# *Fundamentos de Forense en Red*

## Enfoque dado a Redes IPv6

**Wendy Tatiana Rincón Correal**
Esp. Seguridad Informática Cohorte 14
Universidad Piloto de Colombia
Bogotá D.C

**Jesús Alexander Botero Torres**
Esp. Seguridad Informática Cohorte 14
Universidad Piloto de Colombia
Bogotá D.C

***ABSTRACT***

**This article aims to provide some concepts of this new version, the new protocols and other features that should be taken into account when performing a network forensics.**

**It is a brief outline of the major changes in some of the protocols that support and interact with the Internet Protocol. It is not intended to be thoroughly but a reference to some of the major changes and technical documents that support this change**.

***Palabras Clave:*** **IP, formato, protocolo**

### I. INTRUDCCIÓN

Con este artículo se pretende ofrecer algunos conceptos de esta nueva versión, los nuevos protocolos y demás características que deben ser tenidas en cuenta a la hora de realizar un análisis forense en red.

Es un breve bosquejo de los principales cambios de algunos de los protocolos que se apoyan e interactúan con el protocolo de internet. No se pretende realizar un análisis profundo sino una referencia de algunos cambios y de los principales documentos técnicos que soportan este cambio.

### II. IPv4

Cuando utilizamos Internet para cualquier actividad, ya sea correo electrónico, navegación web, descarga de ficheros, o cualquier otro servicio o aplicación, la comunicación entre los diferentes elementos de la red y nuestro propio ordenador o teléfono, utiliza un protocolo que denominamos Protocolo de Internet (IP, Internet Protocol) [1].

Para que los dispositivos se conecten a la red, necesitan una dirección IP. Cuando se diseñó IPv4, casi como un experimento, no se pensó que pudiera tener tanto éxito comercial, y dado que sólo dispone de 2^32 direcciones (direcciones con una longitud de 32 bits, es decir, 4.294.967.296 direcciones), junto con el imparable crecimiento de usuarios y dispositivos, implica que en pocos meses estas direcciones se agotarán.

Por este motivo, y previendo la situación, el organismo que se encarga de la estandarización de los protocolos de Internet (IETF, Internet Engineering Task Force), ha trabajado en los últimos años en una nueva versión del Protocolo de Internet, concretamente la versión 6 (IPv6), que posee direcciones con una longitud de 128 bits, es decir 2^128 posibles direcciones (340.282.366.920.938.463.463.374.607.431.768.211.456), o dicho de otro modo, 340 sextillones.

El despliegue de IPv6 se irá realizando gradualmente, en una coexistencia ordenada con IPv4, al que irá desplazando a medida que dispositivos de cliente, equipos de red, aplicaciones, contenidos y servicios se vayan adaptando a la nueva versión del protocolo de Internet.

.

### III. IPv6

La versión 6 de IP, diseñado para coexistir con IPv4 durante una fase de transición, hasta que de forma transparente, IPv4 deje de utilizarse y desaparezca de la red.

Una dirección IPv6 tiene un tamaño de 128 bits y se compone de ocho campos de 16 bits, cada uno de ellos unido por dos puntos. Cada campo debe contener un número hexadecimal, a diferencia de la notación decimal con puntos de las direcciones IPv4. En la figura siguiente, las equis representan números hexadecimales [2].

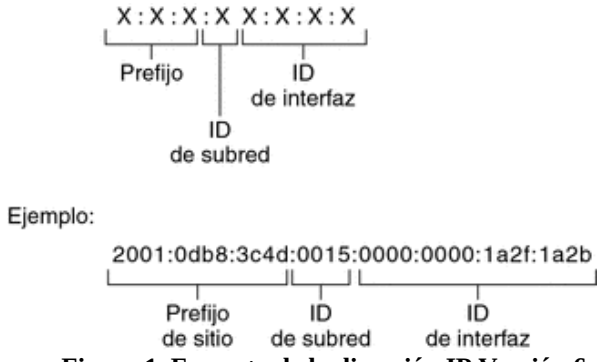


**Figura 1. Formato de la dirección IP Versión 6**

Los tres campos que están más a la izquierda (48 bits) contienen el **prefijo de sitio**. El prefijo describe la **topología pública** que el ISP o el RIR (Regional Internet Registry, Registro Regional de Internet) suelen asignar al sitio.

El campo siguiente lo ocupa el **ID de subred** de 16 bits que usted (u otro administrador) asigna al sitio. El ID de subred describe la **topología privada**, denominada también **topología del sitio**, porque es interna del sitio.

Los cuatro campos situados más a la derecha (64 bits) contienen el **ID de interfaz**, también denominado **token.** El ID de interfaz se configura automáticamente desde la dirección MAC de interfaz o manualmente en formato EUI-64.

Este nuevo formato en la dirección IP es muy importante que sea tenido por el analista de red, ya que el mismo contiene bastante información tanto del ISP, posible arquitectura y host de una manera resumida en la dirección. Adicional con el uso de la versión 6 supondría que se dejaría a un lado el uso de NAT y proxys; permitiendo así una mejor identificación de pistas de los posibles violadores de la seguridad de red o participando en opciones de mejora de la arquitectura de red actual.

## IV. CARACTERÍSTICAS DE LA IPV6

Quizás las principales características de la IPv6 se sintetizan en el mayor espacio de direccionamiento, seguridad, autoconfiguración y movilidad. Pero también hay otras que son importantes mencionar[3]:

- Infraestructura de direcciones y enrutamiento eficaz y jerárquica.
- Mejora de compatibilidad para Calidad de Servicio (QoS) y Clase de Servicio (CoS).
- Multicast: envío de un mismo paquete a un grupo de receptores.
- Anycast: envío de un paquete a un receptor dentro de un grupo.
- Movilidad: una de las características obligatorias de IPv6 es la posibilidad de conexión y desconexión de nuestro ordenador de redes IPv6 y, por tanto, el poder viajar con él sin necesitar otra aplicación que nos permita que ese enchufe/desenchufe se pueda hacer directamente.
- Seguridad Integrada (IPsec): IPv6 incluye IPsec, que permite autenticación y encriptación del propio protocolo base, de forma que todas las aplicaciones se pueden beneficiar de ello.
- Capacidad de ampliación.
- Calidad del servicio.
- Velocidad.

Seguridad IP o IPsec, Proporciona servicios interoperables de alta calidad y de seguridad de forma criptográfica para el tráfico en la capa IP, para la versión 4 del protocolo IP era opcional, pero en la versión 6 se ha vuelto obligatoria. Adicional IPsec mejora el protocolo IP original, proporcionando la autenticidad, integridad, confidencialidad y control de acceso a cada paquete de IP mediante el uso de dos protocolos como es AH (encabezado de autenticación) y ESP (carga útil de seguridad de encapsulación).

Cabe aclarar que el cambio no solo fue del protocolo de internet (IP), sino de los demás protocolos complementarios que son necesario en la comunicación con las demás capas del modelo OSI y/o para el control de la comunicación. En ese orden de ideas se generaron versiones compatibles con la versión 6 del protoclo IP como el de Internet Control Message Protocol (ICMP) version 6, Routing Information Protocol NextGeneration (RIPng), Open Shortest Path First (OSPF) version 3, 6in4 y Generic Routing Encapsulation (GRE).

Es importante resaltar el surgimiento del ICMP versión 6 como apoyo fundamental para el protocolo IP versión 6, ya que se utiliza para enviar mensajes informales y de error, para la resolución de los datos dirección de capa de enlace de nodos vecinos y de dirección sin estado de Auto-Configuración. Estos mensajes utilizan un espacio mínimo pero utilizan la unidad máxima de transferencia (MTU ) en IPv6 la cual es de es de 1280 bytes, lo que permite que puede ser usado de manera mal intencionada para trasportar información (generando un canal para la extracción de información o de denegación de servicio).

Adicional el protocolo ICMP versión 6 es usado para descubrir la dirección de la capa de enlace de datos de nodos vecinos, este proceso se denomina llama Descubrimiento Vecino (ND) y es el par de Protocolo de Resolución de Direcciones (ARP) en IP versión 4. Cabe resaltar que ND posee la misma vulnerabilidad de ARP con respecto al ataque por ARP Spoofing.

El Sistema de Resolución de Nombres de Domino (DNS) también fue actualizado para aceptar el cambio de versión del protocolo de internet, ya que fue necesario crear un registro de recursos AAAA para registros IPv6. Este tipo de registros son atacados al igual que los de IPv4

El protocolo de configuración dinámica de host (DHCP) es totalmente nuevo y no compatible con su par de la versión de IPv4. Se puede trabajar con un servidor que contenga estas dos versiones y de esta manera puede entregar dirección dependiendo el tipo de petición que realiza el host.

Dentro del análisis forense se puede inferir que la mayoría de ingenieros que realizan este tipo de tareas, están bastante familiarizados con la topología de los protocolos de versión IP v4. Esto conlleva a que no se tengan nociones de los cambios de estructura de las nuevas versiones de los protocolos; adicional no se ha tenido en cuenta esto para el hardeninig de los servidores y PCs, los cuales quedan con la opción habilitada de direccionamiento IPV6; lo que conlleva a tener

potenciales vulnerabilidades y/o ataques a los host por desconocimiento.

Con este artículo se pretende dar una pequeña perspectiva de los cambios de los protocolos y de la importancia de que se genere la actualización respectiva a los ingenieros de red y analistas forenses en red, ya que el desconocimiento a la hora de realiza un captura de red puede entorpecer o ralentizar las investigaciones forenses.

A continuación referenciamos los documentos técnicos a los cuales se hace referencia cada uno de los nuevos protocolos versión 6.

- IP versión 6:

RFC 2460 Definición del protocolo
RFC 4291Estandarización de la arquitectura

- ICMP Versión 6

RFC 443 Especificaciones para ICMP ver 6 para IPver 6

- RIPng (Protocolo de de Información de Enrutamiento de Nueva Generación)

RFC 2080 Detalles del Protocolo de nueva Generación.

- OSPF Ver 3 (Protocolo de Enrutamiento de Estado del Enlace Versión 3)

RFC 5340 Detalles del Protocolo de nueva Generación.

- 6 en 4

RFC 4213 Detalles del mecanismo de encapsulación de IPv6 en IPv4

- DHCP Ver 6

RFC 3315 Define el protocolo DHCP versión 6

- DNS

RFC 3901 Relaciona una red con tráfico mixto IPv4 e IPv6

## V. MECANISMO DE TRANSICION DE IPv6

En este punto se pretende detallar el mecanismo 6 en 4, ya que es uno de los más usados para encapsular IPv6 en las redes actuales IPv4, [4] dado que todos los ISPs, hoy en dia, dispone de IPv6 en sus redes, es necesario utilizar lo que denominamos mecanismos de transición y coexistencia

Básicamente, estos mecanismos, permiten que IPv4 e IPv6 coexistan, e incluso que cuando IPv6 no está disponible en forma "nativa", se puede utilizar IPv6 a través de la red IPv4, fundamentalmente mediante lo que denominamos "túneles".

Los mecanismos de túneles, se ocupan de que IPv6 sea "empaquetado" o "encapsulado", dentro de los paquetes IPv4. Los siguientes gráficos permite visualizar como funcionan estos túneles y como se "empaqueta" IPv6 en IPV4

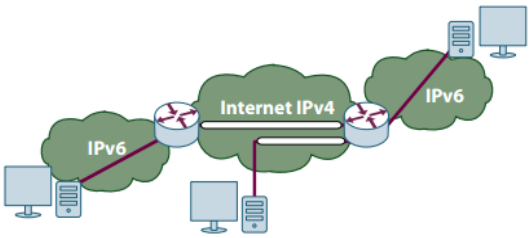


**Figura 2: Túneles IPv6 en IPv4**


**Figura 3. Encapsulado de IPv6 en IPv4**

Hay muchos mecanismos de transición y se trata de un tema sumamente complejo por lo que este apartado, se centra solo en aquellos mecanismos de túneles que consideremos más útiles, y que se denominan túneles automáticos y más concretamente en los denominados 6to4 y teredo.

6to4 se lo funciona cuando se dispone de direcciones IPv4 públicas, por ejemplo, cuando un ordenador está conectado a una red ADSL mediante un modem USB. En este caso, lo que ocurre es que utiliza la dirección IPv4 para configurar automáticamente una dirección IPv6 y un túnel automático.

Teredo (Mirado en sistemas Linux,BSD y Mac OS X) en cambio, funciona con direcciones IPv4 privadas, es decir detrás de los denominados NAT, es decir, por ejemplo, cuando una conexión a una red ADSL se realiza mediante un enrutador en lugar de un modem. De forma parecida al caso de 6to4, se genera de forma automática una dirección IPv6 para cada ordenador conectado a dicho en caminador/NAT, y de igual modo, se utiliza IPv6 a través de la red de IPv4.

Dado que estamos hablando de mecanismo de transición automática, generalmente no se requiere configuración alguna y el sistema operativo se ocupara automáticamente, de detectar si existe conectividad IPv6 en la red.

## VI. EJEMPLO DE VULNERABILIDADES DE IPV6

Vulnerabilidades que usan el campo 'Flow Label':

La etiqueta de "Flow Label" sirve para dar un tratamiento diferenciado a los flujos de datos que recorre una red por medio de IPv6, éste comportamiento de la red puede ser usado por competidores y personas mal intencionadas para obtener un mejor servicio, o en un extremo la denegación de servicio del tráfico que nos pertenece al inyectar paquetes con direcciones IPv6 falsas o etiquetas "Flow Label" adulteradas [4].

Además una de las desventajas que se presenta en una red IPv6 es que las cabeceras de los paquetes que pasan por los nodos intermedios no se verifican, por lo que no existe garantía que éstos datos sean confiables, por lo que la red confía en que estos datos son tan confiables como los nodos que originan éste tráfico.

Vulnerabilidad por IPv6 en paquetes RA (Router Advertisement)

- Para Windows XP no se han identificado ningún tipo de vulnerabilidad dado a que IPv6 no es soportado por el sistema operativo, por esto el sistema lo que hace es ignorar este tipo de trafico

- Para Windows 7, cuando se recibe el ataque, se incrementa en su totalidad el uso del procesador del equipo, si se detiene el ataque de igual forma queda la carga y rendimiento permanentemente, afectando requerimientos como el apagado forzado, además el equipo queda sin navegación y comunicación de red, además de quedar virtualmente muerto

El escaneo de puertos es el más común, este permite "Black-hats" es usado para escuchar a determinados servicios de los puertos, puede definirse como na vulnerabilidad en las redes de IPv6, subredes de 64 bits de uso para la asignación de direcciones de host, los atacantes aprovechan debilidades para superar los firewalls del protocolo.

Otra de las vulnerabilidades mas comunes en IPv6, es cuando asigna múltiples direcciones a una interfaz que desafía las reglas de filtrado en las listas de control de acceso del firewall [5] En tales casos, un firewall tendrá que aprender todas las direcciones de forma dinámica y las reglas de filtrado deberá ser automáticamente generable utilizando sofisticados conjuntos de reglas de política. Y tales capacidades no son disponible [6]

Si tenemos en cuenta las formas de una red en IPv4 o IPv6 puede verse comprometidas, hay muchas similitudes, Los ataques contra las redes suelen caer dentro de uno de los siguientes ataques más comunes [7],[8],[9].

- Internet (DMZ, Páginas web, pop-ups)
- Sniffing, header manipulation, session hijacking, man-in-the middle.
- Buffer overflows, SQL injection, cross-site scripting.
- Email (attachments, phishing, hoaxes)
- Worms, viruses, distributed denial of service (DDoS)
- Macros, Trojan horses, spyware, malware, key
- Loggers
    - VPN, business-to-business (B2B)
    - Chat, peer-to-peer (P2P)
- Malicious insider, physical security, rogue devices, dumpster diving.

Como se pudo observar anteriormente, es importante para considerar que IPv6 no es necesariamente más seguro que IPv4, de hecho el enfoque de IPv6 a la seguridad sea solo ligeramente mejor que IPv4 pero no funcionalmente nuevo.

## VII. CONCLUSIONES

Tener en cuenta los siguientes aspectos de la seguridad de tráfico de IPv6:

- Protection host from scanning and attacking
- Preteccion de los parquets IPv6
- Protección y control del tráfico e intercambio con internet
- Prevención en los sistemas ( Firewall y detección)

Sin embargo, dado a que IPv6/v4 son protocolos de capa de red, muchas de las vulnerabilidades de capa de red, por tanto, son similares.

La protección es requerida por cada dispositivo que está participando en la comunicación de red. Así, IPSec debe ser considerado más en serio para proporcionar la necesaria autenticación, integridad y confidencialidad de los servicios

## REFERENCIAS


[1] Ministerio de Tecnologías de la Información y las Comunicaciones, Bogotá, Colombia, 05 de Febrero 2013, http://ipv6.renata.edu.co/index.php/introduccion.html

[2] http://docs.oracle.com/cd/E19957-01/820-2981/ipv6-overview-10/index.html

[3] http://www.consulintel.es/pdf/ipv6paratodos.pdf

[4] J.Cesar Hidalgo, Sebastian Jaramillo, Seguridad de IPversion 6, Vulnerabilidades sobre tramas y protocolos, http://www.supertel.gob.ec/pdf/Consideraciones%20de%20Seguridad%20para%20Implementacion%20de%20IPv6%20FA.pdf

[5] Choudhary, A. R. Sekelsky, A. 2010. Securing IPv6 Network Infrastructure: a New Security Model. IEEE Conference, USA

[6] Yoo, H. S. Cagalaban, G. A. Kim, S. H. 2009, A Study on the Connectivity of IPv6 to IPv4 Domains and Its Security Issues, International Journal of Advanced Science and Technology, Vol. 10, Korea.

[7] Sotillo, S. 2006. IPv6 Security Issues. East Carolina University, USA

[8] Hauser, V. 2008. Attacking the IPv6 Protocol Suite, The Hacker's Choice, http://www.thc.org/thc-ipv6.

[9] Roman Ammann. Network Forensic Readiness:A Bottom-up Approach for IPv6 Networks. 2012. http://aut.researchgateway.ac.nz/bitstream/handle/10292/4605/AmmannR.pdf?sequence=3