ANEXOS

ANEXO 1

LISTA DE TUNNEL BROKERS

A continuación se muestra un listado de sitios webs que permiten o brindan la facilidad de realizar conexiones mediante el método de Túnel Brokers.

- **MANIS IPv6 Tunnel Broker**
  http://tbroker.manis.net.my/
  Este tunnel broker da la flexibilidad de conectar con el 6bone que es la red IPv6 más grande que existe. No se necesita de un router IPv6 para realizar la conexión todo lo que se necesita es un host que soprte tanto las pilas IPv4 e IPv6. Este servico o el tunel está disponible por 30 días solamente.
- **Hurricane Electric IPv6 Tunnel Broker**
  http://IPv6tb.he.net
  Hurricane Electric IPv6 Tunnel Broker brinda el servicio tunnel broker gratuito que permite conectarse al Internet IPv6 haciendo un túnel con las conexiones IPv4 existentes mediante el uso de un host o router IPv6 existente en este sito web. Para utilizar este servicio se necesita tener un host con capacidad para IPv6 o un router que tenga conectividad IPv4. Este servicio se orienta hacia los desarroladores y experimentadores que desean un túnel permanente y estable para realizar pruebas de conectividad.
- **BTexact IPv6 Tunnel Broker**
  https://tb.IPv6.btexact.com/
  Este sitio perite configurar y manejar túneles IPv6 a través de la red del mismo sitio. El único requisito es registrarse en este sitio para ingresar a la configuraciónc del tunel.
- **Ngnet IPv6 Tunnel Broker**
  https://tb.ngnet.it/cgi-bin/tb.pl
  Este servicio esta disponible solamente para acceder con direcciones IP asignadas por Telecom Italia group.

ANEXO 2
LISTA DE ENRUTADORES *6TO4 RELAY*

Norteamérica

Nombre	Locación	Ancho de Banda	Contacto
6to4.ipv6.microsoft.com	**Redmond, WA / Qwest**	**?**	**www.ipv6.microsoft.com**
6to4.kfu.com	**Santa Clara, CA / Pacific Bell**	**128 kbps**	**www.kfu.com/~nsayer/mail.html**
ipv6-lab-gw.cisco.com	**San Jose / Sprint**	**100 mbps**	**ipv6-support@cisco.com**

Asia / Océano Pacifico

Nombre	Locación	Ancho de Banda	Contacto
kddilab.6to4.jp	**Tokyo, Japan / ?**	**100 mbps**	**kddilab@6to4.jp**

Europa

Nombre	Locación	Ancho de Banda	Contacto
6to4.ipv6.bt.com	**Adastral Park, UK / ?**	**10 mbps**	**stuart.prevost@bt.com**
skbys-00-00.6to4.xs26.net	**Banska Bystrica, Slovakia**	**34 mbps**	**http://www.xs26.net/**

6to4.ipv6.uni-leipzig.de	**Leipzig, Germany**	**100 mbps**	**uwe@6bone.informatik.uni-leipzig.de**
6to4.ipv6.fh-regensburg.de	**Regensburg, Germany**	**34 mbps**	**hubert.feyrer@informatik.fh-regensburg.de**
6to4.ipng.nl	**The Netherlands / AMS-IX**	**100 mbps**	**peering@ipng.nl**

ANEXO 3

CONEXION AL 6BONE

CONEXIÓN MEDIANTE EL MECANISMO 6TO4

La conexión con el 6bone que se realizo mediante el método 6to4 se resume en los siguientes pasos:

.

1. El protocolo IPv6, por defecto trae configurado este mecanismo como parte de la pila del protocolo. Al usar una direccion IPv4 pública este se autoconfigura de la siguiente manera:

```
Interfaz 3: Seudo interfaz de túnel 6to4
{A995346E-9F3E-2EDB-47D1-9CC7BA01CD73}
  no usa unidad de detección de equipos cercanos (Neighbor Discovery)
  no utiliza decubrimiento de enrutador
  retransmite paquetes
  preferencia de enrutamiento 1
    preferred global 2002:3fad:60e3::3fad:60e3, duración infinite
  vínculo MTU 1280 (vínculo MTU verdadero 65515)
  limite de saltos actual 128
  tiempo accesible 37000ms (base 30000ms)
  intervalo de retransmisión 1000ms
  transmisiones DAD 0
```

2. Se asigna una dirección 6to4 IPv6 que nos proporciona conectividad hacia routers relay IPv6 mismos que nos redireccionaran hacia el 6bone. Resolviendo las direcciones IPv6 de los sitios IPv6 a los que queremos acceder y permitiéndonos conectarnos a los mismos.

3 Podemos probar la conectividad y la resolución de direcciones con el comando **ping6,** por ejemplo con el sitio 6bone.net y obtenemos la siguiente respuesta:

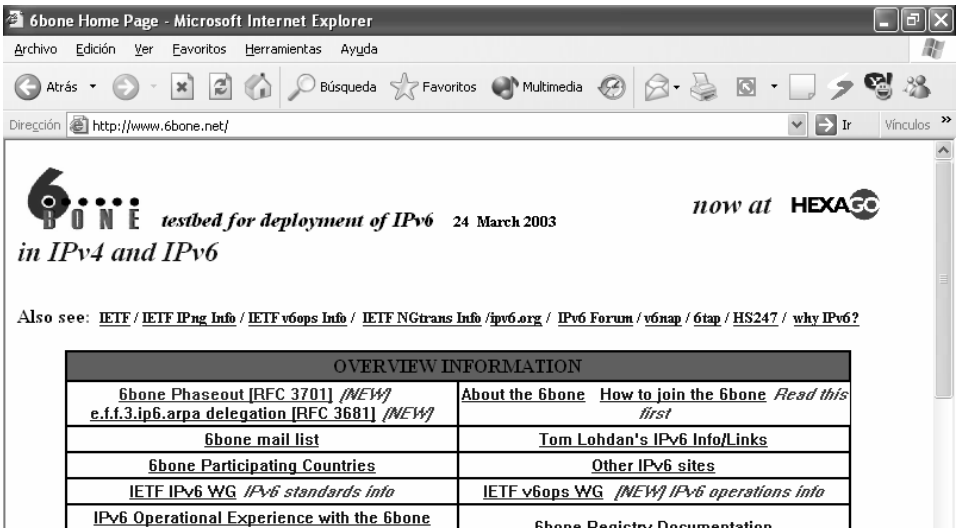
```
C:\>ping 6bone.net
```

Haciendo ping a 6bone.net [3ffe:b00:c18:1::10] con 32 bytes de datos:

Respuesta desde 3ffe:b00:c18:1::10: tiempo=1589ms
Respuesta desde 3ffe:b00:c18:1::10: tiempo=1565ms
Respuesta desde 3ffe:b00:c18:1::10: tiempo=1644ms
Respuesta desde 3ffe:b00:c18:1::10: tiempo=1634ms

Estadísticas de ping para 3ffe:b00:c18:1::10:
Paquetes: enviados = 4, recibidos = 4, perdidos = 0
(0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
Mínimo = 1565ms, Máximo = 1644ms, Media = 1608ms

Entonces ya tendremos acceso a sitios IPv6, pero es importante que nuestro explorador de Internet tenga la funcionalidad necesaria para permitirnos acceder a sitios que manejan IPv6. Por ejemplo el sitio www.6bone.net es accesible solamente a través de IPv6.



CONEXIÓN MEDIANTE TUNELES

La manera más simple de conectar al 6bone es usar el mecanismo Túnel Broker El concepto de este mecanismo es crear un túnel (IPv6 en IPv4) entre uno de los servidores de túnel y nuestro host dual-stak.

El sitio de Consulintel ofrece este servicio. Cuando configuramos nuestro tunel tenemos que proporcionar la dirección IPv4 global entregada por el ISP, entonces el tunel del lado de nuestro servidor de IPv6 over IPv4 es creado.

Antes de estar en línea con IPv6, necesitamos también configurar nuestro lado del túnel. Podemos hacerlo manualmente o podemos bajar y correr un archivo batch (script) que configurara automáticamente.

Entonces, nuestro túnel se configura totalmente y estamos conectando al 6bone. Algunos sitios 6bone podrían ser inaccesibles. Nosotros también podríamos experimentar problemas de conectividad.

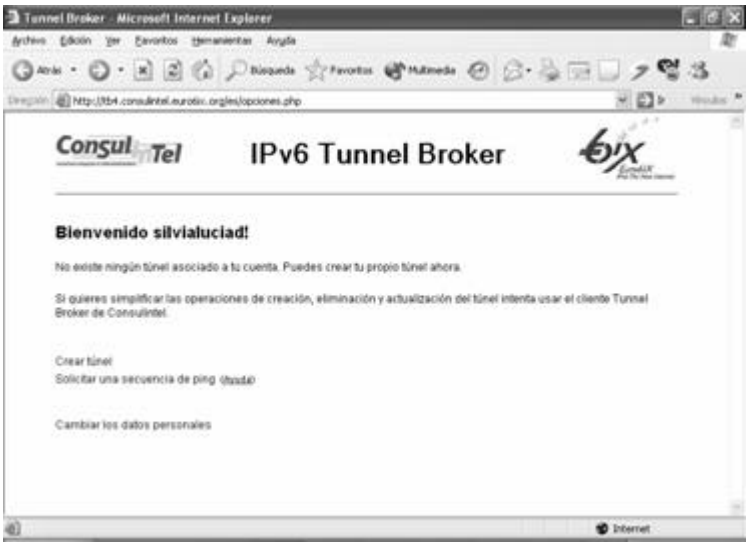
Para configurar un Tunel Broker necesitamos que un servidor de Tunel Brokers nos permita el acceso, para estos nos asigna unos datos para que podamos configurar nuestro lado del tunel y activa el tunel de su lado.

En este caso y para nuestras pruebas nos conectamos al sitio de Consulintel mediante los siguientes pasos:

1. Debemos registrarnos en el sitio de Conulintel.

2. Aquí nos pedirán datos personales del responsable del túnel a crearse, y un correo electrónico para enviarnos los datos, una vez que el túnel es aprobado podemos logarnos

3. Esto nos permitirá usar algunos servicios del Servidor de tuneles



4. Para la creación del tunel debemos proporcionar algunos datos:

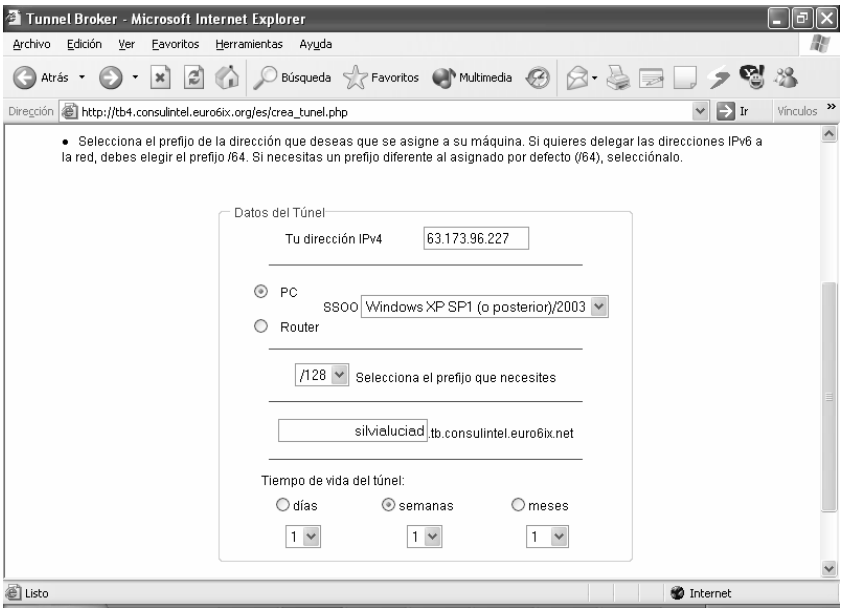
Nuestra dirección IPv4

La plataforma en que vamos a configurar

El prefijo que necesitamos que se nos asigne

El dominio que queremos

El tiempo de vida del tunel



5. Con esto el Servidor de Tunel Broker configurara su lado del tunel y nos enviara los datos necesarios para configurar nuestro lado.

Los datos que se nos proporciono son:

Nombre del tunel: tb-0063
Nuestra dirección IPv4: 63.173.96.227
Dirección IPv4 del Servidor: 213.172.48.138
Nuestra dirección IPv6: 2001:800:40:2AA0:0001::3E2

Dirección IPv6 del Servidor: 2001:800:40:2AA0:0001::3E1
silvialuciad.tb.consulintel.euro6ix.net ha sido registrado en el DNS como el nombre de dominio de nuestro extremo del túnel.

6. Los comandos que nos permiten configurar estos datos en WinXp son:

```
Install ipv6
netsh interface ipv6 add v6v4tunnel Consulintel 63.173.96.227 213.172.48.138
netsh interface ipv6 add address Consulintel 2001:800:40:2AA0:0001::3E2
netsh interface ipv6 add route 0::/0 Consulintel publish=yes
```

Al revisar la configuración con el comando **ipv6 if** se observa la interfaz de túnel que hemos configurado hacia Consulintel

Interfaz 6: Se configuró la interfaz de túnel
{0B586A2E-6651-8FBB-8995-332695BCA067}
no usa unidad de detección de equipos cercanos (Neighbor Discovery)
no utiliza decubrimiento de enrutador
preferencia de enrutamiento 1
dirección de capa de vínculo: 63.173.96.227
dirección de capa de vínculo remota: 213.172.48.138
preferred global 2001:800:40:2aa0:1::3e2, duración infinite (manual)
preferred link-local fe80::6:3fad:60e3, duración infinite
vínculo MTU 1280 (vínculo MTU verdadero 65515)
limite de saltos actual 128
tiempo accesible 18500ms (base 30000ms)
intervalo de retransmisión 1000ms
transmisiones DAD 1

7. La misma página nos permite probar nuestra conectividad mediante su servicio de prueba de conectividad.

Se debe enviar al servidor una secuencia de ping con un tamaño especifico para usar el servicio ping del tunnel broker de consulintel en nuestro caso fue el siguiente:

Tamaño del paquete ping 1: **18**
Tamaño del paquete ping 2: **121**
Tamaño del paquete ping 3: **104**
Tamaño del paquete ping 4: **48**

8. Para crear el túnel con éxito en el extremo remoto, debe recibirse la secuencia de paquetes ping completa en un tiempo inferior a 5 segundos.

Después de enviar la secuencia de paquetes ping, se configurar el túnel en nuestro extremo ejecutando el script apropiado para el sistema operativo. En tal script se usa la dirección IPv6 que el TB ha asignado a nuestra máquina cuando se uso el servicio de ping para crear el túnel.

```
ipv6 rtu ::/0 2/::213.172.48.138 pub
ipv6 adu 2/
```

9. Finalmete, si queremos eliminar este túnel en el extremo remoto se tiene que acceder a las páginas personales del TB y seleccionar la opción 'Eliminar' que aparece junto al túnel que se quiere eliminar.

Para eliminar el túnel en la máquina se ejecuta el siguiente script:

```
netsh interface ipv6 del route 0::/0 Consulintel
netsh interface ipv6 del address Consulintel 2001:800:40:2AA0:0001::3E2
netsh interface ipv6 delete interface Consulintel
```

ANEX0 4

PRUEBAS DE CONECTIVIDAD DE LA ISLA IPv6

A continuación se describe las pruebas realizadas en la Isla IPv6 para verificar el correcto funcionamiento del protocolo y la conectividad entre los elementos activos de la Isla.

Ping Link-local

Para hacer ping a un nodo usando las direcciones link-local y ver las entradas creadas en las caches neighbor y route, se realizan los siguientes pasos:

1. En ROUTER1, teclee el comando **netsh interface ipv6 show interface "Local Area Connection"** para obtener la dirección link-local de la interfaz llamada Sub red1.
2. En CLIENTE1, teclee el comando **ipv6 if** para obtener la dirección link-local y el indice de interfaz de la interfaz llamada Conexión de Área Local.
3. En CLIENTE1, teclee el comando siguiente para hacer ping a la dirección link-local de la interfaz del ROUTER1 en la Subred 1:

   ping6 *ROUTER1LinkLocalAddress%InterfaceIdentifier*

   Por ejemplo si la dirección link-local de la interfaz del ROUTER1 en la Subred 1 es FE80::2AA:FF:FE9D:10C5, y el indice de interfaz para la interfaz Conexión de Área Local en CLIENTE1 es 3, el comando es:

   ping6 FE80::2AA:FF:FE9D:10C5%3

4. En CLIENTE1, teclee el siguiente comando:

   ipv6 nc

   para ver la entrada en la cache neighbor del CLIENTE1 para ROUTER1. Usted debe ver una entrada para la dirección link-local del ROUTER1.

5. En CLIENTE1, teclee el siguiente comando:

   ipv6 rc
   para ver la entrada en la cache route del CLIENTE1 para ROUTER1

6. En CLIENTE1, teclee el siguiente comando:

   ipv6 rt
   Para ver las entradas en la tabla de ruteo del CLIENTE1.

Creación de una infraestructura de ruteo estático

Para configurar una infraestructura de ruteo estático tal que todos los nodos en la Isla IPv6 sean alcanzables usando tráfico IPv6 (exepto DNS1), complete los siguientes pasos:

1. En ROUTER1, teclee el comando **netsh interface ipv6 show interface "Local Area Connection"** para obtener la dirección link-local y el indice de interface de las interfaces llamadas Subred1 y Subred2.
2. En ROUTER1, teclee los siguientes comandos:

netsh interface ipv6 set interface [**interface=**]*Subnet1InterfaceIndex* [**forwarding=**]**enabled** [**advertise=**]**enabled**

netsh interface ipv6 set interface [**interface=**]*Subnet2InterfaceIndex* [**forwarding=**]**enabled** [**advertise=**]**enabled**

netsh interface ipv6 add route [**prefix=**]**FEC0:0:0:1::/64** [**interface=**]*Subnet1InterfaceIndex* [**publish=**]**yes**

netsh interface ipv6 add route [**prefix=**]**FEC0:0:0:2::/64** [**interface=**]*Subnet2InterfaceIndex* [**publish=**]**yes**

netsh interface ipv6 add route [**prefix=**]**::/0** [**interface=**]*Subnet2InterfaceIndex* [**nexthop=**]*ROUTER2AddressOnSubnet2* [**publish=**]**yes**

donde:

- *Subnet1InterfaceIndex* es el indice de interface de la Subred1 del ROUTER1
- *Subnet2InterfaceIndex* es el indice de interface de la Subred2 del ROUTER1
- *ROUTER2AddressOnSubnet2* es la dirección link-local asignada a la interfaz Subred 2 del ROUTER2

Por ejemplo, si el indice de interfaz de la Subred1 del ROUTER1 es 4 y el indice de interface de la Subred2 es 5, y la dirección link-local de la interfaz Subred 2 del ROUTER2 es FE80::2AA:FF:FE87:4D5C, los comandos deben ser como sigue:

netsh interface ipv6 set interface 4 forwarding=enabled advertise=enabled

netsh interface ipv6 set interface 3 forwarding=enabled advertise=enabled

netsh interface ipv6 add route FEC0:0:0:1::/64 4 publish=yes

netsh interface ipv6 add route FEC0:0:0:2::/64 3 publish=yes

netsh interface ipv6 add route ::/0 3 nexthop=FE80::2AA:FF:FE87:4D5C publish=yes

3. En ROUTER2, teclee el comando **netsh interface ipv6 show interface "Local Area Connection"** para obtener la dirección link-local y el indice de interfaz de las interfaces Subred 2 y Subred 3.
4. En ROUTER2, tipee los sigueintes comandos:

netsh interface ipv6 set interface [**interface=**]*Subnet2InterfaceIndex* [**forwarding=**]**enabled** [**advertise=**]**enabled**

netsh interface ipv6 set interface [**interface=**]*Subnet3InterfaceIndex* [**forwarding=**]**enabled** [**advertise=**]**enabled**

netsh interface ipv6 add route [**prefix=**]**FEC0:0:0:2::/64** [**interface=**]*Subnet2InterfaceIndex* [**publish=**]**yes**

netsh interface ipv6 add route [**prefix=**]**FEC0:0:0:3::/64** [**interface=**]*Subnet3InterfaceIndex* [**publish=**]**yes**

netsh interface ipv6 add route [**prefix=**]**::/0** [**interface=**]*Subnet2InterfaceIndex* [**nexthop=**]*ROUTER1AddressOnSubnet2* [**publish=**]**yes**

Por ejemplo, si el indice de interfaz de la Subred2 es 4, el indice de interface de la Subred3 es 5, y la dirección link-local de la interfaz Subred 2 de el ROUTER1 es FE80::2AA:FF:FE9A:203F, los comandos deben ser como sigue:

netsh interface ipv6 set interface 4 enabled enabled

netsh interface ipv6 set interface 3 enabled enabled

netsh interface ipv6 add route FEC0:0:0:2::/64 4 yes

netsh interface ipv6 add route FEC0:0:0:3::/64 3 yes

netsh interface ipv6 add route ::/0 4 FE80::2AA:FF:FE9A:203F publish=yes

5. En CLIENTE1, teclee el comando **ipv6 if** para ver una nueva dirección en la interfaz LAN que esta basada en el prefijo de site-local FEC0:0:0:1::/64.
6. En CLIENTE1, teclee el comando **ipv6 rt** para ver nuevas rutas para FEC0:0:0:1::/64, FEC0:0:0:2::/64, y ::/0.
7. En CLIENTE2, teclee el comando **ipv6 if** para ver una nueva dirección en la interfaz LAN que esta basada en el en el prefijo de site-local prefix FEC0:0:0:3::/64.
8. En CLIENTE2, teclee el comando **ipv6 rt** para ver nuevas rutas para FEC0:0:0:2::/64, FEC0:0:0:3**:**/64, y ::/0.
9. En CLIENTE1, teclee el comando ping6 para hacer ping a la dirección site-local del CLIENTE2:

   ping6 *CLIENT2SiteLocalAddress*

   En CLIENTE1, teclee el siguiente tracert6 con la opción -d para trazar la ruta entre CLIENTE1 y CLIENTE2:

   tracert6 -d *CLIENT2SiteLocalAddress*

   El despliegue del comando tracert6, muestra la dirección link-local de la Subred1 para el ROUTER1 y la dirección link-local de la Subred2 para el ROUTER2.

10. En ROUTER1, teclee los siguientes comandos:

    ipv6 nc

    para ver las entradas en la cache neighbor del ROUTER1 para CLIENTE1 y ROUTER2.

    ipv6 rc
    para ver las entradas en la cache route del ROUTER1 para DNS1 y ROUTER2.

Usando resolución de nombres

Para configurar el servidor DNS y el archivo Hosts local para resolver nombres a direcciones IPv6, complete los siguientes pasos:

1. En DNS1, cree una zona de reenvió lookup primaria standar llamada isla.ipv6.net.
2. Cree un registro AAAA (quad-A) para CLIENTE2 con el nombre DNS cliente2.isla.ipv6.net para su dirección site-local IPv6 usando el tipo de registro de recurso **IPv6 Host**.

   Por ejemplo, si la dirección site-local del CLIENTE2 es FEC0::3:260:8FF:FE52:F9D8, el registro de recurso AAAA es configurado como sigue:

   Host: cliente2
   Dirección de host IP version 6: FEC0:0:0:3:260:8FF:FE52:F9D8

3. En CLIENTE1, teclee el siguiente comando:

   ping6 cliente2.isla.ipv6.net

   El nombre cliente2.isla.ipv6.net se resuelve a su dirección site-local enviando una pregunta de DNS a DNS1.

4. En CLIENTE2, cree la entrada siguiente en el archivo Hosts (localizado en la carpeta *SystemRoot*\System32\Drivers\Etc):

   cliente1.isla.ipv6.net *Client1SiteLocalAddress*

   Por ejemplo, la dirección site-local del CLIENTE1 es FEC0::1:260:8FF:FE2A:15F2, la entrada en el archivo Hosts es:
   cliente1.isla.ipv6.net FEC0::1:260:8FF:FE2A:15F2

5. En CLIENTE2, teclee el siguiente comando:

   ping6 cliente1.isla.ipv6.net

   El nombre cliente1.isla.ipv6.net es resuelto por su dirección site-local usando el archivo Hosts local.

Usando direcciones temporales

Para usar direcciones temporales (también conocidas como direcciones anónimas) para prefijos de dirección globales, complete los siguientes pasos:

1. En ROUTER1, teclee el siguiente comando:

   ipv6 rtu 3FFE:FFFF:0:1::/64 *Subred1InterfaceIndex* **publish**

   donde *Subred1InterfaceIndex* es el indice de interfaz de la Subred1 del ROUTER1.

2. Por ejemplo, si el indice de interfaz de la Subred1del ROUTER1 es 4, el comando es:

   ipv6 rtu 3FFE:FFFF:0:1::/64 4 publish

3. En CLIENTE1, teclee el comando **ipv6 if** para ver las nuevas direcciones en la interfaz llamada Local Area Connection que esta basada en el prefijo global 3FFE:FFFF:0:1::/64.

   Debe haber dos direcciones que son basadas en el prefijo 3FFE:FFFF:0:1::/64. Una dirección usa un identificador de interfaz que esta basado en la dirección EUI-64 de la interfaz La otra dirección es una dirección temporal desde la cual el identificador de interfaz es derivado al azar.

4. En ROUTER1, tecle el siguiente comando:

   ipv6 rtu 3FFE:FFFF:0:1::/64 *Subred1InterfaceIndex* **life 0**

   donde Subred1InterfaceIndex es el indice de interface de la Subred1 del ROUTER1.

   Por ejemplo, si el indice de interfaz de la Subred1 es 4, el comando es:
   ipv6 rtu 3FFE:FFFF:0:1::/64 4 life 0

Esto remueve el prefijo global de la tabla de ruteo del ROUTER1 y le impide al ROUTER1 anunciarlo en sus interfaces.

Tabla de comandos utilizados en la pruebas

ipv6 if	Permite ver la dirección local de un host
ipv6 install	Instala el protocolo IPv6 en plataformas Windows
ping6	Para probar la conectividad entre dos host vecinos
ipv6 ifc… forwards advertises	Reenvio de trafico IPv6
ipv6 rtu	Anuncio de direcciones IPv6
netsh interface ipv6 6to4 set relay	Para especificar un router relay a buscar.
tracert6	Para trazar la ruta entre entre dos host
ipv6 nc	Para ver la entrada en la cache neighbor de un host a otro
ipv6 rc	Para ver la entrada en la cache route de un host a otro
ipv6 rt	Para ver las entradas en la tabla routing del CLIENT1.

ANEXO 5

Metodología para la migración IPv4 a IPv6 del backbone de la Universidad Técnica del Norte

La tecnología IP ha pasado a ser una herramienta vital de las organizaciones en el aumento de su productividad, por lo que es necesario planificar la transición de IPV4 a IPV6 (incluso su coexistencia). La transición debe incluir la preparación de operadores de redes, un inventario y migración de aplicaciones y una actualización completa de la infraestructura de redes.

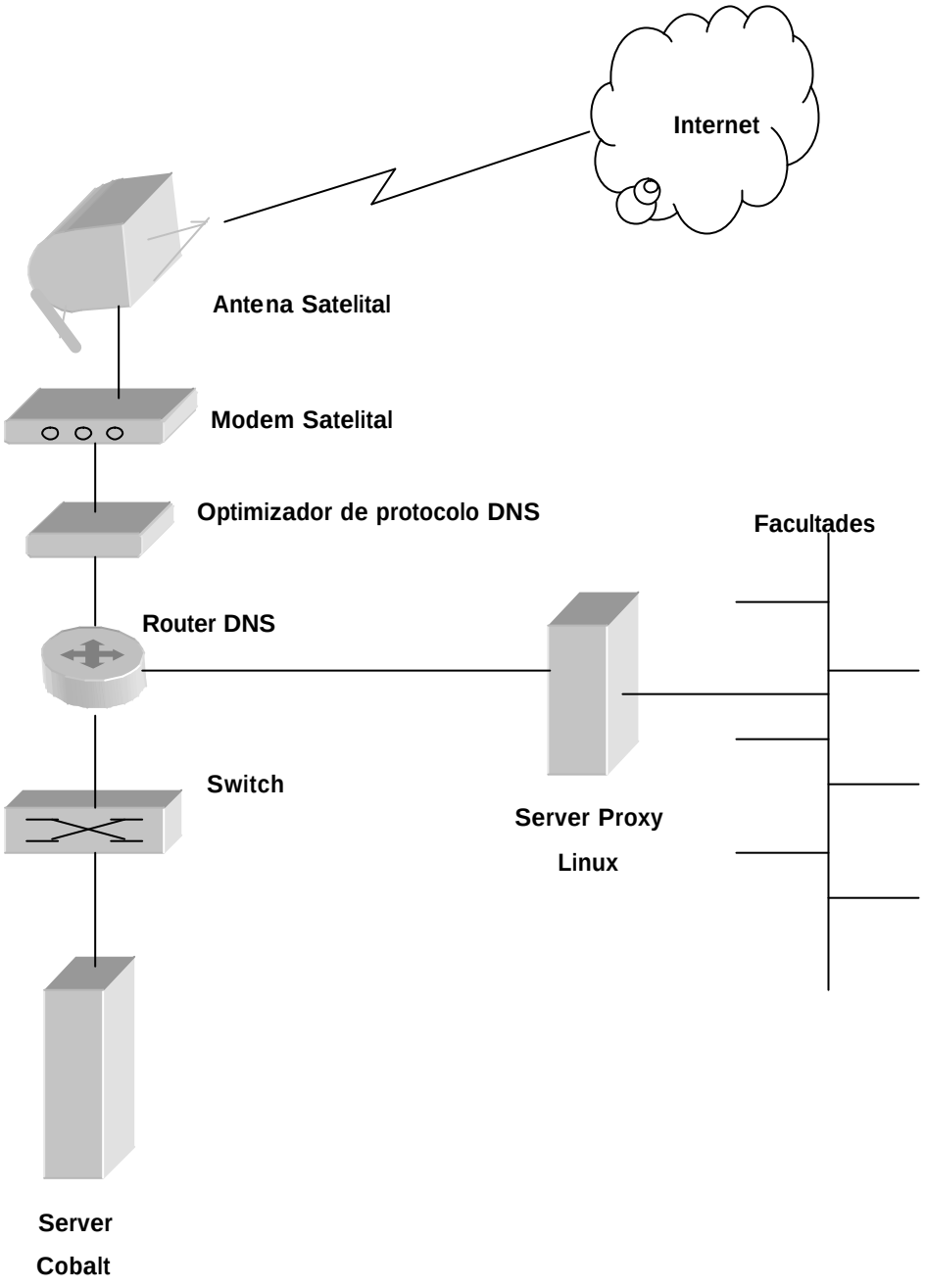
Descripción de componentes del Backbone red UTN

La solución satelital de Intellicom está constituida por dos secciones: la Unidad Interna, que incluye el módem satelital, el optimizado! de protocolo, router, switch y servidor Edge Conector; la Unidad Externa, conformada por la antena parabólica satelital de 2.4 metros de diámetro y la unidad transreceptora en la banda Ku.

Estudio preliminar

El Backbone principal de la Red UTN actualmente esta formado como se describe a continuación:

Diagrama Backbone Red UTN



Unidad Interna (IDU)

El Módem Satelital DT8000

La función principal del módem satelital es la de convertir las señales TCP-PRO, que vienen del optimizador de protocolo Mental SkyX, a señales RF, enviarlos al ODU (Outdoor Unit - Unidad Extema) y viceversa. El ancho de banda del "upiink", es programado en este componente para satisfacer el requerimiento del cliente, y puede colocarse a 19.2 Kbps, 32 Kbps, 64 Kbps, 96 Kbps, 128 Kbps ó 256 Kbps. El ancho de banda del "downlink" es de 2 Mbps compartido. El sistema VSAT trabaja en la banda de frecuencia Ku, lo que significa que transmite la señal del tluplink" en la banda 14.0-14.5 GHz y recibe la señal de "downlink" usando la banda de frecuencias 11.7-12.2
GHz. La potencia de transmisión máxima de la unidad transreceptora es de +33 dBm (2Watts) y la modulación usada es QPKS. Intellicom incorpora dentro de esta unidad la tarjeta DVB ÷ Reed - Solomon Card que permite un mejor aprovechamiento del ancho de banda.

Router Cisco 2501

Los routers Cisco 2501 están diseñados para ambientes como oficinas sucursales y sitio remotos y viene con la tecnología Flash EPROM para el mantenimiento simplificado del software. Los routers se configuran típicamente para soportar las interfases siguientes:

Ethemet (AUI)
10 BaseT Ethernet hub
Token Ring
Synchronous serial
Asynchronous serial
ISDN BRI

El router se configura para trabajar con direcciones de IP privadas, permitiendo que el tráfico dentro de los componentes de red de Intellicom, pase. Se configura también para restringir la dirección IP de otras redes. En otras palabras, permitirá únicamente, el tráfico autorizado por Intellicom, Inc.

El Optimizador de Protocolo

El Optimizador de Protocolo SkyX aumenta el flujo de información y reduce la latencia introducida por el enlace satelital, reemplazando en forma transparente TCP por el Protocolo SkyX. Especialmente optimizada para el uso en redes satelitales, este protocolo provee máximo desempeño frente a la latencia, altas pérdidas y condiciones asimétricas del ancho de banda típicas de las comunicaciones satelitales.

El Optimizador de Protocolo, intercepta las conexiones TCP del remitente y convierte los datos al Protocolo de SkyX para la transmisión por el satélite. El Optimizador de Protocolo en el lado opuesto del enlace satelital, traduce los datos de vuelta a TCP, para la comunicación con los receptores. Mediante esta arquitectura única, el Optimizador de Protocolo no requiere de ningún cambio a los stacks de TCP/ÍP en los nodos finales y no modifican la operación de TCP/IP en los segmentos terrestres de la conexión.

El servidor de Protocolo se instala entre el router y la red de computadoras local por medio de puertos duales Ethemet y es enteramente transparente para los usuarios finales. No se requiere realizar ningún cambio o modificación a los clientes (PC) ó servidores. El Optimizador de Protocolo provee desempeño mejorado sin considerar el sistema operativo, el stack TCP/IP, ó seteos de los servidores ó clientes finales.

La incorporación del Optimizador de Protocolo a una red satelital permite a los usuarios tomar plena ventaja del ancho de banda disponible. Para condiciones satelitales típicas, el Optimizador de Protocolo aumenta la velocidad de conexión a la web hasta 3 veces, o más, y hasta entre 10 y 100 veces para bajada de archivos.

El Switch Cisco 1900 Catalyst

La serie de switches Catalyst 1900 proveen la mejor solución para las redes Ethemet de hoy. Estos switches proveen 10 Mbps de ancho de banda dedicada, a la vez que alto rendimiento de conectividad entre los grupos de trabajo.

La serie de switches Catalyst 1900 ofrecen facilidad de uso mediante una interfaz de gestión intuitiva y completa. El equipo soporta las siguientes características estándar:

- Operación full dúplex en todos los puertos Ethernet y Fast Ethernet.
- Auto - negociación sobre puertos 100BaseTX para la selección automática de operación half o füll dúplex.
- Control de congestión, incluyendo control de flujo basado en IEEE 802.3x, y control de flujo basado en back-pressure sobre puertos l0BaseT.
- Doce puertos l0BaseT, proveen 10 Mbps de ancho de banda dedicados, a usuarios individuales ó a grupos de trabajo para el soporte de aplicaciones de ancho de banda intensa.
- Dos puertos 100BaseT, eliminan embotellamientos a servidores y otros dispositivos de red.
- El control mejorado de congestión acelera la transmisión de paquetes cuando los buffers del switch están llenos
- Contra-presión en los puertos Ethernet half-dúplex acelera la transmisión en la red utilizando IEEE 802.3
- Layer 2 back-offalgorithm

- Control de flujo IEEE 802.3x, sobre puertos 100BaseTX, provee gestión de flujo inteligente entre switches y entre un switch y un servidor

El Servidor Edge Connector™

Es la tercera generación de servidores que proporciona una plataforma dedicada para alojamiento de páginas web y ofrece nuevas funcionalidades para aplicaciones de alto tráfico, sitios web y de comercio electrónico. El servidor Edge Connector ™ ofrece una gama de servicios de Internet con capacidad de administración remota. El Edge Connector ™ viene pre configurado con el servidor de Red Apache, Send Mail (programa para correo electrónico), servidor para Protocolo de Transferencia de Archivos (FTP), Sistema de Nombre de Dominio (DNS), el sistema operativo Linux y extensiones de Servidor de FrontPage.

El Edge Connector ™ también provee a sus usuarios con Cuentas "Shell", Autenticación de Usuario y Archivos de Registro RADIUS. Este servidor personalizado, con su capacidad de proxy/caching y de filtrar direcciones IP, aumenta el desempeño del sistema en un 25% a 30% y trabaja conjuntamente con el sistema "caching" primario, o principal, en nuestro Centro de Operaciones de la Red, en Livermore, California. Este "cache" matriz, provee a los clientes VSAT de Intellicom, capacidad interna y extema de almacenamiento dinámico en el sistema, reflejando, efectivamente, una imagen de cada “twebsite" del cliente en el centro de datos de Livermore. Los "websites", DNS, FTP y servicios de noticias son

almacenados (cached) en la Matriz (Livermore) y el Edge Connector ™ (cliente), cada uno trabajando conjuntamente con el otro, aumentando el desempeño global del sistema.

El Edge Connector ™ mejora aún más la gama de servicios, ofreciendo administración de ancho de banda, SSL (Secure Socket Layer) pre-cargada, soporte de respaldo mejorado (backup) y reporte completo de uso del sitio.

El Edge Connector ™ provee una solución completa para el alojamiento de sitios virtuales (virtual sites), publicación en la web, transferencia de archivos, correo electrónico y desarrollo de aplicaciones de terceros. Estos servicios pueden usarse para dar soporte a sitios particulares o múltiples dentro de un entorno ya sea extranet o intranet, o a través del Internet.

A diferencia de nuestros competidores, quienes requieren de un segundo servidor para crear una barrera de seguridad, Intellicom provee una barrera de seguridad integrada que es usada en las redes internas y externas.

El Edge Connector ™ tiene dos discos duros de 30 Gbytes. El primero se usa para la operación normal del servidor y para servicios como: correo electrónico (Sendmail), DHCP (Protocolo Dinámico de Configuración de Anfitrión) y NAT (Transacción de Dirección de Red), acceso a Internet (APACHE), autenticación de suscriptor (RADIUS), FTP (Protocolo para Transferencia de archivos), DNS (Servidor de Nombre de Dominio), etc. El segundo se usa para "caching" de los sitios web usando el software SQUID. En caso de requerirse mayor capacidad de almacenamiento, se pude implementar unidades externas con discos duros adicionales.

Unidad Externa (ODU)

Antena parabólica satelital

Intelücom ofrece dos tamaños de antenas parabólicas satelitales: 1.8 y 2.4 metros de diámetro, que garantizan la recepción y transmisión de la información hacia y desde el Internet. Estas antenas son del tipo "offset" que permiten tener un menor nivel de ruido de recepción y disminuye las posibilidades de obstrucciones en la instalación de la estación.

El material de la antena parabólica satelital es de fibra y otros componentes especiales, optimizada para la recepción de señales en la banda K-u. La antena es desarmable y diseñada para soportar altas velocidades del viento, hasta 125 mph.

La base de soporte de la antena viene en dos versiones: tubo mástil penetrante y soporte no penetrante para techos. Estos soportes son de materiales galvanizados para reducir los efectos corrosivos del medio ambiente.

Unidad Transreceptora

La función de la unidad transreceptora es la de convertir la señal recibida de la Banda Ku (RF) en una señal en la banda L (IF). Adicionalmente, esta misma unidad transmite la información al satélite con una potencia máxima de transmisión es de +33 dBm (2 Watts), posee incorporado un filtro y un alimentador (Peed) para recoger y enviar las señales bidereccionales en la banda Ku de la estación Vsat.

Esta unidad está diseñada para operar en la intemperie y soportar las distintas condiciones climáticas del ambiente y se instala en el brazo de la antena satelital y por medio de cables coaxiales y de control se interconecta con el Modem satelital. Normalmente Intellicom proporciona estos cables de baja pérdidas con una longitud máxima de 80 metros, es decir que es la máxima distanc ia por medio de cable para interconectar la Unidad Interna con la Extema.

Equipo de Trabajo

Cargo	Tarea
Director de Proyecto	Dirección, coordinación y gestión del proyecto
Jefe del Laboratorio	Brindar facilidades cooperar con el análisis de requerimientos
Realizadores del Proyecto	Análisis diseño e implementación de la migración
Autoridades Universitarias	Involucrarse y cooperar con el proyecto de mejorar la tecnología con que cuenta la universidad

Análisis de Requerimientos

Equipo	Requerimiento de Migración
Router Cisco 2501	Requiere
Optimizador de protocolo	No requiere
Switch Cisco 1900 Catalyst	No requiere
Servidor Edge Connector	El equipo no especifica
Servidor Proxy Linux	Requiere

Análisis De Equipos Que Requieren Cambios

Características Técnicas Servidor UTN

Componentes Hardware

Compaq Prolaint ML 350

Procesador Intel Pentium III de 1000 MHz

128 Mb de Ram Dim

1 Disco Duro 18 GB Ultrawide SCSI III Expandible a 6 discos

1 Disk drive de 35” (1.4MB)

Memoria de video de 4 MB

Monitor Color 17” SVG428 Compaq

CDROM de 32X

Tarjeta de red 10/100 PCI

Teclado 100 teclas Win 95/98

Mouse 2 botones

Slots 2 PCI de 64 bits, 4 PCI de 32 bits, 1 ISA

ADICIONALES

3 DIMMS de memoria de 128 MB ultrawide SCSI

1 III (compaq) disco adicional

1 Kit Multimedia DVD 12X Creactive

1 Procesador Intel Pentium III de 1000 MHz

Sistema Operativo Linux Red Hat 7.2

Características Técnicas Router Cisco 2500

Interfaces :

Ethernet (AUI)

10BaseT Ethernet

Asynchronous Serial

Memoria:

Flash Memory 8 MB	Sistema Operativo, Cisco IOS
DRAM	Ambiente de Trabajo
NVRAM	Configuración y almacenamiento
ROM	Mini IOS, Bootstrap, algoritmo POTS

Procesador:

20 MHz 68030 (Motorola)

Software Options-Cisco IOS 11.2:

IP Routing

IP/IPX whit IBM base funcionalidad y APPN

Desktop (IP/IPX/AppleTalk/DEC)

Enterprise/APPN/Plus

Análisis de costos para la migración a Ipv6 de la red UTN

Equipo	**Requerimiento**	**Costo**
Servidor Proxy Linux	Instalar iproute2	Gratuito
	Instalar stak IPv6	Gratuito
	Instalar ultimas versiones de aplicaciones como el servidor Web, Proxy, DNS, etc	Gratuito
	O Instalar Red Hat 9	Gratuito
Router Cisco 2501	IOS 12.3 T Release Memoria Cisco de 16MB DRAM para Router Cisco 2500 series	550 dólares 600 dólares
	TOTAL	1150

Otros	**Costo**
Personal	1000
Investigación	2000
Documentación	300
Otros	200
TOTAL	3500

COSTO TOTAL 4650 dólares

Diseño del proceso de Migración

Una vez actualizados los equipos que describimos anteriormente, se puede proceder a escoger una de las técnicas de migración que hemos descrito en esta tesis. Una de las mas recomendable es pedir a un upstream un rango de direcciones IPv6 reales que permitan a la Universidad asignarlas a sus clientes y convertirse en una isla IPv6 de pruebas reales en el Backbone de IPv6, lo que le permitirá desarrollar la tecnología y ser parte de los cambios y pruebas que se están realizando en varios centros de investigación y universidades alrededor del mundo. Es por esto que la vamos a describir a continuación.

Los pasos a seguir son:

Los equipos actualizados deben tener capacidad de ruteo IPv6 y se les debe asignar una dirección IPv4 estática.

Preparar el router para que soporte IPv6.

Debe configurarse el router para el soporte del protocolo.

Elegir un pTLA o pNLA como upstream y contactar a sus administradores.

Los nodos del 6bone que pueden dar conexión a otros se llaman pTLA o pNLA Para conectar al 6bone precisamos que alguien nos provea de tráfico hacia la red. Habrá entonces que encontrar algún nodo del 6bone dispuesto a hacerlo. Estos son los upstream.

Debemos indicar por lo menos los siguientes datos:

- Dirección IPv4 de nuestro router.
- Número de sistema autónomo (si es que disponemos de uno)

Necesitaremos de nuestro upstream:

- Dirección IPv4 de su router.
- Número de sistema autónomo.
- Direcciones IPv6 para el túnel.
- Bloque IPv6 que nos será asignado.

Nuestro upstream debe asignarnos un bloque de direcciones IPv6 para nuestra isla. Estos bloques son equivalentes a los CIDR en IPv4, normalmente tienen un prefijo /48 (esto es, los primeros 48 bits identifican nuestra isla, y tenemos 16 bits para organizar nuestras redes, teniendo capacidad para una cantidad a los efectos prácticos infinita de dispositivos conectados a cada red)

Crear el túnel hacia el upstream.

Hemos de crear el túnel asignando las direcciones IPv4 local y remota y luego configurar la interfaz del túnel como una punto a punto normal.

Una vez hecho esto (y si nuestro upstream hizo su parte) podríamos verificar la conectividad por el túnel usando el comando ping6

Activar protocolos de ruteo.

En esta isla, sería suficiente trabajar con rutas estáticas, sin embargo, dado que estamos experimentando es conveniente hacerlo también con los nuevos protocolos de ruteo y generar estos mapas automáticamente, con el fin de realizar pruebas de su funcionamiento.

Agregar otros equipos (clientes y servidores) a la isla.

Una vez conectado este equipo al 6bone. Se puede ir expandiendo la isla hasta que toda nuestra red funcione con IPv6.

El paso inicial es configurar el router para que anuncie su existencia en la red local a la que esté conectado.

Ahora, cualquier equipo con capacidad IPv6 se autoconfigurará e ingresará al 6bone con solo conectarlo al mismo segmento que el router.

De aquí en más, el trabajo principal será ir modificando las aplicaciones que solo funcionan en IPv4 por aquellas que lo hagan con IPv6.

Registrar la isla enel 6bone.

El último paso es anotarse en el registro de islas del 6bone.

Pruebas y Mantenimiento

Después de configurada la isla es importante que se siga con la investigación, y con el proceso de pruebas y migración con los nuevos cambios que se vayan realizando al protocolo hasta que su implementación sea global en Internet.

Documentación

Se va realizando a la par que se realiza todo el trabajo.

ANEXO 6
Instalación de IPv6 en plataformas Linux

Este ANEXO presenta o describe como instalar el protocolo IPv6 en plataformas Linux
En Linux, IPv6 se implementa como un módulo del kernel. Así, las distribuciones con kernel 2.2.x y 2.4.x ya vienen con este soporte y normalmente el módulo IPv6 ya está instalado. De todas formas, habrá que asegurarse que el módulo se carga al arrancar.

Ya existen muchas aplicaciones que funcionan con IPv6. Las últimas versiones de los servidores más usados para los servicios básicos ya soportan IPv6:
WEB (Apache: http://www.apache.org).
DNS (BIND: http://www.isc.org).
FTP
TELNET
SSH (OpenSSH: http://www.openssh.com).
E-MAIL (Sendmail: http://www.sendmail.org).

También existen clientes de estos servicios con soporte IPv6. Incluso se pueden encontrar escritorios completos que ofrecen la mayoría de sus aplicaciones en IPv6, un ejemplo de esto es KDE.

Para comprobar que el kernel soporta IPv6, habrá que comprobar que existe la siguiente entrada:
/proc/net/if_inet6

Si no existe, se puede intentar cargar el módulo ipv6 con:
#> modprobe ipv6

Si se ha cargado correctamente debe existir la entrada mencionada arriba. Descargar el módulo puede, a veces, provocar la caída del sistema. Aunque en versiones actuales de los módulos (kernel 2.4.19 adelante) el soporte es muy estable.

Para que cargue de forma automática el módulo IPv6 cuando se demande, se añade al fichero /etc/modules.conf la siguiente línea:

```
alias net-pf-10 ipv6
alias sit0 ipv6
alias sit1 ipv6
alias tun6to4 ipv6
```

Para deshabilitar la carga automática se debe usar alias net-pf-10 off

Para configurar IPv6 se necesitan herramientas como las siguientes:

Paquete net-tools: Usando ifconfig, route. Todas las versiones actuales soportan las extensiones IPv6.

Paquete iproute: Debe existir el programa /sbin/ip, dado que este programa es una extensión del paquete anterior, todas las versiones tienen incorporado el soporte IPv6.

Scripts de configuración IPv6

Se utilizan scripts para inicializar todo lo relacionado con IPv6 y para configurar la direcciones v4/v6 de las interfaces. Conviene actualizar a la última versión de los mismos. Estos scripts pueden obtenerse en:

http://www.bieringer.de/linux/IPv6/IPv6-HOWTO/scripts/current/index.html

Aun qué la mayoría de distribuciones actuales configuran estos script en la instalación del sistema.

Para la configuración realizamos los siguientes pasos:

1. Se descarga la última versión (IPv6-initscripts-20020125.tar.gz) y se descomprime. Se copian los ficheros de script a los directorios correspondientes:

```
/etc/sysconfig/network-scripts/network-functions-ipv6
/etc/sysconfig/network-scripts/init.ipv6-global
/etc/sysconfig/network-scripts/ifup-ipv6
/etc/sysconfig/network-scripts/ifdown-ipv6
/etc/sysconfig/network-scripts/ifup-sit
/etc/sysconfig/network-scripts/ifdown-sit
/etc/ppp/ip-up.ipv6to4
/etc/ppp/ip-down.ipv6to4
```

/etc/ppp/ipv6-up
/etc/ppp/ipv6-down
/usr/sbin/test-ipv6-installation
/etc/sysconfig/static-routes-ipv6

2. A continuación se aplican "parches". Algunos parches solo se aplican a determinadas versiones de Red Hat, por ejemplo con ifup.diff que solo se usa para RH 7.1.

Copiar el archivo .diff al mismo directorio donde está el archivo a parchar

#>cat network.diff | patch (/etc/sysconfig/)
#>cat ifup.diff | patch (/etc/sysconfig/network-scripts/ [link /sbin/)(RH 7.1)]
#>cat network.diff | patch (/etc/rc.d/init.d/) (RH 7.1)

Se recomienda instalar ipv6calc para habilitar la detección de direcciones extendidas. Puede obtenerse de:

http://www.bieringer.de/linux/IPv6/ipv6calc/index.html

3. El tar.gz (ipv6calc-0.39.tar.gz) incluye el fichero spec-file, de forma que se puede crear el RPM mediante:

root# rpm –ta ipv6calc-version.tar.gz

Para instalar:

root# cd /usr/src/redhat/RPMS/i386
root# rpm –i ipv6calc-version.i386.rpm

Debe existir, ahora, /bin/ipv6calc

En el fichero sysconfig-ipv6.txt que viene con el paquete de scripts, se da información detallada de los parámetros que se pueden configurar en cada script.

Para comprobar que la configuración es correcta, se puede ejecutar el script:

/usr/sbin/test-ipv6-installation, que viene con el paquete.

Configuración de red

Realizamos los siguientes pasos:
1. Para cambiar el nombre del host se pone en /etc/sysconfig/network, la línea:

HOSTNAME=nombre_host

Conviene, después de esto, añadirlo en el fichero /etc/hosts:

::1 nombre_host

El nombre de host puede verse en /proc/sys/kernel/hostname, o simplemente ejecutando /bin/hostname sin ningún parámetro.

2. Se deben añadir entradas en /etc/hosts para IPv6:

::1 localhost ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
ff02::3 ip6-allhosts

3. Comprobar que en /etc/protocols/ aparecen:

ipv6 41 IPv6
ipv6-route 43 IPv6-Route
ipv6-frag 44 IPv6-Frag
ipv6-crypt 50 IPv6-Crypt
ipv6-auth 51 IPv6-Auth
ipv6-icmp 58 IPv6-ICMP
ipv6-nonxt 59 IPv6-NoNxt
ipv6-opts 60 IPv6-Opts

4. Comprobar que el fichero /etc/nsswitch.conf es correcto. Si no se pretende utilizar NIS (ni NIS+), habrá que comentar/eliminar las entradas con nisplus.

hosts: files dns
networks: files dns

Configurar /etc/host.conf:
order hosts,bind
multi on

De forma que el resolver primero consulte el fichero /etc/hosts y luego al servidor de nombres. La segunda línea hace que el resolver devuelva todas las direcciones válidas para un host encontrado en /etc/hosts/, en vez de sólo la primera.

5. Configurar /etc/resolv.conf

domain: especifica el nombre del dominio local

search: lista de nombres de dominio alternativo para búsqueda del nombre de un host

nameserver: dirección IP de servidores de nombre a los que consultar (pueden ser varios, varias líneas "nameserver").

6. Para cada interfaz existirá un fichero con la configuración que se le asignará al arrancar. Supongamos que se tiene una interfaz hacia la red local (10.0.0.x/24). En etc/sysconfig/networkscripts/

ifcfg-eth0
DEVICE=eth0
IPADDR=10.0.0.3
NETMASK=255.255.255.0
NETWORK=10.0.0.0
BROADCAST=10.0.0.255
GATEWAY=10.0.0.1
ONBOOT=yes

El fichero /etc/sysconfig/network tiene, respecto a IPv4:
GATEWAYDEV=eth0
GATEWAY=10.0.0.1

Que añade la ruta por defecto a través de eth1 y la IP del switch de salida hacia el ISP.

Para establecer rutas de manera estática al arrancar el equipo (o la configuración de red) se puede utilizar el fichero /etc/sysconfig/static-routes (para IPv4) o /etc/sysconfig/staticroutes- ipv6 (para IPv6).

En el script /etc/init.d/network se encuentra:

```
# Add non interface-specific static-routes
if [-f /etc/sysconfig/static-routes]; then
grep "^any" /etc/sysconfig/static-routes | \
while read ignore args; do
/sbin/route add -$args
done
fi
```

Un ejemplo de fichero /etc/sysconfig/static-routes:
any net 10.0.0.0/24 gw 192.168.11.1

Que añade la ruta para la red 10.0.0.0/24 a través de la puerta de enlace 192.168.11.1.

7. Para asignar a eth0 direcciones IPv6 se realiza lo siguiente:

En el directorio /etc/sysconfig/network-scripts/ habrá un fichero para cada interfaz (eth0).

Se añade:
A ifcfg-eth0 (CASO DE AUTOCONFIGURACIÓN):

IPV6INIT=yes # Habilita IPv6 en este interfaz
IPV6AUTOCONF=yes # habilita autoconfiguracion
Es esta red se encuentra un router con el RA activado, de forma que la dirección IPv6 se configura automáticamente.

A ifcfg-eth0 (CASO ASIGNACIÓN IPv6 ESTÁTICA):

IPV6INIT=yes # Habilita IPv6 en este interfaz
IPV6AUTOCONF=no # No habilita autoconfiguracion
IPV6ADDR=3ffe:3328:6:2a03::3 # asigna direccion IPv6 fija
A esta interfaz se le asigna una dirección IPv6 fija.

El fichero /etc/sysconfig/network tiene, respecto a IPv6:
NETWORKING_IPV6=yes
IPV6FORWARDING=no
IPV6_AUTOCONF=yes
IPV6_AUTOTUNEL=no
IPV6_DEFAULTGW="3ffe:3328:6:2a03::1%eth0"

Que establece como gateway para IPv6 el router que se conecta por la interfaz eth0.

Mediante ifconfig, comprobar la configuración IPv6. Cuando se haga un cambio en la configuración de red, se puede reiniciar todo el sistema de red ejecutando el script: /etc/rc.d/init.d/network restart.

También acepta otros parámetros (stop, start, status, etc).

Comandos útiles

Mostrar direcciones IPv6
Se puede hacer mediante el uso de ip o ifconfig:
#> /sbin/ip -6 addr show dev <interface>
#> /sbin/ifconfig <interface>

Donde <interface> puede ser lo, eth0, etc. Por ejemplo:

#> /sbin/ip -6 addr show dev eth0
#> /sbin/ifconfig eth0

Añadir una dirección IPv6
Se puede hacer mediante el uso de ip o ifconfig:
#> /sbin/ip -6 addr add <ipv6address>/<prefixlength> dev <interface>
#> /sbin/ifconfig <interface> inet6 add <ipv6address>/<prefixlength>

Donde <interface> puede ser lo, eth0, etc. Por ejemplo:
#> /sbin/ip -6 addr add 3ffe:ffff:0:10:2a01::2/64 dev eth0
#> /sbin/ifconfig eth0 inet6 add 3ffe:ffff:0:10:2a01::2/64

Eliminar una dirección IPv6
Se puede hacer mediante el uso de ip o ifconfig:
#> /sbin/ip -6 addr del <ipv6address>/<prefixlength> dev <interface>
#> /sbin/ifconfig <interface> inet6 del <ipv6address>/<prefixlength>

Donde <interface> puede ser lo, eth0, etc. Por ejemplo:
#> /sbin/ip -6 addr del 3ffe:ffff:0:10:2a01::2/64 dev eth0
#> /sbin/ifconfig eth0 inet6 del 3ffe:ffff:0:10:2a01::2/64

Mostrar rutas IPv6
Se puede hacer mediante el uso de ip o route:
#> /sbin/ip -6 route show [dev <device>]
#> /sbin/route -A inet6

Donde <device> puede ser lo, eth0, etc. Por ejemplo:
#> /sbin/ip -6 route show dev eth0
#> /sbin/route -A inet6 |grep -w "eth0"

Añadir una ruta IPv6 a través de un gateway
Se puede hacer mediante el uso de ip o route:
#> /sbin/ip -6 route add <ipv6network>/<prefixlength> via <ipv6address>
[dev <device>]
#> /sbin/route -A inet6 add <ipv6network>/<prefixlength> gw <ipv6address>
[dev <device>]

Donde <device> puede ser lo, eth0, etc. Por ejemplo:
#> /sbin/ip -6 route add 2000::/3 via 3ffe:ffff:0:f101::1 dev eth0
#> /sbin/route -A inet6 add 2000::/3 gw 3ffe:ffff:0:f101::1 dev eth0

Eliminar una ruta IPv6 a través de un gateway
Se puede hacer mediante el uso de ip o route:
#> /sbin/ip -6 route del <ipv6network>/<prefixlength> via <ipv6address>
[dev <device>]
#> /sbin/route -A inet6 del <ipv6network>/<prefixlength> gw <ipv6address>
[dev <device>]

Donde <device> puede ser lo, eth0, etc. Por ejemplo:
#> /sbin/ip -6 route del 2000::/3 via 3ffe:ffff:0:f101::1 dev eth0
#> /sbin/route -A inet6 del 2000::/3 gw 3ffe:ffff:0:f101::1 dev eth0

Añadir una ruta IPv6 a través de una interfaz
Se puede hacer mediante el uso de ip o route:
#> /sbin/ip -6 route add <ipv6network>/<prefixlength> dev <device>
metric 1
#> /sbin/route -A inet6 add <network>/<prefixlength> dev <device>

Donde <device> puede ser lo, eth0, etc. Por ejemplo:
#> /sbin/ip -6 route add 2000::/3 dev eth0 metric 1
#> /sbin/route -A inet6 add 2000::/3 dev eth0

Eliminar una ruta IPv6 a través de una interfaz
Se puede hacer mediante el uso de ip o route:
#> /sbin/ip -6 route del <ipv6network>/<prefixlength> dev <device>
metric 1
#> /sbin/route -A inet6 del <network>/<prefixlength> dev <device>

Donde <device> puede ser lo, eth0, etc. Por ejemplo:
#> /sbin/ip -6 route del 2000::/3 dev eth0 metric 1
#> /sbin/route -A inet6 del 2000::/3 dev eth0

Ping6
Normalmente incluido en el paquete iputils. Uso:
#> ping6 <hostwithipv6address>
#> ping6 <ipv6address>
#> ping6 [-I <device>] <link-local-ipv6address>

Traceroute6
Normalmente incluido en el paquete iputils. Uso:
#>traceroute6 www.kame.net

Tracepath6
Normalmente incluido en el paquete iputils. Uso:
#>tracepath6 www.kame.net

Tpcdump
Herramienta muy útil para capturar paquetes en la red.

ANEXO 7

REFERENCIAS RFC'S

Numero	Titulo	Fecha	Autor
RFC3056:	Connection of IPv6 Domains via IPv4 Clouds	February 2001	B. Carpenter, K. Moore
RFC3053:	IPv6 Tunnel Broker	January 2001	A. Durand, P. Fasano, I. Guardini, D. Lento
RFC3041:	Privacy Extensions for Stateless Address Autoconfiguration in IPv6	January 2001	T. Narten, R. Draves
RFC3019:	IP Version 6 Management Information Base for The Multicast Listener Discovery Protocol	January 2001	B. Haberman, R. Worzella
RFC2976:	The SIP INFO Method	October 2000	S. Donovan
RFC2974:	Session Announcement Protocol	October 2000	M. Handley, C. Perkins, E. Whelan
RFC2928:	Initial IPv6 Sub-TLA ID Assignments	September 2000	R. Hinden, S. Deering, R. Fink, T. Hain
RFC2921:	6BONE pTLA and pNLA Formats (pTLA)	September 2000	B. Fink
RFC2894:	Router Renumbering for IPv6	August 2000	M. Crawford
RFC2893:	Transition Mechanisms for IPv6 Hosts and Routers	August 2000	R. Gilligan, E. Nordmark
RFC2874:	DNS Extensions to Support IPv6 Address Aggregation and Renumbering	July 2000	M. Crawford, C. Huitema
RFC2848:	The PINT Service Protocol: Extensions to SIP and SDP for IP	June 2000	S. Petrack, L. Conroy
RFC2772:	6Bone Backbone Routing Guidelines	February 2000	R. Rockell, R. Fink
RFC2767:	Dual Stack Hosts using the Bump-In-the-Stack Technique (BIS)	February 2000	K. Tsuchiya, H. Higuchi, Y. Atarashi
RFC2766:	Network Address Translation - Protocol Translation (NAT-PT)	February 2000	G. Tsirtsis, P. Srisuresh
RFC2765:	Stateless IP/ICMP Translation Algorithm (SIIT)	February 2000	E. Nordmark
RFC2740:	OSPF for IPv6	December 1999	R. Coltun, D. Ferguson, J. Moy
RFC2732:	Format for Literal IPv6 Addresses in URL's	December 1999	R. Hinden, B.

			Carpenter, L. Masinter
RFC2711:	IPv6 Router Alert Option.	October 1999	C. Partridge, A. Jackson
RFC2710:	Multicast Listener Discovery (MLD) for IPv6.	October 1999	S. Deering, W. Fenner, B. Haberman
RFC2675:	IPv6 Jumbograms.	August 1999	D. Borman, S. Deering, R. Hinden
RFC2590:	Transmission of IPv6 Packets over Frame Relay Networks.	May 1999	A. Conta, A. Malis, M. Mueller
RFC2553:	Basic Socket InterfaceExtensions for IPv6.	March 1999	R. Gilligan, S. Thomson, J. Bound, W. Stevens
RFC2545:	Use of BGP-4 Multiprotocol Extensions for IPv6 Inter-Domain Routing	March 1999	P. Marques, F. Dupont
RFC2543:	RFC 2543 - Session Initiation Protocol	March 1999	M. Handley, H. Schulzrinne, E. Schooler, J. Rosenberg
RFC2529:	Transmission of IPv6 over IPv4 Domains without Explicit Tunnels.	March 1999	B. Carpenter, C. Jung
RFC2526:	Reserved IPv6 Subred Anycast Addresses.	March 1999	D. Johnson, S. Deering
RFC2509:	IP Header Compression over PPP.	February 1999	M. Engan, S. Casner, C. Bormann
RFC2508:	Compressing IP/UDP/RTP Headers for Low-Speed Serial Links.	February 1999	S. Casner, V. Jacobson
RFC2507:	IP Header Compression.	February 1999	M. Degermark, B. Nordgren, S. Pink
RFC2497:	Transmission of IPv6 Packets over ARCnet Networks.	January 1999	I. Souvatzis
RFC2492:	IPv6 over ATM Networks.	January 1999	G. Armitage, P. Schulter, M. Jork
RFC2491:	IPv6 over Non-Broadcast Multiple Access (NBMA) networks.	January 1999	G. Armitage, P. Schulter, M. Jork, G. Harter
RFC2474:	Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers.	December 1998	K. Nichols, S. Blake, F. Baker, D. Black
RFC2473:	Generic Packet Tunneling in IPv6 Specification.	December 1998	A. Conta, S. Deering
RFC2472:	IP Version 6 over PPP.	December 1998	D. Haskin, E. Allen
RFC2471:	IPv6 Testing Address Allocation.	December 1998	R. Hinden, R.

			Fink, J. Postel (deceased)
RFC2470:	Transmission of IPv6 Packets over Token Ring Networks.	December 1998	M. Crawford, T. Narten, S. Thomas
RFC2467:	Transmission of IPv6 Packets over FDDI Networks.	December 1998	M. Crawford
RFC2466:	Management Information Base for IP Version 6: ICMPv6 Group.	December 1998	D. Haskin, S. Onishi
RFC2465:	Management Information Base for IP Version 6: Textual Conventions and General Group.	December 1998	D. Haskin, S. Onishi
RFC2464:	Transmission of IPv6 Packets over Ethernet Networks.	December 1998	M. Crawford
RFC2463:	Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification.	December 1998	A. Conta, S. Deering
RFC2462:	IPv6 Stateless Address Autoconfiguration.	December 1998	S. Thomson, T. Narten
RFC2461:	Neighbor Discovery for IP Version 6 (IPv6).	December 1998	T. Narten, E. Nordmark, W. Simpson
RFC2460:	Internet Protocol, Version 6 (IPv6) Specification.	December 1998	S. Deering, R. Hinden
RFC2454:	IP Version 6 Management Information Base for the User Datagram Protocol	December 1998	M. Daniele
RFC2452:	IP Version 6 Management Information Base.	December 1998	M. Daniele
RFC2450:	Proposed TLA and NLA Assignment Rules.	December 1998	R. Hinden
RFC2428:	FTP Extensions for IPv6 and NATs.	September 1998	M. Allman, S. Ostermann, C. Metz
RFC2406:	IP Encapsulating Security Payload (ESP).	November 1998	S. Kent, R. Atkinson
RFC2402:	IP Authentication Header.	November 1998	S. Kent, R. Atkinson
RFC2401:	Security Architecture for the Internet Protocol.	November 1998	S. Kent, R. Atkinson
RFC2375:	IPv6 Multicast Address Assignments.	July 1998	R. Hinden, S. Deering
RFC2374:	An IPv6 Aggregatable Global Unicast Address Format.	July 1998	R. Hinden, M. O'Dell, S. Deering
RFC2373:	IP Version 6 Addressing Architecture.	July 1998	R. Hinden, S. Deering
RFC2365:	Administratively Scoped IP Multicast	July 1998	D. Meyer
RFC2327:	SDP: Session Description Protocol	April 1998	M. Handley, V. Jacobson

RFC2292:	Advanced Sockets API for IPv6.	February 1998	W. Stevens, M. Thomas
RFC2185:	Routing Aspects of IPv6 Transition.	September 1997	R. Callon, D. Haskin
RFC2081:	RIPng Protocol Applicability Statement.	January 1997	G. Malkin
RFC2080:	RIPng for IPv6.	January 1997	G. Malkin, R. Minnear
RFC2030:	Simple Network Time Protocol (SNTP) Version 4 for IPv4, IPv6 and OSI.	October 1996	D. Mills
RFC1981:	Path MTU Discovery for IP version 6.	August 1996	J. McCann, S. Deering, J. Mogul
RFC1924:	A Compact Representation of IPv6 Addresses.	April 1996	R. Elz
RFC1888:	OSI NSAPs and IPv6.	August 1996	J. Bound, B. Carpenter, D. Harrington, J. Houldsworth, A. Lloyd
RFC1887:	An Architecture for IPv6 Unicast Address Allocation.	December 1995	Y. Rekhter, T. Li, Editors
RFC1886:	DNS Extensions to support IP version 6.	December 1995	S. Thomson, C. Huitema
RFC1884:	IP Version 6 Addressing Architecture	December 1995	R. Hinden, S. Deering, Editors
RFC1881:	IPv6 Address Allocation Management.	December 1995	IAB, IESG
RFC1829:	The ESP DES-CBC Transform.	August 1995	P. Karn, P. Metzger, W. Simpson
RFC1828:	IP Authentication using Keyed MD5.	August 1995	P. Metzger, W. Simpson
RFC1810:	Report on MD5 Performance	June 1995	J. Touch
RFC1809:	Using the Flow Label Field in IPv6.	June 1995	C. Partridge
RFC1752:	The Recommendation for the IP Next Generation Protocol.	January 1995	S. Bradner, A. Mankin

ANEXO 8

ANTEPROYECTO DE TESIS

ANTEPROYECTO DE TESIS

TEMA:

ANÁLISIS DEL PROTOCOLO IPv6 SU EVOLUCION Y APLICABILIDAD

APLICATIVO:

CONFIGURACION DE UNA ISLA IPv6

AUTORES:

SILVIA DUQUE

DAVID VALLEJO

DIRECTOR: ING. RODRIGO NARANJO

ASESORES:

ING. DENNIS CRIOLLO

2002

1. TEMA:

ANÁLISIS DEL PROTOCOLO IPv6 SU EVOLUCIÓN Y APLICABILIDAD

2. APLICATIVO:

CONFIGURACIÓN DE UNA ISLA IPv6

3. PROBLEMA:

Los creadores de IPv4 a principio de los 70 no predijeron el gran éxito que este protocolo iba a tener en muy poco tiempo y en una variedad de campos. Por esto ha sido necesario crear parches al protocolo básico como QoS (calidad de servicio), Ipsec(seguridad y movilidad), NAT(traslación de direcciones), estos tienen el inconveniente de que si bien solos son sencillos de usar en conjunto es muy poco practico y a veces imposible, además de ser soluciones temporales, por esto es imprescindible buscar un estándar que se adapte mejor a las necesidades del entorno.

En el seno del IETF (Internet Engineering Task Force) se esta desarrollando el IPv6 como la solución a varios de los problemas de IPv4, siendo el principal la falta de direcciones, la razón de utilización de las direcciones IP esta pasando en muy pocos meses de 10:1 a 1:1, y la tendencia pronto se invertirá. O problemas como la gran dimensión de las tablas de routing en la troncal de Internet, aplicaciones y dispositivos que solo trabajan con IPs reales, routers que no reconocen IPs ficticias, el desarrollo de la telefonía, voz sobre IP, dispositivos inalámbricos, electrodomésticos, dispositivos de seguridad, de control, médicos, etc, que requieren comunicarse transparentemente con otros independientemente de su localización en la red global , nos lleva a la necesidad de un espacio de direcciones mucho mayor al existente. El IPv6 nos brinda este espacio además de ventajas adicionales.

4. JUSTIFICACIÓN :

- *La tecnología progresa rápidamente. Un ejemplo de ello es el Internet que nos va brindando cada vez más infinidad de posibilidades de aplicación. Por esta razón sus bases fundamentales necesitan ser actualizadas para que esta gran infraestructura ya creada tenga posibilidades de seguir creciendo y mejorando, para beneficio de todos sus usuarios.*

- *El presente trabajo, pretende enfocar un estudio sobre la nueva generación del protocolo en el que esta basado Internet IP, ahora llamado IPv6 , a fin de recopilar información que facilite la comprensión de este tema, así como su implementación, ya que, por estar su experimentación restringida a un número de personas limitadas, esta información no ha sido mayormente difundida y documentada, a pesar de su indiscutible importancia.*

- *El éxito no sospechado al principio que ha tenido Internet ha llevado al rápido agotamiento del espacio de direcciones que fue diseñado para IPv4, a pesar de contar con mas de cuatro billones de direcciones (4.294.967.296) no es suficiente, debido al rápido crecimiento de los usuarios conectados, y a la falta de coordinación que durante la década de los ochenta se produjo en la delegación de direcciones*

- *El desarrollo de redes de telefonía celular, dispositivos inalámbricas(Note Books, Palms, Walkman Mp3), modems de cable, xDSL, sistemas de seguridad, aplicaciones como la videoconferencia, la voz en IP, seguridad, etc, que requieren direcciones IP únicas globales, la creación de nuevos dispositivos domésticos, industriales, médicos, de control, etc que son conectados a la red con diversos fines, además del desarrollo de tecnologías emergentes como Bluetooth o WAP, hacen que las necesidades de direcciones IP crezcan exponencialmente conforme la tecnología avanza, haciendo necesaria la búsqueda de alternativas al estándar de direccionamiento actual.*

5. OBJETIVOS:

Generales

- *Establecer generalidades del protocolo IPv6, su evolución y aplicabilidad.*
- *Aplicar el protocolo en una isla IPv6 para probar su funcionalidad y conexión al 6bone.*

Específicos

- *Realizar un estudio de IPv4, sus problemas actuales, el porque y la historia del proceso de transición de IPv4 a IPv6. CAP I.*
- *IPv4 versus IPv6. Pros, contras, ventajas y desventajas. CAP I*
- *Conocer los conceptos relacionados con IPv6: definiciones básicas, direccionamiento, configuración, seguridad, aplicaciones, implementaciones, etc. CAP II.*
- *Estudiar los mecanismos de transición usados, como Stacks dobles, túneles, etc. CAP III.*
- *Recopilar información sobre algunas plataformas y equipos en las que IPv6 se a implementado, aprender a configurar IPv6 en los mismos. CAP IV*
- *Proporcionar una fuente de consulta de IPv6 y sus aplicaciones en nuestro medio, para ayudar en el proceso de cambio a la nueva generación de IP. CAP IV*
- *Unirnos a sitios que son la base del nuevo Internet, Internet6. CAPIV*
- *Desarrollar una red interna que permita la puesta en práctica de IPv6 para probar su funcionamiento y el de sus aplicaciones. CAP IV*

6. MARCO TEORICO:

PROTOCOLO IP VERSIÓN 6 (IPv6)

El Internet Enginnering Task Force, IETF, creó el proyecto IPng: ***Internet Protocol the Next Generation****, también llamado IPv6. Esta nueva versión del Internet Protocol sustituirá progresivamente a IPv4, ya que brinda mejores características, entre las que destacan: espacio de direcciones prácticamente infinito, posibilidad de autoconfiguración de hosts, eficaz soporte para seguridad, computación movil, calidad de servicio, transporte de tráfico multimedia en tiempo real y aplicaciones anycast y multicast, posibilidad de transición gradual de IPv4 a IPv6, etc.*

IPv6 es la versión nueva del Protocolo en que se basa Internet que está diseñada como un paso evolutivo del IPv4. Representa el fruto de muchas propuestas del IETF y de grupos de trabajo centrados en desarrollar un IPng (IP next generation).

IPv6 (IPng)

IP "next generation" ha sido el nombre con el que se ha bautizado a la versión seis del protocolo Internet (IP). Se trata de la definición de un nuevo protocolo de red destinado a sustituir a la actual versión IP, la cuatro.

¿Por qué se necesita un nuevo protocolo de red?. La respuesta es muy simple. Cuando IPv4 fue estandarizado, hace unos quince años, nadie podía imaginar que se convertiría en lo que es hoy: una arquitectura de amplitud mundial, con un número de usuarios superior al centenar de millones y que crece de forma exponencial. Aquella primera "Internet" fundada, sobre todo, con fines experimentales, científico-técnicos y, por supuesto, con objetivos militares, no se parece en nada a la actual. Cada día se advierte una mayor

tendencia hacia su comercialización, ya sea por el propio acceso en sí a la red (empresas proveedoras) o por servicios accesibles desde ella.

Estos cambios de escala y orientación suponen varios problemas para IPv4 [RFC1287] [RFC1338] [RFC1917]:

- ***Escala:***

Cada máquina presente en la red dispone de una dirección IP de 32 bits. Ello supone más de cuatro mil millones de máquinas diferentes. Esa cifra, no obstante, es muy engañosa. El número asignado a un ordenador no es arbitrario, sino que depende de una estructura más o menos jerárquica (en especial, pertenece a una red), lo cual ocasiona que se desperdicie una enorme cantidad de direcciones.

- ***Enrutado:***

Existe un límite tecnológico al número de rutas que un nodo puede manejar, y como dado que Internet crece mucho más rápidamente que la tecnología que la mantiene, se vió que las pasarelas pronto alcanzarían su capacidad máxima y empezarían a desechar rutas, con lo que la red comenzaría a fragmentarse en subredes sin acceso entre sí.

¿Por qué cambiar TCP/IP e Internet?

La tecnología básica TCP/IP ha funcionado bien por mucho tiempo. ¿Por qué debería cambiarse? En términos generales, los procesos que estimulan la evolución del TCP/IP y de la arquitectura de Internet son los siguientes:

- *Nuevas tecnologías de comunicación y computación*
- *Nuevas aplicaciones*
- *Incrementos en el tamaño y en la carga*
- *Multiprotocolo*
- *Seguridad*

- *Tiempo Real*
- *Tarificación*
- *Comunicaciones Móviles*
- *Facilidad de Gestión*
- *Política de enrutado*

La evolución de la tecnología TCP/IP está vinculada a la evolución de Internet por varias razones. En primer lugar, Internet es la red de redes del TCP/IP instalada más extensa, de manera que muchos problemas aparecen en Internet antes de que salgan a la superficie en otras redes de redes TCP/IP. En segundo lugar, los investigadores e ingenieros fundadores del TCP/IP provienen de compañías y dependencias gubernamentales que utilizan Internet, de manera que tienden a fundar proyectos que impactan a Internet. En tercer lugar, la mayoría de los investigadores participantes en el TCP/IP tienen conexiones con Internet y la utilizan diariamente. Así pues, tienen una motivación inmediata para resolver problemas que mejorarán el servicio y ampliarán su funcionalidad

Con millones de usuarios en decenas de miles de localidades alrededor del mundo que dependen de la red global de Internet como parte de su ambiente diario de trabajo, puede parecer que Internet es una infraestructura de producción estable. Hemos pasado de las primeras etapas de desarrollo, en las que los usuarios eran también expertos, a una etapa en la cual pocos usuarios comprenden la tecnología. Sin embargo, a pesar de las apariencias, ni Internet ni el conjunto de protocolos TCP/IP son estáticos. Nuevos grupos conectan sus redes y descubren nuevas formas de utilizar la tecnología. Los investigadores resuelven nuevos problemas de redes y los ingenieros mejoran los mecanismos subyacentes. En pocas palabras, la tecnología continúa evolucionando.

La versión 4 del protocolo de Internet () proporciona los mecanismos de comunicación básicos del conjunto TCP/IP y la red global Internet; se ha mantenido casi sin cambio desde su inserción a fines de los años setenta. La antigüedad de la versión 4 muestra que el diseño es flexible y poderoso. Desde el momento en que se diseñó el IPv4, el desempeño de los procesadores se ha incrementado exponencialmente, el tamaño de las memorias se ha

incrementado por un factor de 32, el ancho de banda de la columna vertebral de la red Internet se ha incrementado en un factor de 800, las tecnologías LAN han emergido y el número de anfitriones en Internet ha crecido inconteniblemente. Además, los cambios no ocurren de manera simultánea –el IP se ha adaptado a los cambios de una tecnología antes de adaptarse a los cambios de otras.

A pesar de su diseño, el IPv4 también debe ser reemplazado. El inminente agotamiento del espacio de direcciones. Cuando el IP se diseñó, un espacio de 32 bits era más que suficiente. Sólo un puñado de organizaciones utilizaba las LAN; pocas tenían una WAN corporativa. Ahora, sin embargo, muchas corporaciones de tamaño mediano tienen varias LAN y varias de las grandes corporaciones cuentan con una WAN corporativa. En consecuencia, el espacio de direcciones IP de 32 bits que se usa actualmente no puede adaptarse al crecimiento proyectado de la red global de Internet.

Aun cuando la necesidad de un espacio de direcciones extenso está forzando un cambio inmediato en el IP, hay otros factores que también contribuyen. En particular, gran parte de éstos se refieren al soporte de nuevas aplicaciones. Por ejemplo, debido a que el audio y el video en tiempo real necesitan determinadas garantías en los retardos, una nueva versión del IP debe proporcionar un mecanismo que haga posible asociar un datagrama con una reservación de fuente preasignada. Además, como varias de las nuevas aplicaciones de Internet necesitan comunicaciones seguras, una nueva versión del IP deberá incluir capacidades que hagan posible autenticar al emisor.

El camino hacia una nueva versión del IP

Los grupos en el IETF han estado trabajando para formular una nueva versión del IP por varios años. Como tratan de producir un estándar abierto, el IETF ha invitado a toda la comunidad a participar en el proceso de estandarización. En consecuencia, investigadores, fabricantes de computadoras, vendedores de hardware y software de red, programadores, administradores, usuarios, compañías telefónicas y televisoras por cable han especificado sus requerimientos para la próxima versión IP y han comentado todos sus propuestas específicas.

Se han propuesto muchos diseños para servir a un propósito en particular o a una comunidad en especial. Uno de los diseños propuestos haría al IP más sofisticado y el costo por el incremento en la complejidad de procesamiento se elevaría. Otro diseño propone utilizar una modificación protocolo CLNS de OSI. Un tercer diseño mayor propone conservar la mayor parte de las ideas del IP, y hacer extensiones para adaptarlo a direcciones extensas. El diseño conocido como SIP (Simple IP) ha sido la base para una propuesta extendida que incluye ideas de otras propuestas la versión extendida del SIP ha sido llamada Simple IP Plus (SIPP) y finalmente emerge como el diseño elegido como base para el próximo IP.

Seleccionar una nueva versión del IP no ha sido fácil. La popularidad de Internet hace que el mercado de productos IP alrededor del mundo se tambalee. Muchos grupos consideran esto como una oportunidad económica y tratan de que la nueva versión del IP les ayude a obtener ganancias sobre sus competidores. Además, se han involucrado algunas personalidades --algunas opiniones técnicas individuales se mantienen fuertemente; otros consideran la participación activa como una manera de hacerse promoción. En consecuencia, las discusiones han generado argumentaciones acaloradas.

Nombre del próximo IP

Al comienzo de las discusiones sobre el cambio del IP, el IAB publicó una declaración política que se refería a la próxima versión como IP versión 7, el informe causó una confusión general. La gente preguntaba "¿qué sucedió con la versión 5 y 6?" ¿El IAB se refiere a la versión 5, o se refiere al establecimiento de una política para un futuro a largo plazo. Evidentemente, el error ocurrió por el protocolo ST estaba asignado como la versión número 5 y uno de los documentos disponibles por el IAB reportaba erróneamente a la versión actual como la versión 6.

Para evitar la confusión, el IETF cambió el nombre. Retornando el nombre de una popular serie de televisión, el IETF eligió "IP - la próxima generación" y el esfuerzo comenzó a conocerse como IPng.

Formalmente, se ha decidido que a la próxima versión del IP se le asigne el número de versión 6. Así, para distinguirlo de la versión actual del IP (), la próxima generación se llamará IPv6.

En definitiva, el IPv6 se esta convirtiendo en una realidad, pero todavía queda un largo trecho hasta que se implante de forma mayoritaria, pero sin duda incorpora numerosas características que lo hacen atractivo, como el soporte de comunicaciones en tiempo real, la auto configuración de sistemas, seguridad, etc.

7. HIPÓTESIS:

El proceso de migración de una red IPv4 hacia una red IPv6 puede ser optimizado con el estudio de la tecnología que se esta desarrollando reduciendo el impacto en las aplicaciones y elementos activos de la red

8. METODOLOGÍA:

Para la recopilación de la parte teórica de este trabajo usaremos las técnicas de recopilación de datos de la investigación científica que permite un desarrollo estructurado y cronológico. Los datos serán recogidos de libros, revista e Internet.

Se hará una investigación detallada de la fundamentación teórica del protocolo, sus conceptos fundamentales.

Se recopilará información sobre las aplicaciones y los proyectos que se llevan a cabo en torno a este protocolo.

Revisaremos el impacto sobre los elementos activos, protocolos y software, los cambios que necesiten, o si es transparente al usuario.

Se hará un estudio de las formas de implementación del protocolo en diferentes plataformas.

Para la implementación se escogerán las herramientas más adecuadas luego de hacer un análisis de las que están disponibles en el mercado local. Si es posible se buscará la asignación de una dirección IP de la versión 6, o la posibilidad de formar un túnel con alguno de los nodos IPv6 que están realizando pruebas del protocolo.

Se desarrollara el proyecto siguiendo las etapas del ciclo de vida del desarrollo de proyectos computacionales.

Por último se realizará la documentación buscando que sea de utilidad para los usuarios de la nueva generación de Internet.

9. TABLA DE CONTENIDOS:

CAPITULO 3: TRANSICION DE IPv4 A IPv6

3.1 Mecanismos de transición
3.2 Stacks dobles
3.3 Túneles
3.4 Comparativa IPv4 frente a IPv6

CAPITULO 4: CONFIGURACION DE UNA ISLA IPv6.

4.1 Marco teórico
4.2 Análisis sobre requerimientos, procedimientos y propósitos específicos
4.3 Selección de herramientas software.
4.4 Diseño de la red
4.5 Desarrollo de la red
4.6 Prueba del funcionamiento
4.7 Conexión al 6bone
4.8 Evaluación

CAPITULO 5: CONCLUSIONES Y RECOMEDACIONES

5.1 Comprobación de la hipótesis
5.2 Conclusiones
5.3 Recomendaciones

ANEXOS
GLOSARIO
BIBLIOGRAFIA.