ESCUELA POLITÉCNICA DEL EJÉRCITO

DEPARTAMENTO DE CIENCIAS DE LA COMPUTACIÓN

CARRERA DE INGENIERÍA DE SISTEMAS E INFORMÁTICA

"MULTIHOMING IPv6 CASO PRÁCTICO"

Previa a la obtención del Título de:

INGENIERO/A EN SISTEMAS E INFORMÁTICA

POR: FLORES DUQUE ORLANDO ADOLFO
TOAPANTA FAICÁN ZOILA SUSANA

SANGOLQUÍ, 20 de Marzo del 2.007

CAPÍTULO I
INTRODUCCIÓN

1.1 JUSTIFICACIÓN E IMPORTANCIA 1
1.2 OBJETIVOS 3
1.2.1 OBJETIVO GENERAL 3
1.2.2 OBJETIVOS ESPECÍFICOS 3
1.3 ALCANCE 4
1.4 METODOLOGÍA 5

CAPÍTULO II
MARCO TEÓRICO

2.1 Inicios y Evolución de Internet 6
2.2 IPv4 11
2.2.1 DEFINICIÓN 11
2.2.2 Limitaciones de IPv4 12
2.2.3 Cabecera IPv4 12
2.2.4 Direccionamiento en IPv4 14
2.3 CIDR (Classless Inter Domain Routing) 18
2.3.1 Definición 18
2.3.2 Prefijo de una Dirección IP “CIDR” 20
2.4 SUBNETTING 22
2.4.1 Tipos de Subnetting 23
2.4.1.1 Estático 23
2.4.1.2 Longitud Variable 23
2.5 SUPERNETTING 23
2.5.1 Supernetting (Sumarización) 25
2.6 VLSM (Variable Length Subnet Mask Mascara de Subred de Longitud Variable) 27
2.6.1 Ventajas 28
2.7 PROXY 28
2.8 NAT (Network Address Translation Traducción de Dirección de Red) 29
2.9 PAT (Port Address Traslation Traducción de Direcciones de Puerto) 31
2.10 RPAT (Reverse Port Address Translation Traducción de Dirección de Puerto Reverso) 32
2.11 IPv6 33
2.11.1 Definición 33
2.11.2 Cabecera IPv6 35

2.11.2.1 Tipos de Cabecera de Extensión IPv6 36
2.11.3 Direccionamiento en IPv6 42
2.11.3.1 Direcciones Unicast 42
2.11.3.1.1 Global Unicast 43
2.11.3.1.2 Link Local 43
2.11.3.1.3 Direcciones Unicast de Sitio Local 44
2.11.3.1.4 Direcciones Especiales 44
2.11.3.1.4.1 Direcciones No Especificadas 44
2.11.3.1.4.2 Dirección de Bucle Local (Loopback). 45
2.11.3.1.5 Direcciones Unicast Basadas en Proveedor 45
2.11.3.2 Direcciones Anycast 45
2.11.3.3 Direcciones Multicast 46
2.11.4 Representación de Direcciones en IPv6 48
2.11.5Comparación de Cabeceras de IPv4 a IPv6 51
2.11.6 Equipos que Soportan IPv6 53
2.11.7 Formas de Conexión de IPv6 55
2.11.7.1 Dual IP Layer (Doble capa IP) 55
2.11.7.2 IPv6 over IPv4 Tunneling (IPv6 sobre IPv4) 55
2.11.8 Comparación de las Características de IPv4 e IPv6 59

2.12 MULTIHOMING 62
2.12.1 Definición 62
2.12.2 Ventajas de Multihoming 65
2.12.3 Multihoming en Organizaciones Pequeñas. 66
2.12.4 Multihoming en Organizaciones Grandes 66
2.12.5 Problemas 67

CAPÍTULO III

ANÁLISIS Y DISEÑO

3.1 Diseño Lógico 69

3.2 Diseño Físico 71

3.3 Elementos Físicos para la Implementación de Multihoming con IPv6 72
3.3.1 Requisitos para la Instalación de los Sistemas Operativos 72
3.3.2 Equipos para la Conexión 74
3.3.2.1 Router Cisco 2500 74
3.3.2.1.1 Configuración de un Enrutador Nuevo 74
3.3.2.1.2 Configuración de Interfaces 75
3.3.2.1.3 Modos de Acceso al Router 76
3.3.2.1.4 Configurar el Enrutador 77
3.3.2.1.5 Mostrar la Configuración 77
3.3.2.1.6 Dónde está la Configuración 78
3.3.2.1.7 Guardar la Configuración en Sitios más Permanentes 78
3.3.2.1.8 Borrar la Configuración 79
3.3.2.1.9 Recuperación de Desastres 80
3.3.2.1.10 Puertos del Router Cisco 2500 81

CAPÍTULO IV

CONFIGURACIONES

4.1 Configuración de IPv6 en Windows 2000 Server 82
4.2 Configuración de IPv6 en Windows 2003 Server 86
4.2.1 Pruebas de Conectividad con Windows 2003 Server 91
4.3 Configuración IPv6 en Linux Mandrake 10.1 93
4.3.1 Pruebas de Conectividad Linux Mandrake 10.1 95

CAPÍTULO V

PRUEBAS E IMPLEMENTACIÓN

5.1 Implementación de los Túneles 99
5.1.1 Implementación del Tunneling Público con Linux 99
5.1.2 Implementación de Tunneling para Windows 101
5.2 Configuración de IPv6 en el Router Cisco 2500 106
5.3 Pruebas de Conectividad de los Túneles 110
5.3.1 Pruebas de Conectividad de IPv6 en Windows 110
5.3.1.1 Pruebas de Rutas a través de la página www.klingon.nl 112
5.3.2 Pruebas de Conectividad de IPv6 en Linux 119
5.3.3 Pruebas de Conectividad a través del Router 129
5.3.3.1 Traceroute desde Túnel 0 al Túnel 2 129
5.3.3.2 Traceroute Configurada la Salida por el Túnel 0 con Dirección de Origen Túnel 0 129
5.3.3.3 Traceroute Configurada la Salida por el Túnel 0 con Dirección de Origen Túnel 2 134
5.3.3.4 Traceroute Configurada la Salida por el Túnel 2 con Dirección de Origen Túnel 0 138
5.3.3.5 Traceroute Configurada la Salida por el Túnel 2 con Dirección de Origen Túnel 2 142

CAPÍTULO VI

CONCLUSIONES Y RECOMENDACIONES

6.1 CONCLUSIONES 146
6.2 RECOMENDACIONES 148

BIBLIOGRAFÍA 150

GLOSARIO 153

ANEXOS 157

RESUMEN

El presente proyecto de tesis esta encaminado a realizar el desarrollo de Multihoming IPv6 caso práctico la cuál se ha implementado en la empresa “netXperts Consulting S.A”.

Para realizar la conexión de IPv6, se siguieron los pasos que se muestran a continuación:

- Realizar la configuración de los diferentes equipos que se utilizó para este desarrollo, con los siguientes Sistemas Operativos: Windows 2003 Server y Linux Mandrake 10.1. Esta configuración permitirá crear los túneles, los cuáles van a realizar la transición del Protocolo IPv4 a IPv6.
- Un Router Cisco 2500 para la conexión a Internet.

Además se realizó un estudio sobre la evolución y las nuevas formas de conectividad del Protocolo IPv6, el cuál posee mejores características sobre su antecesor, una de las principales es el mejor tratamiento en las comunicaciones y la información, por lo que para la implementación del presente proyecto se realizó conexiones a Internet por medio de túneles, demostrando así el uso de Multihoming a través de IPv6, lo que permitirá que los diferentes usuarios mantengan una conexión a Internet permanente.

CAPÍTULO I

INTRODUCCIÓN

En la actualidad las direcciones IPv4 se están saturando debido al rápido crecimiento del Internet, por lo cual se ha visto la necesidad de desarrollar la nueva versión de Ip que es IPv6, el cuál permitirá realizar nuevas asignaciones de direcciones a los usuarios, lo que ayudara en el mejor tratamiento y manejo de la información.

1.1 JUSTIFICACIÓN E IMPORTANCIA

Al reconocer la importancia del manejo de información y de los datos en la actualidad, se puede observar que las personas que acceden al Internet u otros servicios necesitan una mejor calidad de servicio, y una mayor expansión de las redes, es así como se ha visto necesario la realización de la puesta en marcha de una aplicación basada en **IPv6** ayudados por medio de lo que también se estudiará como es **Multihoming**. De esta manera permita agilitar, facilitar y personalizar los repositorios y forma de manejo de la información para dar soluciones a los requerimientos de los usuarios finales, es así que por medio de este proyecto se pretende proporcionar un mejor servicio al realizar el análisis del funcionamiento de una red como se mencionó anteriormente.

Es por este motivo que con la ayuda de herramientas que permitan implementar la red con **Multihoming** se realizará el desarrollo de este proyecto ya que brinda muchas soluciones ante el manejo eficaz de la información para todos los usuarios en una red.

1.2 OBJETIVOS

1.2.1 OBJETIVO GENERAL

Análisis, diseño e implementación en la Empresa “netXperts Consulting S.A.”, de una red basado en IPv6 con la aplicación de Multihoming para un mejor manejo de la información.

1.2.2 OBJETIVOS ESPECÍFICOS

- ✓ Estudiar las necesidades de la expansión de una red para el mejor manejo de la información.

- ✓ Especificar un esquema de multihoming y manejo de una red con IPv6.

- ✓ Implementar una red que valide el uso de multihoming dentro de la organización en cualquier momento por medio de la aplicación, configuración y utilización de nuevos equipos.

1.3 ALCANCE

El presente plan a desarrollarse y ser implementado, va a partir desde un estudio de IPv6 basándose en los conceptos de Multihoming para entender el funcionamiento, y por ende obtener una mayor aplicabilidad.

Una vez autorizada la ejecución de dicho plan, consecuentemente se realizará el análisis, diseño, implementación y pruebas respectivas, para así poder realizar y cumplir con todos los requerimientos de una red con la ayuda de nuevas tecnologías y mejores formas de utilizar éstas, basándose en la implementación de una red que puede ayudar a todos los sectores.

Previo al desarrollo de la implementación se procederá al levantamiento de la documentación para así verificar la aplicabilidad real y factibilidad del diseño y construcción de dicha red por medio de la integración de elementos que constituyan el Multihoming.

Se realizará la implementación y pruebas correspondientes, para verificar si los objetivos planteados se han cumplido en una forma correcta y completa, y así realizar un excelente desarrollo final.

1.4 METODOLOGÍA

Las metodologías a utilizarse en el presente proyecto son las siguientes:

1. Plan de Investigación como se detalla a continuación:

- ✓ Búsqueda y recopilación de información.
- ✓ Elaboración de resúmenes y paráfrasis del proyecto.
- ✓ Creación del diseño lógico, diseño físico de Multihoming con IPv6
- ✓ Análisis de los requerimientos y configuraciones de los equipos y los Sistemas Operativos:
    - Windows 2000 Server.
    - Windows 2003 Server
    - Linux Mandrake 10.1.
- ✓ Creación y Configuración de los Túneles para cada uno de los proveedores:
    - Hexago.
    - Consulintel.
- ✓ Pruebas preliminares de Multihoming con IPv6.
- ✓ Implementación y pruebas finales de Multihoming con IPv6.

2. Entrevista con el Director de Tesis para plantear los lineamientos a seguir para la Investigación Técnica.

CAPÍTULO II

MARCO TEÓRICO

2.1 Inicios y Evolución de Internet

INTERNET ha revolucionado el mundo de los ordenadores y las comunicaciones de una forma radical sin precedencia, representa uno de los mayores ejemplos de los beneficios obtenidos mediante la investigación y el desarrollo en el campo de la información. Los primeros indicios pueden encontrarse en una serie de memorándums escritos por J.C.R. Licklider (MIT Instituto de Tecnología en Massachusetts) en Agosto de 1962, que describía su idea como una red galáctica (Galactic Network), donde todos los ordenadores estarían conectados entre sí, Licklider fue el primer director del programa de desarrollo de ordenadores en el DARPA (Agencia de Investigación de Proyectos Avanzados de Defensa) en Octubre de 1962.

En 1965 Lawrence G. Roberts en colaboración con Thomas Merill conecta un ordenador TX-2 (Massachusetts) con un ordenador Q-32 (California) mediante la línea telefónica, creando la primera red de gran alcance (WAN, Red de Área Distribuida). En 1972 Ray Tomlinson introduce la primera versión de un programa de correo (e-mail) que permitía leer y escribir mensajes. Unos meses después, Roberts re-escribe el programa de correo añadiendo los servicios tales como:

reenvío de mensajes, la lectura selectiva de mensajes y el manejo de ficheros (FTP[1]).

Con la nueva red ARPANET[2], se empiezan a descubrir las limitaciones del NCP:

- ✓ CP[3] no proporciona fiabilidad a las comunicaciones, ni al mecanismo de control sobre el número de paquetes enviados, y el control de errores.
- ✓ NCP[4] no proporciona ningún mecanismo de direccionamiento (para ordenadores y/o redes).

De esta manera Kahn y Vincent Cerf deciden desarrollar una nueva versión del protocolo NCP, denominado Transmission Control Protocol/Internet Protocol (TCP/IP)[5], este nuevo diseño se basará en los siguientes principios:

1. Cada una de las redes conectadas debe ser independiente del resto.

2. Si un paquete no alcanza su destino, deberá ser retransmitido por el origen.

3. Se utiliza gateways o routers para la interconexión de redes, que tendrán la función de conducir los paquetes hacia los nodos de destino, lo que implica un direccionamiento dentro de una red.

4. Se deben permitir simultáneamente diferentes comunicaciones entre los ordenadores facilitando la interactividad.

5. Es necesario un sistema de direccionamiento global para todos los nodos.

FTP[1] File Transfer Protocol/Protocolo de Transferencia de Archivo
ARPANET[2] Red de la Agencia de Investigación de Proyectos Avanzado
CP[3] Control Protocol/Protocolo de Control
NCP[4] Protocolo de Control de Red
TCP/IP[5] Transmission Control Protocol/Internet Protocol Protocolo de Control de Transmisión/Protocolo de Internet

Se llegó a la conclusión que el protocolo debe subdividirse en dos: IP encargado de enviar paquetes individuales por la red hacia un nodo de destino, TCP que se encargará de proveer un control de flujo de los paquetes enviados, asegurando que lleguen a su destino de una forma correcta y ordenada.

Figura 2.1 Primer Diseño del TCP/IP

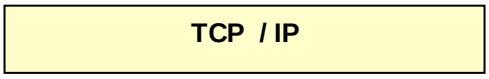
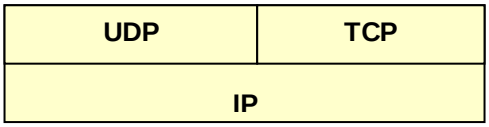
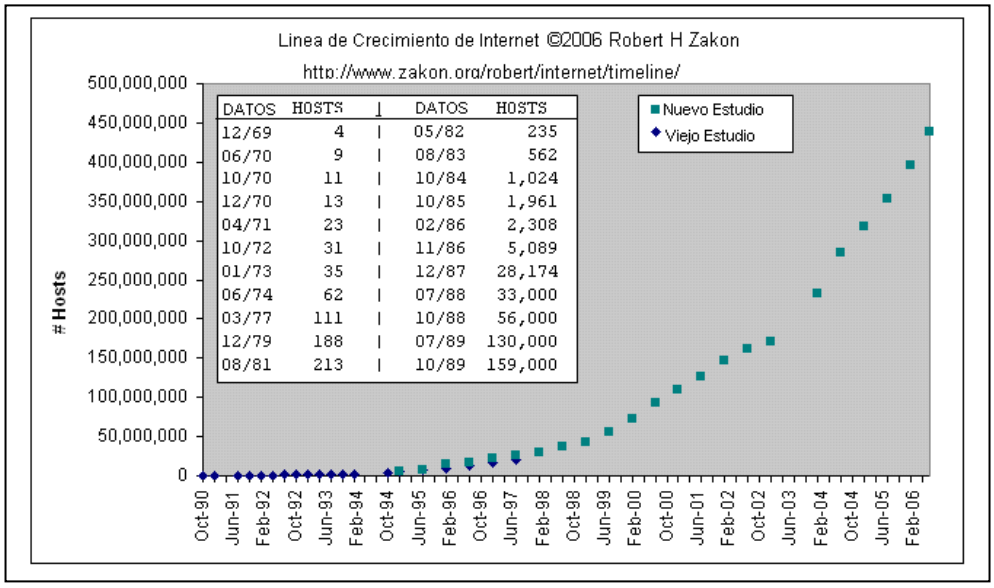


Figura 2.2 Estructura Jerárquica



En 1980 los protocolos TCP e IP fueron definitivamente adoptados por el Departamento de Defensa Americano, lo que permitió su integración en ARPANET.



DATOS	HOSTS		DATOS	HOSTS
12/69	4		05/82	235
06/70	9		08/83	562
10/70	11		10/84	1,024
12/70	13		10/85	1,961
04/71	23		02/86	2,308
10/72	31		11/86	5,089
01/73	35		12/87	28,174
06/74	62		07/88	33,000
03/77	111		10/88	56,000
12/79	188		07/89	130,000
08/81	213		10/89	159,000

Figura 2.3 Crecimiento de Internet

Según FNC (Federal Networking Council): INTERNET hace referencia a un sistema global de información en que se está lógicamente conectado por un sistema global y único de direcciones basados en el Internet Protocol (IP).

- Resumen de la evolución histórica de INTERNET desde 1950 hasta el año 2000.

Tabla 2.1 Evolución Histórica de Internet

1950. ➢ 1957 URSS lanza el satélite Sputnik. **1960.**
➢ 1962 J.C.R. Licklider acuña el concepto de *Red Galáctica.* ➢ 1966 Se presenta el primer plan para la creación de ARPANET. ➢ 1969 Creación de ARPANET con dos nodos iniciales. UCLA y SRI[6]. Primer RFC **1970.**
➢ 1970 Publicación del protocolo de ARPANET. Adopción del protocolo NCP. ➢ 1972 Mejora del e-mail. Elección del signo @. Publicación del protocolo TELNET [RFC318]. ➢ 1973 El 75% del uso de ARPANET son e-mail's. Ethernet. Publicación del FTP [RFC454]. ➢ 1974 Publicación de la primera versión del TCP/IP.

- 1978 División del protocolo TCP/IP en TCP e IP. **1980.**

- 1980 El 27 de Octubre un virus produce una parada total de ARPANET.
- 1983 Substitución de NCP por TCP e IP. División en ARPANET y MILNET[7].
- 1984 Introducción del DNS[8]. Hay conectados más de 1.000 nodos.
- 1986 Creación IETF[9] y IRTF[10]. Primer acceso no gubernamental (Freenet).
- 1988 Creación IANA[11] y CERT[12]. Conexión a FIDONET[13], NSF[14] impulsa la privatización.
- 1989 Se superan los 100.000 nodos conectados. **1990.**

- 1990 Nace INTERNET substituyendo a ARPANET. Aparece el servicio de búsqueda Archie.
- 1991 El CERN presenta HTML, base del WWW. P. Zimmerman desarrolla el PGP[15].
- 1992 Creación de la ISOC[16]. Ya hay más de 1.000.000 de nodos conectados a INTERNET.
- 1993 NSF crea INTERNIC[17] para gestionar el registro de dominios.
- 1995 www se convierte en el servicio más utilizado. El Registro de un dominio cuesta $50.
- 1998 Se presenta la privatización del DNS. Gran auge del comercio electrónico (e-comerce).
- 1999 Aparición del SETI@Home, búsqueda de vida extraterrestre utilizando INTERNET. **2000.**

6-17 pag. 153,154 GLOSARIO

2.2 IPv4

2.2.1 DEFINICIÓN

IPv4 es el protocolo de direccionamiento de Internet que hace posible la interconexión con cada computadora o recursos conectado a la red. Desarrollado en 1975, está basado en las direcciones IP convencionales, formadas por cuatro grupos de 8 bits (32 bits). IPv4 ofrece un servicio de datos basado en datagramas no fiable, no orientado a conexión, por lo que se usa con TCP[18] que ofrece la confiabilidad que hace falta.

Los protocolos IP definen la forma en que las subredes se interconectan y la manera en que funcionan los dispositivos de interconexión. IP define la manera que se enrutan los paquetes entre las redes; cada nodo tiene una dirección IP diferente. Para efectuar su labor, los protocolos IP se apoyan en diversos conceptos como son:

- ✓ DNS (Domain Name Servers)
- ✓ Direcciones Internet (Direcciones IP)
- ✓ Paquetes IP
- ✓ Enrutamiento IP/Protocolos de Enrutamiento
- ✓ ICMP (Internet Control Message Protocol)

[18] TCP Transmission Control Protocol/Protocolo de Control de Transmisión.

IPv4 tiene entre otras funciones la designación de las direcciones de todos y cada uno de los nodos que componen la red, y la identificación de cualquier usuario.

2.2.2 Limitaciones de IPv4

- ✓ Se requiere soportar aplicaciones de videoconferencia, multimedia en tiempo real lo que limita el crecimiento.
- ✓ Se requieren mecanismos de seguridad, ya que está es opcional.
- ✓ Difícil de administrar la parte Móvil.
- ✓ Escasez de direcciones IP.
- ✓ En la actualidad el ruteo es ineficiente.

2.2.3 Cabecera IPv4

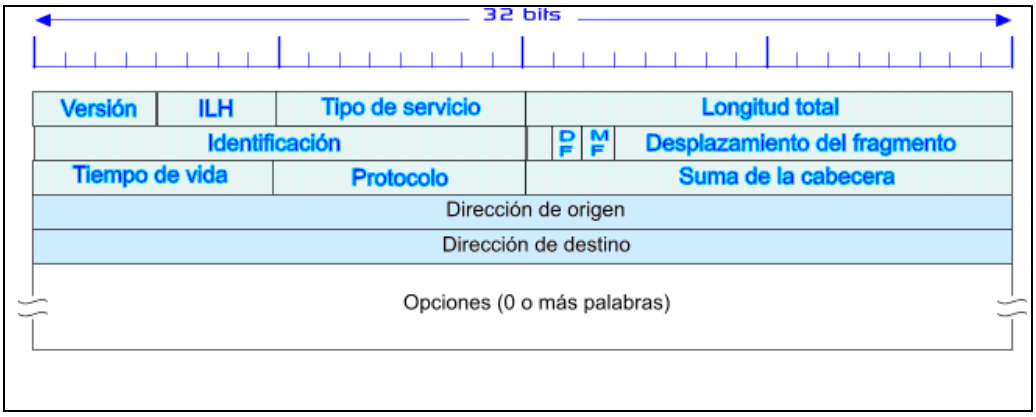


Figura 2.4 Cabecera IPv4

- ✓ **Versión:** Tamaño 4 bits, de la versión del IP que se está utilizando.

- ✓ **Tamaño de la Cabecera (ILH[19]):** Tamaño 4 bits, es la longitud de la cabecera, en palabras de 32 bits. El valor mínimo para la longitud es 5 y el máximo es 15.

- ✓ **Tipo de Servicio:** Tamaño 8 bits, indica la calidad del servicio deseado especificado como un protocolo de la capa superior, este campo se utiliza para la asignación de la precedencia, retraso, rendimiento de procesamiento y confiabilidad.

- ✓ **Longitud Total:** Tamaño 16 bits, especifica la longitud en octetos del paquete entero del IP, incluyendo los datos y la longitud de la cabecera.

- ✓ **Identificación:** Tamaño 16 bits, contiene un número entero que identifique el datagrama actual.

- ✓ **Flags:** Tamaño 3 bits, del cual los dos bits (menos significativos) de orden inferior controlan la fragmentación. El bit de peso inferior (DF) especifica si el paquete puede ser hecho fragmentos. El bit medio (MF) especifica si el paquete no es fragmento. El tercer bit no se utiliza.

- ✓ **Posición del Fragmento:** Tamaño 13 bits, indica la posición de los datos que permite que el proceso del IP de la destinación reconstruya correctamente el datagrama original.

ILH[19] Internet Header Length/Longitud de Cabecera Internet

- ✓ **Tiempo de Vida:** Tamaño 8 bits, indica el máximo de segundos que un paquete puede circular en una red, se decrementa gradualmente hasta 0, si es 0 se desecha dicho paquete.

- ✓ **Protocolo:** Tamaño 8 bits, indica qué protocolo de la capa superior recibe los paquetes entrantes después de que el proceso sea completado.

- ✓ **Checksum de la Cabecera:** Tamaño 16 bits, se recalcula cada vez que algún nodo cambia alguno de sus campos (por ejemplo, el Tiempo de Vida). El método de cálculo (intencionadamente simple) consiste en sumar el complemento a 1 de cada palabra de 16 bits de la cabecera y hacer el complemento a 1 del valor resultante.

2.2.4 Direccionamiento en IPv4

Para dotar de flexibilidad al sistema, se dispuso que existieran cinco modelos o clases distintas de direcciones: A, B, C, D y E. Dicho de otro modo, el espacio total de direcciones posibles se dividió en cinco categorías o clases predefinidas. Cada clase asigna un espacio distinto para la identificación de red y de host, dentro de los 32 bits disponibles.

El principio de funcionamiento es el siguiente: al recibir un paquete IP un enrutador, este necesita conocer la dirección de destino para reenviarlo, para lo que examina los cuatro primeros bits.

Una vez conocida el tipo de dirección se puede establecer la dirección de destino y el paquete es reenviado al router que pueda realizar esta operación. Cuando el paquete llega finalmente a su destino se utiliza el número identificativo de la dirección de host y se le envía.

- ✓ **Clase A.** Esta clase se puede representar hasta 2^24 computadoras incluidas en cada una de las 2^7 posibles redes.

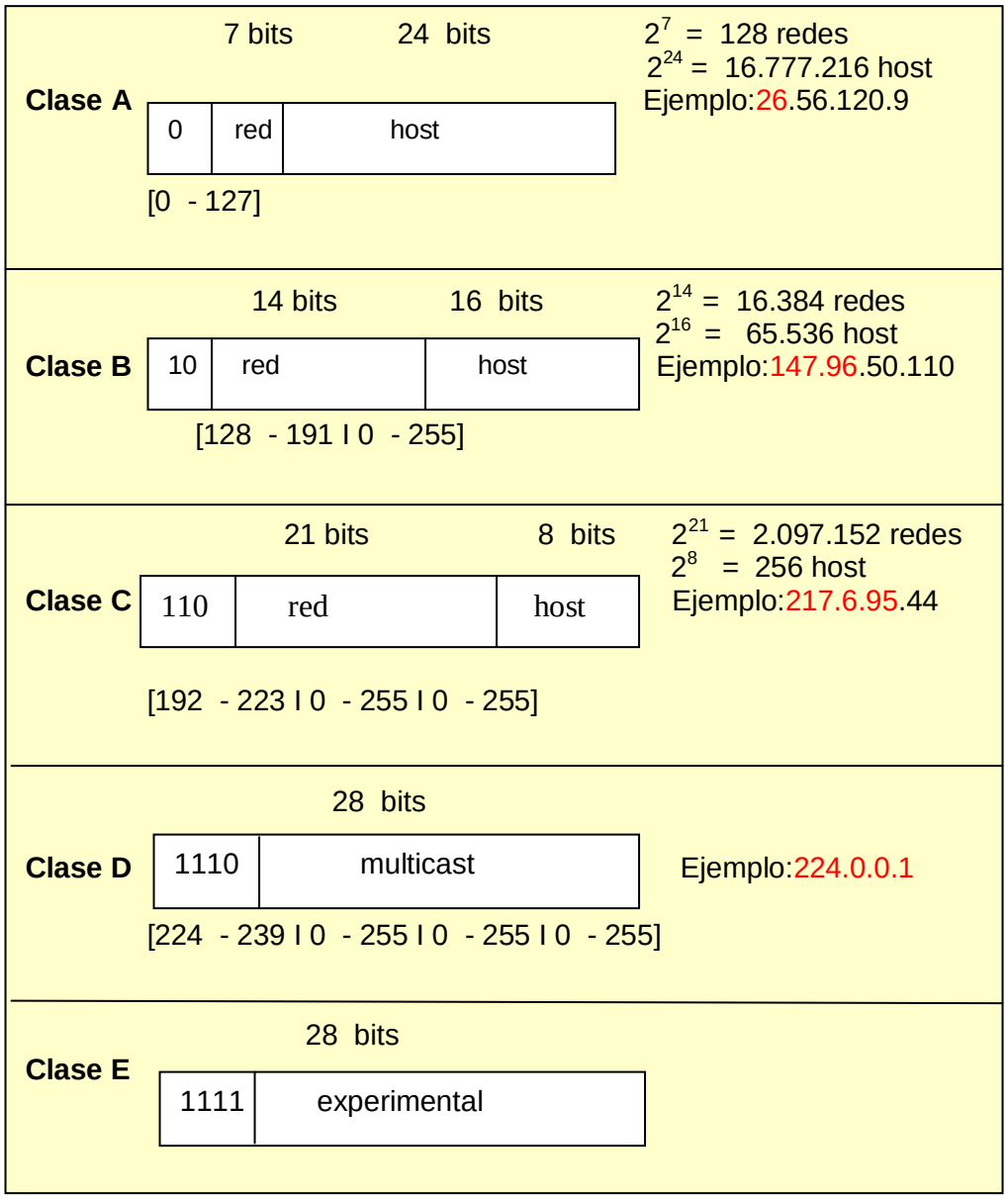
- ✓ **Clase B.** En esta clase se puede representar hasta 2^16 computadoras incluidas en cada una de las 2^14 posibles redes.

- ✓ **Clase C.** En esta clase se puede representar hasta 2^8 computadoras incluidas en cada una de las 2^21 posibles redes.

- ✓ **Clase D y E.** Las direcciones que forman parte de la clase D son utilizadas por los protocolos que hacen uso de la comunicación tipo multicast.

  Las direcciones que forman parte de la clase E son utilizadas para experimentación.

Tabla 2.2 Cuadro de Resumen Direccionamiento IPv4



En cuanto a direcciones IP no es posible utilizar las siguientes direcciones:

- La primera dirección del rango es la dirección de red (suele acabar en 0).
- La última dirección del rango es la dirección de broadcast (difusión), suele acabar en 255.

- **Clase A:**

  10.0.0.0 10.255.255.255.

  127.x.y.z Dirección de Loopback.

- **Clase B:**

  172.16.0.0 172.31.255.255.

- **Clase C:**

  192.168.0.0 192.168.255.255.

- **Clase D:**

  Se utilizan para Multicast.

- **Clase E:**

  Se utilizan para direcciones Experimentales.

Tabla 2.3 Cuadro de Clases

Clase de dirección IP	Primer intervalo de dirección de octeto	Cantidad de host por red
Clase A	0 - 127	16,777,216
Clase B	128 - 191	65,535
Clase C	192 - 223	254
Clase D (Multicast)	224 - 239	No es aplicable

Aunque en un principio la capacidad de direccionamiento del modelo IPv4 parecía más que suficiente. **Por ejemplo**, a pequeñas redes con varios cientos de nodos se les asignaron direcciones únicas clase B en vez de haberles asignado varias clase C, en consecuencia se desaprovechó el espacio de direcciones, con lo que las tablas globales de direcciones en Internet han crecido desmesuradamente.

ARIN reserva las direcciones de Clase A, a empresas de gran envergadura como, por ejemplo, Hewlett Packard, las direcciones de Clase B para las medianas empresas y las direcciones de Clase C para todos los demás solicitantes.

2.3 CIDR (Classless Inter Domain Routing)

2.3.1 Definición

Se comenzó a introducir en 1993, y es la última mejora al sistema por el cual se interpretan las direcciones IP, reemplaza a la anterior generación de direcciones IP, y permite una mayor flexibilidad a la hora de dividir rangos de direcciones en redes separadas.

Es un método de direccionamiento IP, en donde no importan las clases, lo que importa es el prefijo, de ahí el término "classless", sin clase. Implementa un método de enrutamiento inter dominios sin clases, ya que las redes de clase B son demasiado grandes y las de clase C son demasiado pequeñas, CIDR[20] permite

CIDR[20] Classless Inter Domain Routing/Ruteo de Interdominio sin Clases

unir varias redes de clase C contiguas, marcando los bits de la máscara de red como máquina (bit a 0). Tienen una máscara que puede ser cualquier número de bits, e intentan resolver el problema del agotamiento de direcciones. Las máscaras no tienen que ser múltiplos de 8 bits.

Cuando un ruteador recibe un datagrama este hace un AND de la dirección IP destino con la máscara correspondiente a cada una de las redes y selecciona aquella que corresponde a la dirección de base. CIDR utiliza esta misma idea para todas las direcciones, por lo que no necesita la distinción entre las clases A, B y C para enrutar los datagramas. Al establecer conexiones con las redes IPv6 de los afiliados conectados, utilizar filtros con el fin de anunciar únicamente los prefijos delegados.

Por ejemplo, un bloque de 8 direcciones clase C que inicia en 198.125.0.0 hasta 198.131.255.255.

Nombre de la Organización: Energy Sciences Network

Identificación: ENSN

Dirección: Berkeley Lab

Dirección: 1 Cyclotron Road MS 50A3111

Ciudad: Berkeley

Estado/Provincia: CA

Código Postal: 94720

País: USA

2.3.2 Prefijo de una Dirección IP “CIDR”

A medida que el número de redes "sub-redes y/o redes" se incrementa, la tabla de rutas administradas por el enrutador aumenta proporcionalmente hasta llegar al punto de colapsar la capacidad de procesamiento del enrutador, cuya función principal es incluir a un grupo de redes en una dirección IP. Un prefijo determina el bloque de direcciones IP y su nivel jerárquico. **Por Ejemplo:**

192.40.1.0/24
192.40.2.0/24
192.40.3.0/24

Para poder hacer uso de la técnica CIDR el enrutador debe elegir de la tabla de rutas la red que posea el mayor número de bits continuos iguales a la dirección IP destino "Longest Match Prefix", para ello debe definirse en el enrutador el bloque de direcciones IP "Agregación". Haciendo uso de la notación CIDR las siguientes redes clase A, B o C se pueden incluir en el bloque:

Tabla 2.4 Prefijo de una Dirección IP "CIDR"

Prefijo	Notación punto decimal	# de redes clase A, B o C
/1	128.0.0.0	128 redes clase A
/2	192.0.0.0	64 redes clase A
/3	224.0.0.0	32 redes clase A
/4	240.0.0.0	16 redes clase A

Prefijo	Notación punto decimal	# de redes clase A, B o C
/5	248.0.0.0	8 redes clase A
/6	252.0.0.0	4 redes clase A
/7	254.0.0.0	2 redes clase A
/8	255.0.0.0	1 redes clase A
/9	255.128.0.0	128 redes clase B
/10	255.192.0.0	64 redes clase B
/11	255.224.0.0	32 redes clase B
/12	255.240.0.0	16 redes clase B
/13	255.248.0.0	8 redes clase B
/14	255.252.0.0	4 redes clase B
/15	255.254.0.0	2 redes clase B
/16	255.255.0.0	1 redes clase C
/17	255. 255.128.0	128 redes clase B
/18	255. 255.192.0	64 redes clase B
/19	255. 255.224.0	32 redes clase B
/20	255. 255.240.0	16 redes clase B
/21	255. 255.248.0	8 redes clase B
/22	255. 255.252.0	4 redes clase B
/23	255. 255.254.0	2 redes clase B
/24	255.255.255.0	1 redes clase C
/25	255. 255. 255.128	1/2 de redes clase C
/26	255. 255. 255.192	1/4 de redes clase C
/27	255. 255. 255.224	1/8 de redes clase C
/28	255. 255. 255.240	1/16 de redes clase C

Prefijo	Notación punto decimal	# de redes clase A, B o C
/29	255. 255. 255.248	1/32 de redes clase C
/30	255. 255. 255.252	1/64 de redes clase C
/31	255. 255. 255.254	1/128 de redes clase C
/32	255. 255. 255.255	1/256 de redes clase C

2.4 SUBNETTING

Consiste en tomar una dirección IP y dividirla en tantas subredes como sean necesarias y obtener la cantidad de host que se necesitan o al menos algo cercano; surgió por el agotamiento de las direcciones IP, clase A, clase B además el costo de cada una es muy alto.

La división en subredes o subnetting da la posibilidad de crear múltiples redes, partiendo de una sola dirección de red clase A, B o C, la máscara de subred identifica qué porción de los cuatro octectos está determinando la red y subred y qué porción está determinando al host. Subnetting ayuda a fragmentar las redes de tipo A, B y C en subredes para expandir el espacio de direccionamiento dentro de una organización, además ayuda a compartir una dirección en red IP entre varias redes físicas lo cual ayuda a aprovechar al máximo una misma dirección IP de red sobre varias redes físicas pertenecientes a la misma organización, es decir los routers dentro de una red necesitan conocer las subnets de su red; esto se

hace similar a la partición de una dirección IP en red y host, cada campo en la dirección IP no es fijo.

2.4.1 Tipos de Subnetting

2.4.1.1 Estático

Consiste en que todas las subredes de la red dividida empleen la misma máscara de red, esto es simple de implementar y de fácil mantenimiento, pero implica el desperdicio de direcciones para redes pequeñas.

2.4.1.2 Longitud Variable

Las subredes que constituyen la red pueden hacer uso de diferentes máscaras de subred. Una subred pequeña con solo unos pocos host necesita una máscara que permita estar dentro de dicha red. Una subred con muchos puede requerir una máscara distinta para direccionar esa elevada cantidad de host. La posibilidad de asignar máscaras de subred de acuerdo a las necesidades individuales de cada subred ayuda a conservar las direcciones de la red.

2.5 SUPERNETTING

Es un proceso el cuál usa una máscara de bits para agrupar subredes con clase como una sola dirección de red es decir, cuando se trabaja con supernetting

implica que se utiliza una máscara con ceros y se realiza el mismo salto para distintas direcciones esto se hace cuando un conjunto de direcciones consecutivas necesita tener los 8,16,24 bits de la dirección que sean iguales. Los protocolos de encaminamientos que utilizan esta técnica con las máscaras se denominan CIDR, las tablas de direccionamiento deben estar ordenadas y pueden hacerse manualmente.

Debido a la disponibilidad limitada de direcciones de red en la clase B, las autoridades del Internet han proporcionado la habilidad para consolidar múltiples direcciones de clase C en una red lógica, para eliminar la necesidad de mantener el registro de cada dirección de red en la tabla de ruteo sobre los routers de Internet se usa una técnica llamada Classless Inter Domain Routing (CIDR), para descartar las múltiples direcciones de red en una entrada simple que representa a todas las direcciones asignadas de clase C. Para usar supernetting, Internic ubica 8 direcciones de red clase C. **Por Ejemplo:**

192.168.168.0	192.168.171.0	192.168.174.0
192.168.169.0	192.168.172.0	192.168.175.0
192.168.170.0	192.168.173.0	

Estas direcciones son combinadas usando la máscara de subred 255.255.248.0, como la máscara de subred está particionando la dirección IP esta aparece como perteneciente a la misma subred. Esto significa que los host con **IP = 192.168.168.11** y el de **IP = 192.168.174.33** están ubicados en la misma subred.

2.5.1 Supernetting (Sumarización)

Reduce el prefijo hacia la izquierda y permite reducir el tamaño de las tablas de ruteo y tráfico de intercambio de información de ruteo al posibilitar que un router anuncie y tenga una única entrada en la tabla para un conjunto de rutas.

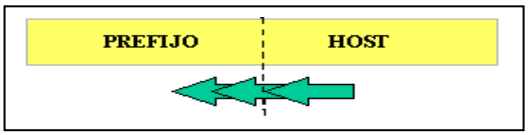


Figura 2.5 Supernetting (Sumarización)

Para las tres redes, se dispone de una única dirección clase C: 202.2.2.0.

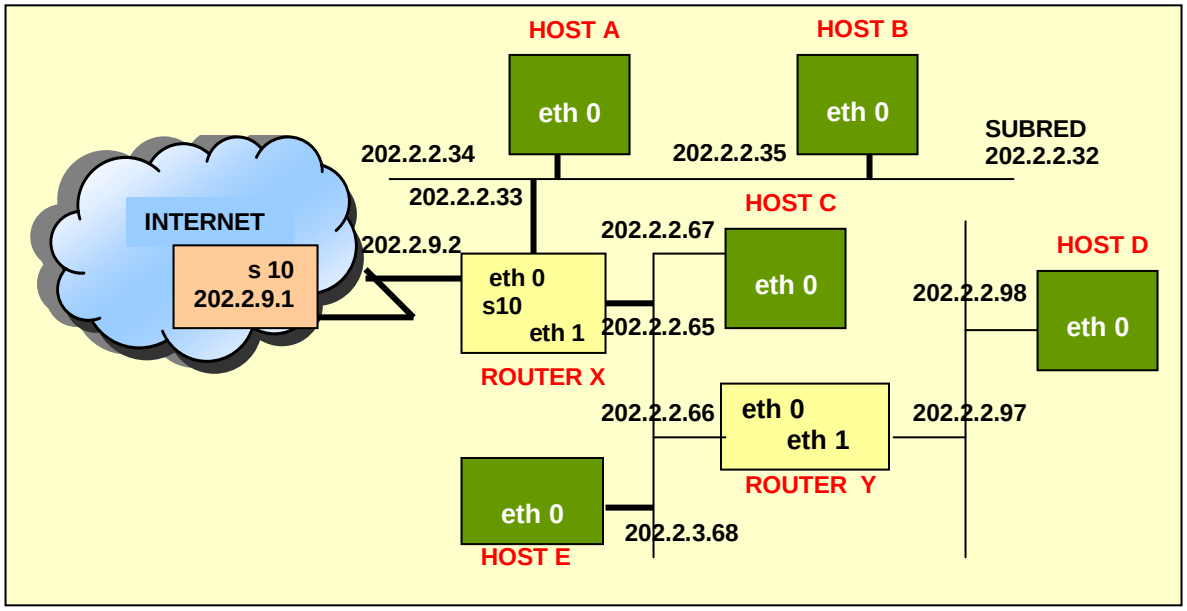


Figura 2.5.1 Supernetting (Sumarización)

Crecimiento previsto: hasta 5 subredes de no más de 20 hosts cada una Máscara utilizada: 255.255.255.224 (FF.FF.FF.E0) (3 bits para subred = 6 subredes).

Subredes: 001 CA.02.02.20 202.2.2.32

010	011	100	101	110
CA.02.02.40	CA.02.02.60	CA.02.02.80	CA.02.02.A0	CA.02.02.C0
202.2.2.64	202.2.2.96	202.2.2.128	202.2.2.160	202.2.2.192

Subredes utilizadas: 202.2.2.32, 202.2.2.64, 202.2.2.96

ROUTER X

RED DESTINO	D/I	ROUTER	MASCARA	IF
202.2.2.32	D	.....	255.255.255.224	eth 0
202.2.2.64	D	.....	255.255.255.224	eth 1
202.2.2.96	I	202.2.2.66	255.255.255.224	eth 1
default	I	202.2.9.1	.....	s10

ROUTER Y

RED DESTINO	D/I	ROUTER	MASCARA	IF
202.2.2.32	I	202.2.2.65	255.255.255.224	eth 0
202.2.2.64	D	.....	255.255.255.224	eth 0
202.2.2.96	D	.....	255.255.255.224	eth 1
default	I	202.2.2.65	.....	eth 0

ROUTER DE INTERNET

RED DESTINO	D/I	ROUTER	MASCARA	IF
202.2.2.0	I	202.2.9.2	255.255.255.0	s10

HOST A ó B

RED DESTINO	D/I	ROUTER	MASCARA	IF
202.2.2.32	D	.....	255.255.255.224	eth 0
202.2.2.64	I	202.2.2.33	255.255.255.224	eth 0
202.2.2.96	I	202.2.2.33	255.255.255.224	eth 0
default	I	202.2.2.33	.....	eth 0

Figura 2.5.2 Supernetting (Sumarización)

2.6 VLSM (Variable Length Subnet Mask Mascara de Subred de Longitud Variable)

Las características de la máscara de subred de longitud variable son:

- El uso de las direcciones IP es más eficaz.
- Subredes de subredes, soporta subredes no contiguas (subredes separadas por parte de otra subred).

Reglas de asignación de direcciones:

- El espacio de direcciones en el que el campo subred es 0 ó -1 para una máscara de una cierta longitud, puede ser utilizado en una subred con una máscara de menor longitud.
- Bajo una cierta máscara, las direcciones con campos de subred o host 0 ó -1 no pueden ser utilizados.
- El espacio de direcciones asignado bajo una máscara no puede ser asignado bajo otra máscara (prefijo más largo).
- Mayor capacidad de resumen de ruta.

La configuración de VLSM es más bien organizativa a nivel esquemático, se debe tomar en cuenta los esquemas de direccionamiento.

2.6.1 Ventajas

- Impide el mal uso del espacio de direcciones.
- Aligera la carga de recursos en los routers.
- Permite una jerarquía más ordenada.
- Sólo es posible en protocolos de enrutamiento sin clase.
- En redes muy divididas, podría ocasionar conflictos en tablas de enrutamiento.
- Implica un orden de direccionamiento cuidadoso.

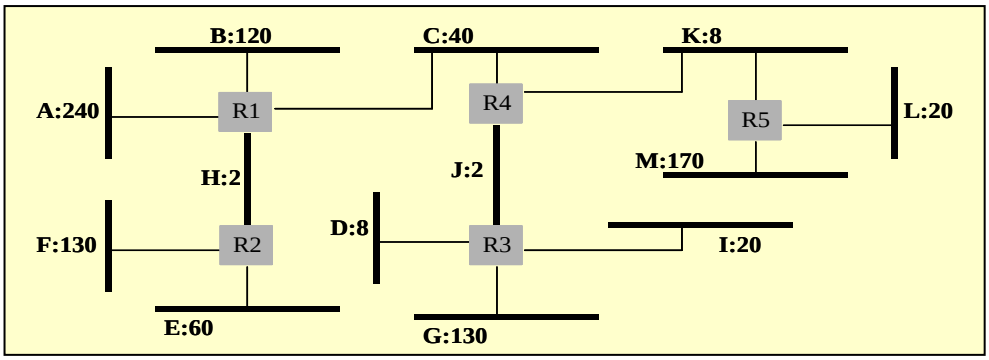


Figura 2.6 VLSM (Máscara de Subred de Longitud Variable)

2.7 PROXY

Un servidor proxy es un equipo intermediario situado entre el sistema del usuario e Internet puede utilizarse para registrar el uso de Internet y también para bloquear el acceso a una sede Web. El servidor proxy bloquea algunas sedes o páginas Web por diversas razones, además son un mecanismo de seguridad implementado por el ISP o los administradores de la red en un entorno de Intranet

para desactivar el acceso o filtrar las solicitudes de contenido para ciertas sedes Web consideradas ofensivas o dañinas para la red y los usuarios.

Algunas características son:

- Mejora el rendimiento.
- Guarda en la memoria caché las páginas Web a las que acceden los sistemas de la red durante un cierto tiempo. Cuando un sistema solicita la misma página web, el servidor proxy utiliza la información guardada en la memoria caché en lugar de recuperarla del proveedor de contenidos. De esta forma, se accede con más rapidez a las páginas Web.

Los servidores proxy además son capaces de controlar el tipo de tráfico que fluye a través de la red (correo electrónico, páginas web, archivos de ftp, etc.) y supervisan la seguridad en la red, la ventaja es que se obtiene mayor velocidad de transmisión al no tener que buscar la página. El uso de un servidor proxy puede aumentar considerablemente la velocidad con la que se navega.

2.8 NAT (Network Address Translation Traducción de Dirección de Red)

La Traducción de Direcciones de Red (NAT) cambia las direcciones IP en el encabezado IP, NAT reemplaza la dirección origen con una dirección ruteable permitiendo a hosts con direcciones privadas accesar a Internet, además provee de conectividad transparente, escalable y bidireccional entre distintos lugares de la misma empresa.

La característica especial de todos los tipos de NAT son las cinco tuplas que identifican de forma inequivoca una conexión: protocolo, IP origen y puerto, IP destino y puerto. Esta información la debe mantener el sistema o router en una de sus tablas. Una interfaz en el ruteador puede ser definida como inside u outside.

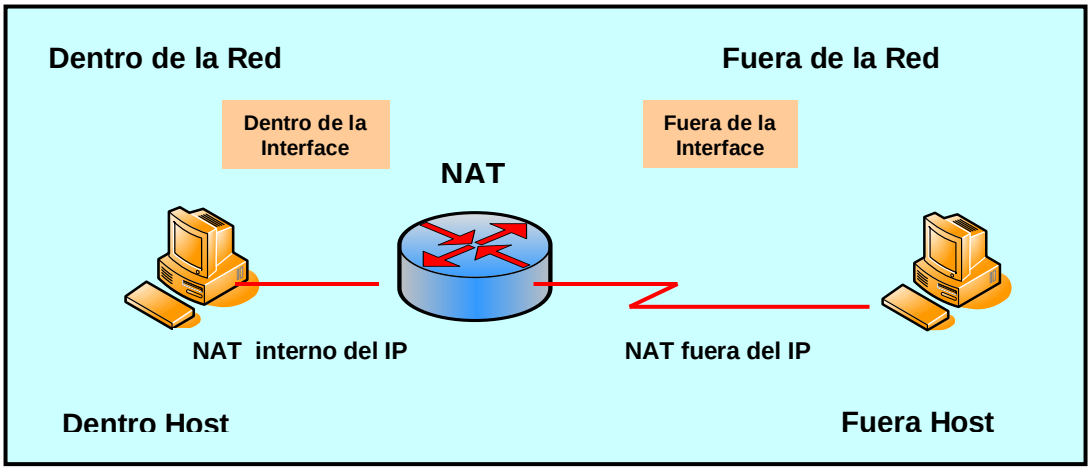


Figura 2.7 Dirección de NAT

✓ **IP Nat Inside Source**

Se utiliza cuando se tienen hosts con dirección IP que no deben ser vistos en la red externa.

✓ **IP Nat Outside Source**

Se utiliza cuando se están usando los mismos IP en ambas redes, interna y externa ó cuando se tienen varios gateways. Las direcciones IP privadas que se pueden utilizar para la red interna son:

- ✓ **Clase A:** 10.x.x.x
- ✓ **Clase B rango**: 172.16.x.x – 172.31.x.x
- ✓ **Clase C rango:** 192.168.1.x – 192.168.254.x

Se puede usar una traducción de NAT es 1 a 1 ó de varios a 1.

- Las traducciones 1 a 1 (NAT) asignan un diferente IP a cada traducción.
- Las traducciones varios a 1 (PAT) pueden asignar el mismo IP para cada traducción.

NAT y sus modalidades **PAT Y RPAT** ofrecen una manera rápida y eficaz de ampliar el acceso seguro a Internet en redes privadas nuevas y existentes, sin tener que esperar una nueva y mejor estructura de direcciones IP. Estos ofrecen mayor flexibilidad y funcionamiento que el uso alternativo de proxies y se ha convertido en el standard para el acceso compartido.

2.9 PAT (Port Address Traslation Traducción de Direcciones de Puerto)

Básicamente consiste en que el router cuando le solicitan información a través de un puerto TCP determinado, éste le pasa la solución al servidor apropiado ubicado dentro de la red y vuelve a enviar la respuesta del servidor hacia el usuario de Internet que lo solicitó.

Este sistema es muy utilizado por empresas que quieren tener presencia en Internet, la mayor ventaja es que toda la red interna puede tener acceso a Internet, esto es importante porque como se mencionó anteriormente las direcciones IP han llegado a ser excesivamente costosas, además resuelve conflictos en direcciones IP reemplazando direcciones sin registrar en paquetes IP por direcciones

registradas, que son encaminadas en Internet. Las direcciones sin registrarse o direcciones privadas IP, son utilizadas en la mayoría de redes internas.

El número de conexiones está limitado por el número de puertos TCP disponibles como:

- Dirección fuente.
- Puerto fuente, número 3021.
- Puerto de destino.

Un problema especial es que en algunos servicios de ciertos ordenadores sólo se aceptan conexiones que vienen de puertos privilegiados para asegurarse de que no vienen de un usuario no deseado, la mayoría de las implementaciones de PAT usan puertos no privilegiados para evitar interferir con las conexiones “regulares” a esos puertos, habitualmente utiliza puertos en el rango superior, el cuál típicamente inicia el puerto 61.000 y termina en 61.000 + 4096.

2.10 RPAT (Reverse Port Address Translation Traducción de Dirección de Puerto Reverso)

Permite usar una sola computadora conectada a Internet con una dirección IP “real” como una entrada para máquinas que no están conectadas y sin registro de dirección IP privada. La entrada con dirección IP pública maneja paquetes verificados desde Internet a direcciones privadas de las computadores en la red interna o privada. Utiliza el mismo dispositivo que en el paquete del protocolo

TCP/IP para multiplexación inversa es decir utiliza un comando pasivo comúnmente utilizado para conectividad FTP. Para utilizar RPAT un cliente elige dos puertos TCP para su propio uso, el primer puerto identifica a un canal de comando y el segundo a un canal de datos. El usuario abre el puerto del canal comando para contactar con el **RPAT** pasivo, con el propósito de descubrir la dirección y la edición del comando pasivo.

2.11 IPv6

2.11.1 Definición

IPv6 es la abreviatura de “Internet Protocol Versión 6”. Se trata del protocolo de “la nueva generación”, diseñado por la IETF (Internet Engineering Task Force) para reemplazar la versión actual del protocolo de Internet IPv4. Aunque IPv4 demostró ser elástico y resistente a pesar de los años, está comenzando a traer problemas, por lo que IPv6 soluciona muchos de éstos problemas. Una característica esencial de IPv6 es soportar el gran aumento de dispositivos conectados a Internet en tiempo real, permitiendo calidad a nivel de paquetes. Además usa direcciones de 128 bits, con esto cualquier dispositivo capaz de conectarse a Internet obtendrá una dirección IPv6 propia.

El cambio de IPv4 a IPv6 ya ha comenzado (inicialmente en los servidores raíz de Japón (.jp) y Corea (.kr)); existe una serie de mecanismos que permite la migración progresiva. Entre los más destacables son los túneles.

Actualmente el protocolo IPv6 está soportado en la mayoría de los sistemas operativos modernos, en algunos casos como una opción de instalación. Las mejoras que aporta IPv6 son:

- ✓ Convivencia con IPv4, que hará posible la migración.
- ✓ Gran cantidad de direcciones, que hará virtualmente imposible que queden agotadas.
- ✓ Direcciones unicast, multicast y anycast.
- ✓ Soporte de audio y vídeo, que permite establecer rutas de alta calidad.
- ✓ Formato de la cabecera más flexible que IPv4, para agilizar el encaminamiento.
- ✓ Nueva etiqueta de flujo para identificar paquetes de un mismo flujo.
- ✓ Etiqueta clase de tráfico, para soportar calidad de servicio (QoS[21]).
- ✓ No se usa checksum, ni fragmentación, ni reensamblado.
- ✓ Nuevas características de seguridad. IPSEC formará parte del standard.
- ✓ Nueva versión de ICMP[22] y desaparición del IGMP[23].
- ✓ Auto configuración de los nodos finales, que permitirá a un equipo aprender automáticamente una dirección IPv6 al conectarse a la red.
- ✓ Movilidad incluida en el standard, que permitirá cambiar de red sin perder la conectividad.

Los principales cambios entre las dos versiones son los siguientes:

[21] **QoS Quality of Service/Calidad de Servicio**
[22] **ICMP Internet Control Message Protocol/Protocolo de Control de Mensajes de Internet**
[23] **IGMP Internet Group Management Protocol/Protocolo de Administración del Grupo Internet**

- ✓ **Mayor número de direcciones de Internet:** El tamaño de las direcciones IP cambia de ser de 32 bits a un tamaño de 128 bits.
- ✓ **Simplificación del Formato de los Encabezados:** Algunos de los campos de IPv4 se han eliminado ó se han hecho opcionales.
- ✓ **Soporte Mejorado para Extensiones y Opciones:** Cambios en la forma en que los encabezados de opciones están codificados.
- ✓ **Etiquetamiento de Flujos:** Tratamiento especial para los paquetes.
- ✓ **Autenticación y Privacidad:** Extensiones para el manejo de autenticación.

2.11.2 Cabecera IPv6

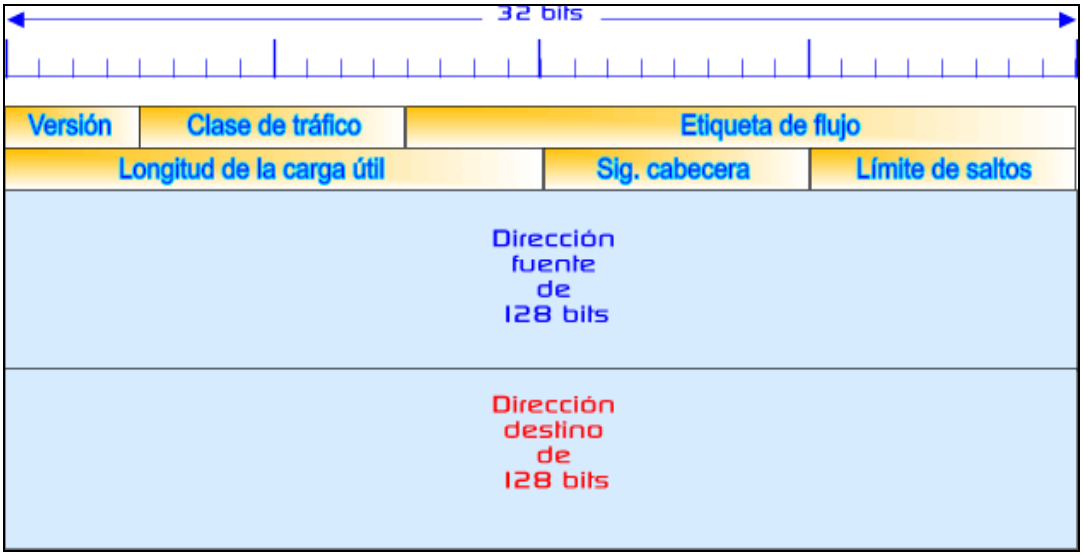


Figura 2.8 Cabecera IPv6

- ✓ **Versión:** Tamaño 4 bits, versión del Protocolo de Internet IPv6.
- ✓ **Clase de Trafico (Traffic Class):** Tamaño 8 bits, es el tráfico de clase.

- ✓ **Etiqueta de Flujo (Flow Label):** Tamaño 20 bits, es el que contiene información a ser usada por los routers para asociar un paquete con un flujo específico y prioridad.
- ✓ **Longitud de Datos (Length of Data):** Tamaño 16 bits, longitud de la carga útil de IPv6.
- ✓ **Siguiente Cabecera (Next Header):** Tamaño 8 bits, identifica la siguiente cabecera la cual seguirá a la cabecera principal.
- ✓ **Limite de Saltos (Hop Limit):** Tamaño 8 bits, análogo al campo tiempo de vida (Time-To-Live) de IPv4.
- ✓ **Dirección de Origen (Source Address):** Tamaño 128 bits, dirección de origen del paquete.
- ✓ **Dirección de Destino (Destination Address):** Tamaño 128 bits, dirección del destinatario del paquete, posiblemente no el destinatario final.

2.11.2.1 Tipos de Cabecera de Extensión IPv6

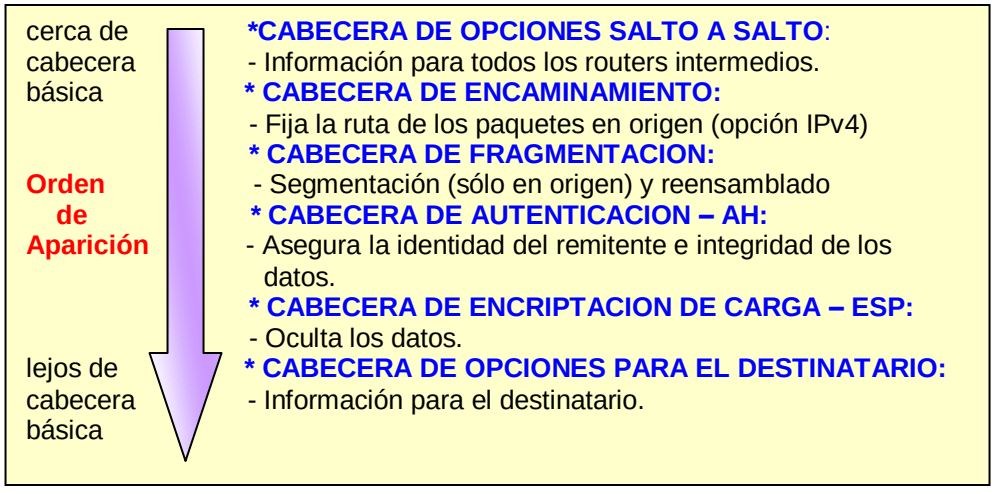


Figura 2.9 Tipos de Cabeceras

- ✓ **Cabecera de Opciones Salto a Salto IPv6.**

Objetivo: Contiene información adicional, además de opciones que éstas debe ser examinadas por cada router a lo largo del camino que recorre el paquete.

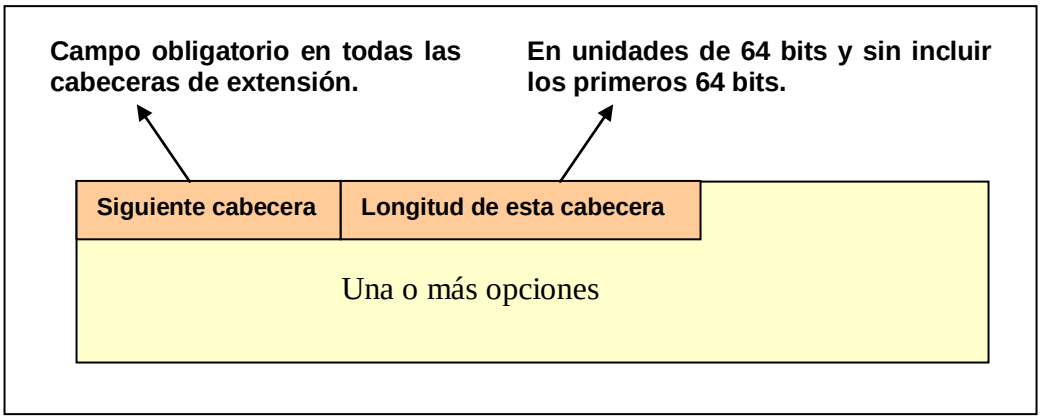


Figura 2.10 Cabecera de Opciones Salto a Salto IPv6

Opciones (Una o más Opciones): Un campo de longitud variable que consta de una o más definiciones de opciones. Cada definición está formada por 3 subcampos.

- ❖ **Tipo de opción:** Tamaño 8 bits, identifica la opción.

- ❖ **Longitud:** Tamaño 8 bits, que especifica la longitud del campo de datos.

- ❖ **Datos de opción:** Consiste en la especificación de la opción (longitud variable).

- ✓ **Cabecera de Opciones para Destinatario IPv6.**

Objetivo: Almacenar opciones que serán examinadas únicamente por los nodos finales.

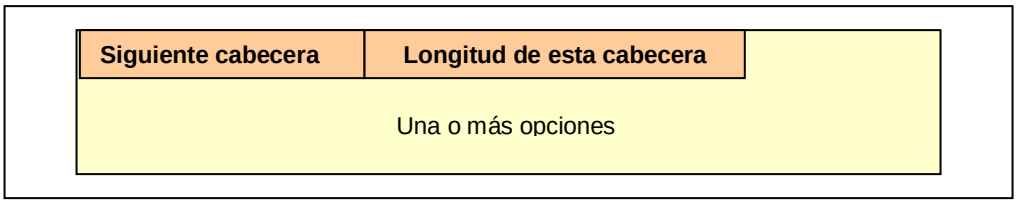


Figura 2.11 Cabecera de Opciones para Destinatario IPv6

- ✓ **Cabecera de Encaminamiento IPv6.**

Objetivo: Fijar en la dirección de origen una lista de todos los routers por los que debe pasar obligatoriamente el datagrama.

- ✓ Sólo dichos routers procesarán esta cabecera.

Equivale a la opción de encaminamiento en el origen de IPv4, todos los routers debían comprobar la opción de encaminamiento aunque no estuvieran en la lista de los nodos.

Figura 2.12 Cabecera de Encaminamiento IPv6

- ✓ **Siguiente Cabecera:** Identifica el tipo de cabecera que sigue.

- ✓ **Longitud de Cabecera:** Longitud de cabecera en unidades de 64 bits.

- ✓ **Tipo de Encaminamiento:** Identifica una cabecera de encaminamiento particular dentro de las posibles variantes.

- ✓ **Nodos Restantes:** Números de nodos indicados explícitamente del camino que quedan por visitarse antes de alcanzar el destino final.

Ejemplo

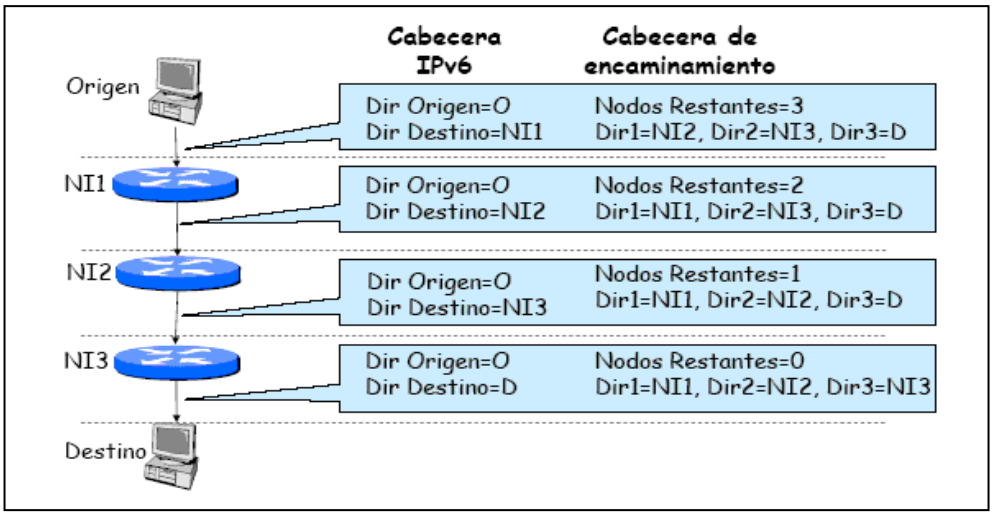


Figura 2.13 Cabecera de Encaminamiento IPv6

- ✓ **Cabecera de Fragmentación IPv6.**

Objetivo: Fragmentar datos, esto solo puede hacerse en los nodos de origen.

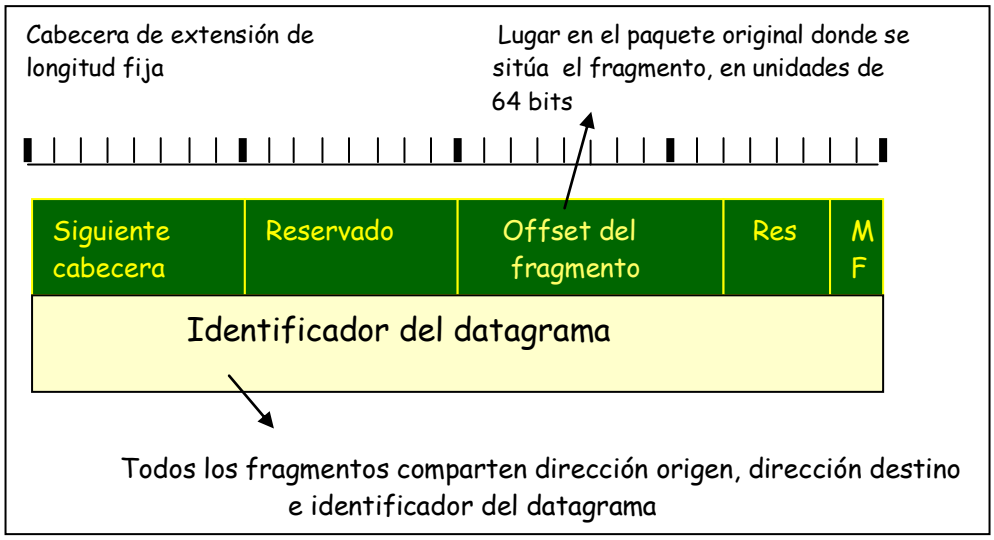


Figura 2.14 Cabecera de Fragmentación IPv6

- ✓ **Res:** Tamaño 2 bits, reservado para uso futuro.

- ✓ **MF (Flag):** Tamaño 1 bit (1 es más fragmentos, 0 es último fragmento).

- ✓ **Cabecera de Autenticación/Encriptación.**

Modo Transporte:

- ✓ Se asegura (encripta/autentica) la carga de datos del datagrama (PDU de transporte).

- ✓ Se establece entre nodos extremos de la red.

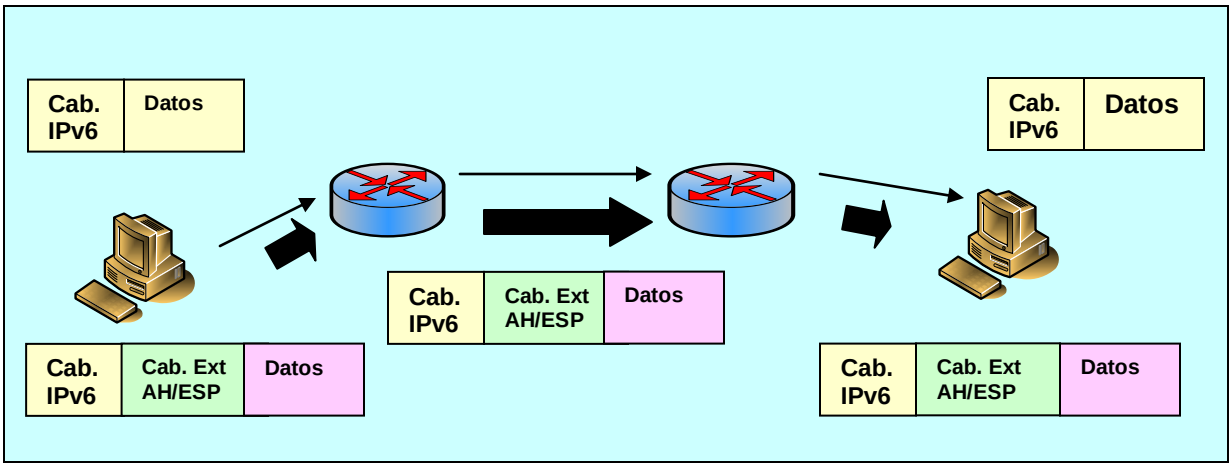


Figura 2.15 Modo Transporte

Modo Túnel:

- ✓ Se asegura (encripta/autentica) el datagrama completo → túnel seguro en la red.
- ✓ Se establece entre nodos intermedios/extremos de la red.
- ✓ Las direcciones origen y destino se modifican con las de los nodos intermedios que implementan IPsec.

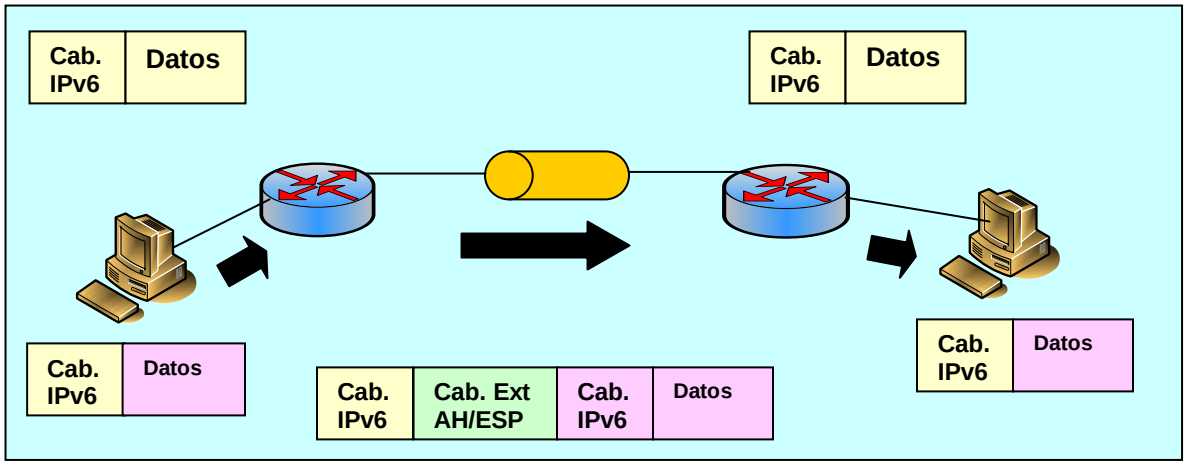


Figura 2.16 Modo Túnel

2.11.3 Direccionamiento en IPv6

Las direcciones de IPv6 son identificadores de 128 bits. Existen tres tipos de direcciones, los cuáles son: unicast, anycast y multicast. En IPv6 no hay direcciones de broadcast; su función es reemplazada por las direcciones multicast.

2.11.3.1 Direcciones Unicast

Identifican una única interface para que los paquetes con una dirección unicast se entreguen a un solo destinatario.

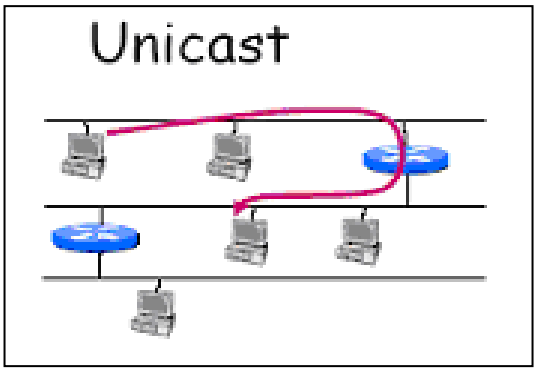


Figura 2.17 Direcciones Unicast

Hay varias formas de asignación de direcciones unicast en IPv6.

- ✓ Global Unicast
- ✓ Link Local
- ✓ Sitio Local
- ✓ Especial
- ✓ Direcciones unicast basadas en el proveedor global

2.11.3.1.1 Global Unicast

Prefijo 2000::/3

Equivalentes a direcciones públicas IPv4.

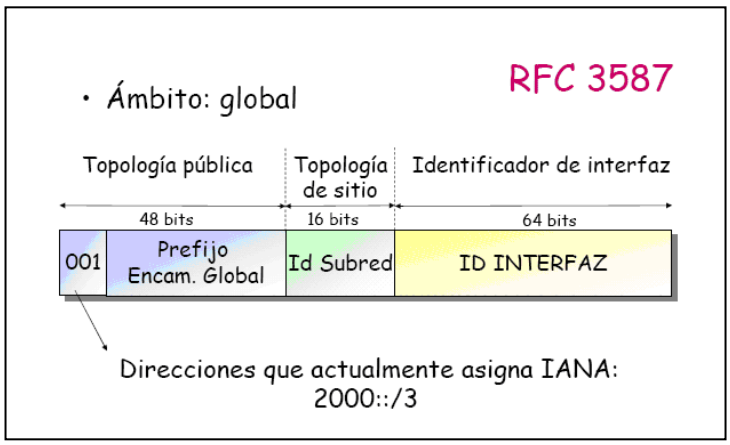


Figura 2.18 Dirección Global Unicast

2.11.3.1.2 Link Local

Prefijo FE80::/64

Requeridas por el proceso Neighbor Discovery.

Se configuran automáticamente.

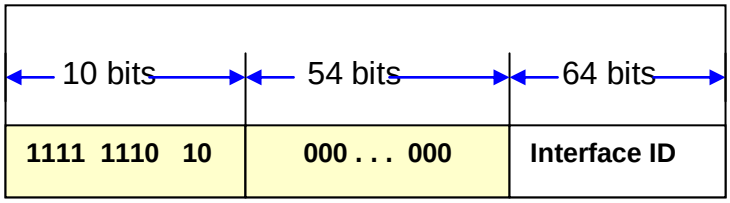


Figura 2.19 Dirección Link Local

2.11.3.1.3 Direcciones Unicast de Sitio Local

Prefijo: 1111111011

Una dirección de sitio local es usada para direccionar dentro de un sitio local u organización.

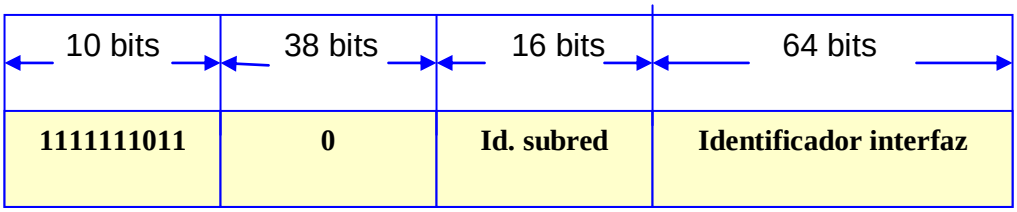


Figura 2.20 Dirección Unicast de Sitio Local

2.11.3.1.4 Direcciones Especiales

Se dividen en dirección:

- ✓ Dirección no especificada y Dirección loopback.

2.11.3.1.4.1 Direcciones No Especificadas

- ✓ Equivalente a 0.0.0.0 de IPv4, indica la ausencia de una dirección.

0:0:0:0:0:0:0:0 = ::

Figura 2.21 Dirección No Especificada

2.11.3.1.4.2 Dirección de Bucle Local (Loopback).

- ✓ Equivalente a 127.0.0.1 de IPv4, dirección de la interfaz de bucle local.

0:0:0:0:0:0:0:1 = :: 1

Figura 2.22 Dirección Loopback

2.11.3.1.5 Direcciones Unicast Basadas en Proveedor

Las direcciones unicast basadas en proveedor son usadas para la comunicación global, tienen el siguiente formato:

Tabla 2.5 Direcciones Unicast Basadas en Proveedor

3 bits	n bits	m bits	p bits	125- n-m-p bits
010	ID registro	ID proveedor	ID subscriptor	Intra-Subscriptor

2.11.3.2 Direcciones Anycast

Identifican un conjunto de interfaces generalmente pertenecientes a diferentes nodos, los paquetes con una dirección anycast se entregan a los

miembros del grupo más cercano al remitente según lo determine el protocolo de enrutamiento utilizado.

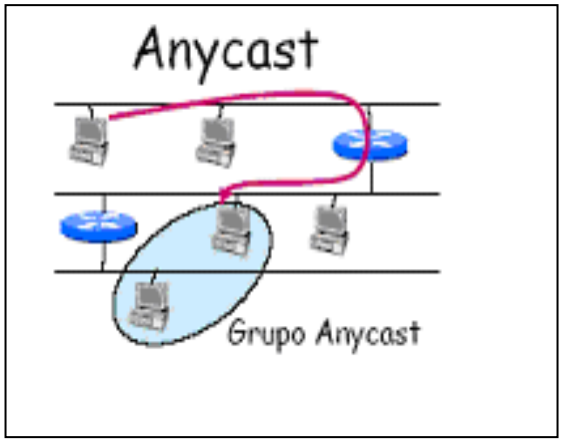


Figura 2.23 Direcciones Anycast

2.11.3.3 Direcciones Multicast

Una dirección multicast es un identificador para un grupo de nodos, y su formato es el siguiente:

Tabla 2.6 Direcciones Multicast

8 bits	4 bits	4 bits	112 bits
11111111	Bandera	Alcance	ID de grupo

Los paquetes con una dirección multicast se entregan a todos los destinatarios pertenecientes a ese grupo.

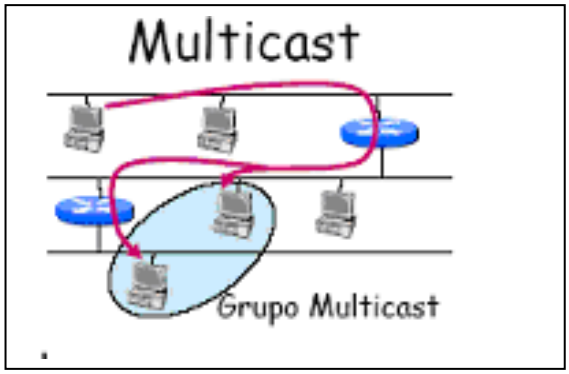


Figura 2.24 Direcciones Multicast

La descripción de los campos es la siguiente:

- ✓ **11111111** al comienzo identifica a la dirección como una dirección multicast.

- ✓ **Bandera** es un conjunto de 4 bits. Los 3 primeros están reservados y deben inicializarse en 0. Si el cuarto bit tiene un valor 0, indica que la dirección es una dirección multicast permanente "well-know" asignada por una autoridad de Internet. Si este bit tiene un valor 1, indica que no se trata de una dirección permanente, sino que se trata de una dirección transitoria.

- ✓ **Alcance** son cuatro bits utilizados para limitar el alcance del grupo multicast. Los valores son:

Tabla 2.7 Direcciones Multicast

0	Reservado
1	Alcance de nodo local

2	Alcance de enlace local
3, 4	No asignado
5	Alcance de sitio local
6, 7	no asignado
8	Alcance de organización local
9 – D	No asignado
E	Alcance global
F	Reservado

2.11.4 Representación de Direcciones en IPv6

Existen tres formas de representar las direcciones IPv6 como strings de texto. x:x:x:x:x:x:x:x donde cada x es el valor hexadecimal de 16 bits, de cada uno de los 8 campos que definen la dirección. No es necesario escribir los ceros a la izquierda de cada campo, pero al menos debe existir un número en cada campo 128 bits se agrupan los octetos de 2 en 2, se separan por "**:**" y se representan en hexadecimal:

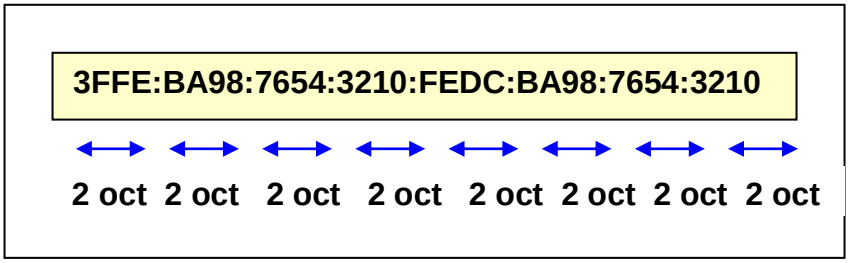


Figura 2.25 Representación de una Dirección

✓ Simplificación:

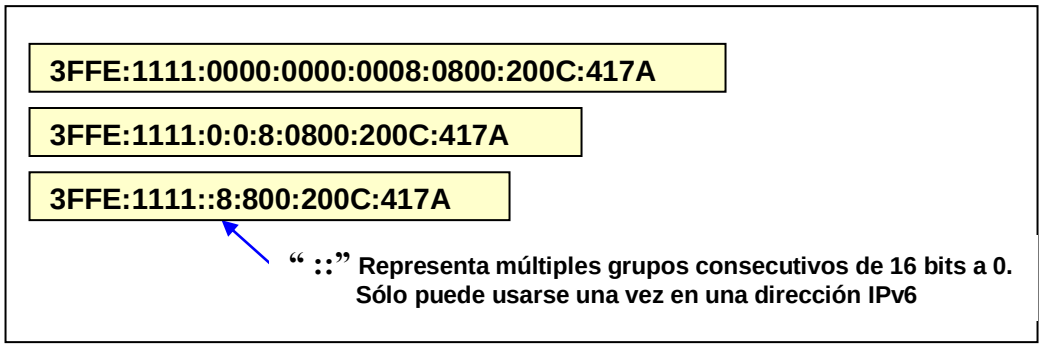


Figura 2.25.1 Simplificación de las Direcciones

✓ Representación de prefijos IPv6: dirección IPv6/longitud-prefijo.

Tabla 2.7.1 Representación de Prefijos en IPv6

FEDC: BA98:7654:3210: FEDC: BA98:7654:3210
1080:0:0:0:8:800:200C:417A

Como será común utilizar esquemas de direccionamiento con largas cadenas de bits en cero, existe la posibilidad de usar sintácticamente **::** para representarlos. El uso de **::** indica múltiples grupos de 16 bits de ceros. Dicho símbolo podrá aparecer una sola vez en cada dirección. **Ejemplo:**

Tabla 2.7.2 Representación de Prefijos en IPv6

1080:0:0:0:8:800:200C:417A	dirección unicast
FF01:0:0:0:0:0:0:101	dirección multicast
0:0:0:0:0:0:0:1	dirección loopback
0:0:0:0:0:0:0:0	dirección unspecified

También podrán ser representadas de la siguiente forma:

Tabla 2.7.3 Representación de Prefijos en IPv6

1080::8:800:200C:417A	unicast address
FF01::101	multicast address
::1	loopback address
::	unspecified addresses

Para escenarios con nodos IPv4 e IPv6 es posible utilizar la siguiente sintaxis: x:x:x:x:x:x:d.d.d.d, donde x representan valores hexadecimales de las seis partes más significativas (de 16 bits cada una) que componen la dirección y las **d**, son valores decimales de las 4 partes menos significativas (de 8 bits cada una), de la representación standard del formato de direcciones IPv4. **Ejemplo:**

0:0:0:0:0:0:13.1.68.3

0:0:0:0:0:FFFF:129.144.52.38

0:0:0:0:0:0:13.1.68.3

0:0:0:0:0:FFFF:129.144.52.38

o en la forma comprimida

::13.1.68.3

::FFFF:129.144.52.38

2.11.5 Comparación de Cabeceras de IPv4 a IPv6

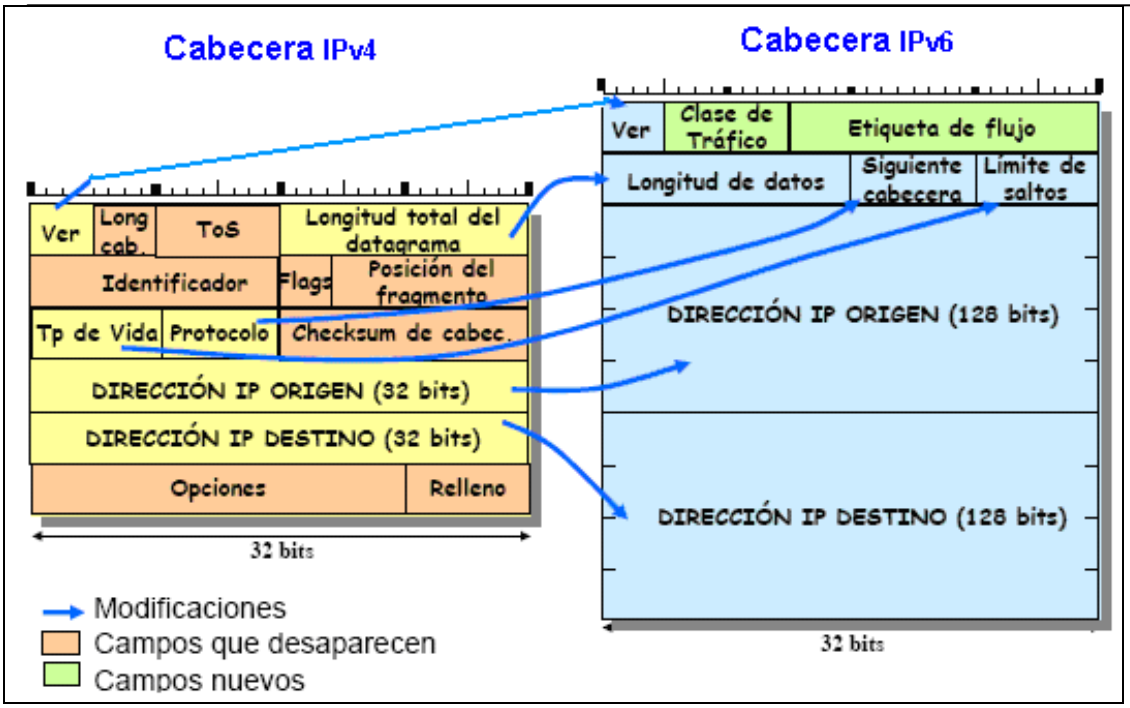


Figura 2.26 Evolución de Cabecera de IPv4 a IPv6

- **Los Campos que se han Modificado son:**

✓ Se ha cambiado la versión de IPv4 a IPv6, el tamaño se mantiene.

✓ El campo Longitud Total del Datagrama en IPv4 se ha renombrado por el campo Longitud de Datos en IPv6, y su tamaño se mantiene fijo de 16 bits. Su diferencia radica en que el tamaño máximo del datagrama en IPv4 es de 516 octetos, mientras que en IPv6 es de 64000 octetos, lo que aumenta la eficiencia en la transmisión de paquetes grandes.

- ✓ El campo Tiempo de Vida en IPv4 se ha modificado por el campo Límite de Saltos en IPv6, y su longitud es de 8 bits. En IPv4 se hace relación al tiempo de vida de un paquete, mientras que en IPv6 es el número de saltos.

- ✓ El campo Protocolo en IPv4 se lo conoce como Siguiente Cabecera en IPv6, y el tamaño de la longitud es de 8 bits. Con la diferencia que IPv4 indica el protocolo que se va a utilizar mientras que en IPv6 indica la siguiente cabecera con la que se va a trabajar.

- ✓ El tamaño de las Direcciones de Origen y Destino en IPv4 que eran de 32 bits cambian a 128 bits en IPv6, lo que permite soportar más nodos direccionables y más niveles de direccionamiento.

La meta del IPv6 es la de conseguir una mayor rapidez y flexibilidad con bastante espacio de direcciones y todos estos se han cumplido, existen algunos proyectos como los siguientes:

- ✓ 6bone, se trata de una red internacional dedicada a probar el funcionamiento real de IPv6. Está formada por backbones regionales, como el que opera en Japón perteneciente al proyecto WIDE, una de las primeras implementaciones de IPv6, que dispone de su propia línea dedicada.

- ✓ Proyecto de IPv6 en Francia llamado INRIA.

2.11.6 Equipos que Soportan IPv6

Tabla 2.8 Equipos que Soportan IPv6

SWITCHS DE DISTRIBUCION	**SISA 3750-24PS-E**	**INTEGRAR MATRIX C2G124-48P**	**LINK WS-C3750G-48TS-E**	**EBD OS6800-48**
ESPECIFICACIONES				
CALIDAD DE SERVICIO				
Mapeo de Información de QoS de nivel 2 a nivel 3 y viceversa, para garantizar el manejo de QoS extremo a extremo aún en ambientes donde los usuarios finales están conectados a switches de nivel 2.	Mapeo de información de QoS de nivel 2 a nivel 3 y viceversa, para garantizar el manejo de QoS extremo a extremo aún en ambientes donde los usuarios finales están conectados a switches de nivel 2.	Soporta mapeo de QoS de nivel 2 a nivel 3 y viceversa.	Los switches hacen mapeo de niveles de QoS 802.1p a DSCP[24].	Incrementa el limite de uso de banda de ancho por puerto en 64 Kb., limita el incremento en puertos en 1Mg.
SEGURIDAD				
Filtrado de flujos de tráfico entrantes al switch basado en información de nivel 2 (direcciones MAC[25] origen y/o destino), información de nivel 3 (direcciones IP origen y/o destino) e información de nivel 4 (puertos TCP/UDP origen y/o destino).	Soporte de filtrado de flujos de tráfico entrantes al switch basado en información de nivel 2 (direcciones MAC origen y/o destino), información de nivel 3 (direcciones IP origen y/o destino) e información de nivel 4 (puertos TCP/UDP origen y/o destino).	Realiza control y filtrado de flujo de trafico multinivel, para esto provee: -Capa 2/3/4 clasificación - IP TOS[26] Rewrite - Ingress Rate Limiting.	Cumple Advanced QoS.	Acepta.

SWITCHS DE DISTRIBUCION	SISA 3750-24PS-E	INTEGRAR MATRIX C2G124-48P	LINK WS-C3750G-48TS-E	EBD OS6800-48
ESPECIFICACIONES				
Para el control de los usuarios que entran a configurar el switch, el equipo deberá soportar la autenticación, autorización y contabilización en algún servidor basado en protocolos tales como Remote Access Dial-In User Service – RADIUS, KERBEROS[27] etc.	Para el control de los usuarios que entran a configurar el switch, el equipo deberá soportar autenticación, autorización y contabilización en algún servidor basado en protocolos tales como Remote Access Dial-In User Service – RADIUS, KERBEROS, TACACs etc.	Los siguientes, son métodos de seguridad que están disponibles para controlar cuáles usuarios están habilitados para accesar, monitorear y administrar el C2: - Cuentas y contraseñas de usuarios - Host Access Control Autenticación: permite la autentificación de usuarios que acceden al dispositivo a través de Telnet, consola local de interfase WEB a través del servidor Radius. Comunidades y nombres de usuarios SNMP.	Cumple.	Autenticación y Administración por radios y LDAP[28], SSL[29],SNMP[30].

24-30 pag.154,155 GLOSARIO

2.11.7 Formas de Conexión de IPv6

Para mantener la compatibilidad con IPv4, los cuáles agilizan la expansión de IPv6 en Internet y facilitan la transición. La clave para una transición exitosa a IPv6 es la compatibilidad con IPv4. Algunos de los mecanismos son los siguientes:

2.11.7.1 Dual IP Layer (Doble capa IP)

Consiste en proveer en hosts y routers un soporte completo tanto para IPv6 como para IPv4.

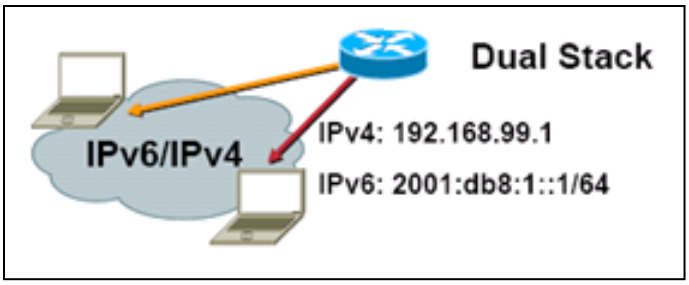


Figura 2.27 Dual IP Layer (Doble capa IP)

2.11.7.2 IPv6 over IPv4 Tunneling (IPv6 sobre IPv4)

Consiste en encapsular los paquetes de IPv6 dentro de las cabeceras de IPv4 para transportarlos sobre las estructuras de enrutamiento actuales.

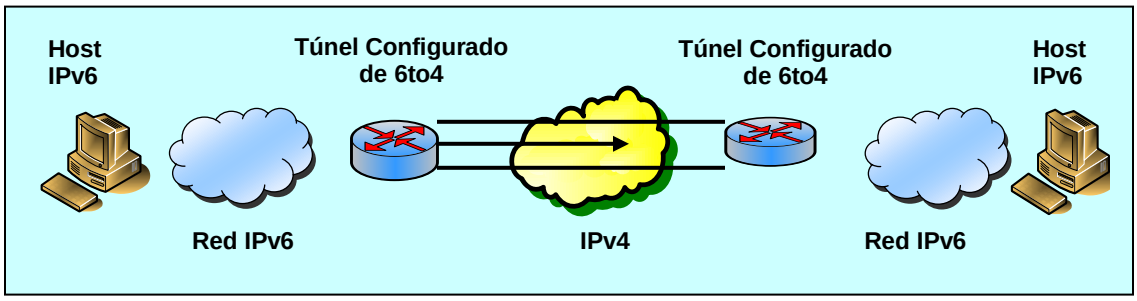


Figura 2.28 Tunneling IPv6 sobre IPv4

Formas de Conexión de Tunneling:

- **Router a Router:** Los routers IPv6/IPv4 interconectados con una infraestructura IPv4 pueden pasarse entre sí paquetes IPv6, en este caso el túnel abarca un segmento del trayecto que toma el paquete IPv6.

Su principal aplicación es unir islas IPv6 a través de IPv4.

- A cada isla IPv6 se le asigna un prefijo IPv6: 2002::/16 además de la dirección del router frontera.
- Siguiente salto IPv4 contenido en la dirección IPv6.
- El encaminamiento entre las distintas islas se apoya en el encaminamiento IPv4 subyacente.
- Implementaciones: Windows NT, Proyecto Kame, Linux y FreeBSD, entre otros.

Pasos para realizar la Configuración:

1. Enable.
2. Configure {terminal | memory | network}.
3. Interface tunnel *tunnel-number.*
4. IPv6 address *IPv6-prefix*/*prefix-length* [eui-64].
5. tunnel source {*ip-address* | *type number*}.
6. tunnel mode IPv6ip 6to4.
7. exit.
8. IPv6 route *IPv6-prefix*/*prefix-length* tunnel *tunnel-number.*

Funcionalidad: Interconectar islas IPv6 a través de océanos IPv4, cada extremo es un nodo dual y en ellos se configura direcciones IPv6 e IPv4 tanto local como remotas.

Pasos para realizar la Configuración manual:

1. Enable.
2. Configure {terminal | memory | network}.
3. Interface tunnel *tunnel-number.*
4. IPv6 address *IPv6-prefix*/*prefix-length* [eui-64].
5. Tunnel source {*ip-address* | *type number*}.
6. Tunnel destination *ip-address.*
7. Tunnel mode IPv6IP.

- **Host a Router:** Los host IPv6/IPv4 pueden pasar paquetes IPv6 por un router IPv6/IPv4 intermediario que sea alcanzable por la infraestructura IPv4. Este tipo de túnel abarca el primer segmento del trayecto del paquete.

Pasos para realizar la Configuración:

1. Enable.
2. Configure {terminal | memory | network}.
3. Interface tunnel tunnel-number.
4. IPv6 address IPv6-prefix/prefix-length [eui-64].
5. Tunnel source {ip-address | IPv6-address | interface-type interface-nu.
6. Tunnel destination {host-name | ip-address | IPv6-address}.
7. Tunnel mode {aurp | cayman | dvmrp | eon | gre | gre multipoint | gre IPv6 | ipip [decapsulate-any] | iptalk | IPv6 |mpls | nos}.

- **Host a Host:** Los hosts IPv6/IPv4 interconectados con una infraestructura IPv4 pueden pasarse paquetes IPv6 entre sí. En este caso el túnel abarca el recorrido completo que toman los paquetes.

- ✓ Permite a nodos duales comunicarse a través de una infraestructura IPv4.
- ✓ Direcciones IPv6 “IPv4 compatible”: Prefijo 0::/96 + direcciones IPv4.
- ✓ Se define una Interfaz virtual para la dirección “IPv4 compatible”.
- ✓ Los paquetes destinados a direcciones “IPv4 compatible local”, se envían por el túnel automático. Algunas reglas son:

- Dirección de origen IPv6: Dirección IPv4 compatible “Remota”.
- Dirección de destino IPv4: Extraída de la dirección “IPv4 Compatible”.

- **Router a Host:** Los routers IPv6/IPv4 pueden pasar paquetes IPv6 hasta su host IPv6/IPv4 destinatario (final). Este túnel abarca el último segmento del recorrido.

2.11.8 Comparación de las Características de IPv4 e IPv6

Tabla 2.9 Comparación de las Características de IPv4 e IPv6

	IPv4	**IPv6**
Direcciones	Las direcciones de origen y destino tienen una longitud de 32 bits (4 bytes).	Las direcciones de origen y destino tienen una longitud de 128 bits (16 bytes).
IPSec	La seguridad es opcional.	La seguridad es obligatoria.
Identificación del número de paquetes	No existe ninguna identificación de flujo de paquetes para que los enrutadores controlen al QoS en el encabezado IPv4.	Se incluye la identificación del flujo de paquetes para que los enrutadores controlen al QoS en el encabezado IPv6, utilizando el campo Flow Label (etiqueta de flujo).

Fragmentación	La llevan a cabo los enrutadores y el host que realiza el envío.	No la llevan a cabo los enrutadores, sino únicamente el host que realiza el envío.
Encabezado	Incluye una suma de comprobación.	No incluye una suma de comprobación.
Opciones	El encabezado lo incluye.	Todos se trasladan a los encabezados de extensión IPv6.
Marcos de solicitud ARP	El Protocolo de resolución de direcciones (ARP[31]) utiliza los marcos de solicitud ARP de difusión para resolver una dirección IPv4 como una dirección de capa de vínculo.	Los marcos de solicitud ARP se sustituyen por mensajes de solicitud de vecinos de multidifusión.
Administrar la pertenencia a grupos locales de subred	Se utiliza el Protocolo de administración de grupos de Internet (IGMP).	IGMP se sustituye con los mensajes de descubrimiento de escucha de multidifusión (MLD[32]).
Determinar la dirección IPv4 de la	Se utiliza el descubrimiento de enrutadores ICMP[33], y es opcional.	El Descubrimiento de enrutadores ICMP queda

mejor puerta de enlace predeterminada		sustituido por la Solicitud de enrutadores ICMPv6 y los mensajes de anuncio de enrutador, y es obligatorio.
Direcciones de multidifusión	Se utilizan para enviar tráfico a todos los nodos de una subred.	No hay direcciones de multidifusión IPv6. De forma alternativa, se utiliza una dirección de multidifusión para todos los nodos de ámbito local del vínculo.
Configuración	Debe configurarse manualmente o a través de DHCP[34].	No requiere configuración manual o a través de DHCP.
DNS	Utiliza registros de recurso (A) de dirección de host en el Sistema de nombres de dominio (DNS) para correlacionar nombres de host con direcciones IPv4.	Utiliza registros de recurso (AAA) de dirección de host en el Sistema de nombres de dominio (DNS) para correlacionar nombres de host con direcciones IPv6.
Direcciones IP relacionados con host	Utiliza registros de recurso (A) de puntero en el dominio DNS IN-ADDR.ARPA para correlacionar direcciones IPv4 con nombres de host.	Utiliza registros de recurso (PTR[35]) de puntero en el dominio DNS IP6.INT para correlacionar direcciones IPv6 con nombres de host.

Tamaño de paquete	Debe admitir un tamaño de 576 bytes(posiblemente fragmentado)	Debe admitir un tamaño de 1280 bytes (sin fragmentación)

2.12 MULTIHOMING

2.12.1 Definición

Se llama Multihoming a la aplicación con los proveedores de la red y los proveedores de acceso a Internet a conectarse con más de una red. Una red con Multihoming mantiene la conexión a Internet cuando se interrumpe una conexión y puede dirigir el tráfico a cualquier destino a través de otra conexión, ofreciendo mejor servicio y evitando la congestión en el destino. Multihoming se utiliza principalmente para fines de duplicación de seguridad y de redundancia, con vistas a garantizar la calidad del servicio. Las organizaciones en la actualidad depende cada vez más de su conectividad hacia Internet, lo que implica la necesidad de tener redundancia de proveedores de acceso (Multihoming) para asegurar su conectividad hacia Internet. Existen varias formas de conexión como son:

- Varias conexiones con un solo ISP, consiste en conectar un único router de Internet a dos o más routers de distintos POP (Punto de Presencia) de un ISP (Proveedor de Servicio de Internet).

31-35 pag. 155 GLOSARIO

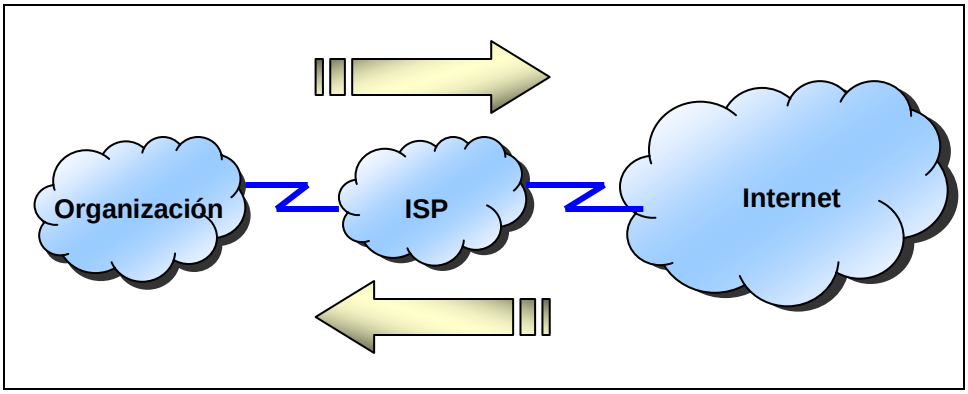


Figura 2.29 Multihoming

Cuando la conexión a este ISP o la conexión entre este e Internet dejan de funcionar, la organización queda aislada de la red, y con los costos de pérdida que esto conlleva.

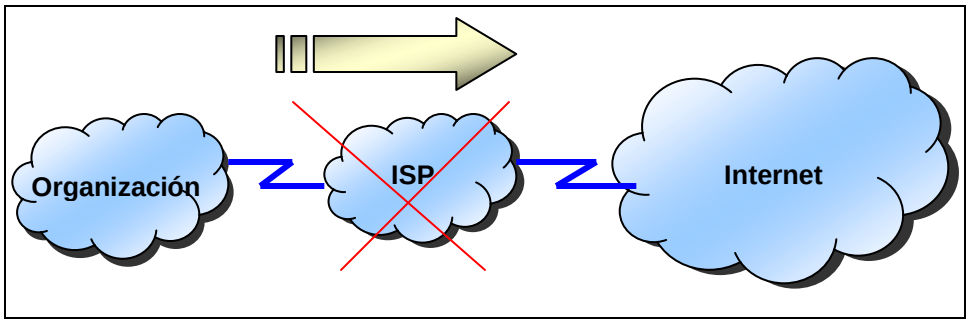


Figura 2.30 Multihoming

- Varias conexiones con varios ISP's y esto es posible con la conexión de una empresa a Internet. Una forma de evitar esto o al menos de reducir la probabilidad de que se de es mediante la conexión a múltiples ISP's, a esto se le llama Multihoming.

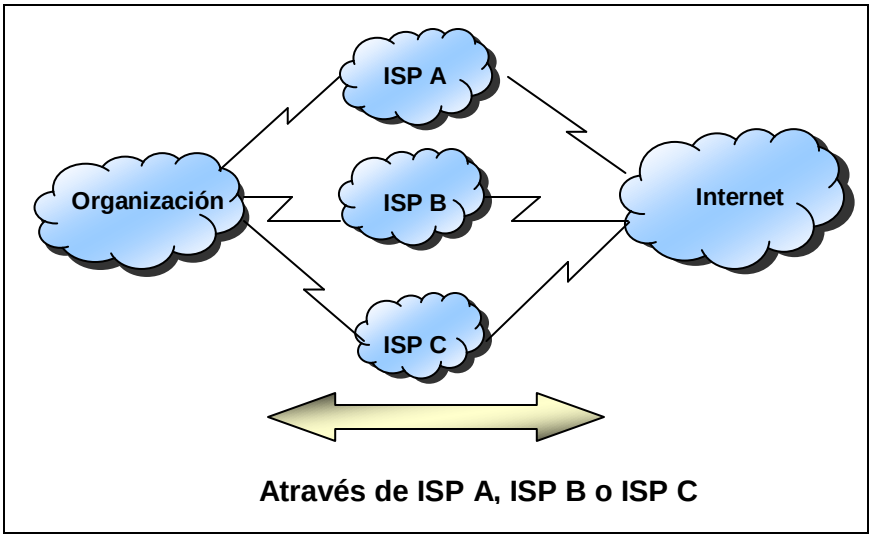


Figura 2.31 Multihoming

De este modo si la conexión a través de uno de los ISP falla, la organización sigue estando conectada a la red a través de los otros ISP's.

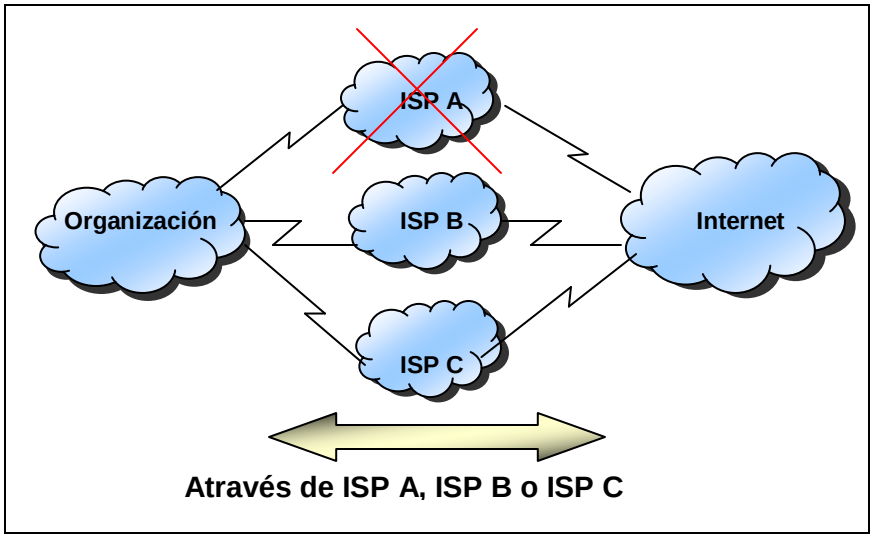


Figura 2.32 Multihoming

2.12.2 Ventajas de Multihoming

En IPv6 se ha desarrollado mecanismos que permiten gestionar de forma automática el traslado de los dispositivos de unas redes a otras, permitiendo así la conexión automática a su red de origen los dispositivos que se encuentran temporalmente en redes de acceso remotas.

- Si la conexión falla con un ISP, mediante Multihoming se levantarán los servicios del otro ISP y por lo tanto seguirá trabajando normalmente la organización.

- Mientras una conexión esté funcionando, los servidores tienen acceso a Internet, y las estaciones de trabajo tienen acceso a la red.

- Esto acarrea una serie de costos, los números de sistemas autónomos son limitados y costosos así como de las direcciones de Internet, por lo que los proveedores acostumbran a subir los precios.

- Las comunicaciones siempre van estar activas.

- Fácil de configurar, lo cual le hace menos susceptible a los errores.

2.12.3 Multihoming en Organizaciones Pequeñas.

Se debe considerar los siguientes puntos para trabajar con organizaciones pequeñas, los cuáles son:

- No pueden acceder a estos servicios porque los costos son muy altos, y su implementación es difícil.
- La comunicación se puede cortar debido a las modificaciones en los estados de los enlaces.
- Se cuenta con algunos recursos adicionales, pero muy limitados.

2.12.4 Multihoming en Organizaciones Grandes

Se debe considerar algunos puntos que son importantes al trabajar con organizaciones grandes como son:

- Multihoming con IPv6 se aplica por lo general para empresas grandes, aunque no es una restricción, se tiene que tomar en cuenta las necesidades de la organización.

- Facilita un número mayor de direcciones (128 bits), seguridades y calidad de servicio (QoS), entre algunas de sus características.

- Los diferentes fabricantes tanto de hardware como de los sistemas operativos han permitido una mejora en las aplicaciones.

2.12.5 Problemas

- Los costos son muy altos, debido a que la adquisición de las direcciones es elevado y los proveedores han incrementado sus valores.

- Se ha impuesto restricciones en la conectividad, éstas solo deben aplicarse a los puntos de acceso de los dominios ó a toda la red en la que se va aplicar Multihoming.

- La actualización del software es importante, ya que es una nueva técnica que necesita nuevas versiones del mismo.

- Se debe capacitar a los usuarios, para lograr un mejor desempeño de la aplicación.

- El tráfico de retorno no puede controlarse de manera eficaz a pesar de que se maneja calidad de servicio (QoS).

CAPÍTULO III

ANÁLISIS Y DISEÑO

Para realizar el diseño Lógico y Físico, se debe de hacer un estudio (Análisis) sobre la forma de conexión de los equipos para poder realizar la implementación del mismo.

En la actualidad en el Ecuador los proveedores de Internet no ofrecen conexiones a IPv6, por lo que se ha visto la necesidad de realizar la conexión a proveedores externos por medio de la creación y configuración de túneles.

En el diseño Lógico y en el diseño Físico se mostrará la forma que se va a realizar las conexiones con los diferentes equipos:

1. Ingresar a Multihoming con IPv6 es soportar el gran aumento de dispositivo a través de dos salidas a Internet, como se indica a continuación.

   La Empresa “netXperts Consulting S.A.”, posee una red Lan que está conectada a un solo proveedor ya que permite acceder al Diseño Lógico para la implementación de Multihoming con IPv6, lo cual está representada en el siguiente diseño.

3.1 Diseño Lógico

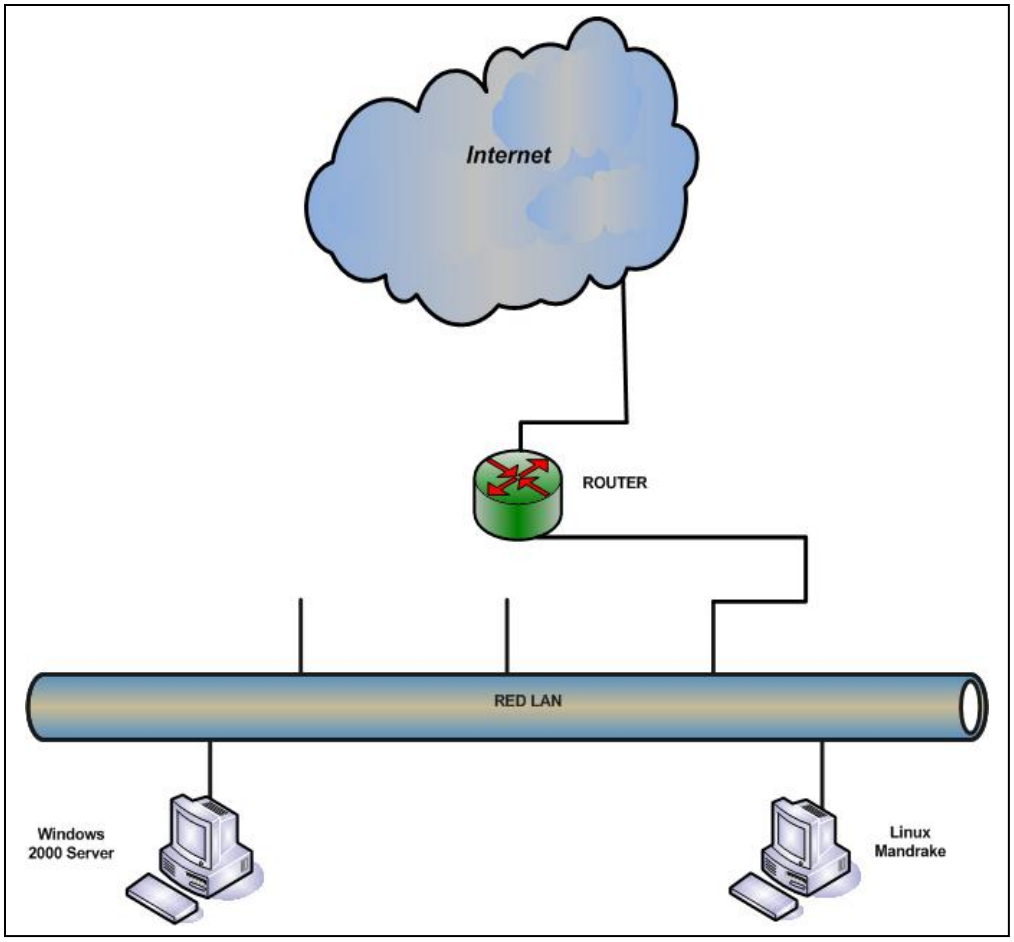


Figura 3.1 Diseño Lógico

2. Para la Implementación de Multihoming con IPv6 en la Empresa "netXperts Consulting S.A.", se debe de realizar las conexiones a IPv6 a través de:

- ✓ Dos equipos con sistemas operativos diferentes que son: Windows y Linux, los cuáles cumplen con los requisitos necesarios para la funcionalidad del mismo.

- ✓ Un switch que permitirá la conexión de la red Lan.
- ✓ Dos Routers Cisco modelo 2500.

Estos elementos se conectarán a los túneles creados como se muestra a continuación.

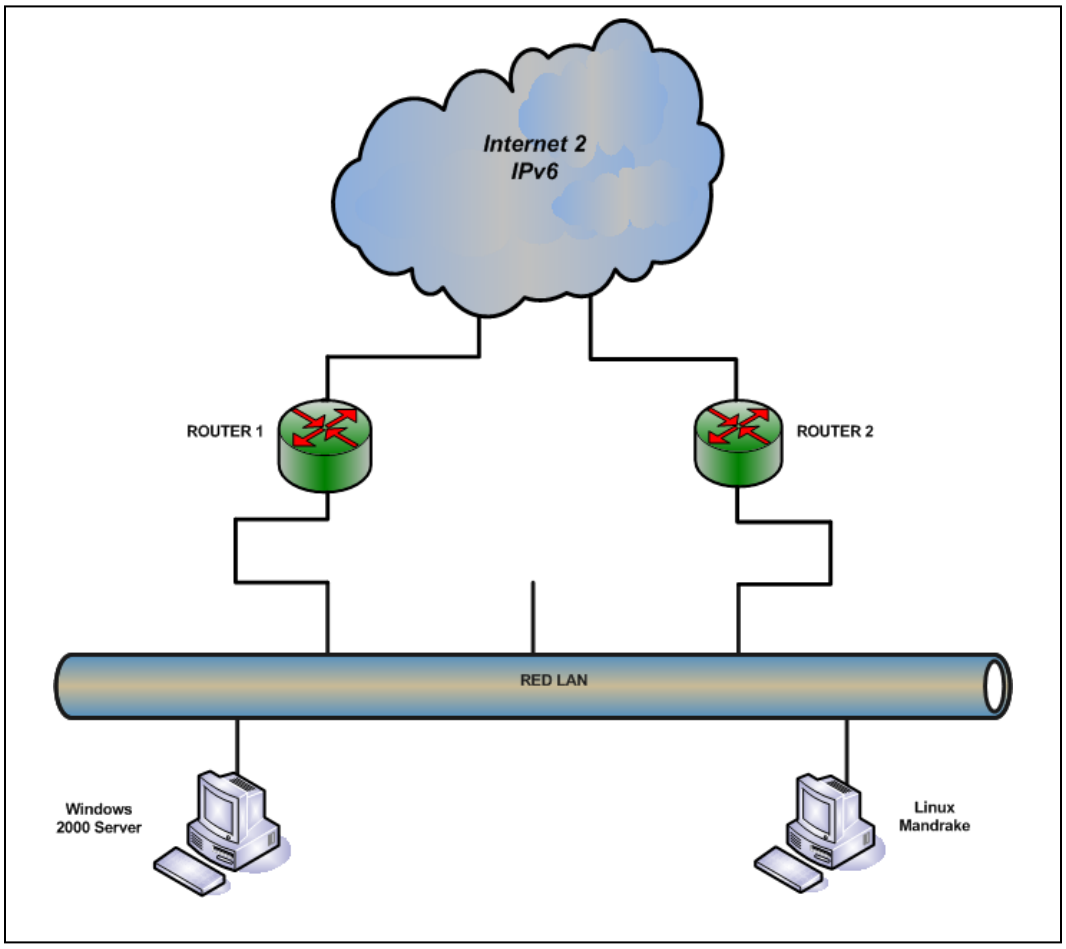


Figura 3.2 Diseño Lógico

3. Para realizar la aplicación de Multihoming con IPv6, se debe crear conexiones con proveedores del exterior ya que en nuestro país “Ecuador” los proveedores que existen no brindan soporte para IPv6.

Para implementar Multihoming con IPv6 en la Empresa “netXperts Consulting S.A.”, se realizará por medio de la configuración de los equipos que están conectados a un dispositivo que es el router 1 permitiendo la conexión a Internet IPv4, y a través de un dispositivo que es el router 2 permitiendo con los proveedores externos en creación de los túneles y llegar a Internet con IPv6.

3.2 Diseño Físico

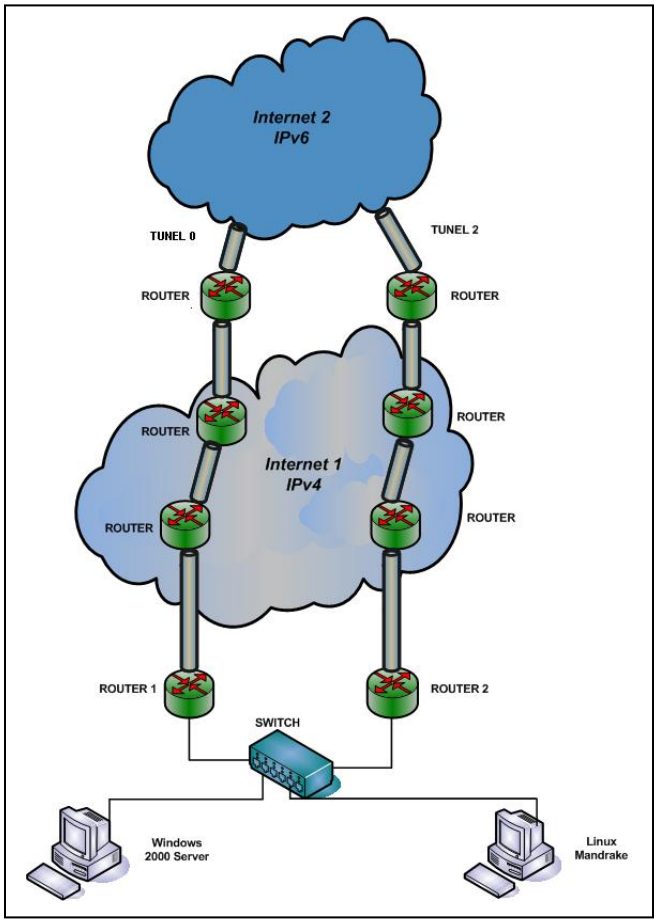


Figura 3.3 Diseño Físico

3.3 Elementos Físicos para la Implementación de Multihoming con IPv6

3.3.1 Requisitos para la Instalación de los Sistemas Operativos

- **Requerimientos Básicos para Windows 2000 Server**
  - ✓ Procesador Celeron Pentium III.
  - ✓ Sistema Operativo: Windows 2000 Server.
  - ✓ Procesador 133 MHz.
  - ✓ 128 MB (Memoria Ram).
  - ✓ Espacio en Disco (2Gb con 650 de espacio libre).
  - ✓ Monitor (VGA), teclado y mouse.
  - ✓ CD-ROM, disquetera.
  - ✓ Tarjeta de Red.

- **Requerimientos Básicos para Linux**
  - ✓ Procesador Celeron Pentium II.
  - ✓ Sistema Operativo: Linux Mandrake 10.1.
  - ✓ Procesador 133 MHz.
  - ✓ 64 MB (Memoria Ram).
  - ✓ Espacio en Disco (2Gb con 650 de espacio libre),
  - ✓ Monitor (VGA), teclado y mouse.
  - ✓ CD-ROM, disquetera.
  - ✓ Tarjeta de Red.

- Los equipos que se tienen para realizar esta aplicación son:

Equipo 1:

- ✓ Sistema Operativo: Windows 2003 Server con Service Pack1.
- ✓ Procesador 2.1 GHz.
- ✓ 256 MB (Memoria Ram).
- ✓ Disco Duro de 120 Gb.
- ✓ Monitor (VGA), teclado y mouse USB.
- ✓ CD-RW, disquetera.
- ✓ Tarjeta de Red.

Equipo 2:

- ✓ Sistema Operativo: Linux Mandrake 10.1.
- ✓ Procesador 2.3 GHz.
- ✓ 512 MB (Memoria Ram).
- ✓ Disco Duro de 80 Gb.
- ✓ Monitor (VGA), teclado y mouse PS2.
- ✓ CD-RW, disquetera.
- ✓ Tarjeta de Red.

3.3.2 Equipos para la Conexión

3.3.2.1 Router Cisco 2500

Figura 3.4 Router Cisco 2500

3.3.2.1.1 Configuración de un Enrutador Nuevo

- Los comandos de configuración se pueden ejecutar de forma interactiva. Los cambios se activan casi inmediatamente en la configuración corriente.
- Se puede usar una conexión directa vía puerto serie.
- Hacer Telnet/SSH a las vty's ("terminales virtuales").
- Una conexión vía modem al puerto auxiliar.
- Escribir los comandos en un fichero de texto y cargarlo luego en el enrutador vía TFTP.

  copy tftp start o config net.

- Cargar los parámetros de configuración en la RAM.
- Router#configure terminal.

- Dar al enrutador una identificación.
- Router#(config)hostname RouterA.
- Asignar contraseñas de acceso.
  - RouterA#(config)line console 0.
  - RouterA#(config-line)password cisco.
  - RouterA#(config-line)login.

3.3.2.1.2 Configuración de Interfaces

- **Configuración de la Dirección IP y Máscara.**

  router configure terminal.

  router(config)#interface e0/0.

  router(config-if)#ip address n.n.n.n m.m.m.m.

  router(config-if)#no shutdown.

  router(config-if)#^Z.

  router#.

Se puede cambiar la configuración de un router de diferentes maneras:

- Através del puerto de consola.
- Mediante el puerto auxiliar.
- Accediendo a él por telnet.
- Descargando una configuración de un servidor Tftp.
- Usando herramientas de Cisco, como en ConfigMaker.

3.3.2.1.3 Modos de Acceso al Router

- Modo EXEC de usuario, permite un examen limitado del router. En este modo de utilización el prompt aparece:

  nombre-router>

- Modo EXEC privilegiado (enable), permite un examen detallado del router, manipulación de ficheros y acceso a los modos de configuración.

  nombre-router#

- Modo de configuración global, permite acceder a comandos que afectan a todo el router.

  nombre-router(config)#

- Otros modos de configuración, permite acceder a comandos de configuración concretos (p.e: interfaces, protocolos de ruteo).

  nombre-router(config-if)# (modo de configuración de interfaces)

- **Rom Monitor:** Útil para recuperación de contraseñas y para instalar IOS.

- **Modo Setup:** Disponible cuando no existe el fichero **startup-config.**

- **Fuentes de Configuración Externas:**
  - ✓ **Consola:** Acceso directo vía puerto serie.
  - ✓ **Puerto Auxiliar:** Acceso vía modem.

- ✓ **Terminales Virtuales:** Acceso Telnet/SSH.
- ✓ **Servidor TFTP:** Copiar la configuración en la NVRAM.
- ✓ **Software de Gestión:** CiscoWorks.

- **Entrar al Enrutador (Login)**
  - ✓ **Conectarse al Puerto Consola o hacer Telnet.**

router>

router>enable

password

router#

3.3.2.1.4 Configurar el Enrutador

Terminal (Entrar los comandos directamente)

router# configure terminal

router(config)#

3.3.2.1.5 Mostrar la Configuración

- ✓ Se debe usar “show running-configuration” para ver la configuración actual.
- ✓ Se debe usar “show startup-configuration” para ver la configuración guardada en NVRAM.

3.3.2.1.6 Dónde está la Configuración

- ✓ El enrutador siempre tiene dos configuraciones:
  - ✓ **"Running" (actual).**
- ✓ En RAM, indica con qué parámetros el enrutador está operando actualmente. Se modifica con el comando configure.
- ✓ Para verla: show running-config.
  - ✓ **"Startup" (de inicio).**
- ✓ En NVRAM, determina cómo va a operar el enrutador cuando sea reiniciado.
- ✓ Se modifica usando el comando copy.
- ✓ Para verla: show startup-config.

Para realizar la copia de la configuración el fichero destino debe existir en el directorio antes de ser copiado y debe tener permiso de escritura.

3.3.2.1.7 Guardar la Configuración en Sitios más Permanentes

- ✓ Otras máquinas, usando TFTP (Trivial File Transfer Protocol).
- ✓ En la memoria Flash del enrutador.

Se mueve de un lugar a otro con el comando copy.

- ✓ copy run start.
- ✓ copy run tftp.

- ✓ copy start tftp.
- ✓ copy tftp start.
- ✓ copy flash start.
- ✓ copy start flash.

router# copy run tftp

Address or name of remote host [ ]? 192.168.1.5

Destination filename [Router-confg]? Y !!!!!

15693 bytes copied in 0.792 secs (19814 bytes/sec)

3.3.2.1.8 Borrar la Configuración

Para borrar la Configuración completamente se debe ejecutar el comando:

Router#erase startup-config ó **Router#write erase**, luego de lo cual se debe ejecutar el comando: **Router#reload,** el enrutador se reiniciará en modo “setup”, porque no encontrará el archivo de configuración.

- **Permitir Acceso Telnet a una Red Solamente**

  access-list 1 permit 192.168.32.192 0.0.0.15

  access-list 1 deny any

  line vty 0 4

3.3.2.1.9 Recuperación de Desastres

El archivo **config-register** normalmente es 0x2102; se debe usar **"show versión"** para verificar la versión. Se debe reiniciar el enrutador y enviar la secuencia de "break" durante los primeros 60 segundos para entrar en ROM Monitor, una vez allí se debe ejecutar:

rommon 1>confreg 0x2142

rommon 2>reset

El enrutador se reinicia, ignorando el fichero de configuración. Se realizará una pregunta si se desea iniciar "Setup", a la cual se debe responder no.

Router>enable

router#copy start run (¡¡no al revés!!)

router#show run

router#conf t

router(config)enable secret <clave nueva>

router(config)int e0/0…

router(config-if)no shut

router(config)config-register 0x2102

router(config) end

router#copy run start

router#reload

3.3.2.1.10 Puertos del Router Cisco 2500

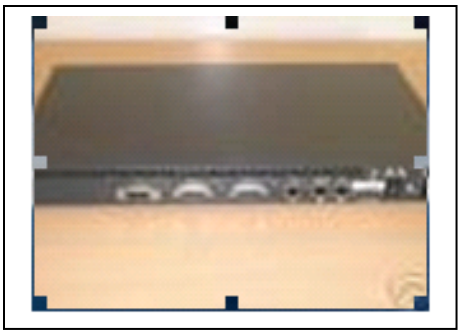


Figura 3.5 Puertos del Router Cisco 2500

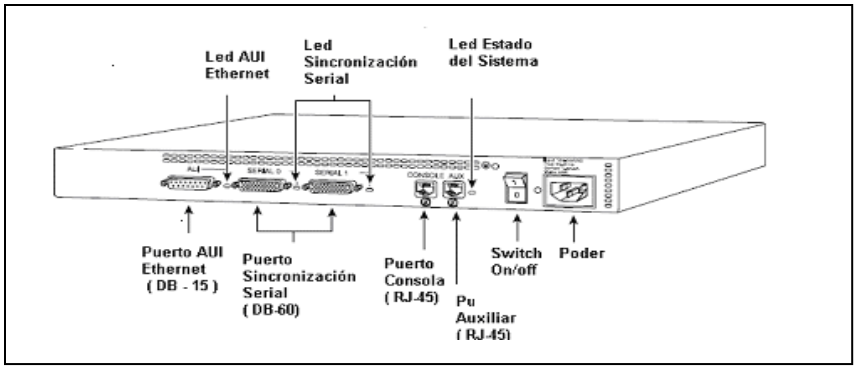


Figura 3.6 Puertos del Router Cisco 2500

Dispositivo que permitirá la conexión a Internet.

- ✓ 2 Routers Cisco modelo 2500 (IOS 12.2) con soporte para BGP.

CAPÍTULO IV

CONFIGURACIONES

4.1 Configuración de IPv6 en Windows 2000 Server

El soporte para IPv6 en los sistemas operativos de Microsoft se ha dado a partir de la versión Windows 2000, Windows 2003 Server, Windows 2000 Server, es necesario cumplir con ciertos requisitos con el fin de lograr su funcionalidad total, los cuáles son:

- ✓ Service Pack # 1 ó superior.
- ✓ Paquete de soporte IPv6 para Microsoft.

Para la instalación del protocolo IPv6 se deben seguir los siguientes pasos:

1. Verificar el Service Pack instalado en el Sistema Operativo, siguiendo los pasos que se indican a continuación:

    - ✓ Dar clic derecho en MiPC
    - ✓ Dar clic en la opción Propiedades

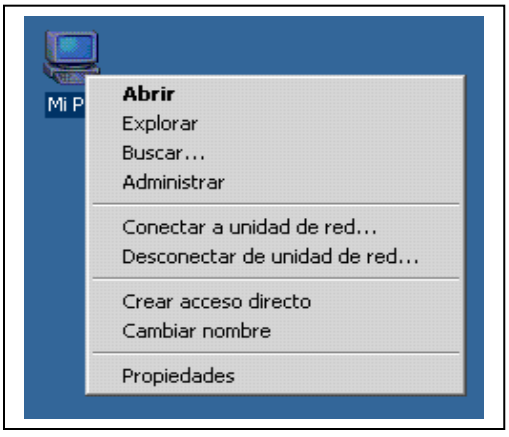


Figura 4.1 Acceso a las Propiedades de MiPC

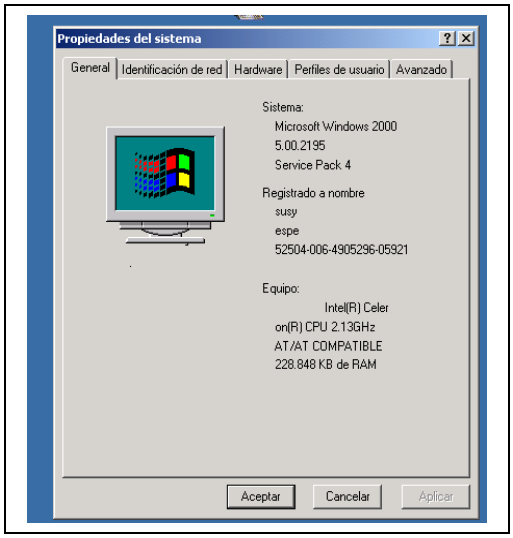


Figura 4.2 Propiedades del Sistema

2. Realizar la descarga desde Internet del paquete de **tpIPv6** para el Service Pack verificado en el paso anterior, el cuál se encuentra en un archivo **.zip,** que se debe descomprimir en la dirección que se muestra a continuación:

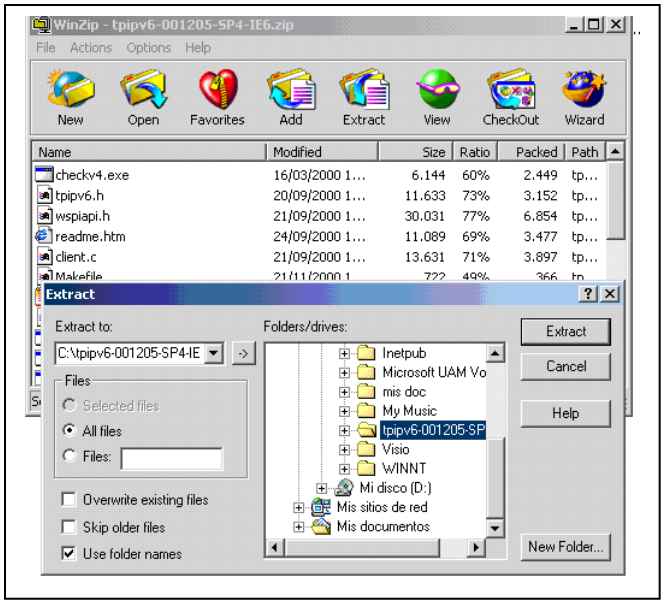


Figura 4.3 Extracción del Archivo TpIPv6 en Winzip

3. Ejecutar el archivo **hotfix.exe** que se encuentra en la dirección **C:\ tpIPv6\setup\hotfix.exe.** Finalizada la instalación se debe reiniciar el computador.

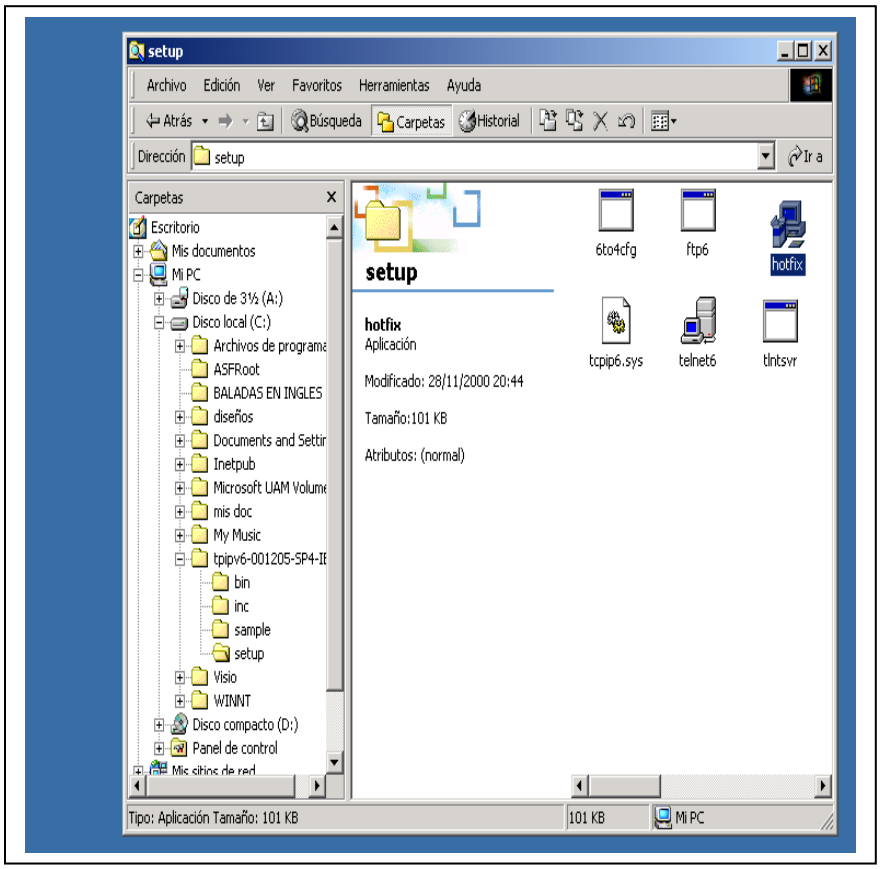


Figura 4.4 Archivo de Instalación de Soporte IPv6

4. Abrir la ventana de **Conexiones de Red** y Acceso Telefónico desde Inicio/ Configuración/Panel de Control ó en la opción *Propiedades* del menú secundario del icono de **Mis sitios de Red** en el escritorio de Windows.

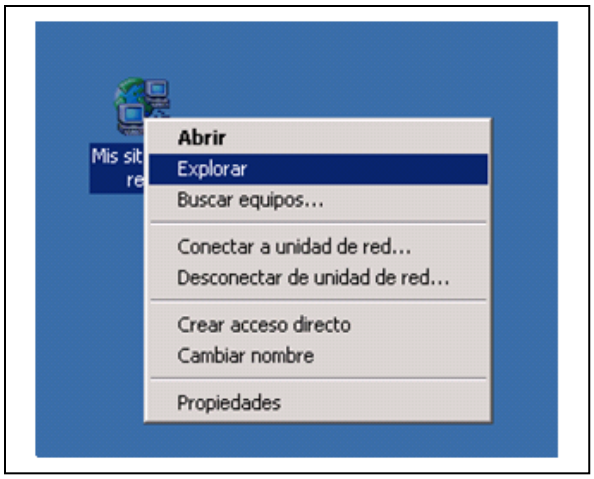


Figura 4.5 Conexión de Red

5.- Dar clic derecho sobre el icono conexión de área local y luego en la opción *Propiedades.*

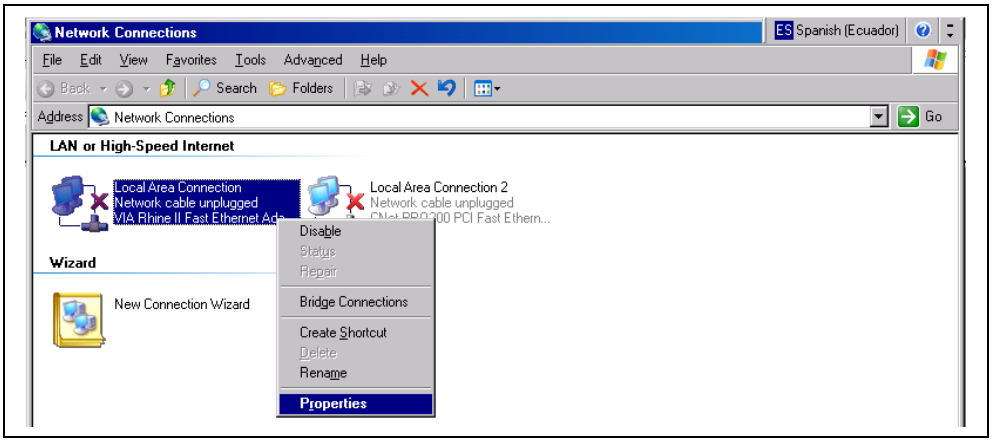


Figura 4.6 Conexiones de Red y de Acceso Telefónico

6. Instalar el protocolo IPv6 siguiendo los pasos que se indican a continuación:

- ✓ Dar clic en la opción Instalar.

- ✓ En la ventana para *Seleccionar tipo de componente de red* escoger la opción *Protocolo* y dar clic en *Agregar.*

- ✓ En la ventana *Seleccione el protocolo de red* elegir el protocolo Microsoft IPv6 y dar clic en Aceptar.

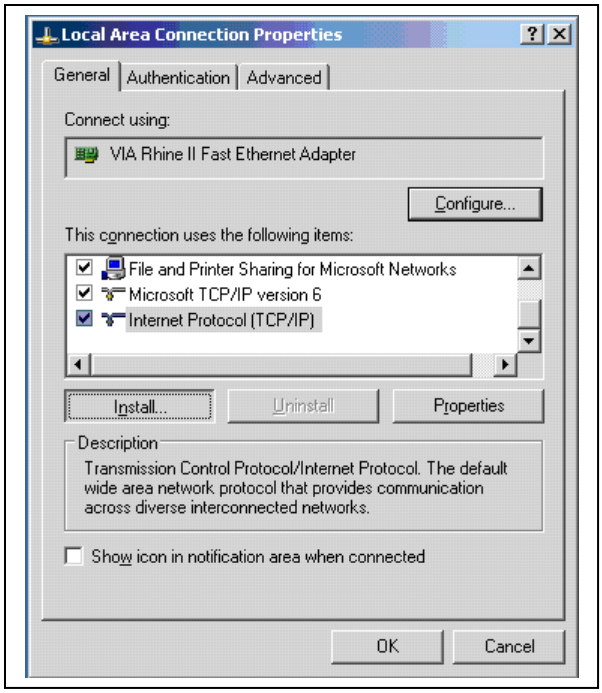


Figura 4.7 Propiedades de Conexión de Área Local

4.2 Configuración de IPv6 en Windows 2003 Server

Para la instalación del protocolo IPv6 se deben de seguir los siguientes pasos:

1. En el icono Panel de Control, seleccionar Conexión de Red y dar clic en la opción Conexión de Área Local.

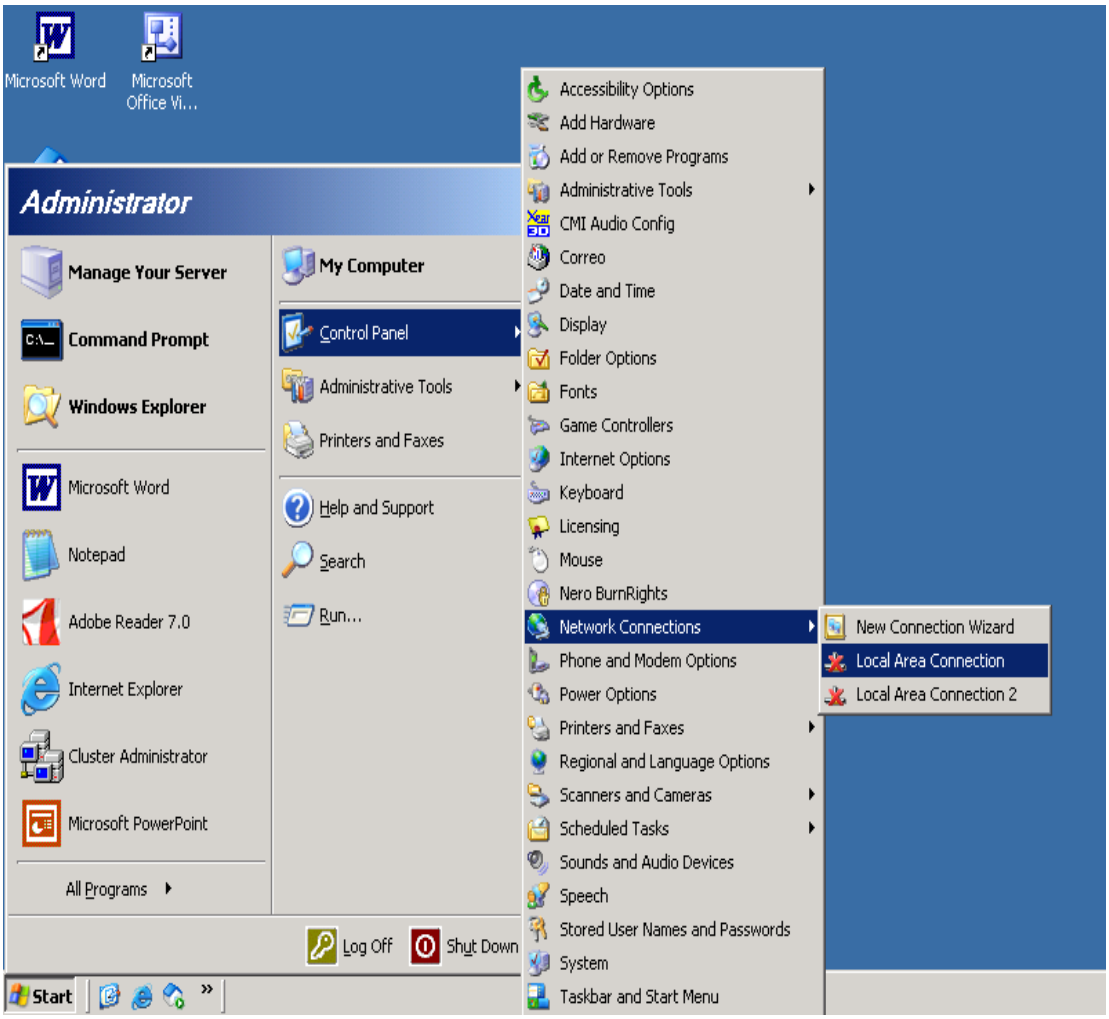


Figura 4.8 Forma de Accesar a Conexión de Área Local

2. Luego de haber realizado el paso anterior se visualizará la siguiente pantalla. Para instalar el protocolo IPv6 se debe dar clic en la opción *Propiedades* como se muestra a continuación.

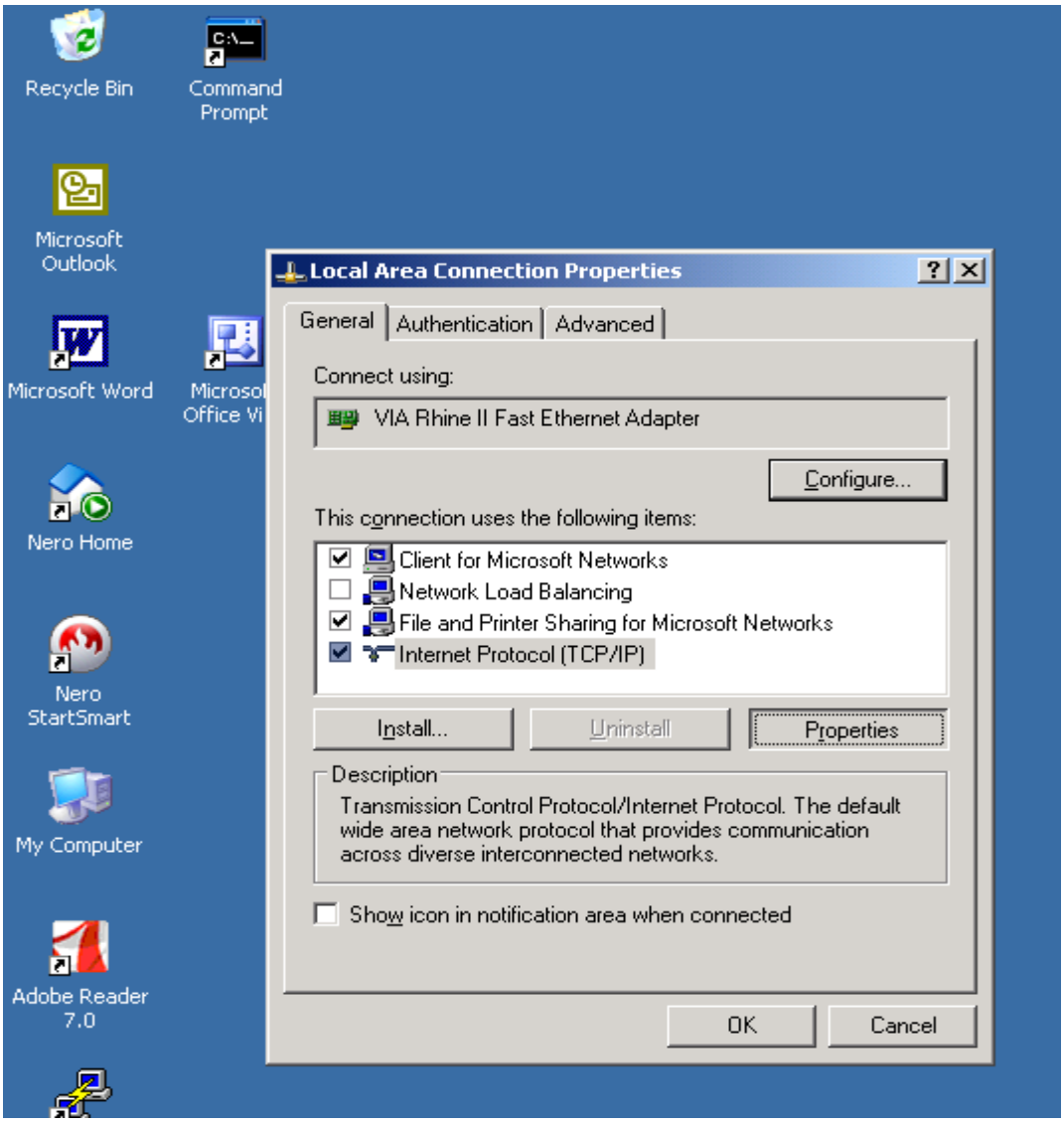


Figura 4.9 Propiedades de Conexión de Área Local

3. El sistema brinda la posibilidad de agregar un cliente, un servicio ó un protocolo, para lo cuál se debe seleccionar la opción *Protocolo*, a continuación dar un clic en la opción agregar como se muestra a continuación.

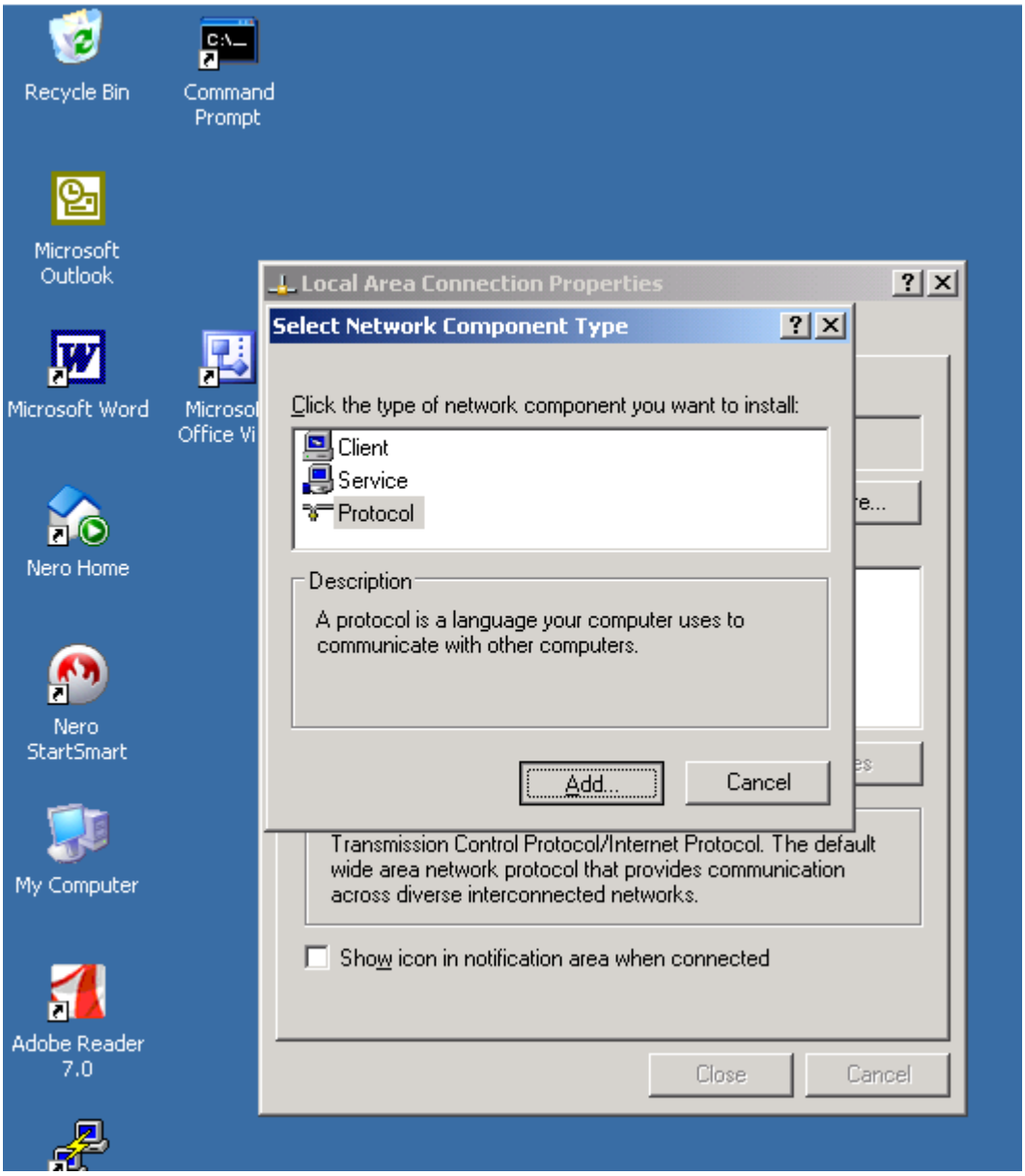


Figura 4.10 Selección de Componente de Red

4. Para completar la instalación del protocolo de red, se debe elegir el protocolo Microsoft IPv6 y dar clic en la opción aceptar.

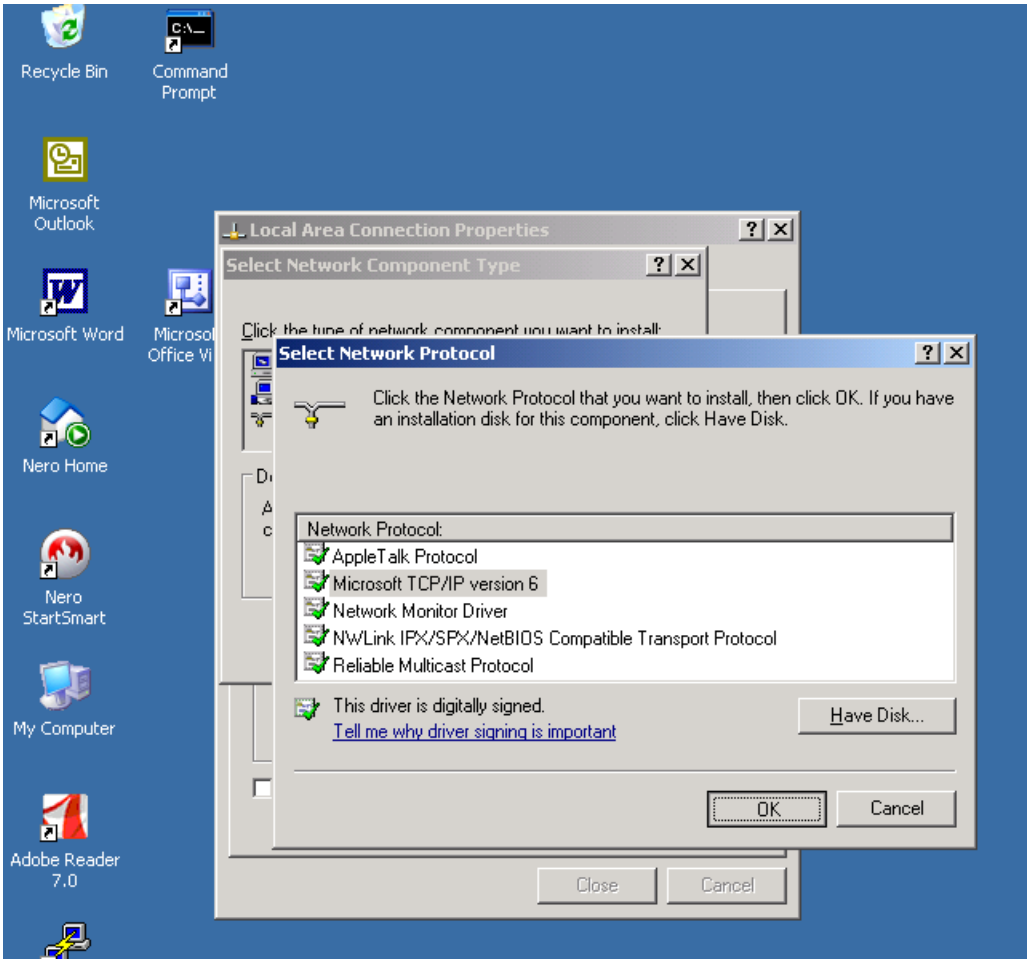


Figura 4.11 Selección del Protocolo de Red

Una vez instalado el protocolo IPv6 con éxito, se mostrará dicho protocolo en la ventana de Propiedades de Conexión de Área Local como se muestra a continuación.

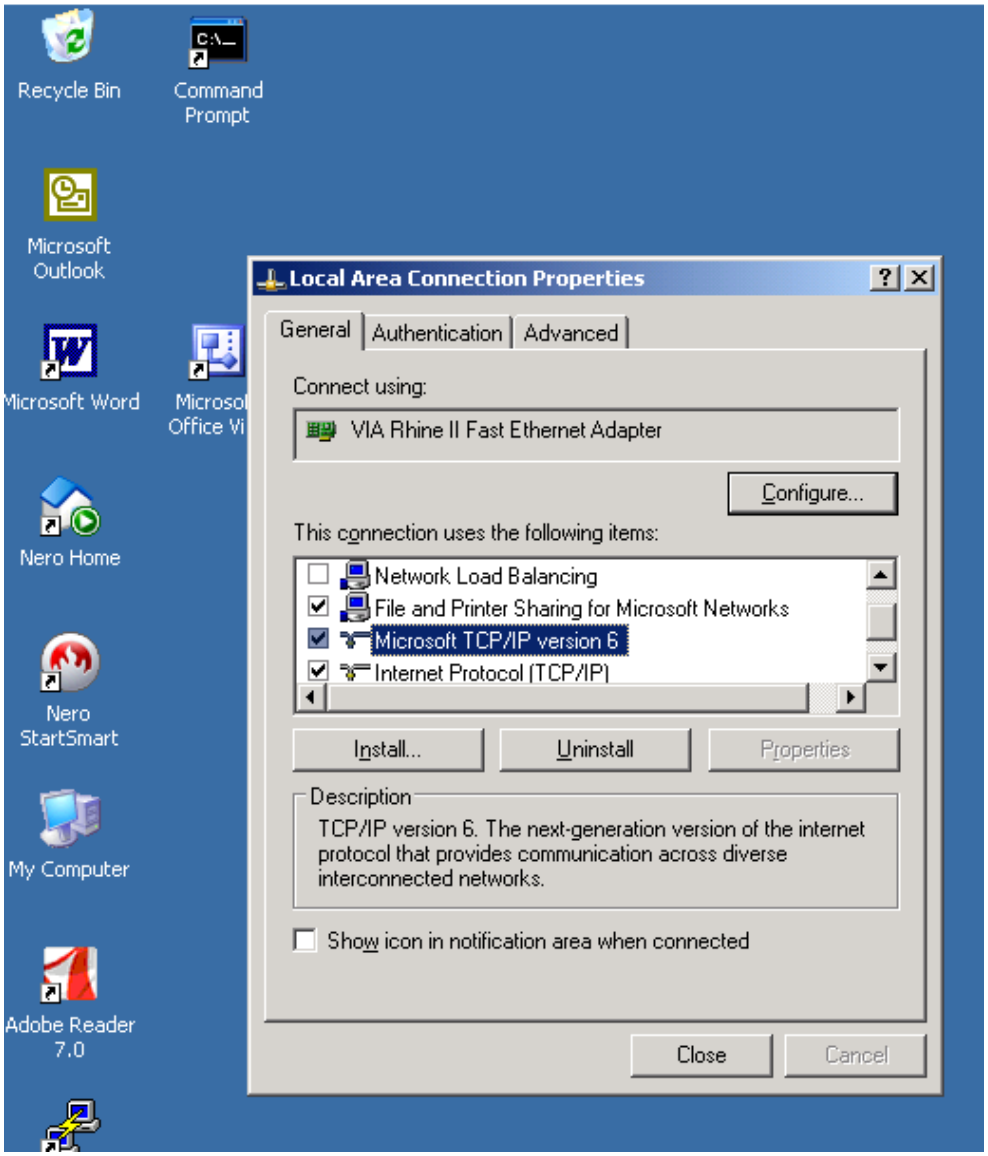


Figura 4.12 Propiedades de Conexión de Área Local

4.2.1 Pruebas de Conectividad con Windows 2003 Server

Una vez realizada la instalación del protocolo IPv6, se debe verificar la configuración y conectividad, para lo cuál se ejecutarán los siguientes comandos:

1. Verificar la Configuración de la Tarjeta de Red por medio del comando **ipconfig /all** como se muestra a continuación:

Figura 4.13 Configuración de la Tarjeta de Red

2. Prueba de conectividad a la Dirección Loopback por medio del comando **ping ::1**

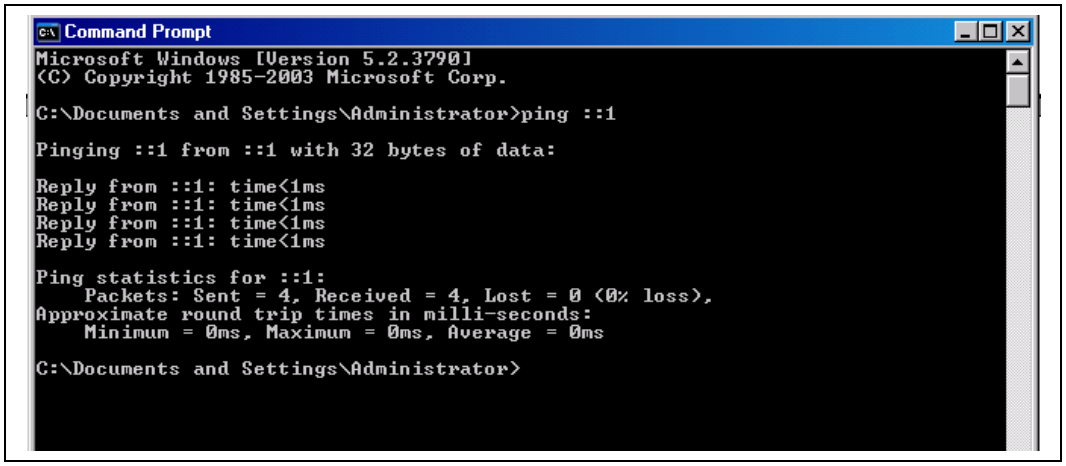


Figura 4.14 Ping a la Dirección de Loopback

3. Prueba a la Dirección de Red de Área Local.

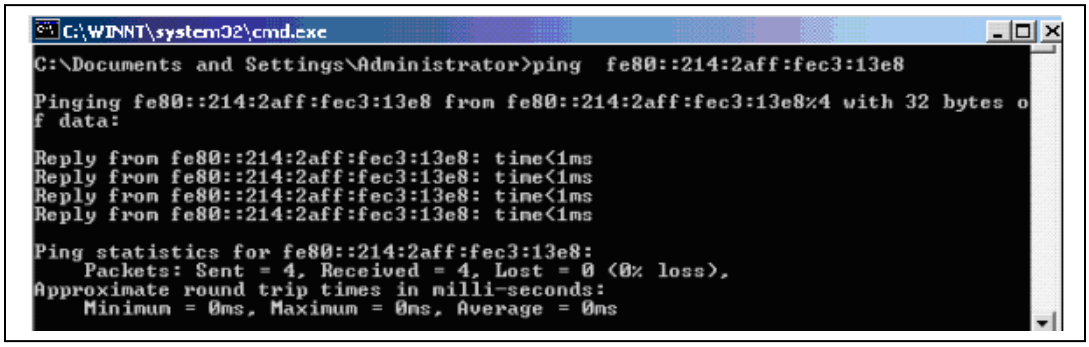


Figura 4.15 Ping de la Dirección de Red Área Local

4.3 Configuración IPv6 en Linux Mandrake 10.1

El protocolo IPv6 se implementa como un módulo en el Sistema Operativo Linux Mandrake 10.1, el cuál debe tener instalado la versión 2.2 ó superior del Kernel.

Para la instalación del protocolo IPv6 se deben seguir los siguientes pasos:

1. Verificación de Soporte de IPv6

2. Procedimiento para Verificar el Soporte de IPv6 en Linux.

1. Para verificar que el Kernel soporta IPv6, se debe comprobar que exista la siguiente entrada:

/proc/net/if_inet6

Si no se ha cargado correctamente se deberá ejecutar el siguiente comando:

 # modprobe IPv6

Si este se ha cargado satisfactoriamente se debe de ejecutar el siguiente comando:

 # lsmod |grep –w 'IPv6' && echo "módulo IPv6 cargado satisfactoriamente"

Una vez verificada la entrada se ejecuta el siguiente comando:

 # test –f /proc/net/if_inet6 && echo "corriendo IPv6 sobre Kernel"

2. Otra manera de cargar IPv6 es :

Agregar la siguiente línea en el archivo de configuración:

/etc/modules.com ó /etc/conf.modules

Para la carga del módulo de IPv6 se utiliza el siguiente comando:

alias net-pf –10 IPv6 #Carga automática del módulo IPv6

Para deshabilitar la carga del módulo de IPv6 se utiliza el siguiente comando:

alias net-pf –10 off #módulo IPv6 deshabilitado

4.3.1 Pruebas de Conectividad Linux Mandrake 10.1

Una vez realizada la verificación del soporte del Protocolo IPv6 en Linux Mandrake se debe verificar la configuración y conectividad, para lo cuál se ejecutarán los siguientes comandos:

1. Para probar la funcionalidad del Protocolo IPv6 sobre la plataforma Linux se debe escribir el comando **ifconfig**, luego de lo cuál se desplegará toda la información de la Configuración de la Tarjeta de Red como se muestra a continuación.

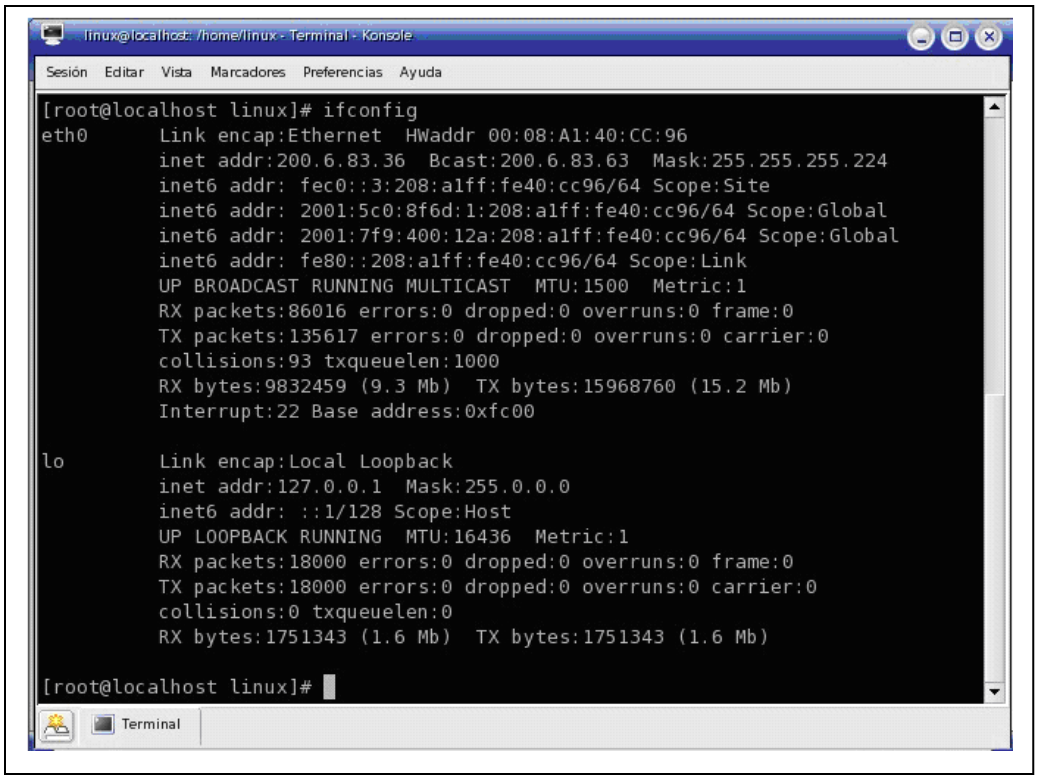


Figura 4.16 Configuración de la Tarjeta de Red

2. Ping a la Dirección de Sitio: **ping6 fec0::3:208:a1ff:fe40:cc96**

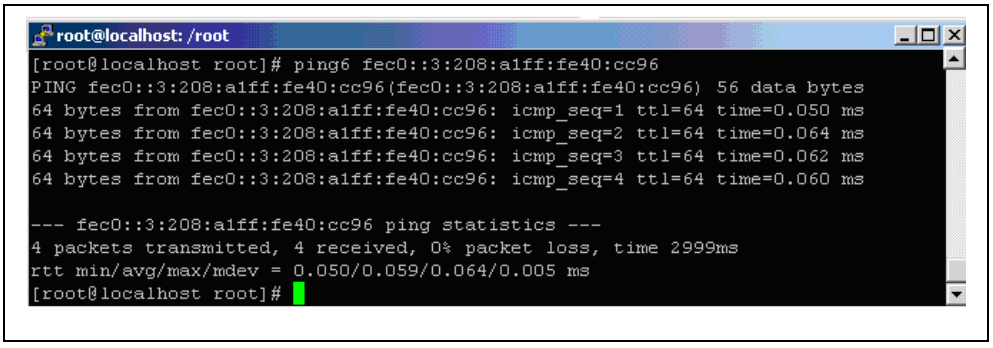


Figura 4.17 Ping a la Dirección de Sitio

3. Ping a la Dirección de Loopback: **ping6 ::1**

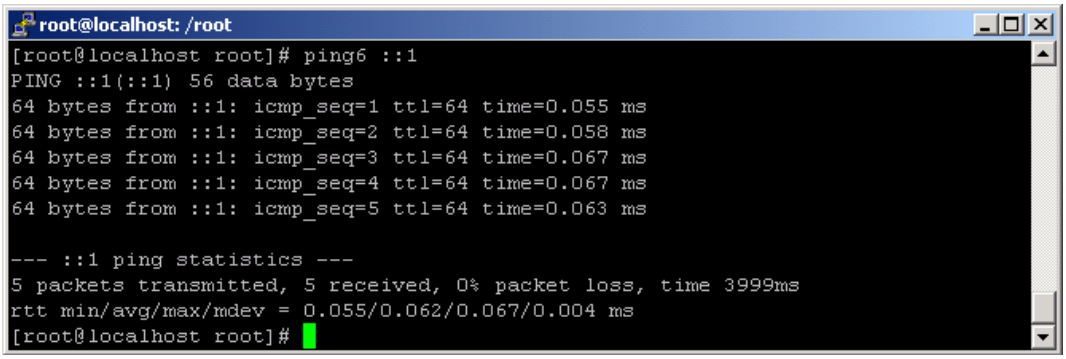


Figura 4.18 Ping a la Dirección de Loopback

4. Ping desde Linux hacia los Túneles

- ✓ **Túnel0: 2001:5c0:8f6d:1:208:a1ff:fe40:cc96**
- ✓ **Túnel2: 2001:7f9:400:12a:208:a1ff:fe40:cc96**

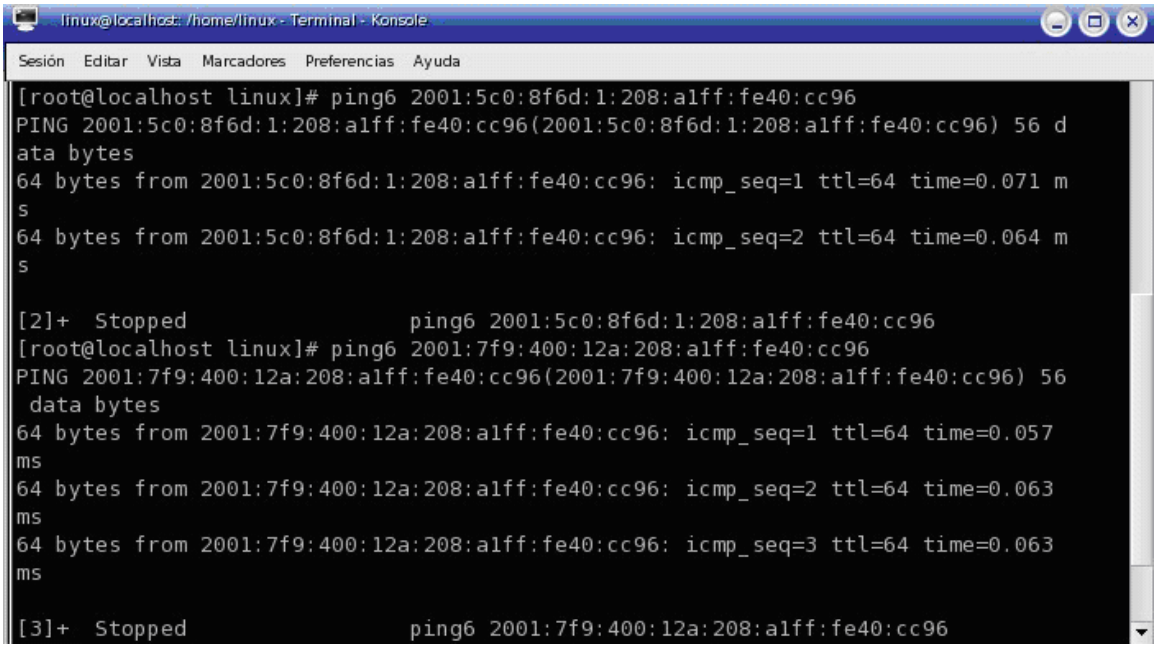


Figura 4.19 Ping desde Linux hacia los Túneles

5. Ping a las Direcciones IPv4

Dirección Windows: **200.6.83.38**

Dirección de Linux: **200.6.83.36**

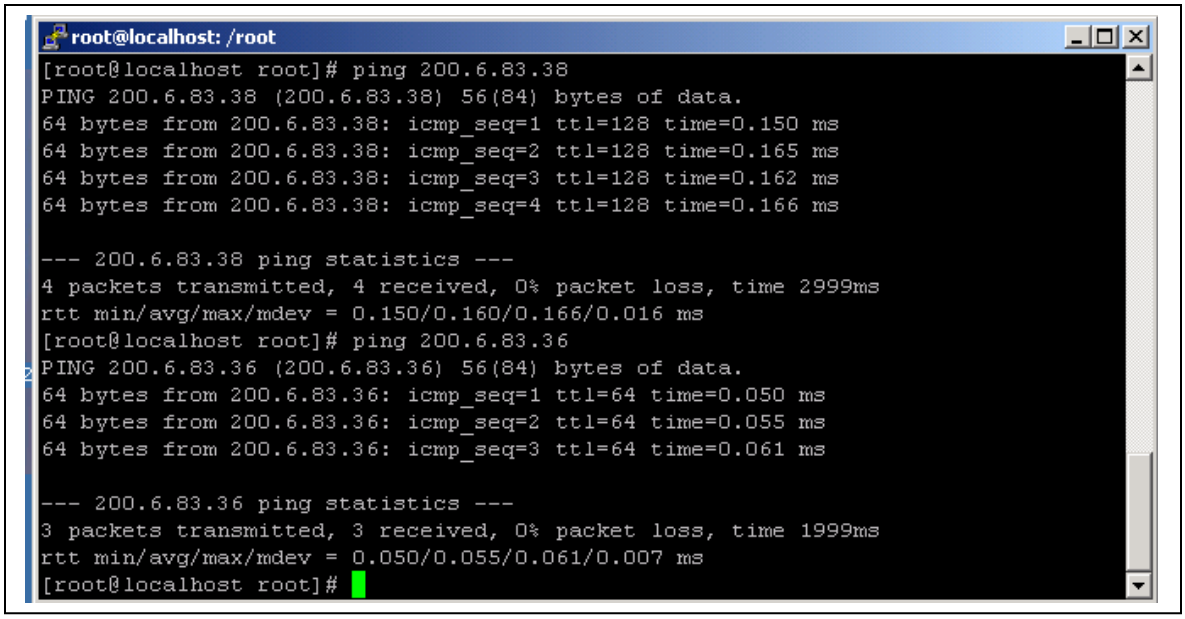


Figura 4.20 Ping a las Direcciones IPv4

CAPÍTULO V

PRUEBAS E IMPLEMENTACIÓN

5.1 Implementación de los Túneles

Para continuar con el desarrollo de Multihoming con IPv6, es necesario la creación de Túneles con proveedores del exterior que permitan realizar la transición de IPv4 a IPv6, ya que en nuestro país el “Ecuador” no existen proveedores que permitan realizar dicha conectividad. Obteniendo como resultado una conexión estable y segura, lo que es un requisito necesario para el desarrollo e implementación del mismo a través de la configuración en el Router, Sistemas Operativos e ISP.

5.1.1 Implementación del Tunneling Público con Linux

- **Creación del Túnel con el Proveedor Hexago**

Para realizar la configuración del primer túnel se utilizará el proveedor Hexago, para lo cuál se deben seguir los siguientes pasos cómo se muestran a continuación:

1. Crear una cuenta en Freenet6

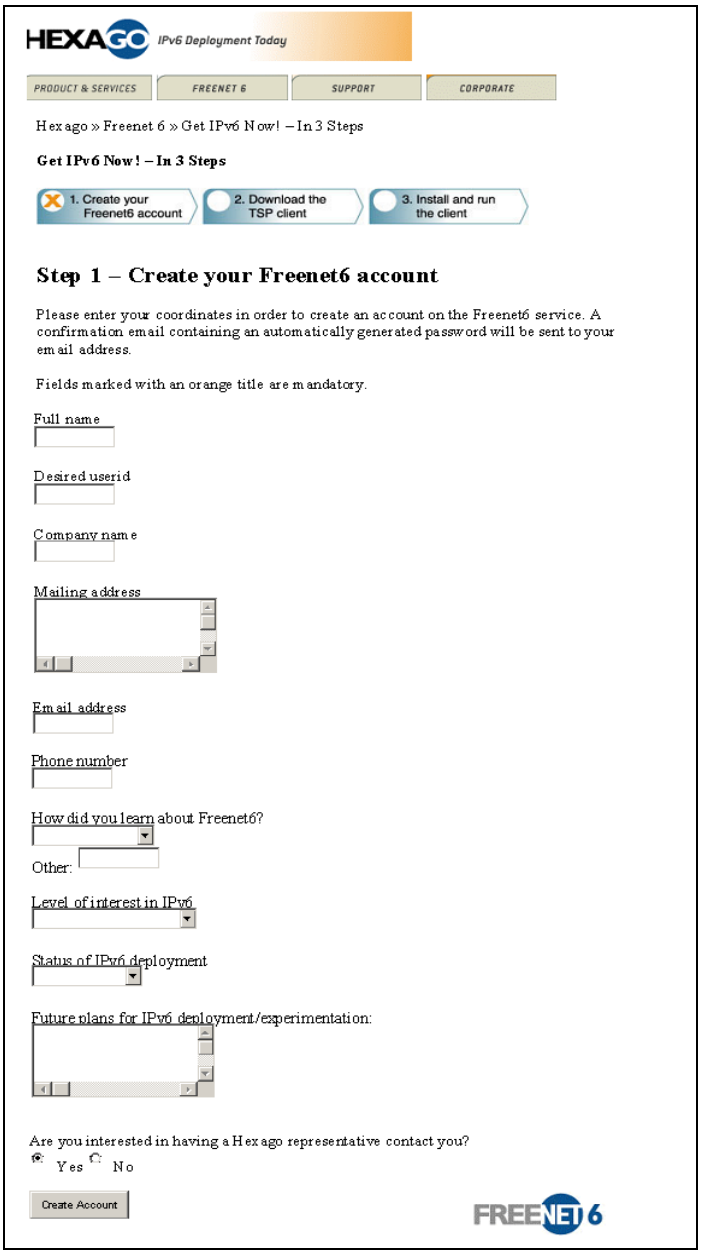


Figura 5.1 Creación de la cuenta en Freenet6

2.- Descargar el archivo TSP para la instalación del cliente en Linux.

Figura 5.2 Descarga del Archivo TSP

5.1.2 Implementación de Tunneling para Windows

Para la implementación del Túnel Consulintel se deben seguir los siguientes pasos:

- Ingreso de los datos personales, lo cual permitirá la creación del usuario y posteriormente la creación del Túnel.

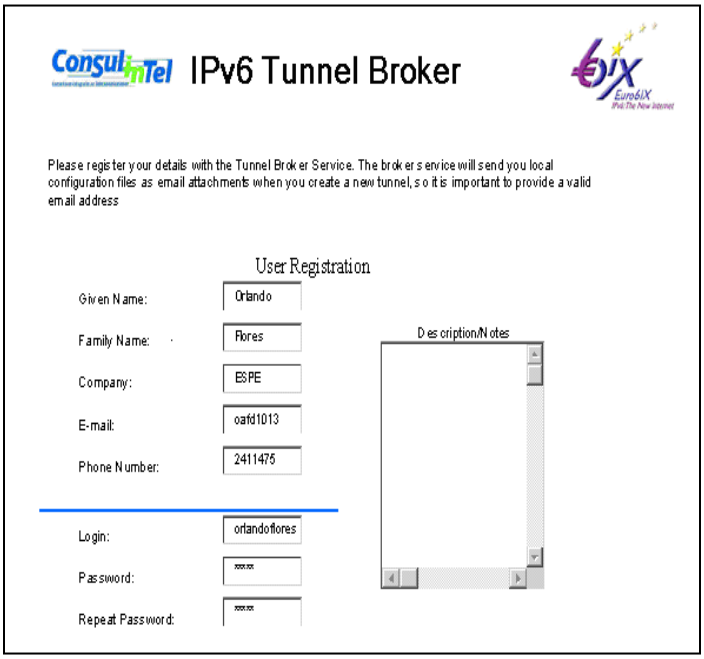


Figura 5.3 Creación de la Cuenta en Consulintel

- Realizar la autenticación en la página de Ingresos en la cuál se comprobará el usuario y la contraseña.

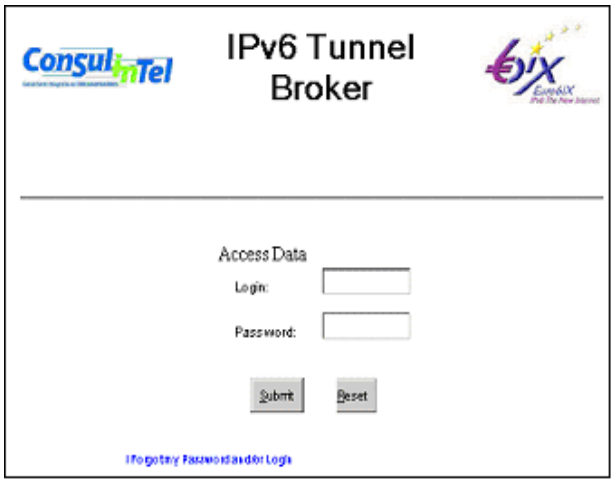


Figura 5.4 Página de Autenticación

- Se debe completar la información del Router Cisco 2500 en la siguiente página para realizar la creación del Túnel.

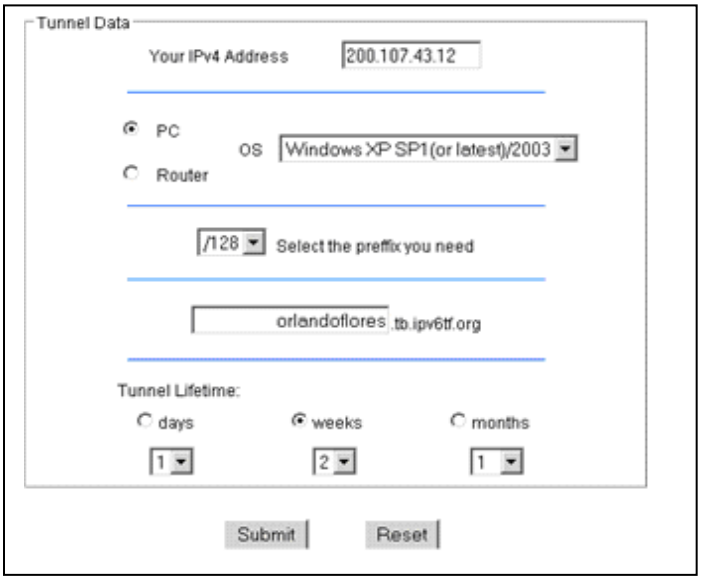


Figura 5.5 Creación del Túnel

- Verificación de la Activación del Túnel.

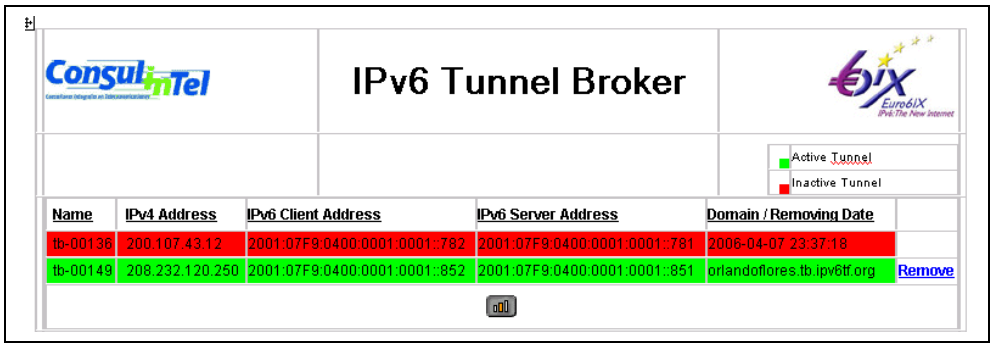


Figura 5.6 Verificación de la Activación del Túnel

- El proveedor de Consulintel, envía a través de Internet un mail al usuario, en el cuál se encuentran los datos para la configuración del Router, la dirección de IPv6 tanto del usuario como del proveedor.

Orlando Flores.

Este es un correo electrónico de confirmación sobre la creación del túnel que se ha solicitado.

Los datos del túnel se muestran a continuación.

Nombre:tb-00149

Dirección IPv4: 208.232.120.250

Dirección IPv4 del Servidor: 213.172.48.138

Dirección IPv6: 2001:0F9:0400:0001:0001::852

Dirección IPv6 del Servidor: 2001:07f9:0400.0001:0001::851

Prefijo de Red: 2001:07F9:0400:012A::/64

orlando es.tb.IPv6tf.org ha sido registrado en el DNS como el nombre de dominio del extremo del túnel.

Para configurar el túnel en el extremo se debe ejecutar el siguiente script en el equipo.

- ✓ ipv6 enable
- ✓ ipv6 uniscast-routing
- ✓ interface tunnelx
- ✓ no ip address
- ✓ IPv6 address 2001:07F9:0400:0001:0001::852/126
- ✓ tunnel source 208.232.120.250
- ✓ tunnel destination 213.1072.48.138
- ✓ tunnel mode IPv6ip
- ✓ ipv6 address 2001:07F9 :0400 :012A ::/64 eui-64
- ✓ ipv6 route::/0 tunnelx

“Adjunto a este correo se encontrará un script de configuración que se puede editar para cambiar la dirección IPv4 si se encuentra detrás de NAT, luego se debe grabar con la extensión .sh (para sistemas *BSD y los basados en Linux) ó .bat(para Windows) en vez de la extensión .txt y ejecutarlo en el equipo”.

“Para eliminar este túnel en el extremo remoto se debe acceder a la página personal del TB y seleccionar la opción ‘Eliminar’ que aparece junto al túnel que se desea eliminar“.

“La dirección es http://tb4.consulintel.euro6tx.org

Para eliminar el túnel en la máquina se debe ejecutar el siguiente script

no IPv6 route::0 tunnel x

no IPv6 address 2001:07F9:0400:012A::/64 eui-64

no interface tunnel x

****

The IPv6 Portal:http://www.IPv6tf.org

Barcelona 2005 Global IPv6 Summit
Slides available at:
http://www.IPv6-es.com”

“The electronic message contains information which may be privileged or confidential. The information is intended to be for the use individual(s) named above. If you are not the intended recipient be aware that any disclosure, copying, distribution or use of the contents of this information, including attached files, is prohibited”.

5.2 Configuración de IPv6 en el Router Cisco 2500

- ✓ **Agregar la Dirección del Túnel 0**

```
redespe#conf t
redespe(config)# int e0
redespe(config-if)#IPv6 address 2001:5C0:8F6D:1:50:54FF:FE80:3D30/64
redespe(config –if)#exit
redespe(config –if)#exit
redespe#sh run
building configuration…
Interface Tunnel0
description Hexago
    no ip address
    ipv6 address 2001:5C0:8FFF:FFFE:4B39/112
    tunnel source 208.232.120.250
    tunnel destination 64.86.88.116
    tunnel mode IPv6
    interface Tunnel2
    description consulintel
    no ip address
    ipv6 address 2001:7F9 :400 :1:1::852/112
    tunnel source 208.232.120.250
```

tunnel destination 213.172.48.138

tunnel mode IPv6ip

!

interface Ethernet0

ip address 192.168.1.254 255.255.255.0 secondary

ip address 200.6.83.33 255.255.255.240

ipv6 address 2001:5C0:8F6D:1:50:54FF:FE80:3D30/64

ipv6 address FEC0:3:50:54FF:FE80:3D30/64

IPv6 enable

no cdp enable

- ✓ **Agregar la Dirección del Túnel 2**

redespe#conf t

redespe(config)# int e0

redespe(config –if)#IPv6 address 2001:7f9:400:12A:50:54FF:FE80:3D30/64

redespe(config –if)#exit

redespe(config –if)#exit

redespe#sh run

building configuration…

Interface Tunnel0

description Hexago

no ip address

ipv6 address 2001:5C0:8FFF:FFFE:4B39/112

tunnel source 208.232.120.250

tunnel destination 64.86.88.116

tunnel mode IPv6

interface Tunnel2

description consulintel

no ip address

Ipv6 address 2001:7F9:400:1:1 ::852/112

tunnel source 208.232.120.250

tunnel destination 213.172.48.138

tunnel mode IPv6ip

!

interface Ethernet0

ip address 192.168.1.254 255.255.255.0 secondary

ip address 200.6.83.33 255.255.255.240

ipv6 address 2001:7F9:400:12A:50:54FF:FE80:3D30/64

ipv6 address FEC0:3:50:54FF:FE80:3D30/64

ipv6 enable

no cdp enable

✓ **Configuración Final del Router**

redespe#sh run

building configuration…

```
Interface Tunnel0
description Hexago
no ip address
ipv6 address 2001:5C0:8FFF:FFFE:4B39/112
tunnel source 208.232.120.250
tunnel destination 64.86.88.116
tunnel mode IPv6
interface Tunnel2
description consulintel
no ip address
ipv6 address 2001 :7F9 :400 :1 :1 ::852/112
tunnel source 208.232.120.250
tunnel destination 213.172.48.138
tunnel mode IPv6ip
!
interface Ethernet0
    ip address 192.168.1.254 255.255.255.0 secondary
    ip address  200.6.83.33  255.255.255.240
    ipv6 address 2001:7F9:400:12A:50:54FF:FE80:3D30/64
    ipv6 address 2001:5C0:8F6D:1:50:54FF:FE80:3D30/64
    ipv6 address FEC0:3:50:54FF:FE80:3D30/64
    ipv6 enable
    no cdp enable
```

5.3 Pruebas de Conectividad de los Túneles

5.3.1 Pruebas de Conectividad de IPv6 en Windows

- **Prueba de Conectividad a través de la página www.hexago.com**
  - **Conectividad con el Túnel 0**

Para comprobar el funcionamiento del túnel se puede utilizar un navegador de Internet y acceder a la página web de HEXAGO. Si el Túnel está trabajando de forma correcta se mostrará en la parte superior izquierda de la página la dirección IPv6 que fue asignada para dicho Túnel.

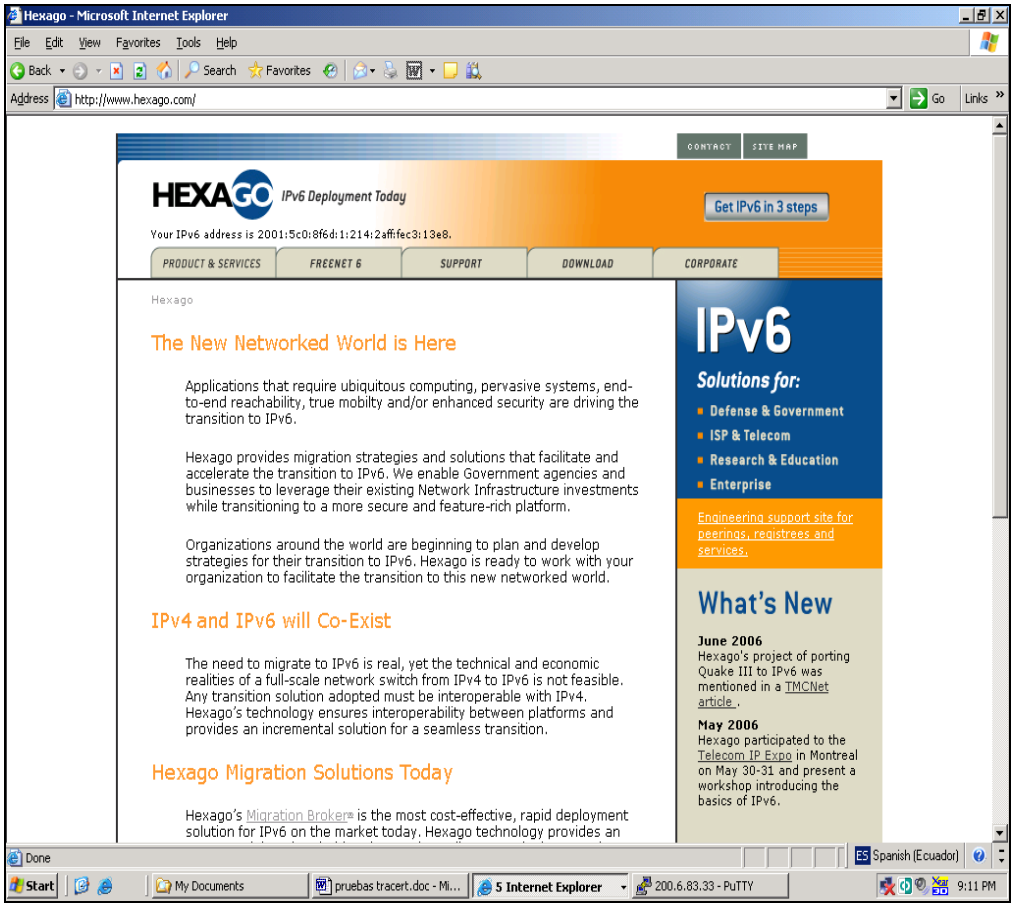


Figura 5.7 Página Web de HEXAGO

- **Prueba de Conectividad a través de la página www.ipv6.org**

  - **Conectividad con el Túnel 0**

En Internet existen sitios web que permitirán verificar la conectividad de IPv6 al ingresar a la dirección (www.ipv6.org), éste indicará la dirección del Túnel que se ha configurado como se muestra a continuación.

- ✓ **Túnel 0: 2001:5c0:8f6d:1:214:2aff:fec3:13e8**

Figura 5.8 Conectividad del Túnel 0

- **Conectividad con el Túnel 2**

- ✓ **Túnel 2: 2001:7f9:400:12a:2aff:fec3:13e8**

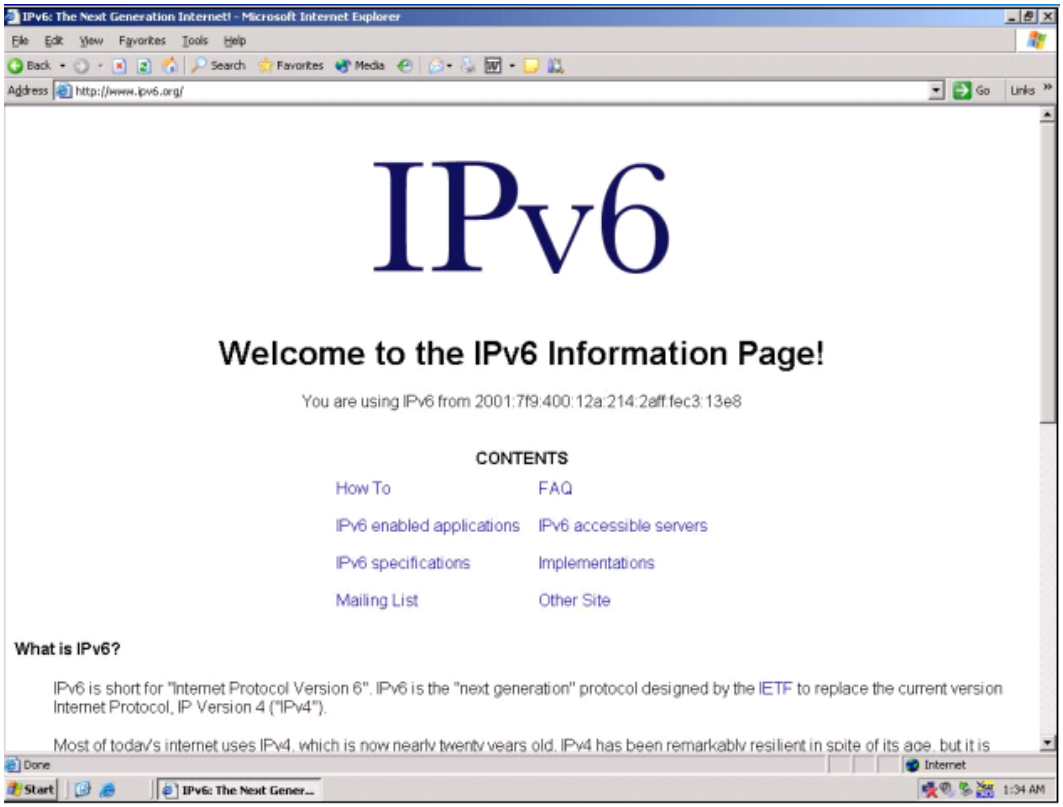


Figura 5.9 Conectividad del Túnel 2

5.3.1.1 Pruebas de Rutas a través de la página www.klingon.nl

Para realizar las pruebas de conectividad en IPv6 a través de Internet, se utilizarán algunos sitios, los cuáles permitirán verificar la ruta que toma el paquete hasta llegar a su destino y una vez más comprobar la funcionalidad del Túnel.

- **Traceroute del Túnel 0 a través de la página www.klingon.nl**

- ✓ **Túnel 0: 2001:5c0:8f6d:1:214:2aff:fec3:13e8**

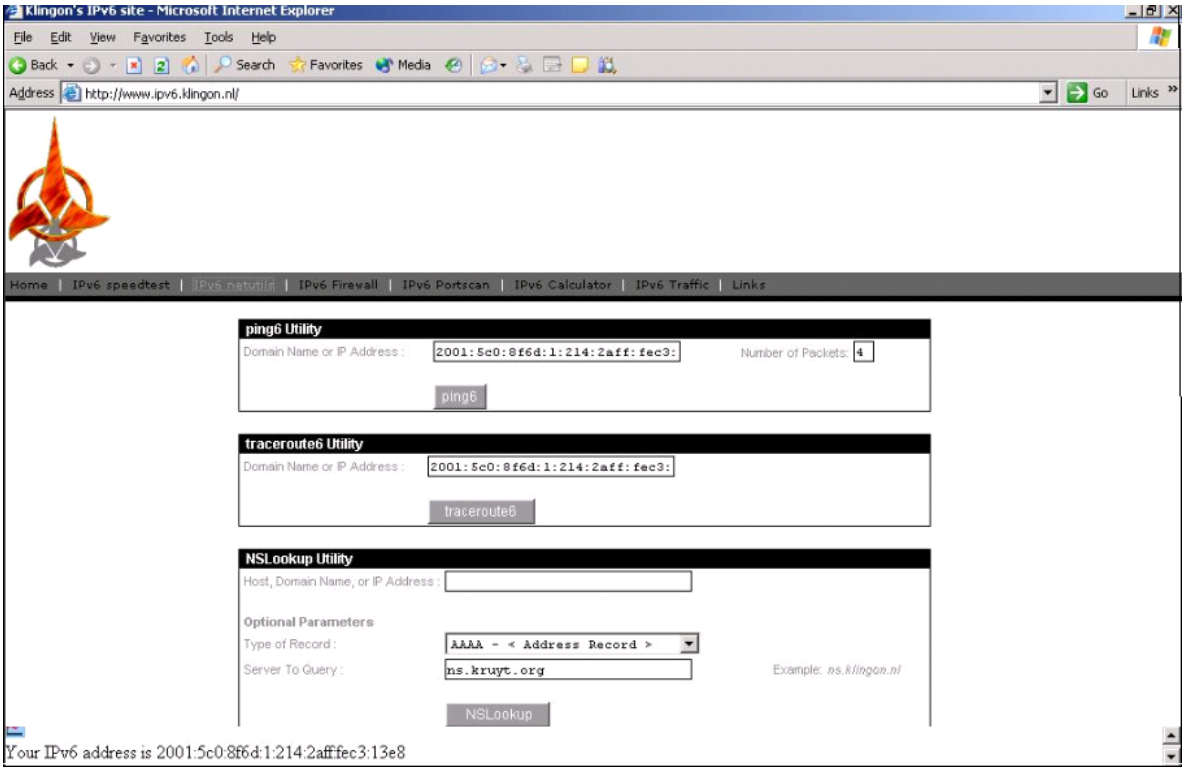


Figura 5.10 Traceroute del Túnel 0

1 gw-292.ams-01.nl.sixxs.net (2001:838:300:123::1) 9.997 ms 9.091 ms 9.941 ms

2 2001:838:2:1::1 (2001:838:2:1::1) 9.074 ms 7.592 ms 6.706 ms

3 se2.ams-ix.IPv6.concepts-ict.net (2001:838:0:10::1) 12.232 ms 8.645 ms 9.305 ms

4 ge0-1-0.rtr1.ams-tc2.io.nl (2001:7f8:1::a502:4587:1) 9.318 ms 9.247 ms 9.431 ms

5 ge-0-1-0-0-v189.IPv6.rtr1.ams-rb.io.nl (2001:1460:2000::1) 8.987 ms 9.814 ms 9.8 ms

6 if-11-0-1-459.6bb1.ad1-amsterdam.IPv6.teleglobe.net (2001:5a0:200::15) 10.12 ms 9.187 ms 9.791 ms

7 gin-ad1-core1.IPv6.teleglobe.net (2001:5a0:d00::13) 10.088 ms 9.728 ms 10.174 ms

8 if-7-0.mcore4.njy-newark.IPv6.teleglobe.net (2001:5a0:f00:100::5) 90.545 ms 91.925 ms 94.76 ms

9 if-12-0.mcore3.njy-newark.IPv6.teleglobe.net (2001:5a0:f00::5) 93.088 ms 94.464 ms 94.245 ms

10 if-5-0.core2.nto-newyork.IPv6.teleglobe.net (2001:5a0:f00::1) 92.64 ms 93.581 ms 94.911 ms

11 if-4-0-0.core2.nto-newyork.IPv6.teleglobe.net (2001:5a0:a00:200::2) 124.421 ms 83.046 ms 92.992 ms

12 if-5-0.mcore4.mtt-montreal.IPv6.teleglobe.net (2001:5a0:300:200::5) 101.738 ms 97.937 ms 97.963 ms

13 * * *

14 in-mtt-6bb1.IPv6.teleglobe.net (2001:5a0:300::1) 98.566 ms 98.926 ms 98.238 ms

15 ix-5-0-1.6bb1.mtt-montreal.IPv6.teleglobe.net (2001:5a0:300::6) 98.643 ms 100.677 ms 98.715 ms

16 2001:5c0:0:5::117 (2001:5c0:0:5::117) 100.389 ms 100.149 ms 91.34 ms

17 2001:5c0:8fff:fffe::4b39 (2001:5c0:8fff:fffe::4b39) 260.173 ms 266.398 ms *

18 2001:5c0:8f6d:1:214:2aff:fec3:13e8 (2001:5c0:8f6d:1:214:2aff:fec3:13e8) 332.195 ms 322.819 ms *

- **Traceroute del Túnel 2 a través de la página www.klingon.nl**

  - ✓ **Túnel 2: 2001:7f9:400:12a:214:2aff:fec3:13e8**

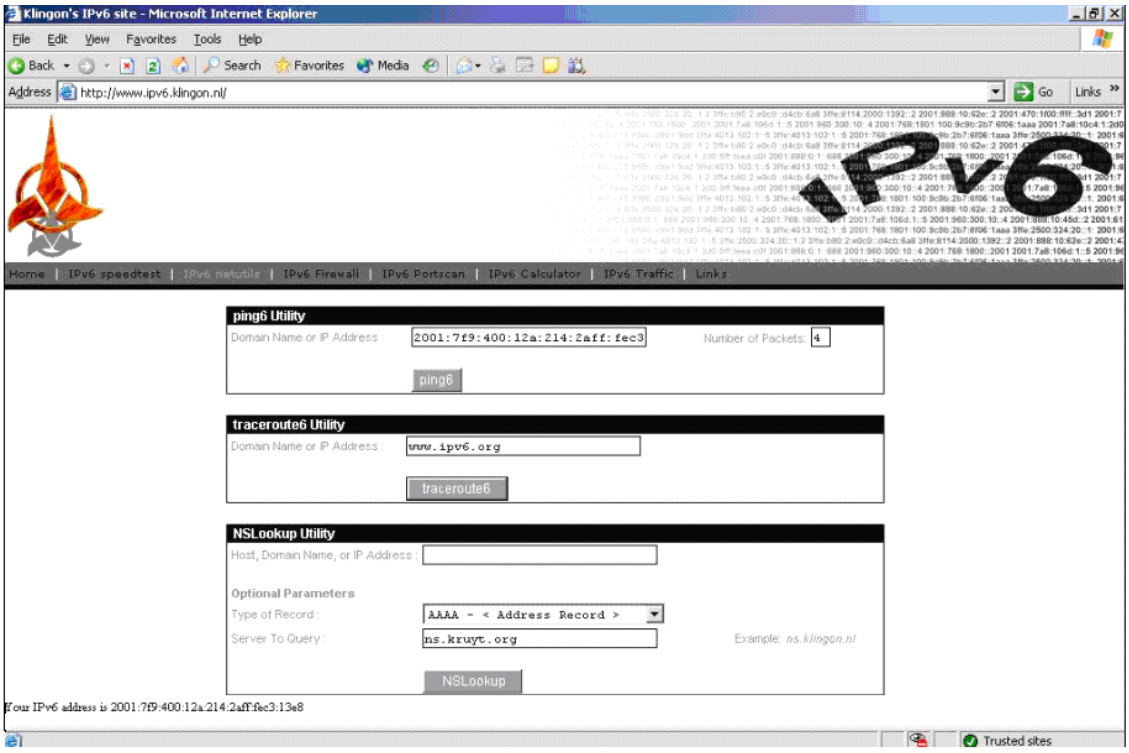


Figura 5.11 Traceroute del Túnel 2

1 gw-292.ams-01.nl.sixxs.net (2001:838:300:123::1) 11.005 ms 10.944 ms 10.966 ms

2 2001:838:2:1::1 (2001:838:2:1::1) 11.485 ms 11.422 ms 10.541 ms

3 se2.ams-ix.IPv6.concepts-ict.net (2001:838:0:10::1) 12.563 ms 12.83 ms 11.657 ms

4 nl-ams04a-re1-fe-0-0.IPv6.aorta.net (2001:7f8:1::a500:6830:1) 13.896 ms 3.873 ms 13.189 ms

5 be-bru01a-re1-t-2.IPv6.aorta.net (2001:730::1:63) 28.026 ms 19.168 ms 18.165 ms

6 uk-lon01a-re1-t-2.IPv6.aorta.net (2001:730::1:31) 24.31 ms 22.628 ms 23.564 ms

7 2001:7f8:4::31f9:1 (2001:7f8:4::31f9:1) 24.165 ms 32.244 ms 22.6 ms

8 52.ge0-3.cr1.lhr1.uk.occaid.net (2001:4830:fe:1100::1) 22.698 ms 23.124 ms 23.406 ms

9 consulintel-gw.customer.egll.occaid.net (2001:4830:d1:8::2) 71.16 ms 74.79 ms 76.911 ms

10 2001:7f9:400:1:1::852 (2001:7f9:400:1:1::852) 328.325 ms 398.304 ms 321.098 ms

11 2001:7f9:400:12a:214:2aff:fec3:13e8 (2001:7f9:400:12a:214:2aff:fec3:13e8) 361.657 ms 331.537 ms *

- **Traceroute a www.ipv6.org a través de la página www.teleglobe.net.**

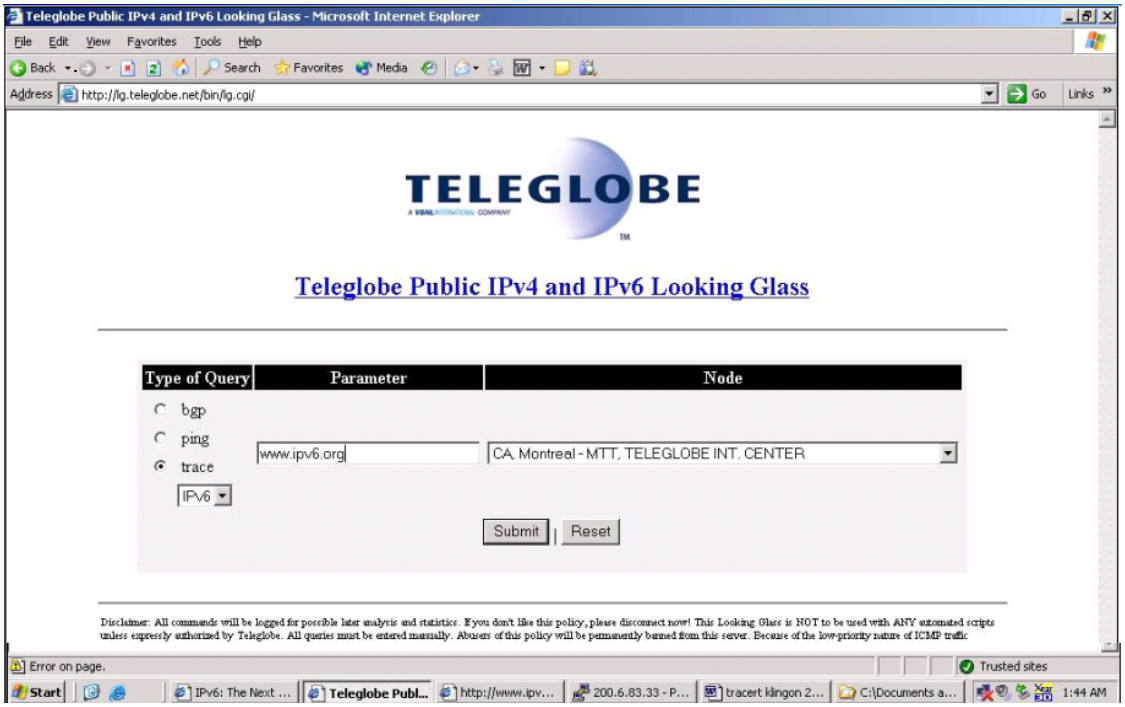


Figura 5.12 Traceroute a www.ipv6.org

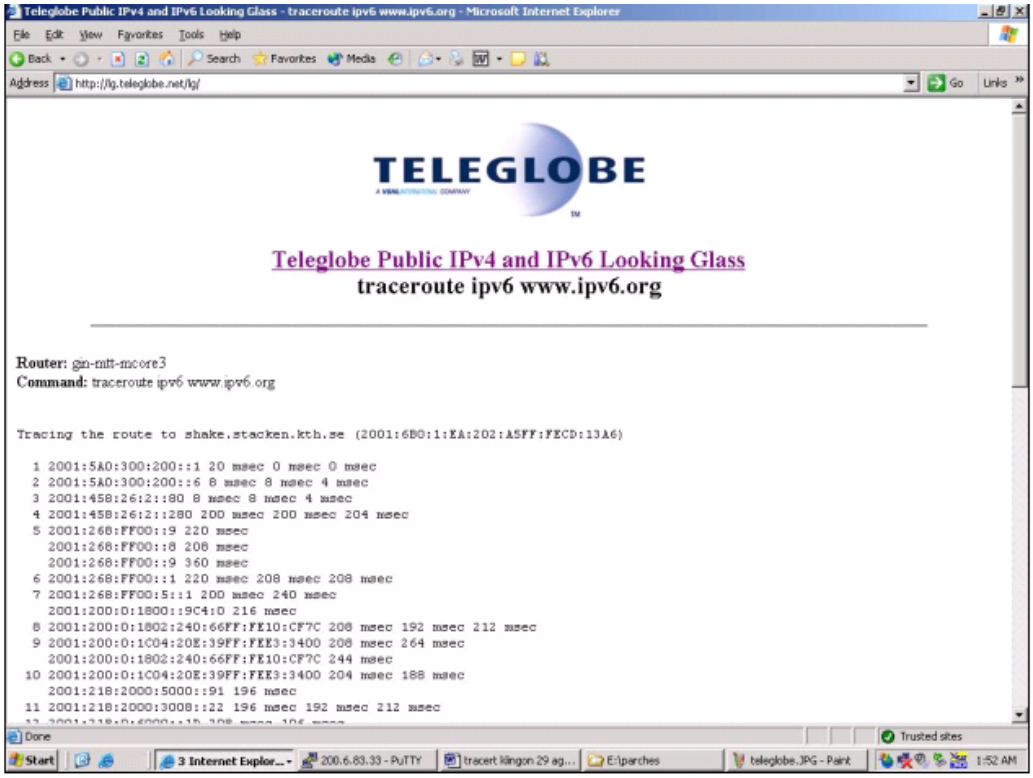


Figura 5.13 Traceroute a www.ipv6.org

Tracing the route to shake.stacken.kth.se

(2001:6B0:1:EA:202:A5FF:FECD:13A6)

1 2001:5A0:300:200::1 20 msec 0 msec 0 msec

2 2001:5A0:300:200::6 8 msec 8 msec 4 msec

3 2001:458:26:2::80 8 msec 8 msec 4 msec

4 2001:458:26:2::280 200 msec 200 msec 204 msec

5 2001:268:FF00::9 220 msec

2001:268:FF00::8 208 msec

2001:268:FF00::9 360 msec

6 2001:268:FF00::1 220 msec 208 msec 208 msec

7 2001:268:FF00:5::1 200 msec 240 msec

2001:200:0:1800::9C4:0 216 msec

8 2001:200:0:1802:240:66FF:FE10:CF7C 208 msec 192 msec 212 msec

9 2001:200:0:1C04:20E:39FF:FEE3:3400 208 msec 264 msec

2001:200:0:1802:240:66FF:FE10:CF7C 244 msec

10 2001:200:0:1C04:20E:39FF:FEE3:3400 204 msec 188 msec

2001:218:2000:5000::91 196 msec

11 2001:218:2000:3008::22 196 msec 192 msec 212 msec

12 2001:218:0:6000::1D 208 msec 196 msec

2001:218:2000:3004::22 204 msec

13 2001:218:0:6000::1D 204 msec 204 msec

2001:218:0:2000::CD 224 msec

14 2001:218:0:2000::CD 220 msec 220 msec

2001:418:0:2000::11 224 msec

15 2001:418:0:2000::2 240 msec 224 msec

2001:418:0:2000::11 220 msec

16 2001:418:0:2000::2 236 msec

2001:418:0:2000::172 240 msec

2001:418:0:2000::2 236 msec

17 2001:418:0:2000::172 216 msec

2001:418:0:2000::10E 308 msec

2001:418:0:2000::172 232 msec

18 2001:418:0:2000::10E 292 msec

2001:728:0:2000::5A 308 msec

2001:418:0:2000::10E 308 msec

19 2001:728:0:2000::5A 288 msec

2001:728:0:7001::B600 292 msec 308 msec

20 2001:728:0:7001::B600 308 msec

2001:728:0:4000::A 352 msec 360 msec

21 2001:948:0:F008::1 340 msec 340 msec 340 msec

22 2001:948:0:F026::2 352 msec 484 msec

2001:948:0:F008::1 412 msec

23 2001:948:0:F046::2 352 msec 336 msec 336 msec

24 2001:6B0:DEAD:BEEF:2::B1 340 msec

2001:948:0:F046::2 352 msec

2001:6B0:DEAD:BEEF:2::B1 340 msec

25 2001:6B0:FEED:DADA::19:68 336 msec

2001:6B0:DEAD:BEEF:2::B1 348 msec 348 msec

26 2001:6B0:1::1:5 356 msec

2001:6B0:FEED:DADA::19:68 332 msec 364 msec

27 shake.stacken.kth.se (2001:6B0:1:EA:202:A5FF:FECD:13A6) 356 msec 356 msec

2001:6B0:1::1:5 332 msec

5.3.2 Pruebas de Conectividad de IPv6 en Linux

- **Prueba de Conectividad a través de la página www.ipv6.org**

- ✓ **Conectividad con el Túnel 0**

Para realizar las pruebas de conectividad en IPv6 a través de Internet, se utilizarán algunos sitios, los cuáles permitirán verificar la ruta que toma el

paquete hasta llegar a su destino y una vez más comprobar la funcionalidad del Túnel.

- ✓ **Túnel 0: 2001:5c0:8f6d:1:208:a1ff:fe40:cc96**

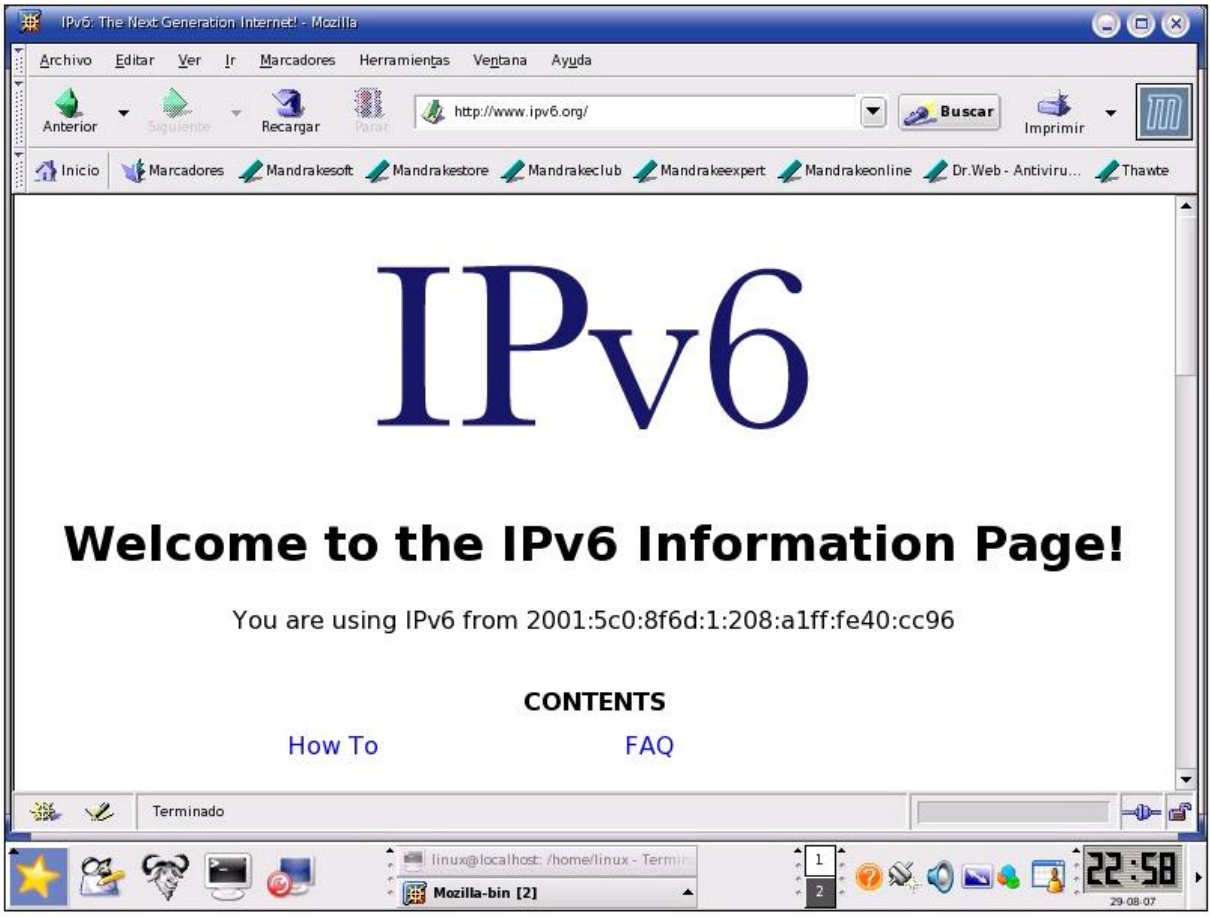


Figura 5.14 Conectividad del Túnel 0

- ➢ **Conectividad con el Túnel 2**

- ✓ **Túnel 2: 2001:7F9:400:12a:208:a1ff:fe40:cc96**

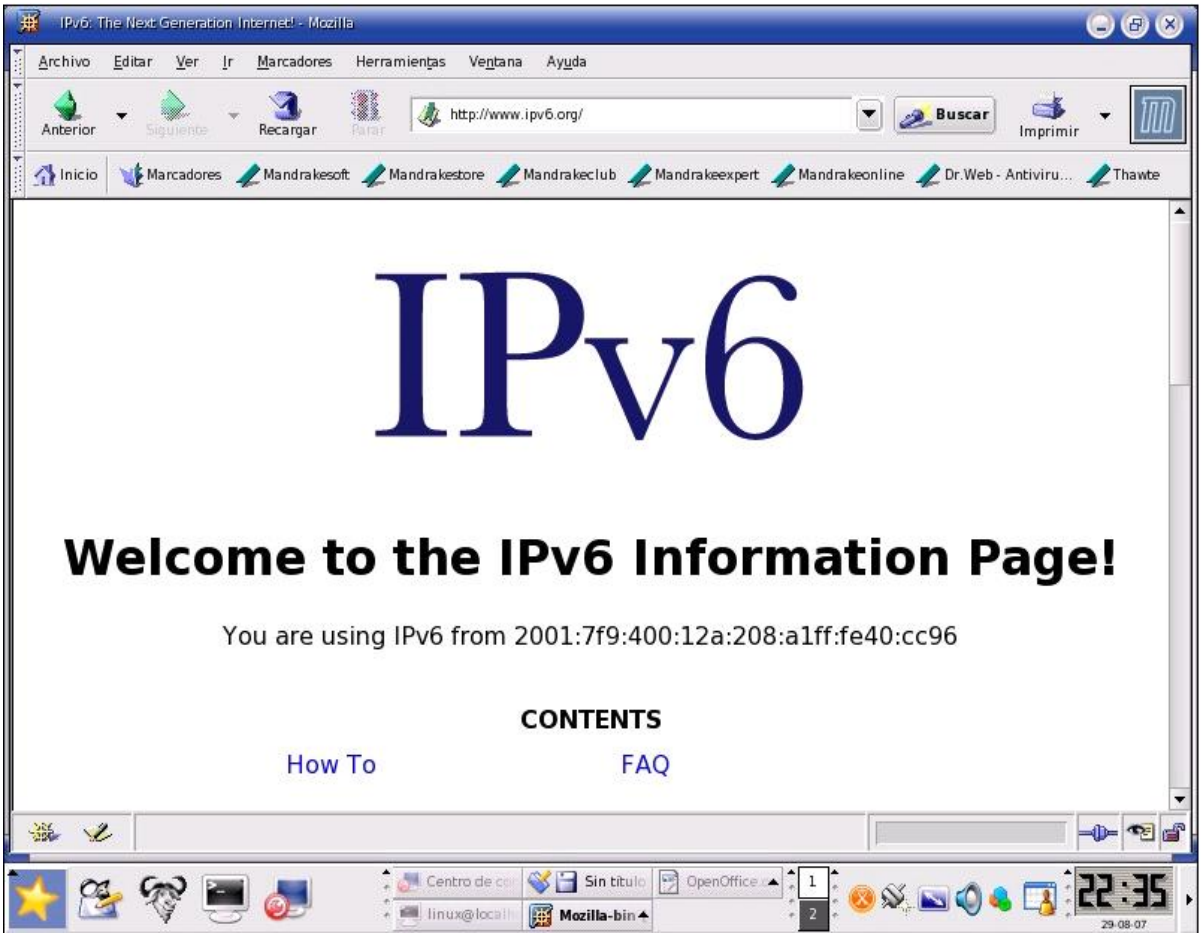


Figura 5.15 Conectividad del Túnel 2

- **Traceroute del Túnel 0 a través de la página www.teleglobe.net**
- **Traceroute al Túnel 0: 2001:5C0:8F6D:1:208:a1ff:fe40:cc96**

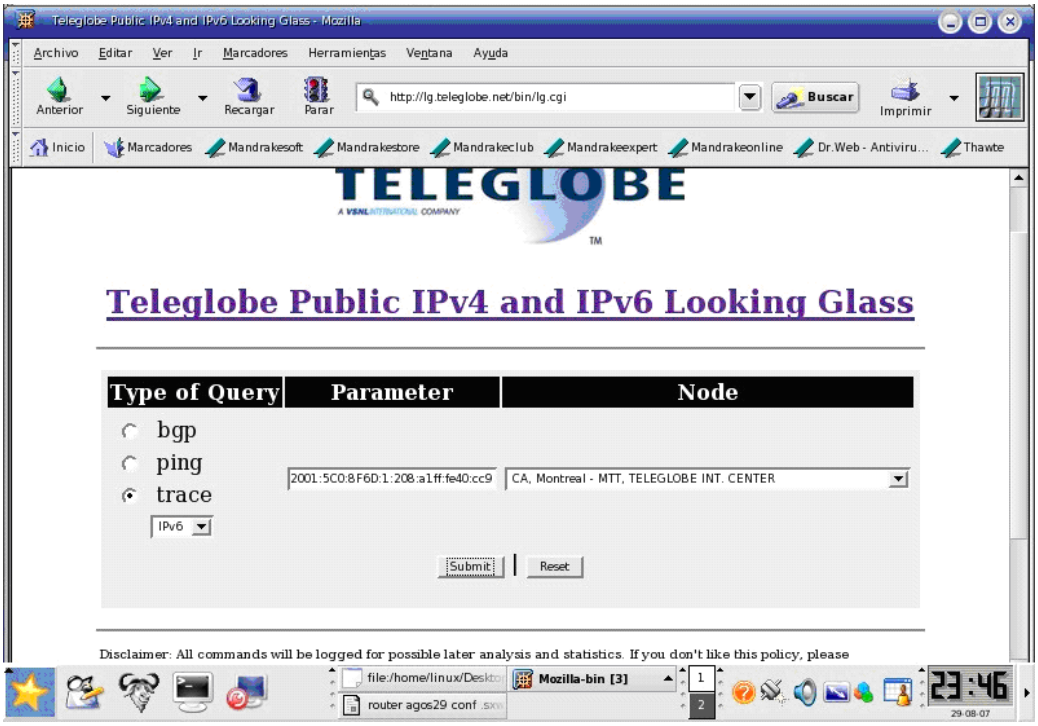


Figura 5.16 Traceroute del Túnel 0

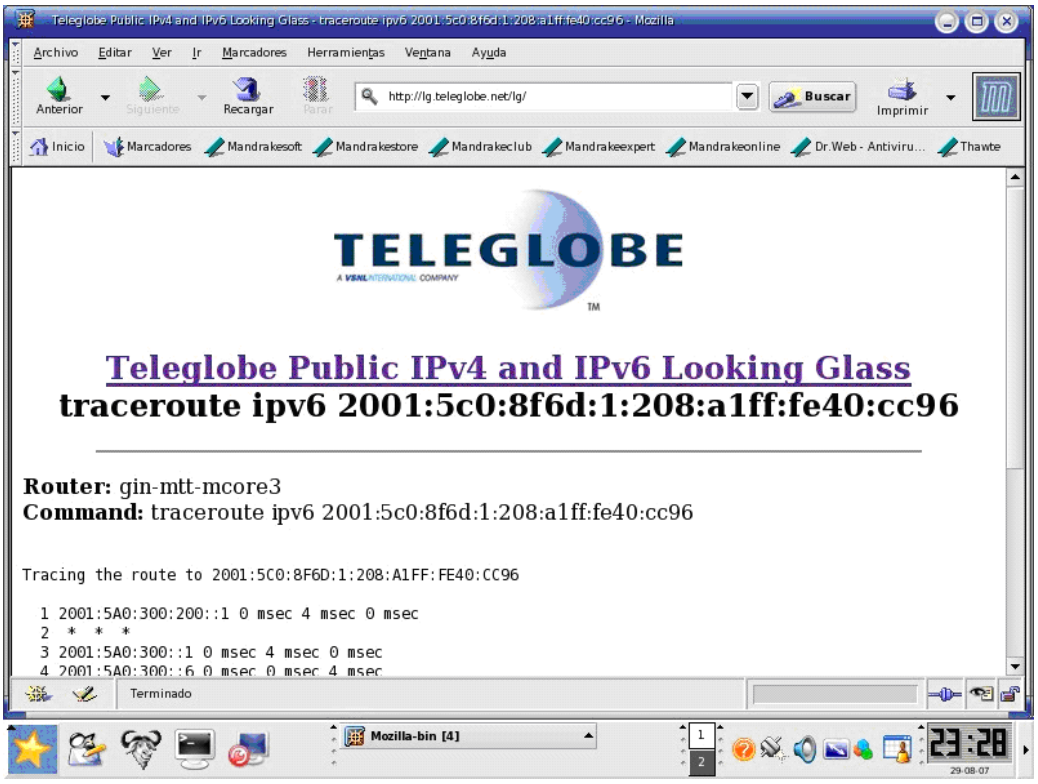


Figura 5.17 Traceroute del Túnel 0

Router: gin-mtt-mcore3

Command: Traceroute IPv6 2001:5C0:8F6D:1:208:a1ff:fe40:cc96

Tracing the route to 2001:5C0:8F6D:1:208:A1FF:FE40:CC96

1 2001:5A0:300:200::1 64 msec 0 msec 0 msec

2 * * *

3 2001:5A0:300::1 0 msec 0 msec 0 msec

4 2001:5A0:300::6 4 msec 4 msec 0 msec

5 2001:5C0:0:5::117 4 msec 4 msec 4 msec

6 2001:5C0:8FFF:FFFE::4B39 136 msec 260 msec 392 msec

7 2001:5C0:8F6D:1:208:A1FF:FE40:CC96 224 msec 136 msec 132 msec

- **Traceroute del Túnel 2 a través de la página www.teleglobe.net**

  - ✓ **Túnel 2:** 2001:7f9:400:12a:208:a1ff:fe40:cc96.

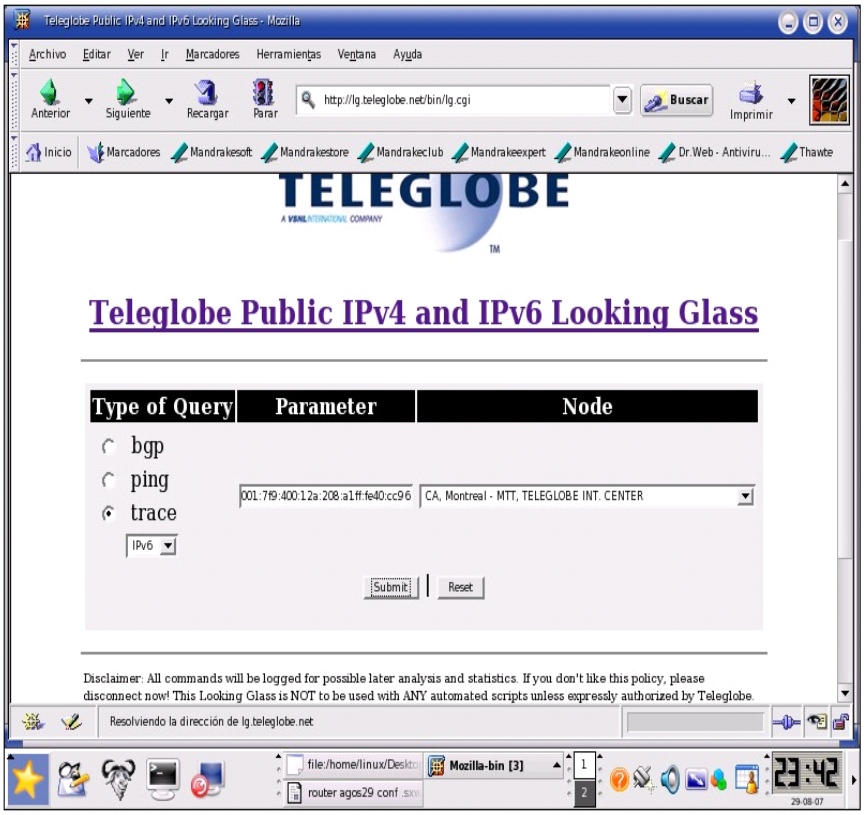


Figura 5.18 Traceroute del Túnel 2

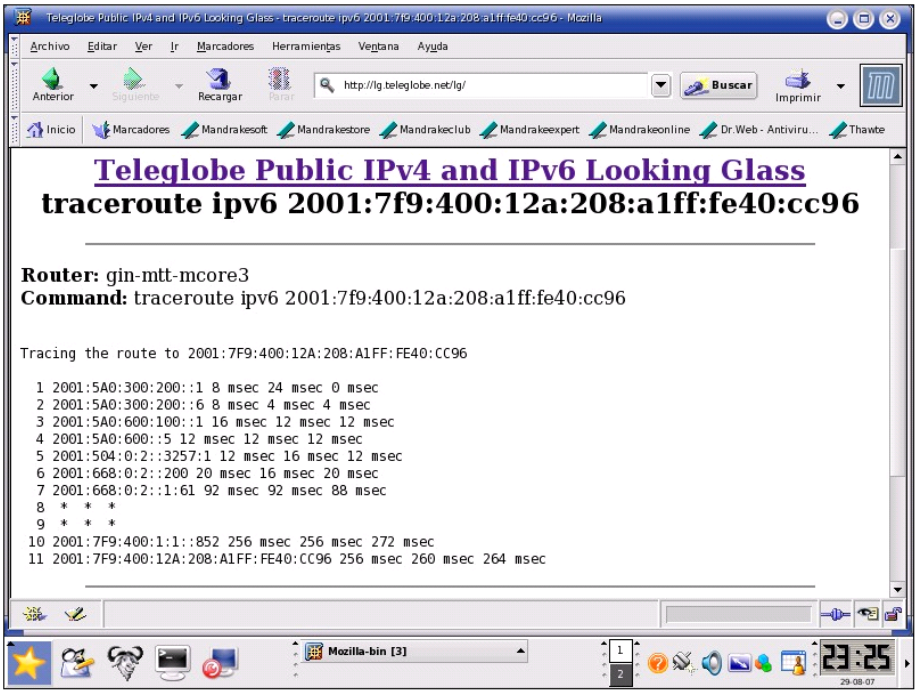


Figura 5.19 Traceroute del Túnel 2

Router: gin-mtt-mcore3

Command: traceroute IPv6 2001:7f9:400:12a:208:a1ff:fe40:cc96

Tracing the route to 2001:7F9:400:12A:208:A1FF:FE40:CC96

1 2001:5A0:300:200::1 4 msec 0 msec 52 msec

2 2001:5A0:300:200::6 200 msec 4 msec 8 msec

3 2001:5A0:600:100::1 16 msec 12 msec 12 msec

4 2001:5A0:600::5 12 msec 12 msec 12 msec

5 2001:504:0:2::3257:1 16 msec 12 msec 12 msec

6 2001:668:0:2::200 20 msec 20 msec 20 msec

7 2001:668:0:2::1:61 88 msec 92 msec 88 msec

8 * * *

9 * * *

10 2001:7F9:400:1:1::852 264 msec 260 msec 256 msec

11 2001:7F9:400:12A:208:A1FF:FE40:CC96 340 msec 268 msec 248 msec

- **Traceroute a www.ipv6.org a través de la página www.teleglobe.net**

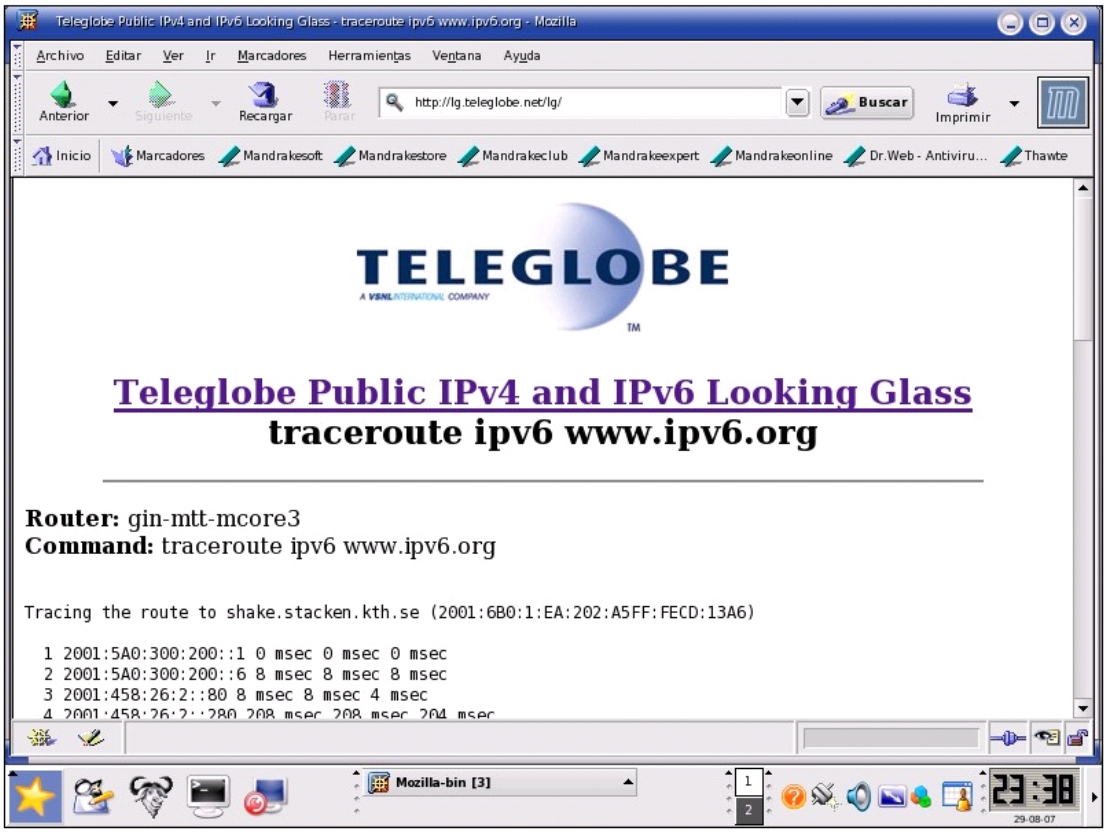


Figura 5.20 Traceroute de www.ipv6.org

router:gin-mtt-mcore3

Command: traceroute **IPv6** **www.ipv6.org**

Tracing the route to shake.stacken.kth.se (2001:6B0:1:EA:202:A5FF:FECD:13A6)

1 2001:5A0:300:200::1 0 msec 0 msec 0 msec

2 2001:5A0:300:200::6 8 msec 8 msec 8 msec

3 2001:458:26:2::80 8 msec 8 msec 4 msec

4 2001:458:26:2::280 208 msec 208 msec 204 msec

5 2001:268:FF00::8 204 msec 248 msec 208 msec

6 2001:268:FF00::1 212 msec

2001:268:FF00::2 260 msec 204 msec

7 2001:268:FF00:5::1 216 msec 284 msec

2001:200:0:1800::9C4:0 208 msec

8 2001:200:0:1802:240:66FF:FE10:CF7C 196 msec 196 msec

2001:200:0:1800::9C4:0 200 msec

9 2001:200:0:1C04:20E:39FF:FEE3:3400 192 msec 196 msec

2001:200:0:1802:240:66FF:FE10:CF7C 192 msec

10 2001:200:0:1C04:20E:39FF:FEE3:3400 212 msec

2001:218:2000:5000::91 208 msec

2001:200:0:1C04:20E:39FF:FEE3:3400 248 msec

11 2001:218:2000:5000::91 188 msec

2001:218:2000:3004::22 208 msec

2001:218:2000:5000::91 188 msec

12 2001:218:0:6000::1D 212 msec

2001:218:2000:3008::22 188 msec

2001:218:0:6000::1D 196 msec

13 2001:218:0:6000::1D 188 msec 204 msec

2001:218:0:2000::CD 224 msec

14 2001:418:0:2000::11 244 msec

2001:218:0:2000::CD 204 msec

2001:418:0:2000::11 240 msec

15 2001:418:0:2000::11 228 msec

2001:418:0:2000::2 240 msec

2001:418:0:2000::11 220 msec

16 2001:418:0:2000::172 220 msec 240 msec 220 msec

17 2001:418:0:2000::10E 296 msec

2001:418:0:2000::172 220 msec

2001:418:0:2000::10E 384 msec

18 2001:728:0:2000::5A 308 msec 292 msec

2001:418:0:2000::10E 308 msec

19 2001:728:0:7001::B600 296 msec 292 msec

2001:728:0:2000::5A 292 msec

20 2001:728:0:4000::A 340 msec 340 msec 356 msec

21 2001:948:0:F008::1 352 msec 340 msec 352 msec

22 2001:948:0:F026::2 340 msec 340 msec 336 msec

23 2001:948:0:F046::2 356 msec

2001:948:0:F026::2 348 msec 348 msec

24 2001:948:0:F046::2 348 msec

2001:6B0:DEAD:BEEF:2::B1 336 msec

2001:948:0:F046::2 332 msec

25 2001:6B0:FEED:DADA::19:68 396 msec

2001:6B0:DEAD:BEEF:2::B1 340 msec

2001:6B0:FEED:DADA::19:68 356 msec

26 2001:6B0:FEED:DADA::19:68 348 msec

2001:6B0:1::1:5 356 msec 356 msec

27 2001:6B0:1::1:5 344 msec

shake.stacken.kth.se (2001:6B0:1:EA:202:A5FF:FECD:13A6) 352 msec 356 msec

5.3.3 Pruebas de Conectividad a través del Router

5.3.3.1 Traceroute desde Túnel 0 al Túnel 2

redespe#traceroute

redespe#IPv6

Target IP6 address: 2001:5c0:8FFF: FFFE:4B39

Source IPV6 address: 2001:7F9:400:1:1::852

Numeric display? [no]:

Timeout in seconds [3]:

Probe count [3]:

Minimum Time to Live [1]:

Maximum Time to Live [30]: 10

Priority [0]:

Port Number [33434]:

Type escape sequence to abort.

Tracing the route to 2001:5C0:8FFF:FFFE:4B39

1 20001:5c0:8FFF:FFFE:4B39 16 msec 16 msec 16 msec

5.3.3.2 Traceroute Configurada la Salida por el Túnel 0 con Dirección de Origen Túnel 0

- **Traceroute a la Dirección www.ipv6tb.he.net.**

redespe# traceroute IPv6

Target IP6 address: 2001:470:FFFF::3

Source IPV6 address: 2001:5c0:8FFF:FFFE:4B39

Numeric display? [no]:

Timeout in seconds [3]:

Probe count [3]:

Minimum Time to Live [1]:

Maximum Time to Live [30]: 10

Priority [0]:

Port Number [33434]:

Type escape sequence to abort.

Tracing the route to 2001:470:FFFF::3

1 2001:5C0:8FFF:FFFE:4B38 136 msec 136 msec 136 msec

2 2001:5C0:0:5::114 144 msec 136 msec 136 msec

3 2001:5A0:300::5 136 msec 132 msec 136 msec

4 2001:5A0:300:100::1 132 msec 144 msec 152 msec

5 2001:5A0:300:200::1 132 msec 324 msec 168 msec

6 2001:5A0:300:200::6 144 msec 144 msec 144 msec

7 2001:458:26:2::80 144 msec 140 msec 140 msec

8 2001:458:26:2::500 336 msec 504 msec 332 msec

9 3FFE:81D0:FFFF:1:: 340 msec 340 msec 340 msec

10 2001:470:FFFF::3 344 msec 344 msec 368 msec

- **Traceroute a la Dirección www.ipv6.org**

redespe# traceroute IPv6

Target IP6 address: 2001:6B0:1:EA:202:A5FF:FECD:13A6

Source IPV6 address: 2001:5c0:8FFF:FFFE:4B39

Numeric display? [no]:

Timeout in seconds [3]:

Probe count [3]:

Minimum Time to Live [1]:

Maximum Time to Live [30]: 10

Priority [0]:

Port Number [33434]:

Type escape sequence to abort.

Tracing the route to 2001: 6B0:1:EA:202:A5FF:FECD:13A6

1 2001:5C0:8FFF:FFFE:4B38 148 msec 136 msec 136 msec

2 2001:5C0:0:5::114 132 msec 136 msec 136 msec

3 2001:5A0:300::5 144 msec 136 msec 132 msec

4 2001:5A0:300:100::1 324 msec 156 msec 132 msec

5 2001:5A0:300:200::1 136 msec 136 msec 136 msec

6 2001:5A0:300:200::6 140 msec 144 msec 144 msec

7 2001:5A0:ad0:100::a 216 msec 216 msec 216 msec

8 * * *

9 * * *

10 * * *

11 2001:5A0:CD0::5 224 msec 228 msec 228 msec

12 * * *

13 2001:1900:5:2::6 448 msec 448 msec 452 msec

14 2001:798:CC:1001:1301::1 452 msec 448 msec 448 msec

15 2001:798:CC:1301:1401::2 452 msec 448 msec 448 msec

16 2001:798:CC:1401:1501::2 464 msec 464 msec 496 msec

17 2001:798:15:10AA::2 464 msec 464 msec 468 msec

18 2001:948:0:F03F::1 472 msec * *

19 2001:948:0:F027::1 472 msec 472 msec 476 msec

20 2001:948:0:F046::2 476 msec 472 msec 476 msec

21 2001:6B0:DEAD:BEEF:2::B1 492 msec 480 msec 492 msec

22 2001:6B0:FEED:DADA::19:6B 476 msec 476 msec 476 msec

23 2001:6B0:1::1:5 484 msec 472 msec 476 msec

24 2001:6B0:1:EA:202:A5FF:FECD:13A6 584 msec 480 msec 480 msec

- **Traceroute a la Dirección www.broker.ipv6.ac.uk**

redespe# traceroute IPv6

Target IP6 address: 2001:630:d0:f000::2

Source IPV6 address: 2001:5c0:8FFF:FFFE:4B39

Numeric display? [no]:

Timeout in seconds [3]:

Probe count [3]:

Minimum Time to Live [1]:

Maximum Time to Live [30]: 10

Priority [0]:

Port Number [33434]:

Type escape sequence to abort.

tracing the route to 2001:630:d0:f000::2

1 2001:5C0:8FFF:FFFE:4B38 136 msec 136 msec 136 msec

2 2001:5C0:0:5::114 136 msec 132 msec 152 msec

3 2001:5A0:300::5 136 msec 132 msec 136 msec

4 2001:5A0:300:100::1 136 msec 136 msec 136 msec

5 2001:5A0:300:200::1 136 msec 132 msec 132 msec

6 2001:5A0:300:200::6 140 msec 152 msec 144 msec

7 2001:5A0:600:100::1 148 msec 148 msec 152 msec

8 2001:5A0:600::5 148 msec 144 msec 144 msec

9 2001:504:0:2::2914:1 180 msec 160 msec 164 msec

10 2001:418:0:2000::d5 160 msec 160 msec 160 msec

11 2001:418:0:2000::5 164 msec 168 msec 168 msec

12 2001:418:0:2000::7a 172 msec 164 msec 164 msec

13 2001:418:0:2000::10E 236 msec 232 msec 236 msec

14 2001:418:0:20000::1CA 236 msec 236 msec 240 msec

15 2001:728:0:2000::22 236 msec 236 msec 240 msec

16 2001:728:1C00:5000::A 448 msec 420 msec 500 msec

17 2001:630:0:10::51 420 msec 436 msec 432 msec

18 2001:630:0:10::129 428 msec 420 msec 440 msec

19 2001:630:0:10::55 420 msec 416 msec 436 msec

20 2001:630:0:10::2A 444 msec 424 msec 424 msec

21 2001:630:0:10::86Z 420 msec 440 msec 424 msec

22 2001:630:0:8017::2 440 msec 444 msec 440 msec

23 * * *

24 2001:630:C1:1::1 420 msec 440 msec 424 msec

25 2001:630:C1:10::2 424 msec 440 msec 424 msec

26 2001:630:D0:F000::2 428 msec 432 msec 456 msec

5.3.3.3 Traceroute Configurada la Salida por el Túnel 0 con Dirección de Origen Túnel 2

- **Traceroute a la Dirección www.ipv6tb.he.net.**

redespe#traceroute IPv6

Target IP6 address: 2001:470:FFFF::3

Source IPV6 address: 2001:7F9:400:1::1:852

Numeric display? [no]:

Timeout in seconds [3]:

Probe count [3]:

Minimum Time to Live [1]:

Maximum Time to Live [30]: 10

Priority [0]:

Port Number [33434]:

Type escape sequence to abort.

Tracing the route to 2001:470:FFFF::3

1 2001:5C0:0:5::117 248 msec 252 msec 256 msec

2 2001:5C0:0:5::114 252 msec 252 msec 248 msec

3 2001:5A0:300:::5 240 msec 248 msec 252 msec

4 2001:5A0:300:200::2 244 msec 248 msec 248 msec

5 2001:5A0:300:200::1 240 msec 244 msec 244 msec

6 2001:5A0:300:200::6 240 msec 232 msec 248 msec

7 2001:458:26:2::80 472 msec 452 msec 456 msec

8 2001:45826:2::500 444 msec 452 msec 432 msec

9 3FFE:81D0:FFFF:1:: 340 msec 344 msec 340 msec

10 2001:470:FFFF::3 352 msec 348 msec 332 msec

- **Traceroute a la Dirección www.ipv6.org**

redespe# traceroute IPv6

Target IP6 address: 2001:6B0:1:EA:202:A5FF:FECD:13A6

Source IPV6 address: 2001:7F9:400:1::1:852

Numeric display? [no]:

Timeout in seconds [3]:

Probe count [3]:

Minimum Time to Live [1]:

Maximum Time to Live [30]: 10

Priority [0]:

Port Number [33434]:

Type escape sequence to abort.

Tracing the route to 2001: 6B0:1:EA:202:A5FF:FECD:13A6

1 2001:5C0:0:5::117 252 msec 232 msec 232 msec

2 2001:5C0:0:5::114 248 msec 236 msec 252 msec

3 2001:5A0:300:::5 240 msec 248 msec 268 msec

4 2001:5A0:300:200::2 248 msec 232 msec 256 msec

5 2001:5A0:300:200::1 240 msec 252 msec 240 msec

6 2001:5A0:300:200::6 248 msec 248 msec 244 msec

7 2001:5A0:A00:100::A260 msec 256 msec 256 msec

8 * * *

9 * * *

10 * * *

11 2001:5A0:C00::5 264 msec 260 msec 264 msec

12 2001:7F8:4::D1C1:1 248 msec 240 msec 248 msec

13 2001:1900:5:2::6 284 msec 240 msec 248 msec

14 2001:798:CC:1001:1301::1 276 msec 280 msec 292 msec

15 2001:798:CC:1301:1401::2 276 msec 300 msec 268 msec

16 2001:798:CC:1401:1501::2 288 msec 284 msec 292 msec

17 2001:798:15:10AA::2 336 msec 344 msec 284 msec

18 2001:948:0:F03F::1 304 msec 296 msec *

19 2001:948:0:F046::2 296 msec 292 msec 296 msec

20 2001:948:0:F027::1 296 msec 300 msec 320 msec

21 2001:6B0:DEAD:BEEF:2::B1 324 msec 296 msec 300 msec

22 2001:6B0:FEED:DADA::19:68 300 msec 300 msec 420 msec

23 2001:6B0:1::1:5 412 msec 292 msec 428 msec

24 2001:6B0:1:EA:202:A5FF:FECD:13a6 436 msec 292 msec 420 msec

- **Traceroute a la Dirección www.broker.ipv6.ac.uk**

redespe# traceroute IPv6

Target IP6 address: 2001:630:D0:F000::2

Source IPV6 address: 2001:7F9:400:1::1:852

Numeric display? [no]:

Timeout in seconds [3]:

Probe count [3]:

Minimum Time to Live [1]:

Maximum Time to Live [30]: 10

Priority [0]:

Port Number [33434]:

Type escape sequence to abort.

tracing the route to 2001:630:D0:F000::2

1	2001:5C0:0:5::117	308 msec	248 msec	276 msec
2	2001:5C0:0:5::114	260 msec	244 msec	256 msec
3	2001:5A0:300:::5	248 msec	252 msec	228 msec
4	2001:5A0:300:200::2	248 msec	244 msec	228 msec
5	2001:5A0:300:200::1	260 msec	236 msec	252 msec
6	2001:5A0:300:200::6	248 msec	240 msec	244 msec
7	2001:5A0:600:100::1	252 msec	244 msec	244 msec
8	2001:5A0:600::5	248 msec	224 msec	244 msec
9	2001:504:0:2:2914:1	320 msec	380 msec	412 msec
10	2001:418:0:2000::D5	312 msec	336 msec	336 msec
11	2001:418:0:2000::5	344 msec	364 msec	340 msec
12	2001:418:0:2000::7A	328 msec	344 msec	332 msec
13	2001:418:0:2000::10E	256 msec	248 msec	240 msec
14	2001:418:0:2000::1CA	252 msec	256 msec	276 msec
15	2001:728:0:2000::22	316 msec	260 msec	248 msec
16	2001:728:1C00:5000::A	260 msec	248 msec	252 msec

17 2001:630:0:10::51 268 msec 248 msec 248 msec

18 2001:630:0:10::129 252 msec 584 msec 484 msec

19 2001:630:0:10::55 252 msec 408 msec 272 msec

20 2001:630:0:10::2a 384 msec 244 msec 292 msec

21 2001:630:0:10::86 256 msec 264 msec 256 msec

22 2001:630:8017::2 328 msec 256 msec 260 msec

23 * * *

24 2001:630:C1:1::1 260 msec 268 msec 236 msec

25 2001:630:C1:10::2 264 msec 256 msec 260 msec

26 2011:630:C1:100::2 264 msec 252 msec 260 msec

27 2001:630:D0:F000::2 260 msec 260 msec 264 msec

5.3.3.4 Traceroute Configurada la Salida por el Túnel 2 con Dirección de Origen Túnel 0

- **Traceroute a la Dirección www.ipv6tb.he.net.**

redespe# traceroute IPv6

Target IP6 address: 2001:470:FFFF::3

Source IPV6 address: 2001:5c0:8FFF:FFFE:4B39

Numeric display? [no]:

Timeout in seconds [3]:

Probe count [3]:

Minimum Time to Live [1]:

Maximum Time to Live [30]: 10

Priority [0]:

Port Number [33434]:

Type escape sequence to abort.

Tracing the route to 2001:470:FFFF::3

1 2001:7F9:400:1:1::851 476 msec 468 msec 472 msec

2 2001:4830:D1 :8:1::596 596 msec 588 msec 580 msec

3 2001:4830:FE :1100:::2 584 msec 580 msec 572 msec

4 2001:4830:FE :1100:::2 572 msec 568 msec 576 msec

5 2001:4830:FE :1301:::2 568 msec 588 msec 584 msec

6 2001:4830:FE :1753:::1 576 msec 596 msec 584 msec

7 2001:4830:FE :1750:::2 580 msec 616 msec 592 msec

8 3FFE:8070:1:13::1 584 msec 536 msec 516 msec

9 3FFE:8070:1:13::2 544 msec 532 msec 644 msec

10 2001:470:FFFF::3 564 msec 540 msec 528 msec

- **Traceroute a la Dirección www.ipv6.org**

redespe# traceroute IPv6

Target IP6 address: 2001:6B0:1:EA:202:A5FF:FECD:13A6

Source IPV6 address: 2001:5C0:8FFF:FFFE:4B39

Numeric display? [no]:

Timeout in seconds [3]:

Probe count [3]:

Minimum Time to Live [1]:

Maximum Time to Live [30]: 10

Priority [0]:

Port Number [33434]:

Type escape sequence to abort.

Tracing the route to 2001: 6B0:1:EA:202:A5FF:FECD:13A6

1 2001:7F9:400:1:1::851 476 msec 472 msec 472 msec

2 2001:4830:D1 :8:1::1 576 msec 600 msec 568 msec

3 2001:4830:FE :1100:::2 620 msec 592 msec 592 msec

4 2001:4830:FE :F150:::2 632 msec 628 msec 652 msec

5 2001:16D8:2 :80:::8473:1 628 msec 628 msec 624 msec

6 2001:7F8:21:9::219 500 msec 504 msec 500 msec

7 2001:6B0:7:4711::6 500 msec 500 msec 500 msec

8 2001:6B0:DEAD:BEEF:DA4A:0:1:8 504 msec 500 msec 492 msec

9 2001:6B0:DEAD:BEEF:2::A9 516 msec 644 msec 620 msec

10 2001:6B0:FEED:DADA::19:68 516 msec 484 msec 524 msec

11 2001:6B0:1::1:5 512 msec 508 msec 496 msec

12 2001:6B0:1:EA:202:A5FF:FECD:13A6 520 msec 504 msec 528 msec

- **Traceroute a la Dirección www. broker.ipv6.ac.uk**

redespe# traceroute IPv6

Target IP6 address: 2001:630:D0:F000::2

Source IPV6 address: 2001:5c0:8FFF:FFFE:4B39

Numeric display? [no]:

Timeout in seconds [3]:

Probe count [3]:

Minimum Time to Live [1]:

Maximum Time to Live [30]: 10

Priority [0]:

Port Number [33434]:

Type escape sequence to abort.

tracing the route to 2001:630:D0:F000::2

1 2001:7F9:400:1:1::851 452 msec 456 msec 456 msec

2 2001:4830:D1 :8:1::1 260 msec 264 msec 272 msec

3 2001:7F8:2:1::7 456 msec 488 msec 504 msec

4 2001:630:0:10::51 460 msec 476 msec 480 msec

5 2001:630:0:10::129 456 msec 456 msec 456 msec

6 2001:7F8:21:9::55 496 msec 480 msec 480 msec

7 2001: 630:0:10::2A 460 msec 472 msec 460 msec

8 2001: 630:0:10::86 484 msec 484 msec 472 msec

9 2001: 630:0:8017::2 460 msec 476 msec 472 msec

10 * * *

11 2001: 630:C1:1::1 456 msec 464 msec 460 msec

12 2001: 630:C1:10::2 568 msec 460 msec 476 msec

13 2001: 630:C1:100:2 476 msec 456 msec 472 msec

14 2001:630:DO:F000::2 468 msec 460 msec 472 msec

5.3.3.5 Traceroute Configurada la Salida por el Túnel 2 con Dirección de Origen Túnel 2

- **Traceroute a la Dirección www.ipv6tb.he.net.**

redespe# traceroute IPv6

Target IP6 address: 2001:470:FFFF::3

Source IPV6 address: 2001:7f9:400:1::1:852

Numeric display? [no]:

Timeout in seconds [3]:

Probe count [3]:

Minimum Time to Live [1]:

Maximum Time to Live [30]: 10

Priority [0]:

Port Number [33434]:

Type escape sequence to abort.

Tracing the route to 2001:470:FFFF::3

1 2001:7F9:400:1:1::851 232 msec 240 msec 252 msec

2 2001:4830:D1:8::1 280 msec 312 msec 308 msec

3 2001:4830:FE:1100::2 284 msec 336 msec 280 msec

4 2001:4830:FE:1010::2 360 msec 360 msec 364 msec

5 2001:4830:FF:1301::2 376 msec 380 msec 384 msec

6 2001:4830:FF:1753::1 396 msec 388 msec 396 msec

7 2001:4830:FF:1750::2 428 msec 460 msec 452 msec

8 2001:4830:E0:15::2 516 msec 536 msec 508 msec

9 3FFE:8070:1:13::2 516 msec 508 msec 512 msec

10 2001:470:FFFF::3 524 msec 524 msec 512 msec

- **Traceroute a la Dirección www.ipv6.org**

redespe# traceroute IPv6

Target IP6 address: 2001:6B0:1:EA:202:A5FF:FECD:13A6

Source IPV6 address: 2001:7f9:400:1::1:852

Numeric display? [no]:

Timeout in seconds [3]:

Probe count [3]:

Minimum Time to Live [1]:

Maximum Time to Live [30]: 10

Priority [0]:

Port Number [33434]:

Type escape sequence to abort.

Tracing the route to 2001: 6B0:1:EA:202:A5FF:FECD:13A6

1 2001:7F9:400:1:1::851 232 msec 236 msec 236 msec

2 2001:4830:D1:8::1 284 msec 284 msec 284 msec

3 2001:4830:FE:1100::2 268 msec 288 msec 280 msec

4 2001:4830:FE:F150::2 316 msec 332 msec 320 msec

5 2001:16D8:2:80::8473:1 320 msec 304 msec 296 msec

6 2001:7F8:21:9::219 304 msec 324 msec 320 msec

7 2001:6B0:7:4711::6 304 msec 324 msec 304 msec

8 2001:6B0:DEAD:BEEF:DA4A:0:1:8 308 msec 320 msec 324 msec

9 2001:6B0:DEAD:BEEF:2::A9 320 msec 328 msec 340 msec

10 2001:6B0:FEED:DADA::19:68 324 msec 324 msec 328 msec

11 2001:6B0:1::1:5 316 msec 316 msec 320 msec

12 2001:6B0:1:EA:202:A5FF:FECD:13A6 332 msec 332 msec 328 msec

- **Traceroute a la Dirección www.broker.ipv6.ac.uk**

redespe# traceroute IPv6

Target IP6 address: 2001:630:D0:F000::2

Source IPV6 address: 2001:7f9:400:1::1:852

Numeric display? [no]:

Timeout in seconds [3]:

Probe count [3]:

Minimum Time to Live [1]:

Maximum Time to Live [30]: 10

Priority [0]:

Port Number [33434]:

Type escape sequence to abort.

tracing the route to 2001:630:D0:F000::2

1 2001:7F9:400:1:1::851 240 msec 244 msec 248 msec

2 2001:7F8:2:C00B::2 288 msec 284 msec 292 msec

3 2001:7F8:2:1::7 296 msec 284 msec 280 msec

4 2001:630:0:10:51 280 msec 280 msec 296 msec

5 2001:630:0:10:129 384 msec 284 msec 292 msec

6 2001:630:0:10::55 292 msec 280 msec 300 msec

7 2001:630:0:10::2A 288 msec 296 msec 304 msec

8 2001:630:0:10::86 272 msec 340 msec 292 msec

9 2001:630:0:8017::2 284 msec 292 msec 292 msec

10 * * *

11 2001:630:C1:1::1 296 msec 896 msec 1012 msec

12 2001:630:C1:10::2 368 msec 284 msec 288 msec

13 2001:630:C1:100::2 296 msec 288 msec 292 msec

14 2001:630:D0:F000::2 316 msec 284 msec 300 msec

CAPÍTULO VI

CONCLUSIONES Y RECOMENDACIONES

6.1 CONCLUSIONES

- Se ha finalizado con éxito el presente proyecto de tesis “Multihoming con IPv6” en la empresa “netXperts Consulting S.A.”, verificando así la funcionalidad del mismo, la cual es no perder conectividad a Internet dentro de la red Lan.

- El protocolo IPv6 reemplazará la versión actual del Protocolo IPv4, debido a que una de sus ventajas es el mayor espacio de direcciones, lo que permitirá el incremento de nuevos dispositivos a las redes actuales.

- Se estableció que una característica esencial que diferencia el protocolo IPv6 de IPv4, es la reducción del número de campos que tiene la cabecera de IPv6, lo que permite mejorar la seguridad, movilidad, y calidad de servicio en las conexiones.

- Otra de las características del Protocolo IPv6 en su cabecera, es que se crean nuevos tipos de cabeceras para realizar el transporte de los paquetes, lo que ayuda a mejorar la forma de transportar los paquetes hacia los nodos de destino.

- Por medio de la Investigación que se ha desarrollo para este proyecto, se han obtenido conocimientos acerca de las diferentes formas de conexión y transcisición del Protocolo IPv4 a IPv6, así como comandos que permitirán realizar las diferentes pruebas y configuraciones.

- Mediante las pruebas realizadas de Multihoming con IPv6 en la empresa "netXperts Consulting S.A.", se pudo verificar que ésta no tendrá pérdidas económicas, debido a las configuraciones realizadas en los equipos de comunicación permitiendo así que la conexión sea permanente, rápida y eficaz.

- Al realizar la conexión de Multihoming con IPv6 mediante la creación de los diferentes túneles, se pudo observar los saltos que sigue un paquete por las diferentes rutas, hasta llegar a su destino, comprobando de ésta manera la ruta más óptima para el envío de dichos paquetes.

- Un problema que se presentó para el desarrollo del proyecto fue la poca disponibilidad de información de Multihoming e IPv6, además que no existen proveedores locales que permitan realizar la creación de los diferentes túneles, para lo cuál se realizó una Investigación acerca de proveedores extranjeros que permitan realizar dicha conexión; lo cuál constituyó una limitación en el desarrollo del mismo.

6.2 RECOMENDACIONES

- Se recomienda a la empresa “netXperts Consulting S.A.”, seguir brindando el apoyo a los estudiantes del Departamento de Ciencias de la Computación que permitan seguir desarrollando nuevas aplicaciones así como se realizó el desarrollo del presente proyecto.

- Se recomienda a las empresas que una de sus herramientas principales es el uso de Internet, la aplicación de Multihoming, dentro de ellas, ya que esto evitará pérdida de conectividad dentro y fuera de su empresa, así como de información, lo que ayudará a disminuir las pérdidas económicas.

- Se recomienda que las empresas públicas y privadas empiecen a realizar la transición de los equipos que soporten la nueva versión del Protocolo el cuál es IPv6, ya que presenta nuevas características, que permitirá el desarrollo y mejora en las comunicaciones dentro de ellas.

- Para realizar el desarrollo de nuevos proyectos con el protocolo de IPv6, es necesario realizar un estudio sobre la bibliografía existente, para que ésta no sea una de las limitaciones, cómo se presento en el desarrollo del presente proyecto.

- En la actualidad en el Ecuador, el costo y mantenimiento de los equipos que soportan IPv6 es alto, por lo que es necesario que las empresas pequeñas realicen un estudio costo/beneficio para solventar la necesidad de la implementación de Multihoming con IPv6 u otros proyectos.

- Se sugiere a las empresas que han aportado ayuda para el desarrollo de las aplicaciones de IPv6, permitan realizar la capacitación al personal de sistemas, para que los proyectos continúen desarrollándose en varias áreas.

- Se recomienda a las diferentes empresas que están brindado el apoyo para el desarrollo de nuevos proyectos dar accesibilidad, así como ayuda sobre la información y equipos necesarios para el desarrollo e implementación de éstos.

- Se recomienda al Departamento de Ciencias de la Computación la implementación de un laboratorio con soporte para IPv6, en donde los estudiantes internos como externos puedan realizar prácticas y poner en ejecución todos los conocimientos adquiridos en los salones de estudio como en investigaciones sobre este tema.

BIBLIOGRAFÍA

- ✓ **Inicios y Evolución de Internet**

http://www tau.uab.es/~gaby/IPv6/ Memoria%20del%20proyecto%20IPv6.pdf

http://www.newdevices.com/tutoriales/IPv4/2.html

http://www.btwsa.com.ar/siteDocs/_IPv6.asp

http://www.idg.es/computerworld/articulo.asp?id=127547

http://revista.robotiker.com/articulos/articulo71/página1.jsp

http://www.zakon.robert/internet/timeline/

- ✓ **IPv4**

http://www.zator.com/Internet/X_Ap_A.htm

http://neo.lcc.uma.es/evirtual/cdd/tutorial/red/cabIPv4.html

http://es.wikipedia.org/wiki/Cabecera_IP

http://es.wikipedia.org/wiki/Direccion_IP

http://www.newdevices.com/tutoriales/IPv4/2.html

http://www.zator.com/Internet/X_Ap_A.htm

http://www.consulintel.es/Html/ForoIPv6/

Documentos/Tutorial%20de%20IPv6.pdf

www.6sos.org/documentos/6S_OS_Tutorial_IPv6_v4_0.pdf

IPv6%20-%20La%20Nueva%20Generaci%C3%B3n.pdf

www.itam.mx/~dai/dsisdig/Cursos/Redes/cidr.pdf

http://personals.ac.upc.edu/joseb/std_t2_f_01.pdf

- ✓ **IPv6**

http://neo.lcc.uma.es/evirtual/cdd/tutorial/red/espIPv6.html

http://www.merlinux.org/traductor/docs/resumenes/resumen_RFC2460.html

www.consulintel.es/Html/ForoIPv6/ Documentos/Tutorial%20de%20IPv6.pdf

http://revista.robotiker.com/articulos/articulo71/página1.jsp

http://www.IPv6.unam.mx/historia.htm

http://www.rau.edu.uy/IPv6/queesIPv6.htm

http://imasd.elmundo.es/imasd/IPv6/queesIPv6.html

http://www.IPv6.org/

http://es.wikipedia.org/wiki/IPv6

http://blyx.com/public/wireless/IPv6.pdf

http://web.frm.utn.edu.ar/codarec/Cursos/IPv6%20Fundamento%20e%20Implementacion.pdf

linda.IPv6.berkom.de/summit/ 01-02_Hans-Peter.Dittler_IPv6-tut1.pdf

http://web.frm.utn.edu.ar/codarec/IPv6/Filminas/jordi_palet_tutorialIPv6introduccion.pdf

http://www.cudi.edu.mx/aplicaciones/dias_cudi/27_02_04/Introduccion.pdf

http://web.frm.utn.edu.ar/codarec/IPv6/Filminas/david_fernandez.pdf

linda.IPv6.berkom.de/summit/ 01-02_Hans-Peter.Dittler_IPv6-tut1.pdf

- ✓ **CIDR (Classless Inter Domain Routing)**

http://elisoft.galeon.com/docus/rfc2901.htm

http://listas.rcp.net.pe/pipermail/winnt/2001-July/000412.html

http://public.pacbell.net/dedicated/cidr.html

http://www.newdevices.com/tutoriales/IPv4/2.html

http://ditec.um.es/laso/docs/tut-tcpip/3376c22.html

http://lacnic.net/sp/flip-6-pres.html

http://es.wikipedia.org/wiki/CIDR

http://public.pacbell.net/dedicated/cidr.html

http://listas.rcp.net.pe/pipermail/winnt/2001-July/000412.html

- ✓ **Comparación de las Características de IPv4 e IPv6**

http://www.maxitrucos.com/articulos/montse/IPv6_el_gran_desconocido_2.htm

http://elisoft.galeon.com/docus/rfc2901.htm

GLOSARIO

Pág. 7

FTP[1]: File Transfer Protocol/Protocolo de Transferencia de Archivo.

ARPANET[2]: Advanced Research Projects Agency NETwork/Red de la Agencia de Investigación de Proyectos Avanzado.

CP[3]: Control Protocol/Protocolo de Control.

NCP[4]: Network Control Protocol/Protocolo de Control de Red.

TCP/IP[5]: Transmission Control Protocol/Internet Protocol Protocolo de Control de Transmisión/Protocolo de Internet.

Subíndice desde 6-17 Pág. 9-10

SRI[6]: Standford Research Institute/Instituto de Investigación de Standford.

MILNET[7]: Red Militar.

DNS[8]: Domain Name System/Nombre del Sistema del Dominio.

IETF[9]: Internet Engineering Task Force/Grupo de Trabajo en Ingeniería de Internet.

IRTF[10]: Internet Research Task Force/Grupo de Tareas de Investigación sobre Internet.

IANA[11]: Internet Assigned Number Authority/Agencia de Asignación de Números de Internet.

CERT[12]: Computer Energency Response Teams/Equipos de Computación de Respuesta de Emergencia.

FIDONET[13]: Sistema de interconexión para la comunicación de archivos y mensajes.

NSF[14]: National Science Foundation/Fundación Nacional de Ciencia.

PGP[15]: Pretty Good Privacy/Intimidad Bastante Buena.

ISOC[16]: Internet Society/Sociedad de Internet.

INTERNIC[17]: Nombre que se le da al conjunto de proveedores de servicio de registro que define el dominio a nivel Mundial.

TCP[18]: Transmission Control Protocol/Protocolo de Control de Transmisión.

ILH[19]: Internet Header Length/Longitud de Cabecera Internet.

ClDR[20]: Classless Inter Domain Routing/Ruteo de Interdominio sin Clases.

QoS[21]: Quality of Service/Calidad de Servicio.

ICMP[22] : Internet Control Message Protocol/Protocolo de Control de Mensajes de Internet.

IGMP[23]: Internet Group Management Protocol/Protocolo de Administración del Grupo Internet.

Subíndice desde 24-30 Pág. 53-54

DSCP[24]: Differential Services Code Point/Código de Punto para Servicios Diferenciados.

MAC[25]: Security Media Access Control Address/Identificador Hexadecimal de 48 bits, que corresponde de una forma única con una tarjeta o interfaz de red.

TOS[26]: Type of Service/Tipo de Servicio.

KERBEROS[27]: Individuos comunicándose sobre una red insegura prueben su identidad a otro en una manera segura.

LDAP[28]: Lighweight Directory Access Protocol/Protocolo de Red que permite el Acceso a un Servicio de Directorio.

SSL[29]: Secure Sockets Layer/Capa de Socket Seguros.

SNMP[30]: Protocolo Simple de Administración de Red.

Subíndice desde 31-35 Pág. 60,61

ARP[31]: Address Resolution Protocol/Protocolo de Resolución de Direcciones.

MLD[32]: Modelo Lógico de Datos.

ICMP[33]: Protocolo de Control de Mensajes de Internet.

DHCP[34]: Dynamic Host Configuration Protocol/Protocolo Dinámico de Configuración del Host.

PTR[35]: Punto de Terminación de Red.

IGMP: Internet Group Management Protocol/Protocolo de Control de Grupo de Internet.

DNS: Domain Name System/Nombre del Dominio del Sistema.

ARP: Address Request Protocol/Protocolo de Solución de Direcciones.

6Bone: Organización que permite la conexión de las diferentes islas de IPv6.

CIDR: Classless Inter Domain Routing/Ruteo Interdominio sin clases.

Dual Stack: Denominación que se da a los equipos que tienen la capacidad de manejar las pilas de protocolos IPv4 e IPv6.

FTP: File Transfer Protocol/Protocolo de Transferencia de Archivos.

IOS: Operation Systems/Realiza las configuraciones de los routers.

IPv4: Internet Protocol de IPv4/Protocolo de Internet Versión4.

IPv6: Internet Protocol de IPv6/Protocolo de Internet Versión6.

ICMP: Internet Control Message Protocol/Protocolo de Control de Mensajes de Internet.

IPsec: Seguridades para IP.

Ping: Comando para comprobar la conectividad.

Protocolo: Conjunto de reglas que controla la secuencia de mensajes que ocurren durante una comunicación entre entidades que forman una red.

QoS: Quality of Service/Calidad de Servicio.

Ruteo: Mecanismo por el cuál los paquetes de información llegan a su destino final, siguiendo un camino o ruta a través de la red.

TCP/IP: Transmission Control Protocol/Protocolo de Control de Transmisión.

Tracert: Comando para verificar la ruta o camino que sigue un paquete hasta llegar a su destino.

ANEXOS

1.- Instalación y Corrida del Cliente

Creación del Túnel del Proveedor de Hexago en Linux:

1. Descomprimir el archivo tspc2, ejecutando el siguiente comando:

[root@localhost /]# ls

bin/ dev/ home/ lib/ opt/ root/ sys/ usr/

boot/ etc/ initrd/ mnt/ proc/ sbin/ tmp/ var/

[root@localhost /]# ls home/susana/

tmp/ tspc-2.1.1-src.tgz

[root@localhost /]# tar zxvf home/susana/tspc-2.1.1-src.tgz

tspc2/

tspc2/Mk/

tspc2/Mk/mk-linux.mk

tspc2/Mk/mk-.mk

tspc2/Mk/mk-darwin.mk

t spc2/Mk/mk-freebsd.mk

tspc2/Mk/mk-netbsd.mk

tspc2/Mk/mk-openbsd.mk

tspc2/Mk/mk-solaris.mk

tspc2/Mk/mk-windows.mk

tspc2/man/

tspc2/man/man5/

tspc2/man/man5/tspc.conf.5

tspc2/man/Makefile

tspc2/man/man8/

tspc2/man/man8/tspc.8

tspc2/GPL_LICENSE.txt

tspc2/Makefile

tspc2/conf/

tspc2/conf/Makefile

tspc2/conf/tspc.conf.in

tspc2/include/

tspc2/include/base64.h

tspc2/include/cli.h

tspc2/include/cnfchk.h

tspc2/include/config.h

tspc2/include/errors.h

tspc2/include/lib.h

tspc2/include/log.h

tspc2/include/md5.h

tspc2/include/net.h

tspc2/include/net_cksm.h

tspc2/include/net_ka.h

tspc2/include/net_rudp.h

tspc2/include/net_tcp.h

tspc2/include/net_udp.h

tspc2/include/tsp_auth.h

tspc2/include/tsp_cap.h

tspc2/include/tsp_client.h

tspc2/include/tsp_net.h

tspc2/include/tsp_setup.h

tspc2/include/version.h

tspc2/include/xml_req.h

tspc2/include/xml_tun.h

tspc2/include/xmlparse.h

tspc2/platform/

tspc2/platform/darwin/

tspc2/platform/darwin/Makefile

tspc2/platform/darwin/platform.h

tspc2/platform/darwin/tsp_local.c

tspc2/platform/freebsd/

tspc2/platform/freebsd/Makefile

tspc2/platform/freebsd/platform.h

tspc2/platform/freebsd/tsp_local.c

tspc2/platform/freebsd/tsp_tun.c

tspc2/platform/freebsd/tsp_tun.h

tspc2/platform/linux/

tspc2/platform/linux/Makefile

tspc2/platform/linux/platform.h

tspc2/platform/linux/tsp_local.c

tspc2/platform/linux/tsp_tun.c

tspc2/platform/linux/tsp_tun.h

tspc2/platform/netbsd/

tspc2/platform/netbsd/Makefile

tspc2/platform/netbsd/platform.h

tspc2/platform/netbsd/tsp_local.c

tspc2/platform/openbsd/

tspc2/platform/openbsd/Makefile

tspc2/platform/openbsd/platform.h

tspc2/platform/openbsd/tsp_local.c

tspc2/platform/solaris/

tspc2/platform/solaris/Makefile

tspc2/platform/solaris/platform.h

tspc2/platform/solaris/tsp_local.c

tspc2/platform/windows/

tspc2/platform/windows/libopenvpn/

tspc2/platform/windows/libopenvpn/Makefile

tspc2/platform/windows/libopenvpn/api.c

tspc2/platform/windows/libopenvpn/api.h

tspc2/platform/windows/libopenvpn/basic.h

tspc2/platform/windows/libopenvpn/buffer.c

tspc2/platform/windows/libopenvpn/buffer.h

tspc2/platform/windows/libopenvpn/common.h

tspc2/platform/windows/libopenvpn/config-win32.h

tspc2/platform/windows/libopenvpn/errlevel.h

tspc2/platform/windows/libopenvpn/error.c

tspc2/platform/windows/libopenvpn/error.h

tspc2/platform/windows/libopenvpn/fdmisc.c

tspc2/platform/windows/libopenvpn/fdmisc.h

tspc2/platform/windows/libopenvpn/inet_aton.c

tspc2/platform/windows/libopenvpn/integer.h

tspc2/platform/windows/libopenvpn/io.c

tspc2/platform/windows/libopenvpn/io.h

tspc2/platform/windows/libopenvpn/memdbg.h

tspc2/platform/windows/libopenvpn/misc.c

tspc2/platform/windows/libopenvpn/misc.h

tspc2/platform/windows/libopenvpn/mtu.c

tspc2/platform/windows/libopenvpn/mtu.h

tspc2/platform/windows/libopenvpn/openvpn.h

tspc2/platform/windows/libopenvpn/options.h

tspc2/platform/windows/libopenvpn/proto.h

tspc2/platform/windows/libopenvpn/proxy.c

tspc2/platform/windows/libopenvpn/proxy.h

tspc2/platform/windows/libopenvpn/route.h

tspc2/platform/windows/libopenvpn/socket.c

tspc2/platform/windows/libopenvpn/socket.h

tspc2/platform/windows/libopenvpn/syshead.h

tspc2/platform/windows/libopenvpn/thread.h

tspc2/platform/windows/libopenvpn/tun.c

tspc2/platform/windows/libopenvpn/tun.h

tspc2/platform/windows/libopenvpn/win32.c

tspc2/platform/windows/libopenvpn/win32.h

tspc2/platform/windows/HOWTO-BUILD-tunv6.sys.txt

tspc2/platform/windows/Makefile

tspc2/platform/windows/platform.h

tspc2/platform/windows/tsp_local.c

tspc2/platform/windows/nsis-installer-code/

tspc2/platform/windows/nsis-installer-code/tunv6/

tspc2/platform/windows/nsis-installer-code/tunv6/devcon.exe

tspc2/platform/windows/nsis-installer-code/tunv6/tunv6.sys

tspc2/platform/windows/nsis-installer-code/README-NEEDED-FILES.txt

tspc2/platform/windows/nsis-installer-code/README-WINDOWS.txt

tspc2/platform/windows/nsis-installer-code/nsis20.exe

tspc2/platform/windows/nsis-installer-code/tspc.nsi

tspc2/platform/windows/tap-win32-IPv6/

tspc2/platform/windows/tap-win32-IPv6/i386/

tspc2/platform/windows/tap-win32-IPv6/i386/OemWin2k.inf

tspc2/platform/windows/tap-win32-IPv6/i386/tap.cat

tspc2/platform/windows/tap-win32-IPv6/i386/tunv6.inf

tspc2/platform/windows/tap-win32-IPv6/MAKEFILE

tspc2/platform/windows/tap-win32-IPv6/SOURCES

tspc2/platform/windows/tap-win32-IPv6/constants.h

tspc2/platform/windows/tap-win32-IPv6/endian.h

tspc2/platform/windows/tap-win32-IPv6/error.c

tspc2/platform/windows/tap-win32-IPv6/error.h

tspc2/platform/windows/tap-win32-IPv6/foo

tspc2/platform/windows/tap-win32-IPv6/hexdump.c

tspc2/platform/windows/tap-win32-IPv6/hexdump.h

tspc2/platform/windows/tap-win32-IPv6/in_cksum.c

tspc2/platform/windows/tap-win32-IPv6/in_cksum.h

tspc2/platform/windows/tap-win32-IPv6/macinfo.c

tspc2/platform/windows/tap-win32-IPv6/macinfo.h

tspc2/platform/windows/tap-win32-IPv6/mem.c

tspc2/platform/windows/tap-win32-IPv6/prototypes.h

tspc2/platform/windows/tap-win32-IPv6/resource.rc

tspc2/platform/windows/tap-win32-IPv6/small.ico

tspc2/platform/windows/tap-win32-IPv6/tap-win32.ico

tspc2/platform/windows/tap-win32-IPv6/tapdrvr.c

tspc2/platform/windows/tap-win32-IPv6/types.h

tspc2/platform/windows/win-ver/

tspc2/platform/windows/win-ver/Makefile

tspc2/platform/windows/win-ver/win-ver.c

tspc2/src/

tspc2/src/lib/

tspc2/src/lib/Makefile

tspc2/src/lib/base64.c

tspc2/src/lib/cli.c

tspc2/src/lib/cnfchk.c

tspc2/src/lib/config.c

tspc2/src/lib/lib.c

tspc2/src/lib/log.c

tspc2/src/lib/md5c.c

tspc2/src/net/

tspc2/src/net/Makefile

tspc2/src/net/net.c

tspc2/src/net/net_cksm.c

tspc2/src/net/net_ka.c

tspc2/src/net/net_rudp.c

tspc2/src/net/net_tcp.c

tspc2/src/net/net_udp.c

tspc2/src/tsp/

tspc2/src/tsp/Makefile

tspc2/src/tsp/tsp_auth.c

tspc2/src/tsp/tsp_cap.c

tspc2/src/tsp/tsp_client.c

tspc2/src/tsp/tsp_net.c

tspc2/src/tsp/tsp_setup.c

tspc2/src/xml/

tspc2/src/xml/Makefile

tspc2/src/xml/xml_req.c

tspc2/src/xml/xml_tun.c

tspc2/src/xml/xmlparse.c

tspc2/template/

tspc2/template/Makefile

tspc2/template/README

tspc2/template/checktunnel.bat

tspc2/template/checktunnel.sh

tspc2/template/darwin.sh

tspc2/template/freebsd.sh

tspc2/template/linux.sh

tspc2/template/netbsd.sh

tspc2/template/openbsd.sh

tspc2/template/solaris.sh

tspc2/template/variables_environ

tspc2/template/windows.bat

[root@localhost /]# cd tspc2/

[root@localhost tspc2]# ls

conf/ include/man/platform/ template/

GPL_LICENSE.txt* Makefile* Mk/src/

[root@localhost tspc2]#

2. Ejecutar la Instalación del Cliente a través del Comando:

[root@localhost /]# cd tspc2/

[root@localhost tspc2]# make install target=linux installdir=/usr/local/tspc

mkdir -p bin

mkdir -p objs

make[1]: Entering directory `/tspc2/src/net'

gcc -O2 -g -Wall -I../../include -I../../platform/linux -c net.c -o ../../objs/net.o - Dlinux

gcc -O2 -g -Wall -I../../include -I../../platform/linux -c net_rudp.c -o ../../objs/net_rudp.o - Dlinux

```
gcc -O2 -g -Wall -I../../include -I../../platform/linux -c net_tcp.c -o ../../objs/net_tcp.o -
Dlinux
gcc -O2 -g -Wall -I../../include -I../../platform/linux -c net_udp.c -o ../../objs/net_udp.o -
Dlinux
gcc -O2 -g -Wall -I../../include -I../../platform/linux -c net_ka.c -o ../../objs/net_ka.o -Dlinux
gcc -O2 -g -Wall -I../../include -I../../platform/linux -c net_cksm.c -o ../../objs/net_cksm.o -
Dlinux

make[1]: Leaving directory `/tspc2/src/net'
make[1]: Entering directory `/tspc2/src/lib'
gcc -O2 -g -Wall -I../../include -I../../platform/linux -c base64.c -o ../../objs/base64.o -
Dlinux
gcc -O2 -g -Wall -I../../include -I../../platform/linux -c cli.c -o ../../objs/cli.o -Dlinux
gcc -O2 -g -Wall -I../../include -I../../platform/linux -c config.c -o ../../objs/config.o -Dlinux
gcc -O2 -g -Wall -I../../include -I../../platform/linux -c lib.c -o ../../objs/lib.o -Dlinux
gcc -O2 -g -Wall -I../../include -I../../platform/linux -c log.c -o ../../objs/log.o -Dlinux
gcc -O2 -g -Wall -I../../include -I../../platform/linux -c md5c.c -o ../../objs/md5c.o -Dlinux
gcc -O2 -g -Wall -I../../include -I../../platform/linux -c cnfchk.c -o ../../objs/cnfchk.o -Dlinux
make[1]: Leaving directory `/tspc2/src/lib'
make[1]: Entering directory `/tspc2/src/tsp'
gcc -O2 -g -Wall -I../../include -I../../platform/linux -c tsp_auth.c -o ../../objs/tsp_auth.o -
Dlinux
gcc -O2 -g -Wall -I../../include -I../../platform/linux -c tsp_cap.c -o ../../objs/tsp_cap.o -
Dlinux
gcc -O2 -g -Wall -I../../include -I../../platform/linux -c tsp_client.c -o ../../objs/tsp_client.o -
Dlinux
```

```
gcc -O2 -g -Wall -I../../include -I../../platform/linux -c tsp_net.c -o ../../objs/tsp_net.o -Dlinux
gcc -O2 -g -Wall -I../../include -I../../platform/linux -c tsp_setup.c -o ../../objs/tsp_setup.o -Dlinux
make[1]: Leaving directory `/tspc2/src/tsp'
make[1]: Entering directory `/tspc2/src/xml'
gcc -O2 -g -Wall -I../../include -I../../platform/linux -c xmlparse.c -o ../../objs/xmlparse.o -Dlinux

gcc -O2 -g -Wall -I../../include -I../../platform/linux -c xml_req.c -o ../../objs/xml_req.o -Dlinux
gcc -O2 -g -Wall -I../../include -I../../platform/linux -c xml_tun.c -o ../../objs/xml_tun.o -Dlinux
make[1]: Leaving directory `/tspc2/src/xml'
make[1]: Entering directory `/tspc2/platform/linux'
gcc -g -Wall -I../../include -I../../platform/linux -c tsp_local.c -o ../../objs/tsp_local.o -Dlinux
gcc -g -Wall -I../../include -I../../platform/linux -c tsp_tun.c -o ../../objs/tsp_tun.o -Dlinux
gcc -g -Wall -I../../include -I../../platform/linux -o ../../bin/tspc ../../objs/*.o
make[1]: Leaving directory `/tspc2/platform/linux'
make[1]: Entering directory `/tspc2/template'
make[1]: No se hace nada para `all'.
make[1]: Leaving directory `/tspc2/template'
make[1]: Entering directory `/tspc2/conf'
Generating basic configuration file
chmod 700 ../bin/tspc.conf.sample
```

```
make[1]: Leaving directory `/tspc2/conf'
make[1]: Entering directory `/tspc2/man'
make[1]: No se hace nada para `all'.
make[1]: Leaving directory `/tspc2/man'
mkdir -p /usr/local/tspc
make[1]: Entering directory `/tspc2/src/net'
make[1]: No se hace nada para `install'.
make[1]: Leaving directory `/tspc2/src/net'
make[1]: Entering directory `/tspc2/src/lib'
make[1]: No se hace nada para `install'.

make[1]: Leaving directory `/tspc2/src/lib'
make[1]: Entering directory `/tspc2/src/tsp'
make[1]: No se hace nada para `install'.
make[1]: Leaving directory `/tspc2/src/tsp'
make[1]: Entering directory `/tspc2/src/xml'
make[1]: No se hace nada para `install'.
make[1]: Leaving directory `/tspc2/src/xml'
make[1]: Entering directory `/tspc2/platform/linux'
make[1]: No se hace nada para `install'.
make[1]: Leaving directory `/tspc2/platform/linux'
make[1]: Entering directory `/tspc2/template'
Installing templates
make[1]: Leaving directory `/tspc2/template'
make[1]: Entering directory `/tspc2/conf'
Generating basic configuration file
```

chmod 700 ../bin/tspc.conf.sample

make[1]: Leaving directory `/tspc2/conf'

make[1]: Entering directory `/tspc2/man'

Installing man pages

mkdir -p /usr/local/tspc/man/man5

mkdir -p /usr/local/tspc/man/man8

cp man5/tspc.conf.5 /usr/local/tspc/man/man5

cp man8/tspc.8 /usr/local/tspc/man/man8

To view man pages run :

man -M /usr/local/tspc/man tspc

man -M /usr/local/tspc/man tspc.conf

make[1]: Leaving directory `/tspc2/man'

[root@localhost tspc2]