Revista Nexos Científicos *ISSN: 2773-7489*
Enero –Junio 2019 pp. 12-29 *Correo: editor@istvidanueva.edu.ec*
Volumen 3, Número 1 *URL: http://nexoscientificos.vidanueva.edu.ec/index.php/ojs/index*
Fecha de recepción: febrero 2019 *Fecha de aceptación: abril 2019*

Coexistencia de IPv4 con IPv6 a través del protocolo BGP

Aguas Luis [1]

[1] *Universidad Tecnológica Israel-Departamento de Ciencias de la Ingeniería –Carrera de Sistemas, Quito, Ecuador, aguaszoft@outlook.es*

Resumen: En la actualidad IPv6 se está implementando lentamente en redes y coexistirá con IPv4 hasta que se produzca una transición hacia IPv6 (una transición que probablemente demore varios años). Si bien el trabajo técnico relacionado con el protocolo, en gran medida, se ha completado, lo que resta es el usoSi bien la conciencia y la implementación de IPv6 están aumentando, muchas organizaciones, del sector público o privado, están adoptando la estrategia que consiste en "esperar a ver qué sucede", a veces junto con "soluciones alternativas" tácticas, como la Traducción de Direcciones de Red (NAT), diseñada para prolongar la viabilidad de la fuente actual de recursos IPv4. La Internet Society no cree que estas estrategias sean viables en el largo plazo: en última instancia, IPv6 es necesario para la continuidad, la estabilidad y la evolución de Internet.

Palabras clave: tecnología, redes, túneles, información.

Coexistence of IPv4 with IPv6 via BGP protocol

Abstract: IPv6 is currently being slowly deployed to networks and will coexist with IPv4 until a transition to IPv6 (a transition that is likely to take several years). While technical work related to the protocol has largely been completed, what remains the useWhile the awareness and implementation of IPv6 are increasing, many organizations, in the public or private sector, are adopting the strategy that It consists of "waiting to see what happens", sometimes along with tactical "alternative solutions", such as Network Address Translation (NAT), designed to prolong the viability of the current source of IPv4 resources. The Internet Society does not believe that these strategies are feasible in the long run: IPv6 is ultimately necessary for the continuity, stability and evolution of the Internet.

Keywords: technology, networks, tunnels, information.

1. INTRODUCCIÓN

Es de dominio público que para aprender a andar en bicicleta es necesario subirse a la bicicleta y empezar a pedalear, normalmente alguien nos sostiene los primeros metros. Adictos, L. (s.f.)
La idea no es muy diferente con las tecnologías nuevas, ¡hay que subirse y pedalear! y sobre el tema de IPv6 la enorme mayoría de iniciativas siguen enfrascadas en la fase de leer el manual de la bicicleta, estudiar el sistema de cambios o a conocer y admirar a las personas que la diseñaron y del porqué es mejor que andar a pie. Aguas Bucheli, L. F. (2014).
Claro, por tratarse de un tema eminentemente tecnológico, hará falta un estudio científico sobre las bases y conceptos sobre las que se fundamenta y obviamente, sobre la tecnología que pretende reemplazar también; pero sólo lo necesario para saber dónde poner los pies, cómo tomar el manubrio y las nociones de funcionamiento, lo elemental para arrancar y avanzar. BIEEC. (s.f.). DSPACE EPN

En la analogía de la bicicleta, gran parte de la batalla es perderle el miedo y con mi propuesta busco

[1] Magíster en Redes de Comunicaciones, aguaszoft@outlook.es

fundamentalmente esto, que de una manera simplificada la gente empiece a conocer y más que nada a adoptar IPv6 en su uso diario y darse cuenta de que no es una tecnología sólo para gurús o especialistas, que es algo que tarde o temprano deberemos adoptar, que se puede hacer de formas sencillas y qué mejor si empezamos de una vez a perderle el miedo y a pedalear sobre IPv6. Chile, I. (s.f.)

Dada la evidente contratación del aumento del ancho de banda con el CEDIA para nuestro laboratorio, debemos incorporarnos analizando y planteando alternativas prácticas y viables de solución para la implementación de IPv6 en equipos y redes. Dhobsd. (s.f.)

2. METODOLOGÍA

2.1.TÚNELES

Es una realidad que en estos momentos estamos en un proceso de transición y muchos proveedores de internet todavía no están preparados para asignar IPv6 a los usuarios finales, sean estas empresas o usuarios home. Core, N. (s.f.)

Esto nos puede estar retrasando en el proceso de implementación de IPv6 en nuestras redes, ya sea porque el usuario desconoce cómo funciona IPv6, cómo se configuran servicios en IPv6 y por tanto el usuario tiene un temor natural al cambio, a algo que no conoce. Electric, H. (s.f.)

La idea detrás de los túneles IPv6 es simple en principio, y consiste en encapsular todo el tráfico IPv6 que vaya saliendo desde mi equipo o mi red en paquetes IPv4. Y enviar estos paquetes IPv4 hacia un proveedor de túnel IPv6 que una vez que lo reciba, lo des encapsula, obteniendo lógicamente el paquete IPv6 original, y procederá a enrutar estos paquetes IPv6 por la red IPv6 que él sí tiene.

Los paquetes que regresan como respuesta a mi red, irán primero hacia este proveedor, pues los servidores remotos enviarán las respuestas a este proveedor de túnel, y entonces el proveedor realizará la función inversa que será la de encapsular este paquete IPv6 de respuesta en un paquete IPv4 y enviar estos paquetes IPv4 hacia mi equipo o red, donde nuevamente serán desencapsulados y entregados a los servicios que están haciendo uso de IPv6.

2.1.1. VENTAJAS DEL USO DE TÚNELES

Usar un túnel nos permitirá acceder a redes IPv6 aun cuando nuestro proveedor no tenga o no ofrezca IPv6 hacia nuestra red o nuestros equipos.

Esto nos permitirá ir avanzando en la configuración de IPv6 en nuestra red, pues además los proveedores de túneles normalmente nos asignan un rango de IPv6 fijas, lo que nos permitiría utilizarles para cualquier actividad de producción que requiramos como por ejemplo tener un servidor web, de correo, etc. Electrónica, A. (2012)

El día que el proveedor de internet nuestro decida comenzar a distribuir IPv6 hacia nuestra red, pues simplemente podemos agradecer al proveedor de túnel por su labor, y apagar el túnel. Lógicamente primero deberíamos mover todos los servicios hacia la nueva IP. Pensemos que sería como mismo se hace cuando uno se está cambiando de proveedor de internet: tiene que cambiar de IP en los equipos y luego dejar al viejo proveedor. Gont, F. (s.f.)

Sólo que en este caso en IPv6 es realmente rápida la asignación de IPS a través del protocolo IPv6, por lo que un cambio sería realmente rápido.

Además que podemos mantener la IP del túnel por el tiempo que requiramos. Esto es: podríamos mantener la IPv6 del proveedor del túnel y la IPv6 del proveedor por todo el tiempo que requiramos para completar el cambio. Así que no sería complicado el cambio. Savinov, P. (2012)

2.1.2. DESVENTAJAS DEL USO DEL TÚNEL

Los túneles no son la panacea, lamentablemente el proceso de encapsular y desencapsular los paquetes harán que el tráfico IPv6 se perciba quizá un pequeño porcentaje más lento.

También recuerda que si queremos hablar por IPv6 con un sitio que está digamos aquí en Ecuador,

como no tenemos IPv6 de un proveedor local sino de un proveedor en EEUU posiblemente. Este paquete IPv6 encapsulado primero tendría que ir a EEUU y luego regresar desencapsulado hacia el servidor local en Ecuador.

También al usar este túnel, tenemos que competir por el canal de entrada del proveedor de túnel sea cual sea el destino al que vamos a ir; por lo tanto si el proveedor de túnel tiene un inconveniente, congestionamiento, etc, la navegación por IPv6 se percibiría más lenta.

Sin embargo debemos concluir afirmando que antes la ausencia de un proveedor que nos asigne IPv6 localmente en el país, es una de las alternativas más adecuadas para comenzar nuestro proceso de aprendizaje, migración y puesta en producción de nuestros servicios en IPv6.

2.1.3. PREFIJOS ASIGNADOS POR LOS PROVEEDORES DE TÚNELES

Un proveedor de túnel normalmente asigna un prefijo /64, que es lo sugerido para conectar equipos standalone a la red IPv6 o para conectar una red IP a IPv6. Por tanto para realizar esta labor de conectar pequeñas redes o equipos a la red IPv6, es suficiente con el prefijo /64 (2^64 ips disponibles).

Por ejemplo ellos asignarán una IP así:
2001:05c0:1000:000b:0000:0000:0000:b9d3,

Lógicamente podríamos reducirla eliminando todos los 0 intermedios quedando así:
2001:5c0:1000:b::b9d3

Esta sería una IP /64 pero solamente ***usaríamos esta IP para nuestra WAN***, para nuestra conexión IPv6 a internet.

La IP del gateway de esta WAN, que estaría de su lado, sería en este ejemplo:
2001:5c0:1000:b::b9d2

Por tanto a partir de que me asignen una IPv6 en el túnel, yo ya podría comenzar a navegar desde este equipo por la red IPv6, pero no solamente esto, sino que podría incluso publicar ya hasta mi sitio web para que se vea desde la red IPv6 con esta IP; siempre y cuando mi proveedor de tunel me garantice que esta será mi IP y que no cambiará.
Sin embargo, en caso de requerirlo te pueden asignar un /56 o un /48 incluso.

2.2. DUAL STACK O DOBLE PILA

Es el método propuesto originalmente para tener una transición suave hacia IPv6. En este caso se necesita contar con suficiente cantidad de direcciones IPv4 para poder desplegar las dos versiones del protocolo en simultáneo en toda la red.

2.3.TÚNELES / ENCAPSULAMIENTO

Es uno de los mecanismos más antiguos para poder atravesar redes que no tienen soporte nativo del protocolo que se está utilizando. En general se utilizan túneles encapsulando IPv6 dentro de IPv4, permitiendo de esta forma atravesar redes que no manejan IPv6, pero también podemos encontrar la situación inversa. Smith, R. (2013).
Los paquetes originales son transportados hasta un punto de la red por medio del protocolo original, luego encapsulados para atravesar la porción de red que no lo soporta y luego des-encapsulados en el otro extremo para ser enviados al destino final en forma nativa.

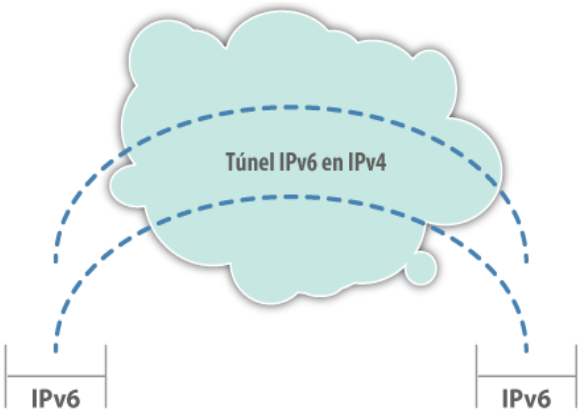

Ilustración 1: Tuneles IPv6 en IPv4, (Chile, s.f.)

Los túneles más habituales son los túneles manuales y los túneles automáticos. Los túneles manuales se deben configurar explícitamente en algún equipo de

la red, mientras que los automáticos se configuran automáticamente en algunos sistemas operativos. En el caso de los primeros, podemos citar los túneles manuales entre dos equipos o mediante "tunnel brokers" como GoGo6 o el de Hurricane Electric. En el segundo caso, los más conocidos son 6to4 y Teredo. Techtectology. (s.f.)

Dentro de los mecanismos de encapsulado podemos mencionar también la técnica conocida como 6PE/6VPE, que se utiliza para encapsular el tráfico IPv6 por parte de carriers que tienen redes MPLS.

2.3.1. TUNNEL BROKERS.

Un tunnel broker es un servicio que provee un túnel de red. Este túnel provee conectividad encapsulada sobre una infraestructura de red existente hacia una infraestructura diferente. Existen varios tipos de tunnel brokers, pero por mucho el término es mayormente usado para referirse a uno de IPv6, tal cual lo definido en la RFC:3053.

Por supuesto los de nuestro interés son justamente éstos últimos, los cuales proveen los servicios de túnel IPv6 hacia sitios o usuarios finales sobre la infraestructura existente de IPv4.

En general estos túneles ofrecen los llamados túneles protocolo 41 o proto-41 tunnels. Estos túneles son aquellos en los que IPv6 es encapsulado directamente dentro de los paquetes IPv4 colocando 41 (IPv6) en el campo protocolo de los paquetes IPv4.

Los túneles Proto-41 (IPv6 directo en IPv4) pueden no operar bien situándose detrás de un dispositivo NAT. Una forma de solventarlo es configurar el punto de destino real del túnel dentro de la DMZ en el equipo que utiliza NAT, lo cual puede no resultar muy práctico. Otro método es usar AYIYA o TSP. Ambos envían IPv6 dentro de paquetes UDP, lo cual permite atravesar la mayoría de configuraciones NAT e incluso firewalls. Este es el más aceptado y usado por los Tunnel Brokers.

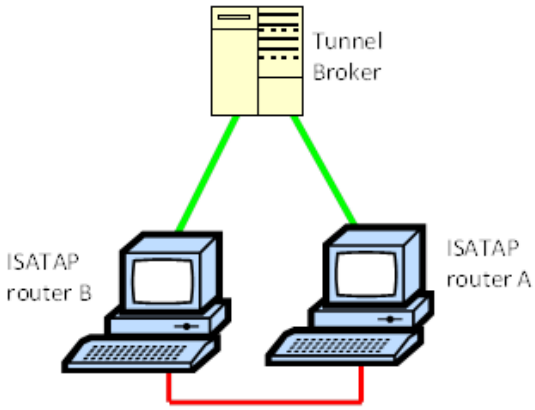

Ilustración 2: Tunnel Broker, (Institute, s.f.)

2.3.2. 6TO4

Al igual que el anterior, este también permite que los paquetes IPv6 sean transmitidos sobre una red IPv4 (generalmente Internet IPv4) sin la necesidad de configurar túneles explícitos. Servidores especiales de reenvío (relay servers) deberán existir y estar en su lugar para permitir a las redes 6to4 comunicarse con las redes nativas IPv6.

6to4 es especialmente relevante durante las fases iniciales del desarrollo hacia una conectividad completamente IPv6, dado que IPv6 no es requerido en todos los nodos entre el host y el destino. Sin embargo, es sólo un mecanismo de transición y no está pensado para usarse de forma permanente.

Puede ser usado por un host individual, o por una red local IPv6. Cuando es usado por un host, debe tener una dirección IPv4 global conectada, y el host será responsable de encapsular los paquetes IPv6 salientes y desencapsular los paquetes 6to4 entrantes. Si este host está configurado para reenviar los paquetes para otros clientes, normalmente una red local, entonces es un enrutador.

La mayoría de redes IPv6 usan autoconfiguración, la cual requiere los últimos 64 bits para el host. Los primeros 64 bits son el prefijo IPv6. Los primeros 16 bits del prefijo son siempre 2002:, los siguientes 32 son la dirección IPv4 y los últimos 16 del prefijo son escogidos arbitrariamente por el enrutador. Dado que los hosts IPv6 usando autoconfiguración ya han determinado la porción única de 64 bits de su dirección de host, simplemente deben esperar por un Router Advertisement indicándole los primeros 64 bits del prefijo para completar la dirección IPv6.

Revista Nexos Científicos *ISSN: 2773-7489*
Enero –Junio 2019 pp. 12-29 *Correo: editor@istvidanueva.edu.ec*
Volumen 3, Número 1 *URL: http://nexoscientificos.vidanueva.edu.ec/index.php/ojs/index*
Fecha de recepción: febrero 2019 *Fecha de aceptación: abril 2019*

Un enrutador 6to4 sabrá enviar un paquete encapsulado directamente sobre IPv4 si los primeros 16 bits son 2002, usando los siguientes 32 como el destino, o de otra forma enviar el paquete hacia un bien conocido servidor de reenvío, el cual tenga acceso IPv6 nativo.

6to4 no facilita la interoperabilidad entre hosts sólo IPv4 y host sólo IPv4. 6to4 es simplemente un mecanismo transparente usado como capa de transporte entre los nodos IPv6. Dado el alto número de hosts mal configurados y bajo performance observado, un aviso sobre cómo debería ser implementado 6to4 fue publicado en agosto de 2011.

2.3.3. TEREDO

Comparado con los anteriores, éste tiene una característica distintiva y es que nativamente puede realizar su función incluso detrás de dispositivos NAT, como por ejemplo un típico enrutador casero.

Teredo opera usando un protocolo de túnel independiente de la plataforma, diseñado para proveer conectividad IPv6 y funciona encapsulando paquetes de datagramas IPv6 dentro de paquetes UDP en IPv4. Estos datagramas pueden ser enrutados en el Internet IPv4 y a través de dispositivos NAT. Otros nodos Teredo en otra parte, llamados Teredo realys que tienen acceso a la red IPv6, reciben entonces los paquetes, los desencapsulan y los enrutan, esta vez ya por IPv6 puramente.

Teredo fue diseñado como una tecnología de último recurso y se pretende que sea una medida temporal: a largo plazo, todos los hosts IPv6 deberían usar conectividad nativa IPv6. Teredo entonces debería ser deshabilitado cuando la conectividad IPv6 nativa esté disponible.

El servidor Teredo escucha en el puerto UDP 3544, aunque en la lista de servicios de Linux por ejemplo, el puerto 3544 está para Teredo también por TCP.

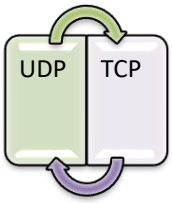

Ilustración 3: Teredo UDP-TCP

2.3.4. TRADUCCIÓN

Esta técnica consiste en utilizar algún dispositivo en la red que convierte los paquetes de IPv4 a IPv6 y viceversa. Este dispositivo tiene que ser capaz de realizar la traducción en los dos sentidos de forma de permitir la comunicación.
Dentro de esta clasificación podemos mencionar NAT64/DNS64: la red es IPv6 nativa y para llegar a sitios que son sólo IPv4 se realiza una traducción al estilo NAT, mediante un mapeo entre los paquetes IPv6 e IPv4. Se utiliza un prefijo especial para mapear direcciones IPv4 a IPv6: 64:ff9b::/96.

Es necesario también utilizar una modificación al DNS, llamada DNS64, que permite generar un registro AAAA aun cuando el destino no tenga dirección IPv6 (es decir, el DNS responda sólo con registros de tipo A).

Vale la pena mencionar que una de las propuestas iniciales de mecanismos de traducción fue NAT-PT (RFC 2766), que al día de hoy ha sido desaconsejado debido a sus fallas (ver RFC 4966) y ha sido reclasificado como "histórico" por la IETF.

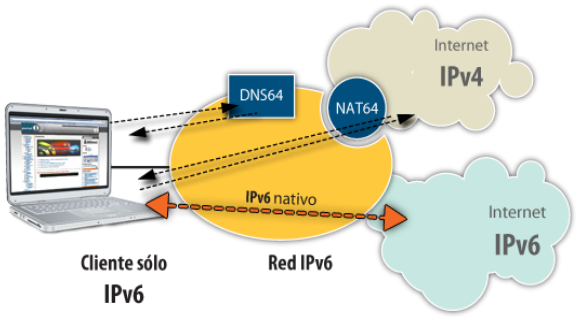

Ilustración 4: Método de Traducción, (Institute, s.f.)

2.3.5. NAT64

Es un mecanismo que permite a hosts IPv6 comunicarse con servidores IPv4. El servidor NAT64 dispone de al menos una dirección IPv4 y un segmento de red IPv6 de 32-bits (por ejemplo

64:ff9b::/96). El cliente IPv6 construye la dirección IPv6 destino utilizando el rango anterior de 96 bits más los 32 bits de la dirección IPv4 con la que desea comunicarse, enviando los paquetes a la dirección resultante. El servidor NAT64 crea entonces un mapeo de NAT entre la dirección IPv6 y la dirección IPv4, permitiendo la comunicación. Young, S. (s.f.).

Un entorno de NAT64 simplista puede verse como un dispositivo de red (un router, por ejemplo) con al menos dos interfaces. Uno de los interfaces está conectado a la red IPv4, y el otro a la red IPv6. La red estará configurada de modo que los paquetes de la red IPv6 a la red IPv4 son encaminados a través de este router. El router realizará todas las traducciones necesarias para transferir paquetes de la red IPv6 a la red IPv4, y viceversa.

La traducción no es simétrica, dado que el espacio de direcciones IPv6 es mucho mayor que el de direcciones IPv4, por lo que no es posible una traducción una-una. Para poder llevar a cabo la traducción, el equipo NAT64 debe mantener un mapeo de direcciones IPv6 a IPv4 (es decir, mantiene estados). Este tipo de mapeo de direcciones se configura estáticamente por los administradores del sistema o, habitualmente, se crea automáticamente cuando llega el primer paquete IPv6 al servidor NAT64. Después de que se haya creado este flujo, los paquetes pueden pasar en ambas direcciones.

En general, NAT64 está diseñado para usarse cuando las comunicaciones son iniciadas por los hosts IPv6. Pero también existen algunos mecanismos, (tales como mapeos estáticos de direcciones) para permitir lo contrario.

2.3.6. DNS64

Típicamente se le considera inherente a NAT64 y describe un servidor DNS que cuando es preguntado por registros AAAA de un dominio, pero sólo encuentra registros A, sintetiza registros AAAA a partir de los registros A. La primera parte de las direcciones sintetizadas IPv6 apunta a un traductor IPv6/IPv4 y la segunda parte encierra la dirección IPv4 del registro A. El traductor en cuestión es normalmente un servidor NAT64, que típicamente realiza también esta función.

Existen 2 problemas evidentes con este mecanismo de transición:

- Sólo trabaja para casos donde se usa DNS para encontrar direcciones de host remotas, si se usan literales IPv4, el servidor DNS64 nunca se involucrará.
- Dado que el servidor DNS64 necesita retornar registros no especificados por el propietario del dominio, las validaciones DNSSEC contra los servidores raíz fallarán en casos donde el servidor DNS que hace la traducción no sea el servidor del dueño del dominio.

2.4.ESTADO DE MIGRACIÓN A IPV6 EN EL PAÍS

2.4.1. EN LOS ISP

Antes de que el ISP pueda pensar en dar servicio IPv6, será necesario que obtenga direcciones IPv6 del RIR regional, para el caso de América Latina y el Caribe será a través de LACNIC. Ahora sí, una vez obtenidas las direcciones, el ISP está en condiciones de desplegar IPv6 en 3 pasos, ellos son:

i. **Publicar las direcciones obtenidas en Internet.**

1. Modo nativo. Es necesario que el upstream provider tenga IPv6 implementado
2. Modo tunelizado. Deberán contactarse con un proveedor de nivel superior que sea capaz de terminar el túnel y tenga IPv6 nativo.

Ilustración 5: Publicación de direcciones en internet, (Aguas Bucheli, 2014)

ii. **Desplegar IPv6 en su propia red.**

1. Si el ISP tiene implementado MPLS en su red, entonces la transición es sencilla:
solo basta con desplegar Dual Stack

ISSN: 2773-7489
Correo: editor@istvidanueva.edu.ec
URL: http://nexoscientificos.vidanueva.edu.ec/index.php/ojs/index
Fecha de aceptación: abril 2019

en los PE y luego utilizar 6PE. De esta forma, los routers de core (P) no necesitan ser modificados.

2. Si el ISP no tiene implmentado MPLS en su red, será necesario Dual Stack en todos los routers por los que pasará el tránsito IPv6.

iii. **Llegar al usuario final (clientes) con IPv6.** Existen varias alternativas para llegar a los clientes con IPv6, entre ellas:

1. Dual Stack (es necesario que el CPE soporte ambos protocolos)
2. Túneles
   a. Manuales: no escala bien, solo se justifica en los casos en que se trabaja con pocos clientes.
   b. Automáticos: 6to4 (si el cliente dispone de IPv4 pública) y Teredo/Miredo (en los casos en los que el cliente está detrás de un NAT). En este caso se aconseja que el ISP despliegue Reles 6to4 y Teredo en su red para optimizar el tráfico.

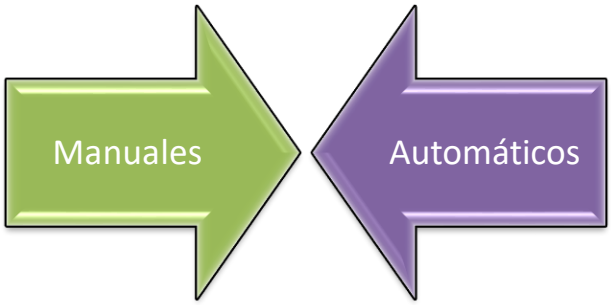

Ilustración 6: Túneles Manuales y Automáticos, (Aguas Bucheli, 2014)

Más allá de las consideraciones técnicas, hay otras cuestiones a tener en cuenta por un ISP, fundamentalmente en los aspectos económicos involucrados en una transición de este tipo, pues seguramente requerirá agregar o reemplazar equipos a la infraestructura, además de capacitación y un cúmulo de cosas que con ello vienen asociadas.

En el portal de IPv6 de LACNIC podemos encontrar las estadísticas por países sobre el avance de IPv6, por supuesto extrajimos la información relacionada al Ecuador. Los valores están representados sólo hasta marzo de este año y desde entonces no han sido actualizados. Sin embargo nos muestran una clarísima tendencia al crecimiento a partir de octubre de 2008. Sin embargo el total de asignaciones llega a ser de sólo 22. De éstas 22 sólo 8 están ruteadas (aunque en algún momento llegaron a ser 10), es decir que en realidad están yendo a alguna parte, las demás están asignadas pero sin uso.

3. RESULTADOS Y DISCUSIÓN

En vista de que al momento nuestros proveedores no nos asignan IPv6 directamente. Queremos presentar un posible camino o propuesta para ir migrando nuestros sistemas a IPv6, en este caso consideraremos al Laboratorio de Tecnologías de Información y Comunicación.

3.1. DESCRIPCIÓN DE CADA PASO Y SUS TIEMPOS ESTIMADOS

En este capítulo propondremos los pasos que debemos dar así como posibles tiempos de duración de cada uno de ellos.

1 En vista de que posiblemente tu proveedor de internet no te está asignando IPv6 todavía. Tenemos que hacer uso de los túneles para nuestra red. Este será el primer paso para lograr conectividad IPv6 y nos mantendríamos en este estado durante el tiempo que nuestro proveedor de internet decida entregarnos IPv6 de forma nativa, directamente él. Este paso podríamos estar usándolo varios meses o años.

2 Una vez que nuestro ISP nos asigne un rango IPv6 de forma nativa, procederíamos a implementar este rango IPv6 en nuestra red y posteriormente eliminar el túnel que usamos durante todo este tiempo.

3 Aquí es importante una aclaración y es que en ninguno de los anteriores pasos hemos mencionado IPv4 y es porque durante todo este tiempo mantendremos ambos sistemas. El de IPv4 que siempre hemos usado y el de IPv6. Este

proceso que se llama "Dual Stack" tomará varios años, posiblemente de 5 a 10 años en utilizarse. Sí, es verdad: durante 5 ó 10 años utilizaremos las redes en IPv4 y en IPv6. Son como dos mundos paralelos, y los sistemas sabrán si deben hablar por IPv4, ó por IPv6.

4 A medida que los años transcurran, todos los sistemas ya estarán trabajando en dual stack e incluso muchos de ellos comenzarán solamente a trabajar en IPv6 (pues se habrán agotado posiblemente ya todas las IPv4 o serán muy caras de conseguir). Cuando llegue este momento, en que todos los sistemas de una forma u otra ya estén configurados para entender y trabajar con IPv6, independientemente de si entienden o trabajan (o no) con IPv4.

3.1.1. ¿CÓMO ESCOGER UN PROVEEDOR DE TÚNEL?

1 **tunnelbroker.net** es un sistema de túnel de la empresa Hurricane Electric.

1 Tunnelbroker tiene varios puntos de presencia, varios lugares hacia donde puedes establecer tu túnel, y por tanto no es normal que ocurra el congestionamiento que en otros proveedores sí ocurre al tener solamente un punto de presencia.

2 Tunnelbroker además te permite obtener si deseas un /64

3 Tunnelbroker se puede configurar tanto en equipos Linux como Windows y seguramente en otros sistemas operativos más.

4 El único inconveniente que presenta tunnelbroker es que necesitas una IPv4 fija, una IPv4 que no varíe pues en base a esta IPv4 es que ellos establecen, permiten, el tunel.

5 Por tanto tunnelbroker es muy útil para cuando quieres conectar equipos que están en una red empresarial, ya que ellos típicamente tienen una IP estática.

2 **gogoc**: en el sitio freenet6.net es un cliente de túnel que se puede instalar en equipos Linux o Windows, e incluso android,

1 te permiten establecer un túnel de forma anónima (te dan una IPv6 que varía de acuerdo a la IPv4 que tengas),

2 o puedes establecer un túnel autenticado que se parece mucho a tunnelbroker, en el túnel autenticado te asignan una IPv6 de forma permanente

3 la ventaja que tiene gogoc es que es muy simples de configurar y que no importa si tu IPv4 varía, ellos te asignarán una IPv6.

4 La desventaja que tiene gogoc es que tiene menos puntos de presencia que tunnelbroker por lo que la posibilidad de que el túnel falle por congestionamiento o caídas del punto de presencia es mayor. Aunque nunca le hemos percibido.

5 Sugiero este sistema gogoc para conectar equipos standalone, equipos que no estén en una red de forma fija, como por ejemplo tu laptop.

3.2.GOGOC

3.2.1. INSTALACIÓN EN LINUX FEDORA:

Para instalar gogoc en Fedora simplemente ejecutamos:

```
sudo yum install gogoc
```

Script 1: Instalación Gogoc-Fedora, (Aguas Bucheli, 2014)

Al finalizar la instalación procedemos a arrancar el servicio:

```
service gogoc start
chkconfig gogoc on
```

Script 2: Forma de Arrancar el servicio en Gogoc-Fedora, (Aguas Bucheli, 2014)

Podemos verificar en los logs si se nos ha entregado una IP:

```
sudo tail /var/log/messages
```

Script 3: Verificación de Logs, (Aguas Bucheli, 2014)

Por ejemplo en este caso los logs nos indican claramente que se nos entregó una IP:

```
Nov  6 14:49:11 lfaguas gogoc[13271]: --- Start of configuration script. ---
Nov  6 14:49:11 lfaguas gogoc[13271]: Script: linux.sh
Nov  6 14:49:11 lfaguas gogoc[13271]: tun setup
Nov  6 14:49:11 lfaguas gogoc[13271]: /sbin/ifconfig tun up
Nov  6 14:49:11 lfaguas gogoc[13271]: This host is: 2001:470:c:93e::2
Nov  6 14:49:11 lfaguas gogoc[13271]: /sbin/ifconfig tun add 2001:470:c:93e::2
```

Script 4: Logs Fedora, (Aguas Bucheli, 2014)

La IP que se nos entregó es: *2001:470:c:93e::2* y es un /128 (una sola IP)

3.2.2. INSTALACIÓN EN LINUX DEBIAN O UBUNTU

En el caso de Debian o de Ubuntu, simplemente hacemos:

```
sudo apt-get install gogoc
```

Script 5: Instalación Debian-Ubuntu gogoc, (Aguas Bucheli, 2014)

Cualquier variante moderna de Debian o Ubuntu tendrá el paquete gogoc y luego le arrancarías con:

```
sudo service gogoc start
```

Script 6: Forma de Iniciar el servicio de gogoc en Debian-Ubuntu, (Aguas Bucheli, 2014)

3.2.3. INSTALANDO GOGOC EN OTRAS VARIANTES DE LINUX

En este caso te tocaría utilizar el manejador de paquetes de la variante de Linux que utilices para que, a través de él, realices la instalación del servicio gogoc y luego arranques el servicio gogoc como se te indique por parte de tu distribución de Linux.

3.2.4. USANDO GOGOC DE MODO AUTENTICADO

Si yo deseara utilizar gogoc no en modo anónimo sino en modo autenticado, debo simplemente entrar a crearme una cuenta "freenet6" en la siguiente URL:

http://www.gogo6.com/freenet6/account

Anota bien tus datos de username y de password.

Con este username y password, procedemos a editar el archivo de configuración de gogoc llamado: **/etc/gogoc/gogoc.conf** y cambiar los siguientes parámetros:

```
#userid es el usuario que te creaste en el sitio de freenet6
#passwd es la clave del usuario que te creaste en freenet6
userid=tuusuario
passwd=tuclave
server=authenticated.freenet6.net
auth_method=any
```

Script 7: Gogoc con Freenet6

Server es el servidor para usuarios autenticados, déjale así. Y el parámetro *auth_method* es el método de autenticación contra la red freenet6, **any** significa que se escogerá el método más seguro.

Por favor ten en cuenta que estos parámetros pueden estar comentados; si es el caso te pido le des comentes. O pueden ya estar des comentados, en este caso te tocaría modificarle los valores por estos que aquí te indico.

Y ya, con estos 4 cambios estaremos autenticando contra la red freenet, por lo tanto siempre se me otorgará una IPv6 fija, que no cambiará y entonces ahora sí podríamos usar esta IPv6 para configurar nuestros servicios en Linux, en el caso del Laboratorio de Tecnologías de Información y Comunicación

3.3.TUNNELBROKER

TunnelBroker, al cual llamaremos también HE, pues es un sistema de Hurricane Electric, es un sistema de túnel cuya ventaja fundamental es que tiene una gran cantidad de POP, por tanto el uptime

del servicio es extremadamente alto. Esto lo hace muy recomendado para equipos Servidores Linux en los cuales yo esté dando un servicio a través de IPv6 y lógicamente no quiera downtime en el servicio de IPv6. IANA. (2013).

3.3.1. PROCESO INICIAL CON TUNNELBROKER:

Para utilizar TunnelBroker tienes que crearte una cuenta en su sitio web www.TunnelBroker.net a través de una sola cuenta puedes manejar o tener 5 túneles diferentes hacia 5 servidores que tengan una IPv4 diferente.

TunnelBroker te permite solicitar y obtener automáticamente un /48 para cada uno de esos 5 túneles. Por tanto si luego deseas podrías asignar IPv6 a máquinas que estén detrás de este servidor.

Una vez creada la cuenta, al entrar a ella verás en la columna izquierda una opción que dice:
"Create Regular Tunnel"

Al escoger esta opción tendrás que llenar 2 datos:
IPv4 EndPoint: Es la IPv4 pública donde esté localizado el servidor al cual conectarás tunnelbroker. Si estás sentado en el mismo servidor, puedes utilizar la IP que te sugerirá abajo, te dice así: "You are viewing from" (estás viendo desde la IP)... esa es la IP tuya. Es la misma del servidor, entonces puedes utilizarla. Si no es la misma del servidor, por favor utiliza la IPv4 pública del servidor

Luego validas el POP (el servidor de tunel) que desees utilizar. Él te recomienda uno de esos servidores, el que mejor RTT (roud trip time) tenga desde tí hacia él, si deseas escoges otro, sino, le dejas así.

Clic en Create Tunnel y el túnel estará listo.

No me canso de insistir: debes haber definido la IPv4 pública que utiliza el servidor al cual configurarás el tunal. Si este servidor tiene una IP privada, delante de él seguramente habrá una ip pública, esa será, si este servidor tiene una ip publica, entonces le pones esa.

Luego de creado el túnel, aparecerá un enlace al medio de la página, uno por cada túnel. Por favor para nuestras pruebas requerimos solamente un túnel, si creas túneles de más, el sistema los eliminará si ve que no les usas en un determinado tiempo.

Si haces clic sobre el túnel que creaste verás varias opciones, las más interesantes son:

- Server IPv4 Address: Es la IPv4 del servidor de hurricane electric. Es la IP hacia donde nos conectaremos para establecer el túnel.
- Server IPv6 Address: Es la IPv6 del servidor de hurricane electric, el gateway hacia donde se enviarán los datos en IPv6.
- Client IPv4 Address: Es la IPv4 pública de tu server.
- Client IPv6 Address: Es tu IPv6. Es la que podrás luego utilizar para apuntar hacia ella los servicios web, mail, etc.

3.3.2. CONFIGURACIÓN DE UN SERVIDOR DEBIAN

Partiendo de que ya tienes el tunel creado, supongamos que el servidor al que le configurarás el tunel es debian, para ello deberás primero que todo garantizar que este servidor ya esté navegando en IPv4. Como siempre hayas hecho en debian.

Entonces procedes a editar el archivo **/etc/network/interfaces** y agregas al final lo siguiente:

```
iface he-ipv6 inet6 v4tunnel
      address 2001:470:1f06:2c2::2
      netmask 64
      endpoint 209.51.161.14
    up ip -6 route add default dev he-ipv6
    down ip -6 route del default dev he-
ipv6
```

Script 8: Edición Archivo en Debian, (Aguas Bucheli, 2014)

Lo único que se debe tener en cuenta y cambiar adecuadamente es:

- **address:** será la IPv6 que te dieron, la que en el tunnel llaman: Client IPv6 Address:
- **endpoint:** es la IPv4 del servidor de hurricane electric, hacia donde enviaré los paquetes

Revista Nexos Científicos *ISSN: 2773-7489*
Enero –Junio 2019 pp. 12-29 *Correo: editor@istvidanueva.edu.ec*
Volumen 3, Número 1 *URL: http://nexoscientificos.vidanueva.edu.ec/index.php/ojs/index*
Fecha de recepción: febrero 2019 *Fecha de aceptación: abril 2019*

encapsulados. Es lo que en el tunnel te llaman: Server IPv4 Address:

Simplemente reiniciamos la red en debian:

```
service networking restart
```

Script 9: Reinicio de la red en debían, (Aguas Bucheli, 2014)

3.3.3. CONFIGURACIÓN DE TUNNELBROKER EN CENTOS-6

Para centos es igual de fácil, una vez creado el tunel en el sitio de tunnelbroker.net editamos un nuevo archivo de configuración que se llamará: ***/etc/sysconfig/network-scripts/ifcfg-sit1***

En este archivo se agrega:

```
DEVICE="sit1"
BOOTPROTO="static"
NM_CONTROLLED="no"
ONBOOT="yes"
IPV6INIT=yes
IPV6TUNNELIPV4=IPv4 del server
IPV6TUNNELIPV4LOCAL=IPv4 del cliente
IPV6ADDR=IPv6 del cliente (mantén el /64)
IPV6_DEFAULTGW=IPv6 del servidor (elimina el /64)
```

Script 10: Edición del Archivo de configuración, (Aguas Bucheli, 2014)

Las primeras líneas son estándar, lo que siempre viene en un archivo de configuración de la red. las últimas son las interesantes, veamos:

- **IPv4 del server:** En tunnelbroker es: Server IPv4 Address
- **IPv4 del cliente :** en tunnelbroker es: Client IPv4 Address (si estás detrás de un NAT ponle la IP privada que tengas)
- **IPv6 del cliente:** en tunnelbroker es: Client IPv6 Address. Al final ponle /64
- **IPv6_DEFAULTGW:** en tunnelboker es: Server IPv6 Address. No le pongas /64 al final.

Al finalizar, se reinicia la red:

```
service network restart
```

Script 11: Reinicio de la Red en CentOS, (Aguas Bucheli, 2014)

3.3.4. ¿QUÉ HACER SI NO FUNCIONA?

Los casos más típicos cuando no funcionan son:

1 No definiste correctamente la IPv4 pública del servidor en el sitio de tunnelbroker.net
2 Tienes un firewall que te bloquea este protocolo, interfaz, servicio. Prueba apagar todo firewall que tengas.
3 No configuraste bien la interfaz sit1, revisa estos parámetros.

3.3.5. CONFIGURACIÓN DE 6TO4 EN SERVIDOR DEBIAN.

Configuración de un servidor Debian en una Red como la de la siguiente figura, usando un túnel 6to4 para acceder a Internet IPv6

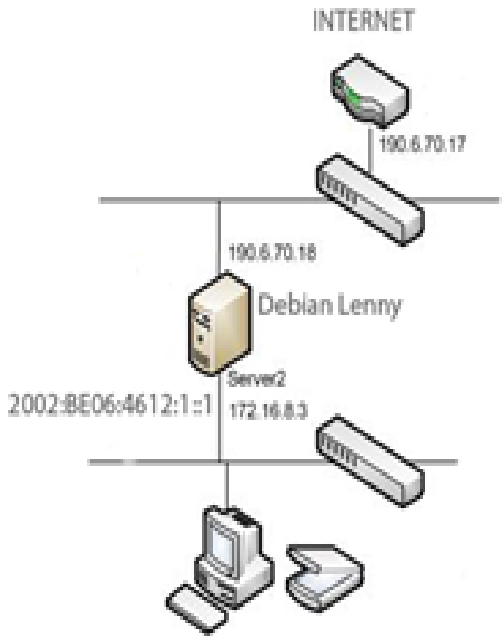

Figura 1: Configuración 6to4, (Young, s.f.)

- Determinar el prefijo ipv6 que se obtiene a partir de la dirección IPv4 publica usada para establecer el túnel, utilizando el comando printf en Linux con la siguiente sintaxis:

```
# printf "2002:%02x%02x:%02x%02x::1\n" 190 6 70 18
```

Script 12: Configuración 6to4 en Debian Parte 1, , (Aguas Bucheli, 2014)

- Configurar las interfaces de red del servidor que funcionara como router.

Revista Nexos Científicos *ISSN: 2773-7489*
Enero –Junio 2019 pp. 12-29 *Correo: editor@istvidanueva.edu.ec*
Volumen 3, Número 1 *URL: http://nexoscientificos.vidanueva.edu.ec/index.php/ojs/index*
Fecha de recepción: febrero 2019 *Fecha de aceptación: abril 2019*

```
iface eth2 inet static
        address 172.16.8.3
        netmask 255.255.255.0
        network 172.16.8.0
iface eth2 inet6 static
        address 2002:BE06:4612:1::1
        netmask 64
```

Script 13: Configuración de las interface de red, (Aguas Bucheli, 2014)

- Configurar la interface del túnel 6to4 utilizando un Relay 6to4 (Ej. ::192.88.99.1)

```
iface tun6to4 inet6 v4tunnel
        address 2002:be06:4612::1
        netmask 16
        gateway ::192.88.99.1
        endpoint any
        local    190.6.70.18    #fits
address
```

Script 14: Configuración de Relay 6to4, (Aguas Bucheli, 2014)

- Instalar y configurar el radvd el cual es el encargado de anunciar el prefijo IPv6 en la red interna.

```
apt-get install radvd
```

Script 15: Instalación de RADVD, (Aguas Bucheli, 2014)

- Configurar el archivo /etc/radvd.conf de la siguiente manera siendo eth2 la interface del FW que se conecta a la LAN

```
interface eth2
{
        AdvSendAdvert on;
        MinRtrAdvInterval 3;
        MaxRtrAdvInterval 10;
        AdvDefaultPreference low;
        AdvHomeAgentFlag off;
        prefix 2002:be06:4612:1::/64
        {
                AdvOnLink on;
                AdvAutonomous on;
                AdvRouterAddr on;
        };
};
```

Script 16: Configuración de archivo para RADVD, (Aguas Bucheli, 2014)

- Activar el routing IPv6 configurando el archivo /etc/sysctl.conf y reiniciando o poniendo a 1 el archivo /proc/sys/net/ipv6/conf/all/forwarding de la siguiente manera:

```
echo                1                >
/proc/sys/net/ipv6/conf/all/forwarding
```

Script 17: Configuración de inicio para el routing,

3.3.6. CONFIGURACIÓN DE UN TÚNEL EN UBUNTU USANDO TEREDO.

Existe en Ubuntu un paquete que implementa los túneles Teredo de manera muy fácil para el cliente. Basta con solo instalar el paquete ***miredo*** y este se configurará automáticamente permitiendo acceder a Internet IPv6, incluso estando detrás de varios niveles de NAT, aunque en determinados tipos de NAT no funciona.

```
apt-get install miredo
```

Script 18: Instalación de la Aplicación, (Aguas Bucheli, 2014)

Por defecto se conectara al servidor **teredo-debian.remlab.net.** Si no le funciona con este servidor puede intentar cambiarlo de la siguiente manera:

- Edita el archive de configuración (sudo vi /etc/miredo.conf)
- Modifica la línea del Servidor (ServerAddress teredo.ipv6.microsoft.com)
- Reinicia el servicio miredo (sudo /etc/init.d/miredo restart)

3.4.IMPLEMENTACIÓN EN WINDOWS DE LOS TÚNELES

3.4.1. HOSTS CON DOBLE PILA.

Uno de los mecanismos que conceptualmente permite la introducción más sencilla de IPv6 es el uso de doble pila. Con este mecanismo un nodo está equipado con ambas pilas en su Sistema Operativo, y contiene direcciones IPv4 e IPv6. Este nodo es capaz de enviar y recibir paquetes de ambos protocolos para comunicarse con nodos que contengan cualquiera de las dos pilas implementadas. Este es el método más simple para la introducción de IPv6. Constituye el próximo paso en la evolución de Internet, hasta que IPv6 sea el único protocolo utilizado.

El mecanismo de doble pila no es un mecanismo de transición en sí, sino más bien, un mecanismo de integración de IPv6 en las redes actuales. Este mecanismo no es nuevo, antes se utilizó para integrar varios protocolos en una red, por ejemplo, IPX/SPX, *AppleTalk*, TCP/IP.
Uno de los retos fundamentales en implementar este mecanismo se encuentra en los protocolos de enrutamiento que se estén utilizando. Puede darse el caso de que sea recomendable cambiar el protocolo de enrutamiento actual.

Otro aspecto importante es la interacción de los dos protocolos. Estas redes con doble pila necesitarán comunicarse con redes nativas IPv4, sobre todo al comienzo de la migración. Cuando se usa este mecanismo se debe tener muy en cuenta cómo funcionan algunos de los servicios fundamentales como son el DNS, o el SMTP.

Por defecto en todos los Sistemas Operativos que normalmente utilizamos ya vienen activadas ambas pilas de protocolo. Para comprobar que efectivamente tenemos activado el protocolo IPv6 podemos ejecutar un ping a la dirección de localhost ipv6.

#ping ::1

Por otra parte podemos ejecutar el comando ipconfig en Windows o ifconfig en Linux para ver las direcciones IPv4 e IPv6 en las interfaces de nuestro host.
En el caso de Windows XP, el cual es aún muy utilizado, se debe ejecutar el comando *ipv6 install* pues por defecto IPv6 no está habilitado.

Hay que tener en cuenta algunos aspectos importantes cuando tenemos activadas ambas pilas de protocolo:

- Las Listas de Acceso que se utilizan para IPv4 no sirven para IPv6 y viceversa, por lo que debemos crear reglas de seguridad para ambos protocolos.
- Como ahora las interfaces de nuestros hosts tienen varias direcciones IP (v4 y/o v6), tienen la posibilidad de comunicarse con otros hosts por cualquiera de ellas, por lo tanto existe un procedimiento para la selección de la dirección de origen y destino en una comunicación entre hosts doble pila.

3.4.2. TÚNELES 6TO4

El mecanismo de transición conocido como 6to4 es una variante de túnel automático de enrutador a enrutador. Este utiliza el prefijo reservado 2002::/16 para asignárselo a un sitio que participe en el túnel. El mismo permite conectar sitios completos con mínima configuración. Para formar el túnel, se le asigna al sitio en cuestión el prefijo 2002:V4ADDR::/48, donde V4ADDR es la dirección global IPv4 del enrutador que constituye el extremo local del túnel. Este prefijo tiene exactamente el mismo formato que cualquier prefijo global IPv6, por lo que puede ser tratado de igual manera. En caso de que un dominio 6to4 quiera comunicarse con otro, no se requiere ninguna configuración adicional. Los extremos del túnel se determinan por el prefijo de la dirección IPv6 de destino que se encuentra en el paquete IPv6, la cual además contiene la dirección IPv4 global para establecer el túnel. De esta forma cualquier dominio IPv6 puede comunicarse con otro sin necesidad de implementar ningún protocolo de enrutamiento, ya que de esto se encarga IPv4. En la siguiente figura se observa el esquema general de los Túneles 6to4.

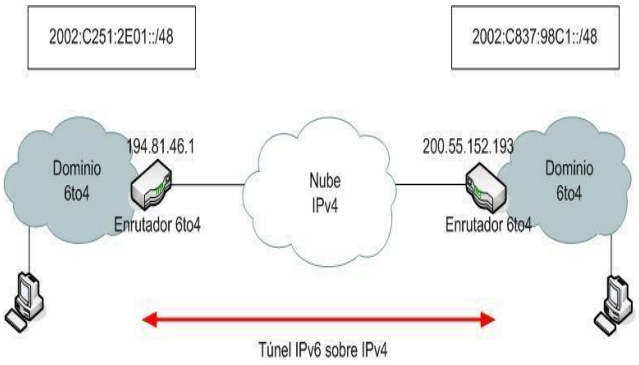

Figura 2: Túneles 6to4 Parte 1, (Profesor, s.f.)

Cuando un dominio 6to4 se quiere comunicar con otro dominio IPv6 no 6to4 la solución es un poco más complicada. En este caso la comunicación se establece a través de un enrutador que tiene al menos una interface 6to4 y otra conectada a una red IPv6 nativa. Este tipo de enrutador se conoce como Retransmisor (*Relay*) 6to4. A diferencia de la comunicación entre dos dominios 6to4, en este caso si se necesita que el *relay* 6to4 anuncie el prefijo

Revista Nexos Científicos *ISSN: 2773-7489*
Enero –Junio 2019 pp. 12-29 *Correo: editor@istvidanueva.edu.ec*
Volumen 3, Número 1 *URL: http://nexoscientificos.vidanueva.edu.ec/index.php/ojs/index*
Fecha de recepción: febrero 2019 *Fecha de aceptación: abril 2019*

2002::/16 en la red IPv6 nativa. Además deberá anunciar rutas hacia los prefijos de las redes nativas en la red 6to4. Para hacer más eficiente el funcionamiento de enrutadores de este tipo se utilizan direcciones *anycast* , la cual, según la RFC3068, debería ser la dirección IPv6 6to4 2002:c058:6301::, equivalente a la dirección IPv4 192.88.99.1 (http://www.ietf.org/rfc/rfc3068.txt). En la siguiente figura se puede observar todos los componentes del servicio 6to4. Martínez, I. (2013)

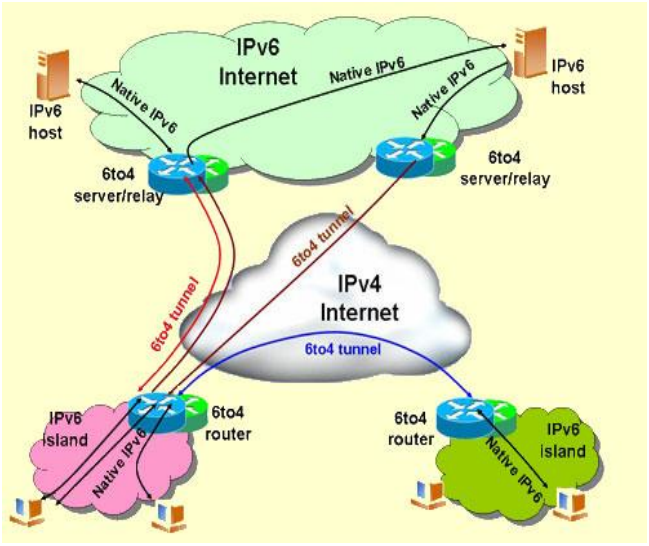

Figura 3: Túneles 6to4 Parte 2, (Profesor, s.f.)

La mayoría de los ISP actualmente solo publican sus *relay* 6to4 a su red, fundamentalmente basados en preocupaciones en cuanto a la seguridad. A pesar de estas preocupaciones y otros problemas con el tráfico *multicast* sobre los dominios 6to4, este constituye una variante muy efectiva para ofrecer conectividad IPv6 a una Intranet a través de un proveedor de servicios IPv4.

Con la escasez de proveedores de servicios IPv6 en la actualidad, generalmente 6to4 es el mecanismo que se utiliza para conectar una Intranet a la red IPv6 pública en Internet, a través de un enrutador de frontera. Otros mecanismos como ISATAP, o tráfico nativo IPv6, pueden ser utilizados dentro de la Intranet.

3.4.3. CONFIGURACIÓN DE TÚNELES 6TO4.

Como se mencionó anteriormente, con los túneles 6to4 podemos configurar uno de nuestros equipos en la frontera de nuestra red para que sirva de enrutador hacia Internet IPv6

3.4.4. CONFIGURACIÓN DE 6TO4 EN ENRUTADOR CISCO.

Como de costumbre, Cisco está en la vanguardia de la implementación de esta nueva tecnología. Desde hace años implementan funciones IPv6 en sus IOS. Si desea saber exactamente que funciones de IPv6 están implementadas en sus Cisco puede visitar el sitio de Cisco (http://www.cisco.com) o revisar este documento, también de Cisco que publico en mi sitio (http://www.net6sol.com/docs/cisco_ipv6.pdf). Para nuestro ejemplo hemos utilizado un Router Cisco 1721 con IOS 12.4T.

El procedimiento consiste básicamente en lo siguiente:

- Activar el enrutamiento IPv6 con el comando Router(config)#ipv6 unicast-routing
- Crear la interface del túnel con el comando Router(config)#interface Tunnel64 y especificar que será un túnel de tipo 6to4.
- Especificar una dirección IPv6 en las interfaces que corresponda.
- Especificar las rutas estáticas para Internet IPv6.
- Aunque no es imprescindible se recomienda especificar al menos un conjunto básico de reglas de seguridad que nos protejan de posibles ataques desde el exterior de nuestra red. Para ellos podemos seguir como criterios, los expuestos en http://www.net6sol.com/docs/

A continuación les muestro un ejemplo simple de configuración que espero sirva de referencia.

```
ipv6 unicast-routing
!
interface Tunnel64
no ip address
no ip redirects
ipv6 unnumbered FastEthernet0
tunnel source FastEthernet0
tunnel mode ipv6ip 6to4
!
interface FastEthernet0
ip address 201.55.183.65 255.255.255.192
ipv6 address 2002:C937:B741::1/64
ipv6 enable
```

Revista Nexos Científicos *ISSN: 2773-7489*
Enero –Junio 2019 pp. 12-29 *Correo: editor@istvidanueva.edu.ec*
Volumen 3, Número 1 *URL: http://nexoscientificos.vidanueva.edu.ec/index.php/ojs/index*
Fecha de recepción: febrero 2019 *Fecha de aceptación: abril 2019*

```
!
ipv6 route 2002::/16 Tunnel64
ipv6 route ::/0 2002:C058:6301::
```

Script 19: Configuración de Túneles en Cisco, (Aguas Bucheli, 2014)

3.4.5. DETALLES EN LA CONFIGURACIÓN DE ALGUNOS CLIENTES.

Aunque en principio, los clientes que se auto-configuren a través del servicio radvd mencionado con anterioridad, tienen la posibilidad de comunicarse a través del túnel 6to4 con Internet IPv6, hay algunos comportamientos específicos de la implementación en cada Sistema Operativo del protocolo IPv6 cuando se utilizan direcciones 6to4.

3.4.6. EL COMPORTAMIENTO POR DEFECTO DE MICROSOFT RESPECTO AL USO DE LAS DIRECCIONES IPV6 6TO4.

Por defecto Microsoft solo utiliza las direcciones IPv6 6to4 para conectarse a otras direcciones 6to4 o a equipos que no tienen IPv4, es decir, por defecto utilizará IPv4 para acceder a servicios en servidores Dual Stack. Para que utilice las direcciones 6to4 en vez de las IPv4 se debe usar el siguiente método.
Para que la dirección IPv6 (6to4) se utilice de forma predeterminada en Microsoft Windows se debe modificar la tabla de políticas para que la etiqueta (Label) del prefijo 6to4 coincida con el de la dirección que representa todas las direcciones IPv6 (::/0), resultando una tabla como la siguiente:

La forma de lograrlo depende de la versión de Windows con la que estemos trabajando pero básicamente consiste en establecer (set) o adicionar (add) la política referida al prefijo 6to4.

```
netsh interface ipv6 set prefixpolicy 2002::/16 30 1
```

Script 20: Configuración de la política parte 1, (Aguas Bucheli, 2014)

En caso de que no exista una política referida al prefijo 2002::/16 debe adicionarla de la siguiente manera:

```
netsh interface ipv6 add prefixpolicy 2002::/16 30 1
```

Script 21: Configuración de la política parte 2, (Aguas Bucheli, 2014)

Es posible que al fijar una política se eliminen el resto de las existentes por lo que se debe guardar la tabla inicial para poder reescribirla (esto sucede en Windows XP). Para mostrar la tabla de políticas:

```
netsh interface ipv6 show prefixpolicies
```

Script 22: Configuración de la política parte 3, (Aguas Bucheli, 2014)

3.4.7. PUBLICACIÓN DEL PREFIJO 6TO4 EN DNS INVERSO.

Una vez que comenzamos a publicar servicios en nuestros servidores con direcciones IPv6 6to4 necesitaremos publicar algunas de estas direcciones en el DNS inverso, fundamentalmente las direcciones de nuestros servidores de correo. Para esto, existe un servicio gratis en internet en el sitio https://6to4.nro.net/. El procedimiento es muy sencillo, solo hay que seguir los pasos especificados en el sitio siempre conectados desde una dirección de nuestro prefijo 6to4. Mkarich. (2013)

3.5.TÚNELES TEREDO.

Teredo, también conocido como Atravesador de NAT (*NAT Traversal*) para IPv6, se ha diseñado para permitirle a los *hosts* con doble pila que se encuentran detrás de uno o varios niveles de NAT, acceder a sitios IPv6 externos mediante un túnel UDP Teredo usa dos entidades, el Servidor Teredo y el *Relay* Teredo.

Teredo usa métodos bastante complejos, y no puede garantizarse que funcione producto de la gran variedad de implementaciones que existen de NAT.

3.5.1. CONFIGURACIÓN DE UN TÚNEL EN WINDOWS 7 USANDO TEREDO.

De forma predeterminada a partir de Windows Vista los Sistemas Operativos de Microsoft incorporan una interface Teredo habilitada. De esta forma, en principio, es posible tener conectividad con Internet IPv6 con solo tener acceso UDP al servidor de Teredo de Microsoft (teredo.ipv6.microsoft.com). Al igual que en el caso de los túneles 6to4 Microsoft

Revista Nexos Científicos *ISSN: 2773-7489*
Enero –Junio 2019 pp. 12-29 *Correo: editor@istvidanueva.edu.ec*
Volumen 3, Número 1 *URL: http://nexoscientificos.vidanueva.edu.ec/index.php/ojs/index*
Fecha de recepción: febrero 2019 *Fecha de aceptación: abril 2019*

prefiere usar las direcciones IPv4 en caso de querer acceder a host con doble pila. Si queremos probar la conectividad IPv6 en este caso podemos intentar un ping a la dirección IPv6 de www.kame.net:

```
ping -6 www.kame.net
```

Script 23: Test de Conectividad, (Aguas Bucheli, 2014)

Si desea deshabilitar Teredo ejecute el comando

```
netsh interface teredo set state disable
```

Script 24: Deshabilitación teredo, (Aguas Bucheli, 2014)

Si desea rehabilitarlo:

```
netsh interface teredo set state client
teredo.ipv6.microsoft.com 60 34567
```

Script 25: Rehabilitación teredo, (Aguas Bucheli, 2014)

3.5.2. TÚNEL BROKER

En vez de usar túneles configurados manualmente se pueden usar túneles configurados mediante tareas programadas (*scripts*). Esta variante es conocida como "*Tunnel Broker*". Como en el caso anterior, estos túneles son necesarios cuando se tiene un nodo con doble pila y se desea comunicar con otra red o nodo IPv6 a través de una red IPv4. La idea general sobre los *Tunnel Broker* es darle al usuario la posibilidad de entrar a un sitio Web y recibir un *script* cuya función es establecer un túnel IPv6-sobre-IPv4 con el servidor de *Tunnel Broker*. Oracle. (2010)

Un *Tunnel Broker* puede establecerse de muchas maneras, el requisito para el servicio es que necesita mantener información sobre quién establece el túnel. Este servicio se implementa de forma pública en varias redes IPv6, por ejemplo, el *Tunnel Broker* de Freenet6 (http://www.freenet6.com) en Canadá, o el de SixXS (http://www.sixxs.com) en Europa, o el de Hurricane Electric en Estados Unidos (http://ipv6.he.net). Cuando se vaya a seleccionar un *Tunnel Broker* se debe tener en cuenta la distancia geográfica ya que generalmente se corresponderá con mayor tiempo de transmisión para llegar al otro extremo del túnel.

Los *Tunnel Broker* pueden servir tanto para *hosts* como para una red entera, en caso de que se establezca desde un enrutador que le de servicio a esa red. Se pueden establecer usando el protocolo TSP (del inglés *Tunnel Setup Protocol*), y pueden necesitar funciones específicas para activar y desactivar el túnel.

La configuración de los *Tunnel Broker* es generalmente sencilla en los clientes, pero no así en los servidores. Esto se evidencia sobre todo en temas relacionados con la seguridad y el manejo de los túneles, cuando los clientes usan direcciones dinámicas. Algunos *Tunnel Broker* son capaces de manejar clientes con direcciones dinámicas o que están detrás de un servidor NAT, lo cual es muy común. OpenStack. (2010)

En nuestro caso nos limitaremos a configurar clientes en dos de los Sistemas Operativos de clientes más conocidos (Microsoft y Ubuntu), pues los servidores raramente los configuremos ya que existen los ya mencionados. A continuación les mostramos tres de los más utilizados:

Provider	Coverage	Subnet	Protocols	Static	RDNS	BGP	Registration	Configuration	Language
Hurricane Electric[4]	United States, Canada, Europe (6 Countries), Hong Kong, Tokyo, Singapore	/64 and /48 subnet	6in4	Yes	Yes	Yes	Signup required	Website	English
SixXS	United States, Brazil, Europe (13 countries), New Zealand[5]	/64 tunnel and /48 subnet	6in4, AYIYA [6]	Yes	Yes		RIPE, ARIN, APNIC, LACNIC, AFRINIC, or direct signup[7]	TIC/AICCU, manual, website	English
gogo6/Freenet6[8]	Montreal, Amsterdam, Taipei, Sydney	/56 subnet	6in4, 4in6, TSP	Yes	Yes		Anonymous, or signup (via registration on gogoNET[2])	TSP, website	English

Figura 4: Principales proveedores de túneles, (Electric, s.f.)

4. CONCLUSIONES

- Para instruirse sobre la coexistencia de IPv4 e IPv6, se debería fomentar temas de disertación como el presentado, ya que se podría fortalecer las vulnerabilidades de ciertos sistemas o infraestructuras.

- La creación de túneles es un modo de utilizar una infraestructura de redes de un protocolo para transferir una carga.

- El tunnel broker es una forma de transmitir que habilita usuarios para obtener conectividad ipv6, estos túneles nos brindan una conectividad encapsulada por una infraestructura existente a una nueva infraestructura, este servicio es

gratuito, para ello hay que registrarse, esta comunicación se basa por vía web.

- Gracias a esta idea no es necesario esperar a que el proveedor de internet nos asigne IPv6 sino que se puede comenzar a utilizar este protocolo a través de túneles.

- En pocos lugares ya se está implementando las direcciones ipv6, por eso crearon varios métodos para que las versión de ip 4 y 6 se pueden comunicar, una de ella es el tunnel bróker.

- Aunque el protocolo ipv6, pueda parecer muy complejo en realidad es muy simple y muy eficiente.

- Este nuevo protocolo presenta una mayor seguridad para sus usuarios ya que las cabeceras pueden ser autenticadas y encriptadas, usando las cabeceras correspondientes y permitiendo además la prevención de ataques ICMP.

- Este además cuenta con una serie de mecanismos que permiten nuevas funciones internas como lo es conseguir routers, prefijos y parámetros, auto configuración de direcciones, resolución de direcciones, determinación del siguiente salto, detección de nodos no alcanzables, detección de direcciones duplicadas o cambios, redirección, balanceo de carga entrante entre otros.
- También le podemos retribuir a este protocolo la movilidad que posee ya que este permite que un nodo mantenga su dirección IP a pesar de su movilidad.

- IPv6 no es eterno, tiene un tiempo de vida de entre 60 y 100 años, sin embargo antes de estas fechas la internet tal y como la conocemos, y por tanto sus protocolos, habrán cambiado hacia otras técnicas.

REFERENCIAS

Adictos, L. (s.f.). Cómo elegir la distribución de Linux apropiada según el nivel de adaptación. Obtenido de Cómo elegir la distribución de Linux apropiada según el nivel de adaptación: http://www.linuxadictos.com/como-elegir-la-distribucion-de-linux-apropiada-segun-el-nivel-de-adaptacion.html

Aguas Bucheli, L. F. (2014). Estudio de la coexistencia de ipv4 con ipv6 a través del protocolo bgp en el laboratorio de tecnologías de información y comunicación de la facultad de ingeniería de la pontificia universidad católica del ecuador. Quito.

BIEEC. (s.f.). DSPACE EPN. Obtenido de DSPACE EPN: http://bieec.epn.edu.ec:8180/dspace/bitstream/123456789/797/4/T10140CAP3.pdf

Chile, I. (s.f.). IPv6 Chile. Obtenido de Categoría Silver de la certificación IPv6 Ready Logo será descontinuada en septiembre: http://www.ipv6.cl/noticia/categoria-silver-de-ipv6-ready-logo-sera-descontinuada

Core, N. (s.f.). Network Core. Obtenido de Network Core: http://www.network-core.net/2011/10/ospfv3-con-ipv6.html

Dhobsd. (s.f.). Dhobsd. Obtenido de Dhobsd: http://dhobsd.pasosdejesus.org/?id=Utilizaci%F3n+de+IPSEC

Electric, H. (s.f.). Hurricane Electric. Obtenido de Hurricane Electric: http://bgp.he.net/country/EC

Electrónica, A. (2012). Audiencia Electrónica. Obtenido de Audiencia Electrónica: http://www.audienciaelectronica.net/2012/06/12/descubra-cual-es-el-mejor-sistema-operativo-movil/

Gont, F. (s.f.). LACNIC.NET. Obtenido de LACNIC.NET: http://lacnic.net/documentos/seminarios/fgont-lacnic-seminario-virtual-seguridad-ipv6.pdf

IANA. (2013). IPv6 Global Unicast Address Assignments. Obtenido de IPv6 Global Unicast Address Assignments: http://www.iana.org/assignments/ipv6-unicast-address-assignments/ipv6-unicast-address-assignments.xhtml

IANA. (s.f.). Internet Protocol Version 6 Address Space. Obtenido de Internet Protocol Version 6 Address Space: http://www.iana.org/assignments/ipv6-address-space/ipv6-address-space.xml

Institute, I. (s.f.). Security Vulnerabilities. Obtenido de Security Vulnerabilities: http://resources.infosecinstitute.com/security-vulnerabilities-ipv6-tunnels/

Martínez, I. (2013). El Chapuzas Informático. Obtenido de El Chapuzas Informático: http://elchapuzasinformatico.com/2012/09/ripe-ncc-entrega-su-ultimo-bloque-de-direcciones-ipv4/ipv4-vs-ipv6/

Mkarich. (2013). Microsoft En Español. Obtenido de Microsoft En Español: http://blogs.technet.com/b/microsoftlatam/archive/2012/02/17/presentamos-el-nuevo-logo-de-windows.aspx

OpenStack. (2010). Sphinix. Obtenido de Sphinix: http://docs.openstack.org/developer/nova/devref/multinic.html

Oracle. (2010). Creación del esquema de numeración de IPv6. Obtenido de Creación del esquema de numeración de IPv6: http://docs.oracle.com/cd/E19957-01/820-2981/ipv6-planning-21/index.html

Profesor, L. W. (s.f.). La Web del Profesor. Obtenido de La Web del Profesor: http://webdelprofesor.ula.ve/ingenieria/gilberto/redes/04_conceptosBasicos2.pdf

Savinov, P. (2012). Integración de Java y .NET vía ActiveMQ. Obtenido de Integración de Java y .NET vía ActiveMQ: http://www.pavelsavinov.info/2012/08/blog-post.html

Smith, R. (2013). Expanding the Embedded Universe: Migrating From IPv4 to IPv6. Obtenido de Expanding the Embedded Universe: Migrating From IPv4 to IPv6: http://www.embedded.com/design/connectivity/4007677/Expanding-the-Embedded-Universe-Migrating-From-IPv4-to-IPv6

Techtectology. (s.f.). Techtectology. Obtenido de Techtectology: http://techtectology.blogspot.com/2012/01/mobile-ip-concept.html

Wiki, S. (s.f.). SixXS Wiki. Obtenido de SixXS Wiki: https://www.sixxs.net/wiki/Routers

Wikipedia. (s.f.). Routing Information Protocol. Obtenido de Routing Information Protocol: http://es.wikipedia.org/wiki/Routing_Information_Protocol

Young, S. (s.f.). Top 5 IPv6 Ready Wireless Routers. Obtenido de Top 5 IPv6 Ready Wireless Routers: http://www.broadbandbuyer.co.uk/Features/Article.asp?TextID=1425