UNIVERSIDAD DE CHILE
FACULTAD DE CIENCIAS FÍSICAS Y MATEMÁTICAS
DEPARTAMENTO DE INGENIERÍA ELÉCTRICA

ESTRATEGIA PARA ABORDAR EL PROCESO DE ADOPCIÓN DE IPV6 EN REDES EMPRESARIALES

MEMORIA PARA OPTAR AL TÍTULO DE INGENIERO CIVIL ELECTRICISTA

RODRIGO ALEJANDRO ALARCÓN REYES

PROFESOR GUÍA:
JUAN GONZÁLEZ ZEPEDA

MIEMBROS DE LA COMISIÓN:
HÉCTOR AGUSTO ALEGRÍA
ÁLVARO SILVA MADRID

SANTIAGO DE CHILE

ABRIL 2010

RESUMEN DE LA MEMORIA
PARA OPTAR AL TÍTULO DE
INGENIERO CIVIL ELECTRICISTA
POR: RODRIGO ALARCÓN REYES
FECHA: 10/04/2010
PROF. GUÍA: SR. JUAN GONZÁLEZ ZEPEDA

"ESTRATEGIA PARA ABORDAR EL PROCESO DE ADOPCIÓN DE IPV6 EN REDES EMPRESARIALES"

La definición del protocolo IPv6 se perfila como la única solución a largo plazo para compensar la inminente escasez de direcciones IP a nivel mundial. Sin embargo, para lograr la adopción de este protocolo en las redes que actualmente operan sobre IPv4, se requiere de una estrategia que permita a una empresa proveedora de servicios de redes abordar este proceso de manera planificada.

Motivado por lo anterior, este trabajo tiene como objetivo identificar las variables que condicionan la factibilidad de adoptar IPv6 en redes empresariales y definir un procedimiento general para abordar el proceso de migración en este tipo de redes. De este modo, se busca que una empresa de servicios de redes esté preparada para apoyar la migración a IPv6 y que las empresas clientes tengan claridad sobre los requisitos que deben cumplir para la adopción del protocolo**.**

El trabajo comienza con un estudio de las ventajas que ofrece la adopción de IPv6, considerando sus características técnicas y su actual soporte por aplicaciones y equipos de uso común en redes productivas. Posteriormente, se propone una estrategia para desarrollar un servicio de validación de compatibilidad con IPv6, orientada a redes empresariales. Esta estrategia contempla cuatro actividades: Levantamiento de la red del cliente, instalación de un laboratorio demostrativo de validación de IPv6, clasificación de los equipos y aplicaciones de la red en función de su compatibilidad con IPv6 y - por último - una evaluación económica de los requisitos necesarios para lograr una compatibilidad total.

Como complemento al servicio diseñado, se implementa en este trabajo el laboratorio demostrativo contemplado dentro del servicio de validación y además se propone una planilla para cuantificar los costos y beneficios asociados al proceso de migración, planilla que sirve de base para la evaluación económica incluida dentro del servicio. También se establecen recomendaciones generales sobre los aspectos a considerar por una empresa de servicios de redes en caso de llevar a cabo la migración a IPv6.

El resultado de este trabajo es una estrategia que permite abordar el proceso de adopción de IPv6 mediante un servicio de validación de compatibilidad orientado a redes empresariales. Este servicio ayuda a las empresas a planificar de manera anticipada la migración y les permite alinear los requisitos de actualización de hardware y software con sus procesos internos de renovación tecnológica.

A mis padres, hermanos y amigos.

Agradecimientos

Quiero comenzar este trabajo agradeciendo a mis padres por la formación recibida, por su enorme paciencia y por sus incansables esfuerzos personales a lo largo de estos años para permitirme llegar hasta este punto. Espero que el tiempo me permita retribuir sus sacrificios de buena manera.

También a los miembros de la comisión por el apoyo brindado durante el desarrollo de este tema, cada uno aportando desde su ámbito de acción. En particular, a Juan González, quien a lo largo de todo este *proceso* siempre manifestó la mejor disposición para resolver mis dudas y aconsejarme en los diversos aspectos del trabajo realizado.

Al mismo tiempo, quisiera reconocer la confianza depositada por la empresa Magenta Computación S. A. (actualmente *Dimension Data Chile*) al financiar esta memoria y permitirme utilizar sus dependencias, su equipamiento y la experiencia de su personal para llevarla a cabo. Reconocer también el aporte del ingeniero Cristián Jara, quien me propuso trabajar en este tema y me dio los tips para desarrollarlo de la mejor forma.

Finalmente, gracias a mis amigos y amigas de Beauchef por todos los buenos momentos vividos en nuestro paso por la Universidad. Mención especial para los miembros del *equipo*, para los Físicos Experimentales y para los distinguidos integrantes de la *ruta*.

Índice de Contenidos

Índice de Figuras

Índice de Tablas

Capítulo 1: Introducción

1.1 Motivación

El número de personas y equipos que se conectan a Internet y a distintas redes IP aumenta cada día. La necesidad de acceder a contenidos en línea independiente de la ubicación física del usuario, ha originado que actualmente no sólo los computadores de escritorio y portátiles permitan el acceso a Internet, sino que además la red de telefonía móvil esté convergiendo gradualmente hacia una red de paquetes, permitiendo ofrecer conectividad a través de distintos dispositivos móviles, tales como teléfonos inteligentes, PDA, módems, etc.

La consecuencia directa de este fenómeno es el agotamiento gradual de las direcciones IP requeridas para establecer la conectividad. Hasta ahora diversas técnicas se han utilizado para mitigar este agotamiento, las cuales se han basado principalmente en el uso de direcciones IP privadas y de traducción de direcciones mediante *Network Address Translation* (NAT) para permitir a un conjunto de usuarios compartir una única dirección IP pública. Sin embargo, incluso utilizando estas técnicas, actualmente menos del 10% de las direcciones IP se encuentran disponibles para ser asignadas [1] y se espera que para el año 2012 esta asignación sea total [2], lo que ocasionará que no existan direcciones para asignaciones futuras si se mantiene el actual esquema de direccionamiento.

La solución a largo plazo para la escasez de direcciones es actualizar el actual protocolo para direccionamiento (IP) de la versión 4 (IPv4) a la versión 6 (IPv6), la cual permite - entre otros beneficios - aumentar drásticamente la cantidad de direcciones disponibles. En este sentido, IPv6 ofrece la posibilidad de asignar hasta 2^{128} direcciones, lo que equivale a $6{,}5 \times 10^{23}$ direcciones por metro cuadrado de la Tierra, en contraste con IPv4 que sólo permite asignar 2^{32}

(aproximadamente 4.300 millones de direcciones en total, las que incluyen una cantidad considerable de direcciones no asignables a usuarios). Pero, como ambas versiones del protocolo IP no son compatibles entre sí, para adoptar IPv6 es necesario llevar a cabo un proceso de migración en las redes actuales, que permita a sus usuarios acceder simultáneamente a los contenidos disponibles en la red IPv4 existente y a los contenidos que se generen sobre IPv6.

Existen técnicas generales propuestas para el período de transición y coexistencia entre ambas versiones del protocolo IP [3], las que se resumen en mantener los equipos con soporte simultáneo de IPv4 e IPv6 (lo que se conoce como Doble Pila o *Dual Stack*) o bien crear túneles que encapsulen los paquetes IPv6 dentro de paquetes IPv4. Sin embargo, se requiere de una estrategia global que permita a una empresa proveedora de servicios de redes abordar este proceso para distintos tipos de clientes empresariales.

En este contexto, lo que se pretende en el presente trabajo es diseñar una estrategia que permita evaluar los equipos y aplicaciones existentes en una red empresarial, con el objetivo de determinar cuáles serán las inversiones que esta empresa debería realizar en una eventual adopción del protocolo IPv6**.**

Este trabajo nace bajo el patrocinio de la empresa de servicios de redes Magenta Computación S.A., con el interés de anticiparse a eventuales requerimientos de adopción de IPv6 por parte de sus clientes. Sin embargo, el trabajo desarrollado pretende ser una referencia para cualquier persona o institución interesada en contar con información actualizada sobre el protocolo y con recomendaciones generales para planificar su adopción.

1.1 Objetivos

1.1.1 Objetivos Generales

- Identificar las variables que permitan evaluar la factibilidad técnico-económica de realizar la migración de IPv4 a IPv6 en distintas redes empresariales.
- Definir un procedimiento para abordar el proceso de migración en redes empresariales.

1.1.2 Objetivos Específicos

- Estudiar las ventajas que brinda la implementación de IPv6 en redes empresariales.

- Evaluar la factibilidad de las aplicaciones y equipos de red más utilizados para soportar una migración IPv4 a IPv6.
- Estimar los recursos requeridos por parte de una empresa de servicios de redes para la migración IPv4-IPv6 de una red empresarial.
- Establecer una recomendación general para abordar el proceso de migración en redes empresariales, desde el punto de vista de una empresa de servicios de redes.

1.2 Alcances

El trabajo presentado en esta memoria se enfoca en el proceso de migración a IPv6 a nivel de equipamiento de redes empresariales y de aplicaciones de uso común alojadas en servidores internos de las empresas. Para estos efectos, se entenderá como red empresarial una red perteneciente a una empresa productiva, con no más de 2 sucursales y un número máximo de 200 usuarios.

Dentro de las aplicaciones y servicios a considerar, se exceptúan aquéllos orientados a la administración y supervisión de la red, debido a que su complejidad hace necesaria la ejecución de un proyecto exclusivo para abordar su actualización a IPv6.

Otro aspecto no considerado en este trabajo se relaciona con la programación interna de las aplicaciones utilizadas por la empresa, particularmente de las que han sido desarrolladas internamente, para soportar IPv6 en su código fuente. Respecto a este punto, es posible encontrar recomendaciones generales en [4].

1.3 Estructura de la memoria

La presente memoria está dividida en 7 capítulos, más anexos.

En el Capítulo 1 se presenta el contexto que motiva este trabajo y se describe y los objetivos a lograr durante su desarrollo.

El Capítulo 2 contiene los antecedentes teóricos necesarios para comprender las características técnicas de IPv4 e IPv6, incluyendo además la situación actual de IPv6 en Chile, enfocada en proyectos relevantes del punto de vista comercial y que se encuentran vigentes al momento de desarrollar la memoria.

En el Capítulo 3 se describen los aspectos que justifican la adopción del protocolo IPv6, considerando las características técnicas del protocolo y además el soporte que actualmente proveen distintas aplicaciones y equipos para su utilización.

En el Capítulo 4 se presenta la estrategia definida para evaluar la red de una empresa mandante, describiendo las actividades contempladas dentro del servicio y las actividades futuras en caso de que la empresa mandante decida contratar un proyecto de migración a IPv6.

El Capítulo 5 describe las configuraciones efectuadas en el laboratorio que se implementó para validar las funcionalidades del protocolo IPv6, el que además forma parte del servicio de evaluación presentado en el Capítulo 4.

El Capítulo 6 abarca los aspectos económicos del servicio ofrecido, proponiendo una planilla que permite estimar los costos y beneficios asociados a un proyecto de adopción de IPv6.

Finalmente, en el Capítulo 7 se realiza una discusión del trabajo realizado y se presentan las conclusiones obtenidas al término de este trabajo, además de las tareas pendientes y propuestas para complementarlo a futuro.

Capítulo 2: Antecedentes[1]

2.1 Modelo OSI y TCP/IP

2.1.1 El Modelo OSI

El comité para la estandarización ISO creó un listado de todas las funciones de red requeridas para el envío de datos y las dividió en siete categorías. Este modelo se conoce como el modelo OSI de siete capas, el cual fue publicado en 1984 y se muestra en la Figura 2.1.

Figura 2.1: Capas del Modelo OSI

Las siete capas pueden ser clasificadas en dos grandes grupos: las capas superiores (capas 5 a la 7) y capas inferiores (capas 1 a la 4). Las capas superiores se preocupan de asuntos relacionados con la aplicación, como la interfaz con el usuario o el formato de los datos. Las capas inferiores, en cambio, se preocupan de asuntos relacionados con el transporte, por ejemplo

[1] Los antecedentes incluidos desde la sección 2.1 hasta la sección 2.4 de este capítulo están basados en las referencias [25], [26], [27] y [28].

cómo los datos atraviesan la red y las características físicas de la red. Para comunicarse e intercambiar información las capas utilizan PDU (*Protocol Data Units*), las cuales mantienen información de control junto a los datos en cada capa del modelo.

Las principales funciones de cada capa, así como la designación de su PDU, se indican en la Tabla 2.1.

Tabla 2.1: Funciones de las capas del modelo OSI

Capa	Descripción Funcional	PDU
Aplicación	Interfaz entre la red y el software de aplicación.	L7PDU
Presentación	Define cómo los datos son representados. Define procesamiento especial, como la encriptación de datos.	L6PDU
Sesión	Establece, mantiene y finaliza las sesiones de comunicación entre aplicaciones ejecutándose en distintos hosts.	L5PDU
Transporte	Conexiones extremo a extremo entre origen y destino, confiables o no-confiables. Provee los servicios de red a las capas superiores.	Segmento
Red	Provee direccionamiento lógico para el ruteo de los datos a través de la red lógica.	Paquete
Enlace	Provee el direccionamiento físico e indica la forma de acceder al medio físico, incluyendo control de flujo y manejo de errores.	Frame
Física	Define especificaciones eléctricas y mecánicas necesarias para la activación, mantención y desactivación del enlace físico entre equipos.	Bits

2.1.2 El modelo TCP/IP

El modelo TCP/IP fue creado por el Departamento de Defensa (en inglés, DoD) de los Estados Unidos para asegurar y preservar la integridad de los datos, así como mantener las comunicaciones, en el evento de una guerra catastrófica. Este modelo es básicamente una versión condensada del modelo OSI, el cual está compuesto de cuatro capas en vez de siete. En la Figura 2.2 se observan las capas del modelo TCP/IP y su comparación con el modelo OSI.

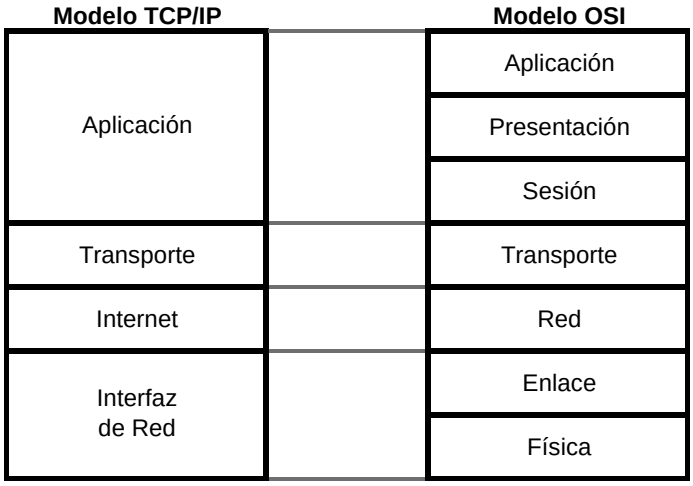


Figura 2.2: Modelo TCP/IP y Modelo OSI

2.2 El Protocolo IP (IPv4)

El protocolo IP es el protocolo definido en el modelo TCP/IP para la capa de Internet (capa 3 del modelo OSI). Es un protocolo no-orientado a la conexión, el cual provee la entrega de paquetes hacia la red mediante *best-effort delivery* (entrega con el mejor esfuerzo). Para esto, una única dirección IP (dirección lógica) se asigna a cada interfaz y cada equipo dentro de la red.

Hoy en día, la versión más ampliamente utilizada del protocolo IP es la versión 4. Sin embargo, como se verá en la Sección 2.3, la versión 6 del protocolo ya se encuentra definida.

2.2.1 Cabecera IP

La Figura 2.3 ilustra la estructura de un paquete IP, incluyendo la longitud en bits de cada campo. La cabecera estándar tiene un largo de 20 bytes, aunque si se incluyen opciones este largo puede ser variable. A continuación se describe cada uno de los campos de esta cabecera:

Versión (*Version*):

Identifica la versión del protocolo IP. En este caso, versión 4.

Longitud de cabecera (*Header length*):

El número de palabras de 32 bits en la cabecera (incluyendo opciones).

Tipo de Servicio (*Type of Service (ToS)*):

Identifica cómo debería ser manejado el paquete dentro de la red. Estos bits marcan el tráfico para una calidad de servicio (QoS) específica.

Longitud Total (*Total Length*):

Especifica el largo del paquete, incluyendo cabecera y datos.

Identificación (*Identification*), etiquetas (*flags*) y desplazamiento del fragmento (*fragment offset*):

Manejan casos donde un datagrama de gran tamaño debe ser fragmentado - dividido en múltiples paquetes - para atravesar una red que no puede manejar datagramas de dicho tamaño.

Tiempo de vida (*Time to Live (TTL)*):

Se asegura que los paquetes no circulen indefinidamente en la red. Este campo debe ser decrementado en 1 por cada router que el paquete atraviesa, es decir, por cada *salto* en la red.

Protocolo (*Protocol*):

Indica el protocolo de capa superior para el cual son los datos. Por lo tanto, este campo indica el tipo de segmento que el paquete está encapsulando, de manera similar a como el puerto de los segmentos TCP y UDP indica el tipo de aplicación a la que corresponde el segmento. Un valor igual a 6 indica que el paquete está encapsulando un segmento TCP, mientras que un valor igual a 17 indica que se está encapsulando un segmento UDP. Este campo puede además tener otros valores, por ejemplo en caso de que se esté encapsulando tráfico correspondiente a algún protocolo de ruteo dentro del paquete.

Suma de comprobación de cabecera (*Header Checksum*):

Se asegura de que la cabecera sea recibida correctamente.

Dirección IP de origen y destino (*Source* y *destination IP address*):

Dirección IP lógica asignada al origen y destino del paquete, respectivamente.

Opciones (*Options*):

Utilizado para pruebas de red y *troubleshooting*, con longitud de múltiplos de 32 bits.

Datos (*Data*):

Los datos de capa superior (capa de transporte).

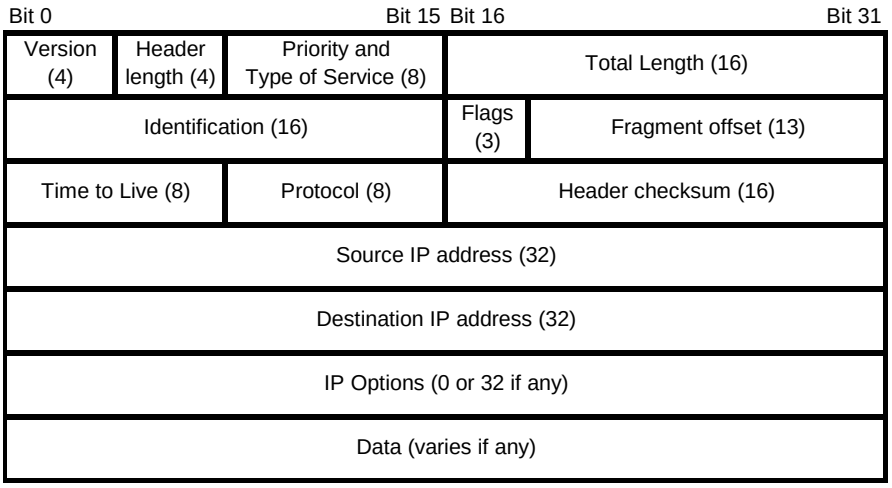


Figura 2.3: Estructura de la cabecera IPv4

2.2.2 Direccionamiento

Las direcciones IP son números de 32 bits representados como 4 octetos (8 bits cada uno), separados por puntos y representados con un número decimal entre 0 y 255.

Ejemplo: 192.168.100.5

2.2.3 Clases de direcciones IP

El primer octeto de la dirección IP define la clase a la que pertenece la dirección, existiendo cinco clases: A, B, C, D y E. Sólo las direcciones de Clase A, B y C se utilizan para direccionar equipos. La Clase D se utiliza para grupos de *multicast* y la Clase E está reservada para uso experimental.

La clase a la que pertenece una dirección define qué parte de la dirección representa los bits de red y qué parte representa los bits de host, como se muestra en la Tabla 2.2 para las direcciones de Clase A, B y C. En la columna Formato, los octetos que representan a la red se identifican con una N, mientras que los de host se identifican con una H. En la tabla se presenta además el número de redes disponibles en cada clase y el número de hosts por cada red.

Se debe notar que las direcciones de Clase A son todas aquellas cuyo bit más significativo es igual a 0. Esto incluiría a las que tienen un valor 0 al 127 en su primer octeto. Sin embargo, la red 0.0.0.0 está reservada y las redes que empiezan con 127 están reservadas para funcionalidades de bucle de retorno (*loopback*). Por esta razón, el rango de valores del primer octeto para direcciones de Clase A es desde el 1 al 126.

Tabla 2.2: Descripción de direcciones de Clase A, B y C

Clase	Formato	Bits más significativos	Rango de direcciones	Número de redes	Número de hosts por red
A	N.H.H.H	0	1.0.0.0 - 126.0.0.0	126	16.777.214
B	N.N.H.H	10	128.0.0.0 - 191.255.0.0	16.386	65.534
C	N.N.N.H	110	192.0.0.0 - 223.255.255.0	2.097.152	254

Las direcciones Clase D tienen sus bits más significativos en el valor 1110 y están en el rango de 224.0.0.0 al 239.255.255.255. Por su parte, las direcciones Clase E tienen sus bits más significativos en el valor 1111 y están en el rango de 240.0.0.0 al 255.255.255.255.

A modo de ejemplo, la dirección IP 192.168.100.5 es una dirección Clase C. Por lo tanto, la parte que identifica a la red es 192.168.100, mientras que la porción de la dirección que identifica al host dentro de la red es 5.

2.2.4 Direcciones IP públicas y privadas

El espacio de direcciones IPv4 se divide en una sección pública y una sección privada. Las direcciones privadas son direcciones reservadas para ser utilizadas solamente en forma interna dentro de la red de una compañía y no hacia Internet. Cuando se requiere enviar algún dato hacia Internet, las direcciones privadas deben ser mapeadas a una dirección externa registrada para la compañía (mediante el uso de NAT). Para este efecto se proveen direcciones IPv4 públicas para la comunicación externa.

Los rangos definidos para las direcciones IPv4 privadas son los que se indican a continuación:

- 10.0.0.0 al 10.255.255.255
- 172.16.0.0 al 172.31.255.255
- 192.168.0.0 al 192.168.255.255

Todas las direcciones restantes son direcciones IP públicas.

2.2.5 Subredes

Como se ilustró en la Tabla 2.2, las direcciones Clase A tienen poco uso en una organización normal, debido a la excesiva cantidad de hosts que son permitidos por estas

direcciones. Debido a esta limitación en la cantidad de direcciones cuando sólo se considera su clase (llamada direccionamiento *classful*) y al reducido rango de dichas direcciones (1 al 127), se introdujo el concepto de subredes.

Las direcciones Clase A, B y C pueden ser divididas en redes más pequeñas, denominadas subredes, resultando en un número mucho más grande de redes posibles, cada una con una menor cantidad de hosts disponibles que la red original.

Las direcciones utilizadas para las subredes se forman quitando bits del campo de host y utilizándolos como bits de subred, mediante una máscara. La máscara de subred es un valor de 32 bits asociado a la dirección IP que especifica cuáles de los bits de la dirección representan bits de red y subred y cuáles representan bits de host. El uso de la máscara de subred permite una jerarquía de 3 niveles: red, subred y host. La máscara de subred por defecto para las direcciones Clase A, B y C se muestra en la Tabla 2.3.

Cuando todos los bits de host de una dirección están en 0, la dirección corresponde a la subred misma. Cuando todos los bits de host están en 1, la dirección corresponde a la dirección de broadcast de la subred, es decir, para todos los equipos de la subred.

Tabla 2.3: Máscara de subred por defecto para direcciones IP

Clase	Máscara por defecto en binario	Máscara por defecto en decimal
A	11111111.00000000.00000000.00000000	255.0.0.0
B	11111111.11111111.00000000.00000000	255.255.0.0
C	11111111.11111111.11111111.00000000	255.255.255.0

Otra forma de indicar la máscara de subred es usar un prefijo. Un prefijo es un slash (/) seguido por un número que representa el número de bits de la porción de red y subred de la dirección IP, en otras palabras, el número de 1's consecutivos en la máscara de subred. Por ejemplo, la máscara 255.255.240.0 es 11111111.11111111.11110000.00000000 en binario, lo que equivale a 20 1's seguidos de 12 0's. Por lo tanto, el prefijo de subred en este caso sería /20 por los 20 bits correspondientes a la porción de red y subred (el número de 1's en la máscara).

2.3 Protocolo IPv6

Debido a que IPv4 sólo permite un máximo teórico de $4{,}3 \times 10^9$ direcciones, lo cual restringe el crecimiento de Internet, se definió en 1998 la versión 6 de este protocolo [5]. Las principales características que incorpora IPv6 son:

Mayor espacio de direcciones

El gran espacio de direcciones (3.4×10^{38}) facilita la agregación de bloques de direcciones en Internet, estableciendo jerarquías de direcciones en función de la red, ISP, información geográfica, etc.

Se elimina la necesidad de traducción de direcciones (NAT/PAT)

Debido a que en todos los equipos se pueden utilizar direcciones únicas registradas globalmente.

Multihoming

IPv6 posibilita que los hosts tengan múltiples direcciones IP y que las redes tengan múltiples prefijos. Esto permite a los sitios tener conexiones a distintos ISP sin alterar la tabla de ruteo global.

Mejoras en privacidad y seguridad

Los hosts IPv6 soportan IPSec (conjunto de protocolos para aplicaciones seguras sobre IP) de forma nativa con IPv6, lo que resulta de utilidad para túneles VPN. Para esto se incluyen cabeceras de seguridad opcionales (AH, ESP) como parte del estándar.

Mejoras en la cabecera

Una cabecera simplificada de tamaño fijo hace más eficiente su procesamiento respecto a la cabecera de tamaño variable de IPv4. Esto se complementa con el hecho de que los routers ya no deben recalcular un *checksum* de cabecera IP para cada paquete, pues este campo ha sido removido en IPv6.

Por otra parte, en IPv6 se incluye una etiqueta de flujo que permite identificar paquetes enviados sobre la misma conexión TCP o datagramas UDP.

Capacidades de movilidad

IPv6 Móvil *(Mobile IPv6)* [6] permite que un nodo cambie su ubicación dentro de una red IPv6 manteniendo sus conexiones existentes, independiente de la ubicación física.

2.3.1 Estructura del protocolo IPv6

La estructura de la cabecera de un paquete IPv6 se especifica en [5]. La cabecera tiene una longitud fija de 40 bytes. Los dos campos para dirección de Origen y Destino utilizan 16 bytes (128 bits) cada uno, de modo que sólo existen 8 bytes para información general de la cabecera. De esta manera, la cabecera IPv6 es mucho más simple y sencilla que la cabecera IPv4, permitiendo un procesamiento más eficiente y, como se verá, más flexible a la hora de extender el protocolo para satisfacer necesidades futuras.

2.3.1.1 Estructura general de la cabecera

En IPv6 se han removido cinco campos de la cabecera IPv4. Estos son:

- Longitud de cabecera.
- Identificación.
- Etiquetas.
- Desplazamiento del fragmento.
- Suma de comprobación de la cabecera.

El campo Longitud de cabecera fue removido porque no es necesario en una cabecera con longitud fija. En IPv4, la longitud mínima de cabecera es 20 bytes, pero si se añaden opciones puede ser extendida en incrementos de 4 bytes hasta llegar a 60 bytes. En cambio, en IPv6 las opciones se definen en cabeceras de extensión.

Los campos Identificación, Etiquetas y Desplazamiento del fragmento manejan la fragmentación de un paquete en la cabecera de IPv4. En IPv6, si un host quiere fragmentar un paquete, debe utilizar una cabecera de extensión para este propósito. En este caso los routers en la ruta de un paquete no proveen fragmentación como en IPv4, de modo que los campos antes mencionados fueron removidos de la cabecera IPv6 y deben ser insertados en la cabecera de extensión en caso de ser requeridos por el host de origen.

El campo Suma de comprobación de la cabecera fue removido para mejorar la velocidad de procesamiento en los routers. Cuando IPv4 fue desarrollado, no era común realizar un *checksum* en la capa de acceso al medio (capa 2), lo que justificaba un *checksum* en la cabecera IPv4. Hoy en día, el riesgo de errores no detectados y paquetes mal ruteados es mínimo. Existe además un *checksum* que se realiza en la capa de transporte (TCP y UDP). Como consecuencia, so en IPv4 el checksum para UDP era opcional, con IPv6 éste es obligatorio. De este modo, se reafirma el hecho de que IP es un protocolo de *best-effort delivery*, por lo que es responsabilidad de las capas superiores asegurar la integridad del contenido.

A continuación se describen los campos de la cabecera de IPv6, los cuales se pueden observar en la Figura 2.4, incluyendo la longitud en bits de cada campo.

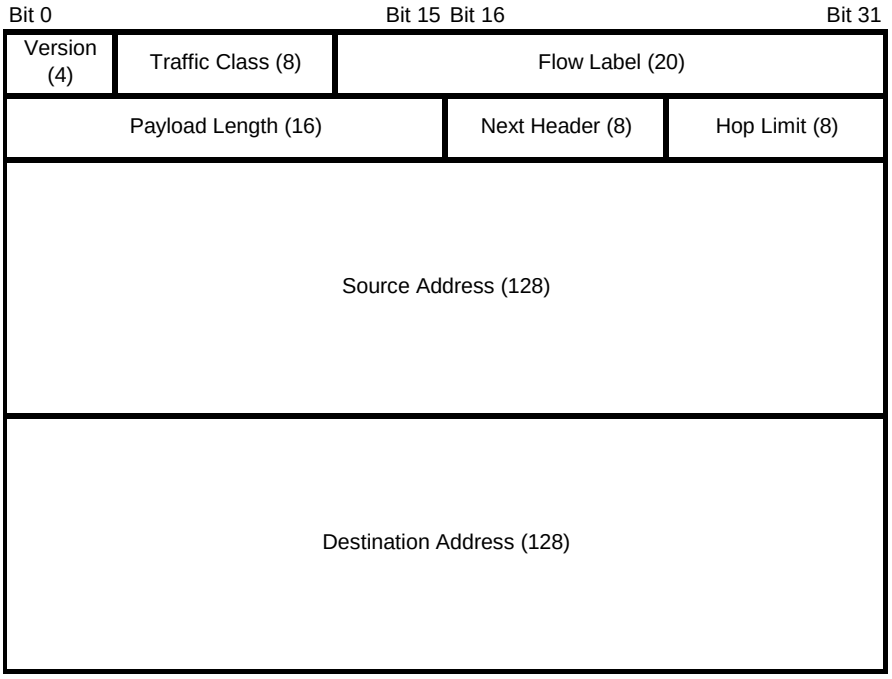


Figura 2.4: Estructura de cabecera IPv6

Versión (*Version*):

Contiene la versión del protocolo. En el caso de IPv6, el número es 6.

Clase de Tráfico (*Traffic Class*):

Reemplaza al campo ToS de IPv4. Facilita la manipulación de datos de tiempo real y cualquier otro tipo de datos que requiera un tratamiento especial. Puede ser utilizado por nodos

de origen o routers de paso para identificar y distinguir entre distintas clases o prioridades de paquetes IPv6.

Etiqueta de Flujo (*Flow Label*):

Este campo distingue paquetes que requieren el mismo tratamiento de modo de facilitar la manipulación de tráfico de tiempo real. Un host que origina tráfico puede etiquetar secuencias de paquetes con un set de opciones. Los routers llevan un registro de flujos y pueden procesar paquetes pertenecientes al mismo flujo de manera más eficiente, puesto que no tienen que reprocesar la cabecera de cada paquete. La etiqueta de flujo y la dirección del nodo de origen identifican de manera unívoca al flujo.

Longitud de carga útil (*Payload Length*):

Este campo especifica la carga útil (*payload*), esto es, la longitud de los datos contenidos después de la cabecera IP, a diferencia del campo Longitud Total en IPv4 que incluye además el largo de la cabecera IPv4. Las cabeceras de extensión son consideradas parte del *payload* y, por lo tanto, también se incluyen en el cálculo.

El hecho de que este campo tenga 2 bytes limita el tamaño del *payload* a un máximo de 64 Kilobytes. IPv6 tiene una cabecera de extensión que permite soportar paquetes de mayor tamaño en caso de ser necesario (para enlaces con un MTU mayor a 64 KB), los cuales se denominan Jumbogramas.

Siguiente Cabecera (*Next Header*):

En IPv4 este campo se denomina Protocolo, pero fue renombrado en IPv6 para reflejar la nueva organización de paquetes IP. Si la siguiente cabecera corresponde a TCP o UDP, este campo contendrá los mismos números de protocolo que en IPv4 (por ejemplo, 6 para TCP y 17 para UDP). Pero si se utiliza IPv6 con cabeceras de extensión este campo contiene el tipo de la siguiente cabecera. Las cabeceras de extensión se ubican entre la cabecera IP y la cabecera TCP o UDP.

Los números asociados a este campo son compatibles con los asignados al campo Protocolo en IPv4.

Límite de Saltos (*Hop Limit*):

Este campo es análogo al campo TTL en IPv4. El campo TTL contiene un número de segundos, indicando cuánto tiempo puede permanecer un paquete en la red antes de ser descartado. En IPv4, la mayoría de los routers simplemente decrementan este valor en uno por cada salto. Por esta razón el campo ha sido renombrado como Límite de Saltos en IPv6, expresando un número de saltos en vez de un número de segundos. Si un router recibe un paquete con un Límite de Saltos de 1, lo decrementa a 0, descarta el paquete y envía el mensaje ICMPv6 "*Hop Limit exceeded in transit*" al host de origen.

Dirección de Origen (*Source Address*):

Contiene la dirección IP del nodo que origina el paquete.

Dirección de Destino (*Destination Address*):

Contiene la dirección IP del nodo que se pretende que reciba el paquete. Esta dirección puede ser la del host de destino final o si, por ejemplo, la cabecera de extensión de ruteo está presente, la dirección del router del siguiente salto.

2.3.1.2 Cabeceras de extensión

La cabecera de IPv4 puede ser extendida desde un mínimo de 20 bytes hasta un máximo de 60 bytes para especificar opciones tales como Opciones de Seguridad, Ruteo de Origen o Marca de Tiempo. Esta capacidad rara vez ha sido utilizada debido a los problemas de desempeño que origina. Por ejemplo, las implementaciones de ruteo de IPv4 basadas en hardware necesariamente tienen que pasar el paquete con opciones a un procesador principal (manipulación por software).

IPv6 presenta una nueva manera de incorporar opciones que mejora de manera sustancial su procesamiento, incluyéndolas en cabeceras adicionales denominadas cabeceras de extensión (*Extension Headers*). Estas cabeceras se insertan en el paquete sólo si las opciones son necesarias.

La especificación actual de IPv6 define seis cabeceras de extensión:

- Opciones Salto por Salto (*Hop-by-Hop Options*)
- Ruteo (*Routing*)

- Fragmentación (*Fragment*)
- Opciones de Destino (*Destination Options*)
- Autenticación (*Authentication*)
- Carga util de seguridad cifrada (*Encapsulated Security Payload*)

En un paquete IPv6 puede haber una, más de una o ninguna cabecera de extensión. Estas se ubican entre la cabecera IPv6 y la cabecera del protocolo de capa superior. Cada cabecera de extensión se identifica por el campo Siguiente Cabecera de la cabecera que la precede.

Las cabeceras de extensión son examinadas o procesadas sólo por el nodo definido en el campo Dirección de Destino de la cabecera IPv6. Si este campo es una dirección de *multicast*, las cabeceras son examinadas y procesadas por todos los nodos pertenecientes al grupo de *multicast*. Las cabeceras de extensión deben ser procesadas estrictamente en el orden en que aparecen en el paquete.

Existe una excepción a la regla de que sólo el nodo de destino debe procesar una cabecera de extensión. Si esta cabecera es de tipo Opciones Salto por Salto, la información aquí incluida debe ser examinada y procesada por cada nodo en la ruta del paquete. La cabecera Opciones Salto por Salto, si está presente, debe ubicarse inmediatamente a continuación de la cabecera IPv6, lo que se indica por un valor 0 en el campo Siguiente Cabecera de esta última cabecera.

Esta arquitectura es muy flexible para desarrollar cabeceras para usos futuros a medida que sean necesarios, sin cambiar la cabecera IPv6. Un ejemplo de esto es la cabecera denominada Cabecera de Movilidad, definida para *Mobile* IPv6 [6].

El largo de cada cabecera de extensión es un múltiplo de 8 bytes, de modo que las cabeceras consecutivas siempre pueden ser alineadas. Si un nodo requiere procesar la cabecera siguiente pero no puede identificar el valor en el campo Siguiente Cabecera, deberá descartar el paquete y enviar un mensaje ICMPv6 "*Parameter problem*" al nodo que originó dicho paquete.

Si se utiliza más de una cabecera de extensión en un paquete, debería utilizarse el siguiente orden [5]:

1. Cabecera IPv6
2. Opciones Salto por Salto

3. Opciones de Destino (para opciones a ser procesadas por el primer destino que aparece en el campo Dirección de Destino de IPv6 y en los destinos consecutivos definidos en la cabecera de Ruteo)

4. Ruteo

5. Fragmentación

6. Autenticación

7. Carga util de seguridad cifrada

8. Opciones de Destino (para opciones a ser procesadas sólo por el destino final del paquete)

9. Cabeceras de capa superior

2.3.2 Direccionamiento[1]

Las direcciones IPv6 tienen una longitud de 128 bits y, a diferencia de IPv4, utilizan una notación hexadecimal. Existen tres formas convencionales de representar direcciones IPv6:

Forma 1: Forma de uso general

Se escriben los 16 bytes (128 bits) de una dirección IPv6 como ocho bloques de cuatro dígitos hexadecimales, separados los bloques por dos puntos. Ejemplos:

- FEDC:BA98:7654:3210:FEDC:BA98:7654:3210
- 8000:0000:0000:0000:0123:4567:89AB:CDEF
- 1080:0:0:0:8:800:200C:417A

Cabe notar que no es necesario escribir todos los ceros iniciales de un bloque hexadecimal individual, pero debe existir al menos un número en cada bloque hexadecimal.

Forma 2: Compresión de ceros

Para comprimir la representación de los ceros dentro de las direcciones IPv6 se definen dos optimizaciones:

1. Los ceros a la izquierda de un bloque hexadecimal pueden omitirse, pero debe existir al menos un número en cada bloque hexadecimal.

[1] La información estandarizada sobre el direccionamiento en IPv6 se encuentra en [33]

2. Pueden reemplazarse uno o más bloques seguidos de 16 ceros por un par de signos de dos puntos, "::".

El símbolo "::" puede ser usado también para comprimir los ceros iniciales o finales en una dirección IPv6. En cualquier caso, el símbolo "::" puede aparecer una sola vez en una dirección. Ejemplos:

- 1080:0:0:0:8:800:200C:417A ⇔ 1080::8:800:200C:417A
- FF01:0:0:0:0:0:0:101 ⇔ FF01::101

Forma 3: Entorno mixto IPv4 e IPv6

En un entorno mixto con nodos IPv4 e IPv6, las direcciones IPv6 pueden ser representadas con una componente hexadecimal (propia de IPv6) y una componente decimal (propia de IPv4), según la estructura:

x:x:x:x:x:x:d.d.d.d

x: valores hexadecimales de los seis campos de 16 bits de orden superior de la dirección.

d: valores decimales de los cuatro campos de 8 bits de orden inferior de la dirección.

Ejemplos:

- 0:0:0:0:0:0:13.1.68.3 ⇔ ::13.1.68.3
- 0:0:0:0:0:FFFF:129.144.52.38 ⇔ ::FFFF:129.144.52.38

A diferencia de IPv4, el direccionamiento IPv6 no considera la existencia de clases (se dice que es un protocolo *classless*). Por esta razón, para definir la porción de la dirección correspondiente a la red se utiliza directamente un prefijo, el cual indica cuántos de los bits más significativos de la dirección IPv6 corresponden a la red.

Las siguientes son representaciones válidas del prefijo de 60 bits 12AB00000000CD3:

- 12AB:0000:0000:CD30:0000:0000:0000:0000/60
- 12AB::CD30:0:0:0:0/60
- 12AB:0:0:CD30::/60

2.3.2.1 Tipos de direcciones IPv6

Dependiendo de la cantidad de interfaces representadas, se definen 3 tipos de direcciones:

Unienvío (*Unicast*)

Identifican a una sola interfaz, a la cual se entregan los paquetes enviados con esta dirección.

Envío a cualquiera (*Anycast*)

Identifican a un conjunto de interfaces (típicamente pertenecientes a distintos nodos), utilizando direcciones *unicast* normales. Un paquete enviado a una dirección *anycast* será entregado a una de las interfaces identificadas por esa dirección (generalmente la más cercana).

Multienvío (*Multicast*)

Identifican a un conjunto de interfaces dentro de la red. A diferencia de *anycast*, un paquete enviado a una dirección *multicast* será entregado a todas las interfaces identificadas por esa dirección.

Es importante destacar que en IPv6 no existen direcciones de *broadcast*, pues éstas han sido sustituidas por las direcciones *multicast*.

A su vez, para las direcciones IPv6 *unicast* existen actualmente 3 tipos de direcciones, dependiendo del ámbito de validez de la dirección. Estas son:

Unienvío Global o Globalmente Únicas (*Global Unicast*)

Direcciones públicas ruteables, similares a las direcciones públicas de IPv4.

Enlace Local (*Link-Local*)

Similares a las direcciones IPv4 privadas en el sentido de que no son ruteables públicamente. Sin embargo, estas direcciones tampoco son ruteables dentro de una red privada por lo que, como su nombre lo indica, son válidas sólo dentro de un mismo enlace físico.

Localmente Únicas (*Unique Local*)

Similares a las direcciones IPv4 privadas en el sentido de que no son ruteables públicamente. Son casi únicas globalmente, pero no se diseñaron con propósitos de ruteo global, sino para reemplazar a las direcciones *Site-Local* (obsoletas en Septiembre de 2004 [7]).

Los rangos hexadecimales asignados a cada una de las direcciones antes descritas se indican en la Sección 2.3.2.2.

2.3.2.2 Direcciones IPv6 especiales

Existen algunas direcciones y rangos de direcciones IPv6 reservadas para propósitos particulares. Las más relevantes se muestran en la Tabla 2.4.

Tabla 2.4: Direcciones IPv6 especiales

Prefijo o dirección	Tipo de Dirección
0:0:0:0:0:0:0:0 (::0/128)	No especificada
0:0:0:0:0:0:0:1 (::1/128)	Loopback
2000::/3	Global Unicast
FE80::/10	Link-local
FD00::/8	Unique local
FF00::/8	Multicast
2001:0DB8::/32	Ejemplos y documentación
2002::/16	Utilizada para túneles 6to4
2001:0::/32	Utilizada para túneles Teredo
x:x:x:x:0:5EFE:d.d.d.d	Utilizada para túneles ISATAP
FEC0::/10	Site-Local Unicast (obsoleto)

2.3.3 Estrategias de asignación de direcciones IPv6

Al igual que en IPv4, el protocolo IPv6 permite la asignación de direcciones tanto de forma estática como de forma dinámica, como se indica a continuación:

2.3.3.1 Asignación estática

De manera similar a la asignación estática de direcciones IPv4, el administrador de la red ingresa manualmente los parámetros relevantes (dirección IPv6, puerta de enlace, servidores DNS, etc.) a cada equipo de la red.

2.3.3.2 Asignación dinámica

La asignación dinámica de direcciones IPv6 se basa en alguna de las siguientes modalidades:

Dirección de Enlace Local

El equipo configura su propia dirección *link-local* de forma autónoma, usando el prefijo FE80::/10 y un identificador de 64 bits para la interfaz, con el formato EUI-64 modificado[1].

Autoconfiguración *stateless*

Un router en el mismo enlace anuncia - de forma periódica o tras un requerimiento de algún equipo - información sobre la red, tal como el prefijo de 64 bits de la red local y su intención de funcionar como el router por defecto para ese enlace. Para esto el router hace uso de un mensaje ICMPv6 "*Router Advertisement*" (RA).

Los equipos pueden generar automáticamente su dirección IPv6 global utilizando el prefijo anunciado en estos mensajes y el formato EUI-64 modificado para los últimos 64 bits, sin necesidad de una configuración manual o del uso de un servidor DHCP.

Esta modalidad es la que le da a IPv6 su característica de protocolo *plug-and-play*.

Configuración *stateful* usando DHCP para IPv6 (DHCPv6)

DHCPv6 es una versión actualizada del protocolo DHCP definido para IPv4. DHCPv6 permite al administrador un mayor nivel de control que la autoconfiguración *stateless* y puede ser utilizado para distribuir otra información (por ejemplo, la dirección del servidor DNS o la pertenencia a un dominio de red). El protocolo DHCPv6 utiliza direcciones *multicast* reservadas para su operación.

[1] Una descripción del formato EUI-64 modificado se puede encontrar en el Anexo A.

Cabe mencionar que las modalidades antes descritas no son excluyentes. Debido a que una interfaz puede tener simultáneamente múltiples direcciones IPv6, es posible que el equipo se asigne automáticamente una dirección de tipo *link-local* y además una dirección global mediante autoconfiguración *stateless* o mediante un servidor DHCPv6. Más aun, es posible utilizar la autoconfiguración *stateless* y, de forma complementaria, un servidor DHCPv6 para obtener la información que no es posible adquirir mediante esta autoconfiguración.

2.3.4 Protocolos de ruteo interior para IPv6

Para manejar la mayor longitud de las direcciones y las diferentes estructuras de cabecera de IPv6 con respecto a IPv4, fue necesario actualizar los protocolos de ruteo existentes para IPv4. A continuación se describen las principales características de los protocolos actualizados de uso más común.

2.3.4.1 *Routing Information Protocol, next generation* (RIPng)

RIPng es un protocolo de ruteo definido en [8], el cual está basado y funciona de forma similar a RIPv2 para IPv4. RIPng utiliza un mecanismo simple para determinar la métrica (costo) de una ruta, contando el número de routers hacia el destino, donde cada router cuenta como un salto. Las rutas con una distancia mayor o igual a 16 son consideradas inalcanzables.

RIPng utiliza IPv6 para el transporte de datos, usando una dirección de tipo *link-local* como dirección de origen y la dirección de *multicast* FF02::9 como dirección de destino para los mensajes de respuesta (análoga a la dirección de *multicast* 224.0.0.9 utilizada en IPv4 para este efecto en RIPv2). Además, a diferencia de RIPv2, ahora se utiliza una dirección de tipo *link-local* para identificar el router del siguiente salto en la tabla de ruteo generada.

2.3.4.2 *Enhanced Interior Gateway Routing Protocol* para IPv6 (EIGRPv6)

EIGRP para IPv6 es un protocolo propietario de Cisco para determinar rutas en una red, disponible a partir del Release 12.4[6]T de Cisco IOS (sistema operativo de Cisco para la configuración y operación de sus routers y switches). Funciona de manera similar a EIGRPv4, el cual es un protocolo de vector de distancias más sofisticado que RIP, que utiliza además un algoritmo denominado DUAL para obtener una convergencia rápida y libre de loops en la tabla de ruteo.

Para enviar sus actualizaciones, EIGRPv6 utiliza la dirección de *multicast* FF02::A, dirección análoga a la dirección de *multicast* 224.0.0.10 usada en IPv4.

2.3.4.3 *Open Shortest Path First*, versión 3 (OSPFv3)

OSPF es un protocolo de estado de enlace que divide la red en áreas jerárquicas, dentro de las cuales se aplica el algoritmo Dijkstra para encontrar la ruta más corta entre dos puntos de la red. OSPFv3 es una nueva implementación de OSPF para IPv6 definida en [9], la cual utiliza los mismos mecanismos que OSPFv2 para IPv4, si bien los protocolos difieren internamente.

OSPFv3 utiliza IPv6 para el transporte de datos usando una dirección de tipo *link-local* como dirección de origen y las direcciones de *multicast* de destino FF02::5 y FF02::6 (análogas a las direcciones 224.0.0.5 y 224.0.0.6 usadas en IPv4).

Por sus características de implementación interna, OSPFv3 podría ser utilizado para rutear en cualquier protocolo de red, no sólo en IP.

2.4 Técnicas de transición de IPv4 a IPv6

A pesar de que IPv6 resuelve muchos problemas de IPv4, es impensable una migración de IPv4 a IPv6 de la noche a la mañana. Existen actualmente miles de millones de hosts utilizando IPv4 e, incluso si se quisiera realizar la migración, podría existir software o equipos aún sin soporte para IPv6. Por esta razón, se espera que este proceso se prolongue por varios años o incluso décadas.

Afortunadamente se han desarrollado diversos estándares sobre cómo abordar el proceso de migración o transición. Las principales opciones desarrolladas se pueden clasificar en:

- Doble Pila (*Dual Stack*)
- Túneles
- Traducción entre las dos versiones de IP con NAT-PT (obsoleta en Julio de 2007 [10])

2.4.1 *Dual Stack* IPv4/IPv6

Esta técnica consiste en la utilización simultánea de IPv4 e IPv6 en un host o router. Esto significa que un host tendrá asignada a su tarjeta de red una dirección IPv4 (para enviar paquetes a otros host IPv4) y una dirección IPv6 (para enviar paquetes a otros host IPv6). En el

caso de los routers, esto significa mantener tablas de ruteo y protocolos de ruteo para IPv4 y para IPv6, y ser capaz de procesar paquetes IPv4 e IPv6.

2.4.2 Túneles

La función de un túnel es tomar un paquete IPv6 enviado por un host y encapsularlo dentro de un paquete IPv4. Este paquete IPv4 puede ser enviado a través de la red IPv4 existente, hasta llegar a otro equipo que remueva la cabecera IPv4 para recuperar el paquete IPv6 original. El funcionamiento general de un túnel se puede observar en la Figura 2.5.

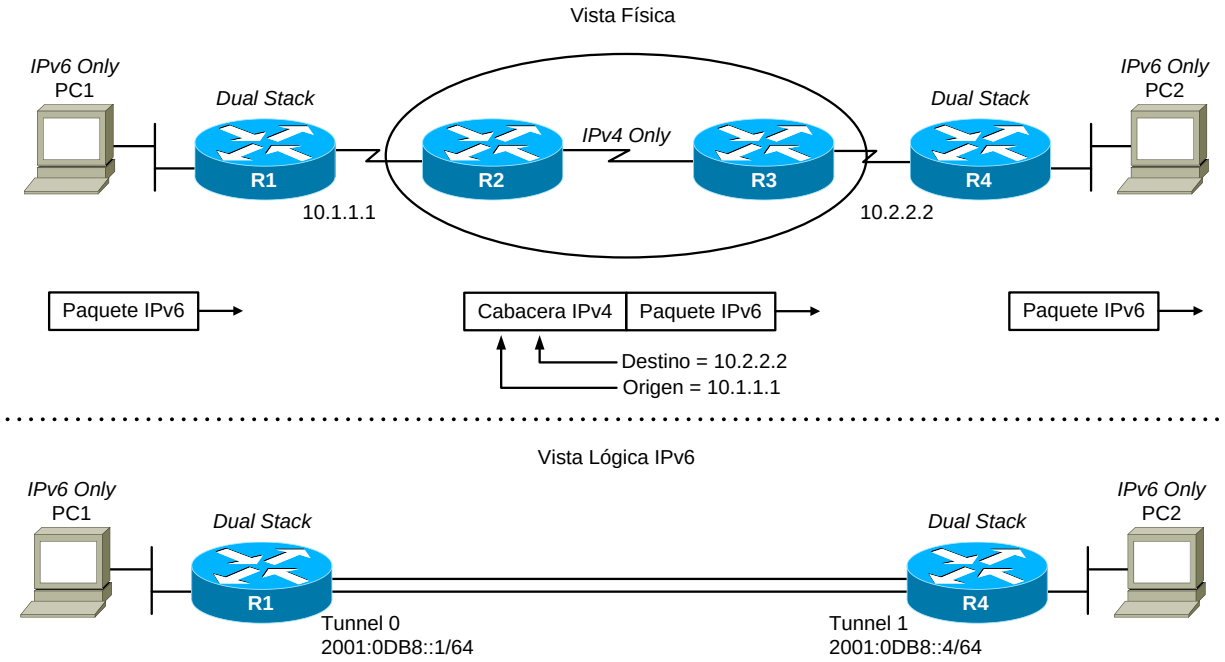


Figura 2.5: Ejemplo de un túnel IPv6-a-IPv4, vista física y lógica

Existen múltiples tipos de túneles, algunos de los cuales se describen a continuación:

Túneles configurados manualmente

Se configuran interfaces virtuales tipo túnel referenciando a la dirección IPv4 utilizada en la cabecera IPv4 que encapsula el paquete IPv6.

Túneles dinámicos 6to4

Un tipo específico de túneles creados dinámicamente, típicamente hecho en Internet, en que las direcciones IPv4 de los extremos del túnel pueden ser encontradas dinámicamente en base a la dirección IPv6 de destino.

***Intra-site Automatic Tunnel Addressing Protocol* (ISATAP)**

Otro tipo de túnel dinámico, típicamente usado dentro de una empresa. A diferencia de túneles 6to4, ISATAP no funciona si se utiliza NAT IPv4 entre los extremos del túnel.

Túneles Teredo

Este método permite a hosts con *dual stack* crear un túnel hacia otro host, realizando el proceso de encapsulación dentro del mismo host.

2.5 Asignación de direcciones IPv6 en Internet

Para obtener acceso a Internet, tanto las direcciones IPv4 como las IPv6 son generalmente asignadas de manera jerárquica. Los usuarios obtienen sus direcciones de un proveedor de servicios de Intenet o ISP (*Internet service provider*). Los ISP, a su vez, obtienen un conjunto de direcciones IP desde un registro local o nacional de Internet (LIR o NIR, respectivamente), o bien desde su registro regional de Internet o RIR (*Regional Internet Registry*).

La organización encargada de coordinar globalmente los sistemas de direccionamiento de IP es IANA (*Internet Assigned Numbers Authority*), quien además coordina los números de sistema autónomo utilizados para rutear tráfico en Internet. Esta organización asigna bloques de direcciones a los cinco RIR existentes mundialmente: AfriNIC para África, APNIC para la región Asia/Pacífico, ARIN para América del Norte, LACNIC para América Latina y el Caribe y RIPE NCC para Europa, Medio Oriente y Asia Central.

Para la asignación de direcciones IPv6 a usuarios finales, en [11] se recomienda en general la asignación de un prefijo /48. Un prefijo /64 puede ser asignado cuando se sabe que una única subred es requerida, mientras que un prefijo /128 (una única dirección) puede ser entregado cuanto se tiene certeza de que un único equipo será conectado a Internet.

2.6 Situación actual de IPv6 en Chile

2.6.1 Asignación de prefijos IPv6 en Chile

Tanto para IPv4 como para IPv6, la organización responsable de la asignación y administración de direcciones IP en Chile es LACNIC, el Registro de Direcciones de Internet para América Latina y Caribe. A la fecha de realización de este trabajo, los prefijos asignados por LACNIC para empresas y organizaciones chilenas son los que se indican en la Tabla 2.5 [12].

Tabla 2.5: Asignación de direcciones IPv6 en Chile

Prefijo	Institución	Fecha Asignación	Activa
2001:1310::/32	Red Universitaria Nacional	21-08-2003	SI
2001:1398::/32	NIC Chile	13-09-2005	SI
2800:8::/32	Netup S.A.	24-11-2005	NO
2800:150::/32	VTR BANDA ANCHA S.A.	03-08-2007	SI
2800:160::/32	Gtd Internet S.A.	30-08-2007	SI
2800:1b0::/32	Pontificia Universidad Católica de Chile	03-10-2007	NO
2800:1f0::/32	Adexus S.A.	27-12-2007	NO
2800:270::/32	Universidad Tecnica Federico Santa María	08-08-2008	SI
2800:290::/32	Netline	08-09-2008	NO
2800:300::/32	ENTEL CHILE S.A.	30-01-2009	SI
2800:330::/32	Entel PCS Telecomunicaciones S.A.	03-04-2009	NO
2800:3b0::/32	Telmex Servicios Empresariales S.A.	14-07-2009	NO
2800:460::/32	Universidad Católica de Valparaíso	05-02-2010	NO
2801:0:10::/48	Quintec Soluciones Informáticas S.A.	12-11-2008	NO

2.6.2 Principales proyectos ejecutados

Al momento de realizar este trabajo, en Chile existe un conjunto de proyectos en desarrollo o ya ejecutados, tendientes a implementar IPv6 con fines comerciales. A continuación se describen algunos de los proyectos más relevantes en este sentido.

Estado de migración de NIC Chile

NIC Chile es la autoridad encargada de administrar los nombres de dominio para el sufijo *.cl*, función que le fue delegada directamente de IANA. NIC Chile tiene conectividad IPv6 en forma experimental desde inicios del año 2006, y ya desde mediados del 2008 cuenta con conectividad nativa en modalidad *dual stack*. Esto permite que actualmente sea posible utilizar direcciones IPv6 para los servidores de nombre al momento de inscribir un dominio nacional [13].

Adicionalmente, esta autoridad se encuentra participando en el proyecto "*Google over IPv6*", el cual está abierto a todos los ISP e instituciones que cuenten con conectividad IPv6 y permite el acceso a todos los servicios de Google utilizando enlaces directos sobre IPv6, desde las redes de los participantes [14].

NIC Chile además de sus labores administrativas ha contribuido a la difusión de IPv6 en Chile. En este sentido, el año 2005 esta entidad organizó junto a LACNIC y la Subsecretaría de Telecomunicaciones (Subtel) el evento *"IPv6 Tour"* en el país; el cual fue repetido el año 2007. Este evento estuvo dirigido a proveedores de Internet, directivos del sector público y empresas que hacen uso de la red, y se llevó a cabo con la misión de divulgar en Chile el conocimiento sobre IPv6 y exponer el estado de las políticas públicas en la distribución de servicios de Internet [15].

Proyecto "IP versión 6 para Chile"

Con el objetivo de implementar tempranamente y de manera planificada IPv6 en las redes nacionales, NIC Labs[1] junto a la Subtel, se han propuesto diseñar un Plan Estratégico que impulse una implementación ordenada de IPv6 en Chile. Para este efecto, se convocó a los proveedores de Internet, tanto fijos como móviles, entendiendo que esta tarea requiere la coordinación y trabajo conjunto de distintos actores en una alianza público-privado. Las empresas que actualmente participan como socias del proyecto son: Entel PCS, Movistar, Claro, VTR y Telmex. Además, el proyecto cuenta con la participación de Cisco como soporte tecnológico.

El desarrollo de este plan permitirá aunar esfuerzos y coordinar las medidas necesarias entre todos los actores involucrados, con miras a que Chile pueda tomar un lugar avanzado a nivel mundial tanto en el mercado de desarrollo de software, como en el desarrollo de productos innovadores que utilicen Internet como medio de comunicación de dispositivos, además de poder liderar la implementación de IPv6 en la región. Para esto se han considerado los siguientes ejes de acción:

- **Desarrollo tecnológico**: Desarrollo del plan de transición técnica a nivel país hacia IPv6
- **Difusión**: Difusión dentro de la comunidad el nuevo protocolo, el proyecto propiamente tal y sus participantes.

[1] NIC Labs es un Laboratorio de Investigación Aplicada y Transferencia Tecnológica creado por NIC Chile, cuya misión es desarrollar investigación de nivel internacional generando nuevo conocimiento en el área de redes IP.

- **Capacitación y formación de recursos humanos**: Capacitación del personal técnico e ingenieros (especialmente de los ISPs y Gobierno) para generar las habilidades técnicas necesarias para el nuevo ambiente.
- **Desarrollo de mercado**: Estudio de las nuevas oportunidades que ofrece el nuevo protocolo.

El proyecto "IP versión 6 para Chile" cuenta actualmente con financiamiento de Corfo y su desarrollo comenzará en marzo de 2010, con una duración estimada de 30 meses. Más infomación sobre las actividades contempladas se puede encontrar en [16].

Oferta de conectividad IPv6 nativa por GTD Internet

Al momento de realizar este trabajo sólo una empresa nacional ofrece conectividad IPv6 de forma nativa a sus usuarios. Esta empresa es GTD Internet, la cual cuenta internamente con una red *dual stack*, lo que le permite conectarse nativamente con IPv6 con algunos proveedores internacionales y además establecer túneles con otros proveedores que permiten comunicar redes IPv6 a través de redes IPv4 [17].

GTD Internet ofrece a sus usuarios (típicamente clientes empresariales) un prefijo /48 derivado del prefijo /32 asignado por LACNIC y que se observa en la Tabla 2.5. De este modo, un usuario que contrata los servicios de GTD recibe una o varias direcciones IPv4 y, además, un prefijo IPv6, lo que le permite acceder simultáneamente y de manera nativa a servicios sobre IPv4 y sobre IPv6, respectivamente [18].

Cabe mencionar que GTD Internet también ha participado dando soporte en eventos de difusión de IPv6. En este sentido, en el último *"IPv6 Tour"* organizado por NIC Chile, GTD fue el encargado de levantar un laboratorio que permitió mostrar a los asistentes cómo operan los servicios con IPv6.

Capítulo 3: ¿Por qué adoptar IPv6?[1]

Al comienzo de la sección 2.3 se presentó el protocolo IPv6 y las principales características que lo hacen superior al actual protocolo IPv4. En este capítulo se profundiza en algunas de estas características, incorporando aspectos adicionales que permiten justificar - al menos desde el punto de vista técnico y operacional - el que una empresa comience el proceso de adopción de IPv6 en sus redes.

A pesar de las justificaciones que aquí se presentan, cabe mencionar que actualmente no existe un consenso respecto a los beneficios desde el punto de vista económico de realizar esta adopción, puesto que aún no se ha demostrado que las inversiones necesarias para incorporar IPv6 por sí solas se traduzcan en un ahorro tangible para la empresa que realice estas inversiones[2].

3.1 Consideraciones de planificación

Tomando en cuenta la experiencia existente sobre procesos de adopción de IPv6, resulta razonable esperar que los proyectos de adopción de IPv6 en distintos tipos de redes se extiendan por períodos de 2 a 3 años, considerando evaluaciones preliminares, implementación de laboratorios experimentales, implementación de pilotos, etapas de adopción parcial, etc. Por lo tanto, adelantar la decisión de iniciar este proceso permitirá a una empresa estar preparada con

[1] Los antecedentes incluidos desde la sección 3.2 hasta la sección 3.6 de este capítulo están basados en [29]

[2] El proyecto "IP versión 6 para Chile" descrito en 2.6.2 busca - además de sus objetivos básicos- estudiar este hecho, para encontrar alguna ventaja económica que haga recomendable la adopción del protocolo.

mayor antelación para acceder a contenidos disponibles sólo en IPv6, una vez que las direcciones IPv4 se encuentren completamente agotadas.

3.2 Capacidad de direccionamiento

La principal motivación para definir esta versión del protocolo IP fue la inminente escasez de direcciones asignables con IPv4. Por una parte, el gran espacio de direcciones disponibles en IPv6 permite facilitar la agregación jerárquica de direcciones en Internet, simplificando las tablas globales de ruteo. Pero además, al interior de redes empresariales el hecho de contar con un prefijo /48 permite desplegar un completo esquema de subredes en estos sitios (16 bits para subredes), incluyendo al mismo tiempo una mayor cantidad de hosts por subred (64 bits para hosts). Esto hace prácticamente imposible el agotamiento de direcciones dentro de cada subred y dentro de la empresa misma, permitiendo utilizar en toda la red direcciones globalmente únicas.

3.3 Mejoras en seguridad

La seguridad que provee el protocolo IPv6 es mucho más avanzada que la ofrecida por IPv4. Existen varios mecanismos de transporte mejorados para permitir que una red opere de manera más segura y con un menor impacto en el desempeño de la red.

En primer lugar, IPv6 tiene la tecnología IPSec directamente integrada en el protocolo, mediante las cabeceras de extensión AH y ESP. Esto permite simplificar la autentificación y encriptación de los datos *peer-to-peer* contenidos en capas superiores a la capa de red, una vez que se establece una arquitectura de llaves en la red, evitando el uso de otros mecanismos menos seguros (por ejemplo un *hash* MD5).

Además, con IPv6 todos los flujos en Internet son rastreables de mejor manera, debido a que cuentan con una dirección IPv6 de origen y destino que es única y ruteable globalmente. Esto permite facilitar, por ejemplo, el seguimiento de ataques de denegación de servicio (*Denial of Service*, DoS) y evitar el acceso ilegal a recursos de la red, usando reglas de filtrado de tráfico más simples.

Por otra parte, el uso del espacio de direcciones privadas en IPv6 ahora se basa en las direcciones *Unique Local*, las cuales evitarán situaciones de conflicto cuando se desee unir dos

redes y asegurar la comunicación interna entre éstas, simplificando de paso el diseño de las reglas de filtrado que se deban aplicar para esta comunicación.

Finalmente, debido a que la cantidad de direcciones disponibles en IPv6 es prácticamente infinita, la probabilidad de realizar un escaneo de puertos exitoso al interior de una red se reduce drásticamente, debido a que para barrer todas las direcciones y puertos de una subred se requiere una cantidad enorme de recursos y tiempo. Incluso si se conoce el prefijo y si se pudiera estimar la porción del identificador de interfaz correspondiente al fabricante (en caso de utilizar EUI-64) se requeriría rastrear 2^{24} direcciones IPv6 con sus respectivos puertos TCP/UDP.

Respecto al último punto, si bien con EUI-64 es posible detectar en Internet a un usuario particular en base a su dirección MAC (debido a que esta porción de la dirección IPv6 no cambia independiente de la red a la que se encuentre conectado), existe la posibilidad de usar Extensiones de Privacidad [19] como complemento a la autoconfiguración *stateless*, lo que permite que la parte de la dirección IPv6 que identifica al host se asigne de manera pseudo-aleatoria, por un período de tiempo breve (horas o días) luego del cual se vuelve a generar un nuevo sufijo para la porción de interfaz de la dirección IPv6. Esta característica viene implementada por defecto como mecanismo de autoconfiguración en entornos Windows y también es soportada por sistemas Linux.

3.4 Eliminación de NAT

Una de las consideraciones iniciales de diseño de Internet era la conectividad *any-to-any*[1]. El crecimiento en el número de equipos y dispositivos conectados a Internet sumado al limitado espacio de direcciones de IPv4 fue lo que gatilló la necesidad de técnicas de conservación de direcciones. En este sentido, NAT se introdujo como una herramienta para reducir la demanda de direcciones IPv4 públicas, pero trajo como consecuencia la eliminación de la capacidad de conectividad *any-to-any*. Al eliminar la necesidad de conservar direcciones (y, por lo tanto, de NAT) IPv6 vuelve al modelo de conectividad *any-to-any*, con lo que ciertas limitaciones en el desarrollo de aplicaciones desaparecen. Por ejemplo, al no existir la necesidad de mecanismos

[1] Conectividad *any-to-any* se refiere a la capacidad de cualquier host de alcanzar a cualquier otro host conectado a Internet. Debido a que NAT apantalla una red privada completa con una única dirección pública, esta conectividad se pierde si, por ejemplo, se desea iniciar una conexión a un host específico situado detrás de un dominio con NAT.

para atravesar NAT es posible mejorar servicios de red avanzados, tales como aplicaciones *peer-to-peer*, mensajería instantánea, telefonía sobre IP, etc.

Cabe mencionar que actualmente existe un paradigma erróneo por parte de algunos administradores de red, quienes asocian el uso de NAT con medidas para aumentar la seguridad en las redes. Si bien el enmascaramiento de las redes privadas que se logra con NAT permite proteger los hosts al interior de estas redes, esta no fue la motivación para la implementación de NAT. Por lo demás, utilizando IPv6 y un conjunto de reglas bien configuradas también es posible controlar el acceso a hosts internos de una red incluso si éstos utilizan direcciones globalmente únicas, mitigando de paso la posibilidad de realizar ataques como escaneo de puertos y técnicas de detección de redes en general. Asimismo, el hecho de eliminar NAT en la red permite simplificar considerablemente la configuración y la administración de los firewalls, debido a que las reglas de filtrado se aplican directamente sobre direcciones de ámbito global sin necesidad de tener en consideración traducciones de direcciones dentro de la red.

3.5 Autoconfiguración

IPv6 ofrece un enfoque escalable para minimizar la interacción humana en la configuración de dispositivos. Las implementaciones de IPv4 requieren configurar cada equipo para indicarle si debe usar DHCP o una dirección estática, además de la administración de un servidor que cuente con un pool de direcciones suficientemente grande para soportar el número potencial de dispositivos conectados. En cambio, de forma alternativa, IPv6 utiliza una mecanismo desde el router para indicar a los equipos conectados el uso de DHCP o bien la opción de autoconfiguración *stateless*, la cual soporta un número de dispositivos prácticamente ilimitados en la subred. En caso de que no exista un router que provea este mecanismo, los equipos se configuran con una dirección de tipo *Link Local*, la cual se deriva de la dirección MAC (dirección física de capa 2) y tiene validez sólo en el enlace local.

3.6 Características adicionales

El protocolo IPv6 integra ciertas capacidades que no existían en IPv4, o bien existían pero con limitaciones en su aplicación. A continuación se describen algunas de las más relevantes.

Multidireccionamiento (*Multihoming*)

IPv6 posibilita que los hosts tengan múltiples direcciones IP y que las redes tengan múltiples prefijos. Esto permite a los sitios tener conexiones a distintos ISP simultáneamente sin alterar la tabla de ruteo global, además de facilitar el proceso de migración cuando se desea cambiar de uno a otro proveedor de Internet sin perder conectividad.

Capacidades de movilidad

IP móvil [6] permite que un nodo cambie su ubicación dentro de una red IPv6 manteniendo sus conexiones existentes, independiente de la red a la que se encuentre conectado. Esta característica ya está implementada para IPv4, pero requiere que los paquetes viajando desde un host hacia el nodo móvil se ruteen a través del agente inicial[1] del nodo móvil, mientras que en el sentido contrario los paquetes viajan directamente desde el nodo móvil al host usando la red de visita, produciéndose lo que se denomina una ruta triangular. En IPv6, en cambio, mediante el uso de cabeceras de extensión, es posible mantener la conectividad entre un nodo móvil y un host de Internet sin necesidad de que parte del tráfico circule a través del agente inicial.

Servicios de *multicast*

Los servicios de *multicast* en IPv4 están fuertemente restringidos al espacio de direcciones limitado del que se dispone para la asignación de grupos (direcciones IPv4 clase D) y a un rango implícito para la pertenencia a grupos definidos localmente. En IPv6, *multicast* corrige esta situación integrando indicaciones explícitas para el ámbito de los grupos y expandiendo la cantidad de direcciones disponibles a 4.000 millones de grupos por ámbito (local, de sitio o global), lo que permite incorporar parámetros adicionales que facilitan el despliegue de *multicast* en las redes.

[1] El agente inicial (*Home Agent*, HA) es un router en la red local del nodo móvil que almacena la dirección permanente de éste mientras se encuentra en una red de visita. En IPv4, cuando un host de Internet quiere comunicarse con el nodo móvil, los paquetes son interceptados por el agente inicial y enviados mediante un túnel hacia el nodo móvil.

3.7 Soporte de IPv6 en aplicaciones y equipos

Un aspecto de suma importancia para la adopción del protocolo IPv6 es contar con el soporte necesario en los equipos y aplicaciones que intervienen en la conectividad, lo que actualmente se puede garantizar en la mayoría de los casos. A continuación se desglosa el estado de los principales sistemas operativos, aplicaciones y equipos respecto de la integración de IPv6 dentro de sus características.

3.7.1 Sistemas Operativos

A nivel de sistemas operativos el soporte de IPv6 es el que se describe en la Tabla 3.1. En esta tabla se presentan las características soportadas tanto de forma nativa (cuando aparece "sí") como mediante la instalación de un complemento (cuando aparece "*addon*"). Se incluye - donde corresponda - la versión desde la cual se cuenta con soporte para IPv6.

Tabla 3.1: Sistemas operativos que soportan IPv6 y características soportadas[1]

Sistema Operativo	Firewall	DHCPv6	Túneles	Comentarios
FreeBSD	sí	*add-on*	sí	Desde versión 6.1
Linux	sí	*add-on*	sí	Desde kernel 2.6.x
Mac OS X	sí	*add-on*	sí	Desde versión 10.2
Solaris	sí	sí	sí	Desde Solaris 8
Windows XP	sí	*add-on*	sí	Desde SP2. IPv6 no habilitado por defecto
Windows Vista	sí	sí	sí	
Windows 7	sí	sí	sí	
Windows 2003 Server	sí	addon	sí	IPv6 no habilitado por defecto
Windows 2008 Server	sí	sí	sí	

3.7.2 Aplicaciones

Las principales aplicaciones para las que se requiere soporte de IPv6 son aquellas que intervienen en los servicios más utilizados en Internet. A nivel empresarial, estos servicios son: Servidor web, DNS, FTP, SSH y correo electrónico. Algunos ejemplos de aplicaciones que actualmente soportan IPv6 en cada uno de estos servicios se indican a continuación[2]:

[1] Información basada en [30]

[2] Un completo listado de aplicaciones que soportan IPv6, separadas por categorías, se puede obtener en [31] y [32]

- **Servidor web**: Apache HTTP Server 2.0 y superiores
- **Servidor DNS**: BIND 9
- **Servidor FTP**: proFTPd 1.2.9 y superiores
- **Servidor SSH**: OpenSSH 3.6.1 y superiores
- **Servidor DHCP**: ISC DHCP 4.0 y superiores
- **Servidor correo electrónico**: Sendmail 8.10.0 y superiores, Microsoft Exchange 2007 SP1 y superiores.

3.7.3 Equipos de red

El siguiente es el estado de los principales equipos presentes en redes empresariales para establecer la conectividad.

Routers y switches

En esta familia de equipos el líder en el segmento empresarial es Cisco, el cual basa la operación de los routers y switches en su *Internetworking Operating System* (IOS). Actualmente, el protocolo IPv6 es soportado en todos los equipos que soporten IOS a partir del *release* 12.2(T), aunque las características disponibles en cada caso dependen tanto de la licencia como del *release* específico instalado. Un detalle de estas características se puede obtener en [20].

Otros fabricantes que soportan características IPv6 en sus líneas de routers y switches son [21]:

- Juniper, para JUNOS a partir del *release* 5.1.
- Alcatel-Lucent en su *Service Routing Operating System* (SR-OS).

Firewalls

Estos equipos permiten - entre otras funcionalidades - filtrar el tráfico que circula por la red, desde y hacia la red interna. Algunos fabricantes que soportan IPv6 en sus productos son [22]:

- Check Point, para equipos con software NGX R65 o superior.
- Juniper, en la línea SSG para equipos con Screen OS 6.0.0 o superior.
- Cisco, en la línea ASA para equipos con Cisco ASA Software *release* 8.0 o superior [23].

Capítulo 4: Estrategia para servicio de validación de compatibilidad con IPv6 en redes empresariales

Con el objetivo de apoyar a las empresas en el proceso de adopción de IPv6 en sus redes, se propone un servicio para estudiar las características de cada red respecto de la capacidad que presentan actualmente para soportar IPv6, tanto a nivel de equipamiento como de aplicaciones y servicios que hacen uso de la red.

La estrategia que a continuación se presenta, para desarrollar el servicio ofrecido, es un marco de referencia para abordar cualquier requerimiento de una empresa mandante para evaluar su red. El diseño de esta estrategia se basa en las recomendaciones brindadas por Cisco para la integración de IPv6 en agencias de gobierno de los Estados Unidos (24), las cuales fueron adaptadas a las características de una red empresarial y contrastadas con la experiencia operacional de la empresa Magenta Computación S.A. para construir un plan de trabajo que resulte completo en términos de los aspectos cubiertos, pero que además sea factible de realizar por la empresa que lo ejecute. En esta estrategia se consideran tanto las actividades incluidas en el servicio como las actividades futuras en caso de que la empresa mandante decida contratar un proyecto de migración a IPv6.

4.1 Actividades contempladas dentro del servicio

El servicio ofrecido a las empresas consta de las actividades que a continuación se describen.

4.1.1 Levantamiento de la red

El objetivo de esta actividad es recopilar toda la información necesaria para estudiar los requisitos técnicos que el cliente actualmente cumple y aquéllos que debe cumplir, con el fin de estimar la inversión que el cliente deberá considerar para la adopción de IPv6.

El levantamiento de la red se efectúa en terreno. Como resultado de la actividad se debe obtener un listado completo que considere, al menos, los siguientes ítems:

- Equipos presentes en la red (routers, switches, firewalls, etc.), identificando fabricante, versiones de hardware y software, cantidad de memoria, licencias asociadas, módulos de hardware de expansión, etc.
- Sistemas operativos utilizados tanto en servidores como en clientes de la red.
- Hardware y/o software asociado a servicios básicos: HTTP(S), DNS, FTP, SSH, DHCP.
- Hardware y/o software asociado a servicios específicos de la red, incluyendo bases de datos y aplicaciones internas de la empresa.

El servicio ofrecido no contempla la evaluación de aplicaciones de monitoreo y administración de la red, las cuales deberán ser evaluadas en un proyecto posterior.

4.1.2 Instalación de laboratorio para demostración de capacidades de IPv6

Esta actividad tiene los siguientes objetivos:

- Mostrar en la empresa el funcionamiento de la red utilizando de forma complementaria IPv6 como protocolo de red.
- Validar cuáles de los servicios más representativos y de los clientes de la empresa cuentan con soporte para IPv6 y cuáles no, sin alterar la red de producción de la empresa.

Utilizando la red actual del cliente, se despliega inicialmente una red en paralelo con la red de producción, donde se habilitan los servicios más importantes actualmente provistos por el cliente, de modo de validar su funcionamiento sobre IPv6. Para esto - debido a que en esta etapa el cliente no contará con conectividad IPv6- se debe implementar un túnel 6to4, lo que

requiere, a su vez, de una dirección IPv4 pública que el cliente deberá proveer. El esquema para la fase piloto de demostración es el que se muestra en la Figura 4.1.

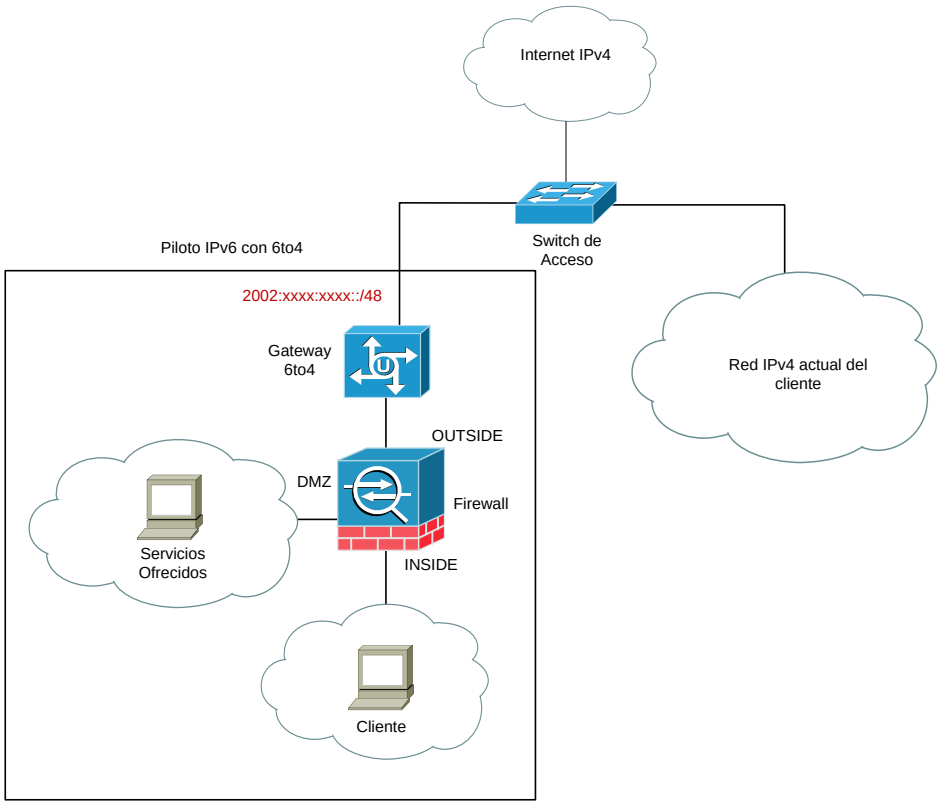


Figura 4.1: Implementación base de laboratorio para demostración en cliente

Sobre la red de laboratorio se deberán realizar las configuraciones de red que permitan obtener una conectividad global tanto mediante IPv4 como usando IPv6. De este modo, los clientes de la red deberán ser capaces de obtener conectividad hacia los servicios presentes usando ambos protocolos.

4.1.3 Clasificación de equipos y aplicaciones

Como resultado del levantamiento y de la validación realizada en el laboratorio demostrativo se procede a agrupar los equipos y aplicaciones identificados en una de las seis categorías que se describen en la Tabla 4.1.

Tabla 4.1: Categorías para clasificación de aplicaciones y equipos

Categoría	Descripción
1	Compatible y actualmente corriendo IPv6
2	Compatible, pero requiere ser configurado para adoptar IPv6
3	Requiere actualización de software para compatibilidad con IPv6
4	Requiere actualización de hardware para soportar una actualización de software que permita adoptar IPv6 (Ej: Aumento de memoria RAM)
5	No puede ser actualizado para soportar IPv6 y debe ser remplazado (*Legacy*)
6	No será actualizado debido a que se prevé que será descontinuado o que se utilizará una medida alternativa para lograr la compatibilidad

En algunos casos, particularmente en routers y switches multicapa, la clasificación de los equipos en alguna de las categorías anteriores dependerá de las características específicas que se requieran para su operación dentro de la red en un proyecto de adopción de IPv6. Por ejemplo, un router podría tener instalada una versión de IOS que soporte asignación de direcciones mediante DHCPv6, pero que no soporte el uso de un servidor DHCPv6 centralizado y un relay DHCPv6, con lo que requeriría una actualización de software en caso de que se desee usar DHCPv6 centralizado en la empresa (por lo tanto, caería en la categoría 3), pero no requeriría dicha actualización si - por ejemplo - se decide utilizar la autoconfiguración *stateless* (en cuyo caso caería en la categoría 2). En este sentido, las consideraciones mínimas que se recomienda contemplar en estos equipos son las siguientes:

- Soporte de conectividad *dual stack*, sin necesidad de soportar túneles, considerando que actualmente ya existe oferta de IPv6 de forma nativa.
- Soporte de DHCPv6 para configuración automática con estado en la red. En caso de contar actualmente con un servicio DHCP centralizado, se debe soportar además un *relay* para DHCPv6 en los equipos de la red que actualmente realicen funciones de *relay* sobre IPv4.
- Soporte de al menos uno de los protocolos de ruteo dinámico que operan con IPv6 (RIPng, OSPFv3, EIGRPv6, BGP4-MP) dependiendo de los requerimientos y el tamaño de la red. En caso de existir un equipo que no soporte protocolos de ruteo dinámico (por

ejemplo, un firewall) o que no estén diseñados para usar estos protocolos, se debe estudiar el impacto que tendría sobre la red usar rutas estáticas en dicho equipo, antes de proceder a la clasificación.

- Soporte de características de administración adicionales, tales como DNS para IPv6, ICMPv6, etc.

Respecto a los sistemas operativos, para decidir si se requiere una actualización, se recomienda que las versiones con que se deberá operar para una adecuada integración con IPv6 sean las siguientes:

- Clientes Windows: Microsoft Windows 7 Professional
- Clientes Linux: Distribución Linux con kernel 2.6.x
- Servidores Windows: Windows 2008 Server
- Servidores Linux: Distribución Linux con kernel 2.6.x

4.1.4 Evaluación económica de los requisitos para compatibilidad con IPv6

Habiendo agrupado exitosamente la infraestructura de la red en alguna de las 6 categorías presentadas, los costos generales asociados a cada una de ellas son los que se presentan en la Tabla 4.2.

Tabla 4.2: Costos generales en función de la categorización de la infraestructura

Categoría / Recursos	1	2	3	4	5	6
No requiere	x					x
HH de configuración		x	x	x	x	
HH de validación		x	x	x	x	
Software			x	x	x	
Módulos de hardware				x		
Hardware					x	

Realizadas las actividades descritas, el servicio finaliza una vez que se le informa a la empresa mandante de las condiciones actuales de su red para soportar IPv6, así como los costos totales involucrados en una eventual adopción del protocolo. Respecto a estos costos, en el

Capítulo 6 se propone una planilla dinámica que permite a la empresa de servicios de redes establecer las inversiones en las que la empresa mandante deberá incurrir.

4.2 Actividades posteriores

En caso de que la empresa mandante tome la decisión de adoptar IPv6, se deberá iniciar un nuevo proyecto, en el cual se deberán considerar los siguientes aspectos:

Capacitación

Se recomienda considerar un plan de capacitación sobre IPv6 que contemple no sólo a los técnicos e ingenieros involucrados en el proyecto (tanto de la empresa de servicios de redes como de la empresa mandante), sino además a los ejecutivos y/o encargados de adquisiciones de la empresa mandante, los cuales deberán tener claridad en la forma de especificar las capacidades de IPv6 requeridas en sus productos al momento de negociar contratos con sus proveedores.

Plan de actualización y configuración de la red

En base a la propuesta resultante del servicio anterior, se debe dejar la red en condiciones de soportar IPv6 como punto de partida para las configuraciones posteriores.

Mecanismo de transición

Se recomienda usar *dual stack*, considerando la actual oferta de IPv6 nativo por parte de los ISP.

Direccionamiento

Basado en el prefijo asignado por el ISP al que se le solicite conectividad IPv6. Se deberá optar entre distintos mecanismos de configuración, considerando además el uso de formato EUI-64 o bien de extensiones de privacidad para la identificación de interfaz de los dispositivos y equipos que se conectan a la red.

Implementación de pilotos

Se recomienda realizar la adopción de IPv6 en forma gradual, mediante la implementación de pilotos en puntos determinados de la red, de manera de probar los servicios internos de la empresa incluso antes de probar la conectividad hacia Internet.

Consideraciones de seguridad

El hecho de adoptar IPv6 trae asociadas consideraciones de seguridad adicionales a las contempladas en IPv4. Por lo tanto, al desarrollar el proyecto de adopción de IPv6 se deben revisar las políticas de seguridad en cada etapa del proyecto. Algunas consideraciones de seguridad relevantes se pueden encontrar en [24].

Plan de excepción

Para los equipos y aplicaciones que no se migrarán, ya sea porque el costo es demasiado elevado, porque no existe soporte o porque se espera que queden en desuso en un futuro cercano.

Capítulo 5: Implementación de laboratorio

Dentro del servicio definido en el Capítulo 4, una de las actividades contempladas es la instalación de un laboratorio en la red de la empresa mandante. Disponer de este laboratorio permite a esta empresa visualizar el funcionamiento del protocolo IPv6 y validar, en sus dependencias, el soporte de sus aplicaciones más representativas.

En el diseño de este laboratorio se escoge una configuración donde se integran tanto equipos de red (firewall, switch multicapa, equipos clientes con distintos sistemas operativos) como servidores con aplicaciones de uso frecuente sobre Internet (WWW, DNS, SSH, etc.), buscando construir una representación a menor escala del tráfico que habitualmente se observaría en una red empresarial.

En este capítulo se describen las actividades realizadas para lograr la implementación del laboratorio que integra el protocolo IPv6 sobre una red IPv4, así como las pruebas efectuadas para validar su funcionamiento.

5.1 Situación inicial: Red con IPv4

La primera actividad consiste en implementar una red completamente operativa sobre IPv4, hospedada detrás del servidor de acceso público (denominado ramiel). Contar con una red operando con IPv4 es fundamental para reproducir las condiciones iniciales que tendrá una empresa que decida adoptar el protocolo IPv6. En esta red se hace uso de los siguientes equipos:

- Servidor de acceso público (ramiel), con funciones de *gateway* hacia la red pública IPv4.
- Firewall Cisco ASA 5520 como firewall de borde entre la red de laboratorio y la red externa (incluyendo al *gateway* como parte de la red externa).

- Switch multicapa Cisco Catalyst 3750, para etapas de distribución y acceso en la red.
- Servidor interno (SRV-memoristas), el cual cuenta con software de virtualización VMWare Server, para simular equipos terminales como si estuvieran físicamente conectados en distintos puntos de la red.
- Equipos virtualizados con sistemas operativos: Fedora Core 11, Windows 2008 Server, Windows 7 RC y Ubuntu 8.04, integrados a la red como máquinas virtuales dentro del servidor SRV-memoristas.

Respecto al firewall y el switch multicapa, la elección de los modelos utilizados se basa fundamentalmante en la disponibilidad de equipamiento dentro de la empresa patrocinadora al momento de implementar el laboratorio, buscando que la red del laboratorio cuente con un modelo de cada equipo típico de una red empresarial.

Asimismo, las versiones de sistemas operativos escogidas pretenden abarcar los principales sistemas operativos utilizados en redes productivas para efectuar funciones tanto de clientes como de servidores dentro de estas redes.

El diagrama de interconexión en capa 2 se puede ver en la Figura 5.1, junto con la descripción de los equipos y el detalle de las VLAN[1] permitidas por cada enlace. Las VLAN que aparecen entre paréntesis corresponden a tráfico que circula por la red pero que pertenece a otro laboratorio ajeno al ámbito de este trabajo e implementado con recursos compartidos.

La interconexión lógica de los equipos dentro de la red se observa en la Figura 5.2, junto con el direccionamiento IPv4 de las distintas subredes. Se utiliza la dirección de red 10.0.0.0 dividida en función de las subredes existentes, las cuales se numeran siguiendo la nomenclatura **10.10.x.0/24**, en que x representa la identificación de la VLAN correspondiente a cada subred. Se utilizan, por lo tanto, identificaciones de VLAN menores a 256.

[1] VLAN (*Virtual LAN*) es un método para crear redes lógicamente independientes dentro de una misma red física.Esto ayuda en la administración de la red, separando segmentos lógicos de una red de área local (como departamentos de una empresa) que no deberían intercambiar datos localmente (aunque podrían hacerlo a través de un router o un switch multicapa, como en este caso).

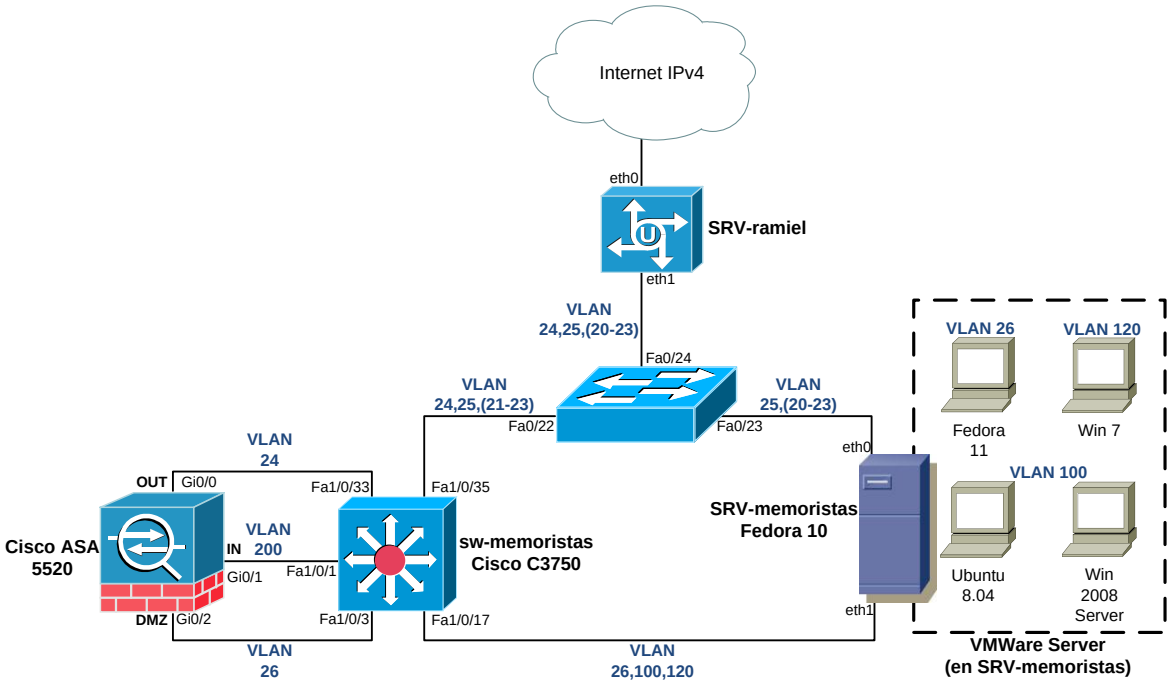


Figura 5.1: Diagrama de interconexión en capa 2 de red IPv4

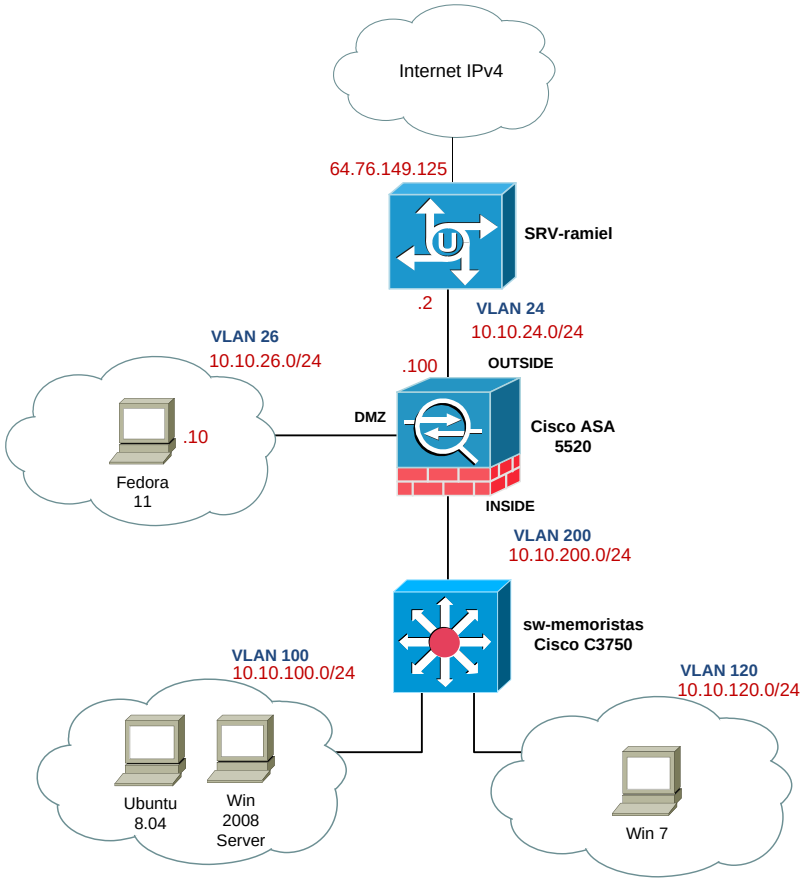


Figura 5.2: Diagrama de interconexión en capa 3 de red IPv4

Respecto a los servicios y tráfico existentes sobre esta red, además del acceso hacia Internet de la red interna, se considera en la DMZ de la red un servidor HTTP público y un servidor DNS tanto para resolver nombres de la red interna como para resolver un subdominio público. También se considera en esta zona un servidor DHCP centralizado para asignación dinámica de direcciones IP en los equipos clientes de la red interna, tanto para la VLAN 100 como para la VLAN 120.

En la red interna se contempla tráfico asociado al protocolo de ruteo establecido entre el switch multicapa y el firewall, correspondiente a OSPF. Por último, en una primera etapa se considera una sesión vía SSH para configurar el firewall desde el equipo con Sistema Operativo Windows 2008 Server. El detalle de todo este tráfico se describe en la Figura 5.3. Asimismo, para proveer los servicios dentro de la red el software utilizado es el que se indica en la Tabla 5.1.Este software se escogió esencialmente por venir incluido dentro del sistema operativo utilizado como servidor de la red (Fedora Core 11) y por ser fácil de configurar.

Tabla 5.1: Software usado para los servicios dentro de la red

Servicio	Software utilizado
Servidor HTTP	Apache HTTP Server v2.2.13
Servidor DNS	BIND 9
Servidor DHCP	ISC DHCP v4.1.1

Para poder dar conectividad hacia Internet en la red implementada, en el firewall de borde se configura una traducción de direcciones mediante PAT, de modo que toda la red interna y la DMZ cuenten con salida a Internet utilizando la dirección IP de la interfaz externa del firewall. Si bien esta interfaz tiene una dirección IP privada (que se traduce dinámicamente a la IP pública de Ramiel para salir a Internet), la configuración de PAT se hace necesaria para mantener en el laboratorio un esquema similar a una red privada típica, considerando que eventualmente la interfaz externa del firewall podría tener una dirección IP pública.

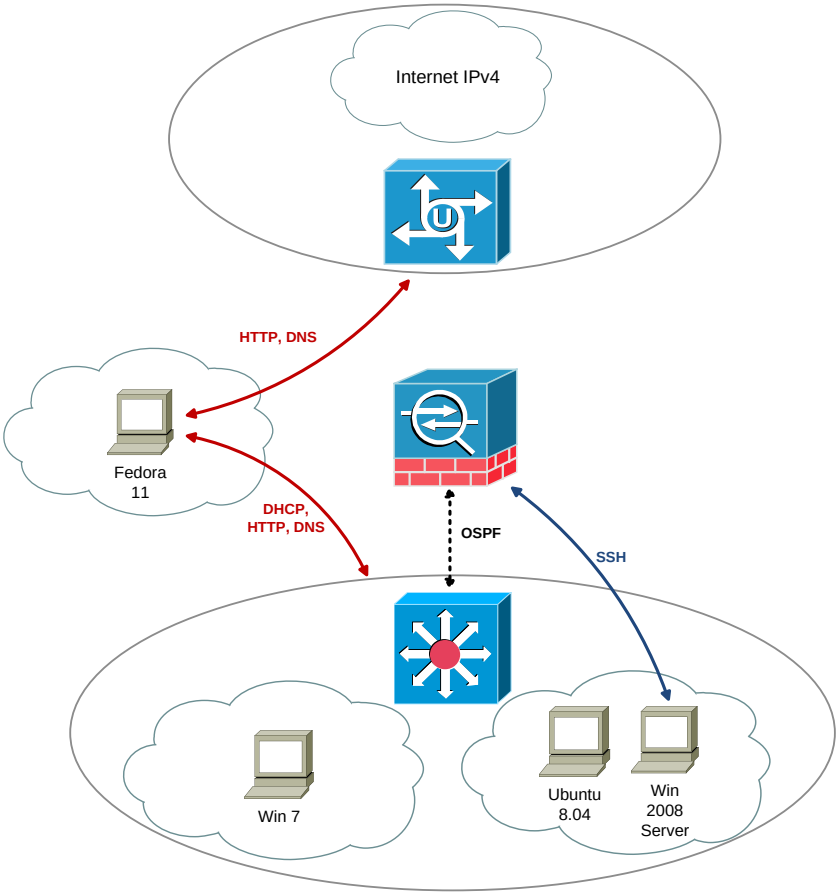


Figura 5.3: Diagrama de tráfico y servicios sobre la red IPv4.

Por otra parte, se realiza un mapeo estático de puertos de la dirección IP del servidor instalado en la DMZ hacia la IP de la interfaz externa del firewall, de modo que los puertos 80 y 53 puedan ser accedidos desde el exterior (para servicios HTTP y DNS, respectivamente).

En la Tabla 5.2 se resumen las traducciones configuradas.

Tabla 5.2: Traducción de direcciones IP en red IPv4

Inside Local	Inside Global	Tipo de NAT
10.10.100.x	10.10.24.100	PAT
10.10.120.x	10.10.24.100	PAT
10.10.26.x	10.10.24.100	PAT
10.10.26.10:80	10.10.24.100:80	Estático
10.10.26.10:53	10.10.24.100:53	Estático

5.2 Implementación de IPv6 mediante túnel 6to4

Debido a que no se cuenta con un enlace IPv6 nativo durante el desarrollo de este laboratorio, se decide dar conectividad IPv6 a la red mediante un túnel 6to4. Para esto se llevan a cabo las actividades que a continuación se describen.

5.2.1 Configuración del túnel en ramiel

Lo primero que se modifica es el archivo asociado a la configuración de la interfaz eth0 del servidor ramiel. Esta interfaz tiene una dirección IPv4 pública, por lo que permite configurar un túnel 6to4. La configuración se realiza de forma sencilla agregando un par de líneas al archivo /etc/sysconfig/network-scripts/ifcfg-eth0.

Configuración de /etc/sysconfig/network-scripts/ifcfg-eth0

```
# Realtek Semiconductor Co., Ltd. RTL-8139/8139C/8139C+
DEVICE=eth0
HWADDR=00:50:ba:8c:2e:93
ONBOOT=yes
TYPE=Ethernet
NETMASK=255.255.255.240
IPADDR=64.76.149.125
GATEWAY=64.76.149.113
IPV6INIT=yes
IPV6TO4INIT=yes
```

Tras reiniciar el servicio *network* se verifica la creación de la interfaz de red tun6to4, la cual tiene los siguientes parámetros:

```
[root@ramiel ~]# ifconfig tun6to4
tun6to4   Link encap:IPv6-in-IPv4
          inet6 addr: 2002:404c:957d::1/16 Scope:Global
          UP RUNNING NOARP  MTU:1480  Metric:1
          RX packets:3666 errors:0 dropped:0 overruns:0 frame:0
          TX packets:5492 errors:5 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:1987400 (1.8 MiB)  TX bytes:701840 (685.3 KiB)
```

Se puede notar que la dirección asignada para el túnel incluye a continuación del prefijo 2002 la dirección IPv4 de la interfaz (expresada en formato hexadecimal). Adicionalmente es necesario habilitar en ramiel el *forwarding* de direcciones IPv6, utilizando el archivo /etc/sysconfig/network

Configuración de /etc/sysconfig/network

```
NETWORKING=yes
HOSTNAME=ramiel
IPV6_DEFAULTDEV=tun6to4
IPV6FORWARDING=yes
```

Con esto, hacia el interior de la red del laboratorio se dispone de un prefijo /48 para direccionamiento interno, por lo que tras verificar el funcionamiento del túnel desde Ramiel se procede a planificar el direccionamiento IPv6 de la red.

5.2.2 Plan de direccionamiento interno sobre IPv6

El hecho de contar con un prefijo /48 para asignar direcciones IPv6 en la red permite tener 16 bits para definir subredes de prefijo /64, dejando los 64 bits restantes para la identificación de los hosts. De este modo, se decide que el direccionamiento en la red mantenga un esquema análogo al utilizado en el caso de IPv4, incluyendo la identificación de VLAN en el segmento destinado a subred. El diagrama de direccionamiento resultante se observa en la Figura 5.4.

Una diferencia relevante entre el direccionamiento IPv4 y el IPv6 es que este último tiene un alcance global hacia Internet, por lo que todas las subredes tienen visibilidad desde y hacia Internet sin ser necesario configurar ningún tipo de NAT para este efecto. Sin embargo, esto implica que se debe tener un mayor cuidado a la hora de definir las reglas de filtrado en el firewall de borde utilizado.

5.2.3 Configuración de sw-memoristas

En el switch multicapa se definen las direcciones IPv6 para las interfaces VLAN 100, 120 y 200. Para esto se utiliza el prefijo considerado en el direccionamiento y el formato EUI-64 modificado para la identificación de host por cada interfaz. El formato EUI-64 se configura automáticamente mediante el comando:

```
Switch(config-if)#ipv6 address 2002:404c:975d:100::/64 eui-64
```

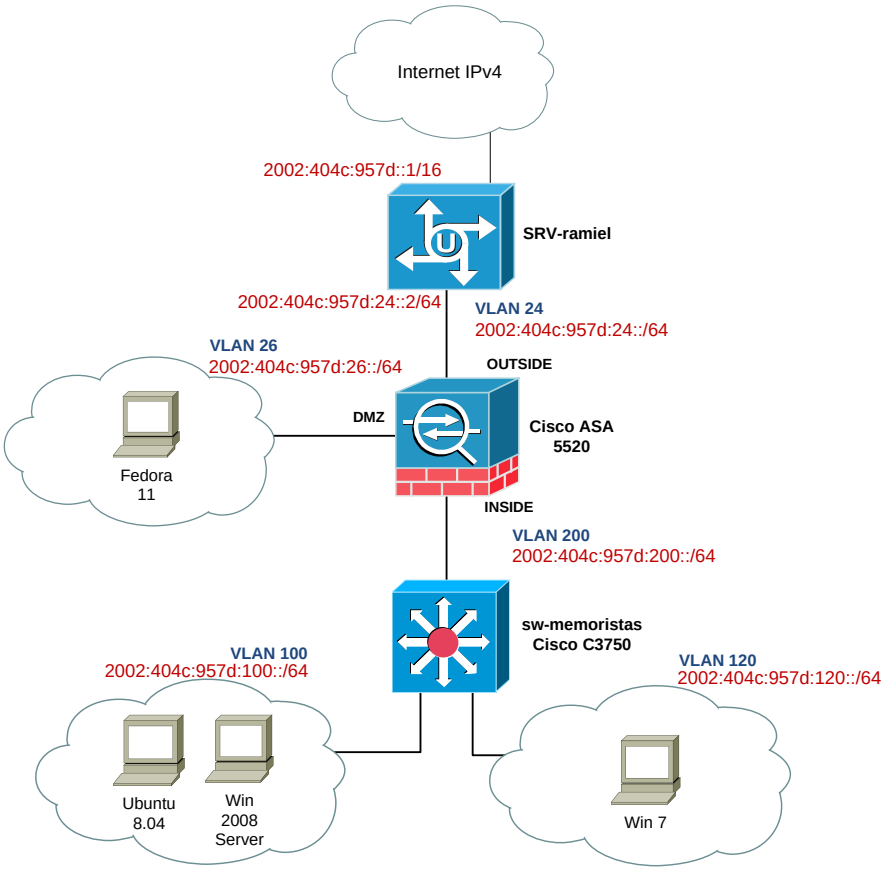


Figura 5.4: Diagrama de interconexión y direccionamiento IPv6 de la red

Al configurar la dirección IPv6 de cada interfaz VLAN, por defecto queda habilitado el envío de mensajes ICMPv6 "*Router Advertisement*" (RA), con los prefijos /64 configurados, lo que permite que los hosts conectados en las VLAN 100 y 120 con capacidades de autoconfiguración *stateless* puedan asignarse una dirección IPv6 y designar como puerta de enlace a la interfaz del switch desde la cual recibieron el paquete RA. Sin embargo, debido a que en esta etapa el firewall aún no tiene IPv6 configurado, ninguno de los hosts tendrá conectividad hacia Internet mediante IPv6.

El detalle de la configuración del switch, incluyendo la configuración IPv4 e IPv6 además de las configuraciones de capa 2, se puede observar en el Anexo B.1.

5.2.4 Configuración del firewall

Dentro del firewall se procede en primer lugar a asignar direcciones IPv6 en cada interfaz, siguiendo al igual que en el switch un formato EUI-64 modificado para la identificación

de host. Posteriormente se definen las reglas de filtrado a aplicar, análogas a las existentes sobre IPv4, que se pueden resumir en las siguientes:

- Permitir tráfico entrante al servidor de la DMZ, hacia los puertos HTTP y DNS.
- Permitir paquetes ICMPv6 hacia el servidor de la DMZ.
- Permitir respuestas de paquetes ICMPv6 hacia los hosts de la red interna (mensajes *time-exceeded* y *unreachable*).

El resto del tráfico circulante por la red se rige por las reglas implícitas asociadas al nivel de seguridad definido para cada interfaz (0 para la interfaz *outside*, 50 para la interfaz DMZ y 100 para la interfaz *inside*). En este sentido, el criterio es el siguiente:

- El firewall permite tráfico de una zona de mayor seguridad a una de menor seguridad.
- El firewall bloquea tráfico en sentido inverso (salvo que pertenezca a una conexión iniciada desde la zona de mayor seguridad).

Otro aspecto que se debe considerar en la configuración del firewall es el ruteo. Para la configuración de IPv4, se habilita el protocolo OSPF para transmitir rutas entre el switch y el firewall. Sin embargo, el modelo de firewall utilizado no permite establecer protocolos de ruteo sobre IPv6, por lo que tanto en el switch como en el firewall se deben establecer rutas estáticas hacia las redes no conectadas directamente, para lograr la visibilidad completa de la red.

El detalle de la configuración del firewall en IPv4 e IPv6 se puede observar en el Anexo B.2. Al respecto, cabe mencionar que toda la configuración para IPv4 se realizó mediante la interfaz gráfica ASDM. Sin embargo, la versión utilizada de esta interfaz no soporta IPv6, por lo que esta última configuración se debió efectuar mediante línea de comandos (CLI).

5.2.5 Configuración de red en Ramiel

Modificando el archivo /etc/sysconfig/network-scripts/ifcfg-eth1.24 se asigna una dirección IPv6 estática a la interfaz conectada hacia el interior de la red.

Configuración de /etc/sysconfig/network-scripts/ifcfg-eth1.24

```
# Realtek Semiconductor Co., Ltd. RTL-8139/8139C/8139C+
DEVICE=eth1.24
HWADDR=00:50:BA:B0:D9:C3
```

```
ONBOOT=yes
#BOOTPROTO=dhcp
TYPE=Ethernet
IPADDR=10.10.24.2
NETMASK=255.255.255.0
IPV6INIT=yes
IPV6_AUTOCONF=no
IPV6ADDR=2002:404c:957d:24::2/64
```

Posteriormente, se revisa la tabla de rutas existente en Ramiel para tráfico IPv6, observando lo siguiente:

```
[root@ramiel ~]# route -A inet6
Kernel IPv6 routing table
Destination                    Next Hop           Flags Metric Ref    Use Iface
2002:404c:957d:24::/64         *                  U     256    1        0 eth1.24
2002::/16                      *                  U     256    3        0 tun6to4
(…)
```

Debido a que por defecto no existe una ruta hacia el interior de la red para los paquetes con IP de destino 2002:404c:957d::/48, es necesario agregar estáticamente esta ruta, tomando como dirección de siguiente salto la asociada a la interfaz *outside* del firewall, según la topología utilizada (Figura 5.4). En caso contrario, en base a la tabla de rutas mostrada anteriormente, éste tráfico sería enviado por la interfaz virtual tun6to4.

```
[root@ramiel ~]# ip -6 route add 2002:404c:957d::/48 via
2002:404c:957d:24:21b:2aff:fe34:d94e metric 256
```

5.2.6 Configuración del servidor

En el servidor se debe modificar manualmente la configuración de propiedades de red para asignar una dirección IPv6 de forma estática. La dirección asignada es 2002:404c:957d:26::1 y al ser un servidor con sistema operativo Fedora 11 esta configuración se realiza modificando el archivo /etc/sysconfig/network-script/ifcfg-eth1.

Configuración de /etc/sysconfig/network-scripts/ifcfg-eth1

```
# Networking Interface
DEVICE=eth1
BOOTPROTO=none
HWADDR=00:0C:29:AC:61:46
ONBOOT=yes
IPADDR=10.10.26.10
NETMASK=255.255.255.0
TYPE=Ethernet
```

```
GATEWAY=10.10.26.100
DNS1=10.10.26.10
USERCTL=no
PREFIX=24
NAME="System eth1"
UUID=9c92fad9-6ecb-3e6c-eb4d-8a47c6f50c04
IPV6INIT=yes
IPV6ADDR=2002:404c:957d:26::1
IPV6_AUTOCONF=no
```

Debido a que la dirección IPv6 se asigna de forma estática, es necesario indicar manualmente cuál es la ruta por defecto para el tráfico fuera de la subred. En este caso, el *default gateway* corresponde a la interfaz DMZ del firewall y el comando a ingresar es el siguiente:

```
[root@server1 ~]# ip -6 route add ::0/0 via 2002:404c:957d:26:21b:2aff:fe34:d950
```

Una vez verificada la conectividad se procede a modificar la configuración del servidor DNS. Para esto se modifica el archivo /etc/named.conf, agregando la escucha del servidor en el puerto 53 para IPv6, lo que permite a los hosts de la red realizar consultas recursivas. Además se incorpora la zona de resolución inversa para los hosts IPv6.

Configuración de /etc/named.conf

```
//
// named.conf
//
// Provided by Red Hat bind package to configure the ISC BIND named[8] DNS
// server as a caching only nameserver (as a localhost DNS resolver only).
//
// See /usr/share/doc/bind*/sample/ for example named configuration files.
//

options {
       listen-on port 53 { any; };
       listen-on-v6 port 53 { any; };
       directory    "/var/named";
       dump-file    "/var/named/data/cache_dump.db";
         statistics-file "/var/named/data/named_stats.txt";
         memstatistics-file "/var/named/data/named_mem_stats.txt";
       allow-query     { localhost; any; };
       //recursion yes;
       allow-recursion      {      localnets;      10.10.100.0/24;      10.10.120.0/24;
2002:404c:957d::/48; };
       dnssec-enable yes;
       dnssec-validation yes;
       dnssec-lookaside . trust-anchor dlv.isc.org.;
};

logging {
        channel default_debug {
                file "data/named.run";
                severity dynamic;
        };
};

zone "." IN {
```

```
        type hint;
        file "named.ca";
};

zone "lab-ipv6" IN {
        type master;
        file "lab-ipv6.zone";
        allow-update { none;};
};

zone "d.7.5.9.c.4.0.4.2.0.0.2.ip6.arpa" IN {
        type master;
        file "lab-ipv6.reverse.arpa";
        allow-update { none;};
};

zone "26.10.10.in-addr.arpa" IN {
        type master;
        file "lab-ipv6.reversev4.arpa";
        allow-update {none;};
};

include "/etc/named.rfc1912.zones";
include "/etc/pki/dnssec-keys//named.dnssec.keys";
include "/etc/pki/dnssec-keys//dlv/dlv.isc.org.conf";
```

En el archivo que define los hosts pertenecientes al dominio lab-ipv6 también se modifica, para incorporar las direcciones IPv6 asociadas a cada host.

Configuración de /var/named/lab-ipv6.zone

```
$TTL 86400
$ORIGIN lab-ipv6.
@             IN     SOA    lab-ipv6.    roalarco.gmail.com. (
              2009090301 ; número de serie
              28800 ; tiempo de refresco
              7200 ; tiempo entre reintentos de consulta
              604800 ; tiempo tras el cual expira la zona
              86400 ; tiempo total de vida
              )
@             IN     NS     dns
@             IN     MX     10     mail
@             IN     AAAA   2002:404c:957d:26::1
server1              IN     AAAA   2002:404c:957d:26::1
server1              IN     A      10.10.26.10
www           IN     CNAME  server1
mail          IN     AAAA   2002:404c:957d:26::1
mail          IN     A      10.10.26.10
ftp           IN     CNAME  server1
dns           IN     CNAME  server1
fw-inside     IN     A      10.10.200.100
fw-inside     IN     AAAA   2002:404c:957d:200:21b:2aff:fe34:d94f
fw-outside    IN     A      10.10.24.100
fw-outside    IN     AAAA   2002:404C:957d:24:21b:2aff:fe34:d94e
fw-dmz        IN     A      10.10.26.100
fw-dmz        IN     AAAA   2002:404C:957d:26:21b:2aff:fe34:d950
ramiel        IN     A      10.10.24.2
ramiel        IN     AAAA   2002:404C:957d:24::2
sw-100        IN     A      10.10.100.254
sw-100        IN     AAAA   2002:404c:957d:100:219:56ff:fe80:f9c4
sw-200        IN     A      10.10.200.254
sw-200        IN     AAAA   2002:404c:957d:200:219:56ff:fe80:f9c8
```

```
sw-120        IN     A      10.10.120.254
sw-120        IN     AAAA   2002:404c:957d:120:219:56ff:fe80:f9c7
```

Finalmente, se define el archivo de resolución inversa para las direcciones IPv6.

Configuración de /var/named/lab-ipv6.reverse.arpa

```
$TTL 3D
@      IN SOA d.7.5.9.c.4.0.4.2.0.0.2.ip6.arpa. roalarco.gmail.com. (
                                  2009111801   ; serial
                                  1D     ; refresh
                                  30m    ; retry
                                  1d     ; expire
                                  1d )   ; minimum
;      NS     @
;      PTR    localhost.
@      IN     NS     server1.lab-ipv6.

$ORIGIN d.7.5.9.c.4.0.4.2.0.0.2.ip6.arpa.

1.0.0.0.0.0.0.0.0.0.0.0.6.2.0.0         IN     PTR    server1.lab-ipv6.
```

Cabe mencionar que para el servidor HTTP no es necesario modificar ninguna configuración, pues el servicio de Apache cuenta con soporte nativo para IPv6 de forma predeterminada.

5.2.7 Configuración de clientes internos

Con el objeto de validar los requerimientos mínimos para obtener conectividad IPv6, en los clientes no se modificó la configuración de red sino que se esperó que lograran la autoconfiguración *stateless* en base a los mensajes RA enviados por el switch multicapa. Puesto que esta autoconfiguración permite a cada cliente asignarse una dirección IP y un router por defecto, el resto de la configuración se sigue basando en el protocolo DHCP implementado sobre IPv4, por lo que se espera que los hosts así configurados utilicen el servicio DNS en su versión IPv4 y no en IPv6, si bien las consultas y posteriores resoluciones DNS (tanto de tipo A como de tipo AAAA) son independientes del protocolo IP utilizado.

No obstante lo anterior, en los clientes con entorno Windows es posible definir manualmente una dirección IPv6 para el servidor DNS adicional al servidor en IPv4 configurado por DHCP, lo que ocasiona que todas las consultas asociadas a este protocolo se hagan por defecto sobre IPv6.

5.2.8 Pruebas de Conectividad

Para cada una de las actividades antes descritas se efectúan pruebas básicas de conectividad, de modo de asegurar que las configuraciones hayan sido correctamente realizadas en función de los resultados esperados. A continuación se presentan algunos resultados relevantes para verificar la conexión en IPv6 de la red tanto para tráfico interno como hacia Internet.

5.2.8.1 Conectividad desde Ramiel hacia Internet IPv6

Se comprueba la conectividad haciendo ping hacia una dirección IPv6 conocida. En este caso se utiliza la dirección de la versión para IPv6 del buscador Google (ipv6.google.com), la cual no puede ser alcanzada desde un host IPv4-only.

```
[root@ramiel ~]# ping6 ipv6.google.com
PING ipv6.google.com(vx-in-x68.1e100.net) 56 data bytes
64 bytes from vx-in-x68.1e100.net: icmp_seq=1 ttl=53 time=335 ms
64 bytes from vx-in-x68.1e100.net: icmp_seq=2 ttl=53 time=335 ms
64 bytes from vx-in-x68.1e100.net: icmp_seq=3 ttl=53 time=335 ms
64 bytes from vx-in-x68.1e100.net: icmp_seq=4 ttl=53 time=334 ms
64 bytes from vx-in-x68.1e100.net: icmp_seq=5 ttl=53 time=336 ms
64 bytes from vx-in-x68.1e100.net: icmp_seq=6 ttl=53 time=334 ms

--- ipv6.google.com ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 4998ms
rtt min/avg/max/mdev = 334.654/335.311/336.118/0.589 ms
```

El resultado anterior permite afirmar que el túnel 6to4 creado funciona correctamente.

5.2.8.2 Conectividad desde la DMZ hacia Internet IPv4 e IPv6

Desde el servidor ubicado en la DMZ se carga una página web que permite obtener la dirección IPv4 del host desde el que se realiza la conexión (URL: http://ipv4.whatismyv6.com). Esto da como resultado la dirección IPv4 pública de Ramiel, como se observa en la Figura 5.5.

Posteriormente se carga la misma página en versión IPv6, la cual muestra la dirección IPv6 del host desde el que se realiza la conexión (URL: http://ipv6.whatismyv6.com). A diferencia del resultado anterior, en este caso se puede ver la dirección perteneciente al propio servidor, lo que da cuenta del ámbito global de esta dirección, según se muestra en la Figura 5.6

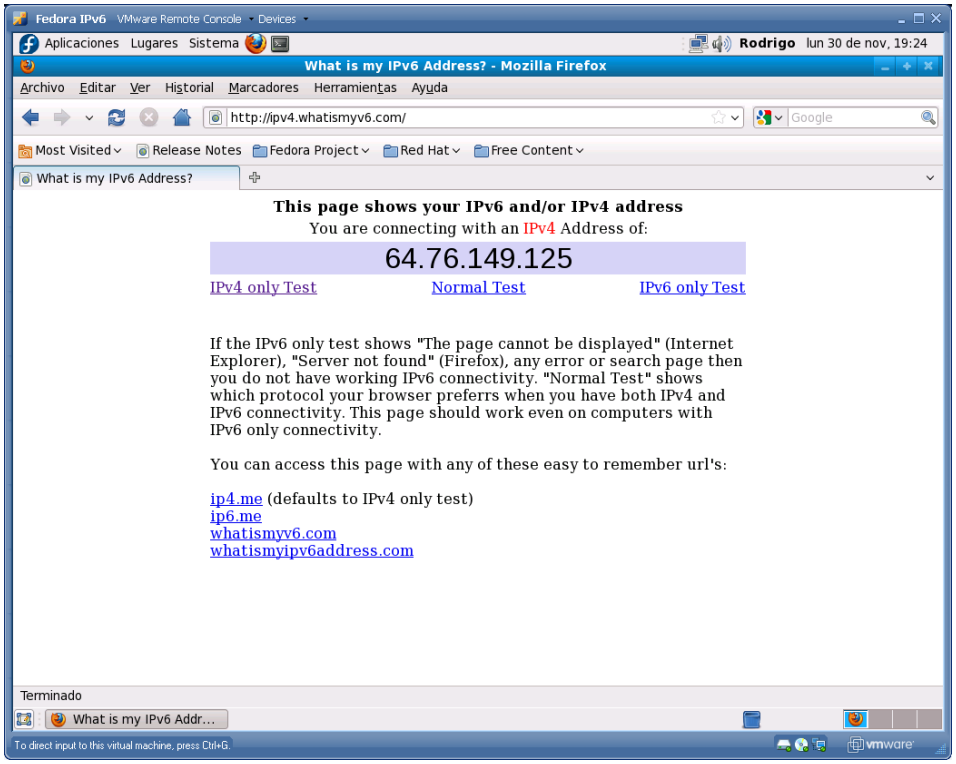


Figura 5.5: Prueba de conexión IPv4 desde la DMZ

.

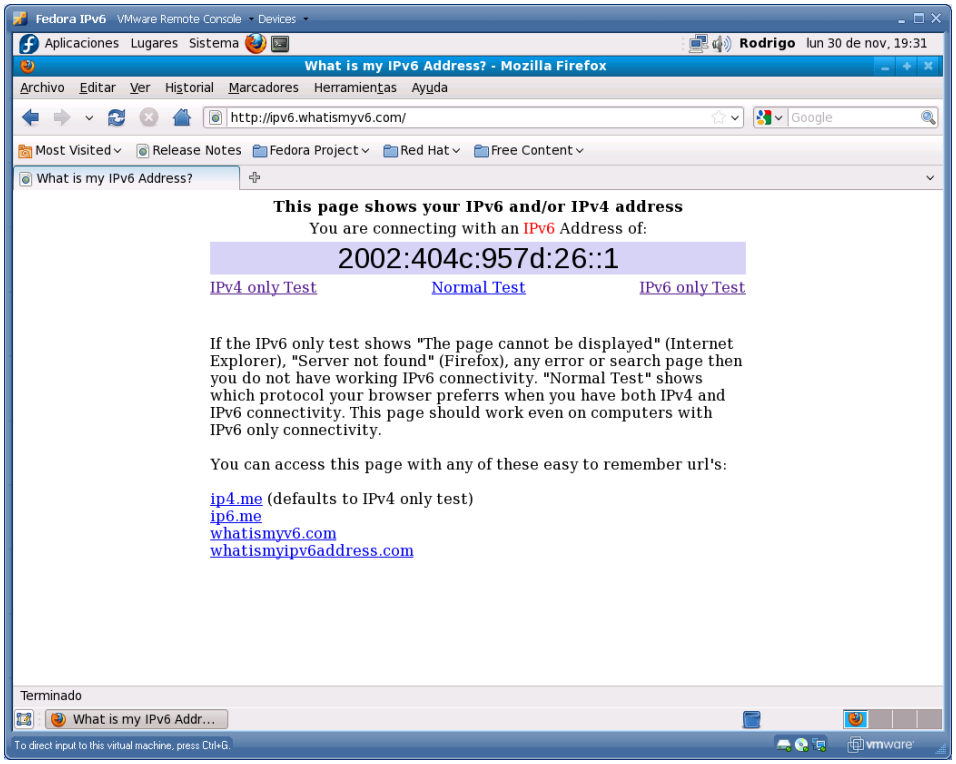


Figura 5.6: Prueba de conexión IPv4 desde la DMZ

5.2.8.3 Conectividad desde la red interna hacia la DMZ

Se efectúa una conexión desde el host con Windows 7 a la página web provista por el servidor ubicado en la DMZ, mediante la URL http://server1/. Esto permite verificar tanto el funcionamiento del servidor DNS (configurado mediante DHCP con la IP del servidor de la DMZ) como el del servidor HTTP, ambos sobre IPv4 (véase Figura 5.7).

Posteriormente se carga la misma página web, pero ahora utilizando la dirección http://server1-v6, que sólo es accesible mediante IPv6, según la configuración del servidor DNS (véase Figura 5.8).

Por último, se asigna de forma estática la dirección IPv6 del servidor DNS (Figura 5.9), de modo que las resoluciones DNS se efectúen sobre IPv6 y no sobre IPv4. La prueba realizada para verificar el funcionamiento del servidor DNS sobre IPv6 consiste en realizar una consulta mediante el comando *nslookup* (véase Figura 5.10).

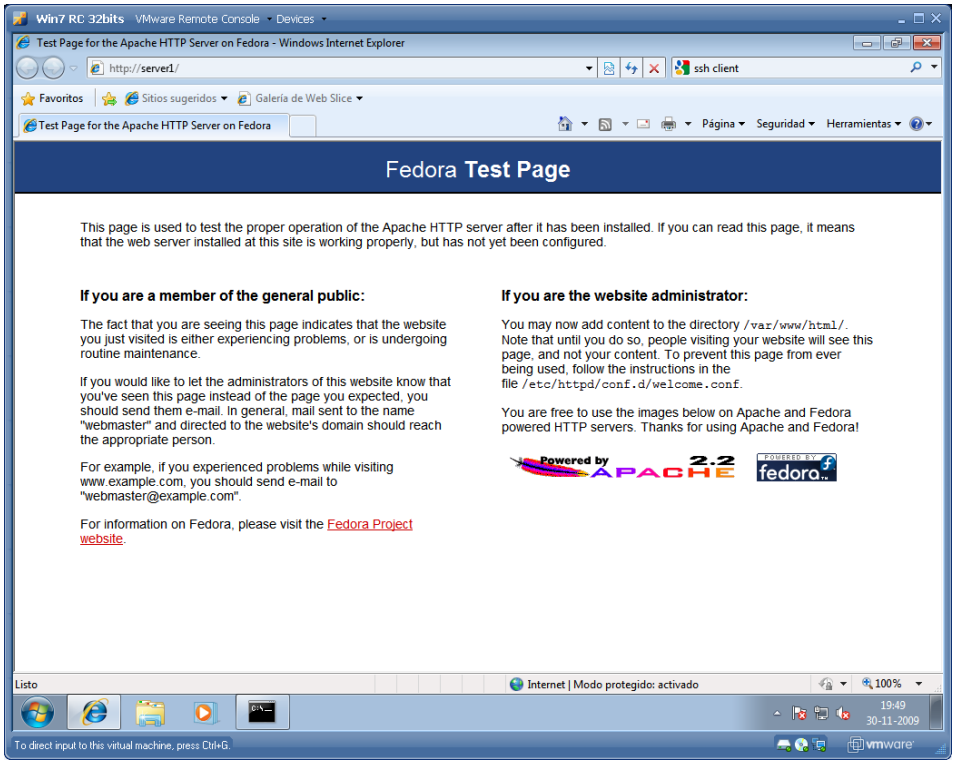


Figura 5.7: Prueba de conexión IPv4 a la DMZ desde red interna

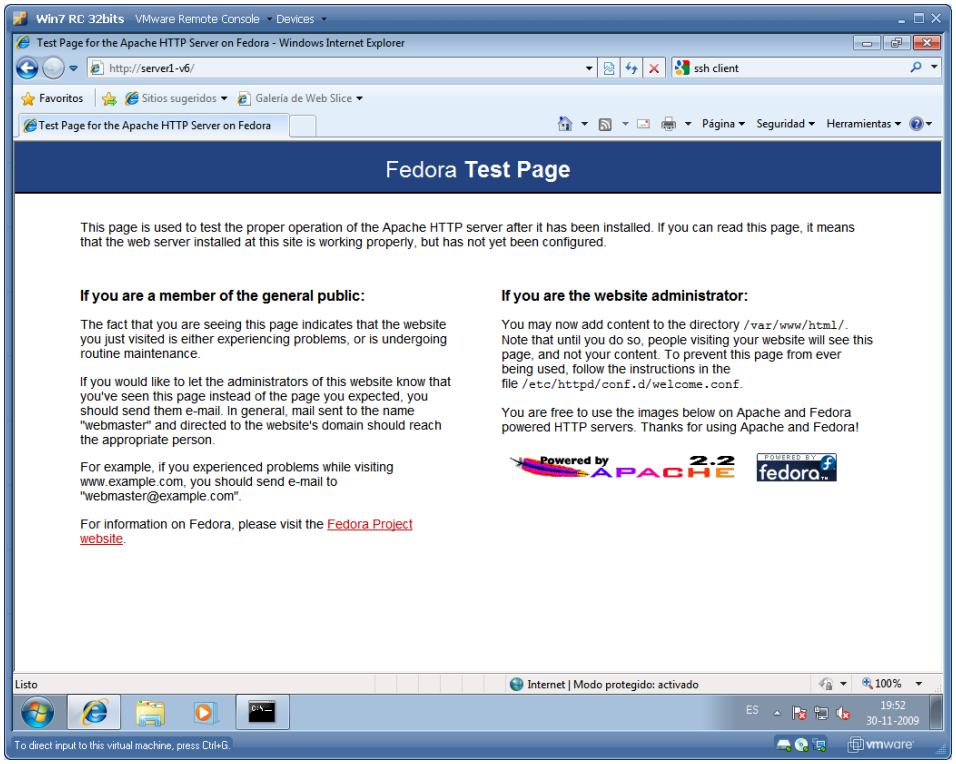


Figura 5.8: Prueba de conexión IPv6 a la DMZ desde red interna

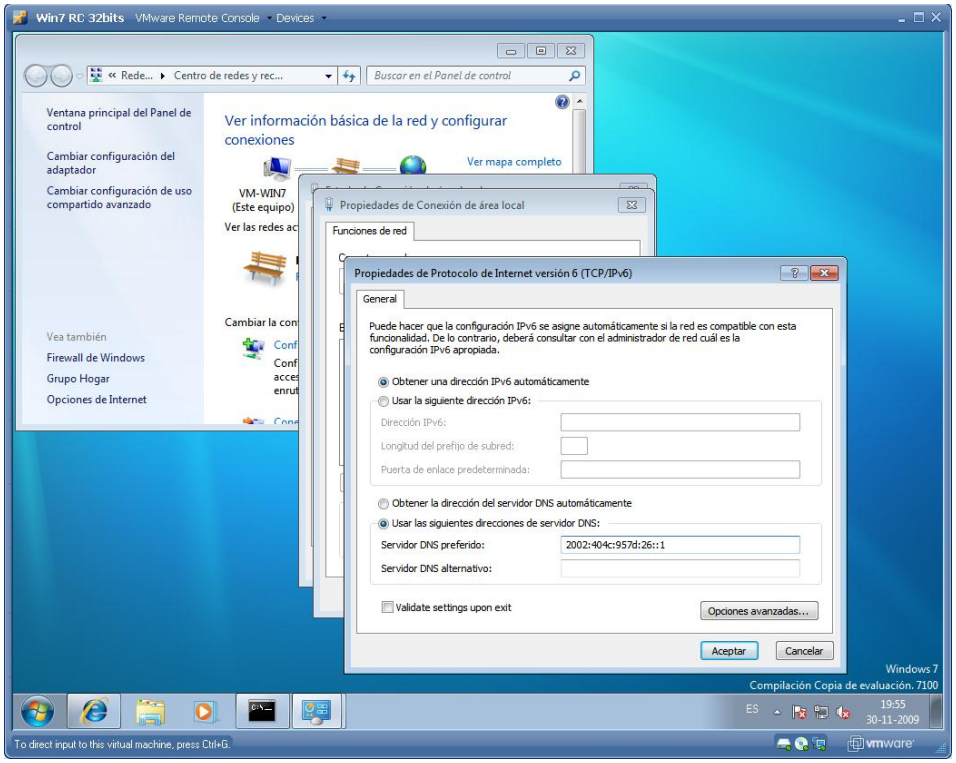


Figura 5.9: Configuración estática de servidor DNS sobre IPv6

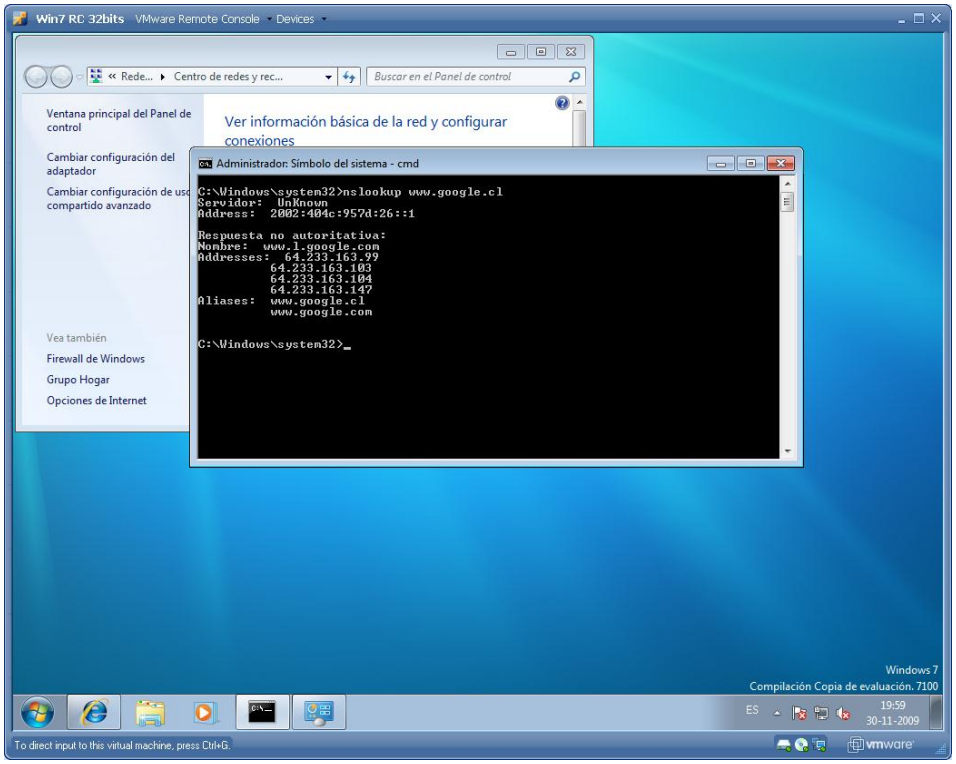


Figura 5.10: Prueba de resolución DNS sobre IPv6

5.2.8.4 Conectividad desde la red interna hacia Internet IPv4 e IPv6

Siguiendo las mismas pruebas realizadas en 5.2.8.2, desde la red interna se cargan las URL http://ipv4.whatismyv6.com y http://ipv6.whatismyv6.com, obteniendo respectivamente los resultados de la Figura 5.11 y Figura 5.12.

Con estas pruebas se puede verificar el funcionamiento del servidor DNS y además la conectividad IPv4 e IPv6, la cual resulta transparente para un eventual usuario de esta red.

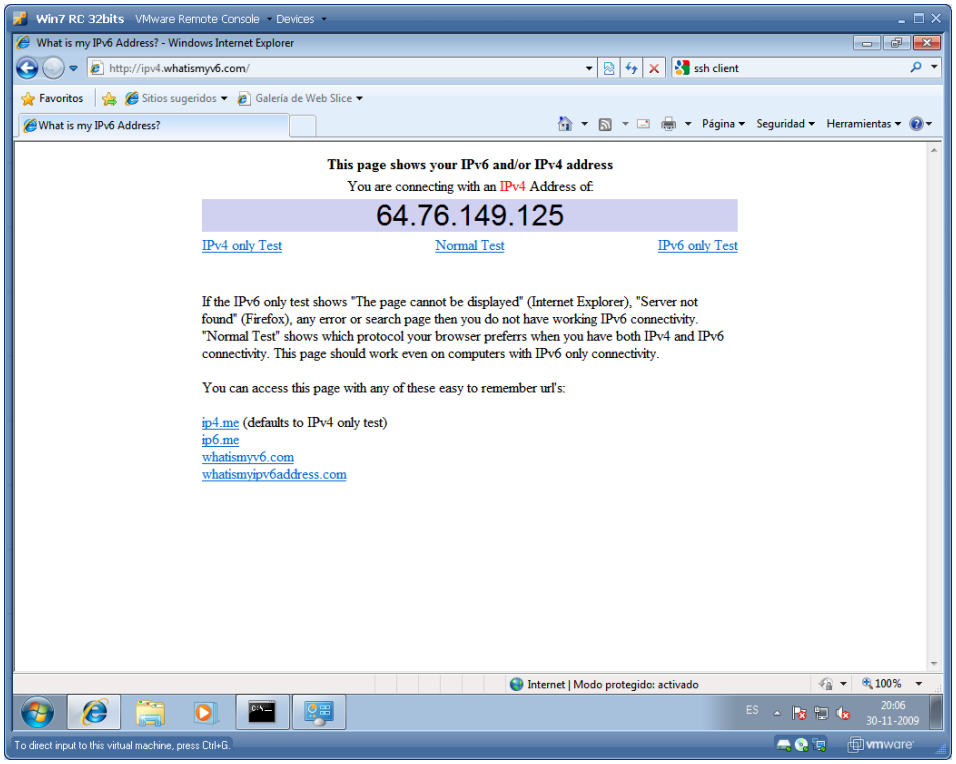


Figura 5.11: Prueba de conexión IPv4 desde la red interna

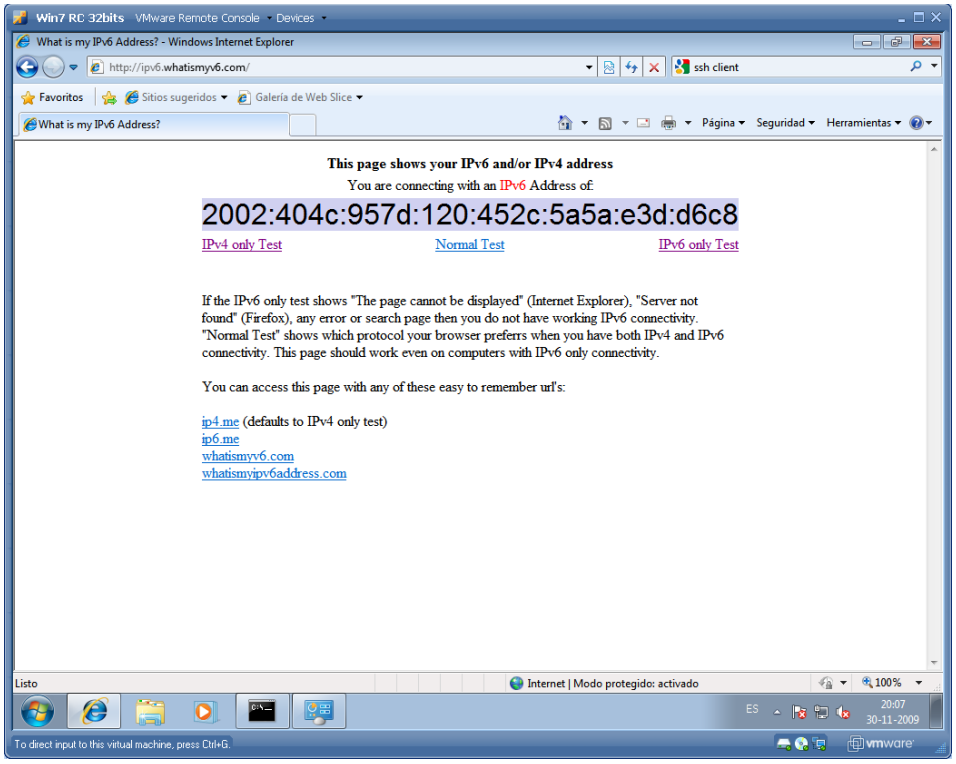


Figura 5.12: Prueba de conexión IPv6 desde la red interna

Capítulo 6: Planilla para evaluación económica

El servicio ofrecido para validar la compatibilidad con IPv6, descrito en el Capítulo 4, finaliza con la evaluación económica de los requisitos necesarios para actualizar la red de la empresa mandante dejándola en condiciones de operar sobre este protocolo.

A continuación se presenta una planilla elaborada con el objetivo de estimar tanto las inversiones en que deberá incurrir la empresa mandante como los beneficios potenciales que le brindará adoptar el protocolo IPv6. Esta planilla fue concebida para su utilización por parte de una empresa de servicios de redes, permitiéndole cuantificar, al menos en una etapa de preventa, los costos y beneficios que este servicio ofrece a cada cliente en particular, facilitando además el cálculo de indicadores relevantes desde el punto de vista económico como lo son el período de recuperación (*payback*), el VAN o la TIR de un proyecto de adopción de IPv6.

En este capítulo se describe en términos generales la planilla diseñada, incluyendo una descripción de los parámetros que se consideran para el cálculo de los costos y beneficios del proyecto e instrucciones para la utilización de la planilla. Cada una de las hojas que la componen se puede visualizar en el Anexo C.

6.1 Características de la planilla

La planilla corresponde a un Libro de Microsoft Excel 2007, compuesto de seis hojas cuya funcionalidad se indica a continuación:

Hoja "Instrucciones"

Descripción del alcance de la planilla, habilidades esperadas del usuario que la utilice e instrucciones de uso (véase Anexo C.1).

Hoja "Parámetros"

Listado de todos los parámetros numéricos que influyen en el cálculo de los costos y los beneficios asociados al proyecto. Por ejemplo: margen de ganancia de venta del proyecto, costo de equipos, costo de licencias de software, valor de hora hombre para cada tarea, etc (véase Anexo C.2). Al agrupar todos los parámetros numéricos, esta hoja es la más importante de la planilla, permitiendo modificar los valores de parámetros existentes o bien agregar nuevos elementos no considerados en la versión original de la planilla.

Hoja "Costos"

Cálculo de la inversión inicial y costos operacionales anuales del proyecto, en función de los elementos seleccionados en la categoría "Parámetros" y de las cantidades indicadas en la misma hoja para cada elemento (véase Anexo C.3).

Para apoyar el llenado de la hoja de costos, debido a que cada cliente podría requerir de equipamiento y servicios distintos para evaluar y eventualmente migrar su red particular, en esta hoja se hace uso de una Macro que permite listar sólo los parámetros seleccionados en la hoja "Parámetros". La forma de utilizar esta Macro es mediante un botón incluido en la misma hoja "Costos". El código utilizado para la Macro se puede visualizar en el Anexo C.7.

Hoja "Beneficios"

Cálculo de los beneficios anuales del proyecto, agrupados en las categorías que se describen en 6.2.2 y cuantificados en función de los parámetros incluidos en la hoja "Parámetros" bajo la categoría "Operación de Red IPv4" (véase Anexo C.4).

Hoja "ROI"

Cálculo del período de recuperación para el proyecto de adopción de IPv6, mediante un gráfico de recuperación de capital en función del tiempo, pero sin considerar una tasa de descuento (véase Anexo C.5).

Hoja "Flujos"

Construcción del flujo de caja del proyecto, a partir de los parámetros seleccionados en las hojas anteriores. Como resultado del flujo de caja es posible obtener el VAN la TIR y el

período de recuperación del proyecto, para una tasa de descuento configurable en la misma hoja (véase Anexo C.6).

6.2 Parámetros considerados

Se describen a continuación los criterios utilizados para cuantificar tanto los costos como los beneficios asociados a la adopción de IPv6 en una red empresarial.

6.2.1 Costos

Los costos involucrados en el proyecto se separan en los costos iniciales, correspondientes a la inversión, y los costos anuales de operación del proyecto.

6.2.1.1 Inversión

Para calcular la inversión necesaria se toman en cuenta los siguientes aspectos:

Hardware

En esta categoría se agrupa todo el equipamiento a instalar en la red. Por ejemplo: Routers, switches, firewalls y servidores para aplicaciones específicas.

Software

Corresponde a las licencias de Sistemas Operativos a instalar en la red, para ser utilizados ya sea como servidores (por ejemplo, Red Hat Linux) o bien como clientes (por ejemplo, Windows 7).

Soporte

Comprende los contratos de soporte asociados a algunos equipos contemplados dentro del proyecto. En algunos casos estos contratos son atendidos directamente por el fabricante, mientras que en otros casos la encargada de brindar soporte técnico a los equipos es la propia empresa de redes.

Instalación

Corresponde al costo asociado al cableado y a las instalaciones requeridas para los equipos de red que se instalan en este proyecto. En la hoja "Parámetros", es posible cambiar el costo unitario (por puerta de red) modificando el ítem 27.

Recursos Humanos (RRHH)

Agrupa a todo el personal técnico y de ingeniería necesario para cada etapa del proyecto. La manera de contabilizar estos recursos es mediante las Horas Hombre (HH) unitarias para cada categoría, cuyo valor se puede ajustar mediante los ítems 40 al 47 de la hoja "Parámetros". Dentro de esa hoja es posible además seleccionar qué tipo de RRHH es requerido para el proyecto según la complejidad de la empresa a la que se le proporciona el servicio.

Enlace

En caso de que la empresa mandante no cuente con conectividad IPv6 nativa, se incluye esta categoría para agrupar los costos asociados a un enlace IPv6.

Margen de ganancia

Sobre el total de la inversión se aplica un margen de ganancia definido por la empresa de redes para la venta del proyecto, el cual se suma a esta inversión. Este margen se puede modificar cambiando el valor del ítem 3 de la hoja "Parámetros".

6.2.1.2 Costos operacionales

Estos corresponden a costos anuales asociados a la operación y el mantenimiento de la red, y se desglosan en las siguientes dos categorías:

Mantención de cables y puntos de red

Este costo se cuantifica en función de las fallas de puntos de red esperables dentro de la red instalada. El cálculo de este costo se obtiene de la siguiente relación:

$$\text{Costo}_{\text{mant puntos}} = n_{\text{fallas cableado}} \times \text{Costo}_{\text{mant 1 punto}}$$

La descripción de cada término se muestra en la Tabla 6.1.

Tabla 6.1: Términos utilizados para el costo de mantención de cables y puntos de red

Término	Descripción	Ítem en hoja "Parámetros"
$\text{Costo}_{\text{mant puntos}}$	Costo de mantención asociado a fallas en puntos de red, en US$	-
$n_{\text{fallas cableado}}$	Número anual de fallas de cableado	54
$\text{Costo}_{\text{mant 1 punto}}$	Costo de reparación de un punto de red, en US$	55

Mantención de equipos de red

Este costo se calcula como un porcentaje del costo asociado al hardware instalado en la red, utilizando la relación:

$$\text{Costo}_{\text{mant equipos}} = \text{Costo}_{\text{HW}} \times \frac{\%_{\text{costo HW}}}{100}$$

La descripción de cada término se observa en la Tabla 6.2.

Tabla 6.2: Términos utilizados para el costo de mantención de equipos de red

Término	Descripción	Ítem en hoja "Parámetros"
$\text{Costo}_{\text{mant equipos}}$	Costo de mantención asociado a equipamiento de la red, en US$	-
Costo_{HW}	Costo total del hardware instalado en la red, en US$	-
$\%_{\text{costo HW}}$	Porcentaje del costo de hardware considerado para mantención y reparaciones, en US$	56

6.2.2 Beneficios

Para evaluar los beneficios se tomaron como referencia algunas de las ventajas descritas en el Capítulo 3, buscando parámetros que permitieran cuantificar los ahorros que produce por si sola la adopción de IPv6 en una red empresarial. A continuación se describe el procedimiento utilizado para cuantificar cada beneficio, incluyendo en cada caso una tabla que permite listas los parámetros relevantes y la ubicación de estos dentro de la hoja "Parámetros".

6.2.2.1 Planificación Anticipada

Se cuantifica en términos del ahorro en el *Project Manager* que deberá dedicarse al proyecto en forma exclusiva en caso de una migración tardía, desarrollando todo el estudio de factibilidad y una propuesta de migración. El supuesto para calcular este ahorro es que en un plazo de 5 años desde el tiempo presente, el protocolo IPv6 se volverá necesario para la operación de las empresas, por lo que este ahorro se considera recién en el año 5 del horizonte de evaluación. El ahorro por una planificación anticipada se calcula según:

$$\text{Ahorro}_{\text{PA}} = \text{HH}_{\text{PM}} \times \text{C}_{\text{PM}} \times \frac{\text{UF}}{\text{USD}}$$

La descripción de cada término se visualiza Tabla 6.3.

Tabla 6.3: Términos utilizados para el ahorro por planificación anticipada

Término	Descripción	Ítem en hoja "Parámetros"
$Ahorro_{PA}$	Ahorro por planificación anticipada de IPv6, en US$	-
HH_{PM}	Horas hombre de *Project Manager* dedicado a migración tardía de IPv6 en la empresa	63
C_{PM}	Costo de una hora hombre de *Project Manager*, en UF	46
UF	Valor de la UF, en CLP	1
USD	Valor del dólar, en CLP	2

6.2.2.2 Diseño escalable en asignación de direcciones

Debido a que en IPv6 se dispone de un número prácticamente infinito de direcciones por cada subred, se evita la necesidad de crear nuevas subredes cuando el número de hosts en un determinado segmento de red aumenta, con el consiguiente ahorro en los recursos necesarios para un proyecto de adición de subredes. Si se considera que en una empresa se agrega en promedio 1 subred al año, involucrando en este proyecto a un *Project Manager* y un *Field Engineer*, el ahorro por este ítem se calcula según:

$$\text{Ahorro}_{\text{DE}} = (HH_{PM} \times C_{PM} + HH_{FE} \times C_{FE}) \times \frac{\text{UF}}{\text{USD}}$$

La descripción de cada término se presenta en la Tabla 6.4.

6.2.2.3 Administración simplificada para la continuidad operativa y fallas

En esta categoría se agrupan beneficios atribuibles a características específicas de IPv6, que permiten mantener la conectividad y mitigar las fallas al interior de una red.

IP móvil

Debido a que con IP móvil se mantienen las conexiones establecidas, independiente de la ubicación dentro de la red, adoptar IPv6 permite ahorrar en consultas a *Helpdesk* debido a problemas con conexiones ya establecidas, en caso de que un usuario deba moverse de un sitio de la red a otro.

Tabla 6.4: Términos utilizados para el ahorro por diseño escalable

Término	Descripción	Ítem en hoja "Parámetros"
$Ahorro_{DE}$	Ahorro por diseño escalable en asignación de direcciones, en US$	-
HH_{PM}	Horas hombre de *Project Manager* dedicado a adición de 1 subred en la empresa	64
C_{PM}	Costo de una hora hombre de *Project Manager*, en UF	46
HH_{FE}	Horas hombre de *Field Engineer* dedicado a adición de 1 subred en la empresa	65
C_{FE}	Costo de una hora hombre de *Field Engineer*, en UF	41
UF	Valor de la UF, en CLP	1
USD	Valor del dólar, en CLP	2

El beneficio asociado a IP Móvil se cuantifica de manera anual, según:

$$\text{Ahorro}_{\text{IP Móvil}} = (n_{consultas} \times t_{HD} \times C_{HD}) \times \frac{\text{UF}}{\text{USD}}$$

La descripción de cada término se muestra en la Tabla 6.5.

Tabla 6.5: Términos utilizados para el ahorro por uso de IP Móvil

Término	Descripción	Ítem en hoja "Parámetros"
$Ahorro_{IP\ Móvil}$	Ahorro debido al uso de IP Móvil, en US$	-
$n_{consultas}$	Número de consultas anuales a *Helpdesk* debido a pérdida de conexiones establecidas al cambiarse de localización (subred)	59
t_{HD}	Tiempo de respuesta de *Helpdesk*, en horas	60
C_{HD}	Costo de una hora hombre de *Helpdesk*, en UF	47
UF	Valor de la UF, en CLP	1
USD	Valor del dólar, en CLP	2

Autoconfiguración

La autoconfiguración en IPv6 permite a un host asignarse de manera sencilla una dirección IP y una puerta de enlace, en base al prefijo de la subred a la que el host se conecta. Esto se traduce en un ahorro en consultas a Helpdesk debido a problemas con ausencia o pérdida de conectividad al llegar a un nuevo punto de red, el cual se calcula usando:

$$\text{Ahorro}_{\text{Autoconf}} = (n_{consultas} \times t_{HD} \times C_{HD}) \times \frac{\text{UF}}{\text{USD}}$$

La descripción de cada término se observa en la Tabla 6.6.

Tabla 6.6: Términos utilizados para el ahorro por uso de autoconfiguración

Término	Descripción	Ítem en hoja "Parámetros"
$\text{Ahorro}_{\text{Autoconf}}$	Ahorro debido al uso de autoconfiguración, en US$	-
$n_{consultas}$	Número de consultas anuales a *Helpdesk* debido a ausencia o pérdida de conectividad al cambiarse de localización (subred)	57
t_{HD}	Tiempo de respuesta de *Helpdesk*, en horas	58
C_{HD}	Costo de una hora hombre de *Helpdesk*, en UF	47
UF	Valor de la UF, en CLP	1
USD	Valor del dólar, en CLP	2

Eliminación de NAT

En IPv4, debido a la utilización de NAT y direccionamiento privado hace necesario realizar un mapeo estático de puertos cada vez que se habilita un nuevo servicio desde la red interna hacia Internet, además de la habilitación de este puerto en el firewall de borde mediante la lista de acceso correspondiente. Con IPv6, al no ser necesario el uso de NAT, sólo se requiere habilitar el puerto en el firewall, lo que conlleva un ahorro en los recursos requeridos para realizar el mapeo de puertos, calculado según:

$$\text{Ahorro}_{\text{NAT}} = \left(n_{app} \times t_{HD} \times C_{HD}\right) \times \frac{\text{UF}}{\text{USD}}$$

La descripción de cada término se presenta en la Tabla 6.7.

Tabla 6.7: Términos utilizados para el ahorro por eliminación de NAT

Término	Descripción	Ítem en hoja "Parámetros"
$Ahorro_{NAT}$	Ahorro debido a la eliminación de NAT, en US$	-
n_{app}	Número de aplicaciones para las cuales se requiere abrir puertos de NAT, anualmente	61
t_{HD}	Tiempo de configuración de *Helpdesk* , en horas	62
C_{HD}	Costo de una hora hombre de *Helpdesk* , en UF	47
UF	Valor de la UF, en CLP	1
USD	Valor del dólar, en CLP	2

6.3 Instrucciones de uso

Para hacer uso de la planilla de evaluación económica se deben seguir las instrucciones presentadas a continuación, tanto para la operación habitual de la planilla (ítems A, B y C) como para la edición de los parámetros contenidos en ella (ítem D). Estas instrucciones están además incluidas en la hoja “Instrucciones” de la misma planilla.

A. Llenado de planilla de Costos

1. En la hoja "Parámetros" elegir los componentes que son relevantes para la estimación de los costos, haciendo click en la casilla ubicada en la misma fila del componente deseado.

2. Tras seleccionar todos los componentes relevantes, en la hoja "Costos" hacer click sobre el botón "Actualizar Planilla" ubicado en la columna G. Esto producirá el borrado y re-llenado de la planilla, salvo los ítems ubicados bajo la fila "Operación y Mantención de la Red" que permanecerán sin modificaciones.

3. Para los elementos cuya categoría aparezca en la columna "Categoría" de la hoja "Costos", indicar en la columna "Cantidad" la cantidad asociada a dichos elementos. Esto actualizará el Costo de Inversión asociado a cada elemento, el margen de ganancia del proyecto y el Total de costo de inversión con los elementos considerados.

4. El gráfico final del ROI se actualizará automáticamente en función de los parámetros definidos en la manipulación de la planilla.

B. Llenado de planilla de Beneficios

1. En la hoja "Parámetros" revisar y, de ser necesario, corregir los valores asignados en la sección "Operación de Red IPv4" (en base al cliente que se esté evaluando).

2. Revisar que los cálculos se hayan realizado de forma correcta en la planilla "Beneficios". El cálculo se realiza de forma automática.

C. Llenado de planilla de ROI

1. En la hoja "ROI", la tabla superior se llena automáticamente con los datos calculados anteriormente (Costo Inversión Inicial, Costo Operacional Anual, Ahorro Operacional Fijo, Ahorro Operación Anual).

2. En la columna Comentario modificar, de ser necesario, la cantidad de años considerados para que se considere el Ahorro Operacional Fijo (por defecto son 5 años).

3. En la tabla inferior de la hoja "ROI" se calculará de forma automática el retorno anual de la inversión. En caso de cambiar la cantidad de años considerados para que se considere el Ahorro Operacional Fijo (5 por defecto), se deben modificar las fórmulas de modo que sean coherentes con las consideraciones realizadas.

D. Inserción de nuevos componentes en el listado de la hoja "Parámetros"

1. En la hoja "Parámetros", situarse en la sección correspondiente al componente que se desea agregar (Equipo Cisco, Licencia de Software, etc).

2. Agregar una fila de manera usual (Botón derecho > Insertar > Filas de la tabla arriba).

3. Agregar los parámetros Item, Categoría, Código, Nombre, Precio Lista, Unidad y Comentarios/Valor Típico relacionados con el componente.

4. En la columna G agregar una casilla de verificación (Menú Programador > Insertar > Casilla de verificación (control de formulario)).

5. Vincular la casilla de verificación con la celda de la columna I en la misma fila.

Capítulo 7: Discusión y Conclusiones

Se presenta a continuación una discusión del trabajo realizado, así como las conclusiones finales al terminar este trabajo y las tareas sugeridas para complementarlo y mejorarlo.

7.1 Discusión

Durante el desarrollo de este trabajo se observó que IPv6 es actualmente un protocolo maduro y completo, lo que se valida con las múltiples recomendaciones y estándares que existen en torno a este protocolo. Sin embargo, su adopción a nivel mundial no ha tenido aún el despegue esperado en función del agotamiento actual de direcciones IPv4. Si bien esta lenta adopción podría sugerir que en el escenario actual es demasiado temprano para ofrecer un servicio de migración hacia IPv6, sí se justifica contar con un servicio de validación como el propuesto en este trabajo, cuyo principal beneficio para una empresa es la posibilidad de diseñar un plan de actualizaciones que aproveche los procesos naturales de renovación tecnológica y que además le permita tener su red completamente preparada para cuando la adopción de IPv6 se vuelva una necesidad imperante.

Respecto al soporte de equipos y aplicaciones, en el Capítulo 3 se mostró que actualmente los principales fabricantes sí están considerando el soporte de IPv6 como un requerimiento para sus plataformas y aplicaciones. Este hecho hace suponer que, mediante los procesos de renovación tecnológica, las empresas -incluso sin saberlo- han ido adquiriendo tecnología que ya tiene compatibilidad con IPv6, por lo que las inversiones necesarias para una adopción completa del protocolo podrían no ser tan elevadas como se esperaría. En la medida que todos los fabricantes se pongan al día con el soporte de IPv6 en sus equipos y aplicaciones y

que las empresas inviertan en renovar sus plataformas tecnológicas, el proceso de migración a este protocolo resultará cada vez más económico.

El servicio diseñado en este trabajo permite guiar los procesos de renovación, recomendando las versiones de software y hardware más adecuadas para una empresa, en función de su equipamiento actual y de las características específicas del protocolo IPv6 que se requieran utilizar a futuro. En este sentido, al integrar estos requisitos técnicos en los procesos de renovación tecnológica, la estrategia definida en el Capítulo 4 permite minimizar el costo incremental en que se incurrirá una vez que el protocolo IPv6 se vuelva una necesidad, puesto que tras contar con el equipamiento y aplicaciones adecuadas, las inversiones que una empresa deberá realizar para la adopción de IPv6 en su red corresponden sólo a recursos humanos destinados para configurar y validar la operación del protocolo.

Tanto para la empresa que provee el servicio como para la empresa lo contrata, la implementación de un laboratorio como el presentado en el Capítulo 5 es fundamental a la hora de probar el protocolo IPv6. Para la primera, esto facilita el aprendizaje en torno al protocolo, homologando el conocimiento entre su personal técnico mediante actividades prácticas de configuración y validación de IPv6, lo que les permite ganar experiencia que diferenciará a la empresa al momento de ofrecer sus servicios. Para la segunda, en tanto, el laboratorio ofrece la oportunidad de observar y evaluar en sus propias dependencias el funcionamiento de IPv6, ya sea en un entorno exclusivo o en una modalidad *dual stack* y, al mismo tiempo, validar el soporte de IPv6 en aplicaciones internas, sin perturbar la red de producción dentro de la empresa.

El hecho de contar con un laboratorio basado en clientes y servidores virtualizados contenidos en un único servidor físico y contar además con scripts de configuración para los equipos utilizados facilita significativamente la replicación de este laboratorio en la red de un cliente, habiendo probado previamente que las configuraciones funcionaban adecuadamente, requiriendo de pocos componentes físicos (con el consiguiente ahorro de espacio) y siendo necesarias sólo adaptaciones menores para su integración en la red de la empresa.

Por otra parte, en relación a los aspectos económicos asociados al servicio ofrecido y a la adopción de IPv6, los parámetros considerados para la evaluación de este proyecto y descritos en el Capítulo 6 podrían no ser suficientes para mostrar un beneficio económico asociado al proyecto de migración. Un resultado preliminar que ejemplifica este hecho, si bien con valores

no totalmente representativos, es el que se observa en el Anexo C en la aplicación práctica de la planilla diseñada. Más allá de las cifras, la naturaleza de la estrategia diseñada no es generar un ahorro absoluto en sus operaciones a los potenciales clientes, sino más bien un ahorro relativo respecto a una adopción descoordinada y planificada tardíamente. Además, este resultado se alínea con lo anticipado al comienzo del Capítulo 3, respecto a que las inversiones necesarias para integrar IPv6 por sí solas no se traducen en un ahorro tangible para la empresa que realice estas inversiones.

En este sentido, todo parece apuntar a que los beneficios económicos de adoptar IPv6 no se verán como un factor intrínseco de esta adopción, sino fundamentalmente en las nuevas oportunidades de servicios y aplicaciones que puedan operar sobre este protocolo (aprovechando sus ventajas técnicas por sobre IPv4) para contribuir a la operación del negocio de una empresa. De todos modos, se considera valioso el ejercicio de cuantificar tanto los costos como los beneficios del proyecto de adopción de IPv6, logrando construir una planilla extensible a nuevos parámetros que surjan para medir los costos y beneficios del protocolo.

7.2 Conclusiones

Con el desarrollo de este trabajo, se logró estudiar las ventajas que brinda la implementación de IPv6 en redes empresariales desde el punto de vista técnico, considerando características que hacen de IPv6 un protocolo superior a IPv4 y que ofrecen oportunidades para crear nuevas aplicaciones y mejorar las existentes. En el proceso de estudiar las ventajas de IPv6, se logró además verificar el actual estado de las principales aplicaciones y equipos de red para soportar la integración con el protocolo.

Respecto al proceso de migración, se definió una estrategia para abordar la adopción de IPv6 mediante un servicio de validación de compatibilidad en redes empresariales. Este servicio permite evaluar los equipos y aplicaciones de este tipo de redes, estableciendo los requisitos para dejarlas en condiciones de operar con IPv6, lo que permite a las empresas planificar de manera anticipada esta adopción y alinear estos requisitos con los procesos naturales de renovación tecnológica. Por otra parte, como complemento al servicio ofrecido fue posible establecer recomendaciones generales sobre los aspectos a considerar por una empresa de servicios de redes en caso de recibir un requerimiento de adopción de IPv6.

Finalmente, en la estrategia diseñada se propuso un procedimiento para clasificar los equipos y aplicaciones de una red empresarial en función de su compatibilidad con IPv6, lo que permite evaluar la factibilidad de realizar la migración a IPv6 en cada empresa. Además, mediante la planilla diseñada para la evaluación económica es posible estimar el costo que tiene para la empresa mandante el actualizar sus plataformas no compatibles, junto con los recursos que la empresa de servicios de redes deberá destinar para soportar el proceso de migración.

En base a estos logros, se consideran cumplidos los objetivos generales y específicos planteados para este trabajo.

7.3 Trabajo Futuro

Antes de ofrecer comercialmente el servicio definido en este trabajo, resulta conveniente realizar una actividad piloto donde este servicio se valide con la propia red de la empresa de servicios de redes. Esto permitirá corregir o agregar detalles no contemplados, así como mejorar la estimación de los recursos requeridos en el proceso. Lamentablemente, esta actividad no pudo ser desarrollada en el presente trabajo, debido a que el tiempo necesario para realizar un levantamiento de la red escapa a los plazos y objetivos planteados en esta memoria.

Otro aspecto que complementaría el desarrollo del servicio ofrecido es el uso de conectividad IPv6 nativa para el laboratorio implementado, de modo de no utilizar túneles sobre IPv4. Esto no fue posible en este caso debido a que requería la contratación de un servicio dedicado de acceso a IPv6, el cual habría sido subutilizado por la empresa si sólo se hubiese destinado a las pruebas del laboratorio implementado en este trabajo, razón por la cual finalmente no fue adquirido.

Finalmente, queda propuesto ahondar en los aspectos relativos a la evaluación económica del proyecto. Se hace necesario estudiar con más detalle los potenciales beneficios económicos de IPv6, pues sólo teniendo claridad respecto a estos beneficios asegurará, en el mediano plazo, el despliegue masivo del protocolo en redes empresariales.

Acrónimos

ASA *Adaptive Security Appliance.*

ASDM *Adaptive Security Device Manager.*

BGP4-MP *Border Gateway Protocol version 4- MultiProtocol.*

CLI *Command Line Interface*. Línea de comandos.

DHCP *Dynamic Host Configuration Protocol.*

DHCPv6 DHCP versión 6.

DMZ *Demilitarized Zone*. Zona Desmilitarizada.

DNS *Domain Name System.*

DoS *Denial of Service.*

EIGRP *Enhanced Interior Gateway Routing Protocol.*

EUI-64 *Extended Unique Identifier, 64-bit.*

FTP *File Transfer Protocol.*

HTTP(S) *Hypertext Transfer Protocol (Secure).*

IANA *Internet Assigned Numbers Authority*

ICMP *Internet Control Message Protocol.*

ICMPv6 ICMP versión 6.

IETF *Internet Engineering Task Force.*

IOS *Internetwork Operating System.*

ISATAP *Intra-site Automatic Tunnel Addressing Protocol.*

ISO *International Standarization for Organization*

IP *Internet Protocol.*

IPSec *Internet Protocol Security.*

IPv4 IP versión 4.

IPv6 IP versión 6.

ISP *Intenet Service Provider.*

LAN *Local Area Network.*

MAC *Media Access Control.*

MTU *Maximun Transfer Unit.*

NAT *Network Address Translation.*

OSI *Open System Interconnection.*

OSPF *Open Shortest Path First.*

PAT *Port Address Translation.*

PDU *Protocol Data Units.*

RA *Router Advertisement.*

RIP *Routing Information Protocol.*

RIPng RIP *next generation*

RIR *Regional Internet Registry*.

SSH *Secure Shell.*

TIR Tasa interna de retorno.

VAN Valor actual neto.

VLAN *Virtual LAN.*

Referencias

[1] NUMBER RESOURCE ORGANIZATION. Less than 10% of IPv4 Addresses Remain Unallocated, says Number Resource Organization. [en línea] <http://www.nro.net/media/less-than-10-percent-ipv4-addresses-remain-unallocated.html> [consulta: 22 febrero 2010]

[2] HURRICANE ELECTRIC INTERNET SERVICES. Hurricane Electric IPv4 Exhaustion Counters. [En línea] <http://ipv6.he.net/statistics/> [consulta: 17 febrero 2010]

[3] NORDMARK, E. y Gilligan, R. RFC 4213 Basic Transition Mechanisms for IPv6 Hosts and Routers. Octubre 2005.

[4] SHIN, M-K., HONG Y-G., HAGINO, J., SAVOLA, P. y CASTRO, E. M. RFC 4038 Application Aspects of IPv6 Transition. Marzo de 2005.

[5] DEERING, S. y Hinden, R. RFC 2460 Internet Protocol Version 6 Specification. Diciembre 1998.

[6] JOHNSON, D., PERKINS, C. y ARKKO, J. RFC 3775 Mobility Support in IPv6. Junio 2004.

[7] HUITEMA, C. y Carpenter, B. RFC 3879 Deprecating Site Local Addresses. Septiembre 2004.

[8] MALKIN, G. y Minnear, R. RFC 2080 RIPng for IPv6. Enero 1997.

[9] COLTUN, R., FERGUSON, D. y MOY, J. RFC 2740 OSPF for IPv6. Diciembre de 1999.

[10] AOUN, C. y Davies, E. RFC 4966 Reasons to Move the Network Address Translator - Protocol Translator (NAT-PT) to Historic Status. Julio de 2007.

[11] IAB e IESG. RFC 3177 IAB/IESG Recommendations on IPv6 Address Allocations to Sites. Septiembre de 2001.

[12] SIXXS. SixXS - IPv6 Deployment & Tunnel Broker. [En línea] <http://www.sixxs.net/tools/grh/dfp/all/?country=cl> [consulta: 22 febrero 2010]

[13] NIC CHILE. Servidores de nombre con IPv6 en .CL. [En línea] <https://listas.nic.cl/pipermail/anuncios/2007-September/000105.html> [consulta: 22 febrero 2010]

[14] NIC CHILE. NIC Chile participa en plan piloto IPv6 con Google. [En línea] <http://www.nic.cl/anuncios/2009-09-08.html> [consulta: 22 febrero 2010]

[15] NIC CHILE. Conferencia IPv6 en Chile - IPv6 en Chile. [En línea] <http://www.ipv6enchile.cl/> [consulta: 22 febrero 2010]

[16] NIC LABS. Estrategia de Implementación | IP versión 6 para Chile. [En línea] <http://ipv6.niclabs.cl/node/4> [consulta: 22 febrero 2010]

[17] GRUPO GTD. Grupo GTD. [En línea] <http://www.grupogtd.com/ipv6/> [consulta: 22 febrero 2010]

[18] FLORES, L**.** Implementando IPv6. [En línea] http://www.ipv6enchile.cl/presentaciones/ipv6gtd.pdf/view [consulta: 22 febrero 2010.]

[19] NARTEN, T., DRAVES, R. y KRISHNAN, S. RFC 4941 Privacy Extensions for Stateless Address Autoconfiguration in IPv6. Septiembre de 2007.

[20] CISCO SYSTEMS, INC. Start Here: Cisco IOS SOftware Release Specifics for IPv6 Features. [En línea] <http://www.cisco.com/en/US/docs/ios/ipv6/configuration/guide/ip6-roadmap.html> [consulta: 22 febrero 2010]

[21] AMOSS, John y Minoli, Daniel. IPv6 Network Software and Hardware. En su: Handbook of IPv4 to IPv6 Transition: Methodologies for Institutional and Corporate Networks. Estados Unidos, Auerbach Publications, 2008. pp.143- 160.

[22] BIERINGER, P. Status of Open Source and commercial IPv6 firewall implementations. [En línea] <http://www.bieringer.de/pb/lectures/2007-ECAI6-Status-IPv6-Firewalling-PeterBieringer-Paper.pdf> [consulta: 23 febrero 2010]

[23] CISCO SYSTEMS, INC. Cisco ASA Software Release 8.2. [En línea] <http://www.cisco.com/en/US/prod/collateral/vpndevc/ps6032/ps6094/ps6120/qa_c67-525310.html> [consulta: 22 febrero 2010]

[24] CISCO SYSTEMS, INC. IPv6 Integration in Federal Government: Adopt a Phased Approach for Minimal Disruption and Earlier Benefits. [En línea] <http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6553/prod_case_study_C11-462676-00_IPv6FedGovt.pdf> [consulta: 15 octubre 2009]

[25] TEARE, Diane. Network Fundamentals Review. En su: Designing for Cisco Internetwork Solutions (DESGN). 2ª ed. Estados Unidos, Cisco Press, 2008. pp.3- 55.

[26] TEARE, Diane. Designing IP Addressing in the Network. En su: Designing for Cisco Internetwork Solutions (DESGN). 2° ed. Estados Unidos, Cisco Press, 2008. pp.377- 426.

[27] HAGEN, Silvia. The Structure of the IPv6 Protocol. En su: IPv6 Essentials. 2ª ed. Estados Unidos, O'Reilly, 2006. pp.17- 34.

[28] ODOM, Wendell. IP Version 6. En su: CCNA ICND2 Official Exam Certification Guide. 2ª ed. Estados Unidos, Cisco Press, 2008. pp.577- 614.

[29] VAN DE VELDE, G., HAIN, T., DROMS, R., CARPENTER, B., KLEIN, E.. Additional Benefits Due to Native IPv6 and Universal Unique Addressing. En su: RFC 4864 Local Network Protection for IPv6. Mayo de 2007. pp.31- 33.

[30] WEISSMANN, P. IPv6 Operating Systems - IPv6 Intelligence. [En línea] <http://ipv6int.net/systems/index.html> [consulta: 23 febrero 2010]

[31] CURRENT Status of IPv6 Support for Networking Applications por Peter Bieringer "et al". [En línea] <http://www.deepspace6.net/docs/ipv6_status_page_apps.html> [consulta: 23 febrero 2010]

[32] IPV6 TO STANDARD TEAM. Vendor Application Database - IPv6 to Standard. [En línea] <http://www.ipv6-to-standard.org/index.php> [consulta: 23 febrero 2010.]

[33] HINDEN, R. y Deering, S. RFC 2373 IP Version 6 Addressing Architecture. Julio de 1998.

Anexo A: El formato EUI-64 modificado

Los últimos 64 bits de las direcciones IPv6 corresponden al identificador de interfaz. En una dirección globalmente única, la porción de dirección correspondiente al identificador de interfaz puede tomar cualquier valor, mientras ningún otro host en la misma subred intente utilizar el mismo (IPv6 incluye un método dinámico para que los hosts averigüen si existe una dirección duplicada en la subred antes de utilizar la dirección). Sin embargo, el tamaño del identificador de interfaz fue escogido intencionalmente para permitir la autoconfiguración de direcciones IPv6 incorporando la dirección MAC de la tarjeta de red en el identificador.

Las direcciones MAC tienen 6 bytes (48 bits) de longitud, de modo que no pueden ser copiadas directamente en el identificador de interfaz, el cual tiene 8 bytes (64 bits). Para completar los 64 bits, en IPv6 se separa la dirección MAC en dos mitades de 3 bytes y se inserta el hexadecimal FFFE entre medio. Además se asigna el valor binario 1 al bit U/L de la dirección MAC. Esto se conoce como el formato EUI-64 modificado y se describe en la Figura A.1.

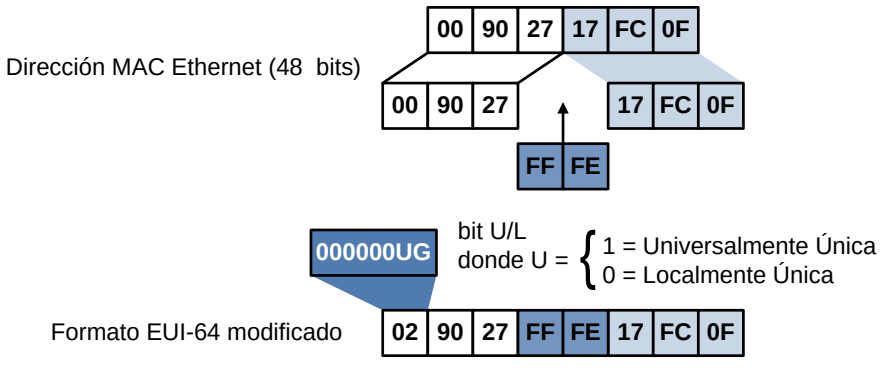


Figura A.1: Construcción del formato EUI-64 modificado

Anexo B: Scripts de configuración de equipos del laboratorio

B.1 Configuración de Switch Catalyst 3750 (sw-memoristas)

```
!
version 12.2
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Switch
!
boot-start-marker
boot-end-marker
!
enable secret 5 $1$bBr5$HFg7QJ8yrXMQ3GLlyv3.b0
!
no aaa new-model
switch 1 provision ws-c3750-48ts
system mtu routing 1500
ip subnet-zero
ip routing
ip domain-lookup source-interface Vlan200
ip domain-name lab-ipv6
ip name-server 2002:404C:957D:26::1
ip name-server 10.10.26.10
!
ipv6 unicast-routing
!
!
crypto pki trustpoint TP-self-signed-1451293056
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-1451293056
 revocation-check none
 rsakeypair TP-self-signed-1451293056
!
!
crypto pki certificate chain TP-self-signed-1451293056
 certificate self-signed 01
  3082023F 308201A8 A0030201 02020101 300D0609 2A864886 F70D0101 04050030
  31312F30 2D060355 04031326 494F532D 53656C66 2D536967 6E65642D 43657274
```

```
  69666963 6174652D 31343531 32393330 3536301E 170D3933 30333031 30303030
  35385A17 0D323030 31303130 30303030 305A3031 312F302D 06035504 03132649
  4F532D53 656C662D 5369676E 65642D43 65727469 66696361 74652D31 34353132
  39333035 3630819F 300D0609 2A864886 F70D0101 01050003 818D0030 81890281
  8100CCCC 2B74CA5F AD2F7F10 CAF6EE01 75893963 4EF0369B B37F157C 2781EAFA
  49C8E1DD 4C590677 96928457 3EC1B076 83308517 6A4A87DA E80AEB52 744F6BD6
  6B798288 64DC5A89 80B3ACED 9E476065 61FEB437 208F3F63 5FDD9E3C B923EBF0
  BFE09A02 0FC9B6AE 00E97B71 D8DD4DEC D7E38EFA 93910F7E 60693855 0B4EE5F9
  D3750203 010001A3 67306530 0F060355 1D130101 FF040530 030101FF 30120603
  551D1104 0B300982 07537769 7463682E 301F0603 551D2304 18301680 14A858D5
  135D1453 7F907469 2F1440B6 EEF0A788 66301D06 03551D0E 04160414 A858D513
  5D14537F 9074692F 1440B6EE F0A78866 300D0609 2A864886 F70D0101 04050003
  81810078 494CAC63 11A31519 04B5DB5E 47894DC6 38AFF465 F00EC71C D9208490
  208B15E5 87B6AE3A AD3EFC47 80D388A8 EC1B24B6 48FBCA76 7249F79F 8FFDD8FD
  D1171D94 06776625 55E4370D 4A7381A5 D3FF52F0 1A9653FE DE2911BC 109128F8
  EEB09BAE 2EBE2659 FB64C418 4B6D3FB5 FF7D2642 AE31549D 3DB740F3 35540F0E 8E2B4D
  quit
!
!
!
!
!
!
spanning-tree mode pvst
spanning-tree extend system-id
no spanning-tree vlan 26,100,120
!
vlan internal allocation policy ascending
!
!
!
!
interface FastEthernet1/0/1
 description IPv6 Inside
 switchport access vlan 200
 switchport mode access
!
interface FastEthernet1/0/2
!
interface FastEthernet1/0/3
 description IPv6 DMZ
 switchport access vlan 26
 switchport mode access
!
interface FastEthernet1/0/4
!
interface FastEthernet1/0/5
!
interface FastEthernet1/0/6
!
interface FastEthernet1/0/7
!
interface FastEthernet1/0/8
!
interface FastEthernet1/0/9
!
interface FastEthernet1/0/10
!
interface FastEthernet1/0/11
!
interface FastEthernet1/0/12
!
interface FastEthernet1/0/13
!
interface FastEthernet1/0/14
!
```

```
interface FastEthernet1/0/15
!
interface FastEthernet1/0/16
!
interface FastEthernet1/0/17
 description Trunk 2 hacia VM
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 26,100,120
 switchport mode trunk
!
interface FastEthernet1/0/18
!
interface FastEthernet1/0/19
!
interface FastEthernet1/0/20
!
interface FastEthernet1/0/21
!
interface FastEthernet1/0/22
!
interface FastEthernet1/0/23
!
interface FastEthernet1/0/24
!
interface FastEthernet1/0/25
!
interface FastEthernet1/0/26
!
interface FastEthernet1/0/27
!
interface FastEthernet1/0/28
!
interface FastEthernet1/0/29
!
interface FastEthernet1/0/30
!
interface FastEthernet1/0/31
!
interface FastEthernet1/0/32
!
interface FastEthernet1/0/33
 description IPv6 Outside
 switchport access vlan 24
 switchport mode access
!
interface FastEthernet1/0/34
!
interface FastEthernet1/0/35
 description Troncal entre Switches
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 21-25
 switchport mode trunk
!
interface FastEthernet1/0/36
 switchport access vlan 24
 switchport mode access
!
interface FastEthernet1/0/37
 switchport access vlan 24
 switchport mode access
!
interface FastEthernet1/0/38
 switchport access vlan 24
 switchport mode access
!
interface FastEthernet1/0/39
```

```
 switchport access vlan 24
 switchport mode access
!
interface FastEthernet1/0/40
 switchport access vlan 24
 switchport mode access
!
interface FastEthernet1/0/41
 switchport access vlan 24
 switchport mode access
!
interface FastEthernet1/0/42
 switchport access vlan 24
 switchport mode access
!
interface FastEthernet1/0/43
 switchport access vlan 24
 switchport mode access
!
interface FastEthernet1/0/44
 switchport access vlan 24
 switchport mode access
!
interface FastEthernet1/0/45
 description LAP1121G
 switchport access vlan 21
 switchport mode access
!
interface FastEthernet1/0/46
 description LAP1232AG
 switchport access vlan 21
 switchport mode access
!
interface FastEthernet1/0/47
 description Service Port WLC
 switchport access vlan 25
 switchport mode access
!
interface FastEthernet1/0/48
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 21
 switchport trunk allowed vlan 21,22
 switchport mode trunk
!
interface GigabitEthernet1/0/1
 description Troncal Management WLC
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 21,22
 switchport mode trunk
!
interface GigabitEthernet1/0/2
!
interface GigabitEthernet1/0/3
!
interface GigabitEthernet1/0/4
!
interface Vlan1
 no ip address
!
interface Vlan21
 description EQUIPOS WIRELESS
 no ip address
!
interface Vlan22
 description Red Wireless 1
 no ip address
```

```
!
interface Vlan23
 description Red Wireless 2
 no ip address
!
interface Vlan24
 description IPv6 Outside
 no ip address
!
interface Vlan25
 description VLAN de Administracion
 ip address 10.10.25.254 255.255.255.0
!
interface Vlan26
 description IPv6 DMZ
 no ip address
!
interface Vlan100
 description Red Interna 1
 ip address 10.10.100.254 255.255.255.0
 ip helper-address 10.10.26.10
 ipv6 address 2002:404C:957D:100::/64 eui-64
!
interface Vlan120
 description Red Interna 2
 ip address 10.10.120.254 255.255.255.0
 ip helper-address 10.10.26.10
 ipv6 address 2002:404C:957D:120::/64 eui-64
!
interface Vlan200
 description IPv6 Inside
 ip address 10.10.200.254 255.255.255.0
 ipv6 address 2002:404C:957D:200::/64 eui-64
!
router ospf 100
 log-adjacency-changes
 passive-interface Vlan21
 passive-interface Vlan22
 passive-interface Vlan23
 passive-interface Vlan24
 passive-interface Vlan25
 passive-interface Vlan26
 passive-interface Vlan100
 passive-interface Vlan120
 network 10.10.100.0 0.0.0.255 area 0
 network 10.10.120.0 0.0.0.255 area 0
 network 10.10.200.0 0.0.0.255 area 0
!
ip classless
ip route 0.0.0.0 0.0.0.0 10.10.200.100
ip http server
ip http secure-server
!
ipv6 route ::/0 2002:404C:957D:200:21B:2AFF:FE34:D94F
!
control-plane
!
line con 0
line vty 0 4
 password magenta3350
 login
line vty 5 15
 login
!
End
```

B.2 Configuración de Firewall ASA 5520

```
: Saved
: Written by enable_15 at 23:11:20.224 UTC Wed Nov 18 2009
!
ASA Version 7.2[3]
!
hostname NW-MGTA
domain-name lab-ipv6
enable password 2KFQnbNIdI.2KYOU encrypted
names
!
interface GigabitEthernet0/0
 nameif outside
 security-level 0
 ip address 10.10.24.100 255.255.255.0
 ipv6 address 2002:404c:957d:24::/64 eui-64
 ipv6 nd suppress-ra
 ospf cost 10
!
interface GigabitEthernet0/1
 nameif inside
 security-level 100
 ip address 10.10.200.100 255.255.255.0
 ipv6 address 2002:404c:957d:200::/64 eui-64
 ipv6 enable
 ospf cost 10
!
interface GigabitEthernet0/2
 nameif DMZ
 security-level 50
 ip address 10.10.26.100 255.255.255.0
 ipv6 address 2002:404c:957d:26::/64 eui-64
 ospf cost 10
!
interface GigabitEthernet0/3
 shutdown
 no nameif
 no security-level
 no ip address
!
interface Management0/0
 shutdown
 no nameif
 no security-level
 no ip address
!
passwd 2KFQnbNIdI.2KYOU encrypted
ftp mode passive
dns server-group DefaultDNS
 domain-name lab-ipv6
access-list acl_inside_in extended permit ip any any
access-list outside_access_in extended permit tcp any host 10.10.24.100 eq www
access-list outside_access_in extended permit udp any host 10.10.24.100 eq domain
access-list outside_access_in extended permit icmp any any
access-list inside_nat0_outbound extended permit ip any host 10.10.26.10
access-list inside_nat0_outbound extended permit ip any host 10.10.24.100
pager lines 24
logging enable
logging asdm informational
mtu outside 1500
mtu inside 1500
mtu DMZ 1500
ipv6 route inside 2002:404c:957d:100::/64 2002:404c:957d:200:219:56ff:fe80:f9c8
ipv6 route inside 2002:404c:957d:120::/64 2002:404c:957d:200:219:56ff:fe80:f9c8
```

```
ipv6 route outside 2000::/3 2002:404c:957d:24::2
ipv6 access-list acl_inside_in6 permit ip any any
ipv6 access-list outside_access_in6 permit tcp any host 2002:404c:957d:26::1 eq www
ipv6 access-list outside_access_in6 permit udp any host 2002:404c:957d:26::1 eq domain
ipv6 access-list outside_access_in6 permit icmp6 any host 2002:404c:957d:26::1
ipv6 access-list outside_access_in6 permit icmp6 any any time-exceeded
ipv6 access-list outside_access_in6 permit icmp6 any any unreachable
no failover
icmp unreachable rate-limit 1 burst-size 1
asdm image disk0:/asdm-523.bin
no asdm history enable
arp timeout 14400
global (outside) 1 interface
global (DMZ) 2 interface
nat (inside) 0 access-list inside_nat0_outbound
nat (inside) 1 0.0.0.0 0.0.0.0
nat (DMZ) 1 10.10.26.0 255.255.255.0
static (DMZ,outside) tcp interface www 10.10.26.10 www netmask 255.255.255.255
static (DMZ,outside) udp interface domain 10.10.26.10 domain netmask 255.255.255.255
access-group outside_access_in in interface outside
access-group outside_access_in6 in interface outside
access-group acl_inside_in in interface inside
access-group acl_inside_in6 in interface inside
route outside 0.0.0.0 0.0.0.0 10.10.24.2 255
!
router ospf 100
 network 10.10.26.0 255.255.255.0 area 0
 network 10.10.200.0 255.255.255.0 area 0
 area 0
 log-adj-changes
!
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00
timeout uauth 0:05:00 absolute
http server enable
http 10.10.100.10 255.255.255.255 inside
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication linkup linkdown coldstart
telnet 10.10.100.10 255.255.255.255 inside
telnet timeout 5
ssh 10.10.100.0 255.255.255.0 inside
ssh timeout 5
console timeout 0
!
class-map inspection_default
 match default-inspection-traffic
!
!
policy-map type inspect dns preset_dns_map
 parameters
  message-length maximum 754
policy-map global_policy
 class inspection_default
  inspect dns preset_dns_map
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect netbios
  inspect rsh
  inspect rtsp
  inspect skinny
  inspect esmtp
  inspect sqlnet
```

```
  inspect sunrpc
  inspect tftp
  inspect sip
  inspect xdmcp
  inspect icmp error
  inspect icmp
!
service-policy global_policy global
ntp server 200.54.149.19 source outside prefer
username adminmag password zpb5o0kgfztiD7Jw encrypted
username cisco password 3USUcOPFUiMCO4Jk encrypted
prompt hostname context
Cryptochecksum:195198f8738186c390faaac719f08583
: end
```

Anexo C: Planilla para evaluación económica (complemento)

Se presenta a continuación la planilla diseñada para realizar una evaluación preliminar de los recursos requeridos en un servicio de adopción de IPv6 y los beneficios potenciales de este servicio. En esta planilla es posible seleccionar los componentes relevantes que aplican a la realidad de cada empresa mandante en función de las características de su red, permitiendo calcular en base a estos componentes tanto el periodo de recuperación como el flujo de caja que tendrá para la empresa este proyecto.

En la planilla, los costos indicados para los equipos que se tomaron de referencia corresponden a precios lista. Para los servicios (RRHH) se expresa el valor en UF, mientras que para el resto de las categorías el precio se expresa en US$. La conversión utilizada en cada caso es la indicada en las primeras filas de la hoja "Parámetros", la cual puede ser actualizada por quien haga uso de esta planilla.

Los elementos seleccionados en la hoja “Parámetros” así como las cantidades indicadas en la hoja “Costos” se escogieron con la única finalidad de ejemplificar el uso de la planilla.

C.1 Hoja “Instrucciones”

INSTRUCCIONES DE USO DE LA PLANILLA ROI
Alcance del proyecto y de la planilla
Esta planilla aplica al proyecto "Servicio de evaluación para la adopción de IPv6".
El proyecto contempla la instalación de una demo en la red del cliente para validar el soporte de equipos y aplicaciones para operar sobre IPv6.
El proyecto además contempla un levantamiento para estimar las inversiones necesarias para dejar la red del cliente preparada para soportar IPv6.
Esta planilla permite seleccionar los componentes relevantes para una evaluación preliminar de recursos y calcular un ROI en base a parámetros predefinidos.
Los costos indicados en esta planilla corresponden a precios lista. Para los servicios (RRHH) se indica el valor en UF, para el resto de las categorías el precio se indica en US$. La conversión utilizada en cada caso es la indicada en las primeras filas de la hoja "Parámetros".
IMPORTANTE: Para utilizar esta planilla se debe habilitar la ejecución de Macros en Microsoft Excel. Para esto:
1. Seleccione el Botón de Office y luego "Opciones de Excel"
2. En la pestaña "Centro de confianza" seleccione "Configuración del Centro de confianza"
3. En la pestaña "Configuración de macros" seleccione "Habilitar todas las macros"
Habilidades del usuario de la planilla
Usuario con conocimientos de IPv6 y del proyecto asociado a la planilla.
Usuario capaz de agregar nuevos ítems a la hoja "Parámetros", incluyendo insercion de casillas de verificación y su vinculación a una celda.
Usuario capaz de manipular una macro sencilla, para modificar parámetros asociados a la inserción de elementos en la hoja "Costos".
¿Cómo usar la planilla?
A. Llenado de planilla de Costos
1. En la hoja "Parámetros" elija los componentes que son relevantes para la estimación de los costos, haciendo click en la casilla ubicada en la misma fila del componente deseado.
2. Tras seleccionar todos los componentes relevantes, en la hoja "Costos" haga click sobre el borón "Actualizar Planilla" ubicado en la columna G. Esto producirá el borrado y re-llenado de la planilla, salvo los ítems ubicados bajo la fila "Operación y Mantención de la Red" que permanecerán sin modificaciones.
3. Para los elementos cuya categoría aparezca en la columna "Categoría" de la hoja "Costos", indique en la columna "Cantidad" la cantidad asociada a dichos elementos. Esto actualizará el Costo de Inversión asociado a cada elemento, el margen de ganancia del proyecto y el Total de costo de inversión con los elementos considerados.
4. El gráfico final del ROI se actualizará automáticamente en función de los parámetros definidos en la manipulación de la planilla.
B. Llenado de planilla de Beneficios
1. En la hoja "Parámetros", revise y de ser necesario corrija los valores asignados en la sección "Operación de Red IPv4" (en base al cliente que se esté
2. Revise que los cálculos se hayan realizado de forma correcta en la planilla "Beneficios". El cálculo se realiza de forma automática.
C. Llenado de planilla de ROI
1. En la hoja "ROI", la tabla superior se llena automáticamente con los datos calculador anteriormente (Costo Inversión Inicial, Costo Operacional Anual, Ahorro Operacional Fijo, Ahorro Operación Anual).
2. En la columna Comentario, modifique de ser necesario la cantidad de años considerados para que se considere el Ahorro Operacional Fijo.
3. En la tabla inferior de la hoja "ROI" se calculará de forma automática el retorno anual de la inversión. En caso de cambiar la cantidad de años considerados para que se considere el Ahorro Operacional Fijo (5 por defecto), modifique las fórmulas de modo que sean coherentes con las consideraciones realizadas.
D. Inserción de nuevos componentes en el listado de la hoja "Parámetros"
1. En la hoja "Parámetros", sitúese en la sección correspondiente al componente que se desea agregar (Equipo Cisco, Licencia de Softw are, etc).
2. Agregue una fila de manera usual (Botón derecho > Insertar > Filas de la tabla arriba).
3. Agregue los parámetros Item, Categoría, Código, Nombre, Precio Lista, Unidad y Comentarios/Valor Típico relacionados con el componente.
4. En la columna G agregue una casilla de verificación (Menú Programador > Insertar > Casilla de verificación (control de formulario)).
5. Vincule la casilla de verificación con la celda de la columna I en la misma fila.

C.2 Hoja "Parámetros"

Item	Categoría	Código	Nombre	Precio Lista	Unidad	Selecció	Comentarios / Valor Típico
			Tasas de Conversión				
1	PARAMETROS		UF	21000	CLP		
2	PARAMETROS		US$	500	CLP		
3	PARAMETROS		*Margen de ganancia de venta del proyecto*	15	%		Calculado sobre el total del proyecto
			Costo de equipos Cisco				
			Switch Multilayer				
4	HARDWARE	WS-C3560-24TS-E	Switch Multilayer Cisco Catalyst 3560 24 10/100 + 2 SFP	4990	US$	☑	
5	SOPORTE	CON-CSSPD-356024TE	SHARED SUPP SDS, Cat 3560 24 10/100 w/2 SFP Enhanced	124	US$	☑	
6	HARDWARE	WS-C3750-24TS-E	Switch Multilayer Cisco Catalyst 3750 24 10/100 + 2 SFP	5990	US$	☐	
7	SOPORTE	CON-CSSPD-375024TE	SHARED SUPP 8X5XNBD Catalyst 3750 24 10/	692	US$	☐	
8	HARDWARE	WS-C3560-48TS-E	Switch Multilayer Cisco Catalyst 3560 48 10/100 + 4 SFP	6990	US$	☐	
9	SOPORTE	CON-CSSPD-C356048E	SHARED SUPP SDS, Cat 3560 48 10/100 w/4 SFP Enhanced	166	US$	☐	
10	HARDWARE	WS-C3750-48TS-E	Switch Multilayer Cisco Catalyst 3750 48 10/100 + 4 SFP	8990	US$	☐	
11	SOPORTE	CON-CSSPD-375048TE	SHARED SUPP 8X5XNBD Catalyst 3750 48 10/	923	US$	☐	
			Firewall				
12	HARDWARE	ASA5510-BUN-K9	Firewall ASA 5510, 5FE, SW v8.2	3495	US$	☐	Throughput 150 Mbps
13	SOPORTE	CON-CSSPD-AS1BUNK9	SHARED SUPP SDS ASA5510 w/50 VPN Peers, 3 FE, 3DES/AES	576	US$	☐	
14	HARDWARE	ASA5510-SEC-BUN-K9	Firewall ASA 5510 Security Plus, 2GE+3FE, SW v8.2	4495	US$	☑	Throughput 150 Mbps
15	SOPORTE	CON-CSSPD-AS1SBK9	SHARED SUPP SDS ASA5510 Sec+ w/150 VPN Prs,5FE,3DES/AES	741	US$	☑	
16	HARDWARE	ASA5510-AIP20SP-K9	Firewall ASA 5510 c/AIP-SSM-20, 2GE+3FE, SW v8.2, IPS	8999	US$	☐	Throughput 300 Mbps
17	LICENCIA	CON-SUSA-AS1A2PK9	IPS SIGNATURE ONLY ASA5510-AIP20SP-K9	1215	US$	☐	
18	SOPORTE	CON-CSSPD-AS1A2PK9	SHARED SUPP SDS ASA5510-AIP20SP-K9	1649	US$	☐	
19	HARDWARE	ASA5520-BUN-K9	Firewall ASA 5520, 4GE+1FE, SW v8.2	7995	US$	☐	Throughput 225 Mbps
20	SOPORTE	CON-CSSPD-AS2BUNK9	SHARED SUPP SDS ASA5520 w/300 VPN Prs, 4GE+1FE,3DES/AES	1319	US$	☐	
21	HARDWARE	ASA5520-AIP20-K9	Firewall ASA 5520 c/AIP-SSM-20, 4GE+1FE, SW v8.2, IPS	15995	US$	☐	Throughput 375 Mbps
22	LICENCIA	CON-SUSA-AS2A20K9	IPS SIGNATURE ONLY ASA5520 w AIP-SSM-20, 4GE+1FE, 3DES/AES	1215	US$	☐	
23	SOPORTE	CON-CSSPD-AS2A20K9	SHARED SUPP SDS ASA5520 w AIP-SSM-20, 4GE+1FE, 3DES/AES	2639	US$	☐	
24	HARDWARE	ASA5520-AIP40-K9	Firewall ASA 5520 c/AIP-SSM-40, 4GE+1FE, SW v8.2, IPS	21995	US$	☐	Throughput 450 Mbps
25	LICENCIA	CON-SUSA-AS2A40K9	IPS SIGNATURE ONLY ASA5520-AIP40-K9	2771	US$	☐	
26	SOPORTE	CON-CSSPD-ASAINC40	SHARED SUPP SDS ASA5520-AIP40-K9	3629	US$	☐	
			Costo de instalación				
27	INSTALACION		Cableado e instalaciones para equipos de red (1 puerta)	100	US$/puerta	☑	* (OBLIGATORIO) Incluye instalación y certificación
			Costo de Servidor de VM				
28	HARDWARE		HW Servidor Quad Core 4Gb RAM, 1 TB HD	830	US$	☑	* (OBLIGATORIO)
			Costo de Licencias de Sistemas Operativos				
29	SOFTWARE		Windows Server 2008 Trial	0	US$	☐	Versión de evaluación válida por hasta 180 días
30	SOFTWARE		Windows Server 2008 Standard	999	US$	☐	Incluye 5 CALs (User or Device)
31	SOFTWARE		Windows Server 2008 Enterprise	3999	US$	☑	Incluye 25 CALs (User or Device)
32	SOFTWARE		Windows 7 Home Premium	200	US$	☐	
33	SOFTWARE		Windows 7 Professional	300	US$	☑	
34	SOFTWARE		Windows 7 Ultimate RC	0	US$	☐	No disponible a partir de marzo de 2010
35	SOFTWARE		Red Hat Enterprise Linux 5 server (kernel 2.6.18)	349	US$	☐	Basic Subscription Web support, 2 business day response, unlimite
36	SOFTWARE		Fedora Core 11	0	US$	☑	
37	SOFTWARE		Ubuntu 8.04	0	US$	☑	

(continuación hoja "Parámetros")

			Costo de acceso dual stack IPv4/IPv6				
38	ENLACE		Enlace dedicado 1 Mbps Int/10 Mbps Nac, basado en FO	5550	US$/año	☐	11 UF/mes. Contrato mínimo 12 meses. Ref: Las Condes
39	ENLACE		Servicio de Firewall basado en Router/Firewall Cisco 1811	1010	US$/año	☐	2 UF/mes. Contrato mínimo 36 meses. Ref: Las Condes
			Hora Hombre				
40	RRHH		Hora Técnico Instalaciones de Redes	1	UF	☐	Opcional al servicio de instalación
41	RRHH		Hora Field Engineer	2	UF	☑	Conocimientos en OS, servidores web, DNS, DHCP, etc.
42	RRHH		Hora System Engineer	3	UF	☑	Une preventa con postventa, involucrado en el proyecto
43	RRHH		Hora Senior Engineer	3	UF	☐	Casos puntuales, escalamiento mayor
44	RRHH		Hora Support Engineer	2	UF	☐	
45	RRHH		Hora Personal de capacitación al cliente	2	UF	☑	Capacitación técnica, generalmente Field Engineer
46	RRHH		Hora Proyect Manager	2	UF	☐	Contraparte con el cliente
47	RRHH		Hora Helpdesk	0,5	UF	☐	
			Instalación de equipos en laboratorio (Parámetros)				
48	PARAMETROS		Cantidad de equipos de HW a instalar	3	equipos		Incluye Servidor de VM, Switch Multilayer y Firewall
49	PARAMETROS		Horas para ingeniería de planificación	15	horas		Estimado en base a prototipo de Magenta
50	PARAMETROS		Horas para instalación de equipos	1	hora/equipo		
51	PARAMETROS		Horas para instalación de software	25	horas		Estimado en base a prototipo de Magenta
52	PARAMETROS		Horas para configuración y validación	75	horas		Estimado en base a prototipo de Magenta
			Capacitación de personal del Cliente (Parámetros)				
53	PARAMETROS		Horas en cursos de capacitación al cliente en uso de laboratorio	15	horas		
			Mantención de Redes Instaladas (Parámetros)				
54	PARAMETROS		Mantención de cableado y puntos de red	100	US$/falla		
55	PARAMETROS		Cantidad de fallas de cableado por año	12	fallas/año		
56	PARAMETROS		Porcentaje anual del precio de equipos en arreglos o reposicion	10	%		
			Operación de Red IPv4				
57	PARAMETROS		Consultas a Helpdesk debido a pérdida de conectividad al cambiarse de localización (subred)	12	consultas/año		
58	PARAMETROS		Tiempo de respuesta de Helpdesk	1	hora		
59	PARAMETROS		Consultas a Helpdesk debido a pérdida de conexiones establecidas al cambiarse de localización	12	consultas/año		
60	PARAMETROS		Tiempo de respuesta de Helpdesk	1	hora		
61	PARAMETROS		Aplicaciones para las cuales se requiere abrir puertos de NAT	4	apps/año		
62	PARAMETROS		Tiempo de configuración de Helpdesk	4	horas/app		
63	PARAMETROS		Horas hombre de Proyect Manager dedicado a migración tardía de IPv6 en la empresa	576	horas/año		
64	PARAMETROS		Horas hombre de Proyect Manager dedicado a adición de 1 subred en la empresa	48	horas/año		
65	PARAMETROS		Horas hombre de Field Engineer dedicado a adición de 1 subred en la empresa	48	horas/año		

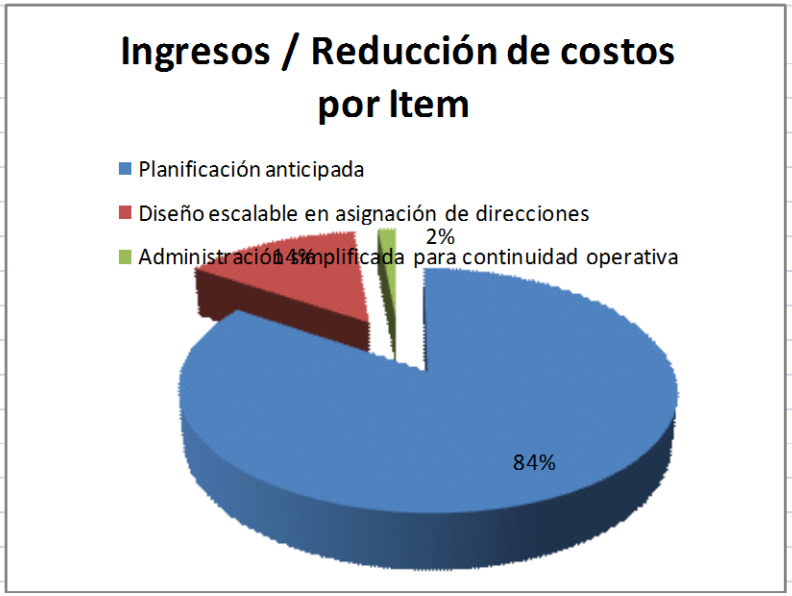
C.3 Hoja "Costos"

Item	Categoría	Descripción	Cantidad	Costo de Inversión (US$)	Costo Operacional Anual (US$)	Actualizar Planilla
	HARDWARE	Switch Multilayer Cisco Catalyst 3560 24 10/100 + 2 SFP	1	$ 4.990,00		
	SOPORTE	SHARED SUPP SDS, Cat 3560 24 10/100 w/2 SFP Enhanced	1	$ 124,00		
	HARDWARE	Firewall ASA 5510 Security Plus, 2GE+3FE, SW v8.2	1	$ 4.495,00		
	SOPORTE	SHARED SUPP SDS ASA5510 Sec+ w/150 VPN Prs,5FE,3DES/AES	1	$ 741,00		
	INSTALACION	Cableado e instalaciones para equipos de red (1 puerta)	55	$ 5.500,00		
	HARDWARE	HW Servidor Quad Core 4Gb RAM, 1 TB HD	1	$ 830,00		
	SOFTWARE	Windows Server 2008 Enterprise	1	$ 3.999,00		
	SOFTWARE	Windows 7 Professional	5	$ 1.500,00		
	SOFTWARE	Fedora Core 11	1	$ -		
	SOFTWARE	Ubuntu 8.04	1	$ -		
	RRHH	Hora Field Engineer	180	$ 15.120,00		
	RRHH	Hora System Engineer	180	$ 22.680,00		
	RRHH	Hora Personal de capacitación al cliente	15	$ 1.260,00		
		Margen de Ganancia sobre el costo de inversión		$ 9.185,85		
		Operación y Mantención del Sistema				
		Mantención red cableada, cables y puntos de red		$ -	$ 1.200,00	
		Mantención red cableada, equipos de red		$ -	$ 1.031,50	
		Total		**$ 70.424,85**	**$ 2.231,50**	

C.4 Hoja "Beneficios"

Item	Descripción	Ingreso / Reducción de Costo Anual (US$)	Comentarios
1	Planificación anticipada	$ 48.384,00	Ahorro en el proyect manager que debe dedicarse al proyecto en caso de una migración tardía. Se asume que en el año 5 la adopción de IPv6 será una necesidad
2	Diseño escalable en asignación de direcciones	$ 8.064,00	Costo de agregar una subred al año, involucra 1 Project Manager y un Field Engineer durante un mes
3	Administración simplificada para la continuidad operativa y fallas		
	Mobile IP	$ 252,00	Consultas a Helpdesk debido a problemas con conexiones establecidas, al cambiarse de localización. Con IP Mobile se mantienen las conexiones independiente de la ubicación dentro de la red (por ejemplo, VPN)
	Eliminación de NAT	$ 336,00	Por cada aplicación nueva ingresada se debe abrir puertos de NAT, en cambio con IPv6 solo modifica listas de acceso.
	Autoconfiguración	$ 252,00	Consultas a Helpdesk debido a problemas con conectividad al cambiarse de localización. Con autoconfiguración es posible asignarse de manera sencilla una dirección IPv6 y un default gateway, en base al prefijo de la subred
	Total	$ 57.288,00	

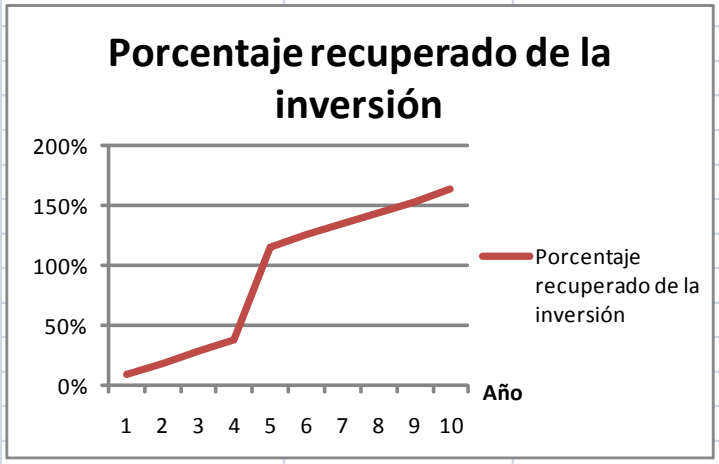
Item	Ingresos / Reducción de costos por Item
Planificación anticipada	$ 48.384,00
Diseño escalable en asignación de direcciones	$ 8.064,00
Administración simplificada para continuidad operati	$ 840,00



C.5 Hoja "ROI"

Item	Valor	Comentario
Costo Inversión Inicial	$ 70.424,85	
Costo Operacional Anual	$ 2.231,50	
Ahorro Operacional Fijo	$ 48.384,00	Ahorro en el Año 5
Ahorro Operacional Anual	$ 8.904,00	

Años desde la inversión	Porcentaje recuperado de la inversión	Ganancias acumuladas (US$)
0	0%	$ (70.424,85)
1	9%	$ (63.752,35)
2	19%	$ (57.079,85)
3	28%	$ (50.407,35)
4	38%	$ (43.734,85)
5	**116%**	**$ 11.321,65**
6	126%	$ 17.994,15
7	135%	$ 24.666,65
8	145%	$ 31.339,15
9	154%	$ 38.011,65
10	163%	$ 44.684,15



C.6 Hoja "Flujos"

Flujo por Año [US$]	0	1	2	3	4	5	6	7	8	9	10	>10
(+) Ingresos		8.904,0	8.904,0	8.904,0	8.904,0	57.288,0	8.904,0	8.904,0	8.904,0	8.904,0	8.904,0	8.904,0
Ahorro Operacional Fijo		0,0	0,0	0,0	0,0	48.384,0	0,0	0,0	0,0	0,0	0,0	0,0
Ahorro Operacional Anual		8.904,0	8.904,0	8.904,0	8.904,0	8.904,0	8.904,0	8.904,0	8.904,0	8.904,0	8.904,0	8.904,0
(-) Costos de Operación		2.231,5	2.231,5	2.231,5	2.231,5	2.231,5	2.231,5	2.231,5	2.231,5	2.231,5	2.231,5	2.231,5
Costo Operacional Anual		2.231,5	2.231,5	2.231,5	2.231,5	2.231,5	2.231,5	2.231,5	2.231,5	2.231,5	2.231,5	2.231,5
(-) Depreciaciones		3.954,1	3.954,1	3.954,1	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0
Hardware (3 años lineales)		3.954,1	3.954,1	3.954,1	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0
(+) Pérdidas de ejercicio anterior		0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0
(=) Utilidad Antes de Impuestos		2.718,4	2.718,4	2.718,4	6.672,5	55.056,5	6.672,5	6.672,5	6.672,5	6.672,5	6.672,5	6.672,5
(-) Impuesto (17%)		462,1	462,1	462,1	1.134,3	9.359,6	1.134,3	1.134,3	1.134,3	1.134,3	1.134,3	1.134,3
(=) Utilidades Despues de Impuestos		2.256,3	2.256,3	2.256,3	5.538,2	45.696,9	5.538,2	5.538,2	5.538,2	5.538,2	5.538,2	5.538,2
(+) Depreciaciones		3.954,1	3.954,1	3.954,1	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0
(-) Pérdidas de ejercicio anterior		0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0
(=) Flujo de Caja Operacional [US$]	0	6.210	6.210	6.210	5.538	45.697	5.538	5.538	5.538	5.538	5.538	5.538
(-) Inversion Inicial (considera margen de 15%)	70.424,9											
Hardware	11.862,3											
Software	6.323,9											
Soporte	994,8											
Instalación	6.325,0											
RRHH	44.919,0											
(+) Valor Residual de los Activos												
(-) Capital de Trabajo												
(+) Recuperacion Capital de Trabajo												
(=) Flujo de Capitales [US$]	-70.425	0	0	0	0	0	0	0	0	0	0	
(=) Flujo de Caja Privado [US$]	-70.425	6.210	6.210	6.210	5.538	45.697	5.538	5.538	5.538	5.538	5.538	
VAN i (Tasa de Desc. de 30% Real Anual)	-70.425	4.777	3.675	2.827	1.939	12.308	1.147	883	679	522	402	
VAN acumulado	-70.425	-65.648	-61.973	-59.146	-57.207	-44.900	-43.752	-42.870	-42.191	-41.668	-41.267	
Tasa de Descuento [%]	30%											
VAN [US$]	-41.267											
TIR [%]	6,65%											
Payback [Años]	11											

C.7 Macro para llenado dinámico de hoja “Costos”

```
Sub Macro1()
' Macro1 Macro
' Paso 1: Limpieza de listas en hoja costos
' Paso 2: Llenado de lista de costos

    Dim Str As String
    Sheets("Costos").Select
' Este for borra el listado existente para llenarlo de nuevo
   For i = 2 To 65000  'Se considera a partir de la fila 2 de la hoja costos
        If (ThisWorkbook.Sheets("Costos").Cells(i, 3) = "Operación y Mantención del
Sistema") Then
            Exit For
        End If
        Str = ThisWorkbook.Sheets("Costos").Cells(i, 3)
        If (Mid(Str, 1, 1) = " ") Then
            ThisWorkbook.Sheets("Costos").Rows(i).Select
            Selection.Delete Shift:=xlDown
            Str = ThisWorkbook.Sheets("Costos").Cells(i, 3)
            If (Mid(Str, 1, 1) = " ") Then
                i = i - 1
            End If
        End If
    Next i

' Este for llena la lista de costos en base a los ítems seleccionados en la hoja
Parámetros
    i = 2
    For j = 1 To 65000
        If (ThisWorkbook.Sheets("Parámetros").Cells(j, 9) = "FIN") Then
            Exit For
        End If
        If (ThisWorkbook.Sheets("Parámetros").Cells(j, 9)) Then
            cat = ThisWorkbook.Sheets("Parámetros").Cells(j, 2)
            nom = ThisWorkbook.Sheets("Parámetros").Cells(j, 4)
            ThisWorkbook.Sheets("Costos").Rows(i).Select
            Selection.Insert Shift:=xlDown, CopyOrigin:=xlFormatFromRightOrBelow
            ThisWorkbook.Sheets("Costos").Cells(i, 2) = cat
            ThisWorkbook.Sheets("Costos").Cells(i, 3) = " " & nom
            If (ThisWorkbook.Sheets("Parámetros").Cells(j, 6) = "UF") Then
                ThisWorkbook.Sheets("Costos").Cells(i, 5) = "='Parámetros'!E" & j &
"*D" & i & "*Parámetros!E3/Parámetros!E4"
            Else
                ThisWorkbook.Sheets("Costos").Cells(i, 5) = "='Parámetros'!E" & j &
"*D" & i
            End If
            i = i + 1
        End If
    Next j
    ThisWorkbook.Sheets("Costos").Rows(i).Select
    Selection.Insert Shift:=xlDown, CopyOrigin:=xlFormatFromRightOrBelow
    ThisWorkbook.Sheets("Costos").Cells(i, 3) = " Margen de Ganancia sobre el costo de
inversión"
    ThisWorkbook.Sheets("Costos").Cells(i, 5) = "=SUM(E2:E" & (i - 1) &
")*Parámetros!E6/100"

End Sub
```