UNIVERSIDAD LUTERANA SALVADOREÑA

LICENCIATURA EN CIENCIAS DE LA COMPUTACIÓN

MATERIA: REDES I

TEMA: TRABAJO FINAL DEL PROYECTO “CONFIGURACION DE SERVICIOS CON IPV6”.

CATEDRATICO: ING. MANUEL FLORES VILLATORO

ESTUDIANTES:

No	APELLIDOS	NOMBRES	CARNET	% DE PART.	NOTA
1	ALFARO ORTIZ	WALTER ORLANDO	AO02110416	20%	
2	ALVARADO GARCIA	CELSO ANTONIO	AG01121540	20%	
3	AVILEZ SANCHEZ	LUIS	AS21315001	20%	
3	GREGORIO CABRERA	NICOLAS	GC01121355	20%	
4	SURIO BONILLA	MARITZA ELIZABETH	SB01100101	20%	

FECHA: SAN SALVADOR 24 DE MAYO DE 2014

Tabla de contenido

INDICE DE TABLAS

INDICE DE ILUSTRACIONES

1.- INTRODUCCION

El creciente número de máquinas conectadas al Internet, en conjunto con la deficiente manera en que las direcciones IP son asignadas, han provocado una pronta escasez en el espacio de direcciones disponibles del protocolo de red actual (IPv4). La asignación de direcciones mediante CIDR (Classless Inter-Domain Routing) que consiste en la agregación de prefijos que son adyacentes para dar lugar a prefijos menores, así como la Traducción de Direcciones de Red (NAT) han intentado resolver este problema sin obtener mucho éxito, y además hay muchas aplicaciones que requieren utilizar direcciones estáticas, por lo que NAT no ayuda en gran medida en estos casos. Otro aspecto a destacar es la seguridad misma que ha tomado un papel muy importante en el manejo de la información que es enviada a través de los medios electrónicos. IPv4 no fue diseñado para ser un protocolo seguro y muchas de las aplicaciones creadas para solucionar este problema de seguridad solo protegen la información en las capas de comunicación más altas (Aplicación y Transporte) haciendo vulnerable la información a ataques en la capa de Red. IPv6 por su parte se presenta como la solución más viable a todos los problemas anteriormente mencionados porque incluye entre otras mejoras, direcciones IP de 128 bits, en vez de las direcciones de 32 bits de IPv4 y seguridad sobre la capa de Red.

2.- OBJETIVO GENERAL

Implantar una pequeña infraestructura de red con soporte para la versión más reciente hasta el día de hoy (protocolo IP versión 6).

2.1 OBJETIVOS ESPECIFICOS

- ✓ Configurar la infraestructura de red implantada para dar soporte a la comunicación entre hosts, brindando servicios básicos bien conocidos como DHCP y HTTP.
- ✓ Comprobar la disponibilidad y soporte del protocolo IPv6 en sistemas operativos bien conocidos, entre ellos GNU/Linux).

3.- MARCO TEORICO.

3.1 Protocolo de internet versión 4 (IPv4).

Como equipo de trabajo hemos decidido investigar sobre los dos protocolos, con el fin de comprender su funcionamiento, tal como lo dijimos en los objetivos. El protocolo de internet IP, es la parte fundamental sustentada por el sistema TCP/IP y de todo el funcionamiento de INTERNET. .La unidad de datos del IP es el datagrama, cuyo esquema se muestra en la figura siguiente.

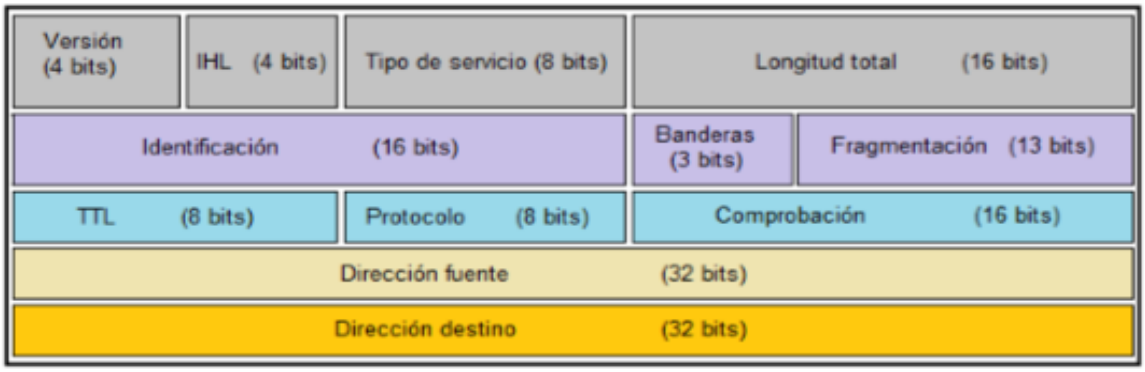

Fig. 1 Mostrando un datagrama IP

En la figura anterior se ilustra a un datagrama IP, cuya estructura es en bloques de 32 bits (4 bytes), su transmisión consiste en enviar primero el bit 0, luego el bit 1, 2, 3 hasta finalizar el datagrama. Dicho orden se denomina network byte order, el mismo es muy importante, debido a que los diferentes computadores tienen diversos sistemas de almacenamiento de bits en memoria. Otro formato es el little

endian, que permite almacenar bits en orden inverso al network byte order, mientras que la otra posibilidad se denomina Big endian.

Según el modelo TCP/IP el protocolo de capa 3 permite direccionar los datagramas en la capa de red, este encabezado se superpone al datagrama manejado, es decir, las características de ruteo y transmisión.

En la capa inmediatamente superior a TCP se agrega el encabezado, quedando el datagrama tal y como se muestra en la figura siguiente: Configuración de un datagrama IPv4.

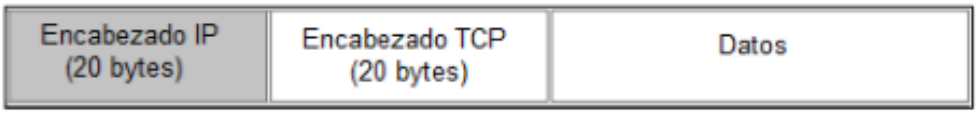

Fig. 2 Mostrando la configuración de un datagrama IPV4.

La longitud que tiene el encabezado IP en la capa de red es de 170 bits, que aproximadamente es 20 bytes, formada por diversos campos con distintos significados. Ilustrada en la primer figura. Los campos descritos en la primera figura se describen a continuación:

a. Versión, nos indica el número de la versión del protocolo de internet (IP), es decir, que para IPv4 el valor será 4.

b. Longitud de encabezado, describe la longitud del encabezado en número de grupos de 32 bits cada uno de 4 bits.

c. Tipo de servicio, nos permite saber la importancia de los datos enviados, condicionando la forma en que serán tratados en la transmisión de 8 bits.

d. Longitud total, nos indica la longitud completa en bytes del datagrama de 16 bits, incluyendo el encabezado y los datos. En la práctica el datagrama es pequeño (16 bits) y teóricamente no será mayor a 65.535 bytes.

e. Identificación, utilizada para el ensamble de los fragmentos de un datagrama de 16 bits.

f. Banderas, es un indicador empleado en la fragmentación de 3 bits.

g. Fragmentación, permite ensamblar los datagramas previamente fragmentados, cuyo valor es de 64 bits (grupos de 8 bytes), inicializado en 0 para fragmento 1 de 16 bits.

h. Límite de existencia (TTL, Time to Live), es aquel número disminuido cada vez que el paquete de datos (8 bits) pasa por un nodo de red, si el valor toma un 0 indica que el paquete se descarta. Por cuestiones de seguridad debemos evadir la redundancia cíclica, empleado por razones de seguridad siendo improbable que esto ocurra en una red bien diseñada.

i. Protocolo, es un número que se emplea para definir el protocolo perteneciente al datagrama (8 bits), de tal manera que sea tratado eficientemente cuando llegue a su destino.

j. Comprobación, permite verificar los datos que contienen al encabezado del IP sean correctos, dicha eficiencia no se utiliza para evaluar los datos ya incluidos, sino que los datos de usuario se comprueban posteriormente del encabezado siguiente, correspondiente al nivel de capa de transporte (16 bits). Adicionalmente, si cambiamos la opción de encabezado, dicho campo será calculado nuevamente.

k. Dirección fuente, es aquella que contiene la dirección del usuario en la que envía el paquete de datos de 32 bits.

l. Dirección destino, es aquella dirección del usuario que recibe la información, es decir, que los routers o gateways (medios intermedios) conocen la dirección para llegar correctamente el paquete de datos de 32 bits.

3.2- PROBLEMAS CON EL PROTOCOLO DE INTERNET IPV4.

Como sabemos IPv4, es la cuarta versión del protocolo IP y dominante en Internet, que permite interconectar redes de manera interna y externa. Las principales características son:

a. Enrutamiento y direccionamiento: Proporciona únicamente una dirección a cada uno de los dispositivos de redes de paquetes. Es decir, que IPv4 fue principalmente diseñado para proveer el enrutamiento de información (paquetes) mediante redes de diversa complejidad.

b. Encapsulación: es una división antigua de TCP (Transmission Control Protocol), localizado en la capa 3 del modelo ISO/OSI y funciona sobre diversos protocolos de nivel inferior.

c. Mejor esfuerzo: El protocolo IP provee un servicio de transmisión de paquetes no fiable(o de mejor esfuerzo). No se asegura que los paquetes enviados lleguen correctamente al destino.

IPv4 utiliza un sistema de direcciones de 32 bits 2 = 4.294.967.296 subdivididas en cinco clases. Con una simple revisión del crecimiento de INTERNET en los últimos 5 años, podemos observar que las direcciones a este ritmo ya se agotaron

La versión de IPv4 usada actualmente en Internet no ha cambiado sustancialmente desde su publicación inicial en 1981. IPv4 ha demostrado ser un protocolo robusto, fácil de implementar y con la capacidad de operar sobre diversos protocolos de capa 2. Si bien fue diseñado inicialmente para interconectar unos pocos computadores en redes simples, ha sido capaz de soportar el explosivo crecimiento de internet.

En aquel momento tanto el número de ordenadores conectados como las expectativas de crecimiento eran mucho más moderados de lo que han sido realmente, y por tanto la suposición de que un tamaño de 32 bits sería suficiente parecía razonable. De esta manera, podemos justificar la revisión de la versión 4 del protocolo IP desde dos puntos de vista principalmente:

1. Técnico: Donde el direccionamiento es insuficiente, debido a la gran demanda y que a futuro incrementa considerablemente. Las tablas de encaminamiento o de direcciones, son las encargadas de almacenar los routers internamente, y empleados para saber hacia dónde deben encaminar un datagrama, son excesivamente grandes debido a la enorme cantidad de direcciones que existen actualmente y al sistema de encaminamiento utilizado, lo que obligaría a los routers a mantener grandes cantidades de direcciones para conocer hacia dónde deben redireccionar los datagramas.

2. **Social**: Las necesidades de los usuarios de INTERNET han aumentado espectacularmente, exigiendo nuevas capacidades (seguridad, privacidad, comercio electrónico, velocidad...) que la versión 4 no puede proporcionar.

3.3- Historia del Protocolo de Internet versión 6.

La historia de Ipv6 se inició en el año 1990, cuando se reveló que las direcciones IPv4disponibles estaban disminuyendo aceleradamente. Según estudios realizados por profesionales que indicaban que las IPv4 se agotarían alrededor del 2005. Dichos estudios fueron muy cuestionados por toda la comunidad de Internet, y es de ahí que iniciaron la búsqueda de posibles soluciones. Para ese entonces se plantearon dos soluciones:

1. Mínimo: Salvaguardar el protocoloIPv4, es decir, mantenerlo intacto, sólo se debe aumentarla longitud de la dirección. Esto es muy sencillo, lo que ocurriría es tener menos suplicio en la fase de despliegue.

2. Máximo: Desplegar completamente la nueva versión del protocolo IPv6, cuyo enfoque permitiría incorporar nuevas características y mejoras en IPv4. Debido a que no existía tanta urgencia en plantear una solución rápida, el desarrollo de un nuevo protocolo fue elegido, es decir, que el nombre original fue IPng (Próxima generación IP, IP Next Generation) mismo que fue desplazado por IPv6, siendo este el nombre definitivo, llevados de la mano por Steven Deering y Robert Hinden.

El primer conjunto de protocolos RFCs que rigen al IPv6, fue presentado finalizando el año 1995, dicho protocolo se lo denomino RFC 1883: Protocolo de Internet versión 6 (IPv6). Una vez que se tenía disponible el RFC 1883 las implementaciones fueron esperadas con entusiasmo, pero nunca ocurrieron.

Para ese entonces (década del año 1990) el auge significativo de Internet en empresas causo incertidumbre entre ellas, donde tenían que resolver un complicado problema de negocio, invertir en IPv6 que traería algunos beneficios a futuro, o invertir en el despliegue de IPv4, ya que cualquiera de los dos protocolos (IPv6 e IPv4) les representarían ganancias. Finalmente la mayoría de las empresas decidieron escoger el retorno rápido y fácil de las inversiones y desarrollaron productos basados en IPv4.

Surgieron otros métodos para mantener el espacio de direcciones, el más importante es el enrutamiento sin clase entre dominios (CIDR, Classless InterDomain Routing), como consecuencia, los sitios recién conectados obtuvieron significativamente menos direcciones que en años anteriores. El uso del CIDR retraso la implementación de IPv6 ante los ojos de muchas personas, pero no en todos.

Aquellos sitios nuevos o en expansión desarrollaron métodos para limitar este recurso, uno de estos enfoques ha sido la traducción de dirección de red (NAT, Network Address Translation) que permitió utilizar a las redes de computadoras un número cualquiera de direcciones privadas, y para luego convertirlas en públicas cuando los paquetes dejaran el sitio y viceversa. NAT utiliza el mecanismo de compartir direcciones públicas a través de hosts, así como otros mecanismos tales como PPP (Point to Point Protocol) y DHCP (Dynamic Host Configuración Protocol) proporcionan un medio para que hosts alquilen direcciones por un cierto período de tiempo.

3.4- Protocolo de internet versión 6 (IPv6)

El Protocolo de Internet versión 6 (IPv6) ha sido definido por el RFC-2460, cuyo diseño ha sido para sustituir alIPv4 (RFC 791), en la actualidad se están incorporando en la gran mayoría de dispositivos electrónicos que acceden a Internet tales como: placas de red, switches, routers y todo dispositivo de conectividad.

Steve Deering de Xerox PARC y Craig Mudge fueron los que crearon y diseñaron el protocolo de internet IPv6 destinado a sustituir a IPv4, cuyo límite en el número de direcciones de red admisibles está empezando a restringir e impedir el crecimiento de Internet y su uso en países de gran densidad de población como: China, India, y otros países Asiáticos, en Ecuador hay aproximadamente 7 millones de usuarios a junio 2012.

Dicha versión (IPv6) mejorará el servicio globalmente; por ejemplo, proporcionará a futuras celdas telefónicas y dispositivos móviles sus direcciones propias y permanentes, esto no sería poca cosa. A inicios del 2010 se tenía al menos 10% de

IP’s disponibles. Es por esto que la IANA (Agencia Internacional de Asignación de Números de Internet, por sus siglas en inglés) entregó en febrero 2011 el último bloque de direcciones disponibles (33 millones) a la organización encargada de asignar IP’s en Asia, un mercado que está en auge y no tardará en consumirlas todas, por lo que hemos mencionado anteriormente, su gran crecimiento en población.

Esta nueva revisión del protocolo IP se numerará con la versión 6 y no versión 5 para evitar confusiones, ya que anteriormente se hicieron pruebas añadiendo extensiones a la versión 4. Dichas extensiones experimentales no terminaron de formalizarse con una nueva versión del protocolo, por esto fue preferible evitar posibles conflictos de numeración, razón por la cual el número de versión es 6.

Bajo estas circunstancias, IPv6 conocido también como IPng (IP de próxima generación) ofrece mayor flexibilidad y eficacia para dar soluciones a una amplia gama de nuevos problemas. Los principales objetivos que sigue IPv6 son:

a) Admitir miles de millones de equipos, superando las limitaciones de espacio para las direcciones IPv4 actuales;

b) Reducir el tamaño de las tablas de enrutamiento;

c) Simplificar el protocolo para permitir que los routers en ruten datagramas de manera más rápida;

d) Brindar mejor seguridad (autenticación y confidencialidad) que la proporcionada por el protocolo IP actual;

e) Prestar más atención al tipo de servicio y, particularmente, a los servicios asociados con el tráfico en tiempo real;

f) Facilitar la difusión a destinos múltiples, permitiendo especificar el tamaño;

g) Permitir la movilidad de un equipo sin cambiar su dirección;

h) Permitir el futuro desarrollo del protocolo;

i) Posibilitar la coexistencia pacífica del protocolo antiguo con el nuevo.

3.5- Características de IPv6.

El protocolo de internet versión (IPv6) conserva muchas de las características que hicieron exitoso a IPv4, dentro de las cuales se puede destacar que opera sin conexiones, es decir, que cada datagrama tiene una dirección de destino y su enrutamiento es independiente. También resaltamos que como IPv4, la cabecera de cada datagrama tiene una cantidad máxima de saltos que deben de hacerse antes de descartarlo.

Sin embargo existen otras características que además de ser conservadas, y que IPv6 también se encarga de mejorarlas.

Existen características muy interesantes que IPv6 trae consigo, ya que resuelven muchos de los problemas de la versión 4. Las características más importantes de IPv6 se describen a continuación:

a. Direccionamiento. El campo para direccionar o identificar dispositivos es de 128 bits (2128), este campo es lo suficientemente grande para manejar el crecimiento continuo de Internet mundial durante muchas décadas. El número de direcciones IP que ofrece IPv6 es alrededor de 340 sextillones.

b. Rendimiento Actualmente, las redes LAN y WAN están progresando respecto a la velocidad de transmisión, pudiendo utilizar velocidades de ciento de Megabits por segundo con la tendencia de llegar a varios Gbps (Gigabits por segundo). Esto se debe a que la tecnología mejora día a día y la existencia de la necesidad de ancho de banda por parte de nuevos servicios y aplicaciones, en especial las basadas en gráficos.

Por esta razón, los routers deben tener la capacidad de reenviar los datagramas IP de manera rápida y así afrontar velocidades inmensas y el incremento de carga lo más rápido y eficiente posible. Para esto es necesario plataformas de hardware robustas, así como también es importante el diseño IP que se tenga. El protocolo de internet versión 6 (IPv6) ofrece tres aspectos de diseño que contribuyen a mejorar el rendimiento de las interredes:

• La simplificación de la cabecera IP. Se reducen los trece campos presentes en IPv4 a sólo ocho campos. Esto permite a los routers procesar con mayor rapidez los paquetes y mejorar el rendimiento.

• Mayor eficiencia en el uso de los campos en la cabecera del paquete. Este cambio fue esencial, ya que algunos campos que antes eran obligatorios ahora son opcionales. Además, la representación de las opciones es diferente, haciendo más sencillo que los routers hagan caso omiso de opciones no dirigidas a ellos, mejorando así el tiempo de procesamiento de paquetes.

• La cabecera del paquete IPv6 es de longitud fija mientras que la cabecera de IPv4 es de longitud variable, simplificando una vez más el proceso.(Lázaro & Miralles, 2004)

• La fragmentación no se permite en lo routers IPv6. Solo puede ser realizada por el origen.

c. Servicios de red: IPv6, cuenta con un mecanismo que permite a un transmisor y un receptor establecer una trayectoria de alta calidad por la red y asociarle los datagramas, garantizando el alto desempeño a aplicaciones de audio y video en tiempo real. IPv6 permite el etiquetado de los paquetes que pertenecen a un flujo de tráfico en particular para la cual el origen solicita un manejo especial.

d. Capacidad de seguridad: IPv6 proporciona soporte nativo para seguridad basándose en sus cabeceras de extensión. Por medio de las cabeceras de autenticación y la cabecera de encapsulamiento seguro, se logra proveer diferentes niveles de seguridad para diferentes usuarios. Esto es muy importante ya que diferentes comunidades de usuarios tienen diferentes necesidades de seguridad.

e. Calidad de servicio: La calidad de servicio en IPv6, es un servicio más robusto que el provisto por datagrama llamados, Prioridad (“priority –4 bits-”) y Etiqueta de Flujo (“Flow Label –24 bits-”). Estos, son usados para que un host pueda identificar los paquetes, para el cual se requiere un manejo especial por parte de los routers IPv6. Esta capacidad es importante, para el momento de soportar aplicaciones que requieren el menor grado de retardos, delay o alteraciones en el flujo. Estos tipos

de aplicaciones son comúnmente descritas como aplicaciones multimedia o de tiempo real.

3.5.1 Tipos de direcciones IPv6
Las direcciones IPv6 se clasifican en tres tipos:

a) **Unicast** .Identifica a solo una interfaz. Un paquete se envía a una dirección unicast que es entregado solo a la interfaz identificada con dicha dirección.
b) **Multicast** .Identifica a un conjunto de interfaces, que por lo general son pertenecientes a diferentes nodos. Un paquete enviado a una dirección multi cast es entregado a todas las interfaces identificadas con dicha dirección.
c) **Anycast** .Identifica a un conjunto de interfaces, que por lo general son pertenecientes a diferentes nodos. Un paquete enviado a una dirección anycast es entregado a una de las interfaces identificadas con dicha dirección, la cual debe ser la más cercana al origen, de acuerdo a las medidas de distancia del protocolo de ruteo.

3.5.2 Los pasos para la transición del protocolo IPv4 al IPv6 son los siguientes:

a) obtener un rango de direcciones IPv6 que utilizará para brindarlas a sus clientes. A través de la autoridad encargada de la delegación de direcciones IPv6 a ISPs debería obtener el rango de direcciones que utilizará.

b) Debe realizar la actualización de su infraestructura del DNS para soportar registros AAAA. Los servidores DNS que forman parte de la infraestructura deben ser actualizados para soportar direcciones IPv6.

c) Debe actualizar los componentes de la red. Los componentes encargados de servir peticiones de los clientes que desean conectarse a redes que utilizan IPv6 deben ser actualizados. Dentro de estos componentes se encuentran los routers

3.5.3 Formato de direcciones

Mientras que en IPv4 se usan 32 bits para representar cada dirección (de 4294967296 posibles), en IPv6 la longitud de este campo1 es de 128 bits, lo que permite representar la cifra de 340282366920938463463374607431768211456 direcciones posibles; en términos más manejables, son $3,4*10^{38}$ valores distintos, o, visto de otra forma, $5,67*10^{28}$ por cada una de las personas de este planeta (asumiendo que son 6.000 millones, aproximadamente)

Los 128 bits se dividen en partes de 16 bits, y se separan por el delimitador: De esta forma, una dirección puede ser fedc: ba65:7654:2333: fedb: ba77:7655:3211, y otra podría ser 1080:0:0:0:8:400:200C:417A. Aunque algunos campos tengan valor 0, es necesario incluirlos en principio.

Sin embargo, cuando se repiten varios campos con valor 0, existe la posibilidad de abreviar la dirección utilizando otra notación, sustituyendo los campos nulos por el delimitador ::

Con este método, la dirección anteriormente indicada 1080:0:0:0:8:400:200C:417A, pasaría a expresarse como 1080::8:400:200C:417A. El delimitador especial :: sólo puede utilizarse una vez para expresar la repetición de varios campos nulos, con objeto de evitar ambigüedades.

A la hora de representar un prefijo que identifique un conjunto de direcciones, se declara una dirección seguida de su longitud. Partiendo de un prefijo como 12AB00000000CD3 (60 bits), su representación sería 12AB:0:0:CD30::/60

Pueden existir entornos mixtos donde un nodo IPv6 pueda manejar en su propio formato direcciones IPv42. Por ejemplo, un nodo con dirección IPv4 222.1.41.90, puede ser identificado por otro nodo IPv6 con la dirección: 222.1.41.90.

4.-INFORMACIÓN SOBRE LA CONSTRUCCIÓN DEL PROYECTO, DETALLANDO CADA UNO DE LOS PASOS, COMANDOS, ARTEFACTOS, PROCEDIMIENTOS QUE REALIZARON.

4.1 CONFIGURACIÓN DE UN SERVIDOR DHCP CON IPV6

Paso #1
Probamos con un test
Test que muestra si estamos aptos para ipv6 “digitamos el siguiente comando en nuestra terminal
test -f /proc/net/if_inet6 && echo "apto para ipv6"

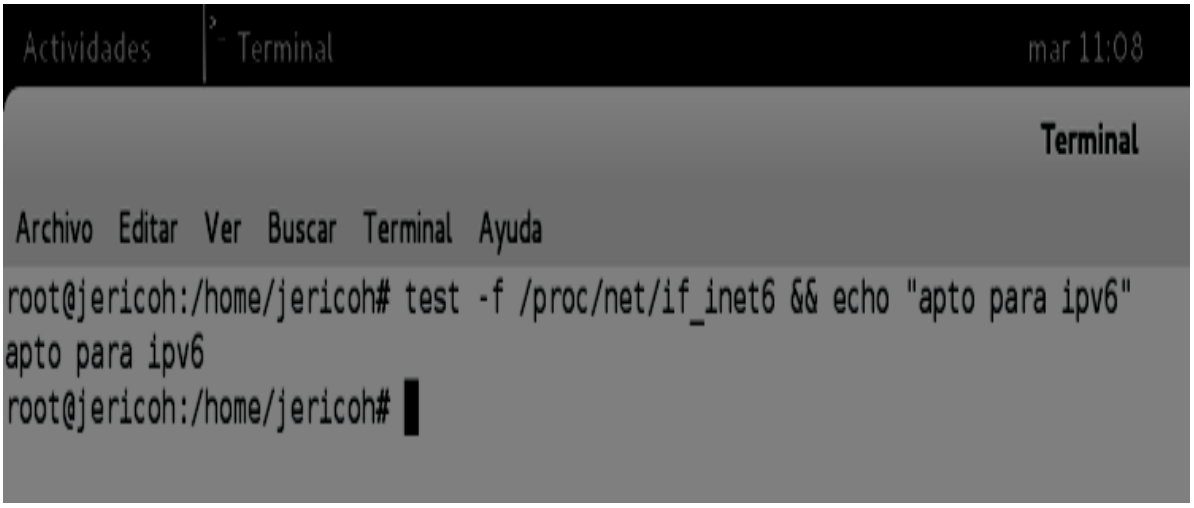

fig.4.1, Probando el comando test.

Paso #2
Configuración de la interfaz eth0
con el comando **nano /etc/network/interfaces**
auto eth0
iface eth0 inet6 static
Address 2002:a14:1e28:1::1netmask 64

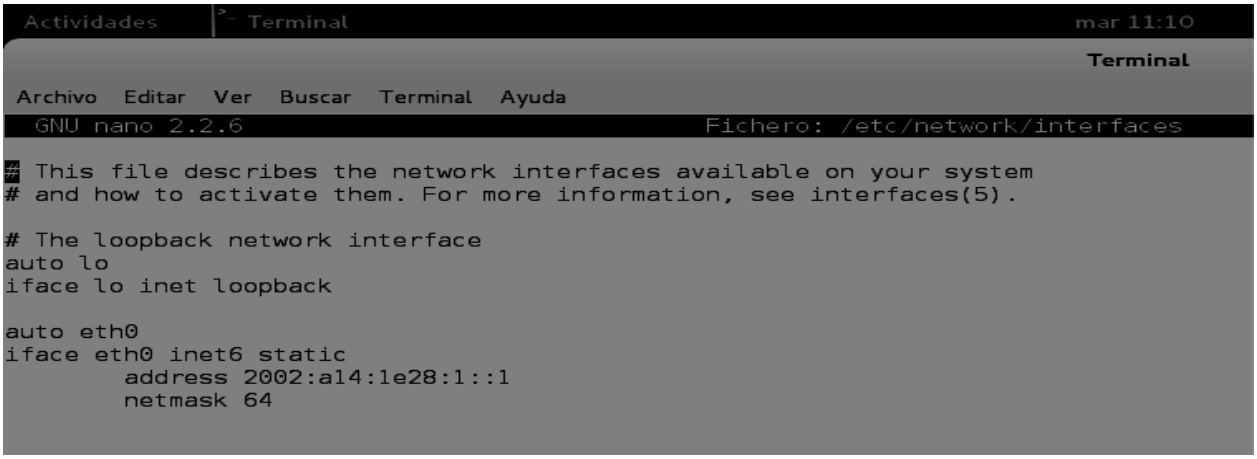

Fig. 4.2 configurando la interfaz eth0

Paso #3
Deshabilitamos la interfaz eth0
Con el comando **ifdown eth0**

Paso #4
Posteriormente habilitamos la interfaz eth0 con el comando
ifup eth0

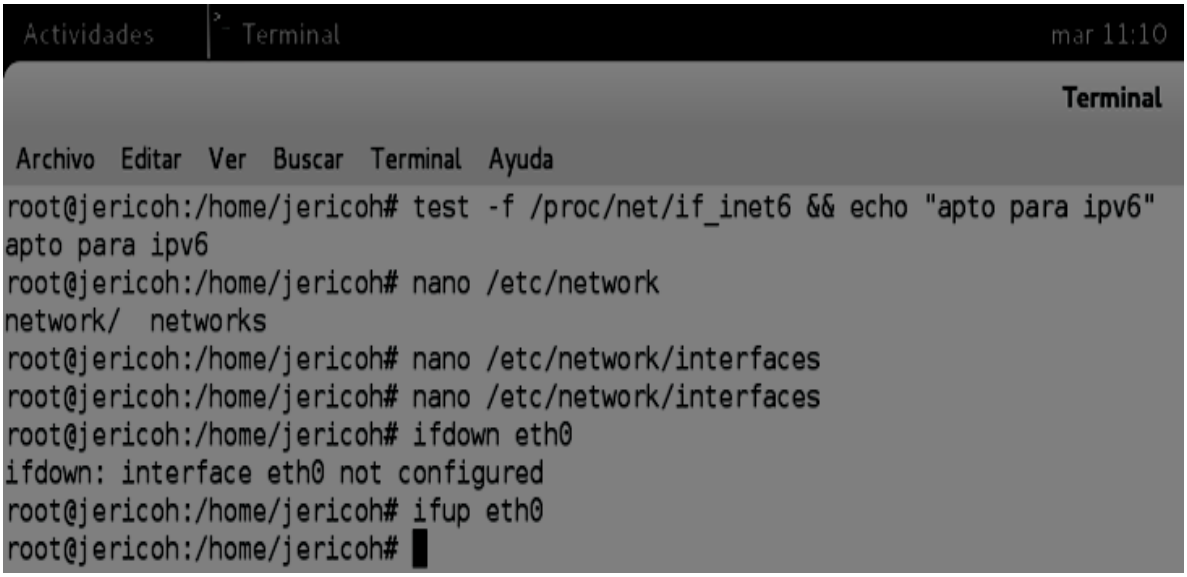

fig. 4.3, utilización de los comandos ifdown e ifup

Paso #5
Instalamos el servidor dhcp
con el comando
apt-get install radvd

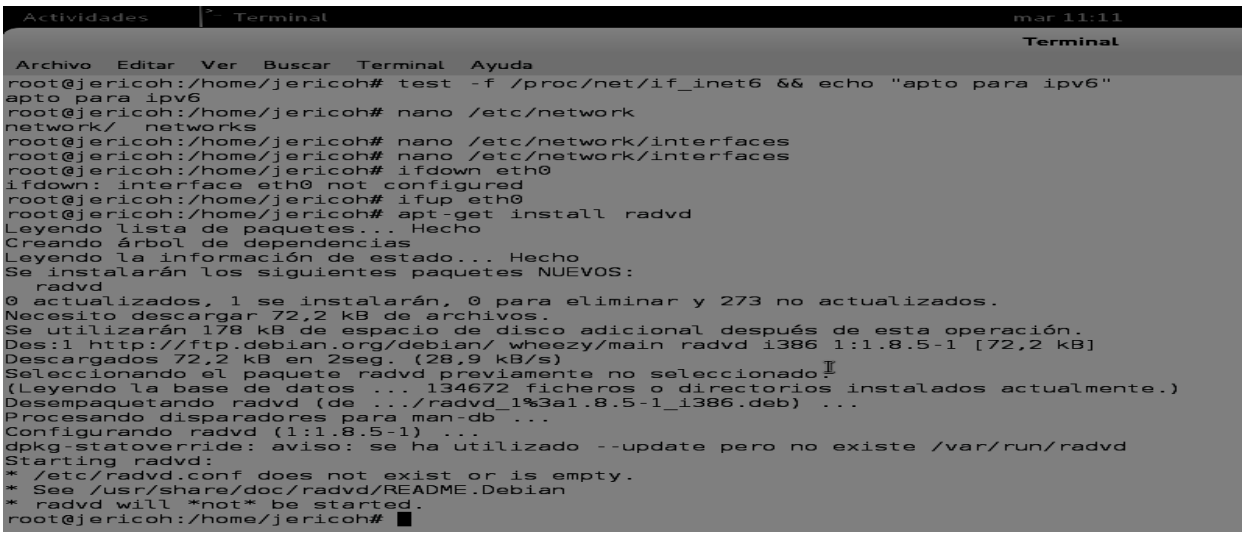

fig. 4.4, instalación del servidor DHCP

Paso #6

Creamos la configuración del servidor dhcp en nano con el comando **nano /etc/radvd.conf**

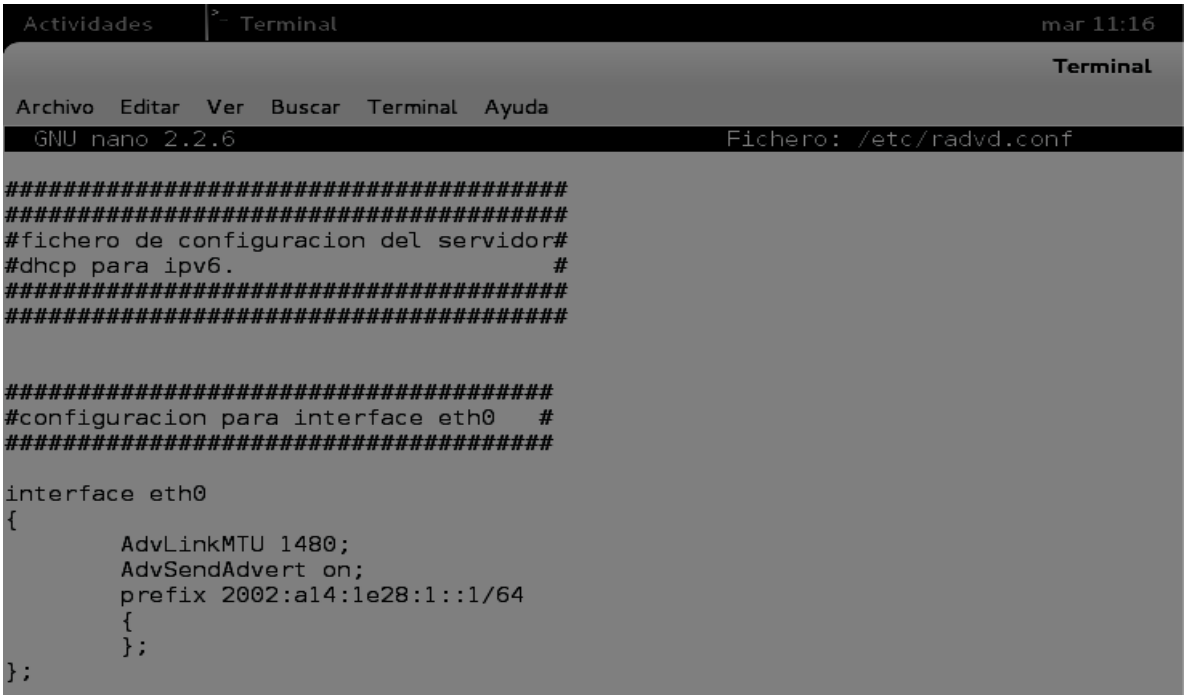

Fig.4.5, creando la conf. del servidor DHCP

Paso #7

Por ultimo

Reiniciamos para que se carguen todas las configuraciones e interfaces con el comando **reboot** desde la terminal.

Hecho esto conectamos la otra computadora por medio de un swich en la cual por medio de la terminal digitamos el comando **ifconfig** para ver nuestra dirección ipv6 y en la otra computadora ya nos aparecerá que está conectada a nuestra dirección ipv6.

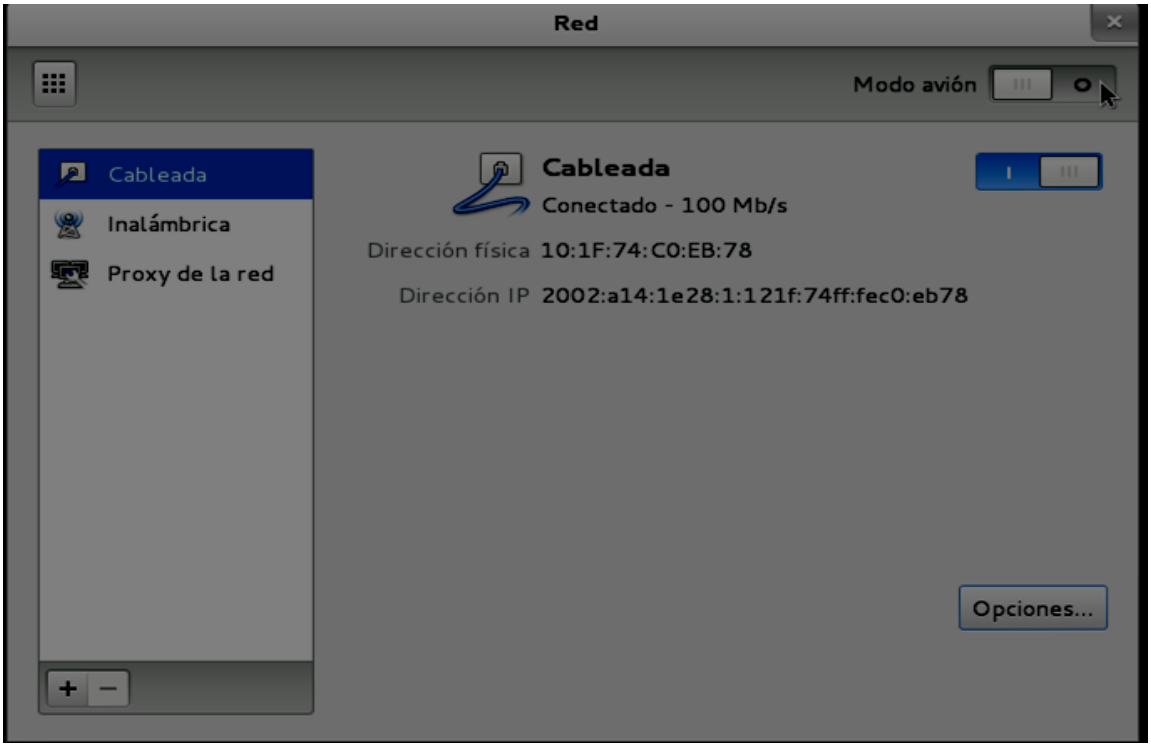

fig. 4.6, utilización del comando reboot.

4.2 CONFIGURACION DE UN SERVIDOR WEB CON IPV6

Paso #1

Desconectamos el fichero /etc/sysctl.conf en la parte

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

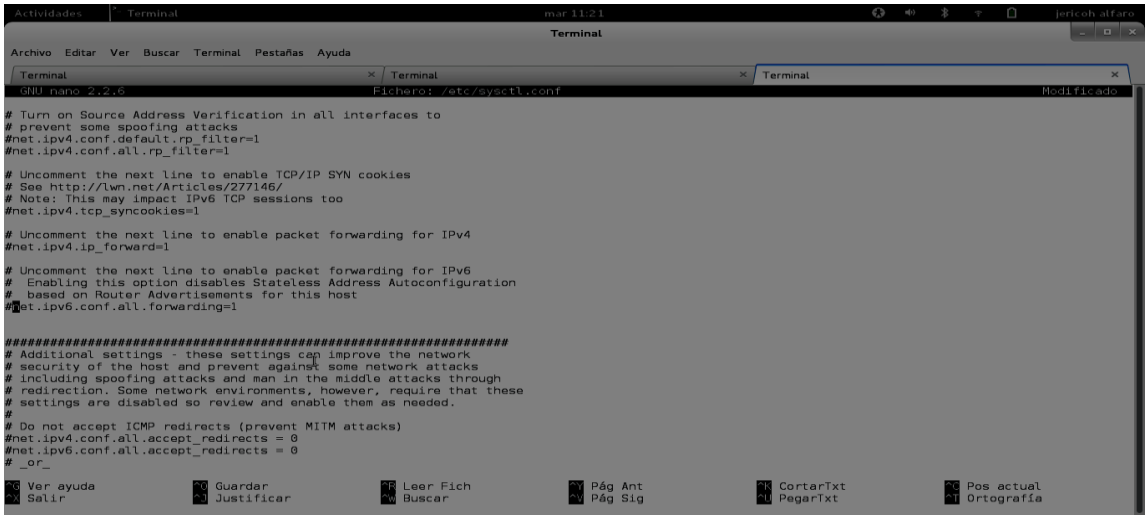

Fig.4.7 desconectando el fichero /etc/sysctl.conf.

Paso #2

nos debe de quedar así

net.ipv6.conf.all.forwarding=1 como se muestra en la imagen

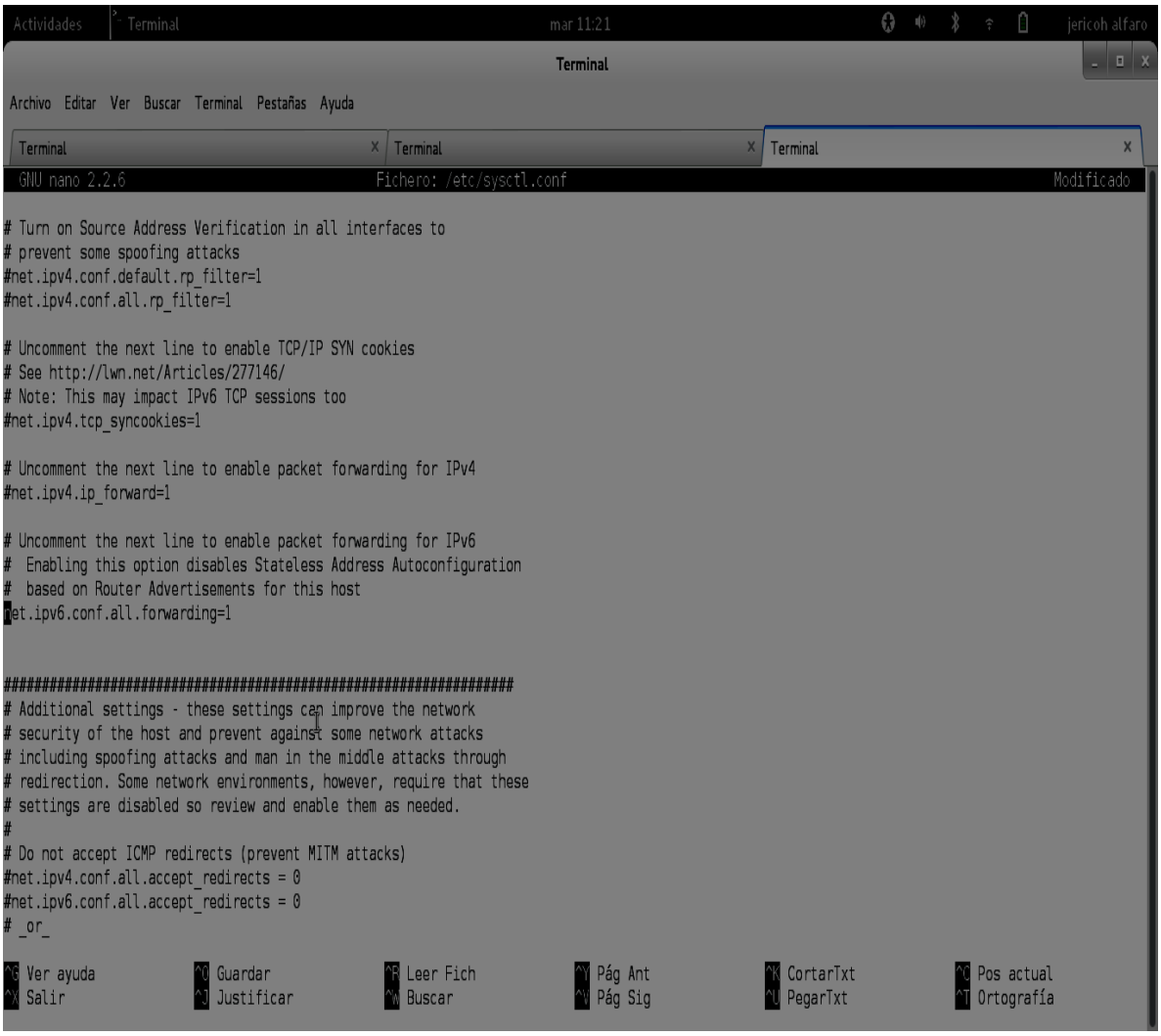

Fig.4.8 mostrando la desconexión del fichero

Paso #3

configuración de apache para que escuchen ipv6

Digitamos el comando

nano /etc/apache2/ports.conf

en nuestra terminal y nos aparecerá esto donde comentamos el puerto ochenta para que escuche ipv6

If you just change the port or add more ports here, you will likely also

```
# have to change the VirtualHost statement in
# /etc/apache2/sites-enabled/000-default
# This is also true if you have upgraded from before 2.2.9-3 (i.e. from
# Debian etch). See /usr/share/doc/apache2.2-common/NEWS.Debian.gz and
# README.Debian.gz
#comentamos estas dos líneas para evitar conflictos con servidor apache en
escucha de ipv4
#NameVirtualHost *:80
#Listen 80

<IfModule mod_ssl.c>
    # If you add NameVirtualHost *:443 here, you will also have to change
    # the VirtualHost statement in /etc/apache2/sites-available/default-ssl
    # to <VirtualHost *:443>
    # Server Name Indication for SSL named virtual hosts is currently not
    # supported by MSIE on Windows XP.
    Listen 443
</IfModule>

<IfModule mod_gnutls.c>
    Listen 443
</IfModule>

#configuración de escucha del servidor web para ipv6
NameVirtualHost [::]:80
Listen [::]:80
```

Paso #4

Reiniciamos el servicio de apache2 con el comando

/etc/init.d/apache2 restart

Comprobamos los puertos que tiene abiertos nuestro servidor debería de aparecer

el puerto 80 abierto.

Esto se hace con el comando para ipv6

nmap -sV -6 2002:a14:1e28:1::1

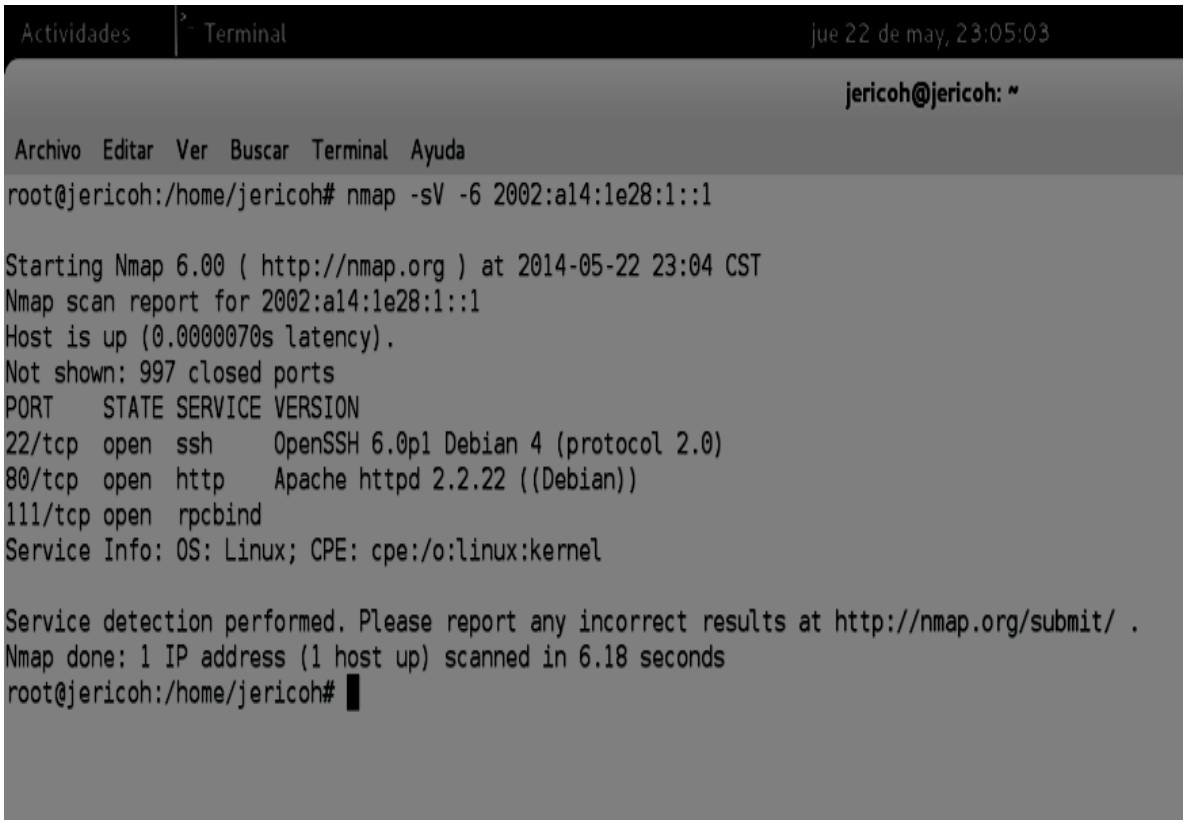

Fig.4.9 probando el comando nmap.

Paso #5

Por ultimo

Reiniciamos la computadora para evitar fallas con el comando **reboot** ya en la otra computadora que está conectada a nuestra red digitamos el comando ifconfig para ver nuestra dirección y luego hacemos **ping6 -c10 -I eth0 fe80::7a2b:cbff:feed:f472** y si todos los paquetes enviados son recibidos entonces tenemos conexión

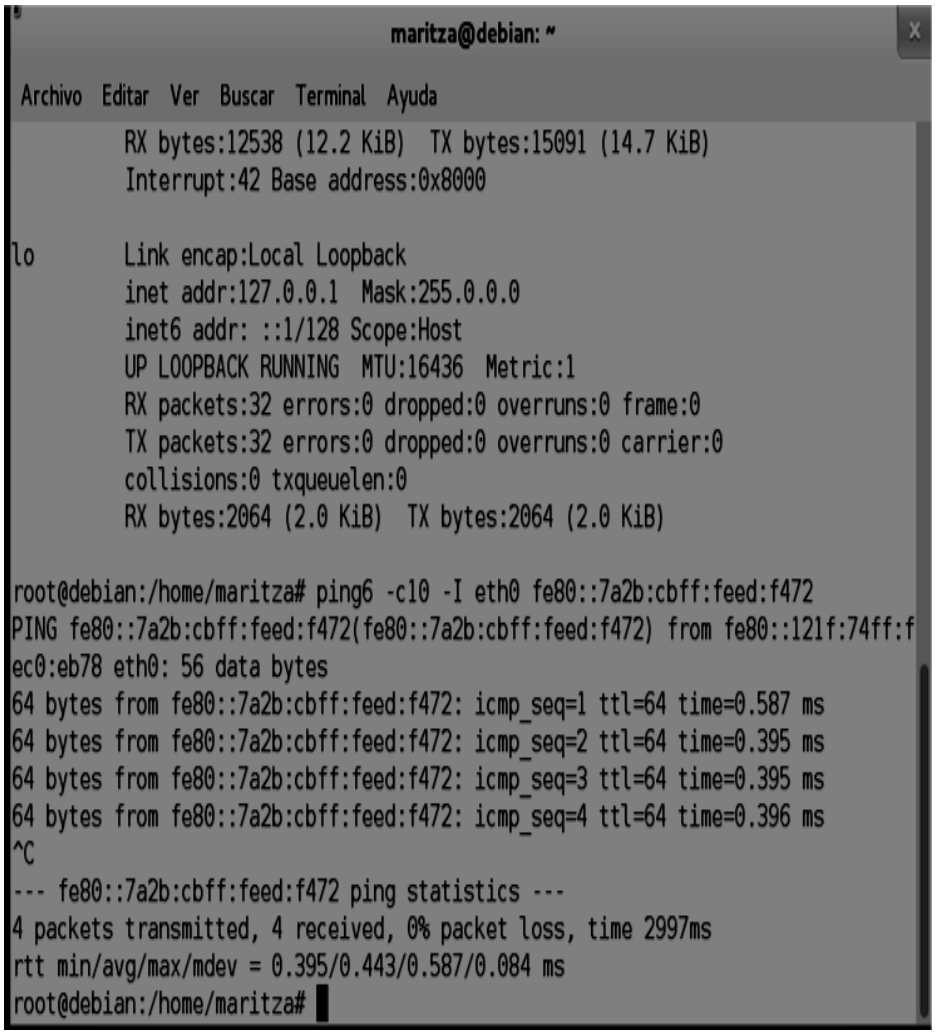

Fig.4.10 probando conexión

Paso #6

Otra manera de hacer ping es a nuestra IP estática, en este caso digitamos el comando

ping6 -c1 -I etho 2002:a14:1e28:1::1

ping 6 = porque nuestro servicio es ipv6

-c1 **=** es la cantidad de veces que haremos ping

Dado esto todos los paquetes enviados son recibidos, tenemos conexión.

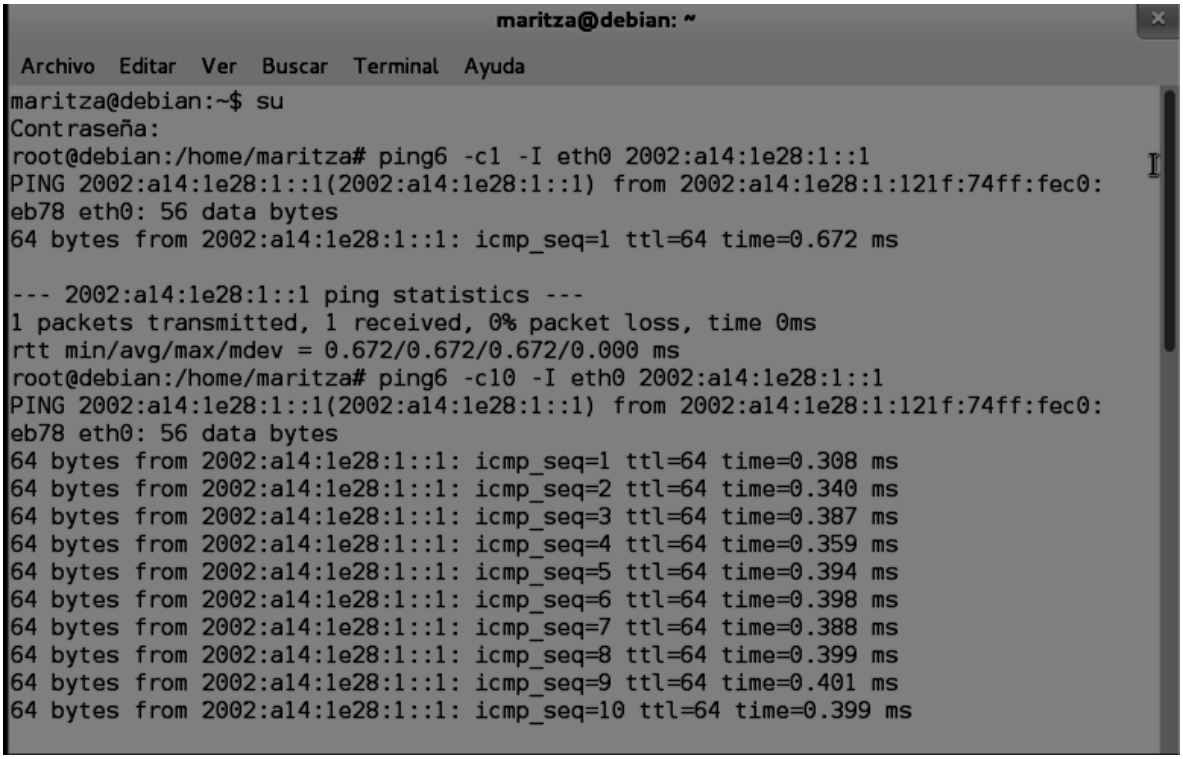

Fig.4.11, haciendo ping a la IP estática

Paso #7

Ponemos la dirección ipv6 en nuestro navegador la cual es

2002:a14:1e28:1::1

Nos mostrara nuestra conexión:

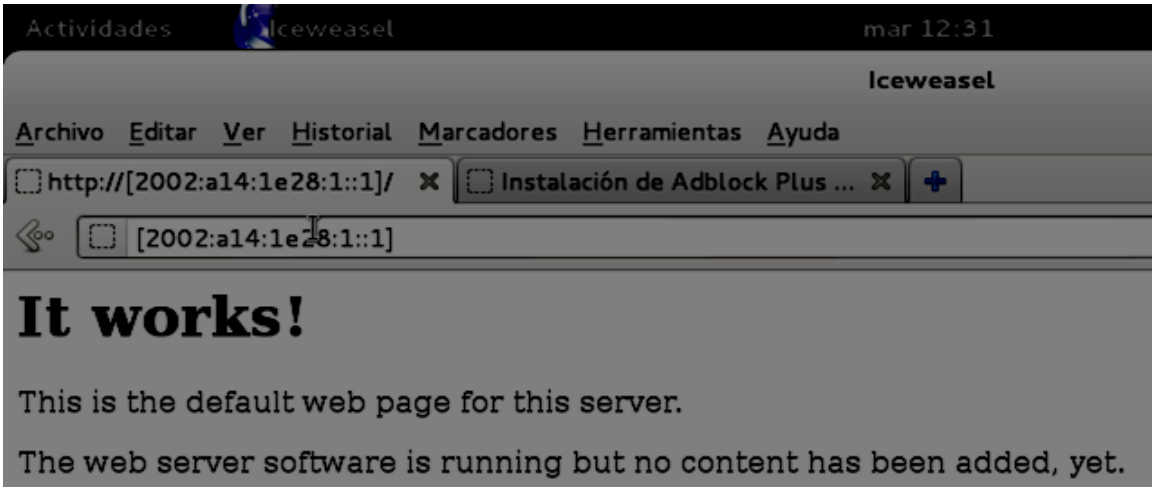

Fig.4.12, mostrando conexión con el servidor

5.- CONCLUSIONES.

Mediante la realización de este proyecto se ha podido comprobar que es posible implementar los servicios básicos y bien conocidos, como DHCP y HTTP en sus versiones para IPV6.

Como equipo de trabajo hemos llegado a la conclusión de que aunque las aplicaciones soporten perfectamente el protocolo IPv6, es necesario forzar expresamente el uso del protocolo mediante algún parámetro del tipo “-6” por línea de órdenes, o utilizando corchetes en la GUI del navegador. Esto puede ser confuso para muchos usuarios, si deben suponer que el problema para comunicar con un servidor es por usar la versión 4 (cuya existencia probablemente desconozcan) en lugar de la versión 6. Es por esto que las transiciones desde IPv4 a IPv6 se están haciendo de forma escalonada y por el momento en nuestro país no se habla demasiado de la adopción de la nueva versión, contrario a otros países, como por ejemplo en sur américa donde existen políticas para realizar esta transición de manera integral.

Como estudiantes podemos evidenciar que es bastante el esfuerzo que tienen que realizar los administradores de redes o compañías que emplean los mecanismos de transición de **IPV4** a **IPV6,** ya que deben elegir el mecanismo más adecuado.

6.- RECOMENDACIONES.

1.- Como estudiantes de la carrera de informática recomendamos que los estudiantes hagamos un buen uso de las herramientas disponibles para la simulación de conexión de redes, específicamente sobre la configuración de servicios con IPV6, con el fin de obtener un buen nivel de conocimientos teóricos prácticos sobre este tema.

2. Que la Universidad Luterana Salvadoreña a través de la carrera de Licenciatura en Ciencias de la Computación se involucre más a fondo mediante investigaciones que den resultados positivos para la migración total del protocolo IPv6, y que puedan invertir en equipos que permitan desarrollar la parte experimental en los alumnos.

3. Que la ULS imparta talleres o seminarios sobre la transición de IPv4 a IPv6 a los alumnos de la carrera de Lic. en Ciencias de la Computación, para que los graduandos salgan a implementar esos conocimientos en el campo laboral.

7.- BIBLIOGRAFIA.

- ✓ TCP-IP. Arquitectura, protocolos e implementación con IPv6 y seguridad de IP Feit, Sidnie Madrid [etc.]: McGraw-Hill/Interamericana de España, 1998

- ✓ Oracle IPv6 Administration Guide
  http://dlc.sun.com/pdf/817-0573/817-0573.pdf

- ✓ radvd.conf Linux Manu Page
  http://linux.die.net/man/5/radvd.conf

- ✓ Internet Protocol, Version 6 (IPv6) Specification
  http://www.faqs.org/rfcs/rfc2460.html