



IPV6: ESTUDIO SOBRE LAS BARRERAS PARA SU IMPLEMENTACIÓN

AUTORES:

GUSTAVO EDUARDO MENDOZA RAMÍREZ

INGENIERÍA DE SISTEMAS

SERGIO ANDRÉS QUINTANA BURGOS

INGENIERÍA ELECTRÓNICA

DIRECTOR:

GIOVANY VASQUEZ MENDOZA

MINOR EN COMUNICACIONES Y REDES

UNIVERSIDAD TECNOLÓGICA DE BOLÍVAR

FACULTAD DE INGENIERÍA

2011

CONTENIDO

LINEA DE INVESTIGACIÓN.....	4
ALCANCE.....	4
CAMPO DE INVESTIGACIÓN.....	4
DESCRIPCIÓN DEL PROBLEMA.....	4
ANTECEDENTES	5
MARCO TEÓRICO	7
ESTADO DEL ARTE	10
JUSTIFICACIÓN	13
OBJETIVOS.....	14
OBJETIVO GENERAL.....	14
OBJETIVOS ESPECÍFICOS	14
METODOLOGÍA.....	15
CAPITULO I: INDAGANDO EN EMPRESAS DE CARTAGENA	16
ENCUESTAS	17
RESULTADOS	26
CAPITULO II: BARRERAS PARA LA IMPLEMENTACIÓN DE IPv6	28
BARRERAS TÉCNICAS	29
EQUIPOS DE RED	30
SEGURIDAD.....	31
FIREWALLS.....	31
IPSEC.....	32
DIRECTACCESS	32
BARRERAS ECONOMICAS	32
CAPITULO III: VENTAJAS Y DIFICULTADES DE IPv6.....	34
CAPITULO IV: MÉTODOS DE TRANSICIÓN DE IPv4 A IPv6.....	39
METODOLOGIAS DE TRANSICION DE IPV4 A IPV6.....	40
DOBLE PILA	41
TÚNELES	41
TRADUCCIÓN.....	44
CREACIÓN DE NODOS	44
SOLUCIONES PARA CLIENTES DE DIRECTACCESS.....	46
HARDWARE – SOFTWARE	47

CONFIGURACIÓN EN SISTEMAS OPERATIVOS UTILIZANDO METODO DE TRANSICION TUNELLING (EJEMPLO PRÁCTICO)	47
TÚNEL BROKER CON HURRICANE ELECTRIC.....	48
CONFIGURACIÓN EN SISTEMA OPERATIVO LINUX	52
CONFIGURACIÓN EN EQUIPOS CISCO LINKSYS WRTS54G.....	53
CONFIGURACIÓN EN SISTEMA OPERATIVO SOLARIS.....	53
CONFIGURACIÓN EN SISTEMA OPERATIVO MAC OSX.....	53
CONFIGURACIÓN EN SISTEMA OPERATIVO WINDOWS XP Y 2000.....	54
CONFIGURACIÓN EN SISTEMA OPERATIVO WINDOWS VISTA Y WINDOWS 7	54
CONCLUSIONES.....	55
RECOMENDACIONES	57
GLOSARIO.....	58
ACRONIMOS.....	58
REFERENCIAS BIBLIOGRÁFICAS.....	59
ANEXOS – Artículo Científico	¡Error! Marcador no definido.

LINEA DE INVESTIGACIÓN

La línea de investigación de este trabajo son las comunicaciones y redes.

ALCANCE

La investigación tendrá un alcance local, basaremos el estudio en empresas ubicadas en la ciudad de Cartagena. El interés es conocer las dificultades que se han encontrado a nivel local para la implementación del protocolo de internet versión 6 y plantear un mecanismo para su implementación.

CAMPO DE INVESTIGACIÓN

Las entidades a las cuales va dirigida la investigación son empresas de la ciudad de Cartagena que se encarguen de temas como: Desarrollo de software, administración de redes, distribución de internet.

DESCRIPCIÓN DEL PROBLEMA

El problema surge debido al agotamiento de direcciones IPv4, al no contar con más direcciones de este tipo, será obligatoria la migración de todas las empresas a este nuevo protocolo IPv6, en la ciudad de Cartagena y el mundo entero. Esta necesidad de migración se ve opacada por el desconocimiento que tienen las empresas sobre este nuevo protocolo y otros factores como los económicos y comerciales que influyen como “barreras” a la hora de pensar en una transición. Es por eso que se pretende establecer las razones por las cuales no se ha realizado la implementación y a partir de dichas razones definir cuál sería la mejor estrategia para su implementación.

ANTECEDENTES

La entrega de los últimos bloques de direcciones IPv4 realizada por IANA el 3 de Febrero de 2011, y el anuncio de ISOC y grandes proveedores de contenidos, de promover una prueba a nivel mundial de conectividad IPv6 el que ocurrió el pasado 8 de Junio, han despertado de nuevo el interés por el tema. Las organizaciones han dado un nuevo ímpetu a la estrategia de revisión de sus redes para dar soporte del protocolo IPv6, de forma que se pueda garantizar la continuidad y el crecimiento de la economía digital. Las nuevas oportunidades de negocio que ofrece IPv6 no podrán desarrollarse plenamente si no se toman las medidas adecuadas para garantizar que la administración pública, proveedores de contenidos, ISPs y la industria en general, toman conciencia del problema y se decidan las acciones pertinentes, de tal forma que los usuarios puedan comenzar a utilizar IPv6 de un modo satisfactorio y casi sin apercibirse del cambio, abriendo la puerta al desarrollo de nuevas aplicaciones y servicios, que a su vez, harán crecer más la demanda de Banda Ancha.

Básicamente ha habido las siguientes fases importantes en el desarrollo de IPv4 hasta Ipv6 [12]:

- 1992 – TUBA (TCP & UDP with Bigger Addresses)
 - Implementación de mecanismos para usar TCP y UDP sobre mayores direcciones.
 - Se emplea ISO CLNP (Connection-Less Network Protocol, “protocol de redes sin conexión”).
 - Se descarta.
 - IETF Publica un llamado para proponer el IPng.
- 1993 – SIPP (Simple IP Protocol Plus)
 - Proyecto “Simple IP Plus”
 - Mezcla de SIP y PIP (dos tentativas anteriores para sustituir IPv4)
 - Direcciones de 64 bits
- 1994 – IPng (IP NextGeneration)

- Se adopta SIPP
- Se cambia el tamaño de las direcciones a 128 bits
- Se renombra como IPv6
- 1995 – Se publica el RFC-1883 con la propuesta del IPv6.
- 1996 – Se crea el 6Bone, como una red de pruebas de Ipv6.
- 1998 – RFC-2460: Especificaciones del Ipv6.
- 2001 – Se implementa IPv6, se presenta el problema de overhead para los carriers.

En Colombia, la Red Nacional Académica de Tecnología Avanzada (RENATA), se ha convertido en la pionera en el uso de IPv6, alcanzando un grado de avance acorde a otras redes académicas en el mundo. Para alcanzar este hito, Telefónica, como proveedor del servicio en Colombia, ha venido trabajando para implementar con éxito la primera red nacional bajo el protocolo IPv6.

Por otro lado, a principios del 2011, se ha conocido que, INTERNEXA, el distribuidor que maneja las redes de telecomunicaciones terrestre más grande y extensa de Suramérica, anunció que ha puesto a disposición de sus clientes una infraestructura preparada para soportar servicios en IPv6, reforzando su compromiso permanente con la calidad y la innovación. Así, INTERNEXA se convierte en una empresa pionera en el continente, que integra el protocolo IPv6 en cada uno de sus 21.217 KM de red de fibra óptica a lo largo de Venezuela, **Colombia**, Perú, Ecuador, Chile y en los próximos meses, Argentina y Brasil.

MARCO TEÓRICO

Las Comunicaciones y Tecnologías de la información en los últimos años, han tomado auge en nuestras vidas. Se han desarrollado y diseñado muchísimas tecnologías y servicios las cuales han permitido a las personas comunicarse y estar en contacto, facilitando de una u otra manera la vida de las personas. Los medios “habituales”, como la televisión, radio, telefonía, se han visto desplazados por el internet, una red que puede incluir todo lo anterior en una sola. Pero como no todo los avances tienden a mostrar cosas positivas, ha quedado al descubierto que el protocolo IPv4, la base en la actualidad del Internet, tiene muchísimas limitantes. El protocolo IP es aquel en el cual se basa la transmisión de datos en Internet, basándose en transmisión de datagramas, haciéndolo por medio de sistemas connectionless y brindando un tipo de servicio besteffort.

El uso de IPv4 ha cambiado drásticamente en los últimos 30 años. La especificación inicial de diseño no tuvo en cuenta la necesidad de que el protocolo manejaría servicios de video bajo demanda, u otros tipos de datos a gran escala, también la llegada de las comunicaciones móviles, donde cada dispositivo requiere una dirección IP. Cuando se creó, se pensó que este constaba con un número amplio de direcciones para todo el mundo. Estas direcciones se veían casi inalcanzable, pero con el crecimiento enorme que ha tenido Internet en los últimos años, se dieron rangos excesivos (millones de IP) a países enteros e incluso miles de IP fueron asignadas a grandes empresas, aparte de eso se utilizó un rango muy amplio para las **redes privadas**, algo que hizo aún más pequeño ese número y lo peor es que muchas de estas IPs que han sido asignadas actualmente no están siendo utilizadas por una u otras razones, pudiéndose decir que estas se están desperdiciando. Se llegaron a proponer soluciones como recuperar algunas de las IPv4 que habían sido asignadas e incrementar el uso de NAT (NETWORK ADDRESS TRANSLATION) [1].

Este tipo de tecnología IPv4 ha mostrado muchas falencias a la hora de perder conectividad “punto a punto” y esto dificulta el accionar o el vuelo de muchas

de las aplicaciones que existen hoy en día, produciendo que muchos por no decir casi todos los servicios y aplicaciones que existen en la red se vuelvan costosas impidiendo innovar.

Como posible solución a este problema, se planteó un protocolo, llamado IPv6, el cual fue desarrollado durante la década de los 90, con el único fin de sustituir al protocolo actual IPv4, buscando solucionar aquellos inconvenientes que se presentan con la versión actual, brindando así una base para aquellos futuros desarrollos y cualquier avance que se desee tener en Internet. Los principales cambios que se realizaron fueron:

- Ampliación del campo de direcciones IP a 128 bits, aumentando de 32 a 128 bits cada dirección, se aumentó el número de direcciones significativamente [6].
- Campos de longitud fija, para facilitar el proceso que se le da a cada datagrama en los enrutadores para encaminarlo hacia su destino, adoptando un formato fijo el cual agiliza el tráfico de estos y las opciones siguen estando pero ya no como parte del encabezado.

Se puede decir que con esta tecnología IPV6 se obtendrá un mayor espacio de direcciones, por lo tanto surgen dos sistemas de agregación de direcciones [8]:

- Agregación por proveedores.
- Agregación geográfica.

Típicamente, los proveedores de servicio proporcionan a sus suscriptores bloques contiguos de direcciones correlativas, que son usadas por organizaciones individuales para crear sus propias jerarquías de direcciones locales e identificar subredes y hosts.

Los routers de Internet deben mantener más de 40000 rutas. Conforme Internet continúe creciendo, la aplicación uniforme encaminamiento jerárquico de IPv6 será posiblemente el único método viable para mantener el tamaño de las tablas de encaminamiento de los routers bajo control. Las direcciones basadas

en agregación sólo son parte del espacio de direcciones total definido por IPv6. Otros rangos de direccionamiento han sido asignados a multicasting y a nodos que solo requieren direcciones únicas en un área delimitada.

La seguridad estará intrínseca en el núcleo del protocolo [7], IPv6 utiliza IPSec en todos los nodos [10]. IPSec se compone de un conjunto de protocolos criptográficos que se proporcionan para asegurar el envío de datos y el uso de clave. Los paquetes IPv6 de acuerdo a su diseño, disponen de una cabecera destinada a la Autenticación de los paquetes, realizada con el “**AuthenticationHeader**”[9].

Por otro lado, se ha incluido un Cifrado de seguridad(**Encrypted Security Payload, ESP**). De esta forma se garantiza que tan sólo el destinatario legítimo del datagrama pueda descifrar el contenido del datagrama, ofreciendo autenticación y confidencialidad (encriptación) dentro del núcleo del protocolo cumpliendo así con los requerimientos de seguridad de cada usuario en particular, es por ello que viene de manera obligatoria IPsec.

La autenticidad y el cifrado de datos (o datagramas) requieren que tanto el emisor como el receptor compartan una clave, un algoritmo de cifrado/descifrado y una serie de parámetros (por ejemplo, el tiempo de validez de la clave) que diferencian una comunicación segura de otra. Estos parámetros conforman la asociación de seguridad (Security Association, SA) [11] que permitan unir la autenticidad y la seguridad en IPSec. También podrá tener una Calidad de Servicio (QoS) y Clase de Servicio (CoS), Multicast, Anycast, paquetes IP eficientes y extensibles, sin que haya fragmentación en los routers.

ESTADO DEL ARTE

Desde hace varios años se ha planteado la incertidumbre de si se debe migrar a IPv6 o no [2] [3] pero han sido muy pocos los avances que se han logrado en este tema, por tanto, han sido pocas las implementaciones en la industria.[4] Interoperabilidad entre hardware y software, mejoras en los equipos, la resistencia que han tenido las personas al cambio de protocolo, la experiencia limitada con el uso y aplicación de este nuevo protocolo, la dificultad de tiempo de programación y el incierto retorno de ganancias a los inversionistas son algunas de las barreras que no han permitido la implementación del nuevo protocolo IPv6[5].

Según estudios realizados, la transición de IPv4 a IPv6 no se dará de la noche a la mañana. Las dos versiones de IP deberán convivir durante muchos años. Básicamente, IPv6 podría implementarse como un tipo de actualización de software en los nodos IPv4 actuales, comenzando un período de transición para minimizar los costos de nuevos equipos y proteger las fuertes inversiones realizadas. Un problema grave es que no se puede saber cuándo las operadoras en Internet migrarán a la tecnología IPv6. En la actualidad la gran mayoría de las operadoras utiliza nodos IPv4, y con esta situación, donde casi todo el tráfico debería adaptarse a redes basadas en IPv4, la motivación para el cambio es muy baja. Las nuevas características de autoconfiguración, que hace que las redes IPv6 más fáciles de configurar y mantener que las redes IPv4, pueden ser atractivas para nuevas operadoras que han de realizar un despliegue de infraestructura muy rápido. Por otro lado, para facilitar la migración es importante que las aplicaciones IPv4 existentes sean capaces de operar también con las aplicaciones IPv6; por ejemplo, los navegadores de Internet deben ser capaces de comunicarse utilizando IPv6 e IPv4.

El principal problema que se ha detectado es que mientras los sistemas IPv6 pueden enviar, encaminar y recibir paquetes IPv4, los sistemas IPv4 actuales no son capaces de manejar paquetes IPv6. En un mundo ideal, lo correcto sería declarar unos días de inactividad, durante los cuales todas las máquinas

de Internet serán desactivadas, y se migraría de IPv4 a IPv6. No obstante, una tarea así, con millones de máquinas y de administradores de redes implicados, es prácticamente un absurdo.

La primera opción es introducir los protocolos, IPv4 e IPv6, en los nodos IPv6, con lo que este nodo IPv6/IPv4 puede enviar y recibir paquetes IPv6 e IPv4. Cuando trabaje con un nodo IPv4, el nodo IPv6/IPv4 puede utilizar paquetes IPv4; cuando trabaje con un nodo IPv6, puede utilizar paquetes IPv6. Los nodos IPv6/IPv4 deben tener tanto direcciones IPv6 como IPv4. Deben de ser capaces también de descubrir si otro nodo es capaz de utilizar IPv6 o sólo IPv4. Esto se puede conseguir utilizando el protocolo de resolución de nombres de dominio o DNS, que puede devolver una dirección IPv6 si el nombre del nodo que se está resolviendo es capaz de utilizar IPv6, o bien una dirección IPv4 en caso contrario. Por supuesto, si el nodo que hace la petición DNS únicamente puede utilizar IPv4, DNS devolverá sólo una dirección IPv4.

Según este método, si cualquiera de los nodos intermedios sólo puede operar con IPv4, se deben utilizar paquetes IPv4. Por ello, es posible que la comunicación entre dos nodos extremos IPv6, tenga lugar con paquetes IPv4. Lo que se hace es que ambos extremos envían paquetes IPv6, pero cuando estos lleguen a un nodo IPv4, todo el paquete IPv6 será encapsulado en el campo de datos del paquete IPv4 y se llevará a cabo una correspondencia de direcciones, perdiendo la información relevante de los campos de la cabecera IPv6.

La segunda opción es utilizar túneles. Esto permitiría que los nodos extremos IPv6 se comuniquen siempre en IPv6, aunque haya nodos intermedios IPv4. Se considera un túnel a todos los nodos IPv4 entre dos nodos IPv6.

Utilizando esta técnica, el nodo IPv6 que hace frontera con el túnel, toma el paquete IPv6, y lo pone en el campo de datos de un paquete IPv4. Este paquete IPv4 tiene como dirección de destino el nodo IPv6 en la parte final del túnel y es enviado al primer nodo IPv4 que conforma el túnel. Los nodos IPv4 del túnel encaminan el paquete, sin tener constancia de que el paquete IPv4

que están manejando contiene un paquete IPv6. Cuando este paquete llega al extremo receptor IPv6 del túnel, que es precisamente el destino del paquete, éste determina que el paquete IPv4 contiene un paquete IPv6, extrae el paquete IPv6 y lo encamina exactamente del mismo modo que si hubiera recibido el paquete IPv6 de un nodo IPv4 vecino.

JUSTIFICACIÓN

Con el pasar de los años las empresas se vuelven más competitivas y usan cada vez más herramientas que las ayuden a ser más productivas y eficientes. Las redes se constituyen en unas de las herramientas indispensables para las empresas, es por eso que cada vez más se implementan. El uso de las redes facilita en gran medida el funcionar de una empresa, pero además trae consigo ciertas preocupaciones que tiene que ver con la parte de seguridad, consistencia, eficiencia, entre otras. Al adoptar cierta red en una empresa se debe tener cuidado porque podrían obtenerse resultados contraproducentes. La tecnología avanza a gran velocidad y se hace necesario estar a la par de dichos cambios para no quedar rezagados, lo que trae consigo la pérdida de la competitividad.

La necesidad de estudiar las barreras para la implementación del Protocolo de Internet versión 6 (IPv6) incidirá en el mejoramiento de las redes empresariales, debido a que con su uso se generaran beneficios a nivel de seguridad y eficiencia. Desde el punto de vista teórico este estudio generará conocimiento concreto acerca de cuáles son las dificultades que se dan al momento que querer pasar de IPv4 a IPv6. El resultado de este estudio sugiere ser una serie de pasos o instrumentos para hacer la transición entre protocolos de una manera más fácil y rápida, es decir se planteará un método para realizar dicha transición para cierto tipo de empresas.

OBJETIVOS

OBJETIVO GENERAL

Proponer un método para superar aquellas barreras que existen y que no han permitido realizar una transición del Protocolo de Internet versión 4 a versión 6.

OBJETIVOS ESPECÍFICOS

- Recopilar información sobre aquellas barreras que impiden la implementación del Protocolo de Internet versión 6 en las empresas de la ciudad de Cartagena.
- Identificar y analizar las barreras más comunes que se presentan al momento de querer hacer el cambio del Protocolo de Internet versión 4 a versión 6.
- Analizar los factores que inciden en las empresas donde se realizó el estudio a raíz de la no transición del protocolo de internet versión 4a versión 6 y mostrar aquellas ventajas que proporcionaría su implementación.
- Proponer la implementación de un método de transición viable a IPv6 para las características de las empresas estudiadas.

METODOLOGÍA

El estudio de las barreras que han retrasado la implementación de IPv6 es bastante amplio, por lo que se ha decidido enfocar la investigación a cierto tipo de problemáticas que pueden considerarse las más importantes o relevantes.

Como primera medida se seleccionarán las empresas sobre las cuales se basará el estudio, para ello se usaran criterios como el tipo de servicio que presta la empresa y la cantidad de empleados, esto con el fin de obtener resultados satisfactorios. Se estudiarán dos tipos fundamentales de empresas, primero las empresas proveedoras de servicios de internet (ISP – Internet Service Provider) y segundo empresas encargadas de desarrollo de software.

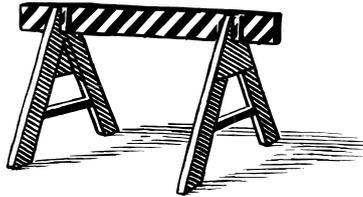
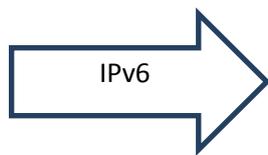
Por medio de una serie de visitas se preguntará sobre los conocimientos de IPv6 y sobre las razones por las cuales no se ha implementado si este fuera el caso.

Por último y luego de un estudio exhaustivo se planteará una solución para que la transición de una versión a otra sea de la forma más rápida, fácil y segura de acuerdo a ciertas características de las empresas.

CAPITULO I: INDAGANDO EN EMPRESAS DE CARTAGENA

En este capítulo se mostrara la información recolectada con relación a las barreras que impiden la implementación de IPv6 en las diferentes empresas de la ciudad de Cartagena.

Objetivo a cumplir:Recopilar información sobre aquellas barreras que impiden la implementación del Protocolo de Internet versión 6 en las empresas de la ciudad de Cartagena.



ENCUESTAS

Las siguientes son encuestas que fueron realizadas a empresas desarrolladoras de software, empresas distribuidoras de servicios de internet y empresas que de una u otra manera necesitan o se ven obligados a trabajar y administrar sus redes. Se realizaron una serie de preguntas con el fin de conocer y analizar las barreras por las cuales no se ha implementado el nuevo protocolo de internet versión 6.

- Empresas Distribuidoras de servicios de Internet:

 Redes Integrales S.A. Soluciones en Informática y Telecomunicaciones		REDES INTEGRALES S.A.
DATOS DEL ENCUESTADO		
Nombre del encuestado:	Rafael Monterroza	
Estudios:	Ingeniería de Sistemas	
Cargo en la empresa:	Gerente Operativo	
Tiempo en la empresa:	8 años.	
DATOS DE LA EMPRESA		
Nombre de la empresa:	Redes Integrales S.A.	
Sitio web:	http://new.redesintegrales.net.co/	
Número de computadores:	15	
Número de servidores:	6	
Sistemas operativos usados:	Windows XP, 7, Linux	
Lenguajes de programación:	Java, PHP	
Motor(es) de base de datos:	MySQL, Oracle	
Ancho de banda externa:	50 Mbps	
Proveedor de servicio de internet:	ISA INTERNEXA S.A. E.S.P.	
¿Con que versión del protocolo de internet se trabaja en la empresa?	IP Versión 4	
¿Conoce el protocolo de internet versión 6?	Si	
¿Por qué no se ha implementado la versión 6 del protocolo de internet?	Porque no poseemos la tecnología a nivel de routers y equipos de red con soporte para IPv6.	

¿Qué características conoce de IPv6?	Numero casi ilimitado de direcciones IP, direccionamiento de 128 Bits, mayor seguridad implementada directamente en el protocolo.
¿Conoce las ventajas y desventajas de implementar el protocolo de internet versión 6?	Si.
Si la respuesta anterior es si, por favor nombre algunas de las ventajas y desventajas que conoce.	Ventajas: Mayor direccionamiento, no se requiere NAT, mejor seguridad. Desventajas: No se ha implementado masivamente, se requiere tecnología de redes de última generación. Casi todo el internet aún está en IPv4.
¿En cuánto tiempo se tiene pensado hacer la transición al protocolo de internet versión 6?	No se tienen planes para migrar de versión por el momento.
¿Se tiene pensada alguna metodología para realizar dicha transición? Si la respuesta es sí indique ¿Cuál sería dicha metodología?	No.

- Empresas desarrolladoras de Software:

	
DATOS DEL ENCUESTADO	
Nombre del encuestado:	Jesús Babilonia Hernández.
Estudios:	Est. Ingeniería de Sistemas, Técnico analista programador de sistemas
Cargo en la empresa:	Desarrollador.
Tiempo en la empresa:	4 años.
DATOS DE LA EMPRESA	
Nombre de la empresa:	P.O. Consultores LTDA.
Sitio web:	http://www.poconsultores.com/

Número de computadores:	7
Número de servidores:	2
Sistemas operativos usados:	Windows Server 2008, Windows XP, Windows Vista, Windows 7, Linux
Motor(es) de base de datos:	Oracle y MSQl Server 2008
Ancho de banda externa:	4 Megas
Proveedor de servicio de internet:	Telefónica
¿Con que versión del protocolo de internet se trabaja en la empresa?	IPV4
¿Conoce el protocolo de internet versión 6?	Si, lo básico.
¿Por qué no se ha implementado la versión 6 del protocolo de internet?	Porque en la actualidad la mayoría de las compañías basan sus diseños y aplicaciones en IPV4 y migrar hacia IPV6 en este momento no es una ventaja.
¿Qué características conoce de IPV6?	Mayor direccionamiento.
¿Conoce las ventajas y desventajas de implementar el protocolo de internet versión 6?	No estoy enterado del tema.
Si la respuesta anterior es si, por favor nombre algunas de las ventajas y desventajas que conoce.	-----
¿En cuánto tiempo se tiene pensado hacer la transición al protocolo de internet versión 6?	Actualmente no se tiene pensado migrar, solo hasta cuando se haga realmente necesario.
¿Se tiene pensada alguna metodología para realizar dicha transición? Si la respuesta es sí indique ¿Cuál sería dicha metodología?	No.

		DW ENTERPRISE
DATOS DEL ENCUESTADO		
Nombre del encuestado:	Galy Ricardo.	

Estudios:	Ingeniería de Sistemas, Tecnología de Sistemas y Técnica Profesional en Computación.
Cargo en la empresa:	Desarrollador.
Tiempo en la empresa:	3 años.
DATOS DE LA EMPRESA	
Nombre de la empresa:	DW Enterprise
Sitio web:	http://www.dwe.com.co/
Número de computadores:	2
Número de servidores:	1
Sistemas operativos usados:	Windows 2008 Server y Windows 7
Motor(es) de base de datos:	MySQL, Oracle y MSQl Server 2008
Ancho de banda externa:	2 Megas
Proveedor de servicio de internet:	Telefónica
¿Con que versión del protocolo de internet se trabaja en la empresa?	IPV4
¿Conoce el protocolo de internet versión 6?	Si he escuchado de él.
¿Por qué no se ha implementado la versión 6 del protocolo de internet?	Porque para el número de equipos utilizados es impráctico.
¿Qué características conoce de IPV6?	Realmente no estoy muy al tanto. Pero una de las características es que no se utilizan números en hexadecimal en vez del conocido formato de cuarteto de 8 bits de la versión IPV4.
¿Conoce las ventajas y desventajas de implementar el protocolo de internet versión 6?	No estoy muy documentado al respecto.
Si la respuesta anterior es si, por favor nombre algunas de las ventajas y desventajas que conoce.	No estoy muy documentado al respecto.....pero lo que podría decir es que hay aplicaciones computacionales que probablemente no estén hechas para este protocolo y quizás no funcionen....por eso los sistemas operativos no pueden simplemente

	eliminar del todo al IPV4 ya que sería un coste muy alto la migración.
¿En cuánto tiempo se tiene pensado hacer la transición al protocolo de internet versión 6?	Dependiendo del tiempo en que se vuelva necesario migrar a esta versión del protocolo.
¿Se tiene pensada alguna metodología para realizar dicha transición? Si la respuesta es sí indique ¿Cuál sería dicha metodología?	A medida del crecimiento corporativo este se iría migrando a este protocolo...pero por ahora es impráctico su uso en una intranet pequeña.



zeus
tecnología

ZEUZ TECNOLOGIA

DATOS DEL ENCUESTADO

Nombre del encuestado:	Fernando Alcalá Arrieta
Estudios:	Tecnólogo en Sistemas
Cargo en la empresa:	Gerente de investigación y desarrollo.
Tiempo en la empresa:	21 años.

DATOS DE LA EMPRESA

Nombre de la empresa:	Zeuz Tecnología S.A.
Sitio web:	http://www.zeustecnologia.com/
Número de computadores:	120
Número de servidores:	6
Sistemas operativos usados:	Windows XP, Windows Vista, Windows 7, Windows Server 2008 R2.
Motor(es) de base de datos:	Microsoft SQL Server (2000 – 2005 – 2008 – 2008 R2).
Ancho de banda externa:	Entre 2 y 6 MB
Proveedor de servicio de internet:	UNE –Telefónica
¿Con que versión del protocolo de internet	IPV4

se trabaja en la empresa?	
¿Conoce el protocolo de internet versión 6?	Poco
¿Por qué no se ha implementado la versión 6 del protocolo de internet?	Por falta de conocimiento e infraestructura.
¿Qué características conoce de IPv6?	Mejora el número de servicios en internet.
¿Conoce las ventajas y desventajas de implementar el protocolo de internet versión 6?	No.
Si la respuesta anterior es si, por favor nombre algunas de las ventajas y desventajas que conoce.	-----
¿En cuánto tiempo se tiene pensado hacer la transición al protocolo de internet versión 6?	No se tiene planeado.
¿Se tiene pensada alguna metodología para realizar dicha transición? Si la respuesta es sí indique ¿Cuál sería dicha metodología?	No.

	
FACTURE SAS ZONA FRANCA	
DATOS DEL ENCUESTADO	
Nombre del encuestado:	Pablo Escobar Pinzón.
Estudios:	Ingeniero de Sistemas.
Cargo en la empresa:	Director de Calidad del Producto.
Tiempo en la empresa:	7 meses.
DATOS DE LA EMPRESA	
Nombre de la empresa:	Facture SAS Zona Franca
Sitio web:	-----
Número de computadores:	25
Número de servidores:	8
Sistemas operativos usados:	Windows 2008 Server, Windows 7 y Linux
Lenguajes de programación:	C#.NET

Motor(es) de base de datos:	SQL Server 2008 R2
Ancho de banda externa:	6 MB
Proveedor de servicio de internet:	Telefónica Telecom
¿Con que versión del protocolo de internet se trabaja en la empresa?	IPv4 e IPv6
¿Conoce el protocolo de internet versión 6?	Si
¿Por qué no se ha implementado la versión 6 del protocolo de internet?	Si se ha implementado. Sin embargo, ninguno de nuestros clientes lo ha requerido.
¿Qué características conoce de IPv6?	Capacidad extendida de direccionamiento, multicast, autoconfiguración, Movilidad de redes enteras, direcciones con máscara de 64 bits, hasta 2^{128} direcciones disponibles.
¿Conoce las ventajas y desventajas de implementar el protocolo de internet versión 6?	Sí.
Si la respuesta anterior es si, por favor nombre algunas de las ventajas y desventajas que conoce.	VENTAJAS: Dirección IP pública para cada dispositivo, seguridad de nivel de red obligatoria, procesamiento simplificado en routers. DESVENTAJAS: No es compatible con IPv4, aún no todos los dispositivos soportan IPv6.
¿En cuánto tiempo se tiene pensado hacer la transición al protocolo de internet versión 6?	A Medida que los clientes lo requieran.
¿Se tiene pensada alguna metodología para realizar dicha transición? Si la respuesta es sí indique ¿Cuál sería dicha metodología?	No.

- Empresas que poseen y administran sus propias redes:



DATOS DEL ENCUESTADO	
Nombre del encuestado:	Alfredo Ardila Labiosa
Estudios:	Ingeniería de Sistemas
Cargo en la empresa:	Jefe de Tecnologías de Información y Comunicaciones.
Tiempo en la empresa:	2 años.
DATOS DE LA EMPRESA	
Nombre de la empresa:	IntertugS.A.
Sitio web:	http://www.intertug.com/
Número de computadores:	70
Número de servidores:	2
Sistemas operativos usados:	Windows XP, Vista, 7, 2003 Server y 2008 Server.
Lenguajes de programación:	C#
Motor(es) de base de datos:	Firebird, MySQL, MS SQL SERVER.
Ancho de banda externa:	4 MB
Proveedor de servicio de internet:	-----
¿Con que versión del protocolo de internet se trabaja en la empresa?	Versión 4
¿Conoce el protocolo de internet versión 6?	Si
¿Por qué no se ha implementado la versión 6 del protocolo de internet?	Porque no se ha requerido aun de manera obligatoria y porque se considera que no hay completa compatibilidad en todos los dispositivos usados. Además los proveedores de internet no lo usan aún.
¿Qué características conoce de IPv6?	Soporta un gran número de direcciones, sus direcciones se escriben en 8 grupos de 4 hexadecimales.
¿Conoce las ventajas y desventajas de implementar el protocolo de internet versión 6?	Si.
Si la respuesta anterior es si, por favor nombre algunas de las ventajas y	Tiene un rediseño que permite optimización del tráfico de los paquetes en la red, además

desventajas que conoce.	de la ventaja inicial de tener mayor cantidad de direcciones disponibles.
¿En cuánto tiempo se tiene pensado hacer la transición al protocolo de internet versión 6?	No se tiene planeado aun. Se hará cuando sea obligatorio.
¿Se tiene pensada alguna metodología para realizar dicha transición? Si la respuesta es sí indique ¿Cuál sería dicha metodología?	No.

		PROCARGO S.A.
DATOS DEL ENCUESTADO		
Nombre del encuestado:	Iván Narváez Mejía	
Estudios:	Ingeniero de Sistemas	
Cargo en la empresa:	Jefe de Sistemas.	
Tiempo en la empresa:	1 años.	
DATOS DE LA EMPRESA		
Nombre de la empresa:	ProcargoS.A.	
Sitio web:	http://www.procargo.com.co/	
Número de computadores:	20	
Número de servidores:	2	
Sistemas operativos usados:	Windows y Linux	
Lenguajes de programación:	PHP y ASP.NET	
Motor(es) de base de datos:	MySQL y SQL Server.	
Ancho de banda externa:	6 MB	
Proveedor de servicio de internet:	Telefónica Telecom y UNE	
¿Con que versión del protocolo de internet se trabaja en la empresa?	IPv4	
¿Conoce el protocolo de internet versión 6?	Si	
¿Por qué no se ha implementado la versión 6 del protocolo de internet?	Las IP's públicas en la empresa no son IPv6 y no hay mucha interoperabilidad.	
¿Qué características conoce de IPv6?	Mayor seguridad y mayor número de equipos por red.	

¿Conoce las ventajas y desventajas de implementar el protocolo de internet versión 6?	Si
Si la respuesta anterior es si, por favor nombre algunas de las ventajas y desventajas que conoce.	Ventajas: Mayor número de bits ya no son 32 sino 128, soporte nuevos servicios, seguridad. Desventajas: Poco soporte.
¿En cuánto tiempo se tiene pensado hacer la transición al IPv6?	En el año 2014 aproximadamente debido al agotamiento de las IP's v4.
¿Se tiene pensada alguna metodología para realizar dicha transición? Si la respuesta es sí indique ¿Cuál sería dicha metodología?	No.

RESULTADOS

Con el cuestionario anteriormente citado, se analizó cuáles son las posibles barreras por las cuales no se ha implementado el nuevo protocolo de internet versión 6 en empresas desarrolladoras de software, empresas distribuidoras de servicios de internet y empresas que de una u otra manera necesitan o se ven obligados a trabajar y administrar sus redes en la ciudad de Cartagena, y se obtuvieron los siguientes resultados:

- Según la encuesta realizada, el 100% de las empresas encuestadas, actualmente tienen sus redes y trabajan bajo el protocolo de internet versión 4.
- Las empresas que tienen un alto número de computadores son las que se encuentran más preocupadas a la hora de realizar la transición, ya que el costo económico que implica dicha transición sería elevado y las retribuciones pueden que no se vean a corto plazo.
- El 100% de las empresas ha escuchado en algún momento hablar de este nuevo protocolo, pero su conocimiento no le proporciona claridad a la hora de pensar en realizar un cambio de severa magnitud.
- El 100% de las empresas plantea que en la actualidad la migración hacia IPv6 no es viable, ya que no se cuenta con la infraestructura, el

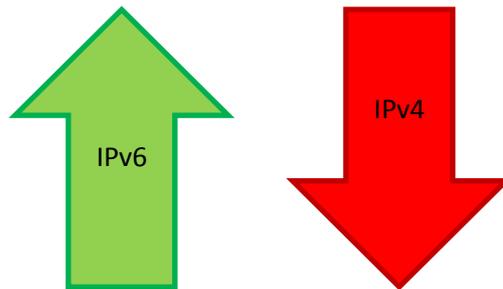
soporte, falta de compatibilidad, los proveedores no han migrado por completo e interoperabilidad.

- El 60% de las empresas encuestadas no tienen el conocimiento adecuado sobre este nuevo protocolo, no conocen cuáles son sus ventajas y desventajas si se llegara a implementar.
- El 86% de las empresas no tiene pensado migrar a este nuevo protocolo, ya que como no es una obligación inmediata, mientras no se vuelva necesario, dichas empresas no migraran sus servicios, por lo que no tienen un esquema de trabajo ni una fecha prevista para realizar este proceso.
- El 14% de las empresas ya han implementado este protocolo en algún servicio, pero sus clientes no lo han requerido ni necesitado.
- El 100% de las empresas encuestadas todavía no conocen o tienen pensada la metodología que utilizarían para realizar dicha transición, por lo tanto no es una necesidad en estos momentos para esas empresas.

CAPITULO II: BARRERAS PARA LA IMPLEMENTACIÓN DE IPv6

En este capítulo se describirán las barreras más comunes que se presentan al momento de querer hacer el cambio de protocolo de internet de versión 4 a 6.

Objetivo a cumplir: Identificar y analizar las barreras más comunes que se presentan al momento de querer hacer el cambio del Protocolo de Internet versión 4 a versión 6.



El problema de ser uno de los primeros en utilizar nuevas tecnologías se conoce a menudo como la "punta de lanza", debido al riesgo de fracaso. Las nuevas tecnologías tienen errores, pueden generar conflicto con los sistemas existentes, o los beneficios no están la altura de su promesa. Por otro lado la motivación de la utilización de riesgos es que la recompensa, si se utiliza una técnica que sus competidores no, entonces usted puede obtener una ventaja sobre los competidores.

Las empresas afrontan muchas barreras para implementar IPv6, el costo, la complejidad y el valor del negocio son unos de ellos. Uno de los problemas que enfrentan los pioneros es el riesgo asociado con la adopción de una nueva norma. Esto es causado por el hecho de que relativamente poca información que existe sobre IPv6, muchos expertos han señalado que el uso de redes IPv6 podría resultar en disminución de la seguridad de la red durante un cierto período durante el cual la red los operadores se familiaricen con el nuevo protocolo y los piratas informáticos identifican fallas en las implementaciones de IPv6 inicial. La escasez de información sobre el tema de los costos de la transición a IPv6, se fusionó con la realidad de que muchas organizaciones no se venden en los supuestos beneficios que ofrece el Protocolo de Internet versión 6 [19].

Las barreras más comunes que se presentan al momento de pensar en realizar una transición efectiva de IPv4 a IPv6, básicamente se puede decir que se dividen en dos principales: barreras técnicas y barreras comerciales.

Las barreras técnicas corresponden a todas aquellos impedimentos que están relacionados con la parte de hardware y software.

BARRERAS TÉCNICAS

En las barreras técnicas encontramos:

- Multihoming aún no definido.
- Compatibilidad con IPv6 de los equipos de red.
- Gestión de red

- Soporte del sistema operativo del host
- Infraestructura DNS
- Seguridad
- Resolución de dirección local de sitio.

EQUIPOS DE RED

A continuación se muestra una descripción de los principales equipos de red y su compatibilidad con el protocolo de internet versión 6 [14].

TARJETAS DE RED

Las tarjetas de red no tienen ningún tipo de incompatibilidad con la nueva versión del protocolo IPv6.

CABLE MODEM / ADSL

El equipo de cable modem o modem ADSL tiene que soportar IPv6, siendo uno de los principales puntos a considerar antes de actualizar el sistema a IPv6. Sin embargo, el modem normalmente es entregado por el ISP y es de responsabilidad del mismo proveer un equipo que soporte IPv6.

ROUTERS / ACCESS POINTS

Los routers caseros no suelen soportar IPv6 por el momento. Sin embargo, muchos de estos dispositivos pueden soportar IPv6 mediante una actualización del Firmware.

IMPRESORAS DE RED

Muchas impresoras no soportan IPv6 a la fecha, sin embargo una red local bien configurada continuará soportando IPv4 e IPv6 simultáneamente por lo que no se necesitará reemplazar estos dispositivos.

Se deberá consultar el fabricante si la impresora soporta o no IPv6 y si existe alguna actualización del Firmware en el caso de requerir su uso en IPv6.

CÁMARAS IP

Muchas cámaras soportan únicamente IPv4, sin embargo una red local bien configurada continuará soportando IPv4 e IPv6 simultáneamente por lo que no se necesitará reemplazar estos dispositivos.

Se deberá consultar el fabricante si la cámara soporta o no IPv6 y si existe alguna actualización del Firmware en el caso de requerir su uso en IPv6.

SEGURIDAD

Amenazas que deben ser consideradas en IPv6 [17]:

- Escaneo de debilidades en *Gateway* y *Hosts*
- Escaneo de direcciones multicast
- Control de acceso no autorizado
- Firewalls
- Debilidades en los protocolos
- Negación del servicio distribuido
- Mecanismos de transición
- Virus y gusanos informáticos (ya existen algunos virus para IPv6 como Rbot, DUD, etc.)

FIREWALLS

En cuanto a los requerimientos y utilización de IPv6 y los firewalls se destacan los siguientes puntos [17]:

- No hay necesidad de utilizar NAT, la seguridad y la privacidad son similares para ambos protocolos, siendo aún mejor en IPv6 dado el posible uso de IPsec para todos los protocolos.
- Soporte de coexistencia y transición de IPv4/IPv6.
- No vulnera la seguridad de IPv4.
- Existen ya diferentes firewalls capaces de trabajar con IPv6 como el Cisco ACL/PIX, iptables, ipfw, Juniper NetScreen, etc.

IPSEC

Es un mecanismo general de seguridad para IP especificada en el RFC 4301. Es aplicable para IPv4/IPv6, siendo obligatorio para IPv6 y opcional para IPv4. Se puede utilizar a través de LANs, WANs públicas y privadas, e Internet. IPsec ofrece un conjunto de bases de seguridad para proveer de ciertos mecanismos a los protocolos, permitiendo a estos una comunicación segura entre pares de dispositivos.

DIRECTACCESS

Un cliente de DirectAccess solo envía tráfico del protocolo de Internet versión 6 (IPv6) al servidor de DirectAccess. Cuando los clientes de DirectAccess envían solicitudes de consultas de nombres del Sistema de nombres de dominio (DNS) a través del túnel de infraestructura a la dirección IPv6 de un servidor DNS de la intranet, solo solicitan registros IPv6 (registros DNS AAAA). Las aplicaciones que solo usan el protocolo de Internet versión 4 (IPv4) en el cliente de DirectAccess nunca enviarán tráfico IPv4 a través del túnel de intranet de DirectAccess. El mismo cliente de DirectAccess, cuando está conectado directamente a la intranet, envía consultas de nombres DNS a los servidores DNS de la intranet y solicita todos los registros, tanto IPv4 como IPv6. En el caso de una aplicación de servidor solo IPv4, los servidores DNS de la intranet devuelven registros IPv4 y la aplicación cliente usa IPv4 para comunicarse [20].

El resultado final es que una aplicación cliente compatible con IPv6 en un cliente de DirectAccess puede usar IPv4 para tener acceso a una aplicación de servidor solo IPv4 mientras está conectado a la intranet, pero no puede tener acceso a la misma aplicación de servidor de forma predeterminada cuando está conectada a Internet.

BARRERAS ECONOMICAS

Las barreras comerciales corresponden a todos aquellos impedimentos que afecten económicamente cualquiera de las partes implicadas en la transición.

En las barreras comerciales encontramos:

- Ahorro en dinero: Sistema operativo, atención al cliente.
- El proceso de transición representa un gasto importante para las empresas, del que no se vería necesariamente un retorno de inversión dado que prácticamente nadie usa IPv6. Además, no provee una ventaja significativa en cuanto a las estrategias de negocios (salvo que el negocio sea la continua publicación de servicios en Internet). Por si fuera poco, el costo que tiene una migración de IPv4 a IPv6 implica entrenamiento, equipo nuevo con mayores capacidades de hardware, inversión en adecuaciones de software, por mencionar algunos. Finalmente, todos los grandes corporativos ya tienen direcciones IPv4 asignadas y no hay razón para migrar a IPv6.
- Costo de ancho de banda para VoIP más alto para IPv6
- Percepción de NAT como una tecnología de seguridad
- Percepción de P2P como una infracción de copyright.
- Ciclos de reemplazo de infraestructura (núcleo de la red)

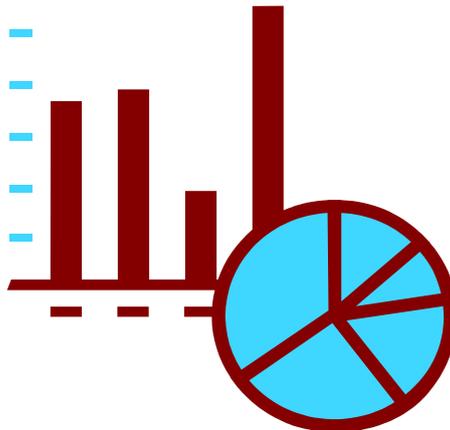
Otros factores:

- Formación de ingenieros, atención al cliente, marketing
- Falta de conciencia de los beneficios de IPv6

CAPITULO III: VENTAJAS Y DIFICULTADES DE IPv6

En este capítulo se describirán los factores que inciden en el rendimiento de las empresas que aún no han implementado IPv6 y se mostraran algunas de las ventajas que proporcionaría su implementación.

Objetivo a cumplir: Analizar los factores que inciden en las empresas donde se realizó el estudio a raíz de la no transición del protocolo de internet versión 4 a versión 6 y mostrar aquellas ventajas que proporcionaría su implementación.



El internet ha tenido un importante valor en los negocios internacionales, gobierno, servicios profesionales, académicos y uso de personas en la última década. La Industria confía ahora en que la amplia gama de beneficios brindados por el Internet los lleven a un aumento significativo de la productividad.

Los beneficios de la Internet son extraídos directamente de la plataforma de interoperabilidad creado por el uso del protocolo de Internet, dando lugar a un "efecto red" de gran tamaño. Es decir, los beneficios de una empresa de Internet no surgen sólo en la medida en que la propia empresa necesita Internet, pero mucho más a partir de la medida en que los demás - proveedores, clientes y personas - también sigan utilizando el internet de forma masiva. Un beneficio de IPv6 será que este protocolo permitirá el aumento en gran medida el tamaño y variedad de dispositivos conectados a la red.

Aunque muchas aplicaciones en la actualidad como la World Wide Web y otras aplicaciones de Internet utilizan la versión 4 del protocolo de Internet - IPv4, IP versión 6 fue desarrollado para hacer frente a una escasez inminente de las direcciones en IPv4. Desde entonces, ha habido numerosas soluciones técnicas para pasar de IPv4 y posponer la necesidad de un cambio a IPv6. Que el debate es ahora generalmente de acuerdo a su fin. Se ha llegado a decir que, en la práctica, la única opción para la construcción de nuevas redes de gran tamaño sería el empleo o uso de IPv6.

IPv6 ofrece la posibilidad de construir un Internet mucho más potente, con una escala mucho más grande en comparación con la situación actual.

IPv6 cuenta además con funciones adicionales, teniendo la nueva característica de autoconfiguración. Esta característica permite que un dispositivo pueda generar una dirección IPv6. Para el uso de esta dirección, no se necesitaría el uso de cualquier otro tipo de infraestructura para permitir que el dispositivo para comenzar a comunicarse a través de IPv6 en su red local, incluyendo la comunicación con otro host local o el router. Si un router IPv6

está presente, cualquier dispositivo con capacidad IPv6 puede generar no sólo una dirección local, también una dirección enrutable por todo el mundo, lo que permitiría el acceso al Internet en general.

El suministro de suficiente espacio de direcciones también permitirá re-establecimiento de una arquitectura de extremo a extremo en el Internet. Los dispositivos con direcciones IPv6 y que posean conectividad puede ser directamente accesible por su dirección desde cualquier parte del mundo. Tal enfoque da lugar a la posibilidad de ir más allá de una "Internet de las computadores de escritorio" a una "Internet de dispositivos". Otrade las capacidades que se incluyeron durante el proceso de desarrollo de IPv6, fue por ejemplo, el apoyo obligatorio para la seguridad a través de IPsec (Internet Protocol Security).

Mientras que algunas de las nuevas características son posibles en redes basadas en IPv6, poco a poco se han esmerado por volver compatibles las redes con el protocolo IPv4, lo que haría más fácil o posible utilizar dicho protocolo para satisfacer las necesidades empresariales actuales y futuras.

Por otro lado, la intervención manual es otro elemento fundamental a considerar en el contexto de la implementación de redes a gran escala. Si la configuración manual es necesaria para cada dispositivo con una dirección IP, existirían costos significativos. En las redes basadas en IPv4, este requisito ha sido subsanado por el uso de Dynamic Host Configuration Protocol (DHCP), que es capaz de asignar automáticamente direcciones IP a los nuevos dispositivos en la red con los parámetros establecidos por el administrador. Sin embargo, para que este método funcione, cada nuevo producto debe interactuar con un servidor DHCP. Por el contrario, la asignación de direcciones IPv6 se hace por el propio dispositivo y puede ocurrir independientemente de un servidor, o en combinación con un router IPv6 habilitado, dependiendo del tipo de red que se tenga.

Mientras que muchas aplicaciones basadas en Internet seguirán funcionando en IPv4, los desafíos de la administración de la red y gestión de la seguridad continuarán creciendo. Por ejemplo, si dos empresas se fusionan y quiere fusionar sus redes basadas en IP, entonces no tendrá que volver a enumerar s. En Internet, si la fuente de la actividad maligna debe ser identificada, el recurso que se tiene más cercano para la identificación sería por dirección IP, siendo posible bajo una arquitectura IPv4 NAT.

En síntesis, algunas de las ventajas en las que se verían inmersas las empresas si deciden realizar el proceso de transición de IPv4 a IPv6 son:

- 1.** Dichas empresas podrán emplear diferentes velocidades en el proceso de adaptación al protocolo, que puede variar en función de los países.
- 2.** Las empresas asegurarían la evolución a futuro, permitiéndoles aprovechar la ventaja de nuevos servicios. IPv6 es más eficiente para aquellos servicios que requieren un gran número de dispositivos, que dispondrán de su propia IP sin necesidad de utilizar mecanismos como NAT.
- 3.** Empresas distribuidoras de internet, asegurarían que los protocolos IPv4 e IPv6 van a coexistir, lo que supone que sus clientes podrían gestionar cualquier plan de transición en el plazo que mejor se adapte a su negocio.
- 4.** Las empresas ganarían capacidades en el área de movilidad, en el cual le permitirán a los ordenadores y dispositivos trabajar sin interrupción, incluso si están en tránsito y se conectan a través de distintas redes.
- 5.** Las empresas manejarían protocolo IPSec, el cual mejoraría la seguridad en el acceso a los recursos y dispositivos de una red privada virtual.
- 6.** Dichas empresas, de acuerdo al nuevo formato del protocolo, les permitirán

tener un mejor control sobre las calidades de servicio, lo que redundará en redes con un mayor rendimiento.

Una de las empresas, que ha comenzado a poner su granito de arena para la migración a IPv6 es **Cisco**, que ha sacado routers con migración a IPv6.

La intención de Cisco con el lanzamiento de estos routers, y también switches, con migración a IPv6 se orienta a que una empresa pueda **trabajar con IPv4 e IPv6 a la vez**, para así poder realizar la transición de una manera tranquila y ausente de problemas. Los routers lanzados tendrán soporte VPNIPSec v2 para la familia ISR G2 y soporte NAT64 para los routers de la plataforma ASR 1000. También añaden soporte para **el método LISP** (un método ideado por Cisco para hacer convivir túneles IPv4 y redes IPv6) en todos sus productos, algo que puede llegar a ser básico para la convivencia entre los dos protocolos.

Con estos lanzamientos Cisco se asegura que sus clientes van a poder **migrar de IPv4 a IPv6 correctamente** y de una manera tranquila y sin agobios. Es un avance positivo ya que muchos usuarios no suelen tener acceso a dispositivos de la marca Cisco (salvo con Linksys, la gama económica), siendo esta gama económica la que la inmensa mayoría de empresas utiliza, siendo este movimiento aplaudido por la inmensa mayoría de sus clientes.

CAPITULO IV: MÉTODOS DE TRANSICIÓN DE IPv4 A IPv6

En este capítulo se describen ciertos métodos para implementar una transición de IPv4 a IPv6 de acuerdo a las características que presenta cada empresa.

Objetivo a cumplir: Proponer la implementación de un método de transición viable a IPv6 para las características de las empresas estudiadas.



Después de analizar exhaustivamente las encuestas realizadas a empresas desarrolladoras de software, empresas distribuidoras de servicios de internet y empresas que de una u otra manera necesitan o se ven obligados a trabajar y administrar sus redes, podemos mostrar que las barreras que se encontraron a la hora de implementar el nuevo protocolo de internet versión 6 en las empresas de la ciudad de Cartagena parten desde el nivel de conocimiento que poseen los diferentes profesionales en el área de Sistemas y Redes con respecto a esta nueva versión del protocolo, desconociendo cuales son aquellas ventajas y desventajas. Por otro lado, el soporte que se tiene actualmente de este nuevo protocolo es muy escaso, ya que como no ha sido obligación el proceso de transición a este nuevo protocolo, muchas de las empresas no se han dado a la tarea de planificar su transición y por lo tanto no se conocen aquí en Cartagena empresas las cuales brinden soportes a IPv6. Para esto, mostramos y planteamos algunas metodologías que se podrían emplear en dichas empresas para la correcta transición del protocolo IPv4 a IPv6.

METODOLOGIAS DE TRANSICION DE IPV4 A IPV6

Antes de plantear metodologías para la transición de IPv4 a IPv6, se tendría que documentar o capacitar a los profesionales en sistemas para que entiendan las bases y definiciones que trae consigo este nuevo protocolo, ya que esta sería la puerta a un nuevo conocimiento y al futuro cercano en el cual se tendrían que ver inmersos tarde o temprano las empresas en la ciudad de Cartagena.

Métodos o mecanismos de transición en redes IPv6. (En Colombia la única red nativa de IPv6 es la de RENATA [Red Privada que transmite internet en protocolo IPv6 dentro de su propia isla]). Estos serían algunos métodos o mecanismos en los cuales se podría basar la transición del protocolo de internet versión 4 al nuevo protocolo de internet versión 6.

DOBLE PILA

Este mecanismo de transición es algo útil ya que permite trabajar conjuntamente entre los dos protocolos, pero existe sobrecarga en los enrutadores, ya que estos tendrían que trabajar con doble tablas de enrutamiento, doble tablas de direcciones ARP, y entonces necesitaría capacidades de cómputo un poco más altas que los enrutadores convencionales. En estos momentos todos los sistemas operativos modernos soportan doble pila y algunos teléfonos móviles.

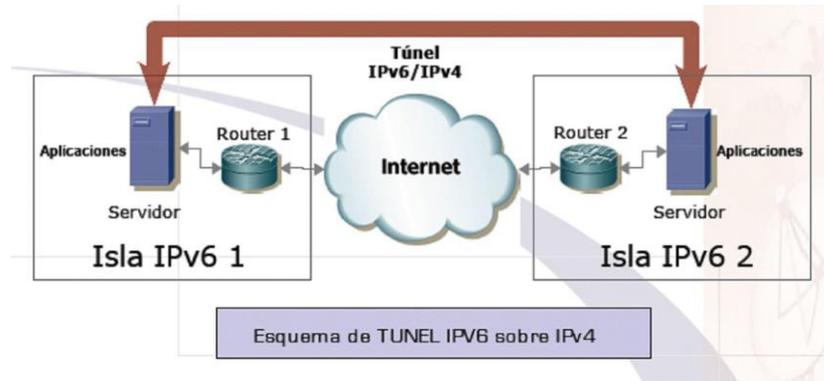
TÚNELES

Es un encapsulamiento de IPv6 dentro de IPv4, se mete todo el tráfico de IPv6 dentro de una conexión IPv4, y por este método se podría llegar a conexiones comerciales a través de túneles propios.

Tipos de Túneles

- RFC 3053 (IPv6 Túnel Broker – Empresa que se encarga de recibir el túnel propio de IPv6): especifica el funcionamiento de IPv6 dentro de IPv4.
- Hurricane Electric: Empresa que permite la creación de túneles propios. La única condición que exige dicha empresa es que se tenga una dirección IPv4 Pública. También se podrían poner a funcionar con direcciones privadas pero necesita usuario y contraseña.
- Dentro del datagrama IPv4, estos túneles se encapsulan mediante el protocolo 41.
- GRE Túneles: túneles genéricos basados en enrutamiento.

Los túneles proporcionan un mecanismo para utilizar las infraestructuras IPv4 mientras la red IPv6 está siendo implantada. Este mecanismo consiste en enviar datagramas IPv6 encapsulados en paquetes IPv4.



Los extremos finales del túnel siempre son los responsables de realizar la operación de encapsulado del paquete o paquetes IPv4.

Estos túneles pueden ser utilizados de formas diferentes:

Router a router

Routers con doble pila (IPv6/IPv4) se conectan mediante una infraestructura IPv4 y transmiten tráfico IPv6. El túnel comprende un segmento que incluye la ruta completa, extremo a extremo, que siguen los paquetes IPv6.

Host a router

Hosts con doble pila se conectan a un router intermedio (también con doble pila), alcanzable mediante una infraestructura IPv4. El túnel comprende el primer segmento de la ruta seguida por los paquetes.

Host a host

Hosts con doble pila interconectados por una infraestructura IPv4. El túnel comprende la ruta completa que siguen los paquetes.

□ **Router a host**

Routers con doble pila que se conectan a hosts también con doble pila. El túnel comprende el último segmento de la ruta.

Los túneles se clasifican según el mecanismo por el que el nodo que realiza el encapsulado determina la dirección del nodo extremo del túnel.

En los dos primeros casos (router a router y host a router), el paquete IPv6 es tunelizado a un router. El extremo final de este tipo de túnel, es un router intermedio que debe desencapsular el paquete IPv6 y reenviarlo a su destino final. En este caso, el extremo final del túnel es distinto del destino final del paquete, por lo que la dirección en el paquete IPv6 no proporciona la dirección IPv4 del extremo final del túnel. La dirección del extremo final del túnel suele ser determinada a través de información de configuración en el nodo que realiza el túnel. Es lo que se denomina “túnel configurado”, describiendo aquel tipo de túnel donde el extremo final del túnel es explícitamente configurado.

En los otros dos casos (host a host y router a host), el paquete IPv6 es tunelizado, durante todo el recorrido, a su nodo destino. El extremo final del túnel es el nodo destino del paquete, y por tanto, la dirección IPv4 está contenida en la dirección IPv6. Este caso se denomina “túnel automático”. [21]



TRADUCCIÓN

Este mecanismo vale aclarar que no es o sería muy utilizado por la demanda computacional que necesita, en este método se toma la dirección IPv4 de origen y al convierte en una dirección IPv6, se podría decir que es algo muy parecido al NAT, llamándolo de alguna manera como una conversión de dirección y el paquete que se devuelve el servicio debe ser convertido nuevamente de IPv6 a IPv4 para ser entregado correctamente.

CREACIÓN DE NODOS

A continuación se describe una metodología de transición de IPv4 a IPv6, [13] la cual consiste en ir creando nodos que soporten tanto IPv4 como IPv6 hasta cuando todos los nodos puedan llegar a hablar la misma versión de IP (IPv6). Para implementar dicha metodología existen dos formas:

- **Nodos IPv4/IPv6:** Los enrutadores y máquinas de esta categoría tienen tanto IPv4 como IPv6. Además poseen un mecanismo llamado tunelado IPv6 sobre IPv4. Estos nodos pueden interoperar directamente tanto con nodos IPv4 como con nodos IPv6.
- **Enrutadores traductores:** Son enrutadores que traducen paquetes de IPv6 a paquetes IPv4 y viceversa. El enrutador podría saber cuál es la versión por medio del campo “versión” del encabezado del paquete.

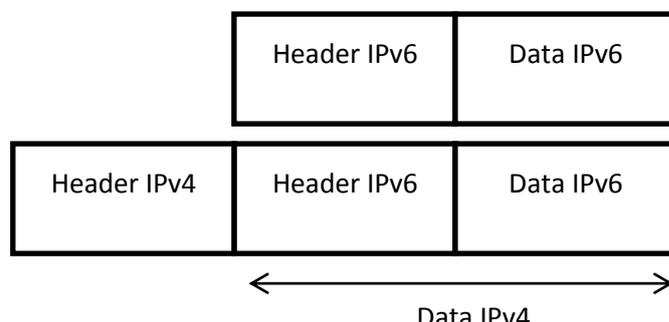


Ilustración 1 - Encapsulamiento de IPv6 dentro de IPv4

Ahora, este tunelado se puede realizar por medio de un encapsulamiento, es decir que el paquete en el cual vienen encabezados y datos en IPv6 se

convierte sólo en datos para IPv4 y luego se le adiciona el encabezado de IPv4. Pero si el nodo es únicamente IPv4, entonces la dirección IPv6 se tendrá que mandar en formato de IPv4 de la siguiente forma:

0:0:0:0:0:128.10.2.1 o en su defecto ::128.10.2.1

Aquí surge un gran interrogante con respecto a si el tamaño del paquete que se arma en IPv4 es mayor al MTU en todo el trayecto. ¿Qué pasaría si el nodo origen es IPv4 y él no sabe ni está diseñado para buscar el mínimo MTU entre el nodo de origen y el nodo de destino?

La solución propuesta a este caso es que los nodos (*Host* y *Routers*) que sean IPv4 fragmentarán de acuerdo al MTU que conocen; y lo seguirán realizando mientras que los nodos por donde transite el paquete sean IPv4. Cuando lleguen a un nodo IPv4/IPv6 que sepa que tiene que buscar el mínimo MTU en la ruta escogida, éste procederá a encontrarlo, y una vez hallado tomará la decisión de fragmentar o no y a qué tamaño, en caso de requerir la fragmentación. Estos nodos sí están en capacidad de fragmentar, puesto que tienen en su pila de protocolos tanto Ipv4 como Ipv6, es decir que pueden fragmentar y reensamblar, y además pueden encontrar el mínimo MTU en la ruta escogida.

Ahora, ¿de qué forma se enviarían los paquetes por medio de la red? Al respecto se pueden plantear varias soluciones:

- **Mapeo de direcciones:** Esta técnica consiste en enviar la dirección IPv4 de 32 bits en el extremo derecho del formato de IPv6, es decir, ocupando 4 bytes de los 16 que lo componen. Los 12 bytes ubicados a la izquierda se rellenan con ceros (0).

96 bits (12 bytes)	32 bits (4 bytes)
0:0:0:0:0:0:0:0:0:0:0:0	Dirección IPv4

- **Capa IP dual:** Esta técnica consiste en incluir completamente el IPv4 en un sistema nuevo con IPv6. Estos son los llamados nodos IPv6/IPv4.

Estos nodos están en capacidad de transmitir información tanto en formato IPv4 como en IPv6.

- **Protocolo de encapsulación:** Esta técnica también es llamada IPv6 en IPv4 o tunelado de IPv6 sobre IPv4. El tunelado se utiliza para llevar paquetes de IPv6 a través de áreas de red de envío tipo IPv4. Uno de los requisitos para el tunelado es que el comienzo y los extremos del túnel sean nodos IPv6/IPv4 con direcciones IPv6 compatibles con IPv4. Tunelado significa que todos los paquetes IPv6 son mapeados en el cuerpo de un paquete IPv4 y enviados a través de áreas de red de IPv4. La forma más sencilla de realizar el tunelado consiste en adicionar al paquete IPv6 los encabezados de IPv4 y transmitirlo; cuando se necesite recibir, se le remueve el encabezado IPv4 y se procesa el resto del paquete como IPv6.

SOLUCIONES PARA CLIENTES DE DIRECTACCESS

Las soluciones para proporcionar conectividad a las aplicaciones compatibles con IPv6 en clientes de DirectAccess con aplicaciones de la intranet solo IPv4 son las siguientes:

- Actualizar la aplicación de la intranet solo IPv4 para que admita IPv6. Esta actualización podría incluir la actualización del sistema operativo del servidor, la actualización de la aplicación que se ejecuta en el servidor o ambas. Es la solución recomendada. En el caso de aplicaciones integradas y servicios del sistema de equipos que ejecutan Windows XP o Windows Server 2003, debe actualizar Windows XP a Windows 7 o Windows Vista y actualizar Windows Server 2003 a Windows Server 2008 R2 o Windows Server 2008.
- Usar una conexión de red privada virtual (VPN) de acceso remoto convencional en el cliente de DirectAccess para tener acceso a la aplicación solo IPv4.
- Use un traductor IPv6/IPv4 y una puerta de enlace DNS IPv6/IPv4, que realizan los servicios de traducción del tráfico IPv6/IPv4 y de resolución de nombres DNS IPv6 a IPv4 para el tráfico entre los clientes de

DirectAccess y los servidores de aplicaciones de la intranet solo IPv4. Una combinación de traductor IPv6/IPv4 con puerta de enlace DNS IPv6/IPv4 es un NAT64 con DNS64.

HARDWARE – SOFTWARE

Teniendo claro cuáles son algunas de las diferentes metodologías con las cuales se podría realizar la transición de IPv4 a IPv6, cabe preguntar, ¿Cómo podemos desplegar una red IPv6 y comenzar a dar servicio? ¿Qué hardware y software se necesitarían?

La mayor parte de los principales fabricantes de equipos de red proporcionan ya soluciones para IPv6. Routers como los Hitachi, 6WIND, Telebit, Cisco, Juniper, etc. Disponen de IPv6 directamente o cambiando alguna de las IOS que lo proveen. Incluso alguno de ellos, como los 6WIND o Hitachi empiezan a basar su negocio en el buen soporte de IPv6 que proporcionan.

En cuanto a sistemas operativos, el kernel estándar de Linux también provee un soporte básico de IPv6, aunque el kernel proporcionado por el proyecto USAGI permite muchas más cosas. La mayor parte de las distribuciones modernas incluye soporte para esta nueva versión en mayor o menor medida, aunque casi todas se basan en el kernel estándar. Otros sistemas como Windows XP, Windows .Net o Solaris también incorporan una pila de IPv6 perfectamente usable, aunque los proyectos Open Source sean los que más funciones incorporan.

Respecto a las aplicaciones, hay soporte para casi cualquier cosa de las que queramos hacer o saber. Apache, Netscape/Mozilla, MS Internet Explorer, sendmail, bind, quake2, clientes y servidores de FTP, clientes y servidores de IRC, son ejemplos de aplicaciones que ya incorporan soporte para IPv6. [16]

CONFIGURACIÓN EN SISTEMAS OPERATIVOSUTILIZANDO

METODO DE TRANSICION TUNELLING (EJEMPLO PRÁCTICO)

A la hora de configurar los túneles, primero que todo se debe tener en cuenta el sistema operativo que se esté utilizando, ya que los comandos pueden llegar a

variar dependiendo de este. Por otro lado, se debe conocer que para la correcta configuración de los Túneles, para esto se debe realizar un proceso con alguna empresa prestadora de servicios de creación de TunnelBroakers como por ejemplo Hurricane Electric.

TÚNEL BROKER CON HURRICANE ELECTRIC

Hurricane Electric es un proveedor de conectividad para estructuras (backbone) a escala global, especializado en IPv6, que opera actualmente el backbone más grande de IPv6 en el mundo, medido por el número de redes conectadas. [18]

PROCEDIMIENTO

1. Dirigirse al sitio de Hurricane Electric www.tunnelbroker.net. Se desplegará la pantalla principal. Para crear tu túnel es necesario registrarse. Haz clic en "Register" para ir a la página de registro.

HURRICANE ELECTRIC
INTERNET SERVICES

Tunnelbroker Login

Username:

Password:

[Login](#) [Register](#)

Hurricane Electric Free IPv6 Tunnel Broker

You need to login to access this page.

[Please Register](#) if you do not have an account. If the system can not re-issue you a password please re-register, you can reclaim your old tunnel if you have your last IPv4 endpoint.

[Have you lost/forgotten your password?](#)

Please make sure Javascript is enabled.

Quick Links

- [Certification](#)
- [Tunnelbroker](#)
- [Free DNS](#)
- [BGP Toolkit](#)
- [Forums](#)
- [FAQ](#)
- [Video Presentations](#)
- [IPv6 Blog Posts](#)
- [Usage Statistics](#)
- [Tunnel Server Status](#)
- [Network Map](#)
- [Looking Glass \(v4/v6\)](#)
- [Route Server \(telnet\)](#)
- [Global IPv6 Report](#)
- [IPv6 BGP View](#)

Services

- [Transit](#)
- [Colocation](#)
- [Dedicated Servers](#)

v4 Exhaustion

IPv4 & IPv6 Statistics

RIR v4 /24s Left	
AfriNIC	247,390
APNIC	75,681
ARIN	54,600

Top 10 Certs

admcd	[1500]
gstueve	[1500]
pasquik	[1500]
gathron	[1500]
adriangr...	[1500]
Karstenlwen	[1500]
jermiman	[1500]
cholzshauer	[1500]
kneissel	[1500]
phagras	[1500]

Latest 10 Certs

jwininger	[Newb]
davidsch...	[Newb]
fudnet	[Admn]
nemmik	[Newb]

2. En el formulario de registro, llena los datos y selecciona el botón de "Register" como muestra la figura.

Tunnelbroker Login Username: <input type="text"/> Password: <input type="password"/> <input type="button" value="Login"/> <input type="button" value="Register"/>	HE.net IPv6 Tunnel Broker Registration After successfully completing registration, an email will be sent to the listed email address with your account password. * = Required Information * Account Name: <input type="text" value="nombredocuenta"/> * Email: <input type="text" value="nombredocuenta@gmail.com"/> * First Name: <input type="text" value="Juan"/> * Last Name: <input type="text" value="Perez"/> Company Name: <input type="text" value="MiEmpresa"/> * Country: <input type="text" value="Chile"/> * Address: <input type="text" value="Mi direccion"/> * City: <input type="text" value="Santiago"/> * State/Region: <input type="text" value="RM"/> * ZIP/Postal Code: <input type="text" value="0000000"/> * Phone: <input type="text" value="+56991231234"/> <input checked="" type="checkbox"/> I have read and agreed to the Terms and Services <input type="button" value="Register"/>	Quick Links Certification Tunnelbroker Free DNS BGP Toolkit Forums FAQ Video Presentations IPv6 Blog Posts Usage Statistics Tunnel Server Status Network Map Looking Glass (v4/v6) Route Server (telnet) Global IPv6 Report IPv6 BGP View																												
Top 10 Certs <table border="1"> <tr><td>wsyoung</td><td>[1500]</td></tr> <tr><td>swsystem</td><td>[1500]</td></tr> <tr><td>leenoux</td><td>[1500]</td></tr> <tr><td>alexrich...</td><td>[1500]</td></tr> <tr><td>krtekne...</td><td>[1500]</td></tr> <tr><td>xori86</td><td>[1500]</td></tr> <tr><td>tongrider</td><td>[1500]</td></tr> <tr><td>mhwarfield</td><td>[1500]</td></tr> <tr><td>sagard123</td><td>[1500]</td></tr> <tr><td>vamh</td><td>[1500]</td></tr> </table>	wsyoung	[1500]	swsystem	[1500]	leenoux	[1500]	alexrich...	[1500]	krtekne...	[1500]	xori86	[1500]	tongrider	[1500]	mhwarfield	[1500]	sagard123	[1500]	vamh	[1500]		Services Transit Colocation Dedicated Servers								
wsyoung	[1500]																													
swsystem	[1500]																													
leenoux	[1500]																													
alexrich...	[1500]																													
krtekne...	[1500]																													
xori86	[1500]																													
tongrider	[1500]																													
mhwarfield	[1500]																													
sagard123	[1500]																													
vamh	[1500]																													
Latest 10 Certs <table border="1"> <tr><td>Anthraxi...</td><td>[Exp]</td></tr> <tr><td>fwinger</td><td>[Newb]</td></tr> <tr><td>davidsch...</td><td>[Newb]</td></tr> <tr><td>fudnet</td><td>[Admn]</td></tr> <tr><td>nemmlk</td><td>[Newb]</td></tr> <tr><td>tdavis</td><td>[Guru]</td></tr> <tr><td>patux</td><td>[Sage]</td></tr> </table>	Anthraxi...	[Exp]	fwinger	[Newb]	davidsch...	[Newb]	fudnet	[Admn]	nemmlk	[Newb]	tdavis	[Guru]	patux	[Sage]		v4 Exhaustion IPv4 & IPv6 Statistics <table border="1"> <tr><td>RIR v4 /24s Left</td><td></td></tr> <tr><td>AfrINIC</td><td>247,390</td></tr> <tr><td>APNIC</td><td>75,681</td></tr> <tr><td>ARIN</td><td>514,497</td></tr> <tr><td>LACNIC</td><td>246,192</td></tr> <tr><td>RIPE</td><td>225,172</td></tr> <tr><td>v6 ASNs</td><td></td></tr> </table>	RIR v4 /24s Left		AfrINIC	247,390	APNIC	75,681	ARIN	514,497	LACNIC	246,192	RIPE	225,172	v6 ASNs	
Anthraxi...	[Exp]																													
fwinger	[Newb]																													
davidsch...	[Newb]																													
fudnet	[Admn]																													
nemmlk	[Newb]																													
tdavis	[Guru]																													
patux	[Sage]																													
RIR v4 /24s Left																														
AfrINIC	247,390																													
APNIC	75,681																													
ARIN	514,497																													
LACNIC	246,192																													
RIPE	225,172																													
v6 ASNs																														

3. Una vez que completes el registro llegarás a tu página principal, donde aparecerá la opción de "Create Regular Tunnel" en el menú del lado izquierdo. Selecciona esta opción



Account Menu Main Page Account Info Logout	Hurricane Electric Free IPv6 Tunnel Broker Name: Alejandro Salinas User ID: tb4da5abf3430a61.30284590 Tunnel Broker News: +DynDns support for dns.he.net [March 23, 2011] +Last 2 /8s, before the reserved 5 are assigned, now allocated. [January 31, 2011] +Re: PPTP Tunnel Beta [October 29, 2010] +UPDATE - August 14th, 2010 [August 14, 2010] +Re: PPTP Tunnel Beta [July 02, 2010] <table border="1"> <thead> <tr> <th>Tunnel [1 / 5]</th> <th>Routed /64</th> <th>Routed /48</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>asalinaf- 1.tunnel.tserv12.mia1.ipv6.he.net</td> <td>2001:470:5:37::/64</td> <td>2001:470:d991::/48</td> <td>Test 1</td> </tr> </tbody> </table>	Tunnel [1 / 5]	Routed /64	Routed /48	Description	asalinaf- 1.tunnel.tserv12.mia1.ipv6.he.net	2001:470:5:37::/64	2001:470:d991::/48	Test 1	Quick Links Certification Tunnelbroker Free DNS BGP Toolkit Forums FAQ Video Presentations IPv6 Blog Posts Usage Statistics Tunnel Server Status Network Map Looking Glass (v4/v6) Route Server (telnet) Global IPv6 Report IPv6 BGP View
Tunnel [1 / 5]	Routed /64	Routed /48	Description							
asalinaf- 1.tunnel.tserv12.mia1.ipv6.he.net	2001:470:5:37::/64	2001:470:d991::/48	Test 1							
User Functions Combine Tunnels <input checked="" type="button" value="Create Regular Tunnel"/> Create BGP Tunnel IPv6 Portscan		Services Transit Colocation Dedicated Servers								
		v4 Exhaustion IPv4 & IPv6 Statistics								

4. En la página de creación de un nuevo túnel, coloca el IPv4 de tu lado en el cuadro de texto disponible. Este IP debe ser público (En caso de que quieras saber tu IP la página te lo muestra en "You are viewingfrom"). En la misma página selecciona el servidor de destino, el de Miami es una buena opción para

alguien que está en Chile (esto es solo una sugerencia, todos funcionan). Para finalizar haz click en el botón de "CreateTunnel" al final de la página (no mostrado en la imagen).

Create New Tunnel

You currently have 1 of 5 tunnels configured.

- If you are trying to reclaim a tunnel simply use your last IPv4 address here. If you have any issues please email ipv6@he.net.
- If you have a public ASN and wish to setup a full BGP feed, please use [this form](#) instead.

IPv4 Endpoint (Your side):

IP is a potential tunnel endpoint.

You are viewing from: 201.239.124.248

We recommend you use: **Checking...**

Available Tunnel Servers:

Region	Location	IP Address
Asia	Hong Kong, HK	216.218.221.6
	Singapore, SG	216.218.221.42
	Tokyo, JP	74.82.46.6
Europe	Amsterdam, NL	216.66.84.46
	Frankfurt, DE	216.66.80.30
	London, UK	216.66.80.26
	Paris, FR	216.66.84.42
	Stockholm, SE	216.66.80.90
	Zurich, CH	216.66.80.98
North America	Ashburn, VA, US	216.66.22.2
	Chicago, IL, US	209.51.181.2
	Dallas, TX, US	216.218.224.42
	Fremont, CA, US	72.32.104.74
	Los Angeles, CA, US	66.220.18.42
	Miami, FL, US	209.51.161.58
	Miami, FL, US	209.51.161.44

5. Ahora tu nuevo túnel aparece en tu página principal (en la figura es el segundo túnel abajo). Selecciónalo para ver los detalles.

Hurricane Electric Free IPv6 Tunnel Broker

Name: Alejandro Salinas
User ID: tb4da5abf3430a61.30284590

Tunnel Broker News:

- ☛DynDns support for dns.he.net [March 23, 2011]
- ☛Last 2 /8s, before the reserved 5 are assigned, now allocated. [January 31, 2011]
- ☛Re: PPTP Tunnel Beta [October 29, 2010]
- ☛UPDATE - August 14th, 2010 [August 14, 2010]
- ☛Re: PPTP Tunnel Beta [July 02, 2010]

Tunnel [2 / 5]	Routed /64	Routed /48	Description
1.tunnel.tserv4.mia1.ipv6.he.net	2001:470:5:37::/64	2001:470:d991::/48	Test 1
2.tunnel.tserv8.dal1.ipv6.he.net	2001:470:1f0f:bcf::/64	None	

6. En la página de detalles puedes ver los detalles de tu túnel. Esta es toda la información que necesitas para configurar tu túnel. Para saber específicamente

como configurar tu computador selecciona la pestaña de "ExampleConfigurations".

The screenshot shows the 'Tunnel Details' page with the 'Example Configurations' tab selected. The page is divided into several sections:

- Account Menu:** Main Page, Account Info, Logout.
- User Functions:** Combine Tunnels, Create Regular Tunnel, Create BGP Tunnel, IPv6 Portscan.
- Tunnel Details:**
 - IPv6 Tunnel:** Tunnel ID: 115505, Creation Date: May 25, 2011, Description: [empty].
 - IPv6 Tunnel Endpoints:** Server IPv4 Address: 216.218.224.42, Server IPv6 Address: 2001:470:1f0e:bcf::1/64, Client IPv4 Address: 201.239.124.248, Client IPv6 Address: 2001:470:1f0e:bcf::2/64.
 - Available DNS Resolvers:** Anycasted IPv6 Caching Nameserver: 2001:470:20::2, Anycasted IPv4 Caching Nameserver: 74.82.42.42.
 - Routed IPv6 Prefixes:** Routed /64: 2001:470:1f0f:bcf::/64, Routed /48: [empty].
 - rDNS Delegations:** rDNS Delegated NS1: [empty], rDNS Delegated NS2: [empty], rDNS Delegated NS3: [empty], rDNS Delegated NS4: [empty], rDNS Delegated NS5: [empty].
- Quick Links:** Certification, Tunnelbroker, Free DNS, BGP Toolkit, Forums, FAQ, Video Presentations, IPv6 Blog Posts, Usage Statistics, Tunnel Server Status, Network Map, Looking Glass (v4/v6), Route Server (telnet), Global IPv6 Report, IPv6 BGP View.
- Services:** Transit, Colocation, Dedicated Servers.
- v4 Exhaustion:** IPv4 & IPv6 Statistics, RIR v4 /24s Left: AfriNIC (247,390), APNIC (75,681), ARIN (514,497), LACNIC (246,192), RIPE (225,172).

7. En la página de "ExampleConfigurations" selecciona tu sistema operativo para que se muestren los comandos necesarios para la configuración de tu lado. La siguiente imagen muestra la configuración para un equipo con Windows 7.

The screenshot shows the 'Tunnel Details' page with the 'Example Configurations' tab selected. The page is divided into several sections:

- Account Menu:** Main Page, Account Info, Logout.
- User Functions:** Combine Tunnels, Create Regular Tunnel, Create BGP Tunnel, IPv6 Portscan.
- Tunnel Details:**
 - IPv6 Tunnel:** Tunnel ID: 115505, Creation Date: May 25, 2011, Description: [empty].
 - Operating System:** Windows Vista/2008/7.
 - Commands:** Copy and paste the following commands into a command window:

```
netsh interface teredo set state disabled
netsh interface ipv6 add v6v4tunnel IP6Tunnel 201.239.124.248 216.218.224.42
netsh interface ipv6 add address IP6Tunnel 2001:470:1f0e:bcf::2
netsh interface ipv6 add route ::/0 IP6Tunnel 2001:470:1f0e:bcf::1
```
 - NOTE:** When behind a firewall appliance that passes protocol 41, use the IPv4 address you get from your appliance's DHCP service instead of the IPv4 endpoint you provided to our broker.
 - Disclaimer:** The configurations provided are example configurations and may be different depending on the version of the OS or the tools you are using. If you have any issues getting your tunnel to work please contact us at ipv6@he.net and we will be happy to assist you.
- Quick Links:** Certification, Tunnelbroker, Free DNS, BGP Toolkit, Forums, FAQ, Video Presentations, IPv6 Blog Posts, Usage Statistics, Tunnel Server Status, Network Map, Looking Glass (v4/v6), Route Server (telnet), Global IPv6 Report, IPv6 BGP View.
- Services:** Transit, Colocation, Dedicated Servers.
- v4 Exhaustion:** IPv4 & IPv6 Statistics, RIR v4 /24s Left: AfriNIC (247,390), APNIC (75,681), ARIN (514,497), LACNIC (246,192), RIPE (225,172).

8. Eso es todo, si todo salió bien ya deberías poder hacer ping desde tu computador al IPv6 del otro lado (la dirección que aparece como "Server IPv6 Address" en la página de TunnelDetails).

PROBLEMAS

Si tu túnel no funciona aquí hay algunas cosas básicas que puedes chequear.

1.- **¿Estas utilizando una IP pública?** El extremo de tu lado del túnel debe ser alcanzable desde Internet. Si estás detrás de un routes casero lo más probable es que no estés utilizando una dirección pública y esto podría ser el problema.

2.- **¿Hay filtros en el camino a tu computador?** El tunnelbroker encapsula paquetes IPv6 dentro de paquetes IPv4. Este tipo de paquetes podrían ser bloqueados por algunos firewalls de computadores personales. Permite que el protocolo 41 pase por tu firewall (nótese que es protocolo 41 y no puerto 41) o bien desactiva tu firewall temporalmente para ver si este es el problema (¡no olvides activarlo después de la prueba!).

Después de haber configurado el TunnelBroker correctamente, se necesita una dirección de destino pública, una dirección fuente pública y un prefijo. [Imágenes tomadas de referencia 15].

CONFIGURACIÓN EN SISTEMA OPERATIVO LINUX

```
modprobe ipv6
ip tunnel add he-ipv6 mode sit remote 216.66.38.58 local 186.82.173.237 ttl 255
ip link set he-ipv6 up
ip addr add 2001:470:1c51d::2/64 dev he-ipv6
ip route add ::0 dev he-ipv6
ip -f inet6 addr
```

Dirección destino: 216.66.38.58 (Donde se va a hacer llegar el túnel).

Dirección fuente: 186.82.173.237(Dirección pública que se tiene en el enrutador).

Prefijo: 2001:470:1c:51d::2/64 (Prefijo que entrega el proveedor del túnel).

En la segunda línea, estamos agregando un túnel llamado “he-ipv6” (nombre cualesquiera), esta se verá como una nueva interfaz de red, anteriormente eth0.

CONFIGURACIÓN EN EQUIPOS CISCO LINKSYS WRTS54G

```
insmod ipv6
modprobe ipv6
ip tunnel add he-ipv6 mode sit remote 216.66.38.58 local 186.82.173.237 ttl 255
ip link set he-ipv6 up
ip addr add 2001:470:1c:51d::2/64 dev he-ipv6
ip route add ::/0 dev he-ipv6
ip addr add 2001:470:1c:51d::0014:bf0b:d2e5/64 dev br0
ip -f inet6 addr
```

Básicamente, la configuración que se utiliza en los equipos enrutadores Cisco Linksys, son muy similares a la configuración que se realiza en los equipos Linux, ya que el sistema operativo de estos dispositivos es basado en Linux.

CONFIGURACIÓN EN SISTEMA OPERATIVO SOLARIS

```
ifconfig ip.tun0 inet6 plumb
ifconfig ip.tun0 inet6 tsrsrc 186.82.173.237 tdst 216.66.38.58 up
ifconfig ip.tun0 inet6 addif 2001:470:1c:51d::2 2001:470:1c:51d::1 up
route add -inet6 default 2001:470:1c:51d::1
```

Se crea una interfaz que en este caso se llama ip.tun0, y además se le asigna el direccionamiento. Al final se coloca la ruta IPv6 por defecto para que nuestros paquetes IPv6 puedan salir por medio de ese túnel.

CONFIGURACIÓN EN SISTEMA OPERATIVO MAC OSX

```
ifconfig gif0 create
ifconfig gif0 tunnel 186.82.173.237 216.66.38.58
ifconfig gif0 inet6 2001:470:1c:51d::2 2001:470:1c:51d::1 prefixlen 128
route -n add -inet6 default 2001:470:1c:51d::1
```

La configuración en Mac, es muy parecida a la de Solaris, siendo que en este se colocan algunos comandos diferentes por cuestión de sistema operativo.

CONFIGURACIÓN EN SISTEMA OPERATIVO WINDOWS XP Y 2000

```
ipv6 install
ipv6 rtu ::/0 2/::216.66.38.58 pub
ipv6 adu 2/2001:470:1c51d::2
```

Primero se debe instalar el protocolo puesto que este NO viene instalado por defecto. Automáticamente después de esto el sistema lo monta la interfaz IPv6 y procedemos a la configuración de IP's para el envío de paquetes a través del túnel.

CONFIGURACIÓN EN SISTEMA OPERATIVO WINDOWS VISTA Y WINDOWS 7

```
netsh interface teredo set state disabled
netsh interface ipv6 add v6v4tunnel IP6Tunnel 186.82.173.237 216.66.38.58
netsh interface ipv6 add address IP6Tunnel 2001:470:1c51d::2
netsh interface ipv6 add route ::0 IP6Tunnel 2001:470:1c51d::1
```

En Windows vista o Windows 7, hay que ejecutar un comando básico llamado netsh, este se debe ejecutar siempre como administrador para tener los privilegios y poder efectuar la configuración del túnel de IPv6.

CONCLUSIONES

En la Actualidad, hablar de IPv6 no es un mito, es más que una realidad, una definición tangible, en la cual al pasar los días las empresas se verán obligadas a ir migrando sus aplicaciones y entorno hacia este nuevo tema. De acuerdo a la escasez de direcciones IPv4, la necesidad de migración es algo necesario, y en base a esto, nuestro estudio analizo y observo cuales han sido aquellas barreras en las cuales se ha visto inmersa la transición a este nuevo protocolo.

De acuerdo a las encuestas planteadas y las investigaciones realizadas, se ha podido llegar a concluir que una de las barreras más comunes al tratar este tema es la falta de conocimiento que se posee del protocolo IPv6. Muchas de las empresas no ven viable esta transición ya que en la actualidad los operadores o distribuidores de internet no han migrado en mucho de los casos hacia esa nueva tecnología, por lo tanto se sigue utilizando IPv4, y aseguran que si su proveedor de servicios no ha migrado porque lo tendrían que hacer ellos, si el mundo se mueve en el antiguo protocolo y las redes actuales muchas de ellas no soportan IPv6, y el proceso de transición representa un gasto importante para dichas empresas, del que no se vería necesariamente un retorno de inversión dado que prácticamente nadie usa IPv6. Además, no provee una ventaja significativa en cuanto a las estrategias de negocios (salvo que el negocio sea la continua publicación de servicios en Internet). Por si fuera poco, el costo que tiene una migración de IPv4 a IPv6 implica entrenamiento, equipo nuevo con mayores capacidades de hardware.

Por otro lado, la investigación realizada nos muestra que el mejor método para realizar de transición es por medio de la creación de túneles de IPv6 sobre IPv4 (6over4). Esta metodologíatiene como ventaja que proporciona seguridad por medio de direcciones específicas para cada interface y permite al enrutador tener el enlace por medio de IPv4, independizando así la red existente de las redes IPv6 que se conectan en los puertos Ethernet del enrutador. Esta opción nos permite trabajar sobre la red existente IPv4 sin tener que hacer una inversión fuerte en infraestructura, el cambio se haría solamente en los nodos

nuevos o para beneficios de la empresa, se haría un cambio paulatino en las maquinas existentes, pero dicho cambio no afecta la infraestructura de la red.

RECOMENDACIONES

Las ventajas y bondades que nos brinda IPv6 se pueden ir aprovechando poco a poco mientras más equipos se vayan migrando a la nueva red, por lo tanto lo más importante en lo que se tiene que pensar es en la concientización que tienen que ir tomando las empresas respecto al nuevo protocolo de internet (IPv6), puesto que el cambio viene pronto, y se debe comenzar a analizar cuáles son aquellas alternativas con las que se cuentan actualmente, para que al realizar esta transición, se den las cosas dentro de parámetros accesibles a las empresas Cartageneras.

Se recomienda implementar talleres para fomentar el conocimiento que se debe tener acerca de este nuevo protocolo IPv6, partiendo desde sus ventajas y desventajas para que así, las empresas analicen su situación con respecto a este nuevo fenómeno, porque IPv6 es más que un mito, es una realidad!

GLOSARIO

DIRECTACCESS: Otorga a los usuarios acceso sin problemas a redes corporativas sin necesidad de una VPN.

DNS: Es un sistema de nomenclatura jerárquica para computadoras, servicios o cualquier recurso conectado a internet o a una red privada.

Firewall: (Cortafuegos en español) es una parte de un sistema o una red que está diseñada para bloquear el acceso no autorizado, permitiendo al mismo tiempo comunicaciones autorizadas. Se trata de un dispositivo o conjunto de dispositivos configurados para permitir, limitar, cifrar, descifrar, el tráfico entre los diferentes ámbitos sobre la base de un conjunto de normas y otros criterios.

ISP (Internet Service Provider): Es una empresa que brinda conexión a internet a sus clientes.

MTU (Maximum Transfer Unit): Unidad máxima de transferencia, es un término de redes de computadores que expresa el tamaño en bytes de la unidad de datos más grande que puede enviarse usando un protocolo de internet (IP).

Multihoming: Se define como la conexión de un host o sitio a más de un ISP a la vez.

Tunneling: Este concepto se refiere al proceso de hacer encapsulamiento de paquetes IPv6 a través de redes IPv4.

ACRONIMOS

NAT: Network Address Translation

VLAN: Virtual Local Area Network.

IPv4: Internet Protocol version 4.

IPv6: Internet Protocol version 6.

REFERENCIAS BIBLIOGRÁFICAS

- [1] Cicileo, Guillermo; Gagliano, Roque; O’Flaherty, Christian; Olvera, César; Palet, Jordi; Rocha, Mariela; Vives, Álvaro; “*IPv6 para Todos, Guía de uso y aplicación para diversos entornos*”; ISOC – AR, Internet Society Capitulo Argentina.
- [2] G. Turchanyi, J. Mohacsi, “*IPv4-IPv6 Transition - Just to cut the Gordian Knot?*”, The 13th International Telecommunications Network Strategy and Planning Symposium, 2008.
- [3] S. H. Gunderson, “*Global IPv6 statistics - Measuring the Current State of IPv6 for Ordinary Users*”, Google White Paper, 2008.
- [4] G. Goth, “*Close to the Edge: NAT vs. IPv6 Just the Tip of a Larger Problem*”, IEEE Internet Computing, vol.9, 2005.
- [5] Xianhui, Che; Dylan, Lewis; “*IPv6: Current Deployment and Migration Status*”, International Journal of Research and Reviews in Computer Science (IJRRCS) Vol. 1, No. 2, June 2010.
- [6] PaletMartinez, Jordi; Cabellos-Aparicio, Alberto; “*El Protocolo IPv6*”, 6SOS, v4 2004.
- [7] Sotillo, Samuel; “*IPv6 Security Issues*”, East Carolina University.
- [8] Bagnulo Braun, Marcelo; “*Herramientas para la Conectividad IPv6 con Múltiples Proveedores*”, Universidad Carlos III de Madrid, 2005.
- [9] SANS Institute, “*Security Features in IPv6*”; SANS Institute InfoSec Reading Room, 2002.
- [10] Kent, S.; Seo, K., “*Security Architecture for the Internet Protocol*”; RFC 4301, Dec. 2005.
- [11] Larson, Robert; Cockcroft, Lance, “*CCSP Cisco Certified Security Professional Certification Tutorial*”, McGraw-Hill/Osborne.

- [12] Palet Martinez, Jordi; "IPv6 Overall Status".
- [13] Yezid Donoso Meisel; "Comparación, ventajas problemas y una metodología para la transición de IPv4 a IPv6 en las redes de comunicaciones".
- [14] Proyecto "IPv6 para Chile" (<http://www.ipv6.cl/usuario-final/equipamiento-de-redes>).
- [15] Becerra, Darío; "Conferencia, Innovación Taller Próxima parada IPv6", Campus Party Colombia, 2011.
- [16] Sedano, Javier; editor Revistas Profesionales; "Mundo Linux de Revistas Profesionales".
- [17] Granados Reyes, ISE Eduardo; "Transición de IPv4 a IPv6 en las empresas"; *UVM – Tlalpan*.
- [18] Proyecto "IPv6 para Chile" (<http://www.ipv6.cl/ipv6-para-usuarios-finales/guia-tunel-broker>).
- [19] Bons, Emile; H. Weigand; "IPv6: Drivers and Barriers for Adopting"; Department of Information Management, Tilburg University.
- [20] <http://technet.microsoft.com/es-es/library/ee382298%28WS.10%29.aspx>
- [21] Fabian, Baez; Cueva. Rebeca; Guevara, Eduardo; Rios, Edgar; Laso, Santiago; Valencia, Janeth; "Creación de Túneles"; Escuela Politecnica Nacional, Ecuador, 2006.