PROTOCOLO DE SEGURIDAD ORIENTADO A IPv6 - IPsec

RICARDO ALFONSO PARAMO MELO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ D.C.
2020

PROTOCOLO DE SEGURIDAD ORIENTADO A IPv6 - IPsec

RICARDO ALFONSO PARAMO MELO

Proyecto de Grado – Monografía presentado para optar por el titulo de
ESPECIALISTA EN SEGURIDAD INFORMATICA

John Freddy Quintero Tamayo
Director de Proyecto
Yenny Stella Núñez Alvarez
Asesora - Ingeniero de Sistemas, Especialista en Seguridad Informática

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ D.C.
2020

NOTA DE ACEPTACIÒN

Firma del Presidente de Jurado

Firma del Jurado

Firma del Jurado

Bogotá D.C., 23 noviembre de 2020

DEDICATORIA

Dedico el presente trabajo a toda mi familia que de una u otra forma apoyaron el esfuerzo, dedicación y constancia para dar cumplimiento a una meta trazada, en donde con cada una de las palabras de aliento en los momentos más difíciles lograron dar el impulso necesario para procurar el cumplimiento en una las etapas de la vida.

AGRADECIMIENTOS

Agradezco a todas las personas que hacen e hicieron parte de la familia Unadista, quienes apoyaron y brindaron una orientación oportuna en este camino del conocimiento, por otro lado, mi agradecimiento va dirigido a la entidad donde laboro, la cual me apoyo económicamente, logrando así cumplir con las metas personales propuestas.

CONTENIDO

pág.

INTRODUCCIÓN 19

1 DEFINICIÓN DEL PROBLEMA 21

1.1 ANTECEDENTES DEL PROBLEMA 21

1.2 FORMULACIÓN DEL PROBLEMA 21

2 JUSTIFICACIÓN 24

3 OBJETIVOS 25

3.1 OBJETIVOS GENERAL 25

3.2 OBJETIVOS ESPECÍFICOS 25

4 MARCO REFERENCIAL 26

4.1 MARCO CONCEPTUAL Y TEÓRICO 26

4.2 MARCO HISTORICO 30

5 DISEÑO METODOLÓGICO 34

5.1 METODOLOGIA DE LA MONOGRAFIA 34

5.2 FASES PARA EL DISEÑO DE LA MONOGRAFIA 34

6 ANALIZAR LA ESTRUCTURA DE CADA UNO DE LOS PROTOCOLOS DE COMUNICACIONES VIGENTES IPV4 E IPV6 35

6.1 PROTOCOLO IPV4 35

6.2 PROTOCOLO IPV6 39

6.2.1 CABECERAS DE IPV6 39

6.2.2 CABECERAS DE EXTENSIÓN 43

6.2.3 ESTRUCTURA DE DIRECCIONES IPv6 44

6.2.4 REGLAS PARA LA ESCRITURA DE DIRECCIONES IPv6 47

6.2.5 PROTOCOLO ICMPV6 48

6.2.6 TIPOS DE PROTOCOLOS DE ENRUTAMIENTO EN IPv6 49

6.2.6.1 PROTOCOLOS DE RUTEO INTERNOS (IGP) 50

6.2.6.2 PROTOCOLOS DE RUTEO EXTERNOS (EGP) 51

6.2.7 CONFIGURACION DEL PROTOCOLO IPV6 SOBRE LINUX 51

7 IDENTIFICAR VENTAJAS DE SEGURIDAD DEL PROTOCOLO IPV6 SOBRE LA INFRAESTRUCTURA DE LA RED EN LA ORGANIZACION 55

7.1 INTEGRIDAD Y AUTENTICIDAD DE LOS DATOS TRANSMITIDOS 55

7.2 CONFIDENCIALIDAD 55

7.3 DETECCIÓN DE REPETICIONES 55

7.4 CONTROL DE ACCESO: AUTENTICACIÓN Y AUTORIZACIÓN. 56

8 CONOCER LAS MEDIDAS DE SEGURIDAD QUE IMPLEMENTA EL NUEVO PROTOCOLO IPV6 57

8.1 SEGURIDAD DE IPSEC EN IPV6 57

8.2 AMENAZAS A LA SEGURIDAD DE IPV6 58

8.3 AMENAZA NDP - (NEIGHBOR DISCOVERY PROTOCOL) 59

8.4 RFC QUE APLICAN SEGURIDAD EN IPV6 60

8.5 RIESGOS AL NO IMPLEMENTAR IPV6 64

8.6 ESTABLECER LAS RAZONES POR LAS CUALES SE DEBE MIGRAR EL PROTOCOLO IPV4 A IPV6 64

8.6.1 PROBLEMAS IDENTIFICADOS DE IPv4 66

8.6.2 CARACTERISTICAS DEL PROTOCOLO IPV6 67

8.6.3 RECURSOS NUMERICOS 69

8.7 DESCRIBIR LOS MODOS DE TRANSMISION DE LA INFORMACION A TRAVÉS DEL PROTOCOLO IPV6 74

8.7.1 MODO TRANSPORTE CON IPSEC 74

8.7.2 MODO TÚNEL CON IPsec 75

8.8 RELACIONAR LOS TIPOS DE DIRECCIONAMIENTO CON QUE CUENTA IPV6 77

8.8.1 TIPO DE DIRECCIONAMIENTO EN IPv6 77

8.8.1.1 DIRECCIÓN UNICAST (UNO a UNO) 77

8.8.1.2 DIRECCIÓN MULTICAST (UNO A VARIOS) 78

8.8.1.3 DIRECCIÓN ANYCAST (UNO A LA MAS CERCA) 79

8.8.2 DIRECCIONES RESERVADAS EN IPv6 79

8.8.2.1 DIRECCIONES IPv6 NO ESPECIFICADA (::/128) 80

8.8.2.2 DIRECCIONES DE LOOPBACK (::1/128) 81

8.8.2.3 DIRECCION UNICAST DE ENLACE LOCAL (FE80::/10) 81

8.8.2.4 DIRECCIÓN LOCAL ÚNICA – ULA (FC00::/7 HASTA FDFF::/7) 82

8.8.2.5 DIRECCIÓN DE DOCUMENTACIÓN (2001:0db8::/32) 82

8.8.2.6 DIRECCIÓN LINK -LOCAL (FE80::/10) 82

8.8.2.7 DIRECCIÓN DE BUCLE INVERTIDO 82

8.8.3 DIRECCIONAMIENTO IPv6 Y SU CONFIGURACIÓN 83

8.8.3.1 STATELESS ADDRES AUTO-CONFIGURACTION (SLAAC) 83

8.8.3.2 DYNAMIC HOST CONFIGURACTION PROTOCOL VERSIÓN 6 (DHCPV6) 84

8.8.4 DIRECCIONES IPv4 QUE SON COMPATIBLES DE IPv6 84

8.9 IDENTIFICAR LOS MOTIVOS POR LOS CUALES DEBE EXISTIR UNA CONVIVENCIA DE IPV4 CON IPV6. 86

8.9.1 DOBLE PILA - DUAL-STACK 86

8.9.2 TÚNELES 87

8.9.2.1 CLASES DE TÚNELES 89

8.9.2.2 TIPOS DE TÚNELES 90

8.9.3 MECANISMOS BASADOS EN TRADUCCION 94

8.9.3.1 SOLO IPV6 A SOLO IPV4 94

8.9.3.2 SOLO IPv4 A SOLO IPV6 (OBSOLETO SEGÚN RFC 4966) 95

8.10 ESTRUCTURA, FUNCIONALIDAD Y SEGURIDAD OFRECIDA POR IPSEC 96

8.10.1 ESTRUCTURA DE IPSEC 96

8.10.1.1 PROTOCOLOS DE SEGURIDAD DE TRAFICO (AH) 99

8.10.1.2 PROTOCOLOS DE SEGURIDAD DE TRAFICO (ESP) 101

8.10.1.3 PROTOCOLO SEGURIDAD - IKE 103

8.10.1.4 BASES DE DATOS: “SECURITY ASSOCIATION DATABASE – SAD” Y “SECURITY POLICY DATABASE – SPD” 104

8.10.2 MÉTODO DE COMUNICACIÓN SEGURA MEDIANTE IPSEC (MODO DE FUNCIONAMIENTO IPSEC) 105

9 CONCLUSIONES 107

10 RECOMENDACIONES 108

BIBLIOGRAFÍA 109

LISTA DE TABLAS

pág.

Tabla 1. Comparativo entre la estructura del modelo OSI y TCP/IP 27
Tabla 2. Diferencias y similitudes entre modelo OSI y TCP/IP 27
Tabla 3. Tipo de servicio según aplicación en IPv6 37
Tabla 4. Siguiente Cabecera IPv6 “ 42
Tabla 5. Referencias RFC para las Cabecera de Extensión IPv6 43
Tabla 6. Estructura de una dirección IPv6 44
Tabla 7. Hexadecimales utilizados por en el direccionamiento IP 45
Tabla 8. Mensajes básicos de error en ICMPv6 49
Tabla 9. RFC que aplican todos los temas de IPv6 incluida la seguridad 60
Tabla 10. Ejemplo de estructura de una dirección IPv6 para un Usuario 71
Tabla 11. Direcciones reservadas en IPv6 80
Tabla 12. Formatos de direcciones IPv6 compatibles con IPv4 85
Tabla 13. Ejemplo de Direcciones compatibles 85
Tabla 14. Direccionamiento 6to4 92

LISTA DE FIGURAS

Pág.

Figura 1. Estructura IPv4 36
Figura 2. Campos de la cabecera IPv6 40
Figura 3. Estructura de asignación de direcciones IP 46
Figura 4. Repositorio de carga de IPsec 52
Figura 5. Configuración del archivo de configuración IPsec 53
Figura 6. Aplicación de la configuración del archivo IPsec 53
Figura 7. Verificación de la configuración del IPsec 54
Figura 8. Ataque ND 60
Figura 9. Organizaciones para asignación de direccionamiento IPv6 69
Figura 10. Jerarquía de asignación de direcciones IP 71
Figura 11. Modo de transporte IPsec 75
Figura 12. Modo de transporte Punto a Punto 75
Figura 13. Modo Túnel Ipsec 76
Figura 14. Red Interna - Intranet de una organización 76
Figura 15. Canal VPN 77
Figura 16. Dirección IPv6 local. 81
Figura 17. Proceso EUI-64 84
Figura 18. Dual-Stack 87
Figura 19. Estructura Router a Router 88
Figura 20. Estructura Router a Host 88

Figura 21. Estructura Host a Router 89
Figura 22. Estructura Host a Host 89
Figura 23. Estructura Túnel 6over4 91
Figura 24. Túnel 6to4 92
Figura 25. Túnel DS-Lite 94
Figura 26. Mecanismo Basado en Traducción de IPv6 a IPv4 95
Figura 27. Mecanismo basado en Traducción IPv4 a IPv6 96
Figura 28. Estructura de seguridad Protocolo IPsec 98
Figura 29. Arquitectura General IPsec 99
Figura 30. Protocolo AH 100
Figura 31. Protocolo ESP 102
Figura 32. Método de cifrado AES 103

LISTA DE GRAFICAS

pág.

Grafica 1. Distribución de bloques IPv6 por País 73

Grafica 2. Adopción de IPv6 a nivel mundial 74

GLOSARIO

CABECERA IP: Es la parte del protocolo IP que unido a los datos que vienen de la capa de transporte crean el datagrama IP.

AH: Protocolo encargado de verificar las cabeceras para garantizar integridad, autenticación del datagrama desde el origen hasta su destino.

DIRECCIONAMIENTO IP: Protocolo de Internet utilizado a nivel de la capa 3 (capa de red) para transmisión de datos a través de conexión a internet

DIRECCIONAMIENTO IPv6: Interfaz de red entre host bajo el protocolo IPv6.

DATAGRAMA: Paquete de datos básico asociada a una red de comunicación

DHCP: "Dynamic Host Configuration Protocol – Protocolo de direccionamiento dinámica de host", brinda a los usuarios de una red los parámetros necesarios para la conexión a una red.

DISPONIBILIDAD: Servicio o información presente para ser accezada en el momento que se requiera.

EGP: "Exterior Gateway Protocol" Protocolo utilizado por los routers para el intercambio de información.

ENCAPSULAMIENTO: Proceso de transmisión en paquetes sobre la red de datos

ESP: Carga de seguridad encapsulada utilizada en IPsec para proporcionar autenticación integridad de los mensajes transmitidos mediante el cifrado de paquetes.

ICMP: Protocolo utilizado por IPv6 para generación de mensajes de errores de control sobre la capa de internet.

IGP: "Interior Gateway Protocol" Protocolo utilizado por los routers para el intercambio de información.

IKE: "Internet Key Exchange" Protocolo encargado de la gestión e intercambio de claves en internet

INTEGRIDAD: Es la característica en la cual la información no es modificada por persona diferente a la autorizada.

IPng: "Internet Protocol Next Generation - Protocolo de Internet de Siguiente Generación". Este término fue utilizado mientas se establecía la nueva versión de

dirección IP, la que en su momento fue la versión 6, por tal motivo cambio se nombre a IPv6.

IPv4: Cuarta versión del protocolo de internet destinado a la interconexión de redes a través del servicio de internet

IPv6: Sexta versión del protocolo de internet destinado a la interconexión de redes a través del servicio de internet

IPsec: Conjunto de protocolos de seguridad que cuenta con tres servicios puntuales como son: autenticación, integridad y confidencialidad de los datos transmitidos a través del canal de internet.

LACNIC: Organización encargada de la asignación de direccionamiento IP para América Latina y el Caribe

NAT: "Network Addres Translation - Traducción de Direcciones de Red", este mecanismo fue implementado por el agotamiento de direccionamiento IPv4, el cual consiste en utilizar una o varios direcciones publicas frente a múltiples direcciones privadas.

NAT64 / DNS64: Son mecanismos que permiten a host configurado con IPv6 una comunicación con un host configurado con IPv4, mediante un servidor NAT64 el cual crea un mapeo de NAT entre las direcciones IPv4 e IPv6 permitiendo así una comunicación entre los dos protocolos. El servidor DNS64 resuelve las peticiones de dominio realizadas por un host IPv4 sobre direcciones IPv6[1].

RFC: Publicaciones realizadas por un grupo interdisciplinario de ingenieros expertos en temas de comunicación.

TCP: Protocolo de transporte de internet, destinado a la conexión de equipos de comunicaciones.

TUNEL: Camino protegido y seguro por el cual es transportado los paquetes de datos a través de un canal de internet.

TÚNELES PUNTO A PUNTO: Se conectan dos puntos de red, o interfaces de túnel, en donde por un extremo ingresa al túnel un encapsulado para llegar al otro extremo del túnel donde será desencapsulada para obtener el paquete original.

[1] FRANCISCONI, Hugo Adrian. 2005. IPsec en Ambientes IPv4 e IPv6. Carril Godoy Cruz 2801, Villa Nueva, Guaymallén : Mendoza Argentina, 2005.

TÚNELES MULTIPUNTO: Conecta varios puntos de red o interfaces de túnel, de tal manera que un paquete se encapsula y puede ser entregado en uno de varios posibles puntos de salida del túnel.

RESUMEN

Con la necesidad de expansión que tiene internet y la declaratoria de agotamiento del direccionamiento IPv4 por parte de IANA, entidad dedicada a supervisar la asignación global de direcciones IP, surgió en 1998 el nuevo protocolo de comunicaciones denominado IPV6 el cual reemplazaría a IPv4 gracias a que cuenta con un direccionamiento de 128 bits en comparación con los 32 bits de la versión anterior, cubriendo las necesidades de direccionamiento IP y con ella viene una solución de seguridad muy potente denominada IPsec.

El protocolo IPsec integrada en IPv6 características de seguridad como: encabezados de autenticación AH, autenticación de origen de los datos, cifrado de seguridad ESP y utilización de VPN o túneles.

Es de precisar que para una entidad, la realización de la transición de IPv4 a IPv6 debe realizarse de manera gradual y con anterioridad efectuar un estudio en donde se contemple infraestructura existente, software utilizado y la red de internet brindada por el ISP, todo este conjunto de variables debe estar alineado y configurado para que mediante la ayuda de ambientes de transición como dual-stack se permita la comunicación de paquetes tanto de IPv4 como IPv6 de tal forma que no exista traumatismo y sea transparente para los usuarios que utilizan la red.

ABSTRACT

With the need for expansion of the internet and the declaration of exhaustion of IPv4 addressing by IANA, an entity dedicated to supervising the global allocation of IP addresses, the new communications protocol called IPV6 emerged in 1998, which would replace IPv4 thanks to the fact that It has 128-bit addressing compared to 32-bit in the previous version, covering IP addressing needs and with it comes a very powerful security solution called IPsec.

The IPsec protocol built into IPv6 security features such as: AH authentication headers, data origin authentication, ESP security encryption, and use of VPNs or tunnels.

It is necessary to specify that for an entity, the transition from IPv4 to IPv6 must be carried out gradually and beforehand carry out a study that includes existing infrastructure, software used and the internet network provided by the ISP, all this set The number of variables must be aligned and configured so that through the help of transitional environments such as dual-stack, the communication of both IPv4 and IPv6 packets is allowed in such a way that there is no trauma and is transparent for the users who use the network.

INTRODUCCIÓN

Para el presente trabajo de monografía se tratará el tema de **Seguridad IPsec en el protocolo IPV6**, dado que existe una necesidad vigente a nivel mundial de que todas las organizaciones implementen este protocolo a la mayor brevedad posible dado el agotamiento de direccionamiento actual de IPv4[2], se hace necesario la migración a un estándar que proporcione la esencia de IPv4 sumado a atributos necesarios en la actualidad como protocolo más seguridad, movilidad, mayor rendimiento, soporte a aplicaciones en tiempo real, compatibilidad, asignación de IPs desde el cliente.

El internet se ha convertido en un servicio indispensable tanto a nivel de organización, empresarial y personal, y dado que con el pasar de los años se han detectado vulnerabilidades en el protocolo de comunicaciones IPV4, en donde se han corregido dichas falencias de seguridad mediante la versión 6 con IPsec.

La función principal de IPsec es de asegurar las comunicaciones de extremo a extremo mediante mecanismos de seguridad como es el de encapsulado y encriptación utilizando protocolos de seguridad como ISAKMP para el intercambio de mensajes entre redes, definiendo enrutamiento y envió de paquetes.

El protocolo IPv6 ó IPng (IP Next Generation – IP de nueva generación)[3], es un protocolo que ha generando grandes posibilidades de conectividad a las nuevas tecnologías como es el auge de IoT (Internet of Things – Internet de las Cosas)[4], inteligencia artificial y en general permitirá a internet seguir creciendo, más aun teniendo en cuenta la cuarta revolución industrial en la que actualmente nos encontramos[5].

Teniendo en cuenta que, aunque IPv6 incorpora nuevas funcionalidades y protocolos de seguridad mediante la autenticación de datos, encriptación de datagramas, no existe una completa seguridad si no se realiza todas las configuraciones de manera adecuada en los equipos de comunicaciones que intervienen en una comunicación de información.

---

[2] BARRIO, Moises. 2018. Las direcciones IP se agotan y ahora llega el problema de IPv6. [En línea] 22 de enero de 2018. [Citado el: 2020 de abril de 25.] https://retina.elpais.com/retina/2018/01/19/innovacion/1516375772_148950.html.

[3] TELEMATIQUE – Revista electronica de Estudios Telematicos, IP Versión 6: La Nueva Generación IP, Universidad Rafael Belloso Chacib, 2003, Volumen 2, Edición 2, tomado de: https://dialnet.unirioja.es/descarga/articulo/2968291.pdf

[4] JJTORRES. 2014. ¿Qué es y cómo funciona el Internet de las cosas? [En línea] 20 de octubre de 2014. https://hipertextual.com/archivo/2014/10/internet-cosas/.

[5] CARROLLO EDINA, Carlos, Caracterización de IPv6, Docente de la Universidad del Bosque y la Universidad Católica. Bogotá, Colombia, p114.

Otro de los temas que son relevantes en la seguridad IP corresponde a que en muchos de los sistemas no se puede realizar una implementación de IPv6 limpia, es decir, que solamente se cuente con el protocolo IPv6, dejando completamente de lado IPv4, sin embargo, es de precisar que al establecer una comunicación y al otro extremo no se cuenta igualmente solamente con IPv6, se tendría que realizar conversiones que pueden crear en un momento dado brechas de seguridad.

1 DEFINICIÓN DEL PROBLEMA

1.1 ANTECEDENTES DEL PROBLEMA

Debido al aumento de la tecnología a nivel mundial , muchos de los equipos tecnológicos que se han venido desarrollando y produciendo requieren un direccionamiento IP como medio de comunicación, lo cual genera un gran problema , teniendo en cuenta que desde hace ya varios años, el organismo LACNIC destinado a la asignación de direccionamiento IP tanto en América Latina como a la región del Caribe, dio a conocer sobre el agotamiento del direccionamiento IPV4[6], por lo cual se debía adoptar el direccionamiento IPV6[7], el cual cuenta con mayor direccionamiento y corrección de falencias en su estructura, sumado a esto, IPv6 cuenta con mayor nivel de seguridad de extremo a extremo en una comunicación a través de los canales de internet .

1.2 FORMULACIÓN DEL PROBLEMA

Teniendo en cuenta el auge tecnológico a nivel mundial y el surgimiento del internet de las cosas[8], gran parte de los nuevos aparatos tecnológicos requieren direccionamiento IP, situación que ha retrasado en cierta medida el avance tecnológico, ya que no se cuenta con la cantidad necesaria de direccionamiento para que dichos aparatos se puedan comunicar a través de las redes, adicionalmente, es importante recalcar la seguridad que debe contener cada uno de éstos equipos tecnológicos al ser conectados a las redes de comunicaciones, teniendo en cuenta que afecta la seguridad y privacidad[9] de los usuarios finales, mediante equipos como: cámaras, sensores, televisores, neveras, etc.

---

[6] BARRIO, Moises. 2018. Las direcciones IP se agotan y ahora llega el problema de IPv6. [En línea] 22 de enero de 2018. [Citado el: 2020 de abril de 25.] https://retina.elpais.com/retina/2018/01/19/innovacion/1516375772_148950.html.

[7] LACNIC. Fases de Agotamiento de IPv4. [En línea] https://www.lacnic.net/1001/1/lacnic/fases-de-agotamiento-de-ipv4.

[8] JJTORRES. 2014. ¿Qué es y cómo funciona el Internet de las cosas? [En línea] 20 de octubre de 2014. https://hipertextual.com/archivo/2014/10/internet-cosas/.

[9] MOLINA GARCÍA, Jorge Alberto. La Importancia de la Gestión de Riesgos y Seguridad en el Internet de las Cosas (IOT). Universidad Piloto de Colombia Bogotá, Colombia. [En línea] http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277

Con el protocolo IPV6 viene una nueva solución de seguridad llamada IPsec[10] la cual es importante conocer a detalle dado que actualmente es una necesidad de conocimiento para cualquier organización ya sea pública o privada, teniendo en cuenta que se quiera o no, se debe realizar un despliegue de manera masiva a nivel mundial[11].

El desconocimiento de la infraestructura del protocolo IPv6 y su correspondiente protocolo de seguridad IPsec, podría causar en cierta medida a una organización tomar decisiones a la ligera y poco favorable a nivel estructura física y seguridad información[12].

IPsec es una parte esencial de IPv6 dado que implementa cifrado, autenticación y redes privadas VPN desde extremo a extremo, utilizando extensiones de encabezado ESP el cual proporciona confidencialidad en el flujo de tráfico, autenticación de las fuentes y protección contra ataques de repetición[13].

A nivel tecnológico se realizan anualmente gran cantidad de reuniones presenciales, conferencias vía web y charlas entre otras actividades, las cuales van dirigidas a dar a conocer la problemática en cuanto al agotamiento de direccionamiento IP[14] y ventajas de implementación del nuevo protocolo de IPv6, las cuales requieren un conocimiento previo para lograr entender de manera teórica las comunicaciones seguras mediante IPsec de IPv6[15].

---

[10] HOGG, Scott and VYNCKE Eric . 2009. IPv6 Security. [En línea] 2009. https://books.google.es/books?hl=es&lr=&id=kwOv0Aw2lIUC&oi=fnd&pg=PT26&dq=ipv6+ipsec+and+vpns&ots=Qnl27HBWYg&sig=aKqVWpudX6guT_QebX6LRG5xgi8#v=onepage&q=ipv6%20ipsec%20and%20vpns&f=false.

[11] MINTIC, Guía de Transición de IPv4 a IPv6 para Colombia, https://www.mintic.gov.co/gestionti/615/articles-5482_G20_Transicion_IPv4_IPv6.pdf

[12] RISTI, Edwin Barrientos; AVENDAÑO, Dewar Rico; BAUTISTA, Luis Anderson Coronel y ROJAS, Fabian Ranulfo, Granja inteligente: Definición de infraestructura basada en internet de las cosas, IpV6 y redes definidas por software, 2018, tomado de: https://www.researchgate.net/profile/Dewar_Rico-Bautista/publication/331178386_Smart_farm_Defining_of_infrastructure_based_on_internet_of_things_IpV6_and_software_defined_networks/links/5d09acf8299bf1f539cf062c/Smart-farm-Defining-of-infrastructure-based-on-internet-of-things-IpV6-and-software-defined-networks.pdf

[13] JASON G., Andres, IPv6: the nextInternet protocol, abril 2005, tomado de: https://static.usenix.org/publications/login/2005-04/pdfs/andress0504.pdf (JASON G, 2005)

[14] BARRIO, Moises. 2018. Las direcciones IP se agotan y ahora llega el problema de IPv6. [En línea] 22 de enero de 2018. [Citado el: 2020 de abril de 25.] https://retina.elpais.com/retina/2018/01/19/innovacion/1516375772_148950.html.

[15] MINTIC, Guía de Transición de IPv4 a IPV6 PARA Colombia, tomado de: https://www.mintic.gov.co/gestionti/615/articles-5482_G20_Transicion_IPv4_IPv6.pdf

Las organizaciones del estado deben cumplir los lineamientos establecidos por Mintic en la resolución 2710 de 2017[16] sobre la implementación del protocolo IPv6 en Colombia. Dentro de los aspectos más relevantes descritos en la resolución se tiene que las entidades estatales de carácter nacional a más tardar el 31 de diciembre del 2019 deben implementar la tecnología IPv6, en coexistencia con el IPv4. Para entes territoriales, el plazo máximo es el 31 de diciembre del 2020[17].

Así mismo las organizaciones no gubernamentales que desee hacer un salto tecnológico hacia el futuro con miras a una interconexión que brinde mayor seguridad mediante IPsec enmarcada en el protocolo de IPv6[18], debe tener en cuenta que el protocolo IPv6 no es lo mismo que IPv4 y que dicha transición es un proceso costoso y que puede generar un alto riesgo en cuanto a la disponibilidad de la información[19], situación que implica que el personal involucrado en el proyecto adquiera en un principio los conocimientos teóricos, los cuales están dados en la presente monografía.

[16] MINTIC, Resolución 2710 de 2017, 2017, tomado de : https://www.mintic.gov.co/portal/inicio/61000:Resolucion-2710-de-2017

[17] MINTIC, Entró en vigencia la resolución 2710 del 2017 para la implementación del protocolo IPv6 en Colombia, 23 de octubre de 2017, tomado de: https://www.mintic.gov.co/portal/inicio/Sala-de-Prensa/Noticias/61192:Entro-en-vigencia-la-resolucion-2710-del-2017-para-la-implementacion-del-protocolo-IPv6-en-Colombia

[18] AMBROSIO, Paola – CIO Función Pública, Gobiernos de la región ayudan a promover el despliegue de IPv6, 20 diciembre 2017, tomado de: https://www.funcionpublica.gov.co/eva/red/publicaciones/gobiernos-de-la-regi%C3%B3n-ayudan-a-promover-el-despliegue-de-ipv6.

[19] MINTIC, Guía de Transición de IPv4 a IPV6 PARA Colombia, tomado de: https://www.mintic.gov.co/gestionti/615/articles-5482_G20_Transicion_IPv4_IPv6.pdf

2 JUSTIFICACIÓN

Siguiendo los lineamientos establecidos por MINTIC, se hace necesario que todas las entidades tanto estatales como privadas a nivel nacional realicen una migración del protocolo de comunicaciones de IPv4 a IPv6 por razones de seguridad y agotamiento de direcciones IPv4.

Dado lo anterior, es importante conocer toda la estructura del protocolo IPv6, lo relacionado la seguridad con Ipsec y sus beneficios, funcionalidades que trae éste nuevo protocolo sobre la infraestructura de la red de cualquier organización.

Debido a que el protocolo IPv6 es un protocolo que se está implementando desde hace muy poco tiempo en Colombia, muchas de las organizaciones no cuentan con la información y conocimientos necesarios para la adopción de este nuevo protocolo y más teniendo en cuenta que no es compatible con IPv4 en su totalidad[20], situación que obliga a que las organizaciones para que tengan una convivencia entre los dos protocolos durante un periodo de cambio o transición de IPv4 a IPv6[21], mientras todos los aplicativos y equipos de infraestructura sean configurados o migrados a la nueva tecnología[22].

Es importante tener en cuenta que no todos los equipos tecnológicos cuentan con la posibilidad de configuración sobre IPv6, por tal motivo antes de que una organización tome la decisión de migración, se debe realizar un estudio que debe contener un inventario de activos físicos y lógicos para poder determinar si requieren o no de una renovación tecnológica[23].

Dada la gran cantidad de información que se tiene en la red, es importante recopilar esa información y darla a conocer de una manera sencilla y fácil de entender, de tal forma que algún directivo de una organización pueda asimilarla y tomar una decisión acorde a su capacidad y con miras cumplir los requerimientos establecidos por los entes Tecnológicos del estado Colombiano como es Mintic.

---

[20] MEDINA CASTILLO, Carlos A. y FORERO RODRIGUEZ, Felipe. 2011. Caracterización de IPv6. [En línea] 14 de noviembre de 2011. https://dialnet.unirioja.es/descarga/articulo/4239524.pdf.

[21] VIVES, Alvaro. . 2015. LACNIC. Curso IPv6 Básico Módulo 2: Agotamiento espacio IPV4, coexistencia y transición – Mecanismos de Transición. [En línea] 5 de junio de 2015. https://www.youtube.com/watch?v=LQQD7-8E4c8&list=PLJ3jHT8E6frAuYS73uN2QLWi8qyXRyxo1&index=9.

[22] GOOGLE IPV6. Adopción de IPv6 . [En línea] https://www.google.com/intl/es/ipv6/statistics.html#tab=ipv6-adoption.

[23] Ibid.

3 OBJETIVOS

3.1 OBJETIVOS GENERAL

Investigar y documentar la estructura del protocolo IPv6 con el propósito de identificar las mejoras de seguridad a nivel de IPsec.

3.2 OBJETIVOS ESPECÍFICOS

- Analizar la estructura de cada uno de los protocolos de comunicaciones vigentes IPv4 e IPV6
- Identificar ventajas de seguridad del protocolo IPV6 sobre la infraestructura de la red en la organización.
- Conocer las medidas de seguridad que implementa el nuevo protocolo IPV6

4 MARCO REFERENCIAL

4.1 MARCO CONCEPTUAL Y TEÓRICO

Desde la aparición de los primeros equipos de cómputo, se creó la necesidad de comunicación entre ellos, es por eso que la organización internacional de estándares (International Organization for Standardization – ISO) en 1980 estandarizó el protocolo de comunicaciones mediante la adopción del modelo OSI (Open System Interconnection) 7 capas permitiendo así la comunicación de computadores al interior de una red[24], proporcionando un conjunto de normas que aseguraban la compatibilidad entre las distintas tecnologías de red utilizadas por las empresas fabricantes.

Tras múltiples intentos y al ser inventada las primeras computadoras, se creó la necesidad de establecer comunicación entre ellas, es por ello que se conformaron redes de comunicaciones entre computadoras, estableciéndose un protocolo denominado TCP/IP[25], el cual permitía la comunicación entre las computadoras que se encontraban dentro de una misma red. Este desarrollo fue dado por el Departamento de Defensa de los Estados Unidos dentro del proyecto denominado ARPANET[26].

En la tabla 1 se observa el comparativo en entre el modelo OSI[27] y el protocolo de modelo de transmisión TCP/IP, teniendo en cuenta que el modelo TCP/IP describe las funcionalidades de la transmisión, mientras que el modelo OSI describe las interconexiones de sistemas abiertos. Ambos protocolos describen una arquitectura para establecer comunicación entre computadores o equipos de comunicación que se encuentran dentro de una misma organización o a kilómetros de distancia al otro lado del planeta.

---

[24] FERNÁNDEZ ALDANA Luis Antonio, Transmisión Y Comunicación de Datos, p. 4,5 y 6, tomado de: http://www.ilustrados.com/documentos/transmiscomunicacaciondatos.doc.

[25] ROBLEDANO, Ángel. 2019. OpenWebinars. Qué es TCP/IP. [En línea] 18 de junio de 2019. https://openwebinars.net/blog/que-es-tcpip/.

[26] ARPANET, diciembre 2017, tomado de: https://nic.ar/es/enterate/novedades/arpanet-el-origen-de-internet.

[27] FERNÁNDEZ ALDANA Luis Antonio, Transmisión Y Comunicación de Datos, p. 4,5 y 6, tomado de: http://www.ilustrados.com/documentos/transmiscomunicacaciondatos.doc.

Tabla 1. Comparativo entre la estructura del modelo OSI y TCP/IP

Modelo OSI	**Modelo TCP/IP**
Open System Interconnection	Transmission Control Protocol/Internet Protocol
7. Aplicación (FTP,HTTP,SMTP,DND,SNMP) 6. Presentación (ASN.1, MIME) 5. Sesión (SCP,RCP,SQL,NFS)	Aplicación
4. Transporte (TCP)	Transporte
3. Red (IP)	Internet
2. Enlace de Datos (Ethernet -Red) 1. Fisica (Cables, Conectores)	Acceso a la Red

Fuente: TICO, R. P. (s.f.). Comparativa OSI frente TCP/IP. Obtenido de https://sites.google.com/site/raquelpereztico/trasmision-de-datos-en-las-redes/0-6-comparativa-osi-frente-tcp-ip

En la tabla 2 se observa algunas diferencias y similitudes representativas entre el modelo TCP/IP – Protocolo de Control de Transmisión/ Protocolo de Internet, los cuales en conjunto son utilizados para que los equipos de comunicaciones de conecten a internet de manera fiable, este modelo fue definido mucho antes del modelo OSI – Interconexión se Sistemas Abiertos, sin embargo, ambos protocolos tienen como propósito el mismo fin[28].

Tabla 2. Diferencias y similitudes entre modelo OSI y TCP/IP

Descripción	**Modelo OSI**	**Modelo TCP/IP**
DIFERENCIAS	Modelo teórico	Modelo práctico
	Sesión, Presentación y Aplicación son niveles independientes	Sesión y Presentación son combinadas en la capa de aplicación
	Las capas Física y Enlace de datos son niveles independientes	Las capas Física y Enlace de datos son combinadas en la capa de subred
	Las redes bajo éste modelo no se despliegan normalmente	Contiene protocolos sobre los cuales se desarrollan la

[28] FERNÁNDEZ ALDANA Luis Antonio, Transmisión Y Comunicación de Datos, p. 4,5 y 6, tomado de: http://www.ilustrados.com/documentos/transmiscomunicacaciondatos.doc.

	sobre OSI pero se utiliza como guía[29]	mayoría de las redes actuales como la internet[30]
SIMILITUDES	Ambos modelos se dividen en capas, sin embargo cada uno de ellos poseen diferente número de capas, es así, que el modelo OSI cuenta con 7 capas y el modelo TCP/IP cuenta con 4 capas Los dos modelos utilizan tecnología de conmutación por paquetes, es decir, que en una transmisión los datos son ensamblados en paquetes y transmitidos por un canal compartido, posteriormente son reensamblados en su destino para obtener la comunicación original. Ambos modelos son útiles y ayudan en la comunicación	

Fuente: "elaboración propia"

Desde que el internet es utilizado comercialmente, su protocolo de comunicación ha sido el IPV4, la cual cuenta con disponibilidad de 2^{32} direcciones IP, es decir, 4.294.967.296 direcciones, lo cual ha sido insuficiente dada la gran demanda que se ha tenido en los últimos años dado el avance tecnológico, situación que obligó la creación del nuevo protocolo IP versión 6, el cual cuenta con 2^{128} es decir 340.282.366.920.938.463.463.374.607.431.768.211.456, lo cual eliminaría la demanda y con un mayor nivel de seguridad[31].

Dentro de las bondades que nos brinda el nuevo protocolo de comunicaciones IPv6, se encuentran los factores de Seguridad como llaves, encriptación, integridad, autenticación y privacidad de la información que es transmitida entre dos hosts[32].

Por lo anterior es importante mencionar las siguientes teorías para soportar la presente monografía:

[29] TICO, Raquel Perez. Comparativa OSI frente TCP/IP. [En línea] https://sites.google.com/site/raquelpereztico/trasmision-de-datos-en-las-redes/0-6-comparativa-osi-frente-tcp-ip

[30] Ibid.

[31] LACNIC. *Curso IPv6 Básico Módulo 2: Agotamiento espacio IPV4, coexistencia y transición - Proyecciones de Agotamiento.* [En línea] 5 de junio de 2015. https://www.youtube.com/watch?v=-HIUT2ilCyU&list=PLJ3jHT8E6frAuYS73uN2QLWi8qyXRyxo1&index=6

[32] STALLINGS, William. Fundamentos de Seguridad en Redes Aplicaciones y Estandares, segunda edición, Person Preatice Hall, 2004.

1. Protocolo IPv4: De acuerdo a lo registrado en el RFC 791[33] se especifica el protocolo de internet estándar el cual establece la estructura y funcionalidades del protocolo IPv4, siendo esta teoría uno de los pilares que se ajusta a los documentos consultados para la elaboración del trabajo de monografía.

2. Protocolo IPv6: Según el RFC 2460 - Internet Protocol, Version 6 (IPv6)[34] expone el protocolo IPv6, definido como: "Este documento especifica un protocolo del track de estándares Internet para la comunidad Internet, y solicita debate y sugerencias para mejorías. Por favor remítase a la edición actual de los "Estándares de Protocolos Oficiales Internet" (STD 1) para el estado de estandarización y estatus de este protocolo. La distribución de este memorándum es ilimitada"[35], siendo un documento relevante dado que especifica la estructura principal del protocolo IPv6.

3. Estandarización del protocolo de comunicación: Según lo considerado por Herrera Perez[36], quien expone en su libro "Tecnología y Redes de Transmisión de Datos" de manera amplia el Modelo OSI, el cual conforma la base introductoria al tema objeto del presente trabajo sobre Protocolo IPv6 enfocado a la seguridad.

4. IPv6, una realidad: Según lo expuesto por Vélez Varela y Gutiérrez Rancruel[37] expone la evolución del internet y el auge que ha tenido a nivel mundial y por ende el agotamiento de direcciones IP, así mismo, describe los beneficios que trae el nuevo protocolo de comunicaciones IPv6 explicando su estructura, características y topología, coexistencia con IPv4[38], entre otros, lo cual se ajusta perfectamente con el proyecto de monografía planteado.

---

[33] INFORMATION SCIENCES INSTITUTE UNIVERSITY OF SOUTHERN CALIFORNIA. 1981. RFC: 791 - Especificacion del Protocolo. [En línea] septiembre de 1981. https://www.rfc-es.org/rfc/rfc0791-es.txt.

[34] NETWORK WORKING GROUP. 1998. Especificación Protocolo Internet, Versión 6 (IPv6). [En línea] diciembre de 1998. https://www.rfc-es.org/rfc/rfc2460-es.txt.

[35] Ibid.

[36] HERRERA PEREZ, Enrique. Tecnología y Redes de Transmisión de Datos, p 42-53

[37] VELEZ VARELA, Fernando y RANCRUEL GUTIERREZ, Liliana 2019. IPv6, una realidad. Bogotá - Colombia : Ediciones de la U, 2019, p 128.

[38] ALONSO,Juan Carlos. 2015. LACNIC. Curso introductorio de IPv6. [En línea] 2 de junio de 2015. https://www.youtube.com/watch?v=kwvINZmmXeM&list=PLJ3jHT8E6frAuYS73uN2QLWi8qyXRyxo1&index=1.

5. Protocolo de Seguridad IPsec: De acuerdo a lo expuesto por el ingeniero Marquez[39] "IPsec es un marco de trabajo que nos permite utilizar diversos protocolos y herramientas que dotan a nuestro tráfico con dicha seguridad", por lo cual esta teoría está directamente relacionada con el trabajo de monografía.

4.2 MARCO HISTORICO

Desde los inicios del internet siempre se tuvo la necesidad de aumentar los niveles de seguridad en la transmisión de datos, desde la aparición de la primera red de computadores llamada ARPANET[40] hasta nuestros días, con la utilización del protocolo IPv4 hasta la llegada del protocolo IPv6, el cual se encuentra actualmente en implementación a nivel global.

Para el año de 1969, se creó la primera red de computadoras en Estados Unidos llamada ARPANET, la cual poseía estructuras importantes y que aun hoy en día se mantienen, en donde se transmitía mensajes fragmentados por diferentes caminos y ensamblados en su destino[41].

Ya para septiembre de 1981, se definió el Protocolo de Internet (IPv4) en la RFC 791[42], en donde se establecieron las especificaciones y funcionalidades a nivel mundial por parte de ingenieros y personal especializado en el área de las comunicaciones[43]. En este documento se tomaron conceptos importantes ya tratados anteriormente en el protocolo ARPA y aspectos nuevos como tratamiento de errores, códigos opcionales, mejor nivel de seguridad, prioridad, comportamiento y características limitadas para el protocolo de internet.

En el año de 1983 ARPANET se divide en dos secciones: Una la sección militar de ARPANET adopta el protocolo TCP/IP para ser utilizados en las comunicaciones para la red de internet de manera independiente, creando su propia red denominada MILNET y una segunda sección utilizada por universidades y organizaciones empresariales las

---

[39] MARQUEZ, Guillermo. IPsec y redes Privadas Virtuales, p 4-14

[40] ARPANET, diciembre 2017, tomado de: https://nic.ar/es/enterate/novedades/arpanet-el-origen-de-internet

[41] Ibid.

[42] INFORMATION SCIENCES INSTITUTE University of Southern California, RFC: 791 - Internet Protocol, septiembre 1981, tomado de: https://www.rfc-es.org/rfc/rfc0791-es.txt

[43] SPEED CHECK, IPv4, tomado de: https://www.speedcheck.org/es/wiki/ipv4/

cuales igualmente debían de adoptar el protocolo TCP/IP, ya que de lo contrario serian desconectadas[44].

Para el año de 1990, debido al aumento de manera importante en la transmisión de información a través de las redes de internet, se realizaron los primeros estudios sobre el agotamiento de las direcciones de IPv4, dado que para este año ya se contaba con 313.000 equipos conectados a la red y para el año 1992 de se contaba con 1.130.000 equipos conectados[45].

En 1993 investigaciones un método de seguridad por AT&T Laboratorios Bell y la universidad de Columbia crearon un software llamada SIPP[46] uno de los precursores de Ipsec. Igualmente, para este año, se liberó por parte de Estados Unidos el servicio de internet a nivel comercial, situación que evidencio aún más que no se contaba con las direcciones IP necesarias para dar cumplimiento a las demandas de la época, pasando de 2.000 equipos conectados a más de 26.000.000 en el año 1997[47].

En 1986 se creó un grupo de trabajo IETF[48], conformada por ingenieros, programadores y desarrolladores donde crearon un conjunto de protocolos definidos en los estándares RFC 4301[49] y 4309[50], en donde dichas funciones se aplicaban en la capa IP y capas superiores como la de comunicaciones TCP/IP y UDP, dichos protocolos daban

---

[44] ARPANET, diciembre 2017, tomado de: https://nic.ar/es/enterate/novedades/arpanet-el-origen-de-internet.

[45] LACNIC, Curso IPv6 Básico, Modulo 2, agotamiento del espacio IPv4, Coexistencia y Transición, tomado de: https://www.youtube.com/watch?v=-HIUT2ilCyU&list=PLJ3jHT8E6frAuYS73uN2QLWi8qyXRyxo1&index=6

[46] AVILA DIAZ, Luis Miguel. 2013. Configurar IPSec. [En línea] 14 de may de 2013. https://www.youtube.com/watch?v=PuQRlRhv-BU.

[47] ALONSO, Juan Carlos. 2015. LACNIC. Por que utilizar IPv6 hoy. [En línea] 2 de junio de 2015. https://www.youtube.com/watch?v=5IvTIzhrvC4&list=PLJ3jHT8E6frAuYS73uN2QLWi8qyXRyxo1&index=4. de 2015. https://www.youtube.com/watch?v=2zjHCe0Y66I&list=PLJ3jHT8E6frAuYS73uN2QLWi8qyXRyxo1&index=3

[48] AVILA DIAZ, Luis Miguel. 2013. Configurar IPSec. [En línea] 14 de may de 2013. https://www.youtube.com/watch?v=PuQRlRhv-BU.

[49] NETWORK WORKING GROUP S. KENT. 2005. RFC 4301 – Security Architecture for the Internet Protocol. [En línea] diciembre de 2005. https://www.ietf.org/rfc/rfc4301.txt.

[50] FUSARIO, Ruben Jorge, Vulnerabilidades en la seguridad de las transacciones interactivas de comercioelectronico a traves de la web, 25 de octubre 2017, p 117.

integridad, confidencialidad y autenticidad en los datos. Para este mismo año se analizaron unas posibles soluciones para el agotamiento de direccionamiento como:

- Creación de un grupo llamado Grupo ROAD, encargado de analizar posibles soluciones y alargar en lo posible la cantidad de direccionamiento.
- Utilización de la característica CIDR normalizado mediante la norma RFC 4632[51], en donde se estableció un plan de asignación y agregación de direcciones de internet mediante las mejores prácticas.
- Utilización de prefijos según los grados de necesidad sin pensar en las clases A, B o C.
- Agregación de rutas mediante tablas de ruteo.
- Utilización los mecanismos de NAT mediante RFC 1918[52], para este mecanismo solamente se necesita una dirección publica de internet para tener salida a una red completa de computadores.

  Estas soluciones, aunque retardaron el agotamiento de direccionamiento en un 14%, no fue una solución definitiva para la demanda que se tenía para aquella época, sin embargo, fue fundamental para que se extendiera por algún periodo de tiempo e impulso la creación del Protocolo IPv6, la cual termino su desarrollo en 1996, sin embargo, hasta 1996 se implementaron las primeras redes sobre dicha versión 6[53].

  En 1998 definido por el RFC 2460[54] el cual especifica un grupo de estándares y estado del protocolo de internet que define las características del nuevo protocolo IPv6 en donde se describe el formato de cabecera, cabecera de extensión, tamaño de paquetes, clases de tráfico y manejo de capa superior del protocolo, definiendo características[55] como:

---

[51] NETWORK WORKING GROUP V. FULLER. 2006. RFC 4632 - Classless Inter-domain Routing (CIDR): The Internet Address Assignment and Aggregation Plan. [En línea] agosto de 2006. https://www.ietf.org/rfc/rfc4632.txt.

[52] NETWORK WORKING GROUP Y. REKHTER. 1996. RFC 1918 - Address Allocation for Private Internets. [En línea] febrero de 1996. https://www.ietf.org/rfc/rfc1918.txt.

[53] LACNIC. Curso IPv6 Básico Módulo 2: Agotamiento espacio IPV4, coexistencia y transición – Recomendaciones. [En línea] 5 de junio de 2015. https://www.youtube.com/watch?v=md80CcXGjY8&list=PLJ3jHT8E6frAuYS73uN2QLWi8qyXRyxo1&index=13

[54] NETWORK WORKING GROUP. 1998. Especificación Protocolo Internet, Versión 6 (IPv6). [En línea] diciembre de 1998. https://www.rfc-es.org/rfc/rfc2460-es.txt.

[55] LACNIC. Estadísticas de Asignación de LACNIC. [En línea] https://www.lacnic.net/web/lacnic/estadisticas-asignacion.

- Ampliación de direccionamiento IP a 128 bits
- Cabecera base simplificado
- Cabecera de extensión
- Calidad de los servicios (QoS)[56]
- Direccionamiento Unicast, Multicast y Anycasrt.
- Realiza la fragmentación al inicio del envió de paquetes de datos y reensamblaje del paquete de datos en su destino
- No utiliza NAT, dado que al contar con el protocolo IPv6, se tendría direcciones públicas en todos los dispositivos de comunicación.
- Comunicación cifrada y con nivel de seguridad mediante el protocolo IPsec en una comunicación de extremo a extremo

[56] ALONSO, Juan Carlos. 2015. https://www.youtube.com/watch?v=2zjHCe0Y66I&list=PLJ3jHT8E6frAuYS73uN2QLWi8qyXRyxo1&index=3

5 DISEÑO METODOLÓGICO

5.1 METODOLOGIA DE LA MONOGRAFIA

La presente monografía está basada en conocimientos académicos y profesionales adquiridos, apoyados en consultas documentales de tipo cualitativo en razón de que se analizará el problema, utilizando fuentes diversas como Libros, artículos, sitios web y monografías, con lo cual se podrá obtener los datos necesarios para desarrollar la documentación que permita un conocimiento específico sobre la seguridad que brinda el Protocolo IPsec sobre IPv6.

5.2 FASES PARA EL DISEÑO DE LA MONOGRAFIA

El trabajo de monografía se realizó con base en las siguientes etapas:

- Analizar la estructura de cada uno de los protocolos de comunicaciones vigentes IPv4 e IPV6

- Identificar ventajas de seguridad del protocolo IPV6 sobre la infraestructura de la red en la organización.

- Conocer las medidas de seguridad que implementa el nuevo protocolo IPV6

6 ANALIZAR LA ESTRUCTURA DE CADA UNO DE LOS PROTOCOLOS DE COMUNICACIONES VIGENTES IPV4 E IPV6

6.1 PROTOCOLO IPV4

El protocolo IPv4, corresponde a la versión 4 del protocolo IP (Internet Protocolo), siendo esta la primera versión del protocolo de comunicaciones que permitió la conexión masiva de equipos de comunicaciones mediante el servicio de internet, en donde la función principal es la de asignar una dirección de internet para cada uno de los equipos de comunicaciones [57](llámese PC, Router, Celular, Cámara de video, etc)[58].

IPv4 usa un direccionamiento de 32 bits (2^{32} = 4.294.967.296 direcciones IP). Teniendo en cuenta el avance tecnológico y el auge que ha tenido de manera acelerada el internet y por ende las comunicaciones en los últimos años[59], sumado a esto a la necesidad de contar con mayor seguridad y funcionalidad presentes en las conexiones, surgió el nuevo protocolo de comunicaciones IPv6, con muchas y mejoras sustanciales tanto a nivel de capacidades de direccionamiento como el de funcionalidades y características de seguridad (IPsec).

Dentro de los mecanismos utilizados ante al agotamiento de direccionamiento IP, se utilizó NAT (Network Address Traslation), el cual consistía en utilizar un rango de IPs sobre redes privadas de tal forma que se ocupaba solamente una o varias IPs públicas. Con esta alternativa las grandes empresas utilizaban unas pocas direcciones IP publicas en lugar de tantas como equipos hubiese en la empresa.

En IPv4 se tienen varios tipos de direccionamiento, unicast, Broadcast y Multicast. UNICAST, se utiliza en una comunicación host a host[60]. BROADCAST, cuando se requiere enviar información de un host a varios host de manera simultánea dentro de una red, sin la necesidad de realizar transmisión host por host, a este mecanismo se le

---

[57] FUENTES, Raul. IPv4 - Encabezado y estructura. [En línea] https://rfuentess.blogspot.com/2012/01/ipv4-encabezado-y-estructura.html

[58] ZAPATA VALDES, Rodrigo Horacio. 2013. Análisis de Seguridad en el Protocolo IPv6. [En línea] 2013. http://157.92.136.59/download/tpos/1502-0820_ZapataValdezRH.pdf.

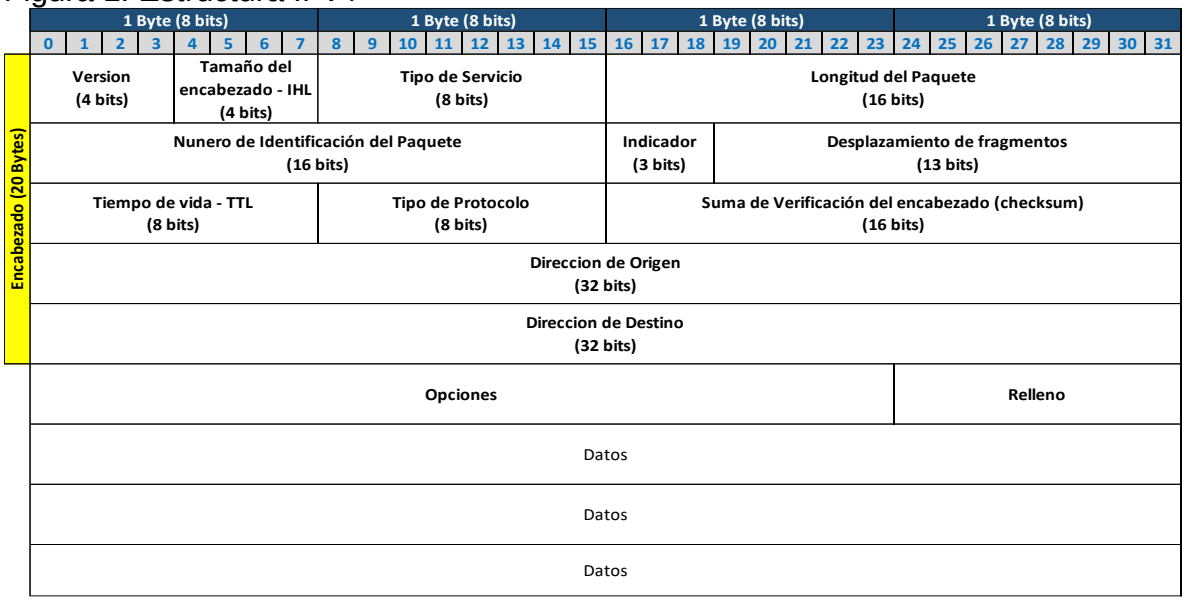
[59] LACNIC. Fases de Agotamiento de IPv4. [En línea] https://www.lacnic.net/1001/1/lacnic/fases-de-agotamiento-de-ipv4

[60] SPEED CHECK. IPv4. [En línea] https://www.speedcheck.org/es/wiki/ipv4/.

conoce como Broadcast. MULTICAST, envía paquetes de información de un host a un grupo de host que hagan parte de un grupo host establecidos[61].

Tanto los términos NAT como BROADCAST, no son tenidos en cuenta en IPv6, dado que con NAT se rompe el principio de comunicación directa de host a host y con BROADCAST no se requiere ya que se utilizaría Multicast local, que en principio se tendría el mismo efecto.

Figura 1. Estructura IPv4



Fuente: FUENTES, Raul; recuperado en 2017; Disponible en https://rfuentess.blogspot.com/2012/01/ipv4-encabezado-y-estructura.html

La estructura del protocolo IPv4 está dividida en paquetes de 32 bits (4 bytes). Dado que en IPv4 el orden en que se transmite la información es importante (denominada NBO - "Network Byte Order", es por eso que se tiene que el primer bit es el 0. Los datos de los encabezados en IPv4 son verdaderamente importantes, ya que se encuentra la información necesaria para que todos los dispositivos de comunicaciones interpreten la información que está siendo enviada teniendo claro cada uno de los campos[62]. La

[61] DORDOIGNE, Jose. 2015. Redes Informaticas - Nociones Fundamentales. Barcelona - España : Ediciones ENI, 2015. Primera.

[62] UPM, Grupo de Sistemas Operativos DATSI FI. 2012. Protocolo IPsec. [En línea] 8 de octubre de 2012, tomado de: http://laurel.datsi.fi.upm.es/proyectos/teldatsi/teldatsi/protocolos_de_comunicaciones/protocolo_ipsec.

estructura IPv6 la podemos ver en las figuras 1 y el detalle cada uno de ellos a continuación.

Versión: Especifica el formato de la versión del paquete, la información contenida es utilizada por los router y la capa IP de comunicación, en la cual cuentan con varias versiones de IP en un mismo host conectado a internet, es de tener en cuenta que por defecto los sistemas Operativos ya vienen con preconfiguración del protocolo IPv6[63].

Tamaño del Encabezado IHL – IP HEADER LENGTH: Este espacio indica la cantidad de palabras de 32 bits que puede ocupar el encabezado. Teniendo en cuanta que el valor mínimo son 5 palabras: se tendría, 5 palabras de 32 bits para un total de 160 bits, es decir, 5 x 32 = 160 como longitud de cabecera. El valor máximo son 15 palabras: se tendría, 15 palabras de 32 bits para un total de 480 bits, es decir 15x32=480 como longitud de cabecera[64].

Tipo de servicio: De los 8 bit que cuenta este campo, se tiene una distribución de la siguiente manera: Los 3 bits iniciales no son utilizados, los siguientes 4 bits identifican el tipo de servicio, y el último bit bebe ser siempre 0. En la tabla 3, muestra los valores típicos de acuerdo al tipo de aplicación[65].

Tabla 3. Tipo de servicio según aplicación en IPv6

Tipo de aplicación	Minimizar retraso	Maximizar rendimiento	Maximizar fiabilidad	Minimizar costo	Valor en Hexadecimal
TELNET	1	0	0	0	0X10
FTP	0	1	0	0	0x08
SMTP	0	1	0	0	0x08
DNS (UDP)	1	0	0	0	0x10
DNS(TCP)	0	0	0	0	0x00
ICMP	0	0	0	0	0x00
BOOTP	0	0	0	0	0x00

Fuente: AHUATZIN SÁNCHEZ, Gerardo L.: ”Desarrollo de un esquema de dirección de traducciones IPv6-IPv4-IPv6”. Año 2016, p28.

[63] UPM, GRUPO DE SISTEMAS OPERATIVOS DATSI FI. 2012. Protocolo IPsec. [En línea] 8 de octubre de 2012. http://laurel.datsi.fi.upm.es/proyectos/teldatsi/teldatsi/protocolos_de_comunicaciones/protocolo_ipsec.

[64] Ibid.

[65] Ibid.

Indicador: Estos 3 bit especifican a que actividad pertenece según su posición. Si el bit de la primera posición esta activo significa que el paquete es parte de uno de mayor tamaño, si el bit de la segunda posición esta activo significa que el paquete no puede fragmentarse y por último el tercer bit deberá estar inactivo[66].

Desplazamientos de fragmentos: Si los paquetes fueron fragmentados, en este espacio se especifica el número de bytes en que se encuentran ubicados los paquetes originales para llegar a ser reensamblados en su destino nuevamente sin perder la estructura inicialmente transmitida en la comunicación desde el origen[67].

Tiempo de Vida TTL: Con el propósito de que un paquete no se quede indefinidamente circulando por la red, en este campo se define el tiempo de vida de un paquete que es transmitido (tiempo máximo 255), de tal forma que cada vez que pase por un Router el valor del tiempo de vida se decrementara en 1. Dado el caso de que el contador llegue a 0, este último Router enviara un mensaje ICMP al origen informando que debe reenviar el paquete debido a que este nunca llego a su destino[68].

Tipo de Protocolo: El tamaño del campo es de 8 bits. Este campo es utilizado para especificar el protocolo que es utilizado en la capa superior, es decir, en la de transporte, entre ellos podemos encontrar: TCP, UTP, ICMP, IP. Mediante la identificación de los números naturales se identifica que protocolo encapsula el datagrama, es decir, TCP equivale a un 6, UDP equivale a un 17, ICMP equivale a un 1, IP equivale a un 0[69].

Suma de Comprobación (Checksum Cabecera) : El tamaño del campo es de 16 bits. En este campo se verificar que la información que contiene el paquete llegue completo a su destino y se desecha aquella información que contenga mensaje erróneo por perdida de información en el trayecto a su destino. Es de precisar que el algoritmo de chequeo se centra en la evaluación de la cabecera[70].

---

[66] UPM, GRUPO DE SISTEMAS OPERATIVOS DATSI FI. 2012. Protocolo IPsec. [En línea] 8 de octubre de 2012. http://laurel.datsi.fi.upm.es/proyectos/teldatsi/teldatsi/protocolos_de_comunicaciones/protocolo_ipsec.

[67] UPM, GRUPO DE SISTEMAS OPERATIVOS DATSI FI. 2012. Protocolo IPsec. [En línea] 8 de octubre de 2012. http://laurel.datsi.fi.upm.es/proyectos/teldatsi/teldatsi/protocolos_de_comunicaciones/protocolo_ipsec.

[68] Ibid.

[69] Ibid.

[70] Ibid.

6.2 PROTOCOLO IPV6

El protocolo IPV6 fue creada para reemplazar a la versión IPv4, la cual fue diseñada por el Grupo de Trabajo de Ingeniería de Internet - IETF “Internet Engineering Task Force” y definida en el RFC 2460[71] -RFC 8200, con el fin de cumplir con las necesidades de direccionamiento y mejorar la seguridad mediante cifrado IPsec nativo.

6.2.1 CABECERAS DE IPV6

El encabezado IPv6 cuenta con una estructura más simple y gestión mejorada en comparación con IPv4. El encabezado de IPv6 es de hasta 40 bytes de longitud, es decir, el doble de tamaño del encabezado de IPv4. Para el encabezado IPv6 no cuenta con los campos como Padding (Relleno), Header checksum (Suma de verificación del encabezado), Fragment offset (Desplazamiento de fragmentos), Flags (Indicadir), Identification (Identificación), IHL (Longitud del Encanezado), aunque cuenta con unos campos adicionales como prioridad, Flow label (Longitud total), Paiload lenght (Tamaño de los datos), Next header (Próxima Cabecera) y Hop limit (Limites de saltos), sin embargo, IPv6, es más eficiente que IPv4[72]. La estructura IPv6 la podemos ver en las figuras 2.

Tal como lo definió en el documento RFC 2460[73] de diciembre de 1998, se especifica el protocolo utilizado en la versión 6 para la transmisión de datos a través del canal de internet, diseñado como el sucesor de IPv4, en la cual se puede visualizar su estructura en la figura 2, tales como: formato, cabecera, tamaño de paquetes, etiquetas de flujo, clases de tráfico y protocolos de capas superiores[74].

---

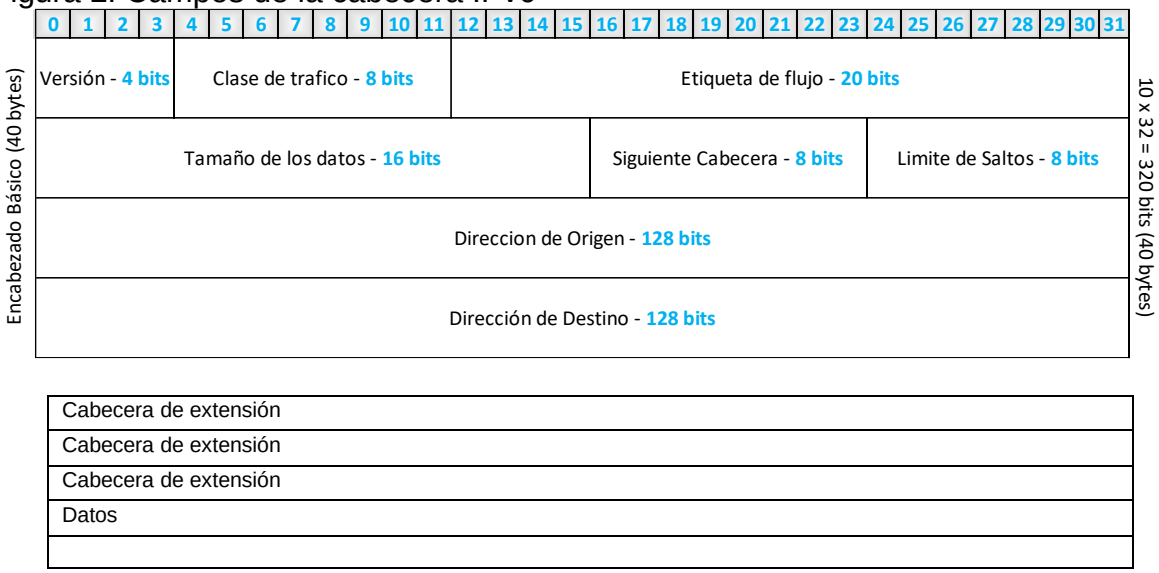
[71] NETWORK WORKING GROUP, Especificación Protocolo Internet, Versión 6 (IPv6). 1998, tomado de: https://www.rfc-es.org/rfc/rfc2460-es.txt.

[72] MEGS. 2019. Estructura de un paquete IPv6. [En línea] 2019. http://dmrodriguez.50megs.com/IPV6/IPV6_7.html.

[73] Network Working Group S. Deering, RFC 2460 - Internet Protocol, Version 6 (IPv6), diciembre 1998, tomado de: https://www.rfc-es.org/rfc/rfc2460-es.txt

[74] LACNIC. Curso IPv6 Básico, tomado de: . [En línea] https://www.youtube.com/watch?v=-HIUT2ilCyU&list=PLsQToyLJISPWSMPF2DSbFmw_2HtzNpCSj& index=7

Figura 2. Campos de la cabecera IPv6



Fuente: IPv6 Go; Cual es mi IPv6?, Disponible en http://www.ipv6go.net/cabecera_ipv6.php

La cabecera IPv6 básica cuenta con una longitud de 40 bytes[75], conformada así:

- **Versión (6 bits)**: Versión de IP (binario 0110 = decimal 6), este campo debe ser verificado por el router antes de procesar el datagrama con el propósito de identificar si corresponde a IP versión 4 o versión 6[76].

- **Clase de tráfico (8 bits)**: Clasifican los datos de acuerdo a la importancia del datagrama. Esté campo está definido en la norma RFC 791[77] y RFC 1349[78].
- 0-7 Especifica un identificador de tráfico de datos con control de congestión.

[75] MEGS, 50. 2019. Estructura de un paquete IPv6. 2019, tomado de: http://dmrodriguez.50megs.com/IPV6/IPV6_7.html.

[76] VELEZ VARELA, Fernando y GUTIERREZ RANCRUEL, Liliana. 2019. IPv6, una realidad. Bogotá - Colombia : Ediciones de la U, 2019, p. 9.

[77] INFORMATION SCIENCES INSTITUTE UNIVERSITY OF SOUTHERN CALIFORNIA. 1981. RFC: 791 - Especificacion del Protocolo. [En línea] septiembre de 1981. https://www.rfc-es.org/rfc/rfc0791-es.txt.

[78] NETWORK WORKING GROUP P. ALMQUIST. 1992. RFC 1349 - Type of Service in the Internet Protocol Suite. [En línea] julio de 1992. https://www.ietf.org/rfc/rfc1349.txt.

- 8-15 Especifica un identificador de tráfico de datos con control de congestión en video y audio[79].

- **Etiqueta de flujo (20 bits)**: Este es un campo que fue agregado en comparación con IPv4, su función es brindar información a cada uno de los router por donde pasan los datagramas suministrando tipo de flujo mínimo sin necesidad de analizarlos en detalle lo cual agiliza la comunicación, tal como sucede en una transmisión de videoconferencia en donde no puede haber retardo entre el audio y el video[80]. Así mismo este campo es utilizado por los proveedores de servicio de internet ISP para para determinar flujos específicos con sus clientes[81].

- **Longitud de paquetes (16 bits**): Este espacio está destinado para contener la información de la longitud total del mensaje. Aunque en este campo no se incluye el encabezado base si está incluido los encabezados extendidos y campos opcionales de la cabecera los cuales contienen una información necesaria[82].

- **Siguiente cabecera (8 bits)**: En este campo se almacena información sobre la próxima cabecera como TCP, UDP o cabecera de extensión, el cual es de gran importancia debido a que por cada enrutador en que pasa el mensaje, se podrá identificar si hay encabezados consecutivos que hagan parte del mensaje transmitido[83].

  En la tabla 4, se puede identificar los encabezados que puede contener el campo de encabezado siguiente y su valor decimal, entre los cuales puede ser: Opciones de salto, TCP, UDP, Encabezado de IPv6 encapsulado, Encabezado de enrutamiento, Encabezado de fragmentación, Protocolo de reserva de recursos (RSVP), Carga de seguridad encapsulada, Encabezado de autenticación, ICMPv6, Opciones de destino, entre otros.

---

[79] VELEZ VARELA, Fernando y GUTIERREZ RANCRUEL, Liliana. 2019. IPv6, una realidad. Bogotá - Colombia : Ediciones de la U, 2019, pág. 9

[80] VELEZ VARELA, Fernando y GUTIERREZ RANCRUEL, Liliana. 2019. IPv6, una realidad. Bogotá - Colombia : Ediciones de la U, 2019, p. 9.

[81] TELEMATIQUE. 2003. Revista electronica de Estudios Telematicos. IP Versión 6: La Nueva Generación IP. [En línea] 2003. https://dialnet.unirioja.es/descarga/articulo/2968291.pdf.

[82] VELEZ VARELA, Fernando y GUTIERREZ RANCRUEL, Liliana. 2019. IPv6, una realidad. Bogotá - Colombia : Ediciones de la U, 2019, pág. 9

[83] Ibid. p. 9.

Tabla 4. Siguiente Cabecera IPv6

Valor Decimal	Encabezado
0	Hop-by-hop Header (Opciones de salto a salto): En esta opción se especifica los parámetros de entrega en cada salto en la ruta de acceso a su destino.
6	TCP
17	UDP
41	Encabezado de IPv6 encapsulado
43	Routing Header (Encabezado de Enrutamiento): Se utiliza para especificar una ruta de origen, una lista de destinos intermedios, para que el paquete viaje por su ruta de acceso a su destino final
44	Fragmentation Header (Encabezado de Fragmentación)
46	Protocolo de reserva de recursos (RSVP)
50	Encapsulating Security Payload (Carga de seguridad encapsulada)
51	Authentication Header (Encabezado de Autenticación)
58	ICMPv6
59	No hay encabezado siguiente
60	Encabezado Destination Options (Opciones de destino)

Fuente: IANA.ORG, Internet Protocol Version 6 (IPv6) Parameters, Disponible en https://www.iana.org/assignments/ipv6-parameters/ipv6-parameters.xhtml

- **Limite de saltos (8 bits)**: Indica la máxima cantidad de saltos que le hacen falta al paquete para llegar a su destino. en caso de llegase a presentar un problema con el enrutador y para que este no se quede en un ciclo infinito. Cada vez que el mensaje pasa por Router el valor del "Limite de saltos" va disminuyento hasta llegar a cero para lo cual el ultimo router descarta el datagrama.

- **Dirección Origen (128 bits)**: En este campo se almacena la dirección IP desde donde partió el paquete, definido en RFC 2373[84].

[84] NETWORK WORKING GROUP R. HINDEN. 1998. RFC 2373 - Arquitectura de Direccionamiento en IPv6. [En línea] julio de 1998. https://www.ietf.org/rfc/rfc2373.txt.

- **Dirección Destino (128 bits)**: En este campo se almacena la dirección IP hasta donde debe llegar el paquete[85].

6.2.2 CABECERAS DE EXTENSIÓN

IPv6 le permite agregar opciones al datagrama IP, las cuales se ubican entre la cabecera IP y la cabecera TCP, agregando funcionalidad, confidencialidad e integridad al protocolo[86]. Dicha información puede ser vista en la tabla 5, en el cual se menciona cada una de las referencias que integran las cabeceras de extensión de IPv6[87].

Tabla 5. Referencias RFC para las Cabecera de Extensión IPv6

Valor Decimal	Referencia	Encabezado
0	RFC8200	Hop-by-hop Header - Opciones de salto a salto.
43	RFC8200 RFC5095	Routing Header -Encabezado de Enrutamiento.
44	RFC8200	Fragmentation Header - Encabezado de Fragmentación
50	RFC4303	Encapsulating Security Payload – Carga de seguridad encapsulada.
51	RFC4302	Authentication Header - Encabezado de Autenticación.
60	RFC8200	Encabezado Destination Options - Opciones de destino.
135	RFC6275	Mobility Header
139	RFC7401	Host Identity Protocol
140	RFC5533	Shim6 Protocol
253	RFC3692 RFC4727	Use for experimentation and testing

[85] Ibid.

[86] MEDINA CASTILLO, Carlos A. y FORERO RODRIGUEZ, Felipe. 2011. Caracterización de IPv6. [En línea] 14 de noviembre de 2011. https://dialnet.unirioja.es/descarga/articulo/4239524.pdf.

[87] VIVES, Alvaro. 2015. LACNIC. Curso IPv6 Básico Módulo 3: Direccionamiento y planes de numeración – El cabezal de IPv6. [En línea] 5 de junio de 2015. https://www.youtube.com/watch?v=qoJkahpB5do&list=PLJ3jHT8E6frAuYS73uN2QLWi8qyXRyxo1&index=14

254	RFC3692 RFC4727	Use for experimentation and testing

Fuente: : IANA.ORG, Internet Protocol Version 6 (IPv6) Parameters, Disponible en https://www.iana.org/assignments/ipv6-parameters/ipv6-parameters.xhtml

---

- **Opción Hop-by-Hop**: (salto por salto) la información que contiene esta cabecera debe ser analizada en cada salto a fin de llevar información a los equipos de comunicaciones por los que atraviesa la información.
- **Enrutado**: En la cabecera va una lista con los nodos por los cuales el paquete debe pasar.
- **Fragmento**: Esta cabecera es procesada por el host final dividiendo los paquetes demasiado grandes que no pueden ser transmitidos en algunas redes.
- **Opciones de destino**: lleva información a procesar por el host final.
- **Autenticación (AH)**: Proporciona integridad y autenticación.
- **Carga útil de seguridad encriptada (Encrypted Security Payload o ESP)**: proporciona confidencialidad, además de integridad y autenticación de datos. La información transmitida de manera cifrada a través de la red de comunicaciones.

6.2.3 ESTRUCTURA DE DIRECCIONES IPv6

La estructura de direcciones IP, presenta un formato hexadecimal de 128 bits, utilizando 8 hextetos, teniendo en cuenta que cada digito hexadecimal cuatro bits, se tiene 16 bit por cada octeto separado por dos puntos ":", distribución que se encuentra representada en la tabla 6.

Tabla 6. Estructura de una dirección IPv6

Descripcion	Octeto 1		Octeto 2		Octeto 3		Octeto 4		Octeto 5		Octeto 6		Octeto 7		Octeto 8
Hextetos	2001	:	ODB8	:	0001	:	2350	:	0135	:	00CD	:	CAFC	:	0E1F
1 digito decimal = 4 bits	4+4+4+4		4+4+4+4		4+4+4+4		4+4+4+4		4+4+4+4		4+4+4+4		4+4+4+4		4+4+4+4
bit x hexteto	16 bits		16 bits		16 bits		16 bits		16 bits		16 bits		16 bits		16 bits
bit x dirección IPv6	128														

Fuente: "elaboración propia"

En la tabla 7, se relacionan los códigos hexadecimales que podría tomar cada uno de los hextetos , los cuales van de 0 a 15 en decimal, o lo que es lo mismo, de 0 a F en hexadecimal, en donde por cada 4 dígitos hexadecimales conforman uno de los ocho hextetos que hacen parte de la dirección IPv6.

Tabla 7. Hexadecimales utilizados por en el direccionamiento IP

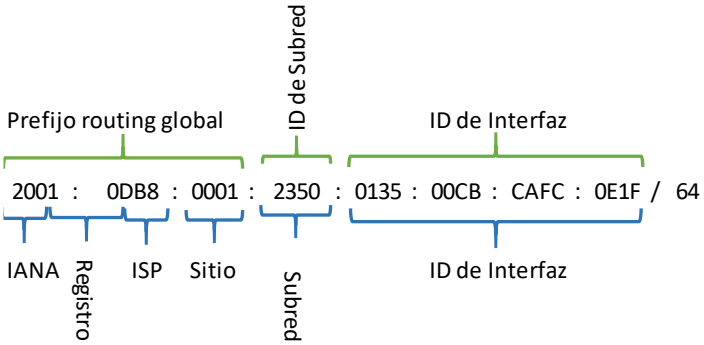
Decimal	Hexadecimal	Binario
0	0	0000
1	1	0001
2	2	0010
3	3	0011
4	4	0100
5	5	0101
6	6	0110
7	7	0111
8	8	1000
9	9	1001
10	A	1010
11	B	1011
12	C	1100
13	D	1101
14	E	1110
15	F	1111

Fuente: “elaboración propia”

Dentro de la estructura IPv6, se tienen 48 bits destinados para la identificación del Prefijo Routing Global, 16 bits para la identificación de la subred (Contiene: código IANA, Registro LACNIC, ISP e Identificación del Cliente) y 64 bits que hacen parte de la ID interfaz[88], dicha estructura puede ser visualizada en la figura 3.

[88] VIVES, Alvaro. 2015. LACNIC. Curso IPv6 Básico Módulo 3: Direccionamiento y planes de numeración – Proveedores. [En línea] 5 de junio de 2015. https://www.youtube.com/watch?v=IJ7sbiJqxnM&list=PLJ3jHT8E6frAuYS73uN2QLWi8qyXRyxo1&index=17.

Figura 3. Estructura de asignación de direcciones IP



Fuente: “elaboración propia”

- **Prefijo de routing global**: Corresponde a los primeros tres hextetos (16x3=48 bits), asignado por el proveedor de internet, quien a su vez fue asignado por el proveedor de servicios RIR “Registro Regional de Internet”, establecido en el RFC 4291[89] provista por IANA, como ejemplo de prefijo global se tiene 2001:0D88:0001.

- Los primeros 3 bits se fijan desde 001 a 200::/12 (número de routing global de IANA).
- Los bit del 16 al 24 el Registro Regional: Afric, Apnic, Lacnic, Ripe Ncc y Arin.
- “2001:0000::/23IANA
- 2001:0200::/23 APNIC
- 2001:0400::/23 ARIN
- 2001:0600::/23 RIPE” (Iana.org, 2019 pág. 1)
- Los 8 bit hasta /32 identifican el ISP
- El tercer hexteto representa el identificador del sitio / cliente

- **ID de subred**: Corresponde al cuarto hexteto (16 bits) de la dirección IPv6.

- Permite 65536 subredes, con 18 trillones para cada subred
- No forma parte del campo de direcciones del host

- **ID de interfaz**: Corresponde a los cuatro últimos hextetos (64 bits) de la dirección IPv6.

[89] NETWORK WORKING GROUP R. HINDEN. 2006. RFC4291 - IP Version 6 Addressing Architecture. [En línea] febrero de 2006. https://www.ietf.org/rfc/rfc4291.txt.

- Se asigna de manera manual o dinámica mediante el comando EUI-64 (identificador único extendido)
- El comando EUI-64 utiliza la dirección MAC de 48 bits del dispositivo y la convierte en 64 bits mediante la edición de FF:FE en la mitad de la dirección.
- Es posible asignar la primera red y última dirección a una interfaz. Una interfaz puede contener más de una dirección IPv6.
- No existen direcciones de difusión, sino que se utilizan direcciones multicast.

Visto desde otra agrupación dentro de la estructura de IPv6 se tiene:

- **IANA**: Número de Routing global de IANA (Desde 001 a 200)
- **Registro:** Identificación registro regional (Para nuestra región =LACNIC)
- **ISP:** Identificación del ISP (Proveedor de Servicio de Internet)
- **Sitio**: Identificador del cliente
- **Subred:** Topología de la subred
- **ID de interfaz:** Configuración manual o dinámica mediante EUI-64 (Identificador único extendido)

6.2.4 REGLAS PARA LA ESCRITURA DE DIRECCIONES IPv6

Según la norma RFC 5952[90], el direccionamiento IPv6, cuenta con ciertas reglas las cuales permiten su escritura de manera correcta y eficiente. Como ejemplo se tomara la dirección IPv6 2001:1BB5:81A6:35D4:1425:8C2F:5774:2334, el cual puede ser representado de varias maneras sin que este afecte el valor real:

a. 8 hextetos de cuatro dígitos cada uno
   2001:1BB5:81A6:35D4:1425:8C2F:5774:2334

[90] INTERNET ENGINEERING TASK FORCE (IETF) S. KAWAMURA. 2010. RFC5952 - A Recommendation for IPv6 Address Text Representation. [En línea] agosto de 2010. https://www.ietf.org/rfc/rfc5952.txt

b. Suprimir valores nulos en los cuartetos, tener presente de no eliminar los dos puntos ":"

   2001:4BB5:81A6:0000:1425:25F6:33DA:2334
   2001:4BB5:81A6::1425:25F6:33DA:2334

c. Si existe más de dos grupos nulos seguidos, solamente se podrá suprimir uno de ellos, mediante dos puntos dobles "::"

   2001:4BB5:81A6:0000:0000:0000:33DA:2334
   2001:4BB5:81A6:0::0:33DA:2334
   o
   2001:4BB5:81A6:0:0:0:33DA:2334

d. Dentro de cada uno de los 8 grupo (hextetos) se pueden suprimir los ceros iniciales.
   2001:0BB5:81A6:35D4:1425:0C2F:5774:2334
   2001:BB5:81A6:35D4:1425:C2F:5774:2334

6.2.5 PROTOCOLO ICMPV6

El Protocolo ICPMv6 – "Internet Control Message Protocol - Protocolo de Mensajes de Control de Internet", ha sido diseñado para ser utilizado en IPv6 y cuenta con muchas más funciones a las establecidas en su predecesor ICMP de IPv4, por lo tanto, son incompatibles entre sí. Con el propósito de prevenir ataques ICMP de negación de servicio DoS este protocolo puede ser autenticado y encriptado usando la cabecera correspondiente[91].

En la tabla 8 se identifican los códigos básicos de los mensajes utilizados por ICMPv6 tanto de error (van desde 0 a 127) como informativos (van de 128 a 255). Este protocolo esta descrito en RFC 2463[92] y su función es detectar y reportar errores durante el proceso de transmisión de paquetes, realizar diagnóstico (mediante el comando ping) realizar

[91] VEATO, Valentin. 2015. ICMP en IPv6. Redes Locales y Globales. [En línea] 2015. https://sites.google.com/site/redeslocalesyglobales/6-arquitecturas-de-redes/6-arquitectura-tcp-ip/7-nivel-de-red/8-direccionamiento-ipv6/7-icmp-en-ipv6.

[92] NETWORK WORKING GROUP A. CONTA, RFC2463 Protocolo de Mensajes de Control de Internet para IPv6 (ICMPv6), diciembre 1998, tomado de: https://www.ietf.org/rfc/rfc2463.txt

funciones como Neigbor Discovery (equivalente a ARP en IPv4), detección de direcciones multicast de IPv6)[93].

Tabla 8. Mensajes básicos de error en ICMPv6

Mensajes de error ICMPv6		
Tipo	**Descripción y códigos**	
1	Destino no alcanzable (Destination Unreachable)	
	Código	**Descripción**
	0	Sin ruta hacia el destino
	1	Comunicación prohibida administrativamente
	2	Sin asignar
	3	Dirección no alcanzable
	4	Puerto no alcanzable
2	Paquete demasiado grande (Packet Too Big)	
3	Tiempo excedido (Time Exceeded)	
	Código	**Descripción**
	0	Límite de saltos excedido
	1	Tiempo de desfragmentación excedido
4	Problema de parámetros (Parameter Problem)	
	0	Campo errónea en cabecera
	1	Tipo de Cabecera Siguiente desconocida
	2	Opción IPv6 desconocida
Mensajes informativos ICMPv6		
128	Solicitud de eco (Echo Request)	
129	Respuesta de eco (Echo Reply)	

Fuente: VEATO, Valentin. ICMP en IPv6. 2015. disponible en https://sites.google.com/site/redeslocalesyglobales/6-arquitecturas-de-redes/6-arquitectura-tcp-ip/7-nivel-de-red/8-direccionamiento-ipv6/7-icmp-en-ipv6

6.2.6 TIPOS DE PROTOCOLOS DE ENRUTAMIENTO EN IPv6

Un equipo de comunicaciones router maneja múltiples protocolos de ruteo, a continuación, se describirán los protocolos que pueden ser configuradas en un router, tanto internas como externas. Como punto a tener en cuenta Un dispositivo Router solamente puede manejar una sola tabla de ruteo.

[93] FRANCISCONI, Hugo Adrian. IPsec en Ambientes IPv4 e IPv6. [En línea] http://redes-linux.com/manuales/seguridad/IPsec_IPv4_IPv6.pdf, p.30.

El protocolo de enrutamiento en IPv6 determina rutas estáticas como dinámicas tal como lo viene haciendo IPv4, el cambio primordial esta dado en la determinación del nivel de direccionamiento, programación y la utilización de comandos dentro de los sistemas operativos.

6.2.6.1 PROTOCOLOS DE RUTEO INTERNOS (IGP)

Dentro de los protocolos de ruteo internos se tienen varios tipos de protocolos como IS-IS, RIPng, EIGRP, OSPF. Dentro de estos protocolos se compiten para determinar cuál es la ruta más favorable según un término denominado “distancia administrativa” y es ésta la que quedará establecida en la tabla de ruteo[94].

RIPng: Usa multicast con direcciones FF02::9, sin embargo, solamente fue utilizado al comienzo cuando se realizaban los primeros despliegues de IPv6, este fue rápidamente reemplazado por protocolos de router OSPF, BGP. El protocolo utilizado por los routers para compartir información de las redes IP que se encuentran conectadas[95].

OSPFv3: Es utilizada para intercambiar prefijos IPv6. Se asigna manualmente al Router-ID, Link-state ID y Área ID. Asigna prefijos IPv6 y se ejecuta directamente en este. OSPFv3 se ejecuta sobre un enlace link y se puede conectar a un enlace y múltiples interfaces pueden conectarse a un enlace.

IS-ISv6: Se define como un protocolo de intercambio de routing entre dominios para tráficos de servicios de redes y requieren de un protocolo de red no orientado a conexión (CLNP). Un CLNP usa direcciones NSAP (Network Service Access Point) se utiliza para identificar las etiquetas que usan los extremos o puntos terminales de una red .El protocolo IS-IS se encuentra descrito en el RFC 1195[96].

---

[94] VELEZ VARELA, Fernando y RANCRUEL GUTIERREZ, Liliana 2019. IPv6, una realidad. Bogotá - Colombia : Ediciones de la U, 2019, p 128.

[95] DORDOIGNE, Jose. 2015. Redes Informaticas - Nociones Fundamentales. Barcelona - España : Ediciones ENI, 2015. Primera.

[96] NETWORK WORKING WORKING GROUP. 1900. RFC 1195 - Use of OSI IS-IS for Routing in TCP/IP and Dual Environments. [En línea] diciembre de 1900. https://www.ietf.org/rfc/rfc1195.txt.

6.2.6.2 PROTOCOLOS DE RUTEO EXTERNOS (EGP)

Dentro de este protocolo de ruteo solamente se cuenta con el protocolo BGP, el cual intercambia información y garantiza que la ruta o camino por el cual viajan los paquetes para llegar a un destino estén libres de loops. BGP4+ transporta información de routing para IPv6 e IPv4[97] las cuales se encuentran definidos en RFC 2545[98].

6.2.7 CONFIGURACION DEL PROTOCOLO IPV6 SOBRE LINUX

El protocolo de seguridad IPsec, permite cifrar y/o proteger el tráfico de los protocolos TCP/IP de una organización, evitando que la información sea rastreada[99]. Para instalar Ipsec sobre un Sistema de Operativo de Kali Linux, se debe descargar desde el siguiente link establecido en la página oficial: *http://http.kali.org/pool/main/i/ipsec-tools/*[100].

En la figura 4, se observa los repositorios que pueden ser descargados desde la página oficial de Kali Linux, en el cual se deberá seleccionar y descargar el archivo que cumpla con los requerimientos del equipo al cual se realizará la instalación, como ejemplo y teniendo en cuenta que se instalará en un equipo a 64 bits, se procederá a descargar el archivo ***ipsec-tools_0.8.2+20140711-12_amd64.deb***.

---

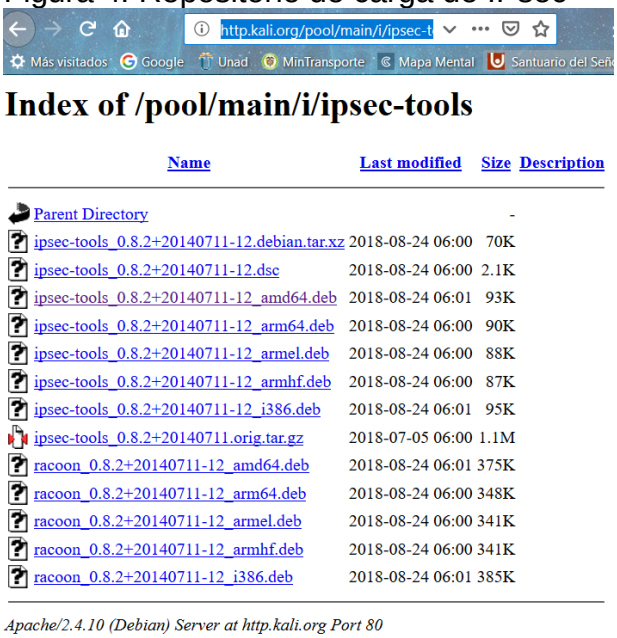
[97] VELEZ VARELA, Fernando y GUTIERREZ RANCRUEL, Liliana. 2019. IPv6, una realidad. Bogotá - Colombia : Ediciones de la U, 2019, pág. 205.

[98] NETWORK WORKING GROUP P. MARQUES. 1999. RFC2545 Uso de las Extensiones Multiprotocolo de BGP-4 para Routing entre dominios para IPv6. [En línea] marzo de 1999. https://www.ietf.org/rfc/rfc2545.txt.

[99] RED HAT INC. 2003. Establecimiento de una conexión IPsec. [En línea] 2003. http://web.mit.edu/rhel-doc/3/rhel-sag-es-3/s1-network-config-ipsec.html.

[100] AVILA DIAZ, Luis Miguel, Configurar IPsec, 2013, tomado de: https://www.youtube.com/watch?v=PuQRlRhv-BU

Figura 4. Repositorio de carga de IPsec



Fuente: “elaboración propia”

Una vez descargado el archivo .deb, se debe ejecutar la aplicación mediante el comando: ***sudo dpkg -i ipsec-tools_0.8.2+20140711-12_amd64.deb***. Una vez realizada la instalación, se debe realizar la configuración del archivo ***ipsec-tools.conf***, para lo cual se debe configurar el protocolo AH y ESP.

Para la configuración de los protocolos AH y ESP, el cual está dirigida a la configuración de topologías pequeñas con clave manual, lo cual permite comunicación entre equipos de manera encriptada, para el ejemplo, se tomó como conexiones las IP 192.168.1.64 y 192.168.166 equivalente a direcciones de entrada y salida.

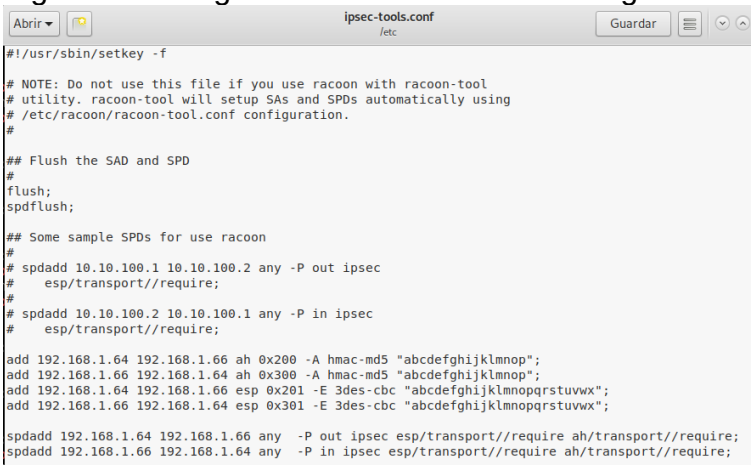
El protocolo AH se encarga de verificar las cabeceras, por lo tanto, se debe colocar las IP tanto de la maquina local como de la maquina destino[101]. El protocolo ESP, se encarga de cifrar el mensaje, por lo cual se debe colocar las IP tanto de la maquina local como de la maquina destino, adicionalmente se debe especificar entradas y salidas para crear comunicación representada en la figura 5, para cumplir con este objetivo se debe digitar las siguientes líneas de comando: sudo gedit /etc/ipsec-tools.conf,

- add 192.168.1.64 192.168.1.66 ah 0x200 -A hmac-md5 "abcdefghijklmnop";

[101] SANCHEZ, Julio. 2011. Ejemplo de Uso de SSH Secure Shell, 10 de enero de 2011, tomado de: https://www.youtube.com/watch?v=qI9DZmRKgHQ.

- add 192.168.1.66 192.168.1.64 ah 0x300 -A hmac-md5 "abcdefghijklmnop";
- add 192.168.1.64 192.168.1.66 esp 0x201 -E 3des-cbc "abcdefghijklmnopqrstuvwx";
- add 192.168.1.66 192.168.1.64 esp 0x301 -E 3des-cbc "abcdefghijklmnopqrstuvwx";
- spdadd 192.168.1.64 192.168.1.66 any -P out ipsec esp/transport//require ah/transport//require;
- spdadd 192.168.1.66 192.168.1.64 any -P in ipsec esp/transport//require ah/transport//require;

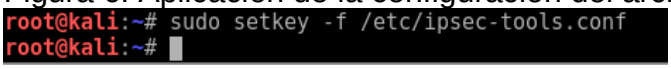
Figura 5. Configuración del archivo de configuración IPsec



Fuente: “elaboración propia”

Una vez se tengan las configuraciones y con el propósito de que dichas reglas se establezcan y queden activas, es decir, que cada IP genere su propia clave a partir de la clave manual suministrada *"abcdefghijklmnop"*, para esta actividad se requiere ejecutar el comando: *sudo setkey -f /etc/ipsec-tools.conf,* representada en la figura 6.

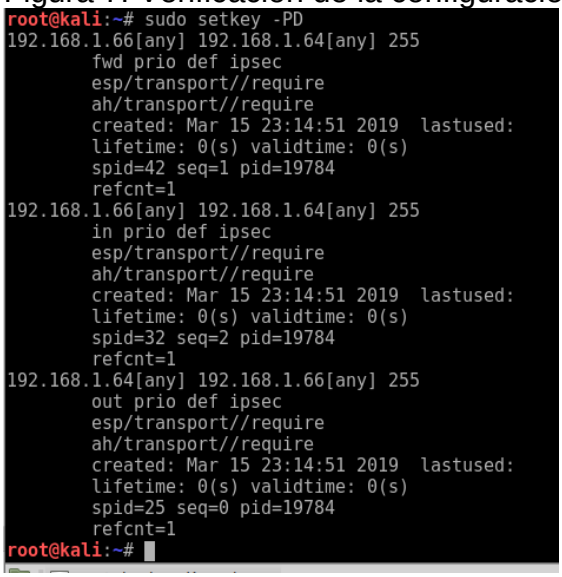
Figura 6. Aplicación de la configuración del archivo IPsec



Fuente: “elaboración propia”

Así mismo, en la figura 7, mediante el comando *sudo setkey -PD* se visualiza las configuraciones previas realizadas en donde las reglas fueron efectivamente aplicadas, en este punto se puede establecer una comunicación entre los host perfectamente cifrada y con las medidas de seguridad que brinda IPsec activas.

Figura 7. Verificación de la configuración del IPsec



Fuente: “elaboración propia”

7 IDENTIFICAR VENTAJAS DE SEGURIDAD DEL PROTOCOLO IPV6 SOBRE LA INFRAESTRUCTURA DE LA RED EN LA ORGANIZACION

Como en todo, siempre se cuenta con ventajas y desventajas, a lo largo de la monografía se ha detallado la arquitectura y funcionalidades, en el presente apartado se tratará las ventajas con que se cuenta al realizarse la instalación y puesta en funcionamiento en cualquier organización el protocolo de comunicaciones Ipv6.

7.1 INTEGRIDAD Y AUTENTICIDAD DE LOS DATOS TRANSMITIDOS

La funcionalidad de integridad y autenticidad la dan tanto el protocolo AH como el protocolo ESP, dado que garantiza que los paquetes transportados no han sido alterados o modificados. La autenticación del protocolo IPsec brinda seguridad e integridad en un gran número de campos del encabezado IPv6, pero no en aquellos que cambian durante la trayectoria de la comunicación.

7.2 CONFIDENCIALIDAD

Mediante el protocolo ESP se obtiene la función de cifrado, lo cual garantiza la integridad y confidencialidad de los datos. Es así que mediante el cifrado de datos el protocolo ESP oculta los datos que están siendo transmitidos. Sobre el protocolo ESP se provee confidencialidad en la comunicación, integridad de los paquetes y protección contra ataques de repetición.

7.3 DETECCIÓN DE REPETICIONES

La autenticación protege frente la suplantación de identidad IP, impidiendo el reenvió de paquetes a un destinatario previa captura de dichos paquetes por parte de un atacante. Con el propósito de prevenir este tipo de incidentes de seguridad los protocolos AH y ESP cuentan con métodos de detección de Repeticiones (RDM) utilizando el campo “Replay Detección”, en donde se incrementa el numero consecutivo de envió que se encuentra en los encabezados AH y ESP de tal forma que se descarta los paquetes iguales.

7.4 CONTROL DE ACCESO: AUTENTICACIÓN Y AUTORIZACIÓN.

Mediante la utilización de los protocolos ESP y AH, se crean claves que son enviadas de manera segura mediante una sesión IKE en la que tanto el emisor como el receptor se autentican mutuamente, evitando que equipos que no pertenezcan a la comunicación intervengan en ella. Aunque se realice una autenticación valida no existe una viabilidad de acceso total dado que Ipsec proporciona funciones de autorización[102].

[102] RICO BAUTISTA, Dewar Willmer y MEDINA CÁRDENAS, Yurley Constanza y SANTOS JAIMES, Luz Mari. 2008. IPSec DE IPv6 EN LA UNIVERSIDAD DE PAMPLONA. Universidad Tecnológica de PereiraColombia. [En línea] 2008. https://www.redalyc.org/pdf/849/84920503057.pdf. p. 323-324.

8 CONOCER LAS MEDIDAS DE SEGURIDAD QUE IMPLEMENTA EL NUEVO PROTOCOLO IPV6

IPv6 ofrece medidas de seguridad superiores a la establecida por IPv4 gracias a que se integran nuevas herramientas y técnicas, por lo cual es importante que los administradores de la infraestructura se capaciten en el tema, dado que existe la posibilidad de que los activos de información (equipos tecnológicos y software) no sean configurados de manera adecuada y correcta, lo cual genera huecos de seguridad, aprovechada por la ciberdelincuencia para establecer sus puntos de ataque[103].

La gran mayoría de Sistemas Operativos vienen con IPv6 por defecto, pero dado que la infraestructura tanto de los usuarios finales como organizaciones aún no están configuradas para el manejo de tráfico sobre este protocolo, el sistema debe reconfigurarse sobre el manejo del protocolo IPv4. Es importante tener claridad que la seguridad de IPv4 como IPv6 está dada principalmente por la configuración correcta y adecuada que se realice sobre la plataforma por parte de cada uno de los administradores de la red e infraestructura.

8.1 SEGURIDAD DE IPSEC EN IPV6

IPsec es un estándar IETF que brinda el servicio de seguridad a la capa de IP (capa 3 Red) y a todos los protocolos que se encuentran en un mayor nivel como TCP, UDP, ICMP, DCCP,FCP (Capa 4 Transporte), mediante procesos de autenticación, encriptación e integridad de los datos utilizando algoritmos de seguridad para su funcionamiento, permitiendo conexiones seguras a través de canales no seguros, sin modificar las aplicaciones de capa superior para su uso. IPsec proporciona un alto nivel de seguridad mediante cifrado, proporcionando control de acceso, integridad sin conexión, autenticación y confidencialidad de extremo a extremo[104].

Los paquetes IP están compuestos por dos elementos: Los datos y la cabecera a la que pertenecen los datos, uno de los inconvenientes existentes con los paquetes de datos es la falta de confidencialidad, autenticidad e integridad, debido a que dichos datos al pasar

[103] Ibid. p 324

[104] DIGITAL GUIDE. 2016. Conexiones de red seguras con IPsec. [En línea] 3 de agosto de 2016. https://www.ionos.es/digitalguide/servidores/know-how/ipsec-arquitectura-de-seguridad-para-ipv4-e-ipv6/.

por los diferentes routers en su viaje al destino final pueden llegar a ser interceptados y manipulados dado que no cuentan con mecanismos propios de cifrado y de autenticación.

Por lo anterior se creó el protocolo de seguridad para internet denominado IPsec “Internet Protocol Security”, el cual cuenta con una gran variedad de funciones que permiten la navegación de paquetes de datos por las diferentes redes de manera segura y confiable, utilizando protocolos de seguridad AH, ESP y protocolo de gestión de claves IKE para comunicaciones IP.

Dentro de las características de IPsec, se tiene:

- Estándar IETF “Internet Engineering Task Force” – RFC 4301[105]
- Integridad a nivel de red
- Seguridad de extremo a extremo en el cual la información transmitida es encriptada.
- Brinda servicios de seguridad a la capa IP
- Permite acceso a un usuario remoto a recursos privados de la red
- Control de acceso sobre personal no autorizado
- IPsec está orientado a la conexión
- Integridad sin conexión: Puede detectar modificación en un mensaje.
- Autenticación de los datos desde el origen.
- Protección antireplay: Descubre y elimina los mensajes duplicados
- Confidencialidad: mediante la encriptación de datos
- Mediante el proceso de encriptación de datos realizada por el modo túnel sobre las cabeceras IP internas, identificación del origen del tráfico y su último destino, se realiza el proceso de confidencialidad de tráfico.

IPsec incluye funcionalidades para el manejo de tráfico por el firewall, sin embargo, es importante tener en cuenta que restricciones adicionales sobre el firewall y/o prácticas de seguridad pueden afectar el flujo de datos impuesto por IPsec, adicionalmente malas prácticas de seguridad sobre los sistemas operativos pueden degradar la seguridad con que cuenta el protocolo IPsec.

8.2 AMENAZAS A LA SEGURIDAD DE IPV6

Como en todo sistema por más novedoso y seguro que sea, siempre existe riesgos y amenaza que tienen que enfrentar, por tal motivo y con el propósito de conocer los

[105] NETWORK WORKING GROUP S. KENT. 2005. RFC 4301 – Security Architecture for the Internet Protocol. [En línea] diciembre de 2005. https://www.ietf.org/rfc/rfc4301.txt.

posibles riesgos a que se enfrenta el protocolo IPv6, se realizó una clasificación en la que se engloban cada una de ellas: Las que viene desde la versión de IPv4 y se mantienen con la versión de IPv6, Las que se tenían en la versión de IPv4 y que vario con la versión de IPv6, as nuevas amenazas presentes con IPv6.

Las que viene desde la versión de IPv4 y se mantienen con la versión de IPv6, dentro de estas tenemos: Sniffing (captura de paquetes mediante un snifing como WareShere), ataques a otras capas (a nivel TCP, UDP, ataques a nivel de aplicación Web como SQL inyección, XXS), fooding (inundación de paquetes como ICMP). Las que se tenían en la versión de IPv4 y que vario con la versión de IPv6, dentro de esta clasificación se tiene, como el escaneo de red (Nmap) y el smurf (amplificación). Las nuevas amenazas presentes con IPv6, como por ejemplo, amenazas a NDP, Routing Header tipo 0, Cabeceras de extensión.

8.3 AMENAZA NDP - (NEIGHBOR DISCOVERY PROTOCOL)

Teniendo en cuenta que Neighbor Discovery Protocol (NDP - Protocolo de Descubrimiento de Protocolos) sobre IPv6 se utiliza tanto en los host como en el router, cumple la misma función que ARP - Protocolo de Resolución de Dirección que “Address Resolution Protocol” en IPv4, en donde su función principal dentro de la capa de enlace es identificar los terminales vecinos y los nuevos host que se incorporan a la red, adicional mantiene limpio el cache de cada uno de los nodos dentro del enlace.

Este Protocolo de IPv6 presenta amenazas, las cuales se encuentran documentadas en RFC 4861[106], RFC 3756[107], RF C6583[108], RFC 3971[109], las cuales tiene como propósito proteger el Neighbor Discovery (Descubrimiento del Vecino). Dentro de estas amenazas tenemos Neighbor Advertisement no solicitado, el cual será descrito a continuación.

Neighbor Advertisement no solicitado

---

[106] NETWORK WORKING GROUP T. NARTEN. 2007. RFC4861 - Neighbor Discovery for IP version 6 (IPv6). [En línea] septiembre de 2007. https://www.ietf.org/rfc/rfc4861.txt.

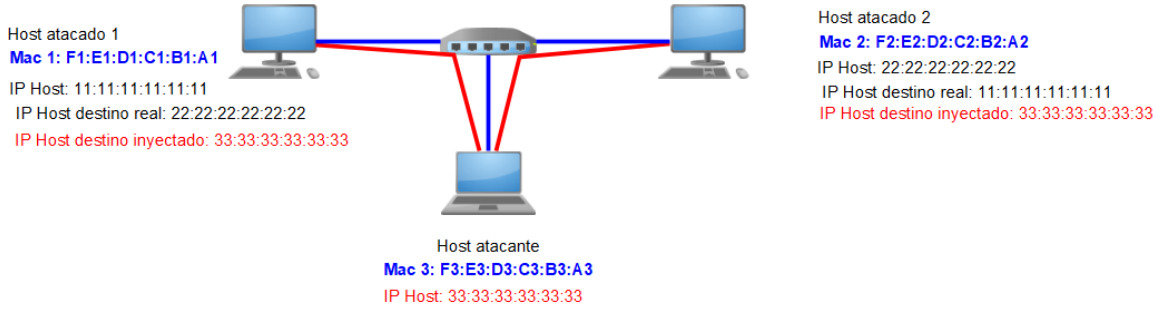
[107] NETWORK WORKING GROUP P. NIKANDER, ED. 2004. RFC3756 - IPv6 Neighbor Discovery (ND) Trust Models and Threats. [En línea] mayo de 2004. https://www.ietf.org/rfc/rfc3756.txt.

[108] INTERNET ENGINEERING TASK FORCE (IETF) I. GASHINSKY. 2012. RFC6583 - Operational Neighbor Discovery Problems. [En línea] marzo de 2012. https://www.ietf.org/rfc/rfc6583.txt.

[109] NETWORK WORKING GROUP J. ARKKO, ED. 2005. RFC3971 - SEcure Neighbor Discovery (SEND). [En línea] marzo de 2005. https://www.ietf.org/rfc/rfc3971.txt.

Esta amenaza acurre cuando un host (atacante) se encuentra conectado a otros dos host (atacados) mediante un switch, de tal forma que al realizar transferencia de datos entre estos dos host (atacados) su comunicación es interceptada por un tercer host (atacante), previa inyección de información falsa a los dos host atacados, de tal forma que se captura información transmitida entre host, representada en la figura 8.

Figura 8. Ataque ND



Fuente: "elaboración propia"

8.4 RFC QUE APLICAN SEGURIDAD EN IPV6

En la tabla 9 se registran los documentos elaborador por ingenieros o expertos en el tema de las comunicaciones pertenecientes al Grupo de Trabajo de Ingeniería de Internet IETF[110] "Internet Engineering Task Force", dichos documentos son denominados RFC y se encuentra destinados para dar soporte al IPv6.

Tabla 9. RFC que aplican todos los temas de IPv6 incluida la seguridad

TEMA	DOCUMENTO	DESCRIPCIÓN
Especificaciones Básicas	RFC2460	Especificaciones del Protocolo Internet Versión 6 (IPv6)
	RFC2461	Descubrimiento del Vecindario para IPv6 (ND)
	RFC2462	Autoconfiguración de Direcciones "stateless" IPv6
	RFC2463	Protocolo de Mensajes de Control de Internet para IPv6 (ICMPv6)

[110] MINTIC. 2019. Protocolos de Internet Version 6. [En línea] 14 de febrero de 2019. https://www.mintic.gov.co/portal/604/w3-article-5938.html.

	RFC1981	Descubrimiento del MTU de la ruta para IPv6
	RFC1809	Uso del campo "Etiqueta de Flujo" en IPv6
Direccionamiento	RFC2373	Arquitectura de Direccionamiento en IPv6
	RFC1887	Arquitectura para la Asignación de Direcciones Unicast IPv6
	RFC2374	Formato de Direcciones Unicast Agregables Globales
	RFC2450	Propuesta de normas de asignación de TLA y NLA
Routing	RFC2080	RIP para IPv6
	RFC2081	Aplicabilidad de RIPng para IPv6
	RFC2283	Extensiones Multiprotocolo para BGP-4
	RFC2545	Uso de las Extensiones Multiprotocolo de BGP-4 para Routing entre dominios para IPv6
	RFC2740	OSPF para IPv6
DNS	RFC1886	Extensiones DNS para soportar IPv6
IPv6 sobre transmisión	RFC2464	Transmisión de paquetes IPv6 sobre redes Ethernet
	RFC2467	Transmisión de paquetes IPv6 sobre redes FDDI
	RFC2470	Transmisión de paquetes IPv6 sobre redes Token Ring
	RFC2472	IPv6 sobre PPP
	RFC2491	IPv6 sobre redes de Acceso Múltiple Sin Broadcast
	RFC2492	IPv6 sobre redes ATM
Seguridad	RFC2401	Arquitectura de Seguridad para IP Protocol (Actalizado por RFC 3168), Soporte para IPsec-V2.
	RFC2402	Cabecera de Autenticación IP
	RFC2406	Encriptación de datos en IP (ESP)
	RFC2408	Asociaciones de Seguridad y Protocolo de Gestión de Claves en Internet (ISAKMP)
	RFC 5619	Software Security Considerations, Agosto 2009
	RFC 5269	FMIP Seurity Distributing a Symectric Fast Mobile IPv6 (FMIPv6)
	RFC 4942	IPv6 Transition/Coexistence Security Considerations
	RFC 4218	Threats Relatiing To IPv6 Multihoming Solutions

	RFC 4891	Using IPsec To Secure IPv6 Tunnels
	RFC 4890	Recommendations For Filtering ICMPv6 Messages in Firewalls
	RFC 4864	Local Network Protection For IPv6
	RFC 4843	An IPv6 Prefix For Overlay Routable Cryptographic hash Identifiers (ORCHID)
	RFC 5213	Proxy Mobile IPv6
	RFC 4835	Cryptographic Algorithm Implementation Requeriments for Encapsulatiing Security Payload (ESP) and Authentication Header (AH)
	RFC 4487	Mobile IPv6 And Firewalls: Problem Statement
	RFC 4449	Securing Mobile IPv6 Route Optimization Using a Static Shared Key
	RFC 4303	IP Encapsulating Security Payload (ESP)
	RFC 3756	IPv6 Neighbor Discovery (ND) Trust Models Threats
	RFC 4301	Asociaciones de seguridad (SA). Security Architecture for the Internet Protocol. Soporte para IPsec-V2. (Hace obsoleto el RFC 2401)
	RFC 4302	IP Authentication Header (Hace obsoleto RFC2402)
	RFC 4303	IP Encapsulation Security Payload
	RFC 5282	Using Authenticated Encription Algorithms with the encrypted payload of the internet key Exchange Versión 2 (IKEv2) Protocol.
	RFC 5996	Internet Key Exchange (IKEv2) Protocol
	RFC 4877	Mobile IPv6 Operation with IKEv2 and the revised IPSec Architecture
	RFC 4581	Cryptographically Generated Addresses (CGA) extention field format (Actualiza el RFC 3972)
	RFC 4982	Support For Multiple Hash Algorithms in Cryptographically Generated Addresses (CGA). (Actualiza el RFC 3972 errata)
	RFC 3414	User –Based Security Model (USM) for Version 3 of the Simple Network Management Protocol (SNMPv3)
	RFC 4807	IPSec Security Policy Database Configuration –MIB.✓RFC 2406: IP Encapsulating Security Payload (ESP)

	RFC 4718	IKEv2 Clarifications and implementation Guidelines
Multicast	RFC2375	Asignación de Direcciones Multicast
	RFC2710	Descubrimiento de nodos que desean recibir Multicast para IPv6
	RFC2776	Protocolo de Anunciación de Zonas de Ambito Multicast (MZAP)
Anycast	RFC2526	Direcciones de Subredes para Anycast en IPv6
Multi-Homing	RFC2260	Soporte Escalable de Multi-homing para Conectividad Multi-Proveedor
	RFC2497	Transmisión de paquetes IPv6 sobre redes ARCnet
Transición	RFC1933	Mecanismos de Transición para Routers y Hosts IPv6
	RFC2185	Aspectos de Routing de la Transición IPv6
	RFC2473	Especificaciones Genéricas de Tunelización de Paquetes en IPv6
	RFC2529	Transmisión de IPv6 sobre Dominios IPv4 sin Túneles Explícitos
	RFC2765	Algoritmo de Traslación Stateless IP/ICMP (SIIT)
	RFC2766	Protocolo de Traslación - Traslación de Dirección de Red
	RFC2767	Doble Pila en Hosts usando la Técnica "Bump-In-the-Stack" (BIS)
API	RFC2292/bis	Advanced Sockets API para IPv6
	RFC2553/bis	Basic Socket API para IPv6
MIB	RFC2452	Base de Información de Gestión para IPv6: TCP
	RFC2454	Base de Información de Gestión para IPv6: UDP
	RFC2465	Base de Información de Gestión para IPv6: Convenciones Textuales y Grupo General
	RFC2466	Base de Información de Gestión para IPv6: ICMPv6
Otros	RFC1881	Gestión de la Asignación de Direcciones IPv6
	RFC1924	Representación Compacta de Direcciones IPv6
	RFC2147	TCP y UDP sobre Jumbogramas IPv6
	RFC2428	Extensiones FTP para IPv6 y NAT

	RFC2471	Plan de Asignación de direcciones IPv6 para Pruebas
	RFC2474	Definición del Campo de Servicios Diferenciados (DS) en Cabeceras IPv4 e IPv6
	RFC2546	Prácticas de Routing en 6Bone
	RFC2663	Consideraciones y Terminología de IP NAT
	RFC2732	Formato para la representación literal de direcciones IPv6 en URL's
	RFC2772	Guías de Routing en el troncal 6Bone
	RFC2775	Transparencia de Internet" (MINTIC, 2019)

Fuente: MINTIC. 2019. Protocolos de Internet Version 6. [En línea] 14 de febrero de 2019. https://www.mintic.gov.co/portal/604/w3-article-5938.html.

8.5 RIESGOS AL NO IMPLEMENTAR IPV6

Dentro de los riesgos que se tienen al no efectuar la implementación de IPv6 a nivel mundial a la mayor brevedad posible[111] se tiene:

- Perdida para el desarrollo del internet
- Dado el crecimiento de la red de comunicaciones en internet, cada día nuevas redes son creadas, como es el internet de las cosas[112], dispositivos celulares, sin tener la posibilidad de crecimiento en estas áreas.
- Se corre un gran riesgo al no realizar la implementación de IPv6 en materia de costo.
- Las entidades proveedores del servicio de internet (ISP) no tendrían desarrollo e innovación para ofrecer a sus usuarios y mantenerse a la vanguardia.

8.6 ESTABLECER LAS RAZONES POR LAS CUALES SE DEBE MIGRAR EL PROTOCOLO IPV4 A IPV6

[111] ALONSO, Juan Carlos. 2015. LACNIC. Desarrollo de IPv6 en la región. [En línea] 2 de junio de 2015. https://www.youtube.com/watch?v=qKJdCFFO3K0&list=PLJ3jHT8E6frAuYS73uN2QLWi8qyXRyxo1&index=5

[112] JJTORRES. 2014. ¿Qué es y cómo funciona el Internet de las cosas? [En línea] 20 de octubre de 2014. https://hipertextual.com/archivo/2014/10/internet-cosas/.

A finales de 1992 y una vez se vio el inconveniente con IPv4 con relación al agotamiento de direcciones IP a causa del auge que tiene el servicio de internet a nivel mundial y algunas medidas para su mejoramiento entre ellas la de seguridad, se inició con el proceso de diseñar una nueva arquitectura, la cual fue terminada y denominada IPv6.

El agotamiento de espacio de direccionamiento se vio agravado aún más teniendo en cuenta que por falta de programación de los delegados de la entrega de direccionamiento, se dejaron grandes espacios discontinuos de direcciones sin utilizar y además hubo una mala distribución de dicho direccionamiento asignando grupos de direcciones a empresas y entidades que realmente no la necesitaban.

La principal característica para la adopción de IPv6 está dada por el incremento de direcciones IP, donde se aumentó de 32 a 128 bits, la autoconfiguración de las direcciones, se realizaron mejoras en el direccionamiento que se tenía con IPv4 y se definió el direccionamiento anycast[113].

Dentro de las mejoras establecidas en el protocolo IPv6 se tiene el campo destinado para la etiqueta de flujo, los encabezados de extensión, el nivel de jerarquía, lo cual le permite a los routers mayor eficiencia al momento de realizar escalas para el servicio de internet, generado mayor eficiencia en los tiempos de respuesta[114].

Los host conectados a una red IPv6 se configuran de manera automática. El router recibe una configuración sobre el grupo de IPv6 correspondiente a la subred a configurar, en forma de IPv6 de manera que el mascara define la subred a la que pertenece el Router, creando una jerarquía de direcciones.

Para los usuarios finales el proceso de transición de los proveedores de IPv6[115] es total mente transparente, por lo tanto, un usuario normal no podrá identificar si se trata de una transmisión sobre IPv4 o IPv6. El proceso de trasmisión lo realizan los equipos de comunicaciones internamente, como Router, switch, entre otros.

---

[113] VIVES, Alvaro. 2015. LACNIC. Curso IPv6 Básico Módulo 4: Autoconfiguración – Conclusiones. [En línea] 5 de junio de 2015. https://www.youtube.com/watch?v=K3w_Gl3VCgI&list=PLJ3jHT8E6frAuYS73uN2QLWi8qyXRyxo1&index=22.

[114] DINERO. 2019. Las siete tendencias tecnológicas que se moverán en el 2020. [En línea] 26 de diciembre de 2019. [Citado el: 15 de mayo de 2020.] https://www.dinero.com/tecnologia/articulo/tecnologia-2020-estas-son-las-tendencias-tecnologicas-que-se-moveran/280471.

[115] MINISTERIO DE ECONOMIA Y EMPRESA DE ESPAÑA. ¿Qué es la transición a IPv6? [En línea] http://www.ipv6.gob.es/ipv6/transicion-IPv6/Paginas/que-es-transicion-IPv6.aspx.

El protocolo IPv6 no utiliza direcciones de red NAT, como si lo hacía IPv4, en donde un grupo de host que se encontraban en una misma red, se conectaban a una única dirección IP publica para salir a internet, sin embargo, la utilización de tablas de ruteo de gran dimensión en el backbone de internet, perjudicaba los tiempos de respuesta.

8.6.1 PROBLEMAS IDENTIFICADOS DE IPv4

Actualmente uno de los principales problemas es el agotamiento de direcciones IPv4 contratado en el crecimiento de la red y las necesidades de los usuarios. Dicho estado de agotamiento ya había sido identificado desde 1992 por los miembros de IETF, pero solamente desde hace unos años se están tomando las medidas necesarias para obligar a todas las empresas y organizaciones a migrar y adoptar el nuevo protocolo IPv6, lo cual liberaría las direcciones necesarias.

IPv4 no cuenta con servicios nativos tales como: calidad de servicios, seguridad y movilidad, por lo tanto, estos servicios deben ser añadidos para que trabajen sincronizadamente y dado el avance de las aplicaciones desarrolladas y la creación de nuevos equipos tecnológicos se está demandando cada vez mayor capacidad de respuesta, velocidad y seguridad en la comunicación.

Distribución inadecuada sobre la delegación de direccionamiento a nivel mundial. Las tablas de enrutamiento en donde se establecen las principales conexiones troncales de internet se han hecho tan grandes que han degradado los tiempos de respuesta degradando de manera sustancial la velocidad de transmisión y respuesta en las comunicaciones.

En los años 70 la preocupación principal de los ingenieros era el de establecer una comunicación entre los equipos conectados y no se tenía una concepción clara sobre la seguridad en la estructura de IPv4 sobre cada uno de los paquetes enviados y recibidos en la red, y solamente cuando al paso de los años y después de realizarse la detección de debilidades delicadas de seguridad y inicio a configurar parches de seguridad como SSL[116] e IPsec[117].

La utilización de NAT surgió a raíz del agotamiento de las direcciones IP, cuyo objetivo principal era el de establecer comunicaciones internas utilizando direcciones privadas y

---

[116] FUSARIO, Ruben Jorge . 2017. Vulnerabilidades enla seguridad delas transacciones interactivas de comercioelectronico a traves de la web. [En línea] 25 de octubre de 2017. http://bibliotecadigital.econ.uba.ar/download/tesis/1501-1279_FusarioRJ.pdf

[117] AVILA DIAZ, Luis Miguel. 2013. Configurar IPSec. [En línea] 14 de may de 2013. https://www.youtube.com/watch?v=PuQRlRhv-BU.

solamente se tenia salida al internet mediante una o varios direcciones publicas de un gran número de equipos conectados dentro de una red, lo cual rompía el principio del modelo end-to-end, es decir, una comunicación de extremo a extremo, lo cual afectaba la seguridad causando una falsa sensación de seguridad.

8.6.2 CARACTERISTICAS DEL PROTOCOLO IPV6

El protocolo IPv6 contiene en su gran mayoría las mismas características de IPv4 con las mejoras necesarias para enfrentar los retos de seguridad y expansión que a tenido el mercado tecnológico, dentro de las características principales que enmarcan el nuevo protocolo se pueden mencionar:

- **Mayor direccionamiento**

  Direccionamiento de 128 bits (16 bytes), permite contar con combinaciones posibles acorde a las necesidades actuales, dado que se tendría 2^{128} direcciones IP, es decir, 3,40282366920938 x 10^{38} alternativas viables, permitiendo varios niveles de subredes dentro de la organización.

- **Infraestructura eficaz y jerárquica**

  La infraestructura de direcciones globales de IPv6 esta estructurada para diseñar una infraestructura eficaz y jerárquica, con la capacidad de tener en cuenta varios niveles de servicios de internet, adicionalmente cuenta con tablas de enrutamiento más pequeñas y eficientes.

- **Formato de encabezado**

  El nuevo formato de encabezado cuenta con un diseño que permite la reducción al mínimo la carga del encabezado generando así más eficacia en los enrutadores intermedios, moviendo los campos no esenciales a los encabezados de extensión. Dado que la longitud de cabecera es fija, el encabezado permite optimizar el procesamiento y enrutamiento de paquetes[118].

  Es de precisar que el protocolo IPv6 no es compatible con el IPv4, por lo tanto un equipo de comunicación como PC o router debe utilizar un implementador de IPv4 y

[118] ZAPATA VALDES, Rodrigo Horacio. 2013. Análisis de Seguridad en el Protocolo IPv6. [En línea] 2013. http://157.92.136.59/download/tpos/1502-0820_ZapataValdezRH.pdf.

otra de IPv6 de manera simultánea para que se pueda reconocer los encabezados de cada uno de estos protocolos.

- **Mayor seguridad**

  Adicional a la estructura de IPV4, se cuenta con nuevos servicios de seguridad mediante un conjunto de protocolos IPsec, el cual mediante encabezados de autenticación AH encargado de la autenticación de la información verificando que estos no sean modificados y en segundo lugar el Cifrado de seguridad ESP, de tal forma que solamente el destinatario puede la legitimidad para proceder a desencriptar la información transmitida[119].

- **Configuración de direcciones**

  Dentro de las características principales de IPv6, estas se realizan automáticamente en cada uno de los host que se encuentran vinculados a la red mediante el protocolo DN, en donde el host solicita al enrutador IPv6 un vinculo local y un prefijo de sitio determinando mediante los mecanismos del sistema operativo una dirección global.

- **Mejora en la compatibilidad**

  Dado que los campos de encabezados añadidos en IPv6 (como Flow Label) controlan y permiten que los enrutadores identifican el tráfico proporcionando un control especial y sencillo de los paquetes transmitidos desde un origen a un destino dado, aun si estos son cifrados con IPsec.

- **Capacidad de ampliación**

  Una de las características de IPv6 esta dada por los encabezados de extensión, los cuales tienen una limitación correspondiente al tamaño del paquete, situación que hace que pueda ampliarse la capacidad de las características en IPv6 solamente agregando encabezados de extensión, situación que en IPv4 no podría darse.

- **Mejoramiento en la capacidad autenticación y privacidad**

  Los paquetes trasmitidos ofrecen mejoramiento en la capacidad de autenticación y privacidad de la información transmitida, los cuales son indicados en la cabecera de autenticación dado que se encuentran protegido por el protocolo de seguridad IPsec,

[119] BAUTISTA, Josué y CONTRERAS, Lobo y RICO, Dewar Willmer. 2011. Implementación de la seguridad del protocolo de internet. [En línea] Octubre de 2011. https://dialnet.unirioja.es/descarga/arti.

establece internamente protocolos de Seguridad de tráfico AH y ESP y el protocolo IKE encargado de la gestión de claves (Internet Key Exchange).

8.6.3 RECURSOS NUMERICOS

IANA - “Internet Assigned Numbers Authority”, es la organización encargada de suministrar direccionamiento de internet a nivel global, al igual que los números de sistemas autónomos para el enrutamiento del tráfico de internet, a través de las organizaciones no gubernamentales (RIR) cubriendo una región geográfica como: Afrinic, Apnic, Arin, Lacnic y Ripe NCC[120].

En la figura 9 se puede observar la cobertura de cada una de las organizaciones a nivel mundial (“Registros Regionales de Internet” - RIR) los cuales asignan y administran los protocolos de internet (IP) y la numeración de los sistemas autónomos (ASN) tanto a IPv4 como IPv6. Por intermedio de cada una de las RIR (AFRINIC, APNIC, ARIN, LACNIC y RIPE NCC) asignan grupos de direcciones a las regiones correspondientes[121].

Figura 9. Organizaciones para asignación de direccionamiento IPv6

REGISTRO	ÁREA CUBIERTA
AFRINIC	Región de África
APNIC	Región Asia Pacífico
ARIN	Canadá, Estados Unidos y algunas islas del Caribe
LACNIC	América Latina y algunas islas del Caribe
RIPE NCC	Europa, Medio Oriente y Asia Central

Fuente: IANA INTERNET ASSIGNED NUMBERS AUTHORY;. Number Resources. [En línea] https://www.iana.org/numbers.

[120] IANA INTERNET ASSIGNED NUMBERS AUTHORY;. Number Resources. [En línea] https://www.iana.org/numbers.

[121] Ibid.

- **IANA "Internet Assignet Numbers Authority - Autoridad de Números Asignados de Internet"**, asigna bloques de números de direccionamiento a los RIR (Registro Regional de Internet) bloques de números previo análisis[122].

- **RIR "Regional Internet Registry – Registro Nacional de Internet"**: Vigila la ubicación y registro de los números asignados para internet de los recursos dentro de una región en particular del mundo[123].

- **LIR "Registro Local de Internet"** o **NIR "Registro Nacional de Internet"**, le asigna direccionamiento IP a los Proveedores de Servicio de Internet (ISP)[124].

- **ISP "Los Proveedores de Servicio de Internet",** Es una compañía que ofrece a los consumidores acceso a internet. Asignan las direcciones IP a los usuarios[125].

- **UF – Usuario Final**: Estos usuarios pueden ser individuales o corporativos que requieren de un servicio de conectividad (servicio de internet)

En la figura 10, se observa toda la cadena de asignación la cual empieza con la IANA como coordinadora de reservas globales de números IP y números de sistemas autónomos la cual le asigna a los RIR de las diferentes regiones un número de bloques de direcciones quienes a su vez disponen de los registros locales (LIR) y nacionales (NIR) bloques de direcciones más pequeños que se asignan a los proveedores de servicio de internet (ISP), quienes a su vez asignan direcciones IP a las empresas y personas naturales[126].

---

[122] IANA INTERNET ASSIGNED NUMBERS AUTHORY;. Number Resources. [En línea] https://www.iana.org/numbers.

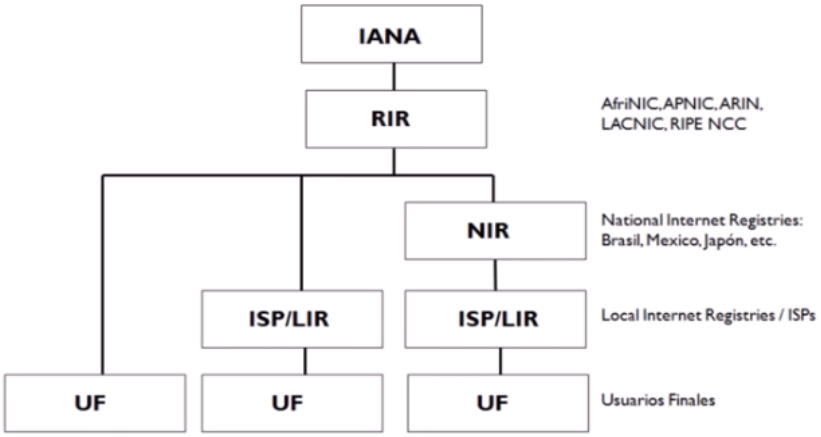
[123] Ibid.

[124] IANA.ORG. 2020. Internet Protocol Version 6 (IPv6) Parameters. [En línea] 11 de 08 de 2020. https://www.iana.org/assignments/ipv6-parameters/ipv6-parameters.xhtml.

[125] Ibid.

[126] LACNIC, Curso IPv6 Básico, tomado de: https://www.youtube.com/watch?v=-HIUT2ilCyU&list=PLsQToyLJISPWSMPF2DSbFmw_2HtzNpCSj& index=7

Figura 10. Jerarquía de asignación de direcciones IP



Fuente: LACNIC. Curso IPv6 Básico, tomado de: . [En línea] https://www.youtube.com/watch?v=-HIUT2ilCyU&list=PLsQToyLJISPWSMPF2DSbFmw_2HtzNpCSj& index=7

Normalmente IANA y los RIR asignan normalmente prefijos IPv6 "/23" a los LIR e ISP y estos a su asignan segmentos más grandes a los clientes o usuarios finales con bloques siempre mayores o iguales al prefijo "/48" el cual tendría una subred de 16 bits y una interface de 64 bits, visualmente se puede ver un ejemplo en la tabla 10.

Tabla 10. Ejemplo de estructura de una dirección IPv6 para un Usuario

PREFIJO ROUTING GLOBAL	ID DE SUBRED	ID DE INTERFACE
← **48 bits** →	← 16 bits →	← 64 bits →
2001:0DB8:0001	:5270:	0127:00AB:CAFÉ:0E1F

Fuente: "elaboración propia"

Para el territorio colombiano, la asignación de direccionamiento IP tanto de IPv4 como IPv6 está dada por la Organización LACNIC, la cual ofrece sus servicios de Registro de Direcciones de Internet de América Latina y Caribe, a treinta y tres países[127], dentro de los cuales se tienen:

"Argentina

[127] LACNIC. 2002. Lacnic. [En línea] 2002. https://www.lacnic.net/966/1/lacnic/acerca-de-lacnic.

Aruba
Belice
Bolivia
Bonaire
Brasil
Chile
Colombia
Costa Rica
Cuba
Curazao
Ecuador
El Salvador
Guatemala
Guyana
Guyana Francesa
Haití
Honduras
Islas Malvinas (Falkland Islands)*
México
Nicaragua
Panamá
Paraguay
Perú
República Dominicana
Saba
San Eustaquio
San Martin
South Georgia and The South Sandwich Islands
Suriname
Trinidad y Tobago
Uruguay
Venezuela

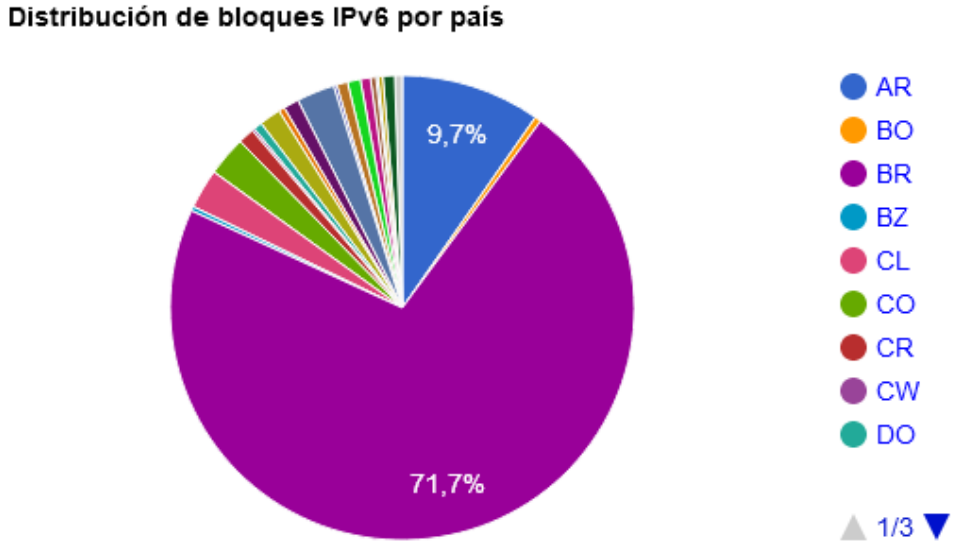
**Existe un conflicto entre los Gobiernos de Argentina y el Reino Unido e Irlanda del Norte con respecto a soberanía de las Islas Malvinas (Falkand Islands).*" (Lacnic, 2002 pág. 1)

Distribución de Bloques de IPv6 por país (América Latina)

Según la gráfica se puede apreciar que Brasil ha sido uno de los primeros países con asignación con un 71,7%, seguido por Argentina con un 9,7%, en Colombia solo cuenta

con 2,8% de las asignaciones un porcentaje relativamente muy bajo, teniendo en cuenta el inicio de implementación del protocolo IPv6[128], representado en la Grafica 1.

Grafica 1. Distribución de bloques IPv6 por País



Fuente: LACNIC**.** Estadísticas de Asignación de LACNIC. [En línea] https://www.lacnic.net/web/lacnic/estadisticas-asignacion.

Aproximadamente el 30% de las organizaciones a nivel mundial han realizado el despliegue y adopción del nuevo protocolo, tal como se puede evidenciar en la gráfica 2[129], en donde cada vez se toma con más fuerza la implementación y configuración del nuevo protocolo gracias a las políticas gubernamentales actuales establecidas a nivel interno en cada uno de los países[130].

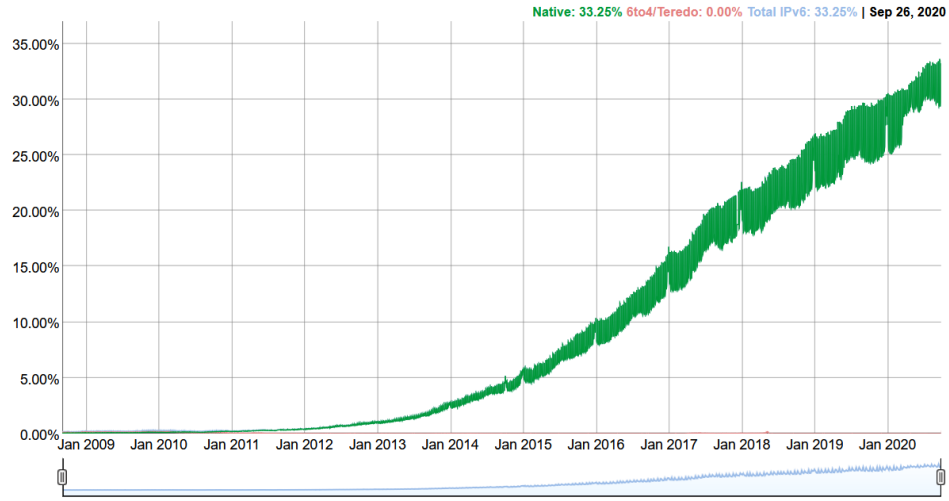
---

[128] BLANCHER, M. 2010. Migration to IPV6: A practical guide to implementing IPv6 in mobile and fixeed networks.Wiley. [En línea] 2010. http://www.isaca.org/COBIT/Pages/COBIT-5-spanish.aspx.

[129] LACNIC. Estadísticas de Asignación de LACNIC. [En línea] https://www.lacnic.net/web/lacnic/estadisticas-asignacion.

[130] AMBROSIO, Paola- CIO FUNCION PUBLICA. 2017. Red de los Servicios Públicos. Gobiernos de la región ayudan a promover el despliegue de IPv6. [En línea] 20 de diciembre de 2017. https://www.funcionpublica.gov.co/eva/red/publicaciones/gobiernos-de-la-regi%C3%B3n-ayudan-a-promover-el-despliegue-de-ipv6.

Grafica 2. Adopción de IPv6 a nivel mundial



Fuente: Google IPv6. Adopción de IPv6 . [En línea] https://www.google.com/intl/es/ipv6/statistics.html#tab=ipv6-adoption.

8.7 DESCRIBIR LOS MODOS DE TRANSMISION DE LA INFORMACION A TRAVÉS DEL PROTOCOLO IPV6

Existe una diferencia entre el modo transporte y el modo túnel, donde su principal diferencia radica en el nivel de seguridad.

8.7.1 MODO TRANSPORTE CON IPSEC

El modo transporte es más utilizado en comunicaciones punto a punto donde tanto el emisor como el receptor utilizan IPsec para que se puedan entender los dos extremos[131]. La cabecera AH o ESP se inserta entre los datos del datagrama y la cabecera IP original por o tanto solamente los datos que son transmitidos son cifrados y autenticados.

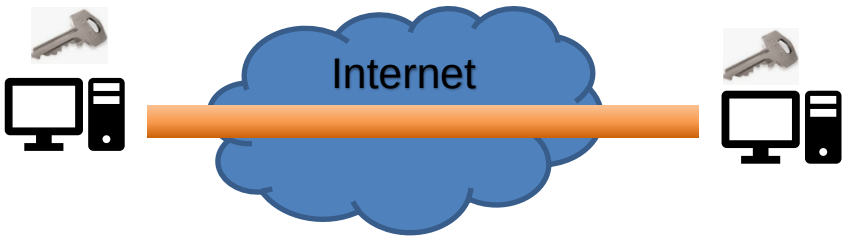
El paquete de datos son encriptados de desde el origen y desencriptado una vez se haya entregado a su destino final, por lo tanto, se tiene una comunicación segura entre los dos extremos de la comunicación, sin embargo, es importante tener en cuenta que ambos host cuenten con el protocolo IPsec como seguridad en la comunicación entre dos hosts que intercambien paquetes de datos.

---

[131] DIGITAL GIGES IONEO, Conexiones de red seguras con IPsec, tomado de: https://www.ionos.es/digitalguide/servidores/know-how/ipsec-arquitectura-de-seguridad-para-ipv4-e-ipv6/

Es de tener presente que este modo de transferencia solo se garantiza seguridad en los datos más no en el direccionamiento de origen y destino. IPsec puede establecer diferentes directivas de seguridad desde lo general hasta lo particular como el establecimiento de un puerto único de transmisión. El modo transporte se encuentra representado en la figura 11.

Figura 11. Modo de transporte IPsec



Fuente: “elaboración propia”

En el modo transporte se inserta la cabecera IPsec después de la cabecera IP del paquete original, la cual contiene un identificador de SA “Asociación de seguridad” un numero de secuencia y un resumen del campo de datos. El modo transporte es más utilizado en comunicaciones host a host dado que el emisor y el receptor utiliza IPsec, aumentando la seguridad de punto a punto. Esta situación está representada en la figura 12.

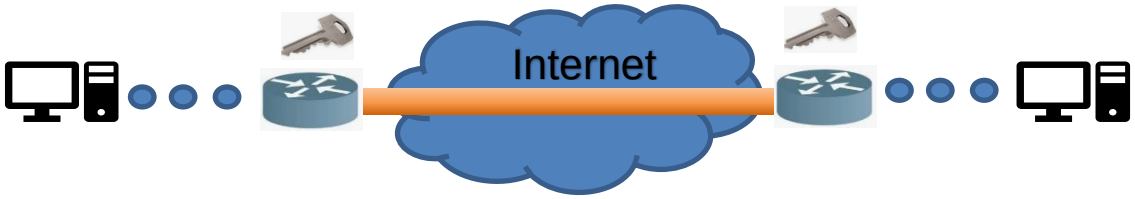
Figura 12. Modo de transporte Punto a Punto

Fuente: “elaboración propia”

8.7.2 MODO TÚNEL CON IPsec

Para el modo túnel se aplica varias capas o niveles de seguridad en donde la información es transmitida por un túnel en donde al iniciarse la transmisión, los datos son encapsulados y se genera una nueva dirección IP ficticias de tal forma que las reales son durante el recorrido de la transmisión y solamente cuando los datos trasmitidos llegan a su destino se desencapsula para que sean legibles por el receptor, este proceso es representado en la figura 13.

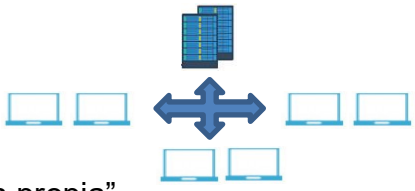
Figura 13. Modo Túnel Ipsec



Fuente: “elaboración propia”

El modo túnel es utilizado en conexiones desde la casa a un equipo ubicado en un equipo centralizado, comúnmente en una red interna de la empresa, como es el caso de la Intranet, conexión a aplicativos que deban ser ejecutadas desde el dominio de la organización, para poder ser utilizado desde una red externa, grafica representada en la figura 14.

Figura 14. Red Interna - Intranet de una organización



Fuente: “elaboración propia”

En la figura 15, se representa una comunicación desde un equipo centralizado ubicado en una empresa y que requiere brindar información a usuarios que se encuentran tanto interna como externa a la red de la entidad, por lo tanto la información será encapsula para que los equipos que se conectan a la internet este encriptada es decir una VPN por IPsec[132].

[132] DELGADO, Diego Álvarez Delgado; JORQUERA CACERES, Carolina; SEPÚLVEDA JORQUERA, GABRIEL; ZAMORA ESQUIVEL, Camila. 2014. Redes Privadas Virtuales (VPN). [En línea] 28 de julio de 2014. http://profesores.elo.utfsm.cl/~agv/elo322/1s14/projects/reports/G20/Redes%20Privadas%20Virtuales%20%28VPN%29.pdf.

Figura 15. Canal VPN

Fuente: “elaboración propia”

8.8 RELACIONAR LOS TIPOS DE DIRECCIONAMIENTO CON QUE CUENTA IPV6

8.8.1 TIPO DE DIRECCIONAMIENTO EN IPv6

8.8.1.1 DIRECCIÓN UNICAST (UNO a UNO)

Este tipo de direcciones descubren de forma única una interfaz de red exclusiva para un dispositivo con IPv6, de tal forma que si se envía un paquete desde un host hacia una dirección unicast[133], este es recibido específicamente por una interfaz que tiene asignada dicha dirección unicast[134].

- Se identifica de forma única, por lo cual permite una sola interfaz en un dispositivo IPv6.
- Se envía un paquete directamente del Host origen al Host destino
- Cuenta con doble pila, es decir puede contar con una dirección IPv6 y una dirección IPv4.

---

[133] CARABELLI, Mariano- LONGO, Lucas - MONTENEGRO, Jose Maria, SISTEMAS DISTRIBUIDOS “El protocolo IPv6”. 2006, tomado de :. https://www.dsi.fceia.unr.edu.ar/downloads/distribuidos/material/monografias/IPV6.pdf.

[134] IANA.ORG. 2019. IPv6 Global Unicast Address Assignments. [En línea] 13 de marzo de 2019. https://www.iana.org/assignments/ipv6-unicast-address-assignments/ipv6-unicast-address-assignments.xhtml.

De las direcciones Unicast se tiene los siguientes tipos:

- **Dirección Unicast Global "Global Unicast"**: Son direcciones globalmente ruteables y accesibles desde conexiones en internet IPv6. Este tipo de direcciones es la comúnmente llamada en IPv4 como direcciones públicas. Para IPv6 pueden ser configuradas estáticas o que sean asignadas de manera dinámica. Las direcciones globales inician en 2000::/3[135].

- **Unicast de enlace local (Link -Local**): Son direcciones cuyo origen y destino son direcciones locales, por lo tanto, los router no deben enviar y recibir paquetes hacia otros enlaces. Este tipo de dirección es asignado automáticamente usando el prefijo FE80::/10.

- **Unicast local única (Unique Local Address-ULA)**: Direcciones locales únicas utilizadas dentro de un mismo enlace, dentro de un sitio. Las direcciones ULA no deben ser ruteables en internet global. Son las comúnmente llamadas en Ipv4 como direcciones privadas y se encuentran definidas en RFC 1918[136], establecidas en el rango FC00::/7 a FDFF::/7.

8.8.1.2 DIRECCIÓN MULTICAST (UNO A VARIOS)

Este direccionamiento es el reemplazo de las direcciones Broadcast que existen en IPv4. Es utilizado por los host que obtienen la dirección multicast entre los router de la red. Cuando se transmite un paquete a una dirección multicast, ésta es enviada a todas las interfaces que pertenezcan a esa dirección[137].

- Identifica un grupo de interfaces

- Se identifica mediante un rango de dirección reservado FF00::0/8

---

[135] Ibid.

[136] NETWORK WORKING GROUP Y. REKHTER. 1996. RFC 1918 - Address Allocation for Private Internets. [En línea] febrero de 1996. https://www.ietf.org/rfc/rfc1918.txt.

[137] IANA.ORG. 2019. IPv6 Global Unicast Address Assignments. [En línea] 13 de marzo de 2019. https://www.iana.org/assignments/ipv6-unicast-address-assignments/ipv6-unicast-address-assignments.xhtml.

- Si se envía un paquete a una dirección multicast, se envía a todas las interfaces que pertenezcan a esa dirección.

- Aunque el protocolo IPv6 no implementa broadcast, un paquete puede ser enviado a varios dispositivos mediante enlace multicast local a todos los nodos (all host).

- Multicast conserva muchas de las funciones establecidas en IPv4 y muchas mejoradas y nuevas, como multicast entre dominios RFC 3306[138], el simplificando soluciones entre dominios mediante RFC 3959[139].

8.8.1.3 DIRECCIÓN ANYCAST (UNO A LA MAS CERCA)

En comparacion con las direcciones multicast estas identifican multiples interfaces en varios dispositivos, con la diferencia que la información enviado por dirección anycast solo se entrega al dispositivo más cercano en términos de distancia de enrutamiento. Normalmente este tipo de direcciones solo es configurado en routers más no en los host[140].

- Se puede asignar a diferentes dispositivos

- El paquete se envía a una dirección más cerca del grupo

- El paquete se envía solo a un dispositivo

8.8.2 DIRECCIONES RESERVADAS EN IPv6

Una parte de las direccione IPv6 está reservada para varios usos, representados en la tabla 11, las cuales son direcciones no enrutables a internet, por lo tanto, no pueden ser

---

[138] NETWORK WORKING GROUP B. HABERMAN. 2002. RFC3306 - Unicast-Prefix-based IPv6 Multicast Addresses. [En línea] agosto de 2002. https://www.ietf.org/rfc/rfc3306.txt.

[139] NETWORK WORKING GROUP G. CAMARILLO. 2004. RFC3959 - The Early Session Disposition Type for the Session Initiation Protocol (SIP). [En línea] diciembre de 2004. https://www.ietf.org/rfc/rfc3959.txt.

[140] CARABELLI, Mariano; LONGO, Lucas; MONTENEGRO, Jose Maria. SISTEMAS DISTRIBUIDOS “El protocolo IPv6”. 2006, tomado de :. https://www.dsi.fceia.unr.edu.ar/downloads/distribuidos/material/monografias/IPV6.pdf.

utilizadas como direcciones unicast convencionales. IANA tiene reservado un uso y definición en el futuro para este tipo de direcciones, dentro de ellas se tienen:

Tabla 11. Direcciones reservadas en IPv6

Dirección IPV6	Identificación
2001:0000::/23	Direccion sin especificar
2002:0000::/16	Reservada para 6to4
2001:db8::/32	Reservado para documentación
::/128	Reservado para IANA, usada para la asignación de protocolos
::/0	Ruta por Defecto
::1/128	Dirección de Loopback, paquetes enviados a si mismo, representa lo mismo que en IPv4 127.0.0.1
::FFFF:0:0/96	Direccion IPv4 mapeada
FE80::/10 **FEBF::/10**	Prefijo de enlace local, enlace valido solamente para enlace físico local.
FEC0::	Enlace de emplazamiento local, solamente es valida localmente dentro de una organización, declarado obsoleto según RFC3879[141].
FC00::/7 **FDFF::/7**	Es utilizada para direcciones locales únicas – ULA (Unique-Local-Addresses), definido en la RFC 4193[142]
FF00::/8	Es utilizada para direcciones multicast
2000::/3 **3FFF::/3**	Direcciones globales unicast

Fuente: “elaboración propia”

8.8.2.1 DIRECCIONES IPv6 NO ESPECIFICADA (::/128)

La dirección all-zeros address o no especificada se representa mediante 0:0:0:0:0:0:0:0 y por lo tanto no debe ser asignada a ningún nodo, dado que no tiene dirección como tal, por tal motivo un router no podrá enviar un paquete IPv6 con origen no especificado e igualmente no se podrá enviar paquetes con destino no especificado.

[141] NETWORK WORKING GROUP C. HUITEMA. 2004. RFC3879 - Deprecating Site Local Addresses. [En línea] septiembre de 2004. https://www.ietf.org/rfc/rfc3879.txt.

[142] NETWORK WORKING GROUP R. HINDEN. 2005. RFC 4193 - Unique Local IPv6 Unicast Addresses. [En línea] octubre de 2005. https://www.ietf.org/rfc/rfc4193.txt.

8.8.2.2 DIRECCIONES DE LOOPBACK (::1/128)

La dirección unicast es igualmente denominada la dirección de Loopback y se representa 0:0:0:0:0:0:0:1. Se utiliza para auto enviarse un paquete IPv6, por lo tanto es una dirección unicast de link-local de interfaz virtual “loopback interface”. La dirección loopback no debe ser dirección física. La dirección loopback no debe ser utilizada como una dirección IP origen ni destino en paquetes IPv6 y debe ser descartados por un router IPv6.

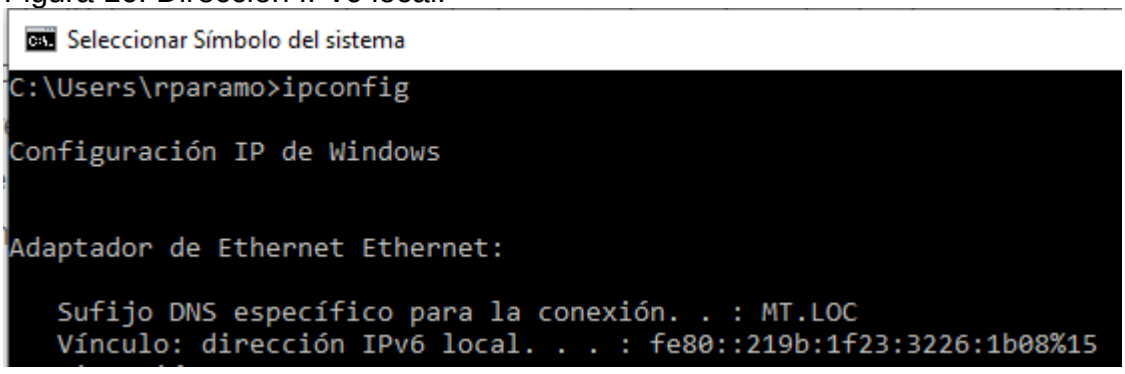
8.8.2.3 DIRECCION UNICAST DE ENLACE LOCAL (FE80::/10)

En este direccionamiento hay dos clases de uso local para las direcciones unicast:

Link-Local: Se utiliza dentro de un solo enlace con el propósito de hacer configuraciones de dirección automáticas vecinas. Los router no deben enviar paquetes con direcciones IP origen o destino con direcciones tipo Link-Local a otros enlaces fuera de la red.

Site-Local: Se utiliza como sitio local, estas direcciones se refieren únicamente a una red física en particular, representada en la figura 16. Los router no reenvían los datagramas usando una dirección de enlace local. Estas son únicamente para la comunicación local sobre un segmento de red físico en particular. Este enlace es con el propósito de hacer configuraciones de dirección automática, descubrimiento de vecinos, descubrimiento de routers y protocolos de routing de IPv6.

Figura 16. Dirección IPv6 local.



Fuente: “elaboración propia”

8.8.2.4 DIRECCIÓN LOCAL ÚNICA – ULA (FC00::/7 HASTA FDFF::/7)

Son similares a las direcciones privadas de IPv4 definido en RFC 4193[143]. La función principal es facilitar el espacio de direcciones IPv6 para las comunicaciones dentro de un sitio local, la cual normalmente es denominada red privada, por lo tanto este tipo de direcciones esta libre para ser utilizada en redes privadas y no puede ser enrutada a internet.

8.8.2.5 DIRECCIÓN DE DOCUMENTACIÓN (2001:0db8::/32)

Este direccionamiento está reservado a la documentación, es decir, representar ejemplos de direccionamiento IPv6 o modelos de red IPv6, establecido en el RFC 3849[144], lo anterior debido a que se han detectado conflictos de dirección y enrutamiento con los servicios existentes al realizarse una asignación explicita de una documentación prefijo de direcciones 2001:0DB8::/32 y no debe ser enrutada a internet.

8.8.2.6 DIRECCIÓN LINK -LOCAL (FE80::/10)

Este es un tipo de direccionamiento unicast, la cual es una herramientas útil para realizar conexiones LAN, en donde las comunicaciones no pueden ser enrutadas directamente a internet pero si puede ser utilizada para compartir y realizar comunicaciones internas y locales entre host dentro de una organización.

- Está diseñada para enlaces locales
- Se configura de manera automática
- No permite enviar paquetes a una dirección link-local

8.8.2.7 DIRECCIÓN DE BUCLE INVERTIDO

---

[143] NETWORK WORKING GROUP R. HINDEN, RFC 4193 - Unique Local IPv6 Unicast Addresses, octubre 2005, tomado de: https://www.ietf.org/rfc/rfc4193.txt

[144] NETWORK WORKING GROUP G. HUSTON, RFC 3849 - IPv6 Address Prefix Reserved for Documentation, julio 2004, tomado de: https://www.ietf.org/rfc/rfc3849.txt

El tipo de direccionamiento bucle invertido es el grupo de direcciones IP reservado desde la dirección 127.0.0.1 a 127.255.255.255 en IPv4, su función es apuntar nuevamente al equipo de emisión, es decir, los paquetes enviados nunca llegan a red, sino que llegan al mismo equipo origen. Este tipo de direccionamiento es utilizado para realizar pruebas a recursos del mismo equipo, o lo que es lo mismo equivale a la dirección web “localhost”.

- Función de dirección local similar a 127.0.0.1 de IPv4
- 0:0:0:0:0:0:01representa la dirección de bucle invertido, que es igual a ::1
- La utiliza un dispositivo para enviarse un paquete a si mismo

8.8.3 DIRECCIONAMIENTO IPv6 Y SU CONFIGURACIÓN

Para la configuración de direccionamiento IPv6 se puede realizar de manera manual o automática mediante dos mecanismos: StateLess Addres Auto-Configuraction (SLAAC) y Dynamic Host Configuraction Protocol versión 6 (DHCPv6), entendiéndose que el primero es obligatorio y el segundo es opcional.

8.8.3.1 STATELESS ADDRES AUTO-CONFIGURACTION (SLAAC)

El Router al recibir una solicitud de un host que requiere unirse a una red, le responde con un prefijo IPv6 de red local al que se debe añadir su correspondiente identificador de interfaz (IID) para completar su direccionamiento IPv6. La diferencia de contar con un servidor DHCPv6 es que esta característica la puede generar cualquier router que este configurado con la instrucción IPv6 unicast-routing mediante el cruce de mensajes RS – Solicitud Router y RA-Anuncio de Router, a través de ICMpv6. El IID de 64 bits basado en la capa de enlace de la red, utiliza la tecnología IEEE Extended Unique Identifield 64 bits.

Proceso EUI-64 (Extended Unique Identifiel) : Es el proceso que emplea la MAC “Control de Acceso a Medios” del host, es decir la cédula de un PC y la utiliza como Identificación de interfaz en la dirección IPv6, pero dado que la MAC de un equipo solo cuenta con 48 bit y la Identificación de interfaz es de 64 bits, se debe agregar el número 0xFFFE entre el OUI (Identificador Único Organizacional) de la MAC y el serial de la misma. Durante este proceso se realizan cambio como: Cambiar el séptimo bit más significativo de la MAC de 0 lógico a 1 lógico. Este proceso puede ser visualizado en la figura 17.

Figura 17. Proceso EUI-64

Direccion MAC	OUI - 24 bits (Identificador Único de Organización)			Identificador de Dispositivo - 24 bits		
	D9	9E	F3	0B	DF	D0

Numero 0xFFFE	FF	FE
	11111111	11111110

Union de OUI + 0xFFFE + Id. Disp	D9	9E	F3	FF	FE	0B	DF	D0
	11011001	10011110	11110011	11111111	11111110	1011	11011111	11010000

Cambio el 7 bit de 0 po 1	DB	9E	F3	FF	FE	0B	DF	D0
	11011011	10011110	11110011	11111111	11111110	1011	11011111	11010000

ID de interfaz EUI-64	**DB**	**9E**	**F3**	**FF**	**FE**	**0B**	**DF**	**D0**

Fuente: “elaboración propia”

8.8.3.2 DYNAMIC HOST CONFIGURACTION PROTOCOL VERSIÓN 6 (DHCPV6)

El protocolo DHCPv6 se encuentra establecido en RFC 3315[145] de la IETF, este tipo de protocolo es cliente-servidor, en donde se asigna un direccionamiento IPv6 por parte del servidor de DHCP a cada uno de los hosts pertenecen a la a red específica, asignando un rango especifico y secuencial de acuerdo a las políticas establecidas previamente en el servidor[146].

8.8.4 DIRECCIONES IPv4 QUE SON COMPATIBLES DE IPv6

El direccionamiento de IPv6 fue basado en el direccionamiento IPv4, por tal motivo y teniendo en cuenta que la dirección IPv4 solo cuenta con 32 bits, una dirección IPv6 esta formada por 96 bits iniciales con cero y los 32 bits finales corresponderán a la dirección IPv4 para completar 128 bits de la dirección completa IPv6[147]. En la práctica este tipo de

[145] NETWORK WORKING GROUP R. DROMS, ED. 2003. RFC 3315 - Dynamic Host Configuration Protocol for IPv6 (DHCPv6). [En línea] julio de 2003. https://www.ietf.org/rfc/rfc3315.txt.

[146] VIVES, Alvaro. 2015. LACNIC. Curso IPv6 Básico Módulo 4: Autoconfiguración – Stateful (DHCPv6). [En línea] 5 de junio de 2015. https://www.youtube.com/watch?v=Eiy4gHNxjaw&list=PLJ3jHT8E6frAuYS73uN2QLWi8qyXRyxo1&index=21.

[147] Ibid.

direccionamiento no es utilizado y no están contempladas en los mecanismos de transición a IPv6[148], pero si es importante tener claro esta concepción, la cual se puede visualizar en la tabla 12.

Tabla 12. Formatos de direcciones IPv6 compatibles con IPv4

DIRECCIONES IPv4 COMPATIBLES CON IPv6	PREFIJO DE ENRUTAMIENTO GLOBAL	ID DE SUBRED	ID DE INTERFACE
	← 80 bits →	← 16 bits →	← 32 bits →
Dirección Mapeable	0000:0000:0000	FFFF	Dirección IPv4
Dirección Compatible	0000:0000:0000	0000	Dirección IPv4

Fuente: “elaboración propia”

Tal como se muestra a continuación, existen una dirección IPv6 que es compatible con IPv4, es decir, una dirección IPv4 puede ser representada como como una dirección IPv6 de acuerdo a direcciones mapeadas ::ffff:Bloque 1.Bloque 2.Bloque 3.Bloque 4 /96 o direcciones compatibles Bloque 1.Bloque 2.Bloque 3.Bloque 4 /96.

Dirección IPv4 mapeada → ::ffff: Bloque 1.Bloque 2.Bloque 3.Bloque 4 /96
Dirección Compatible → :: Bloque 1.Bloque 2.Bloque 3.Bloque 4 /96

Como ejemplo de lo anteriormente visto, al tener la **dirección mapeada** IPv4 ffff.192.168.10.25, esta puede ser convertida a IPv6 colocando los primeros 96 bits en cero “0” ::ffff, posteriormente se convierte cada grupo en un numero hexadecimal, es decir, 192 = C0, 168=A8, 10=0A y 25=19, con lo cual quedará: ::ffff:C0A8:0A19. Así mismo una dirección compatible IPv4 puede ser convertida a IPv6, tal como se visualiza en el ejemplo de la tabla 13.

Tabla 13. Ejemplo de Direcciones compatibles

Tipo de Ejemplo	IPv4	IPv6
Dirección Mapeada	::ffff:192.168.10.25	::ffff:C0A8:0A19
Dirección Compatible	::192.168.10.25	::C0A8:0A19

Fuente: “elaboración propia”

---

[148] VELEZ VARELA, Fernando y GUTIERREZ RANCRUEL, Liliana. 2019. IPv6, una realidad. Bogotá - Colombia : Ediciones de la U, 2019, p. 114.

8.9 IDENTIFICAR LOS MOTIVOS POR LOS CUALES DEBE EXISTIR UNA CONVIVENCIA DE IPV4 CON IPV6.

Desde la creación de IPv6, se tenía claro que debía haber una transición con IPv4[149], por lo tanto, se debía introducir el nuevo protocolo sin interferir el ya existente, sin embargo, se debe tener en cuenta que entre los dos protocolos no existe una compatibilidad, dado que si un paquete es enviado en IPv6, este no será entendido por un equipo con IPv4[150].

8.9.1 DOBLE PILA - DUAL-STACK

Se debe contar con los dispositivos necesarios para los dos tipos de protocolos, con una estructura de red, con una interfaz tanto del protocolo IPv4 como IPv6, de tal forma que se trabaja en paralelo[151]. En la figura 18, se muestra un servidor Dual-Stack donde se puede acceder desde cualquier tipo de host, para ello se debe configurar en el DNS del servidor un direccionamiento tanto IPv4 como IPv6, de tal forma que permita tráfico desde ambos protocolos[152].

Con el propósito de no contar con retardos en la conexión desde un host bien sea con IPv4 o IPv6, se tiene establecido el mecanismo Happy -eyeballs en el RFC 6555[153], de tal forma que el host se intenta conectar de manera simultánea por IPv4 e IPv6, y deja el protocolo por el cual se pueda conectar, el cual es almacenado en el navegador si se requiere conectar en una próxima oportunidad.

---

[149] ESPAÑA, MINISTERIO DE ECONOMIA Y EMPRESA DE ESPAÑA. ¿Qué es la transición a IPv6? [En línea] http://www.ipv6.gob.es/ipv6/transicion-IPv6/Paginas/que-es-transicion-IPv6.aspx.

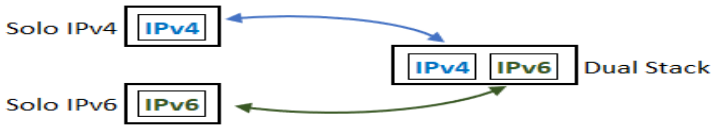
[150] Ministerio de Economia y Empresa de España, ¿Qué es la transición a IPv6?, tomado de: http://www.ipv6.gob.es/ipv6/transicion-IPv6/Paginas/que-es-transicion-IPv6.aspx.

[151] VIVES, Alvaro. 2015. LACNIC. Curso IPv6 Básico Módulo 2: Agotamiento espacio IPV4, coexistencia y transición – Doble Pila. [En línea] 5 de junio de 2015. https://www.youtube.com/watch?v=C_ekmx7v9m0&list=PLJ3jHT8E6frAuYS73uN2QLWi8qyXRyxo1&index=10.

[152] TUTORIALSPOINT, IPv6 Tutorial. 2016, tomado de: https://www.tutorialspoint.com/es/ipv6/ipv6_ipv4_to_ipv6.htm.

[153] INTERNET ENGINEERING TASK FORCE (IETF) D. WING. 2012. RFC6555 - Happy Eyeballs: Success with Dual-Stack Hosts. [En línea] abril de 2012. https://www.ietf.org/rfc/rfc6555.txt.

Figura 18. Dual-Stack



Fuente: “elaboración propia”

8.9.2 TÚNELES

Encapsular una versión de IP dentro de otra versión IP, de tal forma que se pueda permitir una comunicación. Estos mecanismos basados en túneles permiten encapsular paquetes de IPv6 en infraestructura de trasporte IPv4. Los puntos de salida de las redes interconectadas encapsulan paquetes de IPv6para los destinos IPv6 a través de interfaces de IPv4. Los paquetes son transportados por el sistema de ruteo IPv4 y son desencapsulados al otro extremo del túnel[154]. Estos mecanismos basados en túneles permiten encapsular:

- Encapsular IPv6 directamente dentro de IPv4
- Encapsular IPv6 dentro de IPv4 utilizando una cabecera GRE
- Encapsular IPv4 directamente dentro de IPv6
- Encapsular IPv4 dentro de IPv6 utilizando UDP (Para atravesar NAT)

La configuración de túneles recomendada en la RFC 2893[155], túneles que manejan tráfico IPv4 entre nodos IPv6/IPv4 sobre infraestructura IPv4. Es importante que el túnel IPv6 sobre IPv4 solo describe la encapsulación en la cabecera IPv4 de manera que los noves IPv6 resulten alcanzables mediante la infraestructura IPv4 existente. La configuración de túneles recomendada en la RFC 2893[156], se tiene: comunicación entre Router, Router a Host y viceversa, y entre Host.

Router a Router: Los routers configurados como Dual-Stack que se encuentren conectados en una infraestructura de IPv4, puede enviar y recibir paquetes IPv6 sin

---

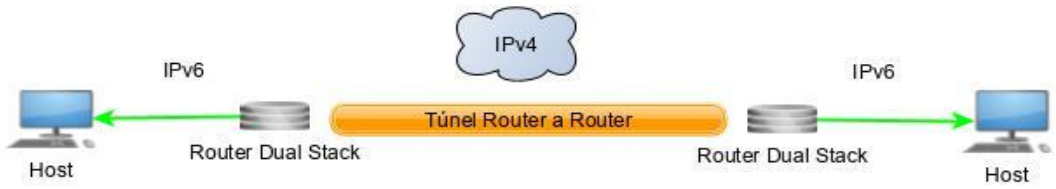
[154] UPM, GRUPO DE SISTEMAS OPERATIVOS DATSI FI. 2012. Protocolo IPsec. [En línea] 8 de octubre de 2012. http://laurel.datsi.fi.upm.es/proyectos/teldatsi/teldatsi/protocolos_de_comunicaciones/protocolo_ipsec.

[155] NETWORK WORKING GROUP R. GILLIGAN. 2000. RFC 2893 - Transition Mechanisms for IPv6 Hosts and Routers. [En línea] agosto de 2000. https://www.ietf.org/rfc/rfc2893.txt.

[156] Ibit

ningún inconvenientes, dado que los routers se encargan de encapsular el paquete para que viaje dentro de la infraestructura de IPv4. Esta representación puede ser visualizada en la figura 19.

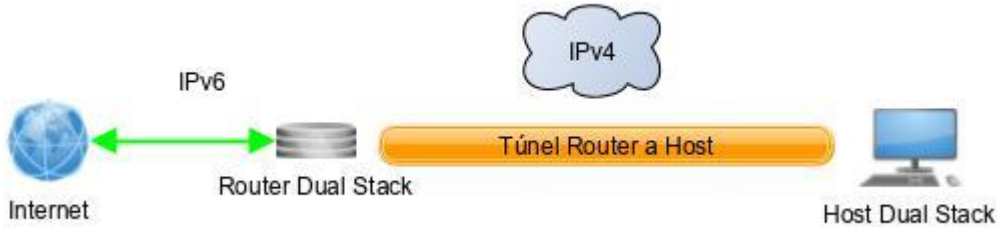
Figura 19. Estructura Router a Router



Fuente: “elaboración propia”

Host a Router: Es la transmisión de paquetes IPv6 de un Host configurado como Dual Stack a un Router configurado como Dual Stack y viceversa mediante una infraestructura de IPv4. Los router Dual Stack interconectados con una infraestructura IPv4 pueden enviar y recibir entre si paquetes IPv6. Esta representación puede ser visualizada en la figura 20.

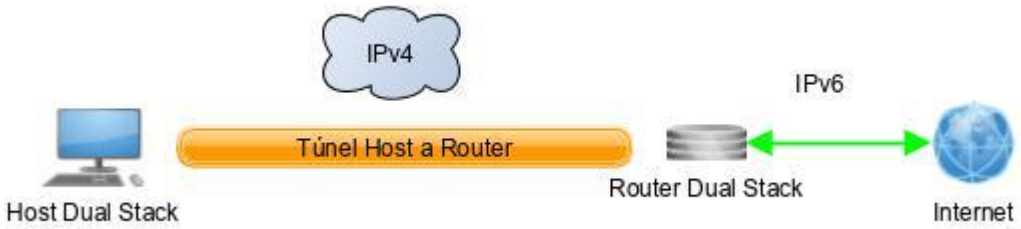
Figura 20. Estructura Router a Host



Fuente: “elaboración propia”

Router a Host: Es la transmisión de paquetes IPv6 de un Host configurado como Dual Stack a un Router configurado como Dual Stack mediante una infraestructura de IPv4. Los router Dual Stack interconectados con una infraestructura IPv4 pueden enviar y recibir entre si paquetes IPv6. Esta representación puede ser visualizada en la figura 21.

Figura 21. Estructura Host a Router



Fuente: "elaboración propia"

Host to Host: Los host tanto origen como destino al ser configurados como Dual Stack pueden al ser interconectados en una infraestructura IPv4 y consiguen enviar y recibir entre si paquetes IPv6, con lo cual puede atravesar paquetes por una infraestructura de IPv4. La representación gráfica se puede observar en la figura 22.

Figura 22. Estructura Host a Host

Fuente: "elaboración propia"

8.9.2.1 CLASES DE TÚNELES

a. **Túneles Estáticos / Manuales**: Cuando se configuran de manera estática y manual los extremos de túnel[157]. Esta clase de túnel esta basado en dos direcciones IPv4 y dos direcciones IPv6; Las dos direcciones IPv4 se utiliza entre la dirección del host o router origen y la dirección del servidor del túnel en el lado del destino, entre tanto, las dos direcciones IPv6 van dentro del túnel y se asignan a la fuente y al destino. Entre esta clase se encuentran el tipo de túnel 4to6.

---

[157] LACNIC. Capacitación-LACNIC - HD MODULO-2 Video-f Tuneles v01. [En línea] https://www.youtube.com/watch?v=sE3rPzhiswM&list=PLJ3jHT8E6frAuYS73uN2QLWi8qyXRyxo1&index=11.

b. **Túneles Automáticos/ Dinámicos**: Cuando se establece su configuración o parte de ella manera automática. Entre esta clase se encuentran 6to4, Isatab y Toredo, en donde su característica principal es la de proporcionar una dirección IPv6 o prefijo basado en dirección IPv4 (dirección dinámica), con la desventaja de que si se cae la conexión se tendría que solicitar nuevamente el direccionamiento dado que el direccionamiento no es fijo[158].

8.9.2.2 TIPOS DE TÚNELES

a. Túnel 6over4: Utiliza encapsulado IPV6 dentro de un paquete IPv4[159].

Este tipo de túnel se encuentra definido en RFC 2529[160], también es conocido como tunelado multicast. Este mecanismo permite la comunicación de nodos IPv6 dentro de una red IPv4, en donde se encapsula comunicación IPv6 dentro de direcciones IPv4 mediante routers sin soporte a IPv6[161]. Este tipo de túneles usa direcciones IPv4 con identificador de interfaces creando un enlace virtual IPv4 con alcance local, este tipo de tunelado se puede observar en la figura 23.

- Encapsula IPV6 dentro de un paquete IPv4
- Utiliza el protocolo 41.
- Estático, configurado manualmente.
- Se puede encapsular directamente sobre IPv4 o con cabecera GRE

---

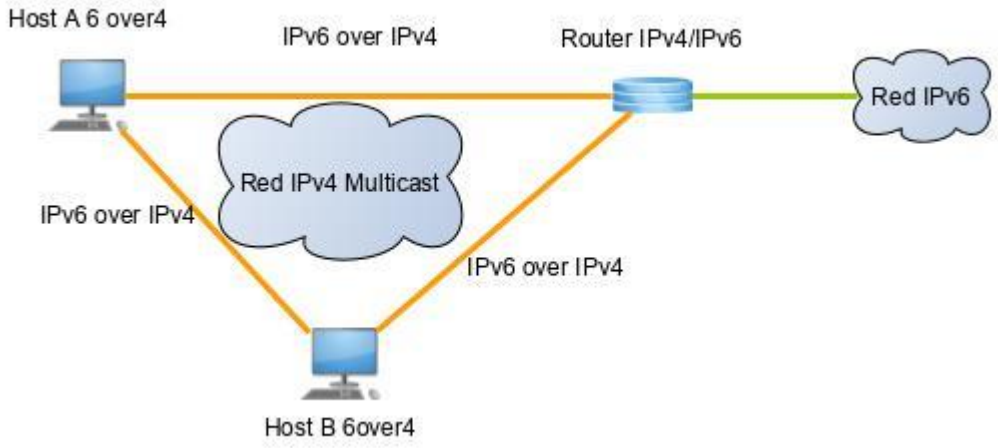
[158] Ibid.

[159] Ibid.

[160] NETWORK WORKING GROUP B. CARPENTER. 1999. RFC2529 - Transmisión de IPv6 sobre Dominios IPv4 sin Túneles Explícitos. [En línea] marzo de 1999. https://www.ietf.org/rfc/rfc2529.txt.

[161] LACNIC, Curso IPv6 Básico, Modulo 2 Agotamiento del espacio IPv4, coexistencia y transición, https://www.youtube.com/watch?v=sE3rPzhiswM&list=PLJ3jHT8E6frAuYS73uN2QLWi8qyXRyxo1&index=11.

Figura 23. Estructura Túnel 6over4



Fuente: SALVADOR, Fernandez. Fundamentos de migración. 2008, p26.

b. Túnel Tunnel-broker

- Corresponde al mismo tipo de túnel 6 in 4 pero de manera sistematizada, para lo cual se debe registrar en una pagina web solicitando la creación del túnel, en donde el tunnel-broker se encarga de configurar el extremo del túnel (Router) contra el servidor de Túneles, posteriormente se remitirá instrucciones al usuario del host para configurar Sistema Operativo, y su IP. Este tipo de túneles pueden ser creados de manera gratuita en la página tunnelbroker.net[162].

c. Túnel 6 to 4

Este tipo de túnel está definido en RFC 3056[163], el cual se utiliza para unir redes con soporte para IPv6 y que tengan que comunicarse a través de infraestructura IPv4[164], este esquema se puede observar en la figura 24. Para este propósito IANA dispuso

---

[162] LACNIC. Capacitación-LACNIC - HD MODULO-2 Video-f Tuneles v01. [En línea] https://www.youtube.com/watch?v=sE3rPzhiswM&list=PLJ3jHT8E6frAuYS73uN2QLWi8qyXRyxo1&index=11.

[163] NETWORK WORKING GROUP B. CARPENTER. 2001. RFC 3056 -Connection of IPv6 Domains via IPv4 Clouds. [En línea] febrero de 2001. https://www.ietf.org/rfc/rfc3056.txt.

[164] LACNIC, Curso IPv6 Básico, Modulo 2 Agotamiento del espacio IPv4, coexistencia y transición, https://www.youtube.com/watch?v=sE3rPzhiswM&list=PLJ3jHT8E6frAuYS73uN2QLWi8qyXRyxo1&index=11

un espacio reservado y específico para las direcciones 6to4[165] mediante el direccionamiento 2002::/16 la cual se puede observar en la tabla 14.

- Encapsula IPV6 dentro de un paquete IPv4
- Automático
- Multi-punto
- Prefijo de reserva 2002::/16
- Se requiere una dirección IPv4 publica
- Router 6to4: Crea interfaz 6to4 virtual, la cual encapsula y des encapsula el paquete de datos.
- Se utiliza entre nodos 6to4 frente 6to4 y 6to4 frente IPv6 nativo

Figura 24. Túnel 6to4

Fuente: "elaboración propia"

Tabla 14. Direccionamiento 6to4

2002	Dirección IPv4 Externa del Router	IP de Subred	ID de la Interfaz
16 bits	32 bits	16 bits	64 bits

Fuente: SALVADOR, Fernandez. Fundamentos de migración. 2008, p32.

d. Túnel 6RD

Este tipo de túnel al igual que 6to4 se utiliza para transportar de manera encapsulada el protocolo IPv6 dentro de una infraestructura de red que opera únicamente bajo direccionamiento IPv4, sin embargo a diferencia de 6to4 un proveedor de servicios

[165] LACNIC, Curso IPv6 Básico, Modulo 2 Agotamiento del espacio IPv4, coexistencia y transición, https://www.youtube.com/watch?v=sE3rPzhiswM&list=PLJ3jHT8E6frAuYS73uN2QLWi8qyXRyxo1&index=11

(ISP) que maneje 6rd utiliza un prefijo de IPv6 de su propiedad en lugar del prefijo 6to4 (2002::/16)[166].

- Hereda características de 6to4
- Encapsula IPV6 en IPv4
- Automático
- Multi-punto
- Evolución de 6to4
- No requiere un prefijo reservado
- Puede utilizar IPv4 privadas
- Es transparente al resto de usuarios de internet, por tal motivo es una solución para los ISP
- Concatena prefijo IPv6 con dirección IPv4 formando el prefijo 6RD de usuario
- Se utiliza entre nodos 6RD frente 6RD y 6RD frente IPv6 nativo

e. Túnel DS-Lite

Permite a los usuarios que solo cuentan con una versión de protocolo de comunicaciones IPx y requieren comunicación con otra versión de protocolo IPx que no es soportada, para esta situación se utiliza túneles, en donde se encapsula el protocolo IPx dentro de la otra versión que si lo es, haciendo posible que exista comunicación. El objetivo de estos túneles es atravesar una red que no soporte IPv(4 o 6)[167].

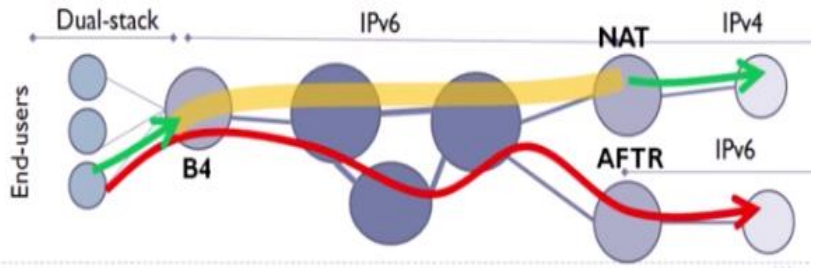
- Basado en la red IPv6
- Encapsula IPV4 dentro de IPv6 nativo
- Se comparten las direcciones IP4 públicas
- Genera un solo nivel NAT grande frente a un AFTR (Addres Family Transition Router), representado en la figura 25.

---

[166] LACNIC. Capacitación-LACNIC - HD MODULO-2 Video-f Tuneles v01. [En línea] https://www.youtube.com/watch?v=sE3rPzhiswM&list=PLJ3jHT8E6frAuYS73uN2QLWi8qyXRyxo1&index=11.

[167] LACNIC. Capacitación-LACNIC - HD MODULO-2 Video-f Tuneles v01. [En línea] https://www.youtube.com/watch?v=sE3rPzhiswM&list=PLJ3jHT8E6frAuYS73uN2QLWi8qyXRyxo1&index=11.

Figura 25. Túnel DS-Lite



Fuente: LACNIC**.** Capacitación-LACNIC - HD MODULO-2 Video-f Tuneles v01. [En línea] https://www.youtube.com/watch?v=sE3rPzhiswM&list=PLJ3jHT8E6frAuYS73uN2QLWi8qyXR yxo1&index=11.

8.9.3 MECANISMOS BASADOS EN TRADUCCION

Este mecanismo será necesaria para la comunicación de dos hosts para una sola versión diferente de la IP. Aunque esta técnica no es la más adecuada, pero es muy efectiva dado que traduce de IPv4 a IPv6 y viceversa, es decir, se realiza la transmisión de paquetes entre host sin importar el protocolo que maneja los entre origen y destino.

Aunque son los menos recomendados, es una opción cuando se pretende comunicar un host que solo entiende una versión de protocolo IPv(x) con otro host que solamente entiende una versión de protocolo IPv(y) en cualquiera de los sentidos. Estas traducciones pueden realizarse a distintos niveles de la capa de protocolos utilizadas por TCP/IP

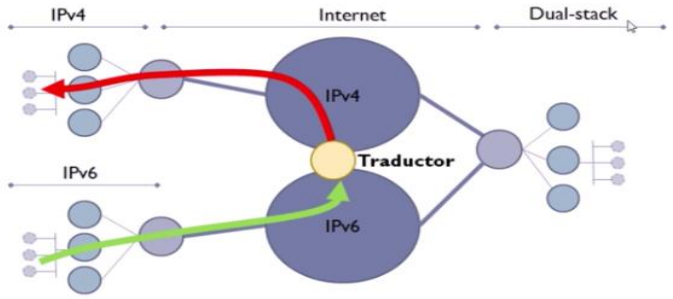
8.9.3.1 SOLO IPV6 A SOLO IPV4

Para dar solución a este modelo (Solo IPv6 a solo IPv4), se utiliza el mecanismo NAT64/DNS64, el cual permite un a un host solo IPv6 comunicarse con un host solo IPv4, en donde se traduce unicast solamente para TCP, UDP e ICMP, diferente a estos protocolos no será factible la traducción[168], representado en la figura 26.

[168] LACNIC. Capacitación-LACNIC - HD MODULO-2 Video-f Tuneles v01. [En línea]

Los usuarios solo IPv6 comparten direcciones publicas IPv4 públicas, para que los usuarios con protocolo IPv4 puedan recibir l transmisión de datos enviada, dado que existe una traducción automática de direcciones usando información estática. Para que esta solución funcione se utiliza un prefijo como 64:ff9b::/96 (96 bits) a la dirección IPv4 (32 bits) para completar la dirección de 128 de IPV6 y esta pueda ser reconocida por el equipo solo IPv6.

Figura 26. Mecanismo Basado en Traducción de IPv6 a IPv4



Fuente: LACNIC. Capacitación-LACNIC - HD MODULO-2 Video-f Tuneles v01. [En línea] https//www.youtube.com/watch?v=gTLK6uyLPCc&list=PLJ3jHT8E6frAuYS73uN2QLWi8qyXRyxo1&index=12

8.9.3.2 SOLO IPv4 A SOLO IPV6 (OBSOLETO SEGÚN RFC 4966[169])

Cuando un host solamente con IPv4 que inicia la transmisión requiere de un traductor para que implemento la cabecera de IPv4 como IPv6, para que el host destino solamente con protocolo IPv6 lo entienda[170], dado que este mecanismo esta obsoleto, cuando se presente este escenario lo recomendado es que se utilice un mecanismo de Doble Pila o Dual -Stack, representado en la figura 27.

---

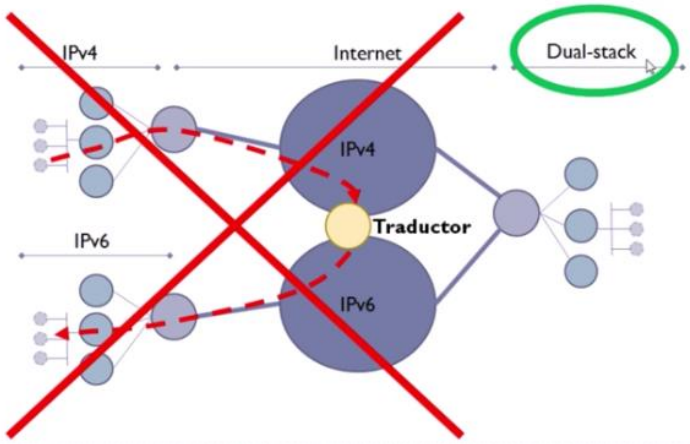
https//www.youtube.com/watch?v=gTLK6uyLPCc&list=PLJ3jHT8E6frAuYS73uN2QLWi8qyXRyxo1&index=12

[169] NETWORK WORKING GROUP C. AOUN. 2007. RFC4966 - Reasons to Move the Network Address Translator - Protocol Translator(NAT-PT) to Historic Status. [En línea] julio de 2007. https://www.ietf.org/rfc/rfc4966.txt.

[170] LACNIC. Capacitación-LACNIC - HD MODULO-2 Video-f Tuneles v01. [En línea]

https//www.youtube.com/watch?v=gTLK6uyLPCc&list=PLJ3jHT8E6frAuYS73uN2QLWi8qyXRyxo1&index=12

Figura 27. Mecanismo basado en Traducción IPv4 a IPv6



Fuente: LACNIC. Capacitación-LACNIC - HD MODULO-2 Video-f Tuneles v01. [En línea] https//www.youtube.com/watch?v=gTLK6uyLPCc&list=PLJ3jHT8E6frAuYS73uN2QLWi8qyXRyxo1&index=12

8.10 ESTRUCTURA, FUNCIONALIDAD Y SEGURIDAD OFRECIDA POR IPSEC

El protocolo IPsec “Internet Protocol Security” cuenta con una arquitectura de seguridad cifrada y con autenticación IP, propuesta por IETF “Grupo de Trabajo de Ingeniería de Internet”. El protocolo IPsec aunque ya existía desde IPv4, este no era obligatoria su utilización, pero para el protocolo IPv6 si lo es. Es importante tener en cuenta que solamente Ipsec puede proteger la capa de red, la capa IP y superiores, transporte y usuarios[171].

8.10.1 ESTRUCTURA DE IPSEC

IPsec establece protocolos de Seguridad de tráfico: AH y ESP y un protocolo de gestión de claves IKE “Internet Key Exchange”, en donde el protocolo AH aplica algoritmos de autenticación de datos verificando si los datos enviados son enviados por quien dice ser, representado en la figura 8. El protocolo ESP emplea algoritmos de encriptación para generar integridad de los datos transportados de tal forma que al ser modificados esta sea detectada.

---

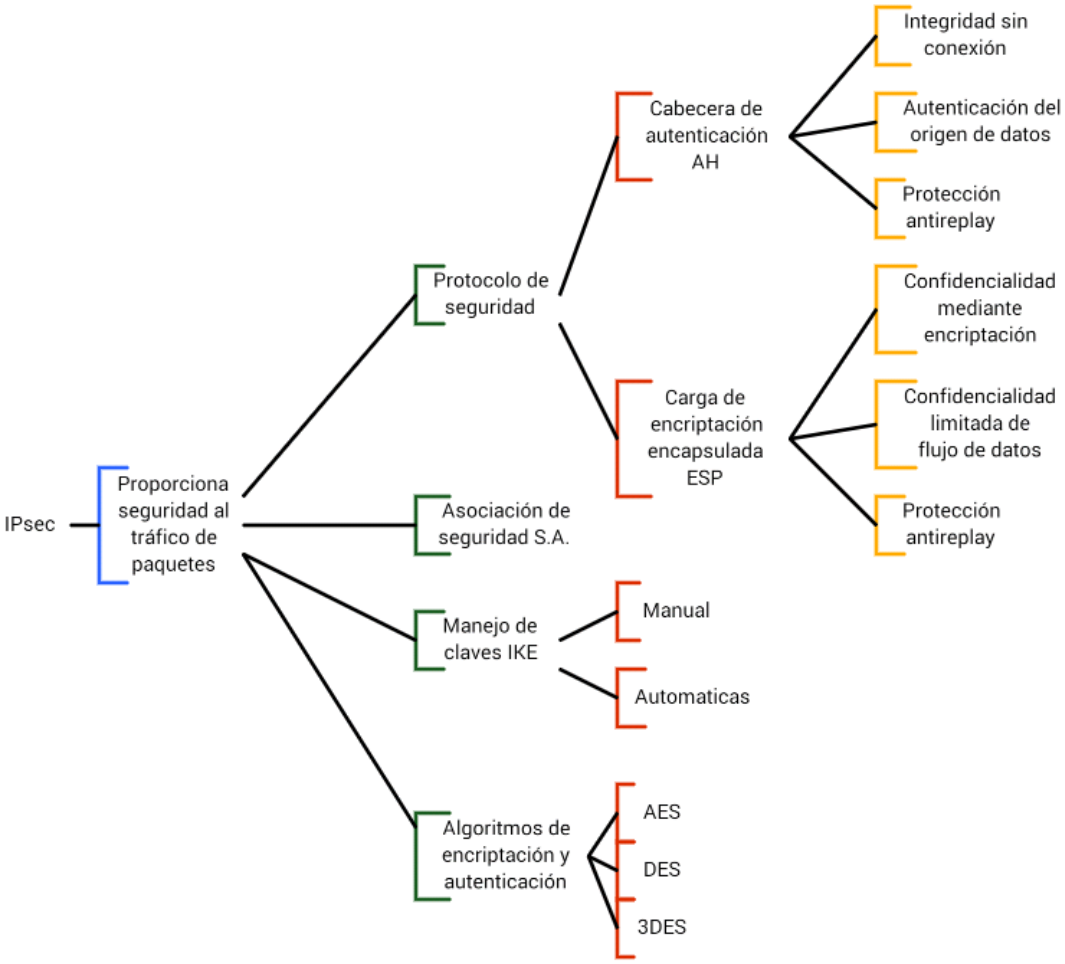
[171] JASON G, Andres. 2005. IPv6: the nextInternet protocol. [En línea] 2005. https://static.usenix.org/publications/login/2005-04/pdfs/andress0504.pd

La seguridad de un sistema está dada por muchos factores, entre ellos la implementación correcta y adecuada de los protocolos de seguridad Ipsec[172]. La seguridad de IPsec está sujeta a diversos factores como los defectos de seguridad en un sistema operativo o falta de conocimientos por parte de los encargados del manejo de la infraestructura en una organización sobre la práctica de protocolos.

El Domain Interpretation – DOI define los parámetros de negociación entre host para establecer canales seguros en un proceso de comunicación como: identificadores para algoritmos de autenticación (AH), identificadores para algoritmos de encriptación (ESP), parámetros operacionales para el protocolo de intercambio de llaves IKE y la ubicación de las claves criptográficas para cumplir con el proceso de encriptado y desencriptado.

[172] BLANCHER, M. 2010. Migration to IPV6: A practical guide to implementing IPv6 in mobile and fixeed networks.Wiley. [En línea] 2010. http://www.isaca.org/COBIT/Pages/COBIT-5-spanish.aspx.

Figura 28. Estructura de seguridad Protocolo IPsec

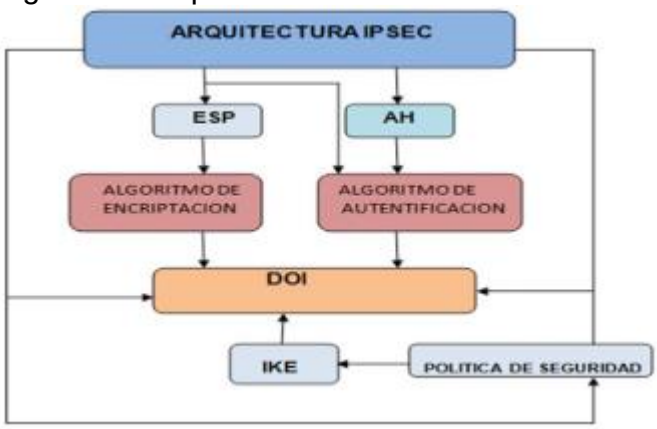


Fuente: “elaboración propia”

La política de seguridad “Security Police”, almacena la información adicional requerida para definir - qué - y – cuando - proteger el tráfico y actuar sobre un paquete IPv6, dichas políticas son almacenadas en una base de datos de políticas de seguridad SPD “Security Policy Database”[173] y la SAD “Base de Datos de Asociación” le específica a IPv6 como debe crear el canal de comunicación entre los dos hosts, representada en la figura 29.

[173] FRANCISCONI, Hugo Adrian. 2005. IPsec en Ambientes IPv4 e IPv6. [En línea] http://redes-linux.com/manuales/seguridad/IPsec_IPv4_IPv6.pdf. P. 13

Figura 29. Arquitectura General IPsec



Fuente: RICO BAUTISTA, Dewar Willmer y MEDINA CÁRDENAS, Yurley Constanza y SANTOS JAIME, Luz Marina. 2008. IPSec DE IPv6 EN LA UNIVERSIDAD DE PAMPLONA. [En línea] septiembre de 2008. https://www.redalyc.org/html/849/84920503057/.

8.10.1.1 PROTOCOLOS DE SEGURIDAD DE TRAFICO (AH)

El protocolo de seguridad AH garantiza la integridad y autenticidad de la información, constatando que el host receptor reciba exactamente lo que el host emisor envía, este protocolo corresponde a una cabecera ubicada entre la cabecera IP y los datos transportados como TCP, UDP o ICMP. Es importante tener en cuenta que el protocolo AH es susceptible de ataques contra repeticiones, copiar y pegar, por tal motivo se debe activar la protección contra repeticiones con lo cual descarta paquetes viejos[174].

El funcionamiento del protocolo AH se basa en las huellas digitales mediante un algoritmo HMAC, es decir un código de autenticación de mensajes (Message Authentication Code = MAC) como MD5 o SHA-1, la cual implica una función hash criptográfica combinada con una llave criptográfica secreta, para lo cual se siguen los pasos representados en la figura 30.

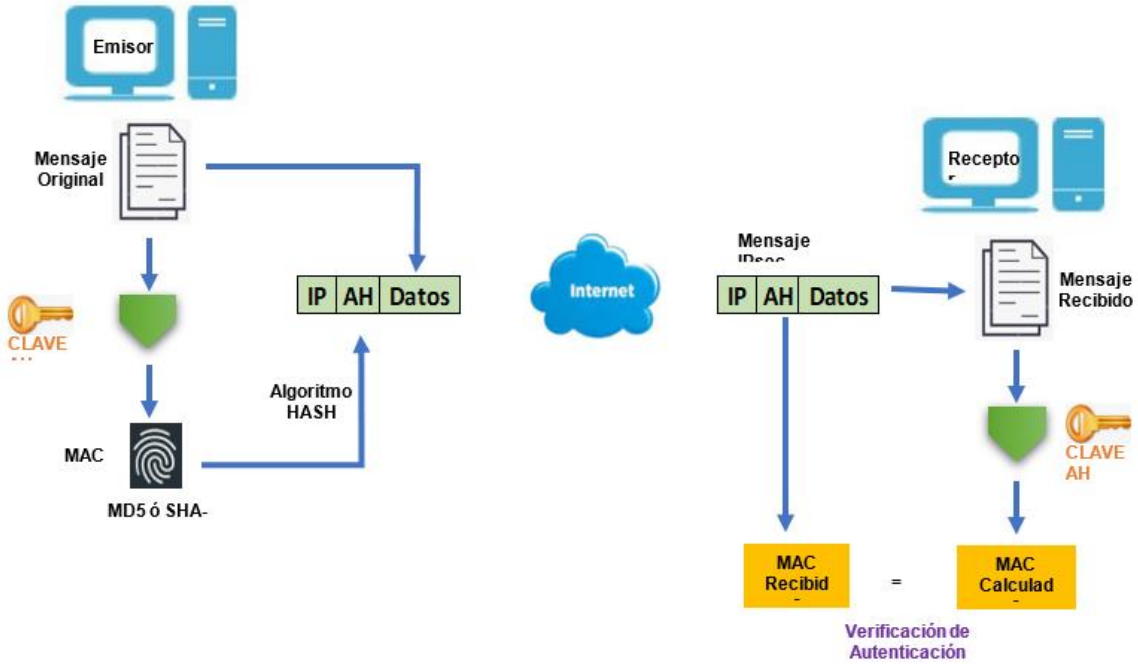
- El emisor requiere enviar un mensaje (datos)

[174] FROSALADM. Protocolo IPsec, 2014. tomado de: http://laurel.datsi.fi.upm.es/proyectos/teldatsi/

teldatsi/protocolos_de_comunicaciones/protocolo_ipsec.

- A partir del mensaje a transmitir y mediante un algoritmo de hashing como MD5 o SHA-1, con lo cual se genera un código de autenticación de mensaje o código MAC al cual se le asigna una clave, que será utilizado por el protocolo AH.
- Los algoritmos MD5 y SHA-1 utilizan una clave secreta compartida para el cálculo de los valores de autenticación. Estos algoritmos toman datos de entrada de longitud variable y crean un hash de longitud fija.
- La dirección IP + Protocolo AH + mensaje son trasportados vía internet
- Cuando el mensaje llega a su destino, aplica el proceso inverso, toma los datos del mensaje, aplica el cálculo de la MAC utilizando la clave simétrica que ya tenía y la compara con la MAC que trae la cabecera AH.
- Si las MAC coinciden significa que el mensaje (datagrama) no ha sido modificado.

Figura 30. Protocolo AH



Fuente: DELGADO, Diego Álvarez Delgado, et al. 2014. Redes Privadas Virtuales (VPN). [En línea] 28 de julio de 2014. http://profesores.elo.utfsm.cl/~agv/elo322/1s14/projects/reports/G20/Redes%20Privadas%20Virtuales%20%28VPN%29.pdf

8.10.1.2 PROTOCOLOS DE SEGURIDAD DE TRAFICO (ESP)

El protocolo de seguridad ESP "Encapsulating Security Payload"[175] proporciona confidencialidad de los datos, por lo que encripta el mensaje, es más robusto que el protocolo AH, utiliza un algoritmo de cifrado simétrico, adicionalmente puede ofrecer integridad y autenticidad de los datos empleando un mensaje similar a AH. El protocolo ESP consta de dos partes cabecera y cola, los cuales cobijan los datos transportados[176].

El funcionamiento del protocolo ESP está dado por el envío de un mensaje que será cifrado mediante una clave y la clave se envía junto al mensaje a través de la cabecera ESP, el receptor aplica el algoritmo de cifrado y recupera la información encriptada, de tal forma que proporciona confidencialidad, pasos que se pueden observar en la figura 31:

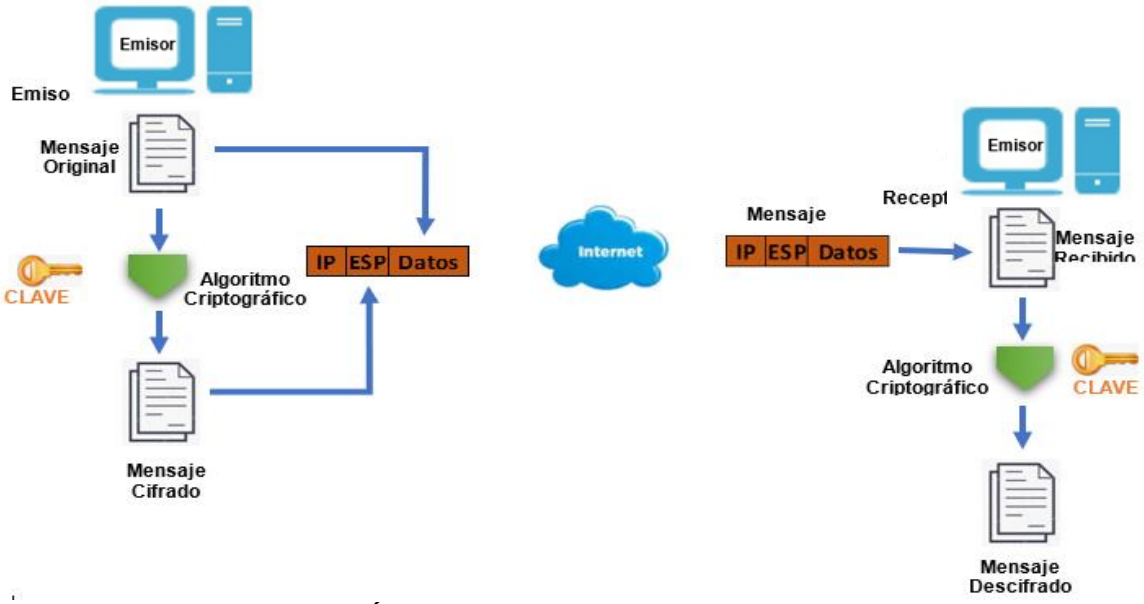
- Se tiene un mensaje
- Se aplica un algoritmo de cifrado utilizando una clave ESP
- Se generan datos cifrados que van a la cabecera ESP
- La dirección IP + Protocolo ESP + mensaje son trasportados vía internet
- Cuando el mensaje llega a su destino, aplica el proceso inverso, toma los datos del mensaje, aplica el algoritmo de cifrado mediante clave simétrica ESP.
- Si al protocolo ESP se le aplicó integridad y autenticidad se le aplica los mismos pasos que al protocolo AH.

---

[175] FROSALADM. 2014. Protocolo IPsec. [En línea] 31 de 1 de 2014. http://laurel.datsi.fi.upm.es/proyectos/teldatsi/teldatsi/protocolos_de_comunicaciones/protocolo_ipsec.

[176] REDES@ZONE. IPsec. Todo lo que debes saber. Recopilación de Artículos, 31 de marzo de 2013, tomado de: https://www.redeszone.net/ipsec-todo-lo-que-debes-saber-sobre-ipsec-recopilacion-de-articulos/.

Figura 31. Protocolo ESP



Fuente: DELGADO, Diego Álvarez Delgado, et al. 2014. Redes Privadas Virtuales (VPN). [En línea] 28 de julio de 2014. http://profesores.elo.utfsm.cl/~agv/elo322/1s14/projects/reports/G20/Redes%20Privadas%20Virtuales%20%28VPN%29.pdf

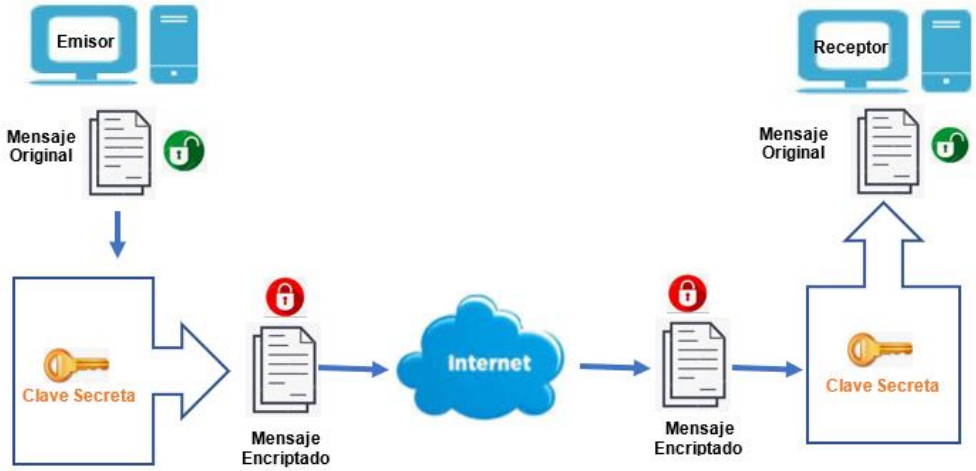
Los siguientes son los procesos de encriptación que se encuentran disponibles en ESP.

DES ("Data Encryption Standard"): Utiliza clave de 56 bits, lo cual es demasiado corta, este cifrado realiza combinaciones, sustituciones y permutaciones entre el texto a cifrar y la clave.

3DES ("Triple Data Data Encryption Standard"**)**: Realiza un triple cifrado de DES, es decir, aplica tres veces el cifrado DES con tres claves distintas, lo cual hace más seguro el mensaje, sin embargo, hace el proceso un poco más lento que el cifrado DES.

AES ("Advanced Encryption Standard"): Cifrado de bloques de datos de 128, 192 o 256 bits utilizando una clave simétrica, utilizando una matriz de 4 x 4 que cambian de valor de acuerdo a los procesos que ejecuta el algoritmo utilizando algoritmos de sustitución, permutación u operaciones polinómicas. El proceso de cifrado de un mensaje se representa en la figura 32, en la cual se visualiza los siguientes pasos:

Figura 32. Método de cifrado AES



Fuente: DELGADO, Diego Álvarez Delgado, et al. 2014. Redes Privadas Virtuales (VPN). [En línea] 28 de julio de 2014. http://profesores.elo.utfsm.cl/~agv/elo322/1s14/projects/reports/G20/Redes%20Privadas%20Virtuales%20%28VPN%29.pdf

- Se tiene un mensaje en claro que debe ser remitido desde un host origen a un host destino.
- Mediante la generación de una clave simétrica se genera una encriptación del mensaje.
- Se remite el mensaje vía internet
- Se realiza el proceso inverso en el cual una vez llegue el mensaje encriptado se utiliza la clave simétrica para la desencriptación.
- Mensaje en claro recibido por el host destino.

8.10.1.3 PROTOCOLO SEGURIDAD - IKE

El protocolo IKE “Internet Key Exchange” autoconfigura la gestión de claves, autenticación mutua, intercambio de claves, negociación de algoritmos criptográficos, es decir crea un canal de comunicación seguro entre emisor y receptor por donde se

transmite la información de tal forma que esta no puede ser leída de manera clara por un tercero no autorizado[177].

IKE es un protocolo hibrido que integra los protocolos ISAKMMP “Internet Security Association and Key Management Protocol” y OAKLEY. El protocolo criptográfico ISAKMP utiliza el protocolo IKE para el intercambio de claves criptográficas que establece procedimientos de seguridad en la red como intercambio de claves y datos de autenticación. El protocolo OAKLEY establece la forma en que se realizara el intercambio de claves de manera segura mediante algoritmos de cifrado como DES, 3DES, algoritmos Hash como MD5, SHA-1[178]

8.10.1.4 BASES DE DATOS: “SECURITY ASSOCIATION DATABASE – SAD” Y “SECURITY POLICY DATABASE – SPD”

Aunque gran parte del del procesamiento de tráfico IP se encuentra de manera local, sin embargo, existen procesos de estandarización externos con el propósito de asegurar la interoperabilidad y suministrar el proceso de seguridad en IPsec para el funcionamiento global.

Dentro del modelo de Base de Datos se pueden definir dos tipos de modelos, tales como:

- **Base de Datos de Políticas de Seguridad (SPD)**, establece las políticas que estarán presentes en el tráfico IP que entra o sale de un host, router o firewall.
  Una **Asociación de Seguridad – SA “Security Association” establece políticas de seguridad en IPsec**, en donde la base de datos SPD debe ser consultada durante todo el proceso de tráfico tanto entrante como saliente, para lo cual existen tres posibles opciones:

- Descartar: No se permite salir tráfico del host
- Desviada: No IPsec: Tráfico sin protección de IPsec.
- Procesada: Protección con IPsec: Trafico protegido por IPsec, por lo tanto, se debe especificar los servicios de seguridad según protocolos de seguridad, algoritmos a utilizar, etc.

---

[177] REDES@ZONE. IPsec : Todo lo que debes saber. Recopilación de Artículos, 31 de marzo de 2013, tomado de: https://www.redeszone.net/ipsec-todo-lo-que-debes-saber-sobre-ipsec-recopilacion-de-articulos/.

[178] FRANCISCONI, Hugo Adrian. 2005. IPsec en Ambientes IPv4 e IPv6. [En línea] http://redes-linux.com/manuales/seguridad/IPsec_IPv4_IPv6.pdf, p. 30.

Un SPD cuentan con las políticas de seguridad necesarias para establecer una comunicación y generar tráfico seguro mediante el protocolo IPsec entre dispositivos de comunicación.

- **Base de Datos de Asociaciones de Seguridad (SAD)**, En esta base de datos se almacenan los parámetros que son establecidos con cada Asociación de Seguridad SA activas[179].

  Para las interfaces en las cuales se habilita IPsec se requiere entradas y salidas de las bases de datos por separado de acuerdo a cada una de ellas, bien sea SAD o SPD, y de acuerdo a las interfaces externas de router o host puede que sea necesario tener SPD o SAD por cada una de ellas.

8.10.2 MÉTODO DE COMUNICACIÓN SEGURA MEDIANTE IPSEC (MODO DE FUNCIONAMIENTO IPSEC)

La **Asociación de Seguridad "Security Association"** es primordial para IPsec, dado que tiene dentro de sus funciones proporcionar el método para que la comunicación entre dos host se realice de manera segura, la cual está definida para una comunicación en un solo sentido (unidimensional), por lo tanto en una comunicación de ida y regreso debe existir dos SA (Security Association), es decir, una en cada sentido[180].

En la identificación de una asociación de seguridad se utiliza un Índice de Parámetros de Seguridad "Security Parameter Index" la cual es utilizada por el ISP (Proveedor de internet)[181] para saber a qué Asociación de Seguridad pertenece para poder autenticarlo y descifrarlo[182].

---

[179] FRANCISCONI, Hugo Adrian. 2005. IPsec en Ambientes IPv4 e IPv6. [En línea] http://redes-linux.com/manuales/seguridad/IPsec_IPv4_IPv6.pdf, p. 7.

[180] Ibit, p. 8.

[181] VIVES, Alvaro.. 2015. LACNIC. Curso IPv6 Básico Módulo 3: Direccionamiento y planes de numeración – Proveedores. [En línea] 5 de junio de 2015. https://www.youtube.com/watch?v=IJ7sbiJqxnM&list=PLJ3jHT8E6frAuYS73uN2QLWi8qyXRyxo1&index=17

[182] FRANCISCONI, Hugo Adrian. 2005. IPsec en Ambientes IPv4 e IPv6. [En línea] http://redes-linux.com/manuales/seguridad/IPsec_IPv4_IPv6.pdf, p. 8.

Los servicios de seguridad ofrecidos por la Asociación de Seguridad (SA) son usados por la cabecera de autenticación (AH) o carga de seguridad encapsulada (ESP) pero no por ambos. Una Asociación de Seguridad (SA) está identificada por tres partes: 1) Índice de parámetros de seguridad (SPI)[183], 2) Una dirección IP de destino y 3) Un identificador de protocolo, bien sea AH o ESP[184]. Los mecanismos están dados para para que la dirección de destino sea dirección Unicast aunque el concepto puede ser aplicado a direcciones Multicast, es decir, conexiones punto a multipunto[185].

En una Asociación de Seguridad se cuenta con la siguiente información:

Algoritmo y claves de autenticación
Algoritmo y claves de cifrado
Duración en que estarán las claves activas
Duración de la Asociación de Seguridad
Dirección IP de origen de la Asociación de Seguridad.

El protocolo IPsec cuenta con dos modos de funcionamiento el modo transporte y el modo túnel.

[183] FRANCISCONI, Hugo Adrian. 2005. IPsec en Ambientes IPv4 e IPv6. [En línea] http://redes-linux.com/manuales/seguridad/IPsec_IPv4_IPv6.pdf, p. 9.13.

[184] Ibit, p. 9.

[185] DIGITAL GIGES IONEO, Conexiones de red seguras con IPsec, tomado de: https://www.ionos.es/digitalguide/servidores/know-how/ipsec-arquitectura-de-seguridad-para-ipv4-e-ipv6/

9 CONCLUSIONES

Los avances en la tecnología y el aumento a nivel individual y organizacional conectados a internet, sumado al surgimiento de delincuencia cibernética, creo una percepción de inseguridad en los internautas por los numerosos ataque a nivel personal como institucional, situación que ha generado la necesidad de contar con mecanismos de seguridad más robustos a nivel de infraestructura y comunicación, es por ello que una de las razones para la creación de un nuevo y más potente protocolo de comunicación es el IPv6, el cual implementa mecanismos de seguridad como IPsec con aspectos como encabezados de autenticación AH y cifrado de seguridad ESP.

Tanto IPv4 como IPv6 son protocolos que inicialmente deben coexistir mientras se realiza y se configura una migración total, teniendo en cuenta que muchos de los dispositivos de comunicaciones como aplicaciones aun no soportan el protocolo IPv6, situación que ha generado demora dado que las organizaciones deberán invertir en la adquisición de nuevos equipos con características que soporten el nuevo protocolo.

La autenticación como el cifrado de datos requieren que los dos actores en una comunicación (emisor y receptor) compartan una clave, un algoritmo de cifrado y un conjunto de parámetros que hacen que se efectué una comunicación segura. Es de tener presente que estos parámetros forman parte de la seguridad y que permiten autenticidad y seguridad en IPsec.

El intercambio de llaves cumple con el protocolo KDE en el cual se establecen un canal de autenticidad y seguridad entre dos usuarios, este protocolo utiliza una infraestructura ISAKMP para el intercambio de mensajes claves y parámetros de seguridad en IPsec.
.

10 RECOMENDACIONES

Dado el gran auge que a tenido las comunicaciones vía internet y adicionalmente teniendo como prioridad aumentar la seguridad en la transmisión de datos, se creó IPv6 como sucesor de IPv4, el cual cuenta mayor direccionamiento IP, mayor fluidez y mejoras en los protocolos de seguridad mediante IPsec.

Gracias a que IPv6 cuenta con un elevado número de direcciones IP, le puede brindar a las comunicaciones la posibilidad de asignar a todos los dispositivos inteligentes una dirección única a nivel global y con todos los protocolos de seguridad, brindando así: integridad, autenticación, confidencialidad y detección de repeticiones.

Por lo anterior y teniendo en cuenta las mejoras con que cuenta el protocolo IPv6, es importante que todas las entidades tanto publicas como privadas realicen las gestiones necesarias para efectuar la transición al protocolo IPv6, obteniendo así las mejoras ya señaladas.

BIBLIOGRAFÍA

ALONSO, Juan Carlos. 2015. LACNIC. *Desarrollo de IPv6 en la región.* [En línea] 2 de junio de 2015. https://www.youtube.com/watch?v=qKJdCFFO3K0&list=PLJ3jHT8E6frAuYS73uN2QLWi8qyXRyxo1&index=5.

—. 2015. LACNIC. *Por que utilizar IPv6 hoy.* [En línea] 2 de junio de 2015. https://www.youtube.com/watch?v=5IvTIzhrvC4&list=PLJ3jHT8E6frAuYS73uN2QLWi8qyXRyxo1&index=4.

—. 2015. LACNIC. *Definición del Protocolo IPv6 – Parte 2.* [En línea] 2 de junio de 2015. https://www.youtube.com/watch?v=2zjHCe0Y66I&list=PLJ3jHT8E6frAuYS73uN2QLWi8qyXRyxo1&index=3.

—. 2015. LACNIC. *Curso introductorio de IPv6.* [En línea] 2 de junio de 2015. https://www.youtube.com/watch?v=kwvINZmmXeM&list=PLJ3jHT8E6frAuYS73uN2QLWi8qyXRyxo1&index=1.

—. 2015. LACNIC. *Definición del Protocolo IPv6 – Parte 1.* [En línea] 2 de junio de 2015. https://www.youtube.com/watch?v=cVyhDp14fac&list=PLJ3jHT8E6frAuYS73uN2QLWi8qyXRyxo1&index=2.

AMBROSIO, Paola- CIO FUNCION PUBLICA. 2017. Red de los Servicios Públicos. *Gobiernos de la región ayudan a promover el despliegue de IPv6.* [En línea] 20 de diciembre de 2017. https://www.funcionpublica.gov.co/eva/red/publicaciones/gobiernos-de-la-regi%C3%B3n-ayudan-a-promover-el-despliegue-de-ipv6.

AVILA DIAZ, Luis Miguel. 2013. Configurar IPSec. [En línea] 14 de may de 2013. https://www.youtube.com/watch?v=PuQRlRhv-BU.

BARRIO, Moises. 2018. Las direcciones IP se agotan y ahora llega el problema de IPv6. [En línea] 22 de enero de 2018. [Citado el: 2020 de abril de 25.] https://retina.elpais.com/retina/2018/01/19/innovacion/1516375772_148950.html.

BAUTISTA, Josué y CONTRERAS, Lobo y RICO, Dewar Willmer. 2011. Implementación de la seguridad del protocolo de internet. [En línea] Octubre de 2011. https://dialnet.unirioja.es/descarga/arti.

BLANCHER, M. 2010. Migration to IPV6: A practical guide to implementing IPv6 in mobile and fixeed networks.Wiley. [En línea] 2010. http://www.isaca.org/COBIT/Pages/COBIT-5-spanish.aspx.

CARABELLI, Mariano; LONGO, Lucas Y MONTENEGRO, Jose Maria. 2006. Sistemas Distribuidos “El protocolo IPv6”. [En línea] 2006. https://www.dsi.fceia.unr.edu.ar/downloads/distribuidos/material/monografias/IPV6.pdf.

DELGADO, Diego Álvarez Delgado; JORQUERA CACERES, Carolina; SEPÚLVEDA JORQUERA, GABRIEL; ZAMORA ESQUIVEL, Camila. 2014. Redes Privadas Virtuales (VPN). [En línea] 28 de julio de 2014. http://profesores.elo.utfsm.cl/~agv/elo322/1s14/projects/reports/G20/Redes%20Privadas%20Virtuales%20%28VPN%29.pdf.

DIGITAL GUIDE. 2016. Conexiones de red seguras con IPsec. [En línea] 3 de agosto de 2016. https://www.ionos.es/digitalguide/servidores/know-how/ipsec-arquitectura-de-seguridad-para-ipv4-e-ipv6/.

DINERO. 2019. Las siete tendencias tecnológicas que se moverán en el 2020. [En línea] 26 de diciembre de 2019. [Citado el: 15 de mayo de 2020.] https://www.dinero.com/tecnologia/articulo/tecnologia-2020-estas-son-las-tendencias-tecnologicas-que-se-moveran/280471.

DORDOIGNE, Jose. 2015. *Redes Informaticas - Nociones Fundamentales.* Barcelona - España : Ediciones ENI, 2015. Primera.

ESPAÑA, MINISTERIO DE ECONOMIA Y EMPRESA DE. ¿Qué es la transición a IPv6? [En línea] http://www.ipv6.gob.es/ipv6/transicion-IPv6/Paginas/que-es-transicion-IPv6.aspx.

FERNÁNDEZ ALDANA Luis Antonio. *Transmisión Y Comunicación de Datos, p. 4,5 y 6.* [En línea] http://www.ilustrados.com/documentos/transmiscomunicacaciondatos.doc.

FRANCISCONI, Hugo Adrian. 2005. *IPsec en Ambientes IPv4 e IPv6.* Carril Godoy Cruz 2801, Villa Nueva, Guaymallén : Mendoza Argentina, 2005.

—. IPsec en Ambientes IPv4 e IPv6. [En línea] http://redes-linux.com/manuales/seguridad/IPsec_IPv4_IPv6.pdf.

FROSALADM. 2014. Protocolo IPsec. [En línea] 31 de 1 de 2014. http://laurel.datsi.fi.upm.es/proyectos/teldatsi/teldatsi/protocolos_de_comunicaciones/protocolo_ipsec.

FUENTES, Raul. IPv4 - Encabezado y estructura. [En línea] https://rfuentess.blogspot.com/2012/01/ipv4-encabezado-y-estructura.html.

FUSARIO, Ruben Jorge . 2017. Vulnerabilidades enla seguridad delas transacciones interactivas de comercioelectronico a traves de la web. [En línea] 25 de octubre de 2017. http://bibliotecadigital.econ.uba.ar/download/tesis/1501-1279_FusarioRJ.pdf.

GOOGLE. Adopción de IPv6. [En línea] https://www.google.com/intl/es/ipv6/statistics.html#tab=ipv6-adoption.

HOGG, Scott and VYNCKE Eric . 2009. IPv6 Security. [En línea] 2009. https://books.google.es/books?hl=es&lr=&id=kwOv0Aw2lIUC&oi=fnd&pg=PT26&dq=ipv6+ipsec+and+vpns&ots=Qnl27HBWYg&sig=aKqVWpudX6guT_QebX6LRG5xgi8#v=onepage&q=ipv6%20ipsec%20and%20vpns&f=false.

IANA INTERNET ASSIGNED NUMBERS AUTHORY;. Number Resources. [En línea] https://www.iana.org/numbers.

IANA.ORG. 2020. Internet Protocol Version 6 (IPv6) Parameters. [En línea] 11 de 08 de 2020. https://www.iana.org/assignments/ipv6-parameters/ipv6-parameters.xhtml.

—. 2019. IPv6 Global Unicast Address Assignments. [En línea] 13 de marzo de 2019. https://www.iana.org/assignments/ipv6-unicast-address-assignments/ipv6-unicast-address-assignments.xhtml.

ICONTEC. Norma ISO 27001. [En línea] http://intranet.bogotaturismo.gov.co/sites/intranet.bogotaturismo.gov.co/files/file/Norma.%20NTC-ISO-IEC%2027001.pdf.

INFORMATION SCIENCES INSTITUTE UNIVERSITY OF SOUTHERN CALIFORNIA. 1981. RFC: 791 - Especificacion del Protocolo. [En línea] septiembre de 1981. https://www.rfc-es.org/rfc/rfc0791-es.txt.

INTERNET ENGINEERING TASK FORCE (IETF) D. WING. 2012. RFC6555 - Happy Eyeballs: Success with Dual-Stack Hosts. [En línea] abril de 2012. https://www.ietf.org/rfc/rfc6555.txt.

INTERNET ENGINEERING TASK FORCE (IETF) I. GASHINSKY. 2012. RFC6583 - Operational Neighbor Discovery Problems. [En línea] marzo de 2012. https://www.ietf.org/rfc/rfc6583.txt.

INTERNET ENGINEERING TASK FORCE (IETF) S. KAWAMURA. 2010. RFC5952 - A Recommendation for IPv6 Address Text Representation. [En línea] agosto de 2010. https://www.ietf.org/rfc/rfc5952.txt.

IPV6 GO. 2012. Cual es mi IPv6? [En línea] 2012. http://www.ipv6go.net/cabecera_ipv6.php.

JASON G, Andres. 2005. IPv6: the nextInternet protocol. [En línea] 2005. https://static.usenix.org/publications/login/2005-04/pdfs/andress0504.pdf.

JJTORRES. 2014. ¿Qué es y cómo funciona el Internet de las cosas? [En línea] 20 de octubre de 2014. https://hipertextual.com/archivo/2014/10/internet-cosas/.

LACNIC. Capacitación-LACNIC - HD MODULO-2 Video-f Tuneles v01. [En línea] https://www.youtube.com/watch?v=sE3rPzhiswM&list=PLJ3jHT8E6frAuYS73uN2QLWi8qyXR yxo1&index=11.

—. Curso IPv6 Básico, tomado de: . [En línea] https://www.youtube.com/watch?v=-HIUT2ilCyU&list=PLsQToyLJISPWSMPF2DSbFmw_2HtzNpCSj& index=7.

—. Estadísticas de Asignación de LACNIC. [En línea] https://www.lacnic.net/web/lacnic/estadisticas-asignacion.

—. Fases de Agotamiento de IPv4. [En línea] https://www.lacnic.net/1001/1/lacnic/fases-de-agotamiento-de-ipv4.

—. 2015. HD MODULO-2 Video-f Tuneles v01. [En línea] 5 de junio de 2015. https://www.youtube.com/watch?v=sE3rPzhiswM&list=PLJ3jHT8E6frAuYS73uN2QLWi8qyXRyxo1&index=11.

—. 2002. Lacnic. [En línea] 2002. https://www.lacnic.net/966/1/lacnic/acerca-de-lacnic.

MEDINA CASTILLO, Carlos A. y FORERO RODRIGUEZ, Felipe. 2011. Caracterización de IPv6. [En línea] 14 de noviembre de 2011. https://dialnet.unirioja.es/descarga/articulo/4239524.pdf.

MEGS. 2019. Estructura de un paquete IPv6. [En línea] 2019. http://dmrodriguez.50megs.com/IPV6/IPV6_7.html.

MINTIC. Guía de Transición de IPv4 a IPV6 PARA Colombia. [En línea] https://www.mintic.gov.co/gestionti/615/articles-5482_G20_Transicion_IPv4_IPv6.pdf.

—. 2019. Protocolos de Internet Version 6. [En línea] 14 de febrero de 2019. https://www.mintic.gov.co/portal/604/w3-article-5938.html.

MOLINA GARCÍA, Jorge Alberto. La Importancia de la Gestión de Riesgos y Seguridad en el Internet de las Cosas (IOT). *Universidad Piloto de Colombia Bogotá, Colombia.* [En línea] http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277.

NETWORK WORKING GROUP R. GILLIGAN. 2000. RFC 2893 - Transition Mechanisms for IPv6 Hosts and Routers. [En línea] agosto de 2000. https://www.ietf.org/rfc/rfc2893.txt.

NETWORK WORKING GROUP A. CONTA. 1998. RFC2463 Protocolo de Mensajes de Control de Internet para IPv6 (ICMPv6). [En línea] diciembre de 1998. https://www.ietf.org/rfc/rfc2463.txt.

NETWORK WORKING GROUP B. CARPENTER. 2001. RFC 3056 -Connection of IPv6 Domains via IPv4 Clouds. [En línea] febrero de 2001. https://www.ietf.org/rfc/rfc3056.txt.

—. 1999. RFC2529 - Transmisión de IPv6 sobre Dominios IPv4 sin Túneles Explícitos. [En línea] marzo de 1999. https://www.ietf.org/rfc/rfc2529.txt.

NETWORK WORKING GROUP B. HABERMAN. 2002. RFC3306 - Unicast-Prefix-based IPv6 Multicast Addresses. [En línea] agosto de 2002. https://www.ietf.org/rfc/rfc3306.txt.

NETWORK WORKING GROUP C. AOUN. 2007. RFC4966 - Reasons to Move the Network Address Translator - Protocol Translator(NAT-PT) to Historic Status. [En línea] julio de 2007. https://www.ietf.org/rfc/rfc4966.txt.

NETWORK WORKING GROUP C. HUITEMA. 2004. RFC3879 - Deprecating Site Local Addresses. [En línea] septiembre de 2004. https://www.ietf.org/rfc/rfc3879.txt.

NETWORK WORKING GROUP. 1998. Especificación Protocolo Internet, Versión 6 (IPv6). [En línea] diciembre de 1998. https://www.rfc-es.org/rfc/rfc2460-es.txt.

NETWORK WORKING GROUP G. CAMARILLO. 2004. RFC3959 - The Early Session Disposition Type for the Session Initiation Protocol (SIP). [En línea] diciembre de 2004. https://www.ietf.org/rfc/rfc3959.txt.

NETWORK WORKING GROUP J. ARKKO, ED. 2005. RFC3971 - SEcure Neighbor Discovery (SEND). [En línea] marzo de 2005. https://www.ietf.org/rfc/rfc3971.txt.

NETWORK WORKING GROUP P. ALMQUIST. 1992. RFC 1349 - Type of Service in the Internet Protocol Suite. [En línea] julio de 1992. https://www.ietf.org/rfc/rfc1349.txt.

NETWORK WORKING GROUP P. MARQUES. 1999. RFC2545 Uso de las Extensiones Multiprotocolo de BGP-4 para Routing entre dominios para IPv6. [En línea] marzo de 1999. https://www.ietf.org/rfc/rfc2545.txt.

NETWORK WORKING GROUP P. NIKANDER, ED. 2004. RFC3756 - IPv6 Neighbor Discovery (ND) Trust Models and Threats. [En línea] mayo de 2004. https://www.ietf.org/rfc/rfc3756.txt.

NETWORK WORKING GROUP R. DROMS, ED. 2003. RFC 3315 - Dynamic Host Configuration Protocol for IPv6 (DHCPv6). [En línea] julio de 2003. https://www.ietf.org/rfc/rfc3315.txt.

NETWORK WORKING GROUP R. HINDEN. 1998. RFC 2373 - Arquitectura de Direccionamiento en IPv6. [En línea] julio de 1998. https://www.ietf.org/rfc/rfc2373.txt.

—. 2005. RFC 4193 - Unique Local IPv6 Unicast Addresses. [En línea] octubre de 2005. https://www.ietf.org/rfc/rfc4193.txt.

—. 2006. RFC4291 - IP Version 6 Addressing Architecture. [En línea] febrero de 2006. https://www.ietf.org/rfc/rfc4291.txt.

NETWORK WORKING GROUP S. DEERING. 1998. RFC 2460 - Internet Protocol, Version 6 (IPv6). [En línea] diciembre de 1998. https://www.rfc-es.org/rfc/rfc2460-es.txt.

NETWORK WORKING GROUP S. KENT. 2005. RFC 4301 – Security Architecture for the Internet Protocol. [En línea] diciembre de 2005. https://www.ietf.org/rfc/rfc4301.txt.

—. 2005. RFC 4301 - Security Architecture for the Internet Protocol,. [En línea] diciembre de 2005. https://www.ietf.org/rfc/rfc4301.txt.

NETWORK WORKING GROUP T. NARTEN. 2007. RFC4861 - Neighbor Discovery for IP version 6 (IPv6). [En línea] septiembre de 2007. https://www.ietf.org/rfc/rfc4861.txt.

NETWORK WORKING GROUP V. FULLER. 2006. RFC 4632 - Classless Inter-domain Routing (CIDR): The Internet Address Assignment and Aggregation Plan. [En línea] agosto de 2006. https://www.ietf.org/rfc/rfc4632.txt.

NETWORK WORKING GROUP Y. REKHTER. 1996. RFC 1918 - Address Allocation for Private Internets. [En línea] febrero de 1996. https://www.ietf.org/rfc/rfc1918.txt.

NETWORK WORKING WORKING GROUP. 1900. RFC 1195 - Use of OSI IS-IS for Routing in TCP/IP and Dual Environments. [En línea] diciembre de 1900. https://www.ietf.org/rfc/rfc1195.txt.

NIC ARGENTINA. 2017. Arpanet: El Origen de internet. [En línea] diciembre de 2017. https://nic.ar/es/enterate/novedades/arpanet-el-origen-de-internet.

RED HAT INC. 2003. Establecimiento de una conexión IPsec. [En línea] 2003. http://web.mit.edu/rhel-doc/3/rhel-sag-es-3/s1-network-config-ipsec.html.

RICO BAUTISTA, Dewar Willmer y MEDINA CÁRDENAS, Yurley Constanza y SANTOS JAIME, Luz Marina. 2008. IPSec DE IPv6 EN LA UNIVERSIDAD DE PAMPLONA. [En línea] septiembre de 2008. https://www.redalyc.org/html/849/84920503057/.

RICO BAUTISTA, Dewar Willmer y MEDINA CÁRDENAS, Yurley Constanza y SANTOS JAIMES, Luz Mari. 2008. IPSec DE IPv6 EN LA UNIVERSIDAD DE PAMPLONA. *Universidad Tecnológica de PereiraColombia.* [En línea] 2008. https://www.redalyc.org/pdf/849/84920503057.pdf.

RISTI. 2018. Granja inteligente: Definición de infraestructura basada en internet de las cosas, IpV6 y redes definidas por software. [En línea] 2018. https://www.researchgate.net/profile/Dewar_Rico-Bautista/publication/331178386_Smart_farm_Defining_of_infrastructure_based_on_internet_of_things_IpV6_and_software_defined_networks/links/5d09acf8299bf1f539cf062c/Smart-farm-Defining-of-infrastructure-based-.

ROBLEDANO, Ángel. 2019. OpenWebinars. *Qué es TCP/IP.* [En línea] 18 de junio de 2019. https://openwebinars.net/blog/que-es-tcpip/.

SANCHEZ, Julio. 2011. Ejemplo de Uso de SSH Secure Shell. [En línea] 10 de enero de 2011. https://www.youtube.com/watch?v=qI9DZmRKgHQ.

SCOTT, Hogg y VYNCKE, Eric. 2009. *Information Assurance for the next-generation Internet Protocol.* USA : CISCO SYSTEM INC, 2009.

SERGIO DE, Luz. 2013. REDES@ZONE. *IPsec : Todo lo que debes saber. Recopilación de Artículos.* [En línea] 31 de marzo de 2013. https://www.redeszone.net/ipsec-todo-lo-que-debes-saber-sobre-ipsec-recopilacion-de-articulos/.

SPEED CHECK. IPv4. [En línea] https://www.speedcheck.org/es/wiki/ipv4/.

STALLINGS, William. 2004. *Fundamentos de Seguridad en Redes Aplicaciones y Estandares,.* Madrid : Person Preatice Hall,, 2004. Segunda edición.

TELEMATIQUE. 2003. Revista electronica de Estudios Telematicos. *IP Versión 6: La Nueva Generación IP.* [En línea] 2003. https://dialnet.unirioja.es/descarga/articulo/2968291.pdf.

TICO, Raquel Perez. Comparativa OSI frente TCP/IP. [En línea] https://sites.google.com/site/raquelpereztico/trasmision-de-datos-en-las-redes/0-6-comparativa-osi-frente-tcp-ip.

TUTORIALSPOINT. 2016. IPv6 Tutorial. [En línea] 2016. https://www.tutorialspoint.com/es/ipv6/ipv6_ipv4_to_ipv6.htm.

UPM, GRUPO DE SISTEMAS OPERATIVOS DATSI FI. 2012. Protocolo IPsec. [En línea] 8 de octubre de 2012. http://laurel.datsi.fi.upm.es/proyectos/teldatsi/teldatsi/protocolos_de_comunicaciones/protocolo_ipsec.

VEATO, Valentin. 2015. ICMP en IPv6. *Redes Locales y Globales.* [En línea] 2015. https://sites.google.com/site/redeslocalesyglobales/6-arquitecturas-de-redes/6-arquitectura-tcp-ip/7-nivel-de-red/8-direccionamiento-ipv6/7-icmp-en-ipv6.

VELEZ VARELA, Fernando y GUTIERREZ RANCRUEL, Liliana. 2019. IPv6, una realidad. Bogotá - Colombia : Ediciones de la U, 2019, pág. 205.

VIVES, Alvaro. 2015. LACNIC. *Curso IPv6 Básico Módulo 4: Autoconfiguración – Conclusiones.* [En línea] 5 de junio de 2015. https://www.youtube.com/watch?v=K3w_Gl3VCgI&list=PLJ3jHT8E6frAuYS73uN2QLWi8qyXRyxo1&index=22.

—. 2015. LACNIC. *Curso IPv6 Básico Módulo 3: Direccionamiento y planes de numeración – Caracteristicas Generales de Direccionamiento IPv6.* [En línea] 5 de junio de 2015. https://www.youtube.com/watch?v=qxVUOL9prHk&list=PLJ3jHT8E6frAuYS73uN2QLWi8qyXRyxo1&index=15.

—. 2015. LACNIC. *Curso IPv6 Básico Módulo 3: Direccionamiento y planes de numeración – El cabezal de IPv6.* [En línea] 5 de junio de 2015. https://www.youtube.com/watch?v=qoJkahpB5do&list=PLJ3jHT8E6frAuYS73uN2QLWi8qyXRyxo1&index=14.

—. 2015. LACNIC. *Curso IPv6 Básico Módulo 2: Agotamiento espacio IPV4, coexistencia y transición – Recomendaciones.* [En línea] 5 de junio de 2015. https://www.youtube.com/watch?v=md80CcXGjY8&list=PLJ3jHT8E6frAuYS73uN2QLWi8qyXRyxo1&index=13.

—. 2015. LACNIC. *Curso IPv6 Básico Módulo 2: Agotamiento espacio IPV4, coexistencia y transición – Traducción.* [En línea] 5 de junio de 2015. https://www.youtube.com/watch?v=gTLK6uyLPCc&list=PLJ3jHT8E6frAuYS73uN2QLWi8qyXRyxo1&index=12.

—. 2015. LACNIC. *Curso IPv6 Básico Módulo 2: Agotamiento espacio IPV4, coexistencia y transición – Doble Pila.* [En línea] 5 de junio de 2015. https://www.youtube.com/watch?v=C_ekmx7v9m0&list=PLJ3jHT8E6frAuYS73uN2QLWi8qyXRyxo1&index=10.

—. 2015. LACNIC. *Curso IPv6 Básico Módulo 2: Agotamiento espacio IPV4, coexistencia y transición – Mecanismos de Transición.* [En línea] 5 de junio de 2015. https://www.youtube.com/watch?v=LQQD7-8E4c8&list=PLJ3jHT8E6frAuYS73uN2QLWi8qyXRyxo1&index=9.

—. 2015. LACNIC. *Curso IPv6 Básico Módulo 2: Agotamiento espacio IPV4, coexistencia y transición - Espacio IPv6 disponible.* [En línea] 5 de junio de 2015. https://www.youtube.com/watch?v=iItLZ8IUorI&list=PLJ3jHT8E6frAuYS73uN2QLWi8qyXRyxo1&index=8.

—. 2015. LACNIC. *Curso IPv6 Básico Módulo 2: Agotamiento espacio IPV4, coexistencia y transición – Túneles.* [En línea] 5 de junio de 2015. https://www.youtube.com/watch?v=sE3rPzhiswM&list=PLJ3jHT8E6frAuYS73uN2QLWi8qyXRyxo1&index=11.

—. 2015. LACNIC. *Curso IPv6 Básico Módulo 4: Autoconfiguración – Stateless.* [En línea] 5 de junio de 2015. https://www.youtube.com/watch?v=D86t7ZITU2A&list=PLJ3jHT8E6frAuYS73uN2QLWi8qyXRyxo1&index=20.

—. 2015. LACNIC. *Curso IPv6 Básico Módulo 2: Agotamiento espacio IPV4, coexistencia y transición - Proyecciones de Agotamiento.* [En línea] 5 de junio de 2015. https://www.youtube.com/watch?v=-HIUT2ilCyU&list=PLJ3jHT8E6frAuYS73uN2QLWi8qyXRyxo1&index=6.

—. 2015. LACNIC. *Curso IPv6 Básico Módulo 2: Agotamiento espacio IPV4, coexistencia y transición - Espacio IPv4 disponible.* [En línea] 5 de junio de 2015. https://www.youtube.com/watch?v=XqHPrtiE2_I&list=PLJ3jHT8E6frAuYS73uN2QLWi8qyXRyxo1&index=7.

—. 2015. LACNIC. *Curso IPv6 Básico Módulo 3: Direccionamiento y planes de numeración – Distribución y asignación de recursos.* [En línea] 5 de junio de 2015. https://www.youtube.com/watch?v=sioBvZ7ciQE&list=PLJ3jHT8E6frAuYS73uN2QLWi8qyXRyxo1&index=16.

—. 2015. LACNIC. *Curso IPv6 Básico Módulo 3: Direccionamiento y planes de numeración – Proveedores.* [En línea] 5 de junio de 2015. https://www.youtube.com/watch?v=IJ7sbiJqxnM&list=PLJ3jHT8E6frAuYS73uN2QLWi8qyXRyxo1&index=17.

—. 2015. LACNIC. *Curso IPv6 Básico Módulo 4: Autoconfiguración – Stateful (DHCPv6).* [En línea] 5 de junio de 2015. https://www.youtube.com/watch?v=Eiy4gHNxjaw&list=PLJ3jHT8E6frAuYS73uN2QLWi8qyXRyxo1&index=21.

—. 2015. LACNIC. *Curso IPv6 Básico Módulo 4: Autoconfiguración – Protocolos asociados (Path MTU Discovery, NDP).* [En línea] 5 de junio de 2015. https://www.youtube.com/watch?v=Chzbg-il2z8&list=PLJ3jHT8E6frAuYS73uN2QLWi8qyXRyxo1&index=19.

—. 2015. LACNIC. *Curso IPv6 Básico Módulo 3: Direccionamiento y planes de numeración – Planes de Numeración.* [En línea] 5 de junio de 2015. https://www.youtube.com/watch?v=xKFHp_tWOEM&list=PLJ3jHT8E6frAuYS73uN2QLWi8qyXRyxo1&index=18.

WORLD IPV6 LAUNCH. IPv6 Is The New Normal. [En línea] https://www.worldipv6launch.org/author/danyork/.

ZAPATA VALDES, Rodrigo Horacio. 2013. Análisis de Seguridad en el Protocolo IPv6. [En línea] 2013. http://157.92.136.59/download/tpos/1502-0820_ZapataValdezRH.pdf.

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
METODOLOGÍA DEL TRABAJO ACADÉMICO

RESUMEN ANALÍTICO DE ESCRITOS

PAÍS O REGIÓN:	Colombia	NÚMERO:	
TÍTULO:	Protocolo de Seguridad Orientado a IPv6 - IPsec		
TRADUCCIÓN:	Protocolo de Seguridad Orientado a IPv6 - IPsec		
AUTOR:	Ricardo Alfonso Paramo Melo		
PUBLICACIÓN:	Repositorio Institucional UNAD		
UNIDAD:	Universidad Nacional Abierta y a Distancia		
PALABRAS CLAVES:	Cabecera IP, Direccionamiento IP, Direccionamiento IPv6, Datagrama, DHCP, Disponibilidad, EGP, Encapsulamiento, Esp, ICMP, IGP,IKE, Integridad, Protocolo AH, Protocolo ESP, IPng, Protocolo IPv4, Protocolo IPv6, Protocolo IPsec, Lacnic, NAT, NAT64 / DNS64, RFC, TCP, Túnel, Túneles punto a punto, Túneles multipunto		

DESCRIPCIÓN:

Debido al aumento de la tecnología a nivel mundial , muchos de los equipos tecnológicos que se han venido desarrollando y produciendo requieren un direccionamiento IP como medio de comunicación, lo cual genera un gran problema , teniendo en cuenta que desde hace ya varios años, el organismo LACNIC destinado a la asignación de direccionamiento IP tanto en América Latina como a la región del Caribe, dio a conocer sobre el agotamiento del direccionamiento IPV4, por lo cual se debía adoptar el direccionamiento IPV6, el cual cuenta con mayor direccionamiento y corrección de falencias en su estructura, sumado a esto, IPv6 cuenta con mayor nivel de seguridad de extremo a extremo en una comunicación a través de los canales de internet .

Teniendo en cuenta el auge tecnológico a nivel mundial y el surgimiento del internet de las cosas, gran parte de los nuevos aparatos tecnológicos requieren direccionamiento IP, situación que ha retrasado en cierta medida el avance tecnológico, ya que no se cuenta con la cantidad necesaria de direccionamiento para que dichos aparatos se puedan comunicar a través de las redes, adicionalmente, es importante recalcar la seguridad que debe contener cada uno de éstos equipos tecnológicos al ser conectados a las redes de comunicaciones, teniendo en cuenta que afecta la seguridad y privacidad de los usuarios finales, mediante equipos como: cámaras, sensores, televisores, neveras, etc.

Con el protocolo IPV6 viene una nueva solución de seguridad llamada IPsec la cual es importante conocer a detalle dado que actualmente es una necesidad de conocimiento para cualquier organización ya sea pública o privada, teniendo en cuenta que se quiera o no, se debe realizar un despliegue de manera masiva a

nivel mundial.

El desconocimiento de la infraestructura del protocolo IPv6 y su correspondiente protocolo de seguridad IPsec, podría causar en cierta medida a una organización tomar decisiones a la ligera y poco favorable a nivel estructura física y seguridad información.

IPsec es una parte esencial de IPv6 dado que implementa cifrado, autenticación y redes privadas VPN desde extremo a extremo, utilizando extensiones de encabezado ESP el cual proporciona confidencialidad en el flujo de tráfico, autenticación de las fuentes y protección contra ataques de repetición.

A nivel tecnológico se realizan anualmente gran cantidad de reuniones presenciales, conferencias vía web y charlas entre otras actividades, las cuales van dirigidas a dar a conocer la problemática en cuanto al agotamiento de direccionamiento IP y ventajas de implementación del nuevo protocolo de IPv6, las cuales requieren un conocimiento previo para lograr entender de manera teórica las comunicaciones seguras mediante IPsec de IPv6.

FUENTES:

106 Fuentes Bibliográficas

CONTENIDOS:

Con la necesidad de expansión que tiene internet y la declaratoria de agotamiento del direccionamiento IPv4 por parte de IANA, entidad dedicada a supervisar la asignación global de direcciones IP, surgió en 1998 el nuevo protocolo de comunicaciones denominado IPV6 el cual reemplazaría a IPv4 gracias a que cuenta con un direccionamiento de 128 bits en comparación con los 32 bits de la versión anterior, cubriendo las necesidades de direccionamiento IP y con ella viene una solución de seguridad muy potente denominada IPsec.

El protocolo IPsec integrada en IPv6 características de seguridad como: encabezados de autenticación AH, autenticación de origen de los datos, cifrado de seguridad ESP y utilización de VPN o túneles.

Es de precisar que para una entidad, la realización de la transición de IPv4 a IPv6 debe realizarse de manera gradual y con anterioridad efectuar un estudio en donde se contemple infraestructura existente, software utilizado y la red de internet brindada por el ISP, todo este conjunto de variables debe estar alineado y configurado para que mediante la ayuda de ambientes de transición como dual-stack se permita la comunicación de paquetes tanto de IPv4 como IPv6 de tal forma que no exista traumatismo y sea transparente para los usuarios que utilizan

la red.

METODOLOGÍAS:

El documento presenta una metodología de investigación llevada a una monografía

CONCLUSIONES:

Los avances en la tecnología y el aumento a nivel individual y organizacional conectados a internet, sumado al surgimiento de delincuencia cibernética, creo una percepción de inseguridad en los internautas por los numerosos ataque a nivel personal como institucional, situación que ha generado la necesidad de contar con mecanismos de seguridad más robustos a nivel de infraestructura y comunicación, es por ello que una de las razones para la creación de un nuevo y más potente protocolo de comunicación es el IPv6, el cual implementa mecanismos de seguridad como IPsec con aspectos como encabezados de autenticación AH y cifrado de seguridad ESP.

Tanto IPv4 como IPv6 son protocolos que inicialmente deben coexistir mientras se realiza y se configura una migración total, teniendo en cuenta que muchos de los dispositivos de comunicaciones como aplicaciones aun no soportan el protocolo IPv6, situación que ha generado demora dado que las organizaciones deberán invertir en la adquisición de nuevos equipos con características que soporten el nuevo protocolo.

La autenticación como el cifrado de datos requieren que los dos actores en una comunicación (emisor y receptor) compartan una clave, un algoritmo de cifrado y un conjunto de parámetros que hacen que se efectué una comunicación segura. Es de tener presente que estos parámetros forman parte de la seguridad y que permiten autenticidad y seguridad en IPsec.

El intercambio de llaves cumple con el protocolo KDE en el cual se establecen un canal de autenticidad y seguridad entre dos usuarios, este protocolo utiliza una infraestructura ISAKMP para el intercambio de mensajes claves y parámetros de seguridad en IPsec.