CONSIDERACIONES PARA LAS BUENAS PRÁCTICAS DE SEGURIDAD DEL PROTOCOLO IPV6 EN REDES DE ÁREA LOCAL CORPORATIVAS

OLGA LUCIA MORALES NOVA

CAMILO ERNESTO LOSADA BURBANO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD

ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA

ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA

BOGOTÁ, 2018

CONSIDERACIONES PARA LAS BUENAS PRÁCTICAS DE SEGURIDAD DEL PROTOCOLO IPV6 EN REDES DE ÁREA LOCAL CORPORATIVAS

Olga Lucia Morales Nova
Camilo Ernesto Losada Burbano

Asesor:

MARIANO ESTEBAN ROMERO TORRES

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD

ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA

ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA

BOGOTÁ, D.C., 2018

Nota de aceptación:

Firma del presidente del jurado

Firma del presidente del jurado

Firma del presidente del jurado

Bogotá D.C., Fecha (día, mes, año)

A nuestras hijas Ana Sofía y Laura Juliana. Con todo nuestro amor, siempre están en nuestros corazones y son nuestra razón de crecimiento permanente

AGRADECIMIENTOS

A nuestros padres por su apoyo incondicional y ejemplo de superación. A Helena, Roberto, Gladys y Maximino nuestro profundo respeto y finalmente a esta casa la Universidad Nacional Abierta y a Distancia que nos abrió las posibilidades de crecimiento espiritual, humano y profesional.

TABLA DE CONTENIDO

Pág.

LISTA DE TABLAS

LISTA DE FIGURAS

INTRODUCCIÓN

Con el agotamiento de direcciones IPv4 la entidad encargada de su desarrollo la IETF[1] definió una serie de estándares que se conformaron en el protocolo de red IPv6 que actualmente se está desplegando a nivel mundial. Dicha suite de protocolos no solo aumenta el rango de direccionamiento para los nuevos equipos que se conectan a las redes, sino que a su vez determinan nuevas forman como dispositivos y aplicaciones envían e interactúan en la red.

El nuevo protocolo IPv6 ha desencadenado la necesidad de implementar de la mejor manera dicho estándar lo que según nuestra experiencia y corroborado por la IPv6 Forum significa en buena medida el conocimiento a profundidad del protocolo IPv6 y el desarrollo de buenas prácticas con la finalidad de contar con redes corporativas lo más seguras posibles. Consientes de ello buscamos desarrollar una guía de buenas prácticas que faciliten la adopción e implementación segura del nuevo estándar.

IPv6 fue diseñado para resolver algunos problemas del protocolo de comunicación de redes de computadores IPv4, como: Permitir la comunicación extremo a extremo, proveer de un gran número de direcciones IP, resolver los problemas de seguridad detectados en IPv4 y permitir la prestación de nuevos servicios como: la autoconfiguración y la movilidad y la conexión de dispositivos diversos (Internet Cosas) en los nuevos estándares de las comunicaciones (IPv6, DNSSEC e IPSec).Debido a esta situación el mundo tendrá un tiempo de transición entre los dos protocolos y se espera que los dispositivos y direcciones IPv4 coexistan durante un buen tiempo con los dispositivos y direcciones IPv6 a través de los mecanismos de transición contemplados por el protocolo IPv6, pues hay dispositivos y aplicaciones que no son compatibles con las dos pilas.

Con el advenimiento de esta nueva tecnología se presentan varios retos como la necesidad de contar con recurso humano capacitado en el nuevo protocolo, formular, desarrollar e implementar buenas prácticas de seguridad en el protocolo para que sea fiable y se acelere su proceso de adopción y garantizar mecanismos de transición que permitan la coexistencia de las dos pilas. Con este trabajo de grado se busca apoyar estas necesidades pues plantea objetivos concretos como plantear un marco teórico robusto que permita al lector empaparse de todos los aspectos relevantes e innovadores del protocolo IPv6, Presentar un documento de ataques y principales vulnerabilidades descubiertos en el protocolo IPv6 y

[1] IETF es una organización no gubernamental que interviene en la formulación y toma de decisiones sobre la infraestructura de la red y sus protocolos.

presentar una Guía de Buenas prácticas de seguridad a tener en cuenta para contar con una implementación segura del protocolo sobre una red LAN corporativa.

1. EL PROBLEMA DE INVESTIGACIÓN

1.1 Descripción del problema

Las direcciones asignadas para el protocolo IPv4 ya fueron agotadas y las entidades que administran dicho recurso como el IETF y la IANA han definido el estándar IPv6 como su reemplazo. La implementación de dicho protocolo desencadeno en no solo nuevos retos en materia de infraestructura, sino que a su vez la necesidad de implementarlos de manera segura, con las prácticas más adecuadas. Las entidades gubernamentales y grandes corporaciones ya han comenzado la migración de sus aplicaciones e infraestructuras. Por ello las empresas requieren no solo un método donde se implemente el protocolo IPv6, sino que genere una dinámica de seguridad en dicha transición implementación.

De igual manera el IETF aprovechó estos cambios que implicaba el desarrollo de un nuevo protocolo e incorporó en los nuevos trabajos prácticas para solucionar problemas en materia de velocidad, cobertura y seguridad en las redes. Esto a su vez ha generado un marco conceptual distinto a cómo se implementas las nuevas redes en el marco de IPv6.

Los cambios han implicado que las entidades que coadministran el desarrollo de internet hayan instado a gobiernos a que generen un marco legal para su implementación y promuevan su uso. A su vez las empresas desarrolladoras de hardware y software ya se han puesto a la tarea y han sacado nuevos equipos que por defecto traen implementaciones de IPv6 o por lo menos parches para que sean compatibles en algún grado con la nueva tecnología.

Dentro del desarrollo de este trabajo de grado buscamos apoyar implementaciones de IPv6 con prácticas seguras en entornos corporativos; ya que las implementaciones y metodologías del protocolo IPv6 están enfocadas fundamentalmente a la puesta en marcha del protocolo teniendo consideraciones limitadas en materia de seguridad.

1.2 Formulación del problema

A partir de la descripción anterior nace la siguiente interrogante:
¿Cómo proponer consideraciones para las buenas prácticas de seguridad del protocolo IPv6 en redes de área local corporativas?

1.3 OBJETIVOS

1.3.1 Objetivo General

Proponer consideraciones para las buenas prácticas de seguridad del protocolo IPv6 en redes de área local corporativas.

1.3.2 Objetivos Específicos

Conocer la estructura y configuración del protocolo IPv6 en redes corporativas de área local.

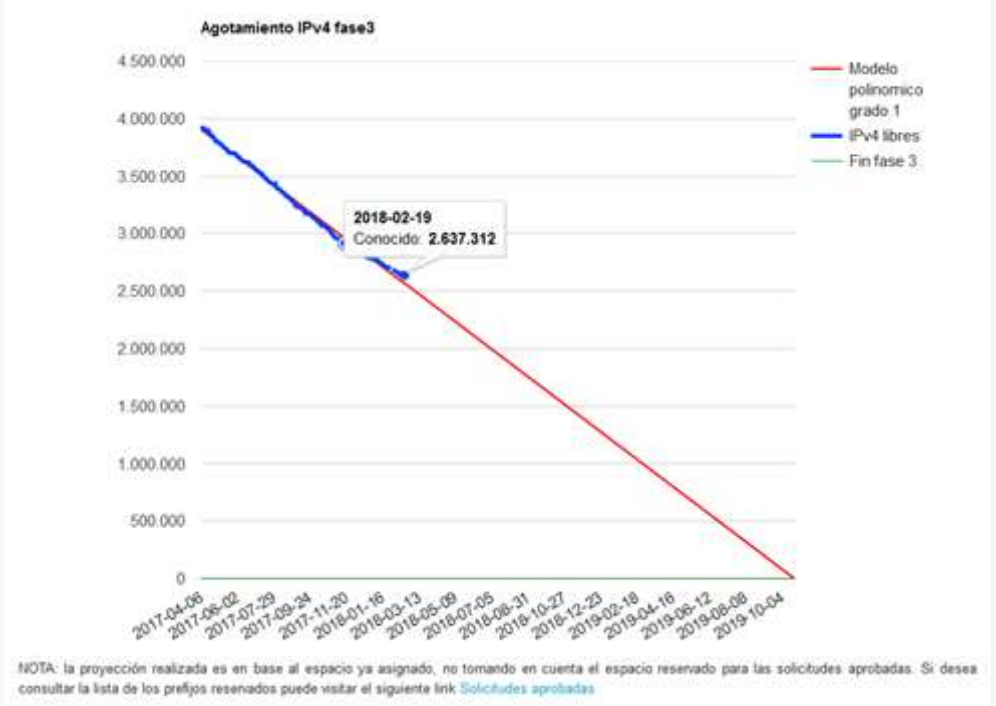
Identificar las principales vulnerabilidades a que están expuestas las configuraciones del protocolo IPv6 en redes LAN corporativas.

Establecer una guía de prácticas seguras en la configuración del protocolo IPv6, así como en las diferentes capas de interacción del protocolo IPv6 y sus protocolos auxiliares.

1.4 JUSTIFICACIÓN

A nivel global se está realizando la adopción de los protocolos de nueva generación (IPv6), las empresas deberán adaptar su infraestructura actual a estos nuevos mecanismos de comunicación para lograr interoperar con el resto de infraestructura externa e interna, para ello deberán contar con guías que les ayuden a implementarlos de la manera más sencilla y segura. La adopción del protocolo IPv6 requiere de un enfoque de seguridad ampliado ya que no es suficiente las tácticas de seguridad perimetral que eran tan comunes en redes IPv4 y se debe adicionar un esquema de seguridad distribuida que implica prácticas de seguridad por capas del protocolo TCP/IPv6 y lo más importante: la implementación de políticas y herramientas de seguridad en el host final. Lo anterior aunado al propio agotamiento de las direcciones IPv4 que dio origen en un primer momento a los protocolos de nueva generación lo que se evidencia en la Figura 1.

Figura 1. Agotamiento de direcciones IPv4 en la zona administrada por LACNIC (América latina y el Caribe)



Fuente LACNIC febrero 2018 - http://www.lacnic.net/agotamiento

Desde el año 2015 el Ministerio de las tecnologías de la información y las comunicaciones MinTIC realizó una serie de cambios en su Estrategia de Gobierno en Línea GEL con el fin de estar a la vanguardia del e-government o gobierno electrónico de cara al ciudadano. Por ello el MinTIC incorporó nuevos elementos a su ya conocido Manual de Gobierno en Línea 3.1, uno de estos nuevos elementos corresponde al ámbito de la Seguridad y Privacidad de la Información en las entidades del orden Nacional.

Esta reestructuración de la Estrategia de gobierno en línea GEL llego acompañada de un cronograma de implementación que debería entrar a operar desde el 2015 pero que por problemas de divulgación en las Entidades del Orden Nacional sólo inicio curso hasta el año 2016. De esto surge la necesidad de orientar un conjunto de buenas prácticas en la configuración e implementación del protocolo IPv6 desde el punto de vista de la seguridad informática.

IPv6 Forum[2] afirma que, aunque IPv6 ya es un estándar para la industria y la opción a tomar como alternativa a IPv4, es un protocolo inmaduro respecto al desarrollo y formulación de buenas prácticas.

Dichas reglamentaciones de Gobierno en Línea suponen un cambio y adopción acelerados en el país por lo que en el momento de su implementación se requieren tener medidas y buenas prácticas en materia de seguridad. Por lo tanto, es necesario conocer de manera clara las distintas opciones de configuración del protocolo y sus interacciones con otras capas del modelo TCP/IP, así mismo es importante evidenciar las vulnerabilidades a que está expuesta una red LAN corporativa bajo el protocolo IPv6 y como facilitar la aplicación de prácticas seguras en la configuración del protocolo IPv6 y sus protocolos auxiliares.

[2] IPv6 Forum es una organización internacional sin ánimo de lucro cuyos objetivos están la adopción, promoción y divulgación del protocolo IPv6.

1.5 ALCANCE Y DELIMITACIÓN DEL PROYECTO

Ámbito y calidad de aplicación

Este trabajo dada su complejidad, novedad y dimensión debe ser acotado, esto supone que los autores limitan su aplicabilidad a una guía de buenas prácticas enfocadas en la seguridad al momento de implementar aspectos importantes del protocolo IPv6; teniendo en cuenta claramente que se abarcaran algunos temas inherentes a la configuración de protocolos auxiliares y a la identificación y solución de ataques más conocidos al protocolo. Así mismo el trabajo no se puede interpretar como una metodología para la transición de redes IPv4 a IPv6 o un método para determinar cuál es la estrategia de transición IPv4 a IPv6.

2. METODOLOGÍA

Mediante un tipo de estudio descriptivo, el método de investigación a aplicar es deductivo - síntesis por ello se plantea en este documento una estructura basada en el desarrollo propedéutico que va desde lo general a lo especifico.

Para ello los autores recogimos en el maremágnum de distintas fuentes sobre los temas relevantes donde se ubica al lector en los antecedentes del desarrollo de la infraestructura que soporta la Internet para luego desembocar en los protocolos IPv4 su descripción y problemas generados. Luego se da a conocer los fundamentos de la arquitectura que soportan IPv6, así como la configuración de cada paquete que se envía en la red. Para luego terminar en una serie de prácticas que involucra a los responsables de las implementaciones y tienen muy en cuenta los métodos de implementación de IPv6 y recomendaciones de seguridad, el plan de enumeración, los protocolos auxiliares y los métodos de configuración y autoconfiguración de nodos usando direcciones administradas.

3. MARCO DE REFERENCIA

3.1 DEFINICIONES

Los siguientes términos y definiciones de este documento están basados en la Norma ISO 27000:2013, ISO 31000, GTC ISO/IEC 27035 así como documentación de normas de la IANA y el RFCs respectivos.

Amenaza: Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización.

Anycast: Envió de un paquete a un host receptor de un grupo.

Análisis de Riesgo: Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo.

Análisis de riesgos cualitativo: Análisis de riesgos en el que se usa algún tipo de escalas de valoración para situar la gravedad del impacto y la probabilidad de ocurrencia.

Análisis de riesgos cuantitativo: Análisis de riesgos en función de las pérdidas financieras que causaría el impacto.

Autenticidad: Propiedad de que una entidad es lo que afirma ser.

Balanceo de carga: Es una técnica empleada para evitar la sobrecarga en un servidor o servidores de manera que se evite la disminución en el desempeño del mismo.

Checksum: Verificación de integridad de la cabecera, mecanismos como IEEE802 MAL, Framing PPP, y las redes IPv4.

Confiabilidad de la Información: La confiabilidad de la información hace referencia que la información y su fuente no han sufrido alteración alguna, son integra.

Confidencialidad: La confidencialidad es la propiedad que permite garantizar de la información solo sea accesible o consultada por aquellos que están autorizados para ello.

Control: El control es todo el andamiaje que permite mantener en su nivel aceptable el riesgo de seguridad de la información asumido por la entidad, entiéndase por andamiaje: Control es también llamado salvaguarda o contramedida.

Disponibilidad: La disponibilidad es la propiedad de la información que la hace accesible y utilizable cuando se requiera, o sea cuando la requiera una entidad autorizada. La disponibilidad también hace referencia al formato y los recursos que se requieran para acceder a los datos, la no disponibilidad de la información puede generar el deterioro de la imagen institucional.

DoS (Denialof Service): Ataque que hace muchas peticiones a un servicio o un servidor y logra que deje de funcionar el servicio o protocolo atacado. Cuando el ataque se lleva a cabo desde varios puntos se habla de un ataque distribuido DDoS (DistributedDoS).

Evaluación de riesgos: Evaluar un riesgo implica identificarlo, analizarlo y estimarlo, la parte complementaria de este proceso es el tratamiento del riesgo.

Exhaustion: Busca agotar un recurso para que deje de funcionar algo. Esto puede dar lugar a un DoS, o puede usarse para acceder a otras técnicas de ataque.

Flooding: Inundar una red de tráfico, buscando desbordar su capacidad.

Hardening(endurecimiento): Técnica para asegurar un sistema mediante la instalación y configuración de lo estrictamente necesario, pues así se reducen las vulnerabilidades en el mismo sobre la premisa de reducir la “superficie” atacable.

Hijacking(Secuestro): Ataque fundamentado en la alteración de los datos, sesiones, o comunicaciones, como por ejemplo el Browser Hijacking que hace que el usuario vea páginas modificadas.

Impacto: El impacto no es otra cosa, que el costo que tiene para la organización un incidente de seguridad de la información y esto va más allá de término estrictamente financiero como puede ser: la pérdida de reputación y las implicaciones legales que se desprenden de un incidente.

Incidente de seguridad de la información: Suceso o sucesos no esperados que tienen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.

Integridad: La información debe ser clara y completa, y solo podrá ser modificada por el personal expresamente autorizado para ello. La falta de integridad de la información expone a una toma de decisiones incorrectas, lo que conlleva a pérdidas de imagen o económicas.

MITM (Man-In-The-Middle): Poner un punto de escucha en la comunicación entre dos nodos.

Multicast: Envió de un mismo paquete a varios host o grupo receptor.

Poisoning: Envenenar con información errónea un sistema informático con fines maliciosos.

Probabilidad: Estimación de la ocurrencia del riesgo.

Propietario del riesgo: Es la persona o entidad responsable de gestionar un riesgo.

Propietario del riesgo: Persona o entidad responsable de gestionar un riesgo.

Protocolo: Son las reglas que permiten que dos host, o más, puedan establecer una comunicación, permitiendo el intercambio de información. Estas reglas abarcan desde la sintaxis, la semántica y la sincronización de la comunicación.

Redundancia: Es una técnica en la cual se replica un mismo servicio o funcionalidad para evitar fallas o para crear dinamismo en el diseño o acceso a las mismas. En caso de fallas el servicio redundante asume las actividades.

Riesgo Inherente: Incertidumbre propia de una actividad, que carece de control alguno.

Riesgo residual: Riesgo que sobrevive al tratamiento del riesgo.

Riesgo: Es la probabilidad que sea explotada una vulnerabilidad por una amenaza con el fin de daño o pérdida en un activo de información.

Otra forma de definir el riesgo es como la combinación de la probabilidad de un evento y sus consecuencias.

Seguridad de la Información: Una información es segura en la medida que preserva su confidencialidad, su integridad y su disponibilidad.

Selección de controles: es definir las salvaguardas que mitiguen los riesgos, llevándolos a un nivel aceptable.

Sniffing: Capturar el tráfico de red que llega a una interfaz y procesarlo, se configura esta información se puede guardar en un archivo. Requiere de una interfaz en “modo promiscuo”.

Spoofing: Ataque basado en la suplantación, puede ser suplantación de MAC Spoofing o de IP Spoofing, o de ARP Spoofing, o de DNS Spoofing o de Web Spoofing.

Valoración del riesgo: Es el proceso de análisis y evaluación de los riesgos a que están expuestos los activos de información.

Vulnerabilidad: Se dice que un activo es vulnerable cuando tiene una debilidad que puede ser explotada por una o más amenazas.

IANA Internet Assigned Numbers Authority, Es la autoridad encargada de definir las políticas y estándares de internet.

IETF Internet Engineering Task Force, Es la entidad designada por la IANA para llevar a cabo el desarrollo de los estándares que rigen los protocolos internet (TCP/IP).

DARPA US Defense Advanced Research Project Agency – Agencia de Proyectos de Investigación Avanzados de Defensa dependiente del Departamento de Defensa perteneciente al gobierno de los Estados Unidos.

ICANN Internet Corporation for Assigned Names and Numbers, Es una entidad encargada de asignar y controlar numerous y espacios de nombres de internet.

AfriNIC African Network Information Centre Es la RIR para el territorio de África.

APNIC Asia-Pacific Network Information Centre Es la RIR para el territorio para Asia y la región pacifica.

ARIN American Registry for Internet Numbers Es la RIR para el territorio para Norte América.

LACNIC Latin America and Caribbean Network Information Centre, Es la RIR para el territorio de para Sur América y el Caribe.

RIPE NCC, Réseaux IP Européens Network Coordination Centre Es la RIR para el territorio de Europa, Asia Central el medio oeste.

RIR Regional Internet registry, Registro regional de internet es la denominación que tienen las 5 entidades encargadas de realizar seguimiento del direccionamiento ip.

3.2 ANTECEDENTES

Mientras que las aproximaciones a la seguridad en redes IPv4 dado a que la normativa ya lleva 35 años son ampliamente estudiadas y trabajadas en los campos de la seguridad informática[3], la administración de redes, sistemas de encriptación, pentesting y otros, en los últimos años se ha venido trabajando y concentrando en las implementaciones y configuraciones IPv6 en menor medida; como lo evidencia el ingeniero especializado de Cisco Mark Townsley en su charla IPv6 y el IETF muestra que la cantidad de documentación oficial de parte de RFC es mucho menor IPv6 versus IPv4 (ver Tabla 3. Número y estado de los RFCs en el IETF).

Según el Ingeniero Arth Grossy Sabogal en 2017 sustenta en el documento "Elaboración de una guía abierta para la administración de riesgos de seguridad en el protocolo de internet IPv6 sobre estándares de enrutamiento dinámico en equipos con plataforma Cisco"[4]señala que, "*IPv6 si obliga a incorporar dentro del paquete IP al protocolo IPSec (eliminando la variedad de protocolos de seguridad existentes en IPv4)".*

Igualmente encontramos también en el trabajo *"Migración de red IPv4 A IPv6 sobre la red del Ejército Nacional"* del ingeniero Gómez Prieto[5], donde enfoca su pertinencia a infraestructura Cisco, que para el caso de Routing sabemos maneja un protocolo propietario exclusivo de la firma Cisco (EIGRP) por lo tanto protocolos de ruteo genéricos como OSPF o IS-IS no están siendo considerados.

De igual forma pasa con características de seguridad propias de Cisco como la presentada en el trabajo del Ing. Grossy, ya que AES ofrece cifrado para mensajes SNMP, pero es una característica exclusiva de esta infraestructura.

A su vez algunos trabajos reflejan la disponibilidad de los mecanismos de IPSec como el "Phase-2 Interoperability Test Scenario IPSec Technical Document" del

---

[3] Townsley M, (2009), IPv6 &the IETF, CISCO & IETF. Recuperado de http://www.cu.ipv6tf.org/pdf/CAA7ULEL.pdf

[4] Sabogal Ortiz, A. (2017). Elaboración de una guía abierta para la administración de riesgos de seguridad en el protocolo de internet IPv6 sobre estándares de enrutamiento dinámico en equipos con plataforma CISCO.. Colombia: Recuperado de: http://hdl.handle.net/10596/12015

[5] Gómez Prieto, N. y Torres Rojas, Y. (2008). Migración de red IPV4 A IPV6 sobre la red del Ejército Nacional. Colombia: Recuperado de: http://hdl.handle.net/10596/1570

IPv6 Forum y el IPv6 Ready Logo Committee[6] donde la guía asume que IPv6 implementa por default IPSec activamente y eso es solo una opción, por lo que una implementación de IPv6 puede o no tener activo IPSec, de hecho, IPSec se corresponde a dos cabeceras de extensión y en el trabajo se aborda como una característica activa por Default. Así mismo los ingenieros Rico Bautista y otros en el año 2008 en su trabajo para la Universidad de Pamplona abordan el tema de IPSec e IPv6 desde la implementación en entornos académicos[7].

Para el ingeniero Sabogal[8] se observa un reconocimiento de la autoconfiguración SLAAC de una manera muy superficial y se dejan de contemplar las opciones para mitigar los posibles riesgos que pueda tener esta asignación de direcciones SLAAC. Consideramos muy apresurado establecer como única opción el bloqueo de la autoconfiguración de direcciones SLAAC, para muchos escenarios esto no es lo más apropiado pues es por SLAAC que se dice que IPv6 es plug and play y es uno de los logros más importantes del nuevo protocolo IPv6.

En cuanto a configuración de seguridad en Redes IPv6 se destacan trabajos como el aportado por CISCO en su libro Cisco self-study: implementing IPv6 Networks (IPv6)[9] donde abarcan el diseño y configuración enfocado principalmente a temas como el direccionamiento y a mecanismos específicos de ruteo. Aunque tiene un interesantísimo capítulo sobre tunneling (IPv4 – IPv6) o IPv6 Security de la misma casa editorial[10] Donde se exploran a profundidad mecanismos de seguridad en entornos Cisco.

---

6 Phase-2 Interoperability Test Scenario IPSec Technical Document Revision2.0.0b. [online] Available at: https://www.ipv6ready.org/docs/Phase2_IPSec_Conformance_v2_0_0b.pdf [disponible 27 Jan. 2018].

7 Rico Bautista, Dewar Willmer, Medina Cárdenas, Yurley Constanza, Santos Jaimes, Luz Marina, IPSec DE IPv6 EN LA UNIVERSIDAD DE PAMPLONA. Scientia Et Technica [en línea] 2008, XIV (Septiembre-Sin mes) : Fecha de consulta: 27 de febrero de 2018] Disponible en: http://www.redalyc.org/articulo.oa?id=84920503057 ISSN 0122-1701

8 Sabogal Ortiz, A. (2017) Ídem.

9 Desmeules, R. (2007). *Cisco self-study* implementing IPv6 Networks (IPv6). Indianapolis, IN: Cisco Pr.

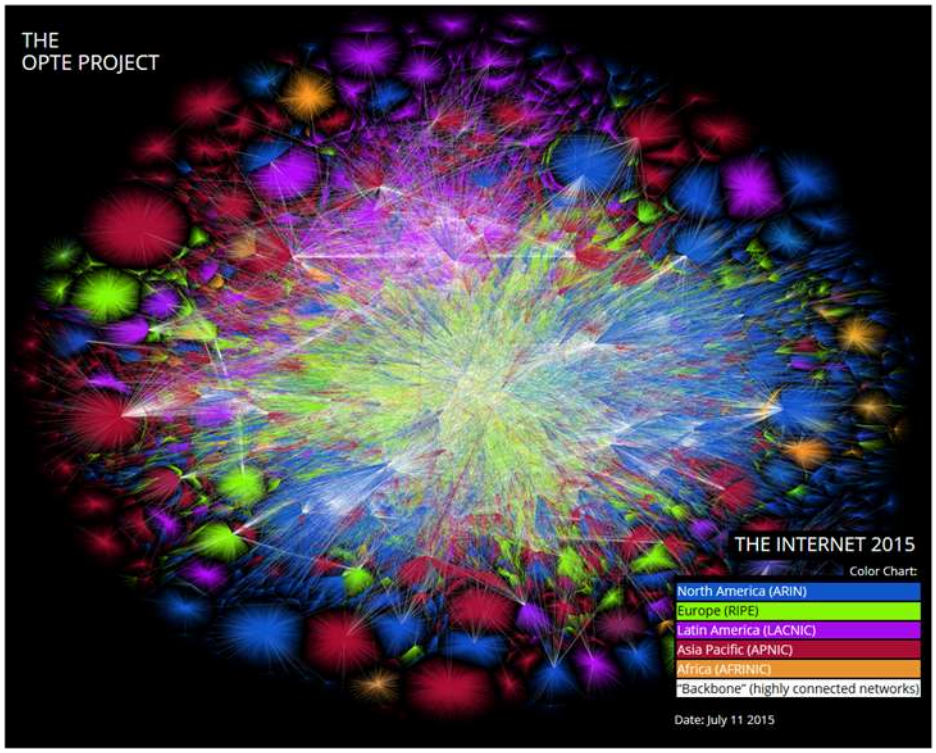
10 Hogg, S., Vyncke, E., Karpenko, J. and Miller, D. (2009). *IPv6 security*. Indianapolis, Ind.: Cisco Press.

3.3 MARCO LEGAL

3.3.1 Ecosistema de las entidades de Internet

La interconexión de computadoras y la no dependencia de una de ellas para el transporte de la información éste inicio de la internet implico per se una serie de normas que hicieran posibles dicha comunicación. Por ello la agencia de seguridad de estados unidos -DARPA[11]- desarrolló, en conjunto con varias universidades la ARPANET y con ella lo que hoy se conoce como el modelo internet (TCP/IP), que en resumen es una serie de protocolos que determinan la forma, modos y lenguajes en que se deben enviar las informaciones, así como las formas como cada uno de los involucrados puede interactuar en la comunicación. A esta variedad de actores, normas, tecnologías, lenguajes y protocolos se le denomina “Ecosistemas de Internet”. Este ecosistema tiene una jerarquía por territorio que es la que representa la Figura 2 donde se presentan los diferentes RIR´s.

Figura 2. Mapa de la Internet actual



[11] DARPA, US Defense Advanced Research Project Agency – Agencia de Proyectos de Investigación Avanzados de Defensa dependiente del Departamento de Defensa perteneciente al gobierno de los Estados Unidos

Ilustración de los autores basada en el proyecto OPTE[12] Fuente http://www.opte.org/the-internet/

De la simplicidad administrativa del ARPANET se pasó a organismos colegiados (académicos fundamentalmente) para luego ser administrados y reglados de manera que la participación (de entidades académicas y gobiernos federales inicialmente de estados unidos) de los países y regiones tuviese cabida. Aunque existen múltiples organizaciones y entidades que tienen la responsabilidad de orientar y organizar lo que se conoce ahora como el ecosistema de internet. Las organizaciones más relevantes en este trabajo son la Internet Society, IANA, IETF, RIR. La función de cada uno de ellos se deriva tal y como lo refleja la Figura 3.

Figura 3. Ecosistema de las entidades de Internet

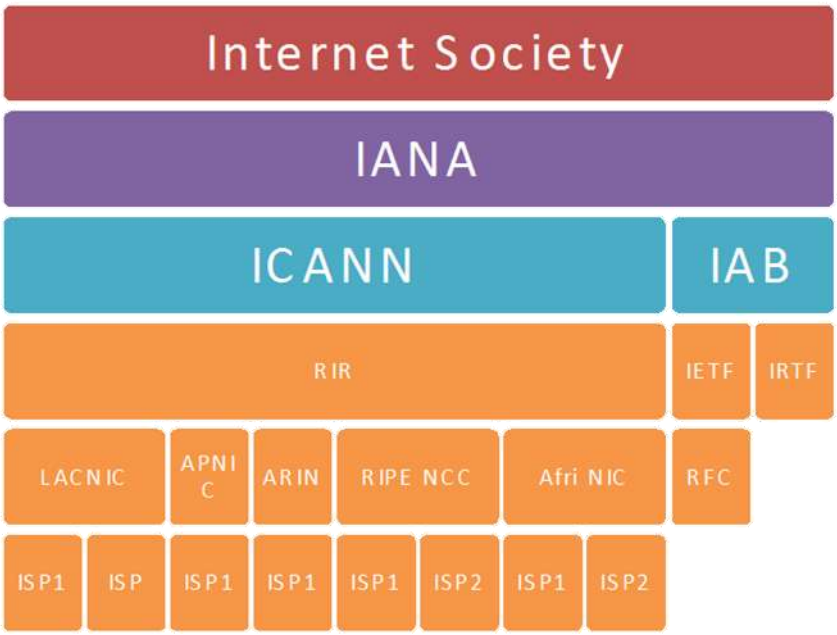


Ilustración propia basada de internet society:https://cdn.prod.internetsociety.org/wp-content/uploads/2017/

La Internet Society es una organización sin fines de lucro que da cuenta de la mayoría de decisiones que realizan a nivel de políticas de internet su evolución y uso. Adscrita a ella está la IANA que junto con el ICANN administran los números de direcciones IP y nombres de dominio y los TDLs más relevantes. El ICANN a su vez ha designado a 5 RIRs (registros de Internet regionales) para la administración

[12] OPTE es un proyecto de carácter independiente que busca evidenciar mediante una representación precisa la amplitud de Internet utilizando gráficos.

y seguimiento a la asignación de nombres y administrar espacios de direcciones IP y que como su nombre lo indica es de alcance regional. El grupo de trabajo para la ingeniería de internet (IETF) tiene a su cargo el desarrollo e investigación entre otros de los estándares que usa la internet actualmente, estos desarrollos se ven reflejados en documentos que son conocidos como RFCs (Request for comments – Solicitud de comentarios).

Los RIR están a su vez divididos en cinco regiones geográficas así:

- AfriNIC para África
- APNIC para Asia y la región pacifica
- ARIN para Norte América
- LACNIC para Sur América y el Caribe
- RIPE NCC para Europa, Asia Central el medio oeste.

Dado el alcance técnico de estas organizaciones los países a que hacen parte de la ONU tienen en el ITU (Unión Internacional de Telecomunicaciones) su representación, donde se resuelven problemáticas como asignación de espectro electromagnético, órbitas satelitales y promueven protocolos e interoperabilidad entre equipos y sistemas de telecomunicación, así como la gobernanza de internet por lo tanto tiene estrecha relación con las organizaciones mencionadas anteriormente.

3.3.2 Normatividad internacional

La unión internacional de telecomunicaciones -ITU–ha definido una serie de normativas sobre la adopción y uso del protocolo IPv6 para garantizar la continuidad de las redes y su interoperabilidad entre los estados miembros.

Concretamente desde el año 2006 la ITU ha reunido a miembros plenipotenciarios y en las resoluciones 101 y 102 hablan de la escases de direcciones IPv4 y la importancia de migrar a IPv6, que posteriormente mediante resoluciones como la 64 de 2008 instan a los miembros a fortalecer la implementación del protocolo IPv6[13] o como la resolución 180 de 2010 donde desarrollan políticas dentro del

[13]ITU-T Resolution 64 – IP address allocation and encouraging the deployment of IPv6, Johanesburgo Oct 2008.

organismo para fortalecer el avance de IPv6 que se vio reflejado en el año 2012 mediante la resolución 64 de la Asamblea Mundial de Normalización de las Telecomunicaciones[14] Donde además de involucrar a los estados miembros a que se comprometan con IPv6 se vincula a los miembros del sector de las telecomunicaciones a participar en dicho actividad.

3.3.3 Normatividad Nacional

El ministerio de las telecomunicaciones en Colombia también ha resaltado la importancia de la implementación de IPv6. Teniendo como base la Ley 1341 de 2009[15] y el decreto 2573 de 2014 donde implementa la política pública Gobierno en Línea (GEL) han desarrollado una serie de guías y circulares para la adopción de dicho protocolo en el país.

La circular 002 de 2011 del ministerio insta a todas las entidades públicas a que desde ese momento todos los contratos que involucren compras en el sector de las TIC se exija soporte de protocolo IPv6 y compatibilidad con IPv4.

El ministerio además ha desarrollado adicionalmente un par de guías para la transición a IPv6[16] donde dan cuenta de los requerimientos para dicha transición y algunas características generales en el mismo.

Finalmente, el mismo ministerio ha expedido la resolución 2710 de 2017 donde obliga a los entes territoriales a migrar a IPv6 al 31 de diciembre de 2019 y a entidades regionales en el año 2020. Así mismo obliga a las entidades a contratar toda la infraestructura TIC con protocolo nativo IPv6.

---

[14]ITU-T Resolution 64 – IP address allocation and facilitating the transitionto and deployment of IPv6, Dubái Nov. 2012.

[15] Ley 1341 de 2009 – Congreso de la República. Ley marco del sector de las comunicaciones, sus entidades adscritas y vinculadas así como la política pública en materia de TIC,

[16]MinTIC - “Guía de transición de IPv4 a IPv6 para Colombia” y “Guía para el aseguramiento del Protocolo IPv6” Colombia 2015

3.4 MARCO TEÓRICO

3.4.1 TCP/IP y el modelo internet

El conjunto de protocolos que rige ese mundo se le conoce como modelo o pila de protocolos TCP/IP, y que como se ilustra en la Figura 4 alberga un conjunto de protocolos agrupados en cinco capas (anteriormente la OSI había desarrollado siete capas por las cuales se debería realizar la comunicación y actualmente se usa como referencia en los estándares de comunicación).

Figura 4. Capas del Modelo TCP/IP con sus protocolos más conocidos

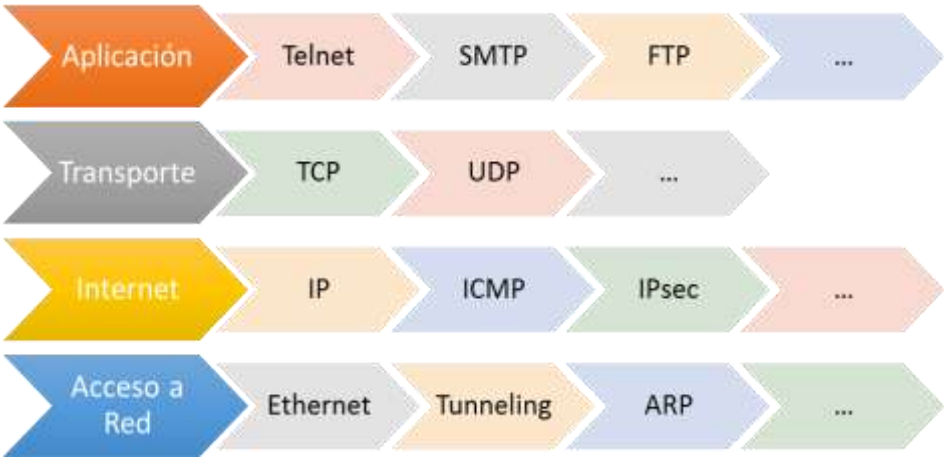


Ilustración propia - basado en RFC 793[17]

Para ello los miembros que concibieron la Internet como proyecto inicial dividieron los mensajes en partes donde las llamaron paquetes o datagramas, dichos paquetes tenían un encabezado donde definían algunas características dependiendo el uso y destino y una carga donde se alojan los datos (payload o carga útil) que se desean transmitir. Entre estos atributos para la capa de red definieron un protocolo llamado IP (internet protocolo) que se fue definiendo en la medida de las necesidades del proyecto (en ese momento se definieron tres protocolos de prueba hasta que se definió una cuarta versión, por eso su nombre actual: IPv4).

[17] RFC793 - Transmission control protocol Specification. *Tools.ietf.org*. Fecha de consulta: 9 May 2018, from https://tools.ietf.org/html/rfc793

Tabla 1 Hitos en la construcción del protocolo IPv6

Año	Suceso	Documentación
1991	IETF genera un grupo de trabajo para que trabaje el tema de agotamiento de las direcciones IPv4.	
1992	IETF se determina que hay la necesidad de generar un nuevo protocolo para atender el problema del direccionamiento	
1993	IPv4 se hacen las primeras estimaciones sobre en qué tiempo de agotaran las direcciones IPv4.	
1993	Se generan técnicas para prolongar las direcciones IPv4 como CIDR (Classless Inter-Domain Routing).Fue la última mejora que tuvo el protocolo IPv4 sobre el modo de interpretar las direcciones IP, esto es conocido VLMS o máscaras de subred de tamaño variable.	RFC 1519
1994	Nace la técnica de prolongación de IPv4 conocida como NAT. Recordemos que NAT (Network Address Translation) es un mecanismo de traducción de direcciones IPv4 Públicas y Privadas y viceversa.	RFC 1634
1994	Distintos grupos de trabajo dentro del IETF hacen que se concrete un memorando donde se estipula por primera vez una opción de IPng	RFC 1752
1995	Se da a conocer el borrador del protocolo IPv6	RFC 1883
1996	Se implementa el uso de IPv4 Privadas	RFC 1918
1998	Se promulga el Core del protocolo IPv6	RFC 2460
2012	La clase especial de direcciones IPv6 q permite la compatibilidad de los formatos de direcciones deja de ser opcional. Es una dirección IPv6 cuyos primeros 96 bits son ceros y los 32 siguientes representan a la IPv4que quieren compatibilizar.	RFC 6540
2012	Se declara el 6 de junio como día mundial de IPv6	

Fuente, Los autores basados en documentación de las RFCs.

3.4.2 Dispositivos de capa de red

3.4.2.1 Router

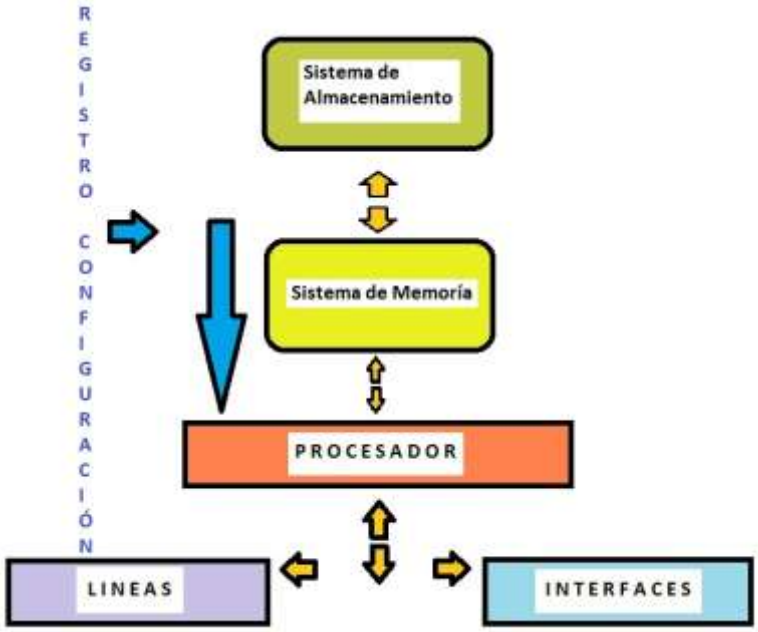
Un Router o enrutador es un dispositivo de red que permite establecer comunicaciones entre redes (nivel tres de OSI).Los enrutadores son esenciales para permitir el enrutamiento de los datagramas entre diferentes subredes, dicho de otra manera, los routers permiten la interconexión de redes.

Subred: conjunto de computadores con IP que se pueden intercomunicar mediante puentes de red o un Switch, tienen prefijos de red distintos. Una subred no requiere de un Router para su existencia.

3.4.2.2 Arquitectura de Router

Un Router es un computador empotrado en una caja, por lo que tiene un procesador, un sistema de memoria, y unas líneas de comunicación con el exterior, su diseño esta optimizado para el reenvió de datagramas. Como se evidencia en la Figura 5.

Figura 5. Arquitectura de Router



Diseño propio Fuente Los autores

PROCESADOR: Controla las líneas y las interfaces y el sistema de memoria, el sistema de memoria incluye el trabajo con medios de almacenamientos permanentes.

MEMORIA: Un Router maneja varios tipos de memoria desde los medios más Permanente a los más volátiles la memoria se clasifica en:

Tabla 2 Sistema de memoria de un Router

ROM	Memoria invariable, inmodificable, construida de fábrica, realiza el post o programa de chequeo del hardware una vez se prende el router, de haber un error encenderá ciertas luces. Contiene el Bootstrap o programa de arranque del BIOS. La ROM también aloja el ROM Monitor que es una versión reducida y no funcional del S.O. y es solo para actividades de recuperación, por ejemplo, si se pierde el S.O con esta versión reducida se arranca el Router y desde ella se puede llamar al S.O. o sus instaladores desde otro dispositivo.
FLASH	Memoria basada en chip, es la conocida tecnología Pendrive propia de los dispositivos de almacenamiento USB. Equivale al disco duro del router contiene un fichero imagen comprimido del S.O. y los ficheros del usuario, por ejemplo, otras imágenes de versiones del S.O. del Router o copias de seguridad de las configuraciones del router. Desde acá arranca el sistema operativo que ejecuta el Router.
NVRAM	La memoria NVRAM tecnológicamente es igual a la FLASH. Es la memoria RAM no volátil. Contiene el Startup-Config o fichero de configuración inicial del router en texto plano. Ésta memoria no pierde la información al retirar la electricidad del Router. Esta configuración se puede sobrescribir o borrar. Esta configuración no se ejecuta nunca.
RAM	Memoria de trabajo volátil, aloja al Running-Config o fichero de configuración activo escrito en texto plano. En la memoria Flash se alojan los datos de trabajo como la tabla ARP, la Tabla de enrutamiento y el S.O. Ejecutable. Cuando se arranca el router se hace una copia del Startup-config en la RAM con el nombre de Running Config. El running config es editable por eso cuando un router es nuevo lo primero que se hace es establecer la configuración del mismo en el running config y al guardarlo se crea una copia llamada startup config.

Fuente Cisco IOS Network Foundation Protection (NFP). www.cisco.com

Líneas: Son entradas del router (que no tiene conector, que no tiene teclado) para la conexión de un terminal con el fin de programar el router. Las líneas son:

Línea de Consola: Que permite la conexión directa por puerto serie de un terminal al puerto de consola (Rj45) del router, es la típica línea console 0.

Línea Auxiliar: Permite una antigua conexión telefónica por modem al router. Requiere conexión por modem y línea telefónica en el otro punto remoto desde donde se desea conectar al router. El lado del router también debe contar con un modem conectado a una línea telefónica. Esta línea de configuración del router está entrando en desuso, además tiene algunas limitaciones frente a la línea de consola por ejemplo no se puede ejecutar el procedimiento de restablecimiento de contraseña.

Líneas Virtuales: como su nombre lo indica físicamente no existen, aprovecha las interfaces que tiene conectado el router para establecer conexiones telnet de configuración del router. Los router actuales tienen 16 líneas virtuales para

conexión telnet (vty 0 a vty 15), los routers antiguos solo tenían 5 líneas de conexión virtual (vty 0 a vty 4); son conexiones simultaneas, actualmente se prefieren las conexiones ssh al telnet por temas de seguridad, pues las conexiones ssh vienen cifradas y las de telnet en texto claro.

Interfaces: Permiten al router recibir paquetes IP o datagramas por sus interfaces y en función de su tabla de enrutamiento reenvía esos paquetes por otras interfaces. Un router puede tener varias y diferentes interfaces y son identificadas en el sistema operativo del router de una manera inequívoca (Ethernet, Serial, Bri, fast Ethernet, etc.) dentro de cada tipo de interfaz se enumeran partiendo del cero "0".

Registro de configuración: Todos los router tienen un registro de configuración numérico, binario que equivale a un campo de 16 bits que equivalen a 4 dígitos hexadecimal y según su valor (2102 o 2142) tomara la sesión de inicio normal (arrancar el S.O. desde la Flash o un servidor TFTP) o arrancar la versión reducida del ROM MONITOR (aunque tenga S.O. en el flash) respectivamente. Según lo valores 2102 o 2142 en el registro de configuración del router también se toma la decisión de buscar el startup-config o ir al Setup de configuración (aunque exista el startup-config).Si el registro es 2102 se hace una copia del startup-config en la RAM del router y el router está operativo y listo a atender nuevas peticiones. De lo contrario se irá por el modo Setup de configuración del router que es una lista de preguntas que definirán la configuración de la máquina este modo no es nada recomendable ya que es un modo muy general diseñado para usuarios neófitos lo que hace que la configuración no cuente con optimización alguna.

3.4.2.3 El Proceso de Enrutamiento

Es la actividad que permite que un datagrama sea enviado por un router a su ip de destino, el router y demás dispositivos intermedios toma decisiones en función de su IP de destino del datagrama. Para cumplir con esta función los routers deben aprender la ruta hacia redes remotas que son las redes que no tiene conectadas directamente.

3.4.2.4 Network Foundation Protection

Es un marco de referencia original de la compañía Cisco que define la arquitectura lógica de los equipos de red como Switch o Router, conocidas también como las áreas funcionales de estos equipos de red. Pese a ser un framework propietario de cisco el CCNA Security no hace énfasis en el marketing de las soluciones Cisco y por el contrario hace énfasis en los aspectos técnicos a dominar e implementar para establecer soluciones robustas de seguridad.

Las áreas funcionales de un Switch o un Router son:

3.4.2.5 El plano de control

El plano de control (CONTROL PLANE): Esta estructura se encarga del enrutamiento de la data, son los mensajes generados por los equipos en concordancia con el protocolo de enrutamiento configurado: OSPF, BGP y RIP. En conclusión, es el área funcional de control de los equipos de red. Desde el punto de vista de seguridad se debe proteger el intercambio de mensajes de estos equipos, por ejemplo, si establezco protocolos de enrutamiento como RIP, BGP U OSPF el intercambio de mensajes es en texto plano lo que hace muy fácil establecer un vecino. Esta exposición es lo que se conoce como el Routing Protocol Exploit (Ataques directos sobre los protocolos de enrutamiento).Por ello es importante establecer la autenticación en los protocolos de enrutamiento y establecer una tasa de transferencia o mecanismos de filtrado que controle posibles tormentas de broadcast y exceso de tráfico que de no ser controlado pueda llegar a sacar a los equipos de red de control.

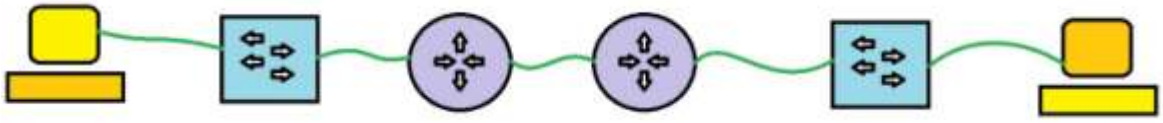
3.4.2.6 El plano de administración

El plano de administración (management plane):Esta estructura se encarga del control de acceso a los equipos de red, es el área que garantiza la conectividad al Router, esta conectividad es entre una estación final y el Router administrado y puede ser por un cable de consola, un cable de red, un modem, un celular. Esta administración se realiza a través de mensajes entre el equipo de red y una estación final, los mensajes de autenticación ante el dispositivo switch o router por lo general son a través de SSL (https), Telnet, SSH, Acceso remoto vía web y otras opciones del estándar 802.1x (Servicios triple A /AAA); los servicios AAA dan soporte al plano de datos y al management plane.

3.4.2.7 El plano de datos

El plano de datos (data plane Y 802.1X): Es la estructura encargada de enviar el tráfico del origen al destino, es el área funcional encargada del ingreso y egreso de paquetes, es la comunicación de extremo a extremo. Se puede ver un plano de comunicación en la Figura 6. Los servicios triple A del estándar 802.1x también dan soporte a este plano de datos.

Figura 6. Plano de comunicación extremo a extremo en una red



Diseño propio Fuente Los autores

3.4.3 El protocolo IPv4

El protocolo IP versión 4 es un protocolo no orientado a conexión enmarcado en las RFCs 760 y 791 eso implica que los paquetes que se transmitan en la capa de red bajo este protocolo no requieren que el origen y el destino acordaran previamente una comunicación. De igual manera implica que en la transmisión se pueden perder paquetes que tendrían que ser reenviados para completar la comunicación.

Así mismo las RFCs del protocolo definían que los datagramas en su encabezamiento deberían tener una estructura que informara a los distintos nodos su destino, origen entre otros para que de esta manera se pudiera enrutar.

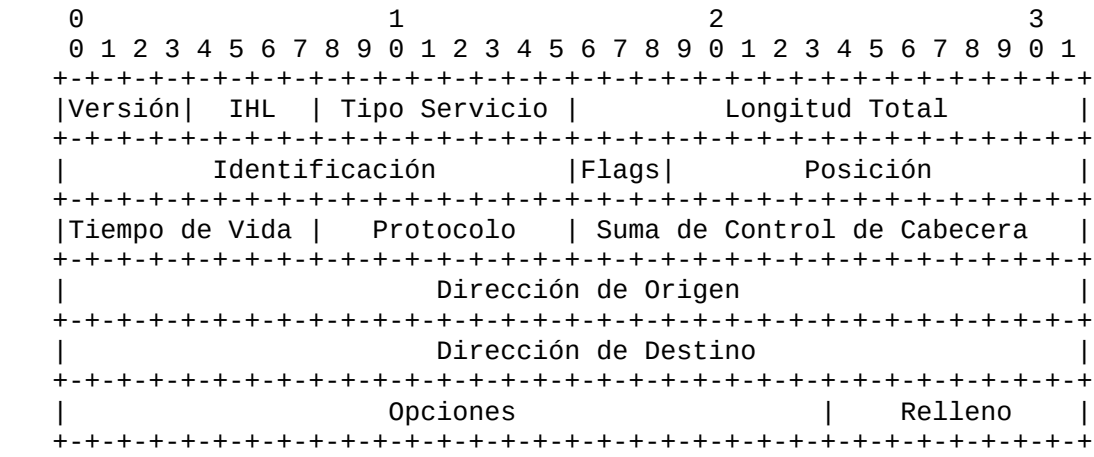
En cuanto a la identificación de los distintos nodos o host que hacen parte de una red el protocolo establece un método de identificarlo. Esto se conoce como direccionamiento y en IPv4 se identifica como un conjunto de 32 bits que para su interpretación y administración se dividen en cuatro octetos que en notación decimal van de 0 a 255. Así es que al usar un conjunto de 32 bits teóricamente es posible definir un conjunto de 2^{32} direcciones posibles, es decir, un total de 4.294’967.296 de hosts.

Con ese número de direcciones de dispositivos conectados a Internet parecía inicialmente que iba a ser suficiente (en los años 70s existían únicamente en estados unidos alrededor de 100 máquinas conectadas y para los 80s ya superaban los 2 millones).

3.4.3.1 IPv4 Campos Especiales del Encabezado IPv4

La dirección de IPv4 está conformada por 4 bytes. La longitud de la cabecera IPv4 es de 20 a 60 bytes. La Figura 7 Muestra la cabecera del datagrama en el protocolo IPv4.

Figura 7. Cabecera el Datagrama Internet IPv4



Fuente IETF RFC791[18]

Algunos de sus campos:

DiffServ (Diferencia de Servicio) RFC2474/8bits/6bits y 2 bits. Tiene dos funciones reportar congestión (explicit congestión) y QoS calidad de servicio. Con estas funciones se reporta congestión y se toman medidas sobre esa congestión es algo más bien nuevo en IPv4 (rfc971), antes este campo era PRECEDENT, q otorgaba un trato predilecto a un paquete ip en la red (RFC 2474) permite q este campo quede homologado para IPv6.

DiffServ es un campo para calidad de servicio 4/6 bits es el campo sucesor de precedence y type of service.

PacketLength (longitud de datagrama) campo de 16bits incluido en la cabecera recibe valores de 0 a 65.535 define el payload.

Datagrama IP está conformado por dos bloques: la cabecera del paquete y la data (payload).

MTU tamaño del datagrama en IPv6 viene un protocolo para establecer el MTU.

En IPv4 los routers tenían que calcular la carga útil de un paquete =packetlength – tamaño cabecera ip. En IPv6 esto no se requiere pues es fijo.

IPv4 y soporte a la fragmentación.

[18] RFC791 - Internet Protocol In-text: Tools.ietf.org. Fecha de consulta: Noviembre 2017, Disponible en: https://tools.ietf.org/html/rfc791

Campo identificación 16b/flag3b/ fragment offset 13b.

Dar soporte a la fragmentación en paquetes.

IDENTIFICACIÓN: Permite reensamblar los paquetes en el destino.

** FLAG: Soporte a la fragmentación cuando una aplicación no fragmenta. Está conformado por 3 bits el bit0 es reservado no se usa, bit 1 toma valor 0/1 para indicar fragmentación / No fragmentación respectivamente, y el bit 2 toma valores 0/1 0 para marcar inicio o fin de paquete y 1 para indicar más fragmentación.

Ejemplo: ping 4 -s bit 60.000 enciende flag entonces queda así ping -4 -n 5 -f -1 60.000

** FRAGMENT OFFSET: 13bits puede albergar valores de 0 a 8192.Lleva a cabo el concepto de fragmentación indica al destino los bloques de fragmento de datagrama (grandes trozos de datagrama) (define bloque en 8 octetos)-8bytes) lleva la cuenta de bloques de fragmentos. Esto cuello de botella en la internet en IPv6 no se da porque la fragmentación se maneja en el origen y el destino y no en los routers.

**TTL: Contado 791 resta tiempo cada vez que pasa por el router ej.: tracerouter contador de saltos que impide que los paquetes estén por siempre en la red, en bucle, CUANDO TTL=0 SE DESCARTA EL PAQUETE y se envía mensaje al emisor

TRACEROUTE

TTL=0

Envío de mensaje a emisor mensaje de error.

Toma ip del router y nombre que devuelve el paquete.

Regresa el paquete vuelve a salir el TTL incrementa en 2 devuelve el paquete en segundo router.

Tracerouter utiliza el valor de TTL ayuda a tener el paquete en red solo por tiempo determinado.

**PROTOCOL: Campo de cabecera IPv4 que indica el número de protocolo de capa superior o de una subcabecera IPv4.Los protocolos de capa superior son TCP#6, UDP#7, ICMP#1, IGMP#2,

**HEADER CHECKSUM: Campo de verificación de cabecera, valida la longitud de la cabecera con cada cambio de los campos. Busca garantizar que si salgo con una cabecera de 20b regrese con una cabecera de 20.Verifica los cambios que puedan existir en los routers.

Indica si la cabecera está completa o errada Headerchecksum se actualiza cada que hay un cambio en algún campo de la cabecera IPv4, esto a través del router activo en ese momento. Son 16bits que requería IPv4, este valor es de confiabilidad. En IPv6, tcp y los protocolos de capa superior garantizan la confiabilidad en la data.

3.4.3.2 Inconvenientes Técnicos de IPv4

El auge y evolución de Internet impuso un reto al protocolo IPv4 el cual no considero dificultades atadas a la cantidad de las direcciones disponibles y a problemas por falta de seguridad del mismo.

3.4.3.3 Problemas de rendimiento del Protocolo IPv4

Una de las funcionalidades más extendidas del protocolo IPv4 es el mal uso de Broadcast en la red; esto hace que el medio en algunos casos se sature porque los paquetes que son enviados intencionalmente a todas las estaciones haciendo que la posibilidad de colisiones aumente y por lo tanto tengan que ser reenviadas ralentizando la comunicación. Así mismo es susceptible la manipulación de los datos dado que los paquetes en este medio compartido quedan a merced de ser interceptado, produciéndose gran cantidad de demoras que afectan ostensiblemente a aplicaciones sensibles a los retardos como servicios de VoIP.

Las comunicaciones de tipo broadcast son otro factor que afecta el rendimiento de la red, pues los mismos protocolos hacen uso de estas difusiones generando colisiones y retransmisiones de datos.

Los datagramas requieren procesamiento y esto genera otro tiempo de espera, por ejemplo, cada que llega un paquete a un router hay que determinar si es de esa red o debe ser enrutado nuevamente, si el datagrama debe de ser enrutado el router debe aplicar algoritmos de ruta para que la ruta elegida sea la óptima, esto suma nuevos tiempos de retraso que han hecho que el tema de rendimiento del protocolo sea siempre comentado.

3.4.3.4 Problemas de seguridad del Protocolo IPv4

El protocolo IPv4 en términos generales no implementa ningún tipo de control de seguridad lo que lo hizo blanco de ataques por parte de hackers y aficionados. Con el tiempo se implementaron dos parches que son la estructura de la

seguridad del protocolo: el SSL (Secure Socket Layer) e IPSec. Estas técnicas de seguridad generan un nuevo procesamiento de datos, lo que representa otro retardo en la entrega de la información.

3.4.3.5 Problemas asociados al uso de NAT (Network Address Translation) en IPv4

Debido al agotamiento de las direcciones IPv4 se ideó el NAT que permite que una red privada salga a internet a través de una o de un rango reducido de direcciones IPv4 públicas, por esta razón claramente se crea un cuello de botella en la red, se rompe el concepto end-to-end, que permitía que los paquetes fueran de origen al destino sin alteraciones o intermediación alguna. El NAT altera a los protocolos y a las aplicaciones, generando una sensación de seguridad inexistente. Algunas de las RFCs que explican los inconvenientes de NAT son: 2775, 3027 y 2993.

3.4.4 Protocolos auxiliares en IPv4

Dado que la IETF describe el protocolo IP en la capa de red y está limitado a configuración y entrega de datagramas, son necesarios otros protocolos tanto de la capas de red, transporte y enlace como se puede evidenciar en la Figura 8.

Figura 8. Ubicación de los protocolos IP y sus protocolos auxiliares en la pila Tcp/Ip

<table>
<tr><td>CAPA APLICACIÓN</td><td>HTTP</td><td>…..</td><td>FTP</td><td>TELNET</td></tr>
<tr><td>CAPA TRANSPORTE</td><td>TCP</td><td></td><td>UDP</td><td></td></tr>
<tr><td rowspan="2">CAPA DE INTERNET</td><td>ICMP</td><td>ARP</td><td>IGMP</td><td>ICMPv6</td></tr>
<tr><td colspan="3">IPv4</td><td>IPv6</td></tr>
<tr><td>CAPA DE ACCESO AL MEDIO</td><td>Ethernet</td><td>….</td><td>PPP</td><td>Token Ring</td></tr>
</table>

Ilustración propia - basado en RFC793

3.4.4.1 Protocolo ARP

los cuales se usaban generalmente para identificar las direcciones físicas (MAC) de los dispositivos conectados a la red enviando una solicitud de resolución al broadcast y el dispositivo que correspondía contestaba el llamado. En cambio en IPv6 se crean tablas de vecino más cercano y el multicast en link local.

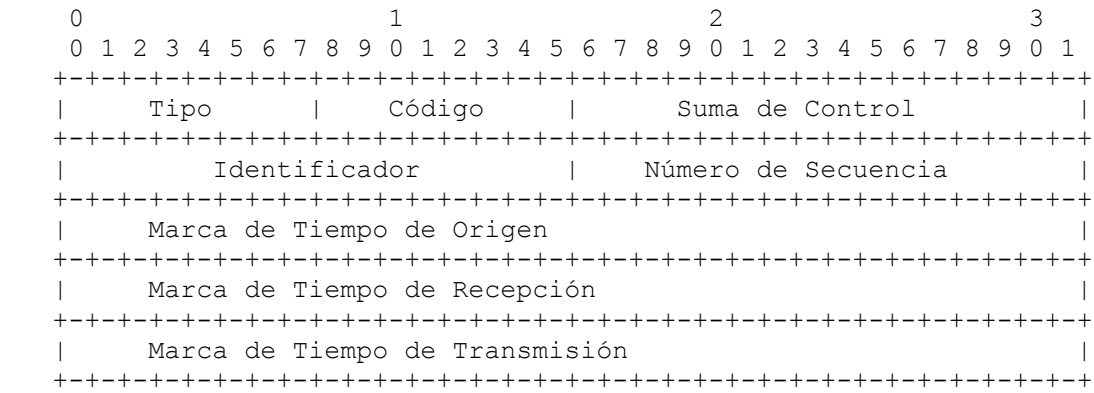
3.4.4.2 Protocolo ICMP

El protocolo de control de mensajes de internet ICMP (Internet Control Messages Protocol)[19] es un protocolo que se ubica en la capa de red y es considerado por algunos como subprotocolo de IP. Las funciones principales en las redes IPv4 son la notificación de errores en las redes y el diagnostico de las interconexiones de las mismas.

El porqué del desarrollo de ICMP radica en que IP no posee ningún control de rastreo a datagramas perdidos o cuando suceden errores en el proceso de transmisión o para verificar el estado de esta interconexión. Por ejemplo, cuando IP descarta un datagrama el origen o destinatario no tienen forma de verificar el estado de la comunicación a menos que se use ICMP.

Cada paquete del protocolo se encapsula dentro de un datagrama IP convencional en el campo de datos y luego es dirigido al destino de manera transparente. Luego es procesado para remitir una respuesta según corresponda. La cabecera de los paquetes ICMP se describen en la Figura 9.

Figura 9. Cabecera el Datagrama ICMP



Fuente IETF RFC792[20]

Para efectos prácticos de la gestión de redes vamos a identificar en la Tabla 2 algunos ejemplos (basados en la documentación oficial de la IANA[21]).

---

[19] RFC792 - Internet Control Messages Protocol, (ICMP) Specification. *Tools.ietf.org*. Fecha de consulta: 9 Mar 2018, from https://tools.ietf.org/html/rfc792

[20] Ibid.

[21] Internet Control Messages Protocol (ICMP) Parameters, IANA Last Updated 2018-02-26, Consultado el 15 Mar 2018 https://www.iana.org/assignments/icmp-parameters/icmp-parameters.xhtml

Tabla 2. Mensajes dentro del protocolo ICMP

Descripción	Tipo	Código	Descripción	RFC
Estado de red host	3	0	red inaccesible	RFC792
		1	"host" inaccesible	
		2	protocolo inaccesible	
		3	puerto inaccesible	
		4	se necesitaba fragmentación pero df estaba activado	
		5	Fallo en la ruta de origen.	
Tiempo de vida (TTL)	11	0	Tiempo de vida superado en transito	RFC792
		1	Tiempo de reensamblaje de fragmentos superado.	
Cabecera IP errónea	12	0	El puntero indica el error.	RFC792
Control de congestión	4	0	Control de congestión	RFC792
	5	0	Redirigir datagramas debido a la red.	RFC792
		1	Redirigir datagramas debido al "host".	
		2	Redirigir datagramas debido al tipo de servicio y la red.	
		3	Redirigir datagramas debido al tipo de servicio y el "host".	
Solicitud/ Respuesta echo	8	0	mensaje de solicitud de eco	RFC792
	0	0	mensaje de respuesta de eco	
Para el mensaje de solicitud / respuesta de marca de tiempo	13	0	solicitud	RFC792
	14	0	respuesta	
Para mensaje de solicitud / respuesta de información	15	0	solicitud	RFC792
	16	0	respuesta	
Anuncio de router	9	0	Anuncio de router	
Descubrimiento de router	10	0	Descubrimiento de router	

Basados en RFC792[22]

ECHO / Ping

Para verificar si un dispositivo se encuentra activo en la red se usa normalmente la herramienta Ping el cual devuelve el estado del mismo.

[22] RFC792 - Ibid.

Host envía solicitud de echo – (Tipo 8 Código 0)

Si el host llega al destino éste regresa su respuesta devolviendo solicitud de respuesta echo – (tipo 0 Código 0).

Si uno de los router no encuentra la red devuelve al host otro mensaje de red inaccesible– (Tipo 3 código 0).

3.4.4.3 Protocolo IGMP

IGMP es el protocolo de red que permite sincronizar enrutadores y grupos de difusión, fue una de las innovaciones finales del ya conocido protocolo IPv4, pero que en IPv6 se vuelve nativo. Con este protocolo los host que hacen parte de algún grupo de multidifusión se enteran y se presentan ante los routers que controlan estos grupos. Este protocolo esta detallado en la RFC 3376 que ya va por la versión 3.

3.4.4.4 Protocolo DHCP

Es el protocolo de configuración dinámica de host del inglés Dynamic Host Configuration Protocol (DHCP) que permite la asignación de direcciones IP a los Host de una red a través de una arquitectura cliente/servidor. Al Servidor se le delimita el rango de direcciones IP sobre el cual tiene administración y las va asignando a los host en la medida que la solicitan, de igual forma cuando un host termina sesión y se libera la dirección para poder ser asignada a otro host solicitante; de todo esto el Servidor guarda trazabilidad sobre la IP, tal y como lo establece la RFC 2131 para IPv4 y la RFC 3315 para IPv6.

3.4.5 Protocolo IPv6

Para el año 1993 la IETF encontró que las direcciones que son administradas por la IANA y son asignadas para su uso serian asignadas pronto, por lo que cito a concurso público la estructuración de un nuevo marco de referencia para el internet de nueva generación (ING o NGN). El desarrollo de este nuevo conjunto de protocolos es lo que se conoce como IPv6. Como resultado el IETF expidió en 1995 la RFC1883 donde expuso la primera versión de la especificación de IPv6 o IP de nueva generación (IPng)[23]. El avance y desarrollo de dichos protocolos se evidencian en la Tabla 3. Número y estado de los RFCs en el IETF el continuo desarrollo de los protocolos IPv4 e IPv6.

---

[23] RFC1883 - Internet Protocol, Version 6 (IPv6) Specification. *Tools.ietf.org*. Fecha de consulta: 7 October 2017, from https://tools.ietf.org/html/rfc1883

Tabla 3. Número y estado de los RFCs en el IETF

Estado IETF	IPv4	IPv6
Informativo	933	374
Experimental	151	59
Mejores prácticas actuales	86	34
Normas propuestas	772	407
Estándares en borrador	48	17
Entandares completos	48	5
Total	2038	896

Adaptación propia según Fuente Townsley M, (2009)[24]

El protocolo IPv6 es una evolución del bien conocido protocolo de transporte (enrutamiento) IPv4, por lo que además de ampliar el rango de direcciones en internet, el nuevo protocolo apunta a subsanar errores presentes en IPv4, así como nuevas funcionalidades como la posibilidad de tener comunicación punto a punto.

3.4.5.1 Características de IPv6

Dentro de las principales características que definen el protocolo IPv6 está el aumento en la diversidad y rango de direcciones y sus procesos de autoconfiguración, el establecimiento de un encabezado fijo, la necesidad de una metodología de agregación, la implementación nativa del estándar IPSEC en IPv6, el aumento de conexiones y su movilidad para los llamados dispositivos nómadas y la posibilidad de tener conexiones de extremo a extremo.

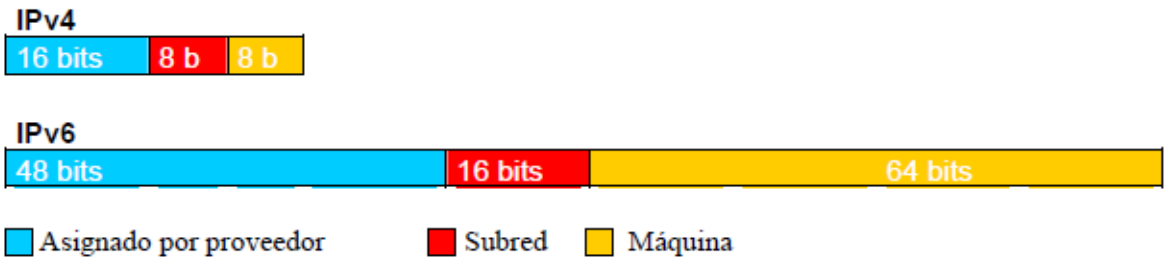
Una de las fortalezas de IPv6 es el direccionamiento que se define como una serie de 128 bits y que para su administración se establece como de 32 dígitos en formato hexadecimal como se puede ver en la Figura 10.

Este tipo de direccionamiento provee a la IANA y sus subsidiarias un conjunto de 2^{128} hosts que es aproximado de 3,402823669×1038 por lo que se garantizaría a muy largo plazo su asignación y de paso cambia la forma, por ejemplo, de hacer un escaneo de red y puertos pues por la cantidad de host posibles por redes y puertos por host los tiempos de escaneo se vuelven imposibles de realizar con la tecnología actual.

---

[24] Townsley M, (2009), IPv6 & the IETF, CISCO & IETF. Recuperado de http://www.cu.ipv6tf.org/pdf/CAA7ULEL.pdf

Figura 10. Cambio en el espacio de direccionamiento con IPv6



Fuente NEconomia UNAM 2017

Para su asignación la IANA y sus subsidiarias proveen un total de 2^{48}redes que se son asignados normalmente a los proveedores ISP locales o nacionales, estos a su vez, reparten conjuntos más pequeños de subredes los cuales se pueden mediante distintos métodos asignar a los hosts o dispositivos que se tengan en la red.

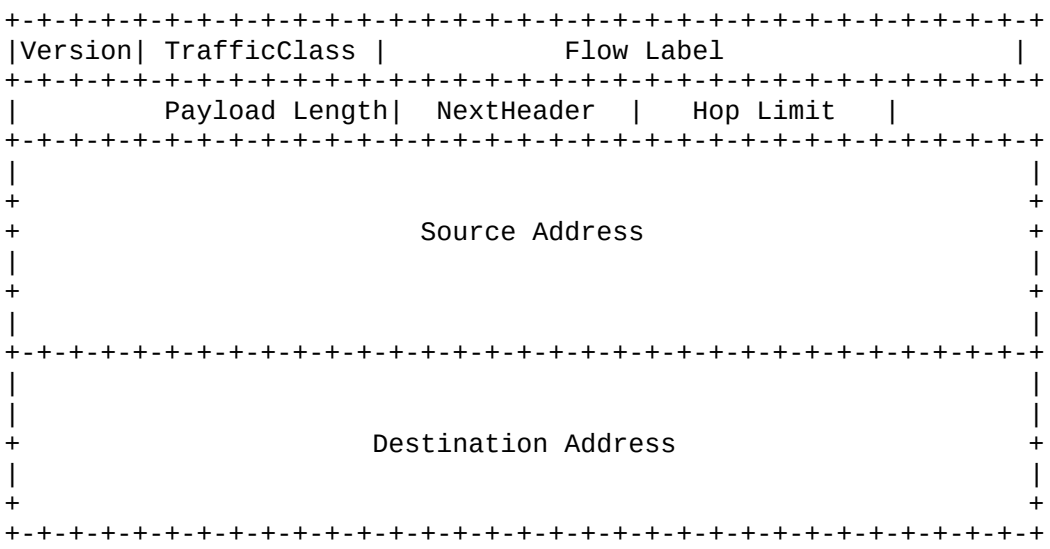
Así mismo el protocolo define que los datagramas aunque pueden tener tamaños distintos según lo defina el protocolo auxiliar llamado MTU (Maximum Transmission Unit Unidad máxima de transmisión), viajaran por la red sin modificarse. Esto como consecuencia hace que el host que inicia la comunicación envíe los paquetes con un tamaño definido y a su vez los dispositivos como routers ya no pierdan tiempo calculando tamaños de paquetes o ensamblando y desensamblando los mismos en el transcurso de la comunicación.

3.4.5.2 Encabezado IPv6

El encabezado del paquete también cambió en IPv6 pasando de 12 a 8 campos los cuales tienen un tamaño total de 320 bits (128 para el origen y 128 para el destino), el tamaño de paquete mínimo para una transmisión. Dicha cabecera la podemos ver en la Figura 11 con sus respectivos campos.

En el protocolo IPv6 se ha eliminado la constante interacción de capa enlace (ARP) y por ende el costoso tráfico de Broadcast en cambio en IPv6 se crea las tablas de vecino más cercano y el multicast en link local.

Figura 11.Cabecera el Datagrama Internet IPv6



Cabecera el Datagrama Internet – Fuente IETF RFC2460

3.4.5.3 Nuevos campos en el encabezado IPv6

Pese a que en el protocolo IPv6 sólo aparece un campo nuevo Flow Label es importante hablar del campo de servicio, pues a la fecha Flow label no es usado en cambio el campo QoS ha tomado gran importancia en este protocolo.

3.4.5.4 Calidad de servicio (QoS)

Es el nuevo campo del protocolo IPv6 que permitirá tener un nivel de servicio diferencial según el tipo de tráfico. Si cuento con este campo puedo dar preferencia a las aplicaciones críticas en una red de recursos compartidos. Este concepto implica mecanismos de verificación y evasión de la congestión de manera que se preferencia a ciertos tipos de tráfico logrando un rendimiento más predecible y un ancho de banda más eficiente. Este campo está inspirado en el campo Traffic Class de IPv4 que casi nunca se uso realmente por lo que su valor más conocido fue cero (0) que significa que no requiere calidad especial. Este campo tendrá gran relevancia en las próximas aplicaciones pues ante el gran universo de dispositivos que puede llegar a tener una red IPv6 empresarial se hace importante priorizar el tráfico.

Niveles del campo calidad de servicio

Mejor Esfuerzo: Es la opción por defecto. La red se encarga de entregar los paquetes a su destino, pero sin garantía de ello. Se recomienda para aplicaciones del tipo FTP o HTTP.

Servicios Integrados: Esta opción hace que se negocien algunas características de la red de manera que provea a las aplicaciones un grado de servicio. La aplicación solicita la QoS que requiere para que la red reserve esos recursos para comenzar a operar.

Servicios Diferenciados: Conjunto de herramientas para clasificación según los requerimientos de la aplicación y los protocolos que establecen prioridades sobre el resto de la red. Estos tres niveles están ampliamente descritos en la RFC 1633.

3.4.5.5 Flow Label:

En este momento no es muy aplicado especialmente cuando se habla de tráfico fragmentado o con encriptación o por el uso de las cabeceras de extensión. Se creó con el fin de etiquetar los paquetes de un flujo. Su valor por defecto es cero (0) que indica que el paquete no pertenece a ningún flujo.

3.4.5.6 Cabeceras de extensión

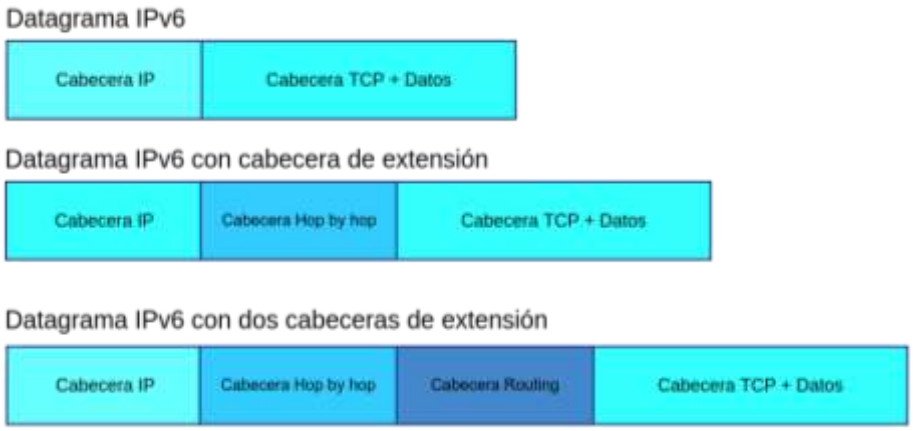
Las cabeceras de extensión llevan la información opcional que requiera una transmisión por lo que existe posibilidad de añadir nuevas funcionalidades al protocolo IPv6 a través de nuevas cabeceras. En la Tabla 4 se puede ver las características y descripción de las cabeceras de extensión. En el momento hay 6 cabeceras de extensión activas.

Tabla 4. Cabeceras de extensión

NOMBRE DE LA CABECERA	ID	DESCRIPCIÓN
Hop by hop	0	Es leída por cada router de la ruta del paquete
Destination Options	60	Es la información para el nodo destino del paquete. Es la única cabecera que se puede repetir.
Fragment	44	Es poco común porque se usa descubrimiento de camino MTU para determinar la unidad máxima de transmisión entre los nodos extremos. Cuando una aplicación no puede ajustar su tamaño de paquete, el nodo origen usa la cabecera de fragmentación para dividir el paquete, en el nodo destino se desfragmentara.
Authentication	51	Parte de IPSec que proporciona integridad sin conexión, autenticación del origen de datos y protección anti replay.
Encapsulating Security Payload	50	Esta cabecera dota de seguridad los datos o payload. Proporciona integridad, autenticación, confidencialidad y servicio anti replay.
Destination Options	60	Es la que se puede repetir.
Mobility Header	135	Esta cabecera está reservada para los dispositivos móviles para que puedan saltar de una a otra red sin perder conexión.
Routing	43	Funciona similar a las opciones loose source record route de IPV4, es decir define 1 o más nodos intermedios que deben ser incluidos en la trayectoria del paquete.
No Next Header	59	Indica que es el último paquete de un mensaje.

Como se describe en la Figura 12 donde se evidencia que los datagramas IPv6 contienen un encabezado y que dependiendo de la comunicación puede llevar un nuevo encabezado.

Figura 12. Ejemplo de paquetes IPv6 con cabeceras de extensión



Diseño propio basado en IPv6 specification

3.4.5.7 Direccionamiento

La IANA asignó el direccionamiento de IPv6 en octavos (⅛), es decir que de todo el conjunto disponible de direcciones IPv6 posibles dicha entidad ha subdividido el conjunto de direcciones en ocho espacios los cuales se pueden ver claramente en la Figura 13, los cuales se han distribuido de manera que los RIR entregan a sus usuarios de una manera coordinada y organizada.

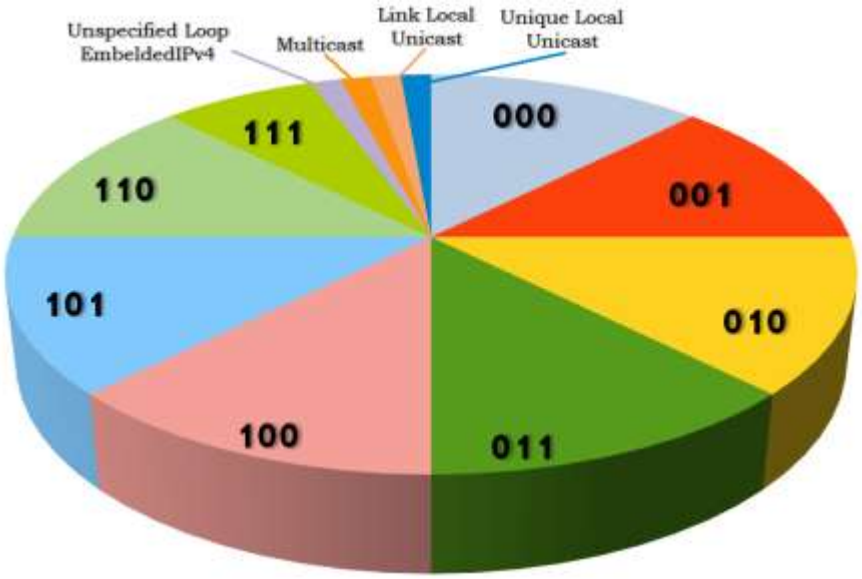
La IANA entrega espacios de asignación /23 (RFC4291)[25] a los RIR estos, a su vez entregan a los ISP /32 y estos últimos entregan a los clientes que lo requieran espacios de direccionamiento equivalentes a /48 (RFC6177)[26]. Dependiendo de la cobertura de sus redes los clientes pueden distribuir / 56 para las sucursales y /64 para las subredes.

---

[25] RFC4291 - Internet Protocol, Version 6 (IPv6) Specification. *Tools.ietf.org*. Fecha de consulta: 7 Febrero 2018, from https://tools.ietf.org/html/rfc4291

[26] RFC6177 - Internet Protocol, Version 6 (IPv6) Specification. *Tools.ietf.org*. Fecha de consulta: 7 Febrero 2018, from https://tools.ietf.org/html/rfc6177

Figura 13. Distribución de la asignación de direcciones IPv6



Diseño propio basado en esquemas de la IANA– Fuente IANA

3.4.5.8 Notación De Los Prefijos

Un prefijo corresponde a los Bits de Mayor Peso (Prefijo de Enrutado Global) dentro de una dirección IPv6, con ellos se identifica el tipo de dirección y sirve para identificar la red o las subredes (RFC 4291). Este formato está basado en la notación de prefijo que propuso en su momento la CIDR por lo que una vez se cita la dirección IP se debe indicar la cantidad de bits que conforman el ID de la red, a esto se le conoce como la Longitud de Prefijo. Es con el prefijo que los routers dirigen los paquetes a su destino. La IANA estableció prefijos de enrutamiento global, de enrutamiento privado, reservados y direcciones especiales.

Ejemplo: En la dirección IPv6 **2EDE:DA11:3**311::/36, se indica que los primeros 36 bits conforman el prefijo y eso nos lleva a que el prefijo corresponde a:**2EDE:DA11:3** **(**corresponde a lo marcado en azul**)** esta es la parte de identificación de la Red.

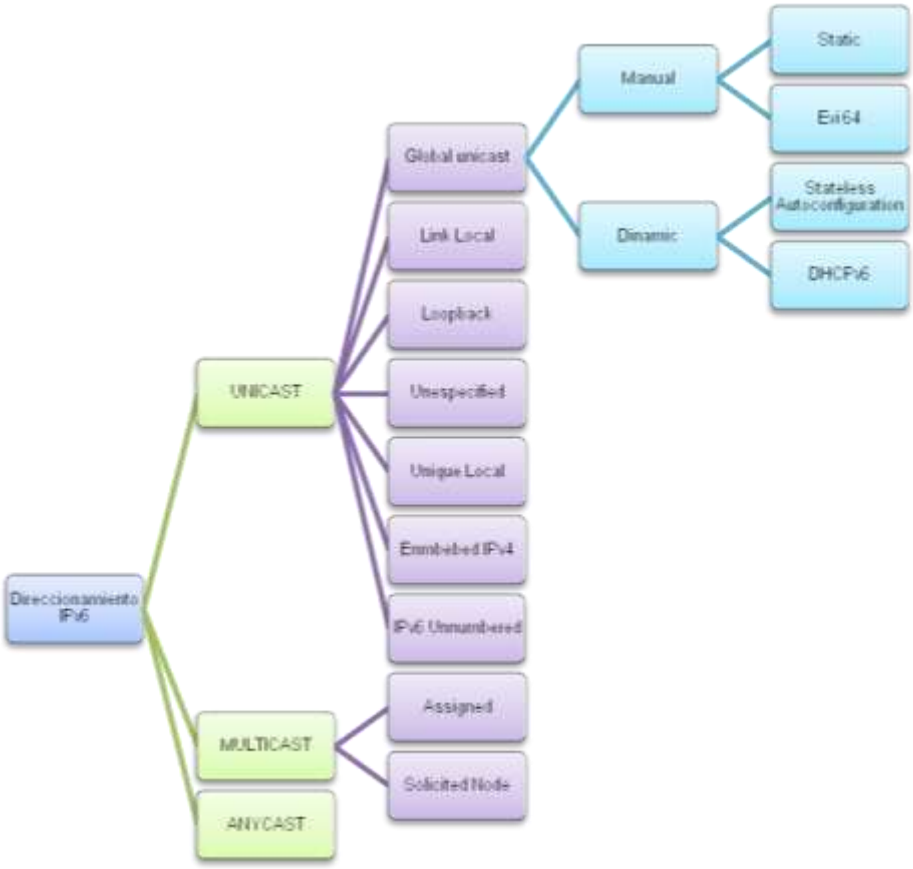
3.4.5.9 Direccionamiento IPv6

Las direcciones IPv6 están conformadas por 128 bits, pero organizadas en dos bloques de 64 bits para aprovechar las nuevas arquitecturas de procesadores de 64 bits. La cantidad de direcciones posibles equivale a 2 elevado a la 128 (2^{128}) que es una cifra extremadamente grande.

La RFC 4291 clasifica las direcciones en tres tipos a saber: las unicast, multicast y anycast. Las direcciones Unicast se usan en comunicación (emisor receptor)

individuales es decir son direcciones únicas, de tal forma que si se envía un paquete a esta dirección unicast sólo lo recibirá ese dispositivo. Esta clasificación la podemos ver en la Figura 14. Las direcciones Multicast engloban varios equipos, haciendo que los receptores de un envío de paquetes de una dirección multicast solo sean los dispositivos que tienen esa misma dirección multicast (broadcast controlado). Por su parte las direcciones Anycast engloban varios dispositivos, pero al hacer un envió a esa dirección, el paquete llegará sólo al que se encuentre cerca y que tenga dicha dirección como podemos ver en la Figura 15.

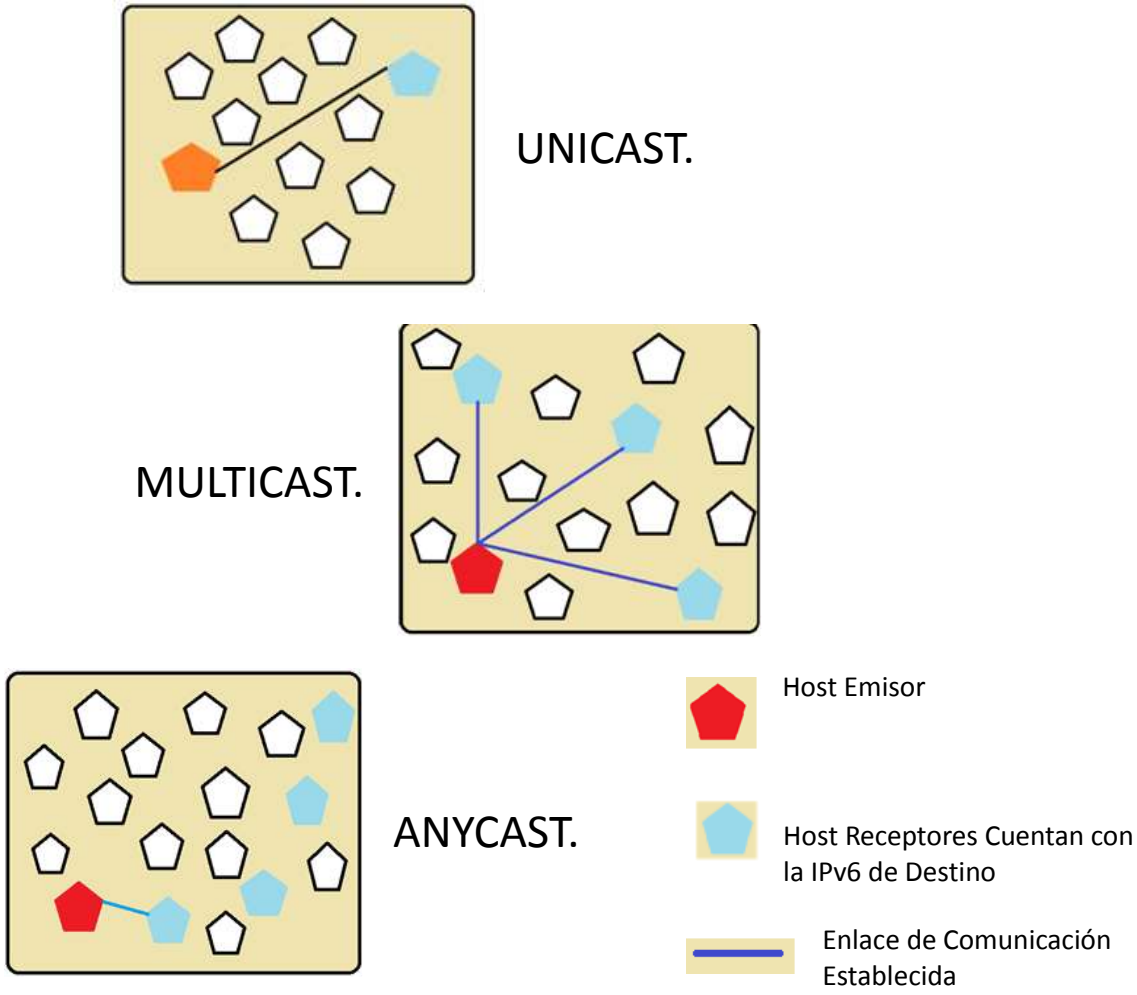
Figura 14. Direccionamiento IPv6



Diseño propio basado en el RFC 4291– Fuente IETF

En IPv4 las interfaces de red por lo general solo tienen una dirección del rango 192.168.0.10, sólo en situaciones excepcionales se asignaban más de una Ip a una interfaz, como cuando tengo "interfaces de red virtuales" para ofrecer diferentes servicios de red por cada IP configurada.

Figura 15.Tipos de Direcciones IPv6



Diseño propio basado en la RFC 4260 – Fuente Autores

En IPv6 lo común es que les sean asignadas varias direcciones a las interfaces de red, la RFC 4291 determina mínimo las direcciones IPv6 que un host debe tener IPv6 las cuales serían: La dirección de Loopback, una dirección de enlace local por cada dispositivo, direcciones unicast y anycast que se requieran, Una dirección multicast el segmento de red, por cada dirección unicast y anycast se asigna una dirección multicast de nodo solicitado y las direcciones de grupos de multidifusión que se haga parte.

La RFC 3484 establece como seleccionar la dirección IPv6 predeterminada de varias direcciones para ello presenta dos (2) algoritmos generales, con uno para cada dirección (origen y destino). Es obligatorio que todos los nodos de una red IPv6 soporten esta RFC. El comportamiento esperado de los nodos IPv6 se especifica con estos algoritmos, esto no quiere decir que sea obligatoria y el

comportamiento puede ser asumido según la programación de los protocolos o aplicaciones de capas superiores.

Las direcciones IP son asignadas a las interfaces con un tiempo de uso, mientras esté vigente ese tiempo de uso, se habla de una dirección preferida. La dirección está en estado de obsoleta o deprecated cuando se expira ese tiempo y hasta que se libera la dirección, en este estado la dirección aún se puede usar, pero no es lo recomendado.

3.4.5.10 UNICAST

Direcciones Globales Unicast: Estas direcciones deben tener sus 3 primeros bits en 001, su prefijo es 2000::/3 (RFC 4291). Estas direcciones se corresponden con las direcciones públicas de IPv4 (nivel global) y por ello deben ser direcciones controladas en una primera asignación por la IANA y luego por los ISP (ver Figura 16). Teniendo en cuenta el nibble del prefijo existe la posibilidad que el 4 bit sea 1 o 0 estas direcciones inician por 2000 o 3000, sin embargo, la IANA tiene restringidos ciertos rangos, para una futura asignación.

Figura 16. Estructura de la dirección unicast global

Prefijo de Enrutado Global		
001 + 45 bits	Identificador de Subred	Identificador de Interfaz
3 bits primeros obligatorios **001**	16 bits	64 bits
64 bits		64 bits

Fuente Los autores

El Prefijo de enrutado global: Se restringe a las direcciones asignadas a la red, para una red pequeña el prefijo es de 48 bits y es gestionado por los RIR e ISPs tres bits + 45 (ver Figura 17).

Figura 17. Espacios Reservados

PREFIJO	DETALLE PREFIJO	RESERVADO PARA	RFC
2001::/23	2001:0000::/32	Teredo	4380
	2002:0000::/16	6to4	3056

Fuente Los autores

Identificador de Subred: Por lo general son los 16 bits siguientes al prefijo de enrutado global (48 bits) para hacer subredes en una organización, lo que da la posibilidad de tener 65.535 subredes. Este identificador es de administrador local; si requiere más subredes debe solicitar un prefijo de enrutado global menor de 48 bits.

Identificador de Interfaz: Conjunto de bits único en una subred, correspondiente a los bits de host de IPv4, identifica una interfaz en una subred. El ID de Interfaz se puede asignar por Configuración Manual, Autoconfiguración (EUI-64 exclusividad basado en MAC), Configuración dinámica (DHCPv6), Identificador de Interfaz Aleatorio e Identificador generado criptográficamente.

Direcciones Unicast Local Única (ULA Unique Local Unicast Address): Estas direcciones tienen sus primeros 7 bits de mayor peso en 1111 110 y su prefijo es FC00::/7. En sus inicios fueron conocidas como Direcciones de Sitio Local y hoy se les conoce como Dirección IPv6 Local. Pese a ser direcciones UNICAST a nivel global NO deben enrutarse para no generar conflicto pues están diseñadas para el uso local en sitios corporativos y conjuntos de redes (RFC 4193). A través de su prefijo global único se puede implementar su filtrado en los límites de la red (ver Figura 18).

Figura 18. Formato de Direcciones Unicast Local Única

1111 110	**L**	**Identificador Global**	**Identificador de Subred**	**Identificador de Interfaz**
Prefijo	Si L=1, el prefijo ha sido asignado localmente.	40 bits	16 bits	64 bits
FC::/7	L=0 No se ha definido.			

Fuente Los autores

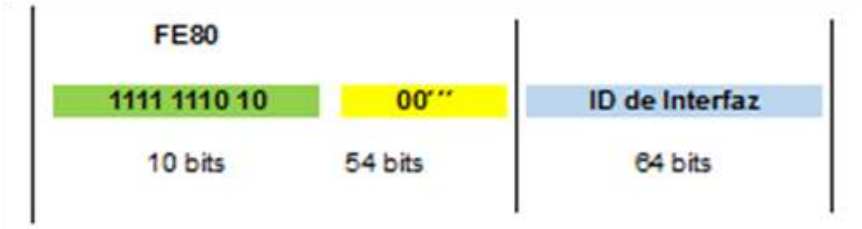
Las ULAS fueron concebidas para permitir la interconexión de redes evitando que surjan conflictos por direcciones duplicadas, esto maximiza estos procesos de interconexión que de otra manera llevarían a tareas de remuneración de una de las redes, además no se requiere la intervención de los ISPs pues no requieren Internet, por ejemplo, por las aplicaciones de la organización en lugar de las direcciones unicast globales.

Cuando L=1 el prefijo es local y pasaría de FC00::/7 a **FD::/8** (1111 1101), además el Identificador Global se genera con un algoritmo pseudo-aleatorio de altísima probabilidad de exclusividad. El algoritmo toma la estampa de hora y fecha del NTP (Network Time Protocol 64 bits), luego se calcula un identificador EUI - 64 con la dirección física, se unen estos dos datos y a la concatenación se aplica el

algoritmo SHA-1por último se toman para el identificador global los 40 bits menos significativos.

Direcciones Unicast de Enlace Local (Local-Link Address): Son aquellas direcciones cuyos primeros 10 bits son 1111 1110 10 y su prefijo es **FE80::/10** de asignación automática. Asemejan a las direcciones privadas de IPv4 del rango 169.254.0.0/16 (RFC 1918) con las que se identifican a los nodos de una red. No son enrutables en internet (ver Figura 19). Estas direcciones las puede utilizar el protocolo Neighbor Discovery para autoconfiguración, también se pueden usar en redes que no requieren router o para crear redes temporales. El prefijo de estas redes es de enrutado Local y no Global.

Figura 19. Estructura de direcciones Local-Link Address



Fuente los autores

Direcciones No Especificadas:(Unspecifiedaddress): Es la dirección de todo en ceros y se corresponde a la IPv6 :: que tiene por función, la misma que en IPv4,ser la dirección de origen cuando un host no cuenta con una IP válida y se requiere una configuración de arranque, por ejemplo, para asignar la configuración de la tarjeta de red.

Dirección de Loopback: Corresponde a la dirección ::1, al igual que con la dirección anterior es el equivalente a en IPv4 (127.0.0.1).Con esta dirección se pueden hacer pruebas en el host que permitan establecer la actividad de la dirección o de algún servicio.

Direcciones Reservadas: Reservadas por la IETF: Las que empiezan con 8 ceros su prefijo sería:0000::/8.

3.4.5.11 MULTICAST

Las direcciones Multicast son direcciones cuyo prefijo de red empiezan por FF lo que en binario representa 1111 1111, dicho de otra forma, tienen sus primeros 8 bits en 1 lo establece por prefijo de este tipo de direcciones a **FF00::/8**. Estas direcciones agrupan nodos por lo que forman los llamados grupos de multidifusión. Un host puede estar en varios grupos de multidifusión. Los paquetes enviados a una dirección Multicast garantizan que todos los miembros del grupo procesen el

paquete. Como ya comentamos los primeros 8 bits de este tipo de direcciones identifican que se trata de una dirección Multicas, podemos ver en la Tabla 5 más a fondo la arquitectura de este tipo de direcciones:

Tabla 5. Esquema de una dirección Multicast

IDENTIFICADOR MULTICAST	**FLAGS**	**SCOPE**	**IDENTIFICADOR DEL GRUPO**
←8 bits→	←4 bits→	←4 bits→	←112 bits→
Son los 8 primeros bits y q están marcados como FF	Marca las banderas ORPT. (O).Por ahora este primer bit es cero, pues la IANA lo ha reservado para un futuro. (R). Este bit indica si la multidifusión incluye Rendezvous Point (RP). Es un problema con multicasting entre dominios, el protocolo usado (PIM - SM) impide informar a los dominios de multidifusión las fuentes de multidifusión disponibles. La RFC 3956 da pautas de cómo debe ser la dirección de un grupo multicast y su bit de "Rendezvous Point" (RP). (P) Da información sobre el prefijo (asignación dinámica de direcciones multicast, RFC 3306). (T) indica si la dirección es permanente de las Bien Conocidas (Well-known) definidas por la IANA, o es una dirección temporal.	Establece el alcance de la difusión de la dirección. Sus valores posibles son: 0 Reservado 1 Interfaz local 2 Enlace local 3 Realm Local 4 Admin Local 5 Site Local 6 Sin asignar 7 Sin asignar 8 organización Local 9 Sin asignar D Sin asignar E Global (Internet) F Reservada Ejemplo 1: La dirección FF02::1 es la dirección "Link Local AllNodes", lo que garantiza un envío de paquetes a todos los nodos de la subred. Se	Limitan los paquetes multicast enviados. Cuando finaliza en 2 indica a todos los routers y cuando el grupo termina en 1 indica a los host Por ejemplo, si el identificador de grupo termina en 1 (AllNodes) y su ámbito es 2 (Scope = 2) estamos alcanzando a todos los nodos del enlace local (Subred).

		puede equiparar esta dirección a la "255.255.255.255" en IPv4. Ejemplo 2: La FF02::2, es la dirección que corresponde a todos los routers del enlace para RS (Router Solicitation).	
FF →1111 1111 atendiendo a su valor en binario.	ORPT. O=0 al 2018 R=0 cuando no lleva (RP) P=0 No envía información del Prefijo. T=0 Well-known	Estos valores están definidos en las RFC 4291 y RFC 7346.	Corresponde a 112 bits

Fuente los autores basado en las RFCs de Multicast

A continuación, haremos mención a algunas direcciones multicast de alta importancia en IPv6:

Dirección Multicast De "Nodo Solicitado" (Solicited-Node): Es la dirección Multicast que tienen todos los nodos en sus direcciones unicast y anycast, se usa con el Protocolo de Descubrimiento de Vecinos (Neighbor Discovery RFC 4291).

En IPv4 para comunicarse con un nodo del cual se conoce la IP se usa el protocolo ARP para resolver su MAC, la búsqueda es por difusión broadcast en todos los hosts del segmento de red, lo que hace que se congestione el canal. En IPv6 se resuelve la MAC de una IP a través un mensaje de descubrimiento de vecino a la dirección multicast de "nodo solicitado", liberando a la red de un tráfico innecesario.

La Dirección de Nodo Solicitado se conforma con un prefijo de 104 bits de una dirección multicast bien conocida (ver Tabla 6) está entre las direcciones: FF02:0:0:0:0:1:FF00:0000 y la FF02:0:0:0:0:1:FFFF:FFFF y para los 24 bits menos significativos añade los bits correspondientes de la dirección IP del nodo. Veamos, para el host de MAC 00-18-F8-29-D1-D7, su dirección local sería FE80::218:F8FF:FE29:D1D7 y la de nodo solicitado será FF02::1:FF29:D1D7. En IPv6 por cada dirección unicast/anycast el host tendrá una dirección de nodo solicitado.

Tabla 6. Principales direcciones Multicast bien conocidas

DIRECCIÓN	DESCRIPCIÓN
FF02::1	Todos los nodos del segmento de red
FF02::2	Todos los routers del segmento de red
FF02::5	Todos los routers del segmento de red OSPFv3
FF02::9	Todos los routers del segmento de red RIP
FF02::A	Todos los routers del segmento de red EIGRP
FF02::D	Todos los routers del segmento de red PIM
FF02::16	Todos los routers del segmento de red MLDv2
FF02::1:2	Todos los servidores DHCP del segmento de red
FF02::1:3	Todos los servidores DHCP de la red local
Ff0x::fb	Multicast DNS
FF0x::101	Network time Protocol
FF0x::102	Network Information Service

Fuente Los Autores

Direcciones Anycast: Estas direcciones son un subconjunto de las direcciones Unicast, por lo que es imposible reconocerla por su prefijo. Las direcciones anycast pueden ser asignadas a más de una interfaz y de diferente nodo según la RFC 1546 (1993) a nivel experimental para IPv4 para ser usadas en DNS y HTTP. Es por ello que las direcciones Anycast se establecen a través de una Dirección Unicast Compartida, lo que equivale a asignar direcciones unicast comunes a varias interfaces, ejemplo de este método son los servidores DNS raíz en Internet.

Con Anycast sé obtiene el servidor más cercano y apropiado para un servicio bajo las características de redundancia y de balanceo de carga que requieren las aplicaciones de hoy, para ellos es necesario configurar la dirección unicast en todas las interfaces que se requiera y configurar esos nodos para que vean la dirección anycast.

Cuando un cliente envía un paquete a un dominio, un conjunto de routers darán acceso al router disponible más cercano, siempre que ellos tengan una dirección única Anycast configurada como se puede evidenciar en la Figura 20. Veamos con un ejemplo el funcionamiento de estas direcciones: Cuando una estación envía un

datagrama a la dirección anycast, el enlace determina la ruta menor para alcanzar a uno de esos host que reciben paquetes dirigidos a esa dirección anycast. Estos esquemas son muy usados en algunos mecanismos de transición como 6to4 (RFC 3068) y en tecnologías como Mobile IPv6. En este tipo de comunicaciones el emisor desconoce la interfaz de recibo ya que esto lo define el protocolo de enrutamiento y por ello se pueden presentar las siguientes situaciones:

Que lleguen a diferentes host los envíos de un mismo emisor, lo que complica el envió de fragmentos de un mismo paquete o el establecimiento de una comunicación.

Como ya ha sido comentado el prefijo de subred es el prefijo que identifica un segmento de red.

La dirección anycast de una interfaz de enlace tiene el identificador de interfaz en ceros.

Teniendo en cuenta que la dirección expuesta es la anycast del/los routers de subred, cada paquete que se envié a esta dirección anycast será entregado a un Router del segmento (ver Figura 20). Este esquema requiere que todos los routers cuenten con soporten para direcciones anycast de la red a las que tiene acceso la interfaz.

Figura 20. Estructura de una dirección Anycast (subnet-router anycastaddress)

PREFIJO DE SUBRED	IDENTIFICADOR DE INTERFAZ
Identifica un enlace determinado	0000 0000 ….
n bits	(128 – n) bits

Fuente Los Autores

3.4.5.12 Asignación dinámica de direcciones multicast

Según la RFC 3306 los prefijos unicast se transmiten por direcciones multicast, para ello se afectan los últimos 112 Bits (ID Grupo) del formato multicast para que lleve el prefijo (ver Figura 21).

Figura 21. Formato modificado quedaría así:

RESERVADO	P-LEN	PREFIJO DE LA RED (Para la Dir. Unicast)	ID GRUPO
←8 →	←8 →	←---------64 --------→	←32 →

Fuente Los Autores

En el formato original de la dirección multicast la bandera "**P**" indica si la dirección multicast contiene información de prefijo (P=1), si P=1 la bandera "T" también se pondrá en 1 lo que indica que se trata de una dirección multidifusión temporal y no de una Well-known. La otra modificación es el campo Reservado que valdrá 0 cuando P = 1. El campo de Scope no tiene alteración en su funcionalidad. El campo P-LEN indica la longitud del prefijo de la Ip unicast. Longitudes menores a 64 bits, ponen en 0 los bits no utilizados.

3.4.6 La seguridad en la pila de protocolos IP

3.4.6.1 IPSec

El estándar de seguridad en IP se introdujo de manera que es compatible con IPv4 e IPv6, en este último el estándar es obligatorio aunque viene apagado por defecto. El estándar es en realidad una serie de protocolos los cuales proveen un método de seguridad extremo a extremo en los datos de los paquetes IP.

El cifrado se realiza normalmente en el host de envío y es desencriptado en el receptor. Estas llaves criptográficas se realizan usando algoritmos criptográficos complejos. Estos algoritmos dependen de normalmente de la implementación realizada. Puede ser usado en implementaciones de transporte (transporte mode) o en tunnel mode este último usado en implementaciones como el dual stack (medio para proveer comunicación entre IPv4 e IPv6).

AH: Dentro de IPv6 se implemento como una cabecera de extensión que brinda Integridad, Autentificación del origen de datos y Opcionalmente servicio anti-replay.

ESP: Estipulada como otra cabecera de extensión independiente de la AH, brinda los de la cabecera AH más confidencialidad que debe usarse en conjunto con la opción de integridad.

En los inicios del protocolo IPv6 la RFC4294 hizo obligatorio que cualquier pila IPv6 tuviera soporte para IPSec, pero en las implementaciones se fue notando que no todas lo requerían, hay implementaciones mínimas que no pueden permitirse IPSec, pues no todos los dispositivos los soportan y no todas las implementaciones lo requieren. Adicional se descubrió que la cabecera de

extensión IPSec (ESP) no permite ser inspeccionada, por lo que en 2011 se promulga la RFC6434 en donde IPSec deja de ser obligatorio para las implementaciones estándar. Una de las grandes bondades de IPSec es el envío de información cifrada al punto que los firewalls no la pueden inspeccionar, la inspección de este tipo de paquetes requiere su desfragmentación y revisión por ejemplo en un sandbox.

Dentro de los objetivos de IPSEC se encuentra dar seguridad criptográfica sin afectar la infraestructura de red que carece de IPSec. Los protocolos AH, ESP e IKE son independientes del cifrado de IPSec y de sus algoritmos. Así las cosas con IPSec se puede dar acceso controlado, Confirmación de la identidad (origen de los datos), Integridad (UDP), Protección contra re-actuación y discreción en el flujo de tráfico. En las implementaciones IPSec es obligatorio el soporte de ESP pero opcional el soporte a AH.

3.4.6.2 Elementos básicos de IPSec

La RFC 4301 da la Arquitectura Base de IPSec y el concepto de asociaciones de seguridad tan propio de este esquema de seguridad. Los Protocolos de Seguridad de IPv6 son los de Autenticación de la cabecera (AH RFC4302) y el de Encapsulamiento de seguridad de datos (ESP RFC4303) incluyendo la gestión de claves (Manual yAutomáticaRFC7296). En cuanto a los algoritmos de autentificación tenemos la RFC 7321 para AH y ESP y la RFC 4307 para IKEv2.

IPv6 maneja el concepto de Asociaciones de Seguridad (SA) que es básico y es una simple conexión que provee seguridad al tráfico que transporta, este concepto es aplicado en las extensiones AH y ESP. Las SA requieren del protocolo IKE para su establecimiento y mantenimiento; en una comunicación bidireccional típica se requieren dos SAs, una por nodo. Las SAs se identifican unívocamente por tres factores, a saber:

1. El Índice de Parámetros de Seguridad (SPI) es un conjunto de bits asignado a la SA, que apunta a su base de datos SAs.

2. La Dirección IP Destino que puede ser una dirección Unicast, Multicast y en los casos de IPv4 una de Broadcast.

3. El Identificador del protocolo de seguridad.

3.4.6.3 Como opera IPSec

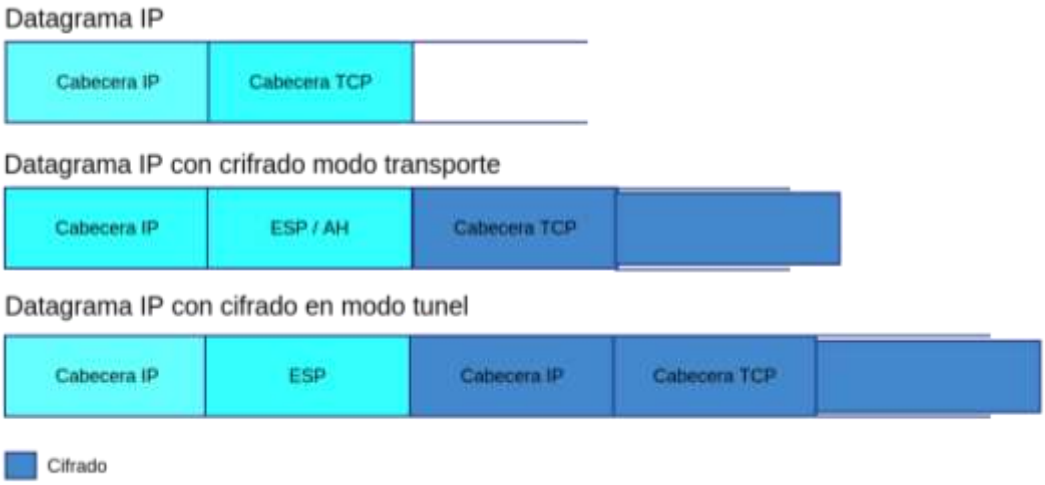
IPSec convierte un dispositivo en un gateway de seguridad similar a un host independiente. La base de datos SAs establece que protección ofrecerá IPSec. De acuerdo a la información de de las cabeceras IP y ‘nextlayer’ se clasifica el paquete para buscar coincidencias en la Base de Datos SAs. Los paquetes pueden ser DESCARTADO o PERMITIDO. IPSec usa uno o más “caminos” entre

dos hosts, pasarelas de seguridad y su combinación. Como venos en la Figura 22 IPSec tiene dos modos de uso:

Modo Transporte: Está pensado para capas superiores, es una comunicación directa entre dos extremos donde soporten el protocolo.

Modo Túnel: Encapsula paquetes IP, es decir que los datagramas son encapsulados totalmente y este a su vez es dispuesto en un nuevo datagrama para ser enrutado.

Figura 22. Modos de IPSec



Fuente Los autores

3.4.6.4 Seguridad perimetral

Tiene por premisa que la seguridad de un host depende del punto de la red donde se conecte. Se fundamenta en:

Piensa que los nodos internos son confiables y que las amenazas a considerar son externas, también que los nodos internos tiene poca o nula conectividad externa, ellos no requieren ser accedidos desde afuera. Este modelo tampoco contempla las puertas traseras. Por ello conlleva cierta simplicidad y madurez pero tiene desventajas como la dependencia del firewall, descuida posibles amenazas provenientes del interior de la red.

3.4.6.5 Seguridad distribuida

Está fundamentada en tres pilares, a saber: Un lenguaje de especificación de políticas, un protocolo de intercambio de políticas y la autenticación de las entidades. Entonces con el lenguaje se define la política de seguridad y se

distribuye a los hosts a través del protocolo, los hosts y todas las entidades de la red deben autentificarse para que sean confiables.

Los supuestos de la Seguridad Distribuida son: Se parte del hecho que los host son identificables de forma unívoca y segura y su lugar de conexión en la red no es relevante para efectos de la seguridad. Las amenazas vienen de cualquier parte de la red. Si las políticas lo permiten un host puede ser alcanzable por un equipo externo por ello la seguridad se puede escalar a las demás capas: red, transporte y aplicación.

Las Ventajas que trae la Seguridad Distribuida son: La seguridad basada en un host es más completa, funcional para las comunicaciones extremo a extremo propias de IPv6, no es relevante el punto de conexión del host en la red, hay seguridad en la red interna, cuenta con mayor información de auditoría.

Desventajas: es un modelo más complejo que el de la seguridad perimetral, debe forzarse a que un nodo cumpla las políticas de seguridad, siendo el reto los nodos no conectados, un host comprometido es un riesgo para la red.

3.4.7 Protocolos Auxiliares en IPv6

3.4.7.1 Protocolo ICMPv6

El protocolo de control de mensajes de internet ICMP (Internet Control Messages Protocol)[27] es un protocolo que se ubica en la capa de red y es considerado por algunos como subprotocolo de IP. Las funciones principales en las redes IPv4 son la notificación de errores en las redes y el diagnostico de las interconexiones de las mismas.

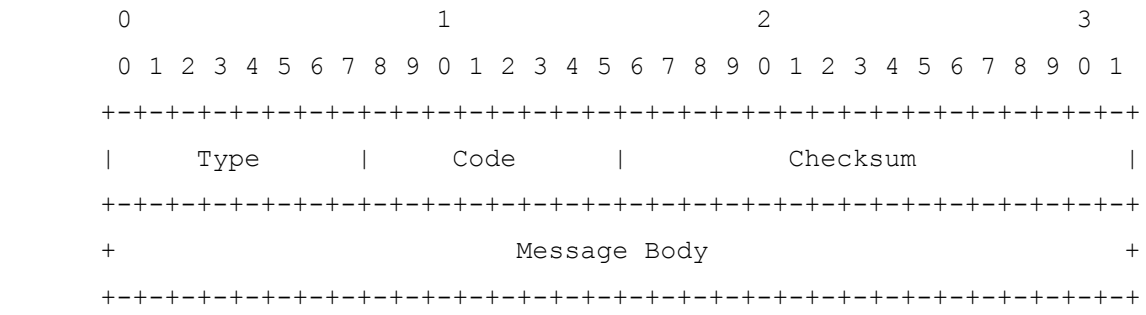
ICMP es el protocolo neurálgico del protocolo IPv6 se identifica con el número 58 en IPv6 a través de mensajes que controla el flujo de los protocolos enviando información o reportando errores.

Los mensajes ICMP se identifican según su tipo en Mensajes de Error y Mensajes Informativos (ver Figura 23), los tipos del 0 al 127 son reservados para los mensajes de error y para los mensajes informativos los tipos van del 128 al 255. Los únicos mensajes de Error son: Destino Inalcanzable, Paquete muy grande, Tiempo Excedido y Parámetro del Problema que tienen asignados los tipos del 1 al 4 respectivamente.

---

[27] RFC4443 - Internet Control Messages Protocol, (ICMPv6) Specification for the Internet Protocol Version 6 (IPv6) Specification. *Tools.ietf.org*. Fecha de consulta: 18 Mar 2018, from https://tools.ietf.org/html/rfc4443

Figura 23. Cabecera el Datagrama ICMPv6



Fuente IETF RFC4443

Dentro de cada una de estas cuatro categorías de mensajes de error el campo código perfila más el tipo de error que representa. Los mensajes informativos más representativos son el echo request y el echo reply. En la Tabla 7 identificamos el tipo de mensajes y la descripción de cada uno de ellos.

Tabla 7. Mensajes dentro del protocolo ICMPv6

MENSAJES DE ERROR		
DESTINATION UNREACHABLE	**TYPE 1**	**PARAMETER 0**
	Code 0	No route to destination
	Code 1	Communication with destination administratively prohibited
	Code 2	Dirección de origen sin ese alcance, más allá del alcance de la dirección de origen.
	Code 3	Address Unreachable
	Code 4	Port Unreachable
	Code 5	Source address failed ingress/egress policy
	Code 6	Reject route to destination
PACKET TOO BIG	**TYPE 2**	**PARAMETER 0**
	Code 0	Packet too big
TIME EXCEEDED	**TYPE 3**	**PARAMETER 0**
	Code 0	Hop limit exceeded in transit

	Code 1	Fragment reassembly time exceeded
PARAMETER PROBLEM	**TYPE 3**	**PARAMETER 0**
	Code 0	Erroneous header field
	Code 1	Unrecognized next header type
	Code 2	Unrecognized IPv6 Option
	Code 3	IPv6 first fragment has incomplete ipv6 header chain
MENSAJES INFORMATIVOS		
ECHO REQUEST	TYPE 128	CODE 0
ECHO REPLY	TYPE 129	CODE 0

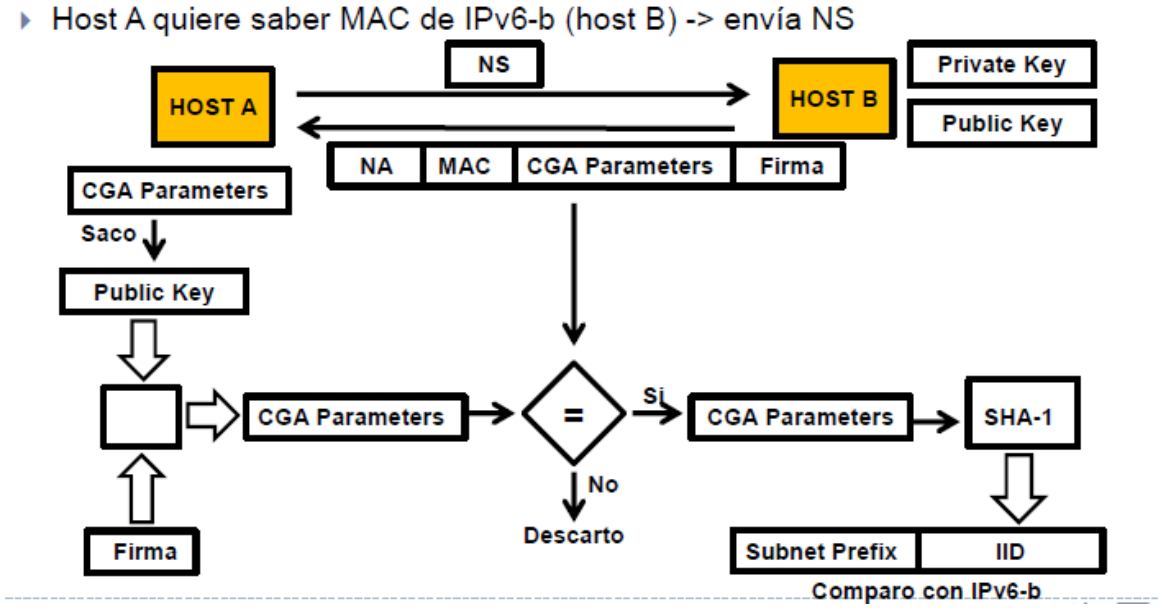
Diseño basado en el RFC4443

3.4.7.2 Send- Secure Neighbor Discovery

Los dispositivos IPv6 utilizan de manera frecuente el protocolo NDP para buscar vecinos en el segmento de red o en el segmento de enlace según el diseño de la red y mantener esta información actualizada, pero el protocolo NDP es vulnerable si no se asegura por lo que la RFC3971 establece el protocolo de seguridad de NDP, el Secure Neighbor Discovery (SEND) que especifica ciertos mecanismos de seguridad para NDP. Es de resaltar que estos mecanismos no usan IPSec, como fue habitual en las primeras implementaciones de NDP Seguro. El protocolo SEND es la opción segura del protocolo NDP y está pensado para entornos de seguridad física no tan fuerte, como por ejemplo redes inalámbricas.

Send opera en conjunto con CGA (Cryptographically Generated Address) de tal manera que un host con SEND requiere un par de claves pública-privada y está basado en la RFC3972 que lo que busca es que la dirección IPv6 genere su IID criptográficamente. La siguiente gráfica (Figura 24) presenta la comunicación entre dos nodos a través del protocolo SEND:

Figura 24. Comunicación entre dos nodos a través del protocolo SEND



Fuente IPv6 Forum (2018)

3.4.7.3 NDP

Es el protocolo para descubrir los host del enlace al que se pertenece por lo que usa comunicaciones host-host y router-host. Sirve para descubrir su router, el prefijo de la red, los parámetros de la red, para aplicar si así se desea la autoconfiguración. Este protocolo está acompañado de dos funcionalidades: DAD para detectar si una dirección ip ya esta asignada para evitar hacer una doble asignación o duplicación y el NUD que establece si el host o el vecino es alcanzable en el segmento de red. NDP hace uso de 5 tipos de paquete ICMPv6, a saber:

RA: Router Advertisement
RS: RouterSolicitation
NA: NeighborAdvertisement
NS: NeighborSolicitation
Redirect

Los NS son enviados por los host y se utilizan para resolver una dirección MAC y comprobar alcanzabilidad en el enlace. Los host también envían NA como respuestas a un NS o para entregar nueva información solicitada o no. Los host también pueden enviar RS es típica de cuando se levanta una interfaz y los Routers envían RA que son mensajes muy importantes ya que entregan información de la red como su prefijo y DNS entre otros, los RA se envían como respuesta a un RS y periódicamente para brindar información a la red.

Con el Neighbor Discovery los nodos envían mensajes de RS a la dirección multicast y los Routers de la red de ese nodo le responden con un RA. Los Routers envían periódicamente mensajes de anunciación de routers RA para anunciar su presencia, los prefijos que se encuentran en el enlace, ayudar a la configuración de la dirección ip y compartir otra información sobre el enlace.

A continuación vemos el funcionamiento del protocolo Discovery Neighbor (ver Figura 25) los host hace RS preguntando quién es su Router y los Router le responden con un RA. También se observa que un nodo pregunta por la MAC del nodo C (NS) y el nodo **C** le responde con un NA. Si el nodo C no responde el host le hace una solicitud NS y la respuesta será el nodo al que debe redirigir el paquete, con estos mensajes el router informa el vecino o el próximo salto.

Figura 25. Funcionamiento del Protocolo Discovery Neighbor.

Fuente Los Autores

El descubrimiento de vecinos combina y mejora la funcionalidad en IPv6 y añade nuevas características, como:

Mueve la resolución de dirección a ICMP que es menos dependiente de los medios de comunicación que ARP. Esto también permite el uso de la seguridad de la capa IP cuando se requiera.

NDP usa direcciones locales de enlace lo que permite que todos los nodos mantengan sus asociaciones de router, incluso si el site se vuelve a numerar a un nuevo prefijo global.

Los mensajes de descubrimiento de vecino llevan información de la dirección de enlace, 1 o 2 mensajes es todo lo que se requiere para que los nodos resuelvan las direcciones de los otros nodos.

Mejoras detección de inaccesibilidad: La detección de inaccesibilidad se logra con la entrega de paquetes por lo que puede establecer si hay falla en el router o la falla es en el enlace y si la falla es total o de una sola vía.

3.4.7.4 MTU

El protocolo MTU es un protocolo no orientado a la conexión que envía un paquete MTU estándar (1500 bytes) para saber si el paquete hay que fragmentarlo o no, esto se notifica a través de mensaje ICMP6 packet too big. Si el paquete es grande se fragmenta, la fragmentación sólo se da en los host extremos de la comunicación para optimizar la función de los routers.

3.4.8 Técnicas de configuración de host SLAAC y DHCPv6

SLAAC: Stateless Address AutoConfiguration es un mecanismo de configuración automático que permite el establecimiento de parámetros de red en los host de un segmento, con este mecanismo no es necesario tener un servidor dedicado y especifico. El descubrimiento de vecinos permite la autoconfiguración de direcciones libres de estado (SLAAC), es una configuración de dirección ligera que dota al protocolo IPv6 de conectividad Plug and Play en dos fases.

A través de un RA el router del segmento indica como autoconfigurar cada host y la información suficiente para este proceso como el default gateway, cuenta con tres formas posibles de configuración según el valor de las banderas:

M = O: SLAAC para IP y otros parámetros

M = 0: SLAAC para IP

O = 0: SLAAC para otros parámetros (no se usa)

FASE 1 Dirección de Enlace Local: Todos los nodos requieren una dirección de enlace local derivada de la mac de cada interfaz de red y el prefijo fe80::/10, luego

se debe comprobar que la dirección sea única a través de un mensaje a la nueva dirección, si hay respuesta el proceso se detiene de lo contario se asigna esa dirección a la interfaz para la que fue generada y brinda conectividad automática con los nodos del enlace.

FASE 2 Dirección Global: El nodo envía un RS a todos los routers del enlace, mientras el nodo este habilitado para proporcionar SLAAC habrá un RA que contendrá un prefijo global por ejemplo 2001::bd8::/32. Con este el nodo genera su dirección global añadiendo su ID de interfaz, por último se debe verificar que la dirección no esté duplicada a través del protocolo DAD. Suponiendo que la dirección no está duplicada el nodo la asigna a su interfaz.

A continuación en la Figura 26 se presenta las configuraciones principales de las banderas que determinan que tipo de autoconfiguraciòn se dará en la red si SLAAC o DHCPv6 y dentro de éste si se envía la configuración completa y se guarda la traza de cada asignación o por el contrario se opta por una configuración Stateless.

Figura 26. Indicadores de mecanismos de autoconfiguración

Auto-address Configuration Method	ICMPv6 RA (Type 134)			Resulting IPv6 Addresses Configured	Additional Configuration Options *(DNS servers, domain search list, etc.)*
	A Flag	M Flag	O Flag		
SLAAC	1	0	0	Link-local, IPv6, Temporary IPv6	Manual (unless client supports RFC 6106/RDNSS)
Stateless DHCPv6	1	0	1	Link-local, IPv6, Temporary IPv6	DHCPv6
Stateful DHCPv6	0	1	N/R	Link-local, DHCPv6	DHCPv6

Fuente IPv6 CoE Blog[28]

DHCPv6: Es el mismo concepto de IPv4 por lo que utiliza comunicación UDP y tiene opción del uso de relays, lo que cambian son los nombres de los mensajes (solicit, advertise, request, reply (confirm, renew, rebind, release, decline, reconfigure, relay-forw, relay-repl), los puertos UDP para cliente es el 546 y para Servidores/Relays el 547. La escucha se realiza por direcciones multicast conocidas como: FF02::1:2 (Servidores y Relays miembros de este grupo), FF05::1:3 (Servidores miembros de este grupo: Relay-> Servidores, para comunicarse con todos o porque no conoce dirección Unicast). Existen dos opciones de implementación la opción DHCPv6 stateless (RFC3736) que solo

[28]INFOBLOX IPv6 COE Blog, (2012). The IPv6 Center of Excellence (COE) Disponible en línea. 12 Abril 2018, https://community.infoblox.com/t5/IPv6-CoE-Blog/

proporciona “otra” información de la red pero NO su IP y la stateful que proporciona todo.

DHCPv6 respecto de la versión 4 tiene una leve diferencia y es que no envía el default Gateway lo que hace más complejo un ataque al DHCPv6.

MLD: MulticastListener Discovery es el equivalente de IGMP para IPv4, va por la versión 2 que es la más segura pero se conserva la 1 por compatibilidad (con un solo host que hable MLDv1 toda la red hablará MLDv1). Este protocolo es vulnerable a agotamientos de RAM por el envió de muchos MLDReports.

3.4.9 DNS

El sistema de nombres de dominio (DNS) tiene como principal característica la asignación de un nombre de dominio o nombre único que identifica un recurso en internet es decir un sitio (site) esta relación se realiza para descubrir la ip a un nombre inteligible por el ser humano por ejemplo la página de google.com está identificada con una IP 172..17.8.68. Estas relaciones nombres de dominio y direcciones IP se guardan en bases de datos distribuidas.

Jerarquía

La importancia de la notación de los nombres DNS se leen de derecha a izquierda y van separadas por un punto (.) por ejemplo en el dominio maps.google.com

Ejemplo:.com es el TLD

Google pertenece al subdominio .com

Maps. Pertenece al subdominio .google

Está basada en el TLD (Top Level Domain) nivel de dominio principal actualmente existen más de 1500 dominios principales[29] distribuidos entre genéricos, países y otros como puede verse en la Tabla 8. La autoridad responsable de dicha administración IANA encarga a la TDLco.

Tabla 8. Tipos de TDLs según el tipo

Tipo	Total de tipos (Cantidad)	Ejemplos
country-code	312	.co, .us, .ar, .ec, .fr

[29] IANA, Base de datos de zonas raíz, última actualización Abril 12 de 2018, consultado el Abril 14 de 2018, https://www.iana.org/domains/root/db

Tipo	Total de tipos (Cantidad)	Ejemplos
generic	1235	com, org, net
generic-restricted	3	biz, name, pro
infrastructure	1	.arpa
sponsored	14	.asia, .gov, int, .mil
test	11	آزمایشی. .測試
Total Resultados	1576	

Fuente IANA, Base de datos de zonas raíz

El sistema de nombres de dominio es enorme y consigue un buen rendimiento mediante el uso de la delegación y la asignación de caches (aloja los DNS más consultados y los recientes) en algunos de los puntos de las redes como host y routers.

El software de búsqueda del DNS en la PC se llama RESOLVER, este se encarga de comparar las direcciones de búsqueda en la cache que se encuentra en el dispositivo, sino encuentra un resultado adecuado realiza la solicitud en los DNS de la red interna de lo contrario pasa a los DNS de la red externa obedeciendo a la estructura de la jerarquía de DNS.

La práctica del DNS Cache optimiza los tiempos de consulta y dificulta las falsificaciones del DNS.

En una red IPv6 los servidores DNS se dan a conocer a través de:

Por RA (router adverteimen) (RFC 6106) anuncios de router donde envía mensajes a los host de la red indicándoles la IP de sus DNS.

Por DHCv6 (RFC 3315) hace referencia a la implementación completa del DHCP que incluye la asignación de la ip a los host y la dirección ip de sus DNS.

Por DHCv6statelless (RFC 3736) hace referencia a la implementación parcial de DHCP, ya que no incluye la asignación de IP a los host; eso implica que los host ya tienen IPv6 en la mayoría de dispositivos.

Para estos envíos de DHCP se hace uso de estas direcciones multicast (Well know site local)

Fec::0:0:FFFF::1

Fec::0:0:FFFF::2

Fec::0:0:FFFF::3

Fec::0:0:FFFF::4

3.4.10 DNSSEC

Es un sistema de extensiones de seguridad para DNS que añade firmas criptográficas seguras a los datos devueltos por los servidores DNS.

Las PC´s de los usuarios comprueban validez de la firma y aseguran los datos del DNS. El talón de Aquiles de esta propuesta es la gestión algo compleja de las claves.

3.4.11 Protocolos de Routing

Los protocolos de routing tienen campo de acción sobre los equipos de red para encaminar paquetes y los protocolos de la capa de aplicación, por ellos es Importante la activación de la doble pila IPv4/IPv6 como compartir el mismo esquema lógico en ambas redes. Es importante configurarla versión con soporte IPv6 para cada protocolo, según lo expresado en la tabla siguiente:

Tabla 9. Protocolos de routing acorde con las pilas IP.

TIPO	NOMBRE	IPv4	IPv6	COMENTARIOS
IGP	RIP	RIPv2	RIPng	Nueva versión solo IPv6
	OSPF	OSPFv2	OSPFv3	Nueva versión solo-IPv6
	IS-IS	IS-IS	IS-IS	Se extendió para soportar IPv6
	EIGRP	EIGRP	EIGRPv6	Propietario Cisco
EGP	BGP	BGP4	MBGP	Se extendió para soportar IPv6 Multiprotocol BGP o BGP4+ soporta Unicast IPv6, Multicast, IPv6, VPN3

Fuente los autores basado en los protocolos de enrutamiento

Los routers deben configurarse para que sean gestionables por IPv4 e IPv6. Los procesos de routing son con protocolos diferentes por lo que el consumo de recursos como CPU y memoria es diferente, según los trabajos de monitorización, gestión y solución de problemas. Se debe tener actualizaciones al día en el firmware del router y conocer con exactitud que funcionalidad está soportada para IPv6 por el router y cuáles no.

Los protocolos más seguros para infraestructura no Cisco son OSPFv3 e IS-IS para infraestructura Cisco se recomienda EIGRPv6 y para Border MBGP.

4. RESULTADOS

4.1 Conocer el protocolo IPv6

El reconocimiento de una infraestructura es vital para cualquier proyecto de TI y como se ha dicho con anterioridad el cambio normativo y técnico han hecho que la transición hacia IPv6 sea un factor crítico y obligatorio.

Por ello se ha abordado el protocolo IPv4 describiendo la estructura de los paquetes, los campos auxiliares los cuales hacen uso las capas superiores, algunos inconvenientes técnicos y problemas inherentes al mismo; también se conoce los protocolos auxiliares principales de los cuales el mismo hace uso de manera generalizada.

Cuando se aborda el protocolo IPv6 se tiene en cuenta además de los temas relacionados con IPv4 la jerarquía de direccionamiento y subneting, los nuevos campos en el encabezado así como protocolos auxiliares, los mecanismos de autoconfiguración, DNS y los mecanismos de transición.

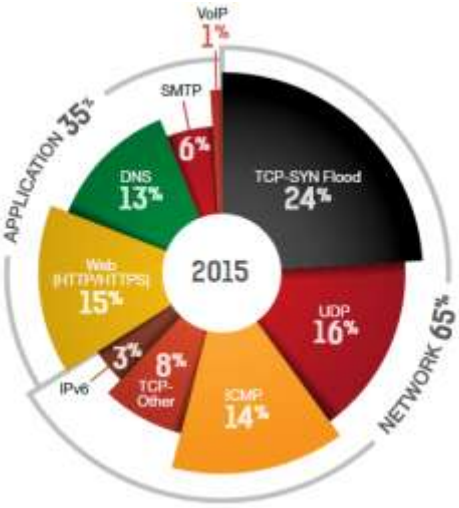
4.2 Vulnerabilidades

Como se ha tratado anteriormente, la llegada del nuevo estándar es inminente y ello trae consigo una serie de efectos adversos sobre las implementaciones. Esto era de esperarse dado el impacto que cada día tiene sobre el mundo moderno las redes y sus infraestructuras.

De hecho aunque la implementación de IPv6 no llega en su conjunto al 40% de las redes corporativas mundiales ya se visualiza una serie de ataques sobre las mismas, así lo evidencia la encuesta realizada a más de trescientas empresas y compañías en 2016 sobre el problemática de la seguridad en temas de TI (ver Figura 27. Porcentaje de ataques según aplicación / infraestructura en 2015). En donde el 52% de dichas empresas correspondían a ambientes de escala global y el 49% de dichas empresas tienen máximo 3000 empleados[30].

[30] Radware (2016) global application & network security report, Fecha de consulta: 30 de Marzo 2018, disponible en www.radware.com

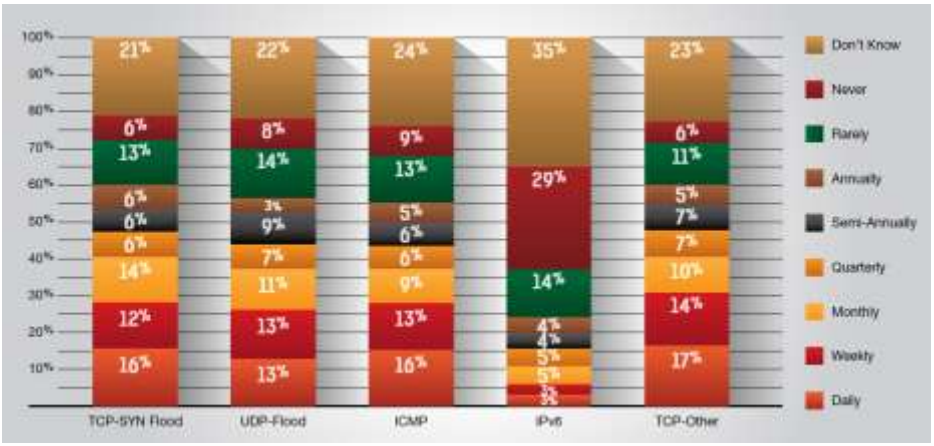
Figura 27. Porcentaje de ataques según aplicación / infraestructura en 2015



Fuente Radware Global application & network security report 2016[31]

Como se evidencia en la Figura 28, aunque es posible inferir que muchos ataques corresponden a ataques conocidos en IPv4 los que tienen referencia directa con IPv6 tienen baja actividad e incidencia, pero igualmente se destaca el desconocimiento de un ataque por esta vía.

Figura 28. Frecuencia de ataques en la infraestructura de Red



Fuente Radware Global application& network security report[32]

[31] Radware (2016) global application & network security report, Fecha de consulta: 30 de Marzo 2018, disponible en www.radware.com
[32] Ibid.

4.2.1 Principales ataques y vulnerabilidades del protocolo IPv6

Las redes de computadores y dispositivos electrónicos son vulneradas principalmente en tres aristas, a saber: el plano de control donde tiene alta relevancia la seguridad de los dispositivos de la red, el transporte en sí mismo y el software que opera en los host y servidores de la red. IPv6 presenta mayor vulnerabilidad comparada con IPv4, en el sentido que la extensión de estas tres zonas es mayor, se requieren de nuevos puertos abiertos, la presencia de nuevos protocolos en los host, las vulnerabilidades sin descubrir y la falta de conocimiento en el Protocolo.

4.2.1.1 Ataques de capa dos o capa de enlace

Ataques de IP: Se refiere a las computadoras que mienten acerca de su IP, entonces el tráfico saliente de esta PC, que por lo general requerirá una respuesta, hará que con esa respuesta se inunde la máquina que señalo como IP Origen, si es mucho el tráfico se puede generar una denegación de servicio.

Ataques a ARP: Es un ataque típico de capa 2, del protocolo ARP, y el Inverse ARP son susceptibles de ataque. ARP se usa para obtener la dirección IP de la interfaz de la que se conoce la dirección MAC. Inverse ARP permite el proceso inverso. Se parte del hecho que el protocolo ARP es un protocolo “Inocente”, así cualquiera que sepa la respuesta puede enviarla, esta misma inocencia permite que se acepten respuestas desde un equipo que no tiene la MAC solicitada. a lo anterior se añade que el Protocolo ARP acepta ARP Reply aunque no se hayan enviado solicitudes o ARP Request.

ARP Exhaustion (Ataque por flooding): Consiste en llenar la memoria de almacenamiento de las direcciones MAC de un switch, lo que hace que algunos switches pasan a actuar como un hub. Se puede utilizar para recibir todos los paquetes enviados al switch.

ARP Spoofing son ataques de suplantación que envían mensajes ARP falsos buscando asociar la dirección Mac del equipo atacante con una IP de la red, así cualquier información enviada a esa IP la recibirá el computador atacante; este puede optar por enviar la información a la puerta de enlace de la red (ataque pasivo). El atacante también podría modificar la información y luego si retransmitirla (ataque activo). También se puede iniciar un ataque DDoS (denegación de servicio) contra un objetivo de tal manera que registre una Mac inexistente a la IP de la puerta de enlace del nodo atacado.

En estos casos donde se escala a un DDos el ARP Spoofing enlazará varias direcciones IP de una red con una misma MAC haciendo que este nodo sea sobrecargando.

Secuestro De Sesiones (Session hijacking): son ataques que buscan robar los identificadores de sesión para tener acceso a los sistemas informático objetivo, o el número de secuencia de una conexión para desincronizarla, esto implica la escucha de la red física. El ataque busca desincronizar ambos lados de la conexión TCP, esto se logra afectando los números de secuencias de la conexión. La desincronía se genera a través de un paquete con la IP de la máquina origen y el número de TCP de secuencia esperado por el host destino, este paquete también permite enviar un comando a través de la sesión o con esta desincronía genera el envió de muchos ACK más conocido como la tormenta de ACK.

Ataques a VLANs: Son ataques fundamentados en las vulnerabilidades del protocolo 802.1q que siguen siendo iguales a los de IPv4 razón por la que no se abordan en este trabajo.

Switch Spoofing: Se aprovecha la mala configuración de un puerto del switch tipo trunk. El host conectado a ese puerto se hace pasar por un switch y si el ataque es efectivo se puede complementar con un “802.1q ARP poisoning”.

Double Tagging: Consiste en poner doble etiquetado al tráfico generado por el sistema. La etiqueta de fuera es la de la VLAN del host atacante y la de dentro es de la VLAN a la que se quiere llegar/atacar. El tráfico generado es sólo de un sentido. Se puede atacar VTP (VLAN TrunkProtocol) de Cisco con Yersinia. Permitiría cambiar la configuración de VLANs de los switches. Se puede proteger con password (hash tipo MD5). Si la clave no es robusta se podría atacar fácilmente.

4.2.1.2 Ataques de capa tres o capa de transporte

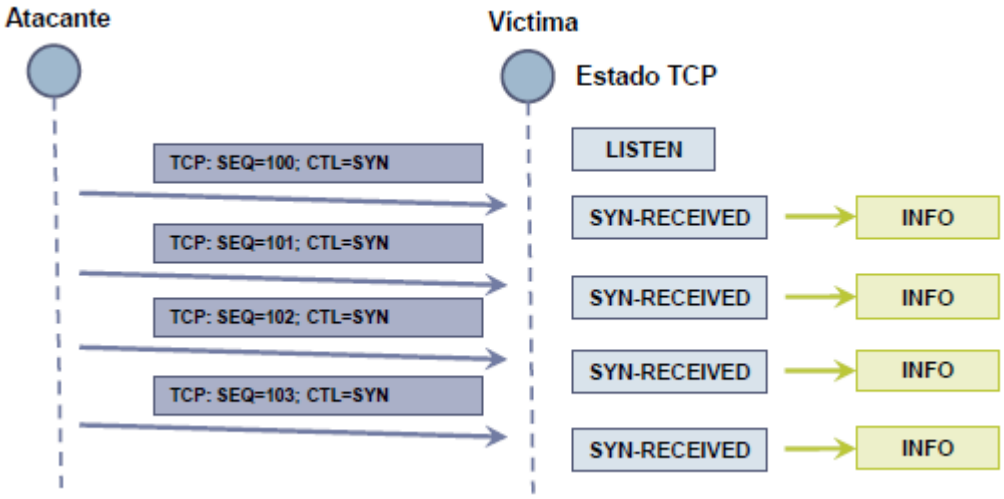
Son ataques basados en la configuración de información de routing errónea ya que al alterar las rutas permitiría al atacante redirigir el tráfico hacia sí mismo para generar un (DoS) o para analizarlo (MITM).

Recordemos que la capa de transporte ofrece servicios a la capa de aplicación a través de la capa de red, por lo que existen varios ataques: TCP SYN Flood [RFC4987], ataques a los números de secuencia TCP [RFC6528], ataques al ICMP (smurf, ping of death, ICMP redirect bomb) por lo cual es importante la implementación de protocolos que añaden seguridad como TLS, DTLS y SSL entre los principales. Los principales ataque se clasifican en: Ataque ICMP Redirect Y Spoofing de protocolos de routing.

4.2.1.3 Tcp Syn Flooding:

Ataque que busca agotar los recursos reservados para las conexiones medio abiertas, es la generación de un (DoS) en un servidor informático como se observa en la Figura 29.

Figura 29. TCP SYN Flooding Attacks



Fuente Curso Certified Security Engineer IPv6 (Febrero 2018).

Este ataque envía varias peticiones Syn y el receptor lo trata como una petición de conexión haciendo que este se sature por las muchas solicitudes o que si vienen con una dirección de origen falsa el proceso de conexión TCP de 3 vías llegue a múltiples conexiones que están a la espera de un paquete de respuesta TCP/ACK que nunca llegará, cómo lo muestra la Figura 30. TCP SYN Flooding Attacks.

Con estos procesos de conexión el servidor consume recursos hasta copar su límite generando incapacidad de responder las peticiones legales de conexión.

Figura 30. TCP SYN Flooding Attacks

1 Cliente	**→→→**	**SYN**	**2 Servidor**
4 Cliente	←←←	SYN / ACK	3 Servidor
5 Cliente	**→→→**	**ACK**	**6 Servidor**

Fuente Curso Certified Security Engineer IPv6 (Febrero 2018).

4.2.1.4 Ataque de Predicción de Secuencia TCP:

Busca atinar con él número de secuencia usado en los paquetes TCP de una conexión con el fin de dañarlos, alterarlos o conocerlos. Si el atacante logra atinar al número se pueden enviar paquetes falsos al destino. Por lo general esto implica una escucha pasiva de la red y el envió de paquetes falsos bajo la misma IP de origen del host emisor confiable, el atacante debe preocuparse es de que su paquete llegue primero que el paquete original y muchas veces ataca al host

origen por ejemplo con un DOS, si el atacante logra enviar el paquete de primeras tendrá el control de la conexión y puede continuar enviando paquetes falsos pese a que no tenga respuesta.

4.2.1.5 Ataque ICMP:

Las mayores vulnerabilidades se presentan en el tema de filtrado en los paquetes con Next Header con valor 58 que es el asignado al protocolo ICMP. ICMP es el protocolo más importante de IPv6 ya que da soporte de las comunicaciones para los Protocolos PMTUD, NDP, SLAAC, DAD, MLD entre otros. Las principales vulnerabilidades de este protocolo están relacionadas con la fragmentación en paquetes pequeños para no ser filtrados y la fragmentación dentro de un túnel ya que se acostumbran ataques a través de una cabecera exterior que se oculta dentro de la fragmentación.

4.2.1.6 Ataques en capa de aplicación

Es la capa relacionada con el usuario final en sí, pues tiene que ver con los formularios, las contraseñas, las conversaciones y los documentos de aplicación principalmente. Desde el punto de vista estadístico, los ataques a las capas inferiores tienen por objetivo el obtener información de esta capa, por ejemplo obtener las credenciales de login de un usuario o sus datos de tarjetas de crédito. Son muy usuales los ataques MITM ya que se pueden guardar la comunicación y escudriñarla hasta obtener la información referida o ficheros transferidos.

Ante esto es importante recordar que algunas aplicaciones facilitan un posible ataque ya que envían su información en texto claro como por ejemplo las aplicaciones HTTP, Telnet, FTP, POP3, IMAP4, etc., es por ello que es importante el uso de las versiones seguras de ellas, como: HTTPS, SSH, SCP, POP3S, IMAPS. Se deben proteger adecuadamente los protocolos de Gestión, de lo contrario es fácil obtener la información en los dispositivos gestionados.

4.2.1.7 Ataques a protocolos de configuración o de información de los hosts

Hace referencia a los protocolos usados para configurar parámetros u obtener información utilizada en las comunicaciones, u similares usos en otras capas, por ejemplo: DHCP, DNS, NTP; son protocolos de capa de aplicación por Ejemplo: DNS Spoofing y Rogue DHCP.

DNS Spoofing:

El ataque consiste en interceptar la petición DNS y devolver un valor equivocado. Requiere MITM previo, ejemplo: ARP Poisoning. Se puede usar para hijacking de una conexión web, pudiendo obtener los datos de Login.

RogueDHCP:

El ataque es más bien simple, consiste en enviar OFFER a peticiones DISCOVERY de clientes. El primer OFFER en llegar al cliente será el que use. Con Rogue DHCP es muy probable que se envíe al atacante el tráfico (MITM) cambiando el default Gateway, o que las peticiones DNS se envíen al atacante una vez modificado el servidor DNS (DNS Spoofing).

Dhcp Ack Injection:

Es un ataque más complejo que el anterior, pues consiste en escuchar el intercambio cliente-servidor DHCP y antes de que el servidor envíe el ACK lo envía el atacante con los parámetros que quiera poner. Se hará caso del ACK que llegue antes, ya sea el del servidor o del cliente.

DAD (Duplicated Address Detection):

Se utiliza para saber si una dirección ya está asignada en una interfaz. Es susceptible a los ataques DOS por un nodo q responde lo preguntado al nodo original esto impide que se pueda actualizar la tabla de vecinos.

NUD (Neighbor Unreachability Detection):

Actualiza de manera proactiva la información de su vecino determinando si es alcanzable a través de un NS y su NA. Así se puede saber por ejemplo información del Gateway, su MAC y si es alcanzable en la Tabla de vecinos o Neighbor Cache que tienen la ip, si es router o host y si es alcanzable. La tabla Destination Cache contiene las direcciones a las que se ha enviado tráfico recientemente, mapea direcciones de destino con next hop.

4.2.1.8 Vulnerabilidad en el Protocolo NDP

El protocolo NDP está definido en la RFC 4861, sus vulnerabilidades permiten que nodos maliciosos envíen múltiples NAS permitiendo la consolidación de un DoS, por lo que se requirió de IPSec para proteger estos mensajes lo cual no ha sido muy práctico y por ende se prefiere la implementación de SEND.

El ataque principal es el Router de último salto malicioso que es cuando un nodo atacante se hace pasar por un router y envía un paquete RA multicast o unicast como respuesta a un RS logrando ser el gateway.

Otro ataque común es el de "Muerte del encaminador por defecto" A través de un DOS clásico contra el encaminador que no responderá y enviando RA Falsos con tiempo de vida cero, así los dispositivos del enlace asumen que son locales.

4.2.1.9 Vulnerabilidad en MLD

Este protocolo es vulnerable a agotamientos de RAM por el envió de muchos MLD Reports. Este tipo de mensajes en una escucha pasiva permiten identificar los routers. Por sus características es muy vulnerable a DoS.

4.2.1.10 Ataques a protocolos de aplicación

SSDP:

Hace parte del protocolo UPnP, que sirve para descubrir los servicios de una red, utiliza UDP y multicast tanto IPv4 como IPv6. Es de resaltar que este protocolo es muy usado por los Sistemas operativos Windows de forma automática, lo que lo puede convertir en un vector de ataque.

HTTP/HTTPS:

Estos famosos protocolos permiten ataques para interceptar el tráfico HTTP y HTTPS, esto implica un MITM previo.

Cookies de Sesión:

Las cookies alojan información propia de la autenticación de un usuario en una web, las cookies son válidas mientras la sesión está abierta o para algunas aplicaciones son válidas para siempre. Al interceptar el tráfico HTTP se puede acceder a la información de estas cookies y con ello es posible la suplantación de la identidad de un usuario en la web.

4.2.1.11 Ataques a los protocolos de routing

Se mantienen las amenazas de IPv4 y se le añaden las amenazas de IPv6 como Packet Flooding, Gusanos (Worms) y Ataques DDoS, las veremos a continuación.

4.2.1.12 Packet Flooding:

Ataque también conocido como Smurf consiste en la inundación de datagramas defectuosos en la red donde se han modificado su encabezado o estado.

Ataques de Amplificación Broadcast (Smurf): Se envía echo ICMP al grupo multicast de una red, se falsifica la dirección de origen del dispositivo víctima, generando que los dispositivo del prefijo envíen una respuesta masiva echo reply a la víctima colapsándola.

4.2.1.13 Gusanos (Worms):

Ataques que se propagan por sí solos, ubican nuevos sistemas, detectan si son vulnerables y atacan. Su propagación usual es por email en protocolos p2p e IM, pero se es más susceptible si usan IP como slapper que permite hacer flooding IPv6 O W32/Sdbot-VJ que aunque no usa IPv6 se instala como wipv6.exe simulando archivos de IPv6 en Windows.

4.2.1.14 Ataques DDoS:

Se caracteriza por la presencia de computadoras Controllers que son las que envían comandos y los zombies que son las máquinas que llevan a cabo los ataques y están distribuidas por internet. Estos ataques son iguales en las dos pilas del protocolo IP con la salvedad que IPv6 tendrá mayor cantidad de dispositivos en Internet, pese a ello también hay que destacar que puede ser más fácil de establecer la trazabilidad del atacante ya que el direccionamiento IPv6 es jerárquico y ordenado.

4.2.1.15 Ataques relacionados con Mecanismos de Transición

Cada vez que se hace uso de un mecanismo de transición se están habilitando en la red las viejas vulnerabilidades de IPv4, por lo que las Redes doble-pila pueden ser atacadas por IPv6 o por IPv4, por lo que se recomienda usar medidas de seguridad similares en ambos protocolos. De otra parte con este tipo de mecanismos de transición requieren de puertos abiertos nuevos en los firewalls, por lo que debe haber un Control milimétrico del uso de túneles especialmente en lo referente a la inspección en del tráfico encapsulado por parte de los firewalls. A continuación en la Tabla 10 se muestra un cuadro que resume las consideraciones de seguridad a implementar según hablemos de nodos IPv6 ó IPv4 versus Infraestructura IPv4/IPv6.

Tabla 10. Seguridad IPv6 en Redes IPv4/IPv6

	INFRAESTRUCTURA	Solo IPv4	Solo IPV6	Doble Pila
NODOS	Solo IPv4	Riesgos de Seguridad solo IPv4	No es operativa Posibles ataques de Enlace IPv4	Muy Común Riesgos de Seguridad IPv6 E IPv4
	Solo IPv6	No es operativa Posibles ataques de Enlace IPv6	Riesgos de Seguridad solo IPv6	Poco Común Riesgos de Seguridad IPv6 E IPv4
	Doble Pila	Muy Común Riesgos de Seguridad IPv6 E IPv4	Riesgos de Seguridad IPv6 E IPv4	Muy Común Riesgos de Seguridad IPv6 E IPv4

Fuente Los autores basados en fundamentos de IPv6 Forum

4.2.2 Seguridad para BGP

El protocolo de Borde BGP (Border Gateway Protocol) es el protocolo de routing externo o de encaminamiento en internet, esto permite que se pueda enviar información entre sistemas autónomos. A continuaciones mencionamos los aspectos más relevantes del protocolo BGP en cuanto a seguridad se refiere:

Usar claves secretas compartidas en los peering

Controlar el TTL de los paquetes BGP (RFC 5082)

Prevenirse contra AS_PATH largos

Limitar el número de prefijos recibidos

Prevenirse contra BGP updates con ASN privado

Usar direcciones loopback para peering (iBGP)(+IGP)

Filtrado de prefijos de las direcciones según su ámbito

El Remote Triggered Black Hole Filtering (RTBH) es igual que en IPv4.

4.2.3 Seguridad en IGPs

Para el protocolo RIPng pide usar IPSec, RIPng no soporta autenticación usando MD5, es un protocolo poco seguro.

Para el protocolo EIGRPv6 y teniendo en cuenta que este protocolo ha tenido vulnerabilidades como información en texto claro, uso de multicast y los famosos mensajes goodbye se debe habilitar la autenticación MD5 y vecinos estáticos (en lo posible), y el uso de comunicaciones unicast para mensajes hello.

Para el protocolo IS-IS que es menos usado que OSPFv3. El protocolo IS-IS tiene dos modos: Single-topology y multitopology. El modo Single Topology optimiza recursos con las mismas métricas que usa la versión de IPv4, al igual que la misma topología. El modo Multitopology consume más recursos que el modo Single. Se caracteriza por ser flexible lo que permite tener topologías distintitas para IPv4 e IPv6, además soporta autenticación vecinos con password y MD5.

Para el protocolo OSPF empezar por aclarar que OSPFv2 es para IPv4 y soporta autenticación MD5 y OSPFv3 es para IPv6 y soporta autenticación MD5 pero de

distinta manera, no en campos del mensaje Hello, hace uso de IPSec que proporciona integridad (AH) y confidencialidad (ESP).

4.2.4 Otros Ataques

Escaneo de Red: Es una actividad ampliamente usada en el Hacking pero resulta que bajo el nuevo protocolo IPv6 es muchísimo más difícil de ejecutar que con IPv4, dada a la amplitud de direcciones en una red tanto el espectro de direcciones como con direcciones aleatorias automatizadas es muy difícil conseguir un ataque efectivo.

Amenazas a NDP: La primera amenaza por este lado es el hecho que el protocolo hace uso del protocolo ARP (IPv4), First-hop security y cabeceras de extensión (EHs).

4.2.4.1 Envenenamiento de Cache (DNS)

Este tipo de ataque consiste en ingresar datos falsos en la cache DNS, es difícil de detectar la información falsa.

De acuerdo con la Figura 31 se describe el ataque por envenenamiento de cahe en DNS:

1. Atacante modifica el cache del servidor DNS.

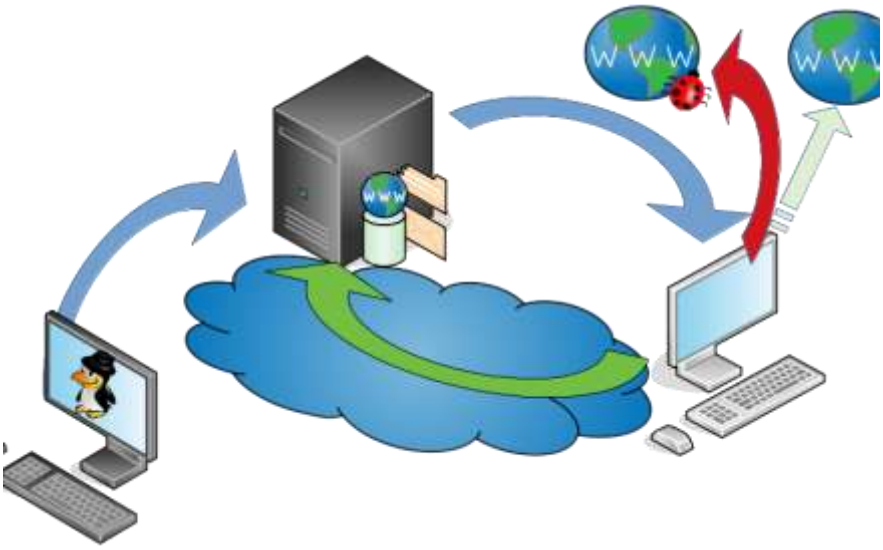
2. A Realizar una consulta el usuario solicita una dirección.

3. El servidor regresa una dirección falsa o adulterada al usuario.

4. El usuario en vez de dirigirse a un sitio legítimo va a un sitio fraudulento o inexistente.

La explotación de la vulnerabilidad de los resolvers ocurre completamente dentro ISO y los sistemas operativos de la red sin necesidad de comprometer los host de usuarios.

Figura 31. Envenenamiento de cache DNS



Fuente Los autores

4.2.4.2 Malware que se dirige al DNS

Es cuanto al malware modifica cada PC usuario para cambiar la resolución DNS que utiliza normalmente por la controlada por un atacante. El usuario que está controlado por la resolución de DNS puede dar respuestas correctas o falsas.

4.2.5 Herramientas de Detección y Testeo

A medida que los protocolos e infraestructuras van adquiriendo una madurez se requieren realizar distintas pruebas dependiendo de las labores que los expertos en TI requieren. Esto incluye herramientas de configuración, pentesting y diagnósticos de red enfocadas a IPv6. Dada la multitud de herramientas que ya existen en IPv4 y que, ellas ya incluyen algunas funcionalidades enfocadas a IPv6 se muestran algunas que se consideran importantes a tener en cuenta.

4.2.5.1 THC “The Hackers Choice” attack tools

THC es un grupo de herramientas desarrollada para realizar test de intrusión, escaneo y verificación de los principales aspectos que la implantación del protocolo IPv6 debe tener en cuenta. En la Tabla 11 se puede ver algunas herramientas desarrolladas por THC.

Tabla 11. Herramientas de análisis de The Hackers Choice

Herramienta	**Descripción**
Alive6	Herramienta para inspeccionar host en redes locales bajo protocolo IPv6
DETECT-NEW-IPV6	Herramienta para detectar nuevos hosts en redes locales bajo protocolo IPv6
DOS-NEW-IPV6	Herramienta para probar sistemas bajo DOS
FAKE_MIPV6 FAKE_MLD6 FAKE_ROUTER6	Herramientas para falsificar enrutadores, crear nuevas rutas, redirección de nodos, detección de mensajes multidifusión
PARSITE6	Spoofer vecino ICMP para ataques Man-In-The-Middle
REDIR6	Redirigir tráfico en redes LAN
RSMURF6	
SENDPEES6	Solicitud de vecinos con muchos CGA Probador de implementación de protocolo: Fragmentación + encabezado de enrutamiento Encabezados masivos Punteros inválidos
SMURF6	Herramienta Local Smurf (ataca tu LAN)
TOOBIG6	herramienta para reducir la MTU en un ataque

Fuente The Hackers Choice attack tools. http://thc.org/thc

4.2.5.2 IPv6toolkit – SI6NETWORKS

La empresa si6networks ha desarrollado igualmente un conjunto especializado de herramientas enfocadas al análisis, detección y verificación en los contextos de redes locales que soporten el protocolo IPv6. La última versión estable del conjunto de herramientas es la 1.2.3. En la Tabla 12 se describen algunas funcionalidades de estas herramientas.

Tabla 12. Herramientas ipv6toolkit de si6networks

Herramienta	**Descripción**
flow6	Herramienta para realizar evaluación de seguridad de la etiqueta de flujo IPv6.
frag6	Herramienta para realizar ataques basados en la fragmentación de IPv6 y para realizar evaluación de seguridad de serie de aspectos relacionados con la fragmentación.
icmp6	Herramienta para realizar ataques basados en mensajes de error ICMPv6.

jumbo6	Herramienta para evaluar fallas potenciales en el manejo de jumbo gramas IPv6.
na6	Herramienta para enviar mensajes de Neighbor Advertisement.
ni6	Herramienta para enviar mensajes de información de nodo ICMPv6, y evaluar posibles fallas en el procesamiento de dichos paquetes.
ns6	Herramienta para enviar mensajes de solicitud de vecinos.
ra6	Herramienta para enviar mensajes de anuncio de enrutador.
rd6	Herramienta para enviar mensajes de redirección ICMPv6.
rs6	Herramienta para enviar mensajes de solicitud de enrutador.
scan6	Herramienta de escaneo de direcciones IPv6.
tcp6	herramienta para enviar segmentos TCP entre otras funcionalidades.

Fuente si6toolkit www.si6networks.com

4.2.5.3 Scapy

Scapy es un conjunto de herramientas inicialmente desarrollado por secdev y que luego se convirtió en un proyecto independiente. Cuenta con funcionalidades de escaneo, manipulación de paquetes y es altamente configurable, actualmente se ejecuta de manera nativa en Linux usando como base pyton. Se puede descargar de manera libre en scapy.org.

4.3 Guía y buenas prácticas

4.3.1 Seguridad en IPv6

IPv6 si fue pensado como un protocolo más seguro por ello tiene integrado IPSec (pero como se ha anotado anteriormente no está configurado por defecto), además esto reduce el tiempo de procesamiento de seguridad. Hay cabeceras de extensión especiales para la seguridad como: AH = Authentication Header y ESP = Encapsulating Security Payload que permiten seguridad basada en la encriptación de la información transmitida. A un nivel más alto, a nivel de entidades la seguridad se basa en los certificados digitales. Es buena práctica activar IPSec en la implementación de IPv6.

Con IPv6 se supone el restablecimiento original del protocolo IPv4 con su modelo end-to-end, minimizándose las dificultades y el doble procesamiento que NAT implicaba para los protocolos y las aplicaciones. Otra buena práctica desde el punto de vista de la seguridad es la Transición gradual de IPv4 a IPv6, lo que implica tiempos de convivencia entre los dos protocolos.

4.3.1.1 Buena práctica de la seguridad distribuida

Como primera medida se debe controlar el modo promiscuo de la interfaz de red.

Hacer uso de herramientas anti-riesgos para ser instaladas en los host como:

Cisco NAC (Network Access Protection): El host obtiene acceso a la red cumpliendo con la política de seguridad.

Microsoft NAP (Network Access Protection): Esta herramienta valida el estado de salud del host y solo permite conexión a la red a los hosts sanos.

McAfee Epo: Esta herramienta cuenta con una consola centralizada de herramientas para host, a la fecha varias suites antivirus están entrando en esta tendencia permitiendo contar con más que un antivirus con una suite de seguridad para host (endpoint). Ejemplos de otras similares son la de Trend Micro Enterprise.

4.3.1.2 Calidad de Servicio (QoS) en IPv6

Se debe implementar la RFC 1633 para activar el campo de calidad de servicio del encabezado IPv6 con la finalidad de activar los niveles de tráfico: Mejor esfuerzo, servicios integrados o servicios diferenciados.

Este campo permite dar trato preferencial a las aplicaciones criticas de una red aplicando métodos de control y evasión de la congestión por lo que servicios VoIP serán de mejor calidad sobre IPv6.

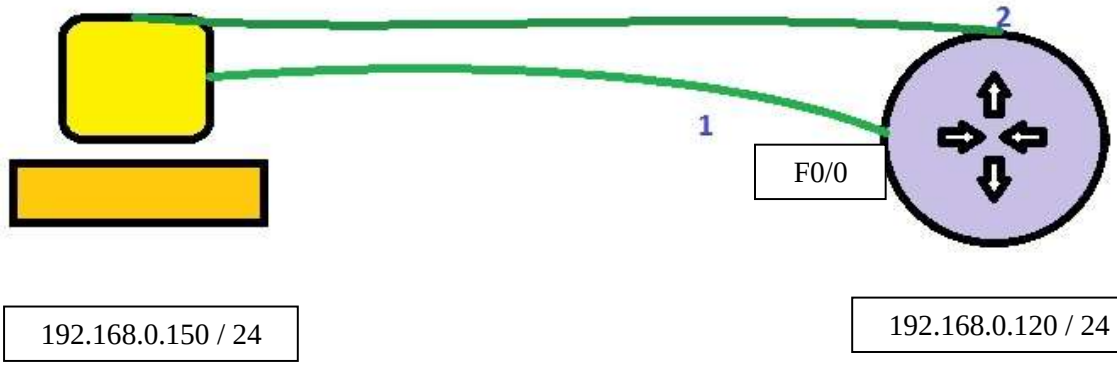
TrafficClass 8 bits = Type of Services IPv4 0 dice que no requiere QoS especialistas.

Flow Label: No puede estar disponible por fragmento o encriptación o estando disponible por estar detrás de la secuencia de cabeceras de extensión IPv6 puede resultar ineficiente; por lo que su valor debe ser cero (0).

4.3.1.3 Principio de aseguramiento y control del plano de administración de un router:

Explicamos este principio a través de la Figura 32 ejemplo que da acceso al Router por la consola y lo deniega por una conexión telnet.

Figura 32. Acceso a Router por telnet



Fuente Los Autores

Conexión vía TELNET (corresponde a la conexión **1**)

El Router aplica una política que impida el acceso al Router desde el PC 192.168.0.150 / 24, estos dos equipos están en la misma subred.

Conexión de consola (corresponde a la conexión 2)

La conexión por consola es la conexión por defecto para acceder al Router para configurarlo en este ejemplo se establecerá a través de esta conexión una Lista de Control de Acceso estándar (Tabla 13):

Tabla 13. Lista de Control de Acceso estándar

INSTRUCCIÓN	MODO ROUTER
R1>***ENABLE***	Usuario
R1#***Configure Terminal***	Privilegiado
R1 (config)#***access-list 10 deny host 192.168.0.150***	Configuración Global
R1 (config)#***access-list 10 permit 192.168.0.0 ∏ 0.0.0.255***	
R1 (config)#***access-list 10 deny any***	
R1 (config)#***exit***	
R1#	

Fuente Configuración de Listas de Acceso IP www.cisco.com

Las Listas de Control de Acceso (ACL) sirven para identificar tráfico interesante, tienen una numeración de 1 a 99, no entienden protocolos, ni IPs de Destino, lo

único que entienden las ACLs son IPs de Origen. En el ejemplo se define la ACL número 10. Entonces se procede a identificar el tráfico interesante, luego se crea una ACL estándar que indique el host al cual se niega el acceso vía Telnet. Luego se niega el tráfico de la ip 192.168.0.150 y se permite cualquier otro.

Luego se asocia la ACL a las líneas VTY 0/4 (Tabla 14)

Tabla 14. Negación de acceso mediante lista de control de acceso

INSTRUCCIÓN	**MODO ROUTER**
R1>***ENABLE***	Usuario
R1#***Configure Terminal***	Privilegiado
R1 (config)#***line vty 0 4***	Configuración Global
R1 (config-line)#***access-class 10 in***	
R1 (config-line)#***exit***	
R1 (config)#***exit***	
R1#	

Fuente Configuración de Listas de Acceso IP www.cisco.com

Se asocia la ACL 10 en las interfaces vty 0 a la 4 a través del comando Access-class, luego del número de la ACL se indica si la verificación será para el tráfico de ingreso o el que egresa del Router, en el ejemplo es el tráfico que Ingresa. Los Router/Switch modernos soportan las vty de la 0 a la 15 para Telnet (en total 16 conexiones telnet).

De otra parte, establecemos una conexión serial para acceder al Router y con los siguientes comandos se puede acceder al Router y verificar el número de intentos de acceso denegados al PC 192.168.0.150 al intentar acceder desde una conexión TELNET al Router.

R1>**ENABLE**

R1# **PASSW**

R1# **SH RUN**

R1# **Show Access-list 10**

Este ejercicio evidencia el principio de aseguramiento y control del plano de administración de un Router.

4.3.2 DNS

4.3.2.1 Buenas prácticas para evitar el envenenamiento DNS

Para mitigar esta vulnerabilidad se puede en el ISP o en los servidores de red de los operadores que proporcionan la resolución del DNS. Otra opción es activar los servicios de DNSSEC que evita este tipo de ataques.

Gestión diligente del software de servidor DNS (detectar y corregir errores y vulnerabilidades explotables).

Con cada actualización existe la posibilidad de nuevas vulnerabilidades desconocidas.

Incuso con DNSSEC implementado se requieren parches para corregir errores de software recientes y tener una buena higiene de seguridad en las máquinas.

Detectar respuestas falsas implica la existencia de otra fuente de DNS privada y comparar las respuestas que los usuarios obtienen con las fuentes conocidas.

Bloqueo de url legítimos que sirvan contenido malicioso y gestión rápidas de listas negras y blancas.

Tener una lista de los acortadores de url que redireccionen a sitios maliciosos o no preventivos.

Incluir pruebas de reputación de direcciones.

Mejores prácticas

Apoyar la implementación de DNSSEC.

Apoyar e implementar pruebas de software en el DNS para asegurarse que los errores son detectados rápidamente.

Contar con un documento de higiene de los resolvedores DNS.

Capacitar de manera periódica a los administradores de redes y sistemas.

Monitorear puntos de comparación para detectar la explotación de resolución DNS y hayan tenido lugar con el fin de identificar las vulnerabilidades del software.

4.3.2.2 Buena práctica para mitigar malware que se dirige al DNS

Detectar este cambio es posible a nivel de ISP monitoreando el tráfico saliente del cliente DNS que lleve una resolución distinta de la que ellos proporcionan.

Sin embargo siempre queda la posibilidad y el cliente se suscriba a distintos servicios DNS y envíe su tráfico a otra parte.

Los clientes pueden ser engañados mediante ingeniería social o algún incentivo a cambiar a otra resolución de DNS (Figura 33).

Se deben conocer los caches DNS no locales consultados desde la red para poder identificar posibles DNS corruptas. Tener listado de las DNS legítimas y fraudulentos y bloquear con listas.

Asegurarse que los sitios tengan certificados de validación extendidos.

Apoyar DNS pasivos como el ISC (Security Information Exchange) quienes reciben notificación de DNS falsos y alertan sobre ellos.

Figura 33. Resolución DNS

Fuente Los autores

Ejemplo de este tipo de ataque es el troyano DNS Changer que atraía al usuario a este cambio ofreciéndole un dinero, en este caso se requirió la intervención FBI para tomar posesión de esas IP´S.

Tenga en cuenta que también hay ataques NO TECNICOS AL DNS, como:

Uso de dominios registrados con tarjetas de crédito robadas.

Uso de dominios maliciosos a los pocos minutos de haber sido creados.

Uso de subdominios maliciosos en dominio legítimos.

Uso de dominios semejantes al original pero que usan caracteres que no son parte de los caracteres latinos del dominio.

4.3.3 Buenas prácticas en la implementación

4.3.3.1 buenas prácticas de seguridad de IPSec

IPSEC permite mitigar las técnicas de sniffing y puede usarse para evitar ataques de Aplicación, pese a que trae dificultades para los IDS. Se usa también para blindara nivel de Aplicación, IPSec co-ayuda con los ataques de ‘Hombre-en-el-medio.

4.3.3.2 Buenas Prácticas En La Asignación De Direccionamiento

Se debe establecer con claridad que direcciones se van a usar públicas y privadas, también es importante resaltar la importancia de usar la aleatoriedad en la asignación de direcciones especialmente para los dispositivos de la infraestructura como Servidores, si se va a implementar el dual stack es necesario que el modelo de la red se copie idéntico para IPv6 nos referimos a conservar los modelos organizacionales de red (VLANs, redes, segmentación y DMZ).

En IPv6 se aplican los siguientes postulados para elegir de entre varias direcciones que tenga una interfaz con cual envía o recibe un paquete, siempre y cuando no haya otros criterios (aplicación o protocolo de capa superior):

- Se deben preferir direcciones pares, del mismo tipo (unicast con unicast).
- Se debe preferir la dirección de destino del ámbito más pequeño.
- Se debe preferir una dirección preferida sobre una obsoleta.
- Se debe preferir una dirección nativa a direcciones de transición (ISATAP o 6to4).
- Se debe preferir los pares de direcciones con el prefijo común más largo.
- Se debe preferir para dirección de origen, una dirección global a una temporal.
- Se debe preferir para Mobile IP, direcciones “home” sobre las “care-of”.

La RFC 3484 también permite fijar una política que puede reemplazar estos valores por predeterminados para las direcciones de origen y de destino. Por lo tanto teniendo en cuenta que se puedan aplicar este algoritmo es requisito indispensable que las tarjetas de red soporten la RFC3484.

Se deben monitorear las direcciones multicast en el sentido de quienes son sus integrantes y que no se deben enrutar en internet.

Para loopback sólo existe una dirección IPv6, en IPv4 era todo un bloque.

Las direcciones ULA son global y únicas pese a ellos no se deben enrutar en internet por lo que se debe filtrar su prefijo fc00::/7.

Para la administración de los segmentos de red se deben usar las link local fe80.

Las direcciones anycast solo pueden ser direcciones de destino nunca de origen.

Las direcciones Global asignadas a una LAN local son de miles de millones pese a ello es buena práctica aplicar subneting.

4.3.3.3 Buenas Prácticas en los mecanismos de configuración del direccionamiento

De los métodos de configuración de direcciones el más seguro pasa por una solución DHCPv6, sin embargo, la clasificación en general sería:

- Direcciones estáticas
- Autoconfiguración ‘Stateful’ con DHCPv6
- Autoconfiguración ‘Stateless’: con IID calculado aleatoriamente
- Autoconfiguración ‘Stateless’: IID a partir de la MAC

Otro punto importante a tener en cuenta es el uso de Direcciones Globales (excepto ULAs) ya que proporciona direccionamiento global, lo que no implica alcanzabilidad global. Por otro lado desmitificar esa falsa práctica de seguridad “NAT”, pues NAT no protege el que protege es una máquina de estados (firewall) que procesa los paquetes.

Las direcciones IEEE son asignadas centralmente y se pueden suponer únicas buscan atender a la preocupación por generar IIDs difíciles de adivinar y de seguir este concepto esta expresado en la RFC 4941 que añade una extensión a SLAAC que le permite a los nodos obtener IIDs aleatorios que cambien con él.

Las direcciones reservadas o especiales no deben usarse, se deben filtrar, así como protegerse de su uso como IP origen. También es una mala práctica construir direcciones similares a palabras como: ::DEAD:BEEF, ::CADA:CA5A o las famosas direcciones IPv4 mapeadas que son direcciones en apariencia IPv6 pero que llevan inmersas las direcciones IPv4 por ejemplo: 2001:df8::10.0.0.2, 2001:df8::11:0:0:2.

Tampoco se deben usar las direcciones IPv6 secuenciales tan típicas de IPv4 y recordar que EUI-64 entro en desuso, si por algún motivo se requiere asignar IPs debe hacerse manualmente con IID “complicados”(usando los 64 bits). Si la asignación es automática asegúrese que DHCP asigne IIDs aleatorios de un pool muy grande y para finalizar hacer uso de CGAs en caso de que se use SEND.

4.3.3.4 Configuración Stateless Con Router:

El host construye su dirección IPv6 basándose en los mensajes ICMPv6 de “Anuncio de Router (Router Advertisement)” que informan al host del segmento de red que routers IPv6 están conectados al segmento y así entregar a los hosts el prefijo con el que generaran las direcciones IPv6.

4.3.3.5 Configuración Automática DHCPv6:

Un servidor DHCPv6 puede entregar y configurar a un host una dirección IPv6 y de ser requerido otros parámetros de configuración como la IPv6 de los servidores DNS. La dirección Ip de los servidores DNS no es posible recibirla con un paquete Router Advertisement (enviando por los routers IPv6 de la red). El Router Advertisement que le llega a un host durante el descubrimiento de routers contiene información sobre si se va a utilizar también DHCPv6 para configurar la dirección IPv6.

4.3.3.6 Configuración Manual De La Dirección:

Como ya se expresó los host no requieren de configuración manual, este tipo de configuración es propia de servidores y/o routers IPv6. Se realiza mediante comandos IP (Linux) o el set de comandos Netsh en Windows y como es de costumbre puede hacerse por la interfaz de comandos o por consola gráfica, entornos ya habituales en los sistemas operativos modernos.

4.3.3.7 Buenas prácticas de seguridad en capa dos o capa de enlace

La primera buena práctica al respecto del protocolo IPv6 consiste en la formación de la gente de TI lo que implica tener personal actualizado para que pueda entender cómo se moverá ahora la red y cuando haya una situación pueda entender lo que pasa.

Tener una identificación detallada de la red (dispositivo, serie, mac, firmware, configuración, deshabilitación de puertos sensibles o sin uso), tipo y versiones de software de tal manera que se evidencie su bastionado. Usar IPS de perímetro ante posibles escaneos.

El diseño de la red debe tener en cuenta el uso de direcciones globales (GUA) para tener control sobre las comunicaciones de extremos a extremo.

Segmentar la red en varias sub-redes físicas o virtuales (VLANs). Requiere distintos prefijos de red y al menos un elemento de capa 3 que haga el routing entre LANs/VLANs.

Identificación en capa 2 por MAC para dispositivos y/o limitar su acceso a la red, por Ejemplo: APscon filtrado por MAC. Switchcon “Port Security” solo permite

acceso a una MAC por un puerto. Otra buena práctica relacionada con el Switch es establecer una contraseña robusta para el switches con password y hash tipo MD5. En este mismo sentido se considera buena práctica el cifrado de datos para proteger la tabla ARP.

4.3.3.8 Buenas prácticas ataques de ip

Filtrar el tráfico descartando el tráfico con direcciones de origen por fuera del rango o con tipo de direccionamiento no acorde al tráfico.

De ser posible tener ISP con BGPSEC que protege criptográficamente los anuncios de ruta y evita publicación de datos falsos.

Consultar los dominios RIR para verificar una identidad de los dueños de un ciberespacio.

4.3.3.9 Buenas prácticas de seguridad en capa tres o capa de red

Configuración en la capa de transporte de protocolos que añaden seguridad como TLS, DTLS y SSL entre los principales.

4.3.3.10 Buenas prácticas para ICMP

El primer fragmento de un paquete debe llevar la información de la capa superior y de las cadenas de cabecera.

No permitir fragmentos superpuestos.

Filtrar paquetes pequeños (Tiny).

Eliminar paquetes a la espera del último fragmento pasados 60 segundos.

Eliminar paquetes marcados como único fragmento (Frag. Offset y M = 0).

No permitir Fragmentos dentro de Fragmentos.

Inspeccionar el tráfico encapsulado a través de firewall o IDS.

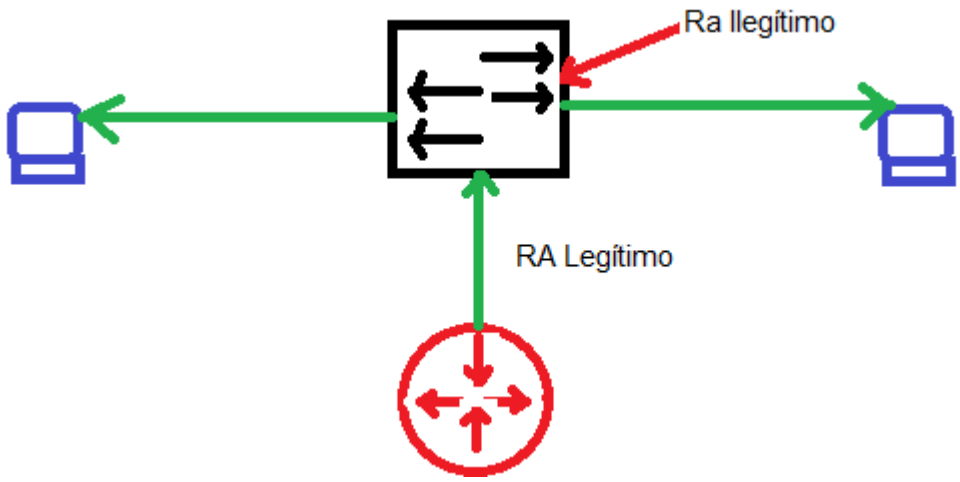
Las organizaciones pueden aprovechar algunos firewalls y dispositivos IPS para detener ataques smurf. Las soluciones diseñadas para detectar y proteger las redes de asaltos DDoS pueden detectar fácilmente este tipo de ataques. Los ataques de Packet Flooding en IPv6 se caracterizan por tener cabecera de routing tipo 0.

4.3.3.11 Buenas Prácticas Para Los Protocolos De Configuración O De Información Para Hosts

Los Certificados X.509: El protocolo SEND utiliza los Router Advertisement (RA) para su descubrimiento de vecinos, por lo que es importante asegurar esos RA a través de certificados. Los certificados X.509 estampan la firma en todos los mensajes de Ras. Estos certificados deben ser expedidos por una CA confiable. Por esta implementación en el protocolo ICMPv6 hay dos tipos de mensajes: los CPS (Certification Path Solicitation) a través del cual el host solicita al enrutador una ruta y los CPA (Certification Path Advertisement) que son la retroalimentación al mensaje anterior el cual incluye el certificado.

Ra-Guard: Los RA o router advertisement es un tipo de mensaje "muy poderoso" por lo que puede ser usado para múltiples ataques o causar problemas de manera accidental principalmente por fallas en la configuración del Administrador o del usuario, por ataques malintencionados de tal suerte que en una red pueden existir Ras lícitos e ilegales o problemáticos. En la Figura 34 vemos el funcionamiento de RA-Guard en una red.

Figura 34. Funcionamiento de RA-Guard en una red



Fuente Los Autores

Funcionamiento De Ra Guard: Se aplica en los dispositivos de nivel 2 (switches) que son quienes pueden identificar Ras con el fin de detectar Ras inválidos y bloquearlos, esto a través de establecerle una regla al Switch que le indique cual es el puerto válido para RAs. Esto parte del supuesto que todos los mensajes pasan por el switch, no se envían directamente entre hosts. RA Guard junto a los certificados X.509 son una excelente práctica de seguridad. La implementación de RA-Guard puede ser Stateless RA Guard o Stateful RA Guard, en la RFC6105 esta descrita en detalle la implementación de esta buena práctica de seguridad en

conjunto con el uso de SEND. Otra forma de implementar RA Guard es a través del uso de ACLs en Switches L2 gestionables.

Snooping Dhcp O Dhcp R-Guard: Conocido también como DHCP Guard son técnicas que permiten asegurar la asignación DHCP haciendo que los host solo puedan trabajar con las IP que le fueron asignadas y de igual forma que el o los servidores DHCP sean los autorizados, esto también facilita le georeferenciación de las máquinas de ser necesario. Esto se logra a través de la configuración de una Lista Blanca en el Switch de puertos de direcciones IP que pueden acceder a la red, así el servidor DHCP dirige el control de acceso de tal manera que las direcciones IP con direcciones MAC específicas y en puertos definidos tienen acceso a la red. De otra parte snooping DHCP controla los servidores DHCP e impide añadir un DHCP no autorizado (Rogue DHCP) ya que un servidor ilegal puede controlar o inducir al fallo de la red corporativa. Otras técnicas interesantes son IPv6 Destination Guard (o ND Resolution rate limiter) que es una variación de esta técnica en razón de un tiempo de respuesta.

Buenas prácticas de seguridad para DHCPv6: Implementación del DHCP Unique ID o DUID que remplaza las direcciones MAC por un ID Único así que cada servidor y cada cliente tienen un DUID que hacen más seguro a DHCPv6. La mejor implementación, en temas de seguridad para DHCPv6 es la stateful que requiere de un prefijo GUA y un IID aleatorio (RFC 3315).

Otra buena práctica es la implementación de Secure DHCPv6 que es un mecanismo autenticación e integridad basado en PSK simétrico que permiten verificar las identidades cliente/servidor (clave publica/privada + PKI) y permiten comprobar la integridad del mensaje DHCPv6.

Al igual que con IPv4 se requiere de un IPS/IDS para detectar posibles DHCPv6 Server ilícitos en la red.

Buenas Prácticas De Seguridad Para NDP: Sus mensajes deben tener Hop Limit =255, los mensajes con valores diferentes deben ser descartados. Otra buena práctica es el uso de la funcionalidad RA-Guard, manejar el routing HeaderType0 [RFC5095]. Trabaja con mayor de seguridad si se activa IPSec pero sin duda la mejor práctica es el uso de SEND en lugar de NDP.

Buenas Prácticas De Seguridad Para MLD: Limitar la CPU (hardware) la tasa de mensajes MLD REPORTS aceptados, limitar en memoria el número de estados asociados a MLD. La dirección de origen siempre debe ser una link local, el hop limit debe ser 1 y los mensajes que no cumplan se deben descartar.

MLD Snooping: Es una buena práctica de seguridad basada en switch que solo permiten el tráfico multicast en puertos con listeners, así el switch construye una

tabla MLD de grupo multicast vs puertos que lo han solicitado. Escucha REPORTs.

MLD Guard: Es filtrado mediante ACL que controlan los puertos de las QUERIES (ICMPv6 type 130), sólo permiten puerto con router multicast.

Protección de los Routers: Limitar la frecuencia de aceptación de REPORTs de cada host, descartando los que excedan ese tiempo, además si no se usa routing multicast inter-dominio se debe desactivar la funcionalidad de router multicast/MLD.

Otras Buenas Prácticas Para Garantizar Ras Legítimos

- Usar Router Preference Option [RFC4191].
- Usar filtrado de paquetes en el Host.
- Monitorizar el enlace (con aplicaciones como NDPmon).
- Los mensajes ICMPv6 usados por estos protocolos deben tener Hop Limit de 255, para tener la certeza que el paquete se generó en el enlace.

4.3.3.12 Buenas prácticas en los protocolos de Routing

Mientras una red corporativa maneje nodos IPv4 e IPv6 se debe activar la doble pila y tener el mismo esquema lógico en la red IPv4 que en la red IPv6. Los routers deben configurarse para que sean gestionables por IPv4 e IPv6. Los procesos de routing son con protocolos diferentes por lo que el consumo de recursos como CPU, Memoria es diferente según los trabajos de monitorización, gestión y solución de problemas. Se debe tener actualizaciones al día en el firmware del router y conocer con exactitud que funcionalidad está soportada para IPv6. Por el router y cuáles no.

Los protocolos más seguros para infraestructura NO Cisco son OSPFv3 e IS-IS y para infraestructura Cisco se recomienda EIGRPv6 y para Border MBGP. Las amenazas se afrontan empezando por las amenazas generales de Internet, las del protocolo de borde y las de routing interno.

Packet Flooding: Se pueden atender contando con buenos equipos firewalls y dispositivos IPS para detener estos ataques. Para tal fin hay que contar con soluciones diseñadas para detectar y proteger las redes de asaltos DDoS y se debe filtrar la cabecera de routing tipo 0. Aplicar las recomendaciones de filtrado de paquetes presentadas más adelante en esta guía.

Gusanos (Worms): Se deben implementar la seguridad para los protocolos p2p e IM, pero se es más susceptible si usan IP como slapper que permite hacer flooding IPv6 O W32/Sdbot-VJ que aunque no usa IPv6 se instala como

wipv6.exe simulando archivos de IPv6 en Windows. Aplicar las recomendaciones de filtrado de paquetes presentadas más adelante en esta guía.

Ataques DDoS: Estos ataques son iguales en las dos pilas del protocolo IP con la salvedad que IPv6 tendrá mayor cantidad de dispositivos en Internet, pese a ello también hay que destacar que puede ser más fácil de establecer la trazabilidad del atacante ya que el direccionamiento IPv6 es jerárquico y ordenado. Aplicar las recomendaciones de filtrado de paquetes presentadas más adelante en esta guía.

Seguridad para BGP

- Usar claves secretas compartidas en los peering
- Controlar el TTL de los paquetes BGP (RFC 5082)
- Prevenirse contra AS_PATH largos
- Limitar el número de prefijos recibidos
- Prevenirse contra BGP updates con ASN privado
- Usar direcciones loopback para peering (iBGP)(+IGP)
- Filtrado de prefijos de las direcciones según su ámbito
- El Remote Triggered Black Hole Filtering (RTBH) es igual que en IPv4.

Seguridad en IGPs

Para el protocolo RIPng pide usar IPSec, RIPng no soporta autenticación usando MD5, es un protocolo poco seguro.

Para el protocolo EIGRPv6 y teniendo en cuenta que este protocolo ha tenido vulnerabilidades como información en texto claro, uso de multicast y los famosos mensajes goodbye se debe habilitar la autenticación MD5 y vecinos estáticos (en lo posible), y el uso de comunicaciones unicast para mensajes hello.

Para el protocolo IS-IS que es menos usado que OSPFv3. El protocolo IS-IS tiene dos modos: Single-topology y multitopology. El modo Single Topology optimiza recursos con las mismas métricas que usa la versión de IPv4, al igual que la misma topología. El modo Multitopology consume más recursos que el modo Single. Se caracteriza por ser flexible lo que permite tener topologías distintitas para IPv4 e IPv6, además soporta autenticación vecinos con password y MD5.

Para el protocolo OSPF empezar por aclarar que OSPFv2 es para IPv4 y soporta autenticación MD5 y OSPFv3 es para IPv6 y soporta autenticación MD5 pero de distinta manera, no en campos del mensaje Hello, hace uso de IPSec que proporciona integridad (AH) y confidencialidad (ESP).

Consideraciones De Seguridad Generales En El Routing

- Implementar ingress y egress filtering de tráfico IPv6
- Deshabilitar routing en interfaces LAN no necesarias
- Usar protocolos con características de seguridad
- Aprovechar características de seguridad de los protocolos

4.3.3.13 Filtrado con IPv6

Los firewall del nodo destino deben procesar no sólo la cabecera básica de un paquete IPv6 sino también las cabeceras de extensión y los datos ya que en ellos puede ir código malicioso.

La primera buena práctica es asegurarse que los paquetes IPv6 (ICMPv6) no estén filtrados en una red, más en detalle revisar la cabecera del paquete IPv6 el campo Next header este marcado con 58 que es el número asignado para paquetes ICMPv6. Los mensajes de ICMPv6 de Error manejan de los tipos 0 al 127, sin embargo en la actualidad solo se han activado los tipos 1 al 4 por ende todo mensaje de error identificado como tipo 5 al 127 o tipo 0 debe ser analizado ya que NO corresponde a una implementación estándar, por su parte los mensajes informativos de ICMPv6 tienen tipos válidos del 128 al 255.

Filtrado de paquetes del tráfico a través de ACLs y Firewalls y el filtrado de prefijos y rutas (BGP/IGP). Ver la Tabla 15. Reglas de filtrado más comunes para BGP.

Tabla 15. Reglas de filtrado más comunes para BGP

TYPE – CODE	**DESCRIPTION**	**ACTION**
Type1 – all	Destination unreachable	Allow
Type2 – all	Packet Too Big	Allow
Type3 – code 0 y 1	Time exceeded	Allow
Type4 – code 0, 1 y 2	Parameter Problem	Allow
Type 128	Echo Reply	Allow for connectivity check and some services. Rate limit.
Type 129	Echo Request	Allow for connectivity check and some services. Rate limit.
Type 130,131,132, 143	MLD	ALLOW if Multicast or MLD goes through FW

Type 133	Router Solicitation	ALLOW if NDP goes through FW
Type 134	Router Advertisement	ALLOW if NDP goes through FW
Type 135	Neighbor Solicitation	ALLOW if NDP goes through FW
Type 136	Neighbor Advertisement	ALLOW if NDP goes through FW
Type 137	Redirect	NOT ALLOW
Type 138	Router Renumbering	NOT ALLOW
Type 139 y 140	Node information Query & Reply	NOT ALLOW

Fuente RFC 4890[33]

En IPv6 se hace obligatorio hacer filtrado de las cabeceras de extensión, en contraposición de IPv4 con las options del encabezado.

Filtrado De Paquetes Fragmentados

Se hace necesario el filtrado de fragmentos enviados a los host para evitar ataques DoS. Todo datagrama fragmentado menor a 1280 bytes (excepto el último) debe ser filtrado. Si un fragmento es entregado después de los 60 segundos debe descartarse.

Hacer reglas homogéneas en la medida de lo posible de tal forma que no se presenten escenarios donde se restringa todo con IPv6 y se permita todo con IPv4. Contar con un Firewall que soporte filtrado por dirección origen y destino, inspección de paquetes encapsulados y de las cabeceras de extensión, filtrado según necesidades de capas superiores.

Filtrado Con ACLs (Listas De Control De Acceso)

Son una herramienta para controlar el tráfico en los equipos de red (routers, algunos switches) permitiéndolo o denegándolo en una dirección IP. Al igual que con IPv4 las listas de control de acceso permiten establecer una condición que

[33] RFC4890 - Internet Control Messages Protocol, (ICMP) Specification. *Tools.ietf.org*. Fecha de consulta: 9 Mar 2018, from https://tools.ietf.org/html/rfc4890

determina el tráfico de un router, veamos dos ejemplos de la ingeniera Rosa Estriégana:

Ejemplo 1. Creación de la ACL

ipv6 access-list nombre-de-lista

Definición de las reglas a través de permitir o denegar, observemos que se específica el protocolo (IP | TCP | UDP | ICMP | telnet) a través de comparación como gt = greater than, lt = lesser than, eq = equal y el origen de una sola ip: host u el origen de cualquier ip: any.

permit tcp 2001:8BD::1/32 eq telnet any

Finalmente se aplica la ACL a una interfaz y se define si es

***ipv6 traffic-filter nombre-de-lista [out/in** si la regla es de entrada o salida]*

IPv6 soporta ACL extendidas por lo que se puede especificar el protocolo y las direcciones de origen y de destino. Recordemos que las ACL deben ir cerca del destino por el contrario las ACL extendidas deben ir cerca del origen. Si el switch soporta IPv6 se pueden definir ACL para proteger los RA DHCPv6, veamos:

1) Ethertype en la cabecera Ethernet (siempre 0x86DD)

2) Source MAC address en la cabecera Ethernet

3) Destination MAC address en la cabecera Ethernet

4) Versión debe ser IPv6

5) Source IPv6 address en la cabecera IPv6

6) Destination IPv6 address en la cabecera IPv6

7) Next-header en la cabecera IPv6

8) Type y Code en la cabecera ICMPv6

9) UDP source port

10) UDP destination port

Ejemplo 2. Filtrado ACL en switches

Protección entrada

ipv6 access-list INBOUND-ACL

remark permitir paquetes NDP

permit Icmp any any nd-na

permit Icmp any any nd-ns

permit Icmp any any router-advertisement

permit Icmp any any router-solicitation

remark Denegar RH0 y otras cabeceras de extensión desconocidas

deny ipv6 any any routing-type 0 log

deny ipv6 any any log undetermined-transport

permit ipv6 any any

!

interface FastEthernet0/0

ipv6 address 2001:dd3::1

ipv6 traffic-filter INBOUND-ACL in[34]

Filtrado De Prefijos IPv6

A nivel de seguridad en IPv6 se deben filtrar los prefijos no asignados para ello se sugiere denegar todo y luego activar sólo los que se van a usar, esta activación puede ser gruesa por ejemplo permitiendo 2000::/3 o más refinado permitir 2600:0000::/12.

Otro de los prefijos a controlar son las ULA que no deben entrar ni salir de la red corporativa en otras palabras estos prefijos no debe enrutarse en Internet.

[34] ESTRIÉGANA, Rosa. (2017). Listas de control de acceso ACLs. Laboratorio de redes de computadores, Universidad de Alcalá.

Se debe filtrar también los bordes del site-scoped multicast.

Se deben activar los prefijos Multicast con los que se va a trabajar.

Filtrado De Prefijos BGP

Esta práctica que ya es muy común y necesaria sobre redes IPv4 en los ISP le permite al proveedor recibir tráfico de prefijos que sabe los tienen asignados sus clientes. Los ISP también deben filtrar los prefijos no asignados o reservados ya que no son enrutables en internet: como los ULA, los de Link-local, 6bone, y otros establecidos en la RFC 5156, nuevamente lo mejor es bloquear todo y permitir solo las direcciones globales (RFC 4291).

La configuración de BGP se puede configurar de dos maneras: prefix-list o route-map. Route-map utiliza per se una prefix-list lo que la hace la opción más robusta y flexible a través de ella se permite o no, la ruta que al cotejarla coincida. El prefix-list es la manera con la que se establece si la ruta tiene coincidencia o no. El route-map por defecto deniega todo, para permitir todo se debe ingresar un registro de permit.

4.3.3.14 Buenas prácticas en los mecanismos de transición

Contar con un diagnóstico de software, hardware y recursos humanos en razón de su compatibilidad IPv4/IPv6. Es necesario aplicar una política de seguridad en redes con dos tecnologías diferentes a través de listas de control de acceso (ACL) y reglas de cortafuegos en ambas pilas IPv6. Las técnicas de transición en IPv6 en algunos casos son tan especializadas, por lo que solo funcionan en determinados entornos.

Monitoreo permanente del tráfico de red con el fin de analizarlo y tomar las acciones que correspondan a las situaciones vulnerables detectadas. Planificar la elección y adquisición de software (Sistemas Operativos IPv6 Ready) y hardware (Firewall, Detector de intrusos IPS) de gestión de redes IPv4/IPv6 compatible entre sí y con soporte para IPv6. El resultado de esto es que se utiliza IPv6 en islas que se comunican a través de IPv4. A continuación se describen algunos mecanismos para llevar a cabo esta transición.

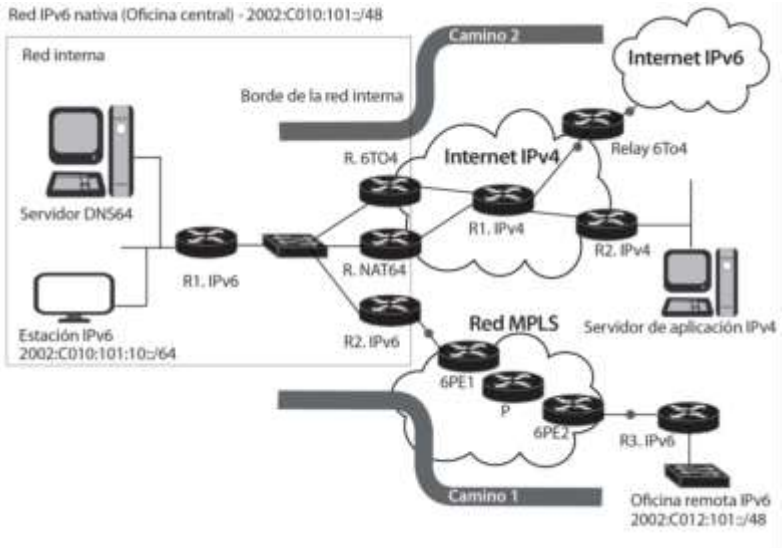
Aunque se ha trabajado para facilitar la migración durante la última década, la realidad es muy diferente a lo que la industria había planeado. Existen varias razones para esta realidad, como la existencia de dispositivos de red incompatibles, proveedores ISP que no soportan IPv6, o los costes de migración de una tecnología que no parece inmediatamente necesaria.

Buenas Prácticas En La Implementación De Dual Stack: Imprescindible la formación del recursos humano, la selección del segmento de red con menor tráfico para llevar a cabo una prueba piloto, la configuración de IPv6 en este segmento, el monitoreo del nuevo tráfico y la estabilidad de la implementación. Logrado esto se debe trazar una planeación por segmentos, aplicar el plan de transición e iniciar la implementación de IPv6, mientras se vigila el tráfico IPv6 y se estabiliza la convivencia de las dos pilas IPv6, de esta manera se minimizan los riesgos de utilizar ambos protocolos en una misma red. Una de las mejores prácticas de seguridad es el uso de la funcionalidad RA-Guard, manejar el routing Header Type0 [RFC5095].

Buenas prácticas de seguridad en el mecanismo de traducción Es el mecanismo de transición menos recomendado pues tiene un alto riesgo de romper las aplicaciones o servicios, además que dificulta la resolución de ataques y delitos informáticos ya que impide la geolocalización que se requiere. Este mecanismo de transición es el más costoso.

Reglas de filtrado en los mecanismos de transición: Garantizar la aplicación de estas reglas de filtrado de paquetes IPv6 según el mecanismo de transición implementado.

Figura 35. Ejemplo de una red IPv6 diseñada con los mecanismos 6to4, NAT64 + DNS64 y 6PE sobre MPLS



Fuente Luis E. Bolívar (2012)[35]

[35] BOLIVAR, Luis et al. (2012) Diseño e implementación de una red IPv6 para transición eficiente desde IPv4, Escuela de Ingeniería Eléctrica y Electrónica, Universidad del Valle, Cali, Colombia

Tabla 16. Reglas de filtrado en los mecanismos de transición

Tecnología	Regla de Filtrado
IPv6 Nativo	EtherType 0x86DD
6in4	IP proto 41
6in4 (GRE)	IP proto 47
6in4 (6-UDP-4)	IP proto 17
6to4	IP proto 41
6RD	IP proto 41
ISATAP	IP proto 41
Teredo	UDP dest port 3544
Tunnel Broker con TSP	(IP proto41)||(UDP dst port 3653||TCP dst port 3653)

Fuente IPv6 Forum

4.3.3.15 Buenas prácticas de seguridad en capa de aplicación

La implementación de la ISO y un framework de programación seguro que tiene entre otras el uso de HTTPS (si no te interceptan la conexión), cerrando de sesión adecuado en las aplicaciones y hasta donde sea posible uso de cookies válidas sólo por la sesión, recordar también que en IPv6 se manejan cadenas y datos “más grandes” lo que puede llevar a un “overflows”. Se debe garantizar que las aplicaciones en los desarrollos usen las librerías correspondientes a IPv6 en vez de las IPv4; este es el error más frecuente en las implementaciones de aplicaciones IPv6.

También es importante el uso de aplicaciones que envían su información cifrada, es importante el uso de aplicaciones seguras de HTTPS, SSH, SCP, POP3S, IMAPS.

En la medida que la aplicación lo permita se deben cambiar los Protocolos y puertos asociados al mismo, por ejemplo es oficial que el puerto 21 es para FTP, el puerto 23 para SSH o el 443 para HTTPS. Así las cosas puedo configurar bajo el puerto 8080 un proxy HTTP, también se busca utilizar los puertos superiores al 30000 ya que su sola estructura de cinco dígitos en si misma da complejidad al tema. Todos los cambios deben quedar documentados. Utilizar versiones seguras de los protocolos de gestión de red, por ejemplo: SNMP Versión 3.

5. CONCLUSIONES

Las redes de computadores y dispositivos electrónicos son vulneradas principalmente en tres aristas, a saber: el plano de control donde tiene alta relevancia la seguridad de los dispositivos de la red, el transporte en sí mismo y el software que opera en los host y servidores de la red. IPv6 presenta mayor vulnerabilidad comparada con IPv4, en el sentido que la extensión de estas tres zonas es mayor, esto implica nuevos puertos abiertos, la presencia de nuevos protocolos en los host, la posibilidad de nuevas vulnerabilidades aun no conocidas y la falta de personal calificado en el Protocolo IPv6.

Es necesario aplicar una política de seguridad en redes para las dos tecnologías activas (IPv4 e IPv6), muchas de estas políticas se implementan a través de listas de control de acceso (ACL) y reglas de cortafuegos en ambas pilas del protocolo IP. Las técnicas de transición en IPv6 en algunos casos son tan especializadas, que solo funcionan en determinados entornos, por lo que es necesario garantizar esos entornos si fuera el caso. Esto se complementa con un monitoreo permanente del tráfico de red con el fin de analizarlo y tomar las acciones que correspondan a las situaciones vulnerables que se puedan detectar.

Es imprescindible planificar la elección y adquisición de software (Sistemas Operativos IPv6 Ready) y hardware (Firewall, Detector de intrusos IPS) de gestión de redes IPv4/IPv6 compatible entre sí y con soporte para IPv6. El resultado de esto al día de hoy es que se utiliza IPv6 en islas que se comunican a través de IPv4. En ese mismo sentido es importante considerar muy bien el proveedor ISP que soportara la comunicación IPv4 e IPv6 y los temas de costos.

Dentro de las grandes ventajas de trabajar con el protocolo IP de nueva generación sobre IPv4, tenemos:

- Provee Comunicación extremo a extremo.
- Proveer de un gran número de direcciones IP de formato más amplio (128 bits).
- Proveer seguridad mediante la implementación nativa, más no obligatoria de IPSec, que permite disponer de servicios de cifrado y autenticación.
- Permitir la prestación de nuevos servicios como: la autoconfiguración.
- IPv6 facilita la interconexión de dispositivos diversos (Internet Cosas) en los nuevos estándares de las comunicaciones: IPv6, DENSE e IPSec.

La implementación de IPv6 se está dando y es inevitable, por ello por un buen tiempo van a coexistir IPv4 e IPv6 a través de los mecanismos de transición, ya que hay dispositivos y aplicaciones que no son compatibles con las dos pilas.

El principal aporte a la seguridad en IPv6 es la incorporación nativa IPSec cuyo fin es dar seguridad a las comunicaciones en la capa de red y a los protocolos de capa superior; con la cantidad de direcciones IPv6 disponibles por segmento de red es casi imposible hacer escaneos de direcciones y esto dificultad en gran manera la posibilidad de hacer ataques de fuerza bruta o ataques de tipo broadcast, ya que este tipo de comunicación desaparece en IPv6. Finalizamos resaltando que en las redes IPv6 son más seguras y rápidas ya que no requieren de NAT y la fragmentación sólo se da en los nodos extremos.

6. RECOMENDACIONES

Se requiere que las nuevas aplicaciones de misión crítica de una empresa hagan uso del campo calidad de servicio para tener un tráfico preferencial cuando la aplicación así lo amerite. En IPv4 las aplicaciones sólo trabajan tráfico de mejor esfuerzo por lo que no hay calidad de servicio real.

Se debe buscar que el tiempo de convivencia de nodos IPv4 con redes IPv6 sea el más corto posible ya que la seguridad en IPv4 representa una mayor vulnerabilidad que hace comprometer la red.

La característica de Plug and Play de IPv6 puede ser segura con la implementación de prácticas como RA-GUARD, los certificados X.509 u otras prácticas para garantizar RA (Router Advertisement) legítimos.

Las mayores prestaciones de seguridad en una Red las da IPv6 cuando se implementa IPSec, por lo tanto para entornos muy seguros se recomienda la activación de esta directiva de seguridad.

El uso de herramientas de seguimiento, análisis y monitoreo en redes IPv6 se debe restringir a los administradores de redes y a los implantadores de directivas de seguridad.

IPv6 representa la posibilidad de un nuevo mercado para herramientas de monitoreo de redes ya que en la actualidad el mercado está dirigido a IPv4 en un 90%.

Se recomienda iniciar los procesos de implementación del protocolo IPv6 lo más pronto posible ya que con el tiempo dicha transición será más costosa y puede implicar un mayor riesgo.

ÍNDICE

REFERENCIAS BIBLIOGRÁFICAS

AGARWAL Monika y Singh Abhinav, Metasploit Penetration Testing Cookbook, 2012. Pack Publishing.

ÁLVAREZ Moraga, Sebastián Andrés, González Valenzuela, Agustín José, Estudio y configuración de calidad de servicio para protocolos IPv4 e IPv6 en una red de fibra óptica wdm. Revista Facultad de Ingeniería [en línea] 2005: Fecha de consulta: 27 de febrero de 2018] Disponible en: http://www.redalyc.org/articulo.oa?id=11414672014ISSN 0717-1072.

BOLÍVAR, Luis, et al. Diseño e implementación de una red IPv6 para transición eficiente desde IPv4, Escuela de Ingeniería Eléctrica y Electrónica, Universidad del Valle; 2012, Cali, Colombia.

CASTILLO MEDINA, CARLOS A., FORERO RODRÍGUEZ, FELIPE, Caracterización de IPv6. Tecnura 2013, 17 (Abril-Junio) [en línea]: Fecha de consulta: 27 de febrero de 2018] Disponible en: http://www.redalyc.org/articulo.oa?id=257028093010ISSN 0123-921X.

CISCO, Cisco SAFE Reference Guide [en línea]; 2007. Fecha de consulta: enero 30 de 2018, Disponible en: https://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Security/SAFE_RG/SAFE_rg/chap2.pdf

CISCO, Configuración de Listas de Acceso IP [en línea]; 2007. Fecha de consulta: enero 30 de 2018, Disponible en: https://www.cisco.com/c/es_mx/support/docs/security/ios-firewall/23602-confaccesslists.html

COLS, Carolina. Fundamentos de la seguridad informática [en línea]; 2012. Fecha de consulta: enero 18, 2018, Disponible en: https://carolinacols.files.wordpress.com/2012/03/fundamentos-bc3a1sicos-de seguridad-informc3a1tica.pdf.

De León, O. Despliegue de IPv6 para el desarrollo socio económico en América Latina y el Caribe; 2016 [en línea], LACNIC, CAF. Disponible en: http:// http://www.scioteca.caf.com/handle/123456789/837.

DEPARTAMENTO ADMINISTRATIVO PARA LA FUNCIÓN PUBLICA, Metodología para la administración del riesgo [en línea]. Consultado mayo 2017. Disponible en: http://www.funcionpublica.gov.co/documents/418537/506911/1592.pdf/73e5a159-2d8f-41aa-8182-eb99e8c4f3ba.

DEPARTAMENTO NACIONAL DE PLANEACIÓN, Política Nacional de Seguridad Digital – CONPES 3854 [en línea]. Consejo nacional de política económica y social, República de Colombia, departamento nacional de planeación. Disponible en: https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3854.pdf.

ESTRIÉGANA, Rosa. Listas de control de acceso ACLs. Laboratorio de redes de computadores [en línea], Universidad de Alcalá. 2017. Consultado noviembre 2017 Disponible en: atc2.aut.uah.es/~rosa/.

GEROMETTA, O. IPv6 - Introducción. Mis Libros de Networking [en línea]. 2008, consultado mayo 2017. Disponible en: http://librosnetworking.blogspot.com.co/2008/09/IPv6-introduccin.html.

GÓMEZ López, J., Villar Fernández, E. and Alcayde García, A. Introducción a la seguridad informática. En (Ed.), Seguridad en sistemas operativos Windows y GNU/Linux. Ra-Ma. Ed. 2011. (pp.13-41) Madrid, España

GÓMEZ Prieto, N. y Torres Rojas, Y. Migración de red IPv4 A IPv6 sobre la red del ejército nacional Colombia [en línea], 2008. Consultado noviembre 2017. Disponible en: http://hdl.handle.net/10596/1570.

INFOBLOX IPv6 COE Blog, The IPv6 Center of Excellence (COE) [en línea]. 2012. Fecha de consulta: 12 abril 2018, Disponible en: https://community.infoblox.com/t5/IPv6-CoE-Blog/.

IPv6 FORUM (febrero 2018). Curso Certified Security Engineer IPv6. IPv6 forum Ed. 2018.

ISO/IEC 27005:2011, Tecnología de la Información. Técnicas de Seguridad. Administración de Riesgos de Seguridad de la Información.

MADERA V., Lennart Enrique, Roa G., Mario Alejandro, Cuéllar Q., Juan C., A guide to best practices for the transition from IPv4 to IPv6. Sistemas & Telemática [en línea] 2015, 13 Fecha de consulta: 27 de febrero de 2018] Disponible en: http://www.redalyc.org/articulo.oa?id=411543658006 ISSN 1692-5238.

MAESTRIA I Taller de investigación Unidad 5. La delimitación del problema. Disponible en: https://sites.google.com/site/maestriaitallerdeinvestigacion/unidad-2.

MARTINEZ, D. Seguridad Informática [Ethical Hacking, Pen-test, Anti Script-kiddies] [en línea]. 2015. Fecha de consulta: 6 noviembre 2017, Disponible en: http://antisec-security.blogspot.com.co/2015/02/sparta-red-de-herramientas-para.html.

MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES [en línea]. Consultado mayo 2017. Disponible en: http://www.mintic.gov.co/portal/604/w3-channel.html.

NTC-ISO27001:2013, Tecnología de la Información. Técnicas de Seguridad Sistemas de gestión de seguridad de información. Descripción y vocabulario.

NTC-ISO27002:2013, Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de la Seguridad de la Información. Requisitos.

NTC-ISO 31000. La gestión de riesgos, principios y directrices.

O´Flaherty, C. (Ed.1). IPv6 para Operadores de Red [en línea]. Buenos Aires, Argentina: Editorial Asociación Civil Argentinos en Internet. 2014. Consultado Marzo 2018. Disponible en: http://portalipv6.lacnic.net/.

PERDOMO Vargas, M., Sabogal Rozo. E. Introducción A La Seguridad De Los Sistemas Operativos. En (Ed.) Curso Seguridad De Sistemas Operativos Modulo Del Curso. Universidad Nacional Abierta y a Distancia. 2012. (pp.10-36) Huila, Colombia.

PHASE-2 Interoperability Test Scenario IPSec Technical Document Revisión 2.0.0b. [En línea]. IPv6 Ready Logo Committee and IPv6 Forum. 2017. Consultado 27 enero 2018 Disponible en: https://www.ipv6ready.org/docs/Phase2_IPSec_Conformance_v2_0_0b.pdf.

RAGHAVAN S.V. et Dawson E., An Investigation into the Detection and Mitigation of Denial of Service (DoS Attacks), 2011, Springer Ed.

RADWARE, global application & network security report [en línea]. 2016. Fecha de consulta: 30 de Marzo 2018, disponible en www.radware.com.

RFC 2460 - Internet Protocol, Version 6 (IPv6) Specification [en línea]. IETF Org. Fecha de consulta: 7 Octubre 2017, Disponible en: https://tools.ietf.org/html/rfc2460.

RFC 4291 - Internet Protocol, Version 6 (IPv6) Addressing Architecture [en línea]. IETF Org. Fecha de consulta: 7 Febrero 2018, Disponible en: https://tools.ietf.org/html/rfc4291.

RFC 760 - DoD standard Internet Protocol [en línea]. IETF Org. Fecha de consulta: 2 Noviembre 2017, Disponible en: https://tools.ietf.org/html/rfc760.

RFC 791 - Internet Protocol [en línea]. IETF Org. Fecha de consulta: Noviembre 2017, Disponible en: https://tools.ietf.org/html/rfc791.

RICO Bautista, Dewar Willmer, Medina Cárdenas, Yurley Constanza, Santos Jaimes, Luz Marina, IPSec DE IPv6 EN LA UNIVERSIDAD DE PAMPLONA. Scientia Et Technica [en línea] 2008, XIV (Septiembre-Sin mes): Fecha de consulta: 27 de febrero de 2018] Disponible en: http://www.redalyc.org/articulo.oa?id=84920503057ISSN 0122-1701.

RODRÍGUEZ, I., Cartagena Díaz, B., Acosta Caicedo, L., Tovar, P. y Alape, M. Diplomado profundización CISCO [en línea]. (Tesis de pregrado). Universidad Nacional Abierta y a Distancia. 2017, consultado 27 marzo 2018. Colombia. Disponible en: http://hdl.handle.net/10596/14769.

SABOGAL Ortiz, A. Elaboración de una guía abierta para la administración de riesgos de seguridad en el protocolo de internet IPv6 sobre estándares de enrutamiento dinámico en equipos con plataforma CISCO [en línea]. 2017. Colombia: Disponible en: http://hdl.handle.net/10596/12015.

Seguridad y protección. (s.f). Curso de sistemas operativos [en línea]. Universidad de Murcia. 2016. Fecha de consulta: enero 18, 2018 Disponible en: http://www.ditec.um.es/so/apuntes/teoria/tema7.pdf.

THE BEST OF PENTEST MAGAZINE, Vol I Nro I. Software Press. 2012. (pp. 188-195).

TIKHIY, Yar. IPv6 for IPv4 Experts (draft) [en línea]. 2013, consultado 17 enero 2018. Disponible en: https://sites.google.com/site/yartikhiy/home/ipv6book.html.

TORI Carlos, Hacking Ético. 1ª Edición. Mastroiani impresiones. 2008.

VILLALÓN Huerta, A, Seguridad física de los sistemas. En (Ed. 2) seguridad en unix y redes. 2002. (pp.19-34).

ZUÑIGA, V. Puertos tcp/ip - udp [en línea]. Universidad Nacional Abierta y a Distancia. 2011. Consultado el 11 de octubre de 2017. Bogotá, Colombia. Disponible en: http://hdl.handle.net/10596/5210.