PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR

FACULTAD DE INGENIERÍA

MAESTRÍA EN REDES DE COMUNICACIONES

TESIS DE GRADO PREVIO A LA OBTENCION DEL TÍTULO DE:

MAGISTER EN REDES DE COMUNICACIONES

TEMA:

"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 "

AUTOR: ING. LUIS FERNANDO AGUAS BUCHELI

DIRECTOR: ING. FRANCISCO RODRÍGUEZ CLAVIJO MSC.

QUITO, MARZO 2014

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.

La idea no es muy diferente con las tecnologías nuevas, ¡hay que subirse y pedalear! y sobre el tema de IPv6[1] 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.

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.

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

[1] IPv6: Protocolo de Internet versión 6

Dada la evidente contratación del aumento del ancho de banda con el CEDIA [2] para nuestro laboratorio, debemos incorporarnos analizando y planteando alternativas prácticas y viables de solución para la implementación de IPv6 en equipos y redes.

[2] CEDIA: Consorcio Ecuatoriano para el Desarrollo de Internet Avanzado

RESUMEN

En la actualidad IPv6 se está implementando lentamente en redes y coexistirá con IPv4[3] 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 uso. Lamentablemente, este proceso no se está realizando con la rapidez necesaria y puede tornarse en un gran desafío para el abordaje global integral ininterrumpido.

Si 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.

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.

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.

[3] IPv4: Protocolo de Internet versión 4

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. Sólo que en este caso en IPv6 es realmente rápida la asignación de IPs [4]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.

La importancia de este proyecto radica en plantear soluciones prácticas para la implementación del IPv6 en el diario vivir, lo cual permita adaptarnos de mejor manera al cambio que vendrá en estos años.

[4] IP: Una dirección IP es una etiqueta numérica que identifica, de manera lógica y jerárquica, a un interfaz (elemento de comunicación/conexión) de un dispositivo

DEDICATORIA

"Dedico este proyecto a mi Madre, ya que gracias a ella soy quien soy hoy en día, fue quién me dio ese cariño y calor humano necesario, quién ha velado por mi salud, mis estudios, mi educación alimentación entre otros, es ella a quien debo todo, horas de consejos , de regaños, de reprimendas de tristezas y de alegrías de las cuales estoy muy seguro que las han hecho con todo el amor del mundo para formarme como un ser integral y de las cuales me siento extremadamente orgulloso"

AGRADECIMIENTO

Quiero expresar mi agradecimiento

- A mis padres y hermanas por brindarme un hogar cálido y enseñarme que la perseverancia y el esfuerzo son el camino para lograr objetivos.

- A mi madre por su cariño, comprensión y constante estímulo, por su paciencia y por enseñarme a enfrentar los obstáculos con alegría.

- A mi Director de Tesis, Ing. Francisco Rodríguez por su generosidad al brindarme la oportunidad de recurrir a su capacidad y experiencia científica en un marco de confianza, afecto y amistad, fundamentales para la concreción de este trabajo.

- A los Ingenieros. Alberto Pazmiño y Oswaldo Espinoza, por sus valiosas sugerencias y acertados aportes durante el desarrollo de este trabajo.

- A mis ex - compañeros del COTAC por su continuo y afectuoso aliento.

- A mis ex – profesores del COTAC, por sus enseñanzas no he tenido problemas en la Universidad.

- A mis amigos y amigas actuales, quienes me ayudan con su apoyo, su comprensión y sobre todo me escuchan.

ÍNDICE DE CONTENIDOS:

ÍNDICE DE ILUSTRACIONES:

CAPÍTULO 1: MARCO TEÓRICO

1. ¿POR QUÉ SE ES NECESARIO UTILIZAR IPV6?

Hasta ahora hemos utilizado el protocolo IPv4, que nació para dar cobertura a todos los aparatos vigentes y, en teoría, futuros. IPv4 asignaba 4.294.967.296 (2 elevado a la potencia 32) direcciones de Red diferentes y se calcula que las direcciones pertenecientes al protocolo IPv4 disponibles en la reserva global de IANA, organismo encargado de asignarlas, se agotaron el jueves 3 de Febrero de 2011 oficialmente. Los Registros Regionales de Internet deben, desde ahora, manejarse con sus propias reservas, que se estima que alcanzarán hasta septiembre de 2011. Es aquí donde se ve clara la utilidad de un protocolo más avanzado y recomendado por la mayoría de los expertos en telecomunicaciones: IPv6.

La novedad fundamental de este sistema, creado en 1994, con respecto a su versión anterior es el aumento masivo de direcciones IP que, lógicamente, son más largas. Si las direcciones IP actuales constan de cuatro tercetos de cifras, las direcciones IPv6 son de 128 bits, esto es: están formadas por 32 dígitos hexadecimales. De esta forma, IPv6 puede generar unos 340 sextillones de direcciones, una cifra que, si no vuelven a fallar los cálculos, cubrirá con suficiencia las necesidades futuras de la Red.

1.1. ASPECTOS HISTÓRICOS

El Internet está basado en el protocolo IP, el cual permite la asignación de direcciones lógicas de todos los equipos que componen el Internet y de esta manera se permite la interoperabilidad entre

ellas. Actualmente se utiliza el direccionamiento IPv4, el cual no es muy nuevo, la verdad esta versión fue lanzada en el año de 1981 y desde esta fecha hasta hoy sigue vigente en el Internet. Para ese entonces se estimaba era suficiente la capacidad de direcciones que ofrece este protocolo sin embargo en los siguientes años el incremento de equipos conectados a Internet creció de manera sorprendente, por lo que surge ya la idea de que eventualmente las direcciones Ipv4 se agotarían.

Como parte experimental para mejorar el procesamiento de flujo de audio y video, se diseñó el protocolo IPv5, el cual no llegó a ser el sucesor de IPv4 por lo que se quedó en experimental.

Para 1992 las redes eran muy grandes, por lo que se comenzó a buscar mecanismos para mejorar los problemas de asignación de IP por un posible agotamiento en los años posteriores, es así que se crean los Protocolos IPng[1] creado por la IETF[2], el cual tenía la misión de ser el sucesor de IPv4, este protocolo es el que ahora conocemos como IPv6 el cual fue lanzado finalmente en el año 1999.

Con lo explicado anteriormente, nos damos cuenta que IPv6 ya cumple 13 años desde su lanzamiento, sin embargo al no ser compatible con IPv4, hasta ahora no se ha difundido como se esperaba. En el transcurso de esta investigación, seguiremos revisando varios motivos por el cual no se ha difundido este protocolo, así como cuál es el futuro de las comunicaciones con el uso del mismo.

[1] IPNG: Internet Protocol Next Generation. http://goo.gl/QjChl
[2] IETF: Internet Engineering Task Force. http://goo.gl/zH2k0

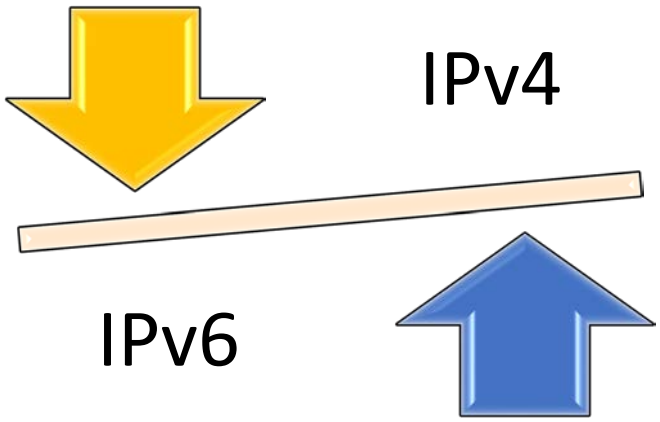

Ilustración 1: *Tendencia IPv4 vs IPv6, (Aguas Bucheli, 2014)*

1.2. ¿ES UNA OPCIÓN QUEDARNOS EN IPV4?

Definitivamente no, desde un sentido práctico, el espacio de direccionamiento de IPv4 es simplemente insuficiente, cada día que pasa las direcciones IPv4 se van agotando gracias a la gran demanda existente y esta demanda no hará otra cosa que seguir creciendo.

Desde un punto de vista técnico, IPv6 nos provee con un grupo de nuevas características que están más acorde a las necesidades tecnológicas de hoy. Entre otras cosas promete ser más seguro y está más preparado para el tipo de tráfico al que estamos empezando a acostumbrarnos.

Hoy en día no solo equipos como: computadores de escritorio, servidores o computadores portátiles necesitan estar conectados a Internet, pues actualmente cualquier equipo electrónico ve la

necesidad de hacerlo, por ejemplo: Electrodomésticos, consolas de juego, dispositivos móviles (celulares, tabletas), cámaras de video entre otros.

IPv6 promete estar mejor preparado para este crecimiento y los retos tecnológicos del mañana.

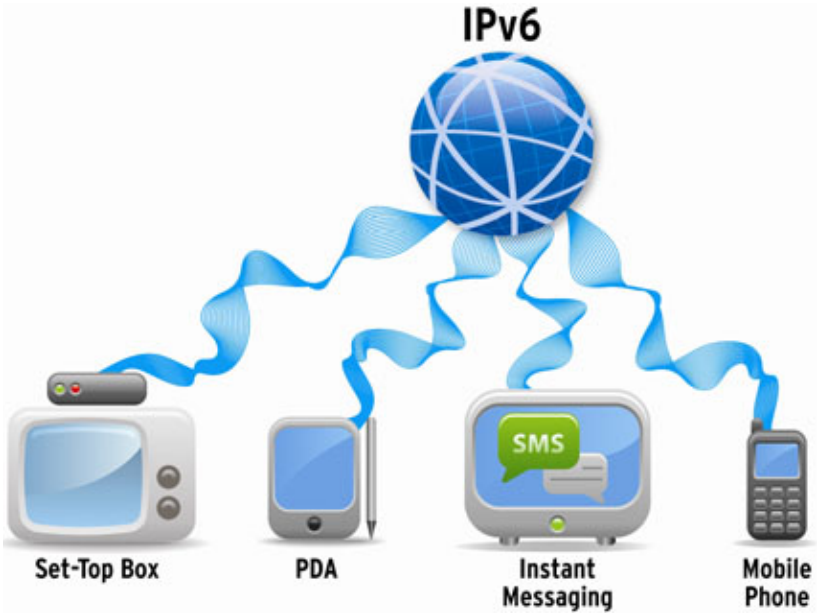

Ilustración 2: *Relación de IPv6 con los demás dispositivos, (Smith, 2013)*

1.3. PROPUESTA TEÓRICA Y COMPARACIÓN CON IPV4

La primera razón técnica entre los dos protocolos radica en el número de bits que se emplean para representar direcciones. En el protocolo IPv4, el número de bits empleados para representar una dirección está limitado a 32 bits, separados en cuatro bytes de ocho bits cada uno. Dada esta representación el límite teórico máximo de direcciones utilizables es de 2^{32} direcciones o cerca de 4300 millones de direcciones, de las cuales un porcentaje se desperdiciaba por los mecanismos especificados para pruebas/aplicaciones específicas. La representación de estos bytes para las personas que administran las redes operando en este

protocolo se denotan como cuatro octetos en nomenclatura decimal separados por puntos de la forma ###. ###. ###. ###, Donde cada octeto puede tomar valores entre cero y 255.

Por su parte el protocolo IPv6 emplea 128 bits para esta representación, otorgando un número enormemente más grande de direcciones máximas a ser empleadas. Este número podemos representarlo como $3.4x10^{38}$, por lo que sobra decir que esta capacidad de direcciones debiera ser suficiente para muchos años más de operaciones tecnológicas en el mundo.

El formato de direcciones en IPv6 se representa en forma hexadecimal mediante dieciséis campos separados por dos puntos (:), agregando algunas reglas para proveer un resumen en las direcciones y así proveer mecanismos de administración más simple. El formato de tal direccionamiento toma entonces el formato de ocho palabras de dieciséis bits cada una: AAAA: BBBB: CCCC: DDDD: EEEE: FFFF: GGGG: HHHH.

En este formato es posible realizar un abreviado de las direcciones cuando existan campos consecutivos de las palabras con valor cero. Esto es, por ejemplo, si se tiene la dirección 805B:2D9D:DC28:0000:0000:FC57:D4C8:1FFF, al aplicar la regla que acabamos de mencionar, la misma dirección se representaría como 805B:2D9D:DC28:FC57:D4C8:1FFF.

A esta convención se le denomina como compresión de ceros y sólo puede aplicarse en una ocasión en una dirección del formato IPv6.

La representación empleada para el direccionamiento de IPv6 tiene además algunas restricciones de asignación, según lo especifica IANA, organismo asignado para la administración de direcciones en el Internet y se simplifica en el cuadro a continuación[3]:

IPv6 Prefijo	Asignación	Referencia
0000::/8	IETF	RFC4291
0100::/8	IETF	RFC4291
0200::/7	IETF	RFC4048
0400::/6	IETF	RFC4291
0800::/5	IETF	RFC4291
1000::/4	IETF	RFC4291
2000::/3	Unicast	RFC4291
4000::/3	IETF	RFC4291
6000::/3	IETF	RFC4291
8000::/3	IETF	RFC4291
A000::/3	IETF	RFC4291
C000::/3	IETF	RFC4291
E000::/4	IETF	RFC4291
F000::/5	IETF	RFC4291
F800::/6	IETF	RFC4291
FC00::/7	Unicast	RFC4291

[3] Ref: http://goo.gl/FEfBm

FE00::/9	IETF	RFC4293
FE80::/10	Unicast	RFC4291
FEC0::/10	IETF	RFC3879
FF00::/8	Multicast	RFC4291

Tabla 1: *Asignación de Principales Prefijos de IPv6, (IANA, Internet Protocol Version 6 Address Space, s.f.)*

Los tipos de direcciones que encontramos en IPv6 son tres y nos sirven para identificar tanto origen como destino:

- Unicast: Son aquellas que representan una interface única hacia un sistema único a la vez. Los paquetes son enviados sólo a un destino.
- Multicast: Representa aquellos casos donde desde una interface se generan datagramas hacia varios destinos al mismo tiempo, pero no a todos.
- Anycast: Este representa un caso especial donde un paquete se envía a múltiples destinos, no a todos, solo algunos al mismo tiempo, seleccionados según convenga. Esta es una implementación única de IPv6.

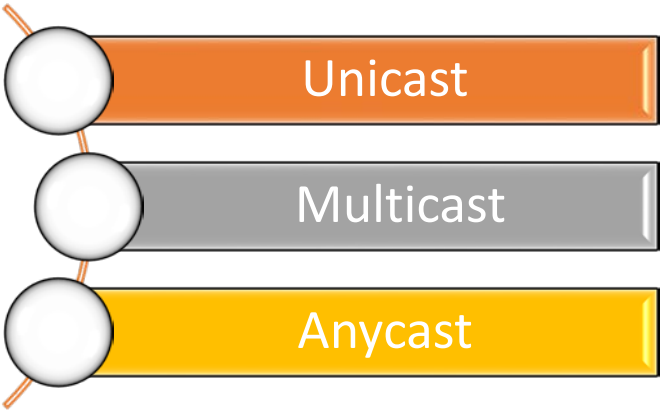

Ilustración 3: *Tipos de Direcciones en IPv6, (Aguas Bucheli, 2014)*

A diferencia de IPv4, no existe el concepto de broadcast[4], el cual estaba destinado para enviar un paquete a todos los dispositivos de la misma red (o subred si fuera el caso).

1.4. ENCABEZADO DE IPV4 VS. IPV6

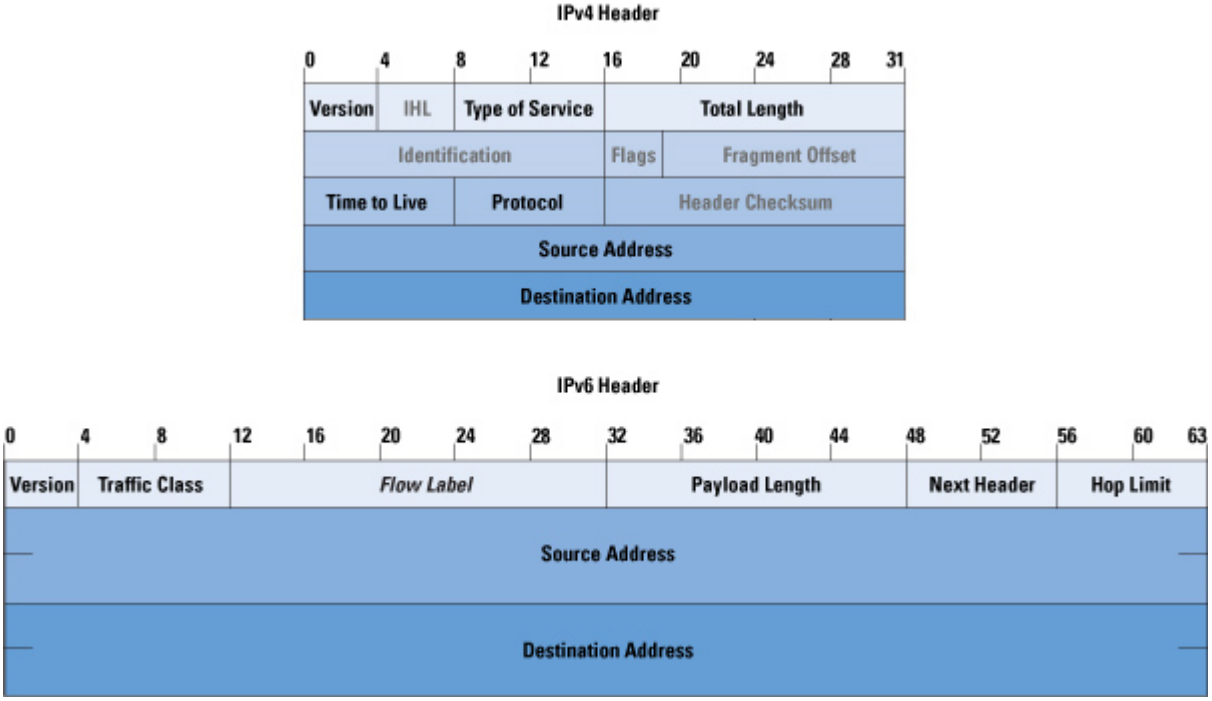

Ilustración 4: *Encabezados de IPv4 e IPv6, (Martínez, 2013)*

El encabezado IPv6 tiene un nuevo formato que está diseñado para reducir al mínimo la sobrecarga del encabezado. Esto se consigue al mover los campos que no son esenciales y los campos de opciones a encabezados de extensión que se colocan a continuación del encabezado IPv6. La simplificación del encabezado IPv6 permite un procesamiento más eficaz en los enrutadores

[4] Broadcast: Transmisión de datos que serán recibidos por todos los dispositivos en una red

intermedios.

Los encabezados IPv4 y los encabezados IPv6 no son interoperables y el protocolo IPv6 no es compatible con el protocolo IPv4. Un host o un enrutador deben utilizar simultáneamente una implementación de IPv4 e IPv6 para reconocer y procesar ambos formatos de encabezado. El nuevo encabezado IPv6 sólo tiene el doble de tamaño que el encabezado IPv4, a pesar de que las direcciones IPv6 son cuatro veces mayores que las direcciones IPv4.

Dentro de las especificaciones técnicas entre los dos protocolos, la primera diferencia que encontramos es el formato del encabezado de los paquetes entre los dos protocolos.

El primero de los campos del encabezado es la versión, la cual como es de esperarse se usaba con un valor 4 para IPv4 y debe usar 6 para el protocolo IPv6.

El segundo[5] de los campos es un valor de cuatro bits, el cual tiene dos esquemas de aplicación. El primero de ellos acorde al RFC 1883, se utiliza cuando desde la perspectiva del dispositivo que los envía, se puede controlar la congestión en el medio. Los usos de este campo se denotan como se indica a continuación:

[5] Aunque en IPv4 algunos de los campos tenían especificación para manejar calidad de servicio, ésta aplicación era rara vez habilitada por parte de los fabricantes de equipo de telecomunicaciones. En IPv6 ésta aplicación es forzosa

Valor	Tipo de tráfico
0	Tráfico no caracterizado
1	Tráfico de llenado de muy baja prioridad (Ejm: Noticias)
2	Transferencia de datos no atendida (Ejm: e-mail)
3	Uso reservado
4	Transferencia de datos masiva (Ejm: FTP[6] o NFS[7])
5	Uso reservado
6	Tráfico interactivo (Ejm: Telnet o terminal remota)
7	Tráfico de control de Internet (Ejm: protocolos ruteo)

Tabla 2: *Tráfico de IPv6, (Aguas Bucheli, 2014)*

El segundo método de aplicación de este campo se refiere a cuando el dispositivo que envía los datos no tiene control sobre la congestión del medio y por tanto se deben enviar los datagramas en forma continua para que lleguen al destino en forma continua. Los valores restantes de la tabla son los disponibles para este método.

El tercero de los campos del RFC 1883, se refiere al manejo de una etiqueta de flujo de los datos. Este campo se emplea para dar un tratamiento especial a los paquetes (desde la perspectiva del dispositivo que lo genera), ya sea unicast o multicast y tiene que ver con aplicaciones de uso futuro principalmente.

[6] FTP: Protocolo de Transferencia de Archivos

[7] NFS: Sistema de Archivos de Red

El cuarto de los campos del encabezado de los paquetes de IPv6 se podría traducir como carga y se refiere a la cantidad de datos que lleva el paquete. Dado que se emplean 16 bits para tal representación un solo paquete puede contener entonces hasta 65536 bytes de longitud. Una característica inherente en IPv6 es el tratamiento de paquetes jumbo, y en cuyo caso este campo se indica como cero y el valor verdadero deberá ser indicado en la extensión de encabezado llamada salto por salto.

El quinto de los campos se refiere a la identificación de un paquete posterior a ser enviado. El sexto campo se indica como límite de saltos y de manera análoga al campo TTL de IPv4 sirve para indicar el número máximo de dispositivos por los que ese paquete puede pasar antes de llegar al destinatario.

Los últimos dos campos del encabezado de IPv6 se emplean para indicar la dirección IP del origen (sexto campo) y la dirección IP del destino (séptimo campo).

1.5. NUEVAS CARACTERÍSTICAS DE IPV6

Además del espacio de direcciones más grande y nuevo formato del encabezado, IPv6 provee algunas mejoras y novedades respecto a IPv4:

- **Infraestructura de direcciones y enrutamiento eficaz y jerárquica.** Las direcciones globales de IPv6 que se utilizan en la parte IPv6 de Internet están diseñadas para crear una infraestructura eficaz, jerárquica y que se puede resumir y que tiene en cuenta la existencia de múltiples niveles

de proveedores de servicios Internet. En la red Internet IPv6, los enrutadores[8] de red troncal tienen tablas de enrutamiento mucho más pequeñas.

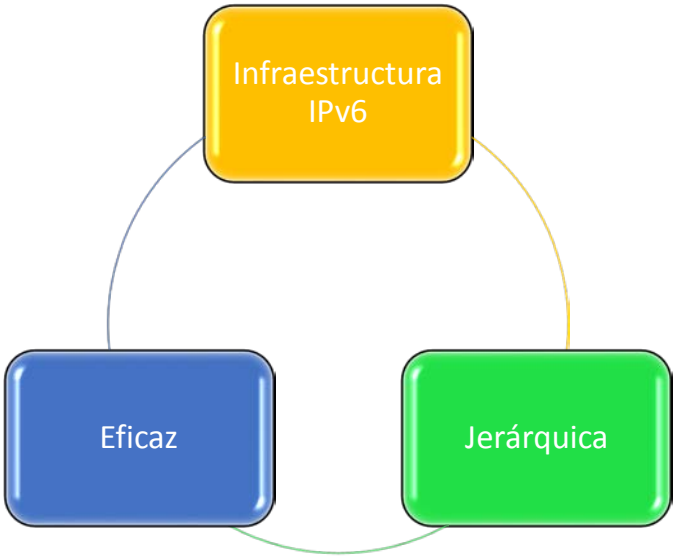

Ilustración 5: *Ventajas Infraestructura IPv6, (Aguas Bucheli, 2014)*

- **Configuración de direcciones con y sin estado.** Para simplificar la configuración de los hosts, IPv6 admite la configuración de direcciones con estado, como la configuración de direcciones con la presencia de un servidor DHCP[9], y la configuración de direcciones sin estado (configuración de direcciones sin la presencia de un servidor DHCP). Con la configuración de direcciones sin estado, los hosts de un vínculo se configuran automáticamente con direcciones IPv6 para el vínculo (direcciones locales del vínculo) y con direcciones derivadas de prefijos anunciados por los enrutadores locales. Incluso sin la presencia de un enrutador, los hosts del

[8] Enrutador: Es un dispositivo que proporciona conectividad
[9] DHCP: es un protocolo de red que permite a los clientes de una red IP obtener sus parámetros de configuración automáticamente

mismo vínculo se pueden configurar automáticamente con direcciones locales del vínculo y comunicarse sin necesidad de configuración manual.

Ilustración 6: *Estado de los Hosts, (Aguas Bucheli, 2014)*

- **Seguridad integrada.** La compatibilidad con IPSec[10] es un requisito del conjunto de protocolos IPv6. Este requisito proporciona una solución basada en estándares para las necesidades de seguridad de red y aumenta la interoperabilidad entre diferentes implementaciones de IPv6.

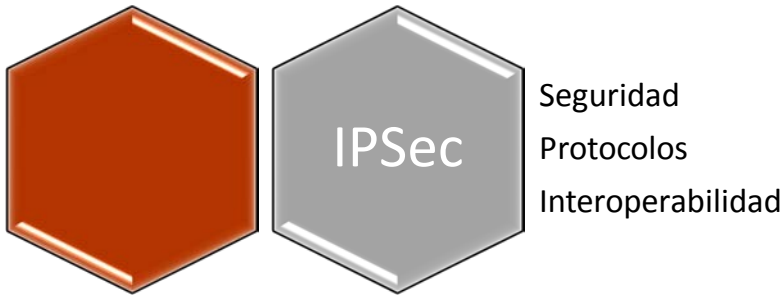

Ilustración 7: *Opciones IPSec, (Aguas Bucheli, 2014)*

[10] IPsec: Es un conjunto de protocolos cuya función es asegurar las comunicaciones

- **Mejora de la compatibilidad para la calidad de servicio (QoS).** Los nuevos campos del encabezado IPv6 definen cómo se controla e identifica el tráfico. La identificación del tráfico, mediante un campo *Flow Label* (etiqueta de flujo) en el encabezado, permite que los enrutadores identifiquen y proporcionen un control especial de los paquetes que pertenecen a un flujo dado. Un flujo es un grupo de paquetes entre un origen y un destino. Dado que el tráfico está identificado en el encabezado IPv6, la compatibilidad con QoS se puede obtener de forma sencilla incluso si la carga del paquete está cifrada con IPSec.

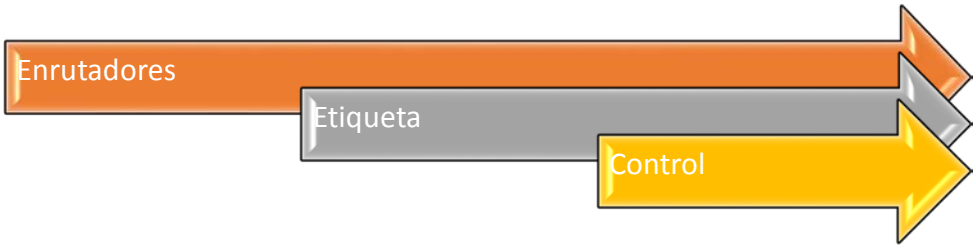

Ilustración 8: *Funciones Enrutadores, (Aguas Bucheli, 2014)*

- **Nuevo protocolo para la interacción de nodos vecinos.** El protocolo *Neighbor Discovery* o descubrimiento de vecinos en IPv6 consiste en un conjunto de mensajes del Protocolo de mensajes de control de Internet para IPv6 (ICMPv6, Internet Control Message Protocol for IPv6) que administran la interacción de nodos vecinos (es decir, nodos que se encuentran en el mismo vínculo). El descubrimiento de vecinos reemplaza los mensajes de Protocolo de resolución de direcciones (ARP, Address Resolution Protocol), Descubrimiento de enrutadores ICMPv4 y Redirección ICMPv4 con mensajes eficaces de multidifusión y unidifusión, y proporciona funciones adicionales.

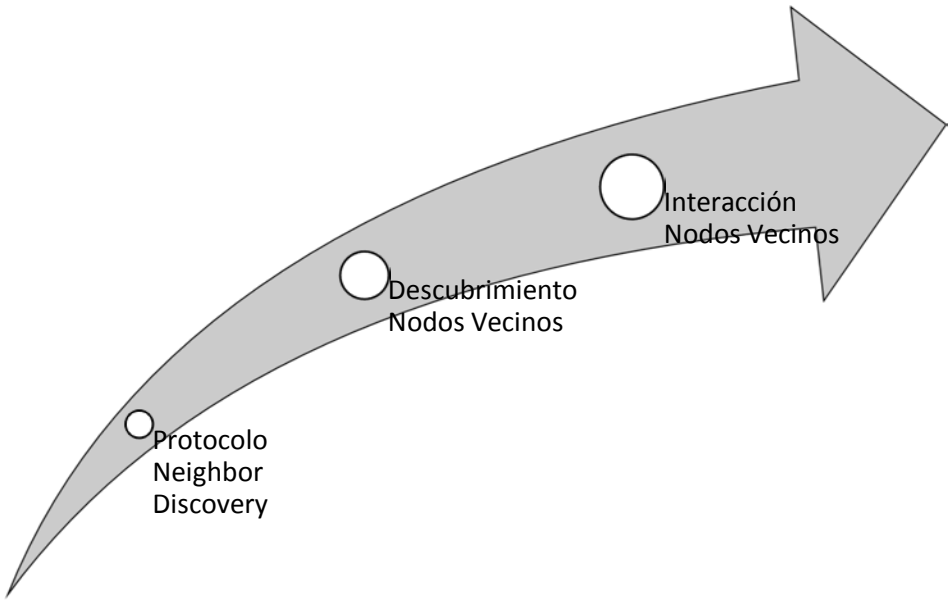

Ilustración 9: *Protocolo Neighbor Discovery para Nodos Vecinos, (Aguas Bucheli, 2014)*

- **Capacidad de ampliación.** IPv6 se puede ampliar con nuevas características al agregar encabezados de extensión a continuación del encabezado IPv6. A diferencia del encabezado IPv4, que sólo admite 40 bytes de opciones, el tamaño de los encabezados de extensión IPv6 sólo está limitado por el tamaño del paquete IPv6.

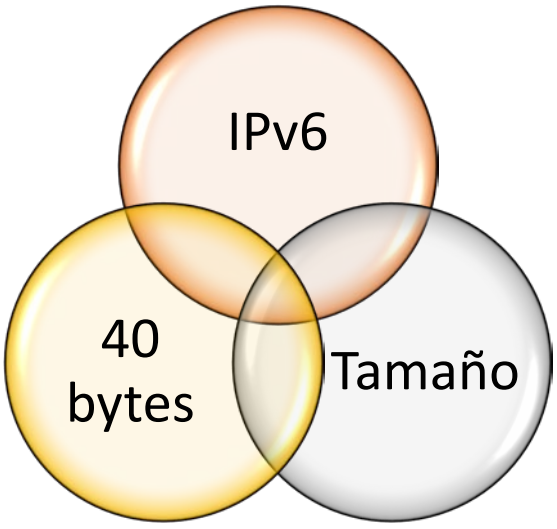

Ilustración 10: *Capacidad de Ampliación, (Aguas Bucheli, 2014)*

1.6. LA NUMERACIÓN EN IPV6

En la mayoría de los hosts, la configuración automática sin estado de direcciones IPv6 para sus interfaces constituye una estrategia válida y eficaz. Cuando el host recibe el prefijo de sitio del enrutador más próximo, el protocolo ND genera de forma automática direcciones IPv6 para cada interfaz del host.

Los servidores necesitan direcciones IPv6 estables. Si no configura manualmente las direcciones IPv6 de un servidor, siempre que se reemplaza una tarjeta NIC[11] del servidor se configura automáticamente una dirección IPv6

Prefijo de subred IPv4	Prefijo de subred IPv6 equivalente
192.168.1.0/24	2001:db8:3c4d:1::/64
192.168.2.0/24	2001:db8:3c4d:2::/64
192.168.3.0/24	2001:db8:3c4d:3::/64
192.168.4.0/24	2001:db8:3c4d:4::/64

Tabla 3: *Ejemplos de Prefijos de Subred IPv4 vs IPv6, (Oracle, 2010)*

1.7. PREFIJOS

Los campos que están más a la izquierda de una dirección IPv6 contienen el prefijo, que se emplea para enrutar paquetes de IPv6. Los prefijos de IPv6 tienen el formato siguiente:

[11] NIC: Tarjeta de interfaz de red

prefijo/tamaño en bits

El tamaño del prefijo se expresa en notación CIDR (enrutamiento entre dominios sin clase). La notación CIDR consiste en una barra inclinada al final de la dirección, seguida por el tamaño del prefijo en bits.

El prefijo de sitio de una dirección IPv6 ocupa como máximo los 48 bits de la parte más a la izquierda de la dirección IPv6. Por ejemplo, el prefijo de sitio de la dirección IPv6 **2001:db8:3c4d:0015:0000:0000:1a2f:1a2b/48** se ubica en los 48 bits que hay más a la izquierda, **2001:db8:3c4d. 2001:db8::/32** es un prefijo especial de IPv6 que se emplea específicamente en ejemplos de documentación También se puede especificar un prefijo de subred, que define la topología interna de la red respecto a un enrutador. La dirección IPv6 de ejemplo tiene el siguiente prefijo de subred: 2001:db8:3c4d:15::/64. El prefijo de subred siempre contiene 64 bits. Estos bits incluyen 48 del prefijo de sitio, además de 16 bits para el ID de subred.

Los prefijos siguientes se han reservado para usos especiales:

- **2002::/16:** Indica que sigue un prefijo de enrutamiento de 6to4.
- **fe80::/10:** Indica que sigue una dirección local de vínculo.
- **ff00::/8:** Indica que sigue una dirección multidifusión.

El siguiente gráfico muestra el formato de las direcciones global unicast.

Ilustración 11: *Direcciones Globales Unicast, (Oracle, 2010)*

Donde:

- **Prefijo de ruteo global.-** Es el prefijo asignado a un sitio, generalmente están estructurados por los RIRs e ISPs.
- **ID de subred.-** Es el identificador de una red, dentro de un sitio.
- **Identificador de Interfaz.-** Es el identificador de una interfaz, es de 64 bits.

Tomando en cuenta el ejemplo el gráfico podemos decir lo siguiente:

- n puede tener hasta 48 bits
- m es la resultado de la resta 64 - n
- y la interface de red tiene los 64 bits restantes de la dirección.

Prefijo	Designación	Whois	Status
2001:0000::/23	IANA[12]	whois.iana.org	ALLOCATED
2001:0200::/23	APNIC[13]	whois.apnic.net	ALLOCATED
2001:0400::/23	ARIN[14]	whois.arin.net	ALLOCATED
2001:0600::/23	RIPE NCC[15]	whois.ripe.net	ALLOCATED

[12] IANA: Es la entidad que supervisa la asignación global de direcciones IP.
[13] APNIC: Es un Registro Regional de Internet (RIR), y es una organización sin fines de lucro responsable de la administración y el registro.
[14] ARIN: Es el Registro Regional de Internet para América Anglosajona, varias islas de los océanos Pacífico y Atlántico
[15] RIPE NCC: Proporciona la coordinación administrativa de la infraestructura de Internet.

2001:0800::/23	RIPE NCC	whois.ripe.net	ALLOCATED
2001:0A00::/23	RIPE NCC	whois.ripe.net	ALLOCATED
2001:0C00::/23	APNIC	whois.apnic.net	ALLOCATED
2001:0E00::/23	APNIC	whois.apnic.net	ALLOCATED
2001:1200::/23	LACNIC[16]	whois.lacnic.net	ALLOCATED
2001:1400::/23	RIPE NCC	whois.ripe.net	ALLOCATED
2001:1600::/23	RIPE NCC	whois.ripe.net	ALLOCATED
2001:1800::/23	ARIN	whois.arin.net	ALLOCATED
2001:1A00::/23	RIPE NCC	whois.ripe.net	ALLOCATED
2001:1C00::/22	RIPE NCC	whois.ripe.net	ALLOCATED
2001:2000::/20	RIPE NCC	whois.ripe.net	ALLOCATED
2001:3000::/21	RIPE NCC	whois.ripe.net	ALLOCATED
2001:3800::/22	RIPE NCC	whois.ripe.net	ALLOCATED
2001:3C00::/22	IANA		RESERVED
2001:4000::/23	RIPE NCC	whois.ripe.net	ALLOCATED
2001:4200::/23	AFRINIC[17]	whois.afrinic.net	ALLOCATED
2001:4400::/23	APNIC	whois.apnic.net	ALLOCATED
2001:4600::/23	RIPE NCC	whois.ripe.net	ALLOCATED
2001:4800::/23	ARIN	whois.arin.net	ALLOCATED
2001:4A00::/23	RIPE NCC	whois.ripe.net	ALLOCATED
2001:4C00::/23	RIPE NCC	whois.ripe.net	ALLOCATED

[16] LACNIC: Registros de Direcciones de Internet para Latinoamérica y el Caribe.
[17] AFRINIC: Es el Registro Regional de Internet para África.

2001:5000::/20	RIPE NCC	whois.ripe.net	ALLOCATED
2001:8000::/19	APNIC	whois.apnic.net	ALLOCATED
2001:A000::/20	APNIC	whois.apnic.net	ALLOCATED
2001:B000::/20	APNIC	whois.apnic.net	ALLOCATED
2002:0000::/16	6to4[18]		ALLOCATED
2003:0000::/18	RIPE NCC	whois.ripe.net	ALLOCATED
2400:0000::/12	APNIC	whois.apnic.net	ALLOCATED
2600:0000::/12	ARIN	whois.arin.net	ALLOCATED
2610:0000::/23	ARIN	whois.arin.net	ALLOCATED
2620:0000::/23	ARIN	whois.arin.net	ALLOCATED
2800:0000::/12	LACNIC	whois.lacnic.net	ALLOCATED
2A00:0000::/12	RIPE NCC	whois.ripe.net	ALLOCATED
2C00:0000::/12	AFRINIC	whois.afrinic.net	ALLOCATED
2D00:0000::/8	IANA		RESERVED
2E00:0000::/7	IANA		RESERVED
3000:0000::/4	IANA		RESERVED
3ffe::/16	IANA		RESERVED
5f00::/8	IANA		RESERVED

Tabla 4: *Asignación IANA direcciones Unicast, (IANA, IPv6 Global Unicast Address Assignments, 2013)*

[18] 6to4: Es un sistema que permite enviar paquetes IPv6 sobre redes IPv4 obviando la necesidad de configurar túneles manualmente.

Dentro de este tema se ha desatado una polémica sobre las asignaciones que se darían, tanto a las empresas como a los clientes home, sin embargo podemos explicar las tendencias de las mismas.

ISP. Se entiende se les asignará un /32 lo que se entiende que para cada red pueden tener 2^{96} direcciones (7.922816251×10^{28} aproximadamente) que si lo comparamos con el número total de direcciones IPv4 actual de todo el mundo (4294967296 aproximadamente) son mucho pero mucho más.

Empresas. Tomando en cuenta que los últimos 64 bits serán utilizados para los host, decimos que se tiene dos variantes de asignación:

- **/56.** Esto quiere decir que de los 64 bits primeros - los 56 que demanda esta variante, nos quedan 8 bits que servirían para la creación de subredes. 2^8 = 256 subredes y cada una de ellas con 2^{64} = 1.844674407×10^{19} números de host.
- **/48.** A nuestro criterio será la que finalmente triunfe sobre la estudiada anteriormente, esta significa que tendremos 64 - 48 = 16 bits para subredes. 2^{16} = 65536 subredes de cada una de ellas con 2^{64}= 1.844674407×10^{19} números de host.

Home. Se presume que existe la tendencia de asignación /64 para todo lo que tiene que ser home, pero entendiendo esto, decimos que tendremos UNA SOLA RED, pero con la capacidad de 2^{64}= 1.844674407×10^{19} números de host.

Como podemos darnos cuenta, nosotros tendríamos en nuestros hogares una asignación /64 que significa poder usar un número de direcciones mucho más grande que las existentes en todo el

planeta actualmente, esto se lo puede ver como una ventaja si hablamos de seguridad por ejemplo... ya que escanear un rango de IP demasiado grande, será muy lento y poco factible de que se lo haga, así que lo podemos tomar como otra de las ventajas del direccionamiento IPv6.

Estas son las tendencias que se están dando en el tema de asignación de direcciones IPv6, veremos en qué termina esto, pero de lo que podemos estar casi seguros, es que no harán falta direcciones al menos hasta que nuestra generación y tal vez algunas más por debajo de nosotros existan en el planeta.

1.8. ENRUTAMIENTO

El enrutamiento de IPv6 es muy similar por no decir idéntico al de IPv4 en la dirección de enrutamiento entre dominios sin clase (CIDR). La única diferencia es que direcciones de IPv6 son de 128 bits, en lugar de IPv4 de 32 bits.

Por lo tanto tenemos disponible los protocolos de enrutamiento de IPV4, también para IPv6 como son: OSPF, RIP, IDRP e IS-IS

Las direcciones IPv6 son asignadas a interfaces, no a nodos, por lo que cada interface de un nodo necesita al menos una dirección unicast. A una sola interfase se le pueden asignar múltiples direcciones IPv6 de cualquier tipo (unicast, anycast, multicast). Por lo cual un nodo puede ser identificado por la dirección de cualquiera de sus interfaces.

Existe la posibilidad de asignar una dirección unicast a múltiples interfaces para balanceo de cargas.

Una dirección típica de IPv6 consiste de tres partes como se muestra en la figura de abajo:

- El prefijo de enrutamiento global
- El Identificador de subred
- El Identificador de interface

Ilustración 12: *Estructura de una dirección IPv6, (Aguas Bucheli, 2014)*

Con esta introducción, podemos decir que el enrutamiento de IPv6 se basa en lo siguiente:

- La coincidencia del mayor prefijo.
- El posible uso de enrutamiento fuente.
- Re direcciona con ICMP.
- Los mismos protocolos de enrutamiento que IPv4: RIP, OSPF, IS-IS y BGP.

Rutas Estáticas.

Son utilizadas para forzar el enrutamiento de algunos prefijos a través de ruteadores específicos. La ruta por omisión (::/0) es un ejemplo de ruta estática. Las rutas estáticas en una tabla de

enrutamiento tienen una mayor preferencia sobre rutas aprendidas por protocolos de enrutamiento.

Una ruta estática contiene el prefijo a ser enrutado y la dirección IP del ruteador. Dicha ruta tiene como nombre el siguiente salto, es el responsable de enrutar cualquier paquete con un destino dentro del rango de prefijo dado. No existen diferencias entre IPv4 e IPv6 para las rutas estáticas, sin embargo, se debe usar una dirección de enlace local como la dirección de siguiente salto.

RIP (Routing Information Protocol)

RFC 1058. Es un protocolo para redes de tamaño de pequeño a mediano. La versión mejorada para IPv6 conocida como RIP Siguiente Generación (RIPng, RIP next generation) (RFC 2080 y 2081) está basada en RIP versión 2 (RFC 1723) y hereda las mismas características genéricas:

- Algoritmo vector-distancia Bellman-Ford.
- Actualizaciones cada 30 segundos.
- Tiempo de expiración de 180 segundos para rutas desconectadas.
- Métricas fijas.
- Diámetro de red de 15 saltos.
- Horizonte dividido y envenenamiento en reversa de trayectoria.
- Etiquetas de ruta.

Nuevas características de RIPng.

Característica	Descripción
Rutas Anunciada	RIPng anuncia rutas IPv6 compuestas de prefijos IPv6 con longitud y métrica.
Siguiente Salto	La dirección de Siguiente Salto es la dirección de enlace local IPv6 de la interfase del ruteador que anuncia el prefijo.
Transporte de Protocolo IP	IPv6 es utilizado para llevar datagramas RIP usando UDP como protocolo de transporte.
Dirección IPv6 Fuente	La actualización RIP de la dirección fuente IPv6 es la dirección de enlace-local de la interfase del ruteador fuente. Con excepción de cuando se contesta un Mensaje de Solicitud unicast desde un puerto distinto al puerto RIPng, en dicho caso, la dirección fuente es una dirección global válida).
Dirección IPv6 Destino	La dirección destino de la actualización RIP es FF02::9, que es la dirección multidifusión de todos los ruteadores RIP. Únicamente los ruteadores RIPng atienden esta dirección multidifusión. Es una dirección multidifusión con alcance de enlace-local, la cual no es retransmitida a otros enlaces.
Límite de Salto = 255	Las actualizaciones RIP tienen el Límite de Salto de paquete IPv6 configurado en 255. Esto permite a los involucrados verificar si las actualizaciones vienen de ruteadores externos falsos.
Número de Puerto = 521	El puerto UDP es 521, en lugar de 520 para RIPv1 y 2.

RIPng versión = 1	El número de versión RIPng en el paquete RIP es 1, lo que representa que es la primera versión de RIPng. Se utiliza un puerto de transporte distinto. Los involucrados pueden diferenciar entre paquetes RIPv1, RIPv2 y RIPng.
Tabla de Enrutamiento	La tabla de enrutamiento de Pv6 es distinta de la tabla de enrutamiento de IPv4 para RIPv1 o RIPv 2. La ruta por omisión es anunciada como ::/0.
Autenticación	La autenticación RIPng se basa en la seguridad proveída por IPSec.

Tabla 5: *Nuevas características RIPng, (Wikipedia, s.f.)*

OSPF. (Open Shortest Path Firts)

RFC 2328. OSPFv2, es un protocolo sólo para IPv4. OSPFv3 (RFC 2740) es un protocolo de red independiente, similar a IS-IS. De esta manera puede incluir rutas IPv6. OSPFv3 comparte los fundamentos de OSPFv2. Este protocolo tiene las siguientes características:

- Inundación (flooding).
- Elección de ruteador designado.
- Área de soporte.
- Cálculos de Djikstra para abrir la trayectoria más corta primero.
- Soporte de circuito en demanda.

Nuevas características de OSPFv3

Características	Descripción
LSAs de ruteador y red	Estos no tienen semántica de direccionamiento y sólo llevan información de topología.
Nuevo LSA-con-Prefijo-Intra-Area	Este lleva direcciones y prefijos IPv6.
Direcciones en LSA	Estas son descritas como prefijo con una longitud de prefijo. La ruta por omisión es ::/0.
Identificación de Ruteador	ID del Ruteador es un valor de 32 bit sin importar si es dirección IPv4 o IPv6. Se usa en DR, BDR, LSAs, base de datos.
Alcance de la Inundación	Enlace, Area o AS.
Siguiente-Salto	La dirección de Siguiente-Salto es la dirección de enlace-local IPv6 de la interfase de ruteador que anuncia el prefijo.
Nuevo LSA de Enlace-Local	Este lleva la dirección de enlace local de la interfase de ruteador, los prefijos del enlace y las opciones.
Ejecución por cada enlace, en lugar de cada IP de subred	Ahora una interfase OSPF se puede conectar a un enlace en lugar de una subred IP. Están soportadas múltiples instancias en un enlace sencillo.
Usa IPv6 para el transporte de paquetes OSPF	Encabezado Siguiente = 89 para identificar un paquete IPv6 OSPFv3.
Paquetes OSPF con dirección IPv6 fuente	La dirección fuente del paquete OSPF es la dirección enlace-local de la interfase del ruteador origen.

Paquetes OSPF con dirección IPv6 destino	Todos los ruteadores OSPF envían paquetes Hello y atienden a FF02::/5, que es la dirección multidifusión con enlace a todos-los-ruteadores-ospf.
Límite de Salto = 1 de paquetes OSPF	1 significa de enlace-local.
OSPF versión = 3	Versiones previas son iguales a 1 o 2.
La Autenticación es realizada con IPSec	Se quitaron todos los datos de autenticación interna OSPF y ahora se provee seguridad con IPSec para proteger la integridad y ofrecer autenticación.

Tabla 6: *OSPF con IPv6, (Core, s.f.)*

1.9. DETALLE DE LOS PRINCIPALES DISPOSITIVOS Y SOS "IPV6 READY"

El IPv6 ready es el programa internacional de certificación de productos IPv6 gestionado por el comité de logo IPv6 Ready, que define las especificaciones de las pruebas de cumplimiento e interoperatibilidad que deben cumplir dispositivos y sistemas para poder declararlo (Chile, s.f.).

Ilustración 13: *IPv6 Ready, (Young, s.f.)*

1.9.1. DISPOSITIVOS

Existen marcas populares como son: D-Link, Linksys y Belkin, las mismas que no han demostrado apoyo en a IPv6 en un futuro inmediato. Una solución para implementar IPv6 en estas marcas, es cambiando de firmware construidos por terceros como: OpenWrt, DD-WRT y Sveasoft.

Finalmente podemos decir que si un equipo es IPv6 ready, no se asume que puede funcionar para conectarse mediante un túnel, hay que asegurarse mirando detenidamente las características de los mismo.

El siguiente link, tiene una lista muy extensa (alrededor de 600 modelos), de ruteadores que soportan IPv6, sin embargo a continuación ofrecemos una lista de los más relevantes.[19]

Modelos Home:

Nombre	**Fabricante**
Airport Extreme	Apple
Time Capsule	Apple
ARxxx	Allied Telesis
Fritz!Box WLAN 3270	AVM
Fritz!Box Fon WLAN 7270	AVM

[19] Referencia: http://www.sixxs.net/wiki/Routers

Fritz!Box Fon WLAN 7340	AVM
Fritz!Box Fon WLAN 7390	AVM
Fritz!Box Fon WLAN 7570 VDSL	AVM
FRITZ!Box 6360 Cable	AVM
WHR-HP-AG108	Buffalo Technology
WZR-AG300NH	Buffalo Technology
WBMR-G54	Buffalo Technology
Cisco 827	Cisco
Cisco 83x	Cisco
Cisco 87x	Cisco
DIR-615	D-Link
DIR-825	D-Link
Vigor 2130	DrayTek
bintec RS-Series	Funkwerk Enterprise Communications
bintec R-Series	Funkwerk Enterprise Communications
ScreenOS 5.0	Juniper Networks
RVS4000	Lnksys
Linksys E-Series	Cisco(Linksys)
Sonicwall TZ	Sonicwall

EW-652BRP	Trendnet
TEW-639GR	Trendnet
Zyxel Keenetic series (Classic, 4G,Lite, Giga)	ZyXEL

Tabla 7: *Dispositivos Home Parte 1, (Wiki, s.f.)*

Nombre	**Fabricante**
Cisco ASA	Cisco
Cisco PIX	Cisco
Cisco 1700	Cisco
Fortigate	Fortinet
A-MSRx0 series	HP
JunOS	Juniper Networks
PA series	Palo Alto Networks
Mikrotik Routerboard	Mikrotik
Sonicwall NSA series	Sonicwall
Netlron XMR series	Brocade

Tabla 8: *Dispositivos Home Parte 2, (Wiki, s.f.)*

1.9.2. SISTEMAS OPERATIVOS Y SISTEMAS EMBEBIDOS

IPv6 no es una tecnología que nació hace dos o tres años, sino desde la década de los noventas estaba ya su desarrollo, es por esta razón que los fabricantes de hardware como de software, comenzaron a soportar a IPv6.

En lo que tiene que ver a sistemas operativos, en la actualidad la mayoría por no decir todos, tiene soporte de IPv6, es así que a continuación vamos a enumerar los sistemas operativos más usados e indicar desde la versión que soportan IPv6.

Windows.

En versiones de servidores, tenemos el soporte a IPv6 de: Windows server 2003 y 2008.

En versiones para equipos de escritorio, tenemos el soporte de IPv6de: Windows XP (desde Service Pack 2), Windows Vista, Windows 7 y Windows 8.

También la versión para dispositivos móviles (Windows Mobile), tiene soporte de IPv6.

Ilustración 14: *Versiones Windows, (Mkarich, 2013)*

Linux.

Este Sistema Operativo, tiene muchas variantes dependiendo de las Distribuciones que existen, sin embargo citaremos las más importantes y el soporte de IPv6:

- Linux RedHat (7 o superior)
- Linux SUSE (10 o superior)
- Linux Fedora
- Linux Ubuntu
- Debian
- FreeBSD

Ilustración 15: *Versiones Linux, (Adictos, s.f.)*

Existen otros sistemas Operativos que de igual manera soportan IPv6, estos son: Mac OS, Sun Solaris (8 a superior), Symbiam (7 o superior).

Sabemos que tenemos sistemas operativos que manejan los dispositivos de hardware, entre ellos tenemos: Cisco, Jupiter, Huawei, etc. De igual manera ya tienen porte de IPv6.

Ilustración 16: *Sistemas Móviles, (Electrónica, 2012)*

Finalmente podemos señalar las plataformas de desarrollo que tienen soporte de IPv6, estas son:

- Java SDK
- .Net Framework 1.1 o superior.

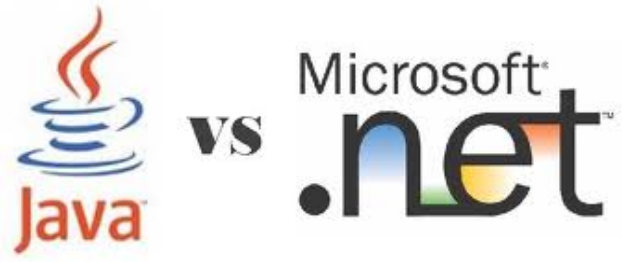

Ilustración 17: *Java vs .Net, (Savinov, 2012)*

Como podemos concluir, a nivel de software, tenemos un amplio soporte a esta tecnología por lo que en este caso no tendremos inconvenientes para poder implementar IPv6.

1.10. RADVD

El Demonio de Anuncio de Enrutador (radvd por sus siglas en inglés) es un producto de software de código abierto que implementa el anunciamiento en enlaces locales de direcciones de enrutadores IPv6 y prefijos de enrutado IPv6, usando el Protocolo de Descubrimiento de Vecinos (NDP) que describimos más adelante. El Demonio de Anuncio de Enrutador es usado por los administradores de sistemas en los métodos *stateless*[20] de configuración de equipos de red, en redes IPv6.

Cuando los equipos IPv6 configuran sus interfaces de red, éstos emiten pedidos de solicitud de enrutador (RS) hacia la red, para descubrir los enrutadores disponibles. El software de radvd responde estos pedidos con mensajes de anuncio de enrutador (RA). Adicionalmente, radvd periódicamente emite paquetes RA al enlace adjunto para actualizar los equipos de red. Los mensajes de anuncio de enrutador contienen el prefijo de enrutado usado en el enlace, la unidad máxima de transmisión (MTU) del enlace y la dirección del enrutador predeterminado responsable.

[20] Stateless: Método usado para confirmación de envío y recepción

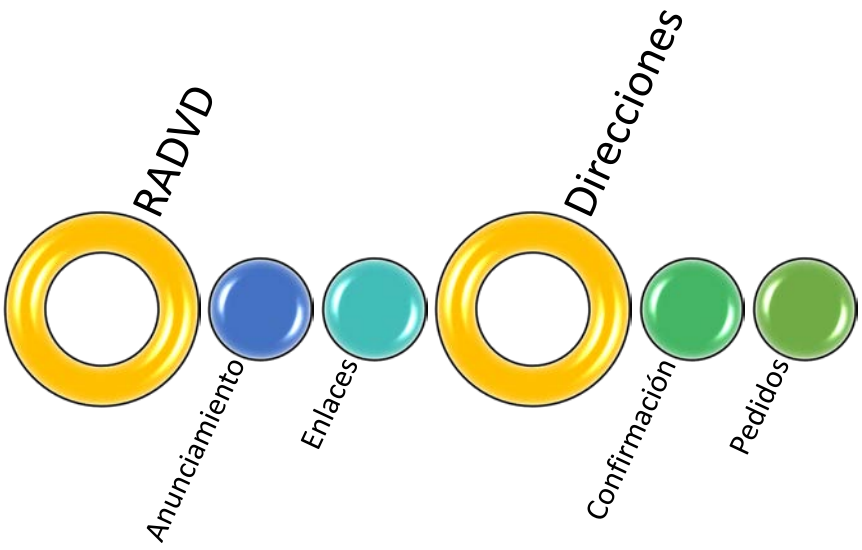

Ilustración 18: *RADVD, (Aguas Bucheli, 2014)*

1.11. ASPECTOS IMPORTANTES DEL PROTOCOLO NDP

NDP (Neighbor Discovery Protocol) es un protocolo del conjunto de protocolos de Internet, usado en IPv6 que opera en la capa de Internet del modelo de Internet y es responsable de:

- La autoconfiguración de direcciones de los nodos,
- El descubrimiento de otros nodos en el enlace,
- La determinación de las direcciones de capa de enlace de otros nodos,
- La detección de direcciones duplicadas,
- Encontrar enrutadores y servidores DNS disponibles,
- Descubrir prefijos de direcciones y

- El mantenimiento de la accesibilidad de información sobre las rutas a otros nodos vecinos activos.

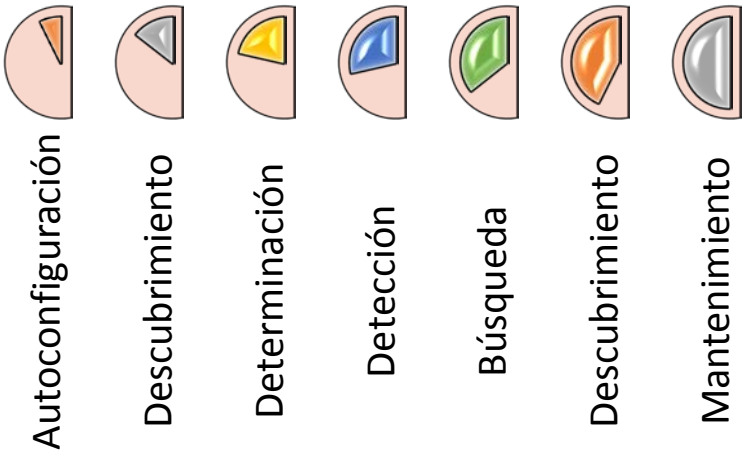

Ilustración 19: *Fases Protocolo NDP, (Aguas Bucheli, 2014)*

El protocolo define cinco diferentes tipos de paquetes ICMPv6 para ejecutar funciones para IPv6, similares a las de los protocolos ARP, descubrimiento de enrutador por ICMP y Redireccionamiento de Enrutador en IPv4. Sin embargo, provee muchas mejoras sobre sus contrapartes IPv4, por ejemplo, incluye Detección de Vecino Inalcanzable (NUD por sus siglas en Inglés), mejorando así la robustez de la entrega de paquetes en la presencia de fallas en enrutadores, enlaces o nodos móviles.

Los 5 tipos de paquetes ICMPv6 que define son:

- Router Solicitation
- Router Advertisement
- Neighbor Solicitation

- Neighbor Advertisement
- Redirect

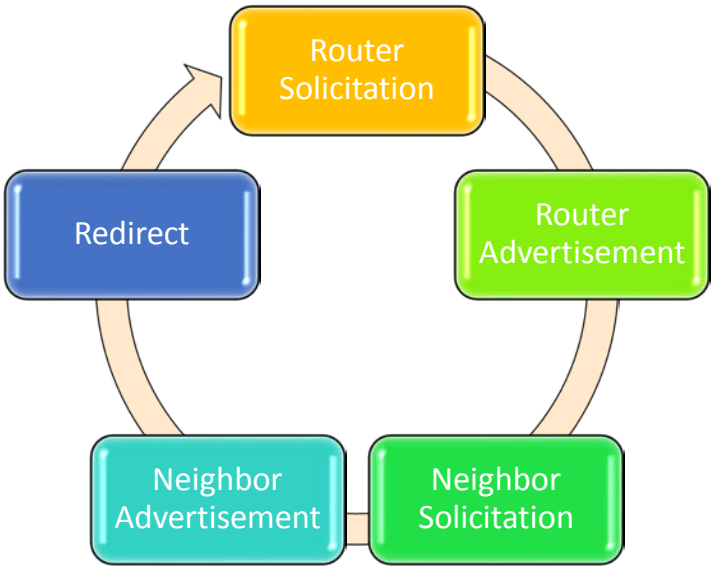

Ilustración 20: *Paquetes definidos por ICMPv6, (Aguas Bucheli, 2014)*

Estos mensajes son usados para proveer las siguientes funcionalidades:

- Descubrimiento de Enrutador: los equipos puedes localizar enrutadores residentes en los enlaces adjuntos.
- Descubrimiento de prefijo: los equipos puedes descubrir prefijos de direcciones que están en el enlace para los enlaces adjuntos.
- Descubrimiento de parámetros: los equipos pueden encontrar los parámetros del enlace (por ejemplo, MTU).
- Configuración automática de direcciones: configuración de direcciones sin estado de interfaces de red.

- Resolución de direcciones: mapeo entre las direcciones IP y las direcciones de capa de enlace.
- Determinación de salto siguiente: los equipos pueden encontrar el enrutador de siguiente-salto para cierto destino.
- Detección de vecinos inalcanzables (NUD): determina que un vecino ya no es accesible en el enlace.
- Detección de direcciones duplicadas (DAD): los nodos pueden comprobar si una dirección ya está en uso.
- Re direccionamiento: el enrutador puede informar a un nodo sobre el mejor enrutador de primer-salto.
- Asignación de Servidor DNS recursivo (RDNSS) y Lista de Búsqueda de DNS (DNSSL) a través de una opción de anuncio de enrutador (RA). Se trata de una característica nueva y no está ampliamente soportada por los clientes.

1.12. DIFERENCIAS ENTRE RADVD Y DHCP6

RADVD permite sólo distribuir el prefijo y la longitud del prefijo. No permite distribuir otra información como servidores DNS o NTP y no permite mantener direcciones fijas IPv6 centralizadas. RADVD es un protocolo sin estado, como resultado, no requiere mucho poder de CPU como en el caso de DHCP, además, a diferencia de DHCP, no requiere mantener una base de datos de los "préstamos" de direcciones que son realizados. Si no se requiere toda aquella configuración de servidores de tiempo/DNS/otros sincronizada en una red grande, entonces correr radvd puede ayudar a deshacerse de la sobrecarga de mantenimiento y procesamiento que de todas formas no se requeriría.

Un servidor DHCP debe mantener la pista de las direcciones que ha entregado a los clientes. Entonces, debe grabar en un medio de almacenamiento persistente, cada "préstamo" que entregue; lo cual dificulta la implementación de DHCP en enrutadores sin disco.

Con RADVD, el enrutador simplemente emite la información de prefijo y los nodos escogen una dirección IP por sí solos. No existe un estado en el enrutador, entonces si el enrutador colapsa, no existe estado que recuperar.

Nótese que en IPv6 se puede combinar RADVD con DHCPv6 y entonces usar RADVD para la configuración de direcciones y DHCPv6 para configurar otros datos como DNS, NTP, etc. Pero al menos en cuanto a los servidores DNS, RDNSS que mencionamos unos párrafos más arriba, podría ser una salida al uso de DHCPv6.

Ilustración 21: *RADVD y DHCP, (Aguas Bucheli, 2014)*

1.13. VULNERABILIDAD

Algunos ruteadores tienen una vulnerabilidad al negociar con el protocolo NDP. Frecuentemente, los enrutadores tienen muchas menos entradas NDP disponibles que las posibles direcciones en la red IPv6 (típicamente 2^{64} o más).

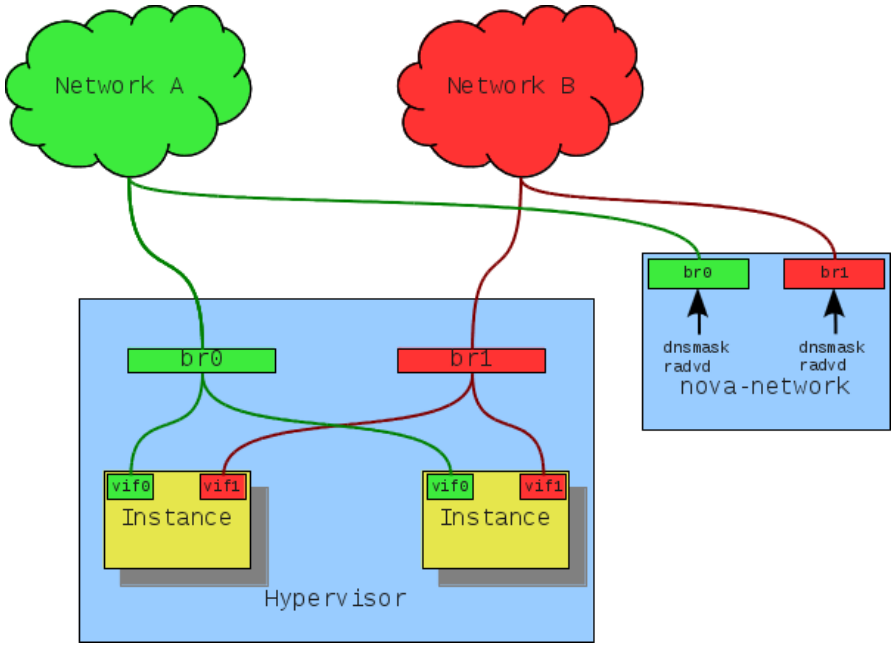

Ilustración 22: *Comportamiento RADVD en dos redes 1, (OpenStack, 2010)*

Los sistemas Windows, a partir de la versión Vista, soportan nativamente IPv6 y lo traen activado por defecto, sin embargo el procesamiento del tráfico de mensajes RA consume recursos excesivamente, por lo que incluso una pequeña-mediana inundación de paquetes de este tipo, puede provocar un colapso total del sistema .

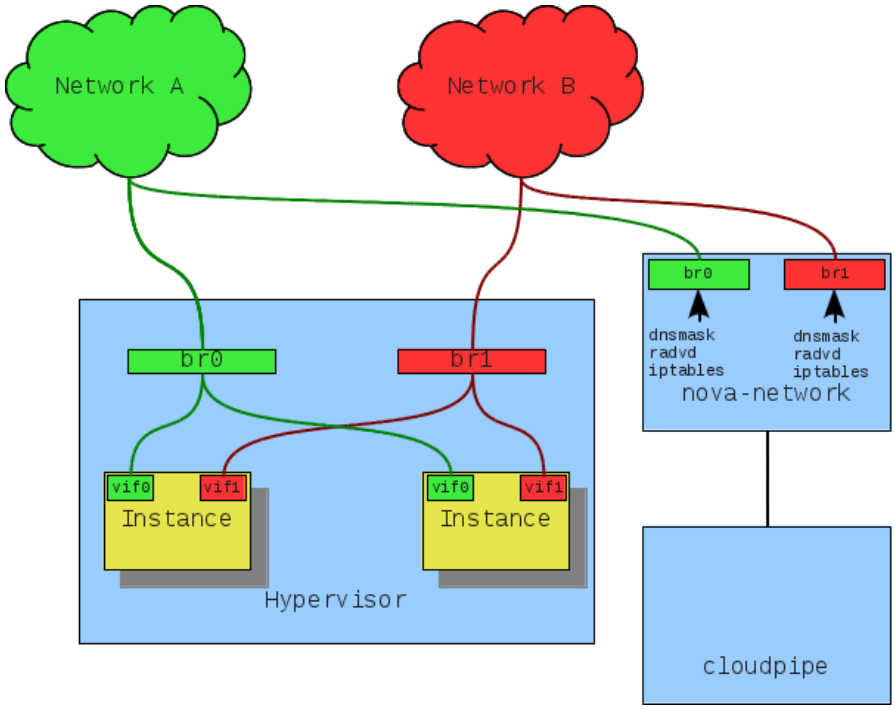

Ilustración 23: *Comportamiento RADVD en dos redes 1, (OpenStack, 2010)*

1.14. SEGURIDAD EN IPV6

El Internet está agotando su espacio y, como resultado, está a punto de someterse a una transición importante para ampliar el número de direcciones en línea disponibles. Esta transición es desde el actual protocolo IP versión 4 al nuevo estándar IP versión 6. Las empresas necesitan saber y entender esta transición, ya que habrá nuevos problemas de seguridad en el período intermedio.

Aunque una de las promesas de IPv6 es de más seguridad, IPv4 se ha ganado su reputación en las últimas décadas, y nos hemos familiarizado con lo que puede y no puede hacer. Por otro lado, se tiene poca o ninguna experiencia con IPv6 en el mundo real. En papel, IPv6 parece ser excelente,

pero es seguro que lo mismo sucedió con el Titanic. En el mejor de los casos, IPv6 ofrece mejor seguridad pero no la garantiza. (Gont, s.f.)

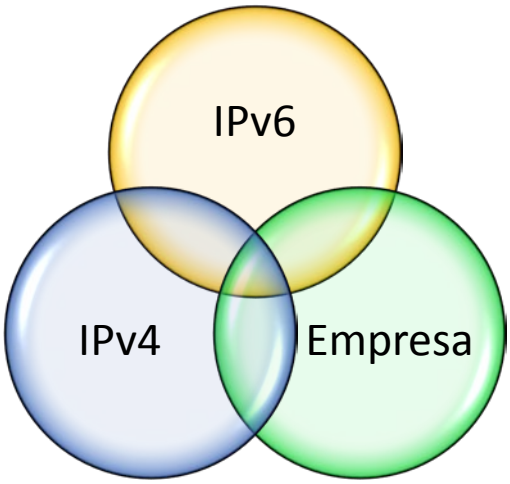

Ilustración 24: *Componentes para la seguridad hacia IPv6, (Aguas Bucheli, 2014)*

Caso en cuestión: IPSec. Esencialmente, esto asegura la comunicación IP al encriptar y autenticar paquetes IP. En IPv4, era una característica opcional; en IPv6, es obligatoria. Volver una característica obligatoria, no significa que tendrá un amplio soporte; el punto es que IPv6 no es automáticamente más seguro. Va a tomar mucha preparación de pre-lanzamiento y una inmensa cantidad de vigilancia de seguridad para ejecutarla correctamente.

Para las empresas, hay mucho que considerar, y esto muy seguramente cae en la responsabilidad del Jefe de Seguridad de la Oficina.

1.14.1. IPSEC

Lo primero que debemos señalar, es que históricamente no fue tomado en cuenta la seguridad en ninguna de las capas que forman la estructura TCP/IP, sin embargo con el incremento de equipos conectados a Internet y con el aumento de las funcionalidades adoptadas en este medio de comunicación masivo, cada día se comenzó a notar la necesidad de implementar la seguridad en las redes, por supuesto otro de los factores primordiales, es que comenzaron a existir ataques a diferentes servidores de: bancos, universidades, instituciones de estado, inclusive a la NASA; por lo que se comenzó a tomar en serio a la seguridad.

Sin embargo existió la reacción tardía en modificar los protocolos de los servicios para implementar seguridad, por lo que surgieron soluciones comerciales como SSL (Secure Sockets Layer o SEL (Secure Electronic Transaction) y así con el uso de estos protocolos los usuarios puedan experimentar la seguridad en Internet.

Con la necesidad de ir adoptando todos los protocolos para implementar la seguridad, se optó por introducir una serie de especificaciones para garantizar la seguridad de manera implícita en los protocolos. Estas especificaciones es lo que conocemos como IP Security o IPsec.

Uno de los primeros problemas que tuvieron que solventar estas especificaciones especiales, fue concordar en qué capa era la idónea para trabajar, finalmente para evitar duplicidades con las soluciones comerciales y que puedan trabajar en todas las capas se optó por incluirle en el nivel más bajo de la pila de protocolos esto quiere decir la implementación de estas especificaciones en el protocolo IP versión 6.

Las especificaciones al trabajar en la capa inferior de protocolos TCP/IP, funcionando a nivel de datagramas y así siendo independientes de los protocolos que trabajan en capas superiores.

IPsec proporciona la seguridad mediante dos criterios:

- **Cabecera de autenticación (AH. Authentication Header):** Verifica que los datagramas provienen del origen especificado y que los datagramas no hayan sido modificados.

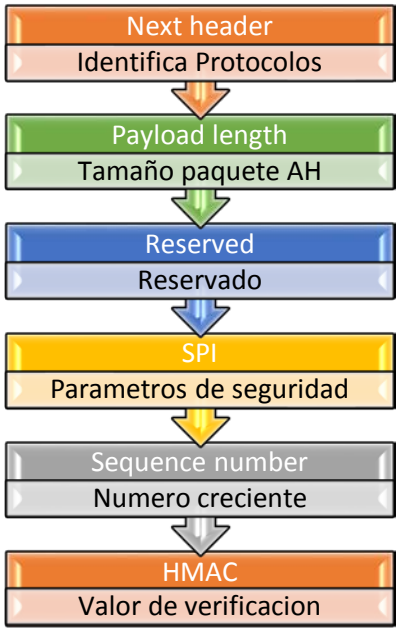

Ilustración 25: *Campos de la Cabecera de Autenticación, (Aguas Bucheli, 2014)*

- **Cifrado de Seguridad ESP. Encapsulated Security Payload.:** Se garantiza que sólo el legítimo destinatario pueda descifrar el contenido del datagrama.

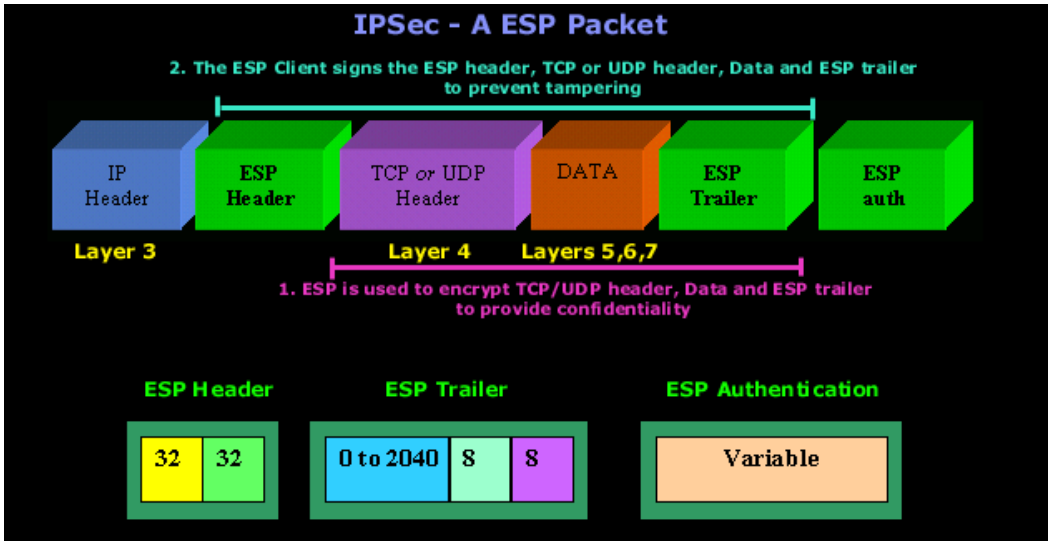

Ilustración 26: *Cifrado de Seguridad, (BIEEC, s.f.)*

Se debe indicar que tanto el emisor como el receptor, comparten una clave con el algoritmo de cifrado/descifrado y adicional el tiempo de validez de la clave, lo cual diferencia considerablemente una comunicación segura con otra.

1.14.2. FUNCIONAMIENTO DE IPSEC EN IPV6

En IPv6, existen dos modos para el funcionamiento de IPsec:

1.- Modo Transporte

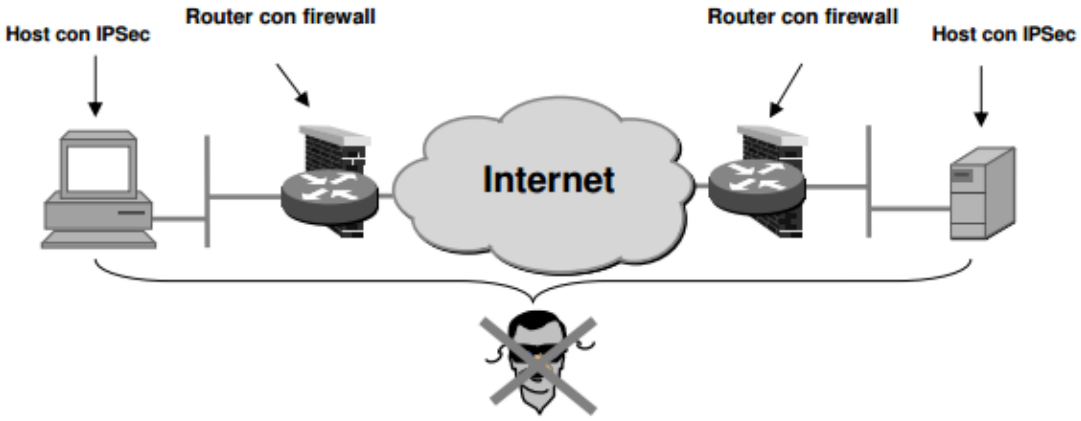

Ilustración 27: *Modo Transporte, (Dhobsd, s.f.)*

Como se muestra en la figura, en el modo transporte debemos implementar IPsec en los dos extremos de la conexión, esto es en los host, por lo tanto los dos equipos deben conocer e interpretar IPsec.

- **AH en modo transporte.**

Se inserta después de la cabecera IP y antes de los protocolos de la capa superior (UDP, TCP, ICMP, etc)

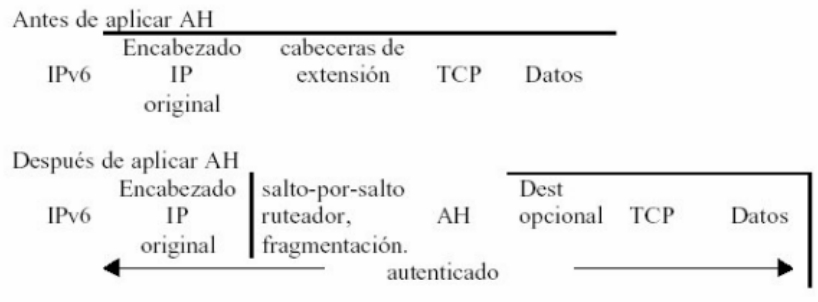

Ilustración 28: *AH en modo transporte, (Profesor, s.f.)*

- **ESP en modo transporte**

Al igual que el modo AH, se inserta después de la cabezera IP y antes de los protocolos de capa superior (UDP, TCP, ICMP, etc).

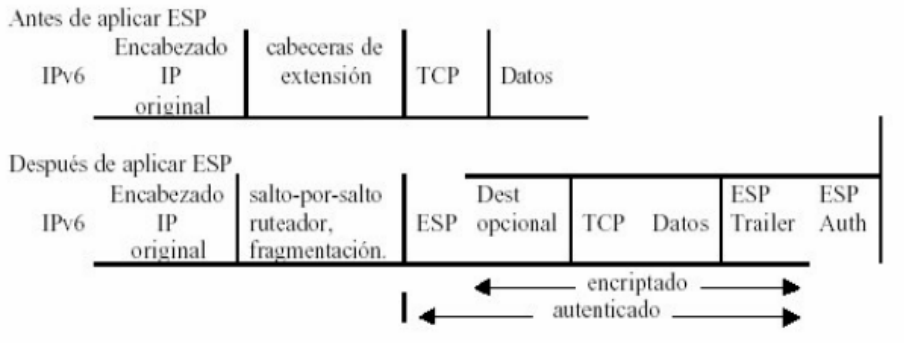

Ilustración 29: *ESP en modo transporte, (Profesor, s.f.)*

2.- Modo Túnel

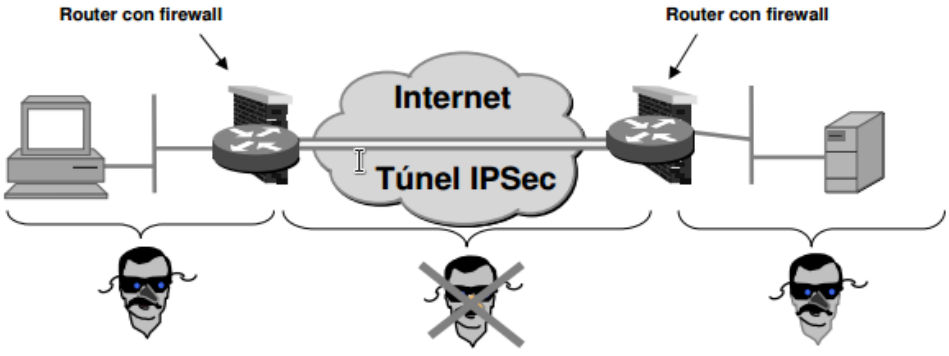

Ilustración 30: *Modo Túnel, (Dhobsd, s.f.)*

En este caso como muestra la figura, el IPsec se lo implementa en los routers que tienen el firewall, lo que permite la creación de un túnel entre ellos, en este modo, no se requiere que los equipos a los extremos (host), estén implementados con IPsec.

La característica de este modo es que cuando usamos ESP, se puede ocultar la identidad de los nodos que se están comunicando.

Es implementado principalmente en ruteadores que sirven como puerta de enlace, y mediante este modo, podemos tener una de las funcionalidades interesantes de IPsec que son las VPN.

- **AH en modo túnel**

En este modo, la cabecera interna posee el origen y destinos finales, mientras que la cabecera externa (la identificada por los ruteadores) incluye direcciones distintas.

La cabecera AH, protege a toda la cabecera interna.

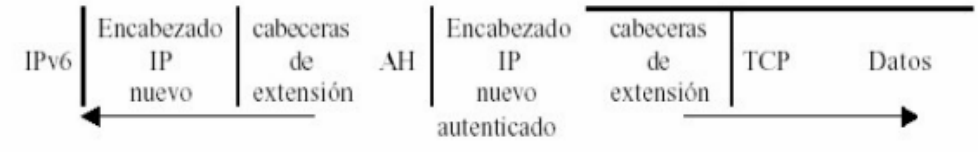

Ilustración 31: *AH en modo túnel, (Profesor, s.f.)*

- **ESP en modo túnel**

Al igual que el AH, tiene la cabecera interna con las direcciones de origen y destino final y la cabecera externa.

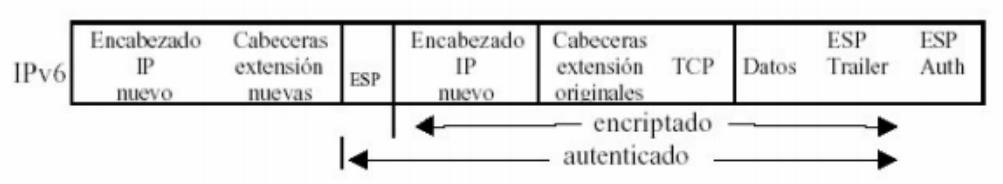

Ilustración 32: *ESP en modo túnel, (Profesor, s.f.)*

Finalmente podemos indicar los métodos de trabajo en los cuales se puede implementar IPsec con IPv6.

- **Seguridad extremo a extremo.-** Es también conocida de host a host y la seguridad adquirida es alta, ya que se tiene el control de los extremos.
- **VPN.-** Es uno de los métodos más usados y se refiere a la creación de un túnel en un medio no seguro.
- **Road Warrior.-** Puede ser un tipo de VPN, que permite acceder desde un equipo remoto a una red empresarial usando un medio no seguro mediante la generación de un túnel

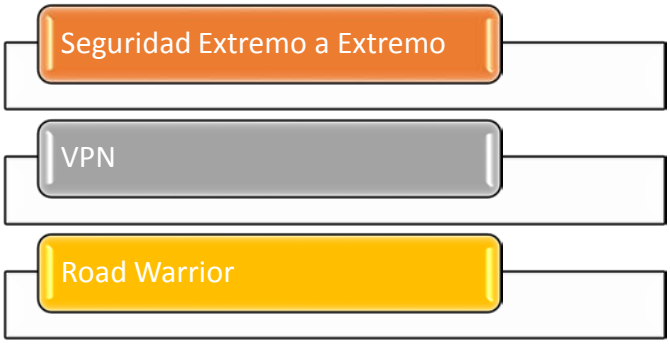

Ilustración 33: *Métodos de trabajo IPsec, (Aguas Bucheli, 2014)*

1.15. MOBILE IP, MOBILE IPV6.

Mobile IP o IP móvil o movilidad IP, es un protocolo de comunicaciones estándar de la IETF diseñado para permitir a los usuarios de dispositivos móviles moverse de una red a otra manteniendo una dirección IP permanente. En realidad el protocolo existe tanto para IPv4 (RFC 5944) como para IPv6 (RFC 6275) pero en esta última es que el protocolo encuentra el escenario propicio para su funcionamiento.

El protocolo Mobile IP permite el enrutamiento de datagramas IP en el internet independientemente de la ubicación. Cada nodo móvil es identificado por su dirección doméstica sin importar su localización real en el Internet. Mientras que fuera de su red doméstica, un nodo móvil está asociado con una dirección de custodia (CoA[21]) que identifica su ubicación actual y su dirección doméstica está asociada con el extremo local de un túnel a su agente doméstico. Mobile IP especifica cómo un nodo móvil se registra con su agente doméstico y cómo el agente doméstico enruta los datagramas al nodo móvil a través del túnel.

[21] Care of Address. http://goo.gl/Qk1ly

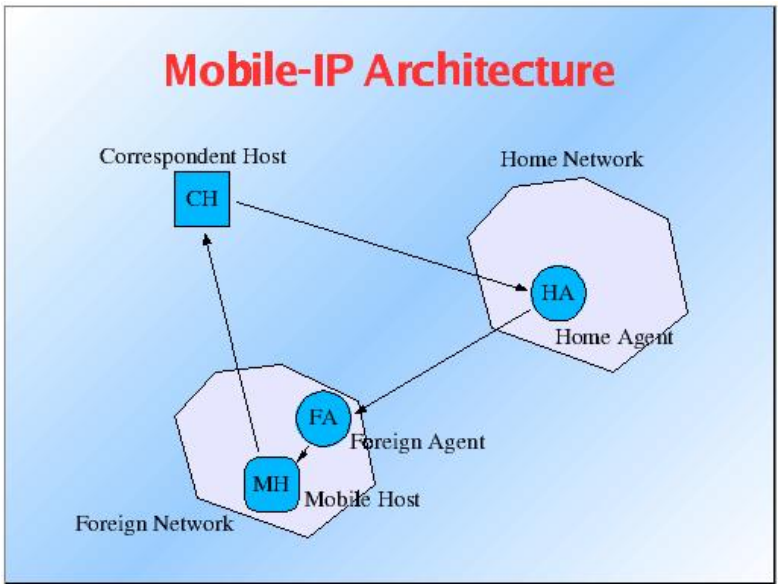

Ilustración 34: *Arquitectura IP Mobile, (Techtectology, s.f.)*

Su utilidad está clara pues en muchas aplicaciones como VPN y VoIP, cambios repentinos en la conectividad de red y direcciones IP pueden obviamente causar problemas. Mobile IP fue diseñado para soportar una conectividad a Internet fluida y constante. Se encuentra más frecuentemente en entornos cableados e inalámbricos donde los usuarios necesitan llevar sus dispositivos móviles a través de múltiples subredes LAN. Ejemplos de la utilización aparecen en la itinerancia entre el sistema inalámbrico superpuesto, por ejemplo, IP sobre DVB, WLAN, WiMAX y BWA.

Un nodo móvil tiene dos direcciones: una dirección doméstica permanente y una dirección de custodia (CoA), la cual está asociada con la red que el nodo móvil está visitando. Dos clases de entidades comprenden una implementación Mobile IP:

- Un agente doméstico almacena la información acerca de los nodos móviles cuyas direcciones domésticas permanentes están en la red del agente doméstico.
- Un agente foráneo almacena la información acerca de los nodos móviles que están visitando su red. Los agentes foráneos también anuncian las direcciones de custodia que son usadas por Mobile IP. Si no existe un agente foráneo en la red anfitriona, el dispositivo móvil debe encargarse de obtener una dirección y anunciarla por sus propios medios.

Un nodo esperando comunicarse con el nodo móvil, usa la dirección doméstica permanente del nodo móvil como dirección de destino para enviar los paquetes. Dado que la dirección doméstica lógicamente pertenece a la red asociada con el agente doméstico, mecanismos normales de enrutamiento IP reenvían estos paquetes al agente doméstico. En lugar de reenviar estos paquetes al destino que está físicamente en la misma red que el agente doméstico, el agente doméstico re direcciona estos paquetes hacia la dirección remota a través de un túnel IP, encapsulando el datagrama con un nuevo encabezado IP, usando la CoA del nodo móvil.

Cuando actúa como un transmisor, un nodo móvil envía paquetes directamente al otro nodo comunicante, sin enviar los paquetes a través del agente doméstico, usando su dirección doméstica permanente como la dirección origen para los paquetes IP. Esto es conocido como enrutamiento triangular. De ser necesario, el agente foráneo puede emplear un túnel inverso, tunelizando los paquetes del nodo móvil al agente doméstico, quien en respuesta los reenviará al nodo comunicante. Esto es necesario en redes cuyos enrutadores chequean que la dirección IP de origen del host móvil pertenezca a su subred o de lo contrario descartará los paquetes.

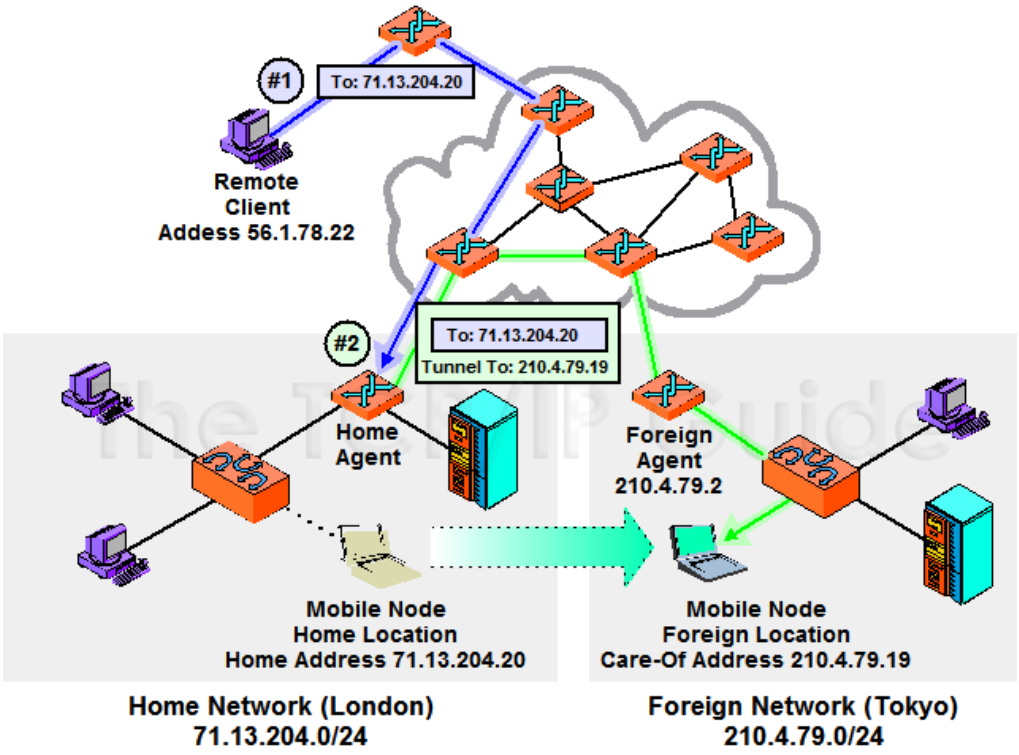

Ilustración 35: *Ejemplo de una red con mobile ip, (Techtectology, s.f.)*

Están en desarrollo algunas mejoras a la técnica Mobile IP, tales como Mobile IPv6 y Hierarchical Mobile IPv6 (HMIPv6[22]), para mejorar las comunicaciones móviles en ciertas circunstancias, haciendo el proceso más seguro y más eficiente.

Adicionalmente, en el propio protocolo IPv6 se han implementado cambios para soportar de mejor forma IPv6 Móvil, tales como:

- Un grupo de opciones de movilidad para ser incluidos en mensajes móviles.
- Una nueva opción de Dirección Doméstica para el encabezado de Opciones de Destino.

[22] Más detalles sobre HMIPv6 en: http://goo.gl/2IkyU

- Un nuevo encabezado de enrutamiento de tipo 2
- Nuevos mensajes del Protocolo de Mensajes de Control de Internet para IPv6 (ICMPv6) para descubrimiento del conjunto de agentes domésticos y obtención del prefijo del enlace doméstico.
- Cambios a los mensajes y opciones de descubrimiento de enrutadores y opciones adicionales de Descubrimiento de Vecinos.

Los investigadores están también trabajando en crear el soporte para redes móviles entre subredes completas con soporte desde Mobile IPv6. Un ejemplo de aquello es Network Mobility (NEMO) y Network Mobility Basic Support Protocol de la IETF Network Mobility Working Group, que soporta la movilidad para redes móviles completas que se mueven y anexan a través de diferentes puntos en el Internet. El protocolo es una extensión de Mobile IPv6 y permite mantener la continuidad de las sesiones para cada nodo en la Red Móvil según la red se vaya moviendo.

1.16. BGP

BGP se diseñó para permitir la cooperación en el intercambio de información de encaminamiento entre dispositivos, llamados pasarelas, en sistemas autónomos diferentes. El protocolo opera en términos de mensajes, que se envían utilizando TCP[23]. El repertorio de mensajes es el siguiente:

1.- Open

2.- Update

[23] TCP: Protocolo de Transporte.

3.- Keepalive

4.- Notification

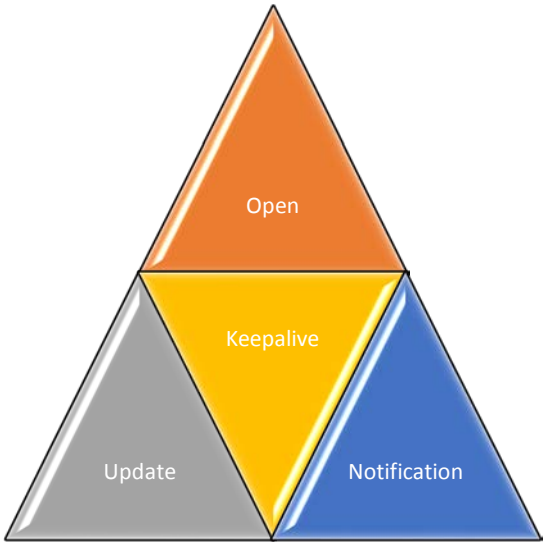

Ilustración 36: *Repertorio de Mensajes BGP, (Aguas Bucheli, 2014)*

BGP supone tres procedimientos funcionales:

- Adquisición de vecino.
- Detección de vecino alcanzable.
- Detección de red alcanzable.

Ilustración 37: *Procedimientos Funcionales BGP, (Aguas Bucheli, 2014)*

En el protocolo de adquisición de vecino, un dispositivo envía un mensaje de petición al otro, el cual puede aceptar o rechazar el ofrecimiento. El protocolo no indica cómo puede saber un dispositivo la dirección o incluso la existencia de otro dispositivo de encaminamiento. Estas cuestiones se tratan en el momento de establecer la configuración del sistema o por una intervención activa del gestor de la red.

Para llevar a cabo la adquisición de vecino, un dispositivo envía al otro un mensaje OPEN. Si el otro dispositivo acepta la relación, envía un mensaje de KEEPALIVE.

Una vez establecida la relación de vecino, se utiliza el procedimiento de detección de vecino alcanzable para mantener la relación. Este procedimiento consiste en enviarse entre los dos vecinos periódicamente mensajes de KEEPALIVE para asegurarse de que la relación sigue establecida.

El último procedimiento especificado por BGP es la detección de red alcanzable. Cada dispositivo de encaminamiento mantiene una base de datos con las redes que puede alcanzar y la ruta preferida para llegar hasta esa red. Siempre que se realiza un cambio en esa base de datos, el dispositivo de almacenamiento envía un mensaje de UPDATE por difusión a todos los dispositivos de encaminamiento que implementan BGP.

CAPÍTULO 2: METODOLOGÍA

2. MECANISMOS DE TRANSICIÓN A IPV6

Una de las premisas del diseño de IPv6, fue que pudiera realizarse una transición suave hacia la nueva versión del protocolo IP, sin que fuera necesario pasar de una versión a otra en forma abrupta. Con esta idea en mente, se diseñaron muchos mecanismos que pudieran ayudar a la convivencia entre ambas versiones.

Si bien en un comienzo se pensó que la adopción gradual de IPv6 crecería lo suficiente como para ir desplazando a IPv4 antes de su agotamiento, esto no sucedió así, razón por la cual estos mecanismos de transición tienen hoy en día una relevancia incluso mayor. Podemos hacer una clasificación general entre los mecanismos de transición de acuerdo al tipo de técnica que se utiliza:

- Dual stack
- Túneles
- Traducción

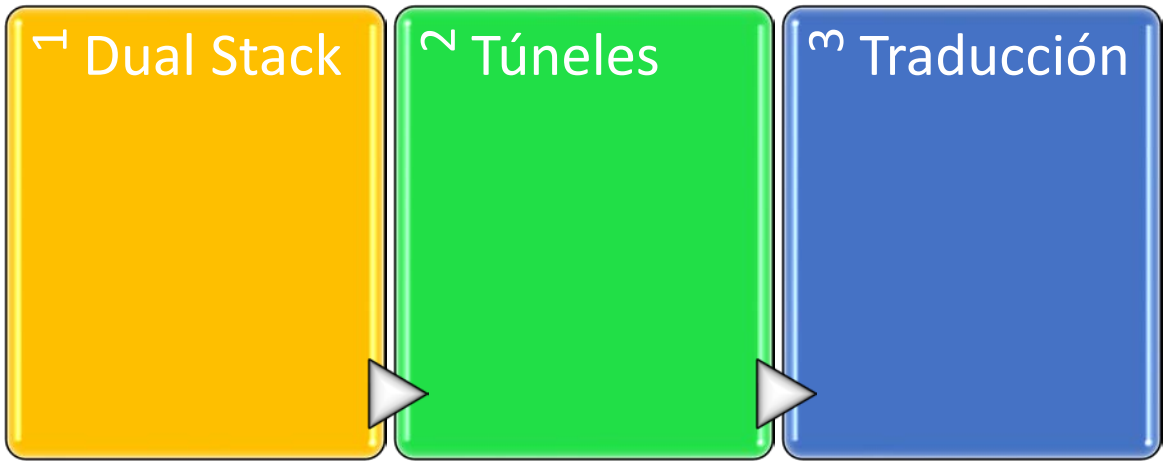

Ilustración 38: *Mecanismos IPv6, (Aguas Bucheli, 2014)*

También es posible hacer una división entre los mecanismos de transición según estén basados en una infraestructura mayoritariamente IPv4 o IPv6: si bien en un comienzo teníamos redes IPv4 que iban incorporando el acceso a IPv6 gradualmente, a medida que el agotamiento de IPv4 se extiende, los proveedores comienzan a pensar en redes de acceso exclusivamente IPv6, con lo cual es necesario suministrar mecanismos que permitan continuar accediendo a aquellas redes que sólo poseen IPv4.

Existe una gran variedad de mecanismos de transición propuestos y muchos de ellos están actualmente en discusión en la IETF. Se describen a continuación los principales y a los que se considera más maduros.

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 estos empresas o usuarios home.

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.

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.

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. 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.

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 [24]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.

[24] Standalone: Sistemas de control de acceso autónomos no requieren de un software que controle el *equipo* durante su funcionamiento

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.

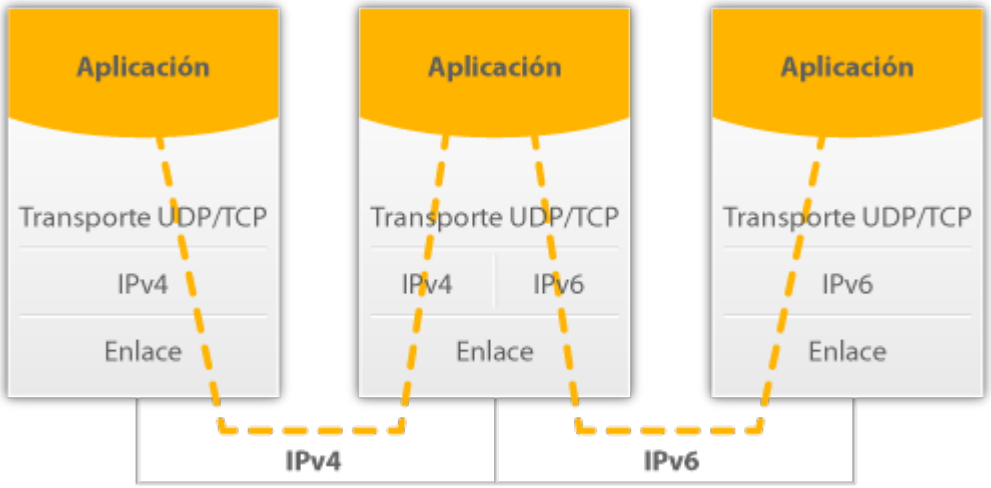

Ilustración 39: *Dual Stack, (Aguas Bucheli, 2014)*

De esta forma, cuando se establece una conexión hacia un destino sólo IPv4, se utilizará la conectividad IPv4 y si es hacia una dirección IPv6, se utilizará la red IPv6. En caso que el destino tenga ambos protocolos, normalmente se preferirá intentar conectar primero por IPv6 y en segunda instancia por IPv4 (si bien esto se ha ido modificando para solucionar problemas de timeouts[25]).

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

[25] Ver "Happy Eyeballs". http://goo.gl/ubPy5

encontrar la situación inversa. 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.

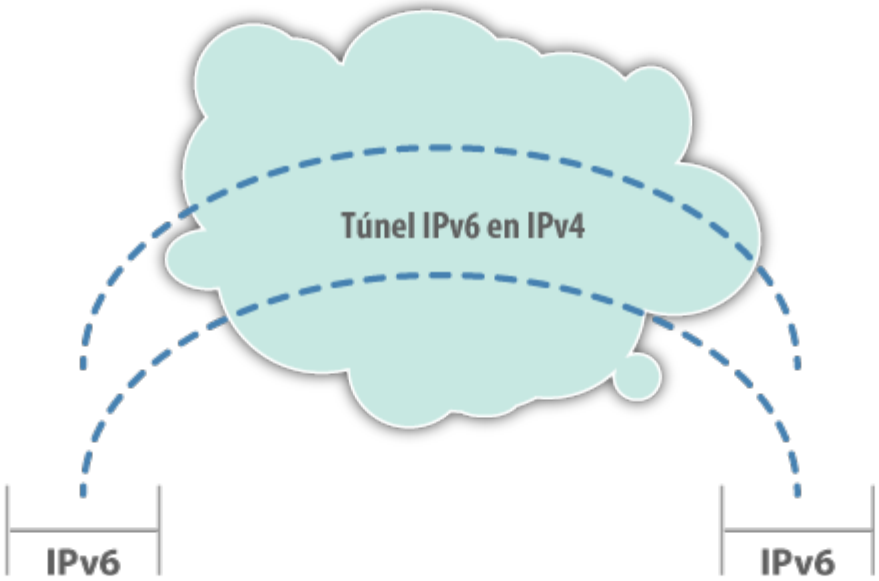

Ilustración 40: *Tuneles IPv6 en IPv4, (Chile, s.f.)*

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.

Dentro de los mecanismos de encapsulado podemos mencionar también la técnica conocida como 6PE/6VPE[26], 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[27]. Una forma de solventarlo es configurar el punto de destino real del túnel dentro

[26] 6PE. http://goo.gl/vVhiU
[27] NAT: Network Address Translation

de la DMZ[28] en el equipo que utiliza NAT, lo cual puede no resultar muy práctico. Otro método es usar AYIYA[29] o TSP[30]. Ambos envían IPv6 dentro de paquetes UDP[31], lo cual permite atravesar la mayoría de configuraciones NAT e incluso firewalls. Este es el más aceptado y usado por los Tunnel Brokers.

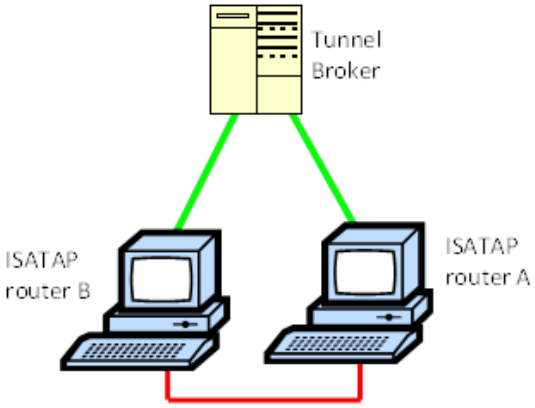

Ilustración 41: *Tunnel Broker, (Institute, s.f.)*

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.

[28] DMZ: Es un diseño conceptual de red donde los servidores de acceso público se colocan en un segmento separado
[29] AYIYA: Anything in anything
[30] TSP: Tunnel Setup Protocol
[31] UDP: Es un protocolo del nivel de transporte basado en el intercambio de datagramas (Encapsulado de capa 4 Modelo OSI)

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.

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.

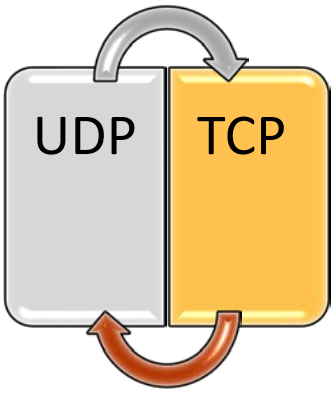

Ilustración 42: *Teredo UDP-TCP*

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.

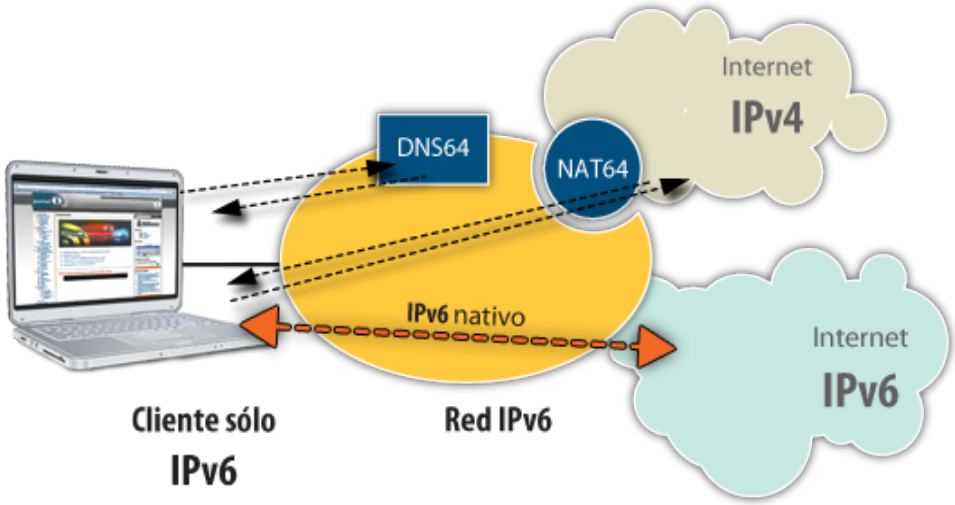

Ilustración 43: *Método de Traducción, (Institute, s.f.)*

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.

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[32] regional, para el caso de América Latina y el Caribe será a través de LACNIC[33]. 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.

[32] Regional Internet Registry. http://goo.gl/82Z3d
[33] Latin America & Caribbean Network Information Centre. http://goo.gl/UmxFa

Ilustración 44: *Publicación de direcciones en internet, (Aguas Bucheli, 2014)*

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

1. Si el ISP tiene implementado MPLS[34] en su red, entonces la transición es sencilla: solo basta con desplegar Dual Stack en los PE[35] 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

[34] Multiprotocol Label Switching. http://goo.gl/70B1e
[35] Provider Edge. http://goo.gl/uUjza

aconseja que el ISP despliegue Redes 6to4 y Teredo en su red para optimizar el tráfico.

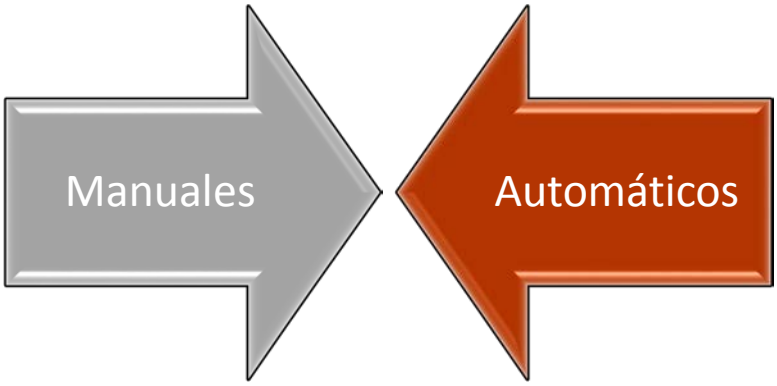

Ilustración 45: *Túneles Manuales y Automáticos, (Aguas Bucheli, 2014)*

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[36]. 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

[36] Ref: http://goo.gl/n6jzG

momento llegaron a ser 10), es decir que en realidad están yendo a alguna parte, las demás están asignadas pero sin uso.

Los bloques /32 asignados versus los ruteados siguen el mismo patrón, siendo 19 los bloques asignados totales y 7 los ruteados.

También se muestran el número de ASNs[37] distribuidos por LACNIC anunciando IPv4 e IPv6, de los cuales 26 son IPv4 puros, 14 son IPv6 e IPv4 y sólo 1 es IPv6 puro.

ASN	Name	Adyacencias v4	Rutas v4	Adyacencias v6	Rutas v6
AS27947	Telconet S.A	18	733	8	27
AS27757	CORPORACION NACIONAL DE TELECOMUNICACIONES - CNT EP	14	309	3	9
AS27765	TRANSNEXA S.A. E.M.A.	10	39	4	2
AS19169	Telconet S.A	8	159	5	23
AS23487	CONECEL	7	640	0	0
AS26613	CORPORACION NACIONAL DE TELECOMUNICACIONES - CNT EP	6	625	4	2
AS19114	Otecel S.A.	6	71	2	3
AS27814	Aeprovi	5	5	3	4

[37] Autonomous System Number. http://goo.gl/8Np37

AS22724	PUNTONET S.A.	5	167	2	2
AS52274	NIC.EC S.A.	4	4	3	3
AS19582	GRUPO BRAVCO	4	12	0	0
AS52238	SPEEDYCOM	3	8	0	0
AS27841	CEDIA	3	3	2	5
AS27820	Universidad Técnica Particular de Loja	3	3	2	1
AS27668	ETAPA EP	3	125	0	0
AS23216	MEGADATOS S.A.	3	177	0	0
AS52417	BPAC AMERAFIN S.A.	2	1	0	0
AS52345	BANCO DE LOJA	2	1	0	0
AS52331	CORPORACION FINANCIERA NACIONAL	2	1	0	0
AS28097	Farcomed	2	2	0	0
AS28058	Stealth Telecom del Ecuador	2	5	2	3
AS28025	CENTROSUR	2	40	0	0
AS28021	ASEGLOB S.A.	2	8	0	0
AS27968	CORPORACION NACIONAL DE TELECOMUNICACIONES - CNT EP	2	43	0	0
AS27958	FIX GROUP	2	5	0	0
AS27948	CORPORACION NACIONAL DE TELECOMUNICACIONES - CNT EP	2	465	2	7
AS27740	NEW ACCESS S.A.	2	24	0	0

AS27738	Ecuadortelecom S.A.	2	557	0	0
AS14522	Satnet	2	543	0	0
AS52377	GILAUCO S.A.	1	5	0	0
AS52343	Universidad Tecnológica Equinoccial	1	2	1	1
AS52257	Telconet S.A	1	10	0	0
AS28027	Escuela Superior Politecnica del Litoral	1	17	1	1
AS28006	CORPORACION NACIONAL DE TELECOMUNICACIONES - CNT EP	1	97	1	2
AS27998	Contecon Guayaquil S.A.	1	1	0	0
AS27919	LUTROL S.A.	1	12	0	0
AS27902	GPF CORPORACION - POWERFAST	1	4	0	0
AS27868	Ecuaonline	1	3	0	0
AS27816	ESPOLTEL	1	15	0	0
AS27784	Bco. Pichincha Matriz	1	1	0	0
AS262223	Nettplus - Necusoft Cia. Ltda.	1	4	0	0
AS262212	Escuela Politecnica Nacional	1	4	1	1
AS262169	SOLINTELSA	1	1	0	0
AS262157	Tame Linea Aerea del Ecuador	1	1	0	0
AS262154	Comm & Net S.A.	1	7	1	1
AS14420	CORPORACION NACIONAL DE TELECOMUNICACIONES - CNT EP	1	457	1	7

Tabla 9: *Tabla BGP Ecuador, (Electric, s.f.)*

La tabla BGP provista por Hurricane Electric donde podemos ver el número de adyacencias y rutas en IPv4 e IPv6 de prácticamente todos los proveedores de Internet en nuestro país. Las cifras no son muy alentadoras o al menos no indican un gran interés en el tema.

2.4.2. INSTITUCIONES PÚBLICAS / PRIVADAS

Para este punto, se ha preparado un script BASH que permite, mediante el comando host, determinar si cierto nombre de hosts de un dominio en particular, dispone o no de un registro AAAA que representa una dirección IPv6. Preparamos entonces un archivo de texto (dominios.txt) con una lista de los nombres de host que deseábamos analizar, llenando en él una lista de los registros que se usan para acezar a las páginas Web de entidades públicas y privadas.

La muestra que hemos tomado para este estudio está detallado por algunas entidades del estado como: ministerios, sub secretarías, municipios, empresas de tecnología y empresas proveedores de Internet.Como referencia, el código del script en BASH.

```
#!/bin/bash
for dominio in $(cat dominios.txt)
do
     host -t AAAA $dominio
done
exit 0
```

Script 1: *Línea de Código para los Dominios Locales, (Aguas Bucheli, 2014)*

De esta corrida obtuvimos los siguientes resultados:

Institución	Dominio	IPv6 ready
Presidencia de la República del Ecuador	www.presidencia.gob.ec	NO
Secretaría Nacional de Administración Pública	www.administracionpublica.gob.ec	NO
Secretaría Nacional del Agua	www.agua.gob.ec	NO
Secretaría Nacional de Desarrollo Amazónico	www.desarrolloamazonico.gob.ec	NO
Secretaría Nacional de Educación Superior, Ciencia, Tecnología e Innovación	www.educacionsuperior.gob.ec	NO
Secretaría Nacional de Comunicación	www.comunicacion.gob.ec	NO
Secretaría Nacional de Gestión de Riesgos	www.gestionderiesgos.gob.ec	NO
Secretaría Nacional de Planificación y Desarrollo	www.planificacion.gob.ec	NO
Secretaría Nacional de Migrante	www.migrante.gob.ec	NO
Secretaría Nacional de Pueblos, Movimientos Sociales y Participación Ciudadana	www.pueblos.gob.ec	NO
Secretaría Nacional de Transparencia	www.transparencia.gob.ec	NO
Ministerio Coordinador de Desarrollo Social	www.desarrollosocial.gob.ec	NO

Ministerio Coordinador de Patrimonio Natural y Cultural	www.patrimonio.gob.ec	NO
Ministerio Coordinador de Política Económica	www.politicaeconomica.gob.ec	NO
Ministerio Coordinador de Política y Gobiernos Coordinador Autónomos Descentralizados	www.politica.gob.ec	NO
Ministerio Coordinador de Producción, Empleo y Competitividad	www.produccion.gob.ec	NO
Ministerio Coordinador de Sectores Estratégico	www.sectoresestrategicos.gob.ec	NO
Ministerio Coordinador de Seguridad	www.seguridad.gob.ec	NO
Ministerio Coordinador de Conocimiento	www.conocimiento.gob.ec	NO
Ministerio de Agricultura, Ganadería, Acuacultura y Pesca	www.agricultura.gob.ec	NO
Instituto Nacional de Patrimonio Cultural	**www.inpc.gob.ec**	**OK**
Ministerio del Ambiente	www.ambiente.gob.ec	NO
Ministerio de Cultura	www.cultura.gob.ec	NO
Ministerio de Defensa Nacional	www.defensa.gob.ec	NO
Ministerio de Deporte	www.deporte.gob.ec	NO
Ministerio de Desarrollo Urbano y Vivienda	www.habitatyvivienda.gob.ec	NO
Ministerio de Educación	www.educacion.gob.ec	NO
Ministerio de Electricidad y Energía Renovable	www.energia.gob.ec	NO

Ministerio de Finanzas	www.finanzas.gob.ec	NO
Ministerio de Inclusión Económica y Social	www.inclusion.gob.ec	NO
Ministerio de Industrias y Productividad	www.industrias.gob.ec	NO
Ministerio del Interior	www.ministeriointerior.gob.ec	NO
Ministerio de Justicia, Derechos Humanos y Cultos	www.justicia.gob.ec	NO
Ministerio de Recursos Naturales no Renovables	www.recursosnaturales.gob.ec	NO
Ministerio de Relaciones Exteriores, Comercio e Integración	www.cancilleria.gob.ec	NO
Ministerio de Relaciones Laborales	www.relacioneslaborales.gob.ec	NO
Ministerio de Salud Pública	www.salud.gob.ec	NO
Ministerio de Telecomunicaciones y de la Sociedad de la Información	www.telecomunicaciones.gob.ec	NO
Ministerio de Telecomunicaciones y de la Sociedad de la Información	**www.mintel.gob.ec**	**OK**
Ministerio de Transporte y Obras Públicas	www.obraspublicas.gob.ec	NO
Ministerio de Turismo	www.turismo.gob.ec	NO
Municipio del Distrito Metropolitano de Quito	www.quito.gob.ec	NO
Municipio de Guayaquil	**www.guayaquil.gob.ec**	**OK**
Municipio de Cuenca	www.cuenca.gob.ec	NO
Municipio de Tulcán	www.gmtulcan.gob.ec	NO
Municipio de Ibarra	www.ibarra.gob.ec	NO

Municipio de Latacunga	www.latacunga.gob.ec	NO
Municipio de Ambato	www.ambato.gob.ec	NO
Municipio de Guaranda	www.guaranda.gob.ec	NO
Municipio de Riobamba	www.admriobamba.gob.ec	NO
Municipio de Azogues	www.azogues.gob.e	NO
Municipio de Loja	www.loja.gob.ec	NO
Municipio de Manta	www.manta.gob.ec	NO
Municipio de Portoviejo	www.portoviejo.gob.ec	NO
Municipio de Machala	www.machala.gob.ec	NO
Municipio de Esmeraldas	www.esmeraldas.gob.ec	NO
Municipio del Tena	www.tena.gob.ec	NO
Municipio del Puyo	www.puyo.gob.ec	NO
Policía Nacional de Ecuador	www.policiaecuador.gob.ec	NO
Consejo Nacional Electoral	www.cne.gob.ec	NO
Consejo Nacional de Telecomunicaciones	www.cnt.com.ec	NO
Servicio de Rentas Internas	www.sri.gob.ec	NO
Universidad de Cuenca	**www.ucuenca.edu.ec**	**OK**
Universidad Nacional de Loja	**www.unl.edu.ec**	**OK**
Pontificia Universidad Católica del Ecuador **Sede Ibarra**	**www.pucesi.edu.ec**	**OK**
Escuela Politécnica Nacional	**ipv6.epn.edu.ec**	**OK**
Escuela Politécnica de Chimborazo	**www.espoch.edu.ec**	**OK**
Consejo Nacional de Telecomunicaciones	www.conatel.gob.ec	NO

NIC.ec	**www.nic.ec**	**OK**
IPv6 Task Force Ecuador	**www.ipv6tf.ec**	**OK**
Escuela Politécnica del Ejército	www.espe.edu.ec	NO
Universidad Central del Ecuador	www.uce.edu.ec	NO
Telconet S.A	www.telconet.net	NO
Transnexa S.A.	www.transnexa.com	NO
CONECEL	www.claro.com.ec	NO
OTECEL S.A.	www.movistar.com.ec	NO
PUNTONET S.A.	www.punto.net.ec	NO
ETAPA EP	www.etapa.net.ec	NO
SATNET	www.satnet.net	NO
Stealth Telecom de Ecuador	www.stealthtelecom.net	NO
Superintendencia de Telecomunicaciones	www.supertel.gob.ec	NO
Pontificia Universidad Católica de Quito	www.puce.edu.ec	NO

Tabla 10: *Resultado Corrida de Script AAAA en principales instituciones del país, (Aguas Bucheli, 2014)*

Donde podemos observar que de los 82 sitios analizados, sólo 10 obtuvieron el status de OK, algo más del 12% del total. De estas escasas 10, 3 son de gobierno, 5 son instituciones educativas y las últimas 2 son de entidades orientadas a los servicios de Internet, una de ellas de hecho es la IPv6 Task Force ecuatoriana.

A todos los registros de la lista que obtuvieron un positivo los analizamos luego con un telnet al puerto 80 a ver si efectivamente el servicio web estaba respondiendo por IPv6, todos los 10 analizados respondieron, por ende los 10 obtuvieron el status de OK.

CAPÍTULO 3: APLICACIONES

3. PROPUESTA DE PROGRAMACIÓN EN EL PROCESO DE MIGRACIÓN EN BASE A LOS PROBLEMAS ACTUALES Y TIEMPOS ESTIMADOS.

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.

3.2. ¿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.

3.3. GOGOC

3.3.1. INSTALACIÓN EN LINUX FEDORA:

Para instalar gogoc en Fedora simplemente ejecutamos:

```
sudo yum install gogoc
```

Script 2: *Instalación Gogoc-Fedora, (Aguas Bucheli, 2014)*

Al finalizar la instalación procedemos a arrancar el servicio:

```
service gogoc start

chkconfig gogoc on
```

Script 3: *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 4: *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 5: *Logs Fedora, (Aguas Bucheli, 2014)*

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

3.3.2. INSTALACIÓN EN LINUX DEBIAN O UBUNTU

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

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

Script 6: *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 7: *Forma de Iniciar el servicio de gogoc en Debian-Ubuntu, (Aguas Bucheli, 2014)*

3.3.3. 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.

3.3.4. 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 8: *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

3.4. 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.

3.4.1. 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.

3.4.2. 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 9: *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 encapsulado. Es lo que en el tunnel te llaman: Server IPv4 Address:

Simplemente reiniciamos la red en debian:

```
service networking restart
```

Script 10: *Reinicio de la red en debían, (Aguas Bucheli, 2014)*

3.4.3. 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 11: *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 12: *Reinicio de la Red en CentOS, (Aguas Bucheli, 2014)*

3.4.4. ¿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.

3.4.5. 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

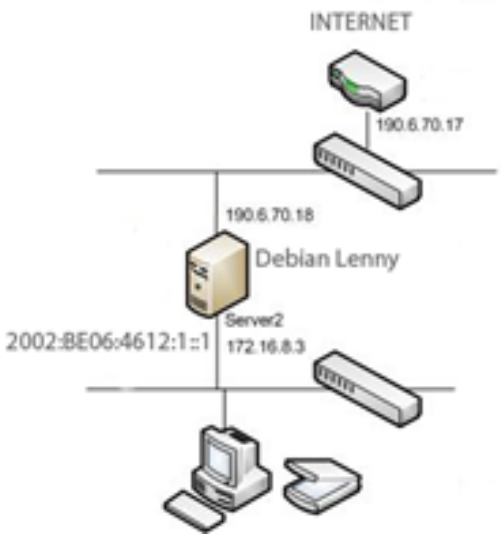

Ilustración 46: *Configuración 6to4, (Young, s.f.)*

- 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 13: *Configuración 6to4 en Debian Parte 1,*

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

```
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 14: *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 15: *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 16: *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 17: *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 18: *Configuración de inicio para el routing,*

3.4.6. 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 19: *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)

3.5. IMPLEMENTACIÓN EN WINDOWS DE LOS TÚNELES

3.5.1. 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.

3.5.2. 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.

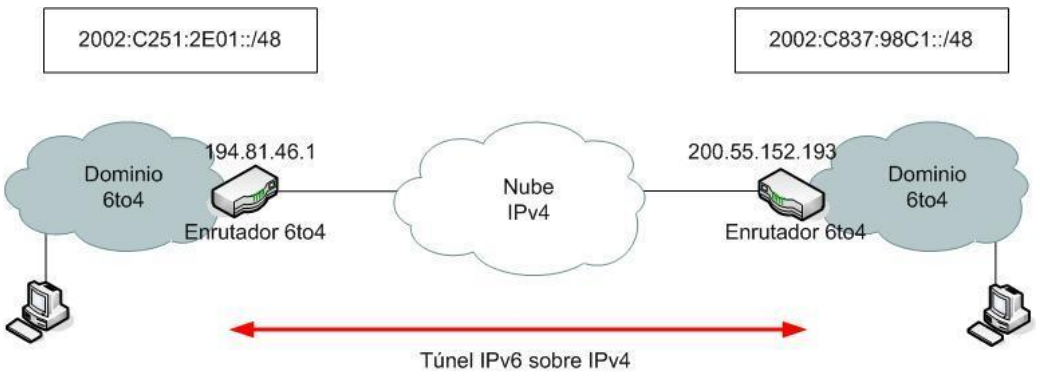

Ilustración 47: *Túneles 6to4 Parte 1, (Profesor, s.f.)*

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 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.

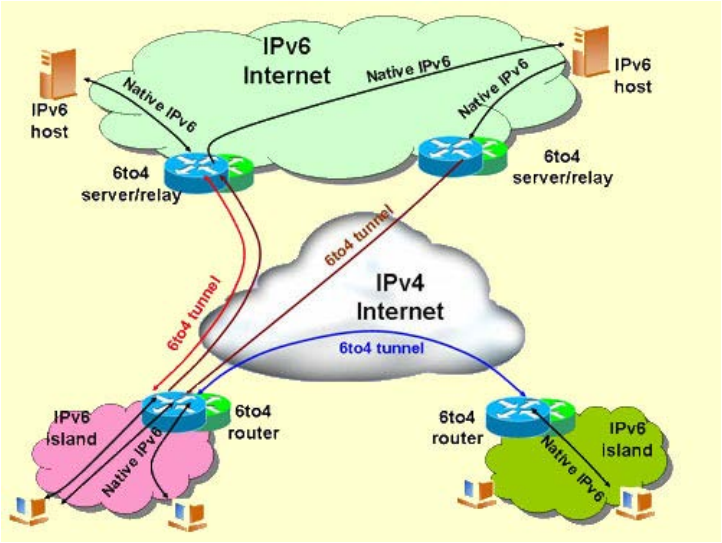

Ilustración 48: *Túneles 6to4 Parte 2, (Profesor, s.f.)*

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.

3.5.3. 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

3.5.4. 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
!
```

```
ipv6 route 2002::/16 Tunnel64

ipv6 route ::/0 2002:C058:6301::
```

Script 20: *Configuración de Túneles en Cisco, (Aguas Bucheli, 2014)*

3.5.5. 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.

3.5.6. 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:

Precedence	*Label*	*Prefix*
50	***0***	***::1/128***
40	***1***	***::/0***

30	***1***	***2002::/16***
20	***3***	***::/96***
10	***4***	***::ffff:0:0/96***
5	***5***	***2001::/32***

Tabla 11: *Tabla de IPv6 para Microsoft, (Aguas Bucheli, 2014)*

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 21: *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 22: *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 23: *Configuración de la política parte 3, (Aguas Bucheli, 2014)*

3.5.7. 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.

3.6. 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 [75]. Teredo usa dos entidades, el Servidor Teredo y el *Relay* Teredo. Los servidores escuchan las peticiones de los clientes en el puerto 3544 UDP, respondiendo con la dirección IPv6 que usará el cliente. Las direcciones Teredo tienen el siguiente formato:

32 bits	32 bits	16 bits	16 bits	32 bits
Prefijo Teredo (2001:0/32)	Dirección IPv4 del Servidor Teredo	Banderas	Puerto UDP asociado al cliente	Dirección IPv4 asociada al cliente

Tabla 12: *Prefijos Teredo, (Core, s.f.)*

A continuación se muestra una figura representando los componentes de Teredo.

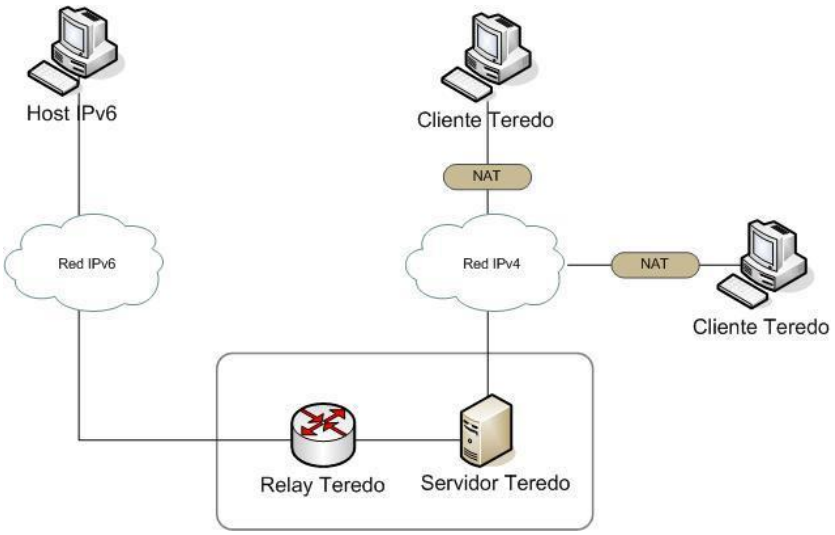

Ilustración 49: *Componentes Teredo, (Aguas Bucheli, 2014)*

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

3.6.1. 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 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 24: *Test de Conectividad, (Aguas Bucheli, 2014)*

Si desea deshabilitar Teredo ejecute el comando

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

Script 25: *Deshabilitación teredo, (Aguas Bucheli, 2014)*

Si desea rehabilitarlo:

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

Script 26: *Rehabilitación teredo, (Aguas Bucheli, 2014)*

3.6.2. 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*.

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. 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 [2]	Montreal, Amsterdam, Taipei, Sydney	/56 subnet	6in4, 4in6, TSP	Yes	Yes		Anonymous, or signup (via registration on gogoNET[2])	TSP, website	English

Ilustración 50: *Principales proveedores de túneles, (Electric, s.f.)*

3.7. CONFIGURACIÓN DE UN TÚNEL USANDO EL SERVICIO DE HURRICANE ELECTRIC.

Existen varios servidores de Tunnel Broker, entre los que se encuentran Hurricane Electric (http://ipv6.he.net),

Para crear un túnel con Hurricane Electric debe:

- Crear una cuenta gratuita en su sitio (http://ipv6.he.net, o http://www.tunnelbroker.net).
- Crear un túnel en la página http://www.tunnelbroker.net/ipv6_normal.php. En esa página solo será necesario especificar la dirección pública IPv4 con la que te conectas a Internet. El propio sitio te recomienda a cuál de sus servidores debes conectarte teniendo en cuenta la conectividad de nuestro sitio por lo que solo debemos aceptar los valores mostrados. Debo señalar que es imprescindible permitir al menos PING hacia esa dirección pues antes de crear la configuración HE verifica su disponibilidad.

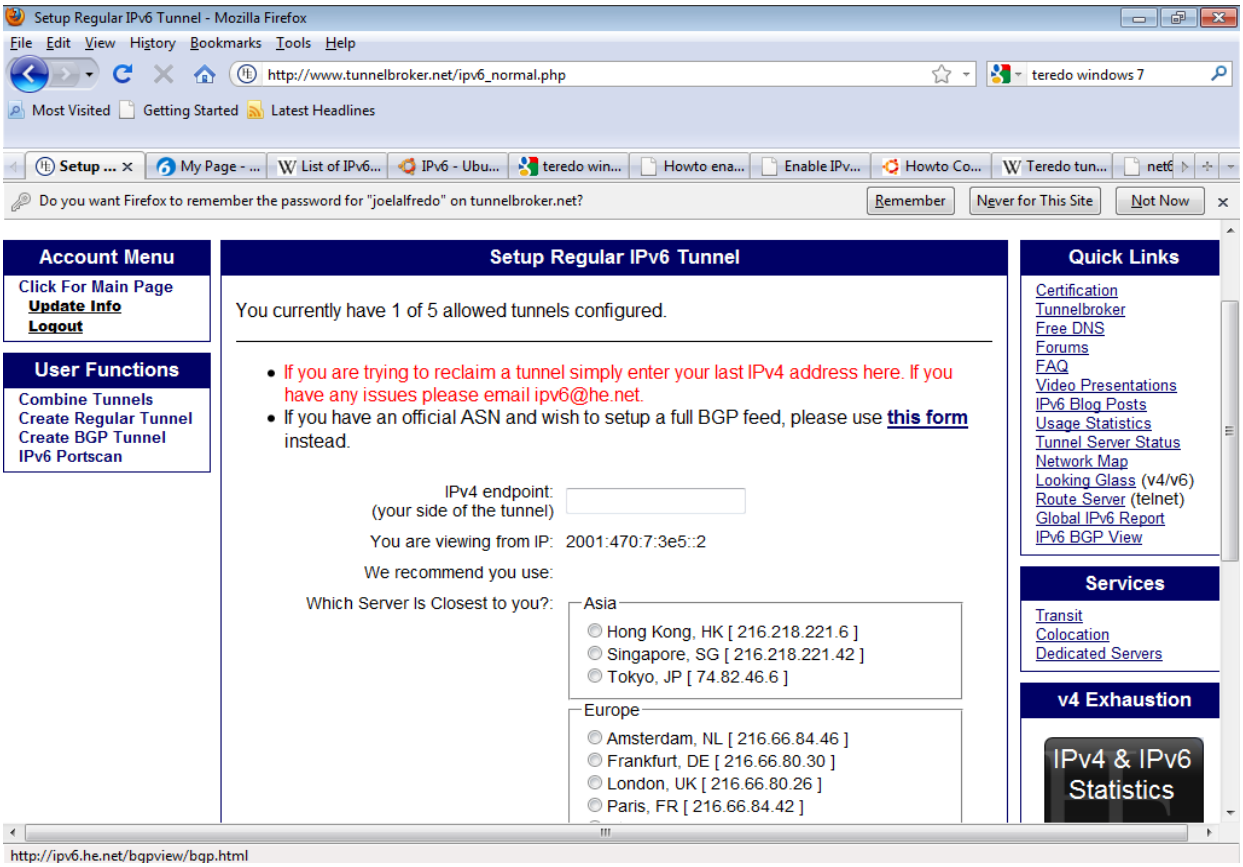

Ilustración 51: *Hurricane Electric, (Aguas Bucheli, 2014)*

- A continuación aparece una página que nos indica que el túnel fue configurado correctamente en el servidor y nos brinda un enlace donde nos ofrecen la configuración que debemos utilizar en nuestro cliente, para múltiples Sistemas Operativos diferentes. Es importante destacar que si nuestro host se encuentra detrás de un NAT debemos sustituir la IP Pública que suministramos en la configuración del servidor de TunnelBroker por la IP privada que tiene nuestro host. Por ejemplo, como resultado de la creación del Túnel nos indican que debemos introducir esta configuración en nuestro host Windows 7:

```
netsh interface teredo set state disabled
netsh interface ipv6 add v6v4tunnel IP6Tunnel 190.6.70.18
216.66.22.2
netsh interface ipv6 add address IP6Tunnel 2001:470:7:3e5::2
netsh interface ipv6 add route ::/0 IP6Tunnel 2001:470:7:3e5::1
```

Script 27: *Configuración de HE en nuestro Windows 7, (Aguas Bucheli, 2014)*

- Como podemos observar nos indican que utilicemos la IP pública que le suministramos en el paso 1 de la configuración, pero si nuestro host lo que tiene es una IP privada que sale a internet haciendo NAT con esa dirección, la que debemos especificar en la segunda línea de configuración es la privada:

```
netsh interface ipv6 add v6v4tunnel IP6Tunnel 172.16.8.9
216.66.22.2
```

Script 28: *Configuración para túneles Hurricane, (Aguas Bucheli, 2014)*

A partir de este momento disponemos de una conexión IPv6 a través de un túnel configurado con el servicio de TunnelBroker de Hurricane Electric.

3.8. DESCRIPCIÓN DE UN CASO PRÁCTICO DEL USO DE TUNNEL BROKER EN WINDOWS

- Ingresamos a www.tunnelbroker.net

Ilustración 52: *Hurricane Electric en Windows 7, (Aguas Bucheli, 2014)*

- Después de ingresar, tenemos lo siguiente:

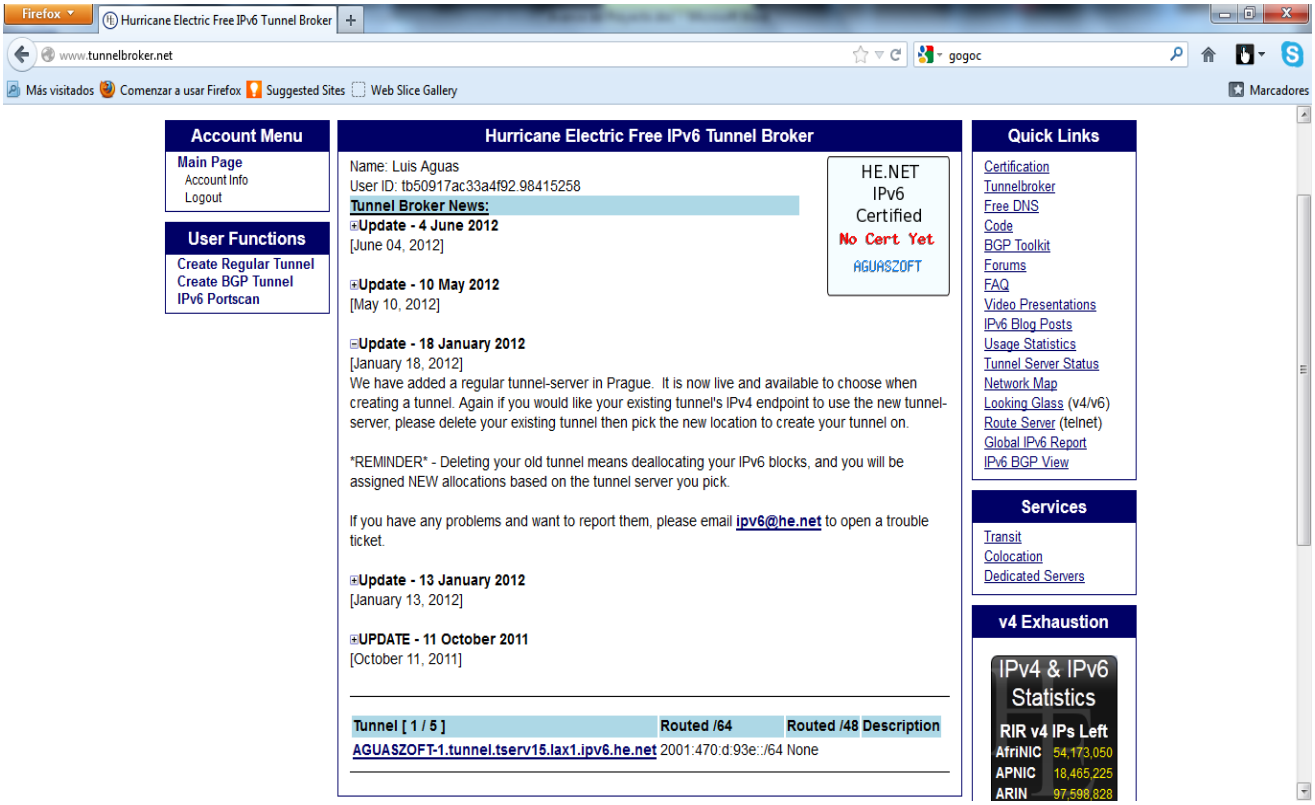

Ilustración 53: *Pantalla Inicial de Hurricane Electric en Windows 7, (Aguas Bucheli, 2014)*

- Damos clic en crear un tunnel regular
- Pero antes realizamos ping, para conocer la dirección IP

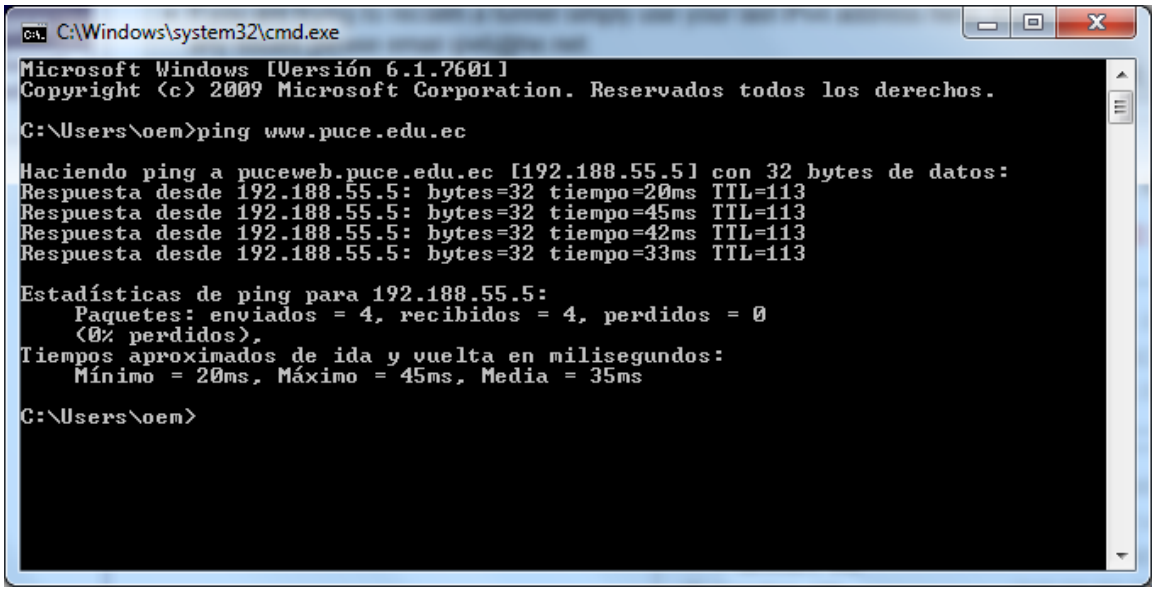

Ilustración 54: *Prueba de Ping, para conocer una dirección IP indicada, (Aguas Bucheli, 2014)*

- Luego colocamos la dirección IP en el campo que nos pide:

Ilustración 55: *Configuración de IP con Hurricane Electric 1, (Aguas Bucheli, 2014)*

- Y seleccionamos que el tunnel se haga desde Hong Kong.

- Damos clic en Create Tunnel

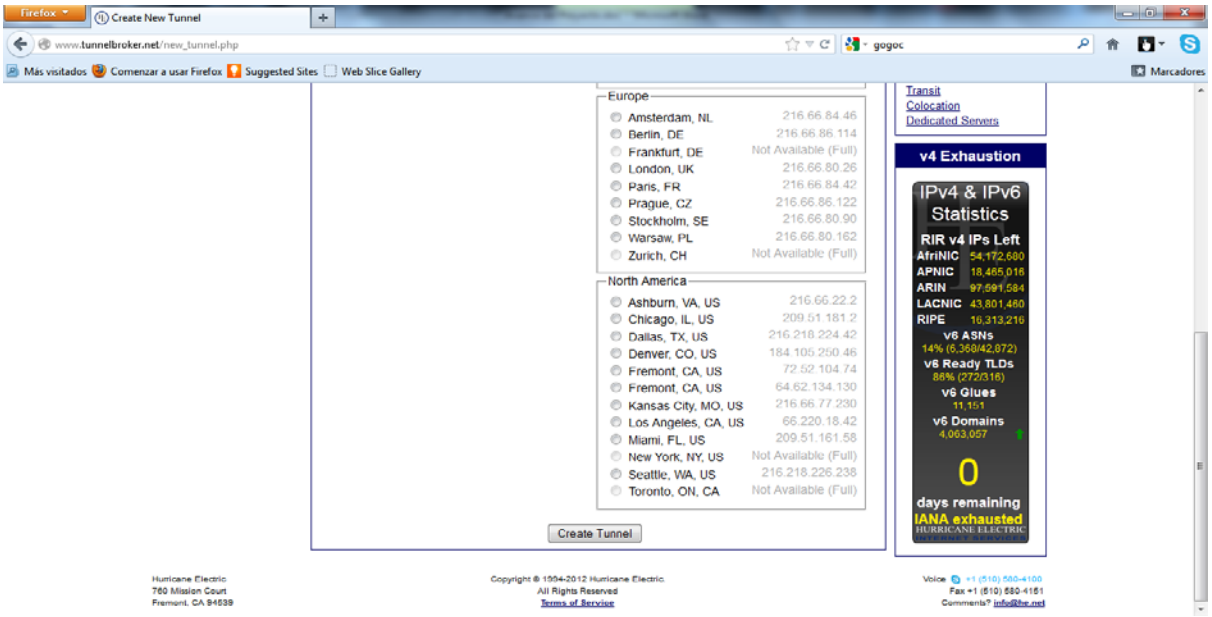

Ilustración 56: *Configuración de IP con Hurricane Electric , (Aguas Bucheli, 2014)*

- Despues tenemos lo siguiente

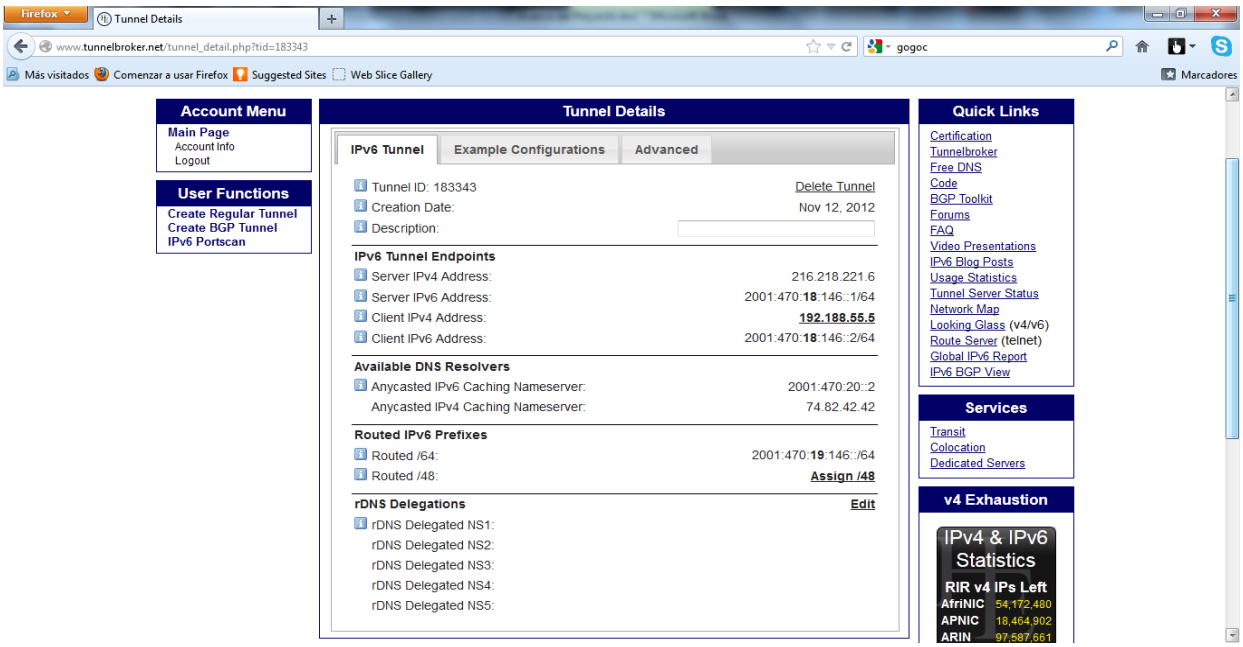

Ilustración 57: *Propiedades del túnel creado con Hurricane Electric, (Aguas Bucheli, 2014)*

- Luego damos clic en Example Configurations y seleccionamos el sistema operativo, en este caso Windows 7

Ilustración 58: *Ventana de Resultados Hurricane Electric, (Aguas Bucheli, 2014)*

- En la ventana de comandos, copiamos ese código.
- Para verificar que se realizó la acción correctamente, enviamos un ping a la siguiente dirección:
    - *2001:470:c:93e::2*

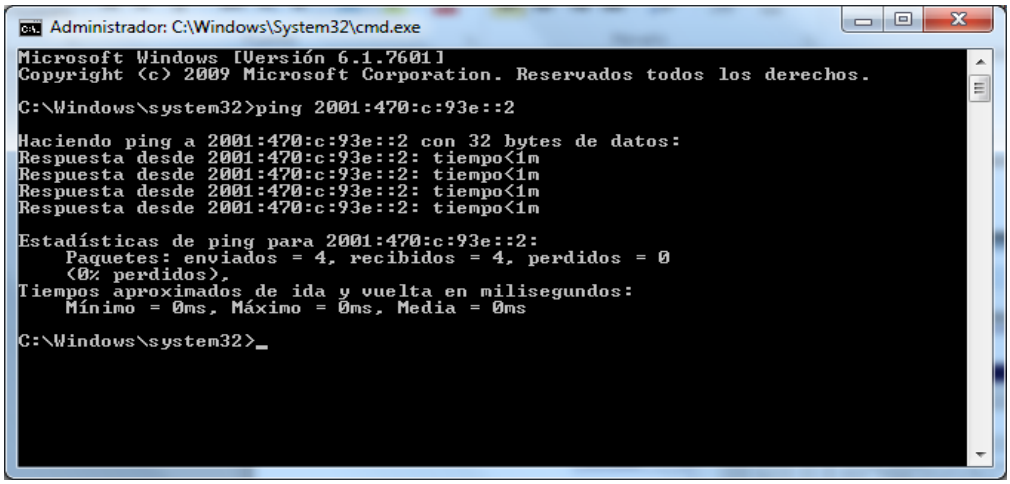

Ilustración 59: *Demostración de Conectividad al túnel creado, (Aguas Bucheli, 2014)*

- Con esto se demostró que el túnel se creó perfectamente.
- Cabe mencionar que internamente podemos también

  verificar: http://www.tunnelbroker.net/portscan.php

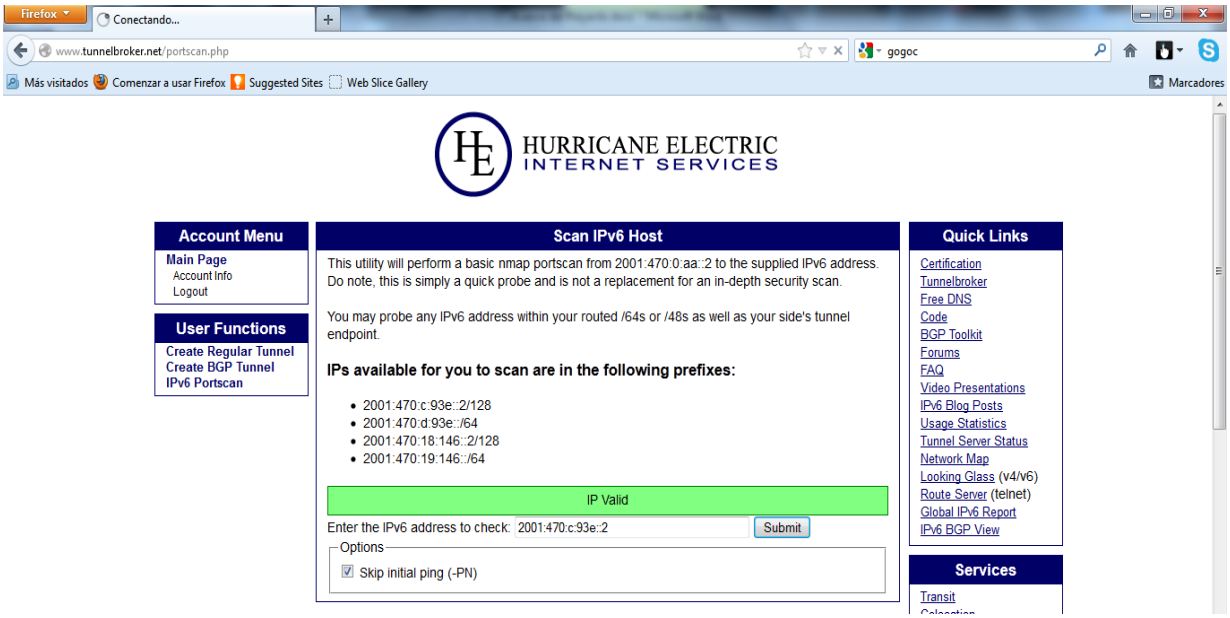

Ilustración 60: *Página de Verificación, (Aguas Bucheli, 2014)*

- Nos ayudara a verificar las IP válidas.
- A través de esto hemos habilitado la configuración de IPv6 para esa computadora, usando la red de nuestro laboratorio.

3.9. IPV6 MEDIANTE GOGOC EN WINDOWS 7

En Windows es muy sencillo crearnos un túnel para tener conexión IPV6. Lo primero que debemos hacer es crearnos una cuenta en gogo6, les enviaran un correo para verificar, ingresan por el link en tu correo, creas el usuario y la clave para el cliente gogoc, y descargas en el menú Freenet6, opción Download, el cliente que necesites de acuerdo a la versión de tu Windows, lo instalas y lo ejecutas, te pedirá el usuario y la clave

Por lo que con esto ya tendríamos nuestra conexión IPv6 para hacer pruebas. Otro ejemplo para verificar si te funciona.

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.

Por ello, es importante que entendamos cómo se realiza el despliegue del nuevo protocolo de Internet, tanto si somos usuarios residenciales, como corporativos, proveedores de contenidos, proveedores de servicios de Internet, así como la propia administración pública.

La aplicación se ha hecho en el Laboratorio de Tecnologías de Información y Comunicación de la Facultad de Ingeniería, en una computadora conectada a la red Sistemas_WPA, mediante lo cual desarrollamos lo siguiente:

- Entramos a:

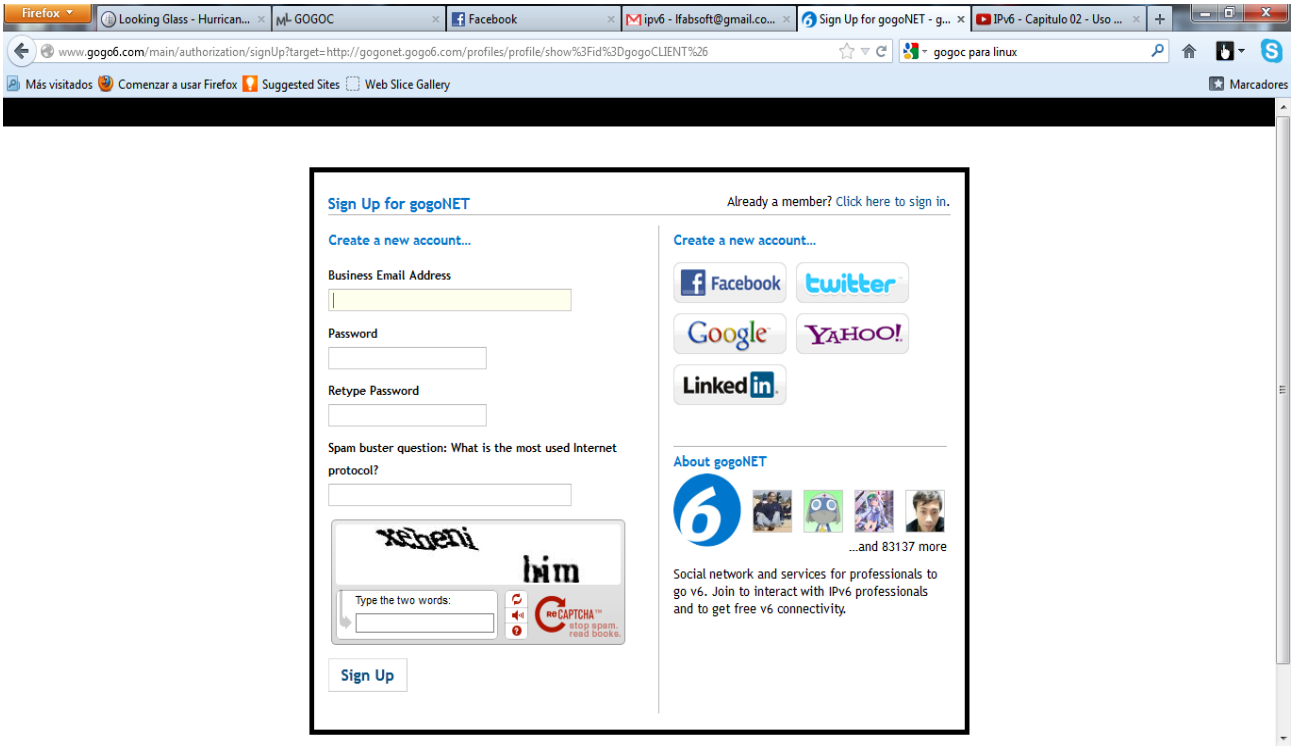

Ilustración 61: *Gogoc 1, (Aguas Bucheli, 2014)*

- Nos registramos:

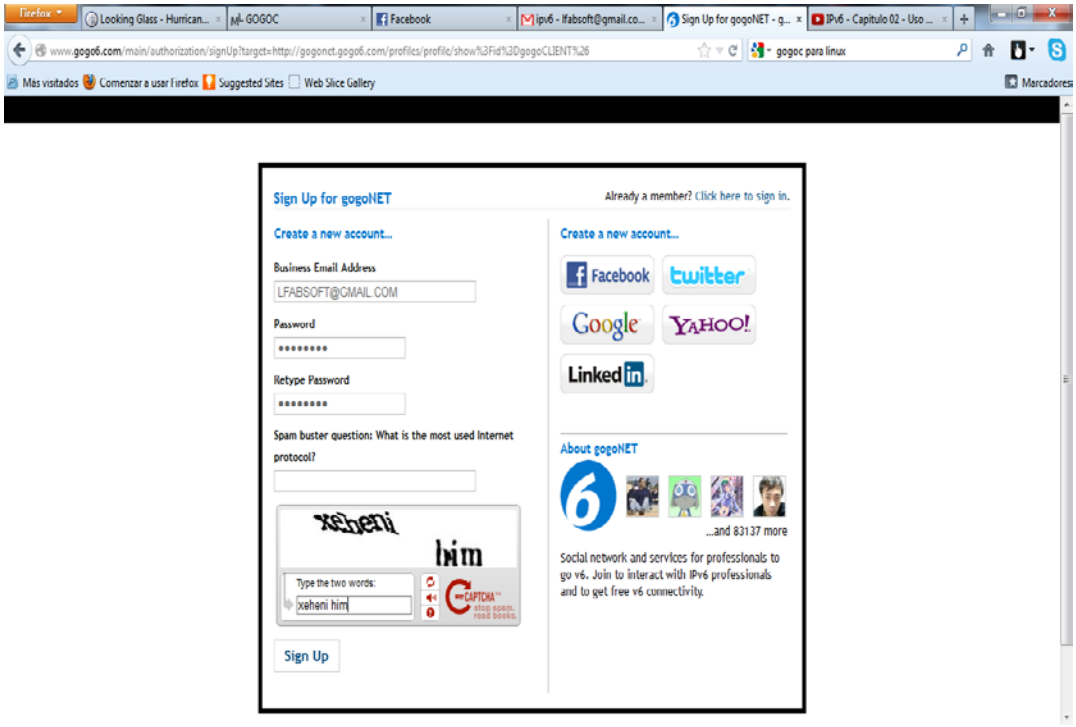

Ilustración 62: *Gogoc 2, (Aguas Bucheli, 2014)*

- Después de registrarnos, pasamos a:

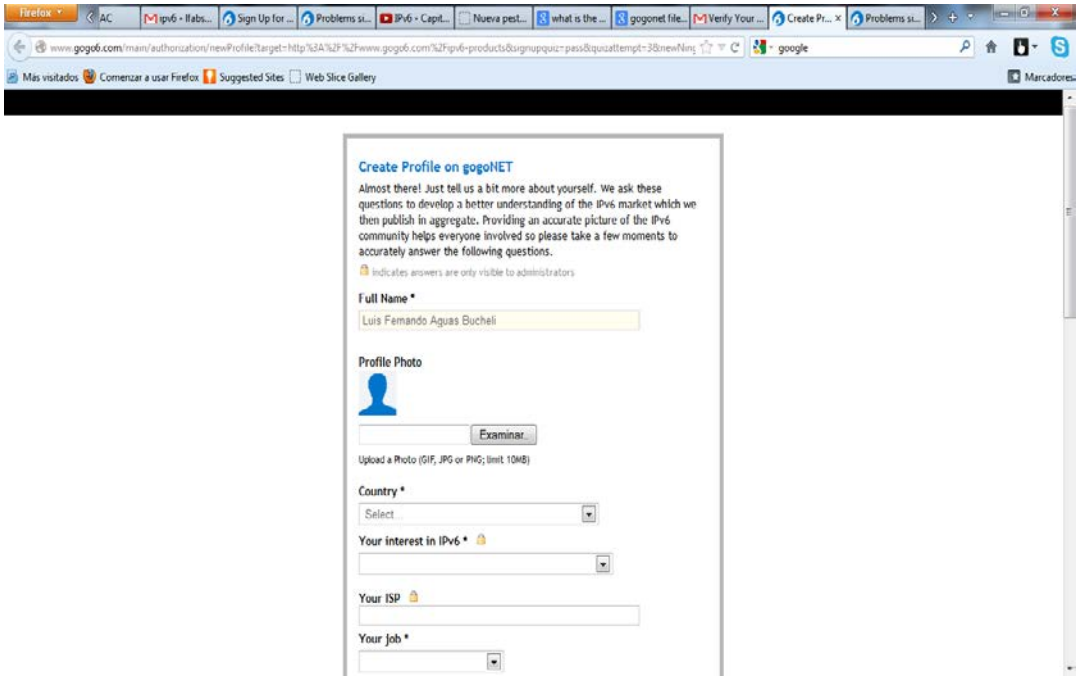

Ilustración 63: *Gogoc 3, (Aguas Bucheli, 2014)*

- Luego después de registrarnos

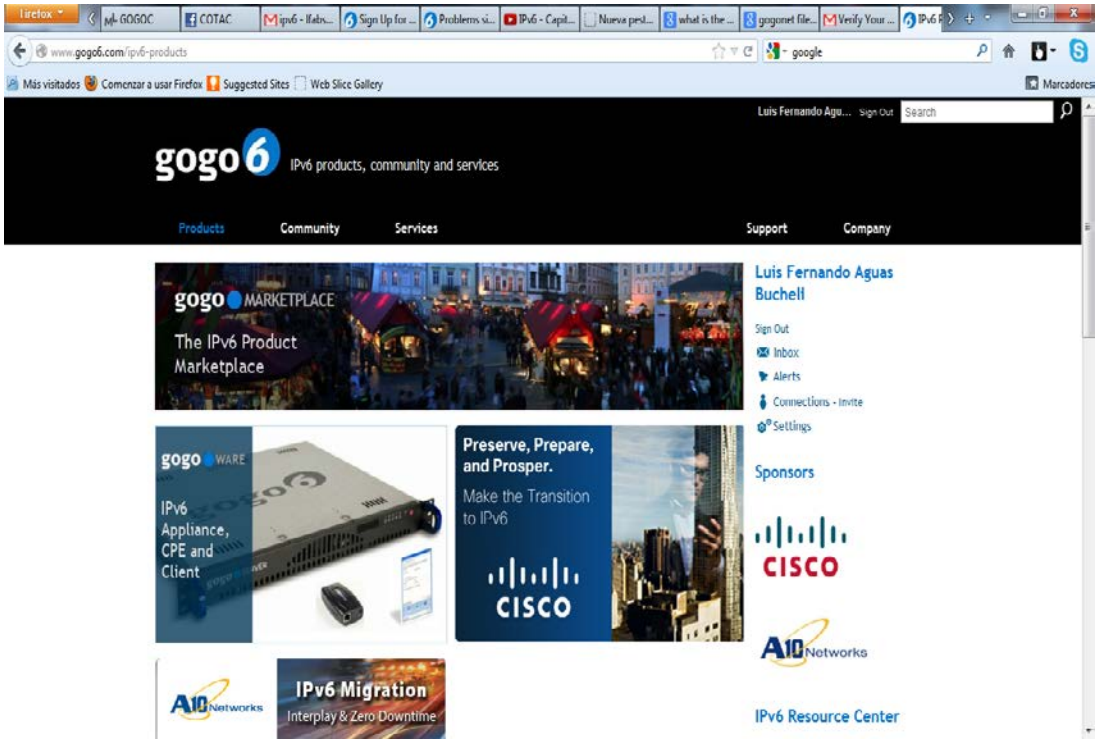

Ilustración 64: *Gogoc 3, (Aguas Bucheli, 2014)*

- Luego vamos a esta página http://www.gogo6.com/profile/gogoCLIENT o nos vamos para products y descargamos el cliente de gogoc para Windows

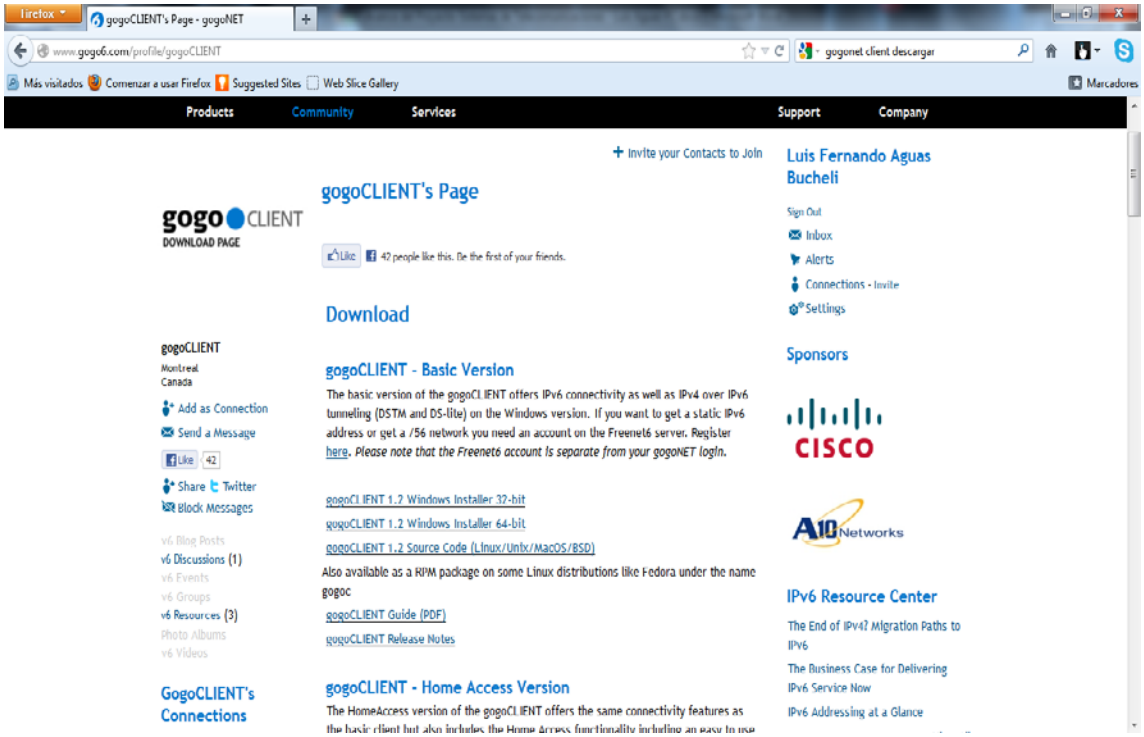

Ilustración 65: *Gogoc 4, (Aguas Bucheli, 2014)*

- Descargamos la versión de 64 bits, ya que nuestro sistema es de 64 bits.

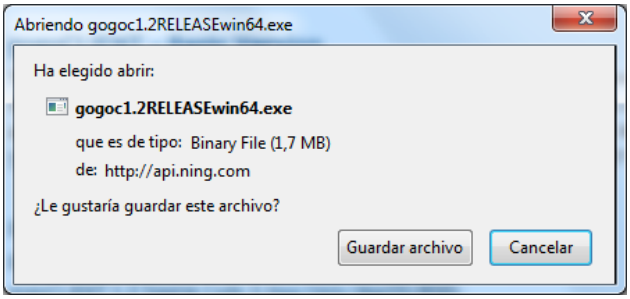

Ilustración 66: *Instalación Gogoc 1, (Aguas Bucheli, 2014)*

- Luego instalamos gogoc

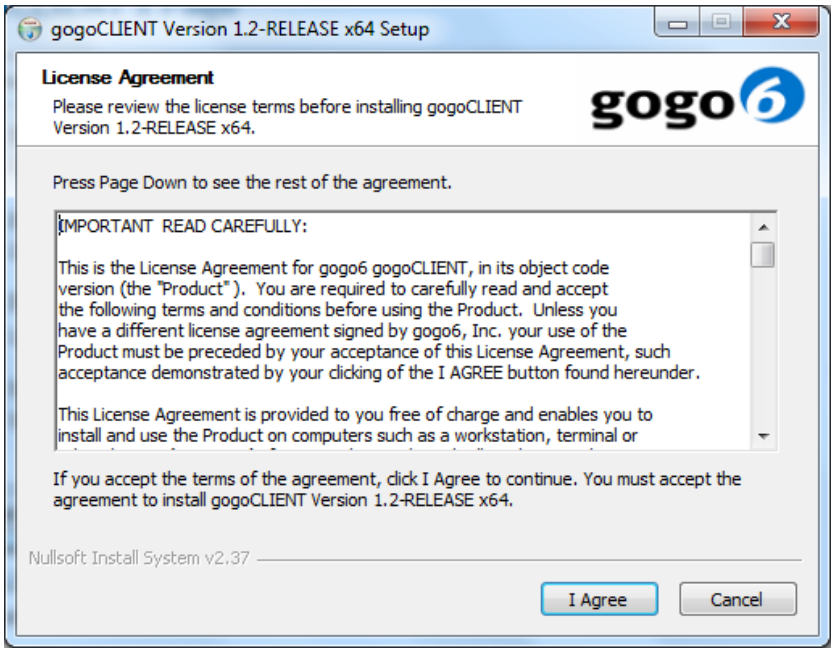

Ilustración 67: *Instalación Gogoc 2, (Aguas Bucheli, 2014)*

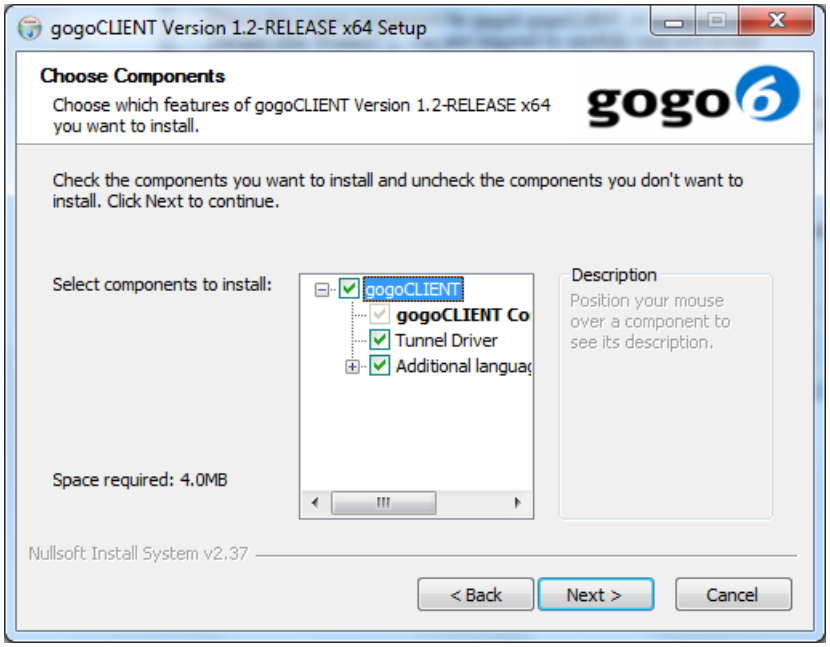

Ilustración 68: *Instalación Gogoc 3, (Aguas Bucheli, 2014)*

- Damos clic en aceptar

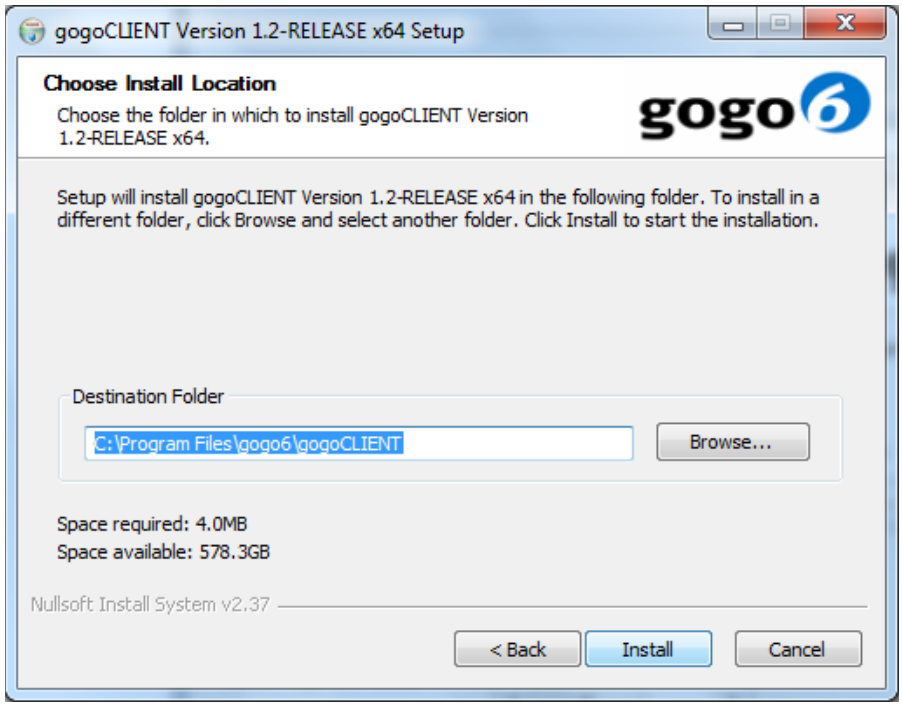

Ilustración 69: *Instalación Gogoc 4, (Aguas Bucheli, 2014)*

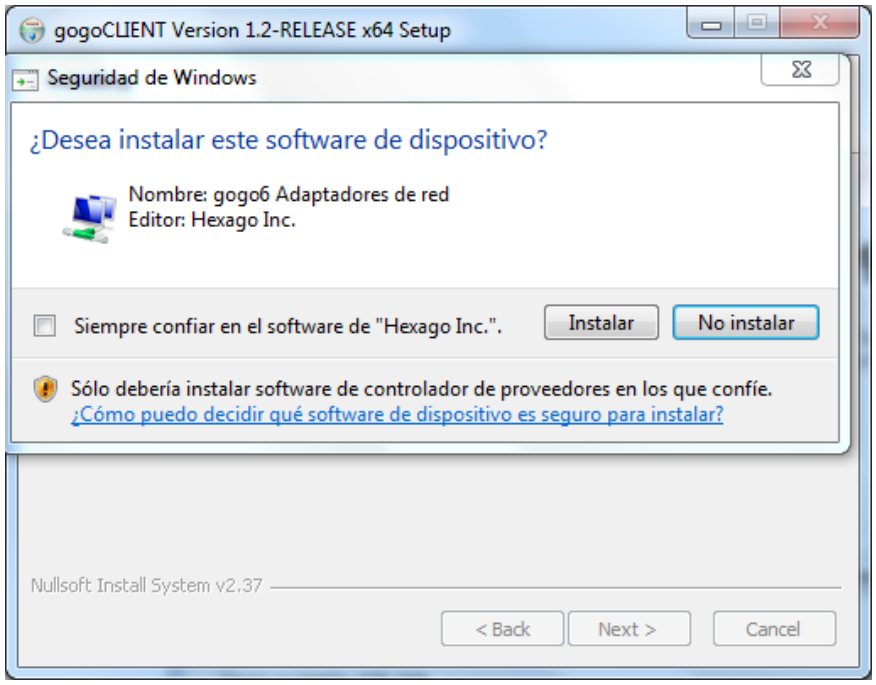

Ilustración 70: *Instalación Gogoc 4, (Aguas Bucheli, 2014)*

- Damos clic en instalar

- Despues de instalar, aparece la siguiente ventana:

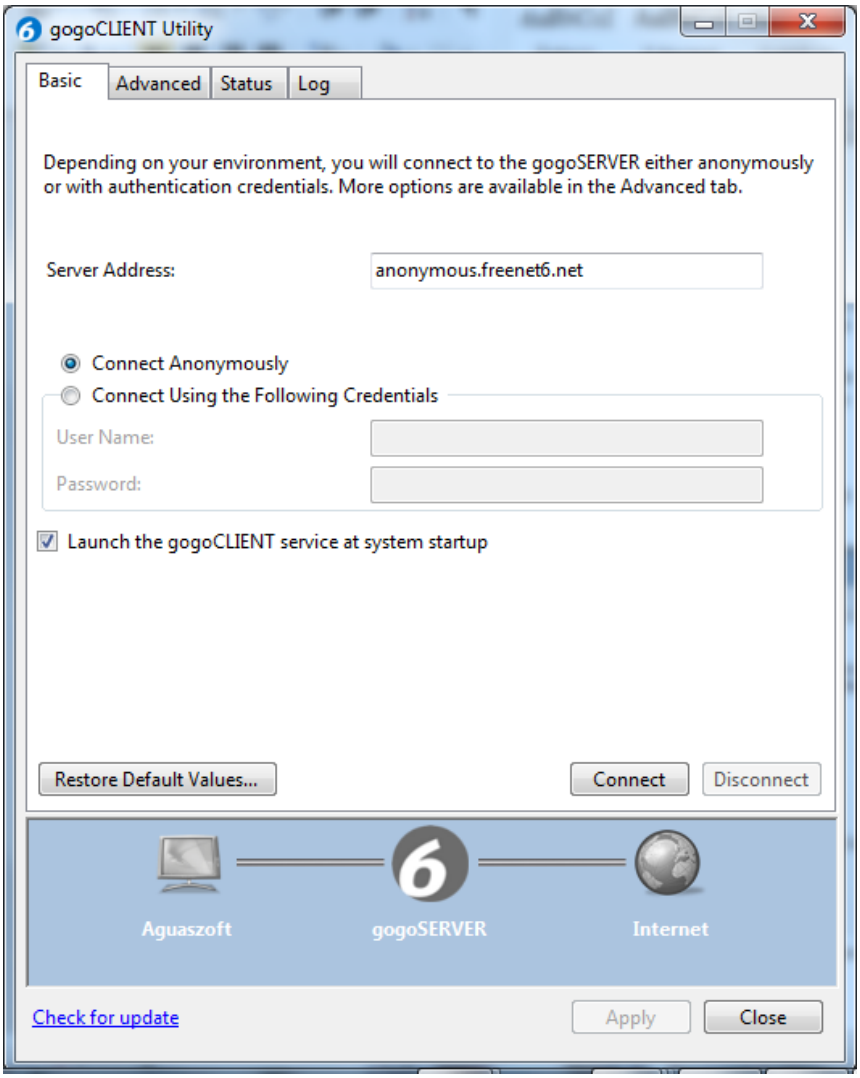

Ilustración 71: *Funcionamiento Gogoc 1, (Aguas Bucheli, 2014)*

- Después dando clic en el botón connect de la barra de tarea

- En la ventana de gogoclient Utility, aparece lo siguiente:

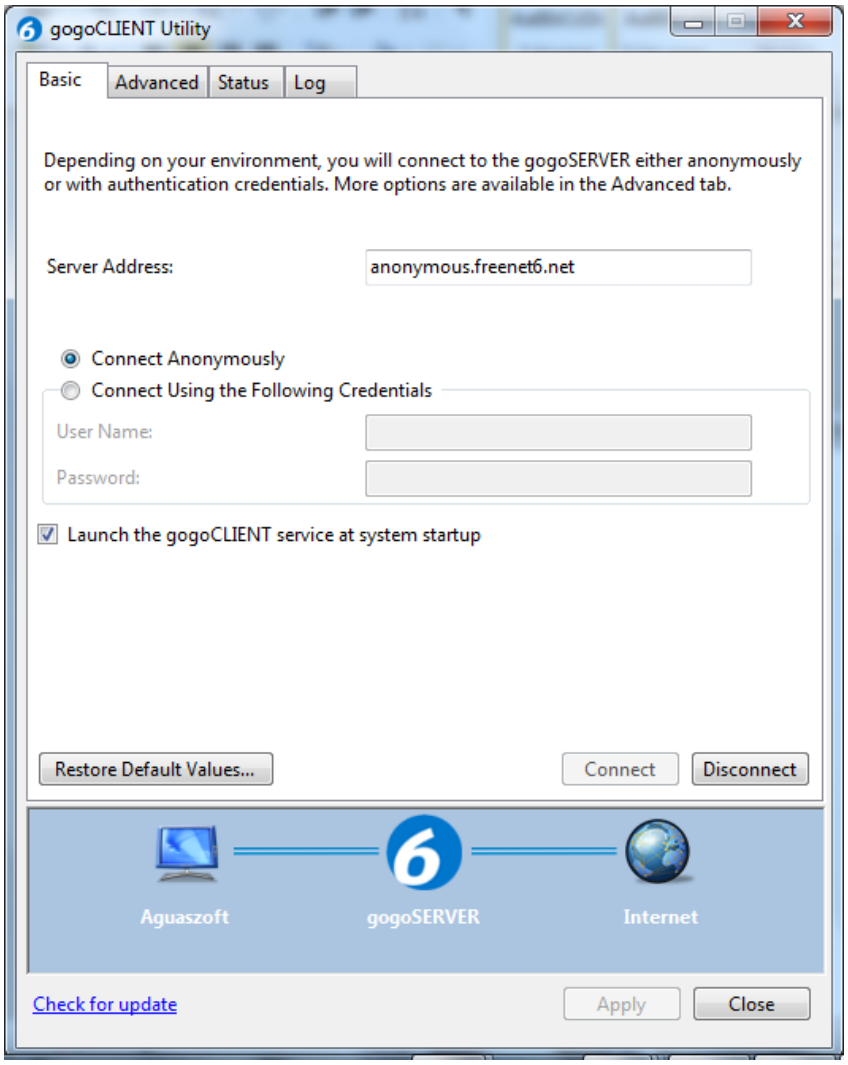

Ilustración 72: *Funcionamiento Gogoc 2, (Aguas Bucheli, 2014)*

- En la pestaña de avanzado tenemos:

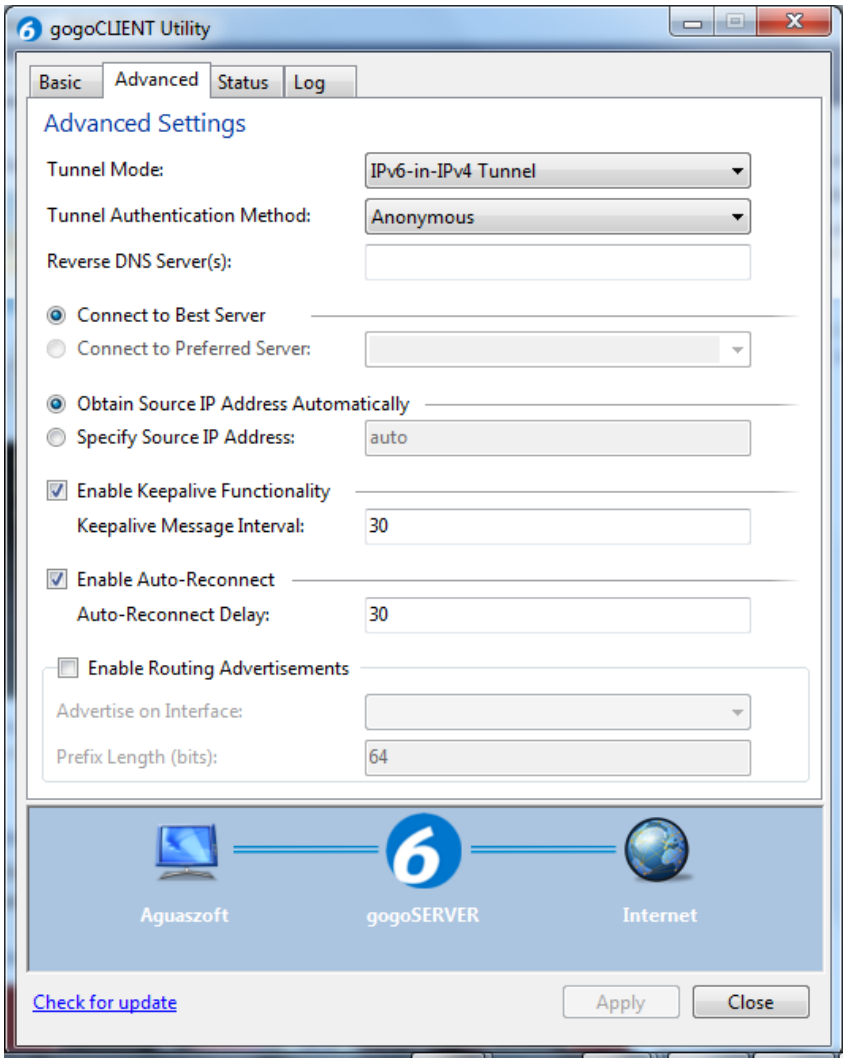

Ilustración 73: *Funcionamiento Gogoc 3, (Aguas Bucheli, 2014)*

- En esta opción podemos escoger parámetros como el modo de túnel, el tipo de autentificación, y las funcionalidades
- En status observamos lo siguiente:

Ilustración 74: *Funcionamiento Gogoc 4, (Aguas Bucheli, 2014)*

- En este caso observamos, el modo de tunnel, la dirección IPV4 y IPV6 asignada. Dando clic en la pestaña de log, tenemos lo siguiente:

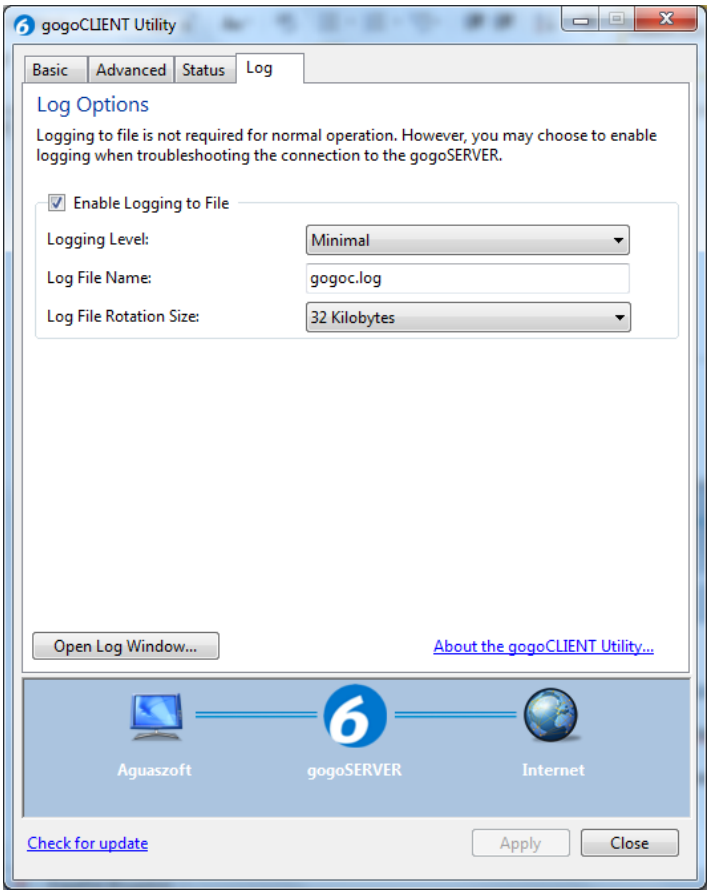

Ilustración 75: *Funcionamiento Gogoc 5, (Aguas Bucheli, 2014)*

- Si damos clic en el botón open log, tenemos:

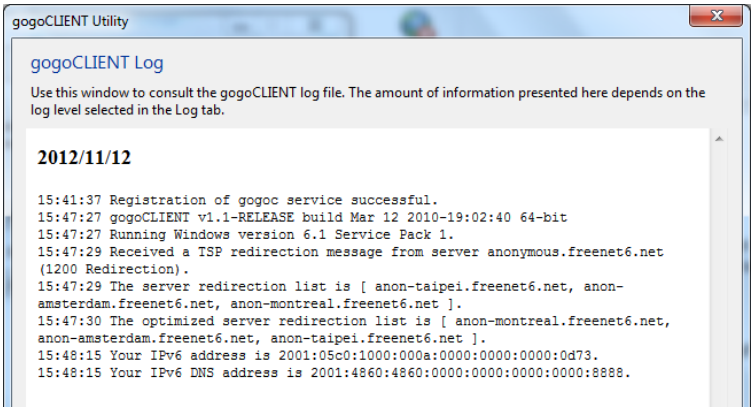

Ilustración 76: *Logs de gogoclient, (Aguas Bucheli, 2014)*

- En esta parte se visualiza la ip que se creó a través del gogoc.

- Para verificar si todo fue creado satisfactoriamente, ingresamos a la siguiente dirección:

  http://test-ipv6.com/

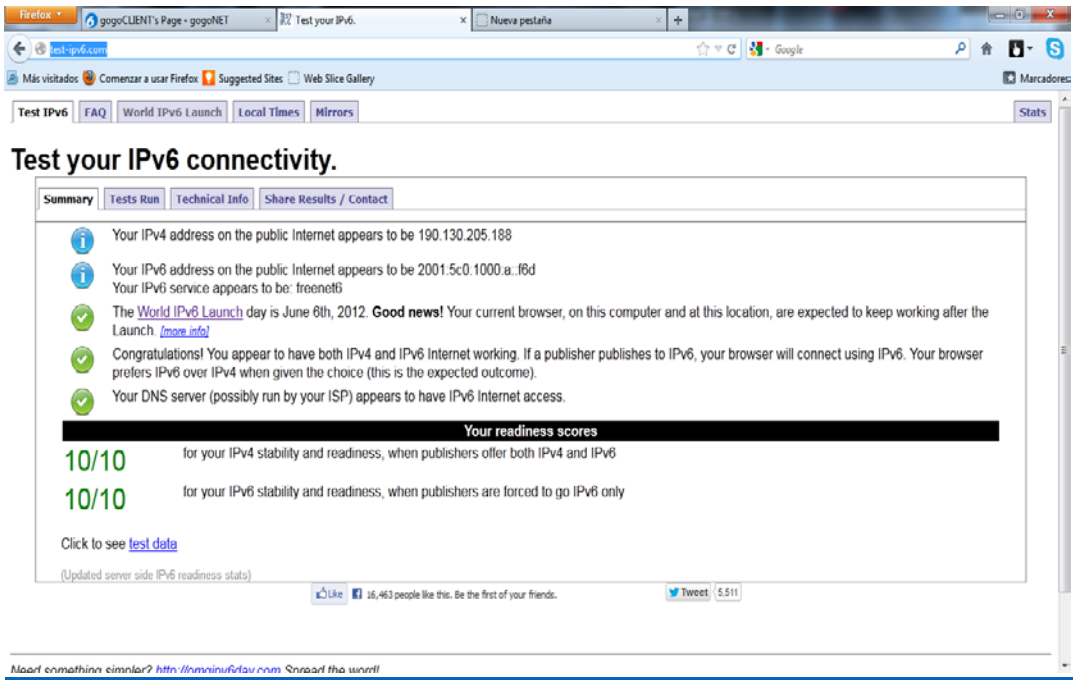

Ilustración 77: *Verificación de Conectividad, (Aguas Bucheli, 2014)*

- Otra forma de verificar es realizando un ping a la dirección:

2001:05c0:1000:000a:0000:0000:0000:0f6d

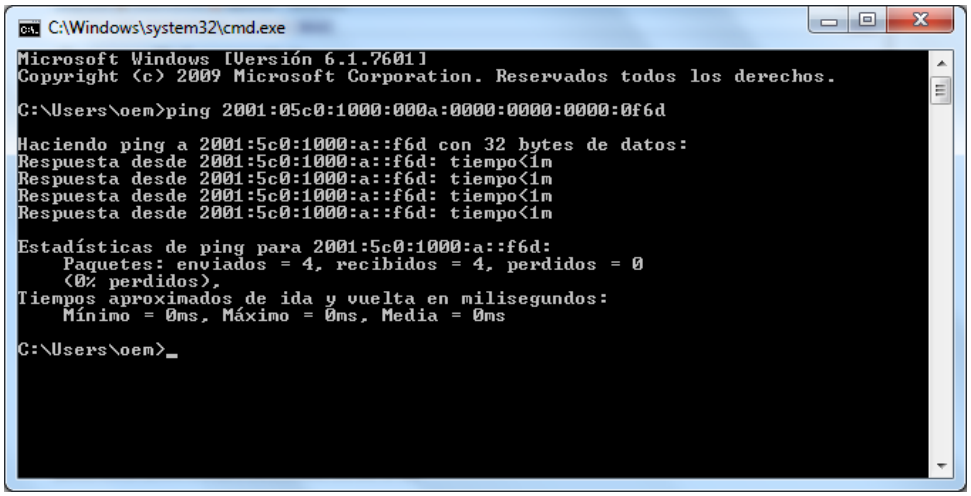

Ilustración 78: *Verificación de conectividad mediante el comando ping, (Aguas Bucheli, 2014)*

- Si el ping fue exitoso, la configuración fue correcta.

3.10. ¿CÓMO SERÁ EL FUTURO CON IPV6?

La verdad resumida es que todo será normal, igual que con IPv4, con ciertas pequeñas diferencias que poco a poco se irán olvidando.

Si te fijas ahora, es relativamente fácil recordar la IPv4, pues no sé, asi rápidamente puedo acordarme de un servidor que tuvimos hace muchos años: 67.15.12.90, o de una IP de otra red que tuvimos 174.142.111.40, pues son IPs con las que hemos trabajado durante mucho tiempo.

Sin embargo no creo acordarme de cuál es la IPv6 que usamos, pues son números muy largos. Y bueno, no sé, quizá es que no ha pasado suficiente tiempo, pero quién sabe dentro de unos años hayan personas que les comiencen a recordar.

Hay propuestas de ponerles nemotécnicos a las IPv6 aprovechando el hecho de que IPv6 utiliza letras desde la a hasta la f y números que pueden pasar por letras (la O sería el 0, la I sería el 1, el 5 sería la S, una t pasaría por un 7, etc). Por ejemplo esta IPv6:

2a03:2880:10:cf01:face:b00c::

Pero volvamos a la realidad: es un tema que no nos debe preocupar mucho, quizá yo puedo recordar dos IPv4, y ninguna IPv6, quizá dentro de un año o dos pueda reconocer de dónde es una de las IPv6 pero la idea detrás de IPv6 es que todo equipo que se conecte a la red tenga una IPv6 pública para él, y no es que vamos a tener 3 ó 4 equipos, sino que incluso dentro de una misma casa, e incluso sin que el dueño lo sepa, los equipos vendrán con IPv6 para realizar tareas administrativas en ellos.

Cisco estima que para el 2016 existan unas 18.9 mil millones de conexiones de red (equipos), comparado con los 10.3 mil millones del 2011 se ve que es un incremento gigantesco a 5 años plazo. Por tanto esta variante de crear IPs mnemotécnicas, quizá sea gracioso, curioso, interesante, pero no será la regla para las direcciones IPs dentro de 10 años. Y recaeremos nuevamente en nombres fáciles de recordar o protocolos que nos ayuden a encontrar equipos en esta siempre creciente red; no sólo DNS sino protocolos de autodescubrimiento, de reporte, etc.

Encontrar a un ciber-delincuente será más difícil, puede serlo, pero no dudo que las técnicas de detección de eventos de ciberdelincuencia deban ser mejoradas o creadas. Por un lado cada equipo tendrá su propia IP, ya no habrá o no se requerirá de NAT que era usado por los delincuentes para

cometer sus fechorías con la esperanza de quedar impunes, ahora todo equipo tendrá su propia IPv6, por tanto se sabrá con mucha certeza cuál es la IPv6 que cometió un determinado delito.

Pero no podemos asociar al responsable de una IP con un delito, como tampoco podemos asociar al dueño de un teléfono con una acción delictiva (llamada delictiva), hay que buscar otros mecanismos.

Si bien es cierto que se recomienda que una IPv6 se asigne por la máquina en virtud de su MAC address, existen personas que promueven el que no se asigne la IP dada la MAC address, pues por esta parte de la IP (sufijo) basada en la mac address podrían tracearte comerciantes interesados en tu perfil: tus gustos, necesidades, lugares por donde vas, etc, es por esto que muchos sistemas operativos asignan la IP no por la MAC sino mediante un número aleatoriamente generado. Así que no podemos confiar en una IP para encontrar una MAC

Esta afirmación es total y absolutamente incorrecta. Asume que el firewall es el dispositivo de IPv4 que hace NAT, pues un NAT a la final se convirtió en un “firewall de facto”.

La realidad es que antes de que existiera NAT, en los años 80 y 90, los equipos en las redes IPv4 tenían IPs públicas y enfrente de esas redes existían firewalls que capturaban, analizaban y permitían o denegaban el tráfico que quería atravesarles. Por tanto lo mismo se hará ahora en IPv6. Habrá un equipo que actuará de firewall, quizá con dos interfaces de red (o más), una hacia la WAN, hacia la internet y otra hacia la interfaz LAN..

En la interfaz WAN tendrá una IPv6 y hacia la interfaz LAN tendrá y repartirá otras IPv6 dentro de la red. Todas públicas sí, pero el firewall podrá decidir qué paquete deja pasar o no. Por ejemplo el firewall podrá decidir: excepto la IPv6 del servidor web, ningún paquete con destino al puerto 80 le dejaré pasar. Por tanto, aunque, las máquinas tengan una IPv6 que es pública, ellas no podrán tener un servidor web, excepto al que se haya definido como server web.

O más estricto aún, como seguro será: todo paquete que esté intentando abrir una conexión hacia una IPv6 de mi red LAN, no le dejes pasar. Y así nadie podrá llegar a los equipos de la red LAN si es que no se le permitió por otras vías. Y solamente se dejarían pasar paquetes que hayan sido originados desde la LAN si así lo desea el administrador.

Como podemos ver, con IPv6 se nos facilita la labor administrativa, y nos permite que ahora sí, todos los equipos que se deseen; sean estos un ruteador, un servidor, un celular o un refrigerador inteligente, puedan conectarse a la red. Esto augura un futuro espectacularmente interesante, complejo y novedoso para todas las labores de domótica, de control remoto y de administración de dispositivos que aunque actualmente existen, se dificulta mucho su trabajo por el hecho de tenerse que utilizar NAT en las redes.

3.10.1. ¿Y QUÉ HABRÁ DESPUÉS DE IPV6?

Es lógico, luego que te hemos hablado de esta explosión en la cantidad de dispositivos que se conectarán por IPv6 pues pensarás que la IPv6 se agotará ¿verdad?

Imagínate, si antes cada persona de este planeta tenía como promedio 1.5 dispositivos conectados a la red, se espera que este número se duplique para dentro de 5 años, y cómo será dentro de 10 ó 20 años. Definitivamente se agotarán las IPv6.

Sí, IPv6 contiene un número finito de direcciones, que como seguramente has visto son 2^128 direcciones IPs, es decir, 340 trillones de trillones de trillones de direcciones. La verdad es que es un número que simplemente no cabe en nuestras mentes, no intentes visualizarlo pues no es fácil de comprender. Pero es un número inmenso, inmensamente finito!!

Se estima que haya disponibilidad de IPv6 para unos 60 años, con medidas de ahorro y de sabia asignación de direcciones IPv6, este sistema debe durar para unos 100 años en realidad.

A mi me tranquiliza, pues en 100 años no estaré aquí. Y me tranquiliza aún más una realidad: ningún protocolo de red ha llegado a durar tanto. Piensa en los antiguos protocolos: aloha, netbios, ipx/spx, etc han desaparecido luego de varios años, 10, 20, 30, etc.. Y me tranquiliza aún más la certeza de que muy posiblemente dentro de 100 años esta internet que hoy vemos maravillados y emocionados, sea un rudimento de lo que se use en ese momento, con sistemas integrados en el cuerpo, transporte virtual, internet interplanetaria. Algo así como lo que era la comunicación cuando samuel morse y lo que es ahora la comunicación entre personas.

La verdad sea dicha: estoy seguro que dentro de 20 ó 30 años, ya cuando seamos viejitos los que ahora nos vemos jóvenes. Dentro de este tiempo se habrán creado posiblemente más de un protocolo que venga a sustituir a IPv6, porque quizá demuestre ser más eficiente, o más abarcador,

o más universal, o lo que sea. Entonces no es de temer, es casi seguro que mucho antes de que IPv6 se agote, este haya sido lentamente reemplazado por uno mejor.

4. CONCLUSIONES Y RECOMENDACIONES

4.1. 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.
- 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.
- El protocolo ipv6 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.

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

4.2. RECOMENDACIONES

- Que se realicen temas de disertación partiendo de este como: IPv4 e IPv6 en dispositivos móviles, IPv6 en Wireless, Vulnerabilidades de IPv6, entre otros.
- Incrementar la presencia de la industria y la comunidad académica en proyectos nacionales, relacionados con IPv6.
- Incrementar las actividades de investigación aplicada en la industria y en la comunidad académica.
- Apoyar e impulsar las iniciativas del sector privado para el desarrollo de nuevas redes, servicios y aplicaciones IPv6 por parte de las administraciones públicas.
- Promover la implantación de IPv6 por parte de las asociaciones profesionales y empresariales

- Promover el uso de nuevas redes, servicios y aplicaciones IPv6 en el sector público por parte de las administraciones públicas.
- Explorar el impacto de IPv6 en la provisión de seguridad extremo a extremo y auditoría de la información, así como de la protección de datos de carácter personal.
- Potenciar proyectos que permitan la exploración de dicho impacto mediante provisión de plataformas de seguridad en pilotos y redes emergentes IPv6.

5. 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

6. GLOSARIO

802.11a: Estándar de red inalámbrica IEEE que especifica una tasa de transferencia máxima de 54 Mbps y una frecuencia de funcionamiento de 5 GHz.

802.11b: Estándar de red inalámbrica IEEE que especifica una tasa de transferencia máxima de 11 Mbps y una frecuencia de funcionamiento de 2,4 GHz.

802.11g: Estándar de red inalámbrica IEEE que especifica una tasa de transferencia máxima de 54 Mbps y una frecuencia de funcionamiento de 2,4 GHz y con compatibilidad con versiones anteriores con dispositivos 802.11b.

Actualizar: Sustituir el software o firmware existente con una versión más moderna.

Adaptador: Dispositivo que añada funcionalidad de red a su equipo.

Ad-hoc: Grupo de dispositivos inalámbricos que se comunican directamente entre ellos (punto a punto) sin la utilización de un punto de acceso.

AES: (Estándar avanzado de cifrado) Técnica de cifrado de datos simétrica de bloque de 256 bits.

Ancho de banda: Capacidad de transmisión de un dispositivo o red determinado.

Banda ancha: Conexión a Internet de alta velocidad y siempre activa.

Banda ISM: Banda de radio utilizada en las transmisiones de redes inalámbricas.

Base de datos: Recopilación de datos que puede organizarse de forma que pueda sus contenidos puedan accederse, gestionarse y actualizarse fácilmente.

Bit: (dígito binario). La unidad más pequeña de información de una máquina.

Byte: Una unidad de datos que suele ser de ocho bits.

Cargar: Transmitir un archivo a través de una red.

CSMA/CA: (Acceso múltiple de detección de portadora) Un método de transferencia de datos que se utiliza para prevenir una posible colisión de datos.

Cifrado: Cifrado es la manipulación de datos para evitar que cualquiera de los usuarios a los que no están dirigidos los datos puedan realizar una interpretación precisa.

Conmutador:

1. Dispositivo que es el punto central de conexión de equipos y otros dispositivos de una red, de forma que los datos puedan transmitirse a velocidad de transmisión completa.
2. Dispositivo para realizar, interrumpir o modificar las conexiones de un circuito eléctrico.

CTS: (Limpiar para enviar) Señal enviada por un dispositivo para indicar que está preparado para recibir datos.

DDNS: (Sistema dinámico de nombres de dominio) Permite albergar un sitio Web, servidor FTP o servidor de correo electrónico con un nombre de dominio fijo (por ejemplo, www.xyz.com) y una dirección IP dinámica.

Descargar: Recibir un archivo transmitido a través de una red.

DHCP: (Protocolo de configuración dinámica de host) Protocolo que permite a un dispositivo de una red, conocido como servidor DHCP, asignar direcciones IP temporales a otros dispositivos de red, normalmente equipos.

Dirección IP: Dirección que se utiliza para identificar un equipo o dispositivo en una red.

Dirección IP dinámica: Dirección IP temporal que asigna un servidor DHCP.

Dirección IP estática: Dirección fija asignada a un equipo o dispositivo conectado a una red.

Dispersión de secuencia: Técnica de frecuencia de radio de banda ancha que se utiliza para la transmisión más fiable y segura de datos.

DMZ: (Zona desmilitarizada) Suprime la protección de servidor de seguridad del enrutador de un equipo, permitiéndole que pueda “verse” desde Internet.

DNS: (Servidor de nombres de dominio) La dirección IP de su servidor ISP, que traduce los nombres de los sitios Web a direcciones IP.

DSL: (Línea de suscriptor digital) Conexión de banda ancha permanente a través de las líneas de teléfono tradicionales.

DSSS: (Espectro de dispersión de secuencia directa). Transmisión de la frecuencia con un patrón de bit redundante que se traduce en una menor probabilidad de que la información se pierda durante dicha transmisión.

DTIM: (Mensaje de indicación de tráfico de entrega). Mensaje incluido en paquetes de datos que puede aumentar la eficacia inalámbrica.

Dúplex completo: La disponibilidad de un dispositivo de red para recibir y transmitir datos de forma simultánea.

Dúplex medio: Transmisión de datos que puede producirse en dos direcciones a través de una única línea, pero sólo en una dirección cada vez.

EAP: (Protocolo de autenticación extensible). Protocolo general de autenticación que se utiliza para controlar el acceso a redes. Muchos métodos de autenticación específicos trabajan dentro de este marco.

EAP-PEAP: (Protocolo de autenticación extensible-Protocolo de autenticación extensible protegido). Método de autenticación mutua que utiliza una combinación de certificados digitales y otros sistemas, como contraseñas.

EAP-TLS: (Protocolo de autenticación extensible-Seguridad de la capa de transporte) Método de autenticación mutua que utiliza certificados digitales.

Encadenamiento de periféricos: Método utilizado para conectar dispositivos en serie, uno tras otro.

Enrutador: Dispositivo de red que conecta redes múltiples, tales como una red local e Internet.

Enrutamiento estático: Reenvío de datos de una red a través de una ruta fija.

Ethernet: Protocolo de red estándar de IEEE que específica la forma en que se colocan los datos y se recuperan de un medio de transmisión común.

Finger: Programa que le facilita el nombre asociado con una dirección de correo electrónico.

Firmware: El código de la programación que ejecuta un dispositivo de red.

Fragmentación: Dividir un paquete en unidades menores al transmitirlas a través de un medio de red que no puede admitir el tamaño original del paquete.

Frase secreta: Se utiliza con mucha frecuencia como una contraseña, ya que una frase secreta simplifica el proceso de cifrado WEP generando de forma automática las claves del cifrado WEP para los productos Linksys.

FTP: (Protocolo de transferencia de archivos) Protocolo estándar de envío de archivos entre equipos a través de redes TCP/IP e Internet.

Hardware: El aspecto físico de equipos, telecomunicaciones y otros dispositivos de tecnologías de la información.

HTTP: (Protocolo de transferencia de hipertexto) Protocolo de comunicaciones utilizado para conectarse a servidores de la World Wide Web.

IEEE: (Instituto de ingenieros eléctricos y electrónicos) Instituto independiente que desarrolla estándares de redes.

Infraestructura: Equipo de red e informático actualmente instalado.

Inicio: Iniciar un dispositivo y provocar que comience a ejecutar instrucciones.

Intervalo de indicador: El intervalo de frecuencia del indicador, que es una emisión de paquetes de un enrutador para sincronizar una red inalámbrica.

IP: (Protocolo Internet) Protocolo utilizado para enviar datos a través de una red.

IPCONFIG: Utilidad de Windows 2000 y XP que muestra la dirección IP de un dispositivo de red concreto.

IPSEC: (Seguridad del protocolo Internet) Protocolo VPN utilizado para implementar el intercambio seguro de paquetes en la capa IP.

ISIP: (Proveedor de servicios de Internet) Compañía que proporciona acceso a Internet.

Itinerancia: Capacidad de transportar un dispositivo inalámbrico desde el alcance de un punto de acceso hasta otro sin perder la conexión.

LAN: (Red de área local) Los equipos y productos de red que componen la red doméstica o de oficina.

LEAP: (Protocolo de autenticación extensible ligero) Método de autenticación mutua que utiliza un sistema de usuario y contraseña.

MAC: (Dirección de control de acceso al medio) Una dirección MAC es la dirección de hardware de un dispositivo conectado a un medio de red compartido.

Máscara de subred: Código de dirección que determina el tamaño de la red.

Mbps: (Megabits por segundo) Un millón de bits por segundo, unidad de medida de transmisión de datos.

MIRC: Programa de Internet Relay Chat que se ejecuta bajo Windows.

Módem de cable: Un dispositivo que conecta una equipo a la red de la televisión por cable que a su vez se conecta a Internet.

Modo infraestructura: Configuración en la que se realiza un puente entre una red inalámbrica y una red con cable a través de un punto de acceso.

Multidifusión: Envío de datos a un grupo de destinos a la vez.

NAT: (Traducción de direcciones de red) La tecnología NAT traduce direcciones IP de la red de área local a una dirección IP diferente para Internet.

Navegador: Programa de aplicación que proporciona una forma de consultar e interactuar con la información de la World Wide Web.

NNTP: (Protocolo de transferencia de noticias a través de la red) Protocolo utilizado para conectar a los grupos Use net de Internet.

Nodo: Unión de red o punto de conexión, habitualmente un equipo o estación de trabajo.

OFDM: (Multiplexado por división de frecuencia ortogonal) La transmisión de frecuencia que separa la corriente de datos en un número de corrientes de datos de velocidad inferior que se transmiten en paralelo para prevenir que se pierda información durante la transmisión.

Paquete: Un paquete es un pequeño bloque de datos transmitido en una red de conmutación de paquetes.

PEAP: (Protocolo de autenticación extensible protegido) Protocolo para la transmisión de datos de autenticación, incluyendo contraseñas, a través de redes inalámbricas 802.11.

Ping: (Buscador de paquetes de Internet) Utilidad de Internet que se utiliza para determinar si una dirección IP determinada está en línea.

Pirata informático: Un término de jerga para un entusiasta informático. También hace referencia a los individuos que obtienen acceso no autorizado a sistemas informáticos con el fin de robar y corromper datos.

Poe: (Alimentación a través de Ethernet) Tecnología que permite a un cable de red Ethernet transmitir tanto datos como corriente.

POP3: (Protocolo de oficina de correo 3) Protocolo estándar utilizado para recuperar correo electrónico almacenado en un servidor de correo.

PPPoE: (Protocolo a través de Ethernet punto a punto) Tipo de conexión de banda ancha que proporciona autenticación (usuario y contraseña) además de transporte de datos.

PPTP: (Protocolo de túnel punto a punto) Protocolo VPN que permite tunelar el protocolo Punto a punto (PPP) a través de una red IP. Este protocolo se utiliza también como tipo de conexión de banda ancha en Europa.

Preámbulo: Parte de la señal inalámbrica que sincroniza el tráfico de red.

Puente: Dispositivo que conecta dos tipos diferentes de redes locales, como por ejemplo una red inalámbrica a una red Ethernet con cable.

Puerta de enlace: Un dispositivo que interconecta redes con protocolos de comunicaciones diferentes e incompatibles.

Puerta de enlace predeterminada: Dispositivo que re direcciona tráfico de Internet desde su red de área local.

Puerto: Punto de conexión en un equipo o dispositivo de red utilizado para conectar un cable o adaptador.

Punto de acceso: Dispositivo que permite a los equipos y a otros dispositivos equipados con función inalámbrica comunicarse con una red con cable. También se utiliza para ampliar el alcance de una red inalámbrica.

RADIUS: (Servicio de usuario de marcado con autenticación remota) Protocolo que utiliza un servidor de autenticación para controlar acceso a redes.

Red: Serie de equipos o dispositivos conectados con el fin de compartir datos, almacenamiento y la transmisión entre usuarios.

Red troncal: Parte de una red que conecta la mayoría de los sistemas y los une en red, así como controla la mayoría de datos.

Rendimiento: Cantidad de datos que se han movido correctamente de un nodo a otro en un periodo de tiempo determinado.

RJ-45: (Toma registrada 45) Conector Ethernet que alberga hasta ocho hilos.

RTP: (Protocolo de tiempo real) Un protocolo que permite especializar aplicaciones tales como llamadas telefónicas, vídeo y audio a través de Internet que están teniendo lugar a tiempo real.

RTS: (Solicitud para enviar) Método de red para la coordinación de paquetes grandes a través de la configuración Umbral de solicitud de envío (RTS).

Servidor: Cualquier equipo cuya función en una red sea proporcionar acceso al usuario a archivos, impresión, comunicaciones y otros servicios.

Servidor de seguridad: Un servidor de seguridad es cualquiera de los esquemas de seguridad que evitan a los usuarios no autorizados obtener acceso a una red de equipos o que supervisa la transferencia de información hacia y desde la red.

Servidor de seguridad SPI: (Inspección de paquetes de datos) Una tecnología que inspecciona los paquetes de información entrantes antes de permitirles que entren en la red.

SMTP: (Protocolo simple de transferencia de correo) Protocolo de correo electrónico estándar de Internet.

SNMP: (Protocolo simple de administración de redes) Protocolo de control y supervisión de redes ampliamente extendido.

Software: Instrucciones para el equipo. Se denomina “programa” al conjunto de instrucciones que realizan una tarea determinada.

SOHO: (Oficina pequeña/oficina doméstica) El segmento de mercado de profesionales que trabajan en casa o en pequeñas oficinas.

SSID: (Identificador de conjunto de servicio) Nombre de su red inalámbrica.

Tasa TX: Tasa de transferencia.

TCP: (Protocolo de control de transporte) Un protocolo de red para la transmisión de datos que requiere la confirmación del destinatario de los datos enviados.

TCP/IP: (Protocolo de control de transporte/Protocolo Internet) Protocolo de red para la transmisión de datos que requiere la confirmación del destinatario de los datos enviados.

Telnet: Comando de usuario y protocolo TCP/IP que se utiliza para acceder a equipos remotos.

TFTP: (Protocolo trivial de transferencia de archivos) Versión del protocolo FTP TCP/IP que utiliza UDP y no dispone de capacidades de directorio ni de contraseña.

TKIP: (Protocolo de integridad de clave temporal) Protocolo de cifrado inalámbrico que cambia periódicamente la clave de cifrado, haciendo más difícil su decodificación.

TLS: (Seguridad de capa de transporte) Protocolo que garantiza la privacidad y la integridad de los datos entre aplicaciones cliente/servidor que se comunican a través de Internet.

Topología: Distribución física de una red.

UDP: (Protocolo de datagramas de usuario) Protocolo de red para la transmisión de datos que no requieren la confirmación del destinatario de los datos enviados.

URL: (Localizador uniforme de recursos) Dirección de un archivo situado en Internet.

VPN: (Red privada virtual) Medida de seguridad para proteger los datos a medida que abandona una red y pasa otra a través de Internet.

WAN: (Red de área extensa) Grupo de equipos conectados en red en un área geográfica extensa. El mejor ejemplo de WAN es Internet.

WEP: (Protocolo de equivalencia con cable) WEP es un protocolo de seguridad para redes inalámbricas. El objetivo de WEP es proporcionar seguridad mediante el cifrado de datos a través de ondas de radio, de forma que estén protegidos a medida que se transmiten de un punto a otro. Para permitir la comunicación entre los equipos y el enrutador se utiliza una clave compartida (similar a una contraseña). WEP ofrece un nivel básico (pero satisfactorio) de seguridad para la transferencia de datos a través de redes inalámbricas.

WINIPCFG: Utilidad de Windows 98 y Millenium que muestra la dirección IP de un dispositivo de red concreto.

WLAN: (Red de área local inalámbrica) Grupo de equipos y dispositivos asociados que se comunican entre sí de forma inalámbrica.

WPA: (Acceso protegido WiFi) Protocolo de seguridad para redes inalámbricas que se fundamenta en los cimientos básicos de WEP. Asegura la transferencia de datos de forma inalámbrica mediante la utilización de una clave similar a WEP. La robustez añadida de WPA es que la clave cambia de forma dinámica. La clave, en continuo cambio, dificulta que un pirata informático Pueda conocer la clave y obtener acceso a la red.

WPA2: (Acceso protegido Wi-Fi 2) WPA2 es la segunda generación de WPA y proporciona un mecanismo de cifrado más fuerte a través del Estándar de cifrado avanzado (AES), requisito para algunos usuarios del gobierno.

WPA-Enterprise: Versión de WPA que utiliza las mismas claves dinámicas que WPA-Personal y también requiere que todo dispositivo inalámbrico esté autorizado según lista maestra, albergada en un servidor de autenticación especial.

WPA-Personal: Versión de WPA

7. ANEXOS:

7.1. PLAN DE DISERTACIÓN

7.2. REDES

7.3. PROTOCOLOS

7.4. SEGURIDAD

7.5. OTROS