UNIVERSIDAD POLITÉCNICA SALESIANA
SEDE QUITO

CARRERA: INGENIERÍA DE SISTEMAS

Tesis previa a la obtención del título de: INGENIERO DE SISTEMAS

TEMA:
ANÁLISIS, DISEÑO E IMPLEMENTACIÓN DE UNA RED PROTOTIPO UTILIZANDO EL PROTOCOLO IPv6 Y QoS PARA LA EMPRESA SANTANET

AUTOR:
ALEJANDRO PAÚL SANTAMARÍA ALAMAR

DIRECTORA:
VERÓNICA SORIA MALDONADO

Quito, enero de 2014

DECLARATORIA DE RESPONSABILIDAD Y AUTORIZACIÓN DE USO DEL TRABAJO DE GRADO

Yo Alejandro Paúl Santamaría Alamar autorizo a la Universidad Politécnica Salesiana la publicación total o parcial de este trabajo de grado y su reproducción sin fines de lucro.

Además declaro que los conceptos y análisis desarrollados y las conclusiones del presente trabajo son de exclusiva responsabilidad del autor.

Alejandro Paúl Santamaría Alamar

CC. 1719606178

DEDICATORIA

Este proyecto lo dedico a las personas que día a día luchan por ser mejores y por lograr alcanzar sus metas.

A mis seres queridos que me apoyan directa e indirectamente, ya que con sus consejos y experiencias me ayudan a crecer tanto en el aspecto personal y profesional.

A mis jefes que me apoyaron para estudiar y trabajar al mismo tiempo, dedicando esfuerzo y trabajo diario.

Y finalmente este proyecto va dedicado a los que me vieron crecer y formarme como persona, a los que vivieron junto a mí el sacrificio de luchar y salir adelante.

AGRADECIMIENTOS

A mi Universidad, mis maestros y compañeros

Por ser apoyo constante en la vida estudiantil, porque con sus conocimientos supieron orientarme y ser un buen profesional.

¡Gracias a ustedes!

ÍNDICE

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

ÍNDICE DE ANEXOS

RESUMEN

El proyecto realiza el análisis tanto de software y hardware de los equipos que dispone la empresa Santanet, mediante un diseño físico y lógico se procede a utilizar los equipos disponibles y se adquiere lo necesario para la implementación de una red con el protocolo IPv6, utilizando eficientemente los recursos de la empresa.

Utilizando una dirección IPv4 pública fija y mediante Hurricane Electric se creó un túnel 6in4 en donde se obtuvo direcciones IPv6 con prefijos 48 y 64 que permite comunicarse con redes IPv6, mediante un PC que funciona como router se crea el túnel 6in4 y también se ejecuta el software de ruteo Quagga. Adicionalmente en el PC router se ejecutan los servidores DHCPv4, DHCPv6, RADVD, DNS y QoS.

En el servidor principal se ejecutan los servidores web, de correos, FTP y SSH. Estos servidores funcionan tanto para IPv4 e IPv6 y son accesibles desde cualquier destino.

Utilizando QoS se realiza un control de tráfico, en donde mediante filtros e iptables se asigna prioridades a los puertos de determinadas aplicaciones que se utilizan tanto para IPv4 e IPv6.

ABSTRACT

In this project performs the analysis of both software and hardware of computers that have the company Santanet, through a design of hardware and software is proceeds to use the equipment available and necessary for the implementation of an IPv6 network using efficiently the resources of the company.

Using a fixed public IPv4 address and by means of Hurricane Electric is created a 6in4 tunnel where is obtained the IPv6 address with prefixes 48 and 64 to communicate with IPv6 networks, using a PC that works like router is created 6in4 tunnel and runs the Zebra routing software. Additionally in the PC router is running servers DHCPv4, DHCPv6, RADVD, DNS and QoS.

On the primary server running web servers, email, FTP, and SSH. These services work for both IPv4 and IPv6 and are accessible from any destination.

Using QoS is performed traffic control, where by iptables and filters are assigned priorities to ports of certain applications that are used for both IPv4 and IPv6.

INTRODUCCIÓN

Internet ha evolucionado desde ser una simple red que conecta computadoras a una plataforma que entrega diversos tipos de servicios. Esta evolución ha dejado en descubierto las limitantes del protocolo IPv4, base de esta gran red. IPv4 fue desarrollado en la década de los 70 como una forma de interconectar un reducido número de redes y jamás se pensó en que tendría que ser la base de una red de millones de usuarios. Su reducido número de direcciones disponibles junto a problemas de arquitectura, han restringido y limitado el desarrollo de nuevas aplicaciones y tecnologías en Internet (Jara, 2009, pág. 1).

Inicialmente el número de direcciones no era un problema, IPv4 usa un esquema de direccionamiento de 32 bits, por lo tanto el número de host posible es de 2^{32}, lo cual equivale aproximadamente a 4200 millones. El problema real se encuentra en la asignación de direcciones, a pesar de la implementación de estrategias de direccionamiento como VLSM-Variable Length Subnet Mask- (Máscara de Subred de Tamaño Variable), CIDR-Classless Inter Domain Routing- (Enrutamiento Entre Dominios sin Clases) y Sumarización el espacio de direcciones estaba siendo desperdiciado. Adicional a esto, había una necesidad de extender la funcionalidad de la capa de red con características como QoS-Quality Of Service- (Calidad de Servicio), encriptación punto a punto, enrutamiento de origen y autenticación entre otros hicieron cada vez más claro que un nuevo protocolo de Internet tenía que ser adoptado en un futuro cercano (Generalidades de IPv6, 2012).

"En las empresas del Ecuador la adopción del IPv6 se vuelve cada vez más crítica y es necesario emitir políticas y regulaciones que impulsen, promuevan y obliguen a la adopción de IPv6 en el país" (Supertel, 2012).

Las redes actuales no tienen implementado IPv6 ni tampoco poseen un plan de transición de IPv4 a la nueva versión. El problema a largo plazo que se tendrá en la empresa Santanet es en la transición a IPv6, ya que en un tiempo no muy lejano todas las redes deben de tener IPv6 implementado por las razones antes descritas

CAPÍTULO I
GENERALIDADES

1.1 Introducción

Si la empresa Santanet se queda atrasada en la adopción de IPv6 puede tener problemas para utilizar determinados recursos en Internet ya que se espera que con el tiempo las aplicaciones en Internet pasen a funcionar únicamente en IPv6. Si cualquiera de estas aplicaciones se vuelve importante para el negocio, los competidores que ya estén conectados con IPv6 tendrán una ventaja competitiva importante (IPv6 Chile, 2012).

Otro punto a considerar es la pérdida de oportunidades para la empresa Santanet en el desarrollo de aplicaciones innovadoras basadas en IPv6. "También existe el riesgo que la implementación de IPv6 falle, es decir, que se agoten las direcciones IPv4 antes que IPv6 esté bien difundido. Si esto sucede, los costos de implementación de nuevas redes conectadas a Internet pueden aumentar. El uso de NAT-Network Address Translation (Traducción de Dirección de Red) también aumentará, encareciendo la administración de la red y aumentando los costos en la creación de aplicaciones extremo a extremo" (IPv6 Chile, 2012).

1.2 Justificación

Se decide realizar el análisis, diseño e implementación de una red de área local prototipo con IPv6 por que permite dar solución a las necesidades actuales como son la seguridad, movilidad, QoS, comunicación de grupo en tiempo real, entre otros, ya que a poco a poco más contenidos y servicios estarán disponibles con IPv6.

El beneficio que tendrá la empresa Santanet al implementar una red de área local prototipo con IPv6 es que se anticipa al avance tan progresivo de la tecnología, ya que será extendible y permitirá la transición en el futuro.

Este estudio será beneficioso tanto para la empresa Santanet como para otras empresas, ya que se tiene un documento desarrollado acerca de esta tecnología, la cual actualmente ya es requerida en todas las instituciones, fábricas, gobierno, universidades, organizaciones, entre otras.

Se estudia un método adecuado para la futura implementación del protocolo IPv6 dentro de la empresa, con lo cual se tiene un gran beneficio para el mejoramiento y funcionalidad de la red.

Por otra parte IPv6 tiene las siguientes ventajas:

1. Aumento del número de direcciones 2^128.
2. "Todos los campos en la cabecera IPv6 son de 64 bits, mayores ventajas para la generación actual de procesadores de 64 bits" (Fos, 2012).
3. "Los routers no realizan fragmentación en IPv6, esto elimina el tiempo de proceso que necesitaban en IPv4 para realizar la fragmentación, con lo cual se obtiene una mayor velocidad de proceso. Solo los nodos origen pueden realizar la fragmentación" (Fos, 2012).
4. Simplifica la gestión de los ordenadores conectados a la red, soportando de forma automática la conexión de nuevos ordenadores (Plug and Play) sin necesidad de configurarlos explícitamente (Ubidia, 2007, pág. 19).
5. "IPv6 incluye como componente obligatorio el protocolo de seguridad IPsec-Internet Protocol Security- (Protocolo de Seguridad de Internet) e integra más eficazmente que IPv4 facilidades tales como distintos grados de QoS, movilidad IP, multicast o anycast" (Ubidia, 2007, pág. 19).

Mediante estas ventajas se puede justificar por qué las aplicaciones actuales están migrando a IPv6.

1.3 Objetivos

1.3.1 Objetivo general

Realizar el análisis, diseño e implementación de una red de área local prototipo con IPv6 utilizando GNU/Linux para configurar los servidores y desarrollar pruebas desde las estaciones de trabajo con diferentes plataformas.

1.3.2 Objetivos específicos

- Sistematizar la información referente al protocolo IPv6 que sirva de apoyo para justificar las fases posteriores de esta investigación.
- Plantear los requerimientos de hardware y software indispensables en la empresa Santanet para el funcionamiento con el protocolo IPv6.
- Diseñar una red de área local prototipo que trabaje bajo el protocolo IPv6 y realizar las pruebas de control de tráfico en la red utilizando QoS en GNU/Linux.
- Implementar la red de área local de pruebas con los servicios de Internet y/o servidores de red con soporte de IPv6 y manejo de QoS.
- Documentar la configuración de los servicios y kernel utilizados en la red de área local prototipo, los mismos que permitirán la aceptación de nuevas tecnologías en la empresa Santanet, apoyando de esta manera al progreso y desarrollo de las comunicaciones.
- Efectuar pruebas desde las estaciones de trabajo a los servicios configurados en GNU/Linux y documentar los resultados.

1.4 Alcance

- Analizar e investigar los fundamentos, características, arquitectura y componentes del protocolo IPv6.
- Implementar un túnel en el router de la red IPv4 que permita a la empresa Santanet comunicarse con redes nativas IPv6.
- Implementar servicios de Internet con soporte para IPv6 en GNU/Linux como:

- FTP-File Transfer Protocol- (Protocolo de Transferencia de Archivos).
- SSH-Secure Shell- (Interprete de Ordenes Segura).
- SMTP-Simple Mail Transfer Protocol- (Protocolo para la Transferencia Simple de Correo Electrónico).

- POP-Post Office Protocol- (Protocolo de Oficina de Correo).
- HTTP-Hypertext Transfer Protocol- (Protocolo de Transferencia de Hipertexto).
- DNS-Domain Name System- (Sistema de Nombres de Dominio) Interno.
- DHCP-Dynamic Host Configuration Protocol- (Protocolo de Configuración Dinámica de Host).

- Documentar la configuración de cada servicio de Internet con soporte IPv6 tanto en los clientes como en el servidor.
- Configurar el kernel en una distribución GNU/Linux para soporte de IPv6 y QoS.
- Realizar pruebas y resultados de los servicios configurados en GNU/Linux y documentar la información respectiva.
- Realizar control de tráfico en la red de área local utilizando QoS en GNU/Linux y así gestionar de manera eficiente el ancho de banda para cada aplicación.

CAPÍTULO 2
MARCO TEÓRICO

2.1 El modelo TCP/IP

En 1970 DARPA-Defense Advanced Research Projects Agency- (Agencia de Investigación de Proyectos Avanzados de Defensa) crea el modelo TCP/IP el cual es un modelo de descripción de protocolos de red. El modelo TCP/IP también es conocido como Internet Model, modelo DARPA o modelo DoD.

"TCP/IP provee conectividad de extremo a extremo especificando como los datos deberían ser formateados, direccionados, transmitidos, enrutados y recibidos por el destinatario. Existen protocolos para los diferentes tipos de servicios de comunicación entre equipos" (Araguz, 2012).

Figura 1. Capas del modelo TCP/IP

Modelo TCP/IP	Capa	Descripción
Aplicación	4	Donde operan los protocolos de alto nivel, como SMTP y FTP
Transporte	3	Donde existen los protocolos de control de flujo y conexión
Internet	2	Donde se ejecutan el direccionamiento IP y el enrutamiento
Acceso a red	1	Donde existen el direccionamiento MAC y los componentes físicos de red

Fuente: (Redes Informaricas, 2013)

“Para poder aplicar el modelo TCP/IP en cualquier equipo, es decir, independientemente del sistema operativo, el sistema de protocolos TCP/IP se ha dividido en diversos módulos. Cada uno de éstos realiza una tarea específica. Además, estos módulos realizan sus tareas uno después del otro en un orden específico. Ésta es la razón por la cual se habla de modelo de capas” (Kioskea, 2012).

2.2 El modelo OSI

2.2.1 Antecedentes del modelo OSI

El modelo OSI-Open System Interconnection- (Modelo de Interconexión de Sistemas Abiertos) es utilizado para la visualización de entornos de red en sistemas diferentes. “Los fabricantes se ajustan a dicho modelo cuando diseñan sus productos para red. El modelo OSI ofrece una descripción del funcionamiento en conjunto de hardware y software de red por niveles, para poder hacer posible las comunicaciones y desarrollar una compatibilidad total entre sistemas alrededor del mundo” (Jallurana, 2012).

2.2.2 Estructura del modelo OSI

- Estructura multinivel: Se diseña una estructura multinivel con la idea de que cada nivel resuelva solo una parte del problema de la comunicación, con funciones específicas.
- El nivel superior utiliza los servicios de los niveles inferiores: Cada nivel se comunica con su homólogo en las otras máquinas, usando un mensaje a través de los niveles inferiores de la misma. La comunicación entre niveles se define de manera que un nivel n utilice los servicios del nivel n - 1 y proporcione servicios al nivel n + 1.
- Puntos de acceso: Entre los diferentes niveles existen interfaces llamadas “puntos de acceso” a los servicios.
- Dependencia de niveles: Cada nivel es dependiente del nivel inferior como así también lo es del nivel superior.

- Encabezados: En cada nivel, se incorpora al mensaje un formato de control. Este elemento de control permite que un nivel en la computadora receptora se entere de que la emisora le está enviando un mensaje con información.
- Número de capas: La estructura del modelo OSI define un total de 7 capas: Física, Enlace de Datos, Red, Transporte, Sesión, Presentación y Aplicación. (Della, Navarro, & Rey, 2012).

2.2.3 Capas del modelo OSI

Figura 2. Capas del modelo OSI

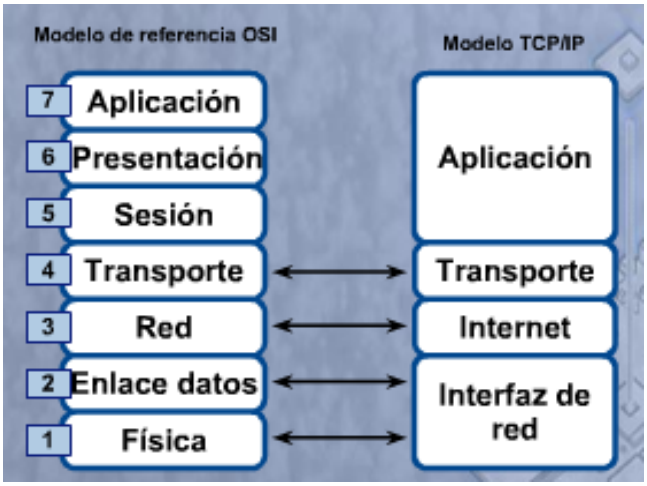
Modelo OSI	Capa	Descripción
Aplicación	7	Responsable de los servicios de red para las aplicaciones
Presentación	6	Transforma el formato de los datos y proporciona una interfaz estándar para la capa de aplicación
Sesión	5	Establece, administra y finaliza las conexiones entre las aplicaciones locales y las remotas
Transporte	4	Proporciona transporte confiable y control del flujo a través de la red
Red	3	Responsable del direccionamiento lógico y el dominio del enrutamiento
Enlace de datos	2	Proporciona direccionamiento físico y procedimientos de acceso a medios
Física	1	Define todas las especificaciones eléctricas y físicas de los dispositivos

Fuente: (Redes Informaricas, 2013)

2.3 Comparación entre la pila de protocolos OSI y TCP/IP

Internet ha hecho que la pila de protocolos basada en TCP/IP sea la más utilizada en la actualidad, ya que hace posible la comunicación entre computadoras desde cualquier parte del mundo.

Figura 3. Comparación entre el modelo TCP/IP y OSI



Fuente: (Redes Informaricas, 2013)

El modelo TCP/IP destaca una mayor flexibilidad en la capa de aplicación; en la capa de transporte involucra dos protocolos: TCP-Transmission Control Protocol- (Protocolo de Control de Transmisión) y UDP-User Datagram Protocol- (Protocolo de Datagrama de Usuario); en la capa de Internet involucra un solo protocolo: IP; y la capa inferior, está relacionada con la tecnología LAN-Local Area Network- (Red de Área Local) o WAN-Wide Area Network- (Red de Área Amplia) que se utilizará.

2.4 El protocolo IPv4

El protocolo IPv4 provee 3 funciones principales: encapsulamiento, enrutamiento y direccionamiento.

- El encapsulamiento define la información de control necesaria, que se añadirá en campos de la cabecera para formar un paquete.
- El enrutamiento consiste en la selección del mejor camino para que la información pueda llegar al destino.
- El direccionamiento establece el formato y reglas de uso de las direcciones IPv4, este punto se profundiza a continuación.

2.4.1 Introducción direccionamiento IPv4

En una red para poder comunicarse cada equipo debe tener una dirección IP exclusiva, ya que es el único identificador que diferencia un equipo de otro. Se necesita una dirección IP para cada equipo y componente de red como un router, que se comunique mediante TCP/IP.

Al igual que el número de la dirección identifica una casa en una ciudad, la dirección IP identifica la ubicación de un equipo en la red, Una dirección IP debe ser exclusiva pero conforme a un formato estándar. Una dirección IP está formada por un conjunto de 32 bits, los mismos que se agrupan en octetos y se convierten a decimales para representarlos, cada número puede oscilar entre 0 y 255. (Urueña, 2012).

2.4.2 Clasificación de las direcciones IPv4

Las direcciones IPv4 se clasifican en:

- **Direcciones IP Públicas.** Una computadora con una IP pública es visible y se puede acceder desde cualquier otra computadora conectado a Internet.
- **Direcciones IP Privadas.** Estas direcciones son visibles únicamente por otros host de la red local o de otras redes privadas interconectadas a través de routers. Las computadoras con direcciones IP privadas pueden salir a Internet por medio de un router que disponga de una IP pública utilizando el protocolo NAT.
- **Direcciones Reservadas.** Estas direcciones no se deben usar nunca, salvo alguna circunstancia para la cual han sido reservadas como ejemplo se puede citar: ruta por defecto, dirección de red, dirección de broadcast, loopback, estado de red, etc.

2.4.3 Asignación de las direcciones IP

Las direcciones IP se pueden asignar a una computadora de dos formas:

- **Direcciones IP estáticas.** La computadora que se conecte a una red con dirección IP estática siempre lo hará con la misma dirección IP. Los servidores de Internet utilizan direcciones IP públicas estáticas para ser siempre localizables por los usuarios de Internet.

- **Direcciones IP dinámicas.** La computadora que se conecte a una red con dirección IP dinámica cada vez lo hará con una dirección IP diferente. En las conexiones de Internet mediante un modem se utilizan direcciones IP públicas dinámicas. (Barajas, 2012).

2.4.4 Estructura de una dirección IPv4

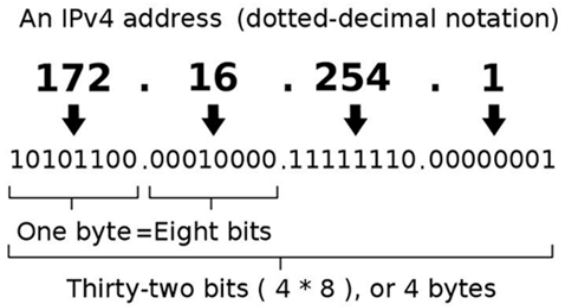
La configuración del protocolo IPv4 está formada por dos elementos:

- La dirección IP. Está formada por dos partes principales, la parte de red y la parte hosts.

- La máscara de red. Que indica mediante 1 los bits utilizados en la parte de red y con 0 los utilizados en la parte de host.

Tanto la dirección IPv4 como la máscara tienen 32 bits agrupados en 4 octetos, cada octeto es de 8 bits. El valor decimal que cada octeto puede tener está entre 0 y 255.

Figura 4. Dirección IPv4



Fuente: (Kantera56, 2012)

2.4.4.1 Clases de direcciones IPv4 y sus formatos

Para determinar las clases de las direcciones IPv4 de 32 bits en clases específicas, se tiene la identificación de red y de host.

Se puede determinar la clase de una dirección IPv4 identificando los primeros bits de la izquierda, a continuación se tiene los bits de red y de host.

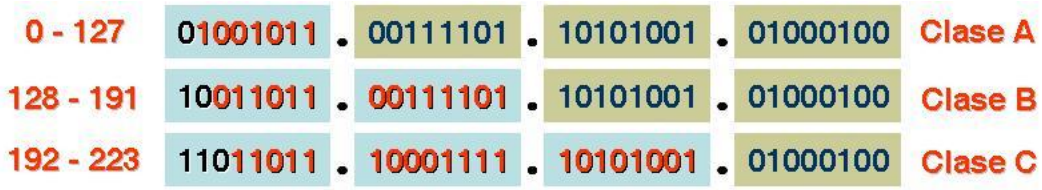
Pertenece a clase A si el primer bit es 0. Los siguientes 7 bits restantes son de red y los últimos 24 bits son de host.

Pertenece a clase B si el primer bit es 1 y el siguiente 0. Los siguientes 14 bits restantes son de red y los últimos 16 bits son de host.

Pertenece a clase C si los dos primeros bits son 1 y el siguiente 0. Los siguientes 21 bits restantes son de red y los últimos 8 bits son de host.

Son direcciones reservadas si los primeros 3 o 4 bits son 1.

Figura 5. Clases de direcciones IPv4



Primer octeto		Direcciones IP				
Primeros bits	Rango de valores	CLASE	Máscara de red	Red y máquina	Número de Redes	Número de máquinas ó hosts
0	0–127	A	255.0.0.0	N.h.h.h	2^7=128	16.777.214
10	128–191	B	255.255.0.0	N.N.h.h	2^14=16.384	65.534
110	192–223	C	255.255.255.0	N.N.N.h	2^21=2.097.152	254
1110	224 – 239	D	No aplicable	Reservado	No aplicable	No aplicable
1111	240 – 255	E	No aplicable	Reservado	No aplicable	No aplicable

Fuente: (Carossella, 2012)

2.4.4.2 Máscara de subred IPv4

"Una máscara de subred es aquella dirección que enmascarando la dirección IPv4, indica si otra dirección IPv4 pertenece a la subred o no." (Barajas, 2012).
La figura 6 muestra las máscaras de subred por defecto correspondientes a cada clase:

Figura 6. Máscara de red IPv4

Clase	Máscara de subred
A	255.0.0.0
B	255.255.0.0
C	255.255.255.0

Fuente: (Barajas, 2012)

Por ejemplo si se expresa la máscara de subred de clase A en notación binaria, se tiene:

11111111.00000000.00000000.00000000

Los unos representan las direcciones de red y los ceros representan las direcciones de host. En el primer octeto se tiene la dirección de red y en los 3 siguientes octetos se tienen las direcciones de host. Por ejemplo, la dirección de clase A 105.10.15.7 pertenece a la red 105.0.0.0. A continuación se detalla ejemplos de subredes IPv4 donde x=192.168.1.

Figura 7. Subredes IPv4

Máscara de subred	Binario	Número de subredes	Núm. de hosts por subred	Ejemplos de subredes (x=a.b.c por ejemplo, 192.168.1)
255.255.255.0	00000000	1	254	x.0
255.255.255.128	10000000	2	126	x.0, x.128
255.255.255.192	11000000	4	62	x.0, x.64, x.128, x.192
255.255.255.224	11100000	8	30	x.0, x.32, x.64, x.96, x.128, ...
255.255.255.240	11110000	16	14	x.0, x.16, x.32, x.48, x.64, ...
255.255.255.248	11111000	32	6	x.0, x.8, x.16, x.24, x.32, x.40, ...
255.255.255.252	11111100	64	2	x.0, x.4, x.8, x.12, x.16, x.20, ...
255.255.255.254	11111110	128	0	ninguna posible
255.255.255.255	11111111	256	0	ninguna posible

Fuente: (Barajas, 2012)

2.4.5 Problemas existentes en IPv4

"IPv4 es un protocolo robusto, fácil de implementar y con la capacidad de operar sobre diversos protocolos de la capa de enlace. Si bien fue diseñado inicialmente para interconectar unas pocas computadoras en redes simples, ha sido capaz de soportar el explosivo crecimiento de Internet" (Ramírez & Hidalgo, 2010, pág. 4).

Actualmente la versión de IPv4 usada en Internet no ha cambiado sustancialmente desde su publicación inicial en 1981.

"Sin embargo en el último tiempo, se han hecho notar diversos problemas existentes en IPv4, asociados al crecimiento de Internet y a la aparición de nuevas tecnologías y servicios que requieren conectividad IP" (Ramírez & Hidalgo, 2010, pág. 5).

"Si no hubiera sido por tecnologías como la NAT o el DHCP, las direcciones IPv4 se habrían acabado hace mucho más tiempo. Esto solo ha sido una muerte anunciada y la alarma que llevaba años sonando para que se tenga que migrar a IPv6" (Xatakaon, 2012).

El cambio de IPv4 a IPv6 se puede justificar de dos maneras, dos puntos de vista principalmente:

- Técnicamente en la actualidad el direccionamiento no es suficiente para la gran cantidad de equipos conectados a la red, la demanda actual y futura no podrá ser satisfecha por IPv4. Las tablas de enrutamiento actuales son demasiado grandes debido a la gran cantidad de direcciones que existen sin tener una autoconfiguración.
- Socialmente las necesidades de los usuarios del Internet han aumentado, exigiendo nuevas capacidades que IPv4 no proporciona como son la seguridad, velocidad, VoIP, multimedia, teleconferencias y aplicaciones de gran demanda. (Ahuatzin, 2012).

2.5 El protocolo IPv6

2.5.1 Introducción

La necesidad de crear un nuevo protocolo surge por la falta de direcciones y en el IETF-Internet Engineering Task Force- (Fuerza de Tareas de Ingeniería de Internet) se crea IPv6 que en un primer momento se denominó IPng-Internet Protocol Next Generation- (Protocolo de Internet de Siguiente Generación).
La posibilidad de ampliar las redes para las demandas futuras requiere una provisión ilimitada de direcciones IP y movilidad mejorada. IPv6 combina direccionamiento ampliado con una cabecera más eficiente para satisfacer las demandas.
A continuación se detallan las principales características que ofrece el protocolo IPv6:

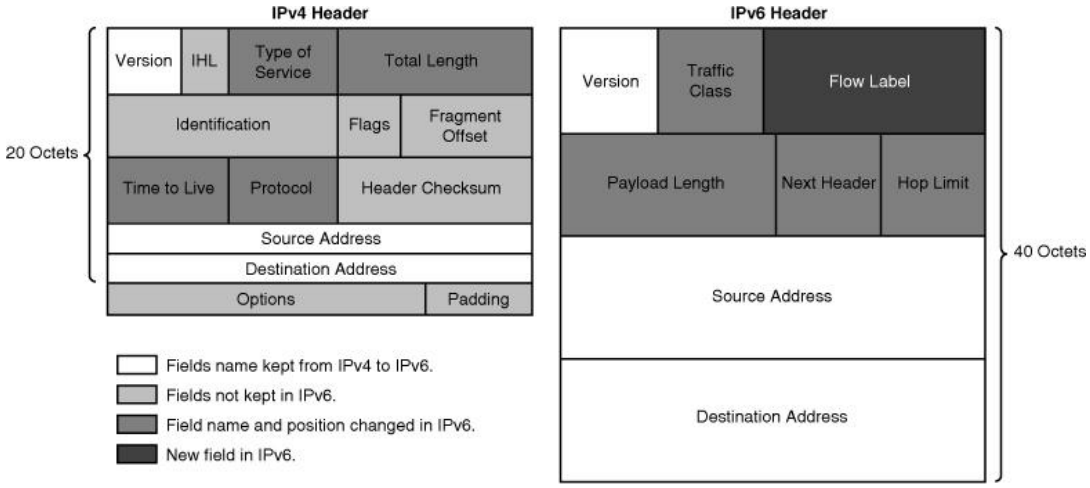
- Aumento del espacio de direcciones: El protocolo IPv4 está basado en una arquitectura que utiliza direcciones de 32 bits (4 octetos). Con la nueva versión del protocolo, las direcciones constan de 128 bits, con lo que se soluciona el problema del agotamiento de direcciones IPv4.
- Autoconfiguración: En el momento que un host se conecta a una red recibe los datos necesarios para empezar a comunicarse. Los routers proveen de información a todos los nodos sobre un enlace local, por lo tanto un host puede autoconfigurarse a sí mismo con la información proporcionada y con su dirección MAC-Media Access Control- (Control de Acceso al Medio).
- Movilidad: La movilidad está llegando a ser una característica importante y crítica en las redes actuales. Es un estándar que permite a los dispositivos móviles desplazarse sin perder las conexiones existentes.
- Seguridad: Mientras el uso de IPsec es opcional en IPv4, el mismo es una característica incorporada en IPv6. Por eso, los diseñadores de las redes podrían habilitar IPsec en todos los nodos IPv6, haciendo de esta manera más seguras a las redes.
- Encaminamiento jerárquico: El encaminamiento bajo IPv6 es jerárquico y sin clases. Con esto se pretende conseguir la disminución en el tamaño de las tablas de rutas en los backbones haciendo más simples las tareas de enrutamiento.

- QoS: El protocolo IPv6 dispone de campos más amplios para definir la prioridad y flujo de cada paquete. Según el contenido de este campo, el router deberá darle un trato más o menos especial. (Peralta, 2012).

2.5.2 Formato de la cabecera IPv6

"La nueva cabecera del protocolo IPv6 es una evolución de la cabecera IPv4, no se han introducido grandes cambios de estructura, solo se la ha mejorado y optimizado. Se han suprimido algunos campos redundantes u obsoletos y se han ampliado algunas características para hacer frente a las nuevas necesidades de los usuarios como son las comunicaciones en tiempo real y la seguridad" (Ubidia, 2007, pág. 8).

Figura 8. Cabecera en IPv6



Fuente: (Cisco, 2012)

IPv6 utiliza un tamaño de cabecera fijo de 40 bytes, que componen un total de ocho campos:

- Versión (4 bits): Versión del protocolo IP en este caso representa versión 6.
- Clase de tráfico (8 bits): En este campo se especifica la clase de tráfico. Los valores de 0 a 7 están definidos para tráfico de datos con control de congestión, de 8 a 15 para tráfico de audio y vídeo sin control de congestión.
- Etiqueta de flujo (20 bits): Permite la diferenciación de flujos de tráfico. Esto tiene importancia a la hora de manejar QoS.

- Longitud de la carga útil (16 bits): Longitud de carga útil IPv6, es decir, el resto del paquete que sigue a esta cabecera IPv6, en octetos.
- Siguiente cabecera (8 bits): Identifica el tipo de cabecera que sigue inmediatamente a la cabecera IPv6.
- Límite de saltos (8 bits): Decrementado en 1 por cada nodo que reenvía el paquete. Se descarta el paquete si el límite de saltos es decrementado hasta cero.
- Dirección origen (128 bits): Corresponde a la dirección de origen.
- Dirección destino (128 bits): Corresponde a la dirección de destino.

2.5.3 Direccionamiento IPv6

2.5.3.1 Espacio de direcciones en IPv6

"La característica más obvia que distingue a IPv6 es el uso de direcciones mucho más largas. El tamaño de una dirección en IPv6 es de 128 bits, es decir, cuatro veces más larga que una dirección IPv4. Con IPv6 es muy difícil concebir que el espacio de direcciones se agote" (Barrera & Guerra, 2005, pág. 55).

Figura 9. IPv4 vs IPv6

	Protocolo Internet versión 4 (Ipv4)	Protocolo Internet versión 6 (IPv6)
Lanzada en	1981	1999
Tamaño de las direcciones	número de 32 bits	número de 128 bits
Formato de las direcciones	Notación decimal con puntos 199.43.0.202	Notación hexadecimal: 2001:500:4::/48
Cantidad de direcciones	2^{32} = ~4 mil millones de direcciones	2^{128} = ~16 trillones de direcciones

Fuente: (CITEL, 2012)

En la figura 9 se observa que el formato de las direcciones en IPv4 e IPv6 es muy diferente. En IPv4 se utiliza la notación decimal y en IPv6 se utiliza la notación hexadecimal lo cual se explica en la página 19.

“El uso de 128 bits permite tener múltiples niveles de jerarquía y flexibilidad en el diseño jerárquico de direccionamiento y ruteo, lo que no se tiene en el actual Internet basado en IPv4” (Barrera & Guerra, 2005, pág. 55).

2.5.3.2 Sintaxis de las direcciones en IPv6

En IPv4 las direcciones tienen un formato decimal el cual es separado por puntos. Están dividas en 4 octetos (32 bits), cada octeto de 8 bits.

En IPv6 las direcciones tienen un formato hexadecimal el cual es separado por dos puntos (:). Están divididas en 8 bloques (128 bits), cada bloque de 16 bits.

A continuación se detalla una dirección IPv6 en forma binaria:

00100001110110100000000011010011000000000000000000010111100111011000000101010101000000000011111111111111110001010001001110001011010

La dirección de 128 bits dividida en límite de 16 bits es la siguiente:

0010000111011010 0000000011010011 0000000000000000 0010111100111011 0000001010101010 0000000011111111 1111111000101000 1001110001011010

La dirección de 128 bits convertida en hexadecimal es la siguiente:

21DA:00D3:0000:2F3B:02AA:00FF:FE28:9C5A

Adicionalmente a una dirección IPv6 se pueden remover los ceros más significativos (a la izquierda) existentes dentro de cada bloque de 16 bits. Sin embargo cada bloque debe tener al menos un dígito.

La dirección de 128 bits al remover los ceros es la siguiente:

21DA:D3:0:2F3B:2AA:FF:FE28:9C5A

Algunos tipos de direcciones contienen largas secuencias de ceros. Para favorecer la simplificación en la representación de las direcciones, una secuencia continua de bloques de 16 bits con valor 0 puede ser compactada utilizando el símbolo "::" conocido como doble dos puntos (double colon) (Barrera & Guerra, 2005, pág. 56).

Por ejemplo, la dirección de enlace local FE80:0:0:0:2AA:FF:FE9A:4CA2 puede ser compactada así: FE80::2AA:FF:FE9A:4CA2.

La dirección multicast FF02:0:0:0:0:0:0:2 puede ser representada así: FF02::2. La compactación de ceros puede ser solamente utilizada una vez en una dirección dada.

2.5.4 Prefijos IPv6

"El prefijo es la parte de la dirección que indica los bits que tienen valores fijos o los bits del identificador de red. Los prefijos de las rutas e identificadores de subred IPv6 se expresan de la misma forma que la notación CIDR de IPv4. Un prefijo IPv6 utiliza la notación dirección/longitud de prefijo" (Microsoft, 2012).

Por ejemplo, 12CA:B3::/48 es un prefijo de ruta y 12CA:B3:0:2E7D::/64 es un prefijo de subred.

En las direcciones IPv4 se usa una representación decimal separado por puntos que es conocido como máscara de subred.

En las direcciones IPv6 se usa la longitud del prefijo para especificar jerarquías en las direcciones, debido a esto es que no tiene tanta importancia como la máscara de subred en IPv4.

2.5.5 Tipos de direcciones IPv6

Existen 3 tipos de direcciones en IPv6:

- Unicast: "Una dirección unicast identifica una interfaz única dentro del ámbito del tipo de direcciones unicast. Con la topología apropiada para ruteo unicast, los paquetes direccionados a una dirección unicast son entregados a una sola interfaz" (Barrera & Guerra, 2005, pág. 48).
- Multicast: "Una dirección multicast identifica múltiples interfaces. Con la topología apropiada para ruteo multicast, los paquetes direccionados a una dirección multicast son entregados a todas las interfaces que son identificadas por la dirección. Las direcciones multicast son usadas para comunicaciones uno a muchos, con entrega a múltiples interfaces" (Barrera & Guerra, 2005, pág. 48).

- Anycast: “Una dirección anycast identifica múltiples interfaces. Con la topología apropiada de ruteo, los paquetes direccionados a una dirección anycast son entregados a una sola interfaz, la interfaz más cercana que es identificada por la dirección. La interfaz más cercana es definida en términos de distancia de ruteo. Las direcciones anycast son usadas para comunicaciones uno a alguno de muchos, con entrega a una sola interfaz” (Barrera & Guerra, 2005, pág. 48).

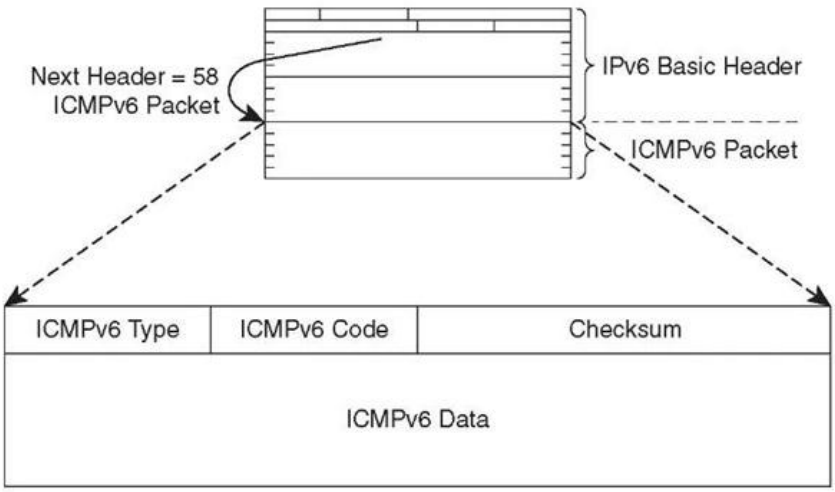
2.5.6 ICMPv6-Internet Control Message Protocol

“ICMP-Internet Control Message Protocol- (Protocolo de Mensajes de Control de Internet) ha sido actualizado para su uso bajo IPv6 y se le ha asignado el valor de 58 en el campo de “siguiente cabecera” para saber que es un ICMPv6. Este protocolo es parte integral de IPv6 y debe ser totalmente incorporado a cualquier implementación de nodo IPv6” (IPv6: ICMPv6, 2012).

“ICMPv6 es empleado por IPv6 para reportar errores que se encuentran durante el procesado de los paquetes, así como para la realización de otras funciones relativas a la capa Internet, como son las de diagnósticos ping” (SEE-MY-IP.COM, 2012).

El formato genérico de los mensajes ICMPv6 es el siguiente:

Figura 10. Mensajes ICMPv6



Fuente: (The-Crankshaft Publishing’s, 2012)

- Tipo: Aquí se detalla el tipo de mensaje ICMPv6 y el valor que toma determina el formato del resto de la cabecera.
- Código: Distingue entre varios mensajes y se emplea para crear un nivel adicional de jerarquía para la clasificación del mensaje.
- Checksum: Almacena una suma de comprobación del mensaje ICMP, también permite detectar errores en el mensaje.
- Cuerpo del Mensaje: Contiene datos del mensaje ICMPv6.

2.5.6.1 Tipos de ICMPv6

"Los mensajes de ICMPv6 se han dividido en 2 clases los que comunican errores y los que piden/dan información sobre un nodo" (Muñoz, 2012). "Los mensajes de error tienen cero en el bit de mayor peso del campo "tipo", por lo que sus valores se sitúan entre 0 y 127 y los valores de los mensajes informativos oscilan entre 128 y 255" (Medina & Moreno, 2012).

2.5.6.2 Tipos de información ICMPv6

Los mensajes de información, pueden ser del tipo:

- Echo Request (Type 128): Una estación de trabajo puede enviar un ICMP Echo Request o también conocido como ping para saber el tiempo de respuesta. A la capa superior de transporte se debe comunicar la recepción de ICMP Echo Request.
- Echo Reply (Type 129): Como respuesta al ICMP Echo Request se envía un ICMP Echo Reply y debe ser trasportado al proceso que origino el ICMP Echo Request.

2.5.6.3 Tipos de errores ICMPv6

- Destination Unreachable (Type 1): "Un ICMPv6 Destination Unreachable es enviado por un router, o por cualquier nodo, para informar de la imposibilidad de que un paquete llegue a su destino. No se deberían enviar estos mensajes si

son ocasionados por problemas de congestión de la red. Un nodo que ha recibido un ICMPv6 Destination Unreachable, debe comunicarlo a la capa superior del proceso" (Muñoz, 2012).

- Packet Too Big (Type 2): "Un ICMPv6 Packet Too Big es enviado cuando el tamaño máximo de un paquete es superior a la MTU-Maximun Transfer Unit-(Unidad Máxima de Transferencia) de la interfaz de red al que se ha enviado. También es enviado por un router si el siguiente salto tiene un MTU inferior al tamaño del paquete. Este ICMPv6 puede ser usado para saber el MTU de una ruta'' (Muñoz, 2012).
- Time Exceeded (Type 3): "Este mensaje se emite cuando se ha llegado al límite de saltos establecido para el envío de un paquete. Si un host no puede ensamblar un paquete en un tiempo dado se descartarán todos los fragmentos recibidos y se enviará un mensaje de este tipo" (Muñoz, 2012).
- Parameter Problem (Type 4): Si al procesar un paquete, un nodo IPv6 encuentra un error en uno de los parámetros de sus campos, enviará un ICMPv6 Parameter Problem informando al destino de la situación del error en el paquete (Muñoz, 2012).

Figura 11. Mensajes de error ICMPv6

Mensajes de error ICMPv6

Tipo	Descripción y Códigos	
1	Destino no alcanzable (Destination Unreachable)	
	Código	Descripción
	0	Sin ruta hacia el destino
	1	Comunicación prohibida administrativamente
	2	Sin asignar
	3	Dirección no alcanzable
	4	Puerto no alcanzable
2	Paquete demasiado grande (Packet Too Big)	
3	Tiempo excedido (Time Exceeded)	
	Código	Descripción
	0	Límite de saltos excedido
	1	Tiempo de desfragmentación excedido
4	Problema de parámetros (Parameter Problem)	
	Código	Descripción
	0	Campo erróneo en cabecera
	1	Tipo de "cabecera siguiente" desconocida
	2	Opción IPv6 desconocida

Mensajes informativos ICMPv6

Tipo	Descripción
128	Solicitud de eco (Echo Request)
129	Respuesta de eco (Echo Reply)

Fuente: (SEE-MY-IP.COM, 2012)

2.5.7 Protocolo de ruteo IPv6

Los protocolos de ruteo IPv6 están basados en los protocolos de ruteo IPv4, pero traen consigo mejoras y compatibilidad con el protocolo IPv6.

2.5.7.1 RIPng-Routing Information Protocol next generation

RIPng-Routing Information Protocol next generation- (Protocolo de Información de Enrutamiento de siguiente generación) "es un protocolo diseñado para pequeñas redes, y por tanto se incluye en el grupo IGP-Interior Gateway Protocol- (Protocolo de

Pasarela Interno), y emplea un algoritmo denominado "Vector-Distancia". Se basa en el intercambio de información entre routers, de forma que puedan calcular las rutas más adecuadas, de forma automática" (Tutorial de IPv6., 2013, pág. 38).

"RIPng solo puede ser implementado en routers, donde requerirá como información fundamental la métrica o número de saltos que un paquete ha de emplear para llegar a determinado destino. Además de la métrica, cada red tendrá un prefijo de dirección destino y la longitud del propio prefijo" (Tutorial de IPv6., 2013, pág. 39).

El router incorporará una entrada para cada destino accesible en la tabla de ruteo. Cada entrada tendrá como mínimo, los siguientes parámetros:

- El prefijo IPv6 del destino.
- La métrica (número de saltos entre este router y el destino).
- La dirección IPv6 del siguiente router, así como la ruta para llegar a él.
- Un indicador relativo al cambio de ruta.
- Varios contadores asociados con la ruta.

Al igual que en IPv4, el inconveniente de RIPng sigue siendo su orientación a pequeñas redes y el hecho de que su métrica es fija y no puede variar en función de las circunstancias de un ambiente de producción (Barrera & Guerra, 2005, pág. 82).

2.5.7.2 OSPFv6-Open Shortest Path First

OSPF-Open Shortest Path First- (Abrir Primero el Camino más Corto) es también un protocolo IGP basado en una tecnología de "estado de enlaces".

"Se trata de un protocolo de ruteo dinámico, que detecta rápidamente cambios de la topología (como un fallo en un router o interfaz) y calcula la siguiente ruta disponible (sin bucles), después de un corto período de convergencia con muy poco tráfico de routing" (Tutorial de IPv6., 2013, pág. 39).

"Cada router mantiene una base de datos que describe la topología de la red y es lo que se denomina base de datos de estado de enlaces. Todos los routers del sistema tienen una base de datos idéntica, indicando el estado de cada interfaz y de cada vecino alcanzable" (Ubidia, 2007, pág. 40).

Los routers por medio de desbordamientos o también conocidos como flooding distribuyen los estados locales, además todos utilizan el mismo algoritmo.

El coste de una ruta se determina por una métrica simple, sin dimensión. El tráfico es distribuido equitativamente entre todas las rutas cuando se tiene rutas de igual coste a un cierto destino.

A pesar que las direcciones IPv6 son más extensas se ha logrado que los paquetes OSPFv6 sean tan compactos como los paquetes IPv4, flexibilizando las opciones y eliminando algunas limitaciones.

"OSPFv6 mantiene los mecanismos fundamentales de IPv4, pero se han tenido que modificar ciertos parámetros de la semántica del protocolo, así como el incremento del tamaño de la dirección. OSPFv6 se ejecuta basado en cada enlace, en lugar de en cada subred; además se ha eliminado la autenticación del protocolo OSPFv6, dado que IPv6 incorpora estas características" (Tutorial de IPv6., 2013, pág. 40).

2.5.7.3 BGP-Border Gateway Protocol

BGP-Border Gateway Protocol- (Protocolo de Pasarela de Borde) fue creado para la interconexión de sistemas autónomos o para el enrutado entre diferentes dominios. Frecuentemente se emplea en grandes empresas que tienen grandes ambientes de comunicaciones y para la conexión entre ISP-Internet Service Provider- (Proveedor de Servicios de Internet).

"Su principal función es, por tanto, el intercambio de información de disponibilidad o alcance entre varios sistemas BGP, incluyendo información de los sistemas autónomos que contienen; permitiendo así construir las rutas más adecuadas y evitar bucles de tráfico" (Tutorial de IPv6., 2013, pág. 40).

La estrategia de salto a salto consiste en que un dispositivo que utiliza BGP solo informa de las rutas que emplea, a los dispositivos que se conectan a él.

2.5.8 NDP-Neighbor Discovery Protocol

NDP-Neighbor Discovery Protocol- (Protocolo de Descubrimiento de Vecinos) “es el mecanismo por el cual un nodo que se incorpora a una red descubre la presencia de otros en su mismo enlace, a fin de determinar sus direcciones en la capa de enlace; además permite localizar los routers y mantener la información de conectividad acerca de las rutas a los vecinos activos” (Barrera & Guerra, 2005, pág. 83).

“Define, entre otros, mecanismos para: descubrir routers, prefijos y parámetros, autoconfiguración de direcciones, resolución de direcciones, determinación del siguiente salto, detección de nodos no alcanzables, detección de direcciones duplicadas o cambios, redirección, balanceo de carga entrante, direcciones anycast, y anunciación de proxies” (Tutorial de IPv6., 2013, pág. 27).

El protocolo Neighbor Discovery define cinco tipos de paquetes ICMPv6:

- Router Discovery (Descubrimiento de router): Es generado cuando una interfaz se activa y solicita información sobre los routers activos. Este mensaje comunica al host y a otros routers la existencia de un nuevo router, la permanencia o la eliminación de los actuales.
- Router Advertisement (Anuncio de router): Se genera periódicamente por los routers, a través de multicast, a fin de informar de su presencia así como de otros parámetros de enlace.
- Neighbor Solicitation (Solicitud de Vecino): Es generado por los nodos para determinar la dirección en la capa de enlace de sus vecinos, o para verificar que el nodo vecino sigue activo, así como para detectar direcciones duplicadas.
- Neighbor Advertisement (Anuncio de Vecino): Es generado por los nodos como respuesta a la solicitud de vecino, o bien para indicar cambios de direcciones en la capa de enlace.
- Redirect (Redirección): Se genera en los routers para informar a los host de un salto más eficiente para llegar a un determinado destino. (Barrera & Guerra, 2005, pág. 84)

2.5.8.1 Ventajas del protocol Neighbor Discovery

Las principales ventajas del protocolo Neighbor Discovery son:

- No es necesario recurrir a protocolos de encaminamiento debido que es parte de la base del protocolo descubrir routers.
- Permite la autoconfiguración de direcciones debido a la anunciación de router.
- El intercambio de paquetes de información entre equipos y el uso de protocolos de enrutamiento es menor.
- La detección de vecinos no alcanzables es utilizada para la robustez en la entrega de paquetes frente a fallos en routers, enlaces, nodos que cambian sus direcciones, nodos móviles, etc.
- Maneja con mayor eficacia la información de ruteo de las redes que es almacenada por los equipos de comunicación.
- Para evitar envíos accidentales o intencionados desde nodos fuera del enlace se limitan los saltos a 255, ya que los routers decrementan automáticamente este campo en cada salto.

2.6 Mecanismos de transición a IPv6

Existen varios mecanismos que permiten que IPv4 e IPv6 coexistan en la misma red, entre ellos están:

2.6.1 Mecanismos tipo túnel

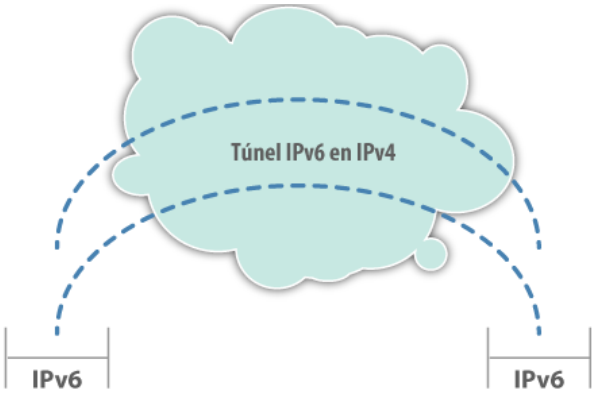
"Encapsular un paquete IP dentro de otro, es un mecanismo conocido y se usa en la actualidad sobre todo para crear redes privadas virtuales. La utilidad que se le da es para enlazar nubes o islas IPv6 en una Internet basada prácticamente en su totalidad en IPv4" (Peralta, 2012, pág. 31).

Entre los mecanismos tipo túnel más utilizado se tiene:

- Túneles estáticos
- 6to4

- 6in4
- 6over4
- Teredo
- ISATAP (Intra Site Automatic Tunnel Addressing Protocol)

Figura 12. Mecanismo tipo túnel



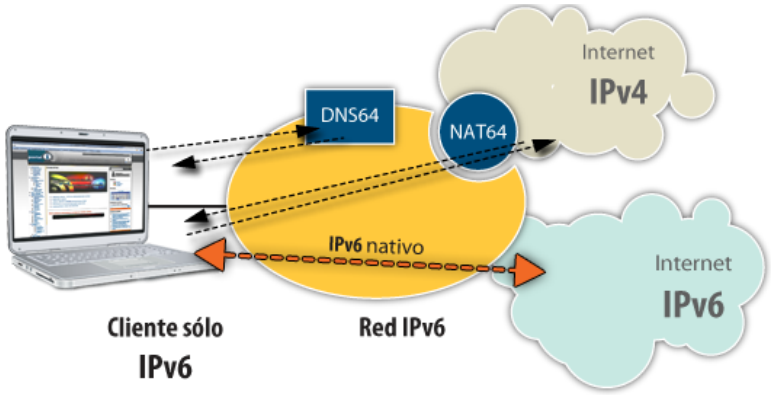
Fuente: (Cicileo, 2012)

2.6.2 Mecanismos de traducción

Su funcionamiento consiste en utilizar algún dispositivo en la red que convierte los paquetes IPv4 a IPv6 y viceversa. Algunos de los mecanismos de traducción son:

- Stateless IP/ICMP Translation Algorithm (SIIT)
- Network Address Translation - Protocol Translation (NAT-PT)
- Bump in the Stack (BIS)

Figura 13. Mecanismos de traducción

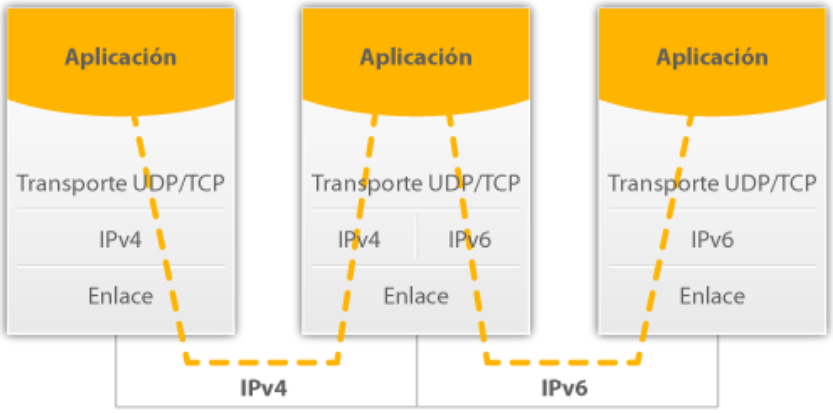


Fuente: (Cicileo, 2012)

2.6.3 Doble pila

"Para que un nodo se pueda comunicar tanto con nodos IPv6 como IPv4, la solución más rápida es pensar en la doble pila de protocolos. Teniendo cada nodo una dirección IPv4 e IPv6 enrutable, se conseguirá que se produzca la comunicación" (Ubidia, 2007, pág. 31).

Figura 14. Doble Pila



Fuente: (Cicileo, 2012)

2.7 Servicios de Internet

Servicios de Internet son todas las prestaciones que ofrece el Internet a los usuarios, entre los servicios con que cuenta, se tiene los siguientes:

- WWW-World Wide Web- (Red Informática Mundial): Permite consultar información almacenada en cualquier computadora de la red. Es el servicio más flexible, porque además de consultar información permite también enviar datos.
- SFTP-Secure File Transfer Protocol- (Protocolo de Transferencia de Archivos Seguro): Permite el intercambio de archivos de una computadora a otra de forma segura, ya que toda la información intercambiada entre su ordenador y el servidor es encriptada.
- Correo electrónico (e-mail): Permite la transferencia personal de mensajes y archivos de un remitente a un destinatario.
- News: Son foros de discusión que permiten intercambiar opiniones entre todos los usuarios de Internet.
- Listas de correo: Están íntimamente relacionadas con el correo electrónico. Son listas de direcciones electrónicas de personas con intereses comunes.
- Chat: Este servicio permite charlar en tiempo real con otros usuarios mediante el teclado de la computadora.
- Videoconferencia: Este servicio permite hablar con otra persona de viva voz y viendo además su imagen.
- SSH: Al igual que telnet es un servicio de acceso remoto a un servidor de la red con la ventaja de que lo que se transmite a través de esta conexión esta codificado. (Lezcano, 2012).

2.8 Protocolos de red

2.8.1 DHCP

"DHCP es un protocolo de red empleado para asignar de forma automática una dirección IP a los hosts que se conectan a ella. En redes pequeñas las direcciones IP pueden asignarse de forma manual, equipo por equipo, pero en redes de un cierto tamaño esta tarea puede convertirse en agotadora, no sólo por tener que editar cada

uno de los hosts, sino por la dificultad de mantener un registro con las IPs asignadas para evitar duplicados.” (Escartin, 2012, pág. 101).

2.8.2 POP

POP es un protocolo estándar para recibir mensajes de correo electrónico almacenados en un servidor remoto. Cuando se hace referencia a POP se refiere a la versión POP3 dentro del contexto de protocolos de correo electrónico.

2.8.3 SMTP

“Este es el protocolo dedicado a la transmisión de mensajes electrónicos sobre una conexión TCP, normalmente utiliza el puerto 25 en el servidor. El protocolo especifica el formato de los mensajes definiendo la estructura de la información sobre el remitente, el destinatario, datos adicionales y naturalmente el cuerpo de los mensajes” (Escartin, 2012, pág. 92).

2.8.4 HTTP

“Este es un sencillo protocolo cliente-servidor que articula los intercambios de información entre los clientes Web y los servidores HTTP. Está soportado sobre los servicios de conexión TCP/IP. Un proceso servidor espera las solicitudes de conexión de los clientes Web, y una vez se establece la conexión, el protocolo TCP se encarga de mantener la comunicación y garantizar un intercambio de datos libre de errores” (Escartin, 2012, pág. 93).

2.9 QoS

“La calidad del servicio es definido como la capacidad de una red para proporcionar diversos niveles de servicio a los diferentes tipos de tráfico. Mediante QoS es posible asegurar una correcta entrega de la información, dando preferencia a aplicaciones de

desempeño crítico, donde se comparten simultáneamente los recursos de red con otras aplicaciones no críticas" (Salcedo, López, & Ríos, 2012, pág. 33).

2.9.1 Clasificación de los protocolos de QoS

De entre todas las opciones, los protocolos y algoritmos más utilizados son:

2.9.1.1 INTSERV-Integrated Services

INTSERV-Integrated Services- (Servicios Integrados) simula un sistema de circuitos sobre IP, utiliza RSVP-Resource Reservation Protocol- (Protocolo de Reserva de Recursos) para señalar el camino por donde se requiere la QoS. "RSVP genera "Soft States" en los routers, estos pueden ser modificados por nuevos mensajes. Trabaja con un esquema per-flow QoS, trata de cubrir los requerimientos de QoS por flujo de datos." (Universidad Nacional de la Plata, 2012, pág. 2).

El RSVP utiliza clases de QoS de las cuales las más utilizadas son:

- Servicios garantizados (Guaranteed Service).
- Servicio de Carga Controlada (Controlled-Load Service)

Desventajas:

- Carencia de escalabilidad. Se necesita demasiados recursos de procesamiento y almacenamiento. Se puede aplicar solo a redes pequeñas.
- Todos los routers deben implementar RSVP, extra al tratamiento de QoS, control de admisión, clasificación, etc.

2.9.1.2 DIFFSERV-Differentiated Services

DIFFSERV-Differentiated Services- (Servicios Diferenciados) es un protocolo de QoS que permite dividir y dar prioridad al tráfico de la red mediante el uso de etiquetas en las cabeceras de los paquetes.

"Permite a los proveedores de servicios de Internet y a usuarios de grandes redes IP corporativas desplegar rápidamente diferentes niveles QoS en la troncal. A diferencia de RSVP no especifica un sistema de señalización, consiste en un método para marcar

o etiquetar paquetes, permitiendo a los routers modificar su comportamiento de envío" (Ubidia, 2007, pág. 44). Cada tipo de etiqueta representa el tipo de QoS y el tráfico.
Los elementos principales de la arquitectura DiffServ son:

- Clasificador: Entidad que selecciona paquetes en base al contenido de las cabeceras, según unas reglas definidas.
- Marcador: Controla el tráfico mediante el re-marcado de los paquetes con un código diferente (si es necesario).
- Medidor: Mide el tráfico enviado que se ajusta a un perfil.
- Modelador: Controla el tráfico retardando paquetes para no exceder la velocidad especificada.
- Elemento de descarte**:** Descarta paquetes cuando la velocidad de transferencia excede de la especificada. (Ubidia, 2007, pág. 44)

Desventajas:

- Se agrupan flujos individuales en una misma clase, no pueden ser diferenciados.
- Modelo más estático en la implementación.
- Puede producirse un delay mayor en el mapeo de las clases. (Universidad Nacional de la Plata, 2012, pág. 5)

2.9.1.3 MPLS-Multiprotocol Label Switching

MPLS-Multiprotocol Label Switching- (Conmutación de Etiquetas Multiprotocolo) "proporciona la posibilidad de administrar el ancho de banda de la red a través de etiquetas en las cabeceras de los paquetes (encapsulamiento) y de encaminadores específicos capaces de reconocerlas" (Ubidia, 2007, pág. 45).
MPLS puede utilizar el modelo Diffserv o IntServ. Se puede utilizar para trabajar con Ingeniería de tráfico, el modelo es más eficiente y es extendible a IPv6.

"MPLS usa un esquema de etiquetado del tráfico hacia delante; el tráfico es marcado en su entrada a la red pero no en los puntos de salida. MPLS reside únicamente en los routers y es independiente del protocolo utilizado" (Ubidia, 2007, pág. 45).

Algunos componentes encontrados en los esquemas de QoS:

- Control de admisión.
- Control de políticas.
- Policing y Shaping.
- Clasificador.
- Planificados.

2.10 GNU/Linux

"GNU/Linux es el primer sistema operativo basado en UNIX que es 100% software libre. Si bien anteriormente había otros sistemas operativos de libre distribución como MINIX, estos no eran totalmente software libre, ya que eran regidos por licencias más restrictivas" (Quintana, 2013).

Dos características muy peculiares lo diferencian del resto de los sistemas que se puede encontrar en el mercado:

- Es libre, esto significa que no se tiene que pagar ningún tipo de licencia a ninguna casa desarrolladora de software por el uso del mismo.
- El sistema viene acompañado del código fuente.

El sistema está formado por el núcleo del sistema o kernel, programas y librerías que hacen posible su utilización.
Linux se distribuye bajo la licencia pública general, por lo tanto el código fuente tiene que estar siempre accesible.

2.10.1 Características

Entre las principales características de GNU/Linux se tiene:

- Multitarea: Varios programas ejecutándose al mismo tiempo.
- Multiusuario: Varios usuarios en la misma máquina al mismo tiempo.
- Multiplataforma: Corre en muchas CPUs distintas, no sólo Intel.
- Tiene protección de la memoria entre procesos, de manera que uno de ellos no pueda colgar el sistema.

- Carga de ejecutables por demanda: Linux sólo lee de disco aquellas partes de un programa que están siendo usadas actualmente.
- La memoria se gestiona como un recurso unificado para los programas de usuario y para el caché de disco, de tal forma que toda la memoria libre puede ser usada para caché y éste puede a su vez ser reducido cuando se ejecuten grandes programas.
- Librerías compartidas de carga dinámica y librerías estáticas.
- Todo el código fuente está disponible, incluyendo el núcleo completo y todos los drivers, las herramientas de desarrollo y todos los programas de usuario; además todo ello se puede distribuir libremente. Hay algunos programas comerciales que están siendo ofrecidos para Linux actualmente sin código fuente, pero todo lo que ha sido gratuito sigue siendo gratuito.
- Soporte para varios sistemas de archivo comunes, incluyendo minix-1, Xenix y todos los sistemas de archivo típicos de System V, tiene un avanzado sistema de archivos propio con una capacidad de hasta 4 Tb y nombres de archivos de hasta 255 caracteres de longitud.
- TCP/IP, incluyendo FTP, telnet, NFS-Network File System- (Sistema de Archivos de Red), etc. (Guadalinfo, 2013).

2.10.2 Distribuciones de Linux

"GNU/Linux se ha convertido en un sistema operativo que rivaliza con los dos más grandes: Windows y Mac. El escritorio que presentan las 10 distribuciones Linux más populares tienen una calidad gráfica que igualan e incluso superan Windows 7 o Mac OS X Leopard" (DistroWatch, 2012).

Entre las distribuciones más populares se tiene:

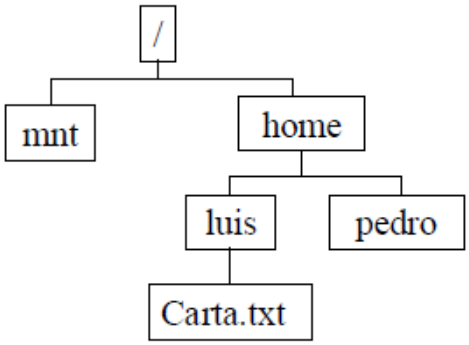
1. Ubuntu: De la empresa Canonical, esta distribución se hizo muy popular por ser de las que envían su CD a los hogares de los que lo soliciten. Es la número uno en la elección de usuarios por su simplicidad y por ser muy completa en el software disponible. Es la que más aplicaciones cuenta en su haber.
2. Fedora: Es un proyecto compuesto por programadores, ingenieros y diseñadores gráficos, que tienen como objetivo ser líderes en el ámbito tecnológico.

3. Linux Mint: Esta distribución está basada en Ubuntu de Canonical, pretende crear un escritorio que sea elegante, actualizado y cómodo.
4. OpenSUSE: Es la distribución Linux sostenida por Novell y AMD, con lo cual pretenden brindar un sistema operativo estable y rápido a los usuarios linuxeros.
5. Debian GNU/Linux: Es la distribución más antigua en uso. Es el referente de muchas distribuciones, por ejemplo Ubuntu se basó en Debian para crear su sistema operativo.
6. Mandriva: Conocida en un comienzo como Mandrake, es considera la distribución más fácil e intuitiva de Linux
7. Puppy Linux: Es una distribución extremadamente pequeña, (64MB lo más básico), ideal para correr como LiveCD y realizar mantenimiento de otros sistemas.
8. CentOS: Es una distribución de Linux gratuita que está basada en la distribución Red Hat Enterprise Linux.
9. Sabayon Linux: Basada en Gentoo, busca adaptarse al diseño llamativo y a brindar software precompilado.
10. Arch Linux: Distribución que se ha propuesto mantener su sistema muy simple pero con una interfaz gráfica agradable. (DistroWatch, 2012).

2.10.3 El camino

"En cualquier sistema operativo moderno la estructura de archivos es jerárquica y depende de los directorios. En general la estructura del sistema de archivos se asemeja a una estructura de árbol, estando compuesto cada nudo por un directorio o carpeta, que contiene otros directorios o archivos" (Universidad de Antoquia, 2012).
"En Windows cada unidad de disco se identifica como una carpeta básica que sirve de raíz a otras y cuyo nombre es especial. En los sistemas UNIX y por lo tanto en Linux, existe una única raíz llamada / de la que cuelgan todos los ficheros y directorios. Además es independiente de qué dispositivos estén conectados al ordenador" (Manuales de Linux, 2012).
El camino de un archivo o directorio es la secuencia de directorios que se ha de recorrer para acceder a un determinado fichero separados por /.

Figura 15. Estructura de archivos en Linux



Fuente: (Universidad de Antoquia, 2012)

Existen dos formas del camino:

- El camino absoluto que muestra toda la ruta a un fichero, /home/luis/Carta.txt.
- El camino relativo a un determinado directorio, por ejemplo si no se encuentra en el directorio /home, el camino relativo al fichero Carta.txt es luis/Carta.txt

2.10.4 Estructura del sistema de archivos de Linux

Existen muchas definiciones acerca de lo que es un sistema de archivos; se trata de la forma en que el sistema operativo estructura los datos en la unidad de almacenamiento. "En GNU/Linux, los datos se ordenan en archivos y directorios. La diferencia especial radica en que generalmente los programas no son almacenados cada uno en su propio directorio, sino que sus diferentes componentes están dispersos por todo el sistema de archivos. Así, se tiene un directorio específico para todos los ejecutables, otro para la documentación, otro para las librerías, etc" (Facundo, 2003, pág. 33).

A continuación se detalla los directorios que componen el árbol de GNU/Linux.

Tabla 1. Directorios de Linux

Directorio	Descripción
/	Directorio raíz, desde aquí "cuelgan" todos los demás directorios del sistema.
/bin	En este directorio se almacenan archivos binarios ejecutables. Generalmente, se encuentran los archivos correspondientes a los comandos básicos del sistema.
/boot	En este directorio se almacena el núcleo Linux, así como los archivos de configuración necesarios para su uso.

/dev	Éste es un directorio muy especial. Los archivos que están aquí dentro representan los diferentes dispositivos del sistema.
/etc	Aquí se almacenan todos los archivos de configuración de GNU/Linux y de los demás programas de usuario.
/home	Este directorio contiene los subdirectorios personales de los usuarios del sistema. Cada usuario posee su propio directorio, en el que puede almacenar archivos personales, tales como documentos, programas y archivos de configuración.
/lib	En este directorio se almacenan las librerías de programación básicas de GNU/Linux
/mnt	Este directorio contiene subdirectorios que actúan como puntos de montaje. Desde aquí se puede acceder al contenido de otras particiones o unidades.
/root	Este es el directorio personal del usuario root.
/sbin	Aquí se encuentran los archivos binarios ejecutables correspondientes a los comandos de administración del sistema.
/proc	Aquí se encuentran los archivos que contienen información sobre el sistema (CPU, memoria, dispositivos PCI, Plug and Play, etc.)
/usr	En este directorio se encuentra "todo lo demás": archivos de documentación, programas, más librerías, código fuente, etc.
/var	En este directorio se almacenan varias cosas, como la cola de impresión, los archivos de registración (log), etc. Será interesante dar un vistazo a este directorio.

Fuente: (Facundo, 2003)

El directorio raíz de un sistema GNU/Linux contiene muchos subdirectorios, todos imprescindibles para el correcto funcionamiento del sistema.

2.10.5 Ventajas de Linux

- Es totalmente gratuito y aunque posea versiones de paga (con soporte técnico) es aún más barato que comprar Windows.
- Un punto muy importante es la seguridad, los Hackers y/o creadores de virus rara vez atacan a software de Linux.
- Se lleva bien en el arranque en conjunto con Windows.
- Linux integra una implementación completa de los diferentes protocolos y estándares de red, con los que se puede conectar fácilmente a Internet y acceder a todo tipo de información disponible.

- Linux puede ser utilizado como una estación personal pero también como un potente servidor de red.
- Carga y realiza tareas con mayor eficiencia que Windows.
- Las distribuciones importantes tienen muchos programas muy útiles y que se los puede encontrar muy fácilmente en Internet.
- Como se puede observar en muchas webs, existe infinidad de información técnica que servirá de ayuda.
- La constante actualización y nuevas versiones es asombrosa. Existen infinidades de distribuciones de Linux.
- Crece mucho gracias a miles de programadores en todo el mundo.
- Linux es básicamente un duplicado de UNIX, lo que significa que incorpora muchas de las ventajas de este importante sistema operativo.
- El paquete incluye el código fuente, lo que permite modificarlo de acuerdo a las necesidades del usuario.
- Utiliza varios formatos de archivo que son compatibles con casi todos los sistemas operacionales utilizados en la actualidad. (Blogdiario, 2013)

2.10.6 Desventajas de Linux

- A la hora de trabajar con documentos de Windows complejos, se podría convertir en una tareas difícil o casi imposible debido a la poca compatibilidad para importar desde Windows para Linux.
- Instalar controladores de hardware y programas resulta ser más complicado que en Windows. Esto debido a que las empresas creadoras de controladores crean sus productos en base a Windows, el sistema operativo más usado a nivel mundial. (Blogdiario, 2013)
- Menos intuitivo porque Windows es muy cómodo para los usuarios comunes. De todas maneras algunas distribuciones de Linux han mejorado este aspecto.
- No se pueden ejecutar programas de Windows (la gran mayoría de los programas están escritos para Windows), además la mayoría de las aplicaciones se encuentran solo en inglés.
- Muchas distribuciones de Linux no tienen una empresa que los respalde. (Aguayo, 2012).

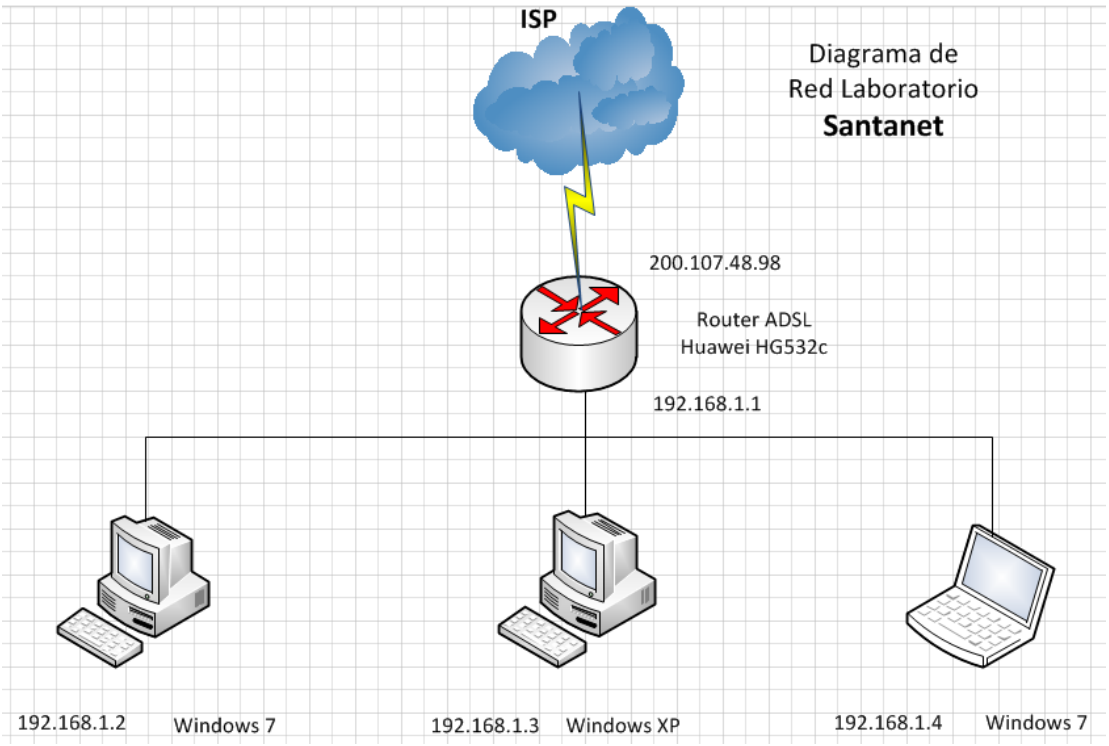
CAPÍTULO 3
ANÁLISIS Y DISEÑO DE UNA LAN CON IPv6 Y QoS

3.1 Análisis de la topología física de la LAN

La topología física es la distribución geométrica de las estaciones de trabajo en una red, los cables y los diferentes componentes.

La empresa Santanet actualmente tiene implementada la topología estrella, debido a que disponen de un router ADSL-Asymmetric Digital Subscriber Line- (Línea de Abonado Digital Asimétrica) al cual están conectados 3 PC-Personal Computer- (Computadora Personal).

Figura 16. Diagrama actual de red IPv4 de la empresa Santanet



Elaborado por: Alejandro Santamaría

3.1.1 Análisis de Hardware

La empresa Santanet dispone de 3 PCs, en la tabla 2 se puede observar las características de hardware.

Tabla 2. Características de hardware

Detalle	PC1	PC2	PC3
Tipo	Desktop	Desktop	Laptop
Procesador	Intel Pentium 4	Intel Atom	Intel Core i5
Mainboard	Biostar	Intel	Intel
Memoria	2 Gb	2 Gb	4 Gb
Disco duro	1 Tb	500 Gb	500 Gb
Tarjeta de red	10/100 Fast Ethernet	10/100 Fast Ethernet	10/100/1000 Gigabit Ethernet

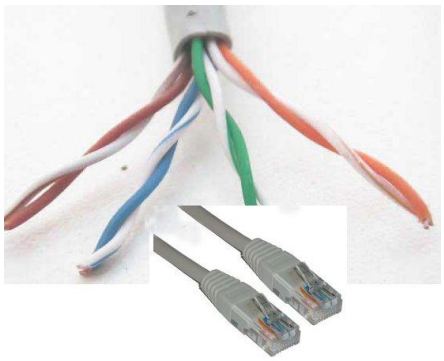
Elaborado por: Alejandro Santamaría

3.1.1.1 Cableado

El cable UTP-Unshielded Twisted Pair- (Par Trenzado No Blindado) es el soporte físico más utilizado en las redes LAN, tanto su costo como la instalación es económico. En este medio se puede enviar señales analógicas y digitales. Está compuesto por conductores de cobre que están trenzados en pares.

La empresa Santanet utiliza para sus equipos el Cable UTP categoría 5e.

Figura 17. Cable UTP categoría 5e



Fuente: (Tele-Hizmo, 2013)

3.1.2 Análisis de equipos de comunicación

Los equipos de red son dispositivos que se encuentra en la LAN y cada uno de ellos cumple una función específica. Estos equipos suelen ayudar a la administración, control y seguridad de la red.

3.1.2.1 Hub

También conocido como repetidor multipuerto, operan en la capa 1 o física del modelo OSI. Su función es retransmitir la señal a todos los dispositivos conectados a él.

Figura 18. Hub

Fuente: (Netgear, 2013)

3.1.2.2 Switch

El switch o conmutador es un dispositivo que opera en la capa 2 o enlace de datos del modelo OSI, se utiliza para múltiples redes. Estos funcionan como un filtro en la red mejorando el rendimiento y la seguridad de las LANs. La diferencia entre el hub y el switch es que los switches toman decisiones basándose en las direcciones MAC y los hubs no toman ninguna decisión, debido a esto los switches hacen más eficiente a la LAN.

Figura 19. Switch

Fuente: (D-Link, 2013)

3.1.2.3 Puente

Un puente es un dispositivo que opera en la capa 2 o enlace de datos del modelo OSI, se encarga de conectar dos segmentos de red. El propósito de un puente es filtrar el tráfico de una red.

Figura 20. Puente

Fuente: (Ramirez, 2013)

3.1.2.4 Router

Un router es un dispositivo que sirve para realizar la conexión de diferentes redes de computadoras.
Los routers operan en la capa 3 o de red del modelo OSI buscando y registrando en las tablas de enrutamiento las diferentes redes para así elegir la mejor ruta hacia ellas.

Figura 21. Router

Fuente: (Ramirez, 2013)

3.1.2.5 Router ADSL

También conocido como encaminador ADSL o modem ADSL debido a que permite conectar una red local a Internet mediante una línea telefónica fija ADSL. Este dispositivo son varios componentes en uno y realiza las funciones de:

- Puerta de enlace
- Encaminador
- Modem ADSL
- Switch LAN
- Punto de acceso inalámbrico

Figura 22. Router ADSL

Fuente: (Jazztel, 2013)

La empresa Santanet actualmente dispone del router ADSL Huawei Echolife HG532c que presenta las características de la tabla 3.

Tabla 3. Características Huawei Echolife HG532c

Huawei Echolife HG532c
Características
Es una serie de acceso desde el hogar diseñados para proporcionar alta velocidad, ADSL2 y ADSL2 + interfaces externas de acceso a WAN de banda ancha. También proporciona WLAN, Ethernet Client.
Configuración Vía Web
Autodiagnóstico
Wi-Fi 802.11n (300Mbps)

4 Puertos Ethernet (RJ45), USB
Firmware Actualizable
Permite Reenvió
Modo simple de activar o desactivar el Wi-Fi
Máximo aprovechamiento del ancho de banda provisto por tu ISP
ADSL2+ de última generación
Rechazo a ruidos de línea de Telefónica
Sistema de LOGS para analizar (tráfico, desconexiones, usuarios conectados, bloqueados, etc.).
Selección manual del tipo de ADSL: ADSL2+, ADSL2, GDMT, GLITE, TI.413, ANNEXM, Wireless Home Gateway.
Uplink: 1 RJ-11 ADSL/ADSL2+ interface Downlink: 4 10/100Base-T Ethernet RJ-45 interfaces;1 Wi-Fi 802.11b/g
Dimensiones (L × W × H): 164 mm × 142 mm × 49 mm
Todos los protocolos de encapsulación: PPPoE, PPPoA, RFC2684 (IPoA), RFC2684B (IPoE).
- CWMP (Protocolo del servicio de Autoconfiguración)
VLAN (Virtual LAN) Único producto de esta categoría que tiene incorporado el nuevo protocolo: IEEE 802.1Q.
SEGURIDAD Wi-Fi ENCRIPTACIÓN WEP DE: 64 y 128 bits Otras encriptaciones :WPA2-PSK(TKIP y AES), WPA-PSK(TKIP y AES) Filtrado por MAC Address

Elaborado por: Alejandro Santamaría

3.2 Análisis de la topología lógica de la LAN

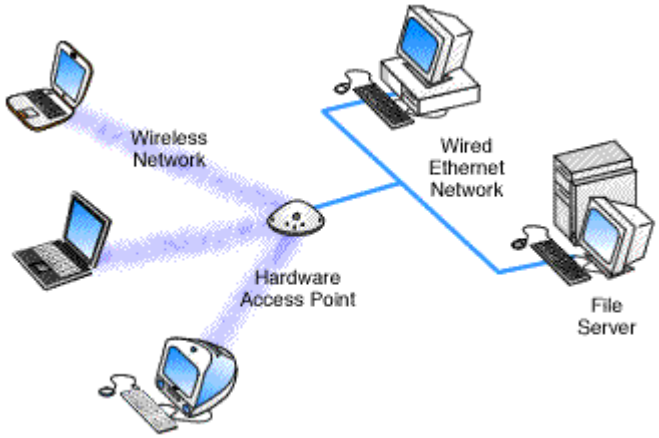
"La topología lógica se refiere al trayecto seguido por las señales a través del medio. Las estaciones de trabajo en una red se pueden comunicar directa o indirectamente" (Universidad de Vigo, 2013).

Entre las topologías lógicas se tiene:

- Topología punto a punto
- Topología punto a multipunto

La empresa Santanet actualmente tiene implementada la topología punto a multipunto, debido a que solo existe una línea de comunicación, que para identificar los transmisores y receptores utiliza el direccionamiento.

Figura 23. Topología punto a multipunto



Fuente: (NetSolutions, 2013)

3.2.1 Análisis de Software

En este análisis se va a buscar software cuyo uso sea sencillo, práctico, aplicable y más que nada que se disponga de la suficiente información para su implementación. Para esto se debe analizar los requerimientos del entorno al cual se va a dar solución.

3.2.1.1 Sistema operativo

La empresa Santanet dispone de 3 PCs, en la tabla 4 se detallan las características de software que poseen.

Tabla 4. Características de software

Detalle	PC1	PC2	PC3
Tipo	Desktop	Desktop	Laptop
SO	Windows 7 SP1	Windows XP SP3	Windows 7 SP1
Versión	Ultimate	Profesional	Home Premium
Plataforma	32 bits	32 bits	64 bits
Licencia	Comercial	Comercial	Comercial
Soporta IPv6	Si	Si	Si
Soporta QoS	Si	Si	Si

Elaborado por: Alejandro Santamaría

3.2.1.2 Protocolos

Un protocolo de red es un conjunto de reglas usadas por estaciones de trabajo para comunicarse unas con otras a través de una red, además es un estándar que controla o permite la conexión, comunicación, y transferencia de datos entre dos puntos finales. Los PCs de la empresa Santanet disponen de los protocolos que se detallan en la tabla 5.

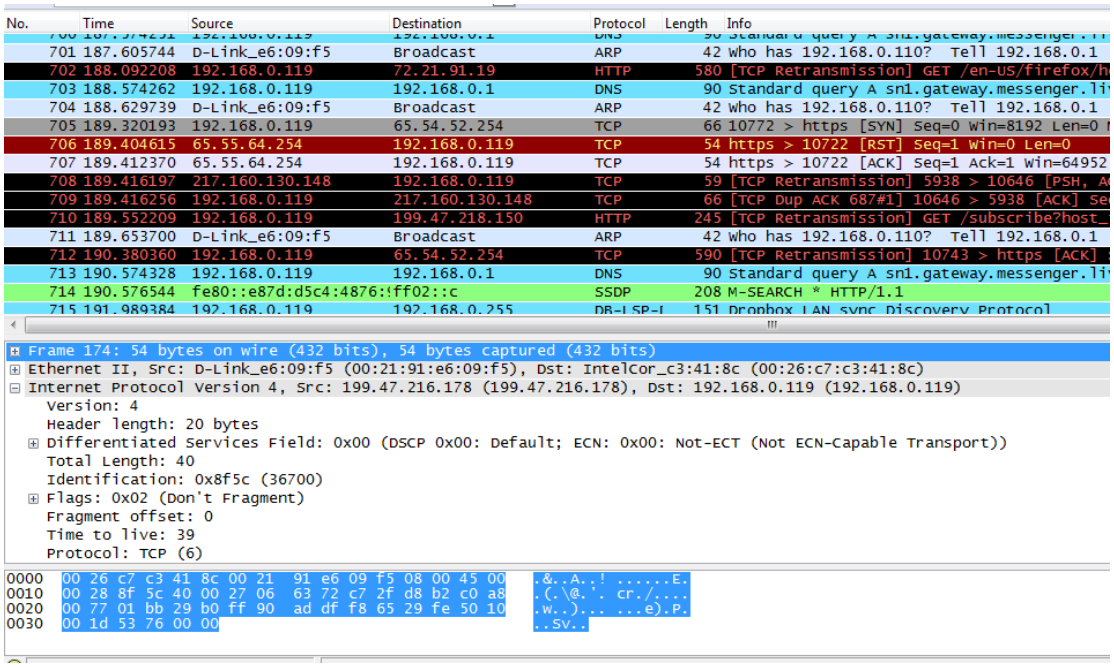
Tabla 5. Protocolos en PCs

Protocolo	PC1–Windows 7	PC2–Windows XP	PC3-Windows 7
FTP	Si	Si	Si
TELNET	Si	Si	Si
SMTP	Si	Si	Si
POP	Si	Si	Si
HTTP	Si	Si	Si
SNMP	Si	Si	Si
TFTP	Si	Si	Si
DNS	Si	Si	Si
DHCP	Si	Si	Si
ICMP	Si	Si	Si

Elaborado por: Alejandro Santamaría

Utilizando el software Wireshark se realizó el análisis de red en uno de los equipos de la empresa Santanet, mediante el cual se pudo analizar el tráfico y protocolos que se pueden observar en la figura 24.

Figura 24. Captura de protocolos



Elaborado por: Alejandro Santamaría

3.2.2 Acceso a Internet

La empresa Santanet actualmente dispone del servicio de Internet del ISP Corporación Nacional de Telecomunicaciones (CNT).

CNT provee el servicio de Internet a la empresa Santanet mediante la línea telefónica o también conocido este sistema como ADSL.

En la última milla la empresa Santanet recibe direcciones IPv4 mediante NAT.

3.2.2.1 Ancho de banda

El ancho de banda es la cantidad de datos que se pueden transmitir en un periodo de tiempo. El ancho de banda es necesario administrar de manera eficiente para satisfacer las necesidades de las aplicaciones o del usuario.

La capacidad de transmisión del canal de Internet de la empresa Santanet es de 2048Kbps de bajada y 512Kbps de subida.

3.3 Diseño físico de la LAN

Para el diseño físico de la red en la empresa Santanet se tendrá en cuenta la distribución y ubicación física de los equipos para dar la mejor solución tecnológica.

3.3.1 Equipos a utilizar en la implementación

Para la implementación se tomará en cuenta los componentes de hardware, estos se dividen en varias categorías.

3.3.1.1 Equipos de red

Los equipos de red son los periféricos necesarios para lograr que los nodos y demás elementos de una red logren comunicarse. Además de los equipos que la empresa Santanet actualmente dispone se necesita de algunos equipos adicionales.

Tabla 6. Comparación de router

Características	Router HP	Router Cisco	PC de Escritorio
Modelo	MSR20-20	1802	Quagga 0.99
Soporte de IPv6	Si	Si	Si
QoS	Si	Si	No
Protocolos	OSPF, BGP-4, IS-IS, RIP-1, RIP-2, IGMPv2, VRRP, OSPFv2, PIM-SM, PIM-DM, IGMPv3, GRE, OSPFv3, BGP, MSDP, RIPng.	OSPF, RIPv1, RIPv2, BGP, EIGRP, NHRP, GRE.	RIPv1, RIPv2, RIPng, OSPFv2, OSPFv3, BGP-4 y BGP-4+
Costo	850,00 USD	800,00 USD	0, 00 USD

Elaborado por: Alejandro Santamaría

Para la implementación de la LAN se utilizará un PC de escritorio como router debido a las prestaciones y su bajo costo.

Tabla 7. Comparación de switch

Características	Switch Nexxt	Switch D-Link	Switch TP-Link
Modelo	NW223NXT29	DES-1016D	TL-SF1016DS
Soporte de IPv6	No	No	No
Puertos	16	16	16
VLAN	No	No	No
Control de Tráfico	No	No	No
Administración	No	No	No
Costo	60,00 USD	50,00 USD	50,00 USD

Elaborado por: Alejandro Santamaría

En lo referente a conectividad se utilizará un Switch D-Link DES-1016D debido a su costo y prestaciones que se necesitan para la implementación de la red prototipo con el protocolo IPv6.

3.3.1.2 Cableado

El cable de red es elaborado para transmitir datos y se usa para interconectar un dispositivo de red a otro, habilitan transferencias de alta velocidad entre diferentes componentes de la red.

Los tipos de cableado que se podrían utilizar en la implementación en base a la topología de red, protocolos en uso y tamaño se detallan en la tabla 8.

Tabla 8. Comparación de cables UTP

Características	UTP cat. 5e	UTP cat. 6	UTP cat. 6a
Velocidad	100 Mbps	1000 Mbps	10000 Mbps
Distancia	Máximo 100 metros	Máximo 90 metros	Máximo 100 metros
Norma	ANSI/TIS/EIA-TSB-95	ANSI/TIA/EIA-568-B.2-1	ANSI/TIA/EIA-568-B.2-10
Otros	Ethernet 100Base-TX y 1000Base-T. Soporte Ethernet Gigabit.	Ethernet Gigabit.	Ethernet 10 Gigabit.
Costo	100,00 USD	150,00 USD	300,00 USD

Elaborado por: Alejandro Santamaría

La empresa Santanet utilizará el cable UTP categoría 6 marca Siemon certificado, debido a que su costo es económico a comparación de otros y la transferencia que provee va acorde a las necesidades del proyecto a implementar.

3.3.1.3 Servidor

El servidor es muy esencial debido a que se lo podría denominar como el jefe de la red, ya que establece los procedimientos de comunicación para las estaciones de trabajo y los recursos compartidos. Mediante este se mantendrá un rendimiento óptimo de la red para nuevos servicios y usuarios.

Tabla 9. Comparación de servidores

Características	HP Proliant MicroServer	Lenovo Thinkserver TS130	PC Clon
Tipo	Server	Server	Desktop
Procesador	Turion II Neo N40L	Xeon	Core i5
Memoria Cache	2Mb	2Mb	2Mb
Memoria	2Gb ECC	2Gb	2Gb
Disco Duro	500Gb SATA	500Gb SATA	500Gb SATA
Tarjeta de red	10/100/1000	10/100/1000	10/100/1000
Costo	500,00 USD	550,00 USD	700,00 USD

Elaborado por: Alejandro Santamaría

El servidor a utilizar para la respectiva implementación es el HP Proliant MicroServer debido a las características y al bajo costo. El motivo por el cual se utiliza un servidor es porque los servicios a configurar deben estar disponibles las 24 horas del día.

3.3.1.4 Estaciones de trabajo

En las estaciones de trabajo de la empresa Santanet se va a mantener tanto el hardware como el software en su estado actual debido a que disponen de varios sistemas operativos funcionales que sirven para las respectivas pruebas en la implementación.

Una de la estaciones de trabajo en la implementación se va a utilizar como router, debido que se necesita una estación básica de trabajo para instalar el software de ruteo.

3.3.2 Topología física

La topología física de una red define únicamente la distribución que interconecta las diferentes estaciones de trabajo. "A la hora de instalar una red, es importante seleccionar la topología más adecuada a las necesidades existentes" (Slideshare, 2013, pág. 5).

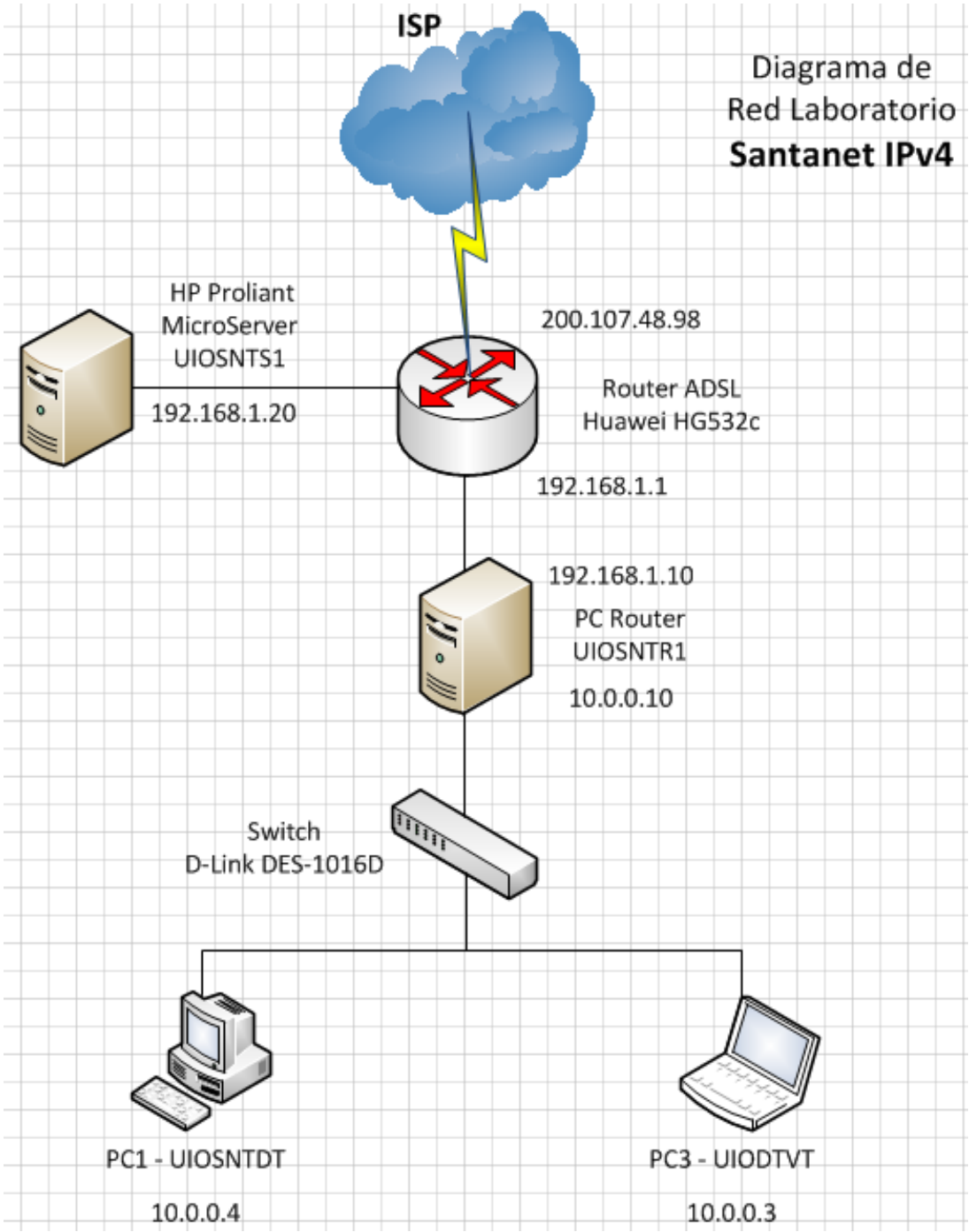
Hay una serie de factores a tener en cuenta a la hora de decidirse por una topología de red concreta, y éstas son:

- La distribución de los equipos a interconectar.
- El tipo de aplicaciones que se van a ejecutar.
- La inversión que se quiere hacer.
- El coste que se quiere dedicar al mantenimiento y actualización de la red local.
- El tráfico que va a soportar la red local.
- La capacidad de expansión. Se debe diseñar una intranet teniendo en cuenta la escalabilidad (Slideshare, 2013, pág. 5).

En la empresa Santanet se va a mantener la topología tipo estrella debido que se tiene un router ADSL al cual están conectadas todas las estaciones de trabajo y otros equipos de red. Al router ADSL se conectaran también equipos de red para el control y la administración.

La topología física que se implementara en la empresa Santanet se puede observar en la figura 25 en donde se detallan los equipos a utilizar y su respectiva ubicación.

Figura 25. Diagrama nuevo de red IPv4 de la empresa Santanet



Elaborado por: Alejandro Santamaría

3.4 Diseño lógico de la LAN

El diseño lógico de la LAN se basa en muchos factores como los tipos de aplicaciones, protocolos, distancia, utilización, estructura de acceso y topologías de redes anteriores.

La empresa Santanet actualmente cuenta con la topología lógica punto a multipunto, la cual se va a mantener debido que la infraestructura de la empresa dispone de varios dispositivos, esto implica que la comunicación es solamente entre el punto central hacia los remotos y viceversa.

3.4.1 Protocolos

La nueva versión del protocolo de Internet trae consigo asociados nuevos protocolos que específicamente funcionan en IPv6. Entre los principales protocolos se tiene:

- **DHCPv6**
- **ICMPv6**
- **IPsec**
- **NDP**
- **RIPng**
- **OSPFv3**
- **BGP4+**
- **EIGRP para IPv6**

3.4.2 Estrategias de migración de IPv4 a IPv6

La empresa Santanet para su migración a IPv6 utilizará mecanismos de tipo túnel, específicamente un túnel 6in4 que será provisto por Hurricane Electric, debido a que el proveedor de Internet CNT no asigna todavía direcciones IPv6 nativas.

Los usuarios home de CNT disponen de routers ADSL que soportan IPv6 pero todavía no llegan con el direccionamiento IPv6 hacia ellos.

Mediante el túnel 6in4 se podrá conectar una red IPv6 con otras redes IPv6 utilizando la infraestructura IPv4 existente.

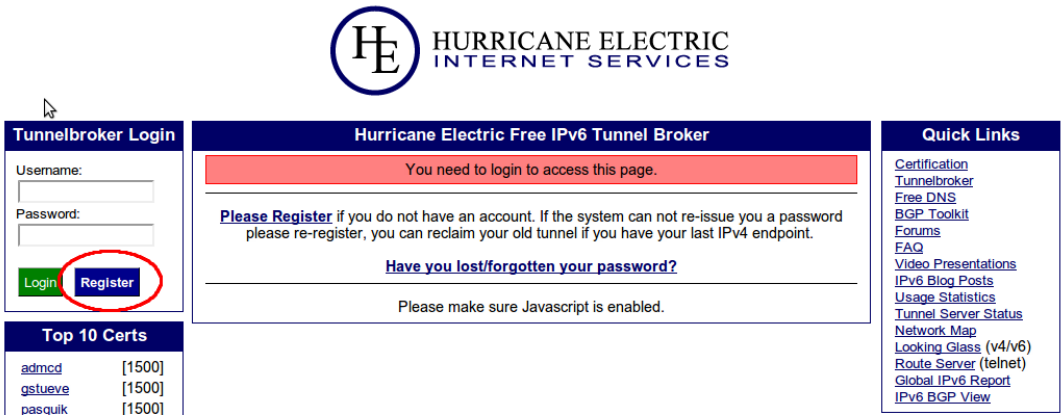
3.4.3 Túnel 6in4 con Hurricane Electric

Hurricane Electric es un backbone global en Internet (ISP), especializado en IPv6. Actualmente es el backbone más grande de IPv6 en el mundo, ofrece servicios gratuitos como un túnel 6in4 IPv6 que permite configurar túneles estáticos y BGP.

Procedimiento para crear un túnel IPv6 con Hurricane Electric:

1. Ingresar a la página de Hurricane Electric www.tunnelbroker.net y proceder a registrarse gratuitamente para poder crear el túnel.

Figura 26. Página inicial de Hurricane Electric

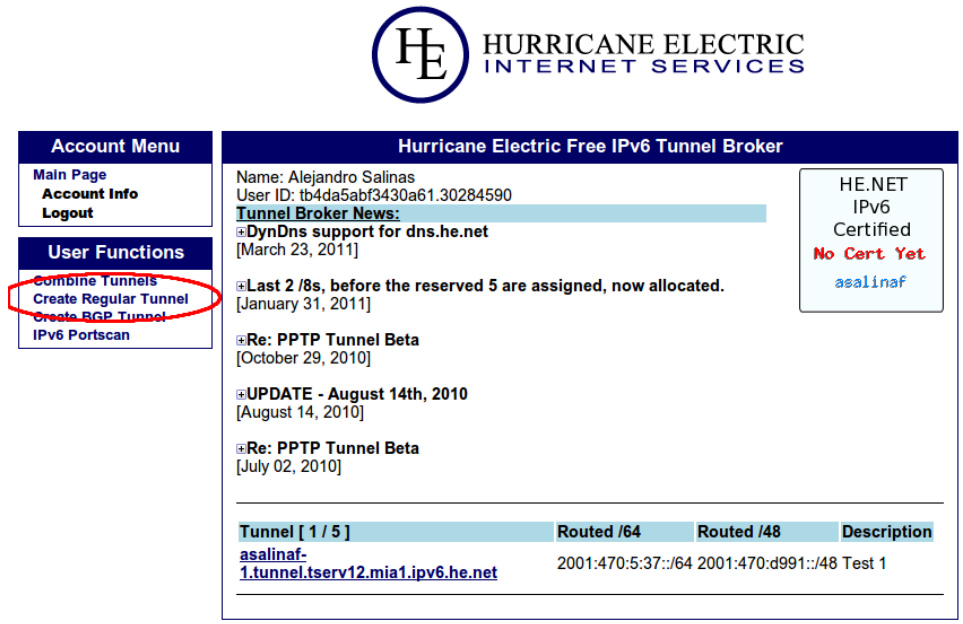


Elaborado por: Alejandro Santamaría

2. En el formulario de registro ingresar los datos respectivos y proceder a registrarse.

3. Al completar el registro en la página principal se procede a escoger la opción "Create Regular Tunnel".

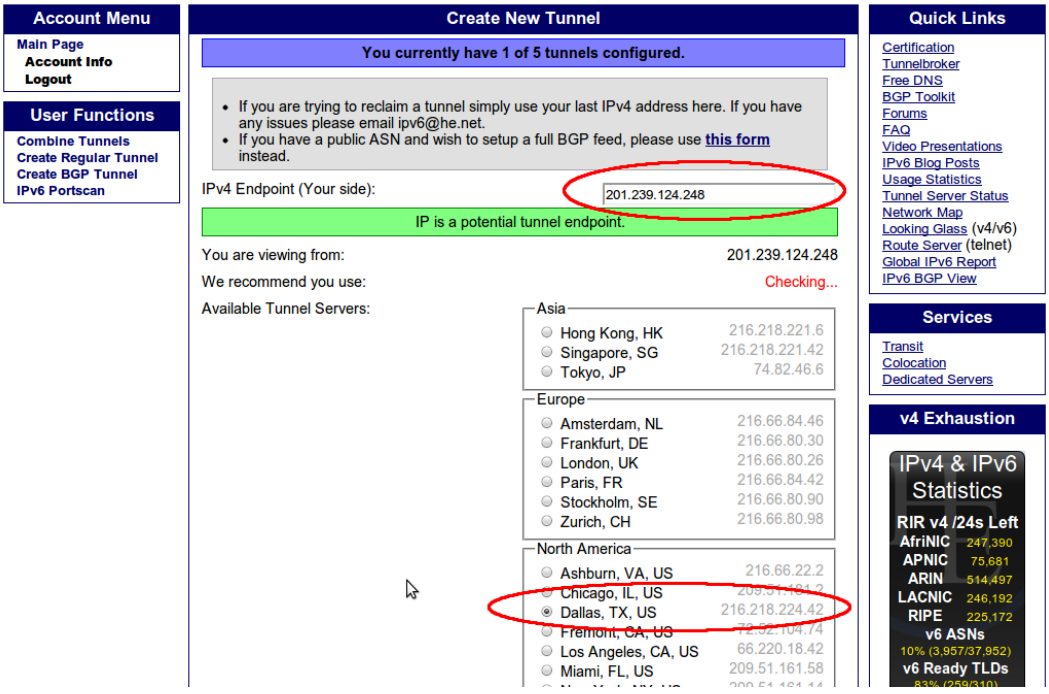
Figura 27. Página principal de Hurricane Electric



Elaborado por: Alejandro Santamaría

4. Para crear el nuevo túnel digitar la dirección IP pública, se puede observar que en la opción "You are viewing from:" se despliega nuestra IP pública actual y escoger el servidor de destino de preferencia ya que todos funcionan.

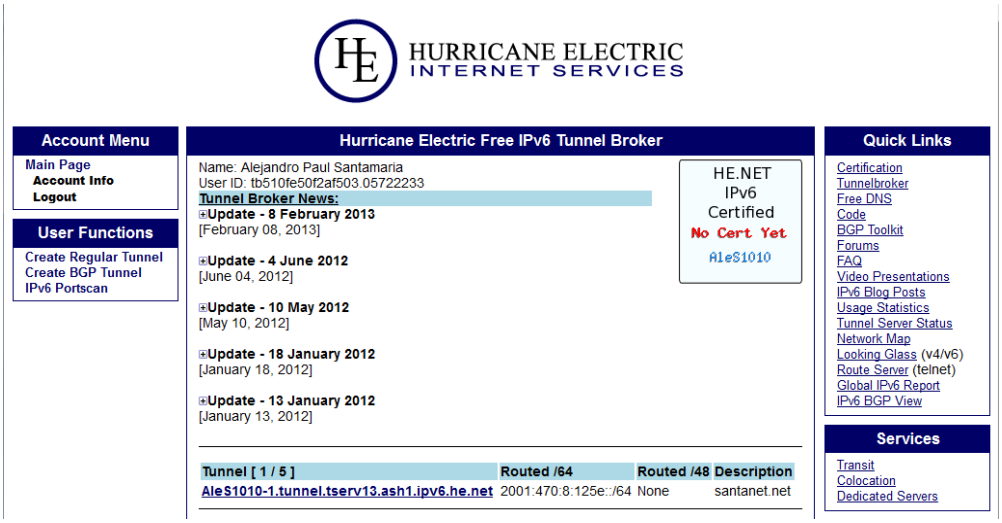
Figura 28. Creación del nuevo túnel 6in4



Elaborado por: Alejandro Santamaría

5. Finalmente al crear el túnel, en la página principal se puede observar que se encuentra creado el túnel.

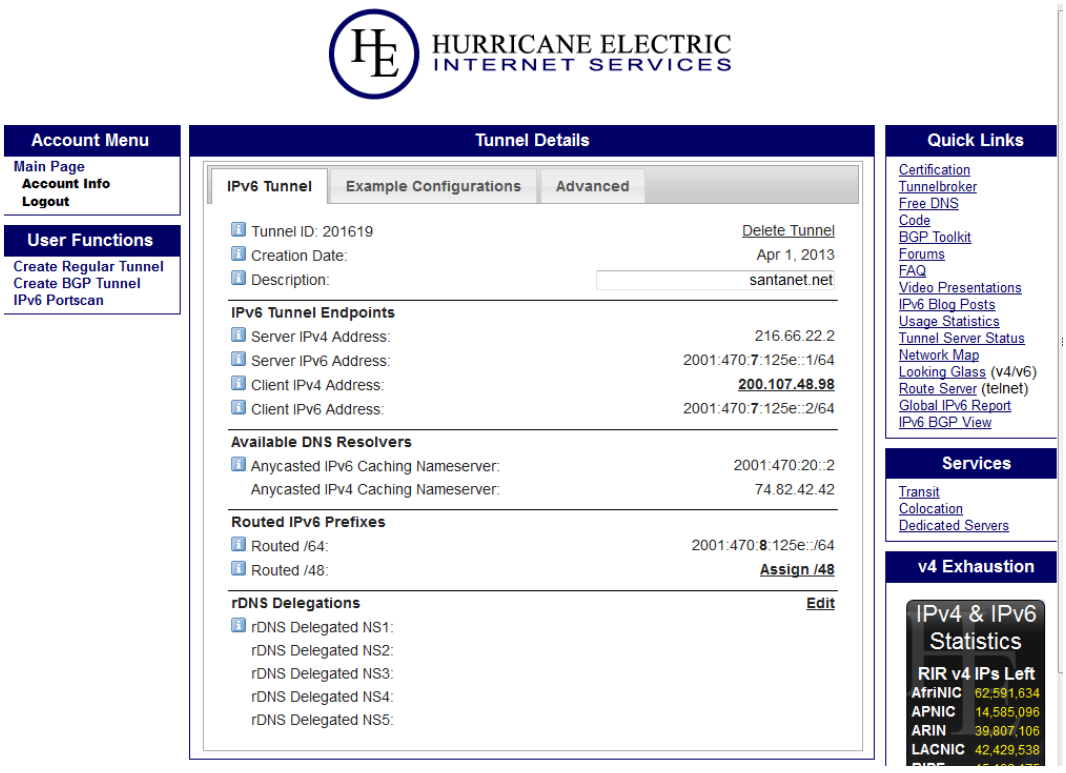
Figura 29. Página principal de Hurricane Electric



Elaborado por: Alejandro Santamaría

6. Seleccionar el túnel creado para poder observar los detalles del mismo.

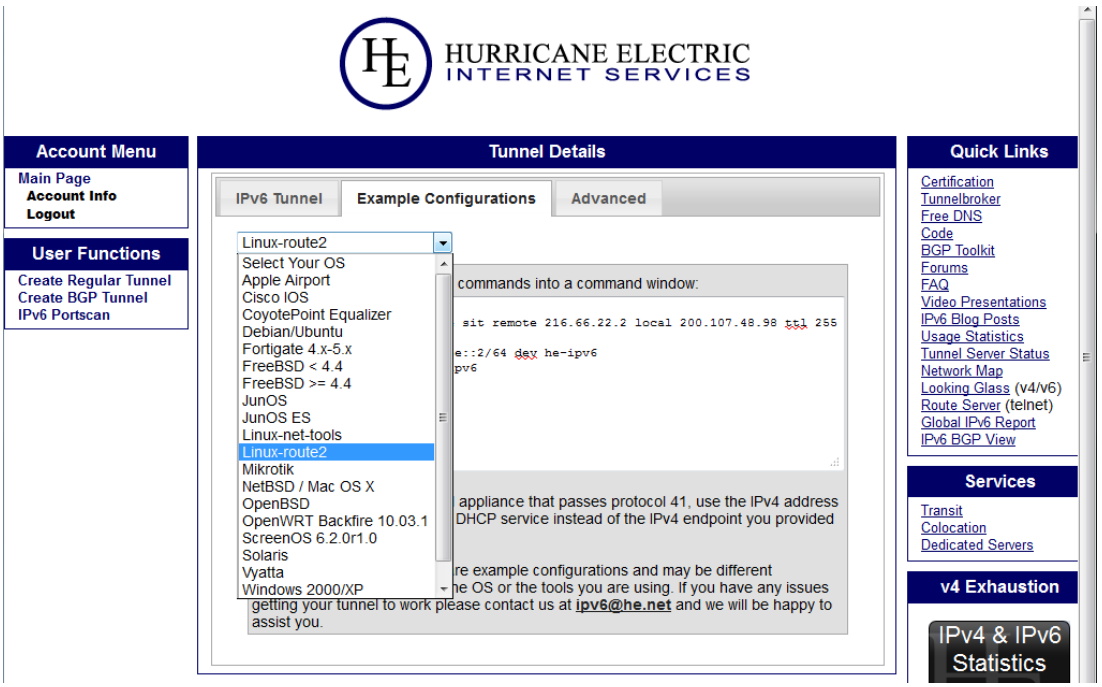
Figura 30. Detalles del túnel 6in4



Elaborado por: Alejandro Santamaría

7. En la pestaña Example Configurations se dispone de varios ejemplos de configuración para diferentes sistemas operativos y así poder crear el túnel deseado.

Figura 31. Ejemplos de configuración del túnel 6in4

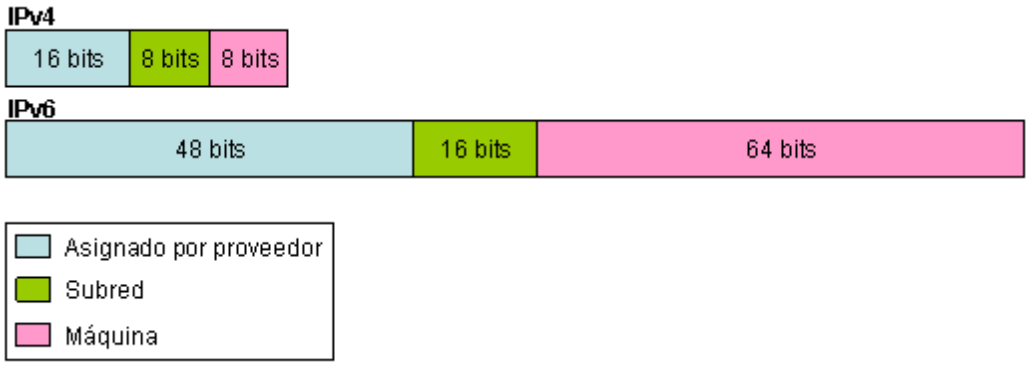


Elaborado por: Alejandro Santamaría

3.4.4 Direccionamiento IPv6

Una dirección IPv6 es una etiqueta numérica que sirve para identificar cada interfaz de red de una estación de trabajo o nodo de red. Tiene una estructura jerárquica más compleja:

Figura 32. Estructura de una dirección IPv6



Fuente: (El Mundo, 2013)

3.4.4.1 Tipos de direcciones IPv6

Las direcciones IPv6 se clasifican según las políticas de direccionamiento y encaminamiento:

- **Dirección Unicast (Uno a uno).** Esta dirección al igual que en IPv4 identifica un host. Sin embargo se tiene varias direcciones:

- Local Única. Similar a las antiguas direcciones privadas, en IPv6 se define como fc00::/7

- Global. Dirección que se pueden usar directamente en Internet.

- Enlace local. Similar a las direcciones APIPA de IPv4. Esta dirección es necesaria para el proceso de descubrimiento de vecinos localmente, se define como fe80::/10.

- Mapeada IPv4. Representa direcciones IPv4 en IPv6, la idea es facilitar a las aplicaciones el uso de IPv4 e IPv6 utilizando una única dirección, se define como ::ffff:172.144.52.58

- IP de Loopback. Conocida en IPv4 como 127.0.0.1 en IPv6 se define como ::1

- **Dirección Multicast (Uno a muchas).** Esta dirección identifica a varios adaptadores. Un paquete que se envía a esta dirección es receptado en todas las interfaces. Este tipo de dirección viene a mejorar las direcciones Broadcast de

IPv4 y son muy utilizadas para el streaming de video y audio. Se definen como ff00::/8 (Acosta, 2013)

- **Dirección Anycast (Uno a la más cercana).** Al igual que la dirección multicast identifica a varios adaptadores. Un paquete que se envía a una dirección anycast se entrega a la interfaz más cercana y esto depende de la topología y el protocolo de enrutamiento. Utiliza direcciones de Unicast. (Acosta, 2013)

Figura 33. Tipos de direcciones IPv6

TIPO DE DIRECCIÓN	INICIA CON:
•Multicast	1111 1111
•Unicast globales	001
•Unicast enlace local	1111 1110 10
•Sitio local (caducado)	1111 1110 11
•Compatible IPv4 (caducado)	0000 ... 0 (96 bits ceros)
•No especificada (por defecto)	000 ... 0 (todo cero)
•De loopback	000 ... 01 (127 ceros, un 1)
•Anycast	los mismos que unicast

Aproximadamente 7/8 del total de prefijos disponibles están reservados.

Fuente: (Mejía, 2013)

En la empresa Santanet se va a utilizar el tipo de direcciones IPv6: Unicast globales y Unicast de enlace local.

3.4.4.2 Representación

Entre las principales reglas de escritura se tiene:

- Se utiliza nomenclatura hexadecimal.
- Los ceros iniciales de cada grupo son opcionales.
- Ceros continuos puede reemplazarse por :: pero solo una vez por dirección.

- Se utiliza mayúsculas o minúsculas.

Ejemplo:

Dirección en su representación normal hexadecimal:

2001:0DB8:0000:0000:130F:0000:0000:140B

Dirección donde se reemplazar los ceros continuos por :: y se utiliza minúsculas:

2001:db8:0:0:130f::140b

Representación de los prefijos:

- Dirección IPv6/Tamaño del prefijo

  Dirección IPv6: Dirección IPv6 en cualquiera de las notaciones válidas.

  Tamaño del prefijo: Valor decimal indicando cuantos bits contiguos de la parte izquierda de la dirección componen el prefijo.

Ejemplo:

Prefijo	2001:db8:3003:2::/64
Prefijo Global	2001:db8::/32
ID de la subred	3003:2

URL:

Ejemplo:

http://[2001:12ff:0:4::22/index.html

http://[2001:12ff:0:4::22]:8080

3.4.4.3 Criterios de asignación

En las direcciones IPv6 el identificador de interfaz que tiene un tamaño de 64 bits puede asignarse de diversos métodos:

- Autoconfiguración Stateless con EUI-64
- Autoconfiguración Stateful asignadas mediante DHCPv6
- Auto-generados pseudo-aleatoriamente
- Configurado manualmente

Un nodo se puede identificar a través de cualquier dirección de sus interfaces:

- Loopback ::1
- Enlace local fe80:
- Global 2001:

3.4.4.4 Asignación de direcciones IPv6

A continuación se presenta como se va a asignar las direcciones IPv6 a los respectivos equipos a utilizar. Para el router y el servidor se va a asignar manualmente direcciones IPv6 fijas, mientras que para los equipos se va asignar mediante el servidor DHCPv6.

En la tabla 10 se detallan las direcciones IPv6 que provee el túnel 6in4 de Hurricane Electric y que se van a utilizar en la empresa Santanet.

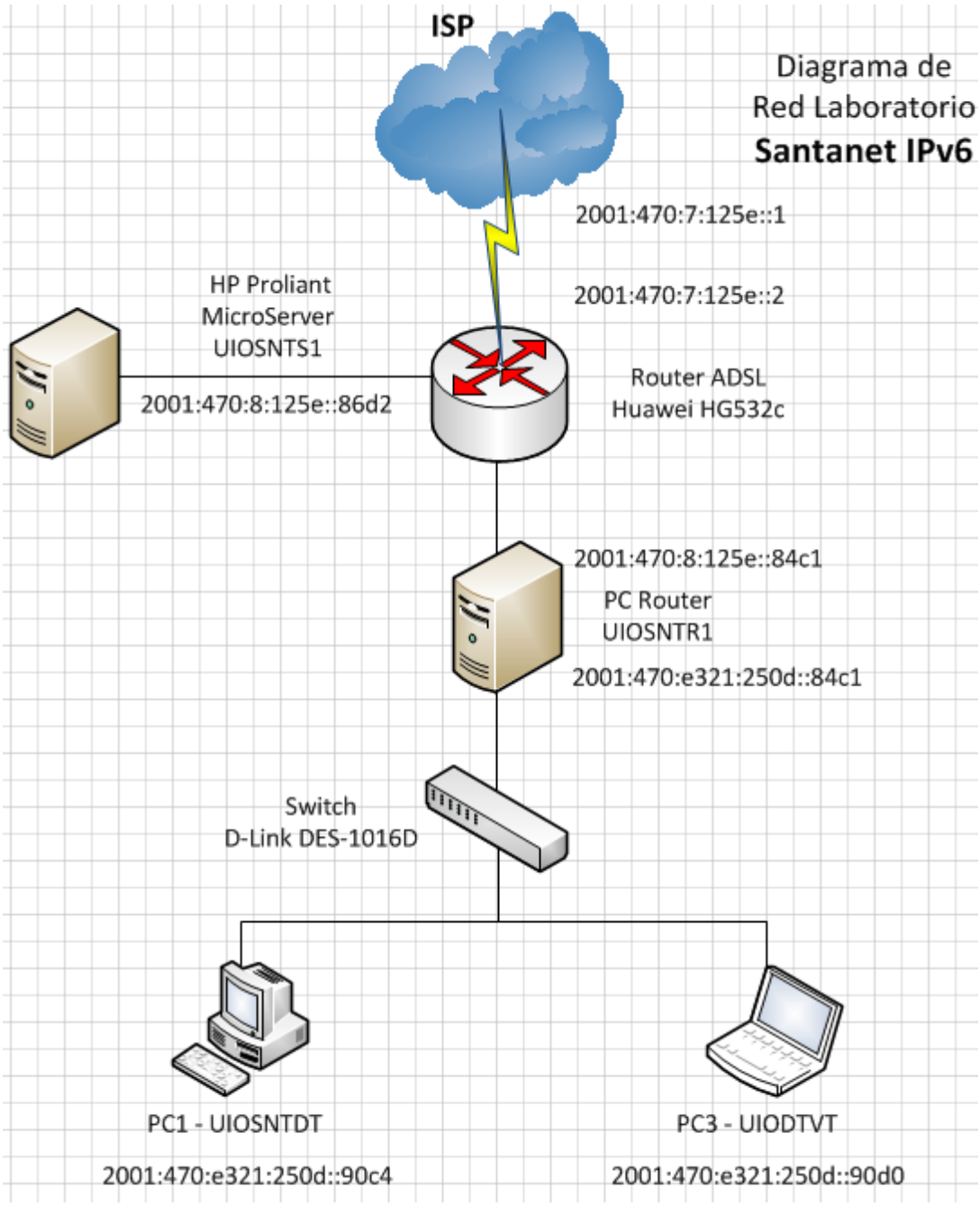
Tabla 10. Direccionamiento IPv4 e IPv6

Direccionamiento IP			
Descripción		**IPv4**	**IPv6**
IP Pública		200.107.48.98	
Server IPv4 Address		216.66.22.2	
Server IPv6 Address			2001:470:7:125e::1/64
Client IPv4 Address		200.107.48.98	
Client IPv6 Address			2001:470:7:125e::2/64
Anycasted IPv4 Caching Nameserver		74.82.42.42	
Anycasted IPv6 Caching Nameserver			2001:470:20::2
Routed /64			2001:470:8:125e::/64
Routed /48			2001:470:e321::/48
Estación de trabajo		**IPv4**	**Dirección IPv6 / Prefijo**
UIOSNTR1	Eth0	192.168.1.10	2001:470:8:125e::84c1/64

	Eth1	10.0.0.10	2001:470:e321:250d::84c1/64
UIOSNTS1	Eth0	192.168.1.20	2001:470:8:125e::86d2/64
UIOSNTDT	Eth0	10.0.0.4	2001:470:e321:250d::90c4/64
UIOSNTVT	Eth0	10.0.0.3	2001:470:e321:250d::90d0/64
Otros		10.0.0.100-200	2001:470:e321:250d::90d0-90ff/64

Elaborado por: Alejandro Santamaría

Figura 34. Diagrama nuevo de red IPv6 de la empresa Santanet



Elaborado por: Alejandro Santamaría

3.4.5 Plataforma a utilizar

3.4.5.1 NOS-Network Operating System

Una red de equipos no puede funcionar sin un sistema operativo de red, debido a que los equipos no pueden compartir recursos y los usuarios no pueden utilizar estos recursos. Un sistema operativo de red, debe estar en la capacidad de:

- Dar soporte para archivos: Crear, compartir, almacenar y recuperar archivos.
- Comunicaciones: Hace referencia a todo el tráfico de la red.
- Servicios para el soporte de equipo: Se habla de los servicios que estarán montados en la red.

Tabla 11. Características de software del servidor

NOS	CentOS	Microsoft Windows	Red Hat Enterprise
Tipo	Server	Server	Server
Versión	6.3	2008	6.2
Plataforma	32 y 64 bits	32 y 64 bits	64 bits
Licencia	Libre	Comercial	Comercial
Soporta IPv6	Si	Si	Si
Soporta QoS	Si	Si	Si
Costo	0,00 USD	782,00 USD	350,00 USD

Elaborado por: Alejandro Santamaría

El sistema operativo de red que se procederá a instalar en el servidor HP Proliant MicroServer es CentOS 6.3 debido a su costo y características.

3.4.5.2 Sistema Operativo de las estaciones de trabajo

El sistema operativo de una de las estaciones de trabajo de la empresa Santanet se va a cambiar por una distribución de Linux, ya que en esta estación se va a instalar el software de conectividad o ruteo.

En las otras estaciones de trabajo el sistema operativo se va a mantener, ya que disponen de varias versiones y en cada una de estas se realizará las respectivas pruebas con IPv6.

3.4.5.3 Software de conectividad

La mayoría de redes utiliza costosos routers físicos, pero la potencia de las estaciones de trabajo ha avanzado hasta el punto que no se necesita comprar uno de estos, las plataformas informáticas reemplazan estos routers físicos por software de enrutamiento.

Tabla 12. Características de software de conectividad

Detalle	Zebra	BIRD	Quagga
Tipo	Ruteo	Ruteo	Ruteo
Versión	6.3	1.3.8	0.99.22
Licencia	Libre	Libre	Libre
Protocolos	RIPv1, RIPv2, OSPF, BGP.	BGP, RIP, OSPF.	RIPv1, RIPv2, RIPng, OSPFv2, OSPFv3, BGP-4 y BGP-4+

Elaborado por: Alejandro Santamaría

"El software de conectividad que se utilizará en la implementación será el Quagga ya que proporciona encaminamiento basado en servicios de TCP/IP con protocolos de encaminamiento que soportan RIPv1, RIPv2, RIPng, OSPFv2, OSPFv3, BGP-4 y BGP-4+" (Collado & Juliá, 2013). Además de los protocolos de encaminamiento tradicionales basados en IPv4, Quagga también soporta protocolos de encaminamiento basados en IPv6.

"Se eligió Quagga ya que el desarrollo por zebra.org de Zebra se ha ralentizado. Mucho trabajo ha sido realizado por terceras personas para intentar mantener libre de bugs el código actual de Zebra, como resultado del cual es la bifurcación de Zebra llamada Quagga" (Collado & Juliá, 2013).

3.5 Diseño de QoS en la LAN con IPv6

Al implementar QoS en la red de la empresa Santanet se logra un rendimiento más predecible y una utilización de ancho de banda más eficiente.

Para la respectiva implementación de QoS en la LAN con IPv6 se debe tener en cuenta:

- Conocer que aplicaciones necesitan QoS.

- Comprender las características de las aplicaciones para definir que herramientas de QoS se van a implementar.
- Definir clases de tráfico.
- Definir y configurar políticas de tráfico.
- Aplicar las políticas de tráfico a las interfaces.

Se detalla la implementación de QoS en la página 153.

3.6 Establecimiento de costos para la implementación de una red con tecnología IPv6

En la tabla 13 se detalla los costos promedio de los equipos adicionales que se necesita adquirir para la respectiva implementación de este proyecto.

Tabla 13. Costos de implementación

Equipo	Precio
Router	
Router PC Quagga	0,00 USD
Switch	
Switch D-Link DES-1016D	50,00 USD
Cableado	
UTP categoría 6	150,00 USD
Servidor	
HP Proliant MicroServer	500,00 USD
Direccionamiento	
IP pública	10,00 USD
NOS	
CentOS	0,00 USD
TOTAL	**710,00 USD**

Elaborado por: Alejandro Santamaría

En este capítulo se realizó el análisis del hardware y software que dispone la empresa Santanet, así como también se realizó comparaciones entre varios equipos y aplicaciones.

Para la respectiva implementación se realizó el diseño físico y lógico que se van a utilizar en la implementación de este proyecto, se tomará en cuenta tanto las prestaciones de los equipos existentes y también de los equipos nuevos.

CAPÍTULO 4
IMPLEMENTACIÓN Y PRUEBAS DE LA LAN CON IPv6 Y QoS

4.1 Instalación del Software

A continuación se detalla el proceso realizado en la instalación de los respectivos programas anteriormente analizados y seleccionados para implementar en este proyecto. Las direcciones IPv6 que a continuación se detallan usan el prefijo de documentación 2001:db8::/32.

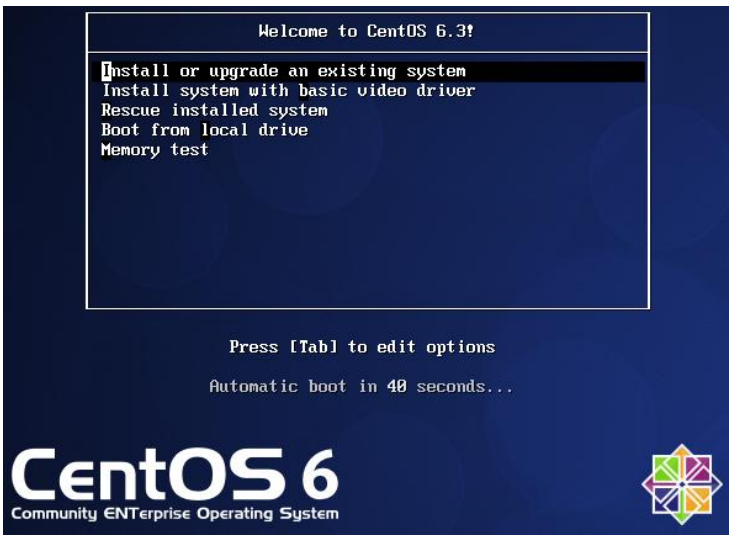
4.1.1 Instalación del sistema operativo

En la respectiva implementación de la red prototipo con el protocolo IPv6 se instalará el sistema operativo CentOS versión 6.3 tanto en el servidor como en el PC router.

Pasos para realizar la instalación del sistema operativo CentOS:

1. Descargar la imagen del CentOS, grabar la imagen en un dispositivo de almacenamiento y luego bootear desde el dispositivo de almacenamiento para comenzar la instalación:

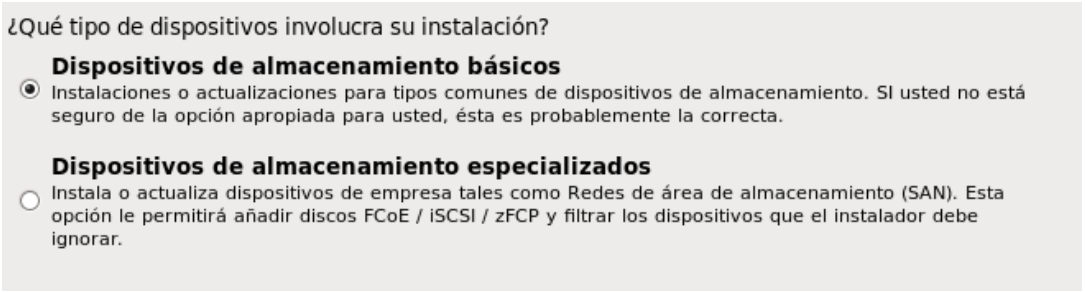
Figura 35. Pantalla inicial de CentOS



Elaborado por: Alejandro Santamaría

2. Escoger los tipos de dispositivos a instalar.

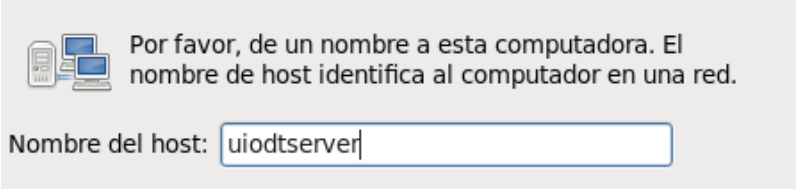
Figura 36. Dispositivos involucrados en la instalación



Elaborado por: Alejandro Santamaría

3. Digitar el nombre que le va identificar al servidor.

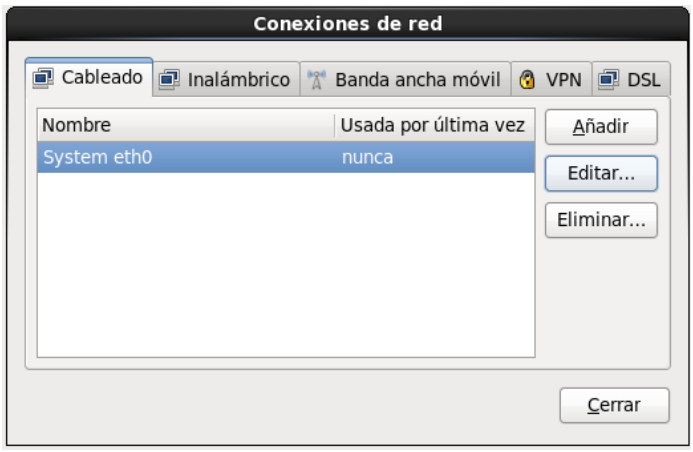
Figura 37. Nombre del host



Elaborado por: Alejandro Santamaría

4. Escoger en la misma pantalla conexiones de red y luego la pestaña de cableado.

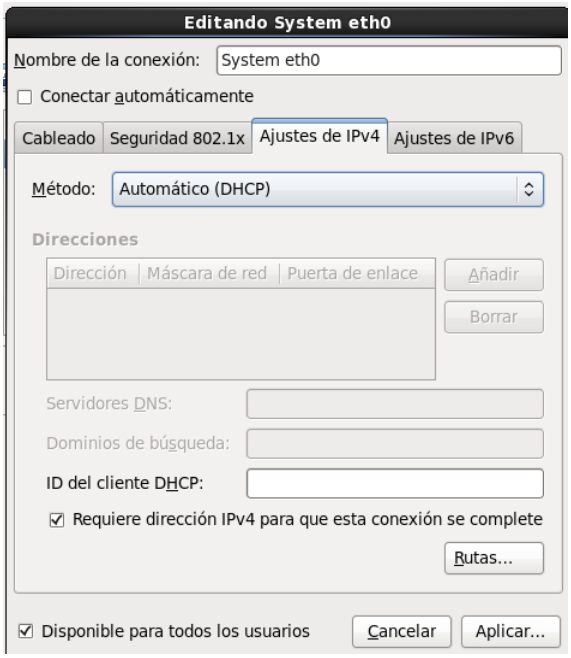
Figura 38. Conexiones de red



Elaborado por: Alejandro Santamaría

5. En la pestaña ajustes de IPv4 escoger la opción automático.

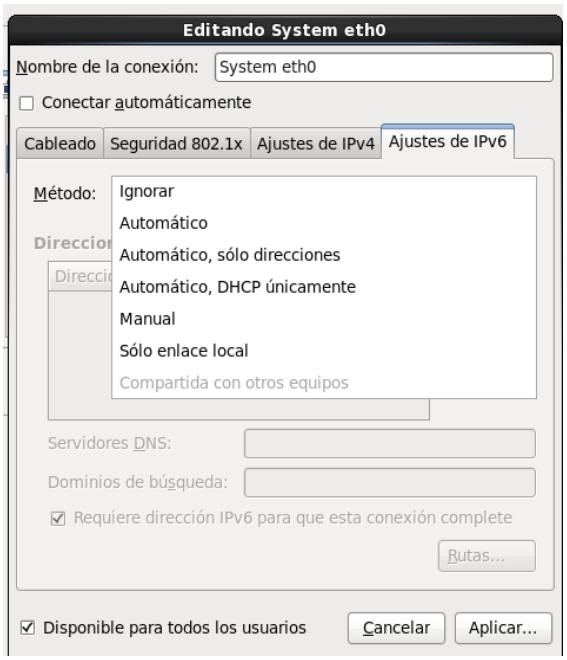
Figura 39. Ajustes de IPv4



Elaborado por: Alejandro Santamaría

6. En la pestaña de ajustes de IPv6 escoger automático.

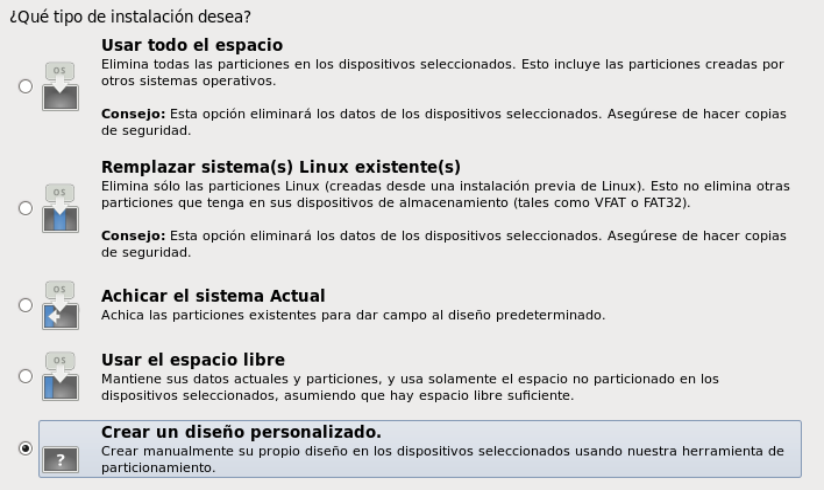
Figura 40. Ajustes de IPv6



Elaborado por: Alejandro Santamaría

7. Escoger la opción crear un diseño personalizado para realizar las respectivas particiones.

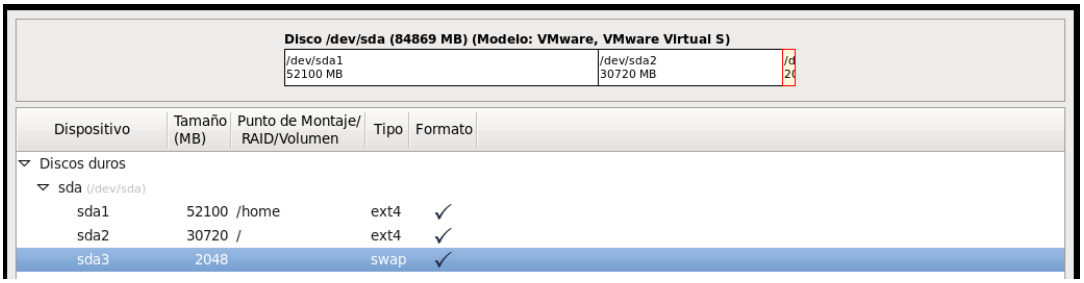
Figura 41. Tipo de instalación de CentOS



Elaborado por: Alejandro Santamaría

8. Crear una partición tipo ext4 para el directorio raíz y también para el directorio home. Asignar 2048Mb para la partición tipo swap, ya que mediante esta se puede ampliar de forma virtual la memoria.

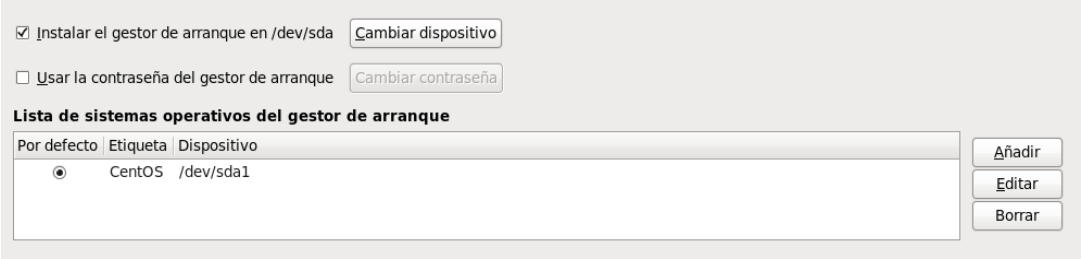
Figura 42. Particiones del disco duro



Elaborado por: Alejandro Santamaría

9. Instalar el gestor de arranque en el disco en el cual se crearon las particiones.

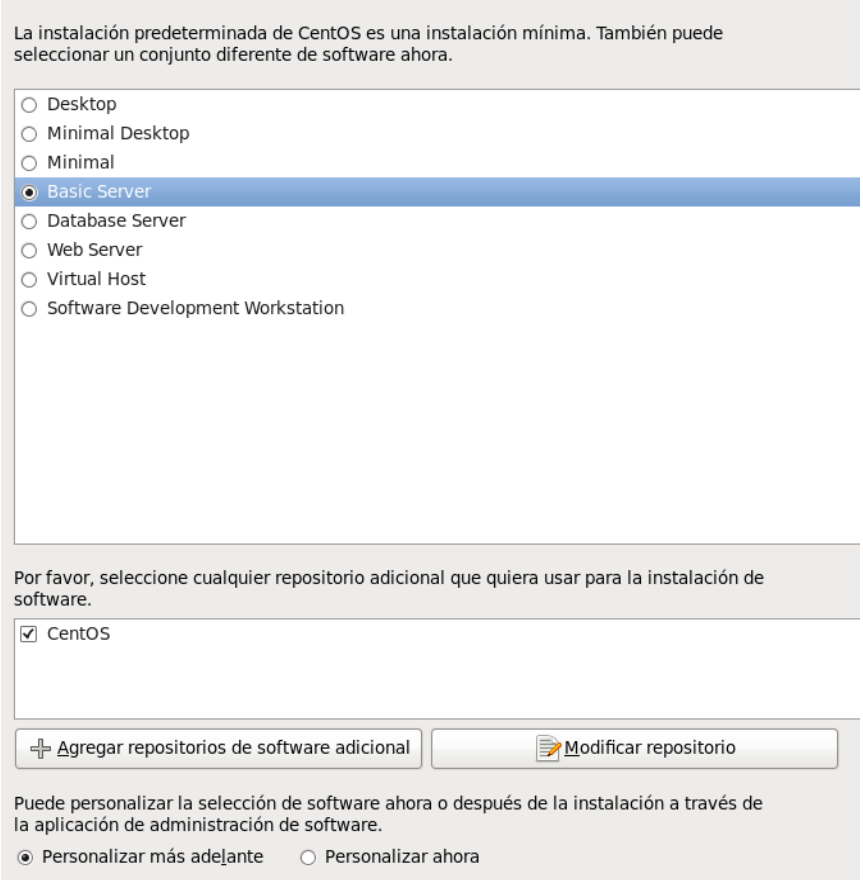
Figura 43. Gestor de arranque de CentOS



Elaborado por: Alejandro Santamaría

10. Seleccionar el tipo de instalación deseado. Se puede seleccionar Desktop para modo gráfico o Basic Server para modo consola.

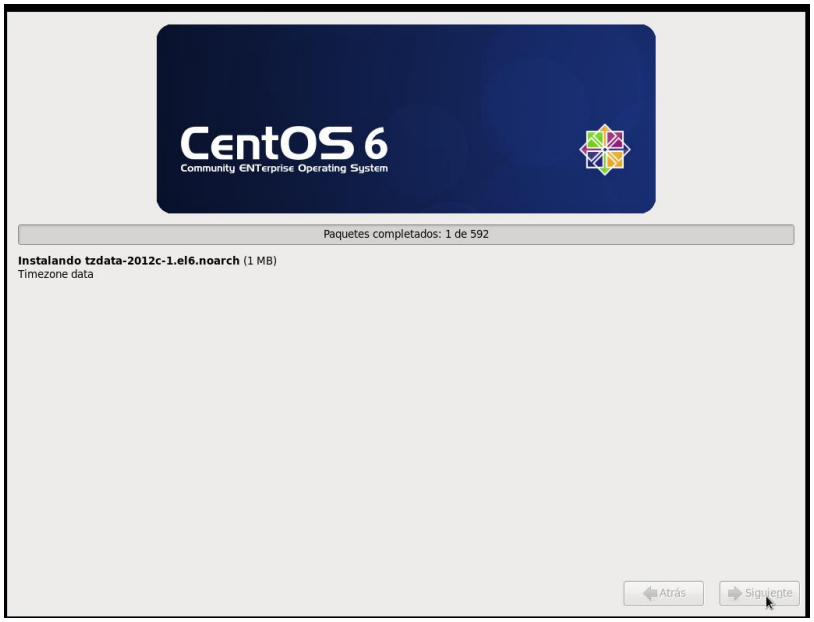
Figura 44. Tipo de instalación de CentOS



Elaborado por: Alejandro Santamaría

11. Una vez seleccionado el tipo de instalación se procede a instalar todos los paquetes seleccionados.

Figura 45. Instalación CentOS



Elaborado por: Alejandro Santamaría

12. Ingresar el nombre del usuario a crear, este usuario es de uso normal no administrativo.

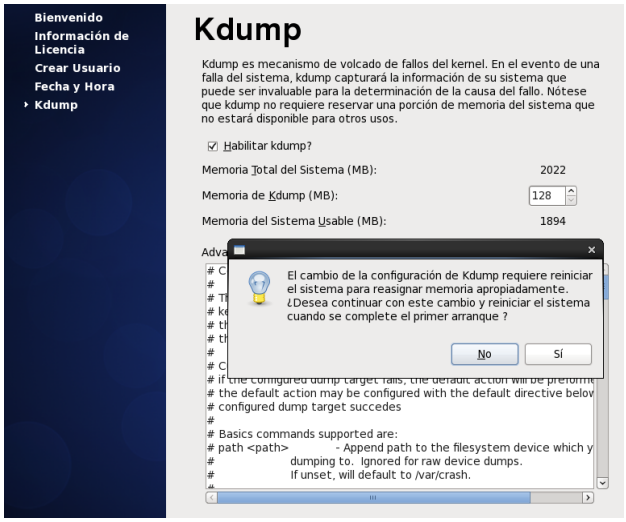
Figura 46. Crear usuario

Elaborado por: Alejandro Santamaría

13. En la última opción solicita habilitar o no Kdump, este es un mecanismo de volcado de fallos del kernel en caso de fallo, se encargará de recopilar la

información del sistema para poder evaluar el fallo. Al habilitar esta opción mantener los valores por defecto de la cantidad de memoria.

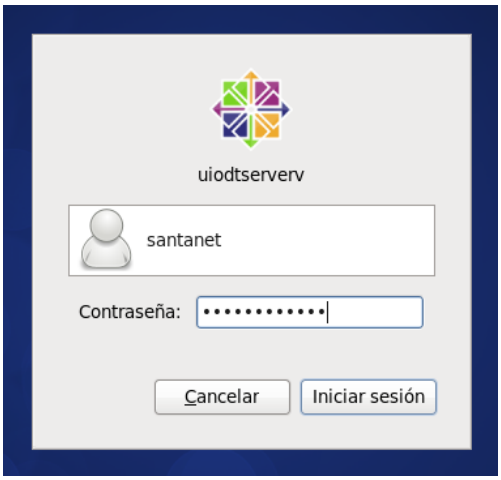
Figura 47. Kdump



Elaborado por: Alejandro Santamaría

14. Finalmente se ve la pantalla de inicio de CentOS.

Figura 48. Inicio de CentOS



Elaborado por: Alejandro Santamaría

4.1.2 Instalación del software de conectividad

El software de conectividad que se utilizará será el Quagga 0.99.22 que es la versión estable por el momento. A continuación se detallan los pasos para su instalación:

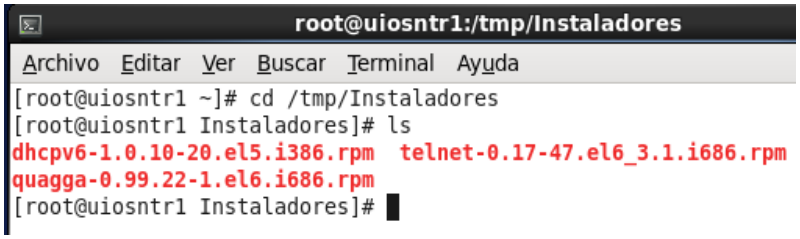
1. Descargar el RPM-Red Hat Package Manager- (Administración de Paquetes de Red Hat) de la página http://pkgs.org/download/quagga
2. Copiar el archivo quagga-0.99.22-1.el6.i686.rpm en la dirección deseada.

Figura 49. Quagga 0.99.22-1

Elaborado por: Alejandro Santamaría

3. Ejecutar el terminal de Linux como administrador o root.
4. Acceder al directorio en donde se encuentra copiado el archivo de instalación.

Figura 50. Directorio del archivo de instalación del Quagga

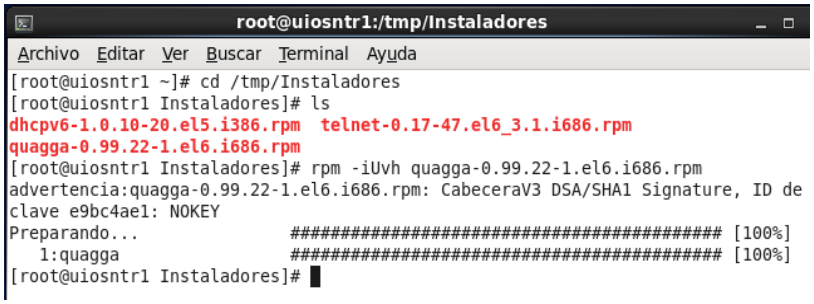


Elaborado por: Alejandro Santamaría

5. Una vez en el directorio del instalador para proceder a instalar se digita:

   #rpm –iUvh quagga-0.99.22-1.el6.i686.rpm

Figura 51. Instalación del Quagga



Elaborado por: Alejandro Santamaría

6. Finaliza la instalación si el proceso llega al 100%.
7. Se procede a iniciar el servicio zebra mediante el siguiente comando:

   #service zebra start

8. Si se desea que el servicio se ejecute cada vez que se inicia la máquina se digita:

   #chkconfig --level 35 zebra on

4.2 Instalación y configuración del protocolo IPv6

La mayoría de los sistemas operativos desde el año 2001 aproximadamente, tienen soporte de IPv6. En diversas plataformas o sistemas operativos el protocolo IPv6 viene por defecto ya activado sin intervención del usuario.

4.2.1 Windows XP

En Windows XP SP2 se podría decir que ya está instalado el protocolo IPv6 y por lo tanto solamente se debería activar.

4.2.1.1 Línea de comandos

En el sistema operativo Windows para configurar mediante línea de comandos se utiliza **netsh**.

Entre los principales comandos a utilizar para direcciones IPv6 son:

- Add. Añade la dirección de red a la interfaz indicada.

netsh interface ipv6 add address <interface> <ipv6address>

- Show. Verifica la dirección de red ingresada en la interfaz.

netsh interface ipv6 show address <interface>

- Set. Modifica las variables de la dirección de red ingresada.

netsh interface ipv6 set address <interface> <ipv6address>

- Delete. Borra la dirección de red ingresada

netsh interface ipv6 delete address <interface> <ipv6address>

Los principales comandos a utilizar para asignar DNS en IPv6 son:

- Add. Añade la dirección de DNS a la interfaz indicada.

netsh interface ipv6 add dnsserver <interface> <ipv6address> <index>

- Show. Verifica la dirección de DNS.

netsh interface ipv6 show dnsserver

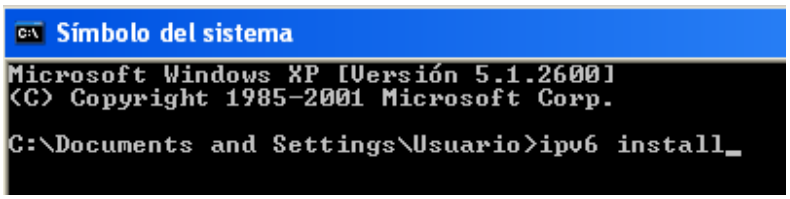
- Delete. Borra la dirección de DNS ingresada

netsh interface ipv6 delete dnsserver <interface> <ipv6address>

Para la respectiva activación del protocolo IPv6 mediante la línea de comandos se debería seguir los siguientes pasos:

1. Abrir el símbolo del sistema.
2. Digitar **ipv6 install.**

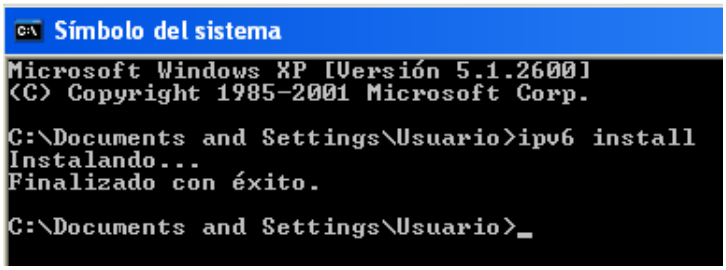
Figura 52. Activación del protocolo IPv6



Elaborado por: Alejandro Santamaría

3. Finaliza el proceso del protocolo IPv6.

Figura 53. Final de instalación del protocolo IPv6



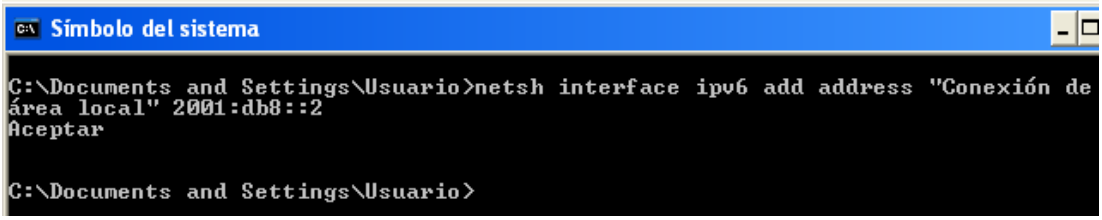
Elaborado por: Alejandro Santamaría

4. Se procede a asignar la dirección IPv6 determinada mediante el comando

   netsh interface ipv6 add address <interface> <ipv6address>

   netsh interface ipv6 add address "Conexión de área local" 2001:db8::2

Figura 54. Asignar IPv6 con el nombre de la interfaz

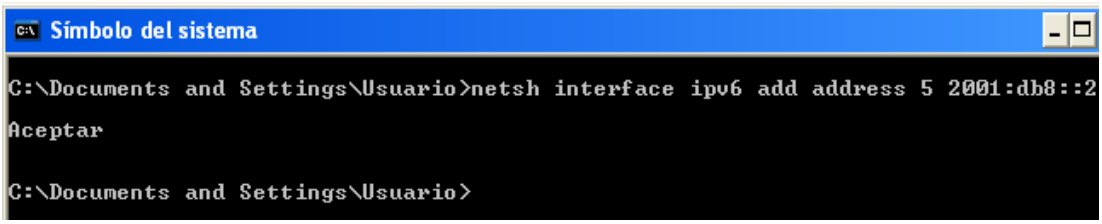


Elaborado por: Alejandro Santamaría

También se puede usar el ID de la interfaz para no utilizar el nombre de la conexión.

netsh interface ipv6 add address 5 2001:db8::2

Figura 55. Asignar IPv6 con el ID de la interfaz

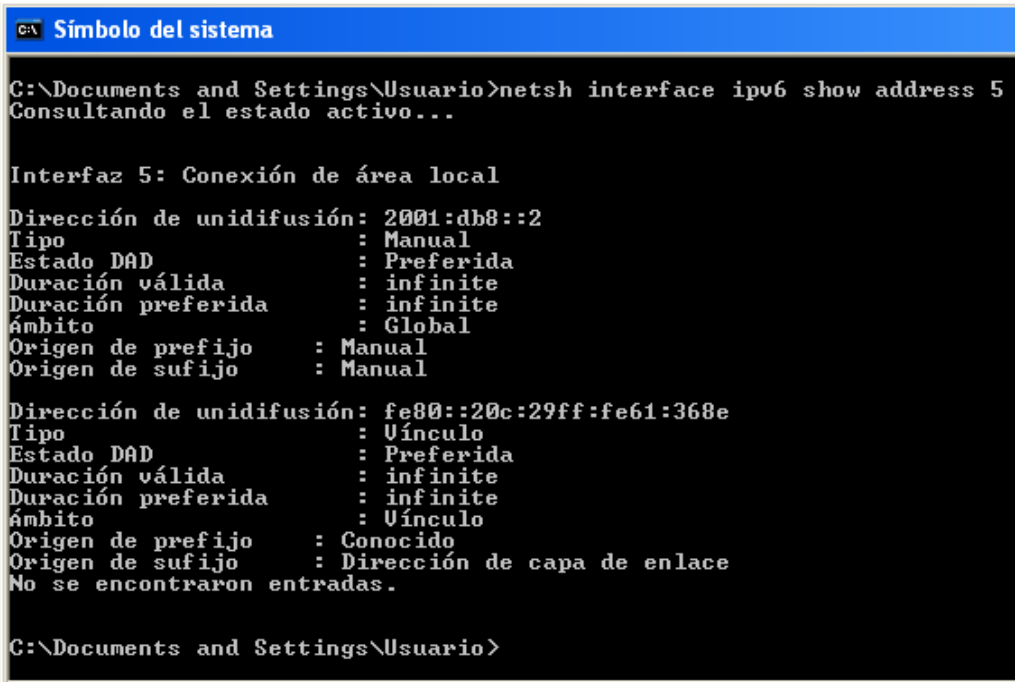


Elaborado por: Alejandro Santamaría

5. Revisar la configuración con el comando:

   netsh interface ipv6 show address 5 asumiendo que es la interfaz es 5.

Figura 56. Interfaz 5 o conexión de área local



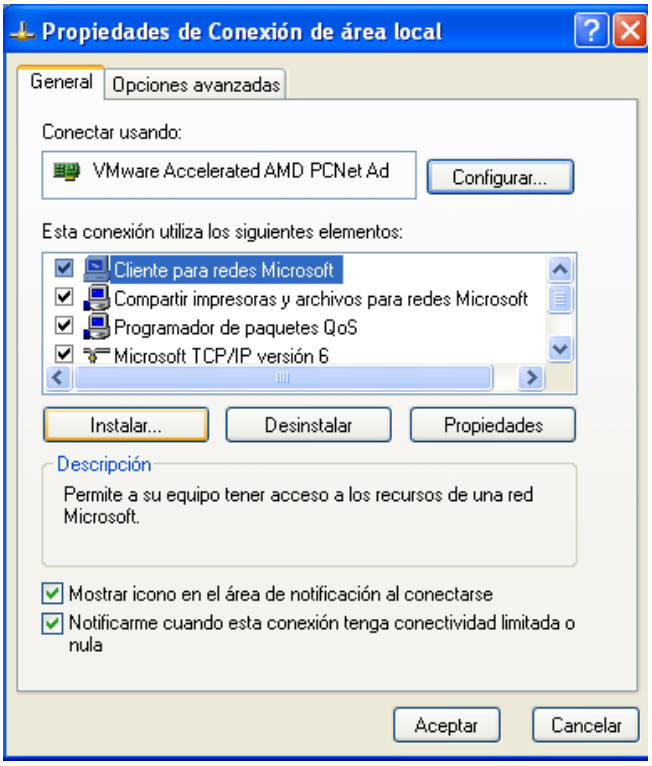
Elaborado por: Alejandro Santamaría

4.2.1.2 Interfaz gráfica

Para la respectiva activación mediante la interfaz gráfica de Windows se procede:

1. Seleccionar propiedad en Mis sitios de red.
2. Seleccionar propiedades en Conexión de área local.
3. Escoger la opción Instalar de la ventana de propiedades.

Figura 57. Propiedades de conexión de área local



Elaborado por: Alejandro Santamaría

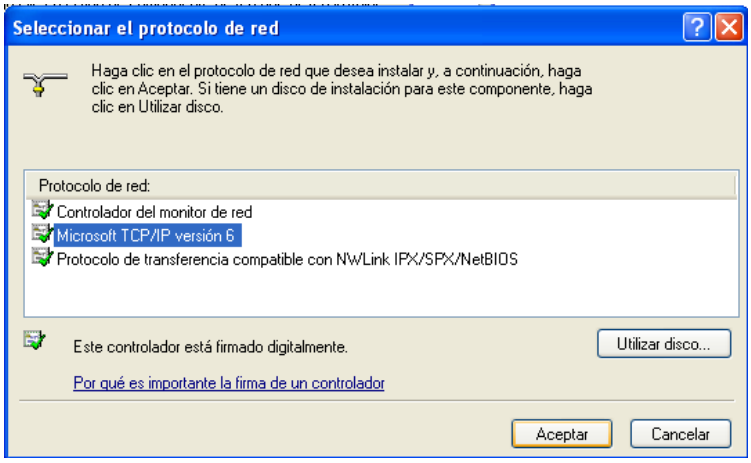
4. Seleccionar la opción protocolo.

Figura 58. Tipo de componente de red

Elaborado por: Alejandro Santamaría

5. Escoger Microsoft TCP/IP versión 6 y seleccionar Aceptar.

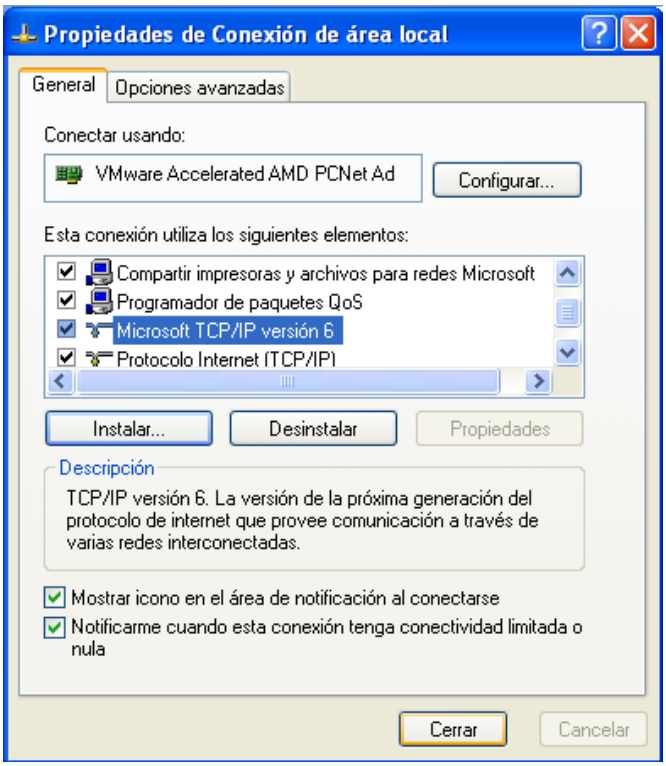
Figura 59. Protocolo de red



Elaborado por: Alejandro Santamaría

6. Verificar que se encuentre añadido el protocolo IPv6.

Figura 60. Propiedades de conexión de área local



Elaborado por: Alejandro Santamaría

7. La configuración del protocolo IPv6 en el SO Windows XP no se puede realizar de forma gráfica, solamente mediante comandos.

4.2.2 Windows 7

En Windows 7 por defecto el protocolo IPv6 ya viene instalado, así que lo único que se debería de revisar es que se encuentre habilitado el protocolo.

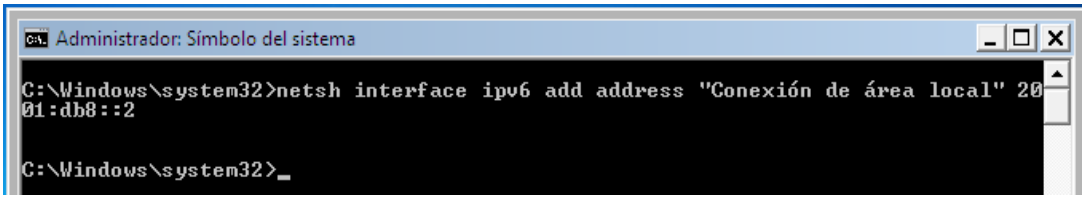
4.2.2.1 Línea de comandos

Para configurar una dirección IPv6 en una conexión de red mediante comandos de Windows 7 se debe realizar los siguientes pasos como Administrador:

1. Abrir el símbolo del sistema.
2. Para añadir una dirección IPv6 a la interfaz conexión de área local se puede digitar:

   netsh interface ipv6 add address “Conexión de área local” 2001:db8::2

Figura 61. Añadir dirección IPv6 con nombre la interfaz

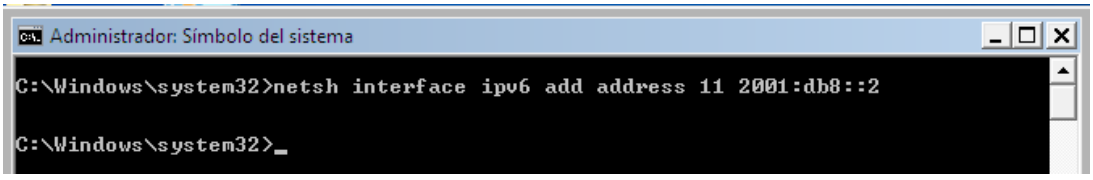


Elaborado por: Alejandro Santamaría

También se puede usar el ID de la interfaz para no utilizar el nombre de la conexión.

netsh interface ipv6 add address 11 2001:db8::2

Figura 62. Añadir dirección IPv6 con ID de la interfaz

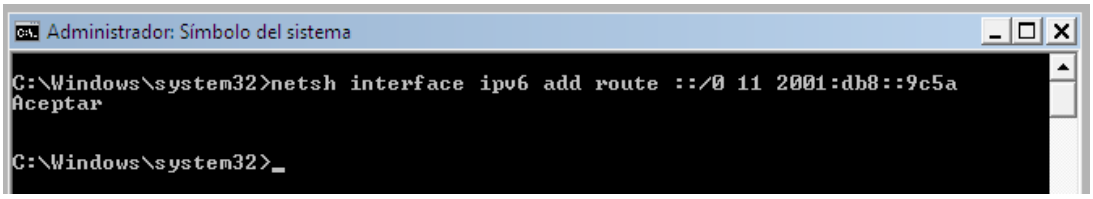


Elaborado por: Alejandro Santamaría

3. Para configurar un Gateway por defecto con una dirección IPv6 se puede añadir una ruta por defecto con la dirección específica del siguiente salto.

netsh interface ipv6 add route ::/0 11 2001:db8::9c5a

Figura 63. Gateway por defecto

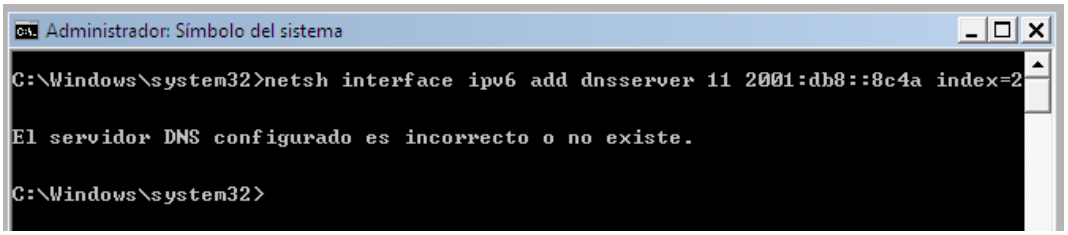


Elaborado por: Alejandro Santamaría

4. Para configurar un servidor DNS IPv6 como servidor DNS alternativo en la lista de servidores DNS para la conexión de área local se procede a digitar:

   netsh interface ipv6 add dnsserver 11 2001:db8::8c4a index=2

Figura 64. Servidor DNS

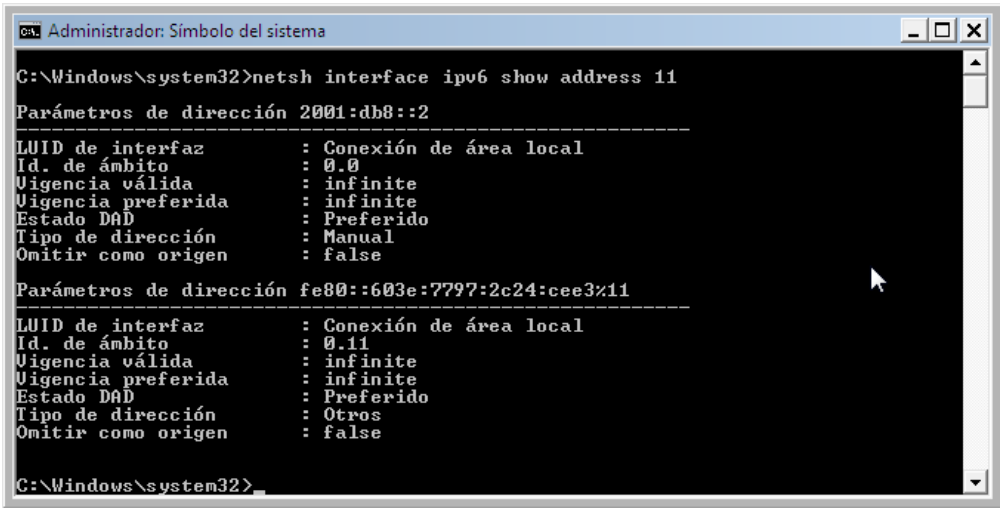


Elaborado por: Alejandro Santamaría

5. Y finalmente para verificar la configuración se puede digitar:

   netsh interface ipv6 show address 11

Figura 65. Configuración de la ID de la interfaz



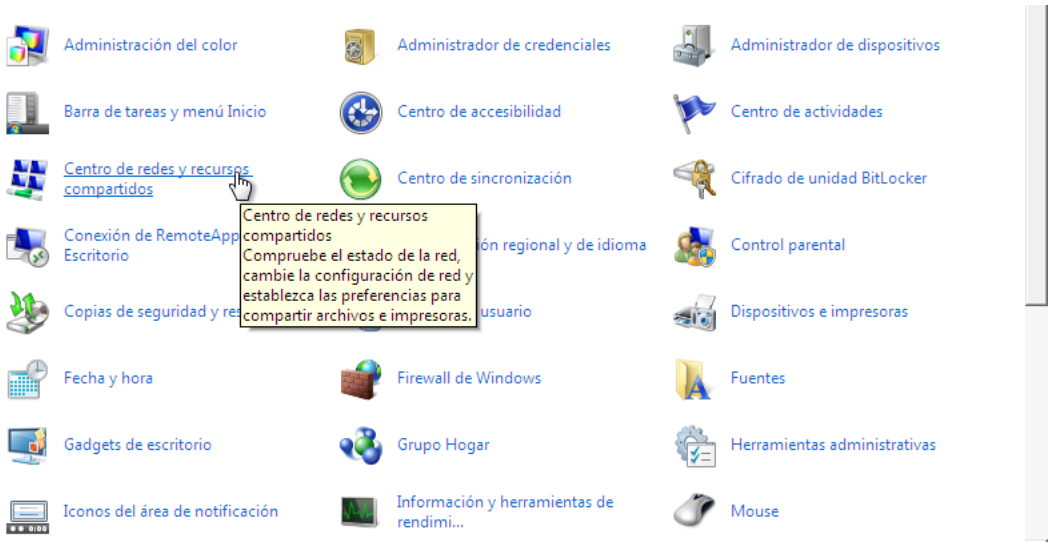
Elaborado por: Alejandro Santamaría

4.2.2.2 Interfaz gráfica

En Windows Vista/7 ya se dispone de una interfaz gráfica para poder configurar direcciones IPv6 manualmente o automáticamente, para lo cual se puede seguir los siguientes pasos.

1. Abrir panel de control del menú inicio.
2. Seleccionar Centro de redes y recursos compartidos.

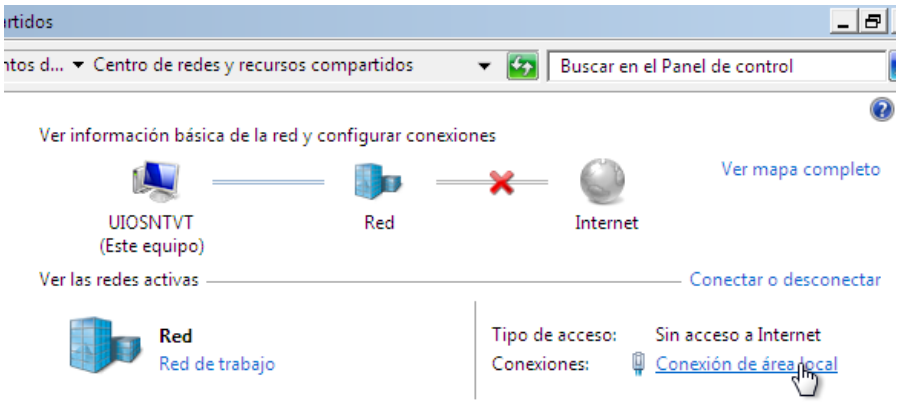
Figura 66. Panel de control



Elaborado por: Alejandro Santamaría

3. Escoger en el panel Conexión de área local.

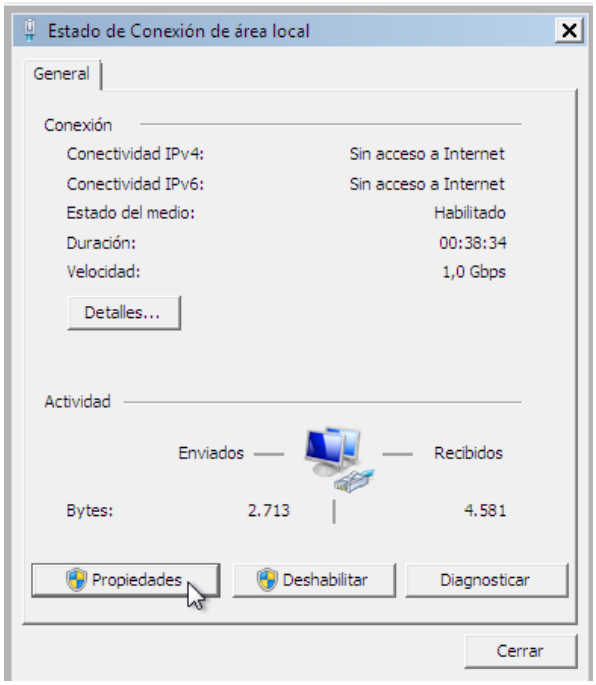
Figura 67. Conexión de área local



Elaborado por: Alejandro Santamaría

4. Seleccionar Propiedades en el estado de la conexión de red.

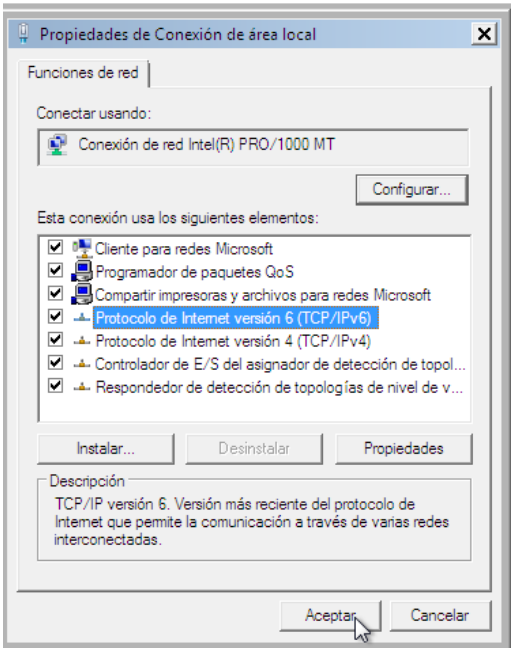
Figura 68. Estado de conexión de área local



Elaborado por: Alejandro Santamaría

5. Escoger Protocolo de Internet versión 6 (TCP/IPv6).

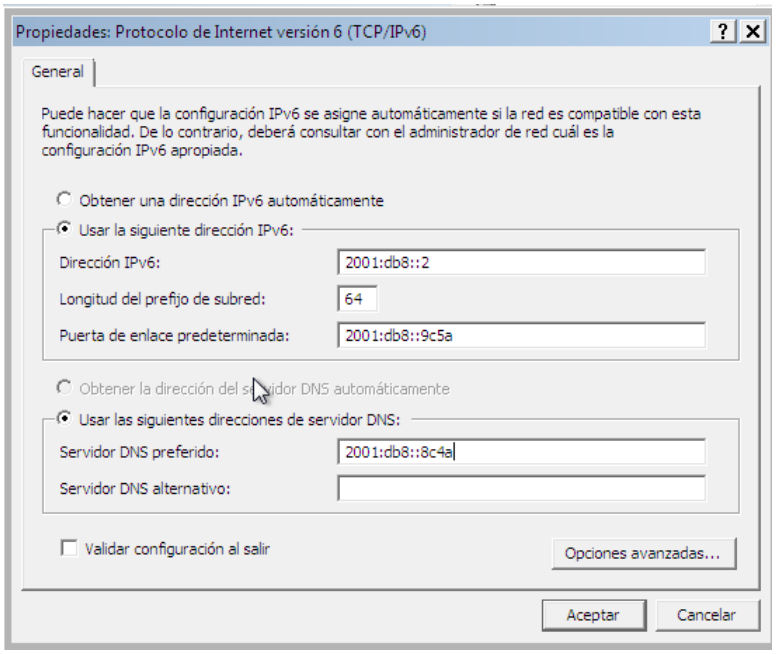
Figura 69. Protocolo de Internet IPv6



Elaborado por: Alejandro Santamaría

6. En propiedades del Protocolo de Internet versión 6 (TCP/IPv6) se puede mantener la configuración automáticamente o para el caso digitar las direcciones IPv6 deseadas.

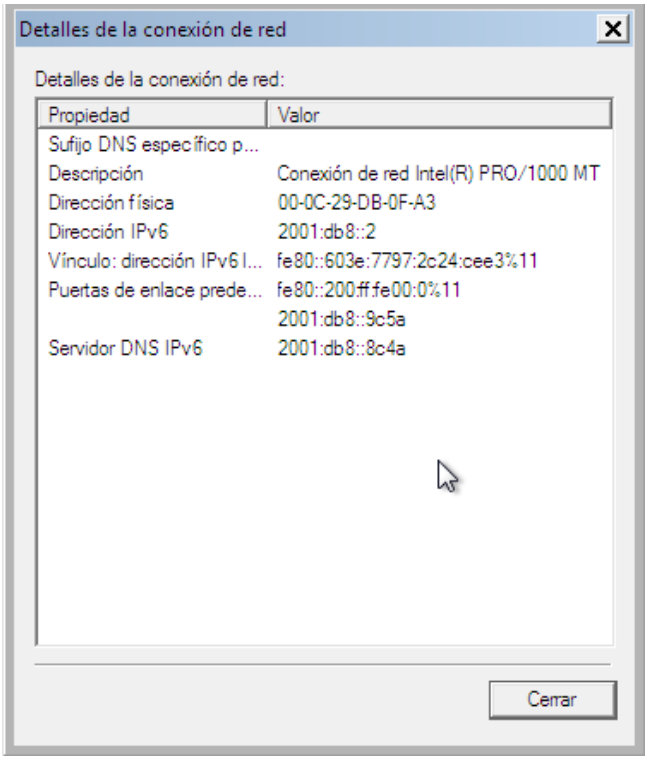
Figura 70. Configuración del protocolo IPv6



Elaborado por: Alejandro Santamaría

7. Verificar la configuración en los detalles de la conexión de red.

Figura 71. Detalles de la conexión de red



Elaborado por: Alejandro Santamaría

4.2.3 CentOS y otras distribuciones Linux

En Linux el protocolo IPv6 es soportado desde la versión del kernel 2.4. Para comprobar que esté instalado se puede proceder de la siguiente manera.

4.2.3.1 Línea de comandos

El modo más completo y común de configurar en Linux es mediante la línea de comandos o también conocido como terminal. Y para configurar temporalmente direcciones IPv6 en Linux se procede con los siguientes pasos:

1. Abrir el terminal del equipo.
2. Una vez en la terminal se digita:

   #test -f /proc/net/if_inet6 && echo "Kernel actual soporta IPv6" para verificar que el SO actual soporta IPv6.

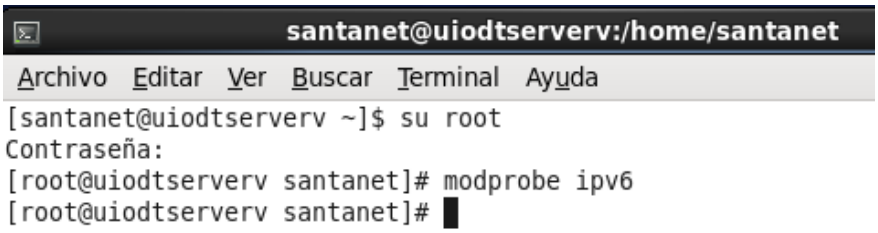
Figura 72. Soporte de IPv6

Elaborado por: Alejandro Santamaría

3. Si no se encuentra instalado se puede digitar:

   #modprobe ipv6

Figura 73. Instalar protocolo IPv6

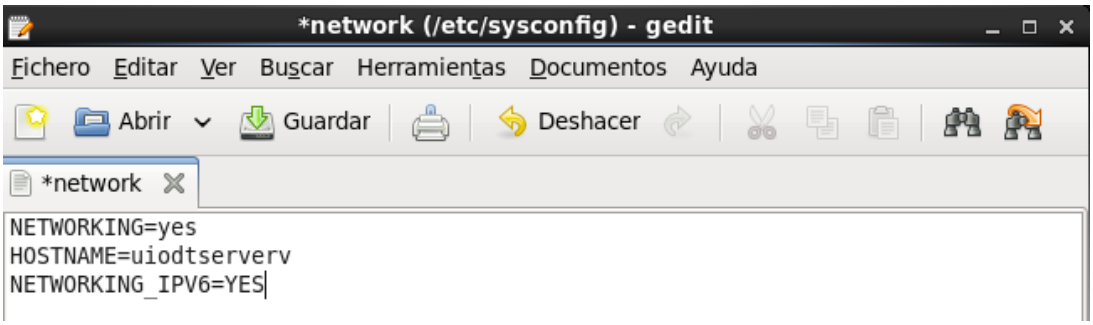


Elaborado por: Alejandro Santamaría

4. Para la configuración del protocolo IPv6 se procede a ingresar como root y añadir en el archivo /etc/sysconfig/network la siguiente línea:

   NETWORKING_IPV6=YES

Figura 74. Modificar archivo network

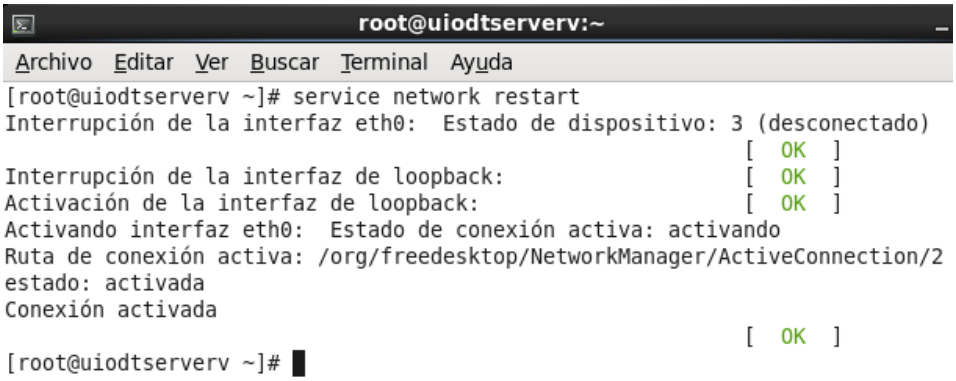


Elaborado por: Alejandro Santamaría

5. Se procede a reiniciar la red mediante:

   #service network restart o #/etc/init.d/network restart

Figura 75. Reinicio de red



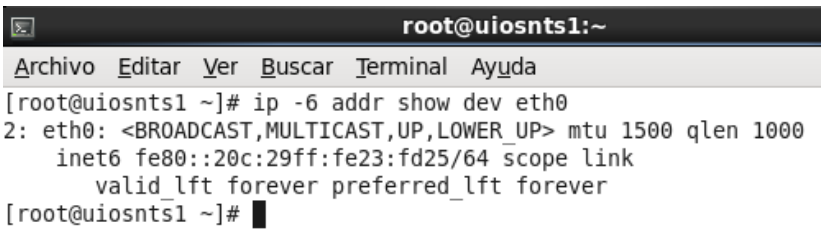
Elaborado por: Alejandro Santamaría

6. Para mostrar las direcciones IPv6 en Linux se puede digitar:

   #ip -6 addr show dev <interface>

   #ip -6 addr show dev eth0

Figura 76. Mostrar direcciones IPv6



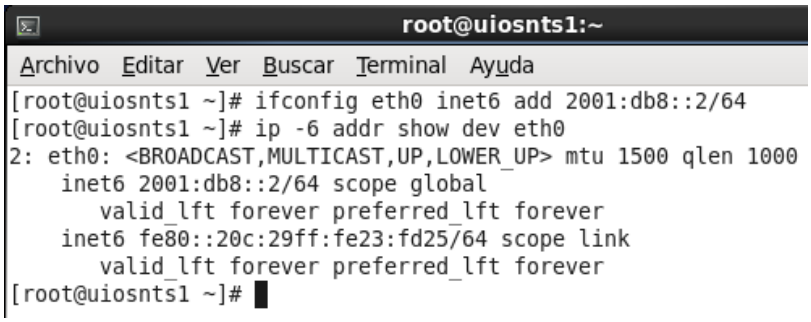
Elaborado por: Alejandro Santamaría

7. Para añadir una dirección IPv6 en Linux se puede digitar en el terminal:

   #ifconfig <interface> inet6 add <ipv6address>/<prefixlength>

   #ifconfig eth0 inet6 add 2001:db8::2/64

Figura 77. Añadir dirección IPv6



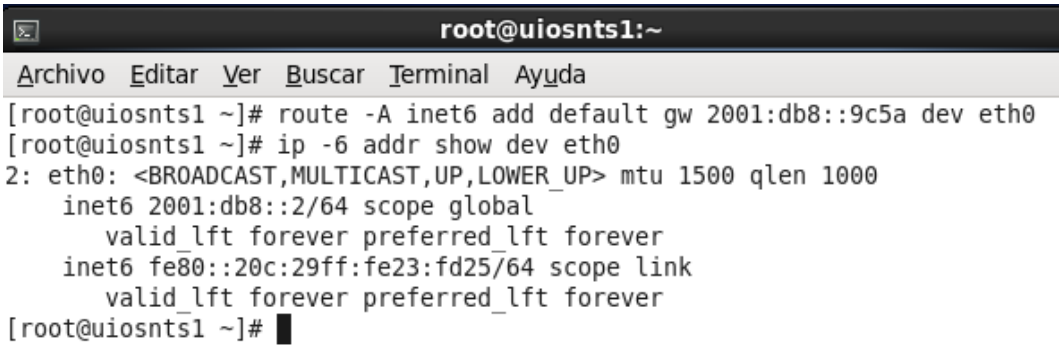
Elaborado por: Alejandro Santamaría

8. Para configurar un Gateway por defecto con una dirección IPv6 en Linux se puede digitar:

   #route –A inet6 add default gw <ipv6gateway> <device> <interfaz>

   #route –A inet6 add default gw 2001:db8::9c5a dev eth0

Figura 78. Configurar Gateway IPv6



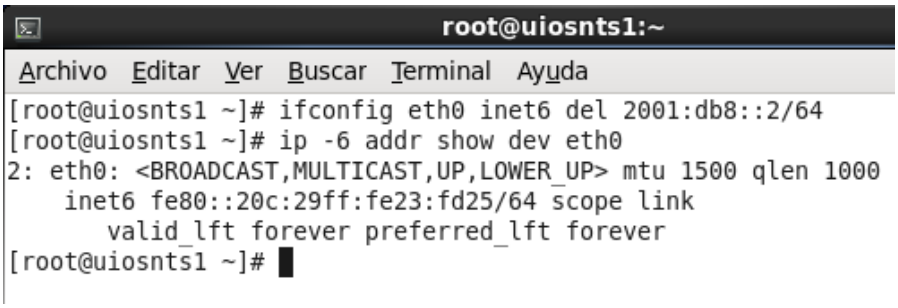
Elaborado por: Alejandro Santamaría

9. Para eliminar una dirección IPv6 en Linux se puede digitar:

   #ifconfig <interface> inet6 del <ipv6address>/<prefixlength>

   #ifconfig eth0 inet6 del 2001:db8::2/64

Figura 79. Eliminar dirección IPv6

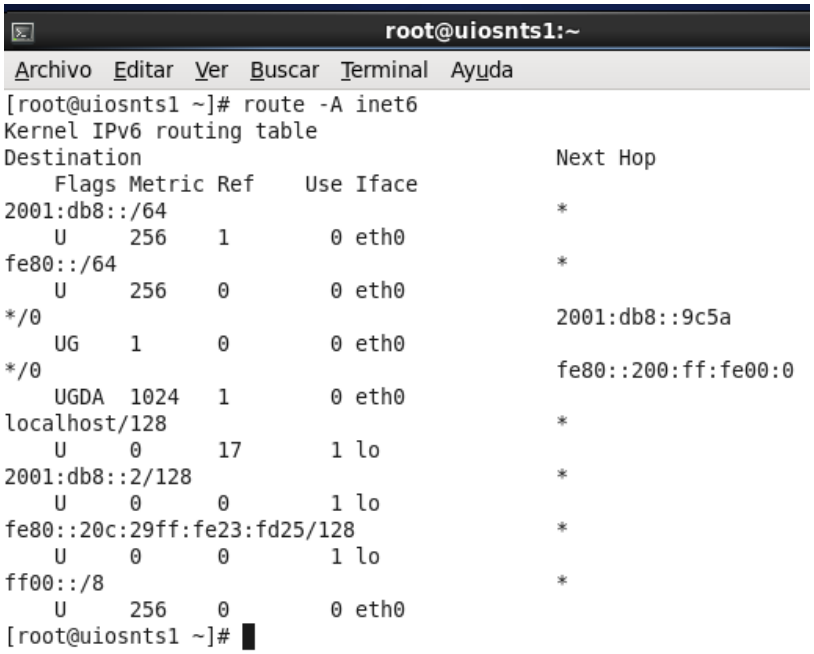


Elaborado por: Alejandro Santamaría

10. Para ver las rutas IPv6 en Linux se puede digitar:

    #route –A inet6

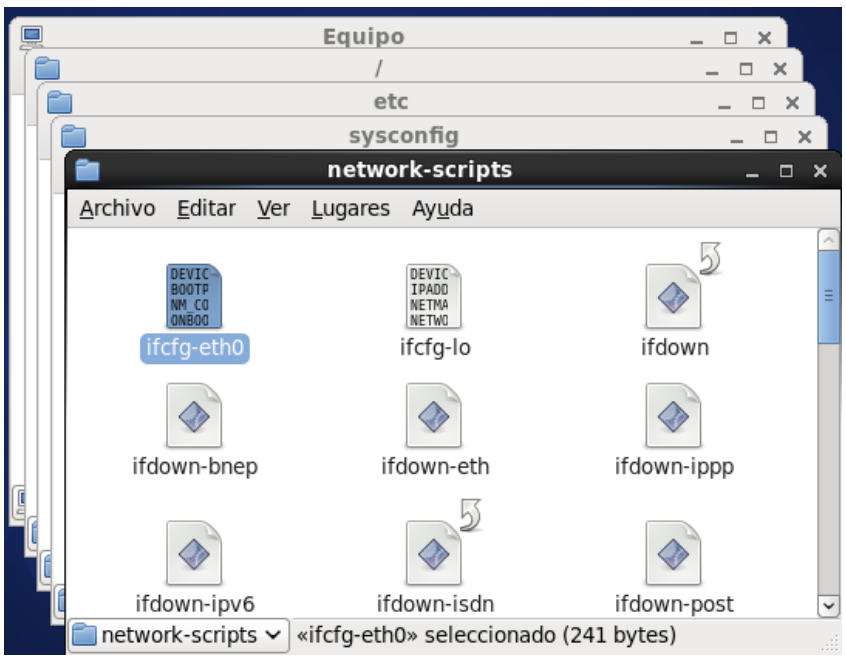
Figura 80. Rutas IPv6



Elaborado por: Alejandro Santamaría

11. La forma de configurar permanentemente direcciones IPv6 en Linux es utilizando los archivos de la carpeta network-scripts. Para lo cual se ingresa a la dirección /etc/sysconfig/network-scripts y abrir el archivo de la interfaz correspondiente.

Figura 81. Añadir dirección IPv6



Elaborado por: Alejandro Santamaría

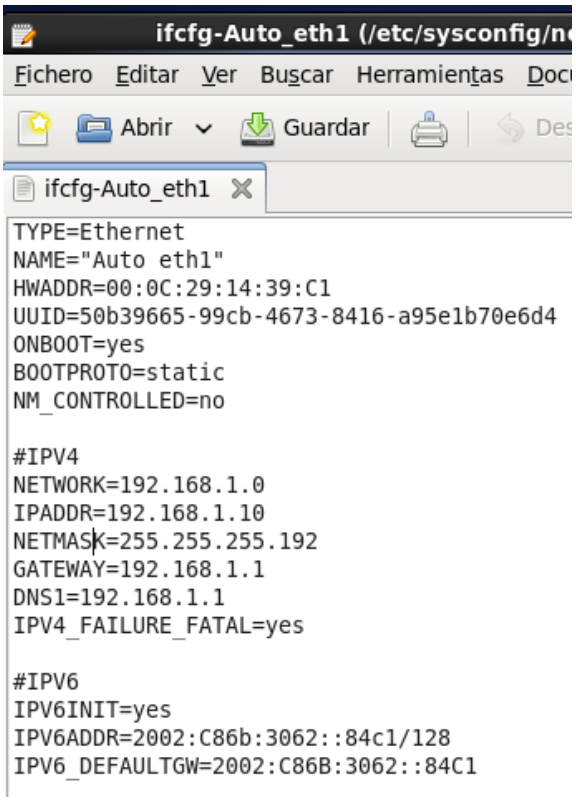
12. Se procede a añadir la dirección IPv6 en el archivo ifcfg-eth0 dependiendo de la interfaz seleccionada.

    IPV6INIT=YES

    IPV6ADDR=2001:db8::2/64

    IPV6_DEFAULTGW=2001:db8::9c5a

Figura 82. Añadir dirección IPv6



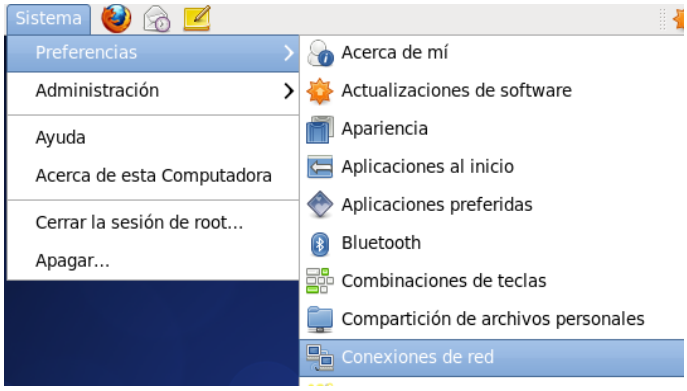
Elaborado por: Alejandro Santamaría

4.2.3.2 Interfaz gráfica

Para configurar una dirección IPv6 en modo gráfico a una interfaz seleccionada se procede de la siguiente manera:

1. En el menú sistema escoger preferencias y luego abrir conexiones de red.

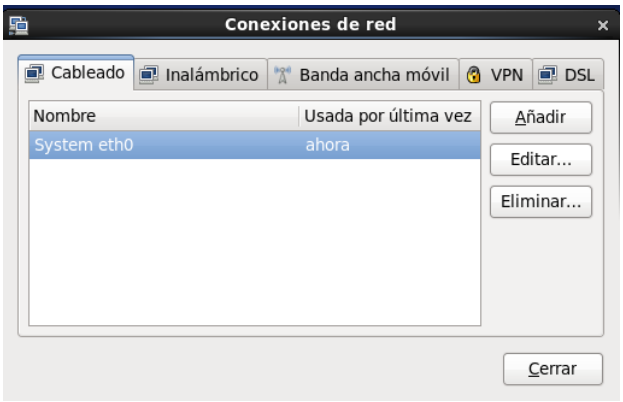
Figura 83. Conexiones de red



Elaborado por: Alejandro Santamaría

2. Escoger la interfaz deseada y editar.

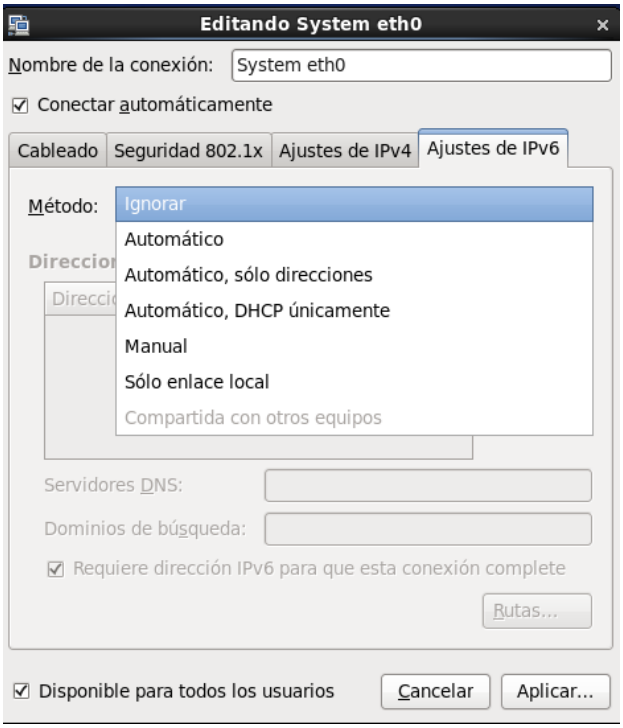
Figura 84. Editar conexiones de red



Elaborado por: Alejandro Santamaría

3. Luego en la pestaña Ajustes de IPv6 escoger el método a asignar.

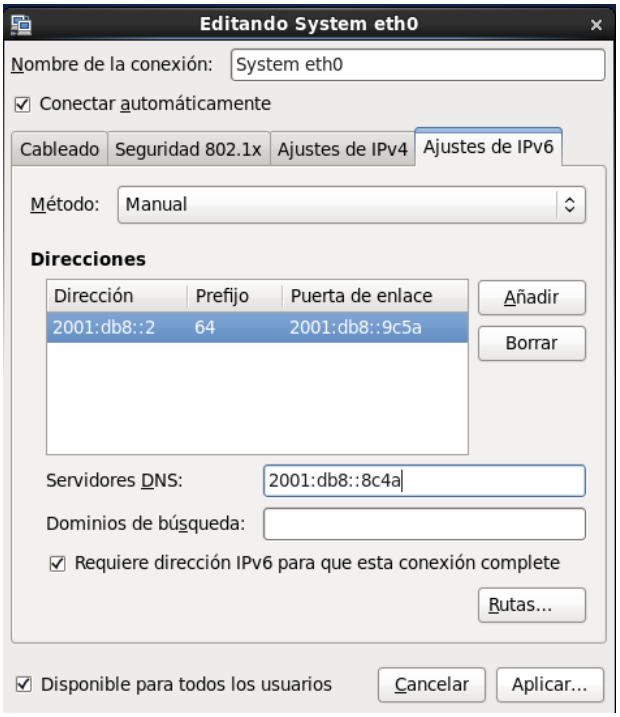
Figura 85. Método de direccionamiento IPv6



Elaborado por: Alejandro Santamaría

4. Escoger el método manual y seleccionar añadir para ingresar la dirección IPv6, su prefijo, la puerta de enlace o Gateway y el servidor DNS.

Figura 86. Editando system eth0



Elaborado por: Alejandro Santamaría

4.3 Configuración del router

4.3.1 Configuración del túnel 6in4

Para la respectiva configuración del túnel 6in4 en el PC router de la empresa Santanet se debe realizar los siguientes pasos:

1. Primero se va a añadir un túnel 6in4 mediante los siguientes comandos:

   #ip tunnel add <interface> mode sit remote <remoteipv4address> local <localipv4address> ttl <ttl>

   # ip tunnel add he-ipv6 mode sit remote 216.66.22.2 local 200.107.48.98 ttl 255

2. Proceder a subir la interfaz mediante el siguiente comando:

   #ip link set <interface> up

   #ip link set he-ipv6 up

3. Se procede a añadir la dirección local de la interface.

   #ip addr add <local6in4address>/16 dev <interface>

   #ip addr add 2001:470:7:125e::2/64 dev he-ipv6

4. Añadir la ruta por defecto de la interface.

   #ip route add ::/0 dev <interface>

   #ip route add ::/0 dev he-ipv6

5. Para eliminar un túnel 6in4 se debe proceder de la siguiente manera:

   #ip tunnel del <interface>

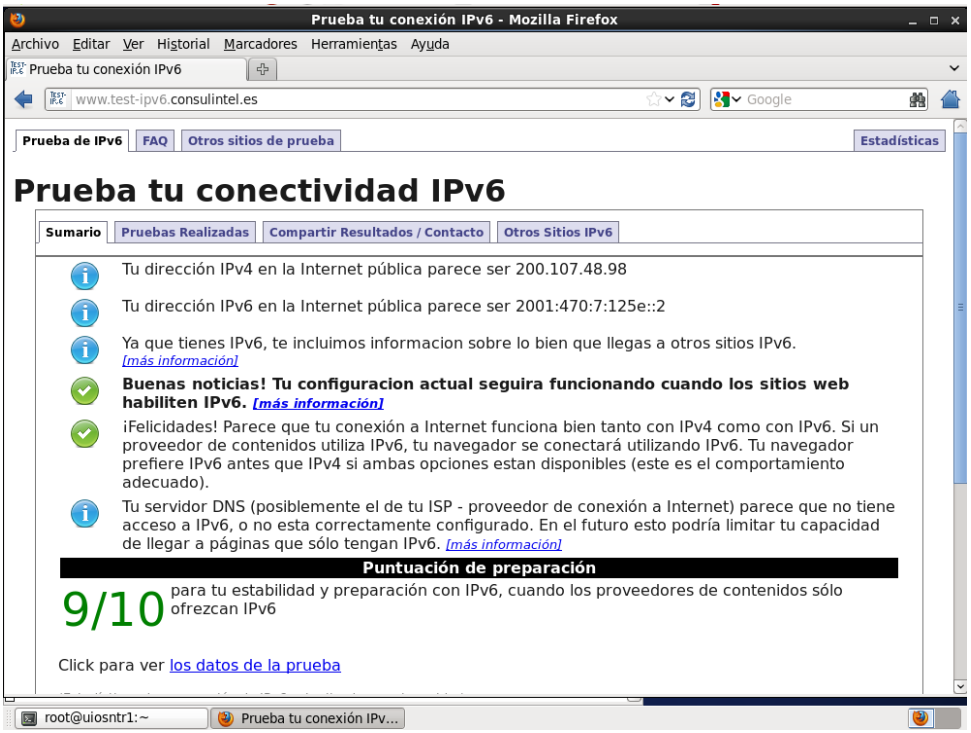
   #ip tunnel del he-ipv6

6. Para comprobar que el túnel 6in4 este funcionado se puede digitar:

   #ping6 ipv6.google.com

7. También para comprobar la conectividad IPv6 se puede imgresar a la página www.test-ipv6.consulintel.es

Figura 87. Prueba de conectividad IPv6



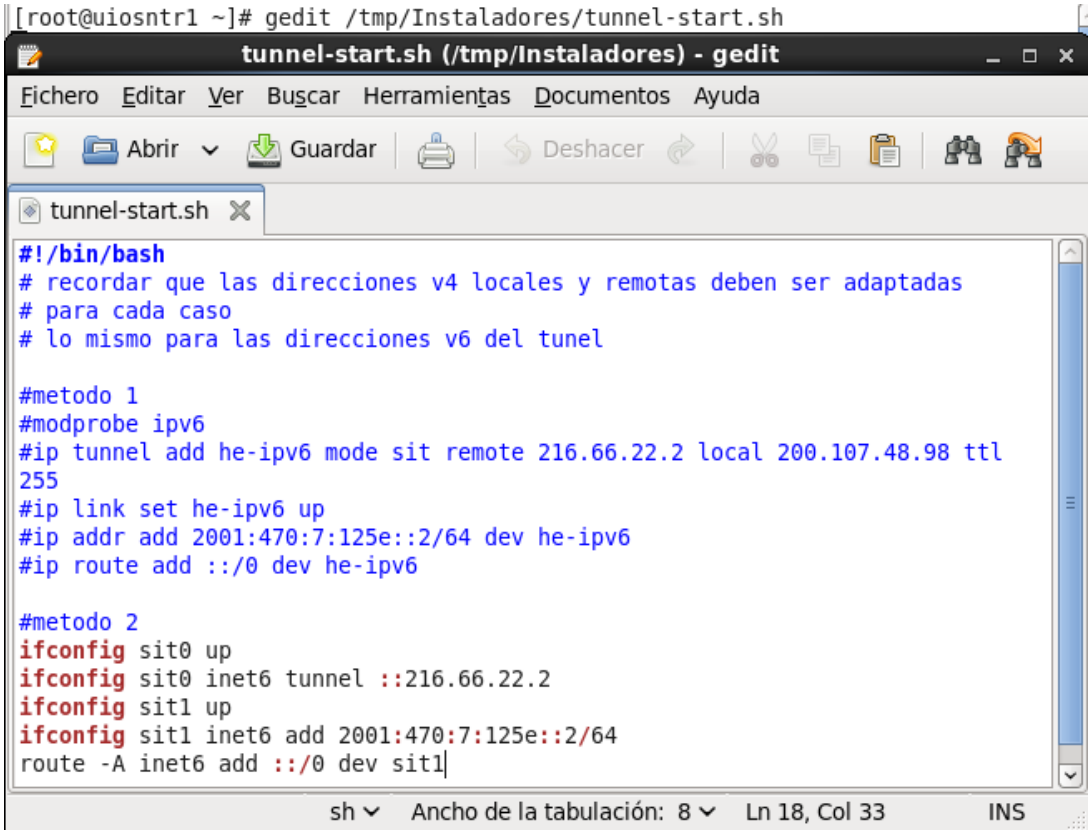
Elaborado por: Alejandro Santamaría

Para configurar que el túnel 6in4 no se borre cada vez que se apague el equipo, se detenga el servicio network o se baje las interfaces se puede crear un script en donde se encuentren los anteriores comandos y así automáticamente crear el túnel 6in4.

Los pasos a seguir son:

1. Crear un script en donde se encuentren los comandos para crear un túnel:

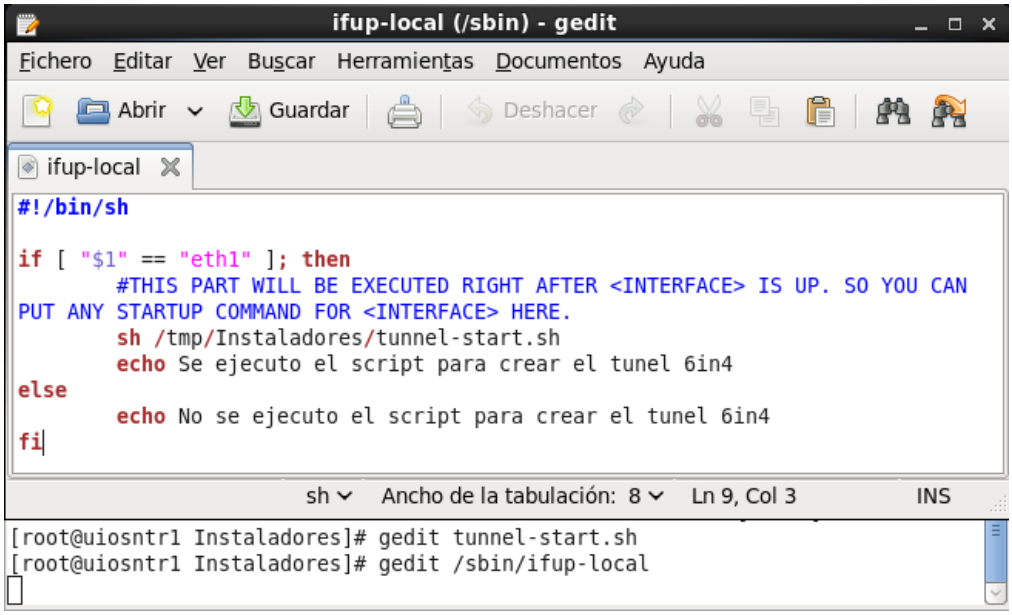
Figura 88. Script para túnel 6in4



Elaborado por: Alejandro Santamaría

2. Copiar o guardar el script en el lugar deseado.
3. Crear o modificar el archivo /sbin/ifup-local y agregar los siguientes comandos, teniendo en cuenta que se va a crear el túnel siempre y cuando se active la interfaz deseada:

Figura 89. Archivo ifup-local



Elaborado por: Alejandro Santamaría

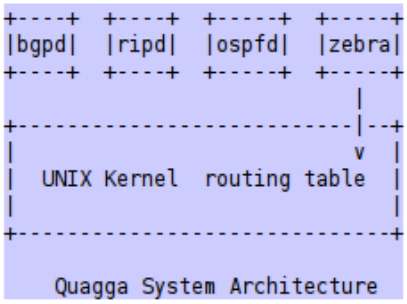
4. Finalmente se asigna el permiso de ejecución al archivo /sbin/ifup-local mediante el siguiente comando:

   #chmod +x /sbin/ifup-local

4.3.2 Quagga

Quagga está compuesto por varios daemons que trabajan de forma colaborativa para construir la tabla de encaminamiento. El daemon ripd maneja el protocolo RIP, el daemon ospfd maneja el protocolo OSPFv2, el daemon bgpd soporta el protocolo BGP-4. Para cambiar la tabla de encaminamiento del kernel y la redistribución de las rutas entre diferentes protocolos se utiliza el daemon zebra (Moreno, 2013).

Figura 90. Arquitectura de Quagga



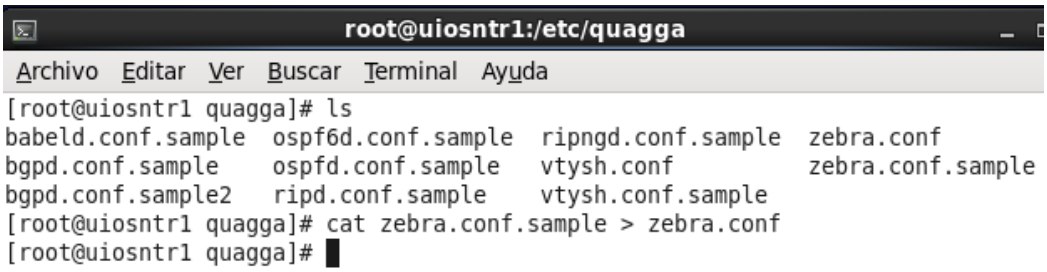
Fuente: (Kunihiro, 2013)

Los pasos a seguir en el equipo que tiene instalado el CentOS para la configuración del Quagga son:

1. Ingresar a la carpeta etc/quagga/
2. Copiar el contenido del archivo zebra.conf.sample al zebra.conf mediante:

   #cat zebra.conf.sample > zebra.conf

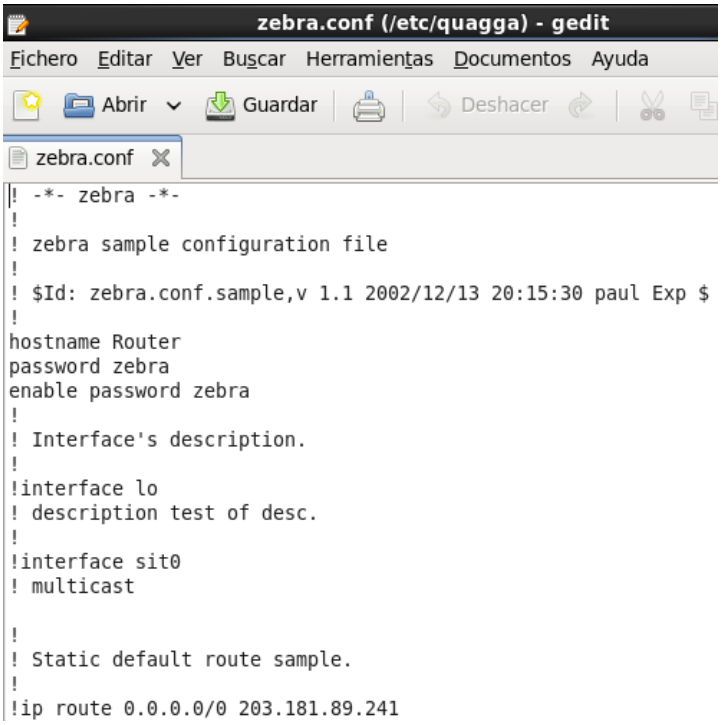
Figura 91. Copia del zebra.conf



Elaborado por: Alejandro Santamaría

3. Editar el archive zebra.conf utilizando el gedit

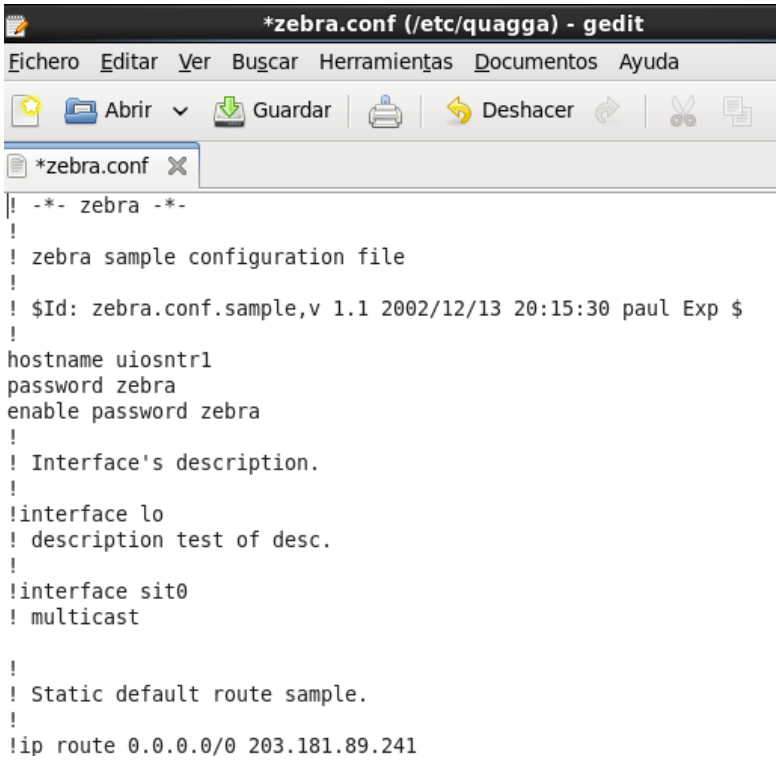
Figura 92. Editando zebra.conf



Elaborado por: Alejandro Santamaría

4. Modificar los campos hostname, password para entrar al zebra y password para entrar en el modo privilegiado. Guardar las modificaciones.

Figura 93. Editando zebra.conf

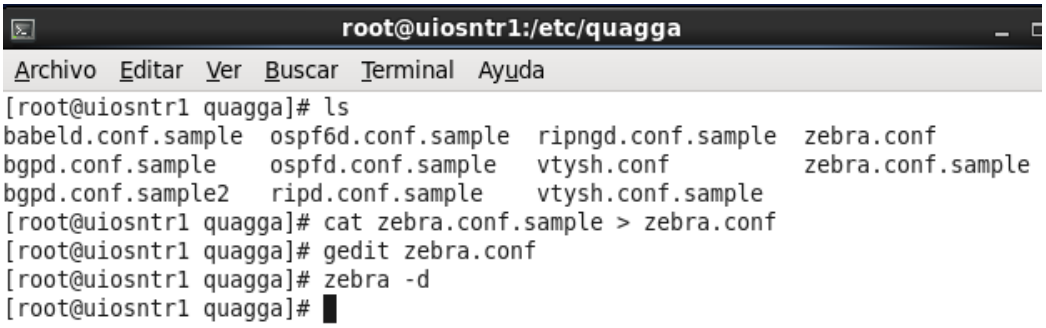


Elaborado por: Alejandro Santamaría

5. Se procede a iniciar el servicio zebra mediante el siguiente comando:

   #service zebra start o #zebra -d

Figura 94. Levantar el servicio zebra



Elaborado por: Alejandro Santamaría

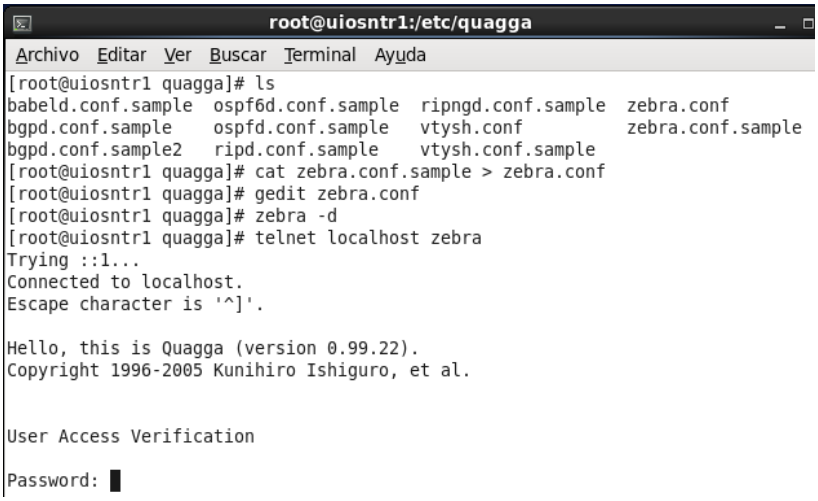
6. Si se desea que el servicio se ejecute cada vez que se inicia la máquina se digita:

   #chkconfig --level 35 zebra on

7. Antes de ingresar a la configuración del zebra verificar que tenga instalado el servicio telnet, caso contrario instalarlo e ingresar a la configuración del zebra mediante:

   #telnet localhost zebra o también se puede digitar **#vtysh**

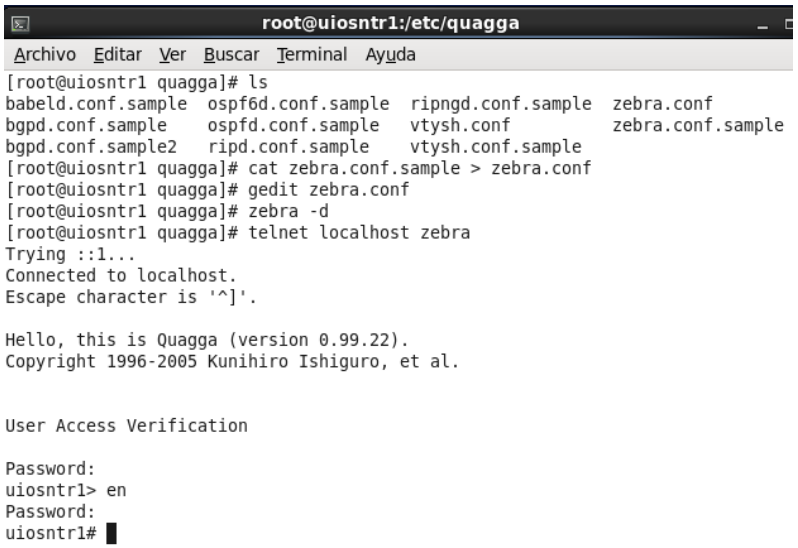
Figura 95. Configuración de Quagga



Elaborado por: Alejandro Santamaría

8. Se procede a ingresar las claves anteriormente configuradas para poder continuar. Para ingresar al modo privilegiado se puede digitar en o enable.

Figura 96. Configuración de Quagga



Elaborado por: Alejandro Santamaría

4.3.3 RIPng

RIPng es un protocolo de tipo vector distancia IGP que para configurar se deben seguir los siguientes pasos en el equipo que tiene instalado CentOS para la configuración del RIPng son:

1. Ingresar a la carpeta etc/quagga/
2. Copiar el contenido del archivo ripngd.conf.sample al ripngd.conf mediante:

   #cat ripngd.conf.sample > ripngd.conf
3. Editar el archivo ripngd.conf utilizando el gedit.
4. Modificar los campos hostname, password para entrar a ripng y password para entrar en el modo privilegiado. Guardar las modificaciones.
5. Se procede a iniciar el servicio ripng mediante el siguiente comando:

   #service ripngd start o #ripngd -d
6. Si se desea que el servicio se ejecute cada vez que se inicia la máquina se digita:

   #chkconfig --level 35 ripngd on
7. Para ingresar a la configuración del ripng se digita:

   #telnet localhost ripngd
8. Se procede a ingresar las claves anteriormente configuradas para poder proceder a configurar. Para ingresar al modo privilegiado se puede digitar en o enable.
9. Una vez en el modo privilegiado se procede a digitar configure terminal para ingresar al modo de configuración del router.
10. Para la respectiva configuración de ripng se puede digitar las siguientes sentencias:

    router ripng

    network 2001:470:8:125e::/64

    network 2001:470:e321:250d::/64

    redistribute connected

Mediante el comando router ripng lo que se hace es habilitar el protocolo ripng, mediante el comando network se especifica las redes directamente conectadas y finalmente mediante el comando redistribute connected se realiza el intercambio de información de enrutamiento mediante las interfaces directamente conectadas.

11. Se procede a guardar la información con el comando write y se despliega un mensaje en donde se indica en donde se guardó la configuración.
12. Para ver la tabla de enrutamiento ripng en IPv6 se puede digitar:

    #show ipv6 ripng

4.4 Instalación y configuración de servidores

4.4.1 Servidor FTP

El protocolo FTP se usa para transferir archivos y utiliza los puertos 20 y 21. Se basa en el modelo cliente-servidor por lo que se requieren ambos para establecer la comunicación. El servidor FTP se instala por medio del programa ftpd mediante los siguientes pasos:

1. Existen varios programas de servidor FTP que soportan IPv6. El programa a instalar es el Vsftpd.
2. Verificar los RPM que se necesitan instalar mediante el comando:

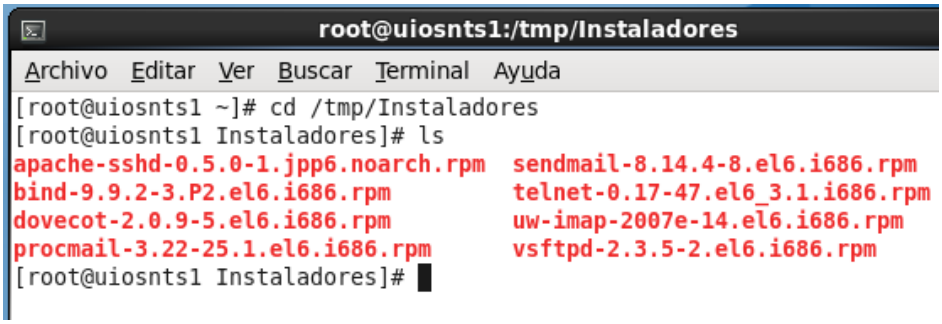
   #rpm –qa | grep httpd
3. Descargar el RPM correspondiente de la página http://pkgs.org/
4. Copiar el archivo vsftpd-2.3.5-2.el6.i686.rpm en la dirección deseada.

Figura 97. Vsftpd 2.3.5-2

Elaborado por: Alejandro Santamaría

5. Ejecutar el terminal de Linux como administrador o root.
6. Acceder al directorio en donde se encuentra copiado el archivo de instalación.

Figura 98. Directorio del archivo de instalación del vsftpd

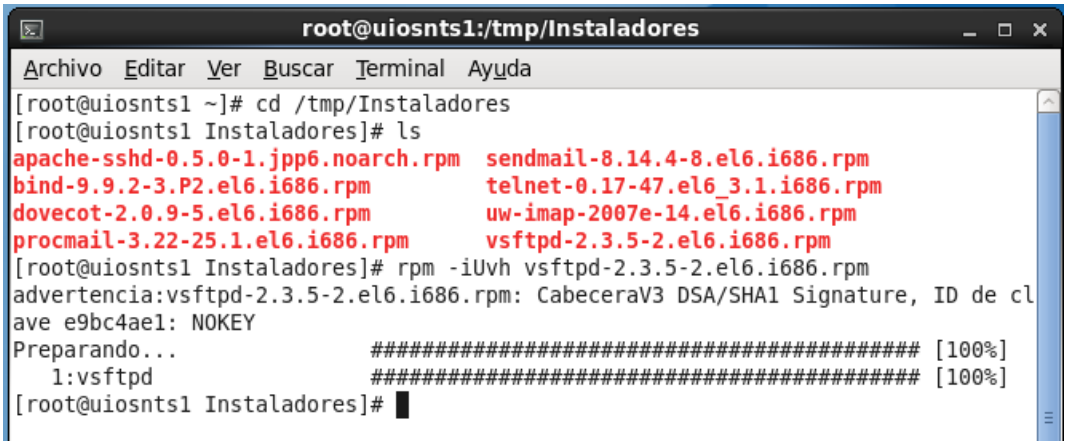


Elaborado por: Alejandro Santamaría

7. Una vez en el directorio del instalador para proceder a instalar se digita:

   #rpm –iUvh vsftpd-2.3.5-.2.el6.i686.rpm

Figura 99. Instalación del vsftpd



Elaborado por: Alejandro Santamaría

8. Finaliza la instalación si el proceso llega al 100%.
9. Modificar las siguientes líneas en el archivo de configuración etc/vsftpd/vsftpd.conf para habilitar el servidor FTP IPv6:

anonymous_enable=no
local_enable=yes
write_enable=yes
local_umask=022
dirmessage_enable=yes
xferlog_enable=yes
connect_from_port_20=yes
xferlog_std_format=yes
ascii_upload_enable=yes
ascii_download_enable=yes
ftpd_banner=Bienvenido al FTP de Santanet
ls_recurse_enable=yes
listen=no
listen_ipv6=yes
pam_service_name=vsftpd
userlist_enable=yes
tcp_wrappers=yes
use_localtime=yes
one_process_model=no

10. Proceder a iniciar el servicio vsftpd mediante el comando:

#service vsftpd start

11. Si se desea que el servicio se ejecute cada vez que se inicia la máquina se digita:

    #chkconfig --level 35 vsftpd on

12. Por defecto el usuario root no tiene permisos para conectarse al servidor ftp por propósitos de seguridad. Para crear un usuario y asignar una contraseña se puede digitar:

    #useradd santanet

    #passwd santanet

13. Proceder a conectarse al servidor ftp mediante el comando:

    #ftp 2001:470:8:125e::86d2

    Si al ejecutar este comando se despliega el mensaje **–bash: ftp: command not found** es debido a que no se tiene instalado el cliente ftp por lo cual se procede a instalar el cliente ftp deseado mediante:

    #yum install ftp

14. Volver a conectarse al servidor ftp.

15. Si se despliega el mensaje **cannot change directory:/home/Santanet**, se puede digitar en el servidor el siguiente comando para cambiar de directorio:

    #setsebool –P ftp_home_dir on

16. En este caso se está utilizando la configuración por defecto de iptables en CentOS, así que se debe añadir las siguientes líneas en /etc/sysconfig/ip6tables o en el script que asigna iptables, este script está más detallado en el Anexo B:

    iptables -A INPUT -m state --state NEW -m tcp -p tcp --dport 20 -j ACCEPT

    iptables -A INPUT -m state --state NEW -m tcp -p tcp --dport 21 -j

17. Finalmente probar la conexión con el servidor ftp y verificar su funcionamiento.

4.4.2 Servidor SSH

SSH permite la comunicación con otro equipo por medio de una interfaz de comandos usando un canal seguro con encriptación. SSH sustituye a telnet cuando se necesita una comunicación segura, utiliza el puerto 22. Se basa en el modelo cliente-servidor por lo que se requieren ambos para establecer la comunicación (ISOC, 2013, pág. 63). El servidor SSH se instala por medio del programa sshd mediante los siguientes pasos:

1. En la versión de CentOS 6.3 ya viene instalado un servidor SSH.
2. Verificar que se encuentre instalado el servidor SSH mediante el comando:

   #service sshd status
3. Una vez verificada la instalación del servidor SSH se procede a modificar el archivo /etc/ssh/sshd_config en donde se habilita el puerto y la dirección del servidor SSH:

   Port 22

   ListenAddress ::
4. Finalmente se reinicia el servicio mediante los siguientes comandos:

   #service sshd restart
5. En este caso se está utilizando la configuración por defecto de iptables en CentOS, así que se debe añadir las siguientes líneas en /etc/sysconfig/ip6tables o en el script que asigna iptables, este script está más detallado en el Anexo B:

   iptables -A INPUT -m state --state NEW -m tcp -p tcp --dport 22 -j ACCEPT

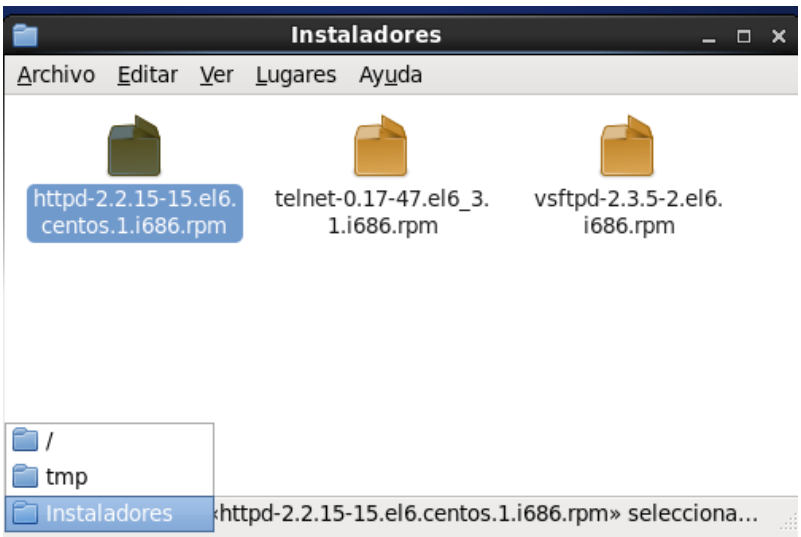
4.4.3 Servidor web

"La navegación web utiliza el protocolo HTTP para transferir hipertextos, páginas web o páginas HTML y para la navegación se usa el puerto 80. Se basa en el modelo cliente-servidor por lo que se requieren ambos para establecer la comunicación" (ISOC, 2013, pág. 70). El servidor web se instala por medio del programa httpd mediante los siguientes pasos:

1. Apache es el más extendido de los servidores web y su entorno natural es Linux. Las versiones 2.x o superiores soportan IPv6.
2. Verificar los RPM que se necesitan instalar mediante el comando:

   #rpm –qa | grep httpd
3. Descargar el RPM correspondiente de la página http://pkgs.org/
4. Copiar el archivo httpd-2.2.15-15.el6.centos.1.i686.rpm en la dirección deseada.

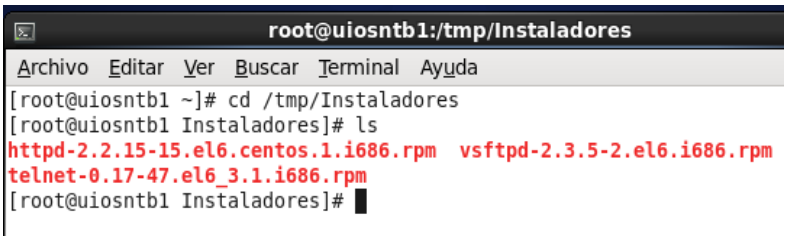
Figura 100. Httpd 2.2.15-15



Elaborado por: Alejandro Santamaría

5. Ejecutar el terminal de Linux como administrador o root.
6. Acceder al directorio en donde se encuentra copiado el archivo de instalación.

Figura 101. Directorio del archivo de instalación del httpd

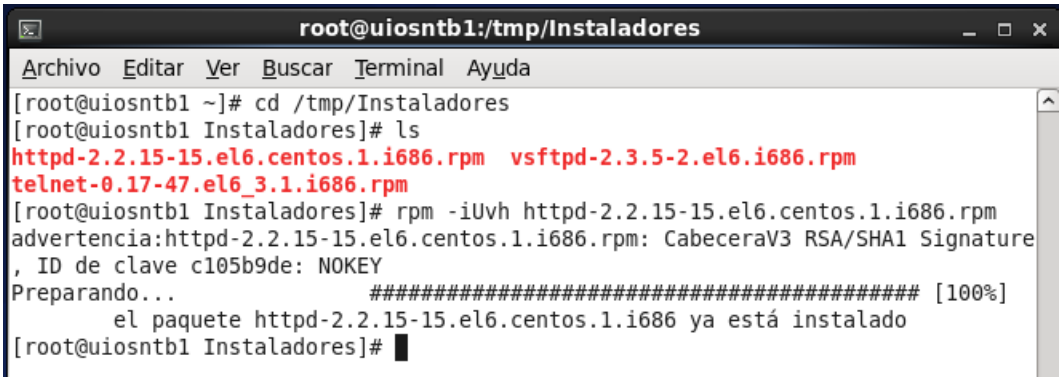


Elaborado por: Alejandro Santamaría

7. Una vez en el directorio del instalador para proceder a instalar se digita:

   #rpm –iUvh httpd-2.2.15-15.el6.centos.1.i686.rpm

Figura 102. Instalación del httpd



Elaborado por: Alejandro Santamaría

8. Finaliza la instalación si el proceso llega al 100%.
9. Asignar el hostname del servidor web en el archivo /etc/sysconfig/network.
10. Agregar en el archivo /etc/host las direcciones del servidor como se indica a continuación:

    127.0.0.1 localhost localhost.localdomain localhost4 localhost4.localdomain4

    ::1 localhost localhost.localdomain localhost6 localhost6.localdomain6

    192.168.1.20 santanet.net.ms

    2001:470:8:125e::86d2 santanet.net.ms

11. Añadir o modificar en el archivo /etc/httpd/conf/httpd.conf la siguiente sentencia, para poder escuchar peticiones IPv6 en el puerto 80.

    Listen 80

12. Al final del archivo /etc/httpd/conf/httpd.conf se procede a crear hosts virtuales IPv6, se debe utilizar corchetes [] para encerrar a una dirección IPv6.

    #Definición de los Host Virtuales

    NameVirtualHost [2001:470:8:125e::86d2]

    NameVirtualHost 192.168.1.20

    #Host Virtual IPv6 con página dual stack

    <VirtualHost [2001:470:8:125e::86d2]>

    DirectoryIndex index.html index.php

    DocumentRoot /var/www/html/ipv4-ipv6-web/

    ServerName www.santanet.net.ms

    </VirtualHost>

    #Host Virtual IPv4 con página dual stack

    <VirtualHost 192.168.1.20>

DirectoryIndex index.html index.php
DocumentRoot /var/www/html/ipv4-ipv6-web/
ServerName www.santanet.net.ms
</VirtualHost>
#Host Virtual IPv6 con página IPv6
<VirtualHost [2001:470:8:125e::86d2]>
DirectoryIndex index.html index.php
DocumentRoot /var/www/html/ipv6-web/
ServerName ipv6.santanet.net.ms
</VirtualHost>

13. En el directorio /var/www/html/ipv4-ipv6-web/ copiar la página dual stack que va a funcionar en IPv4 e IPv6 y en directorio /var/www/html/ipv6-web/ copiar la página IPv6.
14. Proceder a iniciar el servicio httpd mediante el comando:

    #service httpd start

15. Si se desea que el servicio se ejecute cada vez que se inicia la máquina se digita:

    #chkconfig --level 35 httpd on

16. En este caso se está utilizando la configuración por defecto de iptables en CentOS, así que se debe añadir las siguientes líneas en /etc/sysconfig/ip6tables o en el script que asigna iptables, este script está más detallado en el Anexo B:

    iptables -A INPUT -m state --state NEW -m tcp -p tcp --dport 80 -j ACCEPT

17. Para comprobar que el servidor está escuchando IPv6 en el puerto 80 se puede utilizar el comando:

    #netstat –tan | grep 80

18. Abrir cualquier navegador web y digitar la IP o el nombre del host.

4.4.4 Servidor de correo

"El servicio de email o correo electrónico es uno de los más utilizados. Generalmente se usan los protocolos SMTP (puerto 25) para enviar los mensajes de correo, POP3 (puerto 110) y IMAP4 (puerto 143) para obtener los mensajes" (ISOC, 2013, pág. 65).

Se basa en el modelo cliente-servidor por lo que se requieren ambos para establecer la comunicación. Los principales servidores y clientes de correo soportan IPv6, entre ellos se tiene sendmail que es un servidor muy popular en ambiente Linux y se instala mediante los siguientes pasos:

1. Para llevar a cabo la instalación de los paquetes necesarios para instalar un servidor de correo se puede digitar lo siguiente:

   #yum –y install sendmail sendmail-cf dovecot cyrus-sasl cyrus-sasl-plain cyrus-sasl-md5 make m4

2. Si previamente se tenía instalado postfix o exim ejecutar lo siguiente desde un terminal y definir a sendmail como predeterminado:

   #alternatives --config mta

   Si estuviera presente postfix detenga mediante los siguientes comandos:

   #service postfix stop

   #chkconfig postfix off

3. Para dar de alta una cuenta de correo, se procede a digitar los siguientes comandos:

   #useradd -s /sbin/nologin nombredelsuario

4. Para asignar contraseña a una cuenta de correo se puede realizar utilizando los siguientes comandos:

   #passwd nombredelsuario

5. Se procede a editar el archivo /etc/mail/local-host-names para establecer los dominios a administrar:

   santanet.net.ms

6. Crear el archivo /etc/mail/relay-domains mediante los siguientes comandos:

#touch /etc/mail/relay-domains

7. En el archivo /etc/mail/relay-domains agregar los nombres de los dominios que tendrán permitido retransmitir correo electrónico desde el servidor. Por lo general tiene el mismo contenido de /etc/mail/local-host-names a menos que se desee excluir algún domino en particular.

   santanet.net.ms

8. Se procede a configurar los dominios o conjunto de direcciones IP que podrán hacer uso o no del servidor de correo en el archivo /etc/mail/access.

   - Cualquier elemento que tenga la acción RELAY podrá enviar correo sin necesidad de autenticar y re-transmitir éste sin restricción alguna.
   - Cualquier elemento que tenga la acción OK podrá enviar correo sin necesidad de autenticar pero solo a las cuentas locales.
   - Cualquier elemento que tenga la acción REJECT tendrá prohibido cualquier tipo de comunicación de correo.

   Connect:localhost.localdomain RELAY
   Connect:localhost RELAY
   Connect:127.0.0.1 RELAY
   # Dirección IPv4 del servidor de correos
   Connect:192.168.1.20 RELAY
   # Dirección IPv6 del servidor de correos
   Connect:IPv6:2001:470:8:125e::86d2 RELAY
   # Dominio de los correos
   Connect:santanet.net.ms RELAY
   # Dirección IP que entrega correo solamente de forma local
   Connect:192.168.1.10 OK
   # Lista negra
   Connect:IPv6:2001:470:8:125e::88d8 REJECT
   Connect:IPv6:2001:470:e321:250d::99d9 REJECT
   usuario@molesto.com REJECT
   productoinutil.com.mx REJECT

9. Se procede a modificar el archivo /etc/mail/sendmail.mc para definir, cambiar o añadir funciones. La línea **define(`confAUTH_OPTIONS',`A')dnl** viene habilitada de modo predeterminado y permite la autenticación de usuarios a

través del puerto 25 por el método PLAIN o en texto simple. Para habilitar la autenticación mediante cifrado se procede a modificar de la siguiente manera:

dnl define(`confAUTH_OPTIONS',`A')dnl

define(`confAUTH_OPTIONS', `A p')dnl

TRUST_AUTH_MECH(`EXTERNAL DIGEST-MD5 CRAM-MD5 LOGIN PLAIN')dnl

define(`confAUTH_MECHANISMS', `EXTERNAL GSSAPI DIGEST-MD5 CRAM-MD5 LOGIN PLAIN')dnl

10. Sendmail por defecto escucha peticiones solo a través de la interfaz de retorno del sistema 127.0.0.1, para poder recibir correo desde Internet o desde la LAN modifique la siguiente línea:

    DAEMON_OPTIONS(`Port=smtp,Addr=127.0.0.1, Name=MTA')dnl

    Y elimine el valor Addr=127.0.0.1 incluida la coma (,) de modo que quede así:

    DAEMON_OPTIONS(`Port=smtp, Name=MTA')dnl

11. Para el envío de correo también se puede utilizar el puerto 587, por estándar se utiliza como puerto alternativo cuando está bloqueado el puerto 25. Para utilizar este puerto modificar de la siguiente manera:

    DAEMON_OPTIONS(`Port=submission, Name=MSA, M=Ea')dnl

12. Sendmail por defecto escucha peticiones solo a través de la interfaz de retorno del sistema ::1 en el caso de IPv6, para poder recibir correo desde Internet o desde la LAN modifique la siguiente línea:

    dnl DAEMON_OPTIONS(`port=smtp,Addr=::1, Name=MTA-v6, Family=inet6')dnl

    Eliminar la palabra dnl y asignar la IPv6 del servidor de modo que quede así:

    DAEMON_OPTIONS(`port=smtp, Addr=2001:470:8:125e::86d2, Name=MTA-v6, Family=inet6')dnl

13. Para impedir que se acepte correo de dominios inexistentes que se suelen utilizar para correo masivo no solicitado o spam se procede a modificar de la siguiente manera:

    dnl FEATURE(`accept_unresolvable_domains')dnl

14. En este caso como se va a enviar correo con un solo dominio se procederá a enmascarar todos los correos emitidos desde el servidor con el nombre del dominio. Para ello se procede a modificar de la siguiente manera:

    MASQUERADE_AS(`santanet.net.ms')dnl

    FEATURE(masquerade_envelope)dnl

    FEATURE(masquerade_entire_domain)dnl

15. El archivo /etc/mail/sendmail.mc es un archivo de macros y por lo cual una vez modificado se debe reiniciar el servicio sendmail y ejecutar el siguiente comando:

    #m4 /etc/mail/sendmail.mc > /etc/mail/sendmail.cf

16. En el archivo /etc/hosts se agrega la dirección del servidor y el dominio de los correos mediante:

    192.168.1.20 santanet.net.ms

17. El servidor dovecot por defecto tiene deshabilitados los protocolos POP e IMAP los cuales son necesarios para la entrega de correo. Se procede a descomentar el parámetro protocols en el archivo /etc/dovecot/dovecot.conf de la siguiente manera:

    protocols = imap pop3 lmtp

18. Establecer en el archivo /etc/dovecot/conf.d/10-mail.conf el valor del parámetro mail_location de la siguiente manera:

    mail_location = mbox:~/mail:INBOX=/var/mail/%u

19. En el mismo archivo en la opción mail_privileged_group proceder a descomentar la línea y definir el valor del grupo como mail:

    mail_privileged_group = mail

20. En el mismo archivo en la opción mail_access_groups proceder a descomentar la línea y definir el valor del grupo como mail:

    mail_access_groups = mail

    Se requiere que los usuarios locales pertenezcan al grupo mail.

21. Dovecot permite autenticarse con texto simple solamente desde el mismo PC, para permitir la autenticación de usuarios desde equipos remotos se debe editar el archivo /etc/dovecot/conf.d/10-auth.conf y asignar el valor no a la opción disable_plaintext_auth de la siguiente manera:

    disable_plaintext_auth = no

22. Iniciar el servidor de correo sendmail mediante el siguiente comando:

    #service sendmail start

23. Iniciar el servidor de correo dovecot mediante el siguiente comando:

    #service dovecot start

24. Iniciar el servidor de autenticación para SMTP mediante el siguiente comando:

    #service saslauthd start

25. Si se desea que el servicio se ejecute cada vez que se inicia la máquina se digita:

    #chkconfig --level 35 <servicio> on

26. En este caso se está utilizando la configuración por defecto de iptables en CentOS, así que se debe añadir las siguientes líneas en /etc/sysconfig/ip6tables o en el script que asigna iptables, este script está más detallado en el Anexo B:

    iptables -A INPUT -m state --state NEW -m tcp -p tcp --dport 25 -j ACCEPT

    iptables -A INPUT -m state --state NEW -m tcp -p tcp --dport 110 -j ACCEPT

    iptables -A INPUT -m state --state NEW -m tcp -p tcp --dport 143 -j ACCEPT

    iptables -A INPUT -m state --state NEW -m tcp -p tcp --dport 465 -j ACCEPT

    iptables -A INPUT -m state --state NEW -m tcp -p tcp --dport 587 -j ACCEPT

    iptables -A INPUT -m state --state NEW -m tcp -p tcp --dport 993 -j ACCEPT

    iptables -A INPUT -m state --state NEW -m tcp -p tcp --dport 995 -j ACCEPT

27. Para poder instalar SquirrelMail primero se debe instalar el repositorio EPEL:

    # wget http://dl.fedoraproject.org/pub/epel/6/i386/epel-release-6-8.noarch.rpm

    # rpm -ivh epel-release-6-8.noarch.rpm

    # yum install squirrelmail

28. Ingresar al directorio /usr/share/squirrelmail/config/ y usar el comando **./conf.pl** para comenzar la configuración del squirrelmail.

29. Seleccionar la opción 1 del menú principal para asignar los detalles de la organización y luego presione r para regresar al menú principal.
30. Seleccione la opción 2 del menú principal, e ingresar en la opción 1 el dominio y en la opción 3 SMTP.
31. Presionar s para guardar y q para salir.
32. En el archivo /etc/httpd/conf/httpd.conf agregar las siguientes líneas:

```
Alias /squirrelmail /usr/share/squirrelmail
<Directory /usr/share/squirrelmail>
   Options Indexes FollowSymLinks
   RewriteEngine On
   AllowOverride All
   DirectoryIndex index.php
   Order allow,deny
   Allow from all
</Directory>
ServerName localhost
```

33. Baja evitar el error de permiso denegado se puede ejecutar:

    setsebool -P httpd_can_network_connect=1

34. Reiniciar el servicio httpd:

    #service httpd restart

35. Mediante un explorador ingresar al webmail digitando lo siguiente en la barra de direcciones:

    http://[2001:470:8:125e::86d2]

    http://www.santanet.net.ms/webmail

Figura 103. Squirrelmail

Elaborado por: Alejandro Santamaría

4.4.5 Servidor DNS

"El servidor DNS traduce nombres de dominio a direcciones de red tanto IPv4 como IPv6 y su función es fundamental en el Internet actual" (ISOC, 2013, pág. 77). Este servidor se procederá a instalar en el PC router.

Hay que tener claro que el transporte del tráfico DNS a través de una red IPv4 e IPv6 es diferente y que los datos contenidos en los servidores DNS IPv4 son registros A y en DNS IPv6 son registros AAAA.

Existen varios programas de servidor DNS que soportan IPv6, el que se va a utilizar es BIND incluido en la distribución de CentOS, para la respectiva configuración de BIND se realizará los siguientes pasos:

1. Verificar los RPM que se necesitan instalar mediante el comando:

   #rpm –qa | grep bind

2. Descargar el RPM correspondiente de la página http://pkgs.org/

3. En este caso como son varios RPM a instalar se puede digitar el siguiente comando para que se instalen automáticamente:

   #yum –y install bind*

4. Modificar en el archivo /etc/named.conf los campos deseados para la configuración del servidor DNS, a continuación se detalla la configuración que permitirá utilizar el servidor:

```
options {
# Puerto y direcciones IPv4 del servicio DNS
 listen-on port 53 { 127.0.0.1; 10.0.0.10; };
# Puerto y direcciones IPv6 del servicio DNS
 listen-on-v6 port 53 { ::1; 2001:470:e321:250d::84c1; };
# Directorios de archivos
 directory            "/var/named";
 dump-file            "/var/named/data/cache_dump.db";
 statistics-file      "/var/named/data/named_stats.txt";
 memstatistics-file           "/var/named/data/named_mem_stats.txt";
# Opciones del named.conf
 allow-query     { any;};
 recursion yes;
 dnssec-enable yes;
 dnssec-validation yes;
# Dirección de la llave ISC DLV
 bindkeys-file "/etc/named.iscdlv.key";
 managed-keys-directory "/var/named/dynamic";
# Reenviadores, DNS externos o del ISP
 forward only;
 forwarders {8.8.8.8; 8.8.4.4; 2001:4860:4860::8888; 2001:4860:4860::8844; };
};
logging {
      channel default_debug {
            file "data/named.run";
            severity dynamic;
      };
};

zone "." IN {
 type hint;
 file "named.ca";
};
# Zona del dominio
zone      "santanet.net.ms" IN {
 type master;
 file "fwd.santanet.net.ms";
 allow-update { none; };
};
# Zona inversa del dominio IPv4
```

```
zone      "1.168.192.in-addr.arpa" IN {
 type master;
 file "rev.santanet.net.ms";
 allow-update { none; };
};
# Zona inversa del dominio IPv6
zone      "e.5.2.1.8.0.0.0.0.0.7.4.0.1.0.0.2.ip6.arpa" IN {
 type master;
 file "rev.santanet.net.ms";
 allow-update { none; };
};
# Nombres y direcciones como se comenta en el RFC1912
include "/etc/named.rfc1912.zones";
```

5. Se procede a crear en el directorio /var/named/ el archivo de zona de envío fwd.santanet.net.ms que se detalla en el archivo /etc/named.conf utilizando las siguientes líneas:

```
$TTL 1200
@       IN      SOA     uiosnts1.santanet.net.ms.       root.santanet.net.ms. (
      2011071001  ;Serial
      3600      ;Refresh
      1800      ;Retry
      604800     ;Expire
      86400     ;Minimum TTL
)
@       IN      A               192.168.1.20
@       IN      AAAA            2001:470:8:125e::86d2
@       IN      NS              uiosnts1.santanet.net.ms.
@       IN      MX              10      santanet.net.ms.
@       IN      TXT             "Esta zona es usada por Santanet"
; A Records
uiosnts1 IN     A               192.168.1.20
www     IN      A               192.168.1.20
mail    IN      A               192.168.1.20
; AAAA Records
uiosnts1 IN     AAAA            2001:470:8:125e::86d2
www     IN      AAAA            2001:470:8:125e::86d2
mail    IN      AAAA            2001:470:8:125e::86d2
ipv6    IN      AAAA            2001:470:8:125e::86d2
```

6. Se procede a crear en el directorio /var/named/ el archivo de zona inversa rev.santanet.net.ms que se detalla en el archivo /etc/named.conf utilizando las siguientes líneas:

```
$TTL 1200
@       IN      SOA     uiosnts1.santanet.net.ms.       root.santanet.net.ms. (
        2011071001  ;Serial
        3600        ;Refresh
        1800        ;Retry
        604800      ;Expire
        86400       ;Minimum TTL
)
@       IN      NS              uiosnts1.santanet.net.ms.
;A Records
20      IN  PTR uiosnts1.santanet.net.ms.
20      IN  PTR www.santanet.net.ms.
20      IN  PTR mail.santanet.net.ms.
; AAAA Records
2.d.6.8.0.0.0.0.0.0.0.0.0.0.0.0.0.0     IN      PTR     uiosnts1.santanet.net.ms.
2.d.6.8.0.0.0.0.0.0.0.0.0.0.0.0.0.0     IN      PTR     www.santanet.net.ms.
2.d.6.8.0.0.0.0.0.0.0.0.0.0.0.0.0.0     IN      PTR     mail.santanet.net.ms.
2.d.6.8.0.0.0.0.0.0.0.0.0.0.0.0.0.0     IN      PTR     ipv6.santanet.net.ms.
```

7. Una vez configurado el servidor DNS, se debe indicar en el archivo /etc/resolv.conf las direcciones IP del servidor DNS (En este caso las mismas direcciones IP):

```
search santanet.net.ms

nameserver 192.168.1.20

nameserver 2001:470:8:125e::86d2
```

8. Se procede a iniciar el servicio named mediante el siguiente comando:

```
#service named start
```

9. Si se desea que el servicio se ejecute cada vez que se inicia la máquina se digita:

```
#chkconfig --level 35 named on
```

10. En este caso se está utilizando la configuración por defecto de iptables en CentOS, así que se debe añadir las siguientes líneas en /etc/sysconfig/ip6tables o en el script que asigna iptables, este script está más detallado en el Anexo B:

    iptables -A INPUT -m state --state NEW -m tcp -p tcp --dport 53 -j ACCEPT

4.4.6 Servidor DHCPv6

Este servidor se procederá a instalar en el PC router. Para la autoconfiguración de la LAN se va a utilizar el daemon radvd y mediante este poder anunciar los prefijos IPv6, para que las interfaces se autoconfiguren y utilizando el servidor de DHCPv6 se va anunciar las direcciones de los servidores DNS, entre otros. No se recomienda utilizar el daemon radvd para asignar DNS debido que se necesita la instalación de un daemon cliente rdnssd y tampoco se recomienda utilizar el servidor DHCPv6 para asignar IP, ya que no asigna puertas de enlace debido a su diseño.

Para asignar SLAAC-Stateless Address Autoconfiguration- (Autoconfiguración de direcciones libres de estado) mediante el daemon radvd se procede a instalar y configurar mediante los siguientes comandos:

1. Verificar los RPM que se necesitan instalar mediante el comando:

   #rpm –qa | grep radvd

2. Descargar el RPM correspondiente de la página http://pkgs.org/
3. Copiar el archivo radvd-1.6-1.el6.i686.rpm en la dirección deseada.

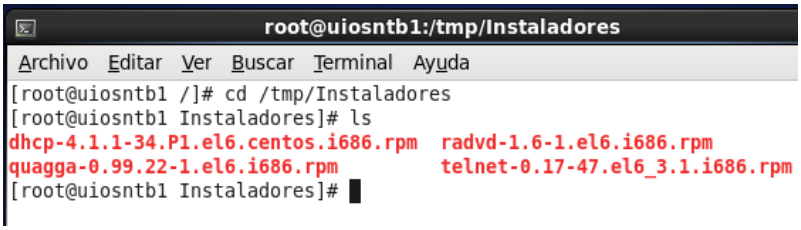
Figura 104. Radvd-1.6-1

Elaborado por: Alejandro Santamaría

4. Ejecutar el terminal de Linux como administrador o root.

5. Acceder al directorio en donde se encuentra copiado el archivo de instalación.

Figura 105. Directorio del archivo de instalación del radvd

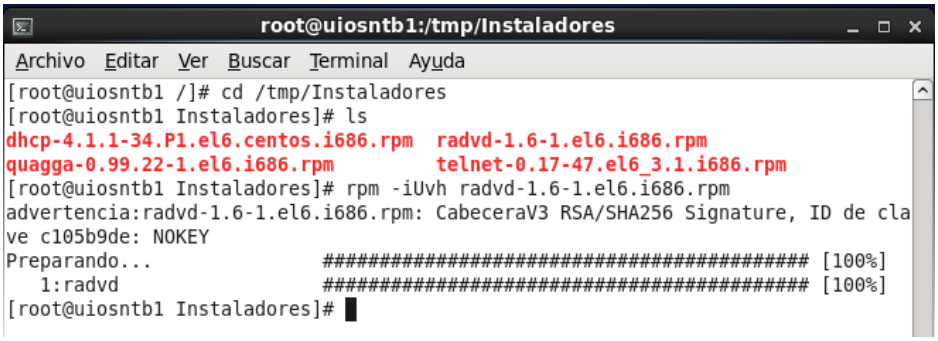


Elaborado por: Alejandro Santamaría

6. Una vez en el directorio del instalador para proceder a instalar se digita:

#rpm –iUvh radvd-1.6-1.el6.i686.rpm

Figura 106. Instalación del radvd



Elaborado por: Alejandro Santamaría

7. Finaliza la instalación si el proceso llega al 100%.

8. Modificar el archivo /etc/sysconfig/network y añadir la siguiente línea:

   IPV6FORWARDING=yes

9. Modificar el archivo /etc/radvd.conf y añadir las siguientes líneas:

```
# Interface que se conecta a la LAN
interface eth1
{
# Se envia anuncios o rutas
  AdvSendAdvert on;
# Frecuencia con que se envían los anuncios en segundos
   MinRtrAdvInterval 60;
   MaxRtrAdvInterval 180;
# Se deshabilita soporte para IPv6 móvil
   AdvHomeAgentFlag off;
# Para la configuración automática de direcciones
   AdvManagedFlag off;
# Para la configuración automática de otras direcciones
   AdvOtherConfigFlag on;
# Prefijo IPv6
   prefix 2001:470:e321:250d::/64
   {
# Indica que este prefijo puede ser usado para la determinación en el enlace
      AdvOnLink on;
# Indica que este prefijo puede ser usado para la configuración de una dirección autónoma
      AdvAutonomous on;
# Indica que la dirección de la interfaz es enviada en lugar de prefijo de red, como es requerido por Mobile IPv6
      AdvRouterAddr off;
   };
};
```

10. Modificar el archivo /etc/sysctl.conf para activar el bit de forward en IPv6 añadiendo la siguiente línea al fichero:

    #net.ipv6.conf.all.forwarding=1

11. Se procede a actualizar la configuración y se aplican los cambios de /etc/sysctl.conf inmediatamente utilizando el siguiente comando:

    #sysctl -p

12. Para que el módulo IPv6 se cargue automáticamente en el arranque se debe ejecutar el siguiente comando:

    #echo "ipv6" >> /etc/modules

13. Finalmente para iniciar el servicio radvd ejecutar el siguiente comando:

    #service radvd start o #/etc/init.d/radvd start

14. Si se desea que el servicio se ejecute cada vez que se inicia la máquina se digita:

    #chkconfig --level 35 radvd on

Para asignar las direcciones DNS mediante el software dhcpv6 se procede a instalar y configurar mediante los siguientes comandos:

1. Verificar los RPM que se necesitan instalar mediante el comando:

   #rpm –qa | grep dhcp

2. Descargar el RPM correspondiente de la página http://pkgs.org/
3. En este caso como son varios RPM a instalar se puede digitar el siguiente comando para que se instalen automáticamente:

   #yum –y install dhcp

4. Finaliza la instalación si el proceso llega al 100%.
5. Se recomienda que el servicio dhcpd6 funcione en la interfaz de red utilizada para la LAN. Editar el archivo /etc/sysconfig/dhcpd6 y agregar la interfaz de red de la siguiente manera:

   DHCPDARGS=eth1

6. Se procede a modificar el archivo de configuración /etc/dhcp/dhcpd6.conf

   # Habilita el RFC 5007
   allow leasequery;

```
# Tiempo predeterminado de vida valido para la dirección IPv6. 30 días
 default-lease-time 2592000;
# Tiempo predeterminado de vida preferente para la dirección IPv6. 7 días
 preferred-lifetime 604800;
# Demora antes de renovar. 1 hora
 option dhcp-renewal-time 3600;
# Demora antes de reconexión. 2 horas
 option dhcp-rebinding-time 7200;
# La ruta del archivo lease
 dhcpv6-lease-file-name "/var/lib/dhcpd/dhcpd6.leases";
# Establece preferencia a 255 con el fin de evitar la espera de servidores adicionales cuando solo hay uno
 option dhcp6.preference 255;
# Comandos del lado del servidor para permitir rapid-commit
 option dhcp6.rapid-commit;
# Demora antes de solicitud de información de actualización
 option dhcp6.info-refresh-time 21600;
subnet6 2001:470:e321:250d::/64 {
   range6 2001:470:e321:250d::eeff 2001:470:e321:250d::ffff;
# Direccion IPv6 del servidor de DNS
       option dhcp6.name-servers 2001:470:8:250::84c1;
# Dominio de los servidores
       option dhcp6.domain-search "santanet.net.ms";
#
}
# Llave de la empresa
key lab.santanet.net.ms {
   algorithm hmac-md5;
   secret kJwBDRaAX1BiyJuQodPGpJENqku+vA==;
}
# Zona del dominio
zone santanet.net.ms {
   key "lab.santanet.net.ms";
   primary localhost;
   }
# Zona inversa del dominio IPv4
zone 1.168.192.in-addr.arpa {    key "lab.santanet.net.ms";
   primary localhost;
   }
# Zona inversa del dominio IPv6
```

```
zone e.5.2.1.8.0.0.0.0.7.4.0.1.0.0.2.ip6.arpa {
  key "lab.santanet.net.ms";
  primary localhost;
  }
```

7. Tanto en el servidor como en el router se va a bloquear SLAAC o deshabilitar que automáticamente se obtenga direcciones IPv6 modificando el archivo /etc/sysctl.conf y agregando los siguientes comandos:

   net.ipv6.conf.all.autoconf = 0

   net.ipv6.conf.default.autoconf = 0

8. Para deshabilitar que las rutas se configuren automáticamente, se puede evitar los router advertisements modificando los siguientes parámetros en /etc/sysctl.conf:

   net.ipv6.conf.all.accept_ra = 0

   net.ipv6.conf.default.accept_ra = 0

9. Para aplicar los cambios realizados se ejecuta el siguiente comando:

   #sysctl -p

10. Se procede a iniciar el servicio dhcpd6 mediante el siguiente comando:

    #service dhcpd6 start

11. Si se desea que el servicio se ejecute cada vez que se inicia la máquina se digita:

    #chkconfig --level 35 dhcpd6 on

12. En este caso se está utilizando la configuración por defecto de iptables en CentOS, así que se debe añadir las siguientes líneas en /etc/sysconfig/ip6tables o en el script que asigna iptables, este script está más detallado en el Anexo B:

    iptables -A INPUT -i eth1 -p udp -m state --state NEW -m udp --sport 67:68 --dport 67:68 -j ACCEPT

4.5 Configuración de clientes

Prácticamente todos los sistemas operativos actuales tienen clientes de los servicios descritos anteriormente. Estos clientes en ocasiones ya están instalados por defecto o son fáciles de conseguir e instalar. A continuación se describe una breve configuración en los clientes.

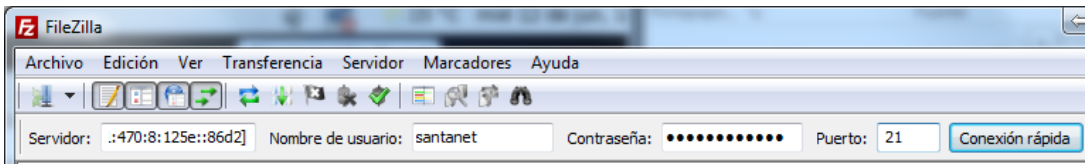
4.5.1 Cliente FTP

El cliente FTP que se va a utilizar tanto para Windows y Linux será el FileZilla, ya que es un cliente multiplataforma rápido y fiable de FTP, FTPS y SFTP. Este cliente soporta el protocolo IPv6, para su respectivo funcionamiento se debe proceder a configurar de la siguiente forma:

1. Descargar e instalar el FileZilla.
2. Iniciar el FileZilla.
3. Se procede a ingresar la información solicitada como:

- Servidor: [2001:470:8:125e::86d2]
- Usuario: santanet
- Contraseña: ***
- Puerto: 21

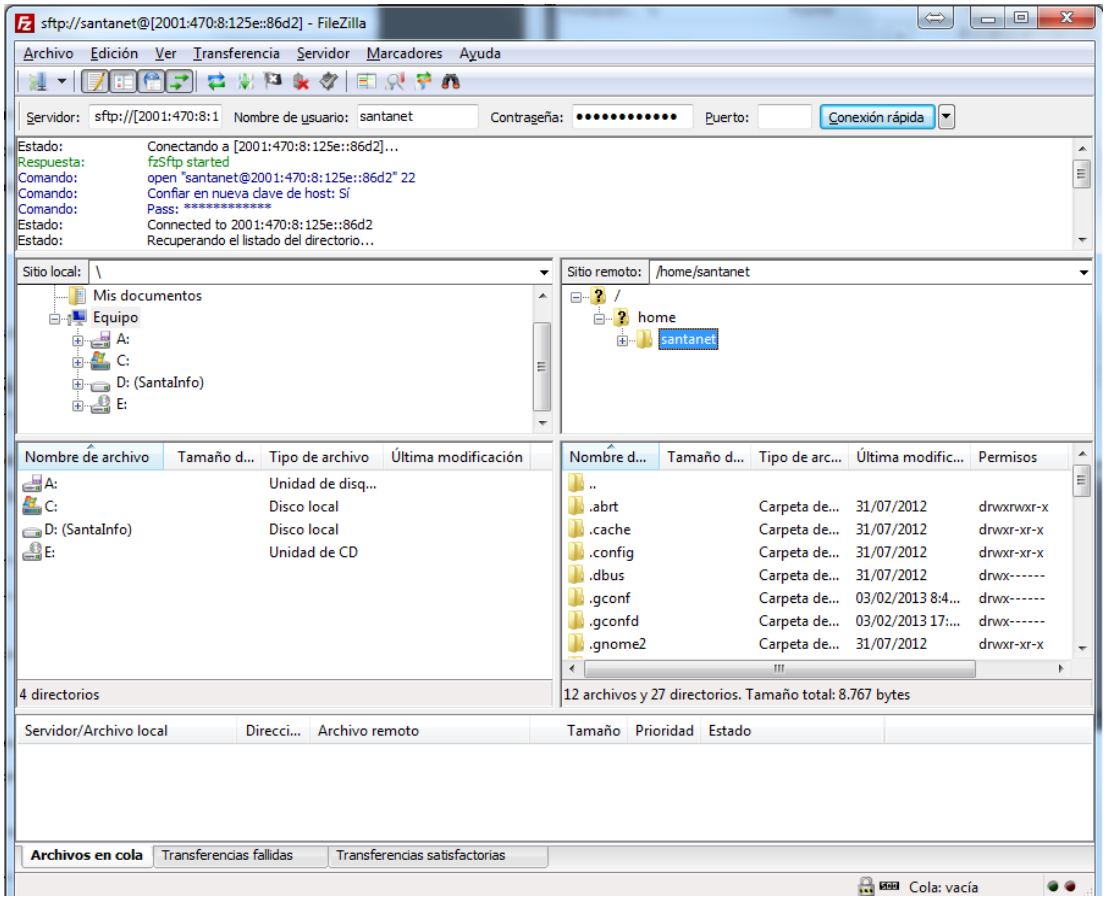
Figura 107. Conexión del FileZilla



Elaborado por: Alejandro Santamaría

4. Finalmente escoger conexión rápida y ya se tiene el cliente FTP configurado.

Figura 108. Cliente FTP configurado



Elaborado por: Alejandro Santamaría

4.5.2 Cliente web

El cliente web que se va a utilizar tanto para Windows y Linux será el Mozilla Firefox el cual soporta el protocolo IPv6, para su respectivo funcionamiento se debe proceder a configurar de la siguiente forma:

1. Abrir el Mozilla Firefox.
2. En la pestaña Configuración se procede a escoger opciones.
3. En la pestaña avanzado se procede a escoger red y luego opciones.
4. Se verifica que la configuración del proxy para salir a Internet este en auto detectar.
5. Se procede a digitar en la barra de dirección la IPv4 o www.santanet.net.ms.

6. Se procede a digitar en la barra de dirección la IPv6 entre corchetes o ipv6.santanet.net.ms.

4.5.3 Cliente de correo

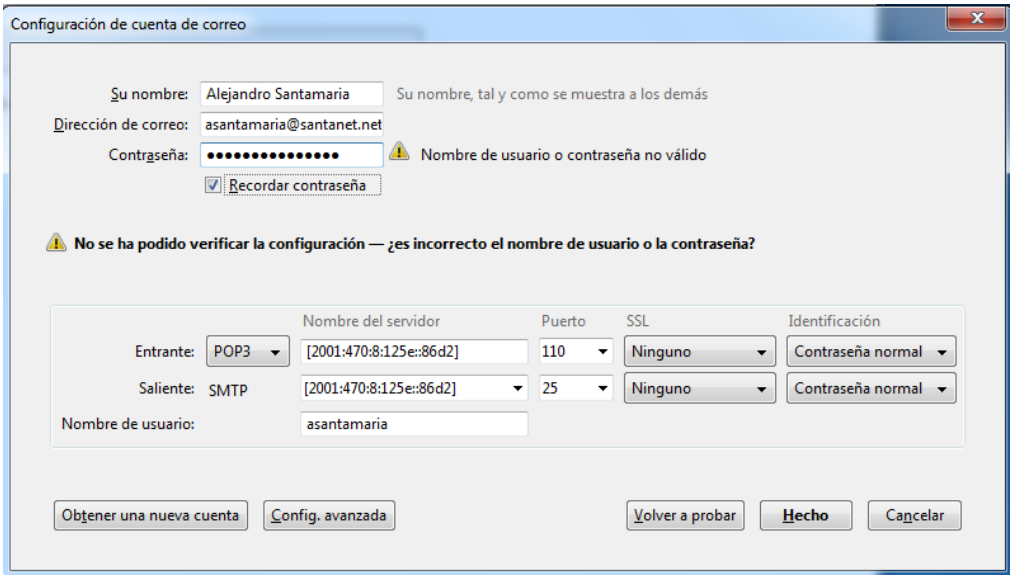
El cliente de correo que se va a utilizar tanto para Windows y Linux será el Mozilla Thunderbird que es un cliente de correo electrónico de software libre y de código abierto para recibir, enviar y almacenar correos electrónicos. Con este software se pueden administrar múltiples cuentas de correo electrónico y también soporta el protocolo IPv6, para su respectivo funcionamiento se debe proceder a configurar de la siguiente forma:

1. Descargar e instalar el Mozilla Thunderbird.
2. Iniciar el Mozilla Thunderbird.
3. Para la respectiva configuración hay que tener en cuenta:

- El servidor de correo entrante y el puerto.
- El servidor de correo saliente y el puerto
- Las opciones de seguridad necesarias para la conexión con el servidor.

4. Crear una cuenta nueva.
5. Escoger configuración manual e ingresar la información solicitada. En servidor de correo entrante escoger POP3.

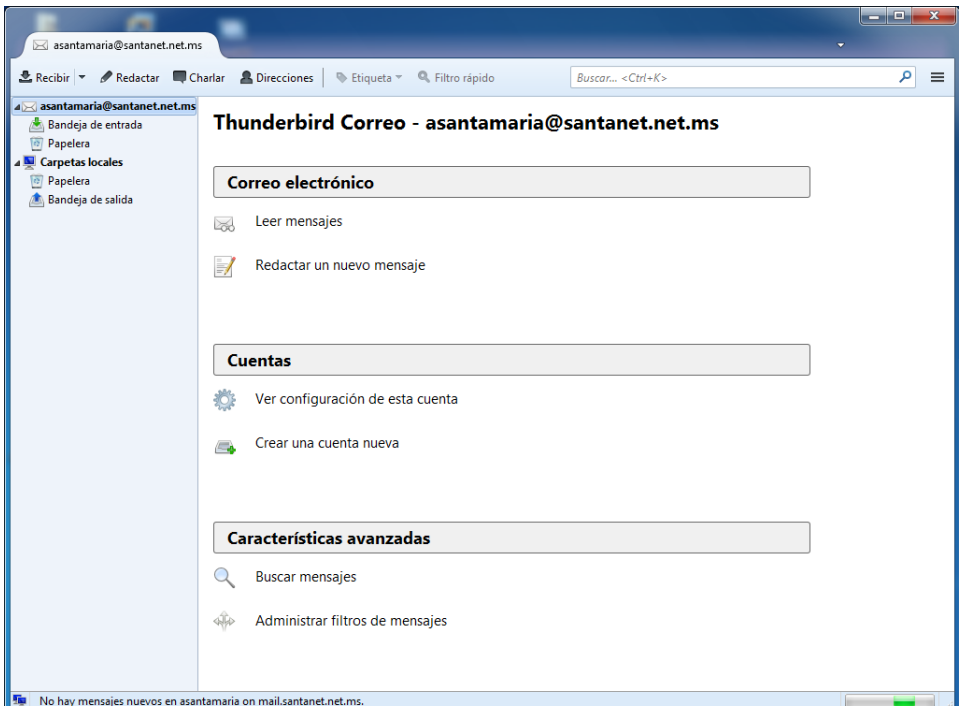
Figura 109. Configuración de cuenta de correo



Elaborado por: Alejandro Santamaría

6. Una vez ingresada la información solicitada se tiene la cuenta configurada correctamente.

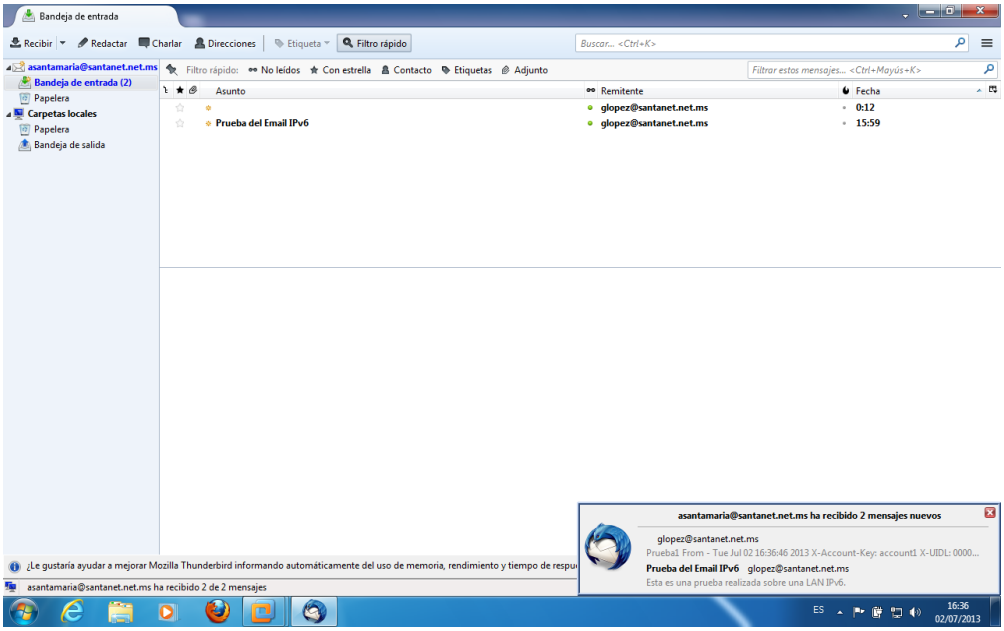
Figura 110. Cuenta de correo en Thunderbird



Elaborado por: Alejandro Santamaría

7. Finalmente se procede a enviar y recibir correos electrónicos.

Figura 111. Bandeja de entrada en Thunderbird



Elaborado por: Alejandro Santamaría

También se tiene configurado el SquirrelMail que es una aplicación webmail que es compatible con la mayoría de servidores web. SquirrelMail está diseñado para trabajar con plugins para agregar nuevas características a la aplicación.

Para utilizar al webmail configurado en el servidor se procede a ingresar mediante los siguientes pasos:

1. Abrir cualquier navegador web.
2. Digitar la dirección IPv4 e IPv6 del servidor de correos o el dominio seguido de la palabra webmail de la siguiente forma:

   http://192.168.1.20/webmail/

   http://[2001:470:8:125e::86d2]/webmail

   http://www.santanet.net.ms/webmail
3. Ingresar el usuario y la clave respectiva para autenticarse.
4. Finalmente se puede enviar, recibir, guardar y borrar mensajes de la cuenta de correo.

4.5.4 Cliente DNS

Para establecer el DNS manualmente en los clientes solo hay que agregar la IP del servidor de nombres de dominio o DNS a la configuración de red.

1. Cuando se desee configurar manualmente las direcciones del servidor DNS en Linux se procede a modificar el archivo /etc/resolv.conf y agregar las siguientes líneas:

   nameserver 192.168.1.20

   nameserver 2001:470:8:125e:86d2

4.6 Configuración de QoS

Los pasos para la compilación de un nuevo kernel se deben ejecutar como root y previamente tener instalados algunos paquete de desarrollo como gcc, make.

Antes de comenzar a utilizar iptables para configurar el firewall se debe configurar el kernel adecuadamente para que soporte el filtrado, QoS y otras opciones.

1. Para saber que versión del núcleo tiene el equipo se utiliza el comando:

   #uname -sr

2. Descargar la última versión del kernel desde https://www.kernel.org/
3. Descomprimir el archivo descargado y copiar en la dirección /usr/src/.
4. Crear un enlace simbólico llamado linux a dicho directorio mediante:

   #ln –s linux-3.9.7 linux

5. Ingresar al directorio /usr/src/linux y ejecutar cualquiera de los siguientes comandos para poder configurar el kernel:

   #make menuconfig

   #make xconfig

   #make config

   Para poder visualizar el menú de configuración es necesario tener instaladas las librerías ncurses.

6. Se procede a configurar las opciones del kernel. En general se pondrá en el kernel las funcionalidades que se necesitan habitualmente y como módulos lo que se utiliza ocasionalmente.
7. Para configurar Netfilter en la configuración del kernel ir a Networking Support, Networking Options, Network Packet Filtering framework (Netfilter), IPv6: Netfilter Configuration y seleccionar todas las opciones.
8. Para configurar QoS en la configuración del kernel ir a Networking Support, Networking Options, QoS and/or fair queueing.
9. Guardar la configuración en el archivo .config y salir del programa.
10. Para compilar el kernel se ejecuta el comando:

    #make

11. Una vez compilado el kernel se procede con los módulos mediante:

    #make modules_install

12. Para instalar la imagen del kernel en el directorio apropiado se ejecuta::

    #make install

13. Para crear un disco duro virtual necesario para el arranque se ejecuta:

    #mkinitrd /boot/initrd-3.9.7.img 3.9.7

14. Por último se actualiza el fichero de configuración del gestor de arranque si es LILO **/etc/lilo.conf** y si es GRUB **/boot/grub/menu.lst** y añadir la entrada:

    title CentOS (3.9.7)

    root (hd0,1)

    kernel /boot/vmlinuz-3.9.7 ro root=/dev/VolGroup00/LogVol00

    initrd /boot/initramfs-3.9.7.img

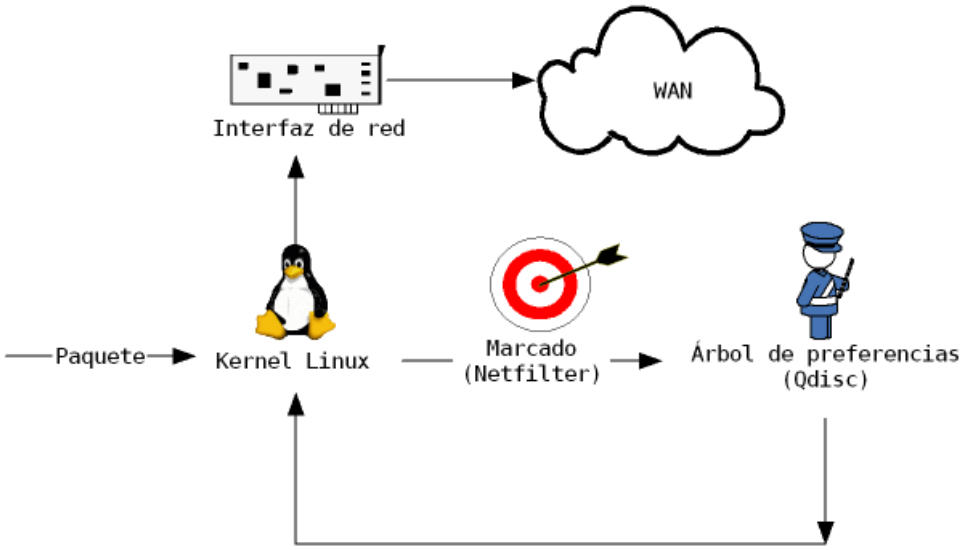
15. Por último se procede a reiniciar el equipo mediante el comando:

    #shutdown –r now

4.7 Implementación de QoS

Para proceder a la implementación de QoS en donde se va a gestionar el ancho de banda, se procede a explicar en el siguiente gráfico cual es el recorrido de un paquete desde que se genera en el router PC hasta que sale a otra red.

Figura 112. Diagrama de paquetes con disciplinas de cola



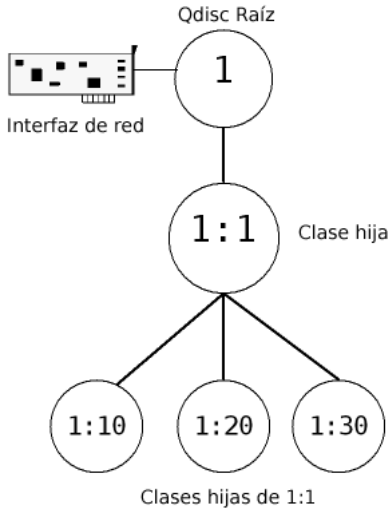
Fuente: (K-nabora Bufete Tecnológico, 2013)

4.7.1 Árbol de preferencias o qdisc

Aquí es donde reside el corazón del mecanismo de control de tráfico. Con el encolamiento se determina como se envían los datos, mediante el uso de disciplinas de cola.

Las disciplinas de cola siguen una estructura jerárquica en árbol. Cada interfaz de red tiene una qdisc raíz. A cada qdisc se le asigna un controlador que tiene dos partes, la primera parte se utiliza para referenciar la raíz de una clase y la segunda parte se utiliza para referenciar a cualquier clase que desciende de la raíz padre. Las clases deben tener la primer parte idéntica a su padre y la segunda parte debe ser única (K-nabora Bufete Tecnológico, 2013).

Figura 113. Ejemplo de árbol de preferencias



Fuente: (K-nabora Bufete Tecnológico, 2013)

Según el ejemplo las clases 1:10, 1:20, 1:30 son las que recibirán los paquetes. En cada una de ellas se puede establecer políticas diferentes. Por defecto en cada clase se asocia una qdisc FIFO-First In First Out (Primera en Entrar Primera en Salir).

El actual kernel de Linux viene con una serie de características que permiten realizar un control avanzado del tráfico aplicando QoS. Se podrá encontrar dos protocolos que realizan dicha tarea: Diffserv y RSVP, aunque se basara en otras características.

4.7.2 El comando TC-Traffic Control

El comando TC es una herramienta que viene incluida en el paquete iproute2, utilizando este comando se crea el árbol de preferencias.

Entre las principales sentencias a utilizar se tiene:

- Para gestionar qdisc.

tc qdisc [add | change | replace | link] dev [parent qdisc-id | root] [handle qdisc-id] qdisc [qdisc specific parameters]

- Para gestionar las clases.

tc class [add | change | replace] dev DEV parent qdisc-id [classid class-id] qdisc [qdisc specific parameters]

- Para gestionar los filtros.

tc filter [add | change | replace] dev DEV [parent qdisc-id | root] protocol protocol prio priority filtertype [filtertype specific parameters] flowid flow-id

- Para mostrar las qdiscs:

tc [-s | -d] qdisc show [dev DEV]

- Para mostrar el tráfico de las clases:

tc [-s | -d] class show dev DEV

- Para mostrar los filtros:

tc filter show dev DEV

4.7.3 Creación del árbol de preferencias

Para crear el árbol de preferencias se procede de la siguiente manera:

1. Utilizando el siguiente cuadro se va a realizar un script en donde se creen clases, tomando en cuenta la aplicación y el ancho de banda del tráfico de subida.

Tabla 14. Aplicaciones y su respectivo ancho de banda

Aplicación	Ancho de banda
HTTP, HTTPS	200
FTP	150
POP3, IMAP	150
SMTP	150
SSH	100
Otro tráfico	250

Elaborado por: Alejandro Santamaría

2. Se genera las clases deseadas tomando en cuenta el uso de cada aplicación por los usuarios, el ancho de banda y la prioridad de cada aplicación. Cuanto menor es el índice prio, mayor es la prioridad y por defecto prio siempre es 0, por lo cual si no se especifica nada se crea una clase con la prioridad más alta.

Tabla 15. Clases a crear

Clase	Aplicación	Ancho de banda	Prioridad
80	HTTP, HTTPS	200	0
21	FTP	150	1
22	POP3, IMAP	150	2
25	SMTP	150	3
110	SSH	100	4
100	Otro tráfico	250	5

Elaborado por: Alejandro Santamaría

3. Se crea la qdisc raíz, esta es la principal y siempre debe estar presente. La tarjeta de red a la cual va estar asociada la qdisc es la Eth0 que tiene salida a Internet.

   tc qdisc add dev eth0 root handle 1: htb default 13

   Se crea la banda principal root con nombre 1 y por defecto enviara paquetes a la clase 13.

4. Se procede a crear la clase hija o clase intermedia 1:1 debido que la qdisc raíz no puede prestar ancho de banda si sobra. La clase hija es dependiente de root y utiliza el algoritmo htb, mediante rate se hace referencia al mínimo garantizado y mediante ceil al máximo posible:

   tc class add dev eth0 parent 1: classid 1:1 htb rate 1000kbit ceil 1000kbit

5. Se procede a crear las clases del anterior cuadro tomando en cuenta la clase, el ancho de banda y la prioridad:

   tc class add dev eth0 parent 1:1 classid 1:80 htb rate 200kbit ceil 1000kbit prio 1

   tc class add dev eth0 parent 1:1 classid 1:21 htb rate 150kbit ceil 1000kbit prio 2

   tc class add dev eth0 parent 1:1 classid 1:22 htb rate 150kbit ceil 1000kbit prio 3

tc class add dev eth0 parent 1:1 classid 1:25 htb rate 150kbit ceil 1000kbit prio 4

tc class add dev eth0 parent 1:1 classid 1:110 htb rate 100kbit ceil 1000kbit prio 5

tc class add dev eth0 parent 1:1 classid 1:100 htb rate 250kbit ceil 1000kbit prio 6

6. Crear qdisc SFQ para cada una de las clases y así lograr que todas las conexiones tengan las mismas oportunidades de salir a la red deseada:

tc qdisc add dev eth0 parent 1:80 handle 80: sfq perturb 10

tc qdisc add dev eth0 parent 1:21 handle 21: sfq perturb 10

tc qdisc add dev eth0 parent 1:22 handle 22: sfq perturb 10

tc qdisc add dev eth0 parent 1:25 handle 25: sfq perturb 10

tc qdisc add dev eth0 parent 1:110 handle 110: sfq perturb 10

tc qdisc add dev eth0 parent 1:100 handle 100: sfq perturb 10

7. Se procede a crear los filtros de la qdisc.

tc filter add dev eth0 protocol ip parent 1: prio 1 handle 80 fw classid 1:80

tc filter add dev eth0 protocol ip parent 1: prio 2 handle 21 fw classid 1:21

tc filter add dev eth0 protocol ip parent 1: prio 3 handle 22 fw classid 1:22

tc filter add dev eth0 protocol ip parent 1: prio 4 handle 25 fw classid 1:25

tc filter add dev eth0 protocol ip parent 1: prio 5 handle 110 fw classid 1:110

tc filter add dev eth0 protocol ip parent 1: prio 6 handle 100 fw classid 1:100

8. Se procede a crear las reglas de marcado de cada uno de los paquetes mediante iptables.

##Para servidor Web, puerto 80

iptables -t mangle -A PREROUTING -p tcp --dport 80 -j MARK --set-mark 80

iptables -t mangle -A PREROUTING -p tcp --dport 80 -j RETURN

##Para servidor VSFTPD, puerto 21

iptables -t mangle -A PREROUTING -p tcp --dport 21 -j MARK --set-mark 21

iptables -t mangle -A PREROUTING -p tcp --dport 21 -j RETURN

##Para servidor SSH, puerto 22

iptables -t mangle -A PREROUTING -p tcp --dport 22 -j MARK --set-mark 22

iptables -t mangle -A PREROUTING -p tcp --dport 22 -j RETURN

##Para servidor de correo, puerto 25

iptables -t mangle -A PREROUTING -p tcp --dport 25 -j MARK --set-mark 25

iptables -t mangle -A PREROUTING -p tcp --dport 25 -j RETURN

##Para servidor de correo, puerto 110

iptables -t mangle -A PREROUTING -p tcp --dport 110 -j MARK --set-mark 110

iptables -t mangle -A PREROUTING -p tcp --dport 110 -j RETURN

##Para cualquier otro tráfico IPv4 e IPv6

iptables -t mangle -A PREROUTING -j MARK --set-mark 100

ip6tables -t mangle -A PREROUTING -j MARK --set-mark 100

ip6tables -t mangle -A OUTPUT -j MARK --set-mark 100

4.8 Pruebas y Resultados

Para las respectivas pruebas de los servicios configurados se va a utilizar varias herramientas que disponen los diferentes sistemas operativos. Para las respectivas conexiones hacia el servidor se puede digitar la IPv6 2001:470:8:125e::86d2 o los nombres asociados al servidor como por ejemplo uiosnts1.santanet.net.ms.

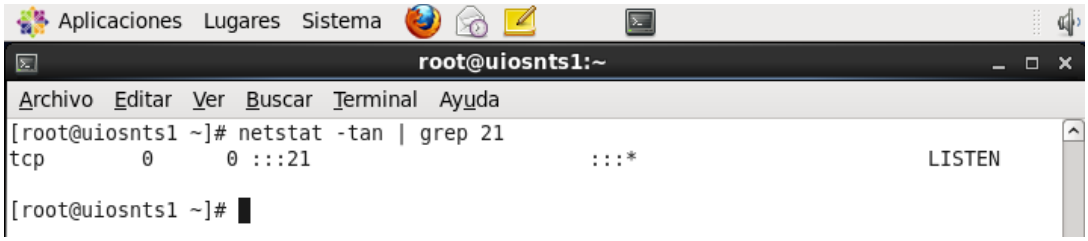
4.8.1 Prueba del servidor FTP

Para realizar pruebas hacia el servidor FTP se puede seguir los siguientes pasos:

1. En el servidor se verifica que los puertos estén abiertos y escuchando.

   #netstat –tan | grep 21

Figura 114. Puertos del servidor FTP

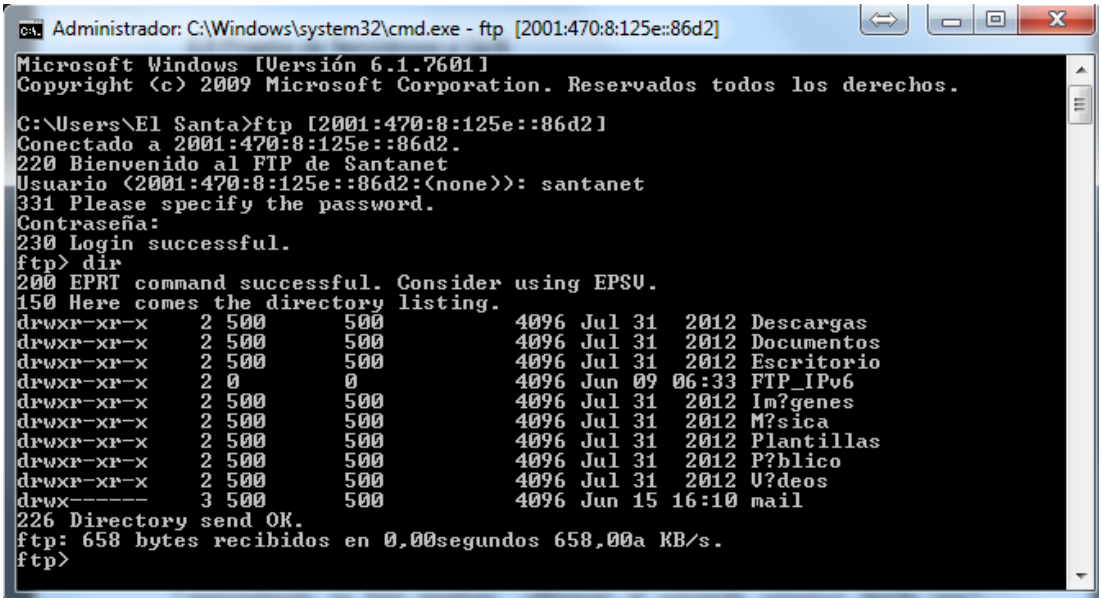


Elaborado por: Alejandro Santamaría

2. Al digitar el comando se verifica que está abierto y escuchando el puerto 21 como se observa en la figura 114.
3. Para verificar el servicio desde los clientes se puede utilizar el símbolo del sistema que tiene incluido Windows o el terminal de Linux.
4. Tanto para Windows o Linux se puede utilizar el siguiente comando:

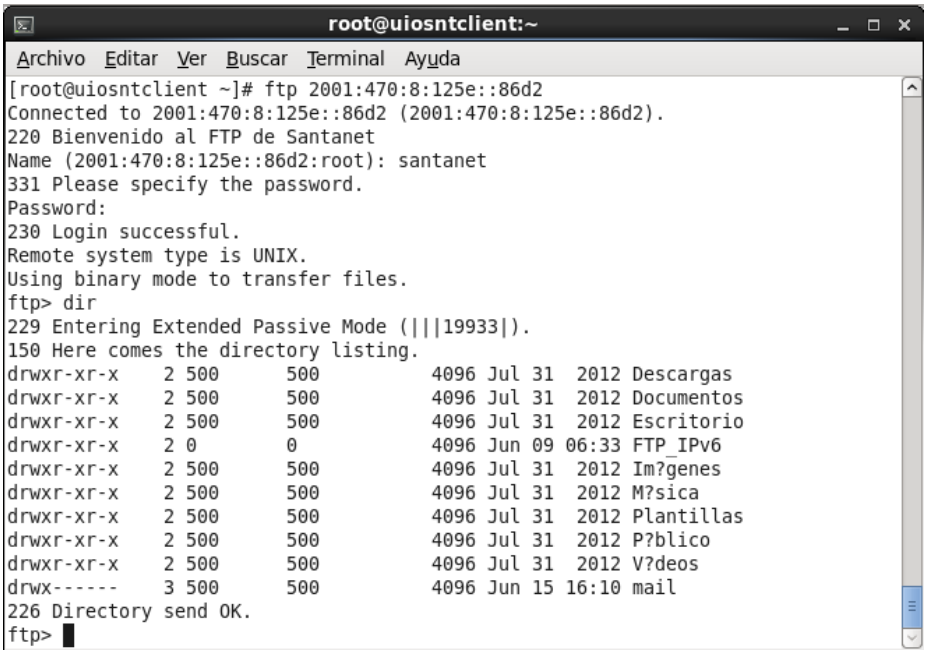
   ftp 2001:470:8:125e::86d2

Figura 115. FTP en Windows



Elaborado por: Alejandro Santamaría

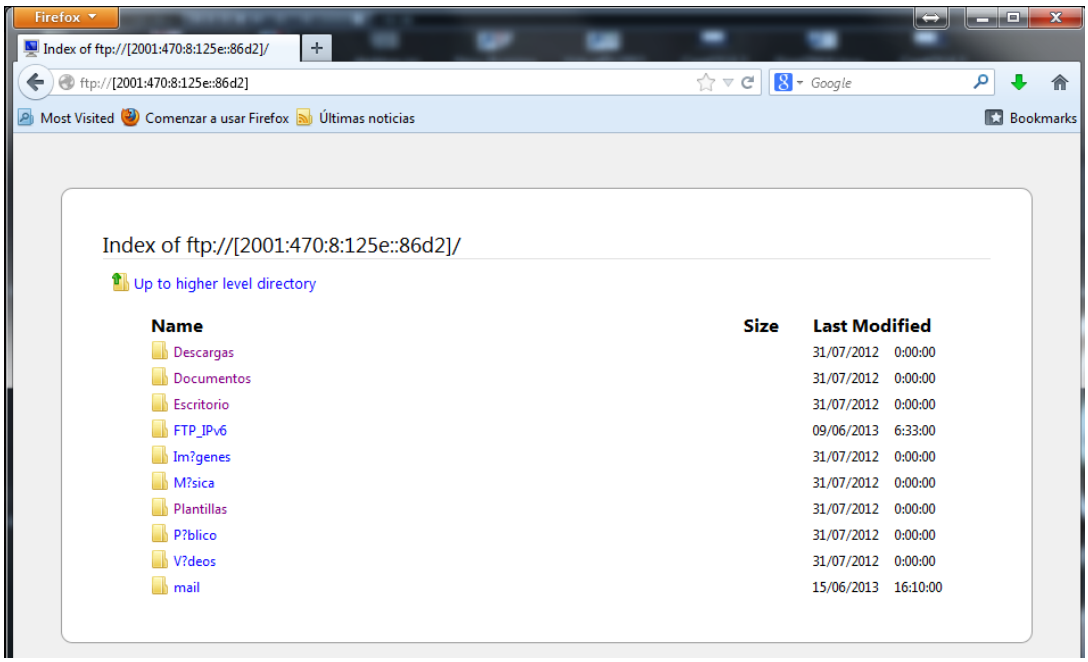
Figura 116. FTP en Linux



Elaborado por: Alejandro Santamaría

5. Otra forma de probar el servidor ftp es mediante un browser, solamente digitando ftp://[2001:470:8:125e::86d2] e ingresando la información solicitada para ingresar.

Figura 117. FTP en navegador web



Elaborado por: Alejandro Santamaría

En las respectivas pruebas del servidor FTP se pudo comprobar que escucha en el puerto 21 y que mediante comandos o interfaz gráfica se puede comunicar con el servidor para enviar y recibir archivos. Los resultados obtenidos en las pruebas son los deseados ya que el servicio está abierto, escuchando y funcionando.

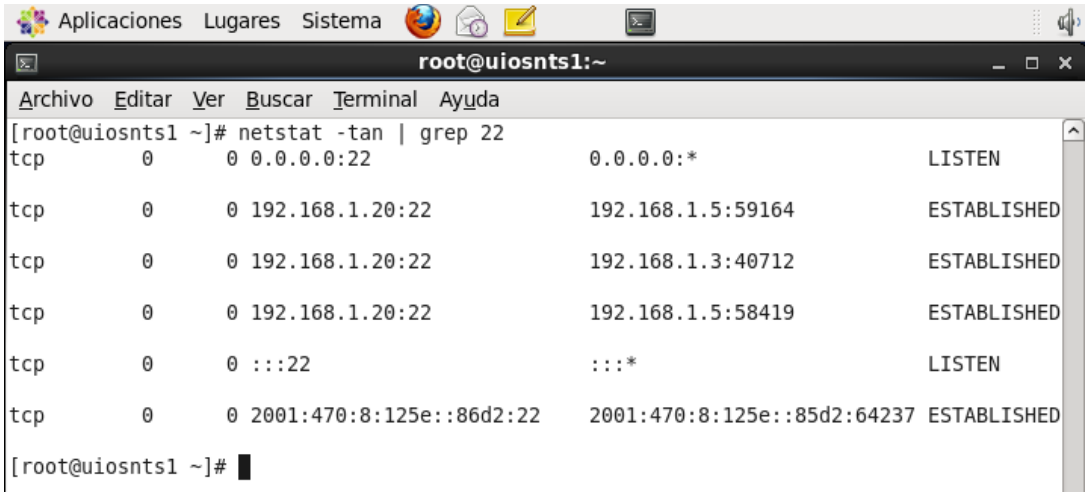
4.8.2 Prueba del servidor SSH

Para realizar pruebas hacia el servidor SSH se puede seguir los siguientes pasos:

1. En el servidor se verifica que el puerto 22 este abierto y escuchando mediante el siguiente comando:

   #netstat –tan | grep 22

Figura 118. Puertos del servidor SSH



Elaborado por: Alejandro Santamaría

2. Se puede observar en la figura 118 que el puerto 22 está abierto y escuchando tanto para IPv4 e IPv6. Además se observa que existen conexiones activas a este puerto.

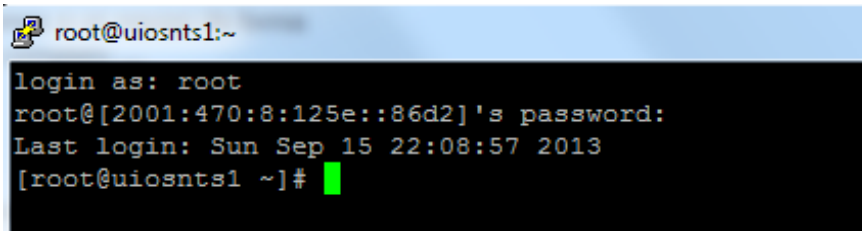
3. Para realizar una conexión SSH se puede utilizar el símbolo del sistema que tiene incluido Windows, el terminal de Linux o también algún software para conectarse de manera remota por SSH.

4. Tanto para Windows o Linux se puede utilizar el siguiente comando:

   ssh 2001:470:8:125e::86d2

5. Ingresar el usuario y la password del servidor SSH.

Figura 119. Conexión al Servidor SSH



Elaborado por: Alejandro Santamaría

6. Finalmente se logra acceder desde cualquier PC al servidor SSH y se puede trabajar como si se estuviera en el servidor.

En las respectivas pruebas del servidor SSH se pudo comprobar que escucha en el puerto 22 tanto para IPv4 e IPv6 y que mediante cualquier cliente SSH se puede realizar la comunicación. Los resultados obtenidos en las pruebas realizadas son los deseados, ya que se puede conectar satisfactoriamente al servidor en donde se encuentra configurado el servicio SSH.

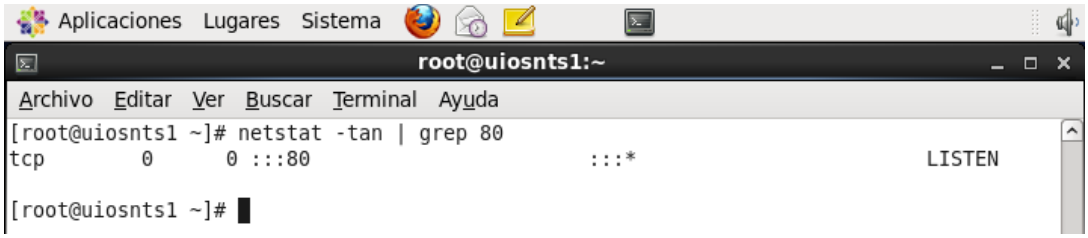
4.8.3 Prueba del servidor web

Para realizar pruebas hacia el servidor web se puede seguir los siguientes pasos:

1. En el servidor se verifica que el puerto 80 este abierto y escuchando.

   #netstat –tan | grep 80

Figura 120. Puertos del servidor web



Elaborado por: Alejandro Santamaría

2. Como se puede observar en la figura 120 el servicio HTTP en el puerto 80 está abierto y escuchando tanto para IPv4 e IPv6.

3. Para comprobar que la página está funcionando en el equipo cliente se puede digitar la dirección IPv4 200.107.48.98, la dirección IPv6 [2001:470:8:125e::86d2] o el nombre de la página web que es santanet.net.ms.

En las respectivas pruebas del servidor web se pudo comprobar que escucha en el puerto 80 tanto para IPv4 e IPv6 y que mediante cualquier explorador web se puede conectar a la página respectiva de la empresa santanet. Los resultados obtenidos en las pruebas realizadas son los deseados. Desde cualquier parte que se tenga acceso a Internet se puede digitar tanto la IPv4 e IPv6 y se puede observar la página de la empresa.

4.8.4 Prueba del servidor de correo

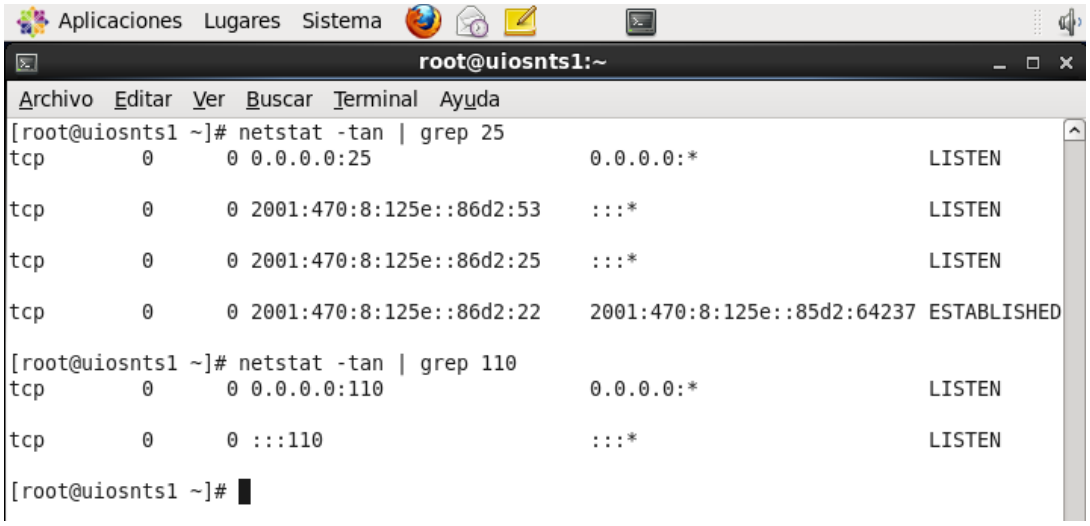
Para realizar pruebas en el servidor de correos se puede seguir los siguientes pasos:

1. En el servidor se verifica que los puertos 25 y 110 estén abiertos y escuchando.

   #netstat –tan | grep 25

   #netstat –tan | grep 110

Figura 121. Puertos del servidor de correos



Elaborado por: Alejandro Santamaría

2. Como se observa en la imagen 123 el puerto 25 y el puerto 110 están abiertos y escuchando tanto para IPv4 e IPv6.

3. Para realizar las respectivas pruebas del SMTP se utilizará el cliente telnet. Se procede a realizar la conexión con el servidor mediante:

   #telnet 2001:470:8:125e::86d2 25

4. A continuación se deben ingresar cada línea por separado con los siguientes comandos :

   HELO uiosnts1.santanet.net.ms

   MAIL FROM: <root@santanet.net.ms>

   RCPT TO: <santanet2009@santanet.net.ms>

   DATA

   Hola. Este es un mensaje de prueba.

   .

   QUIT

5. Si los anteriores comandos se ejecutan satisfactoriamente quiere decir que el servicio SMTP está configurado y funcionando correctamente.

6. Para realizar las respectivas pruebas del POP3 se utilizará el cliente telnet. Se procede a realizar la conexión con el servidor mediante:

   #telnet 2001:470:8:125e::86d2 110

7. A continuación se deben ingresar cada línea por separado con los siguientes comandos :

   USER santanet

   PASS *

   STAT

   LIST

   RETR 1

   QUIT

8. Si los anteriores comandos se ejecutan satisfactoriamente quiere decir que el servicio POP3 se encuentra configurado y funcionando correctamente.

9. Para realizar las respectivas pruebas del IMAP se utilizará el cliente telnet. Se procede a realizar la conexión con el servidor mediante:

#telnet 2001:470:8:125e::86d2 143

10. A continuación se deben ingresar cada línea por separado con los siguientes comandos :

    1 LOGIN santanet *

    2 SELECT inbox

    3 FETCH 1 (flags body[header.fields (subject)])

    4 FETCH 1 (body[text])

    5 LOGOUT

11. Si los anteriores comandos se ejecutan satisfactoriamente quiere decir que el servicio IMAP se encuentra configurado y funcionando correctamente.

En las respectivas pruebas de los servidores de correo se pudo comprobar que escuchan en los puertos 25, 110 tanto para IPv4 e IPv6 y que mediante varias aplicaciones se puede enviar y recibir los correos electrónicos del dominio, al utilizar el webmail es mucho más amigable y con el uso de un explorador web se puede usar el correo sin previa configuración, para mayor detalle se puede revisar la página 129.

Los resultados obtenidos en las pruebas realizadas son los deseados, el correo funciona mediante comandos y mediante aplicaciones, se puede enviar y recibir correos de los usuarios del dominio sin problemas.

4.8.5 Prueba del servidor DNS

Para realizar pruebas en el servidor DNS se puede seguir los siguientes pasos:

1. En el servidor se verifica que el puerto 53 este abierto y escuchando.

   #netstat –tan | grep 53

2. Para realizar pruebas hacia el servidor DNS se puede utilizar las siguientes herramientas de consulta al servidor DNS.

   - Dig. Permite comprobar tanto el mapeo de nombres a IPs, como el mapeo inverso de IPs a nombres. Para comprobar el DNS IPv4 e IPv6 mediante dig digitar:

#dig uiosnts1.santanet.net.ms

#dig –t AAAA uiosnts1.santanet.net.ms

Para comprobar zona inversa del DNS mediante dig digitar:

#dig –x 192.168.1.20

#dig –x 2001:470:8:125e::86d2

- Host. El comando host se usa para encontrar la dirección IP del dominio dado y también muestra el nombre del dominio para la IP dada. Para comprobar el DNS IPv4 e IPv6 mediante host digitar:

  #host uiosnts1.santanet.net

- Nslookup. Es un programa, utilizado para saber si el DNS está resolviendo correctamente los nombres a las IP. Para comprobar el DNS mediante nslookup digitar:

  #nslookup uiosnts1.santanet.net.ms

  #nslookup –type=AAAA uiosnts1.santanet.net.ms

  Para comprobar zona inversa del DNS mediante host digitar:

  #host 192.168.1.20

  #host 2001:470:8:125e::86d2

En las respectivas pruebas del servidor DNS se pudo comprobar que el dominio creado santanet.net.ms está respondiendo a las peticiones. Los resultados obtenidos en las pruebas realizadas son las esperadas, ya que el DNS resuelve nombres tanto para IPv4 e IPv6. Al digitar nombres de las páginas u otros servicios resuelve correctamente según la configuración del DNS.

4.8.6 Prueba del servidor DHCP

Para comprobar que el servidor DHCP funciona correctamente y asigna direcciones IPv6 se puede seguir los siguientes pasos:

1. En cualquier cliente de la empresa se procede a verificar las direcciones IP asignadas.

- En Windows se puede digitar el comando:

  #ipconfig

- En Linux se puede digitar el comando:

  #ifconfig

En las respectivas pruebas del servidor DHCP se pudo comprobar que asigna direcciones IPv6 y que automáticamente tienen salida a Internet mediante el túnel creado. Los resultados obtenidos de las pruebas realizadas son las esperadas, ya que al conectar cualquier equipo a la LAN de la empresa Santanet se configura automáticamente la configuración IP y sin mayor novedad se puede navegar.

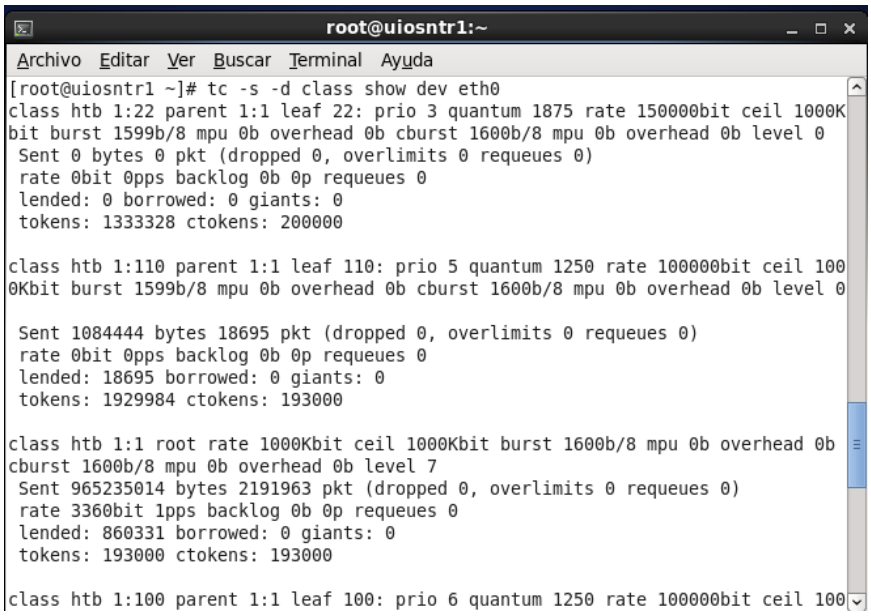
4.8.7 Prueba de QoS

Para comprobar que QoS funciona correctamente y se está aplicando el control de tráfico se va a utilizar las herramientas de TC y se procede de la siguiente manera:

1. Para ver el tráfico en las clases se puede utilizar el comando:

   #tc -s -d class show dev eth0

Figura 122. Tráfico en las clases



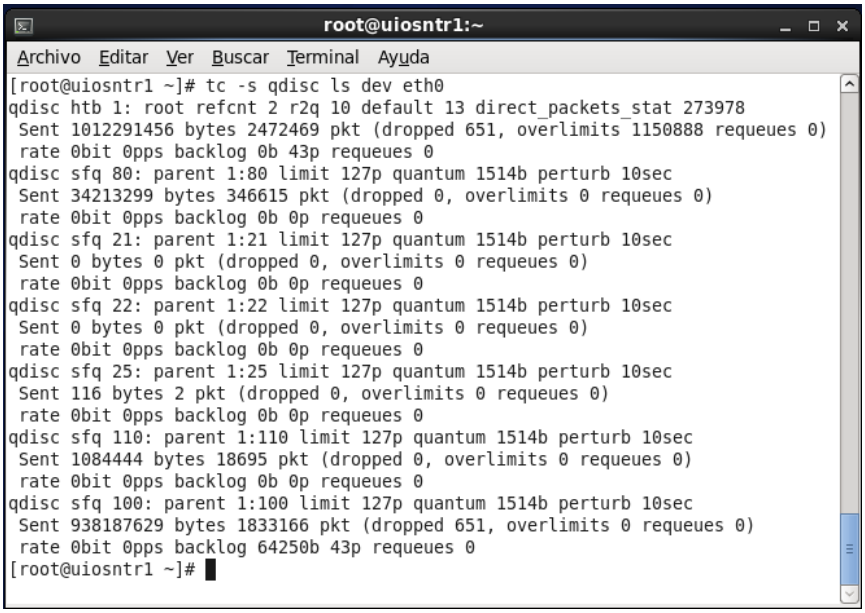
Elaborado por: Alejandro Santamaría

2. Como se puede observar en la figura 122 las clases se dividen según los puertos y en este caso la que mayor tráfico tiene es la clase principal.

3. Para ver el tráfico de las qdiscs se puede utilizar el comando:

   #tc -s qdisc ls dev eth0

Figura 123. Tráfico de las qdiscs



Elaborado por: Alejandro Santamaría

4. Como se observa en la figura 123 el qdisc que mayor tráfico tiene es el principal.

En las respectivas pruebas de QoS se pudo comprobar que mediante el filtro e iptables se controla el tráfico IPv4 e IPv6 y se asigna un respectivo ancho de banda en base a las prioridades y al uso de cada aplicación.

Los resultados obtenidos en las pruebas realizadas son los esperados debido que al utilizar las herramientas de TC se puede observar que el tráfico se clasifica según la aplicación y el ancho de banda asignado. Al priorizar las aplicaciones se optimiza el uso del Internet y por tanto el tráfico de la empresa Santanet.

CONCLUSIONES

En el análisis, diseño e implementación del protocolo IPv6 es muy importante tener el conocimiento previo del mismo. Mediante la descripción de las principales características, ventajas y desventajas se pudo obtener una idea más clara y así utilizar esta información para su respectivo y correcto funcionamiento.

La empresa Santanet mantendrá el Hardware de los equipos que funcionan con el protocolo IPv4, en estos equipos puede funcionar el protocolo IPv6 debido a que también trabaja en la capa de enlace del modelo OSI. Para el correcto funcionamiento del protocolo IPv6 se requiere Hardware adicional como un servidor y un router compatibles con IPv6.

El Software de la empresa Santanet en determinados equipos fue cambiado o actualizado para poder configurar el protocolo IPv6 correctamente.

El conocimiento de las características de la red implementada en IPv4 facilitó el diseño de la LAN para el protocolo IPv6, el mismo que utiliza el túnel 6in4 de Hurricane Electric para proveer direcciones IPv6 que van a ser asignadas a los respectivos equipos de la LAN, se utiliza un prefijo 64 para el dispositivo final que va a funcionar como router y mediante DHCPv6 o radvd se va a asignar direcciones IPv6 con prefijo 48 a los demás equipos o redes internas.

Al realizar las pruebas de control de tráfico en la empresa Santanet se observa que los resultados son los esperados, ya que se controla el ancho de banda según las aplicaciones y las prioridades asignadas en los filtros de QoS.

Para la respectiva implementación de la LAN se solicitó al ISP una dirección IP pública fija para poder utilizar el túnel 6to4, ya que este provee direcciones IPv6 en base a la IPv4 pública, pero debido al uso y eficiencia se decidió utilizar el túnel 6in4. Mediante el túnel 6in4 se provee las direcciones IPv6 para los respectivos servicios a configurar en la empresa Santanet. Entre los ejemplos de configuración para crear el túnel 6in4 de Hurricane Electric se utiliza la opción Linux-net-tools debido a que se

realiza un enlace entre el PC router y la dirección destino. Este método funciona a pesar de tener habilitado NAT en el router ADSL.

Para el QoS de la LAN se utiliza el control de tráfico tanto para IPv4 e IPv6, pero el control se lo realiza en base a los puertos que utiliza cada aplicación y así determinar el ancho de banda respectivo. Para otros puertos que no se encuentren configurados se asigna un determinado ancho de banda compartido tanto para IPv4 e IPv6.

La configuración de los servicios del protocolo IPv6 es similar a la configuración IPv4, ya que para determinados servicios solamente se necesita cambiar la dirección IP y modificar ciertos parámetros. Al documentar paso a paso la configuración de los servicios tanto para IPv4 e IPv6 se apoya al progreso y desarrollo de aplicaciones DualStack.

Es importante ejecutar pruebas de los servicios IPv6 configurados desde estaciones de trabajo con diferentes sistemas operativos, para determinar mediante los resultados obtenidos si los servicios están correctamente configurados y funcionando. Todas las pruebas desarrolladas en la empresa Santanet son ampliamente adaptables para proyectos de gran tamaño, ya que la aplicación de IPv6 es la misma.

RECOMENDACIONES

Para implementar una LAN con IPv6 se recomienda conocer la topología física y lógica de la red IPv4, ya que en base a esta se va a realizar el respectivo diseño en el cual se verifica si se debe adquirir, mantener o cambiar ciertos dispositivos.

Si se va a tener múltiples redes internas en una implementación se recomienda utilizar un prefijo 48 para que los equipos de estas redes puedan salir hacia Internet con IPv6.

Se recomienda actualizar el SO de los equipos a utilizar en una implementación a su última versión, debido a que los desarrolladores actualmente trabajan tanto para IPv4 e IPv6.

Realizar un mapeo de puertos o crear una zona desmilitarizada para que se pueda acceder a los servidores IPv4 desde cualquier sitio debido a que el router ADSL tiene habilitado por defecto NAT.

Se recomienda ejecutar las configuraciones y servicios respectivos al iniciar el SO para de esta manera evitar iniciarlos manualmente.

Utilizar servicios que sean Dual-Stack para que funcionen tanto en IPv4 e IPv6, debido que la transición entre estos protocolos tomará mucho tiempo.

Impulsar las iniciativas de implementar el protocolo IPv6 tanto en empresas públicas como privadas y utilizar este proyecto como guía para las futuras implementaciones.

LISTA DE REFERENCIAS

Acosta, D. R. (Mayo de 2013). *Algunos conceptos sobre IPv6*. Obtenido de http://dreyacosta.com/algunos-conceptos-sobre-ipv6/

Aguayo, M. (Diciembre de 2012). *Aprendiendo a crear un blog: ventajas y desventajas de GNU/Linux*. Obtenido de http://clasedecompu-mikeaguayo1995.blogspot.com/2011/06/ventajas-y-desventajas-de-gnu-linux.html

Ahuatzin Sánchez, G. (Agosto de 2012). *Capítulo I. Panorama actual del cambio de IPv4 a IPv6.* Obtenido de catarina.udlap.mx/u_dl_a/tales/documentos/lis/ahuatzin_s_gl/capitulo1.pdf

Araguz, A. (Junio de 2012). *Sistemas de telefonía STI*. Obtenido de https://sites.google.com/site/sistemasdetelefoniasti/t3-conmutacion-encaminamiento-y-senalizacion-telefonica

Barajas, S. (Julio de 2012). *Protocolos TCP/IP - Saulo.Net*. Obtenido de http://www.saulo.net/pub/tcpip/a.htm

Barrera, J. P., & Guerra, E. M. (Junio de 2005). *Implementación de TUNNELING entre redes IPV4 E IPV6 para la empresa NETXPERTS CONSULTING S.A. (Tesis de Grado).* Obtenido de http://repositorio.espe.edu.ec/bitstream/21000/406/1/T-ESPE-012631.pdf

Blanchet, M. (2006). *Migrating to IPv6 (1º ed.).* Québec: John Wiley & Sons.

Blogdiario. (Diciembre de 2013). *Ventajas y desventajas de Linux - Sistema Operativo Linux*. Obtenido de http://almis.blogspot.es/1224551940/ventajas-y-desventajas-de-linux/

Carossella, J. C. (Julio de 2012). *Direccionamiento IP - ConsulTeach*. Obtenido de http://consulteach.com.ar/Publicacion.asp?codGrupo=58

Cicileo, G. (Agosto de 2012). *Portal IPv6 - LACNIC*. Obtenido de http://portalipv6.lacnic.net/mecanismos-de-transicion/

Cisco. (Agosto de 2012). *Implementing IPv6 in an Enterprise Network.* Obtenido de http://ciscodocuments.blogspot.com/2011/05/chapter-08-implementing-ipv6-in.html

CITEL. (Agosto de 2012). *Migración a IPv6*. Obtenido de http://www.oas.org/en/citel/infocitel/2008/agosto/arin_e.asp

Collado, E., & Juliá, M. (Junio de 2013). *Sobre Quagga - MicroAlcarria.* Obtenido de

http://www.microalcarria.com/descargas/documentos/Linux/redes/routing/Quagga/quagga/quagga-es-1.html

Comer, D. (2005). *Internetworking with TCP/IP.* Indiana: Prentice Hall.

Cricket, L. (2011). *DNS and BIND on IPv6.* Sebastopol: O'Reilly Media.

Della, J., Navarro, M., & Rey, D. (Junio de 2012). *Modelo OSI - Interconexión de Sietmas Abiertos - UTN*. Obtenido de http://www1.frm.utn.edu.ar/comunicaciones/modelo_osi.html

DistroWatch. (Noviembre de 2012). *Distribuciones de linux mas populares*. Obtenido de http://archivoanual.com/distribuciones-linux-mas-populares-2010/

D-Link. (Enero de 2013). *D-Link España*. Obtenido de http://www.dlink.com/es/es/business-solutions/switching/unmanaged-switches/desktop/des-1016d-16-port-10-100mbps-desktop-switch

El Mundo. (Mayo de 2013). *Que es IPv6? - El Mundo*. Obtenido de http://www.elmundo.es/imasd/ipv6/queesipv6.html

Escartin, J. A. (Septiembre de 2012). *Instalacion de Servicios - UPCommons.* Obtenido de http://upcommons.upc.edu/pfc/bitstream/2099.1/3451/6/52096-6.pdf

Facundo, H. (2003). *La Biblia de Linux.* Buenos Aires: MP Ediciones.

Fos, J. A. (Abril de 2012). *Universidad de Valencia*. Obtenido de www.uv.es/montanan/redes/trabajos/IPng.doc

García, J. L. (2012). *Ataques en redes de datos IPv4 e IPv6.* 0xword.

Generalidades de IPv6. (Abril de 2012). Obtenido de http://generalidadesipv6.blogspot.com/feeds/posts/default

Goncalves, M., & Niles, K. (1998). *IPv6 Networks.* McGraw-Hill.

Graziani, R. (2012). *IPv6 Fundamentals.* Indianápolis: Cisco Press.

Guadalinfo, J. L. (Octubre de 2013). *Brecha digital en Periana.* Obtenido de http://brechadigitalperiana.blogspot.com/2009_07_01_archive.html

Hagen, S. (2006). *IPv6 Essentials.* Sebastopol: O'Reilly Media.

Hagen, S. (2011). *Planning for IPv6.* Sebastopol: O`Reilly Media.

IPv6 Chile. (Abril de 2012). Obtenido de http://www.ipv6.cl/pequena-oficina/preguntas-frecuentes

IPv6: ICMPv6. (Agosto de 2012). Obtenido de http://tunnelingipv6.blogspot.com/

ISOC. (Junio de 2013). *IPv6 para todos.* Obtenido de http://www.ipv6tf.org/pdf/ipv6paratodos.pdf

Jallurana, O. (Junio de 2012). *Modelos de redes: el modelo OSI*. Obtenido de http://compu9999.blogspot.com/2012/06/el-modelo-osi_05.html

Jara, F. E. (Abril de 2009). *Estudio e implementación de una red IPv6 en la UTFSM. (Tesis de Grado).* Obtenido de http://share.pdfonline.com/e7fea698e87e43dbbcb6c98d132037b5/ImplementacionIpv6_UTFSM_proyecto.htm

Jazztel. (Febrero de 2013). *Huawei HG532c*. Obtenido de http://www.jazztel.com/ayuda/soporte-internet/soporte-y-manuales-internet/huawei-hg532c.html?_requestid=273581

Kantera56. (Julio de 2012). *Direcciones IP Agotadas*. Obtenido de http://kantera56.blogspot.com/2010_10_01_archive.html

Kioskea. (Junio de 2012). *TCP/IP*. Obtenido de http://es.kioskea.net/contents/282-tcp-ip

K-nabora Bufete Tecnológico. (Agosto de 2013). *Implantación de QoS en un entorno GNU/Linux - K-nabora*. Obtenido de http://www.k-nabora.com/index.php/blog/ImplantaciA-n-de-QoS-en-un-entorno-GNU-Linux.html

Kozierok, C. (2006). *The TCP/IP Guide.* San Francisco: No Starch Press.

Kunihiro, I. (Julio de 2013). *Quagga Software Routing Suite - Savannah*. Obtenido de http://www.nongnu.org/quagga/docs/docs-info.html

Lezcano, T. (Septiembre de 2012). *Tomas Lezcano: Los servicios que brinda*. Obtenido de http://tomaslezcano.blogspot.com/2009/11/los-servicios-que-brinda.html

Linux IPv6 HOWTO. (Abril de 2013). Obtenido de http://www.tldp.org/HOWTO/Linux+IPv6-HOWTO/index.html

Manuales de Linux. (Noviembre de 2012). *Manuales de Linux - Taringa: Estructura de Archivos de Linux*. Obtenido de http://manualesdelinux.blogspot.com/2008/10/estructura-de-archivos-de-linux.html

Medina, F., & Moreno, B. (Agosto de 2012). *ICMPv6 - Scribd.* Obtenido de http://www.scribd.com/doc/72299411/icmpv6

Mejía, F. (Junio de 2013). *Introducción al IPv6.* Obtenido de http://www.aeprovi.org.ec/index.php?option=com_remository&Itemid=75&func=startdown&id=19

Microsoft. (Agosto de 2012). *IPv6 - General - Propiedades de la interfaz*. Obtenido de http://technet.microsoft.com/es-es/library/cc772282(v=WS.10).aspx

Moreno, J. (Julio de 2013). *Redes, Software Libre y Educación: RIPv2 en Linux con Quagga*. Obtenido de http://sw-libre.blogspot.com.es/2011/04/rip-v2-en-linux-con-quagga.html

Muñoz, J. (Agosto de 2012). *Documento antiguo de IPv6*. Obtenido de http://www.jesusdml.es/2011/04/12/ipv6-ya-es-el-presente-y-futuro-de-internet/

Netgear. (Enero de 2013). *What is a Hub?* Obtenido de http://kb.netgear.com/app/answers/detail/a_id/233

NetSolutions. (Abril de 2013). *Wireless - NetSolutions*. Obtenido de http://www.netsolutions.com.mx/servicios/wireless/wireless.shtml

Peralta, L. (Agosto de 2012). *IPv6.* Obtenido de http://www.cu.ipv6tf.org/pdf/ipv6.pdf

Quintana, E. (Octubre de 2013). *LINUX | El deseo intenso crea no sólo sus propias oportunidades.* Obtenido de http://quice85.wordpress.com/2013/10/17/linux/

Ramírez Mosquera, D. E., & Hidalgo Pazmiño, J. d. (2010). *Investigar y desarrollar una guía metodológica de los mecanismos de transición y coexistencia ipv4-ipv6 en el área de sistemas de la facultad de ingeniería de la universidad nacional de Chimborazo. (Tesis de Grado).* Obtenido de http://dspace.unach.edu.ec/bitstream/123456789/55/1/FI-ESC-40A001.pdf

Ramírez, D. E., & Hidalgo, J. d. (2010). *Investigar y desarrollar una guía metodológica de los mecanismos de transición y coexistencia ipv4-ipv6 en el área de sistemas de la facultad de ingeniería de la universidad nacional de Chimborazo. (Tesis de Grado).* Obtenido de http://dspace.unach.edu.ec/bitstream/123456789/55/1/FI-ESC-40A001.pdf

Ramirez, P. (Febrero de 2013). *ThIs Is mY liFe*: CONCENTRADORES*. Obtenido de http://dongato77.blogspot.com/2010/04/concentradores.html

Redes Informaricas. (Noviembre de 2013). Obtenido de http://redesinformaricas.wikispaces.com/Modelo+TCP-IP

Salcedo, O., López, D., & Ríos, Á. (Septiembre de 2012). *Desempeño de la calidad del servicio (QoS) sobre IPv6.* Obtenido de http://www.doaj.org/doaj?func=fulltext&aId=967437

Sanders, C. (2011). *Practical Packet Analysis.* San Francisco: No Starch Press.

SEE-MY-IP.COM. (Agosto de 2012). *ICMPv6*. Obtenido de http://www.see-my-ip.com/tutoriales/protocolos/icmpv6.php

Slideshare. (Mayo de 2013). *F:\Redes\Qué Es Una Red InformáTica (Nuevo).* Obtenido de http://www.slideshare.net/Alkx/fredesqu-es-una-red-informtica-nuevo

Supertel. (18 de Abril de 2012). *IPv6 en Ecuador*. Obtenido de http://www.supertel.gob.ec/index.php?option=com_content&view=article&id=362:formularios-para-la-entrega-de-informacion&catid=65&Itemid=38

Tele-Hizmo. (Enero de 2013). *Tele-Hizmo - Cable Telefocia*. Obtenido de http://www.telehizmo.es/catalogo/html/telefonia/alimentaconmuta.html

The-Crankshaft Publishing's. (Agosto de 2012). *IPv6 Network Management*. Obtenido de http://what-when-how.com/ipv6-for-enterprise-networks/ipv6-network-management/

Tutorial de IPv6. (Abril de 2013). Obtenido de http://www.consulintel.es/html/ForoIPv6/Documentos/Tutorial%20de%20IPv6.pdf

Ubidia, A. J. (Mayo de 2007). *Análisis, diseño e implementación de una intranet IPv6 y QoS. (Tesis de Grado).* Obtenido de http://repositorio.espe.edu.ec/bitstream/21000/1172/1/T-ESPE-021890.pdf

Universidad de Antoquia. (Noviembre de 2012). *Directorio-Linux*. Obtenido de http://docencia.udea.edu.co/cci/linux/dia4/directorio.htm#estructura

Universidad de Vigo. (Marzo de 2013). *TOPOLOGÍA DE REDES LAN.* Obtenido de http://www.lsi.uvigo.es/lsi/jdacosta/documentos/apuntes%20web/Topologia%20de%20redes.pdf

Universidad Nacional de la Plata. (Septiembre de 2012). *Modelos de QoS en redes IPv6, Integración con Otras Redes.* Obtenido de http://sedici.unlp.edu.ar/bitstream/handle/10915/19420/Documento_completo.pdf?sequence=1

Urueña, E. E. (Julio de 2012). *Direccionamiento IPv4 - Monografias.com*. Obtenido de http://www.monografias.com/trabajos30/direccionamiento-ip/direccionamiento-ip.shtml

Xatakaon. (Agosto de 2012). *Magazine - IPv4 vs IPv6*. Obtenido de http://www.xatakaon.com/tag/ipv4-vs-ipv6/rss2.xml

Anexo 1. RIP en Quagga

RIP es un protocolo de tipo vector distancia IGP que para configurar se deben seguir los siguientes pasos en el equipo que tiene instalado el CentOS para la configuración del RIP son:

1. Ingresar a la carpeta etc/quagga/
2. Copiar el contenido del archivo ripd.conf.sample al ripd.conf mediante:

   #cat ripd.conf.sample > ripd.conf
3. Editar el archivo ripd.conf utilizando el gedit.
4. Modificar los campos hostname, password para entrar a rip y password para entrar en el modo privilegiado. Guardar las modificaciones.
5. Se procede a iniciar el servicio rip mediante el siguiente comando:

   #service ripd start o #ripd -d
6. Si se desea que el servicio se ejecute cada vez que se inicia la máquina se digita:

   #chkconfig --level 35 ripd on
7. Para ingresar a la configuración del ripng se digita:

   #telnet localhost ripd
8. Se procede a ingresar las claves anteriormente configuradas para poder proceder a configurar. Para ingresar al modo privilegiado se puede digitar en o enable.
9. Una vez en el modo privilegiado se procede a digitar configure terminal para ingresar al modo de configuración del router.
10. Para la respectiva configuración de ripng se puede digitar lo siguiente:

    router rip

    network 192.168.1.0/26

    network 10.0.0.0/24
11. Se procede a guardar la información con el comando write y se despliega un mensaje en donde se indica en donde se guardó la configuración.

Anexo 2. Script para compartir Internet mediante iptables

Mediante el siguiente script se comparte el Internet a una LAN y para lo cual se utiliza Iptables y NAT. Para que funcione este script se necesita un PC que funcione como router y que disponga de dos tarjetas de red, una que esté conectada directamente a Internet o que esté conectada al router ADSL de nuestro ISP y la otra tarjeta que esté conectada a la red local de la empresa.
Lo que se realiza en el script es enmascarar las IPs de la red 10.0.0.0 con otra diferente, es decir que las los equipos de la red 10.0.0.0 van a salir a la red 192.168.1.0 mediante su respectivo Gateway es decir 10.0.0.10 utilizando NAT.

Datos de la red:
Red1: Eth0: 192.168.1.0
Red2: Eth1: 10.0.0.0

En este script se va a utilizar las capacidades de control de conexiones que dispone Iptables. Hay que tener en cuenta que se debe tener habilitado el bit de forward en el archivo /etc/sysctl.conf modificando la siguiente línea:
net.ipv4.ip_forward = 1

Después de modificar se procede a ejecutar el siguiente comando:

#sysctl -p

Finalmente se procede a crear el script de la siguiente manera:

```
#!/bin/sh
##Borrar Reglas Viejas
iptables -F
iptables -X
iptables -Z
iptables -t nat -F

# ===>> Inicio de las Reglas <<=== #

###ROUTER
##Establecer políticas por defecto
```

```
iptables -P INPUT ACCEPT
iptables -P OUTPUT ACCEPT
iptables -P FORWARD ACCEPT
iptables -t nat -P PREROUTING ACCEPT
iptables -t nat -P POSTROUTING ACCEPT
##Empezar a Filtrar
# El localhost se deja (por ejemplo conexiones locales a mysql)
iptables -A INPUT -i lo -j ACCEPT
##Enmascaramiento de la red local
iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE

####SERVICIOS
##Para servicio VSFTPD
iptables -A INPUT -m state --state NEW -m tcp -p tcp --dport 20 -j ACCEPT
iptables -A INPUT -m state --state NEW -m tcp -p tcp --dport 21 -j ACCEPT
##Para servicio SSH
iptables -A INPUT -m state --state NEW -m tcp -p tcp --dport 22 -j ACCEPT
##Para servicio de correo
iptables -A INPUT -m state --state NEW -m tcp -p tcp --dport 25 -j ACCEPT
iptables -A INPUT -m state --state NEW -m tcp -p tcp --dport 110 -j ACCEPT
iptables -A INPUT -m state --state NEW -m tcp -p tcp --dport 143 -j ACCEPT
iptables -A INPUT -m state --state NEW -m tcp -p tcp --dport 465 -j ACCEPT
iptables -A INPUT -m state --state NEW -m tcp -p tcp --dport 587 -j ACCEPT
iptables -A INPUT -m state --state NEW -m tcp -p tcp --dport 993 -j ACCEPT
iptables -A INPUT -m state --state NEW -m tcp -p tcp --dport 995 -j ACCEPT
##Para servicio Web
iptables -A INPUT -m state --state NEW -m tcp -p tcp --dport 80 -j ACCEPT
##Para servicio DNS
iptables -A INPUT -m state --state NEW -m tcp -p tcp --dport 53 -j ACCEPT
##Para servicio DHCPD6
iptables -A INPUT -i eth1 -p udp -m state --state NEW -m udp --sport 67:68 --dport 67:68 -j ACCEPT

# ===>> Fin de las Reglas <<=== #
```

A continuación se detallan los pasos para crear un script:

1. Abrir cualquier editor de texto y copiar las sentencias deseadas. Tener en cuenta que siempre un script debe de comenzar con la sentencia #!/bin/bash
2. Guardar el script con la extensión deseada, de preferencia sh.

3. Una vez creado el script se procede a dar permisos de ejecución:
   chmod 777 nombre_script
4. Ejecutar el script con el comando:
   ./nombre_script
5. Si se desea que el script se ejecute cada vez que inicie la máquina se puede poner el anterior comando en el archivo /etc/rc.d/rc.local
6. Finalmente verificar que se ejecuta el script al iniciar el SO.

Anexo 3. Servidor DHCP para IPv4

Este servidor se procederá a instalar en el PC router. Para la autoconfiguración de la LAN se va a utilizar el servidor de DHCP que va a asignar IPs, puerta de enlace y DNS.

4 Verificar los RPM que se necesitan instalar mediante el comando:

#rpm –qa | grep dhcp

5 Descargar el RPM correspondiente de la página http://pkgs.org/

6 En este caso como son varios RPM a instalar se puede digitar el siguiente comando para que se instalen automáticamente:

#yum –y install dhcp

7 Finaliza la instalación si el proceso llega al 100%.

8 Se recomienda que el servicio dhcpd funcione en la interfaz de red utilizada para la LAN. Editar el archivo /etc/sysconfig/dhcpd y agregar la interfaz de red de la siguiente manera:

DHCPDARGS=eth1

9 Se procede a modificar el archivo de configuración /etc/dhcp/dhcpd.conf

```
#
# DHCP Server Configuration file.
#   see /usr/share/doc/dhcp*/dhcpd.conf.sample
#   see 'man 5 dhcpd.conf'
#
# Si se tienen problemas con equipos con Windows Vista/7/8 omita el parámetro
# server-identifier. Ésto aunque rompe con el protocolo DHCP, permite a los
# clientes Windows Vista/7/8 poder comunicarse con el servidor DHCP y aceptar
# la dirección IP proporcionada.
# server-identifier 10.0.0.1;
ddns-update-style interim;
ignore client-updates;
authoritative;
default-lease-time 900;
max-lease-time 7200;
option ip-forwarding off;
```

```
option domain-name "santanet.net.ms";
option ntp-servers 0.pool.ntp.org, 1.pool.ntp.org, 2.pool.ntp.org, 3.pool.ntp.org;

shared-network santanet {
subnet 10.0.0.0 netmask 255.255.255.0 {
        option routers 10.0.0.10;
        option subnet-mask 255.255.255.0;
        option broadcast-address 10.0.0.255;
        option domain-name-servers 10.0.0.10;
        option netbios-name-servers 10.0.0.10;
        range 10.0.0.100 10.0.0.200;
}
}
```

10 Se procede a iniciar el servicio dhcp mediante el siguiente comando:

#service dhcpd start

11 Si se desea que el servicio se ejecute cada vez que se inicia la máquina se digita:

#chkconfig --level 35 dhcpd on

Anexo 4. Código PHP para mostrar direcciones IPv4 e IPv6 del cliente

A continuación se detalla el código PHP que permite mostrar en la página web de nuestro servidor la dirección IP que utiliza el cliente para acceder. Lo principal es crear una página web en PHP y agregar el siguiente contenido:

```
<?php if(strpos($_SERVER['REMOTE_ADDR'],".")===false)
{
echo "<font color='#154983' size=2 face='verdana'>Felicitaciones usted está utilizando la dirección IPv6</font><br><br>";
echo "<font color='#154983' size=4 face='verdana'>".$_SERVER['REMOTE_ADDR']."</font><br><br>";
}else{
$DIRv4=str_replace("::ffff:","",$REMOTE_ADDR);
echo "<font color='#FF0000' size=2 face='verdana'>Advertencia usted está utilizando la dirección IPv4</font><br><br>";
echo "<font color='#FF0000' size=4 face='verdana'>".$_SERVER['REMOTE_ADDR']."</font><br><br>";
}
?>
```