# Revisión de la Seguridad en la Implementación de Servicios sobre IPv6*

# Safety Review in Implementing Services Over IPv6

Artículo de investigación científica - Fecha de recepción: 31 de agosto de 2015 - Fecha de aceptación: 24 de noviembre de 2015

**Raúl Bareño Gutiérrez**
Magíster en Telemática. Servicio Nacional de Aprendizaje SENA.
CEET Bogotá (Colombia) y Universidad Manuela Beltrán. Bogotá (Colombia). raulbare@misena.edu.co

**William Navarro Núñez**
Especialista en Gerencia de Proyectos de Ingeniería en Telecomunicaciones.
Servicio Nacional de Aprendizaje SENA. Bogotá (Colombia). williamnm2@misena.edu.co

**Sonia Cárdenas Urrea**
Especialista en Gerencia de Proyectos de Ingeniería en Telecomunicaciones.
Servicio Nacional de Aprendizaje SENA. Bogotá (Colombia). secardenas9@misena.edu.co

**Hugo Sarmiento Osorio**
Magíster en Telemática. Servicio Nacional de Aprendizaje SENA. Bogotá (Colombia). hsarmientoo@misena.edu.co

**Nixon Duarte Acosta**
Magíster en Ingeniería (Sistemas y Computación)
Universidad Manuela Beltrán. Bogotá (Colombia). nixon.duarte@docentes.umb.edu.co

Para citar este artículo / To reference this paper:
R. Bareño Gutiérrez, W. Navarro Núñez, S. Cárdenas Urrea, H. Sarmiento Osorio y N. Duarte Acosta "Revisión de la seguridad en la implementación de servicios sobre IPV6", *INGE CUC*, vol. 12, no. 1, pp. 86-93, 2016.

***Resumen--*** En la actualidad los sistemas de transmisión e interconexión presentan varias vulnerabilidades, entre ellas, la facilidad de analizar tráfico que permite una tasa alta de ataques propios del protocolo IPv4, por ello se hace necesario que servicios como FTP, DHCP y SSH busquen la migración e implementación de redes IP bajo IPv6, la cual cuenta con características propias de la seguridad informática mediante el protocolo IPsec, sin importar el sistema operativo libre o propietario de los clientes finales. El presente artículo evalúa, mediante pruebas de configuración, la funcionalidad del estándar o protocolo IPv6 y sus características de seguridad en la implementación como opción de configuración en un escenario controlado para mitigar ataques en la autenticación, integridad y confidencialidad de la información, permitiendo determinar que los servicios analizados garantizan un mayor nivel de confiabilidad propio y nativo a través de IPsec por cualquier medio sobre el cual viajen los datos.

***Palabras claves--*** DHCP; FTP; SSH; IPv6; IPsec; protocolo; seguridad.

***Abstract--*** Actually, transmission and interconnection systems have several vulnerabilities including the facility to analyze traffic that allows a high rate of attacks own IPv4 protocol, therefore it is necessary for services such as FTP, DHCP and SSH seek Migration and Deployment to IPv6 networks. It has characteristics of computer security by IPSEC protocol, regardless of the free operating system or own end customers. This paper analyzes by testing the functionality of the standard settings or IPv6 protocol and its security features in the implementation and setting in a controlled environment to mitigate attacks on authentication, integrity and confidentiality of information, allowing to determine which scenario services analyzed guarantee a higher level of own native IPSEC reliability through regardless of the medium on which data travel.

***Keywords--*** DHCP; FTP; SSH; IPv6; IPsec; Protocol; Security.

* Artículo derivado del proyecto de investigación "Diseño e implementación de un Data Center Didáctico en el Centro de Electricidad, Electrónica y Telecomunicaciones CEET que apoye la formación tecnológica en áreas relacionadas con las TIC". Financiado por SENNOVA. Fecha de inicio: enero 2015. Fecha de finalización: noviembre 2015.

## I. Introducción

Uno de los mejores avances que ha tenido el mundo ha sido Internet como herramienta de comunicación a nivel mundial. Su funcionamiento se implementa sobre un protocolo conocido como IP (protocolo de internet) con el cual se le asigna una dirección virtual a cada equipo para que éste pueda acceder a la red, pero en la actualidad se he hecho escaso quedando pocas direcciones por distribuir en IPv4, además, tiene una alta tasa de vulnerabilidad y gran demanda de direcciones necesarias para cubrir todos y cada uno de los dispositivos que se quieren interconectar, por ello es necesario estandarizar y utilizar la nueva versión del protocolo IPv6 [1], que involucra un pool de direcciones mucho más amplio dadas sus mejores circunstancias de seguridad. Por esta razón es necesario que las empresas empiecen a implementar sus servicios usando tecnología basada en arquitectura con direccionamiento en IPv6 [2]-[3].

En el protocolo IPv4 cada dirección se compone de 32 bits, lo que permitía la existencia de 4300 millones de direcciones únicas. En comparación las direcciones IPv6 [4], las cuales se componen de 128 bits, permiten la existencia de aproximadamente 340 billones de direcciones IP únicas. En la actualidad, muchos servicios como DHCP [5], FTP [6] y SSH [7] requieren del nuevo estándar y que puedan ser ejecutados en este protocolo para su funcionamiento; razón válida para migrar los servicios y demás protocolos que se basaban en IPv4 a IPv6.

Durante esta investigación se revisa la forma cómo los servicios corporativos antes mencionados deben migrar hacia la implementación del protocolo IPV6 y se analizan algunas características de seguridad en autenticación, confidencialidad e integridad de los mismos. El primer protocolo o servicio que debe migrar es DHCP (Dynamic Host Configuration Protocol) [8]-[9] o protocolo dinámico de configuración de *host*, el cual se encarga de brindar direcciones IP a los diferentes equipos conectados a la red de manera dinámica, necesarios para que un sistema pueda comunicarse efectivamente. Su objetivo principal es simplificar la administración de la red [10]. El servicio DHCP para IPv6 está definido en el RFC 3315; trabaja sobre UDP y utiliza la arquitectura cliente-servidor, y además utiliza *multicast* para los mensajes [11]-[12].

El funcionamiento de DHCPv6, empieza en el momento en el que el cliente escucha en el puerto 546 y los transmisores escuchan en el puerto 547. Éstos se comunican por medio de una dirección local y direcciones *multicast* (Fig. 1) [11]-[13].


Fig. 1. DHCPv6.
Fuente: autor

El segundo servicio que busca la implementación hacia IPV6 es el protocolo Secure Shell (SSH), desarrollado por Tatu Ylonen [14] en la Universidad Tecnológica de Helsinki en Finlandia, y OpenSSH [7]-[15] nace del proyecto de un sistema operativo orientado a la seguridad que permite realizar la comunicación y transferencia de información en forma cifrada, proporcionando una fuerte autenticación sobre un medio inseguro. Permite la ejecución de procesos, el inicio de sesiones a servidores, la ejecución de comandos y la copia de archivos remotamente, brindando comunicaciones cifradas entre el cliente y el servidor, evitando así, el robo de información y manteniendo la integridad de los datos que viajan a través de la red [16], como se explica en el RFC de Secure Shell [17]-[18]. Asimismo, proporciona una exhaustiva autenticación y comunicaciones seguras en redes no seguras. Adicionalmente, provee seguridad para conexiones de servicios X Windows y envío seguro de conexiones arbitrarias TCP. En la autentificación puede utilizar algoritmo de cifrado como RSA o DSA [15], y para el envío de datos a través de la red usa 3DES, IDEA y Blowfish [19]-[20].

El tercer servicio, igual de importante, es el protocolo de transferencia de archivos FTP, muy usado en Internet hoy día [21]. Su objetivo es transmitir archivos exitosamente entre máquinas en una red sin que el usuario tenga que iniciar una sesión en el *host* remoto o que requiera tener conocimientos sobre cómo utilizar el sistema remoto. Su funcionamiento consiste en que un equipo o *host* se pueda conectar a un servidor de archivos para descargar, modificar, consultar, eliminar y enviar documentos, independiente del sistema operativo del cliente. Además, permite a los usuarios acceder a archivos en sistemas remotos usando un conjunto de comandos simples, y se describe en el RFC 959 [22]-[23]. Para acceder a los archivos remotos, el usuario debe identificarse al servidor; en este punto, el servidor es responsable de autenticar al cliente antes de permitir la transferencia de archivos.

Desde el punto de vista de un usuario FTP, el enlace está orientado a conexión y es necesario que ambos *hosts* estén activos y ejecutando TCP/IP [24] para establecer una transferencia de archivos muy usado en redes corporativas [25]-[26]. Un problema básico de este servicio es la seguridad, ya que toda la transferencia de archivos con el servidor se realiza en texto plano sin ningún tipo de cifrado, dando así la opción de que un atacante acceda al servicio de archivos, los modifique o los lea sin ningún inconveniente [27].

Finalmente, dentro de los alcances del trabajo se revisa la utilidad del protocolo de seguridad nativo IPsec [28], [29], [30] en IPV6 de *host* a *host* en lugar de que sea de punto a punto, como se hace en IPV4. El encabezado AH [9]-[30] se utiliza para garantizar la integridad y ataques de no repudio; y ESP [30] para la confidencialidad, integridad y anti-replay. Uno de los problemas potenciales de IPsec en IPv6 es que no se puede garantizar su implementación como mecanismo en cualquier escenario. Es conveniente que se

configure de forma manual y se adicione al servidor DHCPv6, que permite tener un control mayor sobre la asignación de direcciones y suministrar otra información, como por ejemplo, dirección del servidor FTP o DNS [13]. Los algoritmos utilizados en la seguridad son MD-5 y SHA-1 [30] definido en RFC 1827[12] y 2406[13]. Se diseñó para proveer confidencialidad, autenticación del origen de datos, integridad sin conexión y servicio contra reenvío de paquetes. En cuanto a los servicios bajo IPV6 [24], éstos se van estandarizando y más dispositivos se actualizan para trabajar con este protocolo; así, nuevas implementaciones de seguridad en la infraestructura serán necesarias.

Esta investigación está dividida en varias secciones. Primero se encuentran los materiales y métodos utilizados durante el estudio; después se establece la metodología aplicada en el análisis y las herramientas utilizadas. Asimismo, se presentan los resultados de cada uno de los servicios y protocolos utilizados. Otro aspecto es la discusión actual en cuanto a la implementación del protocolo IPV6. Finalmente, están las conclusiones y motivaciones de seguridad de los diferentes servicios implementados.

## II. Materiales y Métodos

Los protocolos DHCP, FTP y SSH son servicios de la capa de aplicación. En esta sección se describen las consideraciones y detalles de su implementación y funcionamiento bajo el protocolo IPv6 en diferentes sistemas operativos (Tabla I) y en una red local utilizando diferentes computadores y sistemas operativos, además de la herramienta Wireshark para la captura de tráfico.

La instalación de cada uno de los servicios se efectuó bajo un escenario controlado en laboratorio una vez configurado el servidor con todos los servicios analizados como DHCP, FTP y SSH corriendo sobre el protocolo IPv6 y los clientes bajo el sistema operativo Linux y Windows (Tabla I).

Tabla I. Equipo y Software utilizado

| | |
|---|---|
| Sistema operativo del servidor | Windows Server 2008-2012 R2 Linux Debian 7.7 y Ubuntu |
| Sistema operativo del cliente | Windows 7 con FileZilla 3.10.3. y Ubuntu Gnome 2.26.0 |
| Herramienta de captura de tráfico | Wireshark 1.12.5 |
| PC1 | Lenovo G40 70 |
| PC2 | Toshiba ultrabook S400u |
| Servidor | Sure everon Tp5504 con 7 discos duros de un 1 tera por slot y 48 gigas en RAM |
| Switch | Cisco catalist 2960-24 puertos Fasthernet |
| Router | Cisco 2901 Enterprise puertos gigabit Ethernet |

Fuente: Autor.

La Fig. 2 muestra el escenario sobre el cual se hicieron las respectivas pruebas de implementación y análisis de cada uno de los servicios funcionando bajo IPv6 y teniendo en cuenta el pool de direcciones asignadas bajo DHCPv6 como ámbito de pruebas.

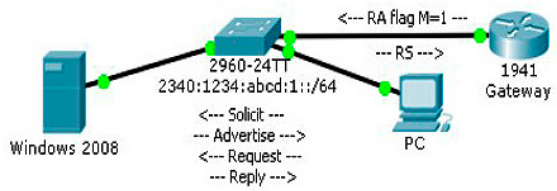


**Fig. 2 Configuración de DHCPv6.**
Fuente: Autor

Para los demás protocolos FTP y SSH se utilizó un escenario muy similar.

## III. Metodología

Durante este análisis se contrastaron algunas políticas de seguridad del protocolo IPv6 en cuanto a autenticación, confidencialidad e integridad usando IPsec como protocolo nativo. Esto se hizo para servicios corporativos como DHCP, FTP y SSH. El procedimiento se efectuó así: se configuró el servidor con el sistema operativo Windows Server 2008 y Server 2012 R2, además, con Linux Debian versión 7.7 y Ubuntu Server, así como con dos máquinas físicas con Windows 7 y Ubuntu para escritorio como clientes. Para el servicio DHCPv6 se configuró el Active Directory y el DNS. Se creó el ámbito para IPv6 el cual se definió a partir del prefijo 2001:db8::1 (Fig. 3), también se asignaron direcciones reservadas o direcciones excluidas y otras opciones como el tiempo de concesión de una dirección asignada y su tiempo de expiración.

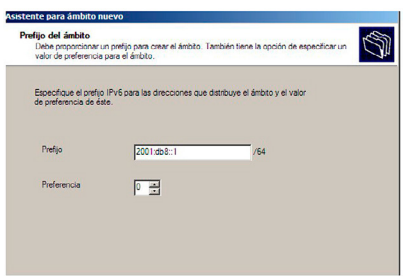


**Fig. 3. Especificación del prefijo de inicio de direcciones IPv6.**
Fuente: Autor

Además, se hizo la conexión de red para todas las máquinas y se realizó la verificación de asignación de direcciones de IPv4 e IPv6 dinámicas y locales en cada una (Fig. 4).

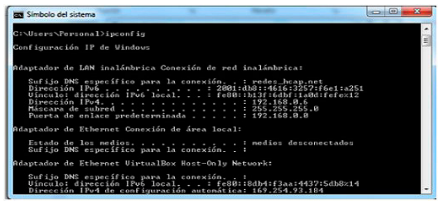


**Fig. 4. Verificación de IPv4 e Ipv6 en el cliente.**
Fuente: Autor.

Para la configuración e implementación del servicio SSH bajo IPv6 en Windows Server 2008 y 2012 R2, así como en Linux Ubuntu y Debian 7.7, se consideran algunas condiciones previas a la conexión, como verificar que las reglas de entrada y salida TCP del firewall de los servidores Windows estén activas, además, se configura una regla de entrada y de salida del protocolo SSH a través del puerto 22 con una configuración estática de las respectivas direcciones IPv6 para efectuar correctamente la captura de los paquetes. Se implementó BitVise SSH Server para hacer uso de SSH sobre IPv6 (Fig. 5), y sobre el cliente se configuró Secure CRT para realizar la conexión respectiva. También se validaron ambos extremos de la conexión con la contraseña de administrador del servidor SSHv6.

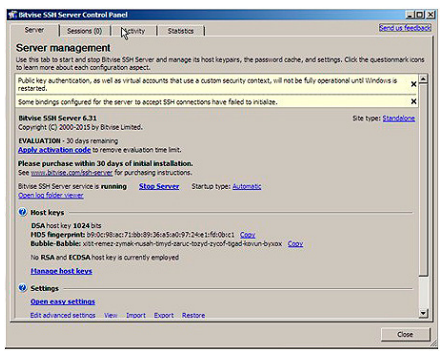


**Fig. 5. Configuración de SSH Server para IPv6.**
Fuente: Autor.

Se pudo destacar y revisar que dentro de los registros de auditoría el servidor SSHv6 (Fig. 6) recibió satisfactoriamente la conexión, y en el lado del cliente, se permitió su acceso remoto.

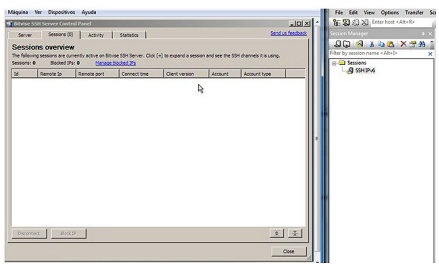


**Fig. 6. Acceso al Server SSH bajo IPv6.**
Fuente: Autor.

Para la configuración del servicio FTP sobre IPv6 se agregó primero el rol de IIS (Internet Information Service) y se pudo activar el servicio FTP; como segunda instancia se creó un sitio al cual se asignó una dirección IP pública para que sea accesible por medio de Internet. Además, se crearon carpetas personalizadas para cada usuario en donde se almacenan todos y cada uno de sus archivos. Se agrega la dirección IPv6 [2001:db8::104] incluyendo los caracteres de paréntesis cuadrados y se especifica el puerto 21 (Fig. 7).

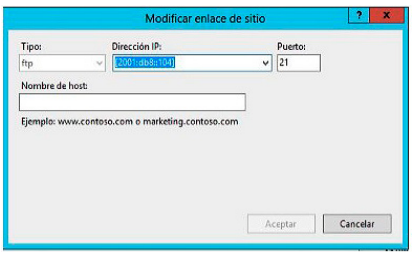


**Fig. 7. Direccionamiento IPv6 para FTP.**
Fuente: Autor.

Para evitar problemas de seguridad se implementa un certificado SSL durante el envío de los datos para que éstos estén cifrados e ilegibles para los atacantes. La seguridad de SSL confirma que la información viaje cifrada y sea totalmente indescifrable (Fig. 8).

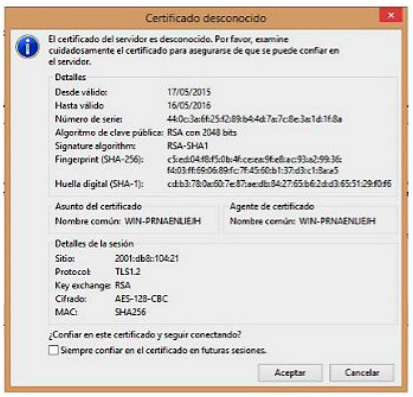


**Fig. 8. Certificado SSL para cliente FTP.**
Fuente: Autor.

Así, el servidor SSHv6 (Fig. 6) ha recibido satisfactoriamente la conexión del cliente, lo que le permite su acceso remoto.

## IV. Resultados

La implementación, configuración de los servicios FTP, DHCP y SSH bajo IPv6, junto con los parámetros de seguridad en cuanto a autenticación, confidencialidad e integridad en cada uno de los sistemas operativos analizados se pueden resumir en la Tabla II.

TABLA II. REVISIÓN DE LA SEGURIDAD EN LOS SERVICIOS IPV6.

| | Server Windows 2008 | | | Server Windows 2012 R2 | | | Server Linux Debian | | | Server Ubuntu | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Servicios | DHCP | FTP | SSH | DHCP | FTP | SSH | DHCP | FTP | SSH | DHCP | FTP | SSH |
| Soporta IPv6 | Sí | Sí | Sí | Sí | Sí | Sí | Sí | Sí | Sí | Sí | Sí | Sí |
| Parámetros de configuración (nivel de dificultad) | Baja | Baja | Baja | Baja | Baja | Baja | Alta | Alta | Alta | Media | Media | Media |
| Soporta IPsec | Sí | Sí | Sí | Sí | Sí | Sí | Sí | Sí | Sí | Sí | Sí | Sí |
| VPN | Sí | Sí | Sí | Sí | Sí | Sí | Sí | Sí | Sí | Sí | Sí | Sí |
| Autenticación clave compartida y certificado digital | RSA/ DSA | RSA/ DSA | RSA/ DSA | RSA/ DSA | RSA/ DSA | RSA/ DSA | RSA/ DSA/ PSK | RSA/ DSA/ PSK | RSA/ DSA/ PSK | RSA/ DSA/ PSK | RSA/ DSA/ PSK | RSA/ DSA/ PSK |
| Confidencialidad entre 56 y 128 bits | DES | DES | 3DES | 3DES | 3DES | 3DES | 3DES/ AES | 3DES/ AES | 3DES/ AES | 3DES/ AES | 3DES/ AES | 3DES/ AES |
| Integridad | MD5 | MD5 | MD5 | MD5 | MD5 | MD5 | MD5/ SHA | MD5/ SHA | MD5/ SHA | MD5/ SHA | MD5/ SHA | MD5/ SHA |

Fuente: Autor.

En la tabla se identifican las mejores condiciones de implementación de DHCP, FTP y SSH bajo IPv6 sobre servidores Linux con algunas ventajas claras frente a Windows en cuanto a la autenticación entre las máquinas físicas, integridad y confidencialidad.

Otro aspecto a destacar es visualizar cada uno de los protocolos implementados como DHCPv6 (Fig. 9). Se refleja aquí cómo el servidor con dirección 2001:db8::1 entrega la dirección IPv6 asignada dinámicamente al cliente, en este caso 2001:db8::4616:3257:f6e1:a251.

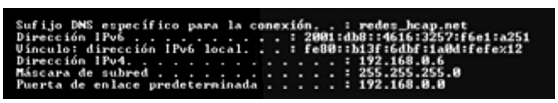


**Fig. 9 Entrega de una IPv6 al cliente por DHCPv6.**
Fuente: Autor.

Para el acceso remoto al servidor usando el servicio SSH mediante direcciones IPv6 se configuró el siguiente escenario controlado (Fig. 10):

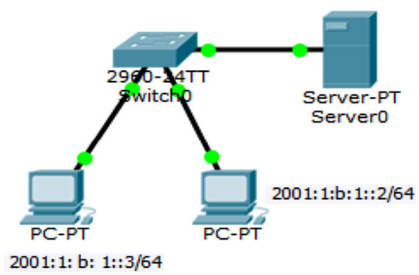


**Fig. 10. Escenario para SSH bajo IPv6.**
Fuente: Autor.

Se utilizó otro tipo de direccionamiento en el server 2001:1:b:1::3 y un cliente 2001:1:b:1::2 (Fig. 11).

Se nota durante los primeros paquetes el intercambio de llaves que realiza SSH al establecer la conexión entre los extremos; en el primer paquete se revisa el cifrado que no permite ver la información. Adicionalmente, TCP hace uso del puerto 22 y su mensaje está cifrado entre las partes (Fig. 12).

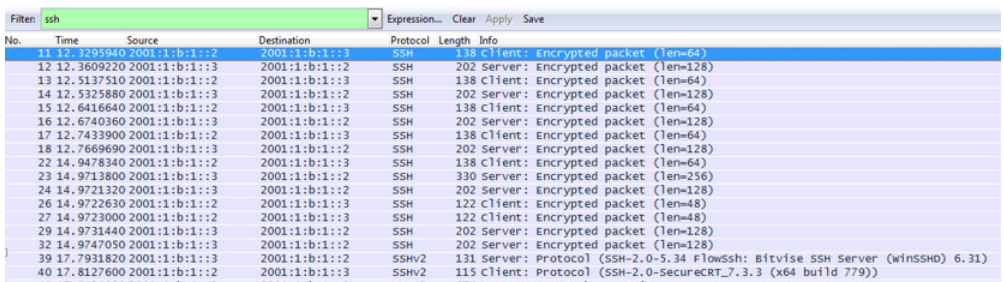


**Fig. 11. Acceso remoto con SSHv2 bajo IPv6.**
Fuente: Autor.

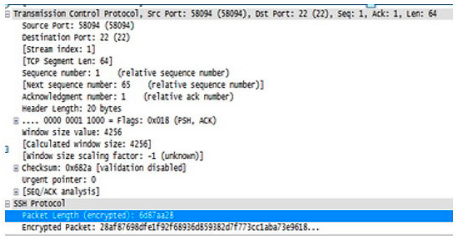


**Fig. 12. Mensaje encriptado entre extremos con IPv6.**
Fuente: Autor.

Sobresale el intercambio de llaves sin contacto previo de Diffie-Hellman [28]-[31] para realizar el intercambio durante la sesión con un paquete de 84 bytes con cifrado AES-256 [29]-[31] sin compresión (Fig. 13). Adicionalmente, el servidor es el que proporciona la respuesta al intercambio de llaves usando la versión de SSH v1, pero rápidamente, antes del primer intercambio de llaves, se realiza el cambio a SSH v2.

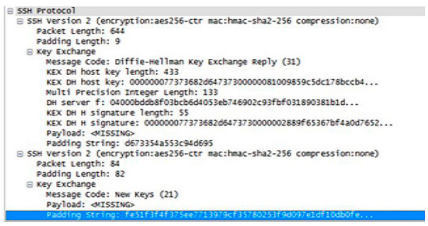


**Fig. 13. Intercambio de claves con SSH para IPv6.**
Fuente: Autor.

La conexión SSH se activa y puede ser terminada por parte tanto del cliente como del servidor (Fig. 14).

En cuanto a la implementación del servicio FTP bajo IPv6, se configuró la red LAN (Fig. 15); en el servidor se configuran usuarios y perfiles para el acceso con la opción de modificar e eliminar archivos de manera segura usando la validación de los puntos mediante IPsec.

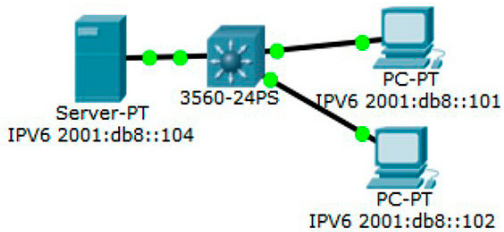


**Fig. 15. Escenario para FTP bajo IPv6.**
Fuente: Autor.

Se adiciona un certificado de seguridad SSL para fortalecer el envío cifrado y que sea oculto para atacantes, esto es obligatorio. También se activó la opción para usar cifrado de 128 bits [13] en estas conexiones. Una vez se activa la sesión FTP bajo IPv6, no permite la lectura del certificado de seguridad. Se pone en evidencia entonces que la información viaja cifrada y totalmente ilegible (Fig. 16).

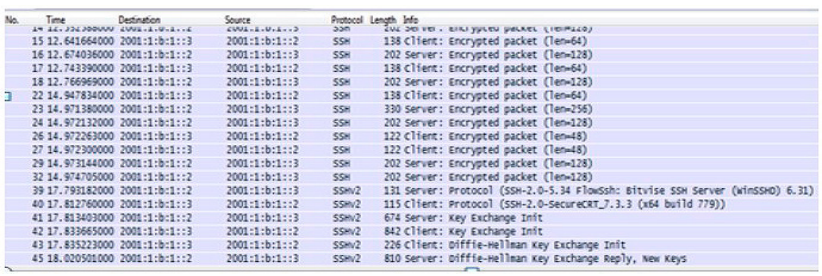


**Fig. 14. Intercambio con SSHv2 en IPv6.**
Fuente: Autor

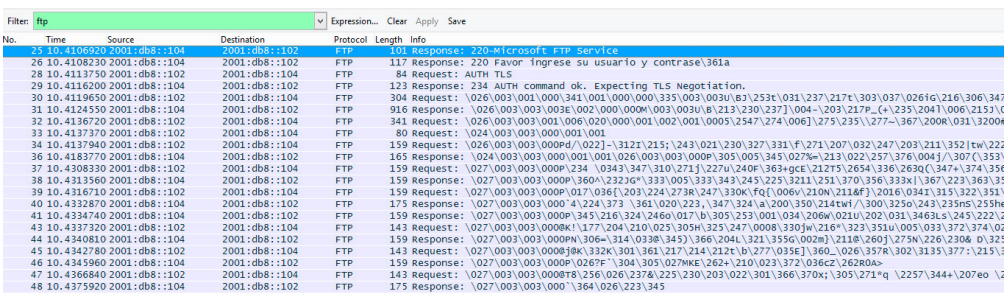


**Fig. 16. Certificado SSL entre el cliente y server IPv6.**
Fuente: Autor.

## V. Discusión

La falta de despliegue del protocolo IPv6 en América Latina y el Caribe se ha demorado por la falta de capacitación del personal encargado en las organizaciones y empresas de Internet de la región, según considera el experto Hans Reyes, coordinador de la Red Nacional Académica de México.

En la actualidad es una realidad que se debe apuntar hacia la implementación de IPv6 como una herramienta clave para lograr un mayor desempeño de las aplicaciones de Internet como DHCP, FTP y SSH entre otras. Según Google en sus estadísticas a 2014, el crecimiento y uso de este protocolo es considerable (Fig. 17).


**Fig. 17. Google uso de direcciones y servicios IPv6.**
Fuente: Autor

El mayor problema que se vislumbra es la falta de personal idóneo para su implementación. Se debe resaltar su importancia y valor para redes en producción y así tener un mayor desempeño en las aplicaciones que ya utilizan el estándar IPv6.

Otro problema es el poco contenido existente bajo IPv6. Proveedores como Google, Facebook, Microsoft y Cisco ya lo soportan en sus redes, sin embargo, se debe sensibilizar a los ISP, gobiernos, empresas y universidades para hacer migración y masificarlo, pues no es sólo un tema de moda, es parte del todo de Internet. Según LACNIC, organismo encargado de la asignación de direcciones IPV6 para América Latina, se refleja el amplio rango de asignaciones IPv6 para la región (Fig.18).

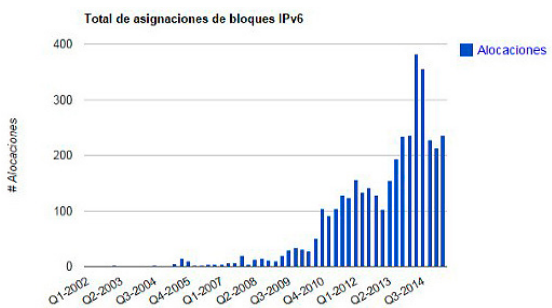


**Fig. 18. Rango de IPv6 en América Latina.**
Fuente: Autor.

Existen diferentes estudios realizados en la implementación de servicios empresariales sobre el protocolo IPv6. Se destaca el análisis de la Universidad Carlos III de Madrid, sobre todo en el campo de la seguridad, concluyendo que pronto existirán ataques exclusivos para IPv6 y para mitigar esto resaltan la importancia del uso de IPsec, que en la actualidad no es muy utilizado [13]. Asimismo, la Universidad de Oriente en Venezuela intentó implementar dentro de su red el protocolo IPV6, dando como conclusión que este tipo de red presenta limitaciones de hardware y software, las cuales no fueron solucionadas por la propia universidad, afectando así la implementación de este protocolo en su red [31].

Los servicios analizados, como el DHCPv6 [31], son una herramienta importante en la administración de redes, al igual que SSH y FTP. Para poder utilizarlos se necesita el conocimiento de sistemas operativos libres como Ubuntu o Debian y propietarios como Windows Server 2008 o 2012 R2, utilizados durante esta investigación, ya que su implementación bajo IPv6 no es un tema exclusivamente de redes, también tiene impacto a nivel de servidores, aplicaciones y dispositivos de seguridad.

## VI. Conclusiones

Es evidente el gran reto durante el diseño e implementación de servicios bajo el protocolo IPv6 para las áreas de tecnología en sectores productivos y académicos, así como para los usuarios de Internet en general. La migración hacia este estándar permite minimizar riesgos de seguridad presentes en su antecesor, el IPv4. Este artículo revisa los mecanismos de configuración de los protocolos DHCP, FTP y SSH, además de su seguridad en los principales sistemas operativos actuales que tienen activado IPv6 por defecto pero no las características de IPsec que le aportan confidencialidad, autenticación e integridad, tanto a los datos como a los usuarios de forma transparente, con la posibilidad de agregar las tradicionales formas de proteger la información que lo hace más robusto y confiable. Por esta razón, es fundamental formar a los administradores de red en el protocolo IPv6 para la aplicación de políticas de seguridad e implementación de nuevos servicios y formas de comunicarse, conscientes de los riesgos que conlleva su utilización y conociendo los mecanismos de seguridad que deben aplicar.

El principal aporte de este trabajo de investigación es el hecho de proveer una solución real y factible para la implementación de los servicios DHCP, SSH y FTP en IPv6; los resultados obtenidos durante las pruebas demuestran que la solución desarrollada es sencilla y funcional e incentiva el uso de estos servicios en un entorno local. Además, presenta una contribución para la comunidad de administradores de redes puesto que se presenta una alternativa sencilla y segura en la asignación de direcciones para el

acceso remoto con este nuevo estándar (siendo altamente escalable), así como para el intercambio de archivos, teniendo como premisa que el proceso será un poco más lento.

Finalmente, la implementación y revisión de la seguridad de los servicios analizados en entornos integrados bajo IPv6 será un proceso continuo en el que diariamente aparecen nuevas vulnerabilidades y riesgos de seguridad. Por ello es importante mantener una buena formación en los protocolos utilizados porque hacia el futuro existirán nuevos riesgos que irán apareciendo a medida que se incremente la utilización del protocolo IPv6. Análisis y estudios como los aquí planteados permiten medidas de protección a las nuevas y versátiles infraestructuras de telecomunicaciones.

## Referencias


[1] R. Bareño Gutiérrez, *Elaboración de un estado de arte sobre el protocolo IPV6; y su implementación sobre protocolos de enrutamiento dinámico como RIPNG, EIGRP y OSPF basado sobre la plataforma de equipos Cisco.* Bucaramanga: Universidad Pontificia Bolivariana, 2011.

[2] W. Lee, S. S. H. Park y C. Lim, "Server authentication for blocking unapproved WOW access," in 2014 International Conference on Big Data and Smart Computing (BIGCOMP), 2014, pp. 155–159. DOI: 10.1109/BIGCOMP.2014.6741427

[3] T. Chown, "IPv6 Campus Transition Experiences," in 2005 Symposium on Applications and the Internet Workshops (SAINT 2005 Workshops), 2005, pp. 46–49. DOI: 10.1109/SAINTW.2005.1619975

[4] I. Beijnum, "An FTP Application Layer Gateway (ALG) for IPv6-to-IPv4 Translation.", 2011. [Online]. Available: https://tools.ietf.org/html/rfc6384

[5] J. C. Becerra Cobos, J. R. Simbaqueva Buitrago y A. F. Valenzuela Suárez, "Diseño e implementación de redes IPv6 en MIPYMES: caso laboratorio de informática," Esc. Colomb. Ing. Julio Garavito, pp. 1–8, 2013.

[6] T. Sanguankotchakorn y M. Somrobru, "Performance Evaluation of IPv6/IPv4 Deployment over Dedicated Data Links," in 2005 5th International Conference on Information Communications & Signal Processing, 2005, pp. 244–248. DOI: 10.1109/ICICS.2005.1689043

[7] F. M. Ángel y J. F. C. Domínguez, "Implementación de servicios IPv6 en la Universidad Autónoma de Guerrero, México," *Vínculos*, vol. 10, no. 2, pp. 393–400, jul. 2014.

[8] B. Stewart, *CCNP BSCI Official Exam Certification Guide*, 4th ed. Cisco Press, 2007.

[9] V. A. Kalusivalingam, "Network Information Service (NIS) Configuration Options for Dynamic Host Configuration Protocol for IPv6 (DHCPv6)," 2004.

[10] A. Carrera Buenaño, "Análisis de las Técnicas de Convivencia entre IPV4 e IPV6 y su Implementación en los Servicios: Web, Mail, FTP, Proxy, DNS y DHCP de la Intranet de la ESPOCH," Escuela Superior Politécnica de Chimborazo, 2009.

[11] J. Bound, "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)," 2003.

[12] T. Chown, S. Venaas y C. Strauf, "Dynamic Host Configuration Protocol (DHCP): IPv4 and IPv6 Dual-Stack Issues," 2006.

[13] R. A. Reina Valladares, G. A. Peláez Brioso y L. A. Gurris Aragón, "Metodología de Implementación de Ipv6 en La Red de La Universidad de Oriente," *Ing. Electrónica, Automática y Común.*, vol. 29, no. 1, pp. 36–43, jul. 2010. DOI: 10.1234/rielac.v29i1.15

[14] C. Ellison, B. Frantz, B. Lampson, R. Rivest, B. Thomas y T. Ylonen, SPKI certificate theory (No. RFC 2693), 1999. [Online]. Available: https://tools.ietf.org/html/rfc2693

[15] L. P. Aguirre, F. González y D. Mejía, "Aplicaciones de MPLS, transición de IPv4 a IPv6 y mejores prácticas de seguridad para el ISP Telconet," *Rev. Politéc.*, vol. 32, 31 jul de 2013.

[16] S. E. Abasolo Aranda y M. A. Carrera Paz y Miño, "Evaluación del modelo de referencia de Internet of things (IoT), mediante la implantación de arquitecturas basadas en plataformas comerciales, open hardware y conectividad IPv6," *Univ. Las Fuerzas Armadas ESPE*, ene. 2014.

[17] F. Gont, "Security Implications of IPv6 on IPv4 Networks," 2014. [Online]. Available: https://tools.ietf.org/html/rfc7123

[18] T. Ylonen y C. Lonvick. "The secure shell (SSH) connection protocol." 2006. [Online]. Available: https://tools.ietf.org/html/rfc4253

[19] O. E. Motta Barrera and R. Peláez Negro, "De la planeación de TIC a la implementación de IPv6 un escenario deseado para desarrollar el 'Internet de las cosas' en la Universidad de Ibagué Colombia." Red CLARA (Cooperación Latino Americana de Redes Avanzadas, 10-Dec-2011.

[20] A. P. Santamaría Alamar, "Análisis, diseño e implementación de una red prototipo utilizando el protocolo IPv6 y QoS para la empresa Santanet," [Tesis de maestría], Depto. Ing. Univ. Politéc. Sales., Ecuador, 2014.

[21] F. R. Flores Calahorrano, "Análisis y emulación de Multihoming y de la publicación al internet de servicios web, transferencia de archivos y correo a través de una red IPV6," [Tesis de maestría], Depto. Ing. Univ. Politéc. Sales., Ecuador, 2014.

[22] M. H. Warfield, Security implications of IPv6. Internet Security Systems, 2003.

[23] F. Baker, X. Li, C. Bao, and K. Yin, "Framework for IPv4/IPv6 Translation," Internet Engineering Task Force (IETF), 2011. [Online]. Available: https://tools.ietf.org/html/rfc6144.

[24] J. P. Martínez. *IPv6 para Todos: Guía de uso y aplicación para diversos entornos*, 2009.

[25] G. U. O. Jian. "Model of FTP server based on spring framework in IPv6 and it's implementation [J]." *Computer Eng. and Design* 19, 2008.

[26] M. Allman y S. Ostermann, "FTP Security Considerations," 1991. [Online]. Available: https://tools.ietf.org/html/rfc2577

[27] W. Zheng, S. Liu, Z. Liu y Q. Fu. "Security transmission of FTP data based on IPsec," In 2009 1st IEEE Symposium on Web Society, pp. 205-208, 2009. DOI: 10.1109/SWS.2009.5271783

[28] R. Atkinson y S. Kent, "IP Encapsulating Security Payload (ESP)",1998. [Online]. Available: https://tools.ietf.org/html/rfc2406

[29] S. Kent, "IP Authentication Header", 2005. [Online]. Available: https://tools.ietf.org/html/rfc4302

[30] C. García Martín, "Análisis de seguridad en redes IPv6," Universidad Carlos III de Madrid, [Tesis de mestría], Dept. Ing. Telem. Univ. Carlos III de Madrid, Getafe, España, 2012.

[31] T. Mrugalski y D. Hankins, "Dynamic Host Configuration Protocol for IPv6 (DHCPv6) Option for Dual-Stack Lite", 2011.[Online]. Available: https://tools.ietf.org/html/rfc6334