cet
41:(2020)
ISSN:1668-9178

Protocolo IPv6: fundamentos y aplicaciones

Sergio Daniel Saade, Carlos Albaca Paraván, Federico Herman Lutz y Javier Ignacio Bilbao

Facultad de Ciencias Exactas y Tecnología, Universidad Nacional de Tucumán, Tucumán, Argentina.

Resumen

El protocolo IPv6 fue estandarizado en el año 1998; sin embargo, su adopción comenzó a realizarse en forma masiva unas dos décadas después. Con este protocolo se soluciona principalmente el problema de la falta de direcciones IPv4 (públicas), que son utilizadas para el acceso global a Internet. El presente trabajo expone sintéticamente los aspectos más destacados del protocolo IPv6, las principales diferencias con IPv4, los diferentes tipos de direcciones IPv6, los mecanismos básicos para brindar direccionamiento automático a los nodos que componen una red privada y ciertas modificaciones que se realizaron en la estructura completa de los protocolos TCP/IP para su correcto funcionamiento. El trabajo también expone el desarrollo de un proyecto para la migración de la infraestructura de la red privada de la Universidad Nacional de Tucumán hacia este protocolo.

Palabras clave: IPv6, direccionamiento IPv6, migración IPv6.

IPv6 Protocol: fundamentals and applications

Abstract

The IPv6 protocol was standardized in 1998; however, its adoption began to take place on a massive scale approximately two decades later. This protocol mainly solves the problem of the lack of (public) IPv4 addresses, which are used for global Internet access. The present work summarizes the most outstanding aspects of the IPv6 protocol, the main differences with IPv4, the structure of the different types of IPv6 addresses, the basic mechanisms for providing automatic addressing to the nodes that conform a private network, and certain modifications that were made to the complete structure of the TCP/IP protocols for their correct operation. The paper also describes the development of a project for migrating the infrastructure of the private network of the Universidad Nacional de Tucumán to this protocol.

Keywords: *IPv6, IPv6 addressing, IPv6 migration.*

Introducción

Deering y Hinden (1998) estandarizaron el protocolo IPv6 mediante el RFC 2460 y fue creado con la intención de reemplazar a la versión 4 del protocolo IP que hoy en día se utiliza mayormente como acceso a Internet. La necesidad del cambio apareció principalmente por el agotamiento global de direcciones IPv4.

El **Registro de Direcciones de Internet de América Latina y Caribe** (2020) informó que, en nuestro contexto regional, a mayo de 2020 la distribución de direcciones IPv4 públicas se encuentra en un alto grado de agotamiento (Fase 3).

Pese a que el protocolo IPv6 tiene más de dos décadas de estandarización, su adopción comenzó en forma medianamente masiva desde la mitad de la década pasada, cuando los principales centros regionales de registro de direcciones (RIR) comenzaron a entrar en fase de agotamiento de direcciones IPv4 públicas. Si se observa la figura 1, **Google** (2020), se tiene un crecimiento sostenido del uso de IPv6 a partir del 2015. Se espera un crecimiento aún mayor con la progresiva implementación de soluciones de IoT (Internet de las Cosas) y asociadas, como así también con la extenuación completa de direcciones IPv4.

En nuestro país, la adopción de IPv6 a mayo de 2020 es de aproximadamente un 11%. **Nader et al.** (2015) muestran el estado de implementación de IPv6 en nuestro país en 2015, concluyéndose en el mismo una falta total de uso del mismo. Actualmente, en la República Argentina solo pueden contratar accesos a IPv6 clientes corporativos, quedando excluido por el momento el acceso domiciliario, excepto en grandes urbes como CABA.

Los objetivos de este trabajo son, en primer lugar mostrar los principales cambios entre el protocolo IPv4 e IPv6, no solo en el sistema de direccionamiento sino también en otros protocolos del *stack* TCP/IP, para finalizar detallando la implementación del mismo en la red de la Universidad Nacional de Tucumán.

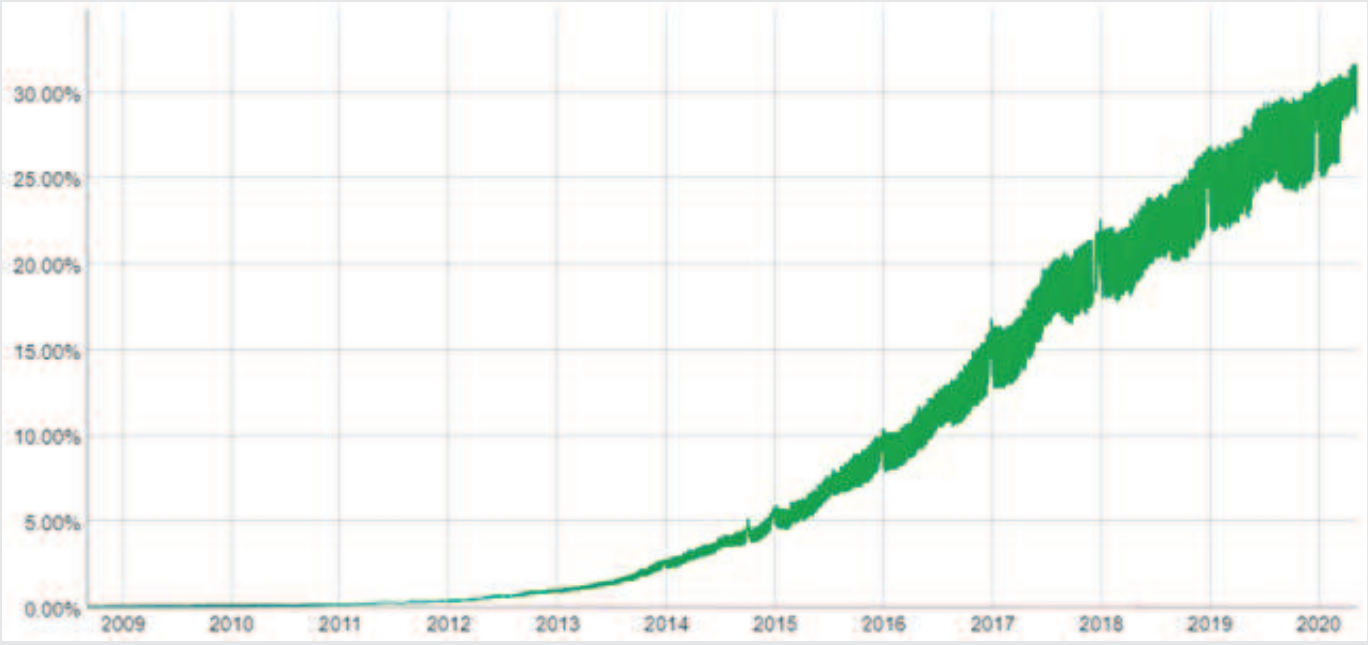


Fig. 1 Adopción de IPv6 para acceso a Internet a través del tiempo.

Principales cambios de IPv6 sobre IPv4

Saade (2016) describe las principales diferencias entre IPv6 e IPv4, las cuales son:

- **Espacio de direcciones expandido**: la longitud del campo dirección cambia de 32 bits a 128 bits.
- **Arquitectura de direccionamiento mejorada**: además de un incremento en el espacio de direcciones, éstas poseen una estructura que permite ser subdividida en dominios de enrutamiento jerárquico que reflejan la topología real y actual de Internet.
- **Encabezado más eficiente**: se eliminaron algunos campos de encabezamiento IPv4, agilizando el procesamiento de paquetes en los *routers*. Por otra parte, las opciones en caso de existir, son ubicadas en cabeceras de extensión (*extension headers*) al final del encabezamiento obligatorio.
- **Seguridad**: se utiliza (como cabecera de extensión, es decir en forma opcional) el protocolo IPSec.

Dentro de los cambios mencionados, el más importante es el del direccionamiento, a desarrollarse con ciertos detalles en el presente artículo.

Direccionamiento IPv6

El principal cambio entre IPv6 e IPv4 radica en el direccionamiento: las direcciones IPv6 tienen una longitud de 128 bits y su arquitectura difiere considerablemente sobre la de IPv4. Incluso la representación es diferente: una dirección IPv6 es representada con 32 dígitos hexadecimales, separándose cada 4 dígitos (hexteto) con un carácter de dos puntos ":". De esta forma una dirección IPv6 queda representada por 8 grupos de 4 dígitos hexadecimales (8 hextetos).

Por ejemplo, la siguiente es una dirección IPv6:

FF02:0000:0000:0000:0000:0000:0000:0001

Para facilidad en la lectura y escritura, se introdujeron dos formas de abreviatura:

1. **Reducción de ceros más significativos de cada grupo de 4 dígitos**: escribiéndose en ese caso, solo a partir del dígito distinto de cero.
2. **Eliminación de un hexteto con todos 0's**: en éste se pueden escribir simplemente dos caracteres ":" en forma consecutiva.

Usando ambas reglas, la dirección del ejemplo quedaría escrita en forma abreviada:

FF02::1

Existen tres tipos de direcciones IPv6: direcciones *unicast, multicast y anycast*. No existen las direcciones *broadcast* siendo reemplazadas por tipos especiales de direcciones *multicast*. La figura 2 muestra esquemáticamente las diferentes direcciones IPv6.

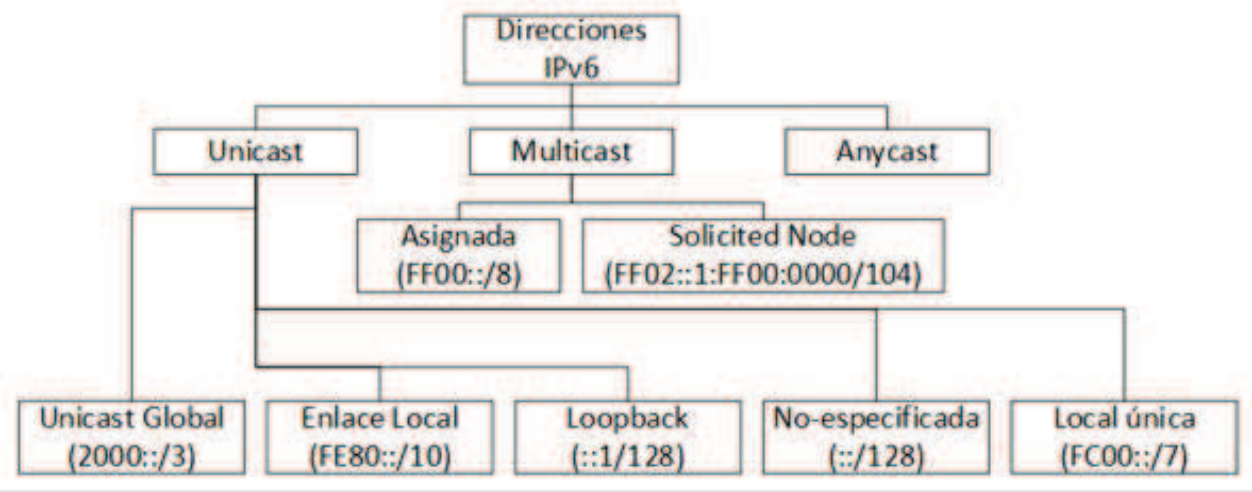


Fig. 2 Clasificación de direcciones IPv6.

Una dirección IPv6 u*nicast* identifica a una interfaz en un dispositivo más que a un dispositivo en sí. De hecho, una interfaz física tiene varias direcciones IPv6 asociadas. Dentro de las direcciones *unicast* las más destacables son las globales (*global unicast*) y las de enlace local (*link-local*), que se verán a continuación con mayor detalle.

Direcciones u*nicast* globales

Las direcciones *unicast* globales son direcciones globalmente alcanzables en Internet, es decir equivalen a las direcciones IPv4 públicas. Poseen la estructura mostrada en la figura 3.

Se distingue a estas direcciones porque los tres primeros bits tienen el valor 001 (rango del primer hexteto de 2000 a 3FFF).

La primera porción de la dirección es lo que se denomina prefijo de ruteo global. Este prefijo es el identificador de red (NetID) y es otorgada por un RIR (o un ISP). Típicamente tiene un tamaño de 48 bits (n = 48 en la figura 3).

Luego del prefijo de ruteo global, la dirección continúa con el ID de subred: a diferencia de IPv4, en IPv6 el identificador de subred es un campo separado y no forma parte de la porción del identificador de nodo. Típicamente esta porción posee un tamaño de 16 bits (m = 16 en figura 3). El prefijo global de ruteo junto con el identificador de subred compone lo que se llama prefijo de subred (la cantidad de bits de éste, constituye lo que se conoce como longitud del prefijo de red).

Finalmente se encuentra la porción de InterfazID, equivalente a la dirección del nodo propiamente dicha de IPv4. Normalmente este campo posee un tamaño de 64 bits para poder utilizar un esquema de direccionamiento automático para la generación del InterfazID.

Un aspecto que debe destacarse en IPv6 es que los nodos privados tienen configurados una dirección *unicast* global. Es decir, los dispositivos privados son accesibles desde la red pública. No existe el concepto de direcciones públicas y privadas, como así tampoco el uso de NAT para su traducción. Si bien esto tiene como desventaja el hecho de que las interfaces están expuestas al mundo a través de Internet, no se utilizan los mecanismos de traducción de direcciones, que imponen ciertos retardos y por lo tanto latencias en las aplicaciones.

Direcciones u*nicast* de enlace local

Las direcciones de enlace local son direcciones *unicast* confinadas a un único enlace o subred, es decir, un paquete que posee una dirección de este tipo como dirección destino, no puede atravesar un *router*. Estas direcciones se crean automáticamente con la habilitación de IPv6 en una interfaz. Por lo tanto, un dispositivo tiene mínimamente dos direcciones IPv6 *unicast* asignadas: una global y una de enlace local.

La principal ventaja de estas direcciones es que un dispositivo la crea en forma automática cuando se activa IPv6. Su uso es amplio: por ejemplo, en la configuración automática de direcciones, como parte del protocolo NDP (*Neighbor Discovery Protocol*) y también para la comunicación entre nodos de una misma subred.

El formato de estas direcciones se muestra en la figura 4.

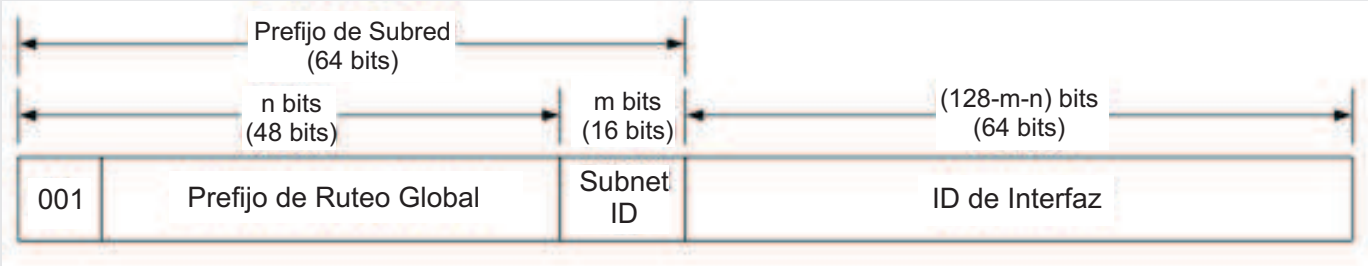


Fig. 3 Estructurada de IP *unicast* global.

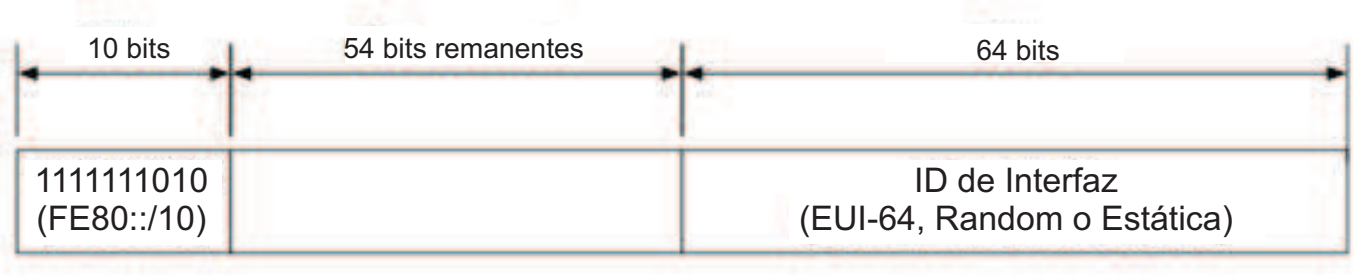


Fig. 4 Formato de direcciones *unicast* de enlace local (*link*-local).

Se observa que estas direcciones tienen un prefijo de 10 bits (1111 1110 10), con los 54 bits restantes del prefijo de red (/64) con valor cero. El ID de interfaz (últimos 64 bits) puede ser obtenido por tres métodos:

- Estático o manual, es decir configurado a través del administrador
- Usando el algoritmo EUI-64, basado en la MAC de la interfaz (**Hinden and Deering** (1998)).
- Aleatorio

La figura 5 muestra un ejemplo de una red con el uso de ambos tipos de direcciones IPv6.

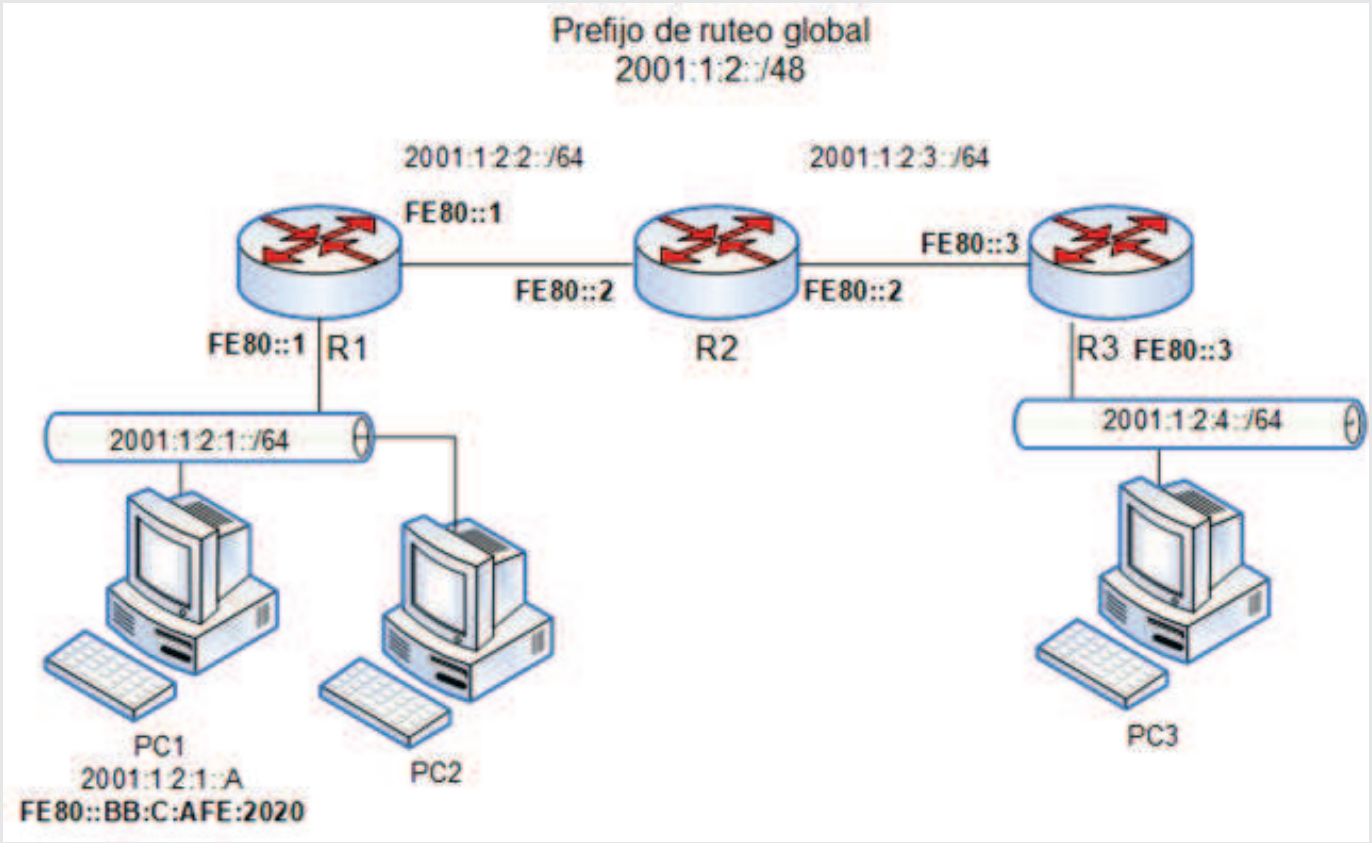


Fig. 5 Ejemplo de direccionamiento IPv6 en una red privada.

Direcciones *multicast*

Este mecanismo de direccionamiento y difusión de paquetes, permite que un dispositivo envíe un único paquete a múltiples destinos. Para identificar el grupo de dispositivos (receptores), se utilizan las direcciones *multicast*.

El esquema de direccionamiento *multicast* en IPv6 es mucho más refinado y complejo que en IPv4. La figura 6 muestra el esquema de este tipo de direcciones.

Estas direcciones comienzan con el prefijo FF::/8. Luego sigue el campo *flag*, de cuatro *bits*, que indica el tipo de dirección *multicast*, habiéndose definido por el momento sólo dos:

- **Direcciones *multicast* permanentes**: valor 0 del *flag*. Son direcciones públicas o bien conocidas, asignadas por IANA.
- **Direcciones *multicast* transitorias o dinámicas**: valor 1 del *flag*. Estas direcciones son asignadas por aplicaciones a medida que se van creando los grupos de multidifusión.

A continuación, se encuentra el campo de ámbito (4 bits). Este campo indica el rango de cobertura del paquete *multicast* (por ejemplo, subred, toda la red privada, etc.). De esta forma se reemplazan los *broadcasts*, generándose un paquete *multicast* dirigido a todos los nodos de la subred.

Finalmente, la dirección contempla al identificador de grupo de multidifusión de 112 bits de longitud.

Direcciones *anycast*

Tienen el mismo significado que en IPv4, es decir son direcciones *unicast* idénticas asignadas a más de un nodo físicamente diferente. El paquete IP cuya dirección destino es *anycast*, se entrega a aquel cuya métrica de ruteo es la mejor. Es utilizada principalmente para el acceso a réplicas de servidores DNS.

Direccionamiento automático

Las direcciones IPv6 *unicast* globales pueden configurarse en forma automática sin la intervención de un administrador. Existen dos métodos para dicha configuración:

- **Autoconfiguración de direcciones sin estado (SLAAC - *StateLess Address Auto Configuration*)**: con este método, se obtiene el prefijo de red (y su longitud) de un *router* mediante un mensaje ICMPv6 denominado *Router Advertisement*[1] (RA). El ID de interfaz se genera en forma aleatoria o utilizando el algoritmo EUI-64.
- **DHCP**: utiliza el protocolo DHCPv6 que es similar al protocolo DHCP para IPv4.

SLAAC

SLAAC está definido por **Thomson et al.** (2007) en el RFC 4862[2]. Este método permite obtener direcciones denominadas sin estado, porque ningún dispositivo (servidor, *router*, etc.) mantiene una base de datos unificada con las direcciones otorgadas a los clientes. El prefijo de red y su longitud es entregado por un *router*, y el ID de interfaz se obtiene a partir de la dirección MAC del nodo (utilizando algoritmo denominado EUI-64 modificado) o en forma aleatoria (dependerá del sistema operativo del cliente).

La figura 7 muestra resumidamente el proceso SLAAC. Cuando PC1 inicia el proceso de arranque envía un mensaje de *Router Solicitation* (RS). El *router* R1 responde a RS con un mensaje RA (*Router Advertisement*). Dentro del mensaje RA está el prefijo de red y su longitud, la dirección del *router* por defecto, el tiempo de vida de la dirección y otros parámetros.

PC1 al recibir el RA, adquiere el prefijo de red (2001:8BFA:1000:1/64). Luego, completa la dirección IPv6, generando el ID de interfaz. En el ejemplo de la figura 7 utiliza el método EUI-64 modificado. Por lo tanto, la dirección IPv6 autoconfigurada resulta:

2001:8BFA:1000:1:22A:C8FF:FEF3:4853

La dirección obtenida permanece en un estado que se denomina tentativo hasta que se verifica su unicidad mediante el proceso de detección de dirección duplicada DAD (*Duplicate Address Detection*). DAD tiene un principio de funcionamiento simple: el nodo que necesita descubrir si existe duplicidad, envía en un mensaje de multidifusión[3] su propia IPv6. Para ello

[1]. Tanto RA como RS son mensajes ICMPv6 y forman parte de NDP.
[2]. Originalmente definido el mismo año de la creación de IPv6 a través del RFC 1971. Es decir, IPv6 nació con SLAAC como mecanismo de direccionamiento automático.
[3]. Es interesante destacar que para todo este proceso de SLAAC no se utiliza el mecanismo de direccionado de b*roadcast*, sino direccionamiento *multicas*t.

Fig. 6 Formato de direcciones *multicast*.

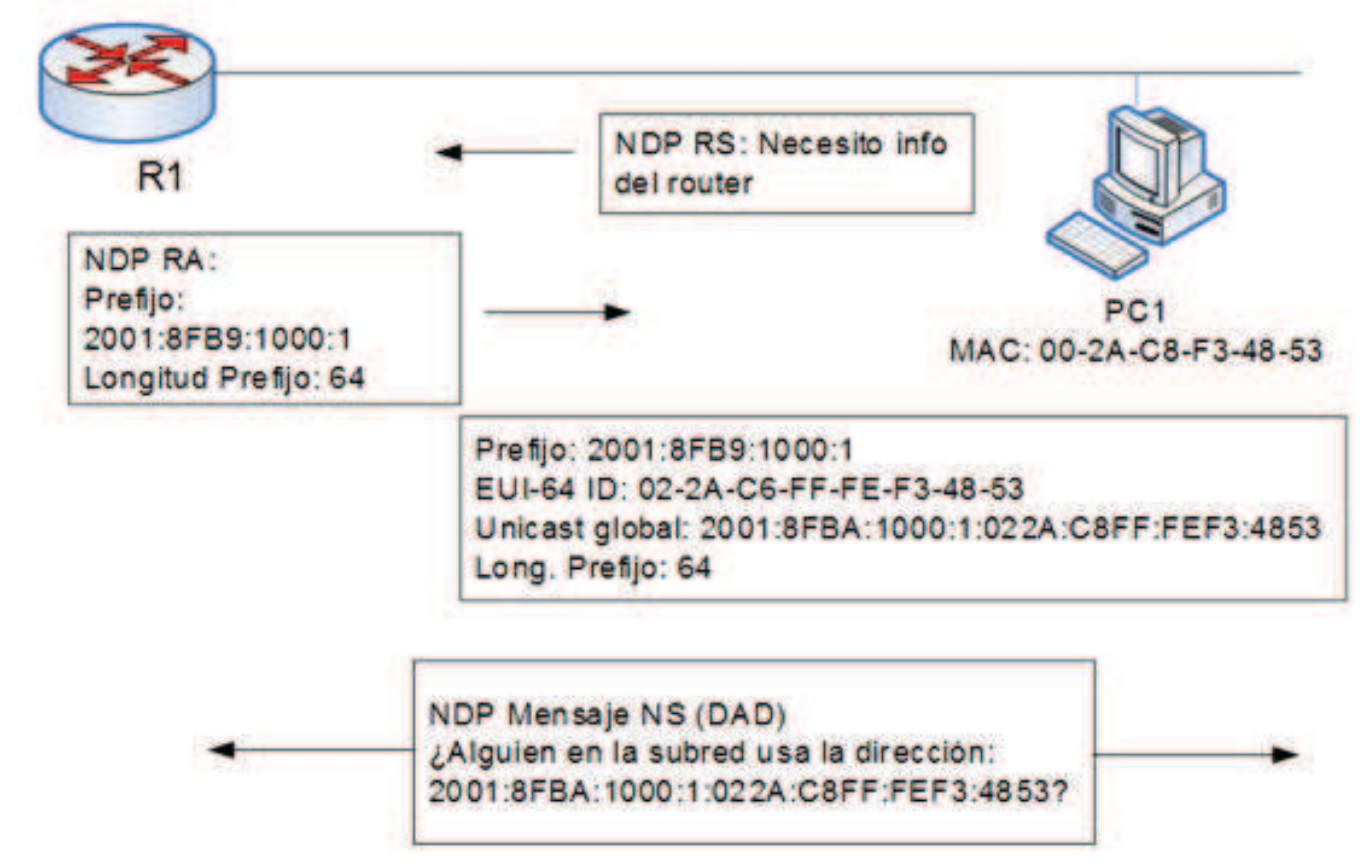


Fig. 7 Mecanismo SLAAC para obtención de direcciones IPv6.

utiliza un mensaje del protocolo ICMPv6 *Neighbor Solicitation* (NS) que consulta si algún otro dispositivo usa dicha IPv6. Si ningún dispositivo contesta dentro de un cierto período de tiempo, se considera que no hay duplicidad de dirección. Si algún dispositivo está utilizando dicha dirección, contestará con un mensaje de *Neighbor Advertisement* (NA) y se abortará su uso.

Una vez detectada la unicidad de la dirección IPv6, la misma pasa del estado tentativo al preferido y puede ser utilizada.

DHCPv6

Un nodo al estar configurado para obtener su dirección en forma automática utilizará el proceso SLAAC o DHCPv6 dependiendo de ciertos parámetros de configuración del *router*.

En el caso que se indique obtener la dirección IPv6 vía DHCPv6, el nodo realiza un intercambio de mensajes especificado por este protocolo, obteniéndose la dirección completa junto con las opciones especificadas en el servidor, **Mrugalski et al.** (2018).

El protocolo DHCPv6 se asemeja al protocolo DHCP para IPv4, **Saade et al.** (2015) realizan un estudio comparativo entre ambas versiones.

Existen dos particularidades de este protocolo que son

importantes de destacar:

• Dentro de las opciones que ofrece DHCPv6, no se encuentra la dirección del *router* por defecto ya que la misma es obtenida del mensaje RA inicial.
• DHCPv6, hasta la fecha, no está soportado por el sistema operativo Android. Por lo que en una red que emplee tabletas, celulares, y otros dispositivos con este sistema operativo deberá utilizarse SLAAC.

Deben tenerse en cuenta estas dos consideraciones en implementaciones reales de configuración automática de direcciones IPv6, permitiendo incluso seleccionar el uso de SLAAC o DHCPv6 como mecanismo de direccionamiento automático.

Finalmente, dependiendo de ciertos *flags* del mensaje RA y del sistema operativo cliente, es posible obtener una dirección tanto por SLAAC como por DHCPv6 (en ese caso una interfaz tendría asociada dos direcciones *unicast* globales).

Modificaciones del resto del *stack* TCP/IP

Debido a la inclusión de IPv6 en el *stack* de protocolos TCP/IP, se generó la necesidad de modificar el funcionamiento de ciertos protocolos del resto de la arquitectura.

Resumidamente, algunas de las principales modificaciones que se realizaron en toda la *suite* TCP/IP para lograr el funcionamiento global de la arquitectura con IPv6 son:

• El protocolo ARP que traduce direcciones IPv4 a direcciones MAC fue reemplazado por mensajes NDP que realizan tal traducción.
• El proceso de ruteo sigue siendo el mismo que en IPv4. Las tablas de ruteo se pueden crear y mantener en forma manual (ruteo estático) y/o en forma automática (ruteo dinámico) con el uso de protocolos de ruteo. Estos últimos fueron adaptados de IPv4 a IPv6, por lo que ahora se tienen nuevas versiones de dichos protocolos como, por ejemplo, para el caso de ruteo interior a RIPng (RIPv3), OSPFv3 o EIGRPv6 (propietario de Cisco) o en el caso de ruteo exterior a BGP-4.
• Los protocolos de transporte no alteran en nada su funcionamiento con IPv6. Es decir, no fue necesario realizar ninguna modificación en TCP y UDP, excepto por el cálculo del *checksum* de los encabezamientos. Particularmente en el caso de UDP, es obligatorio realizar el cómputo del *checksum* en su cabecera, ya que el encabezamiento IPv6 no provee dicho campo.
• DNS introduce un nuevo registro denominado AAAA que permite la resolución de nombres a direcciones IPv6. También se introducen reglas para el retorno de direcciones IPv6 e IPv4 en caso que un mismo nombre de nodo, posea ambas traducciones. El espacio de nombre para la traducción inversa de direcciones fue creado debajo de un nuevo dominio denominado ip6.arpa.

Implementación de IPv6 en la UNT

En el año 2016 desde el Laboratorio de Redes de Computadoras de la Facultad de Ciencias Exactas y Tecnología (FACET), se lideró un proyecto de planificación e implementación de IPv6 en la Universidad Nacional de Tucumán, **FRIDA** (2016). Dicho proyecto contó con el auspicio de LACNIC a través del Programa FRIDA (Fondo para el Fortalecimiento de Internet en América Latina y el Caribe).

El proyecto (**Saade et al.** (2017)) de un año de duración, permitió la adquisición de equipamiento de red de última generación y prestaciones para el soporte de IPv6, tanto en el Centro Herrera como en Rectorado de la UNT y para experimentación dentro del mencionado laboratorio.

La figura 8 muestra el diagrama general de la red de la UNT al día de hoy. Como se observa, se poseen dos accesos a IPv6: a través de RIU (Red Interuniversitaria) con prefijo de ruteo global 2800:110:3E00::/48 y a través de Telecom con prefijo 2001:13d1:3c02::/48.

Dentro de la FACET, tanto los servidores que albergan los sitios web de las Facultades de Ciencias Exactas y Tecnología, Ciencias Económicas y Arquitectura y Urbanismo de la UNT, como el servidor DNS autoritativo para dichos dominios soportan ambos protocolos (IPv4 e IPv6). Es decir, cualquier cliente a nivel mundial podrá acceder a estos servidores con el uso de IPv6 en forma nativa.

Dentro de la FACET, si bien se implementó y adecuó toda la infraestructura de servicios para soporte de IPv6, la diversidad de clientes (en *Hardware*, *Software* y sistemas operativos), no permite por el momento realizar el despliegue completo; solamente se está empleando de manera académica IPv6 dentro del Laboratorio de Redes de Computadoras mediante el uso de un *router* propio y entregando las direcciones por el método de SLAAC.

Fig. 8 Diagrama general de la red UNT con direccionamiento IPv6.

Conclusiones

La implementación a nivel mundial de IPv6 como protocolo de direccionamiento lógico y ruteo viene creciendo sostenidamente, debido al agotamiento de direcciones IPv4. Nuestro país no es ajeno a dicha realidad, con oferta por parte de las empresas de telecomunicaciones de accesos al *backbone* IPv6 a través de diferentes modalidades tanto para clientes corporativos como hogareños (Claro, desde mayo de 2020, empezó un proceso de implementación paulatina del protocolo, brindando direccionamiento IPv6 a algunos clientes de diferentes zonas de San Miguel de Tucumán y Yerba Buena).

Por otra parte, es importante ir adecuando las redes privadas para el uso de dicho protocolo en forma nativa. Si bien existen técnicas de traducción y de tunelizado de IPv4 a IPv6, lo ideal es acceder al *backbone* con el uso de IPv6 nativo, disminuyendo de esa forma la sobrecarga que imponen estos métodos.

La Universidad Nacional de Tucumán (UNT) no es ajena a dicha realidad; con un total de más de diez mil clientes distribuidos en los sitios mostrados en la figura 8, debe adecuar su infraestructura de red para el soporte de IPv6.

Este artículo muestra en forma sintética las principales características de IPv6, ejemplificando con la UNT los primeros pasos de migración que se están tomando en ese sentido.

Las principales conclusiones son:

• Si bien el cambio de IPv4 no es urgente, debe ser analizado y planificado por los administradores de redes privadas, para una transición escalonada.
• En la UNT se encuentra diseñado un esquema general de migración con pruebas de campo y laboratorio; además con algunas redes y servidores en funcionamiento con este protocolo.
• En la planificación, no solo se debe tener en cuenta la adecuación de equipamiento de comunicaciones sino también la adecuación de sistemas operativos de servidores y de clientes, con su correspondiente configuración.
• Puesto que esa adecuación conlleva un gran coste y tiempo de implementación, debe existir una coexistencia de ambos protocolos IP, por ejemplo, utilizando técnica de doble pila (**Saade** (2016)). Con la coexistencia de protocolos, se puede obtener acceso a aquellos servidores públicos que aún no ofrecen servicios sobre IPv6.
• La capacitación es fundamental para el diseño e implementación de redes IPv6. En ese sentido, dentro de la asignatura "Protocolos de Comunicación TCP/IP" de la carrera Ingeniería en Computación, se viene enseñando la temática en forma sostenida y con profundidad desde el año 2017.
• Existen recursos humanos dentro de la FACET con conocimientos y experiencia para la migración a IPv6 y también para brindar capacitación a personal del área informática dentro y fuera de la UNT. De esta manera se puede vincular la Unidad Académica con empresas e instituciones del medio.

Referencias Bibliográficas

Deering, S y Hinden, R. (1998) "RFC 2460: Especificación Protocolo Internet, Versión 6 (Ipv6)". *Documentos RFC en español* [en línea]. Disponible en: https://www.rfc-es.org/rfc/rfc2460-es.txt [Accedido el 13/05/2020].

FRIDA (2016) *"Despliegue de IPv6"*. *LACNIC FRIDA* [en línea]. Disponible en: http://programafrida.net/archivos/project/despliegue-de-ipv6 [Accedido el 13/05/2020].

Google (2020) "Adopción de IPv6". *GoogleIPv6* [en línea]. Disponible en: https://www.google.com/intl/es/ipv6/statistics.html [Accedido el 13/05/2020].

Hinden, R. and Deering, S. (1998) *"RFC 2373: IP Version 6 Addressing Architecture"*. IETF Tools [en línea]. Disponible en: https://datatracker.ietf.org/doc/html/rfc2373 [Accedido el 13/05/2020].

Mrugalski, T., Siodelski, M., Volz, B., Yourtchenko, A., Richardson, M., Jiang, S., Lemon, T. and Winters, T. (2018) *"Dynamic Host Configuration Protocol for IPv6 (DHCPv6)"*. IETF Tools [en línea]. Disponible en: *h*ttps://tools.ietf.org/html/rfc8415 [Accedido el 13/05/2020].

Nader, F., Saade, S. y Bilbao, J. (2015) "Estado de implementación de IPv6 en Argentina", *Investigaciones en Facultades de Ingeniería del NOA*, pp. 483-490.

Registro de Direcciones de Internet de América Latina y Caribe - LACNIC (2020) "Fases de Agotamiento de IPv4" [en línea]. Disponible en: https://www.lacnic.net/1001/1/lacnic/fases-de-agotamiento-de-ipv4 [Accedido el 13/05/2020].

Saade, S., Albaca Paraván, C., Lutz, F. y Gallardo, A. (2015) "DHCPv6: Una comparativa con DHCPv4", *Investigaciones en Facultades de Ingeniería del NOA*, pp. 483-490.

Saade, S. (2016) *Protocolos de comunicación en Internet*, Editorial EDUNT, Argentina.

Saade, S., Bilbao, J., Albaca Paraván, C., Lutz, F., Dip, R. y Berettoni, M. (2017) Despliegue del protocolo IPv6 en la red de la Universidad Nacional de Tucumán, En: *1er. Congreso Latinoamericano de Ingeniería (CLADI)*, Entre Ríos, Argentina, pp. 1142-1145.

Thomson, S., Narten, T. and Jinmei, T. (2007) "RFC 4862: IPv6 Stateless Address Autoconfiguration". *IETF Tools* [en línea]. Disponible en: https://tools.ietf.org/html/rfc4862 [Accedido el 13/05/2020].

Este trabajo se realizó en la Facultad de Ciencias Exactas y Tecnología de la Universidad Nacional de Tucumán, en el marco del Proyecto de Investigación "Comunicaciones y aplicaciones de Internet de las Cosas", PIUNT E652/2, que forma parte del programa "Internet de las Cosas: desde los Sistemas Embebidos a las Aplicaciones".

Sergio D. Saade

Ingeniero Electricista (Or. Electrónica), graduado de la Facultad de Ciencias Exactas y Tecnología (FACET) de la Universidad Nacional de Tucumán (UNT) y M.Sc. en "Electrical and Computer Engineering", University of California. Profesor Titular, dedicación exclusiva (UNT). Director de la Especialización de Posgrado en Integración de Tecnologías Informáticas. Director de Programa de Investigación "Internet de las Cosas: desde los Sistemas Embebidos a las Aplicaciones", PIUNT E652 (2018-2022). Participó en diversas actividades de extensión y vinculación. Publicó diferentes trabajos de investigación y artículos en revistas, ademas de 2 (dos) libros de texto del Área Computación.
Contacto vía e-mail a: ssaade@herrera.unt.edu.ar

Carlos Albaca Paraván

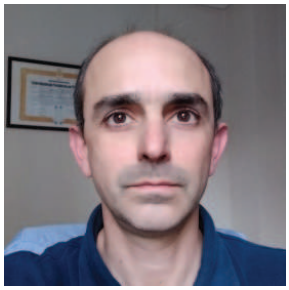
Ingeniero en Computación, graduado de la Facultad de Ciencias Exactas y Tecnología (FACET) de la Universidad Nacional de Tucumán (UNT) y Magister en Ingeniería de Software. Jefe de Trabajos Prácticos, dedicación exclusiva (UNT). Docente de la Especialización de Posgrado en Integración de Tecnologías Informáticas. Participante del Programa de Investigación "Internet de las Cosas: desde los Sistemas Embebidos a las Aplicaciones", PIUNT E652 (2018-2022). Participó en diversas actividades de extensión y vinculación. Publicó diferentes trabajos de investigación y artículos en revistas.
Contacto vía e-mail a: calbaca@herrera.unt.edu.ar

Federico Herman Lutz

Ingeniero en Computación, graduado de la Facultad de Ciencias Exactas y Tecnología (FACET) de la Universidad Nacional de Tucumán (UNT). Jefe de Trabajos Prácticos, dedicación media (UNT). Alumno de la Especialización de Posgrado en Integración de Tecnologías Informáticas. Participante del Programa de Investigación "Internet de las Cosas: desde los Sistemas Embebidos a las Aplicaciones", PIUNT E652 (2018-2022). Participó en diversas actividades de extensión y vinculación. Publicó diferentes trabajos de investigación y artículos en revistas.

Contacto vía e-mail a: fhlutz@herrera.unt.edu.ar

Javier Ignacio Bilbao



Ingeniero en Computación, graduado de la Facultad de Ciencias Exactas y Tecnología (FACET) de la Universidad Nacional de Tucumán (UNT). Jefe de Trabajos Prácticos, dedicación media (UNT). Participante del Programa de Investigación "Internet de las Cosas: desde los Sistemas Embebidos a las Aplicaciones", PIUNT E652 (2018-2022). Participó en diversas actividades de extensión y vinculación. Publicó diferentes trabajos de investigación y artículos en revistas.

Contacto vía e-mail a: jibilbao@herrera.unt.edu.ar

cet
REVISTA DE CIENCIAS EXACTAS E INGENIERIA
FACULTAD DE CIENCIAS EXACTAS Y TECNOLOGÍA

www.facet.unt.edu.ar/revistacet