PONTIFICIA UNIVERSIDAD CATÓLICA DE VALPARAÍSO
FACULTAD DE INGENIERÍA
ESCUELA DE INGENIERÍA INFORMÁTICA

Implementación de IPv6 con seguridad en el segmento de red de la Escuela

Alexis Guillermo Abarca Hidalgo
Matías Gastón Arancibia Yudiche

INFORME FINAL DEL PROYECTO
PARA OPTAR AL TÍTULO PROFESIONAL DE
INGENIERO DE EJECUCIÓN EN INFORMÁTICA

Diciembre, 2012

PONTIFICIA UNIVERSIDAD CATÓLICA DE VALPARAÍSO
FACULTAD DE INGENIERÍA
ESCUELA DE INGENIERÍA INFORMÁTICA

Implementación de IPv6 con seguridad en el segmento de red de la Escuela

Alexis Guillermo Abarca Hidalgo
Matías Gastón Arancibia Yudiche

Carrera: Ingeniería de Ejecución en Informática

Profesor guía: Iván Mercado Bermudez

Diciembre, 2012

Agradezco con cariño la realización del presente trabajo a mis padres Vilma y Gastón, a mi polola Solange y a mi compañero Alexis, por la ayuda y apoyo de todos ellos en todo momento. Agradezco también a nuestro profesor Iván Mercado por toda su ayuda en la realización del presente informe.

Gracias a mis padres Patricia y Guillermo, junto a mi compañero Matias y mis amigos que me brindaron el apoyo y ayuda necesaria para completar este informe de Proyecto. Agradezco también el apoyo de la Universidad brindado por el profesor Iván Mercado y la DSIC quien proporcionó conectividad IPv6 nativa.

Resumen

El presente informe trata sobre la factibilidad de implementar IPv6 en la Escuela de Ingeniería Informática de la PUCV, llevando a cabo como primera medida la descripción de qué es esta nueva versión (IPv6) del protocolo IP, cómo funciona y las diferencias que posee dicha versión en comparación al actual utilizado IPv4.
Para comprobar si el cambio es factible se investigó la situación actual de IPv4 en la Escuela y se llevaron a cabo múltiples pruebas y pequeños prototipos con el fin de llegar a una conclusión y corroborar si es realmente conveniente realizar la migración de IPv4 a IPv6 en este momento. También se discutió sobre el método de seguridad más apropiado que ofrece Wifi actualmente utilizando IPv4, y según la investigación realizada se concluyó que por motivos técnicos se usará el Portal Cautivo. Posteriormente se probó la compatibilidad de los servicios que se utilizan en la Escuela con esta nueva versión del protocolo IP.

Palabras Claves: IPv6, seguridad Wifi.

Abstract

This report discusses the feasibility of implementing IPv6 in the School of Computer Engineering of the PUCV, performing as a first step description of what is this new version (IPv6) of the IP protocol, how it works and the differences that have that version compared to the currently used IPv4. To check if the change is feasible we investigated the current status of IPv4 and performed multiple tests and small prototypes in order to reach a conclusion and confirm if it is really convenient to migrate from IPv4 to IPv6 at this time. They also discussed the appropriate method of security offered by Wireless currently using IPv4, and according to research concluded that this method corresponds to captive portal by technical reasons. Then we tested the compatibility of the services utilized in school with the new version of IP protocol.

Keywords: IPv6, Wifi security.

Índice

1. Introducción **1**
1.1. Objetivos . . . 3
1.2. Objetivos específicos . . . 3
1.2.1. Actividades . . . 3
1.2.2. Riesgos . . . 4

2. IPv6 **7**
2.1. Definición . . . 7
2.2. Características . . . 7
2.3. Tipos de direccionamiento . . . 9
2.3.1. Configuración automática sin estado . . . 9
2.3.2. DHCPv6 . . . 10

3. Situación actual del protocolo IP **13**
3.1. En el mundo . . . 13
3.2. En Chile . . . 15
3.3. En la universidad . . . 17
3.4. En la escuela de informática . . . 18

4. Seguridad WLAN **19**
4.1. WEP . . . 19
4.2. WPA2-Personal . . . 20
4.3. Portal cautivo . . . 21
4.4. WPA2-Enterprise . . . 22

5. Soporte de IPv6 en dispositivos y sistemas ope-rativos **23**

6. Pruebas de implementación **26**
6.1. Conectividad IPv6 . . . 26
6.1.1. pfSense . . . 27
6.1.2. Mikrotik . . . 30
6.1.3. Ubuntu Server . . . 33
6.2. Seguridad Wifi . . . 36
6.2.1. WPA2-Enterprise . . . 36
6.3. Pruebas y criterios de comparación . . . 38

7. Pruebas de servicios **40**
7.1. Compatibilidad servicios 40
7.1.1. VPN 41
7.1.2. RADIUS 41
7.1.3. Portal cautivo 41
7.1.4. LDAP 42
7.1.5. Proxy 42
7.1.6. HTTP 43
7.1.7. PostgreSQL 43
7.1.8. NFS 43
7.1.9. MySQL 44
7.1.10. SAMBA 44
7.1.11. SSH 44
7.1.12. Escritorio remoto RDP 45
7.1.13. DNS 45
7.1.14. SMTP/POP3/IMAP 45
7.2. Comparación de rendimiento entre IPv4 e IPv6 46

8. Implementación **48**
8.1. Conversaciones con DSIC 48
8.2. Plan de contingencia 49
8.3. Instalación router IPv6 51
8.3.1. Solución de problemas 55
8.4. Red inalámbrica 56

9. Pruebas IPv6 nativo **58**
9.1. Pruebas LAN 58
9.2. Pruebas WAN 58
9.3. Análisis de resultados 59

10. Conclusiones **60**

Lista de Figuras

1. Topología de red probada del plan de contingencia. 5
2. Definición de un encabezado IPv6 [1]. 8
3. Dirección IP asignada por configuración automática sin estado. 10
4. Paquete *Router Advertisement* desde un router IPv6. 11
5. Asignaciones actuales del DHCPv6. 11
6. Sitio Web de World IPv6 Launch 14
7. Configuración de WPA2 en un AP con firmware DD-WRT . . 20
8. Lista de usuarios activos del portal cautivo. 21
9. Configuración de WPA2-Enterprise en un AP (DD-WRT). . . 22
10. Configuración del túnel en pfSense. 27
11. Configuración LAN en pfSense. 28
12. Asignación IPv6 por DHCPv6 en Windows 7. 28
13. Configuración DHCPv6 en pfSense. 29
14. Configuración LAN en Mikrotik. 30
15. Configuración de la ruta IPv6 en Mikrotik. 31
16. Direcciones IPv6 en Mikrotik. 32
17. Conexión al AP con WPA2-Enterprise en Fedora 17. 37
18. Mensaje de error de Squid 2.X al usar una dirección IPv6 literal. 42
19. Mapa de red Escuela de Informática 50
20. Registro de túnel en Hurricane Electric 52
21. Parámetros del túnel IPv6 con Hurricane Electric 55

Lista de Tablas

1. Adopción de A y AAAA en los distintos TLD 13
2. Prefijos IPv6 en uso en Chile. 16
3. Soporte de IPv6 en los SO más populares. 23
4. Sistemas Operativos que se conectan a la red Wifi. 24
5. Sistemas Operativos Móviles que se conectan a la red Wifi. . . 24
6. Rendimiento IPv6 v/s IPv4 (en segundos). 46
7. Pruebas IPv6 nativo en equipos de la misma LAN 58
8. Pruebas IPv6 nativo hacia Internet 58

1. Introducción

El presente informe da a conocer la factibilidad de la implementación del protocolo IP versión 6 en la red de área local (LAN) de la Escuela de Ingeniería Informática, donde se deben considerar importantes factores como la seguridad de la nueva versión del protocolo en contraste a la actual versión 4 del mismo, la escalabilidad y disponibilidad para los usuarios de la red. El Wifi de la Escuela (`192.168.127.0/24`) inicialmente disponía de la cantidad total de 235 IP's (con los Access Point ya descontados) para proveer a los usuarios que requieran conectarse, sin embargo, el problema surgía cuando éstos últimos no pueden hacerlo dado que la cantidad de IP's disponibles en la misma no daba abasto para cubrir a todos los clientes que deseaban conectarse a Internet, ya que al agotarse las IP's disponibles se comienzan a asignar direcciones duplicadas a los equipos, lo que produce inminentes colisiones y posteriormente la imposibilidad de establecer una conexión satisfactoria. Para dar solución a este problema se incrementó la cantidad de IP disponibles modificando la máscara de red, de `255.255.255.0` a `255.255.240.0`. Como el rango de direcciones del Wifi era privada de clase C, era posible realizar tal cambio sin posteriores inconvenientes.

Sin embargo ésta no es la solución definitiva al problema, debido a que los dispositivos al estar tras un router que hace NAT (*Network Address Translation*) están compartiendo una dirección IP pública, lo que genera problemas en ciertas aplicaciones, además de no poder ser alcanzables directamente desde Internet, y que el router debe mantener una tabla de NAT con las conexiones de todos los clientes para rutearlas de vuelta.

Para dar una solución definitiva al problema mencionado se debe migrar a IPv6, cuya principal ventaja es el espacio de direccionamiento ampliado. Esto elimina la necesidad de usar NAT, entre otras ventajas que serán detalladas en este informe. Para migrar a IPv6 se presentan tres posibles alternativas: la primera consiste en que la Dirección de Servicios de Informática y Comunicaciones en la Casa Central (DSIC) de la universidad disponga de conectividad nativa IPv6 a Internet y la Escuela haga un enlace con ésta a través de IPv6 nativo, la segunda es iniciar un túnel en el servidor de la Escuela para hacer pasar IPv6 sobre la red IPv4 actual utilizando un *tunnel-broker* proporcionado por Hurricane Electric [8], y finalmente la tercera es que exista conectividad nativa hacia la DSIC y que ésta abra el túnel hacia la Escuela sobre IPv4.

Las pruebas se están haciendo sobre los Sistemas Operativos Linux y FreeBSD como router, utilizando las distribuciones Ubuntu y pfSense, respectivamente. Además se están realizando pruebas sobre Mikrotik, que es una distribución también basada en Linux. Como cliente se usarán los Sistemas Operativos más populares actualmente, los que corresponden a Windows 7 y Windows XP de Microsoft, Ubuntu y Fedora como distribuciones de Linux, y Android e iOS como Sistemas Operativos móviles.

Para la seguridad inalámbrica se está evaluando utilizar los métodos disponibles actualmente, los cuales son: Portal Cautivo, WPA2-Personal y WPA2-Enterprise.

1.1. Objetivos

El objetivo general del presente trabajo de investigación es el siguiente:

- **Determinar el costo y los beneficios de migrar las redes de la Escuela de Ingeniería Informática de la Pontificia Universidad Católica de Valparaíso a la versión 6 del protocolo IP, y entregar un manual de configuración para ello.**

1.2. Objetivos específicos

- Seleccionar la forma de implementación de IPv6 más apropiada según cómo está la red según como está la red de la Escuela de Ingeniería Informática de la PUCV.
- Realizar pruebas del funcionamiento de IPv6 considerando concurrencia, rendimiento y seguridad.
- Seleccionar el mejor método para ofrecer una conexión más segura y eficiente a la red Wifi.

1.2.1. Actividades

- Investigar sobre la nueva versión del Protocolo de Internet, sus ventajas y desventajas, características y comprobar con esto si es conveniente o no el realizar la migración de IPv4 a IPv6.
- Coordinar con la Dirección de Servicios de Informática y Comunicaciones (DSIC) para llevar a cabo la implementación de IPv6 a nivel de Universidad.
- Trabajar junto con el Administrador de Recursos de TI de la Escuela de Informática para llevar a cabo pruebas con IPv6 con el fin de implementar esta nueva versión del protocolo a nivel de Escuela.
- Confeccionar pequeños prototipos en un segmento de red de la Escuela para lograr conectividad IPv6.
- Probar los distintos tipos de seguridad inalámbrica que ofrece Wifi para elegir cuál es el método más conveniente.
- Realizar un estudio de los usuarios de la red de la Escuela de Informática para conocer y tener una estadística acerca de los recursos que utilizan para conectarse, esto para tener conciencia de cuál es el público objetivo

que será migrado y así poder estimar de manera más precisa el impacto del cambio en la red entre los usuarios.

- Implementar IPv6 en la red de la Escuela si se corroborase que es conveniente en cuanto a rendimiento y seguridad, de lo contrario demostrar su mal desempeño.

- Junto con el Administrador de Recursos de TI elaborar una lista de los servicios de red que están operando actualmente en la Escuela, para posteriormente investigar si son compatibles con IPv6, y de no ser así comprobar si hay disponible alguna actualización que soporte este protocolo.

1.2.2. Riesgos

Plan de implementación alternativo

En caso de que en la Casa Central no prospere la implementación de IPv6, se debe realizar lo siguiente:

Implementar en la Escuela un servidor que brinde conectividad IPv6 a través de un túnel, para operar en modalidad Dual-Stack. Este servidor puede ser distinto de la puerta de enlace, ya que los servidores DHCP y los servicios de anuncio por router (*radvd*) se anuncian a través de la red mediante broadcast, lo que agiliza su implementación, y hace que no sea necesario reemplazarla como en el caso de la Escuela que la única versión que soporta IPv6 es la versión de desarrollo de pfSense, y los desarrolladores de esta plataforma estiman que en septiembre estará lista la versión definitiva.

Este plan está probado en una red con conectividad IPv4 nativa (figura 1), donde se agregó conectividad IPv6 a través de un túnel con un equipo servidor (ipv6) y que anuncia su conectividad a la red para que los equipos además de recibir dirección IPv4, se auto asignen una dirección IPv6 en base a la dirección MAC de la interfaz de red.

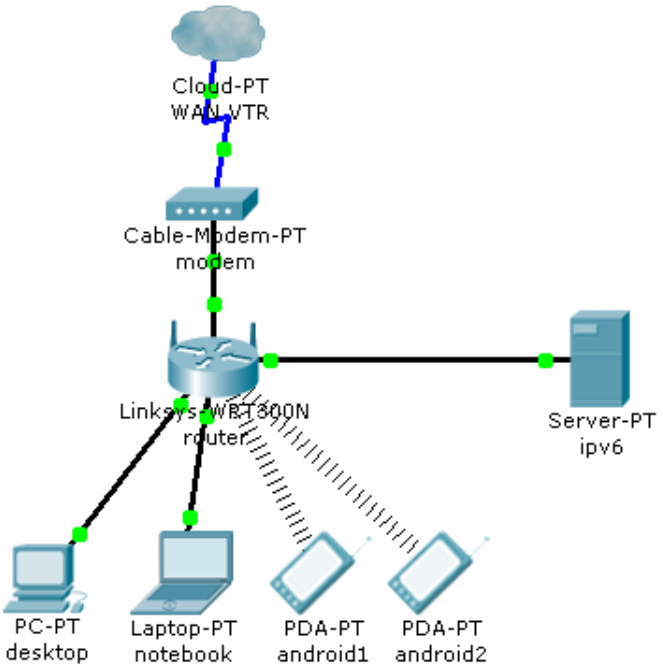

Figura 1: Topología de red probada del plan de contingencia.

Actividades del plan de contingencia

- En caso de no poder coordinarse exitosamente con la DSIC se deberá trabajar e intentar implementar IPv6 a nivel de Escuela y no a nivel de Universidad.

- De no poder llevarse a cabo el trabajo en conjunto con el Departamento de TI de la Escuela se deberá trabajar en forma particular.

- En caso de no poder llevarse a cabo la conexión IPv6 nativa por parte de la DSIC en el corto plazo se deberá implementar IPv6 utilizando conectividad por túnel IPv4, las que deben considerar las implicancias de usar este método, especialmente en cuanto a rendimiento.

- En caso de que haya en la Escuela un servicio no compatible con IPv6 y que no disponga de actualizaciones que incluyan soporte para este protocolo, dependiendo de cuál es el servicio afectado, se deben evaluar alternativas compatibles con dicho protocolo.

2. IPv6

2.1. Definición

Para comenzar la investigación se definirá primeramente qué se entiende por IPv6, dando una breve definición de esto para luego especificar sus beneficios y porqué se debe sustituir IPv4 por él.

IP versión 6 (IPv6) es la nueva versión del Protocolo de Internet, diseñada para ser el sucesor de la actual versión 4 (IPv4). Las diferencias entre ambos protocolos se centran en las categorías que se mencionarán a continuación.

2.2. Características

Capacidad de direccionamiento expandida

IPv6 incrementa el tamaño de la dirección IP de 32 a 128 bits, lo que ofrece un número bastante mayor de nodos direccionables y además ofrece una auto-configuración simple de direcciones. La escalabilidad del ruteo *multicast* fue mejorada agregando el campo *scope* (alcance) a las direcciones *multicast*. También se añadió un nuevo tipo de direcciones llamadas direcciones anycast, utilizadas para enviar paquetes a cualquier equipo dentro de un grupo de nodos para levantar servidores que necesiten alta disponibilidad, como por ejemplo, los servidores DNS raíces de Internet.

Simplificación del formato del encabezado
Algunos campos del encabezado de IPv4 ahora fueron eliminados o hechos opcionales para reducir el procesamiento y manejo de los paquetes, además de limitar el ancho de banda requerido por los mismos.

Soporte mejorado para extensiones y opciones
Debido a los cambios en las opciones del encabezado IP la transmisión de los paquetes es más eficiente, límites menos rigurosos en la longitud de las opciones, y mayor flexibilidad para introducir nuevas opciones en el futuro.

Capacidad de etiquetar el tráfico
Se agregó una nueva capacidad para permitir etiquetar los paquetes pertenecientes a cierto tráfico, por los cuales el que los envía solicita un manejo es-

pecial, como un nivel de Quality of Service (QoS) o servicio en tiempo real.

Capacidades de autenticación y privacidad
IPv6 soporta extensiones para agregar autenticación, integridad de datos y opcionalmente también confidencialidad de datos.

Transmisión eficiente
La fragmentación de paquetes en IPv4 ocurre en cada nodo intermedio, donde cada uno al momento de transmitir al siguiente lo fragmenta si es necesario, según el MTU (*Maximum Transmission Unit*). En IPv6 la fragmentación ocurre sólo en los nodos origen y destino, no en los nodos intermedios lo que aumenta la eficiencia, ya que ambos nodos negocian el tamaño máximo del paquete previamente. Además en IPv4 si uno de los fragmentos llega con errores o no llega, se debe retransmitir el paquete completo.

```
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|Version| Traffic Class |           Flow Label                  |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|         Payload Length        |  Next Header  |   Hop Limit   |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
+                                                               +
|                                                               |
+                         Source Address                        +
|                                                               |
+                                                               +
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
+                                                               +
|                                                               |
+                      Destination Address                      +
|                                                               |
+                                                               +
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Figura 2: Definición de un encabezado IPv6 [1].

La figura 2 muestra la composición de un encabezado IPv6, donde hay un campo para la *Version* del protocolo IP, en este caso es la 6, el campo *Traffic Class* que contiene el tipo de tráfico, la etiqueta de tráfico (*Flow Label*), el largo del contenido (*Payload Length*), el tipo de encabezado que viene

después de éste (*Next Header*), la cantidad máxima de saltos (TTL) (*Hop Limit*) y las direcciones IP de origen (*Source Address*) y destino (*Destination Address*).

2.3. Tipos de direccionamiento

IPv6 utiliza dos tipos de direccionamiento, los cuales se describen a continuación:

2.3.1. Configuración automática sin estado

Al iniciar el sistema se crea automáticamente una dirección de enlace local por cada interfaz que tenga IPv6 activado, esa dirección tiene como prefijo `fe80::/64`, los demás 64 bits se rellenan con el identificador EUI-64 Modificado, el que se deriva de la dirección MAC de la interfaz de red, en que a la dirección física se inserta `FF:FE` en el medio y luego se cambia un bit de EUI64 para reducir la posibilidad de colisión. El sistema de autoasignación de IPv6 es equivalente al de IPv4 que asigna direcciones `169.254.0.0/24`. Para obtener una dirección IP pública el router debe enviar paquetes tipo *Router Announcement* periódicamente, los que contienen el prefijo de la red, entre otros parámetros, como los servidores DNS. El equipo al recibir esos paquetes crean una dirección IP pública rellenando el prefijo con la dirección MAC en formato EUI-64 Modificado, y luego de verificar que esa dirección no está duplicada en la red la asignan a la interfaz. En la figura 4 se muestra un paquete *Router Advertisement* donde aparece el prefijo de red con el que los equipos pueden crear su dirección IP y la figura 3 muestra un equipo que se le asignó IP mediante este método. Se puede apreciar que el equipo tiene varias direcciones (`fe80::219:21ff:fe42:bf4c`, `2001:470:d:2cb:219:21ff:fe42:bf4c`), que son relativamente similares, la primera es la dirección de enlace local que sólo es válida en la LAN, y la segunda es la dirección pública creada localmente junto a los anuncios del router, que manda el prefijo de red (`2001:470:d:2cb::/64`). Cabe destacar que las direcciones de enlace local se deben usar con un indicador de zona que señala la interfaz que se debe usar, el que se le agrega a la dirección, como `%eth0`. Esto se debe indicar ya que toda NIC debe tener una dirección de este tipo, lo que impide crear una tabla de enrutamiento para este tipo de direcciones.

```
Adaptador Ethernet eth0          :

        Sufijo de conexión específica DNS : alexisabarca.com
        Descripción. . . . . . . . . . . : VIA Rhine II Fast Ethernet Adapter
        Dirección física. . . . . . . . . : 00-19-21-42-BF-4C
        DHCP habilitado. . . . . . . . . : No
        Autoconfiguración habilitada. . . : Sí
        Dirección IP. . . . . . . . . . . : 192.168.2.11
        Máscara de subred . . . . . . . . : 255.255.255.0
        Dirección IP. . . . . . . . . . . : 2001:470:d:2cb:9db:442:465:dbd1
        Dirección IP. . . . . . . . . . . : 2001:470:d:2cb:219:21ff:fe42:bf4c
        Dirección IP. . . . . . . . . . . : fe80::219:21ff:fe42:bf4c%5
        Puerta de enlace predeterminada   : 192.168.2.1
                                            fe80::210:14ff:fe02:8b8f%5
        Servidor DHCP . . . . . . . . . . : 192.168.2.1
        Servidores DNS . . . . . . . . . .: 74.82.42.42
                                            fec0:0:0:ffff::1%2
                                            fec0:0:0:ffff::2%2
                                            fec0:0:0:ffff::3%2
        Concesión obtenida . . . . . . . . : jueves, 07 de junio de 2012 15:29:59

        Concesión expira . . . . . . . . .: jueves, 07 de junio de 2012 17:29:59
```

Figura 3: Dirección IP asignada por configuración automática sin estado.

2.3.2. DHCPv6

Además del sistema de autoconfiguración también las interfaces pueden obtener una dirección IP a través de un servidor DHCPv6 [11], para un mayor control de las asignaciones por el administrador de red. Este mecanismo de asignación se le dice que es con estado ya que el servidor mantiene una tabla con las direcciones asignadas a los clientes con los identificadores del equipo como se puede ver en la figura 5.

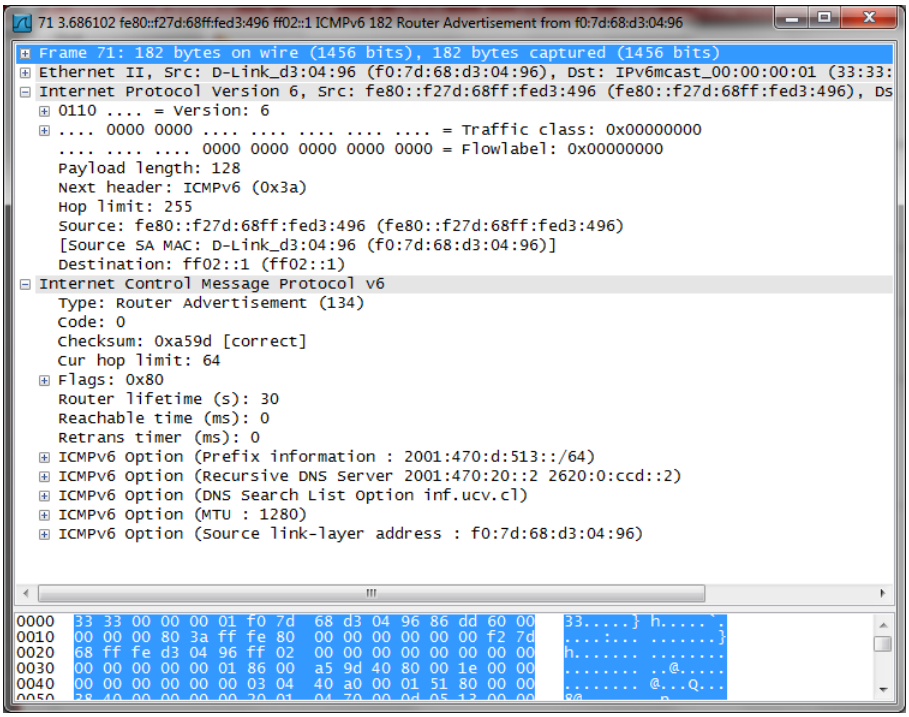

Figura 4: Paquete *Router Advertisement* desde un router IPv6.

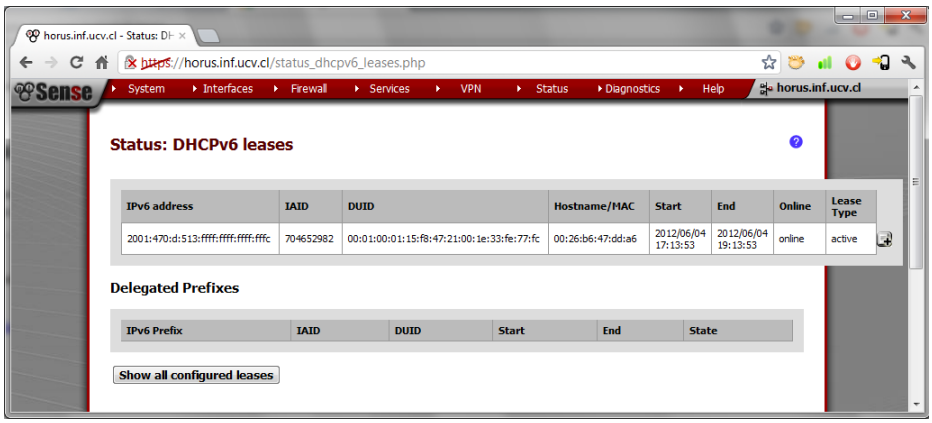

Figura 5: Asignaciones actuales del DHCPv6.

A diferencia de IPv4 es posible que convivan ambos métodos de direccionamiento (configuración sin estado y DHCPv6), e incluso un cliente puede recibir múltiples direcciones IPv6. Los mensajes *Router Advertisement* (RA) que envía el router anunciándose determinan qué método(s) se va(n) a utilizar.

3. Situación actual del protocolo IP

Esta sección describe la problemática actual de las redes en el mundo, en Chile, en la Universidad y en la Escuela, la que se pretende solucionar mediante la implementación de IPv6.

3.1. En el mundo

Ante el agotamiento global de las direcciones IPv4 los países han comenzado a implementar IPv6, así como los servicios de resolución de nombres, comenzando por los servidores raíz de resolución que corresponden a los *Top Level Domain* (TLD), los que han tenido que actualizar sus servicios para soportar los registros AAAA requeridos para retornar direcciones IPv6 y conectividad nativa para así poder recibir conexiones a través de este protocolo. En la actualidad la mayoría de los TLD ya tienen soporte IPv6 a nivel de servidor raíz, a nivel de dominio la cantidad de dominios accesibles directamente por IPv6 (se cuentan sólo los que tienen registro AAAA en el dominio principal, como google.com que tiene dirección A `173.194.37.6` y AAAA `2001:4860:8007::6a`) está aumentando con el paso del tiempo.

La tabla 1 muestra el nivel de adopción de registros AAAA en los distintos TLD.

TLD	dominios	A	AAAA
com	102.169.177	9.169.2033	761.164
net	14.652.647	12.593.573	169.805
de	13.155.766	10.611.153	2.025.526
org	9.916.595	8.714.846	104.735
info	7.951.940	6.866.547	102.841

Tabla 1: Adopción de A y AAAA en los distintos TLD

Sitios importantes y empresas como ISP's alrededor del mundo están implementando IPv6 en sus redes, como el sitio Web de Apache (servidor web), Facebook, Google, Terra, los que pueden ser visitados por IPv6. Además debido a que las direcciones IPv6 al ser hexadecimales permiten letras de la A a la F pueden ser creativos en las direcciones IP, como el sitio Web de Fedora (distribución de linux) `2610:28:3090:3001:dead:beef:cafe:fed3` y Facebook que incorpora su abreviatura `2620:0:1c18:0:face:b00c::`.

El día 8 de Junio del 2011 la Internet Society organizó el llamado *World IPv6 Day* donde los sitios web más importantes e ISP's activaron IPv6 por 24

horas de manera experimental para probar la conectividad y además verificar si activando IPv6 se producen problemas como que los clientes prefieran conectarse a través de IPv6 en lugar de IPv4, aún si la conexión no es confiable o es más lenta. Esto puede producir problemas de conexión, donde por cada intento de conexión IPv6 se espera que se supere el tiempo de espera antes de intentar usando IPv4. Los resultados de este experimento fueron exitosos donde Cisco y Google no reportaron problemas significativos, Facebook mantuvo su sitio de desarrolladores sobre IPv6, sin embargo se reconoció que se necesita más trabajo en esta área [10].

Para el año 2012 se planeó un nuevo día mundial de IPv6, el *World IPv6 Launch* para el 6 de Junio, donde los ISP's, empresas de redes y empresas web activaron IPv6 permanentemente para todo el mundo. Como participantes estaban confirmados Akamai (Content Delivery Network), D-Link, Cisco, Google, Facebook, Bing y Yahoo, entre otras empresas.

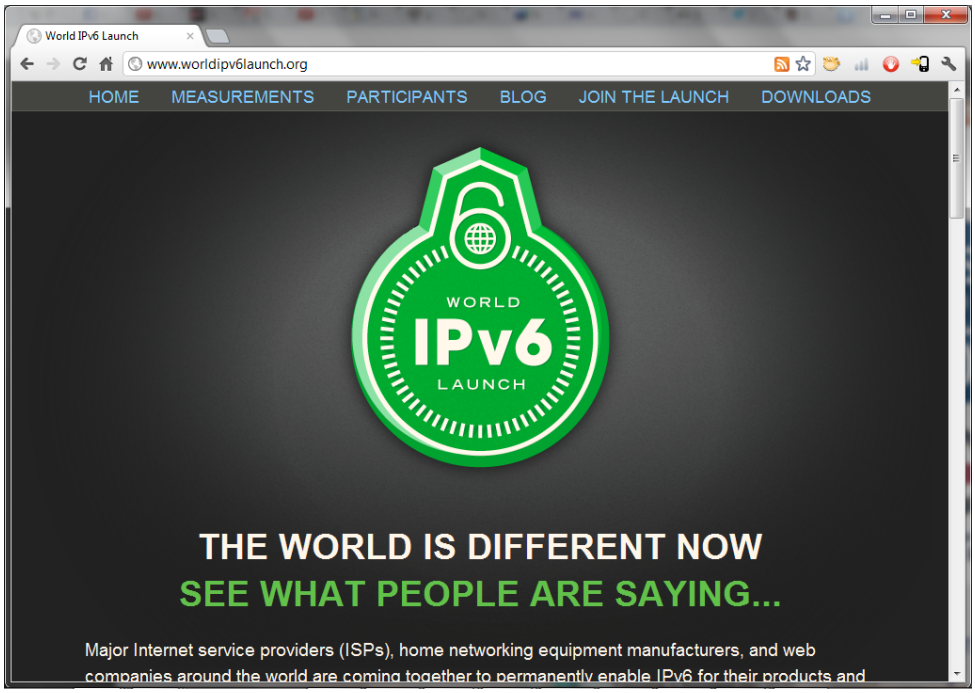

Figura 6: Sitio Web de World IPv6 Launch

3.2. En Chile

En la actualidad (Marzo de 2012) ya varias empresas e ISP han implementado IPv6 en sus redes utilizando la modalidad *Dual-Stack*, en la que pueden operar con IPv4 e IPv6 de manera simultánea y no de forma exclusiva una u otra. Dicha modalidad hace referencia a que los equipos tienen la capacidad de traficar paquetes utilizando ambas versiones del Protocolo de Internet en la misma red, permitiendo conectarse utilizando direcciones IPv4 e IPv6, siendo el Sistema Operativo quien decida cual versión utilizar según sea el caso, ya que si un equipo se trata de conectar a una dirección IPv4 entonces se asignará la pila correspondiente a esa conexión, pero de suceder lo contrario y darse el caso de que el equipo intente conectarse a una dirección IPv6 entonces la pila que será asignada corresponde a la versión 6 de IP. Algunas empresas e ISP que se identifican con la característica mencionada anteriormente se encuentran actualmente en fases de pruebas y experimentación con la nueva versión, mientras que otros ya se encuentran entregando direcciones IPv6 a sus usuarios finales.

NIC Chile, que corresponde a la entidad que administra los nombres de dominio .cl, desde el 2005 que soporta registros AAAA para sus dominios, además de que su sitio web dispone de dirección IPv6 (`2001:1398:1::6003`). Desde del 2006 que disponía de conectividad en forma experimental y de mediados del 2008 con conectividad nativa.

A nivel universitario la UTFSM dispone de dos segmentos de IPv6 en el que están trabajando de manera experimental [15]. En la Red Universitaria Nacional (REUNA) desde el 2011 se levantaron los servicios en IPv6, su sitio Web también es accesible a través de este protocolo. El direccionamiento lo solicitaron a LACNIC desde el 2004 [17]. El ISP GTD para sus clientes corporativos ya dispone de soporte completo de IPv6, mientras que Entel y VTR están en fase de pruebas. Para el caso de VTR para completar la migración se necesita sustituir los cablemodems de sus clientes por otros que soporten DOCSIS 3.0 o 2.0+IPv6. La Subtel el día Mundial de IPv6 en el 2011, activó el soporte IPv6 en su sitio Web, el cual es accesible a través del protocolo (`2800:160:168b:1::80`).

De todas maneras en Chile la implementación de IPv6 ha sido lenta, eso se puede ver en el sitio de SixXS [9] en que los prefijos IPv6 asignados no todos son anunciados a nivel mundial, y por lo tanto no están activos aún. La tabla 2 detalla los prefijos en uso en Chile.

Prefijo	Operador	Fecha asignación	% anuncio
2001:1310::/32	Red Universitaria Naciona...	21/08/2003	82 %
2001:1398::/32	NIC Chile	13/09/2005	100 %
2800:8::/32	Netup S.A.	24/11/2005	0 %
2800:150::/32	VTR BANDA ANCHA S.A.	03/08/2007	99 %
2800:160::/32	Gtd Internet S.A.	30/08/2007	100 %
2800:1b0::/32	PUC	03/10/2007	0 %
2800:1f0::/32	Adexus S.A.	27/12/2007	100 %
2800:270::/32	Universidad Tecnica Feder...	08/08/2008	100 %
2800:290::/32	Netline	08/09/2008	0 %
2800:300::/32	ENTEL CHILE S.A.	30/01/2009	100 %
2800:330::/32	Entel PCS Telecomunicacio...	03/04/2009	0 %
2800:3b0::/32	Telmex Servicios Empresar...	14/07/2009	100 %
2800:460::/32	**PUCV**	**05/02/2010**	**0 %**
2800:4c0::/32	TELEFONICA MOVIL...	11/06/2010	100 %
2800:4d0::/32	TELEFÓNICA CHILE S.A.	18/06/2010	100 %
2800:4e0::/32	CTC. CORP S.A.	28/07/2010	100 %
2800:540::/32	CLARO CHILE S.A.	05/11/2010	0 %
2800:550::/32	CTC Transmisiones Regiona...	16/11/2010	100 %
2800:590::/32	Telefonica Empresas	30/11/2010	100 %
2800:670::/32	INTERNEXA Chile S.A.	17/02/2011	0 %
2800:8e0::/32	Manquehuenet	09/06/2011	0 %
2800:8f0::/32	SERV. INTERNET LTDA	10/06/2011	0 %
2800:990::/32	Redcol S.A.	05/08/2011	0 %
2800:a60::/32	TV Cable Loncomilla S.A.	30/09/2011	0 %
2800:be0::/32	Mainstreet Ltda	07/12/2011	0 %
2800:c60::/32	Wirecrossing Networks	22/12/2011	0 %
2801:0:10::/48	Quintec Soluciones Inform...	12/11/2008	0 %
2801:0:50::/48	NIC Chile	26/04/2010	0 %
2801:0:b0::/45	SONDA S.A.	22/07/2011	0 %
2801:0:120::/48	Celulosa Arauco y Constit...	04/10/2011	0 %
2801:0:150::/48	SEGIC USACH LTDA	18/08/2011	0 %
2801:2::/32	Ministerio del Interior y...	28/02/2012	0 %
2803:2800::/32	ZAM LTDA.	27/02/2012	0 %
2803:3800::/32	NETLAND CHILE S.A.	16/03/2012	0 %
2803:4200::/32	SOC. COM. WIRENET CH...	30/05/2012	0 %
2803:ac00::/32	MARIZE NET S.A	26/04/2012	0 %
2803:e800::/32	Intercity	12/03/2012	0 %

Tabla 2: Prefijos IPv6 en uso en Chile.

3.3. En la universidad

La Universidad se encuentra utilizando IPv6 de forma experimental en un laboratorio del DSIC, ya que dispone de un bloque IPv6 (`2800:460::/32`) asignado por LACNIC [16], correspondiente a la gran cantidad de 2^{96} IP's (79.228.162.514.264.337.593.543.950.336). La Universidad posee dos Proveedores de Servicios de Internet (ISP), los cuales corresponden a GlobalCrossing y Telefónica, los que ya poseen soporte de IPv6 nativo, por lo que la Universidad al momento de implementar la nueva versión del protocolo antes mencionado tendrá conectividad directa y no a través de un túnel. Para poder extender el uso de IPv6 a la Universidad completa y no sólo a nivel de Escuela (de Informática en este caso) se debe actualizar el equipamiento de red de todas las facultades, comenzando por el servidor principal ubicado en la Casa Central, los routers y los switches, que suman la cantidad aproximada de 400 conmutadores entre los dos tipos. Debido a esto, para obtener conectividad IPv6 la Escuela deberá realizar la conexión a través de un túnel IPv4 (utilizando el método del encapsulamiento) con la Casa Central hasta que el equipamiento sea compatible con IPv6 en su totalidad y así poder mantener una conexión a Internet de forma nativa y sin pasar por algún tipo de túnel. Probablemente una de las primeras áreas por donde se comience a añadir soporte de IPv6 es en la red inalámbrica `PUCV-PRO`, ya que la cantidad de usuarios que presenta diariamente esta red es bastante grande y por lo tanto la demanda es bastante alta y al mejorar dicha red se verían beneficiados, por tanto, la mayor cantidad de usuarios de la Universidad.

Actualmente se está trabajando con la DSIC para llevar a cabo la implementación de IPv6 en sus redes de forma nativa, aunque aún no se ha anunciado públicamente el segmento IPv6 asignado como se pudo ver en la tabla 2. Para llevar a cabo la actualización se debe comenzar por actualizar el equipamiento de red, establecer conectividad y actualizar sus servicios para que sean compatibles con IPv6, como los servidores Web, de correo, DHCP, etc. La actualización de equipos está planeada para el mediano plazo, mientras que la actualización de los servicios se está trabajando en este momento. Se estima que para el mes de Septiembre se disponga de una conexión IPv6 estable para realizar pruebas entre la escuela y la Casa Central.

3.4. En la escuela de informática

Actualmente la Escuela sufre escasez de direcciones IPv4 únicas para cada equipo, producto de que hay una gran cantidad de usuarios conectados a la red, entre profesores, personal administrativo, equipos del laboratorio, equipos de las salas y los de los alumnos que se conectan vía inalámbrica a Internet. Inicialmente la Escuela sólo disponía de un rango de IP's provisto por la Universidad, el cual era `158.251.10.0/24`, que luego fue cambiado por `158.251.88.0/24`. Como 253 direcciones eran insuficientes se tuvo que solicitar un rango adicional que es `158.251.93.0/24`, el que está asignado a los equipos del laboratorio. En la actualidad ambos rangos sólo tienen aproximadamente 50 IP disponibles, por lo que éstas deben ser racionadas, para ello el servidor DHCP está configurado para sólo entregar direccionamiento a equipos previamente autorizados los que tendrán su IP asignada de antemano. Cualquier equipo no autorizado no recibirá dirección IP alguna. De persistir la situación se tendrá que solicitar un nuevo rango de IP a la DSIC, ya que esta entidad manifestó que del rango de IP que tiene la Universidad de clase B `158.251.0.0/16` aún quedan direcciones disponibles.

Para la red inalámbrica se está usando un rango de IP privada clase C `192.168.127.0/24`, en el cual en momentos de alta concurrencia se ocupan todas las direcciones disponibles. Esto ha producido problemas ya que al estar todas las direcciones asignadas, a los nuevos usuarios se les asignan direcciones duplicadas, y esto impide la conectividad porque al tener dos direcciones MAC asignada una misma IP se producen conflictos al momento de la autenticación frente al portal cautivo.

Frente a este problema el Administrador de Recursos de TI tomó inicialmente como medida reducir los tiempos de asignación a cada IP, para así liberar las direcciones más rápidamente. Luego como medida definitiva cambió la máscara de subred de la red inalámbrica, dejándola en `192.168.112.1/20`, con lo que ahora se pueden conectar más de 4.000 equipos de forma simultánea.

4. Seguridad WLAN

La seguridad inalámbrica es una de las más importantes cuando se habla de una conexión a Internet, ya que actualmente es una de las más utilizadas para navegar por la red. Con el paso del tiempo se han ido implementando muchas y variadas técnicas de seguridad en cuanto a conexiones, entre las cuales se utilizan mayoritariamente cifrado y autenticación con usuario y/o contraseña. El gran problema de este tipo de conexión (inalámbrica) es que al transmitirse la onda con los paquetes de datos a través del aire, y no por un medio cableado, facilita a uno o más usuarios malintencionados que se encuentren dentro del área de cobertura de la señal wireless a capturar fácilmente dichos paquetes y poder utilizarlos a su favor. Dada la situación de esta forma, se hace imprescindible el uso de algún metodo que dificulte o imposibilite el caso mencionado anteriormente y así asegurar la privacidad y seguridad de los datos enviados y recibidos hacia y desde un servidor. A diferencia de la conexión inalámbrica, la conexión cableada o alámbrica asegura de mejor manera que el tráfico de datos desde y hacia otro equipo se realizará de forma un poco más segura, ya que para poder intervenir o capturar dichos paquetes de datos sería necesario estar conectado por cable a la red en cuestión, siempre y cuando los equipos conectados de forma cableada no envíen ni reciban datos desde un equipo conectado por Wifi.

4.1. WEP

Este sistema simplemente consistía en que los routers aceptaban una clave preconfigurada que se daba a los usuarios de la red, para conectarse, los clientes sólo deben ingresar dicha clave y ya pueden navegar por Internet. Tiene la ventaja de que es muy fácil de configurar tanto para el administrador del sistema como para el usuario final y tiene la desventaja de que no permite individualizar a los usuarios para llevar un registro de navegación y además por esto último no permite asegurar que el usuario es alumno de la Escuela y no alguna persona externa al que se le haya compartido la clave. WEP se limita a cifrar el tráfico con la clave compartida. Como parte del cifrado cada paquete incorpora un *Initialization Vector* (IV) de 24 bits que conforma la semilla para cifrar cada paquete. Este sistema tiene el inconveniente de que como se trafican muchos paquetes en una red, los 24 bits del IV son insuficientes, además de que el algoritmo que los genera tiene un enfoque directo y previsible, por lo que con un *sniffer* capturando el tráfico necesario y con técnicas estadísticas se puede obtener la clave. Este proceso sólo tarda unos minutos dependiendo de la cantidad de tráfico en la red, y

el largo de la clave, que si es mayor se incrementa la cantidad de paquetes necesarios. Debido a esto se ha declarado este método de seguridad como roto y ya no es considerado como sistema de cifrado seguro y fue sustituido por WPA/WPA2, así que no se recomienda su implementación y sólo está mencionado en este informe como referencia.

4.2. WPA2-Personal

Al igual que en WEP se compone de una clave precompartida que se configura en router (figura 7) y equipos, por lo que también es fácil de configurar. Sin embargo, a diferencia de WEP, se genera una clave individual por cliente con la que se cifra el tráfico con él, obtenida a través de las MAC del AP, del dispositivo y el BSSID, además de usar otro algoritmo de cifrado que es AES, a diferencia de RC4. Aunque en la página de configuración del AP puedes ver los clientes conectados con su IP y dirección MAC, no se tiene la opción de desconectar a los usuarios individualmente por demanda. Finalmente, aunque el tráfico esté cifrado por la contraseña, si un usuario malintencionado conoce la contraseña de la red, puede capturar tráfico para obtener las claves de cifrado individual por cliente y así descifrar el tráfico de éste, y aunque las claves de cifrado individual se negocian al momento de la asociación del cliente, el atacante puede forzar la reasociación inyectando paquetes de deautenticación en la red. En consecuencia este tipo de red ofrece seguridad ante atacantes externos que no conozcan la contraseña pero luego de conocerla no ofrece ninguna seguridad adicional.

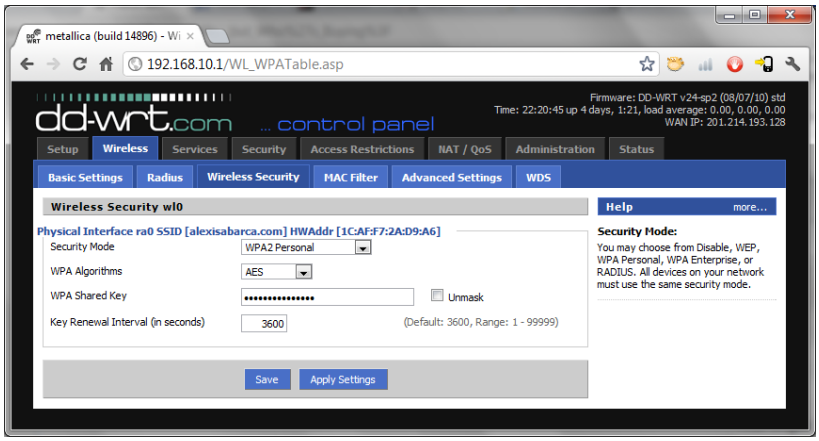

Figura 7: Configuración de WPA2 en un AP con firmware DD-WRT

4.3. Portal cautivo

Esta alternativa consiste en configurar los Access Point (AP) sin contraseña o con una clave compartida, pero en el momento en que el usuario intente navegar por Internet se le redirigirá a un portal de autentificación, donde deberá ingresar su usuario y contraseña para validarse como usuario registrado en el sistema. De haberse efectuado correctamente la validación, el usuario podrá navegar por la Red, pero de lo contrario no se tendrá acceso a la misma y por ende a Internet. Este método tiene la ventaja de que al haber identificación de usuarios se pueden registrar las actividades que éstos realizan, haciendo posible además controlar si la cuenta está siendo utilizada en varios equipos simultáneamente. Como desventaja se puede observar que la autenticación se encuentra centralizada en un solo servidor, por lo que si hay muchos usuarios intentado conectarse a la vez, eso puede conllevar problemas de rendimiento. Sumado a esto, si además el AP está configurado sin contraseña, entonces el tráfico entre los equipos y los puntos de acceso viaja sin cifrar, lo que puede permitir que cualquier persona pueda capturar el tráfico sin necesidad de autenticarse, ya que esta solución de por sí sólo provee la autenticación de usuarios, no asegurando el cifrado de los datos transmitidos. Considerado como medida adicional de seguridad, esta solución permite además la opción de desconectar manualmente a los usuarios de forma individual desde un panel de control (figura 8), en caso de que fuera necesario.

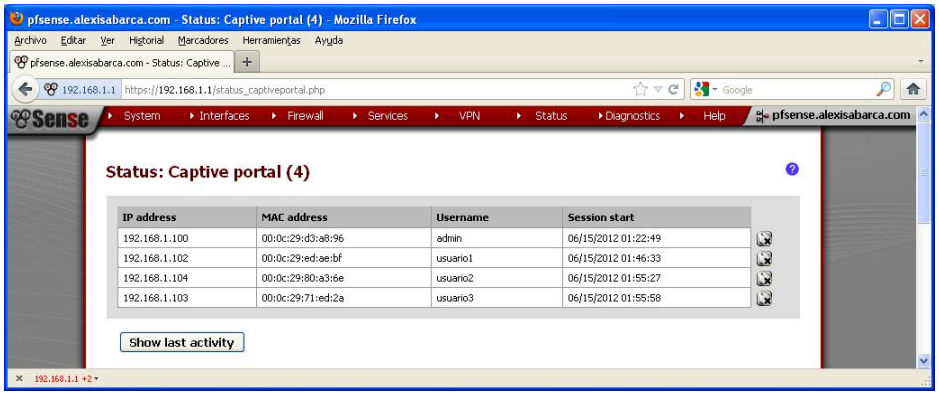

Figura 8: Lista de usuarios activos del portal cautivo.

4.4. WPA2-Enterprise

Este modelo de autenticación consiste en que los clientes para conectarse al AP deben ingresar un usuario y una contraseña, los que luego son validados contra un servidor RADIUS (*Remote Authentication Dial-In User Server*), el que responde con un `Access-Accept` cuando las credenciales son correctas y en ese momento se le otorga acceso a la red. De lo contrario se obtendrá un `Access-Reject` como respuesta y se denegará el acceso. Este método tiene como ventaja que permite identificar a los usuarios y además cifrar el tráfico entre el cliente y el AP, por lo que protege ante capturas de tráfico por usuarios maliciosos, además de que a cada cliente el AP se le genera una clave individual diferente, lo que evita el problema que sufría WPA2-Personal que la clave de red para todos era la misma, por lo que se puede aseverar que esta solución provee la autenticación y confidencialidad. Además se puede afirmar que si una cuenta de usuario es comprometida, los datos de los demás usuarios permanecerán seguros. También se requiere un certificado firmado por una entidad certificadora de confianza como Verisign, Thawte u otras, ya que el cliente al conectarse valida dicho certificado para autenticar al servidor. Como desventaja tiene que es relativamente complejo de implementar, requiere un servidor RADIUS quien procese las conexiones de los usuarios y puede requerir configuración adicional en el lado del cliente para conectarse a la red inalámbrica.

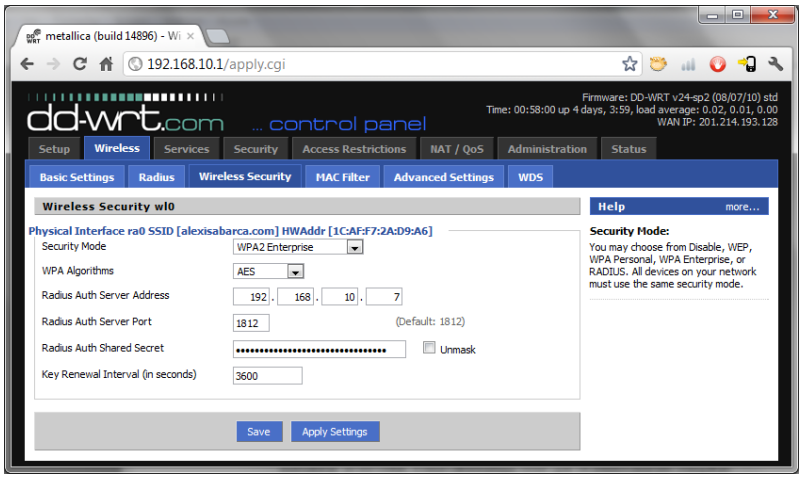

Figura 9: Configuración de WPA2-Enterprise en un AP (DD-WRT).

5. Soporte de IPv6 en dispositivos y sistemas operativos

En la actualidad la gran mayoría de los Sistemas Operativos tiene soporte para IPv6. La tabla 3 muestra el soporte de los Sistemas Operativos más populares de este protocolo.

Sistema Operativo	Soporte	RADVD	DHCPv6
Windows 7	Si	Si	Si
Windows Vista	Si	Si	Si
Windows XP	Manual	Si	No
Android	Sólo wifi [12]	Si	No
iOS	Desde iOS 4 [13].	Si	Si
Mac OS	Desde Lion	Si	Si
Symbian	Si	Si	No
Windows Phone 7	No	N/A	N/A

Tabla 3: Soporte de IPv6 en los SO más populares.

Se llevó a cabo un estudio utilizando la herramienta Google Analytics para determinar cuáles son los Sistemas Operativos que se conectan comúnmente a la red Wifi, el cual está basado en 1155 visitantes únicos conectados en el plazo de 4 semanas. Los resultados que arrojó dicho estudio se muestran en la tabla 4.

Sistema Operativo	Porcentaje de uso
Windows	41,46 %
Android	27,30 %
iOS	7,63 %
iPhone	4,01 %
Nokia	3,78 %
SymbianOS	3,54 %
Linux	3,07 %
Macintosh	2,05 %
iPod	1,97 %
BlackBerry	1,26 %

Tabla 4: Sistemas Operativos que se conectan a la red Wifi.

Como parte del estudio mencionado anteriormente se llevó a cabo también una estadística para conocer qué Sistemas Operativos Móviles se conectan a la red Wifi de la Escuela de Informática, y para ello se utilizó nuevamente la herramienta Google Analytics. Los resultados se muestran en la tabla 5.

SO Móvil	Porcentaje de uso
Android	51,95 %
iOS	14,52 %
iPhone	7,63 %
Nokia	7,19 %
SymbianOS	6,74 %
iPod	3,74 %
BlackBerry	2,40 %
LG	2,25 %
Samsung	1,95 %
iPad	1,05 %

Tabla 5: Sistemas Operativos Móviles que se conectan a la red Wifi.

Según la estadística que arrojó el estudio realizado a través de Google Analytics se puede observar que más del 80 % de los equipos que se conectan a la red Wifi de la Escuela de Informática cuentan con el SO Android e iOS, por lo tanto según este estudio más del 65 % (66,47 %) de los clientes poseen la capacidad para conectarse a redes utilizando IPv6, al menos utilizando la configuración sin estado.

6. Pruebas de implementación

6.1. Conectividad IPv6

Para determinar cuál es la mejor forma de implementar IPv6 se están realizando varias pruebas con distintos SO como servidor. Se utilizó Ubuntu Server, pfSense y Mikrotik, los que están basados en Linux y en el caso de pfSense está basado en FreeBSD.
Las pruebas se hicieron abriendo un túnel a Hurricane Electric, el cual es compartido con los clientes de la red vía Ethernet y Wireless con un AP configurado con WPA2. El túnel es abierto tanto desde la Universidad como desde un domicilio particular. Como cliente se emplearon SO de escritorio como Fedora, Ubuntu y Windows, y como SO móviles se utilizaron iPhone y Android.
La configuración del túnel por parte de la Universidad es la siguiente:

- Dirección IPv4 local: `158.251.88.3`
- Dirección IPv4 remota del túnel: `66.220.18.42`
- Dirección IPv6 local: `2001:470:c:513::2`
- Dirección IPv6 remota (puerta de enlace): `2001:470:c:513::1`
- Segmento de red IPv6 ruteado: `2001:470:d:513::/64`
- Asignación de direccionamiento: DHCPv6

La configuración en el domicilio particular es como sigue:

- Dirección IPv4 local: `201.214.193.128`
- Dirección IPv4 remota del túnel: `66.220.18.42`
- Dirección IPv6 local: `2001:470:c:2cb::2`
- Dirección IPv6 remota (puerta de enlace): `2001:470:c:2cb::1`
- Segmento de red IPv6 ruteado: `2001:470:d:2cb::/64`
- Asignación de direccionamiento: Sin estado (sólo *Router Advertisements*)

6.1.1. pfSense

PfSense cuenta con soporte de IPv6 a contar de la última versión de desarrollo que es la `2.1-DEVELOPMENT`. Al ser una versión en desarrollo tiene varios *bugs*, por lo que no se recomienda su uso en entornos de producción. Las pruebas realizadas con este SO fueron exitosas, se estableció el túnel correctamente y se pudo compartir con los usuarios de la red obteniendo el máximo rendimiento acorde a la velocidad de conexión, por supuesto considerando la pérdida de rendimiento asociada a que la misma se realiza a través de un túnel.

Para configurar el túnel se debe ir a Interfaces, *Assign* y crear una nueva interfaz GIF (figura 10).

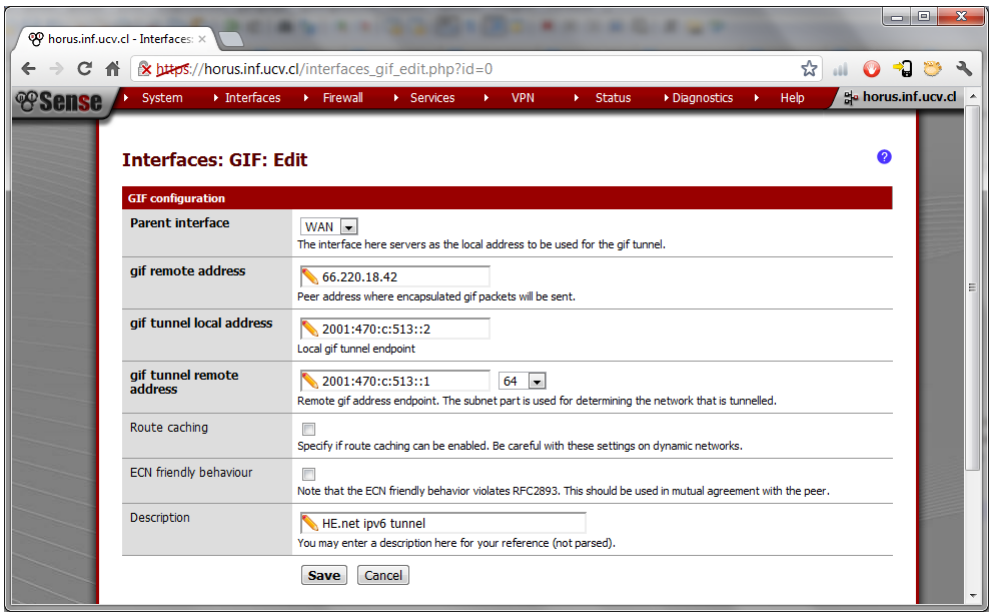

Figura 10: Configuración del túnel en pfSense.

Luego a la interfaz que corresponde a la LAN se le debe asignar una dirección IPv6 estática perteneciente al segmento ruteado `2001:470:d:513::/64` como se muestra en la figura 11.

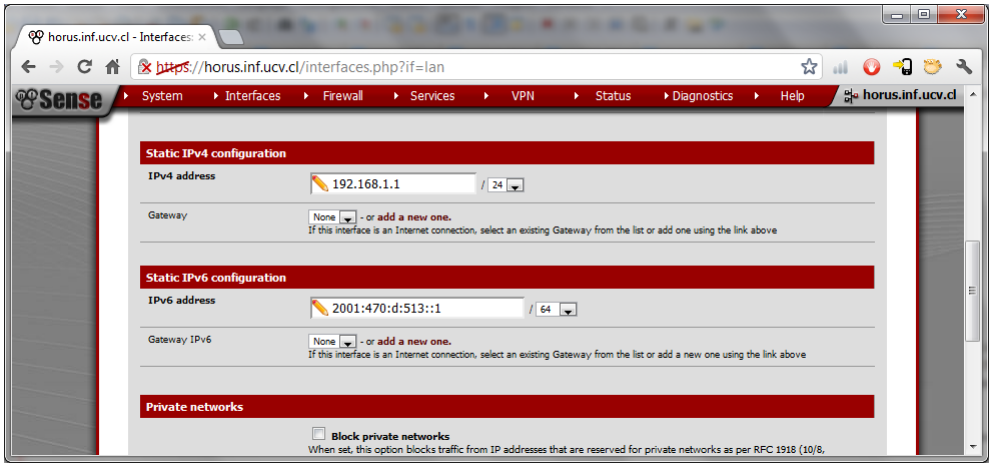

Figura 11: Configuración LAN en pfSense.

Finalmente para distribuir direcciones IP a los clientes se tienen dos alternativas: la configuración sin estado y la configuración con estado (DHCPv6). Cabe destacar que la función DHCPv6 de pfSense aún está en desarrollo, por lo que no se encuentra completamente funcional, e incluso puede no funcionar en algunas versiones de desarrollo. En la universidad se está utilizando DHCPv6 (figura 13), mientras que en el domicilio particular se está usando configuración sin estado.

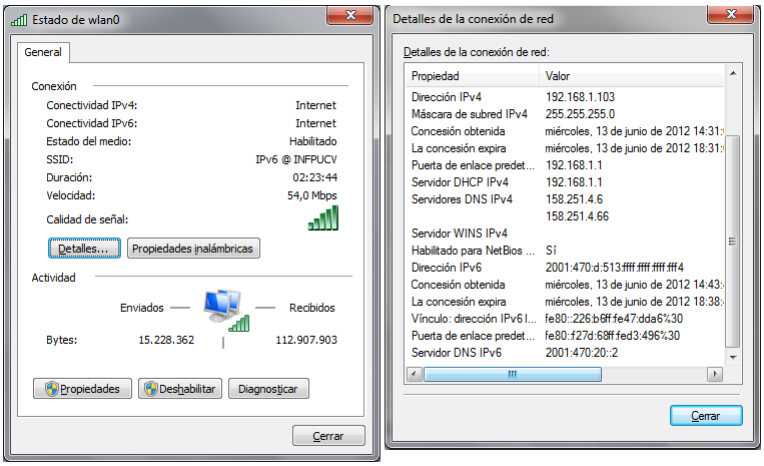

Figura 12: Asignación IPv6 por DHCPv6 en Windows 7.

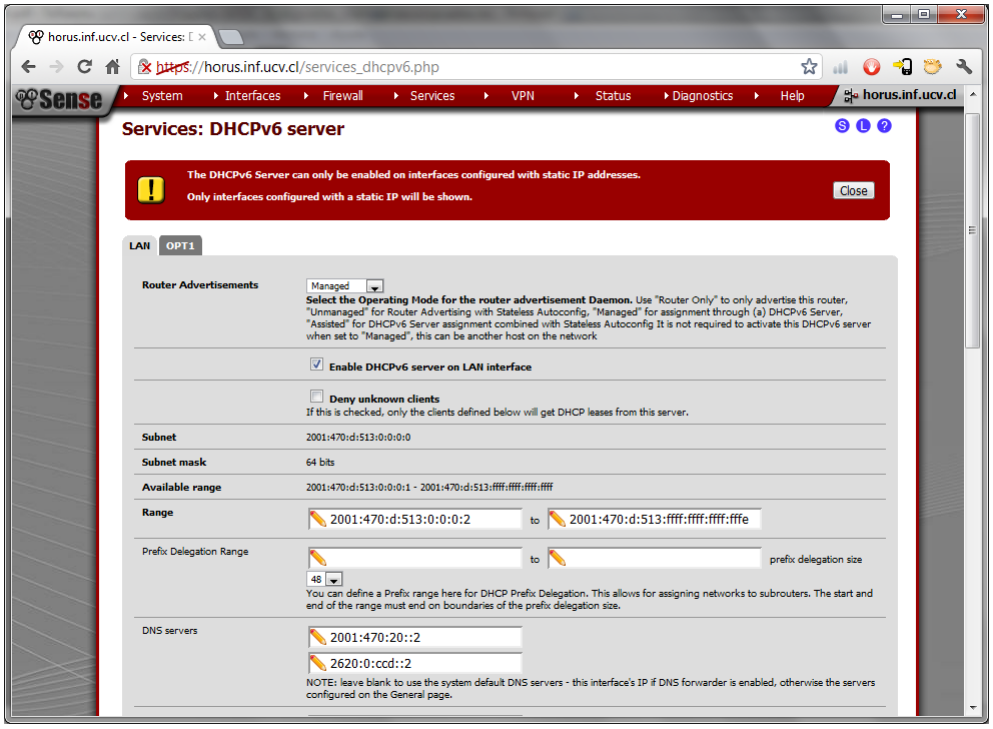

Figura 13: Configuración DHCPv6 en pfSense.

6.1.2. Mikrotik

Para llevar a cabo las pruebas en esta plataforma se utilizó la última versión estable (5.17), la cual cuenta con soporte estable de IPv6. Soporta tanto direccionamiento sin estado como DHCPv6, y también dispone de cliente DHCPv6 para conexiones IPv6 nativas e interfaces 6to4 para crear túneles sobre IPv4, tal como se hará en las presentes pruebas.

Para utilizar este software se deben tener mínimo 2 tarjetas de red (NIC), las que deben estar con su dirección IPv4 asignada. Para ello se debe ir al menú IP ->Interfaces y asignar direcciones a cada interfaz. A la LAN se le asignó la dirección `192.168.9.1/24`, mientras que a la WAN se le asignó la IP estática `192.168.10.8/24`.

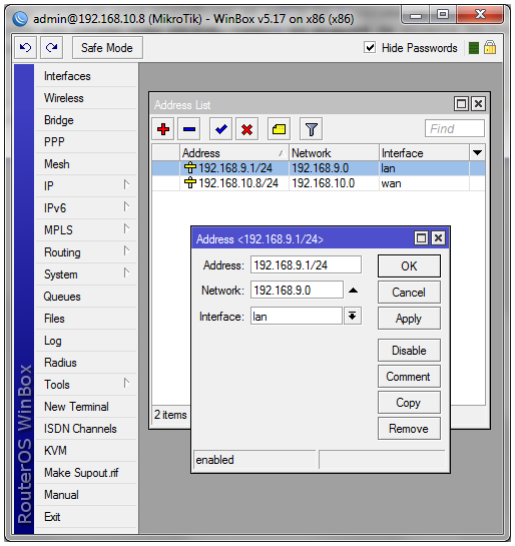

Figura 14: Configuración LAN en Mikrotik.

Acto seguido, se debe crear la interfaz 6to4 que hará de túnel, para ello se hace clic en Interfaces y luego se agrega la nueva interfaz de este tipo, que debe tener como parámetros:

- MTU: 1280
- Local Address: `192.168.10.8` (IP de la WAN)
- Los demás campos se dejan por defecto.

Ahora se debe agregar la ruta IPv6, que contiene la dirección IPv4 remota del túnel, y esto se hace en IPv6 ->Routes. Ésta debe tener la siguiente configuración:

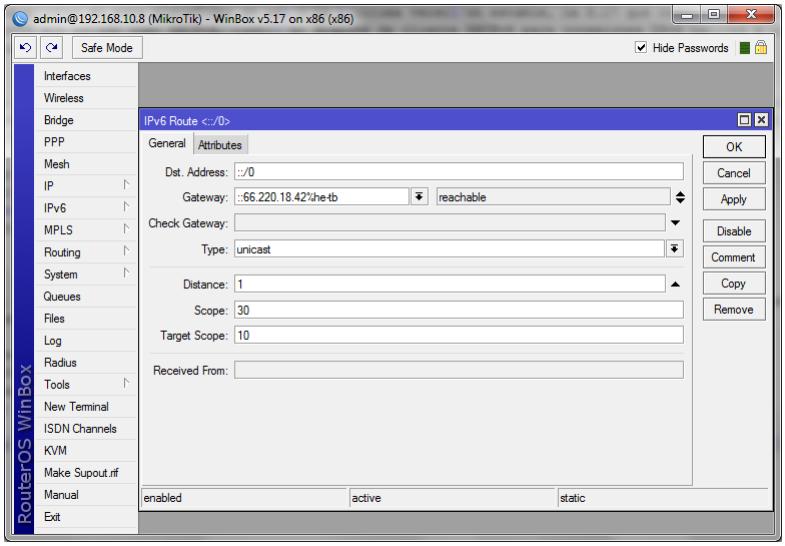

Figura 15: Configuración de la ruta IPv6 en Mikrotik.

- Dst Address: `::/0` (enviar todo el tráfico IPv6)
- Gateway: `::66.220.18.42%he-tb` (dirección IPv4 del túnel junto a la interfaz IPv6)
- Los demás campos se dejan por defecto.

Y finalmente hay que asignar las direcciones IPv6 tal como se hizo con IPv4 al principio. Mikrotik tiene la opción Advertise que permite anunciar el prefijo en la red, que corresponde al direccionamiento sin estado.

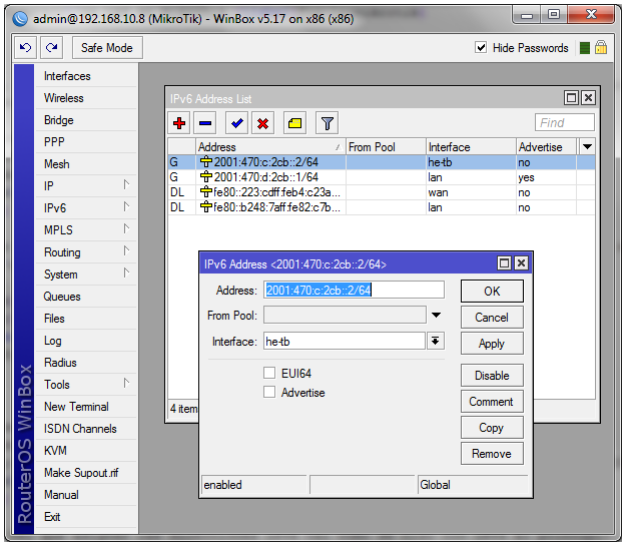

Figura 16: Direcciones IPv6 en Mikrotik.

Para la interfaz 6to4:

- Address: `2001:470:c:2cb::2/64`
- Advertise: desmarcado

Para la interfaz LAN:

- Address: `2001:470:d:2cb::1/64` (o cualquier IP dentro del segmento `2001:470:d:2cb::/64`)
- Advertise: marcado

Mikrotik también dispone de servidor DHCPv6 para asignación de direcciones con estado, sin embargo éste no funcionó ya que el equipo no recibía dirección IPv6, por lo que se descartó este método de asignación de direcciones.

6.1.3. Ubuntu Server

En el caso de Ubuntu Server se empleó la última versión estable correspondiente a la 12.04 LTS, la cual se utilizó únicamente como router IPv6. Para ello se levantó el túnel con Hurricane Electric y se instaló el servicio `radvd` que envía a la red *Router Advertisements* anunciando su IP y que es un router capaz de rutear paquetes IPv6.
Para levantar el túnel se usaron los siguientes comandos, los que se pusieron en un script configurado para ejecutarse automáticamente al inicio del sistema:

```
modprobe ipv6
ip tunnel add he-ipv6 mode sit remote 66.220.18.42 \
local 192.168.10.7 ttl 255
ip link set he-ipv6 up
ip addr add 2001:470:c:2cb::2/64 dev he-ipv6
ip route add ::/0 dev he-ipv6
ip -f inet6 addr

/sbin/ip -6 addr add 2001:470:d:2cb::1/64 dev br0

echo nameserver 2001:470:20::2 >> /etc/resolv.conf
```

Los comandos descritos anteriormente realizan lo siguiente:

1. Cargar el módulo IPv6 en el kernel si es que no estaba cargado desde antes.
2. Agrega la interfaz 6to4, configurando las direcciones IPv4 de los extremos del túnel.
3. Levanta la interfaz recién creada .
4. Establece la dirección IPv6 local del túnel.
5. Modifica la tabla de ruteo para enviar todo el tráfico IPv6 a través de la interfaz del túnel.
6. Configura el sistema para que prefiera IPv6 en lugar de IPv4.
7. Establece la dirección IPv6 de la interfaz física conectada a la LAN. Esta dirección debe estar dentro del segmento ruteado IPv6 del túnel (`2001.470:d:2cb::/64`).

8. Agrega el servidor DNS IPv6 al sistema.

Las interfaces están configuradas con direcciones estáticas. La configuración del archivo `/etc/network/interfaces` es la siguiente:

```
# The loopback network interface
auto lo
  iface lo inet loopback

# The primary network interface
auto eth0

# bridge
auto br0
  iface br0 inet static
  bridge_ports eth0 tap0
  address 192.168.10.7
  network 192.168.10.0
  netmask 255.255.255.0
  broadcast 192.168.10.255
  gateway 192.168.10.1
```

OpenVPN también se encuentra instalado en este servidor, el que además de distribuir direcciones IPv4 a los clientes para acceder a la red local, entrega direcciones IPv6 públicas válidas globalmente, ya que los *Router Advertisements* pueden transmitirse a través de la VPN. Este servicio utiliza la interfaz `tap0`, que está enlazada con la interfaz `eth0` conectada a la red para formar la interfaz `br0`. Ésta forma de conexión permite ofrecer IPv6 a equipos que no están conectados directamente a la LAN donde está ubicado el servidor que tiene establecido el túnel.

Como este servidor entrega direccionamiento sin estado, se debe configurar el servicio `radvd` para que envíe *Router Advertisements* a la red, los que contienen el prefijo `/64` público y los servidores DNS. La configuración del archivo `/etc/radvd.conf` es la siguiente:

```
interface br0
{
        AdvSendAdvert on;
        MinRtrAdvInterval 5;
        MaxRtrAdvInterval 15;
        prefix 2001:470:d:2cb:1::/64
        {
                AdvOnLink on;
                AdvAutonomous on;
                AdvRouterAddr on;
        };

        RDNSS 2001:470:20::2{
        };
};
```

Finalmente hay que configurar el kernel para que permita el reenvío de paquetes por la red, ya que como será un router IPv6, ésta será su función. Para ello se debe editar el archivo `/etc/sysctl.conf` y agregar la siguiente línea: (en caso de existir se debe modificar para que sea igual a la mostrada aquí)

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

Luego reiniciar el sistema o ejecutar `# sysctl -p /etc/sysctl.conf` para aplicar los cambios.

6.2. Seguridad Wifi

6.2.1. WPA2-Enterprise

Para probar este método de seguridad se levantó un servidor RADIUS que debe manejar las cuentas de usuarios y procese las solicitudes de autenticación que envía el AP. Las pruebas se llevaron a cabo sobre Ubuntu Server, y como servidor RADIUS se utilizó el paquete de software libre freeradius, el cual soporta cuentas de usuario locales, autenticación por LDAP o por base de datos.

Configuración de `/etc/freeradius/eap.conf` (sólo se mostrarán las secciones modificadas, debido a lo extenso del archivo)

```
eap{
default_eap_type = peap

...
tls{
# Aqui se debe usar un certificado firmado por una CA reconocida
# o crear una PKI para este efecto.
private_key_file = ${certdir}/servidor.key
certificate_file = ${certdir}/servidor.pem
# CA_file = ${cadir}/ca.pem (comentar)

cache{
enable = yes
...
}


ttls{
use_tunneled_reply = yes
...
}
}

peap{
use_tunneled_reply = yes
...
}
```

```
}
```

Luego se deben agregar los AP que van a conectarse al servidor RADIUS para hacer solicitudes de autenticación. Los mismos se deben agregar en `/etc/freeradius/clients.conf` al final.

```
client 192.168.10.3 {  # IP del AP
   shortname = ap
   # clave precompartida, se debe poner la misma en el AP
   # la clave debe ser segura, la siguiente es salida
   # del comando "dmesg | md5sum"
   secret = 8eac099d9572bb827bbfe2ffe672224a
}
```

Finalmente se configuró un AP para utilizar WPA2-Enterprise junto con el servidor RADIUS y así realizar pruebas de autenticación, las que se completaron exitosamente en Windows 7, Fedora 17 (figura 17) y Android.

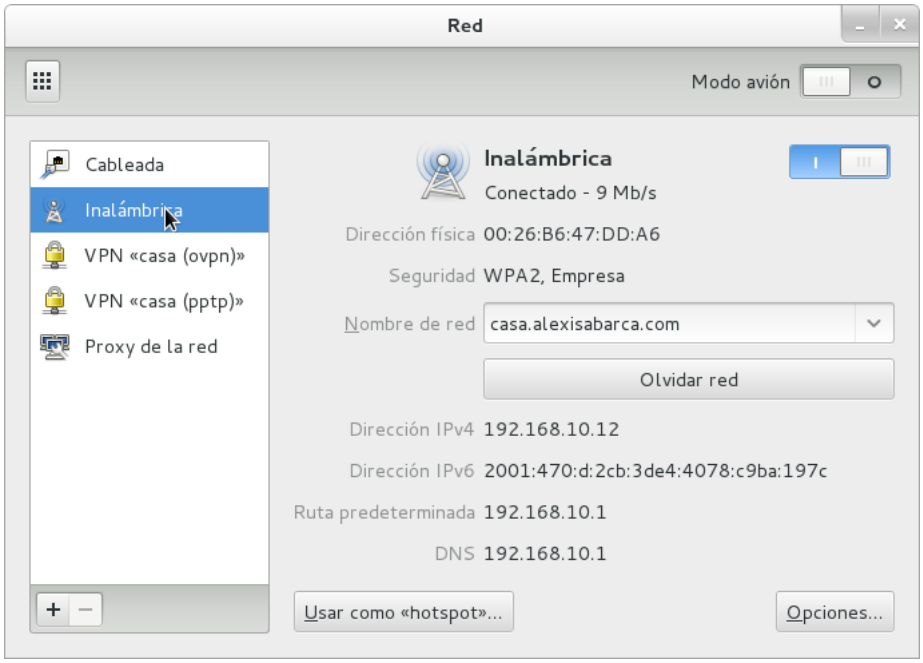

Figura 17: Conexión al AP con WPA2-Enterprise en Fedora 17.

6.3. Pruebas y criterios de comparación

Para poder determinar si es conveniente realizar la migración a IPv6 se deben realizar pruebas comparativas con IPv4, las cuales deben retornar resultados con cierto margen de tolerancia para ser consideradas exitosas. Si las pruebas muestran como conclusión que el rendimiento es significativamente menor, entonces eso demuestra que no es conveniente migrar a IPv6 por el momento.

Las pruebas a realizar son las siguientes:

- Ping a otros equipos de la misma LAN, usando la dirección de enlace local de los mismos (`fe80::/64`)
- Ping a servidores remotos usando su nombre, para eso el dns debe soportar y retornar registros AAAA.
- Ping a servidores remotos usando su IP pública (`2000::/3`)
- Pruebas de ancho de banda, considerando velocidad de bajada y subida

En las pruebas anteriormente mencionadas se llevará a cabo IPv6 contra IPv4, y los márgenes de tolerancia son los siguientes:

- Ping 1 %
- Ancho de banda 10 %

En términos de concurrencia debe soportar mínimo la misma cantidad que hay actualmente con IPv4. Es importante considerar que las pruebas se deben realizar sobre una conexión cableada para obtener resultados confiables, ya que si se realiza por una conexión inalámbrica los resultados variarán por factores ajenos al protocolo, como cantidad de usuarios conectados en ese momento, distancia del AP, entre otros factores asociados a este tipo de conexiones.

Aquí hay un ejemplo de prueba de ping, que se realizó a la dirección IP de la interfaz LAN del router, efectuada en Fedora.

```
--- 2001:470:d:2cb::1 ping statistics ---
100 packets transmitted, 100 received, 0% packet loss, time 99080ms
rtt min/avg/max/mdev = 0.721/3.921/175.484/20.061 ms
```

```
--- 192.168.10.7 ping statistics ---
100 packets transmitted, 100 received, 0% packet loss, time 99075ms
rtt min/avg/max/mdev = 0.674/4.433/202.577/23.622 ms
```

Se puede observar que aunque la prueba tardó 5ms más con IPv6, los *Round Trip Time* (RTT) son menores, lo que muestra el mejor rendimiento de este protocolo. La diferencia de tiempo se produjo porque la prueba se realizó a través de una conexión inalámbrica.

En las pruebas de velocidad IPv6 tuvo velocidades similares a IPv4. Para realizar esta prueba se configuraron dos equipos en modalidad *Dual-Stack* por LAN cableada (Ethernet 100mbit/s Full-Duplex) y se transfirió un archivo de 500 MB. En ambos protocolos se pudo alcanzar la velocidad máxima que permite esta conexión que es de 11,1 MB/s, con un tiempo de descarga de 49s en IPv6 y 48s en IPv4, por lo que tienen un rendimiento similar.

Se llevó a cabo un test de velocidad a servidores de Internet públicos comparando IPv4 e IPv6, y el sitio Web donde se realizó dicha prueba es http://ipv6-test.com/. Se efectuaron 6 mediciones de velocidad consecutivas y luego se calculó un promedio sobre los valores obtenidos, dando como resultado 9,66 Mbit/s para IPv4 y 9,74 Mbit/s para IPv6, demostrando así que en promedio, y a pesar de tener conexión IPv6 a través de un túnel, los resultados fueron satisfactorios favoreciendo a IPv6.

7. Pruebas de servicios

Para implementar IPv6 con éxito en la Escuela, se debe comprobar que los servicios de red que estén en funcionamientos sean compatibles con IPv6, en caso de que no lo sean se deberá buscar una alternativa equivalente que lo pueda reemplazar.

En la Escuela se pueden encontrar los siguientes servicios:

- VPN
- RADIUS
- Portal Cautivo
- LDAP
- Proxy
- HTTP
- PostgreSQL
- NFS
- MySQL
- SAMBA
- SSH
- RDP
- DNS
- SMTP/POP3/IMAP4

7.1. Compatibilidad servicios

Cada uno de estos servicios se describirá su compatibilidad IPv6 en las siguientes secciones:

7.1.1. VPN

En el servidor `ptah` se puede encontrar la VPN de la Escuela, la que emplea el conjunto de protocolos IPsec, el que es completamente compatible con IPv6, ya que desde su diseño se incluyó su compatibilidad. Para provisionar las claves de seguridad a IPsec se utiliza el protocolo IKE (*Internet Key Exchange*) que se apoya en intercambio secreto de claves tipo Diffie-Hellman sobre certificados o claves precompartidas. Este protocolo es compatible con IPv6 en su implementación para linux, que es el Sistema Operativo utilizado para ofrecer este servicio.

La alternativa a IPsec, es openVPN, la que soporta traficar IPv6 sobre el túnel virtual, pero ambos extremos de la conexión deben usar IPv4. Sin embargo en la futura versión 2.3 tendrá soporte completo IPv6 [3].

7.1.2. RADIUS

El portal cautivo y la VPN utilizan este servicio para autenticar a los usuarios que se conectan a la red inalámbrica y a la VPN, respectivamente. Para comprobar a los usuarios se buscan en un directorio, el que está en un servidor LDAP.

Para ofrecer este servicio tiene el paquete *freeradius*, el que cuenta con soporte IPv6 para recibir conexiones, además se pueden definir los clientes autorizados para consultar al servidor como direcciones IPv6. Este paquete está disponible para Windows, Linux, BSD y Mac.

7.1.3. Portal cautivo

En la última versión estable de pfSense (2.0) el portal cautivo no soporta IPv6, pero en la próxima versión (2.1) el portal soportará este protocolo [5].

Mikrotik si bien cuenta con soporte IPv6, en el módulo de portal cautivo (hotspot) no soporta este protocolo, debido a que aún requiere modificaciones a los programas que utiliza, además para IPv4 depende del NAT, característica que IPv6 no dispone ya que no hace falta, por lo que requiere una solución alternativa.

7.1.4. LDAP

Este servicio se utiliza para almacenar la base de datos de usuarios de la Escuela, en la que se consideran alumnos y personal, para autentificarlos en los servicios como VPN, Portal Cautivo y antiguamente en los equipos del laboratorio. El paquete OpenLDAP cuenta con soporte para conexiones IPv6.

Se puede habilitar IPv6 en el archivo de configuración o al momento de levantar el servidor con el parámetro `-6`.

7.1.5. Proxy

Este servicio se utiliza como intermediario para acceder a Internet por parte de los equipos cuando éstos tienen bloqueado el acceso directo a la Red. Se utiliza en los equipos de los docentes y administrativos, excepto en el computador de la recepción del laboratorio (`158.251.88.0/24`).

Para proveer este servicio, se dispone del paquete *squid* que es un proxy HTTP/HTTPS/FTP de alto rendimiento y estabilidad. Desde la versión 3 dispone de soporte IPv6 para conexiones entrantes y salientes. En caso de utilizar una versión anterior sin soporte, ésta no soportará la nomenclatura de direcciones IPv6, que incluye el uso del `[` y múltiples `:` que son parte de una dirección IP. Al intentar acceder a una IP literal se obtendrá un error de sintaxis, como muestra la figura 18.

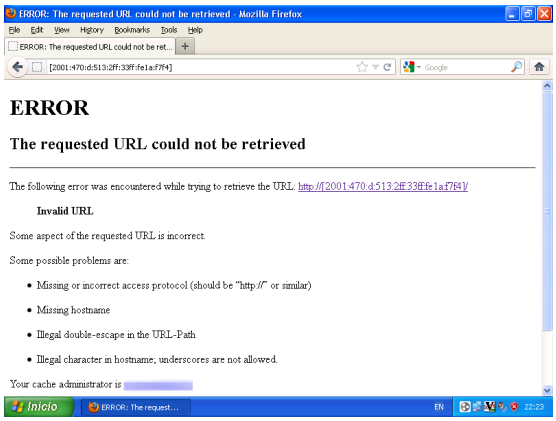

Figura 18: Mensaje de error de Squid 2.X al usar una dirección IPv6 literal.

7.1.6. HTTP

El servidor web Apache cuenta con soporte IPv6, depende de la distribución puede que venga habilitado o no por defecto. En caso de que no esté habilitado se debe modificar el archivo de configuración `apache2.conf` en la carpeta `/etc/apache2/` y modificar la directiva `Listen` para que quede de esa forma:

```
Listen 0.0.0.0:80
Listen [::]:80
```

Si además de HTTP se utiliza HTTPS se debe agregar al `Listen` correspondiente al puerto 443:

```
<IfModule mod_gnutls.c>
    Listen 0.0.0.0:443
    Listen [::]:443
</IfModule>
```

7.1.7. PostgreSQL

PostgreSQL soporta IPv6 desde la versión 9.1 para recibir conexiones de clientes, además de soportarlo como tipo de datos para guardar direcciones IPv6 en las tablas de la base de datos.

```
alexis@mastodon:~$ psql -h ::1 -U postgres -W
Password for user postgres:
psql (9.1.5)
SSL connection (cipher: DHE-RSA-AES256-SHA, bits: 256)
Type "help" for help.

postgres=#
```

7.1.8. NFS

NFS soporta IPv6 para cliente y servidor. En el cliente se define la dirección del servidor como IPv6 entre corchetes. Lo mismo aplica para el servidor al momento de configurar las carpetas exportadas a través de NFS.

7.1.9. MySQL

MySQL soporta IPv6 para conexiones de cliente, sin embargo no viene activado por defecto, para activarlo se debe editar el archivo `/etc/mysql/my.cnf` [2] y sustituir la variable `bind-address` que viene como `0.0.0.0` por `::`. Luego para aplicar los cambios se debe reiniciar el servicio con el comando `/etc/init.d/mysqld restart` como root.

7.1.10. SAMBA

SAMBA desde la versión 3.2.0 cuenta con soporte IPv6 [4], aunque en las pruebas no se ha podido conectar por IPv6 a un servidor SAMBA. Sin embargo hay una alternativa, que implica usar el servicio `xinetd` que escuche por IPv6 y pase las conexiones a SAMBA.

En el caso de Windows, desde Vista este servicio cuenta con soporte IPv6 por defecto, no es necesario activarlo manualmente. Es importante considerar que las rutas UNC (*Universal Naming Convention*) no consideran válido el caracter `":"`, el que en IPv6 es usado para separar cada grupo de dos octetos de la IP. Para enfrentar este problema Microsoft implementó un sistema de traducción en que se convierte la dirección IPv6 a un host del dominio `ipv6-literal.net`. Los clientes al conectarse reconocen este nombre de host y hacen la conversión inversa automáticamente, sin necesidad de hacer consultas DNS. Siguiendo este caso, la dirección IPv6 `2001:470:d:513:381e:9f55:598c:b9c2` pasaría al host `2001-470-d-513-381e-9f55-598c-b9c2.ipv6-literal.net`. Si es una dirección de enlace local (`fe80::/32`), el índice de zona se debe agregar al final luego de la letra `s`, como `fe80--2ff-33ff-fe1a-f7f4s6.ipv6-literal.net`.

7.1.11. SSH

SSH cuenta con soporte IPv6 habilitado por defecto en varias distribuciones, en caso de que no esté habilitado, se puede habilitar editando el archivo `/etc/ssh/sshd_config` y descomentar la línea `#ListenAddress ::`.

Es importante mencionar que los servicios de la Escuela corren sobre Linux o BSD, el que tiene mayor soporte IPv6 en sus servicios.

7.1.12. Escritorio remoto RDP

RDP es soportado por IPv6 por defecto desde Windows Vista como servidor. Aunque Windows XP y Windows Server 2003 no dispongan de soporte IPv6 como servidor, se puede hacer traducción de puertos con un comando, el cual será explicado más adelante.

Desde el punto de vista de cliente, de la versión XP de Windows hacia arriba se soporta conexiones a servidores IPv6.

7.1.13. DNS

Se comprobó por medio de pruebas realizadas a través de los comandos `dig` y `nslookup` que el servicio DNS soporta tanto IPv4 como IPv6, ya que pudo obtener como resultado los registros AAAA exitosamente de varios dominios, entre ellos ipv6.google.com, fedoraproject.com y facebook.com.

7.1.14. SMTP/POP3/IMAP

En la Escuela los servicios de correo los provee el software *dovecot* para POP3 e IMAP y *postfix* para SMTP. En el el primer caso, este programa soporta sockets IPv6 e IPv4 de forma simultánea [6]. Para el segundo caso desde la versión 2.2 [7] soporta IPv6 e IPv4 simultáneamente, al igual que el caso de los protocolos POP3 e IMAP.

Para servicios no compatibles con IPv6 en Windows se puede hacer traducción IPv6 a IPv4 a través del siguiente comando:

```
%windir%\system32\netsh.exe interface portproxy add v6tov4 ^
listenport=3389 connectaddress=127.0.0.1 connectport=3389
```

En el ejemplo anterior se utiliza el puerto 3389 correspondiente al servicio de Escritorio Remoto de Windows utilizando como dirección de destino la máquina local o `localhost`. Lo que realiza dicho comando es, a groso modo, escuchar el tráfico a través del puerto 3389 utilizando el protocolo IPv6, para luego redirigirlo al puerto 3389 en la máquina local por IPv4. En este ejemplo se redirecciona el puerto 3389 a la máquina local, pero este mismo comando puede utilizarse para otras direcciones y puertos de destino.

7.2. Comparación de rendimiento entre IPv4 e IPv6

A nivel de protocolo se han llevado a cabo varias pruebas con distintas herramientas de medición para lograr obtener resultados promedio de la velocidad de conexión y transmisión de datos, usando las versiones 4 y 6 de IP. Dichas pruebas se llevaron a cabo utilizando el sistema operativo Ubuntu basado en Linux, y además se ha creado y utilizado un archivo con datos aleatorios con el peso exacto de 100 MB, el cual ha sido transferido y descargado en la misma y en distintas máquinas. Las herramientas utilizadas para cada protocolo en cuestión son: *wget* para el caso de HTTP, FTP y SQUID proxy, *scp* para el protocolo SSH, *dig* para DNS y finalmente *smbclient* para el caso del protocolo SAMBA de Windows. A continuación se muestra en la tabla 6 los resultados obtenidos (expresados en segundos) utilizando algunos de los protocolos más conocidos y empleados a nivel de Escuela:

Protocolo	IPv4	IPv6	Diferencia (IPv4 - IPv6)
HTTP (Local)	11,19	11	0,19
HTTP (Internet)	1625	1947	-322
Proxy (SQUID)	11,14	11	0,14
SAMBA	9,24	9,39	-0,15
SSH	9	9,25	-0,25
DNS (Local)	0,0015	0,00138	0,00012
DNS (Internet)	0,02138	0,01888	0,0025
FTP	11,2	11,05	0,15

Tabla 6: Rendimiento IPv6 v/s IPv4 (en segundos).

Como se puede observar en los resultados de la tabla anterior, con excepción de los protocolos SSH y SAMBA, la diferencia de tiempo obtenida es ligeramente menor en el caso de IPv6 con respecto a IPv4, lo cual significa que, exceptuando a los 2 protocolos mencionados anteriormente, la versión 6 de IP presenta una mejora en cuanto a la velocidad de transmisión de datos. Con respecto a los protocolos que presentaron una diferencia de tiempo negativa, teóricamente sus tiempos de transmisión y su velocidad deberían ser mejores ya que para efectos de las pruebas realizadas se utilizaron túneles para proporcionar IPv6, por lo que no se han hecho pruebas empleando IPv6 de forma nativa. Esta desventaja se hizo más notoria en el caso de HTTP (Internet), ya que el servidor de destino también se conectaba a IPv6 por túnel, lo que penalizó el rendimiento. Al llevarse a cabo las mediciones aplicando el segundo método los tiempos de todos los protocolos presentados en

la tabla debieran mejorar en IPv6 con respecto a IPv4, ya que en la versión 6 los encabezados de los paquetes son mas simples y ligeros, lo que provoca menos procesamiento en los equipos y junto con esto una mayor velocidad de transmisión de los primeros.

8. Implementación

8.1. Conversaciones con DSIC

Para implementar IPv6 nativo en la Escuela de Ingeniería Informática (EII) se debían completar estas tareas:

- Los ISP de la Universidad deben proporcionar IPv6 nativo.
- Los routers principales que se conectan con estos ISP, los que están ubicados en la Casa Central deben soportar IPv6.
- Los routers y switches administrables de las facultades, por lo menos los de la EII deben soportar IPv6.
- El router de la EII debe soportar IPv6.

De los puntos anteriores, todos excepto el último son responsabilidad de la DSIC, ya que administra todo el equipamiento de la Universidad. Lo que se ha avanzado en estos puntos es lo siguiente:

- Los ISP, como se mencionó en el capítulo 3 que son Telefonica y GlobalCrossing soportan IPv6 nativo.
- Este año la DSIC actualizó el router principal en el primer semestre. Este nuevo equipo soporta IPv6.
- La DSIC tiene contemplado actualizar los equipos de las facultades en el año 2013, debido que el presupuesto para este ítem no fue aprobado para el 2012, por lo que deben presentarlo nuevamente el próximo año.
- El router de la EII actualmente no soporta IPv6, pero hay alternativas compatibles, las que se trataron previamente en este informe.

Por lo mencionado anteriormente no es posible implementar IPv6 de forma nativa en este momento, ya que aún la DSIC no cuenta con enlace nativo operativo, así que se tendrá que recurrir al plan de contingencia.

8.2. Plan de contingencia

El plan de contingencia consiste en implementar IPv6 en modalidad *Dual-Stack* en un servidor de la Escuela siguiendo el procedimiento detallado en la página 4 montando un equipo que hará de servidor IPv6, donde se iniciará el túnel y enviará periódicamente *Router Advertisement* a los equipos para que puedan autoconfigurar su dirección mediante el *Stateless Addressing*.

La figura 19 muestra el mapa de la red de la Universidad, comenzando desde los ISP (Telefonica y GlobalCrossing), luego para pasar por el router principal (denominado *core* por la DSIC), después el switch que conecta las facultades, donde sale el enlace de fibra óptica que llega al router del IBC, el que enlaza las escuelas, incluida la Escuela de Ingeniería Informática.

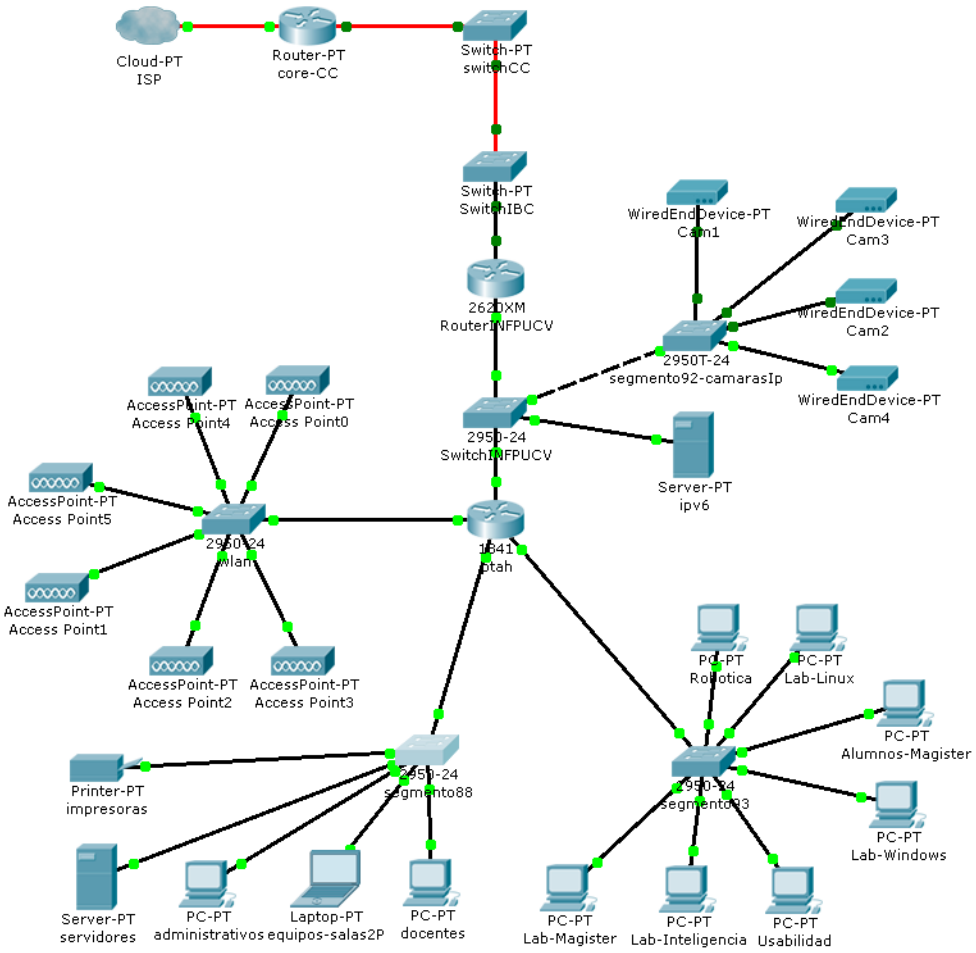

Figura 19: Mapa de red Escuela de Informática

8.3. Instalación router IPv6

De las soluciones planteadas en este informe se seleccionó Ubuntu por ser flexible, sencilla de instalar y con soporte estable IPv6. El servicio de túnel IPv6 a utilizar es Hurricane Electric, por ser gratuito, sencillo de activar y proporcionar un ancho de banda suficiente para aplicaciones comunes de Internet.

A este informe se adjunta un *script* que realizará la configuración del sistema para activar el túnel IPv6 y distribuirlo a la red mediante *stateless addressing*.

Como requerimientos se tienen los siguientes:

- Sistema Operativo Ubuntu, se recomienda recién instalado.
- 1 NIC, conectada a una LAN IPv4 con acceso a Internet.
- Protocolo 41 (*6in4*) permitido en el firewall.
- Ping permitido desde el exterior, por lo menos desde la IP del Tunnel-Broker.

El script de instalación consta de dos archivos: `config.sh` y `setup.sh`. El primer archivo contiene las variables de configuración, que corresponden a la interfaz de red en el sistema y a los parámetros del túnel, los que se pueden obtener desde el sitio de Hurricane Electric.

Para comenzar se debe visitar el sitio de Hurricane Electric [14] y registrar una cuenta de usuario. Una vez obtenida, se debe iniciar sesión y agregar el primer túnel haciendo clic en *Create Regular Tunnel*. En este formulario se debe ingresar la dirección IPv4 pública y elegir un servidor, tal como lo muestra la figura 20.

Posteriormente se debe acceder a la configuración del túnel, en esa página se proporciona toda la información del túnel, que debe ser configurada en el script `config.sh`. El contenido de este script es el siguiente:

```
#!/bin/bash

export IPV6_IP4PUB="192.168.10.10"
export IPV6_GW4IP="66.220.18.42"
```

```
export IPV6_CLIENT6IP="2001:470:c:2cb::2"
export IPV6_NET6="2001:470:d:2cb::1"

export IPV6_IFACE="eth0"
export IPV6_DNS6="2001:470:20::2"
```

Figura 20: Registro de túnel en Hurricane Electric

La primera variable (IPV6_IP4PUB) corresponde a la dirección IP de la interfaz conectada a Internet, esta información se puede obtener con el comando `ifconfig`. La siguiente variable (IPV6_GW4IP) corresponde a la dirección IPv4 remota del túnel, correspondiente a *Server IPv4 Address*. Posteriormente se configura la dirección IPv6 del cliente (*Client IPv6 Address*) y el segmento IPv6 de red asignado (*Routed /64*). La penúltima variable contiene la interfaz que se conecta a la LAN y la última es el servidor DNS IPv6. La figura 21 muestra todos los parámetros del túnel IPv6.

Una vez configurados todos estos parámetros se puede iniciar la instalación ejecutando el script `setup.sh` como root. Su contenido es el siguiente:

```
#!/bin/bash

if [ "$UID" != "0" ] ; then
   sudo $0
```

```
   exit 1
fi

echo "Este script configurara su equipo para que haga de
router IPv6 con configuracion stateless addressing"
echo
echo "Requerimientos"
echo "- Ubuntu Server o Debian, ideal recien instalado"
echo "- 1 NIC con acceso a Internet"
echo "- Debe estar permitido el protocolo 41 en el firewall"
echo "- Debe estar permitido el ping desde el exterior
(por lo menos desde el tunnelbroker)"
echo
echo "Si cumple los requisitos presione ENTER para continuar."
read

modprobe ipv6

if [ "$?" != "0" ] ; then
echo "No se pudo cargar el modulo del kernel para IPv6,
compruebe que esta usando una version reciente de su
distribucion Linux"
exit 1
fi

if [ ! -x ./config.sh ] ; then
echo "Falta el archivo config.sh, este debe estar situado
en la misma carpeta que este script y debe tener
permiso de ejecucion."
exit 1
fi

. ./config.sh

echo "Creando script..."

rm ipv6up.sh 2>&1 > /dev/null
echo "#!/bin/bash" >> ipv6up.sh
echo "ip tunnel add he-ipv6 mode sit remote $IPV6_GW4IP
local $IPV6_IP4PUB ttl 255" >> ipv6up.sh
```

```
echo "ip link set he-ipv6 up" >> ipv6up.sh
echo "ip addr add $IPV6_CLIENT6IP/64 dev he-ipv6" >> ipv6up.sh
echo "ip route add ::/0 dev he-ipv6" >> ipv6up.sh
echo "ip -f inet6 addr" >> ipv6up.sh
echo "/sbin/ip -6 addr add $IPV6_NET6/64
dev $IPV6_IFACE" >> ipv6up.sh
echo "echo nameserver $IPV6_DNS6
>> /etc/resolv.conf" >> ipv6up.sh

chmod +x ipv6up.sh

echo "Copiando script a inicio del sistema..."
cp ipv6up.sh /etc/init.d/ipv6up
update-rc.d ipv6up defaults 2>&1 > /dev/null

./ipv6up.sh

echo -n "Instalando radvd..."
apt-get update > /dev/null

echo -n "......"
apt-get install radvd -y > /dev/null

echo -n "......"

echo "interface $IPV6_IFACE
{
AdvSendAdvert on;
MinRtrAdvInterval 5;
MaxRtrAdvInterval 15;
prefix $IPV6_NET6/64
{
AdvOnLink on;
AdvAutonomous on;
AdvRouterAddr on;
};
};" >> radvd.conf

echo -n "......"
cp radvd.conf /etc/radvd.conf
```

```
echo -n "......"
echo "net.ipv6.conf.default.forwarding=1" >> /etc/sysctl.conf
echo "net.ipv6.conf.all.forwarding=1" >> /etc/sysctl.conf
sysctl -w net.ipv6.conf.all.forwarding=1 > /dev/null

echo "......"

echo "Iniciando radvd..."
/etc/init.d/radvd start > /dev/null
```

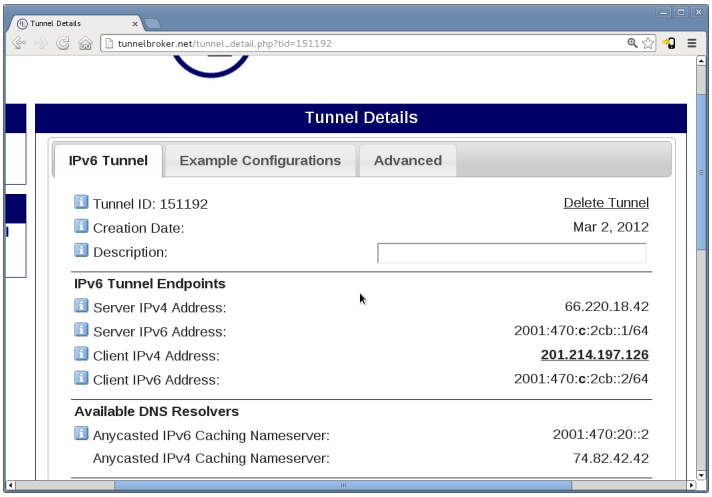

Figura 21: Parámetros del túnel IPv6 con Hurricane Electric

Una vez terminada la instalación el equipo comenzará a enviar *Router Advertisement* a la LAN y se podrá realizar conexiones a direcciones IPv6.

Para probar la conectividad se puede ejecutar el comando: `ping6 ipv6.google.com`.

8.3.1. Solución de problemas

Si el comando anterior no arrojó respuesta del servidor, es porque la conexión IPv6 no está funcionando correctamente. Se debe comprobar lo siguiente:

- La dirección *Client IPv4 Address* debe corresponder con la dirección IP con que se sale a Internet.
- La variable IPV6_IP4PUB debe corresponder con la dirección IPv4 de la interfaz con conexión a Internet. Si esta interfaz está conectada a un router que proporciona direcciones IP privadas, se debe colocar la dirección asignada a esa interfaz.
- El firewall no debe bloquear los paquetes correspondientes al protocolo 41 (*IPv6-in-IPv4*).
- Para establecer la IP pública como dirección cliente, se debe permitir el ping desde Hurricane Electric. Si no está permitido, al momento de introducir la IP pública dará error. El mensaje de error contendrá la dirección IP que se debe agregar a las excepciones del firewall.

8.4. Red inalámbrica

El método de autenticación WPA2-enterprise con un servidor RADIUS es bastante robusto y seguro, pero sin embargo presenta el inconveniente de que el cifrado del tráfico en general consume mucho ancho de banda, lo cual reduce de forma considerable el *throughput* (volúmen de información que fluye por un sistema informático). De no existir la cantidad suficiente de AP's, la falta de ancho de banda haría que el actual portal cautivo no cargara o lo hiciera muy lentamente, y de suceder esto sólo tendría que dejarse el método actual y no podría implementarse un servidor RADIUS con WPA2-Enterprise. Actualmente en la Escuela de Informática no existe este problema ya que se encuentran instalados la cantidad de 18 AP's y no se produce el efecto mencionado anteriormente, sin embargo dicho problema puede ocurrir si se implementa la solución propuesta al comienzo ya que la cantidad de AP's instalados actualmente sigue siendo baja para el *throughput* y la solución a esto sería abastecerse de más AP's e instalarlos para poder así distribuir mejor el tráfico.

Adicionalmente, como medida de seguridad se utiliza en la Escuela un software llamado *Snort*, el cual actúa como IDS (*Intruder Detection System*) y a su vez como IPS (*Intruder Prevention System*), ya que éste es un sistema hibrido. La función de este programa es detectar cualquier tipo de ataque, amenaza, intrusión o malware y, como medida de precaución, llevar a cabo el bloqueo de la dirección IP de donde provino dicha anomalía y generar un reporte de lo ocurrido. A pesar de ser este método muy efectivo y proteger la

red de forma bastante automatizada y eficaz, presenta el inconveniente de que detecta falsos positivos continuamente hasta que se "afine" dicha herramienta y así finalmente reduzca al mínimo la tasa de detección de falsos positivos.

9. Pruebas IPv6 nativo

En el mes de diciembre del 2012 se consiguió conectividad IPv6 nativa por parte de la DSIC. En esta etapa inicial el enlace sólo está dis

ponible en las oficinas de la DSIC en la Casa Central de la PUCV, por lo que se tuvo que acudir a dicho lugar a llevar a cabo las pruebas de rendimiento.

Si bien son los primeros y únicos en utilizar el enlace IPv6, se puede pensar que se dispone de todo el ancho de banda de la Universidad, por lo que las pruebas pueden ser no representativas, pero en la DSIC afirmaron que el enlace físico es compartido con los usuarios IPv4, por lo que las pruebas sí serán representativas con el uso del ancho de banda en un día normal.

9.1. Pruebas LAN

Nombre prueba	IPv4	IPv6	Diferencia (IPv6-IPv4)
Ping (ms)	0,2236	0,2419	0,0183
Proxy IPv6 (s)	8,9	9,1	0,2
Proxy IPv4 (s)	8,9	9,1	0,2
SAMBA (kb/s)	10.983,59	10.950,13	-33,46
FTP (s)	9,7	9,74	0,04
SSH (s)	8,8	8,8	0
HTTP (s)	8,92	9,2	0,28

Tabla 7: Pruebas IPv6 nativo en equipos de la misma LAN

9.2. Pruebas WAN

Nombre prueba	IPv4	IPv6 túnel	IP nativo	Dif. (IPv6 Nat.-IPv4)
Ping (ms)	167,4085	254,1192	151,6513	-15,7572
HTTP (s)	395,609	598,5685	357,8	-37,809
DNS (ms)	198,4	194,6	128,7	-69,7

Tabla 8: Pruebas IPv6 nativo hacia Internet

9.3. Análisis de resultados

Se observó que en Internet los resultados favorecen a IPv6, ya que si bien las direcciones de origen y destino en los paquetes son mucho más grandes que en IPv4 (256 bits contra 64 bits), hay menos campos que en este último. Eso hace que el encabezado IPv6 (sin extensiones) sea más pequeño, lo que explica la mejora de rendimiento en comparación a IPv4.

Por diseño el MTU (*Maximum Transmission Unit*) mínimo de IPv4 es de 68 bytes, mientras que en IPv6 es de 1280 bytes. A mayor MTU, el protocolo es más eficiente ya que el paquete transmite más datos útiles que encabezados o *headers*.

A través de Internet IPv6 supera a IPv4 ya que en este ambiente se pueden aprovechar las ventajas de IPv6. A nivel de router no hay fragmentación de paquetes, y esto sumado a los encabezados simplificados, repercutió en el rendimiento final.

10. Conclusiones

A modo de conclusión se puede observar que, según el estudio realizado para el presente trabajo, si se migrara la red a IPv6 se estima que más del 80 % de los equipos ya se encuentran preparados para soportar el nuevo protocolo y no presentarán problemas para conectarse a Internet utilizando esta nueva versión de IP. El 20 % restante irá disminuyendo progesivamente a corto plazo ya que dado el rápido avance de la tecnología los equipos que no soporten la nueva versión de IP quedarán obsoletos y serán desplazados por otros equipos compatibles. En el caso de los equipos que no entran en la categoría mencionada anteriormente, lo más recomendable sería actualizarse, de lo contrario sólo podrán navegar por sitios IPv4, los que irán disminuyendo progresivamente a medida que se masifique IPv6. Como método de direccionamiento se recomienda utilizar el basado en *Router Announcements* que corresponde al direccionamiento sin estado, ya que ofrece mayor compatibilidad con dispositivos y sistemas operativos antiguos, además basado en los anuncios de router los equipos pueden generar sus propias direcciones IP, las que al estar basadas en la dirección MAC hacen que éstas sean más variables y únicas, y esto ofrece mayor seguridad porque hace más difícil adivinar la dirección IP de un dispositivo para conectarse. Sin embargo, el direccionamiento sin estado no es recomendado en redes empresariales ya que presenta el problema de que al asignarse cada equipo una dirección IP de forma automática a partir de su propia dirección MAC no se tiene un control sobre dicha asignación de cada equipo, por lo que una persona no autorizada a la red podría lograr un acceso indebido a la misma y autoasignarse una dirección válida, lo que podría desembocar en posibles ataques a los usuarios de la red empresarial y a datos sensibles de la organización provocando un gran fallo y peligro de seguridad. Por lo mencionado anteriormente, para redes empresariales se recomienda utilizar direccionamiento con estado o *DHCPv6*.

De acuerdo a las pruebas realizadas a nivel de servicios se puede concluir que la mayoría de éstos son compatibles con IPv6 en los Sistemas Operativos más actuales. A nivel de Escuela los servicios se encuentran montados sobre servidores Linux o FreeBSD, lo que permite una fácil escalabilidad en cuanto a nuevas características que surjan en consecuencia de la migración de IPv4 a IPv6, ya que los mismos servicios que actualmente corren sobre IPv4 ahora lo podrán hacer sobre IPv6 con mínimos o nulos cambios en la configuración. Los servicios esenciales para navegar en Internet se encuentran disponibles en IPv6 (DHCP, DNS, HTTP, Proxy), lo que permite una adopción sin proble-

mas. Para servicios más específicos no se dispone de compatibilidad, aunque se está desarrollando en este momento, se puede emplear como solución un túnel local que reciba la conexión por IPv6 y la traduzca a IPv4.

En cuanto a las pruebas que se realizaron y los prototipos construidos que se utilizaron a modo de comparación entre IPv4 e IPv6 se pudo llegar a la conclusión de que IPv6 presentó mejores resultados en los tiempos de respuesta de dichas pruebas a través de Internet con respecto a IPv4, ya que de forma local (LAN) IPv4 fue quien se impuso observando pequeñas direfencias de tiempo. Esto puede ocurrir porque IPv6, en su estructura, aunque presenta un encabezado más simple que IPv4 es más largo debido a que las direcciones IP ocupan más espacio, por lo que al trabajar de forma local hay una penalización de rendimiento. Sin embargo a través de Internet los tiempos son mejores que IPv4 ya que se pueden aprovechar las ventajas de IPv6 en este sentido, ya que como que no hay fragmentación a nivel de router y posee encabezados simplificados, se reduce el procesamiento necesario por el enrutador para enviar el paquete al siguiente nodo y, por ende, mejora el rendimiento.

Para la seguridad inalámbrica se concluye que el método más conveniente a utilizar es WPA2-Enterprise, ya que permite registrar los usuarios que se encuentran conectados a la red y permite cifrar el tráfico que circula por el aire con claves distintas por usuario, por lo que si una cuenta es comprometida no afectará a los demás usuarios. A pesar de que este es el mejor método a utilizar para proteger la conexión inalámbrica, se tiene la desventaja del alto consumo de recursos, lo que disminuye notablemente el *throughput* en el caso de existir una baja cantidad de AP's disponibles para soportar la gran cantidad de tráfico generado. Debido a esto se concluye que sólo se utilizará como medida de seguridad en la Escuela el uso del actual Portal Cautivo, ya que es el método mas eficaz dadas las condiciones actuales de la Escuela y funciona correctamente, además de utilizar bajos recursos.

Finalmente como última conclusión se llevará a cabo la implementación de IPv6 en la Escuela de Ingeniería Informática de la PUCV a través de un túnel IPv6, para luego distribuirlo utilizando la modalidad *Dual-Stack* junto a la conexión IPv4 actual. Esto se debe a que la implementación de IPv6 nativo en la Escuela de Informática aún no es posible por razones de presupuesto de la Universidad y sólo se tiene actualmente acceso nativo desde la Casa Central de la PUCV en los laboratorios de la DSIC. Dado el caso anterior, se puede concluir que se implementará IPv6 en la Escuela de Informática a través de un túnel, ya que a pesar de trabajar a través de dicho túnel presenta una mejoría en el rendimiento con respecto a IPv4, además de la cantidad de ventajas presentadas a lo largo del presente trabajo.

Referencias

[1] Ipv6 specification rfc 2460. http://tools.ietf.org/html/rfc2460#section-3, visitado 07/06/2012.

[2] Ipv6 mysql server config. http://dev.mysql.com/doc/refman/5.5/en/ipv6-server-config.html, visitado 11/09/2012.

[3] Openvpn ipv6 compatibility. http://openvpn.net/index.php/open-source/faq/77-server/287-is-ipv6-support-plannedin-the-works.html, visitado 11/09/2012.

[4] Samba ipv6 support. http://www.samba.org/samba/history/samba-3.2.0.html, visitado 11/09/2012.

[5] Captive portal ipv6 support pfsense. http://redmine.pfsense.org/issues/1831, visitado 12/09/2012.

[6] dovecot ipv6 support. http://wiki.dovecot.org/MainConfig, visitado 14/09/2012.

[7] Postfix ipv6 support. http://www.postfix.org/IPV6_README.html, visitado 14/09/2012.

[8] Hurricane electric. http://www.tunnelbroker.com, visitado 15/04/2012.

[9] Ipv6 dfp visibility. http://www.sixxs.net/tools/grh/dfp/all/?country=cl, visitado 15/06/2012.

[10] World ipv6 day 2011. http://en.wikipedia.org/wiki/World_IPv6_Day, visitado 17/04/2012.

[11] Dhcpv6 rfc. http://tools.ietf.org/html/rfc3315, visitado 18/04/2012.

[12] Full ipv6 android support issue. http://code.google.com/p/android/issues/detail?id=3389, visitado 18/04/2012.

[13] ios ipv6 support from 4. http://isc.sans.edu/diary.html?storyid=9058, visitado 18/04/2012.

[14] Hurricane electric. http://tunnelbroker.net, visitado 23/11/2012.

[15] Ipv6, la nueva version de internet. http://www.dgc.usm.cl/2010/08/16/ipv6-la-nueva-version-de-internet/, visitado 09/04/2012.

[16] Rango de ipv6 asignado por lacnic. http://lacnic.net/cgi-bin/lacnic/whois?lg=SP&query=2800:460::/32, visitado 15/04/2012.

[17] Reuna entro de lleno en la era del ipv6. http://www.reuna.cl/index.php/es/noticias-nuestros-socios/1494-reuna-entro-de-lleno-en-la-era-del-ipv6-, visitado 09/04/2012.