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

ESTRATEGIA DE ADOPCIÓN DE IPV6 EN LA RED CORPORATIVA DE CODELCO.

MEMORIA PARA OPTAR AL TÍTULO DE INGENIERO CIVIL ELECTRICISTA

ORLANDO RAMÓN VALDENEGRO MÉNDEZ

PROFESOR GUÍA:
EDUARDO VERA SOBRINO.

MIEMBROS DE LA COMISIÓN:
NESTOR BECERRA YOMA.
JOSÉ MIGUEL PIQUER GARDNER.

SANTIAGO DE CHILE
OCTUBRE 2008

RESUMEN DE LA MEMORIA PARA OPTAR
AL TÍTULO DE INGENIERO CIVIL
ELECTRICISTA.
POR: ORLANDO VALDENEGRO MÉNDEZ.
FECHA: 27-XI-2008
PROF. GUÍA: Sr. EDUARDO VERA S.

“ESTRATEGIA DE ADOPCIÓN DE IPV6 EN LA RED CORPORATIVA DE CODELCO”

Esta memoria de título corresponde al diseño de una estrategia de adopción del nuevo protocolo de Internet IPv6 para la Red Corporativa de Codelco-Chile. El trabajo busca una solución factible para dicho problema y plantea la solución con su correspondiente programación.

Dada la vertiginosa evolución de las tecnologías de información, en particular de Internet, nace la necesidad de contar con un protocolo capaz de manejar un mayor número de dispositivos conectados a la red, permitiendo mejorar el rendimiento de las comunicaciones, en particular las multimediales. De esta forma se desarrolla IPv6, destinado a reemplazar IPv4, el protocolo que actualmente rige las comunicaciones en Internet. Así la migración desde un sistema a otro está cada día más cercana, por lo que es de suma importancia estar preparados para dicho cambio.

Por ello la importancia de contar con un plan que permita realizar este cambio en forma estructurada, a costo razonable y habilitando a Codelco-Chile para consolidar su liderazgo tecnológico. En este marco, se desarrolla una estrategia que consta de cuatro etapas: la implementación de un laboratorio; la difusión y promoción del proyecto; la expansión de la conectividad a toda la empresa; y las proyecciones futuras una vez concluida la etapa de adopción. La estrategia está diseñada de modo que el plazo de implementación de este cambio tecnológico sea lo más corto posible (aproximadamente dos años). Además permite realizarlo en forma ordenada, y prepara a la empresa para enfrentar los desafíos tecnológicos que trae la minería del futuro.

A MIS PADRES, YESSY Y ORLANDO…….

AGRADECIMIENTOS.

Primero que todo, agradecer a Dios por brindarme la oportunidad de seguir este camino. A mis padres y mi hermana Catalina, por su apoyo incondicional. A Catherine Acevedo por incentivarme en esta importante etapa de mi vida.

Agradezco también a mi profesor guía, Eduardo Vera, por creer en mí y otorgarme la oportunidad de realizar esta memoria, investigando un tema interesante y de carácter innovador.

A NIC Chile, en especial a Tomás Barros y al equipo de NIC LABS por toda la ayuda brindada en este proyecto. A Codelco por la oportunidad de realizar este proyecto, en especial a Héctor Romero, a Mario Morales, a Ricardo Díaz y su equipo por el apoyo ofrecido en estos meses de arduo trabajo.

También me gustaría agradecer a todos mis amigos que me acompañaron en mi vida universitaria y la hicieron una etapa inolvidable. A Yofer & The Pussycats, mi banda de música universitaria por todos los momentos de alegría vividos junto a ellos: Philip, Pablo, Rubén, Hernán y Cristián. Al Grupo de Cine de Ingeniería, por la amistad entregada y por todos los proyectos que pude realizar con su ayuda (y los que quedaron inconclusos). A la rama de Judo de Ingeniería, en especial al Sensei Héctor Urrutia por enseñarme disciplina y a continuar esforzándome a pesar de las caídas.

A todos ellos muchas gracias.

Índice

Capítulo I: Introducción.

La creciente evolución de las tecnologías de la información, y el aumento progresivo de la demanda de direcciones de Internet, han creado la necesidad de contar con un protocolo que permita solucionar los nuevos requerimientos de red, en particular una mayor cantidad de direcciones para conectar los diversos equipos que desean contar con Internet. Este nuevo protocolo es IPv6 [1], el cual remplazará al actual IPv4 [2] en un tiempo relativamente corto.

La Figura 1.1 [3], muestra el agotamiento y las predicciones del estado de la asignación de direcciones IPv4 en el corto plazo. La línea roja indica la cantidad de direcciones disponibles a asignar, la línea verde indica el número de direcciones disponibles en los registros regionales de Asia Pacífico y la línea vertical indica la situación en el 2007. De esta figura se desprende la predicción de escasez de direcciones IPv4 que tendrá lugar alrededor del 2010.

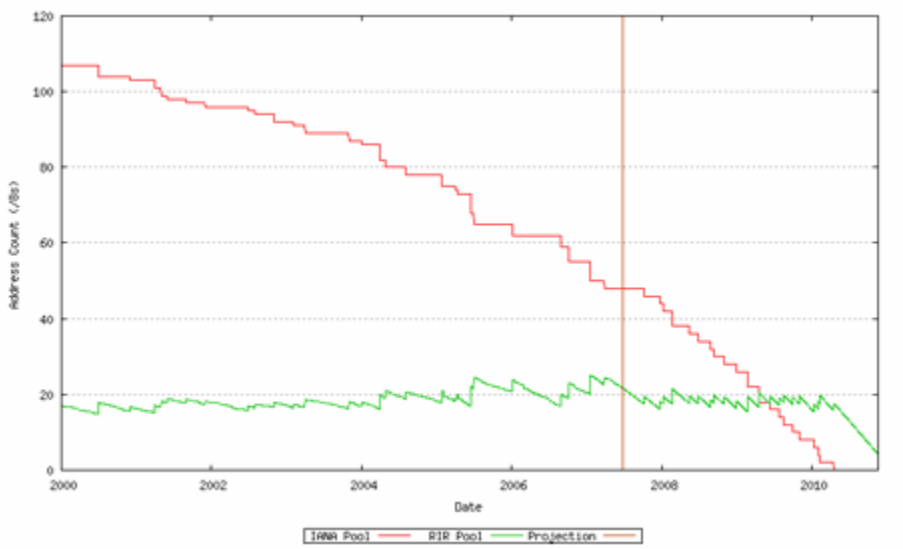

Figura 1.1: Predicción del agotamiento de direcciones IPv4.

Por otra parte, la empresa Codelco-Chile [4] nace a partir de la nacionalización del cobre en 1971, proceso que culminó con la creación de la corporación. La como lo explica [5], “el Decreto de Ley 1350 creó en 1976 la Corporación Nacional del Cobre de Chile, Codelco, concebida como una empresa propiedad del Estado chileno, minera, industrial y comercial, con personalidad jurídica y patrimonio propio” . Esta corporación cuenta con un directorio propio con siete integrantes, nombrados por el Presidente de la República. Tal como su nombre lo indica, Codelco-Chile tiene como principal rubro la extracción de cobre, contando con las divisiones Codelco Norte (Chuquicamata y Radomiro Tomic) Salvador, Andina, El Teniente, Ventanas y Casa Matriz, ubicadas a en la zona norte y centro del país. Además cuenta con oficinas en las ciudades de Calama, Antofagasta, La Serena, Los Andes y Rancagua. Dada la diversidad de lugares donde

la empresa funciona, nace la necesidad de contar con tecnología de punta que permita realizar las labores asociadas a la producción de cobre de la manera más eficiente posible. Considerando estas necesidades, y dada la importancia de la información en el día a día, surge la exigencia de contar con una red de datos de alta velocidad, alta disponibilidad y alta seguridad que permita interconectar las divisiones y, por ende, a los trabajadores geográficamente separados pero a un “click de distancia”.

La evolución tecnológica más las necesidades de Codelco-Chile, crean la importancia de contar con un estudio que permita desarrollar una estrategia de adopción de IPv6 no sólo en Codelco-Chile, que cuenta con más de 12 mil usuarios y cuya posición en el país le obliga el liderazgo tecnológico, sino en cualquier empresa. En este marco, esta memoria desarrolla una estrategia que permite adoptar IPv6 en la red corporativa de Codelco-Chile en el corto plazo (2 a 3 años). Para lograr este objetivo, se busca una solución que permita utilizar los recursos disponibles en la empresa y optimice los tiempos de implementación. Así, esta memoria estudia la factibilidad técnica de integrar este nuevo protocolo de Internet en la red corporativa de Codelco-Chile, analizando las diferentes opciones, para luego concluir en una recomendación que permita integrar este nuevo protocolo de red en dicha empresa.

Para comenzar la investigación, se tiene como base la red corporativa de Codelco-Chile, la cual es descrita y analizada, y que cuenta como protocolo vigente, al igual que la gran mayoría de las redes de datos en el mundo, el protocolo de red IPv4. Partiendo de esta base, y teniendo en mente que el objetivo final es la coexistencia de ambos protocolos de red, IPv4 e IPv6, el estudio comienza recopilando información, analizando los casos posibles, describiendo el mejor caso y desarrollándolo de manera de ajustar sus parámetros a la realidad de la empresa.

En el capítulo 2 se realiza una descripción del nuevo protocolo desde sus fundamentos hasta las estrategias de transición disponibles actualmente. Además se analiza el estado del arte tanto de IPv6 como de la red corporativa de Codelco-Chile, que permita en primer lugar conocer el avance en la transición mundial hacia IPv6, y en segundo lugar conocer la arquitectura de la red y los componentes de la misma.

En el capítulo 3, se busca la estrategia óptima de adopción de IPv6 para una empresa de las características de Codelco-Chile. También se describen los pasos a seguir para establecer un laboratorio IPv6 de pruebas con los equipos disponibles.

En el capítulo 4, se realiza una comparación entre la experiencia de NIC Chile en el transcurso de su adopción del nuevo protocolo de Internet y la estrategia propuesta. De esta experiencia, se recogen los antecedentes necesarios para definir los plazos y los recursos necesarios para efectuar dicha adopción. Finalmente, se plantea la programación del proyecto, definiéndose cada paso a tomar y proyectando una Carta Gantt.

En el capítulo 5 de esta memoria, se plantean las conclusiones y se definen los temas que pueden seguir siendo investigados en este ámbito.

Capitulo II: Contexto Tecnológico: IPv6 y Codelco-Chile.

A pesar de que Codelco Chile es una de las empresas más grandes del país, de que cuenta con tecnologías de punta no sólo a nivel nacional, sino que también internacional, aún no ha considerado el nuevo protocolo de Internet. La Corporación Nacional del Cobre sólo ha realizado estimaciones anteriores en lo que este tema se refiere, concluyendo al momento de esos estudios, posponer la adopción del nuevo protocolo[1]. Es por esto que para comenzar un proyecto en este tema, es necesario analizar el marco teórico de lo que es IPv6 y de la red de Codelco. A continuación se presentan los conocimientos previos necesarios para enfrentar dicho proyecto.

2.1 ¿Qué es IPv6?

Creado por *Steve Deering* de *Xerox PARC* y *Craig Mudge* [6], la nueva versión de IP, IPv6 está destinada a reemplazar al protocolo de red IPv4, cuya capacidad de direcciones de red admisibles comienza a restringir el crecimiento y uso de Internet, especialmente en China, India, y otros países asiáticos densamente poblados y cuyo desarrollo tecnológico posee una fuerte demanda de direcciones IPv4. Este nuevo estándar no solo corrige la limitación de disponibilidad de direcciones que la versión 4 posee, sino que además mejorará el servicio globalmente; por ejemplo, proporcionando a celdas telefónicas y dispositivos móviles con sus direcciones propias y permanentes. Al día de hoy se calcula que dos tercios de las direcciones que ofrece IPv4 ya están asignadas.

2.1.1 Direccionamiento en IPv6.

Como se dijo anteriormente, la principal diferencia entre las dos versiones de los protocolos, es la cantidad de bits que forman la dirección IP. En el caso de IPv4, la dirección IP está compuesta por 32 bits y su forma (formato xxx.xxx.xxx.xxx) ya es familiar para todos nosotros. En cambio, para el caso de IPv6, la dirección tiene un largo de 128 bits, por lo que a primera vista es extraña. El cambio en el largo de las direcciones fue el motivo central del desarrollo de IPv6, junto a la optimización de tablas de enrutamiento, especialmente en Internet. En esta sección, se explicará la forma de las direcciones, de manera tal que para el lector sean familiares, como lo son las de IPv4. La arquitectura de las direcciones en IPv6 ha sido definida en [7].

[1] Este estudio fue de carácter informal, por lo que no se tuvo acceso a él, solo fue comentado por los funcionarios de la Gerencia Corporativa TICA.

Las direcciones del nuevo protocolo se clasifican en 3 categorías: *Unicast; Multicast y Anycast* Una dirección *Unicast* identifica únicamente a una interfaz de un nodo IPv6, un paquete enviado a una dirección *Unicast* es entregado a la interfaz identificada con esa dirección. Una dirección *Multicast* identifica un grupo de interfaces IPv6, un paquete enviado a una dirección *Multicast* es recibido por todos los miembros del grupo. Una dirección *Anycast* es asignada a múltiples interfaces (usualmente en múltiples nodos). Un paquete enviado a una dirección *Anycast*, es entregada sólo a una de las interfaces, usualmente la más cercana.

Tal como se puede apreciar, las direcciones IP son asignadas a interfaces, no a nodos, luego cada interfaz de un nodo debe tener al menos una dirección *unicast*. Una interfaz puede además tener asignadas múltiples direcciones IPv6 de cualquier tipo (*unicast, multicast, anycast*). Una dirección IPv6 típica, consiste en tres partes, el prefijo global de ruteo, el ID de sub red, y el ID de interfase, tal como se muestra en la figura siguiente.

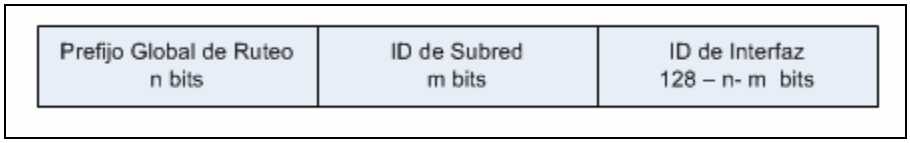

Figura 2.1 Forma General de una Dirección IPv6.

El prefijo global de ruteo, es usado para identificar una dirección especial, como *multicast* o un rango de direcciones asignadas a un sitio. El ID de subred está relacionado con un enlace. Múltiples ID de subred pueden ser asignados a un enlace. El ID de interfaz es utilizado para identificar una interfaz en un enlace y debe ser única en ese enlace.

2.1.1.1 Notación.

Los 128 bits o 16 bytes que componen la dirección IPv6, son divididos en 8 bloques de 16 bits en notación hexadecimal, separados por doble puntos. Por ejemplo:

FE80:0000:0000:0000:0202:B3FF:FE1E:8329

Para simplificar esta notación, algunas abreviaciones son posibles. Por ejemplo, los ceros que lideran los bloques pueden ser resumidos a un sólo cero. La dirección de ejemplo se escribe entonces:

FE80:0:0:0:202: B3FF:FE1E:8329

Un doble punto puede reemplazar ceros consecutivos, o ceros que estén al comienzo o al final de la dirección. Si se aplica esta regla, la dirección de ejemplo queda entonces como:

FE80::202: B3FF:FE1E:8329

Hay que notar que el doble punto puede aparecer sólo una vez, pues el computador siempre utiliza direcciones de 128 bits, incluso cuando han sido abreviadas. Luego, el computador rellena los espacios faltantes con ceros hasta obtener los 128 bits, por lo que si existe más de una abreviación, el computador no sabría cuantos ceros poner en cada parte.

En ambientes donde las dos versiones de IP coexistan, existe otra notación de las direcciones IPv6 mucho más conveniente. Ésta consiste en escribir la dirección IPv4 en los cuatro bytes de menor orden de la dirección IPv6. Luego la dirección 192.168.0.2 puede ser representada como 0:0:0:0:192.168.0.2.

2.1.1.2 Prefijos.

Los prefijos son otra parte importante de las direcciones, los cuales también están especificados en [6]. Un prefijo son los bits de mayor orden de una dirección IP que son usados para identificar la subred o un tipo específico de dirección. La notación agrega el largo del prefijo, escrito como un número de bits con un *slash*, es decir, el formato es el siguiente:

Dirección IPv6 / Largo del prefijo

El largo del prefijo indica cuantos bits más significativos corresponden al prefijo de la dirección. El siguiente ejemplo muestra como el prefijo es interpretado. Considere la notación 2E78:DA53:12::/40. Para entender esta dirección, se convierten los hexadecimales a binarios, tal como se muestra en la tabla siguiente:

Notación Hexadecimal	Notación Binaria	Número de Bits
2E78	0010111001111000	16 bits
DA53	1101101001010011	16 bits
12	00010010	8 bits, total 40 bits

Tabla 2.1: Entendiendo la notación de prefijo.

La notación comprimida (reemplazar una secuencia de ceros con un doble punto) también es aplicable para la representación de prefijo. Debe ser usada con cuidado, pues usualmente hay dos o más rangos de ceros en una dirección, y solo una puede ser comprimida.

2.1.2 Encabezados en IPv6

Al conocer como se distribuyen los campos del encabezado de un paquete IPv6, será mucho más fácil entender cómo funciona este nuevo protocolo. En comparación con el estándar actual, en la nueva versión hay 5 campos que han sido removidos (En caso de no estar familiarizado con la versión cuatro del protocolo, referirse a [8]):

- Header Length
- Identification
- Flags

- Fragment Offset
- Header Checksum

El primer campo, (*Header Length* o “Largo del Encabezado”), fue removido removido puesto que en el nuevo protocolo de red el header es de largo fijo (40 bytes. En IPv4, el encabezado tiene un largo mínimo de 20 bytes, y un máximo de 60 bytes, este largo variable se debe a que en IPv4 hay campos opcionales en el header que pueden ir o no; en cambio en IPv6 las opciones, son definidas como *Extension Headers*, o “Encabezados de Extensión” que no son parte del mismo header del paquete sino que se adjuntan a continuación.

Los campos de identificación (*Identification field*), el de banderas (*Flags field*), y el de fragmentación (*Fragment Offset field*), manejan la fragmentación en IPv4, la cual ocurre cuando un paquete enviado es demasiado grande para la red receptora. En IPv6, esto no ocurre, ya que cada host aprende el tamaño máximo de paquete aceptado por la red, gracias a un procedimiento llamado “Path MTU *Discovery*” (Descubrimiento de la MTU del camino), por lo que los campos mencionados, ya no son necesarios.

El campo *Header Checksum* (“Suma de chequeo de encabeazado”), fue removida, con el objetivo de mejorar la velocidad de procesamiento, Si los *routers* no deben comprobar y actualizar la suma, el procesamiento ocurre mucho más rápido. Además hay que recordar que el protocolo IP actúa según el “mejor esfuerzo”, es decir, es responsabilidad de los protocolos de las capas superiores asegurar la integridad de los datos**.**

Finalmente, el campo *Type of Service* (Tipo de Servicio), fue reemplazado por el campo Traffic Class (Clase de Tráfico). IPv6 posee un mecanismo diferente para manejar las preferencias. Los campos *Protocol Type* (Tipo de Protocolo) y *Time to Live* (Tiempo de Vida*)*, fueron renombrados y ligeramente modificados, además un campo llamado *Flow Label* (Etiqueta de Flujo), fue agregado.

Una vez conocidos los cambios existentes entre los dos protocolos, es posible hablar más en detalle del encabezado de los paquetes en IPv6. La figura siguiente muestra como está compuesto el encabezado de los paquetes en IPv6.

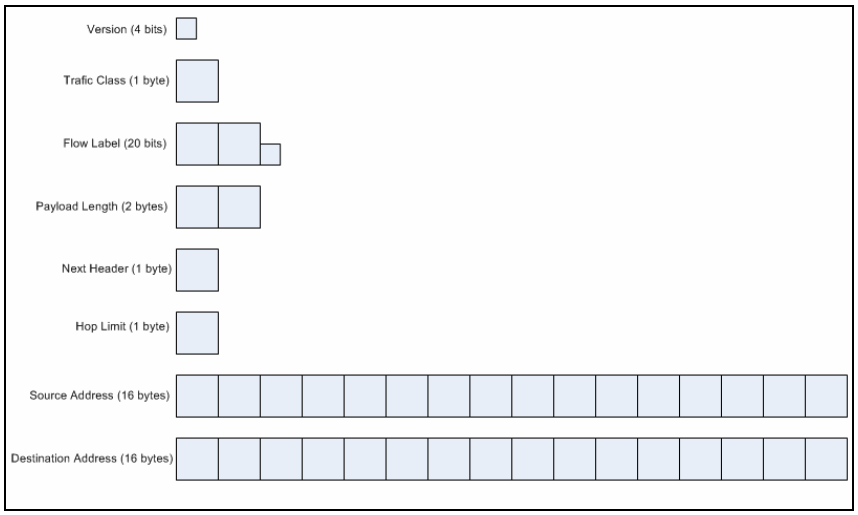

Figura 2.2 Campos en un Encabezado IPv6.

Los campos mostrados en Figura 2.2, se detallan a continuación:

- *Version* (4 Bits): Contiene la versión del protocolo, que en este caso es 6.
- *Traffic Class* (1Byte): Como ya se dijo, este campo reemplaza al *Type of Service* de IPv4. Este campo facilita el manejo de datos de tiempo real y de cualquier otro dato que requiera un manejo especial.
- *Flow Label* (20 Bits): Este campo distingue paquetes que requieren el mismo tratamiento, para facilitar el manejo de tráfico de tiempo real.
- *Payload Length* (2 Bytes): Este campo especifica la carga, es decir el tamaño de los datos llevados después del encabezado IP. Este campo, a diferencia de IPv4, contiene sólo el tamaño de la carga después del encabezado. Los encabezados extendidos, son considerados parte de la carga, por lo que son incluidos en el cálculo. El hecho de que el campo sólo sea de dos bytes de largo, limita el tamaño máximo del paquete a 64KB. IPv6 tiene un paquete Jumbo (*Jumbogram Extension Header*) que soporta tamaños más grandes de paquetes.
- *Next Header* (1 Byte): En IPv4, este campo corresponde al *Protocol Type* (Tipo de Protocolo). Fue renombrado para reflejar la nueva organización de los paquetes IP. Si el encabezado siguiente es UDP o TCP, el campo contiene el mismo número de protocolo que en IPv4. Pero si los encabezados de extensión son utilizados, el campo tendrá entonces el número correspondiente al siguiente encabezado. Ese encabezado se localiza entre el encabezado IP y el TCP o UDP. La Tabla 2.2, muestra una lista de los posibles valores en el campo *Next Header*.

- *Hop Limit* (1 Byte): Este campo es análogo al campo TTL (*Time to Live*) en IPv4. El campo TTL contiene un número de segundos, indicando cuanto tiempo el paquete puede permanecer en la red antes de ser destruido. La mayoría de los *routers* simplemente disminuyen este valor en uno en cada salto (*Hop*). Por este motivo, el campo fue renombrado en IPv6, de manera tal que representara el número de saltos y no el número de segundos.
- *Source Address* (16 Bytes): Este campo contiene la dirección IP del que origina el paquete.

- *Destination Address* (16 Bytes): Este campo contiene la dirección IP del destino del paquete. En IPv4, este campo siempre contiene la dirección del último destino del paquete. En IPv6, este campo puede no contener la IP del último destino, si hay un encabezado de ruteo presente.

Valor	Descripción
0	En IPv4 no se utiliza. En IPv6, indica el encabezado *Hop-by—Hop*
1	ICMPv4
2	*IGMP*v4
4	IP en IP (encapsulación)
6	TCP
8	*Exterior Gateway Protocol* (EGP)
9	Utilizado por Cisco para sus IGRP
17	UDP
41	IPv6
43	Encabezado de Ruteo
44	Encabezado de fragmentación
45	*Interdomain Routing Protocol* (IDRP)
46	Resource Reservation Protocol
50	*Encrypted Security Payload header*
51	Encabezado de autentificación
58	ICMPv6
59	No hay encabezado siguiente
60	Encabezado de opciones de Destino
88	EIGRP
89	OSPF
108	*IP Payload Compresion Protocol*
115	Layer 2 Tunneling Protocol (L2TP)
132	*Stream Control Transmission Protocol*
134-254	Sin asignar
255	Reservado

Tabla 2.2: Valores posibles del campo *Next Header*

2.1.2 Mecanismos de Auto configuración.

IPv6 ofrece una gran ayuda a todos los administradores de sistemas de red. A diferencia de IPv4 donde es necesario utilizar un servidor especial para realizar una auto configuración de los clientes dentro de la red [9]; el nuevo protocolo realiza este proceso de forma nativa. Existen dos formas de realizar la auto configuración en IPv6.

2.1.1.1 Auto Configuración *Stateless.*

Utilizando la dirección física de la interfaz de red (MAC *Address*) es posible configurar las direcciones IP de los clientes de una red. Un mecanismo llamado EUI-64 [6] permite convertir la MAC *Address* en el interfaz ID que completa la dirección IPv6. De esta forma, cuando el cliente recibe el prefijo desde el router al cual está conectado, éste completa su dirección utilizando esta herramienta.

2.1.1.2 Auto Configuración *Stateful.*

Si lo que interesa es saber que dirección IPv6 posee cada interfaz, la auto configuración *stateful* es la opción a utilizar. Este método consiste en usar un servidor que asigne automáticamente las direcciones IPv6 y guarde quién tuvo que dirección y durante cuanto tiempo la tuvo (DHCPv6). Método de similares características que DHCP [9] para IPv4.

2.2 Implementación en distintos sistemas operativos.

2.2.1 Linux

A pesar que de que existen un gran número de diferentes distribuciones de Linux, todas están basadas en el mismo núcleo (*kernel*), identificado por número de versión. A partir de la versión 2.2.x y 2.4.x, IPv6 es soportado (IPv6-*ready*). Sin embargo, [10] recomienda utilizar las versiones 2.6.x en adelante, pues las versiones anteriores no se continúan manteniéndose al día con lo que se refiere a IPv6.

A pesar de que las versiones actuales de Linux ya poseen el protocolo instalado, es necesario saber cómo comprobar la existencia del protocolo, en caso de que por algún motivo, éste no se encuentre instalado. Para esto, se utiliza el siguiente comando en Linux:

```
test -f /proc/net/if_inet6 && echo "Running kernel is IPv6 ready"
```

La Figura 2.10, muestra la realización de la prueba y su correspondiente resultado correcto.

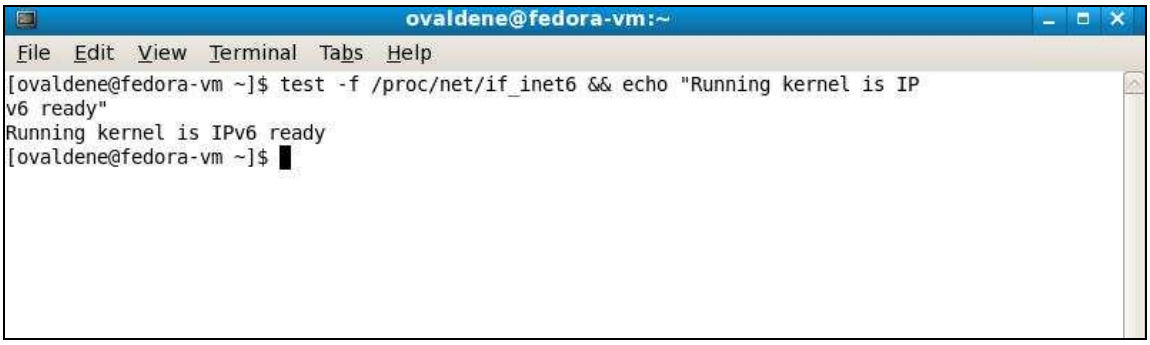

Figura 2.10: Prueba de instalación de IPv6 en Linux.

Si esta prueba falla, entonces es muy probable que el módulo IPv6 no se encuentre cargado. En tal caso, es posible cargar de manera automática el módulo IPv6. Sólo es necesario agregar las siguientes líneas en el archivo de configuración del módulo encargado de cargar el núcleo (*kernel*) (normalmente ubicado en /etc/modules.conf o en /etc/conf.modules):

```
alias net-pf-10 ipv6 # automatically load IPv6 module on demand
```

También en posible desactivar automáticamente el módulo IPv6, utilizando la siguiente línea de comando:

```
alias net-pf-10 off # disable automatically load of IPv6 module on demand
```

2.2.2 Microsoft

La empresa Microsoft, ya publicó su primera investigación del protocolo IPv6 en 1998 [11]. Este protocolo funciona en Windows NT y Windows 2000, pero no lo hace en Windows 95/98, Windows ME o SE. Si posee estos sistemas operativos puede utilizar la herramienta *Trumpet´s Winsock* o considerar en actualizar sus sistemas operativos a Windows XP o Windows Vista, los cuales incluyen el *stack* IPv6. Obviamente lo más recomendado es actualizar los sistemas a las versiones más recientes (XP o Vista), pues poseen muchas características (en lo que refiere a IPv6) que los sistemas más antiguos no poseen.

2.2.2.1 Windows XP.

El sistema operativo Windows XP con *Service Pack* 1, posee el protocolo en sus librerías, aunque no se encuentra instalado (es decir, viene preinstalado). Para instalar el protocolo, se siguen los siguientes pasos [12]. El primer paso a seguir, es abrir una ventana de comandos (Símbolos de Sistema), ubicada en Menú de inicio – ejecutar – cmd – Enter. Luego, se ejecuta el siguiente comando (mostrado en la figura 2.11), con privilegios de administrador:

Figura 2.11 Instalación de IPv6 en Windows XP.

Al ejecutar este comando, aparecerá un mensaje que indica que se ha configurado correctamente.

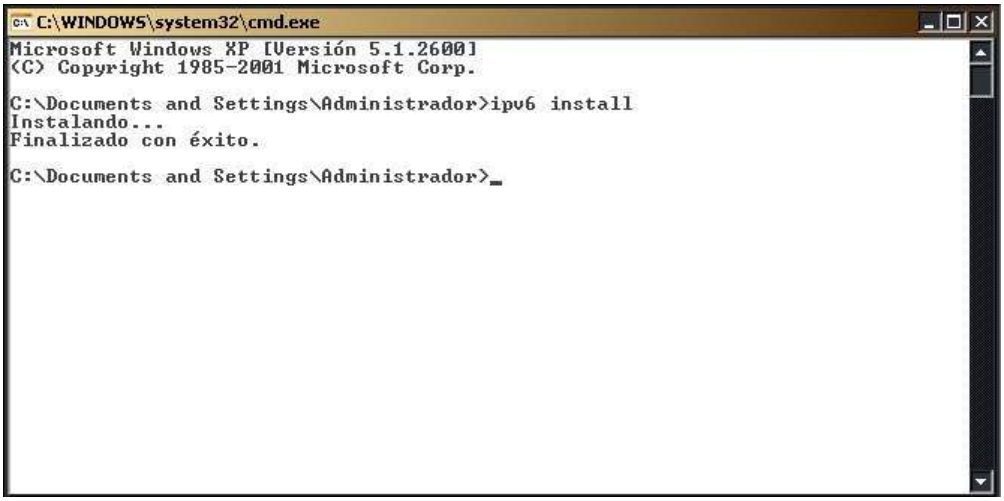

Figura 2.12 Finalización de la instalación de IPv6 en Windows XP.

Para comprobar la correcta instalación del protocolo, se puede utilizar el siguiente comando, el cual es mostrado junto con su resultado, en la Figura 2.13:

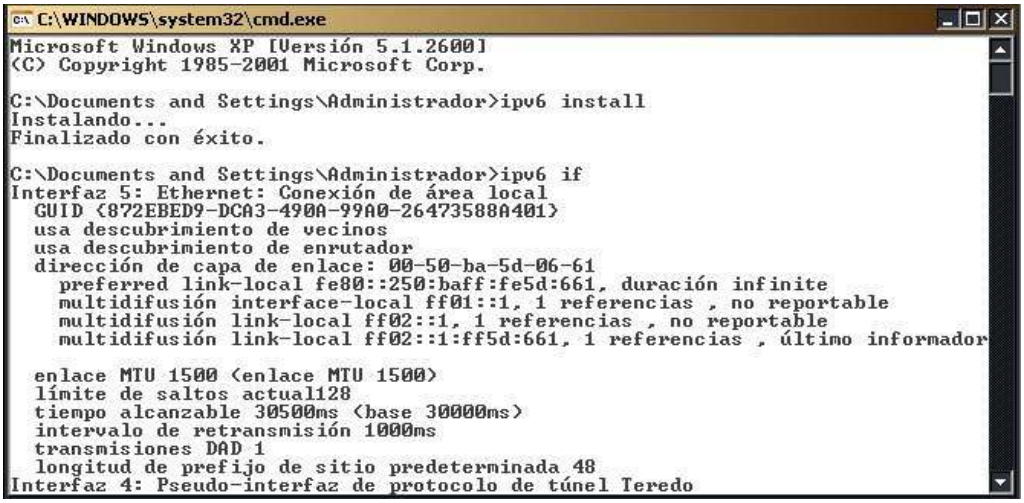

Figura 2.13. Comprobación de la instalación en Windows XP.

La figura anterior, muestra la configuración y las direcciones IPv6 adquiridas (auto-configuradas) para cada interfaz de red existente. Otra forma de comprobar el correcto funcionamiento del protocolo, es realizar un "*ping*" a la dirección de "*loopback*" (auto referida), tal como se muestra a continuación:

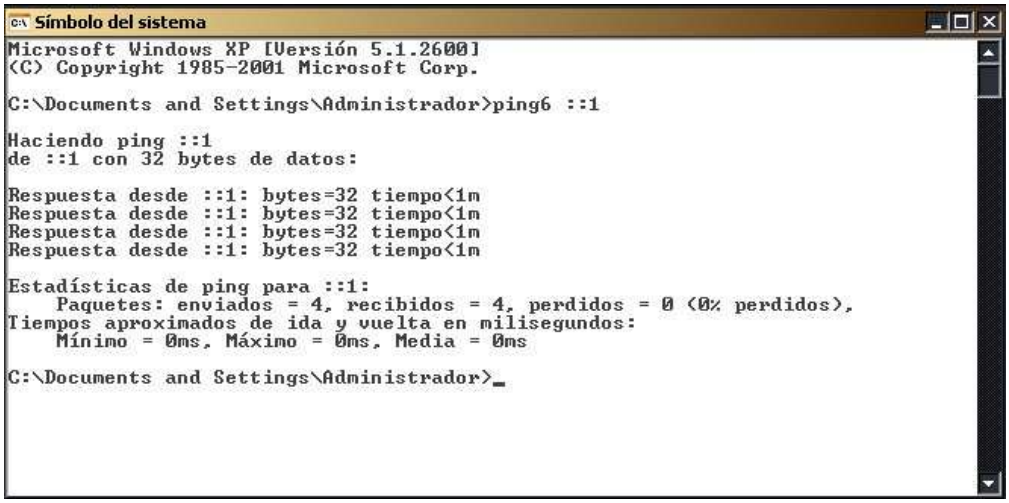

Figura 2.14. Haciendo *ping* a la dirección de *Loopback.*

2.2.2.1 Windows Vista.

Este sistema operativo, ya tiene instalado y habilitado el protocolo de Internet Ipv6. Además, Windows Vista incluye un buen soporte del protocolo IPv6, no solo de características básicas como ocurre en anteriores versiones de Windows como Windows XP y 2003, sino también características avanzadas como [13]: Doble pila IPv4/IPv6 instalada y habilitada por defecto; configuración basada en interfaz grafico de usuario (GUI); Soporte completo para IPsec ; MLDv2; LLMNR; Direcciones IPv6 literales en las URLs ; Soporte de IPv6 en conexiones PPP; DHCPv6 ; Identificadores de interfaz aleatorios.

Para comprobar que el protocolo funciona correctamente, se puede realizar un *ping* a la dirección de *loopback*, tal como se hizo en la sección anterior. La figura 2.15 muestra el comando y su resultado cuando IPv6 se encuentra correctamente instalado en Windows Vista.

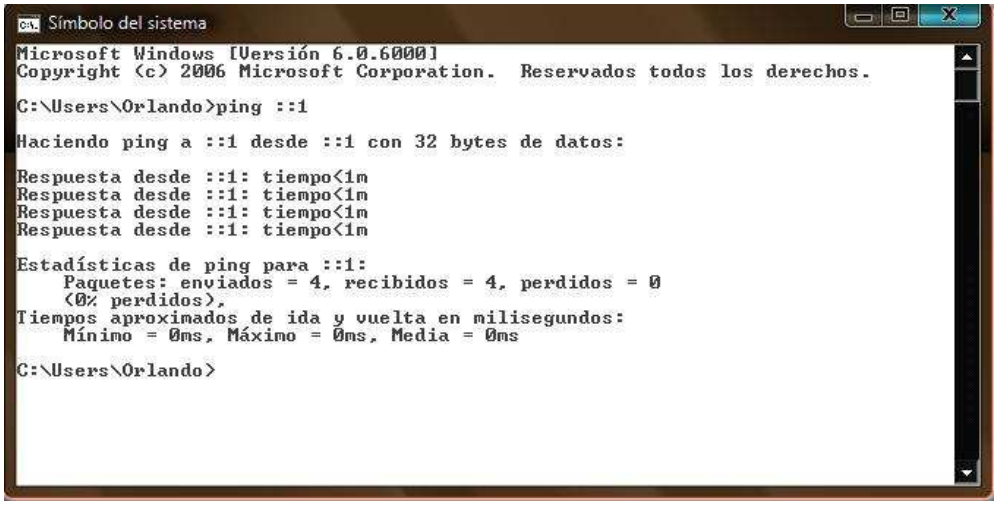

Figura 2.15. Haciendo *ping* a la dirección de *Loopback* en Windows Vista.

2.2.3 Sun Solaris

Para utilizar IPv6 en un el sistema operativo Solaris [14], lo primero que debe hacerse es habilitar IPv6 en una interfaz. La admisión de IPv6 puede establecerse durante la instalación de Solaris 10 o configurando IPv6 en las interfaces de un sistema instalado.

En el proceso de instalación de Solaris 10, IPv6 se puede habilitar en una o varias interfaces del sistema. Tras la instalación, se colocan los siguientes archivos y tablas relativos a IPv6:

- Cada interfaz habilitada para IPv6 tiene asociado un archivo /etc/hostname6.interfaz, por ejemplo hostname6.dmfe0.
- En Solaris 10 11/06 y versiones anteriores, se ha creado el archivo /etc/inet/ipnodes. Después de la instalación, en general este archivo sólo contiene las direcciones de bucle de retorno de IPv6 e IPv4.
- Se ha modificado el archivo /etc/nsswitch.conf para permitir búsquedas mediante direcciones IPv6.
- Se crea la tabla de directrices de selección de direcciones IPv6. En esta tabla se da prioridad al formato de direcciones IP que debe utilizarse en las transmisiones a través de una interfaz habilitada para IPv6.

Para instalar una interfaz IPv6 en un sistema operativo ya instalado, consultar [10].

2.3 Principales mecanismos de transición.

Tal como lo dice el White Paper IPv6 Transition Technologies de Microsoft Corporation [15], la migración de IPv4 a IPv6 no puede ocurrir de un día para otro. Para lograrla es necesario un período de transición, en el cual ambos protocolos deberán coexistir en armonía. De este modo, es necesario contar con los mecanismos adecuados que permitan realizar esta migración, pasando por este período de transición. Es así como los diseñadores de IPv6, crearon tecnologías capaces de hacer que los nodos pertenecientes a la red se puedan comunicar en ambientes mixtos, incluso si están aislados en ambientes donde el protocolo regente es la versión antigua. Es por esto que ver los principales mecanismos de transición, es importante en el desarrollo de esta memoria.

Antes de describir las diferentes técnicas a mencionar, lo primero es realizar una pequeña definición. En [16] se define los siguientes tipos de nodo:

- Nodo IPv4-*only*: Es un nodo que sólo posee implementado IPv4 (y posee solo direcciones IPv4) y no soporta IPv6. La mayoría de los *host* y *routers* instalados hoy en día, son nodos IPv4-*only*.
- Nodo IPv6-*only*: Es un nodo que sólo posee implementado IPv6. (y posee solo direcciones IPv6). Este nodo solo es capaz de comunicarse con nodos y aplicaciones IPv6. Este tipo de nodo no es común hoy en día, pero podría llegar a ser más frecuente, cuando pequeños aparatos, como celulares, incluyan el protocolo IPv6.
- Nodo IPv6/IPv4: Corresponde al nodo que tiene implementados ambos protocolos IPv4 e IPv6.
- Nodo IPv4: Es un nodo que tiene implementado IPv4. Un nodo IPv4 puede ser un nodo IPv4-*only* o un nodo IPv6/IPv4.
- Nodo IPv6: Es un nodo que tiene implementado IPv6. Este puede ser un nodo IPv6-*only* o un nodo IPv6/IPv4.

2.3.1 Mecanismos de transición.

Para que coexistan los dos protocolos, IPv4 e IPv6, y provean una eventual transición a una infraestructura IPv6-*only*, los siguientes mecanismos son utilizados:

- Utilizar IPv4 e IPv6 juntos
- Utilizar túneles IPv6 sobre IPv4
- Infraestructura DNS

2.3.1.1 Utilizar IPv4 e IPv6 juntos.

Durante el período de transición, es necesario que los *hosts* sean capaces de acceder a destinos utilizando ya sea IPv4 o IPv6, pues durante la transición, algunos servidores de servicios serán alcanzables utilizando sólo IPv6 y otro solo IPv4. Es por esto que los

hosts deben ser capaces de utilizar ambos protocolos. Para esto, los nodos IPv6/IPv4 pueden tener las siguientes arquitecturas:

- Arquitectura Dual en la capa IP
- Arquitectura dual del *stack*

La arquitectura dual en la capa IP, corresponde a tener ambos protocolos IPv4 e IPv6 en la capa de red, con una sola implementación de los protocolos de la capa de transporte (como TCP y UDP). La idea es que el protocolo correspondiente se haga cargo de los paquetes, cuando llegan a la capa de red. Las figura 2.4 muestran la representación de esta implementación en el modelo de capas de Internet, y cómo funciona la comunicación en esta implementación.

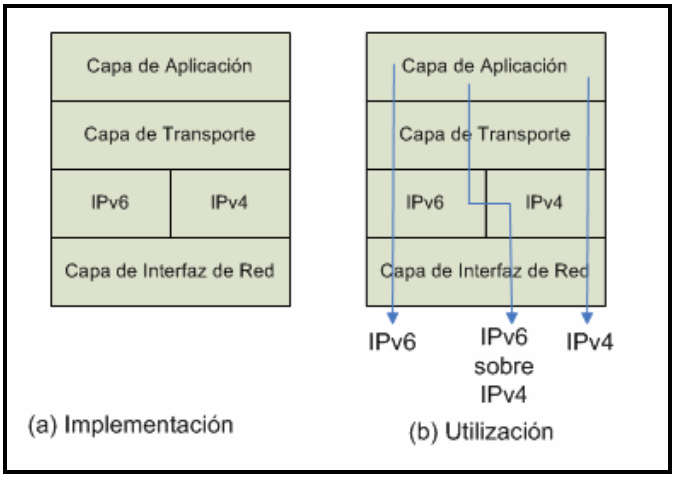

Figura 2.4: Implementación y utilización de la arquitectura dual de la capa IP.

En la implementación dual del *stack* en cambio, se implementan IPv4 e IPv6 con protocolos separados en la capa de transporte. La figura siguiente muestra su implementación y utilización.

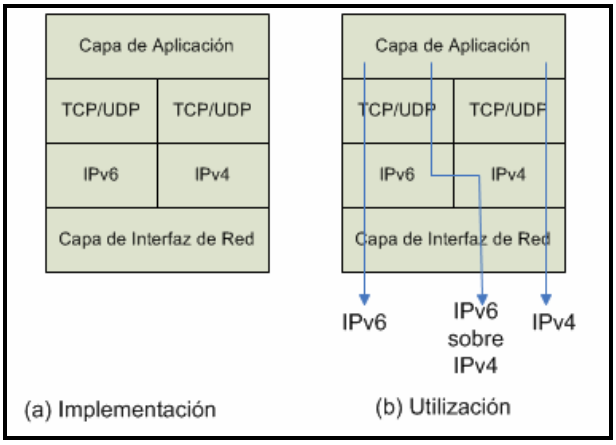

Figura 2.5: Implementación y utilización de la arquitectura dual del stack.

2.3.1.2 Infraestructura DNS.

Actualizar la infraestructura DNS (*Domain Name System*) es de vital importancia. Esto se debe al uso dominante de nombres sobre direcciones para referirse a un recurso de red. Actualizar la infraestructura DNS, significa agregar datos para resolver las peticiones de nombre a dirección y viceversa. Para esto, los servidores deben contener:

- Archivos A para nodos IPv4
- Archivos AAAA para nodos IPv6
- Archivos PTR en el dominio IN-ADDR.ARPA para nodos IPv4 (para el proceso inverso)
- Archivos PTR en el dominio ip6.ARPA para nodos IPv6 (opcional) (para el proceso inverso)

Para el caso de resolución nombre a dirección, el nodo debe ser capaz de determinar cuales direcciones usar como origen y destino. Para el caso de IPv4, esto es irrelevante, pero para el caso de IPv6, cuando un nodo usualmente tiene más de una dirección (o cuando ambos protocolos están implementados), es una decisión importante. Para tomar dicha decisión, el *host* usa un conjunto de reglas de selección, las cuales son descritas en el RFC 3484.

2.3.1.3 Túneles IPv6 sobre IPv4

Realizar un túnel, significa encapsular un paquete IPv6 con un encabezado IPv4, de manera tal de que los paquetes IPv6 puedan viajar en una infraestructura IPv4. Dentro del encabezado IPv6, es importante destacar que:

- El campo protocolo del encabezado IPv4 debe contener el número 41, el cual indica que se trata de un paquete IPv6 encapsulado.
- Los campos de origen y destino del encabezado IPv4, deben contener las direcciones IPv4 de los extremos del túnel. Los extremos del túnel son configurados, ya sea manualmente como parte de la interfase del túnel, o automáticamente derivados de una dirección de siguiente salto de una ruta hacia un destino o interfaz de túnel.

Figura 2.6 muestra un paquete de túnel.

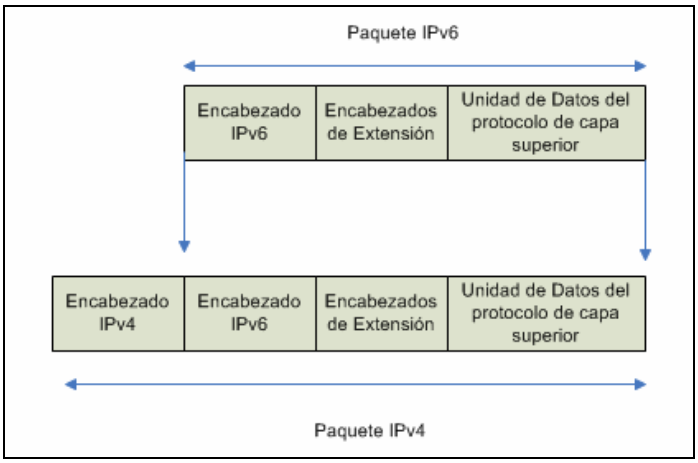

Figura 2.6: Túnel IPv6 sobre IPv4.

2.3.2 ISATAP

ISATAP (*Intra-Site Automatic Tunnel Addressing Protocol*) [16] corresponde a una tecnología que se ocupa de asignar direcciones y realizar túneles de *host* a *host*, *host* a *router*, y *router* a *host* de manera automática, la cual es utilizada para proveer conectividad entre *hosts* IPv6/IPv4 a través de una intranet IPv4, descrita en la RFC 4214. Los *host* ISATAP no requieren ninguna configuración manual y pueden crear direcciones ISATAP utilizando los mecanismos estándar de auto configuración.

Las direcciones ISATAP usan el identificador de interfaz localmente administrada ::0:5EFE:w.x.y.z en la cual, w.x.y.z es una dirección privada unicast. Si la dirección es pública, entonces el identificador de interfaz es ::200:5EFE:w.x.y.z Estos identificadores de interfaz, pueden ser combinados con cualquier prefijo de 64 bits que sea válido para una dirección unicast IPv6. Como se observa, el identificador de interfaz de una dirección ISATAP contiene una dirección IPv4 embebida, la cual es utilizada para determinar el destino para el encabezado IPv4, cuando el trafico IPv6 es realizado a través de un túnel sobre una red IPv4.

2.3.2.1 Comunicación ISATAP

La figura 2.7, muestra como un *host* ISATAP se comunica con otro *host* ISATAP en la misma subred lógica ISATAP.

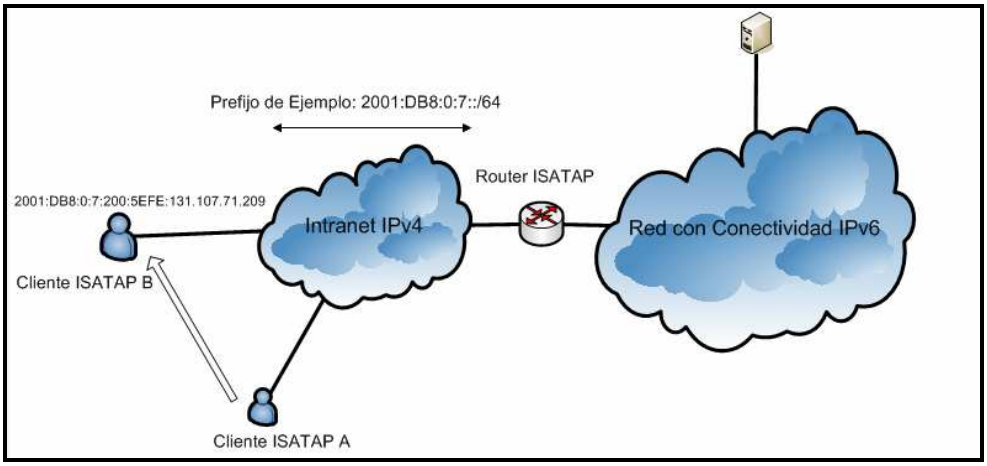

Figura 2.7: Comunicación ISATAP host a host.

En este ejemplo, el *host* A, quiere enviar un paquete al *host* B. El *host* A resolvió la dirección de B a través de un requerimiento DNS. Cuando se envía un paquete IPv6, el host A realiza la elección de la ruta y decide que la ruta más cercana a la dirección, 2001:DB8:0:7::/64. Como corresponde a una dirección en el mismo enlace, el siguiente salto es fijado como la dirección de destino (2001:DB8:0:7:200:5EFE:131.107.71.209). El paquete IPv6 y la dirección del siguiente salto son dados a la interfaz ISATAP para ser procesados.

La interfaz ISATAP fija la dirección de destino IPv4 en el encabezado IPv4, según los últimos 32 bits de la dirección del siguiente salto, donde en este caso, es la dirección IPv4 del *host* B. IPv4 en el *host* A determina que la mejor dirección de origen para ser usada es la dirección IPV4 designada al *host* A y envía el paquete.

2.3.3 6to4

Al igual que en el caso anterior, 6to4 es una tecnología de asignación de direcciones y túneles de manera automática, la cual es utilizada para proveer conectividad entre sitios y *hosts* IPv6 a través de una red IPv4. 6to4 trata la Internet completa como un solo *link* y es descrita en el RFC 3056.

La tecnología 6to4, usa el prefijo de dirección global 2002:WWXX:YYZZ::/48, donde WWXX:YYZZ es la representación hexadecimal de una dirección pública IPv4 (w.x.y.z) asignada a un sitio o *host*. La figura siguiente muestra la estructura de una dirección 6to4.

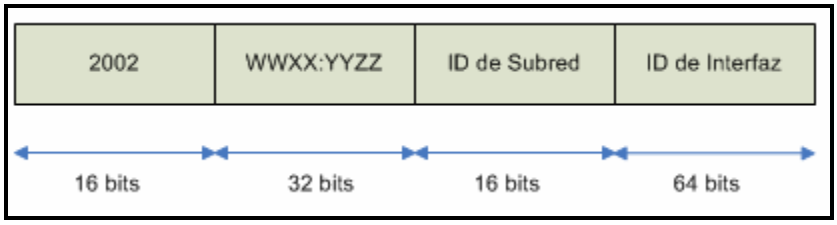

Figura 2.8: Estructura de una dirección 6to4

2.3.3.1 Comunicación 6to4

La figura 2.9 muestra un ejemplo de comunicación entre dos *hosts* IPv6. Cuando un *host* IPv6 el envía un paquete a otro *host* IPv6 (este último en una red IPv6), el viaje del paquete consta de 3 partes.

- Desde el *host* de origen al *router*
- Desde el *router* al 6to4 *relay*
- Desde el 6to4 *relay* al host de destino

En la primera parte del viaje, el *host* A resuelve la dirección del *host* B y envía el paquete IPv6 al *router*. En la segunda parte del viaje, el protocolo IPv6 determina la ruta y encuentra que la ruta más cercana al destino, es la ruta por defecto. El siguiente salto es fijado como la dirección del 6to4 relay (Un 6to4 relay, es un router IPv6/IPv4 que envía los paquetes entre routers 6to4 y host/routers IPv6 en una Internet IPv4 y host en la Internet IPv6). El paquete IPv6 y la dirección del siguiente salto son entregados a la interfaz 6to4 para ser procesados. La interfaz 6to4 fija la dirección de destino IPv4 (en el encabezado IPv4) correspondiente al segundo y tercer bloque de la dirección de destino 6to4, la cual en este caso, es la dirección del 6to4 relay 192.207.1.5. El protocolo IPv4 determina que la mejor dirección de origen a usar es la dirección IPv4 pública asignada al *router* 6to4 (157.60.0.1) y envía el paquete.

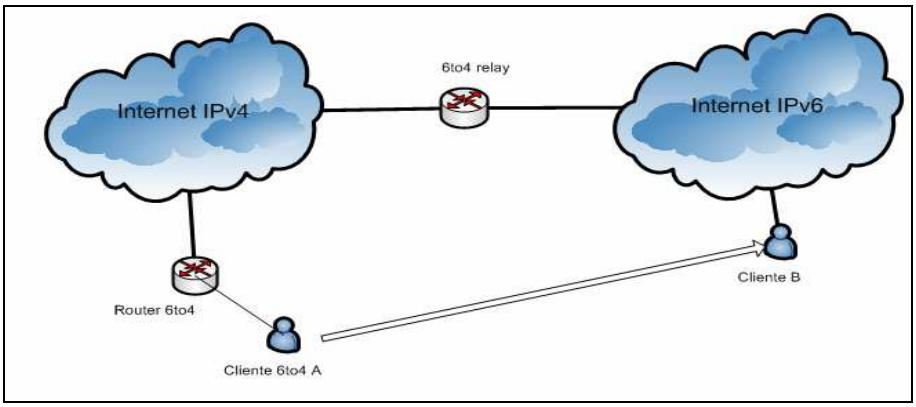

Figura 2.9. Comunicación 6to4 entre 2 *hosts*.

En la tercera parte del viaje, el protocolo IPv4 en el 6to4 *relay*, procesa el encabezado y debido a que en el campo Protocolo se encuentra un 41, el paquete se entrega al

protocolo IPv6 para ser procesado. El protocolo IPv6 determina la ruta a seguir y envía el paquete a un router IPv6 nativo (que no aparece en la figura), por lo que el encabezado IPv4 es retirado del paquete.

2.3.4 Teredo

Teredo, también conocido como NAT-T (*Network Address Translator Transversal*) para IPv6, provee asignación de direcciones y servicios de túnel para entregar conectividad IPv6 en una Internet IPv4, incluso cuando los *hosts* se encuentran detrás de una o más IPv4 NATs. Para atravesar las IPv4 NATs, los paquetes IPv6 son enviados como mensajes UDP.

El mecanismo 6to4 provee una función similar a Teredo, sin embargo, el servicio 6to4 de los *routers* es requerido en el dispositivo de frontera que está conectado a la Internet, siendo su funcionalidad no totalmente compatible con las IPv4 NATs. Incluso si el servicio NAT estuviese habilitado, 6to4 de todos modos no funcionaría para configuraciones en las cuales existan múltiples NATs entre un sitio y la Internet IPv4. Teredo resuelve el problema de la falta de funcionalidad de 6to4 en las modernas NATs de hoy en día o en las NATs configuradas en multicapa, realizando los túneles entre *hosts* dentro de éstos sitios. En contraste, 6to4 realiza los túneles desde el dispositivo frontera.

Utilizar túneles desde los *hosts*, presenta otro problema para las NATs: Los paquetes IPv6 encapsulados con encabezados IPv4, poseen en el campo protocolo el número 41, y la mayoría de las NATs sólo traducen tráfico TCP o UDP, por lo que debe ser configurado manualmente para que sea capaz de realizar la traducción o debe tener instalador un editor de NAT que maneja la traducción. Debido a que la traducción del protocolo 41 no es una característica común de las NATs, el tráfico encapsulado no fluirá a través de las NATs típicas. Es por esto que el paquete es encapsulado como un paquete UDP IPv4, que contiene ambos encabezados IPv4 y UDP, pues los mensajes UDP pueden ser traducidos por la mayoría de los NATs y puede atravesar múltiples capas de NATs.

Teredo ha sido diseñado como último recurso dentro de las tecnologías de transición. Si existe IPv6 nativa, ISATAP o 6to4 presente entre nodos, Teredo no es utilizado. Además las NAT IPv4 son actualizadas para soportan 6to4.

2.4 IPv6 en la actualidad.

Después de todas las explicaciones del caso, de escuchar en todos lados que Internet se está quedando chica, que no hay suficientes direcciones y todas las visiones apocalípticas que incluso afirman que el mundo (cibernéticamente hablando) se va a partir en dos, surge una pregunta obvia ¿Qué se está haciendo para evitar todo esto? La respuesta es clara y fluye de todas las explicaciones teóricas que este mismo documento hace para intentar explicar las ventajas de la nueva versión del protocolo

que, hasta lo mencionado no va más allá de lo puramente teórico. Es fácil pensar de esta manera pues, entre tanta especulación técnica, en esta memoria aún no se ha dicho nada sobre el estado actual del mundo. Es por esto que una revisión del estado del arte respecto a este tema, es algo sumamente necesario en un documento como éste.

2.4.1 LAC NIC y EEUU.

En este contexto, lo primero que cabe mencionar es como se está comportando IPv4 en este momento. El 20 de junio del 2007, en una reunión realizada en Montevideo, Uruguay, LAC NIC, el Registro de Direcciones de Internet para Latinoamérica y el Caribe [17], anunció que para el 2011, el stock de direcciones de Internet versión 4 (IPv4) podría estar definitivamente agotado, por lo que inició una campaña regional para lograr que antes del 1 de Enero del 2011, se logre la total adaptación de las redes de la región al nuevo estándar de IP. Es decir, el problema existe y ya está sobre nosotros.

Como será la presión que se vive en el mundo cibernético, que *The Office of Management and Budget* de EEUU*,* ha ordenado a sus dependencias que convierta sus redes troncales a IPv6 antes del 30 de junio del 2008. Aunque IPv6 no debe estar totalmente operativa para esa fecha, se espera que las redes troncales estén listas para mover tráfico IPv6 y soportar direcciones IPv6.

2.4.2 IANA *(Internet Assigned Numbers Authority*)

IANA [18] asigna y mantiene los códigos exclusivos y sistemas de numeración que se utilizan en las normas técnicas (“protocolos”) que impulsan Internet. Las diversas actividades de IANA pueden agruparse en tres categorías:

- Nombre de Dominio: IANA administra el DNS raíz, los dominios .int y .arpa, y una práctica de recursos IDN.
- Número de Recursos: IANA coordina la reserva mundial de números IP y AS, proporcionándolos a los registros regionales de Internet.
- Asignación de Protocolos: El sistema numérico de protocolos de Internet es manejado por IANA en conjunto con organismos de normalización.

IANA es una de las instituciones más antiguas de Internet, teniendo actividades desde 1970. Hoy en día es operada por la *Internet Corporation for Assigner Names and Numbers* [19], una organización internacional sin fines de lucro creada por la comunidad de Internet para ayudar a coordinar las áreas de responsabilidad de IANA.

Así, en el ámbito de los nombres de dominio, otro paso importante que se ha llevado a cabo durante los últimos meses. IANA ha puesto en funcionamiento desde los primeros días de febrero del 2008, seis de los trece servidores principales de Internet, conocidos como *root servers* [20], con direcciones correspondientes a la nueva versión de IP. La siguiente tabla muestra los servidores cambiados [21]:

Authority	IPv6 Address	Prefix Length*
A.ROOT-SERVERS.NET	2001:503:ba3e::2:30	/48
F.ROOT-SERVERS.NET	2001:500:2f::f	/48
H.ROOT-SERVERS.NET	2001:500:1::803f:235	/48
J.ROOT-SERVERS.NET	2001:503:c27::2:30	/48
K.ROOT-SERVERS.NET	2001:7fd::1	/32
M.ROOT-SERVERS.NET	2001:dc3::35	/32

Tabla 2.3: *Root Servers* que cuentan con IPv6

2.4.3 IPv6 Ready Logo.

A pesar de la urgencia que se tiene para cambiar de un protocolo a otro, todavía existen temas que preocupan a las diversas compañías existentes alrededor del mundo sobre como afrontar este tema, siendo uno de ellos el desconocimiento de que dispositivos están listos para ser utilizados. El protocolo IPv6 pone en la mesa nuevos temas de seguridad, es decir, soluciona problemas viejos pero crea problemas nuevos. Al contar con una configuración IPv6-IPv4 *dual stack,* se incrementa la posibilidad de potenciales vulnerabilidades de seguridad, como consecuencia de tener dos infraestructuras con problemas específicos de seguridad. Utilizar técnicas de tunneling también tiene su riesgo, pues es posible realizar ataques basados en *spoofing*. Por estos y otros problemas, es comprensible que las principales compañías sean reacias al cambio, pues no saben con certeza cómo les va a afectar el cambio y si las aplicaciones disponibles, están ya capacitadas para solucionar dichos problemas [22].

Una buena forma de solucionar este desconocimiento que existe sobre que dispositivos están capacitados de operar con IPv6, lo presenta el IPv6 *Forum,* el cual ha lanzado el IPv6 *Ready Logo* [23]. Este logo, tiene como objetivo informar al consumidor que el producto que adquiere cumple con los requerimientos que garantizan un buen funcionamiento del nuevo *stack* de protocolos, el cual cuenta con 2 tipos o “fases”. La primera fase corresponde al logo de color plateado de fondo (figura 2.3a) que indica que el producto cumple con las especificaciones básicas. La segunda fase, cuyo logo es de color dorado (figura 2.3b), extiende la exigencia a categorías que son consideradas recomendadas (“*should*” y no “*must*”). Para obtener este logo, los productores deben enviar sus productos a los laboratorios de *IPv6 Ready* ubicados en varios lugares del globo (Estados Unidos, Japón, Francia, Taiwán, China y Corea) para que sean sometidos a las pruebas correspondientes, o descargar las herramientas de auto-prueba (*self-testing*), ejecutarlas y enviar los resultados por *e-mail* al ente correspondiente.

(a) Fase 1 (b) Fase 2

Figura 2.3: IPv6 Ready Logo

Actualmente se está trabajando en una fase 3, la cual será igual a la fase 2 en términos de contenido, excepto que la prueba extendida para IPsec [24] será obligatoria.

2.4.4 Microsoft e IPv6

Los principales fabricantes de sistemas operativos también están preocupados de lanzar al mercado productos que sean compatibles con ambos protocolos, de manera que si existe alguna conexión que no funcione con IPv6, funcione con IPv4. Así, la idea es realizar una transición limpia, para que sea posible seguir utilizando sistemas antiguos, y a la vez sacar todo el provecho posible de las nuevas funcionalidad de IPv6 con los que pueden utilizarla. De esta forma, *Microsoft*, por ejemplo, lleva ya varios pasos hacia la transición, teniendo claro que las características nuevas del protocolo pueden afectar a viejas aplicaciones (como el mayor largo de direcciones), por lo que ha definido nuevas APIs de *Windows*, integradas desde el *Service Pack* 2 de *Windows* XP. Siguiendo este objetivo, los principales pasos que Microsoft ha tomado para integrar IPv6, son los siguientes [25]:

- La transición a IPv6 comenzó en 1998 con la disponibilidad de una implementación de IPv6 ofrecida por *Microsoft Research*. Esta versión se suministraba como ayuda a la comunidad de desarrollo de estándares IPv6 a fin de poder conocer y probar el protocolo durante su fase de definición.
- En marzo de 2000 se dio a conocer una primera revisión de la tecnología, para sistemas *Windows* 2000. Esta versión permitió a los desarrolladores conocer y familiarizarse con los conceptos y características del protocolo, necesario para poder hacer compatibles sus aplicaciones con IPv6
- En octubre de 2001 *Windows* XP sale al mercado con una pila IPv6 provisional para desarrolladores y los componentes principales de un sistema compatible con IPv6, de forma que los programadores podían empezar a diseñar y probar aplicaciones capaces de utilizar IPv6.
- En marzo de 2003 hace su aparición *Windows Server* 2003, con la primera versión de producción del protocolo IPv6 y componentes compatibles.
- En julio de 2003, hace su aparición el *Advanced Networking Pack* para *Windows* XP. Este paquete incluía un cliente Teredo, llamado IPv6 *Internet Connection Firewall*, así como soporte para redes *peer-to-peer* con *Windows*.
- En agosto de 2004 aparece el *Service Pack* 2 (SP2) de *Windows* XP. Este *Service Pack* incluye el cliente Teredo, soporte para redes *peer-to-peer* de *Windows* (tal y como se ofrecía en el *Advanced Networking Pack* para *Windows*

XP), y soporte integrado para tráfico IPv6 con el nuevo *Firewall* de *Windows* (que sustituye al *Firewall* de IPv6 *Internet Connection*).

Así, los últimos sistemas operativos de Microsoft (principal proveedor de sistemas operativos en el mundo), ya cuentan con los mecanismos de transición de IPv6 instalados, siendo estos *Windows* XP con *Service Pack* 1 y posterior, *Windows Server* 2003, *Windows Vista* y el *Windows Server* 2008, cuya fecha de lanzamiento en Chile fue el 15 de abril del 2008.

2.4.5 Sitios Web e IPv6.

Otra información de interés es que sitios Web se pueden acceder a través de IPv6. A pesar de lo que se podría pensar, existen varios sitios que cuentan con accesibilidad para el nuevo protocolo de Internet. Un buen ejemplo de esto es la página oficial de las olimpiadas de Beijing 2008 [26] la cual ya está disponible en su versión IPv6. Por otro lado, existe un sitio muy común para todos los usuarios de Internet que también posee actualmente una versión en IPv6: Google [27].

Así la lista de sitios Web de empresas que ya han adoptado este nuevo protocolo crece día a día, siendo imposible mencionarlas todas en este documento. Este crecimiento indica que el mundo ya está migrando hacia el nuevo protocolo, mostrando que la transición es posible y está más cerca de lo que se cree. Para una lista más exhaustiva de sitios Web accesibles a través de IPv6 consulte [28] y [29].

2.5 La red de Codelco-Chile.

Codelco-Chile tiene una red compleja. Considerando las diferentes divisiones que posee y la cantidad de personal perteneciente a cada una de ellas, hacen que la red con aproximadamente 12 mil clientes sea bastante complicada de analizar detalladamente. Sin embargo, lo que sí se puede hacer, es describir la arquitectura, diseño y distribución que esta red posee. En este ámbito, en los siguientes párrafos, se procede a describir de manera general, pero sin dejar de lado los aspectos más importantes, la red de Codelco-Chile.

2.5.1 La red WAN.

Codelco-Chile, al ser una empresa que cuenta con divisiones a lo largo de la zona centro y norte de Chile, necesita contar con una red expedita, de alta disponibilidad y de una velocidad lo suficientemente rápida como para permitir comunicar de manera transparente y segura sus distintas dependencias, a pesar de que geográficamente se encuentran separadas por varios cientos de kilómetros. Para lograr satisfacer esta necesidad, Codelco-Chile cuenta con una red WAN (*Wide Area Network)* que une todos

estos puntos, la cual es un servicio entregado por una empresa de Telecomunicaciones externa a la corporación.

Esta red WAN es capaz de cubrir cientos de kilómetros y le entrega la confidencialidad necesaria a los datos, a pesar de ser compartida por otras empresas (pues es un servicio arrendado). La confidencialidad mencionada es entregada por el protocolo MPLS [30] que permite separar lógicamente una conexión de otra.

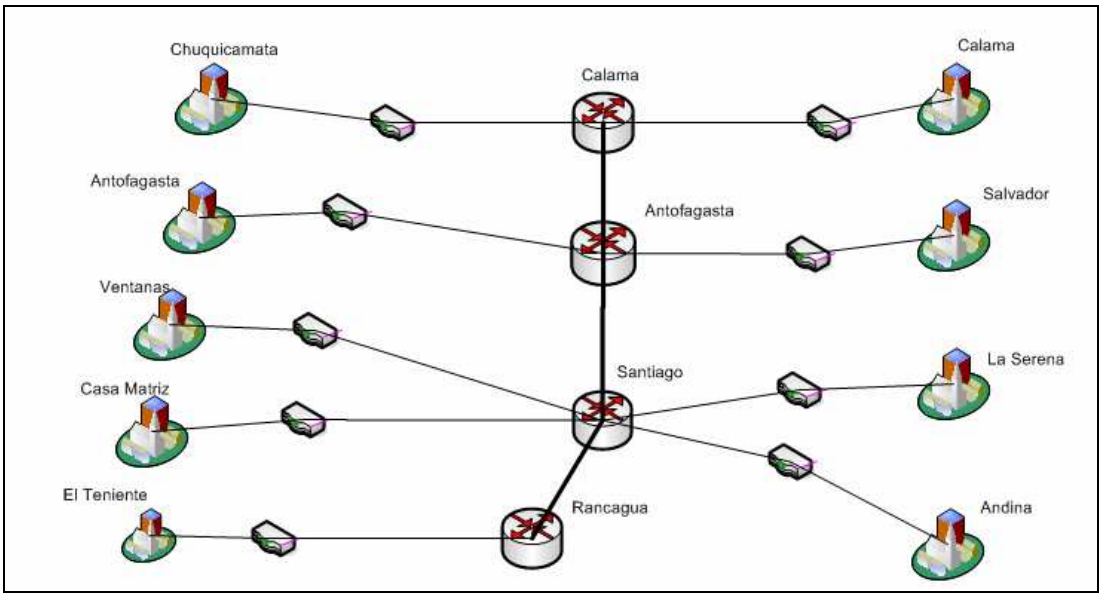

Figura 2.16. Esquema Final de Interconexión Red WAN Corporativa - 2006

La figura 2.16, muestra el esquema utilizado en la red WAN. Este esquema no muestra la red completa de Codelco, solo muestra la conexión entre divisiones, pues dentro de cada una de ellas, se encuentra una red local completa, la cual será descrita más adelante.

2.5.2 Red de Datos de las Divisiones.

El contar con una red interna, es una necesidad básica para cualquier empresa. Distintos trabajos son realizados o supervisados a través de una red de computadores, desde el e-mail hasta las cámaras *web*, representan ahora herramientas fundamentales de trabajo, lo que se traduce en la exigencia de conectividad entre los diferentes puntos de trabajo. Es por esto que cada división creó en algún momento redes que les permitieran realizar sus trabajos habituales. Mientras la necesidad iba creciendo, las redes crecían también, tratando de satisfacer las necesidades naturales de cada división de la empresa.

Sin embargo, este crecimiento espontáneo, tiene sus desventajas. Debido a que hasta hace no mucho tiempo atrás, Codelco no contaba con un organismo centralizado que

se preocupara de diseñar, implementar y mantener dichas redes, éstas crecieron en forma inorgánica en cada división según la necesidad y visión del lugar. Distintas arquitecturas, distintos equipos y distintas tecnologías, llevaron a que la red interna de cada división fuese complemente diferente una de otra, lo que creó un gran desorden tecnológico.

A partir de la creación de la Gerencia Corporativa T.I.C.A. (Tecnologías de Información, Comunicación y Automatización), se inició el proyecto de ordenar y unificar las arquitecturas y topologías de red, de manera de contar con la información centralizada y con un organismo que velará por el buen funcionamiento de la red corporativa en su totalidad. De esta forma, se comenzó a desarrollar un plan de estandarización de la arquitectura de la red, la cual consiste en ordenar las diferentes divisiones, de manera que cuenten con características similares de red. Según las necesidades de cada una se ordenaron los servicios y servidores dispuestos en la red, de manera de facilitar la mantención y mejorar la seguridad informática.

Durante este proyecto de ordenamiento de red, que lleva ya unos 4 años, se diseñó una arquitectura de red la cual sería el molde a seguir en las divisiones y que presenta diferentes soluciones para las distintas necesidades. En la figura siguiente, se muestra el esquema de dicha arquitectura. En ella se puede observar que a partir de la conexión a la red WAN se crean diferentes sub-redes. En una sub-red se agrupan los servidores que proveen los servicios de e-mail, etc, en otra sub-red se encuentran los clientes (el personal de Codelco-Chile), etc. Este agrupamiento tiene como objetivo controlar de mejor forma a los distintos computadores que pertenecen a la red, pues por ejemplo, donde se encuentran los servidores, no debe haber bajo ningún caso un cliente, y si hubiese alguno en esa sub red, significaría una brecha de seguridad en el sistema.

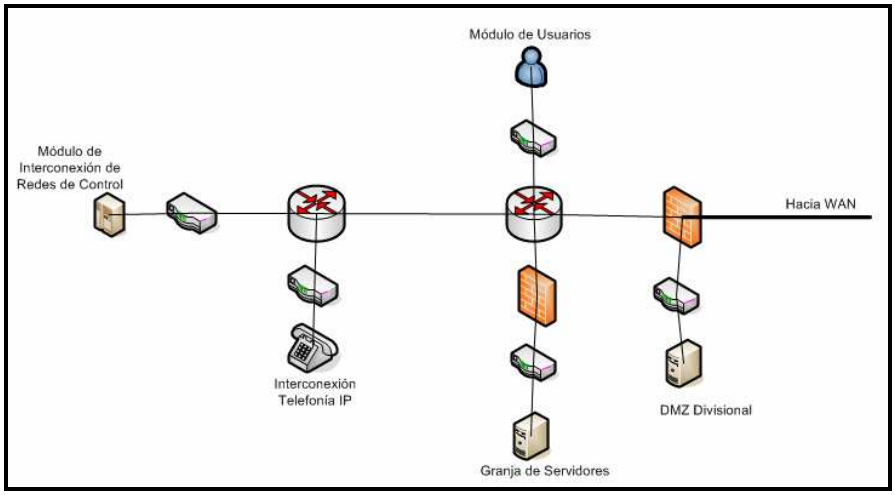

Figura 2.17 Esquema Red de Datos de una División Genérica.

La figura 2.17, muestra el plano de red de manera conceptual, esto se debe a que según las políticas de seguridad de la empresa, no es posible publicar toda la información disponible. Sin embargo con el diagrama mostrado en las figuras 2.16 y 2.17, es suficiente para comprender la distribución de la red en la Corporación.

2.5.3 Distribución de direcciones IP.

Debido al crecimiento desequilibrado de las redes de las distintas divisiones, las direcciones IP fueron asignadas según las necesidades presentes en el momento. Es por esto que después de un tiempo, la distribución de las direcciones fue confusa y desordenada, por lo que se planteó un proyecto de ordenamiento de las direcciones IP. Así, después de varios años, se ha ido cambiando las direcciones de las interfaces de red, de manera tal de que exista orden y claridad en las asignaciones dadas.

La asignación actual de las direcciones IPv4, se pensó de manera que fuesen fijadas de manera clara y concisa, de fácil manejo y acceso, para que en futuras generaciones no existiesen nuevamente los problemas mencionados. Lo primero que se cambió, fue el número de direcciones IP disponibles, desde una Clase B a una Clase A, por lo cual se cuentan con 16 777 214 direcciones disponibles a ser asignadas, a diferencia de las 65 534 que cuenta una Clase B. Luego, el siguiente paso fue definir cómo se haría la asignación de modo de evitar en un futuro el problema descrito en los párrafos anteriores. El problema se solucionó de la siguiente manera: al contar con una Clase A, solo el primer octeto se encuentra fijo en las direcciones, por lo que los 3 octetos siguientes, se encuentran complemente disponibles a ser utilizados. Entonces el paso siguiente es pensar en como realizar una utilización eficiente de éstos octetos. La solución fue bastante simple e interesante, y se presenta a continuación.

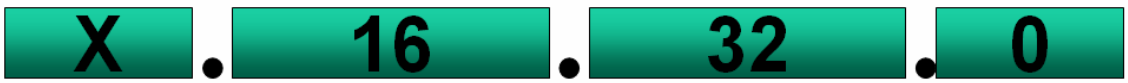

Figura 2.18: Dirección IP a Asignar

La figura 2.18, muestra una dirección ejemplo que será asignada a un equipo de una división. Si se escriben los bits de la dirección, se tiene la figura 2.19

Figura 2.19: Dirección IP escrita con bits

Los primeros 4 a 8 bits del primer octeto son utilizados para identificar la división o módulo al cual pertenece el equipo, los siguientes 0 a 4 bits se utilizan para identificar el Centro de Trabajo al que pertenece el usuario. Para el tercer octeto, se tiene que los primeros 5 bits se utilizan para identificar subdivisión (edificio, piso, segmento), y los últimos 3 restantes para servicios (administrador, usuarios, voz, etc).

El modelo presentado, no solo posee las ventajas de ordenamiento ya mencionadas, sino que además posee otras características que son grandes ventajas en comparación con la asignación anterior: disminución de las tablas de enrutamiento de los equipos de la red; disminución del uso de la CPU y memoria de los equipos de comunicaciones y un enrutamiento más eficiente ya que cada división (Site o edificio) se conoce por uno o dos prefijos.

Capitulo III: Plan de Adopción de IPv6 para Codelco-Chile.

A continuación se presenta el plan de adopción de IPv6 para la red corporativa de Codelco-Chile, partiendo desde el estado de la red descrito en el capítulo anterior, es decir desde IPv4, llegando a una red donde ambos protocolos conviven.

3.1 Antecedentes Previos.

Sin importar si se trata de una corporación de gran magnitud, como lo es Codelco-Chile, o si se trata de una micro empresa comenzando sus labores, el proceso de adopción de IPv6, comienza de la misma forma, definiendo el escenario correspondiente a la empresa. Para poder definir las necesidades de la firma y lograr acotar la discusión en los temas relevantes, es necesario contar con una descripción clara de la realidad de la empresa y conocer también cual es el objetivo final de la migración. Con ello se puede saber con mayor seguridad cuales son los cambios requeridos para lograr el objetivo final.

Cuando se habla de escenario inicial, se refiere al estado en que se encuentra la red empresarial en el momento en el cual se piensa realizar la migración. El escenario final, en cambio, indica los requerimientos que se deben cumplir al final del proceso.

Teniendo en mente la necesidad de conocer los escenarios correspondientes, el siguiente paso corresponde a definir que tipo de empresa es la que se desea migrar. Según [31], la primera empresa a distinguir, es una empresa proveedora de servicios de Internet (ISP: *Internet Service Provider*), la cual, tal como su nombre lo indica, es la encargada de brindar Internet a otras empresas. Este tipo de empresas no están en el alcance de este documento, siendo [32] la referencia indicada para continuar el estudio. El siguiente tipo de empresa a distinguir, es una empresa pequeña, la cual posee una red de menor complejidad, menor número de equipos en la red, y distintas políticas de seguridad y calidad. Este tipo de red, junto con las redes hogareñas, tampoco está en el alcance de este documento [33]. Finalmente, el último tipo de empresa a distinguir, es una empresa grande, o una corporación. Este tipo de empresa posee cientos de equipos de trabajo, una red bastante compleja y políticas de seguridad y calidad bastante exigentes. Este tipo de empresa corresponde a Codelco-Chile, siendo entonces la que se desarrollará en detalle en este documento.

En lo que a una empresa grande se refiere, la referencia [34] define los escenarios de la siguiente manera: el primer escenario asume que la empresa decide desplegar IPv6 en conjunto con IPv4; el segundo escenario asume que la empresa decide desplegar IPv6 debido a la necesidad de utilizar un conjunto específico de aplicaciones sobre una red

IPv6; y finalmente, el tercer escenario asume que la empresa construye una nueva red, o desea reestructurar una ya existente y decide desplegar IPv6 como el protocolo dominante dentro de la empresa, coexistiendo con IPv4. A continuación se definen de manera más detallada dichos escenarios.

3.1.1 Definición de los Escenarios Base.

Mientras es difícil cuantificar todos los escenarios factibles que enmarquen todas las necesidades que una empresa pueda tener, si es posible desglosar un grupo abstracto de escenarios que permita ayudar con la planificación. Luego, tal como se hace en la referencia [34], se definen tres escenarios base, los cuales pretenden capturar las necesidades esenciales de un grupo de empresas, donde en cada uno existen suposiciones y requerimientos.

3.1.1.1 Escenario 1.

El primer escenario a definir, corresponde a un despliegue de IPv6 a través de una arquitectura dual del *stack* del protocolo, es decir haciendo que los equipos sean capaces de utilizar IPv4 e IPv6 conjuntamente. Este despliegue es total, es decir dentro de la red existente se busca insertar IPv6 en conjunto con IPv4 .

Existe solo una suposición en este escenario, la cual dice que la infraestructura de red disponible para IPv4 posee las mismas capacidades para IPv6. Es decir, la infraestructura de red es capaz de desplegar IPv6 de igual forma que IPv4. Por otro lado, el requerimiento que debe cumplir este escenario, pide que las suposiciones dadas no perturben la infraestructura de red IPv4. El protocolo IPv6 debe ser equivalente o “mejor” que su antecesor, aunque se entiende que éste no debe porque resolver los problemas de red que no han sido resueltos por IPv4. Además puede que no sea factible desplegar IPv6 en toda la red inmediatamente.

3.1.1.2 Escenario 2.

En este escenario se busca un despliegue parcial de IPv6 dentro de la red de la empresa. Este caso corresponde a una empresa que posee una red IPv4 y que desea utilizar ciertas aplicaciones IPv6, por lo cual el despliegue del protocolo es limitado al mínimo requerido para operar este conjunto de aplicaciones.

Se supone en este escenario que los componentes de hardware/software necesarios para la utilización de dichas aplicaciones están disponibles y que las plataformas para las aplicaciones son capaces de soportar IPv6. Finalmente, el único requerimiento de este escenario es que la infraestructura IPv4 no se vea perturbada.

3.1.1.3 Escenario 3.

El tercer y último escenario a distinguir es el siguiente. La empresa decide desplegar una nueva red o reestructurar la existente, teniendo al protocolo IPv6 como la base para

las comunicaciones. Pueden que sea necesario pasar por algunos nodos IPv4 para comunicar la red.

Como suposición, se tiene que están disponibles los componentes de infraestructura necesarios para que la red utilice IPv6, o en el peor de los casos, éstos estarán disponibles en un tiempo definido, apoyando así el plan de la empresa. El requisito a cumplir, es que debe existir interoperabilidad y coexistencia con la red IPv4 en infraestructura y aplicaciones para permitir las comunicaciones.

3.1.2 Componentes de la Infraestructura de Red en los Distintos Escenarios.

Una vez establecido el escenario final al cual se pretende llegar, el que a grandes rasgos debería corresponder a uno de los tres descritos en la sección anterior, es importante distinguir cual es la infraestructura de red que se posee y a la cual se desea llegar. Cuando se habla de infraestructura de red, se refiere a los programas utilizados, operadores de red, configuraciones de red y los métodos empleados para operar una red en una empresa.

Una forma de describir la infraestructura en cuestión, la presenta [16], y corresponde a contestar un grupo de preguntas que ayudan a entender los requerimientos de red, y se presentan como funciones que la empresa debe analizar como parte de definir su escenario específico. Las preguntas listadas en [34], están divididas en 5 componentes de red las cuales serán mostrados a continuación.

3.1.2.1 Componente de Red 1: Requerimientos del Proveedor de Empresa.

A continuación se muestra un grupo de preguntas que ayudan a definir los requerimientos que involucran al proveedor de la empresa. Para una lista más extensa de preguntas, consulte [34].

- ¿Se necesita conectividad externa?
- ¿La empresa posee sitios en diferentes lugares geográficos?
- ¿Líneas arrendadas o VPNs?
- Si existen múltiples sitios, ¿Cómo es intercambiado el tráfico de forma segura?
- ¿Cuántas direcciones IPv4 están disponibles para la empresa?
- ¿Ofrece el proveedor de Internet servicios IPv6?
- ¿IPv6 estará disponible usando los mismos enlaces de acceso de IPv4 o se utilizarán diferentes?

3.1.2.2 Componente de Red 2: Requerimientos de las Aplicaciones de la Empresa.

Nuevamente es presentada la lista de preguntas que corresponde a las necesidades de la empresa, en lo que a aplicaciones se refiere. Esta lista no está completa, solo se muestran algunas preguntas correspondientes al tema. Para mayor información consulte [34].

- ¿Cuáles son las aplicaciones que utiliza la empresa?
- ¿Qué aplicaciones deben ser migradas a IPv6?
- ¿Pueden ser las aplicaciones actualizadas a IPv6?
- ¿Las aplicaciones utilizan direcciones IP ruteadas de manera global?
- ¿Las aplicaciones corren sólo en la red interna de la empresa?

3.1.2.3 Componente de Red 3: Requerimientos del Departamento IT de la Empresa.

A continuación se presenta la lista de preguntas correspondiente a los requerimientos del departamento de IT (Tecnologías de la Información). Para una lista más detallada refiérase a [34].

- ¿Quién es dueño y opera la red: es propia o arrendada?
- ¿Trabaja remotamente? (i.e. a través de VPNs?
- ¿Es necesaria la comunicación entre los sitios?
- ¿Cuántos sitios geográficamente separados poseen su propia conexión a Internet?
- ¿Cuál será la política de QoS?
- ¿Cuál será la política de seguridad?

3.1.2.4 Componente de Red 4: Sistema de Gestión de Red de la Empresa.

Las preguntas correspondientes a este requerimiento, se muestran a continuación. Para mayor información, consulte [34].

- ¿Qué rendimiento de la gestión es requerido?
- ¿Qué aplicaciones de gestión de red son requeridas?
- ¿Qué configuraciones son requeridas?
- ¿Cuáles serán las políticas de gestión y ejecución?
- ¿Cuál es la política de seguridad requerida?
- ¿Cuál será la gestión de las herramientas y mecanismos de transición?
- ¿Qué nuevas consideraciones crea IPv6 en lo que se refiere a gestión de red?

3.1.2.5 Componente de Red 5: Ínter operación y Coexistencia de la red de la Empresa.

Finalmente, las preguntas correspondientes al último ítem, son las siguientes. Para mayor información, consulte [34].

- ¿Cuáles plataformas deben ser capaces de trabajar con IPv6?
- ¿Qué puntos de acceso a la red deben ser capaces de trabajar con IPv6?
- ¿Qué mecanismos de transición deben soportar operaciones de red en IPv6?
- ¿Qué políticas y procedimientos son requeridos para lograr la transición a IPv6?
- ¿Qué políticas y procedimientos son necesarias para apoyar la inter operación con el legado de los nodos y las aplicaciones?

3.1.3 Requerimientos de los Componentes de la Infraestructura de Red.

Luego de identificar los distintos componentes, el siguiente paso corresponde a identificar cuales son los requerimientos de cada uno de éstos. Es importante que la empresa determine cuales requieren mejoras o necesitan ser agregados para desplegar IPv6, las cuales deben ser entendidas y manejadas como recursos críticos. Los requerimientos identificados, tal como aparece en [34], son los siguientes.

3.1.3.1 DNS.

El servicio de nombres de dominio, DNS, tendrá ahora que soportar ambos protocolos: IPv4 e IPv6. Es por esto que la empresa debe determinar cómo el DNS será gestionado, accedido y asegurado. Para mayor información sobre cómo operar DNS en IPv6, refiérase a [35].

3.1.3.2 Ruteo.

Tanto el ruteo exterior e interior deberán soportar IPv6 e IPv4. La empresa por lo tanto, deberá definir la topología de ruteo, los puntos de ingreso a la red (desde el proveedor de servicios) y los mecanismos de transición que desea utilizar para adoptar IPv6. La empresa deberá averiguar también que mecanismos de transición son soportados por su proveedor aguas arriba.

3.1.3.3 Configuración de los Equipos.

IPv6 introduce el concepto de auto configuración *stateless*, junto con la auto configuración *stateful*, para la configuración de *hosts* dentro de la empresa. Es por esto que se deberá decidir el mejor método para la configuración de los equipos dentro de la red, y como actuará la auto configuración para actualizar los registros de DNS. También habrá que decidir cómo se realizará la delegación de prefijos desde el ISP y como se entregarán en la red empresarial. Las políticas para DNS o para la elección de la autoconfiguración, están fuera del alcance de este documento, para mayor información, refiérase a [36], [37], [38].

3.1.3.4 Seguridad.

Los mecanismos utilizados para proveer seguridad en IPv4 deben ser soportados por IPv6. El nuevo protocolo no debe crear ninguna nueva preocupación de seguridad. Toda la infraestructura de seguridad utilizada en la red, debe ser revisada y analizada para saber cuales son compatibles con IPv6. Los requerimientos de filtros de seguridad y *firewalls* deben ser determinados por la empresa y contrastados con la información del proveedor sobres el tema de compatibilidad con IPv6.

3.1.3.5 Aplicaciones.

Las aplicaciones existentes deberán ser revisadas y actualizadas si es necesario, para que sean compatibles con IPv6. Para mayor información, consulte [39].

3.1.3.6 Gestión de la Red.

Los operadores de red, deberán investigar que herramientas de red son compatibles con IPv6 para ser utilizadas en la gestión de ella. La gestión de la red no necesita ser compatible con ambos protocolos y no necesariamente debe ver los nodos como *dual stack*.

3.1.3.7 Plan de Direcciones.

La cantidad de direcciones disponibles deberá ser definida y coordinada con la topología de ruteo de la red empresarial. También es importante conocer la lista de direcciones IPv4 disponibles para ser utilizadas por los mecanismos de transición.

3.1.3.8 Multicast.

Si la empresa utiliza *multicast* IPv4, deberá considerar cómo estos servicios pueden ser implementados en un ambiente con IPv6 habilitado.

3.2 Definición del Escenario de Codelco-Chile.

Para crear un plan de migración a IPv6 para Codelco-Chile, es necesario seguir los pasos descritos en la sección anterior, para posteriormente analizar la situación definida y luego plantear la solución al problema. Entonces, siguiendo la lógica ya descrita, el primer paso es definir el escenario inicial y final. El primero de ellos, corresponde al estado actual de la red empresarial, la cual fue descrita en el capitulo 2 de este documento. El escenario final, es al que se espera llegar una vez terminada la migración.

3.2.1 El Escenario Final Esperado.

Analizando los escenarios descritos en la sección anterior, se tiene lo siguiente. Codelco-Chile, no tiene intenciones de desplegar toda una nueva red para el uso de IPv6. Las razones que Codelco-Chile esgrime es que hacerlo es caro y además no se ve la necesidad de un cambio tan radical, debido a que el uso del nuevo protocolo aún no es una necesidad inmediata. Por consiguiente, armar una red desde cero para utilizar IPv6 se ve como un gasto innecesario lo que descarta el escenario 3. Codelco-Chile tampoco desea utilizar aplicaciones especialmente diseñadas en IPv6, pues sus

aplicaciones nativas son todas creadas bajo el antiguo protocolo de Internet. Entonces, pensar en el escenario 2 no tiene sentido. Es así entonces, como el escenario que más se ajusta a las necesidades de la empresa, es el escenario 1.

Además, tal como se mencionó anteriormente, todas las aplicaciones nativas de la empresa han sido creadas bajo el antiguo protocolo de Internet, por lo cual no es seguro que todas funcionen correctamente al realizar el cambio a IPv6. Luego es necesario, como paso intermedio hacia un dominio total del protocolo de nueva generación, hacer convivir IPv4 e IPv6 de manera tal que las aplicaciones que no son compatibles con el cambio puedan seguir en funcionamiento. Por consiguiente, la arquitectura de *dual-stack* es necesaria en este escenario.

Por otro lado es importante tener en mente que, si se espera una migración total en el largo plazo, es necesario contar con un plan intermedio que permita adquirir conocimientos y realizar las pruebas correspondientes para ajustar la funcionalidad del proyecto a los requerimientos específicos de la empresa. Luego, mantener una doble pila de protocolos con el objetivo de mantener de respaldo bajo cualquier eventualidad el sistema antiguo, es siempre una buena idea. Además realizar un despliegue total del protocolo permite probar su funcionamiento en distintos ambientes de la empresa, pues la diversidad de usuarios con la que Codelco-Chile cuenta puede poner a prueba cualquier sistema de telecomunicaciones. Además, el despliegue total de IPv6 en forma de *dual stack*, permite tener la red preparada para la migración final. Bastaría, en teoría, sólo desactivar IPv4 para concluir una migración total, una vez realizados todos los ajustes correspondientes.

No está demás mencionar también que el apunte a una arquitectura de doble pila, permite realizar los cambios de manera gradual, enfrentando los problemas paso a paso y con menos riesgo de afectar negativamente el sistema de comunicaciones. Así entonces, el escenario final planteado para el proceso de adopción corresponde al escenario 1, el cual es un paso intermedio hacia el dominio total del nuevo protocolo de Internet.

3.2.2 La Respuesta a las Interrogantes.

El siguiente paso, tal como se describe en la sección anterior, corresponde a depurar el escenario seleccionado, de manera de describir de mejor manera, el futuro y la realidad de la empresa. Dentro del conjunto de preguntas presentado, hay interrogantes que se responden de manera inmediata, otras con un poco más de análisis y algunas más con una investigación más a fondo.

3.2.2.1 Componente de Red 1: Requerimientos del Proveedor de Empresa.

Este conjunto de preguntas referidas al primer componente de red definido en las secciones anteriores, ve sus respuestas al final del capítulo 2 de este documento. Para mostrar la relación entre las preguntas y respuestas, a continuación se presenta en forma detallada las respuestas enunciadas en la sección 3.1.2.1.

- ¿Se necesita conectividad externa?

  Sí, es necesaria la conectividad externa. Para la utilización de servicios como el correo electrónico e incluso para navegar por Internet, es necesario contar con un enlace nativo externo.

- ¿La empresa posee sitios en diferentes lugares geográficos?

  Sí, la empresa posee divisiones desde Antofagasta hasta Rancagua.

- ¿Líneas arrendadas o VPNs?

  Las líneas son arrendadas.

- Si existen múltiples sitios, ¿Cómo es intercambiado el tráfico de forma segura?

  Se utiliza el protocolo MPLS para el intercambio seguro de información.

- ¿Cuántas direcciones IPv4 están disponibles para la empresa?

  Actualmente Codelco posee asignada una dirección IPv4 Clase A, por lo que cuenta con 16.777.214 direcciones disponibles.

- ¿Ofrece el proveedor de Internet servicios IPv6?

  No, hasta el momento no existe ningún proveedor de servicios de Internet (ISP) que entregue servicios IPv6.

- ¿IPv6 estará disponible usando los mismos enlaces de acceso de IPv4 o se utilizarán diferentes?

  Puesto que se desea minimizar los costos, se pretende utilizar los mismos enlaces de acceso (aunque no se descarta la idea de poseer un enlace nativo IPv6 desde algún ISP).

3.2.2.2 Componente de Red 2: Requerimientos de las Aplicaciones de la Empresa.

Las preguntas enunciadas en 3.1.2.2 se responden de la misma forma que en el caso anterior. Para no volver a enunciarlas, en resumen se tiene que la mayoría de las aplicaciones pueden funcionar sin mayores problemas en IPv6, pues las aplicaciones de Microsoft ya han sido actualizadas por la empresa para soportar ambos protocolos. Linux, por su parte también cuenta con un gran soporte a IPv6, por lo que no debería presentar problema alguno. Por otro lado, las aplicaciones nativas de la empresa, son las que probablemente presentarán dificultades en la migración, por lo cual deben ser analizadas en un laboratorio de pruebas de manera de definir si son o no actualizables.

3.2.2.3 Componente de Red 3: Requerimientos del Departamento IT de la Empresa.

Nuevamente nos encontramos con preguntas cuyas respuestas se deducen de la descripción previa de la red de Codelco-Chile. Sin embargo, también hay interrogantes que necesitan un análisis exhaustivo. Las políticas de seguridad y de calidad de servicio de la empresa requieren un enfoque especial y están fuera del alance de este documento.

3.2.2.4 Componente de Red 4: Sistema de Gestión de Red de la Empresa.

El sistema de gestión de red debe ser investigado y probado en laboratorio, y está fuera del alcance de este documento.

3.2.2.5 Componente de Red 5: Ínter operación y Coexistencia de la red de la Empresa

Con respecto al último conjunto de preguntas, se tiene que, los mecanismos de transición a utilizar, será tal como se definió *dual stack*, y a medida que se necesite, se utilizarán técnicas de túnel. Nuevamente las políticas están fuera del alcance del documento.

3.2.3 Requerimientos de la Infraestructura de Red.

Para definir las respuestas de este grupo de preguntas, es necesario un análisis más detallado de lo que este documento pretende realizar. Con respecto a las plataformas que utilizarán IPv6 es bastante obvio, pues en Codelco-Chile sólo se utilizan equipos con un sistema operativo Microsoft (de preferencia Windows XP) y para los dispositivos de red se utilizan equipos Cisco. En la sección 3.4 se realiza un experimento para evaluar la dificultad de conectar estas plataformas con IPv6. Solo existe un punto de acceso a la red que debe ser compatible con IPv6, pues solo existe una conexión hacia Internet la cual se encuentra en casa matriz, y desde ahí se provee de conectividad al resto de las divisiones. Los mecanismos de transición que deben soportar las operaciones de red dependen del desarrollo del proceso de adopción. Si bien se planifica con una arquitectura dual del protocolo IP, los tipos de túneles a realizar dependen del comportamiento de la red y de las restricciones técnicas que posea la misma. Por otro lado, para definir las políticas y procedimientos necesarios para apoyar la conectividad dentro de la empresa, se requiere un estudio posterior el cual se deja propuesto para una futura investigación.

3.3 Análisis del Escenario.

Conociendo el escenario inicial y final, se desea incorporar el nuevo protocolo de red, IPv6, de manera estructurada dentro de la infraestructura de red existente. Esto quiere decir que, el despliegue del protocolo no es inmediatamente a gran escala, pues lo esencial es preparar no solo la red, sino que también a los administradores de red, ingenieros, técnicos, etc, que se encuentren a cargo de ella. Además es posible que no todos los nodos sean capaces de migrar a IPv6 en el corto plazo. Este proceso es posible gracias a la arquitectura Dual IP, pues permite desplegar el nuevo protocolo dentro de la infraestructura de red mientras éste no es utilizado. Es decir, la empresa tiene la capacidad de migrar según sea requerido, sin necesidad de forzar el proceso.

Partiendo de esta base, y tal como se explica en [40], es posible generar una estrategia planteada en etapas que permita la integración de IPv6 en la red. Así, una buena etapa 1, considera el establecimiento de un laboratorio de pruebas, en donde sea posible evaluar plataformas específicas de la empresa, aplicaciones y configuraciones que permitan extender el despliegue hacia el resto de la red empresarial.

Una parte crítica que puede ser solucionada con un despliegue por etapas, corresponde a la selección de la infraestructura de enrutamiento que soporte IPv6. Dependiendo de los equipos con los que se cuenten, de la experiencia ganada en el laboratorio de pruebas y del presupuesto; es posible elegir según las necesidades de cada segmento de red si es necesario desplegar un segmento de red nuevo, IPv6 nativo; o si es posible actualizar la infraestructura para obtener la capacidad Dual IP. Por otro lado, puede suceder que en ciertas subredes no sean factibles ninguna de las dos soluciones, es decir, cuando un segmento de la red (o incluso la *backbone* empresarial) no soporta IPv6 (escenario B de la tabla 3.1). En este caso, es posible utilizar técnicas de túnel explicadas en la sección 2.3.

Para el caso de desplegar una red paralela en la cual el protocolo IPv6 sea el dominante (en el caso que la arquitectura dual stack dentro del segmento de red no sea factible), es posible crear una red VLAN, la cual tiene la ventaja de no necesitar ningún cambio físico en la red y ofrece todas las ventajas ya conocidas de una VLAN para el nuevo ambiente Dual IP. Para mayor información sobre VLAN en IPv6, consultar [41]. La infraestructura paralela debe ser vista sólo como un paso intermedio hacia el despliegue total de la infraestructura Dual IP. Sin embargo, esto permite desplegar todos los otros aspectos de IPv6 (como las direcciones), preparando la red empresarial para el paso unificador en una fecha posterior.

Es importante notar que, todas las preguntas que no han sido respondidas en este documento, pueden encontrar solución tras investigar en el laboratorio de pruebas. Cómo se configurará el DNS, que tipo de configuración de *hosts* se utilizará, cuales serán las políticas de QoS o seguridad, son problemas que la experiencia es capaz de solucionar.

3.4 Plan de Migración para Codelco-Chile.

Tal como se enunció en la sección anterior, para lograr una migración exitosa, es necesario contar con un plan estructurado en etapas que permita desplegar paso a paso la infraestructura Dual IP requerida en la red empresarial. A continuación se describirá el proceso propuesto, describiendo cada etapa dentro del plan de migración.

3.4.1 Etapa 1: Primeros Pasos Hacia la Conectividad.

El primer paso en este plan, consiste en construir un laboratorio de pruebas. Esta instalación permitirá realizar los estudios correspondientes para definir la mejor configuración posible dentro de los requerimientos de la red empresarial. Este laboratorio, puede ser una red pequeña de unos 2 computadores y un *router*, obviamente contando con la infraestructura Dual IP correspondiente. Con este primer paso, se obtiene una conectividad interna IPv6, con la cual se puede aprender a utilizar los diferentes mecanismos de auto configuración que presenta IPv6, y por supuesto probar el desempeño de aplicaciones de red.

En el caso de que cuando este plan sea ejecutado, el proveedor de servicios de Internet de la empresa ofrezca conectividad IPv6, el siguiente paso corresponde a solicitar una dirección IPv6 ruteable de manera global al proveedor correspondiente.

Si aún no existe un proveedor que ofrezca conectividad IPv6 hacia Internet, el paso siguiente corresponde a definir otro segmento de red que pueda ser migrado a Dual IP. Este paso tiene como objetivo ganar experiencia en configuraciones de túneles y direcciones IPv6, pues será necesario definir un plan de direccionamiento dentro de la empresa, para comenzar a conectar diferentes puntos de ella.

Una buena idea para diseñar un plan de direccionamiento para el nuevo protocolo de IP en Codelco-Chile sería utilizar un esquema parecido al explicado en el capítulo 2. Es decir, la idea sería asignar un identificador de subred definido para cada división (o sitio, edificio, etc) de manera ordenada con el fin de relacionar la subred con el lugar geográfico en el que se encuentra. Dado que una dirección IPv6 cuyo prefijo sea de 48 bits (es decir xxxx:xxxx:xxxx:/48) permite utilizar 16 bits para definir subredes, lo que admite un total de $2^{16} = 65536$ subredes, cantidad más que suficiente para Codelco, sin contar además los $2^{64} = 18446744077095516 16$ *hosts* que tolera cada subred. Si se quiere facilitar aún más el direccionamiento, es posible crear una especie de “patente” para cada lugar geográfico, por ejemplo la división Casa Matriz podría ser AAXX, donde XX representa un par de números. Esta “patente” permite asignar un total de 256 subredes sólo en Casa Matriz (pues se tienen 8 valores posibles para cada elemento del par, es decir se tiene que la cantidad de combinaciones posibles es de $2^8 = 256$) y 256 sitios para asignar (Casa Matriz, El Teniente, Andina, etc) cantidad más que suficiente. Luego, el esquema de direccionamiento propuesto se muestra en la figura 3.1. Cabe señalar que con este esquema es posible utilizar auto configuración *stateless*.

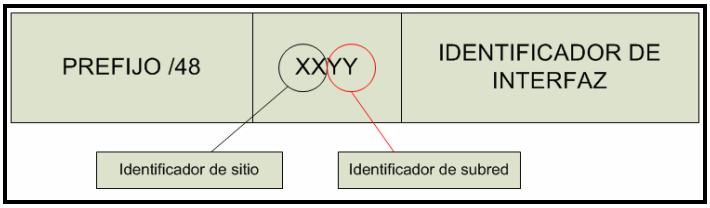

Figura 3.1: Esquema de dirección propuesto

Otro punto a solucionar en el despliegue del laboratorio, corresponde a la situación del DNS. La empresa debe desplegar el servicio DNS de manera tal que sea capaz de utilizar registros IPv6, es decir el formato AAAA (véase [42] para mayor referencia). Es importante también investigar en esta etapa que protocolos de ruteo se utilizarán en la red, pues la empresa puede optar por utilizar protocolos de ruteo externo, especialmente si posee más de un proveedor de servicios. Por consiguiente, es importante también ganar experiencia en este ámbito.

La misión dentro del laboratorio continúa con otro punto crítico: la política de seguridad de la red. Al desplegar IPv6 es importante definir y revisar los diferentes mecanismos utilizados por la empresa. Por ejemplo, es necesario revisar si el *firewall* utilizado es compatible o no con el nuevo protocolo. Además la empresa deberá definir qué tipo de configuración utilizará (por motivos de seguridad o comodidad) debido a la existencia de NAT como parte de la política de seguridad en IPv4. Una buena referencia de como puede ser utilizada IPv6 para entregar la misma seguridad que NAT, es descrita en [43].

3.4.2 Etapa 2: Educar e Informar.

Una vez adquirida la experiencia necesaria para desarrollar las políticas más apropiadas para cumplir con los requerimientos de la red empresarial, la etapa siguiente no es técnica si no informativa. Es importante educar a los técnicos y profesionales que trabajan diariamente en el mantenimiento de los sistemas de comunicaciones. Realizar capacitaciones, charlas informativas y talleres; permite infundir los conocimientos necesarios en las personas indicadas para afrontar mejor los cambios en sus labores. Además este paso da la posibilidad de integrar más gente en el equipo de trabajo y ubicarla en distintos puntos geográficos de manera de, por ejemplo, realizar túneles entre divisiones.

Además de educar, es importante informar. Comunicar al resto de la empresa los cambios que se están llevando a cabo, por qué es necesario realizarlos y avisar sobre la eventualidad de posibles problemas durante el proceso, es también importante. La comunicación con el resto de los usuarios permite además involucrarlos en el proceso de migración, hacerlos sentir partícipes en él, comprendiendo la importancia de éste.

3.4.3 Etapa 3: Expandiendo la Conectividad.

Una vez informado el personal de la empresa, educados los profesionales encargados de los sistemas y comprendida ya la labor que se esta realizando, es posible ahora replicar las islas IPv6 creadas en la etapa inicial para expandir la conectividad. Teniendo ahora a más gente involucrada es factible comenzar a trabajar de forma paralela en los distintos puntos de la empresa. Ahora es cuando se puede actualizar, cambiar o crear las redes necesarias, configurar los túneles requeridos y realizar las últimas pruebas pertinentes que permitan llegar al escenario final. Para un mejor control del tráfico de red y para monitorear mejor el funcionamiento de la misma, se recomienda conectar todos las islas hacia el laboratorio y no conectarlas entre ellas (aunque podría hacerse si se observa que existe mucho tráfico desde una isla hacia la otra) de manera de crear un “PIT” (punto de interconexión de tráfico) La figura 3.2 muestra el esquema mencionado.

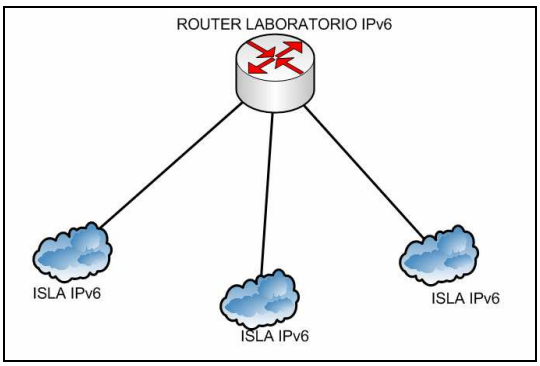

Figura 3.2: PIT: Punto de Interconexión de Tráfico.

3.4.4 Etapa 4: El Término de la adopción.

Una vez completados los puntos anteriores, es posible hablar de una adopción del protocolo IPv6 satisfactoria. Al llegar a esta etapa, se puede suponer que la mayoría de los segmentos de la red cuentan ya con una arquitectura de doble pila, quedando sólo los remanentes. Puede suceder que los puntos que aún no posean conectividad IPv6 no puedan ser migrados como parte de los requerimientos del sistema, o por otro tipo de problemas técnicos. Sin embargo al llegar a esta etapa, los puntos mencionados deberían ser casos aislados.

Un paso a dar importante en esta etapa es evaluar cómo se ha ido desempeñando el sistema y si es necesario realizar algún cambio en las políticas diseñadas. A pesar de que el despliegue sea ya masivo dentro de la empresa y que las pruebas ya realizadas hayan dado todas las pautas a seguir, todavía es posible enfrentar problemas del sistema, debido al gran número de clientes y a la creciente (pero quizás aún incompleta) experiencia en el tema.

3.4.5 Últimos Comentarios.

Es necesario comentar a esta altura que, durante todo el proceso de migración es importante tener en mente los siguientes puntos. Es necesario mantener en todo momento un monitoreo constante de la red, de los procedimientos utilizados y realizar las mantenciones correspondientes. Es de suma importancia detectar a tiempo cualquier posible problema que pueda generar un cambio en las estrategias señaladas y afectar las políticas generadas durante el transcurso de la migración. Mantener una vigilancia constante en éstos puntos, permite encausar de manera más eficiente la transición de protocolos, y realizar los cambios necesarios en los momentos más oportunos.

No está demás decir también que, a partir del momento en el que se decida realizar dicho proceso, las políticas de adquisición de equipos nuevos para la red empresarial, debe estar orientada a satisfacer la capacidad de manejar el nuevo protocolo de red. Muchos de los componentes de red que se encuentran en el mercado ya son capaces de manejar paquetes IPv6, por lo cual es posible prepararse desde ya para la migración.

Finalmente, es importante tomar la decisión lo antes posible. Un comienzo anticipado de la migración, permite efectuar todos los cambios y estudios necesarios de manera tranquila y mesurada. Es posible realizar todas las pruebas necesarias y verificar las políticas generadas, pudiendo componer los errores y modificarlas cuantas veces sea necesario. En cambio, si la decisión de migrar se toma demasiado tarde, es muy probable que al apurar todo el proceso los errores cometidos en el camino sean más graves y más difíciles de componer que en el caso anterior. Es por esto que, la decisión tomada en el momento adecuado permite minimizar los costos de la transición y maximizar la experiencia del equipo de personas que participan en este procedimiento.

3.5 El comienzo de un Laboratorio de Pruebas.

Para comenzar la migración a IPv6 dentro de la empresa, el primer paso a seguir, es montar un laboratorio de pruebas donde sea posible ganar experiencia en el manejo del nuevo protocolo. Así, en esta sección, se pretende armar una pequeña red dentro de Codelco Chile, la cual cuente con la arquitectura Dual IP.

3.5.1 Equipos Disponibles en el Laboratorio.

Los equipos que Codelco-Chile tiene a disposición para montar el laboratorio de pruebas IPv6 son los siguientes:

Dispositivo	Marca	Modelo	Cantidad
Switch	**Cisco**	**WS-C2960-24TTL-L**	**6**
Switch	**Cisco**	**WS-C2960G-24TC**	**1**
Switch	**Cisco**	**WS-C2960G-24-EI**	**1**
Switch	**Cisco**	**WS-CE500-24PC**	**2**
Router	**Cisco**	**CISCO 2821**	**1**
Router	**Cisco**	**CISCO 2811**	**2**
Router	**Cisco**	**CISCO 2621XM**	**1**
Router	**Cisco**	**CISCO 851**	**8**

Tabla 3.2: Dispositivos Disponibles en Laboratorio.

La tabla 3.2 muestra los dispositivos disponibles, especificando la marca, el modelo y la cantidad presente en el laboratorio. Para saber si es posible o no utilizar estos equipos en la construcción de dicho laboratorio, es necesario analizarlos en función de la conectividad IPv6 requerida para este fin.

3.5.2 Análisis de la Compatibilidad de los Equipos con IPv6.

Para conocer la compatibilidad de los instrumentos de red mostrados en la sección anterior, lo primero es separar los equipos en dos categorías obvias: *Switchs* y *Routers*. Con respecto a los primeros, solo se debe recordar que los paquetes IPv6 son transparentes a los *switchs* capa 2 pues éstos no examinan la información de los paquetes correspondiente a la capa 3 antes de reenviar la información. Luego los *hosts* IPv6 pueden ser conectados a cualquier *switch* capa 2. Para conocer la compatibilidad del segundo grupo, el camino a seguir es revisar la documentación entregada por el fabricante, que en este caso corresponde a Cisco. Según la documentación [44], para saber si la interfaz es compatible o no con IPv6, es necesario revisar el sistema operativo de la misma, es decir la versión de la Cisco IOS instalada. Las características IPv6 que soporte el dispositivo están limitadas por la IOS instalada y [44] provee una lista extensa de las distintas características IPv6 en los distintos sistemas operativos. Entonces, ahora lo importantes es conocer que sistema operativo poseen los *routers* y luego comparar esta información con la entregada en [44]. Según la información entregada por Codelco las interfaces poseen la IOS que se muestra en la tabla 3.3.

Router	Versión IOS Instalada
Cisco 2821	12.4(10) Advanced Security
Cisco 2811	12.4(10) Advanced Security
Cisco 851	12.4(4)T6 Advanced security
Cisco 2621XM	12.3(15a) IP Base

Tabla 3.3: IOS instaladas en los Routers.

Según [44], la conectividad IPv6 es soportada en las Cisco IOS softwares 12.0S; 12.*x*T; 12.2S; 12.2SB; 12.2SE; 12.2SG; 12.2SR; 12.2SX; XE; 12.3; y 12.4, partiendo del la versión 12.0(22)S; 12.2(2)T; 12.2(14)S; 12.2(28)SB; 12.2(25)SEA; 12.2(33)SRA; 12.2(17a)SX1; Cisco IOS XE Release 2.1; 12.3; y 12.4, respectivamente. Es decir, todas las versiones instaladas son compatibles con IPv6, por lo cual es posible montar la red IPv6 sin mayores complicaciones.

3.5.3 Primer intento de Conectividad.

Después de examinar la compatibilidad es posible proceder a construir una pequeña red IPv6. Debido a que se quiere realizar de la forma más simple posible (para demostrar que los requerimientos para poseer conectividad IPv6 no son muy elevados) se utilizará el *router* más simple de los 4 modelos mostrados, es decir se utilizará el Cisco 851. Una vez en el laboratorio, y contando con la ayuda de Michael Duque alumno en práctica de Inacap, se dispusieron los elementos necesarios y se procedió a iniciar la configuración del *router*. Cuando se inició el proceso apareció el primer obstáculo: La IOS instalada no era compatible con IPv6. Este problema, que supuestamente debido al trabajo previo no debió ocurrir, se debe a que la información consultada no fue interpretada de la forma correcta. Al consultar la documentación de Cisco no se consideraron dos cosas importantes que por la falta de experiencia en el manejo de estos dispositivos no se estimaron. El primer punto no considerado fue que para cada *release* del *software* existen varias versiones (por ejemplo *advance security , advance enterprise, etc*) y no todas cuentan con el soporte IPv6. El segundo punto corresponde a las características del hardware, pues para que las características IPv6 funcionen en el dispositivo, éste debe contar con 256 mb DRAM y 64 mb de memoria flash. Lamentablemente, el *router* Cisco 851 no cumple con el requerimiento de memoria, por lo que se descarta en el proceso.

Siguiendo entonces en el camino hacia la red IPv6, se revisaron nuevamente los sistemas operativos de cada dispositivo utilizando la ayuda de [45] y se concluyó que ninguno de las IOS presentadas en la tabla 3.3 eran compatibles con IPv6. Como descargar otro *software* desde Cisco requiere una cuenta autorizada y para ello es necesario pagar por ella, se decidió intentar configurar un *router* IPv6 en un computador con Linux. Se configuró entonces este equipo con la ayuda de [46] y se logró que los *hosts* se autoconfiguraran, pero no se logro la conectividad deseada. Además esta solución no fue del agrado de Codelco, pues se acostumbra a utilizar equipos Cisco

para la construcción de redes por motivos de seguridad. Luego no se investigó más en este ámbito y se prosiguió la investigación en la plataforma que provee Cisco.

3.5.4 Segundo intento de Conectividad.

A pesar de que en Codelco-Chile se descartó la solución de utilizar un computador con Linux como *router* IPv6, se investigó paralelamente el por qué del no funcionamiento del equipo como era esperado y se llegó a la conclusión de que es necesario configurar y compilar el *kernel* con las características necesarias habilitadas para lograr el objetivo planteado. Este trabajo no se continúa en Codelco debido a que fue descartado como solución óptima (para la empresa).

Continuando entonces con la investigación en la plataforma Cisco hacia la conectividad IPv6, el siguiente paso fue investigar cuales equipos cumplen con los requisitos de memoria y poseen un sistema operativo compatible con IPv6. Siguiendo entonces la línea de utilizar los equipos más sencillos, el siguiente equipo a analizar fue el *router* Cisco 2811, el cual se encuentra disponible en el laboratorio perteneciente a Codelco-Chile. Las especificaciones técnicas de este dispositivo se muestran en la tabla 3.4 [47].

Cisco 2800 Series	Cisco 2801	Cisco 2811	Cisco 2821	Cisco 2851
DRAM	Default 128 mb Max. 384 mb	Default 256 mb Max. 768 mb	Default 256 mb Max. 1 gb	
Compact Flash	Default 64 mb Max. 128 mb	Default 64 mb Max. 256 mb	Default 64 mb Max. 256 mb	

Tabla 3.4: Detalles de Memoria Dispositivos Cisco 2800 Series

Entonces, según la tabla 3.4 el *router* Cisco 2811 cuenta con la cantidad necesaria de memoria DRAM y Flash para soportar un sistema operativo IOS compatible con IPv6. Una vez comprobado el requisito de memoria, se procede a buscar el IOS adecuado para el *router*. Utilizando nuevamente [45] y colocando los parámetros necesarios (plataforma 2811, *feature name* IPv6) se llegó a la conclusión de que el IOS necesario correspondía a 12.4(11)XJ *advance enterprise* , el cual cuenta con las características IPv6 necesarias para el experimento.

Una vez seleccionado el sistema operativo a instalar en la interfaz de red se solicitó la descarga desde el sitio Web de Cisco pues se necesita una cuenta para acceder a ella. Después de esperar unas horas se recibió otra imagen (IOS 12.4(19) *advance enterprise*) que a pesar de no ser la solicitada, se corroboró en el sitio Web de Cisco

que efectivamente ésta era compatible con IPv6, por lo que se procedió al siguiente paso del experimento: la configuración de la red.

3.5.5 Configuración de la red IPv6.

Ya con la seguridad de que el *router* posee la IOS correcta, el primer paso hacia la conectividad es configurar este dispositivo, pues tal como se comentó en el capítulo 2 de este documento la configuración en los *hosts* es mínima o nula. Los pasos seguidos para el correcto funcionamiento del equipo se describen a continuación:

- Primer paso: Instalar la IOS correcta: Para esto, se utilizó un servidor tftp para que el dispositivo descargase la imagen desde un computador y la instalase correctamente. Este procedimiento se realizó siguiendo los pasos descritos en [48].

- Segundo paso: Establecer Conexión con el *Router*: Para configurar el dispositivo es necesario conectar un computador con éste a través de un cable especial (serial-rj45) que permite comunicar el puerto serial del computador con el puerto de consola del *router*. Una vez instalado el cable se utiliza algún programa que permita enviar paquetes a través del puerto serial de manera de lograr introducir los comandos correspondientes a la configuración. Para lograr este objetivo se contó con la ayuda del estudiante en práctica mencionado anteriormente. Una buena referencia descriptiva para este segundo paso es [49], donde los primeros puntos corresponde a lo descrito acá.

- Tercer paso: Configuración del *Router*: Una vez establecida la conexión entre el computador y el router a través del puerto de consola, el paso siguiente es configurar el dispositivo para que posea conectividad IPv6. Para la disposición correcta de la interfaz, se utilizó la guía provista por Cisco [50]. El *router* se configuró con un prefijo unicast de 64 bits, el cual era 2001:0db8:0:1/64 y se utilizó la auto configuración *stateless*, descrita en el capítulo anterior. La figura 3.1 muestra la correcta configuración del dispositivo.

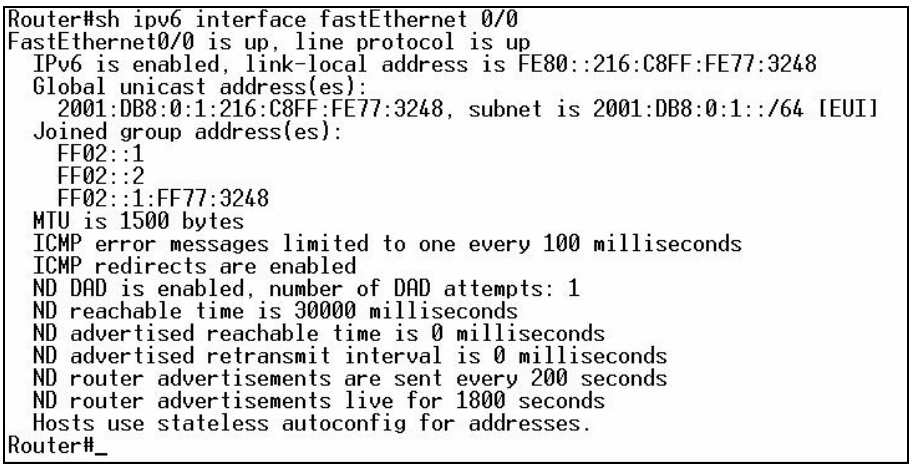

Figura 3.3 Correcta Configuración del *router* IPv6

- Cuarto paso: El primer *hosts*: Para comprobar que el *router* se encontrase correctamente instalado, se conectó directamente un computador y se comprobó la conectividad mediante un ping desde el *router* y hacia el computador. La figura 3.2 muestra el resultado de esta prueba. Cabe señalar que el *host* corresponde a un computador utilizando Windows XP.

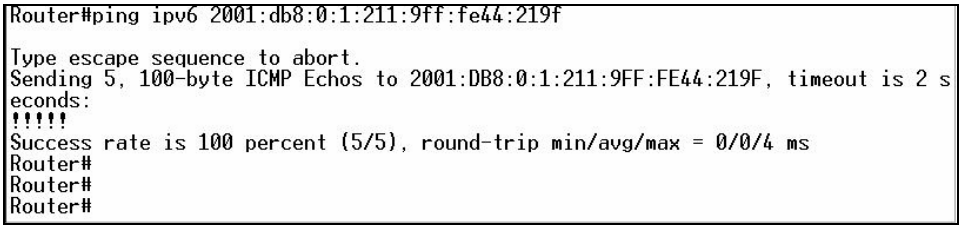

Figura 3.4 Ping desde el *router* al primer *host*.

- Quinto paso: Disposición del resto de los *hosts*: Una vez comprobada la correcta configuración del *router*, se instalaron 3 *hosts* más para poseer una red más completa. Puesto que el Cisco 2811 sólo posee dos puertos de entrada, se utilizó un *switch* Cisco *Catalyst* 2960 para lograr la conectividad entre los computadores. De esta forma, la arquitectura de la red es la mostrada en la figura 3.3 en donde se observa que se utilizaron 4 clientes, dos con Windows XP los cuales son propiedad de Codelco-Chile y dos *Laptops* con Windows Vista que pertenecen al estudiante en práctica y al memorista.

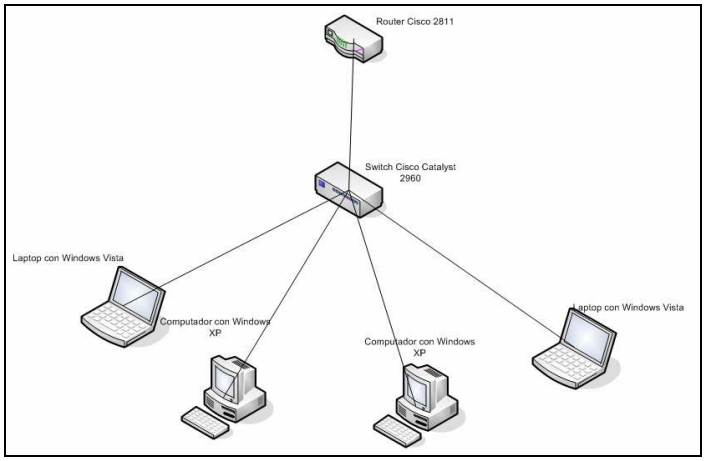

Figura 3.5 Arquitectura de la red experimental.

Una vista real de la red instalada se muestra en la figura 3.4. En ésta se observan los distintos dispositivos reales utilizados para esta red experimental.

Figura 3.6 Foto de la red experimental.

Para comprobar el correcto funcionamiento de la red se realizaron pruebas de ping desde un *host* a otro, siendo un ejemplo de esto la figura 3.5

```
C:\Users\Orlando>ping 2001:db8:0:1:211:9ff:fe44:219f

Haciendo ping a 2001:db8:0:1:211:9ff:fe44:219f desde 2001:db8:0:1:9c27:7201:3099
:67ed con 32 bytes de datos:

Respuesta desde 2001:db8:0:1:211:9ff:fe44:219f: tiempo<1m
Respuesta desde 2001:db8:0:1:211:9ff:fe44:219f: tiempo<1m
Respuesta desde 2001:db8:0:1:211:9ff:fe44:219f: tiempo<1m
Respuesta desde 2001:db8:0:1:211:9ff:fe44:219f: tiempo<1m

Estadísticas de ping para 2001:db8:0:1:211:9ff:fe44:219f:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 0ms, Máximo = 0ms, Media = 0ms

C:\Users\Orlando>
```

Figura 3.7: Ping desde Laptop con Windows Vista a computador con Windows XP

- Sexto paso: Configuración de ambos protocolos: Nuevamente siguiendo los pasos descritos en [50] se configuró la red de manera tal de poseer conectividad tanto con IPv4 como con IPv6. A cada uno de los equipos se le asignó una dirección IPv4 tal como se configura cualquier red que utilice el protocolo actual y se procedió a realizar las pruebas correspondientes.

- Séptimo paso: Pruebas en la red: Una vez instalada la arquitectura Dual IP se procedió a realizar pruebas de conectividad en ambos protocolos. A cada *host* se le asignó un nombre para su fácil identificación, el cual es mostrado en las figuras 3.6 a 3.9. Los resultados de las pruebas se muestran desde la figura 3.10 a la figura 3.15.

Figura 3.8: *Host* Vista 1.

Figura 3.9: *Host* Vista 2.

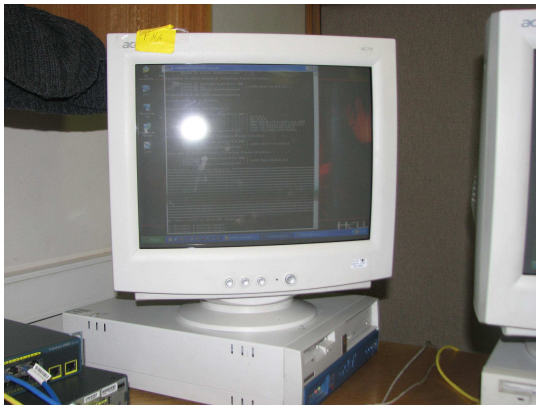

Figura 3.10: *Host* XP 1.

Figura 3.11: *Host* XP 2.

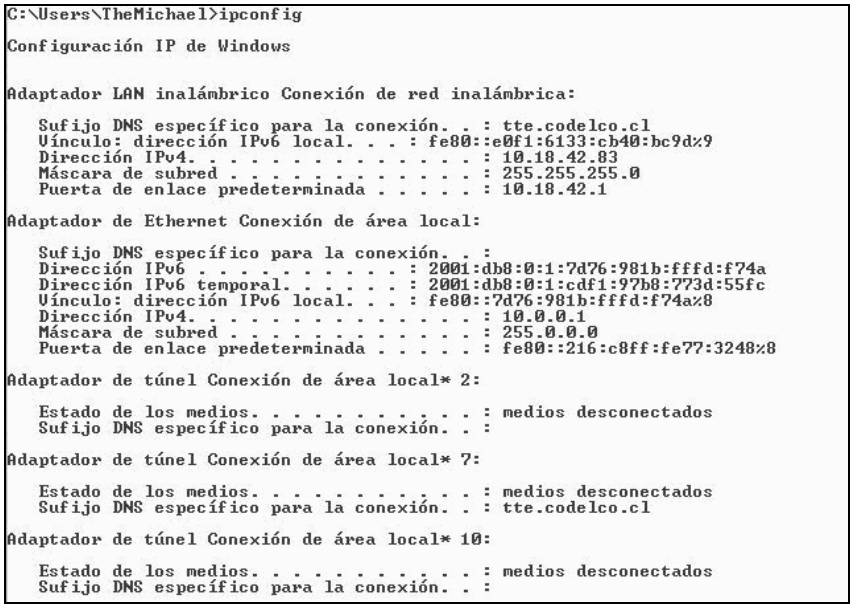

Figura 3.12: Configuración IP del *host* Vista 2.

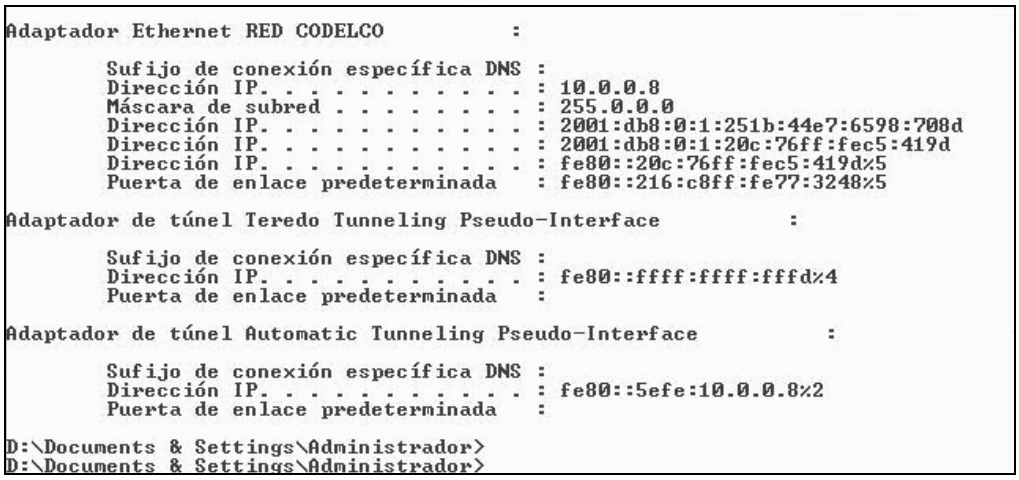

Figura 3.13: Configuración IP del *host* XP 2.

```
C:\Users\TheMichael>ping 2001:db8:0:1:216:c8ff:fe77:3248

Haciendo ping a 2001:db8:0:1:216:c8ff:fe77:3248 desde 2001:db8:0:1:cdf1:97b8:773
d:55fc con 32 bytes de datos:
Respuesta desde 2001:db8:0:1:216:c8ff:fe77:3248: tiempo=2ms
Respuesta desde 2001:db8:0:1:216:c8ff:fe77:3248: tiempo<1m
Respuesta desde 2001:db8:0:1:216:c8ff:fe77:3248: tiempo<1m
Respuesta desde 2001:db8:0:1:216:c8ff:fe77:3248: tiempo<1m

Estadísticas de ping para 2001:db8:0:1:216:c8ff:fe77:3248:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 0ms, Máximo = 2ms, Media = 0ms

C:\Users\TheMichael>
```

Figura 3.14: Ping IPv6 desde *host* Vista 2 a *router.*

```
C:\Users\Orlando>ping 10.0.0.2

Haciendo ping a 10.0.0.2 con 32 bytes de datos:

Respuesta desde 10.0.0.2: bytes=32 tiempo<1m TTL=128
Respuesta desde 10.0.0.2: bytes=32 tiempo<1m TTL=128
Respuesta desde 10.0.0.2: bytes=32 tiempo<1m TTL=128
Respuesta desde 10.0.0.2: bytes=32 tiempo<1m TTL=128

Estadísticas de ping para 10.0.0.2:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 0ms, Máximo = 0ms, Media = 0ms

C:\Users\Orlando>ping 2001:db8:0:1:211:9ff:fe44:219f

Haciendo ping a 2001:db8:0:1:211:9ff:fe44:219f desde 2001:db8:0:1:9c27:7201:3099
:67ed con 32 bytes de datos:

Respuesta desde 2001:db8:0:1:211:9ff:fe44:219f: tiempo<1m
Respuesta desde 2001:db8:0:1:211:9ff:fe44:219f: tiempo<1m
Respuesta desde 2001:db8:0:1:211:9ff:fe44:219f: tiempo<1m
Respuesta desde 2001:db8:0:1:211:9ff:fe44:219f: tiempo<1m

Estadísticas de ping para 2001:db8:0:1:211:9ff:fe44:219f:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 0ms, Máximo = 0ms, Media = 0ms

C:\Users\Orlando>
```

Figura 3.15: Ping IPv4 e IPv6 desde *host* Vista 1 a *host* XP 1.

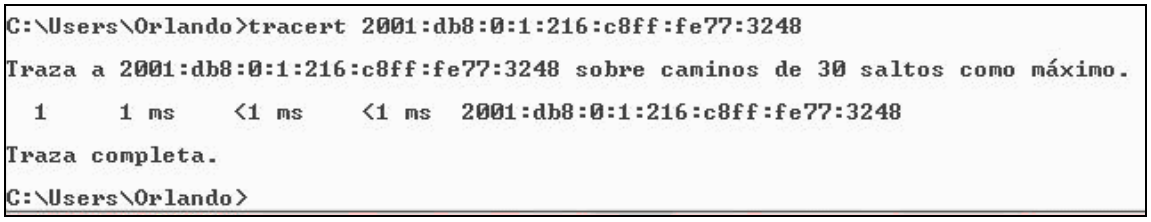

Figura 3.16: *Traceroute* IPv6 desde *host* Vista 1 a *router*.

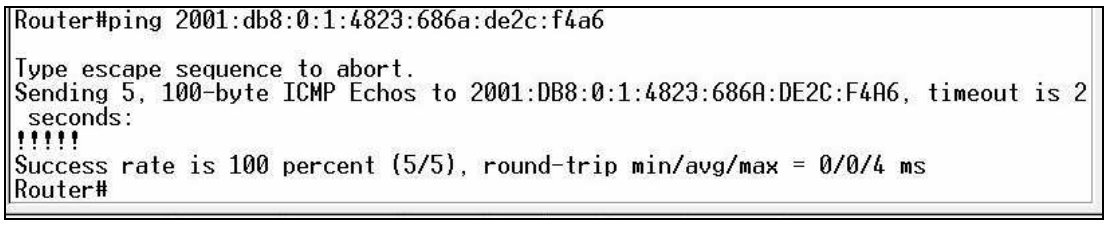

Figura 3.17: Ping IPv6 desde *router* a *host* Vista 2

Una vez comprobada la conectividad en la arquitectura Dual IP de la red experimental se concluye la fase de experimentación. Posibles pruebas futuras son posibles con esta red, tal como realizar un túnel hacia otra división ubicada en un lugar geográficamente alejado o también un túnel hacia un 6to4 *relay* de manera tal de navegar por Internet a través de IPv6. Sin embargo estas pruebas no son posibles de realizar por el momento, pues para lograr el objetivo se necesita, en el primer caso acceso a una dirección IPv4 pública, la cual por motivos de seguridad de la empresa es muy difícil de conseguir; y en el segundo caso, debido a la dificultad de replicar este laboratorio en otra división, pues esto implica conseguir los permisos correspondientes lo que conlleva más tiempo de lo que se posee para finalizar este documento. Por este motivo estos experimentos quedan propuestos para continuar con la investigación.

Capitulo IV. Programación del Proyecto de Adopción del Protocolo IPv6 en la red corporativa de Codelco-Chile.

Para contrastar el plan propuesto en el capítulo anterior, y conocer la experiencia de otra empresa que se aventuró en la experimentación con el nuevo protocolo de Internet, a continuación se describirá la experiencia de NIC Chile en este ámbito. Luego, una vez conocido el estudio de NIC Chile en la materia, se utilizará el conocimiento para pulir la estrategia de adopción propuesta.

4.1 NIC Chile e IPv6.

La razón principal por la que se escogió esta institución para comparar el plan desarrollado en este documento, se debe a que NIC Chile utiliza los recursos entregados por Internet para desarrollar su negocio, es una empresa que posee una gran cantidad de clientes, por lo que tiene un fuerte impacto en la comunidad. Además, cabe señalar que el autor de esta memoria efectuó su práctica profesional en dicha organización por lo que el acceso a la información no tuvo mayores complicaciones.

4.1.1 Introducción.

NIC [51] es una sigla que significa *"Network Information Center"*, o *Centro de Información de Redes*, nombre histórico usado en todo el mundo para definir la organización encargada de administrar los nombres de dominio en alguna categoría en Internet. La organización mundial administradora de los nombres de dominio en Internet, IANA (Internet Assigned Number Authority), en el año 1986, delegó el ejercicio de esa función en el Departamento de Ciencias de la Computación de la Universidad de Chile, con el objeto de permitir la creación de nombres de dominio correspondientes a nuestro país, originándose el sufijo "**.cl**", momento en el que se creó NIC Chile.

De esta forma, NIC Chile es el encargado de administrar los nombres de dominio de Chile. Un nombre de dominio es un recurso que permite implementar a través de Internet, ciertos servicios como una red de correo electrónico, una página Web, transferencia de archivos (FTP), comercio electrónico, etc. Cuando una persona inscribe un dominio en NIC Chile, adquiere la posibilidad técnica de asociar el nombre de dominio con un computador específico que él escoja [51].

Actualmente NIC Chile administra más de 215 mil dominios (al 30 de junio del 2008 [52]) por lo que el rol que juega en el desarrollo de las tecnologías de información en el país es bastante grande. Así, una de las obligaciones de esta empresa es liderar el avance tecnológico en Chile, labor que lleva a cabo en forma constante. Luego,

experimentar en el proceso de migración hacia el protocolo IPv6 es una tarea que no puede dejar de lado, preparando el camino para que Chile pueda utilizar libremente los nombres de dominio en esta nueva Internet. Junto con el liderazgo asumido por NIC Chile en el desarrollo tecnológico del país, LACNIC [53] ha estado empujando el desarrollo de esta nueva tecnología en Latinoamérica, desafío que fue aceptado una vez que se consideró que ésta tecnología estaba lo suficientemente madura como para ser utilizada.

4.1.2 Antecedentes Previos.

Para conocer en que condiciones se desarrolló esta migración, lo primero es conocer como está estructurada la red interna de NIC Chile, de manera de tener un esquema que ayude a entender los cambios realizados e identificar físicamente en que lugar se realizaron. De esta forma, en la figura 4.1, se presenta la topología de la red de NIC Chile, la cual es la materia prima para el proceso de adopción de esta nueva tecnología.

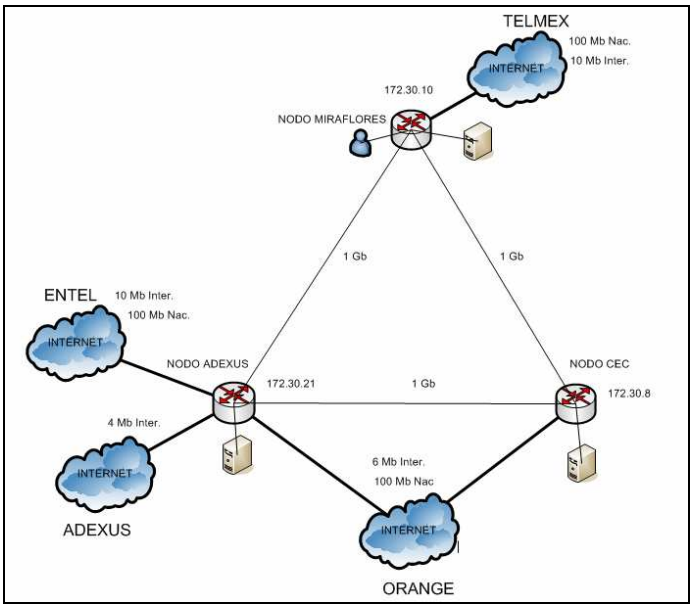

Figura 4.1: Topología de la red de NIC Chile.

Tal como se observa en la figura 1, la red de NIC Chile cuenta con tres nodos principales cada uno en un lugar geográficamente distinto y unidos por un enlace de 1 Gb/s de capacidad. Cada nodo está formado por un *router* (más uno de respaldo) que maneja el tráfico de red utilizando el protocolo de enrutamiento BGP contando además con *switches* capa 2 que ayudan a distribuir el tráfico de red en los distintos equipos (por simplicidad de la figura éstos no se muestran en ella). Según la función que cumpla el nodo, serán los equipos que se encuentran unidos a él, por ejemplo en el caso del

nodo Miraflores, en él se encuentran conectados el personal de la empresa, desde el personal técnico hasta el administrativo, además de los servidores necesarios para realizar la labor encomendada. En el caso de los demás nodos (Adexus y CEC) sólo poseen servidores, pues no existe personal que trabaje físicamente en esos lugares. Por otro lado, los nodos cuentan con conexión a Internet suministrada por las compañías mostradas en la tabla 4.1, cuyo enrutamiento está a cargo del protocolo BGP tal como se enunció anteriormente.

Nodo	ISP	Capacidad Enlace Nacional	Capacidad Enlace Internacional	Dirección IP
CEC	Orange	100 Mb/s	6 Mb/s	172.30.8
Adexus	ENTEL	100 Mb/s	10 Mb/s	172.30.21
	Adexus	0 Mb/s	4 Mb/s	
	Orange	100 Mb/s	6 Mb/s	
Miraflores	Telmex	100 Mb/s	10 Mb/s	172.30.10

Tabla 4.1: Capacidad de ISP de cada nodo y dirección IP.

4.1.3 Adopción de IPv6 en la red de NIC Chile.

El 29 de agosto de 2005 se realizó el primer IPv6 Tour en Santiago [54], organizado por la Subsecretaria de Telecomunicaciones de Chile, LACNIC, la Universidad de Chile y NIC Chile, en donde se discutieron temas relevantes a este nuevo protocolo, en particular el estado de Latinoamérica en el proceso de adopción de esta nueva tecnología. En esta oportunidad fue cuando partió el interés de comenzar a investigar este tema, lo que se tradujo en un estudio financiado por NIC-Chile del estado del arte del protocolo a nivel mundial. Por otro lado, durante el 2004, Netglobalis empresa en la que NIC Chile dispone uno de sus servidores secundarios, obtuvo un enlace IPv6 nativo hacia Internet y tras un acuerdo informal que permitiera utilizar dicha conexión se comenzó el estudio en la materia, comenzando con el estudio de túneles y otras funcionalidades IPv6.

Dentro de la red institucional, el primer paso para comenzar el estudio del protocolo fue pedir la asignación de una dirección IPv6 a LACNIC la cual se entregó el 2006 (2001:1398::/32). Luego, se probó la conectividad utilizando los equipos internos de la empresa, configurándolos con IPv6 y realizando pruebas de ping, comunicación vía Telnet, etc. Las direcciones asignadas a los equipos en esa oportunidad fueron estáticas, es decir no se utilizó ningún mecanismo de auto configuración y se utilizaron las estaciones de voluntarios que permitieron el uso de ellas para la realización de estas pruebas. Una vez completada esta tarea, se adoptó el protocolo en la red con una arquitectura dual stack formándose así una isla IPv6 (es decir, aislados de Internet).

Durante la organización del segundo IPv6 Tour a realizarse en Santiago de Chile [55], NIC Chile se propuso ofrecer a los asistentes conectividad a través de este nuevo protocolo. Para lograr dicho objetivo, se conectó el Salón Gorbea, ubicado en la Facultad de Ciencias Físicas y Matemáticas de la Universidad de Chile, con el nodo CEC de la red a través de una VLAN y se realizó desde allí un túnel hacia el servidor ubicado en Netglobalis, contándose además con una conexión *Wireless* en el lugar del evento. De esta forma cuando se realizó el evento, el 12 de Septiembre del 2007, se realizaron demostraciones del funcionamiento del nuevo protocolo y se abasteció a los asistentes de la conferencia de conectividad IPv6. Se dispuso además un *router* IPv6 de manera de utilizar la auto configuración *stateless* durante el evento, de manera de aprovechar su facilidad de uso para el usuario final. Lamentablemente, la conexión de NetGlobalis hacia IPv6 se fue degradando hasta el punto de tener un 60% de pérdidas en los paquetes por lo cual se optó por bajar ese servicio una vez finalizado el evento.

4.1.4 Condición Actual de Ipv6 en la red de NIC Chile.

Actualmente se cuenta con conectividad interna IPv6 en el nodo Miraflores, pues el enlace externo de IPv6 hacia Internet no esta habilitado. Dada la degradación del enlace proveído por NetGlobalis, NIC Chile comenzó a buscar su propio enlace realizando una licitación pública a principios de Mayo del 2008. Se presentaron 2 proyectos, escogiéndose el de GTD pues ellos contaban con el servicio ya disponible, a diferencia del segundo en el cual se estaba planeando desplegar la red, y se comenzó a discutir el contrato. En el intertanto, NIC Chile conversó con Telmex, Orange, Adexus y otras empresas del sector para negociar algún posible contrato, pero no se logró acuerdo, siendo la más cercana la de Adexus la cual se comprometió a contar con un enlace IPv6 entre agosto y octubre del 2008. De esta forma, se tendrá una salida hacia Internet vía IPv6 en el nodo CEC y otra salida de respaldo en el nodo Adexus.

Por otro lado, se compraron equipos nuevos lo cuales se configurarán para que soporten ambos protocolos, con lo que se logrará que el anillo de NIC-Chile completo soporte IPv6 e IPv4. Una vez se cuente con ambos enlaces, y se complete la adopción del nuevo protocolo en la red completa, NIC Chile comenzará a otorgar los servicios de DNS IPv6, para finalizar con un sitio Web IPv6 de NIC Chile y con el resto de los servicios que otorga la empresa.

Una vez completado el proceso de adopción, NIC-Chile comenzará a recolectar información sobre la cantidad de usuarios que utilizan este servicio como estadística importante del proceso de migración en Chile.

4.1.5 Problemas Durante la Adopción de IPv6.

El gran problema que se enfrentó durante el segundo IPv6 tour (es decir, durante el proceso de conectividad externa IPv6) fue que los servidores raíz (*Root Servers*) no se anunciaban en IPv6. Dado que existían algunos que ofrecían el servicio IPv6, el problema tenía solución y se optó por partir con el servidor cache (en el servidor dispuesto en Adexus) con una zona raíz modificada que los incluyera, con lo que el

problema fue solucionado. Este error producía que todas las consultas a los servidores raíz las contestaba el protocolo IPv4 por lo que no se obtenían las respuestas necesarias para navegar en IPv6. Este problema se encuentra actualmente solucionado a priori, pues ya existen seis servidores raíz con registros AAAA que corresponden a los de IPv6 [21] disponibles para navegar por Internet.

Otra dificultad que apareció en el camino fue la configuración de los *routers* para que soportaran ambos protocolos. Los equipos dispuestos (se utilizan computadores con Linux como dispositivos de enrutamiento) no poseían IPv6 habilitado en todos sus módulos y al habilitar dicho protocolo, se producía un error en el funcionamiento del artefacto pues se restringían algunas funcionalidades de IPv4 (específicamente el *iptable*). Este problema se solucionó recompilando el *kernel* del sistema operativo de manera tal que soportasen ambos protocolos de manera nativa y agregando además las rutas correspondientes al *iptable*.

Otros problemas enfrentados fueron causados directamente por la falta de experiencia en el manejo del protocolo. Uno de ellos fue el direccionamiento, pues existían algunos prejuicios que venían del legado de IPv4. Por ejemplo la dirección xxx.xxx.xxx.0 representa la red en IPv4 y en IPv6 representa al *router*. Otro problema fue el uso de los comandos necesarios para ejecutar las acciones deseadas, pues en algunos casos éstos son iguales a los utilizados en IPv4 y en otros cambian levemente su sintaxis. Estos errores de inexperiencia se solucionaron rápidamente al experimentar internamente con el protocolo.

4.1.6 Recursos Utilizados para la Adopción de IPv6.

Para realizar este proceso, dos personas altamente calificadas estuvieron a cargo de la adopción del protocolo en la red. Sin dejar de lado sus otras obligaciones, durante una semana lograron realizar exitosamente la adopción del protocolo de manera de formar la isla descrita en los párrafos anteriores. Según la experiencia relatada por ellos, los equipos de red, servidores y de usuarios no presentaron problemas más que los descritos en la sección anterior.

El costo asociado a este proceso, se radica básicamente en la conexión externa IPv6. Es necesario contar con un proveedor de servicios que otorgue conectividad IPv6, pues de otro modo las conexiones se hacen más lentas si el protocolo se encuentre habilitado, ya que se espera obtener un *timeout* en el enlace antes de intentar la conexión a través de IPv4. Esto quiere decir que el navegador de Internet espera agotar el tiempo de respuesta antes de utilizar IPv4.

4.1.7 Conclusiones.

Durante el proceso de adopción del protocolo IPv6 en la red de NIC-Chile, no hubo estrategia definida. Para realizar esta tarea, se realizaron las conexiones de manera

experimental y una vez que se avanzaba en ello, se continuó hacia la conectividad externa. Los recursos utilizados en el desarrollo de este proyecto fueron principalmente las horas hombre dedicadas a él, pues para la conexión externa no se necesitó más que un acuerdo informal, por lo que se asumirá el costo de un enlace en un futuro no muy lejano. El principal avance se obtuvo durante el segundo IPv6 Tour realizado en Chile, pues en ese instante se instaló una red IPv6 como tal, aprovechando todos los recursos suministrados por el nuevo protocolo. Actualmente, NIC-Chile se encuentra todavía en proceso de adopción del protocolo, aunque se cuenta ya con un plan de trabajo a futuro (se tienen claras las metas a cumplir y la forma de llegar a ellas) y se espera que esta evolución concluya en el corto plazo.

4.2 Comparación entre la experiencia de NIC-Chile y la estrategia para Codelco-Chile.

Para validar la estrategia propuesta en este documento y afinar algunos detalles de la misma, se presentó en la sección anterior la experiencia en la adopción de IPv6 de NIC-Chile. De esta información se puede deducir sin mayores complicaciones que el proceso llevado fue bastante desordenado. Tanto así que todavía se encuentra en proceso en algunos servidores y servicios. Es por esto importante la presencia de un plan detallado como el que se presenta en este documento, donde se resaltan los puntos importantes a tener en cuenta en una tarea como ésta.

A pesar del desorden descrito es posible distinguir (aunque de manera desordenada) las mismas etapas propuestas. Todo partió experimentando con el protocolo en los computadores de los mismos usuarios de la institución, asignándoles una dirección IPv6 entregada por LACNIC y realizando pruebas para conocer este protocolo. Este paso se identifica claramente con el laboratorio de pruebas propuesto. Luego, NIC-Chile se preocupó de habilitar IPv6 en la red interna para ofrecer conectividad en el segundo IPv6 tour realizado en Chile. Situación que mezcla las etapas 2 y 3 propuestas, pues en la primera se propone difundir el proyecto a nivel local (empresa) y nacional, y en la segunda conectar otros segmentos de red al laboratorio para expandir la conectividad IPv6 en la empresa. La cuarta etapa propuesta aún no es llevada a cabo en NIC-Chile, pues se encuentran en negociación con empresas que provean conectividad IPv6 nativa hacia Internet antes de completar la habilitación del protocolo en el resto de los equipos y servicios que entrega la institución. De esta forma, se observa que el planteamiento propuesto en este documento, se presenta como una alternativa factible para adoptar IPv6 en cualquier empresa, en particular en Codelco-Chile.

Además de realizar la comparación entre las estrategias, otro punto importante a destacar es la utilización de recursos y tiempos de manera de pulir el plan propuesto y fijar fechas, plazo y requerimientos de equipos y personal. Luego el primer punto a destacar es el tiempo. En el proceso llevado a cabo por NIC-Chile, desde que se comenzó a investigar el estado del arte del protocolo, hasta encontrar un ISP que sea capaz de brindarles el servicio han pasado cuatro años, tiempo que con la estrategia adecuada hubiese sido considerablemente más corto. Este dato es importante pues

permite fijar un plazo máximo para el desarrollo del proyecto: menos de 4 años. Otro punto importante corresponde a los recursos utilizados. NIC-Chile asignó a dos personas altamente calificadas la labor de habilitar IPv6 en la red institucional, dato que permite fijar también la cantidad de recursos humanos necesarios para llevar a cabo este proyecto. En cuando a la calificación del personal, Codelco-Chile cuenta con profesionales igualmente capacitados, si bien no en el protocolo mismo, si en redes de computadores, cuya experiencia es valiosa en este proyecto.

Un tema que no se ha tocado hasta el momento, pero que es igualmente importante y posee una gran similitud en ambos casos, corresponde a la razón de explorar esta nueva tecnología. Ambas empresas, cada una en su rubro particular, son líderes en tecnología a nivel continental, por lo que tienen la misión de impulsar el avance tecnológico en el país. Esta razón es suficientemente poderosa por si sola para comenzar a investigar el tema. Además al implementar esta nueva herramienta, Codelco-Chile se encontrará liderando el proceso del cambio tecnológico abriendo la posibilidad a nuevos nichos de negocios y oportunidades que podrán cambiar la forma de gestionar la empresa. Es posible que gracias a implementar esta nueva tecnología, Codelco-Chile se encuentre ahora con la posibilidad de asesorar otras empresas de gran envergadura en su proceso de migración, desarrollar nuevas herramientas que faciliten la producción y reduzcan los costos de la misma al integrar equipos nuevos en las labores (por ejemplo celulares, taladros, martillos, etc.). En este mismo ámbito, también es importante mencionar la imagen que proyectará la empresa al difundir este proyecto. Codelco-Chile se encontrará liderando un proceso que tomará fuerza en algunos años más y tendrá la influencia necesaria para dictar los pasos a seguir y condicionar incluso el mercado de las telecomunicaciones a su favor, pues al contar con una red tan grande se encuentra (en tamaño) al mismo nivel que cualquier proveedor de servicios de Chile.

Analizando ahora desde otro punto de vista las razones enunciadas en el párrafo anterior sobre el por qué de la exploración en esta nueva tecnología, se tiene que conforme existe una mayor cantidad de dispositivos móviles que pueden ser conectados a la red y a la vez ser utilizados en el trabajo diario (teléfonos, PDA's (*Personal Digital Assistants*), etc) crece la necesidad de contar con un protocolo capaz de manejar esta movilidad. La interconexión de estos aparatos y la identificación de ellos de manera única y transparente es entregada por IPv6, pues es la manera más elegante y que posee un nivel de administración menos complejo para este fin. Luego el no contar con este protocolo, limita la conectividad de la empresa, restringiendo la cantidad de equipos y servicios utilizables en los procesos de producción, administración, etc.

Por otro lado, existen además aplicaciones que funcionarán de mejor manera utilizando IPv6. Si se piensa por ejemplo en VoIP (voz sobre IP) o la telefonía móvil (en particular los servicios 3GPP ó *3rd Generation Partnership Project*) se tiene un sin fin de posibilidades a desarrollar que sin IPv6 sería imposible. Las aplicaciones multimedia también experimentarán una gran mejora en este ámbito pues la posibilidad de contar con un procesamiento de los flujos de paquetes distinto (en la cabecera de los paquetes) aumentará el rendimiento de estos servicios.

Así, teniendo claro la importancia de este proyecto y la posibilidad de finalizarlo en un corto plazo, se procederá a programar las actividades, teniendo como base la experiencia de NIC Chile.

4.3 Programación del Proyecto IPv6 y Codelco-Chile.

Para ordenar un poco las ideas y presentar este trabajo de una manera más serie y profesional, se presenta una propuesta de programación de este proyecto con miras a un futuro desarrollo quizás no muy lejano. De esta forma, a continuación se detallarán las etapas de la programación de este proyecto, comentando en cada sección las especificaciones mencionadas en los capítulos y secciones anteriores.

4.3.1 Gestación del Proyecto.

El nacimiento del nuevo protocolo de Internet, IPv6, nace principalmente de la necesidad de contar con una mayor cantidad de direcciones para asignar a las diferentes interfaces de red que son utilizadas por un número de usuarios que crece cada día con una mayor rapidez a nivel mundial. De esta forma, el mundo cibernético esta cambiando de manera tal de adoptar este nuevo sistema de manera limpia y sin mayores complicaciones. Es por esto que Codelco-Chile debe comenzar a pensar en unirse a este cambio, que tarde o temprano llegará al país y afectara a los millones de usuarios que cuentan con una conexión a Internet.

Actualmente Codelco-Chile se encuentra en la misma posición que muchas empresas en el Mundo: cuenta con una red desplegada a gran escala, que abastece de conectividad a miles de usuarios que utilizan esta red para realizar sus funciones dentro de la firma y con el fantasma de la migración a la vuelta de la esquina. Es por esto que analizar un proyecto de esta envergadura es de suma importancia, sin importar el tamaño de la empresa y más aún en Codelco-Chile que, como empresa líder en el país debe liderar los procesos de cambios de tecnología.

4.3.2 Generación del Objetivo del Proyecto.

Para definir de mejor manera cual es el norte de este proyecto, se realizará un análisis en donde se aclararán los objetivos y las etapas de este proyecto.

4.3.2.1 Anteproyecto.

Como estudio de prefactibilidad de este proyecto, se tiene que actualmente existen muchos programas, dispositivos y sistemas (descritos en el Capítulo 2 de este

documento) que son compatibles con el protocolo de nueva generación y están listos para ser usados. Algunos de éstos necesitan una pequeña configuración previa (como por ejemplo Windows XP en el cual se necesita ejecutar un comando para habilitar IPv6 en el sistema operativo), y en otros se necesita cambiar la versión del sistema operativo para hacerlo compatible con IPv6 (como es el caso de los *routers* Cisco que fueron utilizados para las pruebas del capítulo 3). Sin embargo, estos cambios a realizar son mínimos en comparación a la inversión de infraestructura con la que se cuenta en Codelco-Chile, por lo que realizar un cambio gradual en la red para adoptar este nuevo protocolo es factible con recursos relativamente bajos.

4.3.2.2 Diseño Conceptual.

Para darle solución a este problema, se cuenta con tres posibles soluciones a desarrollar: un despliegue a gran escala del protocolo en la infraestructura de red con una arquitectura dual del *stack* IP, un despliegue escaso en el la red (con la misma arquitectura del caso anterior) para utilizar ciertas aplicaciones en cierto segmento de red y un despliegue de una red totalmente nueva que cuente con el protocolo de manera nativa. (Sección 3.1.1)

4.3.2.3 Evaluación de Alternativas.

Tal como se discutió en la sección 3.2.1, para definir la mejor solución se evaluaron los recursos disponibles y se privilegió una mínima intervención en la red Corporativa de Codelco-Chile. Así en resumen se tiene que el despliegue total con la arquitectura dual *stack* del protocolo IP es la mejor alternativa, pensando en la futura migración final hacia el protocolo IPv6. Los factores que determinaron desechar las otras soluciones son en el caso del despliegue escaso, que se busca como objetivo final (a largo plazo) una migración total al utilizar por completo IPv6 en la red; y en el caso de construir una red separada, los costos asociados a replicar completamente la red hacen que esta opción sea desechada.

4.3.2.4 Diseño Básico.

El despliegue total en la red de Codelco-Chile con una arquitectura dual del *stack* IP, se llevará a cabo en cuatro etapas descritas en la sección 3.4. La primera etapa consiste en construir un laboratorio IPv6 de manera tal de ganar conocimientos y experticia en este ámbito, realizando a la vez las pruebas correspondientes para desarrollar, diseñar e implementar los puntos críticos que quedaron sin solución en el análisis de este documento.

La segunda etapa corresponde a educar profesionales y técnicos para entregarles las herramientas necesarias de manera que puedan desarrollar sus labores cuando involucren la utilización del nuevo protocolo. Además la idea es involucrar a toda la empresa en este cambio, que conozcan en que consiste la adopción del protocolo y comprendan la importancia de esta labor.

La tercera etapa es continuar la implementación de la arquitectura doble, creando nuevos segmentos de red e integrarlos a la red Ipv6 a través del laboratorio. La cuarta y última etapa corresponde a la adopción total del protocolo y comenzar con la

evaluación del desempeño y aplicar posibles mejoras a la infraestructura IPv6 de la red.

4.3.2.5 Diseño Detallado.

Para la construcción del laboratorio IPv6 planteado en este documento, se llevarán a cabo tres etapas que se describirán a continuación. Lo primero es armar la red con la arquitectura propuesta, para ello en la sección 3.5 se describen los pasos para construir dicha red utilizando un *router* Cisco 2811 disponible en el laboratorio de redes de Codelco-Chile, en conjunto con computadores estándar de propiedad de la empresa. Para el laboratorio con cuatro computadores, un *router* de las mismas características que el utilizado en la sección 3.5, y un *switch* cualquiera y por supuesto un espacio adecuado habilitado correctamente para este propósito, son suficientes. Paralela a esta etapa, se encuentra solicitud de dirección IPv6 a LACNIC, la cual al momento de la realización de este documento, es gratuita [56]. Luego, el paso siguiente es conectar esta red a Internet. Para esto es necesaria la construcción de un túnel IPv6-IPv4 que permita conectar el laboratorio a un 6to4 *relay* para obtener la conectividad deseada. Una vez concretada la conectividad, la instalación del laboratorio estará completa.

La segunda etapa de este proyecto, se desarrollará a medida que avancen las investigaciones en el laboratorio. La idea es dictar charlas informativas en las distintas divisiones de la empresa, de manera tal de comunicar a los usuarios finales en que cosiste este desarrollo, como los va a afectar a ellos y la importancia que tiene el llevarlo a cabo. Además es importante capacitar a los profesionales de área que estén interesados en participar en este proyecto, de manera de unir gente a éste y hacer posible el trabajo simultáneo en distintas zonas geográficas. Otra medida fundamental es la creación de un eslogan que permita comunicar de manera simple y directa el nuevo desafío asumido por la empresa. Además de comunicar este proyecto internamente, publicar en los medios de comunicación el compromiso aceptado por Codelco-Chile, permitirá empujar el desarrollo tecnológico en el país y además intercambiar experiencias con otras empresas que acepten ese reto.

Para continuar con la conectividad IPv6 dentro de la empresa, el siguiente paso tal como se describió con anterioridad, es integrar otros segmentos de red a IPv6. La idea acá es integrar gradualmente la red troncal de cada división, pasando por el laboratorio hacia Internet. El esquema de direccionamiento propuesto, junto con el esquema de conexión propuesto se describe en la secciones 3.4.1 y 3.4.3 respectivamente.

Finalmente, la última etapa corresponde a la finalización del proyecto y el comienzo de la evaluación del desempeño de éste. Una vez conectadas cada red troncal de la empresa, comienza el proceso de diagnóstico del desempeño de la red y la creación de posibles enlaces entre divisiones si el tráfico entre ellas lo amerita.

4.3.3 Materialización del Proyecto.

A continuación se describe el procedimiento a seguir para llevar a cabo el diseño presentado en la sección anterior. A partir de esto, se desarrollará además una carta Gantt que permita evaluar el progreso de éste.

4.3.3.1 Planeamiento.

Para llevar a cabo la materialización del proyecto, se seguirán los siguientes pasos en cada una de las etapas.

- Etapa 1: Esta etapa está compuesta por los siguientes pasos:
  - Paso 1: Gestión de la Instalación del Laboratorio. El primer paso es meramente administrativo y corresponde a conseguir los recursos necesarios para la instalación del laboratorio. En este grupo de recursos están considerados el lugar en donde se emplazará, los equipos necesarios (1 *router*, 1 *switch* y 4 computadores), los permisos para obtener una dirección IPv4 pública y conectar el laboratorio a la red interna y solicitar la dirección IPv6 a LACNIC.
  - Paso 2: Instalación del Laboratorio. Siguiendo los pasos descritos en la sección 3.5 se instala el laboratorio en el lugar destinado.
  - Paso 3: Túnel hacia Internet IPv6. Se construye el túnel desde el laboratorio hacia el exterior utilizando la técnica 6to4 descrita en la sección 2.3.3.

- Etapa 2: Para realizar las labores de comunicación se propone lo siguiente:

  - Paso 1: Organización de las charlas informativas. Antes de comenzar el proceso de informar, es necesario organizar cómo y dónde se realizarán y cuanto tiempo durarán. Según el público objetivo del la charla a expone,r se dictarán en diferentes horarios, lugares y con diferente duración. Por ejemplo, para un técnico es necesaria una charla más extensa en la que se expliquen las bases del protocolo, como funciona y en que cambia con respecto a su antecesor. Para un administrativo, basta con contarle por que se hace, cual es la importancia global de esto y en que le va a afectar, por lo que esta charla es mucho más breve.
  - Paso 2: Dictar las charlas. Una vez definidos los detalles, se pone en marcha esta etapa, la cual debe partir localmente. Es mejor partir en la división en la que se ésta trabajando con el laboratorio para que los compañeros de trabajo conozcan el objetivo del mismo. En este paso se crea toda la publicidad al respecto, el slogan publicitario, algún tipo de comercial, etc.
  - Paso 3: Presentación del proyecto al país. No es necesario que este paso se inicie cuando se concluya el anterior, pero sí es necesario que se inicie cuando el paso 2 se encuentre ya bien encaminado. La idea acá es presentar en los medios de comunicación que se está haciendo y por qué

se hace de manera de incentivar a otras empresas a realizar los mismos cambios e incentivar así el crecimiento tecnológico del país.

- Paso 4: Integración de nuevos miembros al equipo. Para trabajar paralelamente en varias divisiones, se seleccionará entre los técnicos presentes en las charlas a los que deseen unirse al proyecto y cuenten con las habilidades necesarias para esto. De esa forma, el proceso de adopción de la red troncal de cada división se puede hacer de manera paralela disminuyendo así el tiempo de ejecución del proyecto notablemente.

- Etapa 3: Esta etapa se divide en los siguientes pasos.

  - Paso 1: Replicar la primera isla IPv6. El primer paso en esta etapa, corresponde a replicar el laboratorio en algún lugar geográficamente distinto de la división, de manera de probar los túneles entre esta isla y el laboratorio, a través de la red WAN con la que cuenta la empresa.
  - Paso 2: Primera troncal migrada. Una vez completado el paso 1, se procede a habilitar el protocolo IPv6 en la primera red troncal. Por motivos de procesos de producción, se recomienda que la primera intervenida sea la red de Casa Matriz.
  - Paso 3: Conexión de la red troncal con el laboratorio. En este paso se replica el procedimiento utilizado en el paso 1 de manera de conectar a través de un túnel la red troncal con el laboratorio. Cabe señalar que el enrutamiento de los paquetes en la red troncal, debe tener una ruta por defecto que los dirija al laboratorio para dirigirse al exterior.
  - Paso 3: Confección de una guía de adopción para Codelco. Para ayudar a los nuevos miembros del equipo, se confeccionará una guía que describa paso a paso el procedimiento realizado para la habilitación del nuevo protocolo en la red troncal y su conexión al laboratorio.
  - Paso 5: Migración masiva de red troncal. Una vez completada la operación anterior, y utilizando a los nuevos miembros del equipo integrados en la etapa anterior, es posible migrar las redes de las diferentes divisiones paralelamente siguiendo los pasos descritos en la guía confeccionada en el paso anterior.

- Etapa 4. La última etapa de este proyecto se realizará siguiendo el siguiente procedimiento:
  - Paso 1: Evaluación de la red IPv6. Con la mayoría de las redes troncales conectadas al laboratorio, es posible evaluar como se ha desarrollado la conectividad a través de este nuevo protocolo analizando el tráfico de paquetes en la red. Se puede decidir conectar alguna red con otra de modo de descongestionar la red y analizar la posibilidad de habilitar algún servicio nuevo dependiendo de las necesidades de la empresa.

- Paso 2: Evaluación del desempeño en comparación con el servicio IPv4. También es importante analizar el desempeño de la red en comparación con los servicios entregados por el antiguo protocolo. Con los datos obtenidos en esta etapa, es posible realizar una comparación y decidir que aspectos de la nueva red hay que mejorar para alcanzar la calidad de servicio entregada por el protocolo anterior.
- Paso 3: Proyección a futuro: En este último paso del proyecto, se analizan los resultados de los pasos anteriores y se proyecta el avance hacia la migración total del protocolo. Se puede desarrollar alguna estrategia para habilitar IPv6 en el usuario final de la red y obtener la adopción en la red corporativa completa.

Finalmente, cabe señalar que la etapa 1 es transversal al proyecto, es decir el laboratorio continuará funcionando hasta incluso después de terminado el proyecto, como medio de control del tráfico y medio de pruebas para posibles soluciones posteriores.

4.3.3.2 Programación del proyecto.

Para realizar la programación del proyecto, se partirá elaborando la tabla de precedencia y secuencia, que se derivan del planeamiento del proyecto.

- Elaboración de tabla de precedencia y secuencia: Esta tabla se construye ordenando las actividades según el orden de ejecución necesario para llevar a cabo el proyecto de manera satisfactoria. Las tablas 4.2, 4.3 y 4.4 muestran esta secuencia.

Precedente	Actividad	Siguiente
	▪ Elaborar Plan	▪ Conseguir lugar de emplazamiento ▪ Adquirir equipos ▪ Solicitar y recibir Dirección IPv6 ▪ Conseguir permisos de conectividad hacia red empresarial.
▪ Elaborar Plan	▪ Conseguir emplazamiento	▪ Adecuar lugar para realizar instalaciones
▪ Elaborar Plan	▪ Adquirir equipos	▪ Instalación de laboratorio
▪ Elaborar Plan	▪ Solicitud dirección IPv6	▪ Conectividad Interna del laboratorio
▪ Elaborar Plan	▪ Conseguir permisos conectividad hacia la red empresarial	▪ Conexión del laboratorio hacia la red empresarial
▪ Conseguir emplazamiento	▪ Adecuar lugar para realizar instalaciones	▪ Instalación Laboratorio
▪ Adquirir equipos	▪ Instalación laboratorio	▪ Conectividad interna laboratorio
▪ Solicitud y recepción dirección IPv6	▪ Conectividad Interna laboratorio	▪ Conexión del laboratorio hacia red empresarial
▪ Conseguir permisos conectividad hacia red empresarial	▪ Conexión del laboratorio hacia red empresarial	▪ Túnel hacia Internet IPv6
▪ Adecuar lugar para realizar instalaciones ▪ Adquirir equipos	▪ Instalación Laboratorio	▪ Conectividad interna laboratorio
▪ Instalación laboratorio ▪ Solicitud y recepción dirección IPv6	▪ Conectividad interna laboratorio	▪ Conexión del laboratorio hacia red empresarial
▪ Conectividad interna laboratorio ▪ Conseguir permisos conectividad hacia red empresarial	▪ Conexión del laboratorio hacia red empresarial	▪ Túnel hacia Internet IPv6

Tabla 4.2: Tabla de precedencia y secuencia, primera parte.

Precedente	Actividad	Siguiente
▪ Conexión del laboratorio hacia red empresarial	▪ Túnel hacia Internet IPv6	▪ Organización de las charlas informativas ▪ Pruebas de Conectividad
▪ Túnel hacia Internet IPv6	▪ Organización de las charlas informativas e instructivas	▪ Dictar Charlas ▪ Presentación del proyecto al país
▪ Túnel hacia Internet IPv6	▪ Pruebas de Conectividad	▪ Evaluación de soporte IPv6 en aplicaciones. ▪ Replicar isla IPv6
▪ Organización de las charlas informativas e instructivas	▪ Presentación del proyecto al país	▪ Recolección de experiencias de otras empresas.
▪ Organización de las charlas informativas e instructivas	▪ Dictar Charlas	▪ Capacitación nuevo personal
▪ Pruebas de Conectividad	▪ Evaluación de soporte IPv6 en aplicaciones.	▪ Modificación y obtención de nuevas aplicaciones con soporte IPv6.
▪ Pruebas de Conectividad	▪ Replicar isla IPv6	▪ Conexión isla IPv6 con laboratorio.
▪ Dictar Charlas	▪ Capacitación nuevo personal	▪ Integración nuevo personal
▪ Replicar isla IPv6	▪ Conexión isla IPv6 con laboratorio.	▪ Habilitación de IPv6 en primera red troncal
▪ Conexión isla IPv6 con laboratorio.	▪ Habilitación de IPv6 en primera red troncal	▪ Conexión red troncal con laboratorio
▪ Presentación del proyecto al país	▪ Recolección de experiencias de otras empresas.	▪ Confección guía de adopción para Codelco.
▪ Habilitación de IPv6 en primera red troncal	▪ Conexión red troncal con laboratorio	▪ Confección guía de adopción para Codelco.
▪ Conexión red troncal con laboratorio ▪ Recolección de experiencias de otras empresas.	▪ Confección guía de adopción para Codelco.	▪ Migración masiva de red troncal
▪ Capacitación nuevo personal	▪ Integración nuevo personal	▪ Migración masiva de red troncal

Tabla 4.3: Tabla de precedencia y secuencia, segunda parte.

Precedente	Actividad	Siguiente
▪ Evaluación de soporte IPv6 en aplicaciones.	▪ Modificación y obtención de nuevas aplicaciones con soporte IPv6.	▪ Migración masiva de red troncal
▪ Confección guía de adopción para Codelco ▪ Integración nuevo personal ▪ Modificación y obtención de nuevas aplicaciones con soporte IPv6.	▪ Migración masiva de red troncal	▪ Conexión redes al laboratorio.
▪ Migración masiva de red troncal	▪ Conexión redes al laboratorio.	▪ Evaluación de la red IPv6 ▪ Evaluación del desempeño
▪ Conexión redes al laboratorio.	▪ Evaluación de la red IPv6 ▪ Evaluación del desempeño	▪ Proyección a futuro

Tabla 4.4: Tabla de precedencia y secuencia, tercera parte.

- Elaboración de la red de actividades: Para elaborar la carta Gantt, es necesario relacionar los pasos descritos en la sección anterior, con el tiempo de ejecución de éstos. Para ello, lo primero es realizar un diagrama que muestre la red de actividades, para luego fijar los plazos de cada una de las etapas y finalizar con el plazo del proyecto completo. La figuras 4.2, 4.3 y 4.4 muestran el diagrama (separado por el espacio disponible) mencionado.

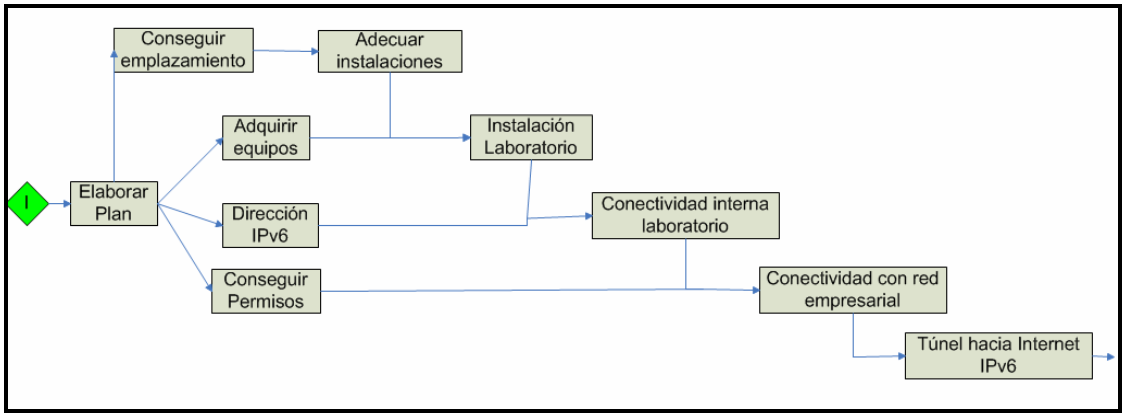

Figura 4.2: Red de actividades, primera parte.

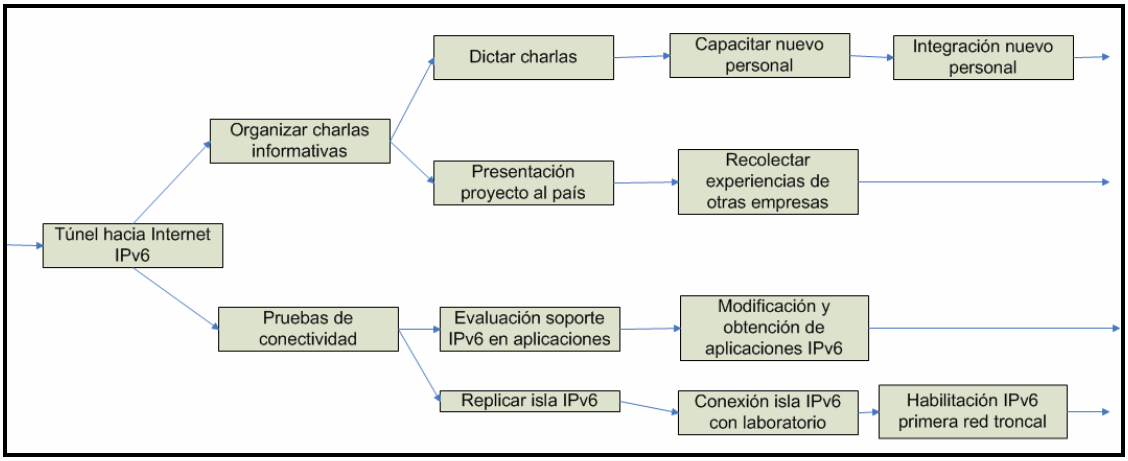

Figura 4.3: Red de actividades, segunda parte.

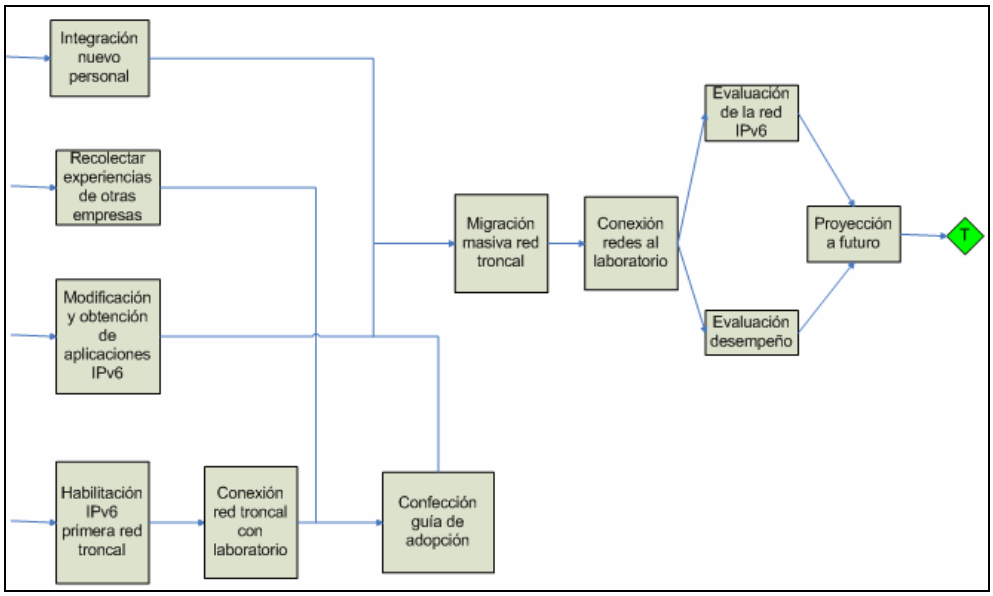

Figura 4.4: Red de actividades, tercera parte.

- Asignación de los tiempos necesarios: Una vez obtenida la red de actividades, se procede a definir los tiempos de cada actividad. Las tablas 4.5 y 4.6 muestra los tiempos asignados a cada tarea.

Actividad	Tiempo
Elaborar Plan	24 semanas
Conseguir lugar de emplazamiento	1 semana
Adquirir equipos	1 semana
Solicitar y recibir Dirección IPv6	8 semanas
Conseguir permisos de conectividad hacia red empresarial	4 semanas.
Adecuar lugar para realizar instalaciones	1 semana
Instalación de laboratorio	3 días
Conectividad Interna del laboratorio	3 días
Conexión del laboratorio hacia la red empresarial	1 semana
Túnel hacia Internet IPv6	1 semana
Organización de las charlas informativas	1 semana
Pruebas de Conectividad	1 semana
Dictar Charlas	8 semanas
Presentación del proyecto al país	4 semanas
Evaluación de soporte IPv6 en aplicaciones	4 semanas
Replicar isla IPv6	1 semana
Recolección de experiencias de otras empresas	2 semanas
Capacitación nuevo personal	3 semanas
Modificación y obtención de nuevas aplicaciones con soporte IPv6	8 semanas
Conexión isla IPv6 con laboratorio	1 semana
Integración nuevo personal	2 semanas
Habilitación de IPv6 en primera red troncal	4 semanas
Conexión red troncal con laboratorio	4 semanas
Confección guía de adopción para Codelco	4 semanas
Migración masiva de red troncal	24 semanas
Actividad	Tiempo
Conexión redes al laboratorio	8 semanas
Evaluación de la red IPv6	8 semanas
Evaluación del desempeño de la red	8 semanas
Proyección a futuro	4 semanas

Tabla 4.6: Asignación de tiempos para cada actividad, segunda parte

La asignación de cada tiempo se justifica de la siguiente manera. La etapa de elaborar plan, corresponde al desarrollo de esta memoria, por lo que el tiempo asignado es el que demoró la realización de este documento. La adquisición del lugar y de los equipos no debería tomar demasiado tiempo, pues Codelco-Chile cuenta con varios lugares disponibles y posee también un buen stock de equipos. La asignación de la dirección IPv6 tomará algo más de tiempo y se estima que durará 8 semanas debido al trámite a realizar. Los permisos necesarios, se espera que no tomen más de cuatro semanas, pues son una parte importante del proyecto. Para adecuar las instalaciones con una semana es más que suficiente, pues la idea es hacer el espacio físico necesario para instalar el laboratorio. La instalación del laboratorio no debería tomar más de tres días, pues en la sección 3.5 se presenta una guía de cómo realizar este procedimiento, al igual que la conectividad interna. La conexión con la red empresarial puede tomar una semana debido a que se requiere una revisión total de la instalación para no provocar daño alguno. El túnel también tomará alrededor de una semana debido a la complejidad técnica que posee. La organización de las charlas necesita una semana para conseguir los espacios para realizarla y decidir el contenido de éstas. Las pruebas de conectividad no deberían presentar mayores inconvenientes por lo que se estima que con una semana es suficiente. Para las charlas se necesita un tiempo algo mayor, los lugares en los que se dictarán están separados geográficamente por varios kilómetros. La presentación del proyecto al país debería tomar un mes, en cuanto a la organización de los medios por los cuales se realizará. Para evaluar las aplicaciones, se necesita algo más de tiempo por lo que se estima un mes. Para replicar la isla nuevamente no se necesita más que una semana pues ya se cuenta con la experiencia del laboratorio. Se dedicarán además dos semanas para recolectar experiencias de otras empresas, para poder visitar las instalaciones y conversar con los técnicos, si fuera el caso. La capacitación del nuevo personal puede tardar a lo más tres semanas, tiempo en el que se le enseñarán los principios básicos necesarios para realizar su futura labor. La modificación de las aplicaciones puede tomar 2 meses debido a la complejidad de algunas, e incluso puede ser necesario evaluar ayuda externa para disminuir el tiempo de ejecución de este paso. La conexión de la isla con el laboratorio no debería tomar más de una semana pues se cuenta con la experiencia del túnel realizado anteriormente. Para la integración del nuevo personal se estiman dos semanas para poder explicar detalladamente el trabajo a realizar. La confección de la guía requiere más tiempo pues la idea es completarla de manera que sea de fácil lectura. El punto que tomará más tiempo de todo el proyecto es la migración en forma paralela de las redes troncales de cada división, el cual se estima en 6 meses. La conexión del laboratorio con las redes ya migradas tomará alrededor de 2 meses como máximo. Las respectivas evaluaciones tomarán 2 meses. Finalmente la proyección a futuro del proyecto se realizará en un mes para decidir calmadamente los pasos a seguir a futuro.

- Relación entre tiempos y red de actividades: A continuación se muestra el vínculo entre ambos ítems, definiéndose así la duración del proyecto y mostrando además que actividades se pueden desarrollar en paralelo. Las

figuras 4.5, 4.6 y 4.7 muestran entonces las actividades con sus respectivas fechas de inicio y término (en semanas a partir del inicio del proyecto).

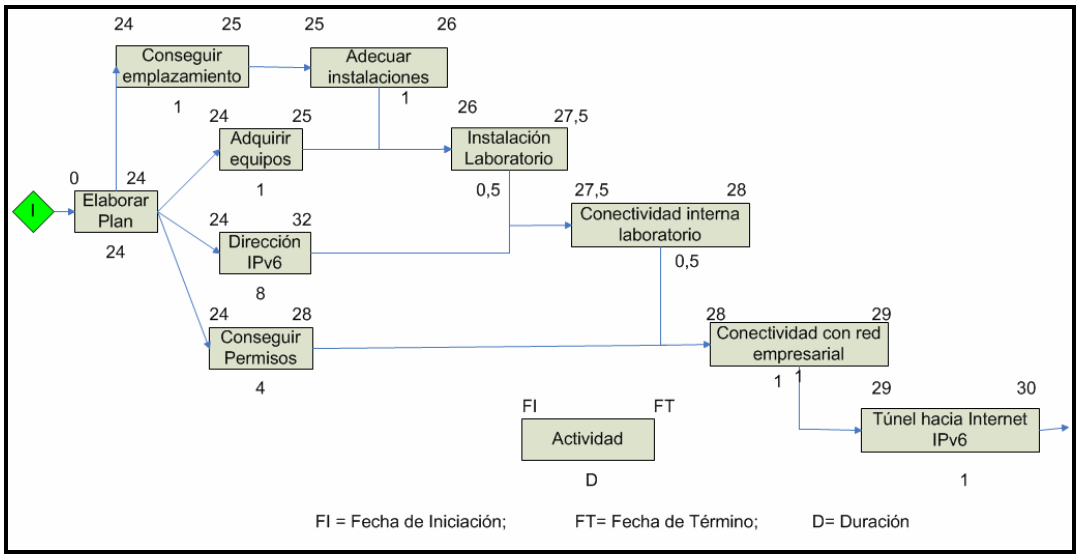

Figura 4.5: Fechas de inicio y término (en semanas desde el inicio del proyecto) de las actividades

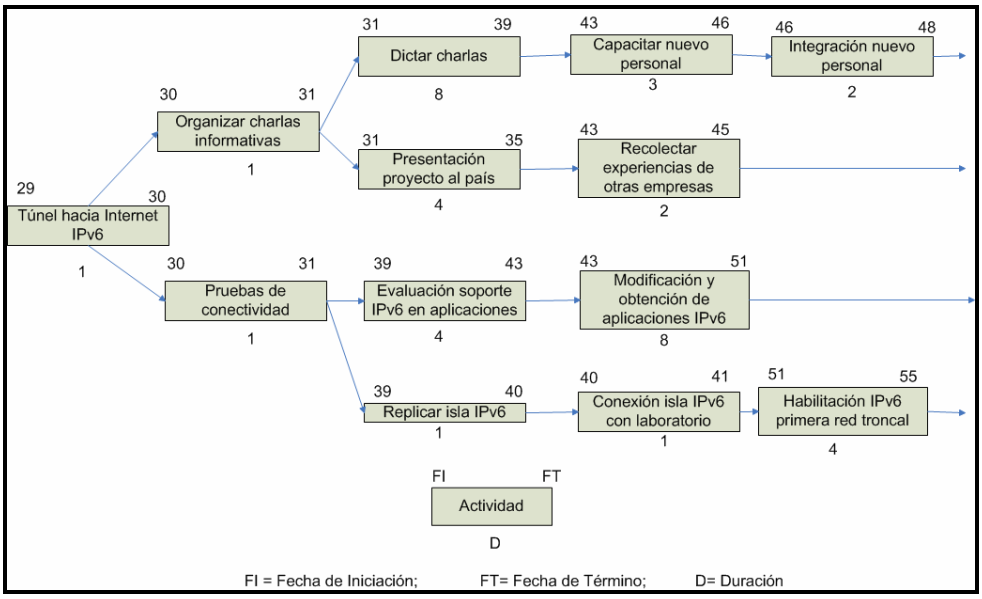

Figura 4.6: Fechas de inicio y término (en semanas desde el inicio del proyecto) de las actividades, segunda parte.

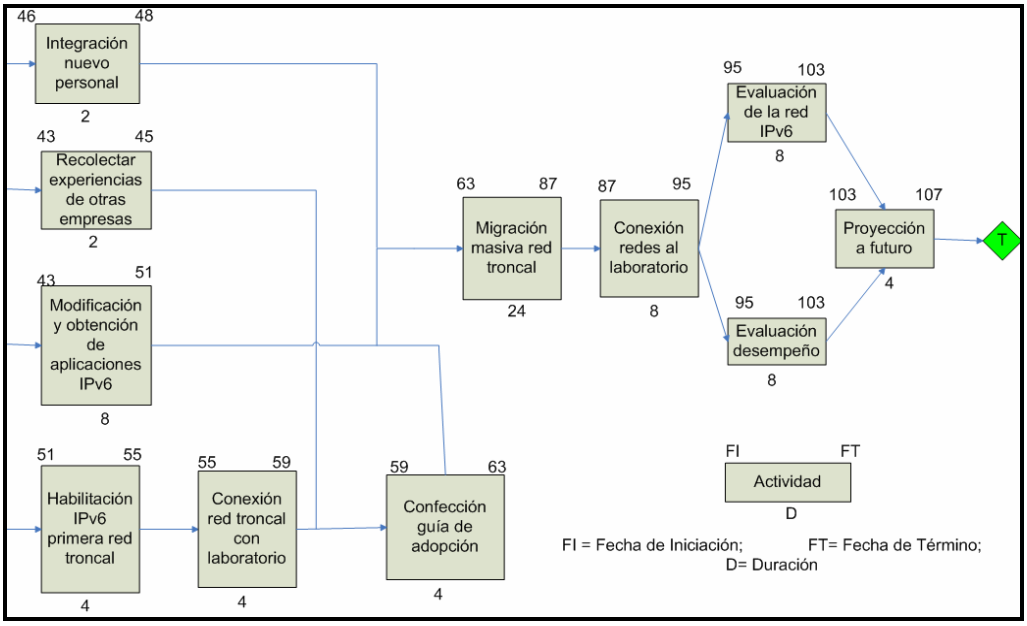

Figura 4.7: Fechas de inicio y término (en semanas desde el inicio del proyecto) de las actividades, tercera parte.

Luego, de las figuras anteriores se observa que el proyecto completo desde el inicio de la memoria hasta el término de la adopción de las redes troncales de la empresa, tiene una duración de 107 semanas, es decir de $\frac{107}{48} = 2{,}22916667$ años. El decimal corresponde a $0{,}22916667 \bullet 12 = 2{,}75$ meses, es decir el proyecto, contando los seis meses de duración de esta memoria, tiene una longitud de 2 años y 3 meses aproximadamente.

La carta Gantt asociada al proyecto se deriva entonces de los datos mostrados en las figuras 4.5, 4.6 y 4.7 y se presenta a continuación. (Para observar la carta Gantt con mayor detalle, dirigirse al anexo A).

Id	Nombre de tarea	Duración	Comienzo	Fin
1	Elaborar Plan	24 sem.	lun 03-03-08	vie 15-08-08
2	Conseguir emplazamiento	1 sem	lun 18-08-08	vie 22-08-08
3	Adquirir equipos	1 sem	lun 18-08-08	vie 22-08-08
4	Solicitud y recepción dirección II	2 mes	lun 18-08-08	vie 10-10-08
5	Conseguir permisos	4 sem.	lun 18-08-08	vie 12-09-08
6	Adecuar instalaciones	1 sem	lun 25-08-08	vie 29-08-08
7	Instalar Laboratorio	3 días	lun 01-09-08	mié 03-09-08
8	Conectividad interna Lab	2 días	jue 04-09-08	vie 05-09-08
9	Conectividad con red empresarial	1 sem	lun 15-09-08	vie 19-09-08
10	Túnel hacia Internet IPv6	1 sem	lun 22-09-08	vie 26-09-08
11	Organizar charlas informativas	1 sem	lun 29-09-08	vie 03-10-08
12	Pruebas de conectividad	1 sem	lun 29-09-08	vie 03-10-08
13	Dictar Charlas	8 sem.	lun 06-10-08	vie 28-11-08
14	Presentación proyecto al país	4 sem.	lun 06-10-08	vie 31-10-08
15	Evaluación aplicaciones	4 sem.	lun 01-12-08	vie 26-12-08
16	Replicar isla IPv6	1 sem	lun 01-12-08	vie 05-12-08
17	Capacitar nuevo personal	3 sem.	lun 29-12-08	vie 16-01-09
18	Recolectar experiencias	2 sem.	lun 29-12-08	vie 09-01-09
19	Modificación aplicaciones	8 sem.	lun 29-12-08	vie 20-02-09
20	Conectividad isla IPv6	1 sem	lun 08-12-08	vie 12-12-08
21	Integración nuevo personal	2 sem.	lun 19-01-09	vie 30-01-09
22	Habilitación ipv6 1ra red troncal	4 sem.	lun 23-02-09	vie 20-03-09
23	Conexión red troncal con Lab	4 sem.	lun 23-03-09	vie 17-04-09
24	Confección Guía	4 sem.	lun 20-04-09	vie 15-05-09
25	Migración masiva red troncal	24 sem.	lun 18-05-09	vie 30-10-09
26	Conexión redes al Lab	8 sem.	lun 02-11-09	vie 25-12-09
27	Evaluación red IPv6	8 sem.	lun 28-12-09	vie 19-02-10
28	Evaluación desempeño	8 sem.	lun 28-12-09	vie 19-02-10
29	Proyección a futuro	4 sem.	lun 22-02-10	vie 19-03-10
30	Fin	0 días	vie 19-03-10	vie 19-03-10

Figura 4.8: Carta Gantt del proyecto, primera parte.

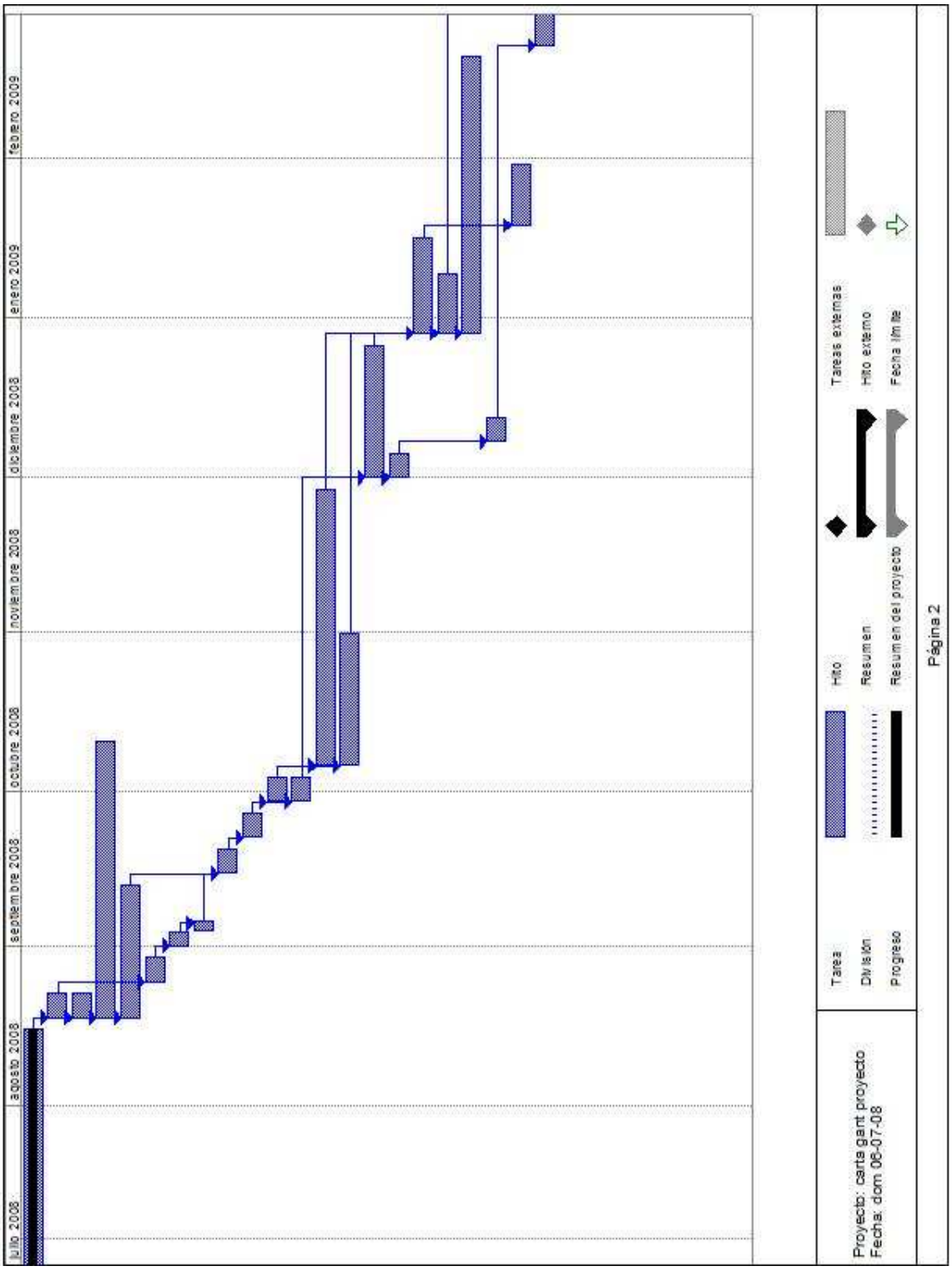

Figura 4.9: Carta Gantt del proyecto, segunda parte.

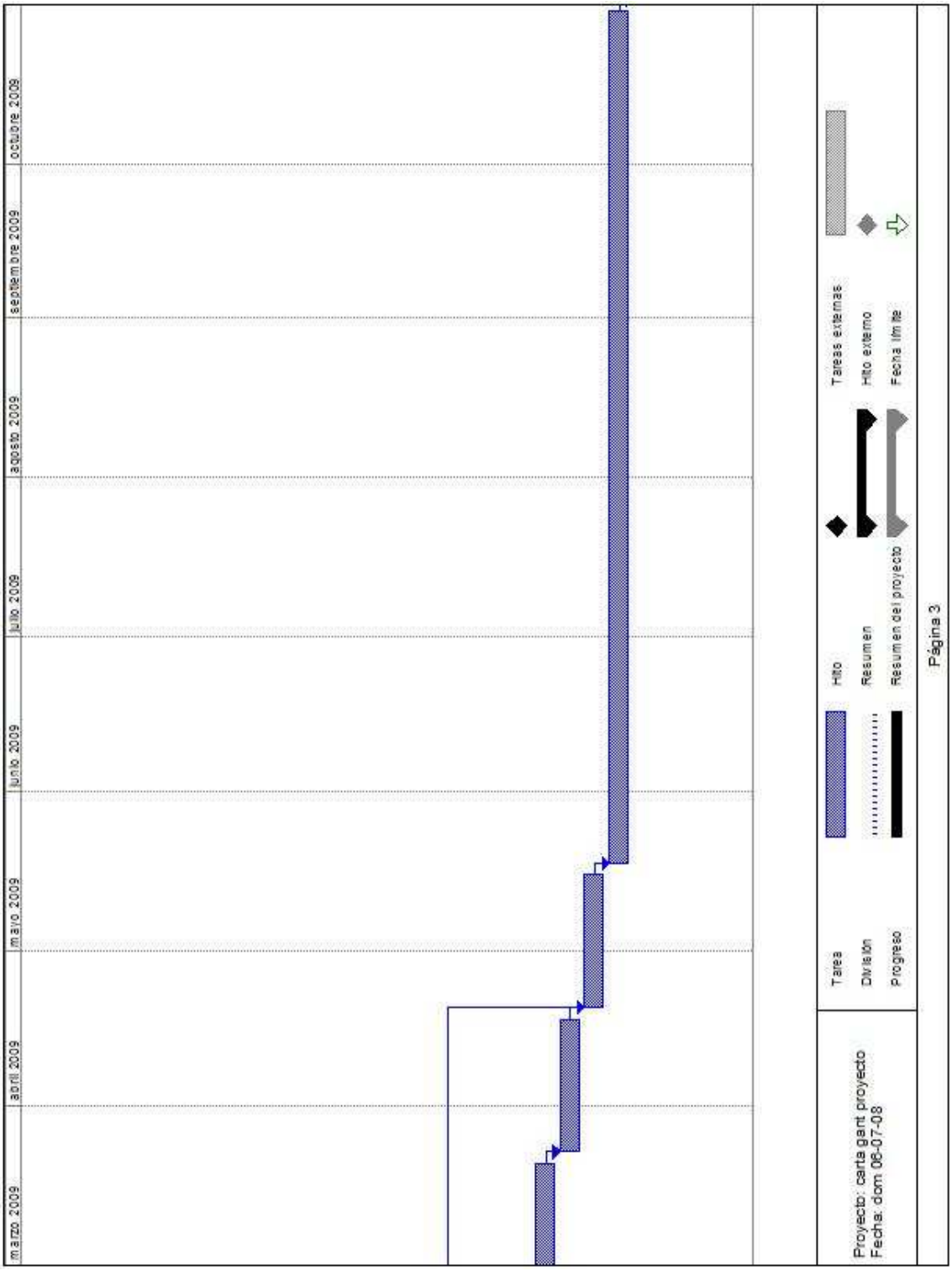

Figura 4.10: Carta Gantt del proyecto, tercera parte.

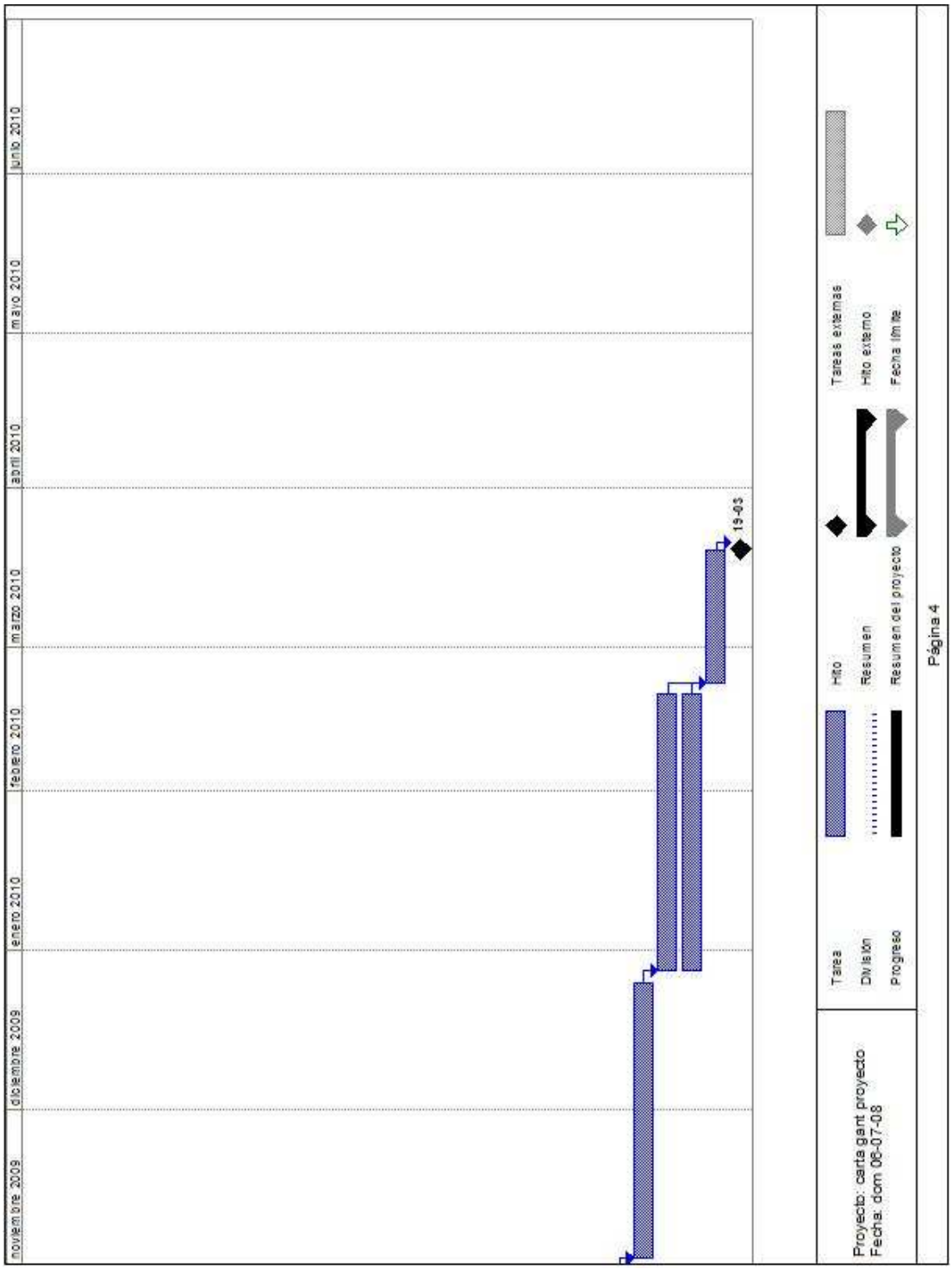

Figura 4.11: Carta Gantt del proyecto, cuarta parte.

De esta forma, se concluye la programación del proyecto, contando con un tiempo estimado de duración de dos años y tres meses desde el inicio de esta memoria. Así la adopción de IPv6 en la red corporativa de Codelco es factible realizarla y en un plazo relativamente corto.

4.3.3.3 Recursos Asociados al proyecto.

Los recursos asociados a este proyecto, se derivan sin mucha discusión de la sección anterior. Según la actividad a desarrollar se necesitarán diversos profesionales y técnicos asociados al proyecto. En los comienzos del proyecto, es suficiente contar con un ingeniero y un técnico de manera de instalar el laboratorio y comenzar la investigación. Cuando se comienza la conectividad hacia la red puede ser necesario contar con otra “cuadrilla ipv6”, es decir con otro ingeniero y otro técnico, de manera de dividir las labores y trabajar simultáneamente en distintos lugares para llevar a cabo más rápidamente la tarea encomendada. Para organizar las charlas, basta con un ingenierio, pero además se necesitará la ayuda de un publicista de manera de seleccionar y desarrollar técnicas efectivas para difundir de mejor forma el proyecto a nivel local (empresa) y país. Así al presentar el proyecto al país además se necesitará contar con un periodista que se encargue de los contactos y la distribución correcta de la información.

El siguiente cambio de cantidad de personal aparece cuando se integra más gente al equipo. En ese instante será necesario contar con 4 ingenieros y 4 técnicos de manera de lograr habilitar correctamente las 4 divisiones de la empresa simultáneamente y en el menor tiempo posible. Desde ahí para adelante, este equipo se encargará de culminar la tarea y finalizar exitosamente el proyecto.

Con respecto a los equipos, sólo se necesitarán equipos extra en la construcción del laboratorio y de su posterior réplica. Esto se debe a que se pretende utilizar los equipos ya instalados en la red, de manera de intervenir lo menos posible el sistema. Este punto puede variar si existe alguna razón técnica que determine el cambio de algún equipo en particular para lograr llevar a cabo este proyecto.

A continuación se muestra la tabla 4.11 en la cual se encuentran los datos descritos anteriormente de forma más esquematizada. Es importante además notar que la medicación de las aplicaciones necesitará 2 ingenieros pero no precisamente los a cargo del proyecto, sino expertos en computación que puedan realizar los cambios sin mayores complicaciones.

	Recursos							
Actividad	**Humanos**				**Equipos**			**Dependencias**
	Ingenieros	Técnicos	Publicistas	Periodistas	Computadores	*Routers*	*Switchs*	Lugar habilitado
Elaborar Plan	1				1			1
Conseguir emplazamiento	1	1						1
Adquirir equipos	1	1						
Solicitud y recepción dirección IPv6	1	1						
Conseguir permisos	1							
Adecuar instalaciones	1	1						
Instalar Laboratorio	1	1			4	1	1	1
Conectividad Interna Lab	1	1						
Conectividad con red empresarial	2	2						
Túnel hacia Internet IPv6	2	2						
Organizar charlas informativas	1		1					
Pruebas de conectividad	2	2						
Dictar Charlas	2							
Presentación proyecto al país			1	1				
Evaluación aplicaciones	2							
Replicar isla IPv6	2	2			4	1	1	1
Capacitar nuevo personal	2	2						
Recolectar experiencias	1			1				
Modificación aplicaciones	2							
Conectividad isla IPv6	2	2						
Integración nuevo personal	2							
Habilitación Ipv6 1ra red troncal	2	2						
Conexión red troncal con Lab	2	2						
Confección Guía	2							
Migración masiva red troncal	4	4						
Conexión redes al Lab.	4	4						
Evaluación red IPv6	4							
Evaluación desempeño	4							
Proyección a futuro	4							

Tabla 4.7: Recursos asociados al proyecto.

Capítulo V: Conclusiones.

Una estrategia de adopción de este nuevo protocolo es de suma importancia para cualquier empresa, en particular para una de la magnitud de Codelco-Chile. La exploración de esta nueva tecnología e impulsar su uso en el país es una tarea que la Corporación del Cobre no puede dejar de lado.

Así, durante el desarrollo de esta memoria, se diseñó una estrategia factible de adopción de IPv6, cuya duración desde el inicio de esta memoria no excede los 2 años y medio, y utiliza los recursos disponibles en la empresa, por lo que los costos asociados son relativamente bajos. La estrategia desarrollada consta de cuatro etapas base: La primar etapa corresponde a la confección de un laboratorio de pruebas que permita estudiar el protocolo, usarlo como base de análisis y como semilla para el crecimiento de la conectividad IPv6. La segunda etapa define la necesidad de difundir el proyecto para impulsar la carrera tecnológica en el país y lograr intercambiar experiencias que permitan mejorar el desempeño del proyecto. La tercera etapa pretende expandir el uso del protocolo en la empresa, migrando la red troncal de las cuatro divisiones a lo largo del país, y conectarlas al laboratorio para evaluar su desempeño. La última etapa corresponde a la planeación futura del proyecto, teniendo en mente la migración final a IPv6.

Adoptar el nuevo protocolo, no solo significa estar preparado para el cambio de tecnología que está a la vuelta de la esquina, sino que también permite continuar liderando el avance tecnológico en Latinoamérica. Por otro lado, este impulso es una contribución al país pues motiva el acercamiento a nuevas tecnologías tanto a empresas particulares como al estado.

Para estructurar de mejor forma el proyecto, se detallaron los pasos a seguir y se definieron los plazos y recursos necesarios para llevarlo a cabo, concluyendo con una carta Gantt.

Por otro lado, la automatización de los procesos de producción se vuelve una herramienta importante en la labor llevada por cualquier empresa. Este nuevo protocolo permite facilitar este cambio, pues proporciona la factibilidad técnica de acceder a dispositivos que dispongan de una conexión a la red desde cualquier punto del planeta, ya que la utilización del protocolo NAT queda completamente obsoleto, dejando públicas las direcciones de cada uno de ellos. Así, adoptar esta nueva tecnología permite estar preparados para comenzar la innovación tecnológica mencionada.

Los estudios a futuro que parten desde la iniciación de esta memoria son principalmente definir las políticas de seguridad y de calidad de servicio asociadas a la nueva conectividad. También es importante definir las modificaciones necesarias a las aplicaciones nativas de Codelco y la factibilidad de continuar su uso. Por otro lado, queda pendiente también las modificaciones de la infraestructura DNS (Domain Name Service) que permitan utilizar este recurso.

De esta forma se concluye este estudio que permitirá la integración de esta nueva tecnología en la red corporativa de Codelco-Chile. Esta investigación es un gran avance en el desarrollo tecnológico del país, pues abre el camino a la incorporación de tecnologías de punta en la industria nacional y además posicionar al país entre los pocos que han comenzado con la investigación e integración de este nuevo protocolo de red en el mundo. Es por esto que no sólo Codelco-Chile, sino que todas las empresas nacionales deben unirse a este desarrollo para fomentar el crecimiento tecnológico del país.

Referencias.

[1]. Deering, S., Hinden, R., “Internet Protocol, Version 6 (IPv6) Specification”, RFC 2460, Diciembre 1998.

[2]. Information Sciences Institute, University of Southern California, “Internet Protocol”, RFC 791, Septiembre 1981.

[3]. http://www.apnic.net/news/2007/0626.html

[4]. http://www.codelco.cl/

[5]. http://www.codelco.com/la_corporacion/fr_organizacion.html

[6]. Hagen, Silvia., “IPv6 Essencials”, O’Reilly, 2002

[7]. Deering, S., Hinden, R., “IP Version 6 Addressing Architecture”, RFC 2373, Julio 1998.

[8]. Comer, Douglas., “Internetworking With TCP/IP Volume 1: Principles Protocols, and Architecture”, 5th edition, 2006

[9]. Droms, R., “Dynamic Host Configuration Protocol”, RFC 2131, Marzo 1997.

[10]. http://www.linux.org/docs/ldp/howto/Linux+IPv6-HOWTO/index.html

[11]. http://technet.microsoft.com/es-cl/library/bb726949(en-us).aspx

[12]. 6SOS, “Instalación de Ipv6 en plataformas Windows”, 2004.

[13]. http://www.ipv6day.org/action.php?n=Es.Configuration-WindowsVista

[14]. http://docs.sun.com/app/docs/820-2981/ipv6-config-tasks-64?1=es&a=view

[15]. Microsoft Corporation, “IPv6 Transition Technologies”, Febrero 2008

[16]. Gilligan, R., Nordmark, E., “Transition Mechanisms for IPv6 Hosts and Routers”, RFC 2893, Agosto 2000

[17]. http://lacnic.net/sp/index.html

[18]. www.iana.org

[19]. http://www.icann.org/

[20]. http://www.root-servers.org/

[21]. http://www.iana.org/reports/2008/root-aaaa-announcement.html

[22]. Sotillo Samuel., "IPv6 Security Issues", 2008.

[23]. http://www.ipv6ready.org/frames.html

[24]. Kent, S., Akitson, R., "Security Architecture for the Internet Protocol", RFC 2401, Noviembre 1998.

[25]. http://www.microsoft.com/spain/windowsserver2003/technologies/ipv6/ipv6.mspx

[26]. http://en.beijing2008.cn/ipv6

[27]. ipv6.google.com

[28]. http://www.lab.bt.es/ipv6/global_results_local.html

[29]. http://www.ipv6.org/v6-www.html

[30]. Millán, Ramón; Huidobro, José; "¿Qué es MPLS?", Revista BIT, Septiembre-Octubre 2002

[31]. http://www.ipv6.org.au/map.html#businesses

[32]. Lind, M., Ksinant, V., Park, S., Baudot, A., Savola, P., "Scenarios and Analisys for Introducing IPv6 into ISP Networks", RFC 4029, Marzo 2005.

[33]. Huitima C., Austein, R., Satapati, S., Van der Pol, R., "Unmanaged Networks IPv6 Transition Scenarios", RFC 3750, Abril 2004.

[34]. Bound, J., "IPv6 Enterprise Network Scenarios", RFC 4057, Junio 2005.

[35]. Durand, A., Ihren, J., "DNS IPv6 Transport Operational Guidelines", RFC 3901, Septiembre 2004.

[36]. Thomson, S. and T. Narten, "IPv6 Stateless Address Autoconfiguration", RFC 2462, Diciembre 1998.

[37]. Droms, R., Bound, J., Volz, B., Lemon, T., Perkins, C., and M. Carney, "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)", RFC 3315, Julio 2003.

[38]. Nikander, P., Kempf, J., and E. Nordmark, "IPv6 Neighbor Discovery (ND) Trust Models and Threats", RFC 3756, Mayo 2004.

[39]. Shin, M-K., Hong, Y-G., Hagino, J., Savola, P., and E. Castro, "Application Aspects of IPv6 Transition", RFC 4038, Marzo 2005.

[40]. Bound, J., Pouffary, Y., Klynsma, S., Chown, T, Green, D., "IPv6 Enterprise Network Analysis – IP Layer 3 Focus", RFC 4852, Abril 2007.

[41]. Chown, T., "Use of VLANs for IPv4-IPv6 Coexistence in Enterprise Networks", RFC 4554, Junio 2006.

[42]. Thomson, S., Huitema, C., Ksinant, V., Souissi, M., "DNS Extensions to Support IP Version 6", RFC 3596, Octubre 2003.

[43]. Van de Velde, G., Hain, T., Droms, R., Carpenter, B., Klein, E., "Local Network Protection for IPv6", RFC 4864, Mayo 2007.

[44]. Cisco Systems, Inc., "Start Here: Cisco IOS Software Release Specifics for Ipv6 Features".

[45]. http://tools.cisco.com/ITDIT/ISTMAIN/

[46]. Gordon, David., Haddad, Ibrahim., "Building an IPv6 Linux Router Server", 2003.

[47]. Cisco Systems, Inc., Datasheet Cisco 2800 Series.

[48]. Cisco Systems, Inc., "Loading Cisco IOS Software".

[49]. www.uhu.es/marcos.deltoro/archivos/TR/Hyperterminal.pdf

[50]. Cisco Systems, Inc., "Implementing IPv6 Addressing and Basic Connectivity", Mayo 2008

[51]. http://www.nic.cl/faq/general.html#1

[52]. http://www.nic.cl/

[53]. http://www.lacnic.net/sp/index.html

[54]. http://www.lacnic.net/ipv6tour/sp/santiago.html

[55]. http://www.ipv6enchile.cl/

[56]. http://www.lacnic.net/sp/registro/table.html

ANEXO A: CARTA GANTT DE LA ESTRATEGIA DE ADOPCIÓN DE IPV6 EN LA RED CORPORATIVA DE CODELCO.