INSTITUTO TECNOLÓGICO Y DE ESTUDIOS
SUPERIORES DE MONTERREY

CAMPUS MONTERREY

PROGRAMA DE GRADUADOS EN TECNOLOGÍAS DE INFORMACIÓN Y ELECTRÓNICA

MODELO DE MIGRACIÓN DE IPV4 A IPV6 PARA LA RED DEL SISTEMA ITESM

TESIS

PRESENTADA COMO REQUISITO PARCIAL PARA OBTENER EL GRADO ACADEMICO DE:

MAESTRO EN CIENCIAS CON ESPECIALIDAD EN TECNOLOGÍA INFORMÁTICA

POR:

JESÚS PIÑA SALDAÑA

MONTERREY , N.L. **DICIEMBRE 2005**

INSTITUTO TECNOLÓGICO DE ESTUDIOS SUPERIORES DE MONTERREY

DIVISIÓN DE TECNOLOGÍAS DE INFORMACIÓN Y ELECTRÓNICA

PROGRAMA DE GRADUADOS EN TECNOLOGÍAS DE INFORMACIÓN Y ELECTRÓNICA

Los miembros del comité de tesis recomendamos que la presente tesis del Ing. Jesús Piña Saldaña sea aceptada como requisito parcial para obtener el grado académico de Maestría en Ciencias con Especialidad en Tecnología Informática.

Comité de tesis:

_____

Dr. Raúl Ramírez Velarde
Asesor

_____

Kristian Manuel Ayala Moreno, MC.
Sinodal

_____

Takenori Makita Tafoya, MC.
Sinodal

_____

David Alejandro Garza Salazar, PhD.
Director del Programa de Graduados en Tecnologías de Información y Electrónica
Diciembre de 2005

MODELO DE MIGRACIÓN DE IPV4 A IPV6 PARA LA RED DEL SISTEMA ITESM

POR:

JESÚS PIÑA SALDAÑA

TESIS

Presentada al Programa de Graduados en Tecnologías de Información y Electrónica

Este trabajo es requisito parcial para obtener el grado de Maestría en Ciencias con Especialidad en Tecnología Informática

INSTITUTO TECNOLÓGICO Y DE ESTUDIOS SUPERIORES DE MONTERREY

DICIEMBRE 2005

Dedicatoria

A mi madre por darme su apoyo y cariño, e impulsar los proyectos emprendidos a lo largo de mi vida.

Gracias.

Lista de Figuras

Agradecimientos

A Dios, por guiarme por el mejor camino.

Al Dr. Raúl Ramírez Velarde, por todo su apoyo y valiosa asesoría para realizar este documento.

A mis sinodales Kristian Manuel Ayala Moreno y Takenori Makita Tafoya .

A toda la comunidad de open source y a la gente que trabaja en google.

A todos mis amigos Baltasar, Benito, Edgardo, Luis, Pepe, Marcelo, Dreyser, Muñoooz, Porro, Elaine, Patricia, Montse y Sara por compartir conmigo este trayecto y que siempre estuvieron ahí.

A mis amigos de siempre Pedro, Julio y Antonio.

Gracias.

Resumen

Durante algunos años hemos reconocido que la versión 4 de IP está alcanzando sus límites, y la IETF ha estado trabajando en IPv6 desde 1994. Ahora, las especificaciones básicas han sido acordadas e implementadas, y es el momento de seguir adelante, añade el Dr. Brian E. Carpenter, Presidente del comité de Arquitectura de Internet y Director de Programa en la División Internet de IBM[2].

Pero lo más importante es el imparable crecimiento de aplicaciones que necesitan direcciones IP públicas únicas, globales, válidas para conexiones extremo a extremo, y por tanto encaminadores que soporten este protocolo para poder efectuar servicios como: Videoconferencias, Voz sobre IP, seguridad, e incluso juegos.

Este presente trabajo de tesis presenta el trabajo de investigación, configuración y transición del nuevo protocolo que regirá la Internet en un futuro cercano, este es IPv6 (Protocolo Internet versión 6). A través del presente trabajo se pretenden mostrar básicamente dos cosas. Por una parte el proceso de transición recomendado que debe seguir el ITESM para migrar a IPv6 y por un lado, ver todo lo referente a configuración de equipos Linux, encaminadores Cisco y la configuración clientes Windows para formar parte de una red LAN y WAN sobre IPv6.

Es por ello, que el presente trabajo de tesis, presenta una serie de implicaciones que deben considerarse para la migración de este protocolo tomando en cuenta reducir el coste lo menos posible y ser lo m**a**s trasparente para el usuario.

Para ello, se analizaron la infraestructura de red actual y los procesos que interviene sobre ella para poder usar este protocolo independientemente del campus o sede donde te encuentres dentro del sistema tecnológico.

Tomando lo anterior como base para la elaboración del producto final, para poder aprovechar los beneficios que este protocolo nos ofrece, se expone en esta tesis.

Lista de Tablas

Capítulo 1

1 INTRODUCCIÓN

1.1 Situación Actual

Desde principios de la década pasada, la Internet ha venido enfrentando un consecuente y creciente agotamiento de sus recursos básicos. Muchas de las razones de esta merma, se debe a la definición nativa del stack de protocolos TCP/IP y en particular la capa de red, protocolo de Internet versión 4 (IPv4). IPv4 no ha cambiado substancialmente desde su definición inicial y aunque ha probado ser robusto y trabajar en redes globales, está mostrando su imposibilidad de adaptarse a las exigencias actuales. Situaciones indeseables como el agotamiento del bloque de direcciones IPv4 y las condiciones desfavorables que provoca el congestionamiento en aplicaciones de bajo retardo entre otras, son índices claros que hacen pensar en una reestructuración del IPv4 [1].

IPv6 es una tecnología joven que merece atención y por consiguiente un lugar en los límites de la Red Académica. Varios avances han sido ya impulsados en algunos países de la región y, nuestro aporte y apoyo será de mucha utilidad para elevar nuestra apariencia en la visión mundial y regional.

Las tecnologías IP transforma a pasos agigantados el mundo de las comunicaciones, la convergencia tecnológica es uno de los elementos clave para la integración interoperabilidad de los procesos empresariales en tiempo real. Voz, datos, video alguno de lo requisitos para logra esto es la calidad de servicio (QoS) . Debido a que era necesaria una tecnología capaz de tener la menor degradación en cuanto a calidad e servicios en tiempo real se llego a la utilización de este nuevo protocolo de comunicación IPv6 la cual surge de la base del actual protocolo IPv4.

1.2 Motivación

Los esfuerzos de desarrollo e implementación de productos IPv6 están disponibles en la comunidad desde hace algunos años. Consorcios como Internet2, hacen grandes esfuerzos para desarrollar y probar escenarios reales de implementación con la finalidad de preparar y alentar a la adopción de esta nueva tecnología. Redes IPv6, han nacido en diferentes sitios del planeta, manteniendo la prestación de servicios duales intentando no omitir ni denegar servicio a usuarios legítimos. Ejemplos importantes como 6Bone en Norteamérica, IRIS en Europa, REUNA en Sudamérica y muchas otras son prototipos de fuerza que hacen despertar inquietud.

Otro factor importante es que los recursos de Internet como bloques de direcciones IPv6 ya están disponibles y en ciertos casos han sido asignados. La IANA ha dispuesto a cada uno de los Registros Regionales de Internet (LACNIC, ARIN, RIPE NCC Y APNIC) bloques IPv6 para su gestión. Todo esto sugiere que la línea de vida de IPv6 a superado al menos los pasos básicos de aceptación, que con una debida promoción y publicación, se espera sea adoptado en las próximas décadas.

Por lo consecuente mi trabajo de tesis radica en incorporar al ITESM de nuevo a los esfuerzos de los grupos de IPV6 construyendo un modelo de transición de IPv4 a IPv6 y analizar el impacto que causara esta transición así comprobando que es mejor usar el protocolo IPV6 en la red del ITESM y quitar todos los parches de IPv4 como NAT.

1.3 Objetivo

La presente tesis plantea un modelo de transición para la red del ITESM la cual consistirá en dos fases.

Para la primera fase se usara una herramienta para conectarte dinámicamente a la red de IPv6 del ITESM sin importar en que parte del sistema del Tecnológico te encuentres mediante túneles. En este caso, se creara un análisis de transición de IPv6 a IPv4 con un enfoque sobre la arquitectura actual de red tratando de obtener el menos coste posible ya que el futuro son las aplicaciones de voz sobre IP y de tiempo real que son las que mas ancho de banda consumen, permitiendo saber su comportamiento sobre la nueva generación del protocolo de Internet IP.

La segunda fase consistirá en implementar una infraestructura de red IPv6 paralela a IPv4 , que provea un manejo eficiente de aplicaciones y haga frente a los actuales proyectos desarrollados por el Instituto Tecnológico De Estudios Superiores De Monterrey.

1.3.1 Objetivos específicos

Teniendo las herramientas que servirán para realizar la interconexión entre las entidades, la planificación de la implementación se cumplirá la siguiente línea:

- Determinar servicios actuales y nuevos a ser implantados para la infraestructura IPv6.
- Estudiar los distintos escenarios de implantación fundamentados en las estrategias de coexistencia.
- Dictaminar los requerimientos necesarios para la implementación.
- Establecer una serie de lineamientos, recomendaciones y requerimientos para la implementación de IPv6, dirigido a los nodos de la Red del ITESM.
- Estudiar y proponer políticas de asignación de los bloques de direcciones IPv6 a entidades de la Red del ITESM.
- Comparar el avance de esta tecnología con otras universidades.
- Migrar la nueva red proporciona por LANIC.
- Documentar Ipv6
- Reducir al máximo el coste de la migración.

Capítulo 3

3 TRANSICIÓN IPV4 A IPV6 EN EL ITESM

La migración ha de verse como un proceso evolutivo que comenzará con la implantación del nuevo protocolo en las infraestructuras de comunicaciones, para continuar luego con la modificación de aplicaciones, servicios y sistemas de gestión de las mismas, acabando con la extensión del protocolo a la mayor parte de los dispositivos interconectados a la red de redes.

Durante la implantación del nuevo protocolo los sistemas han de verse afectados lo menos posible, con el fin de que la migración en la capa de red se pueda realizar de forma escalonada y según las necesidades que vayan surgiendo. Sólo en la última fase se contempla la posibilidad de que desaparezca finalmente el protocolo de red actual, IPv4. Aunque esto puede ser que nunca llegue a producirse, ya que ambas tecnologías
deben poder convivir sin demasiados problemas. En la figura 12 se muestra la Arquitectura de una transición..

Figura 12. Arquitectura de transición(Tomada de [39]).

3.1 Requisitos

Entre los requisitos que hemos de contemplar en el proceso de migración, están el poder ofrecer a nuestros usuarios al menos lo siguiente:

1. Acceso a la nueva red, sea cual sea la infraestructura de acceso a la red utilizada. Es decir, crear un estándar para el acceso al nuevo protocolo de red.

2. Acceso a los servicios básicos de red, necesarios para utilizar el nuevo protocolo.

3. Acceso a los servicios de información con IPv6, necesarios para utilizar los recursos informáticos comunes de la organización.

4. Documentación y apoyo técnico a los usuarios, para ayudarles a realizar la migración al nuevo nivel de red e informarles de las ventajas que se obtienen.

5. Servicio de soporte de los problemas de migración que puedan seguir.

6. Servicio de gestión de los rangos de direccionamiento (address space) asignados al nuevo protocolo.

7. Servicio de gestión de la seguridad en las redes corporativas (filtrado, auditoria, control de acceso, copias de backup, etc).

3.2 Arquitectura de la nueva red

Para introducir el nuevo protocolo de red probablemente habremos de modificar la estructura y arquitectura de nuestra infraestructura de comunicaciones.

Esto podría ser así, tanto para el nivel de enlace, como para el nivel de red (niveles 2 y 3 del modelo de referencia OSI) y sin afectar a niveles superiores.

Una de las soluciones más deseables para el desarrollo de la nueva red corporativa IPv4 e IPv6, estriba en tener la posibilidad de acceder a los segmentos de red IPv6 desde cualquiera de los puntos de acceso a la red actual. Es así, porque hay que pensar que muchos ordenadores y sistemas de los que están funcionando en la red IPv4 tendrán que disponer de dirección IPv6, y por tanto, cuanto más sencillo sea acceder a la nueva red, menor será la inversión necesaria en coste y en tiempo.

Para ello, si las redes de acceso local están basadas en tecnología Ethernet, caben dos soluciones técnicas:

1. La red IPv4 y la red IPv6 conviven en los mismos segmentos de red (doble pila). Lo que implica la comparación de la misma red física (y por tanto el mismo dominio de

broadcast y la misma VLAN) entre todos los dispositivos de red, independientemente de que estén utilizando IPv4 o IPv6 a nivel de red .

2. La red IPv4 y la red IPv6 utilizan distintos segmentos de red (red paralela donde solo existirá IPv6). O lo que es lo mismo, la división de los dominios de broadcast (también llamados segmentos de red) mediante la técnica de etiquetado VLAN de las diferentes redes.

3.2.1 Red con doble pila de protocolos

Esta resulta ser la técnica más sencilla de implementar. No requiere duplicar redes ni interfaces de red para que los sistemas accedan a IPv4 o a IPv6. Sólo es necesario que los sistemas operativos de los ordenadores y encaminadores sean capaces de utilizar ambas pilas de protocolos en paralelo, distinguiendo el paquete en el momento de la recepción por medio de la cabecera de nivel de red y más concretamente a través del campo de versión de protocolo IP.

La desventaja principal de este método está en que ambas redes podrían llegar a interferir entre sí, sobre todo en los casos en que los recursos de red estén explotados al límite antes de introducir IPv6, o en los casos en que los routers implicados no tuviesen las capacidades necesarias para encaminar los paquetes de ambos niveles de red. Esta problemática, si bien será poco frecuente en redes corporativas de pequeña dimensión, sí será necesario analizarla en profundidad en las redes de los proveedores de servicio a terceros o en las que se deba garantizar estrictamente la calidad de servicio. Un ejemplo de esta red se muestra en la figura 13 y 14.

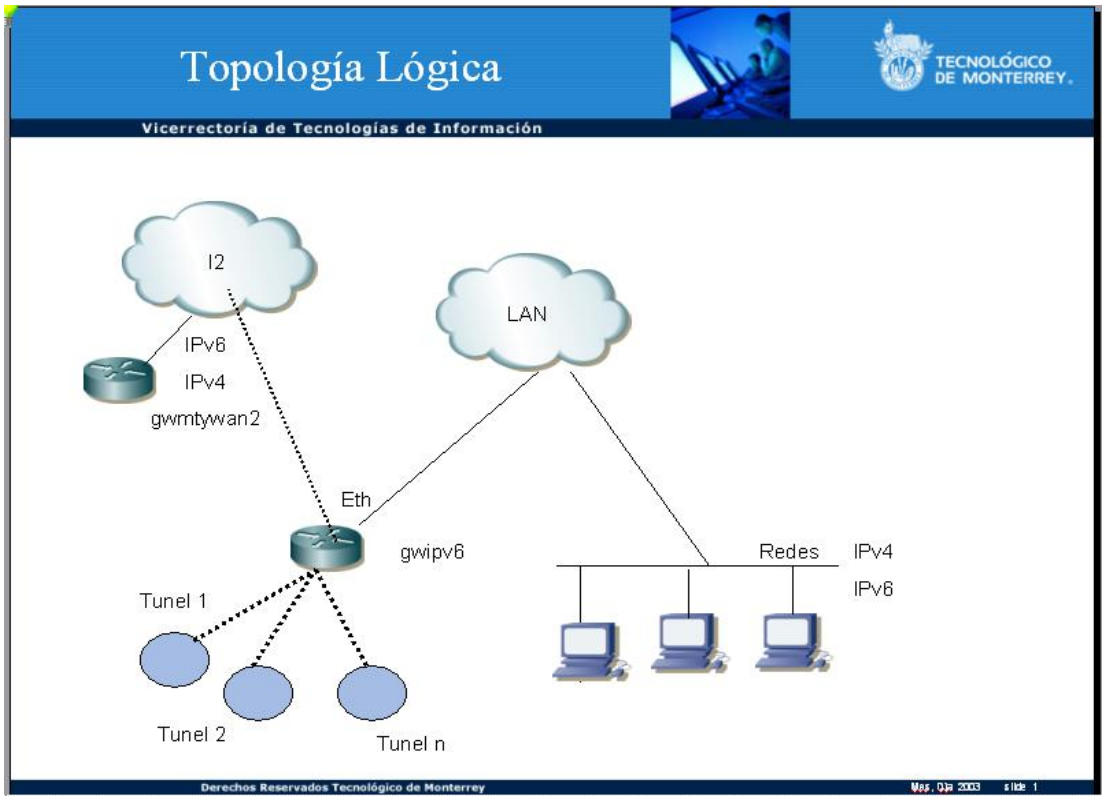


Figura 13. Red con doble pila de protocolos.

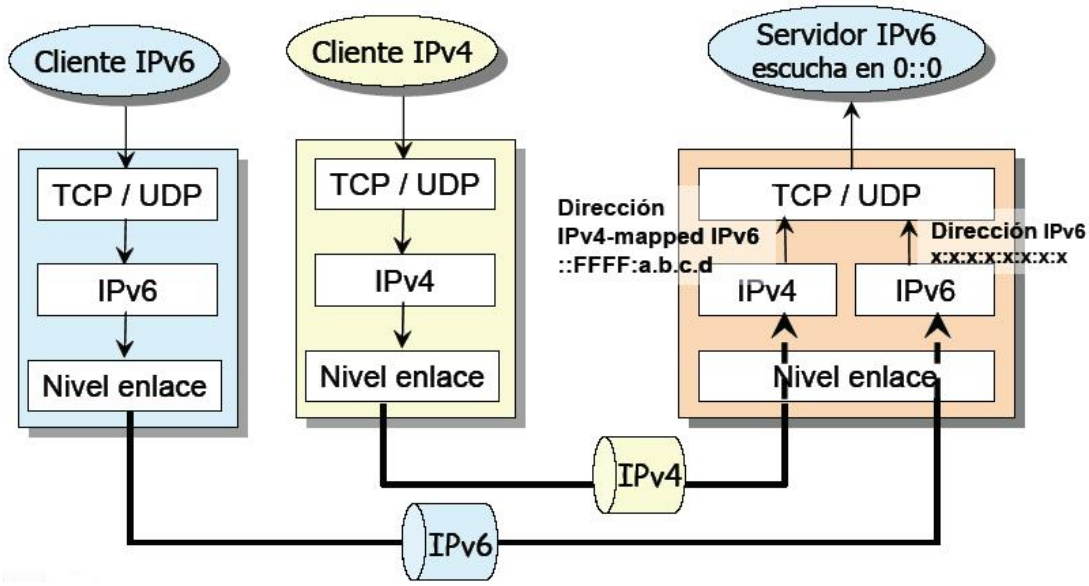


Figura 14. Aplicaciones servidor nodo dual(Tomada de [39]).

3.2.2 Red paralela IPv6

Esta técnica consiste en separar los segmentos físicos de red por los que circularán los paquetes IPv6 de aquellos por los que circulan en la actualidad los paquetes IPv4. Esto implica que también los enrutadores habrán de ser diferentes a los utilizados en la red IPv4, lo que, en general, supondrá un esfuerzo extra.

Esta solución es la más indicada en redes con altas exigencias de calidad y de estabilidad, ya que evita las posibles interferencias entre ambos protocolos de manera drástica. Hoy en día, gracias a la segmentación de redes ethernet utilizando las técnicas de VLAN, la red paralela IPv6 puede no ser tan costosa en hardware, pero aún así, habría un alto coste de configuración, sobre todo si se considera necesario llevar las dos redes a los equipos finales de usuario. La figura 15, ejemplifica esta red.

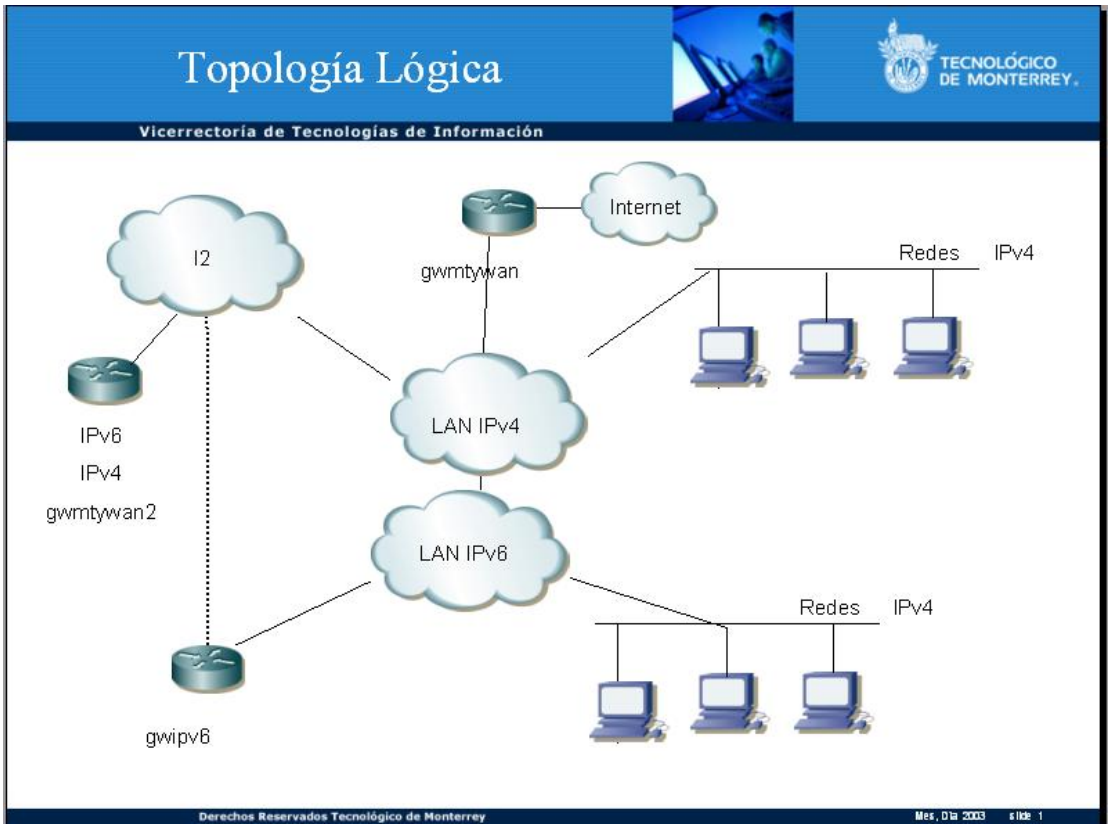


Figura 15. Red paralela ipv6.

Capítulo 4

4 CONFIGURACIÓN GENERAL

Antes de comenzar la configuración particular de los equipos es necesario hacer alcances de la configuración básica y necesaria para poder trabajar con el protocolo en maquinas Linux y Windows y encaminadores Cisco. Las configuraciones que vienen a continuación pueden ser revisadas en [7], [8], [10], [14] y [15]. Si bien no todos ellos son específicos de IPv6 también esclarecen situaciones y configuraciones que se realizan de forma similar en IPv4.

4.1 Máquinas Linux

4.1.1 Requisitos

- Núcleo 2.2.x o superior.

4.1.2 Configuración Linux

Antes de cualquier uso del protocolo en el S.O. GNU/Linux se necesita cargar el modulo ipv6, para esto existen varias formas de hacerlo:

En forma manual: esto quiere decir que una vez que se inicio Linux, se abre una consola y como ***root*** se escribe:

[root@ipv6 root]# modprobe ipv6

Con esto se carga el modulo y ya es posible comenzar a utilizar el protocolo, ya sea asignar direcciones, configuraciones, etc.

Una vez echo esto ya se esta en condiciones de continuar con la configuración de cualquier tipo. Podríamos por ejemplo hacer un /sbin/ifconfig y se deberíamos obtener algo como:

eth0 Link encap:Ethernet HWaddr 00:04:75:81:26:45
inet addr:146.83.206.114 Bcast:146.83.206.255 Mask:255.255.255.0
inet6 addr: fe80::204:75ff:fe81:2645/10 Scope:Link
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:3019997 errors:0 dropped:0 overruns:30 frame:0

TX packets:1570211 errors:0 dropped:0 overruns:0 carrier:0
collisions:157201 txqueuelen:100
RX bytes:439717982 (419.3 Mb) TX bytes:885637606 (844.6 Mb)
Interrupt:10 Base address:0xbc00

lo Link encap:Local Loopback
inet addr:127.0.0.1 Mask:255.0.0.0
inet6 addr: ::1/128 Scope:Host
UP LOOPBACK RUNNING MTU:16436 Metric:1
RX packets:19604 errors:0 dropped:0 overruns:0 frame:0
TX packets:19604 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:2998019 (2.8 Mb) TX bytes:2998019 (2.8 Mb)

En este ejemplo podemos apreciar la existencia de una dirección IPv6 del tipo :

fe80::204:75ff:fe81:2645/10

Que es del tipo de auto configuración, esto quiere decir que de forma automática se ha asignado esta dirección. También se ven las direcciones de loopback:

- 127.0.0.1 en IPv4.
- ::1/128 en IPv6.

4.1.3 Configuración de Túnel al enrutador de IPv6

Para poder manejar trafico con IPv6 en redes separadas por enrutadores IPv4 se debe recurrir a los llamados TÚNELES [10]. A través de ellos se envían los paquetes IPv6 encapsulados en paquetes IPv4 hacia otra red que maneje también el protocolo. Con esto se logra unir nubes de IPv6, pero encapsulados en redes de IPv4.

Antes de la creación de los tuneles se necesitan varios datos:

- Dirección IPv4 de nuestro enrutador: 131.178.100.8
- Dirección IPv4 anfitrión : 10.X.X.X
- Dirección IPv6 para el túnel:
  - Dirección ipv6 para el equipo remoto.
  - Dirección IPv6 para el equipo local.

Los comandos a través de consola son los siguientes :

Estas instrucciones crean el túnel con el enrutador:

[root@ipv6 root]# ip tunnel add sixbone mode sit remote 131.178.100.8 local [ipv4 local] ttl 255

[root@ipv6 root]#ip link set sixbone up

Estas instrucciones asignan ip y puerta de enlace a la maquina :

[root@ipv6 root]#ip addr add [ipv6 local] dev sixbone

[root@ipv6 root]#ip route add ::/0 dev sixbone

Esta instrucción permite el flujo trafico homogéneo entre ipv4 y ipv6:

[root@ipv6 root]#echo 1 >/proc/sys/net/ipv6/conf/all/forwarding

Editar el archivo /etc/resolv.conf y agregar esta linea :
nameserver 2001:498:2:2::2

Y listo ya estara lista la maquin apara usar ipv6.

4.2 Máquinas Windows XP

La instalación del protocolo se hace como se explica a continuación. Para agregar direcciones, prefijos y enrutador por defecto se deben ejecutar los siguientes comandos en una ventana de DOS.

Para la instalación de ipv6

C:\ipv6 install

Esta instrucción crean el túnel con el enrutador:

C:\ipv6 ifcr v6v4 10.17.98.152 131.178.100.8

Estas instrucciones asignan ip y puerta de enlace a la maquina :

C:\ipv6 adu 8/2001:498:3:2::2

C:\ipv6 rtu ::/0 8

Al hacerlo de esta forma se pierde la configuración cuando se reinicie el equipo. La manera de hacer permanente esta configuración es crear un archivo con extensión .cmd que contenga estas instrucciones y posteriormente añadirlo en el *Programador de Tareas* para que sea ejecutado cada vez que se inicia el equipo. Una vez hecho esto ya quedara guardado en el equipo correctamente para comenzar a usar el protocolo.

4.3 Enrutador Cisco

Para que una red de redes funcione hace falta que los enrutadores tengan mapas (totales o parciales) de la red. Estos mapas pueden generarse manualmente mediante rutas estáticas o automáticamente mediante protocolos de ruteo como BGP-4. En la isla que se trabajo, se convino protocolos de ruteo y rutas estáticas.

Ejemplo de configuración de túnel en un encaminador cisco para mas información [38].

1. enable
2. configure {**terminal** | **memory** | **network**}
3. interface tunnel *tunnel-number*
4. ipv6 address *ipv6-prefix/prefix-length* [**eui-64**]
5. tunnel source {*ip-address* | *type number*}
6. tunnel destination *ip-address*
7. tunnel mode ipv6ip

```
interface Tunnel900
 description iBGP+4 --> NIC
 no ip address
 ipv6 enable
 ipv6 address 3FFE:1CF1:3::A/127
 tunnel source Ethernet0
 tunnel destination 200.33.111.6
 tunnel mode ipv6ip
```

Verificando la configuración del túnel

Pasos
1. enable
2. show interfaces tunnel *number* [**accounting**]
3. ping [*protocol*] *destination*
4. show ip route [*address* [*mask*]]

RouterA# **ping** 2001:0DB8:1111:2222::2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:0DB8:1111:2222::2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 20/20/20 ms

RouterA# **show ip route 10.0.0.2**
Routing entry for 10.0.0.0/24
Known via "connected", distance 0, metric 0 (connected, via interface)
Routing Descriptor Blocks:
* directly connected, via Ethernet0/0
Route metric is 0, traffic share count is 1

Versiones de cisco que soportan la configuración de túneles manuales 12.0(21)ST, 12.0(23)S, 12.2(2)T, or 12.2(14)S, 12.3, 12.3(2) T

Ejemplo de la configuración de GBP en encaminador gwipv6wan

```
router bgp 6342
 no synchronization
 bgp log-neighbor-changes
 bgp dampening
 timers bgp 60 300
 neighbor 2001:498:1:2::2 remote-as 6342
 neighbor 2001:498:1:2::2 description gwmtywan2
 no neighbor 2001:498:1:2::2 activate
 neighbor 2001:1888::1:3:1 remote-as 6435
 no neighbor 2001:1888::1:3:1 activate
 neighbor 3FFE:200:1:50::1 remote-as 1654
 no neighbor 3FFE:200:1:50::1 activate
 neighbor 3FFE:C00:8023:25::1 remote-as 109
 no neighbor 3FFE:C00:8023:25::1 activate
 neighbor 3FFE:1CF1:3::B remote-as 6342
 no neighbor 3FFE:1CF1:3::B activate
 neighbor 3FFE:8070:1:11::1 remote-as 278
 no neighbor 3FFE:8070:1:11::1 activate
 neighbor 3FFE:81F1:1:2002:1000::3A remote-as 65272
!
 address-family ipv6
 neighbor 2001:498:1:2::2 activate
 neighbor 2001:1888::1:3:1 activate
 neighbor 2001:1888::1:3:1 prefix-list 6bone-out out
 neighbor 3FFE:200:1:50::1 activate
```

```
 neighbor 3FFE:200:1:50::1 prefix-list 6bone-out out
 neighbor 3FFE:C00:8023:25::1 activate
 neighbor 3FFE:C00:8023:25::1 prefix-list 6bone-out out
 neighbor 3FFE:1CF1:3::B activate
 neighbor 3FFE:1CF1:3::B prefix-list bgp-itesm out
 neighbor 3FFE:8070:1:11::1 activate
 neighbor 3FFE:8070:1:11::1 prefix-list 6bone-out out
 neighbor 3FFE:81F1:1:2002:1000::3A activate
 neighbor 3FFE:81F1:1:2002:1000::3A prefix-list private-as-in in
 neighbor 3FFE:81F1:1:2002:1000::3A prefix-list 6bone-out out
 neighbor 3FFE:81F1:1:2005::1 activate
 neighbor 3FFE:81F1:1:2005::1 prefix-list private-as-in in
 neighbor 3FFE:8240:7013:2::2 activate
 neighbor 3FFE:8240:800A::2 activate
 neighbor 3FFE:8240:800A::2 prefix-list 6bone-out out
 neighbor 3FFE:8240:800D::2 activate
neighbor 3FFE:8240:8017:6::2 soft-reconfiguration inbound
 neighbor 3FFE:8240:8017:6::2 prefix-list 6bone-out out
 neighbor 3FFE:8240:8018::2 activate
 neighbor 3FFE:8240:8026::2 activate
 neighbor 3FFE:8240:8026::2 prefix-list 6bone-out out
 neighbor 3FFE:8240:8030::2 activate
 neighbor 3FFE:8270:0:1::20 activate
 neighbor 3FFE:8270:0:1::20 prefix-list 6bone-out out
 neighbor 3FFE:8280:0:2000::8 activate
 bgp dampening
 network 2001:498::/32
 network 3FFE:8240::/28
 exit-address-family
```

Aquí se aprecian algunas de las configuraciones de las redes involucradas en el ruteo, primero se define la red local, luego se da el extremo remoto del túnel asociado a ciertos parámetros

Aquí se muestra el resultado de show bgp sum.

```
gwipv6#show bgp sum
BGP router identifier 131.178.107.1, local AS number 6342
BGP table version is 914675, main routing table version 914675
547 network entries and 551 paths using 109125 bytes of memory
485 BGP path attribute entries using 29100 bytes of memory
479 BGP AS-PATH entries using 13864 bytes of memory
1 BGP community entries using 24 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
```

```
Dampening enabled. 0 history paths, 0 dampened paths
BGP activity 57898/3548333 prefixes, 580770/580219 paths, scan interval 15 secs

Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
2001:498:1:2::2 4  6342  406015  799734        0    0    0 2w6d     Active
3FFE:C00:8023:25::1
            4   109 1751246 1818432   914675    0    0 1d05h          3
3FFE:8070:1:11::1
            4   278 1915330 1500117   914675    0    0 22:35:37      538
3FFE:81F1:1:2002:1000::3A

3FFE:8240:800D::2
            4 11340  195265  429767        0    0    0 1y14w    Active

3FFE:8240:8012::1
            4  2549  186250  144009        0    0    0 1y43w    Active
3FFE:8240:8016:6::2
Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
            4 64985 1027864 1638975   914675    0    0 1d05h          1
3FFE:8240:8017:6::2
            4 64985  819333 1308164   914675    0    0 1d05h          1
3FFE:8240:8018::2
            4 64600 1046202 1584575   914675    0    0 1d00h          1
3FFE:8240:8026::2
            4  3597 1582434 1596933   914675    0    0 1d05h          4
3FFE:8240:8030::2
            4 65196   14445   34482   914675    0    0 08:55:11       1

3FFE:8280:0:2000::8
            4  3265  579882 1036115        0    0    0 43w0d    Active
```

Capítulo 5

5. DECISIONES DE DISEÑO Y MIGRACIÓN

5.1. Decisión de Arquitectura

Por parte del usuario, la técnica de la doble pila se perfila como la solución técnica más sencilla de implementar para entornos corporativos en los que los potenciales usuarios de IPv6 o resulta imposible prever quiénes serán o están dispersos por todas las subredes de la organización. También en el entorno de los servidores de red es la técnica más cómoda y sencilla de gestionar, puesto que permite reducir al máximo las tareas administrativas en la red y requiere la mínima inversión en hardware.

5.2. Plan de numeración

La red actual de una organización típica tiene varios rangos de direcciones IPv4. En muchos casos, dispondrá de una parte de direccionamiento privado (direcciones IP que no se pueden rutar hacia el exterior) y otra parte de direccionamiento público (direcciones IP que pueden salir al exterior y a las que se sabe cómo llegar desde el exterior).

El plan de numeración se encarga de realizar una asignación de direccionamiento nuevo a cada una de esas redes para así dotarlas de conectividad en IPv6. El plan de numeración también afectará a los encaminadores de paquetes que tendrán que anunciar los prefijos adecuados a cada red según la configuración especificada, así como configurar sus rutas para encaminar sus paquetes en la intranet.

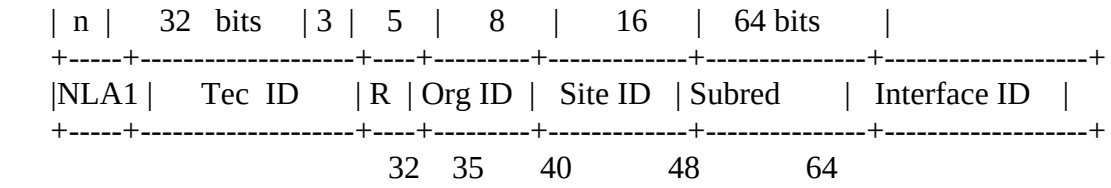
Si el Tec tiene:

OrgName: Tec de Monterrey Campus Monterrey
OrgID: V6MC
Address: Eugenio Garza Sada 2501 Sur
City: Monterrey
StateProv: Nuevo Le=F3n
PostalCode: 64849
Country: MX
NetRange:2001:0498:0000:0000:0000:0000:0000:0000 -
2001:0498:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF
CIDR: 2001:0498:0000:0000:0000:0000:0000:0000/32
NetName: ITESM-IPV6

NetHandle: ITESM-IPV6-NET
Parent: ARIN-001-NET
NetType: Direct Allocation
NameServer: MAINIPV6.IPV6.ITESM.MX
NameServer: DNS1.MTY.ITESM.MX
Comment:
RegDate: 2001-08-23
Updated: 2002-08-05

TechHandle: TA-ORG-ARIN
TechName: Administrador de Dominios
TechPhone: 52-(81)-8358-2000
TechEmail: hostmaster@itesm.mx

2001:0498::/32



Los tres bits + 5 bits de Org ID no se usaran por el momento

Se dejan libres los 8 bits más significativos

m=8

Entonces por sitio agregador se tiene un 2001:0498::/40

Queda 8 bits (a partir de: 2001:0498::/40)

4 bits para Zone ID
4 bits para Site ID

Zone ID (2001:0498:00:/40)

ITESM Backbone 01
Reservado 02-10 (tuneles)
ITESM Zona 1 11 (RMM)
ITESM Zona 2 12 (Occidente)

.....

ITESM Zona 9	19
Reservado	20 - 31

Zone Reservado Se usa para backbone, túneles.

ITESM Backbone (2001:0498:1::/40)

Sistema	00
Monterrey	01
UV	02
GDA	03
....	

Ejemplo :

Nodo	Bloque
gwgdawan	2001:0498:0103:2::/52

Ejemplo : Sistema Túneles

Sistema (2001:0498:0001::/48)

Reservado bloque 10
Direccion Inicial de Bloque
2001:0498:1000:0000/64

Nodo	Bloque
gwipv6	2001:0498:1000:0::/52
gwipv6-2	2001:0498:1000:1::/52
gwmtywan2	2001:0498:1000:2::/52

Sites:
2001:0498::/48

Subredes
2001:0498::/64

5.3. Gestión de la conectividad

Dependiendo principalmente del tamaño de la red interna, hay que tomar una decisión acerca del procedimiento de actualización de las rutas de la organización. Generalmente, caben dos opciones:

1. Utilizar protocolos de encaminamiento interior (IGPs, Interior Gateway Protocols). Éstos normalmente se usan para que los dispositivos tengan conocimiento de la topología de red y puedan encaminar el tráfico a través del camino más eficiente. El protocolo que se usa en el ITESM es EIGRP lo cual será el que usaremos.
2. Utilizar rutas estáticas de configuración semiautomática. Son útiles cuando la topología de red no varía con frecuencia. Se activan de forma automática una vez configuradas en el encaminador y son las más adecuadas para redes de tamaño pequeño o de disposición estática, en las que los enlaces de comunicación no son redundantes.

En el caso de la red IPv6 de nuestro departamento, la solución que hemos considerado más adecuada es la de gestionar rutas estáticas, para los túneles y para la parte de ipv6 puro protocolos de ruteo. Además, dentro de la opción de la doble pila IP para los dispositivos de red, cabe proponer dos soluciones a nivel de encaminamiento. La primera y más sencilla consistiría en hacer que los encaminadores de la red IPv4 pasen a ser también los encaminadores de la nueva red.

La segunda fase, es algo más complicada, pero en algunos casos la más indicada consiste en hacer que los encaminadores de la nueva red sean diferentes máquinas que los de la red actual. Esto implicaría un nivel superior de dificultad en la configuración pero sería la solución más conveniente en los casos en que o bien los encaminadores IPv4 no soportarán algunos de los nuevos protocolos que conforman la solución IPv6 o bien se quiere dar un tratamiento diferente a los paquetes de una y otra red.

En nuestro caso, la solución que nos proponemos adoptar para la migración es una solución mixta entre las descritas. En ella, habrá dos encaminadores/cortafuegos véase la figura 16 .

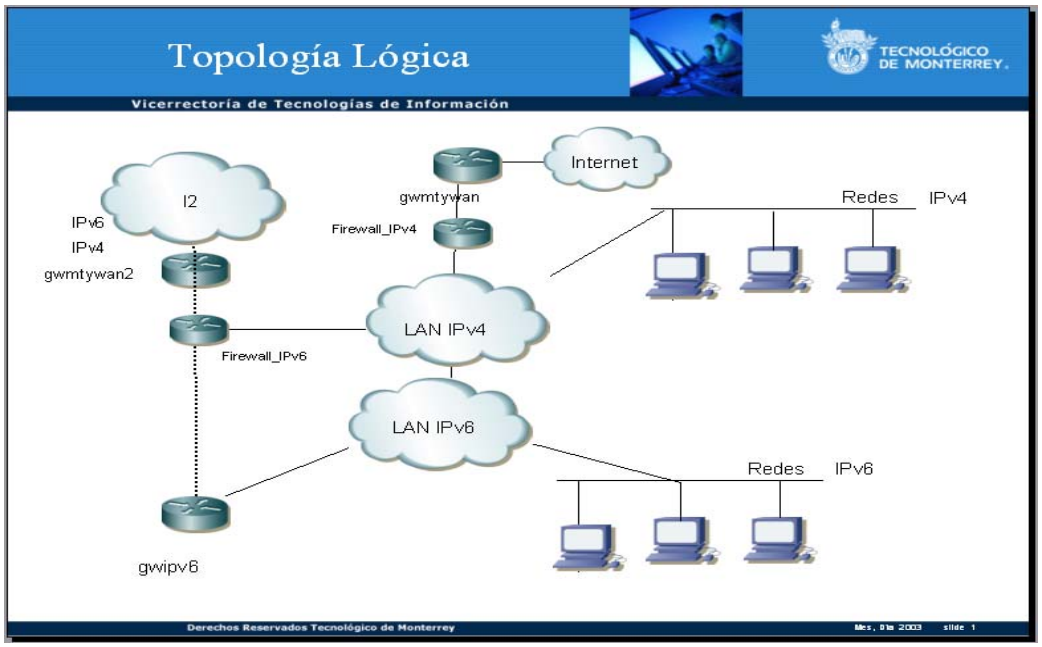


Figura 16. Propuesta para la red Ipv6.

5.4 Consideraciones importantes

Si queremos que los dos protocolos de red compartan una infraestructura común, habremos de tener en cuenta los diversos aspectos que las caracterizan y las diferencian, y que principalmente son:

1. **Configuración Cero:** Mientras que en IPv6 se resuelve de forma más sencilla la auto configuración sin estado del dispositivo de red en tiempo de arranque, sigue sin resolverse a nivel práctico la configuración automática con estado de los anfitrión (también llamada proceso Zero-config) para lo que se prevé utilizar protocolos como DHCP modificados para IPv6 y que al día de hoy están aún en desarrollo.

2. **Ancho de Banda:** El protocolo IPv4 hace uso de las capacidades de broadcast (protocolo ARP) para obtener la dirección física de cada anfitrión en la red (también llamada dirección MAC), para así poder componer la trama de nivel de enlace. La propia definición de broadcast implica que todos los paquetes de este tipo lleguen a todos los dispositivos conectados a un mismo dominio de broadcast. Dado que en IPv6, el broadcast podría no ser necesario, este efecto actuará disminuyendo el ancho de banda disponible en aquellos segmentos de red que sean compartidos entre clientes IPv4 y clientes IPv6. Este efecto, sin embargo, dadas las capacidades

actuales de redes locales y procesadores se prevé que provoque una interferencia prácticamente despreciable entre ambas redes.

3. **Seguridad:** Mientras que los mecanismos de seguridad de protocolo (IPsec) para IPv4 son opcionales, en IPv6 todos los dispositivos que pretendan pertenecer a la red deberían ser capaces de manejarlos, lo que de por si, ya introduce un grado de complejidad en la red que hasta ahora no era de obligado cumplimiento. Además, hay que tener en cuenta que los nodos IPv6, al utilizar el protocolo Neighbour Discovery (ND) para diversas funciones de red, son susceptibles a varios ataques si no se utiliza la arquitectura de seguridad ofrecida por IPsec Authentication Header (AH). Además, como los métodos automáticos de gestión de claves (p.ej. el Internet Key Exchange, IKE) actualmente están en fase de desarrollo, es obligatorio llevar a cabo la gestión manual de las claves de autenticación de los nodos en caso de ser necesario, lo cual puede introducir una gran carga de trabajo de administración si el número de dispositivos a configurar es grande. Por todo ello, en la actualidad se está desarrollando soluciones basadas en IPsec (SEcure Neighbour Discovery, SEND [32]) y en direcciones generadas criptográficamente (Criptographically generated addresses, CGA [33]) que permiten identificar el nodo origen de un paquete y saber si el paquete ha sido modificado en tránsito [34]. Este tipo de problemas es previsible que se solucionarán en un futuro próximo, dada la gran cantidad de gente que está desarrollando la tecnología de este campo.

4. **Rendimiento:** Los balanceadores de carga comerciales son dependientes del nivel de red, estando los actualmente disponibles diseñados para utilizar IPv4. Esto puede ser un problema a la hora de desplegar en la actualidad servicios en producción con el nuevo protocolo de red.

5.5 Costes

Para llevar a cabo una migración sin sorpresas desagradables, habría que sopesar en costes al menos las siguientes tareas administrativas fundamentales:

- Formación del personal no técnico (usuarios) para la implantación de la nueva red en sus dispositivos.

- Formación del personal técnico para la gestión de IPv6 en las redes de la organización .

- Actualización del software necesario, incluyendo el S.O.

- Configuración de los dispositivos a nivel de S.O para utilizar direcciones IPv6.

- Configuración del software de los dispositivos que tengan que manejar varias VLAN.

- Configuración de los diferentes S.O para gestionar las preferencias entre v4 y v6 en caso de que el host destino tenga ambas direcciones.

- Configuración de las aplicaciones de red para que soporten ambos tipos de direccionamiento.

Capítulo 6

6 APLICACIONES Y HERRAMIENTAS

6.1 My SQL

MySQL ha demostrado que puede competir con los grandes nombres del mundo de la gestión de bases de datos, y con la última versión esto es más cierto que nunca. Lo que durante un tiempo se consideró como una sencilla aplicación para su uso en sitios Web, se ha convertido en la actualidad en una solución viable y de misión crítica para la administración de datos. Ahora incorpora muchas de las funciones necesarias para otros entornos y conserva su gran velocidad. MySQL supera desde hace tiempo a muchas soluciones comerciales en velocidad y dispone de un sistema de permisos elegante y potente [35].

En este caso se creo una base de datos llamada ipv6.db con la siguiente estructura :

```
mysql> CREATE DATABASE ipv6;
mysql> USE ipv6;
mysql> CREATE TABLE ipv6 (dir_ipv4 VARCHAR(20),dir_ipv6
VARCHAR(20),responsable VARCHAR(20),gateway VARCHAR(20),mascara
VARCHAR(20),tunel VARCHAR(20),ipv4_dest VARCHAR(20),ipv6_dest
VARCHAR(20));
```

Ejemplo de insertar un campo:

```
INSERT INTO ipv6

VALUES('NULL','2001:498:3:2::2/64','NULL','::/0','NULL','5001','131.178.100.8','2001
:498:3:2::1/64');
```

Levantar el demonio mysql

```
/etc/init.d/./mysql start
```

6.2 PHP

A diferencia de otros lenguajes de programación, PHP se creó específicamente para la generación de páginas web, lo que significa que tareas comunes de programación en este campo como acceder a la información enviada en un formulario y hablar con una base de datos, son a menudo más sencillas en PHP. A esto se añaden valores como el hecho de ser un proyecto de código abierto, gratuito y multiplataforma, por lo que desde la aparición de la nueva versión, PHP 5, no ha hecho sino incrementar aún más su número de usuarios [36].

6.3 DNS

Requerimientos :

- Una maquina con unix (linux, solaris, BSD's, Irix, HP-UX, etc).
- BIND 8.2.4 o superior(obtenerla en http://www.isc.org).
- Dispositivos (computadoras o encaminadores) a los cuales configurar direcciones IPv6.
- Conexiones con IPv6 (nativas o por túnel) para esos dispositivos.

Modo de Preparación :

- La maquina que funcione como DNS deberá contar con una versión que soporte todas las librerías y sockets para IPv6, en mi caso yo empleo SUSE 9 con lo parches recomendados.

- Preferentemente configurar la maquina para trabajar de manera dedicada al Servicio de Nombres, por lo que te recomiendo cerrar los puertos y servicios que no estén relacionados con dicha función.

- Obtener y alojar la distribución de BIND en la maquina que será tu DNS.

- Compilar BIND de manera habitual.

- Configurar tu archivo "named.conf" preferentemente incluyendo las opciones de seguridad.

- Deberás tener por lo menos una zona en la cual vas a ubicar tus registros AAAA o A6 dependiendo de la versión de BIND que instales. Si instalas 8.2.x trabajaras con registros AAAA. Si instalas 9.x podrás usar registros A6.

Por ejemplo, yo tengo la zona "ipv6.item.mx" y mi archivo para esa zona es "ipv6.itesm.mx.zone". El dispositivo al cual se le configuro una IPv6 es una computadora llamada "registroipv6".

En el archivo "ipv6.itesm.mx.zone" se configurara una de las siguientes líneas

```
mainipv6        IN    A       10.17.98.53
mainipv6        IN    AAAA    2001:498:2:2::2
```

Si tienes la opción de contar con dominio inverso, configura tu zona para tener la resolución inversa e introducir los registro PTR. En el caso de tener versiones 8.2.x soportaras zonas X.ip6.int y tendrás la posibilidad de usar registros DNAME. En caso de tener versiones 9.x soportaras zonas ip6.arpa.

Por ejemplo, yo tengo la zona para la delegación inversa de 2001:0498

En mi archivo "named.conf" configure una de las siguientes zonas

```
zone "8.9.4.0.1.0.0.2.ip6.int"  {
        type master;
        file "reverse.zone";
};
```

En el archivo de la zona " 2001:0498.zone" tengo

```
$ORIGIN 4.9.8.0.1.0.0.2.ip6.int.

2.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.2.0.0.0.2.0.0.0    IN    PTR
registroipv6.ipv6.itesm.mx.
```

Es importante considerar que actualmente las versiones de BIND 8.2.x y 9.x, tanto los registro A6 como la zona IP6.ARPA, no son compatibles entre ellas. Por lo que si usa las versiones nuevas tendrás que tomar en cuenta las configuraciones soportadas para versiones 8.2.x. Si trabajas con versiones 8.2.x no podrás soportar los nuevos registros ni la nueva zona. Para mas información [37].

6.4 Aplicación para el usuario final

Esta aplicación fue diseñada para los usuarios finales, la cual arrojara una serie de comandos ya preparados con la configuración necesaria para que solamente los apliques en tu computadora y quede listo el túnel de manera trasparente para el usuario.

Para poder acceder a esta aplicación es necesario contra con usuario y palabra clave proporcionada por el departamento de telecomunicaciones y redes del sistema.

Los datos para poder dar permiso a acceder a esta aplicación serán :

- Matricula :
- Túnel temporal o permanente:
- Descripción del uso:
- Comentarios:

6.4.1 Procedimiento para usar la aplicación.

Altas.- Se entra a la pagina http://registroipv6.mty.itesm.mx/ipv6.html una vez adentro seleccionar altas y proporcionar matricula y dirección ipv4, en caso de no saberla teclear el comando ipconfig (windows) y ifconfig (linux).

La pagina arrogara un serie de comandos que simplemente se copearan y se pegaran en una terminal (linux) o cmd (windows) véase figura 19.

Bajas.- Se entra en la misma pagina anterior y se entra a la opción de bajas y se proporciona la matricula y la dirección ipv4 para borrar el túnel véase figura 20.

Consultas .- En la misma pagina ya mencionada se entra a la opción de consultas y se checa si hay túneles disponibles.

Pruebas.- Algunas pruebas que se pueden hacer para revisar que el túnel funcione correctamente son un ping4 véase figura 21 y un tracert véase figura 22.

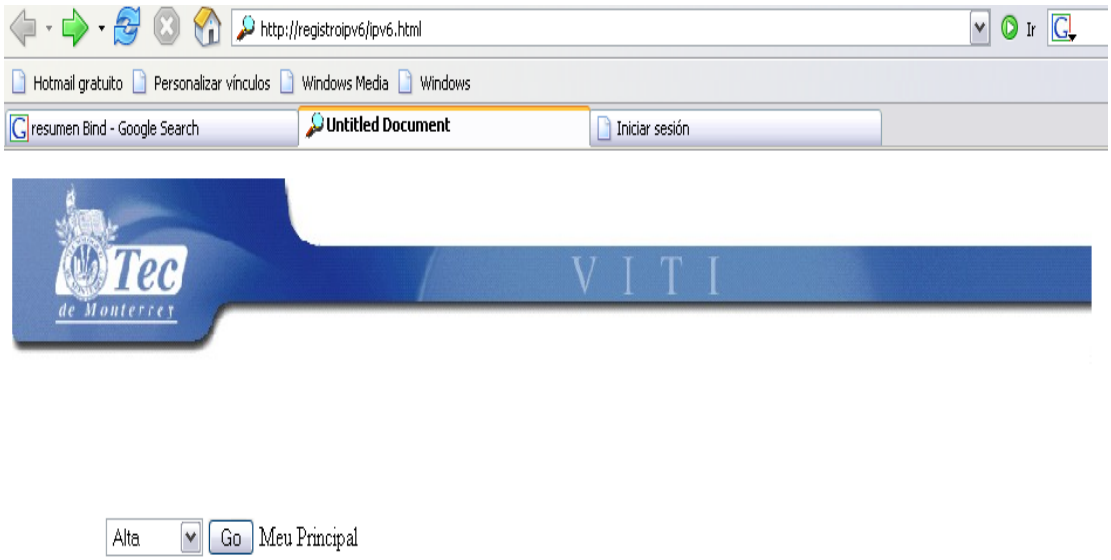


Figura 17 Pagina principal de registro de túneles.

En esta pagina tienes la opción de darte de alta verificar si hay túneles disponibles y dar de baja el túnel.

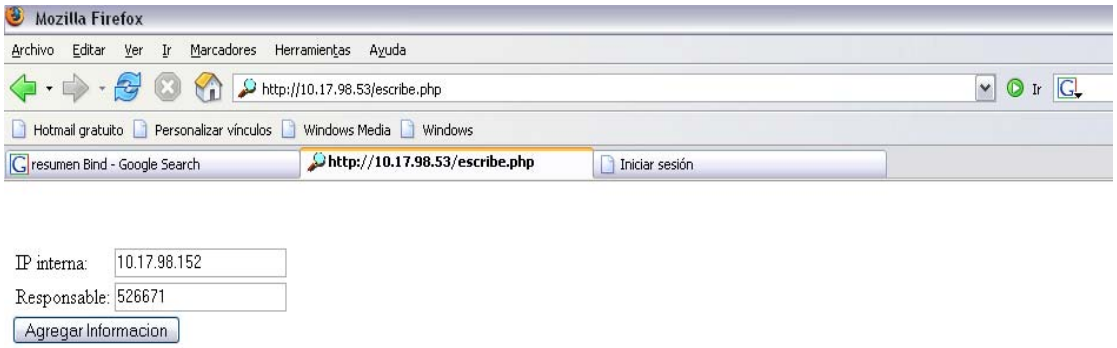


Figura 18 Pagina secundaria donde se proporciona la dirección IPv4.

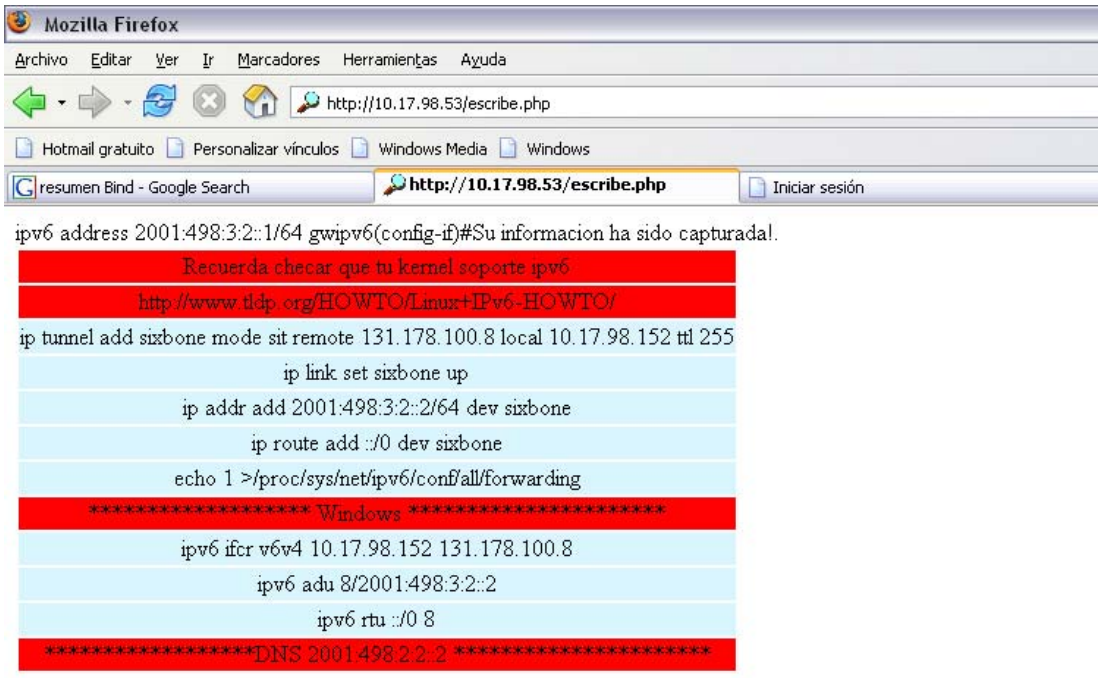


Figura 19 Pagina secundaria donde despliega los comandos a teclear según sistema operativo.

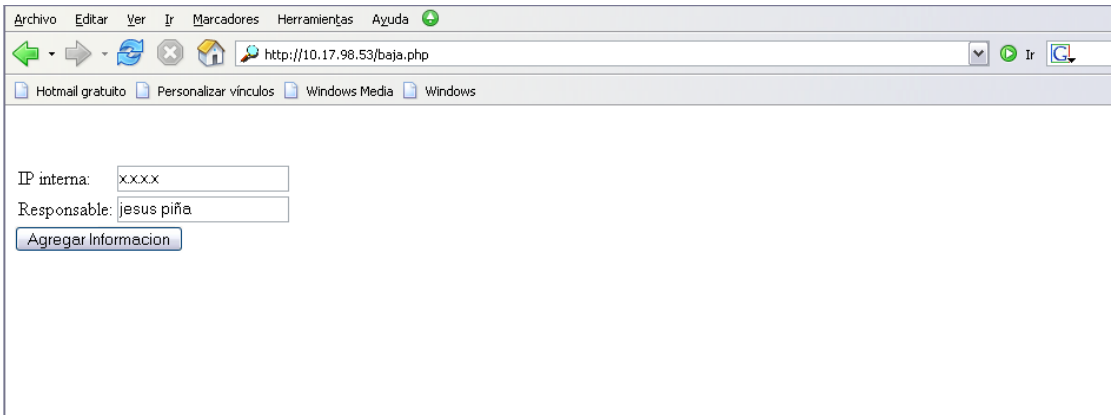


Figura 20 Pagina principal de baja de túneles.

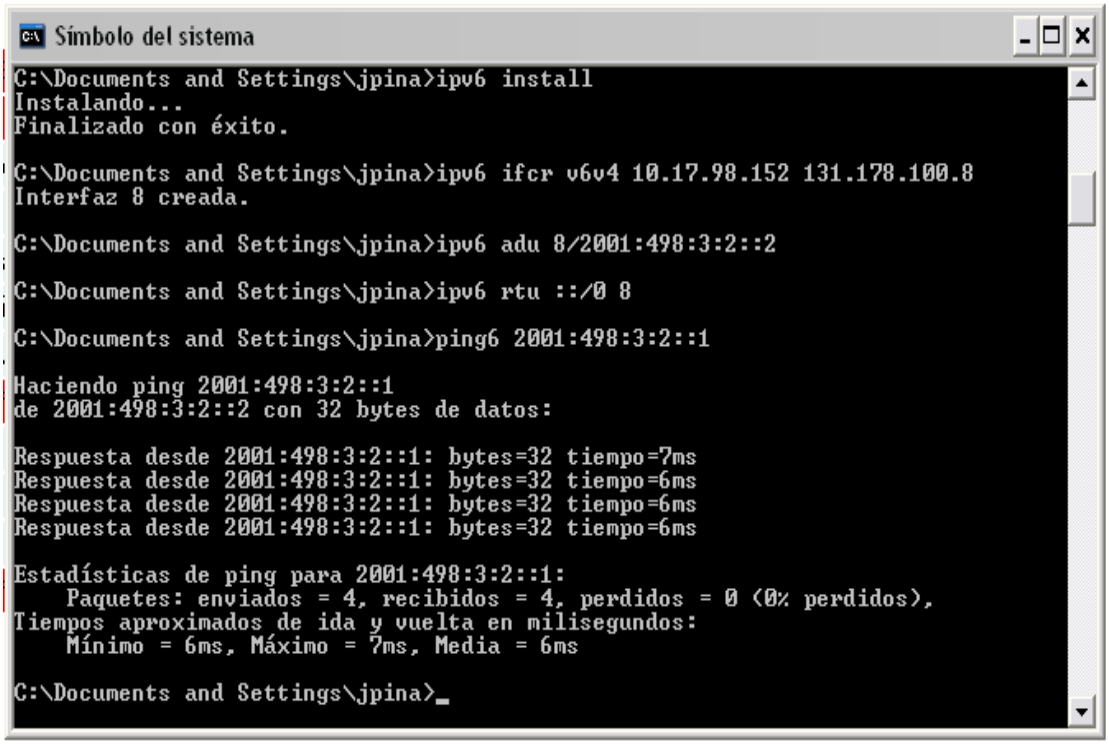


Figura 21 Ping6 al otro extremo del túnel creado.

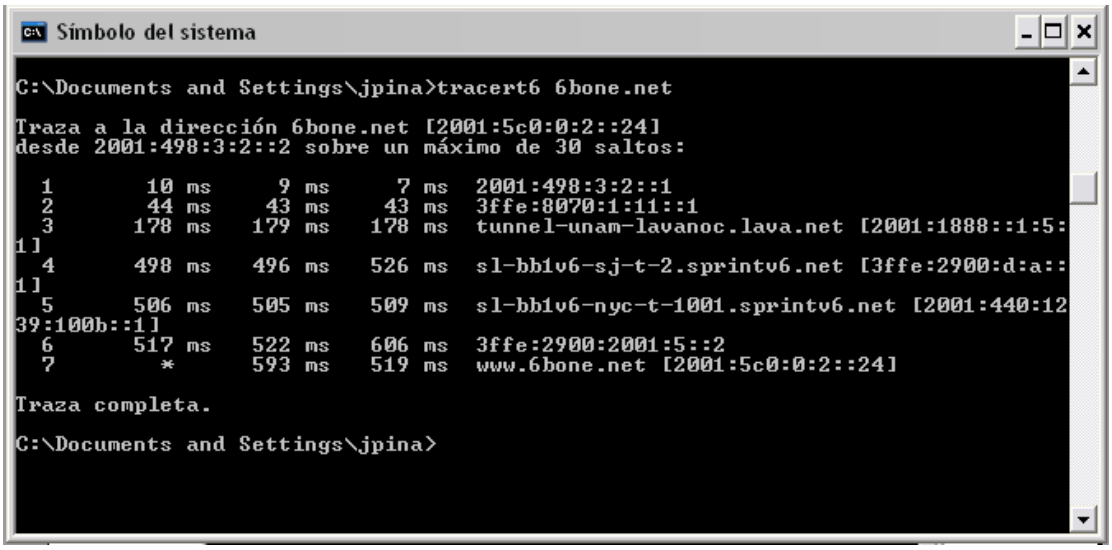


Figura 22 tracert6 a 6bone.net.

Capítulo 2

2 IPV6

2.1 Los motivos de IPv6

El motivo básico por el que surge, en el seno del IETF (Internet Engineering Task Force), la necesidad de crear un nuevo protocolo, que en un primer momento se denominó IPng (Internet Protocol Next Generation, o "Siguiente Generación del Protocolo Internet"), fue la evidencia de la falta de direcciones.

IPv4 tiene un espacio de direcciones de 32 bits. En cambio, IPv6 nos ofrece un espacio de 2^{128} (340.282.366.920.938.463.463.374.607.431.768.211.456)[2].

Sin embargo, IPv4 tiene otros problemas o "dificultades" que IPv6 soluciona o mejora. Los creadores de IPv4, a principio de los años 70, no predijeron en ningún momento, el gran éxito que este protocolo iba a tener en muy poco tiempo, en una gran multitud de campos, no sólo científicos y de educación, sino también en innumerables facetas de la vida cotidiana. Podemos recordar algunas "famosas frases" que nos ayudarán a entender hasta que punto, los propios 'precursores' de la revolución tecnológica que estamos viviendo, no llegaron a prever:

- "Pienso que el mercado mundial de ordenadores puede ser de cinco unidades", Thomas Watson, Presidente de IBM en 1.943.

- "640 Kbps. de memoria han de ser suficientes para cualquier usuario", Bill Gates, Presidente de Microsoft, 1.981.

- "32 bits proporcionan un espacio de direccionamiento suficiente para Internet", Dr. Vinton Cerf, padre de Internet, 1.977.

No es que estuvieran equivocados, sino que las Tecnologías de la Información han evolucionado de un modo mucho más explosivo de lo esperado y debido a la multitud de nuevas aplicaciones en las que IPv4 ha sido utilizado, ha sido necesario crear "añadidos" al protocolo básico. Entre los "parches" más conocidos, podemos citar medidas para permitir la Calidad de Servicio (QoS), Seguridad (IPsec), y Movilidad, fundamentalmente. El inconveniente más importante de estas ampliaciones de IPv4, es que utilizar cualquiera de ellos es muy fácil, pero no tanto cuando pretendemos usar al mismo tiempo dos "añadidos", y no digamos que se convierte en casi imposible o muy poco práctico el uso simultáneo de tres o más, llegando a ser un auténtico malabarismo de circo[4].

2.2 Por que usar IPv6

Como decía en párrafos anteriores, la ventaja fundamental de IPv6 es el espacio de direcciones. El reducido espacio de IPv4, a pesar de disponer de cuatro mil millones de direcciones (4.294.967.296), junto al hecho de una importante falta de coordinación, durante la década de los 80, en la delegación de direcciones, sin ningún tipo de optimización, dejando incluso grandes espacios discontinuos, nos esta llevando a límites no sospechados en aquel momento[2].. Por supuesto, hay una solución que podríamos considerar como evidente, como sería la renumeración, y reasignación de dicho espacio de direccionamiento. Sin embargo, no es tan sencillo, es incluso impensable en algunas redes, ya que requiere unos esfuerzos de coordinación, a escala mundial, absolutamente impensables. Además, uno de los problemas de IPv4 permanecería: la gran dimensión de las tablas de encaminado (routing) en el troncal de Internet, que la hace ineficaz, y perjudica enormemente los tiempos de respuesta. La falta de direcciones no es apreciable por igual en todos los puntos de la red, de hecho, no es casi apreciable, por el momento, en Norte América. Sin embargo, en zonas geográficas como Asia (en Japón la situación esta llegando a ser crítica), y Europa, el problema se agrava. Como ejemplos, podemos citar el caso de China que ha pedido direcciones para conectar 60.000 escuelas, tan sólo ha obtenido una clase B (65.535 direcciones), o el de muchos países Europeos, Asiáticos y Africanos, que solo tienen una clase C (255 direcciones) para todo el país[2]..

Tanto en Japón como en Europa el problema es creciente, dado al importante desarrollo de las redes de telefonía celular, inalámbricas, módems de cable, DSL, etc., que requieren direcciones IP fijas para aprovechar al máximo sus posibilidades e incrementar el número de aplicaciones en las que pueden ser empleados. La razón de utilización de las direcciones IP por parte de los usuarios, esta pasando en pocos meses de 10:1 a 1:1, y la tendencia se invertirá. En pocos meses, podemos ver dispositivos “siempre conectados”, con lo que fácilmente un usuario podría tener, en un futuro no muy lejano, hasta 50 o 100 IP’s (1:50 o 1:100) [2]..

Algunos Proveedores de Servicios Internet se ven incluso obligados a proporcionar a sus clientes direcciones IP privadas, mediante mecanismos de NAT (traslación de direcciones, es decir, usar una sola IP pública para toda una red privada). De hecho, casi todos los PSI’s se ven obligados a delegar tan sólo reducidos números de direcciones IP públicas para sus grandes clientes corporativos. Como ya he apuntado, la solución, temporalmente, es el uso de mecanismos NAT. Desafortunadamente, de seguir con IPv4, esta tendencia no sería “temporal”, sino “invariablemente permanente”. Ello implica la imposibilidad práctica de muchas aplicaciones, que quedan relegadas a su uso en Intranets, dado que muchos protocolos son incapaces de atravesar los dispositivos NAT[2].:

- RTP y RTCP (“Real-time Transport Protocol” y “Real Time Control Protocol”) usan UDP con asignación dinámica de puertos (NAT no soporta esta traslación).

- La autenticación Kerberos necesita la dirección fuente, que es modificada por NAT en la cabecera IP.

- IPsec pierde integridad, debido a que NAT cambia la dirección en la cabecera IP.

- Multicast, aunque es posible, técnicamente, su configuración es tan complicada con NAT, que en la práctica no se emplea.

2.3 Características principales de IPV6

Si resumimos las características fundamentales de IPv6 obtenemos la siguiente relación:

- Mayor espacio de direcciones.
- "Plug & Play": Auto configuración.
- Seguridad intrínseca en el núcleo del protocolo (IPsec).
- Calidad de Servicio (QoS) y Clase de Servicio (CoS).
- Multicast: Envío de UN mismo paquete a un grupo de receptores.
- Anycast: Envío de UN paquete a UN receptor dentro de UN grupo.
- Paquetes IP eficientes y extensibles, sin que haya fragmentación en los encaminadores (routers), alineados a 64 bits (preparados para su procesado óptimo con los nuevos procesadores de 64 bits), y con una cabecera de longitud fija, más simple, que agiliza su procesado por parte del encaminador (router).
- Posibilidad de paquetes con carga útil (datos) de más de 65.535 bytes.
- Encaminado (enrutado) más eficiente en el troncal (backbone) de la red, debido a una jerarquía de direccionamiento basada en la agregación.
- Renumeración y "multi-homing", que facilita el cambio de proveedor de servicios.
- Características de movilidad.

Pero hay que insistir, de nuevo, en que estas son las características básicas, y que la propia estructura del protocolo permite que este crezca, o dicho de otro modo, sea escalado, según las nuevas necesidades y aplicaciones o servicios lo vayan necesitando. Precisamente, la escalabilidad es la baza más importante de IPv6 frente a IPv4 [5].

2.4 Historia IPv6

En Julio de 1.999, del "IPv6 Forum" o Foro IPv6, que ha implicado, en un plazo de tan solo seis meses, un importantísimo crecimiento respecto del fomento, promoción, uso y aplicación del protocolo, con adopciones tan importantes como las realizadas por la OTAN, ETSI, UMTS, 3GPP, o la Comunidad Europea. Por último, en el momento en que estas líneas están siendo escritas, entre el 13 y el 16 de Marzo de 2.000, en Telluride (Colorado – US), una pequeña población, antigua colonia minera fundada por Españoles, convertida ahora en un importante completo turístico dedicado al esquí, mientras se celebraba el 1er Congreso Internacional de IPv6 en Norteamérica (Global IPv6 Summit), organizado por el Foro IPv6, se ha producido un importante acontecimiento, de gran relevancia para IPv6.

La apertura del ciclo de conferencias ha incluido la presentación magistral de Judy Estrin, CTO (Chief Technology Officer) y Vice-Presidente Senior de Cisco Systems, y miembro de las juntas directivas de importantes empresas como Sun Microsystems, Walt Disney y Federal Express. En su cargo es responsable de la planificación de tecnologías estratégicas y desarrollo del negocio, incluyendo inversiones y adquisiciones, ingeniería de consultoría, proyectos avanzados de Internet, así como de asuntos legales y con el gobierno. Fue una de las personas involucradas en los primeros desarrollos del protocolo TCP/IP, desde la Universidad de Stanford[2]..

En su conferencia resaltó frases tan significativas como “Cisco esta comprometido con IPv6, pero estamos comprometidos con la integración, no con la transición”, y urgió a la comunidad IPv6 a proporcionar herramientas y técnicas de gestión que faciliten la integración de IPv6 con IPv4, indicando que “debemos traer IPv6 junto a IPv4, como dos afluentes que convergen para crear un río más poderoso”. Reconoció que Cisco ha percibido un creciente interés en IPv6, lo que les ha obligado, en los últimos seis meses, a tomar alternativas al respecto, con importantes esfuerzos de desarrollo al respecto. Además, citó las siguientes tendencias como conductoras de la necesidad de IPv6:

1. La creciente movilidad de los usuarios de Internet: los usuarios desean poder acceder a los mismos servicios Internet, tanto desde el trabajo, como desde su casa, como desde el coche, lo que crea la necesidad de más de una IP por persona.

2. Redes domésticas: con la venida al hogar de accesos a Internet de gran ancho de banda, y oferta de servicios “siempre conectado”, los consumidores desean conectar a la red dispositivos de seguridad, al igual que otros muchos.

3. La convergencia de voz, vídeo y datos, en infraestructuras basadas en IP: lo que implica el movimiento hacia la arquitectura ofrecida por IPv6, más simple, escalable y más fiable.

Judy Estrin remarcó que la infraestructura actual de IPv4 está extendida, y que el mayor espacio de direcciones de IPv6 ofrece ventajas y eficacias, pero que los métodos de implementación han de asegurar una integración suave, entre IPv4 e IPv6. Según Judy, los desafíos para la implantación de IPv6 no son técnicos, sino de educación de los usuarios finales, y del desarrollo de casos de negocio para la tecnología. No debemos ilusionarnos sólo por una única aplicación definitiva. Pocas horas después, dos relevantes proveedores de la industria de las Tecnologías de la Información, Cisco y Microsoft, han anunciado sus planes inmediatos de soportar “oficialmente” IPv6. Se puede encontrar más información al respecto se hallan en [22][23].

Se trata de los último “gigantes” en confirmar su apoyo incondicional a IPv6, pues previamente, durante un evento similar, celebrado en Diciembre del pasado año, en Berlín, el resto de los fabricantes habían hecho similares anuncios. De hecho, incluso antes de dicho encuentro, todos los fabricantes tenían versiones beta, para algunos de sus productos.

Ericsson Telebit, dispone de productos comerciales con IPv6 desde hace varios años, y diversas plataformas UNIX también ofrecen dicho soporte.

Por otro lado, Sun Microsystems, anunciaba también la disponibilidad actual de la nueva versión de su Sistema Operativo Solaris 8, que YA incluye IPv6, más información en [24].

Además, Nokia y Cernet (red de educación e investigación China), anuncian la implantación mediante encaminadores (routers) de Nokia, de una nueva e importante red, dentro del programa "Internet 6", basada en este protocolo. La noticia completa esta disponible en [25].

Por si no fuera suficiente, NTT Multimedia Communications Laboratories (MCL), subsidiaria de NTT Communications, anuncia la creación del primer nodo neutro de intercambio de tráfico Internet basado en IPv6, en Norteamérica, disponible en el mes de Abril próximo. Información completa disponible en [26].

En Berlín, durante otra de las conferencias del Foro IPv6, NTT hizo un anuncio similar, para el ámbito Europeo, incluso con ofertas de conexión gratuita, a dicho servicio, durante el primer año.

Se trata de un complejo e inesperado cúmulo de noticias al respecto de IPv6 que hacen prever una avalancha de otras nuevas, de similar índole, y que auguran un desarrollo mucho más rápido de los inicialmente previsto para IPv6. Se dispone de un resumen actualizado de las noticias más relevantes respecto de IPv6 en [27] .

2.5 Especificación básicas IPv6 (RFC2460)

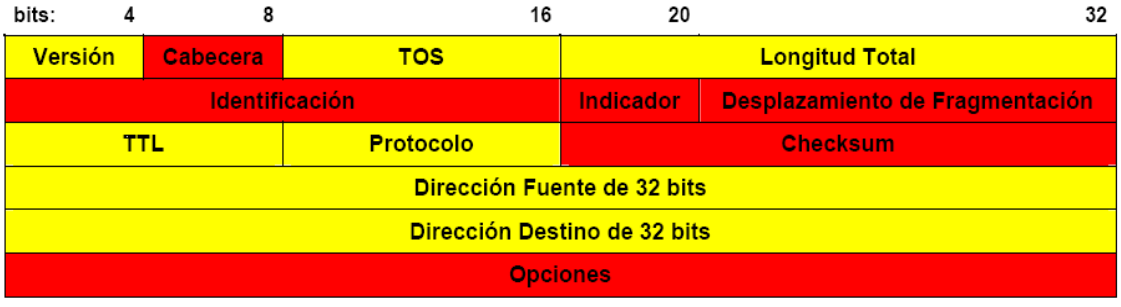


Figura 1 Cabecera de un paquete IPv4(Tomada de [2]).

Como vemos, la longitud mínima de la cabecera IPv4 es de 20 bytes (cada fila de la tabla supone 4 bytes). A ello hay que añadir las opciones, que dependen de cada caso.

En la tabla anterior hemos usado abreviaturas, en aquellos casos en los que son comunes. En el resto, nuestra traducción de la nomenclatura original anglosajona, cuya "leyenda de equivalencias" indicamos a continuación:

- Version – Versión (4 bits)
- Header – Cabecera (4 bits)
- TOS (Type Of Service) – Tipo de Servicio (1 byte)
- Total Length – Longitud Total (2 bytes)
- Identification – Identificación (2 bytes)
- Flag – Indicador (4 bits)
- Fragment Offset – Desplazamiento de Fragmentación (12 bits – 1.5 bytes)
- TTL (Time To Live) – Tiempo de Vida (1 byte)
- Protocol – Protocolo (1 byte)
- Checksum – Código de Verificación (2 bytes)
- 32 bit Source Address – Dirección Fuente de 32 bits (4 bytes)
- 32 bit Destination Address – Dirección Destino de 32 bits (4 bytes)

En la tabla anterior, se han marcado, mediante el color de fondo, los campos que van a desaparecer en IPv6, y los que son modificados, según el siguiente esquema:

Campo Modificado (amarrillo).
Campo que Desaparece(rojo).

Hemos pasado de tener 12 campos, en IPv4, a tan solo 8 en IPv6. El motivo fundamental por el que los campos son eliminados, es la innecesaria redundancia. En IPv4 estamos facilitando la misma información de varias formas. Un caso muy evidente es el checksum o verificación de la integridad de la cabecera: Otros mecanismos de encapsulado ya realizan esta función (IEEE 802 MAC, encapsulado PPP, capa de adaptación ATM, etc.).

El caso del campo de "Desplazamiento de Fragmentación", es ligeramente diferente, dado que el mecanismo por el que se realiza la fragmentación de los paquetes es totalmente modificado en IPv6, lo que implica la total "inutilidad" de este campo. En IPv6 los encaminadores no fragmentan los paquetes, sino que de ser precisa, dicha fragmentación/desfragmentación se produce extremo a extremo.

Algunos de los campos son renombrados:

- Longitud total .-longitud de carga útil (payload length), que en definitiva, es la longitud de los propios datos, y puede ser de hasta 65.536 bytes. Tiene una longitud de 16 bits (2 bytes).

- Protocolo.-siguiente cabecera (next header), dado que en lugar de usar cabeceras de longitud variables se emplean sucesivas cabeceras encadenadas, de ahí que desaparezca el campo de opciones. En muchos casos ni siquiera es procesado por los encaminadores, sino tan sólo extremo a extremo. Tiene una longitud de 8 bits (1 byte).

- Tiempo de vida .- límite de saltos (Hop Limit). Tiene una longitud de 8 bits (1 byte).

Los nuevos campos son:

- Clase de Tráfico (Traffic Class), también denominado Prioridad (Priority), o simplemente Clase (Class). Podría ser más o menos equivalente a TOS en IPv4. Tiene una longitud de 8 bits (1 byte).

- Etiqueta de Flujo (Flow Label), para permitir tráficos con requisitos de tiempo real. Tiene una longitud de 20 bits.

Estos dos campos, como se puede suponer, son los que nos permiten una de las características fundamentales e intrínsecas de IPv6: Calidad de Servicio (QoS), Clase de Servicio (CoS), y en definitiva un poderoso mecanismo de control de flujo, de asignación de prioridades diferenciadas según los tipos de servicios. Por tanto, en el caso de un paquete IPv6, la cabecera tendría el siguiente formato:

Figura 2 Cabecera de un paquete IPv4(Tomada de [2]).

El campo de versión, que es igual a 6, lógicamente, tiene una longitud de 4 bits. La longitud de esta cabecera es de 40 bytes, el doble que en el caso de IPv4, pero con muchas ventajas, al haberse eliminado campos redundantes. Además, como ya hemos mencionado,

la longitud fija de la cabecera, implica una mayor facilidad para su procesado en encaminadores y conmutadores, incluso mediante hardware, lo que implica unas mayores prestaciones.

A este fin ayuda, como hemos indicado anteriormente, el hecho de que los campos están alineados a 64 bits, lo que permite que las nuevas generaciones de procesadores y microcontroladores, de 64 bits, puedan procesar mucho más eficazmente la cabecera IPv6.

El valor del campo "siguiente cabecera", indica cual es la siguiente cabecera y así sucesivamente. Las sucesivas cabeceras, no son examinadas en cada nodo de la ruta, sino sólo en el nodo o nodos destino finales. Hay una única excepción a esta regla: cuando el valor de este campo es cero, lo que indica opción de examinado y proceso "salto a salto" (hop-by-hop). Así tenemos, por citar algunos ejemplos, cabeceras con información de encaminado, fragmentación, opciones de destino, autenticación, encriptación, etc, que en cualquier caso, han de ser procesadas en el orden riguroso en que aparecen en el paquete.

Sin entrar en más detalles, véase a continuación los siguientes ejemplos gráficos del uso del concepto de las "cabeceras de extensión" (definidas por el campo "siguiente cabecera"), mecanismo por el que cada cabecera es "encadenada" a la siguiente y anterior (si existen):

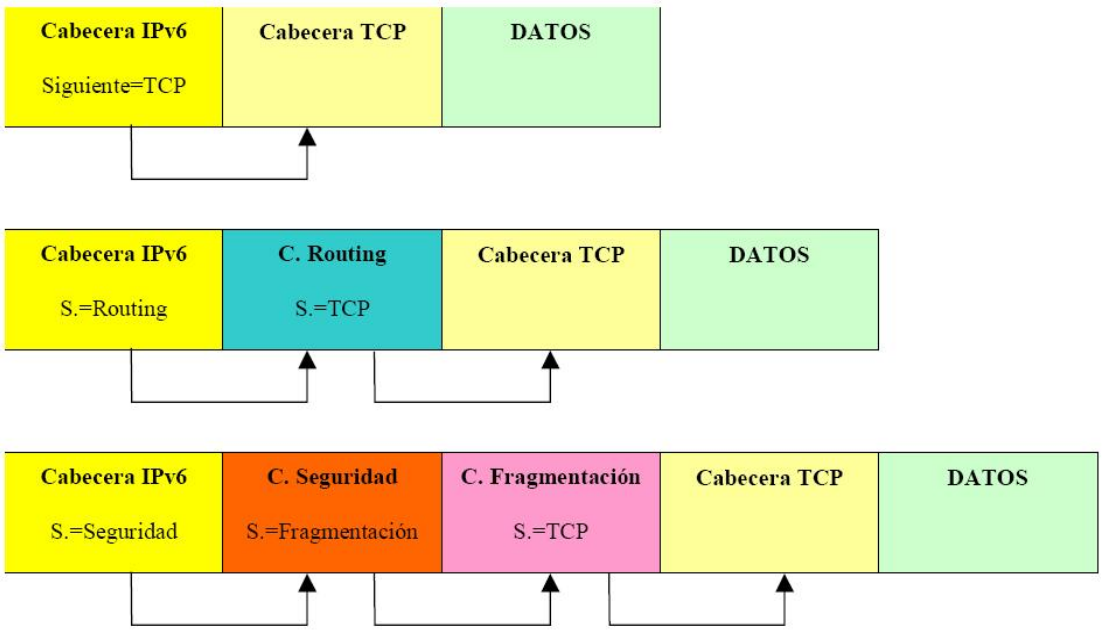


Figura 3 Cabeceras de extensión(Tomada de [2]).

El MTU (Unidad Máxima de Transmisión), debe de ser como mínimo, de 1.280 bytes, aunque se recomiendan tamaños superiores a 1.500 bytes. Los nodos descubren el valor MTU a través de la inspección de la ruta. Se prevé así una optimización de los paquetes y del número de cabeceras, dado el continuo crecimiento de los anchos de banda disponibles, así como del incremento del propio tráfico mas información en [29].

2.6 Direcciones y direccionamiento en (RFC2373)

Las direcciones IPv6 son identificadores de 128 bits para interfaces y conjuntos de interfaces. Dichas direcciones se clasifican en tres tipos:

- Unicast: Identificador para una única interfaz. Un paquete enviado a una dirección unicast es entregado sólo a la interfaz identificada con dicha dirección. Es el equivalente a las direcciones IPv4 actuales.

- Anycast: Identificador para un conjunto de interfaces (típicamente pertenecen a diferentes nodos). Un paquete enviado a una dirección anycast es entregado en una (cualquiera) de las interfaces identificadas con dicha dirección (la más próxima, de acuerdo a las medidas de distancia del protocolo de encaminado). Nos permite crear, por ejemplo, ámbitos de redundancia, de forma que varias máquinas puedan ocuparse del mismo tráfico según una secuencia determinada, si la primera “cae” (deja de funcionar) .

- Multicast: Identificador para un conjunto de interfaces (por lo general pertenecientes a diferentes nodos). Un paquete enviado a una dirección multicast es entregado a todas las interfaces identificadas por dicha dirección. La misión de este tipo de paquetes es evidente: aplicaciones de retransmisión múltiple (broadcast).

2.6.1 Diferencias con IPv4

Hay algunas diferencias importantes en el direccionamiento de IPv6 respecto de IPv4:

- No hay direcciones broadcast (su función es sustituida por direcciones multicast).
- Los campos de las direcciones reciben nombres específicos; denominamos “prefijo” a la parte de la dirección hasta el nombre indicado (incluyéndolo).
- Dicho prefijo nos permite conocer donde esta conectada una determinada dirección, es decir, su ruta de encaminado.
- Cualquier campo puede contener sólo ceros o sólo unos, salvo que explícitamente se indique lo contrario.
- Las direcciones IPv6, indistintamente de su tipo (unicast, anycast o multicast), son asignadas a interfaces, no nodos. Dado que cada interfaz pertenece a un único nodo,

cualquiera de las direcciones unicast de las interfaces del nodo puede ser empleado para referirse a dicho nodo.

- Todas las interfaces han de tener, al menos, una dirección unicast link-local (enlace local).
- Una única interfaz puede tener también varias direcciones IPv6 de cualquier tipo (unicast, anycast o multicast) o ámbito.
- Una misma dirección o conjunto de direcciones unicast pueden ser asignados a múltiples interfaces físicas, siempre que la implementación trate dichas interfaces, desde el punto de vista de internet, como una única, lo que permite balanceo de carga entre múltiples dispositivos.
- Al igual que en IPv4, se asocia un prefijo de subred con un enlace, y se pueden asociar múltiples prefijos de subred a un mismo enlace.

2.6.2 Direcciones especiales en IPv6

Se han definido también las direcciones para usos especiales como[2]:

- Dirección de auto-retorno o Loopback (::1) – No ha de ser asignada a una interfaz física; se trata de una interfaz "virtual", pues se trata de paquetes que no salen de la máquina que los emite; nos permite hacer un bucle para verificar la correcta inicialización del protocolo (dentro de una determinada máquina).

- Dirección no especificada (::) – Nunca debe ser asignada a ningún nodo, ya que se emplea para indicar la ausencia de dirección; por ejemplo, cuando se halla en el campo de dirección fuente, indica que se trata de un host que esta iniciándose, antes de que haya aprendido su propia dirección.

- Túneles dinámicos/automáticos de IPv6 sobre IPv4 (::<dirección IPv4>) – Se denominan direcciones IPv6 compatibles con IPv4, y permiten la retransmisión de tráfico IPv6 sobre infraestructuras IPv4, de forma transparente.

80 bits	16 bits	32 bits
0000 ... 0000	0000	dirección IPv4

- Representación automática de direcciones IPv4 sobre IPv6 (::FFFF:<dirección IPv4>) – permite que los nodos que sólo soportan IPv4, puedan seguir trabajando en redes IPv6. Se denominan "direcciones IPv6 mapeadas desde IPv4".

80 bits	16 bits	32 bits
0000 ... 0000	HF	dirección IPv4

2.6.3 Representación de las direcciones IPv6

La representación de las direcciones IPv6 sigue el siguiente esquema mas información [11]:

a) x:x:x:x:x:x:x:x, donde "x" es un valor hexadecimal de 16 bits, de la porción correspondiente a la dirección IPv6. No es preciso escribir los ceros a la izquierda de cada campo. Ejemplos:
FEDC:BA98:7654:3210:FEDC:BA98:7654:3210

1080:0:0:0:8:800:200C:417A

b) Dado que, por el direccionamiento que se ha definido, podrán existir largas cadenas de bits "cero", se permite la escritura de su abreviación, mediante el uso de "::", que representa múltiples grupos consecutivos de 16 bits "cero". Este símbolo sólo puede aparecer una vez en la dirección IPv6. Ejemplos:

Las direcciones:

1080:0:0:0:8:800:200C:417A (una dirección unicast)
FF01:0:0:0:0:0:0:101 (una dirección multicast)
0:0:0:0:0:0:0:1 (la dirección loopback)
0:0:0:0:0:0:0:0 (una dirección no especificada)

Pueden representarse como:

1080::8:800:200C:417A (una dirección unicast)
FF01::101 (una dirección multicast)
::1 (la dirección loopback)
:: (una dirección no especificada)

c) Una forma alternativa y muy conveniente, cuando nos hallemos en un entorno mixto IPv4 e IPv6, es x:x:x:x:x:x:d:d:d:d, donde "x" representa valores hexadecimales de 16 bits (6 porciones de mayor peso), y "d" representa valores decimales de las 4 porciones de 8 bits de menor peso (representación estándar IPv4). Ejemplos:

0:0:0:0:0:0:13.1.68.3
0:0:0:0:0:FFFF:129.144.52.38

Pueden representarse como:

::13.1.68.3
::FFFF:129.144.52.38

La representación de los prefijos IPv6 se realiza del siguiente modo dirección-IPv6/longitud-del-prefijo donde:

- Dirección-IPv6 = una dirección IPv6 en cualquiera de las notaciones válidas
- Longitud-del-prefijo = valor decimal indicando cuantos bits contiguos de la parte izquierda de la dirección componen el prefijo

Por ejemplo, las representaciones válidas del prefijo de 60 bits

12AB00000000CD3, son:
12AB:0000:0000:CD30:0000:0000:0000:0000/60
12AB::CD30:0:0:0:0/60
12AB:0:0:CD30::/60

Por tanto, para escribir una dirección completa, indicando la subred, podríamos hacerlo como:

12AB:0:0:CD30:123:4567:89AB:CDEF/60

2.7 Formato para representación en URL's (RFC2732)

Cuando navegamos, continuamente aludimos a URL(Localizador de Recurso Uniforme*)*, en muchas ocasiones sin conocer el significado precios de esta abreviatura.

La especificación original (RFC2396), que data del año 1.988, nos dice que URL (Localizador de Recurso Uniforme), es un medio simple y extensible para identificar un recurso a través de su localización en la red. Una vez aclarado esto, y de la misma forma que en ocasiones usamos direcciones en formato IPv4 para escribir un URL, se han descrito unas normas para realizar la representación literal de direcciones IPv6 cuando se usan herramientas de navegación WWW.

El motivo por el que ha sido preciso realizar esta definición es bien simple. Con la anterior especificación no estaba permitido emplear el carácter ":" en una dirección, sino como separador de "puerto". Por tanto, si se desea facilitar operaciones tipo "cortar y pegar" (cut and paste), para trasladar direcciones entre diferentes aplicaciones, de forma rápida, era preciso buscar una solución que evitase la edición manual de las direcciones IPv6.

La solución es bien sencilla: el empleo de los corchetes ("[","]") para encerrar la dirección IPv6, dentro de la estructura habitual del URL.
Veamos algunos ejemplos; las direcciones siguientes:

• FEDC:BA98:7654:3210:FEDC:BA98:7654:3210

- 1080:0:0:0:8:800:200C:4171
- 3ffe:2a00:100:7031::1
- 1080::8:800:200C:417A
- ::192.9.5.5
- ::FFFF:129.144.52.38
- 2010:836B:4179::836B:4179

Serían representadas como:

- http://[FEDC:BA98:7654:3210:FEDC:BA98:7654:3210]:80/index.html
- http://[1080:0:0:0:8:800:200C:417A]/index.html
- http://[3ffe:2a00:100:7031::1]
- http://[1080::8:800:200C:417A]/foo
- http://[::192.9.5.5]/ipng
- http://[::FFFF:129.144.52.38]:80/index.html
- http://[2010:836B:4179::836B:4179]

2.8 IPsec

Una de las grandes ventajas de IPv6 es, sin duda, la total integración de los mecanismos de seguridad, autenticación y confidencialidad (encriptación), dentro del núcleo del protocolo.

Se trata por tanto de algo obligatorio, y no adicional ni "añadido" como en IPv4. Para ello, la siguiente cabecera puede tener valores AH (autenticación – "Authentication Header") y ESP (encriptación – "Encapsulation Security Payload"), que permiten, básicamente, emplear las mismas extensiones de protocolo empleadas en IPv4, y que de hecho, al haber sido desarrolladas con posterioridad al inicio de los trabajos de IPv6, ya lo contemplan.

Dado que los mecanismos asociados ya han sido descritos, simplemente citamos las normas básicas que son aplicables: RFC2401 al RFC2412 y RFC2451.

2.9 Túneles IPv6 sobre IPv4

Los túneles proporcionan un mecanismo para utilizar las infraestructuras IPv4 mientras la red IPv6 esta siendo implantada.

Este mecanismo consiste en enviar datagramas IPv6 encapsulados en paquetes IPv4. Los extremos finales del túnel siempre son los responsables de realizar la operación de encapsulado del paquete/es IPv6 en IPv4 [30].

Estos túneles pueden ser utilizados de formas diferentes[30]:

- Encaminador a encaminador. Encaminador con doble pila (IPv6/IPv4) se conectan mediante una infraestructura IPv4 y transmiten tráfico IPv6. El túnel comprende un segmento que incluye la ruta completa, extremo a extremo, que siguen los paquetes IPv6.

- Anfitrión a Encaminador. Anfitrión con doble pila se conectan a un encaminador intermedio (también con doble pila), alcanzable mediante una infraestructura IPv4. El túnel comprende el primer segmento de la ruta seguida por los paquetes.

- Anfitrión a anfitrión. Anfitrión con doble pila interconectados por una infraestructura IPv4. El túnel comprende la ruta completa que siguen los paquetes.

- Encaminador a anfitrión. Encaminador con doble pila que se conectan a anfitrión también con doble pila. El túnel comprende el último segmento de la ruta.

Los túneles se clasifican según el mecanismo por el que el nodo que realiza el encapsulado determina la dirección del nodo extremo del túnel.

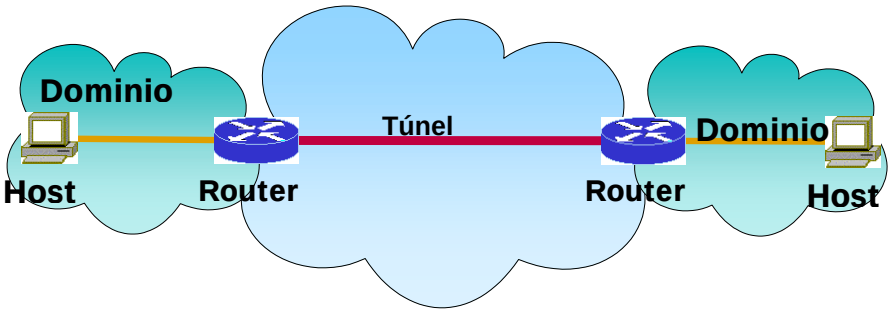


Figura 4 Túnel Encaminador a Encaminador.

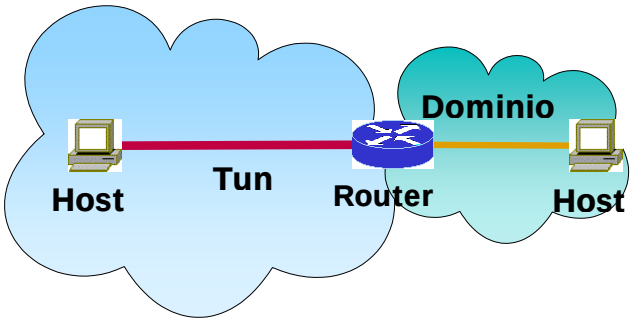


Figura 5 Túnel Anfitrión a Encaminador.

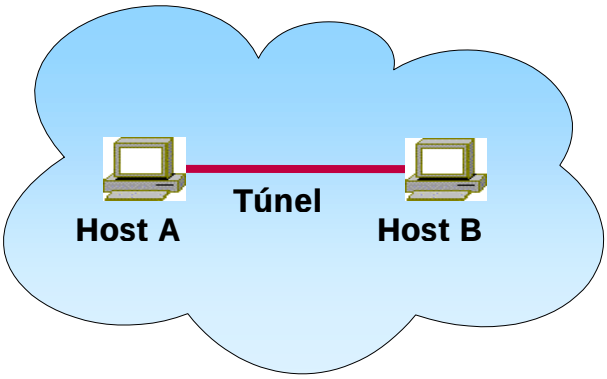


Figura 6 Túnel Anfitrión. a Anfitrión.

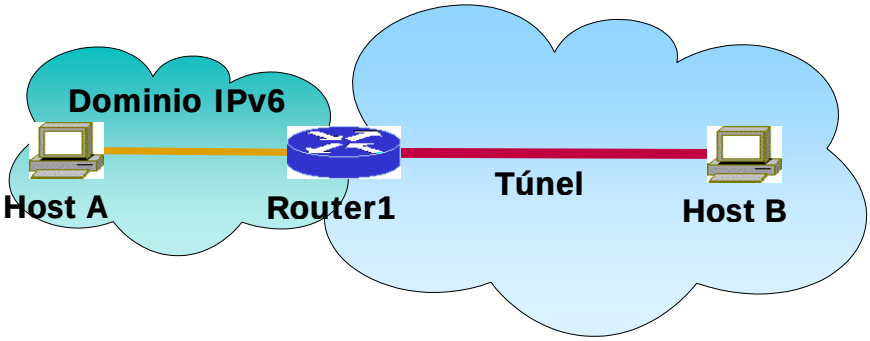


Figura 7 Túnel Encaminador a Anfitrión.

En los dos primeros casos (encaminador a encaminador y anfitrión a encaminador), el paquete IPv6 es tunelizado a un encaminador. El extremo final de este tipo de túnel, es un encaminador intermedio que debe desencapsular el paquete IPv6 y reenviarlo a su destino final. En este caso, el extremo final del túnel es distinto del destino del destino final del paquete, por lo que la dirección en el paquete IPv6 no proporciona la dirección IPv4 del extremo final del túnel. La dirección del extremo final del túnel ha de ser determinada a través de información de configuración en el nodo que realiza el túnel. Es lo que se

denomina “túnel configurado”, describiendo aquel tipo de túnel donde el extremo final del túnel es explícitamente configurado.

En los otros dos casos (Anfitrión a Anfitrión y encaminador a Anfitrión), el paquete IPv6 es tunelizado, durante todo el recorrido, a su nodo destino. El extremo final del túnel es el nodo destino del paquete, y por tanto, la dirección IPv4 está contenida en la dirección IPv6. Este caso se denomina “túnel automático”.

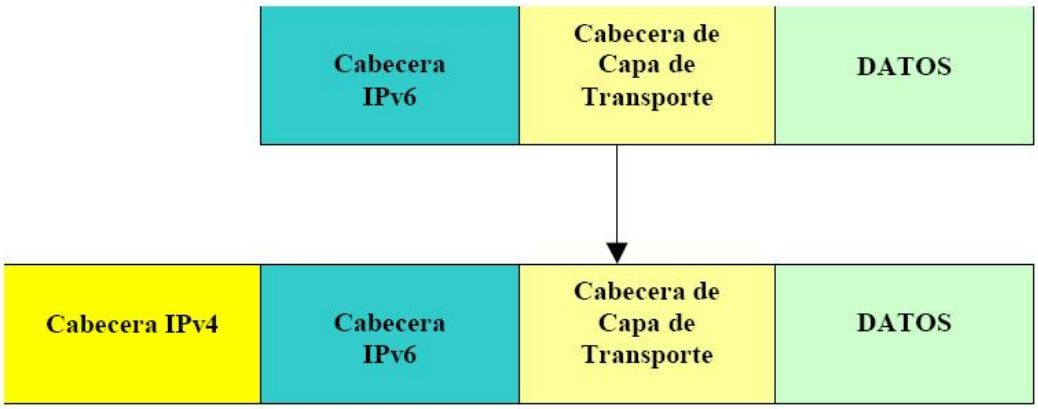


Figura 8 El Desencapsulado(Tomada de [2]).

2.10 IPv6 en el ITESM

Ahora si teniendo una perspectiva y un perfil de lo que es IPv6, su evolución y clara ventaja sobre su predecesor podemos ver la importancia que tiene incorporarse rápidamente a esta nueva tecnología. El Tec de Monterrey ya contaba con cierta infraestructura y algunas conexiones de este tipo, sin embargo actualmente se encuentran inoperantes. Por lo que es necesario una revisión general, desde configuración de enrutadores, conexiones, túneles, servidores y demás que incorporen o puedan incorporar esta tecnología compatiblemente con IPv4.

En partícula en la primera parte del proyecto, hablamos de una revisión general de lo que existe y de lo que es necesario para nuestro fin. Investigar, Implementar y Desarrollar IPv6 en el Campus Monterrey del ITESM.

2.10.1 ALGUNOS DE LOS PASOS A SEGUIR .

Algunos de los pasos a seguir para la documentación de Ipv6 en el ITESM son los siguientes.

1.- Documentación e Investigación de IPv6, estándares y normas en contraste con IPv4
2.- Documentación y Familiarización con el equipo disponible (Enrutadores, Servidores, Conexiones, etc).
3.- Implementación y Configuración de un servidor IPv6 en conjunto con un enrutador IPv6

Continuación se muestra el diagrama físico y lógico de la red Ipv6 en el ITESM.

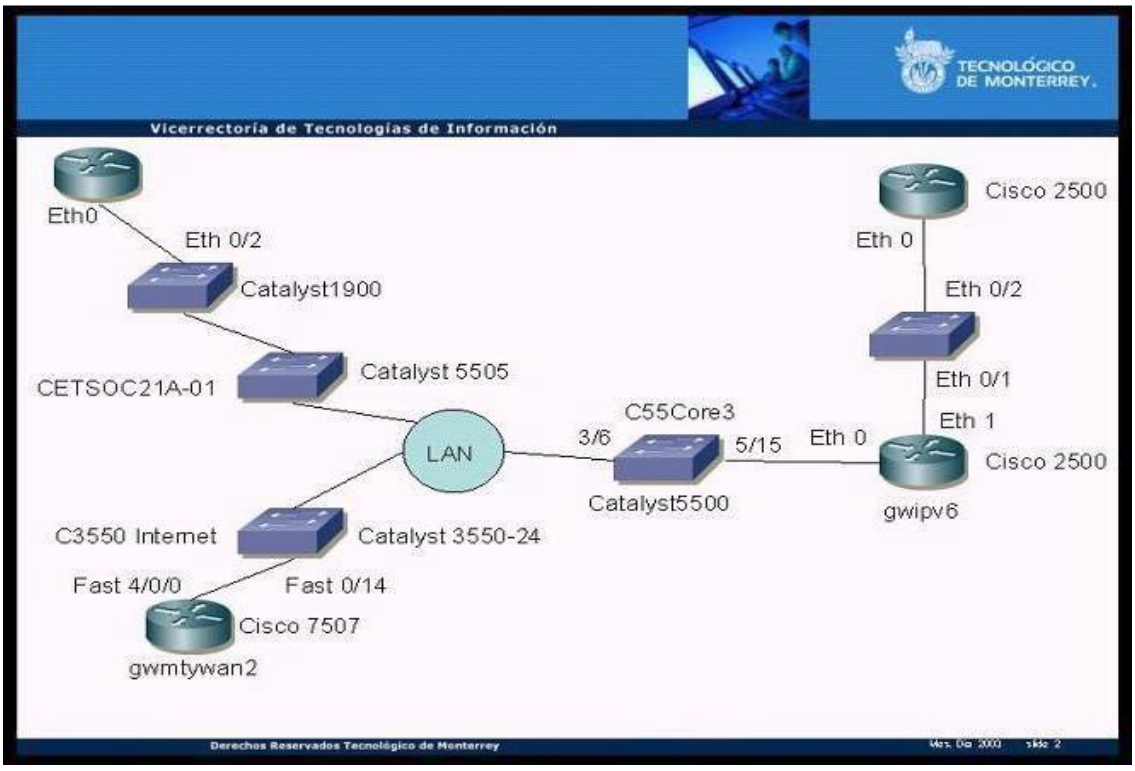


Figura 9 Diagrama Físico.

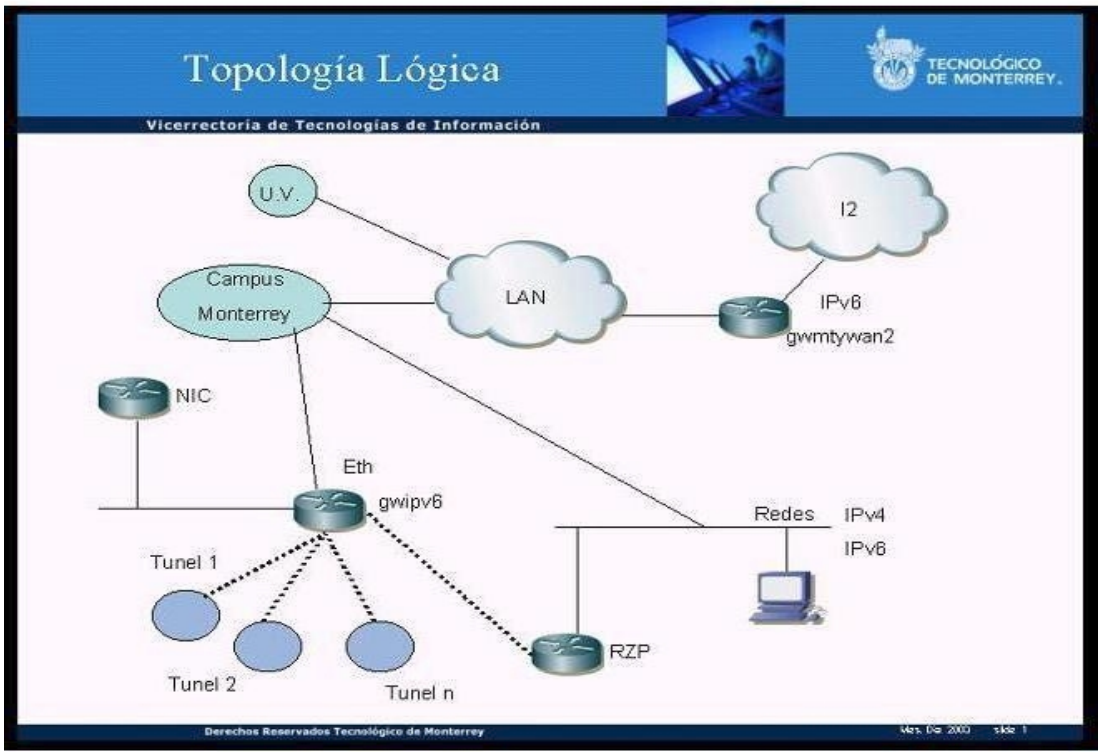


Figura 10 Diagrama Lógico.

	A	B	C	D	E	F	G
1	IPv6 Address	Never Active Tunnel		Propietario	Lugar	Encargado	Correo Electronico
2							
3	2001:498:1::2			ITESM	MX		
4	3FFE:200:1:50::1	600		SICS	SE	Lars Albertsson, Mikael Nehlsen	lalle@sics.se, jogride@sics.se
5	3FFE:1CF1:3::B	900		MERIT	EU	Larry J. Blunk	ljb@merit.edu
6	3FFE:81F1:1:2002:1000::3A	2000		CYBERNET (Returned)	DE		
7	3FFE:81F1:1:2005::1	700		CYBERNET (Returned)	DE		
8	3FFE:8240:8010::1	800		ITESM	MX		
9	3FFE:8270:0:1::20	1200		CALADAN	BR	Chris Smith	chris@caladan.net
10							
11		Never Idle Tunnel					
12							
13	3FFE:8240:800A::2	1100		ITESM	MX		
14	3FFE:8240:800F::2	2200		ITESM	MX		
15							
16		Active Tunnel					
17							
18	3FFE:C00:8023:25::1	300		CISCO	EU	Ole Troan	ot@cisco.com, 6bone-support@cisco.com
19	3FFE:8070:1:11::1	205		UNAM	MX	Azael Fernandez	azael@ipv6.unam.mx, staff_ipv6@ipv6.unam.mx
20	3FFE:8160:0:1::20	1900		LAVANET	EU		system@lava.net
21	3FFE:8240:7013:2::2			ITESM	MX		
22	3FFE:8240:800D::2	700		ITESM	MX		
23	3FFE:8240:8012::1	1300		ITESM	MX		
24	3FFE:8240:8016:6::2	1500		ITESM	MX		
25	3FFE:8240:8018::2	2100		ITESM	MX		
26	3FFE:8240:8026::2	2500		ITESM	MX		

Figura 11 Túneles activos e inactivos.

Capítulo 7

7 RESULTADO DE ENCUESTAS

7.1 Encuesta Administradores de red.

La universidades encuestadas fueron aquellas que ya cuentan con IPv6 y conexión al 6bone por petición de las universidades no será revelado el nombre.

Tipos de Túneles

- A mediante alguna interfaz gráfica usada por el usuario final.
- B mediante una petición y creada por administradores de red.

Caso 1. Tipo de túneles (Donde Si es 100% y No en 0% , escala en porcentaje).

Esta gráfica muestra una comparación de túneles con que cuentan las universidades entrevistadas.

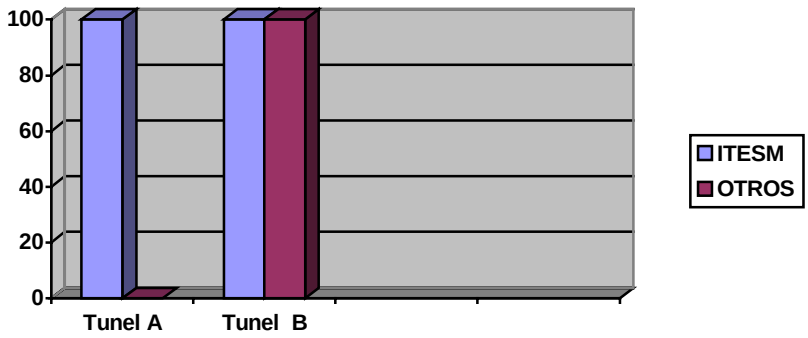


Tabla 1. Caso 1

Caso 2. Soporte a creación de túneles (Donde Si es 100% y No en 0% , escala en porcentaje).

Esta gráfica muestra una comparación de gente que puede dar soporte a la creación de túneles ya sean tipo A o B.

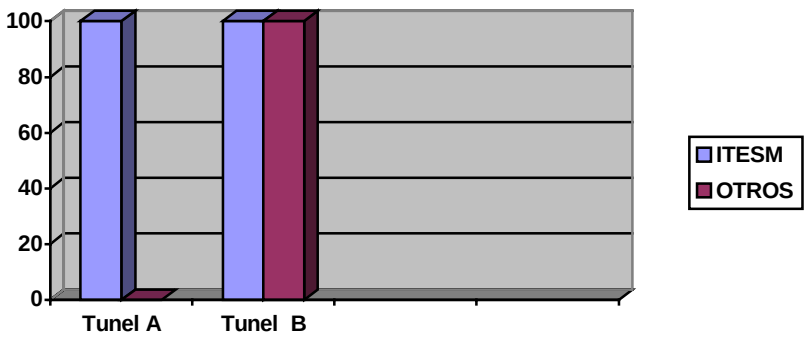


Tabla 2. Caso2

Caso3. Borrado de túneles (Donde Si es 100% y No en 0% , escala en porcentaje).

La siguiente gráfica muestra si se puede borrar túneles automáticamente por medio de un interfaz web.

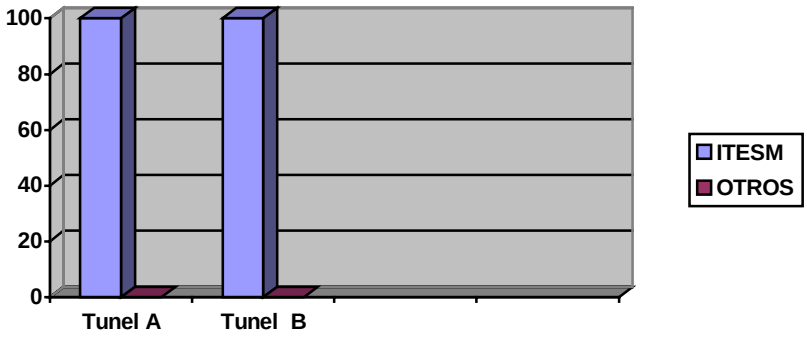


Tabla 3. Caso3

Caso 4 Procedimientos para túneles (Donde Si es 100% y No en 0% , escala en porcentaje).

Gráfica que muestra si tienen un procedimiento para poder hacer túneles con otra universidad y para hacer pruebas.

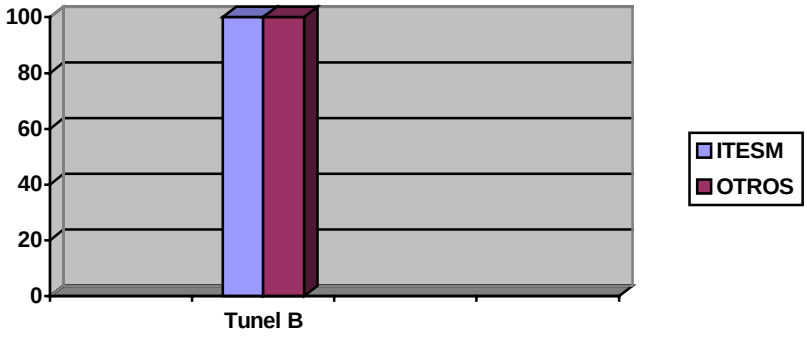


Tabla 4. Caso4

Caso 5. Servicios ofrecidos para ipv6 (escala medida en porcentaje).

La gráfica muestra un porcentaje de las universidades que fueron entrevistadas sobre los servicios que ofrecen para IPv6.

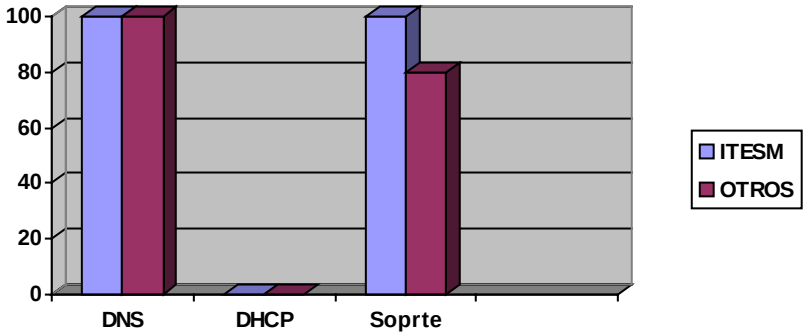


Tabla 5. Caso5

7.2 Encuesta para usuarios finales.

Caso 6 facilidad de uso (escala medida en porcentaje).

Esta gráfica muestra la facilidad de uso de la interfaz grafica para crear y borrar el túnel automáticamente, esta encuesta se le aplicó a los usuarios finales.

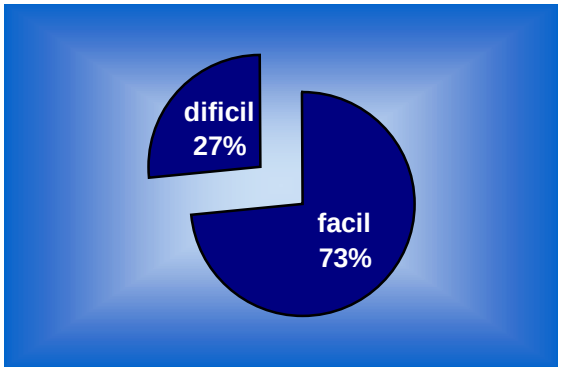


Tabla 6. Caso6

Capítulo 8

8 CONCLUSIONES Y TRABAJO FUTURO

En este capítulo se resumen los resultados obtenidos de la propuesta presentada y presenta una síntesis del trabajo realizado, las lecciones aprendidas y las aportaciones.

8.1 Conclusiones

La migración al nuevo protocolo en las redes actuales es un trabajo no exento de riesgos y costes. Algunos estarán ocultos hasta el momento de llevar a cabo la puesta en escena, pero la planificación y la discusión son las únicas herramientas que nos pueden ayudar a conseguir una migración lo más suave posible. Los riesgos están relacionados con la posible pérdida de eficiencia en las redes en las que se implante IPv6 en los períodos de transición, los costes dependerán de la densidad de cambios, la velocidad del despliegue y el esfuerzo (tanto económico como humano) que vayamos a dedicar a la tarea de migración.

Es más, hemos de ser conscientes que la migración a nivel de red y de servicios sólo será una parte de la migración a IPv6, puesto que si queremos aprovechar las nuevas características del protocolo, habremos de emplear nuevos esfuerzos en extender la red con aplicaciones que soporten calidad de servicio, sistemas preparados para la gestión de claves de seguridad y encaminadores capaces de proveer entornos de movilidad a los usuarios, entre otras cosas.

También es importante remarcar que el éxito de la migración dependerá, además, en gran medida de la disponibilidad de software adecuado a la nueva tecnología, que no sólo permita estar a la altura del servicio proporcionado por la tecnología basada en IPv4, sino que nos permita sacar partido de sus características positivas y que nos permita obviar, en mayor o menor medida, sus posibles desventajas.

Un factor que no hay que olvidar es el estado de la Transición, es muy importante preguntarnos ¿Dónde estamos actualmente? Ya que, existen cerca de 20 mecanismos de transición definidos actualmente definidos actualmente en redes experimentales y proyectos de investigación 6BONE, LONG, ARMSTRONG, etc. Sin embargo, no existen recomendaciones claras para aquellos que deseen comenzar la transición (ISPs, redes corporativas o de campus, redes domésticas, etc). Los grupos ngtrans y v6ops trabajan actualmente en su definición.

8.2 Primera fase

Se observó que es muy importante estudiar las características de cada entorno para escoger los mecanismos de transición, en este caso se usará la red de doble pila de protocolo mencionada en el capítulo 3.

En esta fase demostró que lo más adecuado fueron los túneles usados por la aplicación mencionada en el capítulo 6 por su sencillez en su forma de uso y simplicidad en la administración de los túneles, la cual tiene las siguientes ventajas y desventajas :

Ventajas de este sistema

- Método muy utilizado en el acceso al 6-bone.
- Disponible en multitud de plataformas (Cisco, Telebit, Linux, Solares, Windows NT, etc).
- Es un método totalmente transparente respecto al nivel IPv6 y superiores, con lo cual no afecta a las aplicaciones.
- No consume excesivos recursos, la MTU se reduce en 20 bytes.
- Aplicación Principal: Conexión con ISP IPv6 remoto a través de Internet.

Desventajas

- No son dinámicos, si no que se establecen manualmente o de forma semiautomática.
- Si se unen N islas y la topología no considera un nodo central o intercambiador, el número de túneles a establecer en sitios ascienden a N-1. En el caso de pensar que la conexión entre sí de miles de islas de IPv6 distribuidas por la Internet actual, este método carece de sentido.

Para esta fase se recomienda que el numero de usuarios que sean migrados a IPv6 no se exceda a los 10,000 ya que puede ocasionar que el encaminado se sobrecargué y degrade el servicio y la administración de los túneles se vuela muy compleja.

Las posibles soluciones para esto serían.

- Comprar un encaminador más potente.
- Comprar una maquina servidor con el servicio de zebra el cual es un software que actúa como emcaminador así pasar un poco de la carga a este servidor y agregar unos cuantos aspectos de seguridad.

8.3 Segunda fase

La segunda fase no se pudo concluir por falta de tiempo, pero estos son los pasos a seguir para efectuar dicha fase.

- Terminar de migrar la nueva red proporcionada por LANIC.
- Cambiar a Red de paralela de Ipv6 e Ipv4 mencionada en el capítulo 3.
- Pasar la Red a configuración Stateful (DHCP6).
- Documentar y crear Multi-homing para que los demás campus puedan salir por I2.
- Comprar un router más potente ya que el actual es un 2500 series cisco.
- Reutilizar el equipo ya existente para la nueva red.
- Crear políticas de acceso ya que con la implementación del protocolo desaparecerá NAT de la red.
- Determinar ventanas de tiempo entre migraciones de campus hacia la VPN.
- Crear Vlans para IPv6.
- Capacitar a los personales de redes de los diferentes campus.

8.4 Barreras para IPv6 en el ITESM

- El problema del multi-homing.
- Los “fans” del direccionamiento ajustable en longitud.
- El propio IPv4, de alguna forma, con los “parches” como NAT.
- La falta de soporte real por parte de fabricantes de routers y software “dominantes”.
- La complejidad de la migración/transición.
- Los usuarios necesitan razones comerciales “FORZADAS” para moverse a IPv6.

8.5 Cuándo se debe migrar a IPv6

Muchos de nosotros ya hemos empezado, de alguna manera, probablemente a través de túneles como en nuestro caso, pero necesitamos forzar la creación de plataformas de prueba, y usar IPv6 a través de Internet con otros usuarios IPv6. Las compañías comerciales, en la mayoría de las ocasiones, esperarán hasta que la normalización sea completa y clara, y puedan evaluar adecuadamente los costes, etc. Pero para redes sin ánimo de lucro, como investigación, educación, deben migrar gradualmente ahora, logrando experiencia y compartiéndola con otros. Después de todo, las redes siempre son las primeras en comenzar trabajando con todo, como así fue con Internet, por lo consecuente podemos concluir con.

IPv6 es el futuro, La pregunta NO es si va sustituir a ipv4 o no, sino cuando ?

8.6 Trabajos futuros

Conforme se mueven las actividades de implementación de IPv6, se propone una evaluación que sirva para identificar los servicios básicos para el funcionamiento de ambientes operativos en redes IPv6. Aplicaciones de correo, servicio web y servidores de nombres por ejemplo, pueden estar incluidos en estas actividades. Este último, el servicio de nombres de dominio (DNS), es considerado por muchos, una tarea de coexistencia primaria el cual ya existe ya que fue necesario para la primera fase.

Con referencia a los servicios, se cree conveniente instalar aplicaciones IPv6 determinadas en servidores físicamente distintos a aquellos que proveen el mismo servicio para IPv4. En su defecto, ampliar el nivel de procesamiento y almacenamiento en lo necesario. Se piensa esto, ya que mantener aplicaciones operando simultáneamente sobre el mismo espacio físico, pudiese desmejorar el desempeño de ambas aplicaciones terminando en el perjuicio de servicios prestados a los usuarios. No obstante, este escenario no será el caso de partida, ya que se predice exista poca sintonía con IPv6.

8.6.1 Túneles al 6bone

Una de las tareas futuras es volver a activar todos los túneles con el 6bone los cuales se muestran en las siguientes tablas.

Tun	Route	LastInp	Packets Description
0	00:00:01	47730	Tunel gwmtywan2
101	00:00:07	1148978	6to4
205	00:00:03	726334	BGP+4 -> UNAM_IPV6-1
300	00:00:05	98971	BGP+4 -> Cisco
600	00:00:27	201618	BGP4+ -> SICS
1500	00:00:24	154693	csxxi
1900	00:00:08	47739	LavaNets
2100	1d21h	64348	INICTEL, Peru
2500	00:00:26	62830	RETINA,AR AS3597
2600	00:00:09	459205	Nitcom, Peru
2800	00:00:02	151830	UAdCoahuila
1100	2w5d	151	IPV6 DNS

Tabla 7. Túneles activos al 6bone.

700	Never	0	BGP4+ ->UACH
800	Never	0	BGP4+ -> coruniversitec
900	Never	0	iBGP+4 --> NIC
1000	Never	0	ULSA static
1200	Never	0	Caladan bgp4+
201	Never	0	static -> Freenet6.net
1300	Never	0	udg bgp4+
1400	Never	0	oaxaca
1600	Never	0	XS4ALL
1700	Never	0	FASTNETXP --> changed to NDSOFTWARE
1800	Never	0	Doris
2000	Never	0	TELEPONT AS65272
2200	Never	0	ATT Test QoS
2300	Never	0	VHS POLAND PZK2-6BONE Static
2400	Never	0	UNIX-6BONE Slovenia
2700	Never	0	gwipv6-2

Tabla 8. Túneles inactivos al 6bone.

8.6.2 El futuro de computo móvil

Ipv6 también migra al computo móvil haciéndonos ver que el futuro ya está aquí y el futuro no es futuro sino presente. Esto habla de velocidad, frenetismo por estar siempre en el aquí y ahora.Todo esto, quizá, en un nivel conceptual. En un nivel práctico, IPv6 habla de movilidad. La funcionalidad más nombrada con respecto a este nuevo protocolo es mayor espacio para direcciones. Millones de nuevos usuarios en países como China e India, y nuevos dispositivos como PDAs, teléfonos móviles habilitados para Internet, automóviles conectados a Internet, se están añadiendo a la rama de direcciones. Otra función clave es que ofrece una arquitectura más modelada para IP móvil. Este es un protocolo y una arquitectura de red que permite que un dispositivo funcione en una red convergente de voz y datos como lo hace un teléfono celular. La arquitectura de red IP móvil incluye un encaminador llamado agente residente, que hace un túnel de datagramas para entregas al nodo móvil. Este puede descubrir si está en su red o fuera de ella, por medio del uso de extensiones al Protocolo de control de Mensajes de Internet (ICMP). Las extensiones transmiten información del agente móvil (por ejemplo anuncios de red, solicitudes y respuestas), que permiten este descubrimiento. Los encaminadores que actúan como agentes residentes en la red propia, crean un túnel a los datagramas del nodo móvil cuando éste se encuentra por fuera de la red.

Apéndice A

Diferencias IPv4 y IPv6

Como conclusión obtenemos las siguientes diferencias de IPv4 a IPv6 en la siguiente tabla.

	Ipv4	Ipv6
Direcciones	Las direcciones de origen y destino tienen una longitud de 32 bits (4 bytes).	Las direcciones de origen y destino tienen una longitud de 128 bits (16 bytes).
IPSec	La compatibilidad es opcional.	La compatibilidad es obligatoria.
Identificación del número de paquetes	No existe ninguna identificación de flujo de paquetes para que los enrutadores controlen la QoS en el encabezado IPv4.	Se incluye la identificación del flujo de paquetes para que los enrutadores controlen la QoS en el encabezado IPv6, utilizando el campo Flow Label (etiqueta de flujo).
Fragmentación	La llevan a cabo los enrutadores y el host que realiza el envío.	No la llevan a cabo los enrutadores, sino únicamente el host que realiza el envío.
Encabezado	Incluye una suma de comprobación.	No incluye una suma de comprobación.
Opciones	El encabezado lo incluye.	Todos se trasladan a los encabezados de extensión IPv6.
Marcos de solicitud ARP	El Protocolo de resolución de direcciones (ARP) utiliza los marcos de solicitud ARP de difusión para resolver una dirección IPv4 como una dirección de capa de vínculo.	Los marcos de solicitud ARP se sustituyen por mensajes de solicitud de vecinos de multidifusión.

Administrar la pertenencia a grupos locales de subred	Se utiliza el Protocolo de administración de grupos de Internet (IGMP).	IGMP se sustituye con los mensajes de Descubrimiento de escucha de multidifusión (MLD).
Determinar la dirección IPv4 de la mejor puerta de enlace predeterminada	Se utiliza el Descubrimiento de enrutadores ICMP, y es opcional.	El Descubrimiento de enrutadores ICMP queda sustituido por la Solicitud de enrutadores ICMPv6 y los mensajes de anuncio de enrutador, y es obligatorio.
Configuración manual	Debe configurarse manualmente o a través de DHCP.	No requiere configuración manual o a través de DHCP.
DNS	Utiliza registros de recurso (A) de dirección de host en el Sistema de nombres de dominio (DNS) para correlacionar nombres de host con direcciones IPv4.	Utiliza registros de recurso (AAA) de dirección de host en el Sistema de nombres de dominio (DNS) para correlacionar nombres de host con direcciones IPv6.
Direcciones IP relacionados con host	Utiliza registros de recurso (A) de puntero en el dominio DNS IN-ADDR.ARPA para correlacionar direcciones IPv4 con nombres de host.	Utiliza registros de recurso (PTR) de puntero en el dominio DNS IP6.INT para correlacionar direcciones IPv6 con nombres de host.
Tamaño de paquete	Debe admitir un tamaño de 576 bytes (posiblemente fragmentado).	Debe admitir un tamaño de 1280 bytes (sin fragmentación).

Tabla 9. Comparación entre IPv4 y IPv6.

Referencias Bibliográficas

[1] RFC 791, Internet Protocolo versión 4, 1981, http://rfc.net/rfc791.html

[2] Jordi Palet, Martínez Tutorial de ipv6, Publicación del Foro IPv6.

[3] Bill Ball and Hoyt Duff, Red Hat Linux 9 Unleashed, Sams, United States of America, May 2003.

[4] Mark A. Miller, M&T Books, Implementing IPv6 Supporting the Next Generation Internet Protocols, Second Edition, Unites States of America.

[5] IPv6 The Next Generation Internet Protocol, Stewart S. Miller, Digital Press, United States of America.

[6] Laura Chappell, Advanced Cisco Router Configuration, Cisco Systems Cisco Press, Unites States of America, 1999.

[7] Peter Bieringer. IPv6-HOWTO. http://www.bieringer.de/linux/IPv6/.

[8] Eric Van Buggenhaut. Routing Avanzado con el Núcleo Linux. http://congreso.hispalinux.es/congreso2001/actividades/ponencias/eric/.

[9] S. Deering and R. Hinden. Request for Comments 2460: Internet Protocol, Version 6 (IPv6) Speci-_cation. The Internet Society, December 1998.

[10] Bert Hubert et al. Linux Advanced Routing and Traf_c Control HOWTO. http://www.tldp.org/HOWTO/Adv-Routing-HOWTO.html.

[11] R. Hinden and S. Deering. Request for Comments 2373: IP Version 6 Addressing Architecture.The Internet Society, July 1998.

[12] P. Marques and F. Dupont. Request for Comments 2545: Use of BGP-4 Multiprotocol Extensionsfor IPv6 Inter-Domain Routing. The Internet Society, March 1999.

[13] C. Partridge. Request for Comments 1809: Using the Flow Label Field in IPv6, June 1995.

[14] Horacio Peña. Creación de una isla IPv6 y conexión al 6bone. http://www.uninet.edu/6fevu/text/isla6bone.html.

[15] Luis Peralta. IPv6 @ UJI, Febrero 2002. http://spisa.act.uji.es/peralta/ipv6/.

[16] J. Bound R. Gilligan, S. Thomson and W. Stevens. Request for Comments 2553: Basic SocketInterface Extensions for IPv6. The Internet Society, March 1999.

[17] Y. Rekhter and T. Li. Request for Comments 1771: A Border Gateway Protocol 4 (BGP-4), March1995.

[18] W. Stevens and M. Thomas. Request for Comments 2292: Advanced Sockets API for IPv6. The Internet Society, February 1998.

[19] S. Thomson and T. Narten. Request for Comments 1886: DNS Extensions to support IP version 6. The Internet Society, December 1998.

[20] S. Thomson and T. Narten. Request for Comments 2462: IPv6 Stateless Address Autocon_guration. The Internet Society, December 1998.

[21] SeanWalton. Programaci´on de Socket Linux. Pearson Educaci´on, 2001.

[22] C Duffy Marsan, Cisco embraces IPv6, **http://www.networkworld.com/news/2000/0314ciscoipv6.html**

[23] R Wash, Microsoft Announces IPv6 Technical Preview for Windows 2000, http://www.microsoft.com/presspass/press/2000/Mar00/IPv6PR.asp**.**

[24] IPv6 Administration Guide October 2005 http://docs.sun.com/app/docs/doc/817-0573/6mgc65bbe

[25] IPv6 Internet in China, Helsinki, MAR ,2000 http://www.businesswire.com/webbox/bw.031300/200731676.htm

[27] E. Osterman Brown, Support of New Industry Standard Allows ISPs to Broaden Coverageof IPv6 Internet Access, MAR 200 http://www.businesswire.com/webbox/bw.031300/200730477.htm

[28] Takashi Arano, IPv6 Migration Issues, 2004 Intec Netcore Inc.

[29] Pete Loshin, Morghan Kaufman Publishers Inc., IPv6 Clearly Explained, Unites States of America, 2002.

[30] Stewart S. Miller, Digital Press, IPv6 The Next Generation Internet Protocol, United States of America.

[31] Implemeting Ipv6 Migrating to the next generation internet protocol, Mark A 1997, United States of America.

[32] J.Arkko et al., SEcure Neighbor Discovery (SEND), Oct 2003.http://www.ietf.org/proceedings/03nov/I-D/ draft-ietf-send-ndopt-00.txt

[33] Pekka Nikander, The CGA header approach for SEND, Jul 2003.http://www.ietf.org/proceedings/03jul/slides/send-3/send-3.ppt

[34] T. Aura ,Cryptographically Generated Addresses (CGA), Feb 2003.http://www.ietf.org/internet-drafts/draft-ietf-send-cga-05.txt

[35] Ed.Anaya Multimedia, MYSQL, Ian Gilfillan, Julio 2003

[36] Sklar, David, Ed., Introducción a PHP 5, Anaya Multimedia**,** Febrero 2005

[37] RFC 2874, IPv6 support for DNS, July2000 http://www.ietf.org/rfc/rfc2874.tx

[38] M. Martínez, J. Espinosa, Implementación de Túneles para IPv6 en Router Cisco, Universidad Sudamericana.

[39] Eva M. Castro, Porte de aplicaciones y servicios a Ipv6, http://www.6sos.org/documentos.php

[40] Michael M., Christopher E., IPv6 Transitioning Management – Laying the Foundation for Manage IPv4/IPv6 Interoperation, Computing Dept, Lancaster University, Lancaster, LA1 4YW

[41] David Fernández C, Evolución de Internet desde IPv4 a IPv6, Departamento de Ingeniería de Sistemas Telemáticos ETSIT-UPM 2002.

[42] Marcelo M, Felix E , Jorge Luis Espinoza Lira, Implementación de Túneles para IPv6 en Router Cisco, División de Informática Dpto. de Redes.