IMPLEMENTACION DEL PROTOCOLO IPV6 EN EL ISP DIVEO SYNAPSIS

JONATHAN ANDRÉS CAVIEDES GÓMEZ

UNIVERSIDAD SANTO TOMAS

FACULTAD DE INGENIERÍA DE TELECOMUNICACIONES

BOGOTÁ

2012

IMPLEMENTACION DEL PROTOCOLO IPV6 EN EL ISP DIVEO SYNAPSIS

Realizado Por:

JONATHAN ANDRÉS CAVIEDES GÓMEZ

CODIGO: 2070724

Proyecto de Pasantía para optar el Título de Ingeniero de Telecomunicaciones Universidad Santo Tomas

Dirigido por:

ING. ELVIS EDUARDO GAONA GARCÍA Msc

UNIVERSIDAD SANTO TOMAS

FACULTAD DE INGENIERÍA DE TELECOMUNICACIONES

BOGOTÁ

2012

RECTOR GENERAL
Padre Carlos Mario Alzate Montes, O.P.

VICERRECTOR ADMINISTRATIVO Y FINANCIERO GENERAL
Padre Marco Antonio Peña Salinas, O.P.

VICERRECTOR ACADÉMICO GENERAL
P. Eduardo Gonzales Gil O.P

SECRETARIO GENERAL
Doctor Héctor Fabio Jaramillo Santamaría

DECANO DIVISIÓN DE INGENIERÍAS
Padre Pedro José Díaz Camacho, O.P

SECRETARIA DE DIVISIÓN
E. C. Myriam Gómez Colmenares

DECANO FACULTAD DE INGENIERÍA DE TELECOMUNICACIONES
Ingeniero Miguel Eugenio Arias Flórez

Nota de Aceptación

La monografía para optar al título de Ingeniero de Telecomunicaciones realizado por parte del estudiante Jonathan Andrés Caviedes, la cual comprende el proyecto de pasantía de Implementación del protocolo IPv6 en el ISP Diveo Synapsis, ha sido aprobado para optar al título de Ingeniero de Telecomunicaciones, de acuerdo con lo estipulado por la Facultad de Ingeniería de Telecomunicaciones de la Universidad Santo Tomás.

_____
_____
_____
_____
_____
_____
_____

_____

Firma del Presidente del Jurado

_____

Firma del Jurado

_____

Firma del Director

Fecha:

Santa Fe de Bogotá (7, Septiembre 2012)

ADVERTENCIA

La Universidad Santo Tomás no se hace responsable de las opiniones y conceptos expresados por el autor del trabajo de grado, solo velará por qué no se publique nada contrario al dogma ni a la moral católica y porque el trabajo no tenga ataques personales y únicamente se vea el anhelo de buscar la verdad científica.

Capítulo III –Art. 46 del Reglamento de la Universidad Santo Tomás.

RESUMEN

A continuación se llevará a cabo el desarrollo del proyecto de implementación del protocolo IPv6 en el ISP Diveo Synapsis, haciendo un estudio desde la base del conocimiento sobre el protocolo, atravesando los sistemas de enrutamiento IP, teniendo en cuenta los aspectos claves de seguridad de la información, y aplicando las nuevas tecnologías de Virtualización, para así poder llegar a concluir con el diseño de una red que cumpla con todos los requerimientos sociales como técnicos para el éxito del proyecto.

Palabras Clave

Protocolo IP, IPv4, IPv6, Resolución de nombre de Dominio, Virtualización.

ABSTRACT

The following are carried out the project implementation of IPv6 in ISP Diveo Synapsis, doing a study from the base of knowledge about the protocol, through IP routing systems, taking into account the security key information, and application virtualization technologies, in order to reach a conclusion with a network design that meets all requirements for the social and technical success.

Keywords

IP protocol, IPv4, IPv6, Domain Name Resolution, Virtualization.

CONTENIDO

LISTA DE FIGURAS

LISTA DE TABLAS

PARTE I

(HUMANÍSTICA)

1. CAPITULO: 1 INTRODUCCIÓN AL PROYECTO

1.1. INTRODUCCIÓN

En la siguiente monografía se va a desarrollar todo el aspecto teórico y práctico del protocolo IPv6 aplicado e implementado en un proveedor de servicio de Internet (ISP), en el cual se abordará el problema mediante una red de pruebas la cual debe contener todo lo que se requiera para un ambiente de producción.

Cumpliendo así con el objetivo de la realización de la práctica profesional para optar al título de ingeniero de telecomunicaciones de la universidad Santo Tomás, cumpliendo con todas las pautas integrales y humanistas de la Universidad, yendo desde un ámbito investigativo hasta un ámbito enteramente práctico y funcional, sin que se llegue afectar de manera negativa a la empresa y a la sociedad si no por lo contrario sea un punto fuerte de las mismas.

De aquí que se aborda el problema de una manera humanística y académica, llevando a la compañía a vanguardia en tecnología aplicando nuevos protocolos y nuevos diseños que puedan aportar un patrimonio tecnológico a la humanidad, con el avance y el desarrollo de estas prácticas y aplicaciones de estos nuevos protocolos.

Teniendo como fin aplicar el conocimiento adquirido en la Universidad para el desarrollo de la sociedad, y a favor de la misma.

1.2. PLANTEAMIENTO DEL PROBLEMA

La penetración de Internet a nivel mundial ha sido fundamental para el desarrollo de la ciencia y la evolución del conocimiento, siendo Internet el conjunto global de interconexiones de redes de todas partes del mundo, y para las personas del común un medio de comunicación fundamental para el diario vivir.

Para que esto fuera posible se implemento el protocolo IP (Internet Protocol) que actualmente se encuentra en su versión 4 de la cual en este momento cuenta con direcciones agotadas, por lo que se rediseño el protocolo en su versión más reciente para que pueda subsanar esta falla y algunas otras deficiencias con las que cuenta el protocolo.

Diveo Synapsis de Colombia LTDA. (en adelante Diveo Synapsis) es una corporación que presta servicios de conectividad e Internet “ISP”, a través del cual presta servicios de información y telecomunicaciones a sus diferentes clientes, entre los cuales se destaca el Data Center. En su red de core se encuentra implementado el protocolo IP en su cuarta versión “IPv4”, y cuenta con un número significativo de agregados, y se espera que esto siga creciendo de acuerdo a su modelo de negocio.

De acuerdo con esto en la actualidad el protocolo IPv4 ha agotado sus direcciones, puesto que la entidad encargada de la administración y asignación de direcciones, llamada “IANA”[1] *Internet Assigned Numbers Authority* la cual a su vez delega a diferentes organizaciones regionales la administración de estas direcciones, siendo el caso de “LACNIC”[2] *Latin America and some Caribbean Islands*, la correspondiente en Colombia. Ha otorgado su último bloque de direcciones. Conllevando con esto al irreversible el proceso de cambio a la siguiente versión de IP, la cual cuenta con mayor número de direcciones y prestaciones.

Esta transición se debe hacer paulatinamente de tal manera que IPv4 e IPv6 sigan coexistiendo, puesto que es impensable detener IPv4 en estos momentos, de esa forma hacer menos traumática la implementación de IPv6

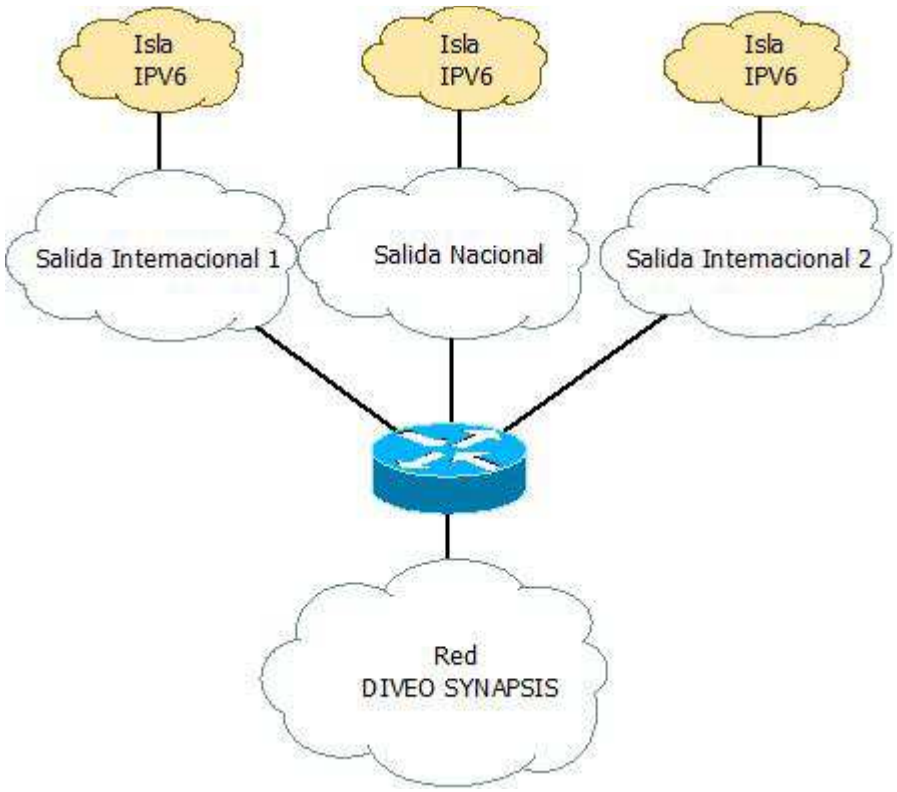
Siendo Diveo Synapsis un ISP es fundamental la implementación y el despliegue de este protocolo en su red de core, puesto que si se espera a crecer en el

[1] Nota: sitio web IANA http://www.iana.org
[2] Nota: sitio web LACNIC http://lacnic.net

número de agregados y servicios es indispensable que no se vea detenido su plan de negocio.

Actualmente Diveo Synapsis cuenta con una red de core por donde transitan todos sus agregados, la cual se encuentra interconectada al NAP Colombia, NAP Américas, y otras redes internacionales, para proveer la salida a Internet del ISP, de aquí que Diveo Synapsis no solo atiende el trafico de sus clientes y de su infraestructura si no que por lo contrario tiene que solventar trafico de internet en especial trafico que pasa por Colombia en el NAP Colombia, de aquí que si algún operador cuenta con alguna red IPv6, esta no podrá ser identificada por Diveo Synapsis por lo que tendrá que hacer peticiones a operadores diferentes a él, teniendo en cuenta esto el protocolo IPv6 ya se encuentra desplegado en algunos sistemas internaciones a manera de islas siguiendo la siguiente figura:

Figura 1: Islas IPv6.



Fuente: Autor

Haciendo incompatible el tránsito de IPv6 en el Back Bone de Diveo Synapsis, por lo que se plantea el despliegue del protocolo y el establecimiento de sesiones de enrutamiento IPv6 entre Diveo Synapsis y los otros operadores, de tal manera que

se implemente una isla IPv6 en Diveo Synapsis y sea alcanzable desde Internet, y de esta manera se empiece a hacer la transición gradualmente hacia IPv6 por parte de Diveo Synapsis y el resto de operadores.

Para esto Diveo Synapsis cuenta con un bloque de direcciones IPv4, para sus actuales clientes y se encuentra agotado en estos momentos, sin embargo el número de abonados está creciendo constantemente, por lo que Diveo Synapsis ha solicitado a LACNIC la asignación de un nuevo bloque de direcciones IPv4, aunque este bloque parece ser insuficiente para la demanda de servicios y el crecimiento de la compañía en los siguientes años. No obstante LACNIC ha entregado un bloque de direcciones IPv6 de un tamaño extremadamente considerable, haciendo que nazca la idea de desplegar este protocolo, y así estar a la vanguardia con los otros operadores en el sector de Colombia.

1.3. JUSTIFICACIÓN

1.3.1. Justificación Técnica.

IP se ha vuelto el protocolo predominante para las comunicaciones en la actualidad, remplazando a tecnologías antiguas como ATM, o Frame Relay, puesto que estas se encontraban orientadas a prestar servicios telefónicos, es decir que la información transportada por estas redes era de volúmenes muy bajos empezando en velocidades que iban desde 64Kbps hasta 2048Kbps en servicios de ultima milla, o en otras palabras velocidades bajas entregadas al usuario final, sin embargo estas velocidades se vieron cortas por el crecimiento exponencial de servicios como el Internet, el cual es hoy en día el servicio por excelencia de transporte de información.

IP aunque ha prestado excelente comportamiento a través del desarrollo de Internet tiene en la actualidad un problema y es que su número de direcciones se ha agotado, pero los servicios y dispositivos que usan esta tecnología vienen en aumento, por lo cual se desarrolla IPv6. Para que Diveo Synapsis no se vea afectado en un futuro por el aumento de su número de agregados se decide desplegar este protocolo y así continuar con el plan de negocio de la compañía.

1.3.2. Justificación Académica

Desde el punto de vista académico se busca conocer a profundidad el funcionamiento del protocolo IPv6, realizado mediante la investigación planteada de tal manera que retroalimente el conocimiento adquirido en las áreas de Telemática en la Universidad, de tal manera que el despliegue en un futuro no sea tan traumático si no por lo contrario de manera continua, aportando así al campo de las Telecomunicaciones el conocimiento para realizar el despliegue e implementación de este protocolo de la manera más optima y oportuna, para que así no se vean afectadas las comunicaciones.

1.3.3. Justificación Económica

Para que el despliegue del protocolo no fuese tan traumático, los fabricantes de los dispositivos hicieron su desarrollo para que fuera compatible con la mayoría de los equipos que se encuentran en funcionamiento, de aquí que Diveo Synapsis cuenta con Routers Cisco de la serie 7600 los cuales soportan este protocolo, haciendo que la implementación de IPv6 coexista con la versión actual y no genere gastos extras en la compañía, ni afecte a los abonados actuales.

1.3.4. Justificación Social

El número de dispositivos que usan conexión a Internet viene en aumento de una manera considerable, ingresando a este campo todo tipo de dispositivos, como por ejemplo teléfonos celulares, computadores portátiles, entre otros, y a nivel empresarial diferentes tecnologías como por ejemplo las comunicaciones unificadas, de las cuales se destacan VoIP, mensajería instantánea y Video en tiempo real, son parte fundamental del desarrollo de la sociedad en la actualidad, por lo que la detención de estos servicios se hace impensable, requiriendo así una solución urgente al problema del agotamiento de direcciones, siendo IPv6 el único protocolo que pueda dar solución a esto.

De tal manera que Diveo Synapsis de Colombia se encuentre a la vanguardia con sus clientes, entregando nuevas tecnologías y aportando así al desarrollo de la sociedad.

1.4. OBJETIVOS

1.4.1. Objetivo general.

Dar interconectividad con internet y otros operadores mediante el despliegue del protocolo IPv6 en la red de Diveo Synapsis de Colombia, impulsando el desarrollo y la investigación en el sector privado de las Telecomunicaciones.

1.4.2. Objetivos específicos.

- Implementar el protocolo IPv6 en una red alterna a la de Diveo Synapsis de Colombia.
- Realizar la compatibilidad entre IPv6 e IPv4 en la red de Diveo Synapsis de Colombia. y los otros operadores de Internet.
- Establecer mediante el protocolo de enrutamiento BGP e IPv6 sesiones de intercambio de rutas con los demás operadores.
- Incrementar la utilización de esta nueva tecnología en la compañía, usando infraestructura ya desplegada, además de virtualización, aportando al medio ambiente.

1.5. ALCANCES Y LIMITACIONES

1.5.1. Alcance

La red que se va a plantear tiene como finalidad un ambiente de pruebas, pero debe estar lista para producción, en el momento que se requiera. De aquí que el alcance estará dirigido a tener la solución completamente funcional, incluyendo todos sus módulos, para que cuando llegue el momento de la migración a nivel mundial, la compañía se encuentre a la vanguardia y sea uno de los puntos fuertes de la misma.

Teniendo en cuenta esto se espera que la transición desde el protocolo IPv4 hacia IPv6 sea menos traumática, y se pueda hacer de manera progresiva, dando con esto solución a los problemas de interconectividad que se esperan a nivel mundial con el agotamiento de direcciones, además de solventar los problemas de seguridad que se están evidenciando en estos momentos.

1.5.2. Limitaciones

Una de las principales limitaciones que tiene la implementación del protocolo IPv6 es el poco uso que se encuentra actualmente, puesto que a pesar de que el protocolo ya se encuentra lanzado y funcional a nivel mundial, son pocas las corporaciones que han empezado a adoptarlo, haciendo con esto que la red sea un tanto limitada, es decir que tenga un contenido pobre en comparación a su antecesor a pesar que la cantidad de direcciones sea considerablemente mayor.

De aquí que la cantidad de personas capacitadas para esto sea mínima, y el soporte para el mismo sea pobre.

Por otra parte, a pesar de que el protocolo fue diseñado hace bastante tiempo, muchos fabricantes y proveedores de equipos de telecomunicaciones no implementen en sus equipos este protocolo, como por ejemplo algunos casos de Routers y firewalls, en los cuales se debe cambiar a nuevos equipos o comprar licencias extras para poder implementar una solución de este tipo.

1.6. DELIMITACIÓN

1.6.1. Espacial

Siendo Diveo Synapsis un ISP en Bogotá con cedes en algunas partes de Colombia, el proyecto tendrá como principal enfoque Bogotá y sus principales clientes, aunque siendo IP la tecnología principal a usar, se podrá extender a cualquier nodo o parte del mundo que se encuentre conectada a esta red, siendo Internet por excelencia la red global en la cual estará implementada.

Por otra Parte, Diveo Synapsis ofrece servicios de Data Center, en donde se encuentran alojados la mayor cantidad de servicios que se manejan, de aquí que se explotara esta función usando este servicio para alojar los servicios que se deseen prestar en esta nueva red.

Todo esto teniendo en cuenta que la nueva red se planteara en un ambiente de pruebas el cual estará ligado directamente a la red de producción en la compañía, con el fin de que esta pueda salir de igual forma a producción sin tener un mayor impacto en el diseño original, tanto en equipos como en protocolos para utilizar.

1.6.2. Cronológica

El proyecto se va a desarrollar en el primer periodo académico del año 2012, en donde tendrá su parte en investigación de la nueva tecnología que se va a aplicar, pasando por el diseño e yendo directamente a la implementación. Con todo esto planteando el siguiente cronograma para culminar con éxito el proyecto:

Tabla 1: Cronograma de desarrollo del proyecto.

Actividad	Febrero	Marzo	Abril	Mayo	Junio	Julio
Introducción del proyecto y enfoque						
Introducción a la monografía						
Desarrollo investigativo, marco teórico						
Diseño técnico del proyecto						
Implementación técnica del proyecto						
Conclusiones						
Revisiones Finales						
Comité de Grado						

Fuente: Autor

1.6.3. Metodológica

La metodología planteada en este proyecto, tiene como primer fin conocer y entender toda la capacidad del protocolo, tanto en su diseño como en su implementación, llevando la adecuada investigación y documentación de esta tecnología, para que así responda al problema con una solución eficiente y eficaz, que además no genere costos adicionales y sea fácil de soportar, ya que en caso de algún problema el tiempo de respuesta debe ser el más mínimo con el mayor éxito posible.

De tal manera que se encuentre alineada con los objetivos de la compañía, sin que se vea afectada la estrategia de la misma siendo un nuevo fuerte, para que así se encuentre a la vanguardia en tecnología y que llegado el momento de una migración global, esto ya se encuentre planteado de manera correcta y se haga de la mejor manera posible.

1.6.4. Financiera

El ambiente financiero de la solución, siempre estará acorde con lo que la empresa cuente en ese instante, es decir se utilizara los equipos y la infraestructura de la misma, para que así no se generen gastos adicionales, por otra parte en el momento que se encuentre implementado el proyecto y cuente con las garantías para prestar el servicio de manera estable, se deberá contemplar la utilización de estos dispositivos de manera continua, o la migración del protocolo a su núcleo, de tal manera que no vaya a afectar a la producción de la empresa.

De aquí que todos los implementos que se van a utilizar serán contemplados en la etapa de diseño del proyecto, en la cual se determinará la estabilidad, la capacidad y la escalabilidad de los equipos, además de otras determinaciones que serán tomadas en esa etapa.

1.7. ENFOQUE HUMANÍSTICO

Correspondientemente a los fundamentos de la Universidad Santo Tomás, y a la formación como Ingeniero de Telecomunicaciones, y persona integral, se planteó el proyecto desde un punto de vista investigativo, apuntando hacia un enfoque social, es decir llevando la academia, hacia la práctica en un ambiente productivo al servicio de la sociedad, implementando nuevas tecnologías para que así la compañía, la universidad y el país se encuentre a la vanguardia.

Teniendo en cuenta, que este es un servicio que a pesar de estar implementado en ambiente corporativo, va a afectar directamente a la sociedad de manera positiva, haciendo que el servicio que se preste a los usuarios finales sea el más adecuado y cumpla con todas las pautas humanísticas de la Universidad Santo Tomás, entre las cuales tiene como principal función formar profesionales éticos e íntegros para el servicio de la sociedad.

Siendo así la implementación de este nuevo protocolo un estandarte de desarrollo en Colombia, estando a la vanguardia en la tecnología y fomentando la investigación para el beneficio del país, para que de esta manera se impulse el desarrollo en el ambiente corporativo y sean más empresas las que se vinculen a la implementación de este protocolo. Impulsando la construcción del bien común, entre las entidades encargadas de prestar servicios como estos, es decir integrando todas las compañías en una sola tecnología, que represente al país como inspirador en Latinoamérica y lleve por la vía del desarrollo; Generando consigo nuevo conocimiento, aplicado a un contexto real, en donde se involucra a la Universidad, la sociedad y la industria en un bien común.

Y a pesar de ser una nueva tecnología, respeta a la ecología, puesto que es implementada en los dispositivos ya existentes sin cambiar o desechar algún material nocivo para el planeta y la sociedad, reutilizando la tecnología ya existente y optimizando a su máximo todos los recursos con los que se cuenta actualmente.

Prestando finalmente un servicio de alta calidad a los clientes de la compañía con tecnología de punta de una manera práctica y eficaz, sin discriminar a ninguno y prestando un servicio equitativo superando las expectativas del cliente quien finalmente es el puente directo frente a la sociedad y es donde se va a ver directamente reflejado en el país.

PARTE II

(INVESTIGATIVA)

2. CAPITULO 2: INTERNET PROTOCOL VERSION 6 (IPv6)

2.1. INTRODUCCIÓN

En la actualidad los dispositivos de red en su gran mayoría utilizan el protocolo de internet (IP) en su versión 4, para realizar sus interconexiones, este protocolo maneja un sistema de direccionamiento de 32 bits, es decir un número de identificación única para cada host o equipo que componga la red, dicho numero se tiene una sintaxis en forma de 4 grupos de octetos separados uno del otro por un punto, de la siguiente forma, llamado así dirección IP:

Dirección IP tradicional.

A.C.D.E

Como se trata de una dirección de 32 bits se tiene la siguiente cantidad de direcciones posibles 2^{32} lo cual corresponde a 4.294.967.296, que para su efecto no es suficiente en la actualidad puesto que el gran crecimiento de dispositivos de este protocolo va ascendiendo de una manera considerable como por ejemplo se destacan los computadores personales, dispositivos móviles ente otros.

Siendo esta la principal razón por la cual se adelantó el desarrollo de un nuevo protocolo con mayores prestaciones, entre ellas un mayor número de direcciones conocido como IP en su versión 6 (IPv6), el cual contiene 128 bits, lo cual corresponde a 2^{128} es decir aproximadamente 340 sixtillones de direcciones, superando con creces la expectativas de crecimiento de la población de dispositivos que usan este protocolo.

La compañía encargada de la administración de estas direcciones es Internet Assigned Numbers Authority IANA en español La Agencia de asignación de Números de Internet, la cual a su vez asigna bloques de direcciones a diferentes compañías regionales para que ellas hagan una gestión más seccional; siendo el caso de LACNIC la encargada del registro de direcciones para Latinoamérica y el Caribe, la cual le corresponderá al caso de Colombia en el momento en que una compañía desee adquirir un bloque de direcciones.

Diveo Synapsis de Colombia tiene entre sus actividades la prestación de servicio de internet ISP (Internet Service Provider) por lo cual cuenta con una red de CORE o BACKBONE en la cual se tiene planteado el despliegue de este protocolo.

2.2. CARACTERISTICAS

La razón principal por la cual se desarrolla IPv6 era para subsanar aquellos defectos que pudo tener IPv4, entre los cuales el principal fue el agotamiento de direcciones, por otra parte se introdujo nuevas características que lo hacen un protocolo eficiente para el estado actual de las redes IP, las características más trascendentales incluidas fueron las siguientes:

- Extensión del número de direcciones.
- Simplificar el direccionamiento.
- Autoconfiguración.
- Descubrimiento de vecinos.
- Nomenclatura.
- Simplificación de la cabecera.
- Seguridad integrada.
- Implementación de la direcciones Anycast y Multicast.
- Movilidad.

De igual forma se diseño para que fuera un protocolo flexible en el momento de la migración para que no fuera de una manera tan dramática.

2.2.1. Extensión del número de direcciones

El protocolo IPv6 posee 128 bits de direccionamiento a diferencia de IPv4 el cual solo contenía 32, de esos 128 bits el primer segmento de bits "*001*" fue reservado para direcciones globales Unicast de aquí que se tiene *128-3* direcciones disponibles es decir $2^{125} = 4.25x10^{37}$. Uno de los usos que se le da a las direcciones IPv6 en las redes de área local, es la utilización de la dirección única, y física del dispositivo de red MAC (Media Access Control) el cual contiene 48 bits más un prefijo de relleno de 16 bits para un total de 64, donde los 64 bits restantes corresponderían a la dirección de red. Esta es una práctica poco eficiente porque si se tiene en cuenta los 3 bits de relleno para las direcciones Unicast globales se tendría un espacio de direccionamiento de 2^{61} aunque es muy práctica para identificar a los host.

2.2.2. Simplificar el direccionamiento

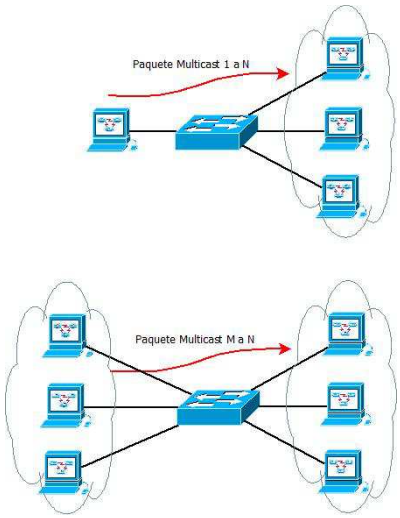
La dirección IPv6 es obtenida mediante la dirección física MAC y la dirección de red en el segmento, mientras que en una red IPv4, la forma típica de direccionamiento era indicar al Router o puerta de enlace la primera dirección del segmento y a los host las siguientes de una manera secuencial. Teniendo en cuenta que la dirección de red en una LAN es de 64 bits y la dirección física MAC es de 48 bits, se debe agregar un relleno de 16 bits el cual para simplificar la nomenclatura se tomo en valor Hexadecimal FF y FE.

2.2.3. Autoconfiguración

Como se mencionó antes una práctica en las redes de tipo LAN es la utilización de la dirección MAC para la asignación de la dirección IP, esto con el fin de facilitar la autoconfiguración en el momento de incorporación de un dispositivo nuevo en la red puesto que en IPv4 se usaba el protocolo encargado de la asignación de direcciones de manera dinámicas DHCP (Dynamic Host Configuration Protocol), el cual lo hacía de una manera secuencial pero de una manera poco eficiente para las expectativas que se tiene con IPv6 porque para un gran número de dispositivos puede ser dispendiosa la configuración de un servidor DHCP en un ambiente tradicional, por ejemplo se espera que los dispositivos de uso domestico usen este protocolo y una persona la cual no tenga conocimiento de esta tecnología no podría usar de manera adecuada sus dispositivos comunes (TV, Móvil , PC, etc.); de aquí que IPv6 asigna de una forma más simple las direcciones IP.

Surgiendo el concepto de dirección Multicast, la cual es una dirección que se asigna para un grupo de host, es decir un grupo de dispositivos que contienen la misma dirección IP, con el fin de simplificar el enrutamiento de tráfico igual hacia los mismos dispositivos, expresado de 2 formas (1 hacia N ó M hacia N host):

Figura 2: Envío de paquete Multicast.

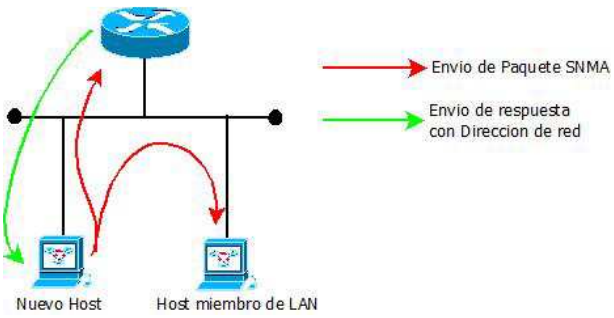


Fuente: Autor

Todo esto con el fin de hacer posible la autoconfiguración de direcciones IP usando estos dos métodos, de manera que cuando un dispositivo es integrado en la red este envía un paquete Multicast el cual es conocido como un estándar dentro de la LAN, este paquete es conocido como *Solicited Node Multicast*

Address, como éste es enviando a todo el segmento de red, en el momento que el Router lo identifica responde enviando un paquete con la dirección de red del segmento. La maquina lo recibe y usando su propia dirección física se auto asigna una dirección IP.

Figura 3: Autoconfiguración IP mediante el envío de paquete Multicast.



Fuente: Autor

Como se expresa en la figura anterior el nuevo host después de tener la respuesta del Router, y usando su propia dirección física configura su IP con un formato similar al siguiente:

Dirección de red 64 bits + Relleno 16 bits + Dirección MAC 48 bits.

2.2.4. Descubrimiento de vecinos

Una de las características propias de IPv6 es el descubrimiento de vecinos, es decir cuando un nuevo miembro a la red es incluido, el protocolo tiene soporte para conocer de manera automática el nuevo miembro, tendiendo así un mapa lógico de la topología de la red.

Esta característica se hace mediante el protocolo ICMPv6, siendo este mecanismo un sustituto de ARP, haciendo mucho más rápida la computación de paquetes. Haciéndolo de una manera sencilla enviando 4 tipos paquetes ICMPv6, los cuales consisten en 2 parejas de Router y Host, siendo un paquete enviado por el Router de solicitación de información, y otro paquete de anuncio de presencia, es decir el Router puede enviar un paquete solicitando información de sus vecinos, o enviar un paquete informando su existencia de manera periódica o en respuesta a un mensaje de solicitud. El host envía de igual manera estos dos tipos de paquetes, con lo cual, cada dispositivo empieza a hacer un cache interno donde contiene información de sus vecinos, haciendo innecesario el protocolo encargado en la conmutación de traducción de direcciones físicas a direcciones IP, siendo actualmente ARP.

2.2.5. Nomenclatura

Para la versión 4 del protocolo se usaba una notación agrupando el numero de bits en grupos de 8, estos octetos se separaban mediante un punto en 4 grupos y se escribían de manera decimal, y su respectiva mascara de red la cual indicaba que parte de la dirección indicaba la red y que parte correspondía a la identificación del host de la siguiente forma:

Dirección A.B.C.D / mascara E.F.G.H

Ejemplo:

Dirección 192.168.0.1 /mascara 255.255.255.0 es decir

Dirección 1100 0000. 1100 0110. 0000 0000. 0000 0001

Mascara 1111 1111. 1111 1111. 1111 1111. 0000 0000

La cual indicaba con *1* la parte de dirección de la red y en *0* la del host, es decir que la dirección del host es 192.168.0.0 y el host es el numero 1.

Como una dirección IPv6 contiene 128 bits al escribirla de la misma forma que IPv4 sería muy larga y complicada para la interpretación y el direccionamiento, por lo que se opto por realizar otra notación, esta vez la agrupación de bits se hace en 16, la separación mediante dos puntos, y se expresa de manera hexadecimal haciendo que sea mucho más comprensible, por otra parte la dirección de mascara de red no se escribe en el mismo formato puesto que se extendería bastante, por lo que solo se decidió solo indicar de manera decimal el numero de bits que se encontraban en *1* delimitado con un *slash*, de la siguiente manera:

Dirección AAAA: BBBB:CCCC:DDDD:EEEE:FFFF:GGGG:HHHH / XX

Ejemplo:

Para la dirección IPv4 192.168.0.0 con mascara 255.255.255.0 seria

C0.A8.00.00 en hexadecimal, la máscara /24 y en IPv6

C0A8:0000:0000:0000:0000:0000:0000:0000/24

Una de las particularidades de esta nomenclatura es la abreviación de 0 consecutivos mediante el uso de "***::***" siguiendo en el ejemplo seria:

C0A8::/24

Esta abreviación solo puede ser usada cuando existe una cadena consecutiva de bytes nulos única es decir si se presenta en 2 segmentos diferentes en la dirección solo debe ser aplicado a uno para que la dirección sea válida.

Las direcciones tradicionales o reservadas en IPv4 como por ejemplo la Loopback también son tenidas en cuenta en IPv6 de la siguiente forma:

::1 Para la dirección Loopback que tradicionalmente en IPv4 era 127.0.0.1

:: Para una dirección sin especificar que tradicionalmente era 0.0.0.0

Un ejemplo[3] del formato de direcciones Multicast y Unicast sería el siguiente:

"1080:0:0:0:8:800:200C:417A Dirección Unicast

FF01:0:0:0:0:0:0:101 Dirección Multicast

De manera abreviada:

1080::8:800:200C:417A Dirección Unicast

FF01::101 Dirección Multicast"

IPv6 para hacer posible la compatibilidad con IPv4, implementa la posibilidad de combinar las direcciones IP de la siguiente forma:

Para la dirección 192.168.0.1

::192.168.0.1 ó :FFFF:192.168.0.1

Que a su vez seria:

::*C0A8:1 ó* ::*FFFF*:*C0A8:1*

El prefijo FFFF hace referencia a que es una dirección IPv4 mapeada.

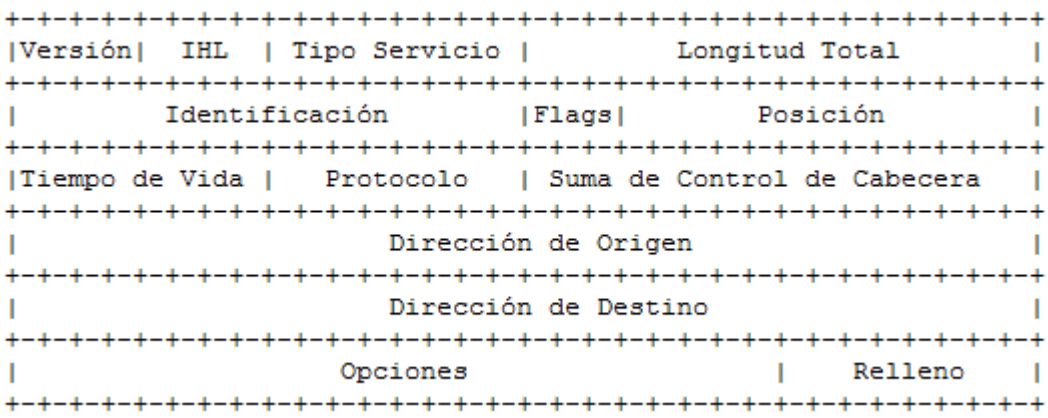
2.2.6. Simplificación de la cabecera.

Con el fin de hacer el procesamiento más ágil en los dispositivos se decidió mejorar, la cabecera de IPv4 haciéndola más simple para así evitar la sobrecarga de procesamiento en los Routers quienes finalmente son los encargados de evaluar la cabecera para decidir cómo debe ser tratado el paquete.

[3] Ejemplo tomado de RFC 2373 en http://www.ietf.org/rfc/rfc2373.txt

En IPv4 se tienen bastantes Campos cumpliendo distintas funciones en la cabecera del paquete, mientras que en IPv6 se ve reducido de manera drástica el numero de campos sin quitar ninguna de las funciones, si no embebiendo estas en los nuevos campos, con lo cual se hace más sencillo el protocolo, como se muestra en las siguientes graficas:

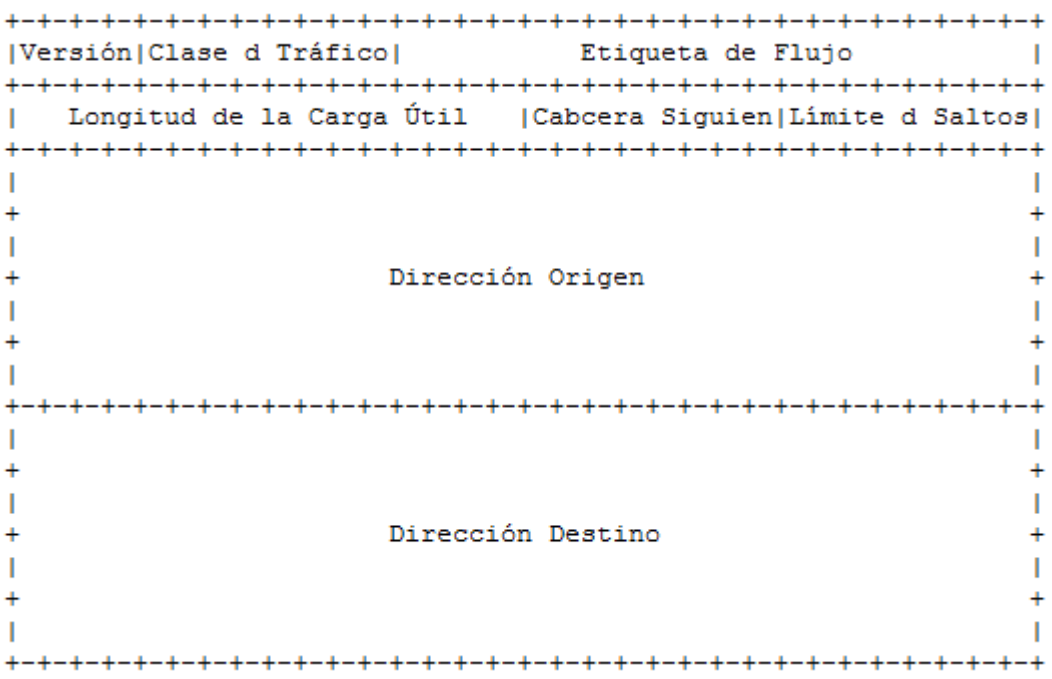
Figura 4: Formato de cabecera IPv4



Tomado de RFC 791[4]

[4] Tomado de RFC 791 en http://www.rfc-es.org/rfc/rfc0791-es.txt

Figura 5: Formato de cabecera IPv6



Tomado de RFC 2460 [5]

Cabe destacar que el tamaño horizontal visto en la grafica de la cabecera es mayor para IPv6 en comparación con IPv4 siendo con esto un número mayor de bits para evaluar pero un numero considerablemente menor de características por evaluar, por otra parte las opciones en IPv6 están definidas de manera implícita en la carga útil, siendo esta la variable mientras que la cabecera fija, quitando carga de procesamiento en el momento de fragmentación de los paquetes que se hacía en IPv4, mientras que en IPv6 se amplía el tamaño de la MTU “Unidad Máxima de Transferencia”. También se quita el campo de CRC “suma de corrección de errores”, puesto que esta corrección de errores le corresponde al Host destino en sí y no a los Routers.

2.2.7. Seguridad integrada

Uno de los grandes cambios en IPv6 fue la inclusión obligatoria de IPsec, estableciendo una capa de seguridad a nivel de transporte, es decir aplicando parámetros de cifrado y autenticación entre los paquetes IP siendo indiferentes a las aplicaciones o protocolos de capas superiores como TCP o UDP. Haciendo con esto la seguridad del protocolo mucho más fuerte.

[5] Tomado de RFC 2460 en http://www.rfc-es.org/rfc/rfc2460-es.txt

De aquí que en la cabecera se incluyen los parámetros de Autenticación y Cifrado, llamados *Authentication Header (AH),* y *Encrypted Security Payload (ESP) Header,* donde *AH* es un campo que contiene información sobre quién y que debe tener acceso a la información que contenga asegurando la integridad de la misma, así como el *ESP* contiene los parámetros de cifrado de la carga útil.

2.2.8. Implementación de la direcciones Anycast y Multicast

2.2.8.1. Direcciones Multicast

Como se ha mencionado anteriormente IPv6 no usa direcciones de difusión "Broadcast", es decir a diferencia de IPv4 no tiene direcciones que identifiquen a todo un segmento de red, puesto que con el número mayor de direcciones un segmento de red se puede hacer realmente grande, y si se desea enviar información para todo el segmento se agregaría un tráfico innecesario a la red, este mismo resultado se puede conseguir usando direcciones Multicast, optimizando el enrutamiento en la red. Por todo lo demás las direcciones Multicast siguen teniendo la misma función que en IPv4, por ejemplo si se desea transmitir contenido (TV, Radio, entre otros) a un grupo de host, se usan estas direcciones.

El formato de estas direcciones tiene las siguientes características:

Tabla 2: Formato de dirección Multicast

8	4	4	112
1111 1111	banderas	ámbito	ID de Grupo

Fuente Autor

La forma para identificar una dirección Multicast es simple puesto que su primer octeto se encuentra en *FF* seguido de las banderas que representan si la dirección es conocida o es transitoria, cabe aclarar que los primeros 3 bits son reservados y se encuentran en *0,* seguido esta el ámbito de la dirección donde puede ser en hexadecimal, *0* de uso reservado*, 1* para un grupo en una interfaz local, *2* para un grupo de un enlace local, *8* para un grupo en una organización ó *E* para un ámbito global, entre otros, por ejemplo para una dirección de enlace de red local el cual emularía una dirección de Broadcast sería la siguiente:

FF02::1

Donde *FF02* representa a una dirección Multicast local y 0:0:0:0:0:0:1 es el identificador de grupo.

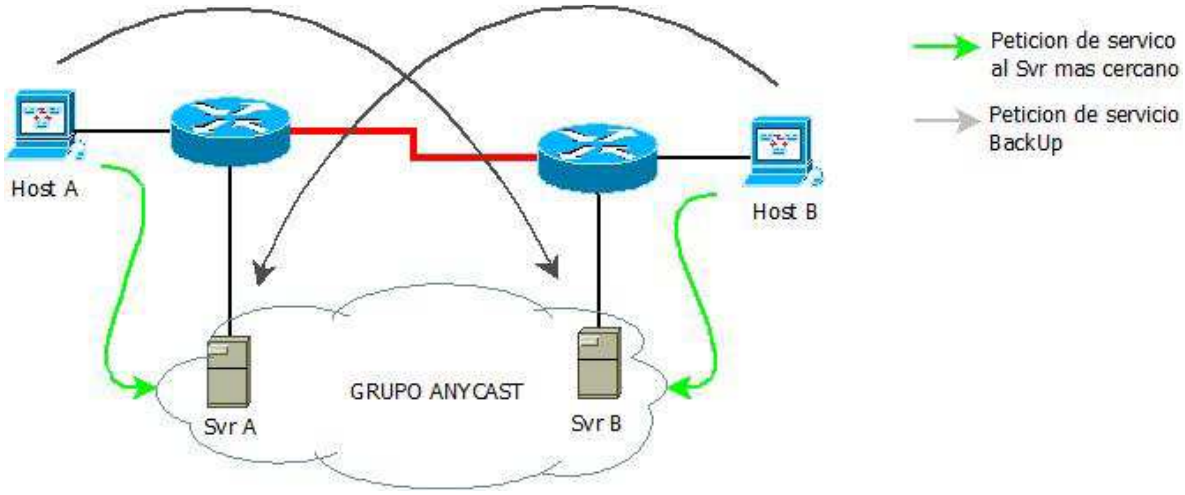
La IANA ha designado para usos frecuentes un número de direcciones en particular, dentro de las más destacadas se encuentran las siguientes:

- Para un ambiente local
  - FF01::1 para todos los nodos
  - FF01::2 para todos los Routers
- Para un enlace local
  - FF02::1 para todos los nodos
  - FF02::2 para todos los Routers
  - FF02::5 para OSPFIGP
  - FF01::9 para los Router RIP
  - FF01::A para los Router EIGRP
  - FF01::1:2 para los agentes DHCP
- Para un ámbito de sitio
  - FF05::2 para los Router
  - FF05::1:3 para los servidores DHCP
  - FF05::1:4 para los servidores repetidores DHCP

2.2.8.2. Direcciones Anycast

Las direcciones Anycast es un tipo de dirección nueva incluida en IPv6, la cual representa una dirección en común para un grupo de dispositivos, de igual forma que las direcciones Multicast con la diferencia que el trafico solo va dirigido para una maquina, la cual se encuentre más cercana al origen del trafico, como se representa en la siguiente grafica:

Figura 6: Representación de direcciones Anycast.



Fuente: Autor

Como se observa en la grafica, los servidores A y B proveen el mismo servicio, y si algún host desea recibir este, hacen la petición a la dirección Anycast donde responde el servidor más cercano, por otra parte se tiene como ventaja una conexión de Backup automática sin hacer ningún tipo de configuración en rutas, suministrando un servicio de alta disponibilidad de manera sencilla. Con esto se ahorra ancho de banda aumentando la disponibilidad de tráfico en los enlaces.

Una dirección Anycast no es fácilmente identificable, puesto que su formato es idéntico a una dirección Unicast, es decir una dirección Unicast se puede convertir en una dirección Anycast en el momento que es asignada a más de una interfaz en un Router, de aquí que el segmento ligado a esa interfaz será parte del grupo Anycast, de aquí que vienen dos restricciones para el uso de estas direcciones, la primera es que solo se permite el uso en interfaz de un Router, y la segunda es que una dirección Anycast no puede ser usada en el origen del trafico puesto que la respuesta a este no siempre llegara a su origen.

2.2.9. Movilidad

Cuando se habla de movilidad en IPv6 se refiere a la capacidad de llevar un host de una red a otra conservando su dirección original, esto fue pensado para la implementación en comunicaciones y dispositivos móviles como laptops y celulares puesto que su número de abonados está en aumento junto con las nuevas tecnologías móviles (UMTS, HSPA+, LTE, etc.), haciendo posible la convergencia de todo tipo de redes a redes NGN (Redes de Nueva Generación), las cuales llevaran como protocolo de funcionamiento el IP.

Para que esto fuese posible se introdujeron nuevos conceptos, dirección de casa “Home Address”, dirección de cuidado “Care-of Address”, y el agente “Home Agent”. La dirección home es aquella dirección local, que pertenece propiamente al dispositivo, y cuando un host es cambiado de red este adquiere una dirección de cuidado a través del proceso de autoconfiguración, estas dos direcciones son asociadas entre sí a través del agente.

2.3. DOMAIN NAME SYSTEM DNS

Actualmente sobre Internet se prestan infinidad de servicios, dentro de los más destacados esta el servicio WEB y el MAIL, cada uno de estos servicios se encuentra alojado en un servidor, el cual para poder acceder a él, se requiere una dirección IP, de aquí que conocer el numero de dirección IP para cada servidor el cual este prestando un servicio en la actualidad, es un imposible para una persona, por lo cual se implemento este sistema el cual, traduce números de

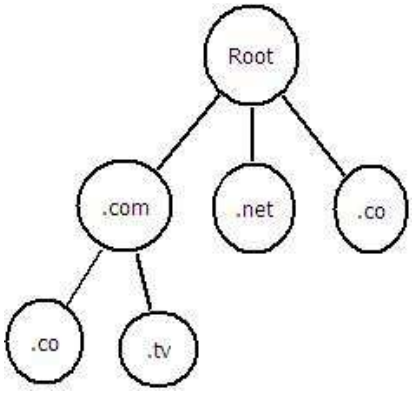
direcciones IP en nombres de dominio, del tipo www.usta.edu.co, siendo así más fácil de recordar.

2.3.1. Funcionamiento DNS

La base del funcionamiento del sistema de resolución de dominios, es el esquema cliente-servidor, donde el cliente le pregunta a cual dirección corresponde el nombre *X* , y el servidor busca, y traduce a la dirección correspondiente, por lo cual en una red de pocos dispositivos solo bastaría un servidor, pero en un ambiente real como Internet el trafico es abundante y el número de consultas seria exorbitante, por lo cual el sistema debe tener un esquema jerárquico donde se divida por zonas de administración independientes, balanceando así el trafico entre los servidores.

Como se menciono el sistema es jerárquico, por lo que en el primer punto de resolución se encuentra el servidor ROOT, de allí se empieza a delegar la administración a subniveles, y ellos a su vez a subniveles, en forma de árbol, esta delegación se conoce como TLD “Top Level Domain”, cada delegación se separa por un punto, y se asigna un código, entre los más comunes se encuentran *.com .net .org .gov,* a su vez también existe un código para la delegación en cada país, por ejemplo en Colombia es *.co*, la siguiente grafica describe de una manera más simple es sistema:

Figura 7: sistema de delegación TLD.



Fuente: Autor

Por lo cual si un dispositivo desea conocer la dirección de www.usta.edu.co, debe primero consultar a su servidor de DNS local por la dirección www.usta, donde www es el nombre del host y usta el dominio, si este no conoce la dirección pregunta a quien tenga delegada .co, este a su vez a *.edu*, y así sucesivamente, hasta llegar al Root quien le responde a quien fue delegada esa zona para su

correspondiente consulta. Donde toda la dirección se denomina FQDN “Fully Qualified Domain Name”.

2.3.2. Servidor BIND9

El servidor que se va a usar en este proyecto es BIND9 servidor DNS, para sistemas Linux, e UNIX, puesto que es de código abierto y este se encuentra implementado en Diveo Synapsis.

En este servidor se describe como zona a cada dominio, el cual contiene un archivo de configuración de zona, que contiene todos los componentes de esta. Los componentes principales en este archivo son:

- SOA: Start of Authority, describe las propiedades de la zona.
- A: Address, describe la dirección propia de un Host.
- NS: Name Server, describe algún servidor DNS, que esté delegado.
- MX, Mail Exchanger, describe algún servidor de correo.
- CNAME, Canonical Name, describe el nombre canónico de un host.

Por ejemplo para un registro de un servidor de dominio tendría la siguiente nomenclatura:

@ IN NS ns1.ejemplo.com

ns1 IN A 192.168.0.1

Donde @ representa el dominio en sí, es decir ejemplo.com, y NS indica que ns1.ejemplo.com será un servidor de dominio delegado para esa zona, y el registro A indica la dirección del servidor.

Por otra parte también existe un archivo de configuración de zona inversa, es decir si se conoce la dirección IP este resuelve el nombre de dominio a quien corresponde.

Otra de la características de BIND9 es la capacidad de delegar cargas a servidores secundarios, es decir la implementación de un segundo servidor quien hace de apoyo, a este se transfiere las zonas primarias para que este sea capaz de resolverlas.

2.3.3. DNS sobre IPv6

Con el fin de dar soporte a IPv6, y que este fuese compatible con IPv4, se introdujeron varios tipos de registro en las zonas de configuración, entre los cuales el más destacado es AAAA que tiene el mismo significado que A en IPv4,

identificar un host en particular por su dirección, siguiendo con el ejemplo para un servidor de dominio seria:

@ IN NS ns1.ejemplo.com

ns1 IN A 192.168.0.1

ns1 IN AAAA 2803:B000::1

Indicando que el servidor tiene por dirección IPv4 *192.168.0.1* e IPv6 *2803:B000::1,* dando así completa compatibilidad entre los dos sistemas.

3. CAPITULO 3: ENRUTAMIENTO

El proceso de enrutamiento es el encargado de dirigir el tráfico que pasa por una red, es decir, debe decidir y conocer como reenviar los paquetes transmitidos de algún segmento de red a otro, para que se cumpla la comunicación entre dos dispositivos y que además se haga con las mejores condiciones posibles, entre las cuales por ejemplo se tienen tiempo de transmisión, velocidad de transmisión, cantidad de información entregada a su destino, entre otros.

Una red puede ser sencilla o compuesta, es decir puede tener solo grupo de dispositivos los cuales por medio de su dirección IP se comunican, pero cuando la red empieza a crecer y se quiere conectar dos redes totalmente apartadas, se hace mediante un dispositivo de enrutamiento, haciendo la red compuesta, cumpliendo con la premisa de que para su direccionamiento e identificación única de dispositivos de red, la dirección IP debe ser única para cada uno de ellos.

De aquí que un bloque de direcciones IP se fracciona y se delega para cada segmento de red, y el dispositivo de enrutamiento decide el camino de un paquete dirigido de un dispositivo en un segmento A, hacia un dispositivo en un segmento B. si una red es lo suficientemente grande la cual puede tener gran cantidad de segmentos interconectados entre sí, pueden existir más de dos rutas diferentes de un destino a otro, siendo la decisión del dispositivo de interconexión de redes decidir cuál es la ruta más optima para la entrega de su información.

Los dispositivos encargados de realizar esta redirección de paquetes de un destino a otro, son llamados Routers, los cuales su principal función es cumplir y garantizar la conectividad en la red.

3.1. MECANISMOS DE ENRUTAMIENTO

Existen varios mecanismos de enrutamiento, los cuales abarcan dos grandes grupos, estáticos y dinámicos, los cuales dependen de la administración sobre el dispositivo, y cada uno lleva diferentes características, aunque su función es la misma.

En el momento en que un router, es conectado a una red, empieza su proceso de reconocimiento de vecinos y empieza a establecer su primera relación ya sea mediante la dirección IP del segmento o mediante el protocolo ARP, el cual fue sustituido en IPv6 por neighbor discovery, y empieza a generar su tabla de

enrutamiento, la cual indica al router como debe tratar los paquetes enviados entre sus diferentes redes.

De aquí que la construcción de la tabla de enrutamiento está dada por los siguientes mecanismos:

- Interfaz directamente conectada.
- Estático.
- Dinámico.
- Ruta por defecto.

3.1.1. Interfaz Directamente conectada

Este mecanismo es el más básico en un proceso de enrutamiento, puesto que consiste en registrar en su tabla de enrutamiento las interfaces que el dispositivo tiene directamente conectadas, es decir si un dispositivo tiene un segmento A y un segmento B directamente conectado, automáticamente registra en su tabla estos segmentos y sabe como pasar trafico del segmento A hacia el segmento B o viceversa, como se muestra en la siguiente imagen:

Figura 8: Interfaz directamente Conectada.

Fuente: Autor

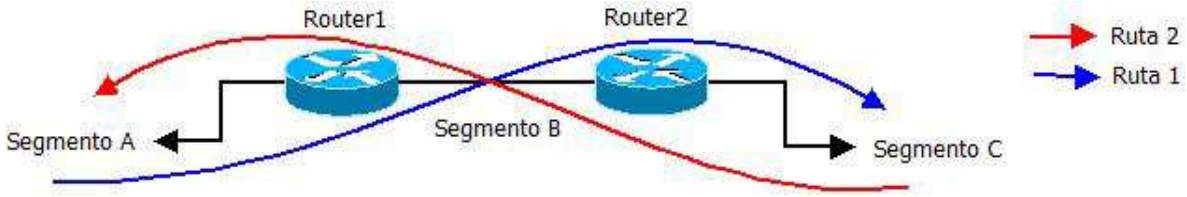
Esto sería un escenario sencillo, de enrutamiento. Pero si por el contrario entra un segmento de red C conectado a B, la red que se encuentra en A no sabría como enviar un paquete hacia C por medio de este mecanismo.

3.1.2. Mecanismo Estático

Este mecanismo es configurado directamente por el administrador del dispositivo, e indica una ruta por donde debe dirigir los paquetes, es decir que el router consulta en su tabla de enrutamiento y envía los paquetes hacia el siguiente dispositivo indicado por el administrador.

Siguiendo con el ejemplo de los tres segmentos de red, en donde existen tres segmentos de red (A, B, C), y dos dispositivos de enrutamiento (Router1, Router2), conectados de la siguiente forma:

Figura 9: Mecanismo Estático



Fuente: Autor

En este escenario el Router1 conoce el segmento A y el segmento B, pero no conoce C, y el Router2 conoce el segmento B, y C pero no el segmento A, de aquí se hace necesario el mecanismo estático, en donde en el Router1 se indica que para enviar un paquete de A hacia C, lo envié al Router2 que el tomara esta decisión, y de igual forma en el Router2.

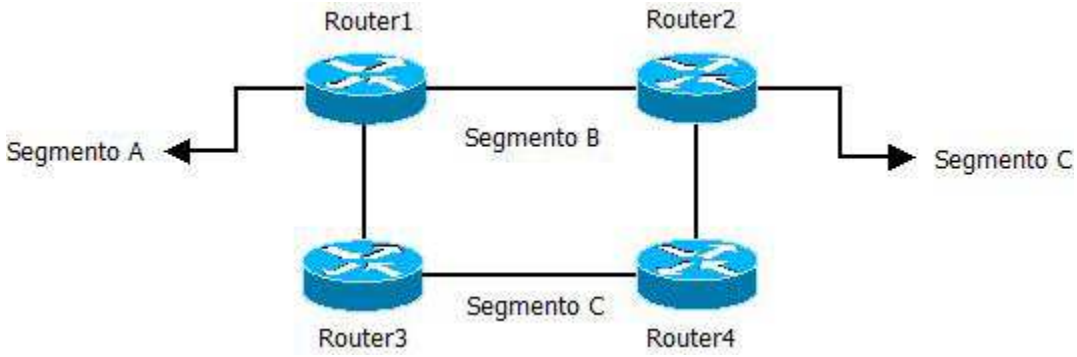
Una vez realizado esto se tiene completamente conectividad entre todos los segmentos, sin embargo si la red llegara a crecer con la cantidad de dispositivos y segmentos de red que estuvieran fuera del alcance del administrador, este sistema de enrutamiento se haría ineficiente y complicado, por lo cual se implementa el mecanismo dinámico

3.1.3. Mecanismo Dinámico.

Este mecanismo fue diseñado para redes lo suficientemente grandes para que se tuviera administración de todos los segmentos, de tal manera que automáticamente los dispositivos de enrutamiento establecieran las rutas para tener completa conectividad de manera automática.

Para esto se diseño diversos protocolos de enrutamiento, los cuales dependiendo de la necesidad y la capacidad de la red fueran implementados, cada protocolo tiene diferentes métodos de decisión y funcionamiento, pero todo orientado con el mismo objetivo, definir cuál es la ruta más optima, puesto que en una red de gran tamaño pueden existir diferentes caminos hacia un mismo destino.

Figura 10: Mecanismo dinámico.



Fuente: Autor

En este ejemplo existen varios caminos para un paquete del segmento A llegue hacia el segmento B.

De aquí que la construcción de la tabla de enrutamiento se hace más compleja, tomando varios valores y varias rutas para un mismo destino, con lo cual la decisión del router se toma usando la métrica, la cual entre más pequeña tiene más prioridad.

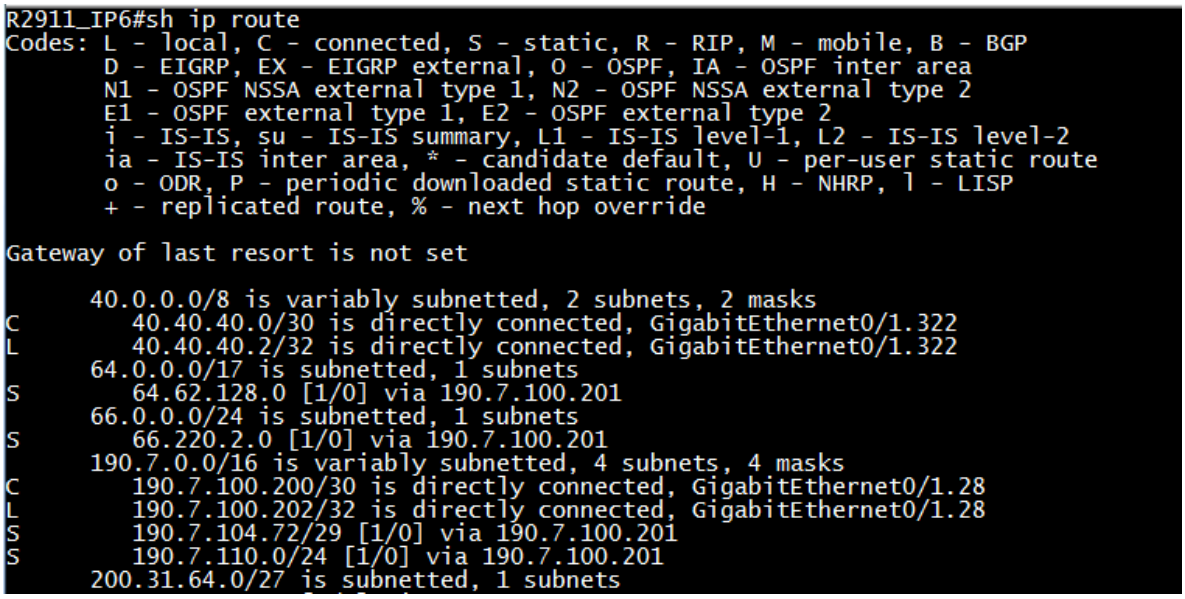
3.1.4. Ruta por defecto

Cuando un router no encuentra una ruta en su tabla de enrutamiento para un paquete recibido, tiene dos posibilidades de elección, descartar el paquete o enviarlo hacia su ruta por defecto, la cual tiene como función ser una pasarela donde se reciben los paquetes, es comúnmente usado en una red jerárquica, cuando todos los Routers de nivel inferior envían sus paquetes hacia el router de nivel superior o de borde.

3.1.5. Tabla de enrutamiento

Como se menciono la tabla de enrutamiento contiene todas las rutas que el router ha aprendido, bien sea directamente conectado, definido por el administrador, o mediante algún protocolo de enrutamiento, la forma de una ruta contiene la siguiente sintaxis: *Destino, mascara de red, siguiente salto y métrica*; en un router cisco se tiene la siguiente figura en una tabla IPv4:

Figura 11: Tabla de enrutamiento IPv4.

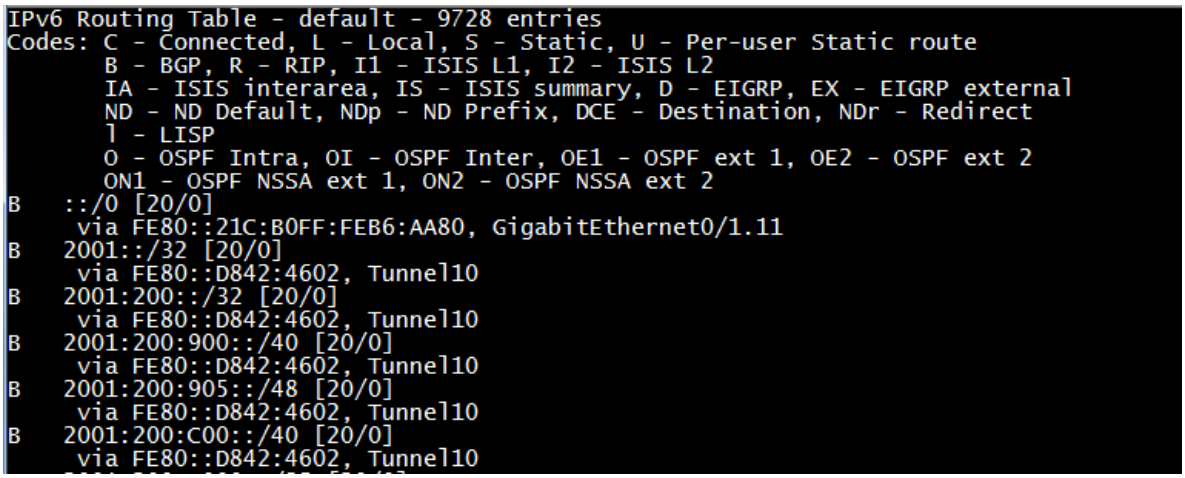


```
R2911_IP6#sh ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is not set

      40.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        40.40.40.0/30 is directly connected, GigabitEthernet0/1.322
L        40.40.40.2/32 is directly connected, GigabitEthernet0/1.322
      64.0.0.0/17 is subnetted, 1 subnets
S        64.62.128.0 [1/0] via 190.7.100.201
      66.0.0.0/24 is subnetted, 1 subnets
S        66.220.2.0 [1/0] via 190.7.100.201
      190.7.0.0/16 is variably subnetted, 4 subnets, 4 masks
C        190.7.100.200/30 is directly connected, GigabitEthernet0/1.28
L        190.7.100.202/32 is directly connected, GigabitEthernet0/1.28
S        190.7.104.72/29 [1/0] via 190.7.100.201
S        190.7.110.0/24 [1/0] via 190.7.100.201
      200.31.64.0/27 is subnetted, 1 subnets
```

Fuente: Autor

Donde la letra inicial indica el método como aprendió la ruta. Y para ipv6 se tiene lo siguiente:

Figura 12: Tabla de enrutamiento IPv6



```
IPv6 Routing Table - default - 9728 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
       B - BGP, R - RIP, I1 - ISIS L1, I2 - ISIS L2
       IA - ISIS interarea, IS - ISIS summary, D - EIGRP, EX - EIGRP external
       ND - ND Default, NDp - ND Prefix, DCE - Destination, NDr - Redirect
       l - LISP
       O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
B   ::/0 [20/0]
     via FE80::21C:B0FF:FEB6:AA80, GigabitEthernet0/1.11
B   2001::/32 [20/0]
     via FE80::D842:4602, Tunnel10
B   2001:200::/32 [20/0]
     via FE80::D842:4602, Tunnel10
B   2001:200:900::/40 [20/0]
     via FE80::D842:4602, Tunnel10
B   2001:200:905::/48 [20/0]
     via FE80::D842:4602, Tunnel10
B   2001:200:C00::/40 [20/0]
     via FE80::D842:4602, Tunnel10
```

Fuente: Autor

En este caso se puede observar una ruta por defecto la cual se marca como *::/0*, o en IPv4 como *0.0.0.0/0*.

3.1.6. Distancias Administrativas

Cuando un router encuentra varias rutas hacia un mismo destino, el toma como la mejor ruta la que tenga una métrica menor, esta métrica se hace conoce como la distancia administrativa, y cada protocolo de enrutamiento tiene su forma particular de calcularla tomando diferentes métricas. La siguiente tabla representa las métricas dadas por cada método:

Tabla 3: Distancias Administrativas

Método	Distancia Administrativa
Directamente Conectada	0
Ruta estática	1
Protocolo BGP Externo	20
Protocolo EIGRP	90
Protocolo IGRP	100
Protocolo OSPF	110
Protocolo RIP	120
Protocolo BGP Interno	200
Desconocido	255

Fuente: Autor

Aunque estas distancias pueden ser modificadas por el administrador del sistema dependiendo de las necesidades de la red.

3.2. BGP

Existen dos clasificaciones en los protocolos de enrutamiento, los protocolos internos y externos, en los internos fueron diseñados para redes de pequeño tamaño, las cuales manejan pequeñas cantidades de rutas y son administradas sobres unas mismas políticas, y los protocolos externos fueron diseñados para manejar un gran volumen de rutas y servir como puente de conexión entre los diferentes protocolos internos entre diferentes redes con independiente administración.

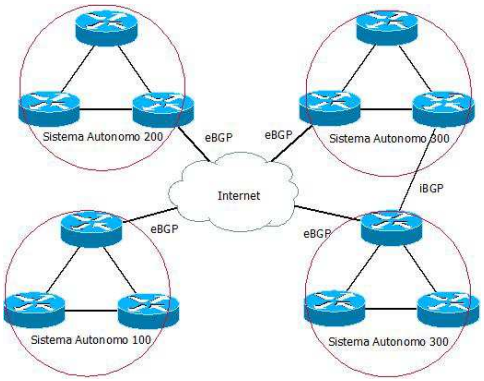
Este protocolo es utilizado en los Routers de borde, los cuales tienen como función compartir y aprender grandes cantidades de rutas como por ejemplo las que se manejan en Internet, es el protocolo más robusto y el cual permite interconectar distintas redes de gran tamaño entre sí.

En los protocolos externos se encuentra iBGP y eBGP, los cuales la *i* representa interno del mismo sistema de administración y la *e* externo del sistema de administración, conocidos como sistemas autónomos.

3.2.1. Sistemas Autónomos

Los sistemas autónomos, son sistemas los cuales están definidos por sus propias políticas de administración, y son independientes de otros, es decir cuando una compañía posee una red pública en Internet, la cual tiene sus propias políticas para su funcionamiento y es independiente del resto de redes en Internet se define como un sistema autónomo, como el caso de un ISP. Como se ve en la siguiente grafica:

Figura 13: Sistemas Autónomos.



Fuente: Autor

Estos sistemas son identificados entre sí por un numero asignado por la IANA, y al igual que una dirección IP, un mismo número no puede ser asignado a dos sistemas autónomos diferentes.

3.2.2. Vecinos BGP

El funcionamiento de BGP se realiza mediante la conexión entre dos Routers de borde, los cuales establecen una sesión entre sí para compartir rutas, en donde tanto uno como el otro anuncia todas las rutas que tiene en su tabla de enrutamiento, de tal manera que enriquece esta, conteniendo una gran cantidad de información.

De tal manera que un router de borde puede establecer cuantas sesiones BGP, con cuantos vecinos contenga la red donde se está compartiendo rutas, por ejemplo el NAP Colombia, el cual contiene todos los ISP de Colombia.

3.2.3. Inicio de sesión BGP

A diferencia de los otros protocolos de enrutamiento BGP utiliza el protocolo TCP/IP para realizar sus sesiones y compartir rutas entre sí, con lo cual utiliza

cuatro tipos de mensajes TCP para establecer la sesión, mantenerla y compartir rutas, son los siguientes mensajes:

- OPEN
- UPDATE
- NOTIFICATION
- KEEPALIVE

En donde OPEN, inicia el inicio de sesión entre los dos pares y contiene identificación del Sistema Autónomo de los pares, para establecer las condiciones de la sesión, el mensaje UPDATE es que se utiliza para compartir las rutas, y contiene información sobre las nuevas rutas que son advertidas, el mensaje NOTIFICATION se presenta en el momento en que ha ocurrido un error en la sesión ya sea por perdida de la sesión, desconexión, error en rutas o tiempos de respuesta demasiado altos, y por último el mensaje KEEPALIVE es el responsable de mantener la sesión abierta emitiendo señales indicando que la sesión se encuentra activa.

PARTE III

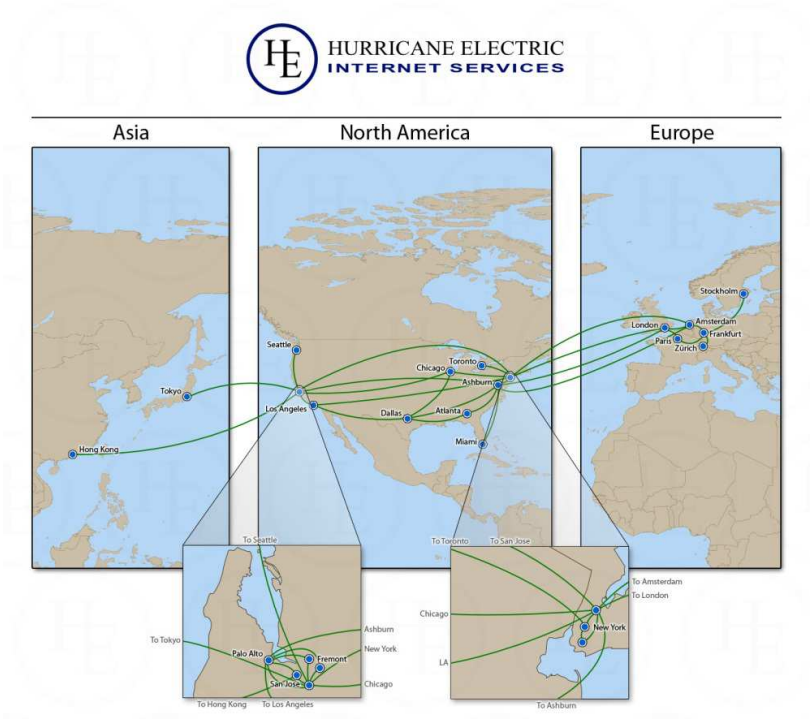
(DISEÑO E IMPLEMENTACIÓN DEL PROYECTO)

4. CAPITULO 4: DISEÑO DEL PROYECTO IPV6 DIVEO-SYNAPSIS

Para el diseño de IPv6 en Diveo-Synapsis, se realizo sobre una red anexa al Back Bone IP de la empresa, es decir sobre la red ya implementada para prestar servicios de ISP, se introdujo un nuevo segmento físico de red, el cual va a ser dedicado a IPv6.

Por otra parte para realizar la interconexión con Internet a nivel IPv6, se utilizaron 2 alternativas, la primera a nivel COLOMBIA, utilizando el NAP Colombia[6] para conectividad a nivel local en el país, y la segunda a nivel global conectándonos con Hurricane Electric[7](HE) quienes tienen un Back Bone IPv6 mundial conectado directamente a Internet. Como se establece en la siguiente grafica:

Figura 14: Back Bone HE

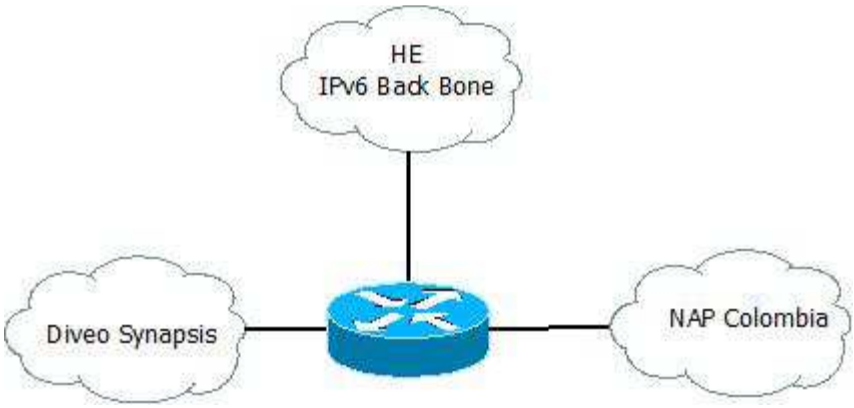


[6] Página web de NAP Colombia http://www.nap.com.co
[7] Página web de Hurricane Electric http://he.net

Fuente: Tomado de Hurricane Electric[8]

De tal manera que Diveo-Synapsis pueda tener conectividad total en IPv6. Siendo la siguiente grafica el esquema de red con el cual se va a Implementar el protocolo.

Figura 15: Esquema de Red IPv6



Fuente: Autor

De aquí que se va a segmentar la implementación del proyecto en 3 grandes aspectos, conexión en Diveo-Synapsis, conexión HE y conexión con el NAP Colombia. Que a pesar que se encuentren separados lógicamente, actuaran en un solo diagrama de red.

Por otra parte es necesario implementar un servidor DNS al cual se le va a delegar la resolución de nombres en el prefijo asignado por LACNIC.

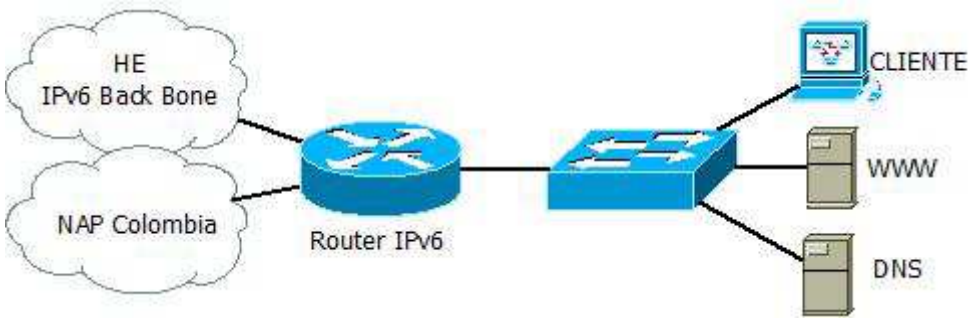
4.1. CONEXIÓN DIVEO-SYNAPSIS

En el segmento que corresponde a Diveo-Synapsis, va a ser subdivido en 2 partes, donde van a estar los dispositivos de uso uno único IPv6, entre ellos el servidor DNS, y la otra parte que es donde estará los dispositivos IPv4 que deseen tener una configuración dual, es decir IPv4 e IPv6 por igual, esto con el fin de dar conectividad a dispositivos ya existentes a la nueva red.

Para la red inherente a IPv6 se va a tener la siguiente topología:

[8] Tomado de http://he.net/Hurricane_Electric_Geographic_Network_Map.jpg

Figura 16: Topología IPv6

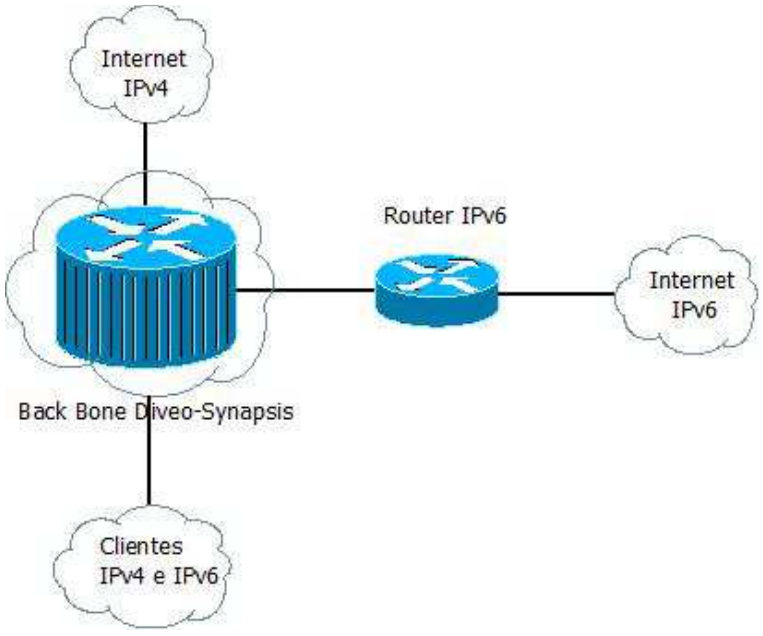


Fuente: Autor

En donde, además del servidor DNS, se va a tener un servidor HTTP y un cliente para realizar las pruebas iníciales.

Para el segmento de red dual, se va a realizar mediante la habilitación de IPv6 en un segmento de red en Diveo-Synapsis de tal manera se pueda realizar mediante una VLAN y sea indiferente a los Clientes del ISP que tiene actualmente, en la siguiente grafica se evidencia la forma:

Figura 17: Topología de red IPv4 e IPv6



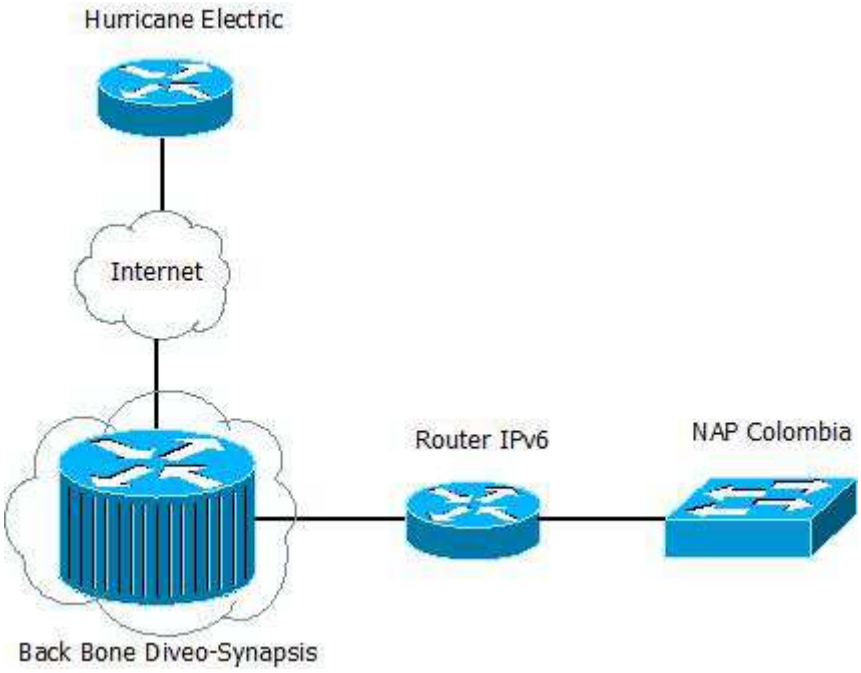
Fuente: Autor

En donde la puerta de enlace será el Back Bone de Diveo-Synapsis, para la salida normal a internet y el Router IPv6 será el encargado de dar salida por este protocolo, ya sea mediante HE o mediante el NAP Colombia para conexiones en el país, haciendo que el trafico que sea local no tenga que dirigirse hasta Estados Unidos y devolverse, aumentando la eficiencia en el diseño.

4.2. CONEXIÓN CON HURRICANE ELECTRIC

A nivel lógico se tiene un enlace entre el Router IPv6 y HE, puesto que no existe una conexión directa IPv6 es necesario hacerlo mediante un túnel, por lo cual se va a usar el protocolo 6to4 usando internet IPv4 de la siguiente manera:

Figura 18: Túnel 6to4 con HE



Fuente: Autor

Es decir el túnel va a realizar una conexión directa con HE y el Router IPv6, usando internet en IPv4, de tal manera que entre los dos dispositivos se identifiquen de manera directa y sea transparente el enlace.

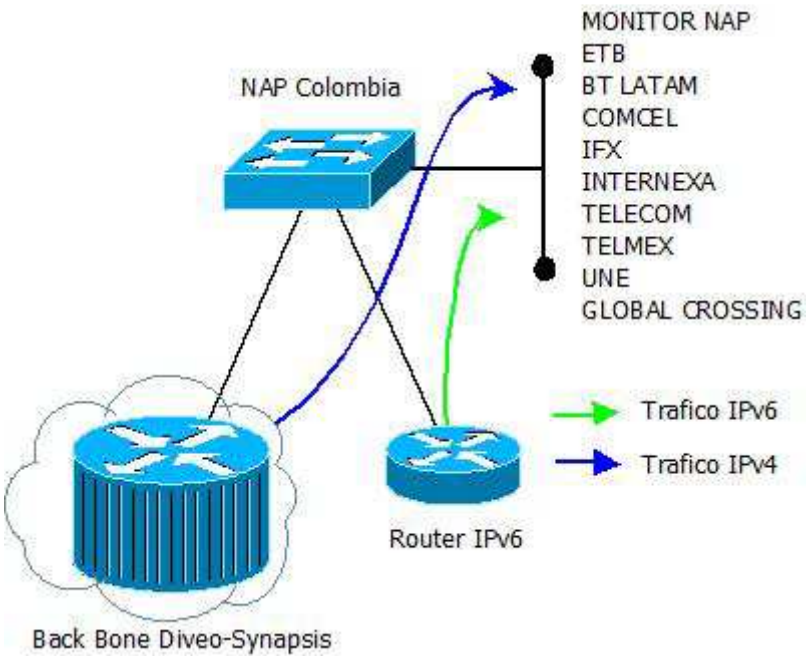
Para que, pueda establecer una sesión BGP entre ellos y se empiece a compartir rutas directo con Internet.

4.3. CONEXIÓN CON EL NAP COLOMBIA

Para la conexión con el NAP Colombia se va hacer mediante el conmutador principal del NAP, en donde llegan todos los ISP en Colombia sin importar si es IPv6 o IPv4, de aquí se va realizar la sesión BGP con cada uno de los participantes, es decir cada ISP tiene una sesión activa con cada miembro, para que así se pueda compartir rutas con todos los miembros. El Router IPv6 va a establecer las sesiones BGP en IPv6, de tal manera que en IPv4 sea encargado el Back Bone de Diveo-Synapsis.

En la siguiente grafica se muestra de una manera más comprensible:

Figura 19: Conexión con el NAP COLOMBIA



Fuente: Autor

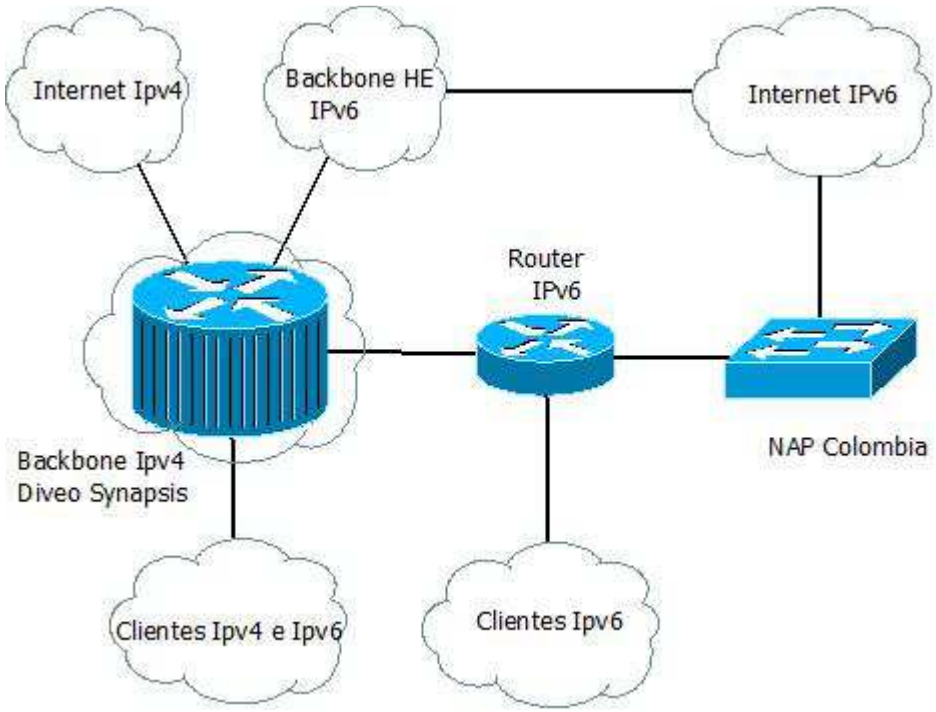
Aquí se puede ver que aunque el trafico IPv6 e IPv4 van a estar en el mismo switch, cada sesión BGP va a ser independiente del protocolo.

*Nota: los ISP nombrados son aquellos con los cuales se va a realizar la sesión IPv6, todos ellos se encuentran conectado en el NAP Colombia y pueden ser consultados en la página web del NAP (*http://www.nap.com.co/Peers.php*).*

4.4 DISEÑO UNIFICADO

Una vez diseñado cada segmento de la red, se procede a unificar todo en un solo diseño, en donde se determine todo el proceso para dar salida a Ipv4 e Ipv6 de manera simultánea como se observa en la siguiente figura:

Figura 20: Diseño unificado



Fuente: Autor

En donde se observa como el dispositivo de enrutamiento IPv6 establece su conexión con el NAP Colombia, y con HE este ultimo mediante un túnel IPv6toIPv4, dando interconectividad con Internet IPv6 he IPv4 simultáneamente.

5. CAPITULO 5: IMPLEMENTACION DEL PROYECTO IPV6

Como se menciona antes, se desarrolla el proyecto en una red anexa a la red de Core de Diveo-Synapsis, en done se va tener como componente principal un Router el cual será el responsable de dar la salida hacia Internet en IPv6, ya sea mediante el NAP Colombia o vía HE.

Además se implementara un Servidor DNS, al cual se le delegara la resolución de nombres correspondientes al prefijo asignado por LACNIC, dos servidores WEB IPv6 en UNIX y WINDOWS para realizar pruebas de servicio independiente del S.O. que se use, para cubrir posibles incompatibilidades, y por ultimo una maquina que será encargada de simular al primer cliente a la nueva red.

Para estos últimos se va a utilizar un servidor de virtualización, en donde estarán alojados todos los servidores, con el fin de disminuir costos en dispositivos físicos y maximizar la utilización de recursos en el servidor.

Teniendo planteado el escenario de red, se enlista los componentes a utilizar para la implementación del mismo:

- Router Cisco con soporte en IPv6 y BGP.
- Servidor con soporte en Virtualización.
- Software de virtualización (VMware).
- Software servidor DNS, servidores WEB y cliente.
- Red de Back Bone IPv4[9].
- Red de distribución (Cableado, switches).

El servidor se encontrara en el Data Center que posee Diveo-Synapsis y este usara la red de distribución que ya posee la empresa para llevar a cabo la conexión entre los diferentes equipos.

Por otra parte se va a proteger la red mediante FIREWALL e IPS, con el fin de salvaguardar la integridad, disponibilidad y confidencialidad de la información y de los equipos que pertenezcan a la red. Para esto se usara un Firewall cisco con soporte IPv6.

[9] Nota Aclarativa: Esta red se nombrara como un componente único para salvaguardar la confidencialidad de la misma.

5.1. DESCRIPCIÓN DE DISPOSITIVOS

A continuación se hará una descripción de los dispositivos y software que se va a utilizar en la implementación del proyecto pasando desde los servidores virtuales hasta el Router de Core IPv6.

5.1.1. Servidor de Virtualización

Para este servidor se va a utilizar una maquina con las siguientes características:

- Servidor HP Proliant DL 360 G5.
- 12GB en memoria RAM física.
- Capacidad de almacenamiento de 146GB en Raid 1, para términos de integridad en la información.
- 2 tarjetas de red con velocidad de 1Gbps.

Nota: la capacidad de memoria RAM fue calculada sumando la capacidad de memoria de cada servidor a virtual izar que se va utilizar y duplicando la misma, es decir si un servidor normal consume 2GB de memoria se contempla 4GB, esto con el fin de dar escalabilidad en recursos virtuales. Por otra parte se tiene una tarjeta de red de gestión del servidor y otra por donde será conectada la red IPv6 para darle acceso a las maquinas virtuales.

5.1.2. Software de virtualización

El software que se va a utilizar para la virtualización es VMware ESXi 5.0[10], puesto que cuenta con la mejor plataforma de virtualización en el mercado, además de poseer una licencia gratuita.

Este Software es un sistema operativo UNIX, el cual se instala en el servidor "Anfitrión", y crea una capa de independencia entre todas las maquinas que tenga alojadas, es decir que para el mismo Hardware se va a utilizar en cada máquina de manera independiente sin que una tenga que relación con la otra. Como se muestra en la siguiente grafica:

[10] Página web de VMware http://www.vmware.com

Figura 21. Servidor ESXi

Fuente: Tomado de VMware[11]

La forma de gestionar las maquinas virtuales, es mediante vSphere Client de VMware, el cual actúa como cliente y posee una interfaz donde se puede visualizar cada máquina de manera nativa como si se tratara físicamente.

5.1.3. Software servidor DNS, servidores WEB y cliente

Para el servidor DNS se va a utilizar como sistema operativo RED HAT ENTERPRISE 5.5, debido a su alto rendimiento en cuanto servidores, teniendo soporte integrado para DNS con paquetes certificados por RED HAT[12].

En cuanto al software para DNS, se utilizara BIND9[13], puesto que es el servidor más robusto utilizado a nivel mundial para la implementación de este tipo de servidores. El cual tiene soporte nativo para IPv6.

Continuando con la implementación, los servidores WEB de prueba van a estar soportados en dos sistemas operativos independientes, para el servidor numero 1 se usara Ubuntu Server[14], puesto que es liviano y no tiene un mayor impacto en el consumo de recursos, y en el servidor numero 2 se utilizara Windows Server 2008 R2[15], siendo un sistema operativo totalmente diferente y uno de los más utilizados a nivel mundial, todo esto con el fin de solventar cualquier problema de incompatibilidad que se presente en la implementación.

---

[11] Tomado de http://www.vmware.com/files_inline/images/products_esx_esxi_diagram.jpg-
[12] Página web de Red Hat http://www.redhat.com/
[13] Página web de BIND9 http://www.isc.org/software/bind
[14] Página web de Ubuntu server http://www.ubuntu.com/business/server/overview
[15] Página web Windows server http://www.microsoft.com/es-xl/servidores-nube/windows-server/default.aspx

Y por ultimo para el cliente se usara Fedora 16[16], debido a que es el sistema operativo libre más usado a nivel corporativo, el cual cuenta con completo soporte para IPv6.

5.1.4. Router Cisco con soporte IPv6

Para el proyecto se decidió usar un Router Cisco de la serie 2900[17], puesto que es un Router de gama media, el cual soporta un tráfico de hasta a nivel WAN 75Mbps, contando con flexibilidad para soportar múltiples tecnologías como ATM, FR, ETH, entre otros. Cuenta con 3 interfaces Giga Ethernet navitas y 4 módulos WAN, fuente de energía redundante, además de soporte en IPv4 e Ipv6, Multicast, MPSL y protocolos de enrutamiento de borde como OSPF, BGP.

Cumpliendo con todas las garantías para el proyecto sin ser sobrevalorado en alguna.

5.1.5. Firewall Cisco con soporte IPv6

Se decidió usar un Firewall Cisco ASA 5510[18], teniendo como principal característica la cantidad de tráfico que soporta llegando hasta 300 Mbps, además se soportar IPS y VPN, con 5 interfaces Fast Ethernet.

Cumpliendo con esto a cabalidad con la seguridad informática de la red, con la utilización de FW e IPS como principal característica.

---

[16] Página web de Fedora http://fedoraproject.org/es/
[17] Página web del Router Cisco 2900 http://www.cisco.com/en/US/products/ps10540/index.html
[18] Página web del Firewall Cisco ASA 5510 http://www.cisco.com/en/US/prod/collateral/vpndevc/ps6032/ps6094/ps6120/product_data_sheet0900aecd802930c5.html

5.2. CARACTERÍSTICAS DE LA RED

La red contara con las siguientes características además del soporte en IPv6, y teniendo en cuenta la capacidad de los equipos:

Tabla 4: Características de la red

Característica	Tipo	Descripción
Trafico por Router Core	Hasta 1Gbps	Trafico total soportado en el Core de la red, saliente y entrante desde y hacia Internet.
Trafico Firewall	Hasta 300Mbps	Trafico total soportado por el Appliance en Firewall.
Trafico IPS	Hasta 150Mbps	Trafico total configurado para prevención de intrusos, en el Appliance Firewall.
Usuarios Soportados por servidor DNS.	Hasta 2000 usuarios simultáneos.	Esta cantidad depende de la cantidad de memoria RAM y procesador que se asigne virtualmente, por lo que tiene un estimado.

Fuente: Autor

5.3. COSTOS DE LA SOLUCIÓN

En los costos se tendrán en cuenta solo los equipos a usar, puesto que los medios ya implementados hacen parte de la red IPv4 de Diveo-Synapsis, como por ejemplo, red de distribución (Switches y cableado), la conexión con el NAP, y la salidas a internet que se tengan.

Por lo que se procede a realizar el cálculo de la solución.

Tabla 5: Costos

Recurso	Marca	Valor en US	Valor en Pesos
Router 2911	Cisco	2.600,00 US	4’680.000,00 $
Firewall Asa 5510	Cisco	4.500,00 US	8’100.000,00 $
Servidor HP Proliant G5.	Hewlett Packard	1.300,00 US	2’340.000,00 $
Software Virtualización VMWARE	Vmware ESXi	0,00 US	0,00 $
Sistema Operativo DNS	RED HAT 5.5 (Sin soporte)	0,00 US	0,00 $
Sistema operativo Servidores Clientes y web.	Ubuntu, Fedora (Libre)	0,00 US	0,00 $
Total		9.300,00 US	16’740.000,00$

Fuente: Diveo-Synapsis.

Estos son los valores en listas, sin tener en cuenta descuentos, y tomando como valor del dólar en $ 1.800 pesos colombianos.

5.4. CONFIGURACIÓN DE LOS EQUIPOS

Como se menciona anteriormente, la red se segmentara por módulos, dentro de los cuales, se tendrá como primer punto de configuración del servidor de Virtualización, seguido de la configuración del servidor DNS, la configuración del Router IPv6 y por último la parte de seguridad en el Firewall. Cada aspecto a configurar se detallara en un anexo correspondiente al los mismos.

Cabe destacar que la configuración del la red de distribución y Core de Diveo-Synapsis no se incluirá puesto que esta de total confidencialidad de la empresa. Además características como direcciones IP públicas, usuarios de administración y demás aspectos de seguridad no se tendrán en cuenta.

PARTE IV

(CONCLUSIONES)

6. CONCLUSIONES

6.1. TÉCNICA

A pesar de que el protocolo IPv6 es un nuevo estándar y un protocolo totalmente apartado de IPv4, su implementación no tuvo impacto alguno sobre la red ya presente a nivel de configuración puesto que los 2 protocolos tienen la capacidad de coexistir de manera independiente. Sin embargo como es un protocolo muy robusto genera una gran cantidad de trafico in oficioso, es decir trafico puramente informativo que puede llegar ocupar capacidad de procesamiento en los dispositivos de enrutamiento y seguridad.

Otro aspecto importante es la seguridad que se debe contemplar puesto al tener un bloque tan grande de direcciones, pueden existir ataques informáticos sobre los dispositivos que tienen conocimiento de la red, como por ejemplo un servidor DNS o un Router. Y en cuanto a control se debe implementar mecanismos más robustos para impedir la asignación de direcciones y recursos a dispositivos no autorizados.

6.2. HUMANÍSTICA

Con esta nueva implementación se espera que no se vean limitados la capacidad de la tecnología que se tiene actualmente, garantizando una calidad de servicio excelente para los usuarios finales, y que de esta manera se utilicen la mayor cantidad de recursos eficazmente sin que se desperdicie energía o capacidad en la tecnología.

Aportando así al medio ambiente una parte importante, economizando en energía y ofreciendo un servicio de gran calidad para los usuarios finales, fomentando una buena práctica en desarrollo e investigación en pro de la sociedad y la academia.

6.3. DE IMPLEMENTACIÓN

Siendo un protocolo nuevo y apartado de IPv4, su implementación no requiere recursos adicionales a los tradicionalmente utilizados por una red IP, aunque se debe tener en cuenta que en algunos equipos antiguos el protocolo no es soportado, especialmente en dispositivos de seguridad, como por ejemplo un firewall.

Además para que su implementación no sea traumática, para los usuarios finales se debe mantener el protocolo anterior es decir IPv4, de tal manera que los 2 protocolos coexistan a medida que Internet va migrando sus servicios a este nuevo protocolo y que no existan espacios discriminados en la red.

BIBLIOGRAFÍA

- **AITCHISON, Ron;** “Pro DNS and BIND 10”, Ed. Apress 2011, consultado en 2012
- **BROWN, Sam; BROWNE, Brian; CHEN, Neal; FONG, Paul J.; HARRELL, Robbie; KNIPP, Eric; SAYLORS, Bart; WEBBER, Rob; PARENTI, Edgar; Jr. “**Configuring IPv6 for Cisco IOS**”**, Ed . Syngress Publishing, Inc. 2002, consultado en 2012
- **CISCO SYSTEMS, “**Cisco IOS IPv6 Command Reference”, Ed. Cisco systems Inc 2011, consultado en 2012
- **CRICKET Liu;** “DNS and BIND on IPv6”, Ed. OReilly 2011, consultado en 2012
- **HOGG, Scott; VYNCKE, Eric;** “IPv6 Security”, Ed Cisco press 2009, consultado en 2012
- **LAMMLE, Todd; ODOM, Sean; WALLACE, Kevin;** “CCNP Routing Study Guide”, Ed. Sybex Inc. Consultado en 2012
- **LAMMLE, Todd; ODOM, Sean; WALLACE, Kevin;** “CCNP Routing”, Ed. Sybex 2001, consultado en 2012
- **LOSHIN, Pete;** “Ipv6 Theory, Protocol, and Practice Second edition”, Ed. Morgan Kaufmann Inc. 2004, consultado en 2012
- **OSTERLOH, Heather;** “Ip Routing Primer Plus”, Ed. Sams 2002, consultado en 2012
- **POPOVICIU, Ciprian; LEVY-ABEGNOLI, Eric; GROSSETETE, Patrick;** “Deploying IPv6 Networks”, Ed. Cisco Press 2006, consultado en 2012
- **TROY, Ryan; HELMKE, Matthew;** “Vmware Cookbook 2nd Edition”, Ed OReilly 2012, consultado en 2012.

REFERENCIAS WEB

- **CISCO SYSTEMS;** “Entidad proveedora de equipos de conectividad”, Características del equipo Router Cisco 2900 http://www.cisco.com/en/US/products/ps10540/index.html, consultado en 2012.
- **CISCO SYSTEMS;** “Entidad proveedora de equipos de conectividad”, Características del equipo Firewall Cisco ASA 5510 http://www.cisco.com/en/US/prod/collateral/vpndevc/ps6032/ps6094/ps6120/product_data_sheet0900aecd802930c5.html, consultado en 2012.
- **DOMÍNGUEZ, José A.;** “SEGURIDAD EN BGP”, Slide sobre configuración BGP http://ws.edu.isoc.org/workshops/2004/CEDIA2/material/Seguridad_en_BGP.pdf, consultado en 2012.
- **FEDORA;** “Entidad proveedora de software de Sistema Operativo Fedora Linux”, Fedora 16 http://fedoraproject.org/es/, consultado en 2012.
- **HURRICANE ELECTRIC ISP;** “Entidad encargada de prestart Servicio de Internet IPv6, a nivel mundial”, Hurricane Electric http://he.net, consultado en 2012.
- **INTERNET ASSIGNED NUMBERS AUTHORITY;** “Entidad encargada de asignar direcciones IP mundiales”, http://www.iana.org, consultado en 2012.
- **INTERNET PROTOCOL, VERSIÓN 6 (IPV6);** “Request for Comments, documentación técnica oficial sobre Internet”, RFC 2460 en http://www.rfc-es.org/rfc/rfc2460-es.txt, consultado en 2012.
- **INTERNET PROTOCOL;** “Request for Comments, documentación técnica oficial sobre Internet”, RFC 791 en http://www.rfc-es.org/rfc/rfc0791-es.txt, consultado en 2012.
- **INTERNET SYSTEMS CONSORTIUM;** “Entidad proveedora de software de servidor DNS BIND9”, BIND9 http://www.isc.org/software/bind, consultado en 2012.
- **IP VERSION 6 ADDRESSING ARCHITECTURE;** “Request for Comments, documentación técnica oficial sobre Internet”, RFC 2373 en http://www.ietf.org/rfc/rfc2373.txt, consultado en 2012.
- **LACNIC;** “Teoría y Configuración de BGP”, Slide sobre configuración de BGP http://lacnic.net/documentos/lacnicxii/presentaciones/08_bgp.pdf, consultado en 2012.
- **LATIN AMERICA & CARIBBEAN NETWORK INFORMATION CENTRE;** “Entidad encargada de asignar direcciones IP en Latinoamérica y el Caribe”, http://lacnic.net, consultado en 2012.

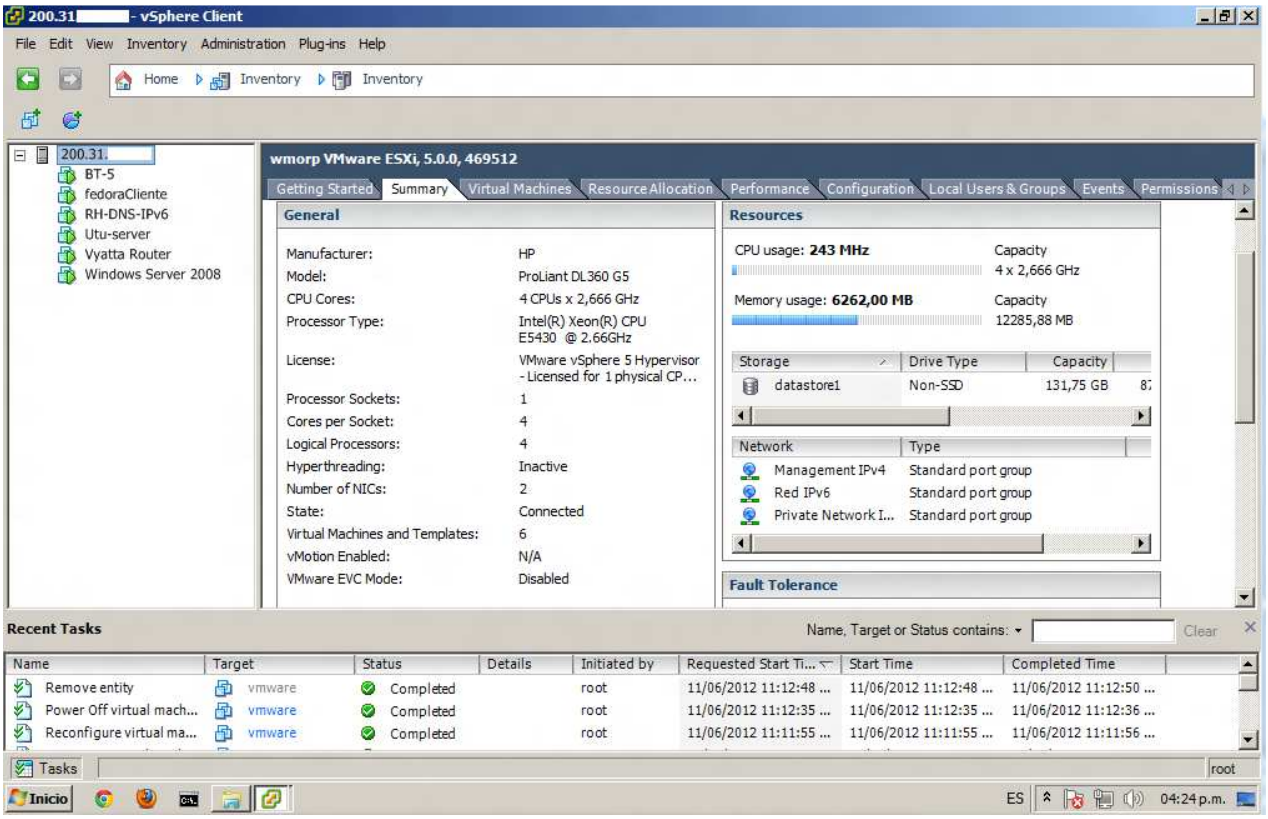
- **MICROSOFT;** “Entidad proveedora de software de Sistema Operativo Windows Server”, Windows Server 2008 http://www.microsoft.com/es-xl/servidores-nube/windows-server/default.aspx, consultado en 2012.
- **NETWORK ACCESS POINT COLOMBIA;** “Punto de acceso de Internet, a nivel nacional”, NAP Colombia http://www.nap.com.co, consultado en 2012.
- **RED HAT;** “Entidad proveedora de software de Sistema Operativo Red Hat Linux”, Red Hat http://www.redhat.com/, consultado en 2012.
- **ROQUE, Gagliano;** “ICMPv6, DHCPv6 y Túneles”, Slide sobre ICMP, DHCP y Túneles http://www.lacnic.net/documentos/ipv6tour2008/costarica/icmpv6-roque_gagliano.pdf, consultado en 2012.
- **UBUNTU;** “Entidad proveedora de software de Sistema Operativo Ubuntu Linux”, Ubuntu Server http://www.ubuntu.com/business/server/overview, consultado en 2012.
- **VMWARE;** “Entidad proveedora de software de virtualización Vmware”, VMware http://www.vmware.com, consultado en 2012.

ANEXOS

En esta sección se tendrán en cuenta todos los aspectos, de configuración del proyecto, incluyendo equipos, servidores y demás. No se tendrán en cuenta aspectos configuración que sean confidenciales de Diveo-Synapsis.

Anexo 1. Configuración Vitalización

Como primer aspecto se debe instalar en el servidor el hypervisor de Vmware, ESXi el cual será el responsable de la ejecución de las maquinas virtuales, al cual se accederá de manera remota para la administración, mediante el cliente vSphere de Vmware obteniendo la siguiente consola:

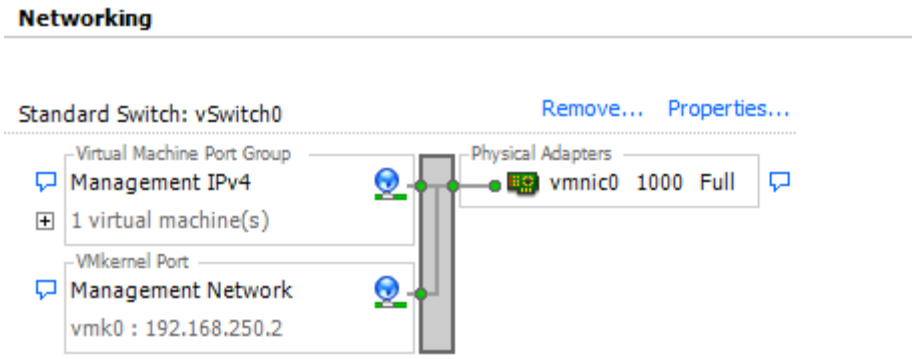


En el cual en la parte izquierda, se listan las maquinas virtuales alojadas en el servidor, de entre las cuales se destaca el servidor DNS, el servidor Ubuntu web, el cliente y el servidor Windows 2008.

En el otro segmento del programa se observa, la consola de configuración donde se enlista a manera de pestañas. Y por último se encuentra en la parte inferior la barra de información, donde se muestra todos los eventos que se hagan sobre el servidor y las maquinas.

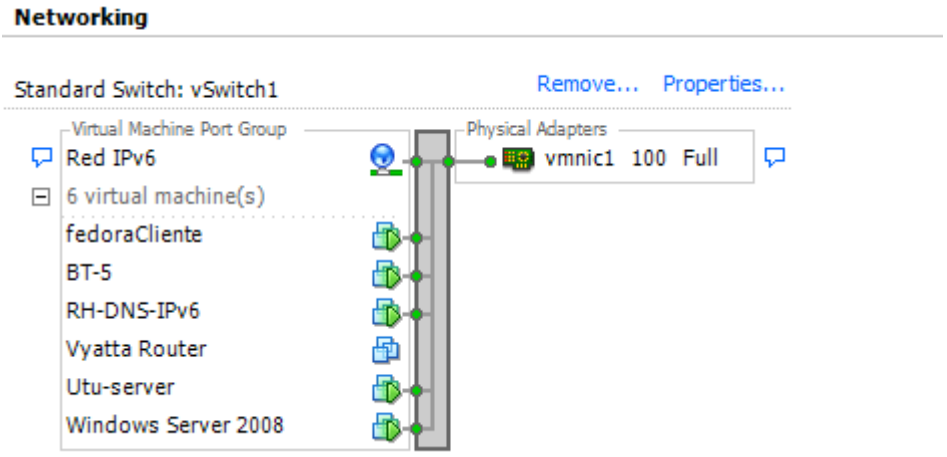
Un aspecto importante a configurar es la red, por lo cual en la pestaña de configuración y Networking. Se obtiene lo siguiente:

2 interfaces de red, las cuales se comportaran como un switch virtual, el cual tendrá la función de dar conectividad tanto a las maquinas virtuales como al servidor en sí.



La primera interfaz será destinada para la gestión del equipo, la cual tendrá un direccionamiento en IPv4, además si alguna maquina virtual necesita ser gestionada, o necesita salir a Internet Ipv4 lo hará mediante esta.

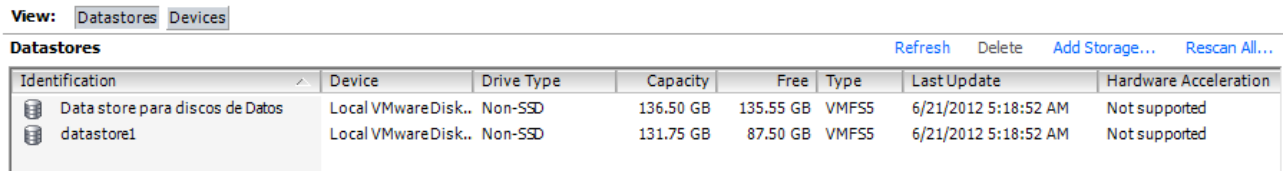
Para la segunda interfaz se tiene lo siguiente:



En esta se decidió crear un grupo de puertos, los cuales tendrán la Vlan nativa para poder ser conectados hacia la red IPv6. En los cuales se encuentra las maquinas virtuales que desean salir hacia Internet Ipv6.

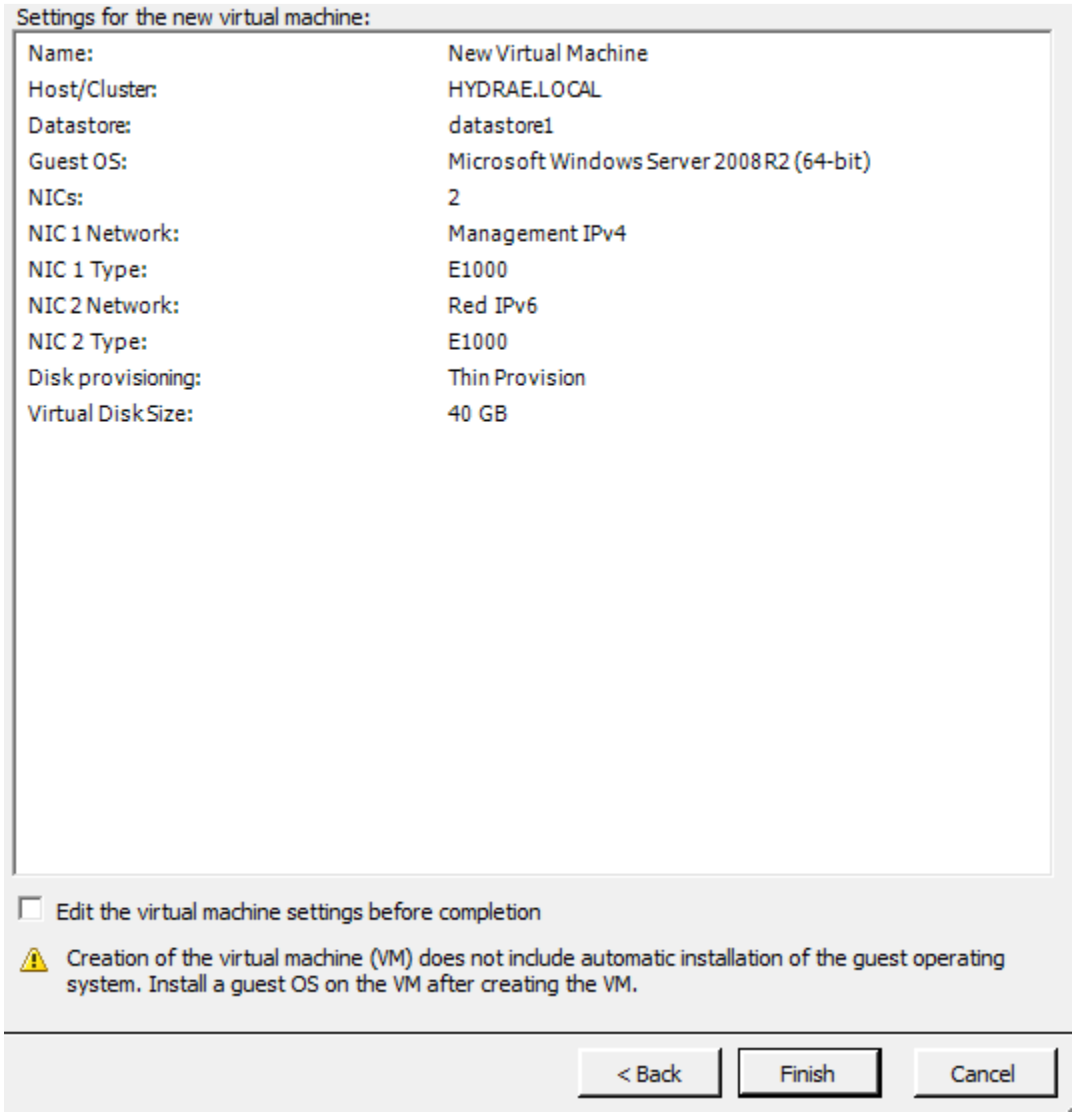
Para el almacenamiento se uso un arreglo de discos Raid 1, de 146 GB, en los cuales se aprovisionara el espacio para los discos virtuales de las maquinas; cabe destacar que se usara thin provisioning para esto, puesto que es una de las tecnologías desarrolladas por Vmware, la cual usa de mejor manera el espacio en disco, asignando solo el espacio consumido a los discos virtuales sin que se

desperdicie zona alguna. Visto en configuración, Data store de la siguiente manera:



También se asigna otro arreglo de discos en Raid 1, para ubicar todos los discos o particiones virtuales que tengan que ver con datos, esto con el fin de no degradar el arreglo principal donde se encuentran los discos duros virtuales de sistemas operativos de las maquinas.

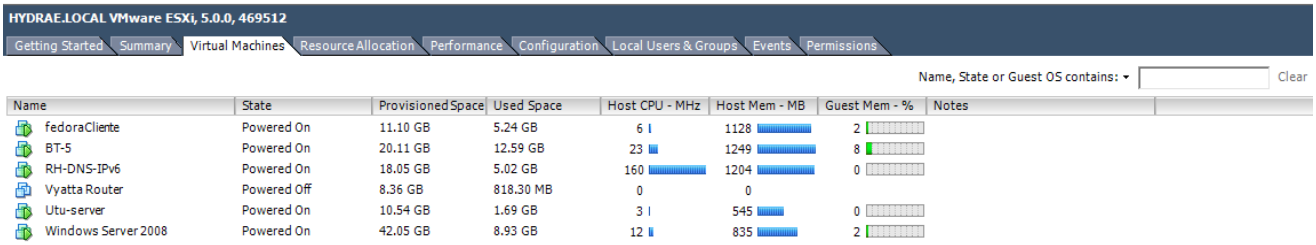
Una vez configurado esto, el proceso para crear una maquina virtual es casi que intuitivo, en donde se asignan recursos físicos de acuerdo a las necesidades de la maquina, sin que estas lleguen a ocasionar conflictos con las demás. Haciéndolo desde la primera pestaña en la opción de creación de una maquina virtual obteniendo los siguientes resultados:



La advertencia que muestra la creación de la maquina virtual, dice que este ha sido un proceso para la creación del hardware de la misma, con lo cual se debe instalar el sistema operativo de manera independiente; esto se hace activando la maquina virtual y asociando el medio donde se encuentre el SO, e instalando como si se tratase de un servidor físico.

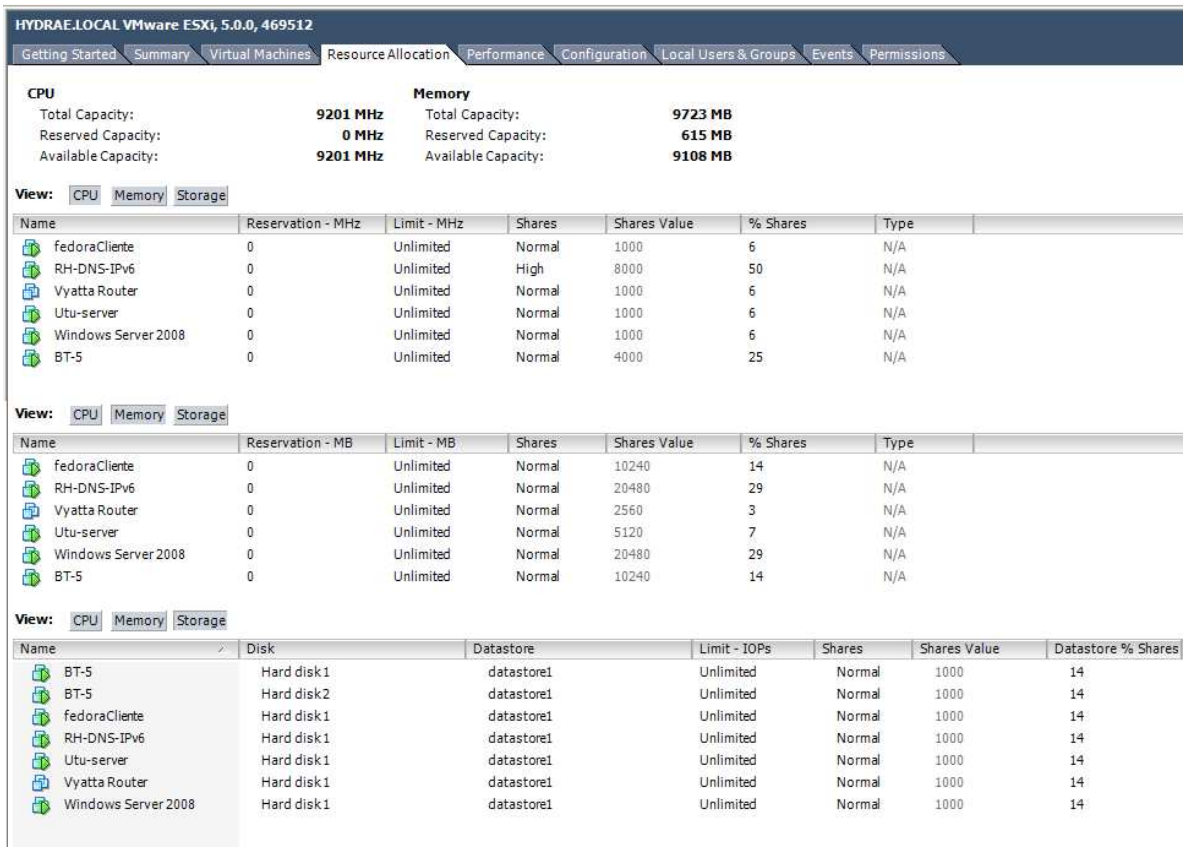
Una vez creadas e instaladas las maquinas virtuales, se procede a verificar el correcto funcionamiento del servidor, y que el rendimiento del mismo no se vea afectado. Para esto se debe tener en cuenta 3 aspectos, el estado de las maquinas, los recursos asignados a las mismas y el rendimiento del servidor.

Para verificar el estado de las maquinas se hace en la pestaña de las mismas en donde se tiene el siguiente resultado:

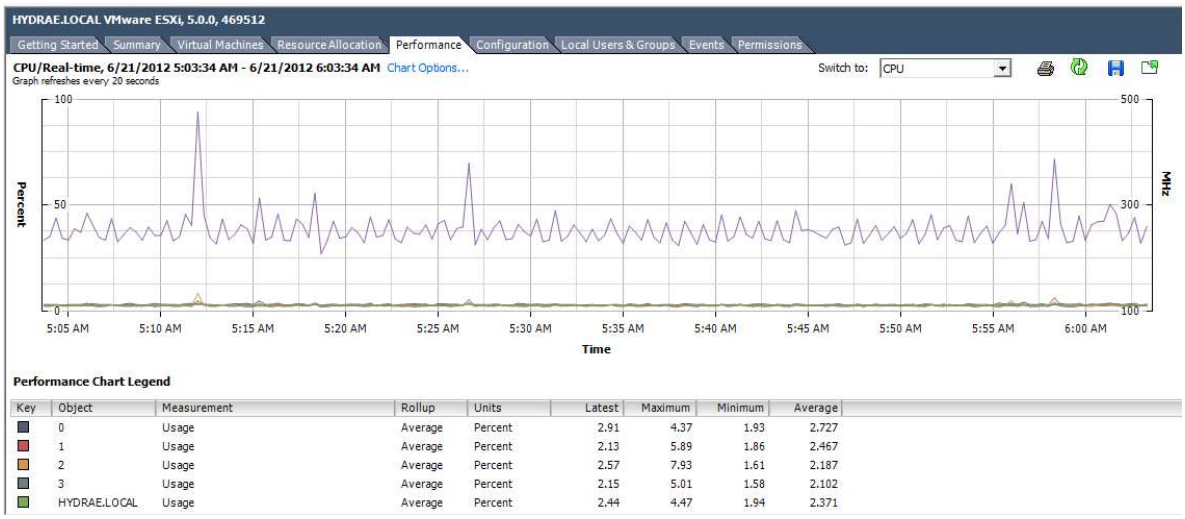


En donde se observa si se encuentra prendida, la cantidad de disco que tiene aprovisionado, la cantidad de disco que está usando, la cantidad de procesamiento en MegaHerz, y el nivel de memoria asignado y usado.

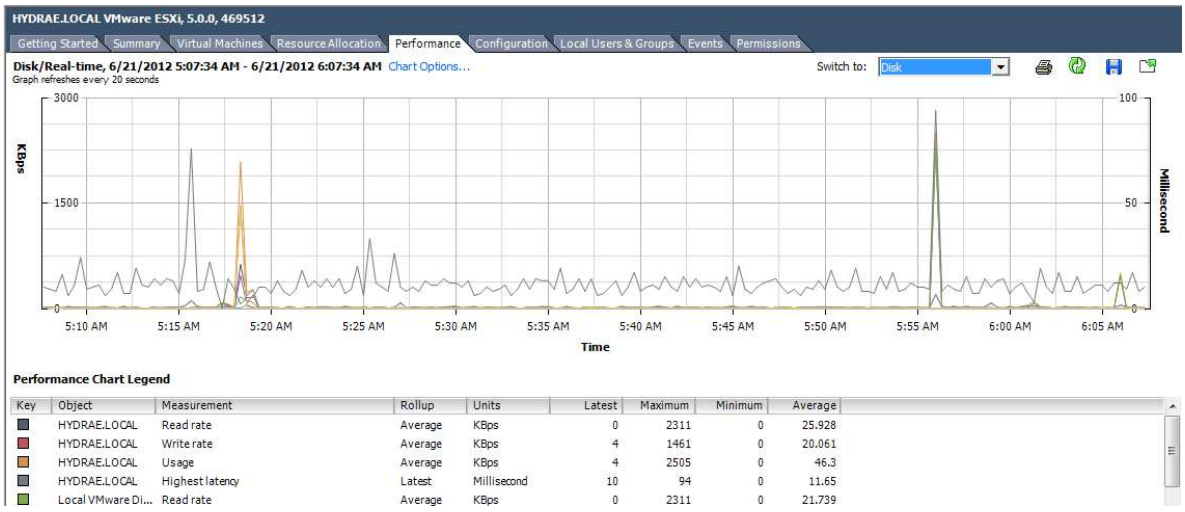
Para verificar el estado de los recursos asignados, se hace en la pestaña correspondiente, en donde se verifica la transaccionalidad de los procesos en CPU, memoria y lectura/escritura en discos duros. Todo esto se puede limitar si se desea tener un mejor control de los mismos.



En la pestaña de rendimiento se puede observar el comportamiento del servidor, y si este se encuentra copado en recursos o por el contrario tiene oportunidades de crecer más.

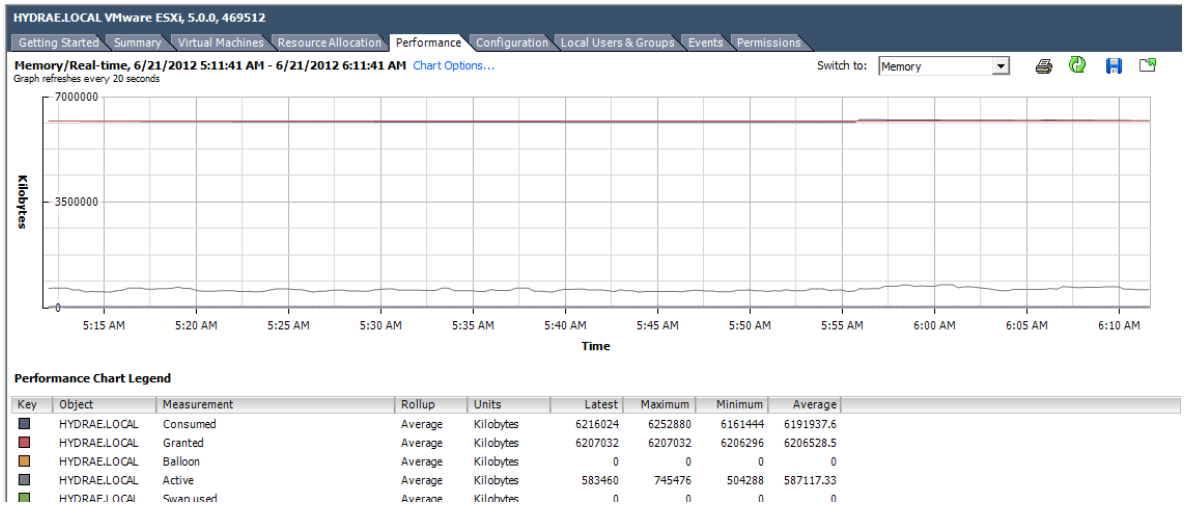


Como primer aspecto se observa que en el rendimiento de procesamiento se encuentra por debajo del 50%, con algunos picos de procesamiento, indicando que el servidor se encuentra en un buen estado en cuanto a procesamiento.



En cuanto al uso de Discos duros se evidencia un comportamiento estable de escritura y lectura, tanto en Kbps como en milisegundos.

Por último se procede a la verificación de rendimiento de memoria, en cuanto a capacidad total utilizada, por las maquinas virtuales.



Con esto se evidencia que el uso aproximado de memoria es de 6 GB, siendo la mitad de la memoria física total del servidor.

Una vez conocido todo esto se concluye que el servidor se encuentra a la mitad de la capacidad máxima, dando posibilidades de escalamiento y crecimiento de la misma.

Anexo 2. Configuración servidor DNS

Como primer aspecto se va a usar Red Hat 5.5 sobre el cual se va a configurar el servidor DNS.

Por lo cual se debe configurar una dirección IP estática la cual responderá a la salida a internet IPv6 de la siguiente manera:

```
[root@nsip6 named]# ifconfig eth0
eth0      Link encap:Ethernet  HWaddr 00:0C:29:66:E7:A9
          inet6 addr: 2803:b000:8000::33/64 Scope:Global
          inet6 addr: fe80::20c:29ff:fe66:e7a9/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:408065 errors:0 dropped:0 overruns:0 frame:0
          TX packets:256399 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:41699854 (39.7 MiB)  TX bytes:26122876 (24.9 MiB)

[root@nsip6 named]#
```

Una vez instalado BIND9 se procede a realizar la configuración respectiva al servicio.

```
  GNU nano 1.3.12            File: named.conf

// Red Hat BIND Configuration Tool
//
// Default initial "Caching Only" name server configuration
//

options {
        directory "/var/named";
        dump-file "/var/named/data/cache_dump.db";
        statistics-file "/var/named/data/named_stats.txt";
        /*
         * If there is a firewall between you and nameservers you want
         * to talk to, you might need to uncomment the query-source
         * directive below.  Previous versions of BIND always asked
         * questions using port 53, but BIND 8.1 uses an unprivileged
         * port by default.
         */
        listen-on-v6 { any; };
        query-source address * port 53;
};

                        [ Read 74 lines ]
^G Get Help  ^O WriteOut  ^R Read File ^Y Prev Page ^K Cut Text  ^C Cur Pos
^X Exit      ^J Justify   ^W Where Is  ^V Next Page ^U UnCut Text^T To Spell
```

Lo anterior corresponde al archivo de configuración del servicio “named.conf”, en donde como primera instancia se va listar las opciones con las que va a cargar el servicio.

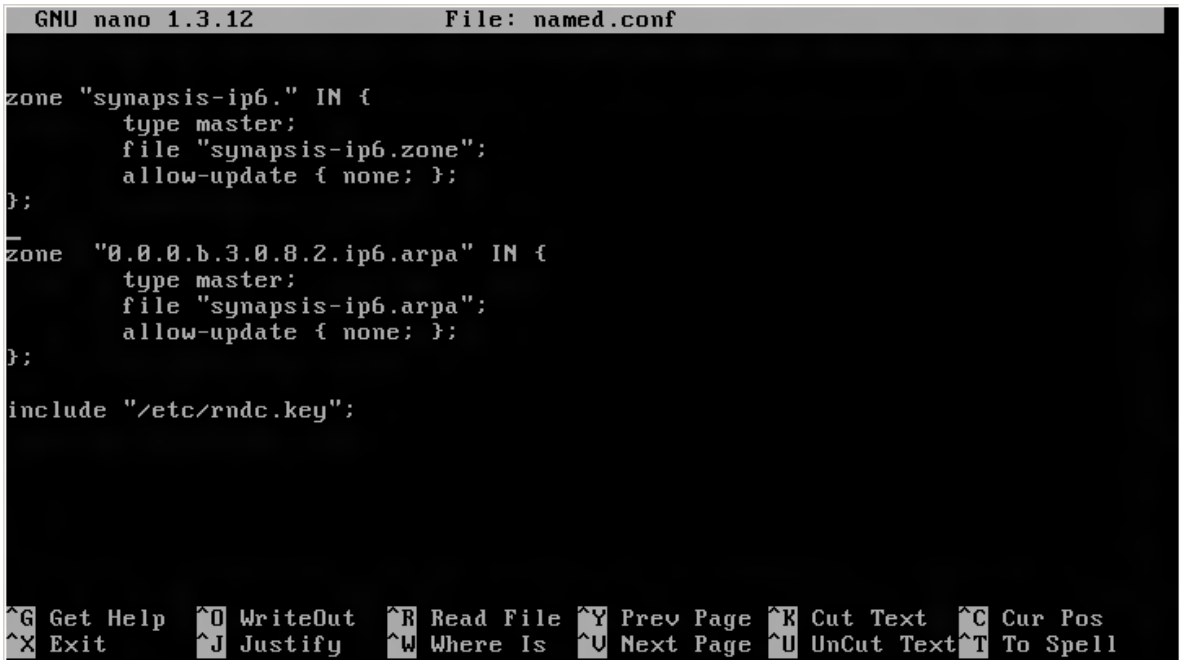
De las más relevantes son:

 # listen-on-v6 { any; };

La cual dice que debe escuchar sobre cualquier dirección IPv6 que tenga configurada.

 # query-source address * port 53;

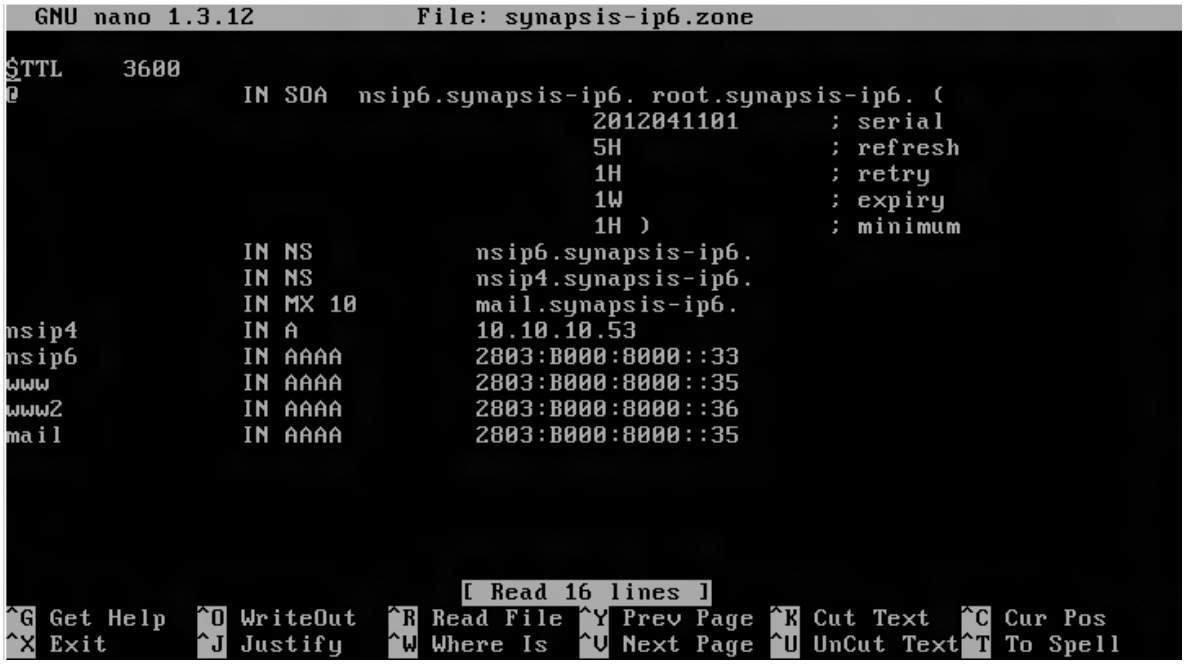
Esto aclara que debe aceptar peticiones que vengan de cualquier dirección y sean dirigidas hacia el puerto 53 el cual es usado por DNS como estándar.



Esto corresponde a la configuración del archivo de zona y de su respectiva resolución inversa.

En donde se creara una zona de ejemplo, llamada sunapsis-ip6 la cual va a ser de tipo maestra y su dirección de configuración inversa corresponderá a la dirección 0.0.0.b.3.0.8.2.ip6.arpa.

Una vez hecho esto se debe realizar la configuración de la zona, donde se incluirá los registros.



En este archivo se encuentra toda la configuración de la zona desde, los parámetros de delegación y autoridad de la zona, done se incluye como principal parámetro el serial, el cual se debe actualizar cada vez que se haga un cambio en la zona con esto determinara la autoridad sobre los servidores que actúen como secundarios de la zona.

Seguido de esto se encuentran los registros, en el ejemplo se incluyen nsip6, www, www2, y mail los cuales responderán a los servidores DNS, Ubuntu y Windows 8 respectivamente.

Seguido de esto se encuentra el archivo de configuración de resolución inversa, donde se encontrara los registros PTR, los cuales apuntan de manera inversa a los servicios.

La forma que tienen es la dirección escrita de manera inversa separando cada símbolo en hexadecimal mediante un punto. Es decir para el registro www.synapsis-ip le corresponderá la dirección finalizada en 8000::35, como el archivo corresponde al segmento 2803:B000:: la dirección final será 2803:B000: 8000::35.

Una vez hecho esto se procede a hacer las pruebas respectivas.

```
[root@nsip6 named]# nslookup
> set type=any
> www.synapsis-ip6
Server:         2803:b000:8000::33
Address:        2803:b000:8000::33#53

www.synapsis-ip6        has AAAA address 2803:b000:8000::35
> exit

[root@nsip6 named]# ping6 www.synapsis-ip6
PING www.synapsis-ip6(www.synapsis-ip6) 56 data bytes
64 bytes from www.synapsis-ip6: icmp_seq=0 ttl=64 time=2.26 ms
64 bytes from www.synapsis-ip6: icmp_seq=1 ttl=64 time=0.328 ms
64 bytes from www.synapsis-ip6: icmp_seq=2 ttl=64 time=0.300 ms
64 bytes from www.synapsis-ip6: icmp_seq=3 ttl=64 time=0.291 ms

--- www.synapsis-ip6 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3004ms
rtt min/avg/max/mdev = 0.291/0.796/2.267/0.849 ms, pipe 2
[root@nsip6 named]# _
```

Como se evidencia el servidor se encuentra funcionando de manera correcta, dando la dirección correspondiente a www.synapsis-ip6, y respondiendo a las pruebas de conectividad.

Por otra parte se debe tener en cuenta que el servidor debe tener configuradas las direcciones IPv6 de los servidores Root, para que así pueda resolver de manera correcta todos los dominios que ellos tengan registrados. Esto se hace mediante el archivo named.root.

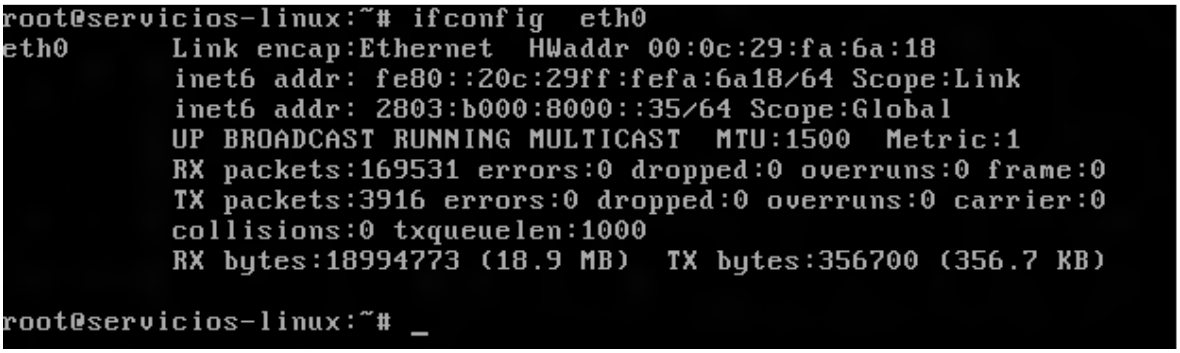
```
A.ROOT-SERVERS.NET.     3600000 IN      A       198.41.0.4
A.ROOT-SERVERS.NET.     3600000 IN      AAAA    2001:503:ba3e::2:30
```

Esto es un fragmento de ese archivo el cual contiene la dirección correspondiente al servidor Root A.root-servers.net.

Anexo 3. Configuración Cliente, y servicios adicionales.

Para la configuración de servicios adicionales se realizo mediante un servidor Ubuntu y un servidor Windows server 2008, en los cuales se configuro respectivamente el servicio web, con lo cual se realiza la prueba mediante una maquina virtual que actúa como cliente la cual tiene como sistema operativo Fedora 16, y se encuentra configurada para tener conectividad IPv6.

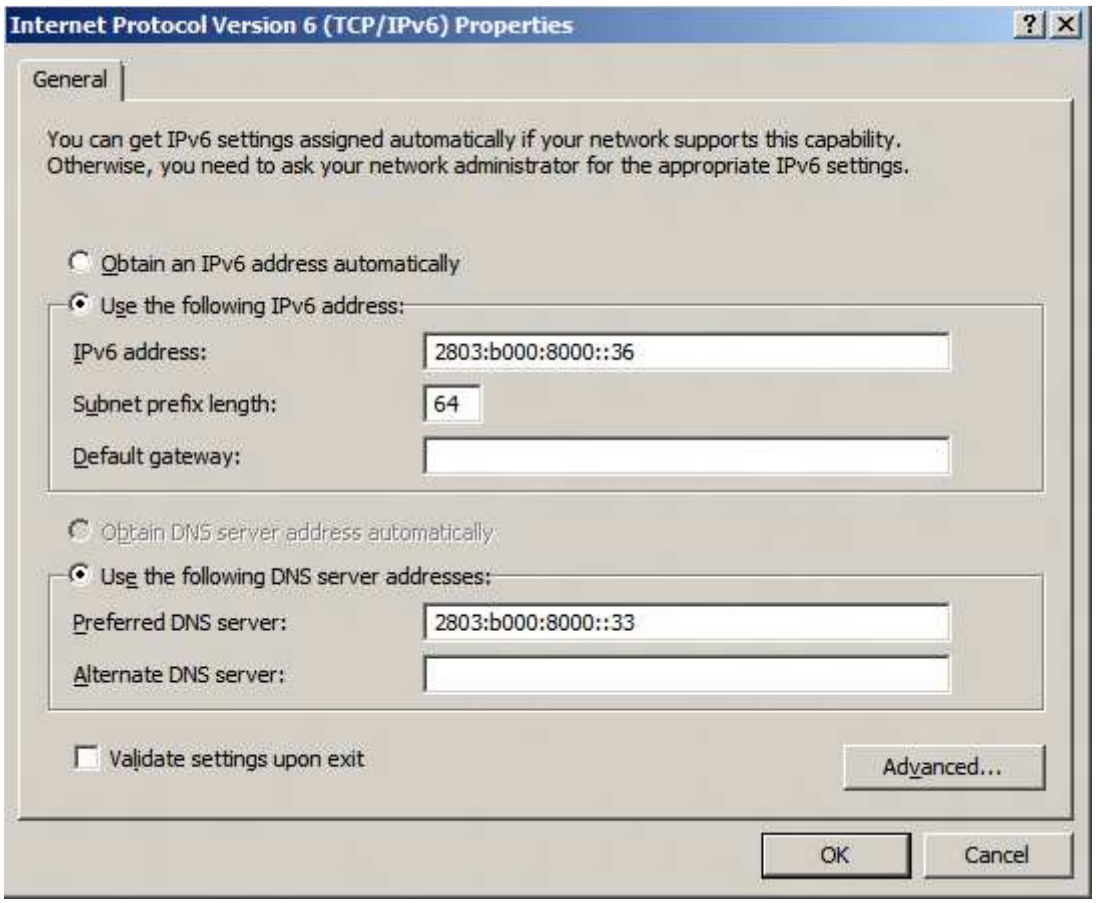
Para el Ubuntu server se va a tener la siguiente configuración.



Como primer aspecto se asignara una dirección IPv6, seguido de esto se procede a configurar el archivo de apache2 el cual funcionara como servidor web.

Con esto el servicio escuchara sobre el puerto 80 en la dirección especificada.

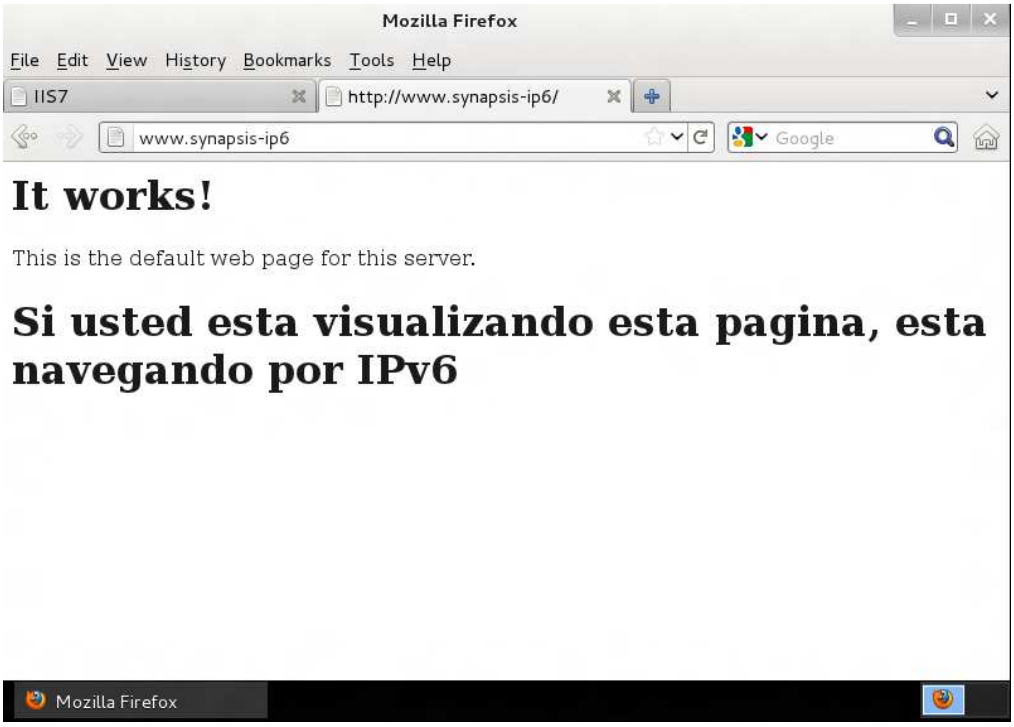
Después de esto se procede a configurar el servidor Windows server 2008, en el cual después de instalar el rol de IIS (Internet Information Services), el cual funcionara como servicio web, se configura la dirección IPv6 de la siguiente manera, en la interfaz que estará publica en Internet Ipv6.



A esto se agrega que se debe dar la configuración del servidor DNS, para que resuelva de una manera correcta.

Una vez realizado esto se realizan las pruebas correspondientes, usando el cliente Fedora, el cual se debe configurar como primer aspecto la dirección IP

De igual forma se asigna como servidor de nombres, la dirección ::33. Continuando se realiza las pruebas desde el navegador obteniendo los siguientes resultados:



Para el servidor Ubuntu, y para el servidor Windows se tiene lo siguiente:

De esta manera se evidencia la correcta configuración del los servicios, y del servidor de nombres de dominio.

Anexo 4. Configuración Router

Toda la configuración del Router se hace mediante consola, es decir mediante interfaz de comandos vía protocolo telnet, en esta sección se tratara la configuración más relevante en el desarrollo del proyecto.

Toda la configuración esta segmentada, a cada caso particular del proyecto y como primera etapa se establece una conexión entre el Router y el NAP Colombia con quienes en primera instancia se abrirá una sesión BGP, para empezar a compartir rutas de internet en IPv6.

El primer aspecto a configurar es la interfaz de conexión hacia el NAP.

```
!
interface GigabitEthernet0/1.11
 description Conexion NAP Colombia
 encapsulation dot1Q 11
 ipv6 address 2001:13C7:6000:[redacted]:[redacted]/48
 ipv6 enable
!
```

De aquí se destaca la habilitación de IPv6, y la dirección publica con la cual se establecerá la sesión BGP.

Seguido a esto se debe establecer la sesión con el par BGP.

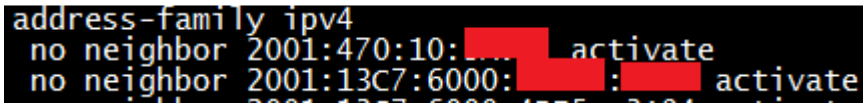
```
router bgp 14867
 bgp router-id 200.31.[redacted]
 no bgp fast-external-fallover
 bgp log-neighbor-changes
 neighbor MONITOR_NAP peer-group
 neighbor MONITOR_NAP remote-as 14970
 neighbor MONITOR_NAP description Monitor BGP NAP as 14970
 neighbor MONITOR_NAP version 4
```

En donde como primera medida se debe dar el sistema autónomo perteneciente al ISP, con se acoge a todas las políticas internas de enrutamiento.

Por otra parte el aspecto más relevante en este segmento de código es la creación de (peer-group) grupo BGP, en donde se definirá toda la política para el inicio de sesión BGP, en este caso con el NAP, en donde se dan parámetros de versión de BGP, sistema autónomo del par y se asocia la dirección o direcciones IP del par al grupo, de la siguiente manera:

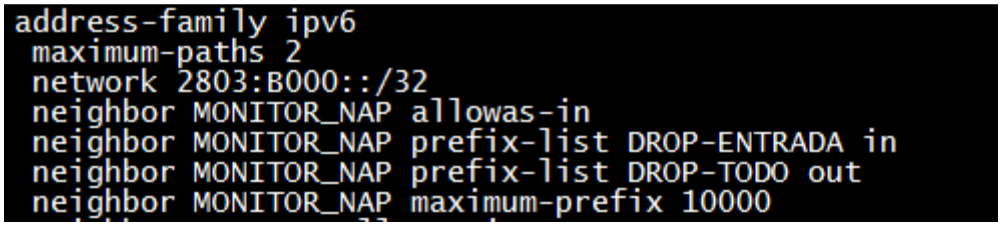
```
neighbor 2001:13C7:6000:[redacted]:[redacted] peer-group MONITOR_NAP
```

Una vez realizada esta configuracion se procede a dar parametros de configuracion de la sesion, eso se debe hacer seguido del segmento de router, en address-familly de la siguiente manera:



Con esto se indica al router, que en IPv4 no active la sesión con los vecinos asociados a esa dirección IP.

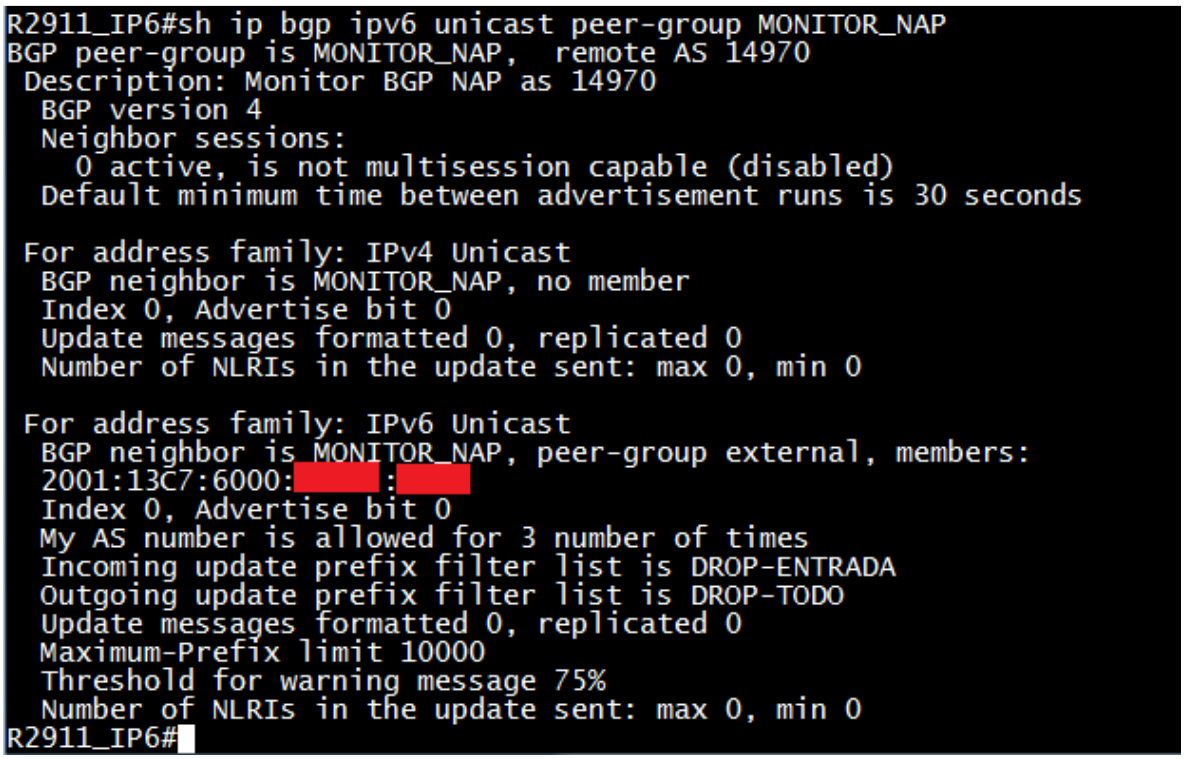
Mientras que para IPv6 se debe tener en cuenta lo siguiente:



Donde se define el número de caminos máximos a permitir, y el segmento de red el cual nos corresponde y que se va hacer público; seguido de esto se debe realizar un filtro sobre los prefijos que se desean recibir e inyectar, mediante prefix-list, y por último se determina la cantidad máxima de prefijos para recibir, esto con el fin de controlar el nivel de procesamiento de la máquina para evitar posibles fallos de disponibilidad del servicio. Por último se debe activar la sesión con los vecinos asociados al grupo de la siguiente manera:

Una vez realizado esto ya se encuentra activa la sesión BGP y se están compartiendo rutas, esto podemos observarlo de la siguiente manera:

 # show ip bgp ipv6 unicast peer-group MONITOR_NAP



De aquí se observa, todos los parámetros configurados anteriormente.

Otra forma de comprobar esto es mediante el siguiente comando:

#show ip bgp ipv6 unicast neighbors 2001:13C7:6000::XXXX

```
R2911_IP6#sh ip bgp ipv6 unicast neighbors 2001:13C7:6000:[redacted]:[redacted]
BGP neighbor is 2001:13C7:6000:[redacted]:[redacted],  remote AS 14970, external link
 Description: Monitor BGP NAP as 14970
 Member of peer-group MONITOR_NAP for session parameters
  BGP version 4, remote router ID 206.223.[redacted].[redacted]
  BGP state = Established, up for 3w4d
  Last read 00:00:19, last write 00:00:22, hold time is 180, keepalive interval is 60 seconds
  Neighbor sessions:
    1 active, is not multisession capable (disabled)
  Neighbor capabilities:
    Route refresh: advertised and received(new)
    Four-octets ASN Capability: advertised
    Address family IPv4 Unicast: received
    Address family IPv6 Unicast: advertised and received
    Multisession Capability:
    Stateful switchover support enabled: NO for session 1
  Message statistics:
    InQ depth is 0
    OutQ depth is 0

                         Sent       Rcvd
    Opens:                  1          1
    Notifications:          0          0
    Updates:                1          0
    Keepalives:         39749      36098
    Route Refresh:          0          0
    Total:              39751      36099
  Default minimum time between advertisement runs is 30 seconds
```

En donde se observa el número de notificaciones Open, Update y Keepalive que están involucrados en la sesión.

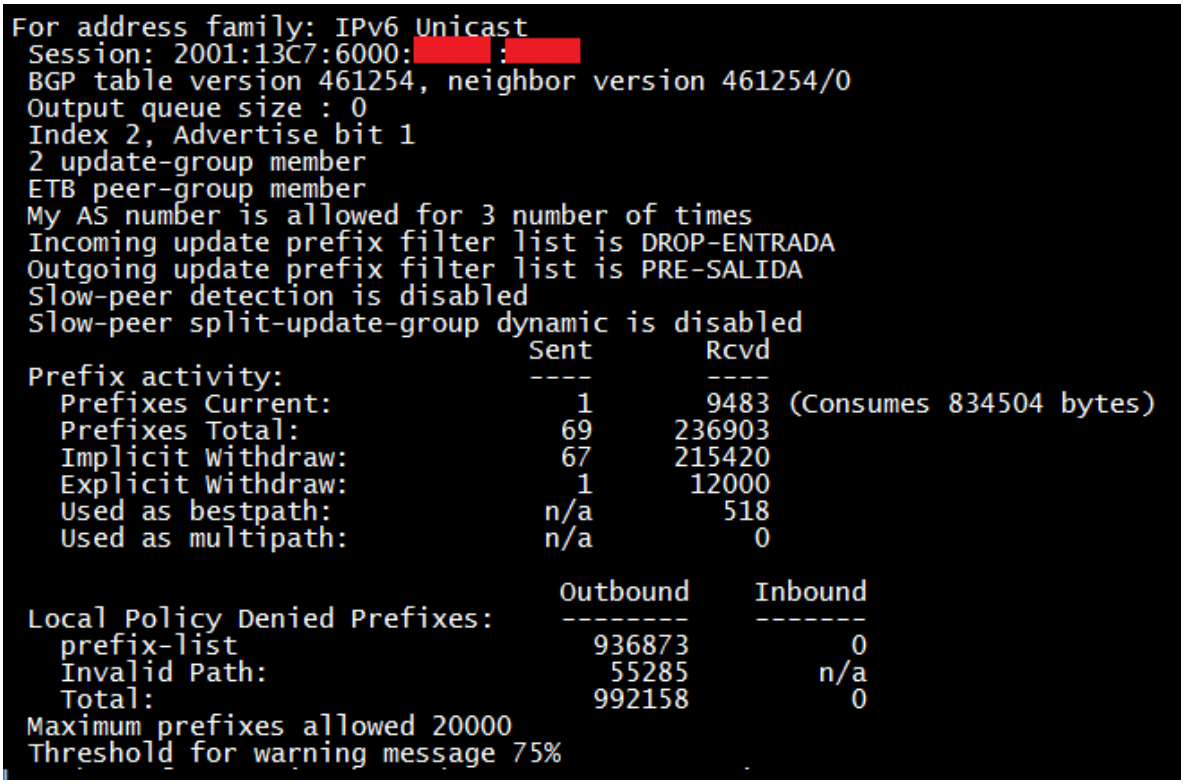
También se observa el número de prefijos tanto enviados como recibidos

```
MONITOR_NAP peer-group member
My AS number is allowed for 3 number of times
Incoming update prefix filter list is DROP-ENTRADA
Outgoing update prefix filter list is DROP-TODO
Slow-peer detection is disabled
Slow-peer split-update-group dynamic is disabled
                                Sent       Rcvd
Prefix activity:                ----       ----
  Prefixes Current:                0          0
  Prefixes Total:                  0          0
  Implicit Withdraw:               0          0
  Explicit Withdraw:               0          0
  Used as bestpath:              n/a          0
  Used as multipath:             n/a          0

                                  Outbound    Inbound
Local Policy Denied Prefixes:     --------    -------
  prefix-list                       366602          0
  Invalid Path:                      40418        n/a
  Total:                            407020          0
Maximum prefixes allowed 10000
Threshold for warning message 75%
```

En este caso no se está enviando ni recibiendo ningún prefijo, por el contrario se está denegando el envío de los mismos, esto debido a que la función de NAP es de monitoreo de tráfico y estado de sesión, las sesiones con las cuales se deben

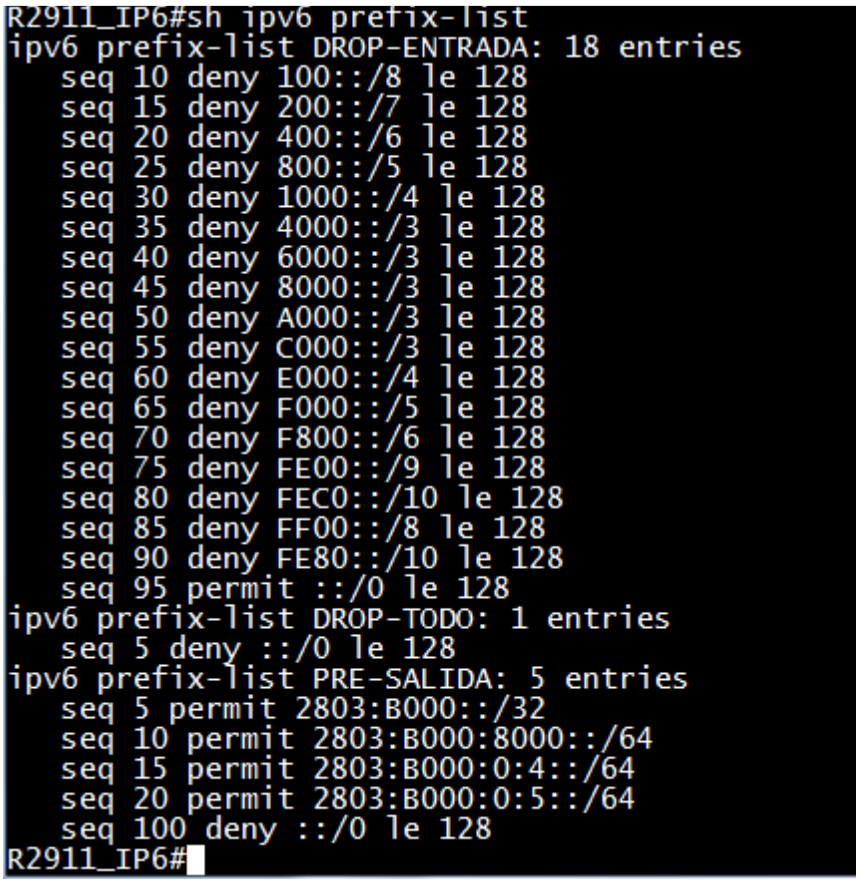
compartir prefijos son directamente con los miembros del NAP, es decir con los ISP que se encuentren en este sistema.

De la siguiente manera se toma como ejemplo otra sesión con un ISP el cual contiene las mismas políticas de configuración:



En este caso se puede observar que el número de prefijos recibidos es bastante alto, dando con esto conectividad total con la red del ISP vecino.

Una parte fundamental de esto es la forma como se hace el filtrado de prefijos usando prefix-list, para así poder controlar el tráfico tanto de entrada como de salida. En estas listas de prefijos se encuentras todas las redes bien sea permitidas o denegadas, de la siguiente manera.



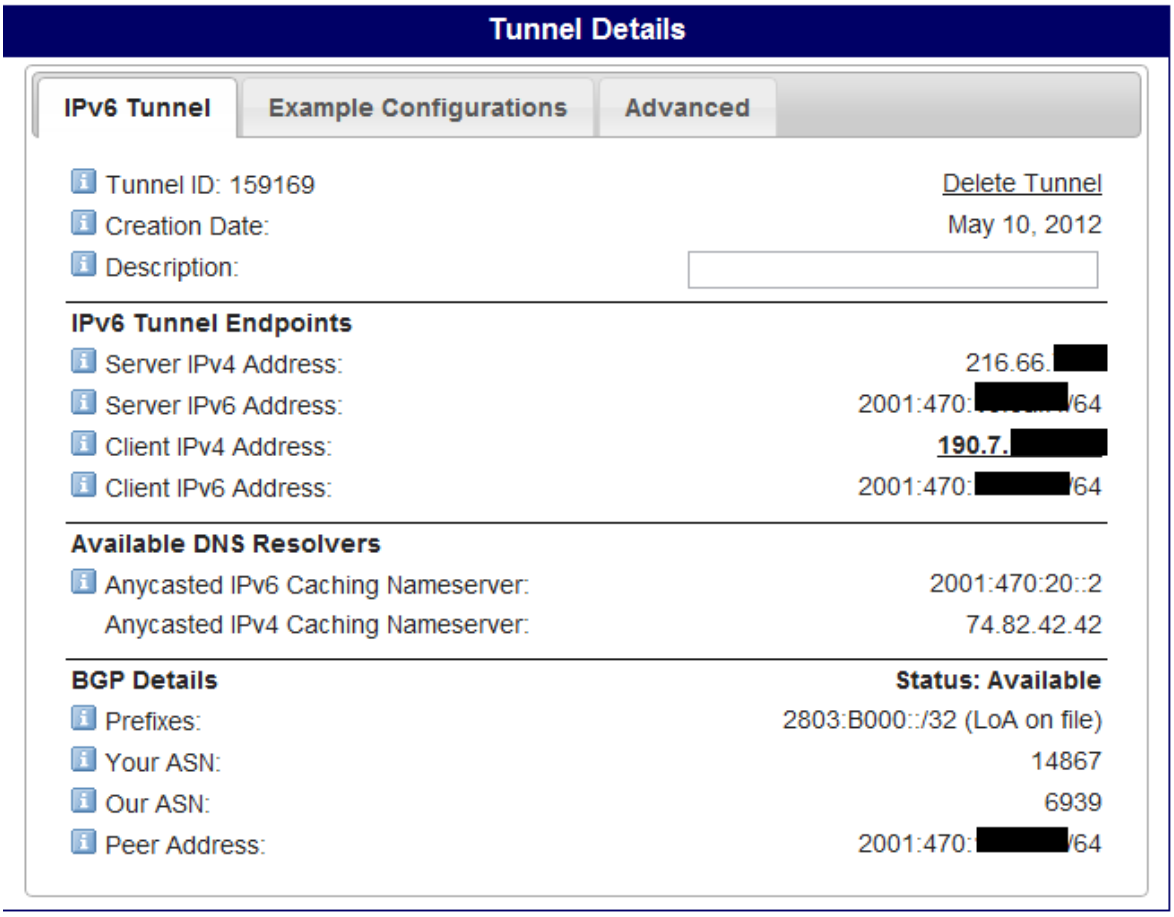
Las cuales son 3 listas, en donde la llamada DROP-ENTRADA se encuentran todas las redes que se van a denegar, estas se tomaron de la IANA[19] siendo los prefijos reservados y los prefijos de ámbitos locales. Para la segunda lista DROP-TODO se denegó todo prefijo, y en la última PRE-SALIDA se listan los prefijos que se van a inyectar, los cuales hacen parte de la red asignada.

Con todo esto tenemos conectividad en Colombia, pero para poder tener conectividad global hace falta configurar una salida a Internet IPv6 mediante algún proveedor global, en este caso Hurricane Electric (HE).

Para poder realizar esto se hace estableciendo alguna sesión BGP con HE, bien sea mediante una interfaz física o lógica, es decir con un enlace directo IPv6 o mediante un túnel IPv4.

Como HE, tiene la posibilidad de crear un túnel IPv4 de manera gratuita se opta por esto, con lo cual solo hace falta diligenciar un formulario y emitir una carta de autorización y realizar la configuración.

[19] http://www.iana.org/assignments/ipv6-address-space/ipv6-address-space.xml

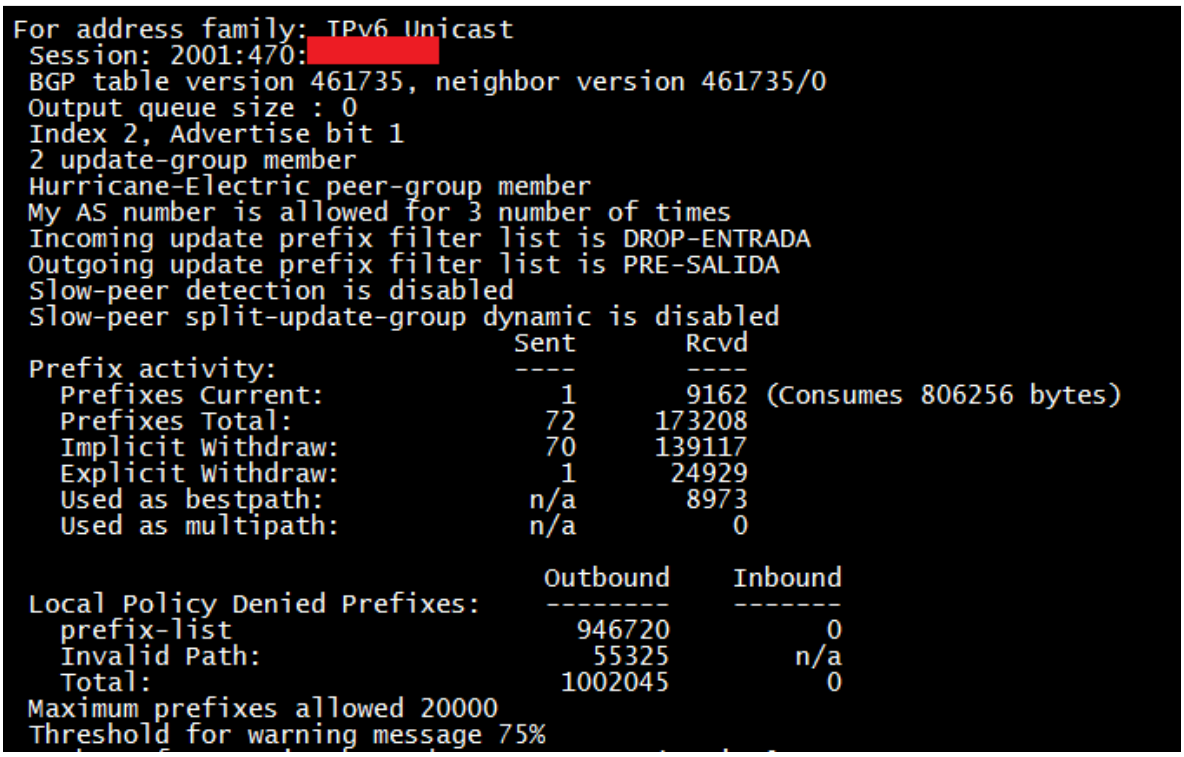


Estos son los detalles de la creación del túnel, y el estatus del mismo.

Una vez creado se debe configurar la interfaz de la siguiente manera:

```
!
interface Tunnel10
 description Hurricane Electric IPv6 Tunnel Broker
 no ip address
 ipv6 address 2001:470:[redacted]/64
 ipv6 enable
 tunnel source 190.7.[redacted]
 tunnel mode ipv6ip
 tunnel destination 216.66.[redacted]
!
```

Con esto se procede a iniciar la sesión BGP con el par de la forma como se menciona anteriormente, observando los siguientes resultados.



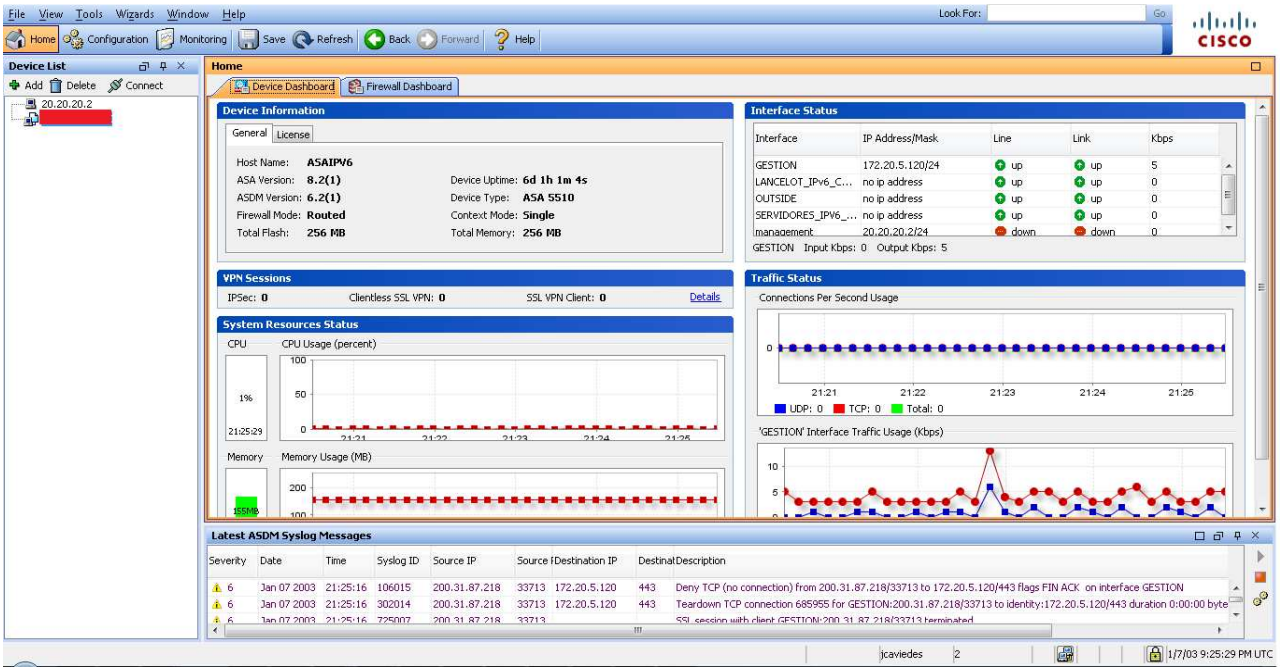
Una vez activada las sesiones se tiene conectividad total con Internet IPv6.

El último segmento a configurar en el router, son las interfaces de acceso en donde ira conectado el firewall que dará acceso a todo el segmento de red corporativo, servidores, y servicios extra.

Anexo 5. Configuración Firewall

En este apartado se detallara la configuración del firewall, el cual dará protección a todo el segmento de red que incluya el protocolo IPv6, teniendo en cuenta servidores, segmento corporativo y demás.

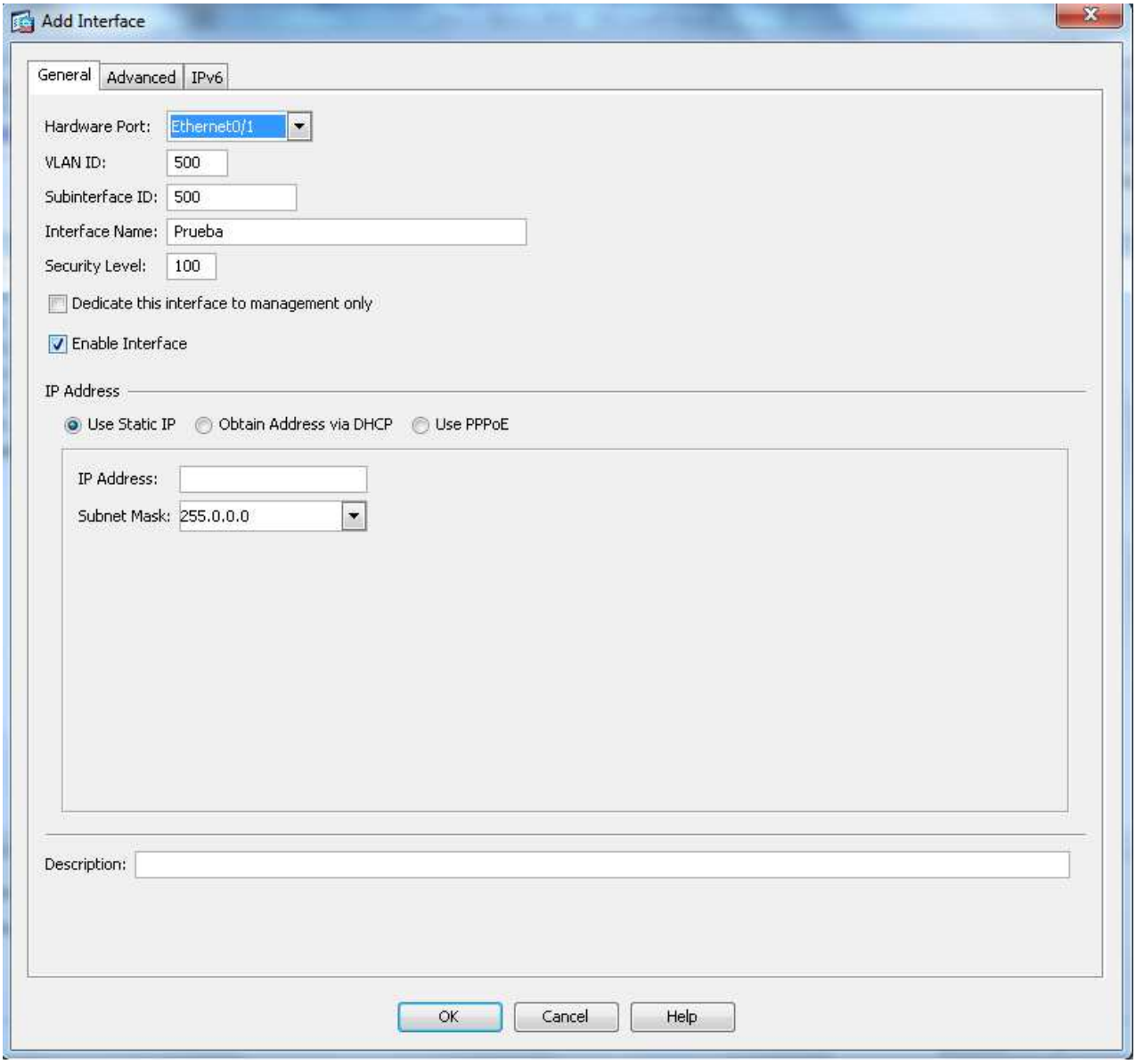
Para la configuración del equipo se uso el software de cisco ASDM, el cual permite tener un control mediante web, incluyendo todos los módulos que pueda tener.



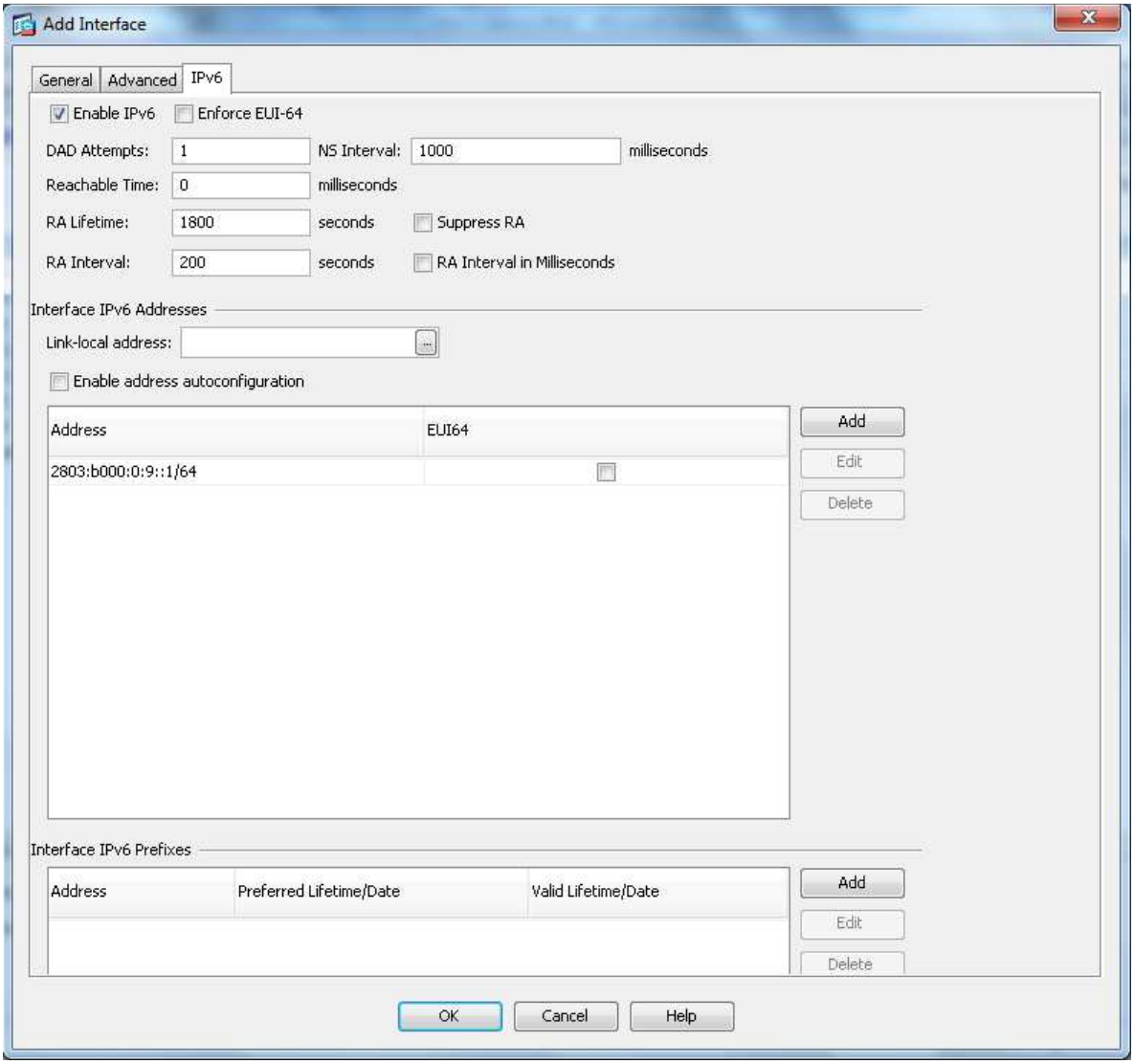
El anterior es un primer vistazo del software en donde se muestran estadísticas de conexión, uso de CPU, estado de las interfaces, entre otros.

Como primer aspecto para la configuración son las interfaces entre las cuales se debe elegir cual será de gestión, por medio de las cual se tendrá control del equipo, la interfaz de salida que dará la cara directo a Internet y las interfaces internas en donde estarán los servidores, LAN corporativa y demás servicios.

Para esto se ubica sobre la sección de configuración e interfaces en donde se desplegara el siguiente menú para la creación de una nueva interfaz



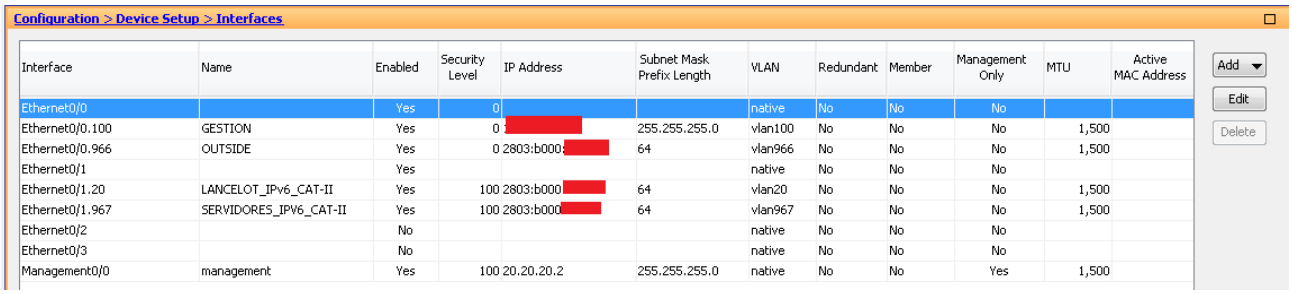
En donde se lista, la interfaz fisica, la VLAN por la cual debera ir, la identificacion, el nivel de seguridad para aplicar el algoritmo ASA, y en la pestaña IPv6 contiene lo siguiente:



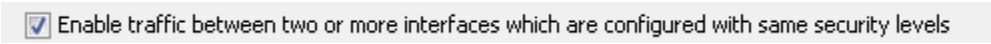
De aquí se debe habilitar el soporte en IPv6 y ademas dar su direccion IP.

De esta manera se realiza la configuracion para interfaz, entre las cuales se va a crear una interfaz de gestion con un nivel de seguridad 0, una interfaz de salida con un nivel de seguridad 0, una interfaz en donde estara alojada el servidor DNS con nivel de seguridad 100 y una interfaz para los servidores con un nivel de seguridad de 100.

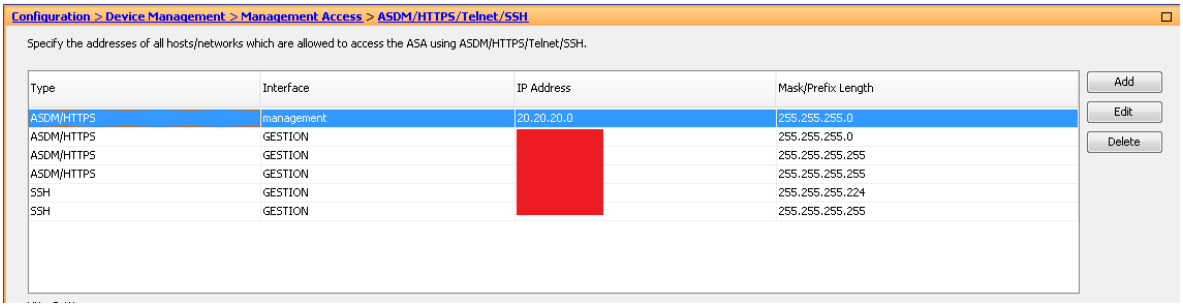
Teniendo el siguiente resultado:



También se debe habilitar el traspaso de tráfico entre interfaces con el mismo nivel de seguridad para los servidores y servicios DNS. Esto se hace en la misma pestaña de configuración de la interfaz.

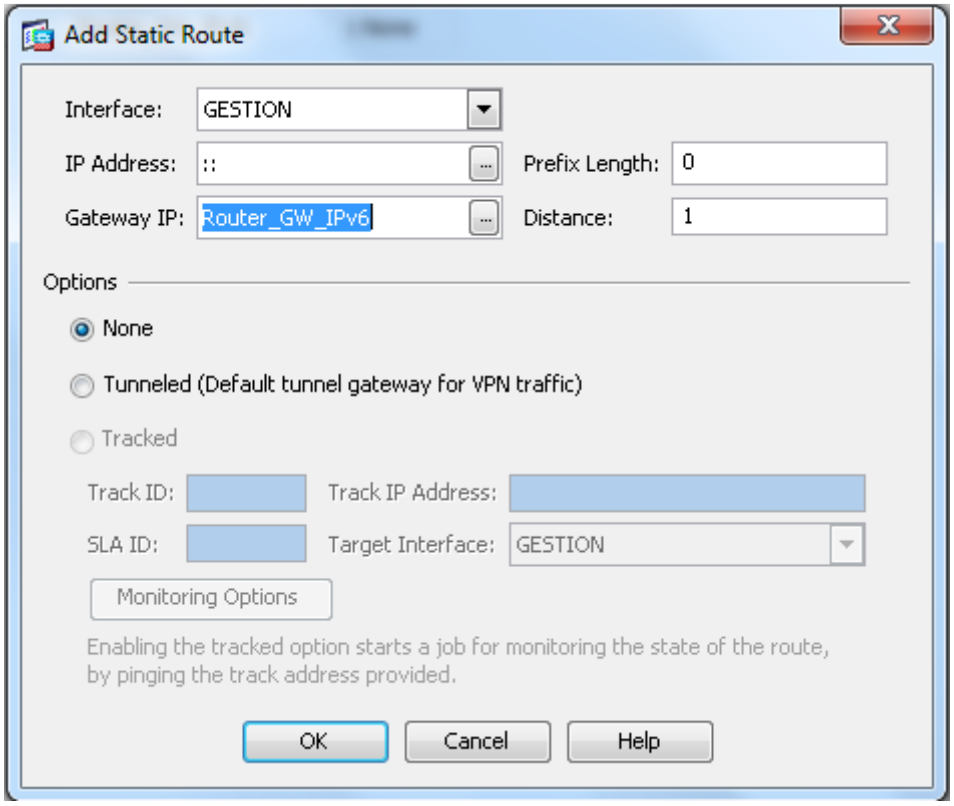


Una vez realizado esto se debe listar desde que direcciones y a que servicios de gestión se debe tener acceso. Esto en la sección de configuración, gestión del equipo, gestión de acceso. Obteniendo el siguiente resultado:



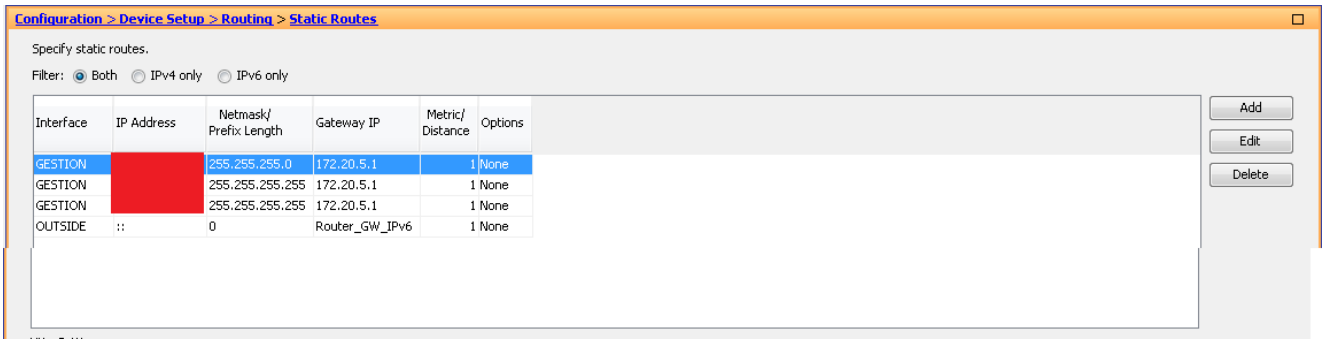
Una vez se tiene habilitadas las interfaz de gestión, se procede a configurar las rutas estáticas para poder dar salida del equipo hacia internet, además tener todo el enrutamiento del equipo.

Para esto se debe hacer en la sección de configuración, configuración del equipo, enrutamiento y rutas estáticas. De la siguiente manera:



En este segmento se debe dar la interfaz de salida, la dirección ip del destino y el próximo salto que debe dar.

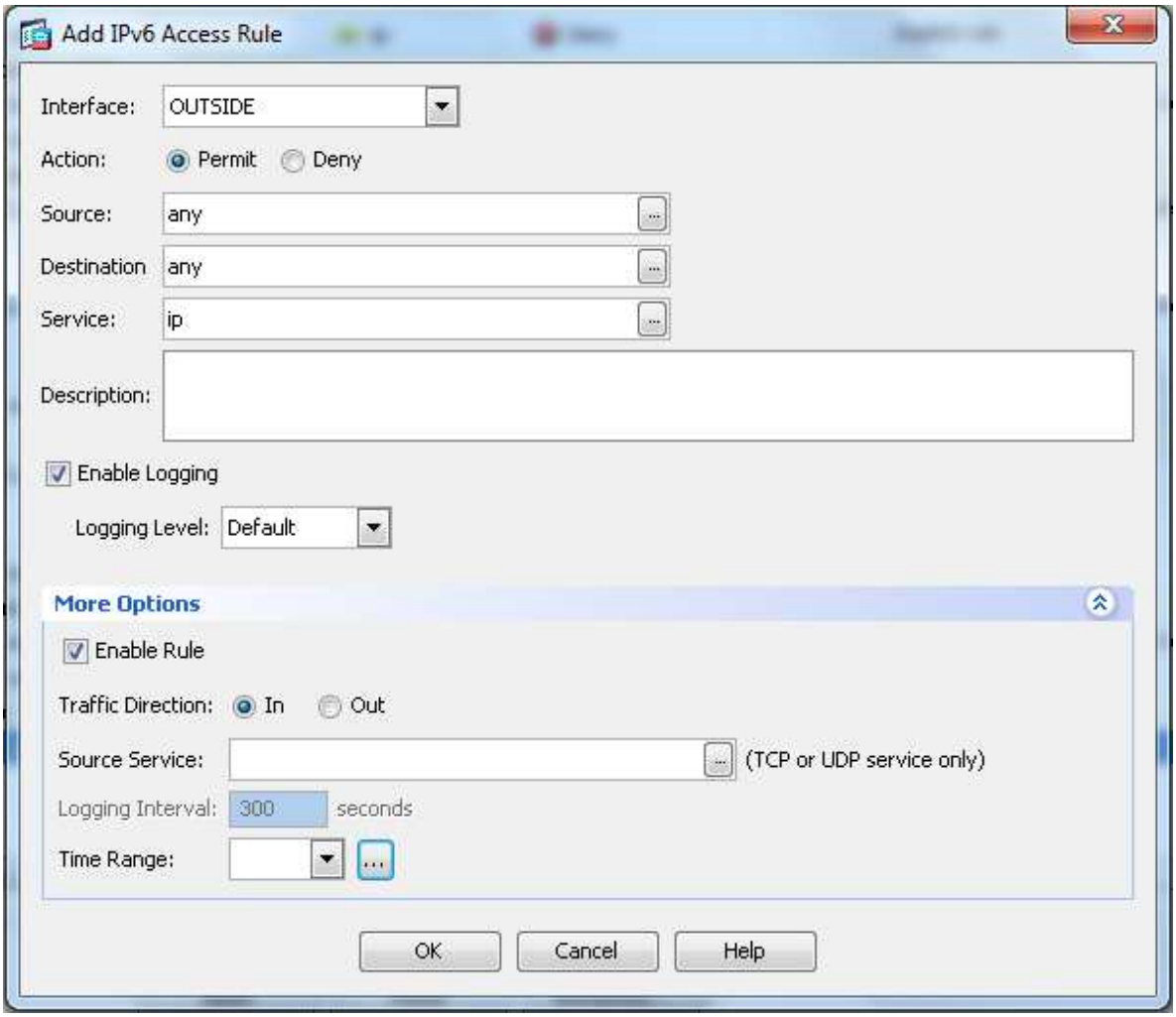
Por el momento solo se debe dar un Default Gateway para la salida de internet puesto que solo se tiene habilitado una, además de rutas para tener acceso a la gestión del mismo. Obteniendo este resultado:



Con esto se procede a la configuración de reglas para permitir o denegar el tráfico que atraviese el firewall, además se debe permitir el paso de tráfico sin que haga una traducción de direcciones (NAT), puesto que esto no existe este protocolo en

IPv6, esto mediante la sección configuración, firewall, reglas NAT habilitando la opción de la siguiente manera:

De aquí que la creación de las reglas se realiza en, configuración, firewall, reglas de acceso, en donde selecciona la interfaz y se crea la regla de la siguiente manera:

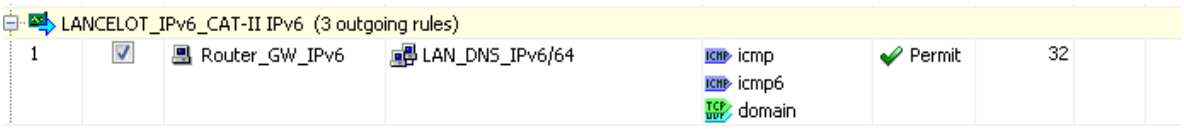


Donde se selecciona la interfaz a la cual se va a aplicar la regla, la acción que se va a aplicar, la o las fuentes y destinos, y que servicios va a dejar pasar. También se debe tener en cuenta en qué dirección de tráfico se va a aplicar.

A partir de aquí se detallan las reglas que se usaron para la configuración del mismo. Aunque la mayor parte de procesamiento la va a realizar el algoritmo

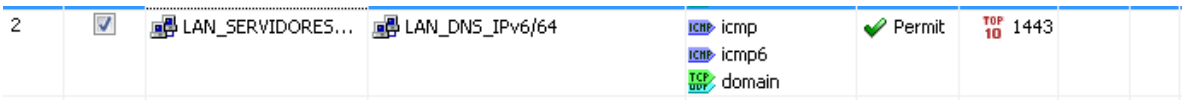
usado por el equipo (ASA), mediante los niveles de seguridad de las interfaces hay que habilitar algunas reglas para el traspaso de tráfico.

La primera regla que se aplica, será dejar pasar todo el tráfico ICMP, y DNS; que venga desde el router IPv6 “interfaz física” hacia la red del servidor DNS sea permitido, de la siguiente manera:



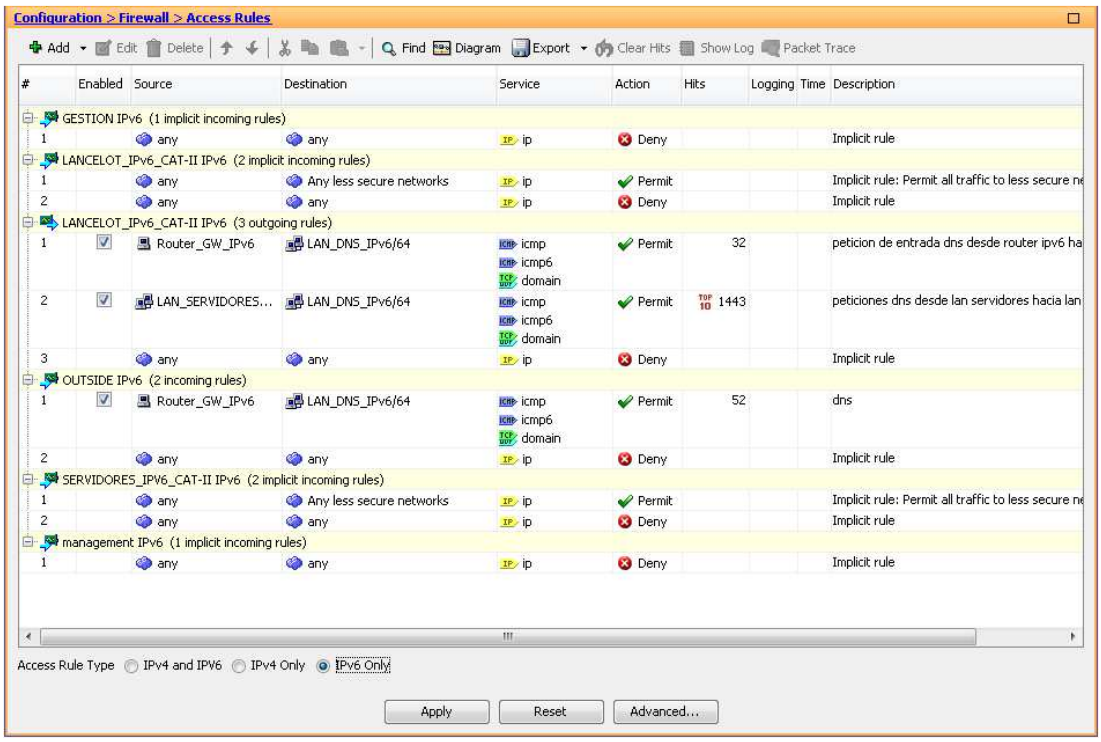
Visto gráficamente:

La segunda regla a aplicar es similar, puesto que cumple los mismos parámetros a diferencia de la fuente, puesto que en esta ocasión será el segmento de red de los servidores.



Visto gráficamente:

Con esto finalizando la configuración del firewall obteniendo el siguiente resultado:


Configuration > Firewall > Access Rules
Add
Edit
Delete
Find
Diagram
Export
Clear Hits
Show Log
Packet Trace
Enabled Source Destination Service Action Hits Logging Time Description
GESTION IPv6 (1 implicit incoming rules)
1 any any ip Deny Implicit rule
LANCELOT_IPv6_CAT-II IPv6 (2 implicit incoming rules)
1 any Any less secure networks ip Permit Implicit rule: Permit all traffic to less secure ne
2 any any ip Deny Implicit rule
LANCELOT_IPv6_CAT-II IPv6 (3 outgoing rules)
1 Router_GW_IPv6 LAN_DNS_IPv6/64 icmp icmp6 domain Permit 32 peticion de entrada dns desde router ipv6 ha
2 LAN_SERVIDORES... LAN_DNS_IPv6/64 icmp icmp6 domain Permit 1443 peticiones dns desde lan servidores hacia lan
3 any any ip Deny Implicit rule
OUTSIDE IPv6 (2 incoming rules)
1 Router_GW_IPv6 LAN_DNS_IPv6/64 icmp icmp6 domain Permit 52 dns
2 any any ip Deny Implicit rule
SERVIDORES_IPV6_CAT-II IPv6 (2 implicit incoming rules)
1 any Any less secure networks ip Permit Implicit rule: Permit all traffic to less secure ne
2 any any ip Deny Implicit rule
management IPv6 (1 implicit incoming rules)
1 any any ip Deny Implicit rule
Access Rule Type IPv4 and IPv6 IPv4 Only IPv6 Only
Apply
Reset
Advanced...