INTERCONECTIVIDAD 6

YENSY CAROLINA GOMEZ CARDENAS
EDWIN YHOVANY GARZON AMEZQUITA

CORPORACION UNIVERSITARIA MINUTO DE DIOS UNIMINUTO
FACULTAD DE INGENIERIA, TECNOLOGIA EN INFORMATICA
SOACHA
2011

INTERCONECTIVIDAD 6

YENSY CAROLINA GOMEZ CARDENAS
EDWIN YHOVANY GARZON AMEZQUITA

PROYECTO DE INVESTIGACION IMPLEMENTACION PROTOCOLO IPv6 EN LA UNIVERSIDAD MINUTO DE DIOS REGIONAL (SOACHA).

TUTOR
PABLO FONSECA
INGENIERO

CORPORACION UNIVERSITARIA MINUTO DE DIOS UNIMINUTO
FACULTAD DE INGENIERIA, TECNOLOGIA EN INFORMATICA
SOACHA
2011

Nota de aceptación

_____

_____

_____

_____

_____

Firma Jurado

_____

Firma Jurado

Soacha, 16 de Enero de 2012

INTRODUCCION

El siguiente documento tiene con fin mostrar una guía teórico-práctica para la transición en la implementación de una red utilizando el protocolo IPv6.

Se debe mencionar que paralelamente al crecimiento de usuarios y dispositivos tecnológicos se ha venido pensando en ¿qué? y ¿cómo? hacer para que la red a la que todos estos se conectan funcione de la manera adecuada, pensando en esto se está trabajando en la transición de la red actual IPv4 a IPv6.

El protocolo IPv6 tiene características que mejoran la conexión a la red, no solo hablando en cuanto al número de direcciones que permite mayor cantidad de usuarios y dispositivos conectados, sino también seguridad en el tránsito de los datos, mayor velocidad entre otros.

Por tanto se pretende fomentar la utilización del IPv6 en las redes actuales aportando el conocimiento para que la universidad adopte este protocolo para hacer uso de las ventajas que este le brinda.

CONTENIDO

LISTA DE TABLAS

LISTA DE ILUSTRACIONES

1. EL PROBLEMA

1.1. PLANTEAMIENTO DEL PROBLEMA

El protocolo Ipv4 dejó de ser suficiente ante el constante crecimiento tecnológico, usuarios de internet y la necesidad de interconexión de los usuarios a través de dispositivos.

1.2. DESCRIPCION DEL PROBLEMA

El ente encargado de la administración del direccionamiento IP (IANA) ya entrego el último paquete de direcciones IPv4 disponibles para la conectividad de los millones de usuarios y dispositivos que han venido en constante crecimiento. Por esto surge la necesidad de adoptar un nuevo protocolo que permita una mayor conectividad que pueda suplir la demanda al que está expuesto el protocolo IPv4.

1.3. FORMULACION DEL PROBLEMA

¿Cómo la universidad Minuto de Dios (Regional Soacha), puede adoptar el protocolo Ipv6 y que se requiere para que este modelo se implemente con las condiciones actuales?

2. OBJETIVOS

2.1. OBJETIVO GENERAL

- Realizar un estudio técnico, económico e infraestructura para sugerir la implementación del protocolo ipv6 en la Universidad Minuto De Dios (Regional Soacha).

2.2. OBJETIVOS ESPECIFICOS

- Dar a conocer los requisitos técnicos que se necesitan para implementar el estándar IPv6 para la Universidad Minuto De Dios (Regional Soacha).

- Describir cómo se puede desarrollar este protocolo con las condiciones actuales y que se necesita para la implementación.

- Mostrar y describir los beneficios de una posible ejecución del proyecto en la Universidad Minuto De Dios.

3. ¿QUE ES IP?

IP es la sigla de Internet Protocolo o Protocolo de Internet. Es un estándar no orientado a conexión que se utiliza para el envío y recepción de datos a través de una red de paquetes conmutados.

El IP no cuenta con mecanismos para confirmar si un paquete de datos alcanzó o no su destino. Esto puede generar que el paquete llegue dañado, duplicado, desordenado o que simplemente, no llegue. En caso que los paquetes a transmitir superen el máximo permitido en el tramo de red, la información es subdividida en paquetes más pequeños y re ensamblada en el momento necesario.

Las direcciones IP hacen referencia a la máquina de origen y destino en una comunicación a través del protocolo de Internet. Los conmutadores de paquetes (conocidos como switches) y los enrutadores (routers) utilizan las direcciones IP para decidir qué tramo de red utilizarán para reenviar los paquetes.

La dirección IP está compuesta por un número que permite identificar, de manera lógica y jerárquica, a la interfaz de un dispositivo que se encuentra dentro una red que utiliza el protocolo de Internet. Los usuarios de Internet, utilizan una dirección IP que suele cambiar al momento de cada conexión. Esta forma de asignación es conocida como dirección IP dinámica.

Las páginas de Internet que deben estar conectados de manera permanente, utilizan una dirección IP fija o estática. Esto quiere decir que la dirección no cambia con el tiempo.

4. PROTOCOLO IPv4

IPv4 es la versión 4 del Protocolo de Internet y constituye la primera versión de IP que es implementada de forma masiva. Este el principal protocolo utilizado en el Nivel de Red del Modelo TCP/IP para Internet. Fue descrito inicialmente en el RFC 791 elaborado por la Fuerza de Trabajo en Ingeniería de Internet (**IETF**) en Septiembre de 1981, documento que dejó obsoleto al RFC 760 de Enero de 1980.

IPv4 es un protocolo orientado hacia datos que se utiliza para comunicación entre redes a través de interrupciones de paquetes (por ejemplo a través de Ethernet). Presenta las siguientes fallas:

- Es un protocolo de un servicio de datagramas no fiable (también referido como de *mejor esfuerzo*).
- No proporciona garantía en la entrega de datos, ni sobre la corrección de los datos.
- Los paquetes se pueden duplicar o desordenar.

Todos los problemas mencionados se resuelven en el nivel superior en el modelo TCP/IP, por ejemplo, a través de TCP o UDP.

El propósito principal de IP es proveer una dirección única a cada sistema para asegurar que una dispositivo en Internet pueda identificar a otro.

Direcciones: IPv4 utiliza direcciones de 32 bits (4 bytes) que limita el número de direcciones posibles a utilizar a 4.294.967.295 direcciones únicas. Sin embargo, muchas de estas están reservadas para propósitos especiales como redes privadas, Multidifusión, etc. Debido a esto se reduce el número de

direcciones IP que realmente se pueden utilizar, es esto mismo lo que ha impulsado la creación de IPv6 como reemplazo eventual para IPv4.

Representación de las direcciones: Cuando se escribe una dirección IPv4 en cadenas, la notación más común es decimal con puntos.

Asignación: Desde 1993 rige el esquema CIDR cuya principal ventaja es permitir la subdivisión de redes y permite a las entidades sub-asignar direcciones IP, como haría un ISP con un cliente.

El principio fundamental del encaminamiento (routing) es que la dirección codifica información acerca de localización de un dispositivo dentro de una red. Esto implica que una dirección asignada a una parte de una red no funcionará en otra parte de la red. Existe una estructura jerárquica que se encarga de la asignación de direcciones de Internet alrededor del mundo. Esta estructura fue creada para el CIDR, y hasta 1998 fue supervisada por la IANA y sus RIR. Desde el 18 de Septiembre de 1998 la supervisión está a cargo de la ICANN. Cada RIR mantiene una base de datos WHOIS disponible al público y que permite hacer búsquedas que proveen información acerca de las asignaciones de direcciones IP. La información obtenida a partir de estas búsquedas juega un papel central en numerosas herramientas las cuales se utilizan para localizar direcciones IP geográficamente.

Redes privadas: De los más de cuatro mil millones de direcciones permitidas por IPv4, tres rangos están especialmente reservados para utilizarse solamente en redes privadas. Estos rangos no tienen encaminamiento fuera de una red privada y las máquinas dentro de estas redes privadas no pueden comunicarse directamente con las redes públicas. Pueden, sin embargo, comunicarse hacia redes públicas a través de la Traducción de Direcciones de Red o NAT.

Anfitrión local (Localhost): Además de las redes privadas, el rango 127.0.0.0 – 127.255.255.255, o 127.0.0.0/8 en la notación CIDR, está reservado para la comunicación del anfitrión local (localhost). Ninguna dirección de este rango deberá aparecer en una red, sea pública o privada, y cualquier paquete enviado hacia cualquier dirección de este rango deberá regresar como un paquete entrante hacia la misma máquina.

Referencia de sub-redes de IP versión 4: Algunos segmentos del espacio de direcciones de IP, disponibles para la versión 4, se especifican y asignan a través de documentos RFC, que son conjuntos de notas técnicas y de organización que se elaboran desde 1969 donde se describen los estándares o recomendaciones de Internet, antes ARPANET.

La máscara de sub-red es utilizada para separar los bits de un identificado de una red a partir de los bits de los identificados del anfitrión. Se escribe utilizando el mismo tipo de notación para escribir direcciones IP.

5. IPv4 vs IPv6

IPv6 no fue pensado únicamente para la aumentar significativamente el número de direcciones IP, sino que también tuvo en cuenta aspectos que buscan tener un transporte de datos más estructurado y confiable. En el siguiente cuadro se muestran las características y cuáles son las diferencias entre IPv4 e IPv6.

CARACTERISTICAS	IPv4	IPv6
Direcciones	Las direcciones de origen y destino tienen una longitud de 32 bits (4 bytes).	Las direcciones de origen y destino tienen una longitud de

		128 bits (16 bytes).
IPSec	La compatibilidad es opcional	La compatibilidad es obligatoria
Identificación del número de paquetes	No existe ninguna identificación de flujo de paquetes para que los enrutadores controlen la QoS en el encabezado IPv4.	Se incluye la identificación del flujo de paquetes para que los enrutadores controlen la QoS en el encabezado IPv6, utilizando el campo FlowLabel (etiqueta de flujo).
Fragmentación	La llevan a cabo los enrutadores y el host realiza el envío.	No la llevan a cabo los enrutadores, sino únicamente el host que realiza el envío.
Encabezado	Incluye una suma de comprobación.	No incluye una suma de comprobación.
Opciones	El encabezado no la incluye	Todos se trasladan a los encabezados de extensión IPv6.
Marcos de solicitud ARP	El protocolo de resolución de direcciones (ARP) utiliza los marcos de solicitud ARP de difusión para resolver una dirección IPv4 como una dirección de capa de vínculo.	Los marcos de solicitud ARP se sustituyen por mensajes de solicitud de vecinos de multidifusión.
Administrar la pertenencia a grupos locales de subred	Se utiliza el protocolo de administración de grupos de internet (IGMP).	IGMP se sustituye con los mensajes de descubrimiento de escucha de multidifusión (MLD).
Determinar la dirección IPv4 de la mejor puerta de enlace predeterminada.	Se utiliza el descubrimiento de enrutadores ICMP, y es opcional.	El descubrimiento de enrutadores ICMP queda sustituido por la solicitud de ICMPv6 y los mensajes de anuncio de enrutador, y es obligatorio.
Direcciones de multidifusión.	Se utiliza para enviar tráfico en todos los nodos de la	No hay direcciones de multidifusión de IPv6. De forma alternativa,

	subred.	se utiliza una dirección de multidifusión para todos los nodos del ámbito local del vínculo.
Configuración Manual	Debe configurarse manualmente o a través de un DCHP.	No requiere configuración manual o a través de un DCHP.
DNS	Utiliza registros de recurso (A) de direcciones de host en el sistema de nombres de dominio (DNS) para correlacionar nombres de host con direcciones IPv4.	Utiliza registros de recursos (AAA) de dirección de host en el sistema de nombres de dominio (DNS) para correlacionar nombres de host con direcciones IPv6.
Direcciones de IP relacionados con host	Utiliza registros de recurso (A) de puntero en el dominio (DNS) IN-ADDR.ARPA para correlacionar direcciones IPv4 con nombres de host.	Utiliza registros de recurso (PTR) de puntero en el dominio DNS IP6.INT para correlacionar direcciones IPv6 con nombres de host.
Tamaño de paquete.	Debe admitir un tamaño de 576 bytes (Posiblemente fragmentado).	Debe admitir un tamaño de 1280 bytes (Sin fragmentación).

Tabla 1: Comparativo Ipv6 vs Ipv4

6. ¿PORQUE IPV6?

IPv6 nace debido a que su antecesor IPv4, fue diseñado con un número de direcciones que inicialmente eran suficientes, por la cantidad de usuarios, aplicaciones y dispositivos conectados en red. Con el tiempo y a pasos agigantados la tecnología se fue posicionando en la vida cotidiana de miles de

usuarios con dispositivos a los cuales cada vez es más fácil acceder, lo que fue haciendo evidente que IPv4 dejo de ser suficiente ante la demanda tecnológica.

Cuando se comenzó a trabajar en este protocolo se tuvo en cuenta la insuficiencia de direcciones para conectarse a la red y como toda evolución trajo consigo la revisión de las características que conjuntamente permiten que la transmisión de datos sea eficiente, por esto se pensó en mejorar la velocidad, la seguridad y calidad etc. Así IPv6 busca dar una solución integral al manejo y trasmisión de paquetes de datos.

7. HISTORIA DE IPv6

IPv6 es la versión 6 del Protocolo de Internet, es el encargado de dirigir y encaminar los paquetes en la red, fue diseñado en los años 70 con el objetivo de interconectar redes.

El IPv6 fue diseñado por Steve Deering y Craig Mudge, adoptado por IETF en 1994. IPv6 también se conoce por “IP Next Generation” o “IPng”.

Esta nueva versión del Protocolo de Internet está destinada a sustituir al estándar IPv4, ya que esta cuenta con un límite de direcciones de red, lo cual impide el crecimiento de la red.

La Internet EngineeringTaskForce (IETF) comienza a promover en 1995 el nuevo protocolo de Internet IPv6. Inicialmente se pensaba que se tenían las direcciones suficientes por lo que no se le dio la importancia a la implementación de dicho protocolo, además de los altos costos que generaba el cambio de infraestructura al adoptar dicho protocolo. En 2000 fue adoptada por Japón y China e India comenzaron a migrar sus sistemas al IPv6 por su cuenta, creando capacidades técnicas localmente. Así, Asia, empieza la migración.

Más adelante, entre 2004 y 2006, Estados Unidos y Europa se abren hacia el nuevo protocolo y en 2008 el gobierno de Estados Unidos decide comenzar la migración institucional al IPv6, así todas las oficinas gubernamentales y estatales trabajan ya sobre esta nueva versión de Internet. Tal es así que hoy en día, las entidades públicas de Estados Unidos tienen que justificar el uso del antiguo protocolo, el IPv4. Lo que obliga a las compañías y demás entidades a adoptar al IPv6 para entablar contacto con el gobierno estadounidense.

En Europa cada país toma sus decisiones al respecto. Por ejemplo, España en 2002 instala el IPv6 en una red de universidades. La Unión Europea (UE) quería estimular el nuevo protocolo desde el 2000, a través de grandes inversiones económicas, pero no podía obligar a los Estados a que llevasen a cabo esta renovación. Con lo que todo quedaba en manos de los grandes operadores de telecomunicaciones, que se resisten a invertir por la ausencia de usuarios potenciales.

Hasta 2004, la mayor parte de las direcciones en IPv6 estaban asignadas a Asia, Estados Unidos comienza a recuperar el terreno perdido.

En Latinoamérica: Brasil, México y Argentina hacen sus intentos con el nuevo protocolo. En 2005 se crea en China la mayor red del país para conectar a las universidades nacionales. Una red de tal magnitud que no hubiera podido tener con IPv4 ante la gran cantidad de direcciones IP que requería el proyecto.

En la actualidad estamos ante una transición mundial hacia el IPv6, aunque no es todavía palpable para el común de los usuarios.

El IPv6 no es un IPv4 mejorado, tiene una mejor infraestructura, posibilita un mejor acceso a los móviles y a las nuevas aplicaciones y dispositivos, además la seguridad intrínseca. IPv6 ofrece un rango de direcciones muchísimo mayor que la versión IPv4, la cual está más limitada, y un acceso a los servicios actuales.

Las nuevas aplicaciones se diseñan ya para el nuevo protocolo, para redes ‘peer-to-peer’ (P2P) que funcionan sin servidores fijos. Estratégicamente, será

preferible abandonar algunos sistemas antiguos porque resultará muy caro y difícil de adaptarlos a la nueva infraestructura mundial.

Los nuevos sistemas ideados para el IPv4 suponen una gran inversión en infraestructuras. Los países en vías de desarrollo necesitan prepararse para la gran aventura, hoy no disponen de capacidades técnicas apropiadas y la brecha digital corre el riesgo de hacerse más grande si no se toman las medidas necesarias.

7.1. ¿QUE ES LA TRANSICIÓN A IPv6?

Para comenzar a hablar de la implementación de IPv6, debemos tener en cuenta que no se puede pensar en migración del protocolo IPv4 hacia el IPv6, internet es una red que permite que el servicio de las comunicaciones este arriba todo el tiempo, por lo que pensar en suspenderla por unos segundos, generaría un caos, en el mundo de las telecomunicaciones, por lo tanto en la vida cotidiana.

Precisamente por ello, la organización encargada de la estandarización de los protocolos de Internet IETF, diseñó junto a IPv6, una serie de mecanismos que llamamos de transición y coexistencia.

Actualmente el protocolo predominante es IPv4, lo que se pretende es que poco a poco se IPv6 vaya siendo el protocolo con más fuerza para conexión a internet, por esto se habla de transición, los dos protocolos deben trabajar simultáneamente hasta que los contenidos y servicios estén disponibles para IPv6.

Para llegar a este punto es importante mencionar que en el diseño del protocolo IPv6 se tuvo en cuenta las deficiencias que presenta el protocolo actual por lo que aunque la transición tome un largo periodo de tiempo, con creación de nuevos dispositivos y aplicaciones además del aumento de usuarios IPv6 tomara más fuerza.

Es importante recordar que el 3 de Febrero de 2011 se agotaron las direcciones IPv4 en el registro central de IANA, por lo que los proveedores de servicios de Internet están acelerando el despliegue de IPv6 en sus redes para que tanto los nuevos usuarios como los existentes sigan disfrutando de un uso habitual y continuado de Internet.

7.2. ACTUALIDAD Y CARACTERISTICAS DE IPv6

IPv6 no es solamente un aumento en el número de direcciones. Este protocolo se presenta como la evolución en la trasmisión de paquetes de datos, ya que para IPv6 será necesario hacer modificaciones que tengan en cuenta los cambios de tráfico que aparecerán en las redes IP globalmente. Es anticipado que esto tendrá mucho más énfasis en transacciones en tiempo real como Internet y metamorfosis de intranets para redes de datos del viejo estilo, dentro de los sistemas de transmisión complejos transportando un enorme tamaño de datos.

Al mismo tiempo IPv6 intenta una dirección de cabeceras largas de una red IP desde el punto de vista de los administrados; configurando la red en el primer lugar. En el trabajo del nuevo protocolo se está teniendo en cuenta que si se tiene un sistema IPv6 y la conexión entre dos redes IPv4, entonces se hablara de paquetes IPv6 a través de redes IPv4 (Transición).

Otro factor que dirige el desarrollo de IPv6 es la necesidad de un cifrado mejorado. La comunicación privada a través de un medio público como Internet requiere servicios de cifrado que impidan que los datos enviados se puedan ver o modificar durante el tránsito. Existe un estándar que proporciona seguridad para los paquetes IPv4 denominado IPSec. No obstante, en IPv4 este estándar es opcional y prevalecen las soluciones propietarias. Las siguientes son las características básicas de IPv6.

Una nueva dirección: Actualmente solo se conoce la convención de direcciones IPv4, donde las direcciones son escritas como 4 números entre 0 y 255 separados por puntos. Este es primer cambio que presenta IPv6, las direcciones de este protocolo son de 32 bits a 128 representadas con hexadecimales.

Para manejar la configuración de direcciones tan largas, IPv6 ofrece 2 caminos; primero usa números hexadecimales (base 16, de 0 a F) en vez de decimal, y segundo comprime las direcciones resultantes permitiendo la comprensión de más ceros. Así una típica dirección en esta forma larga sería algo así: DEAD:BEEF:0000:0000:0000:0073:FEED:F00D.

Ahora después de una dirección típica de IPv6 podría tener un número de ceros, esta dirección puede estar en una versión reducida como DEAD:BEEF::73:FEED:F00D. Aquí la convención es que lleva ceros sin los grupos de 4 dígitos puede estar por cuenta gotas, como 0073 se convierte a 73. Un grupo consecutivo de números de 16 bits con el valor de cero puede ser reemplazado con dos puntos. Esto solo se puede reemplazar unas cadenas vacías con los dos puntos. Si hay solo dos cadenas nulas, solo uno puede ser comprimido como esto porque si ambos fuesen comprimidos no sería posible determinar como de larga es cada una, y así tendríamos una dirección ambigua.

Finalmente, hay una pequeña modificación en la forma de la dirección de IPv6 expresando una dirección IPv4 en formato IPv6. Salvando el final, la conversión entre base 10(decimal) y base 16 (hexadecimal), la convención usa el antiguo estilo de la notación del punto para los últimos 32 bits de la dirección, así la dirección IP aparece como 0000:0000:0000:0000:0000:0000:193.64.30.189, la cual la podemos poner comprimida de la forma::193.64.30.189. Así, a pesar del hecho de tener cuadruplicado el espacio de la dirección, la antigua dirección IP puede ser expresada sin ambigüedades en el nuevo formato con solo añadir 2 caracteres.

Cabeceras: Una de las deficiencias con IPv4, identificada por los comités, fue la complejidad de sus cabeceras. Si se hubiese permitido el creciendo de este factor como el espacio de direcciones esto se había extendido, entonces esto sería muy difícil de manejar. La cabecera de IPv4 tiene un total de 10 campos, los dos campos de 32 bits de direcciones (uno para el origen y otro para el destino), y un campo de opciones el cual es utilizado para llevar la cabecera a una longitud correcta. Aún con el campo de opciones vacío, una cabecera IPv4 tiene 20 bytes de longitud, así claramente la cabecera de 80 bytes de IPv6 no fue algo deseable.

Así la cabecera IPv6 es simplificada para permitir a las cabeceras ser encadenadas juntas. Hay ahora solo 6 campos - las dos direcciones de 128 bytes para origen y destino, y nada de opciones. Variaciones en la cabecera que serían consideradas con la cabecera IPv4, o las opciones de campos, ahora identificadas usando un nuevo campo, con otras especificaciones con otra cabecera incluida después del actual, pero antes del dato mismo. La primera cabecera define la necesidad mínima para un paquete IPv6, incluyendo la versión, prioridad, etiqueta de dirección, payloadhearer y límite de salto, e incluye un campo que dice "y hay otra cabecera después de esta". No hay límite del número de cabecera que pueda ser enlazado en el camino. Como el siguiente campo de cabecera es un número de 8 bits, puede haber 255 tipos diferentes de cabeceras. Solo 6 tipos diferentes están definidos en la actualidad:

- Opciones-salto-por-salto.
- Encaminamiento-de-cabecera.
- Fragmentación-de-cabecera.
- Autentificación-de-cabecera.
- Encapsulamiento-de-seguridad.
- Payload-header.
- Opciones de destino de cabecera.

El resultado de esta simplificación y la flexibilidad mejorada, es que la simplificación de la cabecera IPv6 es de hasta 40 bytes de longitud - o el doble del tamaño de la cabecera IPv4 sin opciones - a pesar del hecho de que dos direcciones incorporadas son 4 veces el tamaño de la cabecera de IPv4. Si decides tener todos los recortes, la cabecera podría hacerse bastante larga, aunque esto no es posible ya que solo han sido definidos 6 tipos de cabeceras. La nueva solución es mucho más elegante, en esas sencillas tareas se necesitan solo crear cabeceras simples y con poco peso, mientras se permite más complejidad para las aplicaciones o sistemas que lo necesiten. La complejidad reducida de las cabeceras IPv6 por defecto hacen que la tarea del router, por término medio, sea mucho más fácil.

Configuración: Para muchos administradores de redes IPv6 parece, a primera vista, ser algo para solucionar los problemas de alguien. Después de todo, muchos de nosotros tenemos realmente un gran bloque de direcciones IP permitidas las cuales veremos completamente los próximos años. IPv6 es probablemente más significante al administrador de una red estable de IP que es para un recién llegado. Esto es porque IPv6 tiene características significativas intensificadas para habilitar un host a su configuración. Muchos de nosotros sabemos que - a pesar de que todos nos ayudamos de BOOTP y DHCP - muchos administradores de redes, o la mayor parte pasan un poco de su tiempo escribiendo números IP en campos de direcciones en uno de los paneles de control. Esto quiere decir que la mitad de las direcciones del mundo han sido definidas manualmente. Un estudio de investigación ha sugerido que la configuración automática de IPv6 podría rendir ella misma - comparando con la configuración manual de IPv4 - en 12 meses.

El propósito de los diseñadores del aspecto de IPv6 fue que el host debería permitir descubrir automáticamente toda la información necesaria para conectarse a internet sin la intervención humana. Esto suena como un pedido

alto pero no es tan complejo o tan telepático como suena. Los requerimientos mínimos para un host son que debería permitirle generar una dirección única IP, y descubrir al menos una dirección de router. Necesita tener permiso para hacer esto con o sin un servidor o un router en la subred local.

En un modo completamente la interfaz se asignaría una dirección a sí misma para establecer una dirección de enlace local, una dirección válida solo en la subred local.

7.3. VENTAJAS Y OBJETIVOS DEL PROTOCOLO IPv6

El encabezado IPv6 tiene un nuevo formato que está diseñado para reducir al mínimo el procesamiento y la validación de encabezados. Una dirección IPv6 tiene una longitud cuatro veces mayor que la de una dirección IPv4. Las direcciones globales que se utilizan en la parte IPv6 de Internet están diseñadas para crear una infraestructura de enrutamiento eficaz, jerárquica y resumida que tiene en cuenta la coexistencia de múltiples niveles de proveedores de servicios Internet. En la parte IPv6 de Internet, los enrutadores de red troncal tienen una infraestructura jerárquica de enrutamiento y direccionamiento que utilizan las tablas de enrutamiento más pequeñas.

IPv6 admite la configuración de direcciones con estado (como la configuración de direcciones con la presencia de un servidor DHCP) y la configuración de direcciones sin estado (como la configuración de direcciones sin la presencia de un servidor DHCP). La compatibilidad con IPSec es un requisito del conjunto de protocolos IPv6. Este requisito proporciona una solución basada en estándares para las necesidades de seguridad de la red y promueve la interoperabilidad entre distintas implementaciones de IPv6. Los nuevos campos del encabezado IPv6 definen cómo se controla e identifica el tráfico.

La identificación del tráfico mediante un campo Flow Label en el encabezado IPv6 permite a los enrutadores identificar y controlar de forma especial los paquetes que pertenecen a un flujo determinado. Un flujo es una serie de paquetes entre un origen y un destino. Dado que el tráfico está identificado en el encabezado IPv6, la compatibilidad con la calidad de servicio QoS se puede obtener de forma sencilla incluso si la carga del paquete está cifrada con IPSec.

El nuevo protocolo Neighbor Discovery para la interacción de nodos vecinos en IPv6 consiste en un conjunto de mensajes del Protocolo de mensajes de control de Internet para IPv6 ICMPv6 que administran la interacción de nodos vecinos. Este protocolo reemplaza el Protocolo de resolución de direcciones (ARP), el Descubrimiento de enrutadores ICMPv4 y los mensajes de Redirección ICMPv4 por mensajes de multidifusión y unidifusión eficaces.

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. En la tabla siguiente se comparan las características clave de los protocolos IPv4 e IPv6.

ESPECIFICACIONES DEL PROTOCOLO INTERNET VERSIÓN IPV6

IPv6 aporta el protocolo ND (NeighborDiscovery, descubrimiento de vecinos), que emplea la mensajería como medio para controlar la interacción entre nodos vecinos. Por nodos vecinos se entienden los nodos de IPv6 que están en el mismo vínculo. Por ejemplo, al emitir mensajes relativos al descubrimiento de vecinos, un nodo puede aprender la dirección local de vínculo de un vecino. El protocolo ND controla las principales actividades siguientes del vínculo local de IPv6:

1. **Descubrimiento de encaminadores:** Ayuda a los hosts a detectar encaminadores en el vínculo local.

2. **Configuración automática de direcciones:** Permite que un nodo configure de manera automática direcciones IPv6 para sus interfaces.

3. **Descubrimiento de prefijos:** Posibilita que los nodos detecten los prefijos de subred conocidos que se han asignado a un vínculo. Los nodos utilizan prefijos para distinguir los destinos que se encuentran en el vínculo local de los asequibles únicamente a través de un encaminador.

4. **Resolución de direcciones:** Permite que los nodos puedan determinar la dirección local de vínculo de un vecino solamente a partir de la dirección IP de los destinos.

5. **Determinación de salto siguiente:** Utiliza un algoritmo para establecer la dirección IP de un salto de destinatario de paquetes que está más allá del vínculo local. El salto siguiente puede ser un encaminador o el nodo de destino.

6. **Detección de inasequibilidad de vecinos:** Ayuda a los nodos a establecer si un nodo ya no es asequible. La resolución de direcciones puede repetirse tanto en encaminadores como hosts.

7. **Detección de direcciones duplicadas:** Permite que un nodo pueda determinar si está en uso o no una dirección que el nodo tenga la intención de utilizar.

8. **Redirección:** Un encaminador indica a un host el mejor nodo de primer salto que se puede usar para acceder a un determinado destino.

El protocolo ND emplea los tipos de mensajes ICMP siguientes para la comunicación entre los nodos de un vínculo:

- Solicitud de en caminador.
- Anuncio de en caminador.
- Solicitud de vecino.
- Anuncio de vecino.
- Redirección.

7.4. DIRECCIONAMIENTO IPv6 BÁSICO

IPv6 es la nueva generación del protocolo de comunicaciones de Internet y gran parte de los sistemas operativos actuales están ya preparados para utilizarlo.

7.4.1. TIPOS DE DIRECCIONES IP

Definiciones previas de los tipos de direcciones IPv6 (extraído de RFC 2462):

- **Unicast**: Dirección que identifica de forma única a una interfaz.
- **Multicast:** Dirección que identifica a un conjunto de interfaces (normalmente pertenecientes a diferentes nodos). Un paquete que se envíe a una dirección multicast es reenviado a todas las interfaces identificadas por esa dirección.
- **Anycast:** Dirección que identifica a un conjunto de interfaces (normalmente pertenecientes a diferentes nodos). Un paquete que se envíe a una dirección anycast es reenviado a una de las interfaces identificadas por esa dirección (la más cercana de acuerdo al protocolo de enrutamiento utilizado
- **Broadcast:** No existen este tipo de direcciones IPv6.
- **Link-local:** Una dirección que sólo tiene el ámbito (*scope*) de enlace y que puede utilizarse para alcanzar los nodos vecinos conectados en el mismo enlace. Todas las interfaces de red tienen una dirección unicast link-local.
- **Site Local:** Una dirección con el ámbito limitado al sitio local, término obsoleto hoy en día y sustituido por unique local.
- **Unique local (ULA):** Sustituyen a las direcciones site-local (RFC-4193) y son direcciones privadas no enrutables o enrutables a través de unos pocos routers que cooperen.
- **Global:** Una dirección con un ámbito sin límite.

7.4.2. NOTACIÓN PARA LAS DIRECCIONES IPV6

Las direcciones IPv6, de 128 bits de longitud, se escriben como ocho grupos de cuatro dígitos hexadecimales.

Por ejemplo, 2001:0db8:85a3:08d3:1319:8a2e:0370:7334 es una dirección IPv6 válida. Se puede comprimir un grupo de cuatro dígitos si éste es nulo (es decir, toma el valor "0000").

Por ejemplo, 2001:0db8:85a3:0000:1319:8a2e:0370:7344 ---- 2001:0db8:85a3::1319:8a2e:0370:7344

Siguiendo esta regla, si más de dos grupos consecutivos son nulos, también pueden comprimirse como "::". Si la dirección tiene más de una serie de grupos nulos consecutivos la compresión sólo se permite en uno de ellos. Así, las siguientes son representaciones posibles de una misma dirección:

2001:0DB8:0000:0000:0000:0000:1428:57ab

2001:0DB8:0000:0000:0000::1428:57ab

2001:0DB8:0:0:0:0:1428:57ab

2001:0DB8:0::0:1428:57ab

2001:0DB8::1428:57ab

Son todas válidas y significan lo mismo, pero 2001::25de::cade no es válida porque no queda claro cuántos grupos nulos hay en cada lado.

Los ceros iniciales en un grupo también se pueden omitir:

2001:0DB8:02de::0e13

2001:DB8:2de::e13

Si la dirección es una dirección IPv4 empotrada, los últimos 32 bits pueden escribirse en base decimal, así:

::ffff:192.168.89.9

::ffff:c0a8:5909

No se debe confundir con:

::192.168.89.9

::c0a8:5909

El formato ::ffff:1.2.3.4 se denomina dirección IPv4 mapeada, y el formato ::1.2.3.4 dirección IPv4 compatible.

Las direcciones IPv4 pueden ser transformadas fácilmente al formato IPv6. Por ejemplo, si la dirección decimal IPv4 es 135.75.43.52 (en hexadecimal, 0x874B2B34), puede ser convertida a 0000:0000:0000:0000:0000:0000:874B:2B34 o ::874B:2B34. Entonces, uno puede usar la notación mixta dirección IPv4 compatible, en cuyo caso la dirección debería ser ::135.75.43.52. Este tipo de dirección IPv4 compatible casi no está siendo utilizada en la práctica, aunque los estándares no la han declarado obsoleta.

Cuando lo que se desea es identificar un rango de direcciones diferenciable por medio de los primeros bits, se añade este número de bits tras el carácter de barra "/".

Por ejemplo:

2001:0DB8::1428:57AB/96 sería equivalente a 2001:0DB8::

2001:0DB8::874B:2B34/96 sería equivalente a 2001:0DB8:: y por supuesto también a 2001:0DB8::1428:57AB/96.

7.4.3. IDENTIFICACIÓN DE LOS TIPOS DE DIRECCIONES

Los tipos de direcciones IPv6 pueden identificarse tomando en cuenta los rangos definidos por los primeros bits de cada dirección.

::/128

La dirección con todo ceros se utiliza para indicar la ausencia de dirección, y no se asigna ningún nodo.

::1/128

La dirección de loopback es una dirección que puede usar un nodo para enviarse paquetes a sí mismo (corresponde con 127.0.0.1 de IPv4). No puede asignarse a ninguna interfaz física.

::1.2.3.4/96

La dirección IPv4 compatible se usa como un mecanismo de transición en las redes duales IPv4/IPv6. Es un mecanismo que no se usa.

::ffff:0:0/96

La dirección IPv4 mapeada se usa como mecanismo de transición en terminales duales.

fe80::/10

El prefijo de *enlace local* (en inglés *link local*) específica que la dirección sólo es válida en el enlace físico local.

fec0::

El *prefijo de emplazamiento local* (en inglés *site-local prefix*) específica que la dirección sólo es válida dentro de una organización local. La RFC 3879 lo declaró obsoleto, estableciendo que los sistemas futuros no deben implementar ningún soporte para este tipo de dirección especial. Se deben sustituir por direcciones Local IPv6 Unicast.

ff00::/8

El prefijo de multicast. Se usa para las direcciones multicast.

Hay que resaltar que no existen las direcciones de difusión en IPv6, aunque la funcionalidad que prestan puede emularse utilizando la dirección multicast FF01::1/128, denominada todos los nodos.

Paquete IPv6

Un paquete en IPv6 está compuesto principalmente de dos partes: la cabecera (que tiene una parte fija y otra con las opciones) y la carga útil (los datos).

Cabecera Fija

Los primeros 40 bytes (320 bits) son la cabecera del paquete y contiene los siguientes campos:

- Direcciones de origen (128 bits).
- Direcciones de destino (128 bits).
- Versión del protocolo IP (4 bits).
- Clase de tráfico (8 bits, Prioridad del Paquete).
- Etiqueta de flujo (20 bits, manejo de la Calidad de Servicio).
- Longitud del campo de datos (16 bits).
- Cabecera siguiente (8 bits).
- Límite de saltos (8 bits, Tiempo de Vida).

Hay dos versiones de IPv6 levemente diferentes. La ahora obsoleta versión inicial, descrita en el RFC 1883, difiere de la actual versión propuesta de estándar, descrita en el RFC 2460, en dos campos: hay 4 bits que han sido reasignados desde "etiqueta de flujo", "clase de tráfico". El resto de diferencias son menores.

En IPv6 la fragmentación se realiza sólo en el nodo origen del paquete, al contrario que en IPv4 en donde los routers pueden fragmentar un paquete. En IPv6, las opciones también desaparecen de la cabecera estándar y son especificadas por el campo "Cabecera Siguiente", similar en funcionalidad en IPv4 al campo Protocolo. Un ejemplo: en IPv4 uno añadiría la opción "ruta fijada desde origen" a la cabecera IPv4 si quiere forzar una cierta ruta para el paquete, pero en IPv6 uno modificaría el campo "Cabecera Siguiente" indicando que viene una cabecera de encaminamiento. La cabecera de

encaminamiento podrá entonces especificar la información adicional de encaminamiento para el paquete, e indicar que, por ejemplo, la cabecera TCP será la siguiente. Este procedimiento es análogo al de AH y ESP en IPsec para IPv4 (que aplica a IPv6 de igual modo, por supuesto).

Cabeceras de extensión

El uso de un formato flexible de cabeceras de extensión opcionales es. una idea innovadora que permite ir añadiendo funcionalidades de forma paulatina. Este diseño aporta gran eficacia y flexibilidad ya que se pueden definir en cualquier momento a medida que se vayan necesitando entre la cabecera fija y la carga útil.

Hasta el momento, existen 8 tipos de cabeceras de extensión, donde la cabecera fija y las de extensiones opcionales incluyen el campo de cabecera siguiente que identifica el tipo de cabeceras de extensión que viene a continuación o el identificador del protocolo de nivel superior. Luego las cabeceras de extensión se van encadenando utilizando el campo de cabecera siguiente que aparece tanto en la cabecera fija como en cada una de las citadas cabeceras de extensión. Como resultado de la secuencia anterior, dichas cabeceras de extensión se tienen que procesar en el mismo orden en el que aparecen en el datagrama. La Cabecera principal, tiene a diferencia de la cabecera de la versión IPv4 un tamaño fijo de 40 octetos. Específica para asignarlos para aplicaciones multicast intra-dominio o entre-dominios (RFC 3306). En IPv4 era muy difícil para una organización.

Todas o parte de estas cabeceras de extensión tienen que ubicarse en el datagrama en el orden especificado:

CABECERA DE EXTENSIÒN	DESCRIPCIÒN	RFC
Opciones salto a salto (Hop-By-Hop Options)	Contiene datos que deben ser examinados por cada nodo a través de la ruta envió de un paquete.	RFC 2460
Ruteo (Routing)	Métodos para especificar la forma de rutear un datagrama (Usado con IPv6 móvil).	RFC 2460, 3775, 5095
Cabecera de fragmentación (Fragment)	Contiene parámetros para la fragmentación de los datagramas.	RFC 2460
Cabecera de autenticación (Authentication Header (AH))	Contiene información para verificar la autenticación de la mayor parte de los datos del paquete.	RFC 4302
Encapsulado de seguridad de la carga útil.	Lleva la información cifrada para comunicación segura.	RFC 4303
Opciones para el destino	Información que necesita ser examinada solamente por los nodos de destino del paquete.	RFC 2460
No Next Header	Vacío indica que no hay más cabeceras.	RFC 2460

Tabla 2: Cabeceras de Extension

Cada cabecera de extensión debe aparecer como mucho una sola vez, salvo la cabecera de opción destino, que puede aparecer como mucho dos veces, una antes de la cabecera ruteo y otra antes de la cabecera de la capa superior.

Carga Útil

La carga útil del paquete puede tener un tamaño de hasta 64 KB en modo estándar, o mayor con una opción de carga jumbo (jumbo payload) en el encabezado opcional Hop-By-Hop.

La fragmentación es manejada solamente en el host que envía la información en IPv6: los routers nunca fragmentan un paquete y los hosts se espera que utilicen el Path MTU discovery.

7.5. AUTOCONFIGURACIÓN DE DIRECCIONES LIBRES DE ESTADO

Los nodos IPv6 pueden configurarse a sí mismos automáticamente cuando son conectados a una red ruteada en IPv6 usando los mensajes de descubrimiento de routers de ICMPv6. La primera vez que son conectados a una red, el nodo envía una solicitud de router de link-local usando multicast (router solicitación) pidiendo los parámetros de configuración; y si los routers están configurados para esto, responderán este requerimiento con un anuncio de router que contiene los parámetros de configuración de capa de red.

Si la autoconfiguración de direcciones libres de estado no es adecuada para una aplicación, es posible utilizar Dynamic Host Configuration Protocol para IPv6 (DHCPv6) o bien los nodos pueden ser configurados en forma estática.

Los routers presentan un caso especial de requerimientos para la configuración de direcciones, ya que muchas veces son la fuente para información de autoconfiguración, como anuncios de prefijos de red y anuncios de router. La configuración sin estado para routers se logra con un protocolo especial de remuneración de routers.

Multicast: la habilidad de enviar un paquete único a destinos múltiples es parte de la especificación base de IPv6. Esto es diferente a IPv4, donde es opcional (aunque usualmente implementado).

IPv6 no implementa broadcast, que es la habilidad de enviar un paquete a todos los nodos del enlace conectado. El mismo efecto puede lograrse

enviando un paquete al grupo de multicast de enlace-local todos los nodos (all hosts). Por lo tanto, no existe el concepto de una dirección de broadcast y así la dirección más alta de la red la dirección de broadcast en una red IPv4 es considerada una dirección normal en IPv6.

Muchos ambientes no tienen, sin embargo, configuradas sus redes para rutear paquetes multicast, por lo que en éstas será posible hacer "multicasting" en la red local, pero no necesariamente en forma global.

El multicast IPv6 comparte protocolos y características comunes con IPv4, pero también incorpora cambios y mejoras. Incluso cuando se le asigne a una organización el más pequeño de los prefijos de ruteo global IPv6, ésta también recibe la posibilidad de usar uno de los 4.2 billones de grupos multicast IPv6 ruteables de fuente específica para asignarlos para aplicaciones multicast intra-dominio o entre-dominios (RFC 3306). En IPv4 era muy difícil para una organización conseguir incluso un único grupo multicast ruteable entre-dominios y la implementación de las soluciones entre-dominios eran anticuadas (RFC 2908). IPv6 también soporta nuevas soluciones multicast, incluyendo Embedded Rendezvous Point (RFC 3956), el que simplifica el despliegue de soluciones entre dominios.

Seguridad de Nivel de Red obligatoria: Internet Protocol Security (IPsec), el protocolo para cifrado y autenticación IP forma parte integral del protocolo base en IPv6. El soporte IPsec es obligatorio en IPv6; a diferencia de IPv4, donde es opcional (pero usualmente implementado). Sin embargo, actualmente no se está usando normalmente IPsec excepto para asegurar el tráfico entre routers de BGP IPv6.

Procesamiento simplificado en los routers: Se hicieron varias simplificaciones en la cabecera de los paquetes, así como en el proceso de

reenvío de paquetes para hacer el procesamiento de los paquetes más simple y por ello más eficiente.

El encabezado del paquete en IPv6 es más simple que el utilizado en IPv4, así los campos que son raramente utilizados han sido movidos a opciones separadas; en efecto, aunque las direcciones en IPv6 son 4 veces más largas, el encabezado IPv6 (sin opciones) es solamente el doble de largo que el encabezado IPv4 (sin opciones).

Los routers IPv6 no hacen fragmentación. Los nodos IPv6 requieren ya sea hacer descubrimiento de MTU, realizar fragmentación extremo a extremo o enviar paquetes menores al MTU mínimo de IPv6 de 1280 bytes. El encabezado IPv6 no está protegido por una suma de comprobación (checksum); la protección de integridad se asume asegurada tanto por el checksum de capa de enlace y por un checksum de nivel superior (TCP, UDP, etc.). En efecto, los routers IPv6 no necesitan recalcular la suma de comprobación cada vez que algún campo del encabezado como el contador de saltos o Tiempo de Vida, cambian. Esta mejora puede ser menos necesaria en routers que utilizan hardware dedicado para computar este cálculo y así pueden hacerlo a velocidad de línea (wirespeed), pero es relevante para routers por software.

El campo Tiempo de Vida de IPv4 se llama ahora Límite de Saltos (Hop Limit), reflejando el hecho de que ya no se espera que los routers computen el tiempo que específica para asignarlos para aplicaciones multicast intra dominio o entre-dominios (RFC 3306). En IPv4 era muy difícil para una organización co el paquete ha pasado en la cola.

Movilidad: A diferencia de IPv4 móvil, IPv6 móvil (MIPv6) evita el ruteo triangular y por lo tanto es tan eficiente como el IPv6 normal. Los routers IPv6 pueden soportar también Movilidad de Red (NEMO, por Network Mobility) (RFC 3963), que permite que redes enteras se muevan a nuevos puntos de conexión de routers sin reasignación de numeración.

Soporte mejorado para las extensiones y opciones: Los cambios en la manera en que se codifican las opciones de la cabecera IP permiten límites menos rigurosos en la longitud de opciones, y mayor flexibilidad para introducir nuevas opciones en el futuro.

Jumbogramas: IPv4 limita los paquetes a 64 KB de carga útil. IPv6 tiene soporte opcional para que los paquetes puedan superar este límite, los llamados jumbogramas, que pueden ser de hasta 4 GiB. El uso de jumbogramas puede mejorar mucho la eficiencia en redes de altos MTU. El uso de jumbogramas está indicado en el encabezado opcional Jumbo PayloadOption.

8. IPV6 Y EL SISTEMA DE NOMBRES DE DOMINIO

Las direcciones IPv6 se representan en el Sistema de Nombres de Dominio (DNS) mediante registros *AAAA* (también llamados registros de *quad-A*, por tener una longitud cuatro veces la de los registros A para IPv4)

El concepto de AAAA fue una de las dos propuestas al tiempo que se estaba diseñando la arquitectura IPv6. La otra propuesta utilizaba registros *A6* y otras innovaciones como las etiquetas de cadena de bits y los registros *DNAME*.

Mientras que la idea de AAAA es una simple generalización del DNS IPv4, la idea de A6 fue una revisión y puesta a punto del DNS para ser más genérico, y de ahí su complejidad.

La RFC 3363 recomienda utilizar registros AAAA hasta tanto se pruebe y estudie exhaustivamente el uso de registros A6. La RFC 3364 realiza una comparación de las ventajas y desventajas de cada tipo de registro.

8.1. MECANISMOS DE TRANSICIÓN A IPV6

Ante el agotamiento de las direcciones IPv4, y los problemas que este está ocasionando ya, sobre todo en los países emergentes de Asia como India o China, el cambio a IPv6 ya ha comenzado. Se espera que convivan ambos protocolos durante un año, aunque se piensa que la implantación mundial y total en internet de IPv6 se hará realidad hacia finales de 2012, dada la celeridad con la que se están agotando las direcciones IPv4. La red no podrá aguantar mucho más sin el cambio, y de no realizarse pronto este las consecuencias podrían ser muy graves. Existe una serie de mecanismos que permitirán la convivencia y la migración progresiva tanto de las redes como de los equipos de usuario. En general, los mecanismos de transición pueden clasificarse en tres grupos:

- Doble pila
- Túneles
- Traducción

La doble pila: hace referencia a una solución de nivel IP con doble pila (RFC 4213), que implementa las pilas de ambos protocolos, IPv4 e IPv6, en cada nodo de la red. Cada nodo con doble pila en la red tendrá dos direcciones de red, una IPv4 y otra IPv6.

- **A favor**: Fácil de desplegar y extensamente soportado.
- **En contra**: La topología de red requiere dos tablas de encaminamiento y dos procesos de encaminamiento. Cada nodo en la red necesita tener actualizadas las dos pilas.

Los túneles: permiten conectarse a redes IPv6 "saltando" sobre redes IPv4. Estos túneles trabajan encapsulando los paquetes IPv6 en paquetes IPv4 teniendo como siguiente capa IP el protocolo número 41, y de ahí el nombre *proto-41*. De esta manera, se pueden enviar paquetes IPv6 sobre una infraestructura IPv4. Hay muchas tecnologías de túneles disponibles. La principal diferencia está en el método que usan los nodos encapsuladores para determinar la dirección a la salida del túnel.

La traducción: es necesaria cuando un nodo que sólo soporta IPv4 intenta comunicar con un nodo que sólo soporta IPv6. Los mecanismos de traducción se pueden dividir en dos grupos basados en si la información de estado está guardada o no:

- **Con estado**: NAT-PT (RFC 2766), TCP-UDP Relay (RFC 3142), Socks-based Gateway (RFC 3089)
- **Sin estado**: Bump-in-the-Stack, Bump-in-the-API (RFC 276)

Despliegue de IPv6

Varios de los mecanismos mencionados más arriba se han implementado para acelerar el despliegue de IPv6. Los distintos servicios de control de Internet han ido incorporando soporte para IPv6, así como los controladores de los dominios de nivel superior (o ccTLD, en inglés).

8.2. RFC'S SOBRE IPV6

Como para todos los protocolos de Internet, la IETF, ha presentado gran cantidad de documentos especificando distintas partes de IPv6 como RFC's. Se trata la especificación básica del protocolo, la seguridad, la política de nombres, la interacción con otros niveles.

IPv6 no tiene una especificación completamente estable. Las especificaciones básicas han aparecido como documentos RFC. Las especificaciones de las capas superiores relacionadas están siendo discutidas ahora en el grupo de trabajo sobre IPng del IETF, y algunos documentos son accesibles como borradores de Internet.

A continuación, enumeramos la lista actual de los documentos de especificación relacionados:

NORMA	DESCRIPCIÒN
RFC 2373	Arquitectura de direccionamiento IPv6.
RFC 2374	Un formato de direcciones unicast globales para IPv6.
RFC 2460	Especificaciones del Protocolo de Internet Versión 6 (IPv6).
RFC 2461	Descubrimiento de vecinos para IPv6.
RFC 2462	Autoconfiguración de IPv6 sin estado.
RFC 2463	Especificación de Internet Control Message Protocol (ICMPv6), para IPv6.
RFC 1886	Extensiones de DNS para soportar IPv6.
RFC 1887	Una arquitectura para asignar direcciones unicast IPv6.
RFC 1981	Descubrimiento de la MTU de la ruta para IPv6.
RFC 2023	IPv6 sobre PPP.
RFC 2080	RIPng para IPv6.
RFC 2452	IPv6 Management Information Base para TCP (Transmisión Control Protocol).
RFC 2454	IPv6 Management Information Base para UDP (User Datagram Protocol).
RFC 2464	Transmission of IPv6 Packets Over Ethernet Networks
RFC 2465	Management Information Base para IPv6: Convenciones

	textuales y grupo general.
RFC 2466	Management Information Base para IPv6: Grupo ICMPv6.
RFC 2467	Transmisión de paquetes IPv6 sobre redes FDDI.
RFC 2470	Transmisión de paquetes IPv6 sobre redes Token Ring.
RFC 2472	Pv6 sobre PPP.
RFC 2473	Especificación de tunneling de paquetes genéricos en IPv6.
RFC 2507	Compresión de la cabecera IP.
RFC 2526	Direcciones anycast de subred IPv6 reservadas.
RFC 2529	Transmisión de IPv6 sobre dominios IPv4 sin túneles explícitos.
RFC 2545	Uso de extensiones multiprotocolo BGP-4 para encaminamiento entre dominios IPv6.
RFC 2590	Transmisión de paquetes IPv6 sobre FrameRelay
RFC 2675	Jumbogramas IPv6.
RFC 2710	MLD (Multicast Listener Discovery, Descubrimiento de receptores multicast) para IPv6.
RFC 2711	Opción de alarma de router IPv6.

Tabla 3: RFC's IPv6

9. IMPLEMENTACIÓN PROTOCOLO IPV6

A continuación se dará una explicación sencilla de cómo se podría implementar y adaptar del protocolo IPv6 en la universidad Minuto De Dios (Regional Soacha), aquí se toma el caso con base en la infraestructura que cuenta actualmente la universidad Minuto de Dios.

Nota: Es importante que para hacer dicha implementación se debe tener conocimientos de un nivel medio de Redes además de haber leído todo el marco teórico de este documento para informarse sobre el tema. Adicional a eso se deberá ver video ***Prueba Física IPv6 Dual Stack*** *(Anexo de Documento Interconectividad 6).*

Para dar inicio a la implementación del protocolo Ipv6 se deben tener en cuenta los siguientes pasos.

a. **Identificar la Infraestructura de red.**
b. **Configurar los componentes de la red**

9.1. IDENTIFICACION DE INFRAESTRUCTURA DE RED

Para llevara a cabo nuestro primer paso trataremos dos puntos importantes a la hora de llevar a cabo dicha implementación.

9.1.1. IDENTIFICAR EL EQUIPAMIENTO DE LA RED

9.1.1.1. DISPOSITIVOS NETWORKING

Identificaremos todos los componentes que no hacen parte de la interfaz de usuario, si no los componentes que establecen la comunicación de la red. Ejemplo: Switch, Router, Access Point, etc.

Figura 1: Dispositivos Networking

9.1.1.2. DISPOSITIVOS TERMINALES

Identificaremos todos los componentes con los cuales interactuamos directamente.

Ejemplo: Computadores, portátiles, iPhone, Smartphone, impresoras de red, Etc.

Figura 2: Dispositivos Networking

9.1.2. IDENTIFICAR LOS SISTEMAS OPERATIVOS

Identificaremos los sistemas operativos de los dispositivos terminales y de networking con los cuales interactuamos directamente.

Ejemplo: Windows, Linux, Mac, Unix, IOS Router, siendo estos los más utilizados en Redes.

Figura 3: Sistemas Operativos

Nota: Para trabajar el protocolo IPv6 el IOS del Router debe ser actualizado y debes ser compatible con IPv6 de lo contrario no se podrá trabajar dicho protocolo.

9.1.3. APLICACIONES DE RED DE SERVIDORES Y COMPUTADORES

Identificaremos las diferentes aplicaciones de los servidores que brindan servicios de red de cómo (e-mail, Ftp, Dns, Web) y de las de las terminales (computadores, Smartphone, laptops) para determinar las aplicaciones para la conexión cliente-servidor.

Figura 4: Aplicaciones de Red

9.2. CONFIGURACION DE COMPONENTES DE RED

Una vez identificada la infraestructura, determinar si la tecnología existente se puede adaptar al nuevo protocolo y que cambio hay que realizar.

Como ya identificado el software y toda la infraestructura de red procedemos a la etapa de configuración la cual dividiremos en 3 procedimientos:

9.2.1. CONFIGURACIÓN DEL SOFTWARE

Aquí haremos la configuración con Windows XP teniendo en cuenta que casi todos los pcs de la Universidad Minuto de Dios (Regional Soacha) cuenta con este sistema operativo.

Windows XP ya tiene instalado el protocolo IPv6, lo que haremos es solo activar el servicio, tiene dos maneras para hacerlo.

- Línea de comandos.
- Interfaz gráfica.

Por línea de comandos

Ingresar a la consola y ejecutar el comando.

Ipv6 install

Como lo podemos ver en la *figura 5.*

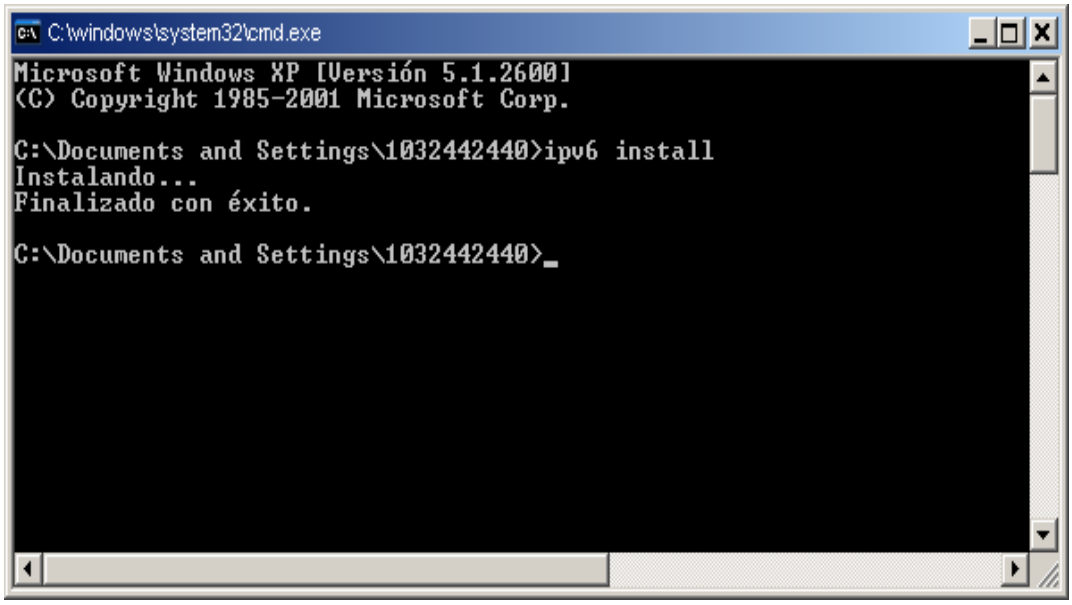

Figura 5: Instalación IPv6 en Xp por comandos

Instalación mediante interfaz gráfica.

Para hacer la instalación por interfaz gráfica seguiremos los siguientes pasos:

- Ingresar al panel de control →Click
- Ir a conexiones de red o Internet →Click
- La red de área local o inalámbrica →Click
- Ir a propiedades → Click
- Instalar → Click
- En protocolos seleccionar →**Microsoft TCP/IP versión 6.**

Si seguimos los pasos en orden nos aparecerá el protocolo activado como lo podemos ver en la *figura 6.*

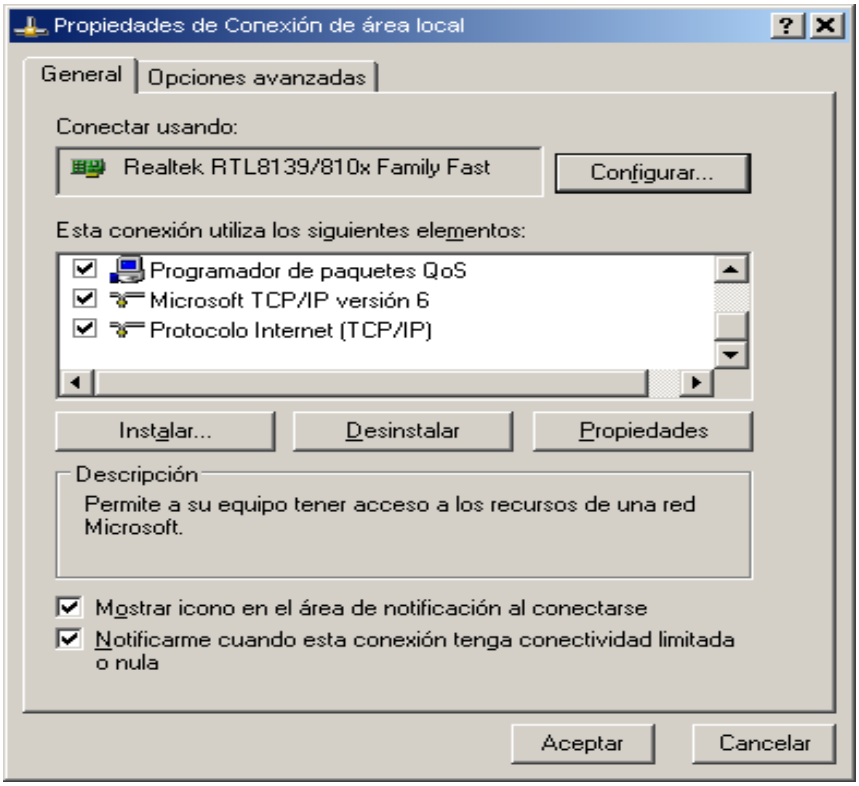

Figura 6: Instalación IPv6 en Xp por Interfaz Grafica

Antes de empezar con la configuración de la red interna y la red externa debemos tener en cuenta que son dos redes aparte es decir que llevan una configuración independiente *(ver figura 7).*

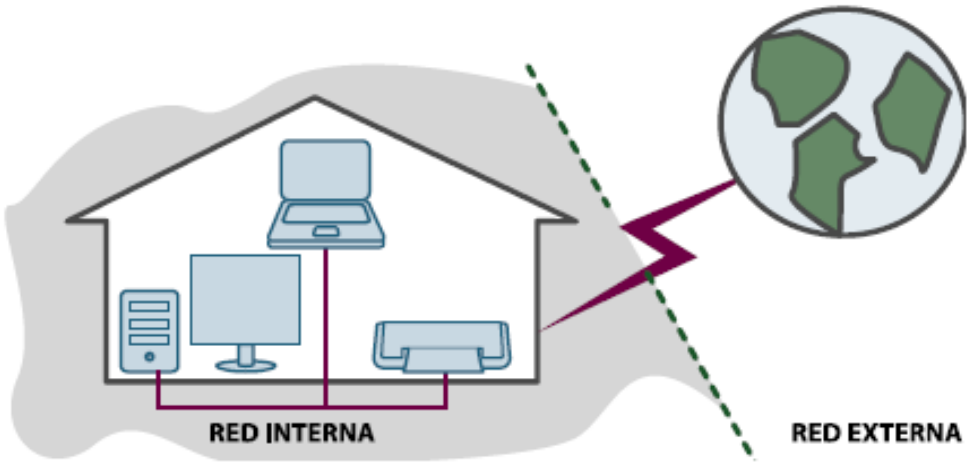

Figura 7: Red Interna y Red externa

En la configuración de las redes, es importante tener en cuenta como obtener las direcciones ip con las que trabajaremos, hay tres formas de hacer esto:

- Que el proveedor de internet asigne un bloque de direcciones
- Utilizar direcciones 6to4 (Es decir alguna dirección IPv4)
- Utilizar Tunels Brokers con algún sitio capaz de proveedor conectividad IPv6.

9.2.2. CONFIGURACIÓN DE LA RED INTERNA

Tenemos dos formas de realizar la configuración de la red Interna para que trabaje bajo el estándar IPv6:

- Manual
- Automática (Autoconfiguración)

Pero en este caso solo trataremos la configuración automática.

Para que se pueda llevarse a cabo la autoconfiguración de interfaces con direcciones IPv6, será necesario que los dispositivos que deseen configurarlas, soliciten los datos y que otro dispositivo, se encargue de anunciar dichos datos.

Estas solicitudes y anuncios forman parte del protocolo **Neighbor Discovery** a través de mensajes **ICMPv6**, para que se constituya la base para la autoconfiguración IPv6.

9.2.2.1. CONFIGURACION AUTOMATICA

En forma simplificada los mensajes IMPv6 que solicitan los datos se denominan:

- NS (Neighbor Solicitation).
- RS (Router Solicitation).

Y las respuestas vienen dadas en otros mensajes ICPv6 llamados:

- NA (Neighbor Advertisement).
- RA (Router Advertisement).

La configuración se hará con base en la *figura 8*.

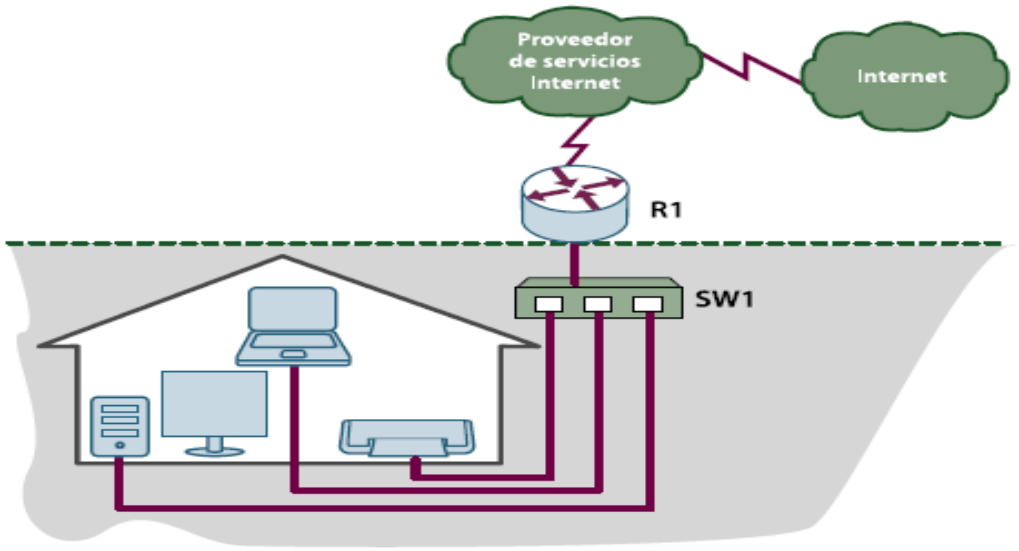

Figura 8: Red con un Enlace Dedicado

En la (*figura 8) nos* muestra la red con enlace a internet dedicado, es decir que dispone de un equipo router a donde llega el enlace internet (es decir que el proveedor deja a disposición del cliente una conexión para que solo pueda ser utilizada por el).Este router se conecta con la red interna a través de un switch adonde se conectan todos los dispositivos de la red.

Básicamente la autoconfiguración funciona así:

- Los dispositivos envían un mensaje NS y un mensaje RS al recibir este último el router le envía un mensaje RA que contiene el prefijo IPv6 para

que el dispositivo pueda realizar la autoconfiguración en la *figura 9* se claramente este proceso.

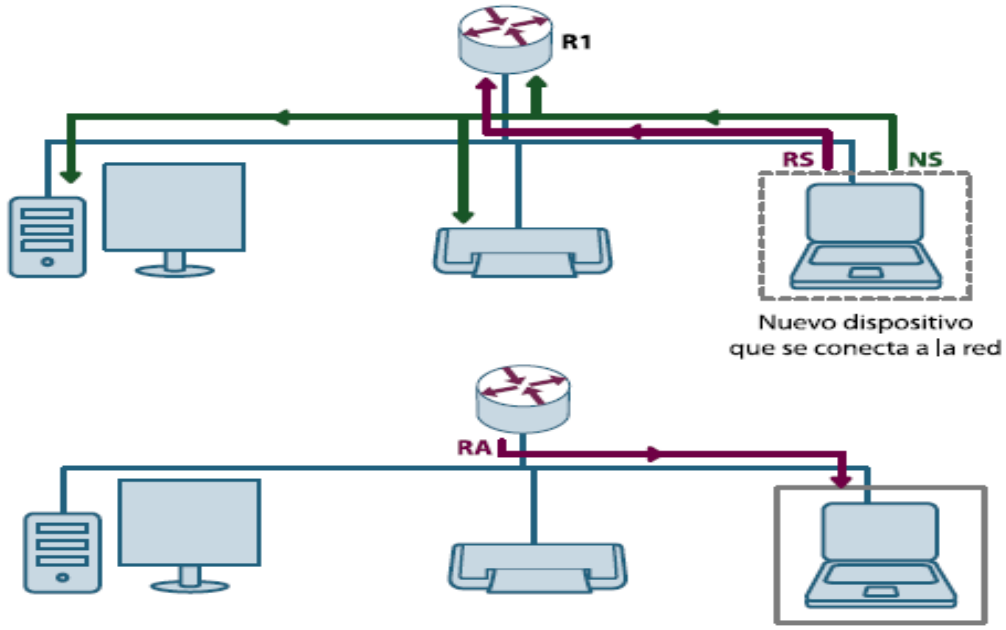

Figura 9: Proceso autoconfiguración automática Red Interna

Para que el router sepa que debe anunciar el prefijo IPv6 para el proceso de autoconfiguración, debemos consultar la tecnología del router y así poder configurar nuestra red interna IPv6. Con los routers Cisco solo es configurar la interfaz con una dirección de IPv6 para que esta pueda ser anunciada en la red interna.

Después de obtener el prefijo, el dispositivo estará en condiciones de tomar por si solo una dirección Ipv6 anunciado por el router y en su propia Mac Adress. En la siguiente *figura 10* veremos la autoconfiguración de la red interna.

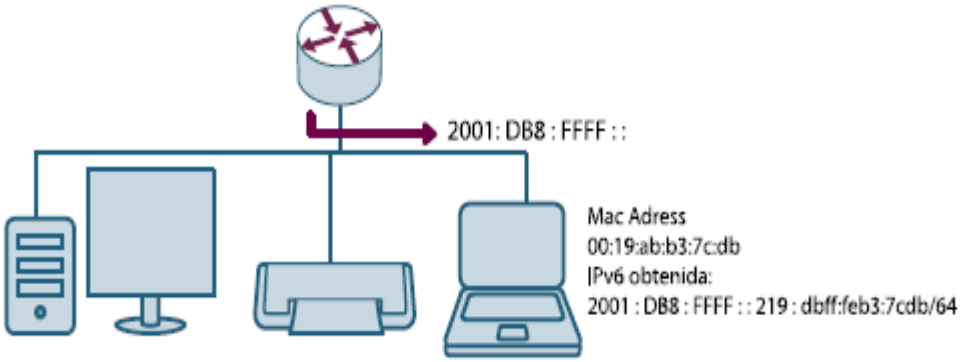

Figura 10: Autoconfiguración automática de Red Interna

9.2.3. CONFIGURACIÓN DE LA RED EXTERNA

Cuando llegamos a este punto tenemos que tener definido como vamos hacer la conexión con el exterior (Red WAN), existen dos tipos de situaciones.

a. Que el proveedor de internet nos brinde la conexión a través de IPv6

b. Que el proveedor de internet no pueda brindarnos la conexión IPv6.

Si nuestro caso es el **A** es posible que el proveedor ya está anunciando su propio prefijo IPv6 a internet y si da servicio a sus clientes. Como lo podemos ver en la *figura 11*.

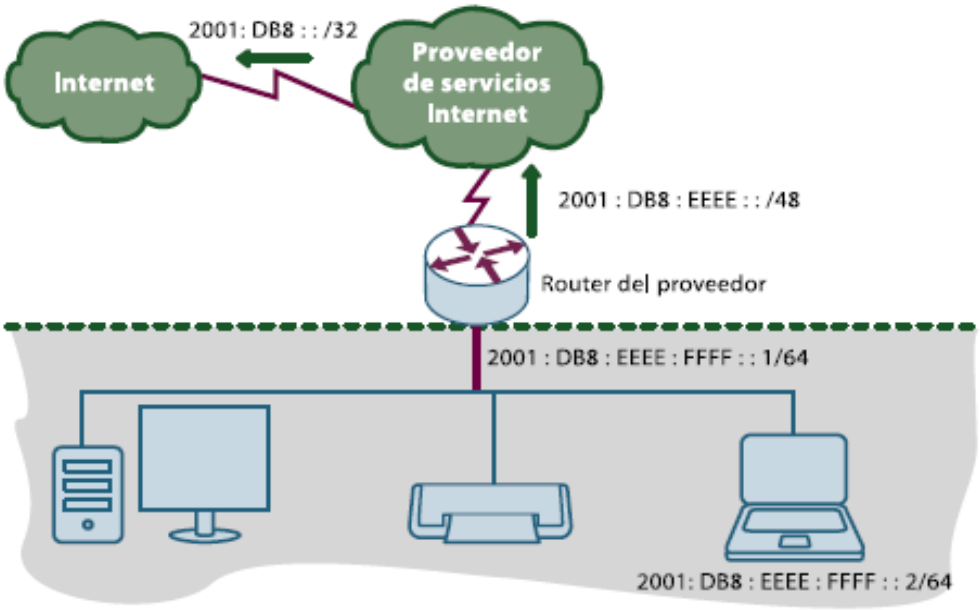

Figura 11: Autoconfiguración IPv6 por Proveedor

Pero si nuestro caso es el **B** debemos hallar la forma de atravesar la red IPv4, hay una forma de hacerlo es a través de los túneles, estos se dividen en dos grandes grupos: manuales y automáticos.

9.2.3.1. TUNELES AUTOMATICOS

Los túneles manuales son túneles que deben ser configurados cada uno de los extremos del túnel, como podemos ver en la *figura 12:*

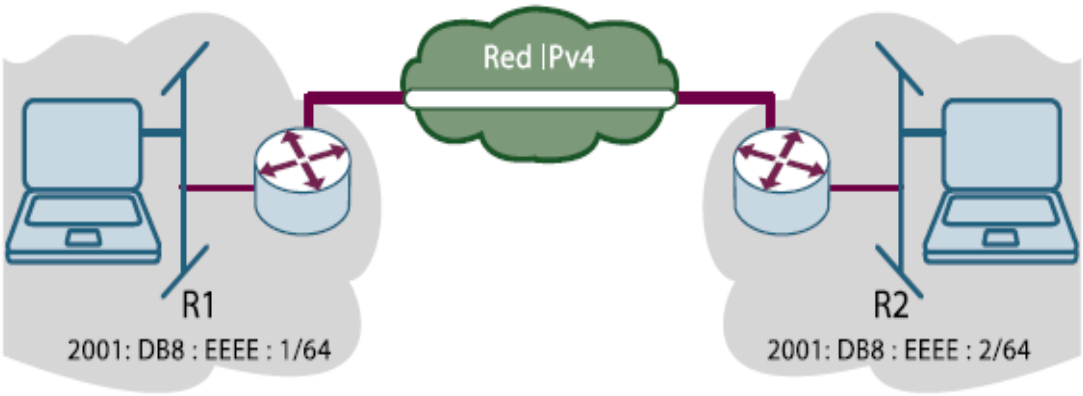

Figura 12: Túnel manual

La manera de configurar un túnel manual es la siguiente*:*

Router 1	Router 2
Interface TunnelR1	Interface TunnelR2
No ip adress	No ip adress
Ipv6 adress 2001:	Ipv6 adress 2001:
DB8:FFFF:1/64	DB8:FFFF:2/64
Tunnel source	Tunnel source
GigabitEthernet0/0	GigabitEthernet0/1
Tunnel Destination 1.1.1.1	Tunnel Destination 2.2.2.2
Tunnel mode ipv6ip	Tunnel mode ipv6ip

9.2.3.2. TUNELES AUTOMATICOS

Los túneles automáticos al contrario de los manuales, no es necesario configurar en forma estática en ambos extremos sino que se establecen una

configuración mínima. Los túneles más conocidos y que trataremos son los siguientes:

A. TUNEL 6to4

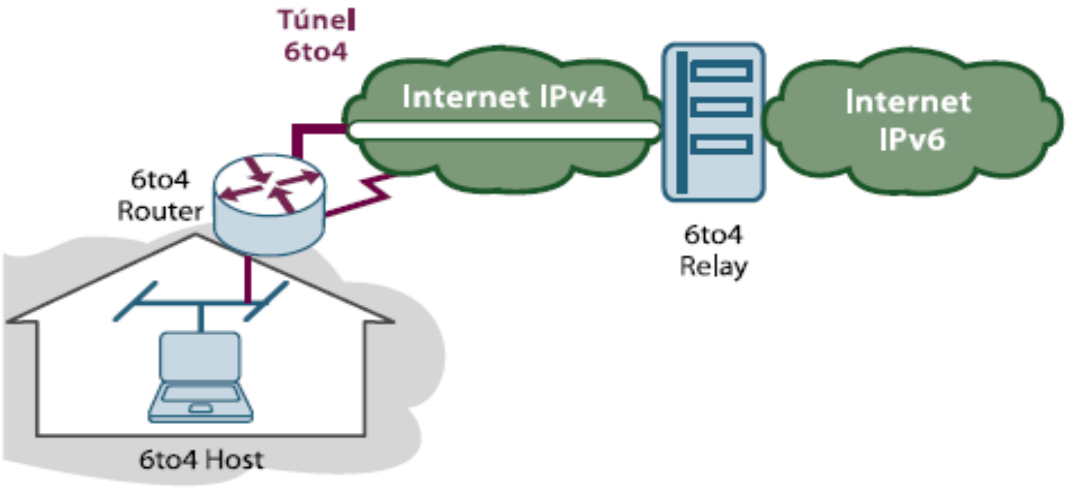

Figura 13: Túnel 6to4

B. TUNEL TEREDO

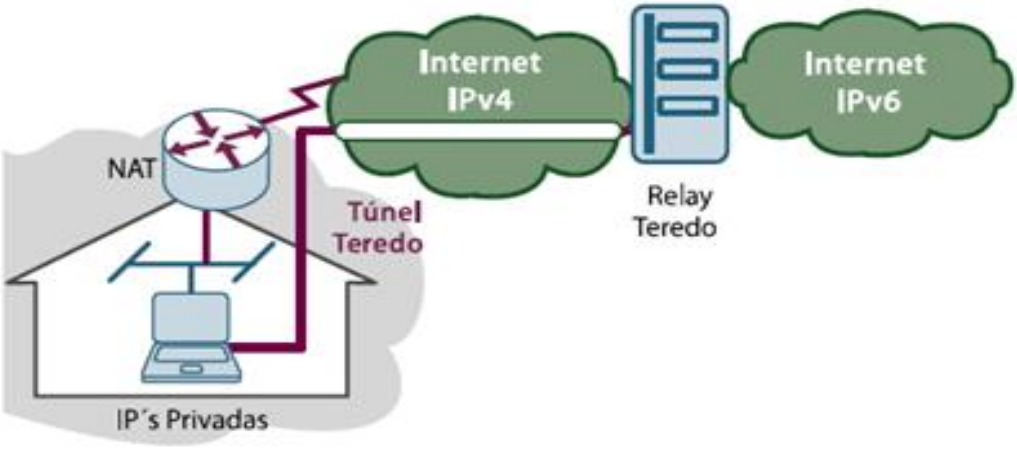

Figura 14: Túnel Teredo

Para ver y entender mejor la configuración de la router es necesario ver video ***Simulación Paquet Tracer Red IPv6 – Dual Stack*** *(Anexo de Documento Inteconectividad 6).*

Cabe resaltar que lo anterior es una guía de instalación básica de instalación e implementación de protocolo Ipv6 por tanto no se garantiza la confiabilidad y seguridad de la misma ya que pueden debido a diversos factores que no se pueda desarrollar de una manera adecuada la adopción del protocolo. Se sugiere que la implementación se realice en compañía de profesionales en redes para asegurar la viabilidad y fiabilidad de la Red.

10. CONCLUSIONES

Después de conocer que es IPv6 conceptos y especificaciones, se puede determinar que la transición hacia dicho protocolo es un hecho, ya que está pensado para mejorar la conexión a internet y la transmisión de datos, lo que se muestra como un paso evolutivo tanto para las redes como para el software y el hardware. Ya que la implementación requiere de infraestructuras que de adapten, así como los dispositivos y las aplicaciones. Por ende es un paso necesario y con el tiempo será obligatorio, para usuarios y proveedores de internet.

El estudio que nos propusimos realizar fue para verificar si la Universidad Minuto de Dios (Regional Soacha), está preparada para comenzar a trabajar bajo este nuevo protocolo.

Para realizar pruebas solicitamos un laboratorio que cuenta con la siguiente infraestructuras 16 computadores en Red LAN todas la conexiones van al rack, están organizadas en patch panel y estas a su vez se conectan al switch y este a un router (cisco Series 1800) que es el que da la conexión a internet (proveedor de servicios ETB) el router también va conectado a un servidor que sirve de proxy pero este no tiene sistema operativo es controlado por otro servidor remotamente.

Tomando como referencia esta infraestructura se puede definir que la universidad si está preparada para comenzar a implementar el protocolo IPv6, ya que el sistema operativo de los equipos es Windows Xp y solo se necesita subir el servicio. Para el router se debe adquirir el IOS Cisco (sistema operativo para routers), ya que es necesario para poder configurar el túnel para hacer el enlace a la red externa o internet ya que los proveedores actualmente no están trabajando este protocolo o no de forma abierta.

Es de aclarar que dichas pruebas no se realizaron en las instalaciones de la universidad porque no se consiguieron los permisos por el tipo de administración que tiene el servidor.

Sin embargo de acuerdo a la infraestructura si es posible comenzar a trabajar en dicho protocolo, por lo antes mencionado (La infraestructura es la adecuada), además de ser un paso de evolución hablando de conectividad e internet.

Después de realizar el estudio para conocer que es IPv6 queda al descubierto que desde el año 2.000 los dispositivos y los sistemas operativos soportan este protocolo, por lo que una de las deficiencias al tratar este tema no es precisamente la infraestructura sino, que no hay personas que tengan conocimiento de este protocolo. Por lo tanto se hace necesario conocer ¿Qué es?, ¿Cómo funciona? , las ventajas y desventajas que tenemos para poder dar un paso adelante en cuento a la conectividad.

De acuerdo con lo que se planteó, este estudio se enfocó en la parte técnica para la implementación del protocolo IPv6, si hablamos de los beneficios económicos que se tendrán a largo plazo, es de aclarar que como todo avance tecnológico los beneficios que ofrece son de evolución, y en este caso es mayor velocidad, más espacio, mejor conectividad entre otros, no podemos decir que se van a reducir o generar más costos pero si habrá un servicio de mejor calidad, que finalmente es lo que se busca cuando se actualizan dispositivos, aplicaciones y como en este caso los protocolos, todo se hace para que el usuario final puede ejecutar sus actividades con mayor eficiencia y eficacia, y la transición será transparente para este último.

Este protocolo muestra su más grande deficiencia de implementación en el desconocimiento del tema, en Latinoamérica solo algunos países como Argentina y México han comenzado a tratar este tema con importancia, en Colombia hasta el julio de 2011 se empezaron a tomar medidas al respecto, por lo que difundir este tema entre los estudiantes y tenerlo en cuenta en las

clases, contribuiría para que el avance en la implementación de este protocolo se acelere.

11. BIBLIOGRAFÍA

IVAN TURMO, Al actual Internet le quedan dos años de vida. [En línea]

< http://www.swissinfo.ch/spa/ciencia_tecnologia> [Citado 15 de marzo de 2010]

JOEL BARRIOS DUEÑAS, Introducción a IP versión 4. [En línea]

<http://www.alcancelibre.org/staticpages/index.php > [Citado 04 de octubre de 2009]

GOBIERNO DE ESPAÑA – MINISTERIO DE INDUSTRIA, TURISMO Y COMERCIO, IPv6 Protocolo de Internet Versión 6. [En línea] <http://www.ipv6.es/es-ES>

MONTSERRAT COLLADO RODRIGUEZ, IPv6 el cercano gran desconocido. [En línea] <http://www.pctrucos.com>

ORACLE CORPORATION AND/OR ITS AFFILIATES, Descripción general del protocolo ND de IPv6. . [En línea] <http://docs.oracle.com > [Citado en 2010].

FUNDACIÓN WINKIMEDIA, IPv6. [En línea] <http://es.wikipedia.org/wiki/IPv6> [Citado en 2011].

CICLEO, Guillermo. IPv6 Para Todos: Guía de Uso y Aplicación para Diversos Entornos: Internet Society, Capitulo Argentina 1ª Edición Octubre de 2009, ISBN 978-897-25392-1-4.

12. GLOSARIO

ARP: Protocolo de resolución de direcciones (Address Resolution Protocol). Es un protocolo de nivel de red, responsable de encontrar la dirección hardware (Ethernet MAC) que corresponde a una determinada dirección IP.

CIDR: Enrutamiento entre dominios sin Clases (Classless Inter Domain Routing) se introdujo en 1993 por IETF y representa la última mejora en el modo como se interpretan las direcciones IP. Su introducción permitió una mayor flexibilidad al dividir rangos de direcciones IP en redes separadas

DNS: Sistema de Nombres de Dominio (Domain Name System o DNS) es un sistema de nomenclatura jerárquica para computadoras, servicios o cualquier recurso conectado a Internet o a una red privada.

FLOW LABEL: Etiqueta de flujo contiene un número único escogido por la fuente que intenta facilitar el trabajo de los routers y permitir la implementación de funciones de calidad de servicio como RSVP (Resource Reservation setup Protocol [Protocolo de reserva de recursos]). Este indicador puede considerarse como un marcador de un contexto en el router. El router puede entonces llevar a cabo procesamientos particulares: escoger una ruta, procesar información en tiempo real.

FRAGMENTACIÓN: Denota la distribución de un paquete IP entre varios bloques de datos, si su tamaño sobrepasa la unidad máxima de transferencia (MTU) del canal.

IANA: La Internet Assigned Numbers Authority, es la entidad que supervisa la asignación global de direcciones IP, sistemas autónomos, servidores raíz de nombres de dominio DNS y otros recursos relativos a los protocolos de Internet. Actualmente es un departamento operado por ICANN.

ICANN: La Corporación de Internet para la Asignación de Nombres y Números es una organización sin fines de lucro creada el 18 de septiembre de 1998 con

objeto de encargarse de cierto número de tareas realizadas con anterioridad a esa fecha por otra organización, la IANA. Su sede radica en California y está sujeta a las leyes de dicho Estado

ICMPv6: Protocolo de Mensajes de Control de Internet Version 6 (ICMPv6 o ICMP para IPv6) es una nueva versión de ICMP y es una parte importante de la arquitectura IPv6 que debe estar completamente soportada por todas las implementaciones y nodos IPv6. ICMPv6 combina funciones que anteriormente estaban subdivididas en varias partes de diferentes protocolos tales como ICMP, IGMP o ARP y además introduce algunas simplificaciones eliminando tipos de mensajes obsoletos que estaban en desuso actualmente.

IETF: Grupo Especial sobre Ingeniería de Internet (Internet Engineering Task Force (IETF)), es una organización internacional abierta de normalización, que tiene como objetivos el contribuir a la ingeniería de Internet, actuando en diversas áreas, como transporte, encaminamiento, seguridad. Fue creada en EE. UU. en 1986. La IETF es mundialmente conocida por ser la entidad que regula las propuestas y los estándares de Internet, conocidos como RFC.

ISP: Un proveedor de servicios de Internet (o ISP, Internet Service Provider) es una empresa que brinda conexión a Internet a sus clientes. Un ISP conecta a sus usuarios a Internet a través de diferentes tecnologías como DSL, Cable módem, GSM, Dial-up, Wifi, entre otros. Muchos ISP también ofrecen servicios relacionados con Internet, como el correo electrónico, alojamiento web, registro de dominios, servidores de noticias, etc.

MTU: La unidad máxima de transferencia (Maximum Transfer Unit - MTU) es un término de redes de computadoras que expresa el tamaño en bytes de la unidad de datos más grande que puede enviarse usando un protocolo de comunicaciones.

NAT: (Network Address Translation - Traducción de Dirección de Red) es un mecanismo utilizado por enrutadores IP para intercambiar paquetes entre dos redes que se asignan mutuamente direcciones incompatibles. Consiste en convertir en tiempo real las direcciones utilizadas en los paquetes

transportados. También es necesario editar los paquetes para permitir la operación de protocolos que incluyen información de direcciones dentro de la conversación del protocolo.

NEIGHBOR DISCOVERY: Es un protocolo de IPv6, y es equivalente al protocolo Address Resolution Protocol (ARP) en IPv4, aunque también incorpora las funcionalidades de otros protocolos de esta versión.

Consiste en un mecanismo con el cual un nodo que se acaba de incorporar a una red, descubre la presencia de otros nodos en el mismo enlace, además de ver sus direcciones IP. Este protocolo también se ocupa de mantener limpios los caches donde se almacena la información relativa al contexto de la red a la que está conectado un nodo. Así cuando una ruta hacia un cierto nodo falla el enrutador correspondiente buscara rutas alternativas. Emplea los mensajes de ICMPv6, y es la base para permitir el mecanismo de autoconfiguración en IPv6.

P2P: Una red Peer-to-Peer o red de pares o red entre iguales o red entre pares o red punto a punto (P2P, por sus siglas en inglés) es una red de computadoras en la que todos o algunos aspectos funcionan sin clientes ni servidores fijos, sino una serie de nodos que se comportan como iguales entre sí. Es decir, actúan simultáneamente como clientes y servidores respecto a los demás nodos de la red. Las redes P2P permiten el intercambio directo de información, en cualquier formato, entre los ordenadores interconectados.

IPsec: Internet Protocol security es un conjunto de protocolos cuya función es asegurar las comunicaciones sobre el Protocolo de Internet (IP) autenticando y/o cifrando cada paquete IP en un flujo de datos. IPsec también incluye protocolos para el establecimiento de claves de cifrado.

QoS: o Calidad de Servicio (Quality of Service, en inglés) son las tecnologías que garantizan la transmisión de cierta cantidad de información en un tiempo dado (throughput). Calidad de servicio es la capacidad de dar un buen servicio. Es especialmente importante para ciertas aplicaciones tales como la transmisión de vídeo o voz.

RFC: Las Request for Comments ("Petición De Comentarios" en español) son una serie de notas sobre Internet, y sobre sistemas que se conectan a internet, que comenzaron a publicarse en 1969.[1] Se abrevian como RFC.

Cada una de ellas individualmente es un documento cuyo contenido es una propuesta oficial para un nuevo protocolo de la red Internet (originalmente de ARPANET), que se explica con todo detalle para que en caso de ser aceptado pueda ser implementado sin ambigüedades.

RIR: Un Registro Regional de Internet o Regional Internet Registry (RIR) es una organización que supervisa la asignación y el registro de recursos de números de Internet dentro de una región particular del mundo.

TCP: Protocolo de Control de Transmisión (Transmission Control Protocol) o TCP, es uno de los protocolos fundamentales en Internet. Fue creado entre los años 1973 y 1974 por Vint Cerf y Robert Kahn. El protocolo garantiza que los datos serán entregados en su destino sin errores y en el mismo orden en que se transmitieron. También proporciona un mecanismo para distinguir distintas aplicaciones dentro de una misma máquina, a través del concepto de puerto.

UDP: El protocolo UDP (Protocolo de datagrama de usuario) es un protocolo no orientado a conexión de la capa de transporte del modelo TCP/IP. Este protocolo es muy simple ya que no proporciona detección de errores (no es un protocolo orientado a conexión).

WHOIS: es una Base de Datos de Internet que contiene información acerca de una IP, de un Dominio o de una organización; sin embargo WHOIS es tambien una herramienta, que es la que se utiliza para consultar esta Base de Datos.

Una Base de Datos de Whois contiene información acerca de los nombres de dominio y de las personas que son el contacto técnico y el administrativo, la fecha de expiración del dominio así como el registrar (compañía que se dedica a registrar nombres de Dominio).