Resumen

Debido al gran éxito de Internet hasta nuestros tiempos, de los avances y cantidad de dispositivos móviles existentes con servicio de Internet y de las aplicaciones que funcionan óptimamente con direcciones públicas, el espacio de direccionamiento público de IPv4 ya no es suficiente para estas necesidades, llegando a ser actualmente un recurso escaso en algunos continentes.

Es de esta manera que se desarrolló hace algunos años el protocolo IPv6 pensando no solo en las aplicaciones y dispositivos actuales, sino pensando en el futuro, pero que hasta la fecha no ha llegado a ser tan popular debido al uso sobretodo de NAT y CIDR en redes empresariales.

La propuesta de este proyecto de tesis es el diseño e implementación del protocolo IPv6 dentro de la red de la Universidad de Cuenca, tanto para enrutamiento como para entrega de servicios, y su uso en Internet Comercial así como hacia redes Académicas.

Abstract

Because of the successful use of Internet in this time, the number and the new technology of mobile devices using the Internet service, and the applications that work better with public IPs, the public IPv4 address space is not big enough for these needs becoming a limited resource in some continents.

In this context, few years ago IPv6 protocol was developed, not only thinking in current applications and devices but thinking in future needs. Unfortunately, it has not become popular around the world because of the use of NAT and CIDR into enterprise networking.

The purpose of this project is to design and implement the IPv6 protocol inside the network of the University of Cuenca to get both IPv6 and IPv4 work with the routing network and institutional servers using Commercial Internet and Academic networks.

UNIVERSIDAD DE CUENCA

FACULTAD DE INGENIERIA

MAESTRIA EN TELEMATICA

Diseño e implementación de IPv6 nativo en la Universidad de Cuenca para su uso en la redCLARA

PROYECTO DE GRADUACIÓN PREVIO A LA OBTENCIÓN DEL GRADO DE MAGISTER EN TELEMÁTICA

Autor:
Ing. Claudio Chacón A.

Director de Tesis:
Ing. Diego Ponce PhD.

Septiembre 2011

Índice

EL CONTENIDO DE ESTA TESIS ES DE ABSOLUTA RESPONSABILIDAD DEL AUTOR

1. Antecedentes

IANA, el organismo internacional de Internet para la asignación de direcciones anunció el agotamiento de direcciones de IPv4 ya hace algún tiempo, e instó a los usuarios a cambiar a la versión más reciente de IP en su versión 6, conocida como Internet de nueva generación.

Por otra parte el estándar IP de nueva generación, publicó su RFC de recomendaciones para el protocolo IP de nueva generación en enero de 1995, y que posteriormente su versión final salió al mercado en diciembre de 1998, desde esta fecha no ha conseguido en estos 13 años un despliegue realmente masivo, pese a los esfuerzos de desarrollo y convergencia de los últimos años.

Las mejoras tecnológicas en telecomunicaciones tales como la masificación de la fibra óptica y los medios inalámbricos, así como el descenso de los precios de dispositivos de conexión y el aumento del rendimiento de microchips, han hecho que sea factible mejorar e implementar los protocolos reduciendo los algoritmos de corrección de errores a favor de tramas de datos más largas.

Actualmente Internet está dominado por IP versión 4, pero este protocolo que ya tiene algunas décadas desde que se creó, al haber tenido un gran éxito y un uso masivo ha hecho que actualmente llegue a tener ciertas deficiencias por las necesidades de nuevos servicios y aplicaciones actuales. Estas deficiencias son superadas ya en su última versión IPv6. Entre algunas de estas mejoras están: mayor capacidad de direccionamiento, una cabecera IP mas simple, un mejor soporte para extensiones y opciones del protocolo, capacidad de etiquetar de flujos de datos, capacidad de usar autenticación y privacidad en la comunicación incluido nativamente en el protocolo.

La versión más usada de IP, llamada IPv4 ya cumple 30 años de existencia, este protocolo tiene algunas deficiencias que no fueron consideradas al momento de diseñarlo, dado que en dicha época la red donde se usaba era pequeña en comparación a la red actual.

Con la llegada de Internet y su uso masivo IPv4 empezó a tener problemas respecto al número de direcciones IP disponibles, el cual hasta la fecha se ha podido mantener gracias al uso de técnicas especiales. Estas técnicas son: el uso de NAT, el cual solucionó la

IANA: Internet Assigned Numbers Authority

IPv4: RFC-791

IPv6: RFC 2460

IPv4: www.ietf.org/rfc/rfc791.txt

NAT: Network Address Translation www.ietf.org/rfc/rfc1918.txt

falta de direcciones públicas. Otra técnica utilizada es el subnetting que permitió un menor desperdicio en el uso de direcciones públicas.

Estas técnicas hicieron que hasta nuestros tiempos IPv4 siga siendo soportado, pero el número de direcciones IP disponibles está llegando a su fin, dado que el uso de la fibra óptica así como las redes inalámbricas y dispositivos móviles va en aumento, tomando en cuenta también que el precio de los dispositivos electrónicos es cada vez menor, hace que día a día exista más dispositivos, mayores servicios y aplicaciones en la nube para dichos dispositivos, lo cual requiere mayor demanda de direcciones IPs públicas para su mejor funcionamiento.

La Universidad de Cuenca ya lleva usando el protocolo IPv4 mas de 15 años, y actualmente el 100 % de aplicaciones existentes así como los dispositivos activos y redes departamentales utilizan este protocolo. Es por ello que normalmente al diseñar nuevos sistemas implícitamente se diseñan usando IPv4, olvidándose de que existe IPv6.

La Universidad de Cuenca tiene registrado en LACNIC solamente un rango de direcciones IPv4, pero no tiene un rango IPv6 ni un Sistema Autónomo por lo cual para este proyecto se obtuvo un prefijo /48 de parte de CEDIA e inicialmente también un prefijo /48 de un proveedor Comercial Internacional de IPv6 para conexión por medio de un túnel, a lo largo del desarrollo de este proyecto se indicará las ventajas y desventajas del uso de uno u otro rango, peerings y manejo de sistemas autónomos.

La Universidad de Cuenca, forma parte de CEDIA, toma el servicio de Internet Comercial del único proveedor que actualmente tiene esta organización, y que en diciembre 2010 empezó a dar IPv6 comercial nativo a las universidades que lo solicitaban.

IPv6 será el protocolo usado en todo el mundo, por ahora IPv4 tiene el mayor tráfico en Internet (IPv4 representa el 99.98 % del tráfico total según estadísticas del World IPv6 Day) pese a las grandes ventajas que IPv6 tiene.

Tomando en cuenta los aspectos anteriormente citados, la falta de un sistema autónomo propio de la Universidad, hace que para tener IPv6 comercial e IPv6 en la red académica hacia redCLARA al mismo tiempo, sea necesario usar ciertas técnicas para tener Multihoming en IPv6.

Subnetting: www.ietf.org/rfc/rfc950.txt

LACNIC: Latin American and Caribbean Internet Addresses Registry, www.lanic.net

AS: Sistema Autónomo, RFC1930

peering: intercambio de tráfico entre sistemas autónomos

World IPv6 Day: 8 de Junio del 2011 se levanto por 24 horas la pila IPv6 en los portales más concurridos a nivel mundial. www.worldipv6day.org

1.1. Realidad Mundial

Una de las formas de medir la popularidad de IPv6 es por medio de las asignaciones de las redes alrededor del mundo. En cada región se tiene diferentes RIRs, estos son:

- *American Registry for Internet Numbers* (ARIN): para Norte América.
- *Réseaux IP Europens Network Coordination Centre* (RIPE NCC): para Europa, medio oriente, y Asia central.
- *Asia-Pacific Network Information Centre* (APNIC): para Asia y la región del Pacífico.
- *Latin American and Caribbean Internet Addresses* (LACNIC): Para latino América y el Caribe.
- *African Network Information Centre* (AfriNIC): para África.

De los cuales podemos obtener el información del número de redes IPv6 /32 asignadas a nivel global, esto se puede apreciar en la figura 1:

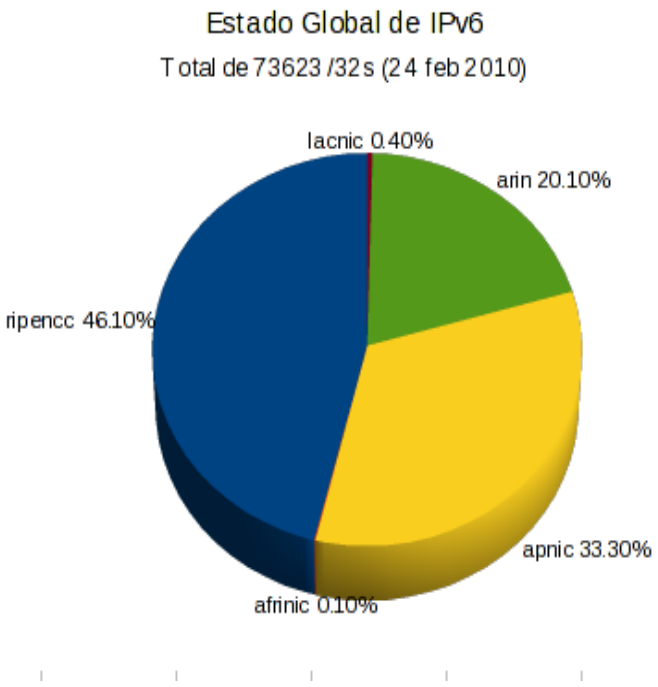

Figura 1: redes IPv6 a nivel global

RIR: Regional Internet Registry

IPv6 tiene 128 bits, un /32 es asignado para redes de ISP, no para redes finales, normalmente un /32 es subdividido en varias /48.

Del gráfico 1 podemos observar que Latino América apenas tiene el 0.4 % de asignaciones IPv6 con prefijo /32 de todo el planeta, es decir los requerimientos de parte de los países Latinos hacia este protocolo son mínimos.

Dentro de cada región también existen redes de investigación y redes académicas que son las que están realizando esfuerzos para llegar a una gran cantidad de usuarios con este protocolo. Alrededor del mundo tenemos a varias organizaciones entre algunas de ellas tenemos a DANTE en Europa, NLR e Internet2 en EEUU, APAN en Asia, redCLARA en Latinoamérica y el Caribe.

Pero ya a estas alturas no solamente son las redes académicas las que trabajan en ello, también las redes comerciales realizan ya implementaciones en algunos lugares a nivel mundial, e incluso en muchos países ya algunos ISPs trabajan sobre IPv6 nativo, entre estos países tenemos:

- Australia
- China
- Alemania
- Francia
- India
- Inglaterra
- Estados Unidos

1.2. Realidad Latinoamericana

Dentro de Latinoamérica y el Caribe LACNIC es la entidad quien otorga direcciones IPv6, esta tiene el registro de asignaciones de rangos /32 para los distintos países, de esta entidad obtenemos la información plasmada en el gráfico 2:

Hay que notar que no todo lo asignado está siendo usado, esto se puede comprobar verificando si existe rutas que van hacia cada una de las redes IPv6 de asignadas, para

DANTE: Delivery of Advanced Network Technology to Europe
NLR: National Lambda Rail
APAN: Asia-Pacific Advanced Network
redCLARA: Cooperación Latino Americana de Redes Avanzadas
ISP: Internet Service Provider
LACNIC: Latin American and Caribbean Internet Addresses Registry

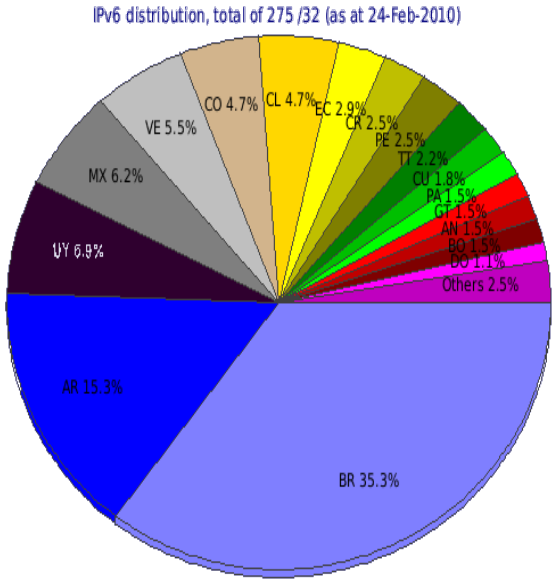

Figura 2: redes IPv6 a nivel de países latinoamericanos

ello LACNIC ofrece información de donde se encuentra el número de locaciones y asignaciones dadas por LACNIC vs el número de locaciones que se encuentran ruteadas, o en funcionamiento. Del gráfico 3 observamos que menos de la mitad de redes IPv6 de Latino América se encuentran activas (dato tomado a diciembre 2010).

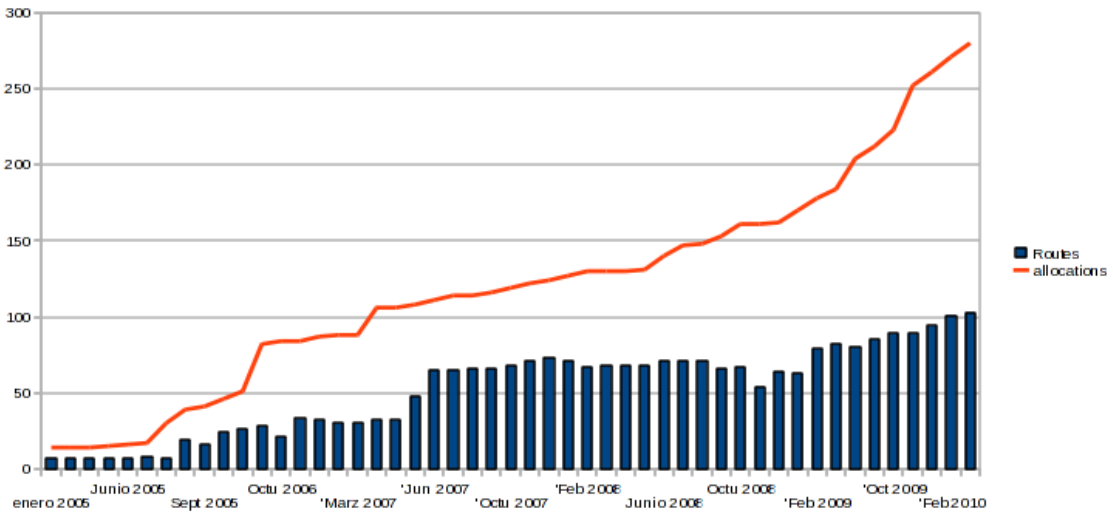

Figura 3: Número de redes IPv6 asignadas vs número de direcciones IPv6 ruteadas

1.3. Realidad Ecuatoriana

LACNIC no solo brinda información general de Latinoamérica, sino también de cada uno de los países, en el caso de Ecuador también tenemos redes IPv6 asignadas por LACNIC. En el gráfico 4 observamos el número de redes asignadas vs el número de redes que están activas (aquellas que aparecen en las tablas de ruteo).

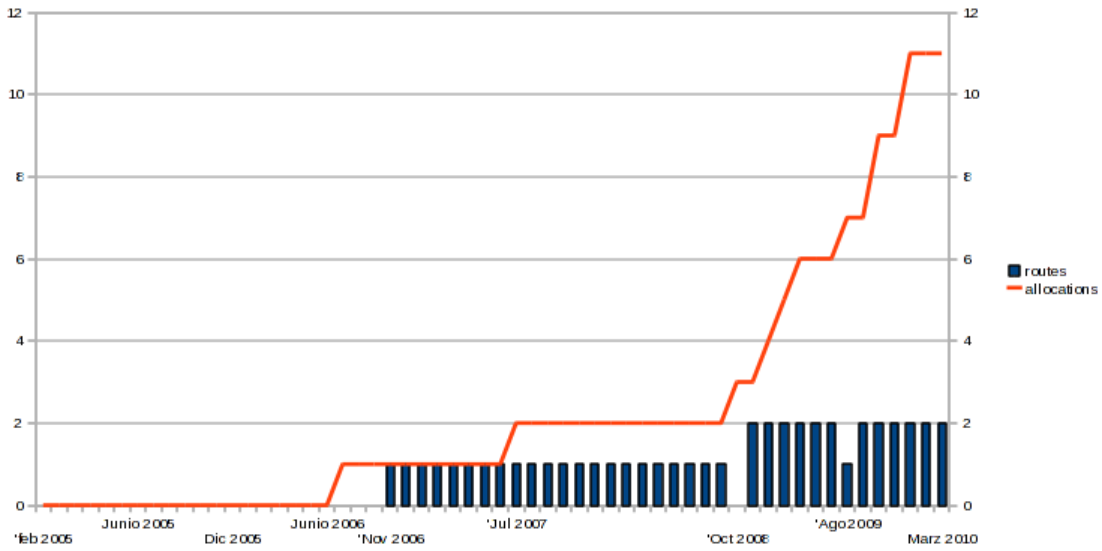

Figura 4: IPv6, realidad Ecuatoriana

De donde vemos que existen 11 redes IPv6 en Ecuador, de las cuales solamente 2 se encuentran activas, una de ellas es la red académica CEDIA la cual es la NREN oficial de Ecuador que tiene asignado por LACNIC una red IPv6 prefijo /32, y a su vez les otorga una red IPv6 prefijo /48 a cada uno de los miembros (Universidades o centros de Investigación). Es esta red académica quien provee de un prefijo IPv6 /48 a la Universidad de Cuenca.

1.4. Realidad Universitaria

La Universidad de Cuenca al formar parte de CEDIA, ya tiene asignada una red IPv6 prefijo/48 que no se encontraba en uso, haciendo que la Universidad no pueda comunicarse con aplicaciones y servicios de IPv6 que ya están dando servicio alrededor del

figura 4, datos estadísticos tomados de LACNIC en Julio 2010

CEDIA: Consorcio Ecuatoriano para el Desarrollo de Internet Avanzado

NREN: National Research and Education Network

mundo, como por ejemplo el software ISABEL PLAZA que en CUDI ya se está usando nativamente sobre IPv6 para ciertos eventos de videoconferencia, también existen servicios comerciales que ya se encuentran en IPv6 como buscadores y servicios varios, entre ellos Google ha sido uno de los pioneros en colocar casi en su totalidad su plataforma en IPv6, pero que solamente está disponible para redes con una conexión IPv6 estable y redundante.

ISABEL PLAZA: Software para Video Conferencia y Colaboración que funciona bajo software GNU/Linux

CUDI: Coorporación Universitaria para el Desarrollo de Internet, NREN oficial de México

Google over IPv6: Programa mediante el cual los administradores de redes pueden suscribir sus redes IPv6 para obtener servicios sobre este protocolo a la mayoría de portales de Google

2. Estado del Arte

Al iniciar este proyecto de tesis la red de la Universidad de Cuenca se encontraba funcionando totalmente en IPv4, con sus dispositivos activos y clientes funcionando solamente en dicho protocolo, la seguridad de las redes en IPv4 se la realiza en el firewall, abriendo en la red DMZ solamente los puertos necesarios, y se consigue salida hacia afuera usando NAT. Para el caso de la red del personal así como de los estudiantes, ellos salen por medio de PAT, con permiso total hacia Internet con excepción del puerto smtp.

La red universitaria se encuentra formada casi en su mayoría de dispositivos de red activos de marca CISCO, los cuales permiten hacer el cambio del su IOS. De los equipos existentes no todos tienen un IOS que tenga el protocolo IPv6, así como las extensiones o aplicaciones necesarias para este proyecto. También existe en la red ciertos lugares que se conectan a la red usando routers inalámbricos, los cuales no permiten una actualización de firmware, por lo que no es posible llegar con IPv6 a estos sitios.

Para la seguridad de transmisión de información entre servidores, esta se la realiza exclusivamente con encriptación usando la capa de aplicación.

NAT: Network Address Translation
PAT: Port Address Translation
SMTP: Simple Mail Transfer Protocol
IOS: Internetwork Operating System

3. Justificación del proyecto

La disponibilidad de redes IPv4 están agotándose, en Febrero del 2011 la IANA agotó su rango de direcciones IPv4 disponibles para la asignación a RIRs, y en los siguientes meses se espera el agotamiento de direcciones dentro de los RIRs con más demanda, por lo cual el único protocolo que podrá ser asignado en el futuro será rangos de direcciones IPv6, y las instituciones que ya lo manejen y que tengan una red IPv6 en funcionamiento, así como aplicaciones ya trabajando en este protocolo tendrán una ventaja competitiva. En el futuro próximo el tener una red IPv6 dejará de ser una ventaja y se convertirá en un requisito para poder competir en el mercado.

Con la realización de este proyecto de tesis se logrará tener el protocolo IPv6 implementado en la mayor parte de la Universidad de Cuenca y en sus servidores, de esta manera poder continuar con los avances tecnológicos que nos brinda este protocolo.

3.1. Necesidades a ser satisfechas

Se tiene la necesidad urgente de tener una red IPv6 universitaria funcionando nativamente, y de producción en IPv6 para poder empezar a desarrollar proyectos sobre este nuevo protocolo, además de la capacidad de transmitir información de manera segura usando el mismo.

Este proyecto plantea llegar con el protocolo IPv6 a cada una de las facultades, donde los ordenadores que cumplan con los requerimientos necesarios para conectarse a esta red lo realicen, así como también se espera llegar a los desarrolladores para que en base esta red, en un futuro se empiece a programar tomando en cuenta la existencia de este protocolo, así como también se espera llegar a los administradores de la red, para que se inicie el uso en producción del protocolo IPSec aplicando cuando sea necesario este protocolo de seguridad en IPv6.

Entre los beneficios que se tendrá al finalizar el proyecto será que los usuarios disfrutarán de navegación a redes IPv6, la cual será transparente, y al terminar este proyecto la Universidad estará entre los pioneros que tienen este protocolo en ya en producción en Latinoamérica (aunque de un uso más común en otros continentes y países de primer mundo), y permitirá poder implementar nuevos programas sobre este protocolo, los cuales podrán ser publicados de una manera transparente hacia Internet comercial así como también hacia redes académicas.

Con respecto al Internet comercial, el cual también es muy importante, dado que

existe ya un gran número de portales comerciales que están usando IPv6, se realizará un túnel que permita usar servicios comerciales, y posteriormente ruteo nativo. Este ruteo será transparente para los usuarios finales, en su comunicación a Internet comercial y redes académicas.

4. Objetivos

4.1. Objetivos Generales

El objetivo General de este proyecto es llegar a tener una red IPv6 en producción así como en sus servidores más importantes, para su uso masivo en la Universidad de Cuenca.

4.2. Objetivos Específicos

Para poder llegar a tener una solución de IPv6 dentro de la Universidad, se plantea realizar las siguientes actividades:

- Diseño e Implementación de una red IPv6, en los dispositivos activos de la Universidad, tanto de frontera, así como internos, en cada uno de los campus y facultades.
- Diseño e implementación de una red de servidores Universitarios que utilizan software FLOSS: DNS, correo, y portal web.
- Pruebas en la red con la extensión nativa de seguridad IPsec.

FLOSS: Free/Libre/Open-Source Software

5. Investigación técnica

5.1. Historia

Para poder comprender el porqué se está tratando de adoptar este nuevo protocolo, es necesario conocer como iniciaron sus predecesores, para ello revisaremos el año 1966, donde el Departamento de Defensa(DoD) y el gobierno de los Estados Unidos crea ARPA, cuyo objetivo principal era conectar diferentes computadores de las instalaciones militares y centros de investigación, pero que esta red pueda trabajar independiente de las fallas que pueda existir, es decir, si una parte de la red dejaba de funcionar, todo lo demás debía continuar su funcionamiento normalmente, a esta red se la llamo ARPANET, la cual tenía varios protocolos, donde el más usado era el NCP, esta red inicialmente tenía 4 nodos, 3 nodos de universidades Norteamericanas y 1 nodo en el centro de investigación, y al tener mucho éxito, esta red fue creciendo hasta que en 1983 llego a tener más de 500 hosts conectados, ya para aquella época se trabajaba en un protocolo estándar que podía ser usado, este protocolo fue creado en septiembre de 1981 y se lo llamo IP, posteriormente se decidió en 1983 que el estándar TCP/IP sería el protocolo a usar en la red.

Para aquella época este protocolo llamado IPv4 fue lo mejor que existía en ese momento, pero no tomaron en cuenta el crecimiento que se venía en años posteriores, y el problema que del agotamiento de las direcciones IP así como el enrutamiento que esto llevaría.

Inicialmente este protocolo IPv4 creado con el RFC791 se enfatizaba en el uso de clases A, B, C, con los prefijos /8 /16 y /24 respectivamente, e inicialmente la única política de distribución de direcciones IP era por estas 3 clases existentes. En aquella época algunas instituciones como HP, MIT, Apple, GE, DEC, At&T, DoD obtuvieron prefijos /8 para sus redes, a parte que las clases C eran muy pequeñas para algunas redes (ya que solo tenían para 254 hosts por cada subred), por lo que muchas organizaciones solicitaban clases B, llegando en cambio a ser demasiado espacio para lo requerido teniéndose un desperdicio grande en el en el direccionamiento. Todos estos parámetros y políticas hizo que la red sea mal distribuida, y así empezaron los problemas.

Del total de rangos /8 existentes para IPv4 que son 256, podemos dividir en dos tipos

DoD: Department of Defense

Adanced Research Projects Agency

NCP: Network Control Protocol

IP: RFC791 o conocido generalmente como IPv4 generado en septiembre de 1981

TCP/IP: Transmission Control Protocol / Internet Protocol

de bloques, los bloques reservados según el RFC 5735 los cuales equivalen a 35,078 /8 (compuesto de la siguiente manera: 16 bloques /8 reservados para multicast, 16 bloques /8 reservados para uso futuro no especificado, un bloque /8 usado para identificación local, un bloque /8 usado como loopback, un bloque /8 usado para uso privado, y bloques adicionales usados para usos varios) y lo asignado a las diferentes RIRs, es decir 220,922 bloques /8. Lo cual es mostrado gráficamente en la figura 5.

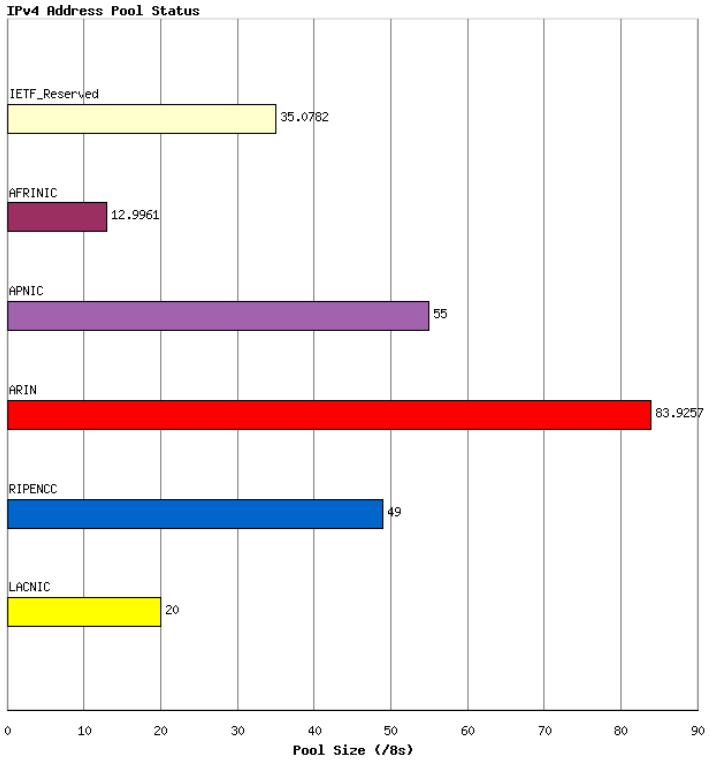

Figura 5: Asignación de rangos /8 de IPv4 a los RIRs

Desde que la red inició, el crecimiento de Internet fue muy rápido, esta información podemos tomarla del RFC1296 el cual fue publicado en 1992, y dio mucha información acerca del crecimiento de Internet desde 1981, que hizo pensar en aquellos años acerca de un posible fin de las direcciones IP. Esta información se encuentra en la figura 6.

Ya con estas cifras muy alarmantes, se buscó soluciones a ello, y la IETF creó el proyecto ROAD el cual diseñó diferentes mecanismos para mejorar el uso de las direcciones

RFC1296: Internet Growth

IETF: Internet Engineering Task Force

ROAD: ROuting and ADdressing group

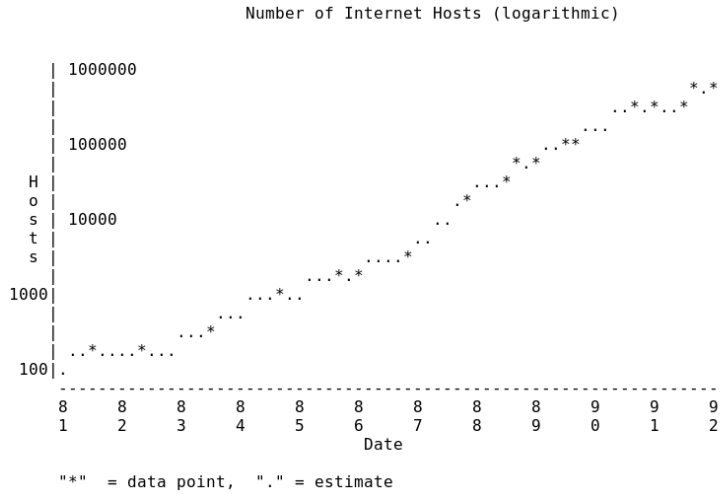

Figura 6: Crecimiento de Internet, rfc 1296

IPv4, entre estas mejoras creó CIDR, NAT y DHCP intentando solucionar el problema de la falta de direcciones IP.

Con todos estos nuevos estándares el crecimiento de las asignaciones de rangos IPv4 fue menor, pero aun seguía en crecimiento. Las ventajas era que CIDR ya permitía entregar prefijos de diferente tamaño, no solamente de /8, /16 y /24. Y en cambio NAT hacía que, una sola dirección IP pública pueda dar conexión a una red completa de IPv4 privado, DHCP permitía auto-configuración de los hosts cliente tan simplemente activando este protocolo. Varias técnicas que ayudaron a un aprovechamiento de las direcciones, pero que no anularían el fin de direcciones IP en el futuro.

Ya para esta época se vio la necesidad de un nuevo protocolo que sustituya a IPv4, a este nuevo protocolo lo llamaron IPng, el cual debía tomar en cuenta los siguientes aspectos (documentados en el RFC1550):

- Escalabilidad.
- Crecimiento en el tiempo.
- Transición del protocolo IPv4 al nuevo.
- Seguridad.

CIDR: Classless Inter-Domain Routing

NAT: Network Address Translation

DHCP: Dynamic Host Configuration Protocol

RFC1550: IP: Next Generation (IPng) White Paper Solicitation, publicado diciembre 1993

- Configuración administración y Operación.
- Host móbiles.
- Reserva de recursos.
- Políticas basadas en ruteo.
- Flexibilidad topológica.
- Aplicabilidad en el mercado.
- Servicios de datagramas.
- Accounting.
- Soporte a medios de comunicación ya existentes.
- Robustez y tolerancia a fallos.
- Tecnologías que puedan influenciar el uso de IPng
- Acciones de grupos de soporte para tomar decisiones acerca de este protocolo.

Luego de publicado estos requerimientos se empezó a trabajar en el nuevo protocolo desde varias comunidades de Internet, es así que se llego a tener un total de 21 documentos en respuesta a las solicitudes del RFC1550, entre algunos de ellos estaban: CNAT, IP Encaps, NimRod y Simple CLNP, posteriormente aparecieron PIP (The P Internet Protocol), SIP (The Simple Internet Protocol) y TP/IX, luego en una reunión de la IETF se incluyó el protocolo Simple CLNP en el nuevo TUBA (TCP and UDP with Bigger Address), y el protocolo IP Encaps fue incluido dentro de IPAE (IP Adress Encapsulation). Ya para el año de 1993 se unió IPAE con SIP y selo continuó nombrando SIP, posteriormente el grupo SIP se unió con PIP y formaron SIPP (Simple Internet Protocol Plus). Al mismo tiempo por otra parte se formaba el protocolo CATNIP(Common Architecture for the Internet).

La comisión de evaluación del RFC1550 de acuerdo a los requerimientos colocados en él, se enfocó en 3 protocolos, CATNIP, SIPP y TUBA, en donde se vio que SIPP y TUBA podrían trabajar en Internet, cada uno de ellos tenía sus problemas que podrían ser mejorados, a CATNIP se lo considero incompleto para lo requerido. Como resultado se consideró a una versión revisada de SIPP como el nuevo protocolo de IP.

Posteriormente la IANA asigno a IPng la versión de Internet número 6, y desde este punto se lo empezó a llamar IPv6, todo ello se encuentra documentado en el RFC1752 en enero del 1995.

En diciembre de 1995 se publica el RFC1883 que publicaba las especificaciones de IPv6, pero luego en el año 1998 es reemplazada por el RFC2460 llegando a ser ésta la especificación usada hasta el día de hoy.

5.2. Introducción

El nuevo protocolo IPv6 al ser relativamente nuevo en su implementación, sobretodo en Latinoamérica, existe limitada documentación y experimentación de los administradores de la red. La mayoría de información existente pertenece a los grupos de trabajo de IPv6 alrededor del mundo como los IPv6TF,, o de proyectos que apoyan iniciativas de IPv6 y de Instituciones que realizan capacitación de uso del mismo, como por ejemplo TERENA, CGI.br o 6Deploy que pertenece a Europa, pero realiza cursos de capacitación alrededor del mundo, al igual que LACNIC que da sus cursos en Latinoamérica y el Caribe.

Como parte importante de la investigación está la revisión de redes académicas similares en otros países (Ya que en Ecuador no existe hasta el momento, e incluso dentro de Latinoamérica es difícil encontrar), la forma de distribución de la red, y los estándares usados para las mismas, seguridad, ruteo, etc.

Para la investigación en el caso de la redes Nacionales, se tomo en cuenta las redes de RENATA y la red CUDI, ambas que ya han tenido experiencia ya algún tiempo con dicho protocolo. Este protocolo al estar aún en implementación globalmente, aún no existen buenas prácticas definidas para su implementación a diferencia de lo existente para IPv4 donde existe infinidad de información.

Entre la información obtenida de otras redes internacionales, se realizó una revisión del diseño de la red, la cual es de manera jerárquica, es decir estas redes inician de una red prefijo /32 propiedad de la NREN del país, en el caso de la red Académica Ecuatoriana sigue este mismo formato de organización, es decir inicia con una red IPv6

rfc1883: Internet Protocol, Version 6 (IPv6) Specification, versión original diciembre 1995

rfc2460: Internet Protocol, Version 6 (IPv6) Specification, versión modificada diciembre 1998

IPv6tf: IPv6 Task Force, son grupos de personas o entidades que se reúnen para trabajar en este protocolo

TERENA: Trans-European Research and Education Networking Association

CGI.br: Comitê Gestor da Internet no Brasil

RENATA: Red Nacional Académica de Tecnología Avanzada, Colombia

CUDI: Corporación Universitaria para el Desarrollo de Internet, México

NREN: National Research and Education Network

prefijo /32 de CEDIA, la cual es anunciada con este prefijo hacia redes internacionales, e internamente a cada universidad se la asigna una red más pequeña normalmente una prefijo /48. Se coloca también un ruteo iBGP entre ellas, en el caso de Ecuador este ruteo actualmente es ofrecido usando RIPng, y la el intercambio de prefijos de redes internacionales por medio de MBGP.

Con toda esta información existente, uno de los objetivos de este proyecto es llegar a la mayor cantidad de usuarios para iniciar su uso masivo, por lo que al finalizarlo, debe cumplir algunos requisitos, que son:

- El uso de este protocolo debe ser de fácil uso para el usuario final.
- Este protocolo debe coexistir con IPv4.
- El ruteo entre Internet Comercial y redes Académicas debe ser transparente al usuario.
- Aquellos usuarios que por dificultades en el Sistema Operativo no puedan usar IPv6, el servicio por medio de IPv4 debería continuar sin realizar ningún cambio.
- Aquellos usuarios que tengan posibilidad de tener un equipo con IPv4 e IPv6, podrán utilizar cualquiera de las 2 versiones para alcanzar su destino.

Para la realización de estos requerimientos por parte de los usuarios, este proyecto usó algunas técnicas como multihomed, Dual Stack, las cuales se van a ir definiendo a lo largo de este proyecto.

Con lo referente a los servidores, éstos deben dar servicio tanto en IPv4 como en IPv6 con la misma calidad de servicio, debe tener la posibilidad en el caso de correo electrónico que un usuario de IPv6 pueda por medio de este servidor enviar un correo a un usuario que está usando IPv4, igualmente debería poder comunicarse con otros servidores sean versión 4 o versión 6. Para ello otra vez se toma en cuenta el uso de Dual Stack y multiHomed para transparencia tanto a usuarios finales, como la comunicación con otros servidores.

Para la seguridad existen grandes diferencias respecto a IPv4, dado que IPv4 daba a los usuarios una falsa seguridad usando NAT o PAT con IPs privadas, ahora en IPv6 es necesario dar una seguridad diferente en el firewall, ya que todas las direcciones IPv6 de los clientes finales son direcciones globales, y pueden ser alcanzadas desde Internet.

MBGP: Multiprotocol Border Gateway Protocol

5.3. Componentes

Para la realización de este proyecto existe algunos componentes que deben trabajar con IPv6 para que el servicio sea eficiente, estos componentes necesarios se encuentran en la tabla 1:

Con estos componentes trabajando en conjunto ya se puede dar un servicio básico de IPv6, ya que luego hay que como en todo sistema nuevo, hay que ir realizando mejoras, pero siempre siguiendo el mismo diseño ya planteado en este proyecto.

5.4. Diferencias con IPv4

Hay que tomar en cuenta que se implementa una red IPv6 sobre una red IPv4 ya existente y en producción, es decir todos los componentes (routers, switchs, firewalls, servidores y usuarios finales) dejarán de tener solamente el protocolo IPv4,a tener DualStack, es decir ambos protocolos funcionando.

Al implementar este nuevo protocolo en la red Universitaria se debe tomar en cuenta ciertos aspectos como por ejemplo:

- Dado que para la implementación de este modelo de red con IPv6 ya tenemos un modelo físico actual, el cual es en forma de estrella jerárquica en el caso de la LAN Universitaria, y un anillo en el caso de la red nacional, es necesario aquí aplicar un modelo lógico de la red IPv6.

- Las diferencias con IPv4 son que ahora todas las direcciones son globales, por lo que no se utiliza ni NAT, ni PAT, ni proxy en cada subred como se realizaba anteriormente en una arquitectura IPv4. En el nuevo diseño con IPv6 en cada subred puede existir un número muy grande de direcciones para su uso, lo que hace que el nuevo direccionamiento sea lo suficientemente grande para cualquier departamento.

- Un aspecto muy importante que diferencia a IPv4 de IPv6 es que actualmente no todas las aplicaciones funcionan con IPv6, por lo que hay que tener mucho cuidado en siempre tener disponible el protocolo IPv4, así mismo es importante que si se implementa IPv6 debe permanecer este siempre activo, ya que las aplicaciones que manejan los dos protocolos, normalmente van a preferir IPv6 que IPv4, y al no encontrar servicio en IPv6 éstas tendrán una demora considerable hasta reconocer esta falta de servicio, dando una mala experiencia de navegación al usuario final.

Router PE frontera con CLARA	ahora este equipo deberá soportar IPv6 en Dual Stack, comunicarse con MBGP con el router PE de red CLARA.
Routers P del proveedor	deben permitir enrutar las redes IPv6 tanto de la Universidad como las de redCLARA.
Router CE frontera de la Universidad	este router es muy importante, ya que es el que realiza multihomed, enrutando transparentemente hacia Internet comercial y hacia redes Académicas.
Firewall	Hablando de la seguridad, este es el componente que controla el ingreso/salida de datos a servidores y usuarios finales, es el componente más importante que protege la seguridad de los equipos.
Servidores	Ya que no solamente es importante poder acceder a servicios por IPv6, sino también ofrecer servicios, estos componentes son importantes para dar visibilidad de la Universidad hacia el mundo.
Capa de distribución y acceso	es importante para permitir la conexión a la red de los usuarios finales de una manera automática y rápida.

Cuadro 1: Componentes activos de red necesarios para la transición a IPv6

- Ya que IPv6 no utiliza broadcast para encontrar a los vecinos de su red, sino multicast con ICMP, así como también para muchas actividades más de manejo de errores entre otros, es por ello importante que ahora el firewall no bloquee este protocolo, pues en caso de hacerlo existirá problemas en el funcionamiento general de IPv6.

- Los servidores de aplicaciones que van a ser modificados, deberán tener soporte dualStack, pues el servicio debe ser ofrecido a ambas versiones de IP, y su funcionamiento interno debe ser el mismo para ambas versiones, es decir servicios ofrecidos para IPv4 e IPv6.

5.5. Desventajas y Ventajas

IPv6 tiene ciertas desventajas que con el tiempo desaparecerán y ventajas muy claras frente a IPv4, entre ellas podemos citar:

Desventajas:

- IPv6 al ser un protocolo relativamente nuevo, sobre todo en nuestro medio, su uso es muy bajo respecto IPv4, por lo que aplicaciones y servicios en este protocolo son muy pocos al momento.

- IPv6 al no tener un uso masivo, los administradores de la red no conocen este protocolo a profundidad como conocen a IPv4, por lo que los tiempos de solución en caso de existir problemas en estas redes requieren mayor tiempo.

- Ya que las direcciones IPv6 son más grandes que en IPv4 ya no es posible memorizarse una dirección para comunicarse directamente de un computador a otro como normalmente se hace para compartir archivos o realizar pruebas de servicios, ahora es necesario asignarle un nombre para facilitar su acceso.

- Dado que todas las direcciones son globales, éstas pueden ser accedidas desde cualquier punto de Internet, haciendo que la seguridad del usuario se vea afectada, la seguridad en IPv6 es diferente que en el caso de IPv4 cuando se usa NAT o PAT.

- En los servidores se debe ahora manejar una doble pila de seguridad, reglas para IPv4 y reglas para IPv6, haciendo más complejo la administración de la seguridad, ya que siempre será necesario aplicar reglas para ambas versiones.

ICMPv6: Internet Control Message Protocol versión 6, documentado en el RFC2463

- IPv6 viene con IPsec incluido dentro de su protocolo, por lo que puede ser usado para transmitir información encriptada, haciendo que no se pueda detectar lo que se transmite, por lo que es una manera en que la transmisión de virus de un usuario a otro se hace más fácil, haciendo que sea indetectable para los dispositivos intermedios que protegen la transmisión de virus por la red.
- Actualmente no todo el hardware nuevo tiene IPv6 dentro de su pila de protocolos, por lo que es necesario de ahora en adelante tener una política de requerimientos para asegurar que todo el nuevo hardware comprado en la Universidad tenga este protocolo incluido.

Pero así mismo IPv6 tiene muchas ventajas respecto a IPv4, entre estas tenemos:

- Este protocolo al tener virtualmente un número ilimitado de direcciones, es posible asignar a cada subred un número muy grande de direcciones, las cuales prácticamente no se terminan, de esta manera se puede dar a un computador una o varias direcciones IPv6 cada vez que lo solicita, mejorando su seguridad.
- Ahora todos tienen direcciones globales, lo que permite comunicación punto a punto sin necesidad de ningún proxy, esto mejorará en el desarrollo de las nuevas aplicaciones, ya que los programadores no se preocuparán de NAT, el cual da muchos problemas sobretodo con ciertos servicios como por ejemplo VoIP o videoconferencias y otras aplicaciones que necesitan una conexion punto a punto.
- El tener una cabecera IP más pequeña hace que el tiempo de retardo en los dispositivos capa 3 sea menor, lo que mejora en el rendimiento tanto del equipo intermedio, así del tiempo requerido para que el paquete pase el dispositivo.
- Las características de seguridad y movilidad que ahora son obligatorias en este protocolo, hace que exista un nuevo panorama para la seguridad y movilidad de estaciones de trabajo.
- Con la llegada de IPv6 se abre la posibilidad de poder enviar grandes packetes IPv6 (jumbogramas) de hasta 4GB de carga (siempre y cuando la capa 2 lo permita) el cual mejorará el throughput en la transmisión de información en líneas de muy alta velocidad.

IPv6 Jumbograms: Paquetes IP de tamaño gigante, definidos en el rfc2675

- El usar IPv6 garantizará que en el futuro todo el trabajo realizado no será desechado, ya que todo funcionará con IPv6 obligatoriamente e IPv4 va a ir desapareciendo.

Como resultado de ventajas y desventajas en este protocolo, podemos decir que aunque la transición, uso y administración de este nuevo protocolo inicialmente requerirá mayores conocimientos y tiempo empleado por los administradores, hay que realizarlo, pues este protocolo es el que dominará en el futuro.

6. Diseño

6.1. Introducción

Para el diseño de la red se analizó primeramente la red interna, y por separado la red externa, ya que el diseño de ambos es diferente. El primero tiene una disposición física ya definida, el segundo un modelo lógico que hay que adaptarlo a las necesidades.

Red Interna: Para el diseño de la red interna se tomó en cuenta el factor físico, disposición física y conexión de los equipos, localización de usuarios finales, localización de la DMZ.

Red Externa: Para la red externa se tomó en cuenta el CE, peering, multihomed, iBGP, eBGP en los dos proveedores (ISP comercial y red Académica).

También se tomó en consideración factores como la inexistencia de un sistema Autónomo propio de la Universidad y de la ausencia de un prefijo IPv6 propio de la Universidad que hayan sido obtenidas por LACNIC.

Otros factores que influyen en el diseño son las características de los equipos, los cuales se encuentran en la tabla 2

Cada uno de los equipos realiza funciones diferentes, estas son:

Router de CEDIA: controla el peering de la red CEDIA hacia el router de red CLARA Internacional, controla el sistema autónomo de CEDIA 27841, envía las redes propias de CEDIA IPv4 190.15.128.0/20, red IPv6 2800:68::/32 así como las redes propias de los miembros. Para este proyecto la red /48 2001:470:d81f::/48 de la Universidad de Cuenca otorgada por el tunnelbroker fue agregada en este router.

Router de frontera de la Universidad: este router tiene hacia el exterior enrutamiento iBGP entre todos sus miembros, está conectada lógicamente a un lado hacia el router de CEDIA para ir hacia red Académica, y hacia el router del ISP para salida a Internet Comercial. Este router es la clave para el funcionamiento de red Académica y Comercial, este router maneja hacia adentro la red IPv4 192.188.48.0/24 propia de la Universidad, la red IPv4 190.15.132.0/24 otorgada por CEDIA a la Universidad, la red IPv6 2800:68:c::/48 que es una subred IPv6 otorgada por CEDIA a la Universidad y que solo tiene salida a la red Académica, y para este proyecto se agregó la red 2001:470:d81f::/48. Hacia afuera tiene conexión IPv4 e IPv6 por medio de Vlans que conectan al router del proveedor y por MPLS hacia otras ciudades del Ecuador.

CE: Customer Edge
iBGP: Internal Border Gateway Protocol
eBGP: External Border Gateway Protocol

Router de CEDIA	Router Cisco modelo 2821
Router de frontera de la Universidad	Router Cisco modelo 7604
Router Universitario	Router Cisco modelo 2821
Firewall Universitario	Cisco ASA 5520
red CORE	Switch capa 3 Cisco 4506
Red de Distribución	Cisco 3560
Red de Acceso	Cisco modelo 2960.
Servidor de Correo	Postfix, instalado en un S.O. GNU/Linux.
Servidor de portales web	Servidor Apache2 instalado en un en S.O. GNU/Linux.
Servidor de DNS	Servidor BIND instalado en un S.O. GNU/Linux.

Cuadro 2: Dispositivos y servidores que funcionarán en dualStack

Router Universitario: Este router tiene administración local, por lo que es usado para conexión de túneles para diferentes usos del departamento que lo administra.

Firewall Universitario: Maneja la seguridad de la red Universitaria, tiene interfaces que conectan a la red DMZ y a la red Interna.

red CORE: Maneja toda la red por medio de VLANS, y VRF para dividir red universitaria de redes inalámbricas.

Red de Distribución: Conjunto de switchs capa 3, uno por facultad, controlan la seguridad y tienen creadas VLANs para cada departamento.

Red de Acceso: Conjunto de Switchs de capa 2 que dan acceso a los usuarios finales y dispositivos.

Servidor de Correo : Da servicio al personal Universitario para envío y recepción de correo.

Portales web: Conjunto de servidores que dan servicio a los portales de las facultades así como de aplicaciones varias que se da en la universidad.

Servidor de DNS: Da servicio de DNS recursivo para los computadores de la universidad, y otro de ellos maneja los dominios.

6.2. Diseño propuesto

La red IPv6 Universitaria debe cumplir con las siguientes características:

- Debe llegar a todos los puntos de la Universidad.
- Debe permitir una navegación IPv6 transparente para el usuario.
- IPv6 debe coexistir con la red IPv4 existente actualmente.
- Debe existir un modelo multihomed IPv6 para red Académica y Comercial transparente al usuario.

Para la realización de este diseño se tiene primeramente que seleccionar la red que se va a usar.

Primera Opción: Para la realización de este proyecto una de las primeras opciones es usar solamente un prefijo IPv6 de la red CEDIA. A noviembre de 2010 la universidad al ser parte de CEDIA obtuvo el prefijo /48 de IPv6 2800:68:C:: , esta subred es parte de

VRF: Virtual Routing and Forwarding, técnica usada para tener dos redes ruteadas virtualmente en el mismo equipo

la red 2800:68::/32 que es manejada por el consorcio, y que está dentro del AS 27841 perteneciente al mismo. Esta red IPv6 de CEDIA se encuentra realizando peering con red CLARA y esta con Geant e Internet2, por lo cual si se utiliza esta red se tiene las siguientes ventajas y desventajas:

Ventajas:

- No es necesario realizar trabajos de ruteo BGP en el iBGP ni peering hacia red CLARA ya que todo se encuentra realizado.
- Al estar publicado como un prefijo /32 de IPv6 hacia los AS de redes internacionales ninguna de ellas la filtrará, ya que incluso las más estrictas siempre aceptarán las /32 y /48.
- En el iBGP dentro de CEDIA Ecuador, no es necesario realizar cambios, ya que todas las instituciones miembros podrían llegar sin problema a la red de la Universidad.

Desventajas:

- La mayor desventaja es que solamente podrá funcionar en redes académicas, haciendo imposible la conexión hacia el Internet Comercial.
- La primera opción haría que el usuario final al tener su equipo con IPv6, este no puede reconocer para donde navega si hacia red Académica o red Comercial, por lo que cuando El trate de acceder a una dirección comercial tomará tiempo hasta que el browser o aplicación detecte la falta de conexión, y solicite su dirección IPv4, esto hace que el usuario tenga una mala experiencia con este protocolo, lo cual no debe suceder ya que se desea promover el uso de IPv6.

Una segunda opción es obtener un prefijo /48 de IPv6 de algún ISP nacional, hasta finales del 2011 ningún proveedor Ecuatoriano brindaba este servicio IPv6 Comercial.

La tercera opción es obtener un prefijo /48 de un proveedor de tunnelBroker para este proyecto se obtuvo la red 2001:0470:d81f::/48 por medio del proveedor Hurricane Electric el cual está registrado dentro de ARIN. Este provee conexión a la red IPv6 comercial por medio de túneles. Las ventajas y desventajas de usar este procedimiento son:

Ventajas:

2800:68::/32: Prefijo IPv6 obtenido de LACNIC el 2006/07/19 por parte de CEDIA

AS: Sistema Autónomo

LACNIC ofrece /32 para ISP en el rango 2001:1200::/23 y para usuarios finales /48 en el rango 2800::/12

Tunnel Broker: permite conectar una isla IPv6 por medio de un tunel 6in4 (sobre una red IPv4) hasta proveedor que entrega dicho servicio.

Hurricane Electric: www.he.net, proveedor de tunnel broker a nivel mundial

- Es independiente del proveedor que tenga la Universidad.
- Si se tiene problemas de conexión simplemente se puede cambiar de proveedor.

Desventajas:

- Al ser un túnel se debe usar DualHomed para poder enviar hacia la red Académica, lo cual requiere configuraciones de BGP en la red CEDIA para poder ir hacia red CLARA.
- Los proveedores actuales del servicio de Tunnel Broker se encuentran en Norte América, Europa y Asia, por lo que los tiempos de retardo de los paquetes hacia estos datacenters son altos.
- Para la conexión hacia las instituciones que forman parte de CEDIA se requiere que el ISP publique la red por iBGP para la conexión dentro del país.

La cuarta opción y la mejor para proveer IPv6 a la Universidad es obtener de LACNIC un rango de direcciones IPv6, con ello sin importar el proveedor no se cambiará de prefijo, y se requiere además de obtener la red, agregar esta red en el iBGP del ISP, y publicar hacia red Académica esta nueva red. Y para el caso de red Comercial es necesario realizar un peering de BGP con algún proveedor de tunnel Broker, en este caso también se necesitaría obtener un AS en LACNIC.

Al iniciar este proyecto se realizó la tercera opción, es decir por medio de un tunnel-Broker se obtuvo una red prefijo /48 de IPv6, el tunnelBroker fue Hurricane Electric, el origen del túnel fué el datacenter de Miami, y el destino del túnel fué el router de borde de la Universidad, también se realizó la publicación por iBGP dentro de Ecuador de la red obtenida /48, y la publicación por BGP en el router de CEDIA en Guayaquil que se conecta hacia la red CLARA Internacional, pero antes de que finalice este proyecto de tesis, se obtuvo por medio del ISP un servicio de IPv6 nativo para la Universidad, razón por la cual en este proyecto se realizó el diseño inicial ejecutado usando un tunnel Broker y a posteriormente se cambio el diseño para adaptarlo al uso de IPv6 nativo.

Para el diseño interior de la red Universitaria se toma en cuenta la topología física, esta topología es en forma de estrella con un router Cisco 4506 como CORE, para la red de distribución se tienen switchs capa 3, uno por facultad, y para la red de acceso switchs capa 2.

El diseño completo usando tunnel Broker (el proveedor fue Hurricane Electric) es que se encuentra en la Figura 7, esta implementación se la realizó en el segundo semestre del 2010, y su funcionamiento se dio hasta mediados de diciembre del 2010.

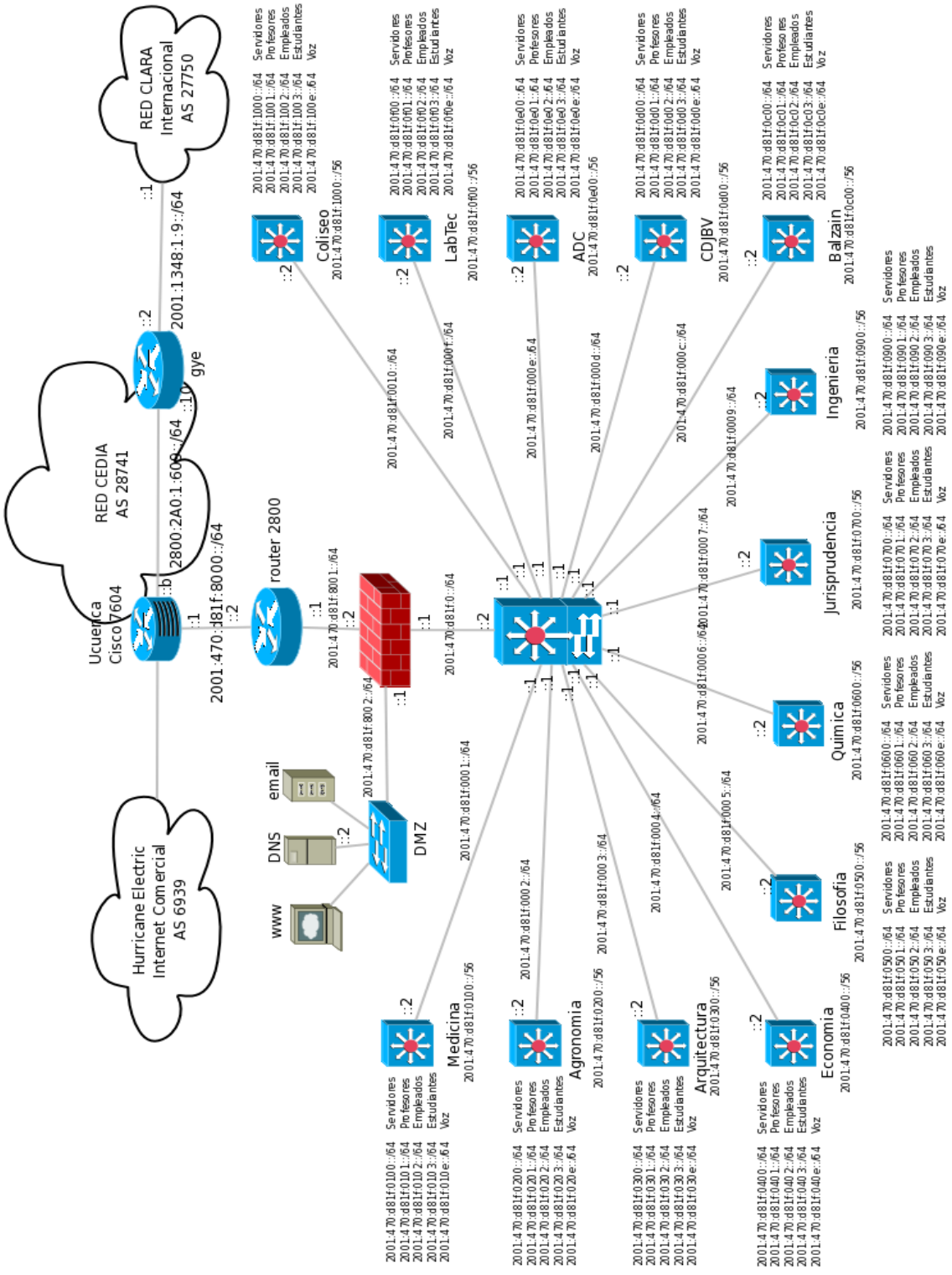

Figura 7: red IPv6 de la Universidad de Cuenca, segundo semestre 2010

En este primer diseño se puede observar que la red global IPv6 que se la publica es la 2001:470:d81f::/48 otorgada por Hurricane Electric. En las conexiones hacia Internet Comercial se puede ver en la parte superior la conexión por túnel 6to4 hacia Hurricane Electric (AS 6939) y por medio de la red CEDIA (AS 28741) la cual toma a la red 2001:470:d81f::/48 como suya para colocar en el router de CEDIA y publicarlo por BGP hacia red CLARA.

El router de CEDIA se encuentra en Guayaquil, es quien hace de router de frontera del AS 28741, ya que quien se conecta con el router de CLARA AS 27750, y entre los dos intercambian rutas. El AS2770 es un AS de tránsito hacia las demás NRENS en Latinoamérica, Norteamérica y Europa, y por medio de ellas a todo el planeta.

La conexión dentro de la Red CEDIA se realiza por el iBGP, se utiliza RIPv2, la red es publicada por el router de frontera de la Universidad, hacia la red Nacional, este router al conocer por iBGP todas las redes Académicas mundiales por medio de BGP, tiene la política de que si el prefijo de la red es conocida, la envía por el AS de red CEDIA, caso contrario la ruta por defecto es el túnel hacia Internet Comercial. De esta manera se obtiene multihomed con los 2 proveedores de IPv6.

La conexión entre el router de frontera de la Universidad Cisco 7604 y el Cisco 2800, es por una interfaz de Gigabit Ethernet dentro del Datacenter de la Universidad, el router Cisco 2800 es manejado totalmente por la universidad, por lo que aquí se realizan túneles hacia redes externas, VPNs, y un control básico de tráfico.

La primera protección para servidores y los usuarios finales es el firewall Universitario, el cual protege a la red de ataques externos. Este equipo es un Cisco ASA 5520, que tiene configurada 3 interfaces Gigabit, la interface OUTSIDE que conecta con el router Cisco 2800, la interface DMZ0 que conecta a la red de servidores Universitarios, como DNS, correo electrónico, portal web entre otros, y la interface INSIDE que se conecta a la red CORE de la Universidad.

La red CORE de la Universidad de Cuenca actualmente está conformada por un único switch capa 3, modelo Cisco 4506 con múltiples interfaces de fibra y UTP, todas en Gigabit Ethernet. Este equipo es el centro de la topología en estrella de la Universidad. A este se conectan por fibra oscura cada una de las facultades y campus universitarios (Campus Paraiso, Campus Yanuncay, Campus Balzaín).

Para la red de distribución se tienen equipos Cisco 3560 en cada Facultad, en todos los campus forman un total de 13 equipos de las mismas características. Estos equipos al ser dispositivos capa 3 proveen servicios de enrutamiento y de DHCP, así como control con listas de acceso para dar seguridad a las redes.

Para la red de acceso se tienen varios equipos modelo Cisco 2960, estos son dispositivos capa 2, los cuales proveen conexión para los usuarios finales a la red. Estos equipos controlan el spanning tree así como también proveen POE. Al ser dispositivos capa 2 el uso de IPv4 o IPv6 no afecta en gran medida, excepto si se desea utilizar jumbo frames en IPv6.

En Diciembre del 2010 el proveedor de Internet Comercial ya logró entregar el servicio de IPv6 de manera nativa a la Universidad de Cuenca, por lo que fue posible usar el prefijo asignado 2800:68:c::/48, pero también fue necesario agregar el peering con sus proveedores internacionales, para de esta manera poder ser alcanzados por el exterior, logrando que la Universidad de Cuenca obtenga una mejora significativa en la disminución del retardo de los paquetes y ancho de banda comparado con el uso del tunnel Broker usado hasta antes de esta fecha. Los cambios realizados en el diseño para esta nueva red se encuentran en la figura 8 y que fueron realizados a partir de diciembre del 2010.

Al tener todo el core de la red nacional en IPv6, y el peering internacional nativo en IPv6 tanto en Internet comercial como en red académica, se logra tener ya una red con mejores prestaciones, mejoras en la velocidad y una disminución considerable en el retardo de los paquetes hacia los diferentes sitios con respecto al uso del tunnelBroker.

En lo referente al diseño en la red de servidores, estos no pueden ser eliminados y migrados a IPv6, ya que no todo el mundo tiene funcionando el nuevo protocolo, lo que se debe realizar es una transición, es decir debe existir un tiempo (varios años) donde el servicio tanto de navegación como de los servidores esté disponible en ambas versiones del protocolo. Una de las mejores opciones para esta transición es usar la doble pila (Dual Stack), la Universidad posee varios servicios, algunos de ellos sobre una plataforma GNU/Linux, y otros en plataformas Microsoft, aunque el Dual Stack se puede ya realizar en ambos sistemas operativos, con las versiones correctas, este proyecto contempla únicamente la implementación en aquellos con plaforma GNU/Linux, estos servidores son:

- Servidor de portales web: Actualmente funcionando en la mayoría de portales de facultades en el sistema operativo GNU/Linux.
- Servidor de correo: Un servidor en GNU/Linux, usando un MTA como Postfix

STP Protocol: IEEE 802.1D

POE: Power Over Ethernet, IEEE 802.3af

MTA: Message Transfer Agent:

Postfix: MTA desarrollado por Wietse Venema

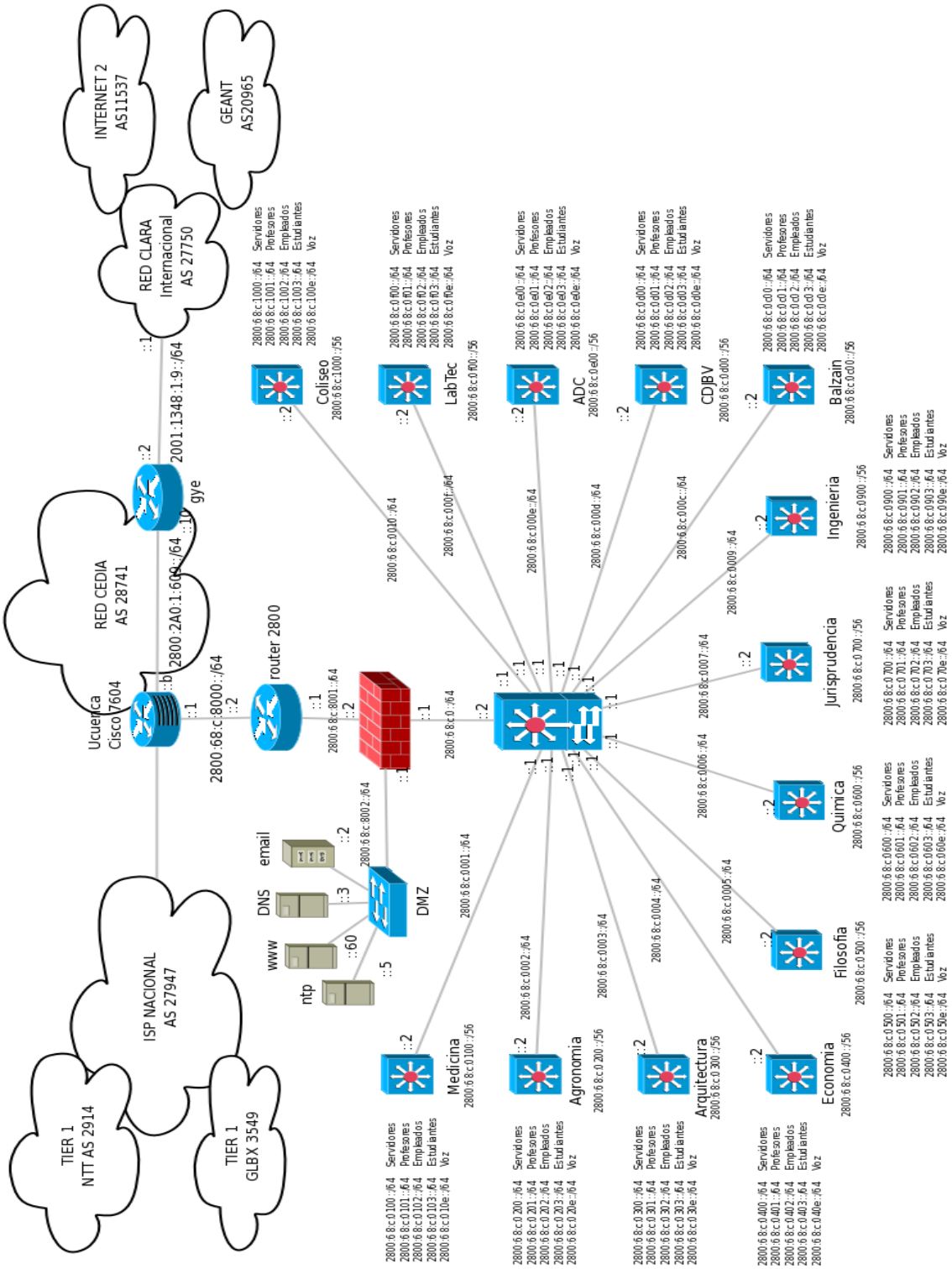

Figura 8: red IPv6 nativa de la Universidad de Cuenca diciembre 2010

6.3. Requerimientos técnicos

La Universidad actualmente cumple con todos los requisitos físicos necesarios para la implementación, con respecto a los requerimientos mínimos de software para los servidores y de IOS en el caso del sistema operativo de los equipos Cisco. Las necesidades de software y hardware son:

- Sistemas Operativos GNU/Linux con soporte IPv6 para los servidores.
- Servidor de páginas web Apache con soporte IPv6.
- Servidor de DNS BIND con soporte IPv6.
- Servidor de correo electrónico con soporte IPv6.
- Router CPE Universitario (Cisco 7604) con un IOS que soporte IPv6, BPG-MP, RIPng para soporte en iBGP de la red CEDIA nacional, y túneles 6in4.
- Router Universitario (Cisco 2800) con IOS que soporte ruteo IPv6.
- Firewall (Cisco ASA 5520) que permita IPv6, ACLs para IPv6.
- Switchs de red de core (Cisco 4506) y distribución (Cisco 3560) con soporte IPv6, OSPFv3, Network Discovery Protocol para IPv6 y ACLS para IPv6.
- Sistemas operativos clientes GNU/Linux que soporten IPv6 y con herramientas necesarias para el uso de la extensión IPSEC.

IOS: Internetwork Operating System

ND: Network Discovery Protocol para IPv6 - rfc2461

7. Implentación

7.1. fases de implementación de la red

Para la implementación total de proyecto, se lo realizó en varias fases, estas son::

7.1.1. Primera Fase: Obtención de una red IPv6 por parte de un proveedor

Esta primera fase se realizó en el segundo semestre del año 2010, en donde el requerimiento inicial era proveer un enlace de IPv6 a la Universidad de Cuenca para poder usarlo para la navegación interna, así como también poder activar sus servidores en IPv6. Dado que hasta ese momento se tenía de parte del proveedor comercial solamente IPv4 más no IPv6, se debió buscar una solución. El estado completo de la Universidad antes de iniciar el proyecto era:

- El proveedor de Internet Comercial en aquella fecha no proveía conexión con IPv6, aunque los proveedores internacionales si lo hacían.
- La red Académica nacional tenía para aquella época conexión IPv6 dentro del Ecuador y hacia RedCLARA por medio de un túnel 6in4 desde el router de frontera en Guayaquil, hasta cada universidad que lo requería. De esta manera se podía proveer conexión hacia redes académicas internacionales.
- La Universidad de Cuenca no tenía un rango de direcciones IPv6 delegadas por LACNIC, ni un sistema autónomo.
- En la Universidad de Cuenca se tenía la posibilidad realizar cambios en el router CPE y solicitar cambios en el router de frontera de la red Académica Ecuatoriana (se conecta con redCLARA, y de allí hacia el mundo) para poder realizar la publicación de sus redes únicamente hacia redes académicas.

Al momento de implementar el proyecto se tuvo dos alternativas, la primera era obtener un rango IPv6 /48 de parte de CEDIA (la cual tiene un rango /32 de IPv6 delegada directamente de LACNIC), y la segunda era obtener un rango /48 de IPv6 de parte de un proveedor de túneles de Internet Comercial, de los cuales existen varios que dan servicios sin costo así como un servicio especial, con un costo adicional. Para iniciar la implementación de este proyecto aquella época se optó por la segunda opción, es decir conexión por medio de un túnel de un proveedor externo por las siguientes razones:

- El proveedor de túneles que se uso para iniciar este proyecto fue Hurricane Electric el cual luego de suscribirse, entrega una red IPv6 /48 y puede ser alcanzado por medio de un túnel 6in4 que va desde el router de la Universidad hasta uno de los datacenters del proveedor. Los paquetes IPv6 son transmitidos encapsulados en paquetes IPv4 dentro del túnel.

- Al obtener un rango de IPv6 /48 del proveedor de túneles, la Universidad queda dentro del mismo AS del proveedor.

- A esa fecha, el servidor de tunnelbroker HE.net era el único que permitía conectarse por BGP dentro del túnel para poder publicar redes IPv6 propias, pero dado que la Universidad no tiene un AS propio, no fué posible usar esta característica, que se encuentra disponible de manera gratuita.

- Dado que es necesario a parte de usar el Internet Comercial también proveer a los usuarios la red Académica tanto nacional como Internacional de una manera transparente, es importante publicar dentro de Ecuador así como hacia redCLARA la red IPv6 que se utilice, en el caso la red académica nacional, es posible realizar la publicación por iBGP desde el CPE de la Universidad. En el caso Internacional es necesario que el router PE de CEDIA publique por eBGP hacia redCLARA la red usada por la universidad, y que esta haga lo propio con las redes internacionales.

7.1.2. Segunda fase: levantamiento del túnel 6in4 entre la Universidad y Hurricane Electric

Luego de haber solicitado un rango de direcciones IPv6 a un proveedor de túneles (Hurricane Electric, por medio del sitio tunnelbroker.net) fué necesario tener un equipo ruteador tenga una IPv4 pública y que tenga la característica de creación de un túnel 6in4. En el caso del a Universidad el router que realizó el túnel fue el CPE, un router modelo Cisco 7604. También fue necesario que al lado del servidor del tunnelBroker proveer la información de los IPs de la Universidad para la correcta configuración del túnel. La configuración de este túnel se encuentra en la figura 9. Los datos suministrados para la creación del túnel fueron:

- Nombre del túnel, solamente para diferenciar un túnel de otro en caso de tener varios administrados.

Hurricane Electric: he.net es actualmente el mayor proveedor de túneles IPv6, tiene datacenters alrededor de todo el mundo, su AS es el 6939

- Selección del servidor más cercano o que tenga las mejores prestaciones (menor retardo, jitter mínimo, menor pérdida de paquetes), se tiene la opción de conectarse a una de las distintas ciudades en donde el proveedor tiene datacenters, dependiendo de ello se coloca automáticamente el *server IPv4 address*, y nos asignan un *server IPv6 address* que son las IPs tanto para hacer el túnel, y para la red de conexión IPv6 respectivamente.
- Siempre se tiene la opción de colocar la dirección IPv4 local, es la IP al lado del cliente, en donde se conecta el túnel, es decir el router que va a hacer 6in4.
- El proveedor asigna una dirección IPv6 interna del túnel para colocarlo en nuestro equipo.
- Con los datos anteriores se tiene una conexión desde el router local hasta el datacenter de HE.net, luego es necesario solicitar un prefijo IPv6 /64 o /48 para distribuirlo dentro de la LAN. Este prefijo es asignado por el proveedor.
- Ya que hay una red asignada para la LAN, es importante mantener el control del DNS reverso, para ello se colocó las IPs de los servidores rDNS que manejarán la zona inversa.

Luego de creado el túnel entre el proveedor (datacenter de HE.net) y la Universidad de Cuenca (el CPE de la Universidad) se logra tener ya una conexión IPv6 hacia el Internet Comercial, pero a una velocidad baja, con existencia de jitter, y un gran retardo en los paquetes debido precisamente al proceso de encapsulación y desencapsulación que se debe realizar en los extremos del túnel. El proceso de transmisión de los paquetes comienza en la Universidad, luego son encapsulados en nuestro extremo del túnel por el CPE y enviados hasta el datacenter del proveedor el cual lo desencapsula y recién allí inicia el enrutamiento hacia su destino final ya en la nube IPv6.

Hasta este punto ya se tiene algunas direcciones entregadas y recibidas la red, los datos son:

- IPv4 inicio del túnel al lado del servidor: 209.51.161.58.
- IPv6 del túnel, al lado del servidor: 2001:470:4:72::1/64.
- Dirección IPv4 del router de la Universidad donde termina el túnel: 200.110.69.120.
- IPv6 del túnel, al lado de la Universidad: 2001:470:4:72::2/64.

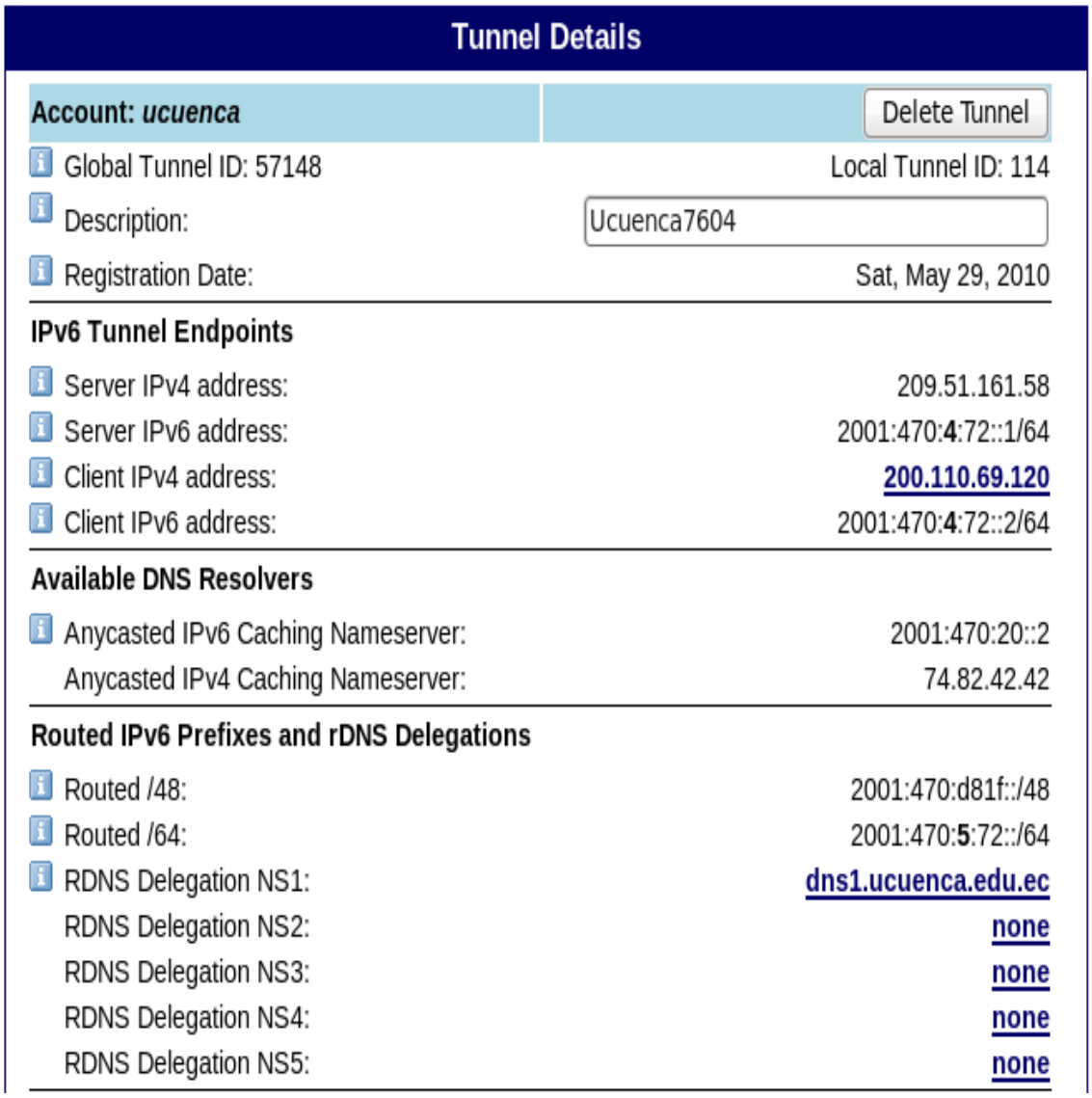

Figura 9: Creación de un tunnel Broker entre HE.net y la Universidad de Cuenca

- Red IPv6 recibida y que se la utilizó dentro de la LAN universitaria: 2001:470:d81f::/48.
- Servidor rDNS que realizará la resolución inversa del prefijo 2001:470:d81f::/48.

Configurando el equipo con esta información en el CPE de la Universidad de Cuenca, se consiguió la conexión a Internet Comercial.

7.1.3. Tercera fase: configuración de iBGP y eBGP con la red obtenida

En esta tercera fase se debe realizar la publicación de la red obtenida del proveedor hacia dentro del Ecuador como hacia afuera, es decir el prefijo 2001:480:d81f::/48. En el caso del ruteo dentro de Ecuador es necesario configurar el router PE para que sea parte de iBGP nacional. Con esta información ya todos los routers miembros de la red nacional que comparten con la Universidad el mismo sistema autónomo conocieron la manera de llegar al nuevo prefijo directamente solucionándose la primera parte.

Hasta este punto existe un túnel hacia IPv6 Comercial, falta aún la configuración para poder conectarse hacia las redes académicas internacionales. Esto se realiza en el router frontera de CEDIA en Guayaquil, la publicación es realizada por eBGP, la cual es necesaria para que los demás sistemas autónomos de las redes académicas internacionales conozcan que el prefijo IPv6 de la universidad es 2001:480:d81f::/48 y que pueden llegar por medio del sistema autónomo de CEDIA.

Al finalizar estas dos publicaciones, desde afuera de la Universidad tendrían diferentes formas de llegar a la red de la Universidad:

1. En el caso de cualquier red dentro del mismo sistema autónomo de CEDIA (AS27841) se enrutaría directamente por la red nacional.

2. En el caso de otros sitios que estén en Internet Comercial, estos accederían por medio del proveedor del tunnelBroker HE.net, cuya puerta de acceso en el caso de la Universidad de Cuenca, se escogió en el datacenter de Miami, pues por su cercanía es el que tuvo mejor calidad en el enlace (menor jitter y retardo de paquetes).

3. Para el caso de otros sistemas autónomos que se encuentren en las redes académicas internacionales, el acceso será por medio de red CLARA, el cual publicó con anterioridad el anuncio del prefijo de la red Universitaria.

Esta fase de publicación de los prefijos hay que realizarla con cuidado, pues en el caso de publicar el prefijo equivocado, o con una mascara incorrecta, puede darse problemas muy graves que pueden llegar incluso a problemas legales por robo de IPs.

YouTube Hijacking: http://www.ripe.net/news/study-youtube-hijacking.html: el 24 de febrero de 2008, por equivocación del personal técnico un ISP de Pakistán, realizó una mala configuración en el router de Pakistan Telecom que anunciaba por medio de BGP, sus redes, se anunció un prefijo perteneciente a Youtube, y empezó a rutearse todo su tráfico hacia Pakistan, por aproximadamente 2 horas.

7.1.4. Cuarta fase: Implementación interna

Al haber finalizado toda la parte del BGP dentro del AS en Ecuador, así como también la publicación internacional, el siguiente paso es desplegar la red hacia adentro de la Universidad, primero se realizó un diseño de las subredes asignadas a todos los departamentos existentes en la Universidad, y se realizó la configuración de los dispositivos activos para proveer navegación, así como también la implementación de IPv6 en los servidores de la Universidad.

Esta implementación se la realizó desde afuera hacia adentro, activando la navegación a los usuarios solamente cuando ya todo el camino se encuentre disponible en IPv6, es por ello que todo fue transparente para los usuarios.

7.1.5. Quinta Fase: Uso de la red propia IPv6 2800:68:c::/48 de la Universidad

En el mes de diciembre del 2010, cuando este proyecto de tesis ya se encontraba en una fase de producción usando el túnel comercial y ya publicado este prefijo hacia redCLARA, el ISP empezó a proveer IPv6 nativo, lo cual representó un gran avance en los niveles de calidad (menor retardo, menor jitter y una mayor tasa de transferencia), para ello fué necesario hacer cambios en la implementación tanto en la red LAN de la Universidad así como en la red nacional dentro del AS, ya que anteriormente se estaba usando un tunnelBroker.

El cambio fue básicamente usar el prefijo asignado por CEDIA, eliminando la red provista por el servidor de túneles, y cambiando dentro de toda la universidad el prefijo en las redes LAN así como de sus servidores, este cambio se lo realizó en pocos días, y fue transparente desde el punto de vista del usuario dado que el túnel permaneció activo mientras se migraba al nuevo prefijo.

La red 2800:68:c::/48 asignada a la Universidad, no pudo ser utilizada anteriormente dado que no se tenía ni se tiene un AS para poder realizar peering hacia Internet Comercial con el proveedor de túneles, pero con la llegada del IPv6 nativo, el ISP nacional es quien realiza peering IPv6 hacia su proveedor internacional, de tal manera que también permite que la Universidad publique su red asignada.

Desde este punto en adelante, IPv6 e IPv4 son tratados de una manera similar, es decir la Universidad se encuentra en un modelo multiHomed en ambos protocolos de IP, ya que tiene 2 proveedores y debe conocer las rutas que estos dos proveedores ofrecen y publicar sus redes, estos proveedores son por un lado CEDIA y por el otro lado el ISP que provee Internet Comercial.

Con la realización de estos cambios, se elimina el uso de tunnelBroker y se pasa a un uso de IPv6 nativo en red comercial, se realizó cambios en el CPE, eliminando el túnel y las rutas que corresponden a dicho túnel, así como en la red interna en producción, la implementación de todas estas configuraciones y cambios realizados se encuentran en la figura 10

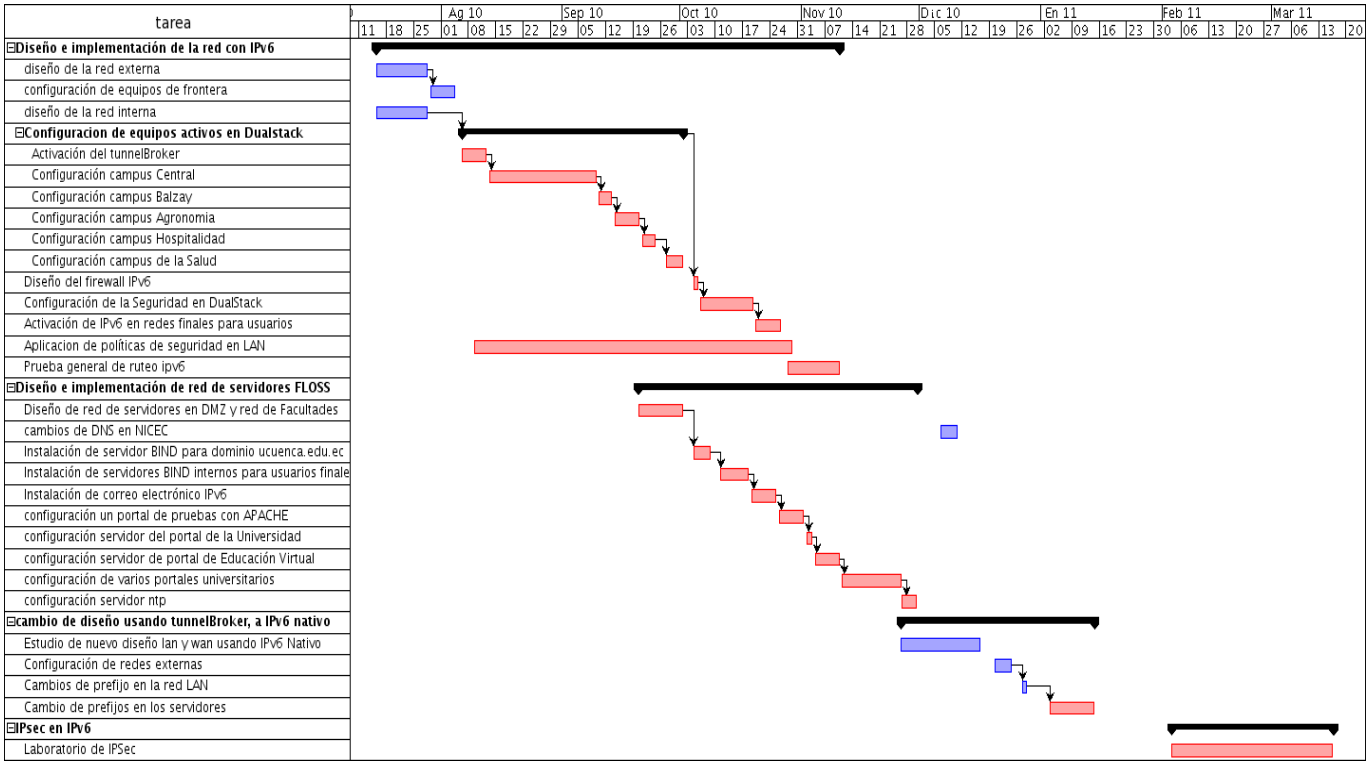

Figura 10: Cronograma de configuraciones realizadas

7.2. Dual stack

Debido a que la versión 4 de IP ya ha sido usada por casi tres décadas, existe en la actualidad una gran variedad de dispositivos que funcionan con dicho protocolo y que no tiene una actualización hacia la versión 6, y que casi toda la infraestructura de Internet se encuentra en versión 4, hay que encontrar una manera que ambas redes coexistan sin hacer un cambio de los equipos activos existentes. Una de las soluciones es utilizar Dual Stack, esta técnica nos permite que un equipo físico pueda trabajar en las dos pilas

Infraestructura Internet IPv4 e IPv6: estadísticas hasta Agosto del 2010 de he.net: solamente 3200 prefijos IPv6 /48 o menores han sido publicados. De 35684 redes que usan BGP, solamente 2487 tienen implementado IPv6

del protocolo IP en versión 4 y en versión 6.

Los equipos activos como routers, firewalls, y switchs capa 3 que la Universidad de Cuenca posee para el transporte de datos, si permite realizar Dual Stack, de esta manera la transición al nuevo protocolo puede realizarse , permitiendo que solamente los que tienen el protocolo IPv6 en sus computadores lo puedan usar, los demás pueden continuar usando el mismo protocolo IPv4.

Para la configuración hacia Dual Stack se inicia con los equipos externos y luego hacia los internos, de esta manera se inicia con los siguientes:

7.2.1. Router CE Universidad de Cuenca

La Universidad de Cuenca tiene un router Cisco modelo 7604 que lo utiliza para conectarse por fibra óptica a la red nacional, este router se conecta hacia la red nacional del protocolo iBGP RIP, la primera interfaz es la que va hacia el proveedor y la segunda la que conecta hacia la LAN Universitaria, las configuraciones de la interfaz que va hacia afuera en el CPE son:

```
description WAN ipv6 address 2800:2A0:1:B09::B/64
ipv6 nd ra suppress
```

Esta IP 2800:2A0:1:B09::B/64 pertenece al rango registrado por el ISP en LACNIC, y es la que da acceso hacia la red nacional.

El siguiente paso es configurar la interfaz que va hacia adentro de la universidad, el ip 2001:470:D81F:8000::1/64 está dentro del rango que el proveedor del túneles entregó a la Universidad de Cuenca, la configuración es la siguiente:

```
description LAN ipv6 address 2001:470:D81F:8000::1/64
ipv6 enable
```

7.2.2. Router interno de la Universidad de Cuenca

La Universidad tiene un router que conecta el CE con el firewall, este router es un Cisco modelo 2800, tiene activas dos interfaces GigaEthernet, la primera hacia afuera, y la segunda hacia la Universidad, la configuración es la siguiente:

Dual Stack: Doble pila, permite dos pilas de protocolos IPv4 e IPv6, RFC 4213

```
interface GigabitEthernet0/1
description WAN
ipv6 address 2001:470:D81F:8000::2/64
ipv6 enable
!
interface GigabitEthernet0/0
description LAN
ipv6 address 2001:470:D81F:8001::1/64
ipv6 enable
ipv6 nd suppress-ra
```

En estas dos interfaces apreciamos ya las direcciones IPv6 del proveedor del túnel que se consiguió anteriormente.

7.2.3. Firewall

Este firewall que es un equipo Cisco modelo 5520 tiene activadas 3 interfaces que corresponden a: OUTSIDE, INSIDE, y DMZ0, las configuraciones son las siguientes:

```
interface GigabitEthernet0/0
nameif outside
ipv6 address 2001:470:d81f:8001::2/64
ipv6 enable
ipv6 nd suppress-ra
```

Esta interfaz GigabitEthernet0/0 conecta el firewall hacia el router 2800, tiene el nombre outside, y se la configura como DualStack, se realiza la activación de IPv6 mediante el comando *ipv6 enable* y se suprime el envío de paquetes RA de autoconfiguración hacia otros dispositivos con el comando *ipv6 nd suppress-ra*.

-

```
interface GigabitEthernet0/1 nameif inside
ipv6 address 2001:470:d81f::1/64
ipv6 enable
ipv6 nd suppress-ra
```

Esta interfaz GigabitEthernet0/1 conecta el firewall hacia el switch core de la Universidad, y de allí hacia las distintas redes de las facultades.

```
interface GigabitEthernet0/2
nameif DMZ1
ipv6 address 2001:470:d81f:8002::1/64
ipv6 enable
ipv6 nd suppress-ra
```

Interfaz GigabitEthernet0/2 es en cambio la que conecta a un switch capa 2 para proveer la zona desmilitarizada, zona en donde se encuentran todos los servidores universitarios que son públicos hacia Internet.

El firewall es el punto donde tradicionalmente en IPv4 termina el direccionamiento público, e inicia la red interna con direccionamiento privado. En el caso de la Universidad la red interna en IPv4 tiene el direccionamiento 172.16.0.0/15 y la red DMZ 10.0.1.0/24. El firewall tiene las siguientes políticas de seguridad las cuales también deben ser realizadas en IPv6:

Para la interfaz OUTSIDE:

- Para servidores en la red DMZ cada uno sale por medio de NAT a una IP pública.
- Todos los servidores en la DMZ tienen bloqueados inicialmente todos los puertos de entrada y salida.
- En el firewall solamente se abre los puertos necesarios para los servicios que se encuentran activo en la red DMZ.
- Si el servidor necesita navegación se colocan los permisos respectivos.
- Se deniega cualquier otro puerto/servicio tanto entrada o salida.

Para la red DMZ:

- ICMP6 se tiene abierto tanto de entrada así como de salida.
- Se tiene abierto los puertos solamente de los servicios ofrecidos a los servidores.

Para la red interna:

- Se da acceso a Internet a la red interna por medio de PAT.

PAT: Port Address Translation, una sola IP pública para varias IPs

- Se permite acceso total hacia Internet con excepción del puerto smtp.

Para IPv6 la seguridad está dada exclusivamente por permisos de entrada y salida que se coloquen en los puertos (ya que en IPv6 no se tiene NAT y cada IP usada es Global), las políticas son las siguientes:

En el caso de la red interna la política es negar la salida del puerto 25 (SMTP) y permitir todo lo demás. Dado que una de las ventajas de IPv6 es permitir que los hosts se conecten punto a punto sin necesidad de traducciones NAT como existe en IPv4, no se tiene una política de permitir el acceso desde la red externa.

La regla por defecto es permitir icmp e ip en inside y outside, para ello se crea un grupo de ACLs

```
ipv6 access-list acl_v6_inside permit icmp6 any any
ipv6 access-list acl_v6_inside permit ip any any
```

Y posteriormente se aplica a la interfaz:

```
interface GigabitEthernet0/1
access-group acl_v6_inside in interface inside
```

Ahora en el diseño del firewall es necesario conocer que puertos son requeridos por cada servidor, para el caso de un servidor web en la DMZ con ip 2800:68:c:8002::4, es necesario abrir ICMP6 y el puerto 80, y todo lo demás bloquearlo, quedando la configuración de la ACLS de la siguiente manera:

```
ipv6 access-list acl_v6_outside permit icmp6 any any
ipv6 access-list acl_v6_outside permit tcp any host 2800:68:c:8002::4 eq 80
ipv6 access-list acl_v6_outside deny ip any any
```

Y luego de ello hay que aplicar la ACL llamada *acl_v6_outside* a la interfaz externa del firewall, con el comando:

```
interface GigabitEthernet0/0
access-group acl_v6_outside in interface outside
```

Hay que tomar en cuenta que el ACL tiene una regla que es ejecutada en caso de no tener coincidencias previas, esta regla es *deny ip any any* la cual bloquea todo tipo de tráfico que ingrese por la interfaz outside. Hay que agregar una regla para que permita el tráfico a toda la red interna Universitaria, y en el caso de servicios de la DMZ ir agregando una línea por cada puerto que se necesite abierto en cada uno de los servidores.

SMTP: Simple Mail Transfer Protocol

ACL: Access List, reglas configuradas en los equipos activos de red, para controlar los paquetes de entrada y salida

Para el caso de la interfaz DMZ es diferente, pues aquí se configura los accesos que se desea que cada servidor pueda tener hacia Internet.

Una de las protecciones adicionales que brinda el protocolo IPv6 es que al tener una gran cantidad de direcciones en una misma red, y al permitir que las IPs no sean secuenciales, el tratar de realizar una búsqueda de IPs por medio del método de escaneo de IPs es prácticamente imposible, tomando en cuenta que también cada vez que un computador cliente se enciende, navega en Internet con una IPv6 diferente.

7.2.4. Switch Core

Este es un switch modular que trabaja en capa 3, tiene interfaces Gigabit Ethernet tanto para fibra como para UTP, y la Universidad le utiliza como switch core principal. A este switch se conectan directamente todas las facultades por medio de fibra multimodo, y también se conectan servidores internos de la Universidad.

Para el manejo de redes se lo realizó por medio de VLANs, y ya que para la transición se usa dual stack, cada VLAN debe tener 2 direcciones, una IPv4 y una IPv6. La configuración es la siguiente:

```
interface Vlan503
description haciaFirewall
ip address 172.16.1.193 255.255.255.192
ipv6 address 2001:470:D81F::2/64
ipv6 enable
ipv6 nd suppress-ra
```

Ahora para poder conectar a los switchs capa 3 de cada facultad se hace una topología en estrella jerárquica colocando como centro al switch core.

7.3. Red interna

Para la red de distribución y acceso se tiene una distribución física de la topología en estrella, con un switch capa 3 modelo 3560 en cada facultad, creado VLANs para cada departamento dentro de cada facultad, se ha asignado un prefijo IPv6 /56 a cada facultad, y un prefijo IPv6 /64 para cada subred. Con esta planificación se tiene direccionamiento para 256 facultades, y cada facultad puede tener hasta 256 subredes para departamentos internos, y cada subred departamental tener hasta 1.84e19 hosts.

Cada switch de facultad tiene la capacidad de enviar mensajes ICMP6 de auto-configuración el cual permite enviar en sus paquetes ciertos parámetros para que los hosts se auto-configuren, parámetros tales como:

- Prefijo IPv6.
- Gateway por defecto.
- Hop limit.
- MTU.

Con esta configuración todos los hosts que tienen protocolo IPv6 y auto-configuración activada, al recibir un mensaje de este tipo de parte de el router, se autoconfiguran con una IPv6 dentro del prefijo asignado y colocando como gateway el ip del router que envió los mensajes, de esta manera se completa la auto-configuración y el host se coloca en la red, listo para realizar enrutamiento de paquetes.

Cada switch capa 3 realiza la publicación de varios mensajes de auto-configuración con diferentes prefijos, dependiendo de la VLAN donde se encuentra como router. Como ejemplo tomaremos la siguiente configuración:

```
ipv6 nd prefix 2001:470:D81F:0703::/64
```

En cada VLAN existe una línea con este formato, el cual analizándolo podemos saber que: el prefijo de la universidad es 2001:470:d81f::/48 , los siguientes 8 bits representan la facultad, en este caso la facultad numero 07 (hexadecimal), y los siguientes 8 bits representan el numero de departamento dentro de la facultad, en este caso es el 03 (hexadecimal) que representa a VLAN de estudiantes de la facultad de Jurisprudencia, de esta manera llegamos a los 64 bits que es el prefijo anunciado en esta VLAN. Este proceso se realizó para cada una de las VLANS existentes en las facultades.

7.4. Túneles

Para la navegación es necesario que la Universidad se conecte a la red Académica y a Internet Comercial, para el caso de red Académica el ruteo es nativo, y este llega hasta el router CE de la universidad, por lo que no fue necesario realizar un túnel para

IPv6 Stateless auto-configuration: RFC2462

llegar hasta esta red. Pero en el caso de Internet comercial al no tener este servicio nativo del ISP nacional hasta antes de diciembre del 2010, fue necesario dar servicio a la Universidad por medio de un túnel 6in4, pero este túnel debe fue realizado en un lugar estratégico, pues se tiene 2 proveedores, Académico y comercial, cada uno entregando sus prefijos.

Dado que para poder conocer ambos prefijos y poder realizar el enrutamiento de manera correcta, el router que realice este trabajo debe ser uno que realice intercambio de tráfico BGP, en nuestro caso al router CE le llega por iBGP las rutas de la red Académica, aquí es donde se realizó el túnel. La Universidad se convierte en una red multihomed, dado que el mismo prefijo 2001:470:d81f::/48 sale por ambas redes. Para el túnel se obtuvo conexión en un IP de Miami del proveedor de tunnelbroker (IPv4 209.51.161.58). La configuración fue la siguiente:

```
interface Tunnel0
description tunnel ipv6 comercial
no ip address
ipv6 address 2001:470:4:72::2/64
ipv6 enable
tunnel source 200.110.69.120
tunnel destination 209.51.161.58
tunnel mode ipv6ip
```

Con la realización de este túnel el router CE, la Universidad tuvo acceso a Internet Comercial IPv6 por medio del enlace 2001:470:4:72::/64. El ruteo al ser en un túnel 6in4, los paquetes IPv6 viajan como datos dentro de los paquetes IPv4, por lo que no se tiene tanta eficiencia como en un enrutamiento nativo. Este túnel fue utilizado durante el tiempo que el ISP no entregaba IPv6 nativo, al momento ya lo hizo, este túnel se lo eliminó.

7.5. Ruteo

Con lo referente al enrutamiento, lo tenemos en dos zonas, y son tratadas de diferente manera, la zona externa a la Universidad a la cual corresponde a el enrutamiento EGP y la zona interna de la Universidad es decir el IGP.

La red nacional utiliza MPLS, en esta arquitectura se tiene 3 tipos de routers:

EGP: External Gateway Protocol
IGP: Internal Gateway Protocol
MPLS: Multiprotocol Label Switching

- Router CE: Customer Edge Router, es el router que conecta la LAN a la red del proveedor.
- Router P: Provider Router, son los routers del proveedor que se encuentran en la red nacional y que sirven de tránsito.
- Router PE: Provider Edge Router, estos routers son propiedad del proveedor y se encuentran en el borde.

Todos estos routers se encuentran trabajando dentro del mismo sistema autónomo, por lo que tienen el mismo iBGP, en la red nacional se utiliza RIPng para IPv6. Con ello todos los routers CE llegan a conocer todos los prefijos IPv6 de las redes académicas que llegan por el router PE que es el que conecta a redCLARA en su nodo en Guayaquil. En este router PE se utiliza Multi-Protocol Extensions para BGP4 para conectarse con el router de redCLARA en Guayaquil.

Hasta este punto se tiene ruteo desde el router PE de CLARA en Guayaquil, que comunica al router PE de CEDIA los prefijos, y este por medio de los routers P en la red nacional llegan al router CE de la Universidad, el cual llega a conocer todos los prefijos de las redes académicas IPv6, pero no conoce nada de IPv6 en red comercial, es aquí donde se colocó una ruta por defecto por el túnel activo hasta diciembre del 2010, que fue: *ipv6 route ::/0 2001:470:4:72::1* (el cual fue eliminado cuando llego el IPv6 Comercial nativo).

El siguiente paso fue realizar el enrutamiento de red IPv6 de la Universidad hacia ambas redes.

1. Ruteo hacia red Comercial
2. Ruteo hacia red Académica

Como la Universidad obtuvo una red 2001:470:d81f::/48 del proveedor de tunnel broker, simplemente con la realización de la ruta por defecto ya se tuvo salida hacia el Internet comercial. Pero el problema estaba en el enrutamiento hacia la red académica. Para este efecto, como primer punto se agregó la ruta hacia la red interna *ipv6 route 2001:470:D81F::/48 2001:470:D81F:8000::2* y además la siguiente línea a la configuración del router CE de la universidad:

LAN: Local Area Network

RIPng for IPv6: definido en el rfc2080

Multi-protocol Extensions for BGP4: RFC2858, permite a BGP llevar información de enrutamiento de protocolos diferentes a IPv4, tales como MPLS, IPv6, Multicast, entre otros

```
ipv6 router rip ISP
redistribute static
```

Lo que realiza este comando *redistribute static* es que la red 2001:470:d81f::/48 sea publicada en la red nacional por iBGP usando RIPng para IPv6, permitiendo que la red de la Universidad pueda ser alcanzada por cualquiera en esta red.

Para que el enrutamiento se realice correctamente fue necesario activar las interfaces que van a participar en el RIPng, para ello se colocó la siguiente linea *ipv6 rip ISP enable* en cada interfaz del router CE que participa en RIPng, que en este caso se ha dado el nombre ISP a la instancia de RIPng.

Con este enrutamiento, el router CE de la Universidad aprende lo siguiente respecto a rutas IPv6:

```
7604-UCUENCA#show ipv6 route summary
IPv6 routing table name is default(0) global scope - 676 entries
IPv6 routing table default maximum-paths is 16
Route Source Networks Overhead Memory (bytes)
connected 12 1152 1536
local 13 1248 1664
rip ISP 649 65856 83072
bgp 65019 0 0 0
Internal: 0 External: 0 Local: 0
static 2 192 256
Static: 2 Per-user static: 0
Total 676 68448 86528

Number of prefixes:
/0: 1, /8: 1, /16: 1, /19: 1, /20: 1, /21: 1, /26: 3, /27: 1
/28: 2, /30: 1, /31: 1, /32: 296, /33: 6, /34: 8, /35: 13, /36: 14
/37: 1, /40: 25, /42: 5, /44: 3, /45: 2, /46: 1, /47: 2, /48: 229
/64: 45, /128: 12
```

Es decir 676 redes IPv6 académicas, lo cual es un número reducido comparado con 8982 redes IPv4 académicas existentes. También podemos observar que la mayoría de redes propagadas por la red Académica Mundial son /32 y /48, seguidas por algunas /64

676 prefijos IPv6 académicos vs 8982 prefijos IPv4 académicos, dato tomado en Septiembre 2010

y /40.

Con todos estos pasos realizados anteriormente, el router CE de la Universidad ya conoce todas las rutas hacia las redes académicas, aprendidas por el iBGP, y por medio del tunnelBroker ya se tiene acceso a Internet Comercial también.

Para comprobar las conexiones, se realizará una búsqueda de rutas desde un router externo a Ecuador, y que tenga red Académica e Internet comercial, en este caso se utilizara el servicio de router-views para ir verificando los cambios realizados.

Antes de realizar los cambios se puede constatar que la única ruta para llegar a la red de la Universidad es por medio de la red del proveedor del tunnel Broker.

```
route-views show ipv6 route 2001:470:d81f::/48
Routing entry for 2001:470::/32
Known via ”bgp 6447”, distance 20, metric 1, type external
Route count is 1/1, share count 0
Routing paths:
2001:470:0:1A::1
Last updated 1w2d ago
```

Por lo que fue necesario publicar la nueva red IPv6 de la Universidad desde el router PE de CEDIA en la frontera (AS 27841), que hace peering con el router PE de CLARA (AS 27750), para ello se agrega la línea *network 2001:470:d81f::/48* en el BGP de CEDIA, quedando de la siguiente manera:

```
router bgp 65001
bgp confederation identifier 27841
..
neighbor 2001:1348:1:B::1 remote-as 27750
...
address-family ipv6
neighbor 2001:1348:1:B::1 activate
network 2001:470:D81F::/48
exit-address-family
```

De donde podemos observar que el numero de AS es el 27841 (CEDIA Ecuador), y que hace peering con el vecino que es el AS27750 (redCLARA), también que en la sección *address-family ipv6* están algunas redes que se publican, entre ellas la nueva 2001:470:d81f::/48. Luego de modificado este parámetro solo se esperó pocos segundos

route-views: Proyecto iniciado por la Universidad de Oregon, que fue originalmente creado como una herramienta para poder obtener información acerca de enrutamiento desde la perspectiva de diferentes localizaciones

para que estos cambios empiecen a verse desde otros sitios. Específicamente para este cambio se espero poco más de un minuto y desde un equipo en la red Internet2 ya se visualizó lo siguiente:

```
route-views# show ipv6 route 2001:470:d81f::/48
Routing entry for 2001:470:D81F::/48
Known via ”bgp 6447”, distance 20, metric 0, type external
Route count is 1/1, share count 0
Routing paths:
2001:388:1::16
Last updated 00:01:08 ago
```

Donde se ve claramente que la ruta de salida cambió, además al realizar consultas sobre cuáles son los caminos disponibles para llegar a la red desde route-views, se obtuvo los siguientes AS que hay que pasar para poder llegar a la red:

```
route-views show bgp ipv6 unicast 2001:470:d81f::/48
BGP routing table entry for 2001:470:D81F::/48, version 4437714
Paths: (5 available, best #3, table Default)
Not advertised to any peer
3277 3267 2603 11537 27750 27841
2001:B08:2:280::4:100 from 2001:B08:2:280::4:100 (194.85.4.16)
Origin IGP, localpref 100, valid, external
7575 11537 27750 27841
2001:388:1::13 from 2001:388:1::13 (202.158.192.19)
Origin IGP, localpref 100, valid, external
Community: 7575:1001 7575:2022 7575:6003 7575:8003 11537:2501
7575 11537 27750 27841
2001:388:1::16 from 2001:388:1::16 (202.158.192.22)
Origin IGP, localpref 100, valid, external, best
Community: 7575:1001 7575:2022 7575:6003 7575:8003 11537:2501
101 101 27750 27841
2001:1860::223 from 2001:1860::223 (209.124.176.223)
Origin IGP, localpref 100, valid, external
Community: 101:20400 101:22200
Extended Community: RT:101:22200
3582 4600 11537 27750 27841
2001:468:D01:FD::A from 2001:468:D01:FD::A (128.223.253.10)
Origin IGP, localpref 100, valid, external
Community: 3582:567 4600:99
```

Se comprueba que para llegar al AS27841 pasa por el AS2770 es decir, ya se encuentra publicado por la red Académica mundial. Como última prueba se coloca un traceroute al router de frontera de la Universidad.

```
route-views traceroute 2001:470:d81f:8000::2

Type escape sequence to abort.
Tracing the route to 2001:470:D81F:8000::2

1 vl-51-gw.uoregon.edu (2001:468:D01:33::1) [AS 11537] 216 msec 212 msec 216 msec
2 vl-3.uonet9-gw.uoregon.edu (2001:468:D01:3::9) [AS 11537] 272 msec 208 msec 204 msec
3 2001:468:D00:2::1 [AS 11537] 208 msec 4 msec 0 msec
4 2001:468:FF:54D::1 [AS 11537] 72 msec 24 msec 24 msec
5 2001:468:FF:305::1 [AS 11537] 56 msec 220 msec 208 msec
6 xe-2-3-0.0.rtr.atla.net.internet2.edu (2001:468:FF:1C2::2) [AS 11537] 216 msec 208 msec 216 msec
7 2001:468:FF:109::2 [AS 11537] 208 msec 232 msec 272 msec
8 2001:468:FF:18C5::2 [AS 11537] 272 msec 508 msec 268 msec
9 2001:1348::25 [AS 27750] 456 msec 312 msec 308 msec
10 2001:1348::22 [AS 27750] 336 msec 336 msec 340 msec
11 2001:1348::4E [AS 27750] 356 msec 356 msec 368 msec
12 2001:1348:1:9::2 [AS 27750] 356 msec 356 msec 356 msec
13 2800:2A0:1:B09::B [AS 19169] 360 msec 364 msec 364 msec
14 routerFrontera.ucuenca.edu.ec (2001:470:D81F:8000::2) [AS 27841] 360 msec 364 msec 360 msec
```

Al finalizar este ruteo se obtuvo multihomed, es decir la misma red de la universidad se publica por varios proveedores, el primer proveedor Internet Comercial por Hurricane Electric, y el segundo proveedor la red Académica por medio de CEDIA. La red 2001:480:d81f::/40 se publica por ambas redes, y puede ser alcanzada indiferentemente por cualquiera de las dos, el diagrama de conexión de la Universidad de Cuenca quedaría como en la figura 11:

Ahora, que ya se tiene multihomed es necesario probar que no solamente se tenga acceso por red Académica, sino también por Internet Comercial, para ello se realizó una prueba de traceroute desde un equipo en Alemania que solamente tenga Internet Comercial, hacia una IP de la Universidad 2001:470:d81f:B002::2 se obtiene:

berkom.blazing.de: Sitio para testers de IPv6, permite realizar ciertos comandos básicos como traceroute y ping, su ip es 2a01:30:100a:0:203:baff:fe2d:6efa

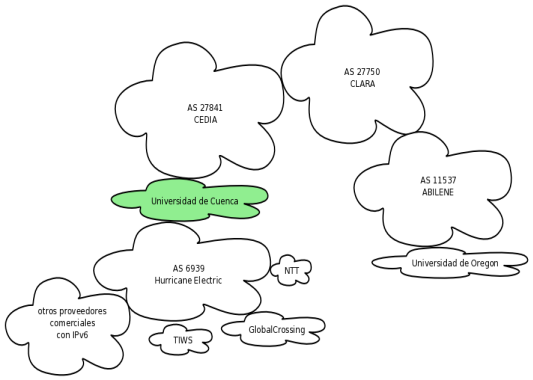

Figura 11: Modelo Multihomed para la Universidad de Cuenca

Results:
1 2a01:30:100a::1 4.793 ms 0.666 ms 0.316 ms
2 2a01:30:1e0f:1::5 22.458 ms 23.399 ms 21.889 ms
3 2a01:30:1e0f:1::a 29.390 ms 28.902 ms 29.595 ms
4 2001:470:15:7a::1 31.189 ms 30.765 ms 31.343 ms
5 gige-g2-5.core1.fra1.he.net (2001:470:0:a5::1) 30.620 ms 31.076 ms 39.747 ms
6 10gigabitethernet1-4.core1.ams1.he.net (2001:470:0:47::1) 38.774 ms 46.219 ms 36.800 ms
7 10gigabitethernet1-4.core1.lon1.he.net (2001:470:0:3f::1) 45.635 ms 45.561 ms 46.017 ms
8 10gigabitethernet4-4.core1.nyc4.he.net (2001:470:0:128::1) 113.419 ms 114.599 ms 122.772 ms
9 10gigabitethernet2-3.core1.ash1.he.net (2001:470:0:36::1) 119.351 ms 120.251 ms 124.036 ms
10 10gigabitethernet1-2.core1.atl1.he.net (2001:470:0:ab::2) 139.624 ms 146.333 ms 149.909 ms
11 10gigabitethernet3-2.core1.mia1.he.net (2001:470:0:a6::1) 154.980 ms 153.914 ms 153.625 ms
12 1g-bge0.tserv12.mia1.ipv6.he.net (2001:470:0:8c::2) 155.973 ms 155.376 ms 156.491 ms
13 2001:470:4:72::2 249.214 ms 248.020 ms 248.370 ms
14 2001:470:d81f:B002::2 251.425 ms 259.252 ms 247.615 ms

Donde se puede observar que el camino tomado es Alemania, Amsterdam, Londres, NewYork, Atlanta, Miami, y últimos saltos el enlace de tunnel Broker y enlaces ya en

la Universidad de Cuenca, pero ninguno de ellos pasa por las redes académicas como Geant, Internet2 o red CLARA, con lo que se confirma que también se tiene acceso por IPv6 en Internet Comercial.

El modelo usado hasta diciembre del 2010 fue un modelo que también es utilizado actualmente por ciertas universidades que desean tener el servicio de IPv6 Comercial y académico pero que no tienen IPv6 nativo de parte de su proveedor de Internet.

Como se indico en capítulos anteriores, este modelo es usado cuando la Universidad no posee su AS propio ni sus direcciones IPv6 propias, y es válido porque el proveedor de Internet Comercial no proveía el servicio IPv6 nativo, el cual cambió cuando ya lo hizo.

7.6. DMZ

En una red IPv4 la zona desmilitarizada es el lugar en donde se encuentran los servidores institucionales que son vistos en Internet. Estos normalmente están protegidos por un firewall con reglas muy estrictas, y son accedidos por medio de NAT, aquí están servidores como portales Web, correo electrónico corporativo, servidor NTP, servidor DNS, servidores de aplicaciones, entre otros.

El firewall es el responsable de la seguridad la red interna, así como de la DMZ, el firewall se encarga de inspeccionar los paquetes que pasan por sus interfaces, y bloquea o permite su reenvío, dependiendo de las reglas, esta protección permite que los servidores internos así como los clientes estén protegidos de ataques externos.

Dentro de los modelos de firewalls tenemos:

Single Firewall: Es el modelo de seguridad básico donde se tiene un solo firewall con tres interfaces, una para la red interna, otra para la red externa y otra para la DMZ como indica la figura 12:

Dual Firewall: En este modelo de firewall la seguridad se incrementa, pues se tiene dos firewalls trabajando para proteger la red interna, como indica la figura 13:

La Universidad de Cuenca tiene el modelo de Single Firewall, con un Firewall modelo Cisco ASA 5520, con interfaces Inside, Ouside, DMZ0, trabajando con IPv4, pero al tener el ASA soporte para IPv6 se realiza un DualStack, y colocando las IPs según el diseño propuesto, y la configuración realizada fue la siguiente:

Stateful Firewall: Tercera generación de firewalls que realiza inspección y seguimiento de cada uno de paquetes existentes

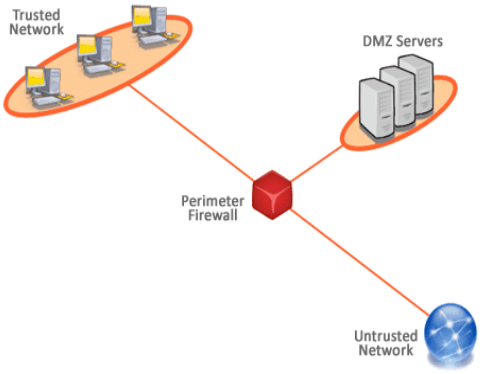

Figura 12: Modelo Single Firewall

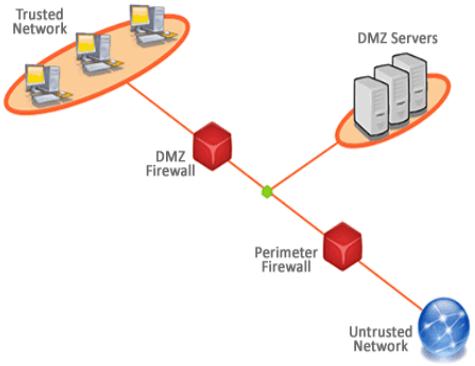

Figura 13: Modelo Dual Firewall

```
interface GigabitEthernet0/0
nameif outside
security-level 0
ipv6 address 2001:470:d81f:8001::2/64
ipv6 enable
ipv6 nd suppress-ra
!
interface GigabitEthernet0/1
nameif inside
security-level 100
ipv6 address 2001:470:d81f::1/64
ipv6 enable
ipv6 nd suppress-ra
! interface GigabitEthernet0/2
nameif DMZ1
security-level 50
ipv6 address 2001:470:d81f:8002::1/64
ipv6 enable
ipv6 nd suppress-ra
```

Se aprecia tres interfaces, GigabitEthernet0/0 que está configurado como OUTSIDE, es decir esta interfaz se conecta al router externo de la Universidad, se coloco el *ipv6 address 2001:470:d81f:8001::2/64* y el comando *ipv6 enable* para activar la pila IPv6 en esta interfaz, dado que en este enlace no va a existir usuarios finales, no es necesario activar el protocolo Network Discovery para que automáticamente descubran el IP del router, ya las direcciones colocadas en toda esta red son estáticas.

De la misma manera se configura la interfaz GigabitEthernet0/1 con la dirección *ipv6 address 2001:470:d81f::1/64* según el diseño planteado, esta interfaz Inside se conecta directamente al switch Core de la Universidad, por lo que tampoco existirán usuarios finales en esta subred, es así que se coloca el comando *ipv6 nd suppress-ra* para bloquear el Network Discovery.

Como última interfaz está la GigabitEthernet0/2 que pertenece a la DMZ de la Universidad y se coloca la dirección *ipv6 address 2001:470:d81f:8002::1/64*, igualmente se cancela el Network Discovery para esta subred, dado que todos los servidores deben tener IP estática.

Se otorga una red /64 para la DMZ, existe en este caso diferencias con respecto al modelo de red en IPv4, normalmente en una DMZ en IPv4 las direcciones que se configuran en los servidores son direcciones privadas, ahora cada servidor tendrá al menos una dirección tipo local y una dirección tipo global de IPv6, dado que la dirección IPv6 local no saldrá de la red no es necesario tener políticas de seguridad en el firewall para este tipo de direcciones, pero en el caso de las direcciones tipo global, el firewall deberá permitir solamente el ingreso a los puertos de los servicios que los servidores entregan solamente.

7.7. Cambio desde red comercial usando túnel a red IPv6 comercial nativa

Desde el inicio del proyecto hasta finales del 2010 se usó la arquitectura e IPs indicadas en la figura 7, pero con la llegada del IPv6 nativo a finales de año fue necesario cambiar el diseño de la red a la mostrada en la figura 8, así como el prefijo usado, los cambios fueron:

- Cambio del prefijo de IPv6, de 2001:470:d81f::/48 a 2800:68:c::/48, lo que implica

Network Discovery IPv6: definido en el rfc2461

cambio en los equipos activos de red LAN, y cambio de prefijo también en los servidores.

- Se realizó la eliminación del router intermedio entre el CPE y el firewall, es decir el router 2800.
- En el router CPE se desactivó el túnel.
- Se eliminó la ruta predeterminada que enviaba los datos por el túnel.
- Se hizo un cambio en el router PE de CEDIA en Guayaquil, cambiando en la configuración del BGP del prefijo 2001:470:d81f::/48 al prefijo 2800:68:c::/48.
- Se hizo un peering de BGP desde el CPE de la Universidad hasta el router PE del ISP nacional, ya que este nuevo peering es el que sustituye al viejo túnel.
- Dentro de las VLANs en la Universidad se hizo el cambio de prefijo, cambiando el parámetro del comando **prefix** en cada una de las VLANs.

Con estos cambios que se realizaron en el lapso de unos pocos días se pudo empezar a enviar todo el tráfico por IPv6 nativo, y cuyo diseño e implementación queda en producción hasta que la Universidad de Cuenca compre su propio rango de IPv6 y Sistema Autónomo.

7.8. DNS

El servicio de DNS es uno de los servicios más importantes en IPv6, y que debe ser configurado correctamente para un buen funcionamiento. Para iniciar la configuración del DNS es necesario definir si se va a realizar en servidores de producción o de desarrollo, ya que una falla en la configuración puede traer varios problemas.

Cuando se realiza una consulta de DNS se tiene un camino ya predefinido que se sigue para obtener una respuesta:

1. Consultar a los DNS root Servers
2. Consultar al ccTDL en el caso de que la consulta sea de un dominio de país, o a un TLD en caso de ser un dominio general como .com, .net .edu, etc.

ccTDL: Country Code Top Level Domain
TLD: Top Level Domain

Servidor A	Verisign, Virginia, USA.
Servidor B	Information Sciences Institute, USA.
Servidor C	Cogent Communications, Virginia, USA.
Servidor D	University of Maryland, USA.
Servidor E	NASA Ames Research Center, California, USA.
Servidor F	Internet Systems Consortium, Inc, USA.
Servidor G	U.S. DOD Network Information Center, USA.
Servidor H	U.S. Army Research Lab, Maryland, USA.
Servidor I	Netnod (formerly Autonomica), Suecia.
Servidor J	VeriSign, Virginia, USA.
Servidor K	RIPE-NCC, Londres, Inglaterra.
Servidor L	ICANN , California, USA.
Servidor M	Wide Project, Universidad de Tokyo, Japón.

Cuadro 3: Root Servers

3.

Internet tiene algunos servidores DNS que son los raíz o llamados root-servers, específicamente son 13, estos 13 servidores están geográficamente separados, 10 en Estados Unidos, 1 en Estocolmo, 1 en Londres y 1 en Japón, son nombrados desde la A hasta la M, y son los mostrados en la tabla 3 :

Dado que existe un límite técnico para la agregación de más root-servers, la solución fué encontrar una manera de poder duplicarlos, permitiendo que existan varias copias usando la misma IP, es por ello que se utilizó anycast.

Anycast en fue aplicado en los root-servers, lo que hace es permitir que una misma IP, ya sea IPv4 o IPv6, pueda estar en lugares geográficamente diferentes, tal como lo muestra la figura 14, para ello lo que se hace es conectar el servidor espejo al AS de destino publicando la red del root server como una /24, esta métrica es utilizada cuando en caso de haber un corte en la red, BGP reconocerá el problema y enviará el requerimiento al /23 del root server original y de esta manera recibe la solicitud que va en un paquete UDP el cual no tiene problemas con tener varias copias ya que UDP es un protocolo orientado a no conexión. Con el uso de anycast se logró implantar un total de 246 root-servers incluyendo las copias alrededor de todo el mundo, de los cuales 10 de los 13 ya tienen asignada una dirección IPv6, pero no todos las copias espejo tienen esta capacidad.

De esta manera y con esta técnica de anycast no solo se tiene 13 root-servers, sino que existe espejos de estos en todo el mundo, en el caso de Ecuador tenemos una copia

Copia DNS root-server F: En Ecuador tenemos una copia del servidor root server alojado en el NAP en Quito

de uno de ellos para una rápida consulta de DNS, y este se encuentra en el NAP.

Figura 14: Root Servers a nivel mundial

En el caso de Ecuador, la copia del root server F del Internet Systems Consortium con la IP anycast 192.5.5.241 localizado físicamente en el NAP de Ecuador de la matriz Quito. Realizando un traceroute a la IP indicada se puede obtener lo siguiente:

```
1 hospitalidad.16.172.in-addr.arpa (172.16.15.1) 1.400 ms 1.699 ms 1.877 ms
2 host-200-110-77-221.cue.telconet.net (200.110.77.221) 1.056 ms 1.045 ms 1.016 ms
3 host-190-95-243-121.cue.telconet.net (190.95.243.121) 1.438 ms 1.422 ms 1.503 ms
4 10.201.33.236 (10.201.33.236) 5.376 ms 5.449 ms 5.490 ms
5 10.201.111.45 (10.201.111.45) 5.284 ms 5.261 ms 5.330 ms
6 10.201.111.46 (10.201.111.46) 5.468 ms 4.864 ms 4.903 ms
7 10.201.111.150 (10.201.111.150) 13.126 ms 13.027 ms 13.010 ms
8 10.201.211.45 (10.201.211.45) 13.008 ms 12.986 ms 13.000 ms
9 10.201.21.122 (10.201.21.122) 14.457 ms 14.436 ms 14.411 ms
10 nap-ec.r1.uio1.isc.org (200.1.6.15) 15.107 ms 15.196 ms 15.332 ms
11 f.root-servers.net (192.5.5.241) 14.667 ms 14.646 ms 14.680 ms
```

NAP: Network Access Point, Es un punto de intercambio público, donde los ISPs pueden conectarse entre sí para hacer un intercambio de tráfico dentro de su misma zona o país.

Se puede ver que se encuentra a tan solo 24ms es decir dentro de Ecuador, usando la IP que originalmente esta en California EEUU, aunque el IPv6 aun no se encuentra haciendo peering hacia los ISPs de Ecuador.

El segundo paso en la resolución de nombres luego de consultar a los root-servers, son los ccTLD, en el caso de Ecuador NIC.ec que es quien administra el ccTLD .EC hasta la fecha tiene solo un servidor de nombres en IPv6, el cual se encuentra en Europa y es un servicio proporcionado por Afilias el cual da servicio tanto en IPv4 como en IPv6 para todos los dominios .ec.

Realizando una consulta para el sufijo de Ecuador .ec obtenemos:

```
;; QUESTION SECTION:
;ec. IN NS

;; ANSWER SECTION:
ec. 129400 IN NS sns-pb.isc.org.
ec. 129400 IN NS dns1.nic.ec.
ec. 129400 IN NS dns2.nic.ec.
ec. 129400 IN NS dns3.nic.ec.
ec. 129400 IN NS dns4.nic.ec.
```

Donde solo la primera tiene IPv4 e IPv6, y los demás solo tienen IPv4, pero todas ellas pueden resolver consultas IPv4 asi como IPv6, en el caso de la Universidad de Cuenca se tiene registrado en NIC.ec cuatro servidores DNS autoritativos donde dns1.ucuenca.edu.ec es un servidor master que tiene direcciones tipo A y AAAA, tal como se ver en la consulta realizada al @dns1.nic.ec.

NIC.ec: Network Information Center Ecuador

Afilias: Empresa internacional da servicios de DNS autoritativo a gTLDs, ccTLDs, permitiendo que los servidores de Afilias sean un nameserver del TLD respondiendo a consultas DNS

Authoritative name server: Servidor DNS que mantiene el archivo de registros de las zonas a las cuales su zona padre ha apuntado como servidor DNS para que responda a las consultas de la zona configurada, es decir responde a consultas de nombres de subdominio de un dominio específico

Master DNS Server: Servidor DNS que almacena una copia original de los registros de zona

```
;; QUESTION SECTION:
;ucuenca.edu.ec. IN NS

;; AUTHORITY SECTION:
ucuenca.edu.ec. 129600 IN NS ns1.he.net.
ucuenca.edu.ec. 129600 IN NS ns3.he.net.
ucuenca.edu.ec. 129600 IN NS dns1.ucuenca.edu.ec.
ucuenca.edu.ec. 129600 IN NS ns2.he.net.

;; ADDITIONAL SECTION:
dns1.ucuenca.edu.ec. 129600 IN A 192.188.48.3
dns1.ucuenca.edu.ec. 129600 IN AAAA 2800:68:c:8002::3
```

Internamente en la DMZ la Universidad se encuentra el servidor dns1.ucuenca.edu.ec que es un servidor DNS autoritativo master configurado en dual stack para la zona ucuenca.edu.ec, es decir es quien maneja todos los nombres de subdominios para el dominio principal de la Universidad, y tiene 3 servidores autoritativos adicionales que se encuentran en modo esclavo.

Es de esta manera que la Universidad de Cuenca en la parte de DNS se encuentra resolviendo nombres de dominio ucuenca.edu.ec incluso en un ambiente de solo-IPv6, es decir desde el cliente que consulta, hasta el que los servidores autoritativos respondan a la consulta, todo el camino con IPv6.

Con lo referente a la inclusión de la doble pila dentro del servidor autoritativo de la Universidad fue necesario primeramente agregarle una IPv6 global al mismo, agregando la siguiente configuración en la interfaz eth0 del servidor el cual es un GNU/Linux:

```
DEVICE=eth0
IPV6INIT=yes
IPV6_AUTOCONF=no
IPV6ADDR=2800:68:c:8002::3/64
IPV6_DEFAULTGW=2800:68:c:8002::1
```

Los parámetros configurados son:

- IPV6INIT: Permite habilitar IPv6 en la interfaz.

Slave Authoritative name server: Servidor Autoritativo, que cada cierto tiempo previamente configurado, que obtiene una copia de todos los registros de zona de su servidor autoritativo master

Solo-Ipv6: Término usado normalmente para describir ambientes donde no existe una doble pila IPv4-IPv6 sino solamente IPv6

- IPV6_AUTOCONF: El servidor no aceptará direcciones provistas por los RA existentes en la red.
- IPV6ADDR: Ya que el servidor no se autoconfigura, es necesario especificar la dirección IPv6 asignada así como la máscara, ya que es una red final se coloca la máscara /64.
- IPV6_DEFAULTGW: Como el servidor es configurado estáticamente, se debe obligatoriamente colocar el gateway de salida, en este caso es la IP del firewall visto desde la red de la DMZ.

En lo que se refiere a manejo de DNS el aplicativo usado es BIND el cual puede ser configurado de varias maneras, como un servidor dns recursivo cache, o DNS autoritativo trabajando tanto de master como en modo esclavo, sirviendo registros tanto de la zona directa o zona reversa, sea en IPv4 como en IPv6 para uno o varios dominios, en la Universidad de Cuenca se tiene uno sirviendo como DNS autoritativo y otro como servidor DNS recursivo.

En lo concerniente a la configuración de BIND, antes de la realización de este proyecto de tesis se tenía una configuración de respuesta de solicitudes solamente en IPv4, es decir las respuestas siempre eran tipo A, lo necesario fue agregarle todas las respuestas AAAA es decir tipo IPv6 para los subdominios existentes, y también agregar un registro de zonas inversas para el rango IPv6 actual.

BIND tiene varios archivos de configuración, el principal de ellos es /etc/named.conf (dentro o fuera de un chroot) el cual requiere los siguientes parámetros:

- Apertura del puerto 53 en IPv6: para este paso es necesario agregar dentro de las opciones una linea *query-source-v6 port 53;*, con ello queda configurado que el puerto 53 será el que escuche requerimientos.
- Abrir la interfaz: colocando la opción *listen-on-v6* y a continuación la dirección IPv6, de esta manera se consigue que dicha interfaz se coloque en modo LISTEN.
- Creación de zona directa: En lo referente a las zonas directas se tendrá una zona ucuenca.edu.ec que será tipo master y dentro de la cual se colocara los registros

BIND (Berkeley Internet Name Domain): Servidor DNS mantenido por Internet Systems Consortium

DNS Zona Directa: registros que al consultar un nombre retornan una IP

DNS Zona Reversa: registros que al consultar una IP retornan su nombre

chroot: En sistemas *nix se refiere el aparentar la existencia de un arbol root completo visto desde un programa o daemon, normalmente llamado jaula chroot

A y AAAA. La configuración general de esta zona ucuenca.edu.ec queda de la siguiente manera:

```
zone 'ucuenca.edu.ec' {
type master;
file 'ucuenca.edu.ec.zone';
};
```

Lo que realiza estas líneas es crear una zona padre llamada ucuenca.edu.ec que es de tipo master y cuyo archivo de configuración se llama ucuenca.edu.ec.zone, el cual se modificará posteriormente, ya que IPv4 e IPv6 utilizará el mismo archivo de zona directa.

- Creación de zona reversa IPv6: Para el caso de IPv6 la creación de la zona reversa necesariamente debe estar en un archivo separado que para la zona reversa de IPv4. Para crear la zona reversa IPv6 primero es necesario conocer cuál es el prefijo IPv6 que la Universidad posee. Ya en IPv6 nativo el prefijo es el 2800:68:c::/48. Lo primero que se debe hacer es colocar los primeros 48 bits en formato hexadecimal, escribirlo desde el ultimo al primero, colocando un punto entre cada dígito hexadecimal, de esta manera creamos la zona reversa para el prefijo de direcciones /48 de la Universidad. La configuración queda de la siguiente manera:

```
zone 'c.0.0.0.8.6.0.0.0.0.0.8.2.ip6.arpa' {
type master;
'file c.0.0.0.8.6.0.0.0.0.0.8.2.ip6.arpa';
};
```

Donde la primera línea define la zona reversa, la segunda línea define a este servidor como master para esta zona reversa, y la tercera linea es el nombre del archivo que contiene ya los registros de cada una de las IPs del rango así como el nombre de cada una.

- Configuración de los registros AAAA en la zona directa: Para este paso es necesario abrir el archivo de zona directa, oséa el archivo ucuenca.edu.ec.zone que se encuentra dentro de /var/named/ (o dentro de su chroot en el mismo subdirectorio), en este archivo de texto agregamos los nuevos registros AAAA, por ejemplo en los

siguientes registros, tenemos un registro A y un AAAA para algunos servidores Universitarios como son, portales web, dns, correo, servidor de hora:

```
dns1 IN A 192.188.48.3
dns1 IN AAAA 2800:68:c:8002::3
mail IN A 192.188.48.2
mail IN AAAA 2800:68:c:8002::2
www IN A 192.188.48.17
www IN AAAA 2800:68:c:8002::60
evirtual IN AAAA 2800:68:c:8002::4
rai IN AAAA 2800:68:c:8002::60
feuedemocratica IN AAAA 2800:68:c:8002::60
arq IN AAAA 2800:68:c:8002::60
monitoreo IN AAAA 2800:68:c:16::2
ntp IN AAAA 2800:68:c:8002::5
```

Se puede apreciar por ejemplo que el portal www.ucuenca.edu.ec (ucuenca.edu.ec es la zona directa y www es el subdominio) apunta a la dirección IPv4 (registro A, osea un registro de 32 bits) 192.188.48.17, y también en la siguiente linea apunta a una dirección IPv6 (registro AAAA, es decir a uno de 128 bits) 2800:68:c:8002::60.

- Configuración de los registros PTR en la zona PTR: Para la zona reversa del prefijo 2800:68:c::/48 es necesario crear el archivo llamado *c.0.0.0.8.6.0.0.0.0.8.2.ip6.arpa* y que se debe encontrar dentro de /var/named/ (o dentro de su chroot), para nuestro caso particular, es necesario colocar los registros de mail y de dns1 en nuestra zona inversa, la cual deberá tener los típicos encabezados como registros SOA, NS (de la misma manera que cualquier otra zona directa), y luego de ello ya los registros PTR de IPv6 apuntando a los nombres de cada uno de los IPs, en este ejemplo se realiza el registro DNS reverso del correo mail.ucuenca.edu.ec y del servidor de nombres autoritativo dns1.ucuenca.edu.ec

```
2.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.2.0.0.8 IN PTR mail.ucuenca.edu.ec.
3.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.2.0.0.8 IN PTR dns1.ucuenca.edu.ec.
```

La zona reversa creada de la Universidad es un /48, es decir faltaría definir 80 bits mas (128bits de una dirección IPv6 menos 48bits ya definidos en la zona inversa

que estamos creando, queda 80 bits por definir, es decir 20 hexadecimales), los cuales son colocados en formato hexadecimal, escrito desde el ultimo al primero y separado por puntos.

- Inicializar el servicio: Dependiendo de la distribución de Linux hay varias maneras de iniciar el daemon BIND, por ejemplo una de las maneras es por medio de */etc/init.d/named start*.

- Delegación del nameserver desde NIC.ec: Una vez creado los registros IPv6 en el servidor, iniciado el servicio y sobretodo colocado el IPv6 global en la interfaz del servidor DNS, es tiempo que los 5 servidores de NIC.ec (dns1.nic.ec dns2.nic.ec dns3.nic.ec dns4.nic.ec sns-pb.isc.org) apunten al IPv6 del servidor dns autoritativo de la Universidad de Cuenca, de esta manera cuando se realiza una consulta desde un computador solo-IPv6, los servidores NIC.ec enviaran la consulta de la zona ucuenca.edu.ec al IPv6 asignado como DNS autoritativo.

- Delegación Inversa de DNS: Una vez que ya se tiene funcionando e iniciado el servicio de nombres, es momento de completar la resolución DNS reverso haciendo que el servidor de la Universidad sea el autoritativo para el rango 2800:68:c::/48. Para realizar aquello es necesario realizar una delegación desde los servidores de LACNIC (que es quien asignó el rango a CEDIA y a su vez éste a la Universidad de Cuenca) hacia el servidor de la Universidad de Cuenca, para ello se solicito que CEDIA realice la delegación hacia dns1.ucuenca.edu.ec, cuyos pasos fueron los que se encuentran en las figuras 15, 16 y 17.

Finalizado toda estas configuraciones se realizó una comprobación usando el comando dig, consultando la asignación de los nameservers a los IPs de la Universidad:

Figura 15: Selección de la red 2800:68:c::/48 en el portal de LACNIC

```
dig NS @dns1.nic.ec ucuenca.edu.ec


;; QUESTION SECTION:
;ucuenca.edu.ec. IN NS


;; AUTHORITY SECTION:
ucuenca.edu.ec. 129600 IN NS dns1.ucuenca.edu.ec.


;; ADDITIONAL SECTION: dns1.ucuenca.edu.ec. 129600 IN A 192.188.48.3
dns1.ucuenca.edu.ec. 129600 IN AAAA 2800:68:c:8002::3
```

Se puede ver claramente que al consultar a los DNS de NICEC acerca del dominio ucuenca.edu.ec, ellos retornan los IPs del servidor DNS autoritativo de la Universidad, tanto en v4 como v6.

Figura 16: Delegación del host master para el rango IPv6 de la Universidad

7.9. Correo Electrónico

Para el caso de correo electrónico tenemos varios servicios que activar, uno es usar el SMTP en el servidor de correo y hacerlo trabajar como MTA o usar SMTP para que el servidor reciba correo desde un MUA también se puede configurar el servidor como MDA para entrega de correos a un usuario usando por ejemplo el protocolo POP3 o IMAP.

En el caso de la Universidad de Cuenca se tiene un solo servidor que entrega todos estos servicios, por lo cual hay que configurar tanto para entrega así como para recepción y envío de correos.

El primer paso en la configuración del servidor es la doble pila, para ello se configura la interfaz conectada a la red, agregándole una dirección IPv6 Global dentro del archivo /etc/sysconfig/network-scripts/ifcfg-eth0, agregando las siguientes líneas.

SMTP: Simple Mail Transfer Protocol
MTA (Mail Transfer Agent): servidor de correo que se comunica a otros servidores de correo para transferir correo
MUA (Mail User Agent): Aplicación de usuario que permite el envío y recepción de correos
MDA (Mail Delivery Agent): servidor que entrega correos a el MUA de un usuario especifico
POP3 (Post Office Protocol): Protocolo usado para enviar correos a un MUA
IMAP (Internet message access protocol): protocolo que al igual que POP3 permite entregar correos a los usuarios

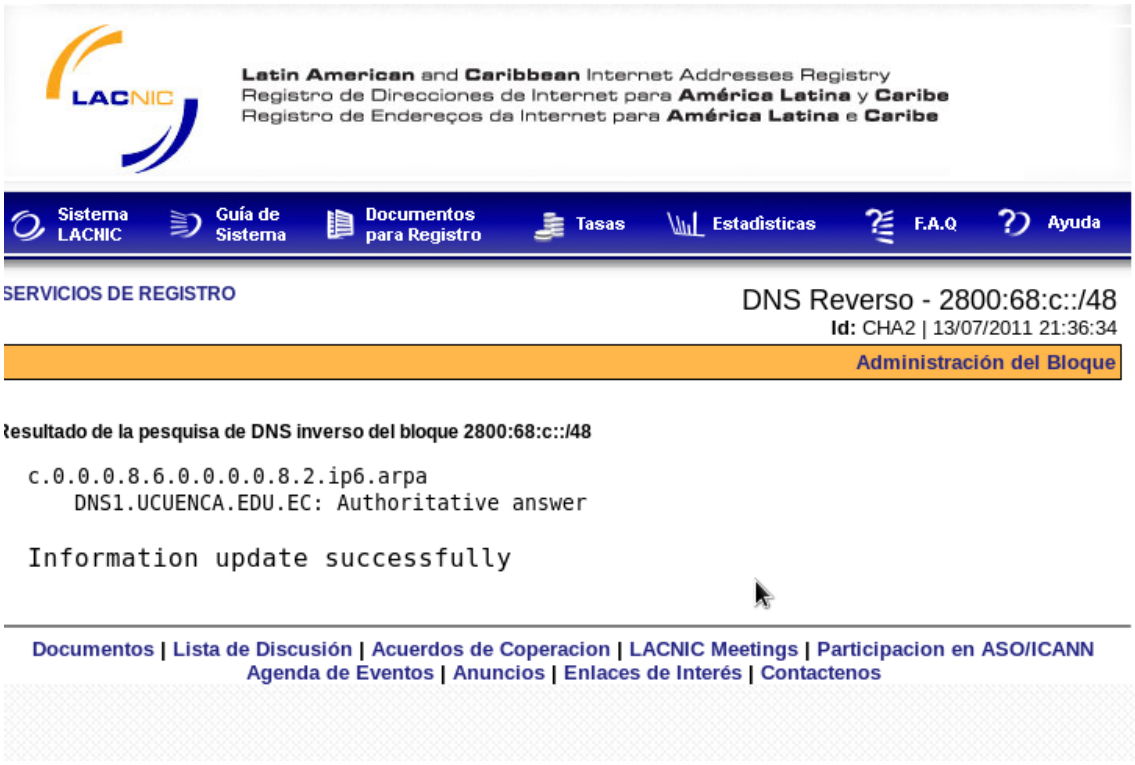

Figura 17: Solicitud de cambio de delegación del rango 2800:68:c::/48 aceptada

```
IPV6INIT=yes
IPV6_AUTOCONF=no
IPV6ADDR=2800:68:c:8002::2/64
IPV6_DEFAULTGW=2800:68:c:8002::1
```

Y posteriormente luego de configurada la dirección y reiniciada la interface es necesario activar los servicios en IPv6, para ello primeramente se realiza una activación de los protocolos necesarios, dependiendo del servicio que se utilice varia, en el caso de la Universidad de Cuenca se utiliza Postfix,aquí es necesario activar los protocolos que se van a usar, por defecto se tiene en el archivo */etc/postfix/main.cf* una línea con el comando: *inet_protocols = ipv4* que lo que hace por defecto es usar solamente IPv4. Hay dos formas de este momento activarlo:

- La primera manera es reemplazando por *inet_protocols = all* con lo cual se activa todos los protocolos existentes en el servidor.
- La segunda manera es agregando en la lista ipv6, es decir sustituyendo la linea por

Postfix: Servidor de correo de código abierto que permite la transferencia de correo entre servidores

inet_protocols = ipv4, ipv6 de esta manera ambos protocolos activan el servicio.

Luego de activados los protocolos, es necesario activar la interface o interfaces para que escuchen uno u otro protocolo, dado que en la Universidad por la cantidad de usuarios (aproximadamente 2000 cuentas de correo) es el mismo servidor utilizado como MTA y como MDA. En el caso del MTA hay que activar el protocolo SMTP, para ello es necesario que en el mismo archivo de configuración main.cf se configure el smtp en IPv6, modificando la linea *smtp_bind_address6 = 2800:68:c:8002::2* se logra que el servicio SMTP sea abierto, colocando la interface en el puerto SMTP en modo LISTEN.

Un parámetro que es importante es el parámetro mynetworks el cual define las redes a las cuales el servidor esta conectado, antes de realizar la actualización a IPv6 solamente debe tener las IPs en versión 4, es necesario agregar de IPv6 la red de localhost, la red fe80 y la subred IPv6 Global pública, quedando de la siguiente manera: *mynetworks = 127.0.0.0/8 10.0.1.0/8 [::1]/128 [fe80::]/10 [2800:68:c:8002::]/64* .

Dentro de las políticas que normalmente se utilizan en Internet para el manejo de spam es colocar a aquellas IPs que no tienen el DNS reverso como IP proveniente de un posible spammer. En pasos anteriores se realizo el DNS reverso de la IP 2800:68:c:8002::2 hacia un registro con el nombre mail.ucuenca.edu.ec, de esta manera queda el servidor sin problemas respecto a este requerimiento. Hay que tomar en cuenta que no quiere decir que el servidor no funcione sin este registro, sino simplemente que el servidor puede ser marcado como spammer en correos de destino, ya que su IP no ha sido debidamente registrada.

7.10. Portales Web

La Universidad de Cuenca usa en la mayoría de los portales software libre para su implementación, normalmente el sistema operativo es un GNU/Linux y como motor de páginas web Apache2. Un aspecto muy importante es que la mayoría de portales se encuentran dentro del mismo servidor y los subdominios se maneja por medio de virtualhost, es decir una servidor con varios registros DNS asociados a la misma IP.

El primer paso para una publicación de un portal es colocar su interfaz en dual stack, para ello se procederá de la misma manera que anteriormente se configuraba las interfaces de servidores GNU/Linux, es decir dentro de su archivo de configuración de interfaz

Apache: Servidor de páginas WEB

se colocará la dirección IPv6:

```
IPV6INIT=yes
IPV6_AUTOCONF=no
IPV6ADDR=2800:68:c:8002::60/64
IPV6_DEFAULTGW=2800:68:c:8002::1
```

Los parámetros configurados son:

- IPV6INIT: Permite habilitar IPv6 en la interfaz.
- IPV6_AUTOCONF: El servidor no aceptará direcciones provistas por los RA existentes en la red.
- IPV6ADDR: Ya que el servidor no se autoconfiguró, es necesario especificar la dirección IPv6 asignada así como la máscara, ya que es una red final se coloca la máscara /64.
- IPV6_DEFAULTGW: Como el servidor es configurado estáticamente, se debe obligatoriamente colocar el gateway de salida, en este caso es la IP del firewall visto desde la red de la DMZ.

Luego de configurado las interfaces es necesario realizar el reinicio de red, dependiendo del tipo de distribución hay que reiniciar las interfaces. Luego de realizado este paso el servidor ya podrá acceder y ser alcanzado por medio de IPv6.

Dentro de lo que se refiere al servidor Apache permite una gran cantidad de configuraciones, y este deberá ser configurado dependiendo de como están creados los portales con IPv4 y subdominios, así como la forma en que esta el DNS aplicado, ya que hay que recordar que lo que se esta realizando es una doble pila, por lo tanto mucho depende de la configuración actual.

Aspectos a tomar en cuenta para la configuración de un servidor de paginas web son:

- Número de portales que se encuentran funcionando en el servidor.
- Verificar si los portales pertenecen a un mismo dominio o a dominios diferentes.
- El número de interfaces y direcciones IP que tiene el servidor.
- El tipo de hosting que se está ofreciendo a los portales, una dirección para cada portal o muchos portales con una misma IP.

Para el caso de la Universidad de Cuenca lo que se refiere a portales web de facultades, departamentos y programas, son todos colocados en un único servidor con una sola interfaz física, a parte sistemas como la plataforma virtual se encuentra en un servidor distinto sin compartir el IP con otros subdominios.

Para el caso más simple que es tener un servidor sin compartir con otros subdominios los pasos para colocar los servicios de apache en dual stack son:

1. En el archivo de configuración /etc/httpd/conf/httpd.conf se debe buscar la linea *Listen* la cual indica el número de puerto en donde se encuentra escuchando peticiones http, hay que colocar una nueva línea donde luego de Listen se encuentre la IPv6 y el número de puerto, por ejemplo: *Listen [2800:68:c:8002::4]:80* en donde 2800:68:c:8002::4 es la dirección IPv6 del servidor del portal de educación Virtual, hay que recordar que siempre es necesario la agregación de corchetes cuando se coloca direcciones IPv6 caso contrario la implementación fallará.

2. Es necesario indicar al servidor Apache la dirección en donde se encuentran las páginas web en el servidor para que cuando un cliente lo solicite este retorne la información solicitada, para ello es necesario buscar dentro del archivo /etc/httpd/conf/httpd.conf la variable DocumentRoot que es la que proporciona el subdirectorio en donde se encuentra las páginas web, y que será la página que aparecerá cuando se coloque el IP anteriormente configurado, por ejemplo en el caso de la plataforma de aprendizaje se colocaría el subdirectorio donde se encuentran las páginas a entregar *DocumentRoot /var/www/moodle*.

3. Cada servidor debe tener un nombre asociado asignado por el nameserver, en el caso de la plataforma virtual que es uno de los portales de la Universidad, hay que indicar a Apache que el nombre es evirtual.ucuenca.edu.ec y se encuentra en el puerto 80, de esta manera cuando se haga solicitudes a dicha dirección, y la petición llegue al servidor Apache solicitando páginas a ese subdominio, Apache retornará la información correspondiente, para ello es necesario configurar la variable ServerName, lo cual se realiza de la siguiente manera: *ServerName evirtual.ucuenca.edu.ec:80*.

4. Luego de terminado toda la configuración es necesario reiniciar el servidor Apache, para ello dependiendo de la distribución hay distintas maneras, una de ellas es enviando el parámetro start a /etc/init.d/httpd, por ejemplo */etc/inid.d/httpd start*.

http (Hypertext Transfer Protocol): Protocolo usado para transferencia de páginas web sin encriptación

Luego de realizado dichas configuraciones es tiempo de realizar pruebas, se puede usar la herramienta telnet, realizando un *telnet ::1 80* desde el mismo servidor, se podrá observar:

```
#telnet ::1 80
Trying ::1...
Connected to ::1.
Escape character is '^]'.
```

Se puede apreciar que al retornar la última línea de mensaje hubo éxito en la conexión, luego de ello se puede hacer un telnet a la IPv6 global, y posteriormente desde un host remoto.

Cuando se da hosting a varios sitios o subdominios, se vuelve necesario realizar configuraciones adicionales dentro del servidor Apache, ya que normalmente se tendrá una sola interfaz de red, con una sola IPv4 y en nuestro caso también una sola dirección IPv6 global, pero varios subdominios dentro del mismo servidor web.

Apache así como otros servidores web para realizar esta tarea lo resuelve manejando VirtualHosts, para la realización de esta configuración se realiza los siguientes pasos:

1. Al igual que cuando se tiene un solo nombre ligado a una IP, es necesario editar el archivo de configuración /etc/httpd/conf/httpd.conf y buscar *Listen* el cual indica el número de puerto e IP en donde se encuentra escuchando peticiones http, en el caso de un servidor con VirtualHosts se coloca simplemente el IP y el puerto, por ejemplo *Listen [2800:68:c:8002::60]:80* , de donde el 2800:68:c:8002::60 es el IPv6 del host que da hosting y 80 el puerto http donde se encuentra escuchando.

2. Ahora es tiempo de activar la característica de VirtualHosts, para ello en la línea *NameVirtualHost* se puede colocar simplemente el parámetro asterisco (*) y lo que hace es escuchar en todas las IPs, en todos los puertos donde se encuentra escuchando, para permitir el uso de VirtualHosts solo en un puerto se ha colocado *NameVirtualHost *:80*.

3. Se debe colocar la parametrización de todos los VirtualHost, para ello se coloca como cabecera el IP y puerto donde se está escuchando, y entre los parámetros importantes a configurar tenemos: el nombre DNS que se está sirviendo, y la direc-

VirtualHosts: Técnica mediante la cual se puede tener una sola IP y varios nombres de dominio hospedados en la misma IP, el browser dentro de las cabeceras HTTP envía el nombre de subdominio que esta solicitando, de esa manera se puede diferenciar a que nombre se esta solicitando

ción de las páginas WEB de donde se están visualizando las páginas. Por ejemplo:

```
VirtualHost *:80
ServerAdmin nombreAdministrador@local.ucuenca.edu.ec
DocumentRoot /var/www/html/prueba
ServerName prueba.ucuenca.edu.ec
ErrorLog logs/prueba.ucuenca.edu.ec-error_log
CustomLog logs/prueba.ucuenca.edu.ec-access_log common
/VirtualHost
```

Así con estas líneas se está entregando páginas web del subdirectorio /var/www/html/prueba cuando un cliente abre un socket hacia el IP 2800:68:c:8002::60 del puerto 80, al conectarse el browser solicitará en su cabecera el dominio prueba.ucuenca.edu.ec.

4. Como último paso esta el reiniciar el servidor apache, y para realizar una prueba se realizará un telnet desde un cliente hacia el servidor para probar correcta configuración del virtualhost llamado prueba.ucuenca.edu.ec.

   Para probar la configuración se realizará un telnet a la IPv6 del servicio:

```
#telnet 2800:68:c:8002::60 80
Trying 2800:68:c:8002::60...
Connected to 2800:68:c:8002::60.
Escape character is '^]'.
get / http/1.1
host: prueba.ucuenca.edu.ec



HTTP/1.1 200 OK
Date: Sat, 19 Feb 2011 22:28:39 GMT
Server: Apache/2.2.3 (CentOS)
X-Powered-By: PHP/5.3.6
Set-Cookie:  379cba4f8b6a73ac9504eb469157df1e=mu7r75onm9g9gctrcma78344g7;
path=/
P3P: CP="NOI ADM DEV PSAi COM NAV OUR OTRo STP IND DEM"
Expires: Mon, 1 Jan 2001 00:00:00 GMT
Last-Modified: Sat, 19 Feb 2011 22:28:42 GMT
Cache-Control: post-check=0, pre-check=0
Pragma: no-cache
Connection: close
Transfer-Encoding: chunked
Content-Type: text/html; charset=utf-8
```

De esta manera comprobamos que realmente se encuentra bien la configuración del VirtualHost en Apache, ya que respondió correctamente a las solicitudes requeridas.

Dentro de la Universidad de Cuenca es de mucha utilidad el uso de VirtualHosts pues con ello se puede crecer sin necesidad de tener una gran cantidad de IPs configuradas, y sobretodo la seguridad se lo hace a una única IPv4 e IPv6, lo cual simplifica el trabajo del administrador referente a la seguridad de la red.

La habilitación de un portal web en IPv6 requiere un buen nivel de conocimientos, y lo más importante es tener todo totalmente funcionando y correctamente, es decir desde el enrutamiento, seguridad, servicios, dns, ya que si uno de estos puntos tiene proble-

mas o no está funcionando completamente, el portal se demorará o fallará, haciendo que el usuario tenga una mala experiencia en navegación, y ya que el portal es la cara que la Universidad presenta en Internet, es una fase de suma importancia el realizarlo correctamente y sin errores.

7.11. ntp

Uno de los servicios no tan instalados en las instituciones es el servidor de hora de red o NTP, es un servicio de suma importancia para el registro de bitácoras en equipos activos, servidores, computadores, dispositivos de uso general, pues si los relojes de los dispositivos no se sincronizan, el administrador tendrá problemas para verificar los registros en el caso de los dispositivos activos, y en el caso de servidores web si no está bien configurado la hora y la zona horaria posiblemente los correos lleguen como spam, si los computadores no se sincronizan a un servidor de hora, luego de algunos meses estos estarán con la hora incorrecta, ya que segundo a segundo los relojes del computador van perdiendo milisegundos.

NTP es un proyecto iniciado desde la década de los 80, y su versión 3 esta documentada en el rfc1305, cuyo objetivo principal es lograr la sincronización de la hora un equipo cliente tomando la hora de un servidor NTP, los servidores NTP están jerarquizados, es decir hay aquellos que están conectados a un reloj GPS o a un reloj atómico y son llamados servidores NTP stratum 1.

En un nivel inferior están los servidores NTP de stratum 2, que son los que están conectados a los Stratum 1 por medio de la red y obtienen la hora de los servidores NTP stratum 1 usando el protocolo NTP, tienen direcciones IPv4 públicas o en el caso de IPv6 son direcciones globales.

En este proyecto de tesis se planteo levantar un servidor NTP, ya que la posibilidad de implementar un servidor NTP stratum 1 o 2 están fuera del alcance de esta tesis por los recursos necesarios, el servidor a continuación es uno tipo Stratum 3.

Para la implementación del servidor NTP stratum 3 de la Universidad de Cuenca, este se lo realiza en un servidor GNU/Linux, el cual debe tener una dirección IPv6 global.

Primeramente es necesario colocar un IPv6 al equipo, para ello se configura el archivo /etc/sysconfig/network-scripts/ifcfg-eth0 con la siguiente información:

NTP (Network Time Protocol: Protocolo usado para sincronizar el reloj del computador con servidores que se encuentran en la LAN o Internet, los cuales se sincronizan con servidores que utilizan tecnología de relojes GPS o relojes atómicos)

```
DEVICE=eth0
IPV6INIT=yes
IPV6_AUTOCONF=no
IPV6ADDR=2800:68:c:8002::5/64
IPV6_DEFAULTGW=2800:68:c:8002::1
```

Con esta configuración el servidor que se encuentra en la DMZ ya puede ser alcanzado por Internet Comercial y redes académicas, el siguiente paso es la configuración del servicio.

Para la implementación del servidor se utilizará el paquete ntp versión 4.2.2 el cual soporta tanto IPv4 como IPv6, una vez instalado el servidor es necesario crear el archivo de configuración /etc/ntp.conf con las siguientes líneas:

- **server**: esta opción permite colocar los servidores de nivel superior a los que se les consultará la hora correcta, normalmente son servidores stratum 2 o de stratum 1, en el caso de la Universidad de Cuenca al ser parte de las redes académicas el servidor stratum 2 en IPv6 mas cercano se encuentra en Brasil, específicamente en SaoPaulo, Rio de Janeiro y Brasilia, por lo cual queda de la siguiente manera la configuración *server a.ntp.br*.

- **restrict servidor NTP**: este parámetro permite controlar los permisos que tienen otros servidores hacia el nuestro, es una recomendación no permitir que cambien la configuración en tiempo de ejecución del servidor NTP y que tampoco se les conteste consultas tipo NTP, de esta manera el servidor a.ntp.br quedará con las siguientes restricciones o parámetros: *restrict a.ntp.br nomodify notrap noquery*.

- **restrict red LAN**: el parámetro restrict también es usado para colocar la o las redes a las cuales se les permite hacer consultas, en el caso de la Universidad de Cuenca, donde la red IPv6 es la 2800:68:c::/48, la línea que permite que la red de la Universidad realice consultas NTP al servidor es: *restrict -6 2800:68:c:: mask ffff:ffff:ffff:: nomodify notrap nopeer*.

- **restrict localhost6**: Se permite que se realice un monitoreo y control total desde la dirección local, para ello se agrega la siguiente línea: *restrict -6 ::1* la cual da acceso total al servidor NTP universitario.

- **restrict por defecto:** Luego de colocado el rango de direcciones permitidas es necesario bloquear el acceso general, ya que el servidor es exclusivo para la Uni-

versidad, se bloquea las solicitudes que lleguen desde redes no autorizadas, esto se realiza con la agregación de la linea *restrict -6 default ignore*, de esta manera cuando un IP no autorizado en las listas superiores consulte la hora, recibirá una respuesta negativa de parte del servidor.

De esta manera queda el servidor preparado para consultas de hora usando transporte IPv6, ahora es necesario que los servidores así como equipos activos lo usen como servidor local de hora, actualmente al menos los servidores universitarios así como los dispositivos de red activos se encuentran ya actualizados con la hora del servidor NTP. Siempre que se desea que los usuarios utilicen un servicio es recomendable ponerle un nombre no publicar solamente la IP, es por ello que el nombre del servidor de hora oficial dentro de la Universidad de Cuenca se llama ntp.ucuenca.edu.ec, el cual se encuentra trabajando en IPv6, permitiendo consultas de parte de su red interna.

8. IPsec

8.1. Introducción

IPsec permite realizar comunicaciones seguras entre dos computadores o entre dos redes, se basa en estándares de la IETF, IPsec es una herramienta poderosa para poner seguridad en la capa de red, lo que permite que toda la información que se encuentre en capas superiores viaje de una manera encriptada. IPsec se encuentra regulado en varios documentos: RFC2401, RFC2402, RFC2406, RFC2407, en ellos se puede encontrar los detalles acerca de su arquitectura. Dentro de la Universidad de Cuenca hay datos que son confidenciales, los cuales deben ser enviados por canales seguros entre ellos, en la actualidad se transmiten por medio de la red Universitaria sin encriptación a nivel de capa 3, sino solamente usando encriptación (en caso que exista) en la capa de aplicación. Uno de los objetivos de este proyecto de tesis es presentar las ventajas de este protocolo, y por medio de pruebas de laboratorio asegurar el canal y transmitir datos, para que de esta manera, se empiece a pensar en asegurar la comunicación entre servidores e incluso entre redes de servidores, ya que cualquier momento podría existir un ataque de man-in-the-middle, a lo cual los servidores no están protegidos.

IPsec ya existe desde hace algún tiempo, y es posible implementarlo en IPv4, pero su implementación no es nativa, pues no necesariamente todos los dispositivos IPv4 tienen el componente IPsec activo, a diferencia de IPv6 en donde el protocolo IPsec no es alternativo sino debe ser obligatoriamente soportado por el dispositivo, aunque esto no quiere decir que debe ser usado obligatoriamente. El objetivo es ahora usarlo para lograr un canal seguro punto a punto.

IPsec es un protocolo que permite asegurar las comunicaciones encriptando la información, es decir todo lo que se encuentre en las capas superiores se transmite de una manera segura, y puede ser implementada tanto en redes LAN como en redes WAN, ya sea en Internet comercial como en redes académicas, ya que su implementación puede ser de dos tipos:

- entre redes: se asegura la información entre dos redes, en este caso son los routers los que realizan la tarea de asegurar la conexión.
- entre hosts: este segundo caso, es un host el que establece una sesión de IPsec con el computador servidor, y luego ambos empiezan a transmitir datos de manera segura al haberse establecido exitosamente la conexión.

Al aplicar IPSec ya sea en cualquiera de los dos modos permite que todo el tráfico de las capas superiores pasen de una manera encriptada, esta transmisión es transparente para las aplicaciones, por lo cual toda aplicación puede ir sobre la capa IPSec, al mismo tiempo hace que sea totalmente transparente para los usuarios finales. Este protocolo realmente proporciona una solución de seguridad punto a punto (end-to-end) .

8.2. Arquitectura

Para el funcionamiento de IPSec, este framework de seguridad utiliza varios protocolos, ellos son:

- **AH (Authentication Headers)**: El cual provee la función de autenticación del origen de la información, y provee el mecanismo de integridad de todo el paquete. Para la implementación de este protocolo es necesario que ambas partes compartan una clave. Para el funcionamiento este protocolo usa los siguientes campos:

  - Next Header: Dado que IPsec se encuentra en la capa de red, es necesario colocar el código de la capa superior que se está transmitiendo.
  - Payload length: Define el tamaño de la cabecera de autenticación.
  - SPI (Security Parameters Index): Define a los parámetros de seguridad usada en la conexión actual.
  - Sequence number: Cada paquete tiene un numero secuencial, el cual no puede ser repetido, en caso de que exista se puede activar la renegociación de la conexión, con nuevos parámetros así como números de secuencia.
  - ICV (Integrity Check Value)/(MAC) Message Authentication Code: Un código que permite integridad de los paquetes.

  AH también da el servicio de Anti-Replay, cuando el destino reciba un paquete duplicado, posiblemente porque éste fue capturado por un atacante y el paquete fue posiblemente modificado y reenviado al destino, si es el caso el destino reconoce la duplicidad del paquete y solicita una nueva conexión.

- **ESP (Encapsulating Security Payloads)**: ESP provee confidencialidad para la información, esta confidencialidad permite que el paquete pueda ser leído solamente por el destino de los datos, opcionalmente ESP puede proveer autenticación al igual

que AH. ESP tiene varios campos, estos son los que se muestran en la figura 18 y son:

.

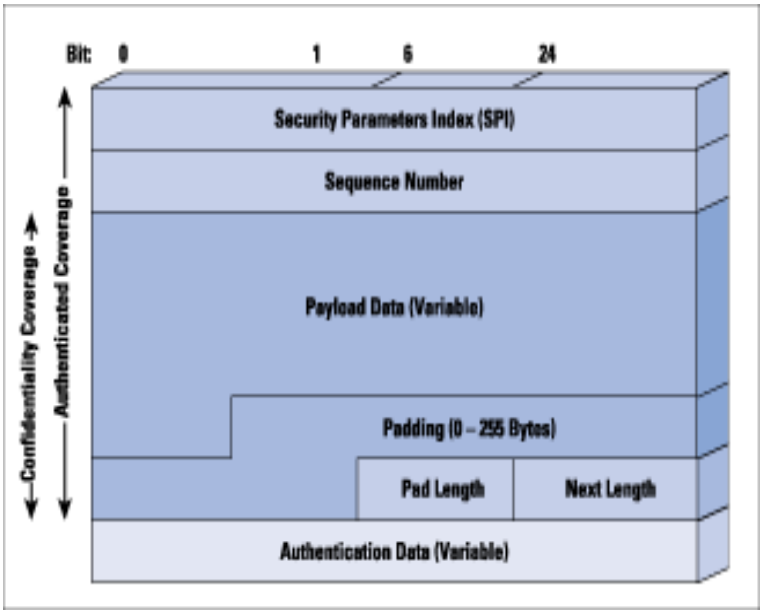

Figura 18: Campos de un paquete ESP de IPSec

- SPI (Security Parameters Index): Este campo identifica a una conexión.
- Sequence Number: Campo incremental que permite realizar anti-reply.
- Payload Data: En este campo va el paquete de datos de manera encriptada, dependiendo del tipo de configuración, estos datos pueden ser segmentos de la capa de transporte o paquetes IP encapsulados, estas configuraciones se verán más adelante.
- Padding: Bytes extras que utiliza en el algoritmo de encriptación en caso de que se requiera un número múltiplo que de octetos.
- Pad Length: Indica el número de bytes de relleno.
- Next header: Este campo identifica el tipo de dato que se esta transmitiendo.
- Authentication Data: Este campo contiene el Check Value de los datos.

Tanto AH como ESP pueden ser transmitidos de dos maneras desde el origen hasta el destino, en modo transporte o en modo túnel.

- **IKE (ISAKMP/Oakley)**: Provee a la conexión, una función para intercambio de llaves, las cuales son creadas y administradas por este protocolo. Para el manejo de las claves se puede tener una manera automática llamada IKE que provee mecanismos para autenticar, negociar y administrar llaves entre los dos dispositivos que están iniciando una comunicación encriptada. Para lograr esta fase de intercambio de claves utilizamos ISAKMP el cual realiza negociación de los atributos a usar en el proceso de encriptación. IKE también utiliza Oakley como mecanismo para intercambio de llaves, el cual está basado en el algoritmo de Diffie Hellman. En este proyecto se realiza un intercambio de llaves entre los dos equipos.

- **SA (Security Associations)**: Permite realizar una relación de conexión entre el equipo que envía datos y el que los recibe, esta relación puede ser en uno o dos sentidos, necesita dos SA para lograr su objetivo. Este protocolo es usado tanto por AH como por ESP,

8.2.1. Modos de comunicación.

Tomando en cuenta los tipos de comunicación existentes, tenemos la primera que es de host a host, y la segunda de red a red, en el primer caso son los hosts los que realizan la encriptación, en el segundo caso son los routers los que la realizan.

Modo Transporte: Si la comunicación se realiza entre dos hosts, esta se llama modo transporte, ya que el payload o carga es lo que va encriptado encima del IPSec, es decir todo lo que entregan las capas superiores. Permite una comunicación punto a punto entre dos hosts, los cuales podrían realizarse entre una estación y un servidor o entre dos servidores. Al usar ESP en modo transporte, IPSec encripta la información y opcionalmente tiene la posibilidad de autenticación.

La transmisión del paquete en modo transporte se realiza de la siguiente manera: en primer lugar se encripta todo lo referente a la capa de transporte, y se lo coloca en lugar de la transmisión original en texto plano, se agrega el ESP y la autenticación en caso que haya sido activado y el paquete se envía a la red. Cada router intermedio para poder rutear el paquete solamente necesita las direcciones IP, no necesita leer los datos

IKE (Internet Key Exchange): Intercambio automático de llaves usadas en IPSec.

ISAKMP: Protocolo parte de IKE que permite el manejo de llaves en una comunicación IPSec

Oakley: Protocolo que forma parte de IKE y que permite la distribución de llaves en una comunicación IPSec

encriptados, de esta manera no hace falta tener una configuración especial en estos routers intermedios. Al llegar al host final este lee el paquete, lo desencripta, pues tiene las llaves correctas para obtener la información, luego de tener la información desencriptada envía el segmento original en texto plano a la capa superior, y de allí continúa su proceso.

Modo Tunel: Cuando se une dos redes, los routers respectivos de cada una de ellas se unen y crean un túnel entre ellos, estos encapsulan todo el paquete IP del origen dentro de otro paquete. El paquete original es encriptado y enviado como carga dentro del segundo paquete que va ruteado desde un router hacia el otro, en donde al finalizar el recorrido, el router destino desencripta y desencapsula la información para reenviarlo al host de destino que puede o no estar directamente conectado.

En el gráfico 19 se aprecia gráficamente las diferencias entre el modo Tunnel, en donde la cabecera IP original (IP HDR) y los datos originales son encriptados, se colocan nuevas direcciones IP (IP del router que envía y de quien recibe) más las cabeceras de IPsec. A diferencia del modo transporte en donde solo se encripta los datos, pero las direcciones IP (tanto origen y destino) quedan intactas, y además agrega una cabecera para IPsec.

.

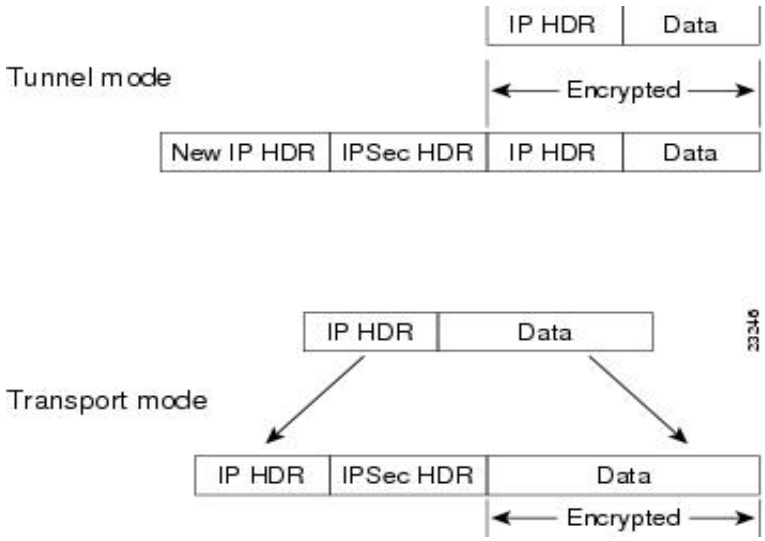

Figura 19: Modo Tunel y modo Transporte (tomado del portal de Cisco)

8.2.2. Asociaciones Seguras (Security Associations SA).

Tanto Authentication Headers como Encapsulation Security Payloads utilizan Asociaciones Seguras para poder conectarse, es simplemente asociar el origen de datos con el destino, y el destino con el origen, de esta manera se puede encriptar en dos vías, de entrada o de salida, cada una de ellas requiere un nuevo SA único el cual requiere los siguientes parámetros:

- SPI (Security Parameters Index): es una cadena asignada al SA que es transportada por un ESP o un AH, para que el destino pueda procesar el paquete transmitido.
- IP Destination address: Es el punto final donde recibe la información, el cual puede ser un equipo de seguridad (Router, Gateway, Firewall, etc) o un host.
- Security Protocol Identifier: Indica que protocolo está en el SA, ya sea AH o ESP.

Las Asociaciones seguras SA contienen toda la información necesaria por el protocolo AH (algoritmos, llaves, tiempos de vida) o el protocolo ESP (algoritmos para encriptación, algoritmos para autenticación, llaves, tiempos de vida) para poder funcionar correctamente, así como también proporcionan el modo de protocolo IPSec usado, ya sea túnel, transporte, u otros parámetros necesarios para el funcionamiento correcto del protocolo IPSec.

8.3. Pruebas de Laboratorio.

Dentro del proyecto de tesis se planteó el realizar pruebas de laboratorio del protocolo IPSec, los parámetros fueron:

- Servidores en producción con protocolo IPv6.
- Comunicación hasta un cliente dentro de la misma LAN universitaria.
- Comunicación con un cliente en Internet.
- Uso de IPSec en modo transporte.
- Transporte de protocolo ICMP y TCP.

8.3.1. Servidor y Cliente en la misma LAN Universitaria.

Con estos items definidos la primera prueba de laboratorio fue entre un servidor en la red CORE y un host en la red del NOC de la Universidad de Cuenca, que se encuentra a 2 saltos de distancia, y todos los equipos intermedios tienen IPv6 nativo. Para esta prueba de laboratorio no se realizó ningún cambio en los equipos intermedios, simplemente modificaciones en el servidor y en el computador cliente.

Para la realización de este laboratorio se tiene los siguientes requisitos:

- El servidor ya tiene una IPv6 Global configurada en su interfaz.
- El servidor tiene un nombre asignado con un registro AAAA hacia su IPv6 global.
- El servidor tiene el firewall interno habilitado.
- El servidor tiene un portal web ya activo en IPv6.
- El servidor es un GNU/Linux.
- El computador cliente es un GNU/Linux.
- El cliente tiene IPv6 habilitado en su interfaz.
- La red entre cliente y servidor debe permitir el ruteo de paquetes IPv6.

Con estos requisitos cumplidos se procedió a la implementación del túnel modo transporte entre el servidor con nombre prueba-evirtual.ucuenca.edu.ec con IPv6 Global 2800:68:c:15::5 y un computador cliente con el IPv6 global 2800:68:c:e01:62eb:69ff:fe7f:725d, en donde el número de saltos para ir de un punto a otro es 3 saltos tal como se puede ver en el siguiente traceroute6:

```
# traceroute6 prueba-evirtual.ucuenca.edu.ec
traceroute to prueba-evirtual.ucuenca.edu.ec (2800:68:c:15::5), 30 hops max, 80 byte packets
1 2800:68:c:e01::1 (2800:68:c:e01::1) 0.769 ms 3.008 ms 3.164 ms
2 2800:68:c:e::1 (2800:68:c:e::1) 4.338 ms 4.656 ms 4.796 ms
3 2800:68:c:15::5 (2800:68:c:15::5) 8.460 ms 8.534 ms 8.686 ms
```

Para la implementación se realizó los siguientes pasos:

1. Se realizó la instalación de ipsec-tools tanto en el cliente como en el servidor. Este paquete permite el manejo de la funcionalidad de IPSec en el kernel 2.5+, brindando al usuario herramientas para el manejo del protocolo IPSec tales como IKE, y manejo de políticas y SAs. Para la instalación dependiendo de la distribución se puede realizar de distintas maneras, en el caso de la familia de RedHat la instalación se realiza mediante el paquete ipsec-tools tanto en el cliente como en el servidor.

2. Como segundo paso es necesario crear un archivo de configuración de interfaz, que lo llamaremos ipsec6, para ello dentro del servidor se debe crear el archivo /etc/sysconfig/network-scripts/ifcfg-ipsec6 que contiene la siguiente información:

```
DST=2001:470:8:ba1:1e65:9dff:fe9d:69de
TYPE=IPSEC
ONBOOT=no
IKE_METHOD=PSK
```

   En donde el destino es la IP del terminal al cual va a transmitir datos.

3. En el servidor, dentro de la configuración IKE es necesario la inserción de una clave compartida (pre-shared key), para ello se edita el archivo /etc/racoon/psk.txt y se coloca el IP de destino, en este caso el del terminal, y la clave compartida, en este caso la palabra passw0rd, tal como lo muestra la siguiente configuración:

```
#cat /etc/racoon/psk.txt
2800:68:c:e01:62eb:69ff:fe7f:725d passw0rd
```

4. Configuración del protocolo IKE en el servidor usando la herramienta Racoon (parte del paquete ipsec-tools). Para ello es necesario la configuración de ciertos parámetros en el archivo /etc/racoon/racoon.conf:

```
sainfo anonymous
{
pfs_group 2;
lifetime time 3 hour;
encryption_algorithm 3des, blowfish 448, rijndael ;
authentication_algorithm hmac_sha1, hmac_md5 ;
compression_algorithm deflate ;
}
```

En donde:

- **sainfo anonymous**: Este parámetro permite que se pueda iniciar un SA anónimamente con cualquier IP que tenga las credenciales correctas.
- **pfs_group 2**: Permite que el intercambio de llaves se realice desde el servidor hacia el cliente mediante el protocolo de intercambio de llaves Diffie-Hellman.
- **lifetime**: El parámetro lifetime especifica el tiempo de vida (medido en tiempo o bytes de datos) de un SA.
- **encryption_algorithm**: Se tiene un gran grupo de algoritmos que pueden ser usados para la encriptación de los datos, este parámetro indica cuáles de ellos son soportados.
- **authentication_algorithm**: Este parámetro configura los algoritmos hash soportados para autenticación.
- **compression_algorithm**: Este parámetro define los algoritmos permitidos para compresión de la carga.

5. Luego de realizado la configuración en el servidor es necesario realizar la misma configuración en el computador cliente, con la diferencia que en el archivo de configuración /etc/sysconfig/network-scripts/ifcfg-ipsec6 en el parámetro DST ahora es necesario colocar la IP del servidor. En el caso del archivo racoon.conf la configuración de *sainfo anonymous* debe ser la misma en todos los parámetros, pues una configuración diferente podría ocasionar problemas en la conexión o en la reconexión. También es importante agregar la línea *include* con el ip del servidor, ya que en este archivo se almacena configuraciones específicas para la conexión a ese punto.

6. como último paso para de este proceso es iniciar racoon, para ello se ejecuta como daemon en modo background mediante el archivo /etc/inid.d/racoon start, así el equipo queda preparado para escuchar, posteriormente se levanta la interfaz mediante el comando *ifup ipsec6* con ello el protocolo IPSec queda preparado para activarse cuando se requiera. Para que el protocolo se active es necesario que llegue un paquete de uno de los dos puntos que hasta el momento ya se encuentras conectados.

Ya una vez configurado se procede a levantar el canal IPsec, donde se puede ver dentro de los registros el inicio del mismo:

```
Jul 8 18:21:41 prueba-evirtual racoon: INFO: respond new phase 1 negotiation: 2800:68:c:15::5[500]¡=¿2800:68:c:e01:62eb:69ff:fe7f:725d[500]
Jul 8 18:21:41 prueba-evirtual racoon: INFO: begin Aggressive mode.
Jul 8 18:21:41 prueba-evirtual racoon: INFO: received Vendor ID: DPD
Jul 8 18:21:41 prueba-evirtual racoon: NOTIFY: couldn't find the proper pskey, try to get one by the peer's address.
Jul 8 18:21:41 prueba-evirtual racoon: INFO: ISAKMP-SA established 2800:68:c:15::5[500]-2800:68:c:e01:62eb:69ff:fe7f:725d[500] spi:bcefb63992a4a7ce:2ac83b71e1e1536a
Jul 8 18:21:42 prueba-evirtual racoon: INFO: respond new phase 2 negotiation: 2800:68:c:15::5[500]¡=¿2800:68:c:e01:62eb:69ff:fe7f:725d[500]
Jul 8 18:21:42 prueba-evirtual racoon: INFO: IPsec-SA established: AH/Transport 2800:68:c:e01:62eb:69ff:fe7f:725d[500]-¿2800:68:c:15::5[500] spi=220060318(0xd1dda9e)
Jul 8 18:21:42 prueba-evirtual racoon: INFO: IPsec-SA established: ESP/Transport 2800:68:c:e01:62eb:69ff:fe7f:725d[500]-¿2800:68:c:15::5[500] spi=5786872(0x584cf8)
Jul 8 18:21:42 prueba-evirtual racoon: INFO: IPsec-SA established: AH/Transport 2800:68:c:15::5[500]-¿2800:68:c:e01:62eb:69ff:fe7f:725d[500] spi=148721306(0x8dd4e9a)
Jul 8 18:21:42 prueba-evirtual racoon: INFO: IPsec-SA established: ESP/Transport 2800:68:c:15::5[500]-¿2800:68:c:e01:62eb:69ff:fe7f:725d[500] spi=249036892(0xed8005c)
```

En esta bitácora de conexión se observa claramente cuando se inician las fases de negociación entre las dos IPs, la cual inicia cuando llega el primer paquete desde la

IP 2800:68:c:e01:62eb:69ff:fe7f:725d cliente hasta la ip del servidor, posteriormente se puede apreciar que se inicia el establecimiento del protocolo ISAKMP con intercambio de claves, y luego se empiezan a establecer los SA para el transporte, cada una con su propio y único SPI por conexión tal como se indico en la parte teórica.

Una vez establecida la comunicación se puede realizar una verificación de los SA abiertos con el comando racoonctl, en el caso de esta conexión podemos observar datos como el tipo de encriptación usado, tipo de autenticación, valor spi, modo de transmisión (transporte o túnel) tanto el SA que va del cliente al servidor, como el que se realizo desde el servidor al cliente:

```
# racoonctl show-sa esp
2800:68:c:e01:62eb:69ff:fe7f:725d 2800:68:c:15::5
esp mode=transport spi=5786872(0x00584cf8) reqid=0(0x00000000)
E: 3des-cbc ae195321 a7e69ed2 498c4e83 80707a12 8c1f2030 a2ea236f
A: hmac-sha1 5159f286 cce1cee1 d8f0dbb3 411e5192 18d517ce
seq=0x00000000 replay=4 flags=0x00000000 state=mature
created: Jul 8 18:21:42 2011 current: Jul 8 18:22:00 2011
diff: 18(s) hard: 10800(s) soft: 8640(s)
last: Jul 8 18:21:43 2011 hard: 0(s) soft: 0(s)
current: 1088(bytes) hard: 0(bytes) soft: 0(bytes)
allocated: 17 hard: 0 soft: 0
sadb_seq=1 pid=13349 refcnt=0
2800:68:c:15::5 2800:68:c:e01:62eb:69ff:fe7f:725d
esp mode=transport spi=249036892(0x0ed8005c) reqid=0(0x00000000)
E: 3des-cbc a7b86cde 6f02bc85 34cca06b 6abeedc0 63471fe3 ac7483e5
A: hmac-sha1 76442398 09bf87ac 4cf06c62 6a118bcb 312ae444
seq=0x00000000 replay=4 flags=0x00000000 state=mature
created: Jul 8 18:21:42 2011 current: Jul 8 8:22:00 2011
diff: 18(s) hard: 10800(s) soft: 8640(s)
last: Jul 8 18:21:43 2011 hard: 0(s) soft: 0(s)
current: 1088(bytes) hard: 0(bytes) soft: 0(bytes)
allocated: 17 hard: 0 soft: 0
sadb_seq=0 pid=13349 refcnt=0
```

También para comprobar se capturó paquetes al realizar la transmisión, en la figura 20 se muestra uno de ellos (es un paquete icmp de ping), en este se puede observar

claramente los datos de capa 3 el cual pertenece a un IPv6, y se aprecia que el Next Header es un tipo 0x33 es decir una cabecera AH. En esta cabecera tiene el SPI asociado y único, la secuencia y el ICV. Coloca como next header a un ESP, el cual contiene el SPI asociado, la secuencia, y sobre este protocolo ya se encuentra la información en si de manera encriptada.

Figura 20: Paquete IPSec modo transporte capturado

Como último paso se procedió a pasar otro tipo de tráfico, dado que el servidor al que se accedió es un servidor público en donde se realizan pruebas beta tiene entre alguno de sus servicios; un servidor Apache con varios virtualhosts, entre ellos una nueva versión de Moodle de la Universidad de Cuenca, los accesos se dieron sin problemas por medio de IPsec modo transporte. Otra aplicación probada fue SSH sobre IPv6, el cual tampoco presento ningún cambio.

IPsec esta implementado en el Kernel de Linux, por lo que no se noto carga extra en los procesadores al utilizar dos SA para la conexión con el cliente IPsec.

8.3.2. Servidor y Cliente en la Diferentes Redes.

Posterior a la realización de las pruebas de laboratorio de IPSec modo transporte dentro de la misma red universitaria, se procedió a realizar las mismas pruebas pero

pruebas beta: Pruebas de confiabilidad y depuración de sistemas y programas ya con clientes verdaderos, luego de estas pruebas, en caso de ser exitosas el servicio se lo podría coloca como estable y en producción

Moodle: Aplicación web usada como soporte a los profesores para la educación , provee herramientas propias de un Entorno Virtual de Aprendizaje

por medio de la Internet comercial, para lograr este objetivo fue necesario la creación de un tunnelBroker dado que aún el servicio de IPv6 en Internet comercial en Cuenca para usuarios finales aún no esta disponible por los ISP. Con la creación de este túnel se logró tener comunicación IPv6 a todas las redes comerciales, y los tiempos así como el número de saltos desde Internet Comercial en Cuenca hasta las IPs de la Universidad de Cuenca subieron, el número de saltos subió de 11 a 14, ya que por IPv4 el paquete llegaba hasta el NAP en Quito y regresaba por el proveedor de Internet Comercial IPv4 de la universidad. El tiempo de respuesta es lo que más aumento, ya que subió de 18ms hasta los 235 ms, y la razón justamente es que si el cliente tiene un tunnelBroker ahora el paquete viaja hasta el lugar donde esta el servidor de tunnelBroker, es decir en EEUU, y luego regresa por Internet Comercial.

Con la realización del túnel para las pruebas con el cliente se procedió consecutivamente a realizar lo siguiente:

- Modificación en el servidor del archivo psk.txt, agregando la IPv6 global externa del cliente.
- Modificación en el servidor del archivo /etc/sysconfig/network-scripts/ifcfg-ipsec6 con el IP del cliente.
- Ya que el computador cliente (laptop) físicamente se traslado de las instalaciones de la Universidad, hasta afuera de la Universidad para conectarlo a la red comercial, no fue necesario hacer cambios en ninguna de las configuraciones.
- Una vez ya configurados se procedió a levantar el servicio racoon en ambos terminales y a subir las interfaces ipsec6.

Luego de la subida de las interfaces se procedió a enviar un ping para que con el primer paquete se creen los SA respectivos, obteniéndose inmediatamente conexión tal como se esperaba. Posterior se empezó a enviar paquetes ping para probar el retardo existente obteniéndose los siguientes resultados:

Por medio del túnelBroker pero sin conexión IPSec se logro unos tiempos promedio de 243 ms con una desviación estándar de 3.04 ms, pero al activar IPsec los tiempos bajaron a 233 ms con una desviación estándar de 4.11 ms, con lo cual se puede creer que en la red del proveedor de túneles existe calidad de servicio para el protocolo IPSec, y por ello la disminución de aproximadamente 10ms.

Luego de levantado IPsec se procedió igualmente que en las pruebas anteriores a pasar diferente tipo de tráfico, tal como http, ssh, obteniéndose los mismos resultados, es decir que las aplicaciones no sufrieron ningún cambio en el rendimiento.

8.4. Políticas

IPSec como protocolo para encriptación de datos es transparente para el usuario, es por ello que tanto en empresas grandes se tiene como política usar VPN entre sucursales, y justamente la VPN se la realiza en IPv4 con direcciones públicas, entre la sucursal y la matriz usando el protocolo IPSec para su transmisión, haciendo que todo el tráfico de los clientes pase encriptado por medio del Internet Comercial, y de esta manera ninguna de las aplicaciones de la empresa sufre cambios. Esto además de encriptación se utiliza porque IPs privadas de los clientes no pueden verse con IPs privadas de otra sucursal, es por ello más que el requerimiento en si de seguridad que se aplican túneles ya en empresas reales.

En IPv6 la necesidad de uso de IPsec cambia totalmente, los IPs de ambas sucursales si logran comunicarse sin la necesidad de IPsec en modo túnel, ahora lo que exclusivamente se requiere es seguridad en la conexión, en el caso de sucursales de empresas, se requiere seguridad entre dos LANs, en el caso de la Universidad de Cuenca lo que se requiere actualmente es seguridad en la transmisión de información entre un servidor y otro, y entre un servidor y los clientes. Algunos de los requerimientos que se puede citar tenemos:

- Seguridad en la transmisión de datos desde los servidores de Base de Datos y los servidores que utilizan sus servicios.
- Seguridad entre distintos servidores que forman un cluster de páginas web.
- Seguridad entre los distintos nodos de un cluster de base de datos.

Estas son algunas de las premisas técnicas que se deberán aplicar para el uso de IPSec en futuro, es decir seguridad en la comunicación entre servidores.

9. Resultados, Conclusiones y Recomendaciones

9.1. Resultados

Finalizado este proyecto de tesis se logró los siguientes resultados:

- Se logró colocar al 95 % de las subredes de la Universidad de Cuenca en dual stack, inicialmente conectada a Internet Comercial con un túnel IPv6, usando al proveedor de tunnelBroker Hurricane Electric.

- Se logró que la red permita conexión IPv6 en cualquier lugar donde exista un computador o equipo permita activar este protocolo.

- Al comienzo de la implementación de IPv6 se registró un tráfico mínimo de pocos Kbps dentro de la red, principalmente debido a que los sitios que proveen contenidos en este protocolo son muy pocos. Igualmente paso con el tráfico generado entre facultades, el cual era practicamente cero.

  En diciembre del 2010 se migró toda la red a IPv6 comercial nativo, una vez hecho esto se trabajó aplicando al programa ”Google over IPv6” el cual tiene como requisitos obligatorios: 1) poseer una red estable IPv6 sin uso de túneles y 2) tener dos salidas Internacionales. El primer requisito fue cumplido mediante este trabajo de tesis y el segundo se lo consiguió por medio de trámites realizados con el proveedor de Internet que da servicio a la Universidad de Cuenca, el mismo que entregó una salida internacional por NTT y otra por Telefónica, permitiendo a la Universidad cumplir los requisitos solicitados por Google.

  Al aplicar este programa pudimos observar que uno de los DNS recursivos de la Universidad (previamente registrado en Google over IPv6) retorne registros AAAA para todos los dominios propiedad de Google (www.google.com, www.youtube.com, docs.google.com, etc.) viéndose ya un incremento realmente significativo en el tráfico de IPv6, llegando aproximadamente a picos de hasta 15 % de tráfico total de llegada que posee la Universidad.

- Todos los cambios realizados fueron totalmente imperceptibles para los usuarios, además con IPv6 mejoraron los tiempos de respuesta a los servicios de Google, que bajaron de 120ms a 100ms.

Google over IPv6: www.google.com/intl/en/ipv6

- Con respecto al servicio DNS en de los servidores autoritativos de la Universidad se realizó la respectiva implementación, gestionando además con NICec para que sus servidores IPv6 apunten al servidor autoritativo de la Universidad, de esta manera que el transporte de las consultas AAAA para el dominio ucuenca.edu.ec se realice por medio de IPv6.

  Vale la pena mencionar que hasta finales del 2010 los servidores de NICec seguían trabajando solamente en IPv4, y recién en el primer semestre del 2011 agregaron un nuevo servidor DNS localizado en Europa con un servicio dualStack, permitiendo ahora, y de manera definitiva, que exista un camino totalmente IPv6 desde cualquier equipo que realice una consulta DNS hasta los servidores de la Universidad.

- Se consiguió también implementar IPv6 en el servidor de correo electrónico, el mismo que empezó a recibir tráfico por medio de este protocolo, sobre todo desde otros servidores de correo ubicados en universidades a nivel internacional, así como también de otras empresas tecnológicas que ya tienen sus servicios también en IPv6.

  Ahora, la transmisión de datos con estas instituciones se los realiza a través de este protocolo, llegando incluso a recibir correo SPAM por medio de IPv6 desde servidores localizados en el continente Asiático.

- La Universidad formó parte de una prueba mundial de funcionamiento del protocolo IPv6. esta prueba fue el día de IPv6, 8 de Junio del 2011, día en que a nivel mundial se promocionó a los sitios con mayor acceso de Internet del mundo, a que por 24 horas coloquen sus servicios en dualstack. Empresas como Google, Facebook, Yahoo, entre otros, colocaron sus portales y contenidos en IPv6. La Universidad de Cuenca, que con anterioridad estaba dentro del programa ”Google over IPv6”, vio solamente un pequeño incremento en la cantidad de tráfico sobre este protocolo comparado con el total previamente medido, principalmente debido a que la mayor cantidad de tráfico IPv6 requerido por la Universidad se lo demanda a Google y sus dominios, que frente a los requerimientos realizados a otros sitios de Internet como Facebook y Yahoo, la demanda a estos últimos es proporcionalmente más baja.

9.2. Conclusiones

- Con respecto a la implementación de un servicio multiHomed se concluye que su diseño así como su implementación depende completamente del servicio que le entreguen sus proveedores, así como de las características propias de la red institucional. Teniendo siempre varias alternativas para su implementación, pero que dependiendo de los costos que la institución este dispuesto a pagar, se puede obtener una mejor red IPv6 en términos de retardo, jitter, ancho de banda, y compatibilidad con servicios IPv6 futuros que la red institucional planee colocar, pues un mejor equipamiento permitirá entregar mayores servicios en futuro, como por ejemplo movilidad o seguridad.

- La implementación de servicios solo-IPv6 en producción dentro de la institución aún no es posible, sino que deberá continuar siendo Dual Stack, por lo menos algún tiempo más, ya que actualmente existen clientes con computadores o dispositivos móviles que solo utilizan el protocolo IPv4 para su conexión.

- En lo referente a IPSec se vio que es una herramienta poderosa para la seguridad de la información, y que los recursos necesarios para su aplicación son mínimos, así como su funcionamiento es transparente para las capas superiores.

- Luego de haber trabajado inicialmente con un túnel internacional, y posteriormente cambiarlo a una red nativa, se notó un verdadero cambio en la calidad de acceso a la red IPv6 internacional.

9.3. Recomendaciones

- La principal recomendación es promocionar el uso de IPv6, no solamente para la administración de infraestructura de redes y comunicaciones, sino también a la gente que trabaja en desarrollo de software comience a programar usando DualStack, ya que IPv6 se viene con fuerza en los próximos años.

- Se recomienda a la Universidad de Cuenca implementar como política de compra de equipos nuevos, exija como requerimiento obligatorio el soporte IPv6.

  En el caso de equipos activos, así como de computadores ya existentes, el realizar el cambio a un sistema operativo que soporte este protocolo es el único requisito. A diferencia de los equipos especializados que quedarán con IPv4 funcionando

dentro de la misma red en DualStack, los cuales se mantendrán por varios años más funcionando de esa manera, tales como cámaras de vigilancia, impresoras y equipos de videoconferencia.

- Con respecto a IPsec, se recomienda empezar a usarlo especialmente dentro de la red de servidores, así como también incentivar su uso en equipos de usuarios finales, utilizando el mecanismo de certificados digitales puesto que esto implica mayor facilidad de uso que el de llave compartida. Para el caso de usuarios finales se recomienda el uso de este protocolo usando certificados digitales.

9.4. Lineas Futuras

IPv6 es un tema que ya ha estado en desarrollo desde hace muchos años, especialmente en países asiáticos, esto debido a que en estos países dada la cantidad de IPs necesarios, han agotado los bloques de direcciones IPv4 que han sido asignado a ellos por parte de IANA. Es por esto que en algunos de ellos se esta comenzando a trabajar en redes solo-IPv6, es decir, están eliminando completamente la pila IPv4 de sus redes, lo que involucra que agreguen equipos proxy que permitan el acceso entre el mundo IPv4 e IPv6.

En Latinoamérica este proceso ha sido completamente diferente, ocasionando que el despliegue de esta tecnología se vuelva un tema completamente nuevo, por lo que las líneas futuras de trabajo hasta terminar el 2011 será justamente iniciar los trabajos con redes solo-IPv6 tal como lo realizan en otros países de primer mundo, pues los principales requerimientos más que nada son de fuerza de trabajo e investigación para la realización de estas tareas.

De esta manera es que se plantea un cambio futuro en ciertas redes donde se pueda colocar un proxy que soporte IPv4 e IPv6, con una red interna en IPv6, este proxy realizará el trabajo de DNS recursivo y de proxy para poder solicitar direcciones IPv4 y traducirlas a los clientes finales a IPv6.

Otra línea de trabajo es desarrollar aplicaciones que funcionen en IPv6, como por ejemplo la telefonía IP, que actualmente se encuentra solo en IPv4, se planteará la necesidad del soporte IPv6 en el Sistema Operativo de los call manager, así como de los teléfonos, y es justamente la voz sobre IP una de las aplicaciones que se verá beneficiada por el uso de la red IPv6.

También es posible el trabajo futuro en el manejo e implementación de IPv6 móvil,

el cual permitirá tener siempre la misma dirección IPv6 sin importar el lugar donde se encuentre el usuario, protocolo que será muy útil cuando se vaya a realizar seguridad IPsec.

Índice de figuras

Índice de cuadros