Revista Difusiones, ISSN 2314-1662, Num. 21, 2(2) julio-diciembre 2021, pp.128-147
Fecha de recepción: 25-10-2021. Fecha de aceptación: 09-11-2021

Seguridad en la configuración de redes IPV6: análisis y buenas prácticas

Ipv6 networks configuration security: analysys and best practices

Germán Eduardo Jerez[1]
germanjerez@yahoo.com.ar
Universidad Católica de Santiago del Estero. Departamento Académico San Salvador, San Salvador de Jujuy, Jujuy, Argentina

Víctor José López[2]
victor.lopez@ucse.edu.ar
Universidad Católica de Santiago del Estero. Departamento Académico San Salvador, San Salvador de Jujuy, Jujuy, Argentina

Víctor Manuel Longo[3]
victor.longo@ucse.edu.ar
Universidad Católica de Santiago del Estero. Departamento Académico San Salvador, San Salvador de Jujuy, Jujuy, Argentina

1 Ingeniero Electrónico. Director del proyecto de investigación titulado "Seguridad en redes IPv6: análisis y buenas prácticas", proyecto de investigación intercátedras aprobado por el Área de Investigación y Desarrollo Científico DASS/UCSE en el año 2020. Profesor adjunto de las cátedras de Información y Comunicación y Redes de Computadoras de la carrera de Ingeniería en Informática en el DASS/UCSE. Administrador de la red de computadoras de la Universidad Nacional de Jujuy.

2 Ingeniero en Informática. Docente investigador en el proyecto de investigación titulado "Seguridad en redes IPv6: análisis y buenas prácticas", proyecto de investigación intercátedras aprobado por el Área de Investigación y Desarrollo Científico DASS/UCSE en el año 2020. Profesor jefe de trabajos prácticos de la cátedra de Información y Comunicación de la carrera de Ingeniería en Informática en el DASS/UCSE.

3 Ingeniero en Informática. Docente investigador en el proyecto de investigación titulado "Seguridad en redes IPv6: análisis y

Resumen

El despliegue de IPv6 en las redes de datos sigue avanzando a medida que se agotan los recursos IPv4.

Algunas organizaciones inician el despliegue de IPv6 con mayor conocimiento acerca del tema y otras lo hacen de forma urgente, sin la debida planificación, ante la carencia de direcciones IPv4 para sus nuevas redes. En general, la adopción de IPv6 no avanza con la rapidez que sería deseada debido a la extendida utilización de herramientas que permiten la reutilización de direcciones IPv4 y, también, por una tendencia habitual entre los administradores de red de continuar con las prácticas conocidas y demorar la implementación de nuevos protocolos.

La demora en la implementación de IPv6 retrasó la capacitación de los administradores de redes y no permitió la generación de valiosas experiencias relacionadas con la configuración segura de los dispositivos de red.

Este trabajo tiene como finalidad aportar información acerca de algunos de los problemas de seguridad que los administradores de red deberán enfrentar en el despliegue y configuración de IPv6 y presentar recomendaciones de buenas prácticas, intentando evitar despliegues que puedan llegar a comprometer la seguridad de los datos en la red.

Palabras clave

Ipv6, Despliegue, Seguridad, Buenas prácticas

Abstract

The deployment of IPv6 in data networks continues to advance as IPv4 resources are depleted.

Some organizations start the deployment of IPv6 with more knowledge about the subject, and others do it urgently, without proper planning, given the lack of IPv4 addresses for their new networks. In general, the adoption of IPv6 is not advancing as quickly as it's desired due to the extensive use of tools that allow the reuse of IPv4 addresses and, also, because of a general tendency among network administrators to continue with established practices and delay the implementation of new protocols.

The delay in the implementation of IPv6 delayed the training of network administrators and did not allow the generation of valuable experiences related to the secure configuration of network devices.

buenas prácticas", proyecto de investigación intercátedras aprobado por el Área de Investigación y Desarrollo Científico DASS/UCSE en el año 2020. Profesor jefe de trabajos prácticos de la cátedra de Redes de Computadoras de la carrera de Ingeniería en Informática en el DASS/UCSE.

The purpose of this work is to provide information about some of the security problems that network administrators will have to face in the deployment and configuration of IPv6 and to present recommendations of best practices, trying to avoid deployments that could compromise the security of the data in the network.

Key Words

Ipv6, Deployment, Security, Best practices

Introducción

La presente investigación se enmarca en el proyecto "Seguridad en redes IPv6: análisis y buenas prácticas", aprobado por la Prosecretaría de Investigación del Departamento Académico San Salvador de la Universidad Católica de Santiago del Estero (DASS/UCSE), mediante Disposición Nº329/2020 y se encuentra financiado por esta entidad. El equipo de investigación está formado por docentes de las cátedras de Información y Comunicación y Redes de Computadoras junto a alumnos avanzados de la carrera de Ingeniería en Informática.

La seguridad en la configuración de redes IPv6 es uno de los temas que integran los contenidos dictados en las cátedras involucradas en este trabajo de investigación. Por lo tanto, se acordó conveniente profundizar en la cuestión para generar contenidos académicos propios y promover las tareas de investigación en el plantel docente y los alumnos avanzados de la carrera.

En la actualidad coexisten en las redes los protocolos Internet Protocol version 4 (IPv4) e Internet Protocol version 6 (IPv6). Los sistemas operativos más utilizados en distintos tipos de dispositivos, tanto de escritorio como móviles, disponen de ambos stack de protocolos activados por defecto. Esta situación debería obligar a los administradores de red y sistemas a prestar atención no solo a la configuración de dispositivos y aplicaciones en IPv4 sino también en IPv6 dado que, muchas veces sin saberlo, existen en las redes actuales servicios y aplicaciones activas en IPv6. Desconocer esta situación puede dejar abiertas algunas puertas para posibles ataques a la seguridad de la información.

Los problemas relacionados con la seguridad en IPv6 abarcan cuestiones vinculadas con la correcta configuración de direcciones tanto en forma manual como así también mediante el proceso de autoconfiguración disponible de forma nativa en IPv6. La utilización de servicios como Dynamic Host Configuration Protocol version 6 (DHCPv6) también presenta desafíos a la seguridad. El uso de virtualización también incorpora vulnerabilidades en los servicios que atienden en IPv6.

Las aplicaciones originalmente diseñadas para IPv4 y luego adaptadas a IPv6, así como aquellas pensadas en forma nativa para ser compatibles con el nuevo protocolo también ofrecen aspectos vinculados a la seguridad para ser atendidos.

Por supuesto, las costumbres legadas de IPv4 y que se encuentran arraigadas en las prácticas profesionales de los administradores de red y sistemas y que no son del todo compatibles con el mundo de IPv6 pueden llegar a incorporar nuevas vulnerabilidades que comprometan la seguridad de la información.

La generación de direcciones IPv6, ya sea mediante autoconfiguración o de forma manual, como se mencionó, no es el único tema existente desde el punto de vista de la seguridad, pero consideramos que se trata del principal problema para tener en cuenta por parte de los administradores de red que se inician en el despliegue de redes IPv6 y, por lo tanto, nos

concentraremos en el análisis de este tópico en particular.

Como ya se hizo referencia, otro factor que atenta contra la seguridad en despliegues de IPv6, es la tendencia de los administradores de red de seguir manejándose con configuraciones de red solo en IPv4.

La mayoría de los dispositivos que cuentan con conectividad en nuestros días ya poseen la compatibilidad para redes IPv6 y, muchos de ellos, poseen configuraciones de red IPv6 por defecto que no deberían ser ignoradas por parte de los administradores dado que pueden llegar a convertirse en puertas de entrada para posibles ataques a la seguridad. Lo recomendable es atender la configuración de ambos stack de protocolos, es decir, prestar atención a las configuraciones IPv4 e IPv6 de manera simultánea.

Si a lo anterior le sumamos el hecho de que muchos desarrollos de aplicaciones compatibles con IPv6 presentes en una variada colección de dispositivos tales como televisores inteligentes, cámaras de seguridad o dispositivos Internet of Things (IoT), tampoco fueron desarrollados con medidas de seguridad apropiadas, la cuestión de la seguridad en IPv6 se transforma en un tema que involucra tanto a administradores de red como así también a desarrolladores de software.

Junto a los problemas en el manejo de las direcciones IPv6 se presenta también un breve análisis de las problemáticas relacionadas con el software compatible con IPv6.

El presente trabajo consiste en una investigación de antecedentes relacionados con la seguridad en la configuración de dispositivos IPv6 junto a un análisis relacionado con las aplicaciones compatibles y la recomendación de buenas prácticas en la materia.

El objetivo principal de este trabajo es presentar algunos de los principales problemas que afectan a las redes IPv6 en sus etapas iniciales de despliegue. Se presentan los resultados obtenidos a partir de una investigación de antecedentes en materia de seguridad en IPv6, principalmente enfocada en la correcta generación de esquemas de direccionamiento de dispositivos y en el uso de aplicaciones compatibles con el nuevo protocolo. Se refuerzan algunos de los conceptos vinculados con las direcciones IPv6 mediante laboratorios de autoconfiguración que muestran algunas de las vulnerabilidades existentes y la manera de disminuir los riesgos según el sistema operativo empleado en los dispositivos de red.

Los objetivos específicos que se propusieron fueron la elaboración de un estado del arte sobre la cuestión de la seguridad en IPv6; analizar las principales vulnerabilidades relacionadas con la seguridad en IPv6; diseñar y realizar prácticas de laboratorio relacionadas con la seguridad en IPv6; proponer buenas prácticas en materia de seguridad para la implementación de IPv6; obtener conclusiones a partir de la investigación teórica y de los laboratorios; promover la investigación entre los docentes de las cátedras involucradas; incorporar a estudiantes en las tareas de investigación y difundir los resultados obtenidos en el marco de las tareas de extensión de la universidad.

En el presente trabajo se comparten los resultados de las investigaciones teóricas sobre el

estado de la seguridad en redes IPv6. Si bien se mencionan un conjunto de vulnerabilidades conocidas en IPv6, la investigación y los posteriores laboratorios y resultados se concentraron en dos aspectos que se consideraron como los de principal importancia para los despliegues de IPv6 que recién se inician. En particular se abordaron las cuestiones relacionadas con la seguridad en los esquemas de direccionamiento y la utilización de aplicaciones compatibles con IPv6. Estos informes vienen a constituir un estado del arte referido a dichas cuestiones.

Se incluyen también una serie de laboratorios de autoconfiguración IPv6 implementados mediante redes de dispositivos virtualizados en los que pueden observarse algunas de las principales vulnerabilidades existentes y propuestas de solución vinculadas con distintos sistemas operativos disponibles.

Tanto las investigaciones teóricas como los laboratorios permitieron elaborar una serie de recomendaciones acerca de buenas prácticas en la configuración de despliegues iniciales de IPv6 y en el adecuado uso de aplicaciones compatibles.

Vulnerabilidades en la configuración de direcciones IPv6

Actualmente en Internet coexisten IPv4 e IPv6. Ambos protocolos se encargan del manejo de datagramas en la red y pueden funcionar simultáneamente gracias a diversas técnicas de coexistencia y transición (Jerez, López & Longo, 2019).

IPv4 se diseñó en la década de 1980. En aquel momento Internet no tenía las características y el despliegue mundial que tiene hoy, por lo tanto, IPv4 no se diseñó teniendo en cuenta la seguridad en las comunicaciones como criterio fundamental. La gran expansión de Internet se inició en la década de 1990 y con ella se incrementaron las amenazas a la seguridad en las comunicaciones (Hogg, 2009).

A inicios de 1990 la Internet Engineering Task Force (IETF) comprendió que, debido al crecimiento de Internet y el agotamiento de las direcciones IPv4, era necesario diseñar una nueva versión del protocolo de capa de red. Así nació IPv6 (Deering & Hinden, 1998) con la intención de superar las limitaciones de IPv4 y con un enfoque en la seguridad de las comunicaciones más acorde con la realidad de la Internet de ese momento.

Las direcciones IPv6 tienen una longitud de 128 bits (cuatro veces más extensas que las direcciones IPv4), lo cual representaría una dificultad para implementar ataques por escaneo de direcciones. En primera instancia se consideraron inviables los ataques por escaneo sobre direcciones IPv6, pero luego se presentaron resultados de análisis en esta cuestión aplicando técnicas tradicionales de escaneo sobre redes IPv6 y otras técnicas adicionales que parecen demostrar que este tipo de ataques son viables en la práctica (Gont & Chown Jisc, 2016).

Por otro lado, el método de autoconfiguración IPv6 (Thomson, Narten, 1996), mostró la

vulnerabilidad de permitir el seguimiento de hosts en Internet debido a que el identificador de interfaz (IID) en la dirección nunca cambia, aún, cuando los hosts IPv6 se unen a distintas redes (Gont, 2017). Esta cuestión fue revisada en versiones posteriores del método de autoconfiguración (Thomson, Narten, Jinmei, 2007).

Las cabeceras de extensión AH (Authentication Header) y ESP (Encrypted Secure Payload) (Wouters, Migault, Mattsson, Nir & Kivinen, 2017) se incorporaron en IPv6 para garantizar integridad y autenticación, pero en la práctica resulta que no son pocos los routers en Internet que descartan cabeceras de extensión IPv6 debido a problemas de seguridad descubiertos en algunas de ellas (Gont, 2017).

La fragmentación de datagramas IPv6 solo en los extremos dificulta también los ataques de fragmentación en tránsito, pero, nuevamente, la fragmentación en IPv6 se maneja según cabeceras de extensión que pueden llegar a ser utilizados para implementar ataques en redes que no implementen filtrados con seguimiento del estado de las conexiones (Chittimaneni, Kaeo & Vincke, 2012).

Las cuestiones citadas son solo una muestra de los posibles campos de estudio vinculados a la seguridad en IPv6, pero quizás el mayor motivo por el cual este sea un tema que merezca ser estudiado es que el tráfico de Internet global en la actualidad continúa siendo mayoritariamente IPv4 y, como consecuencia de ello, los administradores de red están más acostumbrados a interpretar y resolver cuestiones de seguridad en IPv4 y no en IPv6 y, además, muchas aplicaciones y productos en IPv6 no tienen todavía suficiente madurez en materia de seguridad.

Por lo expuesto, la seguridad en redes IPv6 constituye un campo de investigación necesario para detectar nuevas vulnerabilidades, diseñar alternativas de mitigación ante posibles ataques y proponer buenas prácticas para la operación de redes y servicios.

El presente estado del arte se concentrará en el análisis de las vulnerabilidades relacionadas con la configuración de direcciones IPv6, ya sea utilizando la configuración manual como así también el método de autoconfiguración disponible por defecto en IPv6.

Consideramos adecuado iniciar el estudio de la seguridad en IPv6 por las prácticas de configuración de direcciones de red debido a que se trata de la primera tarea de despliegue que deberán implementar los administradores de red y de sistemas.

Si bien el espacio de direcciones de 128 bits de IPv6 parecía, de alguna manera, garantizar la imposibilidad de realizar descubrimiento de direcciones, experiencias realizadas en los últimos años demostraron que, aún con las técnicas de descubrimiento ya conocidas, más algunos métodos más novedosos, resulta posible técnicamente el descubrimiento de direcciones IPv6 con las derivaciones en la seguridad consecuentes.

El primer inconveniente observado con los ataques de descubrimiento de direcciones estuvo relacionado con la forma de creación de las direcciones IPv6. IPv6 incorpora el método de autoconfiguración de direcciones. La configuración automática o

autoconfiguración se implementa mediante el protocolo Neighbor Discovery (NDP) a través de mensajes Internet Control Messages Protocol version 6 (ICMPv6). Estos mensajes se denominan Neighbor Solicitation (NS), Router Solicitation (RS), Neighbor Advertisement (NA) y Router Advertisement (RA).

En la autoconfiguración un router anuncia el prefijo de red a utilizar y los hosts, mediante Extended Unique Identifier – 64 (EUI-64), autocompletan la dirección IPv6 local en base a sus direcciones Media Access Control (MAC) (Jerez, López & Longo, 2019). Los hosts generan automáticamente un identificador de interfaz (IID) de 64 bits para completar una dirección IPv6 válida junto a los 64 bits del prefijo de red suministrados por el router.

El principal problema con la generación automática del identificador de interfaz IPv6 recae en la inclusión del grupo de 16 bits FFFE en la dirección MAC de la interfaz de red para completar los 64 bits necesarios en una dirección IPv6 de 128 bits. Un atacante que decidiera realizar un escaneo de direcciones podría reducir su campo de búsqueda en 216 posibilidades.

Si a la situación anterior le agregamos el hecho de que las direcciones MAC poseen 3 bytes que identifican al fabricante, son valores conocidos y se mantienen inalterados en todos los productos de dicho fabricante, nuevamente, un escaneo de direcciones podría direccionarse a una serie de dispositivos de red bien conocidos reduciéndose así el universo de búsqueda posible.

Escenarios similares se presentan cuando se utilizan dispositivos virtualizados. Los diferentes softwares de virtualización generan direcciones MAC para las máquinas virtuales utilizando patrones bien conocidos que permiten reducir las opciones de búsqueda de direcciones entre 28 y 224 bits, según el método de generación de direcciones MAC utilizado por el software de virtualización.

Todas las situaciones mencionadas hasta aquí se encuentran ampliamente tratadas en el RFC 7707, Reconocimiento de red en redes IPv6 (Gont, 2016).

En el RFC 8981 (Gont et al, 2021) se establece la forma de generar direcciones IPv6 temporales. El IID de la dirección temporal se genera en forma aleatoria para evitar patrones de reconocimiento y seguimiento de direcciones por parte de posibles atacantes. Las direcciones temporales conviven con las direcciones obtenidas mediante autoconfiguración y permiten que los dispositivos que funcionan como hosts en redes IPv6 utilicen direcciones no rastreables y temporales ya que su vida útil se reduce de 24 a 48 horas. Las direcciones generadas mediante autoconfiguración pueden ser empleadas en caso de necesitar ofrecer servicios en la red mediante direcciones estables y se recomienda establecer sobre ellas políticas de seguridad en base a filtrado de tráfico mediante firewalls.

En el RFC 7217 se establece la forma de generar IID mediante el método de autoconfiguración SLAAC que puedan cambiar cuando el host cambie de subred. De esta manera se lograría evitar el rastreo de direcciones derivado del uso de la técnica EUI-64.

Este método se conoce como Semantically Opaque Interface Identifiers y permite generar direcciones en base a funciones de hash y claves privadas. La fortaleza del método reside en mantener secreta la clave. Esta alternativa permite reducir las posibilidades se seguimiento en las direcciones cuando un host cambia de red, pero todavía pueden realizarse seguimientos durante la permanencia de un host en una red determinada (Ullrich, 2017).

Cuando se utiliza la configuración mediante DHCPv6 puede suceder también que las direcciones sean rastreables. Para evitar esta situación en los RFC 5157 (Chown, 2008) y 7707 se recomienda utilizar espacios de direcciones de 64 bits en la configuración del servicio DHCP acompañado por una estrategia de asignación aleatoria de direcciones.

En el método de configuración manual de direcciones también pueden observarse algunas costumbres de asignación de direcciones que facilitarían el seguimiento. Según Gont (2016) es común encontrar asignaciones de direcciones en servidores que replican la dirección IPv4 en los últimos 32 bits de la dirección IPv6, también suelen asignarse los números de puerto para finalizar las direcciones dejando en cero los restantes bits de la IID, por ejemplo 80 para un servidor web y 25 para un servidor de correo. Suelen encontrarse también palabras escritas con los caracteres hexadecimales permitidos en las direcciones IPv6. Todas estas prácticas convierten a las direcciones de servidores en direcciones más fácilmente rastreables dado que se reducen las variantes de búsqueda e, inclusive, pueden usarse ataques de diccionario como en el caso de las direcciones con palabras incluidas en el IID.

Los ataques al proceso de autoconfiguración utilizan mensajes corruptos del tipo ICMPv6 enviados al host víctima. Los mensajes de este tipo son aceptados en la mayoría de los equipos ya que ICMPv6 es un protocolo necesario para las comunicaciones en IPv6 debido a que se usan, por ejemplo, para determinar la Maximum Transmission Unit (MTU), entre otras funcionalidades.

Existe la amenaza de routers no válidos en la red que envíen mensajes de RA. Tal como ya se mencionó, estos mensajes están diseñados para colaborar en la configuración de IPv6, contienen información importante para la conexión tal como la puerta de enlace de la red y el prefijo que se deberá utilizar para la autoconfiguración de los hosts. Entonces cualquier equipo que no contenga la pila IPv6 configurada de manera correcta y segura, optara por la información de estos mensajes falsos, es decir elegirá información fraudulenta para autoconfigurarse. Es así como un atacante podría lograr tener control de las comunicaciones que ocurren dentro de la red, redirigir tráfico en caso de necesitarlo y realizar rastreo de direcciones.

Este ataque es posible de evitar mediante la incorporación de un firewall con capacidades IPv6 y mediante el control de los mensajes ICMPv6 que circulan dentro de la red en los firewalls que delimitan las zonas de la red de la organización.

Si la red no implementa IPv6 se podrá descartar todos los mensajes ICMPv6 entrantes e

informar a los operadores de red de la presencia de dicho tipo de mensajes. También se puede mitigar si se deshabilita la opción de configuración mediante Stateless Address Auto Configuration (SLAAC) y se utiliza para la asignación de direcciones otros métodos tales como DHCPv6. Pero, como ya se mencionó, aun cuando no se despliegue intencionalmente IPv6, muchos dispositivos modernos ya cuentan con el satck IPv6 habilitado por defecto y utilizan ICMPv6 para autoconfigurar sus redes link local.

Transición y vulnerabilidades en aplicaciones compatibles con IPv6

El objetivo principal de esta temática es analizar las posibles vulnerabilidades de IPv6 que afectan, ya sea de manera directa o indirecta, a las aplicaciones en general y/o al desarrollo de software. También es interesante analizar cómo lo anteriormente mencionado condiciona al desarrollador de software.

El despliegue de IPv6 en el mundo no es homogéneo. En países como Estados Unidos, México, Alemania, India, Francia, la adopción de este protocolo supera el 40%. En los países restantes la adopción oscila entre un 5% y 25% (Google, 2021), esto implica que durante la transición de IPv4 a IPv6, estos dos protocolos deberán coexistir.

Así como existen técnicas de transición para el despliegue de IPv6 en las redes relacionadas con la configuración de dispositivos y la habilitación del acceso a internet, también se requieren métodos para la transición de las aplicaciones, tanto para las que actualmente son solo IPv4 como para las nuevas aplicaciones que se desarrollarán con compatibilidad nativa para IPv6.

Para poder hacer efectiva la transición existen diversas metodologías capaces de brindar al usuario una mayor disponibilidad de aplicaciones en IPv6. Si bien la mayoría de las aplicaciones están desarrolladas para redes basadas en IPv4, esto no quiere decir que estén operativas en su versión posterior.

Las aplicaciones pueden trabajar con ambos protocolos simultáneamente, es decir, en formato dual stack. Para poder implementar esto deberán incluir librerías capaces de trabajar con registros A (IPv4) y AAAA (IPv6) de manera que la resolución DNS sea la encargada de definir el protocolo a usar.

En caso de no disponer de la posibilidad de acceso a IPv6 nativo podrán usarse túneles para el acceso a las aplicaciones. Los túneles encapsulan datagramas IPv6 en datagramas IPv4 para poder ser transportados en redes solo IPv4.

En las capas superiores también será necesario hacer traducciones entre ambos protocolos. En el nivel de red, por ejemplo, los drivers de red deberán ser capaces de traducir a medida que los datagramas arriban o parten hacia el enlace.

Los traductores también pueden utilizarse en las interfaces de programación actuando directamente a nivel de socket sin necesidad de manipular encabezados de protocolos.

También pueden emplearse librerías de comunicación a nivel de usuarios mediante traductores en el nivel de aplicación.

En el caso de aplicaciones que originalmente no fueron diseñadas para IPv6 será necesaria una revisión del código fuente para cumplir con los requisitos de compatibilidad. Esto requiere que el programador haga uso de librerías o frameworks específicos.

Las aplicaciones más antiguas pueden estar sujetas a un lenguaje de programación muy anticuado o con soporte oficial y/o de comunidad de desarrollo desactualizado. Esto puede complicar el encontrarse con las herramientas necesarias para realizar su conversión, debido a que en el momento de su desarrollo solo estaba vigente IPv4. En el mejor de los casos quizás pueda encontrarse una librería que permita compatibilidad, pero, en cuanto a aspectos de seguridad, la librería podría encontrarse inmadura, permitiendo así vulnerabilidades.

Existen también numerosas aplicaciones desarrolladas para uso privado que hacen uso de direcciones IP como parte de su código y resulta necesario tener en cuenta algunas cuestiones en estos casos. Para lograr compatibilidad deberá tenerse en consideración el espacio necesario para incluir ahora direcciones de 128 bits a la par de direcciones IPv4 de 32 bits. En las direcciones IPv6 se utiliza ":" para separar las expresiones hexadecimales, por lo tanto, se deberá tener cuidado con las notaciones donde se incluyen puertos lógicos asociados a las direcciones IPv4 para evitar confusiones. Una misma dirección IPv6 puede representarse de distintas formas en representación alfanumérica y esto puede complicar algunos procesamientos automáticos en las aplicaciones. En estos casos se recomienda trabajar en formato binario (Archier, 2017).

Gustavo Mercado y otros (2007) sugieren seleccionar un grupo de herramientas para programar aplicaciones, analizarlas según su utilidad y, a continuación, poner a prueba los mecanismos de comunicación para IPv6. De esta forma podrían realizarse laboratorios mediante la elaboración de servidores y clientes IPv6 en los lenguajes seleccionados.

A partir del material analizado en la investigación sobre las posibles vulnerabilidades que podrían encontrarse en las aplicaciones compatibles con IPv6, se observa que los riesgos no están directamente relacionados con el protocolo, sino con las acciones para lograr su compatibilidad, lo que podría presentar un problema en caso de aplicaciones escritas con códigos antiguos o en el uso de librerías inmaduras desde el punto de vista de la seguridad.

Buenas prácticas para la configuración segura de IPv6

Luego de haber analizado las problemáticas de seguridad asociadas con la configuración de direcciones IPv6 y la utilización de aplicaciones adaptadas a IPv6 o diseñadas compatibles con IPv6 en forma nativa, se presentan una serie de recomendaciones a modo de buenas prácticas con el objetivo de mantener la seguridad en la red.

Desde el punto de vista de las direcciones de red IPv6 resulta fundamental tener presente que, independientemente de desplegar IPv6 o no en nuestras redes, la gran mayoría de los dispositivos que actualmente cuentan con conectividad ya disponen del stack IPv6 activo por defecto. Por lo tanto, resulta muy importante prestar atención a las autoconfiguraciones IPv6 existentes. Con una simple consulta a la configuración de las interfaces de red (ipconfig en entornos Windows o ip address list en entornos GNU/Linux, por ejemplo), los administradores podrán estar al tanto de la actividad del stack IPv6 en sus dispositivos. Esta sería la primera medida a tomar, es decir, el conocimiento de nuestra propia red. Por supuesto, siempre existe la posibilidad de desactivar el stack IPv6 en los dispositivos que lo posean, pero se trata de una práctica no recomendable dado que IPv6 es una realidad y más temprano que tarde los administradores de red deberán incorporarlo como un protocolo de todos los días en sus tareas habituales.

A partir de conocer el estado de la red se presentan dos posibles escenarios. En el primero de ellos si no se tiene previsto el despliegue de IPv6 a la brevedad, correspondería tomar medidas para evitar que los mensajes automáticos de autoconfiguración IPv6 ocasionen problemas en las redes IPv4. Al no tener contemplado el uso de IPv6 convendría el filtrado mediante firewalls o el monitoreo de mensajes ICMPv6. ICMPv6 es el protocolo que transporta los mensajes de autoconfiguración SLAAC. En este sentido sería recomendable limitar los menajes ICMPv6 y observar la aparición de mensajes del tipo Router Advertisement propios de routers IPv6 no autorizados en una red solo IPv4.

En el mismo escenario no debe olvidarse que, aun no configurando direcciones IPv6 globales, los dispositivos dual stack conservarán su configuración IPv6 link local, dicho de otra forma, por más que intencionalmente los administradores no configuren IPv6 en sus dispositivos, existirá una red IPv6 local con direcciones del tipo link local que inician con el prefijo FE80 y autocompletan su IID a través del método EUI-64. Hay que recordar que se conocen vulnerabilidades respecto al rastreo de direcciones generadas a partir de este método.

El segundo escenario posible se presenta en redes que se encuentran en proceso de despliegue de IPv6. Para estos casos y, una vez conocido el estado de la red en materia de configuración IPv6, se recomienda iniciar el despliegue luego de un estudio apropiado del esquema de direccionamiento a utilizar.

Existen vulnerabilidades tanto en los esquemas de configuración manual como también en los esquemas de autoconfiguración. Para el caso de decidir por configuraciones estáticas deberían evitarse prácticas legadas de IPv4 tales como la finalización de las direcciones IPv6 según las direcciones IPv4 equivalentes, por ejemplo, en servidores. Para ejemplificar, si un servidor en IPv4 tiene la dirección IP 192.168.0.2, no es recomendable adoptar la dirección IPv6 2001:db8::192:168:0:2 debido a que un atacante que haya identificado la dirección IPv4 podrá fácilmente replicar ataques en IPv6. Una situación similar se presenta cuando se

identifican servidores según sus puertos lógicos por defecto, tal sería el caso de utilizar los números 80 y 25 en las direcciones IPv6 para identificar servidores web o de correo electrónico. Relacionado con lo anterior, también se recomienda evitar la creación de direcciones IPv6 que hagan uso de juegos de palabras a partir de los caracteres hexadecimales permitidos, por ejemplo, BEBE, CAFE u otras. Este tipo de direcciones resultan vulnerables a los ataques por diccionario.

Como ya se mencionó, la autoconfiguración es una característica propia de IPv6 y se lleva a cabo mediante el procedimiento SLAAC. En caso de decidirse el uso de un router SLAAC en la red debe tenerse en cuenta que, por defecto, SLAAC autoconfigurará los hosts IPv6 según el prefijo de 64 bits anunciado por el router y completará la dirección a través de EUI-64 a partir de los 48 bits de la dirección MAC. Para evitar el rastreo de direcciones a partir de los IID generados por EUI-64 se recomienda la utilización de direcciones IPv6 alternativas que se generen a partir de métodos aleatorios, tal como se describió en los RFC correspondientes. Los principales sistemas operativos de computadoras y dispositivos portátiles ya implementan la generación de estas direcciones alternativas por defecto, tal como pudo observarse en el laboratorio presente en este trabajo. Nuevamente, debe tenerse en cuenta que las direcciones link local también se generan en base a las direcciones MAC y pueden representar posibilidad de seguimiento dentro de la red local.

En caso de optar por utilizar servidores DHCPv6 se sugiere evitar la asignación consecutiva de direcciones y la adopción de esquemas de numeración aleatorios.

En todos los casos de redes dual stack, ya sea con configuración IPv6 global explícita o solo con direcciones link local, debe tenerse la precaución de analizar el tráfico de mensajes de autoconfiguración IPv6 de manera constante, dada la posibilidad de aparición de routers SLAAC no autorizados capaces de entregar información de autoconfiguración fraudulenta (Babik et al, 2017). Para esta última pueden emplearse soluciones como la implementación del protocolo RA-Guard (Levy-Abegnoli et al, 2011), cuyas especificaciones fueran recientemente actualizadas en el RFC 7113 (Gont, 2017).

Desde el punto de vista de las aplicaciones que se ejecutan en la red, resulta necesario realizar un relevamiento de aquellas aplicaciones que solo son compatibles con IPv4 y aquellas que cuenten con la posibilidad de brindar servicios en forma dual, tanto en IPv4 como en IPv6.

Resulta que, dado el despliegue desigual de IPv6 en las redes de todo el mundo, las costumbres de desarrollo de los programadores, el desinterés o desconocimiento de los administradores de red o de sistemas, muchas aplicaciones se adquieren o desarrollan para ser configuradas y puestas en servicio solo en IPv4 y, muchas veces, se desconoce o desatiende la posible configuración IPv6 que existe por defecto en servidores que corren sistemas operativos modernos. Esta situación podría dejar abiertas algunas puertas para los atacantes, que les permitan explotar vulnerabilidades de las aplicaciones IPv6

compatibles. Desde este punto de vista resulta conveniente la buena práctica de identificar todas las aplicaciones de la red, estableciendo una política de seguridad que permita actualizar aplicaciones solo IPv4 para adelantarnos al uso masivo de IPv6 e identificar las aplicaciones IPv6 compatibles mal configuradas desde el punto de vista de la seguridad o desactualizadas en el uso de sus librerías o aplicaciones asociadas.

Todo lo anterior no podrá ser llevado a cabo sin la apropiada capacitación de los administradores de red y sistemas y, para ello, resulta fundamental el compromiso en los niveles de decisión de las distintas organizaciones con el objetivo de mantener redes dual stack seguras.

Laboratorios sobre seguridad IPv6

Con el objetivo de realizar pruebas referidas a la seguridad en la configuración de redes IPv6, se implementó un laboratorio mediante máquinas virtualizadas y computadoras portátiles con sistemas operativos MS Windows 10 y GNU/Linux.

La red se construyó utilizando un switch Ethernet 10/100 Mbps de ocho puertos al cual se vincularon tres computadores portátiles mediante cables UTP categoría 5E, tal como se indica en la figura 1.

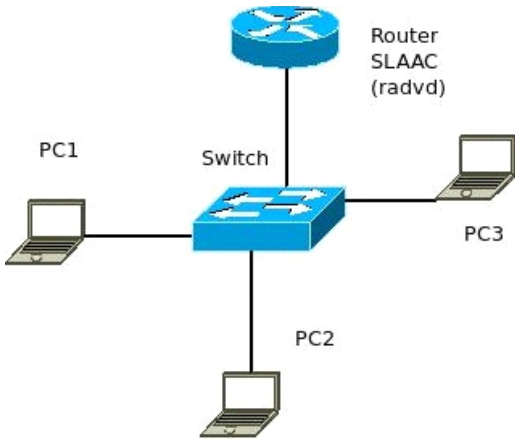

Figura 1 – Topología de laboratorio (Autor: Germán E. Jerez)

Para las pruebas de autoconfiguración IPv6 se incorporó un router SLAAC virtualizado que se implementó mediante una máquina GNU/Linux Debian 9 con el software libre de autoconfiguración radvd (Router Advertisement Daemon).

El laboratorio consistió en autoconfigurar las computadoras portátiles según el prefijo IPv6 de laboratorio 2001:db8:1c5e:da55::/64 que se configuró en el software radvd.

En un estado incial, las computadoras poseían solo la configuración IPv6 link local por defecto, tal como puede observarse en las figuras 2 y 3.

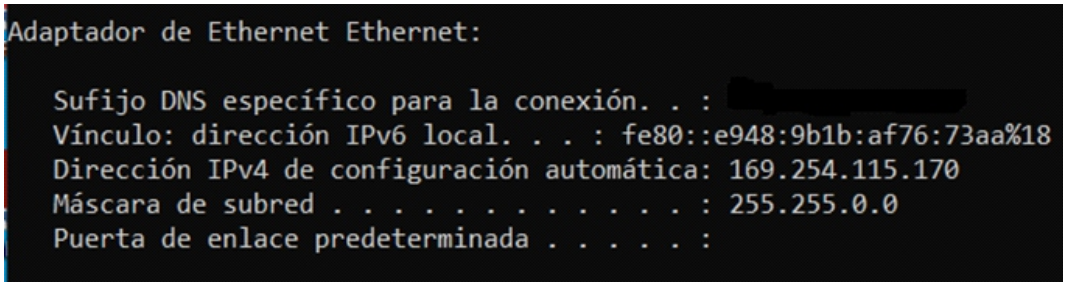

Figura 2 – Configuración IPv6 inicial en MS Windows 10

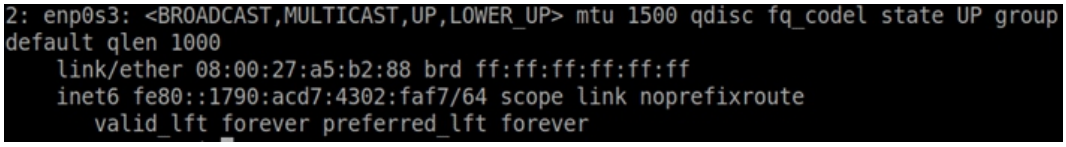

Figura 3 – Configuración IPv6 inicial en GNU/Linux

Luego de verificar el estado inicial de la configuración IPv6 se procedió a habilitar el router SLAAC. Esta máquina virtual procedió a anunciar el prefijo 2001:db8:1c5e:da55 en la red para ofrecer autoconfiguración a las computadoras portátiles.

Se realizó una nueva consulta de configuración de red y los resultados obtenidos fueron los observados en las figuras 4 y 5.

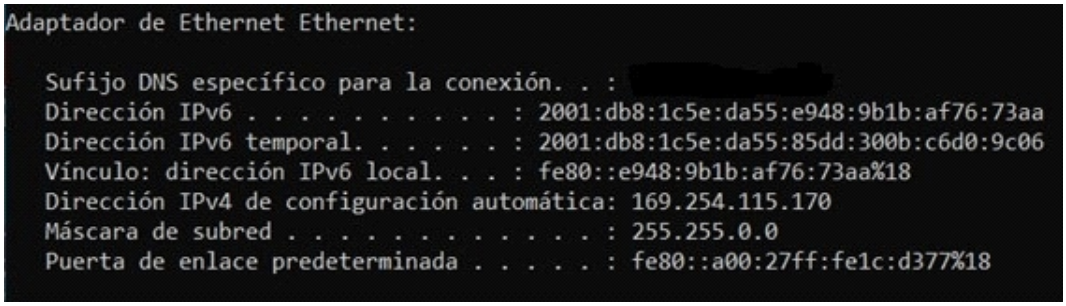

Figura 4 – Autoconfiguración IPv6 en MS Windows 10

Figura 5 – Autoconfiguración IPv6 en GNU/Linux

En ambos casos puede observarse como se autoconfiguraron las interfaces de red según el prefijo anunciado mediante SLAAC. En el caso particular de la computadora con MS Windows 10 pudo observarse la inclusión de una segunda dirección IPv6 global denominada temporal, además de la generada mediante EUI-64. Para la dirección temporal, los 64 bits de la IID son distintos a los generados mediante EUI-64. En el caso del sistema operativo GNU/Linux también se observa una dirección IPv6 global temporal cuya IID no coincide con la correspondiente a EUI-64, lo que puede comprobarse comparando con la IID de la dirección link local.

Esto último se debe a que los sistemas operativos implementan las recomendaciones de seguridad referidas al uso de direcciones IPv6 no rastreables indicadas en los RFC 4941 (Narten et al, 2007) y RFC 8981 (Gont et al, 2021).

Las direcciones IPv6 temporales se generan con tiempos de vida entre 24 y 48 horas, por defecto, y se renuevan pasados estos límites temporales. Para verificar esta última situación se procedió a reconfigurar las computadoras y verificar nuevamente sus configuraciones de red. El resultado se observa en la figura 6.

Figura 6 – Autoconfiguración IPv6 en MS Windows 10 con direcciones temporales renovadas

Las direcciones IPv6 temporales son una de las formas empleadas para superar la vulnerabilidad de rastreo de direcciones generadas según EUI-64.

El hecho de que con EUI-64 se generan direcciones que pueden ser rastreadas queda demostrado si comparamos las direcciones globales, temporales y no temporales, y las direcciones link local de las figuras. Para el caso de las direcciones globales no temporales y las direcciones link local, los últimos 64 bits de las direcciones (IID) son coincidentes dado que se generan a partir de la misma dirección MAC. Si se observan las direcciones temporales no hay coincidencia en estos últimos 64 bits.

Finalmente se procedió a simular el caso de un ataque mediante un router SLAAC no autorizado en la red. Para lograrlo se inició un segundo router radvd virtualizado, pero esta vez anunciando un prefijo distinto al anterior. Se utilizó el prefijo 2001:db8:1c5e:da52::/64.

Los resultados de la experiencia pueden observarse en las figuras 7 y 8.

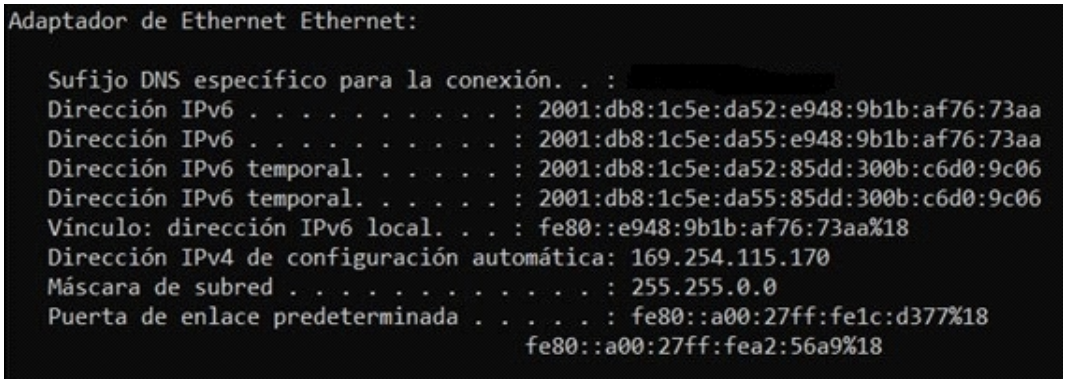

Figura 7 – Segundo router SLAAC en MS Windows 10

Figura 8 – Segundo router SLAAC en GNU/Linux

En ambos casos puede observarse que la introducción de un router SLAAC no autorizado puede llegar a comprometer la seguridad debido a que los hosts IPv6 pueden incorporar la cantidad de direcciones necesarias en cada una de sus interfaces y, por lo tanto, responden a los mensajes Router Advertisement del router no autorizado y se autoconfiguran según el nuevo prefijo de red. Esta situación puede llegar a ser utilizada por atacantes dado que son capaces de generar una red IPv6 paralela y utilizarla para sus propios fines.

Este último escenario hace necesario que los administradores de redes IPv6 implementen métodos de control en los mensajes ICMPv6, que son los encargados de transportar los mensajes del protocolo Neighbor Discovery, para evitar mensajes del tipo Router Advertisement no válidos. Otra técnica sugerida para estos casos consiste en la configuración de firewalls que solo admitan tráfico desde los prefijos autorizados.

Las prácticas de laboratorio presentadas tuvieron como finalidad exponer algunas de las vulnerabilidades propias del método de autoconfiguración IPv6 con el objetivo de alertar a los administradores de red recién iniciados en este protocolo.

Conclusiones

El presente trabajo de investigación constituyó una continuación de otro trabajo centrado en las técnicas de despliegue de IPv6 en redes locales.

Desplegar IPv6 por primera vez en una red que solo trabaja en IPv4 requiere una serie de conocimientos referidos a técnicas de direccionamiento, dispositivos y software para la implementación de servicios y, por supuesto, cuestiones relacionadas con la seguridad en la red.

Al considerar que la cuestión de la seguridad en el despliegue de IPv6 constituye un tema de gran importancia, se decidió ampliar la investigación según dicha orientación.

Durante la investigación se descubrieron múltiples caminos posibles para avanzar sobre el estudio de la seguridad en el despliegue de IPv6. A modo de ejemplos pueden mencionarse temas tales como seguridad en la configuración manual y en la autoconfiguración, vulnerabilidades propias del uso de las cabeceras de IPv6, vulnerabilidades en los mensajes de autoconfiguración, vulnerabilidades en el proceso de fragmentación en los extremos, seguridad en el uso de aplicaciones IPv6 compatibles, prácticas sobre seguridad legadas de IPv4 y aplicadas en IPv6, entre otras temáticas.

Ante la gran variedad de temas para investigar y teniendo tiempos acotados para el desarrollo de la investigación se decidió avanzar específicamente sobre las cuestiones relacionadas con la configuración y las vulnerabilidades en las aplicaciones porque se consideraron como pasos fundamentales para un despliegue inicial de IPv6.

Como conclusión de las investigaciones resulta importante destacar la necesidad de que los administradores de red y sistemas avancen lo antes posible en su capacitación sobre configuración segura de IPv6. En el presente trabajo se brindaron una serie de sugerencias de buenas prácticas al respecto.

Además, la seguridad en las aplicaciones compatibles con IPv6 también constituye una cuestión importante para analizar por parte de los responsables de redes y sistemas. Los especialistas en software deberían tener en cuenta posibles vulnerabilidades en aplicaciones cuyas adaptaciones para IPv6 no se hayan realizado de la manera más segura.

Es importante recordar que el despliegue de IPv6 no solo contempla la configuración de las redes para el correcto transporte de datagramas IPv6, sino también la existencia de aplicaciones compatibles con IPv6 que aporten servicios y contenidos en dicho protocolo. Solo avanzando en ambos frentes podrá acelerarse el despliegue de IPv6 en todas las redes que integran internet.

Bibliografía

Jerez, G., López, V., Longo, M. (2019). Técnicas para el despliegue de IPv6 en redes LAN: laboratorios de auto-configuración utilizando RDNSS y DHCPv6. Revista Difusiones, ISSN 2314-1662, número 17, 273-286.

Hogg S., Vyncke, E. (2009). IPv6 Security. Cisco Press.

Deering, S., Hinden, R. (1998). Internet Protocol, Version 6 Specification. IETF.

Gont, F., Chown Jisc, T. (2016). Network Reconnaissance in IPv6 Networks. RFC 7707. IETF.

Chown, T. (2008). IPv6 Implications for Network Scanning. RFC 5157. IETF.

Thomson, S., Narten, T. (1996). IPv6 Stateless Address Autoconfiguration. RFC 1971. IETF.

Gont, F. (2017). Consideraciones de seguridad en IPv6. Experiencie IPv6 2017. Nairobi, Kenia.

Thomson, S., Narten, T., Jinmei, T. (2007). IPv6 Stateless Address Autoconfiguration. RFC 4862. IETF.

Wouters, P., Migault, D., Mattsson, J., Nir, Y., Kivinen, T. (2017). Cryptographic Algorithm Implementation Requirements and Usage Guidance for Encapsulating Security Payload (ESP) and Authentication Header (AH). RFC 8221. IETF.

Chittimaneni, K., Kaeo, M., Vincke, E. (2012). Operational Security Considerations for IPv6 Networks, draft-ietf-opsec-v6-01.

Gont, F., Krishnan, S., Narten, T., Draves, R. (2021). Temporary Address Extensions for Stateless AddressAutoconfiguration in IPv6. RFC 8981. Internet Engineering Task Force (IETF).

Ullrich, J. (2017). IPv6 Addresses, Security and Privacy. RIPE Labs. RIPE. Recuperado de: https://labs.ripe.net/author/johanna_ullrich/ipv6-addresses-security-and-privacy/

Google. (2021). Google IPv6 Statistics. Recuperado de: https://www.google.com/intl/en/ipv6/statistics.html#tab=per-country-ipv6-adoption&tab=ipv6-adoption

Archier, Jean-Paul. (2017). IPv6, principios e implementación. Ediciones ENI. Recuperado de: https://www.ediciones-eni.com/manuales/libro/ipv6-principios-e-implementacion-version-online-9782409009044

Mercado, G., Taffernaberry, J., Dantiacq, A., Pérez, S., Moralejo, R. (2007). Diseño y simulación de la implementación de tecnologías y procedimientos de transición del protocolo IPv6 en Intranets usando un IPv6 test bed. Sedici, UNLP.

M Babik, J Chudoba, A Dewhurst, T Finnern, T Froy, C Grigoras, K Hafeez, B Hoeft, T Idicull, D P Kelsey, F López Muñoz, E Martelli, R Nandakumar, K Ohrenberg, F Prelz, D Rand, A Sciabá, U Tigerstedt, D Traynor and R Wartel. (2017). IPv6 Security. Journal of Physics: Conference Series. Recuperado de: https://iopscience.iop.org/article/10.1088/1742-6596/898/10/102008/pdf

Levy-Abengnoli, E., Van de Velde, G., Popoviciu, C., Mohacsi, J. (2011). IPv6 Router

Advertisement Guard. RFC 6105. IETF.

Gont, F. (2014). Implementation Advice for IPv6 Router Adevertisement Guard (RA-Guard). RFC 7113. IETF.

Narten, T., Draves, R., Krishnan, S. (2007). Privacy Extensions for Stateless Address Autoconfiguration in IPv6. RFC 4941. IETF.

Gont, F., Krishnan, S., Narten, T., Draves, R. (2021). Temporary Address Extensions for Stateless Address Autoconfiguration in IPv6. RFC 8981. IETF.