



ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

ESCUELA DE POSTGRADO Y EDUCACIÓN CONTÍNUA

***“ANÁLISIS DE LAS TÉCNICAS DE TUNNELING PARA LA
COEXISTENCIA DE IPv4 E IPv6 QUE BRINDE SOPORTE A TRÁFICO
DE VoIP”***

JORGE RIGOBERTO LÓPEZ ORTEGA

Tesis presentada ante la Escuela de Postgrado y Educación Continua de la ESPOCH, como requisito parcial para la obtención del Título de Magister en Interconectividad de Redes.

Riobamba - Ecuador

2013

CERTIFICACIÓN

El Tribunal de Tesis certifica que:

El trabajo de investigación titulado: “**ANÁLISIS DE LAS TÉCNICAS DE TUNNELING PARA LA COEXISTENCIA DE IPv4 E IPv6 QUE BRINDE SOPORTE A TRÁFICO DE VoIP**”, de responsabilidad del señor Jorge Rigoberto López Ortega, ha sido prolijamente revisado y se autoriza su presentación.

TRIBUNAL DE TESIS

Dr. Juan Vargas

PRESIDENTE

Ing. Ms.C. Daniel Haro M.

DIRECTOR

Ing. Ms.C. Gloria Arcos M.

MIEMBRO

Ing. Ms.C. Vinicio Ramos

MIEMBRO

Riobamba, 30 de abril de 2013

DERECHOS DE AUTORÍA

Yo, **Jorge Rigoberto López Ortega**, soy responsable de las ideas, doctrinas y resultados expuestos en esta Tesis; y el patrimonio intelectual de la Tesis de Grado le pertenece a la ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO.

Ing. Jorge R. López O.

DEDICATORIA

A Dios por transformarme en su proyecto de vida y bendecirme a cada momento.

A mis padres Marco y Aurora por brindarme la oportunidad de conocer que nunca se ha logrado nada sin entusiasmo y al mismo tiempo convertirme en una persona íntegra en la sociedad.

A mis hermanas Maritza, Cristina, Licet y a mi hermano David por el temple que me obsequiaron para avanzar en todo momento y dejarme sentir con calidez su amor.

A mis mejores amigos Patricio y Ramiro por su apoyo y ánimo incondicional al enseñarme que los amigos son la familia que uno puede escoger.

AGRADECIMIENTO

Al Ing. Ms.C. Daniel Haro M., Director de la Tesis de Grado, por su valiosa cooperación, soporte y contribución de procesos y métodos creativos en el desarrollo del presente trabajo investigativo.

A la Ing. Ms.C. Gloria Arcos M. y al Ing. Ms.C. Vinicio Ramos, Miembros del Tribunal de Tesis, por las sugerencias y propuestas técnicas formuladas al autor con un estilo eficiente, auténtico, diligente y propositivo.

Al Ing. Ms. C. Alberto Arellano y al Ing. Luis Pazmiño, por la motivación y ayuda brindada en la búsqueda de soluciones a problemas y dificultades que se presentaron en el transcurso del proceso investigativo.

RESUMEN

Este trabajo se refiere al análisis de las Técnicas de Tunneling para la coexistencia de IPv4 e IPv6 que brinde soporte a tráfico VoIP (6to4, ISATAP y GRE), bajo los escenarios de prueba en la Academia Cisco de la Escuela Superior Politécnica de Chimborazo.

La metodología aplicada fue tipo Cuasi-experimental, debido a que la información enviada no fue elegida al azar, sino más bien se tuvo definida junto con los escenarios de prueba (IPv4 puro, IPv6 puro, 6to4, ISATAP y GRE). Además, se manipuló al menos una variable independiente y se pudo aproximar los resultados de una investigación experimental en situaciones en las que no es posible el control y manipulación absolutos de las variables.

Los materiales como software fueron Elastix, VMware Station, CentOS, Wireshark y Jitsi. Como hardware fueron usados un Router Cisco 2811, Switch Cisco 2960, Servidor PBX, Teléfonos IP y Portátiles HP. Sin Técnicas de Tunneling, se pudo determinar que el Jitter más elevado (2,65 ms.) y el mejor Ancho de Banda lo tiene IPv6 (118 Kbps), mientras que la mayor Latencia (80,07 ms.) ocurre en IPv4. Al implementar las Técnicas de Tunneling, se estableció que el Jitter más elevado y la mayor Latencia estuvo en GRE con valores de 2,89ms. y 81,75ms., respectivamente. El mejor Ancho de Banda fue con ISATAP con un valor de 115,67 Kbps.

Según los técnicos encuestados se deduce que GRE lleva menos tiempo para su implementación y presenta una reducida dificultad de configuración, administración y monitoreo. ISATAP exige un mayor grado de conocimiento, por lo que requiere mayor tiempo para implementarse y su grado de dificultad también aumenta. El 6to4 presenta un relativo equilibrio en los índices investigados. En las tres Técnicas de Tunneling existe un relativo balance en lo que respecta a la transmisión de Paquetes RTP. Sin embargo, la Técnica de Tunneling que más evidencia la pérdida de Paquetes RTP, se detectó con GRE con un valor porcentual de eficiencia que no alcanza ni el 1%. El ISATAP mejora este nivel subiéndolo al 33% y 6to4 prácticamente no tiene pérdida de Paquetes RTP.

Luego de realizada la investigación, se puede concluir que en comunicaciones en tiempo real, los factores determinantes son el Jitter y la Latencia. Es por eso, que luego de realizar todas las mediciones necesarias en los diferentes escenarios se concluye que la Técnica de Tunneling ISATAP es la que mejor cumple con estos requerimientos.

Se recomienda, además, impulsar estudios complementarios que permitan mejorar la coexistencia entre redes IPv4 e IPv6. Realizar el análisis de otras Técnicas de Tunneling para evaluar de mejor manera los resultados obtenidos en este proceso investigativo y emitir políticas y regulaciones que impulsen, promuevan y obliguen a la adopción de IPv6 en el país.

SUMMARY

This work concerns the analysis of Tunneling Techniques for the coexistence of IPv4 and IPv6 traffic to provide VoIP support (6to4, ISATAP and GRE) under test scenarios in Cisco Academy at the Polytechnic University of Chimborazo.

The methodology used was quasi-experimental type, because the information sent was not chosen at random but rather it was defined along test scenarios (pure IPv4, pure IPv6, 6to4, ISATAP and GRE). Furthermore, at least one independent variable was manipulated and it could approximate the results of experimental research in situations where it is not possible absolute control and manipulation of variables.

The materials as software were Elastix, VMware Station, CentOS, Wireshark, and Jitsi. As hardware was used Cisco Router 2811, Cisco 2960 Switch, Server PBX, IP Phones and Laptops HP. Without Tunneling techniques, it was determined that the higher Jitter (2.65 ms.) and the best bandwidth had IPv6 (118 Kbps), while the higher latency (80.07 ms.) occurs in IPv4. By implementing Tunneling techniques, it was established that the highest Jitter and Latency was in GRE greater values of 2.89 ms. and 81.75 ms., respectively. The best bandwidth was with ISATAP with a value of 115.67 Kbps.

According to the technicians surveyed GRE takes less time to implement and it has a low difficulty of configuration, management and monitoring. ISATAP requires a higher degree of knowledge, thus it takes longer to implement and its degree of difficulty increases. The 6to4 presents a relative balance on the investigated indexes. In the three Tunneling techniques there is a relative balance with respect to the transmission of RTP packets. However, the technique most evidence Tunneling RTP packet loss is detected with a GRE efficiency percentage value does not reach even 1%. The ISATAP improve this level to 33% and 6to4 virtually no RTP Packet loss is detected.

After completion of the investigation, it is concluded that in real-time communications, the determining factors are the Jitter and Latency. It is for this reason that after making all required measurements in different scenarios it is concluded that the ISATAP tunneling technique is best fulfilling these requirements.

It is recommended further promote complementary studies to improve the coexistence of IPv4 and IPv6 networks. To perform the analysis of other tunneling techniques to better evaluate the results of this research process and generate policies and regulations that encourage, promote and force the adoption of IPv6 in the country.

ÍNDICE GENERAL

DEDICATORIA	4
AGRADECIMIENTO	5
RESUMEN	6
SUMMARY	7
ÍNDICE GENERAL.....	8
ÍNDICE DE TABLAS.....	10
ÍNDICE DE FIGURAS	11
CAPÍTULO I	12
INTRODUCCIÓN	12
1.1 PROBLEMATIZACIÓN (ANTECEDENTES / PLANTEAMIENTO DEL PROBLEMA).....	12
1.1.1 Antecedentes	12
1.1.2 Planteamiento del Problema.....	14
1.2 OBJETIVOS GENERALES Y ESPECÍFICOS.....	16
1.2.1 General	16
1.2.2 Específicos.....	16
1.3 JUSTIFICACIÓN	16
1.3.1 Justificación Práctica (Escenario de Pruebas).....	20
CAPITULO II.....	21
REVISIÓN DE LITERATURA	21
2.1 TELEFONÍA CONVENCIONAL VS. DIGITAL.....	21
2.1.1 Voz sobre IP	21
2.2 IPv4 E IPv6.....	26
2.2.1 Características principales	27
2.2.2 Direccionamiento.....	28
2.2.3 Representación de las direcciones.....	29
2.2.4 Direcciones Global Unicast	31
2.2.5 Mecanismos de transición básicos.....	32
2.3 COEXISTENCIA DE IPv4 A IPv6.....	33
2.3.1 Transición para la coexistencia.....	34
2.3.2 Implicaciones	39
2.4 TÉCNICAS DE TUNNELING	41
2.4.1 Automático	42
2.4.2 Configurado	43
CAPITULO III.....	44
MATERIALES Y MÉTODOS.....	44
3.1 DISEÑO DE LA INVESTIGACIÓN	44
3.2 TIPO DE ESTUDIO.....	45
3.3 POBLACIÓN Y MUESTRA	45
3.3.1 Población	46

3.3.2 Muestra.....	47
3.4 MÉTODOS, TÉCNICAS, FUENTES DE INFORMACIÓN E INSTRUMENTOS	48
3.4.1 Métodos.....	48
3.4.2 Técnicas	50
3.4.3 Fuentes de Información	50
3.5 VALIDACIÓN DE INSTRUMENTOS	51
3.5.1 Wireshark 1.2.8 (SNV) Rev. 32676	51
3.5.2 Cuestionario.....	52
3.6 PROCESAMIENTO DE LA INFORMACIÓN	52
3.7 PLANTEAMIENTO DE LA HIPÓTESIS	53
3.7.1 Tipo de Hipótesis.....	53
3.8 DETERMINACIÓN DE VARIABLES	53
3.8.1 Operacionalización de Variables.....	53
3.8.2 Operacionalización Metodológica.....	54
3.9 AMBIENTES DE PRUEBA.....	55
3.9.1 Software	55
3.9.2 Hardware	58
3.9.3 Notas Aclaratorias.....	59
3.9.4 Escenario de Prueba solo IPv4	60
3.9.5 Escenario de Prueba solo IPv6	61
3.9.6 Escenario de Prueba Tunneling 6to4.....	62
3.9.7 Escenario de Prueba Tunneling ISATAP	63
3.9.8 Escenario de Prueba Tunneling GRE/IPv6	64
CAPITULO IV.....	65
RESULTADOS Y DISCUSIÓN	65
4.1 PRESENTACIÓN DE RESULTADOS.....	65
4.2 ANÁLISIS E INTERPRETACIÓN DE RESULTADOS	66
4.2.1 Análisis de la Variable Independiente.....	67
4.2.2 Análisis de la Variable Dependiente	78
4.2.3 Resumen de los datos obtenidos y equivalencia de pesos.....	89
4.3 PRUEBA DE LA HIPÓTESIS DE INVESTIGACIÓN.....	93
4.3.1 Planteamiento de la Hipótesis.....	94
4.3.2 Cálculo Chi-Cuadrado	94
4.4 PRESENTACIÓN DE LA PROPUESTA DE COEXISTENCIA DE IPv4 E IPv6 CON TÉCNICAS DE TUNNELING	100
CONCLUSIONES	109
RECOMENDACIONES	111
GLOSARIO	112
BIBLIOGRAFÍA	114
ANEXOS	119

ÍNDICE DE TABLAS

TABLA I: Operacionalización de Variables.....	53
TABLA II: Operacionalización Metodológica.....	54
TABLA III: Número de Direcciones IPv4 e IPv6.....	67
TABLA IV: Agotamiento de Direcciones IPv4 al transcurrir el tiempo.....	68
TABLA V: Crecimiento exponencial de IPv6 en el mundo.....	70
TABLA VI: Jitter IPv4 vs. IPv6.....	73
TABLA VII: Ancho de Banda por tipo de conexión.....	74
TABLA VIII: Ancho de Banda IPv4 vs. IPv6.....	74
TABLA IX: Latencia IPv4 vs. IPv6.....	75
TABLA X: Jitter 6to4 vs. ISATAP vs. GRE.....	78
TABLA XI: Ancho de Banda 6to4 vs. ISATAP vs. GRE.....	79
TABLA XII: Latencia 6to4 vs. ISATAP vs. GRE.....	79
TABLA XIII: Escala Cuantitativa para medir el Tiempo.....	82
TABLA XIV: Tabulación encuestas Índice Tiempo.....	82
TABLA XV: Equivalencia porcentual de tabulación de encuestas Índice Tiempo.....	82
TABLA XVI: Escala Cuantitativa para medir la Dificultad.....	83
TABLA XVII: Tabulación encuestas Índice Dificultad.....	83
TABLA XVIII: Equivalencia porcentual de tabulación de encuestas Índice Dificultad.....	84
TABLA XIX: Paquetes RTP Transmitidos 6to4 vs. ISATAP vs. GRE.....	87
TABLA XX: Paquetes RTP Perdidos 6to4 vs. ISATAP vs. GRE.....	88
TABLA XXI: Resumen de los datos obtenidos y Equivalencia de Pesos para los Indicadores e Índices de la Variable Independiente.....	90
TABLA XXII: Promedios de Equivalencia del Peso de los Índices.....	90
TABLA XXIII: Resumen de Equivalencia del Peso de los Índices.....	91
TABLA XXIV: Promedios de Equivalencia del Peso de los Indicadores.....	93
TABLA XXV: Parámetros para Chi-Cuadrado.....	94
TABLA XXVI: Rangos de Idoneidad para demostrar la Hipótesis.....	95
TABLA XXVII: Variable Dependiente vs. Variable independiente.....	96
TABLA XXVIII: Tabla Observada.....	97
TABLA XXIX: Tabla Esperada.....	97
TABLA XXX: Valores del Chi-Cuadrado.....	98

ÍNDICE DE FIGURAS

Figura 1: Escenario de Pruebas.....	20
Figura 2: Diagrama de Elastix.....	26
Figura 3: Situación actual direcciones IPv4 2010.....	27
Figura 4: Mecanismos basados en Túneles.....	33
Figura 5: IPv4 vs. IPv6 (Paquetes).....	36
Figura 6: IPv4 vs. IPv6 (Bytes)	36
Figura 7: Tipos de Tráfico (Paquetes)	37
Figura 8: Tipos de Tráfico (Bytes)	37
Figura 9: Nativo vs. Transición (Paquetes)	38
Figura 10: Nativo vs. Transición (Paquetes)	38
Figura 11: IPv6 vs. IPv4.....	41
Figura 12: Escuela Superior Politécnica de Chimborazo-Academia Cisco.....	48
Figura 13: IPv4 puro.....	60
Figura 14: IPv6 puro.....	61
Figura 15: Técnica Tunneling 6to4.....	62
Figura 16: Técnica Tunneling ISATAP.....	63
Figura 17: Técnica Tunneling GRE.....	64
Figura 18: Agotamiento de direcciones IPv4.....	68
Figura 19: Proyección de Conexiones de Red IPv6 en el 2016.....	70
Figura 20: Proyección de Dispositivos fijos y móviles IPv6 en el 2016.....	70
Figura 21: Jitter IPv4 vs. IPv6.....	73
Figura 22: Ancho de Banda IPv4 vs. IPv6.....	75
Figura 23: Latencia IPv4 vs. IPv6.....	76
Figura 24: Jitter 6to4 vs. ISATAP vs. GRE.....	78
Figura 25: Ancho de Banda 6to4 vs. ISATAP vs. GRE.....	79
Figura 26: Latencia 6to4 vs. ISATAP vs. GRE.....	80
Figura 27: Tiempo Técnicas de Tunneling Indicador 2.....	83
Figura 28: Dificultad Técnicas de Tunneling Indicador 2.....	84
Figura 29: Paquetes RTP Transmitidos.....	87
Figura 30: Paquetes RTP Perdidos.....	88
Figura 31: Flujo de voz vs. Paquetes RTP Perdidos.....	89
Figura 32: Rendimiento Equivalencia en Pesos.....	91
Figura 33: Facilidad de instalación, configuración, administración y monitoreo. Equivalencia en Pesos.....	92
Figura 34: Número de Paquetes RTP Equivalencia en Pesos.....	92
Figura 35: Gráfica Chi-Cuadrado.....	99

CAPÍTULO I

INTRODUCCIÓN

1.1 PROBLEMATIZACIÓN (ANTECEDENTES / PLANTEAMIENTO DEL PROBLEMA)

1.1.1 Antecedentes

VoIP es un grupo de recursos que hacen posible que la señal de voz viaje a través de Internet empleando un protocolo IP. Esto significa que se envía la señal de voz en forma digital, en paquetes de datos, en lugar de enviarla en forma analógica a través de circuitos utilizables sólo por telefonía convencional como las redes PSTN.

Al mismo tiempo, el avance y fuerte impacto de la telefonía IP durante los últimos años junto con el constante crecimiento de diferentes desarrollos, ha servido para:

- ⇒ Conjugar varios mundos de transmisión de contenidos utilizando una infraestructura de red.
- ⇒ Aumentar tecnologías de compresión y digitalización de la voz.
- ⇒ Mecanismos de enrutamiento de datagramas.
- ⇒ Transmisión de tráfico sensible (tiempo real).
- ⇒ Así como, el estudio de diferentes grupos de paquetes según los requisitos de latencia, ancho de banda y QoS.

Todo lo antes mencionado, más el efecto Internet, hace que:

- ⇒ La distinción entre voz y datos se haga cada día más difusa.
- ⇒ El Internet se transforme aceleradamente en la revolución - evolución de las telecomunicaciones.
- ⇒ Al disponer de un protocolo y red única de transporte de voz y datos es más fácil y económico complementar soluciones con un gran valor agregado.

Además, hay que tomar en cuenta que la disponibilidad de direcciones IPv4 en los últimos años ha ido decreciendo de la siguiente manera¹:

- ⇒ 10% a principio de 2010
- ⇒ 6% mediados de 2010
- ⇒ 5% dos meses después
- ⇒ 2% antes de final de 2010
- ⇒ 0% el 3 de Febrero de 2011

¹ The IPv6 Portal (<http://www.ipv6f.org>). The IPv6 Company Consulintel

1.1.2 Planteamiento del Problema

Hoy en día se niega direcciones IPv4 públicas a la mayoría de los nuevos hosts y se emplean mecanismos como NAT, PPP, etc., para compartir direcciones, pero nuevos tipos de aplicaciones y nuevos mecanismos de acceso, requieren direcciones únicas.

El IPv6 en el Ecuador, una vez que las direcciones IPv4 disponibles sin asignar han caído por debajo del 5% del total de direcciones IP posibles con este protocolo, el NRO (www.nro.net) oficialmente, tanto de modo directo como a través de los registros regionales, (LACNIC en el caso de Latinoamérica y Caribe), ha anunciado la terminación de los espacios de direcciones IPv4 y la necesidad de enfocarse en la transición a IPv6 de modo coordinado y generalizado.

Es por esto, que existen Técnicas de Transición / Coexistencia en un amplio abanico de técnicas que han sido identificadas e implementadas, básicamente dentro de tres categorías:

- Doble-pila, para permitir la coexistencia de IPv4 e IPv6 en el mismo dispositivo y redes.
- Técnicas de túneles, para evitar dependencias cuando se actualizan hosts, routers o regiones.
- Técnicas de traducción, para permitir la comunicación entre dispositivos que son sólo IPv6 y aquellos que son sólo IPv4

Todos estos mecanismos suelen ser utilizados, incluso en combinación.

Por ejemplo, la técnica basada en Tunneling permite interconectar las nubes IPv6 a través de un servicio IPv4 nativo por medio de un túnel. Los paquetes IPv6 son encapsulados por un router de extremo antes de ser transportado a través de la red IPv4, siendo desencapsulados en el extremo de la red IPv6 receptora.

Los túneles pueden ser configurados de forma estática o dinámica como 6to4 o 6over4. GRE (Generic Routing Encapsulation) que es un protocolo originalmente desarrollado por Cisco Systems y se ha convertido en un estándar de la industria definido en las RFC² 1701, 1702 y 2784.

ISATAP (Intra-Site Automatic Tunnel Addressing Protocol) es un nuevo borrador Internet que describe otra técnica para evitar la configuración manual de túneles. Shipworm, por su parte, está específicamente diseñado para efectuar Tunneling a través de IPv4 Network Address Translators.

Además, se ha propuesto TB (Tunnel Broker) para gestionar automáticamente y facilitar el proceso de configuración de las peticiones de túneles de los usuarios.

En los estadios finales de la transición, también se emplearán los túneles para interconectar las nubes IPv4 residuales a través de la infraestructura IPv6.

Con esta realidad, la adopción del IPv6 se vuelve cada vez más crítica y es necesario emitir políticas y regulaciones que impulsen, promuevan y obliguen a la adopción de IPv6 en el País.

² RFC es un documento que puede ser escrito por cualquier persona y que contiene una propuesta para una nueva tecnología, información acerca del uso de tecnologías y/o recursos existentes, propuestas para mejoras de tecnologías, proyectos experimentales y demás.

1.2 OBJETIVOS GENERALES Y ESPECÍFICOS

1.2.1 General

- Analizar las técnicas de Tunneling, para la coexistencia de IPv4 e IPv6 que brinde soporte a tráfico VoIP.

1.2.2 Específicos

- Analizar las técnicas de Tunneling (6to4, ISATAP, GRE/IPv6) que permitan la selección y coexistencia entre IPv4 e IPv6.
- Implementar los escenarios de prueba respectivos, para determinar las diferentes métricas de comprobación.
- Seleccionar la técnica de Tunneling adecuada que permita determinar el mejor grado de coexistencia y QoS para transmitir VoIP en los escenarios propuestos.
- Proponer una guía de implementación de coexistencia de IPv4 e IPv6, mediante la utilización de la técnica de Tunneling más adecuada.

1.3 JUSTIFICACIÓN

Para las instituciones que tienen un papel activo en la formación, capacitación y transformación de las sociedades, es inherente su participación en el desarrollo tecnológico del país como catalizador de las tendencias de globalización mundial. El desarrollo tecnológico logrado en los últimos años, hace posible la creación de nuevos servicios comunicacionales antes inimaginables.

Al reducir constantemente los costos, el avance tecnológico permite que los servicios de comunicaciones puedan ser accesibles a un número de ciudadanos cada vez mayor. Sin embargo, cabe señalar que la clave está en transformar la información en conocimiento y, éste, en educación y aprendizaje significativo.

Asimismo, una gran fuente de desequilibrios entre países y regiones residirá en la aplicación de estas tecnologías. En concreto, los nuevos desequilibrios pueden producirse entre: los que hayan sabido adaptarse a esas tecnologías y los que no lo logren por falta de recursos financieros o de voluntad política.

VoIP es una tecnología que ha sobrepasado a las compañías telefónicas y móviles, debido a un aumento en la cobertura de la red. Con el empleo de aplicaciones VoIP de software libre conseguiremos las siguientes prestaciones:

- Reducción de costos utilizando una infraestructura de red con conexión de banda ancha de alta velocidad.
- Es una red que literalmente acompaña a los distintos usuarios.
- Hay muchos servicios de valor añadido ofrecidos por los varios proveedores de servicios de VOIP. Por ejemplo, facilidad del correo de voz, conferencia de tres vías, marca de velocidad, expedición de llamada, anillo simultáneo, entre otros.
- Facturas telefónicas se reducen al mínimo.
- Se evita el monopolio de las compañías telefónicas.

Con esto, se podrá decidir y analizar algunas infraestructuras, combinación de diferentes paquetes y versiones, mantenimiento a futuro, distribuciones disponibles y reducción del tiempo de implantación en ambientes corporativos.

Cabe señalar que, IPv6 no implica solamente más direcciones IP, sino involucra disponer además de mayor confiabilidad y seguridad, junto con nuevas inversiones, desafíos tecnológicos, comerciales y de seguridad, implicaciones regulatorias y de control, entre otras, que llevarán a una transición con coexistencia temporal de IPv4 e IPv6, de manera programada, regulada y controlada en beneficio de una Internet más estable, segura, confiable y usable.

Por esto es necesario mencionar algunas de las ventajas de la utilización IPv6:

- Capacidades expandidas de direccionamiento.
- Autoconfiguración y reconfiguración “sin servidor” (“plug-n-play”).
- Mecanismos de movilidad más eficientes y robustos.
- Incorporación de encriptado y autenticación en la capa IP.
- Formato de la cabecera simplificado e identificación de flujos.
- Soporte mejorado de opciones/extensiones.

Elastix³ es una aplicación software para crear sistemas de Telefonía IP, que integra las mejores herramientas disponibles para PBX's basados en Asterisk en una interfaz simple y fácil de usar.

Además añade su propio conjunto de utilidades y permite la creación de módulos de terceros para hacer de este el mejor paquete de software disponible para la telefonía de código abierto.

La meta de Elastix son la confiabilidad, modularidad y fácil uso. Estas características

³ <http://www.certificacionelastix.es/index.html>

añadidas a la robustez para reportar hacen de él, la mejor opción para implementar un PBX basado en Asterisk.

Elastix integra varios paquetes de software, cada uno con su propio conjunto de características, añade nuevas interfaces para el control y reportes no disponibles por separado, lo que lo hace un paquete más completo que otras soluciones.

Algunas de las características provistas por Elastix son:

- Soporte para video porque se puede usar videollamadas (limitado a llamadas entre extensiones, no conferencias).
- Soporte para virtualización haciendo posible correr múltiples máquinas virtuales de Elastix sobre la misma PC.
- Interfaz Web para el usuario, realmente amigable.
- “Fax a email” para faxes entrantes, también se pueden enviar faxes desde su escritorio a través de una impresora virtual.
- Interfaz para tarificación, informes de llamadas entrantes/salientes y uso de canales.
- Configuración gráfica de parámetros de red y reportes de uso de recursos.
- Opciones para reiniciar/apagar remotamente.
- Módulo de buzones de voz integrados e Interfaz Web para buzones de voz.
- Sección de descargas con accesorios comúnmente usados.
- Interfaz de ayuda embebido y soporte multilinguaje.
- Servidor de mensajería instantáneo (Openfire) integrado.
- Servidor de correo integrado incluye soporte multidominio.
- Interfaz web para email.

1.3.1 Justificación Práctica (Escenario de Pruebas)

El escenario de pruebas será implementado en la Escuela Superior Politécnica de Chimborazo “ESPOCH”, como se muestra en la figura a continuación:

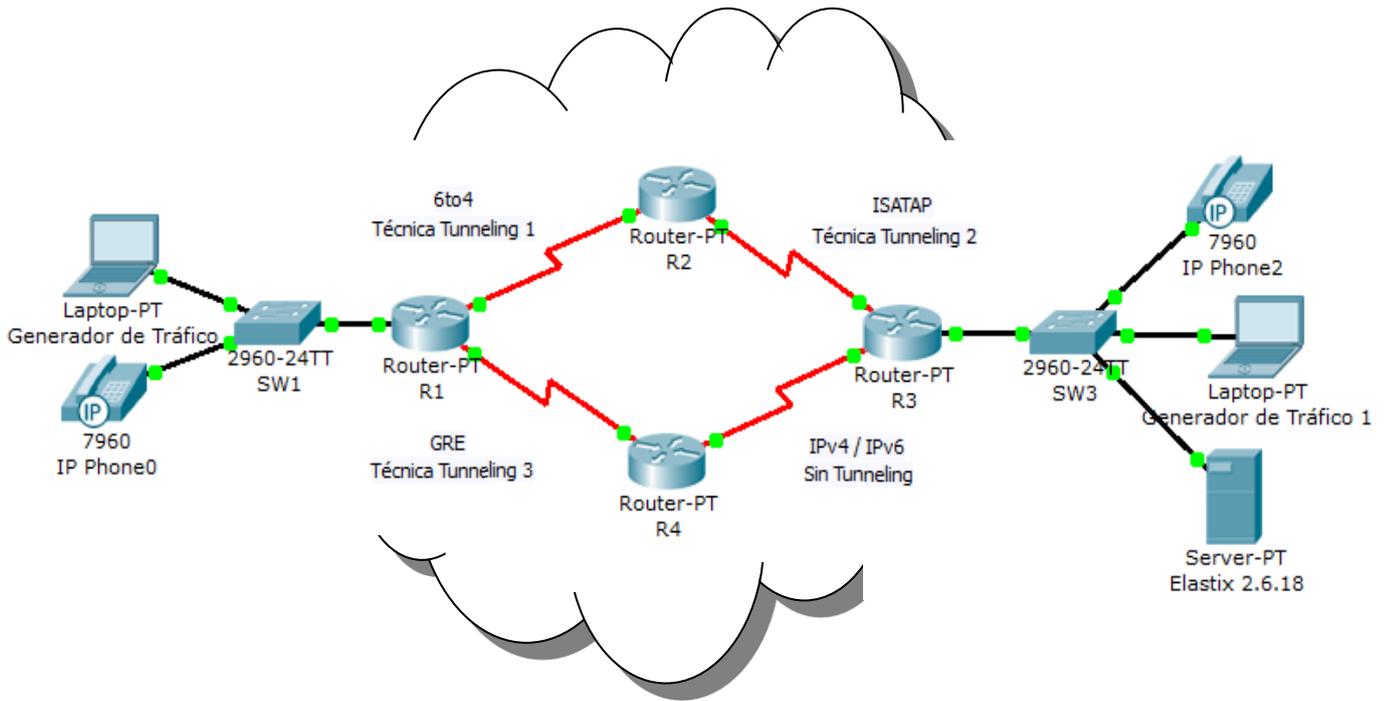


Figura 1: Escenario de Pruebas
Elaborado por: Jorge R. López O.

CAPITULO II

REVISIÓN DE LITERATURA

2.1 TELEFONÍA CONVENCIONAL VS. DIGITAL

2.1.1 Voz sobre IP

Como instituciones por lo menos debemos empezar a observar de cerca lo que se está ofreciendo en el mercado de VoIP. Es indudable que VoIP puede brindar enormes ahorros potenciales: menos cableado en edificios nuevos, una organización más flexible con agentes remotos y Centros de Contacto virtuales, mayor simplicidad de comunicación entre sitios, etc. Pero no podemos darnos el lujo de pasar por alto la tecnología de VoIP [4].

VoIP es una tecnología cada vez más utilizada y las empresas de telecomunicaciones están desarrollando diversos servicios tales como telefonía residencial y servicios de negocios, incluyendo servicios de interacción con el cliente.

Para lograr una ventaja competitiva, la mejor estrategia que una institución puede adoptar es dar la máxima prioridad a la satisfacción del cliente.

No cabe duda que las instituciones se están percatando del vínculo tan estrecho que existe entre excelencia en la interacción con el cliente y desempeño financiero. La solución idónea para las instituciones consistiría en crear un único Centro de Contacto que pudiera utilizar recursos humanos con total independencia de dónde se encuentren geográficamente.

Y es justo aquí, donde entra en juego VoIP. Sin embargo, al igual que con la mayoría de las cosas, para poder cosechar los beneficios hay que evitarse escollos y tropiezos.

A continuación se presentan recomendaciones sobre cómo elegir la configuración más adecuada:

a) *¿Cómo elegir a la institución más adecuada?*

Encontrar una institución que ofrezca toda la gama de servicios de negocios, incluyendo IP Centrex, Red Privada Virtual (VPN) multiservicios, Portal de Voz y Centro de Contacto.

En la actualidad son muy pocas las que ofrecen un espectro completo de servicios, pero el número va en aumento. No se requiere una inversión cuantiosa ya que en un futuro, la migración al modo cien por ciento IP será imperceptible.

b) ***¿Cuándo hacer la transición a VoIP?***

El mejor momento para migrar es cuando se esté considerando cambiar el sistema PBX. Existen varias opciones; se puede optar por un PBX IP, un IP Centrex o ambos. IP Centrex generalmente ofrece una mejor relación costo/beneficio, pues todos los recursos se encuentran en la red y no se requiere contar in situ con un PBX o PBX IP.

c) ***¿Se debe manejar la telefonía internamente o recurrir a un proveedor de servicios?***

En el esquema de outsourcing el proveedor de servicio se encarga de todos los aspectos técnicos que implica el mantenimiento del equipo y la red y, al colocar el Centro de Contacto en la red, puede compartir con todo el mundo los mismos recursos. De este modo se aprovecha mejor el tiempo del personal, se logra un enrutamiento y una distribución más eficientes y se reduce la inversión en equipos propios.

d) ***¿Qué quiere decir PBX, PBX IP o IP Centrex?***

- PBX: Equipo conmutador tradicional in situ que una institución utiliza para sus servicios de telefonía.
- PBX IP: Equipo conmutador in situ para telefonía IP.
- IP Centrex: Todos los servicios y recursos de conmutación para telefonía se encuentran en la red. Se requieren menos equipos in situ, los recursos se comparten entre varias instituciones o Centros de Contacto, hay mayor flexibilidad en los servicios y se abaratan los costos de operación.

e) **¿Cómo elegir un teléfono IP?**

El enfoque tradicional consiste en elegir primero al proveedor del PBX IP y usar el teléfono IP que venga incluido con el sistema (la situación con VoIP es muy distinta). Ahora que todos los PBX son “solamente” software, la mayor parte de los costos asociados a un nuevo sistema VoIP provienen de los teléfonos IP.

Los teléfonos IP son el único hardware que se tendrá que adquirir, y es muy probable que se los conserve a lo largo de toda la vida útil del sistema VoIP.

f) **Manos libres.**

Hay dos tipos de teléfonos a manos libres:

- Los teléfonos más sencillos implementan un control de eco “half dúplex”. Estos teléfonos simplemente “mutean” el micrófono hasta que se habla lo suficientemente fuerte. Es un método sencillo pero por desgracia muy molesto si se utiliza mucho el teléfono porque la otra persona de pronto dejará de escuchar incluso el ruido de fondo en cuanto se deje de hablar y tenderá a preguntarle si sigue en la línea.

- Los teléfonos más sofisticados cancelan el eco acústico, algo especialmente importante cuando se trata de una sala grande. En ocasiones se dice que estos teléfonos manejan una cancelación de eco “full dúplex”.

g) **Interfaces LAN.**

Cualquier teléfono IP o Gateway analógico tendrá por lo menos una interfaz LAN, pero es mejor tener dos. Así, se puede conectar uno de los puertos al conector Ethernet que ya está en la pared y el otro puerto a su PC. Esto permite ahorrar en cableado.

Por su naturaleza “arborescente”, la conectividad Ethernet requiere muchos menos cableado que la topología de “estrella” de las redes telefónicas tradicionales. En la mayoría de los casos el costo del sistema VoIP puede pagarse por completo si se considera que no necesitará ningún tipo de cableado telefónico.

h) **Cómo elegir un PBX IP.**

Anteriormente, muchos proveedores de PBX vendían PBX IP, que de hecho estaban diseñados sobre plataformas PBX tradicionales. Afortunadamente, son muy pocos los proveedores de PBX que aún ofrecen productos de este tipo.

Otro ejemplo, Elastix es una distribución libre de Servidor de Comunicaciones Unificadas que integra en un solo paquete (Ver **Figura 2**):

- VoIP PBX
- Fax
- Mensajería Instantánea
- Correo electrónico
- Colaboración

Elastix implementa gran parte de su funcionalidad sobre cuatro programas de software muy importantes como son Asterisk, Hylafax, Openfire y Postfix; y corre sobre CentOS como sistema operativo.

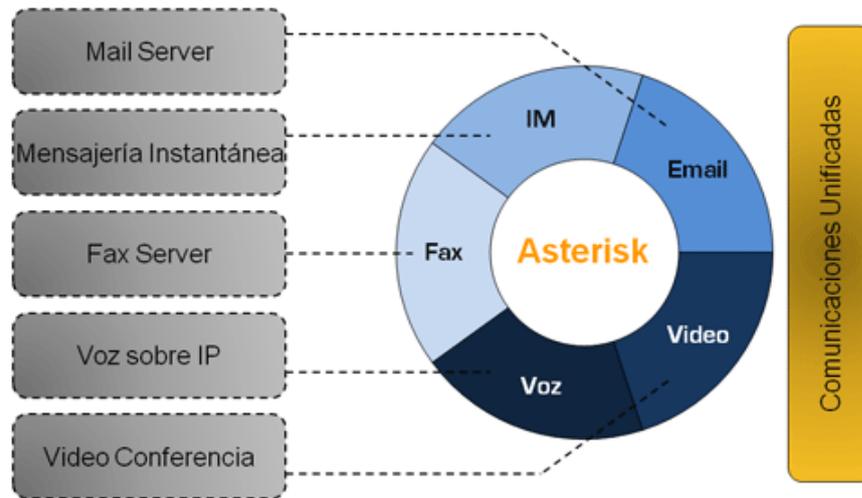


Figura 2: Diagrama de Elastix

Elaborado por: <http://www.elastix.org/index.php/es/informacion-del-producto/informacion.html>

2.2 IPv4 E IPv6

La innovación con IPv6 frente al agotamiento de IPv4, lo impulsó un único motivo “Más direcciones” para (Ver **Figura 3**):

- Miles de millones de nuevos dispositivos, como teléfonos celulares, PDAs, dispositivos de consumo, coches, etc.
- Miles de millones de nuevos usuarios, como China, India, etc.
- Tecnologías de acceso always-on, como xDSL, cable, Ethernet, etc.

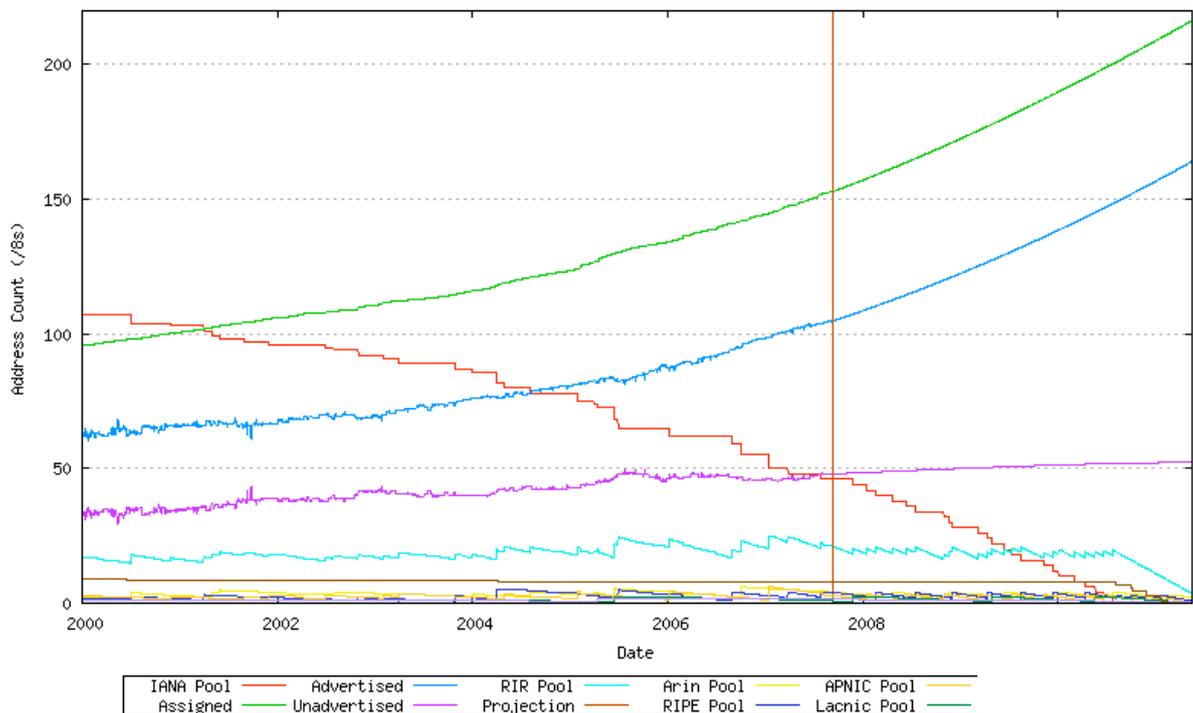


Figura 3: Situación actual direcciones IPv4 2010
Elaborado por: Consulintel. Jordi Palet Martínez⁴

2.2.1 Características principales

- Mayor espacio de direcciones. El tamaño de las direcciones IP cambia de 32 a 128 bits, para soportar más niveles de jerarquías de direccionamiento y nodos direccionables.
- Simplificación del formato de la cabecera. Algunos campos de la cabecera de IPv4 se quitan o se hacen opcionales.
- Paquetes IP eficientes y extensibles, sin que haya fragmentación en los routers, alineados a 64 bits y con una cabecera de longitud fija, más simple, que agiliza su procesado por parte del router.
- Posibilidad de paquetes con carga útil (datos) de más de 65.355 bytes.

⁴ Consulintel: jordi.palet@consulintel.es

- Seguridad en el núcleo del protocolo (IPsec). El soporte de IPsec es un requerimiento del protocolo IPv6.
- Capacidad de etiquetas de flujo. Puede ser usada por un nodo origen para etiquetar paquetes pertenecientes a un flujo de tráfico particular, que requieren manejo especial por los routers IPv6, tal como calidad de servicio no por defecto o servicios de tiempo real.
- Autoconfiguración de direcciones es más simple. Especialmente en direcciones Agregatable Global Unicast, los 64 bits superiores son seteados por un mensaje desde el router (Router Advertisement) y los 64 bits más bajos son seteados con la dirección MAC (en formato EUI-64). En este caso, el largo del prefijo de la subred es 64, por lo que no hay que preocuparse más por la máscara de red. Además el largo del prefijo no depende en el número de los hosts por lo tanto la asignación es más simple.
- Costos y multihoming facilitando el cambio de proveedor de servicios.
- Características de movilidad, la posibilidad de que un nodo mantenga la misma dirección IP.
- Ruteo más eficiente en el backbone de la red, debido a la jerarquía de direccionamiento basada en aggregation.
- Calidad de servicio (QoS) y clase de servicio (CoS).
- Capacidades de autenticación y privacidad.

2.2.2 Direccionamiento

Las direcciones son de 128 bits e identifican interfaces individuales o conjuntos de interfaces. Al igual que en IPv4 en los nodos se asignan a interfaces. Se clasifican en tres tipos:

- a) Unicast (identifican a una sola interfaz): Un paquete enviado a una dirección Unicast es entregado sólo a la interfaz identificada con dicha dirección.
- b) Anycast (identifican a un conjunto de interfaces): Un paquete enviado a una dirección anycast, será entregado a alguna de las interfaces identificadas con la dirección del conjunto al cual pertenece esa dirección anycast.
- c) Multicast (identifican un grupo de interfaces): Cuando un paquete es enviado a una dirección multicast es entregado a todas las interfaces del grupo identificadas con esa dirección.

En el IPv6 no existen direcciones broadcast, su funcionalidad ha sido mejorada por las direcciones multicast.

2.2.3 Representación de las direcciones

Existen tres formas de representar las direcciones IPv6 como strings de texto:

- a) x:x:x:x:x:x:x donde cada x es el valor hexadecimal de 16 bits, de cada uno de los 8 campos que definen la dirección. No es necesario escribir los ceros a la izquierda de cada campo, pero al menos debe existir un número en cada campo.

Ejemplos:

➡ FEDC:BA98:7654:3210:FEDC:BA98:7654:3210

➡ 1080:0:0:0:8:800:200C:417A

- b) Como será común utilizar esquemas de direccionamiento con largas cadenas de bits en cero, existe la posibilidad de usar sintácticamente :: para representarlos. El

uso de :: indica uno o más grupos de 16 bits de ceros. Dicho símbolo podrá aparecer una sola vez en cada dirección.

Por ejemplo:

- 1080:0:0:0:8:800:200C:417A (unicast address)
- FF01:0:0:0:0:0:0:101 (multicast address)
- 0:0:0:0:0:0:0:1 (loopback address)
- 0:0:0:0:0:0:0:0 (unspecified addresses)

Podrán ser representadas como:

- 1080::8:800:200C:417A (unicast address)
- FF01::101 (multicast address)
- ::1 (loopback address)
- :: (unspecified addresses)

- c) Para escenarios con nodos IPv4 e IPv6 es posible utilizar la siguiente sintaxis: x:x:x:x:x:d.d.d.d, donde x representan valores hexadecimales de las seis partes más significativas (de 16 bits cada una) que componen la dirección y las d, son valores decimales de los 4 partes menos significativas (de 8 bits cada una), de la representación estándar del formato de direcciones IPv4.

Ejemplos:

- 0:0:0:0:0:0:13.1.68.3
- 0:0:0:0:0:FFFF:129.144.52.38

O en la forma comprimida:

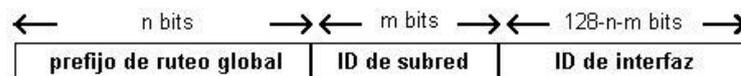
⇒ ::13.1.68.3

⇒ ::FFFF:129.144.52.38

2.2.4 Direcciones Global Unicast

Las direcciones unicast globales agregables basadas en el proveedor, son utilizadas para comunicaciones globales en todo Internet. Estas direcciones son semejantes a las direcciones IPv4 utilizando enrutamiento entre dominios sin clases CIDR (Classless Inter-Domain Routing).

Los tres primeros bits, correspondientes al prefijo son 101. El resto de la dirección la forman los siguientes campos, de longitud variable hasta hacer un total de 128 bits. El formato de las Direcciones Global Unicast.



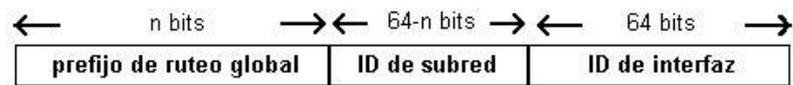
⇒ **Prefijo de ruteo global:** Es un prefijo asignado a un sitio, generalmente está estructurado jerárquicamente por los RIRs⁵ (Registro Regional de Internet) que incluyen direcciones IP (tanto IPv4 como IPv6) y números de sistemas autónomos (para su uso en encaminamiento BGP⁶) e ISPs⁷ (Proveedor de Servicios de Internet).

⁵ **RIR (Registro Regional de Internet o Regional Internet Registry)** es una organización que supervisa la asignación y el registro de recursos de números de Internet dentro de una región particular del mundo.

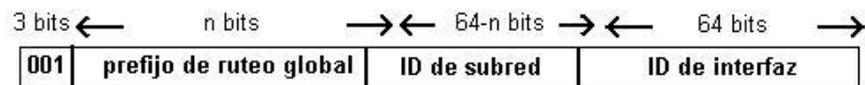
⁶ **BGP (Border Gateway Protocol)** es un protocolo mediante el cual se intercambia información de encaminamiento entre sistemas autónomos.

⁷ **ISP (Internet Service Provider)** es una empresa que brinda conexión a Internet a sus clientes.

- **Identificador de Subred:** Es el identificador de una subred dentro de un sitio. Está diseñado para que los administradores de los sitios lo estructuren jerárquicamente.
- **Identificador de Interfaz:** Es el identificador de una interfaz. En todas las direcciones Unicast, excepto las que comienzan con el valor binario 000, el identificador de interfaz debe ser de 64 bits y estar construido en el formato Modified EUI-64. El formato para este caso es el siguiente:



El siguiente es un ejemplo del formato de direcciones global Unicast bajo el prefijo 2000::/3 administrado por el IANA.



2.2.5 Mecanismos de transición básicos

Los mecanismos de transición son un conjunto de componentes y de protocolos implementados en hosts y routers, junto con algunas guías operativas de direccionamiento designadas para hacer la transición de Internet al IPv6 con la menor interrupción posible [2].

Uno de ellos es:

- ⇒ **Tunneling:** encapsula paquetes IPv6 dentro de la cabecera IPv4 siendo transportados a través de infraestructura de ruteo IPv4 (Ver **Figura 4**).

Dichos mecanismos están diseñados para ser usados por hosts y routers IPv6 que necesitan interoperar con hosts IPv4 y utilizar infraestructuras de ruteo IPv4. Se espera que muchos nodos necesitarán compatibilidad por mucho tiempo y quizás indefinidamente.

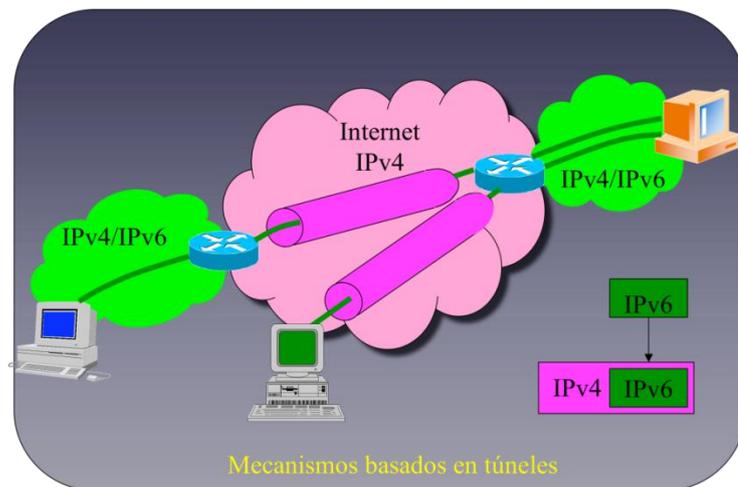


Figura 4: Mecanismos basados en Túneles
Elaborado por: Consultores Integrales de Comunicaciones Consulintel

No obstante, IPv6 también puede ser usado en ambientes donde no se requiere interoperabilidad con IPv4. Nodos diseñados para esos ambientes no necesitan usar ni implementar estos mecanismos.

2.3 COEXISTENCIA DE IPv4 A IPv6

IPv6 es una nueva versión de Protocolo de Internet, diseñada para suceder a la actual IPv4. La transición entre ambas será un largo proceso durante el que se ha de garantizar la coexistencia.

Para ello, IETF⁸ ha creado el NGTrans⁹ Working Group (Grupo de Trabajo de Transición de Próxima Generación). Los mismos que:

- Especifican los instrumentos y mecanismos que podrían utilizarse para la transición a IPv6.
- Redactan documentos que describen cómo las diferentes herramientas de transición y mecanismos podrían aplicarse a diversos escenarios para una transición a IPv6.
- Coordina con el banco de pruebas 6bone IPv6, que opera bajo el IPv6 (Testing Address Allocation allocated in Experimental RFC 2471), a fomentar el desarrollo, las pruebas y el despliegue de IPv6.
- Coordinar apropiadamente con IPv6 otras actividades relacionadas con el IETF y actividades de otras organizaciones.

2.3.1 Transición para la coexistencia

La transición no es sólo un proceso iniciado por el ISP y las redes de organizaciones.

De hecho, la mayoría de los sistemas operativos están disponibles con IPv6 activado por defecto y cada vez más aplicaciones hacen uso automático de IPv6 aun cuando no está disponible por parte del ISP o la red corporativa [3].

⁸ **IETF (Internet Engineering Task Force)** es una organización internacional abierta de normalización, que tiene como objetivos el contribuir a la ingeniería de Internet, actuando en diversas áreas, como transporte, encaminamiento, seguridad.

⁹ **NGTrans (Next Generation Transition)** Transición de Próxima Generación.

- Los clientes en los extremos de las redes comienzan a utilizar más y más aplicaciones con IPv6, de un modo transparente, como aplicaciones peer-to-peer y herramientas de colaboración.
- Para ello, pueden necesitar “terminadores de túneles” (TEP) y estos pueden estar situados fuera de la red su ISP
- Ello implica:
 - ⌘ Retardos adicionales
 - ⌘ Carga (pequeña) adicional por el encapsulado
 - ⌘ Intercambio (pequeño) adicional de paquetes Extra para la configuración del túnel y “keep-alives”
 - ⌘ Tránsito/ancho de banda adicional hasta el TEP y la vuelta hasta el “peer”, lo cual a su vez implicaría tránsito regional/nacional/internacional.
- La transición de los extremos ya es un coste para los ISPs, salvo que desplieguen mecanismos de transición “locales”.
- Por último, pero no menos importante, el valor de los clientes. Para lo cual se ha contemplado la pérdida de ingresos cuando los clientes perciban competidores que ofrecen un mejor servicio, porque han desplegado IPv6 nativo o servicios de transición.

*Por lo tanto: ¿dónde está IPv6? ¿Existe muy poco tráfico en los grandes ISPs?
Incorrecto, en realidad está en todas las redes (Ver **Figura 5 y 6**).*

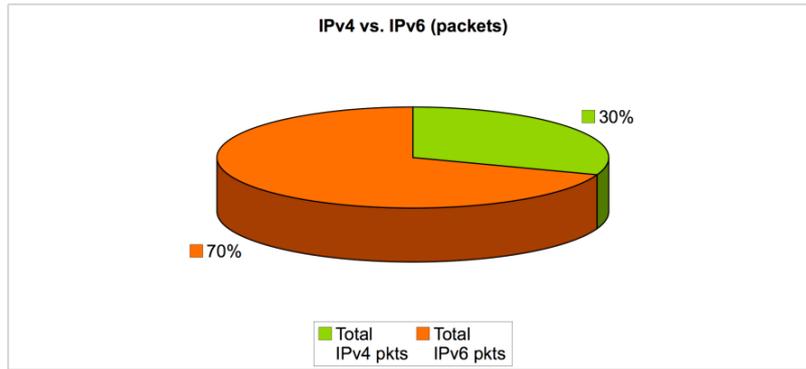


Figura 5: IPv4 vs. IPv6 (Paquetes)
Elaborado por: Consultores Integrales de Comunicaciones Consulintel

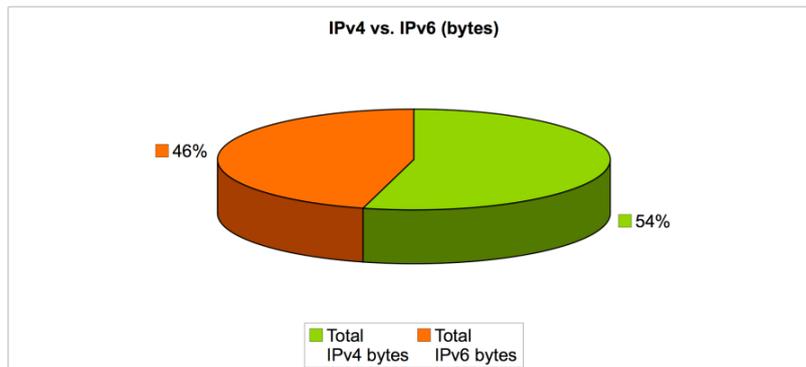


Figura 6: IPv4 vs. IPv6 (Bytes)
Elaborado por: Consultores Integrales de Comunicaciones Consulintel

La especificación IPv6 introduce en el Protocolo de Internet modificaciones fundamentales.

No sólo la longitud de la dirección IP ha sido extendida a 128 bits; también ha sido modificado el formato de la cabecera IP y el modo en el que se procesa la información que en ella está contenida.

Pasar de IPv4 a IPv6 no es sencillo y los mecanismos que permiten la coexistencia y la transición entre las dos versiones han de estar estandarizadas (Ver **Figura 7 y 8**).

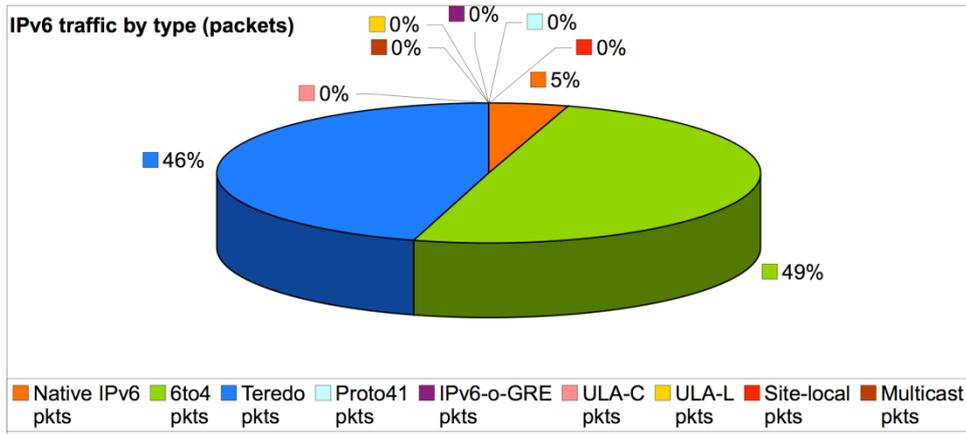


Figura 7: Tipos de Tráfico (Paquetes)

Elaborado por: Consultores Integrales de Comunicaciones Consulintel

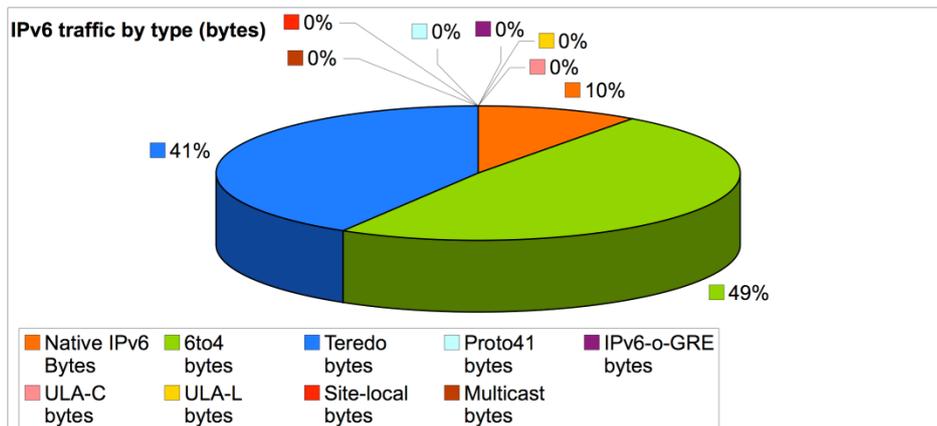


Figura 8: Tipos de Tráfico (Bytes)

Elaborado por: Consultores Integrales de Comunicaciones Consulintel

Hoy, cientos de millones de personas están conectadas a Internet y un número equivalente de hosts y dispositivos implementan el protocolo IP. El paso en un día D de IPv4 a IPv6, siguiendo el modelo del Año 2000, no sería práctico.

La migración al nuevo IP en tan corto periodo de tiempo, requeriría la redefinición de un plan de direccionamiento IPv6 mundial, la instalación del protocolo en cada router y host, y la modificación de las aplicaciones actuales para que puedan soportarlo.

Un proceso caro, sin duda, y que podría causar interrupciones del servicio inaceptables. Sencillamente, tal enfoque no tendría sentido, ya que muchas de las aplicaciones hoy operativas no han sido diseñadas para aprovechar las nuevas características de IPv6; ni siquiera las necesitan.

No hay una regla universal que pueda ser aplicada al proceso de transición de IPv4 a IPv6 (Ver **Figura 9** y **10**).

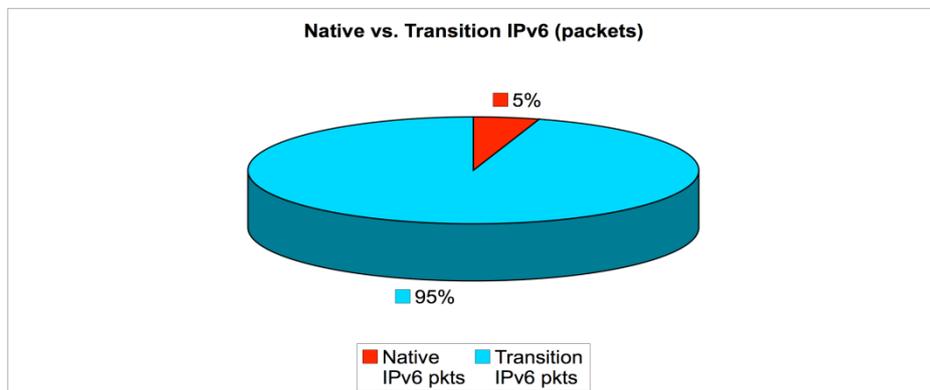


Figura 9: Nativo vs. Transición (Paquetes)
Elaborado por: Consultores Integrales de Comunicaciones Consulintel

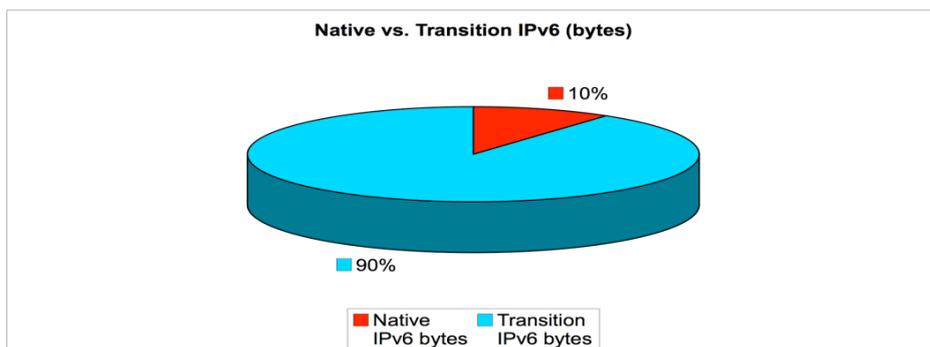


Figura 10: Nativo vs. Transición (Paquetes)
Elaborado por: Consultores Integrales de Comunicaciones Consulintel

En algunos casos, adoptar directamente, sin pasos previos, el nuevo IP será la única solución. Asimismo, se ha de desplegar a gran escala una nueva arquitectura IP para

proporcionar aplicaciones peer-to-peer y servicios innovadores. Pero otros planes de transición habrán de asegurar una interoperatividad gradual entre IPv4 e IPv6 a medida que evoluciona la transición. Es obvio, que los ISP y las empresas preferirán preservar las grandes inversiones realizadas en redes IPv4. Los mecanismos propuestos por el grupo NGTrans permitirán interconectar redes IPv4 e IPv6, así como servidores y clientes basados en ambas versiones.

Algunos estudios pronostican que el periodo de transición finalizará entre 2030-2040; en algún momento de esa década, las redes IPv4 deberían haber desaparecido totalmente. Una historia realmente larga comparada con el rápido crecimiento experimentado por Internet.

2.3.2 Implicaciones

En definitiva, se han definido muchos –quizá demasiados– mecanismos de transición ya maduros, que pueden ser combinadas de múltiples formas. En cualquier caso, siempre habrá que tener en cuenta las siguientes consideraciones [1]:

- **La transición no siempre es la solución.** Es importante tener presente que la transición no es la solución a todos los problemas. De hecho, algunas aplicaciones innovadoras necesitan IPv6 para su despliegue masivo. Desplegar mecanismos de transición a gran escala puede además implicar problemas de escalabilidad que podrían limitar enormemente el rendimiento de IPv6 en comparación una solución nativa. Esta es la razón principal por la que el proyecto 3GPP ha elegido IPv6.
- **Coexistencia de IPv4 e IPv6.** Allí donde los dos protocolos han de coexistir, es esencial mantener bajo control la transición para evitar el despliegue de dos

infraestructuras Internet paralelas. Las aplicaciones IPv6 se beneficiarán de las enormes inversiones realizadas en el despliegue de redes IPv4.

- **La transición no sólo afecta a IPv6.** IP no es una tecnología aislada, pues implica muchas interacciones con las tecnologías actuales y emergentes. Por ejemplo, resulta fundamental definir cómo transportar el tráfico IPv6 sobre una arquitectura MPLS¹⁰ a medida que el nuevo IP vaya consiguiendo beneficios directos de las mejoras introducidas en ese estándar.

- **Continuidad del servicio.** La transición de IPv4 a IPv6 no es sólo una cuestión de direcciones o de routing. Cualquiera que sea la infraestructura habrá que proporcionar progresivamente los nuevos servicios IPv4, como IP QoS, seguridad IP o telefonía IP.

- **Soluciones de conversión.** Los mecanismos de transición propuestos por NGTrans Working Group, implican la utilización de herramientas de ingeniería necesarias para definir estrategias de evolución. Y elegir los mecanismos más convenientes, y decidir dónde y cómo desplegarlos no es sencillo. Será preciso definir pautas y directrices que orienten al usuario durante el proceso de transición. Estas directrices describirían casos reales en función de proveedores, arquitecturas Internet y entornos LAN concretos.

- **Necesidad de servicio IPv6 y plataformas de transición.** ISPs y empresas necesitan soluciones capaces de gestionar eficientemente la transición a IPv6. Se han de proponer soluciones inteligentes en el punto de presencia, en el extremo de

¹⁰ **MPLS (Multiprotocol Label Switching)** es un mecanismo de transporte de datos estándar creado por la IETF y definido en el RFC 3031, opera entre la capa de enlace de datos y la capa de red del modelo OSI.

las infraestructuras cableadas o inalámbricas y en las instalaciones de las empresas para desplegar mecanismos de transición a gran escala y permitir el despliegue de servicios IPv6, tanto sobre las arquitecturas IPv4 actuales como sobre las IPv6 nativas.

- **Actividades de formación.** Se han de emprender actividades de formación específicas en el entorno de las compañías de telecomunicaciones y de los ingenieros de red a fin de difundir los mecanismos de transición y el modo de implementarlos eficientemente.

2.4 TÉCNICAS DE TUNNELING

El Tunneling de paquetes IPv6 sobre IPv4 es muy simple; el paquete IPv6 se encapsula en un datagrama IPv4 (que puede estar fragmentado). Hay dos clases de Tunneling de paquetes IPv6 sobre redes IPv4: automático y configurado (Ver **Figura 11**).

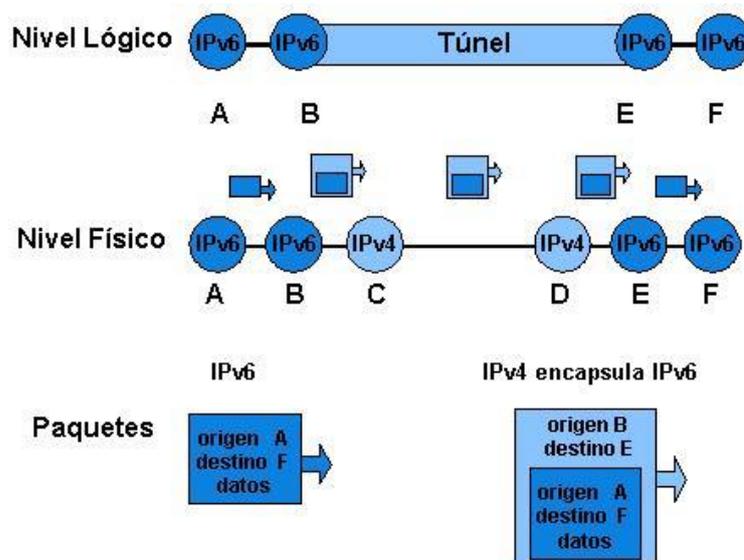


Figura 11: IPv6 vs. IPv4

Elaborado por: <http://www.rau.edu.uy/ipv6/queesipv6.htm#12>

2.4.1 Automático

Como el nombre indica, se realiza siempre que sea necesario. La decisión la toma un host IPv6/IPv4 que tiene un paquete que enviar a través de un área de tipo IPv4-complete, y sigue las siguientes reglas:

- Si el destino es una dirección mapeada a IPv4, envía el paquete usando IPv4 ya que el receptor no soporta IPv6. En otro caso:
- Si el destino se halla en la misma subred, lo envía usando IPv6, ya que el receptor soportará IPv6.
- Si el destino no se halla en la misma subred pero en ella hay al menos un router por defecto que soporta IPv6, o existe una ruta configurada para un router de este tipo, el paquete se le envía a este router mediante IPv6. En otro caso:
- Si la dirección es compatible con IPv4, el paquete se envía usando Tunneling automático. En otro caso:
- El destino es un nodo sólo IPv6 conectado a un área tipo IPv4-complete que no sea IPv6-complete y es por tanto inaccesible.

La dirección IP debe ser compatible con IPv4 para que se pueda usar Tunneling. Las direcciones sólo IPv6 no son susceptibles de ser usadas ya que no se las puede direccionar con IPv4.

Los paquetes de nodos IPv6/IPv4 a direcciones mapeadas a IPv4 no se tunelizan ya que se refieren a nodos sólo IPv4.

Las reglas anteriores enfatizan el uso de un router IPv6 con preferencia al Tunneling por tres razones:

- ⇒ Hay menos overhead ya que no existe encapsulación con cabeceras IPv4.
- ⇒ Sólo están disponibles características de IPv6.
- ⇒ La topología de encaminamiento IPv6 se usará desde su instalación, preferentemente a la de IPv4.

2.4.2 Configurado

Se utiliza para realizar Tunneling host-router o router-router de IPv6-sobre-IPv4. El host emisor o el router retransmisor se configuran de tal forma que la ruta, además de contar con el siguiente salto, tiene una dirección de fin de túnel (que es siempre compatible con IPv4 ya que se debe tratar de un host IPv6/IPv4 accesible desde un área IP-completa).

El proceso de encapsulación es el mismo que en modo automático exceptuando que la dirección IPv4 de destino no se calcula de los 32 bits inferiores de cuando el router del fin del túnel recibe el datagrama, lo procesa como lo haría un nodo que estuviera al final de un túnel automático.

Cuando el paquete IPv6 original pasa a la capa IPv6 del router, este reconoce que no es el destinatario y lo retransmite como lo haría con cualquier paquete IPv6. Puede ocurrir, por supuesto, que tras emerger de un túnel, el paquete entre de nuevo en otro.

CAPITULO III

MATERIALES Y MÉTODOS

La metodología de la investigación proporciona una serie de herramientas teórico-prácticas para la solución de problemas. Estos conocimientos representan una actividad de racionalización del entorno académico y profesional fomentando el desarrollo intelectual a través de la investigación sistemática de la realidad.

La metodología del proyecto incluye el tipo o tipos de investigación, las técnicas y los procedimientos que serán utilizados para llevar a cabo la indagación del Análisis de las Técnicas de Tunneling, para la coexistencia de IPv4 e IPv6 que brinde soporte a tráfico de VoIP. Es el “cómo”, se realizará el estudio para responder al problema planteado.

3.1 DISEÑO DE LA INVESTIGACIÓN

La investigación de este proyecto de tesis llevará a cabo un diseño **Cuasi-experimental**, debido a que la información enviada no será elegida al azar, sino más

bien se tendrá definida junto con los escenarios de prueba y se manipulará al menos una variable independiente. Por medio de este tipo de investigación se puede aproximar a los resultados de una investigación experimental en situaciones en las que no es posible el control y manipulación absolutos de las variables. Además, que es apropiada en situaciones naturales, en que no se pueden controlar todas las variables de importancia.

3.2 TIPO DE ESTUDIO

La naturaleza de este proyecto de tesis determina que su investigación será:

- **Descriptiva:** Debido a que se profundizará en el conocimiento de las técnicas de Tunneling para la coexistencia de IPv4 a IPv6 que brinde soporte a tráfico VoIP. Por lo tanto, los estudios descriptivos se centran en recolectar datos que describan la situación tal y como es. Desde el punto de vista científico, describir es medir.

- **De Laboratorio:** Porque se utilizará el conocimiento conceptual para realizar una guía de implementación de IPv4 a IPv6, con la finalidad de determinar su coexistencia por medio de las técnicas de Tunneling, dirigida al desarrollo tecnológico. Los estudios de laboratorio nos ayudan no sólo al diagnóstico, sino que en muchos casos al tratamiento del proceso.

3.3 POBLACIÓN Y MUESTRA

En el proceso investigativo, la población corresponde al conjunto de referencia sobre el cual se va a desarrollar el estudio y se harán extensivas las conclusiones del

análisis investigativo. La muestra para este proceso investigativo va a ser un subconjunto de la población; muestra que será representativa recogiendo todas las características relevantes de la población.

3.3.1 Población

De acuerdo al Networked Readiness Index (NRI)¹¹ del Foro Económico Mundial, que mide la capacidad de los países de aprovechar las oportunidades de las Tecnologías de la Información y de las Comunicaciones (TIC), en 2012 Ecuador se ubica en el puesto 96 de 142 naciones consideradas, con un índice de 3,46 sobre un máximo de 7.

Esto muestra que, pese a los avances conseguidos, aún falta mucho por hacer. Al analizar el indicador vemos que requerimos de iniciativas que potencien y mejoren servicios en línea que se vuelvan más eficaces y eficientes para los usuarios. Así nace la iniciativa de implementar el Centro Nacional de Datos de Ecuador, por la transversalidad e impacto que tiene un proyecto así en el desarrollo de servicios de gobierno centrados en los usuarios¹². En definitiva, la población para este trabajo investigativo, serán todas las redes existentes a nivel mundial y particularmente las que han sido y son instaladas, configuradas, administradas, monitoreadas y evaluadas en el Ecuador.

Cabe mencionar, que existen varias técnicas de Tunneling las mismas que son: 6to4, ISATAP, GRE, Tunneling manual de IPv6 a IPv4, Teredo, Proto41.

¹¹ **NRI (Networked Readiness Index)** mide de la propensión de los países a aprovechar las oportunidades que ofrecen las tecnologías de información y comunicaciones. Se publica anualmente y busca comprender mejor el impacto de las TIC en la competitividad de las naciones.

¹² <http://www.eclac.org/socinfo/noticias/paginas/3/44733/newsletter19.pdf>

3.3.2 Muestra

En el presente trabajo investigativo se empleará un **Muestreo Dirigido o Intencional**, porque si bien pertenece al muestreo no probabilístico intentaremos que la muestra tenga representatividad para determinar la Técnica de Tunneling más adecuada, para la coexistencia de IPv4 e IPv6 que brinde soporte a tráfico de VoIP.

Además, se considerará aspectos como:

- Costos reducidos.
- Considerable rapidez para obtener resultados.
- Mayor exactitud o mejor calidad de la información debido a:
 - ☞ Volumen de trabajo proporcional al requerido.
 - ☞ Puede existir mayor supervisión en el trabajo.
 - ☞ Se dispone de personal más capacitado.
 - ☞ Menor probabilidad de cometer errores, durante el procesamiento de la información.

Las Técnicas de Tunneling escogidas para el desarrollo del análisis de investigación son:

- 6to4
 - ISATAP
 - GRE
- } Soporte Cisco Certificado. Ver **Figura 12**.

Sin embargo, se realizará un análisis adicional, utilizando la infraestructura creada con:

- IPv4
- IPv6

Todas estas técnicas, serán implementadas en el Laboratorio de Cisco, de la Escuela Superior Politécnica de Chimborazo “ESPOCH”. (Ver Figura 1).



Figura 12: Escuela Superior Politécnica de Chimborazo-Academia Cisco
Elaborado por: <http://www.espoch.edu.ec/index.php?action=programas&id=1>

3.4 MÉTODOS, TÉCNICAS, FUENTES DE INFORMACIÓN E INSTRUMENTOS

3.4.1 Métodos

Los Métodos de Investigación que se emplearán en este proyecto de tesis serán:

- **Método Científico:** Es un proceso destinado a explicar fenómenos, establecer relaciones entre los hechos y enunciar leyes que expliquen los fenómenos físicos del mundo y permitan obtener, con estos conocimientos, aplicaciones útiles al hombre. ¡Sin Ciencia no hay Cultura!

Las ideas, conceptos y teorías expuestas en este proyecto de tesis son verificables, a través de una serie ordenada de procedimientos, que nos permitirá recopilar la información necesaria para determinar el grado de coexistencia de IPv4 a IPv6 que brinde soporte a tráfico VoIP. Las etapas de este método serán:

- ↻ Planteamiento del problema
- ↻ Formulación de hipótesis
- ↻ Levantamiento de información
- ↻ Análisis e interpretación de resultados
- ↻ Comprobación de la hipótesis
- ↻ Difusión de resultados

- **Método Deductivo:** Debido que al realizar la investigación en forma general la coexistencia de IPv4 a IPv6 mediante la utilización de técnicas de Tunneling, nos permitirá determinar la que brinde el mejor soporte a tráfico de VoIP.

- **Método Comparativo:** Debido a que se compara y se establece las características de cada una de las Técnicas de Tunneling, para determinar el grado de coexistencia de IPv4 a IPv6 que brinde soporte a tráfico VoIP.

- ⇒ **Método de Análisis y Síntesis:** Es un método que consiste en la separación de las partes de un todo para estudiarlas en forma individual (análisis) y la reunión racional de elementos dispersos para estudiarlos en su totalidad (síntesis). En esta investigación se considera las Técnicas de Tunneling para determinar el grado de coexistencia de IPv4 a IPv6 que brinde soporte a tráfico VoIP.

3.4.2 Técnicas

Las técnicas empleadas en este proyecto de investigación se detallan a continuación:

- ⇒ Observación
- ⇒ Razonamiento
- ⇒ Recopilación de información.
- ⇒ Comparación de escenarios.
- ⇒ Análisis
- ⇒ Pruebas

3.4.3 Fuentes de Información

- ⇒ Libros
- ⇒ Documentos de Internet
- ⇒ Tesis de Grado
- ⇒ Wireshark versión 1.8.4
- ⇒ Artículos científicos.
- ⇒ Revistas especializadas

3.4.4 Bibliográficos

Los materiales bibliográficos que se explotarán de manera eficiente en este trabajo investigativo, serán aquellos que nos permitan implementar y analizar las técnicas de Tunneling (6to4, ISATAP, GRE/IPv6) referidas en libros, documentos de Internet, Tesis de Grado, artículos científicos y revistas especializadas. Con esto, podremos establecer una propuesta de coexistencia entre IPv4 e IPv6 que brinde soporte a tráfico VoIP con Técnicas de Tunneling.

3.5 VALIDACIÓN DE INSTRUMENTOS

Los instrumentos empleados para el desarrollo del presente trabajo investigativo son:

3.5.1 Wireshark 1.2.8 (SNV) Rev. 32676

Wireshark, uno de los analizadores de protocolos de red más populares, usado para solución de problemas, análisis, desarrollo y educación. Es una herramienta que sirve para desarrollar y depurar protocolos y aplicaciones, tras capturar diversas tramas de red en tiempo real o analizando un archivo previamente capturado.

Admite el formato estándar tcpdump añadiendo interfaz gráfica y múltiples opciones de organización y filtrado de información que soporta más de 480 protocolos. Wireshark es software libre y multiplataforma (soportando hasta 20 plataformas) con versiones para Windows, Mac OS X, Linux o Unix¹³.

¹³ <http://muyseguridad.net/2012/06/23/wireshark-1-8-0-nueva-version-analizador-protocolos-libre/>

3.5.2 Cuestionario

La encuesta se realiza siempre en función de un cuestionario, siendo éste por tanto, el documento básico para obtener la información en la gran mayoría de las investigaciones y estudios de mercado. El cuestionario es un documento formado por un conjunto de preguntas que están redactadas de forma coherente, organizadas, secuenciadas y estructuradas. Este cuestionario, lo podemos observar detenidamente en el **Anexo 12**.

3.6 PROCESAMIENTO DE LA INFORMACIÓN

El procedimiento realizado en el presente trabajo investigativo, cuenta con las siguientes etapas de desarrollo:

- a) Recopilación de la información necesaria y requerida.
- b) Presentación de una propuesta técnica hardware y software.
- c) Análisis de fortalezas y debilidades (mejoras hardware y software) [5].
- d) Ajuste de la propuesta (Topología de la red).
- e) Elaboración de un presupuesto y cronogramas de ejecución.
- f) Diseño de la red.
- g) Elección de la PBX más adecuada (Elastix).
- h) Analizar las técnicas de Tunneling (6to4, ISATAP, GRE/IPv6) que permitan la selección y coexistencia entre IPv4 e IPv6 [6].
- i) Implementar los escenarios de prueba respectivos.
- j) Determinar las diferentes métricas de comprobación.

- k) Evaluar la mejor técnica de Tunneling que permita determinar el mejor grado de coexistencia y QoS para transmitir VoIP en los escenarios propuestos [7].
- l) Elaboración de una guía de implementación de coexistencia de IPv4 e IPv6 (utilización de la técnica de Tunneling más adecuada) [8].
- m) Presentación del proyecto investigativo.

3.7 PLANTEAMIENTO DE LA HIPÓTESIS

Mediante el análisis de las técnicas de Tunneling, se logrará determinar el mecanismo más adecuado de coexistencia de IPv4 e IPv6, que brinde soporte a tráfico de VoIP.

3.7.1 Tipo de Hipótesis

- ⇒ Hipótesis que establece relaciones de causalidad.

3.8 DETERMINACIÓN DE VARIABLES

3.8.1 Operacionalización de Variables

TABLA I: Operacionalización de Variables
Elaborado por: Jorge R. López O.

Variable	Tipo	Concepto
Problemas de coexistencia entre IPv4 e IPv6 que brinde soporte a tráfico de VoIP.	Independiente	<ul style="list-style-type: none">⇒ Introducción del IPv6 en los actuales sistemas de información y comunicaciones basados en IPv4.⇒ Fase de coexistencia: IPv4-IPv6.⇒ Extinción del IPv4.⇒ Redes y sistemas sólo con IPv6.
Coexistencia de IPv4 a IPv6, utilizando Técnicas de Tunneling	Dependiente	<ul style="list-style-type: none">⇒ La técnica de Tunneling consiste en encapsular un protocolo de red sobre otro (protocolo de red encapsulador) creando un túnel dentro de una red de computadoras.⇒ Existencia simultánea o convivencia de dos o más entidades.

3.8.2 Operacionalización Metodológica

TABLA II: Operacionalización Metodológica
Elaborado por: Jorge R. López O.

<i>Variable</i>	<i>Indicadores</i>	<i>Índices</i>	<i>Técnica</i>	<i>Fuente de verificación / Instrumentos</i>
Variable Independiente Problemas de coexistencia entre IPv4 e IPv6 que brinde soporte a tráfico de VoIP	➤ Agotamiento de direcciones IP	➤ Direcciones IPv4 ➤ Direcciones IPv6	➤ Observación ➤ Razonamiento ➤ Recopilación de información ➤ Comparación de escenarios ➤ Análisis ➤ Pruebas	➤ Libros ➤ Documentos de Internet ➤ Artículos científicos ➤ Revistas especializadas
	➤ Rendimiento	➤ Jitter ➤ Ancho de Banda ➤ Latencia	➤ Observación ➤ Razonamiento ➤ Recopilación de información ➤ Comparación de escenarios ➤ Análisis ➤ Pruebas	➤ Documentos de Internet ➤ Wireshark versión 1.8.4 ➤ Artículos científicos
<i>Variable</i>	<i>Indicadores</i>	<i>Índices</i>	<i>Técnica</i>	<i>Fuente de verificación / Instrumentos</i>
Variable Dependiente Coexistencia de IPv4 a IPv6, utilizando Técnicas de Tunneling (6to4, ISATAP, GRE).	➤ Rendimiento	➤ Jitter ➤ Ancho de Banda ➤ Latencia	➤ Observación ➤ Razonamiento ➤ Recopilación de información. ➤ Comparación de escenarios ➤ Análisis ➤ Pruebas	➤ Documentos de Internet ➤ Wireshark versión 1.8.4 ➤ Artículos científicos ➤ Revistas especializadas
	➤ Facilidad de instalación	➤ Tiempo ➤ Dificultad	➤ Observación ➤ Encuesta ➤ Análisis	➤ Cuestionario ➤ Libros ➤ Tesis de Grado ➤ Artículos científicos
	➤ Número de Paquetes RTP	➤ Paquetes Tx. ➤ Paquetes Perdidos	➤ Observación ➤ Razonamiento ➤ Recopilación de información. ➤ Comparación de escenarios ➤ Análisis ➤ Pruebas	➤ Wireshark versión 1.8.4

3.9 AMBIENTES DE PRUEBA

Las instituciones tienen la necesidad de crear ambientes para desarrollar y probar aplicaciones ya sean adquiridas o como parte de una renovación tecnológica reciente.

Este tipo de ambientes, por su naturaleza, requieren de pocas exigencias de alta disponibilidad, pero cada aplicación o prueba puede necesitar una gran cantidad de recursos de TI. Las soluciones de nube para desarrollo y pruebas pueden tener una serie de matices dependiendo del tamaño y las necesidades con la capacidad de consumir recursos de TI virtualizados en un ambiente que sea altamente elástico.

La topología de red definida para intercambiar datos es la misma para todos los escenarios de prueba (determina únicamente la configuración de las conexiones entre nodos). La distancia entre los nodos, las interconexiones físicas, las tasas de transmisión y los tipos de señales no pertenecen a la topología de la red, aunque pueden verse afectados por la misma. El software y hardware empleado en todos los Escenarios de Prueba, se lo describe a continuación.

3.9.1 Software

a) Elastix versión 2.6.18-238.12.1.e15

Software de código abierto para el establecimiento de comunicaciones unificadas (autenticación y acceso) con el objetivo de incorporar en una única solución todos los medios y alternativas de comunicación.

Elastix es la unificación de varios paquetes libres a manera de Servidor de Comunicaciones Unificadas que integra en un solo paquete: VoIP PBX, fax, mensajería instantánea, correo electrónico, etc.

Además, suma a su funcionalidad cuatro programas software: Asterisk (PBX), Hylafax (fax), Openfire (Mensajería) y Postfix (Correo electrónico)¹⁴.

b) VMware Station 9.0.1-894247

VMware es un sistema de virtualización que simula un sistema físico (Central Telefónica) con unas características de HW determinadas y proporciona un ambiente de ejecución similar a PBX para VoIP.

Distinguido con más de 50 premios del sector, el software VMware Workstation goza de reconocimiento por su amplia compatibilidad con sistemas operativos, la experiencia óptima que ofrece al usuario, la completa funcionalidad y su alto rendimiento. Es el compañero perfecto para cualquier profesional técnico que valora las aplicaciones creadas por ingenieros para ingenieros¹⁵.

VMware Workstation proporciona una forma transparente de acceder a todas las máquinas virtuales necesarias, al margen del dispositivo donde se ejecuten. La interfaz web de Workstation permite acceder a las máquinas virtuales locales y alojadas en servidores desde el PC, un smartphone, una tableta o cualquier dispositivo que tenga un navegador moderno.

¹⁴ <http://www.slideshare.net/jarvey4/elastic-como-solucion-asterisk>

¹⁵ http://www.vmware.com/es/products/desktop_virtualization/workstation/overview.html

c) CentOS release 5.7

CentOS (Community ENTerprise Operating System) es una distribución Linux basada completamente en el código fuente de Red Hat Linux, una de las distribuciones más utilizadas en servidores alrededor del mundo, pues la compañía que la desarrolla llamada también Red Hat es líder en cuanto al soporte corporativo se refiere, ofreciendo tranquilidad a las compañías que optan por utilizar Linux en sus empresas ya sea a nivel de servidor o de usuario¹⁶. Además, podemos mencionar que será la base para funcionamiento de la versión de Elastix antes mencionada.

d) Jitsi 1.0-build.3967

Jitsi es un softphone que tiene una gran variedad de características, incluyendo soporte para llamadas de voz y video, chat / mensajería instantánea, compartición de escritorio, llamadas de conferencia, audio de banda ancha y mucho más.

Es compatible con varios protocolos populares de mensajería instantánea y de telefonía.

Adicionalmente simulará a un teléfono IP instalado en una PC. Funciona con el SIP (Session Initiation Protocol), los protocolos XMPP (Jabber) y se conecta a los servicios comunes, como GoogleTalk, AIM, Yahoo! Messenger, Facebook chat, etc.

También es libre y el código fuente está todo disponible¹⁷.

¹⁶ <http://emslinux.com/servidor-centos/>

¹⁷ <http://www.internetsociety.org/deploy360/blog/2012/04/jitsi-is-the-first-voip-softphone-to-support-dnssec/>

3.9.2 Hardware

El equipamiento Hardware será determinado luego de identificar los medios de red requeridos para implementar los diferentes escenarios de prueba, considerando lo siguiente:

- Conexión LAN
 - ☞ Comprobar los tipos de conexiones para los dispositivos finales e intermediarios.
 - ☞ Configurar el diagrama de pines para cables cruzados, directos, puertos, estándares y tipos de cableado.
- Conexión WAN
 - ☞ Administrar dispositivos Cisco.
 - ☞ Designar un esquema de direccionamiento para una infraestructura de red y asignar rangos para los hosts, los dispositivos de red y las interfaces del router.
- Determinar la importancia del diseño de la red.

No obstante, cabe mencionar que los equipos utilizados en la implementación se muestran claramente en la **Figura 1** y los mismos son:

- Router Cisco 2811
- Switch Cisco 2960
- Servidor PBX Elastix 2.6.18
- Teléfonos IP
- Softphone Jitsi 1.0
- Portátiles HP
- Cables seriales y UTP cat. 5e

Además, se debe considerar factores como:

- Costo y redundancia
- Velocidades y tipos de puertos e interfaces
- Expandible / Modular (capacidad de expansión y características del IOS)
- Administrable
- Entre otros.

3.9.3 Notas Aclaratorias

a) Para conocer las configuraciones implementadas en todos los Escenarios de Prueba propuestos en el presente trabajo investigativo, se sugiere ver el **Anexo 1**.

Las configuraciones descritas son las siguientes:

- ✓ IPv4 puro
 - ✓ IPv6 puro
 - ✓ Técnica de Tunneling 6to4
 - ✓ Técnica de Tunneling ISATAP
 - ✓ Técnica de Tunneling GRE
- } Soporte Cisco Certificado

b) Para comprobar el correcto funcionamiento de los distintos Escenarios de Prueba implementados, se muestra el Cliente Telnet empleado, así:

- ✓ IPv4 puro (ver **Anexo 2**)
- ✓ IPv6 puro (ver **Anexo 3**)
- ✓ Técnica de Tunneling 6to4 (ver **Anexo 4**)
- ✓ Técnica de Tunneling ISATAP (ver **Anexo 5**)
- ✓ Técnica de Tunneling GRE (ver **Anexo 6**)

- c) Wireshark es utilizado para realizar el análisis respectivo de lo anteriormente mencionado y lograr solucionar problemas que se presentaron a lo largo de la investigación.

Al añadir una interfaz gráfica y muchas opciones de organización y filtrado de información, podemos ver todo el tráfico que pasa a través de una red. En tal virtud, se propone revisar las capturas de tráfico conseguidas con esta herramienta de red.

- ✓ Wireshark Pruebas IPv4 puro (ver **Anexo 7**)
- ✓ Wireshark Pruebas IPv6 puro (ver **Anexo 8**)
- ✓ Wireshark Pruebas Técnica de Tunneling 6to4 (ver **Anexo 9**)
- ✓ Wireshark Pruebas Técnica de Tunneling ISATAP (ver **Anexo 10**)
- ✓ Wireshark Pruebas Técnica de Tunneling GRE (ver **Anexo 11**)

3.9.4 Escenario de Prueba solo IPv4

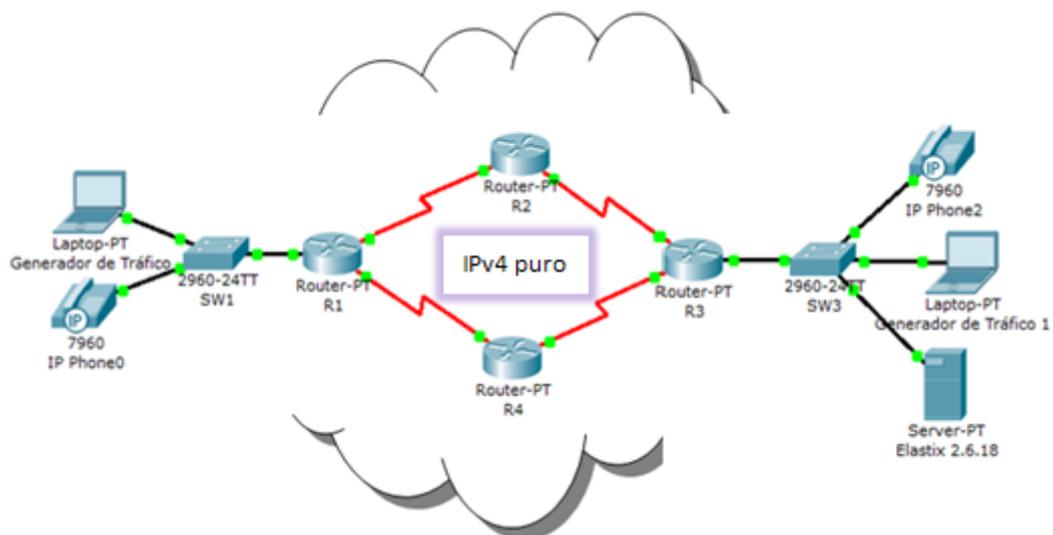


Figura 13: IPv4 puro
Elaborado por: Jorge R. López O.

El Protocolo de Internet versión 4 (IPv4) es la cuarta versión del Protocolo de Internet (IP), y la primera en ser implementada a gran escala. Definida en el RFC 791. IPv4 usa direcciones de 32 bits, limitándola a $2^{32} = 4.294.967.296$ direcciones únicas, muchas de las cuales están dedicadas a redes locales. Por el crecimiento enorme que ha tenido Internet (mucho más de lo que esperaba, cuando se diseñó IPv4), combinado con el hecho de que hay desperdicio de direcciones en muchos casos, ya hace varios años se vio que escaseaban las direcciones IPv4.

Esta limitación ayudó a estimular el impulso hacia IPv6, que está actualmente en las primeras fases de implantación, y se espera que termine reemplazando a IPv4. Las direcciones disponibles en la reserva global de IANA pertenecientes al protocolo IPv4 se agotaron el jueves 3 de Febrero de 2011 oficialmente. Los Registros Regionales de Internet deben, desde ahora, manejarse con sus propias reservas. Actualmente no quedan direcciones IPv4 disponibles para compra, por ende se está en la forzosa y prioritaria obligación de migrar a IPv6.

3.9.5 Escenario de Prueba solo IPv6

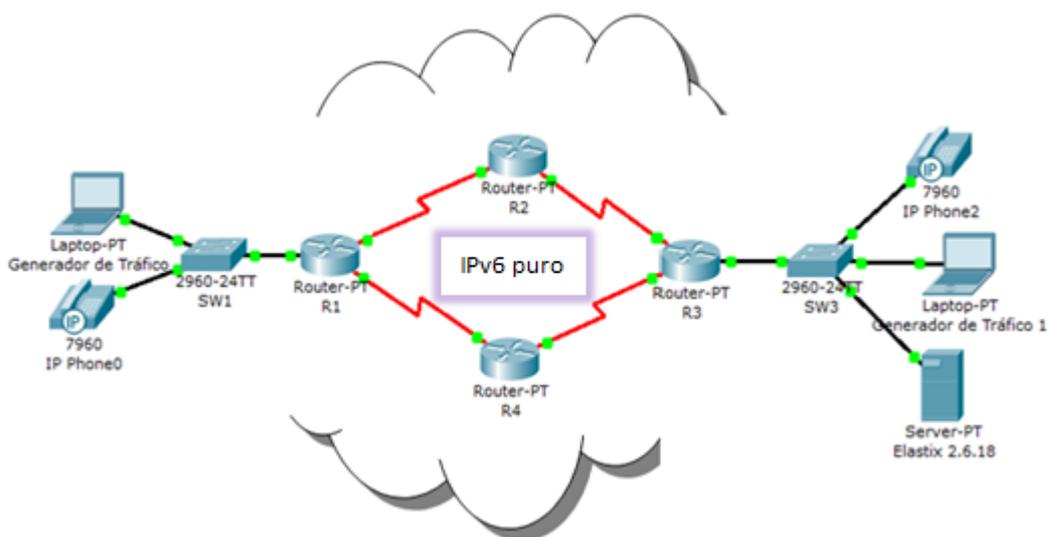


Figura 14: IPv6 puro
Elaborado por: Jorge R. López O.

El Protocolo de Internet versión 6 (IPv6) es una versión del Protocolo de Internet (IP), definida en el RFC 2460 y diseñada para reemplazar a IPv4 RFC 791, que actualmente está implementado en la gran mayoría de dispositivos que acceden a Internet.

IPv6 especifica un nuevo formato de paquete, diseñado para minimizar el procesamiento del encabezado de paquetes. Debido a que las cabeceras de los paquetes IPv4 e IPv6 son significativamente distintas, los dos protocolos no son interoperables.

3.9.6 Escenario de Prueba Tunneling 6to4

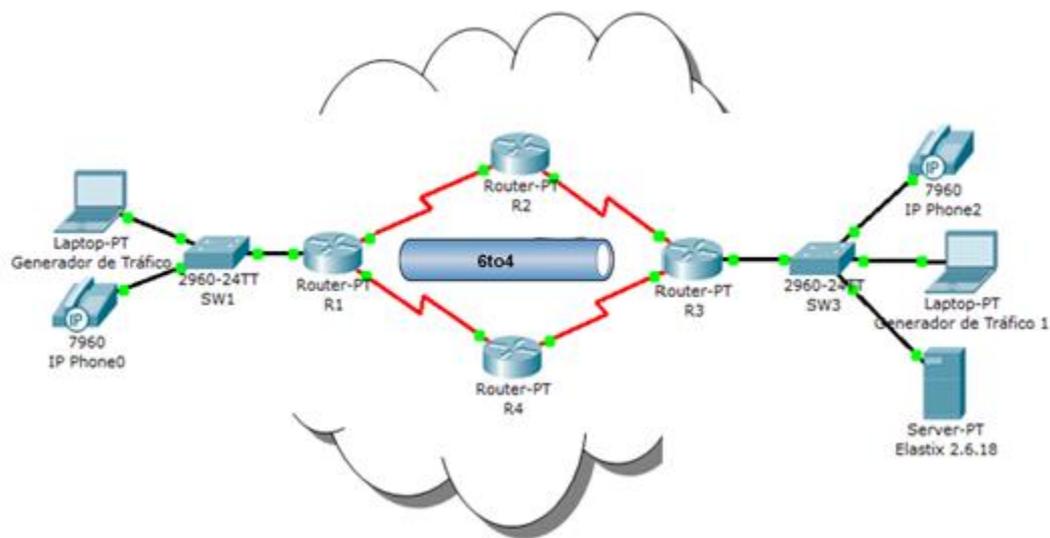


Figura 15: Técnica Tunneling 6to4
Elaborado por: Jorge R. López O.

6to4 es un mecanismo túnel utilizado para transferir paquetes de IPv6 (Protocolo de Internet versión 6) sobre una infraestructura IPv4, por lo general la red Internet IPv4. El mecanismo de 6to4 fue creado para apoyar la coexistencia de ambas versiones durante la transición a IPv6, que va a tomar años.

3.9.7 Escenario de Prueba Tunneling ISATAP

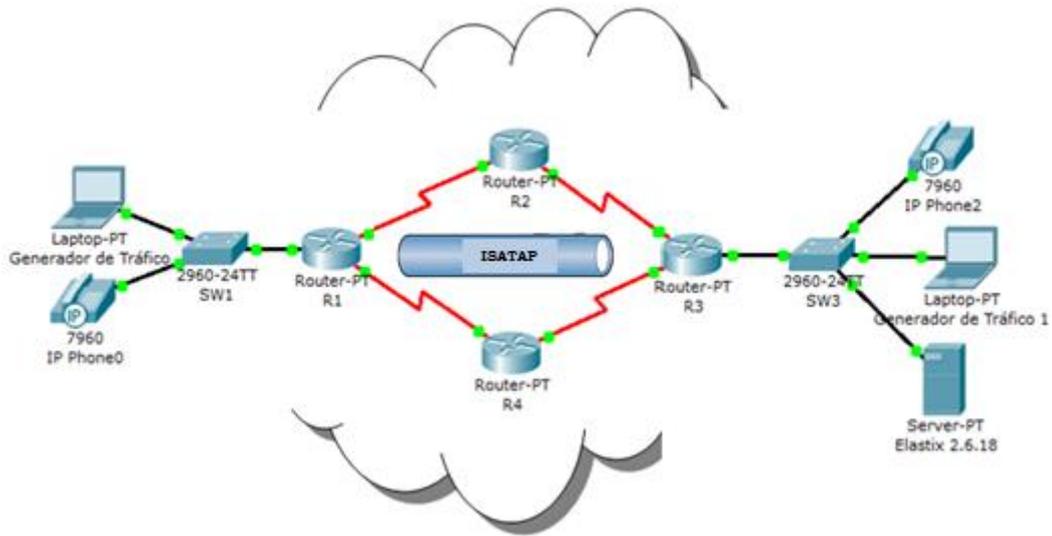


Figura 16: Técnica Tunneling ISATAP
Elaborado por: Jorge R. López O.

ISATAP define un método para generar una dirección IPv6 local a partir de una dirección IPv4, y un mecanismo para realizar el protocolo de descubrimiento de vecinos (Neighbor Discovery Protocol) sobre IPv4.

Como ISATAP utiliza IPv4 como un nivel de enlace sin capacidad de multicast/broadcast-capable (al contrario que Ethernet), el ICMPv6 Neighbor Discovery no se puede hacer de la forma habitual. Este es el motivo por el que ISATAP es un poco más complejo que 6over4.

ISATAP también conlleva los mismos riesgos de seguridad que 6to4: el enlace virtual IPv4 debe definirse con cuidado en el perímetro de la red, para que los hosts IPv4 externos no intenten ser parte del enlace ISATAP. Normalmente se puede evitar asegurando que el protocolo 41 no pueda atravesar los cortafuegos.

3.9.8 Escenario de Prueba Tunneling GRE/IPv6

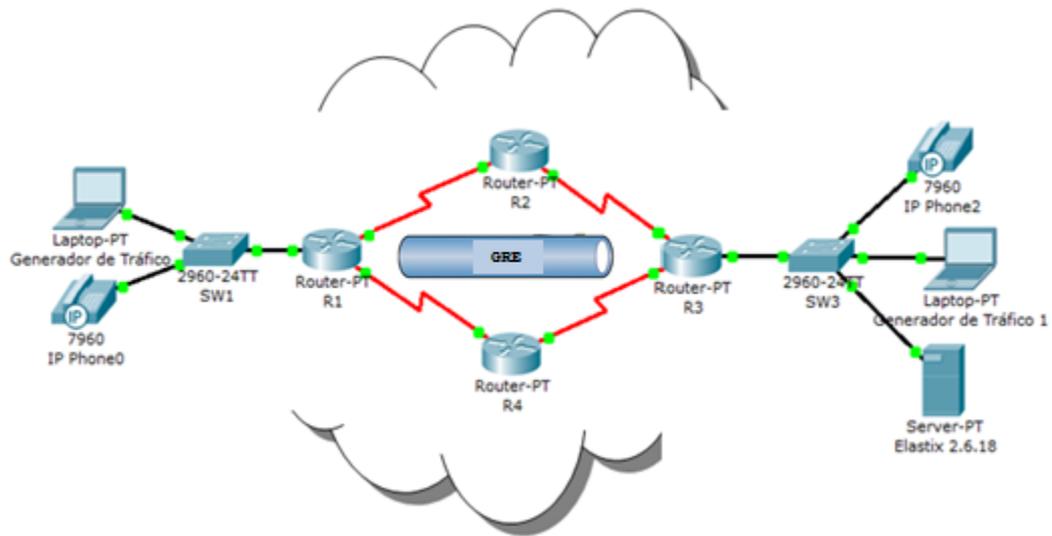


Figura 17: Técnica Tunneling GRE
Elaborado por: Jorge R. López O.

El GRE es un protocolo para el establecimiento de túneles a través de Internet. Está definido en la RFC 1701 y en la RFC 1702, pudiendo transportar hasta 20 protocolos de red distintos. GRE permite emplear protocolos de encaminamiento especializados que obtengan el camino óptimo entre los extremos de la comunicación, soporta la secuencialidad de paquetes y la creación de túneles sobre redes de alta velocidad y establece políticas de encaminamiento y seguridad.

CAPITULO IV

RESULTADOS Y DISCUSIÓN

La técnica de Tunneling consiste en encapsular un protocolo de red sobre otro (protocolo de red encapsulador) creando un túnel dentro de una red de computadoras. De esta manera se encaminan los paquetes de datos sobre nodos intermedios que son incapaces de ver en claro el contenido de dichos paquetes. El túnel queda definido por los puntos extremos y el protocolo de comunicación empleado.

En este capítulo, se determinarán los resultados obtenidos a lo largo de todo el proceso de investigación, para obtener conclusiones relevantes sobre la coexistencia de IPv4 e IPv6 que brinde soporte a tráfico de VoIP con la aplicación de la técnica de Tunneling más adecuada.

4.1 PRESENTACIÓN DE RESULTADOS

La presentación de los resultados es el proceso mediante el cual se dispone el contenido del tema de investigación y es una forma de ofrecer y mostrar la información de los datos y los resultados de una investigación.

Para el presente trabajo investigativo se realizó un análisis de las técnicas de Tunneling para la coexistencia de IPv4 e IPv6 que brinde soporte a tráfico a VoIP, considerando cada uno de los indicadores de la variable independiente y dependiente. Al mismo tiempo, se debe tomar en cuenta cada uno de los índices que conforman y satisfacen a cada indicador.

4.2 ANÁLISIS E INTERPRETACIÓN DE RESULTADOS

El análisis e interpretación de los resultados, se lo realizará en función de los indicadores e índices mencionados en el apartado **3.8 DETERMINACIÓN DE VARIABLES**.

En este análisis se determinarán los diferentes resultados del estudio de la variable independiente y dependiente, junto con los escenarios de prueba de las técnicas de Tunneling (6to4, ISATAP, GRE) escogidas. Adicionalmente, cabe mencionar que las mediciones de los indicadores e índices de las variables, se realizaron bajo la premisa de tres pruebas (llamadas VoIP) con una duración de cinco minutos cada una.

Para cuantificar cada uno de los indicadores se utilizó una **Media Ponderada** de sus respectivos índices. Los valores obtenidos según el nivel de medición van a ir decreciendo desde el 100% al 0%, de acuerdo a la aplicabilidad de cada ámbito del índice.

De igual manera, se establecieron **Pesos** para cada uno de los índices que forman parte de un indicador; con esto se consigue una Calificación Total, Porcentajes

Promedios y Porcentajes Individuales para cada escenario de prueba propuesto en el presente trabajo investigativo.

Posteriormente, se calcula la media ponderada de sus correspondientes indicadores, estableciendo ponderaciones asignadas equitativamente del Porcentaje Total por cada una de las variables.

Para determinar los diferentes valores se empleará la siguiente fórmula:

$$Variable = \sum_{n=1}^n (Peso_i \text{ Indicador}_i)$$

Para fines de comparación, se computó las medias ponderadas de los indicadores de la Variable Dependiente.

4.2.1 Análisis de la Variable Independiente

Problemas de coexistencia entre IPv4 e IPv6 que brinde soporte a tráfico de VoIP

a) **INDICADOR 1: Agotamiento de direcciones IP**

TABLA III: Número de Direcciones IPv4 e IPv6
Elaborado por: Jorge R. López O.

<i>Tipo de Direcciones</i>	<i>Factor de medición</i>	<i>Número de direcciones</i>	<i>Porcentaje (0-100%)</i>
IPv4	2^{32}	4294967296	1,26217744835361888865 87657044525e-27 %
IPv6	2^{128}	3,402823669209384634633 7460743177e+38	100 %

➔ **ÍNDICE 1:** Número de Direcciones IPv4

El crecimiento exponencial de las redes de computadores e Internet, llevó al agotamiento de direcciones IPv4, como se ha demostrado a lo largo de los últimos años:

- ☞ 10% a principio de 2010
- ☞ 6% mediados de 2010
- ☞ 5% dos meses después
- ☞ 2% antes de final de 2010
- ☞ 0% el 3 de Febrero de 2011

TABLA IV: Agotamiento de Direcciones IPv4 al transcurrir el tiempo
Elaborado por: Jorge R. López O.

<i>Año</i>	<i>Meses</i>	<i>Porcentaje %</i>
2010	Enero	10
2010	Junio	6
2010	Agosto	5
2010	Diciembre	2
2011	Febrero	0

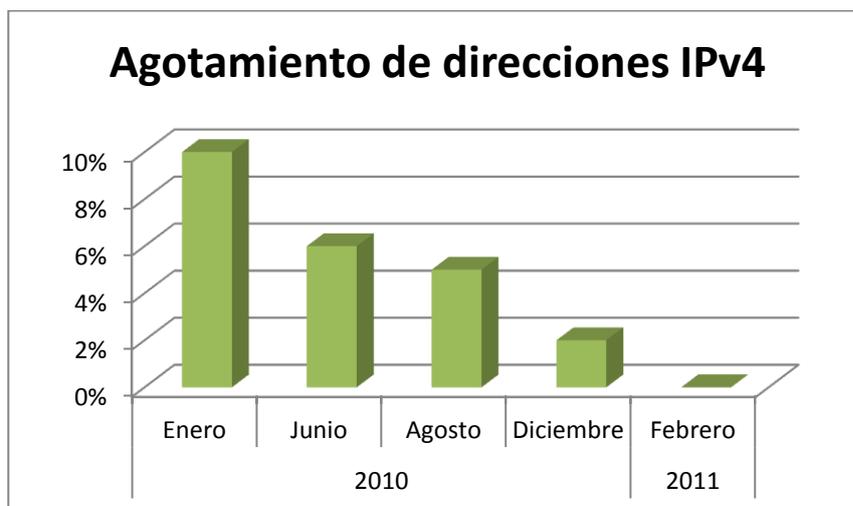


Figura 18: Agotamiento de direcciones IPv4
Elaborado por: Jorge R. López O.

➤ **ÍNDICE 2:** Número de Direcciones IPv6

Las grandes compañías de internet (como Google y Facebook) o fabricantes (como Cisco) animan a las instituciones y empresas particulares a hacer la transición, afirmando que eso hará más eficaz la comunicación entre los diferentes aparatos de una red doméstica o profesional.

Cisco, justamente, ha distribuido una proyección que da una idea de lo que se viene. El informe sugiere que en 2016 habrá 8.000 millones de dispositivos fijos y móviles con capacidad IPv6 en el mundo. En 2011 eran 1.000 millones.

Entre las razones de tal aumento (que a nivel global significará 1,3 zettabytes o más de un billón de gigabytes por año) se cuentan el incremento de dispositivos (en 2016 habrá casi 18.900 millones de conexiones de red contra los 10.300 millones que había en 2011), más usuarios de internet (3.400 millones), mayor velocidad de banda ancha (35 Mbps promedio), más video (un equivalente a 833 días de videos circulando por segundo) y crecimiento de Wi-Fi (más de la mitad del tráfico mundial).

En Latinoamérica, según la misma proyección, el tráfico crecerá a una tasa anual de 49% llegando en 2016 a ser siete veces más grande que hoy¹⁸.

¹⁸ <http://noticiaspe.terra.com.pe/tecnologia/noticias/0,,OI5814050-EI12469,00-IPv+Un+pequeno+cambio+en+la+IP+un+gran+salto+para+internet.html>

TABLA V: Crecimiento exponencial de IPv6 en el mundo
Elaborado por: <http://www.worldipv6launch.org/>

Año	Dispositivos fijos y móviles con IPv6	Conexiones de Red	Crecimiento tráfico de red (Latinoamérica)
2011	1000 millones	10300 millones	7%
2016	8000 millones	18900 millones	49%

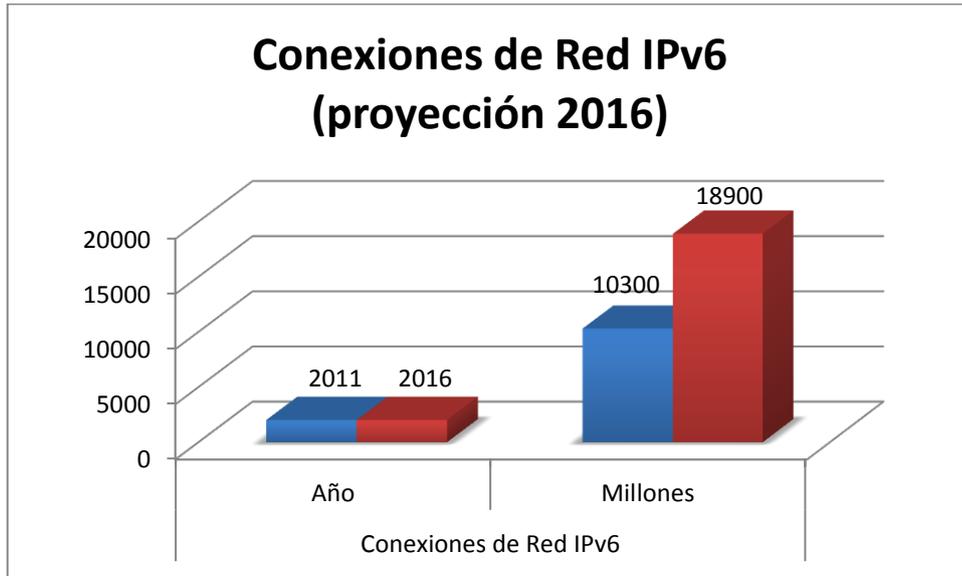


Figura 19: Proyección de Conexiones de Red IPv6 en el 2016
Elaborado por: Jorge R. López O.

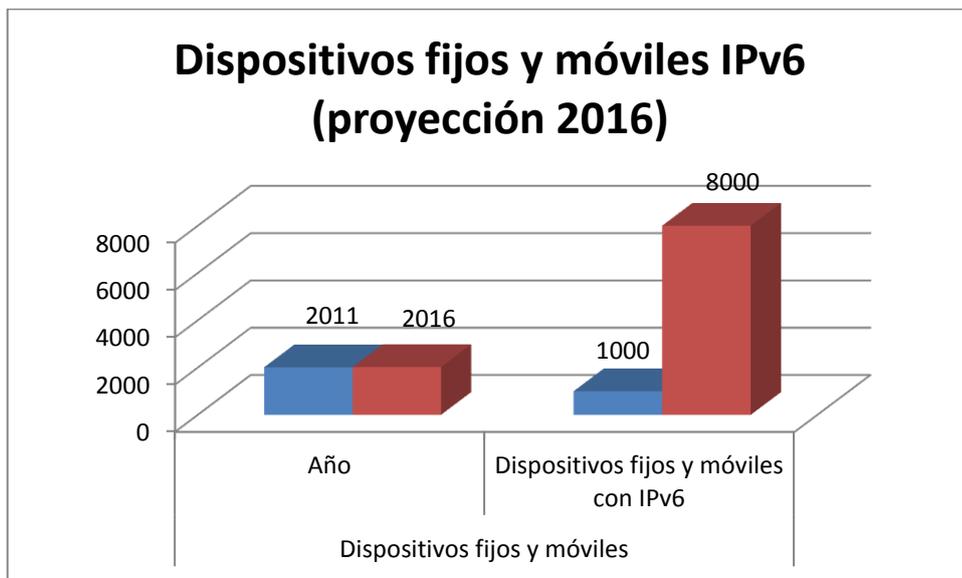


Figura 20: Proyección de Dispositivos fijos y móviles IPv6 en el 2016
Elaborado por: Jorge R. López O.

➤ **INTERPRETACIÓN INDICADOR 1: Agotamiento de direcciones IP**

El protocolo IPv4 en el que se ha basado el sistema de asignación de direcciones en las redes ha llegado a su límite, como ya anunciaron los expertos y organismos implicados en los últimos años.

Por este motivo se diseñó IPv6, la nueva versión, que permitirá a la redes estructuradas continuar creciendo, ya que tiene 128 bits de espacio para direcciones, lo que implica que se podrán crear 3,4 sextillones de direcciones. Los cambios de IPv4 a IPv6 las podemos clasificar en las siguientes categorías¹⁹:

- ☞ **Capacidad extendida de direccionamiento:** IPv6 incrementa el tamaño de dirección IP de 32 bits a 128 bits, para dar soporte a más niveles de direccionamiento jerárquico, un número mucho mayor de nodos direccionables, y una autoconfiguración más simple de direcciones. La escalabilidad del enrutamiento Multicast se mejora agregando un campo “ámbito” a estas direcciones y se define un nuevo tipo de dirección llamada “dirección envío a uno de”, usado para enviar un paquete a cualquiera de un grupo de nodos.

- ☞ **Simplificación del formato de cabecera:** Algunos campos de la cabecera IPv4 se han sacado o se han hecho opcionales, para reducir el costo del procesamiento de los paquetes y para ahorrar ancho de banda.

- ☞ **Soporte mejorado para las extensiones y opciones:** Los cambios en la manera en que se codifican las opciones de la cabecera IP permiten un reenvío más

¹⁹ <http://el-directorio.org/IPv6>

eficiente, límites menos rigurosos en la longitud de opciones, y mayor flexibilidad para introducir nuevas opciones en el futuro.

- ☞ **Capacidad de etiquetado de flujos:** Una nueva capacidad se agrega para permitir el etiquetado de paquetes que pertenecen a “flujos” de tráfico particulares para lo cual el remitente solicita tratamiento especial, como la calidad de servicio no estándar o el servicio en “tiempo real”.

- ☞ **Capacidades de Autenticación y Privacidad:** IPv6 incluye la especificación de extensiones que proveen autenticación, integridad, y (opcionalmente) confidencialidad de los datos.

b) **INDICADOR 2: Rendimiento**

☞ **ÍNDICE 1: Jitter**

Jitter es la variabilidad temporal durante el envío de señales digitales, una ligera desviación de la exactitud de la señal de reloj; es decir un cambio indeseado y abrupto de la propiedad de una señal. Esto puede afectar tanto a la amplitud, la frecuencia y la situación de fase, siendo la primera consecuencia de un retraso de la señal.

El Jitter óptimo debe ser menor a 20ms^{20} . Si el valor es menor a 20ms el Jitter puede ser compensado de manera apropiada, caso contrario debería ser minimizado.

²⁰http://www.dspace.espol.edu.ec/bitstream/123456789/10956/1/Estudio%20de%20Voz%20sobre%20IP%20_VoIP_%20en%20redes%20UMTS.pdf

TABLA VI: Jitter IPv4 vs. IPv6
Elaborado por: Jorge R. López O.

Índices / Pruebas	Jitter ms.	
	IPv4	IPv6
Prueba 1	1,24	3,51
Prueba 2	1,61	3,31
Prueba 3	1,08	1,13
Suma	3,93	7,95
Promedio	1,31	2,65
Porcentaje	100%	49,43%

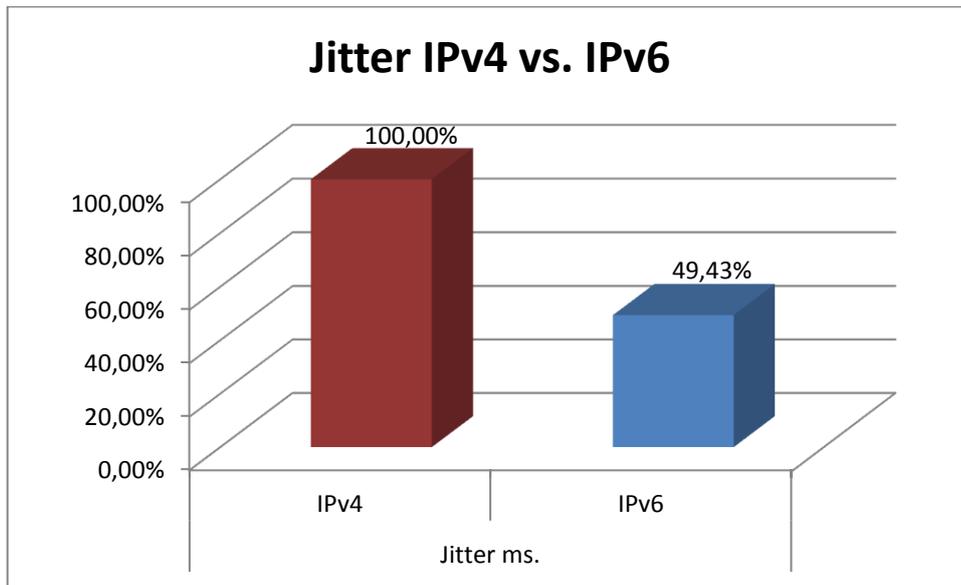


Figura 21: Jitter IPv4 vs. IPv6
Elaborado por: Jorge R. López O.

⇒ **ÍNDICE 2:** Ancho de Banda

Ancho de banda es la medida de datos y recursos de comunicación disponible o consumida expresados en bit/s o múltiplos de él.

En cuanto a la determinación del ancho de banda real, se utilizó la herramienta IPerf, que mide el ancho de banda de la conexión entre los dos host. Se trata de una herramienta Cliente-Servidor. Conectado con el servidor, se envían una serie

de paquetes de prueba desde el Cliente para calcular el ancho de banda en la conexión, utilizando el siguiente comando **iperf**:

☞ *Servidor:* >iperf.exe -s

☞ *Cliente:* >iperf.exe -c Dirección IP

A continuación se presenta una tabla que nos muestra los máximos anchos de banda, de los diferentes tipos de conexiones a Internet:

TABLA VII: Ancho de Banda por tipo de conexión

Elaborado por: Jorge R. López O.

Ancho de Banda	Nombre
56 kbit/s	Modem / Marcado telefónico PPP
1.544 Mbit/s	T1
10 Mbit/s	Ethernet
11 Mbit/s	Inalámbrico 802.11b
43.232 Mbit/s	T3
54 Mbit/s	Inalámbrico-G 802.11g
100 Mbit/s	Ethernet Rápida
155 Mbit/s	OC3
300 Mbit/s	Inalámbrico-N 802.11n
622 Mbit/s	OC12
1000 Mbit/s	Ethernet Gigabit
2.5 Gbit/s	OC48
9.6 Gbit/s	OC192
10 Gbit/s	Ethernet de 10 Gigabit

TABLA VIII: Ancho de Banda IPv4 vs. IPv6

Elaborado por: Jorge R. López O.

Índices / Pruebas	Ancho de Banda Kbps	
	IPv4	IPv6
Prueba 1	93,90	118
Prueba 2	80,20	118
Prueba 3	120	118
Total	294,10	354
Promedio	98,03	118
Porcentaje	87,08%	100%

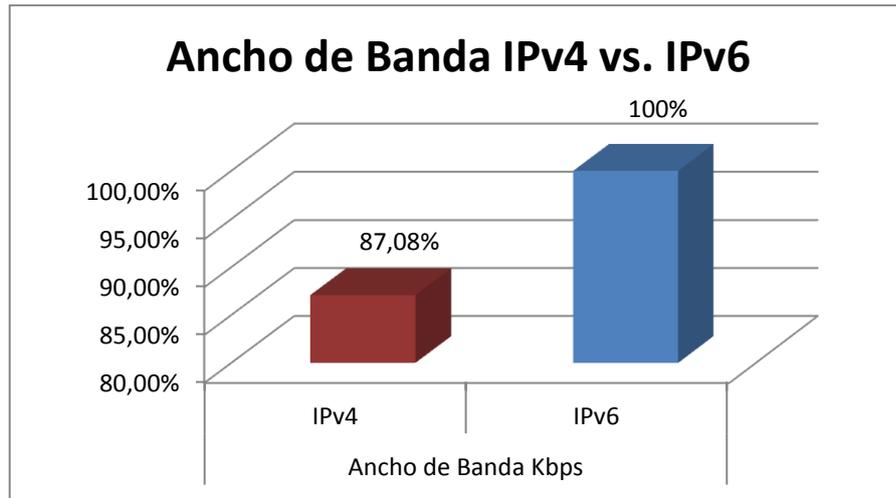


Figura 22: Ancho de Banda IPv4 vs. IPv6
Elaborado por: Jorge R. López O.

➔ **ÍNDICE 3:** Latencia

En las redes informáticas de datos, se denomina latencia a la suma de retardos temporales dentro de una red. Un retardo es producido por la demora en la propagación y transmisión de paquetes.

Otros factores, que influyen en la latencia de una red son:

- ☞ El tamaño de los paquetes transmitidos.
- ☞ El tamaño de los buffers dentro de los equipos de conectividad.

TABLA IX: Latencia IPv4 vs. IPv6
Elaborado por: Jorge R. López O.

Índices / Pruebas	Latencia ms.	
	IPv4	IPv6
Prueba 1	80,17	80,04
Prueba 2	80,03	80,04
Prueba 3	80,03	79,99
Total	240,23	240,07
Promedio	80,07	80,02
Porcentaje	99,94%	100%

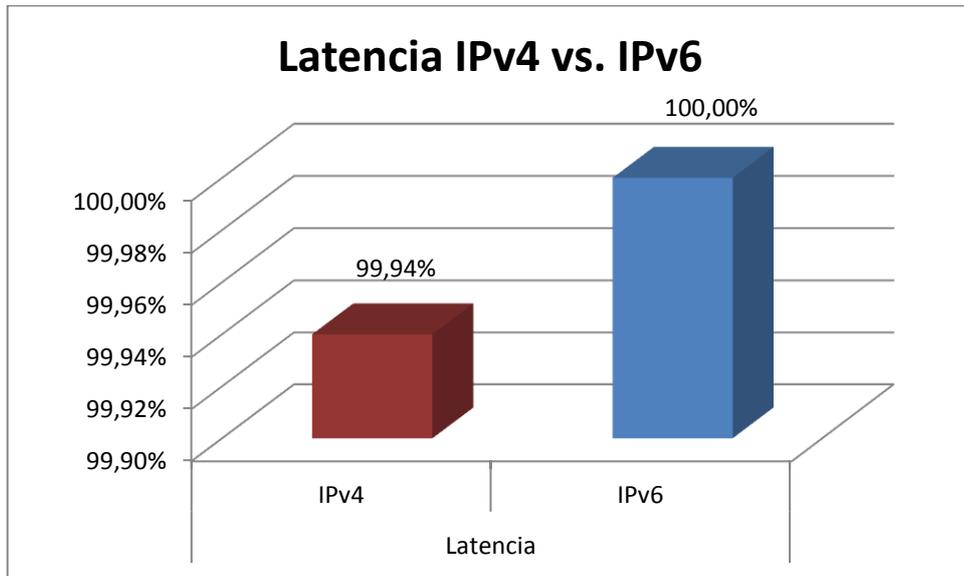


Figura 23: Latencia IPv4 vs. IPv6
Elaborado por: Jorge R. López O.

➔ **INTERPRETACIÓN INDICADOR 2: Rendimiento**

Una evaluación del rendimiento de la red, puede proporcionar la información oportuna y necesaria para la toma de decisiones técnicas, financieras e institucionales adecuadas.

Esta evaluación, incluye; un análisis exhaustivo de diseño, pruebas y mediciones para determinar si el funcionamiento de un sistema es consistente con los requisitos de funcionamiento actuales, y si se dispone de la capacidad de comunicación y arquitectura para soportar futuras actualizaciones, modificaciones y ampliaciones necesarias.

Los datos resultantes, proporcionan también una información importante sobre el estado actual del funcionamiento de la red, con los que se podrán comparar los datos de futuras comprobaciones para asegurar un rendimiento óptimo, efectivo y eficiente.

Para medir el Rendimiento en nuestros diferentes escenarios de prueba consideraremos lo siguiente:

- ☞ Velocidad de transmisión de datos que es una medida concreta y de fácil cálculo.

- ☞ Determinar la cantidad de paquetes de datos que llegan de forma íntegra desde un nodo hacia otro, puesto que los paquetes de datos pueden alterarse de manera significativa. Un elevado porcentaje de paquetes íntegros, significa un buen rendimiento de la red.

- ☞ El tiempo de respuesta también es un factor determinante, debido a que la velocidad en la transferencia de datos puede ser alta, pero puede ser lenta la velocidad que tarda en contactarse un nodo con otro.

En tal virtud, podemos determinar que el Jitter más elevado (2,65 ms.) y el mejor Ancho de Banda lo tiene IPv6 (118 Kbps), mientras que la mayor Latencia (80,07 ms.) ocurre en IPv4.

4.2.2 Análisis de la Variable Dependiente

Coexistencia de IPv4 a IPv6, utilizando Técnicas de Tunneling

6to4 - ISATAP - GRE

a) INDICADOR 1: Rendimiento

⇒ ÍNDICE 1: Jitter

TABLA X: Jitter 6to4 vs. ISATAP vs. GRE

Elaborado por: Jorge R. López O.

<i>Índices / Pruebas</i>	<i>Jitter ms.</i>		
	<i>6to4</i>	<i>ISATAP</i>	<i>GRE</i>
Prueba 1	3,33	1,79	2,79
Prueba 2	1,99	1,23	3,09
Prueba 3	2,71	1,16	2,79
Total	7,41	4,18	8,67
Promedio	2,47	1,39	2,89
Porcentaje	56,28%	100%	48,10%

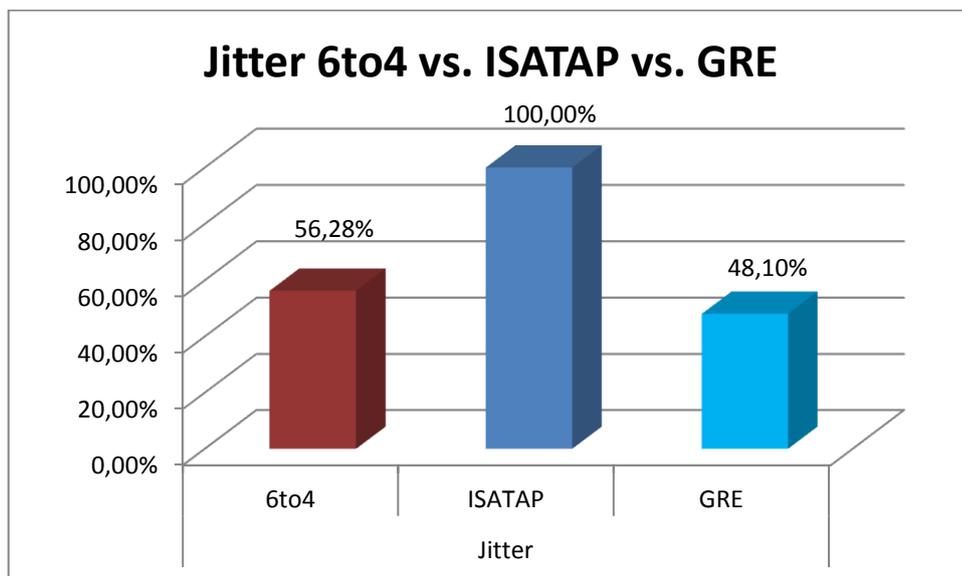


Figura 24: Jitter 6to4 vs. ISATAP vs. GRE

Elaborado por: Jorge R. López O.

➔ **ÍNDICE 2:** Ancho de Banda

TABLA XI: Ancho de Banda 6to4 vs. ISATAP vs. GRE
Elaborado por: Jorge R. López O.

<i>Índices / Pruebas</i>	<i>Ancho de Banda Kbps</i>		
	<i>6to4</i>	<i>ISATAP</i>	<i>GRE</i>
Prueba 1	111	115	72,00
Prueba 2	115	117	61,30
Prueba 3	116	115	86,90
Total	342	347	220,20
Promedio	114,00	115,67	73,40
Porcentaje	98,56%	100%	63,46%

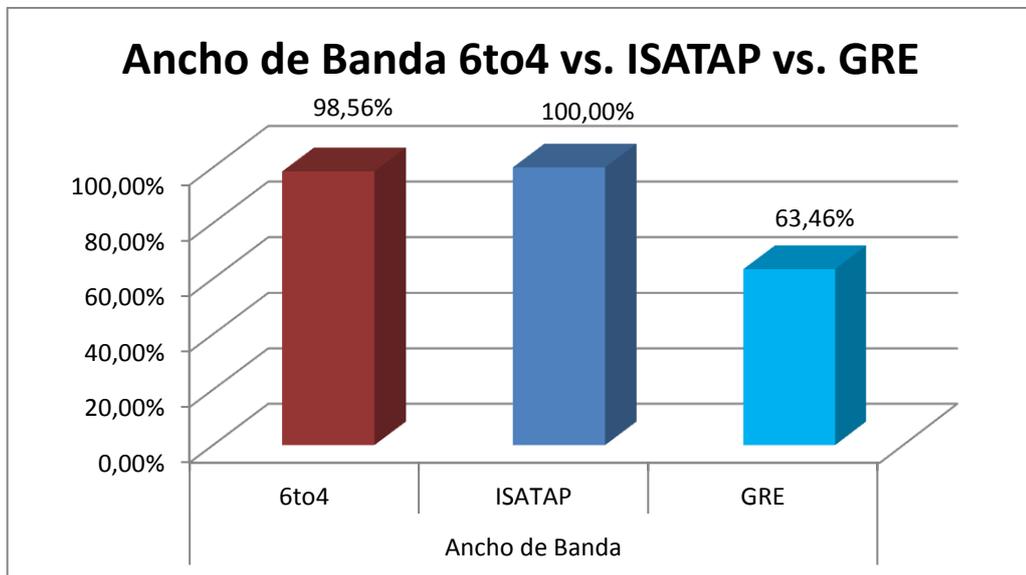


Figura 25: Ancho de Banda 6to4 vs. ISATAP vs. GRE
Elaborado por: Jorge R. López O.

➔ **ÍNDICE 3:** Latencia

TABLA XII: Latencia 6to4 vs. ISATAP vs. GRE
Elaborado por: Jorge R. López O.

<i>Índices / Pruebas</i>	<i>Latencia ms.</i>		
	<i>6to4</i>	<i>ISATAP</i>	<i>GRE</i>
Prueba 1	80,10	80,02	81,69
Prueba 2	79,98	80,02	82,08
Prueba 3	80,00	80,02	81,48
Total	240,08	240,06	245,25
Promedio	80,03	80,02	81,75
Porcentaje	99,99%	100%	97,88%

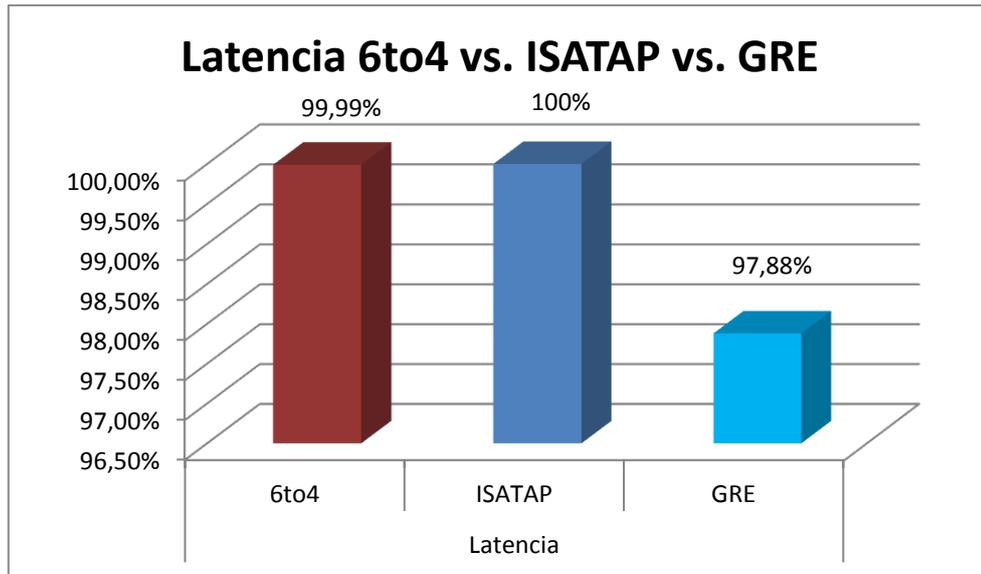


Figura 26: Latencia 6to4 vs. ISATAP vs. GRE
Elaborado por: Jorge R. López O.

⇒ INTERPRETACIÓN INDICADOR 1: *Rendimiento*

Como se mencionó anteriormente, cuando se trabaja con redes es de suma importancia determinar la manera en cómo se están transmitiendo los datos. Con esto se logra, realizar un análisis minucioso que compruebe la calidad del enlace de comunicaciones.

Para esto es imprescindible observar el comportamiento de la red y a su vez estimar su rendimiento; debido a que una red mal configurada o con un pobre rendimiento en sistemas de comunicaciones de gran tamaño puede ocasionar grandes pérdidas de tiempo, bajas en la productividad, capacidad disminuida, colisiones, etc.

En nuestro estudio intentaremos precisar el efectivo y eficiente desempeño de cada una de las Técnicas de Tunneling experimentadas, en los diferentes escenarios de prueba propuestos.

Es por ello, que podemos establecer que el Jitter más elevado y la mayor Latencia los encontramos en la Técnica de Tunneling GRE con valores de 2,89ms. y 81,75ms., respectivamente. A su vez, el mejor Ancho de Banda lo obtenemos de la Técnica de Tunneling ISATAP con un valor promedio de 115,67 Kbps.

b) **INDICADOR 2: *Facilidad de instalación, configuración, administración y monitoreo***

Para la realización del presente apartado de este trabajo investigativo, se recurrió a realizar una encuesta a diez Administradores de Red de varias instituciones, como por ejemplo: Corporación Nacional de Telecomunicaciones CNT, Ministerio de Inclusión Económica y Social MIES, Escuela Superior Politécnica de Chimborazo ESPOCH, entre otras.

La encuesta (técnica de investigación de campo) se utilizó para lograr un mayor acopio de información, como una alternativa a las restricciones que presenta la observación y estuvo encaminada a obtener determinados datos.

Es por ello, que se considerarán los criterios y experiencias emitidas por los Administradores de Red. El formato de la encuesta realizada, la podemos observar detenidamente en el **Anexo 12**.

Estas encuestas nos permitieron determinar el **Tiempo** y la **Dificultad** en la instalación, configuración, administración y monitoreo de las diferentes Técnicas de Tunneling investigadas (6to4, ISATAP, GRE).

➔ **ÍNDICE 1:** Tiempo

TABLA XIII: Escala Cuantitativa para medir el Tiempo
Elaborado por: Jorge R. López O.

Rango (Minutos)	Calificación	Abreviatura	Porcentaje %
30 < t	Muy Adecuado	MD	100%
31 < t < 90	Adecuado	A	75%
91 < t < 150	Poco Adecuado	PA	50%
151 < t < 210	Inadecuado	I	25%
t > 211	Nada adecuado	NA	0%

TABLA XIV: Tabulación encuestas Índice Tiempo
Elaborado por: Jorge R. López O.

Tiempo			
Calificación	6to4	ISATA P	GRE
Muy Adecuado	0	0	5
Adecuado	2	1	3
Poco Adecuado	3	2	2
Inadecuado	3	3	0
Nada adecuado	2	4	0
Total	10	10	10

TABLA XV: Equivalencia porcentual de tabulación de encuestas Índice Tiempo
Elaborado por: Jorge R. López O.

Tiempo			
Calificación	6to4	ISATAP	GRE
Muy Adecuado	0,00%	0,00%	50,00%
Adecuado	15,0%	7,50%	22,50%
Poco Adecuado	15,0%	10,00%	10,00%
Inadecuado	7,50%	0,00%	0,00%
Nada adecuado	0,00%	0,00%	0,00%
Total	37,50%	17,50%	82,50%
Porcentaje	45,45%	21,21%	100%

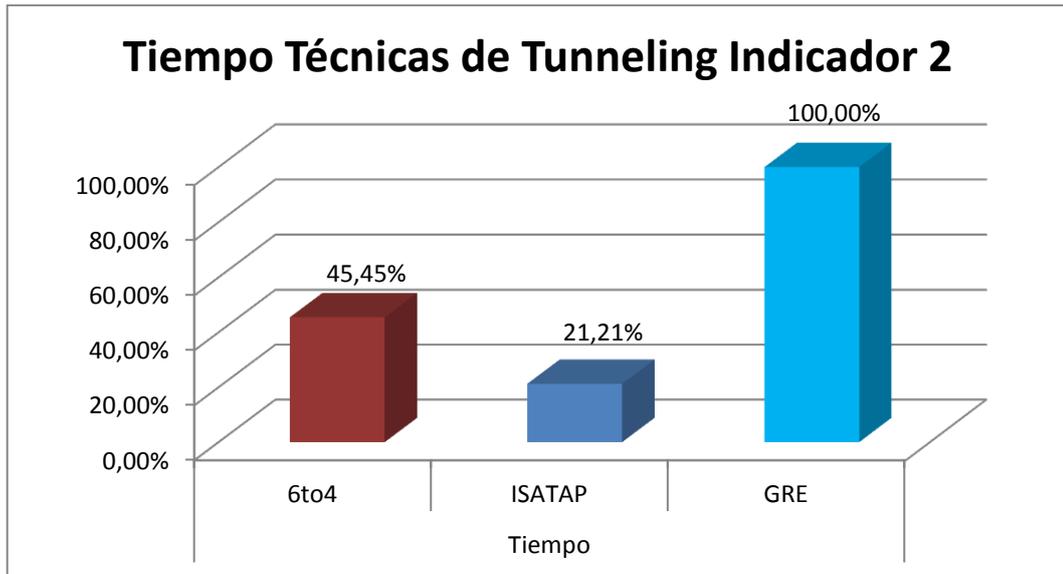


Figura 27: Tiempo Técnicas de Tunneling Indicador 2
Elaborado por: Jorge R. López O.

⇒ **ÍNDICE 2:** Dificultad

TABLA XVI: Escala Cuantitativa para medir la Dificultad
Elaborado por: Jorge R. López O.

<i>Puntos</i>	<i>Calificación</i>	<i>Abreviatura</i>	<i>Porcentaje %</i>
81-100	Muy Adecuado	MD	100%
61-80	Adecuado	A	75%
41-60	Poco Adecuado	PA	50%
21-40	Inadecuado	I	25%
0-20	Nada adecuado	NA	0%

TABLA XVII: Tabulación encuestas Índice Dificultad
Elaborado por: Jorge R. López O.

<i>Dificultad</i>			
<i>Calificación</i>	<i>6to4</i>	<i>ISATAP</i>	<i>GRE</i>
Muy Adecuado	0	0	4
Adecuado	2	1	2
Poco Adecuado	3	1	3
Inadecuado	3	3	1
Nada adecuado	2	5	0
Total	10	10	10

TABLA XVIII: Equivalencia porcentual de tabulación de encuestas Índice Dificultad
Elaborado por: Jorge R. López O.

Dificultad			
Calificación	6to4	ISATAP	GRE
Muy Adecuado	0,00%	0,00%	40,00%
Adecuado	15,00%	7,50%	15,00%
Poco Adecuado	15,00%	5,00%	15,00%
Inadecuado	7,50%	7,50%	2,50%
Nada adecuado	0,00%	0,00%	0,00%
Total	37,50%	20,00%	72,50%
Porcentaje	51,72%	27,57%	100%

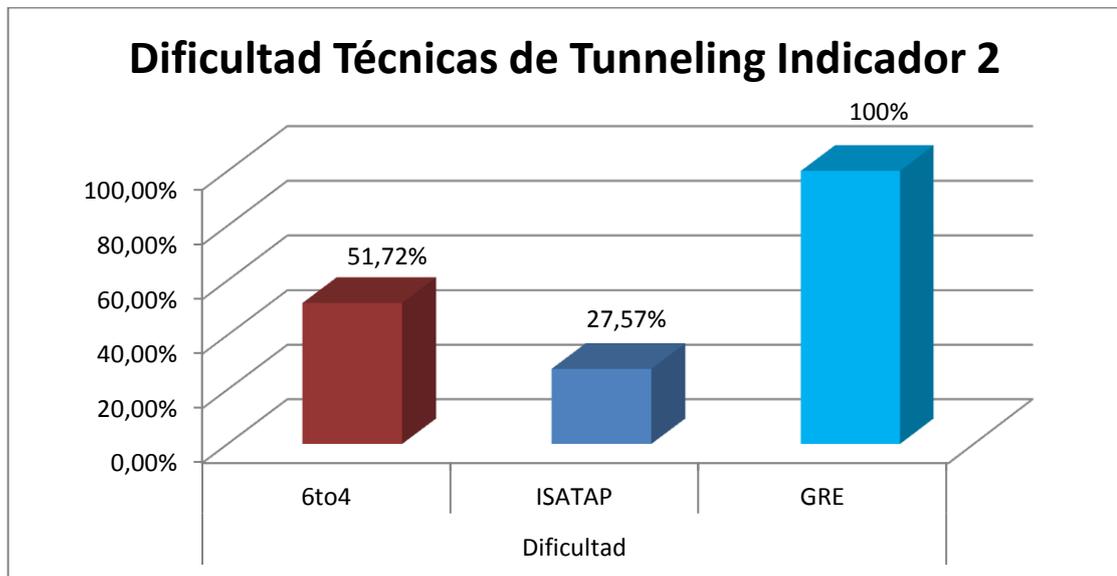


Figura 28: Dificultad Técnicas de Tunneling Indicador 2
Elaborado por: Jorge R. López O.

⇒ **INTERPRETACIÓN INDICADOR 2:** *Facilidad de instalación, configuración, administración y monitoreo*

La conexión de los usuarios entre sí; además, con las diferentes instituciones y éstas con el mundo exterior, es un requisito indispensable en el mundo actual. Es por ello, que los Administradores de Red de todas las instituciones (incluso de las pequeñas instituciones) necesitan conectividad del tipo clase empresarial. Este tipo de conectividad, reúne una combinación de alto rendimiento, seguridad y características

que ayudan a mantener la productividad de los usuarios y al mismo tiempo mantener los activos de una institución de forma segura.

Para conseguir lo anteriormente mencionado, los Administradores de Red eligen una de tantas maneras para conseguir estos objetivos; uno de ellos es la aplicación de las Técnicas de Tunneling que consisten en encapsular un protocolo de red sobre otro (protocolo de red encapsulador) creando un túnel dentro de una red de computadoras.

Es así, que las instituciones obtienen una serie de ventajas del uso de estas Técnicas, como pueden ser las siguientes:

- ☞ Mayor facilidad de comunicación, alto grado de competitividad y dinámica de grupo eficiente.
- ☞ Reducción del presupuesto para el procesamiento de datos y disminución de los costos de los diferentes procesos por usuario.
- ☞ Mejoras en la administración de los programas, integridad de los datos, flexibilidad en el proceso de datos, tiempos de respuesta, facilidad de uso, entre otras.

Por consiguiente, del análisis del indicador *Facilidad de instalación, configuración, administración y monitoreo de las Técnicas de Tunneling*, podemos concluir que:

Según los Administradores de Red encuestados, junto con la experiencia personal adquirida durante la ejecución del presente proyecto investigativo, GRE es la Técnica de Tunneling que lleva menor tiempo para su implementación y a su vez presenta una reducida dificultad de configuración, administración y monitoreo.

No obstante, la Técnica de Tunneling ISATAP exige un mayor grado de conocimiento, configuración de direcciones IP, configuración de MTU (Unidades Máximas de Transmisión), keep-alives, etc., por ende; requiere de mayor tiempo para implementarse y su grado de dificultad también aumenta en comparación con las otras Técnicas de Tunneling analizadas.

Cabe mencionar, que la Técnica de Tunneling 6to4 presenta un relativo equilibrio en los índices investigados.

c) **INDICADOR 3: Número de Paquetes RTP**

El protocolo de transporte en tiempo real RTP es un protocolo basado en IP que proporciona soporte para el transporte de datos en tiempo real. Fue diseñado para funcionar junto con el protocolo de control auxiliar RTCP para conseguir mantener la calidad en la transmisión de datos y proporcionar información sobre los participantes al iniciarse una sesión.

Los paquetes enviados por Internet sufren un retardo y jitter impredecible que las aplicaciones en tiempo real no pueden aceptar.

Por eso, RTP proporciona un mecanismo llamado TimeStamping (es la información más importante en aplicaciones en tiempo real) que ofrece un transporte end-to-end para los datos en tiempo real. El paquete RTP se encapsula en un paquete UDP/IP y tiene las siguientes características:

☞ RTP no es un protocolo completo, está abierto a nuevos formatos y software multimedia.

☞ RTP/RTCP no es responsable de las tareas de alto nivel como la sincronización, recuperación de paquetes perdidos y control de congestión que debe realizarse en la capa de aplicación.

☞ La información de flujo y congestión de RTP es proporcionada por los informes del emisor y receptor del RTCP.

☞ **ÍNDICE 1:** Paquetes RTP Transmitidos

TABLA XIX: Paquetes RTP Transmitidos 6to4 vs. ISATAP vs. GRE

Elaborado por: Jorge R. López O.

Índices / Pruebas	Paquetes RTP Transmitidos		
	6to4	ISATAP	GRE
Prueba 1	12023	12038	11988
Prueba 2	12028	12035	12022
Prueba 3	12042	12038	12074
Total	36093	36111	36084
Promedio	12031	12037	12028
Porcentaje	99,95%	100%	99,93%

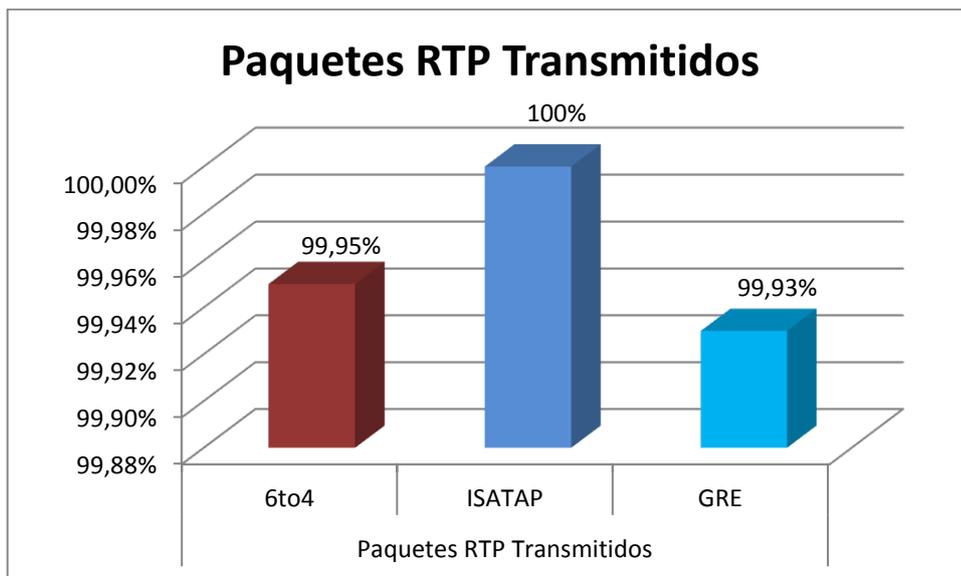


Figura 29: Paquetes RTP Transmitidos

Elaborado por: Jorge R. López O.

⇒ **ÍNDICE 2:** Paquetes RTP Perdidos

TABLA XX: Paquetes RTP Perdidos 6to4 vs. ISATAP vs. GRE
Elaborado por: Jorge R. López O.

<i>Índices / Pruebas</i>	<i>Paquetes RTP Perdidos</i>		
	<i>6to4</i>	<i>ISATAP</i>	<i>GRE</i>
Prueba 1	0	1	427
Prueba 2	0	1	544
Prueba 3	1	1	390
Total	1	3	1361
Promedio	0,33	1	453,67
Porcentaje	100%	33%	0,07%

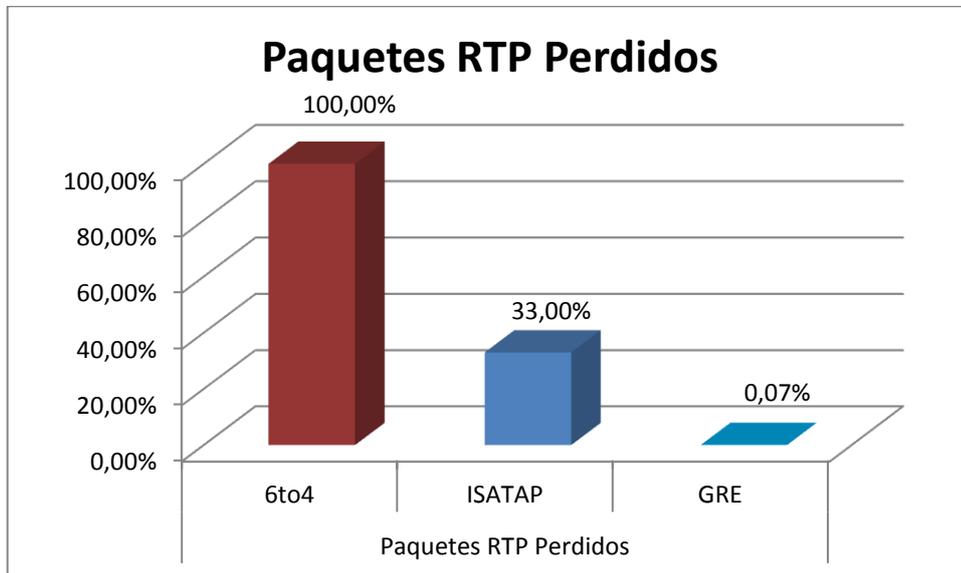


Figura 30: Paquetes RTP Perdidos
Elaborado por: Jorge R. López O.

⇒ **INTERPRETACIÓN INDICADOR 3:** *Número de Paquetes RTP*

El protocolo RTP, establece los principios de un protocolo de transporte sobre redes que no garantizan calidad de servicio para datos “de tiempo real”, como por ejemplo voz y video. El protocolo establece la manera de generar paquetes que incluyen, además de los propios datos de “tiempo real” a transmitir, números de secuencia,

marcas de tiempo, y monitoreo de entrega. Las aplicaciones típicamente utilizan RTP sobre protocolos de red “no confiables”, como UDP. RTP soporta transferencia de datos a destinos múltiples, usando facilidades de “multicast”, si esto es provisto por la red.

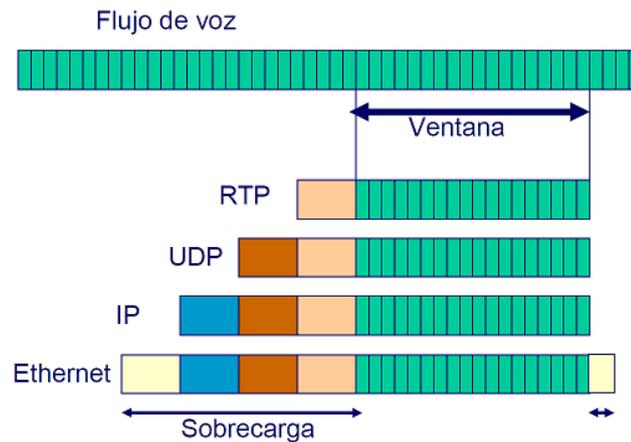


Figura 31: Flujo de voz vs. Paquetes RTP
Elaborado por: José Joskowicz. Universidad de la República Montevideo (Uruguay)

Luego del análisis respectivo, conseguimos comprobar que en las tres Técnicas de Tunneling (6to4, ISATAP y GRE) existe un relativo equilibrio en lo que respecta a la transmisión de Paquetes RTP. Sin embargo, la Técnica de Tunneling que más evidencia la pérdida de Paquetes RTP, la encontramos en la Técnica de Tunneling GRE con un valor porcentual de eficiencia que no alcanza ni el 1%, ISATAP mejora este nivel subiéndolo al 33% y 6to4 prácticamente no tiene pérdida de Paquetes RTP.

4.2.3 Resumen de los datos obtenidos y equivalencia de pesos

Luego de materializar el presente trabajo investigativo acerca de las Técnicas de Tunneling que permitan la coexistencia de IPv4 e IPv6 que brinde soporte a tráfico sobre VoIP, junto con todo el proceso analítico, los escenarios de prueba y las muestras alcanzadas, podemos elaborar la siguiente tabla resumen:

TABLA XXI: Resumen de los datos obtenidos y Equivalencia de Pesos para los Indicadores e Índices de la Variable Independiente
Elaborado por: Jorge R. López O.

<i>Indicador</i>	<i>Peso</i>	<i>Indice</i>	<i>Peso</i>	<i>6to4</i>	<i>ISATAP</i>	<i>GRE</i>	<i>Observación (Mejor valor de acuerdo al Índice, equivale al 100%)</i>
Rendimiento	60%	Jitter	40%	56,28	100,00	48,10	Menor Jitter
		Ancho de banda	30%	98,56	100,00	63,46	Mayor Ancho de Banda
		Latencia	30%	99,99	100,00	97,88	Menor Latencia
Facilidad de instalación, configuración, administración y monitoreo	10%	Tiempo	50%	45,45	21,21	100,00	Menor Tiempo
		Dificultad	50%	51,72	27,57	100,00	Menor Dificultad
Número de Paquetes RTP	30%	Paquetes RTP Tx	60%	99,95	100,00	99,93	Mayor Paquetes Transmitidos
		Pérdida Paquetes RTP	40%	100,00	33,00	0,07	Menor Pérdida de Paquetes

Esto a su vez, nos faculta para determinar la Equivalencia de los Pesos de cada uno de los Índices contenidos en cada Indicador. Por ello, podemos desglosar cada uno de los promedios de los Índices investigados, como se indica en la tabla subsiguiente:

TABLA XXII: Promedios de Equivalencia del Peso de los Índices
Elaborado por: Jorge R. López O.

<i>Indicador</i>	<i>Peso</i>	<i>Indice</i>	<i>Peso</i>	<i>6to4</i>	<i>ISATAP</i>	<i>GRE</i>
Rendimiento	60%	Jitter	40%	22,51	40,00	19,24
		Ancho de banda	30%	29,57	30,00	19,04
		Latencia	30%	30,00	30,00	29,36
		Total	100%	82,08	100,00	67,64
Facilidad de instalación, configuración, administración y monitoreo	10%	Tiempo	50%	22,73	10,61	50,00
		Dificultad	50%	25,86	13,79	50,00
		Total	100%	48,59	24,39	100,00
Número de Paquetes RTP	30%	Paquetes RTP Tx	60%	59,97	60,00	59,96
		Pérdida Paquetes RTP	40%	40,00	13,20	0,03
		Total	100%	99,97	73,20	59,99

A continuación, presentamos el Resumen de Equivalencias de los Pesos de los Índices investigados, conseguidos mediante las pruebas respectivas.

TABLA XXIII: Resumen de Equivalencia del Peso de los Índices
Elaborado por: Jorge R. López O.

Indicador	Peso	6to4	ISATAP	GRE
Rendimiento	60%	82,08	100,00	67,64
Facilidad de instalación, configuración, administración y monitoreo	10%	48,59	24,39	100,00
Número de Paquetes RTP	30%	99,97	73,20	59,99

➤ **INTERPRETACIÓN:** Por lo expuesto en la Tabla XXIV podemos concluir, que la Técnica de Tunneling **ISATAP** es la que nos ofrece un mejor Rendimiento, **GRE** nos facilita la Instalación, configuración, administración y monitoreo, y **6to4** brinda una mejor Transmisión de Paquetes RTP. Para una mejor ilustración de lo expresado, podemos observar las siguientes figuras que describen visualmente la Interpretación detallada en el párrafo anterior.

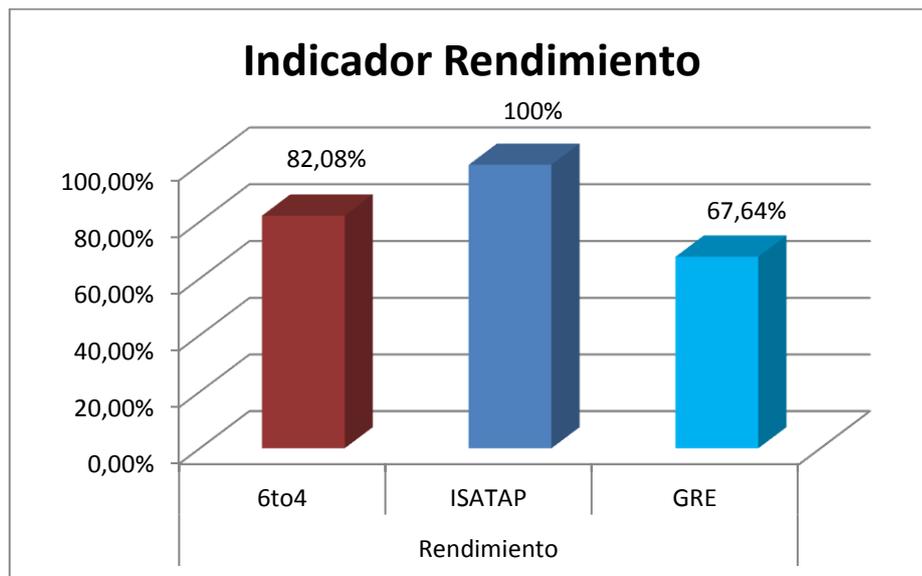


Figura 32: Rendimiento Equivalencia en Pesos
Elaborado por: Jorge R. López O.

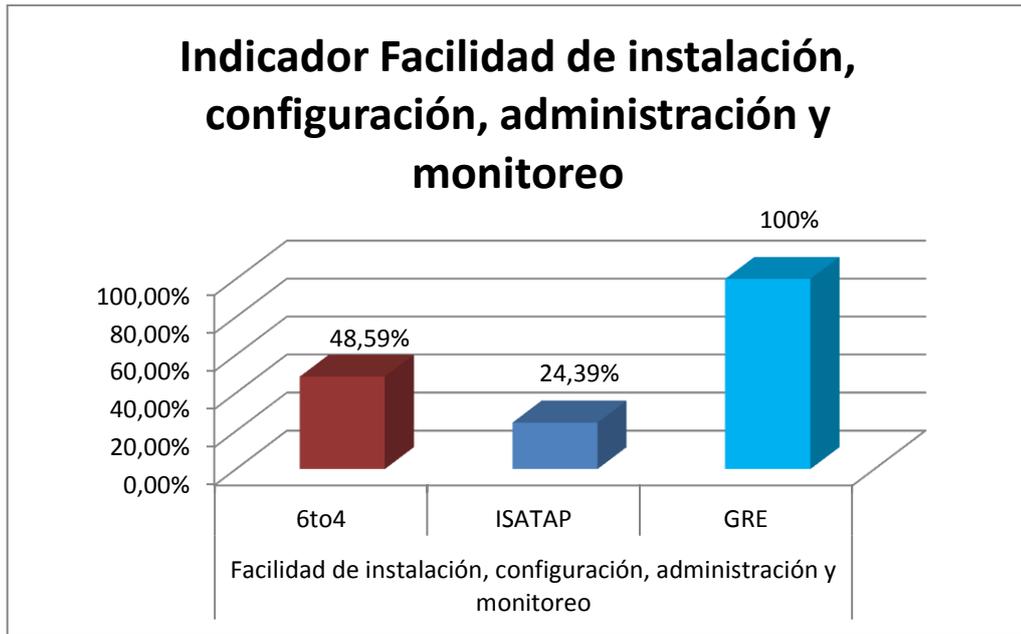


Figura 33: Facilidad de instalación, configuración, administración y monitoreo. Equivalencia en Pesos

Elaborado por: Jorge R. López O.

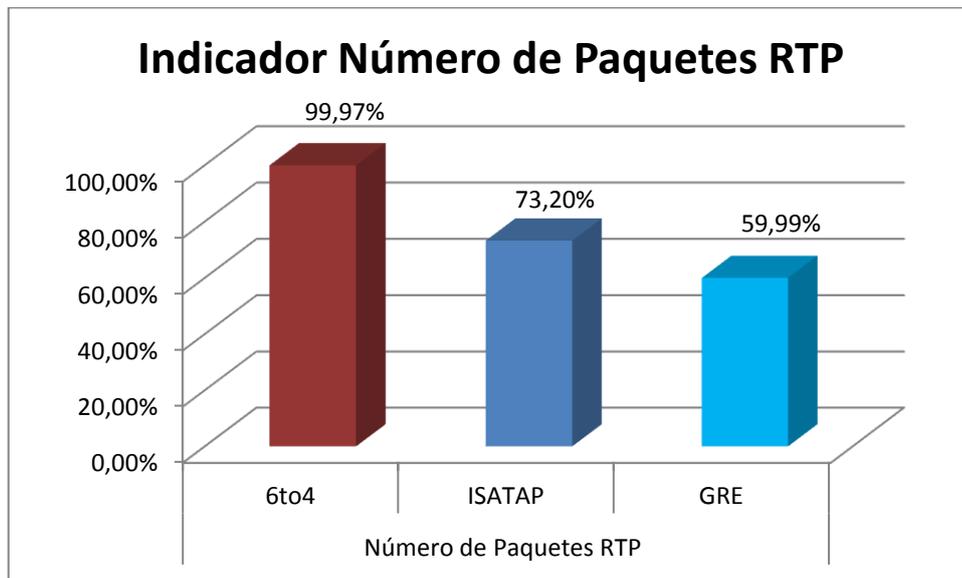


Figura 34: Número de Paquetes RTP Equivalencia en Pesos

Elaborado por: Jorge R. López O.

Al igual que lo realizado para los Índices, ahora podemos subir al nivel de los Indicadores (bajo el mismo razonamiento y modalidad empleada), es decir;

desglosaremos cada uno de los promedios de los Indicadores investigados. La tabla obtenida es la siguiente:

TABLA XXIV: Promedios de Equivalencia del Peso de los Indicadores
Elaborado por: Jorge R. López O.

Indicador	Peso	6to4	ISATAP	GRE
Rendimiento	60%	49,25	60,00	40,58
Facilidad de instalación, configuración, administración y monitoreo	10%	4,86	2,44	10,00
Número de Paquetes RTP	30%	29,99	21,96	18,00

4.3 PRUEBA DE LA HIPÓTESIS DE INVESTIGACIÓN

La importancia de un tema de investigación es el conseguir demostrar la hipótesis planteada y establecer una afirmación sustentada por un debido proceso investigativo.

Al intentar comparar dos posibles alternativas para llegar a una conclusión es preferible utilizar el método de comprobación de hipótesis de Chi-Cuadrado.

Las pruebas Chi-cuadrado son un grupo de contrastes de hipótesis que sirven para comprobar afirmaciones acerca de las funciones de probabilidad (o densidad) de una o dos variables aleatorias. Estas pruebas no pertenecen propiamente a la estadística paramétrica pues no establecen suposiciones restrictivas en cuanto al tipo de variables que admiten, ni en lo que refiere a su distribución de probabilidad ni en los valores y/o el conocimiento de sus parámetros.

4.3.1 Planteamiento de la Hipótesis

H₁= Mediante el análisis de las técnicas de Tunneling, se logrará determinar el mecanismo más adecuado de coexistencia de IPv4 e IPv6, que brinde soporte a tráfico de VoIP.

H₀= Mediante el análisis de las técnicas de Tunneling, no se logrará determinar el mecanismo más adecuado de coexistencia de IPv4 e IPv6, que brinde soporte a tráfico de VoIP.

4.3.2 Cálculo Chi-Cuadrado

Dentro del proceso de cálculo debemos definir algunos parámetros para el Chi-Cuadrado, como se indica en la Tabla XXV.

TABLA XXV: Parámetros para Chi-Cuadrado
Elaborado por: Jorge R. López O.

Nivel de Significación (Ver Anexo 13)	$\alpha=0.05$
Grado de libertad $GL = (\#filas - 1) * (\#columnas - 1)$	$GL=(6-1)(3-1)$ $GL=(5)(2)$ $GL=10$
$X_c^2 = \text{Chi-Tabulado}$	$X_t^2 = 18,31$
Criterio	$X_c^2 \geq X_t^2$

A continuación, encontraremos los valores correspondientes a Chi-cuadrado (X_c^2), mediante la siguiente ecuación:

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

En dónde:

∑ = Es la sumatoria de todos los valores posibles de (O-E)²/E.

O = El valor observado

E = El valor esperado, y

Por último, aplicamos la fórmula mencionada anteriormente para conseguir determinar Chi-Cuadrado.

Para proseguir con la demostración de la Hipótesis, debemos considerar los rangos de Adecuado o No Adecuado, para el presente estudio investigativo realizado.

TABLA XXVI: Rangos de Idoneidad para demostrar la Hipótesis
Elaborado por: Jorge R. López O.

<i>Indicador</i>	<i>Peso</i>	<i>Idoneidad</i>	<i>Rangos Porcentajes</i>	<i>Equivalencia</i>
Rendimiento	60%	Adecuado	55,148-60,003	4
			50,292-55,147	3
		No Adecuado	45,436-50,291	2
			40,580-45,435	1
Facilidad de instalación, configuración, administración y monitoreo	10%	Adecuado	8,14-10,03	4
			6,24-8,13	3
		No Adecuado	4,34-6,23	2
			2,44-4,33	1
Número de Paquetes RTP	30%	Adecuado	27,00-29,99	4
			24-26,99	3
		No Adecuado	21-23,99	2
			18-20,99	1

Establecidos los Rangos de Idoneidad y luego de obtener los promedios de las Equivalencias de Pesos de los Indicadores, elaboramos la Tabla Resumen que confronta la Variable Dependiente con respecto a la Variable Independiente,

considerando si es o no adecuado el mecanismo de coexistencia de IPv4 e IPv6, que brinde soporte a tráfico de VoIP.

TABLA XXVII: Variable Dependiente vs. Variable independiente
Elaborado por: Jorge R. López O.

Variable Dependiente (Indicadores)			Variable Independiente (Técnicas de Tunneling)		
			6to4	ISATAP	GRE
H_i	Mediante el análisis de las técnicas de Tunneling, se logrará determinar el mecanismo más adecuado de coexistencia de IPv4 e IPv6, que brinde soporte a tráfico de VoIP.	Rendimiento	0	4	0
		Facilidad de instalación, configuración, administración y monitoreo	0	0	4
		Número de Paquetes RTP	4	0	0
H₀	Mediante el análisis de las técnicas de Tunneling, no se logrará determinar el mecanismo más adecuado de coexistencia de IPv4 e IPv6, que brinde soporte a tráfico de VoIP.	Rendimiento	2	0	1
		Facilidad de instalación, configuración, administración y monitoreo	2	1	0
		Número de Paquetes RTP	0	2	1

A partir de la Tabla Resumen anterior, se procede a definir la **Tabla Observada**, que se muestra a continuación:

TABLA XXVIII: Tabla Observada
Elaborado por: Jorge R. López O.

Variable Dependiente (Indicadores)		Variable Independiente (Técnicas de Tunneling)			Total
		6to4	ISATAP	GRE	
H₁ = Mediante el análisis de las técnicas de Tunneling, se logrará determinar el mecanismo más adecuado de coexistencia de IPv4 e IPv6, que brinde soporte a tráfico de VoIP.	Rendimiento	0	4	0	4
	Facilidad de instalación, configuración, administración y monitoreo	0	0	4	4
	Número de Paquetes RTP	4	0	0	4
H₀ = Mediante el análisis de las técnicas de Tunneling, no se logrará determinar el mecanismo más adecuado de coexistencia de IPv4 e IPv6, que brinde soporte a tráfico de VoIP.	Rendimiento	2	0	1	3
	Facilidad de instalación, configuración, administración y monitoreo	2	1	0	3
	Número de Paquetes RTP	0	2	1	3
Total		8	7	6	21

Como parte del proceso, obtenemos la **Tabla Esperada**.

TABLA XXIX: Tabla Esperada
Elaborado por: Jorge R. López O.

Variable Dependiente (Indicadores)		Variable Independiente (Técnicas de Tunneling)			Total
		6to4	ISATAP	GRE	
H₁ = Mediante el análisis de las técnicas de Tunneling, se logrará determinar el mecanismo más adecuado de coexistencia de IPv4 e IPv6, que brinde soporte a tráfico de VoIP.	Rendimiento	1,524	1,333	1,143	4
	Facilidad de instalación, configuración, administración y monitoreo	1,524	1,333	1,143	4
	Número de Paquetes RTP	1,524	1,333	1,143	4
H₀ = Mediante el análisis de las técnicas de Tunneling, no se logrará determinar el mecanismo más adecuado de coexistencia de IPv4 e IPv6, que brinde soporte a tráfico de VoIP.	Rendimiento	1,143	1	0,857	3
	Facilidad de instalación, configuración, administración y monitoreo	1,143	1	0,857	3
	Número de Paquetes RTP	1,143	1	0,857	3
Total		8	7	6	21

TABLA XXX: Valores del Chi-Cuadrado
Elaborado por: Jorge R. López O.

<i>Técnica de Tunneling</i>	<i>Indicadores</i>	<i>O</i>	<i>E</i>	<i>O-E</i>	<i>(O-E)²</i>	<i>(O-E)²/E</i>
6to4	Rendimiento	0	1,524	-1,524	2,322	1,524
	Facilidad de instalación, configuración, administración y monitoreo	0	1,524	-1,524	2,322	1,524
	Número de Paquetes RTP	4	1,524	2,476	6,132	4,024
	Rendimiento	2	1,143	0,857	0,735	0,643
	Facilidad de instalación, configuración, administración y monitoreo	2	1,143	0,857	0,735	0,643
	Número de Paquetes RTP	0	1,143	-1,143	1,306	1,143
ISATAP	Rendimiento	4	1,333	2,667	7,111	5,333
	Facilidad de instalación, configuración, administración y monitoreo	0	1,333	-1,333	1,778	1,333
	Número de Paquetes RTP	0	1,333	-1,333	1,778	1,333
	Rendimiento	0	1	-1	1	1
	Facilidad de instalación, configuración, administración y monitoreo	1	1	0	0	0
	Número de Paquetes RTP	2	1	1	1	1
GRE	Rendimiento	0	1,143	-1,143	1,306	1,143
	Facilidad de instalación, configuración, administración y monitoreo	4	1,143	2,857	8,163	7,143
	Número de Paquetes RTP	0	1,143	-1,143	1,306	1,143
	Rendimiento	1	0,857	0,143	0,020	0,024
	Facilidad de instalación, configuración, administración y monitoreo	0	0,857	-0,857	0,735	0,857
	Número de Paquetes RTP	1	0,857	0,143	0,020	0,024
TOTAL					29,833	

Una vez que se ha encontrado el valor de $X_c^2 = 29,833$; se puede indicar que el Criterio a evaluar en el presente trabajo investigativo $X_c^2 \geq X_t^2$ es verdadero. Por lo tanto: se rechaza la H_0 y se aprueba H_1 .

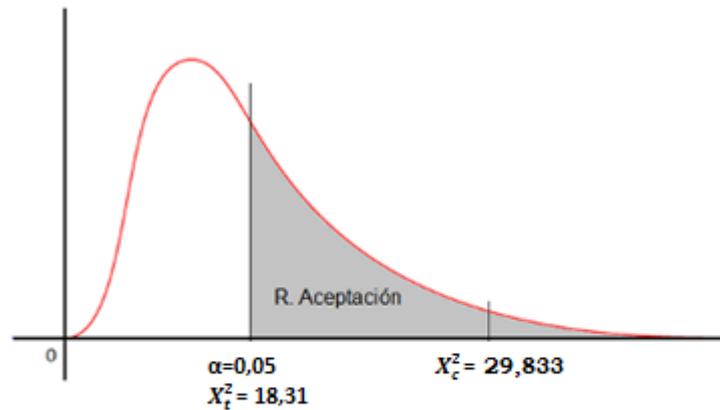


Figura 35: Gráfica Chi-Cuadrado
Elaborado por: Jorge R. López O.

⇒ **CONCLUSIÓN:** Todas las Técnicas de Tunneling, mejoran la coexistencia de IPv4 e IPv6, brindando un eficiente soporte de tráfico de VoIP.

Sin embargo, debemos mencionar y aclarar que la técnica más adecuada analizada en el presente trabajo investigativo y la que nos ofrece el mayor *Rendimiento* es la Técnica de Tunneling ISATAP.

Esto se debe a que esta técnica cumple con los requisitos y parámetros esenciales para una mejor transmisión de la información en tiempo real, los mismos que son:

- ☞ El mínimo Jitter, y
- ☞ La menor Latencia.

4.4 PRESENTACIÓN DE LA PROPUESTA DE COEXISTENCIA DE IPv4 E IPv6 CON TÉCNICAS DE TUNNELING

La Técnica de Tunneling que permite el mecanismo más adecuado de coexistencia de IPv4 e IPv6, debe seguir para su implementación los siguientes pasos:

1) Análisis y Diseño de una Topología de Red

Para lograr un mejor análisis y diseño de la topología de Red debemos tener presente lo siguiente:

- Intercambio de recursos
 - ↻ Archivos
 - ↻ Aplicaciones
 - ↻ Hardware
 - ↻ Conexión a Internet
 - ↻ Entre otras.
- Comunicación entre personas
 - ↻ Correo electrónico
 - ↻ Videollamadas o webconferencias
 - ↻ Datos en tiempo real
- Comunicación entre procesos
- Garantía de acceso único y universal a la información
 - ↻ Bases de datos en red
- Equipos activos y pasivos de una red
- Y, además criterios y aspectos técnicos que consigan un eficiente y efectivo análisis y diseño de la topología de red.

2) Determinación de un esquema de direccionamiento

Especificar la forma de interpretar la información contenida en cada campo, utilizando las técnicas de direccionamiento con los siguientes fines:

- ➔ Dar versatilidad
- ➔ Reducir el número de bits utilizados para alcanzar destinos desde un origen determinado.
- ➔ Disponibilidad de diferentes esquemas.
- ➔ Flexibilidad
- ➔ Tiempo

3) Diagrama de enrutamiento capa 3

- ➔ Mantenimiento de las tablas de enrutamiento.
- ➔ Protocolos de enrutamiento
 - ↻ RIP
 - ↻ IGRP
 - ↻ EIGRP
 - ↻ OSPF
 - ↻ Entre otros.

4) Configuración inicial de los routers

- ➔ Implementación
 - ↻ Equipo necesario
 - ↻ Esquema de pirámide
 - ↻ Configuración IP de los PC

- Cableado de la red, uso del cable de consola
- Configuración del router con los comandos IOS
 - ↳ IOS
 - ↳ Los diferentes modos de usuarios
 - ↳ Poner una contraseña al acceso Privilegiado
 - ↳ Configuración de las interfaces Ethernet del router
 - ↳ Configuración del acceso Telnet al router
- Conocer los comandos IOS básicos
 - ↳ Paso entre los diferentes modos de usuarios
 - ↳ Comandos de información
 - ↳ Comandos de interfaz
 - ↳ Comandos para hacer una copia de seguridad de la configuración actual
 - ↳ Comando de anulación
 - ↳ Anulación de un comando en particular
 - ↳ Cambiar el nombre del router
 - ↳ Poner una contraseña al usuario privilegiado
- Entre otras configuraciones más avanzadas.

5) Configuración de la Técnica de Tunneling

ISATAP

➤ Configuración R1

```
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
```

```
hostname R1
```

```
boot-start-marker
boot-end-marker

logging message-counter syslog
enable secret 5 $1$Snl6$xT5oVv6puavQZ3/Gh8L3X.

no aaa new-model
memory-size iomem 5

dot11 syslog
ip source-route

ip cef

ip dhcp pool red
  network 10.0.0.0 255.255.255.0
  default-router 10.0.0.1

no ip domain lookup
ipv6 unicast-routing
ipv6 cef

multilink bundle-name authenticated

voice-card 0

archive
  log config
  hidekeys

interface Tunnel0
  no ip address
  no ip redirects
  ipv6 address 123::/64 eui-64
  tunnel source 192.168.1.1
  tunnel mode ipv6ip isatap

interface FastEthernet0/0
  ip address 10.0.0.1 255.255.255.0
  duplex auto
  speed auto
  ipv6 address FEC0::1:1/112

interface FastEthernet0/1
  no ip address
  shutdown
  duplex auto
  speed auto

interface Serial0/0/0
  ip address 192.168.2.1 255.255.255.0

interface Serial0/0/1
  ip address 192.168.1.1 255.255.255.0
  clock rate 128000

router ospf 1
  log-adjacency-changes
  network 10.0.0.0 0.0.0.255 area 0
  network 192.168.1.0 0.0.0.255 area 0
  network 192.168.2.0 0.0.0.255 area 0

ip forward-protocol nd
no ip http server
```

```
no ip http secure-server

ipv6 route FEC0::4:0/112 123::5EFE:C0A8:302

control-plane

mgcp fax t38 ecm

gatekeeper
shutdown

line con 0
exec-timeout 0 0
logging synchronous
line aux 0
line vty 0 4
password tesis2012
login

scheduler allocate 20000 1000
end
```

➔ **Configuración R2**

```
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption

hostname R2

boot-start-marker
boot-end-marker

enable secret 5 $1$v4IH$tGPiSl699jxLQiDvDcRnF/

no aaa new-model

resource policy

memory-size iomem 5
ip subnet-zero
ip cef

no ip domain lookup
interface FastEthernet0/0
no shutdown
ip address 10.0.1.1 255.255.255.0
duplex auto
speed auto

interface Serial0/2/1
no shutdown
ip address 192.168.1.2 255.255.255.0
clock rate 2000000

interface FastEthernet0/1
no ip address
shutdown
duplex auto
speed auto

interface Serial0/0/1
```

```
no shutdown
ip address 192.168.3.1 255.255.255.0
clock rate 128000
```

```
interface Serial0/2
no ip address
shutdown
clock rate 2000000
```

```
interface Serial0/3
no ip address
shutdown
clock rate 2000000
```

```
router ospf 1
log-adjacency-changes
network 10.0.1.0 0.0.0.255 area 0
network 192.168.1.0 0.0.0.255 area 0
network 192.168.3.0 0.0.0.255 area 0
```

```
ip classless
```

```
no ip http server
no ip http secure-server
```

```
control-plane
```

```
line con 0
exec-timeout 0 0
logging synchronous
line aux 0
line vty 0 4
password tesis2012
login
```

```
end
```

➔ **Configuración R3**

```
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
```

```
hostname R3
```

```
boot-start-marker
boot-end-marker
```

```
enable secret 5 $1$QICj$Ynoxr6s.zF/8uIP6hNtjA/
no aaa new-model
```

```
resource policy
```

```
memory-size iomem 5
ip subnet-zero
ip cef
```

```
no ip domain lookup
```

```
interface FastEthernet0/0
no shutdown
ip address 10.0.2.1 255.255.255.0
```

```
duplex auto
speed auto

interface Serial0/0/1
no shutdown
ip address 192.168.4.1 255.255.255.0
clock rate 128000

interface FastEthernet0/1
no ip address
shutdown
duplex auto
speed auto

interface Serial0/2/1
no shutdown
ip address 192.168.2.2 255.255.255.0
clock rate 2000000

interface Serial0/2
no ip address
shutdown
clock rate 2000000

interface Serial0/3
no ip address
shutdown
clock rate 2000000

router ospf 1
log-adjacency-changes
network 10.0.2.0 0.0.0.255 area 0
network 192.168.2.0 0.0.0.255 area 0
network 192.168.4.0 0.0.0.255 area 0

ip classless

no ip http server
no ip http secure-server

control-plane

line con 0
exec-timeout 0 0
logging synchronous
line aux 0
line vty 0 4
password tesis2012
login

end
```

➔ **Configuración R4**

```
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption

hostname R4

boot-start-marker
boot-end-marker
```

```
logging message-counter syslog
enable secret 5 $1$mMDI$.ksJxmpvSioqWT8DFWObA/
```

```
no aaa new-model
memory-size iomem 5
```

```
dot11 syslog
ip source-route
```

```
ip cef
```

```
ip dhcp pool red
 network 10.0.3.0 255.255.255.0
 default-router 10.0.3.1
```

```
no ip domain lookup
ipv6 unicast-routing
ipv6 cef
```

```
multilink bundle-name authenticated
```

```
voice-card 0
```

```
archive
 log config
  hidekeys
```

```
interface Tunnel0
 no ip address
 no ip redirects
 ipv6 address 123::/64 eui-64
 tunnel source 192.168.3.2
 tunnel mode ipv6ip isatap
```

```
interface FastEthernet0/0
 ip address 10.0.3.1 255.255.255.0
 duplex auto
 speed auto
 ipv6 address FEC0::4:1/112
```

```
interface FastEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
```

```
interface Serial0/0/0
 ip address 192.168.4.2 255.255.255.0
```

```
interface Serial0/0/1
 ip address 192.168.3.2 255.255.255.0
```

```
router ospf 1
 log-adjacency-changes
 network 10.0.3.0 0.0.0.255 area 0
 network 192.168.3.0 0.0.0.255 area 0
 network 192.168.4.0 0.0.0.255 area 0
```

```
ip forward-protocol nd
no ip http server
no ip http secure-server
```

```
ipv6 route FEC0::1:0/112 123::5EFE:C0A8:101
 control-plane
```

```
mgcp fax t38 ecm
```

```
gatekeeper  
shutdown
```

```
line con 0  
exec-timeout 0 0  
logging synchronous  
line aux 0  
line vty 0 4  
password tesis2012  
login
```

```
scheduler allocate 20000 1000  
end
```

CONCLUSIONES

1. En comunicaciones en tiempo real, los factores determinantes son el Jitter y la Latencia, es por eso que luego de realizar todas las mediciones necesarias en los diferentes escenarios de prueba podemos mencionar que la Técnica de Tunneling ISATAP es la que mejor cumple con estos requerimientos.
2. Sin Técnicas de Tunneling, se pudo determinar que el Jitter más elevado (2,65 ms.) y el mejor Ancho de Banda lo tiene IPv6 (118 Kbps), mientras que la mayor Latencia (80,07 ms.) ocurre en IPv4.
3. Al implementar las Técnicas de Tunneling, se estableció que el Jitter más elevado y la mayor Latencia los encontramos en la Técnica de Tunneling GRE con valores de 2,89ms. y 81,75ms., respectivamente. A su vez, el mejor Ancho de Banda lo obtenemos de la Técnica de Tunneling ISATAP con un valor de 115,67 Kbps.
4. Según los Administradores de Red encuestados, junto con la experiencia personal se deduce que GRE es la Técnica de Tunneling que lleva menos tiempo para su implementación y presenta una reducida dificultad de configuración, administración y monitoreo. ISATAP exige un mayor grado de conocimiento, configuración de direcciones IP, configuración de MTU (Unidades Máximas de Transmisión), keep-alives, etc., por lo que requiere mayor tiempo para implementarse y su grado de dificultad también aumenta en comparación con las otras Técnicas de Tunneling analizadas. 6to4 presenta un relativo equilibrio en los índices investigados.

5. Luego del análisis respectivo, conseguimos comprobar que en las tres Técnicas de Tunneling (6to4, ISATAP y GRE) existe un relativo balance en lo que respecta a la transmisión de Paquetes RTP. Sin embargo, la Técnica de Tunneling que más evidencia la pérdida de Paquetes RTP, la encontramos en la Técnica de Tunneling GRE con un valor porcentual de eficiencia que no alcanza ni el 1%, ISATAP mejora este nivel subiéndolo al 33% y 6to4 prácticamente no tiene pérdida de Paquetes RTP.

RECOMENDACIONES

1. Impulsar estudios complementarios que permitan mejorar la coexistencia entre redes IPv4 e IPv6.
2. Realizar el análisis de otras Técnicas de Tunneling, como por ejemplo: Tunneling manual de IPv6 a IPv4, Teredo, Proto 41, etc., para evaluar de mejor manera los resultados obtenidos en este proceso investigativo. Es decir, que permitan mejorar la visión de un mundo más cambiante en lo que respecta a las Tecnologías de la Información y el Conocimiento TIC's.
3. Fomentar estudios de VoIP, que consigan conjugar varios mundos de transmisión utilizando una sola infraestructura de red.
4. Emitir políticas y regulaciones que impulsen, promuevan y obliguen a la adopción de IPv6 en el país.

GLOSARIO

- ⇒ **QoS** = Calidad de Servicio
- ⇒ **CoS** = Clase de servicio (CoS)
- ⇒ **ISP (Internet Service Provider)** = Empresa que brinda conexión a Internet a sus clientes.
- ⇒ **GRE (Generic Routing Encapsulation)** = Protocolo originalmente desarrollado por Cisco Systems y se ha convertido en un estándar de la industria definido en las RFC 1701, 1702 y 2784.
- ⇒ **ISATAP (Intra-Site Automatic Tunnel Addressing Protocol)**
- ⇒ **TB (Tunnel Broker)**
- ⇒ **RFC** = Documento que puede ser escrito por cualquier persona y que contiene una propuesta para una nueva tecnología, información acerca del uso de tecnologías y/o recursos existentes, propuestas para mejoras de tecnologías, proyectos experimentales y demás.
- ⇒ **VPN** = Red Privada Virtual.
- ⇒ **PBX** = Equipo conmutador tradicional in situ que una institución utiliza para sus servicios de telefonía.
- ⇒ **PBX IP** = Equipo conmutador in situ para telefonía IP.
- ⇒ **IP Centrex** = Todos los servicios y recursos de conmutación para telefonía se encuentran en la red.
- ⇒ **RIR (Regional Internet Registry)** = Registro Regional de Internet
- ⇒ **Unicast** = Identifican a una sola interfaz
- ⇒ **Anycast** = Identifican a un conjunto de interfaces
- ⇒ **Multicast** = Identifican un grupo de interfaces

- ⇒ **CIDR (Classless Inter-Domain Routing)** = Enrutamiento entre dominios sin clases
- ⇒ **BGP (Border Gateway Protocol)** = Protocolo mediante el cual se intercambia información de encaminamiento entre sistemas autónomos.
- ⇒ **IETF (Internet Engineering Task Force)** es una organización internacional abierta de normalización, que tiene como objetivos el contribuir a la ingeniería de Internet, actuando en diversas áreas, como transporte, encaminamiento, seguridad.
- ⇒ **NGTrans (Next Generation Transition)** Transición de Próxima Generación
- ⇒ **MPLS (Multiprotocol Label Switching)** es un mecanismo de transporte de datos estándar creado por la IETF y definido en el RFC 3031, opera entre la capa de enlace de datos y la capa de red del modelo OSI.
- ⇒ **NRI (Networked Readiness Index)** mide de la propensión de los países a aprovechar las oportunidades que ofrecen las tecnologías de información y comunicaciones. Se publica anualmente y busca comprender mejor el impacto de las TIC en la competitividad de las naciones.

BIBLIOGRAFÍA

LIBROS

- [1] **BLANCHET., M.**, Migrating to IPv6: A practical Guide to Implementing IPv6 in Mobile and Fixed Networks., Québec - Canadá., John Wiley & Sons. Ltd., 2006., Pp. 454
- [2] **GRANADOS., R.**, Transición de IPv4 a IPv6 en las Empresas., Universidad del Valle de México., Tlalpan - México., Pp. 16
- [3] **MARRAKECH, M.**, IPv4 and IPv6 Integration, IPv6 Deployment and Support., París - Francia., 2009., Pp. 58
- [4] **STALLINGS, W.**, Comunicaciones y Redes de Computadores., Traducido del Inglés por Jesús Díaz Verdejo y Juan José Ramos., 7ma.Edi., Madrid - España., Pearson Educación S. A., 2004., Pp. 896

GUÍAS CISCO

- [5] **CCNP ROUTE 642-902** Official Certification Guide Implementing Cisco IP Routing., Pp. 919
<http://222.199.6.188/uploadfile/kczy/ckjc/CCNP%E8%AE%A4%E8%AF%81%E6%8C%87%E5%8D%97-%E8%B7%AF%E7%94%B1-%E8%8B%B1%E6%96%87%E7%89%88.pdf>
[2012-10-12]

[6] **CCNP ROUTE 642-902** Quick Reference Implementing Cisco IP Routing., Pp. 156
http://113.161.227.204:8008/thuvienso/bitstream/123456789/5642/1/ROUTE_642-902_Quick_Reference.pdf
[2012-10-12]

[7] **CCNP ROUTE 642-813** Implementing Cisco IP Switched Networks., Pp. 511
<http://222.199.6.188/uploadfile/kczy/ckjc/CCNP%E8%AE%A4%E8%AF%81%E6%8C%87%E5%8D%97-%E4%BA%A4%E6%8D%A2-%E8%8B%B1%E6%96%87%E7%89%88.pdf>
[2012-10-12]

[8] **CCNP ROUTE 642-832** Troubleshooting and Maintaining Cisco IP Networks., Pp. 614
<http://222.199.6.188/uploadfile/kczy/ckjc/CCNP%E8%AE%A4%E8%AF%81%E6%8C%87%E5%8D%97-%E6%8E%92%E9%94%99-%E8%8B%B1%E6%96%87%E7%89%88.pdf>
[2012-10-12]

TESIS

[9] **KOTAL, V.**, Principles, implementation and transition to IPv6 protocol., Universidad de Karlova., Praga - República Checa., PhD Thesis., 2005.

ENLACES DE INTERNET

[10] Migrating to IPv6: A practical Guide to Implementing IPv6 in Mobile and Fixed Networks

<https://void.gr/kargig/ipv6/migrating-to-ipv6-a-practical-guide-to-implementing-ipv6-in-mobile-and-fixed-networks.9780471498926.37343.pdf>

[2012-10-30]

[11] Transición de IPv4 a IPv6 en las Empresas

http://www.tlalpan.uvmnet.edu/oiid/download/Telecomunicaciones%20en%20empresa_04_PO_ISC_PIT_E.pdf

[2012-10-30]

[12] IPv4 and IPv6 Integration

http://www.6deploy.eu/tutorials/130-6deploy_ipv6_transition_v0_3.pdf

[2012-10-30]

[13] IPv6 Deployment and Support

<http://www.6deploy.eu/index.php?page=tutorials>

[2012-10-30]

[14] Cisco. Implementing IPv6 Addressing and Basic Connectivity

http://www.cisco.com/en/US/docs/ios/ipv6/configuration/guide/ip6-addrg_bsc_con.html

[2012-10-30]

[15] **Reporte de terminación de direcciones IPv4**

<http://www.lacnic.net/es/web/lacnic/reporte-direcciones-ipv4>

[2012-10-30]

[16] **Migración de IPv4 a IPv6**

<http://www.slideshare.net/gmarinfr/migracion-ipv4-ipv6>

[2012-10-30]

[17] **Estado del IPv6: ¿Coexistir o no coexistir?**

<http://lmdatacommunications.com/wordpress1/2012/05/16/situacion-del-ipv6-2/>

[2012-10-30]

[18] **Elastix como solución Asterisk**

<http://www.slideshare.net/jarvey4/elastic-como-solucion-asterisk>

[2012-10-30]

[19] **Internet Engineering Task Force IPv6**

<http://www.ietf.org>

[2012-10-30]

[20] **ECUADOR.**, Ministerio de Telecomunicaciones., Augusto Espín

<http://www.mintel.gob.ec>

augusto.espin @mintel.gob.ec

[2012-11-15]

[21] **ESPAÑA.**, Consulintel., Jordi Palet Martínez

<http://www.consulintel.es>

jordi.palet@consulintel.es

[2012-11-15]

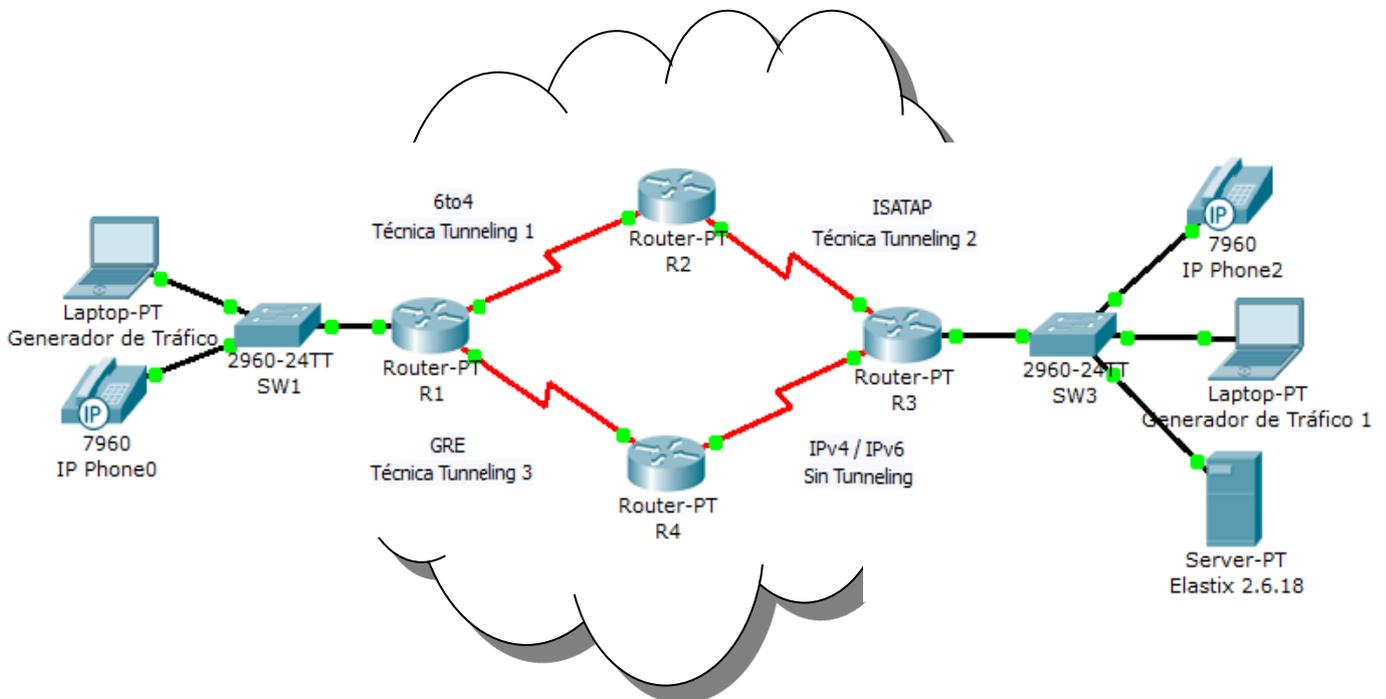
ANEXOS

ANEXO 1

INSTALACIÓN Y CONFIGURACIÓN DE LAS TÉCNICAS DE TUNNELING CON SOPORTE A TRÁFICO VoIP

INSTALACIÓN Y CONFIGURACIÓN DE LAS TÉCNICAS DE TUNNELING CON SOPORTE A TRÁFICO VoIP

1.1 INSTALACIÓN



1.2 CONFIGURACIÓN

1.2.1 Sólo IPv4

⇒ Configuración R1

```
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption

hostname R1

boot-start-marker
boot-end-marker

logging message-counter syslog
enable secret 5 $1$Snl6$xT5oVv6puavQZ3/Gh8L3X.

no aaa new-model
memory-size iomem 5

dot11 syslog
ip source-route
ip cef

ip dhcp pool red
network 10.0.0.0 255.255.255.0
default-router 10.0.0.1
```

```
no ip domain lookup
no ipv6 cef

multilink bundle-name authenticated

voice-card 0

archive
log config
hidekeys

interface FastEthernet0/0
ip address 10.0.0.1 255.255.255.0
duplex auto
speed auto

interface FastEthernet0/1
no ip address
shutdown
duplex auto
speed auto

interface Serial0/0/0
ip address 192.168.2.1 255.255.255.0

interface Serial0/0/1
ip address 192.168.1.1 255.255.255.0
clock rate 128000

router ospf 1
log-adjacency-changes
network 10.0.0.0 0.0.0.255 area 0
network 192.168.1.0 0.0.0.255 area 0
network 192.168.2.0 0.0.0.255 area 0

ip forward-protocol nd
no ip http server
no ip http secure-server

control-plane

mgcp fax t38 ecm

gatekeeper
shutdown

line con 0
exec-timeout 0 0
logging synchronous
line aux 0
line vty 0 4
password tesis2012
login

scheduler allocate 20000 1000
end
```

➔ **Configuración R2**

```
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
```

```
hostname R2

boot-start-marker
boot-end-marker

enable secret 5 $1$v4IH$tGPiSI699jxLQiDvDcRnF/

no aaa new-model

resource policy

memory-size iomem 5
ip subnet-zero
ip cef

no ip domain lookup

interface FastEthernet0/0
no shutdown
ip address 10.0.1.1 255.255.255.0
duplex auto
speed auto

interface Serial0/2/1
no shutdown
ip address 192.168.1.2 255.255.255.0
clock rate 2000000

interface FastEthernet0/1
no ip address
shutdown
duplex auto
speed auto

interface Serial0/0/1
no shutdown
ip address 192.168.3.1 255.255.255.0
clock rate 128000

interface Serial0/2
no ip address
shutdown
clock rate 2000000

interface Serial0/3
no ip address
shutdown
clock rate 2000000

router ospf 1
log-adjacency-changes
network 10.0.1.0 0.0.0.255 area 0
network 192.168.1.0 0.0.0.255 area 0
network 192.168.3.0 0.0.0.255 area 0

ip classless
no ip http server
no ip http secure-server

control-plane

line con 0
exec-timeout 0 0
logging synchronous
```

```
line aux 0
line vty 0 4
password tesis2012
login

end
```

➔ **Configuración R3**

```
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption

hostname R3

boot-start-marker
boot-end-marker

enable secret 5 $1$QICj$Ynoxr6s.zF/8uIP6hNtjA/

no aaa new-model

resource policy

memory-size iomem 5
ip subnet-zero
ip cef

no ip domain lookup

interface FastEthernet0/0
no shutdown
ip address 10.0.2.1 255.255.255.0
duplex auto
speed auto

interface Serial0/0/1
no shutdown
ip address 192.168.4.1 255.255.255.0
clock rate 128000

interface FastEthernet0/1
no ip address
shutdown
duplex auto
speed auto

interface Serial0/2/1
no shutdown
ip address 192.168.2.2 255.255.255.0
clock rate 2000000

interface Serial0/2
no ip address
shutdown
clock rate 2000000

interface Serial0/3
no ip address
shutdown
clock rate 2000000
router ospf 1
log-adjacency-changes
```

```
network 10.0.2.0 0.0.0.255 area 0
network 192.168.2.0 0.0.0.255 area 0
network 192.168.4.0 0.0.0.255 area 0
```

```
ip classless
```

```
no ip http server
no ip http secure-server
```

```
control-plane
```

```
line con 0
exec-timeout 0 0
logging synchronous
line aux 0
line vty 0 4
password tesis2012
login
```

```
end
```

➔ **Configuración R4**

```
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption

hostname R4

boot-start-marker
boot-end-marker

logging message-counter syslog
enable secret 5 $1$mMDI$.ksJxmpvSioqWT8DFWObA/

no aaa new-model
memory-size iomem 5

dot11 syslog
ip source-route

ip cef

ip dhcp pool red
network 10.0.3.0 255.255.255.0
default-router 10.0.3.1

no ip domain lookup
no ipv6 cef

multilink bundle-name authenticated

voice-card 0

archive
log config
hidekeys

interface FastEthernet0/0
no shutdown
ip address 10.0.3.1 255.255.255.0
duplex auto
speed auto
```

```
interface FastEthernet0/1
no ip address
shutdown
duplex auto
speed auto

interface Serial0/0/0
no shutdown
ip address 192.168.4.2 255.255.255.0

interface Serial0/0/1
no shutdown
ip address 192.168.3.2 255.255.255.0

router ospf 1
log-adjacency-changes
network 10.0.3.0 0.0.0.255 area 0
network 192.168.3.0 0.0.0.255 area 0
network 192.168.4.0 0.0.0.255 area 0

ip forward-protocol nd
no ip http server
no ip http secure-server

control-plane

mgcp fax t38 ecm

gatekeeper
shutdown

line con 0
exec-timeout 0 0
logging synchronous
line aux 0
line vty 0 4
password tesis2012
login

scheduler allocate 20000 1000
end
```

1.2.2 Sólo IPv6

➔ Configuración R1

```
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption

hostname R1

boot-start-marker
boot-end-marker

enable secret 5 $1$SnI6$xT5oVv6puavQZ3/Gh8L3X.

no aaa new-model

resource policy

memory-size iomem 5
```

```
ip subnet-zero
ip cef

no ip domain lookup

ipv6 unicast-routing
ipv6 cef

interface FastEthernet0/0
no shutdown
no ip address
duplex auto
speed auto
ipv6 address FEC0::1:1/112
ipv6 ospf 1 area 0

interface Serial0/0/1
no shutdown
no ip address
ipv6 address 2001::1:1/112
ipv6 ospf 1 area 0
clock rate 128000
interface FastEthernet0/1
no ip address
shutdown
duplex auto
speed auto

interface Serial0/0/0
no shutdown
no ip address
ipv6 address 2001::2:1/112
ipv6 ospf 1 area 0
clock rate 128000

interface Serial0/2
no ip address
shutdown
clock rate 2000000

interface Serial0/3
no ip address
shutdown
clock rate 2000000

ip classless

no ip http server
no ip http secure-server

ipv6 router ospf 1
router-id 1.1.1.1
log-adjacency-changes

control-plane

line con 0
exec-timeout 0 0
logging synchronous
line aux 0
line vty 0 4
password tesis2012
login
end
```

➤ **Configuración R2**

```
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption

hostname R2

boot-start-marker
boot-end-marker

enable secret 5 $1$v4IH$tGPiSI699jxLQiDvDcRnF/

no aaa new-model

resource policy

memory-size iomem 5
ip subnet-zero
ip cef

no ip domain lookup

ipv6 unicast-routing
ipv6 cef
interface FastEthernet0/0
no ip address
duplex auto
speed auto
ipv6 address FEC0::2:1/112
ipv6 ospf 1 area 0

interface Serial0/2/1
no shutdown
no ip address
ipv6 address 2001::1:2/112
ipv6 ospf 1 area 0
clock rate 2000000

interface FastEthernet0/1
no ip address
shutdown
duplex auto
speed auto

interface Serial0/0/1
no shutdown
no ip address
ipv6 address 2001::3:1/112
ipv6 ospf 1 area 0
clock rate 128000

interface Serial0/2
no ip address
shutdown
clock rate 2000000
interface Serial0/3
no ip address
shutdown
clock rate 2000000

ip classless
no ip http server
```

```
no ip http secure-server

ipv6 router ospf 1
router-id 2.2.2.2
log-adjacency-changes

control-plane

line con 0
exec-timeout 0 0
logging synchronous
line aux 0
line vty 0 4
password tesis2012
login

end
```

➔ **Configuración R3**

```
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption

hostname R3

boot-start-marker
boot-end-marker

enable secret 5 $1$QICj$Ynoxr6s.zF/8uIP6hNtjA/

no aaa new-model

resource policy

memory-size iomem 5
ip subnet-zero
ip cef

no ip domain lookup

ipv6 unicast-routing
ipv6 cef

interface FastEthernet0/0
no ip address
duplex auto
speed auto
ipv6 address FEC0::3:1/112
ipv6 ospf 1 area 0

interface Serial0/0/1
no shutdown
no ip address
ipv6 address 2001::4:1/112
ipv6 ospf 1 area 0
clock rate 128000

interface FastEthernet0/1
no ip address
shutdown
duplex auto
speed auto
```

```
interface Serial0/2/1
no shutdown
no ip address
ipv6 address 2001::2:2/112
ipv6 ospf 1 area 0
clock rate 2000000
```

```
interface Serial0/2
no ip address
shutdown
clock rate 2000000
```

```
interface Serial0/3
no ip address
shutdown
clock rate 2000000
```

```
ip classless
```

```
no ip http server
no ip http secure-server
```

```
ipv6 router ospf 1
router-id 3.3.3.3
log-adjacency-changes
```

```
control-plane
```

```
line con 0
exec-timeout 0 0
logging synchronous
line aux 0
line vty 0 4
password tesis2012
login
end
```

➡ **Configuración R4**

```
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
```

```
hostname R4
```

```
boot-start-marker
boot-end-marker
```

```
enable secret 5 $1$mMDI$.ksJxmpvSioqWT8DFWObA/
```

```
no aaa new-model
```

```
resource policy
```

```
memory-size iomem 5
ip subnet-zero
ip cef
```

```
no ip domain lookup
```

```
ipv6 unicast-routing
ipv6 cef
```

```
interface FastEthernet0/0
no shutdown
no ip address
duplex auto
speed auto
ipv6 address FEC0::4:1/112
ipv6 ospf 1 area 0
```

```
interface Serial0/0/0
no shutdown
no ip address
ipv6 address 2001::4:2/112
ipv6 ospf 1 area 0
clock rate 2000000
```

```
interface FastEthernet0/1
no ip address
shutdown
duplex auto
speed auto
```

```
interface Serial0/0/1
no shutdown
no ip address
ipv6 address 2001::3:2/112
ipv6 ospf 1 area 0
clock rate 2000000
```

```
interface Serial0/2
no ip address
shutdown
clock rate 2000000
```

```
interface Serial0/3
no ip address
shutdown
clock rate 2000000
```

```
ip classless
```

```
no ip http server
no ip http secure-server
```

```
ipv6 router ospf 1
router-id 4.4.4.4
log-adjacency-changes
```

```
control-plane
```

```
line con 0
exec-timeout 0 0
logging synchronous
line aux 0
line vty 0 4
password tesis2012
login
end
```

1.2.3 6to4

⇒ Configuración R1

version 12.4

```
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
```

```
hostname R1
```

```
boot-start-marker
boot-end-marker
```

```
enable secret 5 $1$Snl6$xT5oVv6puavQZ3/Gh8L3X.
```

```
no aaa new-model
```

```
resource policy
```

```
memory-size iomem 5
ip subnet-zero
ip cef
```

```
no ip domain lookup
```

```
ipv6 unicast-routing
ipv6 general-prefix tunnel 6to4 Serial0/0/1
ipv6 cef
```

```
interface Tunnel0
no shutdown
no ip address
no ip redirects
ipv6 address 2002:C0A8:101::1/64
tunnel source Serial0/0/1
tunnel mode ipv6ip 6to4
```

```
interface FastEthernet0/0
no shutdown
no ip address
duplex auto
speed auto
ipv6 address FEC0::1:1/112
```

```
interface Serial0/0/1
no shutdown
ip address 192.168.1.1 255.255.255.0
clock rate 128000
```

```
interface FastEthernet0/1
no ip address
shutdown
duplex auto
speed auto
```

```
interface Serial0/0/0
no shutdown
ip address 192.168.2.1 255.255.255.0
clock rate 128000
```

```
interface Serial0/2
no ip address
shutdown
clock rate 2000000
```

```
interface Serial0/3
no ip address
shutdown
```

```
clock rate 2000000

router ospf 1
log-adjacency-changes
network 10.0.0.0 0.0.0.255 area 0
network 192.168.1.0 0.0.0.255 area 0
network 192.168.2.0 0.0.0.255 area 0

ip classless

no ip http server
no ip http secure-server

ipv6 route 2002::/16 Tunnel0
ipv6 route FEC0::4:0/112 2002:C0A8:302::2
ipv6 router ospf 1
router-id 1.1.1.1
log-adjacency-changes

control-plane
line con 0
exec-timeout 0 0
logging synchronous
line aux 0
line vty 0 4
password tesis2012
login

end
```

➡ **Configuración R2**

```
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption

hostname R2

boot-start-marker
boot-end-marker

enable secret 5 $1$v4IH$tGPiSI699jxLQiDvDcRnF/

no aaa new-model

resource policy

memory-size iomem 5
ip subnet-zero
ip cef

no ip domain lookup

interface FastEthernet0/0
no shutdown
ip address 10.0.1.1 255.255.255.0
duplex auto
speed auto

interface Serial0/2/1
no shutdown
ip address 192.168.1.2 255.255.255.0
clock rate 2000000
```

```
interface FastEthernet0/1
no ip address
shutdown
duplex auto
speed auto

interface Serial0/0/1
no shutdown
ip address 192.168.3.1 255.255.255.0
clock rate 128000

interface Serial0/2
no ip address
shutdown
clock rate 2000000

interface Serial0/3
no ip address
shutdown
clock rate 2000000

router ospf 1
log-adjacency-changes
network 10.0.1.0 0.0.0.255 area 0
network 192.168.1.0 0.0.0.255 area 0
network 192.168.3.0 0.0.0.255 area 0

ip classless

no ip http server
no ip http secure-server

control-plane

line con 0
exec-timeout 0 0
logging synchronous
line aux 0
line vty 0 4
password tesis2012
login

end
```

➔ **Configuración R3**

```
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption

hostname R3

boot-start-marker
boot-end-marker

enable secret 5 $1$QICj$Ynoxr6s.zF/8uIP6hNtjA/

no aaa new-model
resource policy

memory-size iomem 5
ip subnet-zero
ip cef
```

```
no ip domain lookup

interface FastEthernet0/0
no shutdown
ip address 10.0.2.1 255.255.255.0
duplex auto
speed auto

interface Serial0/0/1
no shutdown
ip address 192.168.4.1 255.255.255.0
clock rate 128000

interface FastEthernet0/1
no ip address
shutdown
duplex auto
speed auto

interface Serial0/2/1
no shutdown
ip address 192.168.2.2 255.255.255.0
clock rate 2000000

interface Serial0/2
no ip address
shutdown
clock rate 2000000

interface Serial0/3
no ip address
shutdown
clock rate 2000000

router ospf 1
log-adjacency-changes
network 10.0.2.0 0.0.0.255 area 0
network 192.168.2.0 0.0.0.255 area 0
network 192.168.4.0 0.0.0.255 area 0

ip classless

no ip http server
no ip http secure-server

control-plane

line con 0
exec-timeout 0 0
logging synchronous
line aux 0
line vty 0 4
password tesis2012
login

end
```

➔ **Configuración R4**

```
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
```

```
hostname R4

boot-start-marker
boot-end-marker

enable secret 5 $1$mMDI$.ksJxmpvSioqWT8DFWObA/

no aaa new-model

resource policy

memory-size iomem 5
ip subnet-zero
ip cef

no ip domain lookup

ipv6 unicast-routing
ipv6 general-prefix tunnel 6to4 Serial0/0/1
ipv6 cef

interface Tunnel0
no shutdown
no ip address
no ip redirects
ipv6 address 2002:C0A8:302::2/64
tunnel source Serial0/0/1
tunnel mode ipv6ip 6to4

interface FastEthernet0/0
no shutdown
no ip address
duplex auto
speed auto
ipv6 address FEC0::4:1/112

interface Serial0/0/0
no shutdown
ip address 192.168.4.2 255.255.255.0
clock rate 2000000

interface FastEthernet0/1
no ip address
shutdown
duplex auto
speed auto

interface Serial0/0/1
no shutdown
ip address 192.168.3.2 255.255.255.0
clock rate 2000000

interface Serial0/2
no ip address
shutdown
clock rate 2000000

interface Serial0/3
no ip address
shutdown
clock rate 2000000

router ospf 1
log-adjacency-changes
```

```
network 10.0.3.0 0.0.0.255 area 0
network 192.168.3.0 0.0.0.255 area 0
network 192.168.4.0 0.0.0.255 area 0

ip classless

no ip http server
no ip http secure-server

ipv6 route 2002::/16 Tunnel0
ipv6 route FEC0::1:0/112 2002:C0A8:101::1

control-plane

line con 0
exec-timeout 0 0
logging synchronous
line aux 0
line vty 0 4
password tesis2012
login

end
```

1.2.4 ISATAP

➔ Configuración R1

```
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption

hostname R1

boot-start-marker
boot-end-marker

logging message-counter syslog
enable secret 5 $1$Snl6$XT5oVv6puavQZ3/Gh8L3X.

no aaa new-model
memory-size iomem 5

dot11 syslog
ip source-route

ip cef

ip dhcp pool red
network 10.0.0.0 255.255.255.0
default-router 10.0.0.1

no ip domain lookup
ipv6 unicast-routing
ipv6 cef

multilink bundle-name authenticated

voice-card 0

archive
log config
```

```
hidekeys

interface Tunnel0
no ip address
no ip redirects
ipv6 address 123::/64 eui-64
tunnel source 192.168.1.1
tunnel mode ipv6ip isatap

interface FastEthernet0/0
ip address 10.0.0.1 255.255.255.0
duplex auto
speed auto
ipv6 address FEC0::1:1/112

interface FastEthernet0/1
no ip address
shutdown
duplex auto
speed auto

interface Serial0/0/0
ip address 192.168.2.1 255.255.255.0

interface Serial0/0/1
ip address 192.168.1.1 255.255.255.0
clock rate 128000

router ospf 1
log-adjacency-changes
network 10.0.0.0 0.0.0.255 area 0
network 192.168.1.0 0.0.0.255 area 0
network 192.168.2.0 0.0.0.255 area 0

ip forward-protocol nd
no ip http server
no ip http secure-server

ipv6 route FEC0::4:0/112 123::5EFE:C0A8:302

control-plane

mgcp fax t38 ecm

gatekeeper
shutdown

line con 0
exec-timeout 0 0
logging synchronous
line aux 0
line vty 0 4
password tesis2012
login

scheduler allocate 20000 1000
end
```

➔ **Configuración R2**

```
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
```

```
hostname R2

boot-start-marker
boot-end-marker

enable secret 5 $1$v4IH$tGPiSI699jxLQiDvDcRnF/

no aaa new-model

resource policy

memory-size iomem 5
ip subnet-zero
ip cef

no ip domain lookup
interface FastEthernet0/0
no shutdown
ip address 10.0.1.1 255.255.255.0
duplex auto
speed auto

interface Serial0/2/1
no shutdown
ip address 192.168.1.2 255.255.255.0
clock rate 2000000

interface FastEthernet0/1
no ip address
shutdown
duplex auto
speed auto

interface Serial0/0/1
no shutdown
ip address 192.168.3.1 255.255.255.0
clock rate 128000

interface Serial0/2
no ip address
shutdown
clock rate 2000000

interface Serial0/3
no ip address
shutdown
clock rate 2000000

router ospf 1
log-adjacency-changes
network 10.0.1.0 0.0.0.255 area 0
network 192.168.1.0 0.0.0.255 area 0
network 192.168.3.0 0.0.0.255 area 0

ip classless

no ip http server
no ip http secure-server

control-plane

line con 0
exec-timeout 0 0
logging synchronous
```

```
line aux 0
line vty 0 4
password tesis2012
login

end
```

➔ **Configuración R3**

```
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption

hostname R3

boot-start-marker
boot-end-marker

enable secret 5 $1$QICj$Ynoxr6s.zF/8uIP6hNtjA/
no aaa new-model

resource policy

memory-size iomem 5
ip subnet-zero
ip cef

no ip domain lookup

interface FastEthernet0/0
no shutdown
ip address 10.0.2.1 255.255.255.0
duplex auto
speed auto

interface Serial0/0/1
no shutdown
ip address 192.168.4.1 255.255.255.0
clock rate 128000

interface FastEthernet0/1
no ip address
shutdown
duplex auto
speed auto

interface Serial0/2/1
no shutdown
ip address 192.168.2.2 255.255.255.0
clock rate 2000000

interface Serial0/2
no ip address
shutdown
clock rate 2000000

interface Serial0/3
no ip address
shutdown
clock rate 2000000

router ospf 1
log-adjacency-changes
```

```
network 10.0.2.0 0.0.0.255 area 0
network 192.168.2.0 0.0.0.255 area 0
network 192.168.4.0 0.0.0.255 area 0
```

```
ip classless
```

```
no ip http server
no ip http secure-server
```

```
control-plane
```

```
line con 0
exec-timeout 0 0
logging synchronous
line aux 0
line vty 0 4
password tesis2012
login
```

```
end
```

➔ **Configuración R4**

```
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption

hostname R4

boot-start-marker
boot-end-marker

logging message-counter syslog
enable secret 5 $1$mMDI$.ksJxmpvSioqWT8DFWObA/

no aaa new-model
memory-size iomem 5

dot11 syslog
ip source-route

ip cef

ip dhcp pool red
network 10.0.3.0 255.255.255.0
default-router 10.0.3.1

no ip domain lookup
ipv6 unicast-routing
ipv6 cef

multilink bundle-name authenticated

voice-card 0

archive
log config
hidekeys

interface Tunnel0
no ip address
no ip redirects
ipv6 address 123::/64 eui-64
```

```
tunnel source 192.168.3.2
tunnel mode ipv6ip isatap

interface FastEthernet0/0
ip address 10.0.3.1 255.255.255.0
duplex auto
speed auto
ipv6 address FEC0::4:1/112

interface FastEthernet0/1
no ip address
shutdown
duplex auto
speed auto

interface Serial0/0/0
ip address 192.168.4.2 255.255.255.0

interface Serial0/0/1
ip address 192.168.3.2 255.255.255.0

router ospf 1
log-adjacency-changes
network 10.0.3.0 0.0.0.255 area 0
network 192.168.3.0 0.0.0.255 area 0
network 192.168.4.0 0.0.0.255 area 0

ip forward-protocol nd
no ip http server
no ip http secure-server

ipv6 route FEC0::1:0/112 123::5EFE:C0A8:101

control-plane

mgcp fax t38 ecm

gatekeeper
shutdown

line con 0
exec-timeout 0 0
logging synchronous
line aux 0
line vty 0 4
password tesis2012
login

scheduler allocate 20000 1000
end
```

1.2.5 GRE

⇒ Configuración R1

```
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption

hostname R1

boot-start-marker
```

```
boot-end-marker

logging message-counter syslog
enable secret 5 $1$SnI6$XT5oVv6puavQZ3/Gh8L3X.

no aaa new-model
memory-size iomem 5

dot11 syslog
ip source-route

ip cef

ip dhcp pool red
  network 10.0.0.0 255.255.255.0
  default-router 10.0.0.1

no ip domain lookup
ipv6 unicast-routing
ipv6 cef

multilink bundle-name authenticated

voice-card 0

archive
  log config
  hidekeys

interface Tunnel0
no shutdown
no ip address
ipv6 address 2001::1:1/64
tunnel source 192.168.1.1
tunnel destination 192.168.4.2

interface FastEthernet0/0
no shutdown
ip address 10.0.0.1 255.255.255.0
duplex auto
speed auto
ipv6 address FEC0::1:1/112

interface FastEthernet0/1
no ip address
shutdown
duplex auto
speed auto

interface Serial0/0/0
no shutdown
ip address 192.168.2.1 255.255.255.0

interface Serial0/0/1
no shutdown
ip address 192.168.1.1 255.255.255.0
clock rate 128000
router ospf 1
  log-adjacency-changes
  network 10.0.0.0 0.0.0.255 area 0
  network 192.168.1.0 0.0.0.255 area 0
  network 192.168.2.0 0.0.0.255 area 0

ip forward-protocol nd
```

```
no ip http server
no ip http secure-server
```

```
ipv6 route ::/0 Tunnel0
```

```
control-plane
```

```
mgcp fax t38 ecm
```

```
gatekeeper
shutdown
```

```
line con 0
exec-timeout 0 0
logging synchronous
line aux 0
line vty 0 4
password tesis2012
login
```

```
scheduler allocate 20000 1000
end
```

➔ **Configuración R2**

```
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
```

```
hostname R2
```

```
boot-start-marker
boot-end-marker
```

```
logging message-counter syslog
enable secret 5 $1$v4IH$tGPiSl699jxLQiDvDcRnF/
```

```
no aaa new-model
memory-size iomem 5
```

```
dot11 syslog
ip source-route
```

```
ip cef
```

```
no ip domain lookup
no ipv6 cef
```

```
multilink bundle-name authenticated
```

```
voice-card 0
```

```
archive
log config
hidekeys
```

```
interface FastEthernet0/0
no shutdown
ip address 10.0.1.1 255.255.255.0
duplex auto
speed auto
```

```
interface FastEthernet0/1
```

```
no ip address
shutdown
duplex auto
speed auto

interface Serial0/0/0
no ip address
shutdown
clock rate 125000

interface Serial0/0/1
no shutdown
ip address 192.168.3.1 255.255.255.0
clock rate 128000

interface Serial0/1/0
no ip address
shutdown
clock rate 2000000

interface Serial0/1/1
no ip address
shutdown
clock rate 2000000

interface Serial0/2/0
no ip address
shutdown
clock rate 2000000

interface Serial0/2/1
no shutdown
ip address 192.168.1.2 255.255.255.0

router ospf 1
log-adjacency-changes
network 10.0.1.0 0.0.0.255 area 0
network 192.168.1.0 0.0.0.255 area 0
network 192.168.3.0 0.0.0.255 area 0

ip forward-protocol nd
no ip http server
no ip http secure-server

control-plane

mgcp fax t38 ecm

gatekeeper
shutdown

line con 0
exec-timeout 0 0
logging synchronous
line aux 0
line vty 0 4
password tesis2012
login
scheduler allocate 20000 1000
end
```

➔ **Configuración R3**

version 12.4

```
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption

hostname R3

boot-start-marker
boot-end-marker

logging message-counter syslog
enable secret 5 $1$QICj$Ynoxr6s.zF/8ulP6hNtjA/

no aaa new-model
memory-size iomem 5

dot11 syslog
ip source-route

ip cef

no ip domain lookup
no ipv6 cef

multilink bundle-name authenticated

voice-card 0

archive
log config
hidekeys

interface FastEthernet0/0
no shutdown
ip address 10.0.2.1 255.255.255.0
duplex auto
speed auto

interface FastEthernet0/1
no ip address
shutdown
duplex auto
speed auto

interface Serial0/0/0
no ip address
shutdown
clock rate 2000000

interface Serial0/0/1
no shutdown
ip address 192.168.4.1 255.255.255.0
clock rate 128000

interface Serial0/2/0
no ip address
shutdown
clock rate 125000
interface Serial0/2/1
no shutdown
ip address 192.168.2.2 255.255.255.0
clock rate 128000

router ospf 1
log-adjacency-changes
```

```
network 10.0.2.0 0.0.0.255 area 0
network 192.168.2.0 0.0.0.255 area 0
network 192.168.4.0 0.0.0.255 area 0
```

```
ip forward-protocol nd
no ip http server
no ip http secure-server
```

```
control-plane
```

```
mgcp fax t38 ecm
```

```
gatekeeper
shutdown
```

```
line con 0
exec-timeout 0 0
logging synchronous
line aux 0
line vty 0 4
password tesis2012
login
```

```
scheduler allocate 20000 1000
end
```

➔ **Configuración R4**

```
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
```

```
hostname R4
```

```
boot-start-marker
boot-end-marker
```

```
logging message-counter syslog
enable secret 5 $1$mMDI$.ksJxmpvSioqWT8DFWObA/
```

```
no aaa new-model
memory-size iomem 5
```

```
dot11 syslog
ip source-route
```

```
ip cef
```

```
ip dhcp pool red
network 10.0.3.0 255.255.255.0
default-router 10.0.3.1
```

```
no ip domain lookup
ipv6 unicast-routing
ipv6 cef
```

```
multilink bundle-name authenticated
```

```
voice-card 0
```

```
archive
log config
hidekeys
```

```
interface Tunnel0
no shutdown
no ip address
ipv6 address 2001::1:2/64
tunnel source 192.168.4.2
tunnel destination 192.168.1.1

interface FastEthernet0/0
no shutdown
ip address 10.0.3.1 255.255.255.0
duplex auto
speed auto
ipv6 address FEC0::4:1/112

interface FastEthernet0/1
no ip address
shutdown
duplex auto
speed auto

interface Serial0/0/0
no shutdown
ip address 192.168.4.2 255.255.255.0

interface Serial0/0/1
no shutdown
ip address 192.168.3.2 255.255.255.0

router ospf 1
log-adjacency-changes
network 10.0.3.0 0.0.0.255 area 0
network 192.168.3.0 0.0.0.255 area 0
network 192.168.4.0 0.0.0.255 area 0

ip forward-protocol nd
no ip http server
no ip http secure-server

ipv6 route ::/0 Tunnel0

control-plane

mgcp fax t38 ecm

gatekeeper
shutdown
line con 0
exec-timeout 0 0
logging synchronous
line aux 0
line vty 0 4
password tesis2012
login

scheduler allocate 20000 1000
end
```

ANEXO 2

CLIENTE TELNET SÓLO IPv4

CLIENTE TELNET SÓLO IPv4

R1

```
192.168.1.1 (1) - SecureCRT
File Edit View Options Transfer Script Tools Help
| 192.168.1.1 (1) | 192.168.1.1 (1) (1)
Sending 5, 100-byte ICMP Echos to 10.0.3.1, timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 28/38/68 ms
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.1, timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 28/28/28 ms
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.2, timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 16/16/16 ms
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.2.1, timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 32/34/44 ms
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.2.2, timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 16/20/32 ms
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.3.1, timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 32/36/52 ms
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.3.2, timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 28/35/52 ms
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.4.1, timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 16/20/32 ms
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.4.2, timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 28/35/52 ms
R1(tc1)#exit
R1#
R1#sh ip int b
Interface IP-Address OK? Method Status Protocol
FastEthernet0/0 10.0.0.1 YES TFTP up up
FastEthernet0/1 unassigned YES TFTP administratively down down
Serial0/0/0 192.168.2.1 YES TFTP up up
Serial0/0/1 192.168.1.1 YES TFTP up up
SSLVPN-VIF0 unassigned NO unset up up
R1#
```

```
192.168.1.1 (1) - SecureCRT
File Edit View Options Transfer Script Tools Help
| 192.168.1.1 (1) | 192.168.1.1 (1) (1)
Success rate is 100 percent (5/5), round-trip min/avg/max = 16/20/32 ms
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.3.1, timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 32/36/52 ms
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.3.2, timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 28/35/52 ms
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.4.1, timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 16/20/32 ms
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.4.2, timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 28/35/52 ms
R1(tc1)#exit
R1#
R1#sh ip int b
Interface IP-Address OK? Method Status Protocol
FastEthernet0/0 10.0.0.1 YES TFTP up up
FastEthernet0/1 unassigned YES TFTP administratively down down
Serial0/0/0 192.168.2.1 YES TFTP up up
Serial0/0/1 192.168.1.1 YES TFTP up up
SSLVPN-VIF0 unassigned NO unset up up
R1#sh ip rou
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
NL - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default, U - per-user static route
o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

O 192.168.4.0/24 [110/128] via 192.168.2.2, 00:10:17, Serial0/0/0
O 10.0.0.0/24 is subnetted, 2 subnets
O 10.0.3.0 [110/129] via 192.168.2.2, 00:10:07, Serial0/0/0
C 10.0.0.0 is directly connected, FastEthernet0/0
C 192.168.1.0/24 is directly connected, Serial0/0/1
C 192.168.2.0/24 is directly connected, Serial0/0/0
O 192.168.3.0/24 [110/192] via 192.168.2.2, 00:10:07, Serial0/0/0
R1#
```

R2

```
192.168.1.1 (1) - SecureCRT
File Edit View Options Transfer Script Tools Help
192.168.1.1 (1) | 192.168.1.1 (1) (1)
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
I - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default, U - per-user static route
o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

O 192.168.4.0/24 [110/128] via 192.168.2.2, 00:10:17, Serial0/0/0
O 10.0.0.0/24 is subnetted, 2 subnets
O 10.0.3.0 [110/129] via 192.168.2.2, 00:10:07, Serial0/0/0
C 10.0.0.0 is directly connected, FastEthernet0/0
C 192.168.1.0/24 is directly connected, Serial0/0/1
C 192.168.2.0/24 is directly connected, Serial0/0/0
O 192.168.3.0/24 [110/192] via 192.168.2.2, 00:10:07, Serial0/0/0
R1#192.168.1.2
Trying 192.168.1.2 ... open

User Access Verification
Password:
R2>ena
Password:
R2#sh ip rou
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
I - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default, U - per-user static route
o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

O 192.168.4.0/24 [110/192] via 192.168.1.1, 00:11:05, Serial0/2/1
O 10.0.0.0/24 is subnetted, 2 subnets
O 10.0.3.0 [110/193] via 192.168.1.1, 00:10:55, Serial0/2/1
O 10.0.0.0 [110/65] via 192.168.1.1, 00:11:58, Serial0/2/1
C 192.168.1.0/24 is directly connected, Serial0/2/1
O 192.168.2.0/24 [110/128] via 192.168.1.1, 00:11:58, Serial0/2/1
C 192.168.3.0/24 is directly connected, Serial0/0/1
R2#
```

```
192.168.1.1 (1) - SecureCRT
File Edit View Options Transfer Script Tools Help
192.168.1.1 (1) | 192.168.1.1 (1) (1)
10.0.0.0/24 is subnetted, 2 subnets
O 10.0.3.0 [110/129] via 192.168.2.2, 00:10:07, Serial0/0/0
C 10.0.0.0 is directly connected, FastEthernet0/0
C 192.168.1.0/24 is directly connected, Serial0/0/1
C 192.168.2.0/24 is directly connected, Serial0/0/0
O 192.168.3.0/24 [110/192] via 192.168.2.2, 00:10:07, Serial0/0/0
R1#192.168.1.2
Trying 192.168.1.2 ... Open

User Access Verification
Password:
R2>ena
Password:
R2#sh ip rou
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
I - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default, U - per-user static route
o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

O 192.168.4.0/24 [110/192] via 192.168.1.1, 00:11:05, Serial0/2/1
O 10.0.0.0/24 is subnetted, 2 subnets
O 10.0.3.0 [110/193] via 192.168.1.1, 00:10:55, Serial0/2/1
O 10.0.0.0 [110/65] via 192.168.1.1, 00:11:58, Serial0/2/1
C 192.168.1.0/24 is directly connected, Serial0/2/1
O 192.168.2.0/24 [110/128] via 192.168.1.1, 00:11:58, Serial0/2/1
C 192.168.3.0/24 is directly connected, Serial0/0/1
R2#sh ip int b
Interface IP-Address OK? Method Status Protocol
FastEthernet0/0 10.0.1.1 YES TFTP up down
FastEthernet0/1 unassigned YES TFTP administratively down down
Serial0/0/0 unassigned YES unset administratively down down
Serial0/0/1 192.168.3.1 YES TFTP up up
Serial0/1/0 unassigned YES unset administratively down down
Serial0/1/1 unassigned YES unset administratively down down
Serial0/2/0 unassigned YES unset administratively down down
Serial0/2/1 192.168.1.2 YES TFTP up up
SSLVPN-VIF0 unassigned NO unset up up
R2#
```

```
192.168.1.1 (1) - SecureCRT
File Edit View Options Transfer Script Tools Help
192.168.1.1 (1) | 192.168.1.1 (1)
+>(tc1)#} {
+>(tc1)#ping $dirreccion
+>(tc1)#}
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.0.0.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 36/40/44 ms
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.0.3.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 40/66/100 ms
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 36/39/44 ms
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 64/85/124 ms
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.2.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 40/56/84 ms
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.2.2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 48/79/136 ms
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.3.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 40/56/60 ms
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.3.2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 20/28/40 ms
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.4.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 44/72/88 ms
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.4.2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 60/66/76 ms
R2(tc1)#
Ready Telnet 45, 9 45 Rows, 132 Cols VT100 CAP NUM
```

R3

```
192.168.1.1 (1) - SecureCRT
File Edit View Options Transfer Script Tools Help
192.168.1.1 (1) | 192.168.1.1 (1)
Sending 5, 100-byte ICMP Echos to 192.168.2.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 40/56/84 ms
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.2.2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 48/79/136 ms
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.3.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 40/56/60 ms
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.3.2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 20/28/40 ms
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.4.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 44/72/88 ms
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.4.2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 60/66/76 ms
R2(tc1)#exit
R2#192.168.2.2
Trying 192.168.2.2 ... open

User Access Verification

Password:
R3>ena
Password:
R3#
R3#
R3#sh ip int b
Interface IP-Address OK? Method Status Protocol
FastEthernet0/0 10.0.2.1 YES TFTP up down
FastEthernet0/1 unassigned YES TFTP administratively down down
Serial0/0/0 unassigned YES unset administratively down down
Serial0/0/1 192.168.4.1 YES TFTP up up
Serial0/2/0 unassigned YES unset administratively down down
Serial0/2/1 192.168.2.2 YES TFTP up up
SSLVPN-VIF0 unassigned NO unset up
R3#
Ready Telnet 45, 4 45 Rows, 132 Cols VT100 CAP NUM
```

```
192.168.1.1 (1) - SecureCRT
File Edit View Options Transfer Script Tools Help
| 192.168.1.1 (1) | 192.168.1.1 (1) (1)
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.4.2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 60/66/76 ms
R2(tc1)#exit
R2#192.168.2.2
Trying 192.168.2.2 ... open

User Access Verification

Password:
R3>ena
Password:
R3#
R3#sh ip int b
Interface IP-Address OK? Method Status Protocol
FastEthernet0/0 10.0.2.1 YES TFTP up down
FastEthernet0/1 unassigned YES TFTP administratively down down
Serial0/0/0 unassigned YES unset administratively down up
Serial0/0/1 192.168.4.1 YES TFTP up up
Serial0/2/0 unassigned YES unset administratively down down
Serial0/2/1 192.168.2.2 YES TFTP up up
SSLVPN-ViF0 unassigned NO unset up up
R3#sh ip rou
R3#sh ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default, U - per-user static route
o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

C 192.168.4.0/24 is directly connected, Serial0/0/1
 10.0.0.0/24 is subnetted, 2 subnets
  O 10.0.3.0 [110/65] via 192.168.4.2, 00:13:57, Serial0/0/1
  O 10.0.0.0 [110/193] via 192.168.4.2, 00:13:57, Serial0/0/1
C 192.168.1.0/24 [110/192] via 192.168.4.2, 00:13:57, Serial0/0/1
C 192.168.2.0/24 is directly connected, Serial0/2/1
O 192.168.3.0/24 [110/128] via 192.168.4.2, 00:13:57, Serial0/0/1
R3#
Ready Telnet 45, 4 45 Rows, 132 Cols VT100 CAP NUM
```

```
192.168.1.1 (1) - SecureCRT
File Edit View Options Transfer Script Tools Help
| 192.168.1.1 (1) | 192.168.1.1 (1) (1)
+>(tc1)# {
+>(tc1)#ping $direccion
+>(tc1)#
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.0.0.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 60/65/80 ms
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.0.3.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 40/49/56 ms
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 60/84/136 ms
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 56/69/88 ms
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.2.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 20/29/44 ms
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.2.2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 76/84/92 ms
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.3.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 60/75/112 ms
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.3.2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 36/45/56 ms
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.4.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 72/96/116 ms
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.4.2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 52/54/56 ms
R3(tc1)#
Ready Telnet 45, 9 45 Rows, 132 Cols VT100 CAP NUM
```

R4

```
192.168.1.1 (1) - SecureCRT
File Edit View Options Transfer Script Tools Help
192.168.1.1 (1) | 192.168.1.1 (1) (1)
Success rate is 100 percent (5/5), round-trip min/avg/max = 36/45/56 ms
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.4.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 72/96/116 ms
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.4.2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 52/54/56 ms
R3(tc1)#exit
R3#192.168.4.2
Trying 192.168.4.2 ... Open

User Access Verification
Password:
R4>ena
Password:
R4#sh ip rou
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
        D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2
        I - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
        ia - IS-IS inter area, * - candidate default, U - per-user static route
        o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

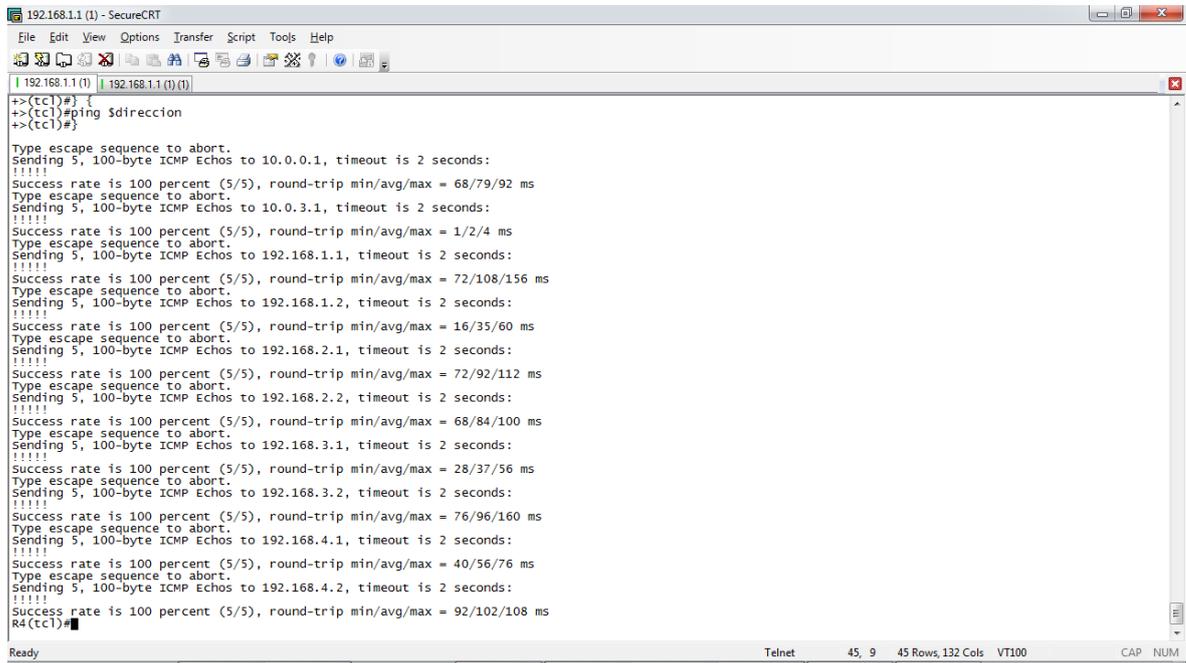
C 192.168.4.0/24 is directly connected, Serial0/0/0
  10.0.0.0/24 is subnetted, 2 subnets
C   10.0.3.0 is directly connected, FastEthernet0/0
O   10.0.0.0 [110/129] via 192.168.3.1, 00:15:01, Serial0/0/1
O  192.168.1.0/24 [110/128] via 192.168.3.1, 00:15:01, Serial0/0/1
O  192.168.2.0/24 [110/192] via 192.168.3.1, 00:15:01, Serial0/0/1
C  192.168.3.0/24 is directly connected, Serial0/0/1
R4#sh ip int b
Interface      IP-Address      OK? Method Status      Protocol
FastEthernet0/0  10.0.3.1        YES TFTP  up          up
FastEthernet0/1  unassigned      YES TFTP  administratively down down
Serial0/0/0      192.168.4.2    YES TFTP  up          up
Serial0/0/1      192.168.3.2    YES TFTP  up          up
SSLVPN-VIF0     unassigned      NO  unset  up          up
R4#
Ready Telnet 45, 4 45 Rows, 132 Cols VT100 CAP NUM
```

```
192.168.1.1 (1) - SecureCRT
File Edit View Options Transfer Script Tools Help
192.168.1.1 (1) | 192.168.1.1 (1) (1)
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.3.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 60/75/112 ms
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.3.2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 36/45/56 ms
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.4.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 72/96/116 ms
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.4.2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 52/54/56 ms
R3(tc1)#exit
R3#192.168.4.2
Trying 192.168.4.2 ... open

User Access Verification
Password:
R4>ena
Password:
R4#sh ip rou
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
        D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2
        I - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
        ia - IS-IS inter area, * - candidate default, U - per-user static route
        o - ODR, P - periodic downloaded static route

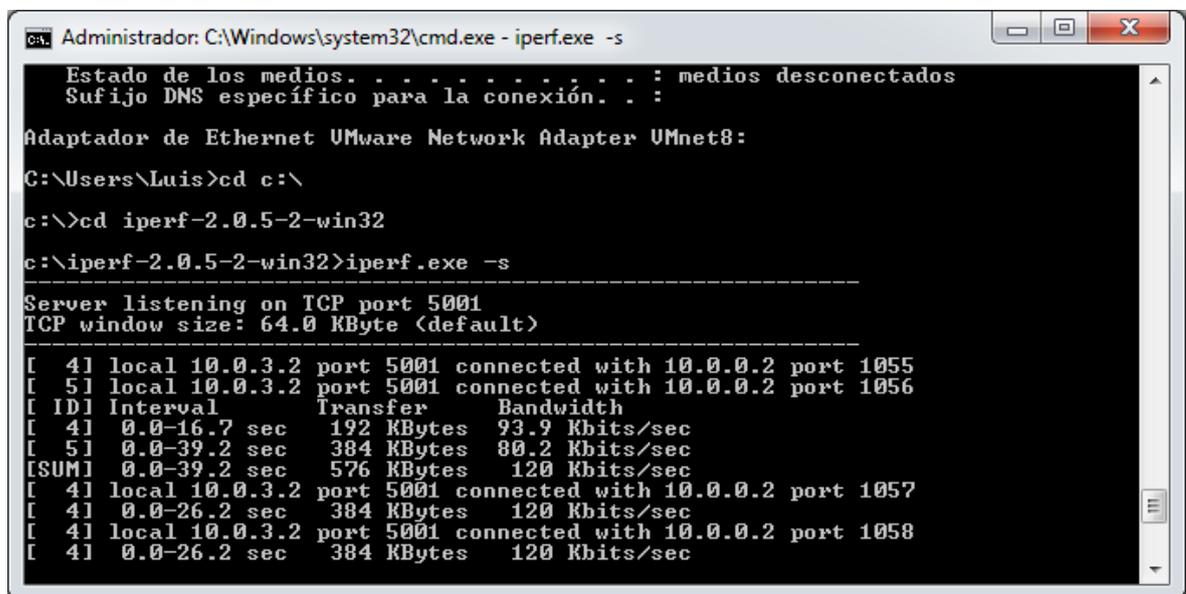
Gateway of last resort is not set

C 192.168.4.0/24 is directly connected, Serial0/0/0
  10.0.0.0/24 is subnetted, 2 subnets
C   10.0.3.0 is directly connected, FastEthernet0/0
O   10.0.0.0 [110/129] via 192.168.3.1, 00:15:01, Serial0/0/1
O  192.168.1.0/24 [110/128] via 192.168.3.1, 00:15:01, Serial0/0/1
O  192.168.2.0/24 [110/192] via 192.168.3.1, 00:15:01, Serial0/0/1
C  192.168.3.0/24 is directly connected, Serial0/0/1
R4#
Ready Telnet 45, 4 45 Rows, 132 Cols VT100 CAP NUM
```



```
192.168.1.1 (1) - SecureCRT
File Edit View Options Transfer Script Tools Help
192.168.1.1 (1) | 192.168.1.1 (1) (1)
+>(tcl)# {
+>(tcl)#ping $direccion
+>(tcl)#
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.0.0.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 68/79/92 ms
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.0.3.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 72/108/156 ms
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 16/35/60 ms
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.2.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 72/92/112 ms
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.2.2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 68/84/100 ms
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.3.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 28/37/56 ms
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.3.2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 76/96/160 ms
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.4.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 40/56/76 ms
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.4.2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 92/102/108 ms
R4(tcl)#
Ready Telnet 45, 9 45 Rows, 132 Cols VT100 CAP NUM
```

Ancho de Banda



```
Administrador: C:\Windows\system32\cmd.exe - iperf.exe -s
Estado de los medios. . . . . : medios desconectados
Sufijo DNS específico para la conexión. . :
Adaptador de Ethernet VMware Network Adapter VMnet8:
C:\Users\Luis>cd c:\
c:\>cd iperf-2.0.5-2-win32
c:\iperf-2.0.5-2-win32>iperf.exe -s
-----
Server listening on TCP port 5001
TCP window size: 64.0 KByte (default)
-----
[ 4] local 10.0.3.2 port 5001 connected with 10.0.0.2 port 1055
[ 5] local 10.0.3.2 port 5001 connected with 10.0.0.2 port 1056
[ ID] Interval Transfer Bandwidth
[ 4] 0.0-16.7 sec 192 KBytes 93.9 Kbits/sec
[ 5] 0.0-39.2 sec 384 KBytes 80.2 Kbits/sec
[SUM] 0.0-39.2 sec 576 KBytes 120 Kbits/sec
[ 4] local 10.0.3.2 port 5001 connected with 10.0.0.2 port 1057
[ 4] 0.0-26.2 sec 384 KBytes 120 Kbits/sec
[ 4] local 10.0.3.2 port 5001 connected with 10.0.0.2 port 1058
[ 4] 0.0-26.2 sec 384 KBytes 120 Kbits/sec
```

ANEXO 3

CLIENTE TELNET SÓLO IPv6

CLIENTE TELNET SÓLO IPv6

R1

```
fec0:1:1 - SecureCRT
File Edit View Options Transfer Script Tools Help
| fec0:1:1
User Access Verification
Password:
R1>ena
Password:
R1#
R1#sh ip rou
R1#sh ipv
R1#sh ipv6 rou
R1#sh ipv6 route
IPv6 Routing Table - Default - 10 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
B - BGP, M - MIPv6, R - RIP, I1 - ISIS L1
I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary, D - EIGRP
EX - EIGRP external
O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
C 2001::1:0/112 [0/0]
  via Serial0/0/1, directly connected
L 2001::1:1/128 [0/0]
  via Serial0/0/1, receive
C 2001::2:0/112 [0/0]
  via Serial0/0/0, directly connected
L 2001::2:1/128 [0/0]
  via Serial0/0/0, receive
O 2001::3:0/112 [110/192]
  via FE80::217:SAFF:FEAD:E210, Serial0/0/0
O 2001::4:0/112 [110/128]
  via FE80::217:SAFF:FEAD:E210, Serial0/0/0
C FEC0::1:0/112 [0/0]
  via FastEthernet0/0, directly connected
L FEC0::1:1/128 [0/0]
  via FastEthernet0/0, receive
O FEC0::4:0/112 [110/129]
  via FE80::217:SAFF:FEAD:E210, Serial0/0/0
L FF00::/8 [0/0]
  via Nu110, receive
R1#
Ready Telnet 40, 4 45 Rows, 132 Cols VT100 CAP NUM
```

```
fec0:1:1 - SecureCRT
File Edit View Options Transfer Script Tools Help
| fec0:1:1
R1#sh ipv6 route
IPv6 Routing Table - Default - 10 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
B - BGP, M - MIPv6, R - RIP, I1 - ISIS L1
I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary, D - EIGRP
EX - EIGRP external
O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
C 2001::1:0/112 [0/0]
  via Serial0/0/1, directly connected
L 2001::1:1/128 [0/0]
  via Serial0/0/1, receive
C 2001::2:0/112 [0/0]
  via Serial0/0/0, directly connected
L 2001::2:1/128 [0/0]
  via Serial0/0/0, receive
O 2001::3:0/112 [110/192]
  via FE80::217:SAFF:FEAD:E210, Serial0/0/0
O 2001::4:0/112 [110/128]
  via FE80::217:SAFF:FEAD:E210, Serial0/0/0
C FEC0::1:0/112 [0/0]
  via FastEthernet0/0, directly connected
L FEC0::1:1/128 [0/0]
  via FastEthernet0/0, receive
O FEC0::4:0/112 [110/129]
  via FE80::217:SAFF:FEAD:E210, Serial0/0/0
L FF00::/8 [0/0]
  via Nu110, receive
R1#sh ipv
R1#sh ipv6 in
R1#sh ipv6 int br
FastEthernet0/0 [up/up]
  FE80::224:14FF:FE02:FE40
  FEC0::1:1
FastEthernet0/1 [administratively down/down]
  unassigned
Serial0/0/0 [up/up]
  FE80::224:14FF:FE02:FE40
  2001::2:1
Serial0/0/1 [up/up]
  FE80::224:14FF:FE02:FE40
  2001::1:1
SSLVPN-VIF0 [up/up]
  unassigned
R1#
Ready Telnet 45, 4 45 Rows, 132 Cols VT100 CAP NUM
```

```
fec0:1:1 - SecureCRT
File Edit View Options Transfer Script Tools Help
| fec0:1:1
+>>(tc1)#} {
+>>(tc1)#ping $direccion
+>>(tc1)#}

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to FEC0::1:1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/0 ms
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to FEC0::4:1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 172/247/332 ms
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001::1:1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/0 ms
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001::1:2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 20/24/36 ms
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001::2:1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/0 ms
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001::2:2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 108/159/224 ms
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001::3:1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 96/124/160 ms
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001::3:2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 60/89/116 ms
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001::4:1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 40/51/60 ms
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001::4:2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 64/85/108 ms
R1(tc1)#
Ready Telnet 45, 9 45 Rows, 132 Cols VT100 CAP NUM
```

R2

```
2001:1:2 - SecureCRT
File Edit View Options Transfer Script Tools Help
| 2001:1:2
Serial0/1/1 unassigned YES unset administratively down down
Serial0/2/0 unassigned YES unset administratively down down
Serial0/2/1 unassigned YES TFTP up up
SSLVPN-Vi0 unassigned NO unset up up
R2#sh ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
I - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default, U - per-user static route
o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

R2#sh ipv
R2#sh ipv6 rou
R2#sh ipv6 route
IPv6 Routing Table - Default - 9 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
B - BGP, M - MIPv6, R - RIP, I1 - ISIS L1
I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary, D - EIGRP
EX - EIGRP external
O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
C 2001::1:0/112 [0/0]
via Serial0/2/1, directly connected
L 2001::1:2/128 [0/0]
via Serial0/2/1, receive
O 2001::2:0/112 [110/128]
via FE80::224:14FF:FE02:FE40, Serial0/2/1
C 2001::3:0/112 [0/0]
via Serial0/0/1, directly connected
L 2001::3:1/128 [0/0]
via Serial0/0/1, receive
O 2001::4:0/112 [110/192]
via FE80::224:14FF:FE02:FE40, Serial0/2/1
O FE00::1:0/112 [110/65]
via FE80::224:14FF:FE02:FE40, Serial0/2/1
O FE00::4:0/112 [110/192]
via FE80::224:14FF:FE02:FE40, Serial0/2/1
L FF00::/8 [0/0]
via Null0, receive
R2#
Ready Telnet 45, 4 45 Rows, 132 Cols VT100 CAP NUM
```

```
2001:1:2 - SecureCRT
File Edit View Options Transfer Script Tools Help
2001:1:2
I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary, D - EIGRP
EX - EIGRP external
O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
C 2001::1:0/112 [0/0]
  via Serial0/2/1, directly connected
L 2001::1:2/128 [0/0]
  via Serial0/2/1, receive
O 2001::2:0/112 [110/128]
  via FE80::224:14FF:FE02:FE40, Serial0/2/1
C 2001::3:0/112 [0/0]
  via Serial0/0/1, directly connected
L 2001::3:1/128 [0/0]
  via Serial0/0/1, receive
O 2001::4:0/112 [110/192]
  via FE80::224:14FF:FE02:FE40, Serial0/2/1
O FE80::1:0/112 [110/65]
  via FE80::224:14FF:FE02:FE40, Serial0/2/1
O FE80::4:0/112 [110/193]
  via FE80::224:14FF:FE02:FE40, Serial0/2/1
L FF00::/8 [0/0]
  via Null0, receive
R2#sh ip int b
FastEthernet0/0 [up/down]
  FE80::217:94FF:FEA5:10F0
FastEthernet0/1 [administratively down/down]
  unassigned
Serial0/0/0 [administratively down/down]
  unassigned
Serial0/0/1 [up/up]
  FE80::217:94FF:FEA5:10F0
  2001::3:1
Serial0/1/0 [administratively down/down]
  unassigned
Serial0/1/1 [administratively down/down]
  unassigned
Serial0/2/0 [administratively down/down]
  unassigned
Serial0/2/1 [up/up]
  FE80::217:94FF:FEA5:10F0
  2001::1:2
SSLVPN-VIF0 [up/up]
  unassigned
R2#
Ready Telnet 45, 4 45 Rows, 132 Cols VT100 CAP NUM
```

```
2001:1:2 - SecureCRT
File Edit View Options Transfer Script Tools Help
2001:1:2
+>>(tc1)# {
+>>(tc1)#ping $direccion
+>>(tc1)#
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to FE80::1:1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 28/42/56 ms
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to FE80::4:1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 64/91/152 ms
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001::1:1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 32/47/56 ms
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001::1:2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/0 ms
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001::2:1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 76/94/120 ms
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001::2:2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 84/116/152 ms
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001::3:1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/1/4 ms
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001::3:2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 20/35/48 ms
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001::4:1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 72/124/196 ms
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001::4:2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 76/91/120 ms
R2(tc1)#
Ready Telnet 45, 9 45 Rows, 132 Cols VT100 CAP NUM
```

R3

```
2001:2:2 - SecureCRT
File Edit View Options Transfer Script Tools Help
2001:2:2

User Access Verification
Password:
R3>ena
Password:
R3#
R3#
R3#sh ip int b
Interface IP-Address OK? Method Status Protocol
FastEthernet0/0 unassigned YES TFTP up down
FastEthernet0/1 unassigned YES TFTP administratively down down
Serial0/0/0 unassigned YES TFTP administratively down down
Serial0/0/1 unassigned YES TFTP up up
Serial0/2/0 unassigned YES TFTP administratively down down
Serial0/2/1 unassigned YES TFTP up up
SSLVPN-VIF0 unassigned NO unset up up
R3#sh ipw int b
FastEthernet0/0 [up/down]
FE80::217:5AFF:FEAD:E210
FE00::3:1
FastEthernet0/1 [administratively down/down]
unassigned
Serial0/0/0 [administratively down/down]
unassigned
Serial0/0/1 [up/up]
FE80::217:5AFF:FEAD:E210
2001::4:1
Serial0/2/0 [administratively down/down]
unassigned
Serial0/2/1 [up/up]
FE80::217:5AFF:FEAD:E210
2001::2:2
SSLVPN-VIF0 [up/up]
unassigned
R3#
```

```
2001:2:2 - SecureCRT
File Edit View Options Transfer Script Tools Help
2001:2:2

FastEthernet0/0 [up/down]
FE80::217:5AFF:FEAD:E210
FE00::3:1
FastEthernet0/1 [administratively down/down]
unassigned
Serial0/0/0 [administratively down/down]
unassigned
Serial0/0/1 [up/up]
FE80::217:5AFF:FEAD:E210
2001::4:1
Serial0/2/0 [administratively down/down]
unassigned
Serial0/2/1 [up/up]
FE80::217:5AFF:FEAD:E210
2001::2:2
SSLVPN-VIF0 [up/up]
unassigned
R3#sh ipv ro
R3#sh ipv route
IPv6 Routing Table - Default - 9 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
B - BGP, M - MIPv6, R - RIP, I1 - ISIS L1
I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary, D - EIGRP
EX - EIGRP external
O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
O 2001::1:0/112 [110/192]
via FE80::217:5AFF:FEAD:4F1A, Serial0/0/1
C 2001::2:0/112 [0/0]
via Serial0/2/1, directly connected
L 2001::2:2/128 [0/0]
via Serial0/2/1, receive
O 2001::3:0/112 [110/128]
via FE80::217:5AFF:FEAD:4F1A, Serial0/0/1
C 2001::4:0/112 [0/0]
via Serial0/0/1, directly connected
L 2001::4:1/128 [0/0]
via Serial0/0/1, receive
O FE00::1:0/112 [110/193]
via FE80::217:5AFF:FEAD:4F1A, Serial0/0/1
O FE00::4:0/112 [110/65]
via FE80::217:5AFF:FEAD:4F1A, Serial0/0/1
L FF00::/8 [0/0]
via Null0, receive
R3#
```

```
2001:2:2 - SecureCRT
File Edit View Options Transfer Script Tools Help
| 2001:2:2
+>(tc1)# {
+>(tc1)#ping $dirrection
+>(tc1)#
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to FEC0::1:1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 52/60/68 ms
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to FEC0::4:1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 36/40/44 ms
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001::1:1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 56/72/84 ms
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001::1:2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 128/244/380 ms
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001::2:1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 24/31/36 ms
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001::2:2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/0 ms
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001::3:1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 76/103/160 ms
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001::3:2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 40/44/56 ms
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001::4:1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/1/4 ms
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001::4:2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 56/76/100 ms
R3(tc1)#
Ready Telnet 45, 9 45 Rows, 132 Cols VT100 CAP NUM
```

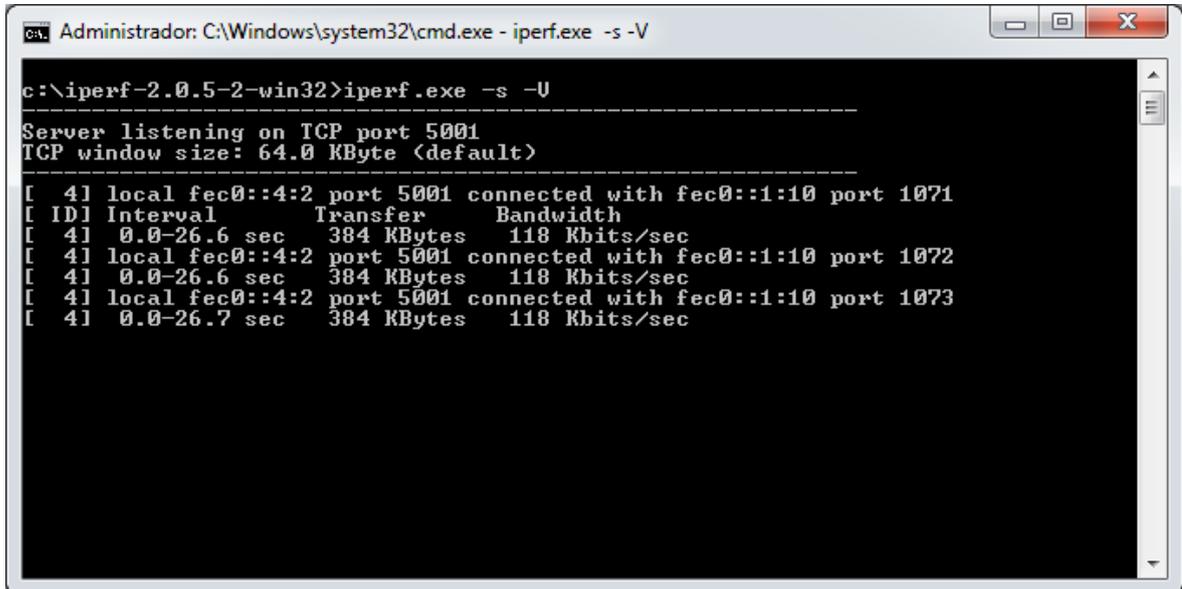
R4

```
2001:4:2 - SecureCRT
File Edit View Options Transfer Script Tools Help
| 2001:2:2 | 2001:4:2
User Access verification
Password:
R4>ena
Password:
R4#sh ipv
R4#sh ipv6 int b
FastEthernet0/0 [up/up]
FE80::217:5AFF:FEAD:4F1A
FE80::4:1
FastEthernet0/1 [administratively down/down]
unassigned
Serial0/0/0 [up/up]
FE80::217:5AFF:FEAD:4F1A
2001::4:2
Serial0/0/1 [up/up]
FE80::217:5AFF:FEAD:4F1A
2001::3:2
SSLVPN-VIF0 [up/up]
unassigned
R4#
Ready Telnet 23, 4 45 Rows, 132 Cols VT100 CAP NUM
```

```
2001:4:2 - SecureCRT
File Edit View Options Transfer Script Tools Help
2001:2:2 | 2001:4:2
R4#sh ipv6 int b
FastEthernet0/0 [up/up]
FE80::217:5AFF:FEAD:4F1A
FE80::4:1
FastEthernet0/1 [administratively down/down]
unassigned
Serial0/0/0 [up/up]
FE80::217:5AFF:FEAD:4F1A
2001::4:2
Serial0/0/1 [up/up]
FE80::217:5AFF:FEAD:4F1A
2001::3:2
SSLVPN-ViF0 [up/up]
unassigned
R4#sh ipv
R4#sh ipv6 rou
R4#sh ipv6 route
IPv6 Routing Table - Default - 10 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
B - BGP, M - MIPv6, R - RIP, I1 - ISIS L1
I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary, D - EIGRP
EX - EIGRP external
O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
O 2001::1:0/112 [110/128]
via FE80::217:94FF:FEA5:10F0, Serial0/0/1
O 2001::2:0/112 [110/192]
via FE80::217:94FF:FEA5:10F0, Serial0/0/1
C 2001::3:0/112 [0/0]
via Serial0/0/1, directly connected
L 2001::3:2/128 [0/0]
via Serial0/0/1, receive
C 2001::4:0/112 [0/0]
via Serial0/0/0, directly connected
L 2001::4:2/128 [0/0]
via Serial0/0/0, receive
O FEC0::1:0/112 [110/129]
via FE80::217:94FF:FEA5:10F0, Serial0/0/1
C FEC0::4:0/112 [0/0]
via FastEthernet0/0, directly connected
L FEC0::4:1/128 [0/0]
via FastEthernet0/0, receive
L FF00::/8 [0/0]
via Null0, receive
R4#
Ready Telnet 45, 4 45 Rows, 132 Cols VT100 CAP NUM
```

```
2001:4:2 - SecureCRT
File Edit View Options Transfer Script Tools Help
2001:2:2 | 2001:4:2
++(tc1)# {
++(tc1)#ping $direccion
++(tc1)#}
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to FEC0::1:1, timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 56/60/72 ms
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to FEC0::4:1, timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/0 ms
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001::1:1, timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 56/59/60 ms
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001::1:2, timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 12/23/36 ms
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001::2:1, timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 52/56/60 ms
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001::2:2, timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 56/56/60 ms
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001::3:1, timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 16/19/20 ms
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001::3:2, timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/4 ms
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001::4:1, timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 20/25/36 ms
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001::4:2, timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/4 ms
R4(tc1)#
Ready Telnet 45, 9 45 Rows, 132 Cols VT100 CAP NUM
```

🔗 Ancho de Banda



```
Administrador: C:\Windows\system32\cmd.exe - iperf.exe -s -V
c:\iperf-2.0.5-2-win32>iperf.exe -s -U
-----
Server listening on TCP port 5001
TCP window size: 64.0 KByte (default)
-----
[ 4] local fec0::4:2 port 5001 connected with fec0::1:10 port 1071
[ ID] Interval      Transfer    Bandwidth
[ 4] 0.0-26.6 sec   384 KBytes  118 Kbits/sec
[ 4] local fec0::4:2 port 5001 connected with fec0::1:10 port 1072
[ 4] 0.0-26.6 sec   384 KBytes  118 Kbits/sec
[ 4] local fec0::4:2 port 5001 connected with fec0::1:10 port 1073
[ 4] 0.0-26.7 sec   384 KBytes  118 Kbits/sec
```

ANEXO 4

CLIENTE TELNET 6to4

CLIENTE TELNET 6to4

R1

```
fec0:4:1 - SecureCRT
File Edit View Options Transfer Script Tools Help
R1 R2 R3 R4 fec0:4:1
% invalid input detected at '^' marker.
R4#sh tunnel ?
R4#sh tunnel endpoints Display endpoints associated with multipoint tunnel
R4#sh tunnel en
R4#sh tunnel endpoints
Tunnel0 running in IPv6 6to4 mode
R4#
R4#192.168.1.1
Trying 192.168.1.1 ... Open

User Access Verification
Password:
R1>ena
Password:
R1#
R1#
R1#sh ipb
R1#sh ip
R1#sh ipv
R1#sh ipv6 int b
R1#sh ipv6 int br
R1#sh ipv6 int brief
FastEthernet0/0 [up/up]
FE80::224:14FF:FE02:FE40
FE00::1:1
FastEthernet0/1 [administratively down/down]
unassigned
Serial0/0/0 [up/up]
unassigned
Serial0/0/1 [up/up]
unassigned
SSLVPN-VIF0 [up/up]
unassigned
Tunnel0 [up/up]
FE80::c0a8:101
2002:c0a8:101::1
R1#
```

```
fec0:4:1 - SecureCRT
File Edit View Options Transfer Script Tools Help
R1 R2 R3 R4 fec0:4:1
R1#sh ipb
R1#sh ip
R1#sh ipv
R1#sh ipv6 int b
R1#sh ipv6 int br
R1#sh ipv6 int brief
FastEthernet0/0 [up/up]
FE80::224:14FF:FE02:FE40
FE00::1:1
FastEthernet0/1 [administratively down/down]
unassigned
Serial0/0/0 [up/up]
unassigned
Serial0/0/1 [up/up]
unassigned
SSLVPN-VIF0 [up/up]
unassigned
Tunnel0 [up/up]
FE80::c0a8:101
2002:c0a8:101::1
R1#sh ipv
R1#sh ipv6 rou
R1#sh ipv6 route
IPv6 Routing Table - Default - 7 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
B - BGP, M - MIPv6, R - RIP, I1 - ISIS L1
I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary, D - EIGRP
EX - EIGRP external
O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
S 2002::16 [1/0]
via Tunnel0, directly connected
C 2002:c0a8:101::64 [0/0]
via Tunnel0, directly connected
L 2002:c0a8:101::1/128 [0/0]
via Tunnel0, receive
C FE00::1:0/112 [0/0]
via FastEthernet0/0, directly connected
L FE00::1:1/128 [0/0]
via FastEthernet0/0, receive
S FE00::4:0/112 [1/0]
via 2002:c0a8:302::2
L FF00::8 [0/0]
via Null0, receive
R1#
```

R4

```
fec0:4:1 - SecureCRT
File Edit View Options Transfer Script Tools Help
R1 R2 R3 R4 fec0:4:1
Tunnel receive bandwidth 8000 (kbps)
Last input 00:08:04, output 00:07:29, output hang never
Last clearing of "show interface" counters never
Input queue: 0/75/0/0 (size/max/drops/Flushes); Total output drops: 0
Queueing strategy: fifo
Output queue: 0/0 (size/max)
5 minute input rate 26000 bits/sec, 15 packets/sec
5 minute output rate 27000 bits/sec, 14 packets/sec
4232 packets input, 1044814 bytes, 0 no buffer
Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
4234 packets output, 1025856 bytes, 0 underruns
0 output errors, 0 collisions, 0 interface resets
0 unknown protocol drops
0 unknown protocol drops
0 output buffer failures, 0 output buffers swapped out
R4#sh interfaces tunnel 0
Tunnel0 is up, line protocol is up
Hardware is Tunnel
MTU 17920 bytes, BW 100 kbit/sec, DLY 50000 usec,
reliability 255/255, txload 79/255, rxload 64/255
Encapsulation TUNNEL, loopback not set
Keepalive not set
Tunnel source 192.168.3.2 (Serial0/0/1)
Tunnel protocol/transport ipv6 6to4
Tunnel TTL 255
Tunnel transport MTU 1480 bytes
Tunnel transmit bandwidth 8000 (kbps)
Tunnel receive bandwidth 8000 (kbps)
Last input 00:08:12, output 00:07:37, output hang never
Last clearing of "show interface" counters never
Input queue: 0/75/0/0 (size/max/drops/Flushes); Total output drops: 0
Queueing strategy: fifo
Output queue: 0/0 (size/max)
5 minute input rate 29000 bits/sec, 17 packets/sec
5 minute output rate 31000 bits/sec, 16 packets/sec
4633 packets input, 1142254 bytes, 0 no buffer
Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
4635 packets output, 1121988 bytes, 0 underruns
0 output errors, 0 collisions, 0 interface resets
0 unknown protocol drops
0 unknown protocol drops
0 output buffer failures, 0 output buffers swapped out
R4#
Ready Telnet 45, 4 45 Rows, 132 Cols VT100 CAP NUM
```

```
fec0:4:1 - SecureCRT
File Edit View Options Transfer Script Tools Help
R1 R2 R3 R4 fec0:4:1
Tunnel receive bandwidth 8000 (kbps)
Last input 00:09:02, output 00:08:28, output hang never
Last clearing of "show interface" counters never
Input queue: 0/75/0/0 (size/max/drops/Flushes); Total output drops: 0
Queueing strategy: fifo
Output queue: 0/0 (size/max)
5 minute input rate 44000 bits/sec, 27 packets/sec
5 minute output rate 44000 bits/sec, 26 packets/sec
7146 packets input, 1756502 bytes, 0 no buffer
Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
7140 packets output, 1723313 bytes, 0 underruns
0 output errors, 0 collisions, 0 interface resets
0 unknown protocol drops
0 unknown protocol drops
0 output buffer failures, 0 output buffers swapped out
R4#SH cdp
R4#SH cdp
Global CDP information:
Sending CDP packets every 60 seconds
Sending a holdtime value of 180 seconds
Sending CDPv2 advertisements is enabled
R4#SH cdp ne
R4#SH cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
S - Switch, H - Host, I - IGMP, r - Repeater
Device ID Local Intrfce Holdtme Capability Platform Port ID
Switch Fas 0/0 162 S I WS-C2960- Fas 0/1
R2 Ser 0/0/1 177 R S I 2811 Ser 0/0/1
R3 Ser 0/0/0 177 R S I 2811 Ser 0/0/1
R4#sh tunn
R4#sh tunnel 0
% Invalid input detected at '^' marker.
R4#sh tunnel
R4#sh tunnel ?
endpoints Display endpoints associated with multipoint tunnel
R4#sh tunnel en
R4#sh tunnel endpoints
Tunnel0 running in IPv6 6to4 mode
R4#
Ready Telnet 45, 4 45 Rows, 132 Cols VT100 CAP NUM
```

```
fec0:41 - SecureCRT
File Edit View Options Transfer Script Tools Help
R1 R2 R3 R4 fec0:41
Tunnel receive bandwidth 8000 (kbps)
Last input 00:08:12, output 00:07:37, output hang never
Last clearing of "show interface" counters never
Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
Queueing strategy: fifo
Output queue: 0/0 (size/max)
5 minute input rate 29000 bits/sec, 17 packets/sec
5 minute output rate 31000 bits/sec, 16 packets/sec
4633 packets input, 1142254 bytes, 0 no buffer
Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
4635 packets output, 1121988 bytes, 0 underruns
0 output errors, 0 collisions, 0 interface resets
0 unknown protocol drops
0 unknown protocol drops
0 output buffer failures, 0 output buffers swapped out
R4#sh interfaces tunnel 0
Tunnel0 is up, line protocol is up
Hardware is Tunnel
MTU 17920 bytes, BW 100 Kbit/sec, DLY 50000 usec,
reliability 255/255, txload 112/255, rxload 97/255
Encapsulation TUNNEL, loopback not set
Keepalive not set
Tunnel source 192.168.3.2 (Serial0/0/1)
Tunnel protocol/transport IPv6 6to4
Tunnel TTL 255
Tunnel transport MTU 1480 bytes
Tunnel transmit bandwidth 8000 (kbps)
Tunnel receive bandwidth 8000 (kbps)
Last input 00:09:02, output 00:08:28, output hang never
Last clearing of "show interface" counters never
Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
Queueing strategy: fifo
Output queue: 0/0 (size/max)
5 minute input rate 44000 bits/sec, 27 packets/sec
5 minute output rate 44000 bits/sec, 26 packets/sec
7146 packets input, 175602 bytes, 0 no buffer
Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
7140 packets output, 1723313 bytes, 0 underruns
0 output errors, 0 collisions, 0 interface resets
0 unknown protocol drops
0 unknown protocol drops
0 output buffer failures, 0 output buffers swapped out
R4#
Ready Telnet 45, 4 45 Rows, 132 Cols VT100 CAP NUM
```

Ancho de Banda

```
Administrador: C:\Windows\system32\cmd.exe - iperf.exe -s -V
[KM] Indicates options that support a K or M suffix for kilo- or mega-
The TCP window size option can be set by the environment variable
TCP_WINDOW_SIZE. Most other options can be set by an environment variable
IPERF_<long option name>, such as IPERF_BANDWIDTH.
Report bugs to <iperf-users@lists.sourceforge.net>
c:\iperf-2.0.5-2-win32>iperf.exe -s
"iperf.exe -s" no se reconoce como un comando interno o externo,
programa o archivo por lotes ejecutable.
c:\iperf-2.0.5-2-win32>iperf.exe -s
-----
Server listening on TCP port 5001
TCP window size: 64.0 KByte (default)
-----
c:\iperf-2.0.5-2-win32>iperf.exe -s -U
-----
Server listening on TCP port 5001
TCP window size: 64.0 KByte (default)
-----
[ 41] local fec0::4:2 port 5001 connected with fec0::1:10 port 1050
[ ID] Interval Transfer Bandwidth
[ 41] 0.0-28.3 sec 384 KBytes 111 Kbits/sec
[ 41] local fec0::4:2 port 5001 connected with fec0::1:10 port 1051
[ 41] 0.0-27.4 sec 384 KBytes 115 Kbits/sec
[ 41] local fec0::4:2 port 5001 connected with fec0::1:10 port 1052
[ 41] 0.0-27.2 sec 384 KBytes 116 Kbits/sec
```

ANEXO 5

CLIENTE TELNET ISATAP

CLIENTE TELNET ISATAP

R1

```
fec0:4:1 - SecureCRT
File Edit View Options Transfer Script Tools Help
| fec0:4:1
input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
Queueing strategy: fifo
Output queue: 0/0 (size/max)
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
50 packets input, 12332 bytes, 0 no buffer
Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
54 packets output, 11268 bytes, 0 underruns
0 output errors, 0 collisions, 0 interface resets
0 unknown protocol drops
0 unknown protocol drops
0 output buffer failures, 0 output buffers swapped out
R4#
R4#fec0::1:1
Trying FEC0::1:1 ... Open

User Access Verification

Password:
R1>ena
Password:
R1#sh ipv rout
IPv6 Routing Table - Default - 6 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
B - BGP, M - MIPv6, R - RIP, I1 - ISIS L1
I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary, D - EIGRP
EX - EIGRP external
O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
C 123::/64 [0/0]
   via Tunnel0, directly connected
L 123::5EFE:C0A8:101/128 [0/0]
   via Tunnel0, receive
C FEC0::1:0/112 [0/0]
   via FastEthernet0/0, directly connected
L FEC0::1:1/128 [0/0]
   via FastEthernet0/0, receive
S FEC0::4:0/112 [1/0]
   via 123::5EFE:C0A8:302
L FF00::/8 [0/0]
   via Null0, receive
R1#
Ready Telnet 45, 4 45 Rows, 132 Cols VT100 CAP NUM
```

```
fec0:4:1 - SecureCRT
File Edit View Options Transfer Script Tools Help
| fec0:4:1
R4#fec0::1:1
Trying FEC0::1:1 ... Open

User Access Verification

Password:
R1>ena
Password:
R1#sh ipv rout
IPv6 Routing Table - Default - 6 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
B - BGP, M - MIPv6, R - RIP, I1 - ISIS L1
I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary, D - EIGRP
EX - EIGRP external
O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
C 123::/64 [0/0]
   via Tunnel0, directly connected
L 123::5EFE:C0A8:101/128 [0/0]
   via Tunnel0, receive
C FEC0::1:0/112 [0/0]
   via FastEthernet0/0, directly connected
L FEC0::1:1/128 [0/0]
   via FastEthernet0/0, receive
S FEC0::4:0/112 [1/0]
   via 123::5EFE:C0A8:302
L FF00::/8 [0/0]
   via Null0, receive
R1#sh ipv int b
FastEthernet0/0 [up/up]
   FE80::224:14FF:FE02:FE40
   FEC0::1:1
FastEthernet0/1 [administratively down/down]
   unassigned
Serial0/0/0 [up/up]
   unassigned
Serial0/0/1 [up/up]
   unassigned
SSLVPN-ViF0 [up/up]
   unassigned
Tunnel0 [up/up]
   FE80::5EFE:C0A8:101
   123::5EFE:C0A8:101
R1#
Ready Telnet 45, 4 45 Rows, 132 Cols VT100 CAP NUM
```

```
fec0:41 - SecureCRT
File Edit View Options Transfer Script Tools Help
| fec0:41
R1#sh ip v int b
FastEthernet0/0 [up/up]
FE80::224:14FF:FE02:FE40
FE00::1:1
FastEthernet0/1 [administratively down/down]
unassigned
Serial0/0/0 [up/up]
unassigned
Serial0/0/1 [up/up]
unassigned
SSLVPN-ViF0 [up/up]
unassigned
Tunnel0 [up/up]
FE80::5EFE:COA8:101
123::5EFE:COA8:101
R1#sh int tun
R1#sh int tunnel 0
Tunnel0 is up, line protocol is up
Hardware is Tunnel
MTU 17920 bytes, BW 100 kbit/sec, DLY 50000 usec,
reliability 255/255, txload 102/255, rxload 83/255
Encapsulation TUNNEL, loopback not set
Keepalive not set
Tunnel source 192.168.1.1
Tunnel protocol/transport IPv6 ISATAP
Tunnel TTL 255
Tunnel transport MTU 1480 bytes
Tunnel transmit bandwidth 8000 (kbps)
Tunnel receive bandwidth 8000 (kbps)
Last input 00:00:00, output 00:00:00, output hang never
Last clearing of "show interface" counters never
Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
Queueing strategy: fifo
Output queue: 0/0 (size/max)
5 minute input rate 38000 bits/sec, 21 packets/sec
5 minute output rate 40000 bits/sec, 22 packets/sec
5677 packets input, 1382739 bytes, 0 no buffer
Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
5684 packets output, 1360914 bytes, 0 underruns
0 output errors, 0 collisions, 0 interface resets
0 unknown protocol drops
0 unknown protocol drops
0 output buffer failures, 0 output buffers swapped out
R1#
Ready Telnet 45, 4 45 Rows, 132 Cols VT100 CAP NUM
```

```
fec0:41 - SecureCRT
File Edit View Options Transfer Script Tools Help
| fec0:41
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 32/37/40 ms
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.2.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 92/103/124 ms
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.2.2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 44/49/60 ms
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.3.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 88/96/104 ms
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.3.2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 72/92/104 ms
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.4.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 48/64/100 ms
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.4.2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 112/140/212 ms
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 123::5EFE:COA8:101, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/4 ms
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 123::5EFE:COA8:302, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 420/554/708 ms
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to FEC0::1:1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/4 ms
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to FEC0::4:1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 260/342/440 ms
R1(tc1)#
Ready Telnet 45, 9 45 Rows, 132 Cols VT100 CAP NUM
```

R2

```
fec0:41 - SecureCRT
File Edit View Options Transfer Script Tools Help
| fec0:41
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 420/554/708 ms
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to FEC0::1:1, timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/4 ms
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to FEC0::4:1, timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 260/342/440 ms
R1(tc1)#exit
R1#exit

[connection to fec0::1:1 closed by foreign host]
R4#fec0::1:2
Trying FEC0::1:2 ...
% Connection timed out; remote host not responding

R4#fec0::2:2
Trying FEC0::2:2 ...
% Destination unreachable; gateway or host down

R4#192.168.1.2
Trying 192.168.1.2 ... Open

User Access Verification
Password:
R2>ena
Password:
R2#
R2#
R2#sh ip int b
Interface IP-Address OK? Method Status Protocol
FastEthernet0/0 10.0.1.1 YES TFTP up down
FastEthernet0/1 unassigned YES TFTP administratively down down
Serial0/0/0 unassigned YES unset administratively down down
Serial0/0/1 192.168.3.1 YES TFTP up up
Serial0/1/0 unassigned YES unset administratively down down
Serial0/1/1 unassigned YES unset administratively down down
Serial0/2/0 unassigned YES unset administratively down down
Serial0/2/1 192.168.1.2 YES TFTP up up
SSLVPN-ViF0 unassigned NO unset up
R2#
```

```
fec0:41 - SecureCRT
File Edit View Options Transfer Script Tools Help
| fec0:41
Serial0/1/0 unassigned YES unset administratively down down
Serial0/1/1 unassigned YES unset administratively down down
Serial0/2/0 unassigned YES unset administratively down down
Serial0/2/1 192.168.1.2 YES TFTP up up
SSLVPN-ViF0 unassigned NO unset up
R2#sh ipv
R2#sh ipv6 int b
FastEthernet0/0 [up/down]
FastEthernet0/1 unassigned [administratively down/down]
Serial0/0/0 unassigned [administratively down/down]
Serial0/0/1 unassigned [up/up]
Serial0/1/0 unassigned [administratively down/down]
Serial0/1/1 unassigned [administratively down/down]
Serial0/2/0 unassigned [administratively down/down]
Serial0/2/1 unassigned [up/up]
SSLVPN-ViF0 unassigned [up/up]
R2#sh ip rou
R2#sh ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
I - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default, U - per-user static route
o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

O 192.168.4.0/24 [110/192] via 192.168.1.1, 00:11:44, Serial0/2/1
O 10.0.0.0/24 is subnetted, 2 subnets
O 10.0.3.0 [110/193] via 192.168.1.1, 00:11:10, Serial0/2/1
O 10.0.0.0 [110/65] via 192.168.1.1, 00:07:58, Serial0/2/1
C 192.168.1.0/24 is directly connected, Serial0/2/1
O 192.168.2.0/24 [110/128] via 192.168.1.1, 00:11:44, Serial0/2/1
C 192.168.3.0/24 is directly connected, Serial0/0/1
R2#
```

```
fec0:41 - SecureCRT
File Edit View Options Transfer Script Tools Help
| fec0:41
+>(tc1)#FEC0::1:1
+>(tc1)#FEC0::4:1
+>(tc1)# {
+>(tc1)#ping $direccion
+>(tc1)#}

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.0.0.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 16/25/40 ms
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.0.3.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 60/66/76 ms
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 24/27/40 ms
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 60/72/84 ms
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.2.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 36/48/60 ms
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.2.2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 60/74/88 ms
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.3.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 80/86/96 ms
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.3.2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 40/55/80 ms
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.4.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 72/76/80 ms
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.4.2, timeout is 2 seconds:
!!!!
Ready Telnet 45, 9 45 Rows, 132 Cols VT100 CAP NUM
```

R3

```
fec0:41 - SecureCRT
File Edit View Options Transfer Script Tools Help
| fec0:41
Success rate is 100 percent (5/5), round-trip min/avg/max = 60/74/88 ms
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.3.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 80/86/96 ms
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.3.2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 40/55/80 ms
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.4.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 72/76/80 ms
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.4.2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 60/79/104 ms% unrecognized host or address, or protocol not running.
% unrecognized host or address, or protocol not running.
% unrecognized host or address, or protocol not running.

R2(tc1)#exit
R2#exit

[connection to 192.168.1.2 closed by foreign host]
R4#192.168.2.2
Trying 192.168.2.2 ... open

User Access Verification
Password:
R3-ena
Password:
R3#
R3#sh ip int b
Interface IP-Address OK? Method Status Protocol
FastEthernet0/0 10.0.2.1 YES TFTP up down
FastEthernet0/1 unassigned YES TFTP administratively down down
Serial0/0/0 unassigned YES unset administratively down down
Serial0/0/1 192.168.4.1 YES TFTP up up
Serial0/2/0 unassigned YES unset administratively down down
Serial0/2/1 192.168.2.2 YES TFTP up up
SSLVPN-VIF0 unassigned NO unset up up
R3#
Ready Telnet 45, 4 45 Rows, 132 Cols VT100 CAP NUM
```

```
fec0:41 - SecureCRT
File Edit View Options Transfer Script Tools Help
| fec0:41
% Unrecognized host or address, or protocol not running.
R2(tc1)#exit
R2#exit
[Connection to 192.168.1.2 closed by foreign host]
R4#192.168.2.2
Trying 192.168.2.2 ... open

User Access Verification
Password:
R3>ena
Password:
R3#
R3#sh ip int b
Interface IP-Address OK? Method Status Protocol
FastEthernet0/0 10.0.2.1 YES TFTP up down
FastEthernet0/1 unassigned YES TFTP administratively down down
Serial0/0/0 unassigned YES unset administratively down down
Serial0/0/1 192.168.4.1 YES TFTP up up
Serial0/2/0 unassigned YES unset administratively down down
Serial0/2/1 192.168.2.2 YES TFTP up up
SSLVPN-ViF0 unassigned NO unset up up
R3#sh ip rou
R3#sh ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
I - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default, U - per-user static route
o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

C 192.168.4.0/24 is directly connected, Serial0/0/1
O 10.0.0.0/24 is subnetted, 2 subnets
O 10.0.3.0 [110/65] via 192.168.4.2, 00:12:54, Serial0/0/1
O 10.0.0.0 [110/193] via 192.168.4.2, 00:09:42, Serial0/0/1
O 192.168.1.0/24 [110/192] via 192.168.4.2, 00:13:27, Serial0/0/1
C 192.168.2.0/24 is directly connected, Serial0/2/1
O 192.168.3.0/24 [110/128] via 192.168.4.2, 00:13:37, Serial0/0/1
R3#
Ready Telnet 45, 4 45 Rows, 132 Cols VT100 CAP NUM
```

```
fec0:41 - SecureCRT
File Edit View Options Transfer Script Tools Help
| fec0:41
+>(tc1)#FEC0::1:1
+>(tc1)#FEC0::4:1
+>(tc1)# {
+>(tc1)#ping $direccion
+>(tc1)#}

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.0.0.1, timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 84/92/96 ms
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.0.3.1, timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 56/60/68 ms
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.1, timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 84/96/104 ms
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.2, timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 96/102/112 ms
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.2.1, timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 20/32/40 ms
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.2.2, timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 76/88/104 ms
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.3.1, timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 76/88/92 ms
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.3.2, timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 52/56/60 ms
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.4.1, timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 112/115/116 ms
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.4.2, timeout is 2 seconds:
!!!!!!
Ready Telnet 45, 9 45 Rows, 132 Cols VT100 CAP NUM
```

R4

```
fec0:4:1 - SecureCRT
File Edit View Options Transfer Script Tools Help
| fec0:4:1
Success rate is 100 percent (5/5), round-trip min/avg/max = 76/88/92 ms
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.3.2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 52/56/60 ms
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.4.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 112/115/116 ms
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.4.2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 56/59/60 ms% unrecognized host or address, or protocol not running.
% unrecognized host or address, or protocol not running.
% unrecognized host or address, or protocol not running.
R3(tc1)#exit
R3#
R3#exit
[Connection to 192.168.2.2 closed by foreign host]
R4#
R4#
R4#
R4#
R4#
R4#sh ipv
R4#sh ipv6 int b
FastEthernet0/0 [up/up]
FE80::217:5AFF:FEAD:4F1A
FE80::4:1
FastEthernet0/1 [administratively down/down]
unassigned
Serial0/0/0 [up/up]
unassigned
Serial0/0/1 [up/up]
unassigned
SSLVPN-VIF0 [up/up]
unassigned
Tunnel0 [up/up]
FE80::5EFE:C0A8:302
123::5EFE:C0A8:302
R4#
Ready Telnet 45, 4 45 Rows, 132 Cols VT100 CAP NUM
```

```
fec0:4:1 - SecureCRT
File Edit View Options Transfer Script Tools Help
| fec0:4:1
R4#
R4#
R4#
R4#
R4#
R4#sh ipv
R4#sh ipv6 int b
FastEthernet0/0 [up/up]
FE80::217:5AFF:FEAD:4F1A
FE80::4:1
FastEthernet0/1 [administratively down/down]
unassigned
Serial0/0/0 [up/up]
unassigned
Serial0/0/1 [up/up]
unassigned
SSLVPN-VIF0 [up/up]
unassigned
Tunnel0 [up/up]
FE80::5EFE:C0A8:302
123::5EFE:C0A8:302
R4#sh ipv roy
R4#sh ipv ro
R4#sh ipv route
IPv6 Routing Table - Default - 6 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
B - BGP, M - MIPv6, R - RIP, I1 - ISIS L1
I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary, D - EIGRP
EX - EIGRP external
O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
C 123::/64 [0/0]
via Tunnel0, directly connected
L 123::5EFE:C0A8:302/128 [0/0]
via Tunnel0, receive
S FE80::1:0:112 [1/0]
via 123::5EFE:C0A8:101
C FE80::4:0:112 [0/0]
via FastEthernet0/0, directly connected
L FE80::4:1:128 [0/0]
via FastEthernet0/0, receive
L FF00::/8 [0/0]
via Null0, receive
R4#
Ready Telnet 45, 4 45 Rows, 132 Cols VT100 CAP NUM
```

```
fec0:4:1 - SecureCRT
File Edit View Options Transfer Script Tools Help
| fec0:4:1
O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
C 123::/64 [0/0]
  via Tunnel0, directly connected
L 123::5EFE:C0A8:302/128 [0/0]
  via Tunnel0, receive
S FEC0::1:0/112 [0/0]
  via 123::5EFE:C0A8:101
C FEC0::4:0/112 [0/0]
  via FastEthernet0/0, directly connected
L FEC0::4:1/128 [0/0]
  via FastEthernet0/0, receive
L FF00::/8 [0/0]
  via Null0, receive
R4#sh int un
R4#sh int tun
R4#sh int tunnel 0
Tunnel0 is up, line protocol is up
Hardware is Tunnel
MTU 17920 bytes, BW 100 kbit/sec, DLY 50000 usec,
reliability 255/255, txload 160/255, rxload 127/255
Encapsulation TUNNEL, loopback not set
Keepalive not set
Tunnel source 192.168.3.2
Tunnel protocol/transport IPV6 ISATAP
Tunnel TTL 255
Tunnel transport MTU 1480 bytes
Tunnel transmit bandwidth 8000 (kbps)
Tunnel receive bandwidth 8000 (kbps)
Last input 00:07:53, output 00:07:56, output hang never
Last clearing of "show interface" counters never
Input queue: 0/75/0/0 (size/max/drops/Flushes); Total output drops: 0
Queueing strategy: fifo
Output queue: 0/0 (size/max)
  5 minute input rate 58000 bits/sec, 27 packets/sec
  5 minute output rate 63000 bits/sec, 35 packets/sec
26357 packets input, 6404804 bytes, 0 no buffer
Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
26067 packets output, 6244047 bytes, 0 underruns
0 output errors, 0 collisions, 0 interface resets
0 unknown protocol drops
0 unknown protocol drops
0 output buffer failures, 0 output buffers swapped out
R4#
Ready Telnet 45, 4 45 Rows, 132 Cols VT100 CAP NUM
```

```
fec0:4:1 - SecureCRT
File Edit View Options Transfer Script Tools Help
| fec0:4:1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 16/28/40 ms
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.2.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 60/68/84 ms
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.2.2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 56/59/60 ms
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.3.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 20/23/28 ms
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.3.2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 44/56/76 ms
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.4.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 20/26/36 ms
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.4.2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 60/72/76 ms
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 123::5EFE:C0A8:101, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 56/64/72 ms
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 123::5EFE:C0A8:302, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/4 ms
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to FEC0::1:1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 60/64/80 ms
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to FEC0::4:1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/0 ms
R4(tc1)#
Ready Telnet 45, 9 45 Rows, 132 Cols VT100 CAP NUM
```

```
fec0:41 - SecureCRT
File Edit View Options Transfer Script Tools Help
| fec0:41
R1#tclsh
R1#tclsh
R1(tcl)#foreach direccion {
+>(tcl)#10.0.0.1
+>(tcl)#10.0.3.1
+>(tcl)#192.168.1.1
+>(tcl)#192.168.1.2
+>(tcl)#192.168.2.1
+>(tcl)#192.168.2.2
+>(tcl)#192.168.3.1
+>(tcl)#192.168.3.2
+>(tcl)#192.168.4.1
+>(tcl)#192.168.4.2
+>(tcl)#123::SEFE:COA8:101
+>(tcl)#123::SEFE:COA8:302
+>(tcl)#FECO:1:1
+>(tcl)#FECO:4:1
+>(tcl)# {
+>(tcl)#ping $direccion
+>(tcl)#}

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.0.0.1, timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.0.3.1, timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 52/66/84 ms
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.1, timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 36/43/52 ms
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.2, timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 20/24/32 ms
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.2.1, timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 60/66/80 ms
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.2.2, timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 36/41/52 ms

Ready Telnet 45, 9 45 Rows, 132 Cols VT100 CAP NUM
```

```
fec0:41 - SecureCRT
File Edit View Options Transfer Script Tools Help
| fec0:41
Tunnel receive bandwidth 8000 (kbps)
Last input 00:03:55, output 00:03:55, output hang never
Last clearing of "show interface" counters never
Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
Queueing strategy: fifo
Output queue: 0/0 (size/max)
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
37118 packets input, 8997410 bytes, 0 no buffer
Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
37845 packets output, 10101692 bytes, 0 underruns
0 output errors, 0 collisions, 0 interface resets
0 unknown protocol drops
0 output buffer failures, 0 output buffers swapped out
R1#sh int tun 0
Tunnel0 is up, line protocol is up
Hardware is Tunnel
MTU 17920 bytes, BW 100 Kbit/sec, DLY 50000 usec,
reliability 255/255, txload 1/255, rxload 1/255
Encapsulation TUNNEL, loopback not set
Keepalive not set
Tunnel source 192.168.1.1
Tunnel protocol/transport IPV6 ISATAP
Tunnel ttl 255
Tunnel transport MTU 1480 bytes
Tunnel transmit bandwidth 8000 (kbps)
Tunnel receive bandwidth 8000 (kbps)
Last input 00:03:58, output 00:03:58, output hang never
Last clearing of "show interface" counters never
Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
Queueing strategy: fifo
Output queue: 0/0 (size/max)
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
37118 packets input, 8997410 bytes, 0 no buffer
Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
37845 packets output, 10101692 bytes, 0 underruns
0 output errors, 0 collisions, 0 interface resets
0 unknown protocol drops
0 unknown protocol drops
0 output buffer failures, 0 output buffers swapped out
R1#

Ready Telnet 45, 4 45 Rows, 132 Cols VT100 CAP NUM
```

QR Ancho de Banda

```
Administrador: C:\Windows\system32\cmd.exe - iperf.exe -s
Vínculo: dirección IPv6 local. . . : fe80::dde6:50e0:4d34:df4%12
Dirección IPv4. . . . . : 10.0.3.2
Máscara de subred . . . . . : 255.255.255.0
Puerta de enlace predeterminada . . . . : fe80::217:5aff:fead:4f1a%12
                                         10.0.3.1

Adaptador de LAN inalámbrica Conexión de red inalámbrica:
Estado de los medios. . . . . : medios desconectados
Sufijo DNS específico para la conexión. . :

c:\iperf-2.0.5-2-win32>iperf.exe -s
-----
Server listening on TCP port 5001
TCP window size: 64.0 KByte (default)
-----
[  4] local 10.0.3.2 port 5001 connected with 10.0.0.2 port 1080
[ ID] Interval      Transfer    Bandwidth
[  4] 0.0-26.2 sec   384 KBytes  120 Kbits/sec
[  4] local 10.0.3.2 port 5001 connected with 10.0.0.2 port 1081
[  4] 0.0-26.3 sec   384 KBytes  120 Kbits/sec
[  5] local 10.0.3.2 port 5001 connected with 10.0.0.2 port 1082
[  5] 0.0-52.7 sec   384 KBytes  59.7 Kbits/sec
```

```
Administrador: C:\Windows\system32\cmd.exe - iperf.exe -s -V
c:\iperf-2.0.5-2-win32>iperf.exe -s -U
-----
Server listening on TCP port 5001
TCP window size: 64.0 KByte (default)
-----
[  4] local fec0::4:2 port 5001 connected with fec0::1:10 port 1077
[ ID] Interval      Transfer    Bandwidth
[  4] 0.0-27.3 sec   384 KBytes  115 Kbits/sec
[  4] local fec0::4:2 port 5001 connected with fec0::1:10 port 1078
[  4] 0.0-27.0 sec   384 KBytes  117 Kbits/sec
[  4] local fec0::4:2 port 5001 connected with fec0::1:10 port 1079
[  4] 0.0-27.4 sec   384 KBytes  115 Kbits/sec
```

ANEXO 6

CLIENTE TELNET GRE


```
192.168.1.1 (3) - SecureCRT
File Edit View Options Transfer Script Tools Help
| 192.168.1.1 (3) | 192.168.1.1 (3) (1) | 192.168.1.1 (3) (2) | 192.168.1.1 (3) (3)
ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
S ::/0 [1/0]
  via Tunnel0, directly connected
C 2001::/64 [0/0]
  via Tunnel0, directly connected
L 2001::1:1/28 [0/0]
  via Tunnel0, receive
C FE00::1:0/112 [0/0]
  via FastEthernet0/0, directly connected
L FE00::1:1/28 [0/0]
  via FastEthernet0/0, receive
L FF00::/8 [0/0]
  via Null0, receive
R1#sh int tun0
Tunnel0 is up, line protocol is up
Hardware is Tunnel
MTU 17916 bytes, BW 100 kbit/sec, DLY 50000 usec,
  reliability 255/255, txload 255/255, rxload 249/255
Encapsulation TUNNEL, loopback not set
Keepalive not set
Tunnel source 192.168.1.1, destination 192.168.4.2
Tunnel protocol/transport GRE/IP
  key disabled, sequencing disabled
  checksumming of packets disabled
Tunnel TTL 255
Fast tunneling enabled
Tunnel transport MTU 1476 bytes
Tunnel transmit bandwidth 8000 (kbps)
Tunnel receive bandwidth 8000 (kbps)
Last input 00:00:06, output 00:00:06, output hang never
Last clearing of "show interface" counters never
Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 2
Queueing strategy: fifo
Output queue: 0/0 (size/max)
5 minute input rate 98000 bits/sec, 84 packets/sec
5 minute output rate 119000 bits/sec, 73 packets/sec
160681 packets input, 21964409 bytes, 0 no buffer
Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
160701 packets output, 21984108 bytes, 0 underruns
0 output errors, 0 collisions, 0 interface resets
0 unknown protocol drops
0 unknown protocol drops
0 output buffer failures, 0 output buffers swapped out
R1#
```

```
192.168.1.1 (3) - SecureCRT
File Edit View Options Transfer Script Tools Help
| 192.168.1.1 (3) | 192.168.1.1 (3) (1) | 192.168.1.1 (3) (2) | 192.168.1.1 (3) (3)
Keepalive not set
Tunnel source 192.168.1.1, destination 192.168.4.2
Tunnel protocol/transport GRE/IP
  key disabled, sequencing disabled
  checksumming of packets disabled
Tunnel TTL 255
Fast tunneling enabled
Tunnel transport MTU 1476 bytes
Tunnel transmit bandwidth 8000 (kbps)
Tunnel receive bandwidth 8000 (kbps)
Last input 00:00:06, output 00:00:06, output hang never
Last clearing of "show interface" counters never
Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 2
Queueing strategy: fifo
Output queue: 0/0 (size/max)
5 minute input rate 98000 bits/sec, 84 packets/sec
5 minute output rate 119000 bits/sec, 73 packets/sec
160681 packets input, 21964409 bytes, 0 no buffer
Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
160701 packets output, 21984108 bytes, 0 underruns
0 output errors, 0 collisions, 0 interface resets
0 unknown protocol drops
0 unknown protocol drops
0 output buffer failures, 0 output buffers swapped out
R1#sh ip rou
R1#sh ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
I - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default, U - per-user static route
o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

O 192.168.4.0/24 [110/128] via 192.168.2.2, 01:06:46, Serial0/0/0
O 10.0.0.0/24 is subnetted, 2 subnets
O 10.0.3.0 [110/129] via 192.168.2.2, 01:06:46, Serial0/0/0
C 10.0.0.0 is directly connected, FastEthernet0/0
C 192.168.1.0/24 is directly connected, Serial0/0/1
C 192.168.2.0/24 is directly connected, Serial0/0/0
O 192.168.3.0/24 [110/192] via 192.168.2.2, 01:06:46, Serial0/0/0
R1#
```

R2

```
192.168.1.1 (3) (1) - SecureCRT
File Edit View Options Transfer Script Tools Help
192.168.1.1 (3) | 192.168.1.1 (1) | 192.168.1.1 (3) (2) | 192.168.1.1 (3) (3)

User Access Verification
Password:
R1>ena
Password:
R1#192.168.1.2
Trying 192.168.1.2 ... Open

User Access Verification
Password:
R2>ena
Password:
R2#sh ip rou
R2#sh ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
I - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default, U - per-user static route
o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

O 192.168.4.0/24 [110/192] via 192.168.1.1, 01:06:56, Serial0/2/1
O 10.0.0.0/24 is subnetted, 2 subnets
O 10.0.3.0 [110/193] via 192.168.1.1, 01:06:56, Serial0/2/1
O 10.0.0.0 [110/65] via 192.168.1.1, 01:06:56, Serial0/2/1
C 192.168.1.0/24 is directly connected, Serial0/2/1
O 192.168.2.0/24 [110/128] via 192.168.1.1, 01:06:56, Serial0/2/1
C 192.168.3.0/24 is directly connected, Serial0/0/1
R2#
```

```
192.168.1.1 (3) (1) - SecureCRT
File Edit View Options Transfer Script Tools Help
192.168.1.1 (3) | 192.168.1.1 (3) (1) | 192.168.1.1 (3) (2) | 192.168.1.1 (3) (3)

Password:
R1>ena
Password:
R1#192.168.1.2
Trying 192.168.1.2 ... open

User Access Verification
Password:
R2>ena
Password:
R2#sh ip rou
R2#sh ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
I - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default, U - per-user static route
o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

O 192.168.4.0/24 [110/192] via 192.168.1.1, 01:06:56, Serial0/2/1
O 10.0.0.0/24 is subnetted, 2 subnets
O 10.0.3.0 [110/193] via 192.168.1.1, 01:06:56, Serial0/2/1
O 10.0.0.0 [110/65] via 192.168.1.1, 01:06:56, Serial0/2/1
C 192.168.1.0/24 is directly connected, Serial0/2/1
O 192.168.2.0/24 [110/128] via 192.168.1.1, 01:06:56, Serial0/2/1
C 192.168.3.0/24 is directly connected, Serial0/0/1
R2#sh ip int b
Interface IP-Address OK? Method Status Protocol
FastEthernet0/0 10.0.1.1 YES TFTP up down
FastEthernet0/1 unassigned YES TFTP administratively down down
Serial0/0/0 unassigned YES unset administratively down down
Serial0/0/1 192.168.3.1 YES TFTP up up
Serial0/1/0 unassigned YES unset administratively down down
Serial0/1/1 unassigned YES unset administratively down down
Serial0/2/0 unassigned YES unset administratively down down
Serial0/2/1 192.168.1.2 YES TFTP up up
SSLVPN-VIF0 unassigned NO unset up up
R2#
```

R3

```
192.168.1.1 (3) (2) - SecureCRT
File Edit View Options Transfer Script Tools Help
192.168.1.1 (3) | 192.168.1.1 (3) (1) | 192.168.1.1 (3) (2) | 192.168.1.1 (3) (3)

User Access Verification
Password:
R1>ena
Password:
R1#
R1#
R1#192.168.2.2
Trying 192.168.2.2 ... open

User Access Verification
Password:
R3>ena
Password:
R3#sh ip int b
Interface IP-Address OK? Method Status Protocol
FastEthernet0/0 10.0.2.1 YES TFTP up down
FastEthernet0/1 unassigned YES TFTP administratively down down
Serial0/0/0 unassigned YES unset administratively down down
Serial0/0/1 192.168.4.1 YES TFTP up up
Serial0/2/0 unassigned YES unset administratively down down
Serial0/2/1 192.168.2.2 YES TFTP up up
SSLVPN-VIF0 unassigned NO unset up
R3#
```

```
192.168.1.1 (3) (2) - SecureCRT
File Edit View Options Transfer Script Tools Help
192.168.1.1 (3) | 192.168.1.1 (3) (1) | 192.168.1.1 (3) (2) | 192.168.1.1 (3) (3)

User Access Verification
Password:
R1>ena
Password:
R1#
R1#
R1#192.168.2.2
Trying 192.168.2.2 ... Open

User Access Verification
Password:
R3>ena
Password:
R3#sh ip int b
Interface IP-Address OK? Method Status Protocol
FastEthernet0/0 10.0.2.1 YES TFTP up down
FastEthernet0/1 unassigned YES TFTP administratively down down
Serial0/0/0 unassigned YES unset administratively down down
Serial0/0/1 192.168.4.1 YES TFTP up up
Serial0/2/0 unassigned YES unset administratively down down
Serial0/2/1 192.168.2.2 YES TFTP up up
SSLVPN-VIF0 unassigned NO unset up
R3#sh ip rou
R3#sh ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
I - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default, U - per-user static route
o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

C 192.168.4.0/24 is directly connected, serial0/0/1
O 10.0.0.0/24 is subnetted, 2 subnets
O 10.0.3.0 [110/65] via 192.168.4.2, 01:14:31, serial0/0/1
O 10.0.0.0 [110/193] via 192.168.4.2, 01:13:23, serial0/0/1
O 192.168.1.0/24 [110/192] via 192.168.4.2, 01:13:23, serial0/0/1
C 192.168.2.0/24 is directly connected, serial0/2/1
O 192.168.3.0/24 [110/128] via 192.168.4.2, 01:14:31, serial0/0/1
R3#
```

R4

```
192.168.1.1 (3) - SecureCRT
File Edit View Options Transfer Script Tools Help
192.168.1.1 (3) | 192.168.1.1 (3) (1) | 192.168.1.1 (3) (2) | 192.168.1.1 (3) (3)

User Access Verification
Password:
R1>ena
Password:
R1#192.168.4.2
Trying 192.168.4.2 ... Open

User Access Verification
Password:
R4>ena
Password:
R4#
R4#sh ip int b
Interface      IP-Address      OK? Method Status      Protocol
FastEthernet0/0 10.0.3.1        YES TFTP   up           up
FastEthernet0/1 unassigned      YES TFTP   administratively down down
Serial0/0/0     192.168.4.2    YES TFTP   up           up
Serial0/0/1     192.168.3.2    YES TFTP   up           up
SSLVPN-VIF0    unassigned      NO unset   up           up
Tunnel0        unassigned      YES manual up           up
R4#

Ready                               Telnet 26, 4 45 Rows, 132 Cols VT100 CAP NUM
```

```
192.168.1.1 (3) - SecureCRT
File Edit View Options Transfer Script Tools Help
192.168.1.1 (3) | 192.168.1.1 (3) (1) | 192.168.1.1 (3) (2) | 192.168.1.1 (3) (3)

User Access Verification
Password:
R1>ena
Password:
R1#192.168.4.2
Trying 192.168.4.2 ... Open

User Access Verification
Password:
R4>ena
Password:
R4#
R4#sh ip int b
Interface      IP-Address      OK? Method Status      Protocol
FastEthernet0/0 10.0.3.1        YES TFTP   up           up
FastEthernet0/1 unassigned      YES TFTP   administratively down down
Serial0/0/0     192.168.4.2    YES TFTP   up           up
Serial0/0/1     192.168.3.2    YES TFTP   up           up
SSLVPN-VIF0    unassigned      NO unset   up           up
Tunnel0        unassigned      YES manual up           up
R4#sh ip rou
R4#sh ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       I - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

C    192.168.4.0/24 is directly connected, Serial0/0/0
O    10.0.0.0/24 is subnetted, 2 subnets
C      10.0.3.0 is directly connected, FastEthernet0/0
O      10.0.0.0 [110/129] via 192.168.3.1, 01:14:29, Serial0/0/1
O    192.168.1.0/24 [110/128] via 192.168.3.1, 01:14:29, Serial0/0/1
O    192.168.2.0/24 [110/192] via 192.168.3.1, 01:14:29, Serial0/0/1
C    192.168.3.0/24 is directly connected, Serial0/0/1
R4#

Ready                               Telnet 45, 4 45 Rows, 132 Cols VT100 CAP NUM
```

```
192.168.1.1 (3) - SecureCRT
File Edit View Options Transfer Script Tools Help
192.168.1.1 (3) | 192.168.1.1 (3) (1) | 192.168.1.1 (3) (2) | 192.168.1.1 (3) (3)

ia - IS-IS inter area, * - candidate default, U - per-user static route
o - ODR, P - periodic download static route

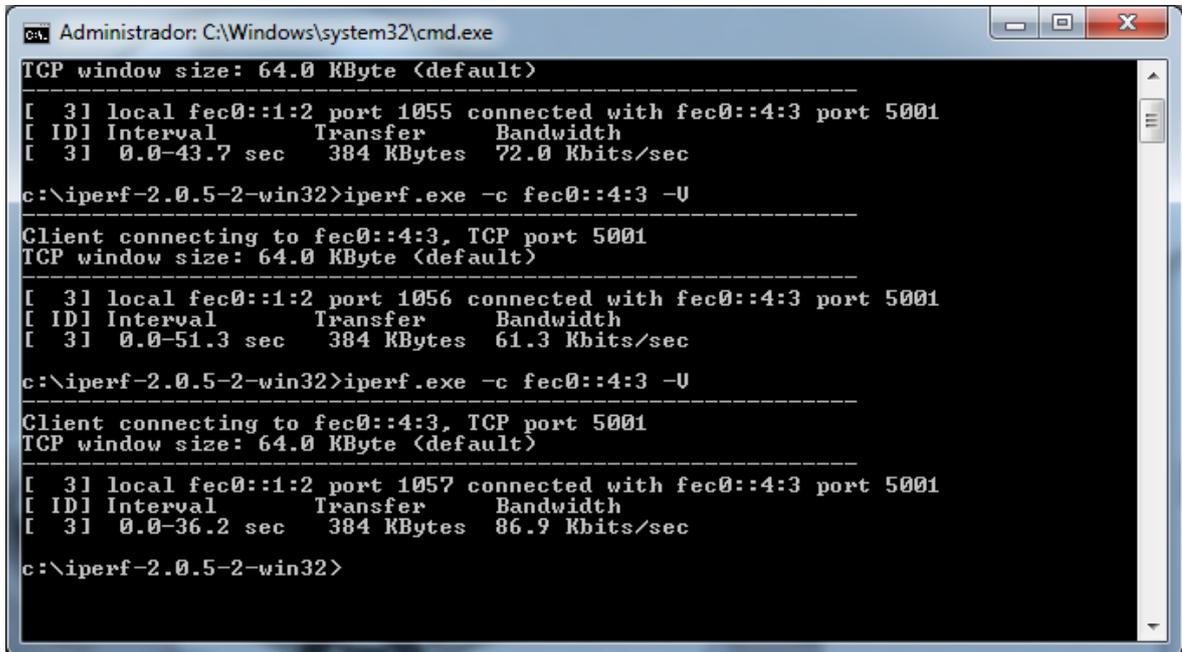
Gateway of last resort is not set

C 192.168.4.0/24 is directly connected, Serial0/0/0
  10.0.0.0/24 is subnetted, 2 subnets
C   10.0.3.0 is directly connected, FastEthernet0/0
O   10.0.0.0 [110/129] via 192.168.3.1, 01:14:29, Serial0/0/1
O 192.168.1.0/24 [110/128] via 192.168.3.1, 01:14:29, Serial0/0/1
O 192.168.2.0/24 [110/192] via 192.168.3.1, 01:14:29, Serial0/0/1
C 192.168.3.0/24 is directly connected, Serial0/0/1
R4#sh int tun
R4#sh int tunnel 0
Tunnel0 is up, line protocol is up
  Hardware is Tunnel
  MTU 17916 bytes, BW 100 Kbit/sec, DLY 50000 usec,
    reliability 255/255, txload 187/255, rxload 199/255
  Encapsulation TUNNEL, loopback not set
  Keepalive not set
  Tunnel source 192.168.4.2, destination 192.168.1.1
  Tunnel protocol/transport GRE/IP
  key disabled, sequencing disabled
  Checksumming of packets disabled
  Tunnel TTL 255
  Fast tunneling enabled
  Tunnel transport MTU 1476 bytes
  Tunnel transmit bandwidth 8000 (kbps)
  Tunnel receive bandwidth 8000 (kbps)
  Last input 00:00:01, output 00:00:01, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 2
  Queueing strategy: fifo
  Output queue: 0/0 (size/max)
  5 minute input rate 105000 bits/sec, 90 packets/sec
  5 minute output rate 86000 bits/sec, 78 packets/sec
  208262 packets input, 29215090 bytes, 0 no buffer
  Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
  0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
  211305 packets output, 28356515 bytes, 0 underruns
  0 output errors, 0 collisions, 0 interface resets
  0 unknown protocol drops
  0 unknown protocol drops
  0 output buffer failures, 0 output buffers swapped out
R4#
```

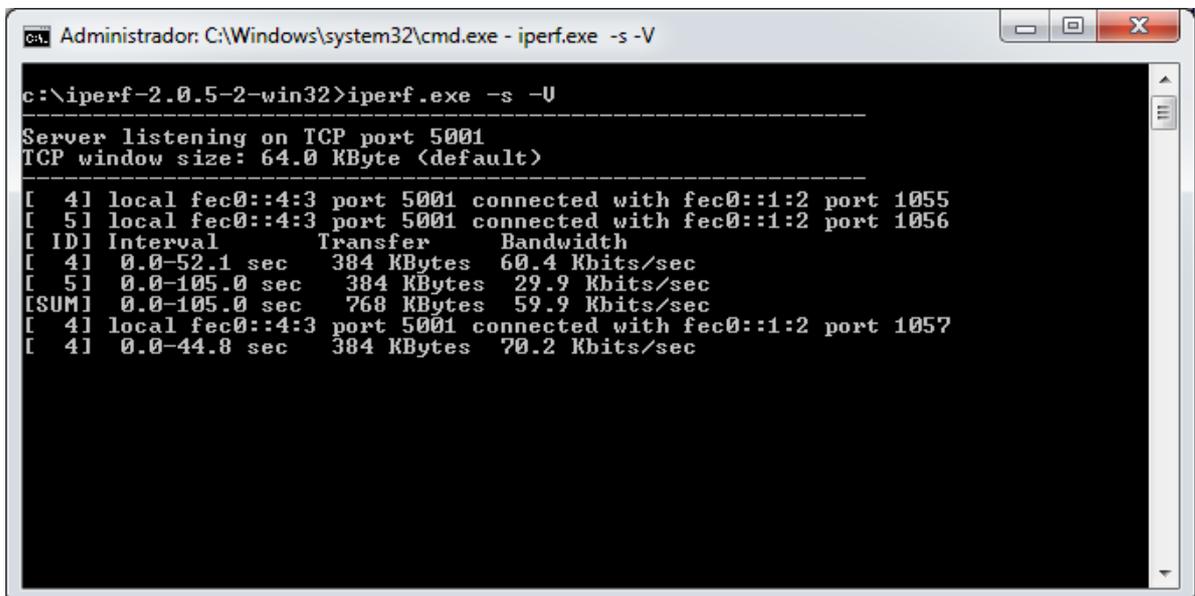
```
192.168.1.1 (3) - SecureCRT
File Edit View Options Transfer Script Tools Help
192.168.1.1 (3) | 192.168.1.1 (3) (1) | 192.168.1.1 (3) (2) | 192.168.1.1 (3) (3)

MTU 17916 bytes, BW 100 Kbit/sec, DLY 50000 usec,
  reliability 255/255, txload 187/255, rxload 199/255
  Encapsulation TUNNEL, loopback not set
  Keepalive not set
  Tunnel source 192.168.4.2, destination 192.168.1.1
  Tunnel protocol/transport GRE/IP
  key disabled, sequencing disabled
  Checksumming of packets disabled
  Tunnel TTL 255
  Fast tunneling enabled
  Tunnel transport MTU 1476 bytes
  Tunnel transmit bandwidth 8000 (kbps)
  Tunnel receive bandwidth 8000 (kbps)
  Last input 00:00:01, output 00:00:01, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 2
  Queueing strategy: fifo
  Output queue: 0/0 (size/max)
  5 minute input rate 105000 bits/sec, 90 packets/sec
  5 minute output rate 86000 bits/sec, 78 packets/sec
  208262 packets input, 29215090 bytes, 0 no buffer
  Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
  0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
  211305 packets output, 28356515 bytes, 0 underruns
  0 output errors, 0 collisions, 0 interface resets
  0 unknown protocol drops
  0 unknown protocol drops
  0 output buffer failures, 0 output buffers swapped out
R4#sh ipw
R4#sh ipw6 int b
FastEthernet0/0 [up/up]
  FE80::217:5AFF:FEAD:4F1A
  FEC0::4:1
FastEthernet0/1 [administratively down/down]
  unassigned
Serial0/0/0 [up/up]
  unassigned
Serial0/0/1 [up/up]
  unassigned
SSLVPN-ViF0 [up/up]
  unassigned
Tunnel0 [up/up]
  FE80::217:5AFF:FEAD:4F1A
  2001::1:2
R4#
```

QR Ancho de Banda



```
Administrador: C:\Windows\system32\cmd.exe
TCP window size: 64.0 KByte (default)
-----
[ 3] local fec0::1:2 port 1055 connected with fec0::4:3 port 5001
[ ID] Interval      Transfer    Bandwidth
[ 3]  0.0-43.7 sec   384 KBytes  72.0 Kbits/sec
c:\iperf-2.0.5-2-win32>iperf.exe -c fec0::4:3 -U
-----
Client connecting to fec0::4:3, TCP port 5001
TCP window size: 64.0 KByte (default)
-----
[ 3] local fec0::1:2 port 1056 connected with fec0::4:3 port 5001
[ ID] Interval      Transfer    Bandwidth
[ 3]  0.0-51.3 sec   384 KBytes  61.3 Kbits/sec
c:\iperf-2.0.5-2-win32>iperf.exe -c fec0::4:3 -U
-----
Client connecting to fec0::4:3, TCP port 5001
TCP window size: 64.0 KByte (default)
-----
[ 3] local fec0::1:2 port 1057 connected with fec0::4:3 port 5001
[ ID] Interval      Transfer    Bandwidth
[ 3]  0.0-36.2 sec   384 KBytes  86.9 Kbits/sec
c:\iperf-2.0.5-2-win32>
```



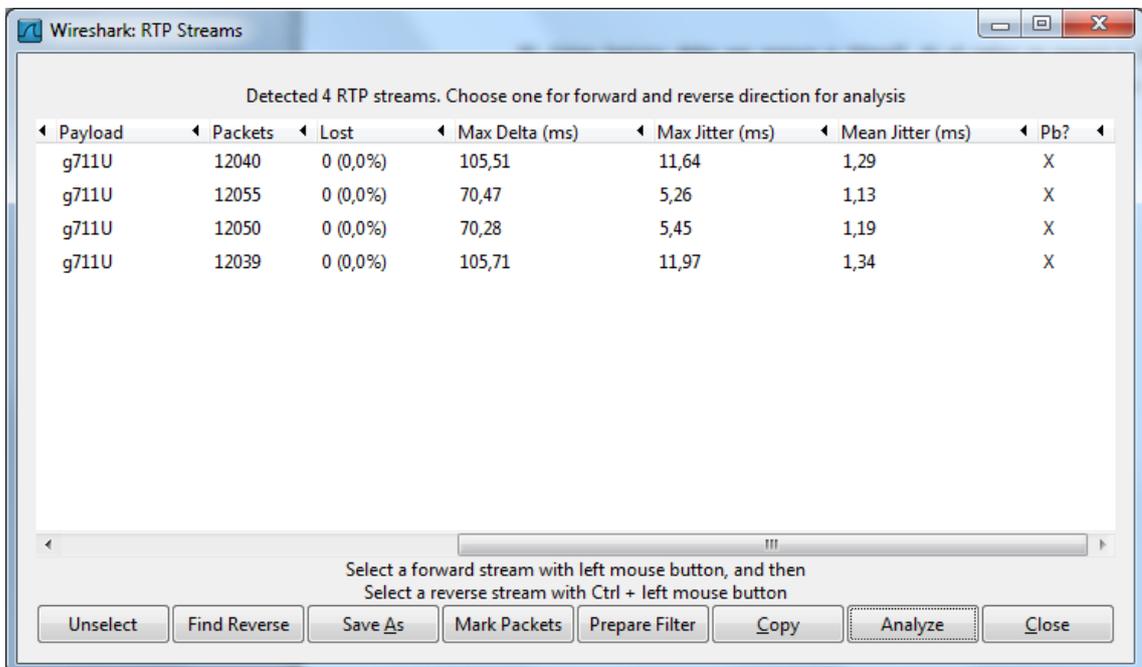
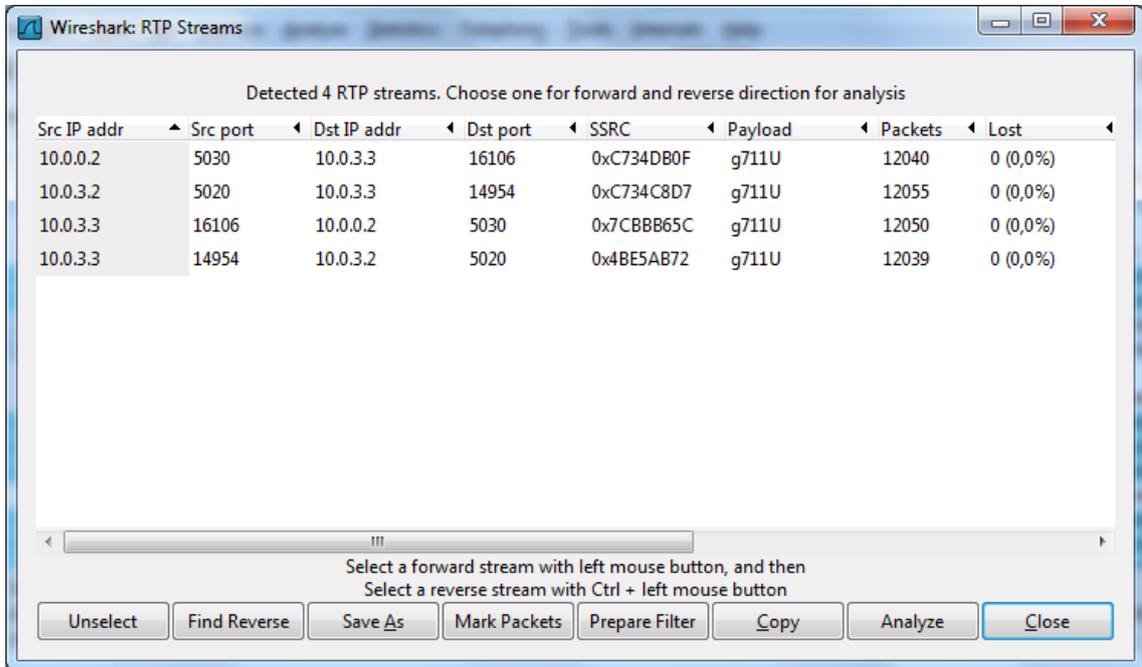
```
Administrador: C:\Windows\system32\cmd.exe - iperf.exe -s -V
c:\iperf-2.0.5-2-win32>iperf.exe -s -U
-----
Server listening on TCP port 5001
TCP window size: 64.0 KByte (default)
-----
[ 4] local fec0::4:3 port 5001 connected with fec0::1:2 port 1055
[ 5] local fec0::4:3 port 5001 connected with fec0::1:2 port 1056
[ ID] Interval      Transfer    Bandwidth
[ 4]  0.0-52.1 sec   384 KBytes  60.4 Kbits/sec
[ 5]  0.0-105.0 sec   384 KBytes  29.9 Kbits/sec
[SUM] 0.0-105.0 sec   768 KBytes  59.9 Kbits/sec
[ 4] local fec0::4:3 port 5001 connected with fec0::1:2 port 1057
[ 4]  0.0-44.8 sec   384 KBytes  70.2 Kbits/sec
```

ANEXO 7

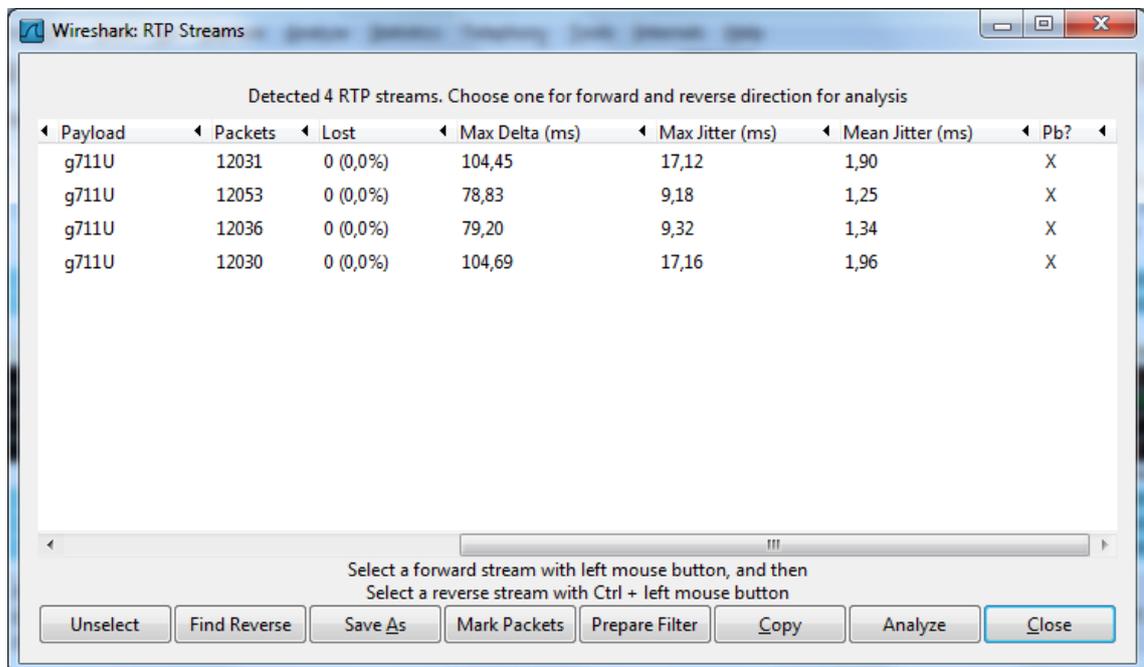
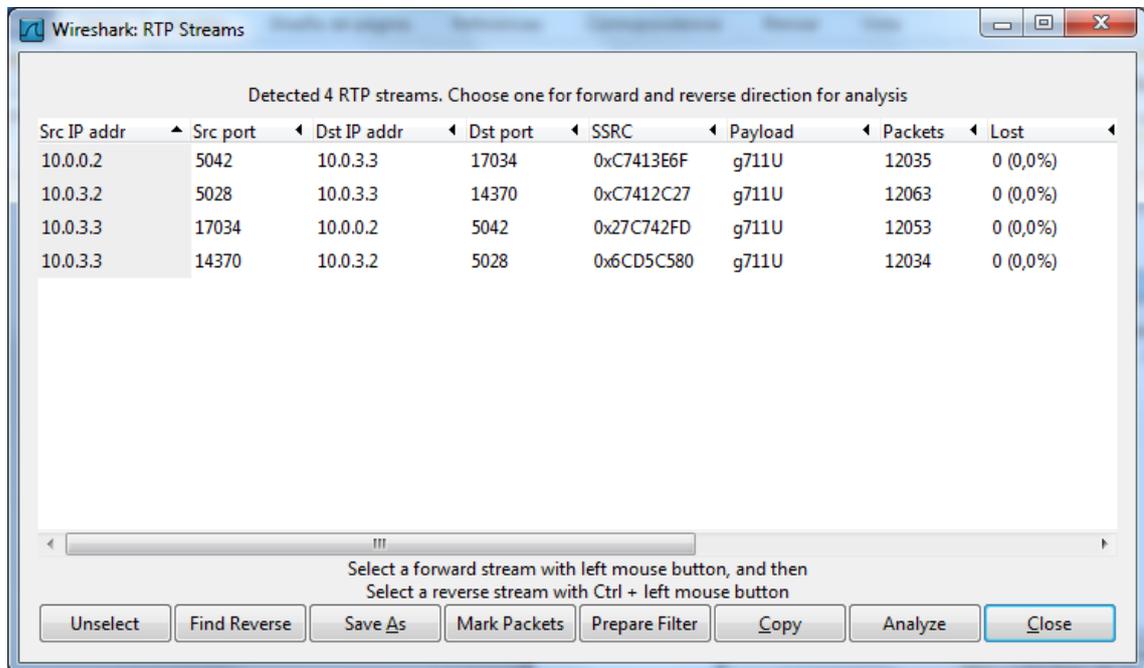
WIRESHARK PRUEBAS IPv4

WIRESHARK PRUEBAS IPv4

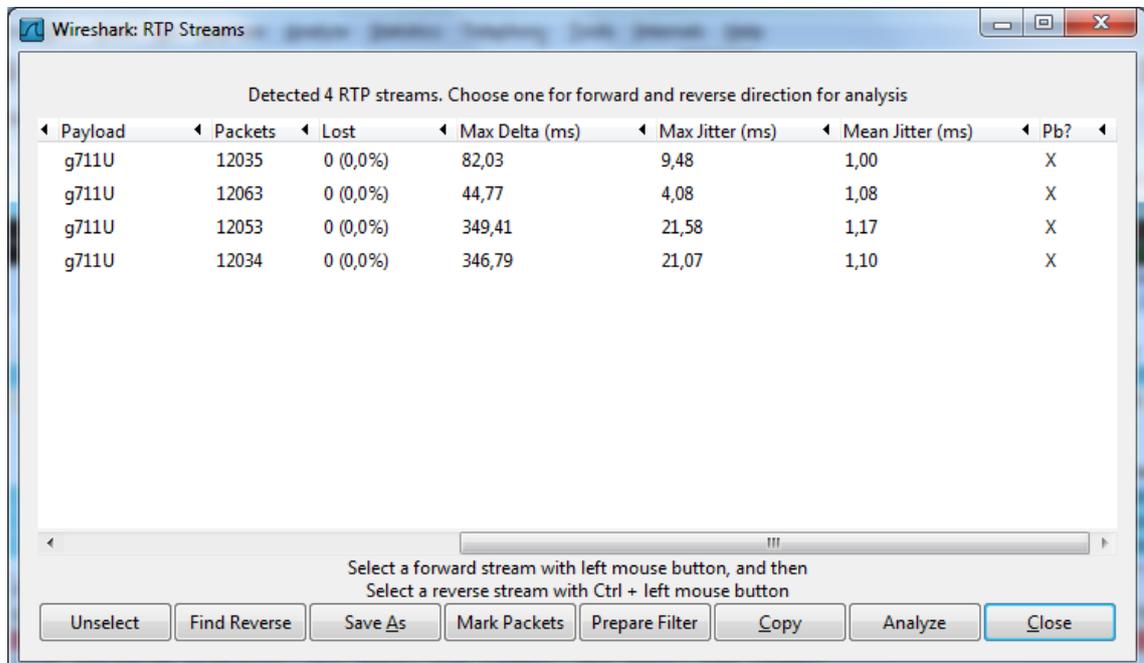
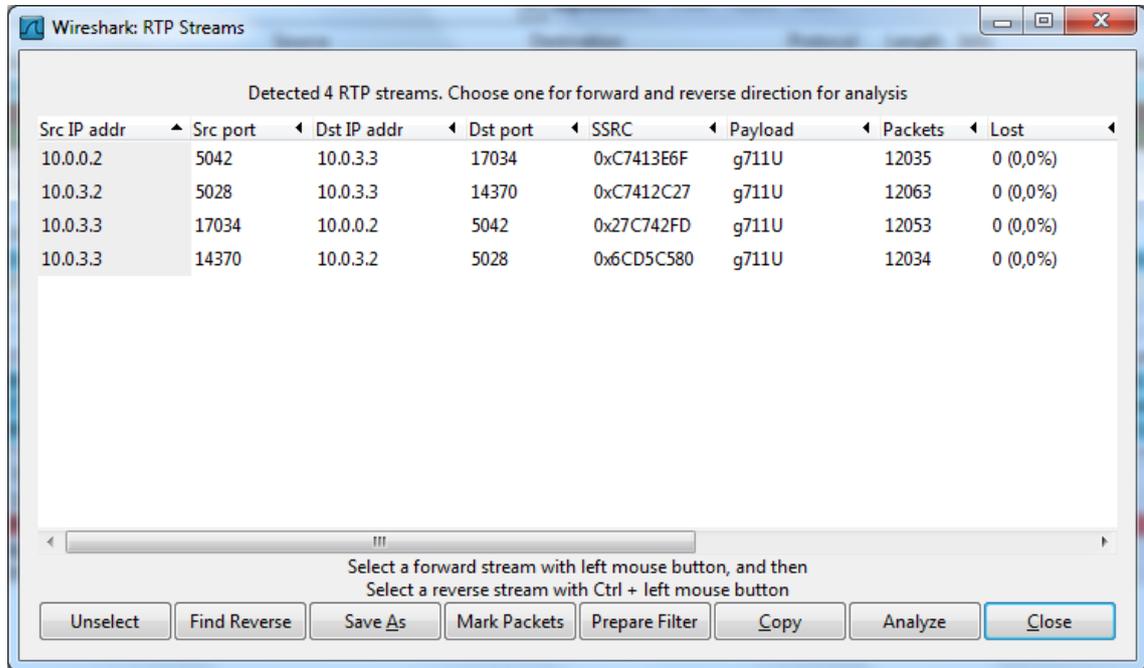
Prueba 1



QR **Prueba 2**



QR **Prueba 3**

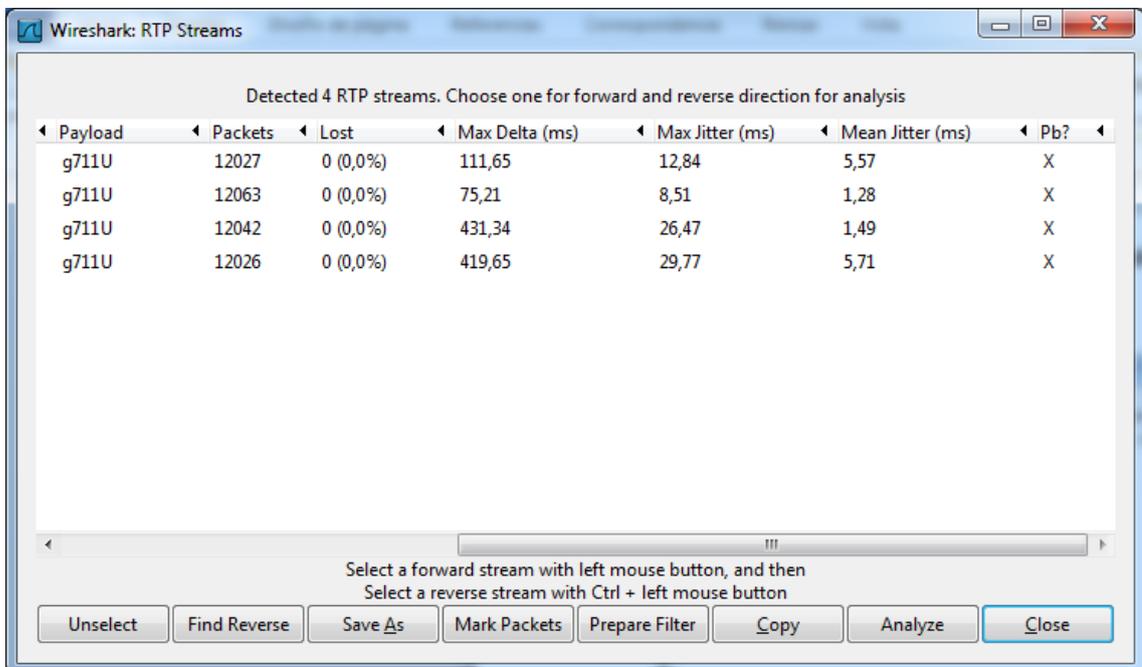
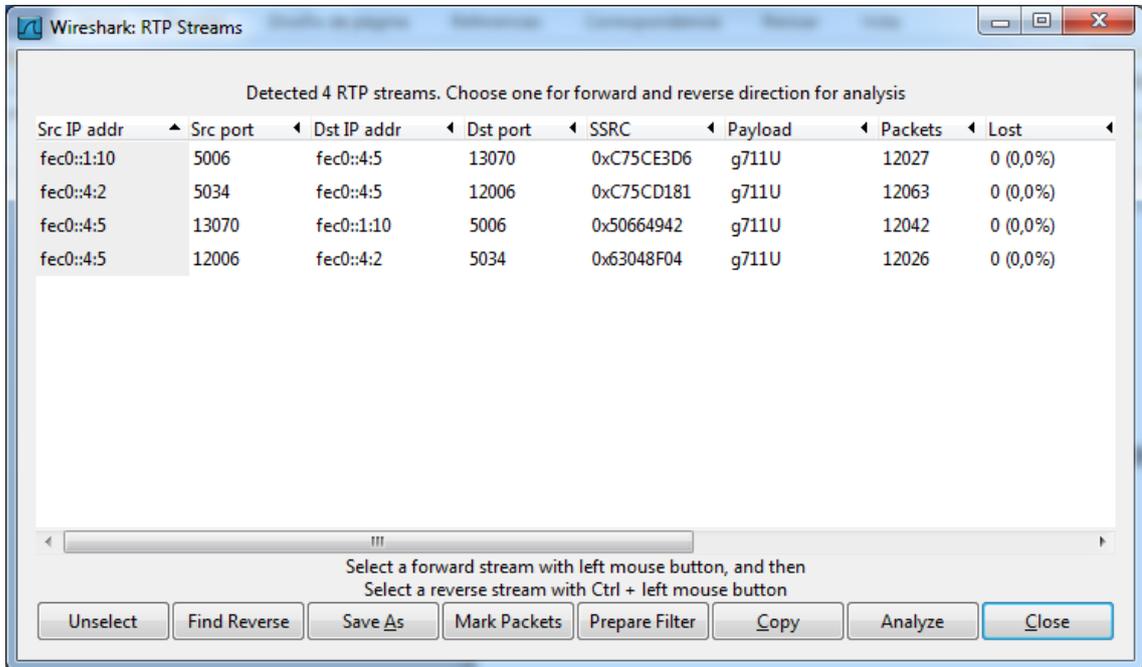


ANEXO 8

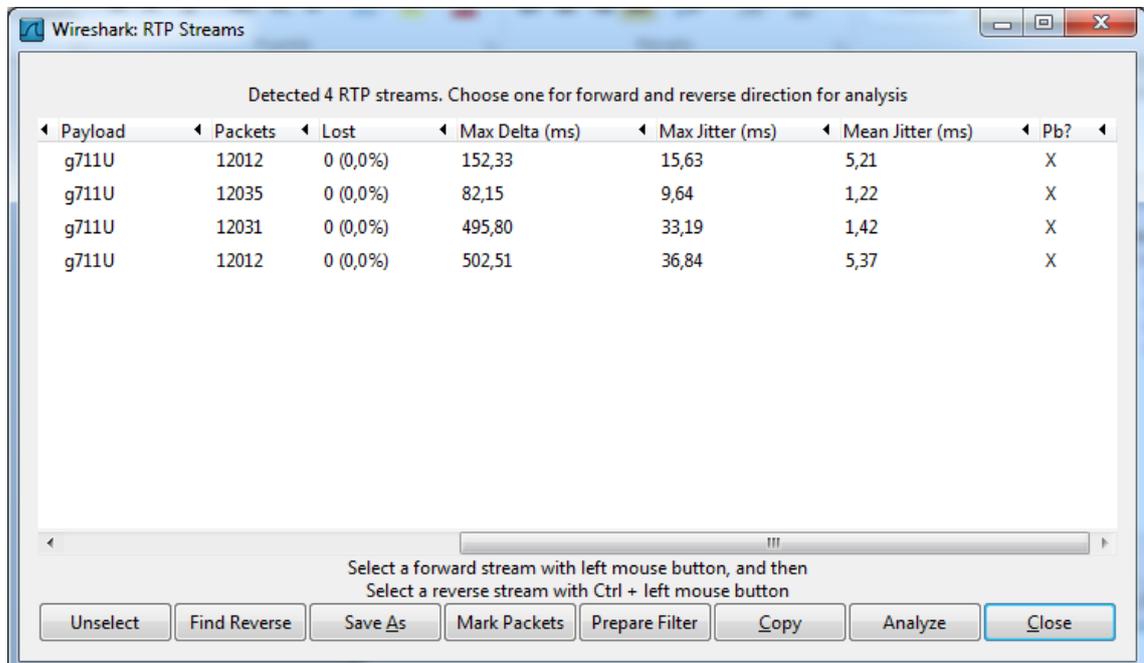
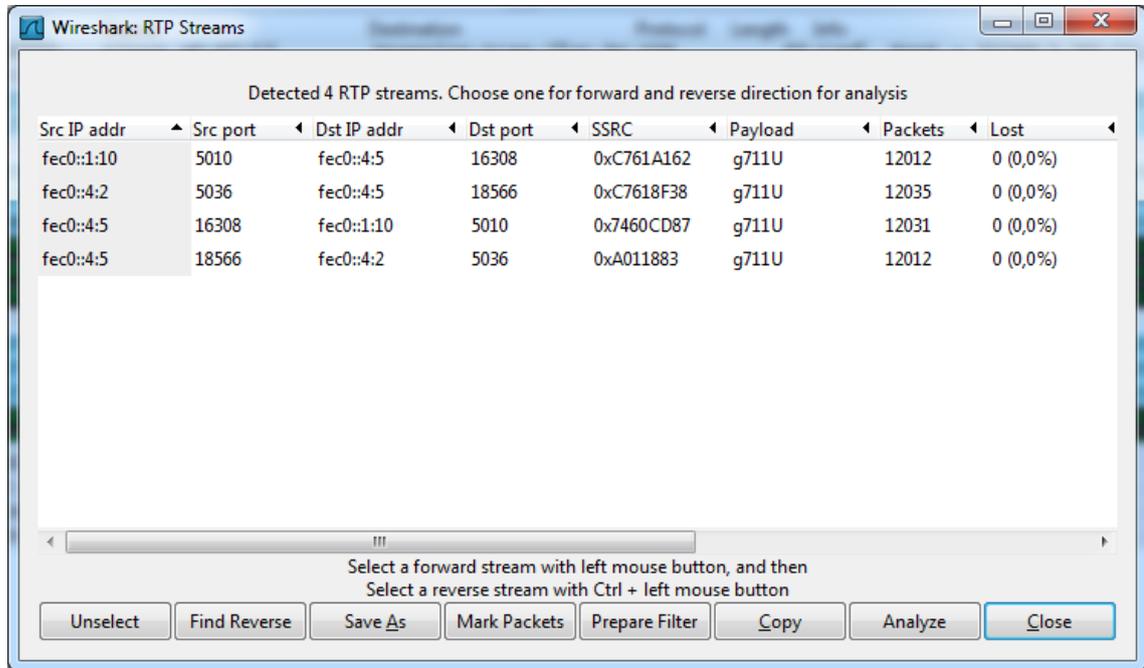
WIRESHARK PRUEBAS IPv6

WIRESHARK PRUEBAS IPv6

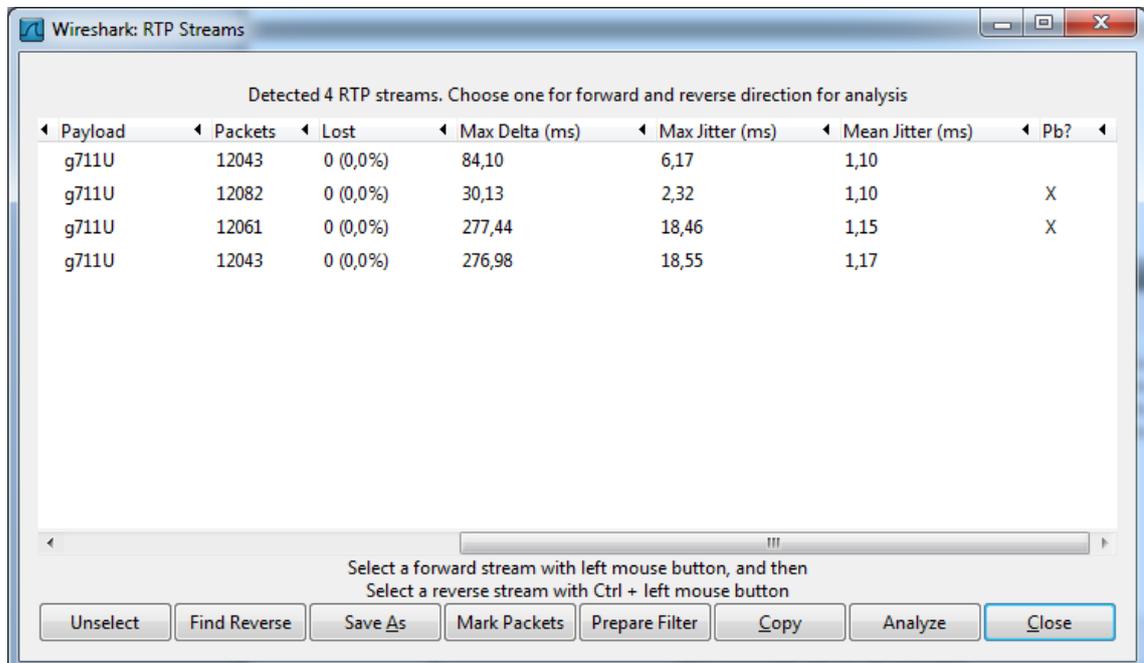
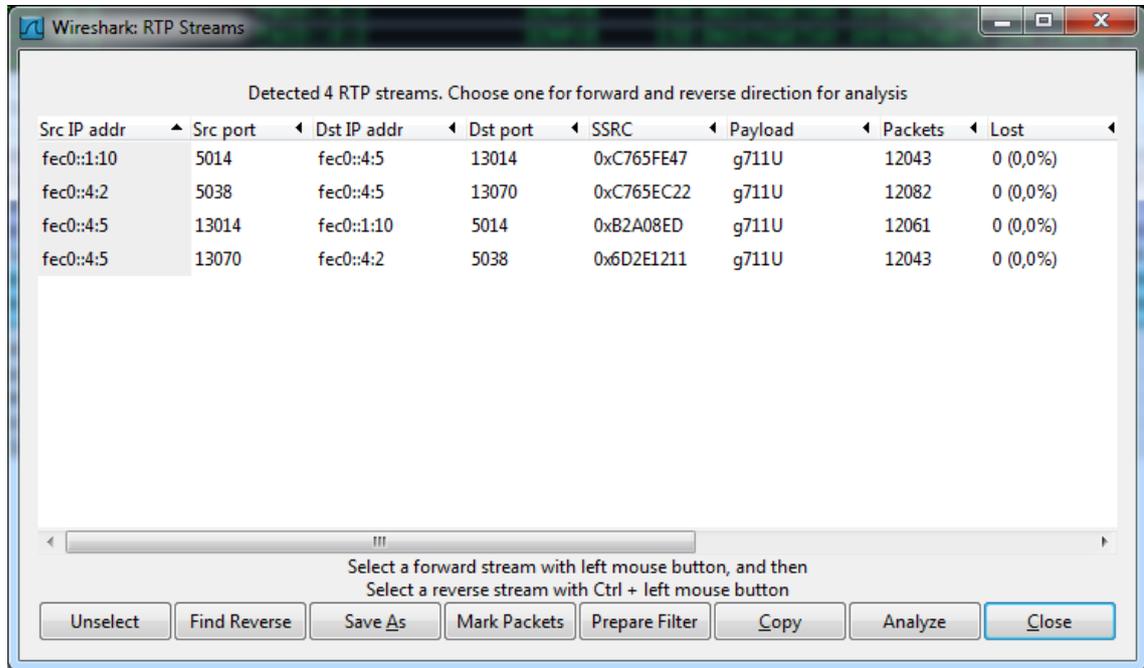
Prueba 1



QR **Prueba 2**



QR **Prueba 3**

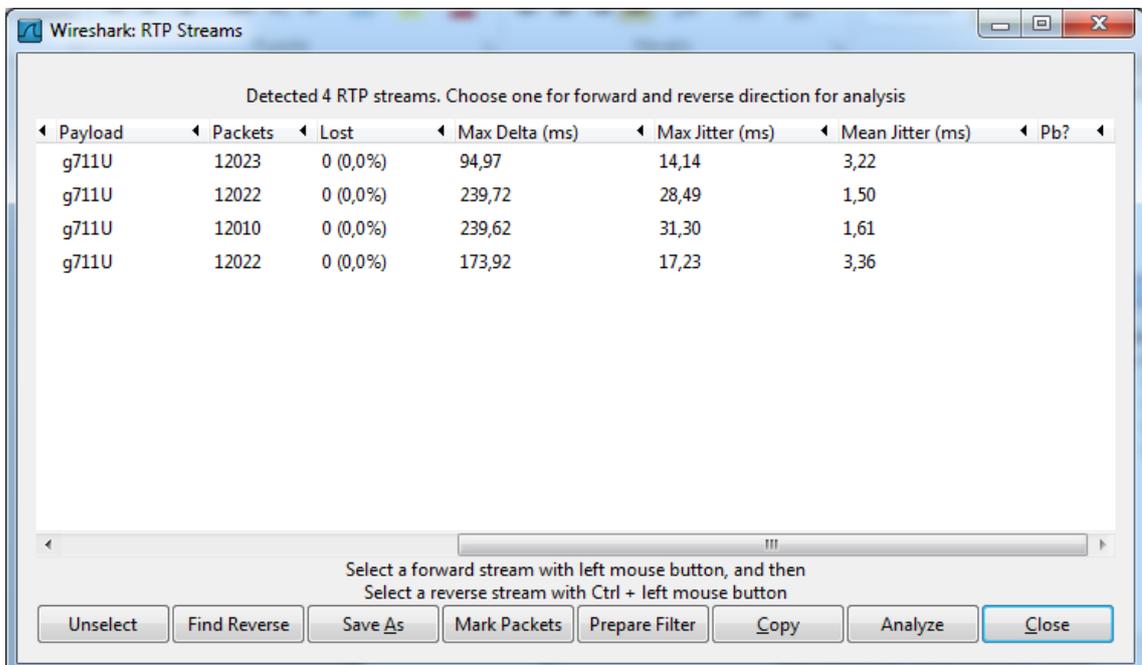
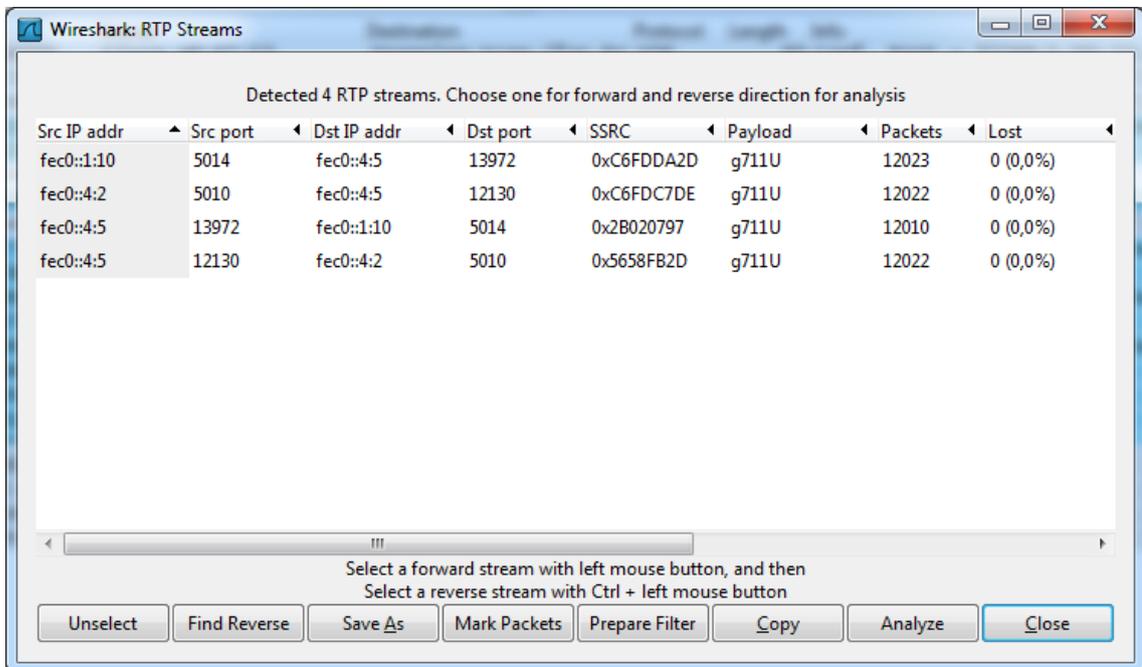


ANEXO 9

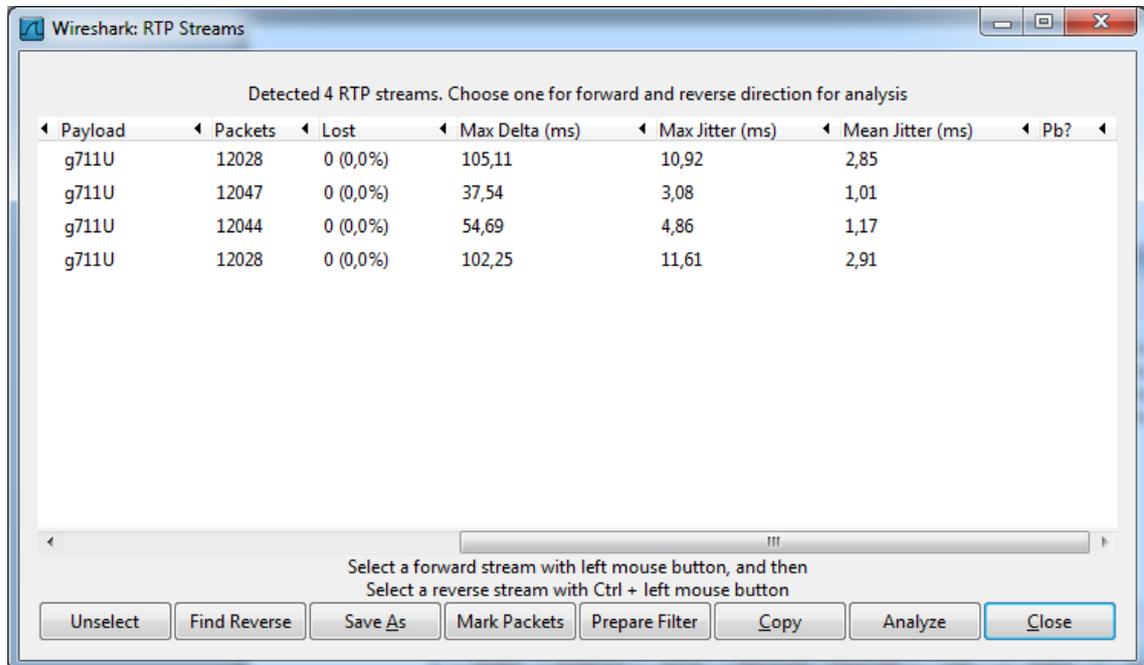
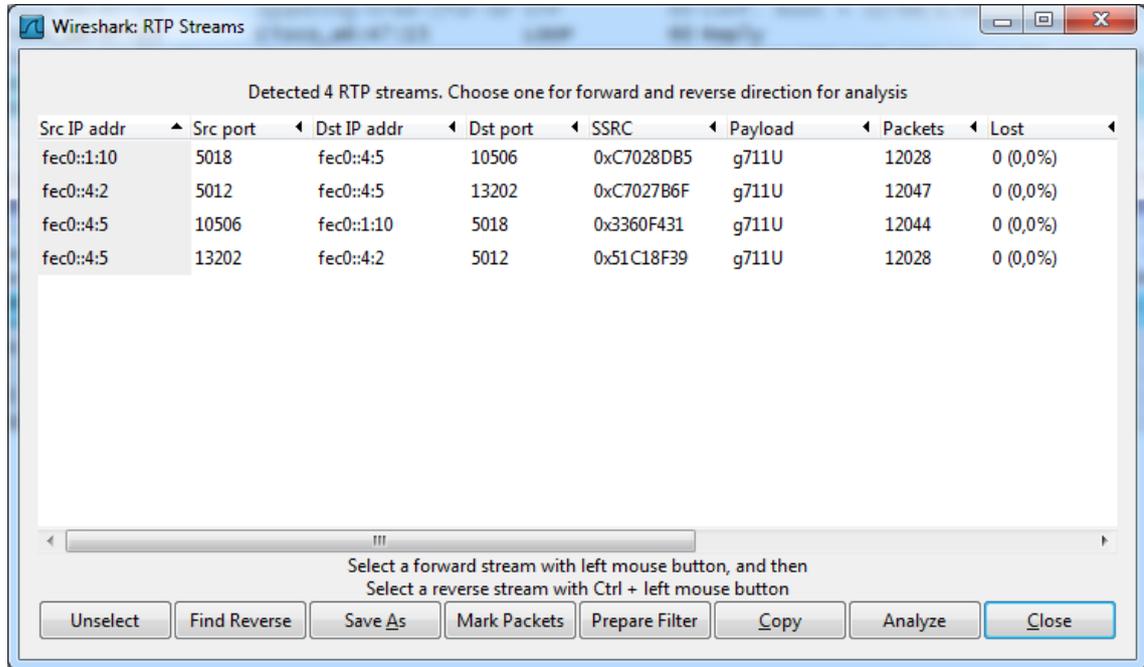
WIRESHARK PRUEBAS 6to4

WIRESHARK PRUEBAS 6to4

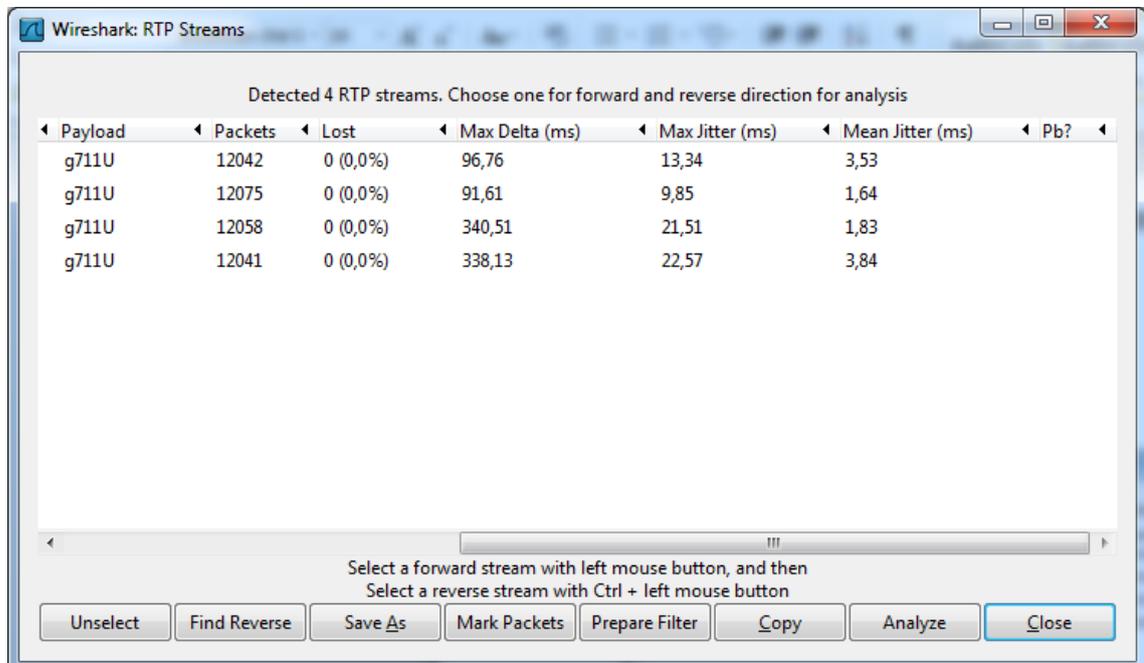
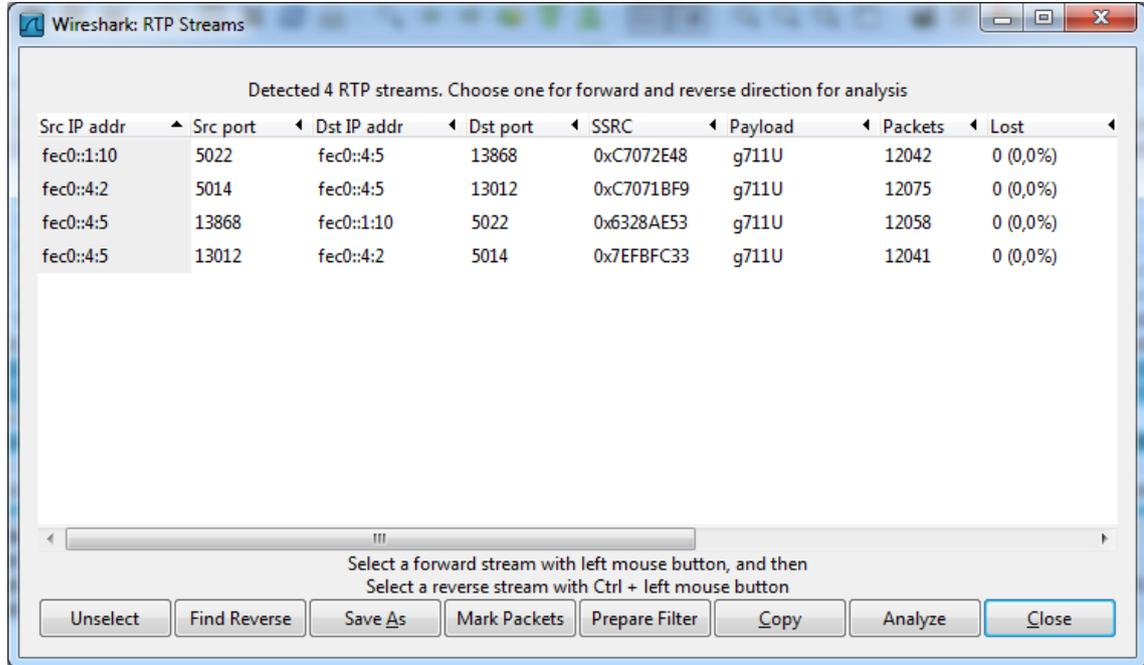
Prueba 1



Prueba 2



QR **Prueba 3**

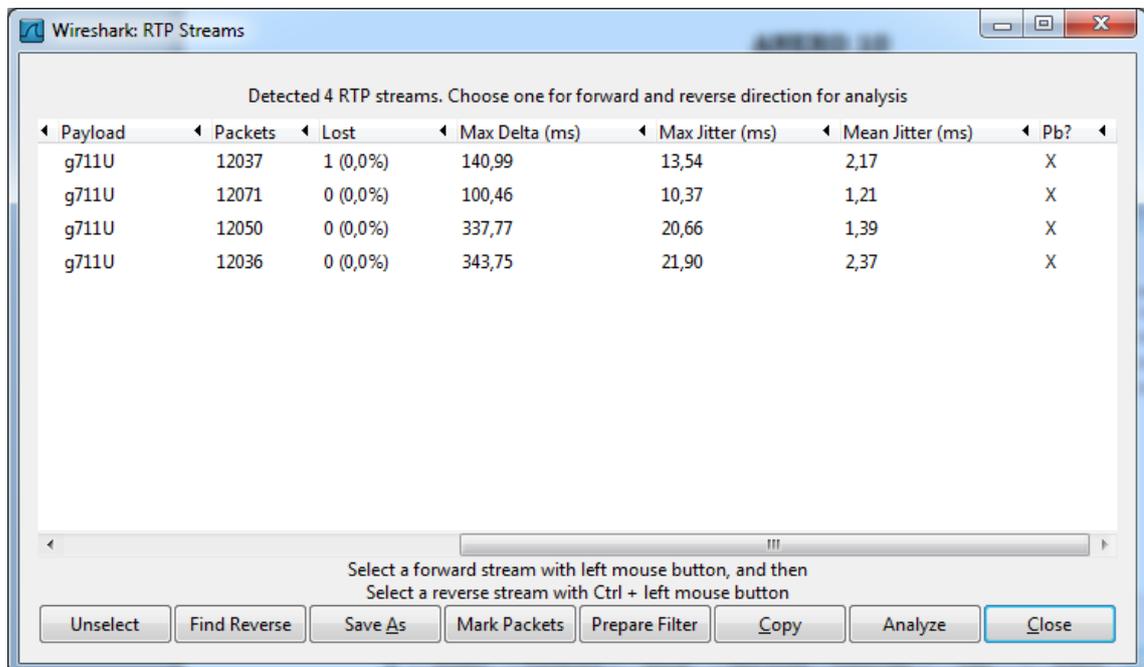
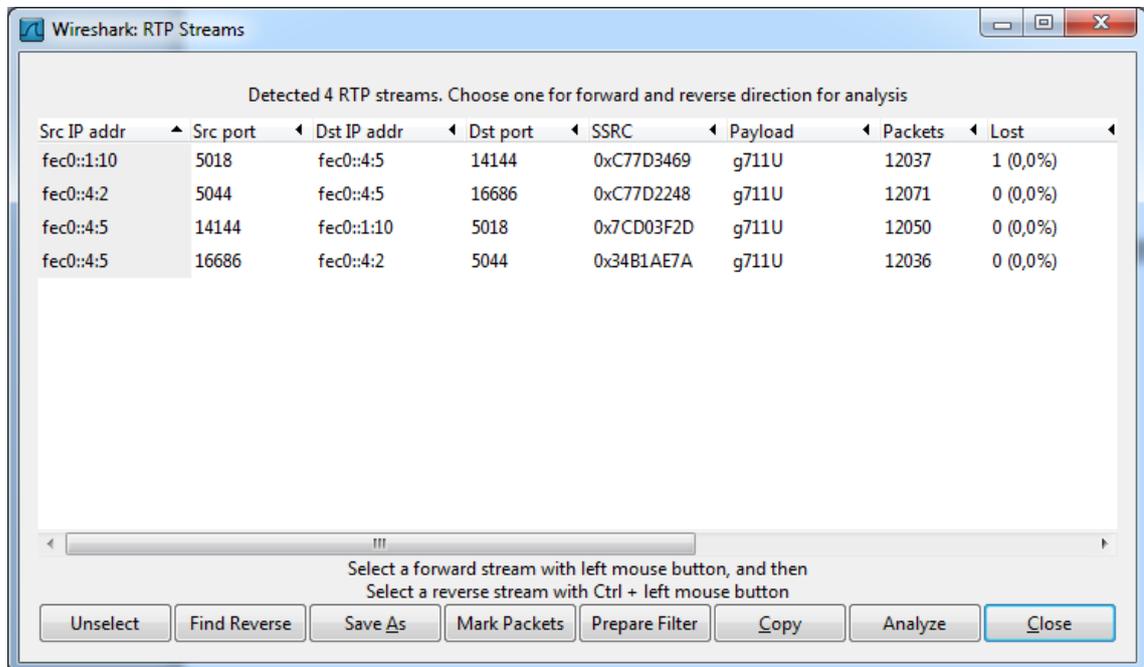


ANEXO 10

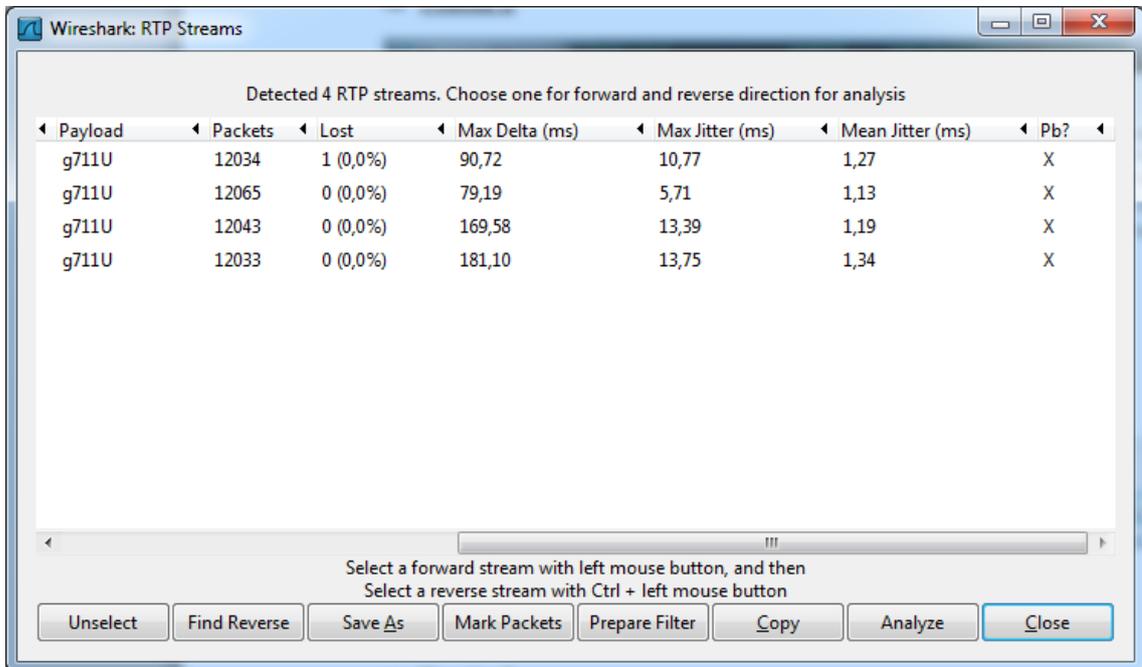
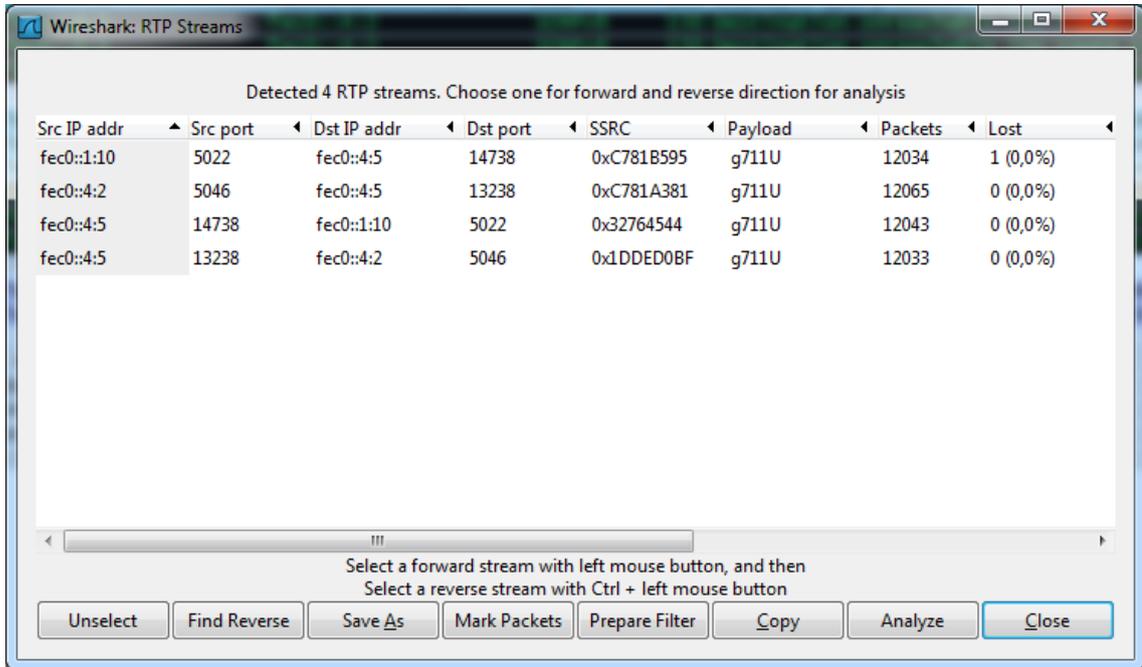
WIRESHARK PRUEBAS ISATAP

WIRESHARK PRUEBAS ISATAP

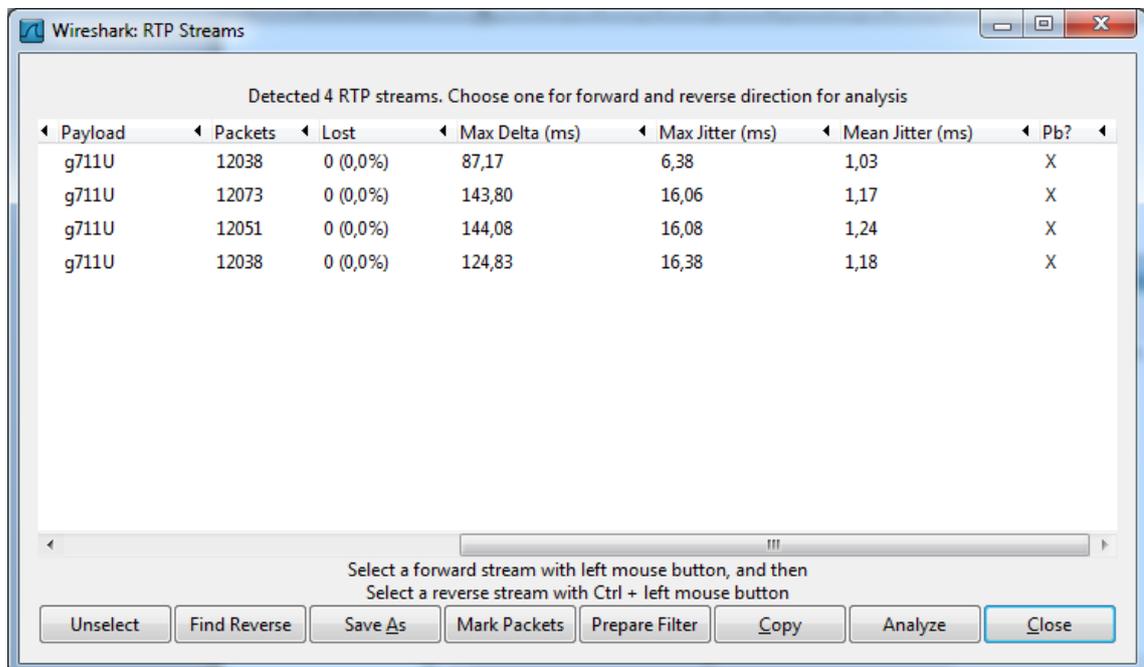
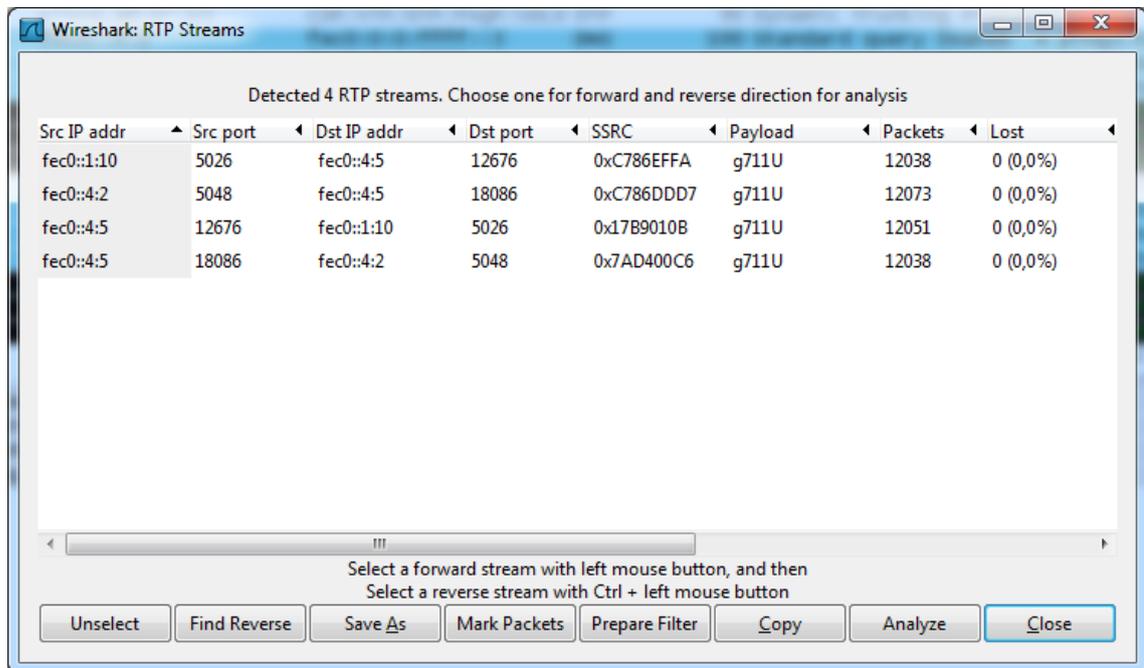
Prueba 1



QR **Prueba 2**



QR **Prueba 3**

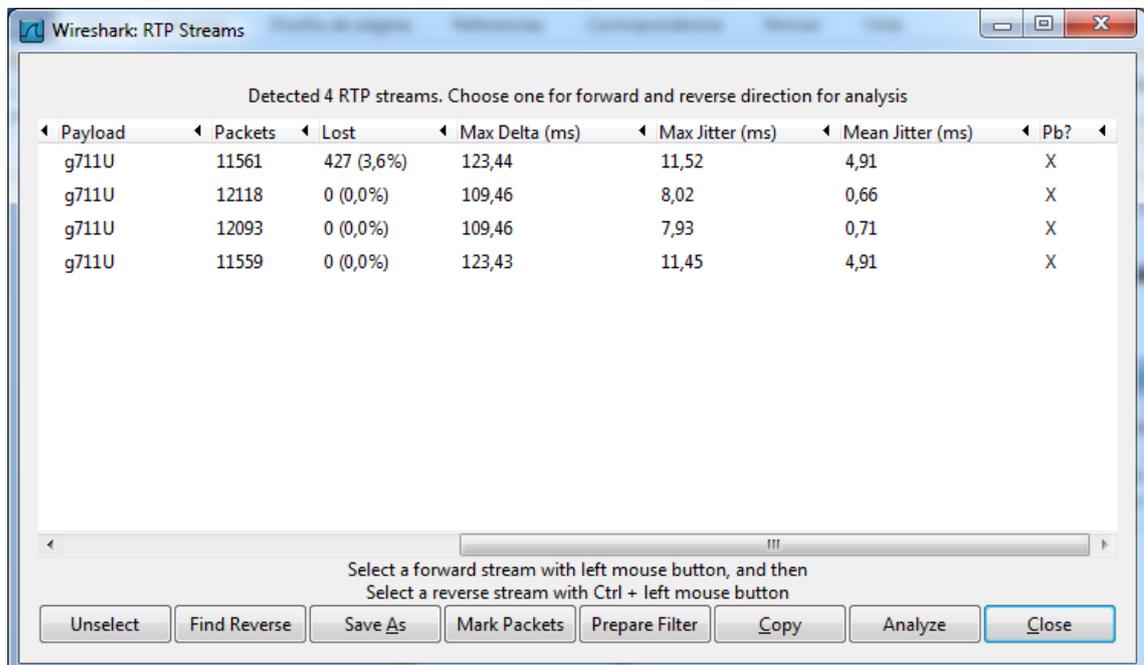
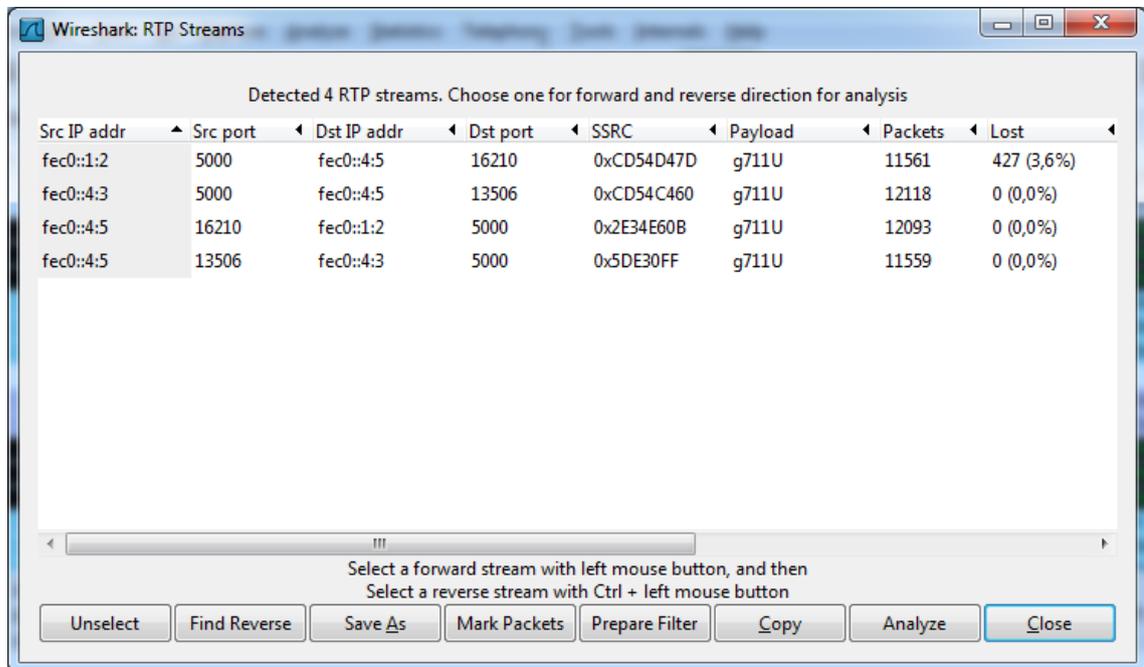


ANEXO 11

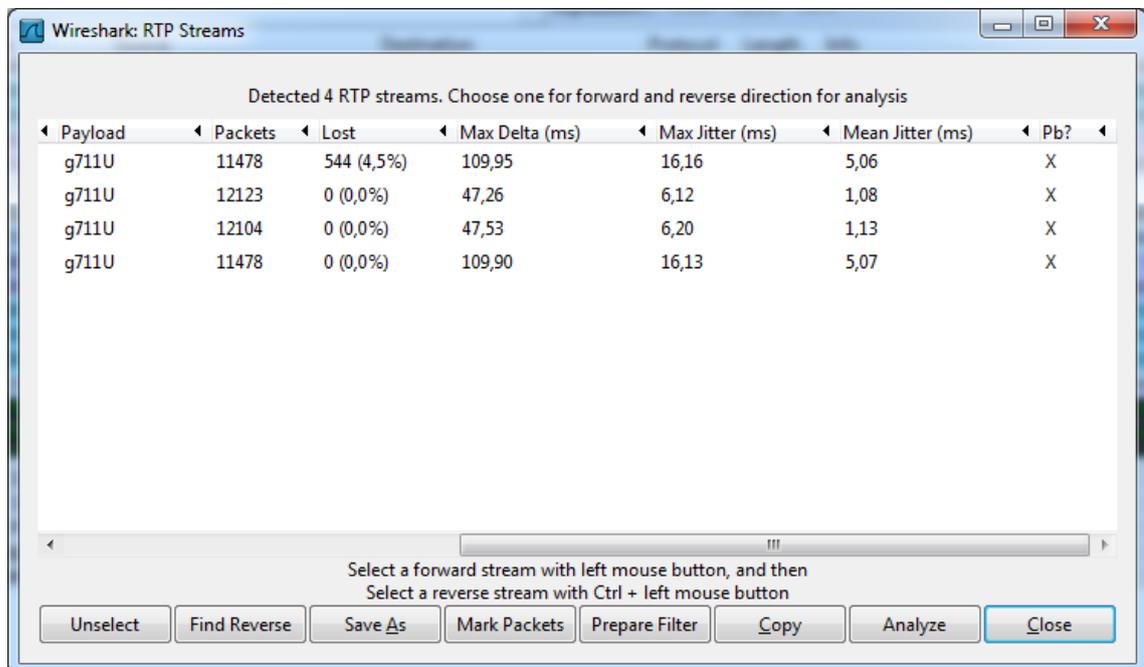
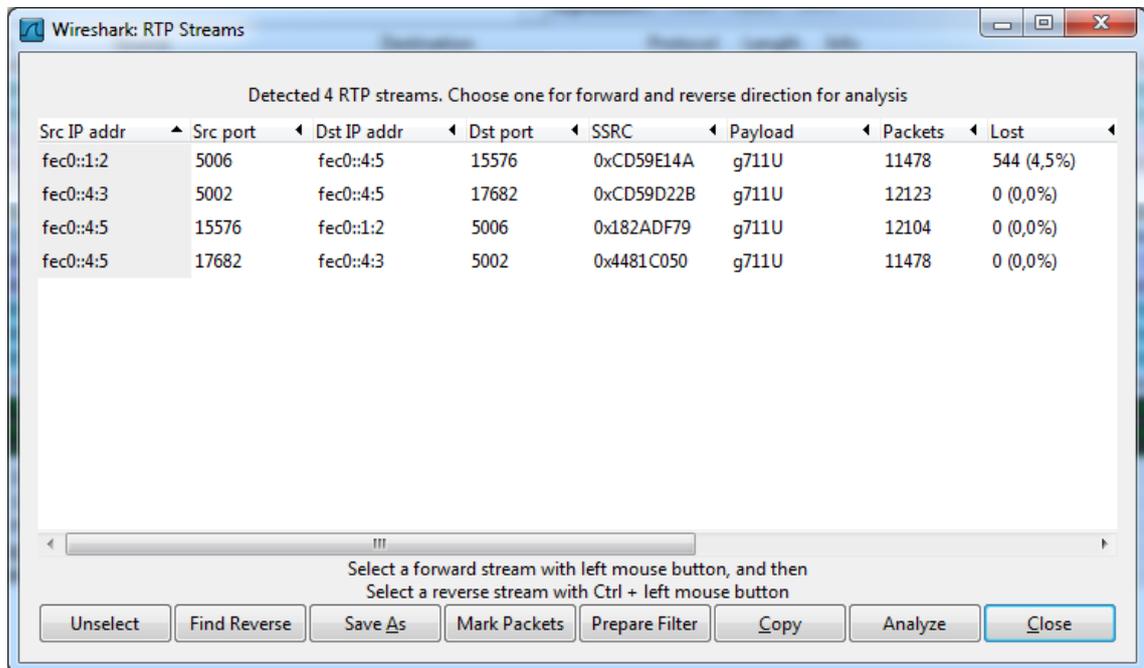
WIRESHARK PRUEBAS GRE

WIRESHARK PRUEBAS GRE

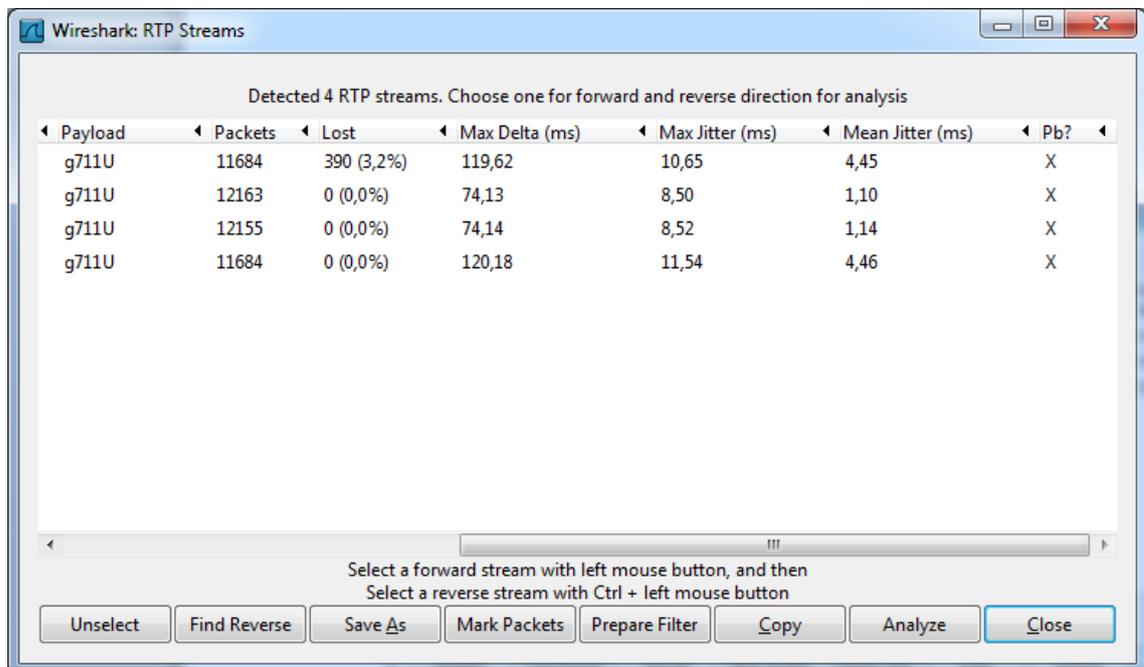
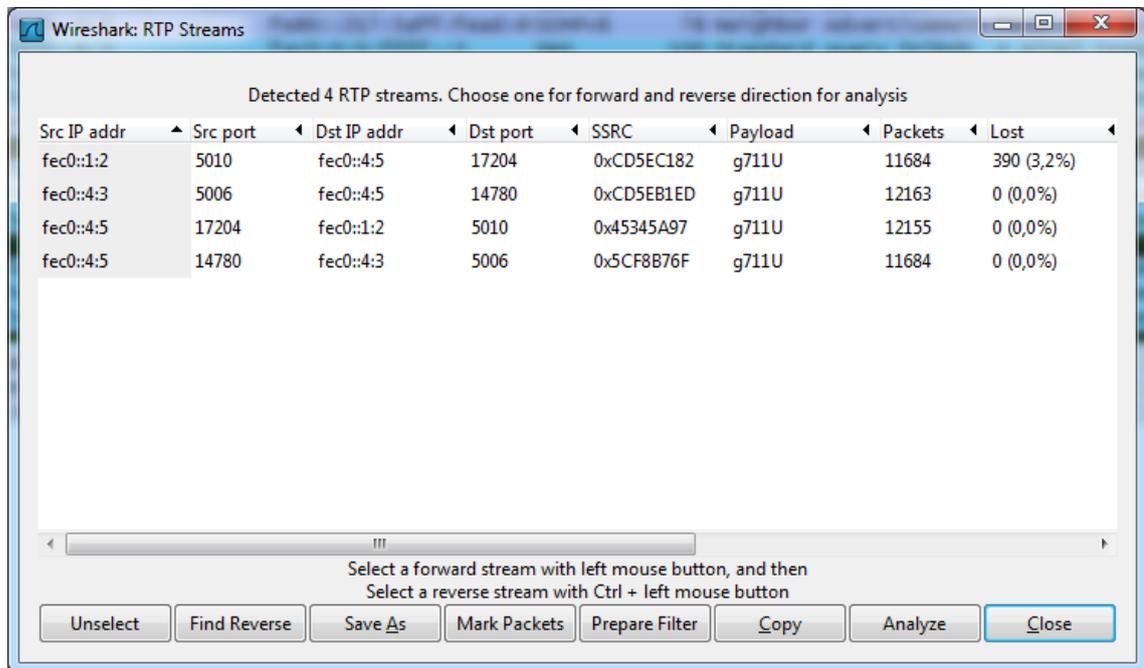
Prueba 1



QR **Prueba 2**



QR **Prueba 3**



ANEXO 12

FORMATO DE ENCUESTA ADMINSITRADORES DE RED

FORMATO ENCUESTA ADMINISTRADORES DE RED

**ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO
ESCUELA DE POSTGRADO Y EDUCACIÓN CONTÍNUA**

ENCUESTA PROYECTO DE TESIS

“Análisis de las Técnicas de Tunneling, para la coexistencia de IPv4 e IPv6 que brinde soporte a tráfico de VoIP”

1. ¿Conoce usted acerca del agotamiento de direcciones IPv4?

SI ____

NO ____

2. ¿Emplea direcciones IPv6 en el desempeño de sus actividades?

SI ____

NO ____

3. ¿Utiliza coexistencia de direcciones IPv4 e IPv6?

SI ____

NO ____

4. De ser afirmativa su respuesta anterior ¿Qué método o métodos conoce?

5. ¿Para medir coexistencia ha implementado Técnicas de Tunneling?

SI ____

NO ____

6. ¿Qué Técnicas de Tunneling conoce?

7. ¿Ha implementado las Técnicas de Tunneling 6to4, ISATAP o GRE?

SI ____

NO ____

8. De ser afirmativa su respuesta anterior evalúe los siguientes Parámetros, bajo las siguientes consideraciones:

➔ **Rendimiento**

☞ Alto

☞ Medio

☞ Bajo

} Experiencia Personal de Administración de Red

Indicador	Indice	6to4	ISATAP	GRE
Rendimiento	Jitter			
	Ancho de banda			
	Latencia			

⇒ **Tiempo**

Rango (Minutos)	Calificación	Abreviatura	Porcentaje %
30 < t	Muy Adecuado	MD	100%
31 < t < 90	Adecuado	A	75%
91 < t < 150	Poco Adecuado	PA	50%
151 < t < 210	Inadecuado	I	25%
t > 211	Nada adecuado	NA	0%

Rango (Minutos)	Calificación	Abreviatura	6to4	ISATAP	GRE
30 < t	Muy Adecuado	MD			
31 < t < 90	Adecuado	A			
91 < t < 150	Poco Adecuado	PA			
151 < t < 210	Inadecuado	I			
t > 211	Nada adecuado	NA			

⇒ **Dificultad**

Puntos	Calificación	Abreviatura	Porcentaje %
81-100	Muy Adecuado	MD	100%
61-80	Adecuado	A	75%
41-60	Poco Adecuado	PA	50%
21-40	Inadecuado	I	25%
0-20	Nada adecuado	NA	0%

Puntos	Calificación	Abreviatura	6to4	ISATAP	GRE
81-100	Muy Adecuado	MD			
61-80	Adecuado	A			
41-60	Poco Adecuado	PA			
21-40	Inadecuado	I			
0-20	Nada adecuado	NA			

⇒ **Parámetros Adicionales**

- ☞ Alto
 - ☞ Medio
 - ☞ Bajo
- } Experiencia Personal de Administración de Red

Parámetros	6to4	ISATAP	GRE
Configuraciones Direcciones IP			
Configuración de MTU			
Configuración keep-alives			

Gracias por su colaboración.

ANEXO 13

NIVEL DE SIGNIFICACIÓN CHI-CUADRADO

NIVEL DE SIGNIFICACIÓN PARA CHI-CUADRADO

Grados de Libertad	ÁREAS DE EXTREMOS SUPERIOR (α)					
	0.25	0.10	0.05	0.025	0.01	0.005
1	1.323	2.706	3.841	5.024	6.635	7.879
2	2.773	4.605	5.991	7.378	9.210	10.597
3	4.108	6.251	7.815	9.348	11.345	12.838
4	5.385	7.779	9.488	11.143	13.277	14.860
5	6.626	9.236	11.071	12.833	15.086	16.750
6	7.841	10.645	12.592	14.449	16.812	18.548
7	9.037	12.017	14.067	16.013	18.475	20.278
8	10.219	13.362	15.507	17.535	20.090	21.955
9	11.389	14.684	16.919	19.023	21.666	23.589
10	12.549	15.987	18.307	20.483	23.209	25.188
11	13.701	17.275	19.675	21.920	24.725	26.757
12	14.845	18.549	21.026	23.337	26.217	28.299
13	15.984	19.812	22.362	24.736	27.688	29.819
14	17.117	21.064	23.685	26.119	29.141	31.319
15	18.245	22.307	24.996	27.488	30.578	32.801
16	19.369	23.542	26.296	28.845	32.000	34.267
17	20.489	24.769	27.587	30.191	33.409	35.718
18	21.605	25.989	28.869	31.526	34.805	37.156
19	22.718	27.204	30.144	32.852	36.191	38.582
20	23.828	28.412	31.410	34.170	37.566	39.997
21	24.935	29.615	32.671	35.479	38.832	41.401
22	26.039	30.813	33.924	36.781	40.289	42.796
23	27.141	32.007	35.172	38.076	41.638	44.181
24	28.241	33.196	36.415	39.364	42.980	45.559
25	29.339	34.382	37.652	40.646	44.314	46.928
26	30.435	35.563	38.885	41.923	45.642	48.290
27	31.528	36.741	40.113	43.194	46.963	49.645
28	32.620	37.916	41.337	44.461	48.278	50.993
29	33.711	39.087	42.557	45.722	49.588	52.336
30	34.800	40.256	43.773	46.979	50.892	53.672