ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

ANÁLISIS DE ESTEGANOGRAFÍA SOBRE EL PROTOCOLO IPv6 COMO ALTERNATIVA PARA UNA COMUNICACIÓN SEGURA DE DATOS

HERMES QUINTERO PINARGOTE

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

MAGISTER EN INTERCONECTIVIDAD DE REDES

RIOBAMBA - ECUADOR

ENERO, 2019

ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

CERTIFICACIÓN:

EL TRIBUNAL DEL TRABAJO DE TITULACIÓN CERTIFICA QUE:

El trabajo de Titulación modalidad Proyectos de Investigación y Desarrollo, denominado: "**ANÁLISIS DE ESTEGANOGRAFÍA SOBRE EL PROTOCOLO IPv6 COMO ALTERNATIVA PARA UNA COMUNICACIÓN SEGURA DE DATOS",** de responsabilidad del señor Hermes Quintero Pinargote, ha sido minuciosamente revisado y se autoriza su presentación:

TRIBUNAL:

Dr. Juan Mario Vargas Guambo, M.Sc. **PRESIDENTE**	**FIRMA**
Ing. Ernesto Pérez Estévez; Mgs **DIRECTOR DE TESIS**	**FIRMA**
Ing. Víctor Hugo Benítez Bravo; Mgs **MIEMBRO DEL TRIBUNAL**	**FIRMA**
Ing. Blanca Faustina Hidalgo Ponce; Mgs **MIEMBRO DEL TRIBUNAL**	**FIRMA**

Riobamba, Enero 2019

DERECHOS INTELECTUALES

Yo, Hermes Quintero Pinargote soy responsable de las ideas, doctrinas y resultados expuestos en el Trabajo de Titulación modalidad Proyectos de Investigación y Desarrollo, y el patrimonio intelectual del mismo pertenece a la Escuela Superior Politécnica de Chimborazo.

_____

HERMES QUINTERO PINARGOTE

No. Cédula 0802269894

DECLARACIÓN DE AUTENTICIDAD

Yo, Hermes Quintero Pinargote, declaro que el presente proyecto de investigación, es de mi autoría y que los resultados del mismo son auténticos y originales. Los textos constantes en el documento que provienen de otras fuentes están debidamente citados y referenciados.

Como autor, asumo la responsabilidad legal y académica de los contenidos de este Trabajo de Titulación de Maestría.

_____

HERMES QUINTERO PINARGOTE

No. Cédula 0802269894

DEDICATORIA

Dedico este trabajo a Dios por acompañarme en cada momento de mi vida, por brindarme esa fortaleza y sabiduría necesaria para tomar decisiones y alcanzar mis metas. También y con mucho cariño a las maravillosas personas que conforman mi familia, quienes son el incentivo de mi vida y el sostén incondicional durante todo este proceso con su tiempo, paciencia y confianza.

Hermes Quintero Pinargote

AGRADECIMIENTO

Sin dudarlo y poniendo toda mi fe, a Dios porque siempre me brinda sabiduría y fortaleza por medio de la práctica.

A mi esposa, hija y familiares, por su tiempo y comprensión.

A la Escuela Superior Politécnica de Chimborazo, por haberme dado la oportunidad de cursar esta maestría y haberme mostrado la senda que contribuyó a mejorar como profesional.

A los docentes, en especial a quienes acompañaron esta investigación, Ing. Ernesto Pérez, Ing. Víctor Hugo Benítez e Ing. Blanca Hidalgo.

CONTENIDO

INDICE DE ABREVIATURAS

ACK	ACKNOWLEDGEMENT
APIPA	AUTOMATIC PRIVATE IP ADDRESSING
ARCNet	ATTACHED RESOURCE COMPUTER NETWORK
ATM	ASYNCHRONOUS TRANSFER MODE
CAPEX	CAPITAL EXPENDITURES
CGN	CARRIER GRADE NAT
CIDR	CLASSLESS INTER-DOMAIN ROUTING
CPE	CUSTOMER PREMISES EQUIPEMENT
DAD	DUPLICATE ADDRESS DETECTION
DCT	DISCRETE COSINE TRANSFORM
DHCP	DYNAMIC HOST CONFIGURATION PROTOCOL
DS	SERVICIOS DIFERENCIADOS.
ECN	NOTIFICACIÓN DE CONGESTIÓN EXPLICITA.
ESP	ENCAPSULATING SECURITY PAYLOAD
ESPE	ESCUELA SUPERIOR POLITÉCNICA DEL EJERCITO
ESPOCH	ESCUELA POLITÉCNICA DEL CHIMBORAZO
ESPOL	ESCUELA POLITÉCNICA DEL LITORAL
FDDI	FIBER DISTRIBUTED DATA INTERFACE
HTTP	HYPERTEXT TRANSFER PROTOCOL
IANA	AUTORIDAD DE NOMBRES Y REGISTROS DE INTERNET
ICMP	INTERNET CONTROL MESSAGE PROTOCOL
ICMPv6	INTERNET CONTROL MESSAGE PROTOCOL VERSION 6
ICV	INTEGRITY VALUE CHECK
IEEE	INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS
IETF	INTERNET ENGINEERING TASK FORCE
IoT	INTERNET OF THINGS
IP	PROTOCOLO DE INTERNET
IHL	INTERNET HEADER LENGTH
IPv4	PROTOCOLO DE INTERNET VERSIÓN 4
IPv6	PROTOCOLO DE INTERNET VERSIÓN 6
ISP	INTERNET STREAM PROTOCOL
LACNIC	LATIN AMERICAN AND CARIBBEAN NETWORK INFORMATION CENTER
LBE	LOW BIT ENCODING
LSB	LEAST SIGNIFICANT BIT
MAC	MEDIA ACCESS CONTROL

MINTEL	MINISTERIO DE TELECOMUNICACIONES
MSE	MEAN-SQUARE ERROR
MTU	UNIDAD DE TRANSMISIÓN MÁXIMA.
NAT	NETWORK ADDRESS TRANSLATION
NIS	NETWORK INFORMATION SERVICE
OFDM	ORTHOGONAL FREQUENCY DIVISION MULTIPLE
ORCHID	OVERLAY ROUTEABLE CRYPTOGRAPHIC HASH IDENTIFIERS
OSI	OPEN SYSTEM INTERCONNECTION
OUI	ORGANIZATIONALLY UNIQUE IDENTIFIER
PDA	PERSONAL DIGITAL ASSISTANT
PDU	PROTOCOL DATA UNIT
PGP.4	PRETTY GOOD PRIVACY
PIB	PRODUCTO INTERNO BRUTO
PPP	POINT-TO-POINT PROTOCOL
PSNR	PEAK SIGNAL-TO-NOISE RATIO
RFC	REQUEST FOR COMMENTS
RIR	REGISTRO REGIONAL DE INTERNET
RSIP	REALM-SPECIFIC IP
SNAP	SUBNETWORK ACCESS PROTOCOL
SIP	SESSION INITIATION PROTOCOL
SPI	SECURITY PARAMENTERS INDEX
SSL	SECURE SOCKETS LAYER
TCP	TRANSMISSION CONTROL PROTOCOL
TOR	THE ONION ROUTER
UDLA	UNIVERSIDAD DE LAS AMÉRICAS
UDP	USER DATAGRAM PROTOCOL
UTA	UNIVERSIDAD TÉCNICA DE AMBATO
VLAN	VIRTUAL LOCAL AREA NETWORK

LISTA DE TABLAS

LISTA DE FIGURAS

LISTA DE GRÁFICOS

LISTA DE ANEXOS

RESUMEN

El presente trabajo de investigación tuvo como objetivo diseñar un mecanismo esteganográfico en el protocolo IPv6. Se realizó un análisis de su arquitectura y características para establecer una comunicación cifrada, hasta llegar al despliegue de dos escenarios de pruebas donde se implementó el mecanismo y se validó su funcionalidad. Se empleó el tipo de investigación experimental y aplicativa; por medio de herramientas de simulación como GNS3, VIRTUALBOX y KALI-LINUX con la aplicación WIRESHARK; se implementó dos escenarios que demostraron el uso y aplicación de los protocolos DNS y SIP usando IPv6 en la capa de red. Se aprovechó dos características que posee el protocolo; la capacidad de autoconfiguración de la porción de ID de interfaz (aleatoria de 64 bits y EUI-64) con una máscara /64 y la gran cantidad de direcciones disponibles. Luego se diseñó un estegograma en la dirección global unicast de los emisores, que facilitó la incrustación de mensajes ocultos entre dos o más nodos. Para la evaluación del mecanismo se consideraron los parámetros de capacidad esteganográfica, probabilidad de detectabilidad, coste esteganográfico y robustez. La prueba de hipótesis de esta investigación consideró la probabilidad de detectabilidad como variable adecuada sobre la que se basó el criterio de decisión. Se utilizó la distribución estadística T-Student para la demostración de la hipótesis planteada y se concluyó que "existe evidencia estadística que la proporción de direcciones IPv6 utilizadas en el mecanismo de esteganografía tienen una probabilidad de detección menor al 50% con un nivel de significancia del 5%. Finalmente se presentó un mecanismo esteganográfico que utilizó la técnica de sustitución, basado en el paradigma "*Modificar con precaución*" en las direcciones IPv6 con una capacidad máxima de 1792 caracteres usando 256 direcciones.

Palabras clave: <TECNOLOGÍA Y CIENCIAS DE LA INGENIERÍA>, <REDES>, <PROTOCOLO IPv6>, <ESTEGANOGRAFÍA>, <TÉCNICAS ESTEGANOGRÁFICAS>, <ESTEGANOGRAMA>, <CAPACIDAD ESTEGANOGRÁFICA>.

THESIS ABSTRACT

The present research work had as objective to design a stenographic mechanism in the IPv6 protocol. An analysis of its architecture and its characteristics was carried out to stablish an encrypted communication, until reach to the deployment of two tests scenarios where the mechanism was implemented and its functionality was validated. An experimental and applicative kind of researching was used; through simulation tools like GNS3, VIRTUALBOX and KALI-LINUX with the application WIRESHARK; two scenarios which proved the use and application of the DNS and SIP protocols using IPV6 in the network layer were implemented. It was seized two of the characteristics that the protocol has; the auto configuration capacity of the portion of the interface ID (aleatory of 64 bits and EUI-64) with a mask /64 and the great amount of possible directions. Then a steganogram in the unicast global direction of the emitters was designed, which made it easy the incrustation of hidden messages between two or more nodes. For the evaluation of the mechanism the stenographic capacity parameters, the detectability probability, the stenographic cost and sturdiness were considered. The hypothesis test of this researching considered the detectability probability like a suitable variable, on which, the decision criteria was based. It was used the statistic distribution T-student for the demonstration of the hypothesis raised and it was concluded that "there is statistic evidence that the proportion of directions IPv6 used in the steganogram mechanism have a detection probability less than 50% with a level of significance of the 5%. Finally, it was presented a stenographic mechanism, which used the substitution technique based on the paradigm "Modify with caution" in the directions IPv6 with a maximum capacity of 1792 characters using 256 directions.

Key words: <TECHNOLOGY AND ENGINEERING SCIENCES>, <NETWORKS>, <IPV6 PROTOCOL>, < STEGANOGRAPHY>, < STEGANOGRAPHY TECHNIQUES>, < STEGANOGRAM>, <STEGANOGRAPHIC CAPACITY>.

CAPÍTULO I

1. INTRODUCCIÓN

1.1. Antecedentes

En la actualidad se evidencia como a través de la globalización, el mundo entero se encuentra interconectado y acortando distancias usando tecnología de vanguardia. El internet se ha convertido en el pilar de este principio, en donde se interconectan millones de dispositivos y no es exclusivo de las computadoras, así lo explica (FUENTES, 2004) en su artículo publicado.

Para lograr que estos dispositivos se comuniquen y puedan transmitir información se fundamentan en el protocolo de internet (IP). El protocolo IPv4 utiliza direcciones de 32 bits para establecer la comunicación entre dos dispositivos en la red. Este fue pensado con cuatro mil millones de direcciones en sus inicios, ya que eran pocos ordenadores por la década de los 70. Además, se confió en estas direcciones serían las suficientes para un futuro.

Al iniciar la década de los 90, la industria e investigadores comenzaron a tomar medidas en cuanto al consumo rápido y excesivo de las direcciones IPv4, razón por lo cual se estaban agotando. Según (MEULEN, 2015), hoy se tiene alrededor de seis mil millones de dispositivos y una proyección para el 2020 de 30000 millones de dispositivos conectados globalmente de acuerdo a la firma (EMC, 2014).

Frente a tal crecimiento exponencial, como medida de solución, se desarrolló el protocolo de siguiente generación IPv6. Dicho protocolo contiene 128 bits para sus direcciones, es decir, 340,282,366,920,938,463,463,374,607,431,768,211,456 direcciones disponibles para su uso. Esto significa que existen aproximadamente 6.67 * 10^27 direcciones IPv6 por metro cuadrado disponibles para todo el planeta Tierra (KAPLAN, 2016). Suficientes para mitigar el problema de agotamiento durante los siguientes años.

En el Ecuador, de acuerdo a los datos presentados por el MINTEL (2010), 3 de cada 10 ecuatorianos usa el internet, de los cuales el 40% lo hace para educación y aprendizaje; el 27,2% para obtener información y el 22,4% para comunicarse (ARCOTEL, 2015). En cuanto a la implementación de IPv6 se tiene 17,14% desplegado (GOOGLE, s.f.), aunque con considerables de latencia o fiabilidad relacionados con la conexión a sitios web con IPv6 habilitados. De acuerdo a estas estadísticas, hay un alto porcentaje de usuarios que acceden a internet y lo hacen para comunicarse. También la adopción de IPv6 está en crecimiento y avanza.

Universidades como la ESPOCH, UTPL y Nacional de Loja tienen implementado IPv6; al igual que organizaciones como CEDIA, NAP.EC y ASEXAT S.A. (LACNIC, http://portalipv6.lacnic.net/, 2015). Además, desde el 2012 el ministro de Telecomunicaciones y Sociedad de la Información, Jaime Guerrero, en una entrevista, dio a conocer que el sector público del Ecuador debe implementar la tecnología de IPv6 (EL TELÉGRAFO, 2012).

De acuerdo al estudio económico presentado por (MEJÍA, 2012), demuestra que el incremento en la penetración del acceso a Internet genera crecimiento en el PIB y por otra parte el acceso a Internet es considerado como un instrumento habilitante para el ejercicio de derechos humanos fundamentales como la libertad de expresión, de ahí que el plan de gobierno de muchos países considera alguna medida para lograr la masificación del Internet y cerrar la brecha digital.

Como derecho y necesidad, la comunicación para las personas se ha convertido en un tema de interés y preocupación para muchos. El monitoreo y la vigilancia es algo común en las redes. A pesar que se haya implementado muchos mecanismos como medidas de protección para la privacidad de los usuarios. Muchas de estas herramientas han fracasado en su intento.

Organismos gubernamentales, proveedores, agencias de inteligencia o personas con intereses personales se encuentran enfocados en observar el comportamiento de los usuarios en la red. Obtienen información de actividades comunes en redes sociales, historial de compras o consultas, accesos a bancos, tipos de contenidos o archivos a los que se accede, entre otras. El fin de tener esta información no está clarificado, pero se obtiene una gran invasión a nuestra privacidad y seguimiento de nuestras actividades.

Una de las primeras voces que dio relevancia internacional a la importancia de mantener enlaces seguros en las comunicaciones fue Julián Assange, uno de los fundadores de WikiLeaks, una organización que filtra documentos que demuestran el comportamiento no ético de gobiernos y organismos (EL COMERCIO, 2012). Para garantizar el anonimato de las fuentes que entregan los

documentos se utiliza TOR, pero también otros programas similares, como Open SSL, Freenet y PGP.4. Assange se encuentra bajo asilo en la embajada de Ecuador en Londres.

Para evitar que toda esta información sea utilizada sin nuestro conocimiento y en nuestro perjuicio (por ejemplo, detenido en un aeropuerto por participar en una manifestación por los derechos de los homosexuales, participación que hemos subido a las redes sociales), muchos, cada vez más usuarios de la red, recurren a sistemas de comunicaciones anónimos, sea para enviar o recibir correos, para realizar búsquedas o para hacer compras.

Periodistas disidentes, mujeres sometidas a malos tratos, familias que buscan proteger a sus hijos, activistas políticos. El espionaje sin duda revela que nuestros movimientos por la red están bajo la lupa y cada huella es almacenada para ser utilizada de alguna manera.

1.2. Formulación del problema

¿El uso de la esteganografía sobre el protocolo IPv6 ofrecerá un mecanismo de comunicación segura entre partes?

1.3. Preguntas directrices

- ¿Cuáles son los mecanismos de esteganografía existentes usando el protocolo IPv6?
- ¿Cuál es el funcionamiento y uso del protocolo IPv6?
- ¿Cómo se aprovecharía la esteganografía usando IPv6?

1.4. Justificación del problema

En la actualidad nuestras comunicaciones se han trasladado a un entorno digital y la seguridad de ellas se ha convertido en un tema de mucho interés debido a los diferentes casos publicados y conocidos a través de la prensa. Muchas personas han sido víctimas de robos, estafas, suplantaciones de identidad y extorsiones debido al robo de información por medio de la intercepción del tráfico y

el monitoreo de sus conversaciones a través de la red. Además, muchos usuarios no están conformes que sus comunicaciones sean revisadas o utilizadas para fines diferentes al que ellos la usan. Esto vulnera a derechos fundamentales como la privacidad e intimidad.

Como solución se implementa técnicas de encriptación para mitigar estos eventos y aunque es un método eficiente, al utilizarla, despierta el interés de terceros por descifrar el contenido. Además, que este está disponible a la vista de todos.

Como alternativa a este método se tiene a la esteganografía, la cual tiene como fin ocultar un mensaje en un medio sin que se note su presencia y el receptor pueda entenderlo. La esteganografía es un recurso muy válido como mecanismo de seguridad en las comunicaciones. Es posible introducir mensajes en textos, archivos multimedia y en protocolos. La mayoría de sus estudios e investigaciones se enfocan al uso de imágenes, audio y texto (79,4 %) y muy poco en los protocolos de internet (1,3%) (JHONSON & SALLE, 2008).

Con el agotamiento de direcciones IPv4 y la creciente implementación de IPv6 en muchos sectores e instituciones del Ecuador, la esteganografía dentro del protocolo ofrece la oportunidad de aprovechar un mecanismo que brinde confianza a los usuarios al establecer una comunicación segura y privada, al enviar mensajes que no quieren que sean leídos por terceros.

Con esta investigación se espera analizar la posibilidad de enviar mensajes ocultos usando esteganografía en el protocolo IPv6 para ofrecer seguridad a la comunicación entre dos partes, considerando que la mayoría de las investigaciones se orientan al uso de técnicas basadas en imágenes, audio o archivos. Además de estar dentro de las líneas de investigación propuestas por la ESPOCH.

1.5. Objetivos de la investigación

1.5.1. Objetivo general

Analizar el uso de esteganografía en el protocolo IPv6 usando mensajes ocultos para una comunicación segura.

1.5.2. Objetivos específicos

- Analizar la arquitectura del protocolo IPv6 para conocer su funcionamiento, riesgos y posibilidades para el uso de un canal encubierto.
- Diseñar un mecanismo esteganográfico en el protocolo IPv6 usando un canal encubierto para enviar mensajes ocultos.
- Demostrar en dos escenarios básicos el uso de esteganografía en el protocolo IPv6 para establecer una comunicación segura.

1.6. Hipótesis

El uso de esteganografía en el protocolo IPv6 usando mensajes ocultos es una alternativa para una comunicación segura.

CAPÍTULO II

2. MARCO TEÓRICO

2.1. Antecedentes del problema

La esteganografía es el mecanismo por el cual se oculta un mensaje dentro de imágenes, audio, archivos u otro tipo de medio como los protocolos de red (FRIDRICH, Steganography in Digital Media, 2010). Las investigaciones y trabajos que se exponen y analizan a continuación presentan los avances realizados con respecto al uso de la esteganografía en las capas del modelo OSI y de la arquitectura TCP/IP, los protocolos en los cuales se han aplicado y la forma en cómo se lo ha explotado; dando el punto de partida para esta investigación.

De acuerdo a (LUBACCZ, MAZURCZYK, & SZCZYPIORSKI, 2014) en su artículo de investigación, refieren tres términos asociados a la esteganografía: anonimato, marcas de derecho de autor (watermarking) y canales secretos. Además, establecen que en una comunicación de red hay tres funcionalidades básicas (servicios, transporte y flujo de información) y a cada funcionalidad se le puede explotar para usar un método esteganográfico como lo detalla la tabla 1-2 como ejemplo.

Tabla 1-2: Funciones de los protocolos del modelo OSI usadas para esteganografía.

Capa del modelo OSI	**Funciones usadas para esteganografía**	**Ejemplo:**
Aplicación	Forma de comunicación: • Consulta-Respuesta • Transferencia de archivos	Http Header Manipulation
Presentación		LSB of voice samples modification for VoIP.
Sesión		SIP Header Manipulation
Transporte	Forma de los mensajes: • Fragmentación.	Intencional TCP segments retransmissions
Red		Packets sorting and IP Header manipulation

	• Segmentación.	
Enlace	Características físicas del medio de comunicación: • Capacidad limitada. • Retardos. • Errores.	Ethernet frame´s padding for different upper layer´s protocols
Física		Padding of OFDM symbols for WLAN.

Realizado por: Quintero Hermes, 2019.

En la investigación realizada por (MILEVA & PANAJOTOV, 2014) también se expone el uso de canales secretos existentes en el stack de TCP/IP, identificándolos por capa y el protocolo en que inciden.

Otra forma de analizar la esteganografía en medios modernos es a través del estudio de canales secretos o encubiertos. Prueba de ello lo demuestra el trabajo realizado por (KUNDUR & AHSON, 2003), identificando dos canales encubiertos existentes en la capa de red de internet y en el análisis del ancho de banda disponible para la comunicación, usando la cabecera del paquete IPv4 en los campos de fragmentación y en el número de secuencia. En una investigación más actual (RAMIREZ, 2014) expone el uso de otros campos de la cabecera del protocolo IPv4 para el mismo fin.

Un enfoque similar sobre el aprovechamiento de canales secretos lo realizan (ZHOU & ZHANG, 2006) vulnerando las medidas de seguridad implementadas en los sistemas para intercambiar información valiéndose del uso del ping e ICMP (protocolos válidos y comunes en las políticas de seguridad de los administradores) sobre los protocolos IPv4 e IPv6. También (MILLER, 2008) lo demuestra, en su tesis doctoral, la existencia de un canal secreto inherente al protocolo IPv6.

Del mismo modo (DHAMADE & KRUNAL, 2014) afirman que la esteganografía en la red es posible usando canales secretos y los clasifican como almacenamiento, de tiempo o híbridos. En su análisis muestran la capacidad esteganográfica en los protocolos TCP, UDP e IP. Con respecto al protocolo IP se usan los resultados del trabajo de (KUNDUR & AHSON, 2003).

Finalmente, (RODRIGUEZ, 2016) afirma que "En el Ecuador la técnica de esteganografía es muy poco conocida y casi no presenta información referente al tema, lo cual no implica que no sea utilizada sin conocer de su existencia misma". En su estudio se analizan diferentes técnicas que usan los medios digitales y sugiere que las más apropiadas son el método semántico para texto, Spread para imagen, Spread Spectrum para audio, LSB para video y TCP para la red. En este estudio se refleja, que en

nuestro país, solo se han analizado en forma general algunas técnicas esteganográficas y no se ha propuesto la situación del aprovechamiento en el protocolo IPv6.

2.2. Bases teóricas

2.2.1. IPv6

2.2.1.1. Introducción

El protocolo IPv4 fue publicado en 1981 en el (RFC 791) y desde esa fecha hasta la actualidad no ha tenido mayores cambios en su arquitectura. Permite tener un conjunto de 4,2 billones de direcciones, las cuales están distribuidas en 4 clases (A, B, C y D) y basadas en sus bits de alto orden. Posee una cabecera de 32 bytes de longitud sin opciones y varios campos de opción en su cabecera como se ilustra en la **Figura 1-2**.

<table>
<tr><td>Versión
4 Bits</td><td>IHL
4 Bits</td><td>Tipo de Servicio
8 Bits</td><td colspan="2">Longitud Total
16 Bits</td></tr>
<tr><td colspan="3">Identificación
16 Bits</td><td>Indica-
Dores
3 Bits</td><td>Desplazamiento del Fragmento
13 Bits</td></tr>
<tr><td colspan="2">Tiempo de vida
4 Bits</td><td>Protocolo
8 Bits</td><td colspan="2">Suma de comprobación de la cabecera
16 Bits</td></tr>
<tr><td colspan="5">Dirección origen
32 Bits</td></tr>
<tr><td colspan="5">Dirección destino
32 Bits</td></tr>
<tr><td colspan="5">Opciones + Relleno
32 Bits</td></tr>
</table>

Figura 1-2: Cabecera IPv4

Fuente. RFC 791

A pesar que posee más de 30 años en uso, en su transcurso se han ido desarrollando problemas que atentan contra el mismo (LOSHIN, 2004) (DAVIES, 2012). Uno de ellos son el conjunto de direcciones disponibles para su uso global. Un objetivo de usar IPv4 era tener una dirección única y accesible globalmente en cada dispositivo. Con el tiempo, existió un crecimiento exponencial de dispositivos que tendrían asociada una dirección IPv4 para su funcionamiento, servicio y/o conectividad; una creciente demanda de direcciones en los sistemas de comunicaciones móviles a partir de la tercera generación.

Todos estos se integran con rapidez al uso de una red y agotan direcciones dando a relucir las falencias de este protocolo. El 3 de febrero del 2011 la IANA asignó el último bloque de direcciones disponibles a los RIR´s (ARIN, 2011) y (LACNIC, http://www.lacnic.net, 2014) anunció que no hay más direcciones IPv4 para América Latina y el Caribe. Por esta razón, la IETF propuso iniciativas con el objetivo de extender la vida útil de IPv4 creando medidas como el racionamiento, reciclaje y reemplazo de direcciones para aprovechar el espacio disponible.

En redes muy grandes con muchos hosts y donde sus usuarios iniciaban sesiones por un tiempo limitado, se hizo vital gestionar y asignar direcciones en forma fácil y rápida. Para este problema se desarrolló DHCP (RFC 2131), el cual permite arrendar direcciones IP por un tiempo determinado y luego devolverlas para ser reutilizadas.

Para el enrutamiento IP se interpretaba las direcciones con clase, considerando el primer octeto como identificador de la red y el resto como el identificador único para los nodos de esa red. El enrutamiento entre dominios sin clase (CIDR) se constituyó a principios de los 90 para mitigar el problema de la desalineación entre la estructura de clases que tenía Internet.

Con esto se permitió la agregación de las direcciones de clase C para proporcionar asignaciones variables de direcciones de red, poniendo más direcciones IPv4 a disposición. El problema con esto radicó en el aumento de más y más redes generando grandes listas de enrutamiento y haciendo compleja dicha tarea. Para 1999 se pasó de una tabla de enrutamiento de unas 60000 entradas a una de 110000 a 120000 para el 2002. Este crecimiento tomó el interés de expertos y en el (RFC 1519) se incluye una discusión del impacto que podría tener CIDR en las tablas de enrutamiento no predeterminadas.

Otro mecanismo para atenuar el agotamiento de direcciones públicas es NAT (RFC 1631) (DAVIES, 2012), el cual permite que una organización utilice un gran número de direcciones privadas para su organización y haga uso de una o pocas direcciones públicas para comunicarse a Internet. Los enrutadores de la organización pueden encaminar paquetes dentro de la red privada y aquellos con

destino a la Internet se pasan a través de un traductor de direcciones que actúa en nombre de los sistemas internos al interactuar con los hosts de Internet siguiendo las reglas de enrutamiento establecidas por el administrador.

A pesar que NAT se ha posicionado como una herramienta que salvaguarda el espacio de direcciones IP y brinda seguridad para los administradores, también plantea dificultades como la interoperabilidad de extremo a extremo, incorrecto funcionamiento de aplicaciones del tipo end-to-end, problemas de re direccionamiento de servicios que usan puertos conocidos dentro de una red privada y la configuración predeterminada de equipos o dispositivos que usan el principio de plug-and-play afectando a servicios y servidores.

IPv4 posee deficiencias relacionados con la administración de la red. Al basarse en una arquitectura de red conmutada por paquetes, requiere de protocolos de enrutamiento para que incluyan nociones de rutas preferenciales basadas en costos, así como la necesidad de indagar sobre características de las rutas disponibles (latencia, rendimiento y confiabilidad). Todas estas basadas en las opciones de cabecera IP.

Una cabecera IP sin opciones tiene 5 bytes y los enrutadores las procesan más fácil, lo que no sucede si posee opciones, al ser así, a esos paquetes los trata como excepciones, dejándolos a un lado para atenderlos cuando lo crea conveniente. Esto afecta a aplicaciones sensibles como audio, video o de tiempo real (DAVIES, 2012).

Al observar estos problemas, muchas organizaciones e ingenieros de Internet han centrado sus esfuerzos en proponer tecnologías alternativas que alarguen la existencia y funcionamiento de IPv4, como RSIP, ISP o CGN. Otros proponen el desarrollo de un nuevo protocolo que reemplace a su predecesor y permita una red más robusta, escalable, con soporte a nuevas aplicaciones sin afectar a la infraestructura de red y dé solución los problemas detallados (Direcciones abundantes, escalabilidad de enrutamiento, no haga uso de NAT y soporte de extremo a extremo más sencillo) como es IPv6.

2.2.1.2. Características del protocolo IPv6

IPv6 se encuentra definido en el RFC 2460. Es una evolución de IPv4, pero no es compatible con él. Para comenzar su estudio en su RFC se detallan algunos términos necesarios para su dominio, los cuales se detallan en la **Tabla 2-2**.

Tabla 2-2: Terminología del Protocolo IPv6

Término	Definición
Nodo	Dispositivo que implementa IPv6. Incluye a enrutadores y hosts.
Enrutador	Nodo que envía paquetes IPv6 no explícitamente dirigido a sí mismo. Por lo general, anuncia su presencia y la información de configuración del host.
Host	Cualquier nodo que no es un enrutador. Se considera la fuente y destino del tráfico IPv6.
Protocolos de capa superior	Protocolo que usa IPv6 como su transporte. Como ejemplo TCP o UDP.
Link	Medio sobre el cual los nodos pueden comunicarse en la capa de enlace.
Vecinos (Neighbors)	Nodos conectados al mismo enlace. Estos pueden resolver las direcciones de capa de enlace, detectar y controlar la accesibilidad a los vecinos.
Interfaz	Adhesión de un nodo a un enlace.
Dirección	Identificador IPv6 para una o varias interfaces.
Paquete	Cabecera IPv6 más su PAYLOAD.
MTU	Unidad de transmisión máxima. El número de bytes del paquete IPv6 más grande que se puede enviar a un enlace.
Ruta MTU	El paquete IPv6 de tamaño máximo que se puede enviar sin realizar la fragmentación del host entre una fuente y un destino a través de una ruta en una red IPv6.

Realizado por: Quintero Hermes, 2019

Se considera como un protocolo más robusto y escalable para manejar las necesidades actuales y futuras de las comunicaciones de los usuarios en Internet. Tiene cambios en varias áreas importantes que se detallan en la **Tabla 3-2** a continuación:

Tabla 3-2: Características del Protocolo IPv6

Punto importante	Características
Nuevo formato de encabezado	• Diseñado para minimizar el procesamiento de paquetes, lo hace más rápida y eficiente en enrutadores intermedios. • Mejora el enrutamiento. • Contiene menos información (8 campos) de los cuales dos son direcciones de origen y destino. • La fragmentación se realiza solo en los hosts. • El campo **flow label** facilita el soporte de calidad de servicio. • Los campos nuevos definen como se maneja y se identifica el tráfico (DS y ECN).
Gran espacio de direcciones	• Se tienen 2^{128} direcciones disponibles. Se podría tener $6{,}65x10^{28}$ direcciones por metro cuadrado.

	• Al tener un gran número de direcciones globales elimina el uso de NAT o servidores proxies. • Se soluciona el agotamiento de direcciones que padece IPv4. • Las distribuciones de direcciones públicas se hacen en función de las necesidades regionales de conectividad. • A partir del 2003, los RIR están asignando prefijos de red **/32** a las organizaciones que los solicitan.
Configuración de direcciones Stateless y Stateful	• Configuraciones automáticas y en segundos de direcciones de enlace (link local) para la comunicación con nodos vecinos. • Sus direcciones son únicas y relevantes. Sus ámbitos están bien definidos y no se confundirán con otras. Se clasifica y optimiza el tráfico. • Las reglas de selección de direcciones son autoconfigurables, dejando múltiples infraestructuras de direccionamiento para una organización. • Los hosts en el mismo enlace pueden configurarse y comunicarse sin una configuración manual ni uso de un enrutador. • Se reducen las tablas de enrutamiento en los enrutadores de una organización y los backbones de Internet.
Posibilidad de comunicación de extremo a extremo	• Con la disponibilidad de muchas direcciones y eliminación de NAT, los paquetes no se modifican en su tránsito ayudando potencialmente a la telefonía peer-to-peer, video y tecnologías de colaboración en tiempo real. • La comunicación basada en pares y la conectividad ad-hoc se mejoran. • Acceso directo por los usuarios a los hosts sin uso de intermediarios. • Protege los paquetes de extremo a extremo al usar un solo espacio de direcciones globales.
Soporte de encabezado IPsec	• Es un requisito dentro del protocolo para brindar protección y promover la interoperabilidad. • Mejor soporte para una entrega priorizada.
Nuevo protocolo para la interacción de nodos vecinos	• El protocolo Neighbor Discovery (NDP) usa una serie de mensajes tipo IMCPv6 para gestionar la interacción de nodos vecinos (RFC 2461). • Reemplaza al protocolo de resolución de direcciones ARP. • Entre sus beneficios tenemos: descubrir la presencia de cada uno, encontrar enrutadores y mantener la información de accesibilidad.
Extensibilidad	• Añade características de extensión después de la cabecera IPv6.

Realizado por: Quintero Hermes, 2019.

2.2.1.3. Estructura del paquete IPv6

Un paquete IPv6 está conformado por tres partes: El encabezado IPv6, los encabezados de extensión y el PDU, siendo los dos últimos el PAYLOAD como se observa en la figura 2-2.

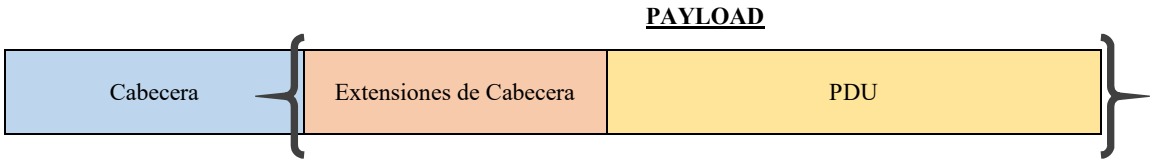


Figura 2-2: Estructura de un paquete IPv6.
Fuente: (DAVIES, 2012) (pág. 91).

La cabecera IPv6 está conformada por 8 campos y tiene una longitud fija de 40 octetos como lo muestra la **Figura 3-2.**

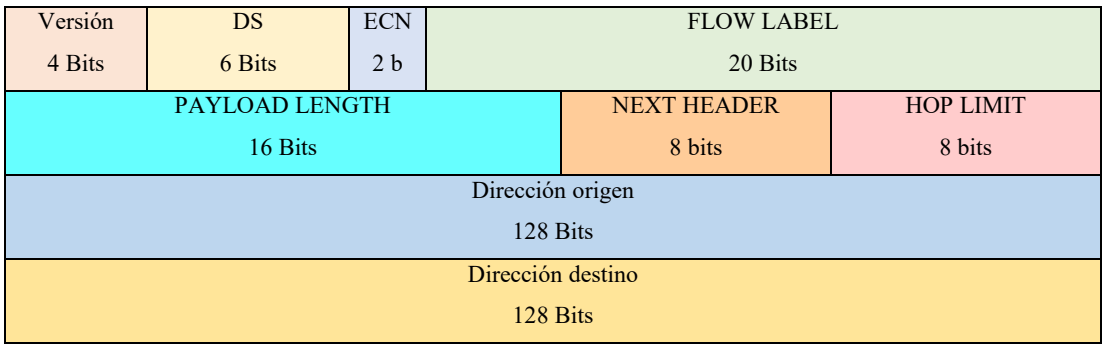


Figura 3-2: Cabecera IPv6.
Fuente: RFC 2460.

- **Versión. -** Identifica la cabecera y debe ser igual a 6.
- **DS (Servicios diferenciados). -** 2 bits son reservados y su nombre cambio a clase de tráfico (RFC 2474).
- **ECN. -** Se usa como indicadores de notificación de congestión explícita (RFC 3168).
- **Flow Label.-** Se usa para identificar paquetes que pertenecen al mismo flujo de una sucesión y para la entrega priorizada (RFC 3697).
- **Payload Length. -** Contiene un valor entero igual a la longitud de la carga útil (Payload) del paquete en bytes. Las extensiones de IPv6 se incluyen como parte de este si las hubiese. Se puede tener un PAYLOAD de hasta 65535 bytes de longitud y cuando se supera esta cifra, su valor se establece en cero y se usa la extensión de cabecera Hop-by-hop.
- **Next Header. -** Indica que protocolo está en uso en el encabezado. El valor de 59 indica que no hay nada después de es encabezado. La **Tabla 4-2** muestra sus valores más comunes.
-

Tabla 4-2: Valores Típicos en el campo Next Header de IPv6**.**

Valor en decimal	Header
0	Hop by hop
6	TCP
17	UDP
41	Cabecera IPv6 Encapsulada
43	Routing Header
44	Fragment Header

50	Encapsulación del encabezado de PAYLOAD de Seguridad.
51	Cabecera de Autentificación.
58	ICMPv6
59	Sin Next Header
60	Cabecera Opciones de destino

Realizado por: Quintero Hermes, 2019.

- **Hot Limit. -** Indica el número máximo de enlaces que puede usar un paquete IPv6 antes de ser descartado. Cada vez que un nodo envía un paquete, resta 1 de su valor y cuando llega a 0 el enrutador envía un mensaje ICMPv6 de límite de tiempo excedido en el tránsito a la fuente y se descarta.
- **Dirección origen. -** Dirección de 128 bits del nodo que origina el paquete IPv6.
- **Dirección destino. -** Dirección de 128 bits del nodo destinatario del paquete IPv6. Puede ser unicast, multicast o anycast.

Las cabeceras de extensión están diseñadas para transportar datos de la capa de Internet opcionales, pueden ser cero o más y son opcionales. Son de tamaño fijo o variable y su extensión debe ser un múltiplo de 8 bytes; si es variable se debe rellenar y cumplir esta condición. Pueden expandirse para acomodar todos los datos necesarios para la comunicación IPv6.

De acuerdo al RFC 2460 se recomienda disponer los encabezados de extensión después de la cabecera IPv6 de acuerdo al orden de la **Tabla 5-2.**

Tabla 5-2: Encabezados de extensión en IPv6

Orden recomendado	Encabezado	Características.
1	**Hop by hop**	Especifica los parámetros de entrega en cada salto en la ruta al destino. Se identifica con el valor de 0 en NEXT HEADER. Consiste en tres campos: Next Header, longitud de extensión de encabezado y opciones (una o más a su vez).
2	**Opciones de destino**	Se usa para definir parámetros de entrega o procesamiento de paquetes de destinos intermedios o para el destino final. Tiene un valor de 60 en Next Header.
3	**Encabezado de enrutamiento**	Especifica una ruta de origen, la cual es una lista de destinos intermedios para el paquete que se desplaza hasta su destino final. Tiene un valor de 43 en Next Header y está conformado por los campos next header, header extension length, routing type, segments left y routing type specific data.
4	**Encabezado de fragmento**	Se usa para los servicios de fragmentación y reensamblado de IPv6. Solo los nodos origen pueden fragmentar. Si el PAYLOAD enviado por el protocolo de capa superior es mayor que el MTU del enlace o la ruta, IPv6 lo fragmenta en el origen y

		usa este campo para ofrecer la información necesaria para reensamblarlo. Tiene un valor de 44 en next header y su estructura incluye los campos next header, fragment offset (13 bit), fragments flag e identification (32 bit).
5	**Encabezado de autenticación**	Proporciona los servicios de autentificación, integridad y protección antireplay para el paquete IPv6. Su especificación en detalle está en el RFC 4302 y tiene el valor de 51 en next header. Está conformado por los campos next header, PAYLOAD length, reserved, SPI, sequence number (para protección antireplay) y authentication data (contiene ICV para proporcionar integridad y autentificación).
6	**Encapsulación del PAYLOAD de seguridad**	Su especificación está en el RFC 4303. Tiene un valor de 50 en next header. Proporciona confidencialidad a los datos. Contiene un campo SPI que identifica a IPsec y un campo de sequence number. El encabezado ESP no proporciona servicios de seguridad a las cabeceras que se producen antes de la cabecera ESP.

Realizado por: Quintero Hermes, 2019.

IPv6 requiere que la capa de enlace soporte un tamaño de MTU mínimo de 1280 bytes y sugiere que se use un MTU de 1500 bytes (Ethernet II). La **Tabla 6-2** detalla los MTU definidas para IPv6 para las tecnologías LAN y WAN.

Tabla 6-2: MTU de IPv6 para las tecnologías LAN y WAN

Tecnología LAN-WAN	MTU
Ethernet (Ethernet II encapsulation)	1500, hasta 9000 para jumboframes.
Ethernet (IEEE 802.3 SNAP encapsulation)	1492
IEEE 802.11	2312
Token Ring	Múltiple
FDDI	4352
ARCNet	9072
PPP	1500
X.25	1280
Frame Relay	1592
ATM	9180

Fuente: (DAVIES, 2012) (p. 114).

Aquellas capas de vínculo que no admiten este tamaño deben proporcionar un esquema de fragmentación y re ensamblado; este debe ser transparente; aunque este proceso no es alentado en IPv6.

2.2.1.4. Sintaxis de una dirección IPv6

Las direcciones IPv6 identifican interfaces y no nodos. Su tamaño es 128 bits y está diseñado para dividirse en dominios de enrutamiento unicast jerárquicos que reflejan la topología del internet moderno. En el RFC 3513 se sugiere 3 enfoques para representar o escribir direcciones IPv6:

a) **Representación Estándar. -** Se escriben 8 bloques de 16 bits y en cada bloque 4 dígitos hexadecimales separados por dos puntos **(:)** denominado colón como lo muestra la figura 4-2. Se usa la notación hexadecimal porque es más fácil convertirla hacia binario. Esta escritura está expresada para ser aprovechada al máximo por los ordenadores y enrutadores, sin embargo, son un poco engorrosas y confusas a la vista de los usuarios.

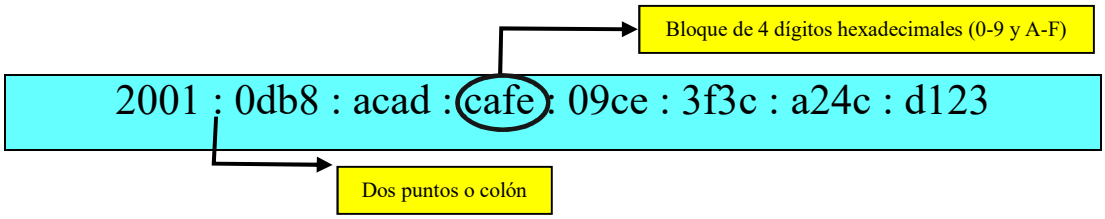


Figura 4-2: Representación estándar de una dirección IPv6.
Realizado por: Quintero Hermes, 2019.

b) **Supresión de ceros. -** Suprimir los ceros a la izquierda de cualquier dígito como lo muestra la figura 5-2.

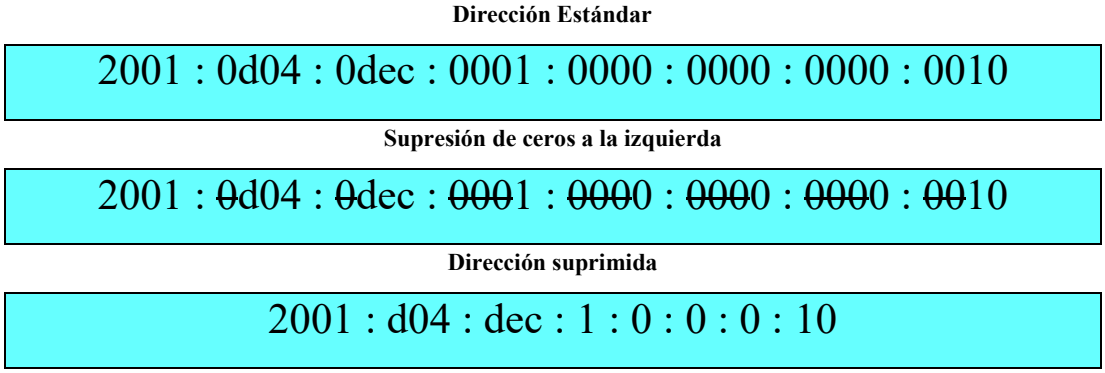


Figura 5-2: Supresión de ceros a la izquierda de una dirección IPv6.
Realizado por: Quintero Hermes, 2019.

c) **Comprimir ceros. -** Se suprime una sola cadena contigua de ceros y se las representa con doble colón (**: :**); También pueden ser los ceros iniciales o finales como lo muestra la tabla 7-2.

Tabla 7-2: Representación de direcciones IPv6 comprimidas.

Tipo de dirección	Representación Estándar	Dirección Comprimida
Unicast	1080:0:0:0:8:800:200C:417[a]	1080**::**800:200C:417A
Multicast	FF01:0:0:0:0:0:0:101	FF01**::**101
Loopback	0:0:0:0:0:0:0:1	**::**1
No especificada	0:0:0:0:0:0:0:0	**::**

Fuente: RFC 3513.

Para reescribir una dirección a su notación de 8 bloques, se cuenta los bloques disponibles, se resta de 8 y se escribe la diferencia rellenando con ceros comenzando siempre de izquierda a derecha.

Una dirección IPv6 está compuesta por un prefijo de 64 bits para subred y 64 bits para identificador de interfaz, con el objetivo de identificar cada segmento (A). También se puede considerar como una representación general de una dirección IPv6 aquella que está conformada por tres partes: un prefijo de enrutamiento global, un ID de subred y un ID de interfaz (B) como lo indica la figura 6-2.

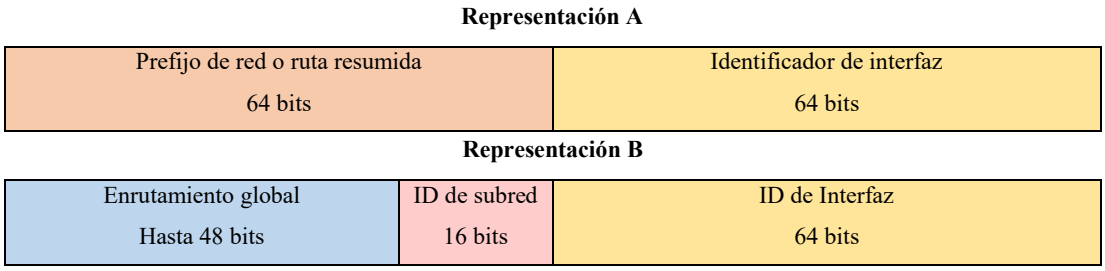


Figura 6-2: Estructura de una dirección IPv6.
Realizado por: Quintero Hermes, 2019.

El prefijo es la parte donde los bits tienen valores fijos y definen una ruta o subred como lo define el RFC 4291 (deja obsoleta al RFC 3513). Todo prefijo menor a 64 bits es una ruta resumida o un intervalo de direcciones que está resumiendo una parte del espacio de direcciones asignadas como lo muestra la figura 7-2.

El prefijo puede ser asignado a personas, empresas, proveedores de servicio u organizaciones y lo otorga la IANA. Las direcciones IPv6 no tienen máscara de subred y usan una diagonal ascendente (/) para indicar el prefijo.

Prefijo de Red	2001:db8:acad:2f3f:: /64
Prefijo de Ruta resumida	2001:db8:af:: /48

Figura 7-2: Prefijos de red en una dirección IPv6.
Realizado por: Quintero Hermes, 2019.

2.2.2. Direcciones unicast

Identifican una única interfaz dentro del ámbito de una dirección. Toda interfaz debe tener al menos una dirección enlace unicast. Para acomodar los sistemas de equilibrio de carga, en el RFC 4291, se establecen múltiples interfaces para utilizar la misma dirección, siempre y cuando aparezcan con una interfaz única para la implementación IPv6 de un host. Se clasifican en cinco como lo muestra la figura 8-2.

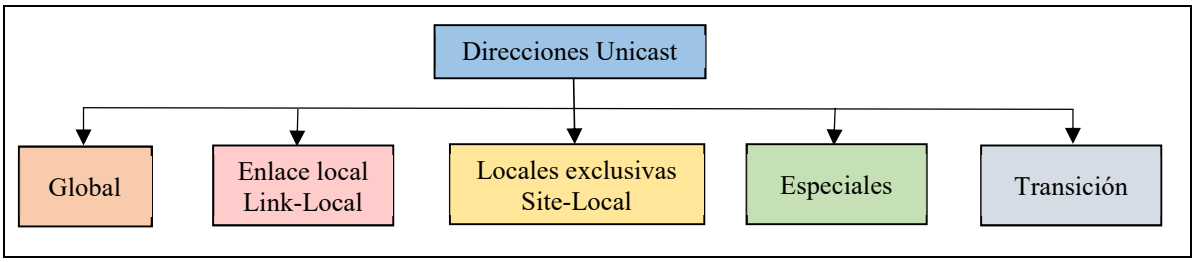


Figura 8-2: Direcciones Unicast.
Realizado por: Quintero Hermes, 2019.

2.2.2.1. Globales

Son globalmente enrutables y accesibles en el Internet IPv6. Están diseñadas para ser agregadas o resumidas en una infraestructura de enrutamiento eficiente. Se define en el RFC 3587 y su estructura esta descrita en la figura 9-2. Conteniendo los siguientes campos:

001 **A**	Prefijo de enrutamiento global **(B)**	ID de Subred **(C)**	ID Interfaz **(D)**

Figura 9-2: Estructura dirección unicast global
Fuente: RFC 3685.

A. **Bits fijos o de orden superior. -** Establecidos a 001 (3 bits).
B. **Prefijo de enrutamiento global. -** Indica el prefijo para una organización en específico. Tienen 45 bits. Los ingenieros y administradores de la organización son quienes determinan el plan de direccionamiento y la política de enrutamiento. Una organización también puede obtener bloques con longitudes de /32, /36, /40 y /44 de acuerdo a los límites de nibble.
C. **Identificador de subred. -** Identifica las subredes o VLAN´s dentro de una organización. Se dispone de 65536 subredes para el direccionamiento jerárquico. Tiene 16 bits.
D. **Identificador de interfaz. -** Identifica la interfaz única dentro de la organización de un nodo o de un host.

Las direcciones globales que se encuentran registradas por la IANA y podrán viajar a través de Internet comienzan con 0010 = “2” (IANA, https://www.iana.org/, 2017).

2.2.2.2. Enlace local

Se detallan en el RFC 4291 y se usan para la comunicación entre nodos vecinos en el mismo enlace cuando no hay un enrutador. Son similares a las direcciones IPv4 de enlace local definidas en el (RFC 3927) con prefijo 169.254.0.0/16 (APIPA para Windows). Estas direcciones reemplazan a las direcciones privadas de IPv4.

Tiene como objetivo la configuración automática de direcciones, descubrimiento de vecinos o cuando no hay enrutadores presentes. Los enrutadores no deben encaminar o enrutar paquetes que tengan estas direcciones Los paquetes enviados a esta dirección nunca deben ser enviados a través de enlaces locales. Su estructura se detalla en la figura 10-2.

1111111010 **10 bits**	0 **54 bits**	ID Interfaz **64 bits**

Figura 10-2: Estructura dirección unicast enlace-local.
Fuente: Fuente RFC 4291

De acuerdo a su prefijo **FE80:: /10** se puede tener un rango desde FE80:: hasta FEBF::, teniendo direcciones como enlace local que comienzan con FE9X:: y FEAX:: (X es cualquier valor de los dígitos hexadecimales).

2.2.2.3. Locales exclusivas

El (RFC 4193) define una dirección privada, única y no enrutable en Internet IPv6. La figura 11-2 muestra su estructura. Tienen un alcance global, pero su accesibilidad se define mediante la topología de enrutamiento y las políticas de filtrado de los límites de Internet o un conjunto de sites.

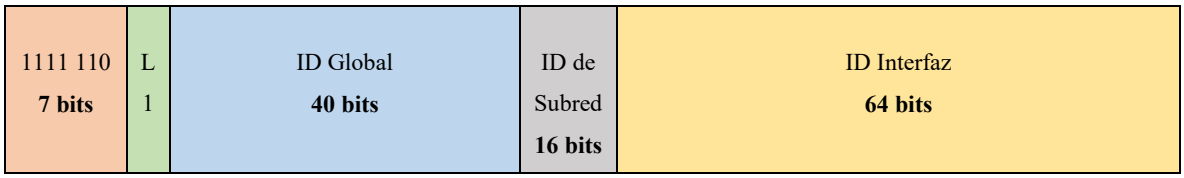


Figura 11-2: Estructura dirección unicast Site-Local.
Fuente: RFC 4193

Los siete primeros bits son fijos con un valor de **FC00:: /7.** El siguiente campo L, es definido como un indicador local y su valor en uno indica que el prefijo está asignado localmente (**FD00:: /8**). Su valor en cero no está definido en el RFC. El identificador global identifica un sitio específico dentro de una organización y se establece en un valor derivado de 40 bits en forma aleatoria.

Estas direcciones son para direccionar paquetes dentro de un sitio completo y pueden incluir hasta 54 bits en la mitad de la red de la dirección para indicar una dirección de subred.

2.2.2.4. Especiales

Las direcciones especiales se detallan a continuación en la tabla 8-2; también están registradas por la (IANA, https://www.iana.org/, 2017).

Tabla 8-2: Direcciones unicast especiales.

Tipo de dirección	Característica	Dirección ejemplo
Loopback	Se asigna a una interfaz de bucle invertido, lo que le permite enviar paquetes a sí mismo.	**::**1
No especificada	Nunca se asigna a una interfaz o se usa como dirección de destino. Indica la ausencia de una dirección.	**::**
IPv4 Mapeada	Se usa para representar una dirección IPv4 como una dirección IPv6 de 128 bits. No están soportadas en todas las plataformas.	**::FFFF:192.168.10.25**
6to4	Se le asigna a un nodo para la tecnología de transición 6to4 IPv6. Usa una IPv4 pública y el prefijo 2002. Está descrita en el (RFC 3056)	**2002:B5C4:1891:2222::1/64**
ISATAP	Tiene un prefijo /64. Contiene una dirección IPv4 privada. Está asignada a un nodo para la tecnología de transmisión IPv6 ISATAP.	**fe80::5efe:192.168.100.20**
TEREDO	Es una dirección global que utiliza el prefijo 2001:: /32 para asignar un nodo para la tecnología de transición Teredo IPv6. Se detalla en el (RFC 4380)	**2001:0000::/32**
Documentación	Se define en el (RFC 3849)	**2001:db8::/32**
ORCHID	Se define en el (RFC 4863)	**2001:10::/28**

Realizado por: Quintero Hermes, 2019.

2.2.3. Direcciones multicast

Se detalla en el (RFC 4291). Reemplaza todas las formas de direcciones de difusión en IPv4. La función de difusión se logra enviando paquetes a la dirección multicast de todos los nodos. Aquellos nodos interesados en el tráfico pueden suscribirse a una dirección multicast y aquellos que no estén interesados ignoran los paquetes.

Este tipo de direcciones no pueden utilizarse como de origen ni destinos intermedios en un encabezado de extensión de enrutamiento. Los nodos IPv6 ubicados arbitrariamente pueden escuchar el tráfico de multidifusión de una dirección multicast. También pueden escuchar múltiples direcciones a la vez y pueden unirse o abandonar un grupo de multidifusión en cualquier momento.

Su estructura está formada por banderas, alcance y el grupo de multidifusión como lo indica la figura 12-2. Tiene los primeros 8 bits establecidos con 1 por lo que siempre comenzará con **FF**.

Figura 12-2: Estructura dirección multicast.
Fuente: RFC 4291

Las banderas señalan los indicadores configurados con la dirección de multidifusión. Tiene 4 bits, con 3 indicadores de orden inferior:

- Primer bit de orden más bajo. - Es el indicador transitorio y se lo representa con la letra T. Sus valores se detallan en la tabla 9-2.

Tabla 9-2: Indicador transitorio de una dirección multicast.

Valor	Indicador
0	Indica que la dirección multicast es bien conocida y asignada permanentemente por la IANA.
1	Indica que la dirección multicast es transitoria.

Fuente: RFC 4291.
Realizado por: Quintero Hermes, 2019

- Segundo bit de más bajo orden. - Se asigna el indicador de prefijo **P** y está descrito en el RFC 3306.
- Tercer bit de más bajo orden. - Es el indicador Rendezvous Point Address (CISCO, 2002) de prefijo **R,** se emplea para permitir un mecanismo escalable de multicast “inter” o “intra” dominios a través del concepto punto de encuentro incrustado.

El campo alcance indica el límite de la red IPv6 para la que se pretende entregar el tráfico multicast. Tiene 4 bits y la tabla 10-2 destaca los valores que puede tomar. Los valores no considerados aún no están asignados.

Tabla 10-2: Indicador alcance de una dirección multicast.

Valor	Alcance
0	Reservado
1	Interface local
2	Link-local
3	Reservado
4	Admin-local
5	Site-local
8	Organización-local
E	Global
F	Reservado

Fuente: RFC 4291.
Realizado por: Quintero Hermes, 2019.

El Id de grupo identifica el grupo de multidifusión y es único dentro del ámbito. Tiene un tamaño de 112 bits. Desde la dirección multicast FF01:: hasta FE0F:: son direcciones reservadas y bien conocidas. En el (RFC 2375) se encuentran las direcciones ya definidas.

2.2.4. Direcciones anycast

Se asigna a múltiples interfaces. Los paquetes enviados a esta dirección son enviados por la infraestructura de enrutamiento a la interfaz más cercana a la que se asigna. Asigna valores en términos de métricas de enrutamiento.

A partir del (RFC 4291) se utilizan solo como direcciones de destino y se asignan solo a enrutadores. Cualquier dirección de unidifusión podría especificarse como una dirección anycast, siempre y cuando todos los nodos configurados para responder a esa dirección sean conscientes de su estado de anycast en lugar de unicast.

2.2.5. Autoconfiguración de direcciones

Los últimos 64 bits de una dirección IPv6 corresponden al identificador de interfaz; este debe ser único para un prefijo de subred y puede ser configurado de diversas formas (~~en~~ direcciones de capa de enlace, números de serie, generarse al azar o en forma manual).

Teniendo en consideración que una de las ventajas del protocolo IPv6 es su fácil implementación y despliegue en una red, de acuerdo a (DAVIES, 2012), hay tres mecanismos básicos de autoconfiguración de direcciones como se detalla en la tabla 11-2.

Tabla 11-2: Mecanismos básicos de autoconfiguración de direcciones IPv6.

Mecanismo	Definición	Ejemplo
Sin Estado Stateless	Se considera sin estado debido a que no depende del estado o disponibilidad de mecanismos de asignación. El dispositivo intenta configurar su propia dirección sin intervención externa o de un usuario. Se basa en la recepción de mensajes de anuncios de enrutador. Estos mensajes tienen los indicadores de configuración de dirección administrada con prefijos de 64 bits.	EUI-64
Con Estado Stateful	Depende de un mecanismo de asignación de direcciones externo (servidor dhcp). Se denominan de estado porque los servidores mantienen tablas que contienen las direcciones IP y las direcciones de capa de enlace de todos los nodos que utilizan sus servicios. Los servidores usan ese estado para evitar que dos o más nodos usen la misma dirección. Se basa en el uso de un protocolo de configuración de direcciones para obtenerlas y proporcionar otros ajustes de configuración. Un host puede usar este mecanismo en la ausencia de un enrutador en el enlace local.	DHCPv6
Híbrida	Autoconfigura una dirección sin estado junto con ciertos parámetros IP adicionales (DNS, NTP, entre otros).	DHCPv6 sin estado

Realizado por: Quintero Hermes, 2019

El uso de servidores DHCP son una parte fundamental para la asignación simultánea de direcciones en una red debido a que mantienen el estado de sus clientes y gestionan las direcciones IP (LOSHIN, 2004). Un servidor asigna direcciones de tres formas:

1. **Asignación automática. -** Asigna una dirección IP permanente a un cliente.
2. **Asignación dinámica. -** Asigna una dirección IP durante un periodo de tiempo limitado.

3. **Asignación manual.** - La dirección es asignada por el administrador de la red y el servidor DHCP la asigna.

Mediante el uso del protocolo Discover Router y sus mensajes de anuncio, Router Solicitation y Router Advertisement, un host puede determinar las direcciones de los enrutadores vecinos, direcciones sin estado adicional, prefijo de conexión y otros parámetros de configuración. Las direcciones autoconfiguradas pueden asumir uno de los estados que se detallan en la tabla 12-2.

Tabla 12-2: Estados de una dirección autoconfigurada.

Mecanismo	Significado
Provisional	La dirección está en proceso de ser verificada como única. La verificación se realiza a través de la detección de direcciones duplicadas.
Válida	La dirección se puede utilizar para enviar y recibir tráfico de unidifusión. Incluye los estados preferido y obsoleto.
Preferida	La dirección es válida, se ha identificado su unicidad y puede utilizarse para comunicaciones ilimitadas.
Obsoleta (Deprecated)	La dirección es válida, se ha identificado su unicidad, pero su uso se desaconseja para una nueva comunicación.
Inválida	La dirección ya no se puede utilizar para enviar o recibir tráfico de unidifusión. Este estado se adquiere cuando expira la vida útil válida.

Realizado por: Quintero Hermes, 2019

Los enrutadores se configuran y anuncian una vida útil preferida y un valor válido de por vida para cada prefijo de red por medio de sus mensajes de anuncios.

2.2.5.1. EUI-64

Se derivan del estándar IEEE 802-2001 (Anexo A). Se describe como una concatenación de 40 bits adicionales a los 24 de OUI. El único cambio que se necesita para transformar un IEEE EUI-64 a un identificador de interfaz IPv6 es invertir el bit "**u**" (Universal/Local).

Para la generación de una EUI-64 se siguen los siguientes pasos (IEEE):

1. Se parte de la dirección MAC de 48 bits (EUI-48) y se debe agregar los octetos hexadecimales **FF** y **FE** después de los primeros 24 bits para obtener el identificador de interfaz de 64 bits.
2. Se invierte el valor del séptimo bit. Si es cero se cambia a uno y viceversa. Este valor nos indica que es administrado localmente.

Este proceso se detalla en la figura 13-2.

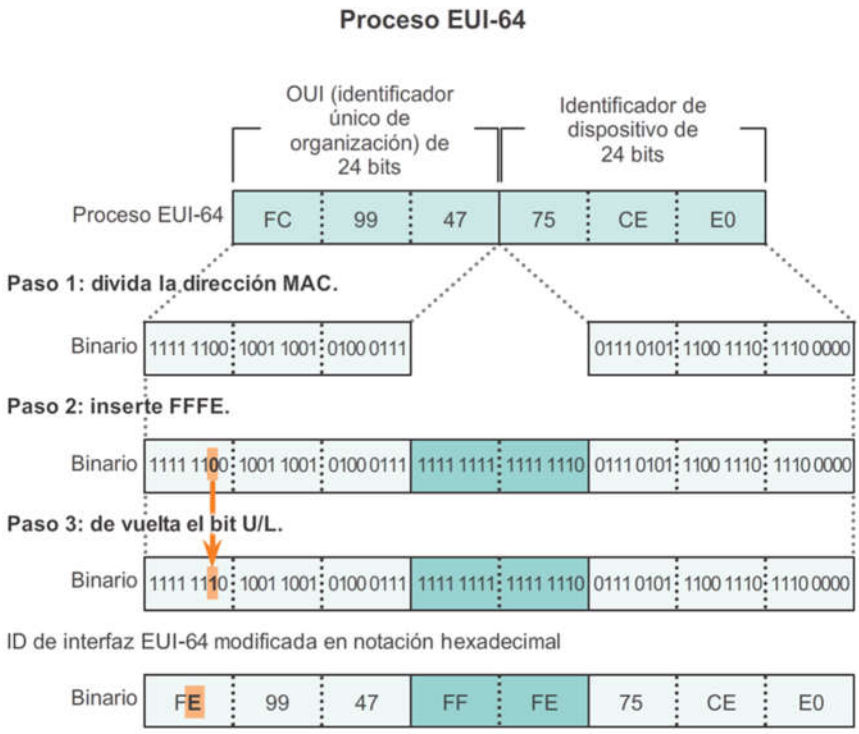


Figura 13-2: Proceso de obtención de una dirección EUI-64.
Realizado por: Quintero Hermes, 2019

El proceso de autoconfiguración de una dirección sin estado (RFC 4862) para una interfaz física de un nodo IPv6 se detalla en los siguientes pasos:

1. Se genera una dirección de enlace-local tentativa basada en el prefijo **FE80:: /64** y un identificador de interfaz derivado de **UEI-64.**
2. Con el uso de DAD, se verifica la unicidad de la dirección de enlace-local tentativa, se envía un mensaje de neighbor solicitation con el campo de dirección de destino que se establece en la dirección local tentativa.
3. Si se recibe un mensaje de neighbor advertisement (como respuesta del mensaje del paso 2), indica que otro nodo en el enlace local está usando la dirección tentativa y se detiene la autoconfiguración. Se debe asignar una configuración manual en el nodo.

4. Si no se recibe ningún mensaje de anuncio por algún vecino, se asume que la dirección tentativa es única y válida; se inicializa dicha dirección a la interfaz local.

Algunos ISP conceden un prefijo /64 a sus usuarios y cuando se realiza la conexión se asigna un identificador de interfaz de acuerdo a EUI-64.

2.2.5.2. DHCPv6

Este mecanismo permite la asignación de múltiples direcciones adicionales en el tiempo. Estas direcciones se asignan con un contrato de arrendamiento, una vida preferida y una vida útil válida. Es similar a DHCPv4 en sus objetivos y alcances, pero la operación del protocolo es diferente (Asigna múltiples direcciones a un nodo).

Las direcciones se agrupan para su gestión en una asociación de identidad entre el host y el servidor. Cada host tiene un identificador único (DUID), el cual permanece sin cambios durante toda la vida del host. Los servidores usan ese DUID para identificar a un host como confiable, incluso si el anfitrión se traslada entre enlaces.

Un cliente DHCPv6 inicia una transacción localizando primero al servidor por medio de una solicitud de información de configuración. Se asigna una dirección IPv6 a un host con un contrato de arrendamiento y el host puede iniciar una transacción con el servidor para extender el contrato. El nodo cliente utiliza una dirección de enlace local al intercambiar mensajes con el servidor DHCPv6.

Este mecanismo también es usado para asignar direcciones temporales. Genera un identificador de interfaz diferente al obtenido por EUI-64 usando técnicas de números aleatorios.

2.2.5.3. DHCPv6 sin estado

Es fácil de implementar y desplegar. Es un protocolo simple que puede ser proporcionado por un CPE. La IETF proporciona una guía para uso del servicio. Utiliza un intercambio de dos mensajes entre un cliente y un servidor. El host envía un mensaje de solicitud de información, el servidor responde con la información de configuración solicitada.

Este servicio solo requiere un subconjunto del mecanismo y los mensajes del protocolo DHCPv6 completo. Se especifica en el RFC 3736 y usa opciones en la sección de formato de variable de un mensaje DHCPv6. Entre ellas se tiene: Opciones de prefijo, Mecanismo de transición de doble pila, configuración de DNS, configuración NIS, configuración de tiempo, preferencia de prefijo para clientes DHCPv6 y equilibrio de carga.

2.2.6. Esteganografía

2.2.6.1. Antecedentes

Al hablar de esteganografía, los primeros ejemplos han sido observados en la naturaleza, en la cual, algunos animales, como los primates, a través de sus aullidos usan técnicas vocales (frecuencias diferentes) para establecer comunicaciones secretas que no sean descifradas. Otros se valen de características especiales de su cuerpo o entorno para realizar camuflaje o mimetización y así evitar o confundir a sus depredadores (WOJCIECH MAZURCZYK, 2016).

A través de la historia y con dotes de ingenio y creatividad, estos mecanismos fueron adaptados y reproducidos por muchas civilizaciones para mantener secretos a salvo de guardias o terceros. Los egipcios lograron establecer mensajes encubiertos a través de sus jeroglíficos, usando una serie de símbolos que solo podían ser interpretados por los que conocían su significado y para los demás representaban simples dibujos o imágenes (ABDELRAHMAN, 2012).

El griego *Herodotus* con el objetivo de enviar información oculta, rapó la cabeza de un esclavo, tatuó su mensaje y espero que le creciera el cabello para enviarlo a su destinatario, burlando los controles de los guardias (SHIH, 2017). Otros métodos conocidos han sido el uso de la tinta invisible, especialmente durante la Segunda Guerra Mundial; las marcas de cualquier tipo sobre ciertos caracteres (desde pequeños pinchazos de alfiler hasta trazos a lápiz que marcan un mensaje oculto en un texto), mensajes escondidos en vestimentas y periódicos en base a patrones o posicionamiento (VILLALÓN, 2002).

Este término fue usado por primera vez por *Johannes Trithemius* (1462-1516) en sus publicaciones denominadas Poligrafía y Esteganografía (KATZENBEISSER & PETITCOLAS, 2000). Etimológicamente proviene del griego *steganos* (cubierto) y *graphos* (escritura), lo que

etimológicamente significa “escritura cubierta”, siendo los griegos los primeros en poner en práctica su uso.

De acuerdo a (FRIDRICH, Steganography in Digital Media, 2010) es la ciencia que estudia los métodos para ocultar la presencia de un mensaje dentro de otro, de forma que pase desapercibida la existencia de dicha información secreta. Esta comunicación es privada y la comprenden solo el remitente y destinatario, aunque está a la vista de todos.

Con la evolución de la tecnología, computadores y redes en el siglo XX, los mecanismos esteganográficos se han trasladado a un entorno digital, desarrollando técnicas más sofisticadas en dispositivos y servicios comunes por usuarios y usando como medios portadores el correo electrónico, los documentos de texto, las impresiones, los archivos multimedia, los protocolos, entre otros. En la ***Figura 14-2:*** *Evolución histórica de los medios esteganográficos* se muestra un vistazo de este cambio a través de la historia.

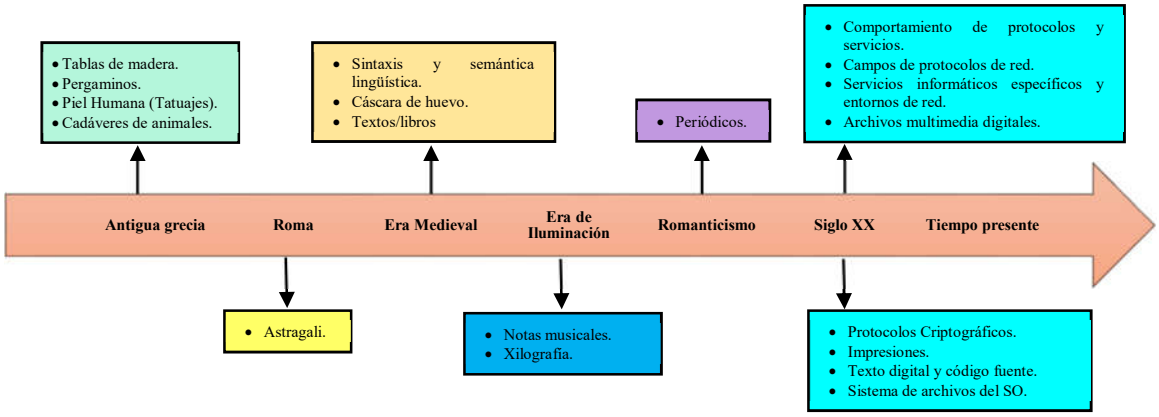


Figura 14-2: Evolución histórica de los medios esteganográficos
Fuente: (WOJCIECH MAZURCZYK, 2016) pág. 12
Realizado por: Quintero Hermes, 2019.

En la actualidad, el medio esteganográfico más extendido está basado en las imágenes digitales, debido a su excelente capacidad para ocultar información y dado que casi todos los estándares gráficos tienen una graduación de colores mayor de lo que el ojo humano puede apreciar, la imagen no cambia su apariencia de forma notable (VILLALÓN, 2002). A pesar que las imágenes son el medio más explotado, otros proporcionan una gran capacidad para ocultar mensajes y se detallan en la ***Tabla 13-2:*** *Medios esteganográficos más utilizados.* a continuación:

Tabla 13-2: Medios esteganográficos más utilizados.

Tipo de medio	Técnica	Ejemplo de aplicaciones
Uso de documentos	Agregando espacios en blanco y tabs porque son más difíciles de identificar para el ojo humano en la mayoría de los editores de texto.	SNOW TextHIDE SapmMimic StegParty
En imágenes	La técnica más utilizada es el LSB (Least Significant Bit), ya que en el computador un archivo de imagen es representado por colores e intensidades de luz en diferentes áreas (pixeles), por lo que los datos del mensaje pueden ser embebidos en la imagen.	EzStego EstegoDOS
En audio	La técnica más utilizada es LBE (Low Bit Encoding) que oculta la información en archivos de audio. Con la técnica Spread Spectrum se añade ruidos al azar a la señal de que la información se oculta dentro de la onda y la propagación en todo el espectro de frecuencias.	MP3Stego MP3Stegz
En video	Suele utilizarse la técnica DCT (Discrete Cosine Transform) que cambia ligeramente cada una de las imágenes en el vídeo, sólo de manera que no sea perceptible por el ojo humano, altera los valores de ciertas partes de las imágenes.	
En archivos de cualquier tipo	En archivos de cualquier tipo: se utiliza el método de inyección o agregado que consiste en agregar al final de un archivo (de cualquier tipo), otro archivo que será el contenedor del "mensaje a ocultar" (de cualquier tipo) (CASTILLO, CASTILLO, & NUÑEZ, 2013).	Covert TCP DiskHIDE StegFS Esteganografía en juegos.

FUENTE: (JOHNSON & JOHNSON Technology Consultants, 2012).
Realizado por: Quintero Hermes, 2019,

También es importante identificar las técnicas que se utilizan para incrustar la información secreta dentro de los medios anteriormente analizados. Estos se detallan en la ***Figura 15-2***.

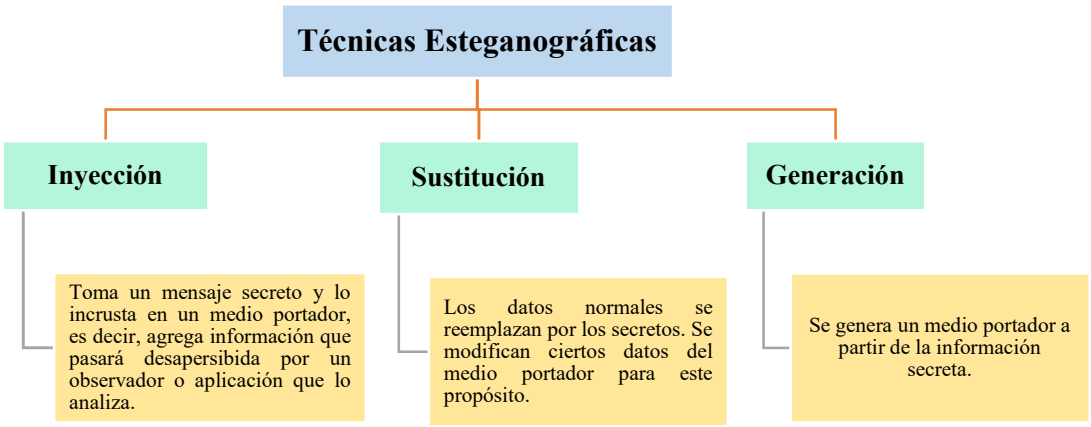


Figura 15-2: Técnicas esteganográficas
Fuente: (WILES & ROGERS, 2007) (pág. 321-322)
Realizado por: Quintero Hermes, 2019.

Para finalizar, el objetivo de la esteganografía no es el de sustituir al cifrado convencional, por el contrario, trata de complementarlo al combinarse, ya que ocultar un mensaje reduce las posibilidades de que sea descubierto durante el intercambio de información a través de medios inseguros y si este está cifrado, agrega un nivel adicional de seguridad y privacidad (GUO&LE, 2010) (LUBACCZ, MAZURCZYK, & SZCZYPIORSKI, 2014).

2.2.6.2. Sistema esteganográfico

El propósito de la esteganografía es transmitir información hacia un destinatario en forma secreta a través de algunas de las técnicas mencionadas anteriormente. Para esto se debe establecer un modelo que represente el escenario como un problema. (LAMPSON, 1973) y (SIMMONS, 1984) lo describen de acuerdo a la **Figura 16-2:** Problema de los prisioneros. En este caso Alice y Bob están prisioneros en celdas diferentes. Pueden intercambiar mensajes usando cartas, pero estas son revisadas por un guardián, que si observa algo extraño o inapropiado suspende la comunicación y los condena. El dilema que se genera es establecer un mecanismo de comunicación que introduzca mensajes en forma confidencial y no sea detectable para el guardia cuando revise el contenido de las cartas para establecer un plan de escape.

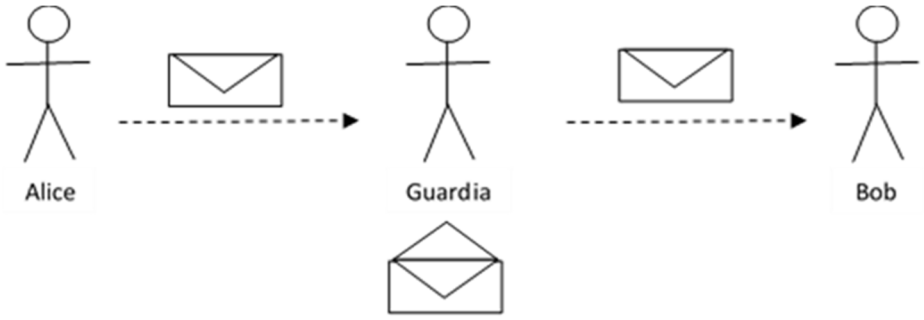


Figura 16-2: Problema de los prisioneros
Realizado por: Quintero Hermes, 2019.

A raíz de este escenario, es posible identificar los elementos necesarios que conforman un sistema esteganográfico para su estudio y aplicación en diferentes campos de acción y se detallan en la

Figura 17-2: Elementos de un sistema esteganográfico. Un emisor genera un estego-objeto al incrustar un mensaje dentro de un medio vulnerable usando una función (estego-función) y lo envía por un canal encubierto. El guardián es capaz de analizar o revisar el estego-objeto, sin levantar sospechas, para verificar la presencia de algo extraño o algún mensaje oculto. Finalmente, el receptor recibe el estego-objeto y separa el mensaje oculto usando la estego-función inversa.

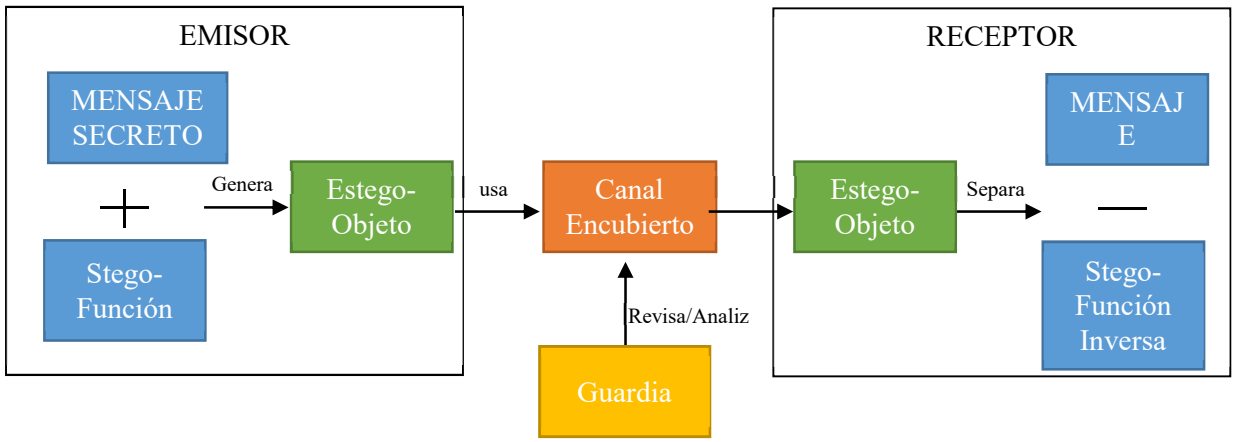


Figura 17-2: Elementos de un sistema esteganográfico
Realizado por: Quintero Hermes, 2019.

2.2.6.3. Características de un sistema esteganográfico

En la obra publicada por el doctor (BÖHME, 2010) establece que un sistema esteganográfico se puede medir por tres criterios básicos. Estos se detallan en la **Tabla 14-2:** *Características de un sistema esteganográfico*.

Tabla 14-2: Características de un sistema esteganográfico de red.

Característica	Definición
Ancho de banda esteganográfico	Cantidad de información que puede ser ocultada en una unidad de tiempo o portador.
Indetectabilidad	Dificultad para un tercero o guardián de detectar la información oculta en un portador. Se usan análisis estadísticos de la información o muestra capturada para compararla con las propiedades típicas del portador.
Robustez	Se define como la cantidad de alteración que un estegograma puede soportar sin alterar la información oculta.

Realizado por: Quintero Hermes, 2019.

La relación entre estos tres factores se describe por el triángulo mágico de (FRIDRICH, Applications of data hiding in digital images, 1999) y se ilustra en la **Figura 18-2***: Relación entre las características de un método esteganográfico de red.*

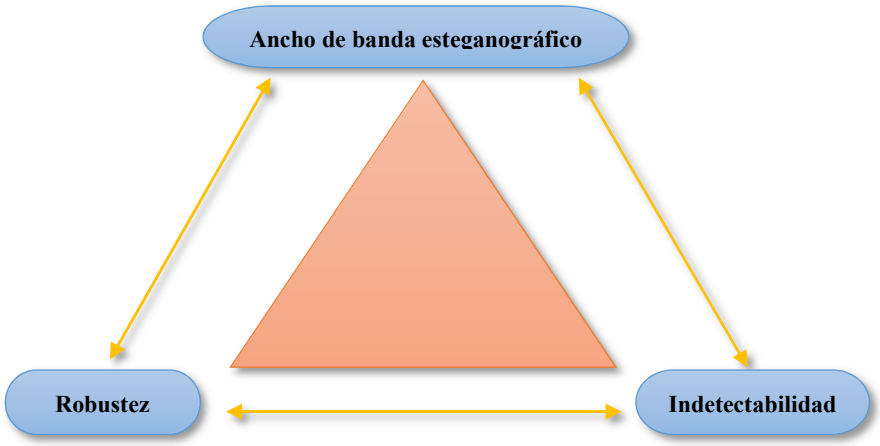


Figura 18-2: Relación entre las características de un método esteganográfico de red.
Fuente: (WOJCIECH MAZURCZYK, 2016, pág. 48)
Realizado por: Quintero Hermes, 2019.

Para finalizar, también es importante mencionar el ***cálculo del costo esteganográfico (CE)*** (MAZURCZYK WOJCIECH, 2014), el cual describe el grado de degradación/distorsión de un portador, causado por la incrustación de la información secreta. Depende del tipo de portador y si su

valor es excesivo indicará una fácil detección del método esteganográfico de red. Para portadores como video, audio o imágenes se usan los parámetros MSE o PSNR.

Cuando un método esteganográfico en red maximiza el ancho de banda aumenta el CE, en consecuencia, afecta y disminuye su robustez, indetectabilidad, funcionalidad y desempeño del portador. Esta relación se expresa en la **Figura 19-2.**

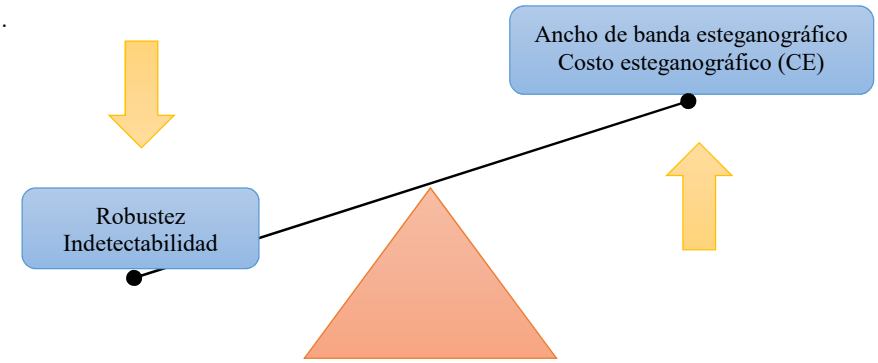


Figura 19-2: Relación entre las características de un método esteganográfico en red y su CE
Fuente: (WOJCIECH MAZURCZYK, 2016, pág. 49)

El valor de CE es igual a la probabilidad de detección del método esteganográfico, esto se muestra en la ***Figura 20*-2.** En donde se expresa que el valor de CE efectivo para guardar indetectabilidad es menor al 50%, ya que, con un valor mayor el mensaje secreto sería detectable y por ende el método esteganográfico no tendría sentido.

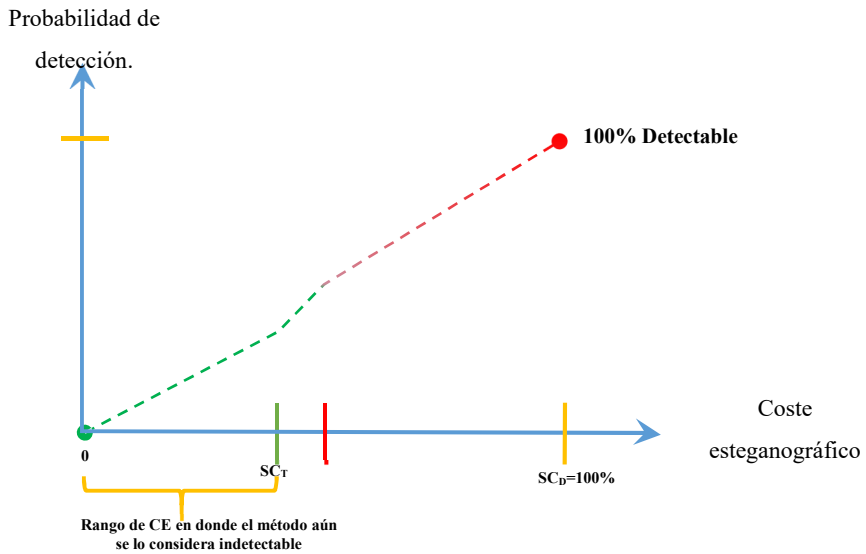


Figura 20-2: Relación entre el CE y la indetectabilidad
Fuente: (MAZURCZYK WOJCIECH, 2014)
Realizado por: Quintero Hermes, 2019.

2.2.6.3. Esteganálisis

Su objetivo se centra en la detección de la existencia de un mensaje oculto en lugar de saber cuál es. Es complementario a la esteganografía y se considera efectivo cuando al analizar el canal esteganográfico logra distinguir entre el medio portador y el estego-objeto incrustado.

De acuerdo a (SHIH, 2017) hay dos métodos para detectar archivos modificados. El primero lo denomina **análisis visual** en el cual se realiza una inspección minuciosa comparando con el archivo original; es un método muy simple. El segundo método se llama **análisis estadístico,** este detecta cambios en los patrones de píxeles y la frecuencia de intensidades. En el caso de una imagen analiza sus propiedades estadísticas comparando si se desvían de la norma, incluso ligeras alteraciones, para revelar las diferencias imperceptibles entre la original y la modificada.

2.2.7. Esteganografía aplicada a la red

En los recientes años, las redes de computadores han crecido en proporción y variedad, permitiendo establecer comunicaciones e intercambio de información entre sus usuarios y dispositivos, pero también han abierto la oportunidad de establecer diversos mecanismos para estos mismos fines en forma secreta. Muchos investigadores y expertos tratan de identificar potenciales vulnerabilidades para luego explotarlas para propósitos propios o diferentes a los comúnmente conocidos.

Se enfocan en el estudio y explotación de los diferentes protocolos en las capas del Modelo Referencial OSI, ya sea modificando/alterando sus propiedades intrínsecas, o aprovechando imperfecciones en los canales de comunicación (errores, retardos, fragmentación y segmentación).

Desde la perspectiva de las comunicaciones en red, existen tres principales tipos de información que están sujetas a ocultarse por parte de sus actores (WOJCIECH MAZURCZYK, 2016) y cada una asociada a técnicas diferentes para cumplir su meta. Estas se resumen en la ***Tabla 15-2:*** *Posibilidades de información a ocultar en las comunicaciones de redes*.

Tabla 15-2: Posibilidades de información a ocultar en las comunicaciones de redes

Tipos de información	Definición
Identidad de los actores en la comunicación	Es importante ocultar las identidades del emisor y receptor de la comunicación. Se usan técnicas de **anonimato.**
Proceso de la comunicación	Su objetivo se centra en ocultar el intercambio de datos o información. Se usan técnicas **esteganográficas.**
Contenido de la información	Protege el contenido de la información usando técnicas de **encriptación.**

Fuente: (WOJCIECH MAZURCZYK, 2016) pág. 40
Realizado por: Quintero Hermes, 2019.

En el caso de la esteganografía de red, esta se apoya en tres características que poseen las comunicaciones en red:

- Un canal de comunicación no es perfecto, por lo tanto, puede ser explotado.
- Uso de campos específicos de los protocolos de red o mensajes que nos son usados en todas las situaciones.
- No todos los protocolos están definidos completamente y es posible que admitan una sobrecarga semántica.

También se puede añadir que cuando las comunicaciones de red son analizadas por expertos forenses digitales, la mayoría de ellos usan muestras que son solo una parte de todo el tráfico capturado o de un intervalo de tiempo.

Partiendo de esto, el principal objetivo de la esteganografía en red se centra en ocultar la información en las transmisiones normales de los usuarios sin levantar sospechas, tratando de engañar otros dispositivos de la red (nodos intermedios o sistemas finales y/o de seguridad) o sin alterar significativamente al portador usado.

Se considera "***portador"*** a los paquetes, tramas o protocolos involucrados en una comunicación entre un emisor y receptor; también ofrece la oportunidad (espacio) para ocultar información. Debe poseer dos características:

- Debe ser de uso común y válido.
- Su modificación con la esteganografía no debe ser visible para las partes que desconocen el proceso.

Cuando a este portador se le aplica alguna técnica de esteganografía se le denomina "***estegograma"*** *o* ***"estego-objeto".*** Vale aclarar, que el término "***covert channel***" es utilizado para describir a las técnicas esteganográficas que se desarrollan en los protocolos de red.

CAPÍTULO III

3. DISEÑO DE LA INVESTIGACIÓN

3.1. Tipo de investigación

La presente investigación puede clasificarse de dos tipos: aplicativa y experimental.

- **Experimental:** Se refiere a un estudio en el que se manipulan intencionalmente una o más variables independientes (supuestas causas antecedentes), para analizar las consecuencias que la manipulación tiene sobre una o más variables dependientes (supuestos efectos consecuentes). Una vez tenido un análisis profundo se procede a realizar pruebas en escenarios de laboratorio usando la simulación, en las que se observará los elementos más importantes del objeto de estudio que se investiga para obtener una captación de los fenómenos a primera vista para realizar conclusiones.
- **Aplicativa:** ya que se basa en conocimientos existentes, derivados de investigaciones previas, dirigida al desarrollo tecnológico para establecer nuevos procesos para mejorar los existentes.

3.2. Diseño de la investigación

El término ***diseño*** se refiere al plan o estrategia concebida para obtener la información que se desea con el fin de responder al planteamiento del problema. El presente tipo de trabajo de investigación es experimental y aplicativa. En donde se propone recopilar información de investigaciones previas para analizar y diseñar un mecanismo esteganográfico sobre el protocolo IPv6. Además de demostrar su funcionamiento sobre dos escenarios simulados, en el cual se establecerá una comunicación por medio de mensajes ocultos usando el protocolo IPv6 como medio esteganográfico entre dos equipos usando servicios comunes como DNS y VoIP.

3.3. Alcance de la investigación

El alcance para esta investigación es ***explicativo***, ya que se busca explicar la relación que existe entre usar una técnica esteganográfica en el protocolo IPv6 y una comunicación segura. Siendo estructurada y fundamentada en la recolección de datos y pruebas de simulación basada en los parámetros para validar el mecanismo implementado.

3.4. Enfoque de la investigación

Los enfoques tomados para esta investigación fueron ***cuantitativo y cualitativo,*** debido a que ambos emplean procesos cuidadosos, metódicos y empíricos en su esfuerzo para generar conocimiento. Ambos enfoques llevan a cabo la observación y evaluación de fenómenos, por medio de la recolección de datos para luego ser analizados e interpretados. Así obtener los resultados que orientan al descubrimiento de la hipótesis y verificar su validez.

3.5. Métodos de investigación

Para este trabajo de tesis se utilizaron los siguientes métodos de investigación:

3.5.1. Método analítico

Este método consiste en un proceso cognoscitivo que consiste en descomponer un objeto separando cada una de las partes del todo para estudiarlas en forma individual. Se lo utilizó para estudiar todas las características asociadas al protocolo IPv6 y la esteganografía.

3.5.2. Método inductivo

Con este método se utiliza el razonamiento para obtener conclusiones que parten de hechos particulares aceptados como válidos, para llegar a conclusiones, cuya aplicación sea de carácter

general. Este inicia con un estudio individual de los hechos y se formulan conclusiones universales que se postulan como leyes, principios o fundamentos de una teoría. Por medio de la inducción, se asoció las características del protocolo IPv6 y la esteganografía para el aprovechamiento y diseño de un mecanismo o técnica que permita establecer una comunicación segura.

3.5.3. Método científico

El método científico fundamenta a un conocimiento válido desde el punto de vista científico, utilizando para esto instrumentos que resulten fiables; consta de las siguientes etapas:

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

Con este método fue posible demostrar, a través del cumplimiento de sus etapas y los escenarios virtualizados, el diseño elaborado en los métodos anteriores. Además de obtener los valores de la variable medible para evidenciar y apoyar la hipótesis planteada.

3.6. Técnicas

Las técnicas que se utilizan en esta investigación son:

Búsqueda de información. - Permite obtener la fuente de información necesaria sobre el objeto de estudio

Pruebas. - Permite realizar experimentos de escenarios de laboratorio.

Observación. - Al ser un examen detenido de los diferentes aspectos de un fenómeno, permite determinar resultados de las pruebas realizadas en la simulación.

3.7. Instrumentos

Los instrumentos para recopilar los datos de los indicadores son los siguientes:

Tabla 1-3: Instrumentos utilizados para la recolección de datos.

Instrumento	Descripción
Wireshark	Antes conocido como Ethereal, es un analizador de protocolos utilizado para realizar análisis y solucionar problemas en redes de comunicaciones, para desarrollo de software y protocolos, y como una herramienta didáctica. Es de código abierto y cuenta con una interfaz gráfica de usuario fácil de usar (VERMA, 2015) (WIRESHARK, 2017).
Oracle VM VirtualBox	Es un software de virtualización de código abierto para arquitecturas x86/amd64, creado originalmente por la empresa alemana innotek GmbH. Actualmente es desarrollado por Oracle Corporation como parte de su familia de productos de virtualización. Por medio de esta aplicación es posible instalar sistemas operativos adicionales, conocidos como «sistemas invitados», dentro de otro sistema operativo «anfitrión», cada uno con su propio ambiente virtual (VIRTUALBOX, 2017) (DASH, 2013).
GNS3	Es utilizado por cientos de miles de ingenieros de redes en todo el mundo para emular, configurar, probar y solucionar problemas de redes virtuales y reales. GNS3 le permite ejecutar una pequeña topología que consta de solo unos pocos dispositivos en su computadora portátil, a aquellos que tienen muchos dispositivos alojados en múltiples servidores o incluso alojados en la nube. Está activamente desarrollado y respaldado, y cuenta con una comunidad en crecimiento de más de 800,000 miembros. Es usado por estudiantes, ingenieros de redes, arquitectos para pruebas y simulaciones; posee más de 10 millones de descargas hasta la fecha (GNS3, 2017).
Kali-Linux	Es una distribución de Linux basada en Debian destinada a pruebas avanzadas de penetración y auditorías de seguridad. Contiene varios cientos de herramientas que están orientadas a diversas tareas de seguridad

	de la información. Entre sus pruebas de aplicación tenemos de penetración, investigación de seguridad, informática forense e ingeniería inversa (KALI-LINUX, 2017).
Microsoft Office Excel 2016	Es un aplicación que es parte de la suite de oficina de Microsoft y trabaja en hojas de cálculo que permitió realizar cálculos, gráficos y tablas de los escenarios simulados para procesar e interpretar los resultados.

Realizado por: Quintero Hermes, 2019.

3.7.1. Validación de los Instrumentos

Los instrumentos considerados para la validación en esta investigación son avalados por los miembros del tribunal, quienes poseen experiencia en su dominio y certifican su uso para la elaboración de entornos simulados, la recolección, procesamiento e interpretación de datos. A continuación, se detallan sus ventajas y características principales:

3.7.1.1. Wireshark

Figura 1-3: Logo de Wireshark
Fuente: https://www.wireshark.org/assets/theme-2015/images/wireshark_logo.png

Dentro de las características principales de esta aplicación se tiene (WIRESHARK, 2017):

- Inspección profunda de la mayoría de protocolos (IPv4 e IPv6).
- Multiplataforma: Se ejecuta en sistemas operativos como: Windows, Linux, macOS, Solaris y FreeBSD.
- Permite la captura de fragmentos, datagramas o paquetes en tiempo real y análisis fuera de línea.
- Los datos de red capturados pueden explorarse a través de una GUI, mediante la utilidad TShark y producir una salida de resultados en formatos XML, Postscript, CSV o texto in formato.
- Lee/Escribe en muchos formatos de archivos de captura.

- Los datos en vivo pueden leerse desde Ethernet, IEEE 802.11, PPP/HDLC, ATM, Bluetooth, USB, Token Ring, entre otros.

En esta investigación se lo usa para analizar en forma visual los paquetes IPv6 del entorno simulado.

3.7.1.2. Oracle VM VirtualBox

Figura 2-3: Logo de VirtualBox
Fuente: https://www.virtualbox.org/graphics/vbox_logo2_gradient.png

Dentro de las características principales de esta aplicación se tiene (VIRTUALBOX, 2017) (DASH, 2013):

- Diseño extremadamente modular con interfaces de programación interna bien definidas y una separación clara del código del cliente y el servidor, facilitando el control desde varias interfaces.
- Optimización de recursos a nivel de hardware y reducción del CAPEX.
- Buen soporte de hardware y no se requiere su virtualización.
- Puede ejecutarse en arquitecturas de 32/64 bits y tiene soporte para varios sistemas operativos y sus diferentes versiones.
- Permite la construcción de ambientes de simulación o pruebas. Se pueden configurar las máquinas virtuales de forma independiente en función de su rol o propósito (servidores, host, firewall, router o entorno de desarrollo).
- Las máquinas virtuales creadas son portables y pueden ser importadas o exportadas.
- Permite guardar estados en momentos específicos de configuración y la organización de máquinas en forma individual o colectiva.

En esta investigación se usa este hipervisor para virtualizar los sistemas operativos del ambiente de pruebas.

3.7.1.3. GNS3

Figura 3-3: Logo de GNS3
Fuente: https://www.gns3.com/assets/images/logo-colour.png

Dentro de las características principales de esta aplicación se tiene (NEUMANN, 2015) (GNS3, 2017):

- Es libre y de código abierto.
- Admite la virtualización de múltiples proveedores.
- Se puede ejecutar con o sin hipervisores, sean estos gratuitos o de pago.
- Soporte nativo en Linux.
- Posee una comunidad activa de más de 800000 a nivel mundial.
- La interfaz gráfica permite crear laboratorios de red virtualizados integrando enrutadores, conmutadores, servidores, hosts y herramientas open-source.

El uso de esta aplicación permite la integración de las herramientas anteriores y la virtualización de un escenario real.

3.7.1.4. Kali-Linux

Figura 4-3: Logo de Kali-Linux
https://www.kali.org/wp-content/uploads/2015/09/kali-2.0-website-logo-300x90.png

Como características principales de esta distribución de Linux tenemos:

- Es libre y de código abierto.
- Contiene más de 300 herramientas de penetración y auditoría informática.

- Soporte de dispositivos inalámbricos para compatibilidad en auditorías WI-FI.
- Paquetes y repositorios firmados por GPG.
- Interfaz gráfica agradable al usuario y con capacidad de personalización.
- Tiene soporte para sistemas ARM.

En esta investigación se usó algunas de las herramientas que dispone para análisis de tráfico, como Wireshark.

3.8. Implementación del entorno de pruebas

En esta investigación se ha desarrollado dos entornos de pruebas virtualizados con las herramientas de GNS3 y VIRTUALBOX. Con ellas se representan la aplicación y demostración de un mecanismo esteganográfico entre dos usuarios que envían mensajes ocultos usando el protocolo IPv6 y como medio portador sus direcciones IPv6 de origen, haciendo uso de dos servicios comunes en una red de datos; permitiendo también la obtención de información relevante respecto a los indicadores propuestos en la variable dependiente. En el primer escenario se simuló la implementación de un servidor DNS usando la aplicación DNSMASQ para registrar las direcciones IPv6 asociadas a un dominio de un servidor web; en el segundo escenario se implementó una central PBX usando la distribución ELASTIX 5.0 basada en Debian y dos clientes con sistema operativo FEDORA 27 que tienen instalada la aplicación LINPHONE como softphone para realizar llamadas.

3.8.1. Recursos de hardware y software utilizados

A continuación, en las tablas 2-3 y 3-3, se detalla los recursos de software y hardware que se utilizaron para el entorno de pruebas propuesto:

Tabla 2-3: Requerimientos de Hardware del escenario de pruebas

Requerimientos de Hardware	
Cantidad	**Descripción**
1	Computador portátil marca DELL, modelo INSPIRON 5566. Procesador Core(TM) i3-71000 a 2.40GHz (4 CPU´s) 8192 MB de memoria RAM. Disco duro de 1000 GB.

Realizado por: Quintero Hermes, 2019.

Tabla 3-3: Requerimiento de software para el escenario de pruebas

Requerimiento de Software			
Cantidad	**Descripción**	**Versión**	**Observación**
1	Sistema operativo Windows HOME	10	Principal
2	Sistema operativo CentOS	7	Máquinas virtuales, usadas para un servidor web y dns.
1	Sistema operativo KALI-LINUX	2019.2	Máquina virtual, usada para el usuario receptor y como instrumento de recolección de datos.
1	WIRESHARK	2.4.0	Herramienta en KALI-LINUX; analizador de protocolos de paquetes.
2	Sistema operativo FEDORA	27	Máquinas virtuales usadas como equipos clientes y con la aplicación LINPHONE instalada para realizar llamadas.
1	Sistema operativo distro ELASTIX	5	Máquina virtual usada como central pbx de alto rendimiento. Basada en DEBIAN 9.
1	GNS3	2.0.3	Simulador de redes y servicios.
1	VIRTUALBOX	5.2.0	Aplicación para crear máquinas virtuales.
3	C3725	12.4	Equipos de capa 3, virtualizados en GNS3, IOS CISCO ROUTER.
1	dnsmasq	2.76	Servidor DNS
1	httpd	2.4.6	Servidor WEB
1	LINPHONE	3.6.1	Aplicación softphone para realizar llamadas (video-teléfono) a través de internet que usa el protocolo estándar SIP y soporta IPv6.

Realizado por: Quintero Hermes, 2019.

3.8.2. Escenario de pruebas #1

A continuación, se detalla el direccionamiento utilizado en el escenario de prueba # 1 para cada uno de los dispositivos:

Tabla 4-3: Direccionamiento del escenario de pruebas 1

Dispositivo	Interfaz	Dirección/Prefijo IPv6	Gateway Predeterminado
R1	F0/0	2001:db8:fe:1::1/64	No aplicable
	S0/0	2001:db8:fe:e001::1/64	No aplicable
	S0/1	2001:db8:fe:e003::1/64	No aplicable
R2	F0/0	2001:db8:fe:2::1/64	No aplicable
	S0/0	2001:db8:fe:e001::2/64	No aplicable
	S1/1	2001:db8:fe:e002::2/64	No aplicable
R3	F0/0	2001:db8:fe:3::1/64	No aplicable
	S0/1	2001:db8:fe:e003::2/64	No aplicable
	S1/1	2001:db8:fe:e00::1/64	No aplicable
PC Kali-pruebas-ipv6	E0/0	2001:db8:fe:1::10/64	
PC svr-dns-ipv6	E0/0	2001:db8:fe:2::10/64	
PC svr-web-ipv6	E0/0	2001:db8:fe:3::10/64	

Realizado por: Quintero Hermes, 2019.

Para ello se usa el escenario de red configurado en GNS3 de la **Figura 5-3.**

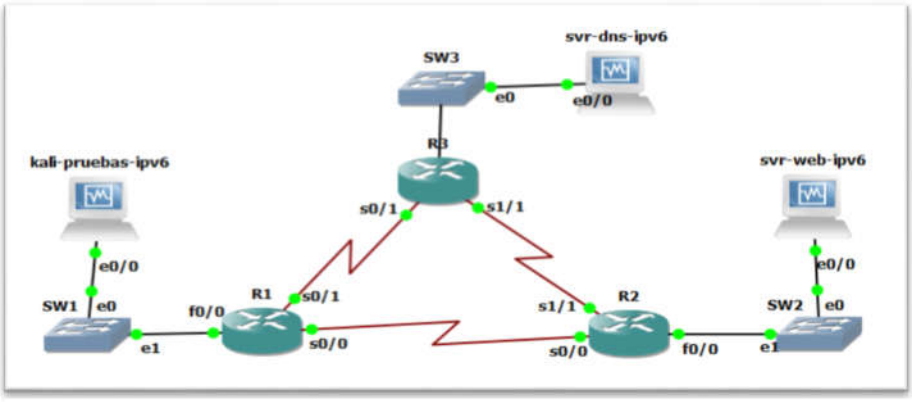


Figura 5-3: Escenario de prueba virtualizado # 1

Realizado por: Quintero Hermes, 2019.

En dicho ambiente virtualizado se configuró con 3 routers usando el direccionamiento IPv6 con prefijo 2001:db8:fe::/48 y OSPFv3 para el routing (**Ver Anexo B** – Configuraciones de Routers). En cada red interna de los routers se levanta un equipo con un sistema operativo Linux. En el momento de terminar las configuraciones de routing cada uno obtiene una dirección IPv6 de acuerdo al prefijo /64 de cada red como se demuestra en la **Figura 6-3.**

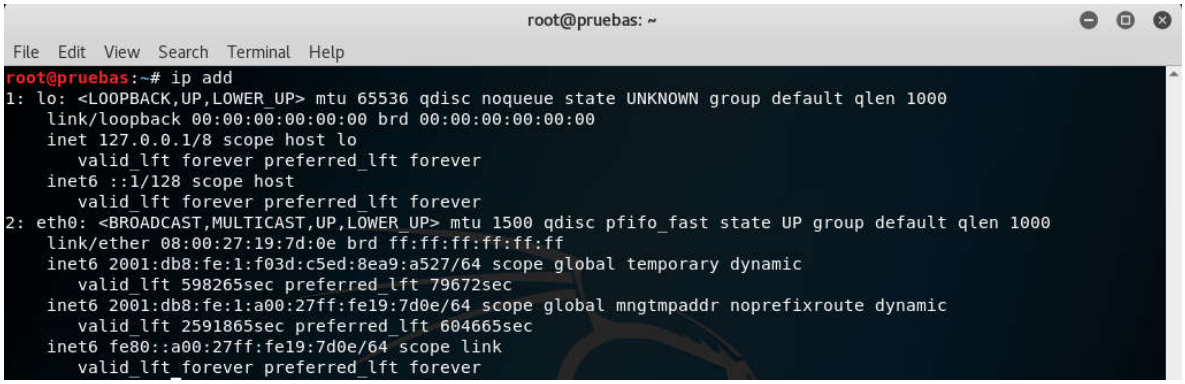


Figura 6-3: Dirección IPv6 asignada automáticamente
Realizado por: Quintero Hermes, 2019

Para configurar las direcciones IPv6 de acuerdo al esquema de direccionamiento se modifica el archivo de configuración **vi /etc/sysconfig/network-scripts/ifcfg-enp0s3** y se agregan al final los campos **IPV6ADDR** y **IPV6_DEFAULTGW** con los valores correspondientes como se muestra en la **Figura 7-3.**

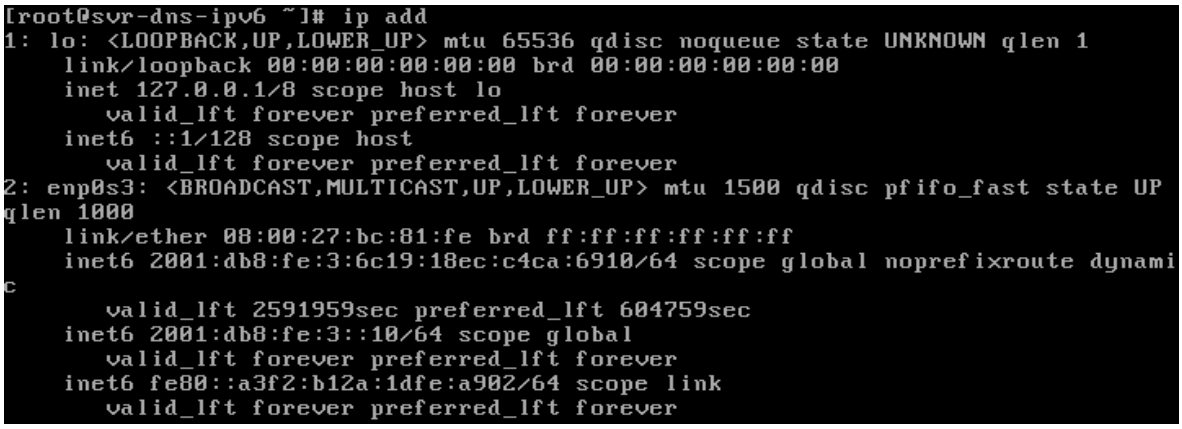


Figura 7-3: Verificación de dirección IPv6 configurada en el servidor DNS
Realizado por: Quintero Hermes, 2019.

Se reinicia el servicio con el comando "***systemctl restart network***" y el equipo queda configurado con la IPv6. Esto se lo realiza ejecutando en la consola el comando ***"ip add"*** y se lo demuestra en la **Figura 8-3**.

```
TYPE="Ethernet"
BOOTPROTO="dhcp"
DEFROUTE="yes"
PEERDNS="yes"
PEERROUTES="yes"
IPV4_FAILURE_FATAL="no"
IPV6INIT="yes"
IPV6_AUTOCONF="yes"
IPV6_DEFROUTE="yes"
IPV6_PEERDNS="yes"
IPV6_PEERROUTES="yes"
IPV6_FAILURE_FATAL="no"
IPV6_ADDR_GEN_MODE="stable-privacy"
NAME="enp0s3"
UUID="931048c7-a8d7-454f-b8d7-71a801f03c31"
DEVICE="enp0s3"
ONBOOT="yes"
IPV6ADDR=2001:DB8:FE:3::10/64
IPV6_DEFAULTGW=2001:DB8:FE:3::1
```

Figura 8-3: Configuración dirección IPv6 en servidor DNS
Realizado por: Quintero Hermes, 2019

En el primer equipo, con dirección 2001:db8:fe:2::10/64, se configura un servidor **http;** en el segundo, con dirección 2001:db8:fe:3::10/64, se configura un servidor dns. Esto se muestra en las **Figura 9-3** y **Figura 10-3** respectivamente.

```
[root@svr-web-ipv6 ~]# systemctl status httpd
● httpd.service - The Apache HTTP Server
   Loaded: loaded (/usr/lib/systemd/system/httpd.service; disabled; vendor prese
t: disabled)
   Active: active (running) since jue 2017-11-16 22:50:09 -05; 5s ago
     Docs: man:httpd(8)
           man:apachectl(8)
 Main PID: 6225 (httpd)
   Status: "Processing requests..."
   CGroup: /system.slice/httpd.service
           ├─6225 /usr/sbin/httpd -DFOREGROUND
           ├─6226 /usr/sbin/httpd -DFOREGROUND
           ├─6227 /usr/sbin/httpd -DFOREGROUND
           ├─6228 /usr/sbin/httpd -DFOREGROUND
           ├─6229 /usr/sbin/httpd -DFOREGROUND
           └─6230 /usr/sbin/httpd -DFOREGROUND

nov 16 22:50:08 svr-web-ipv6.test.com systemd[1]: Starting The Apache HTTP Se...
nov 16 22:50:09 svr-web-ipv6.test.com systemd[1]: Started The Apache HTTP Ser...
Hint: Some lines were ellipsized, use -l to show in full.
```

Figura 9-3: Estado de servicio httpd
Realizado por: Quintero Hermes, 2019.

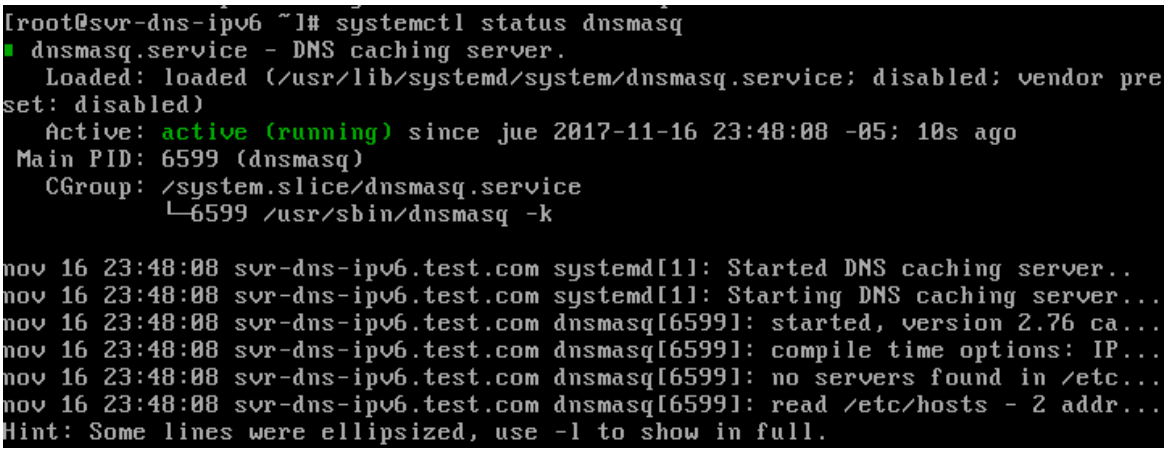


Figura 10-3: Estado de servidor dnsmasq
Realizado por: Quintero Hermes, 2019.

Las configuraciones realizadas en cada uno de los equipos se detallan en el **ANEXO C.** Con esto se propone la idea de configurar un servidor http que posee una o varias direcciones IPv6 global unicasts que serán asociadas a un dominio y guardadas en un servidor DNS público y global. Las direcciones IPv6 pueden ser configuradas por el usuario en forma manual y pueden asignarse de acuerdo a su máscara (/64 por lo general). En esta porción del ID de interfaz es donde se esconderá los mensajes de la comunicación y el usuario que cumpla el rol de emisor lo incrustará en las direcciones asociadas al servidor y luego proporcionará el dominio al receptor para que realice una revisión de contenido habitual.

El receptor revisará el contenido de la página y a la vez, hará una consulta de las direcciones IPv6 asociadas a dicho dominio. Con todas las direcciones guardadas, deberá separar la porción de red del ID de interfaz. Después, ordenará las porciones de las direcciones de acuerdo a un campo especifico y en mutuo acuerdo con el emisor.

Finalmente descifrará los caracteres escondidos en los valores hexadecimales para obtener el mensaje. Una vez realizado esto, podrá devolver una confirmación para que el emisor cambie o elimine dichas direcciones del dominio para borrar la comunicación.

3.8.3. Escenario de prueba #2

A continuación, se detalla el direccionamiento del escenario # 2:

Tabla 5-3: Direccionamiento del escenario de prueba 2

Dispositivo	Interfaz	Dirección/Prefijo IPv6	Gateway Predeterminado
PC svr-pruebaestego	E0/0	2001:db8:cafe:bebe::20/64	NA
PC cliente3_fedora	E0/1	2001:db8:cafe:bebe::100/64	NA
PC cliente4_fedora	E0/2	2001:db8:cafe:bebe::200/64	NA

Realizado por: Quintero Hermes, 2019.

Para ello se usa el escenario de red configurado en GNS3 de la Figura 11-3

.

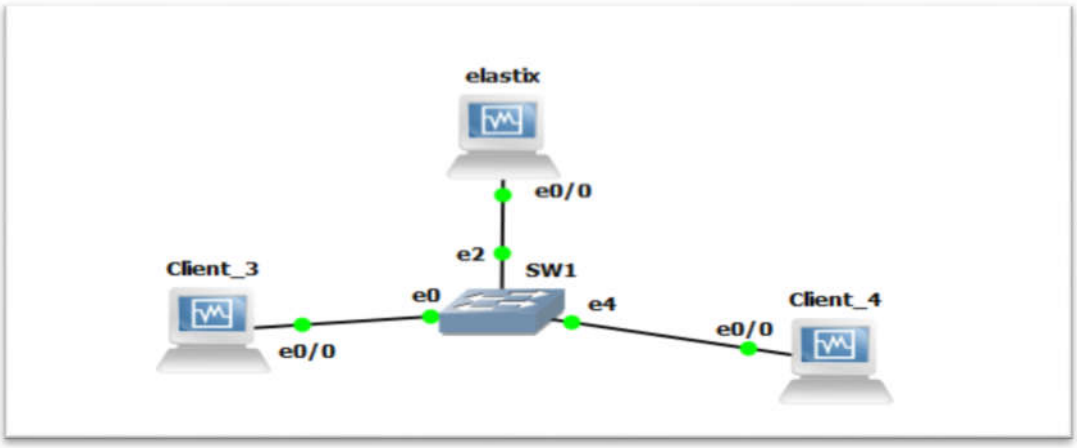


Figura 11-3: Escenario de prueba virtualizado #2
Realizado por: Quintero Hermes, 2019.

Para este segundo entorno virtualizado se configuró una central PBX con la distro-Linux ELASTIX 5.0 (**Figura 12-3**).

Figura 12-3: Instalación de Elastix-5
Realizado por: Quintero Hermes, 2019.

Una vez instalada el sistema operativo se le asigno la dirección IPv6 mediante el comando **"*ip -6 addr add* 2001:db8:café:bebe::20/64 *dev enp0s3"*** en la consola del tty1 (**Figura 13-3**). Después se verifica la dirección asignada mediante el comando **"*ip address"*** (**Figura 14-3**).

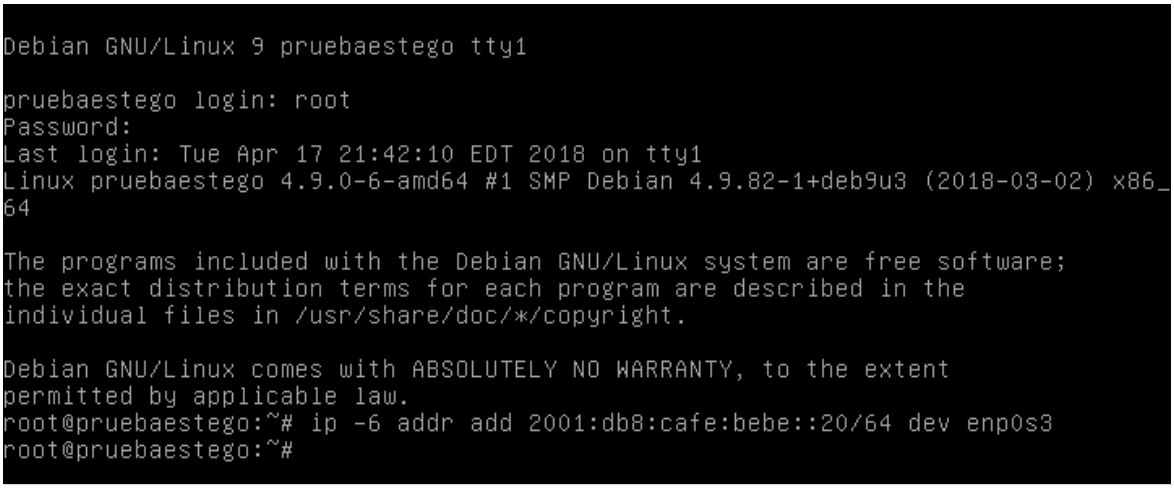


Figura 13-3: Asignación de dirección IPv6 al servidor pbx-ELASTIX
Realizado por: Quintero Hermes, 2019

Figura 14-3: Comprobación de dirección IPv6 al servidor pbx-ELASTIX
Realizado por: Quintero Hermes, 2019.

De esta manera ya está configurado y disponible el servidor pbx para ser configurado desde uno de los navegadores de los equipos clientes.En el navegador Mozilla-Firefox del cliente4 se escribe la dirección configurada para acceder al entorno web de configuración (**Figura 15-3**) se ingresa con el usuario **"*soporte*"** y su credencial.

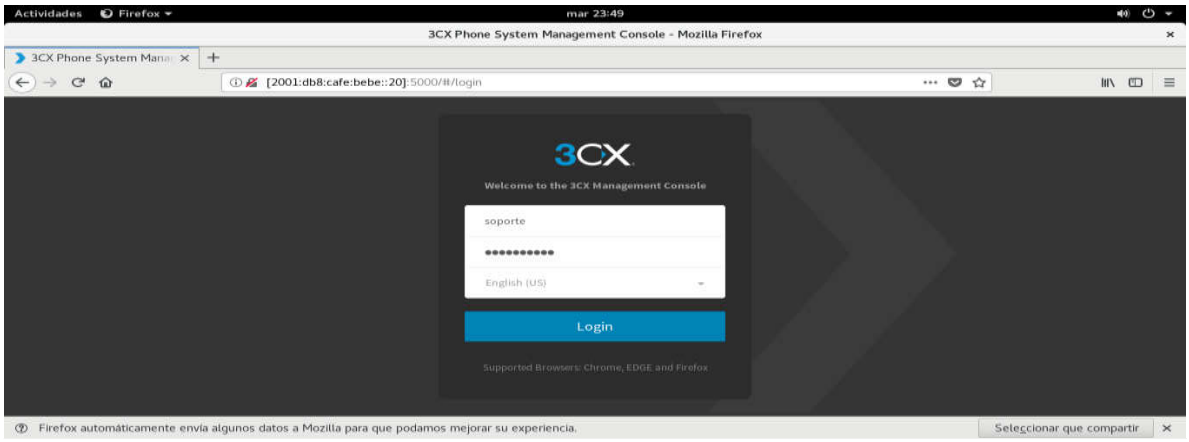


Figura 15-3: Acceso a la pbx desde el navegador del cliente4
Realizado por: Quintero Hermes, 2019.

Dentro del sistema se procede a configurar las extensiones que se utilizarán en los clientes 3 y 4 (**Figura 16-3**). Se crea la extensión 1010 con password ***"Prueba.1"*** para el cliente #3 y las extensiones 2020 con password ***"123456"*** y 5050 con password ***"654321"*** para el cliente #4. Estos valores se deben configurar en la aplicación-softphone LINPHONE en cada cliente.

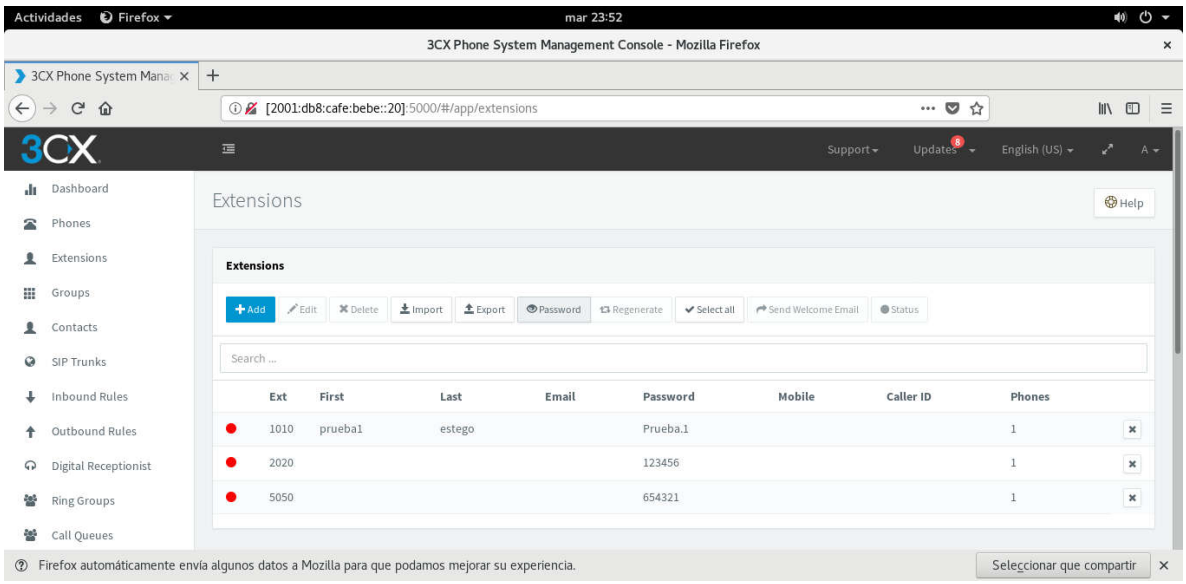


Figura 16-3: Configuración de 3 extensiones para los clientes 3 y 4
Realizado por: Quintero Hermes, 2019.

En cada cliente Fedora se instaló la aplicación LINPHONE desde la consola usando el comando "***sudo yum install linphone***". Después se usó su interfaz gráfica para realizar las configuraciones para las líneas creadas en cada uno. Primero se accede a su casilla de ***"configuration"*** y en la pestaña ***"Network settings"*** se activa la opción ***"Utilizar IPv6 en lugar de IPv4"*** para que se puedan realizar

llamadas usando el protocolo. Luego se da un clic sobre la opción ***"Done"*** para que los cambios realizados queden guardados (**Figura 17-3)**. Siempre al abrir por primera vez la aplicación, se necesita realizar esta configuración.

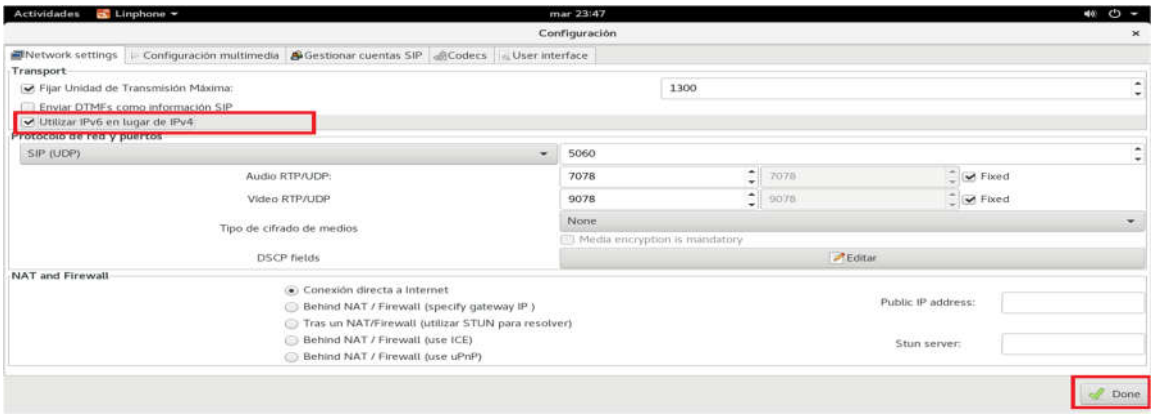


Figura 17-3: Configuración de red en LINPHONE para habilitar IPv6.
Realizado por: Quintero Hermes, 2019.

La segunda configuración de LINPHONE que se realizó está relacionada con las cuentas SIP. Para ello se selecciona la casilla de **"*configuration*"** y se accede a la pestaña de "*Gestionar las cuentas sip".* Dentro de este menú se accede a la opción "***Editar***" como lo demuestra la (**Figura 18-3**).

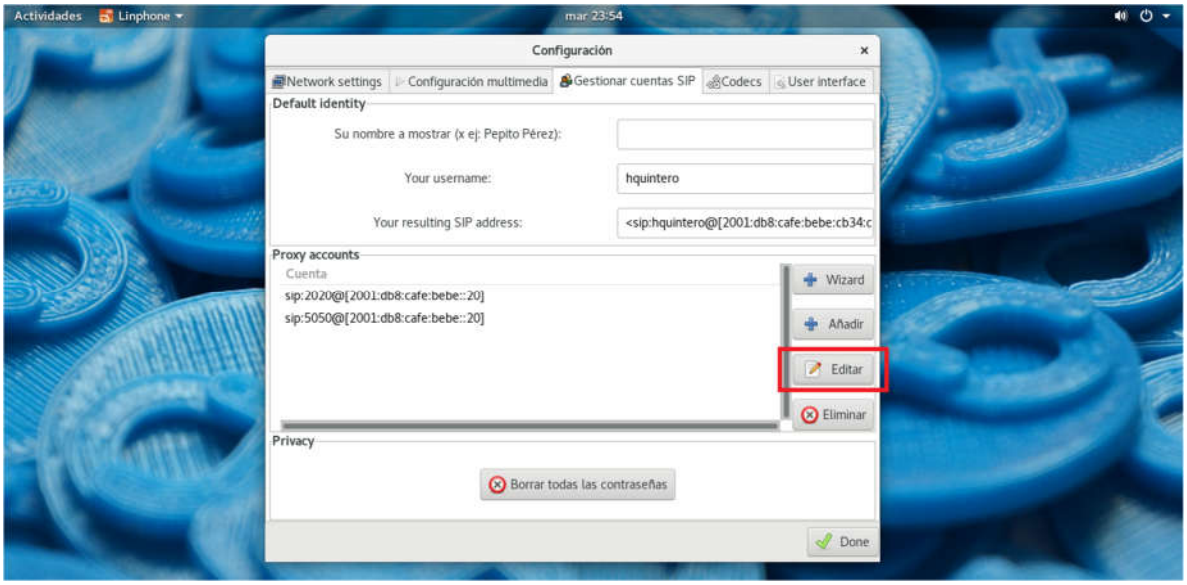


Figura 18-3: Gestión de cuentas SIP en LINPHONE.
Realizado por: Quintero Hermes, 2019.

Acto seguido a esto, se abre una ventana en donde se configuró los datos de la cuenta SIP. En la opción ***"Your SIP identify:"*** se configura el número de extensión con la dirección IPv6 del servidor pbx con el formato ***"número de extensión@dirección IPv6 del servidor entre corchetes"*** para este cliente fue ***"sip:2020@[2001:db8:cafe:bebe::20]".*** Luego en la opción ***"SIP Proxy address"*** se configura la dirección del servidor pbx de ELASTIX, ***"<sip:[2001:db8:cafe:bebe::20]>"*** ; para guardar los cambios se da clic en aceptar (**Figura 19-3**). Este procedimiento se realizó en cada cliente Fedora con sus respectivos datos.

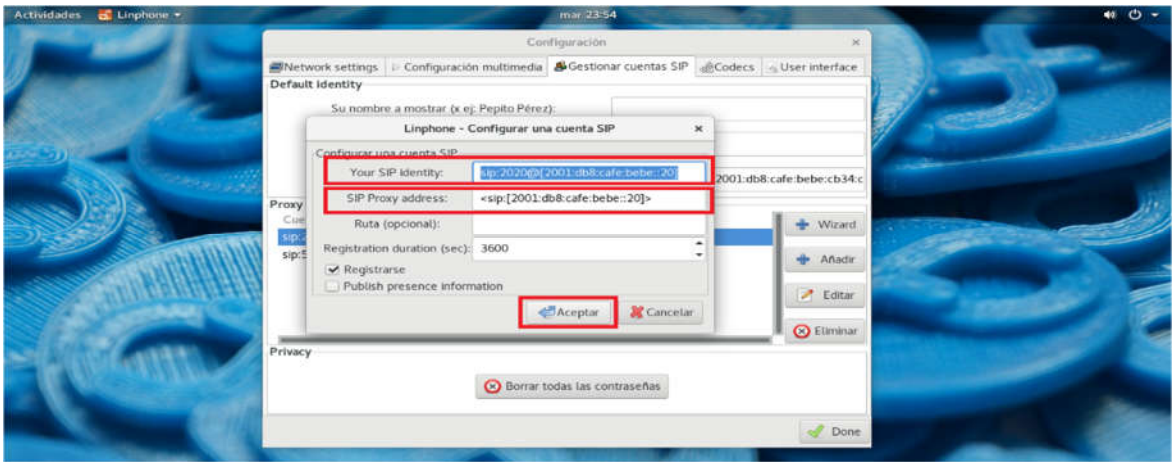


Figura 19-3: Configuración de una cuenta SIP en LINPHONE.
Realizado por: Quintero Hermes, 2019.

Con las configuraciones guardadas, en la ventana principal de LINPHONE, en la parte inferior se muestra un mensaje de registro exitoso de la cuenta SIP. En las figuras **Figura 20-3** para el cliente Fedora 3 y en la **Figura 21-3** para el cliente Fedora 4.

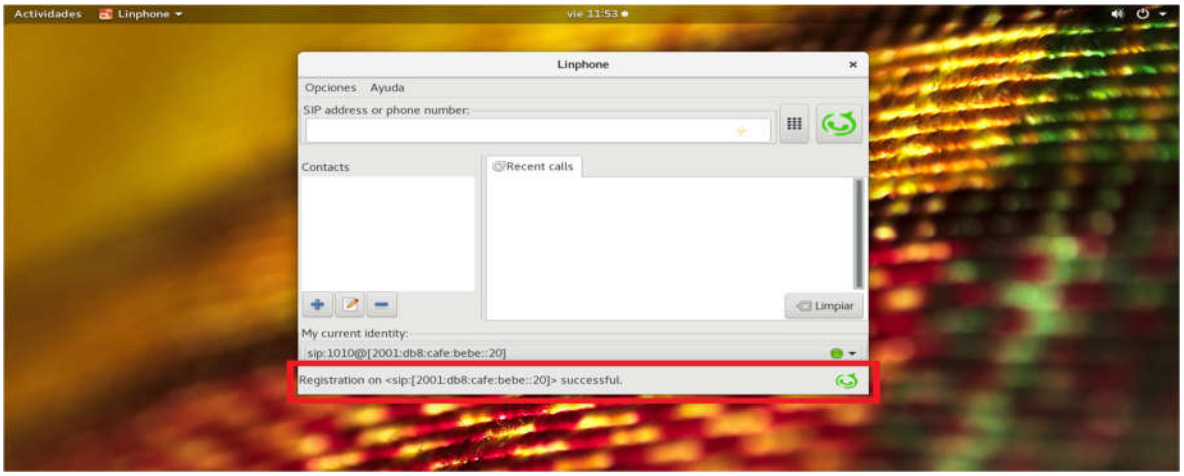


Figura 20-3: Captura registro exitoso de la cuenta SIP en cliente 3
Realizado por: Quintero Hermes, 2019.

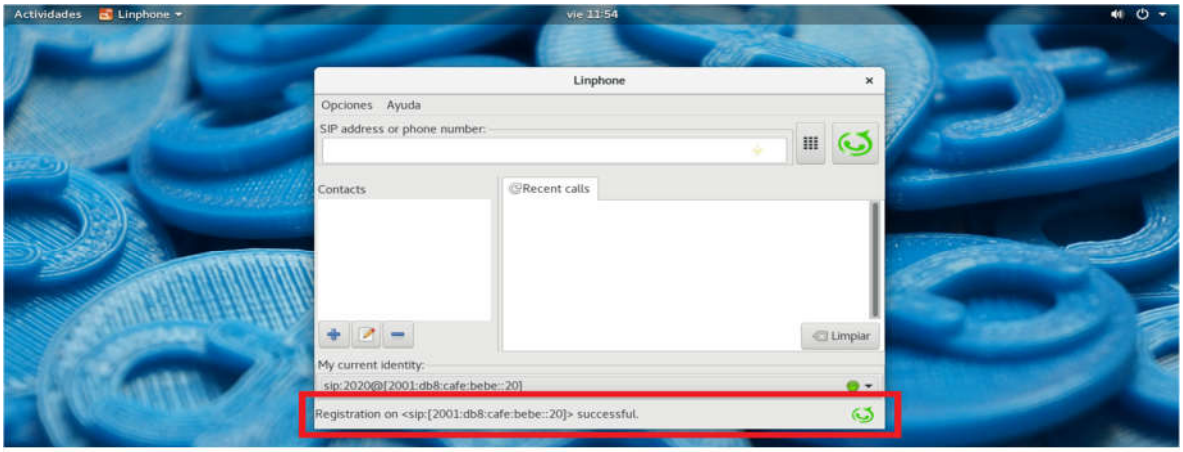


Figura 21-3: Captura registro exitoso de la cuenta SIP en cliente 4.
Realizado por: Quintero Hermes, 2019.

En este segundo escenario se demuestra el uso del servicio de VoIP por medio de llamadas usando un softphone que soporta el protocolo IPv6. Los usuarios pueden configurar sus direcciones IPv6 en sus equipos y ocultar sus mensajes en la parte que le corresponde al ID de interfaz, sin alterar el funcionamiento de las extensiones o llamadas para establecer una comunicación secreta.

3.9. Identificación de variables

En la **Tabla 6-3** se identifica las variables independiente y dependiente en base a la hipótesis planteada en esta investigación:

Tabla 6-3: Identificación de variables

HIPÓTESIS	VARIABLE	TIPO	CONCEPTO
El uso de esteganografía en el protocolo IPv6 usando mensajes ocultos es una alternativa para una comunicación segura.	**INDEPENDIENTE**	Esteganografía en el protocolo IPv6.	La esteganografía trata el estudio y aplicación de técnicas que permiten a los usuarios ocultar mensajes de modo que no se percibirá su existencia por un sistema, observador o vigilante.
	DEPENDIENTE	Comunicación segura	Medidas adoptadas para proteger la información digital de accesos no autorizados, uso, divulgación, interrupción, modificación o destrucción.

Realizado por: Quintero Hermes, 2019.

3.10. Operacionalización de las variables

Tabla 7-3: Operacionalización de variables

HIPOTESIS GENERAL	VARIABLES	INDICADORES
El uso de esteganografía en el protocolo IPv6 usando mensajes ocultos es una alternativa para una comunicación segura.	Independiente: Esteganografía en el protocolo IPv6.	Cantidad de paquetes IPv6 enviados. Capacidad de información enviada. Coste esteganográfico (CE). Robustez.
	Dependiente: Comunicación segura.	Cantidad de paquetes IPv6 recibidos. Indetectabilidad. Integridad.

Realizado por: Quintero Hermes, 2019.

3.11. Matriz de consistencia

Tabla 8-3: Matriz de consistencia

Objetivo General	Hipótesis General	Variables	Indicadores	Índices	Técnicas	Instrumentos
Analizar el uso de esteganografía en el protocolo IPv6 usando mensajes ocultos para una comunicación segura.	El uso de esteganografía en el protocolo IPv6 usando mensajes ocultos es una alternativa para una comunicación segura.	Esteganografía en el protocolo IPv6.	Cantidad de Paquetes IPv6	Número de paquetes enviados.	Pruebas. Toma de datos Captura de tráfico. Observación.	. VirtualBox Wireshark. GNS3.
			Capacidad de información enviada.	Cantidad de caracteres por paquete		
			Coste esteganográfico	% de detección		
			Robustez	No. De direcciones IPv6.		

		Comunicación segura	Cantidad de Paquetes IPv6 recibidos.	Cantidad de paquetes recibidos.	Pruebas. Observación. Análisis.	Kali-Linux. VirtualBox Wireshark. GNS3.
			Integridad	Cantidad de caracteres ordenados recibidos		
			Indetectabilidad	1 - CE		

Realizado por: Quintero Hermes, 2019.

3.12. Procesamiento y análisis para la información

3.12.1. Plan de recolección de información

La información obtenida y recolectada se analizó y comparó entre los dos escenarios implementados, lo cual permitió determinar los valores de los indicadores propuestos. En la presente investigación se utilizó las siguientes técnicas para la recolección de información:

- **Análisis de contenido:** Esta técnica se realizó una investigación sobre la metodología y técnicas propuestas para el desarrollo de un mecanismo esteganográfico. La información fue recolectada de libros, artículos científicos, internet, entre otros.
- **Pruebas de funcionabilidad:** Con el uso de esta técnica se realizaron las configuraciones necesarias en los dos escenarios de prueba haciendo uso de las aplicaciones GNS3 y VIRTUALBOX.
- **Observación:** Permitió obtener la información sobre la cantidad de paquetes enviados y recibidos, así como también el mensaje oculto en la dirección IPv6 propuesto en los escenarios de prueba. Esta información fue recolectada mediante la captura de tráfico con la herramienta WIRESHARK y KALI-LINUX.

3.12.2. Plan de procesamiento de información

Para el análisis y procesamiento de la información compilada se llevan a cabo los siguientes pasos:

1. La información obtenida es revisada y ordenada de acuerdo a cada indicador de la variable dependiente en figuras o gráficos estadísticos descriptivos para facilitar la compresión de los resultados. Para su análisis se efectúa una matriz de datos utilizando el programa computacional Microsoft Office Profesional Excel 2016 para posteriormente realizar una interpretación de los mismos.
2. Se verifica la hipótesis propuesta a través de la varianza de los datos para verificar la fiabilidad de la información y después la relación que existe entre ellas mediante la prueba estadística

3.13. Planteamiento de la Hipótesis

El uso de esteganografía en el protocolo IPv6 usando mensajes ocultos es una alternativa para una comunicación segura.

CAPÍTULO IV

4. RESULTADOS Y DISCUSIÓN

4.1. Demostración del mecanismo esteganográfico sobre el protocolo IPv6

En base al diseño creado y tomando el escenario del problema de los prisioneros de la figura 15-2, se demuestra el uso de la esteganografía usando el protocolo IPv6 con el objetivo de enviar el mensaje secreto "*Lunes Reunión en el parque central 3 pm*".

El punto de partida está en la cantidad de información que se quiere enviar. Se tiene 32 caracteres (sin contar los espacios) y es menor que la capacidad máxima de información a transmitir. Ahora se determina la cantidad de direcciones de acuerdo a la forma de configurar la porción de ID de la dirección global Unicast IPv6, esto se detalla en la **Tabla 1-4**.

Tabla 1-4: Cantidad de direcciones global unicast

Fórmula Cantidad de direcciones global unicast	Configuración de dirección global Unicast	Valores	Cantidad de direcciones global unicast
$\frac{cantidad\ de\ caracteres}{número\ de\ campos\ disponibles}$	Estática /64 Aleatoria	$\frac{32}{7} = 4.57$	5 direcciones
	EUI-64	$\frac{32}{5} = 6.4$	7 direcciones

Realizado por: Quintero Hermes, 2019.

Si el resultado de la relación no es entero, se redondea el valor mayor de la cantidad de direcciones y los espacios que sobren se rellenan con valores aleatorios. Para efectos de esta investigación se tomó las direcciones generadas por el valor aleatorio (segunda fila de la **Tabla 1-**4) y el mensaje secreto en las direcciones generadas se detallan en la **Tabla 2**-4 para el escenario 1 y en la**Tabla 3-4** para el escenario 2.

Tabla 2-4: Direcciones globales con mensaje secreto para el escenario 1

Caracteres a enviar	Estegograma con valor hexadecimal	Dirección generada
lunesre	6c:75:6e:65:73:72:65	2001:db8:fe:2:6c75:6e65:7300:7265/64
unionen	76:6e:69:6f:6e:65:6e	2001:db8:fe:2:766e:696f:6e01:656e/64
elparqu	65:6c:70:61:72:71:75	2001:db8:fe:2:656c:7061:7202:7175/64
ecentra	65:63:65:6e:74:72:61	2001:db8:fe:2:6563:656e:7403:7261/64
l3pm0a9	6c:33:70:6d:30:61:39	2001:db8:fe:2:6c33:706d:3004:6139/64

Realizado por: Quintero Hermes, 2019.

Tabla 3-4: Direcciones globales con mensaje secreto para el escenario 2

Caracteres a enviar	Estegograma con valor hexadecimal	Dirección generada
lunesre	Fe:d7:11:cb:dd:12:cb	2001:db8:cafe::bebe:fed7:11cb:ddff:12cb
unionen	D7:cb:a0:8f:cb:cb:11	2001:db8:cafe::bebe:d7cb:a08f:cbfe:cb11
elparqu	Cb:fe:77:e4:12:d0:d7	2001:db8:cafe::bebe:cbfe:77e4:12fd:d0d7
ecentra	Cb:34:cb:11:aa:12:e4	2001:db8:cafe::bebe:cb34:cb11:aafc:12e4
l3pm0a9	Fe:e5:77:ab:6b:fa:e4	2001:db8:cafe::bebe:fee5:77ab:6bfb:fae4

Realizado por: Quintero Hermes, 2019.

Con esto se obtiene un total de 5 direcciones a utilizar para configurar y utilizar en cada escenario.

4.1.1. Demostración en escenario 1

En el escenario 1, en el equipo del emisor se levanta un servidor http que implementa una página con contenido con el objetivo de ser un distractor o encubridor. Al trabajar con direcciones globales este contenido, a través de su IPv6, se lo asocia con un dominio al que se denominó **www.maestria2017.com** y se registran las 5 direcciones IPv6 en el servidor DNSMASQ global como lo demuestra la **Figura 1-4**.

Figura 1-4: Registro de servidor web en DNS
Realizado por: Quintero Hermes, 2019.

El objetivo de asociar nuestras direcciones globales a un dominio es enviar a nuestro receptor un mensaje que incluya la dirección **www.maestria2017.com** como una revisión rutinaria de consulta en un sitio en la web para no levantar sospechas de los mensajes ocultos. El receptor en su equipo, (usando la distro KALI-LINUX como sistema operativo en este ejemplo), accede a este contenido desde su navegador normalmente como lo muestra la **Figura 2-4.**

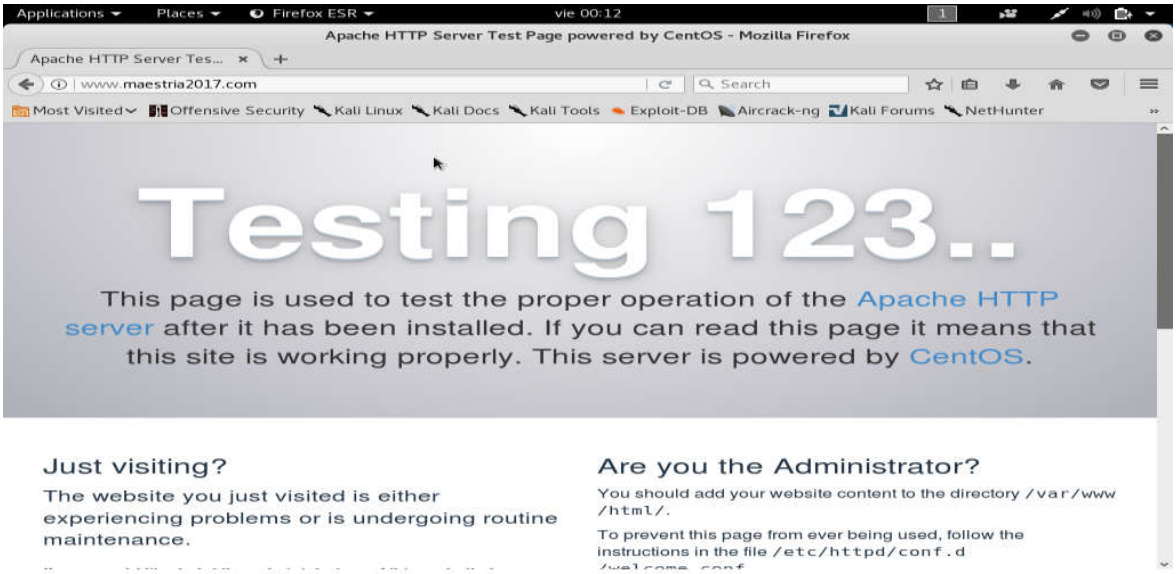


Figura 2-4: Acceso al servidor web desde equipo Kali-Linux
Realizado por: Quintero Hermes, 2019.

Después de verificar la existencia y navegar en el sitio, el receptor del mensaje en un terminal de KALI-LINUX, realiza la consulta de las direcciones asociadas a este sitio web usando el comando "***host –t AAAA www.maestria2017.com***". Esto se ilustra en la **Figura 3-4**. La consulta realizada es de record AAAA, con lo cual nos da todas las direcciones IPv6 asociadas al sitio. Se presentan seis direcciones IPv6; de ellas la primera la de configuración inicial y las otras cinco con el mensaje incrustado. Nótese que las direcciones se encuentran en desorden.

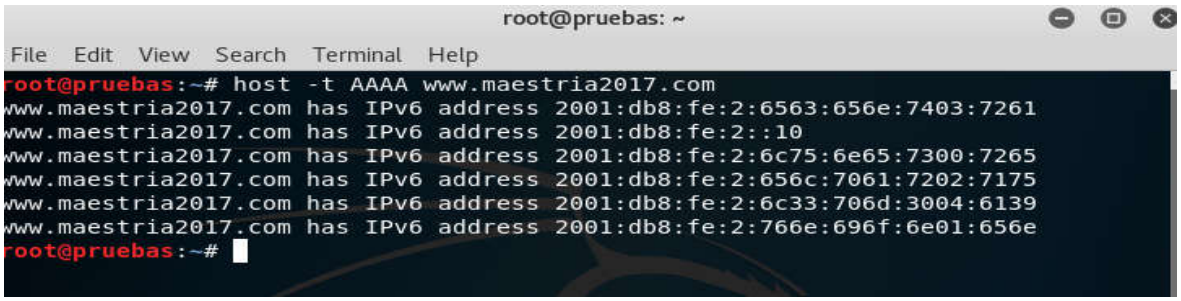


Figura 3-4: Consulta de direcciones globales asociadas a servidor web
Realizado por: Quintero Hermes, 2019.

En la captura de todo el tráfico de la interfaz realizada por Wireshark de la ***Figura 4-4*** también se puede observar que el paquete número 172 realiza una consulta de tipo AAAA al servidor DNS sobre el dominio www.maestria2017.com y en el paquete 173 se obtiene una respuesta de ella con el contenido de seis direcciones IPv6 asociadas al dominio y registradas en el servidor DNS.

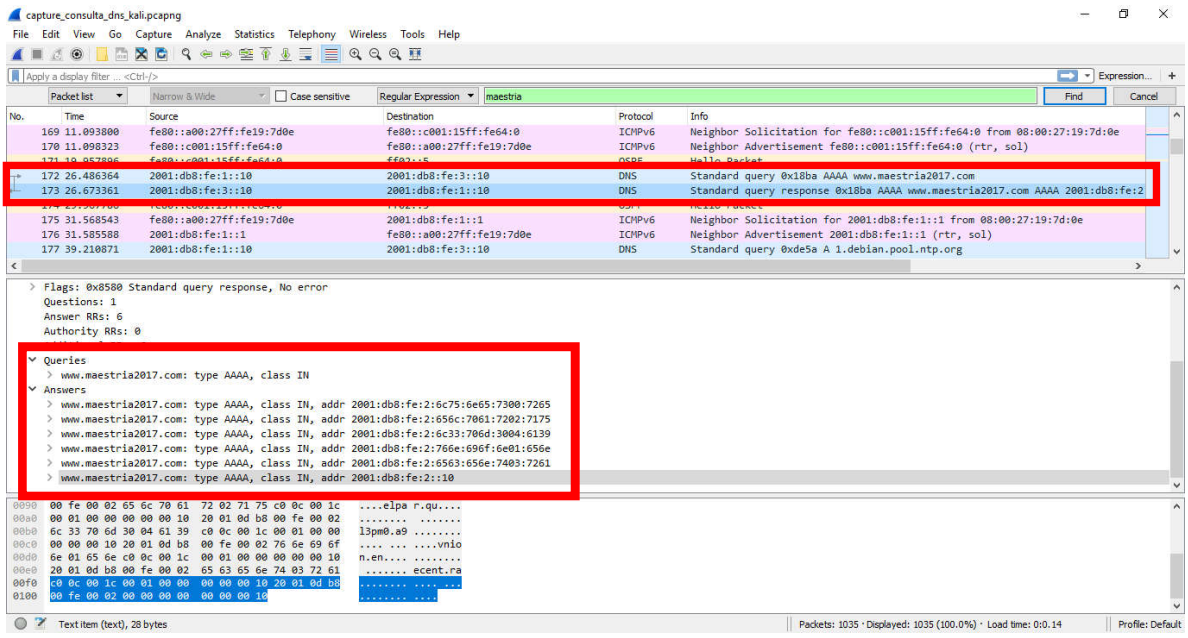


Figura 4-4: Captura de tráfico de consulta DNS del dominio www.maestria2017.com
Realizado por: Quintero Hermes, 2019.

Ahora nuestro destinatario puede reordenar las direcciones de acuerdo al sexto campo, separar la porción de la dirección global unicast que corresponde a los primeros 64 bits, luego realizar la conversión de hexadecimal a ASCII y leer el mensaje "*Lunesreuniónenelparquecentral3pm0a9*". Después de esto, deberá enviar un mensaje de confirmación que ha revisado la página y el emisor

podrá eliminar los registros de las direcciones asociadas al dominio **www.maestria2017.com** y cambiarlos para evitar dejar rastros.

4.1.2. Demostración en escenario 2

En este escenario se aplica el mecanismo esteganográfico en el intercambio de llamadas de una central telefónica que usa el protocolo SIP sobre IPv6. En cada cliente se tiene configurada y habilitada una cuenta SIP en el servidor pxb ELASTIX y cada cliente tiene asignada inicialmente una dirección IPv6 como se muestra en la **Figura 5-4** y **Figura 6-4.**

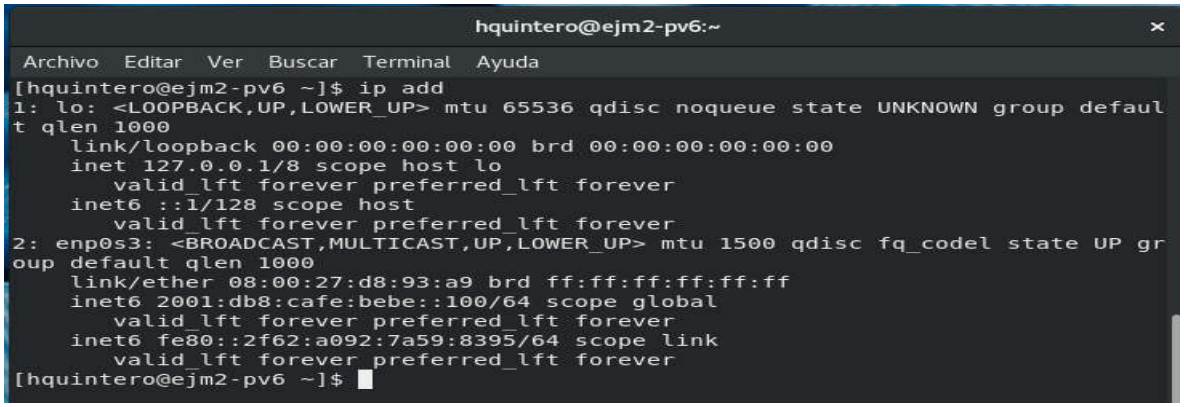


Figura 5-4: Dirección IPv6 asignada al cliente 4
Realizado por: Quintero Hermes, 2019.

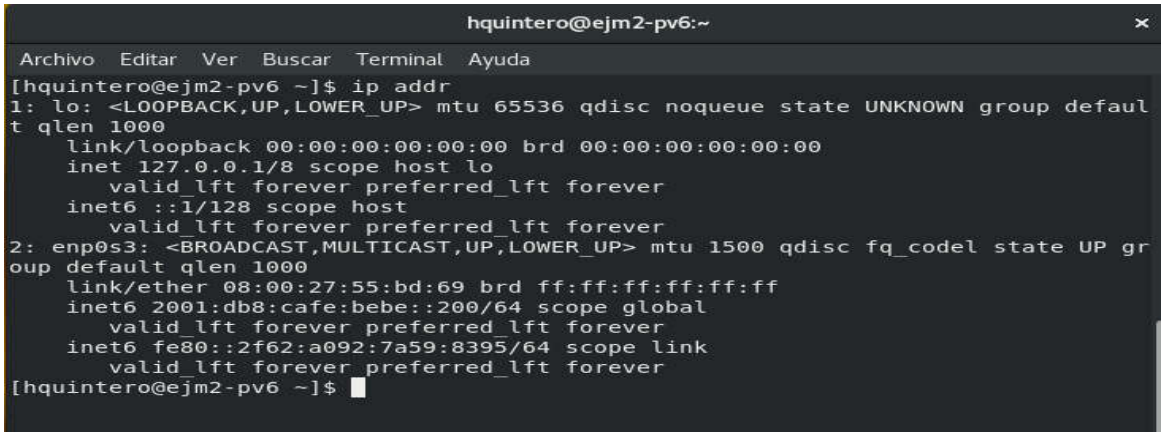


Figura 6-4: Dirección IPv6 asignada para el cliente 3
Realizado por: Quintero Hermes, 2019.

Luego de esto se realiza una llamada desde la extensión 1010 hacia la extensión 5050 como prueba para verificar el servicio. Esto se lo demuestra en la **Figura 7-4**. En esta se puede apreciar que, al realizar la llamada, en la interfaz gráfica de LINPHONE solo aparece el número de extensión desde donde se realiza la llamada y la dirección IPv6 del servidor pbx.

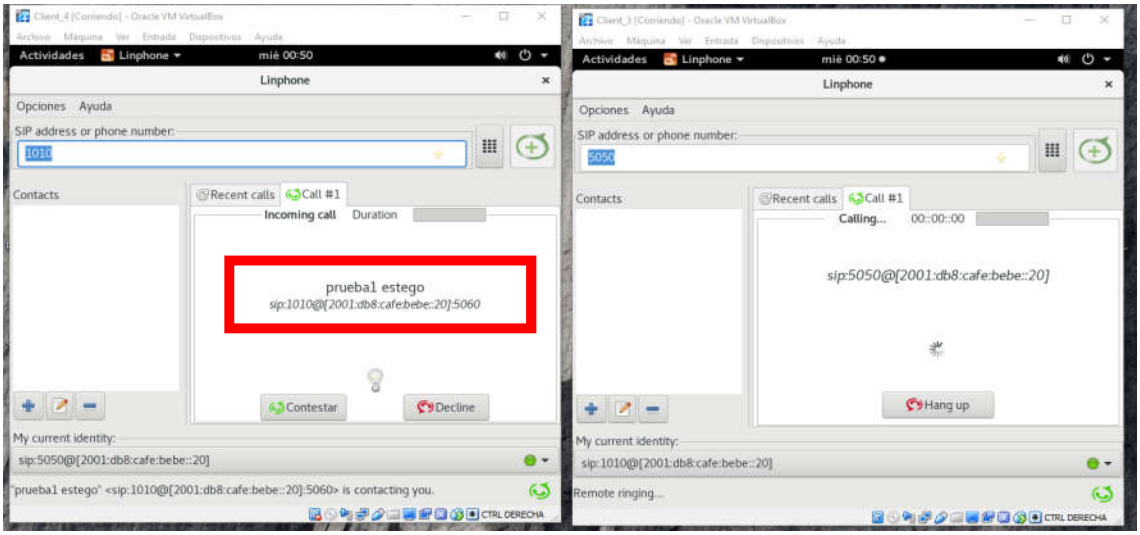


Figura 7-4: Llamada de prueba desde la extensión 1010 hacia la 5050.
Realizado por: Quintero Hermes, 2019.

La dirección IPv6 del cliente 4, donde está configurada la extensión 1010, no aparece en la interfaz de LINPHONE y no es considerada por el usuario; es permitida en el entorno de red y en la central pbx para ser usada en la llamada. Esto permite que se pueda usar el mecanismo de esta investigación para enviar el mensaje secreto y este pase desapercibido.

Entonces en el cliente 4 se asigna las direcciones obtenidas en la**Tabla 3-4** antes de realizar una llamada. Para ello se escribe en consola el comando ***"sudo vi /etc/sysconfig/network-scripts/ifcfg-enp0s3",*** se edita y guarda la dirección IPv6 y luego se ejecuta el comando ***"systemctl network restart"*** para aplicar los cambios. Esto se muestra en la **Figura 8-4.**

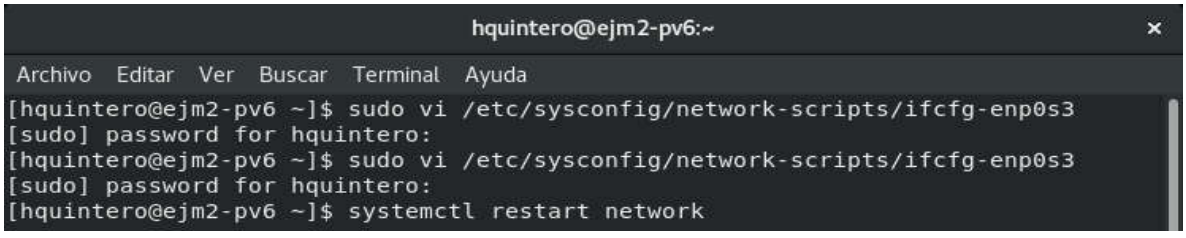


Figura 8-4: Configuración de dirección IPv6 en el cliente 3
Realizado por: Quintero Hermes, 2019.

De lo expuesto de la **Tabla 3-4** se necesitan cinco direcciones para lograr enviar el mensaje. Para esto, se necesita realizar cinco llamadas, en las cuales se puede dialogar sobre asuntos normales o cotidianos para no levantar sospechas. Cada vez que el cliente 4 realice una llamada al cliente 3, este está capturando tráfico de cada llamada con la aplicación de WIRESHARK desde la extensión 1010. En la **Figura 9-4** se muestra la captura de la primera llamada **(**Las capturas de todas las llamadas y configuraciones se adjuntan en el **ANEXO D).**

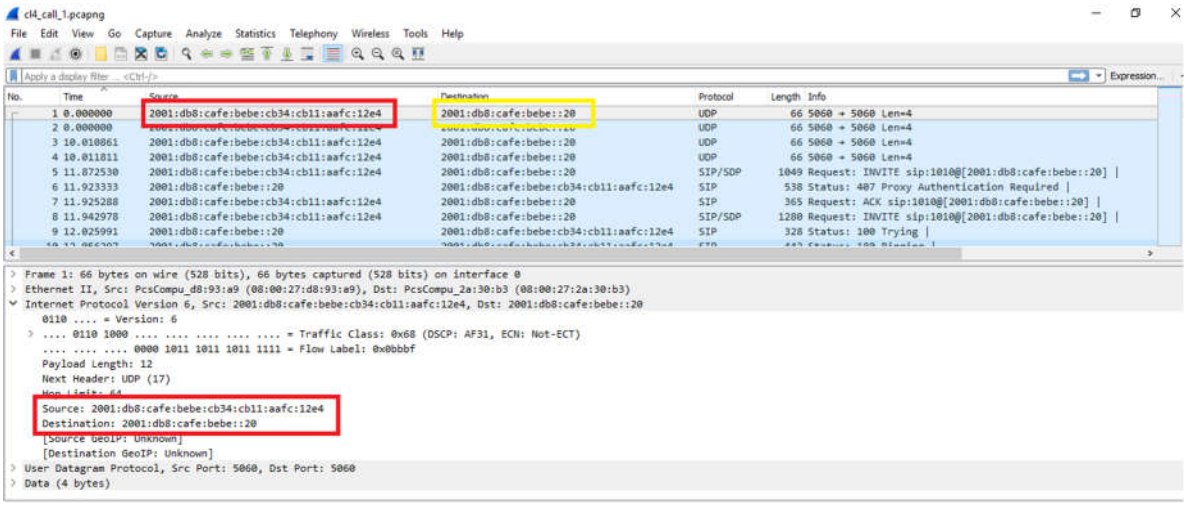


Figura 9-4: Captura con WIRESHARK de la llamada #1
Realizado por: Quintero Hermes, 2019.

En esta captura se puede identificar el proceso de una llamada normal entre dos direcciones IPv6, en la cual, la dirección de origen contiene el **estegograma.** Nótese que se utilizó el alfabeto codificado en un ***"diccionario estático"***. Tampoco es significante configurar las direcciones en orden secuencial antes de realizar una llamada, incluso se podría incluir algunas llamadas como distractores.

Luego, el receptor deberá tomar las direcciones capturadas de las cinco llamadas, separar la porción del estegograma, ordenar las porciones de acuerdo al campo 6 y finalmente realizar la conversión de cada campo con el diccionario estático para descifrar el mensaje oculto "*Lunesreuniónenelparquecentral3pm0a9*".

4.2. Evaluación del mecanismo esteganográfico diseñado

El mecanismo esteganográfico diseñado en esta investigación empleando el protocolo IPv6 fue demostrado en dos escenarios distintos usando dos servicios diferentes a través de la configuración de la dirección IPv6 del emisor. Sus resultados se contrastan en el cuadro comparativo de la **Tabla 4-4**.

Tabla 4-4: Cuadro comparativo del mecanismo esteganográfico desarrollado

	Escenario 1	Escenario 2
Arquitectura utilizada	Cliente-servidor	
Estegograma	Porción de identificador de interfaz de host de la dirección IPv6 del emisor	
Estegofunción	Configuración manual de la dirección IPv6 del emisor.	
Técnica esteganográfica	Sustitución	
Alfabeto	Valores representados en hexadecimal/ASCII	Diccionario estático
Servicio utilizado	1 consulta DNS	5 llamadas SIP
Portador	Protocolo DNS	Protocolo SIP
Campo utilizado en el paquete	Campo **answer** del paquete DNS response, previo registro de direcciones IPv6 de un servicio web.	Dirección de origen IPv6

Realizado por: Quintero Hermes, 2019.

De acuerdo a esta tabla, se obtienen los siguientes resultados:

- Ambos escenarios usan una arquitectura cliente-servidor con servicios válidos para ejecutarse en un entorno de red supervisado que utiliza guardianes activos o normalizadores de tráfico.
- Los caracteres del mensaje secreto codificados de ASCII a hexadecimal aumentan el riesgo de ser descubierto, debido a que su tabla de conversión va en un rango numérico secuencial (desde 61 hasta 7A para las letras y desde el 30 hasta el 39 para los números). La codificación del alfabeto disminuiría este riesgo (uso de un diccionario estático).
- En el escenario 2 se puede lograr una comunicación DUPLEX, ya que tanto emisor y receptor pueden intercambiar mensajes durante una llamada.

Para evaluar al mecanismo diseñado se consideran como indicadores a los resultados de los parámetros: *cantidad de paquetes enviados y recibidos, ancho de banda esteganográfico, indetectabilidad, coste esteganográfico y robustez*.

4.3. Análisis de resultados

Después de realizar la demostración del uso de esteganografía en los dos escenarios usando el protocolo IPv6; a continuación, se analizan sus resultados usando la estadística descriptiva para cada uno de los indicadores detallados en las variables de investigación.

4.3.1. Cantidad de paquetes enviados y recibidos

De acuerdo a las capturas de tráfico de la aplicación WIRESHARK en cada escenario (**ANEXO E-F),** se puede observar en la **Tabla 5-4** y **¡Error! No se encuentra el origen de la referencia.-4** los resultados obtenidos de las pruebas realizadas con relación al indicador *cantidad de paquetes enviados y recibidos*.

Tabla 5-4: Cantidad de paquetes enviados y recibidos del escenario 1

Protocolo DNS	Número de paquetes enviados	Número de paquetes recibidos	Total de paquetes utilizados
Consulta de dominio	1	1	2

Realizado por: Quintero Hermes, 2019.

Tabla 6-4: Cantidad de paquetes enviados y recibidos del escenario 2

Protocolo SIP	Número de paquetes enviados	Número de paquetes recibidos	Total de paquetes utilizados
1ra Llamada	5	5	10
2da Llamada	6	6	10
3ra Llamada	6	6	12
4ta Llamada	6	6	12
5ta Llamada	6	16	12
Totales	29	39	68

Realizado por: Quintero Hermes, 2019.

Para su análisis se ha seleccionado el promedio de paquetes enviados y recibidos, de los cuales se puede evidenciar que en el escenario 1 se utiliza una menor cantidad en promedio de paquetes que el escenario 2. En el **Gráfico 1-4** se puede observar esta diferencia de cantidad de paquetes usados. Esto favorece a la cualidad de no levantar sospechas, aunque involucra mayores procedimientos a realizar (asignar varias direcciones IPv6 a un servidor web, obtener un dominio, registrar el dominio con las direcciones IPv6 asignadas).

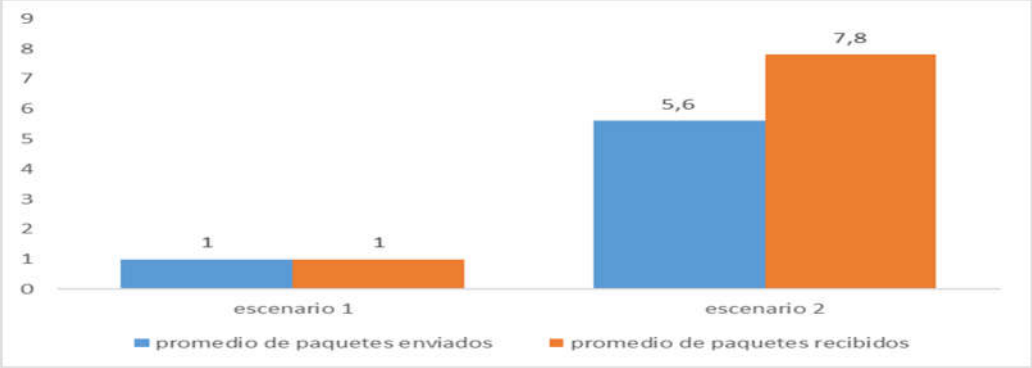


Gráfico 1-4: Paquetes promedio enviados y recibidos
Realizado por: Quintero Hermes, 2019.

4.3.2. Capacidad o ancho de banda esteganográfico

La cantidad de información que se puede ocultar en una dirección IPv6 (portador) depende de la forma en que se configura. De acuerdo a una configuración manual estática es posible incrustar 7 caracteres a cada dirección y 5 por medio de EUI-64. Siendo cada carácter codificado en 8 bits o dos valores hexadecimales del identificador de interfaz. Esto se representa en la **Tabla 7-4.**

Tabla 7-4: Cantidad de direcciones IPv6

Capacidad de información a transmitir	Configuración de dirección global Unicast	Valores	Capacidad máxima de información a transmitir
(número de caracteres que se pueden transmitir)*(cantidad de direcciones con estegograma)	Estática /64	(7)*(5)* =	35 caracteres
	EUI-64	(5)*(5) =	25 caracteres

Realizado por: Quintero Hermes, 2019.

De acuerdo a esto, se determina un porcentaje del 40% mayor de capacidad al usar un estegograma configurado de forma manual estática. En el **Gráfico 2-4** se puede apreciar este resultado de las 5

direcciones utilizadas en total. Se obtiene un ancho de banda aceptable y válido para enviar mensajes ocultos.

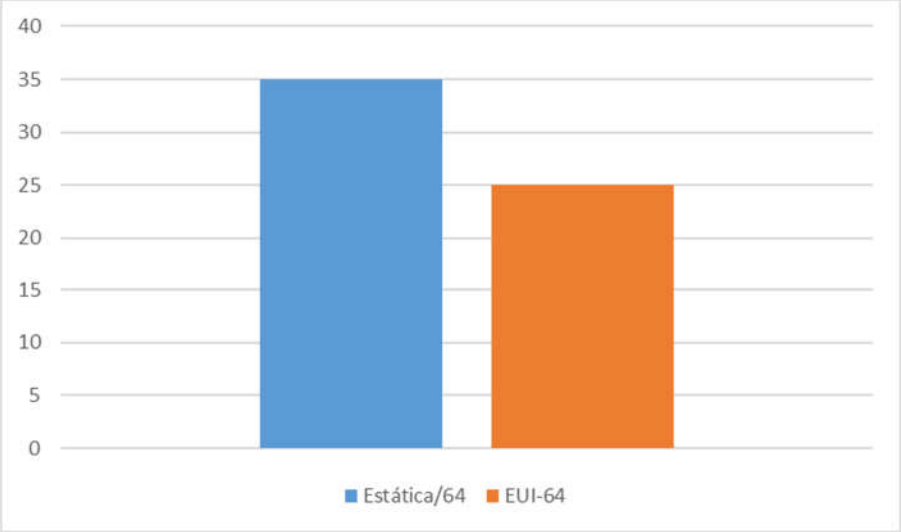


Gráfico 2-4: Gráfico de resultados de comparación de la cantidad de caracteres a transmitir
Realizado por: Quintero Hermes, 2019.

4.3.3. Indetectabilidad

La indetectabilidad está relacionada en la probabilidad de detección que posee el estegograma en el medio portador. Para el mecanismo diseñado se considera lo detallado en la **Figura 10-4,** en la cual CDE representa el conjunto de direcciones para asignar un mensaje secreto y CDT el conjunto total de direcciones IPv6 disponibles para calcular la probabilidad de escoger una de las direcciones IPv6 usadas con un estegograma en una inspección o análisis (TRIOLA, 2009, págs. 136-179).

Probabilidad de detección del mecanismo esteganográfico.	Valores	Resultado en término de probabilidad
$P(\mathbf{A}) = \frac{CDE}{CDT}$	$P(A) = \frac{5}{18446744073709600000}$	0,00000000000000000000271050543121

Figura 10-4: Probabilidad de detección de una dirección IPv6 para los escenarios
Realizado por: Quintero Hermes, 2019.

Para los dos escenarios se tiene una cantidad de 5 direcciones a utilizar que corresponden a CDE y una cantidad de 18446744073709600000 de direcciones disponibles que se asignan a CDT. Teniendo como resultado una probabilidad de $2{,}71051*10^{-19}$ de detección para las direcciones IPv6 utilizadas para enviar el mensaje en esta investigación.

Una vez calculado la probabilidad de detección, se calcula la capacidad de indetectabilidad esteganográfica P(Ā) como se indica en la **Figura 11-4** como la diferencia del todo. Se usa la regla de los sucesos complementarios de probabilidad donde **P(A) + P(Ā) = 1**, al considerar que el complemento de la detectabilidad sería la no detectabilidad (indetectabilidad).

Probabilidad de no detectabilidad	Valores	Resultado en término de probabilidad.
P(Ā)= 1 - P(A)	P(Ā)= 1 – $2{,}71051*10^{-19}$	99,99999999999999999972894946 %

Figura 11-4: Probabilidad de no detectabilidad de una dirección IPv6 con estegograma
Realizado por: Quintero Hermes, 2019.

Con este resultado se concluye que el mecanismo implementado cumple casi al 100% de ser indetectable.

4.2.3. Robustez

Para medir la robustez del mecanismo analizado se consideró el criterio de mantener la integridad de la información, para ello se utilizó 8 bits o dos valores hexadecimales de la porción de identificador de la dirección IPv6 como campo de ordenamiento e indicador de modificación para mantener la integridad del mensaje. Se designó el sexto campo de la dirección para tal propósito, comenzando desde el valor ***FF*** hasta ***00*** (en secuencia descendente).

Por lo tanto, se podría enviar los estegogramas en desorden para despistar alguna supervisión o análisis, si su contenido es alterado o en caso de reenviar una dirección especifica que se haya perdido. Se tendría un conjunto de 256 direcciones como máximo para enviar mensajes ocultos.

4.3. Comprobación de la hipótesis

Para la demostración de la hipótesis se utilizará la estadística descriptiva y la distribución **T-Student.**

4.3.1. Estadística descriptiva

Para la demostración de la hipótesis se utilizará la estadística descriptiva en la que se cuantifican los resultados obtenidos en las pruebas realizadas en cada escenario de cada uno de los indicadores definidos como se muestra en la **Tabla 8-4.**

Tabla 8-4: Resultados de indicadores

N°	Indicadores	Escenario de pruebas 1	Escenario de pruebas 2
1	Cantidad total de paquetes enviados	1	29
2	Cantidad total de paquetes recibidos	1	39
3	Capacidad esteganográfica	35 caracteres	25 caracteres
4	Probabilidad de Detectabilidad	$2{,}71051*10^{-19}$	$2{,}71051*10^{-19}$
5	Robustez	5 direcciones IPv6	5 direcciones IPv6

Realizado por: Quintero Hermes, 2019.

En el **Gráfico 3-4** se muestran los resultados de la comparación realizada por cada uno de los indicadores.

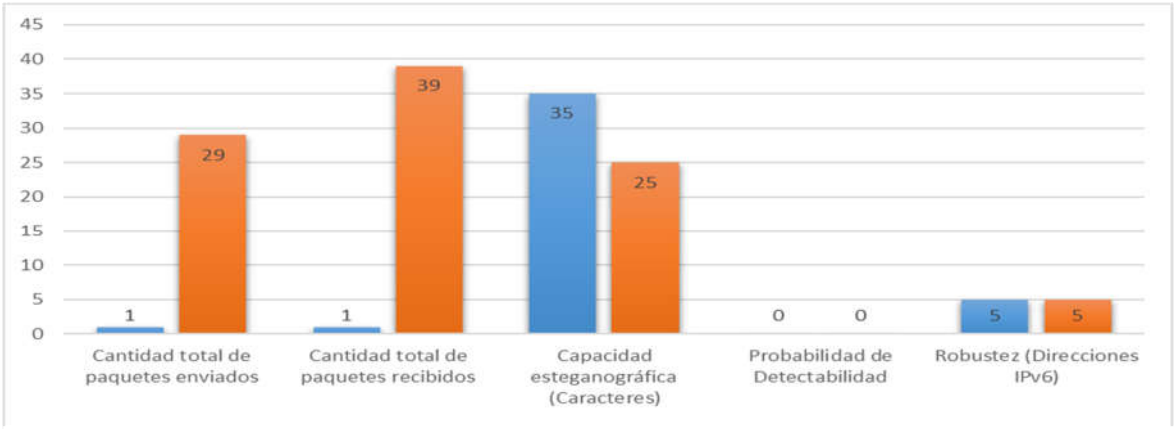


Gráfico 3-4: Resultados de la comparación por indicador de los escenarios 1 y 2
Realizado por: Quintero Hermes, 2019.

4.3.2. Comprobación de la hipótesis a través de la T-Student

Los pasos para comprobar la hipótesis fueron los siguientes (TRIOLA, 2009, págs. 407-410):

Paso 1. Determinación de hipótesis nula y alternativa

La hipótesis definida en la presente investigación es "El uso de esteganografía en el protocolo IPv6 usando mensajes ocultos es una alternativa para una comunicación segura". De lo cual se tiene como hipótesis nula ($\mathbf{H_0}$) e hipótesis alternativa ($\mathbf{H_1}$) lo siguiente:

- $\mathbf{H_0}$= El uso de esteganografía en el protocolo IPv6 usando mensajes ocultos **no** es una alternativa para una comunicación segura.
- $\mathbf{H_1}$= El uso de esteganografía en el protocolo IPv6 usando mensajes ocultos es una alternativa para una comunicación segura.

Paso 2. Determinación del nivel de significancia

El nivel de significancia para esta investigación es α=0.05 (5%).

Paso 3. Elección de prueba estadística

La prueba **T-Student** es un estadístico que se utiliza cuando las poblaciones son pequeñas ($n \leq 30$) y permiten evaluar si dos proporciones difieren significativamente una de otra respecto a una variable de análisis. Se calcula el estadístico de control estandarizado para proporciones de acuerdo a la siguiente fórmula:

$$z_{calculado} = \frac{p' - p}{\sqrt{\frac{p(1-p)}{n}}}$$

Paso 4. Estadístico de prueba

De acuerdo al estudio realizado por (MAZURCZYK WOJCIECH, 2014) determinan el coste esteganográfico como el grado de distorsión o degradación de un portador causado por la incrustación de la información secreta y lo definen como la probabilidad de detección del método esteganográfico. Indican que si su valor es excesivo indicará una fácil detección del método esteganográfico y expresan que una probabilidad menor al 50% se considera efectivo, ya que con un valor mayor el mensaje secreto sería detectable y el método no tendría sentido.

Es por ello, que para la prueba de hipótesis de esta investigación se considera la proporción del **coste esteganográfico** como variable adecuada sobre la que se basó nuestro criterio de decisión. Por tal razón, para probar nuestra hipótesis se establece lo siguiente:

- **H_0:** $p = 0.5$,
- **H_1:** $p < 0.5$.

Teniendo como datos los siguientes:

Variable	Valor
p’	$2{,}71051*10^{-19}$
P	0.50
N	5
1-p	0.50

Paso 5. Cálculos y estimación

Al reemplazar los datos y realizar los cálculos se obtiene el resultado de $z_{calculado}$= **-2.24** como se demuestra en lo siguiente:

$$z_{calculado} = \frac{(2{,}71051 * 10^{-19}) - 0.50}{\sqrt{\frac{0.5(0.5)}{5}}} \approx -2.24$$

Paso 6. Decisión estadística

Debido a que su valor recae en el extremo por la izquierda, ahora se calcula el **p-valor** que corresponde al resultado obtenido de $z_{calculado}$= **-2.24** , es decir, el área que se encuentra bajo la curva izquierda de -2.24. Del valor obtenido de la tabla A-2 (**ANEXO G**), se puede observar que el área que hay por debajo de $z_{calculado}$ es igual a 0.0125.

Paso 7. Conclusión

Por medio de la prueba T-Student, se observa como el **p-valor= 0.0125** es menor que el nivel de significancia de 0.05(5%), con lo cual, se rechaza la hipótesis nula a un nivel de significancia del 5%. Teniendo como conclusión que “**existe evidencia estadística que la proporción de direcciones IPv6 utilizadas en el mecanismo de esteganografía tienen una probabilidad de detección menor al 50%**

4.2. DISCUSIÓN DE RESULTADOS FINALES

El resultado de los indicadores de capacidad esteganográfica, probabilidad de detectabilidad y robustez mantienen iguales valores en los dos escenarios. El indicador que varía es la cantidad de paquetes de acuerdo al protocolo utilizado, DNS ocupa un paquete recibido de una consulta mientras que VoIP 39 paquetes recibidos al realizar un total de cinco llamadas.

Al analizar los resultados de los cuatro parámetros de evaluación del mecanismo esteganográfico, se puede apoyar a la hipótesis que esta investigación plantea, *el uso de esteganografía en el protocolo IPv6 usando mensajes ocultos es una alternativa para una comunicación segura*. Los valores obtenidos son aceptables y respaldan el hecho que se usó un **covert channel** en el protocolo IPv6.

Por medio de la prueba T-Student, se observa como el **p-valor= 0.0125** es menor que el nivel de significancia de 0.05(5%), con lo cual, se rechaza la hipótesis nula a un nivel de significancia del 5%. Teniendo como conclusión que **"existe evidencia estadística que la proporción de direcciones IPv6 utilizadas en el mecanismo de esteganografía tienen una probabilidad de detección menor al 50%**

El mecanismo esteganográfico permitió comunicar un mensaje de 35 caracteres en forma visible, pero no comprensible para un observador o guardián. Fue codificado en el sistema hexadecimal dentro de la porción del ID de interfaz del dispositivo del emisor. Además, se usó los servicios de DNS por medio de consultas de dominios IPv6 y en VoIP dentro de las direcciones de IPv6 en las extensiones.

Las direcciones globales unicast configuradas de forma manual se obtienen de dos mecanismos diferentes, EUI-64 y usando extensiones de privacidad. Para el primero es posible introducir 5 caracteres en una dirección y se mantienen fijos los valores FFFE en los campos cuarto y quinto. Se tiene la consideración que esta dirección se forma a partir de la MAC del computador o dispositivo y los tres primeros 24 bits corresponden a un identificador global de fabricante, en consecuencia, el segundo carácter debe variar de acuerdo al cambio del séptimo bit de la MAC al generar EUI-64. Con respecto a la configuración de direcciones por medio de extensiones de privacidad, se puede introducir 7 caracteres en una dirección y estos son generados por valores aleatorios.

En ambos casos para el diseño del mecanismo se usó el sexto campo como identificador de orden y/o secuencia de los mensajes teniendo un máximo de 256 direcciones en total a disposición. Para mantener la integridad del mensaje se ordena haciendo uso del sexto campo de la dirección.

CAPÍTULO V

5. PROPUESTA

5.1. Objetivos de diseño y métricas para el mecanismo esteganográfico

De acuerdo a lo analizado en la bibliografía y en concordancia con los objetivos planteados en esta tesis, para elaborar un mecanismo esteganográfico se debe considerar los requerimientos que se detallan en la **Tabla 1-5.**

Tabla 1-5: Requerimientos para la elaboración del mecanismo esteganográfico

Requerimientos de un mecanismo esteganográfico
• Establecer un estego-objeto o estegograma a utilizar entre el emisor y el receptor. • Emisor y receptor deben conocer el algoritmo o estego-función para incluir o extraer el mensaje oculto de la comunicación. • Considerar el tamaño del mensaje. • En el caso de los protocolos de red, usar un portador para introducir el estegograma. • Se tienen tres técnicas esteganográficas: inyección, sustitución y generación.

Realizado por: Quintero Hermes, 2019.

5.1.1. Paradigmas para el diseño de un sistema esteganográfico

De acuerdo al trabajo realizado por (BÖHME, 2010, págs. 22-25) establece dos enfoques alternativos para construir un sistema esteganográfico a los que denomina **paradigmas.** Estos son:

- Modificar con precaución.
- Generación encubierta.

Entre estos dos se escogió el paradigma ***"modificar con precaución"*** como modelo para desarrollo del mecanismo esteganográfico en esta investigación debido a su validez a través de sus características, las cuales se adaptan a los requerimientos expuestos anteriormente.

5.*1.2. Paradigma "Modificar con precaución"*

De acuerdo a este paradigma, la función de incrustación de un estego-sistema toma como entrada la información secreta proveída por el usuario que actúa como **emisor,** y es él quien incrusta o embebe el mensaje modificando el portador. Siguiendo una creencia general de que pocos y más pequeños cambios son menos detectables y más seguros. Esos algoritmos están diseñados para preservar cuidadosamente tantas características del portador como sea posible (BÖHME, 2010, págs. 22-23).

5.*1.3. Métricas*

El sistema esteganográfico puede ser medido por tres por tres criterios básicos. Estas 3 dimensiones están interrelacionadas y deben estar equilibradas al momento de diseñar un sistema esteganográfico. Se detallan a continuación.

5.1.3.1. Capacidad o ancho de banda esteganográfico

La capacidad es definida como el máximo tamaño de un mensaje secreto. Puede ser especificado en términos absolutos (bits o caracteres) para un portador determinado, o en relación con la cantidad de bits necesarios para almacenar el estegograma resultante.

5.1.3.2. Detectabilidad o seguridad esteganográfica

El propósito de la comunicación esteganográfica es ocultar la pura existencia de un mensaje secreto. Su seguridad se juzga por la imposibilidad de detectar y no por la dificultad de leer el contenido del mensaje. Su mayor dificultad se centra en un problema de decisión, ¿Un portador contiene o no un mensaje secreto?, con lo cual, se tiene dos posibles tipos de errores y sus probabilidades se definen de acuerdo a:

- La probabilidad que al realizar el esteganálisis clasifique incorrectamente un portador con un estego-objeto incrustado y se le denomina probabilidad de falso positivo **P(α)**.
- La probabilidad que al realizar un esteganálisis no se detecte un estego-objeto en un portador, a esta se le denomina probabilidad faltante **P(β)**.

A partir de estos dos enunciados, se tiene que la ***probabilidad de detección*** se define como 1 – **P(β).** En donde **P(β)** representa todas las posibles frecuencias que se usan para incrustar el estego-objeto en un espacio de muestreo.

De acuerdo a (MAZURCZYK WOJCIECH, 2014) definen el costo esteganográfico y establecen que su valor es igual a la probabilidad de detección. En donde indican que su efectividad está relacionada con resultados menores al 50%

5.1.3.3. Robustez

El término ***robustez*** hace referencia a la dificultad de eliminar información oculta de un estego-objeto. Esta propiedad es muy importante al considerar los errores presentes en los canales o tener guardianes activos que evitan el uso de esteganografía. Las métricas típicas de los algoritmos esteganográficos se expresan en clases de distorsión (integridad). Y (BÖHME, 2010) señala que existen pocas investigaciones sobre este parámetro y las existentes son bastantes superficiales o extremadamente específicas a su sistema. Aunque es un componente muy relevante para el mecanismo esteganográfico.

5.2. Análisis del protocolo IPv6

Como punto de partida para el mecanismo esteganográfico se analizan las características generales del protocolo IPv6 que están detalladas en la Tabla 3-2*: Características del Protocolo IPv6* . De este conjunto se escogen dos, las cuáles pueden ser aprovechadas para el diseño del mecanismo esteganográfico y poder generar un estegograma. Se detallan a continuación:

5.2.1. Configuración de direcciones Stateless y Stateful

La forma de configurar las direcciones Global Unicast en IPv6 se resume en la **Figura 1-5,** en ésta se observa dos formas de configuración: una manual y otra dinámica.

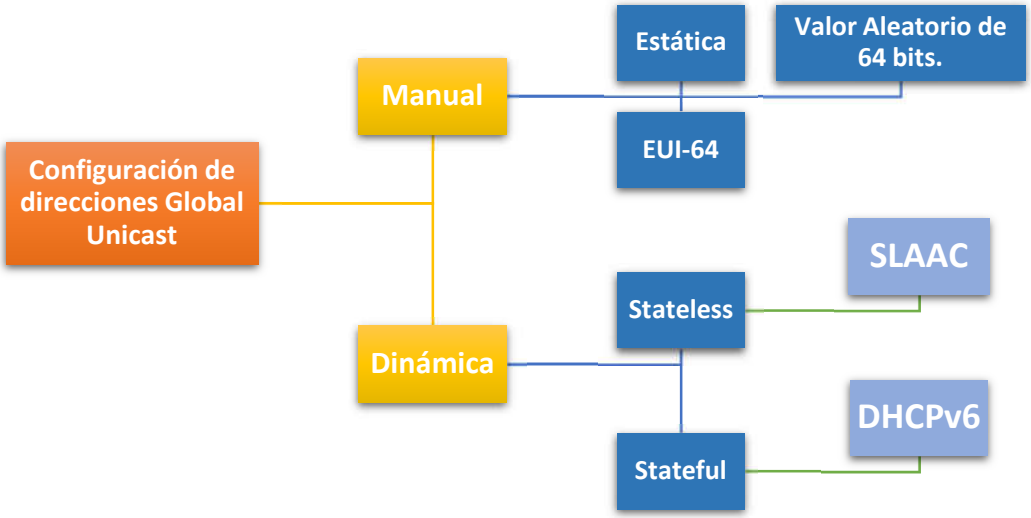


Figura 1-5: Configuración de direcciones Global Unicast en IPv6
Realizado por: Quintero Hermes, 2019.

En la configuración manual, una dirección global unicast se obtiene tres maneras. Una estática o definida directamente por el usuario en el sistema operativo o dispositivo. Otra generada por el mecanismo EUI-64 a partir de la MAC del dispositivo o host; y la última que usa un identificador de interface aleatorio usando extensiones de privacidad para brindar seguridad y confidencialidad al usuario. Todas con una máscara /64.

La configuración de cada dirección es automática y generada por el valor "**stable-privacy**" en el campo **IPV6_ADDR_GEN_MODE** o valor aleatorio de 64 bits por defecto como se demuestra en la **Figura 2-5**. Si se desease que forme la dirección IPv6 usando la MAC del equipo se debe ajustar a "**eui64**".

```
IPV6_ADDR_GEN_MODE="stable-privacy"
NAME="enp0s3"
UUID="931048c7-a8d7-454f-b8d7-71a801f03c31"
```

Figura 2-5: Modo de generación de una dirección IPv6
Realizado por: Quintero Hermes, 2019.

De esto se puede concluir que la porción de identificador de una dirección IPv6 puede ser manipulada para incrustar información, representados o escondidos en sus valores hexadecimales, y a su vez adaptados a sus valores característicos para pasar desapercibido.

5.2.2. Gran número de direcciones

Se cuenta con 2^{64} como conjunto de direcciones globales unicast disponible con una máscara /64. Esta característica se puede explotar para asociarla a la capacidad que tiene un mecanismo esteganográfico de enviar información oculta (ancho de banda esteganográfico) y calcular su probabilidad de ser escogida y analizada (costo esteganográfico) en el momento de una inspección.

5.3. Análisis del estegograma

Para el desarrollo del estegograma de esta investigación, se analizan las técnicas de la ***Figura 15*-2,** de las tres se escoge la ***sustitución***, debido a que su definición se adapta a la primera característica analizada del protocolo IPv6. En la configuración de la dirección, los datos normales que corresponden al identificador de la dirección se reemplazan por los del mensaje secreto de la comunicación. Siendo este el ***medio portador.***

De esta manera, el **estegograma** estaría conformado por la función que se utilizará para incluir el contenido del mensaje secreto en la porción del identificador de la dirección origen y su medio portador o ***"covert channel"*** sería el paquete IPv6. Así, queda representado el sistema esteganográfico (**Figura 3-5**).

<table>
<tr><td colspan="5">Dirección IPv6 de un cliente
medio portador o covert cannel</td></tr>
<tr><td rowspan="2">Enrutamiento global
Hasta 48 bits</td><td rowspan="2">ID de subred
Hasta 16 bits</td><td>Máscara</td><td>Mensaje Secreto</td><td>StegoFunción</td></tr>
<tr><td rowspan="2">/64</td><td>Alfabeto codificado en valores hexadecimales</td><td>Capacidad de autoconfiguración del identificador de la dirección IPv6</td></tr>
<tr><td colspan="2">Prefijo de red
64 bits</td><td colspan="2">Estegograma
64 bits</td></tr>
</table>

Figura 3-5: Representación del estegograma usando el protocolo IPv6
Realizado por: Quintero Hermes, 2019.

Ahora para evaluar el ***estegograma*** se utilizan los criterios detallados en la **Tabla 14-2:** *Características de un sistema esteganográfico de red.* y el costo esteganográfico.

5.4. Diseño del mecanismo esteganográfico

Partiendo del análisis realizado en las dos características identificadas del protocolo IPv6 para realizar y aprovechar un mecanismo esteganográfico, con respecto a la primera, la forma en que un dispositivo obtiene su dirección global unicast y la máscara que se le asigna, para este caso /64, permite que se pueda explotar este espacio disponible para incrustar mensajes usando la dirección IPv6 como un canal secreto.

La figura 2-4 muestra la estructura de una dirección global, en la cual los primeros 64 bits son dados por la organización o proveedor de servicio. Los otros 64 bits son configurados a partir de los métodos analizados en el dispositivo y pueden ser cambiados por el usuario.

El uso de símbolos hexadecimales en la notación del espacio del ID de interfaz permite incrustar información al codificar las letras del alfabeto y los números. En la ***Tabla 2*-5** se presenta la codificación del alfabeto en los caracteres hexadecimales usando la tabla de códigos ASCII (CÓDIGOS ASCII y HTML, 2018).

Tabla 2-5: Tabla de conversión del alfabeto a hexadecimal

Valor Hexadecimal	Letra Alfabeto	Valor Hexadecimal	Letra Alfabeto	Valor Hexadecimal	Letra Alfabeto	Valor Hexadecimal	Letra Alfabeto
61=	a	62=	B	63=	c	64=	d
65=	e	66=	F	67=	g	68=	h
69=	i	6A=	J	6B=	k	6C=	l
6D=	m	6E=	N	6F=	o	70=	p
71=	q	72=	R	73=	s	74=	t
75=	u	76=	V	77=	w	78=	x
79=	y	7A=	Z	30=	0	31=	1
32=	2	33=	3	34=	4	35=	5
36=	6	37=	7	38=	8	39=	9

Realizado por: Quintero Hermes, 2019.

En ésta se observa el uso de 8 bits o dos caracteres hexadecimales para cada letra del alfabeto o número, en consecuencia, se tiene una capacidad de 8 letras para transmitir en los mecanismos estático y valor aleatorio por paquete IPv6. A cada conjunto de 8 bits se lo denomina campo, como lo muestra la **Figura 4-5**.

ID Interfaz de 64 bits mecanismo ALEATORIO										
X X	X X	:	X X	X X	:	X X	X X	:	X X	X X
1 C	2 C	separador	3 C	4 C	separador	5 C	6 C	separador	7 C	8 C

Figura 4-5: Campos de un identificador de interfaz /64
Realizado por: Quintero Hermes, 2019.

Debido a que los valores que se asignan en la ***Tabla 2*-5** son secuenciales y muy parecidos, realizando una simple inspección se daría a notar la sustitución, lo cual levantaría sospechas y la información quedaría expuesta; se propone un conjunto de caracteres, asignándole un valor de dos caracteres hexadecimales aleatorios para representarlos (***Tabla 3*-5**) y así generar un diccionario estático.

Tabla 3-5: Codificación del alfabeto usando dos caracteres hexadecimales aleatorios

Valor Hexadecimal	Letra Alfabeto	Valor Hexadecimal	Letra Alfabeto	Valor Hexadecimal	Letra Alfabeto	Valor Hexadecimal	Letra Alfabeto
E4=	a	2F=	b	34=	c	88=	d
CB=	e	BB=	f	5C=	g	22=	h
A0=	i	59=	j	04=	k	FE=	l
AB=	m	11=	n	8F=	o	77=	p
D0=	q	12=	r	DD=	s	AA=	t
D7=	u	67=	v	10=	w	CC=	x
9A=	y	FA=	z	6B=	0	F7=	1
8A=	2	E5=	3	9D=	4	C1=	5
3F=	6	B4=	7	2C=	8	A1=	9

Realizado por: Quintero Hermes, 2019.

Para el caso de la obtención del ID de interfaz por método de EUI-64, se usan las posiciones del cuarto y quinto símbolo para emplear FF:FE como valor fijo y mostrar una dirección obtenida a partir de la MAC. Esto se muestra en la **Figura 5-5**. Por esta razón la capacidad de transmitir es de 6 caracteres por paquete IPv6.

ID Interfaz de 64 bits mecanismo EUI-64										
X X	X X	:	X X	F F	:	F E	X X	:	X X	X X
1 C	2 C	separador	3 C	Valor Fijo	separador	Valor Fijo	4 C	separador	5 C	6 C

Figura 5-5: ID de interfaz de 64 bits mecanismo EUI-64
Realizado por: Quintero Hermes, 2019.

Con el objetivo de aplicar la característica de **robustez** para el mecanismo a diseñar, se toma arbitrariamente el campo del sexto carácter para indicar el orden del mensaje en las direcciones IPv6. Y la forma en la que se ordenará los paquetes será descendente iniciando con el valor de **FF**. Así se pretende ordenar la información y mantener su integridad. Como lo ilustra la **Figura 6-5.**

ID Interfaz de 64 bits Estática o Valor Aleatorio										
X X	X X	:	X X	X X	:	X X	X X	:	X X	X X
1 C	2 C	separador	3 C	4 C	separador	5 C	6 C	separador	7 C	8 C

Figura 6-5: ID de interfaz de 64 bits mecanismo Estático o valor Aleatorio
Realizado por: Quintero Hermes, 2019.

Con esto se tendría un subconjunto de 2^8 direcciones globales disponibles y al relacionarlo con la segunda característica analizada, el hecho de tener un gran conjunto de direcciones se aprovecha para multiplicar la capacidad la información que se puede transmitir, como se detalla en la **Tabla 4-5**. En esta se detalla la capacidad máxima (ancho de banda esteganográfico).

Tabla 4-5: Cantidad de información a transmitir para los escenarios.

Capacidad de información a transmitir	Configuración de dirección global Unicast	Valores	Capacidad máxima de información a transmitir
(número de caracteres)*(2^8)	Estática /64	(7)*(2^8) =	1792 caracteres
	EUI-64	(5)*(2^8) =	1280 caracteres

Realizado por: Quintero Hermes, 2019.

Esto nos da como resultado una capacidad máxima de información a transmitir de 1792 para una configuración estática y 1280 para una de acuerdo a EUI-64. Esta capacidad máxima está relacionada y limitada con el parámetro de robustez.

El objetivo de tomar solo un subconjunto de 256 direcciones globales está relacionado con el hecho de no levantar sospechas sobre el uso excesivo de paquetes sobre un mismo servicio. Esto se demuestra en la **Tabla 5-5.**

Tabla 5-5: Cantidad máxima de direcciones para el mecanismo esteganográfico

Fórmula Cantidad de direcciones global unicast	Configuración de dirección global Unicast	Valores	Cantidad de direcciones global unicast
$\frac{cantidad\ de\ caracteres}{número\ de\ campos\ disponibles}$	Estática /64	$\frac{1792}{7} = 256$	256 direcciones
	EUI-64	$\frac{1280}{5} = 256$	256 direcciones

Realizado por: Quintero Hermes, 2019.

CONCLUSIONES

La cualidad de comunicación segura se fundamenta en el uso de mecanismos que garanticen su privacidad; la esteganografía es una alternativa válida, confiable y en gran desarrollo. Como herramienta nos permite intercambiar mensajes ocultos e incrustados en medios portadores que pueden ser explotados y a su vez no levantarían sospechas si fuesen analizados o vigilados.

Para el desarrollo de la investigación se empleó el tipo de investigación experimental y aplicativa; y con el uso de herramientas de simulación como GNS3, VIRTUALBOX y KALI-LINUX, se implementó dos escenarios que demuestran el uso y aplicación de los protocolos DNS y SIP usando IPv6 en la capa de red.

Se aprovechó dos características que posee el protocolo; la capacidad de autoconfiguración de la porción de ID de interfaz (aleatoria de 64 bits y EUI-64) con una máscara /64 y la gran cantidad de direcciones disponibles. Con ello se diseñó un estegograma en la dirección global unicast de los emisores, que facilita la incrustación de mensajes ocultos entre dos o más nodos

Al analizar los resultados de los cuatro parámetros de evaluación para el mecanismo esteganográfico, se puede apoyar a la hipótesis que esta investigación plantea, *el uso de esteganografía en el protocolo IPv6 usando mensajes ocultos es una alternativa para una comunicación segura*. Los valores obtenidos son aceptables y respaldan el hecho que se usó un **covert channel** en el protocolo IPv6.

El resultado de los indicadores de capacidad esteganográfica, probabilidad de detectabilidad y robustez mantienen iguales valores en los dos escenarios, teniendo un $2{,}71051*10^{-19}$ de probabilidad de ser detectada la dirección IPv6 utilizada para el estegograma. El indicador que varía es la cantidad de paquetes de acuerdo al protocolo utilizado; DNS ocupa un paquete recibido de una consulta, mientras que VoIP en su protocolo SIP 39 paquetes recibidos al realizar un total de cinco llamadas.

Al haber concluido con el diseño del mecanismo esteganográfico, se demostró en los dos escenarios y haciendo uso de servicios comunes y aceptados, como DNS y voz sobre IP, es posible enviar mensajes ocultos usando el protocolo IPv6, pasando por alto a entornos vigilados o con sistemas perimetrales de seguridad.

La prueba de hipótesis de esta investigación considera la proporción del coste esteganográfico o probabilidad de detectabilidad como variable adecuada sobre la que se basó el criterio de decisión. Por medio de la prueba T-Student, se observó como el **p-valor= 0.0125** es menor que el nivel de

significancia de (5% propuesto), con lo cual, se rechaza la hipótesis nula a un nivel de significancia del 5%. Teniendo como conclusión que **"existe evidencia estadística que la proporción de direcciones IPv6 utilizadas en el mecanismo de esteganografía tienen una probabilidad de detección menor al 50%".**

El mecanismo esteganográfico diseñado propuesto está relacionado con la forma en que se obtiene el ID de interfaz en el equipo y la máscara de red. Se utilizó la técnica de sustitución y en la propuesta el paradigma "*Modificar con precaución*", se alcanzó un máximo de 1792 caracteres para una configuración de valor aleatorio y 1280 para EUI-64. Con ello se usa 256 direcciones IPv6 en el emisor con una máscara /64.

RECOMENDACIONES

Analizar las características que no se consideraron en esta investigación como las direcciones de enlace local o el campo **next header** en la cabecera del paquete IPv6. También el uso y demostración en otros servicios o protocolos de aplicación sobre IPv6.

Desarrollar aplicaciones orientadas al uso de las técnicas esteganográficas de generación o inyección. Estas dos últimas se asocian al paradigma de generación encubierta con el objetivo de automatizar el proceso de incrustación del mensaje en la dirección IPv6 y la eliminación de rastros o registros al realizar el proceso.

Al utilizar mensajes que contengan gran cantidad de caracteres a esconder se podría cometer errores al incrustarlos en las direcciones IPv6. Se recomienda utilizar mensajes precisos y con la menor cantidad de direcciones globales a efectos de no levantar sospechas y reducir la probabilidad de detectabilidad.

Para efectos de añadir una capa más de seguridad al mensaje, se puede cifrar el alfabeto con valores propios, usando las combinaciones resultantes de los símbolos hexadecimales, o creando uno totalmente nuevo.

Para la demostración del mecanismo esteganográfico usando el servicio DNS, el conjunto de nuestras direcciones globales unicast con el mensaje oculto se lo puede registrar en la dirección https://dns.he.net/ en forma gratuita.

El uso de las técnicas esteganográficas demostradas usando el protocolo IPv6 puede ser aprovechadas para fines diferentes a la privacidad o seguridad. Por tal razón, para futuras investigaciones se propone investigar sobre mecanismos efectivos que permitan alertar sobre la alteración del paquete o la presencia de un mensaje oculto.

BIBLIOGRAFÍA

Abdelrahman, D. (2012). *Noiseless Steganography.* Boca Raton: CRC Press, Taylor & Francis Group.

ARCOTEL. (3 de SEPTIEMBRE de 2015). *http://www.arcotel.gob.ec/servicio-acceso-internet/.* Obtenido de http://www.arcotel.gob.ec/wp-content/uploads/2015/09/3.1.1-Cuentas-internet-fijos-y-moviles_ago2017_BANDA-ANCHA.xlsx

ARIN. (3 de FEBRERO de 2011). *https://www.arin.net/*. Obtenido de https://www.arin.net/vault/announcements/2011/20110203.html

Böhme, R. (2010). *Advanced Statistical Steganalysis.* Berlin Heidelberg: Springer.

CASTILLO, CASTILLO, & NUÑEZ. (2013). *http://ccns.jimdo.com/*. Obtenido de http://ccns.jimdo.com/encriptaci%C3%B3n-de-datos

CISCO. (5 de FEBRERO de 2002). *https://www.cisco.com*. Obtenido de https://www.cisco.com/c/en/us/td/docs/ios/solutions_docs/ip_multicast/White_papers/rps.html

CÓDIGOS ASCII y HTML. (20 de 04 de 2018). Obtenido de https://ascii.cl/es/

COLE, E. (2003). *Hiding in Plain Sight: Steganography and the Art of Covert Communication.* Indianapilis, Indiana: Wiley.

DASH, P. (2013). *Getting started with Oracle VM Virtualbox.* Birmingahm: Packt Publishing Ltd.

DAVIES, J. (2012). *Understanding IPv6.* Sebastopol, California: O'Reilly Media, Inc.

DHAMADE, A., & KRUNAL, P. (2014). Network Protocols for Steganography: A Glance. *International Journal of Innovative Research in Technology*, 31-35.

DOOLEY, M., & ROONEY, T. (2013). *IPv6 Deployment and Management.* Hoboken, New Jersey: JohnWiley & Sons, Inc.

DUNMORE, M. (2005). *An IPv6 deployment guide.* The 6net Consortium.

EL COMERCIO. (16 de AGOSTO de 2012). *http://www.elcomercio.com.* Obtenido de http://www.elcomercio.com/actualidad/politica/conozca-julian-assange-y-cronologia.html

EL TELÉGRAFO. (6 de JUNIO de 2012). *http://www.eltelegrafo.com.ec*. Obtenido de http://www.eltelegrafo.com.ec/noticias/economia/8/ipv6-el-ecuador-toma-la-iniciativa-en-latinoamerica

EMC, D. U. (ABRIL de 2014). *https://www.emc.com/*. Obtenido de https://www.emc.com/leadership/digital-universe/2014iview/internet-of-things.htm

FRIDRICH, J. (1999). Applications of data hiding in digital images. *Fifth International Symposium of Signal processing and its Applications*, 1-9.

FRIDRICH, J. (2010). *Steganography in Digital Media.* Cambridge University Press: CAMBRIDGE UNIVERSITY PRESS.

FUENTES, A. (2004 de JULIO de 2004). *www.eltiempo.com*. Obtenido de www.eltiempo.com: http://www.eltiempo.com/archivo/documento/MAM-1508514

GNS3. (29 de JUNIO de 2017). *https://gns3.com/*. Obtenido de https://docs.gns3.com/1PvtRW5eAb8RJZ11maEYD9_aLY8kkdhgaMB0wPCz8a38/index.html

GOOGLE. (s.f.). *https://www.google.com*. Obtenido de https://www.google.com/intl/es/ipv6/statistics.html#tab=per-country-ipv6-adoption

GUO&LE. (2010). *Estudios Esteganográficos de vanguardia.*

HERNÁNDEZ, R., FERNÁNDEZ, C., & BAPTISTA, M. (2014). *Metodología de la invesitgación.* México D.F.: McGRAW-HILL / INTERAMERICANA EDITORES, S.A. DE C.V.

IANA. (10 de AGOSTO de 2017). *https://www.iana.org/*. Obtenido de https://www.iana.org/assignments/ipv6-unicast-address-assignments/ipv6-unicast-address-assignments.xml

IANA. (24 de AGOSTO de 2017). *https://www.iana.org/*. Obtenido de https://www.iana.org/assignments/iana-ipv6-special-registry/iana-ipv6-special-registry.xml

IEEE. (s.f.). *http://standards.ieee.org.* Obtenido de http://standards.ieee.org/develop/regauth/tut/eui64.pdf

JHONSON, N., & SALLE, P. (2008). *Detection of hidden information, covert channels and informatio flows.* NEW YORK: WILEY.

JOHNSON & JOHNSON Technology Consultants, L. (2012). *www.jjtc.com*. Obtenido de www.jjtc.com/Steganography/toolmatrix.html

KALI-LINUX. (19 de OCTUBRE de 2017). *https://www.kali.org/*. Obtenido de https://www.kali.org/

KAPLAN, A. (17 de MAYO de 2016). *https://www.freebsd.org/doc/es/books/handbook/index.html.* Obtenido de https://www.freebsd.org/doc/es/books/handbook/network-ipv6.html

KATZENBEISSER, S., & PETITCOLAS, F. (2000). *Information hiding techniques for steganography and digital watermarking.* Norwood, MA 02062: ARTECH HOUSE, INC.

KUNDUR, D., & AHSON, K. (2003). *Practical Internet Steganography: Data hiding in IP.* Texas: Texas A&M University, College Station.

LACNIC. (10 de JUNIO de 2014). *http://www.lacnic.net*. Obtenido de http://www.lacnic.net/web/anuncios/2014-no-hay-mas-direcciones-ipv4-en-lac

LACNIC. (2015 de Diciembre de 2015). *http://portalipv6.lacnic.net/*. Obtenido de http://portalipv6.lacnic.net/quienes-implementan/

LAMPSON, B. (1973). *A Note on the Confinement Problem.* USA, Xerox Palo Alto Research Center : Association for Computing Machinery, Inc. .

LI, Q., JINMEI, T., & SHIMA, K. (2007). *IPv6 Core Protocols Implementation.* San Francisco: Elsevier Inc.

LOSHIN, P. (2004). *IPv6: Theory, Protocol and Practice.* San Francisco: Elsevier, Inc.

LUBACCZ, J., MAZURCZYK, W., & SZCZYPIORSKI, K. (2014). Principles an Overview of Network Steganography. *IEEE Communications Magazine*, 225-229.

MAZURCZYK WOJCIECH, W. S. (2014). On Importance of Steganographic Cost For Network Steganography. *International Journal of Security and Communication Network*.

MEJÍA, F. (20 de AGOSTO de 2012). *http://www.ipv6tf.ec/*. Obtenido de http://www.ipv6tf.ec/component/content/article?id=2:newsflash-1&catid=3:newsflash

MEULEN, R. (10 de NOVIEMBRE de 2015). *https://www.gartner.com*. Obtenido de https://www.gartner.com/newsroom/id/3165317

MILEVA, A., & PANAJOTOV, B. (2014). Covert Channels in TCP/IP Protocol Stack. *Central European Journal of Computer Science*, 1-30.

MILLER, B. (2008). *A thesis submitted in partial fulfillment of the requirements for the degree of Bachelors of Science in Computer Science.* Arkansas.

MOHAN, L. (2015). A Research Paper on Steganography in IPV6. *International Journal of Computer Applications*, 0975 – 8887.

NEUMANN, J. (2015). *The Book of GNS3.* SAN FRANCISCO: No Starch Press, Inc.

RAMIREZ, D. (2014). *Steganography in TCP & IP Headers.* Barcelona: Universidad Autónoma de Barcelona.

RODRIGUEZ, M. (2016). *Análisis de las técnicas de esteganografía para el oculatamiento de la información.* Quito.

SHIH, F. (2017). *Digital watermarking and steganography : fundamentals and techniques.* Boca Raton, FL: CRC Press.

SIMMONS, G. (1984). Prisoners´ problem and the subliminal channel. *Proc. Int. Conf. Advances in cryptology*, (pág. 51). CA, Santa Barbara.

TRIOLA, M. (2009). *ESTADISTICA, DÉCIMA EDICION.* MÉXICO: PEARSON EDUCACIÓN.

VERMA, P. (2015). *Wireshark Network Security.* Birmingham: Packt Publishing Ltd.

VILLALÓN, A. (15 de JULIO de 2002). *http://www.rediris.es.* Obtenido de http://www.rediris.es/cert/doc/unixsec/node29.html

VIRTUALBOX. (2 de JUNIO de 2017). *https://www.virtualbox.org/*. Obtenido de https://www.virtualbox.org/

WALPOLE, R., MYERS, R., & MYERS, S. (2007). *Probabilidad y estadística para ciencia e ingeniería.* México: PEARSON EDUCATION.

WAYNER, P. (2009). *Disappearing cryptography: Information hiding: Steganography & watermarking.* Burlington, MA 01803, USA: Elsiever.

WIKILEAKS. (16 de AGOSTO de 2012). *https://wikileaks.org/.* Obtenido de https://wikileaks.org/New-translation-Statement-on-UK.html

WILES, J., & ROGERS, R. (2007). *Techno Security's Guide to Managing Risks for IT Managers, Auditors, and Investigators.* Burlington, MA 01803: Elsevier.

WIRESHARK. (10 de OCTUBRE de 2017). *https://www.wireshark.org/*. Obtenido de https://www.wireshark.org/

WOJCIECH MAZURCZYK, S. W. (2016). *Information hiding in communication networks.* U.S.A.: John Wiley & Sons, Inc.

ZHIJUN, W. (2015). *Information Hiding in Speech Signals for Secure Communication.* The Boulevard, Langford Lane, Kidlington, Oxford OX5 1GB, UK: Elsiever Inc.

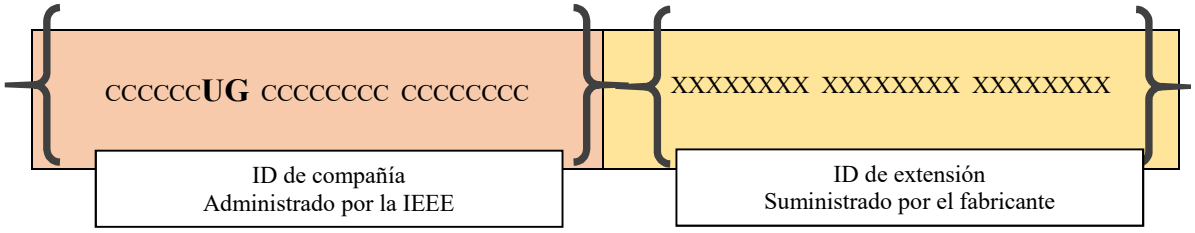
ZHOU, X., & ZHANG, H. (2006). Analysis and Application of Covert Channels of Internet Control Message Protocol. *Wuhan University Journal of the Natural Sciences*, 1857-1861.

ZSEBY, T., & IGLESIAS, F. (2016). A Network Steganography Lab on Detecting. *IEEE*, 1-7.

ANEXOS

ANEXO A Direcciones IEEE 802-LAN

Los adaptadores de red para tecnología LAN comunes como **Ethernet o IEEE 802.11** usan una dirección de 48 bits. Se denomina dirección física, de hardware o **MAC.** Está compuesta por un ID de 24 bits asociados al fabricante y un ID de extensión o de placa de 24 bits como lo muestra la siguiente figura:



Como se observa en la figura, en el primer octeto, el séptimo y octavo bit tienen una función especial y se detalla a continuación:

a. **U/L (Universal/Local). -** Es el séptimo bit del primer byte y se utiliza para indicar si la dirección se administra local o universalmente. Si su valor se establece en cero, se considera que su valor ha sido administrado por la IEEE. Si es uno, se considera que se administra localmente y posee una dirección diferente a la especificada por el fabricante.
b. **I/G (Individual/Grupo). -** Es el octavo bit del primer byte y se utiliza para indicar si es una dirección individual (unicast) o una dirección grupal (multicast). Si su valor es cero se considera una dirección de unidifusión. Si es uno una dirección de multidifusión.

Una dirección típica IEEE 802 asignada a un adaptador de red tiene los valores en el séptimo y octavo bit con cero, es decir, corresponde a una dirección MAC administrada universalmente y unicast.

ANEXO B Configuración de Routers del escenario de pruebas

Router	Comandos ejecutados	Resultado del comando show running-config
R1	R1	Building configuration...
	R1>enable	
	R1#configure terminal	Current configuration : 1610 bytes
	R1(config)# ipv6 unicast-routing	!
	R1(config)#ipv6 router ospf 10	version 12.4
	R1(config-rtr)#router-id 1.1.1.1	service timestamps debug datetime msec
	R1(config)#interface FastEthernet 0/0	service timestamps log datetime msec
	R1(config-if)#ipv6 address	no service password-encryption
	2001:db8:fe:1::1/64	!
	R1(config-if)#ipv6 ospf 10 area 1	hostname R1
	R1(config-if)#no shutdown	!
	R1(config-if)#exit	boot-start-marker
	R1(config)#interface serial 0/0	boot-end-marker
	R1(config-if)#ipv6 address	!
	2001:db8:fe:e001::1/64	!
	R1(config-if)#ipv6 ospf 10 area 1	no aaa new-model
	R1(config-if)#no shutdown	!
	R1(config-if)#exit	resource policy
	R1(config)#interface serial 0/1	!
	R1(config-if)#ipv6 address	memory-size iomem 5
	2001:db8:fe:e003::1/64	ip subnet-zero
	R1(config-if)#ipv6 ospf 10 area 1	no ip icmp rate-limit unreachable
	R1(config-if)#no shutdown	ip cef
	R1(config-if)#exit	ip tcp synwait-time 5
		!
		!
		no ip domain lookup
		!
		ipv6 unicast-routing
		!
		!

		interface FastEthernet0/0 no ip address duplex auto speed auto ipv6 address 2001:DB8:FE:1::1/64 ipv6 ospf 10 area 1 ! interface Serial0/0 no ip address ipv6 address 2001:DB8:FE:E001::1/64 ipv6 ospf 10 area 1 clock rate 2000000 ! interface Serial0/1 no ip address ipv6 address 2001:DB8:FE:E003::1/64 ipv6 ospf 10 area 1 clock rate 2000000 ! interface Serial1/0 no ip address shutdown serial restart-delay 0 no dce-terminal-timing-enable ! ! ip classless ! ! no ip http server no ip http secure-server ! no cdp log mismatch duplex ipv6 router ospf 10

		router-id 1.1.1.1 log-adjacency-changes ! ! control-plane ! ! line con 0 exec-timeout 0 0 privilege level 15 logging synchronous line aux 0 exec-timeout 0 0 privilege level 15 logging synchronous line vty 0 4 login ! ! end
R2	R2 R2>enable R2#configure terminal R2(config)# ipv6 unicast-routing R2(config)#ipv6 router ospf 10 R2(config-rtr)#router-id 2.2.2.2 R2(config)#interface FastEthernet 0/0 R2(config-if)#ipv6 address 2001:db8:fe:2::1/64 R2(config-if)#ipv6 ospf 10 area 1 R2(config-if)#no shutdown R2(config-if)#exit R2(config)#interface serial 0/1	Building configuration... Current configuration : 1589 bytes ! 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 !

	R2(config-if)#ipv6 address 2001:db8:fe:e001::2/64 R2(config-if)#ipv6 ospf 10 area 1 R2(config-if)#no shutdown R2(config-if)#exit R2(config)#interface serial 1/1 R2(config-if)#ipv6 address 2001:db8:fe:e002::1/64 R2(config-if)#ipv6 ospf 10 area 1 R2(config-if)#no shutdown R2(config-if)#exit	! no aaa new-model ! resource policy ! memory-size iomem 5 ip subnet-zero no ip icmp rate-limit unreachable ip cef ip tcp synwait-time 5 ! ! no ip domain lookup ! ipv6 unicast-routing ! ! interface FastEthernet0/0 no ip address duplex auto speed auto ipv6 address 2001:DB8:FE:2::1/64 ipv6 ospf 10 area 1 ! interface Serial0/0 no ip address ipv6 address 2001:DB8:FE:E001::2/64 ipv6 ospf 10 area 1 clock rate 2000000 ! interface Serial1/1 no ip address ipv6 address 2001:DB8:FE:E002::1/64 serial restart-delay 0

		no dce-terminal-timing-enable ! ! ip classless ! ! no ip http server no ip http secure-server ! no cdp log mismatch duplex ipv6 router ospf 10 router-id 2.2.2.2 log-adjacency-changes ! ! control-plane ! ! line con 0 exec-timeout 0 0 privilege level 15 logging synchronous line aux 0 exec-timeout 0 0 privilege level 15 logging synchronous line vty 0 4 login ! ! end
R3	R3 R3>en R3#configure terminal	Building configuration... Current configuration : 1610 bytes

	R3(config)# ipv6 unicast-routing R3(config)#ipv6 router ospf 10 R3(config-rtr)#router-id 2.2.2.2 R3(config)#interface FastEthernet 0/0 R3(config-if)#ipv6 address 2001:db8:fe:3::1/64 R3(config-if)#ipv6 ospf 10 area 1 R3(config-if)#no shutdown R3(config-if)#exit R3(config)#interface serial 0/1 R3(config-if)#ipv6 address 2001:db8:fe:e003::2/64 R3(config-if)#ipv6 ospf 10 area 1 R3(config-if)#no shutdown R3(config-if)#exit R3(config)#interface serial 1/1 R3(config-if)#ipv6 address 2001:db8:fe:e002::2/64 R3(config-if)#ipv6 ospf 10 area 1 R3(config-if)#no shutdown R3(config-if)#exit	! 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 ! ! no aaa new-model ! resource policy ! memory-size iomem 5 ip subnet-zero no ip icmp rate-limit unreachable ip cef ip tcp synwait-time 5 ! ! no ip domain lookup ! ipv6 unicast-routing ! ! ! interface FastEthernet0/0 no ip address duplex auto speed auto ipv6 address 2001:DB8:FE:3::1/64

		ipv6 ospf 10 area 1 ! interface Serial0/1 no ip address ipv6 address 2001:DB8:FE:E003::2/64 ipv6 ospf 10 area 1 clock rate 2000000 ! interface Serial1/1 no ip address ipv6 address 2001:DB8:FE:E002::2/64 ipv6 ospf 10 area 1 serial restart-delay 0 no dce-terminal-timing-enable ! ip classless ! ! no ip http server no ip http secure-server ! no cdp log mismatch duplex ipv6 router ospf 10 router-id 3.3.3.3 log-adjacency-changes ! ! control-plane ! ! line con 0 exec-timeout 0 0 privilege level 15 logging synchronous

		line aux 0 exec-timeout 0 0 privilege level 15 logging synchronous line vty 0 4 login ! ! end

ANEXO C Configuración de servicios en equipos CentOS

Servicio	Configuraciones

http	vi /etc/sysconfig/network-scripts/ifcfg-enp0s3
	
	IPV6INIT=yes # Solo si no se encuentra activado
	IPV6ADDR=2001:DB8:FE:2::10/64 # No olvidar colocar la barra de máscara
	IPV6_DEFAULTGW=2001:DB8:FE:2::1
	:wq
	--- 	
	systemctl restart network
	--- 	
	Yum install http
	--- 	
	Systemctl start httpd
	--- 	
	firewall-cmd --list-all
	firewall-cmd --list-ports
	firewall-cmd --list-services
	firewall-cmd --permanent --add-service=http
	firewall-cmd --reload

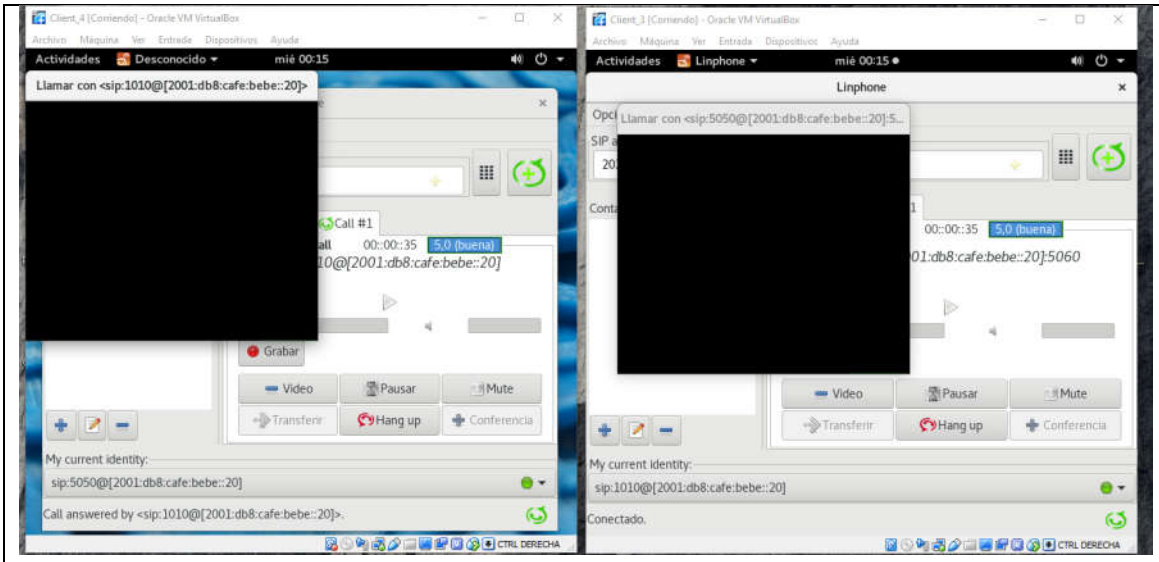
	vi /etc/sysconfig/network-scripts/ifcfg-enp0s3

dns	IPV6INIT=yes # Solo si no se encuentra activado
	IPV6ADDR=2001:DB8:FE:3::10/64 # No olvidar colocar la barra de máscara
	IPV6_DEFAULTGW=2001:DB8:FE:3::1
	:wq
	--- 	
	systemctl restart network
	--- 	
	Yum install dnsmasq
	--- 	
	systemctl start dnsmasq
	--- 	
	firewall-cmd --list-all
	firewall-cmd --permanent --add-service=dns
	firewall-cmd --permanent --add-port=53/tcp
	firewall-cmd –reload
	--- 	
	//configurar dns
	vi /etc/hosts
	2001:db8:fe:2::10 www.maestria2019.com proxy www
	systemctl restart dnsmasq

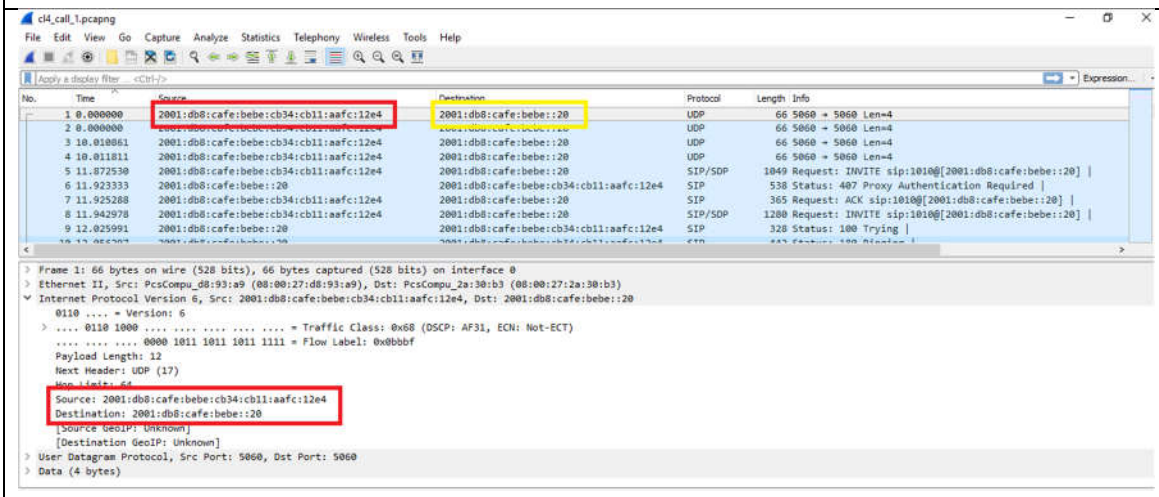
Kali	vi /etc/resolv.conf nameserver 2001:db8:fe:3::10

ANEXO D Captura del tráfico de las llamadas entre la extensión 1010 a la 5050 en el escenario de pruebas #2

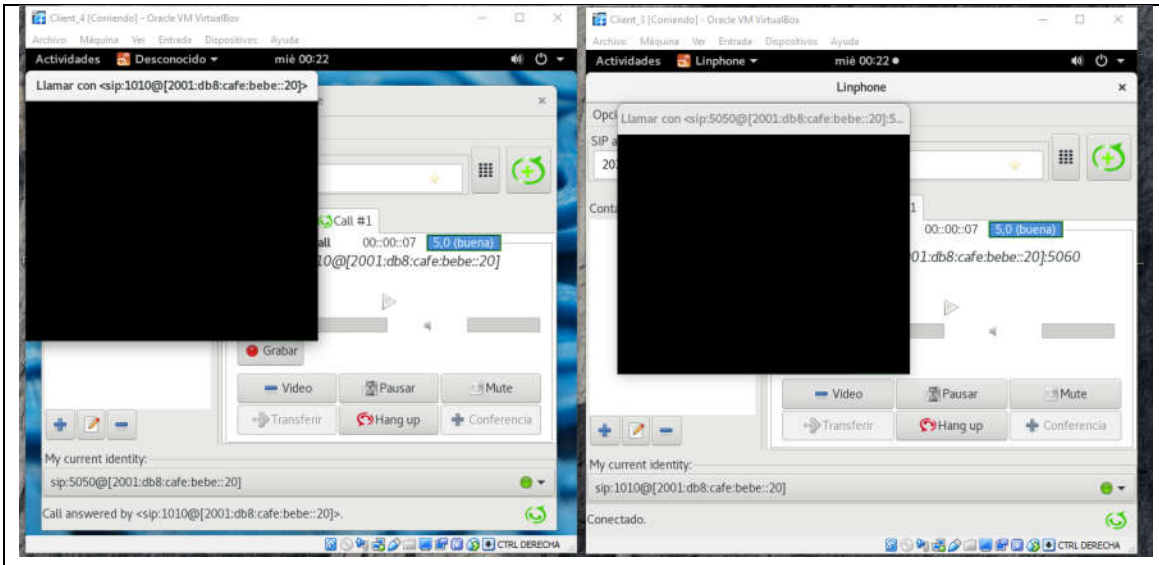
Llamada # 1



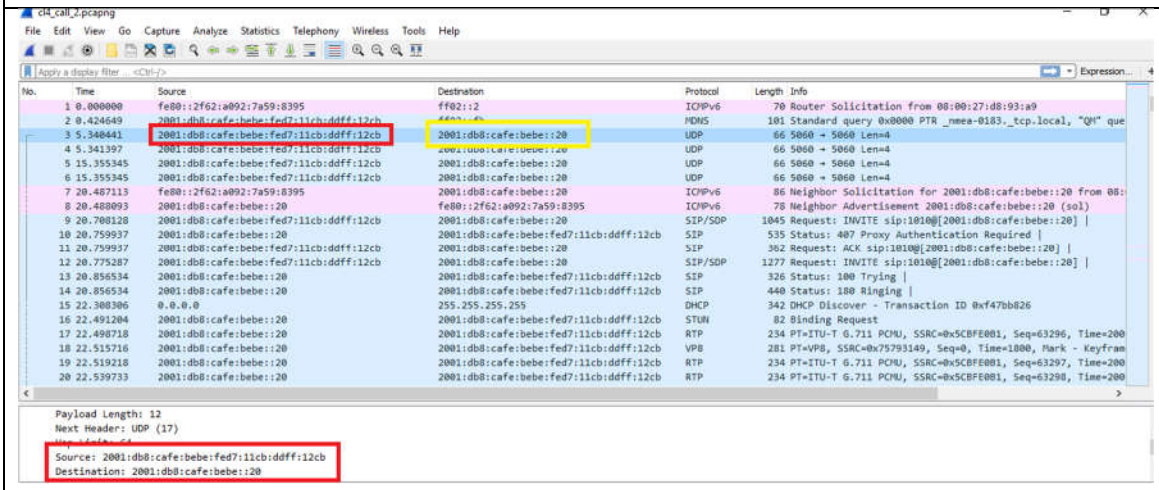
Captura del tráfico de la primer llamada



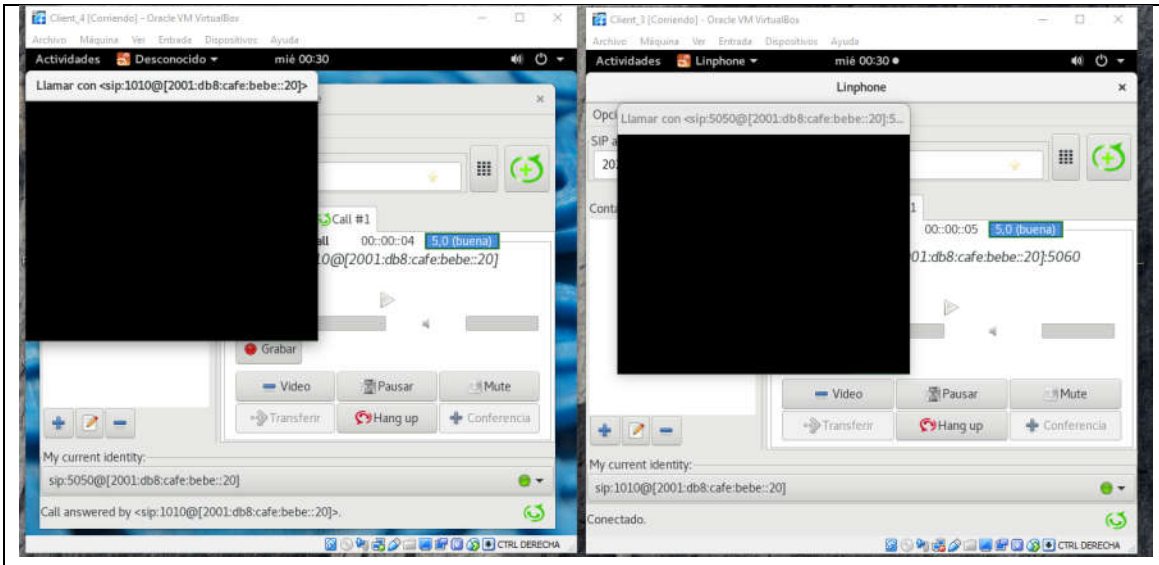
Llamada # 2



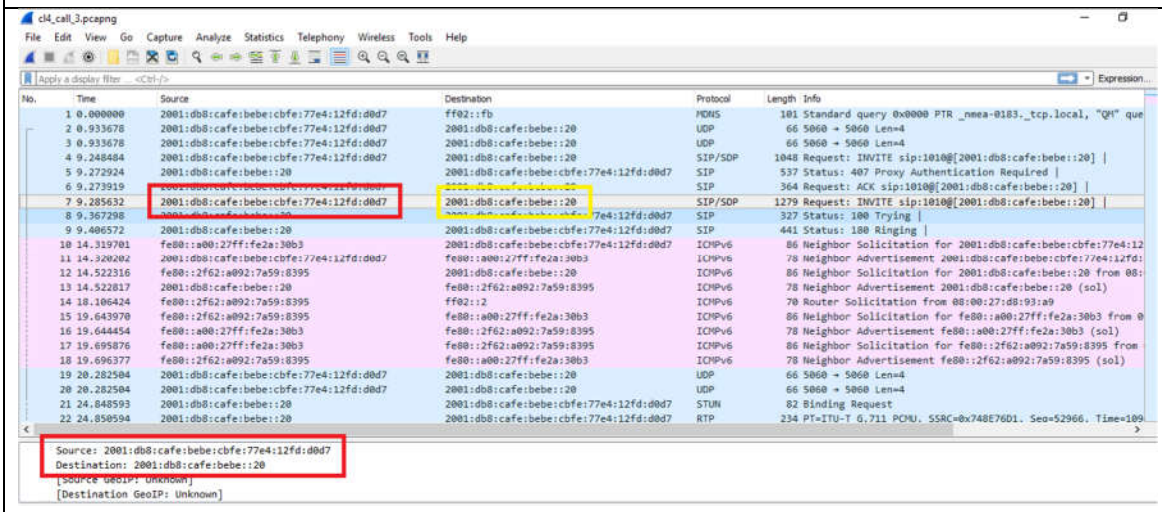
Captura del tráfico de la segunda llamada



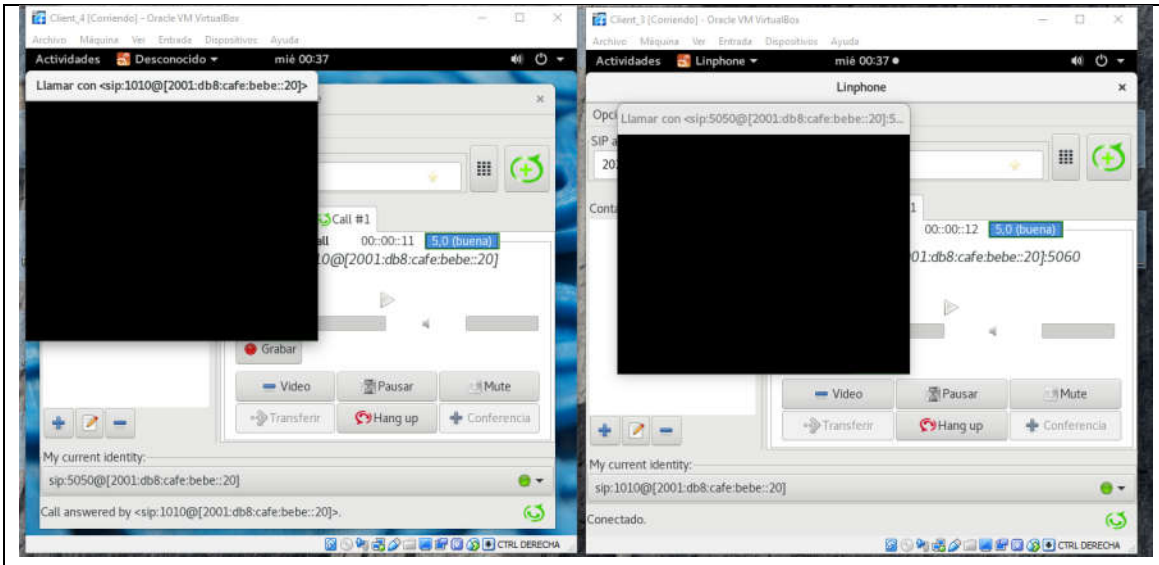
Llamada # 3



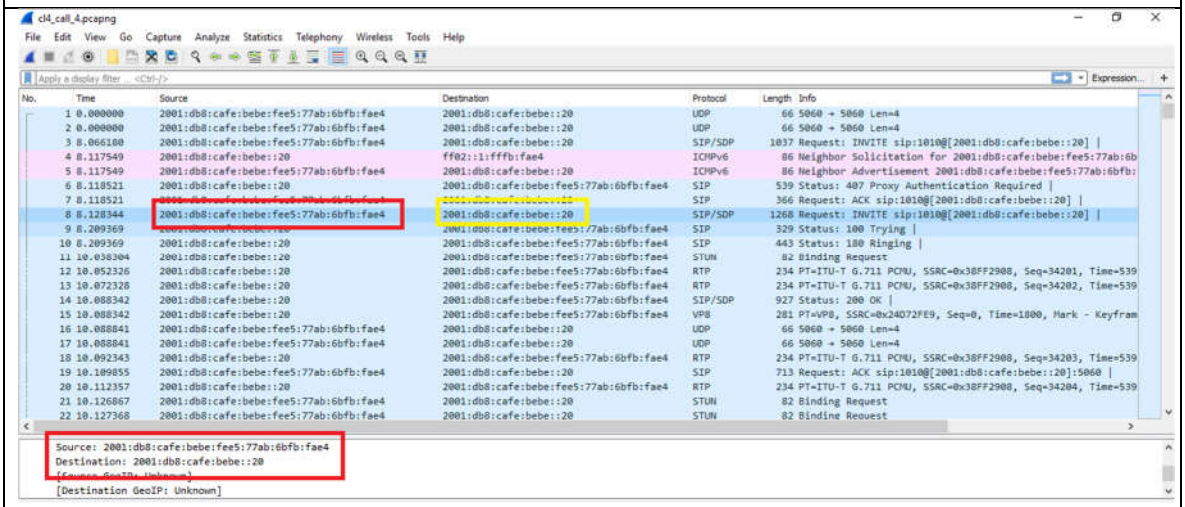
Captura del tráfico de la tercera llamada



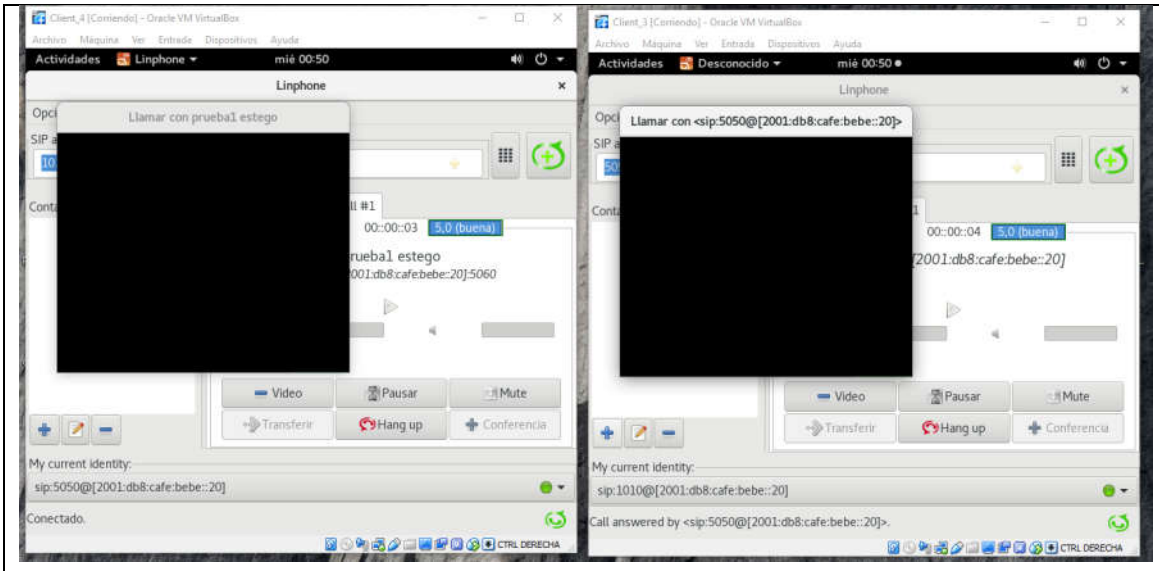
Llamada # 4



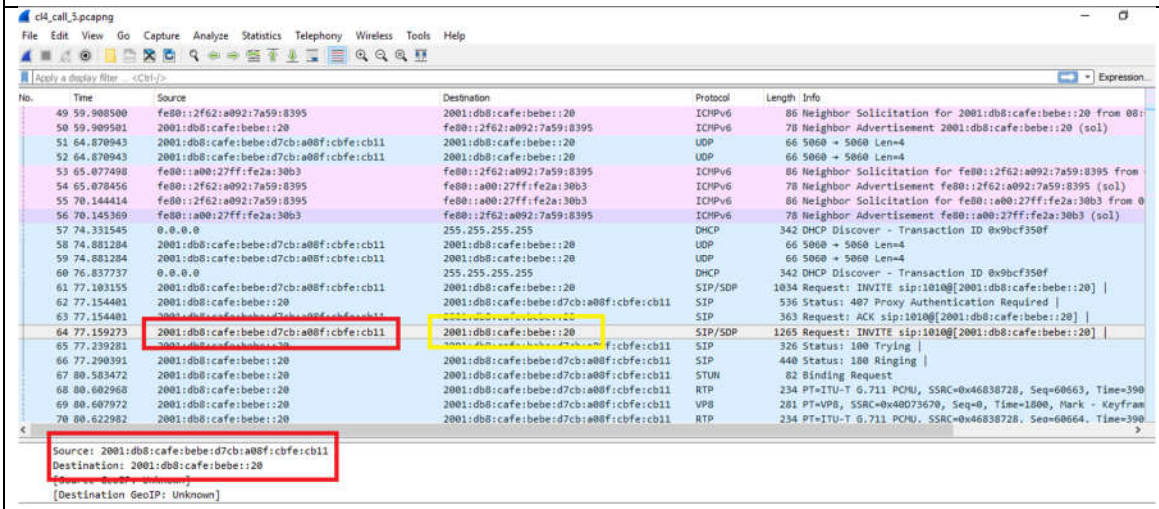
Captura del tráfico de la cuarta llamada



Llamada # 5

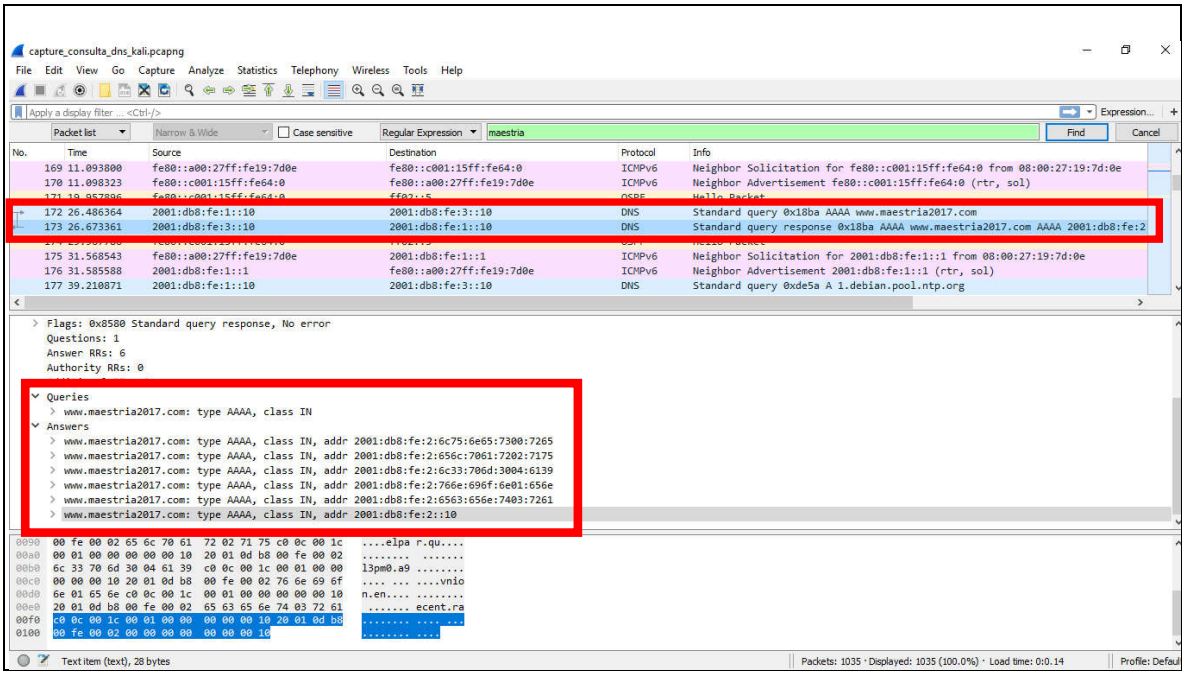


Captura del tráfico de la quinta llamada



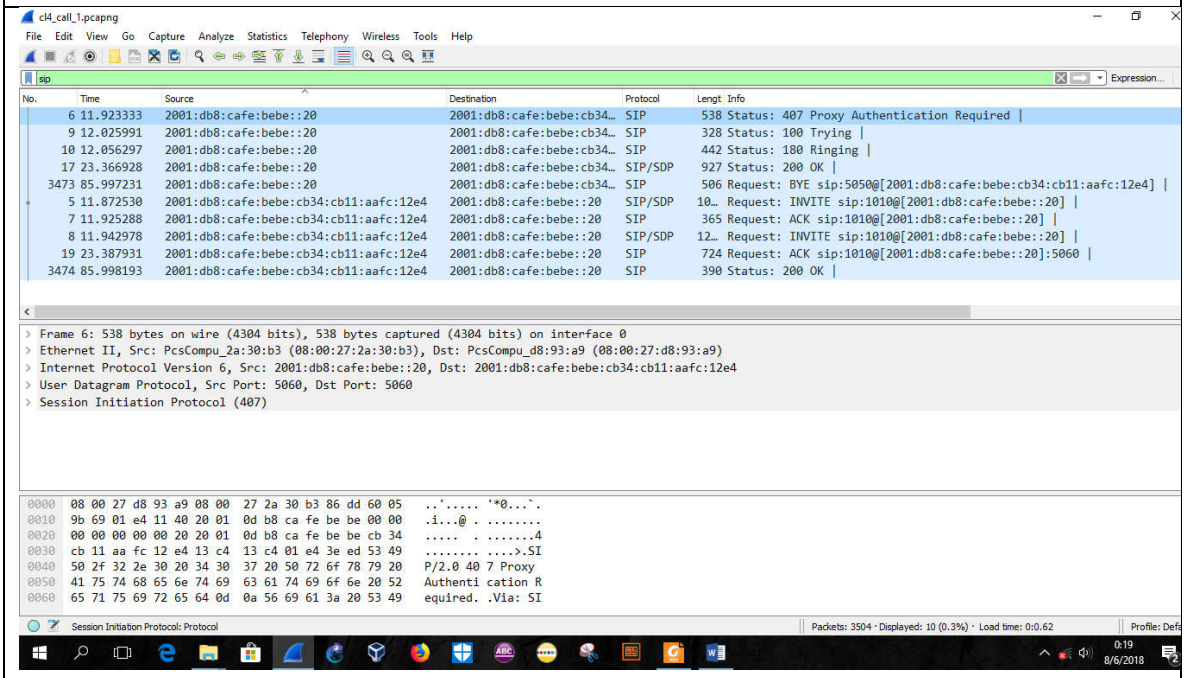
ANEXO E Captura del tráfico de la cantidad de paquetes usados para la consulta al servidor DNS el escenario de pruebas #1

Captura de tráfico de consulta DNS del dominio www.maestria2017.com en el equipo KALI-LINUX

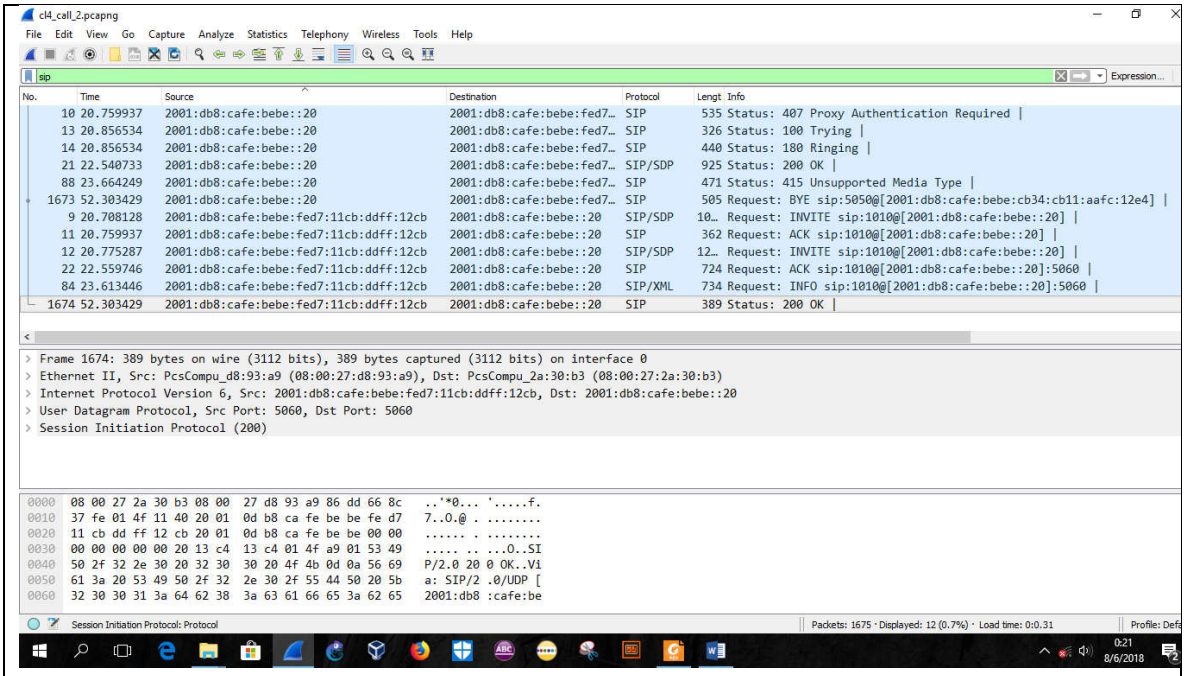


ANEXO F Captura del tráfico de la cantidad de paquetes usados entre la extensión 1010 a la 5050 en el escenario de pruebas #2

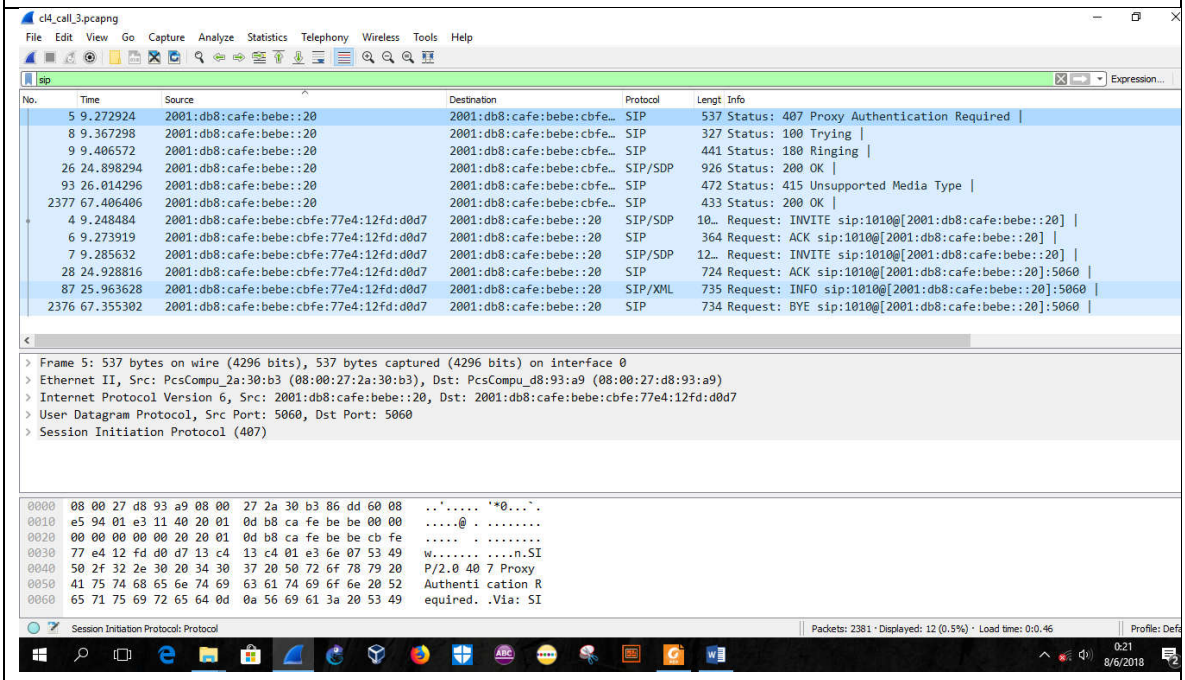
Captura de tráfico de la primera llamada en el cliente 4



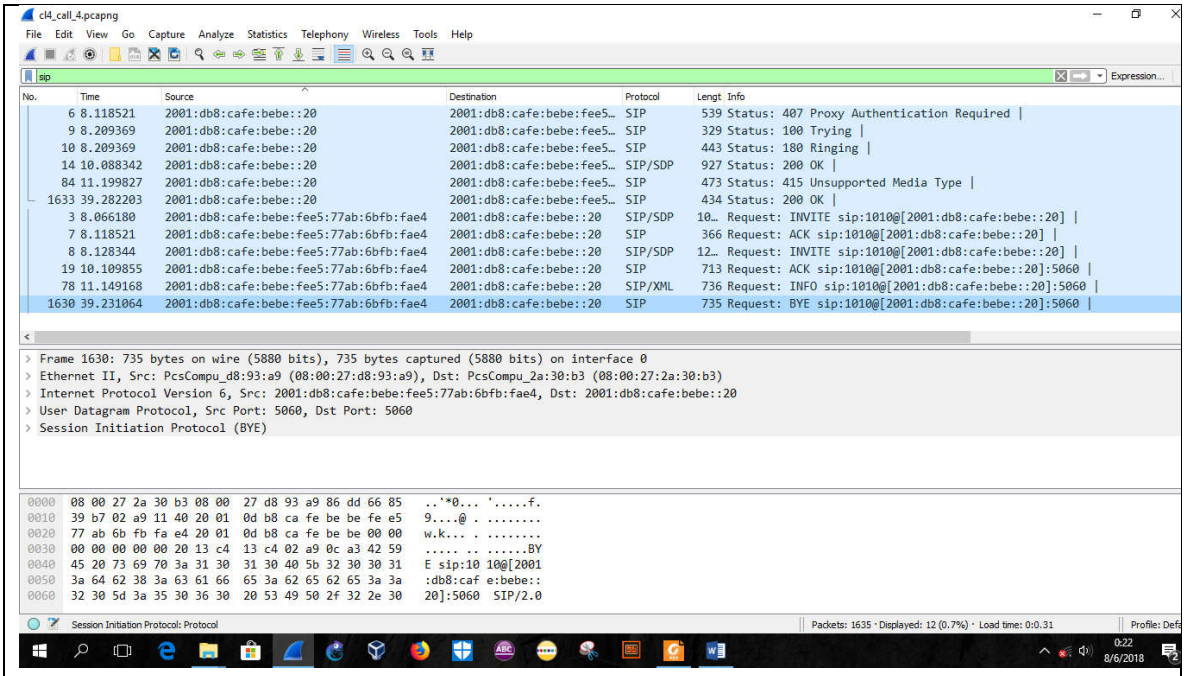
Captura de tráfico de la segunda llamada en el cliente 4



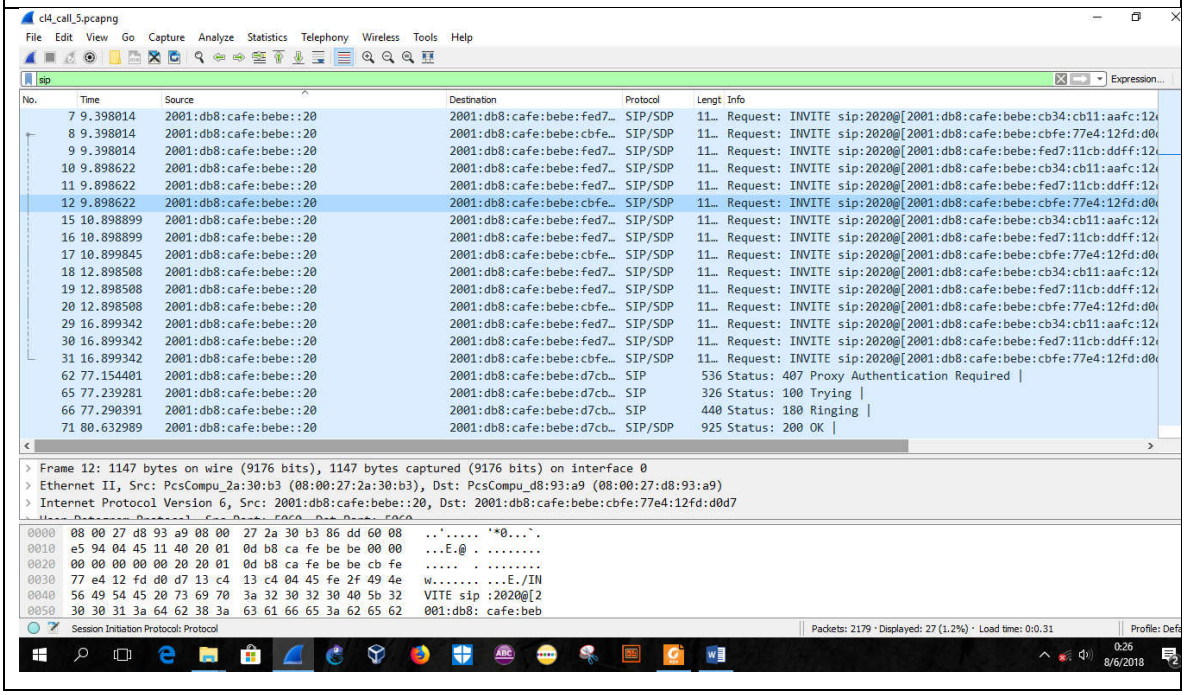
Captura de tráfico de la tercera llamada en el cliente 4



Captura de tráfico de la cuarta llamada en el cliente 4



Captura de tráfico de la quinta llamada en el cliente 4



ANEXO G TABLA DE ÁREAS BAJO LA CURVA (WALPOLE, MYERS, & MYERS, 2007, pág. 751)

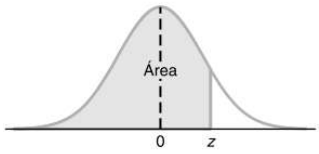


Tabla A.3 Áreas bajo la curva normal

z	.00	.01	.02	.03	.04	.05	.06	.07	.08	.09
−3.4	0.0003	0.0003	0.0003	0.0003	0.0003	0.0003	0.0003	0.0003	0.0003	0.0002
−3.3	0.0005	0.0005	0.0005	0.0004	0.0004	0.0004	0.0004	0.0004	0.0004	0.0003
−3.2	0.0007	0.0007	0.0006	0.0006	0.0006	0.0006	0.0006	0.0005	0.0005	0.0005
−3.1	0.0010	0.0009	0.0009	0.0009	0.0008	0.0008	0.0008	0.0008	0.0007	0.0007
−3.0	0.0013	0.0013	0.0013	0.0012	0.0012	0.0011	0.0011	0.0011	0.0010	0.0010
−2.9	0.0019	0.0018	0.0018	0.0017	0.0016	0.0016	0.0015	0.0015	0.0014	0.0014
−2.8	0.0026	0.0025	0.0024	0.0023	0.0023	0.0022	0.0021	0.0021	0.0020	0.0019
−2.7	0.0035	0.0034	0.0033	0.0032	0.0031	0.0030	0.0029	0.0028	0.0027	0.0026
−2.6	0.0047	0.0045	0.0044	0.0043	0.0041	0.0040	0.0039	0.0038	0.0037	0.0036
−2.5	0.0062	0.0060	0.0059	0.0057	0.0055	0.0054	0.0052	0.0051	0.0049	0.0048
−2.4	0.0082	0.0080	0.0078	0.0075	0.0073	0.0071	0.0069	0.0068	0.0066	0.0064
−2.3	0.0107	0.0104	0.0102	0.0099	0.0096	0.0094	0.0091	0.0089	0.0087	0.0084
−2.2	0.0139	0.0136	0.0132	0.0129	0.0125	0.0122	0.0119	0.0116	0.0113	0.0110