

# “CODAREC6: Transición. Implementación de Tunnel Broker”

**Carlos Taffernaberry, Gustavo Mercado, Santiago Pérez y Raúl Moralejo**

grupo UTN GridTics  
Departamento de Electrónica  
Universidad Tecnológica Nacional - Facultad Regional Mendoza  
Mendoza, 5500, Argentina  
{carlos\_taffe,gmercado,santiagocp,rmoralejo}@frm.utn.edu.ar  
[www.gridtics.frm.utn.edu.ar](http://www.gridtics.frm.utn.edu.ar)

## Abstract

Despite the fact that the current Internet Protocol -known as IPv4- has successfully served for more than 25 years, it is nowadays reaching its own design limits, showing itself unable to provide an adequate response to actual desirable features.

In 1995 the Internet Engineering Task Force (IETF) started developing a new Internet protocol, call IPV6, to replace the older one, that contemplates improvements fundamentally in addressing space, and new required functionalities.

Nowadays millions of host are interconnected using Ipv4 and it's impossible switch to IPv6 immediately and simultaneous in every host. The IETF has defined a set of mechanisms to do the transition, but they need to be evaluated .

This work enumerates the tools and mechanisms available to do a smooth transition tho the new protocol. Finally is explained in detail the implementation in the “Codarec6 Test Bed” a described mechanism, the Tunnel Broker.

**Keywords:** Internet, IP Protocol, Advance Networks, Internet2, Tunnel Broker

## Resumen

La Internet actual utiliza un protocolo de comunicaciones, conocido como IPv4; ha funcionado con éxito por más de 25 años pero hoy está al límite de su diseño, principalmente por el agotamiento de la cantidad de direcciones IP disponible. En 1995 el Internet Engineering Task Force (IETF) desarrolló un nuevo protocolo de Internet para su reemplazo. Este nuevo protocolo, denominado IPv6, fundamentalmente incrementa el espacio de direcciones, aunque también agrega nuevas funcionalidades requeridas.

Como actualmente millones de máquinas están conectadas a Internet usando IPv4, es imposible realizar el pasaje a IPv6 de forma inmediata y simultánea en todas ellas. Si bien la IETF ha definido un conjunto de mecanismos de Transición, los mismos deben aún ser evaluados en su eficacia y usabilidad.

Por tal motivo, este trabajo hace una enumeración de las herramientas y mecanismos con los que se cuentan para para lograr una transición suave hacia el nuevo protocolo, dependiendo del escenario que se trate. Finalmente se explica con detalle la implementación en el “Codarec6 Test Bed” de uno de los mecanismos descriptos, llamado Tunnel Broker.

**Palabras claves:** Internet, Protocolo IP, Redes Avanzadas, Internet 2, Tunnel Broker

## 1. INTRODUCCIÓN

El protocolo IPv4 comienza a dar señales de debilidad. Después de 20 años, la versión 4 del protocolo de Internet (IP) ya no puede seguir brindando respuestas adecuadas, sobretodo en cuanto al paulatino agotamiento de las direcciones IP disponibles, un proceso que culminará en unos pocos años, al ritmo actual de crecimiento de Internet. Formadas por cuatro grupos de tres números cada uno, las direcciones IP identifican a cada uno de los dispositivos (PC, servidor, PDA, teléfono móvil, electrodomésticos, automóviles...) conectados a la red mundial que forma Internet y permiten que la información enviada llegue efectivamente al destino deseado. Ante el enorme crecimiento de usuarios de Internet, que hoy tienen exigencias distintas a las de hace unos años, las poco más de cuatro mil millones de direcciones en todo el mundo que posibilita el IPv4 se han vuelto insuficientes. [1]

La necesidad de ambientes siempre funcionando ("always-on environments", como Internet residencial a través de accesos de banda ancha, cablemódem, o Ethernet-to-the-Home) para ser contactables, excluye conversiones de direcciones IP. Técnicas de pooling y asignación temporaria y "plug and play", que requieren los dispositivos para el hogar con conexión a Internet, ampliarán los requerimientos de direcciones. [2].

Finalmente en 1992 la Internet Engineering Task Force (IETF), convocó a la comunidad de investigadores para estudiar alternativas superadoras para el IPv4. El resultado llegó en 1995 y se llamó IPv6 (Internet Protocol versión 6) [3]. Si bien por estos días IPv6 es especialmente atractivo para los pioneros en los sectores de redes inalámbricas, de juegos, de uso doméstico, redes de investigación nacional conectadas a nivel mundial, organismos militares y gobierno, una vez estandarizada, entre 2005 y 2008, ofrecerá:

- Direccionamiento extendido: Con 128 bits para la dirección IP, hará innecesario el uso de NAT y direccionamiento privado.
- Calidad de Servicio (Qos): IPv6 puede diferenciar los paquetes de datos como pertenecientes a un flujo particular, y así otorgar un ancho de banda en función de cada necesidad, ya sea para correo electrónico, comunicaciones de voz o videoconferencia.
- Capacidades de autenticación y privacidad: IPv6 emplea como parte integral el entorno de seguridad IPSec, que no está implementado en los hosts del IPv4 en forma nativa.
- Autoconfigurable : en IPv6 los nodos no necesitan ser configurados manualmente.
- Simplificación del formato del encabezamiento: Es más sencillo y su tamaño es fijo. Se han suprimido campos como el checksum, tos y fragmentación, y agregado uno para identificar flujos de datos. Las funciones de los campos eliminados se logran con encabezados de extensión, que permiten incorporar nuevas características al protocolo, como IPSec o movilidad.

Desde hace tiempo en el GridTICs de UTN Mendoza se ha venido trabajando en el protocolo IPv6. Se ha generado el proyecto CODAREC6: IPv6 Test Bed [4], como herramienta para el implementación de redes experimentales IPv6, que se continua con el proyecto actual CODAREC6: Intranet [5], para el estudio de la transición en campus universitarios. Una de las tareas más importantes es la transición del viejo protocolo al nuevo IPv6. Después de varios intentos, algunos de ellos fallidos, para llevar adelante la migración de sistemas, la IETF ha formado el grupo de operaciones, el v6ops [6]. El objetivo del v6ops es llevar adelante y fomentar la transición a IPv6 con aportes de la comunidad de Internet y poniendo el foco en la aspectos operacionales y de seguridad.

En este trabajo se utiliza una versión mejorada del IPv6 Test Bed, como el que se muestra en la Fig: 1.

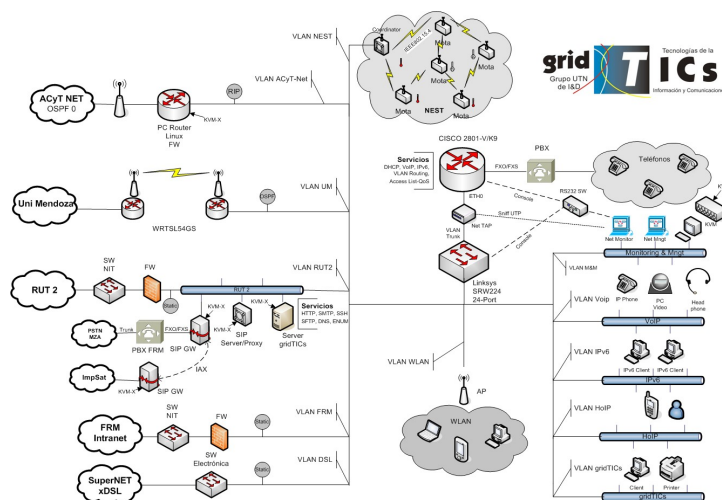


FIGURA 1: CODAREC6: IPV6 TEST BED

## 2. ALTERNATIVAS DE TRANSICIÓN

El soporte de IPv6 está ahora extensamente disponible tanto para la mayoría de los hosts como para routers; ya sea en un nodo sencillo, una red hogareña o en un gran sitio empresarial.

Si se desea tener comunicación con otros sistemas de IPv6, es vital obtener una comunicación con la Internet global IPv6 configurando convenientemente los sistemas locales. Los despliegues de redes solo-IPv6 son raros y la realidad práctica nos muestra que sitios que despliegan IPv6 no hacen la transición directamente a IPv6, sino primero hacen una transición a un estado intermedio donde existen IPv4 e IPv6 (mecanismo de pila dual) [7]. La expansión de la funcionalidad de IPv6 desde una pequeña infraestructura a una red grande puede ser una aventura compleja y difícil. Pero si se planea eficazmente, el despliegue puede hacerse en una manera escalonada y controladamente. Para un sitio grande hay muchos diferentes requisitos y diferentes condiciones, lo que hace necesario emplear varios mecanismos de transición según las peculiaridades de, por ejemplo, una subred dada, ambiente inalámbrico o móvil, una tecnología dial-in, etc. [8]

### 2.1. Pila Dual (Doble Stack)

Uno de las maneras conceptualmente más fáciles de introducir IPv6 en una red, es el denominado "mecanismo de pila dual" [9]. Por este método un host o un router estarán provistos con ambas pilas de protocolos, IPv4 e IPv6, en el sistema operativo. Cada nodo, denominado "nodo IPv4/IPv6", se configura con ambas direcciones IPv4 e IPv6. Por consiguiente los dos envían y reciben datagramas que pertenece a ambos protocolos y así podrán comunicarse con cada nodo IPv4 e IPv6 en la red. Ésta es la manera más simple y deseable de coexistencia y es, en general, el próximo paso en la evolución, antes de una transición más profunda, hacia una Internet mundial solo IPv6.

Un desafío en el despliegue de una red IPv6/IPv4 con pila dual, es la configuración del ruteo tanto externo como interno para ambos protocolos. Si se ha estado usando OSPFv2, por ejemplo, se debería hacer la transición a un protocolo que sea capaz de rutear ambos protocolos IPv4 e IPv6 como IS-IS u OSPv3 en vez de OSPFv2.

### 2.2. Túneles

Para crear redes IPv6, las técnicas de Túneles operan sobre la infraestructura disponible de IPv4 sin tener que hacer cambios en el ruteo IPv4 ni en los routers. Este método se usa a menudo donde la infraestructura completa - o parte de ella - no es todavía capaz de ofrecer la funcionalidad de IPv6 nativa. Por consiguiente el tráfico de IPv6 tiene que cruzar la red IPv4 existente, lo cual es posible con varias técnicas del tunnelling. Estas técnicas son a menudo escogidas como un primer paso

probar el nuevo protocolo y empezar integración de IPv6.

Tunnelling, llamada también encapsulación, es un proceso por el que la información de un protocolo se encapsula dentro del paquete de otro protocolo, permitiendo llevar así los datos originales encima del segundo protocolo. El proceso de túnel involucra tres pasos: encapsulación, desencapsulación y administración del túnel. Se requiere dos extremos del túnel, los cuales son generalmente nodos de pila dual IPv4/IPv6 (normalmente routers), que se ocupan de la encapsulación y la desencapsulación. Un túnel puede configurarse de cuatro maneras diferentes: [10]

1. De router a router, que extiende un segmento de la ruta de extremo a extremo entre dos host. Éste probablemente es el método más común.

2. Host a router, que extiende el primer segmento de la ruta de extremo a extremo entre dos host, tal como puede encontrarse en un tunnel broker.

3. Host to Host, lo cual es la ruta completa extremo a extremo entre dos host.

4. Router a host, que extiende el último segmento de la ruta de extremo a extremo entre dos host. Dependiendo de qué tipo se use, un túnel podría ser "configurado" (ambos lados necesitan ser configurados de acuerdo), "semi-configurado" (sólo un extremo tiene que ser configurado, los otros lados actúan como pasarelas) o "automático" dónde casi nada necesita ser hecho.

### 3. DESCRIPCIÓN DETALLADA DE LOS MECANISMOS Y HERRAMIENTAS

En este capítulo se detallarán los diferentes mecanismos de transición para los escenarios de "pila dual" y "técnicas de túnel".

#### 3.1. Pila Dual (Doble Stack)

Como se mencionó anteriormente no hay mecanismos de transición involucrados, pues los host ya tienen integrado IPv6. Para construir un nodo de pila dual, solo es necesario habilitar en el Sistema Operativo el soporte IPv6. [11]

De esta manera el nodo se convierte en un nodo "hibrido" y dependiendo de la resolución de

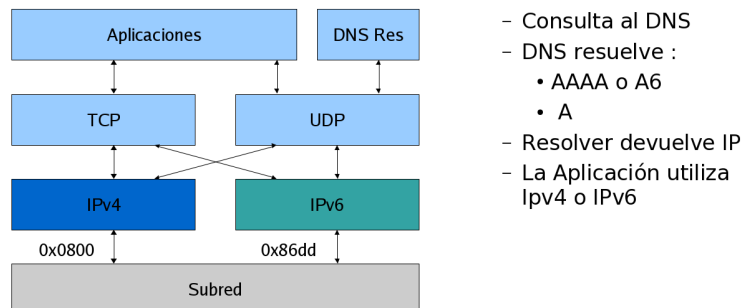


Figura 2: Detalle de funcionamiento de Pila Dual

nombres será el protocolo que usará para cada requerimiento en particular. De acuerdo a lo mostrado en la Figura 2

Un backbone se dice que es de pila dual si todos los routers y switches capa 3 pueden manejar tanto IPv4 como IPv6.

#### 3.2. Implementación de Túneles

Esta sección describe los métodos para transportar IPv6 sobre redes IPv4 existentes, lo que trae aparejado algún tipo de mecanismo de túneles.

##### 3.2.1. Túneles Configurados

Los túneles configurados se definieron en [11] como túneles IPv6-sobre-IPv4. Éste tipo de túneles

son punto a punto y deben ser configurados manualmente en los dos extremos. Si bien es más tediosa la configuración, pues deben intervenir los administradores de ambos extremos, a la hora de controlar las rutas y reducir ataques de denegación de servicio son más convenientes que los túneles automáticos. Debido a que en la actualidad no hay demasiados proveedores que ofrezcan conectividad IPv6, si se tiene posibilidad de tener conectividad hacia un sitio ya conectado a IPv6, una forma muy estable y segura es que el tráfico IPv6 sea encaminado por este tipo de túneles. Como deben ser configurados manualmente, es recomendable no usar demasiados. Si se desea conectar muchos host dual stack para darles acceso a IPv6, hay otros métodos específicamente diseñados, como tunnel brokers, 6to4, Teredo o ISATAP (los cuales se detallan a continuación). Se detalla en la Figura 3 el acceso a IPv6 que tenía el “Codarec6” en los primeros tiempos, a través de la UTN regional La Plata. [4]

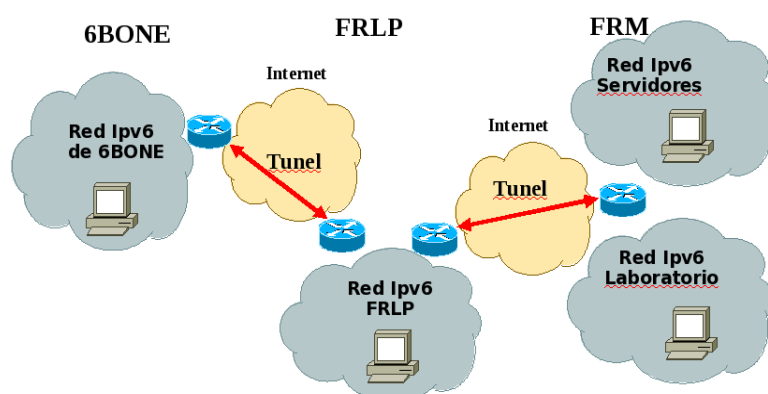


Figura 3: Acceso a 6Bone de Codarec6

### 3.2.2. Tunnel Brokers

En lugar de configurar manualmente cada extremo de los túneles, es posible correr scripts para automatizar la tarea. Esta alternativa "automática" se denomina tunnel broker [12]. La filosofía básica de los tunnel broker es permitir al usuario que ese conecte a una página web, opcionalmente que ingrese datos de autenticación y recibir un script que deberá correr en su host para establecer un túnel IPv4-IPv6 contra el servidor del tunnel broker.

El proveedor del servicio necesita brindar un servicio de web en IPv4 y un router de pila dual capaz de aceptar comandos de configuración automáticos para crear los nuevos túneles hacia los host remotos de los clientes. Esto es posible hacerlo en una sola máquina.

El requerimiento principal para este servicio es saber que túnel pertenece a que usuario.

Los Tunnel brokers deberían poder usarse para conectar hosts de pila dual aislados o para conectar redes enteras. En este último caso, el host que obtenga el túnel debería ser en realidad un Router con soporte IPv6.

Un tunnel broker es una importante ayuda para la transición; habilita fácilmente el acceso a redes IPv6, y en la actualidad existen varios sitios que ofrecen acceso a estos servicios. A la hora de elegir un servicio de tunnel broker, es importante la cantidad de saltos o hops hasta el mismo, pues todos los paquetes traficados con IPv6 tendrán adicionada esa demora; por lo que es importante seleccionar tunnel brokers nacionales.

### 3.2.3. Túneles Automáticos

Este tipo de mecanismo de túnel fue uno de los primeros en desarrollarse, pero también uno de los primeros en ser reemplazado por otros métodos más sofisticados. Usa como extremos del túnel direcciones IPv6 del tipo IPv4-compatible. [13]

La dirección del nodo destino está especificada en el paquete que está siendo encapsulado por el túnel. Debido a esto, este método solo puede ser usado en comunicaciones host-a-host o router-a-host, pues son los únicos esquemas en los que el nodo destino también es el extremo del túnel. Esta es la causa de que solo funcione para túneles IPv6 over IPv4 y no en sentido inverso.

Si bien el mecanismo no es obsoleto, se recomienda seleccionar otras soluciones como ISATAP o 6to4. Una de las causas se basa en que la conectividad que resulta de estos túneles carece de una estructura en el dominio IPv6.

#### 3.2.4. Túnel 6to4

Este mecanismo de transición [10] es una forma de túneles router-a-router que utiliza un prefijo asignado por IANA (2002::/16) para designar los sitios participantes en la técnica 6to4.

Permite que dominios IPv6 aislados se comuniquen con otros dominios IPv6 con una mínima configuración. Un sitio IPv6 aislado se asignará a si mismo una dirección global con prefijo 2002:ADDR\_IPv4::/48, donde ADDR\_IPv4 es la dirección global IPv4 configurada en la interfase de salida del router de acceso a Internet.

Este prefijo tiene exactamente el mismo formato que un prefijo normal /48, y por ello permite a un dominio IPv6 usarlo como cualquier otro prefijo /48 válido. En un escenario en donde dominios 6to4 quieren comunicarse entre si, no es necesaria la configuración explícita de los túneles. Las direcciones IPv4 de los extremos del túnel son determinados al extraerlos del prefijo global IPv6 de la dirección destino del paquete IPv6 a transmitir. Adicionalmente, los routers 6to4 no necesitan correr ningún protocolo de enrutamiento IPv6, pues el enrutamiento IPv4 es el encargado de realizar la tarea. Se puede ver en la Figura 4 los aspectos descriptos.

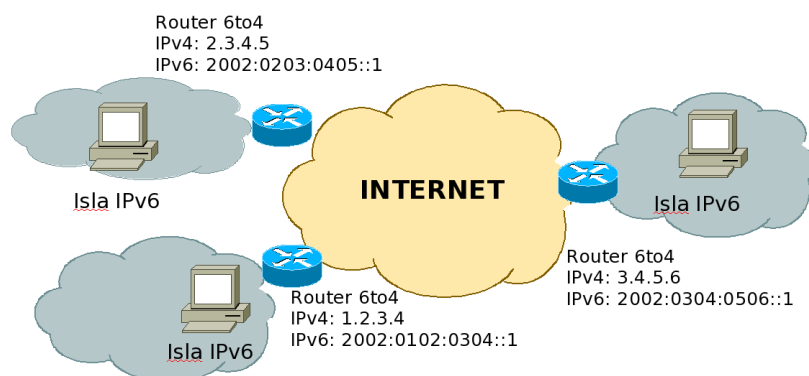


Figura 4: Direcciones IPv6 de routers 6to4

Ahora, cuando los dominios 6to4 desean comunicarse con dominios IPv6 nativos, la situación se vuelve más compleja. En este caso, la conectividad entre los dominios es manejada por medio de routers relays, que son esencialmente routers que tienen como mínimo una interfase del tipo 6to4 y al menos una interfase con dirección IPv6 nativa. A diferencia del escenario previo, se debe usar un protocolo de ruteo exterior IPv6. Un router relay publica el prefijo 2002::/16 en su ruteo IPv6 nativo y adicionalmente, puede publicar rutas IPv6 nativas en su interfase 6to4.

Los routers relay pueden ser descubiertos usando anycast para IPv4 [13].

El uso más común del mecanismo 6to4 es para routers IPv6 de borde. Otros métodos como ISATAP o direccionamiento nativo IPv6 pueden ser usados dentro del sitio.

#### 3.2.5. Túnel 6 over 4

Los túneles 6over4, [14], interconectan host IPv6 aislados en un sitio por medio de una encapsulación IPv6-in-IPv4 sin explicitar túnel alguno. Usa las direcciones IPv4 como identificador

de interfaces y crea un enlace virtual usando un grupo multidifusión IPv4 con alcance local. Este método no es de los favoritos, debido a varias razones, incluyendo entre las principales el escaso soporte de multidifusión en los sitios y en los ISP.

Existen un pequeño número de implementaciones como las realizadas por 3Com y Cisco, pero prácticamente sin adopciones en el mercado, por lo que hace poco recomendable su uso.

### 3.2.6. *Tunnel ISATAP*

Una alternativa a los túneles 6over4 son los túneles ISATAP (Intra-Site Automatic Tunnel Addressing Protocol) [15].

ISATAP también utiliza la infraestructura IPv4 como enlace virtual, pero no hace uso de multidifusión, por lo que el enlace es NBMA (Non-Broadcast Multiple Access).

ISATAP, al igual que 6over4, crea un identificador de interfase basado en la dirección IPv4 de la interfase. Las direcciones en ISATAP pueden ser configuradas manual o automáticamente, pero la dirección IPv4 de la interfase debe estar embebida en los últimos 32 bits de la nueva dirección IPv6. Al igual que 6over4, la dirección IPv4 debe ser única, y si es usada para acceder a Internet, debe ser global.

Como la dirección IPv4 siempre está embebida en la dirección IPv6, la resolución de direcciones es trivial. Se debe tener en cuenta que para que funcionen las router solicitations, el host debe haber aprendido de alguna manera las direcciones IPv4 de los posibles routers ISATAP (por DHCP, DNS, TEP, configuración manual etc), y enviará entonces solicitaciones de manera unicast. El router siempre envía advertisements de manera unicast y solo como respuesta a la solicitud del host. Cada host ISATAP enviará regularmente solicitaciones a los routers ISATAP que conozca. ISATAP se ha implementado en algunas plataformas como Windows XP y Cisco IOS [16], aunque se sacó de la pila dual de USAGI para Linux.

### 3.2.7. *Túnel Teredo*

Teredo, también conocido como un traslado de direcciones de red (NAT) para IPv6, se diseñó para que hosts IPv4 obtengan direcciones IPv6 a través una o más capas de NAT [17] creando túneles sobre el protocolo UDP. Este es un mecanismo de túneles automáticos de host a host que provee conectividad IPv6, mientras que los hosts dual stack se ubican detrás de uno o más NATs, por encapsulamiento de paquetes IPv6 en mensajes UDP de IPv4. Teredo usa dos entidades: un Server Teredo y un Relay Teredo. El Server escucha requerimiento de los clientes en el puerto 3544 del protocolo UDP, respondiendo con una dirección IPv6 para que la usen. Las direcciones Teredo tienen la siguiente estructura: Prefijo Teredo (32 bits) : Dirección IPv4 del Servidor Teredo : Flags (16 bits) : Puerto externo (16 bits) : Dirección externa (32bit).

El método reenvía paquetes IPv6 (con IPv4 encapsulado) enviados desde el cliente al Teredo Relay, y también redirige los paquetes recibidos desde el Teredo Relay. Esta técnica es por lejos una herramienta de “último recurso”, solo diseñada para cuando ningún otro método funcione. El método usado por Teredo es complejo, y no se puede garantizar que trabaje correctamente debido a la gran cantidad de distintas implementaciones de NAT.

## 4. **IMPLAMENTACIÓN DE UN TUNNEL BROKER**

### 4.1. **Objetivos**

El objetivo principal que nos llevó al desarrollo de un tunnel broker [12] fue permitir a usuarios con dual stack (ipv6 e ipv6) poder acceder a redes ipv6, sin que sea necesario configurar entre ellos y nuestro router un túnel manual del tipo IPv6 sobre IPv4.

### 4.2. **Esquema General**

En la Figura 5 se muestra el esquema general del funcionamiento de nuestro Tunnel Broker.

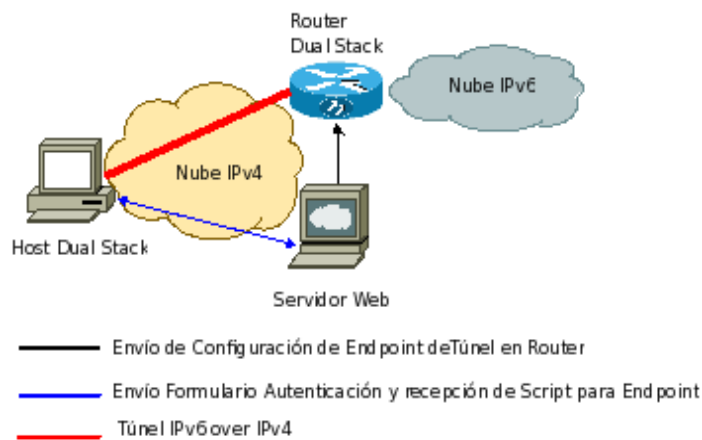


Figura 5: Esquema de funcionamiento

Básicamente la aplicación se dividió en dos componentes:

#### 4.2.1. Servidor Web:

Utilizado para el intercambio de información entre el usuario en el Host Dual Stack y el servicio de Broker. La función se realizó con un servidor http, implementado sobre sistema operativo Gnu/Linux [18] y aplicación Apache[19] con módulos de extensión de lenguaje PHP.

Las tareas que realiza son:

- Autenticación de usuarios o alta de nuevos usuarios, almacenando la información en el sistema de archivos.
- Visualización de túneles existentes para el usuario previamente autenticado.
- Creación de nuevos túneles, permitiendo seleccionar al usuario el tipo de Sistema Operativo de su extremo del Túnel y si será un Túnel Host-to-Host o Host-to-Net.
- Envío de script a Router dual Stack via ssh para creación o baja de túnel.
- Envío de script al cliente, para que éste lo ejecute (el script variará en función de la previa elección de su Sistema Operativo).

#### 4.2.2. Router Dual Stack:

Encargado de crear, modificar o borrar el endpoint en el router del Túnel IPv6 over IPv4 contra el host dual stack del cliente.

El router fue implementado sobre sistema operativo GNU/Linux, y los scripts realizados en bash scripting[20].

En la Figura 6 se muestra el código principal para el manejo de los túneles.

```
#!/bin/sh
unset PATH
IPTUNNEL=/sbin/iptunnel
IFCONFIG=/sbin/ifconfig
ROUTE=/sbin/route
IP=/sbin/ip
BASENAME=/bin/basename
NAME=$2
IPV4_REMOTE=$3
IPV6_LOCAL=$4
IPV6_REMOTE=$5
```

```

case $1 in
  "up")
  (
    $IPTUNNEL add $NAME mode sit remote $IPV4_REMOTE &&
    $IFCONFIG $NAME up &&&
    $IFCONFIG $NAME add $IPV6_LOCAL/128 &&&
    $ROUTE -A inet6 add $IPV6_REMOTE/128 dev $NAME
    )2>&1 &&& exit 0 || exit 1
    ;;

  "down")
  (
    $ROUTE -A inet6 del $IPV6_REMOTE/128 &&&
    $IFCONFIG $NAME del $IPV6_LOCAL/128 &&&
    $IFCONFIG $NAME down &&&
    $IPTUNNEL del $NAME
    )2>&1 &&& exit 0 || exit 1
    ;;

  "status")
    $IFCONFIG $NAME &> /dev/null &&& exit $?
    ;;

  "stats")
    $IP -s tun lis $NAME &&& exit $?
    ;;

  *)
    echo "USO: $($BASENAME $0) (up|down|status|stats) NAME IPV4_REMOTE
IPV6_LOCAL IPV6_REMOTE"
    exit 1
    ;;

esac

```

Figura 6: rutina principal de manejo de túneles

### 4.3. Ensayos

Para realizar el ensayo, se necesitó un host dual Stack con conectividad a Internet y un cliente Web.

#### 4.3.1. Creación de usuario

En el cliente Web se escribió la URL <http://codarec.frm.utn.edu.ar/tunnel/> . Se seleccionó “Si es un nuevo usuario haga Click Aquí”, y se llenó el formulario de registración , como muestra la Figura 7.

The screenshot shows a Mozilla Firefox browser window displaying a registration page. The form contains the following data:

- Usuario: carlos.tafernaberry
- Contraseña: [masked]
- email: carlos\_taffe@frm.utn.edu.ar
- Buttons: "Crear cuenta" and "Volver"

Figura 7: Creación de Usuario Nuevo

### 4.3.2. Creación de Túnel

Una vez que accedió, se seleccionó “Nuevo Túnel”, desplegando un formulario con los datos solicitados, como lo muestra la Figura 8.

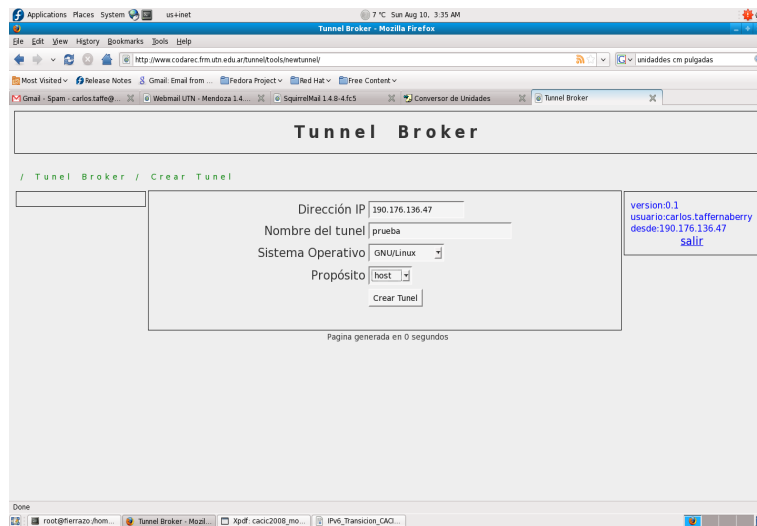


Figura 8: Creación de nuevo Túnel.

### 4.3.3. Ejecución de script de arranque de endpoint local

El punto anterior creó el endpoint del Túnel en el router del Codarec6. Solo restaba crear el endpoint local, siguiendo las instrucciones que aparecen al hacer click en “Enviar Script”, como muestra la Figura 9.

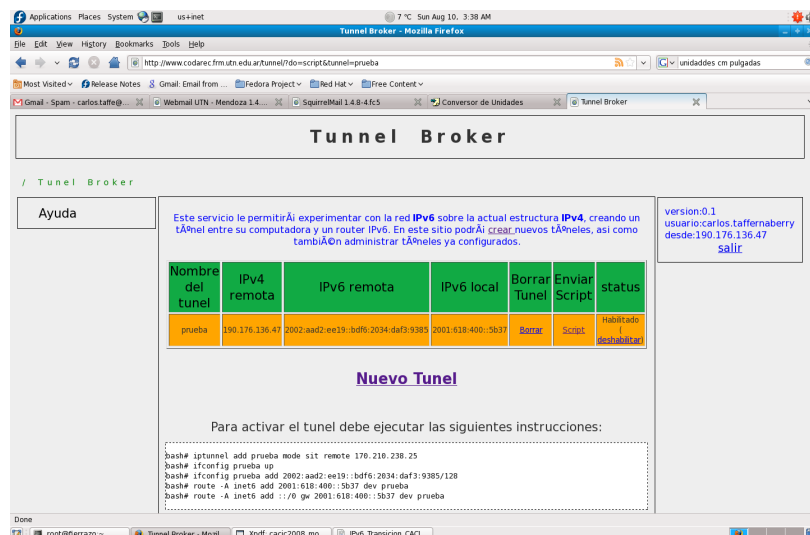


Figura 9: Instrucciones para ejecutar localmente

### 4.3.4. Acceso a la nube IPv6

Se verificó la creación de la nueva interfase y la asignación de la dirección con prefijo global. Finalmente se verificó el acceso a IPv6 por medio del Túnel Broker, como lo demuestra la Figura 10.

```
$ ifconfig prueba
prueba  Link encap:IPv6-in-IPv4
        inet6 addr: fe80::ac04:2/64 Scope:Link
        inet6 addr: 2002:aad2:ee19:0:bd6:2034:daf3:9385/128 Scope:Global
        inet6 addr: fe80::beb0:882f/64 Scope:Link
        UP POINTOPOINT RUNNING NOARP MTU:1480 Metric:1
        RX packets:0 errors:0 dropped:0 overruns:0 frame:0
        TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:0
        RX bytes:0 (0.0 b) TX bytes:0 (0.0 b)

$ ping6 www.deepspace6.net
PING www.deepspace6.net(2001:760:2e01:1::dead:beef) 56 data bytes
64 bytes from 2001:760:2e01:1::dead:beef: icmp_seq=0 ttl=56 time=314 ms
64 bytes from 2001:760:2e01:1::dead:beef: icmp_seq=1 ttl=56 time=313 ms
64 bytes from 2001:760:2e01:1::dead:beef: icmp_seq=2 ttl=56 time=313 ms
64 bytes from 2001:760:2e01:1::dead:beef: icmp_seq=3 ttl=56 time=313 ms
64 bytes from 2001:760:2e01:1::dead:beef: icmp_seq=4 ttl=56 time=315 ms
www.deepspace6.net ping statistics ---
5 packets transmitted, 5 received, 0%
 packet loss, time 18636ms
rtt min/avg/max/mdev = 313.162/313.875/
315.087/0.856 ms, pipe 2
```

Figura 10: Verificación de acceso

#### 4.4. Mejoras Propuestas

Como se mencionó previamente, no se utilizó una base de datos para almacenar la información de autenticación de los clientes. Una mejora planteada es adicionar, al código realizado, un módulo de PHP para interactuar directamente con alguna base de datos. Un ejemplo de esto es php-mysql o php-postgres, para interactuar con Mysql o Postgresql respectivamente [21].

Otro aspecto a mejorar está referido a que muchos clientes, por el servicio que les provee su ISP, tienen una dirección IPv4 dinámica. Por lo tanto, cada vez que dicha dirección cambie, deberán crear un túnel nuevo con su nueva dirección. Una alternativa propuesta es hacer que cada vez que el usuario se autentique se verifique desde que dirección IPv4 lo está haciendo. Si la misma es distinta a la que se configuró mediante el formulario, se borre la configuración actual del túnel en el Broker y se cree una nueva, todo esto de forma automática, de modo que el usuario solo deba ejecutar el script para la configuración de su extremo local.

#### 5. CONCLUSIONES

Tarde o temprano Internet migrará inevitablemente a su versión IPv6. El presente trabajo pretende ser una guía del abanico de herramientas o métodos disponibles en la actualidad para su Transición. Dependiendo de la necesidad, es el método recomendable para implementar.

No están incluidos en el presente los pasos o consideraciones para migrar la red local LAN a IPv6, que es una etapa que debe ser realizada previamente.

Se puede concluir que la implementación de un Túnel Broker permite ayudar a usuarios finales para rápidamente entrar en el mundo IPv6. Así lo demuestra nuestra experiencia llevada a cabo en el laboratorio de IPv6 denominado CODAREC6. Esto hace que no sea necesario esperar que los proveedores ISP den conectividad nativa a IPv6 para poder utilizarla.

Por último creemos que el presente trabajo y el trabajo que lleva a cabo el grupo GridTics, contribuye a la capacitación, difusión y formación de recursos humanos para afrontar en inminente cambio al protocolo de Internet versión 6 en la región.

#### 6. REFERENCIAS

- [1] Robert L. Fink "IPv6—What and Where It Is", The Internet Protocol Journal, Volume 2, Number 1, March 1999.
- [2] Douglas E. Comer "Redes Globales de Información con Internet y TCP/IP", Pearson PH, Tercera Edición, 1996, ISBN 0-13-219687.
- [3] S. Deering y R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification," RFC 2460, December 1998.
- [4] C. Taffernaberry, A. Dantiacq Piccolella, G. Mercado y A. Francisconi "CODAREC6: AN IPv6 TEST BED", XII CACIC, Octubre 2006, Potrero de los Funes, San Luís.
- [5] G. Mercado, C. Taffernaberry, A. Dantiacq Piccolella, S. Pérez, J. J. Ciarlante, R. Moralejo, "Diseño y simulación de la implementación de tecnologías y procedimientos de transición del protocolo IPv6 en INTRANETS usando un `IPv6 test bed`", IX WICC 2007, Mayo 2007 - TRELEW - CHUBUT – ARGENTINA.
- [6] IPv6 Operations (v6ops) <http://www.ietf.org/html.charters/v6ops-charter.html>
- [7] Pete Loshin "IPv6: Theory, Protocol and Practice", Morgan Kaufmann, Segunda Edición, 2004, ISBN 1-55860-810-9.
- [8] T. Chown, "IPv6 Campus Transition Scenario Description and Analysis", Internet-Draft, March 2007.
- [9] R. Gilligan, E. Nordmark, "Transition Mechanisms for IPv6 Hosts and Routers", RFC 2893, August 2000.
- [10] B. Carpenter, K. Moor, B. Fink, "Connecting IPv6 Routing Domains Over the IPv4 Internet", IPJ, March 2000 Volume 3, Number 1
- [11] S. Roy, J. Paugh, A. Durand, "Issues with Dual Stack IPv6 on by Default", Internet-Draft, July 2004.
- [12] A. Durand, P. Fasano, I. Guardini, D. Lento, "IPv6 Tunnel Broker", RFC 3053, January 2001
- [13] C. Huitema, "An Anycast Prefix for 6to4 Relay Routers", RFC 3068, June 2001.
- [14] B. Carpenter, C. Jung "Transmission of IPv6 Packets over IPv4 Domains without Explicit Tunnels (6over4)", RFC 2529, March 1999.
- [15] F. Tremplin, T. Gleeson, M. Talwar, D. Thaler, "Intra-Site Automatic Tunnel Addressing Protocol (ISATAP)", RFC 4214, Octubre 2005.
- [16] JOIN - The IPv6 project at the Center for Information Processing, [http://www.join.uni-muenster.de/Dokumente/Howtos/Howto\\_ISATAP](http://www.join.uni-muenster.de/Dokumente/Howtos/Howto_ISATAP).
- [17] C. Huitema. "Teredo: Tunneling IPv6 over UDP through Network Address Translations (NATs)", RFC 4380, February 2006.
- [18] Richard Stallman, "Linux and the GNU Project" <http://www.gnu.org/gnu/linux-and-gnu.html>, March 2008.
- [19] Nick Kew, "The Apache Modules", 1 edition . Prentise Hall, February 2007.
- [20] Arnold Robbins and Nelson Beebe "Classic Shell Scripting", 1 edition, O'Reilly - ISBN: 9780596005955. May 2005.
- [21] Jason Gilmore and Robert Treat, "Beginning PHP and PostgreSQL 8", 1 edition - Apress , June 2006.