra a continuación la tabla una de las capturas de RTP en IPV4 recuperado desde la hoja de cálculo, de los primeros 300 registros ya que se han obtenido 4860 fila de la captura escogida:

Packet Forward	Sequence	Time stamp	Delta (ms)	Jitter (ms)	Skew(ms)	IP BW (kbps)	Marker	Status
34266	0	1020480	0	0	0	0,66		[Ok]
34267	1	1021440	0	0	0	1,64		[Ok]
34268	2	1022400	0	0	0	2,7		[Ok]
34270	3	1023360	0	0	0	3,74		[Ok]
34271	4	1024320	0	0	0	4,77		[Ok]
34272	5	1025280	0	0	0	5,81		[Ok]
34273	6	1026240	0	0	0	6,81		[Ok]
34274	7	1027200	0	0	0	7,85		[Ok]
34275	8	1028160	0	0	0	8,88		[Ok]
34276	9	1029120	0	0	0	9,9		[Ok]
34278	10	1030080	0	0	0	10,93		[Ok]
34279	11	1031040	0	0	0	12,07		[Ok]
34280	12	1032000	0	0	0	13,23		[Ok]
34289	13	1032960	0	0	0	14,31		[Ok]
34290	14	1033920	0	0	0	15,38		[Ok]
34291	15	1034880	0	0	0	16,5		[Ok]
34292	16	1035840	0	0	0	17,58		[Ok]

34293	17	1036800	0	0	0	18,66		[Ok]
34294	18	1037760	0	0	0	19,74		[Ok]
34295	19	1038720	0	0	0	20,73		[Ok]
34500	21	1040640	0	0	0	21,61		Wrong sequence nr.
34501	22	1041600	0	0	0	22,48		[Ok]
34502	23	1042560	0	0	0	23,36		[Ok]
34503	24	1043520	0	0	0	24,26		[Ok]
34504	25	1044480	0	0	0	25,14		[Ok]
34505	26	1045440	0	0	0	26		[Ok]
34506	27	1046400	0	0	0	26,88		[Ok]
34507	28	1047360	0	0	0	27,81		[Ok]
34508	29	1048320	0	0	0	28,71		[Ok]
34509	30	1049280	0	0	0	29,61		[Ok]
34510	31	1050240	0	0	0	30,49		[Ok]
34511	32	1051200	0	0	0	31,41		[Ok]
34512	33	1052160	0	0	0	32,34		[Ok]
34513	34	1053120	0	0	0	33,3		[Ok]
34514	35	1054080	0	0	0	34,32		[Ok]
34515	36	1055040	0	0	0	35,41		[Ok]
34839	38	1056960	0	0	0	36,35		Wrong sequence nr.
34845	39	1057920	0	0	0	37,38		[Ok]
34846	40	1058880	0	0	0	38,47		[Ok]
34847	41	1059840	0	0	0	39,47		[Ok]
34848	42	1060800	0	0	0	40,45		[Ok]
34849	43	1061760	0	0	0	41,38		[Ok]
34850	44	1062720	0	0	0	42,46		[Ok]
34851	45	1063680	0	0	0	43,56		[Ok]
34852	46	1064640	0	0	0	44,67		[Ok]
34853	47	1065600	0	0	0	45,79		[Ok]
34854	48	1066560	0	0	0	46,93		[Ok]
34855	49	1067520	0	0	0	48,02		[Ok]
34856	50	1068480	0	0	0	49,12		[Ok]
34857	51	1069440	0	0	0	50,24		[Ok]
34889	52	1070400	0	0	0	51,38		[Ok]
35460	55	1073280	454	40,38	139,4	52,42		Wrong sequence nr.
36011	58	1076160	474,65	63,77	-275,2	17,91		Wrong sequence nr.
36013	59	1077120	1,04	60,97	-256,3	18,74		[Ok]
36014	60	1078080	0,19	58,39	-236,5	19,61		[Ok]
36015	61	1079040	0,15	55,99	-216,6	20,48		[Ok]
36016	62	1080000	0,15	53,73	-196,8	21,39		[Ok]
36017	63	1080960	0,15	51,61	-176,9	22,46		[Ok]
36018	64	1081920	0,14	49,63	-157	23,58		[Ok]
36019	65	1082880	0,16	47,76	-137,2	24,62		[Ok]

36020	66	1083840	0,14	46,02	-117,4	25,72		[Ok]
36021	67	1084800	0,14	44,38	-97,5	26,8		[Ok]
36023	68	1085760	0,39	42,84	-77,89	27,92		[Ok]
36024	69	1086720	0,15	41,4	-58,04	29,04		[Ok]
36025	70	1087680	0,14	40,05	-38,18	30,1		[Ok]
36026	71	1088640	0,22	38,79	-18,4	31,21		[Ok]
36027	72	1089600	0,16	37,6	1,44	32,25		[Ok]
36028	73	1090560	0,14	36,49	21,31	33,28		[Ok]
36029	74	1091520	0,14	35,45	41,17	34,32		[Ok]
36030	75	1092480	0,14	34,48	61,03	35,37		[Ok]
36031	76	1093440	0,14	33,57	80,89	36,44		[Ok]
36032	77	1094400	0,14	32,71	100,7	37,54		[Ok]
36033	78	1095360	0,14	31,91	120,6	38,57		[Ok]
36034	79	1096320	0,13	31,15	140,5	39,56		[Ok]
36036	80	1097280	0,36	30,43	160,1	40,54		[Ok]
36037	81	1098240	0,14	29,77	180	41,5		[Ok]
36038	82	1099200	0,13	29,15	199,8	42,48		[Ok]
36039	83	1100160	0,12	28,57	219,7	43,31		[Ok]
36040	84	1101120	0,12	28,03	239,6	44,14		[Ok]
36041	85	1102080	0,14	27,52	259,5	45,14		[Ok]
36042	86	1103040	0,14	27,04	279,3	46,22		[Ok]
36043	87	1104000	0,14	26,59	299,2	47,21		[Ok]
36044	88	1104960	0,14	26,17	319,1	48,25		[Ok]
36045	89	1105920	0,13	25,78	338,9	49,26		[Ok]
36046	90	1106880	0,21	25,4	358,7	50,28		[Ok]
36047	91	1107840	0,14	25,06	378,6	51,3		[Ok]
36048	92	1108800	0,14	24,73	398,4	52,35		[Ok]
36049	93	1109760	0,14	24,43	418,3	53,35		[Ok]
36050	94	1110720	0,13	24,14	438,2	54,3		[Ok]
36051	95	1111680	0,13	23,88	458,1	55,23		[Ok]
36052	96	1112640	0,13	23,63	477,9	56,19		[Ok]
36053	97	1113600	0,13	23,39	497,8	57,2		[Ok]
36054	98	1114560	0,14	23,17	517,6	58,22		[Ok]
36055	99	1115520	0,14	22,96	537,5	59,26		[Ok]
36367	101	1117440	265,72	35,64	311,8	44,41		Wrong sequence nr.
36368	102	1118400	0,22	34,65	331,6	45,52		[Ok]
36369	103	1119360	0,22	33,72	351,4	46,58		[Ok]
36370	104	1120320	0,14	32,85	371,2	47,63		[Ok]
36371	105	1121280	0,16	32,04	391,1	48,67		[Ok]
36372	106	1122240	0,13	31,28	410,9	49,66		[Ok]
36373	107	1123200	0,16	30,56	430,8	50,68		[Ok]
36374	108	1124160	0,14	29,89	450,6	51,71		[Ok]
36375	109	1125120	0,13	29,27	470,5	52,73		[Ok]
36376	110	1126080	0,13	28,68	490,4	53,73		[Ok]

36377	111	1127040	0,13	28,13	510,2	54,72		[Ok]
36378	112	1128000	0,13	27,61	530,1	55,66		[Ok]
36397	113	1128960	16,04	26,13	534	56,67		[Ok]
36421	114	1129920	20,19	24,51	533,9	57,7		[Ok]
36433	115	1130880	9,75	23,62	544,1	58,68		[Ok]
36760	117	1132800	274,86	36,82	309,2	58,66		Wrong sequence nr.
36762	118	1133760	1,12	35,7	328,1	59,7		[Ok]
36763	119	1134720	0,16	34,71	348	60,7		[Ok]
36764	120	1135680	0,13	33,78	367,8	61,68		[Ok]
36765	121	1136640	0,16	32,91	387,7	62,69		[Ok]
36766	122	1137600	0,13	32,1	407,6	63,62		[Ok]
36767	123	1138560	0,13	31,33	427,4	64,42		[Ok]
36769	124	1139520	0,19	30,61	447,2	65,24		[Ok]
36770	125	1140480	0,19	29,94	467	66,14		[Ok]
36771	126	1141440	0,14	29,31	486,9	67,2		[Ok]
36772	127	1142400	0,15	28,72	506,7	68,36		[Ok]
36773	128	1143360	0,14	28,16	526,6	69,38		[Ok]
36786	129	1144320	13,07	26,84	533,5	70,38		[Ok]
37250	131	1146240	398,32	47,55	175,2	29,13		Wrong sequence nr.
37251	132	1147200	0,21	45,82	195	30,17		[Ok]
37252	133	1148160	0,16	44,19	214,8	31,16		[Ok]
37254	134	1149120	0,29	42,66	234,5	32,13		[Ok]
37255	135	1150080	0,21	41,23	254,3	33,12		[Ok]
37256	136	1151040	0,14	39,9	274,2	34,22		[Ok]
37257	137	1152000	0,14	38,65	294,1	35,2		[Ok]
37258	138	1152960	0,14	37,47	313,9	36,21		[Ok]
37259	139	1153920	0,14	36,37	333,8	37,28		[Ok]
37260	140	1154880	0,2	35,34	353,6	38,27		[Ok]
37261	141	1155840	0,14	34,37	373,5	39,27		[Ok]
37262	142	1156800	0,14	33,46	393,3	40,3		[Ok]
37263	143	1157760	0,14	32,61	413,2	41,34		[Ok]
37264	144	1158720	0,14	31,82	433	42,42		[Ok]
37265	145	1159680	0,13	31,07	452,9	43,38		[Ok]
37266	146	1160640	0,21	30,36	472,7	44,42		[Ok]
37267	147	1161600	0,13	29,71	492,6	45,44		[Ok]
37268	148	1162560	0,14	29,09	512,4	46,54		[Ok]
37269	149	1163520	0,14	28,51	532,3	47,59		[Ok]
37502	151	1165440	202,26	36,87	370	48,62		Wrong sequence nr.
37503	152	1166400	0,2	35,81	389,8	49,64		[Ok]
37504	153	1167360	0,21	34,81	409,6	50,66		[Ok]
37505	154	1168320	0,16	33,87	429,4	51,66		[Ok]
37506	155	1169280	0,13	33	449,3	52,62		[Ok]
37507	156	1170240	0,11	32,18	469,2	53,42		[Ok]
37508	157	1171200	0,12	31,41	489,1	54,22		[Ok]

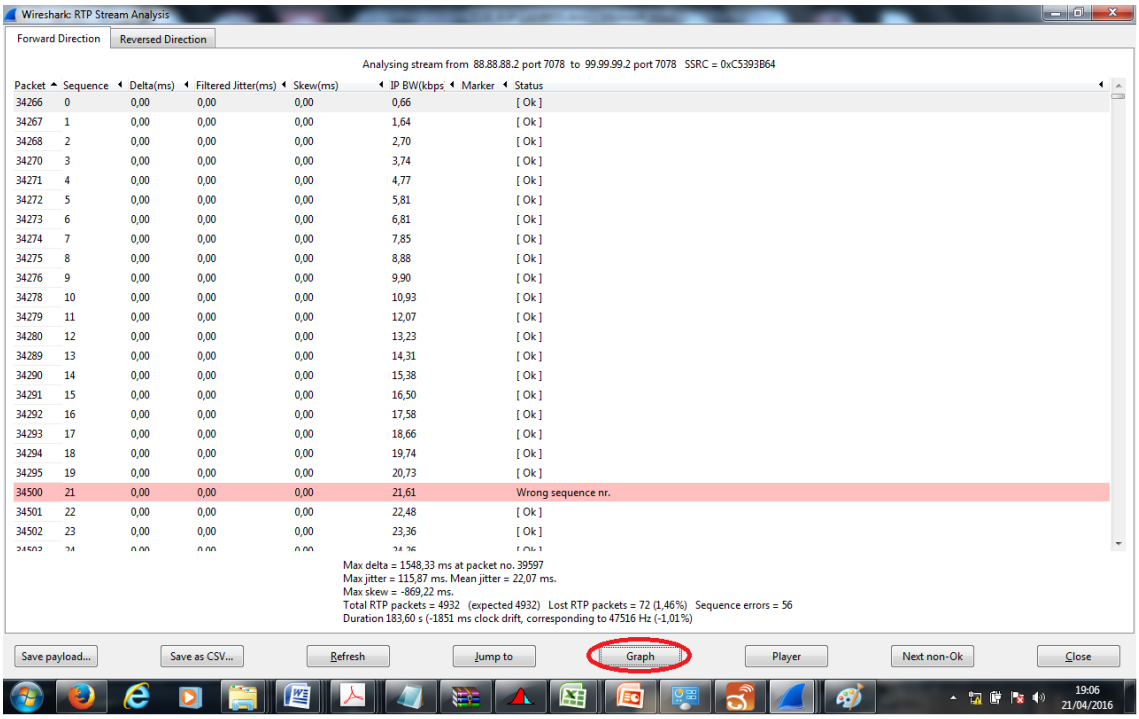
37509	158	1172160	0,19	30,68	508,9	55,05		[Ok]
37510	159	1173120	0,12	30,01	528,8	55,88		[Ok]
37772	161	1175040	208,05	38,64	360,7	41,36		Wrong sequence nr.
37773	162	1176000	0,14	37,46	380,6	42,18		[Ok]
37774	163	1176960	0,12	36,36	400,5	43,02		[Ok]
37775	164	1177920	0,19	35,33	420,3	43,91		[Ok]
37776	165	1178880	0,19	34,36	440,1	44,78		[Ok]
37779	166	1179840	0,42	33,44	459,7	45,7		[Ok]
37780	167	1180800	0,19	32,58	479,5	46,62		[Ok]
37781	168	1181760	0,15	31,79	499,3	47,51		[Ok]
37783	169	1182720	0,21	31,04	519,1	48,39		[Ok]
39597	177	1190400	1548,33	115,87	-869,2	1,05		Wrong sequence nr.
39598	178	1191360	0,29	109,86	-849,5	2,11		[Ok]
39599	179	1192320	0,13	104,23	-829,6	3,14		[Ok]
39600	180	1193280	0,17	98,96	-809,8	4,18		[Ok]
39601	181	1194240	0,14	94,02	-790	5,23		[Ok]
39602	182	1195200	0,14	89,38	-770,1	6,26		[Ok]
39603	183	1196160	0,13	85,04	-750,2	7,3		[Ok]
39604	184	1197120	0,21	80,96	-730,4	8,34		[Ok]
39605	185	1198080	0,14	77,14	-710,6	9,35		[Ok]
39606	186	1199040	0,14	73,56	-690,7	10,38		[Ok]
39607	187	1200000	0,14	70,2	-670,8	11,41		[Ok]
39608	188	1200960	0,17	67,06	-651	12,47		[Ok]
39609	189	1201920	0,14	64,11	-631,2	13,54		[Ok]
39610	190	1202880	0,15	61,34	-611,3	14,66		[Ok]
39611	191	1203840	0,14	58,75	-591,4	15,73		[Ok]
39612	192	1204800	0,14	56,32	-571,6	16,8		[Ok]
39613	193	1205760	0,14	54,04	-551,7	17,86		[Ok]
39614	194	1206720	0,14	51,9	-531,9	18,89		[Ok]
39615	195	1207680	0,13	49,9	-512	19,85		[Ok]
39616	196	1208640	0,14	48,02	-492,1	20,9		[Ok]
39617	197	1209600	0,13	46,26	-472,3	21,91		[Ok]
39624	198	1210560	0,96	44,56	-453,2	22,83		[Ok]
39625	199	1211520	0,12	43,02	-433,4	23,68		[Ok]
39626	200	1212480	0,14	41,57	-413,5	24,7		[Ok]
39627	201	1213440	0,14	40,21	-393,6	25,72		[Ok]
39628	202	1214400	0,13	38,94	-373,8	26,66		[Ok]
39629	203	1215360	0,12	37,75	-353,9	27,54		[Ok]
39630	204	1216320	0,12	36,63	-334	28,42		[Ok]
39631	205	1217280	0,12	35,59	-314,1	29,31		[Ok]
39632	206	1218240	0,13	34,6	-294,3	30,26		[Ok]
39633	207	1219200	0,14	33,68	-274,4	31,32		[Ok]
39634	208	1220160	0,13	32,82	-254,5	32,25		[Ok]
39635	209	1221120	0,13	32,01	-234,7	33,19		[Ok]

39636	210	1222080	0,14	31,25	-214,8	34,22		[Ok]
39637	211	1223040	0,12	30,54	-194,9	35,1		[Ok]
39638	212	1224000	0,13	29,87	-175	36		[Ok]
39639	213	1224960	0,12	29,25	-155,2	36,9		[Ok]
39640	214	1225920	0,12	28,66	-135,3	37,78		[Ok]
39641	215	1226880	0,13	28,11	-115,4	38,69		[Ok]
39642	216	1227840	0,12	27,6	-95,53	39,58		[Ok]
39643	217	1228800	0,13	27,12	-75,66	40,5		[Ok]
39644	218	1229760	0,16	26,66	-55,82	41,48		[Ok]
39645	219	1230720	0,16	26,24	-35,97	42,65		[Ok]
39646	220	1231680	0,15	25,84	-16,13	43,85		[Ok]
39647	221	1232640	0,15	25,46	3,72	44,99		[Ok]
39648	222	1233600	0,15	25,11	23,58	46,11		[Ok]
39649	223	1234560	0,14	24,78	43,44	47,17		[Ok]
39650	224	1235520	0,14	24,48	63,3	48,21		[Ok]
39651	225	1236480	0,14	24,19	83,15	49,33		[Ok]
39652	226	1237440	0,15	23,92	103	50,47		[Ok]
39653	227	1238400	0,18	23,66	122,8	51,67		[Ok]
39654	228	1239360	0,12	23,42	142,7	52,78		[Ok]
39655	229	1240320	0,14	23,2	162,6	53,82		[Ok]
39656	230	1241280	0,15	22,99	182,4	54,91		[Ok]
39657	231	1242240	0,14	22,8	202,3	56,02		[Ok]
39658	232	1243200	0,15	22,61	222,1	57,09		[Ok]
39659	233	1244160	0,14	22,44	242	58,14		[Ok]
39660	234	1245120	0,14	22,28	261,9	59,14		[Ok]
39661	235	1246080	0,13	22,13	281,7	60,13		[Ok]
39662	236	1247040	0,14	21,99	301,6	61,12		[Ok]
39663	237	1248000	0,11	21,86	321,5	61,9		[Ok]
39664	238	1248960	0,12	21,73	341,4	62,76		[Ok]
39665	239	1249920	0,12	21,62	361,2	63,59		[Ok]
39666	240	1250880	0,13	21,51	381,1	64,48		[Ok]
39667	241	1251840	0,12	21,41	401	65,36		[Ok]
39668	242	1252800	0,12	21,31	420,9	66,23		[Ok]
39669	243	1253760	0,12	21,22	440,8	67,09		[Ok]
39670	244	1254720	0,12	21,14	460,6	67,96		[Ok]
39671	245	1255680	0,12	21,06	480,5	68,78		[Ok]
39672	246	1256640	0,12	20,98	500,4	69,66		[Ok]
39673	247	1257600	0,12	20,92	520,3	70,52		[Ok]
40515	251	1261440	702,73	58,53	-102,5	71,48		Wrong sequence nr.
40516	252	1262400	0,17	56,11	-82,63	72,53		[Ok]
40517	253	1263360	0,17	53,84	-62,8	73,69		[Ok]
40519	254	1264320	0,29	51,71	-43,09	74,8		[Ok]
40520	255	1265280	0,14	49,72	-23,23	75,91		[Ok]
40521	256	1266240	0,14	47,85	-3,38	76,98		[Ok]

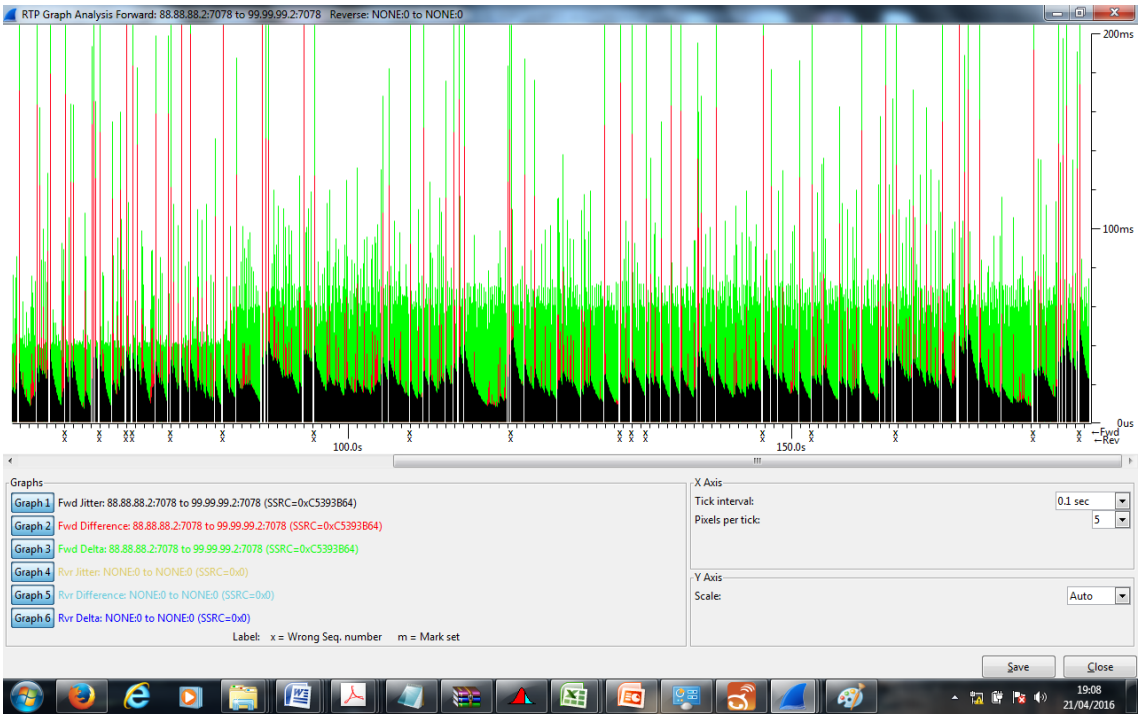
40522	257	1267200	0,14	46,1	16,48	78,04		[Ok]
40523	258	1268160	0,14	44,46	36,35	79,06		[Ok]
40524	259	1269120	0,14	42,93	56,21	80,11		[Ok]
40525	260	1270080	0,15	41,48	76,06	81,22		[Ok]
40526	261	1271040	0,15	40,13	95,91	82,35		[Ok]
40527	262	1272000	0,14	38,86	115,8	83,4		[Ok]
40528	263	1272960	0,17	37,67	135,6	84,47		[Ok]
40529	264	1273920	0,14	36,56	155,5	85,54		[Ok]
40530	265	1274880	0,14	35,52	175,3	86,64		[Ok]
40531	266	1275840	0,14	34,54	195,2	87,74		[Ok]
40532	267	1276800	0,15	33,62	215	88,87		[Ok]
40533	268	1277760	0,14	32,76	234,9	89,98		[Ok]
40534	269	1278720	0,14	31,95	254,7	91,06		[Ok]
40535	270	1279680	0,14	31,2	274,6	92,1		[Ok]
40536	271	1280640	0,14	30,49	294,5	93,11		[Ok]
40537	272	1281600	0,13	29,83	314,3	94,12		[Ok]
40538	273	1282560	0,13	29,2	334,2	95,07		[Ok]
40539	274	1283520	0,13	28,62	354,1	96,06		[Ok]
40540	275	1284480	0,13	28,07	373,9	97,05		[Ok]
40541	276	1285440	0,13	27,56	393,8	98,02		[Ok]
40542	277	1286400	0,2	27,07	413,6	99		[Ok]
40543	278	1287360	0,13	26,62	433,5	99,94		[Ok]
40544	279	1288320	0,12	26,2	453,4	100,79		[Ok]
40545	280	1289280	0,12	25,81	473,2	101,62		[Ok]
40546	281	1290240	0,12	25,44	493,1	102,52		[Ok]
40547	282	1291200	0,12	25,09	513	103,38		[Ok]
40548	283	1292160	0,12	24,76	532,9	104,24		[Ok]
40569	284	1293120	18,98	23,28	533,9	105,11		[Ok]
41408	288	1296960	712,46	61,35	-98,56	35,46		Wrong sequence nr.
41730	290	1298880	265,48	71,61	-324	25,66		Wrong sequence nr.
41731	291	1299840	0,28	68,37	-304,3	24,44		[Ok]
41732	292	1300800	0,29	65,33	-284,6	23,43		[Ok]
41733	293	1301760	0,14	62,49	-264,8	23,44		[Ok]
41734	294	1302720	0,15	59,82	-244,9	23,47		[Ok]
41735	295	1303680	0,14	57,32	-225,1	23,43		[Ok]
41736	296	1304640	0,14	54,98	-205,2	23,38		[Ok]
41737	297	1305600	0,13	52,79	-185,3	23,31		[Ok]
41738	298	1306560	0,14	50,73	-165,5	23,29		[Ok]
41739	299	1307520	0,21	48,79	-145,7	22,33		[Ok]
41740	300	1308480	0,14	46,99	-125,8	22,46		[Ok]
41741	301	1309440	0,14	45,29	-106	22,52		[Ok]
41742	302	1310400	0,14	43,7	-86,1	22,57		[Ok]
41743	303	1311360	0,13	42,21	-66,23	22,62		[Ok]
41744	304	1312320	0,13	40,82	-46,37	23,6		[Ok]

41745	305	1313280	0,14	39,51	-26,51	23,65		[Ok]
41746	306	1314240	0,14	38,28	-6,65	22,93		[Ok]
41747	307	1315200	0,14	37,13	13,2	23,19		[Ok]
41748	308	1316160	0,14	36,05	33,06	23,38		[Ok]
41749	309	1317120	0,14	35,04	52,92	23,58		[Ok]
41750	310	1318080	0,14	34,09	72,78	23,74		[Ok]
41751	311	1319040	0,16	33,2	92,62	24,74		[Ok]
41752	312	1320000	0,13	32,36	112,5	25,7		[Ok]
41753	313	1320960	0,14	31,58	132,4	26,7		[Ok]
41754	314	1321920	0,13	30,85	152,2	27,7		[Ok]
41755	315	1322880	0,14	30,16	172,1	28,73		[Ok]
41756	316	1323840	0,14	29,52	192	29,8		[Ok]
41757	317	1324800	0,14	28,92	211,8	30,84		[Ok]
41758	318	1325760	0,13	28,35	231,7	31,76		[Ok]
41759	319	1326720	0,12	27,82	251,6	32,59		[Ok]
41760	320	1327680	0,12	27,33	271,5	33,43		[Ok]
41761	321	1328640	0,13	26,86	291,3	34,4		[Ok]
41762	322	1329600	0,14	26,42	311,2	35,5		[Ok]
41763	323	1330560	0,14	26,01	331	36,57		[Ok]
41764	324	1331520	0,14	25,63	350,9	37,62		[Ok]

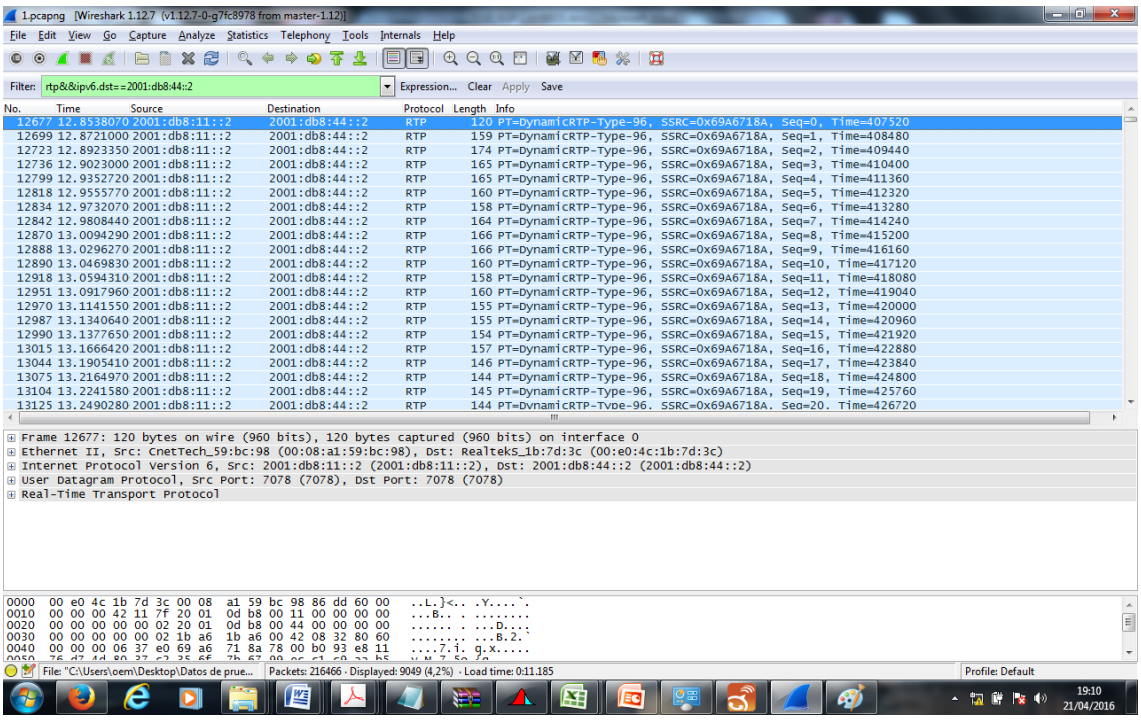
De igual manera podemos generar un gráfico de análisis de los indicadores contenidos en la captura al presionar el botón GRAPH

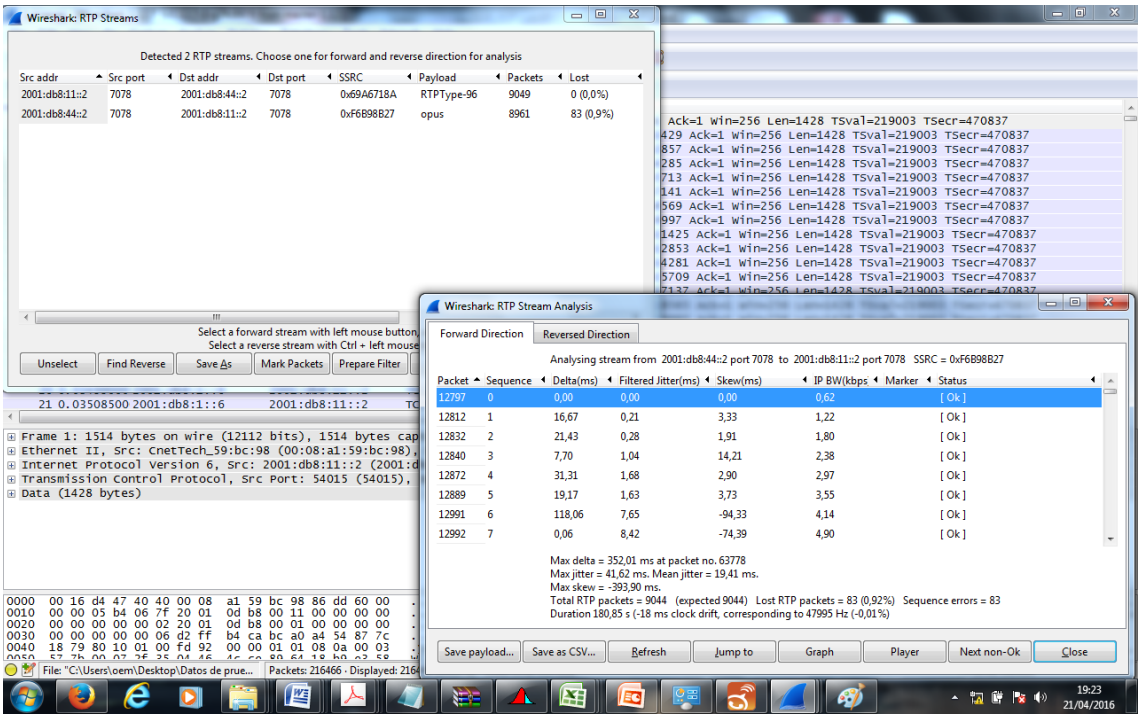


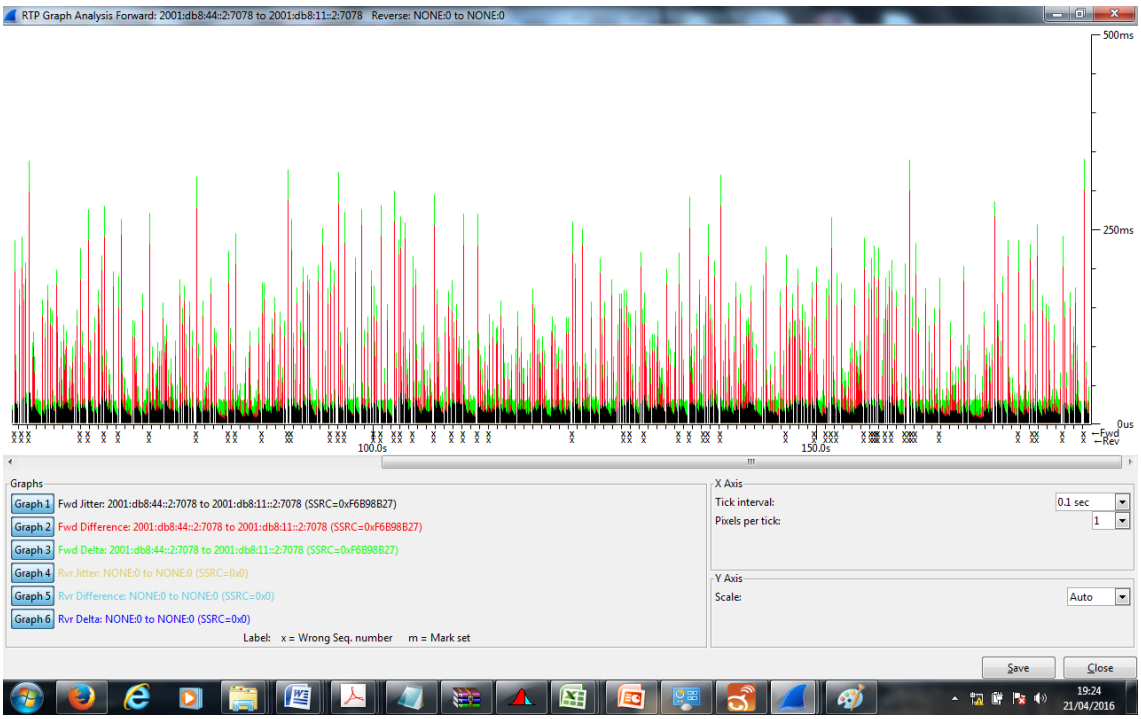
Se pueden obtener las comparaciones gráficas de lo indicado anteriormente:



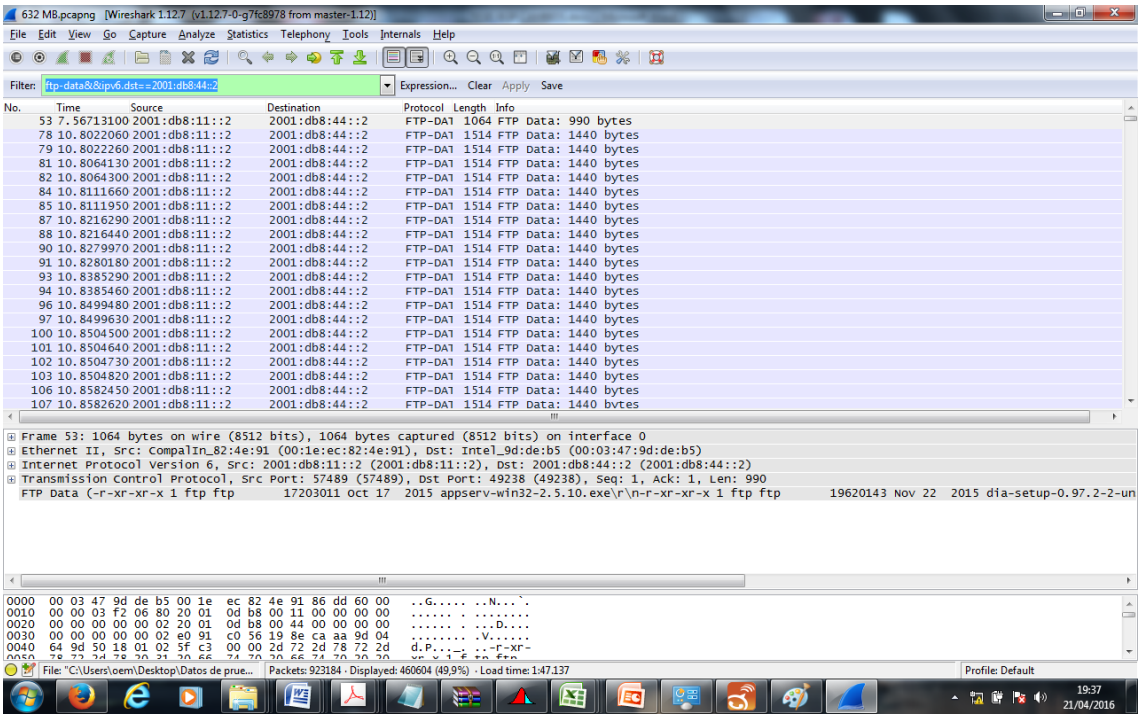
Para IPv6 el procedimiento es el mismo, se muestra a continuación las pantallas de una de las capturas realizadas:



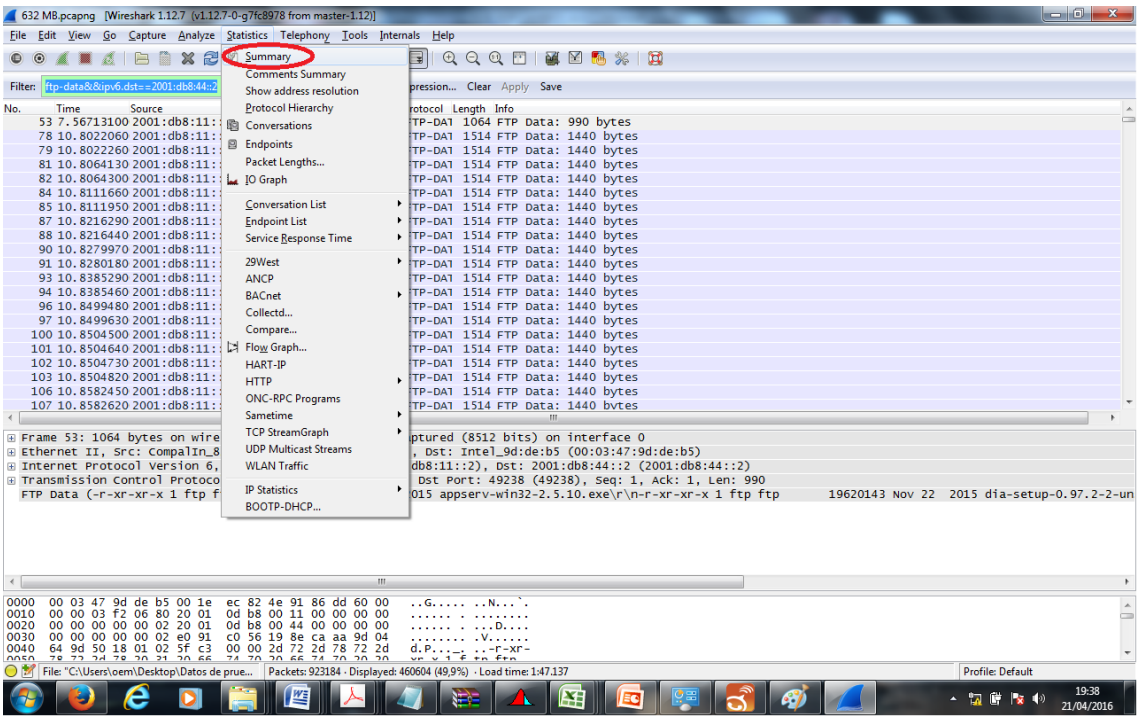


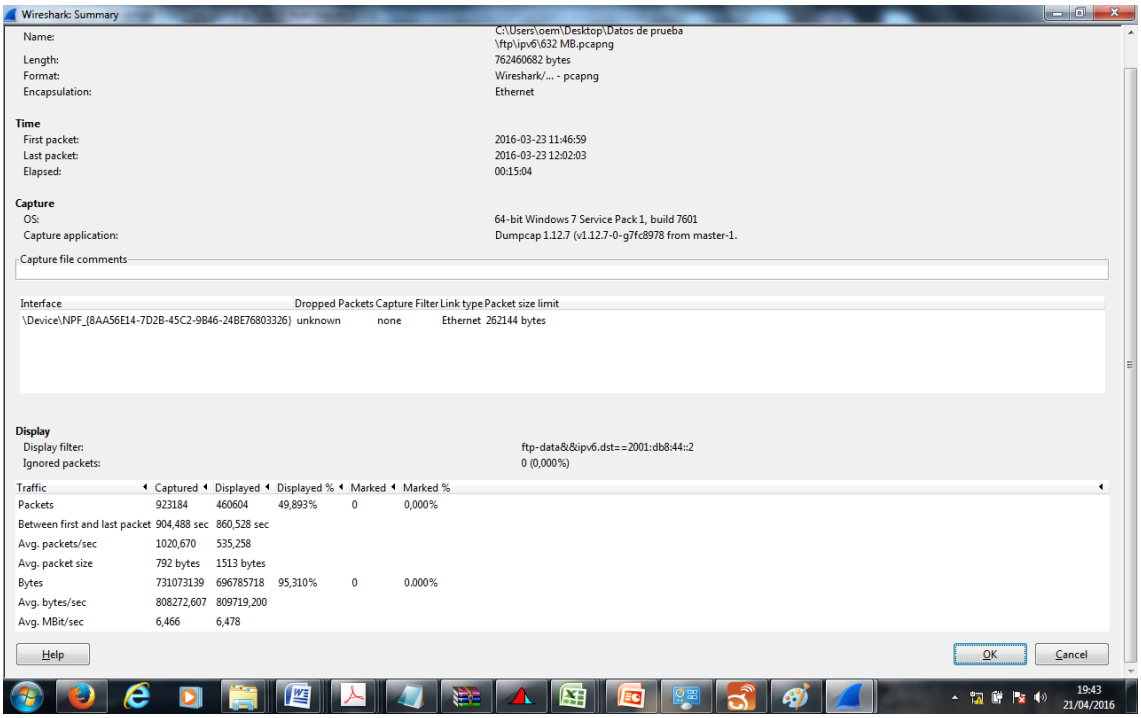


El análisis de paquetes FTP difiere debido a que no existe una característica de WIRESHARK que permita retomar los datos resumidos del protocolo como en el caso de RTP. Como se había indicado anteriormente mediante el filtro ftp-data&&ipv6.dst==2001:db8:44::2 o en el caso de IPv4 ftp-data&&ip.dst==99.99.99.2.



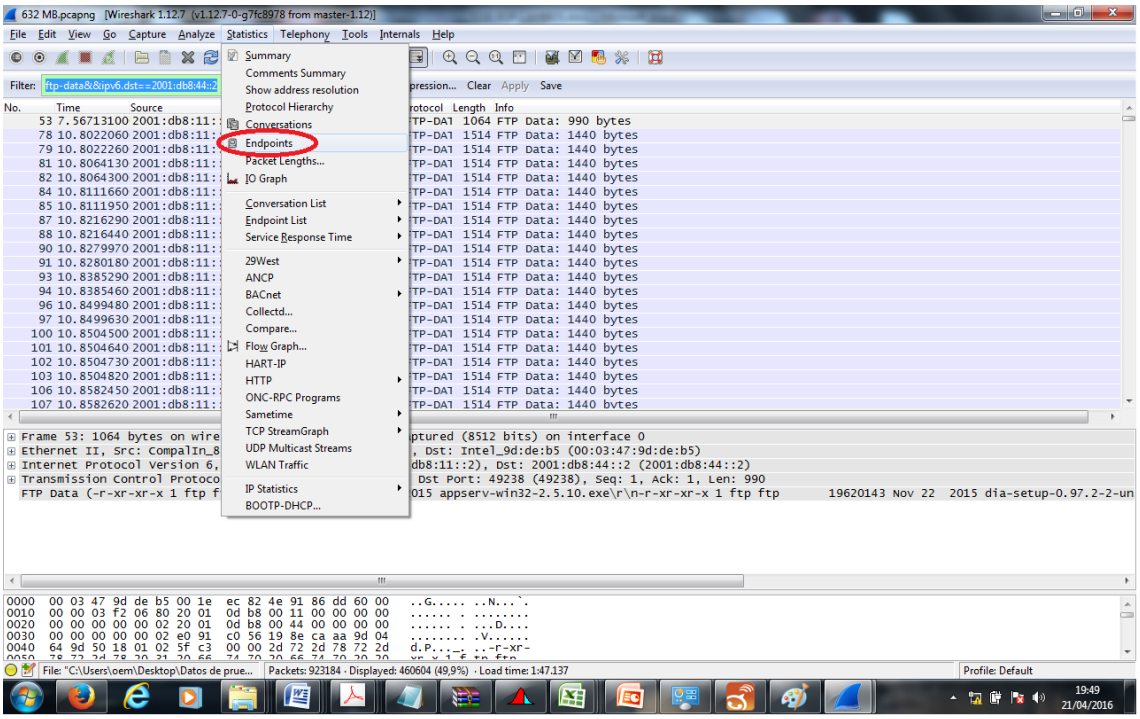
Entrando al menú STATICS => SUMMARY podemos visualizar el resumen del tráfico seleccionado con los parámetros más relevantes para el presente análisis:

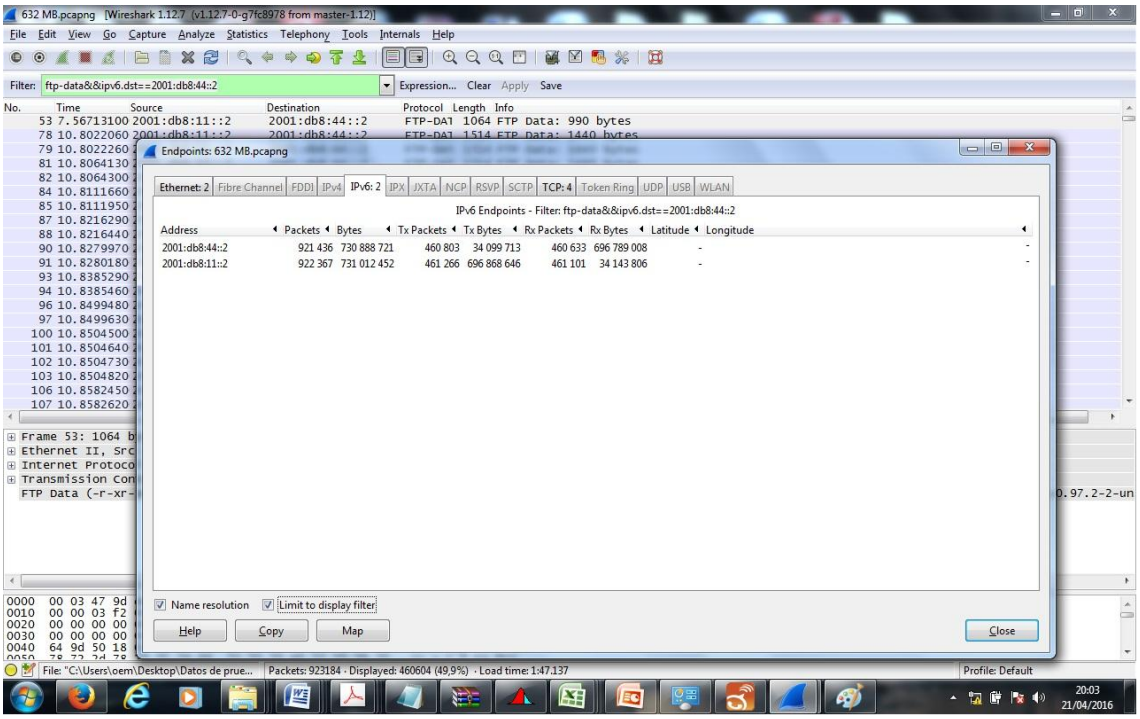




Se pueden obtener de esta manera, el total de paquetes transmitidos, el tiempo total de transmisión entre el primer y el último paquete, cantidad promedio de paquetes enviados y el ancho de banda promedio de la transmisión entre otros datos.

Accediendo al menú STATICS => ENDPOINTS podemos observar la cantidad de paquetes enviados y recibidos para el protocolo mediante el filtro de esta manera se pueden definir la cantidad de paquetes enviados y recibidos en el sentido seleccionado.

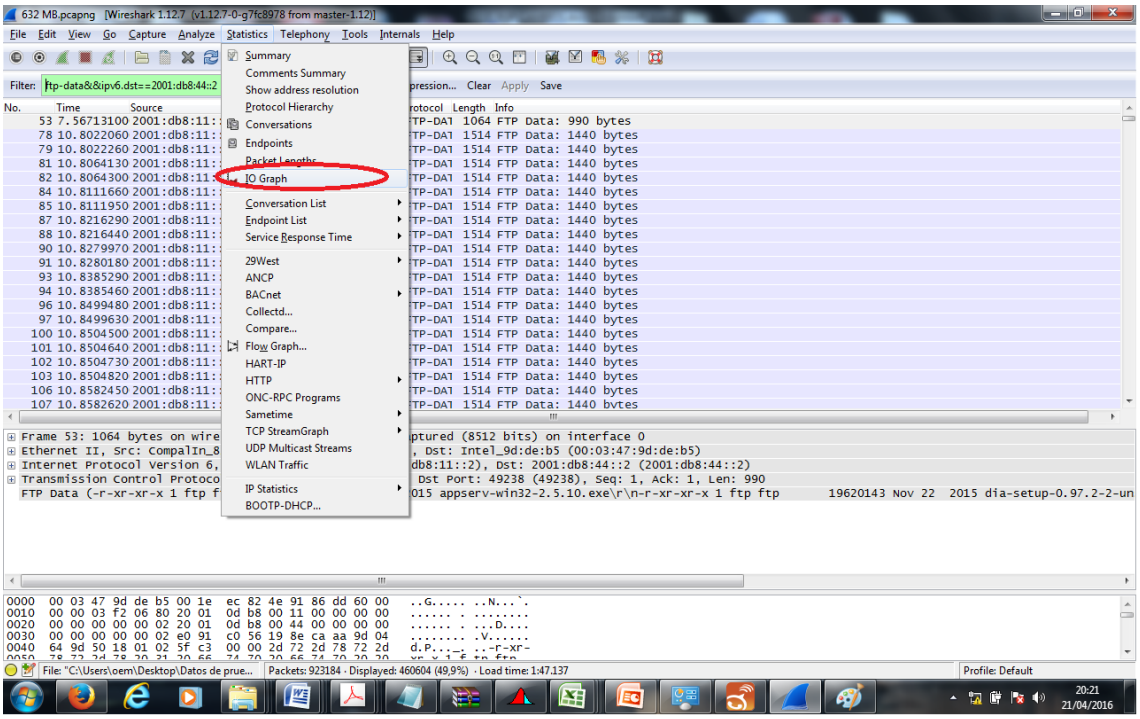




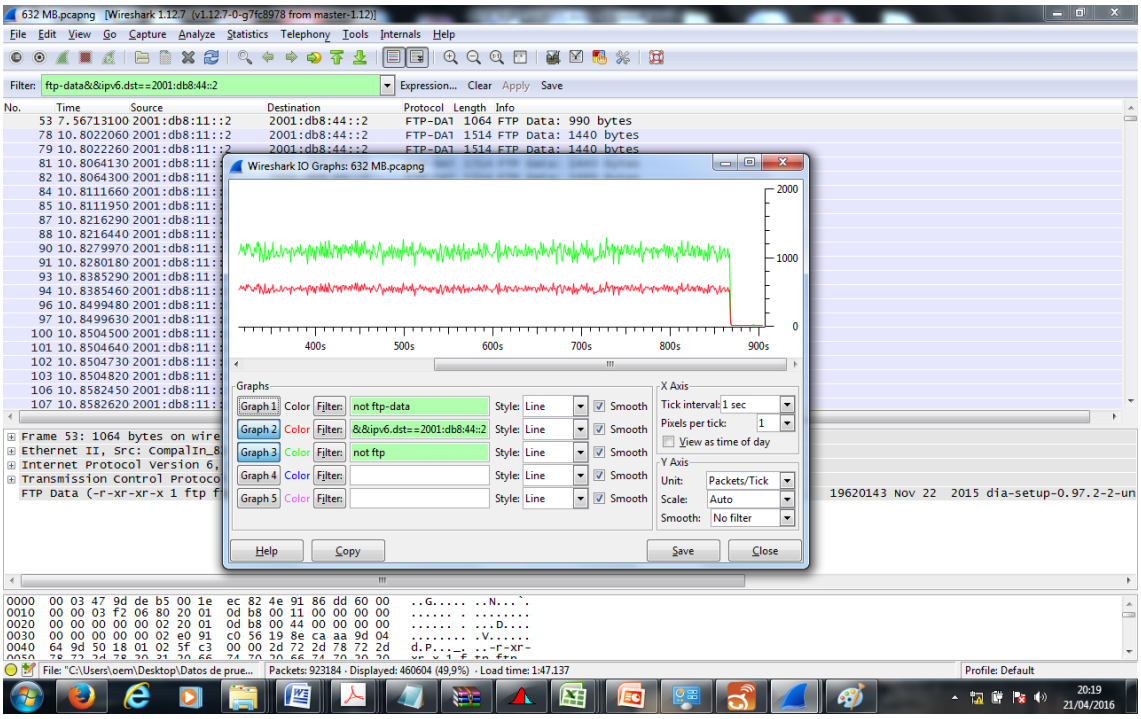
De esta manera se puede determinar el total de paquetes transmitidos y recibidos de origen a destino, a partir del filtro seleccionado.

Con estos parámetros se puede calcular los datos requeridos para la investigación, realizando los cálculos requeridos en una hoja de cálculo.

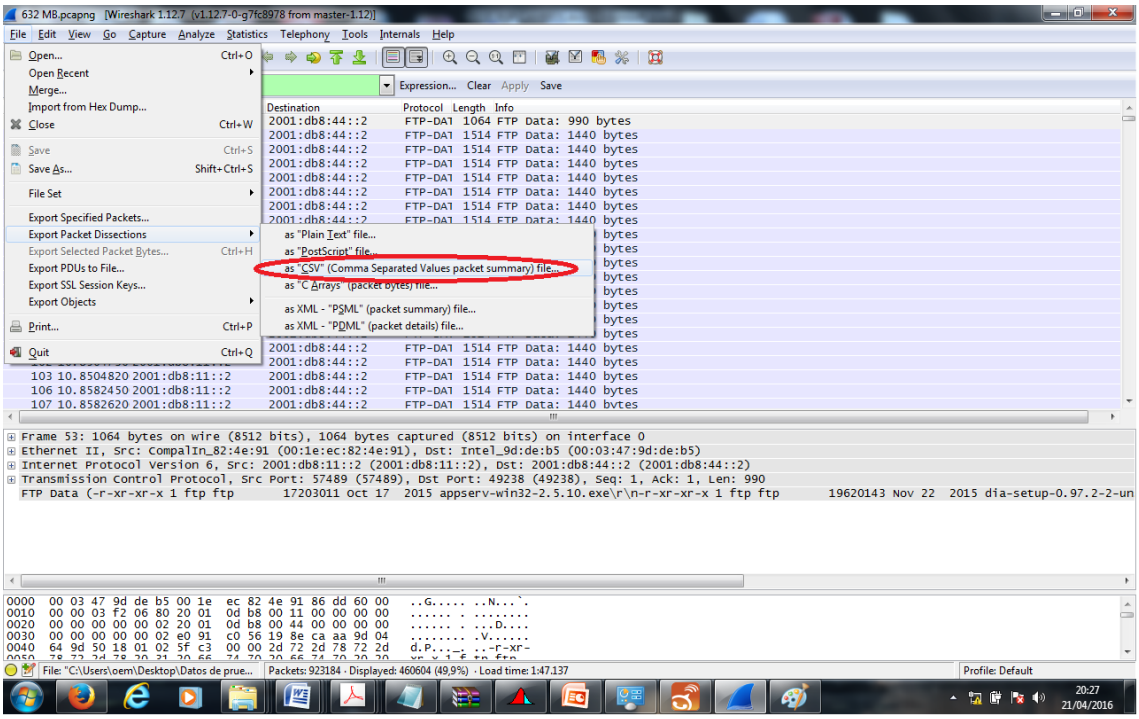
Al seleccionar el menú STATICS => IO GRAPH se puede acceder a la visualización gráfica de los paquetes transmitidos y mediante criterios de filtrado se pueden mostrar representaciones con colores del análisis realizado.



Para poder generar el gráfico de la transmisión de paquetes FTP se han seleccionado los filtros indicados: &&ipv6.dst==2001:db8:44::2, not ftp-data, not ftp



Finalmente podemos guardar la porción de paquetes seleccionados de acuerdo al criterio de filtrado ingresado, para lo cual se debe ingresar al menú FILE => EXPORT PACKETS DISSECTIONS y se puede escoger entre otras un archivo plano de texto en formato *.csv:



A continuación se muestran los primero 300 registros de 460604 filas de la captura realizada para la trasmisión de paquetes FTP:

No.	Time	Source	Destination	Protocol	Length	Info
53	7.567.131.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1064	FTP Data: 990 bytes
78	10.802.206.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
79	10.802.226.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
81	10.806.413.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
82	10.806.430.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
84	10.811.166.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
85	10.811.195.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
87	10.821.629.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
88	10.821.644.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
90	10.827.997.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
91	10.828.018.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
93	10.838.529.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
94	10.838.546.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
96	10.849.948.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
97	10.849.963.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
100	10.850.450.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
101	10.850.464.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
102	10.850.473.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
103	10.850.482.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
106	10.858.245.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
107	10.858.262.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes

108	10.858.271.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
109	10.858.280.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
116	10.858.792.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
117	10.858.810.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
118	10.858.820.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
119	10.858.831.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
120	10.858.842.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
121	10.858.851.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
122	10.858.862.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
123	10.858.872.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
124	10.858.882.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
125	10.858.893.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
126	10.858.902.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
127	10.858.912.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
130	10.860.233.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
131	10.860.244.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
132	10.860.253.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
133	10.860.262.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
135	10.861.551.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
136	10.861.568.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
140	10.887.048.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
141	10.887.069.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
142	10.887.079.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
143	10.887.089.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
144	10.887.099.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
145	10.887.108.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
154	10.887.689.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
155	10.887.706.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
156	10.887.715.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
157	10.887.725.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
158	10.887.735.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
159	10.887.747.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
160	10.887.757.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
161	10.887.766.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
162	10.887.777.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
163	10.887.785.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
164	10.887.796.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
165	10.887.806.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
166	10.887.816.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
167	10.887.826.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
168	10.887.836.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
169	10.887.845.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
171	10.888.470.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
172	10.888.483.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
174	10.889.163.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes

175	10.889.176.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
180	10.889.634.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
181	10.889.657.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
182	10.889.668.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
183	10.889.678.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
184	10.889.689.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
185	10.889.699.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
186	10.889.709.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
187	10.889.719.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
193	10.890.150.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
194	10.890.162.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
195	10.890.172.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
196	10.890.181.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
197	10.890.191.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
198	10.890.200.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
199	10.890.211.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
200	10.890.220.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
201	10.890.230.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
202	10.890.240.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
205	10.948.754.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
206	10.948.771.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
207	10.948.781.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
208	10.948.790.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
215	10.949.252.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
216	10.949.271.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
217	10.949.282.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
218	10.949.309.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
219	10.949.320.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
220	10.949.330.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
223	10.949.909.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
224	10.949.922.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
230	10.965.057.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
231	10.965.081.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
232	10.965.093.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
233	10.965.109.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
234	10.965.121.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
245	10.966.047.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
246	10.966.064.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
247	10.966.074.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
248	10.966.084.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
249	10.966.094.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
250	10.966.106.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
251	10.966.116.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
252	10.966.127.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
253	10.966.138.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes

254	10.966.148.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
261	10.966.360.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
262	10.966.374.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
263	10.966.385.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
264	10.966.394.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
265	10.966.404.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
266	10.966.414.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
277	10.967.529.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
278	10.967.542.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
279	10.967.552.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
280	10.967.576.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
281	10.967.585.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
282	10.967.596.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
283	10.967.606.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
284	10.967.615.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
285	10.967.625.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
286	10.967.635.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
295	10.967.823.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
296	10.967.835.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
297	10.967.845.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
298	10.967.854.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
299	10.967.863.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
300	10.967.872.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
301	10.967.882.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
302	10.967.891.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
309	10.968.770.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
310	10.968.784.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
311	10.968.794.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
312	10.968.803.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
313	10.968.813.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
314	10.968.825.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
317	10.974.859.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
318	10.974.877.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
321	11.036.014.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
322	11.036.031.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
329	11.036.508.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
330	11.036.526.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
331	11.036.536.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
332	11.036.546.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
333	11.036.557.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
334	11.036.567.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
339	11.036.960.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
340	11.036.972.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
341	11.036.982.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
342	11.036.991.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes

346	11.037.335.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
347	11.037.348.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
348	11.037.358.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
354	11.037.738.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
355	11.037.750.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
356	11.037.762.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
357	11.037.773.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
358	11.037.795.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
366	11.038.307.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
367	11.038.320.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
368	11.038.329.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
369	11.038.338.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
370	11.038.346.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
371	11.038.358.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
372	11.038.367.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
379	11.038.826.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
380	11.038.837.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
381	11.038.846.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
382	11.038.855.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
383	11.038.863.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
384	11.038.873.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
391	11.039.258.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
392	11.039.270.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
393	11.039.280.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
394	11.039.289.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
395	11.039.298.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
396	11.039.310.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
397	11.039.320.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1322	[TCP Window Full] FTP Data: 1248 bytes
403	11.039.725.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
404	11.039.738.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
405	11.039.748.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
406	11.039.757.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
407	11.039.767.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	[TCP Window Full] FTP Data: 1440 bytes
409	11.040.140.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	[TCP Window Full] FTP Data: 1440 bytes
438	11.128.991.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
439	11.129.008.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	[TCP Window Full] FTP Data: 1440 bytes
445	11.129.475.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
446	11.129.493.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
447	11.129.503.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
448	11.129.513.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
449	11.129.523.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	[TCP Window Full] FTP Data: 1440 bytes
454	11.129.902.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes

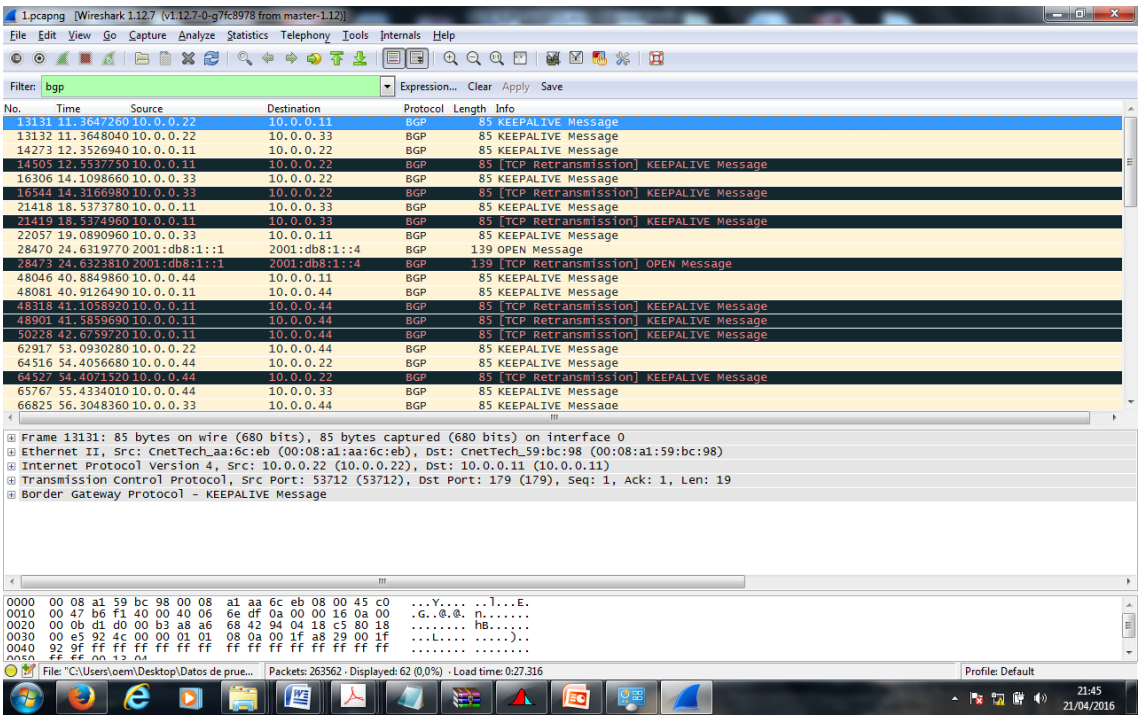
455	11.129.914.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
456	11.129.938.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
457	11.129.947.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	[TCP Window Full] FTP Data: 1440 bytes
462	11.130.303.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
463	11.130.315.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
464	11.130.324.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
465	11.130.334.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	[TCP Window Full] FTP Data: 1440 bytes
471	11.130.715.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
472	11.130.726.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
473	11.130.736.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
474	11.130.746.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
475	11.130.756.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	[TCP Window Full] FTP Data: 1440 bytes
481	11.131.154.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
482	11.131.166.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
483	11.131.175.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
484	11.131.184.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
485	11.131.193.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	[TCP Window Full] FTP Data: 1440 bytes
491	11.131.630.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
492	11.131.641.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
493	11.131.651.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
494	11.131.660.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
495	11.131.669.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	[TCP Window Full] FTP Data: 1440 bytes
501	11.132.024.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
502	11.132.036.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
503	11.132.046.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
504	11.132.055.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
505	11.132.064.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	[TCP Window Full] FTP Data: 1440 bytes
512	11.132.484.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
513	11.132.505.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
514	11.132.514.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
515	11.132.523.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
516	11.132.532.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
522	11.132.961.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
523	11.132.973.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
524	11.132.982.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
525	11.132.990.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
526	11.132.999.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
529	11.209.013.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
530	11.209.033.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
539	11.209.761.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
540	11.209.781.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes

541	11.209.792.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
542	11.209.808.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
543	11.209.818.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
544	11.209.828.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
545	11.209.839.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
546	11.209.851.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
552	11.210.354.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
553	11.210.373.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
554	11.210.384.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
555	11.210.412.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
556	11.210.423.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
564	11.210.947.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
565	11.210.962.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
566	11.210.972.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
567	11.210.981.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
568	11.210.990.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
569	11.211.002.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
570	11.211.012.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
579	11.211.472.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
580	11.211.485.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
581	11.211.495.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
582	11.211.503.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
583	11.211.513.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
584	11.211.524.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
585	11.211.533.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
586	11.211.543.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
593	11.211.930.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
594	11.211.941.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
595	11.211.951.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
596	11.211.960.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
597	11.211.969.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
598	11.211.980.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
603	11.212.355.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
604	11.212.366.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
605	11.212.376.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
606	11.212.386.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
612	11.212.813.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
613	11.212.835.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
614	11.212.846.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
615	11.212.855.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
616	11.212.865.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
618	11.217.366.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
620	11.217.807.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
624	11.221.607.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
625	11.221.627.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes

626	11.221.637.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
628	11.222.884.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
630	11.224.468.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
632	11.225.787.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
634	11.324.391.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
637	11.328.483.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
638	11.328.502.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
642	11.328.843.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
643	11.328.872.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
644	11.328.881.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
646	11.329.278.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
651	11.339.174.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
652	11.339.202.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
653	11.339.214.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
654	11.339.225.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes
662	11.339.741.000	2001:db8:11::2	2001:db8:44::2	FTP-DATA	1514	FTP Data: 1440 bytes

El proceso es exactamente igual para IPv4.

Finalmente podemos ver una captura de los paquetes BGP en la red con el filtro BGP como ya fue indicado anteriormente:



No.	Time	Source	Destination	Protocol	Length	Info
13131	11.364.726.000	10.0.0.22	10.0.0.11	BGP	85	KEEPALIVE Message

13132	11.364.804.000	10.0.0.22	10.0.0.33	BGP	85	KEEPALIVE Message
14273	12.352.694.000	10.0.0.11	10.0.0.22	BGP	85	KEEPALIVE Message
14505	12.553.775.000	10.0.0.11	10.0.0.22	BGP	85	[TCP Retransmission] KEEPALIVE Message
16306	14.109.866.000	10.0.0.33	10.0.0.22	BGP	85	KEEPALIVE Message
16544	14.316.698.000	10.0.0.33	10.0.0.22	BGP	85	[TCP Retransmission] KEEPALIVE Message
21418	18.537.378.000	10.0.0.11	10.0.0.33	BGP	85	KEEPALIVE Message
21419	18.537.496.000	10.0.0.11	10.0.0.33	BGP	85	[TCP Retransmission] KEEPALIVE Message
22057	19.089.096.000	10.0.0.33	10.0.0.11	BGP	85	KEEPALIVE Message
28470	24.631.977.000	2001:db8:1::1	2001:db8:1::4	BGP	139	OPEN Message
28473	24.632.381.000	2001:db8:1::1	2001:db8:1::4	BGP	139	[TCP Retransmission] OPEN Message
48046	40.884.986.000	10.0.0.44	10.0.0.11	BGP	85	KEEPALIVE Message
48081	40.912.649.000	10.0.0.11	10.0.0.44	BGP	85	KEEPALIVE Message
48318	41.105.892.000	10.0.0.11	10.0.0.44	BGP	85	[TCP Retransmission] KEEPALIVE Message
48901	41.585.969.000	10.0.0.11	10.0.0.44	BGP	85	[TCP Retransmission] KEEPALIVE Message
50228	42.675.972.000	10.0.0.11	10.0.0.44	BGP	85	[TCP Retransmission] KEEPALIVE Message
62917	53.093.028.000	10.0.0.22	10.0.0.44	BGP	85	KEEPALIVE Message
64516	54.405.668.000	10.0.0.44	10.0.0.22	BGP	85	KEEPALIVE Message
64527	54.407.152.000	10.0.0.44	10.0.0.22	BGP	85	[TCP Retransmission] KEEPALIVE Message
65767	55.433.401.000	10.0.0.44	10.0.0.33	BGP	85	KEEPALIVE Message
66825	56.304.836.000	10.0.0.33	10.0.0.44	BGP	85	KEEPALIVE Message
67034	56.478.564.000	10.0.0.33	10.0.0.44	BGP	85	[TCP Retransmission] KEEPALIVE Message
85142	71.366.656.000	10.0.0.22	10.0.0.11	BGP	85	KEEPALIVE Message
85143	71.366.745.000	10.0.0.22	10.0.0.33	BGP	85	KEEPALIVE Message
86349	72.359.120.000	10.0.0.11	10.0.0.22	BGP	85	KEEPALIVE Message
88497	74.117.549.000	10.0.0.33	10.0.0.22	BGP	85	KEEPALIVE Message
93275	78.125.568.000	10.0.0.11	10.0.0.33	BGP	85	KEEPALIVE Message
94427	79.094.415.000	10.0.0.33	10.0.0.11	BGP	85	KEEPALIVE Message
120210	101.030.683.000	10.0.0.11	10.0.0.44	BGP	85	KEEPALIVE Message
120407	101.198.957.000	10.0.0.11	10.0.0.44	BGP	85	[TCP Retransmission] KEEPALIVE

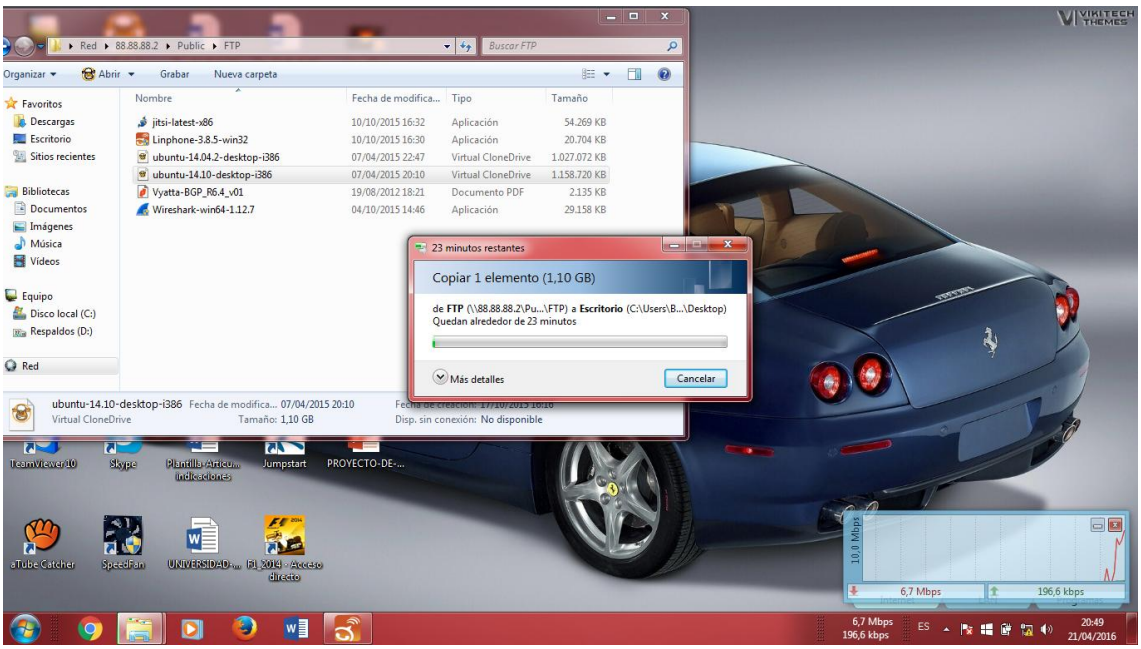
						Message
120460	101.238.098.000	10.0.0.44	10.0.0.11	BGP	85	KEEPALIVE Message
120467	101.239.452.000	10.0.0.44	10.0.0.11	BGP	85	[TCP Retransmission] KEEPALIVE Message
134979	113.615.214.000	10.0.0.22	10.0.0.44	BGP	85	KEEPALIVE Message
136474	114.895.469.000	10.0.0.44	10.0.0.22	BGP	85	KEEPALIVE Message
137150	115.470.289.000	10.0.0.44	10.0.0.33	BGP	85	KEEPALIVE Message
138100	116.279.527.000	10.0.0.33	10.0.0.44	BGP	85	KEEPALIVE Message
155695	131.380.319.000	10.0.0.22	10.0.0.11	BGP	85	KEEPALIVE Message
155711	131.392.921.000	10.0.0.22	10.0.0.33	BGP	85	KEEPALIVE Message
156838	132.362.257.000	10.0.0.11	10.0.0.22	BGP	85	KEEPALIVE Message
158911	134.140.347.000	10.0.0.33	10.0.0.22	BGP	85	KEEPALIVE Message
163724	138.282.127.000	10.0.0.11	10.0.0.33	BGP	85	KEEPALIVE Message
164686	139.103.639.000	10.0.0.33	10.0.0.11	BGP	85	KEEPALIVE Message
168990	142.814.191.000	2001:db8:1::4	2001:db8:1::1	BGP	139	OPEN Message
169015	142.831.211.000	2001:db8:1::1	2001:db8:1::4	BGP	109	NOTIFICATION Message
171135	144.645.070.000	2001:db8:1::1	2001:db8:1::4	BGP	139	OPEN Message
190005	160.886.213.000	10.0.0.11	10.0.0.44	BGP	85	KEEPALIVE Message
190079	160.948.070.000	10.0.0.44	10.0.0.11	BGP	85	KEEPALIVE Message
204184	173.087.812.000	10.0.0.22	10.0.0.44	BGP	85	KEEPALIVE Message
205628	174.322.381.000	10.0.0.44	10.0.0.22	BGP	85	KEEPALIVE Message
206199	174.812.915.000	10.0.0.44	10.0.0.22	BGP	85	[TCP Retransmission] KEEPALIVE Message
206724	175.264.994.000	10.0.0.44	10.0.0.33	BGP	85	KEEPALIVE Message
207914	176.287.315.000	10.0.0.33	10.0.0.44	BGP	85	KEEPALIVE Message
208458	176.756.533.000	10.0.0.33	10.0.0.44	BGP	85	[TCP Retransmission] KEEPALIVE Message
225552	191.463.012.000	10.0.0.22	10.0.0.11	BGP	85	KEEPALIVE Message
225553	191.463.206.000	10.0.0.22	10.0.0.33	BGP	85	KEEPALIVE Message
226604	192.366.764.000	10.0.0.11	10.0.0.22	BGP	85	KEEPALIVE Message
228659	194.130.304.000	10.0.0.33	10.0.0.22	BGP	85	KEEPALIVE Message
229446	194.808.221.000	10.0.0.33	10.0.0.22	BGP	85	[TCP Retransmission] KEEPALIVE Message
233352	198.173.530.000	10.0.0.11	10.0.0.33	BGP	85	KEEPALIVE Message
234464	199.126.114.000	10.0.0.33	10.0.0.11	BGP	85	KEEPALIVE Message

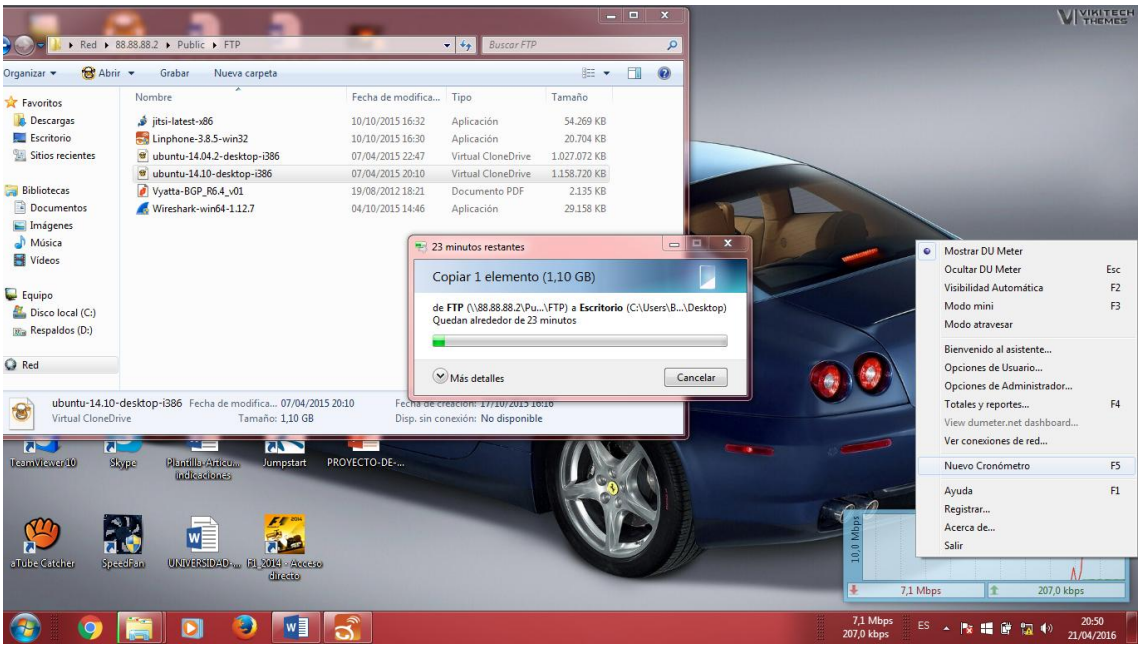
259644	220.895.774.000	10.0.0.11	10.0.0.44	BGP	85	KEEPALIVE Message
261251	222.296.723.000	10.0.0.44	10.0.0.11	BGP	85	[TCP Retransmission] KEEPALIVE Message

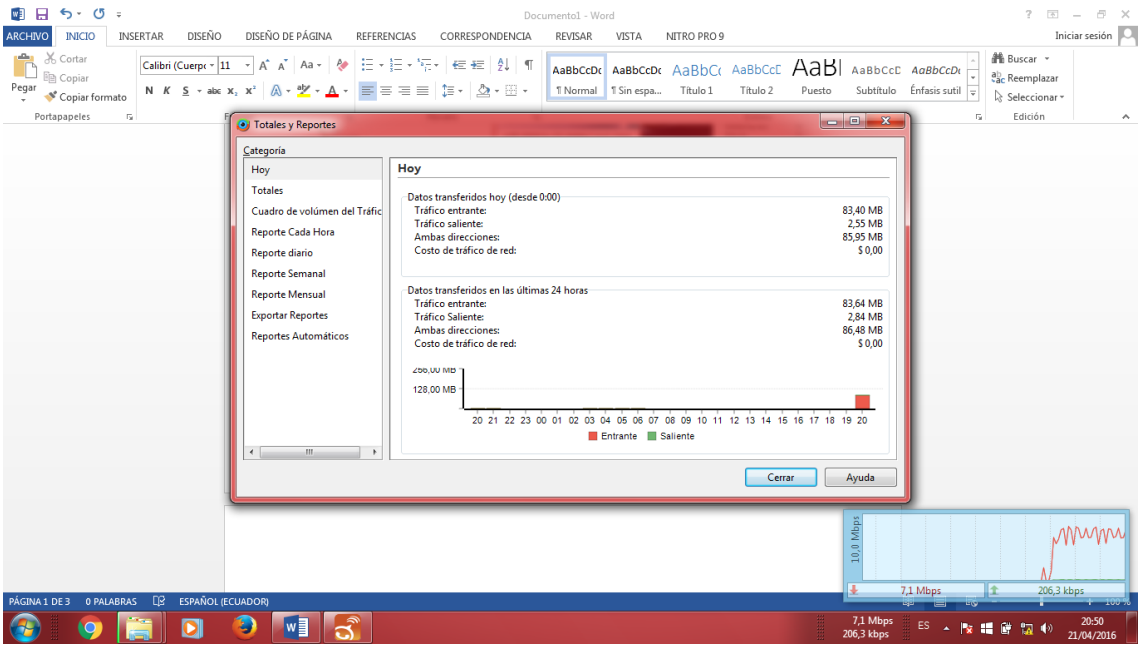
Anexo B. MEDICIÓN DE ANCHO DE BANDA CON DU METER

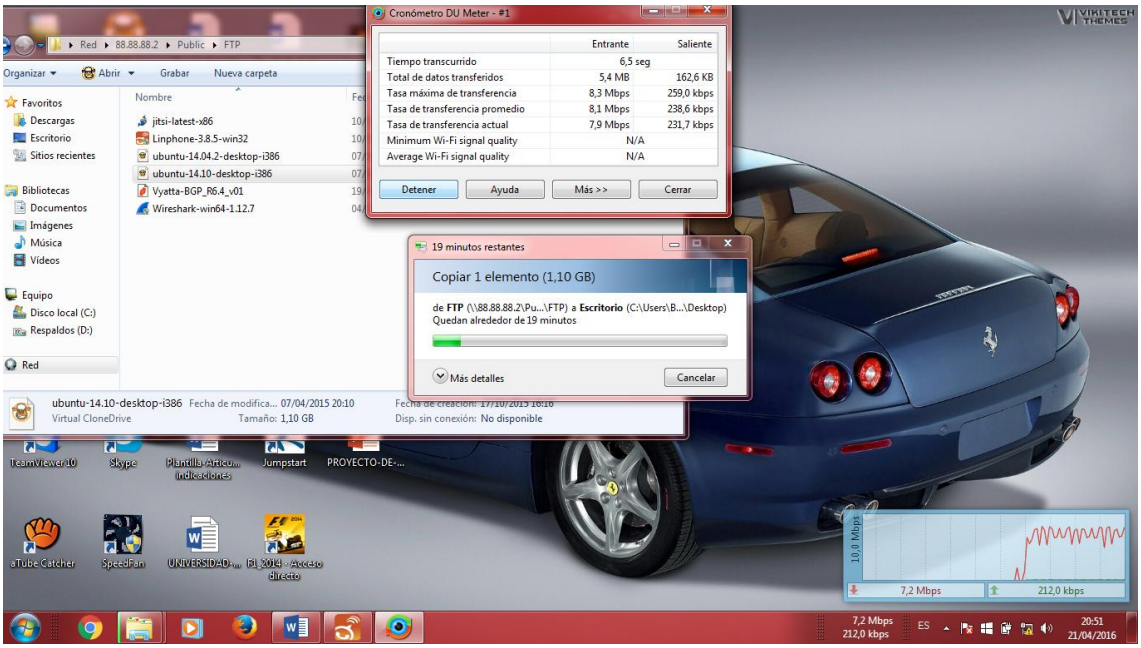
Aplicativo sencillo de utilizar, solo requiere descarga desde la página del desarrollador. A pesar de ser un aplicativo con licencia, la versión de prueba presta todas las características disponibles por un plazo de 30 días luego de lo cual se requiere su compra. Permite administración remota a través del INTERNET a la red de destino, para lo cual se debe programar los equipos host a los que se va a acceder. Entre sus características más importantes se encuentra el análisis en tiempo real del uso del ancho de banda de la red local o de INTERNET a través de una pantalla flotante que se ubica en una de las esquinas del escritorio en Windows.
Permite general gráficos estadísticos cronológicos o ejecutar cronómetros de medición lo cual facilita tareas como las realizadas en esta investigación.

A continuación se detallan capturas de DU – Meter en funcionamiento en el host conectado a R4




Red ▸ 88.88.88.2 ▸ Public ▸ FTP
Buscar FTP
Organizar
Abrir
Grabar
Nueva carpeta
Favoritos
Descargas
Escritorio
Sitios recientes
Bibliotecas
Documentos
Imágenes
Música
Vídeos
Equipo
Disco local (C:)
Respaldos (D:)
Red
Nombre
Fecha de modifica...
Tipo
Tamaño
jitsi-latest-x86 10/10/2015 16:32 Aplicación 54.269 KB
Linphone-3.8.5-win32 10/10/2015 16:30 Aplicación 20.704 KB
ubuntu-14.04.2-desktop-i386 07/04/2015 22:47 Virtual CloneDrive 1.027.072 KB
ubuntu-14.10-desktop-i386 07/04/2015 20:10 Virtual CloneDrive 1.158.720 KB
Vyatta-BGP_R6.4_v01 19/08/2012 18:21 Documento PDF 2.135 KB
Wireshark-win64-1.12.7 04/10/2015 14:46 Aplicación 29.158 KB
23 minutos restantes
Copiar 1 elemento (1,10 GB)
de FTP (\\88.88.88.2\Pu...\FTP) a Escritorio (C:\Users\B...\Desktop)
Quedan alrededor de 23 minutos
Más detalles
Cancelar
ubuntu-14.10-desktop-i386 Fecha de modifica... 07/04/2015 20:10
Virtual CloneDrive Tamaño: 1,10 GB
Disp. sin conexión: No disponible
Mostrar DU Meter
Ocultar DU Meter Esc
Visibilidad Automática F2
Modo mini F3
Modo atravesar
Bienvenido al asistente...
Opciones de Usuario...
Opciones de Administrador...
Totales y reportes... F4
View dumeter.net dashboard...
Ver conexiones de red...
Nuevo Cronómetro F5
Ayuda F1
Registrar...
Acerca de...
Salir
TeamViewer 10
Skype
Plantilla Artícu... Indicaciones
Jumpstart
PROYECTO-DE-...
aTube Catcher
SpeedFan
UNIVERSIDAD-...
F1 2014 - Acceso directo
10,0 Mbps
7,1 Mbps
207,0 kbps
7,1 Mbps
207,0 kbps
ES
20:50
21/04/2016


Documento1 - Word
ARCHIVO
INICIO
INSERTAR
DISEÑO
DISEÑO DE PÁGINA
REFERENCIAS
CORRESPONDENCIA
REVISAR
VISTA
NITRO PRO 9
Iniciar sesión
Pegar
Cortar
Copiar
Copiar formato
Portapapeles
Calibri (Cuerpo)
11
Normal
Sin espa...
Título 1
Título 2
Puesto
Subtítulo
Énfasis sutil
Buscar
Reemplazar
Seleccionar
Edición
Totales y Reportes
Categoría
Hoy
Totales
Cuadro de volúmen del Tráfic
Reporte Cada Hora
Reporte diario
Reporte Semanal
Reporte Mensual
Exportar Reportes
Reportes Automáticos
Hoy
Datos transferidos hoy (desde 0:00)
Tráfico entrante: 83,40 MB
Tráfico saliente: 2,55 MB
Ambas direcciones: 85,95 MB
Costo de tráfico de red: $ 0,00
Datos transferidos en las últimas 24 horas
Tráfico entrante: 83,64 MB
Tráfico Saliente: 2,84 MB
Ambas direcciones: 86,48 MB
Costo de tráfico de red: $ 0,00
256,00 MB
128,00 MB
20 21 22 23 00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20
Entrante
Saliente
Cerrar
Ayuda
10,0 Mbps
7,1 Mbps
206,3 kbps
PÁGINA 1 DE 3
0 PALABRAS
ESPAÑOL (ECUADOR)
7,1 Mbps
206,3 kbps
ES
20:50
21/04/2016



No requiere de mayor configuración y en las opciones de administración facilita la visualización de los estadísticos generados a través de varias selecciones para darle formato a los datos obtenidos.

De manera sencilla gracias al cronómetro programable se puede obtener el valor promedio del ancho de banda utilizado en el medio.

Anexo C. GENERACIÓN DE TRÁFICO CON MAUSEZAHN

Su instalación no resulta compleja al realizarla desde INTERNET, basta con ingresar el siguiente comando para la distribución Ubuntu 15.10 de LINUX:

sudo apt-get install mz

Una vez finalizada la descarga e instalación, se debe proceder a ejecutarlo mediante una pantalla de consola. Dispone de varias opciones de generación de tráfico en distintos protocolos, permite seleccionar una dirección de red o enviar tráfico aleatoriamente a los equipos del sistema. Su sintaxis requiere revisión de documentación que puede ser adquirida en su mayoría en inglés y alemán. Para el proyecto hemos utilizado el siguiente comando para ejecutar la inyección de tráfico IP:

sudo mz –c 0 –t ip –p 1024 –B 99.99.99.2 –d 0.1m

sudo mz –c 0 –t ipv6 –p 1024 –B 2001:db8:44::2 –d 0.1m

Se debe tomar en cuenta los siguientes parámetros utilizados:

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

-t (Creador del paquete)

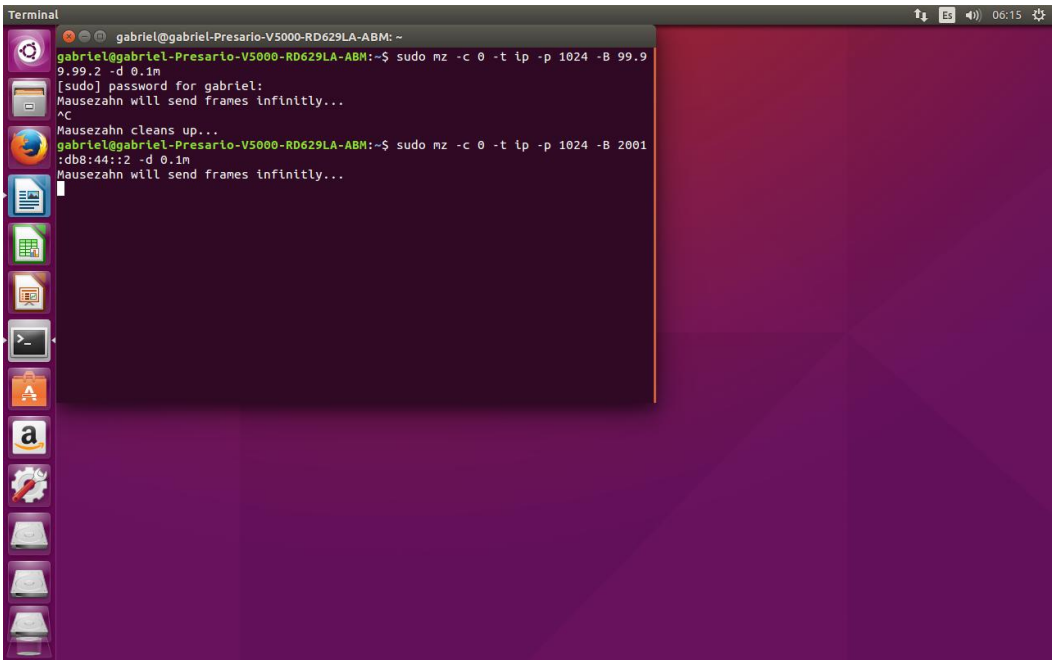
Ip - IPv6(Versión del protocolo)

-p (enviar paquetes de una longitud específica)

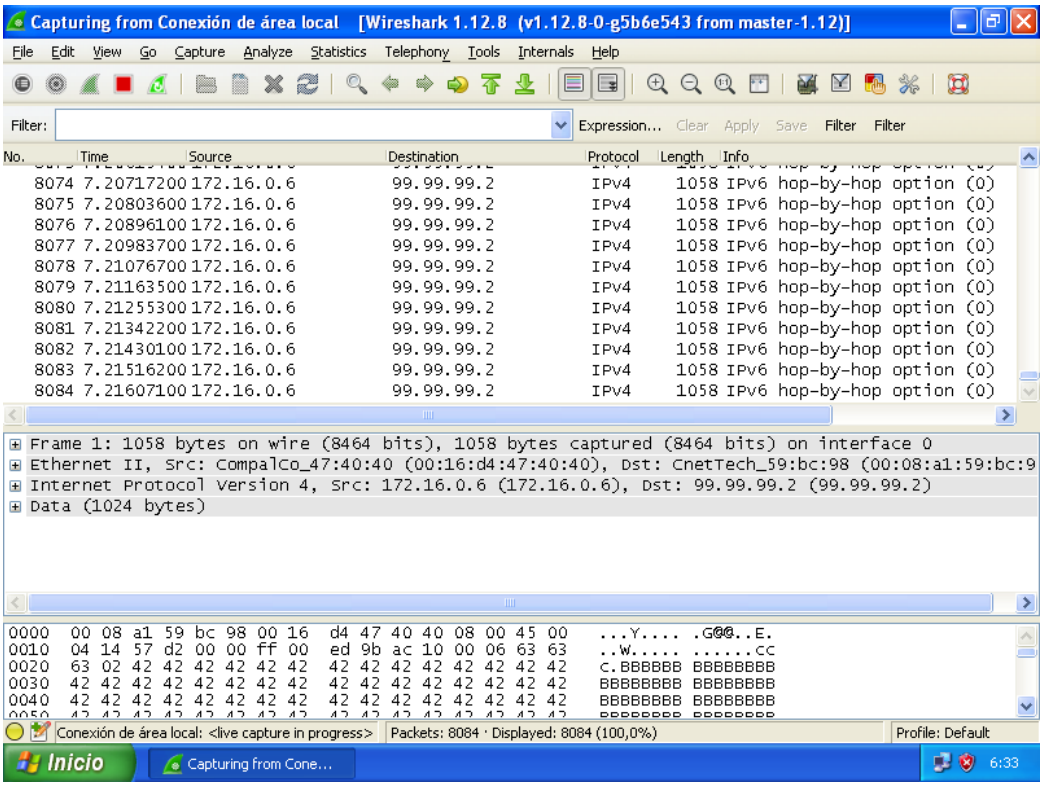
-B (Usar una dirección ip específica)

-d (Retardo entre las transmisiones)

De esta manera se logra saturar la red con tráfico IP, para poder simular el ruido existente por la convivencia de varios dispositivos en la misma.



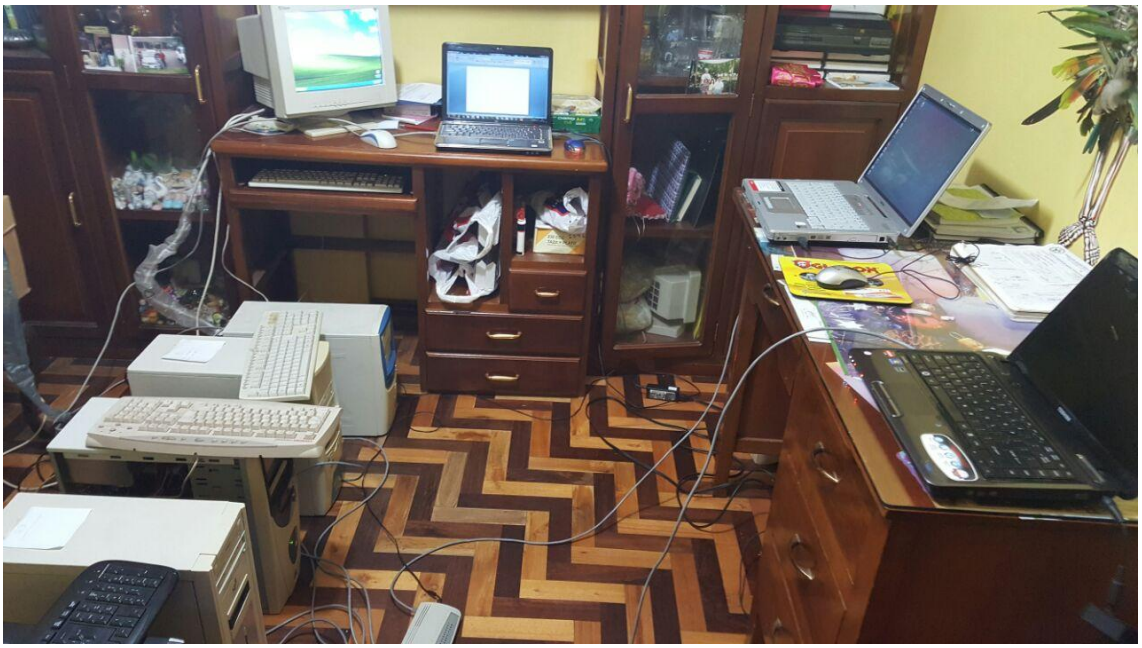
A continuación se muestra una captura de la visualización mediante WIRESHARK del tráfico generado por MAUSEZAHN:



Así se pueden generar envíos infinitos para el propósito indicado.

Anexo D. CAPTURAS DEL ESCENARIO DE PRUEBAS

Se muestran algunas fotografías del escenario en funcionamiento. Se debe detallar la utilización de 5 PCs ensamblados, 2 computadores portátiles y un HUB para la comunicación de los dispositivos y las mediciones.

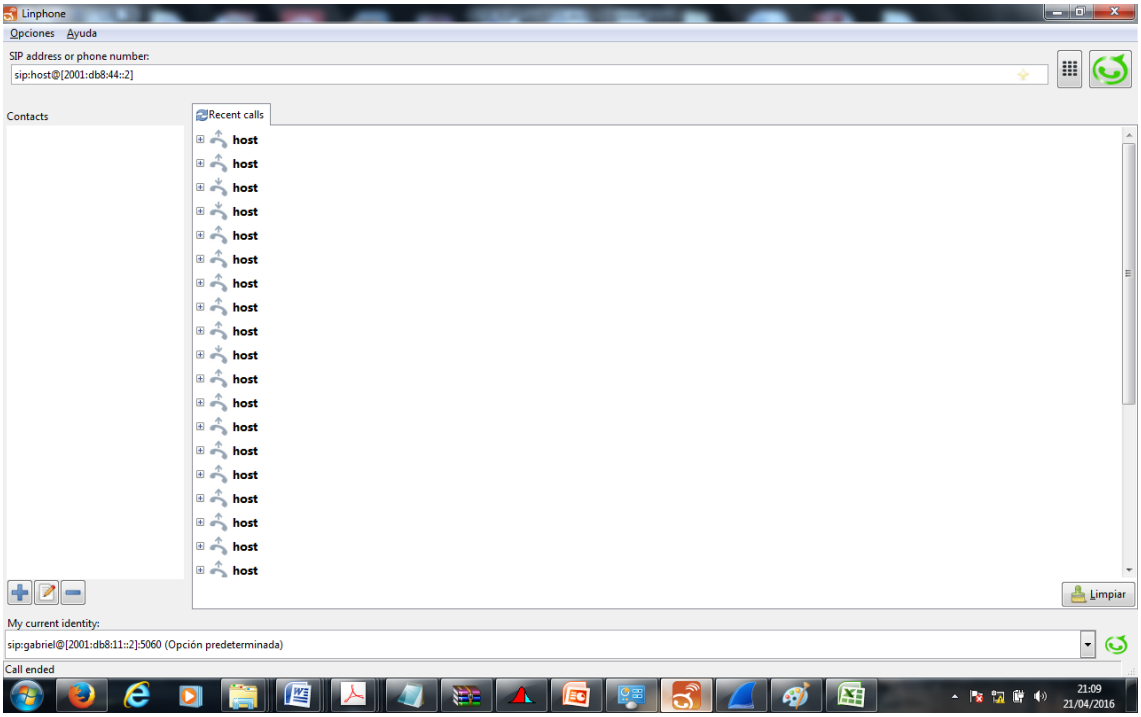


Anexo E. FUNCIONAMIENTO DE LINPHONE

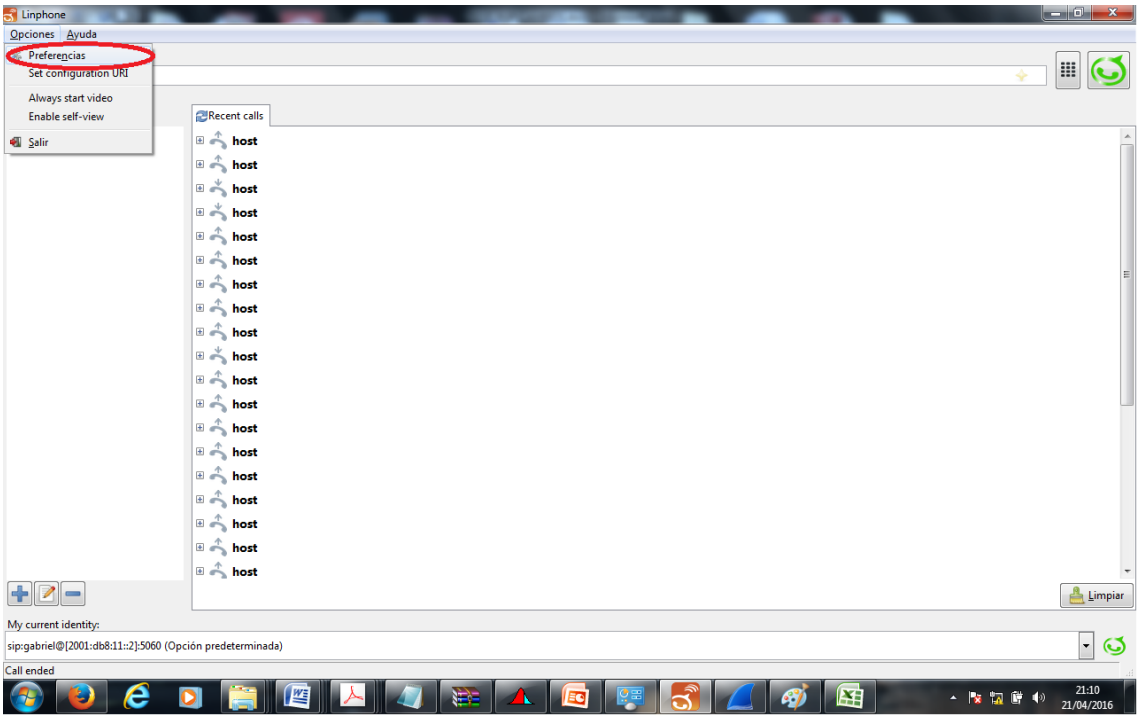
El softphone LINPHONE es de instalación y uso sencillo, permite realizar labores de comunicación IP en una red permitiendo simular en un computador las prestaciones de dispositivos especializados de telefonía IP (llamadas y video llamadas).

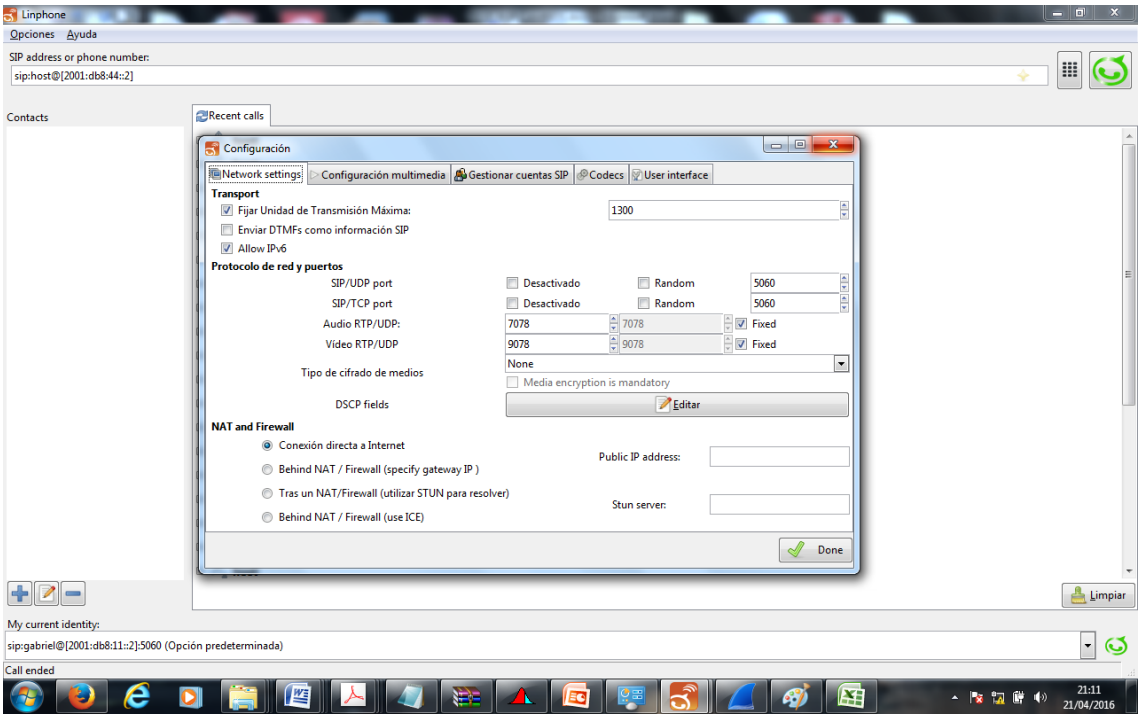
Puede ser configurado para su funcionamiento con el protocolo IPv4 o IPv6 además permite configurar varios aspectos como la codificación de audio utilizada, configuración de los codecs disponibles en el equipo para transmisión y recepción e incluso permite grabar las

conversaciones que se llevan a cabo. A continuación se presenta la pantalla principal del aplicativo:

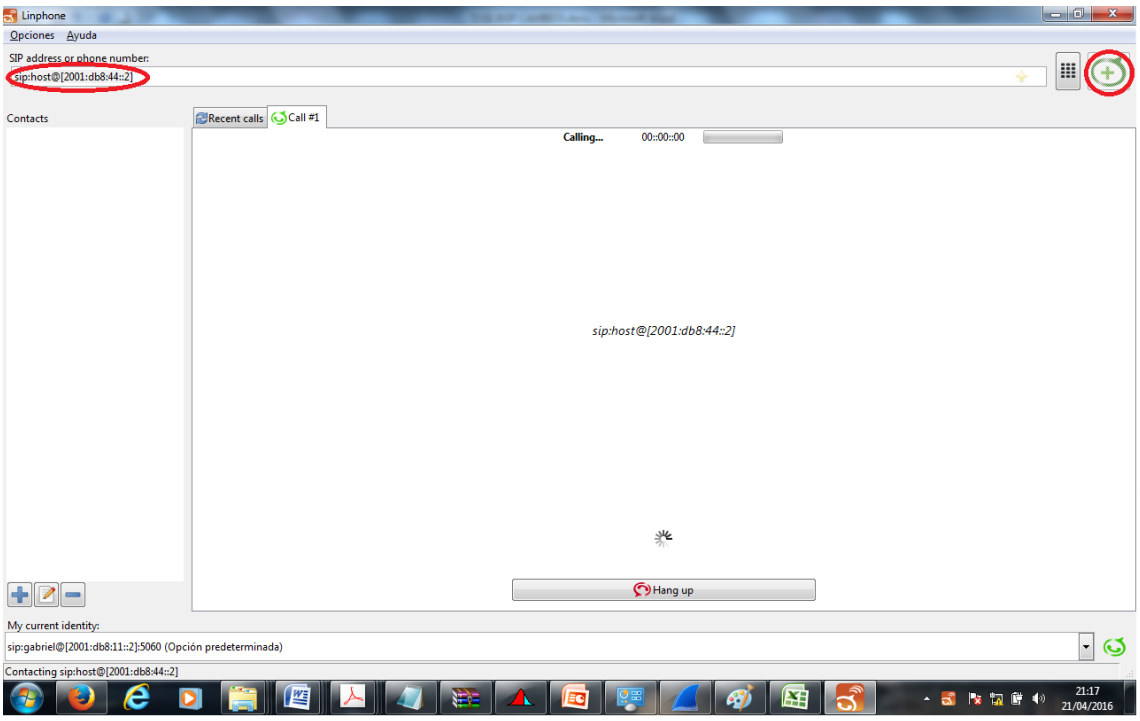


Ingresando al menú OPCIONES > PREFERENCIAS se accede a las opciones de configuración.





Para realizar una llamada se debe ingresar la dirección IP en la versión deseada, del dispositivo al cual se desea contactar, así:



Como se puede apreciar en la figura en el cuadro de texto donde parece la leyenda sip:host...se debe ingresar la dirección IP del dispositivo deseado, el formato para cada caso es el siguiente:

sip:host@[2001:db8:44::2]

sip:host@99.99.99.2

Para realizar la llamada se debe presionar el ícono de color verde presente en la esquina superior derecha de la pantalla del aplicativo.

Anexo F. CONFIGURACIÓN DE ROUTERS VYATTA

A continuación se muestra la programación de los routers utilizados en el escenario de pruebas.

Configuración R1:

```
vyatta@R1:~$ show configuration
interfaces {
    ethernet eth0 {
        address 2001:db8:11::1/64
        address 88.88.88.1/30
        duplex auto
        hw-id 00:03:47:9d:de:b5
        smp_affinity auto
        speed auto
    }
    ethernet eth1 {
        address 172.16.0.1/24
        address 2001:db8:1::1/64
        duplex auto
        hw-id 00:08:a1:59:bc:98
        smp_affinity auto
        speed auto
        traffic-policy {
            out BGP
        }
    }
    loopback lo {
        address 10.0.0.11/32
    }
}
protocols {
    bgp 100 {
        address-family {
```

```
        ipv6-unicast {
            redistribute {
                connected {
                }
            }
        }
    }
    neighbor 10.0.0.22 {
        remote-as 100
        update-source 10.0.0.11
    }
    neighbor 10.0.0.33 {
        remote-as 100
        update-source 10.0.0.11
    }
    neighbor 10.0.0.44 {
        remote-as 100
        update-source 10.0.0.11
    }
    neighbor 88.88.88.2 {
        remote-as 200
    }
    neighbor 2001:db8:1::4 {
        remote-as 200
        update-source 2001:db8:1::1
    }
    network 172.16.0.0/24 {
    }
    parameters {
        router-id 10.0.0.11
    }
}
ospf {
    area 0.0.0.0 {
        network 10.0.0.11/32
        network 172.16.0.0/24
        network 88.88.88.0/30
```

```
        }
        parameters {
            abr-type cisco
            router-id 10.0.0.11
        }
       passive-interface eth0
    }
    ripng {
        interface eth0
        interface eth1
        redistribute {
            connected {
            }
        }
    }
}
service {
    https {
        http-redirect enable
    }
    ssh {
        port 22
    }
}
system {
    config-management {
        commit-revisions 20
    }
    console {
        device ttyS0 {
            speed 9600
        }
    }
    host-name R1
    ipv6 {
    }
    login {
```

```
    user vyatta {
        authentication {
            encrypted-password **********
        }
        level admin
    }
}
ntp {
    server 0.vyatta.pool.ntp.org {
    }
    server 1.vyatta.pool.ntp.org {
    }
    server 2.vyatta.pool.ntp.org {
    }
}
package {
    auto-sync 1
    repository community {
        components main
        distribution stable
        password **********
        url http://packages.vyatta.com/vyatta
        username ""
    }
}
syslog {
    global {
        facility all {
            level notice
        }
        facility protocols {
            level debug
        }
    }
}
time-zone GMT
```

```
}
traffic-policy {
    shaper BGP {
        bandwidth 10000kbit
        class 10 {
            bandwidth 45%
            burst 15k
            ceiling 100%
            description "VOIP - TRAFICO RTP"
            match VOIP-RTP {
                ip {
                    dscp 46
                }
            }
            queue-type fair-queue
        }
        class 20 {
            bandwidth 5%
            burst 15k
            ceiling 100%
            description "VOIP - TRAFICO SIP"
            match VOIP-SIP {
                ip {
                    dscp 26
                }
            }
            queue-type fair-queue
        }
        default {
            bandwidth 15%
            burst 15k
            ceiling 100%
            queue-type fair-queue
        }
        description "POLITICA QoS LIMITA ANCHO DE BANDA"
    }
}
```

Configuración R2:

```
vyatta@R2:~$ show configuration
interfaces {
    ethernet eth0 {
        address 172.16.0.2/24
        address 2001:db8:1::2/64
        duplex auto
        hw-id 00:08:a1:aa:6c:eb
        smp_affinity auto
        speed auto
    }
    ethernet eth1 {
        duplex auto
        hw-id 00:d0:09:f8:cc:b2
        smp_affinity auto
        speed auto
    }
    loopback lo {
        address 10.0.0.22/32
    }
}
protocols {
    bgp 100 {
        neighbor 10.0.0.11 {
            remote-as 100
            update-source 10.0.0.22
        }
        neighbor 10.0.0.33 {
            remote-as 100
            update-source 10.0.0.22
        }
        neighbor 10.0.0.44 {
            remote-as 100
            update-source 10.0.0.22
        }
```

```
        parameters {
            router-id 10.0.0.22
        }
    }
    ospf {
        area 0.0.0.0 {
            network 10.0.0.22/32
            network 172.16.0.0/24
        }
        parameters {
            abr-type cisco
            router-id 10.0.0.22
        }
    }
    static {
    }
}
service {
    ssh {
        port 22
    }
}
system {
    config-management {
        commit-revisions 20
    }
    console {
        device ttyS0 {
            speed 9600
        }
    }
    host-name R2
    login {
        user vyatta {
            authentication {
                encrypted-password **********
            }
```

```
        level admin
      }
    }
    ntp {
      server 0.vyatta.pool.ntp.org {
      }
      server 1.vyatta.pool.ntp.org {
      }
      server 2.vyatta.pool.ntp.org {
      }
    }
    package {
      auto-sync 1
      repository community {
        components main
        distribution stable
        password **********
        url http://packages.vyatta.com/vyatta
        username ""
      }
    }
    syslog {
      global {
        facility all {
          level notice
        }
        facility protocols {
          level debug
        }
      }
    }
    time-zone GMT
}
```

Configuración R3:

vyatta@R3:~$ show configuration

```
interfaces {
    ethernet eth0 {
        address 172.16.0.3/24
        address 2001:db8:1::3/64
        duplex auto
        hw-id 00:e0:4c:a1:46:46
        smp_affinity auto
        speed auto
    }
    ethernet eth1 {
        duplex auto
        hw-id 00:e0:4c:1b:af:4f
        smp_affinity auto
        speed auto
    }
    loopback lo {
        address 10.0.0.33/32
    }
}
protocols {
    bgp 100 {
        neighbor 10.0.0.11 {
            remote-as 100
            update-source 10.0.0.33
        }
        neighbor 10.0.0.22 {
            remote-as 100
            update-source 10.0.0.33
        }
        neighbor 10.0.0.44 {
            remote-as 100
            update-source 10.0.0.33
        }
        parameters {
            router-id 10.0.0.33
        }
    }
```

```
    ospf {
        area 0.0.0.0 {
            network 10.0.0.33/32
            network 172.16.0.0/24
        }
        parameters {
            abr-type cisco
            router-id 10.0.0.33
        }
    }
}
service {
    ssh {
        port 22
    }
}
system {
    config-management {
        commit-revisions 20
    }
    console {
        device ttyS0 {
            speed 9600
        }
    }
    host-name R3
    login {
        user vyatta {
            authentication {
                encrypted-password **********
            }
            level admin
        }
    }
    ntp {
        server 0.vyatta.pool.ntp.org {
        }
```

```
        server 1.vyatta.pool.ntp.org {
        }
        server 2.vyatta.pool.ntp.org {
        }
    }
    package {
        auto-sync 1
        repository community {
            components main
            distribution stable
            password **********
            url http://packages.vyatta.com/vyatta
            username ""
        }
    }
    syslog {
        global {
            facility all {
                level notice
            }
            facility protocols {
                level debug
            }
        }
    }
    time-zone GMT
}
```

Configuración R4:

```
vyatta@R4:~$ show conf
interfaces {
    ethernet eth0 {
        address 2001:db8:44::1/64
        address 99.99.99.1/30
        duplex auto
        hw-id 00:16:76:c8:cb:76
```

```
        smp_affinity auto
        speed auto
    }
    ethernet eth1 {
        address 172.16.0.4/24
        address 2001:db8:1::4/64
        duplex auto
        hw-id 00:e0:4c:1b:7d:3c
        smp_affinity auto
        speed auto
        traffic-policy {
            out BGP
        }
    }
    loopback lo {
        address 10.0.0.44/32
    }
}
protocols {
    bgp 100 {
        neighbor 10.0.0.11 {
            remote-as 100
            update-source 10.0.0.44
        }
        neighbor 10.0.0.22 {
            remote-as 100
            update-source 10.0.0.44
        }
        neighbor 10.0.0.33 {
            remote-as 100
            update-source 10.0.0.44
        }
        neighbor 99.99.99.2 {
            remote-as 300
        }
        neighbor 2001:db8:1::1 {
            remote-as 200
```

```
            update-source 2001:db8:1::4
        }
        network 172.16.0.0/24 {
        }
        parameters {
            router-id 10.0.0.44
        }
    }
    ospf {
        area 0.0.0.0 {
            network 10.0.0.44/32
            network 172.16.0.0/24
            network 99.99.99.0/30
        }
        parameters {
            abr-type cisco
            router-id 10.0.0.44
        }
        passive-interface eth0
    }
    ripng {
        interface eth0
        interface eth1
        redistribute {
            connected {
            }
        }
    }
}
service {
    ssh {
        port 22
    }
}
system {
    config-management {
        commit-revisions 20
```

```
    }
    console {
        device ttyS0 {
            speed 9600
        }
    }
    host-name R4
    ntp {
        server 0.vyatta.pool.ntp.org {
        }
        server 1.vyatta.pool.ntp.org {
        }
        server 2.vyatta.pool.ntp.org {
        }
    }
    package {
        auto-sync 1
        repository community {
            components main
            distribution stable
            password **********
            url http://packages.vyatta.com/vyatta
            username ""
        }
    }
    syslog {
        global {
            facility all {
                level notice
            }
            facility protocols {
                level debug
            }
        }
    }
    time-zone GMT
}
```

```
traffic-policy {
    shaper BGP {
        bandwidth 10000kbit
        class 10 {
            bandwidth 45%
            burst 15k
            ceiling 100%
            description "VOIP - TRAFICO RTP"
            match VOIP-RTP {
                ip {
                    dscp 46
                }
            }
            queue-type fair-queue
        }
        class 20 {
            bandwidth 5%
            burst 15k
            ceiling 100%
            description "VOIP - TRAFICO SIP"
            match VOIP-SIP {
                ip {
                    dscp 26
                }
            }
            queue-type fair-queue
        }
        default {
            bandwidth 15%
            burst 15k
            ceiling 100%
            queue-type fair-queue
        }
        description "POLITICA QoS LIMITA ANCHO DE BANDA"
    }
}
```

Se muestra el resumen del protocolo BGP en cada router:

Resumen de BGP en R1:

```
vyatta@R1:~$ show ip bgp neighbors
BGP neighbor is 10.0.0.22, remote AS 100, local AS 100, internal link
  BGP version 4, remote router ID 10.0.0.22
  BGP state = Established, up for 01:51:35
  Last read 14:52:06, hold time is 180, keepalive interval is 60 seconds
  Neighbor capabilities:
    4 Byte AS: advertised and received
    Route refresh: advertised and received(old & new)
    Address family IPv4 Unicast: advertised and received
  Message statistics:
    Inq depth is 0
    Outq depth is 0
                         Sent       Rcvd
    Opens:                  1          1
    Notifications:          0          0
    Updates:                1          0
    Keepalives:           113        112
    Route Refresh:          0          0
    Capability:             0          0
    Total:                115        113
  Minimum time between advertisement runs is 5 seconds
  Update source is 10.0.0.11

 For address family: IPv4 Unicast
  Community attribute sent to this neighbor(both)
  0 accepted prefixes

  Connections established 1; dropped 0
  Last reset never
Local host: 10.0.0.11, Local port: 46613
Foreign host: 10.0.0.22, Foreign port: 179
Nexthop: 10.0.0.11
Nexthop global: ::1
```

Nexthop local: ::
BGP connection: non shared network
Read thread: on Write thread: off

BGP neighbor is 10.0.0.33, remote AS 100, local AS 100, internal link
 BGP version 4, remote router ID 10.0.0.33
 BGP state = Established, up for 01:51:32
 Last read 14:52:03, hold time is 180, keepalive interval is 60 seconds
 Neighbor capabilities:
  4 Byte AS: advertised and received
  Route refresh: advertised and received(old & new)
  Address family IPv4 Unicast: advertised and received
 Message statistics:
  Inq depth is 0
  Outq depth is 0

	Sent	Rcvd
Opens:	1	1
Notifications:	0	0
Updates:	1	0
Keepalives:	113	112
Route Refresh:	0	0
Capability:	0	0
Total:	115	113

 Minimum time between advertisement runs is 5 seconds
 Update source is 10.0.0.11

For address family: IPv4 Unicast
 Community attribute sent to this neighbor(both)
 0 accepted prefixes

 Connections established 1; dropped 0
 Last reset never
Local host: 10.0.0.11, Local port: 58472
Foreign host: 10.0.0.33, Foreign port: 179
Nexthop: 10.0.0.11
Nexthop global: ::1
Nexthop local: ::

BGP connection: non shared network
Read thread: on Write thread: off

BGP neighbor is 10.0.0.44, remote AS 100, local AS 100, internal link
 BGP version 4, remote router ID 10.0.0.44
 BGP state = Established, up for 01:51:49
 Last read 14:52:20, hold time is 180, keepalive interval is 60 seconds
 Neighbor capabilities:
  4 Byte AS: advertised and received
  Route refresh: advertised and received(old & new)
  Address family IPv4 Unicast: advertised and received
 Message statistics:
  Inq depth is 0
  Outq depth is 0

	Sent	Rcvd
Opens:	1	0
Notifications:	0	0
Updates:	1	1
Keepalives:	113	112
Route Refresh:	0	0
Capability:	0	0
Total:	115	113

 Minimum time between advertisement runs is 5 seconds
 Update source is 10.0.0.11

For address family: IPv4 Unicast
 Community attribute sent to this neighbor(both)
 1 accepted prefixes

 Connections established 1; dropped 0
 Last reset never
Local host: 10.0.0.11, Local port: 179
Foreign host: 10.0.0.44, Foreign port: 43993
Nexthop: 10.0.0.11
Nexthop global: ::1
Nexthop local: ::
BGP connection: non shared network

Read thread: on Write thread: off

BGP neighbor is 88.88.88.2, remote AS 200, local AS 100, external link
 BGP version 4, remote router ID 0.0.0.0
 BGP state = Active
 Last read 01:53:39, hold time is 180, keepalive interval is 60 seconds
 Message statistics:
  Inq depth is 0
  Outq depth is 0
                Sent   Rcvd
  Opens: 0   0
  Notifications: 0   0
  Updates: 0   0
  Keepalives: 0   0
  Route Refresh: 0   0
  Capability: 0   0
  Total: 0   0
 Minimum time between advertisement runs is 30 seconds

 For address family: IPv4 Unicast
 Community attribute sent to this neighbor(both)
 0 accepted prefixes

 Connections established 0; dropped 0
 Last reset never
Next connect timer due in 39 seconds
Read thread: off Write thread: off

BGP neighbor is 2001:db8:1::4, remote AS 200, local AS 100, external link
 BGP version 4, remote router ID 0.0.0.0
 BGP state = Idle
 Last read 01:53:39, hold time is 180, keepalive interval is 60 seconds
Message statistics:
  Inq depth is 0
  Outq depth is 0
                Sent   Rcvd
  Opens: 63   0

```
  Notifications:          0         63
  Updates:                0         0
  Keepalives:             0         0
  Route Refresh:          0         0
  Capability:             0         0
  Total:                  63        63
 Minimum time between advertisement runs is 30 seconds
 Update source is 2001:db8:1::1

For address family: IPv4 Unicast
 Community attribute sent to this neighbor(both)
 0 accepted prefixes

 Connections established 0; dropped 0
 Last reset never
Local host: 2001:db8:1::1, Local port: 60771
Foreign host: 2001:db8:1::4, Foreign port: 179
Nexthop: 10.0.0.11
Nexthop global: 2001:db8:1::1
Nexthop local: fe80::208:a1ff:fe59:bc98
BGP connection: shared network
Next start timer due in 84 seconds
Read thread: off  Write thread: off

vyatta@R1:~$ show ip bgp summary
BGP router identifier 10.0.0.11, local AS number 100
IPv4 Unicast - max multipaths: ebgp 1 ibgp 1
IPv6 Unicast - max multipaths: ebgp 1 ibgp 1
RIB entries 1, using 64 bytes of memory
Peers 5, using 12 KiB of memory

Neighbor        V         AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
10.0.0.22       4        100     116     118                0    0    0        01:54:33        0
10.0.0.33       4        100     116     118        0    0    0        01:54:30        0
10.0.0.44       4        100     116     118        0    0    0        01:54:47        1
88.88.88.2      4        200       0       0                0    0    0        01:54:30    Active
2001:db8:1::4   6        200      65      65                0    0    0        01:54:47    Active
```

Total number of neighbors 5

Resumen de BGP en R2:

vyatta@R2:~$ show ip bgp neighbors
BGP neighbor is 10.0.0.11, remote AS 100, local AS 100, internal link
  BGP version 4, remote router ID 10.0.0.11
  BGP state = Established, up for 01:58:46
  Last read 16:01:11, hold time is 180, keepalive interval is 60 seconds
  Neighbor capabilities:
    4 Byte AS: advertised and received
    Route refresh: advertised and received(old & new)
    Address family IPv4 Unicast: advertised and received
  Message statistics:
    Inq depth is 0
    Outq depth is 0
                         Sent   Rcvd
    Opens: 1   0
    Notifications: 0   0
    Updates: 0   1
    Keepalives: 120   119
    Route Refresh: 0   0
    Capability: 0   0
    Total: 121   120
  Minimum time between advertisement runs is 5 seconds
  Update source is 10.0.0.22

 For address family: IPv4 Unicast
  Community attribute sent to this neighbor(both)
  1 accepted prefixes

  Connections established 1; dropped 0
  Last reset never
Local host: 10.0.0.22, Local port: 179
Foreign host: 10.0.0.11, Foreign port: 46613
Nexthop: 10.0.0.22
Nexthop global: ::1

Nexthop local: ::
BGP connection: non shared network
Read thread: on Write thread: off

BGP neighbor is 10.0.0.33, remote AS 100, local AS 100, internal link
 BGP version 4, remote router ID 10.0.0.33
 BGP state = Established, up for 01:58:45
 Last read 16:01:09, hold time is 180, keepalive interval is 60 seconds
 Neighbor capabilities:
  4 Byte AS: advertised and received
  Route refresh: advertised and received(old & new)
  Address family IPv4 Unicast: advertised and received
 Message statistics:
  Inq depth is 0
  Outq depth is 0

	Sent	Rcvd
Opens:	1	1
Notifications:	0	0
Updates:	0	0
Keepalives:	120	119
Route Refresh:	0	0
Capability:	0	0
Total:	121	120

 Minimum time between advertisement runs is 5 seconds
 Update source is 10.0.0.22

For address family: IPv4 Unicast
 Community attribute sent to this neighbor(both)
 0 accepted prefixes

 Connections established 1; dropped 0
 Last reset never
Local host: 10.0.0.22, Local port: 54823
Foreign host: 10.0.0.33, Foreign port: 179
Nexthop: 10.0.0.22
Nexthop global: ::1
Nexthop local: ::

BGP connection: non shared network
Read thread: on Write thread: off

BGP neighbor is 10.0.0.44, remote AS 100, local AS 100, internal link
 BGP version 4, remote router ID 10.0.0.44
 BGP state = Established, up for 01:59:00
 Last read 16:01:24, hold time is 180, keepalive interval is 60 seconds
 Neighbor capabilities:
  4 Byte AS: advertised and received
  Route refresh: advertised and received(old & new)
  Address family IPv4 Unicast: advertised and received
 Message statistics:
  Inq depth is 0
  Outq depth is 0

	Sent	Rcvd
Opens:	1	0
Notifications:	0	0
Updates:	0	1
Keepalives:	120	119
Route Refresh:	0	0
Capability:	0	0
Total:	121	120

 Minimum time between advertisement runs is 5 seconds
 Update source is 10.0.0.22

For address family: IPv4 Unicast
 Community attribute sent to this neighbor(both)
 1 accepted prefixes

 Connections established 1; dropped 0
 Last reset never
Local host: 10.0.0.22, Local port: 179
Foreign host: 10.0.0.44, Foreign port: 52783
Nexthop: 10.0.0.22
Nexthop global: ::1
Nexthop local: ::
BGP connection: non shared network

Read thread: on Write thread: off

vyatta@R2:~$ show ip bgp summary
BGP router identifier 10.0.0.22, local AS number 100
IPv4 Unicast - max multipaths: ebgp 1 ibgp 1
RIB entries 1, using 64 bytes of memory
Peers 3, using 7572 bytes of memory

Neighbor	V	AS	MsgRcvd	MsgSent	TblVer	InQ	OutQ	Up/Down	State/PfxRcd
10.0.0.11	4	100	122	123	0	0	0	02:00:27	1
10.0.0.33	4	100	122	123	0	0	0	02:00:26	0
10.0.0.44	4	100	122	123	0	0	0	02:00:41	1

Total number of neighbors 3

Resumen de BGP en R3:

vyatta@R3:~$ show ip bgp neighbors
BGP neighbor is 10.0.0.11, remote AS 100, local AS 100, internal link
  BGP version 4, remote router ID 10.0.0.11
  BGP state = Established, up for 02:02:52
  Last read 19:55:36, hold time is 180, keepalive interval is 60 seconds
  Neighbor capabilities:
    4 Byte AS: advertised and received
    Route refresh: advertised and received(old & new)
    Address family IPv4 Unicast: advertised and received
  Message statistics:
    Inq depth is 0
    Outq depth is 0

	Sent	Rcvd
Opens:	1	0
Notifications:	0	0
Updates:	0	1
Keepalives:	124	123
Route Refresh:	0	0
Capability:	0	0
Total:	125	124

  Minimum time between advertisement runs is 5 seconds

Update source is 10.0.0.33

For address family: IPv4 Unicast
Community attribute sent to this neighbor(both)
1 accepted prefixes

Connections established 1; dropped 0
Last reset never
Local host: 10.0.0.33, Local port: 179
Foreign host: 10.0.0.11, Foreign port: 58472
Nexthop: 10.0.0.33
Nexthop global: ::1
Nexthop local: ::
BGP connection: non shared network
Read thread: on Write thread: off

BGP neighbor is 10.0.0.22, remote AS 100, local AS 100, internal link
BGP version 4, remote router ID 10.0.0.22
BGP state = Established, up for 02:02:53
Last read 19:55:38, hold time is 180, keepalive interval is 60 seconds
Neighbor capabilities:
4 Byte AS: advertised and received
Route refresh: advertised and received(old & new)
Address family IPv4 Unicast: advertised and received
Message statistics:
Inq depth is 0
Outq depth is 0

	Sent	Rcvd
Opens:	1	0
Notifications:	0	0
Updates:	0	0
Keepalives:	124	123
Route Refresh:	0	0
Capability:	0	0
Total:	125	123

Minimum time between advertisement runs is 5 seconds
Update source is 10.0.0.33

For address family: IPv4 Unicast
Community attribute sent to this neighbor(both)
0 accepted prefixes

Connections established 1; dropped 0
Last reset never
Local host: 10.0.0.33, Local port: 179
Foreign host: 10.0.0.22, Foreign port: 54823
Nexthop: 10.0.0.33
Nexthop global: ::1
Nexthop local: ::
BGP connection: non shared network
Read thread: on Write thread: off

BGP neighbor is 10.0.0.44, remote AS 100, local AS 100, internal link
BGP version 4, remote router ID 10.0.0.44
BGP state = Established, up for 02:03:08
Last read 19:54:51, hold time is 180, keepalive interval is 60 seconds
Neighbor capabilities:
4 Byte AS: advertised and received
Route refresh: advertised and received(old & new)
Address family IPv4 Unicast: advertised and received
Message statistics:
Inq depth is 0
Outq depth is 0

	Sent	Rcvd
Opens:	1	0
Notifications:	0	0
Updates:	0	1
Keepalives:	125	124
Route Refresh:	0	0
Capability:	0	0
Total:	126	125

Minimum time between advertisement runs is 5 seconds
Update source is 10.0.0.33

For address family: IPv4 Unicast
Community attribute sent to this neighbor(both)
1 accepted prefixes

Connections established 1; dropped 0
Last reset never
Local host: 10.0.0.33, Local port: 179
Foreign host: 10.0.0.44, Foreign port: 40651
Nexthop: 10.0.0.33
Nexthop global: ::1
Nexthop local: ::
BGP connection: non shared network
Read thread: on Write thread: off

vyatta@R3:~$ show ip bgp summary
BGP router identifier 10.0.0.33, local AS number 100
IPv4 Unicast - max multipaths: ebgp 1 ibgp 1
RIB entries 1, using 64 bytes of memory
Peers 3, using 7572 bytes of memory

Neighbor	V	AS	MsgRcvd	MsgSent	TblVer	InQ	OutQ	Up/Down	State/PfxRcd
10.0.0.11	4	100	126	127	0	0	0	02:04:17	1
10.0.0.22	4	100	125	127	0	0	0	02:04:18	0
10.0.0.44	4	100	126	127	0	0	0	02:04:33	1

Total number of neighbors 3

Resumen de BGP en R4:
vyatta@R4:~$ show ip bgp neighbors
BGP neighbor is 10.0.0.11, remote AS 100, local AS 100, internal link
BGP version 4, remote router ID 10.0.0.11
BGP state = Established, up for 02:09:38
Last read 15:39:01, hold time is 180, keepalive interval is 60 seconds
Neighbor capabilities:
4 Byte AS: advertised and received
Route refresh: advertised and received(old & new)

```
    Address family IPv4 Unicast: advertised and received
  Message statistics:
    Inq depth is 0
    Outq depth is 0
                         Sent       Rcvd
    Opens:                  1          1
    Notifications:          0          0
    Updates:                1          1
    Keepalives:           131        130
    Route Refresh:          0          0
    Capability:             0          0
    Total:                133        132
  Minimum time between advertisement runs is 5 seconds
  Update source is 10.0.0.44

 For address family: IPv4 Unicast
  Community attribute sent to this neighbor(both)
  1 accepted prefixes

  Connections established 1; dropped 0
  Last reset never
Local host: 10.0.0.44, Local port: 43993
Foreign host: 10.0.0.11, Foreign port: 179
Nexthop: 10.0.0.44
Nexthop global: ::1
Nexthop local: ::
BGP connection: non shared network
Read thread: on  Write thread: off

BGP neighbor is 10.0.0.22, remote AS 100, local AS 100, internal link
  BGP version 4, remote router ID 10.0.0.22
  BGP state = Established, up for 02:09:37
  Last read 15:39:01, hold time is 180, keepalive interval is 60 seconds
  Neighbor capabilities:
    4 Byte AS: advertised and received
    Route refresh: advertised and received(old & new)
    Address family IPv4 Unicast: advertised and received
```

```
  Message statistics:
    Inq depth is 0
    Outq depth is 0
                         Sent       Rcvd
    Opens:                  1          1
    Notifications:          0          0
    Updates:                1          0
    Keepalives:           131        130
    Route Refresh:          0          0
    Capability:             0          0
    Total:                133        131
  Minimum time between advertisement runs is 5 seconds
  Update source is 10.0.0.44

 For address family: IPv4 Unicast
  Community attribute sent to this neighbor(both)
  0 accepted prefixes

  Connections established 1; dropped 0
  Last reset never
Local host: 10.0.0.44, Local port: 52783
Foreign host: 10.0.0.22, Foreign port: 179
Nexthop: 10.0.0.44
Nexthop global: ::1
Nexthop local: ::
BGP connection: non shared network
Read thread: on  Write thread: off

BGP neighbor is 10.0.0.33, remote AS 100, local AS 100, internal link
  BGP version 4, remote router ID 10.0.0.33
  BGP state = Established, up for 02:09:37
  Last read 15:39:00, hold time is 180, keepalive interval is 60 seconds
  Neighbor capabilities:
    4 Byte AS: advertised and received
    Route refresh: advertised and received(old & new)
    Address family IPv4 Unicast: advertised and received
  Message statistics:
```

Inq depth is 0

Outq depth is 0

	Sent	Rcvd
Opens:	1	1
Notifications:	0	0
Updates:	1	0
Keepalives:	131	130
Route Refresh:	0	0
Capability:	0	0
Total:	133	131

Minimum time between advertisement runs is 5 seconds

Update source is 10.0.0.44

For address family: IPv4 Unicast

Community attribute sent to this neighbor(both)

0 accepted prefixes

Connections established 1; dropped 0

Last reset never

Local host: 10.0.0.44, Local port: 40651

Foreign host: 10.0.0.33, Foreign port: 179

Nexthop: 10.0.0.44

Nexthop global: ::1

Nexthop local: ::

BGP connection: non shared network

Read thread: on Write thread: off

BGP neighbor is 99.99.99.2, remote AS 300, local AS 100, external link

BGP version 4, remote router ID 0.0.0.0

BGP state = Active

Last read 02:11:42, hold time is 180, keepalive interval is 60 seconds

Message statistics:

Inq depth is 0

Outq depth is 0

	Sent	Rcvd
Opens:	0	0
Notifications:	0	0

Updates: 0 0
Keepalives: 0 0
Route Refresh: 0 0
Capability: 0 0
Total: 0 0
Minimum time between advertisement runs is 30 seconds

For address family: IPv4 Unicast
Community attribute sent to this neighbor(both)
0 accepted prefixes

Connections established 0; dropped 0
Last reset never
Next connect timer due in 37 seconds
Read thread: off Write thread: off

BGP neighbor is 2001:db8:1::1, remote AS 200, local AS 100, external link
BGP version 4, remote router ID 0.0.0.0
BGP state = Active
Last read 02:11:42, hold time is 180, keepalive interval is 60 seconds
Message statistics:
Inq depth is 0
Outq depth is 0
Sent Rcvd
Opens: 65 0
Notifications: 0 0
Updates: 0 0
Keepalives: 0 0
Route Refresh: 0 0
Capability: 0 0
Total: 65 0
Minimum time between advertisement runs is 30 seconds
Update source is 2001:db8:1::4

For address family: IPv4 Unicast
Community attribute sent to this neighbor(both)
0 accepted prefixes

Connections established 0; dropped 0

Last reset never

Local host: 2001:db8:1::4, Local port: 59750

Foreign host: 2001:db8:1::1, Foreign port: 179

Nexthop: 10.0.0.44

Nexthop global: 2001:db8:1::4

Nexthop local: fe80::2e0:4cff:fe1b:7d3c

BGP connection: shared network

Next connect timer due in 25 seconds

Read thread: off Write thread: off

vyatta@R4:~$ show ip bgp summary

BGP router identifier 10.0.0.44, local AS number 100

IPv4 Unicast - max multipaths: ebgp 1 ibgp 1

RIB entries 1, using 64 bytes of memory

Peers 5, using 12 KiB of memory

Neighbor	V	AS	MsgRcvd	MsgSent	TblVer	InQ	OutQ	Up/Down	State/PfxRcd
10.0.0.11	4	100	134	135	0	0	0	02:11:47	1
10.0.0.22	4	100	133	135	0	0	0	02:11:46	0
10.0.0.33	4	100	133	135	0	0	0	02:11:46	0
99.99.99.2	4	300	0	0	0	0	0	02:11:46	Active
2001:db8:1::1	6	200	0	66	0	0	0	02:11:46	Active

Total number of neighbors 5