Revista Difusiones, ISSN 2314-1662, Num. 17, diciembre 2019, p273-286

Técnicas para el despliegue de ipv6 en redes lan: laboratorios de auto-configuración utilizando RDNSS y DHCPV6

Autores: **Germán Eduardo Jerez, Víctor José López, Víctor Manuel Longo**
UCSE-DASS
germanjerez@yahoo.com.ar

Germán Eduardo Jerez
Ingeniero Electrónico. Director del proyecto de investigación titulado "Técnicas para el despliegue de IPv6 en redes LAN", proyecto de investigación intercátedras aprobado por el Área de Investigación y Desarrollo Científico DASS/UCSE en el año 2018. 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.

Víctor José López
Ingeniero en Informática. Docente investigador en el proyecto de investigación titulado "Técnicas para el despliegue de IPv6 en redes LAN", proyecto de investigación intercátedras aprobado por el Área de Investigación y Desarrollo Científico DASS/UCSE en el año 2018. Profesor jefe de trabajos prácticos de la cátedra de Información y Comunicación de la carrera de Ingeniería en Informática en el DASS/UCSE.

Víctor Manuel Longo
Ingeniero en Informática. Docente investigador en el proyecto de investigación titulado

“Técnicas para el despliegue de IPv6 en redes LAN”, proyecto de investigación intercátedras aprobado por el Área de Investigación y Desarrollo Científico DASS/UCSE en el año 2018. Profesor jefe de trabajos prácticos de la cátedra de Redes de Computadoras de la carrera de Ingeniería en Informática en el DASS/UCSE.

Resumen

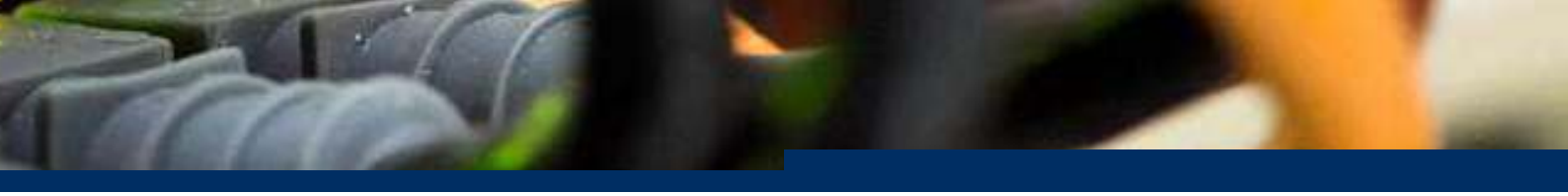
El crecimiento de Internet registrado a lo largo de las últimas décadas trajo consigo el problema del agotamiento de las direcciones IPv4 (Internet Protocol version 4). Como solución a este problema la IETF (Internet Engineering Task Force) propuso la adopción de IPv6 (Internet Protocol version 6).
En redes LAN pueden coexistir ambos protocolos mediante la aplicación de la técnica dual stack que consiste en mantener activos IPv4 e IPv6 en los hosts de manera simultánea.
Con IPv6 se puede ejecutar la auto-configuración en los hosts siempre que se encuentre disponible un router SLAAC (Stateless Address AutoConfiguration) en la red. Adicionalmente también puede emplearse un servidor DHCPv6 (Dynamic Host Configuration Protocol version 6).
El router SLAAC proporciona un prefijo IPv6 para la auto-configuración de los hosts y establece su dirección link local como default gateway de la red. Para el anuncio de servidores DNS (Domain Name System) puede utilizarse DHCPv4 ó DHCPv6. También puede emplearse RDNSS (Recursive DNS Server) en SLAAC para el anuncio de servidores DNS en los mensajes de auto-configuración.
Este trabajo presenta una serie de laboratorios en los cuales se plantean escenarios de auto-configuración IPv6 utilizando servidores SLAAC y DHCPv6 virtualizados en redes LAN. No se contempla en este trabajo el acceso a Internet IPv6.
Actualmente en la Argentina el despliegue de IPv6 no es relevante. El objetivo principal de este trabajo es aportar técnicas que alienten y faciliten el pronto despliegue de IPv6 en redes LAN.

Palabras clave

Ipv6 – Dual Stack – Auto-configuración – Despliegue

Abstract

The growth of the Internet registered over the last decades brought with it the problem of exhaustion of IPv4 addresses (Internet Protocol version 4). As a solution to this problem, the



IETF (Internet Engineering Task Force) proposed the adoption of IPv6 (Internet Protocol version 6).
In LAN networks both protocols can coexist through the application of the dual stack technique that consists of keeping IPv4 and IPv6 active on the hosts simultaneously.
With IPv6, autoconfiguration can be executed on hosts whenever a SLAAC (Stateless Address AutoConfiguration) router is available on the network. Additionally, a DHCPv6 server (Dynamic Host Configuration Protocol version 6) can also be used.
The SLAAC router provides an IPv6 prefix for the autoconfiguration of the hosts and establishes its local link address as the network default gateway. For the announcement of DNS servers (Domain Name System), DHCPv4 or DHCPv6 can be used. RDNSS (Recursive DNS Server) can also be used in SLAAC for the announcement of DNS servers in autoconfiguration messages.
This paper presents a series of laboratories in which IPv6 autoconfiguration scenarios using virtualized SLAAC and DHCPv6 servers in LAN networks are proposed. IPv6 Internet access is not contemplated in this work.
Currently in Argentina the deployment of IPv6 is not relevant. The main objective of this work is to provide techniques that encourage and facilitate the early deployment of IPv6 in LAN networks.

Key Words

Ipv6 - Dual Stack - AutoConfiguration – Deployment

Introducción

La presente investigación se enmarca en el proyecto “Estrategias para el despliegue de IPv6 en redes LAN”, aprobado por el Área de Investigación y Desarrollo Científico del Departamento Académico San Salvador de la Universidad Católica de Santiago del Estero (DASS/UCSE), mediante Disposición Nº461-2018 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.

El estudio de los protocolos IPv4 e IPv6 es un tema que integra 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.

El agotamiento de las direcciones IPv4 es una realidad que afecta e involucra a los sectores

público y privado, a la comunidad técnica en particular, a la sociedad civil en general, y por supuesto, a la comunidad académica, especialmente a los investigadores del área de las comunicaciones (ISOC, 2010). El despliegue tardío de IPv6 (Deering & Hinden, 2017) podría traer como consecuencia un impacto negativo en la experiencia de Internet por parte de los usuarios y la potencial pérdida de negocios para los proveedores de servicio.

Los problemas de IPv4 están relacionados con el agotamiento de sus direcciones, con problemas en la escalabilidad del ruteo y en la ruptura del esquema de comunicaciones extremo a extremo (end-to-end) originalmente diseñado (Wu, Cui, Wu, Liu & Metz, 2012).

El despliegue masivo de dispositivos móviles con capacidades de conectividad ha incrementado rápidamente la demanda de direcciones de red.

IPv6 fue desarrollado como el protocolo de red de nueva generación, proponiéndose como la superación a los problemas de IPv4. Sin embargo, IPv6 no fue diseñado de manera compatible con IPv4, lo que significa que las redes IPv6 no pueden comunicarse con redes IPv4 naturalmente. Dada la incompatibilidad entre ambos protocolos, estos coexistirán durante un período más o menos prolongado y el proceso de transición será gradual.

Durante el período de transición deberá administrarse la disponibilidad de tanto IPv4 como IPv6 y resolver las cuestiones derivadas de la implementación de DNS (Domain Name System), QoS (Quality of Service), seguridad y otros aspectos abarcados por el entorno de doble pila (Dual Stack) (Gilligan & Nordmark, 2005).

Se necesitan un número de técnicas de transición para mantener la conectividad tanto de IPv4 como de IPv6 (Arkko & Baker, 2011) (China Telecom, 2015).

Junto a IPv6 se definió un conjunto de nuevos protocolos tales como Neighbor Discovery (Simpson, Narten, Nordmark & Soliman, 2007), ICMPv6 (Internet Control Message Protocol Version 6) (Gupta & Conta, 2006) y DHCPv6 (Dynamic Host Configuration Protocol Version 6) (Volz, 2006).

Básicamente existen dos formas de configurar una red LAN IPv6. Uno de los métodos es la configuración manual y el otro es la configuración automática, conocida como SLAAC (Stateless Address AutoConfiguration).

La configuración automática o auto-configuración se implementa mediante el protocolo Neighbor Discovery mediante mensajes ICMPv6. Estos mensajes se denominan NS (Neighbor Solicitation), RS (Router Solicitation), NA (Neighbor Advertisement) y RA (Router Advertisement).

En la auto-configuración el router anuncia el prefijo de red a utilizar y el host mediante EUI-64 (Extended Unique Identifier - 64) auto-completa la dirección IPv6 en base a su dirección MAC (Media Access Control). También se utilizan técnicas aleatorias para autocompletar las direcciones IPv6.

A partir del RFC5006, actualizado por el RFC8106, puede usarse la opción RDNSS (Recursive DNS Server) en los anuncios RA (Jeong & Park, 2017).

También se puede hacer uso de un servidor DHCPv6. Mediante DHCPv6 no solo pueden anunciarse direcciones de red sino también otros datos como, por ejemplo, servidores DNS (Cicileo, Gagliano, O'Flaherty, Olvera Morales, Palet Martínez, Rocha & Vives Martínez, 2010).

IPv6 maneja direcciones de 128 bits de longitud que se representan mediante formato hexadecimal, mientras que IPv4 tiene direcciones de 32 bits de longitud en formato decimal. Estas diferencias, sumadas a otras características propias de IPv6 inexistentes en IPv4 y a cierto grado de desconocimiento general en el tema, hacen que muchos operadores demoren el despliegue de IPv6 en sus redes.

El objetivo principal de este trabajo es despejar dudas y alentar el inicio de las tareas de despliegue de IPv6 en redes de área local (LAN: del inglés Local Area Network) mediante la implementación de sencillos laboratorios de auto-configuración IPv6 en entornos dual stack. Por el momento el foco de atención de este trabajo estará centrado en la configuración de hosts dentro de una red LAN, dejando para más adelante la discusión acerca del acceso a Internet mediante IPv6.

El tráfico IPv6 continúa creciendo de manera gradual en la actualidad y la necesidad de realizar la transición hacia el nuevo protocolo será solo cuestión de tiempo. Lo importante en cada caso sería planificar adecuadamente los tiempos necesarios y los mecanismos de transición más adecuados.

No realizar la transición podría implicar deterioro en la experiencia de Internet, pérdida de competitividad en los negocios y, en un caso extremo, la pérdida de conectividad total a Internet.

Objetivos

Los objetivos generales del trabajo de investigación fueron alentar el pronto despliegue de IPv6 en redes LAN. Proponer técnicas para la auto-configuración de hosts mediante la incorporación de routers y servidores configurados para tal fin.

Como objetivos específicos se pretendió informar acerca de las herramientas de software libre disponibles para iniciar tareas de laboratorio de despliegue de IPv6 en redes de prueba y posteriormente en redes en producción. También se persiguió contribuir a la formación técnica de los operadores de red preparándolos para el inminente escenario de no disponibilidad de direcciones IPv4 con la consiguiente necesidad de desplegar IPv6 en sus redes, teniendo en cuenta que los despliegues no debidamente planificados y apresurados pueden llegar a representar importantes costos operativos e impactar en los esquemas de negocios.

Finalmente se apuntó a reforzar la formación docente y de alumnos avanzados y promover la investigación en la cuestión propiciando la generación de conocimiento técnico y científico propio.

Implementación de los laboratorios

Para la implementación de los laboratorios de auto-configuración se emplearon equipamiento y materiales de uso habitual en redes LAN.
En la red de pruebas se utilizaron computadoras portátiles (PC1 y PC2) equipadas con sistemas operativos MS Windows 10 y distintas distribuciones de GNU/Linux.
El core de la red se implementó con un sencillo switch Ethernet 10/100 Mbps de ocho puertos y los hosts se vincularon entre si mediante cables UTP categoría 5E.
Para la implementación de los servicios IPv6 necesarios para la auto-configuración se optó por virtualizar servidores con sistema operativo GNU/Linux mediante el software Oracle VirtualBox.
La topología de la red de laboratorio empleada es la que se muestra en la figura 1.

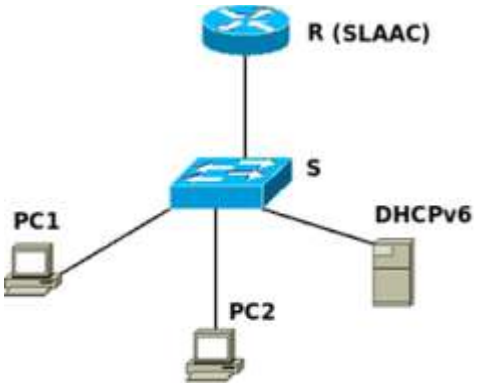
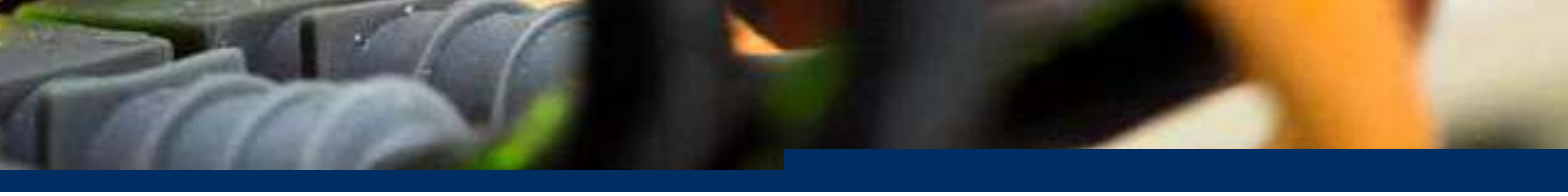


Figura 1 – Topología de laboratorio (Autor: Germán E. Jerez)

El router R fue el encargado de proporcionar el servicio de auto-configuración (SLAAC) y para ello se configuró en el servidor virtual el paquete radvd, disponible en la distribución GNU/Linux Debian Stretch.
El servidor virtual DHCPv6 se implementó también en GNU/Linux Debian Stretch mediante el paquete isc-dhcp-server.
Para la instalación en ambos casos bastó con emplear la metodología típica en Debian mediante la instrucción apt-get install.

Planteo de los laboratorios

Las prácticas de laboratorio se plantearon con el fin de lograr que los hosts de la red obtuvieran auto-configuración IPv6 manteniendo el esquema dual stack por defecto con el que cuentan los sistemas operativos modernos. Esto implica mantener activos tanto el stack de protocolos de red IPv4 como IPv6 de manera simultánea. De esta manera se buscó



mostrar como, sin ningún tipo de intervención adicional por parte del usuario, las computadoras pueden acceder a contar con configuración IPv6 según los parámetros establecidos por el administrador de la red.

Para la auto-configuración IPv6 pueden emplearse diversas técnicas dependiendo de las necesidades y características propias de la red en cuestión y de los servicios brindados a los usuarios.

Los hosts con dual stack al conectarse a la red enviarán mensajes neighbor discovery del tipo router solicitation (RS). En estos mensajes solicitarán los parámetros para la auto-configuración, típicamente un prefijo IPv6. Al estar presente el router R, este responderá los mensajes de los hosts con otros mensajes neighbor discovery del tipo router advertisement (RA) en los cuales ofrecerá la utilización de un prefijo IPv6 para las tareas de auto-configuración. Los hosts completarán su auto-configuración generando direcciones IPv6 globales conformadas por el prefijo IPv6 informado en los RA más un ID de interfaz construido en base al método EUI-64 o bien utilizando algún método de generación aleatoria. La default gateway de los hosts IPv6 será la dirección link local del router SLAAC, en nuestro caso el router R.

En la configuración SLAAC los hosts obtienen una dirección IPv6 global y su default gateway, pero, por defecto, este método no suministra ninguna información referida a servidores DNS. En la especificación original de IPv6 se decidió que la información acerca de servidores de nombres sería suministrada mediante DHCP. Esto es así gracias a que en un entorno dual stack las implementaciones actuales de DHCP pueden suministrar servidores de nombres en IPv4 e IPv6 simultáneamente. Por su parte, los servidores DNS actuales también son capaces de resolver nombres en sus correspondientes direcciones IPv4 e IPv6 y viceversa.

A partir de la publicación del RFC 5006 se incluye la opción RDNSS en los mensajes neighbor discovery como forma alternativa de proveer servidores de nombres en el proceso SLAAC.

En los mensajes RA se informa a los hosts de la red la estrategia de configuración a utilizar de acuerdo a los valores de un par de flags denominadas M (ManagedFlag) y O (OtherConfigFlag). En caso de estar activo el bit M los hosts intentarán configurarse mediante DHCP, lo que se conoce como configuración stateful, mientras que si está activo el bit O, los hosts obtendrán sus direcciones IPv6 mediante SLAAC , pudiendo completar los restantes parámetros mediante RDNSS ó DHCP.

En base a todo lo anterior se definieron para esta investigación una serie de laboratorios para implementar las características mencionadas. Se llevaron a cabo laboratorios de auto-configuración mediante SLAAC+RDNSS y SLAAC+DHCPv6, este último en dos variantes, la primera de ellas configurando el servicio DHCP de manera de suministrar solo servidores de nombres y la segunda para que DHCP suministre tanto direcciones IPv6 globales como así también servidores de nombres.

Para todas las experiencias se utilizó el prefijo de documentación IPv6 tal como se indica en

el RFC 3849 y se seleccionó la subred 2001:db8:1c5e:da55::/64 para las prácticas de laboratorio.

Resultados obtenidos

Laboratorio SLAAC+RDNSS

En este caso el servidor SLAAC (router R) se configuró para proveer prefijo de subred y servidores DNS. El servicio se editó en el archivo /etc/radvd.conf incluyendo la opción RDNSS tal como se muestra en la figura 2.

```
interface enp0s3
{
AdvSendAdvert on;
prefix 2001:db8:1c5e:da55::/64
{
};
RDNSS 2001:db8:1c5e:da55::2;
{
AdvRDNSSLifetime 600;
};
};
```

Figura 2 - Configuración SLAAC+RDNSS en /etc/radvd.conf

En la configuración se anuncia el prefijo a utilizar para la auto-configuración y se incluye la opción RDNSS indicando a 2001:db8:1c5e:da55::2 como la dirección IPv6 del servidor DNS de la red. También se incluye la opción del tiempo de validez del anuncio del servidor de nombres en segundos. Los hosts IPv6 enviarán un nuevo mensaje RS antes de la finalización de este temporizador para verificar si hubo o no cambios en el anuncio RDNSS.
Para verificar el funcionamiento de esta configuración se procedió a reiniciar el servicio radvd mediante la instrucción service radvd restart y luego se hizo un relevamiento de la configuración de red en un host MS Windows y en otro GNU/Linux. Los resultados pueden observarse en las figuras 3 y 4.

```
Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Realtek PCIe FE Family Controller
   Physical Address. . . . . . . . . : 90-CD-B6-3C-76-07
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   IPv6 Address. . . . . . . . . . . : 2001:db8:1c5e:da55:9588:8f84:ce44:e00c(Preferred)
   Temporary IPv6 Address. . . . . . : 2001:db8:1c5e:da55:75f3:1027:1583:1369(Preferred)
   Link-local IPv6 Address . . . . . : fe80::9588:8f84:ce44:e00c%4(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.1.110(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : domingo, 5 de agosto de 2018 23:29:44
   Lease Expires . . . . . . . . . . : martes, 7 de agosto de 2018 16:35:29
   Default Gateway . . . . . . . . . : fe80::a00:27ff:fe27:c82f%4
                                       192.168.1.1
   DHCPv6 IAID . . . . . . . . . . . : 59821494
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-20-5E-81-89-30-E1-71-2B-E5-A1
   DNS Servers . . . . . . . . . . . : 2001:db8:1c5e:da55::2
                                       8.8.8.8
```

Figura 3 - Auto-configuración IPv6 SLAAC+RDNSS en un host MS Windows 10

```
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 08:00:27:c0:3a:a8 brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.104/24 brd 192.168.1.255 scope global dynamic enp0s3
       valid_lft 85954sec preferred_lft 85954sec
    inet6 2001:db8:1c5e:da55:b86f:8e5f:3a33:44f8/64 scope global temporary dynamic
       valid_lft 85954sec preferred_lft 13954sec
    inet6 2001:db8:1c5e:da55:a00:27ff:fec0:3aa8/64 scope global mngtmpaddr noprefixroute dynamic
       valid_lft 85954sec preferred_lft 13954sec
    inet6 fe80::a00:27ff:fec0:3aa8/64 scope link
       valid_lft forever preferred_lft forever


root@hostipv6:~# ip -6 route list
2001:db8:1c5e:da55::/64 dev enp0s3 proto ra metric 100  pref medium
fe80::a00:27ff:fe27:c82f dev enp0s3 proto static metric 100  pref medium
fe80::/64 dev enp0s3 proto kernel metric 256  pref medium
default via fe80::a00:27ff:fe27:c82f dev enp0s3 proto static metric 100  pref medium

# Generated by NetworkManager
nameserver 192.168.1.1
nameserver 2001:db8:1c5e:da55::2
```

Figura 4 - Auto-configuración IPv6 SLAAC+RDNSS en un host GNU/Linux

Para las verificaciones en MS Windows se ejecutó el comando ipconfig, mientras que en GNU/Linux los resultados corresponden a la ejecución de ip address list para las direcciones de red, ip -6 route list para la verificación de la default gateway y cat /etc/resolv.conf para la dirección del servidor DNS.

En ambos casos los hosts ejecutaron satisfactoriamente su auto-configuración IPv6 mientras mantienen sus configuraciones IPv4 originales tal como era de esperar en un entorno dual stack. Ambos hosts obtuvieron una dirección IPv6 global perteneciente a la red del laboratorio y la dirección IPv6 del servidor DNS correcta. Es preciso observar también que siempre la default gateway de los hosts será la dirección link local del router R que cumple la función de servidor SLAAC, en este caso se trata de la dirección fe80::a00:27ff:fe27:c82f.

El servidor SLAAC virtualizado cumplió con su función. El servicio de auto-configuración

también está disponible en algunos modelos comerciales de routers y switches capa 3 con configuraciones muy similares a las vistas en este laboratorio.

Laboratorios SLAAC+DHCPv6

Tal como se anticipó en párrafos anteriores, se trata de dos laboratorios en los cuales varían las funciones del servidor DHCPv6. En el primer laboratorio se experimentó con un servidor DHCPv6 que otorgó solo la dirección IPv6 del servidor DNS, dejando los restantes parámetros de auto-configuración a cargo del router R (SLAAC). En el segundo laboratorio el router R solo proporcionó la información de default gateway mientras que el servidor DHCPv6 se utilizó para suministrar los restantes parámetros, es decir, direcciones IPv6 globales y dirección IPv6 del servidor DNS.
Para el primer laboratorio en la configuración del servicio radvd se suprimió la opción RDNSS utilizada con anterioridad y se activó el bit O tal como se muestra en la figura 5.

```
interface enp0s3
{
AdvSendAdvert on;
AdvOtherConfigFlag on;
prefix 2001:db8:1c5e:da55::/64
{
};
};
```

Figura 5 - Configuración SLAAC sin opción RDNSS en /etc/radvd.conf

De esta manera mediante SLAAC se proporciona el prefijo de auto-configuración IPv6 y la default gateway de la red.
La dirección IPv6 del servidor de nombres quedó a cargo del servidor DHCPv6. La configuración del servidor DHCPv6 (isc-dhcp-server) se realizó editando el archivo /etc/dhcp/dhcpd6.conf tal como se muestra en la figura 6.

```
option dhcp6.name-servers 2001:db8:1c5e:da55::2;

option dhcp6.domain-search "ucse.edu.ar";

subnet6 2001:db8:1c5e:da55::/64 {

}
```

Figura 6 – Configuración DHCPv6 para proporcionar solo servidor DNS

Para la correcta configuración del servicio es necesario incluir la opción subnet6 pero sin declarar un rango de direcciones a asignar debido a que los hosts de la red se auto-configurarán mediante el prefijo IPv6 anunciado en los mensajes RA.

Luego de reiniciar los servicios radvd e isc-dhcp-server mediante la forma habitual en Debian, es decir ejecutando service radvd restart y service isc-dhcp-server restart respectivamente, se procedió a verificar la configuración de red en los hosts. Los resultados en ambos casos fueron satisfactorios y se muestran en las figuras 7, 8 y 9. En ambas figuras solo se muestra un extracto de las líneas con información más relevante. Para el hosts MS Windows se ejecutó ipconfig. En el caso del host GNU/Linux la información acerca de las direcciones de la interfaz se obtuvieron luego de ejecutar ip address list, mientras que la información sobre los servidores de nombres resultaron de la instrucción cat /etc/resolv.conf.

```
IPv6 Address. . . . . . . . . . . : 2001:db8:1c5e:da55:9588:8f84:ce44:e00c(Preferred)
Temporary IPv6 Address. . . . . . : 2001:db8:1c5e:da55:8446:5a24:9065:2180(Preferred)
Link-local IPv6 Address . . . . . : fe80::9588:8f84:ce44:e00c%4(Preferred)
Default Gateway . . . . . . . . . : fe80::a00:27ff:fe27:c82f%4
DNS Servers . . . . . . . . . . . : 2001:db8:1c5e:da55::2
```

Figura 7 – Auto-configuración IPv6 SLAAC+ DNS mediante DHCPv6 en MS Windows 10

```
enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
inet6 2001:db8:1c5e:da55:410a:1b33:8b3f:8d4a/64 scope global temporary dynamic
inet6 2001:db8:1c5e:da55:a00:27ff:fec0:3aa8/64 scope global mngtmpaddr noprefixroute dynamic
```

Figura 8 - Auto-configuración IPv6 SLAAC+ DNS mediante DHCPv6 resultado de ip address list en GNU/Linux

```
# Generated by NetworkManager
nameserver 192.168.1.1
nameserver 2001:db8:1c5e:da55::2
```

Figura 9 - Auto-configuración IPv6 SLAAC+ DNS mediante DHCPv6 resultado de cat /etc/resolv.conf en GNU/Linux

En el último laboratorio se procedió a configurar el servidor DHCPv6 para proporcionar direcciones IPv6 globales y dirección IPv6 del servidor DNS. Para SLAAC solo queda reservada la asignación de default gateway. Este último escenario es el más similar al utilizado habitualmente en IPv4 cuando los hosts obtienen configuración mediante DHCP.

Ahora la configuración del servicio radvd no debe incluir la opción prefix y debe incorporarse el flag M mediante la línea AdvManagedFlag on;, mientras que la

configuración del servidor DHCPv6 debe incluir un rango de direcciones para la opción subnet6 tal como se muestra en la figura 10.

```
option dhcp6.name-servers 2001:db8:1c5e:da55::2;
option dhcp6.domain-search "ucse.edu.ar";
subnet6 2001:db8:1c5e:da55::/64 {
range6 2001:db8:1c5e:da55::3 2001:db8:1c5e:da55::9;
}
```

Figura 10 – Configuración DHCPv6 para asignación de direcciones globales y DNS

Los resultados obtenidos en los hosts de la red fueron satisfactorios y similares a los mostrados en el laboratorio anterior con la única diferencia de que ahora las direcciones IPv6 globales no se auto-generaron en los hosts sino que fueron provistas directamente por el servidor DHCPv6. Como muestra, en la figura 11 puede verse el resultado de la consulta de direcciones de red en un host MS Windows. Nuevamente solo se muestran las líneas con información relevante.

```
IPv6 Address. . . . . . . . . . . : 2001:db8:1c5e:da55::8(Preferred)
Default Gateway . . . . . . . . . : fe80::a00:27ff:fe27:c82f%4
DNS Servers . . . . . . . . . . . : 2001:db8:1c5e:da55::2
```

Figura 11 - Auto-configuración IPv6 SLAAC+DHCPv6 en MS Windows 10

La ejecución de estos últimos laboratorios permitió observar la utilización combinada de los distintos métodos de auto-configuración IPv6 disponibles.

Conclusiones

La investigación permitió elaborar una serie de recomendaciones para iniciar las tareas de prueba y despliegue de IPv6 en redes LAN. Primero se estableció la necesidad de contar con una red de laboratorio implementada de manera física con elementos de conectividad básicos, al alcance de todo operador de red convencional más la incorporación de servicios

de red para la auto-configuración IPv6 que podrían ser habilitados en servidores físicos o virtualizados. La red de pruebas también puede llegar a implementarse de manera totalmente virtual utilizando alguna de las muchas aplicaciones de virtualización disponibles.

Una vez disponible la red de pruebas pudieron iniciarse las tareas de laboratorio seleccionando las diversas opciones de auto-configuración disponibles, tal como se detalló a lo largo de este trabajo. En todos los casos las configuraciones de los servicios necesarios resultaron sencillas y de fácil entendimiento para cualquier operador de red familiarizado con servidores GNU/Linux.

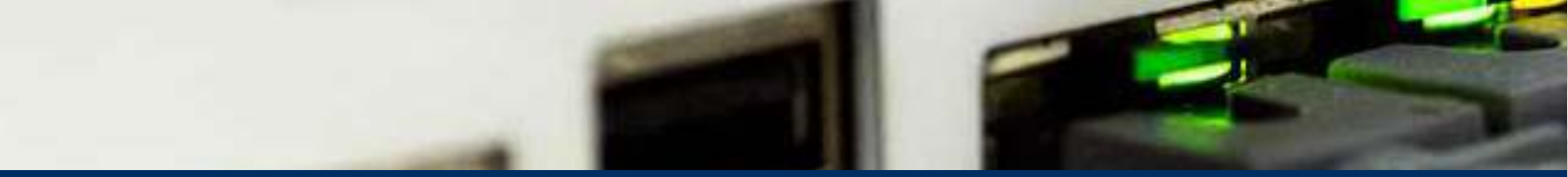
Como resultado de las prácticas de laboratorio pudo demostrarse que la realización de experiencias básicas relacionadas con la auto-configuración IPv6 en redes LAN está al alcance de todo operador de red mínimamente experimentado. Basta con implementar redes de prueba integrando elementos de red básicos y servicios virtualizados mediante herramientas de software libre. También pudo verse el correcto comportamiento de los principales sistemas operativos modernos en entornos dual stack.

Uno de los objetivos planteados para este proyecto de investigación estaba relacionado con incentivar el inicio de tareas de despliegue de IPv6, y tal como se pudo apreciar en el desarrollo de las experiencias de laboratorio, no hay mayores impedimentos técnicos para avanzar en las pruebas de configuración de servicios y despliegue de IPv6 en redes locales. IPv6 puede convivir sin problemas con IPv4 y este hecho facilita a los operadores de red realizar pruebas de rendimiento y análisis de comportamiento de los distintos servicios de red en este entorno dual stack.

Otro de los objetivos del trabajo estuvo relacionado con la formación de recursos humanos, en este sentido, el trabajo de investigación permitió afianzar los conocimientos teóricos sobre IPv6 tanto para los docentes como para los alumnos investigadores. Esto resultó muy beneficioso para las cátedras involucradas en el proyecto debido a que IPv6 es un tema que forma parte de los contenidos a desarrollar. Mucho de lo aprendido podrá ser incorporado no solo como material original en la teoría sino también como parte de trabajos prácticos para los alumnos.

En cuanto a la formación docente en investigación, los docentes involucrados sumaron experiencia en el área y profundizaron los conocimientos relacionados con esta temática. A los alumnos investigadores les permitió ingresar al mundo de la investigación, incorporar nuevos conocimientos y generar importantes antecedentes en el área.

Al DASS/UCSE le permitirá la realización de tareas de extensión mediante la divulgación de los resultados en congresos y publicaciones científicas.



Bibliografía

Internet Society, (2010). The Internet is for Everyone – IPv6 Deployment: State of play and the way forward. ISOC.

Deering, S. E., Hinden, R., (2017). Internet Protocol, Version 6 (IPv6) Specification. RFC 8200. IETF.

Wu, P., Cui, Y., Wu, J., Liu, J., Metz, C., (2012). Transition from IPv4 to IPv6: A State-of-the-Art. IEEE Communications Surveys Tutorials.

Gilligan, R. E., Nordmark, E., (2005). Basic Transition Mechanisms for IPv6 Hosts and Routers. RFC 4213. IETF.

Arkko, J., Baker, F., (2011). Guidelines for Using IPv6 Transition Mechanisms during IPv6 Deployment. RFC 6180. IETF.

China Telecom, (2015). IPv6 Deployment Best Practice by China Telecom.

Simpson, W. A., Narten, T., Nordmark, E., Soliman, H., (2007) Neighbor Discovery for IP version 6 (IPv6). RFC 4861. IETF.

Gupta, M., Conta, A., (2006). Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification. RFC 4443. IETF.

Volz, B., (2006). Dynamic Host Configuration Protocol for IPv6 (DHCPv6) Relay Agent Subscriber-ID Option. RFC 4580. IETF.

Jeong, J. P., Park, S. D., Beloeil, L., Madanapalli, S., (2017). IPv6 Router Advertisement Options for DNS Configuration. RFC 8106. IETF.

Cicileo, G., Gagliano, R., O'Flaherty, C., Olvera Morales, C., Palet Martínez, J., Rocha, M., Vives Martínez, A., (2010). IPv6 Para Todos. Internet Society.