ESCUELA POLITECNICA NACIONAL

ESCUELA DE FORMACION DE TECNOLOGOS

Implementación del Protocolo IPv6 en el laboratorio de Tecnologías de la Información de la carrera de Análisis de Sistemas Informáticos.

PROYECTO PREVIO A LA OBTENCIÒN DEL TITULO DE TECNOLOGO EN ANÁLISIS DE SISTEMAS INFORMÁTICOS

VERONICA ROSALVA VARGAS CALERO

DIRECTOR: ING. PATRICIO PROAÑO

Quito, Enero del 2008

DECLARACION

Yo, Verónica Rosalva Vargas Calero, declaro bajo juramento que el trabajo aquí descrito es de mi auditoria; que no ha sido previamente presentada para ningún grado o calificación profesional; y, que he consultado las referencias bibliográficas que se incluyen en este documento.

A través de la presente declaración cedo mis derechos de propiedad intelectual correspondiente a este trabajo, a la Escuela Politécnica Nacional, según lo establecido por la Ley de propiedad intelectual, por su Reglamento y por la normatividad institucional vigente.

_____

Verónica Vargas C.

CERTIFICACION

Certifico que el presente trabajo fue desarrollado por Verónica Vargas, bajo mi supervisión.

_____

Patricio Proaño

DIRECTOR DE PROYECTO

AGRADECIMIENTO

A todo el Personal Docente de la Escuela de Formación de Tecnólogos que siempre me brindaron sus sabias enseñanzas, les manifiesto mi imperecedera gratitud porque ellos han forjado en mí, ser persona útil a nuestra familia, a la sociedad y a nuestra Patria.

A mi Madre y a mi Abuelita que aunque esta en el cielo sigue presente en mi, que con infinito amor y sabiduría han sabido guiar mí vida por el sendero de la justicia y la libertad, a fin de engrandecerme y de que cada día sea mejor persona.

INDICE

INDICE FIGURAS 6
INDICE TABLAS 10
RESUMEN 11
CAPITULO 1. SITUACIÓN ACTUAL DEL PROTOCOLO 11
IPV4 11
CAPITULO 2. INTRODUCCION AL PROTOCOLO IPV6 11
CAPITULO 3. IMPLEMENTACION DEL PROTOCOLO 12
IPV6 EN EL LABORATORIO 12
CAPITULO 4. CONCLUSIONES Y RECOMENDACIONES. 12
CAPITULO 1: SITUACIÓN ACTUAL DEL PROTOCOLO IPV4 13
1.1 INTRODUCCIÓN 13
1.1.1 PROTOCOLOS TCP/IP 14
1.1.2 VISION DEL TCP/IP 14
1.1.3 ARQUITECTURA DEL MODELO TCP/IP 14
1.2 PROTOCOLO IPV4 23
1.2.1 CABECERA IPV4 24
1.2.2 CLASES DE DIRECCIONES IPV4 28
1.2.3 SUBDIVISION DE UNA RED 32
1.2.4 SUBREDES 33
1.2.5 MÁSCARA DE SUBRED 35
1.2.6 ASIGNACIÓN DE IDs DE RED 37
1.2.7 ASIGNACIÓN DE IDs DE HOST 38
1.2.8 SUBNETTING 39
1.2.9 CIDR - Classless Interdomain Routing 41
1.2.9.1 Restricciones del CIDR 43
1.2.10 VLSM (Máscara de Red de Longitud Variable) 43
1.2.11 CONFIGURACION DE TCP/IP CON IPv4 44
1.3 LIMITACIONES DEL PROTOCOLO IPV4 46
1.4 PERSPECTIVAS 48
CAPITULO 2: INTRODUCCION AL PROTOCOLO IPV6 50
2.1 INTRODUCCION GENERAL 50
2.1.1 CARACTERÍSTICAS DE IPV6 50
2.1.2 BENEFICIOS DE IPV6 52
2.2 ESTRUCTURA DEL PROTOCOLO IPv6 52
2.2.1 FORMATO DE UN PAQUETE 52
2.2.2 CABECERA IPV6 53
2.3 DIRECCIONAMIENTO IPv6 57
2.3.1 REPRESENTACIÓN DE DIRECCIONES IPv6 57
2.3.2 CLASES/TIPO DE DIRECCIONES 59
2.4 CONFIGURACIÓN CON IPv6 65
2.4.1 IPv6 EN WINDOWS XP 66
2.4.2 IPv6 EN RUOTERS CISCO 66
2.4.3 AUTOCONFIGURACIÓN 67
2.4.4 DHCP 70
2.4.5 DNS 72
2.5 MECANISMOS DE TRANSICION IPv4 - IPV6 73
2.6 IPV6 SOBRE IEEE 802.3 74

2.7 COMPARACIÓN ENTRE EL PROTOCOLO IPV4 E IPV6 75
CAPITULO 3: IMPLEMENTACION DEL PROTOCOLO IPV6 EN EL LABORATORIO 77
3.1 ANÁLISIS DE LA RED DEL LABORATORIO DE INFORMACIÓN DE LA CARRERA DE ANÁLISIS DE SISTEMAS INFORMÁTICOS 77
3.1.1 ESTRUCTURA FÍSICA DE LA RED 77
3.1.2 COMPONENTES FISICOS DE LA RED 78
3.1.3 COMPONENTES LÓGICOS DE LA RED 79
3.1.4 CONFIGURACIÓN LÓGICA ACTUAL DE LA RED LTI (IPV4) 80
3.1.5 SEGURIDAD EN LA RED LTI 81
3.1.6 SERVICIOS DE LA RED 83
3.1.7 CONFIGURACIÓN LÓGICA DE LA RED UTILIZANDO EL PROTOCOLO IPv6 83
3.1.8 CONFIGURACIONES POSIBLES DEL PROTOTIPO DE RED 124
3.2 IMPLEMENTACION DE IPv6 EN EL LTI 134
3.3 OBTENCION DE DIRECCIONES IPV6 149
3.3.1 JERARQUIA DE LAS DELEGACIONES 149
CAPITULO 4: CONCLUSIONES Y RECOMENDACIONES 155
4.1 CONCLUSIONES 155
4.3 REFERENCIA BIBLIOGRÁFICA 169
GLOSARIO 171
ANEXOS 176
ANEXO 1: ALGORITMO DE LOS CÓDIGOS DE REDUNDANCIA CÍCLICA 176
ANEXO 2: GUIA DE CONFIGURACION DE TCP/IP CON IPv4 177
2.1 CONFIGURACIÓN AUTOMÁTICA 177
2.2 CONFIGURACIÓN DINÁMICA 180
2.3 CONFIGURACIÓN ALTERNATIVA 187
2.4 CONFIGURACIÓN MANUAL 188
ANEXO 3: RFC`s 193

INDICE FIGURAS

Fig. 1.1 Comparación entre el Modelo OSI y TCP/IP 15
Fig. 1.2 Capa de Aplicación 15
Fig. 1.3 Capa de Transporte 17
Fig. 1.4 Formato de un segmento TCP 17
Fig. 1.5 Formato de un segmento UDP 18
Fig. 1.6 Capa de Red 19
Fig. 1.7 Formato de un paquete IP 19
Fig. 1.8 Formato ARP 20
Fig. 1.9 Formato RARP 21
Fig. 1.10 Capa de Enlace de Datos 22
Fig. 1.11 Formato de la Cabecera IPv4 24
Fig. 1.12 Asignación de Bits en la Cabecera IPv4 27
Fig. 1.13 Clases de Direcciones 28
Fig. 1.14 Direcciones Clase A 28
Fig. 1.15 Direcciones Clase B 29
Fig. 1.16 Direcciones Clase C 29
Fig. 1.17 Asignación de Bits por cada tipo de Direcciones 30

Fig. 1.18 Direcciones Especiales 30
Fig. 1.19 Direcciones Clase D y E 31
Fig. 1.20 Direccionamiento Unicast 31
Fig. 1.21 Direccionamiento Multicast 32
Fig. 1.22 Uso de Direcciones 32
Fig. 1.23 Subredes 33
Fig. 1.24 Asignación de las Subredes 34
Fig. 1.25 Ejemplo de Subredes 35
Fig. 1.26 Máscara de Subred 36
Fig. 1.27 Estructura de la Máscara de Subred 37
Fig. 1.28 Asignación de IDs de Red 38
Fig. 1.29 Asignación de IDs de Host 39
Fig. 1.30 Subnetting 39
Fig. 1.31 Ejemplo de VLSM 44
Fig. 1.32 Red LTI 45

Fig. 2.1 Formato de un Paquete 52
Fig. 2.2 Encabezado IPv6 53
Fig. 2.3 Formato de la siguiente cabecera 54
Fig. 2.4 Opciones de salto a salto 55
Fig. 2.5 Cabecera de Encaminamiento 55
Fig. 2.6 Cabecera de Fragmentación 56
Fig. 2.7 Modo transporte 56
Fig. 2.8 Modo túnel 56
Fig. 2.9 Direcciones Unicast 59
Fig. 2.10 Formato de Direcciones Unicast Globales 60
Fig. 2.11 Formato de Direcciones Unicast Locales de Enlace 61
Fig. 2.12 Formato de Direcciones Unicast Locales de Sitio 61
Fig. 2.13 Direcciones Multicast 62
Fig. 2.14 Formato de Direcciones Multicast 62
Fig. 2.15 Direcciones Anycast 64
Fig. 2.16 Direcciones Anycast únicas 65
Fig. 2.17 Instalación de IPv6 66
Fig. 2.18 Generación de la dirección de enlace local 68
Fig. 2.19 Proceso de Tunelización 74
Fig. 2.20 TCP/IP sobre IEEE 802.3 75

Fig. 3.1 Red LTI 78
Fig. 3.2 Asignación de Direcciones IPv4 81
Fig. 3.3 Seguridad en el LTI 82
Fig. 3.4 Prototipo utilizado para la configuración del protocolo IPv6 84
Fig. 3.5 Instalación de IPv6 85
Fig. 3.6 Dirección IPv6 Asignada por Autoconfiguración 86
Fig. 3.7 Prototipo para la Autoconfiguración sin Router 86
Fig. 3.8 Conectividad entre la WS1 con WS2 y WS3 87
Fig. 3.9 Conectividad entre la WS2 con WS1 y WS3 87
Fig. 3.10 Conectividad entre la WS3 con WS1 y WS2 88
Fig. 3.11 Prototipo para la Autoconfiguración con Router. 88
Fig. 3.12 Dirección IPv6 Asignada por Autoconfiguración conectada al Router 94

Fig. 3.13 Conectividad entre interfaces de WS1 95
Fig. 3.14 Conectividad entre interfaces de WS2 96
Fig. 3.15 Conectividad entre interfaces de WS3 97
Fig. 3.16 Prototipo para la Configuración Manual 98
Fig. 3.17 Subcomandos del comando netsh 99
Fig. 3.18 Subcomandos del comando interface 99
Fig. 3.19 Subcomandos del comando ipv6 100
Fig. 3.20 Asignación de Dirección IPv6 101
Fig. 3.21 Asignación del Prefijo de la Dirección IPv6 101
Fig. 3.22 Comando y subcomandos netsh 102
Fig. 3.23 Interfaz Configurada 102
Fig. 3.24 Conectividad entre Interfaces 104
Fig. 3.25 Interfaz de Red 105
Fig. 3.26 Activación de IPv6 a Interfaz de Red 105
Fig. 3.27 Mensajes de activación de la tarjeta de Red 106
Fig. 3.28 Tarjeta de Red activada 106
Fig. 3.29 Terminal de Consola 107
Fig. 3.30 Fichero de configuración de la Interfaz 107
Fig. 3.31 Comando ifconfig 108
Fig. 3.32 Comando Ping6 109
Fig. 3.33 Comando Ifconfig 112
Fig. 3.34 Comando Ping6 114
Fig. 3.35 Fichero de configuración de la Interfaz 114
Fig. 3.36 Fichero de configuración de Hosts 115
Fig. 3.37 Fichero de configuración de Red 115
Fig. 3.38 Restauración de valores de la tarjeta de Red 116
Fig. 3.39 Comando Ifconfig 116
Fig. 3.40 Comando Ping6 117
Fig. 3.41 Inicio del servicio DNS 118
Fig. 3.42 Configuraciones DNS 118
Fig. 3.43 Archivo de configuración de Hosts en DNS 119
Fig. 3.44 Direcciones de Hosts en DNS 119
Fig. 3.45 Configuración del DNS 120
Fig. 3.46 Agregar DNS 120
Fig. 3.47 Comando ipconfig /all 121
Fig. 3.48 Comando Ping6 122
Fig. 3.49 Comando Dig 123
Fig. 3.50 Comando nslookup 124
Fig. 3.51 Prototipo de Red considerado como Una Sola Red 125
Fig. 3.52 Prototipo de Red considerado como Redes Diferentes 125
Fig. 3.53 Conectividad de interfaces 129
Fig. 3.54 Prototipo de Red considerado como Subredes 129
Fig. 3.55 Conectividad de interfaces 133
Fig. 3.56 Direccionamiento IPv6 en la Polired 133
Fig. 3.57 Red LTI con IPv6 142
Fig. 3.58 Conectividad desde la sala uno 142
Fig. 3.59 Conectividad desde la sala dos 143
Fig. 3.60 Conectividad desde la sala tres 145
Fig. 3.61 Conectividad desde la sala de Servidores 146

Fig. 3.62 Conectividad con Internet 146
Fig. 3.63 RIRs en el mundo 150
Fig. 3.64 Registros regionales 151
Fig. 3.65 Direcciones en Ecuador 153
Fig. 3.66 Asignación de Direcciones IP 153
Fig. 3.67 Solicitud para la Adquisición de Direcciones 154

Fig. 4.1 Comunicación de la Polired 165
Fig. 4.2 Mecanismo Dual 166
Fig. 4.3 Mecanismo de Tunelización 166

Fig. A.1 Asignación de direcciones Automáticas 177
Fig. A.2 Conexiones de Red 178
Fig. A.3 Propiedades de la Red 178
Fig. A.4 Propiedades de la Tarjeta de Red 179
Fig. A.5 Opciones de Configuración 179
Fig. A.6 Asignación de direcciones Dinámicas 180
Fig. A.7 Administración del DHCP 180
Fig. A.8 Configuración del Servidor DHCP 181
Fig. A.9 Ámbito del servidor DCHP 181
Fig. A.10 Rango de direcciones del DHCP 181
Fig. A.11 Exclusión de direcciones del DHCP 182
Fig. A.12 Tiempo de Concesión 182
Fig. A.13 Configuración de opciones del DHCP 183
Fig. A.14 Asignación de Puerta de Enlace 183
Fig. A.15 Asignación de Dominio 184
Fig. A.16 Servidores Wins 184
Fig. A.17 Activación del servicio 185
Fig. A.18 Finalización de configuración 185
Fig. A.19 Comprobación de la creación del servicio 186
Fig. A.20 Verificación del servicio 186
Fig. A.21 Verificación de la existencia del servidor en las estaciones 187
Fig. A.22 Asignación de dirección 188
Fig. A.23 Asignación de dirección Manual 188
Fig. A.24 Opciones de configuración 189
Fig. A.25 Asignación de dirección 190
Fig. A.26 Opciones de configuración Avanzada 190
Fig. A.27 Asignación de dirección 191
Fig. A.28 Configuración de Métrica 191
Fig. A.29 Descripción de RFCs 195

INDICE TABLAS

Tabla 1.1 23
Tabla 1.2 34
Tabla 1.3 35
Tabla 1.4 37
Tabla 1.5 38
Tabla 1.6 41

Tabla 2.1 58
Tabla 2.2 63

Tabla 3.1 79
Tabla 3.2 80
Tabla 3.3 84
Tabla 3.4 134
Tabla 3.5 135
Tabla 3.6 135
Tabla 3.7 136
Tabla 3.8 136

Tabla 4.1 159
Tabla 4.2 165

RESUMEN

El desarrollo, practica y documentado de este proyecto, surgió por la necesidad de dar a conocer lo referente acerca al nuevo protocolo de asignación de direcciones llamado IPv6, crear un prototipo de red y con guías de configuración que permitan a los estudiantes utilizarlo como ayuda para entender la nueva tecnología y realizar con mayor facilidad las practicas de laboratorio.
A continuación se resume los capítulos que se han considerado necesarios para la realización de este proyecto:

CAPITULO 1. SITUACIÓN ACTUAL DEL PROTOCOLO IPV4

En este capitulo se hace una un breve repaso del funcionamiento del protocolo IPv4, estudio de arquitectura del modelo de referencia OSI, además de diseñar un prototipo de red, utilizando todas las formas posibles de configuración con dicho protocolo.
Para la implementación del prototipo se realiza la configuración de los siguientes dispositivos (Router, Switch, Estaciones de Trabajo) para el buen funcionamiento de la red.

CAPITULO 2. INTRODUCCION AL PROTOCOLO IPV6

Este capitulo se basa en el estudio del nuevo protocolo, dentro del cual están:
Esquema de Direccionamiento, Implementación de un prototipo de red con el uso del nuevo protocolo, Formas posibles de Configuraciones, Formas posibles del uso del prototipo, Configuración en los hosts, Configuración de routers, Comprobación del funcionamiento de la red mediante el comando Ping.

CAPITULO 3. IMPLEMENTACION DEL PROTOCOLO IPV6 EN EL LABORATORIO

Configuración del nuevo protocolo en el Laboratorio de Tecnologías de la Información mediante la actualización previa de los routers y hosts, basándose en las políticas de configuración de la Unidad de Gestión de la Información.

CAPITULO 4. CONCLUSIONES Y RECOMENDACIONES.

El uso del protocolo IPv6 no limita la asignación de direcciones IP, es una red con mayor seguridad que con IPv4 aunque debido a la inexistencia de las actualizaciones respectivas tanto en hardware como en software no es posible el uso de varios servicios como la implementación de un servidor DHCPv6, de un servidor para la transferencia de archivos, etc y de otros equipos de red como switches y firewalls.

Se recomienda incorporar el tema del Ipv6 en el pensum de estudio de la carrera de A.S.I., de manera que los estudiantes conozcan y apliquen esta nueva tecnología, además debido al crecimiento tecnológico es recomendable que el LTI disponga de equipos de red que soporten la nueva tecnología, de manera que se pueda implementar de forma adecuada el nuevo protocolo.

CAPITULO 1: SITUACIÓN ACTUAL DEL PROTOCOLO IPV4

1.1 INTRODUCCIÓN

A partir de la aparición de Internet las redes de datos han tenido un crecimiento exponencial que ha desbordado todas de las previsiones iniciales de crecimiento realizadas en sus inicios. Por otro lado, Internet esta construida basándose en un diseño realizado en los años 70 y posee por tanto algunas limitaciones.

Las organizaciones más representativas en Internet como la IETF (*Internet Engineering Task Force,* organización encargada de la evolución de la arquitectura en la Red) y el W3C (*World Wide Web Consortium*) están trabajando continuamente en el desarrollo de nuevos protocolos y aplicaciones centrados en modernizar la arquitectura de Internet para actualizarla y adaptarla a las nuevas necesidades de comunicación.

El modelo de referencia OSI, *(Open System Interconnection)* fue lanzado en 1984 y creado por ISO *(International Organization of Standarization)*. Su función consiste en definir la forma en la que se van a comunicar los sistemas abiertos de telecomunicaciones con otros sistemas.

Al crear este modelo se crearon numerosos protocolos que con el tiempo no fueron satisfactorios y se creo una nueva pila de protocolos llamados TCP/IP. El modelo en sí no puede ser considerado una arquitectura, ya que no especifica el protocolo que debe usarse en cada capa ni realiza funciones especificas.

Este modelo es usado para describir el uso de los datos entre la conexión física de la red y la aplicación del usuario final. Este modelo es el mejor conocido y el más usado para describir los entornos de una red y se conforma de siete capas: Aplicación, Presentación, Sesión, Transporte, Red, Enlace de Datos y Física. El propósito de cada una de las capas de este modelo es proveer los servicios para la capa superior.

1.1.1 PROTOCOLOS TCP/IP

TCP/IP es una familia de protocolos de comunicación de datos, usado para el Internet, para redes de área local LAN y redes de gran tamaño WAN, y es utilizado desde hace muchos años ya que ha demostrado su efectividad.

TCP/IP fue desarrollado para utilizarse en la red ARPANET por el *U.S. Departmant of Defense Advance Research Projects Agency* (DARPA) durante la década de 1960 a 1970.

Estos protocolos fueron creados en cada una de las capas que forman la pila de protocolos TCP/IP y serán descritos posteriormente.

1.1.2 VISION DEL TCP/IP

En 1969, la *Agencia de proyectos de investigación avanzada* (ARPA), perteneciente al Departamento de Defensa de los EE.UU. ARPA estableció una red de conmutación de paquetes de computadoras conectadas mediante líneas punto a punto denominadas *Red de la agencia de proyectos de investigación avanzada* (ARPANET). **[1]**; porque necesitaba una arquitectura que pudiera conectar múltiples redes y que tuviera la capacidad de mantener conexiones aun cuando una parte de la subred esté dañada o perdida, lo que podría ocurrir por ejemplo en caso de algún tipo de catástrofe.

Aunque el modelo de referencia OSI sea universalmente reconocido, el estándar más utilizado de Internet es el *Protocolo de Control de Transmisión/Protocolo Internet* (TCP/IP). Incluso TCP/IP hace que sea posible la comunicación entre dos computadores, desde cualquier parte o ubicación del mundo.
TCP/IP es compatible con cualquier sistema operativo y con cualquier tipo de hardware, proporcionando una abstracción total del medio.

1.1.3 ARQUITECTURA DEL MODELO TCP/IP

El modelo TCP/IP está basado en el tipo de red packet-switched, y tiene cuatro capas: la capa de aplicación, la capa de transporte, la capa de Internet y la capa

de red. En la figura 1.1 se muestra una comparación entre en modelo TCP/IP y el modelo OSI.

Es importante observar que algunas de las capas del modelo TCP/IP poseen el mismo nombre que las capas del modelo OSI, aunque no se corresponden exactamente unas con otras, por lo que no deben confundirse.

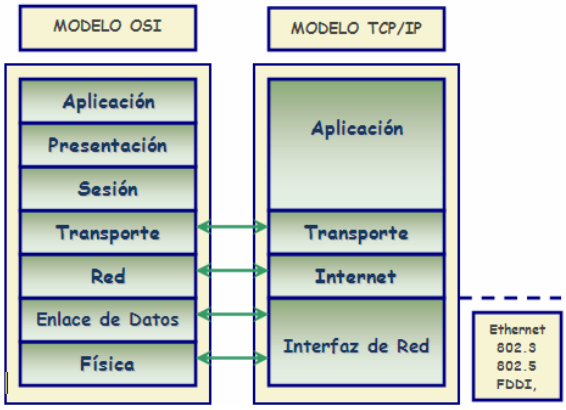


Fig. 1.1 Comparación entre el Modelo OSI y TCP/IP

1.1.3.1 Capa de Aplicación

A través de los protocolos de alto nivel se definen los: modos de representación, codificación y control de diálogo de los datos; garantizando que los datos estén correctamente empaquetados para que puedan pasar a la siguiente capa.

En esta capa se define varios protocolos inicialmente SMTP, FTP, Telnet, DNS, etc. y constantemente se añaden otros como NNTP, HTTP. En la figura 1.2 se presenta las funciones de la capa de aplicación.

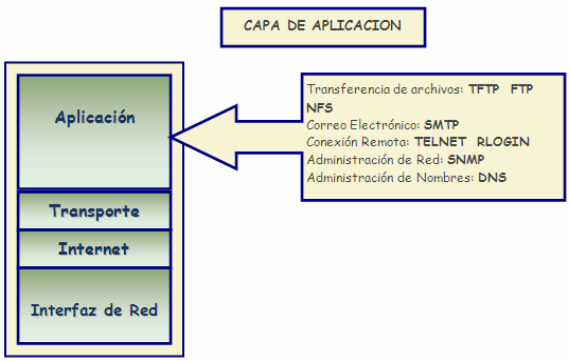


Fig. 1.2 Capa de Aplicación

FTP**:** *File Transfer Protocol;* posee habilidad para enviar grandes bloques de datos de un host a otro por la red; también se lo puede utilizar como navegador Web con su respectiva dirección funciona sobre TCP y se define por la RFC 959.

HTTP**:** *Hypertext Transfer Protocol;* es utilizado por las páginas Web para transferir datos en forma de texto, hipertexto, sonido, vídeo. Es comúnmente conocido como protocolo de transferencia de hipertexto por su eficiencia en los altos de un documento a otro; el mismo que permite accesos dinámicos en la red, funciona sobre TCP.
HTTP es una combinación de FTP con SMTP

SMTP**:** *Simple Mail Transfer Protocol;* realiza el envío de mensajes basándose en direcciones de correo electrónico; además del intercambio de correo electrónico entre host, funciona sobre TCP. SMTP permite: **[1]**

- El envío de un único mensaje a uno o más receptores.
- El envío de mensajes que incluyen texto, voz, video o gráficos.
- El envío de mensajes a usuarios de redes situadas fuera de Internet.

DNS**:** *Domain Name Service;* traduce un nombre a una dirección IP ya que es una base de datos la cual almacena información de los nombres de dominio de las redes tales como las del Internet, DNS es capa de asociar un nombre a diferentes tipos de información, funciona sobre UDP.

DHCP: *Dynamic Host Configuration Protocol;* permite a los nodos de una red obtener sus parámetros de configuración automáticamente, funciona como modo *cliente/servidor* del cual el servidor posee una lista de direcciones IP dinámicas las mismas que luego serán asignadas a sus clientes.

Wins: Este servicio es parecido al servicio que presta DHCP, es decir que un servidor provee las direcciones a sus clientes y la registra en su base de datos pero a diferencia de DHCP el servidor Wins registra varios tipos de nombres como: Nombre de Equipos, Nombre de Grupos de Trabajo, Nombres de Dominios, Usuarios, etc.

1.1.3.2 Capa de Transporte

Proporciona un control de alto nivel para la transferencia de datos y es capaz de eliminar los paquetes que se hayan duplicado, define dos protocolos TCP y UDP. De los cuales UDP es simple ya que ofrece transportación que no asegura secuencia; cuando la fiabilidad y seguridad no son tan importantes como lo es el tamaño y la velocidad. En la figura 1.3 se presenta las funciones de la capa de transporte.

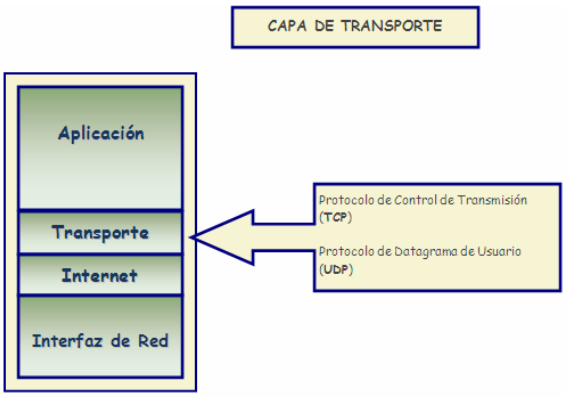


Fig. 1.3 Capa de Transporte

TCP (*Transmisión Control Protocol*); nos ofrece maneras flexibles y con alta calidad para que sus comunicaciones puerto a puerto sean confiables. Además TCP utiliza estos protocolos tales como: FTP, Telnet, SMTP por que está orientado a transmitir gran cantidad de paquetes.

Se responsabiliza en verificar la entrega de los datos. Dado que la información se puede perder en el camino entre el punto de envío y el punto de recepción.
Cuando TCP va a transmitir datos, informa al receptor que se encuentran datagramas en camino y concluye la conexión. Así el receptor conoce toda la transmisión. Para dar fiabilidad se realiza detección de errores y si hay errores entonces se realiza retransmisión de la trama. En la figura 1.4 se presenta el formato que utiliza el protocolo TCP.

# de Bits	16	32	32	4	6	6	16	16	16	0 ó 32	
SPORT	DPORT	Sequence Number	Acknowledge Number	HLEN	Reservado	Code Bits	Window	Checksum	Urgent	Option	Data

Fig. 1.4 Formato de un segmento TCP

A continuación definimos cada uno de los campos existentes en el formato TCP:

***SPORT* (*Source Port*)** - Número de puerto del transmisor

***DPORT* (*Destination Port*)** - Número del puerto receptor

Sequence Number - Número empleado para garantizar la llegada de todos los datos

Acknoledge Number - Indica el siguiente octeto TCP esperado

HLEN - Longitud del encabezado

Reservado - Campo reservado para futuras aplicaciones

Code Bits - Funciones de control (tal como el inicio y el fin de una sesión)

Window - Número de octetos que el transmisor espera sean aceptados

Checksum - Suma de verificación del encabezado y el campo de datos

Urgent - Indica el fin de datos urgentes

Option - Tamaño máximo del segmento TCP

Data - Los datos del protocolo de capa superior

UDP (*User Datagram Protocol*); no es confiable ya que no realiza ningún tipo de verificación ni organización de paquetes. Además utiliza los protocolos DNS, TFTP, y realiza la fragmentación de los datos por que son servicios de UDP.

Un datagrama es un conjunto de datos el cual va a ser enviado como un mensaje independiente.

La capa de transporte no es la encargada de verificar la ruta que van a seguir los datos para llegar a su destino final. En la figura 1.5 se presenta el tipo de formato que utiliza el protocolo UDP.

Fig. 1.5 Formato de un segmento UDP

A continuación definimos cada uno de los campos existentes en el formato UDP:

SPORT (Source Port) - Número de puerto del transmisor

DPORT (Destination Port) - Número del puerto receptor

HLEN - Longitud del encabezado

Checksum - Suma de verificación del encabezado y el campo de datos

Data - Los datos del protocolo de capa superior

1.1.3.3 Capa de Internet

Define el formato de paquete y su protocolo oficial es IP (*Internet Protocol*).
Además define los protocolos que son usados en esta capa tales como: ARP, RARP, ICMP, IGMP. En la figura 1.6 se presenta las funciones de la capa de red.

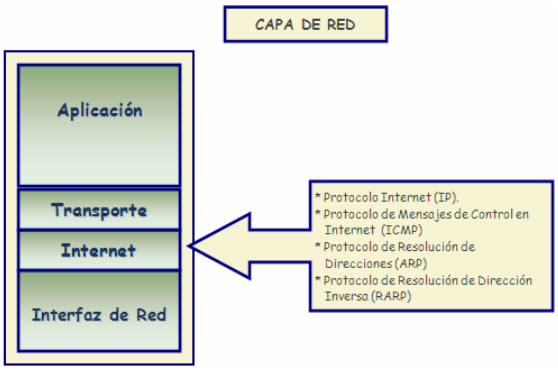


Fig. 1.6 Capa de Red

IP: Su trabajo es entregar paquetes IP (ruteo de paquetes) denominados datagramas desde cualquier red y que los mismos lleguen a su destino sin importar la ruta y evitar la congestión.
Esta capa se encarga de determinar la mejor ruta o camino para llegar a su destino a través de la conmutación de paquetes entre cualquier par de host que forman parte de una red.

El envío de paquetes de un host a otro se lo realiza a través de una dirección destino. En este los paquetes son enrutados en función de direcciones lógicas. Es un protocolo no orientado a conexión y no es confiable. En la figura 1.7 se muestra el formato que tiene el paquete IP.

# de Bits	16	16	32	32	4	4	6	6	16	16	32	32	4	
	Version	HLEN	Tipo de Servicio	Total Length	Identificación	Flags	Flag Offset	TTL	Protocolo	Header Checksum	S Add	D Add	IP Opt.	Data

Fig. 1.7 Formato de un paquete IP

A continuación definimos cada uno de los campos existentes en el formato IP:

Versión – Registra el tipo de versión del protocolo IP (IPv4 ó IPv6).

HLEN – Indica la longitud del encabezado en palabras de 32 bits.

Type of Service – Permite que el host indique a la subred el tipo de servicio que requiere.

Total Length – Incluye la longitud total del paquete (encabezado + datos). Su longitud máxima es de 65.535 bytes.

Identification, Flags, Frag Offset - Proveen fragmentación de datagramas.

TTL - *Time To Live*, es un contador que sirve para limitar el tiempo de vida del paquete.

Protocol - Qué tipo de protocolo de capa 4 se transporta (TCP o UDP).

Header Checksum - Suma de verificación del encabezado de la cabecera.

SAdd - Dirección IP origen

DAdd - Dirección IP destino

IP options – Sirve para realizar Pruebas de red, depuración, seguridad, etc.

ARP: *Addresses Resolution Protocol;* parte en conocer la dirección de red IP y se encarga en averiguar la dirección MAC. También es importante por que ensambla los paquetes en el router.

ARP mapea direcciones IP a direcciones MAC

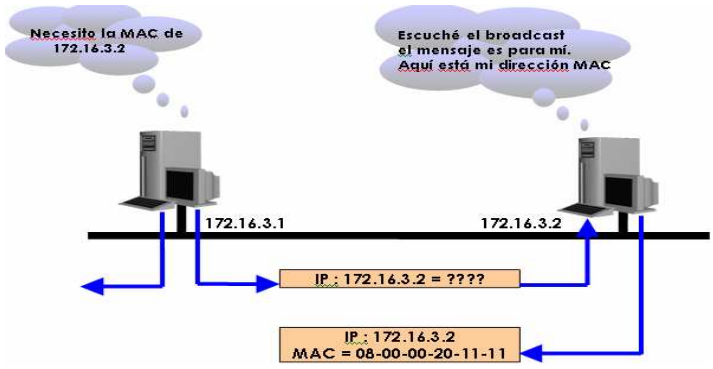


Fig. 1.8 Formato ARP **[2]**

RARP: *Reverse Address Resolution Protocol;* funciona de manera similar a ARP pero realiza la función inversa a la del protocolo ARP.

RARP mapea direcciones MAC a direcciones IP

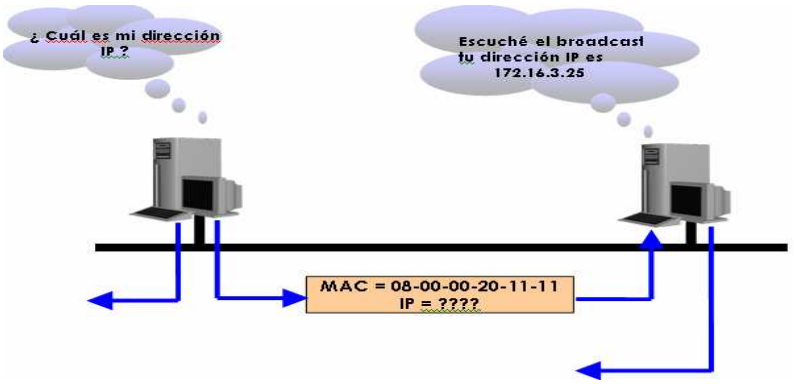


Fig. 1.9 Formato RARP **[2]**

ICMP: *Internet Control Message Protocol;* provee un mecanismo a un router o host destino para reportar un mensaje de error de un paquete transmitido, como objetivo tiene el monitoreo del IP.

IGMP: *Internet Group Message Protocol;* identifica a las estaciones existentes en una red las cuales son parte de un grupo que realizan multienvío. Multienvío es enviar un mismo mensaje a varias receptoras en forma simultánea.

1.1.3.4 Capa de Interfaz de Red

También se la conoce como capa de Host a Red en el Modelo TCP/IP, Enlace de Datos en el modelo OSI.

Haciendo referencia con el modelo OSI esta capa esta formada por dos capas (Enlace de Datos y Física) y la correspondiente a la capa de Enlace del modelo TCP/IP a su vez se subdivide en dos capas: LLC y MAC.

El modelo TCP/IP lo considera una caja negra, se ocupa de todos los aspectos que requiere un paquete IP para ser transportado a través del enlace físico. Además realiza control de flujo, detección de errores, control de errores y gestión de enlace.

Control de Flujo: para que el emisor no sobrecarge de datos al receptor.

Detección de errores: comparación del bit de paridad y CRC *Control de Redundancia Cíclica*

Control de errores: confirma si se transmitió correctamente o no los datos, sino lo retransmite.

En la figura 1.10 se presenta las funciones de la capa de transporte.

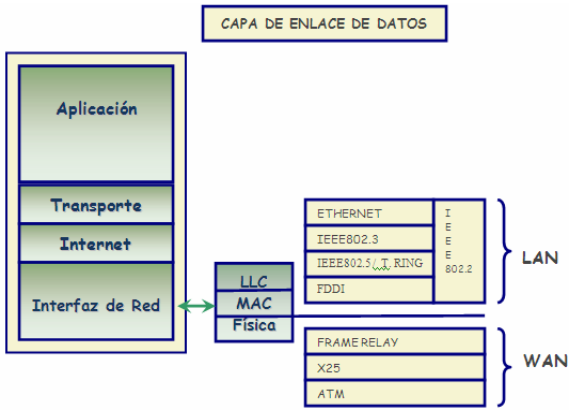


Fig. 1.10 Capa de Enlace de Datos

LLC: *Logical Link Control;* proporciona una interfaz común, único entre las capas superiores y la subcapa MAC, se encarga específicamente del control de errores, control de flujo, entramado y direccionamiento MAC, es utilizada en redes LAN.

En las redes IEEE 802.x esta subcapa opera con la especificación IEEE 802.2.

MAC: *Médium Access Control;* es la encargada de definir la forma de acceder al medio, en IEEE 802.3 se opera con el del protocolo CSMA/CD "*Carrier Sense Multiple Access / Collision Detect*".

Capa Física: La Capa Física es la encargada en definir las especificaciones para las conexiones físicas de la computadora hacia la red

A continuación, en la tabla 1.1 se definen los protocolos del estándar IEEE 802.3 utilizados en cada una de las subcapas de la capa de enlace de datos.

Tabla 1.1: Estándar IEEE 802.3

IEEE 802.3	***- LLC***	*802.2*	Ofrece servicios de conexión lógica a nivel de capa 2.
	- MAC	*CSMA/CD*	Cuando un nodo desea enviar datos, primero debe determinar si los medios de red se encuentran ocupados.
	- Física	*10/100 Base-T*	Es un estándar en el que se define la conexión Ethernet mediante cables de par trenzado (UTP con conectores RJ45).

En el presente proyecto se trabajará con una red TCP/IP sobre IEEE 802.3 (10/100 Base-T).

1.2 PROTOCOLO IPV4

IPv4 es la versión 4 del Protocolo IP (Internet Protocol). Esta fue la primera versión del protocolo que se implemento extensamente, y forma la base del actual Internet.

IPv4 usa direcciones de 32 bits, limitándola a 2^{32} = 4.294.967.296 direcciones únicas, muchas de las cuales están dedicadas a redes locales (LANs). Debido al crecimiento inusitado que ha tenido el Internet, combinado con el hecho de que hay desperdicio de direcciones en muchos casos, ya hace varios años se vio que escaseaban las direcciones IPv4.

Esta limitación ayudó a estimular el impulso hacia la versión 6 del protocolo IP (IPv6), que esta actualmente en las primeras fases de implementación, y reemplazará con seguridad a IPv4.

Seguidamente empezaremos con la descripción del protocolo IPv4.

1.2.1 CABECERA IPV4

La cabecera IPv4 consta de 13 campos los cuales se detallan abajo; la figura 1.11 muestra los campos de la cabecera.

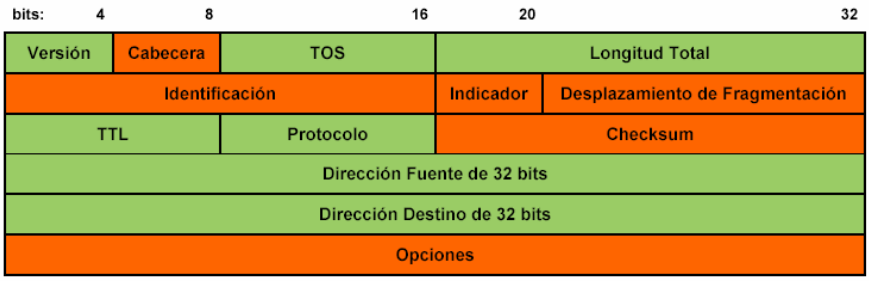


Fig. 1.11 Formato de la Cabecera IPv4 **[3]**

A continuación definimos cada uno de los campos existentes en la cabecera IPv4:
Versión: (4 bits) Registra el tipo de versión del protocolo al que pertenece el datagrama, y este puede ser registrado como: 0100 (versión 4) ó 0110 (versión 6) ya que actualmente existen dos versiones.

IHL: *Tamaño de la Cabecera,* (4 bits) Indica la longitud de la cabecera en palabras de 32 bits. La cual pude tener un valor mínimo de 5 palabras para una cabecera correcta y un valor máximo de 15 palabras. En el ejemplo se transmiten 5 palabras de 32 bits.

ToS: *Tipo de Servicio,* (8 bits) permite que el host indique a la subred el tipo de servicio que requiere e indica una serie de parámetros sobre la calidad de servicio deseada durante el paso por una red. Algunas redes ofrecen prioridades de servicios, considerando determinado tipo de paquetes "más importantes" que otros. Estos 8 bits se agrupan de la siguiente manera. Los 5 bits de menos peso son independientes e indican características del servicio: **[4]**

Bit 0: sin uso, debe permanecer en 0.
Bit 1: 1 costo mínimo, 0 costo normal.
Bit 2: 1 máxima fiabilidad, 0 fiabilidad normal.
Bit 3: 1 máximo rendimiento, 0 rendimiento normal.
Bit 4: 1 mínima demora, 0 demora normal.

Los 3 bits restantes están relacionados con la precedencia de los mensajes, y responden a los siguientes nombres.

000: De rutina.

001: Inmediato.

010: Inmediato.

011: Relámpago.

100: Invalidación relámpago.

101: Procesando llamada crítica y de emergencia.

110: Control de trabajo de Internet.

111: Control de red.

Longitud Total: (16 bits) Incluye el tamaño total del datagrama, en octetos; la cabecera y los datos. El tamaño máximo de los datagramas usados normalmente es de 576 octetos (64 de cabeceras y 512 de datos).

Es decir que para enviar 440 octetos de datos la representación binaria sería (0000000110111000) y esta especificada como 40 octetos de cabecera y 400 octetos de datos

En caso de fragmentación este campo contendrá el tamaño del fragmento, no el del datagrama original.

Identificación: (16 bits) Se utilizará en caso de que el datagrama deba ser fragmentado, para poder distinguir los fragmentos de un datagrama de los de otro, todos lo datagramas tienen un mismo valor de identificación. En el ejemplo decimos que es el fragmento 7 del datagrama 16

Indicadores: (3 bits) Actualmente utilizado sólo para especificar valores relativos a la fragmentación de paquetes: **[4]**

bit **0**: Reservado; debe ser 0

bit **1**: **0** = Divisible, **1** = No Divisible

bit **2**: **0** = Último Fragmento, **1** = Fragmento Intermedio (le siguen más fragmentos)

La indicación de que un paquete es indivisible debe ser tenida en cuenta bajo cualquier circunstancia. Si el paquete necesitara ser fragmentado, no se enviará.

Desplazamiento del Fragmento: (13 bits) Indica en qué parte del datagrama va el fragmento, en unidades de 64 bits, que ocupa el paquete actual dentro del datagrama original. El primer paquete de una serie de fragmentos contendrá en este campo el valor 0.

Tiempo de Vida: (8 bits) Es un contador que sirve para limitar la vida del paquete. Limita el tiempo que un datagrama puede pasar en la red. TTL se decrementa en una unidad cada vez que pasa por un router si todo va bien, o en una unidad por segundo en el router si hay congestión. Al llegar a cero el datagrama es descartado.

Protocolo: (8 bits) Indica el protocolo de siguiente nivel al que debe entregarse (TCP o UDP u otro). Es decir, para pasar al protocolo TCP el cual su número de puerto es el 6 deberíamos especificar este valor en binario (00000110)

Checksum: *Suma de la Cabecera,* (16 bits) Se recalcula cada vez que algún nodo cambia alguno de sus campos (por ejemplo, el TTL). El método 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. Y se lo hace mediante el algoritmo del código de redundancia cíclica. (*Véase e proceso del algoritmo en el anexo 1*)

Dirección Fuente: (32 bits) Estos son divididos en cuatro octetos los cuales pueden estar entre 0 y 255, aunque el número binario de 8 bits más alto es 11111111 (256) ya que como se conoce la ultima dirección no se la utiliza y en su representación decimal cada valor de los octetos son separados por puntos (171.32.41.25)

Dirección Destino: (32 bits) Es similar a la dirección fuente.

Opciones: Se rellena para completar múltiplos de cuatro bytes. Actualmente hay cinco opciones definidas: Seguridad, Enrutamiento estricto desde el origen, Enrutamiento libre desde el origen, Registrar ruta y Marca de tiempo.

Aunque no es obligatoria la utilización de este campo, cualquier nodo debe ser capaz de interpretarlo.

Puede contener un número indeterminado de opciones, que tendrán dos posibles formatos: **[4]**

Simple: Un sólo octeto indicando el "Tipo de Opción":

El Tipo de Opción está dividido en 3 campos:

Indicador de Copia: 1 bit. En caso de fragmentación, la Opción se copiará o no a cada nuevo fragmento según el valor de este campo:

0=no se copia,

1=se copia.

Clase de Opción: 2 bits. Las posibles clases son:

0=control,

1=reservada,

2=depuración y mediciones,

3=reservada.

Número de Opción: 5 bits. Identificador de la Opción.

Compuesto: Un octeto para "Tipo de Opción", otro para "Tamaño de Opción", y uno o más octetos conformando los "Datos de Opción".

El Tamaño de Opción incluye el octeto de Tipo de Opción, el de Tamaño de Opción y la suma de los octetos de datos.

La figura 1.12 muestra como son asignados los bits en cada uno de los campos de la cabecera IPv4.

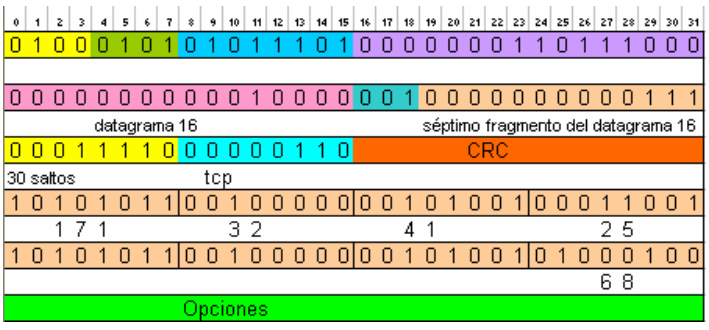


Fig. 1.12 Asignación de Bits en la Cabecera IPv4

1.2.2 CLASES DE DIRECCIONES IPV4

Existen cinco clases de direcciones, de las cuales las más utilizadas para configurar redes son las tres primeras y las dos restantes generalmente son usadas para pruebas. En la figura 1.13 se muestra las clases de direcciones y los bits que utilizan cada una de ellas.

	1er octeto	2do octeto	3er octeto	4to octeto
Clase A	Red	Host	Host	Host
Clase B	Red	Red	Host	Host
Clase C	Red	Red	Red	Host
Clase D,E				

Fig. 1.13 Clases de Direcciones

1.2.2.1 Direcciones Clase A

Las direcciones de clase A utilizan el primer octeto para definir sus redes y los tres octetos restantes es para la utilización de los hosts; como se muestra en la figura 1.14.

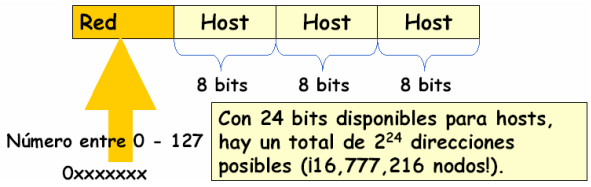


Fig. 1.14 Direcciones Clase A **[5]**

- Hay 126 redes Clase A posibles.
- Sólo asignadas a grandes organizaciones (militares, agencias del gobierno, universidades, grandes empresas)
- ISPs de Cable Modem en USA tienen 24.0.0.0
- Usuario DSL Pacbell en USA tienen 63.0.0.0
- Red radio paquetes (radio aficionados) a nivel mundial 44.0.0.0
- Ocupan un total de 2,147,483,648 de las direcciones de IPv4. (50% del espacio total unicast disponible).

1.2.2.2 Direcciones Clase B

Las direcciones de clase A utilizan los dos primeros octeto para definir sus redes y los dos octetos restantes es para la utilización de los hosts; como se muestra en la figura 1.15.

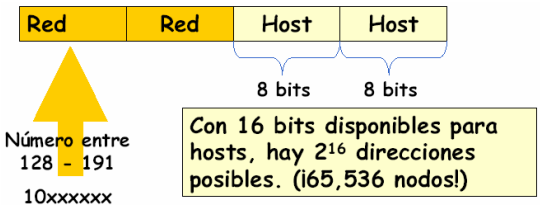


Fig. 1.15 Direcciones Clase B **[5]**

- Hay 16,384 (214) redes Clase B.
- Representan el 25% del espacio total de direcciones unicast IPv4.
- Sólo se asignan a grandes organizaciones incluidas corporaciones (Universidades, agencias del gobierno, ..).
- Red andaluza de Universidades 150.214.0.0
- Universidad Politécnica de Cataluña 147.83.0.0
- IBM 129.42.0.0

1.2.2.3 Direcciones Clase C

Las direcciones de clase A utilizan los tres primer octeto para definir sus redes y el último octetos es para la utilización de los hosts; como se muestra en la figura 1.16.

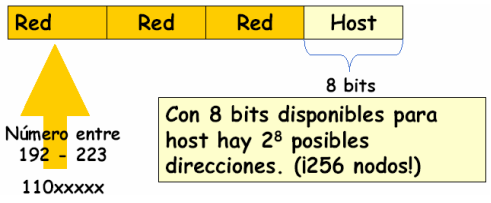


Fig. 1.16 Direcciones Clase C **[5]**

- Hay 2,097,152 redes clase C.
- Representan el 12.5% del espacio total de direcciones unicast IPv4.

La figura 1.17 muestra la asignación de bits a cada una de las diferentes clases de direcciones.

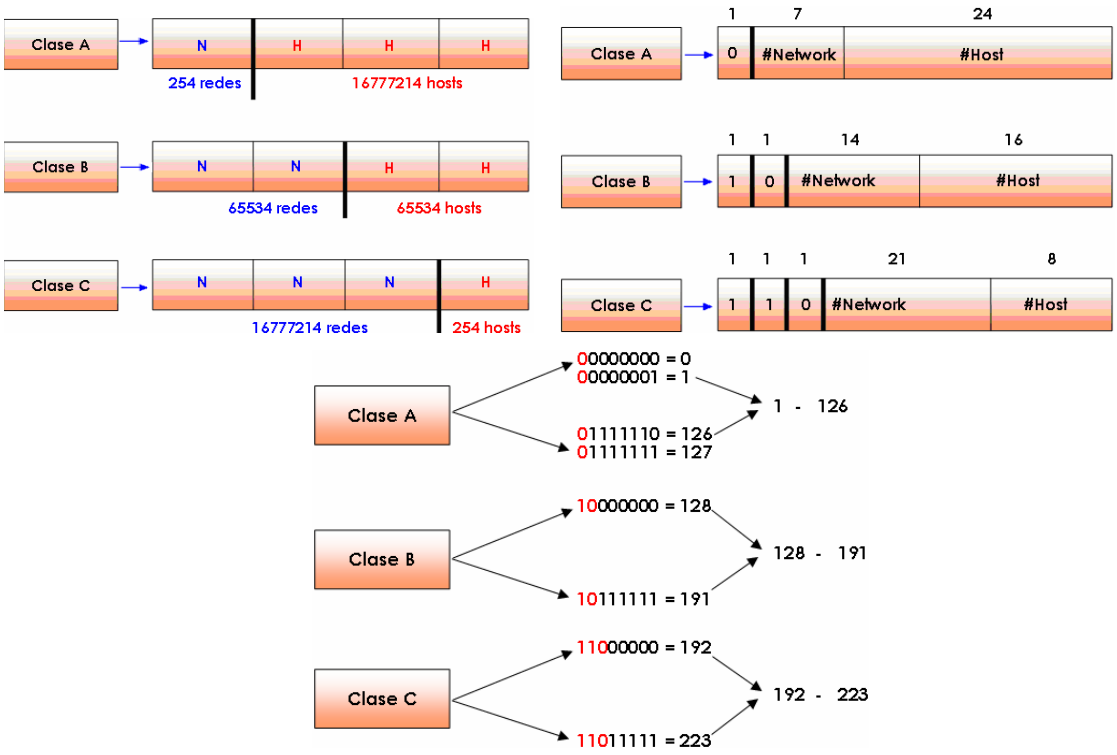


Fig. 1.17 Asignación de Bits por cada tipo de Direcciones **[2]**

1.2.2.4 Direcciones Especiales

Las direcciones especiales son utilizadas para diferentes campos como es mostrado en la figura 1.18.

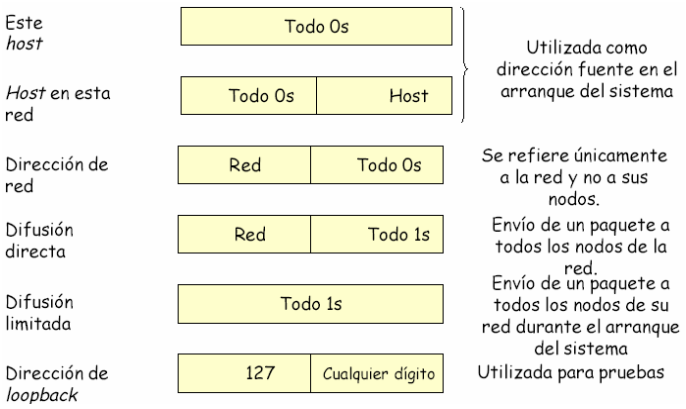


Fig. 1.18 Direcciones Especiales **[5]**

1.2.2.5 Direcciones Clase D, E

Por lo general este tipo de direcciones son utilizadas para realizar únicamente pruebas, en la figura 1.19 se muestra las direcciones D y E.

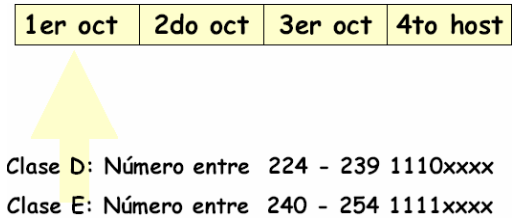


Fig. 1.19 Direcciones Clase D y E **[5]**

- La clase D está reservada para multicast.
- La clase E está reservada para experimentar, se utiliza para fines de investigación.

1.2.2.6 Direcciones Unicast

Son las direcciones dirigidas a un único interfaz de la red, ver figura 1.20.

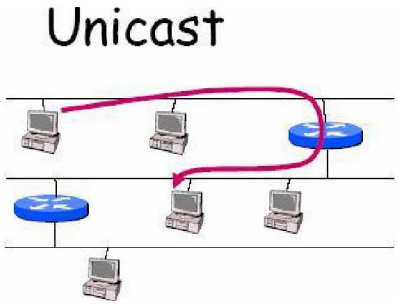


Fig. 1.20 Direccionamiento Unicast **[5]**

1.2.2.7 Direcciones Multicast

Identifica a un conjunto de interfaces de la red, de manera que el paquete sea enviado a cada una de ellos individualmente, ver figura 1.21.

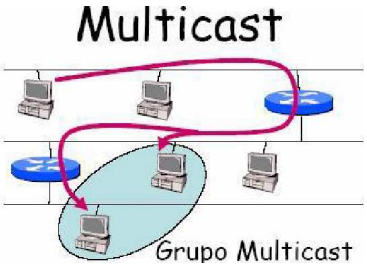


Fig. 1.21 Direccionamiento Multicast **[5]**

Estadísticas entre usos de tipos de direcciones

El uso de las direcciones IP-v4 enfrentaban las siguientes situaciones:

- Al principio las direcciones IP se asignaban a las organizaciones según se pedían sin tener en cuenta las necesidades reales.
- No se tomaba en cuenta el tamaño de las redes.

Bajo estas circunstancias el uso de las direcciones IP se muestran en la siguiente estadística, ver figura 1.22:

– Clase A: 16 millones

– Clase B: 65,536

– Clase C: 256

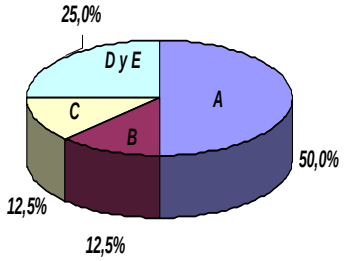


Fig. 1.22 Uso de Direcciones

1.2.3 SUBDIVISION DE UNA RED

Podemos ampliar una red mediante la utilización de dispositivos físicos, como: routers, switchs y puentes, para añadir segmentos de red. También podemos utilizar estos dispositivos para dividir una red en segmentos más pequeños y para incrementar la eficacia de la red.

Los segmentos de red separados por routers se denominan subredes. Cuando creamos subredes, debemos dividir el ID de red para los hosts de las subredes.

Para identificar el nuevo ID de red de cada subred, debemos utilizar una máscara de subred para especificar qué parte de la dirección IP va a ser utilizada por el nuevo ID de red de la subred. Podemos localizar un host en una red analizado su ID de red.

Los IDs de red coincidentes muestran qué hosts se encuentran en la misma subred. Si los IDs de red no son los mismos, sabremos que están en distintas subredes y que necesitaremos un router para establecer comunicación entre ellos.

1.2.4 SUBREDES

El establecimiento de subredes consiste en dividir una gran red lógica en redes lógicas más pequeñas.

Las razones que llevan a dividir una red van desde las limitaciones en las direcciones IP hasta la necesidad de simplificar las cosas, la figura 1.23 muestra un esquema de subredes.

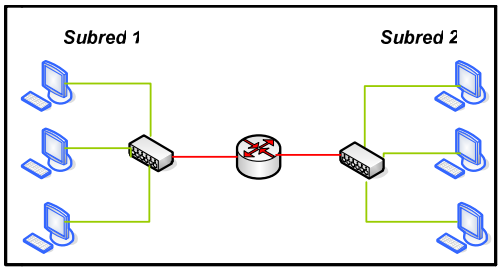


Fig. 1.23 Subredes

A medida que crece el número de equipos y el volumen de tráfico en una red Ethernet, se produce un crecimiento de la colisión de datos y se reduce el rendimiento de la red. Para solucionar este problema, los hosts de una red se agrupan en segmentos que se estructuran con los equipos de interconexión mencionados anteriormente.

En un entorno TCP/IP, los segmentos separados por routers se denominan subredes. Todos los equipos que pertenecen a una subred tienen el mismo ID de red en sus direcciones IP. Cada subred debe tener un ID de red distinto para comunicarse con otras subredes. Basándose en el ID de red, las subredes

definen las divisiones lógicas de una red. Los equipos que se encuentran en distintas subredes necesitan comunicarse a través de routers.

En la figura 1.24 se muestra la forma como se realiza la asignación de subredes.

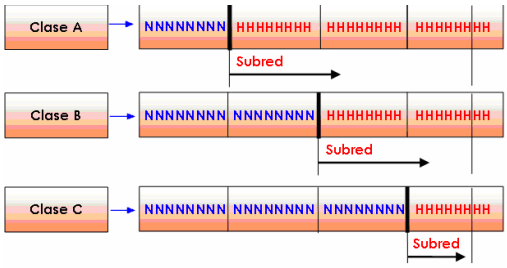


Fig. 1.24 Asignación de las Subredes **[2]**

En las siguientes tablas se muestra la utilización de las subredes de acuerdo al número de bits:

Tabla 1.2: Subredes utilizadas con la dirección clase B.

# de bits	*# de bits de máscara*	*Máscara de Subred*	*# de Subredes*	*# de Hosts*
2	18	255.255.192.0	2	16382
3	19	255.255.224.0	6	8190
4	20	255.255.240.0	14	4096
5	21	255.255.248.0	30	2046
6	22	255.255.252.0	62	1022
7	23	255.255.254.0	126	510
8	24	255.255.255.0	254	254
9	25	255.255.255.128	510	126
10	26	255.255.255.192	1022	62
11	27	255.255.255.224	2046	30
12	28	255.255.255.240	4096	14
13	29	255.255.255.248	8190	6
14	30	255.255.255.252	16382	2

Tabla 1.3: Subredes utilizadas con la dirección clase C.

# de bits	# de bits de máscara	Máscara de Subred	# de Subredes	# de Hosts
2	26	255.255.255.192	2	16382
3	27	255.255.255.224	6	8190
4	28	255.255.255.240	14	4096
5	29	255.255.255.248	30	2046
6	30	255.255.255.252	62	1022

Ejemplo de Subredes

Dada la dirección Clase B 190.52.0.0

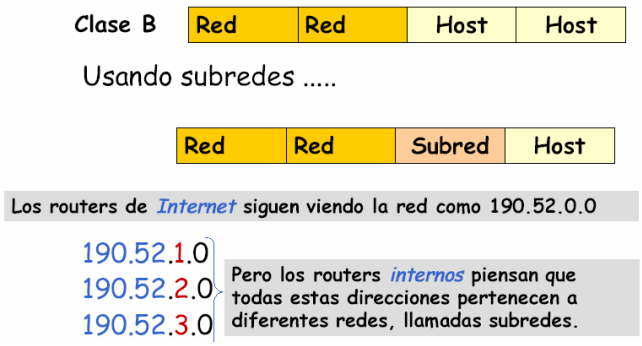


Fig. 1.25 Ejemplo de Subredes **[5]**

1.2.5 MÁSCARA DE SUBRED

Las direcciones IP de clase A, B y C tienen una máscara de red definida, una máscara de red consiste en una dirección IP en donde los bits que representan a la red están puestos a 1 y los bits que representan al host están puestos a 0.

La máscara de red permite determinar cuál es la porción de red y la porción de host en una dirección dada, en la figura 1.26 se muestra las máscaras asignadas a cada tipo de direcciones.

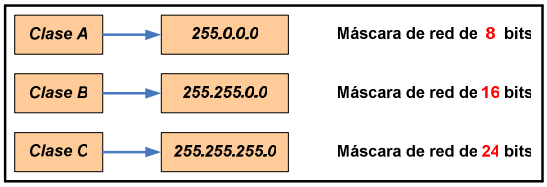


Fig. 1.26 Máscara de Subred

En consecuencia, una organización que tenga asignado un ID de red tiene un único ID de red fijo y un número de hosts específico determinado por la clase de dirección a la que pertenezca la dirección IP.
Con el ID de red único, la organización sólo puede tener una red conectándose a su número asignado de hosts. Si el número de hosts es grande, la red única no podrá funcionar eficazmente. Para solucionar este problema, se introdujo el concepto de subredes.

1.2.5.1 Estructura de las Máscaras de Subred

Para dividir un ID de red, utilizamos una máscara de subred. Una máscara de subred es una pantalla que diferencia el ID de red de un ID de host en una dirección IP pero no está restringido por las mismas normas que el método de clases anterior. Una máscara de subred está formada por un conjunto de cuatro números, similar a una dirección IP.

Para aplicar la máscara, la dirección IP debe ser convertida a formato binario al igual que la máscara, después se aplica una operación lógica AND entre las dos direcciones.

En el método de clases, cada uno de los cuatro números sólo puede asumir el valor máximo 255 o el valor mínimo 0. Los cuatro números están organizados como valores máximos contiguos seguidos de valores mínimos contiguos. Los valores máximos representan el ID de red y los valores mínimos representan el ID de host.

Por ejemplo, 255.255.0.0 es una máscara de subred válida, pero 255.0.255.0 no lo es. La máscara de subred 255.255.0.0 identifica el ID de red como los dos

primeros números de la dirección IP, en la figura 1.27 se muestra la estructura de una máscara de subred.

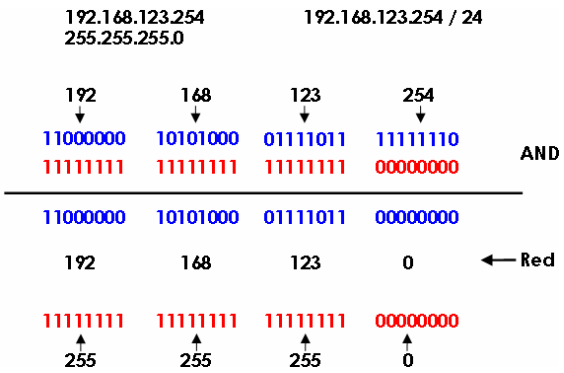


Fig. 1.27 Estructura de la Máscara de Subred **[2]**

1.2.6 ASIGNACIÓN DE IDs DE RED

El ID de red identifica los hosts TCP/IP ubicados en la misma subred física. Todos los hosts de la misma subred deben tener asignado el mismo ID de red para que puedan comunicarse entre sí.

Todas las subredes deben tener un ID de red exclusivo y en la tabla 1.4 se muestra el intervalo de direcciones que tienen cada una de las clases de direccionamiento.

Tabla 1.4: Asignación de IDs de Red

Clase de Dirección	*Inicio del Intervalo*	*Fin del Intervalo*
Clase A	*1.0.0.0*	*126.0.0.0*
Clase B	*128.0.0.0*	*191.255.0.0*
Clase C	*192.0.0.0*	*223.255.255.0*

En la figura 1.28 se muestra un ejemplo de asignación de direcciones para subredes:

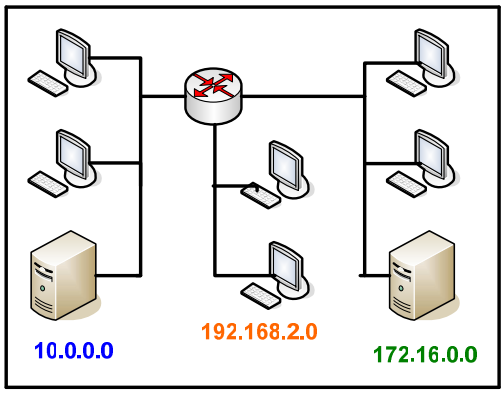


Fig. 1.28 Asignación de IDs de Red

1.2.7 ASIGNACIÓN DE IDs DE HOST

El ID de host identifica a un host TCP/IP de una red y debe ser exclusivo para un ID de red determinado. Todos los hosts TCP/IP, incluyendo las interfaces de red de los routers, requieren IDs de host exclusivos. No existen normas para la asignación de IDs de host en una subred.

La tabla 1.5 se muestra una lista de intervalos válidos de IDs de host para cada clase de red.

Tabla 1.5: Asignación de IDs de Hosts

Clase de Dirección	*Inicio del Intervalo*	*Fin del Intervalo*
Clase A	*w.0.0.1*	*w.255.255.254*
Clase B	*w.x.0.1*	*w.x.255.254*
Clase C	*w.x.y.1*	*w.x.y.254*

En la figura 1.29 se muestra un ejemplo de asignación de direcciones de hosts:

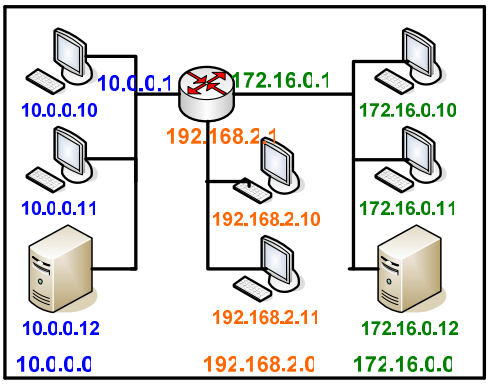


Fig. 1.29 Asignación de IDs de Host

1.2.8 SUBNETTING

Permite dividir una red clase A, B ó C en subredes. Además permite una mejor distribución de direcciones ante la creciente demanda, facilita el control del espacio de las direcciones, oculta la estructura interna de la red, es capaz de reducir las tablas de ruteo.

El subnetting permite segmentar el número de redes (*Implementar subredes*) entre varias redes físicas sin solicitar nuevas direcciones IP. Consiste en agregar un nivel jerárquico en la dirección IP.

En la figura 1.30 se muestra la parte de bits que se puede usar para la creación de subredes para una dirección de clase B.

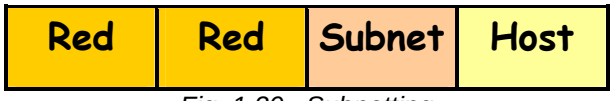


Fig. 1.30 Subnetting

Ejemplo: Usando el tercer octeto, la red 190.52.0.0 se divide en las siguientes 254 subredes:

190.52.1.0 190.52.2.0 190.52.3.0 190.52.4.0
190.52.5.0 190.52.6.0 190.52.7.0 190.52.8.0
190.52.9.0 190.52.10.0 190.52.11.0 190.52.12.0
190.52.13.0 190.52.14.0 190.52.15.0 190.52.16.0
190.52.17.0 190.52.18.0 190.52.19.0 .....

Las subredes se identifican por dirección de subred más la máscara:
192.52.1.0 255.255.255.0 ó 192.52.1.0/24

1.2.8.1 Desperdicio del subnetting

Para evitar el desaprovechamiento del subnetting se utiliza la siguiente política:

- Muchos routers permiten utilizar la subred 0, esta no suele estar habilitado por defecto y es necesario ejecutar algún comando específico en el IOS del router.
- Por ejemplo en los routers de CISCO en versiones del IOS anteriores a la 12.x no estaba habilitado por defecto y había que ejecutar el comando: “ip subnet-zero”.
- Habilitar el uso de la subred 0 implica que el router también intercambia información de ella en sus actualizaciones En general es posible utilizar la subred todo a 1 en los routers aunque no es recomendable.
- Al usar esa subred no es posible enviar broadcast dirigido a la red.

En la presente tabla se muestra el desperdicio de direcciones que se produce al realizar el subnetting.

Tabla 1.6: Desperdicio de Subnetting

		Clase B		
Bits Subred	***Subred Creadas***	***Host por Subred***	***Cant. Total de Host***	***% Utilizado***
2	2	16.382	32764	50
3	6	8.190	49140	75
4	14	4.094	57316	87
5	30	2.046	61380	94
6	62	1.022	63364	97
7	126	510	64260	98
8	254	254	64516	98
9	510	126	64260	98
10	1022	62	63364	97
11	2046	30	61380	94
12	4094	14	57316	87
13	8190	6	49140	75
14	16382	2	32764	50
		Clase C		
Bits Subred	***Subred Creadas***	***Host por Subred***	***Cant. Total de Host***	***% Utilizado***
2	*2*	*62*	*124*	*49*
3	*6*	*30*	*180*	*71*
4	*14*	*14*	*196*	*77*
5	*30*	*6*	*180*	*71*
6	*62*	*2*	*124*	*49*

1.2.9 CIDR - Classless Interdomain Routing

CIDR es una forma estática de hacer subnetting, por lo que Todas las subredes generadas utilizan la misma máscara de subred, no aprovecha el espacio de direcciones.

Desarrollado en 1994, CIDR mejora la eficiencia y escalabilidad de IPv4. CIDR es una nueva forma de dividir números IP en red/host ya que no encamina de acuerdo a la clase de red.
Para determinar la porción de red de la dirección se utilizan prefijos de red (/8, /19,etc.).

Estas mejoras se han logrado hacer mediante:

- La sustitución del direccionamiento con clases por un esquema más flexible y que genera menos desperdicio (VLSM)
- Mejora la agregación de rutas (sumarización).
- CIDR permite a los routers agregar, o sumarizar, la información de enrutamiento y, así, se reduce el tamaño de sus tablas de enrutamiento
- Sólo la combinación de una dirección y su máscara pueden representar la ruta a múltiples redes
- Utilizado por los routers tanto dentro una organización, conocido como AS (*Autonomous Syst*em), como entre ASs gestionados por diferentes administradores.
- Los administradores pueden mantener las número de entradas de las tablas de enrutamiento manejables, utilizando un prefijo de dirección para resumir las rutas, lo que significa:
- Rutado más eficiente.
- Reducción del consumo de CPU cuando haya que recalcular la tabla de enrutamiento o cuando haya que recorrer la tabla para buscar una entrada coincidente.
- Reducción de los requerimientos de memoria en el router.
- La agregación de rutas también se conoce como:
    - Resumen de rutas.
    - Supernetting.
- Supernetting es básicamente la inversa del subnetting.
- Con CIDR la responsabilidad de asignación de direcciones no está centralizada (InterNIC).

- A los ISPs (*Internet Service Providers*) se les asignan bloques de espacio direcciones, que pueden distribuir entre sus clientes.

El CIDR es utilizado por los RSPs *(Regional Service Providers)*, ISPs, NSPs *(Network Service Providers)* para administrar la red Internet, y por tanto hacer un mejor aprovechamiento de las direcciones IP.

1.2.9.1 Restricciones del CIDR

Los protocolos de enrutamiento dinámico deben enviar la información tanto del prefijo como de la máscara en sus actualizaciones de enrutamiento.

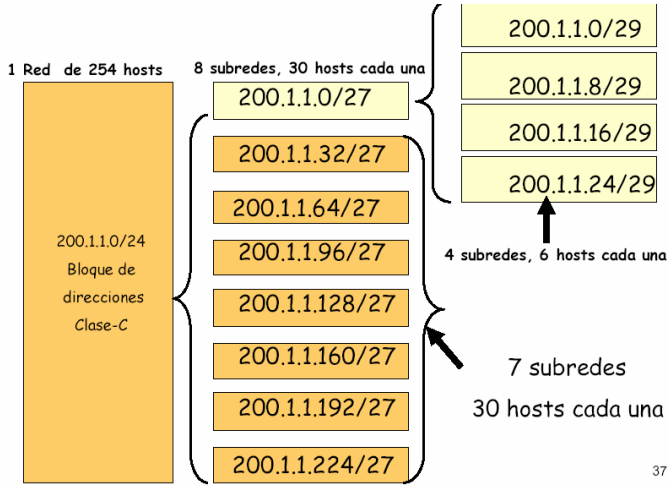
En otras palabras, CIDR requiere *Protocolos de enrutamiento sin clase***.** Cuando se utiliza el enrutamiento sin clase, si un router recibe un paquete destinado a una subred de una red de la que no tiene ruta por defecto, entonces el router reenvía el paquete por la mejor ruta (aquella que tenga mayor coincidencia de prefijo).

1.2.10 VLSM (Máscara de Red de Longitud Variable)

Es un subnetting con mascara variable, cada subred puede utilizar una máscara diferente, es un poco más complejo de implementar y mantener, al contrario que CIDR este si aprovecha el espacio de direcciones.

VLSM permite a una organización utilizar más de una máscara de subred dentro del mismo espacio de direcciones de Red. “hacer subnetting de una subred”

EJEMPLO: Dada la dirección 200.1.1.0/24



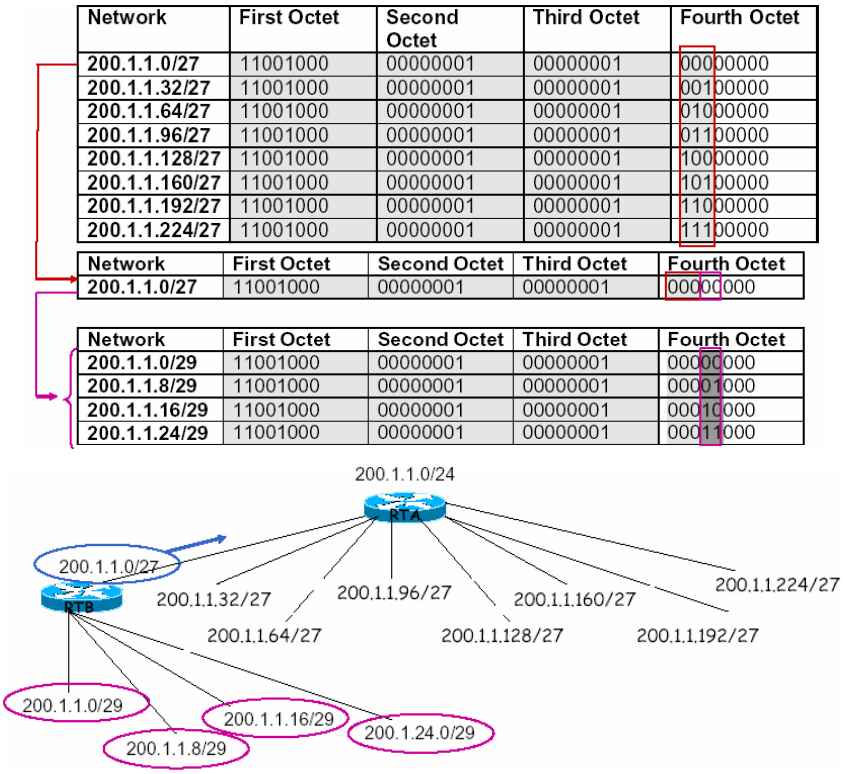


Fig. 1.31 Ejemplo de VLSM **[5]**

1.2.10.1 Restricciones de VLSM

Para utilizar VLSM con protocolos de enrutamiento dinámico, es necesario que éstos envíen la información de subred en sus actualizaciones. VLSM requiere de un Protocolo de enrutamiento

1.2.11 CONFIGURACION DE TCP/IP CON IPv4

En la figura 1.32 que se muestra más abajo se describe el prototipo a utilizarse para la configuración del protocolo IPv4 en el LTI.

El protocolo TCP/IP puede ser configurado en servidores y host con Windows mediante los siguientes métodos: **[6]**

- Configuración automática
- Configuración dinámica
- Configuración alternativa
- Configuración manual

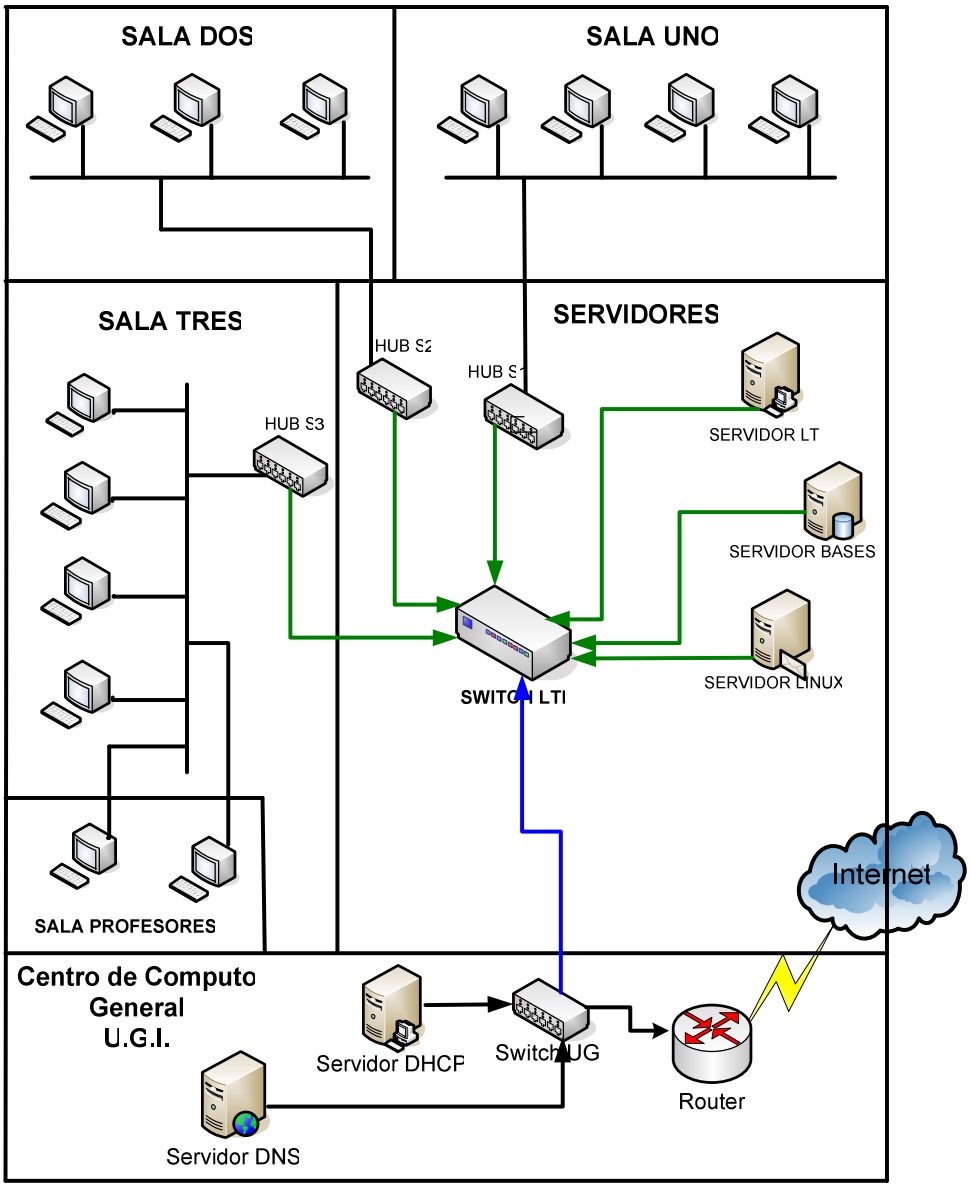


Fig. 1.32 Red LTI

1.2.11.1 Configuración Automática

El protocolo TCP/IP utiliza direcciones IP privadas automáticas (APIPA, *Automatic Private IP Addressing*) de forma predeterminada para proporcionar configuración automática mediante un intervalo de direcciones IP, y la mascara de subred. No se pueden configurar automáticamente puertas de enlace predeterminadas, servidores DNS o servidores WINS, ya que la característica APIPA está concebida para redes formadas por un único segmento de red que no están conectadas a Internet.

1.2.11.2 Configuración Dinámica

Mediante DHCP, la configuración del protocolo TCP/IP se realiza de forma dinámica y automática al iniciar el equipo. Para la configuración dinámica se requiere la configuración de un servidor DHCP. De forma predeterminada, los equipos que ejecutan sistemas operativos Windows Server 2003 son clientes DHCP. Al configurar correctamente el servidor DHCP, los hosts TCP/IP pueden obtener la información de configuración de la dirección IP, máscara de subred, puerta de enlace predeterminada, servidor DNS, tipo de nodo NetBIOS y servidor WINS. Se recomienda la configuración dinámica (con DHCP) para redes TCP/IP medianas y grandes.

1.2.11.3 Configuración Alternativa

La configuración alternativa permite a un equipo utilizar una configuración de dirección IP alternativa configurada manualmente en ausencia de un servidor DHCP. Puede utilizar una configuración alternativa cuando el equipo se usa en más de una red, al menos una de las redes no tiene un servidor DHCP y no se desea una configuración automática.

1.2.11.4 Configuración Manual

Mediante la configuración manual de las propiedades del protocolo TCP/IP a través de las propiedades de una conexión de red, se puede asignar una dirección IP, una máscara de subred, una puerta de enlace predeterminada, un servidor DNS y un servidor WINS. La configuración manual es necesaria en redes con varios segmentos de red cuando no hay servidores DHCP.

En el anexo 2 véase la descripción técnica de los modos de configuración de IPv4 con su respectivo diagrama.

1.3 LIMITACIONES DEL PROTOCOLO IPV4

IPv4 que fue creado hace casi veinte años ha probado ser un protocolo flexible y poderoso, que sin embargo presenta ya algunas limitaciones debido al crecimiento espectacular de Internet. A continuación se menciona sus principales limitaciones:

1. Inminente saturación del espacio de direcciones.

2. Debido al desarrollo tecnológico, IPv4 resulta inadecuado para las nuevas aplicaciones multimedia, como videoconferencia, VoIP, aplicaciones en tiempo real; las cuales requieren garantías en:
    - ✓ Los tiempos de respuesta
    - ✓ La disponibilidad de Ancho de Banda
    - ✓ Seguridad

3. Actualmente Internet proporciona nuevos servicios como: e-comerce; que requiere mayores mecanismos de seguridad que IPv4 no proporciona.

4. IPv4 solo proporciona las siguientes seguridades:
    - ✓ La seguridad es opcional en el protocolo IPv4.
    - ✓ Existen varias herramientas pero ninguna es un estándar debido a que IPv4 no fue diseñado para ser seguro.
    - ✓ Originalmente fue diseñado para una red militar aislada, la misma que posteriormente se convirtió en una red pública para investigación y educación.
    - ✓ Sin embargo se han definido varias herramientas de seguridad para el protocolo IPv4.
        - SSL, SHTTP, IPSecv4
        - Ninguna es un estándar

5. Lentitud debido a protocolos de enrutamiento ineficientes, que además hacen que las tablas de enrutamiento sean de gran tamaño y muy difíciles de mantener, lo que hace ineficaz al Internet y perjudica los tiempos de respuesta.

6. Es difícil distinguir entre las diferentes clases de tráfico para darles un tratamiento especial.

1.4 PERSPECTIVAS

Internet se ha introducido en todos los ámbitos del que hacer diario. El motivo básico para crear un nuevo protocolo fue la falta de direcciones debido al desperdicio de direcciones y limitaciones de IPv4. Además, de que inicialmente no se consideró el enorme crecimiento que iba a tener Internet; es asi que se asignaron bloques de direcciones grandes (de 16,7 millones de direcciones) a países, e incluso a empresas; quedando redes de clase C con pocas direcciones para hosts, y es el Ecuador un claro ejemplo y principalmente la EPN *(Escuela Politécnica Nacional*), limitando el crecimiento ordenado de las redes.

Tomando en cuenta la falta de direcciones, las limitaciones presentadas por el protocolo IPv4 y debido a su imparable crecimiento de requerimientos, ha sido necesario presentar una nueva versión del protocolo IP.

Por lo cual, el IETF (*Internet Engineering Task Force)*, ha diseñado una nueva interpretación, denominada IPv6 (*Internet Protocolo* versión 6). Este nuevo modelo se regirá como el sucesor de la versión 4 puesto que resuelve sus deficiencias y aporta nuevas funciones acordes a la evolución actual de la red.

Esta versión, entre sus principales características, amplia el espacio de direcciones posibles en Internet, ahora el tamaño de una dirección es de 128 bits, dando un total aproximado de 3,4084x1038 direcciones.

El aumento progresivo de las aplicaciones que necesitan direcciones IP públicas, globales, válidas para conexiones extremo a extremo, y por tanto, unido al crecimiento de la nueva generación de telefonía móvil que funcionará sobre IP.

Debido a la multitud de nuevas aplicaciones en las que IPv4 es utilizado, ha sido necesario agregar nuevas funcionalidades al protocolo básico, lo mismo que genera complicaciones en su escalabilidad para nuevos requerimientos y en el uso simultáneo de dos o más funcionalidades.

Entre las más conocidas se pueden mencionar medidas para permitir la Calidad de Servicio (QoS), Seguridad (IPsec) y movilidad.

Otra característica importante es la simplificación del formato de los encabezados; para esto algunos campos que se encontraban en IPv4 se han eliminado o se han hecho opcionales, reduciendo costos en el procesamiento de los encabezados y

en el consumo de ancho de banda. IPv6 puede distinguir entre diferentes clases de flujos y permite que la autenticación, integridad y la confidencialidad de la información se lleven a cabo como parte del protocolo y no como extensiones adicionales.

IPv6 es un activador fundamental para la visión que tenemos de la Sociedad de Información Móvil. Actualmente, el número de teléfonos inalámbricos ya supera con creces el número de terminales fijos de Internet. Además, IPv6 permite la oferta de servicios y prestaciones demandadas por las infraestructuras móviles (GPRS, UMTS), redes de banda ancha, electrónica de consumo y terminales, y la subsecuente interoperatibilidad/gestión.

CAPITULO 2: INTRODUCCION AL PROTOCOLO IPV6

2.1 INTRODUCCION GENERAL

Esta nueva versión de IP viene a cubrir algunos vacíos de la versión anterior IPv4. Es definido como IPv6 o IPng (*Next Generation*) y al igual que IPv4 se trata del protocolo de transmisión de datagramas del nivel IP de la capa Internet.
No se trata de añadir algunos números más a las direcciones IP, sino de un replanteamiento de todos los requerimientos de IP para el futuro del Internet.

Para la definición de este nuevo protocolo IP se han desarrollado algunos RFC:

- En noviembre de 1994 se desarrolla la primera propuesta llamada:
  - **RFC 1752** – The Recommendation for de IP Next Generation
- En 1996 se publican más propuestas como:
  - **RFC 1883** – The IPv6 base protocol.
  - **RFC 1884** – The address specification.
  - **RFC 1885** – Description of the control protocol ICMP.
  - **RFC 1886** – Addressing the problems of on enhaced DNS.
- En Abril de 1996 aparece:
  - **RFC 1933** – Mecanismo de Transición de IPv6, que en el 2000 sería sustituida por el RFC 2983.

Con el pasar del tiempo estos documentos fueron substituidos pero siguieron detallando más y mejores reformas al protocolo; el listado completo de las RFCs que se han publicado se presentan en el anexo 3.

2.1.1 CARACTERÍSTICAS DE IPV6

IPv6 presenta varias características, entre las cuales se puede mencionar las siguientes:

- ✓ Direcciones de 128 bits las que permiten obtener una gran cantidad de direcciones.
- ✓ El Encaminamiento es jerárquico para la agregación de rutas.

- ✓ Cabecera más simple; además que se puede realizar extensiones y agregar más opciones, estas extensiones son alineadas a 64 bits.
- ✓ Gran versatilidad para un formato más flexible de opciones.
- ✓ Para Multimedia presenta un identificador de flujo.
- ✓ Las direcciones Multicast realizan un obligatorio control de ámbitos.
- ✓ En la Seguridad tiene soporte a la autenticación/encriptado (IPSec).
- ✓ Autoconfiguración o configuración automática.
- ✓ En la movilidad mejora la eficiencia y la seguridad.
- ✓ Multihoming facilita el cambio de proveedor.
- ✓ IPv6 tiene QoS *(Calidad de Servicio)* y CoS *(Clase de Servicio).*
- ✓ Paquetes con datos de hasta 65.535 bytes.
- ✓ La escalabilidad es la base más importante frente a IPv4.

La calidad de servicio *(QoS, Quality of Service)* en IPv6 garantiza que se transita cierta cantidad de datos en un determinado tiempo, que exista menos retardo en la transmisión de paquetes en un tiempo definido, mejor distribución del ancho de banda, recuperación de los datos perdidos y mejor administración de trafico en la red. Los usuarios son capaces de tratar con una o más clases de trafico de distinta manera; para lo cual en la cabecera IPv6 existen dos campos fundamentales que son:

- o *Etiqueta de flujo.*- es el más usado por los nodos fuente para marcar grupos de paquetes que demanden mayor calidad.
- o *Clase de tráfico.*- indica la prioridad de reenvió de paquetes.

Esto minimiza el trabajo a los routers para enviar y recibir los paquetes.

La clase de servicio *(CoS)* trabaja juntamente con la calidad de servicio y principalmente hace referencia al campo clase de tráfico de la cabecera IPv6 cuya información sirve para definir la prioridad en el envió de paquetes de acuerdo al tipo de aplicación.

2.1.2 BENEFICIOS DE IPV6

Tomando como referencia las características citadas anteriormente y por la estructura el nuevo protocolo IPv6 se presenta una serie de beneficios, entre los cuales podemos citar a los siguientes:

- ✓ Si antes se requería de un equipo de personas para el manejo de una red, gracias a IPv6 este trabajo ya se lo podrá hacer de forma no-presencial.
- ✓ Ahorro de recursos tanto económicos como humanos por lo que la red se autoconfigura.
- ✓ Gracias a la unión de los Jumbograms (*paquetes de gran tamaño)*, con los servicios de Anycast y Multicast, ya es posible ofrecer una retransmisión de cualquier tipo de eventos en directo y con una gran calidad.
- ✓ Es posible emitir un número mayor de megabytes por paquetes IP; los Jumbograms permiten emitir paquetes de hasta 4 gigabytes, mientras el protocolo actual no llega ni a 1 megabyte.
- ✓ En IPv6 se puede trabajar con Multihoming.

2.2 ESTRUCTURA DEL PROTOCOLO IPv6

2.2.1 FORMATO DE UN PAQUETE

El paquete IPv6, también conocido como datagrama IPv6, consta de un encabezado y de sus datos, como se muestra en la figura 2.1.

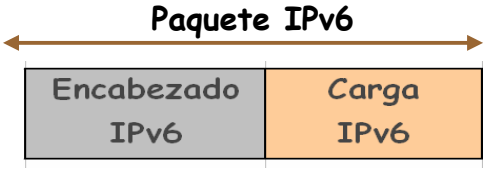


Fig. 2.1 Formato de un Paquete

En este paquete no existe limitación en el número de opciones que se presentan en la cabecera.

Las cabeceras tienen mejores prestaciones debido a su ordenación, las cuales pueden ser por:

- o Cabeceras procesadas por los routers.
- o Cabeceras procesadas en su destino.

2.2.2 CABECERA IPV6

IPv6 ha realizado algunas modificaciones en el formato de la cabecera con respecto a IPv4, razón por la cual el formato de la nueva cabecera se ha reducido a 8 ocho campos solamente. La cabecera que utiliza IPv6 tiene un tamaño fijo de 40 bytes.

En la figura 2.2 se muestra el formato modificado de la cabecera IPv6.

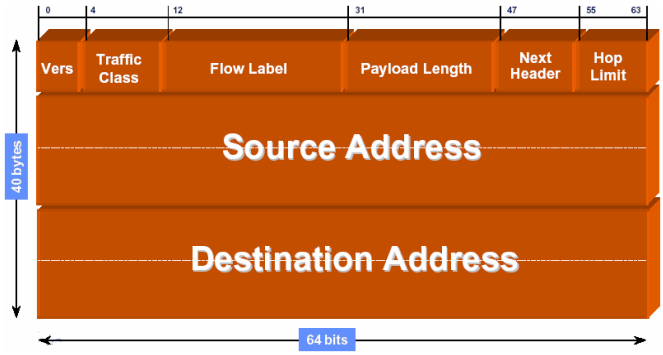


Fig. 2.2 Encabezado IPv6 **[7]**

A continuación se describe la función de cada campo.

Version *(Versión)**:*** Tiene una longitud de 4 bits, indica el tipo de versión del protocolo, en este caso es 0110 (versión 6).

Traffic Class *(Clase de Tráfico)**:*** Su longitud es de 8 bits, distingue los diferentes tipos de tráfico, usado por los host y routers siendo que los router pueden modificar estos valores. A continuación se detalla los más utilizados:

- 0 a 7 son para transmisores capaces de reducir su velocidad.
- del 8 al 15, para tráfico de tiempo real.

  Se sugiere:
- 1 para noticias.
- 4 para ftp.
- 6 para telnet. **[8]**

Este campo puede ser modificado dependiendo de la aplicación que se vaya a realizar, aunque no es necesario por que IPv6 ya hace una asignación.

Flow Label (*Etiqueta de flujo):* este campo es de 20 bits e identifica a una secuencia de datagramas de un origen. Ejemplo: en el caso de flow label sea 0 implica un flujo no identificado, para valores diferentes de cero implica que todos los paquetes pertenecen al mismo flujo.

Payload Length (*Longitud de datos):* este campo utiliza 16 bits, indica el tamaño de datos del paquete en octetos y cuyo paquete puede llegar a tener 64000 bytes.

Next Header *(Siguiente cabecera)**:*** Tiene una longitud de 8 bits, este campo permite añadir cabeceras al paquete original para realizar otras características como encriptación y autenticación. Las cabeceras de extensión son examinadas únicamente en el destino (router o host), y cuando estas llevas el valor de cero lo que indica es que a esta cabecera se le puede examinar en cada nodo y es una cabecera de opción de *"salto-a-salto".*

En la figura 2.3 se muestra como son asignadas las cabeceras de expansión.

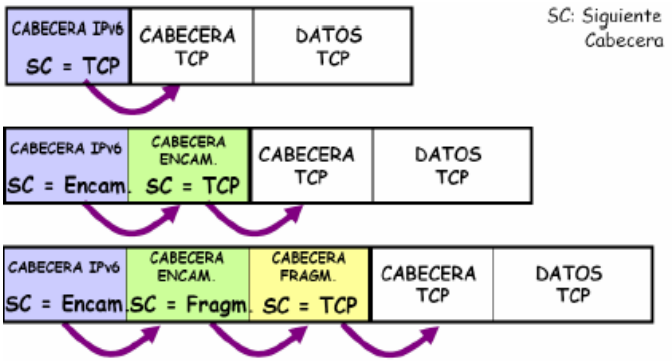


Fig. 2.3 Formato de la siguiente cabecera **[9]**

Las cabeceras opcionales de extensión que actualmente están definidas son las siguientes:

Características de Opciones de Salto a Salto *(hop-by-hop)*

Este tipo de cabecera almacena información que debe ser examinada en cada salto que da el paquete por los nodos. Su valor es de cero (0) ver figura 2.4.

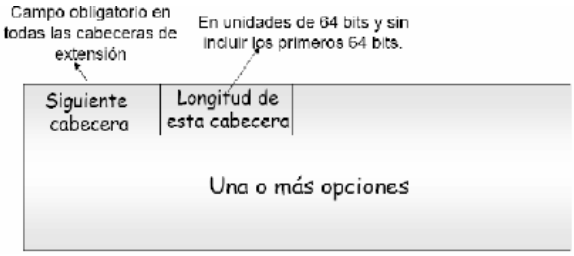


Fig. 2.4 Opciones de salto a salto **[9]**

Cabecera de Opciones para destinatario

La información que lleva esta cabecera será examinada solo en los nodos finales. Su valor es de sesenta (60)

Cabecera de Encaminamiento

Permite un encaminamiento fijándose en el origen, crea una lista en el origen de todos los routers por los que debe pasar el datagrama. Su valor es de (43).

Esta cabecera presenta algunas aplicaciones tales como: la selección de proveedores y la movilidad, en la figura 2.5 se muestra un ejemplo de cómo funciona esta cabecera.

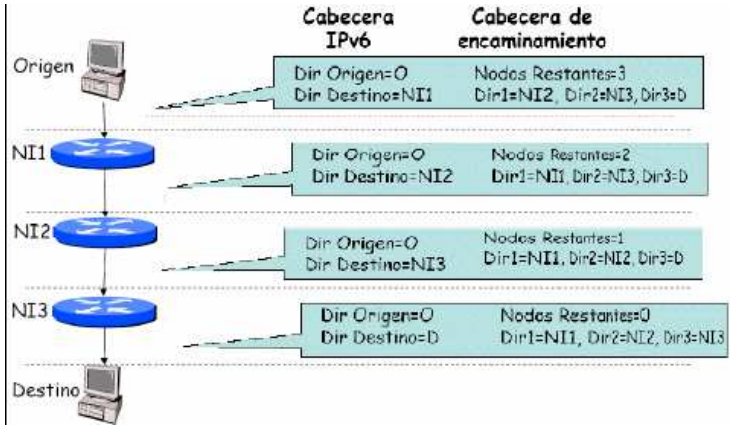


Fig. 2.5 Cabecera de Encaminamiento **[9]**

Cabecera de Fragmentación

Su objetivo es el de fragmentar y/o re-ensamblar los datos y esta función solo se la puede hacer cuando el paquete llega a su origen. El valor de esta cabecera es de (44) ver figura 2.6.

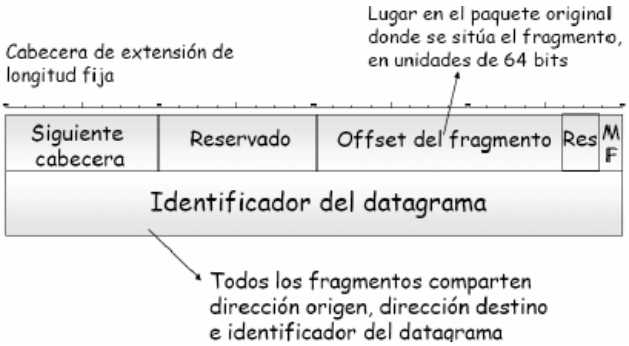


Fig. 2.6 Cabecera de Fragmentación **[9]**

Cabecera de autenticación/encriptado

Su objetivo es el de integrar mecanismos de seguridad y para esto puede utilizar firmas digitales y encriptación, tiene el valor de (50) para cuando sea una cabecera de expansión y de (51) cuando es cabecera de autenticación SC = 50 (ESP), SC = 51 (AH)

Existen de dos tipos de realizar estos mecanismos:

- ***Modo Transporte.-*** Asegura la carga de los datos en el datagrama. Se establece entre los nodos extremos de la red, (ver figura 2.7).

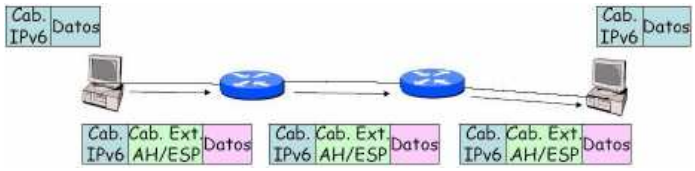


Fig. 2.7 Modo transporte **[9]**

- ***Modo Túnel.-*** Se asegura de que todo el datagrama túnel sea seguro en la red. Se establece entre los nodos intermedios de la red. Las direcciones origen y destino se modifican con la de los nodos intermedios que implementan IPSec, (ver figura 2.8).

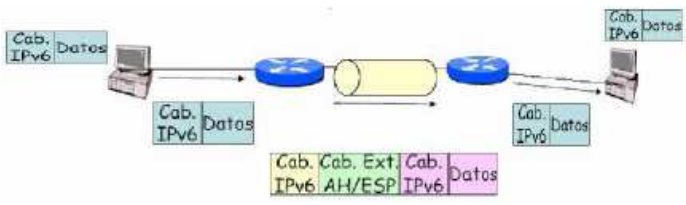


Fig. 2.8 Modo túnel **[9]**

Estas cabeceras opcionales de extensión son agregadas dependiendo de la aplicación a utilizar, aunque IPv6 tiene la facilidad de reconocer y agregar las cabeceras de extensión más adecuada.

Hop Limit *(Limite de saltos):* Tiene 8 bits con los cuales un paquete puede llegar hacer 255 saltos, y es similar al campo TTL de IPv4.

Source Address: *Dirección Origen,* de 16 bytes*.*

Destination Address: *Dirección Destino.*

2.3 DIRECCIONAMIENTO IPv6

Las direcciones IPv6 son de 128 bits (más de 103838 direcciones posibles).
Es posible asignar 1500 direcciones por m^2 teniendo en cuenta las pérdidas por asignación. Estas direcciones pueden ser asignadas a interfaces lógicas.
Una interfaz puede tener muchas direcciones como:

- Link-Local *(locales a subred)*
- Site-Local *(locales a organización)*
- Global *(una por organización)*

Se agregan nuevas direcciones:

- Unicast
- Multicast
- Anycast

2.3.1 REPRESENTACIÓN DE DIRECCIONES IPv6

La notación general que utiliza IPv6 par sus direcciones es:

X:X:X:X:X:X:X:X (X = 2 octetos en hex.)

Ejemplo:

fedc:ba98:7654:3210:fedc:ba98:7654:3210

Los ceros contiguos que existan en una dirección se pueden eliminar y ser sustituidos por (::).

FF01:0:0:0:0:0:0:45 = FF01::45

También existen direcciones compatibles con IPv4:

0:0:0:0:0:0:192.168.46.78 = ::192.168.46.78

Similar con IPv4 también existen tipos de direcciones reservadas, pero en este caso se los denomina prefijos para determinan el tipo de direcciones y se muestran en la tabla 2.1.

Tabla 2.1: Prefijos de direcciones **[10]**

Estado	Prefijo (en binario)	Fracción del Espacio
Reservado	0000 0000	1/256
No Asignado	0000 0001	1/256
Reservado para NSAP	0000 001	1/128
Reservado para IPX	0000 010	1/128
No Asignado	0000 011	1/128
No Asignado	0000 1	1/32
No Asignado	0001	1/16
Direcciones Unicast Globales Agregables	001	1/8
No Asignado	010	1/8
No Asignado	011	1/8
No Asignado	100	1/8
No Asignado	101	1/8
No Asignado	110	1/8
No Asignado	1110	1/16
No Asignado	1111 0	1/32
No Asignado	1111 10	1/64
No Asignado	1111 110	1/128
No Asignado	1111 1110 0	1/256

Direcciones Unicast Locales de Enlace	1111 1110 10	1/1024
Direcciones Unicast Locales de Sitio	1111 1110 11	1/1024
Direcciones Multicast	1111 1111	1/256

Ejemplo:

Dirección-IPv6/longitud-del-prefijo

21AB:0000:0000:CD40:0000:0000:0000:0000/60

21AB:0:0:CD40:123:4567:89AB:CDEF/60

2.3.2 CLASES/TIPO DE DIRECCIONES

Las direcciones IPv6 son identificadores de 128 bits para interfaces, conjuntos de interfaces y son similares al tipo de direcciones existentes en IPv4. Dichas direcciones se clasifican en tres tipos de direcciones:

2.3.2.1 Direcciones Unicast.

Un paquete que es enviado a una dirección unicast es entregado *sólo* a la interfaz identificada con dicha dirección (ver figura 2.9).

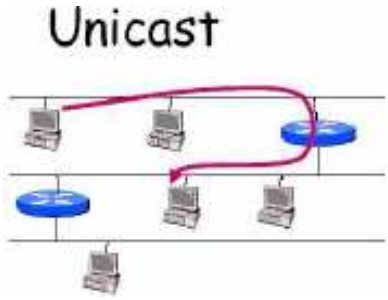


Fig. 2.9 Direcciones Unicast **[9]**

Un host más sofisticado, sería capaz de conocer el prefijo de la subred del enlace al que esta conectado.

El "*identificador de interfaz*" se emplea, para identificar interfaces en un enlace, y deben de ser únicos en dicho enlace, además puede ser utilizado en múltiples interfaces del mismo nodo.

Dentro de las direcciones unicast se han definido dos tipos de direcciones unicast de uso local:

- Local de Enlace *(Link-Local)*
- Local de Sitio *(Site-Local)*

2.3.2.1.1 Direcciones Unicast Globales Agregables:

Actualmente ya se emplea este tipo de direcciones, las cuales se basan en la agregación por parte de los proveedores del Internet, y los mecanismos adoptados para IPv6. Además, se ha incorporado un mecanismo de agregación la cual se basa en “intercambios”.

La combinación de estos tipos de agregación de direcciones es la que permite un encaminamiento mucho más eficiente, dando dos opciones de conectividad. La cual se trata de una organización basada en tres niveles:

- ***Topología Pública:*** es un conjunto de proveedores e “intercambiadores” que proporcionan servicios públicos de Internet.
- ***Topología de Sitio:*** son redes de organizaciones que no proporcionan servicios públicos a nodos fuera de su propio “sitio”.
- ***Identificador de Interfaz:*** identifican interfaces de enlaces.

Una organización puede estar suscrita a múltiples proveedores (multi-homing o multi-localización), a través de un intercambiador, sin la necesidad de tener prefijos de direcciones de cada uno de los proveedores.

Estructura de las Direcciones Unicast Globales Agregables, (ver figura 2.10)

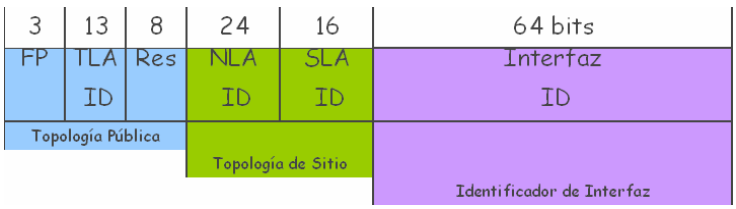


Fig. 2.10 Formato de Direcciones Unicast Globales

FP.- Formato del Prefijo (001)

TLA ID.- Top-Level Aggregation Identifier

RESV.- Reservado (sirve para ampliar TLA o NLA, por el momento contiene ceros)

NLA ID.- Next-Level Aggregation Identifier

SLA ID.- Site-Level Aggregation Identifier

ID.- Interface Identifier

2.3.2.1.2 Direcciones Unicast Locales de Enlace:

Estas direcciones han sido diseñadas para direccionar un único enlace con el propósito de auto-configuración *(mediante identificadores de interfaz)*, descubrimiento del vecindario, o cuando no hayan routers.

En la figura 2.11 se muestra el formato que tratan estas direcciones:

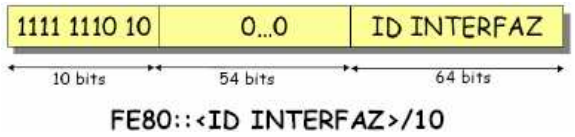


Fig. 2.11 Formato de Direcciones Unicast Locales de Enlace **[9]**

2.3.2.1.3 Direcciones Unicast Locales de Sitio

Nos permiten direccionar dentro de un sitio local u organización, sin la necesidad de utilizar un prefijo global. Son configuradas mediante un identificador de subred, es de 16 bits. Este tipo de direcciones son utilizadas por organizaciones privadas que no están conectadas al Internet, solo sirven para intercambiar información dentro de la organización.

El formato que trata estas direcciones es el siguiente, (ver figura 2.12):

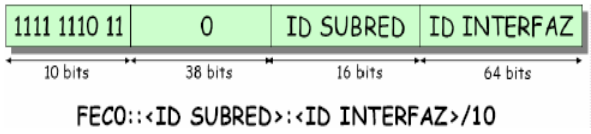


Fig. 2.12 Formato de Direcciones Unicast Locales de Sitio **[9]**

2.3.2.2 Direcciones Multicast.

Un paquete que es enviado a una dirección multicast es entregado a *todas* las interfaces indicadas por dicha dirección. Es decir de uno host a todos los host pertenecientes a un grupo ya que este host puede pertenecer a varios grupos (ver figura 2.13).

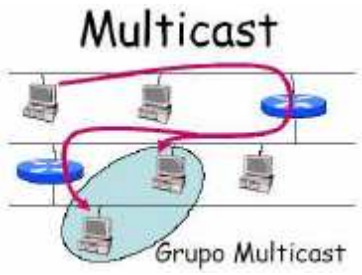


Fig. 2.13 Direcciones Multicast **[9]**

Las direcciones multicast tienen el siguiente formato, ver figura 2.14:

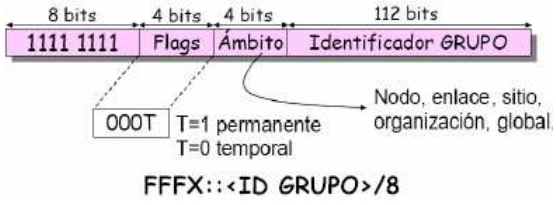


Fig. 2.14 Formato de Direcciones Multicast **[9]**

Dentro del campo flags se encuentra un bit **T** el cual tiene dos valores 0=dirección multicast permanente, y 1=dirección multicast temporal.

Por el momento el campo ámbito tiene el valor de cero ya que están reservados para actualizaciones futuras. Además este campo tienen los siguientes significados, ver tabla 2.2:

Tabla 2.2: Bits para el campo ámbito. **[10]**

0	Reservado
1	Ámbito Local de Nodo
2	Ámbito Local de Enlace
3	No Asignado
4	No Asignado
5	Ámbito Local de Sitio
6	No Asignado
7	No Asignado
8	Ámbito Local de Organización
9	No Asignado
A	No Asignado
B	No Asignado
C	No Asignado
D	No Asignado
E	Ámbito Global
F	Reservado

El campo *"Identificador de Grupo",* identifica, el grupo de multicast concreto al que nos referimos, bien este sea permanente o temporal, dentro de un determinado ámbito.

Las direcciones multicast no deben ser usadas como dirección fuente en un paquete IPv6, ni aparecer en ninguna cabecera de encaminado.

Las principales direcciones multicast reservadas son las incluidas en le rango FF0X:0:0:0:0:0:0:0.
Algunos ejemplos útiles de direcciones multicast, según su ámbito, serían:

- FF01:0:0:0:0:0:0:1 – Todos los nodos (ámbito local)
- FF02:0:0:0:0:0:0:1 – Todos los nodos (ámbito de enlace)

- FF01:0:0:0:0:0:0:2 – Todos los routers (ámbito local)
- FF02:0:0:0:0:0:0:2 – Todos los routers (ámbito de enlace)
- FF05:0:0:0:0:0:0:2 – Todos los routers (ámbito de sitio)

La dirección FF02:0:0:0:0:1:FFXX:XXXX, denominada "*Solicited-Node Address",* o dirección de nodo solicitada, permite calcular la dirección multicast a partir de la unicast o anycast de un determinado nodo. Para ello, se sustituyen los 24 bits de menor peso ("x") por los mismos bits de la dirección original. **[10]**

2.3.2.3 Direcciones Anycast.

Un paquete que se envía a una dirección anycast es entregado a *una* de las interfaces indicadas con dicha dirección. Nos permite crear, por ejemplo, ámbitos de redundancia, de forma que varias máquinas puedan ocuparse del mismo tráfico según una secuencia determinada (ver figura 2.15).

En esta versión del protocolo IP *No existen direcciones broadcast.*

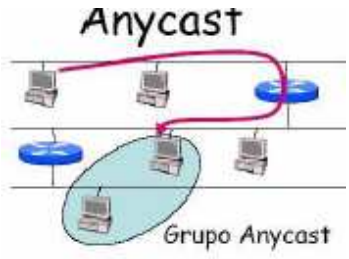


Fig. 2.15 Direcciones Anycast **[9]**

Estas direcciones anycast tienen el mismo rango de direcciones que las direcciones unicast.

Cuando una dirección unicast es asignada a más de una interfaz, convirtiéndose en una dirección anycast, los nodos a los que dicha dirección ha sido asignada, deben ser explícitamente configurados para que reconozcan que se trata de una dirección anycast. **[10]**

Para cada subred se ha definido una dirección anycast única denominada *(subnet-router anycast address*), ver figura 2.16. En este caso el indicador de interfaz es igual a cero:

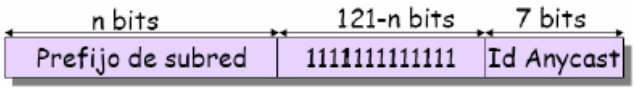


Fig. 2.16 Direcciones Anycast únicas **[9]**

La asignación de la dirección reservada de anycast de subred depende del tipo de direcciones IPv6 que sean usadas dentro de la subred.

2.3.2.4 Direcciones Especiales.

En IPv6 también se han definido direcciones para usos especiales como:

- ✓ *Direcciones de Loopback*, sirven para verificar al protocolo y cuya representación es (::1).
- ✓ *Direcciones sin especificación*, es decir que no hay direcciones asignadas, su representación es (::).
- ✓ *Túneles de IPv6 sobre IPv4*, permiten la retransmisión del tráfico IPv6 sirve la infraestructura de IPv4 y se la representa *(::<dirección IPv4>).*
- ✓ *Representación automática de direcciones IPv4 sobre IPv6,* permite a los nodos trabajar con redes IPv6 aunque estos solo soporten IPv4 también se las conoce como *"direcciones IPv6 mapeadas desde IPv4"* y se las representa de la siguiente manera: *(::FFFF:<dirección IPv4>).*

2.4 CONFIGURACIÓN CON IPv6

Actualmente IPv6 puede ser configurado en la mayoría de los sistemas operativos como Linux y principalmente en las últimas versiones de Solaris y algunas de las versiones de Windows y en varios dispositivos de interconexión de red.

Los sistemas operativos de las *MacOS X* tienen un soporte transparente del usuario y tiene una interfaz gráfica para realizar la configuración automática o manual

Si embargo muchos dispositivos con infraestructura de redes no tienen el soporte adecuado para las configuraciones IPv6, tales como:

- Firewalls.
- VPN Servers.
- AP *(Puntos de Acceso Inalámbrico)*.
- Switches.

Aunque IPv6 trabaja sobre varios sistemas operativos, en el presente proyecto solo se va a hacer referencia a la configuración en el sistema operativo Windows XP y en el dispositivo de red Router Cisco 2600.

2.4.1 IPv6 EN WINDOWS XP

Todas las versiones actuales de Windows XP, incluyen la versión 6 del protocolo IP preinstalado, y simplemente hay que habilitarlo.

Para lo cual es necesario ejecutar, el siguiente comando: *prompt>ipv6 install*, luego aparecerá un mensaje indicando que se ha instalado correctamente (ver figura 2.17)

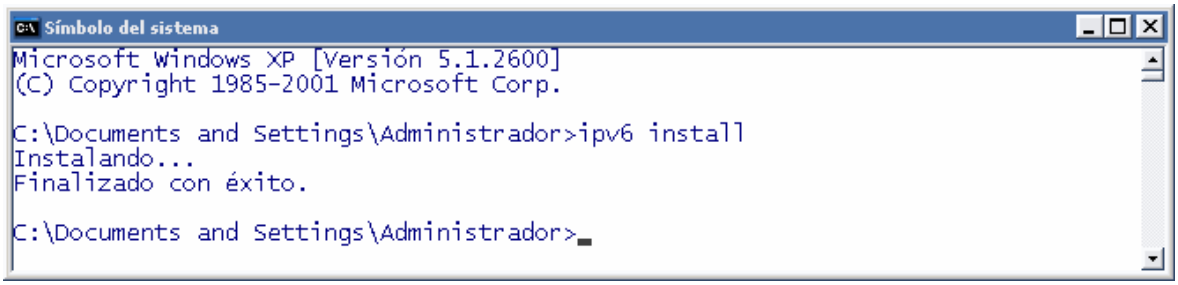


Fig. 2.17 Instalación de IPv6

2.4.2 IPv6 EN RUOTERS CISCO

IPv6 puede configurarse en ruteadores cisco dependiendo de su capacidad para soportar este tipo de configuración, ya que esto no solo depende del hardware del dispositivo sino también del software de los mismos; actualmente las versiones de los router cisco 2600 con software mayores a 12.0T son capaces de soportar la configuración de IPv6.

A continuación se nombra varias versiones de ruteadores cisco: c1000, c1005, c1600, c2500, c2600, c3620, c3660, c4000, c4500, c5200, c7200, c5rsm,

2.4.3 AUTOCONFIGURACIÓN

La autoconfiguración es el conjunto de pasos por los cuales un host decide como configurar sus interfaces en IPv6. Este mecanismo permite afirmar que IPv6 es *"Plug & Play"*.

Este proceso incluye la creación de una dirección de enlace local, verificar que esta dirección no esté duplicada en dicho enlace y la determinación de la información que ha de ser autoconfigurada (direcciones y otra información).
Las direcciones pueden ser obtenidas de forma totalmente manual, mediante DHCPv6 (configuración stateful o predeterminada), o de forma automática (configuración stateless o descubrimiento automático, sin intervención).

2.4.3.1 Autoconfiguración Stateless

La autoconfiguración ***"stateless"*** (sin intervención), no requiere de ninguna configuración manual en el host, es una configuración mínima en los routers, y no requiere de servidores adicionales. Permite que un host sea capaz de generar su propia dirección mediante una combinación de información local y de información anunciada por los routers. Los routers anuncian los prefijos que indica la subred asociada con el enlace, mientras el host genera un identificador de interfaz, el cual indica de forma única la interfaz en la subred. La dirección es compuesta por la combinación de ambos campos. En ausencia de router, el host sólo puede generar la dirección de enlace local, aunque esto es suficiente para permitir la comunicación entre nodos que están conectados al mismo enlace.

2.4.3.1.1 Pasos para la Autoconfiguración

a) Se genera la dirección de enlace local.
b) Verificar que dicha dirección no este duplicada.
c) Si esta duplicada, la autoconfiguración se detiene, y se requiere un procedimiento manual.

d) Si no esta duplicada, la conectividad a nivel IP se ha logrado.
e) Si se trata de un host, se interroga a los posibles routers para indicar al host lo que debe de hacer a continuación.
f) Si no hay routers, se invoca el procedimiento de autoconfiguración stateful.
g) Si hay routers, estos contestarán indicando fundamentalmente, como obtener las direcciones si se ha de utilizar el mecanismo stateful, u otra información, como tiempos de vida, etc. **[10]**

Para obtener el identificador de interfaz Ethernet, para la autoconfiguración stateless, nos basamos en la dirección MAC propia de 48 bits ya que las direcciones MAC configuradas manualmente o por software no deberían ser usadas para encontrar el identificador de interfaz. Tomando los 3 primeros bytes de mayor orden, y les agregamos el valor de FFFE (hexadecimal), y a continuación, el resto de los bytes de la dirección MAC. El identificador así formado se denomina identificador EUI-64 *(Identificador Global de 64 bits);* como se muestra en la figura 2.18.

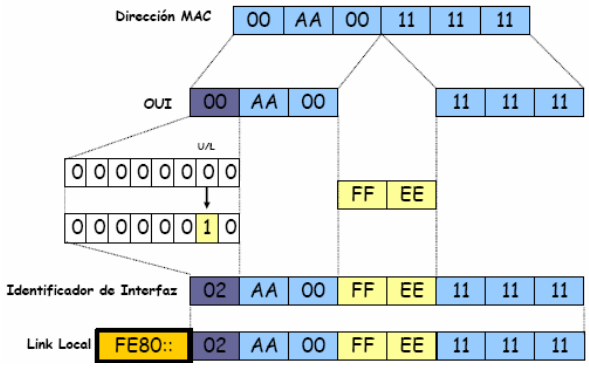


Fig. 2.18 Generación de la dirección de enlace local **[9]**

El identificador de interfaz se obtiene, partiendo del EUI-64, complementando el bit U/L *(Universal/Local).* El bit U/L es el siguiente al de menor valor del primer byte del EUI-64 (el 2^{do} bit por la derecha, el 2^{do} bit de menor peso).
Al complementar este bit, por lo general cambiará su valor de 0 a 1; dado que se espera que la dirección MAC sea universalmente única, el U/L tendrá un valor 0, y por lo tanto se convertirá en 1 en el identificador de interfaz IPv6.

Para mapear direcciones unicast IPv6 sobre Ethernet, se utiliza los mecanismos ND para solicitud de vecinos.
Para mapear direcciones multicast IPv6 sobre Ethernet, se emplean los 4 últimos bytes de la dirección IPv6, a los que se antepone 3333. **[10]**

2.4.3.2 Autoconfiguración Stateful

En esta autoconfiguración ***"stateful"*** (predeterminada), el host obtiene la dirección de la interfaz y la información de parámetros de configuración desde un servidor. Los servidores mantienen una base de datos con las direcciones que han sido asignadas a cada host mediante DHCPv6.

Las autoconfiguraciones (stateless y stateful), se complementan.
Un host puede usar la autoconfiguración stateless, para generar su propia dirección, y obtener el resto de parámetros mediante la autoconfiguración predeterminada (stateful).

El mecanismo de autoconfiguración sin intervención se emplea sólo para asegurarse de que la dirección es única y enrutable sin importar que dirección ha sido asignada al host.
Al contrario, el mecanismo de autoconfiguración predeterminada, asegura que cada host tiene asignada una determinada dirección, la cual es asignada manualmente.

A las direcciones se les asocia un tiempo de vida, que indican durante cuanto tiempo esta dirección va ha estar vinculada a una determinada interfaz. Cuando el tiempo de vida de la dirección expira, la vinculación se invalida y la dirección puede ser asignada a otra interfaz en cualquier punto de Internet.

Una dirección pasa a través de dos fases diferentes mientras está asignada una interfaz. Inicialmente, una dirección es *"preferred" (*predefinida*)*, lo cual significa que su uso es arbitrario y no está restringido. Posteriormente, la dirección es *"deprecated" (*desaprobada*)* en anticipación a que el vínculo con su interfaz actual va a ser anulado, cuando una dirección se encuentra en este estado solo puede

ser usada por aquellas aplicaciones ya utilizadas y a las que les es muy difícil cambiar a otra dirección.

Para asegurarse de que todas las direcciones configuradas son únicas, en un determinado enlace, los nodos ejecutan un algoritmo de detección de direcciones duplicadas, antes de que estas direcciones sean asignadas a una determinada interfaz. Este algoritmo es ejecutado para todas las direcciones, independientemente de que hayan sido obtenidas mediante autoconfiguración stateless o stateful. **[10]**

La autoconfiguración esta diseñada solo para los host, y no para routers; aunque eso no implica que una parte de la configuración de los routers también pueda ser realizada automáticamente. Además, los routers también tienen que aprobar el algoritmo de detección de direcciones duplicadas.

2.4.4 DHCP

DHCP para IPv6 es un protocolo UDP cliente/servidor, diseñado para reducir el coste de gestión de nodos IPv6 en entornos donde los administradores precisan un control sobre la asignación de los recursos de la red, superior al facilitados por el mecanismo de configuración stateless.
Además, DHCP ha sido diseñado para ser fácilmente extensibles con nuevos parámetros de configuración, a través de extensiones que incorporan esta nueva información.

Los objetivos de DHCPv6 son:

- Es un mecanismo, más no una política. Las políticas son establecidas por los administradores de la red.
- Es compatible, con el mecanismo de autoconfiguración stateless.
- No requiere configuración manual de parámetros para la red en los clientes DHCP, excepto en casos donde dicha configuración es requerida debido a las diferentes medidas de seguridad.
- No es necesario requerir un servidor para cada enlace, dado que debe funcionar a través de relés del servidor DHCP.

- Coexiste con nodos configurados estáticamente, así como con implementaciones existentes en la red.
- Los clientes DHCP no necesitan en enlaces con routers IPv6.
- Los clientes DHCP tienen habilidad para renumerar la red.
- Un cliente DHCP puede hacer múltiples y diferentes peticiones de parámetros de configuración, de uno a varios servidores DHCP simultáneamente. DHCP proporciona suficiente información para permitir a los servidores DHCP el seguimiento del estado de configuración de los clientes.
- DHCP incorpora mecanismos apropiados para realizar control de tiempo y retransmisiones para operar eficazmente en los entornos de red con una alta latencia y un reducido ancho de banda.

La diferencia entre DHCPv4 y DHCPv6, se basan en el soporte del formato del direccionamiento y autoconfiguración IPv6; y son las siguientes:

- La dirección de enlace local permite a un host obtener una dirección en el momento en el arranca, por lo que todos los clientes tienen una dirección IP para localizar un servidor que se encuentra en el mismo enlace.
- Los indicadores de compatibilidad y broadcast ya no existen.
- La autoconfiguración stateful se ha de integrar con la configuración stateless, soportando la detección de direcciones duplicadas y los dos tiempos de vida de los paquetes IPv6 para facilitar la renumeración automática de direcciones.
- Son capaces de soportar múltiples direcciones por cada interfaz.
- Varias opciones de DHCPv4 ya no son precisas, debido a que los parámetros de configuración se obtiene a través de ND o del protocolo de localización de servidores.

Debido a estas diferencias, DHCPv6 puede soportan las siguientes funciones:

- Configuración de actualizaciones dinámicas en el servidor DNS.
- Desaprobación de direcciones, para realizar renumeración dinámica.
- Relés preconfigurados con direcciones de servidores, o mediante multicast.

- Autenticación.
- Los clientes pueden solicitar múltiples direcciones IP.
- Las direcciones pueden ser solicitadas nuevamente mediante el mensaje de *"iniciar-reconfiguración.*
- Integración entre autoconfiguración de direcciones stateless y stateful.
- Permitir relés para localizar servidores fuera del enlace.

Funcionamiento del servidor DCHP:

- Basado en modelo cliente/servidor sobre UDP:
    - Los servidores envían en el puerto 546.
    - Los clientes envían en el puerto 547.
- Se intercambian 6 tipos de mensajes:
    - *DHCPv6 Solicit*: Enviado por el cliente a la dirección. Todos Agentes DCHP (FF02::C) para localizar servidores DHCP.
    - *DHCPv6 Advertise:* Enviado por unicast al cliente que envió Solicit.
    - *DHCPv6 Request*: Enviado por el cliente a un servidor para solicitar los parámetros de red.
    - *DHCPv6 Reply:* Respuesta de un servidor a un Request con los parámetros de red.
    - *DHCPv6 Release*: El cliente libera algunos parámetros de red que pueden ser reutilizados por el servidor.
    - *DHCPv6 Reconfigure*: Enviado por el servidor a un cliente para indicarle que se debe reconfigurar. El cliente debe enviar de nuevo un Request.

2.4.5 DNS

Al referirnos a direcciones IP nos referimos a la localización de un host mediante literales URL. Para que este mecanismo funcione, existe un protocolo denominado "Domain Name System*" (Sistema de Nombres de Dominio)*.

Este mecanismo, fue definido inicialmente para IPv4, el mismo que después fue actualizado, el cual incluía un nuevo tipo de riesgo para almacenar las direcciones IPv6, y definiciones actualizadas las que devuelven direcciones de Internet como parte de procesos de secciones adicionales.

El problema del sistema DNS existente es comprensible. Ya que al hacer una consulta, las aplicaciones asumen que se les devolverá una dirección de 32 bits pero para resolverlo hay que definir algunas extensiones:

- Un nuevo tipo de registro para mapear un nombre de dominio con una dirección IPv6: Es el registro AAAA (con un valor decimal de tipo 28).
- Un nuevo dominio para IPv6 es IP6.INT. Su representación se realiza en orden inverso de la dirección, separando por puntos los valores (hexadecimal), seguidos del dominio IP6.INT. Por ejemplo si se da la dirección 4321:0:1:2:3:4:567:89ab, en su proceso inverso sería b.a.9.8.7.6.5.0.4.0.0.0.3.0.0.0.2.0.0.0.1.0.0.0.0.0.0.0.1.2.3.4.IP6.INT.
- Redefinición de las consultas existentes, que localizan direcciones IPv4, para que puedan también procesar direcciones IPv6.

2.5 MECANISMOS DE TRANSICION IPv4 - IPV6

La transición hacia el protocolo IPv6 es inminente, por lo que existen algunos mecanismos llamados también *Técnicas de Interoperación* de IPv4 a IPv6. Los mecanismos de transición se dividen en tres grupos:

- ✓ *Dual Stack*
- ✓ *Traducción*
- ✓ *Túneles*

Dual Stack.- El mecanismo de transición dual stack hace uso de las pilas de protocolos de cada uno de ellos, tanto en los host como en los routers; es decir, que un host puede tener configurado los dos protocolo (IPv4 e IPv6) y cuando hace uso de la dirección IPv4 accede a su respectiva pila, de la misma manera cuando se usa la dirección IPv6; en lo correspondiente a los ruteadores, cada protocolo crea y administra su propia tabla de enrutamiento para poder conectarse con otro host o hacia el Internet.

Traducción.- Este mecanismo de transición es similar al realizado por el proceso NAT, donde se modifican las cabeceras de los paquetes. La traducción es necesaria cuando un nodo solo IPv4 intenta comunicar con un nodo solo IPv6. Este mecanismo no es recomendable.

Túneles.- Esta técnica permite la comunicación de redes que tienen instalados diferentes protocolos. Para este escenario, esta técnica consiste en encapsular los paquetes IPv6 dentro de paquetes IPv4. El proceso inverso se realiza en la maquina destino, que recibe el paquete IPv6 (ver figura 2.19).

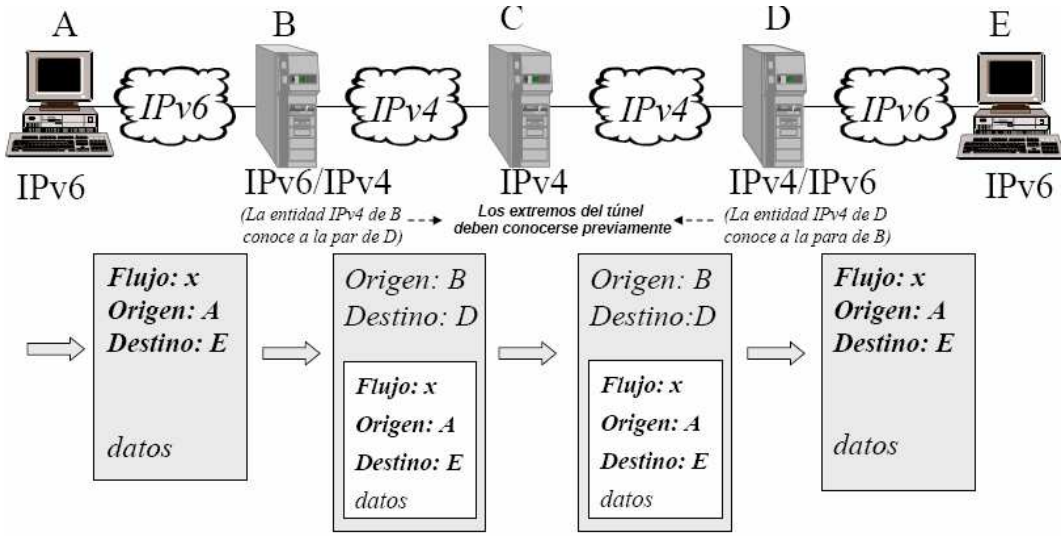


Fig. 2.19 Proceso de Tunelización **[14]**

Túneles 6to4.- Permiten la comunicación de redes IPv6 a través de redes IPv4, estos túneles son configurados de forma automática con ip pública y para realizar pruebas no se necesita de un proveedor de servicios.

Túneles 6over4.- Permite la configuración de túneles de tipo *host-to-host, host-to-router, router-to-host;* realiza neighbor discovery con la red IPv4 con multicast.

2.6 IPV6 SOBRE IEEE 802.3

Aunque ya se han definido protocolos para permitir el uso de IPv6 sobre cualquier tipo de red o topología (*Token Ring, FDDI, ATM, PPP);* en el presente proyecto centraremos este apartado para las redes Ethernet, *(*con el protocolo *CSMA/CD y con tecnologías full-duplex basadas en IEEE 802.3),* (ver figura 2.19). Los paquetes IPv6 son transmitidos sobre tramas Ethernet normalizadas.

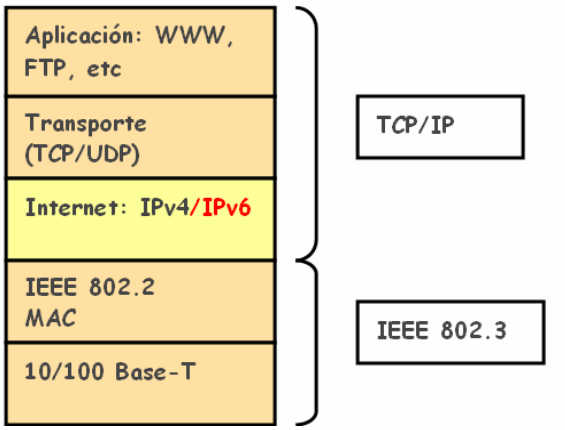


Fig. 2.20 TCP/IP sobre IEEE 802.3

El campo de datos que contiene la cabecera IPv6 seguida por los propios datos, y probablemente algunos bytes para relleno, dan lugar a que se alcance el tamaño mínimo de la trama para el enlace Ethernet.

El tamaño máximo de la unidad de transmisión (MTU), para IPv6 sobre redes Ethernet, es de 1.500 bytes. El cual puede ser reducido, manual o automáticamente (mediante los mensajes de anunciación de routers).

2.7 COMPARACIÓN ENTRE EL PROTOCOLO IPV4 E IPV6

Una de la comparación más importante es la equivalencia entre las direcciones IPv4 e iPv6:

Refiriéndose a las direcciones:

- Las direcciones IPv4 son de 32 bits, pero IPv6 tiene direcciones de 128 bits.
- IPv4 especifica la clase de la dirección IP, mientras que en IPv6 no existe direcciones por clase.
- La notación de las direcciones IPv4 son en base 10 *(decimal)*, y en IPv6 su notación es en base 16 *(hexadecimal)*.
- En IPv4 existen direcciones de broadcast, pero en IPv6 no.
- La dirección sin especificación de IPv4 es la 0.0.0.0, mientras que en IPv6 es la dirección ::.
- La dirección de loop back en IPv4 es 127.0.0.1 y en IPv6 es la dirección ::1.
- En IPv4 las direcciones son privadas y públicas, mientras que en IPv6 son direcciones globales y locales.

- En IPv4 se utilizan las máscaras de las direcciones, pero en IPv6 son los prefijos de longitud única.
- Una única interfaz puede tener varias direcciones IPv6 de cualquier tipo o ámbito.
- El dominio que presenta IPv6 es el registro AAAA.

Refiriéndose al formato de las cabeceras:

- Con respecto al formato de la cabecera esta ha sido modificada en algunos de sus campos y otros eliminados, la cabecera IPv4 tiene 13 campos y en la cabecera IPv6 solo quedaron 8 campos.
- En la cabecera IPv4 esta el campo tipo de servicio que en IPv6 ha sido llamado tipo de tráfico.
- El campo conocido en la cabecera IPv4 como tiempo de vida en la cabecera IPv6 se lo va a conocer como limites de salto de los paquetes.
- En el campo protocolo de la cabecera IPv4, en la cabecera IPv6 se lo mantiene pero con otra función la cual es muy importante ya que es la extensión de la cabecera del paquete.
- En el campo de opciones estas cabeceras de extensión son removidas.

Refiriéndose al tipo de mensajes ICMP:

- Los mensajes ICMPv4 e ICMPv6 son similares por que ambos presentan mensajes ya sea de error o informativos, pero como IPv6 utiliza cabeceras de extensión para lo cual ICMPv6 tiene el valor de (58).
- En IPv4 estos mensajes son redireccionados pero en IPv6 son redireccionados pero con mensajes adicionales como el de descubrimientos de vecinos.

CAPITULO 3: IMPLEMENTACION DEL PROTOCOLO IPV6 EN EL LABORATORIO

3.1 ANÁLISIS DE LA RED DEL LABORATORIO DE INFORMACIÓN DE LA CARRERA DE ANÁLISIS DE SISTEMAS INFORMÁTICOS

El laboratorio LTI cuenta con equipos básicos para la utilización de sus estudiantes, brindándoles una interconexión únicamente de datos y el acceso al Internet para consultas académicas. La red del LTI es tratada como una subred en el contexto de la Polired y esta estructurada sobre la base de la tecnología IEEE 802.3; por ser una subred de a Polired las direcciones IPv4 con las cuales trabaja son asignadas dinámicamente por el servidor DHCP de la Polired, el cual esta ubicado físicamente en la **UGI** (*Unidad de Gestión de Información).*

3.1.1 ESTRUCTURA FÍSICA DE LA RED

Los hosts de la red LTI están distribuidos adecuadamente en cuatro salas contiguas cono se muestra en la figura 3.1.

Sala de Servidores.- En esta sala se encuentran instalados los servidores del LTI.

Sala Uno.- En esta sala se encuentran instalados 18 hosts de la red conectados a un switch.

Sala Dos.- En esta sala se encuentran instalados 16 hosts de la red conectados a un switch.

Sala Tres.- En esta sala se encuentran instalados 6 hosts de la red conectados a un switch, los hosts que se encuentran en esta sala son utilizados únicamente para realizar las correspondientes prácticas de los proyectos de titulación.

Esta distribución física no implica que la red LTI haya sido dividida en subredes, pero si corresponde a requerimientos académicos de la carrera de ASI.

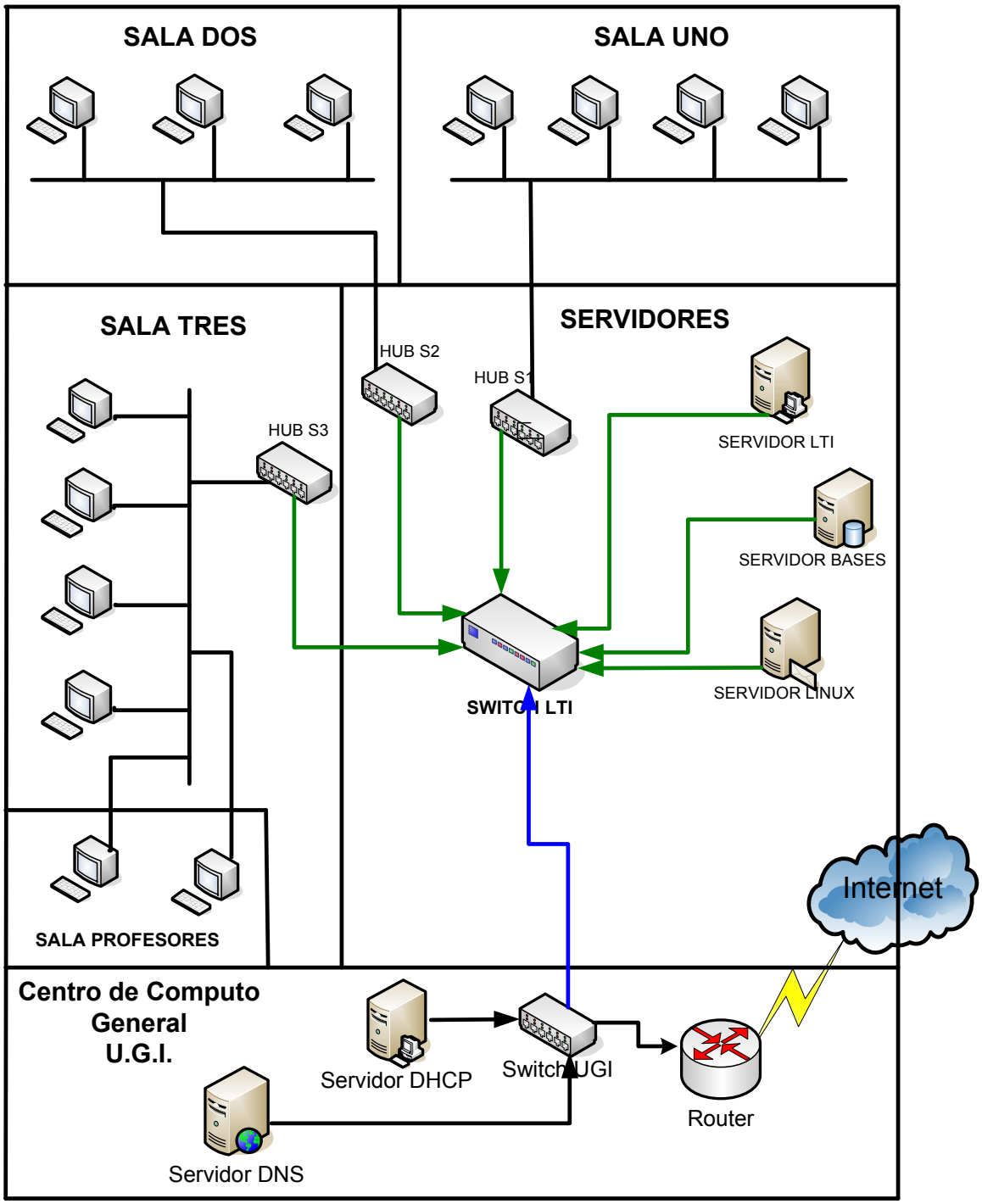


Fig. 3.1 Red LTI

3.1.2 COMPONENTES FISICOS DE LA RED

Los componentes físicos se muestran en la tabla 3.1 en la cual se describe las características generales de los hosts que forman parte de la red LTI.

Tabla 3.1: Componentes Físicos del LTI.

Cantidad	Dispositivo	Estado	Características
1	Switch (capa 2)	Activo	➢ Cisco System ➢ Serie: Catalyst 1900 ➢ Puertos: 24 puertos de 10 Mbps
3	Hub (capa 1)	Activo	➢ 3Com ➢ Puertos: 24 puertos 10/100 base Line/Sup
4	Servidor	Activo	Pentium III de 750 Mhz, con discos Scsi de 40 Gb, memoria RAM de 256.
42	PCs	Activo	➢ Pentium IV de 3.2Ghz con disco de 120 Gb, 512 de memoria RAM ➢ Pentium III de 750Mhz con disco de 40 Gb; y 128 de memoria RAM ➢ Celeron de 2.5Ghz con discos de 120 GB, 256 de memoria RAM
1	Firewall	Activo	➢ Fortinet ➢ Serie: FortiGate_60

3.1.3 COMPONENTES LÓGICOS DE LA RED

En la tabla 3.2 se detallan las plataformas de software con las que trabajan las máquinas existentes en el LTI.

Tabla 3.2: Software del LTI.

Plataforma	Versión
Windows	➢ Windows XP ➢ Windows Advance Server 2003
Linux	➢ Centos ➢ Ubuntu ➢ Mandriva

3.1.4 CONFIGURACIÓN LÓGICA ACTUAL DE LA RED LTI (IPV4)

La configuración lógica se refiere a la asignación de las direcciones IP a las interfaces de los diferentes componentes de la red para la comunicación entre ellos. Las direcciones son asignadas por el servidor DHCP de la UGI, teniendo en cuenta que es una asignación dinámica

En la figura 3.2 se muestra la configuración lógica del esquema de la red LTI.

Formas de Configuración del Protocolo IPv4

El protocolo IPv4 tiene cuatro formas de configuración las cuales son:

- Configuración Automática
- Configuración Dinámica
- Configuración Alternativa
- Configuración Manual

Nota: En el anexo 2 se describen los pasos para realizar la configuración respectiva para cada una de las formas de configuración del protocolo.

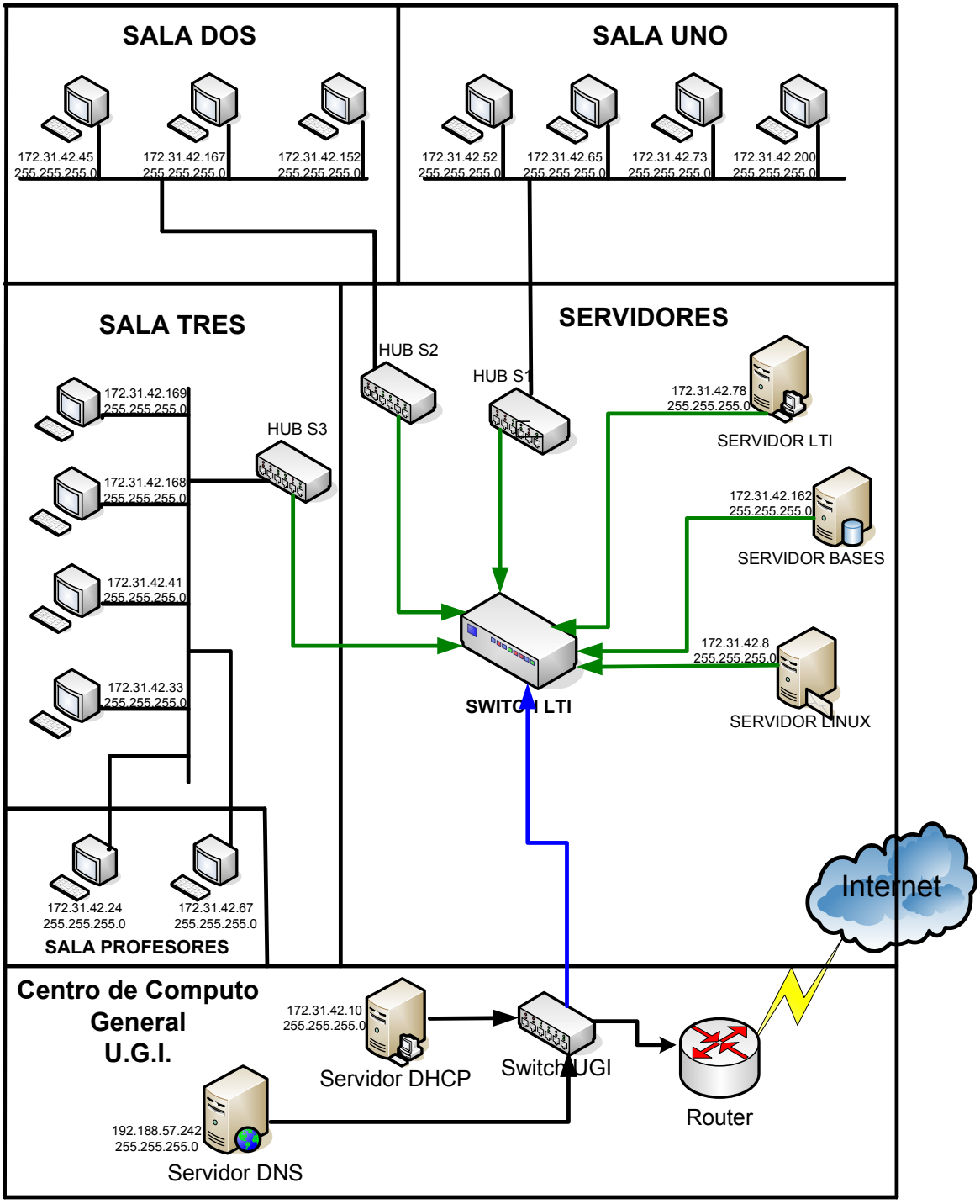


Fig. 3.2 Asignación de Direcciones IPv4

3.1.5 SEGURIDAD EN LA RED LTI

Para completar con la lista de componentes utilizados en la red del LTI, tenemos que mencionar al Firewall *(Fortinet)*, el cual es muy importante para resguardar la red ya que evita que las estaciones de trabajo sean perjudicadas por los virus existentes en el Internet; uno de los servicios de este componente es el Protection

Profile en el que se configura la administración de seguridades en la red como la filtración de URLs, y mediante el servicio Intruders Protection detecta la presencia de Virus. En la figura 3.3 se presenta el esquema de red en el cual ya se encuentra integrado el firewall.

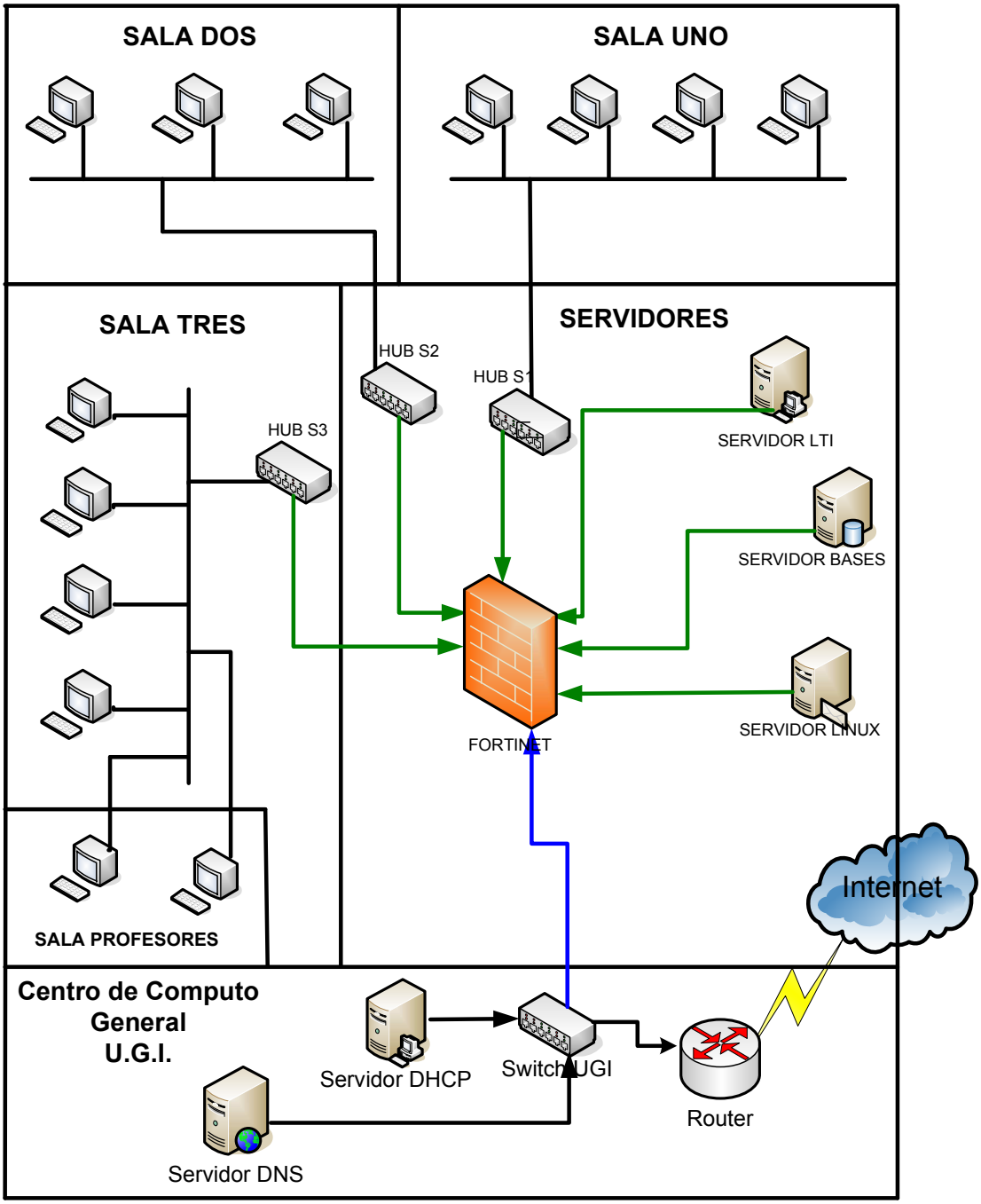


Fig. 3.3 Seguridad en el LTI

Este componente también presta un servicio muy similar al de un servidor DHCP ya que facilita una dirección IP a cada uno los host.

3.1.6 SERVICIOS DE LA RED

Actualmente la red únicamente cuenta con el servicio de Autentificación de Active Directory.

Active Directory es una implementación de los protocolos de nombres el cual funciona bajo la plataforma de Windows. Es un servicio que almacena información acerca de los objetos que se encuentran dentro de una red y esta información es puesta a disposición de los administradores de la red. Este servidor es ayudado para la administración de la subred utilizando el Firewall (*Fortinet*) como soporte de seguridad.

3.1.7 CONFIGURACIÓN LÓGICA DE LA RED UTILIZANDO EL PROTOCOLO IPv6

El protocolo IPv6 puede ser configurado mediante tres formas:

- Autoconfiguración sin Estado *(Stateless Configuration)*
    - Asignación de direcciones *link-local*
    - Anuncio de Prefijos
- Autoconfiguración con Estado *(Stateful Configuration)*
    - DHCPv6
- Configuración Manual

Para efecto de demostración de las diferentes formas de configuración del protocolo IPv6, se utiliza el prototipo de red mostrado en la figura 3.4. Adicionalmente, en la sección del presente proyecto se realiza la configuración lógica de la red del LTI.

A continuación se describe estas formas de configuración.

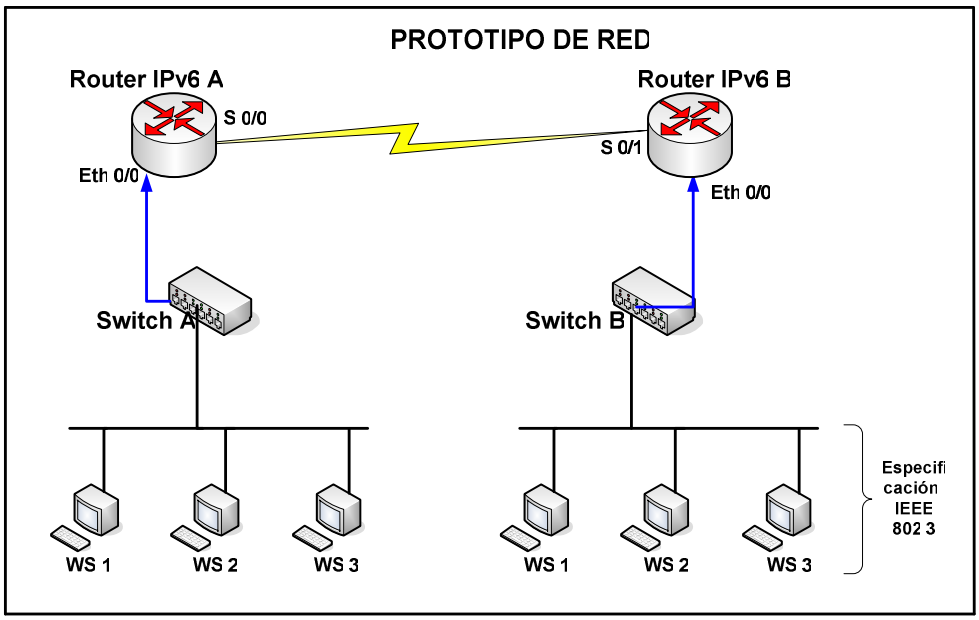


Fig. 3.4 Prototipo utilizado para la configuración del protocolo IPv6

Los componentes utilizados en esta red son los descritos en la tala 3.3 con sus respectivas características:

Tabla 3.3: Componentes de red.

Dispositivos	Cantidad	Características
Routers	2	✓ Serie: Cisco2600 ✓ S.O.: IOS v3 tanabata ✓ Puertos seriales: WAN 0 ✓ Puertos Locales: Eth0 ✓ Puerto de Consola. ✓ RAM: 6500 bytes ✓ Protocolos: IPv4, IPv6, ARP, RIP, IGRP
Switch	2	✓ Serie: Nexxt solutions ✓ Puertos: 8 puertos 10/100 Mbps Fast Ethernet
Hosts	6	Celeron de 2.5Ghz con discos de 120 GB, 256 de memoria RAM.

3.1.7.1 Configuración de Interfaces en Windows

3.1.7.1.1 Configuración Automática sin Estado

Esta forma de configuración es creada por el software del protocolo IPv6 el momento en el que se instala el paquete en el hosts, luego se asigna una dirección IPv6 de manera aleatoria a la interfaz del respectivo hosts, y el tipo de dirección que se asignada es de tipo unicast de enlace local.

Para realizar la instalación del protocolo es necesario abrir una ventana del DOS del sistema operativo en la cual se ejecuta el comando *ipv6 install;* en la figura 3.5 se muestra el mensaje de finalización de la instalación.

Para acceder a la ventada del DOS hacemos clic en *Inicio→Todos los Programas→Accesorios→ Símbolo del Sistema.*

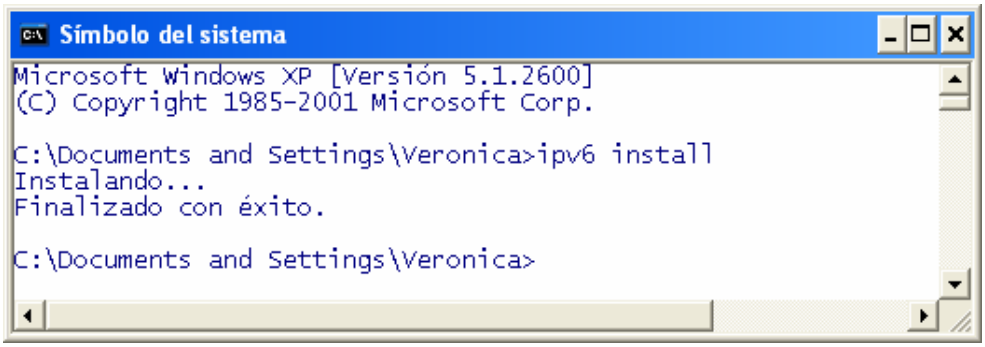


Fig. 3.5 Instalación de IPv6

Luego, en la figura 3.6 se muestra la dirección asignada luego de la instalación del protocolo mediante la ejecución del comando *ipconfig,* este comando es ejecutado en la ventana de símbolo del sistema.

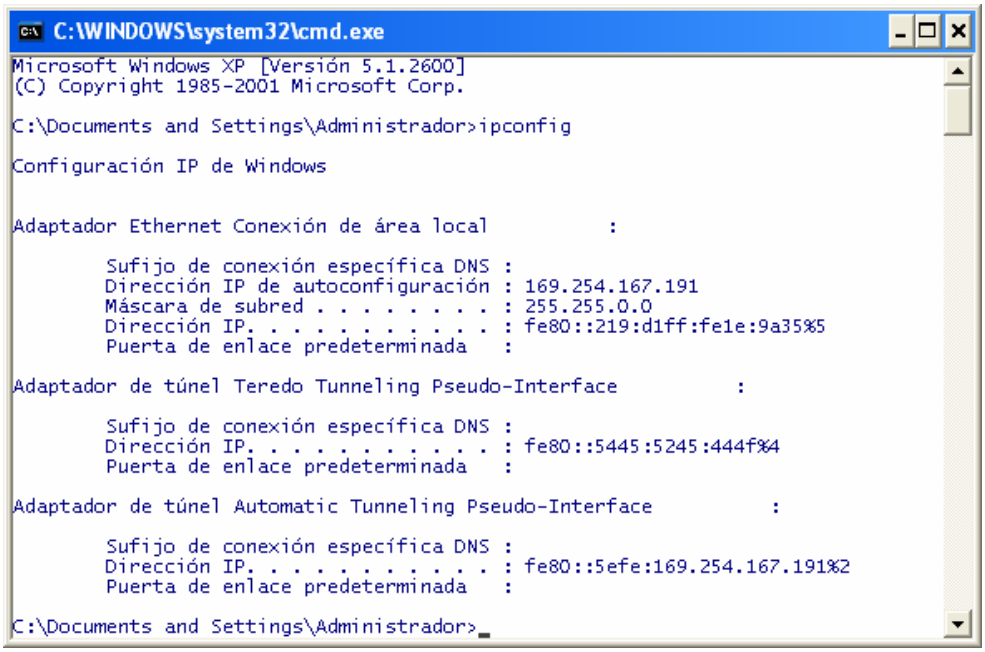


Fig. 3.6 Dirección IPv6 Asignada por Autoconfiguración

Dentro de este tipo de configuración existen dos formas de crear una red:

1. ***Sin Router*** *(direcciones link-local)***.-** Este mecanismo permite al host obtener una dirección partiendo de la información local, generando sus propias direcciones de enlace local. Suficiente para que puedan comunicarse entre sí; en la figura 3.7 se muestra un prototipo de red para este tipo de configuración.

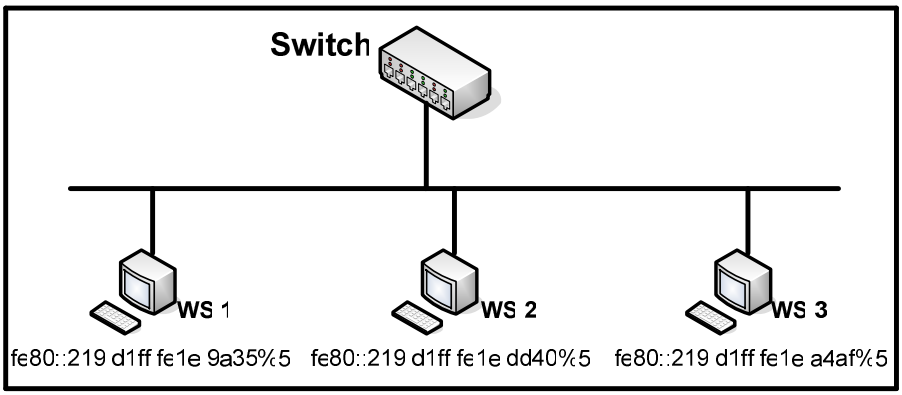


Fig. 3.7 Prototipo para la Autoconfiguración sin Router

Comprobación de la conectividad

En la figura 3.8 se muestra mediante el comando ping la comprobación de la conectividad de la estación **WS1** con las estaciones **WS2** y **WS3**

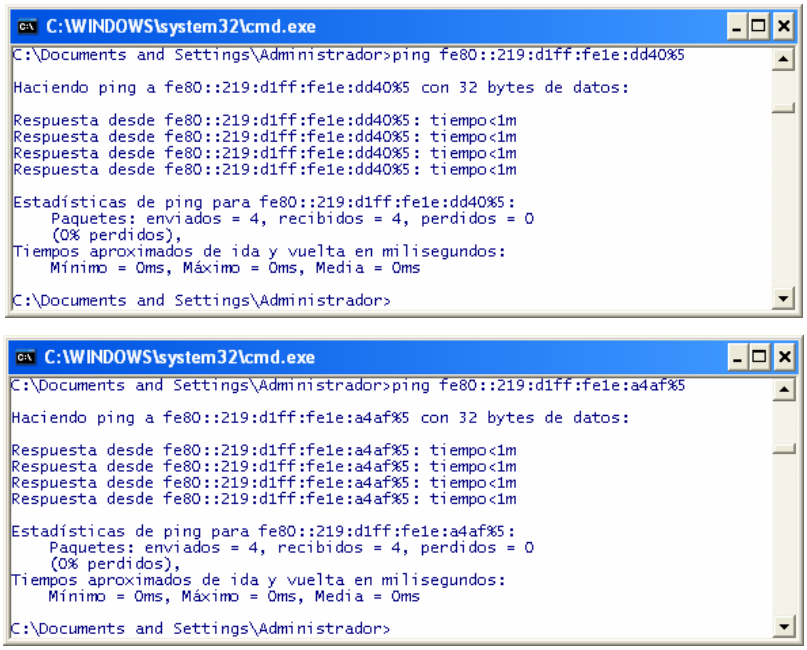


Fig. 3.8 Conectividad entre la WS1 con WS2 y WS3

En la figura 3.9 se muestra mediante el comando ping la comprobación de la conectividad de la estación **WS2** con las estaciones **WS1** y **WS3**

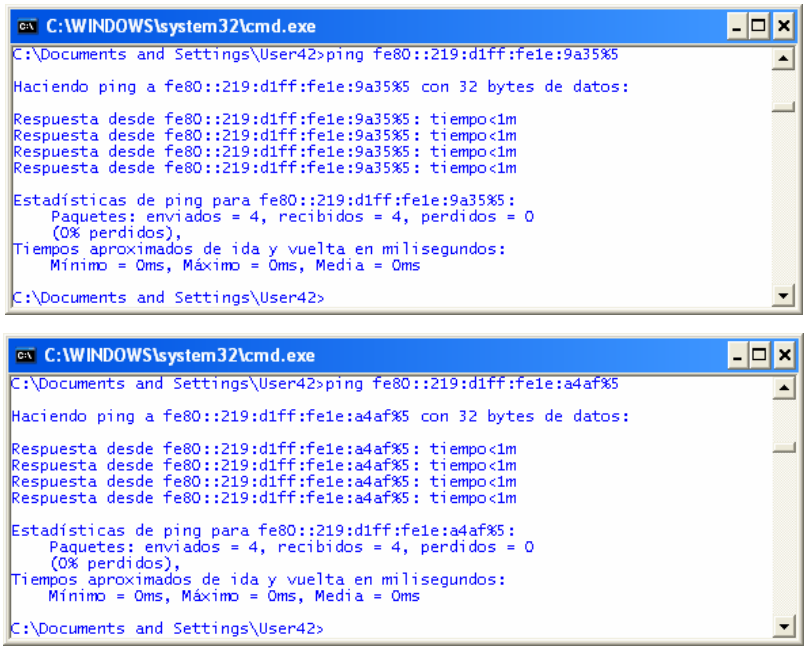


Fig. 3.9 Conectividad entre la WS2 con WS1 y WS3

En la figura 3.10 se muestra mediante el comando ping la comprobación de la conectividad de la estación **WS3** con las estaciones **WS1** y **WS2**

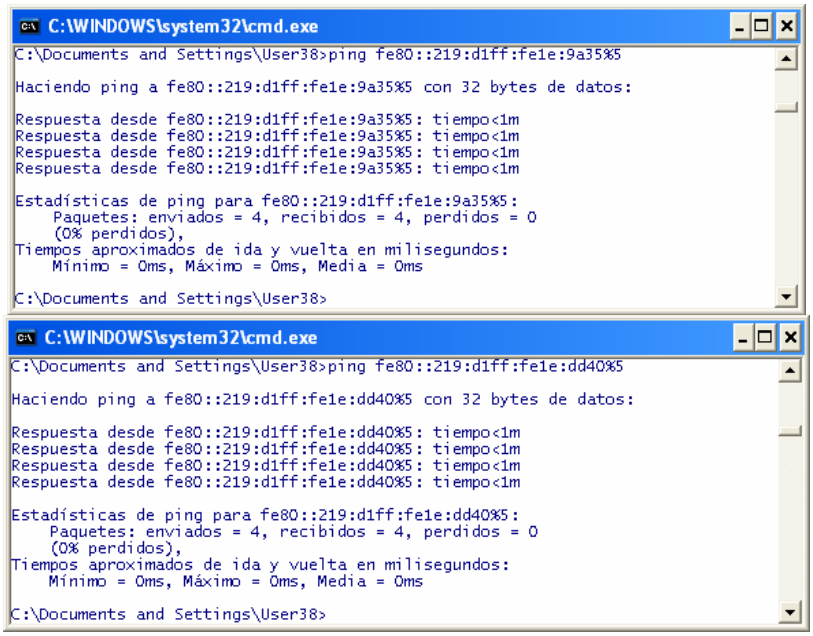


Fig. 3.10 Conectividad entre la WS3 con WS1 y WS2

2. ***Con Router*** *(anuncio de prefijos)****.-*** Este proceso consiste en obtener un anuncio por parte del router, es decir el *prefijo de red* del router previamente configurado manualmente; y esta dirección es completada mediante la información local del host, forman una dirección unicast local de sitio. En la figura 3.11 se muestra el prototipo de red con el router.

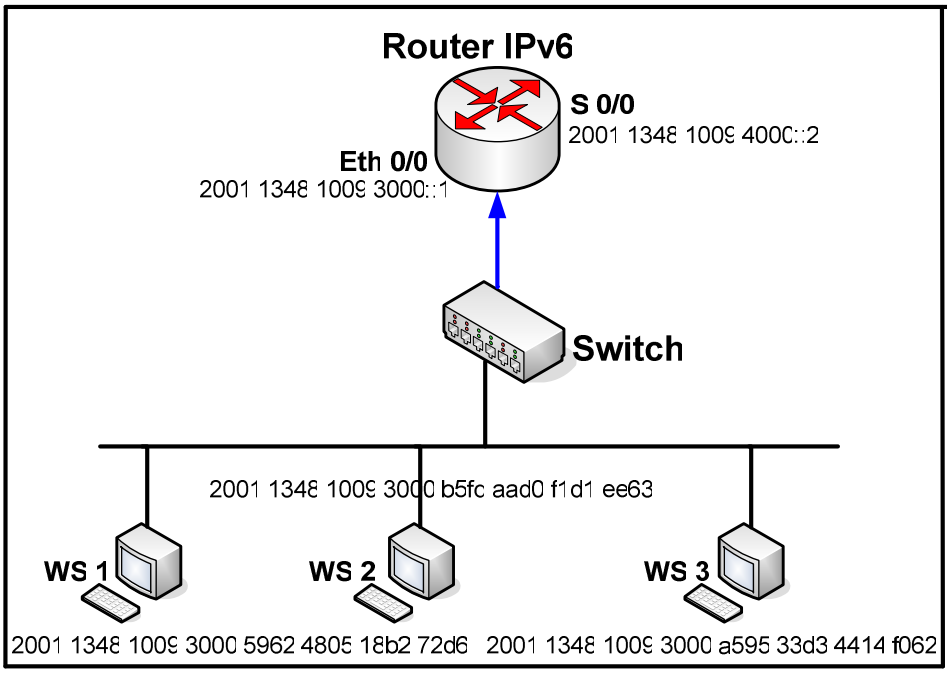


Fig. 3.11 Prototipo para la Autoconfiguración con Router.

3.1.7.1.2 Configuración en Routers Cisco 2600

La configuración de los routers es de forma manual asignada por el administrador, esta configuración esta basada en una serie de comandos; los principales serán detallados a continuación:

Enable.- permite ingresar al modo de configuración.

Configure Terminal.- permite ingresar a la configuración por línea de comandos.

Hostname.- permite asignar un nombre al router.

Interface Ethernet.- permite configurar la interfaz ethernet.

Interface Serial.- permite configurar la interfaz serial.

Address.- agrega una dirección a la interfaz.

IP e IPv6.- es la versión de protocolo, ip para IPv4.

No shut down.- levanta el servicio de direcciones.

Clock Rate.- es la señal de sincronización.

Route.- asigna una ruta de salida estática a otra red.

Write memory.- guarda la configuración.

Show running-config.- despliega la configuración.

Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname CuencaV
CuencaV (config)#enable secret alva
CuencaV (config)#ipv6 rip PRUEBA enable
CuencaV (config)#ipv6 unicast-routing
CuencaV (config)#interface ethernet0/0
CuencaV (config-if)#ipv6 address 2001:1348:1009:3000::1/64
(CuencaV (config-if)#ipv6 address 2001:1348:1009:2000::/64 eui-64)
CuencaV (config-if)#no shut down
CuencaV (config-if)# interface serial0/0
CuencaV (config-if)#ipv6 address 2001:1348:1009:4000::2/64
CuencaV (config-if)#no shut down
CuencaV (config-if)#clock rate 56000
CuencaV (config-if)#^Z

CuencaV #write mem
Building configuration...
[OK]
CuencaV #conf t
Enter configuration commands, one per line. End with CNTL/Z.
CuencaV (config)#ipv6 route 2001:1348:1009:2000::/64 2001:1348:1009:4000::1
CuencaV (config)#^Z
CuencaV#conf t
Enter configuration commands, one per line. End with CNTL/Z.
CuencaV(config)#ip cef
CuencaV(config)#ipv6 cef
CuencaV(config)#^Z
CuencaV#wr
CuencaV #conf t
CuencaV (config)#line console 0
CuencaV (config-line)#pass
CuencaV (config-line)#password alva
CuencaV (config-line)#login
CuencaV (config)#line vty 0 4
CuencaV (config-line)#pass
CuencaV (config-line)#password alva
CuencaV (config-line)#login
CuencaV(config)#^Z
CuencaV#wr

CuencaV #show run
Building configuration...
Current configuration : 1251 bytes
version 12.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
hostname CuencaV

enable secret 5 1D73y$V3R2qulCqAlmNpfwg2YXH1
ip subnet-zero
ip cef
ip audit notify log
ip audit po max-events 100
ipv6 unicast-routing
ipv6 cef
Current configuration : 1093 bytes
version 12.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
ip subnet-zero
ip host manta 192.168.30.1 192.168.10.1
ip host cuenca 192.168.20.1 192.168.10.2
ip audit notify log
ip audit po max-events 100
crypto isakmp nat keepalive 20
ipv6 unicast-routing
ipv6 cef!
mta receive maximum-recipients 0
interface Ethernet0/0
 ip address 192.168.20.1 255.255.255.0
 half-duplex
 ipv6 address 2001:1348:1009:3000::1/64
(ipv6 address 2001:1348:1009:2000::/64 eui-64)
interface Serial0/0
 ip address 192.168.10.2 255.255.255.0
 ipv6 address 2001:1348:1009:4000::2/64
clockrate 56000
 no fair-queue
interface TokenRing0/0
 no ip address

```
 shutdown
 ring-speed 16
router rip
 network 192.168.10.0
 network 192.168.20.0
ip classless
ip http server
ipv6 route 2001:1348:1009:2000::/64 2001:1348:1009:4000::1
call rsvp-sync
voice-port 1/0/0
mgcp profile default
dial-peer cor custom
line con 0
 password alva
 login
line aux 0
line vty 0 4
 password alva
 login
end
```

Comprobación de la Conectividad

Para comprobar la conectividad desde el router a los host conectados en la red se hace uso del comando *ping* y la especificación de la versión del protocolo *ipv6.*

```
CuencaV#ping ipv6 2001:1348:1009:3000::1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:1348:1009:3000::1, timeout is 2 seconds: !!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms

CuencaV#ping ipv6 2001:1348:1009:4000::2
Type escape sequence to abort.
```

Sending 5, 100-byte ICMP Echos to 2001:1348:1009:4000::2, timeout is 2 seconds: !!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms

CuencaV#ping ipv6 2001:1348:1009:4000::1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:1348:1009:4000::1, timeout is 2 seconds: !!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 32/33/37 ms

CuencaV#ping ipv6 2001:1348:1009:2000::
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:1348:1009:2000::, timeout is 2 seconds: !!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 32/32/33 ms

CuencaV#ping ipv6 2001:1348:1009:3000::5962:4805:18b2:72d6
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:1348:1009:3000:5962:4805:18B2:72D6, timeout is 2 seconds: !!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms

CuencaV#ping ipv6 2001:1348:1009:3000:b5fd:aad0:f1d1:ee63
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:1348:1009:3000:B5FD:AAD0:F1D1:EE63, timeout is 2 seconds: !!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms

CuencaV#ping ipv6 2001:1348:1009:3000:a595:33d3:4414:f062
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:1348:1009:3000:A595:33D3:4414:F062, timeout is 2 seconds: !!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms

En la figura 3.12 se muestra la dirección asignada a un host conectado a la interfaz ethernet del ruteador.

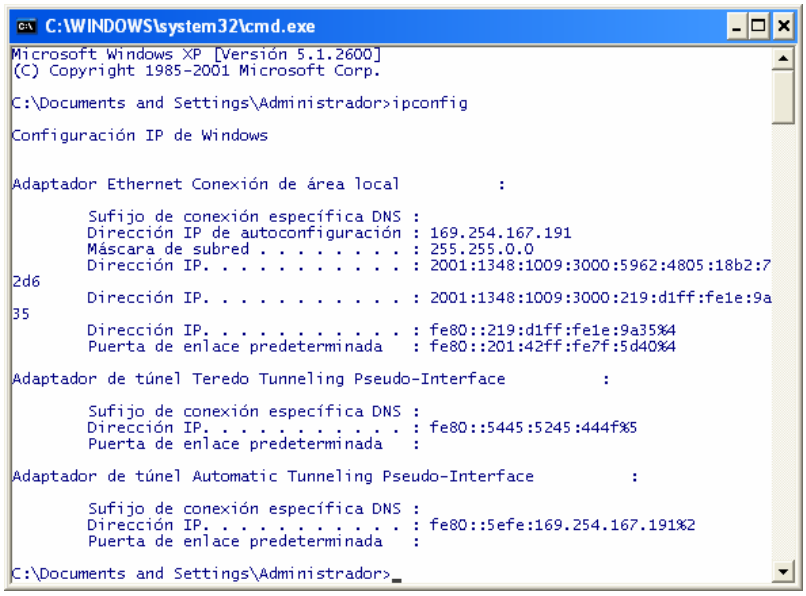
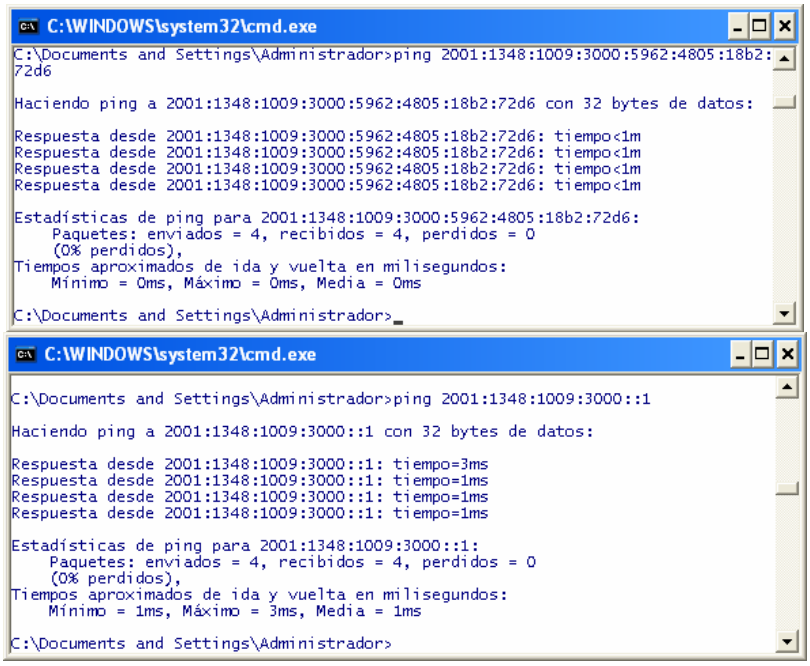


Fig. 3.12 Dirección IPv6 Asignada por Autoconfiguración conectada al Router

Comprobación de la conectividad

En la figura 3.13 se muestra la conectividad desde la **WS1** hacia su propia interfaz, interfaz del router e interfaz de las **WS2** y **WS3**



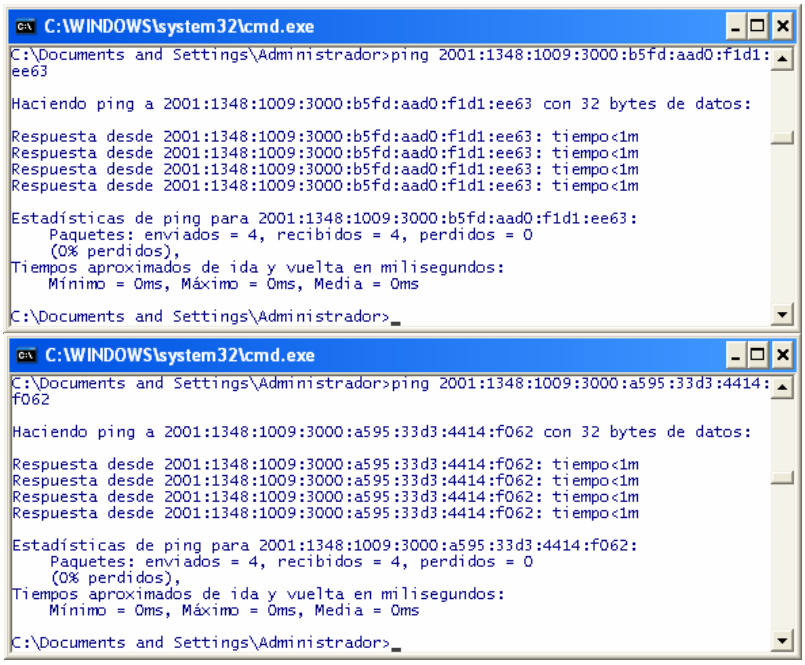
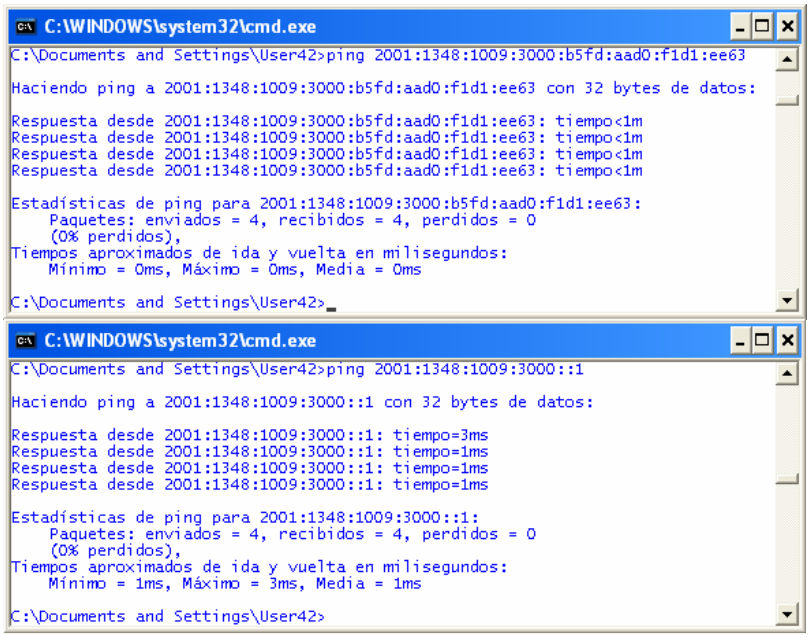


Fig. 3.13 Conectividad entre interfaces de WS1

En la figura 3.14 se muestra la conectividad desde la **WS2** hacia su propia interfaz, interfaz del router e interfaz de las **WS1** y **WS3**



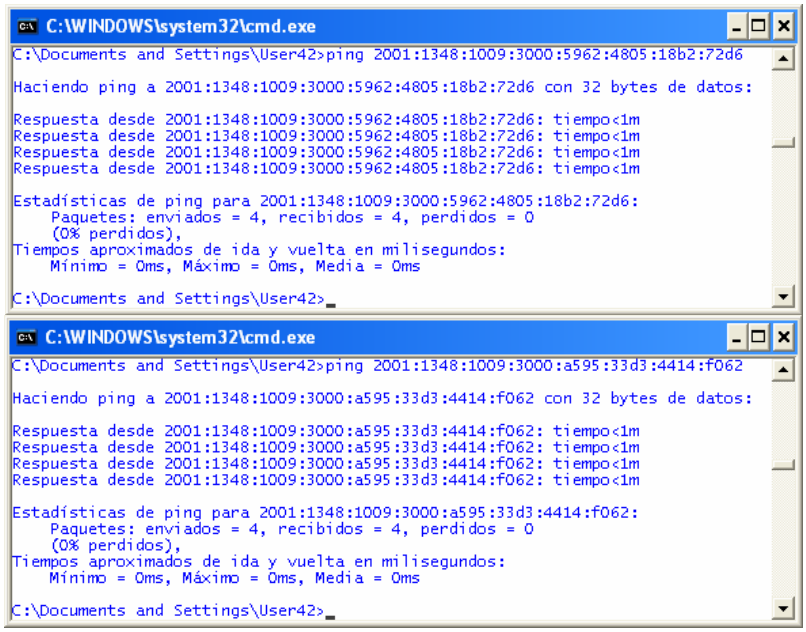
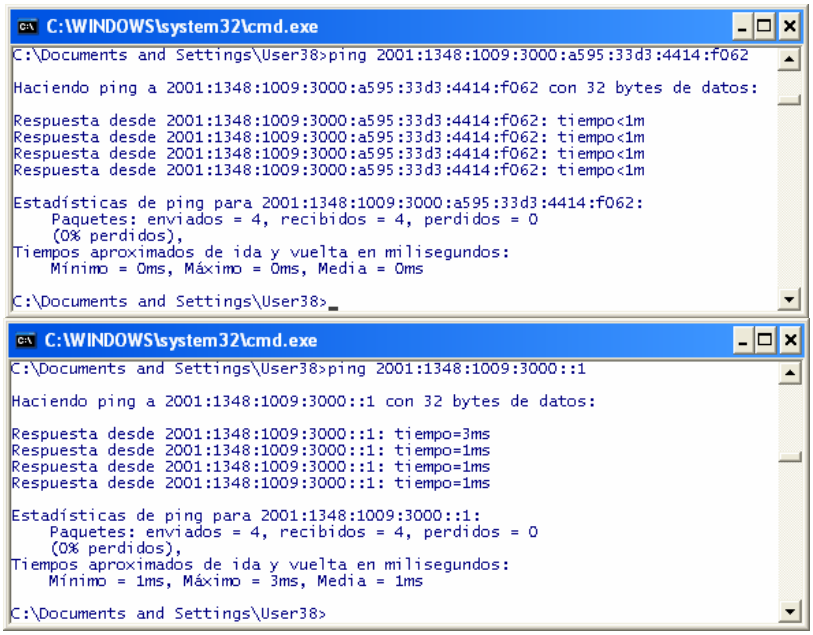


Fig. 3.14 Conectividad entre interfaces de WS2

En la figura 3.15 se muestra la conectividad desde la **WS3** hacia su propia interfaz, interfaz del router e interfaz de las **WS1** y **WS2**



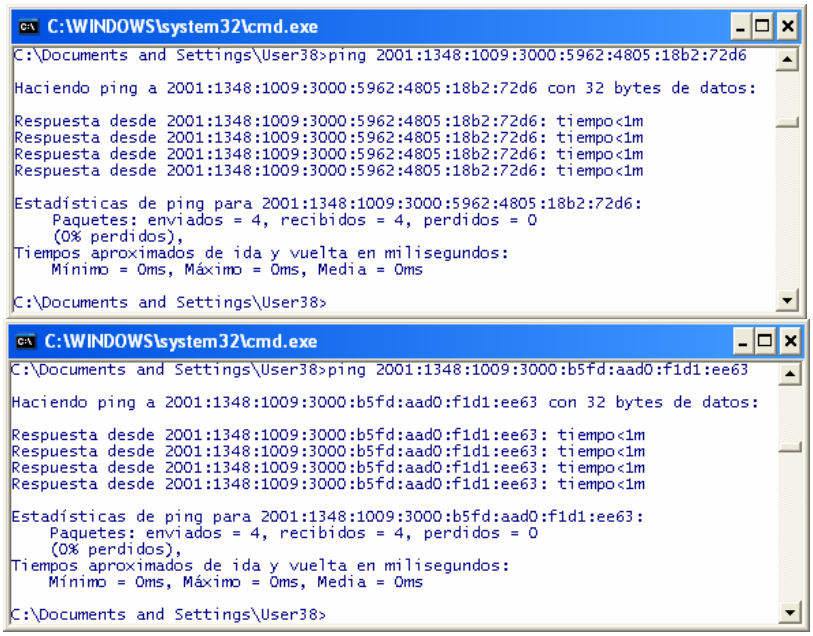


Fig. 3.15 Conectividad entre interfaces de WS3

3.1.7.1.3 Configuración Automática con Estado

Para hacer este tipo de configuración es necesario realizar la configuración de un servidor con servicio DHCPv6, este servicio puede ser configurado sobre las plataformas Linux y Windows y sus clientes pueden estar funcionado sobre las plataformas mencionadas independientemente del sistema operativo con el que se encuentre su servidor DHCPv6; actualmente este servicio no se encuentra en funcionamiento por que todavía no se ha creado las actualizaciones correspondientes sobre Linux pero en el sistema operativo *Windows Vista* ya se puede hacer uso de este servicio.

3.1.7.1.4 Configuración de Interfaces de forma Manual

La configuración manual es realizada mediante la persona encargada de la administración y configuración de la red; para lo cual el administrador ha decidido hacer tres redes utilizando el prototipo mostrado en la figura 3.4.

Para la realización de la configuración manual en Windows se utiliza un shell de comandos de red específico llamado *netshell o netsh,* el cual es un programa de software independiente y la ejecución de este shell se lo hace a través del DoS que se encuentra instalado en el sistema al cual se accede a través de la ventana de símbolo del sistema.

NetShell es una herramienta basada en líneas de comandos que permite a los administradores configurar y administrar los servicios de red de forma remota. La interfaz de líneas de comandos de NetShell se puede utilizar en secuencias de comandos. La API (*Application Programming Interface)* de NetShell amplía la funcionalidad principal de NetShell ya que guarda una secuencia de comandos de configuración, en las siguientes figuras se mostrara una lista de varios subcomandos con su funcionalidad y para visualizarlos lo hacemos mediante el signo ***?***, es decir:

En la figura 3.16 se muestra el prototipo de red a utilizarse con sus respectivas direcciones asignadas manualmente a cada una de las interfaces de red.

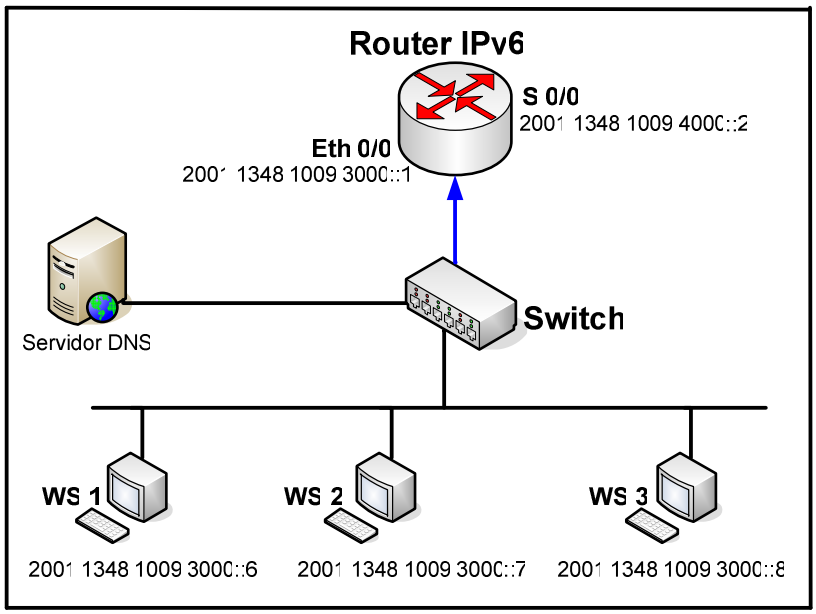


Fig. 3.16 Prototipo para la Configuración Manual

.

Inicialmente se ejecuta el comando *netsh→?* el cual despliega una gama de subcomandos para la configuración de interfaces como se muestra en la figura 3.17.

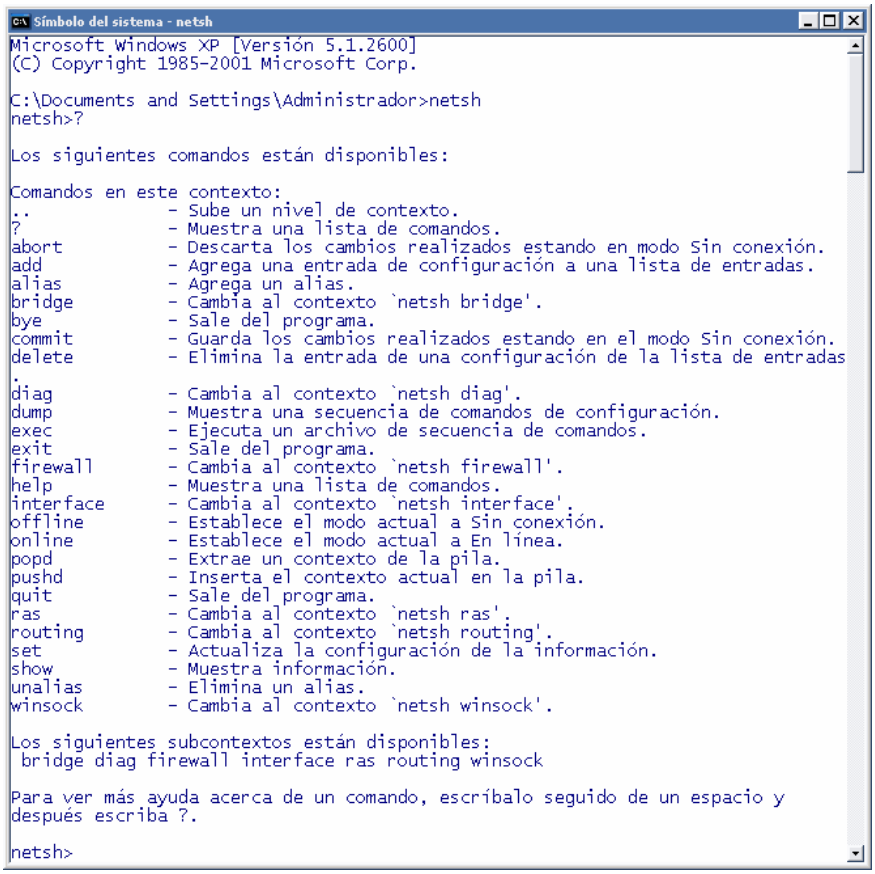


Fig. 3.17 Subcomandos del comando netsh

Seguidamente se ejecuta el comando *interface ?* el cual también presenta una gama de subcomandos para configurar interfaces como se muestra en la figura 3.18.

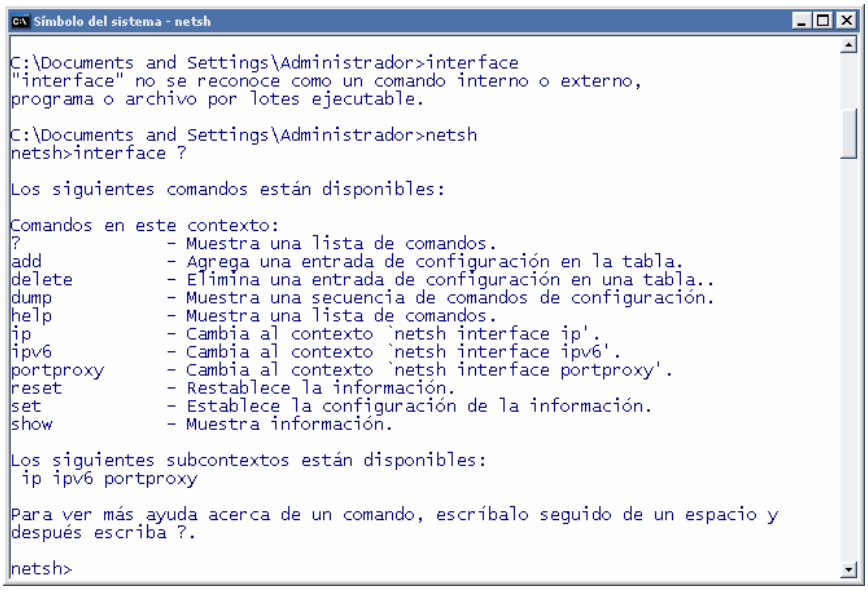


Fig. 3.18 Subcomandos del comando interface

Finalmente se ejecuta el comando *ipv6 ?* el mismo que combinado con algunos de sus subcomandos nos permite realizar varias configuración en una interfaz de red con direcciones IPv6, en la figura 3.19 se muestra los subcomandos existentes.

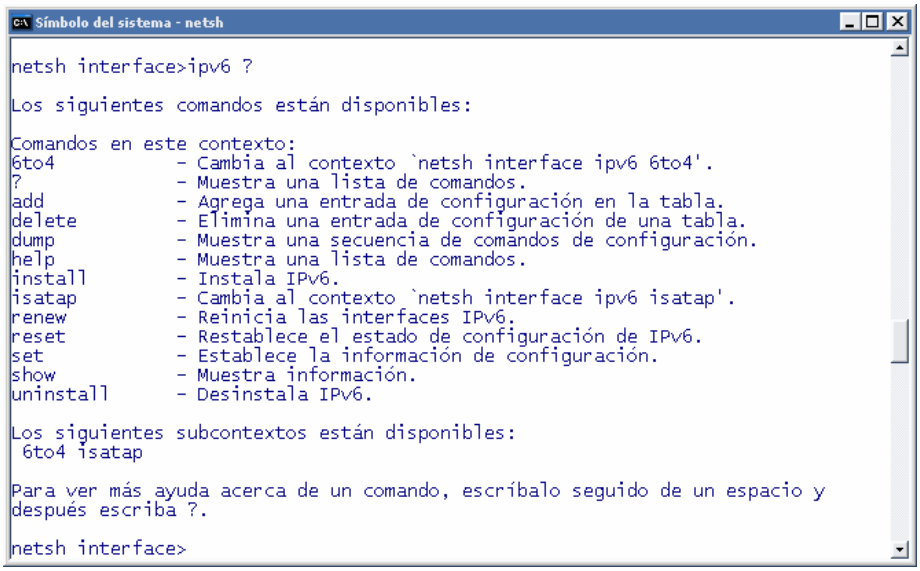


Fig. 3.19 Subcomandos del comando ipv6

A continuación se describe los comandos utilizados por el protocolo IPv6.

6to4.- Este comando es utilizado para realizar el cambio de direcciones IPv6 a direcciones IPv4, lo cual es utilizado cuando se configura un túnel para acceder a otro tipo de interfaz.

Add.- Permite agregar una entrada a la interfaz, la misma que puede ser una dirección IPv6, una dirección fija de un servidor DNS o de alguna ruta.

Delete.- Elimina las entradas de la interfaz.

Install.- Instala todos los componentes del protocolo IPv6.

Renew.- Reinicia la configuración de la interfaz IPv6.

Reset.- Restablece la configuración de la interfaz IPv6.

Set.- Establece la información de la configuración de la interfaz.

Show.- Despliega la información de la interfaz configurada.

Uninstall.- Desinstala los componentes del protocolo IPv6.

Cabe recordar que estos subcomandos pueden ser combinados de acuerdo a la necesidad de la configuración.

En la figura 3.20 se muestra una combinación de los comandos descritos anteriormente como por ejemplo la agregación de una dirección IPv6 y su sintaxis es la siguiente: *protocolo + add address + "nombre-interfaz" + dir-ipv6.*

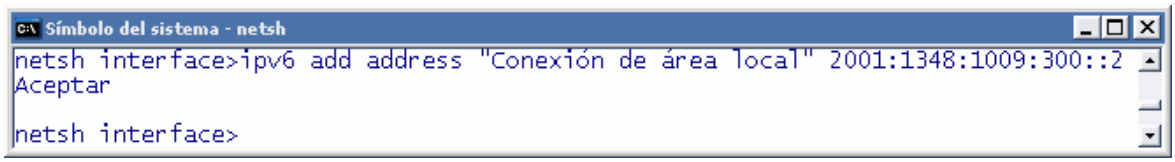


Fig. 3.20 Asignación de Dirección IPv6

En la figura 3.21 se muestra una combinación de los comandos descritos anteriormente como por ejemplo la agregación del tamaño de la longitud del prefijo de red de la dirección IPv6 y su sintaxis es la siguiente: *protocolo + set interface + "nombre-interfaz" + siteprefixlength=entero.*

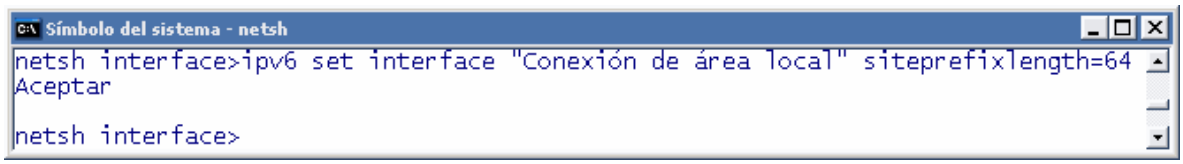


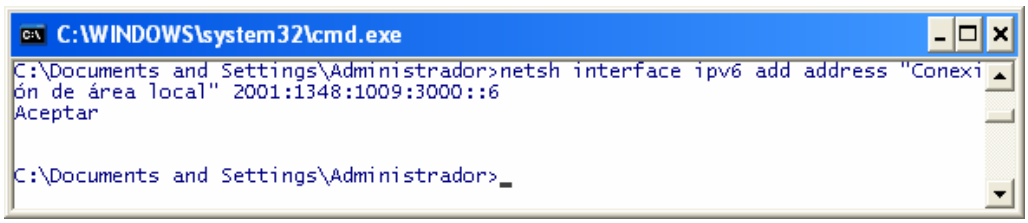
Fig. 3.21 Asignación del Prefijo de la Dirección IPv6

- **Nota:** Para no seguir todos estos pasos y si conocemos los subcomandos necesarios podemos simplemente ejecutarlos seguidamente (ver figura 3.22), el cual nos permiten la asignación de la dirección IPv6 y del tamaño del prefijo de la dirección.

Comandos:

netsh interface ipv6 add address "nombre-interfaz" dir-ipv6

netsh interface ipv6 set interface "nombre-interfaz" siteprefixlength=entero



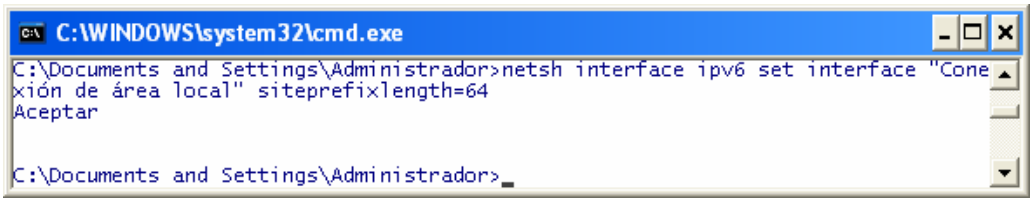


Fig. 3.22 Comando y subcomandos netsh

En la figura 3.23 se muestra la interfaz configurada mediante el comando ipconfig.

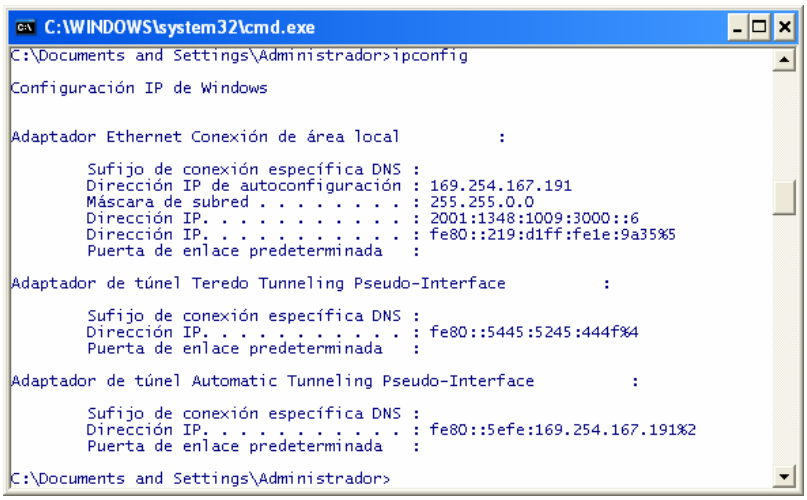


Fig. 3.23 Interfaz Configurada

Comprobación de la Conectividad

Para comprobar la conectividad entre las interfaces ejecutamos el comando *ping* más la dirección de la Interfaz desde la ventada de símbolo del sistema. En la figura 3.24 se muestra la conectividad desde uno de los host, a su propia interfaz, a la interfaz del router, a otras interfaces.

También podemos comprobar la conectividad desde el router hacia las interfaces existentes en la red.

CuencaV#ping ipv6 2001:1348:1009:3000::6

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 2001:1348:1009:3000::6, timeout is 2 seconds: !!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms

CuencaV#ping ipv6 2001:1348:1009:3000::7

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 2001:1348:1009:3000::7, timeout is 2 seconds: !!!!!

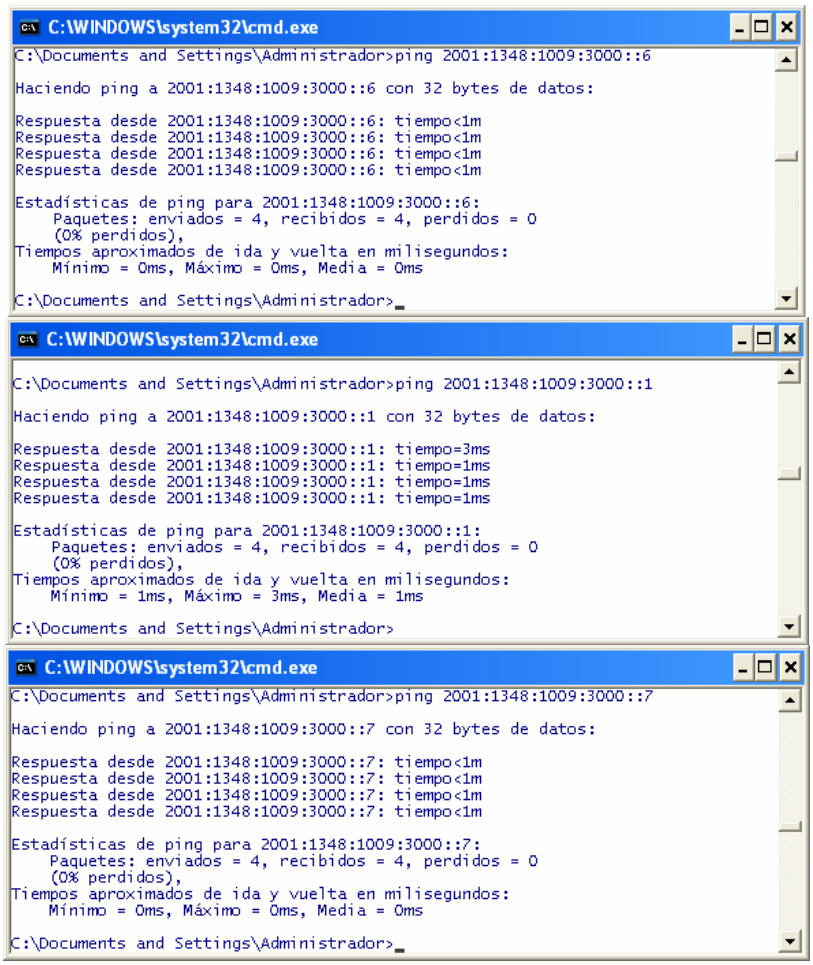
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms

CuencaV#ping ipv6 2001:1348:1009:3000::8

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 2001:1348:1009:3000::8, timeout is 2 seconds: !!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms



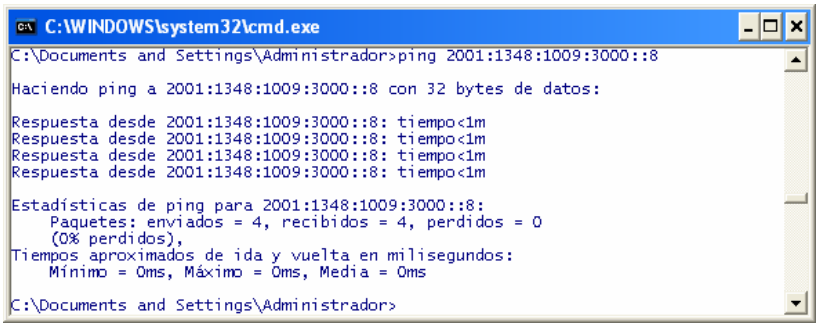


Fig. 3.24 Conectividad entre Interfaces

3.1.7.2 Configuración de Interfaces en Linux

Para la creación de este proyecto se ha considerado la utilización de la distribución Centos versiones 4.5 y 5.0 de Linux, ya que las versiones mencionadas no necesitan actualizaciones por que el protocolo IPv6 ya es parte del software.

Al igual que en el sistema operativo Windows, en Linux también es posible realizar los mismos métodos de configuración a la interfaz de red antes mencionados.

3.1.7.2.1 Configuración Automática

- ✓ **Sin Router.-** Este método de configuración consiste en la asignación de una dirección de enlace local por parte del protocolo IPv6, para este tipo de configuración hay que seguir los siguientes pasos:

1. Accedemos a la interfaz de la tarjeta de red haciendo clic en: *Menú K→Configuración del Sistema→Red.* (ver figura3.25).

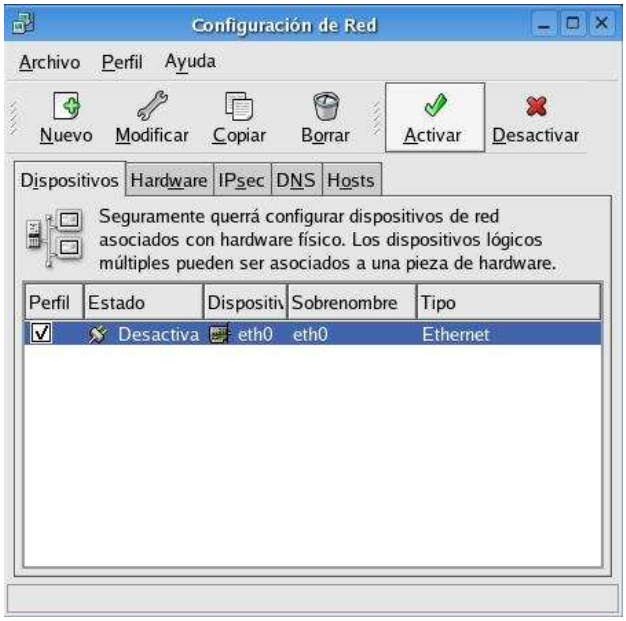


Fig. 3.25 Interfaz de Red

2. Seguidamente seleccionamos la pestaña *Modificar* y activamos la opción correspondiente para el uso del protocolo IPv6. (ver figura 3.26).

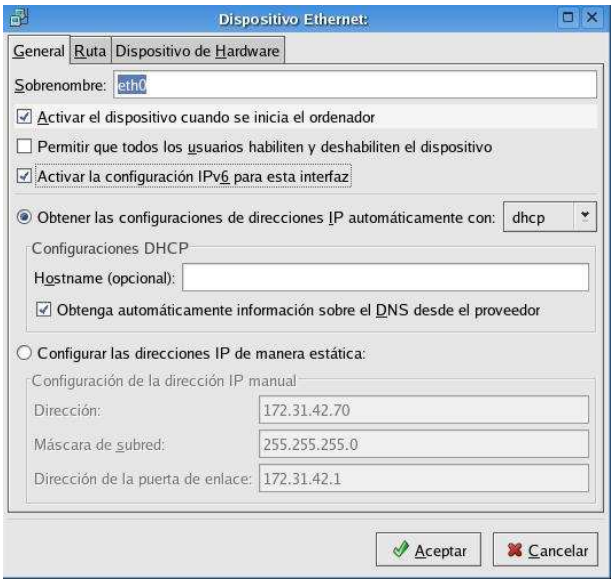


Fig. 3.26 Activación de IPv6 a Interfaz de Red

3. Activamos la tarjeta de red mediante la pestaña *Activar;* para lo cual nos va a presentar una serie de mensajes como se muestra en la figura 3.27 y en la figura 3.28 ya se puede ver la tarjeta activada.

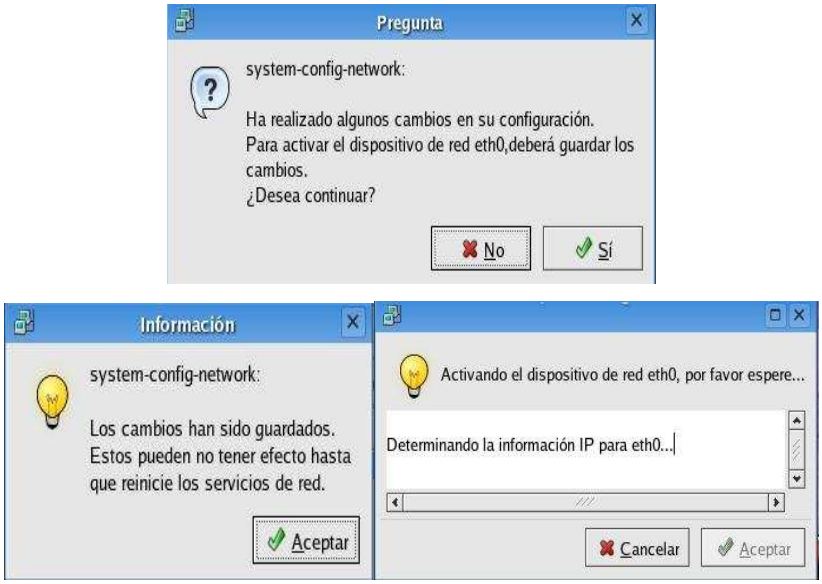


Fig. 3.27 Mensajes de activación de la tarjeta de Red

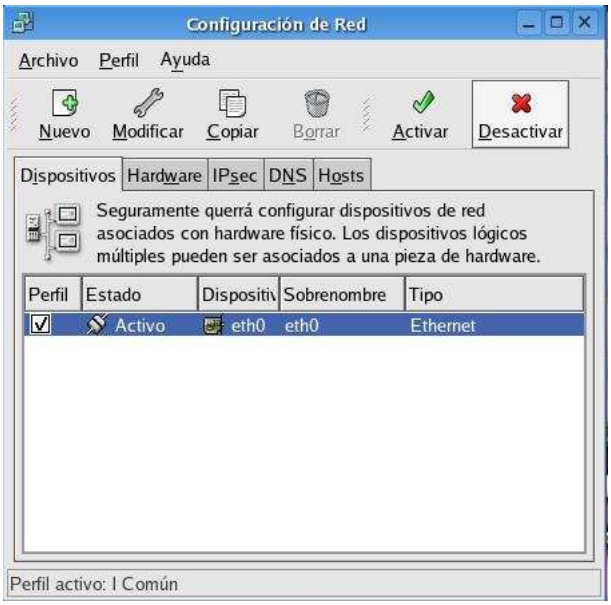


Fig. 3.28 Tarjeta de Red activada

4. Mediante la ventana de Terminal de Consola para hacer uso de algunos comandos para la configuración correspondiente, para esto se hace clic en: *Menú K→Herramientas del Sistema→Terminal* como se muestra en la figura 3.29.

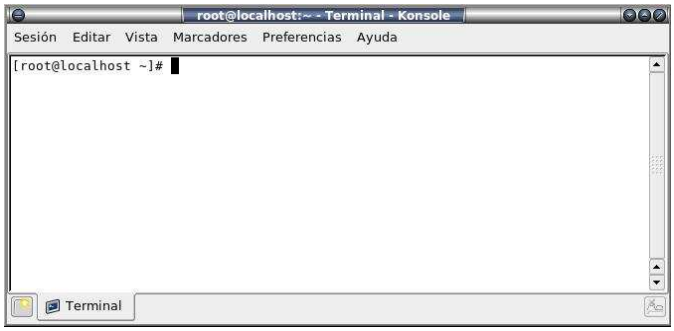


Fig. 3.29 Terminal de Consola

5. Ejecutamos el comando *vi /etc/sysconfig/network-scripts/ifcfg-eth0* el cual nos permite acceder al fichero de configuración de la interfaz de la tarjeta de red para visualizar los valores de configuración predeterminados, como en este caso estamos realizando una autoconfiguración sin estado tenemos que agregar el valor correspondiente a la *Autoconfiguración*: (ver figura 3.30)

   IPv6INIT=yes El cual habilita IPv6 en la interfaz

   IPV6AUTOCONF=yes. El cual habilita la autoconfiguración

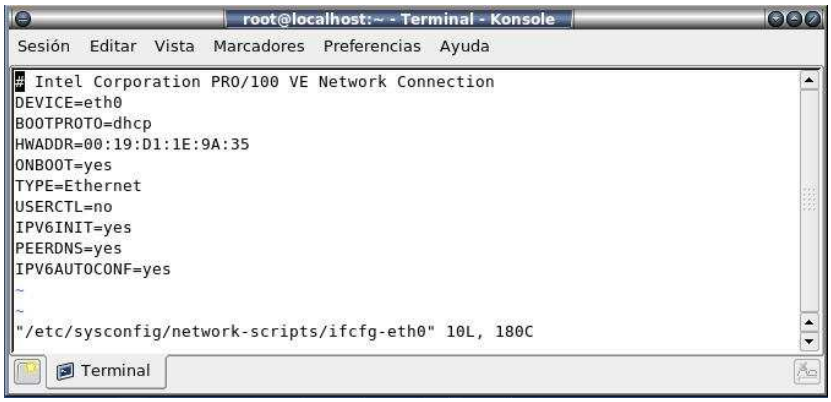


Fig. 3.30 Fichero de configuración de la Interfaz

6. Para comprobar la configuración y verificar la asignación de la dirección IPv6 de enlace local ejecutamos el comando *ifconfig* (ver figura 3.31)

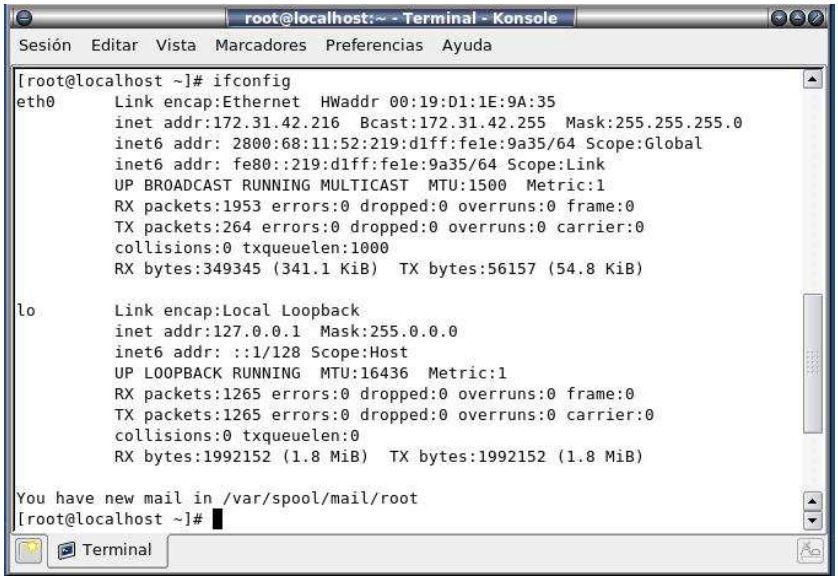
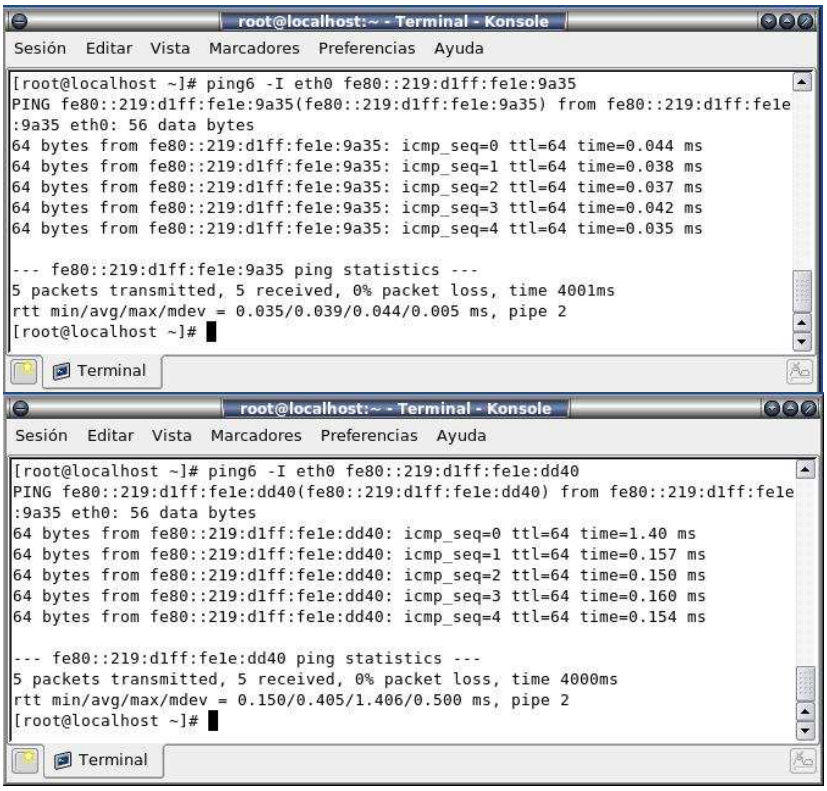


Fig. 3.31 Comando ifconfig

7. Para finalizar comprobamos la conectividad con la dirección local entre las maquinas existentes en la red. En la figura 3.32 se comprueba la conectividad al propio host y a otro host existente en la misma red usando el siguiente comando: *ping6 –I eth0 + dir-ipv6.*



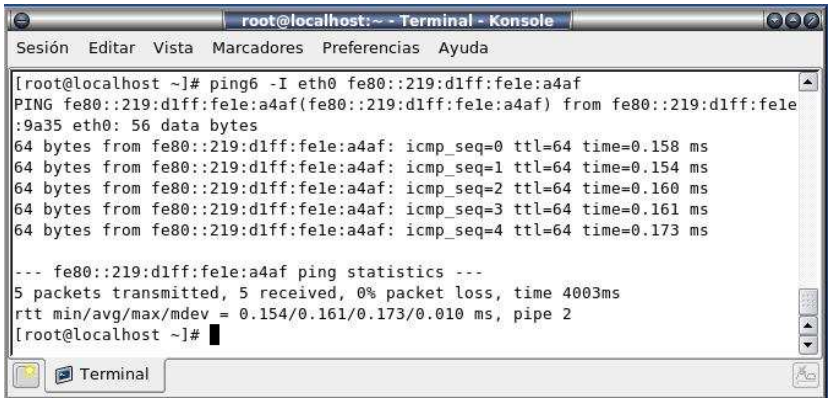


Fig. 3.32 Comando Ping6

Cabe resaltar que para la comprobación de la conectividad de una red, tanto en Windows como en Linux se utiliza el comando *Ping,* pero para el caso de Linux es necesario especificar la versión del protocolo *(ping6),* además agregar la opción necesaria *(-I)* y especificar el nombre de la tarjeta de red *(eth0)* como se mostró en la figura anterior.

A continuación se muestra alguna de las opciones para el uso del comando ping6:
Ping6.- envía los paquetes ICMPv6 que solicitan los host de la red.
-a.- *addrtype* (agregar tipo). Generar la pregunta de las direcciones del nodo de la información del nodo ICMPv6, el addrtype debe ser una secuencia construida de los caracteres siguientes.

a.- solicita las direcciones unicast. Si se omite el carácter, sólo esas direcciones que pertenecen al interfaz que tiene la dirección del respondedor son peticiones.
c.- direcciones de IPv4 compatibles y de IPv4 mapeadas del respondedor de las peticiones.
g.- direcciones de enlace global del respondedor de las peticiones.
s.- solicita las direcciones locales de sitio del respondedor.
l.- solicita las direcciones locales de acoplamiento del respondedor.
A.- direcciones anycast del respondedor de las peticiones.

-b.- *bufsiz.* Fijar el tamaño del almacenador intermediario del zócalo.

-**c.-** *count* (contador) Parar después de enviar y de recibir los paquetes y contar los ecos de respuesta.

-d.- Fija la opción de SO_DEBUG en el zócalo que es utilizado.

-f.- *Flood ping* (desbordamiento de ping). Salida de paquetes tan rápidamente como se vuelven o uno ciento de veces por segundo. Para cada eco de respuesta enviado un período "." se imprime, mientras que para cada eco de replica recibe una tecla de retroceso y se imprime. Esto proporciona una exhibición rápida si se están cayendo los paquetes. Solamente el súper usuario puede utilizar esta opción. Esto puede ser muy duro en un trabajo neto y se debe utilizar con la precaución.

-H.- Específica para intentar operaciones de reverso de búsqueda de las direcciones IPv6. El comando ping6 no intenta las operaciones de reverso de búsqueda a menos que la opción sea específica.

-h.- Fijar el hoplimit *(limite de saltos)* de IPv6.

-I.- *Interface.* Paquete fuente con la dirección dada del interfaz. Esta opción se aplica si el ping destino es una dirección multicast, o una dirección unicast de enlace local o local de sitio.

-i.- *Wait* (esperar). Segundos de espera entre el envió de cada paquete. El defecto a está espera es un segundo entre cada paquete. Esta opción es incompatible con la opción de f.

-l.- *Preload (carga).* Si se especifica la carga, el ping6 envía muchos paquetes tan rápidamente como sea posible antes de caer en su modo normal de comportamiento. Solamente el súper usuario puede utilizar esta opción.

-n.- Salida numérica. No se hará ninguna tentativa a los nombres simbólicos de las operaciones de búsqueda de direcciones en la contestación.

-N.- Prueba la información de los grupos de nodos multicast.

-p.- *Pattern* (modelo). Puede especificar hasta 16 “octetos patrones” para completar el paquete al enviar. Esto es útil para diagnosticar problemas dependientes en una red. Por ejemplo, “- p FF” hará al paquete enviado ser llenado.

-P.- *Policy* (política). *L*a política específica de IPsec es una política que se utilizará para hacer pruebas.

-q.- Salida reservada. No se exhibe nada excepto las líneas sumarias en el tiempo de lanzamiento y cuando está acabada.

-R.- Hace que el núcleo crea que el hosts principal sea accesible. La opción es significativa solamente si el host principal es un vecino.

-S.- *Source addr*. Especifica la dirección fuente de los paquetes de petición. La dirección fuente debe ser una de las direcciones unicast del nodo que envía. Si la interfaz saliente es especificada por la opción de -I también, la dirección origen necesita ser una dirección asignada a la interfaz específica.

-s.- *Packetsize* (tamaño del paquete). Especifica el número de los octetos de datos que se enviarán. El defecto es de 56, que traduce a 64 octetos de datos del ICMP cuando está combinada con los 8 octetos de datos de la cabecera ICMP. Puede necesitar especificar -b también para ampliar el tamaño de almacenamiento intermediario del zócalo.

-t.- Generar la información del nodo ICMPv6, es mejor que solicitar -s no tiene ningún efecto si se especifica -t.

-v.- Salida prolija. Los paquetes del ICMP con excepción de eco de respuesta se reciben y se enumeran.

-w.- Generar la pregunta del nombre del DNS de la información del nodo ICMPv6, es mejor que solicitar -s ya que no tiene ningún efecto si se especifica -W.

-W.- Iguales que -w, pero con el viejo formato del paquete basado en el bosquejo 03. Esta opción está presente para la compatibilidad con -s que no tiene ningún efecto si se especifica -w.

- ✓ **Con Router.-** Cuando en una red contamos con la presencia de un router, este se encarga de asignar su prefijo de red para formar una dirección de tipo unicast local de sitio a cada uno de los host existentes en la red. En la figura 3.33 mediante el comando *ifconfig* se muestra la asignación de prefijo por parte del router.

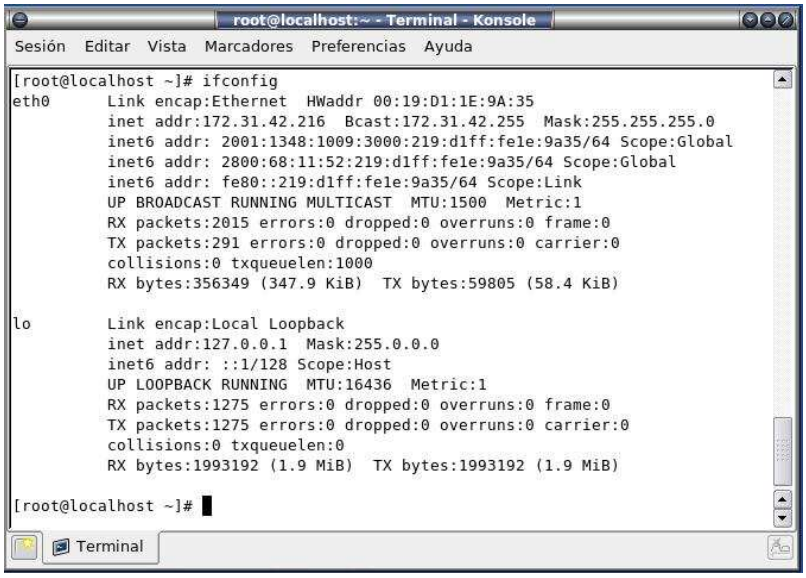
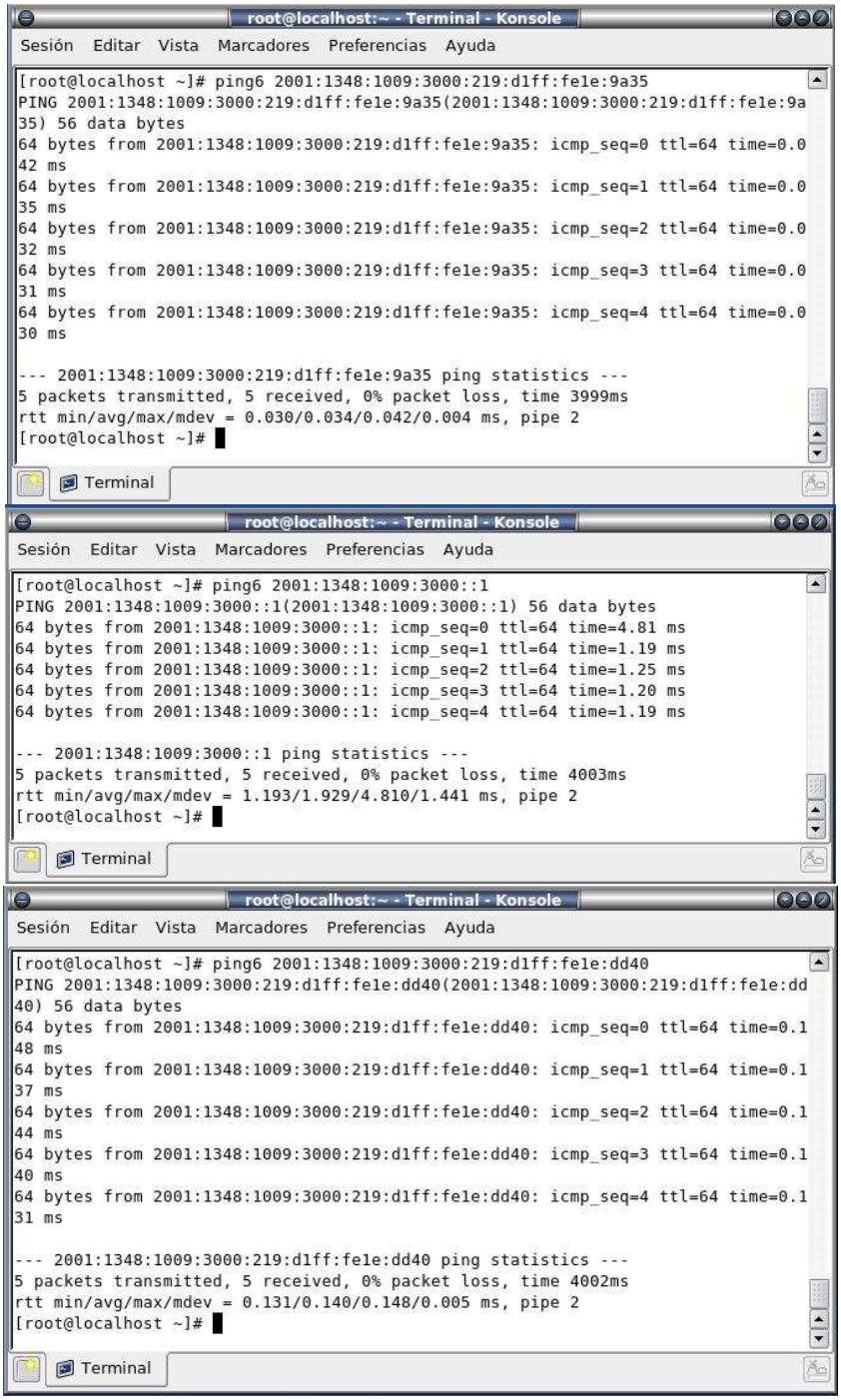


Fig. 3.33 Comando Ifconfig

Para comprobar la conectividad entre los host de la red se hace uso del comando *ping6;* pero para este tipo de direcciones no es necesario agregar ningún tipo de opciones al comando ping6 (ver figura 3.34).


root@localhost:~ - Terminal - Konsole
Sesión Editar Vista Marcadores Preferencias Ayuda
[root@localhost ~]# ping6 2001:1348:1009:3000:219:d1ff:fe1e:9a35
PING 2001:1348:1009:3000:219:d1ff:fe1e:9a35(2001:1348:1009:3000:219:d1ff:fe1e:9a35) 56 data bytes
64 bytes from 2001:1348:1009:3000:219:d1ff:fe1e:9a35: icmp_seq=0 ttl=64 time=0.042 ms
64 bytes from 2001:1348:1009:3000:219:d1ff:fe1e:9a35: icmp_seq=1 ttl=64 time=0.035 ms
64 bytes from 2001:1348:1009:3000:219:d1ff:fe1e:9a35: icmp_seq=2 ttl=64 time=0.032 ms
64 bytes from 2001:1348:1009:3000:219:d1ff:fe1e:9a35: icmp_seq=3 ttl=64 time=0.031 ms
64 bytes from 2001:1348:1009:3000:219:d1ff:fe1e:9a35: icmp_seq=4 ttl=64 time=0.030 ms
--- 2001:1348:1009:3000:219:d1ff:fe1e:9a35 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 3999ms
rtt min/avg/max/mdev = 0.030/0.034/0.042/0.004 ms, pipe 2
[root@localhost ~]#
Terminal
root@localhost:~ - Terminal - Konsole
Sesión Editar Vista Marcadores Preferencias Ayuda
[root@localhost ~]# ping6 2001:1348:1009:3000::1
PING 2001:1348:1009:3000::1(2001:1348:1009:3000::1) 56 data bytes
64 bytes from 2001:1348:1009:3000::1: icmp_seq=0 ttl=64 time=4.81 ms
64 bytes from 2001:1348:1009:3000::1: icmp_seq=1 ttl=64 time=1.19 ms
64 bytes from 2001:1348:1009:3000::1: icmp_seq=2 ttl=64 time=1.25 ms
64 bytes from 2001:1348:1009:3000::1: icmp_seq=3 ttl=64 time=1.20 ms
64 bytes from 2001:1348:1009:3000::1: icmp_seq=4 ttl=64 time=1.19 ms
--- 2001:1348:1009:3000::1 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4003ms
rtt min/avg/max/mdev = 1.193/1.929/4.810/1.441 ms, pipe 2
[root@localhost ~]#
Terminal
root@localhost:~ - Terminal - Konsole
Sesión Editar Vista Marcadores Preferencias Ayuda
[root@localhost ~]# ping6 2001:1348:1009:3000:219:d1ff:fe1e:dd40
PING 2001:1348:1009:3000:219:d1ff:fe1e:dd40(2001:1348:1009:3000:219:d1ff:fe1e:dd40) 56 data bytes
64 bytes from 2001:1348:1009:3000:219:d1ff:fe1e:dd40: icmp_seq=0 ttl=64 time=0.148 ms
64 bytes from 2001:1348:1009:3000:219:d1ff:fe1e:dd40: icmp_seq=1 ttl=64 time=0.137 ms
64 bytes from 2001:1348:1009:3000:219:d1ff:fe1e:dd40: icmp_seq=2 ttl=64 time=0.144 ms
64 bytes from 2001:1348:1009:3000:219:d1ff:fe1e:dd40: icmp_seq=3 ttl=64 time=0.140 ms
64 bytes from 2001:1348:1009:3000:219:d1ff:fe1e:dd40: icmp_seq=4 ttl=64 time=0.131 ms
--- 2001:1348:1009:3000:219:d1ff:fe1e:dd40 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4002ms
rtt min/avg/max/mdev = 0.131/0.140/0.148/0.005 ms, pipe 2
[root@localhost ~]#
Terminal

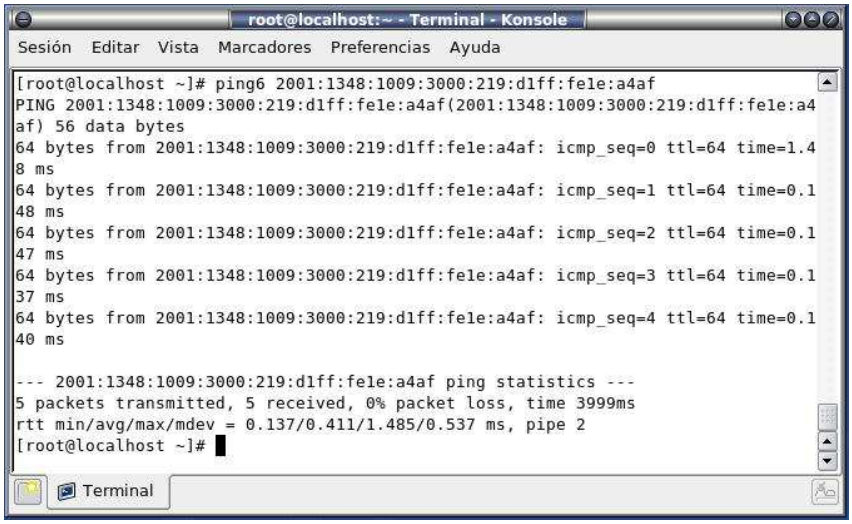


Fig. 3.34 Comando Ping6

3.1.7.2.2 Configuración Manual

Al igual que en la autoconfiguración ingresamos al fichero de configuración de interfaces mediante el comando *vi /etc/sysconfig/network-scripts/ifcfg-eth0,* y se agrega la dirección IPv6, además de cambiar el valor de la autoconfiguración: (ver figura 3.35)

IPV6AUTOCONF=no	No habilita la autoconfiguración
IPV6ADDR=2001:1348:1009:3000::8	Asigna la dirección

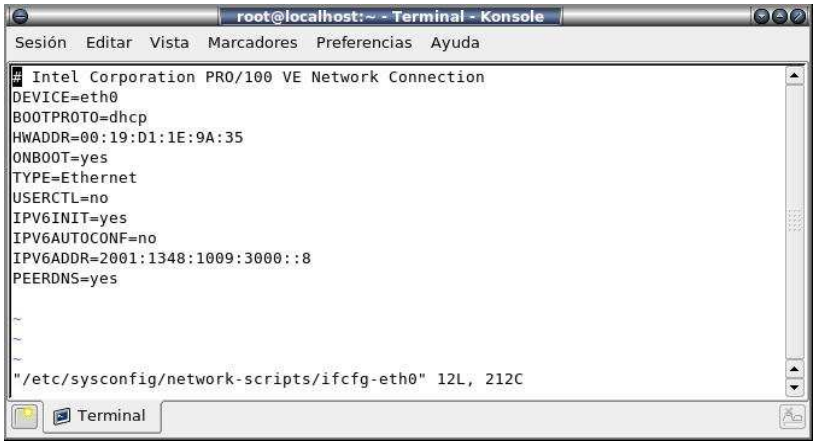


Fig. 3.35 Fichero de configuración de la Interfaz

Para complementar con la configuración y para que no exista ningún tipo de conflicto con el reconocimiento de la versión del protocolo, es necesario agregar

algunos valores en el fichero *vi /etc/hosts* como son los mostrados en la figura 3.36.

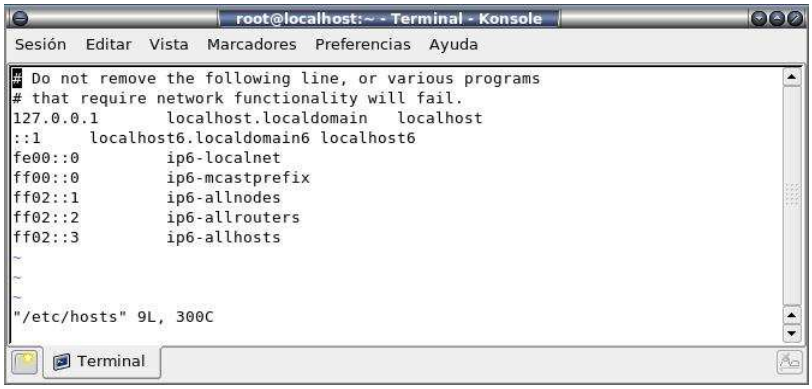


Fig. 3.36 Fichero de configuración de Hosts

Igualmente en el fichero *vi /etc/sysconfig/network* hay que cambiar el valor de la autoconfiguración de positivo a negativo como se muestra en la figura 3.37.

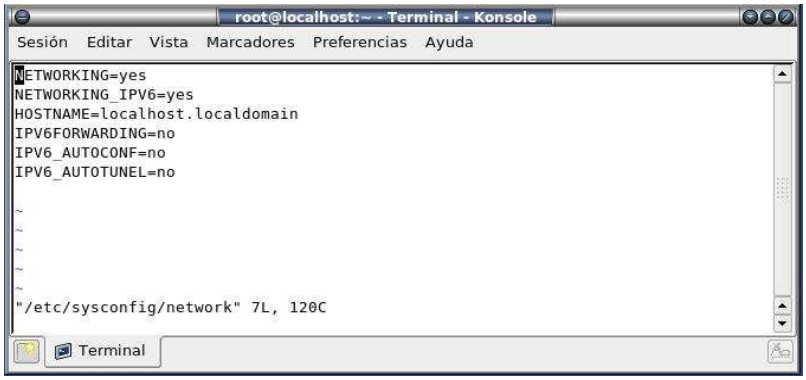


Fig. 3.37 Fichero de configuración de Red

Para que se establezcan los nuevos valores a la tarjeta de red hay que reiniciar la tarjeta de red ejecutando el comando */etc/init.d/network restar* o *service network restart* como se muestra en la figura 3.38

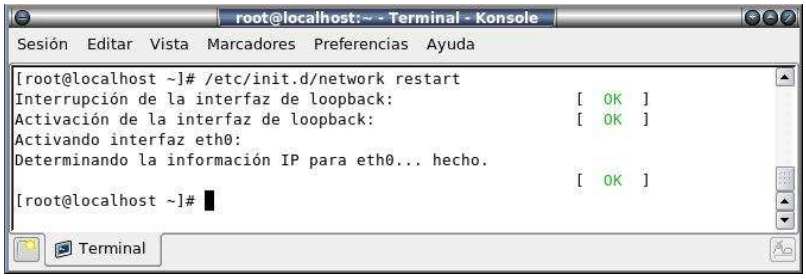


Fig. 3.38 Restauración de valores de la tarjeta de Red

Finalmente, comprobamos los valores asignados mediante el comando *ifconfig* (ver figura 3.39).

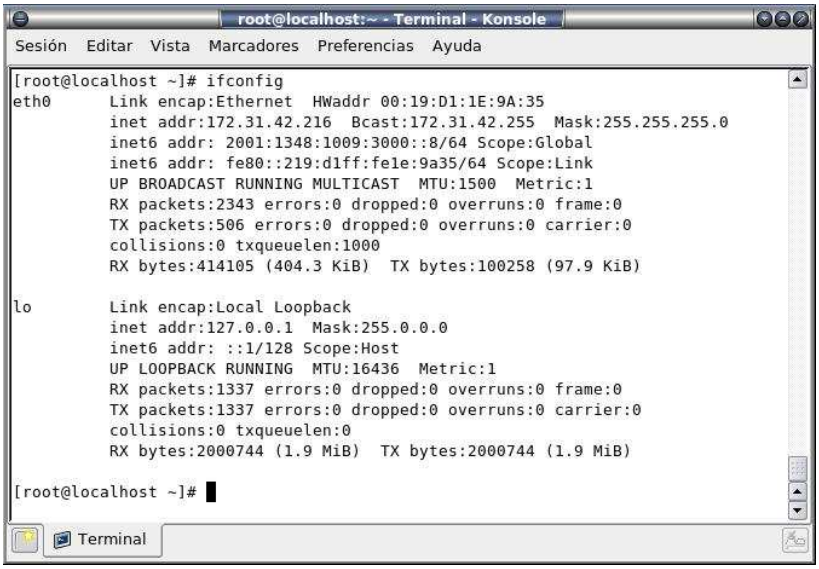


Fig. 3.39 Comando Ifconfig

Comprobación de la Conectividad

La figura 3.40 muestra la conectividad mediante la dirección asignada manualmente, mediante el comando ping6.

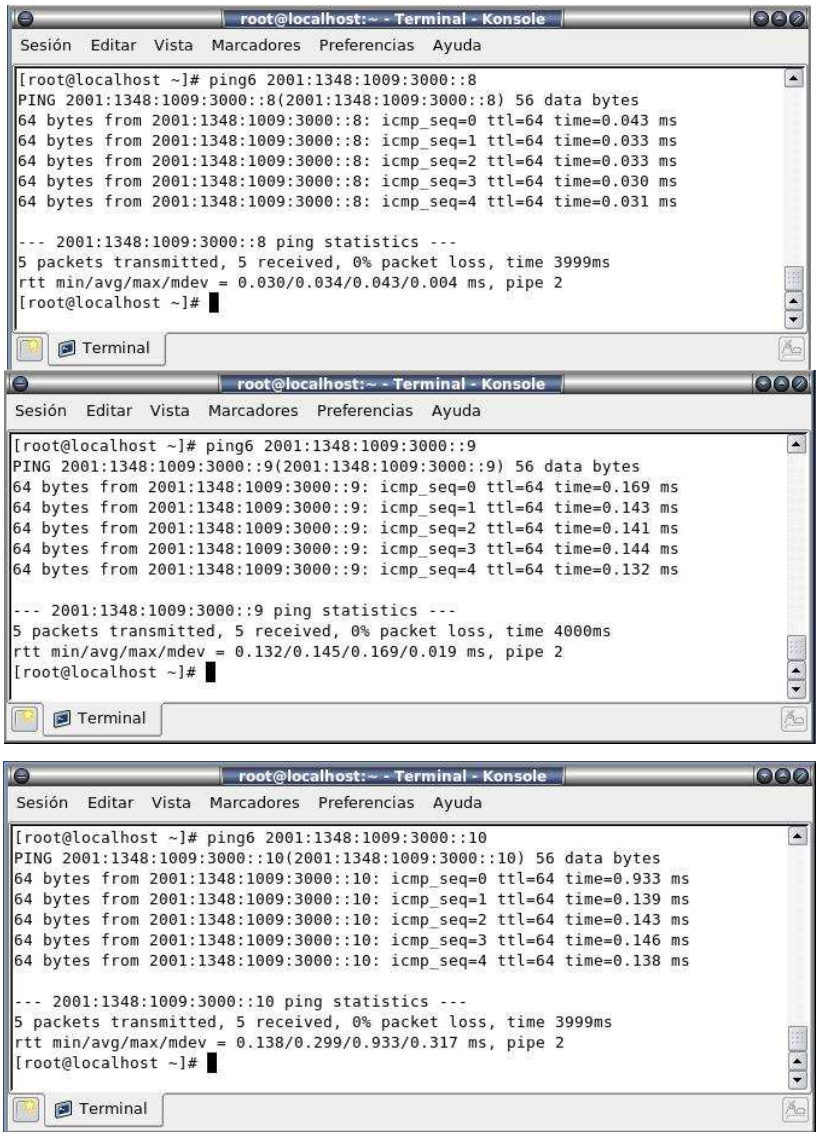


Fig. 3.40 Comando Ping6

3.1.7.3 Configuración del Servidor DNS

El servicio que se va a configurar en la subred del LTI con IPv6 es el Servidor de Dominio de Nombres; este servicio va a ser configurado en el sistema operativo Linux en la distribución Centos ya que sus actualizaciones soportan el uso de direcciones IPv6 y el archivo de configuración ya vienen pre-configurado; las estaciones clientes en cambio serán configuradas sobre el sistema operativo Windows.

Este servicio sirve para resolver nombres de host con direcciones IPv6. Cuando un host IPv6 está configurado con la dirección de un servidor DNS, el host envía

las consultas de nombres DNS al servidor para su resolución. Los registros de recursos AAAA (cuádruple A), que se almacenan en los servidores DNS, permiten la asignación de un nombre de host a la dirección IPv6 correspondiente.

3.1.7.3.1 Pasos de Configuración para el Servidor DNS

1. Iniciamos el servicio ejecutando el comando */etc/init.d/named Start*, el cual nos presentara un mensaje como lo muestra la figura 3.41.

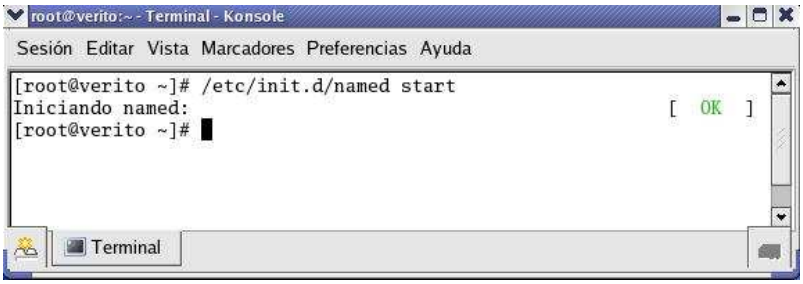


Fig. 3.41 Inicio del servicio DNS

2. En la carpeta *cd /var/named* se encuentran los archivos de configuración (ver figura 3.42) mediante el comando *ls –l* listamos los archivos existentes.

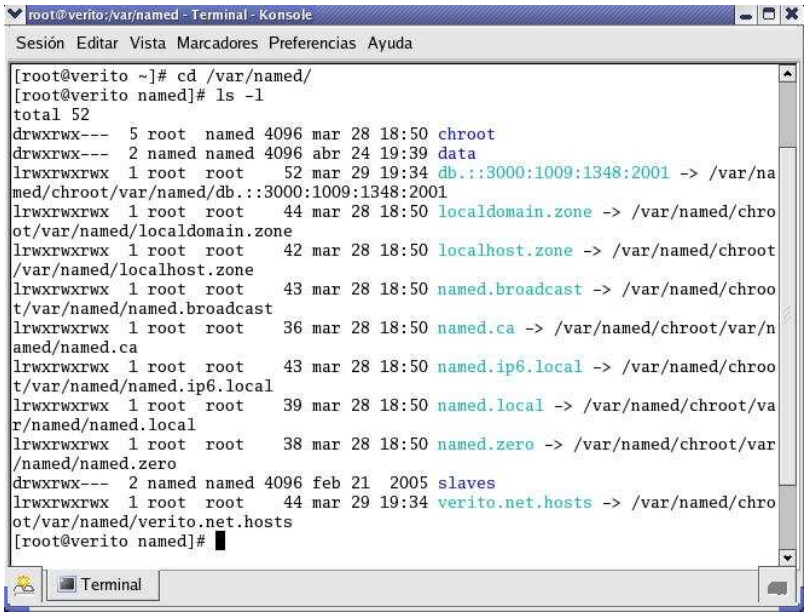


Fig. 3.42 Configuraciones DNS

3. Luego ingresamos al archivo de configuración de hosts mediante el comando *vi verito.net.hosts* el cual nos permite registrar a los host que serán parte de la red con sus respectivas direcciones (ver figura 3.43).

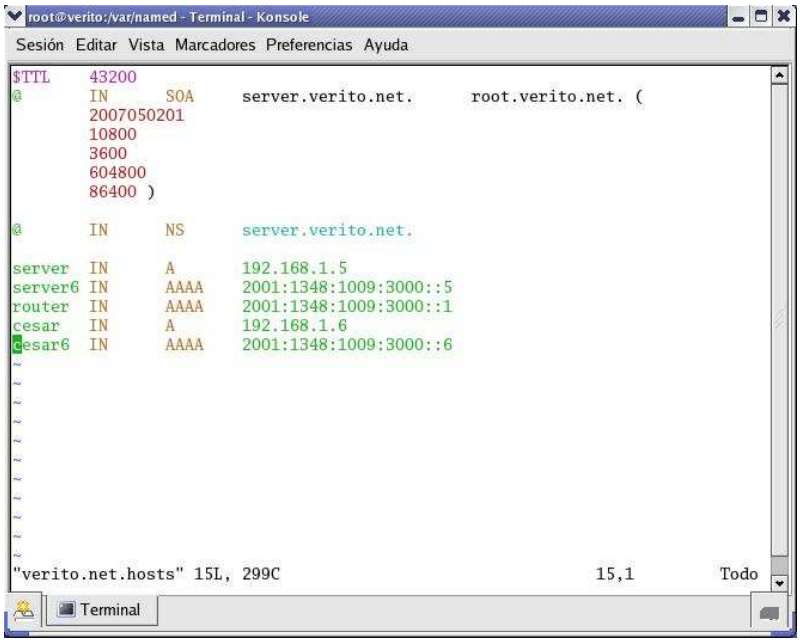


Fig. 3.43 Archivo de configuración de Hosts en DNS

4. Mediante el comando *vi db.\:\:3000\:1009\:1348\:2001* accedemos al archivo para la configuración inversa de las direcciones de los hosts (ver figura 3.44).

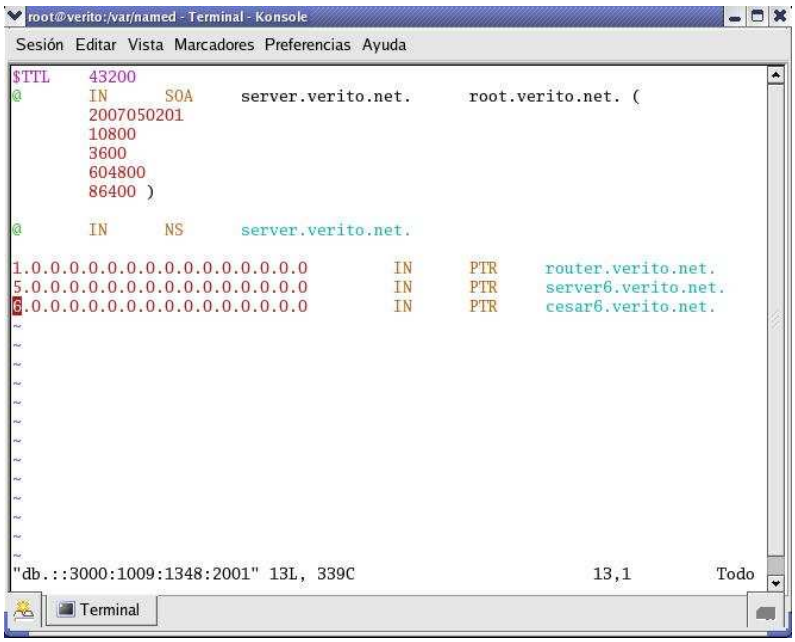


Fig. 3.44 Direcciones de Hosts en DNS

5. Para Ingresar al archivo de configuración principal se ejecuta el comando *vi /named.conf;* pero para ingresar a este archivo tenemos que estar en el prompt etc para lo cual primero se ejecuta *cd /etc.* (ver figura 3.45)

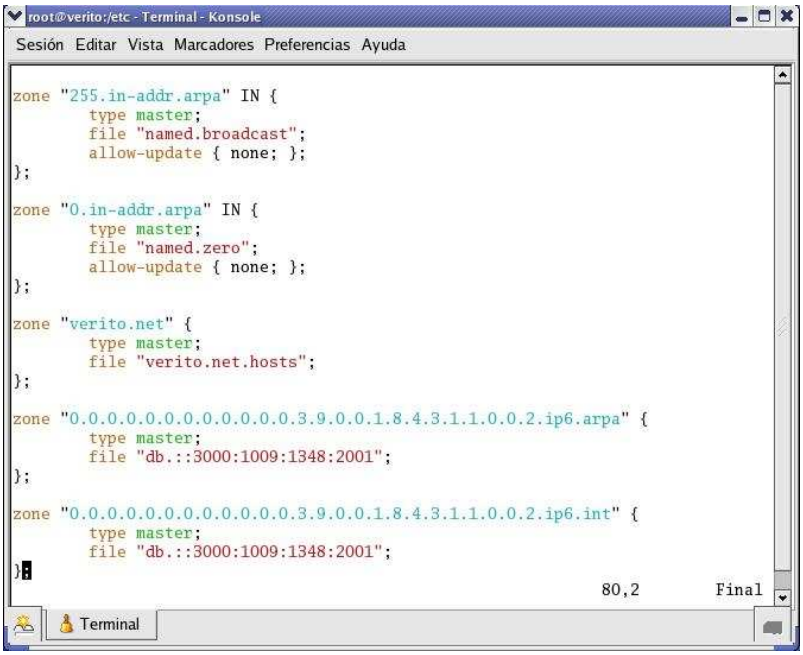


Fig. 3.45 Configuración del DNS

3.1.7.3.2 Pasos de Configuración para las estaciones Clientes

Para agregar el servidor en las estaciones abrimos la ventana de Símbolo de Sistema y ejecutamos el comando (ver figura 3.46):

netsh interface ipv6 add dns "nombre-interfaz" dir-ipv6-dns

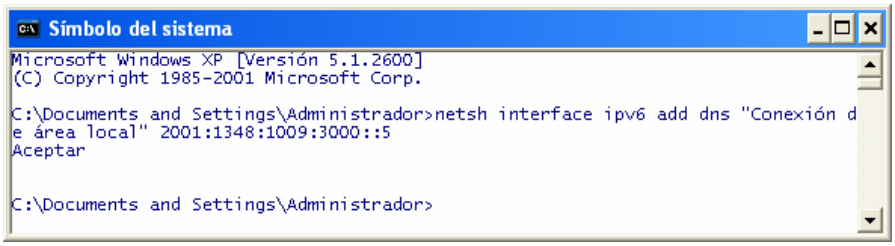


Fig. 3.46 Agregar DNS

Mediante el comando *ipconfig/all* se visualiza la dirección correspondiente al servidor como se muestra en la figura 3.47.

Fig. 3.47 Comando ipconfig /all

Comprobación de la Conectividad

En la figura 3.48 se muestra la comprobación de la conectividad desde el servidor hacia el router, así mismo y las estaciones clientes.

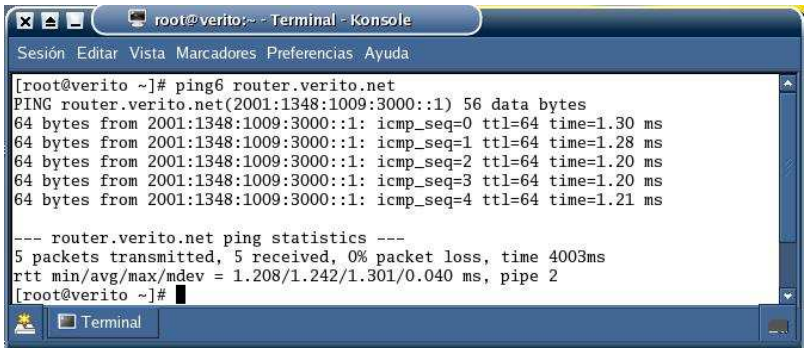


Fig. 3.48 Comando Ping6

En la figura 3.49, mediante el comando *dig aaaa* comprobamos la dirección correspondiente al servidor.

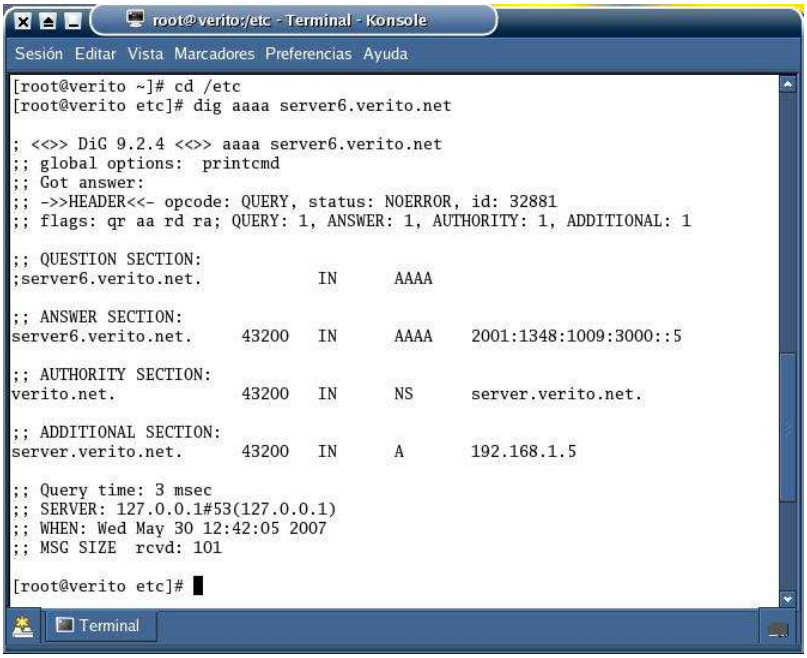
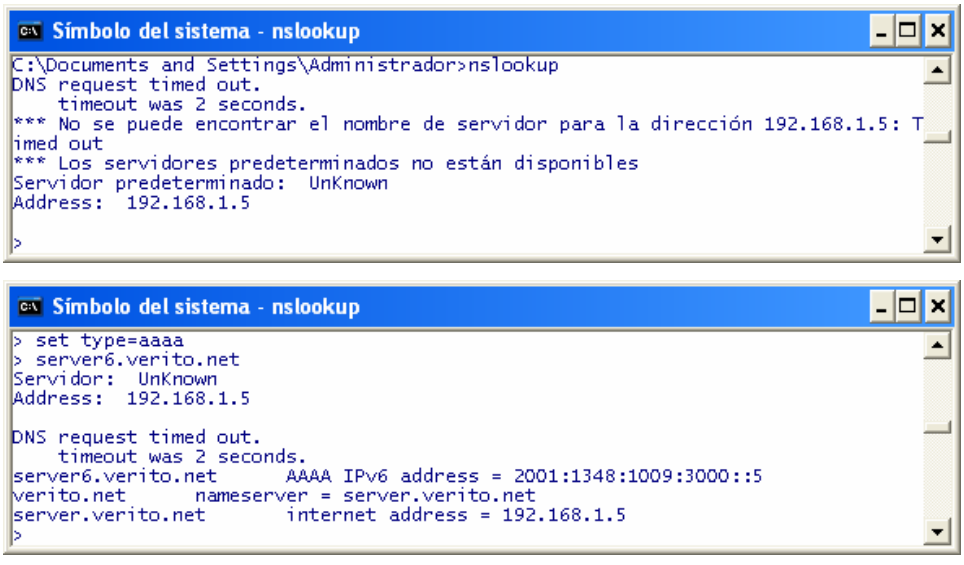


Fig. 3.49 Comando Dig

Los comandos que se ejecutan para la comprobación del servidor DNS son los siguientes: (ver figura 3.50)

- ✓ *nslookup.-* es la herramienta perfecta para averiguar el nombre exacto de una dirección IP de cualquier maquina.
- ✓ *set type=aaaa.-* reconoce direcciones IPv6.
- ✓ *server6.verito.net.-* muestra información del servidor.
- ✓ *vero6.verito.net.-* muestra información de la estación.



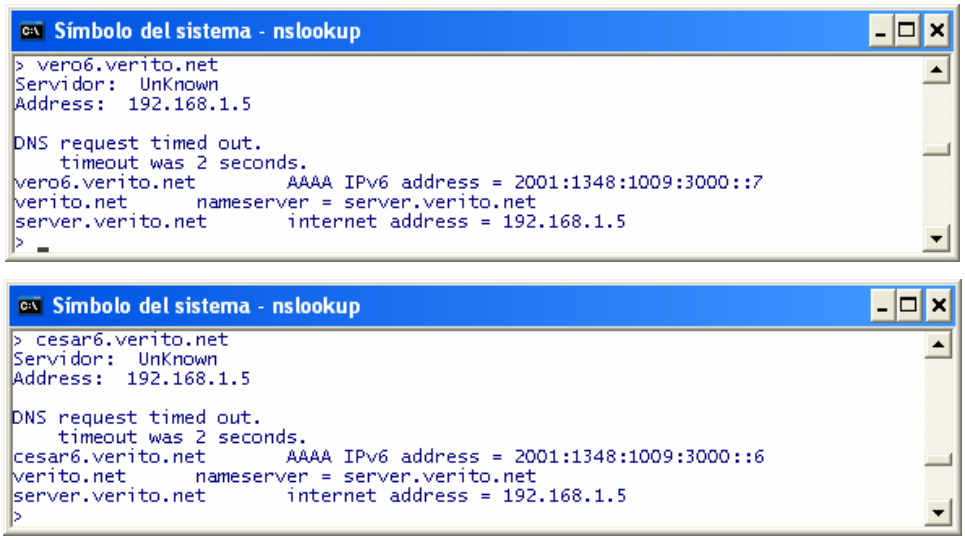


Fig. 3.50 Comando nslookup

3.1.8 CONFIGURACIONES POSIBLES DEL PROTOTIPO DE RED

El prototipo de red mostrado en la figura 3.4 puede ser configurado de tres formas posibles:

1. Considerando a todo el prototipo como una sola red; esto no es posible ya que el router presenta un mensaje de error de longitud del prefijo, al tratar de asignar una dirección a la interfaz serial, luego de haber asignado una dirección a la interfaz ethernet y viceversa. Para hacer que funcione como una sola red no es necesario hacer uso de los dos routers es suficiente con uno solo, ver figura 3.51
2. Considerando a cada uno de los segmentos como si fueran tres redes diferentes con una dirección especifica, ver figura 3.52.
3. Considerando a cada uno de los segmentos como si fueran subredes, ver figura 3.54.

Para lo cual en las siguientes figuras se muestra el prototipo de red para cada una de estas formas de configuración con sus respectivas direcciones IP.

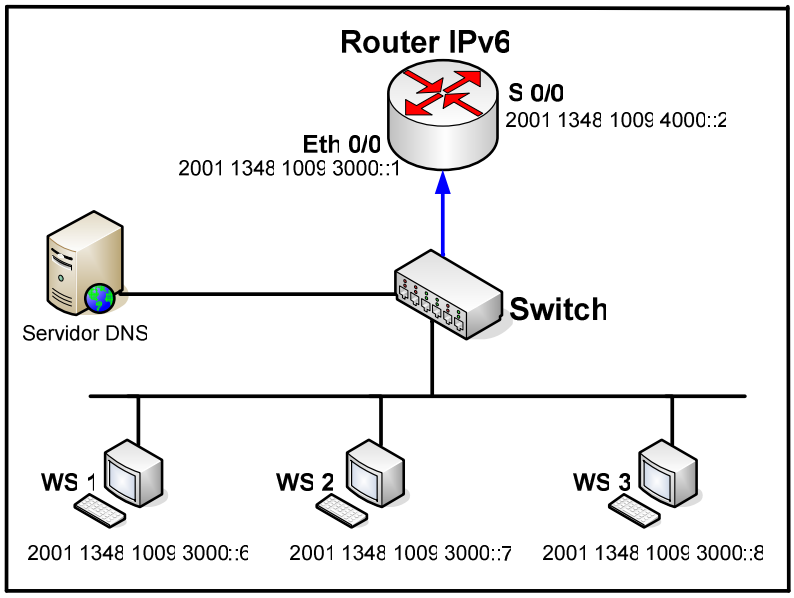


Fig. 3.51 Prototipo de Red considerado como Una Sola Red

Este prototipo fue utilizado anteriormente para realizar la Autoconfiguración con anuncio de prefijo.

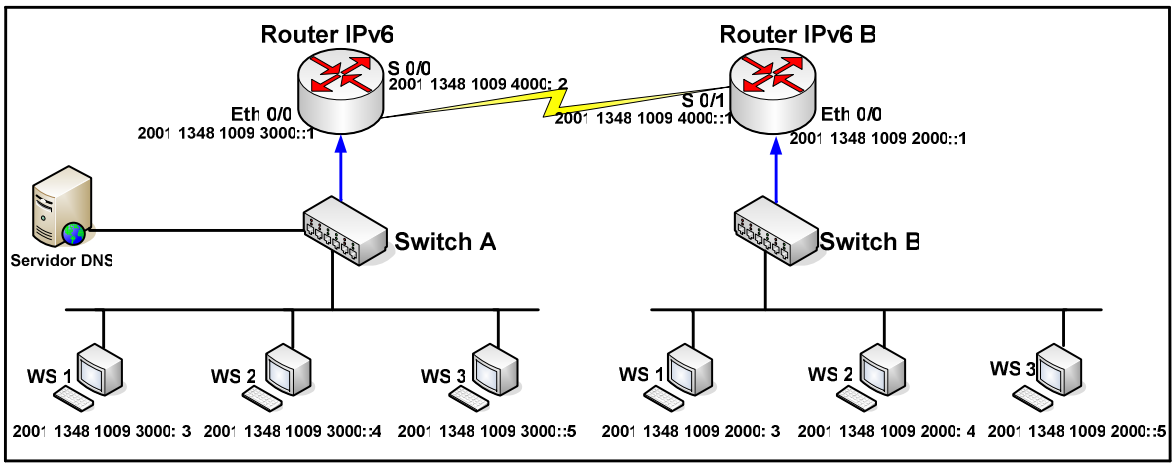


Fig. 3.52 Prototipo de Red considerado como Redes Diferentes

Comprobación de la Conectividad

A continuación se muestra la conectividad de la red desde los routers.

CuencaV#ping ipv6 2001:1348:1009:3000::1

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 2001:1348:1009:3000::1, timeout is 2 seconds: !!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms

CuencaV#ping ipv6 2001:1348:1009:3000::3
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:1348:1009:3000::3, timeout is 2 seconds: !!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms

CuencaV#ping ipv6 2001:1348:1009:4000::2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:1348:1009:4000::2, timeout is 2 seconds: !!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms

CuencaV#ping ipv6 2001:1348:1009:4000::1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:1348:1009:4000::1, timeout is 2 seconds: !!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 32/33/37 ms

CuencaV#ping ipv6 2001:1348:1009:2000::1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:1348:1009:2000::1, timeout is 2 seconds: Success rate is 100 percent (5/5), round-trip min/avg/max = 32/32/33 ms

CuencaV#ping ipv6 2001:1348:1009:2000::3
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:1348:1009:2000::3, timeout is 2 seconds: !!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 32/32/33 ms

MantaV#ping ipv6 2001:1348:1009:2000::1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:1348:1009:2000::1, timeout is 2 seconds:

Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms

MantaV#ping ipv6 2001:1348:1009:2000::3
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:1348:1009:2000::3, timeout is 2 seconds:
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms

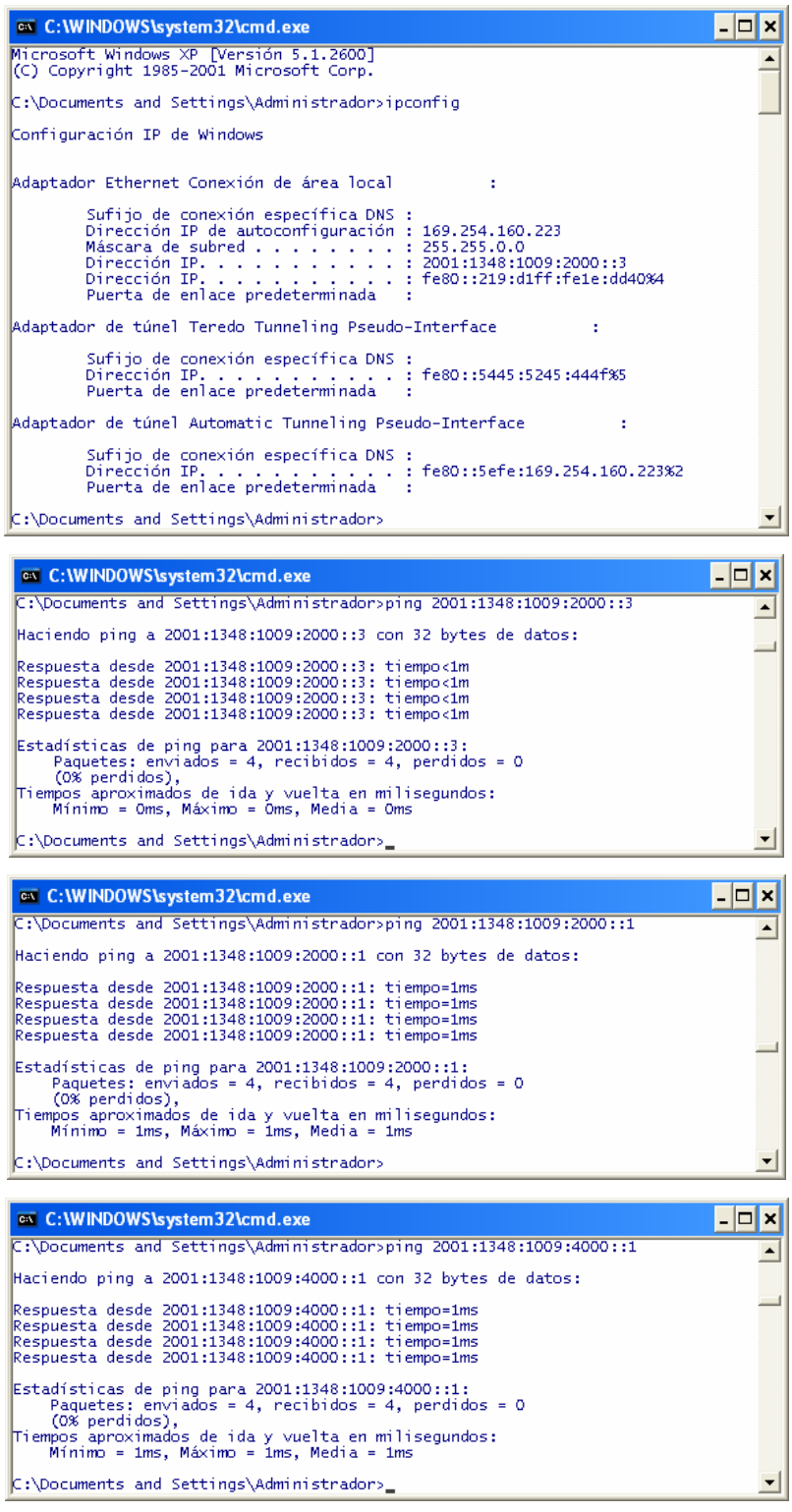
MantaV#ping ipv6 2001:1348:1009:3800::4000::1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:1348:1009:4000::1, timeout is 2 seconds:
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms

MantaV#ping ipv6 2001:1348:1009:4000::2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:1348:1009:4000::2, timeout is 2 seconds:
Success rate is 100 percent (5/5), round-trip min/avg/max = 32/33/37 ms

MantaV#ping ipv6 2001:1348:1009:3000::1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:1348:1009:3000::1, timeout is 2 seconds:
Success rate is 100 percent (5/5), round-trip min/avg/max = 32/33/36 ms

MantaV#ping ipv6 2001:1348:1009:3000::3
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:1348:1009:3000::3, timeout is 2 seconds:
Success rate is 100 percent (5/5), round-trip min/avg/max = 32/32/32 ms

En la figura 3.53 se muestra la configuración y conectividad de la red desde uno de los host hacia las interfaces de los routers y a otro host existente en la otra subred.



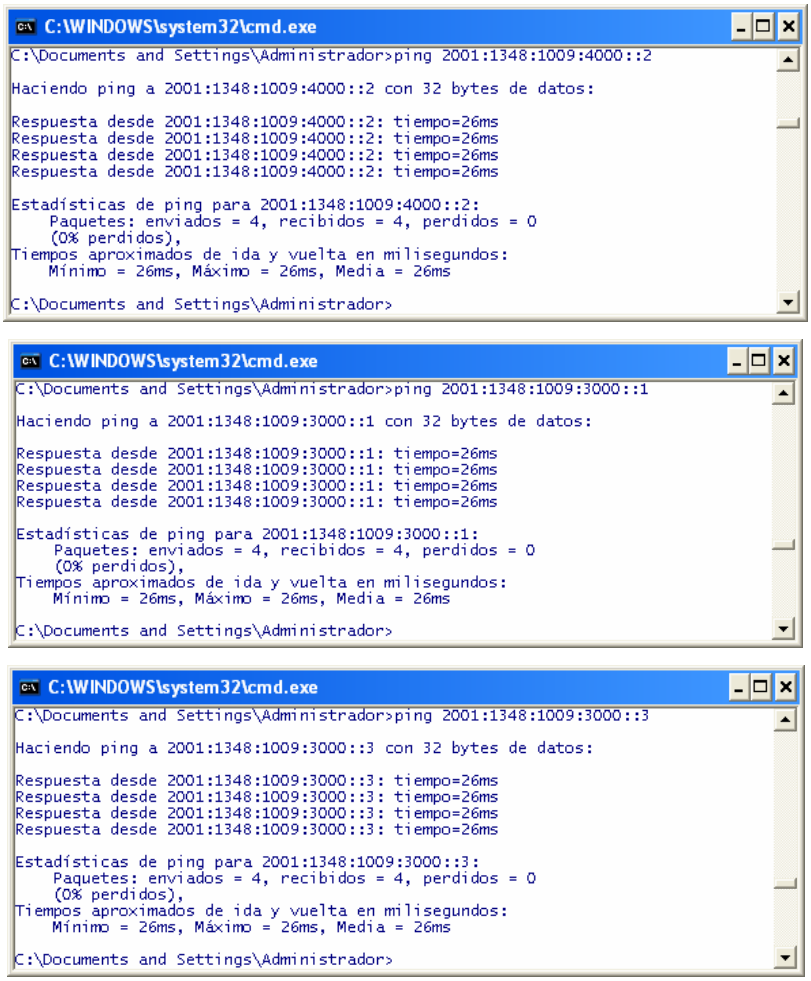


Fig. 3.53 Conectividad de interfaces

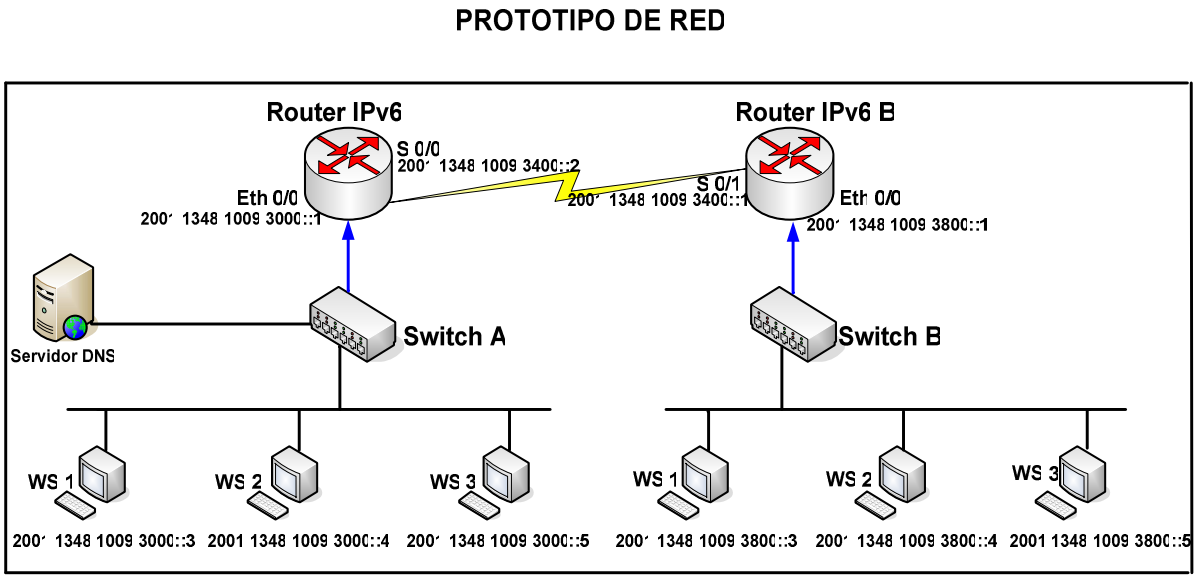


Fig. 3.54 Prototipo de Red considerado como Subredes

Comprobación de la Conectividad

A continuación se muestra la conectividad de la red desde los routers.

MantaV#ping ipv6 2001:1348:1009:3800::1

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 2001:1348:1009:3800::1, timeout is 2 seconds:

Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms

MantaV#ping ipv6 2001:1348:1009:3800::3

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 2001:1348:1009:3800::3, timeout is 2 seconds:

Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms

MantaV#ping ipv6 2001:1348:1009:3800::3400::1

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 2001:1348:1009:3400::1, timeout is 2 seconds:

Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms

MantaV#ping ipv6 2001:1348:1009:3400::2

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 2001:1348:1009:3400::2, timeout is 2 seconds:

Success rate is 100 percent (5/5), round-trip min/avg/max = 32/33/37 ms

MantaV#ping ipv6 2001:1348:1009:3000::1

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 2001:1348:1009:3000::1, timeout is 2 seconds:

Success rate is 100 percent (5/5), round-trip min/avg/max = 32/33/36 ms

MantaV#ping ipv6 2001:1348:1009:3000::3

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:1348:1009:3000::3, timeout is 2 seconds:
Success rate is 100 percent (5/5), round-trip min/avg/max = 32/32/32 ms

CuencaV#ping ipv6 2001:1348:1009:3000::1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:1348:1009:3000::1, timeout is 2 seconds:
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms

CuencaV#ping ipv6 2001:1348:1009:3000::3
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:1348:1009:3000::3, timeout is 2 seconds:
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms

CuencaV#ping ipv6 2001:1348:1009:3000::3400::2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:1348:1009:3400::2, timeout is 2 seconds:
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms

CuencaV#ping ipv6 2001:1348:1009:3400::1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:1348:1009:3400::1, timeout is 2 seconds:
Success rate is 100 percent (5/5), round-trip min/avg/max = 32/32/36 ms

CuencaV#ping ipv6 2001:1348:1009:3800::1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:1348:1009:3800::1, timeout is 2 seconds:

Success rate is 100 percent (5/5), round-trip min/avg/max = 32/33/37 ms

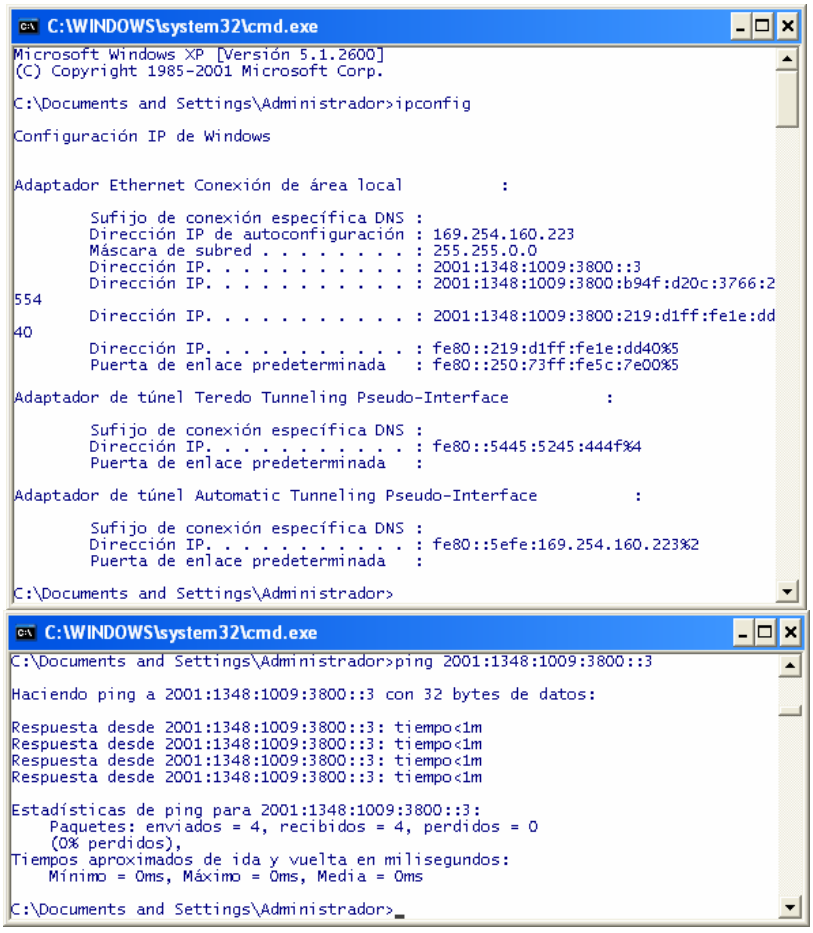
CuencaV#ping ipv6 2001:1348:1009:3800::3

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 2001:1348:1009:3800::3, timeout is 2 seconds:

Success rate is 100 percent (5/5), round-trip min/avg/max = 32/32/32 ms

En la figura 3.55 se muestra la configuración y conectividad de la red desde uno de los host hacia las interfaces de los routers y a otro host existente en la otra subred.



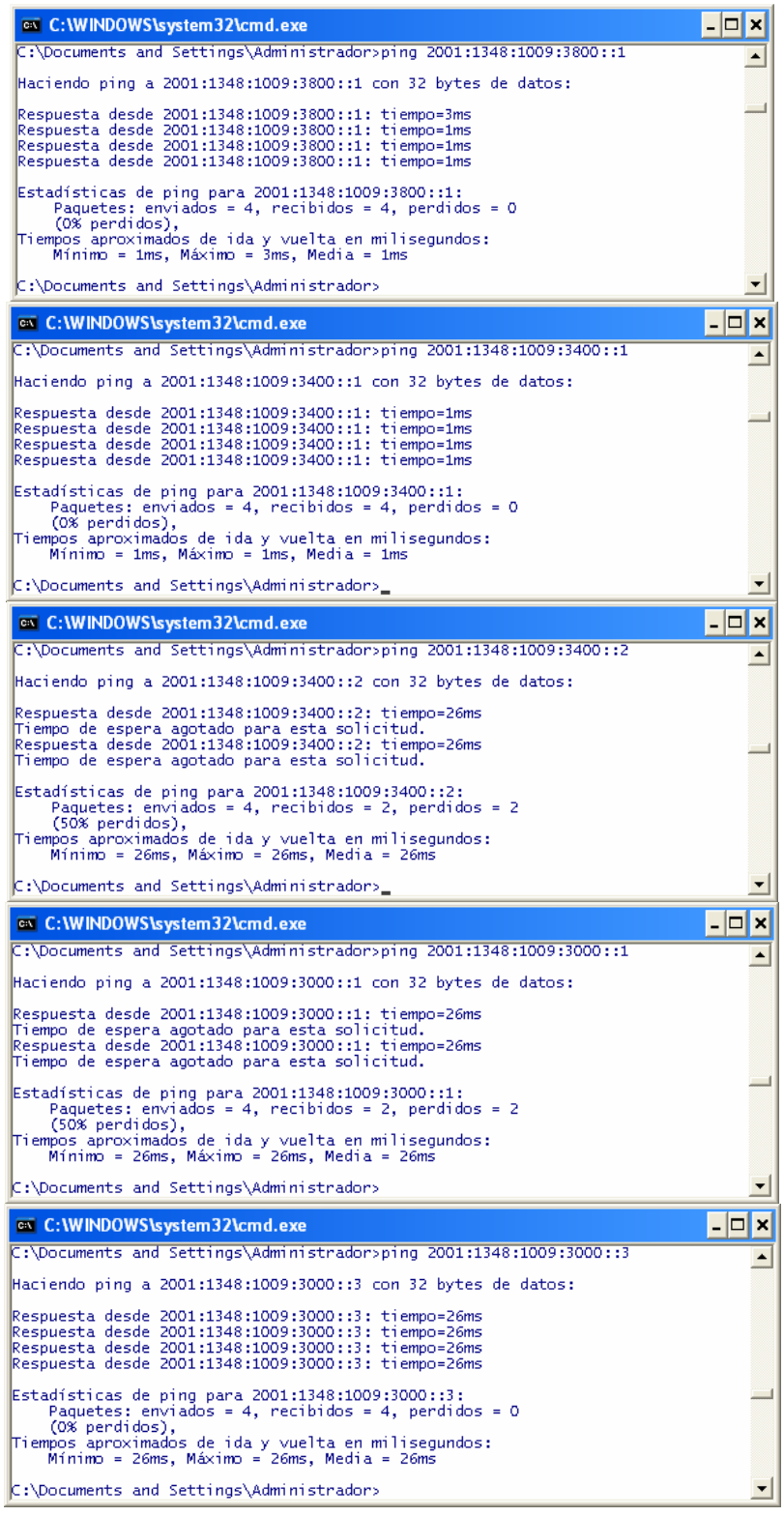


Fig. 3.55 Conectividad de interfaces

3.2 IMPLEMENTACION DE IPv6 EN EL LTI

Para implementar una red con el protocolo IPv6 es necesario contar con algunos requerimientos principales tanto en hardware como en software los cuales deben ser capaces de soportar este protocolo, estos requerimientos ya fueron detallados en la tabla 3.3. Adicionalmente se debe solicitar una dirección IPv6 a la entidad respectiva, para el caso de la E.P.N. han solicitado a CEDIA *(Consorcio Ecuatoriano para el Desarrollo de Internet Avanzado)* la misma que ha asignado la siguiente dirección: ***2800:68:11::/48***.

La UGI tiene un esquema gráfico de direccionamiento el cual consiste en generar subredes distribuidas por cada uno de los switch existentes, estos dispositivos constan de una determinada dirección con un prefijo de */60*, en estos dispositivos se ha creado las *Vlan (Virtual Local Network)* correspondientes, dentro de cada una de estas vlans existen adicionalmente *6* subredes las que necesitan de 4 bits adicionales para su direccionamiento, lo que implica tener 16 redes con un prefijo de */64* para cada switch. En la figura 3.56 se muestra las subredes que forman parte de la Polired; y en las siguientes tablas (3.4, 3.5, 3.6, 3.7, 3.8) se indican las Vlans creadas en cada switch.

Tabla 3.4: Vlans del switch DELECTRIC **[11]**

RED	VLAN	DIR. DE RED	DIR. DE VLAN
delectric		2800:68:11:10::/60	
	Monitoreo		2800:68:11:10::/64
	Profesores		2800:68:11:11::/64
	Estudiantes		2800:68:11:12::/64
	Investigación		2800:68:11:13::/64
	Administrativo		2800:68:11:14::/64
	SAE		2800:68:11:15::/64

Tabla 3.5: Vlans del switch DMECANICA **[11]**

RED	VLAN	DIR. DE RED	DIR. DE VLAN
dmecanica		2800:68:11:20::/60	
	Monitoreo		2800:68:11:20::/64
	Profesores		2800:68:11:21::/64
	Estudiantes		2800:68:11:22::/64
	Investigación		2800:68:11:23::/64
	Administrativo		2800:68:11:24::/64
	SAE		2800:68:11:25::/64

Tabla 3.6: Vlans del switch DSISTEMAS **[11]**

RED	VLAN	DIR. DE RED	DIR. DE VLAN
dsistemas		2800:68:11:30::/60	
	Monitoreo		2800:68:11:30::/64
	Profesores		2800:68:11:31::/64
	Estudiantes		2800:68:11:32::/64
	Investigación		2800:68:11:33::/64
	Administrativo		2800:68:11:34::/64
	SAE		2800:68:11:35::/64

Tabla 3.7: Vlans del switch DCIVIL **[11]**

RED	VLAN	DIR. DE RED	DIR. DE VLAN
dcivil		2800:68:11:40::/60	
	Monitoreo		2800:68:11:40::/64
	Profesores		2800:68:11:41::/64
	Estudiantes		2800:68:11:42::/64
	Investigación		2800:68:11:43::/64
	Administrativo		2800:68:11:44::/64
	SAE		2800:68:11:45::/64

Tabla 3.8: Vlans del switch DUGI **[11]**

RED	VLAN	DIR. DE RED	DIR. DE VLAN
dugi		2800:68:11:50::/60	
	Monitoreo		2800:68:11:50::/64
	Profesores		2800:68:11:51::/64
	Estudiantes		2800:68:11:52::/64
	Investigación		2800:68:11:53::/64
	Administrativo		2800:68:11:54::/64
	SAE		2800:68:11:55::/64

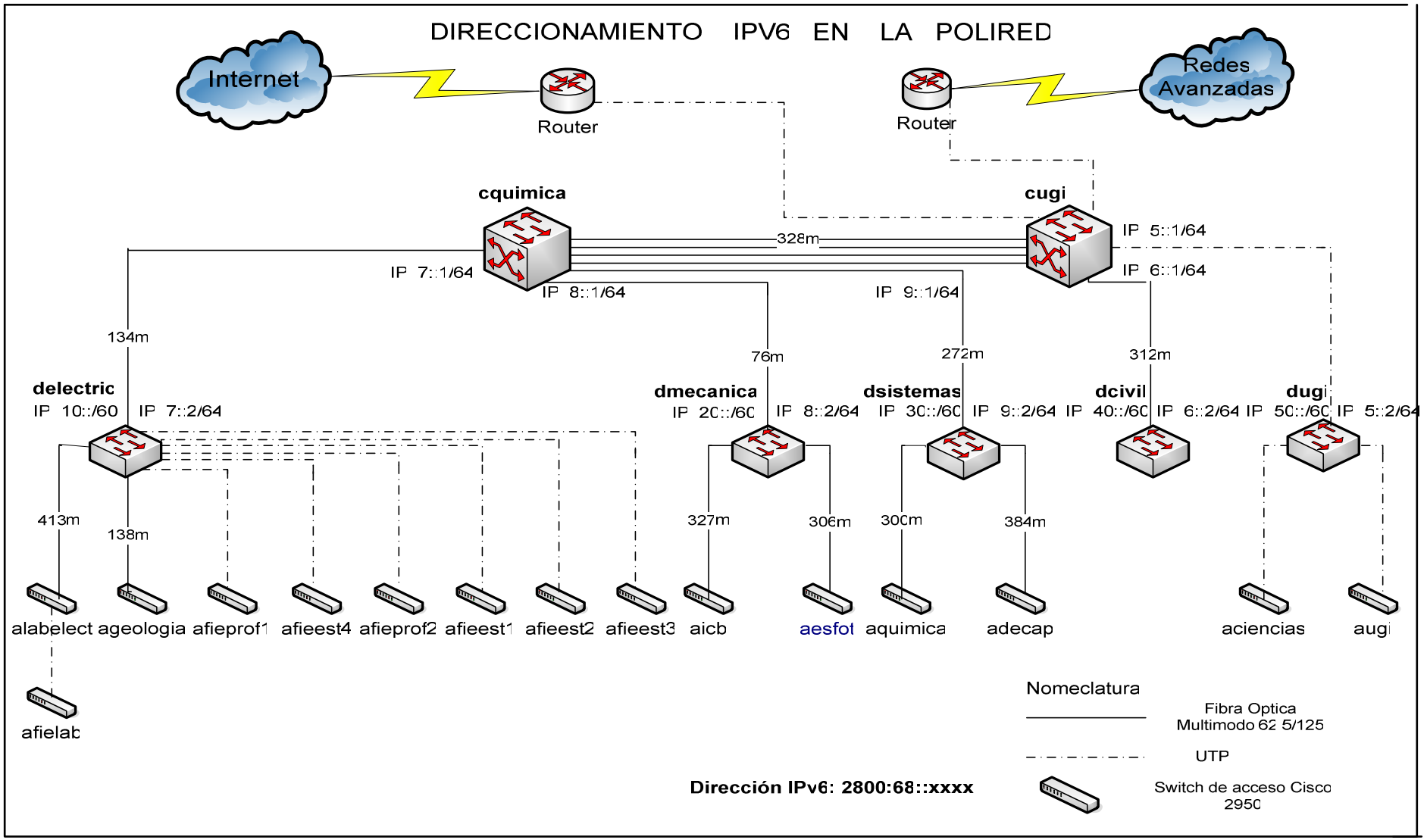


Fig. 3.56 Direccionamiento IPv6 en la Polired **[11]**

Luego de realizar el esquema gráfico, la UGI debe asignar las direcciones a cada uno de los dispositivos de red y en los host de toda la red para lo cual esta unidad debe establecer las políticas para el direccionamiento.
El LTI por ser una subred de la Polired debe acogerse a las políticas de configuración de red establecidas por la UGI ya que es esta unidad la encargada de asignar las direcciones tanto para el protocolo IPv4 como del protocolo IPv6, por tanto la UGI ha decidido implementar el protocolo IPv6 en el LTI basándose en sus políticas de configuración de las direcciones, las cuales son las siguientes:

a) Subneteando la dirección de red principal,
b) Distribución en forma automática de las direcciones, y
c) Asignando eventualmente de forma manual dichas direcciones.

En base a estas políticas se han estado administrado la distribución de la direcciones del protocolo IPv4, para el caso del protocolo IPv6 hasta el momento se esta actuando en base a las políticas a y b.

Algunos de los host que forman parte de la Polired y que ya tienen implementado el protocolo IPv6, se encuentran trabajando en forma Dual Stack *(doble pila).*

Las formas de configuración de red para el protocolo IPv6 son las siguientes:

- Autoconfiguración sin Estado *(Stateless Configuration)*
  - Asignación de direcciones *link-local*
  - Anuncio de Prefijos
- Autoconfiguración con Estado *(Stateful Configuration)*
  - DHCPv6
- Configuración Manual

En la sección 3.17 están detalladas todas estas formas de configuración, luego de las comprobaciones se puede concluir que las formas de configuración más utilizadas en la actualidad son: la autoconfiguración sin estado con anuncio de prefijos y la configuración manual.

La UGI para la distribución de las direcciones IPv6 en la Polired esta haciendo uso de la configuración de red "*autoconfiguración sin estado mediante el anuncio de prefijos"*. Esta forma de configuración consiste en que un host recibe por parte del router un prefijo de red el cual no ocupa todos los 128 bits de una dirección IPv6, para el caso de la E.P.N. el prefijo esta formado de 64 bits, los 64 bits restantes se completan con algunos de los valores de la dirección física de la maquina y otros valores aleatorios. Para la asignación de los prefijos hay que configurar previamente al router de forma *manual*. El prefijo de red para el LTI es ***2800:68:11:52::/64.***

Para que cada una de las máquinas del LTI reciban este prefijo es necesario instalar el protocolo IPv6 mediante el comando *ipv6 install* en la consola del sistema DOS, para mayor información referirse a la sección 3.17*.*

A diferencia de las direcciones IPv6, las direcciones IPv4 son distribuidas para toda la Polired mediante un servidor *DHCPv4* que al igual que el router se encuentran físicamente en la unidad de gestión de direcciones.

La dirección IPv6 que administra la UGI y la mayoría de direcciones IPv6 son direcciones públicas, las direcciones especiales son utilizadas solamente para realizar pruebas, ya que el protocolo IPv6 a diferencia del protocolo IPV4 no realiza el proceso de NAT; por que el protocolo IPv6 tiene muchas direcciones para satisfacer las necesidades del usuario, sin embargo estas direcciones si pueden ser subneteadas para efectos de administración.

La configuración de la red LTI con el protocolo IPv6 hasta la actualidad es el mostrado en la figura 3.57.

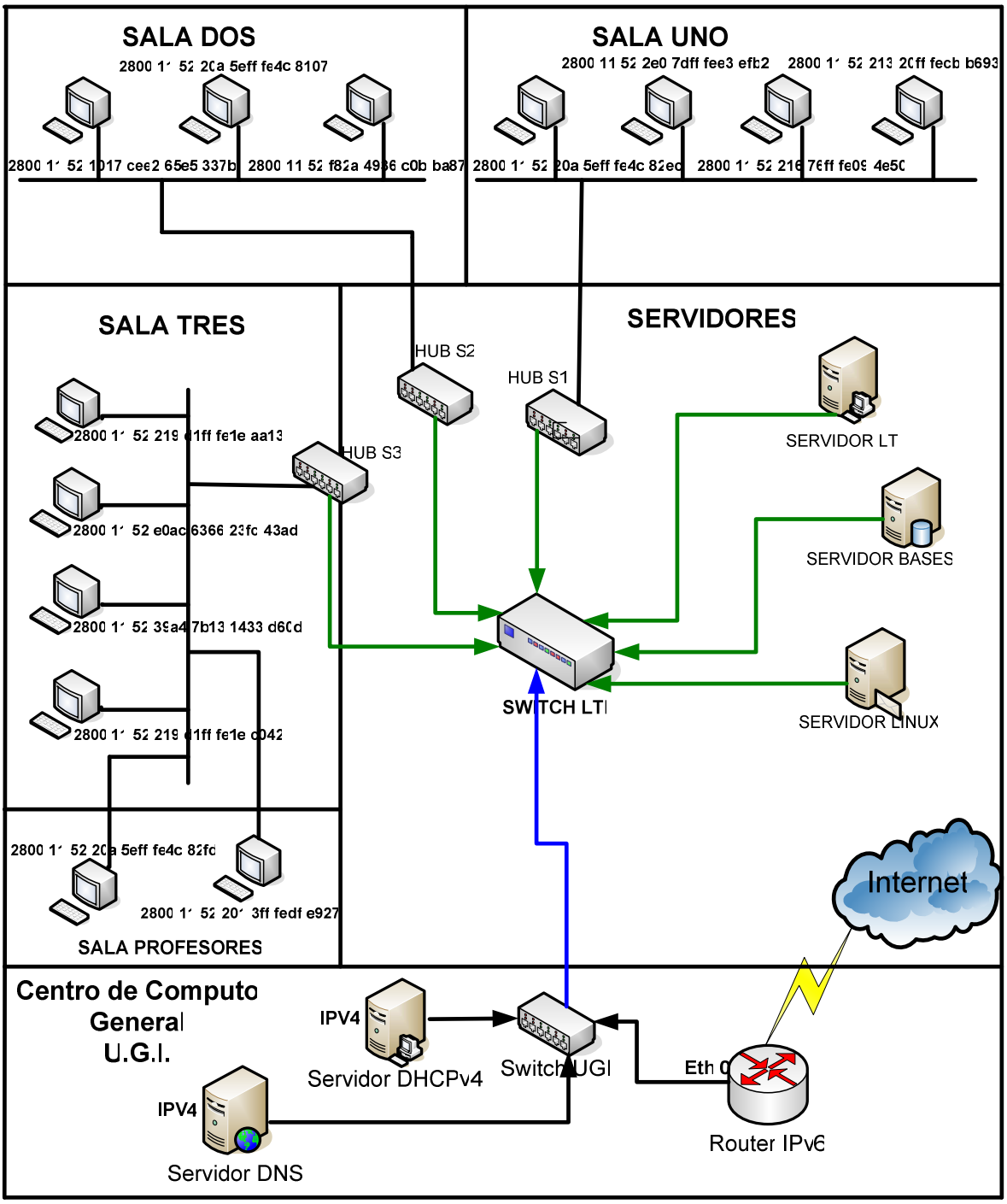
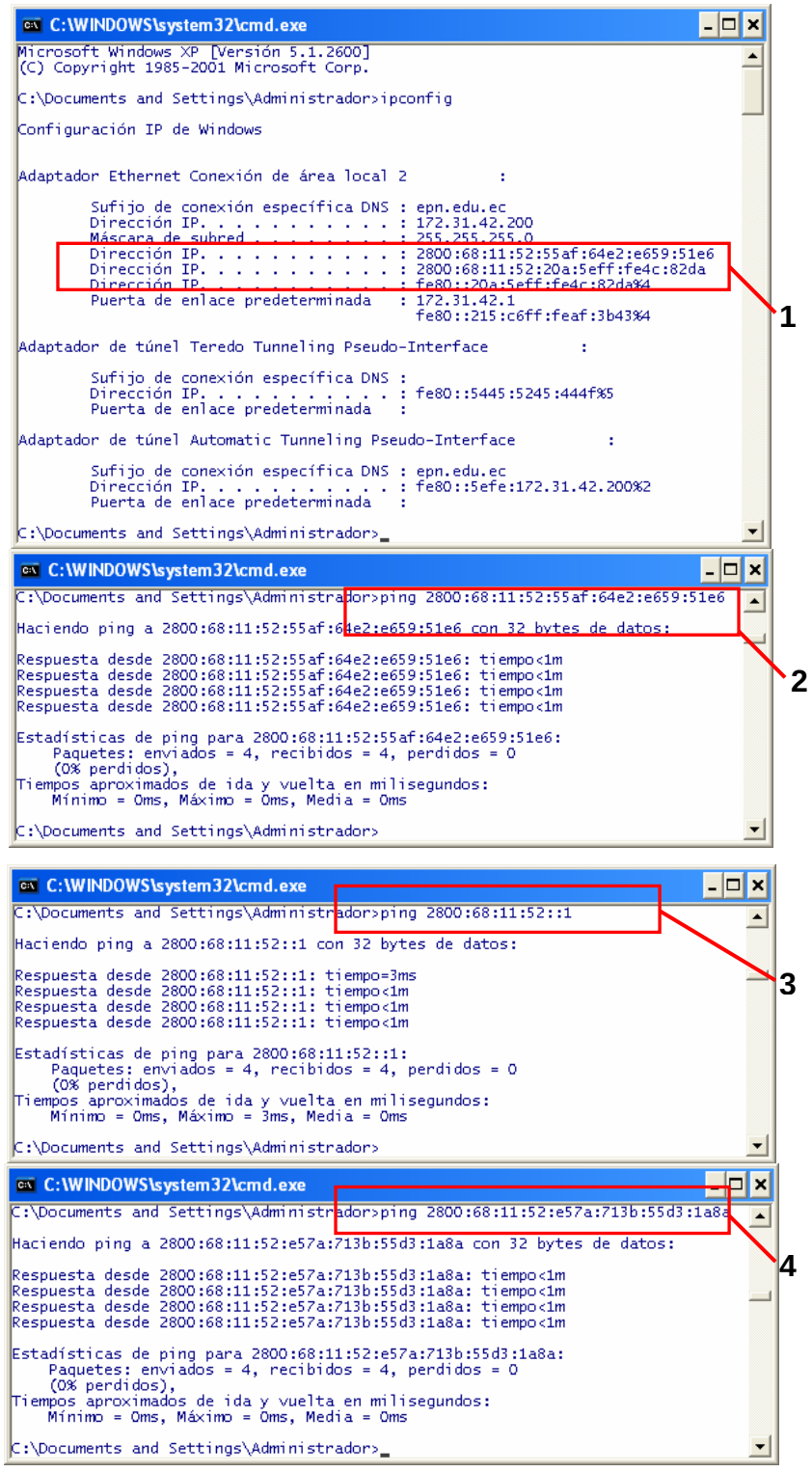


Fig. 3.57 Red LTI con IPv6

Comprobación de la Conectividad de la red LTI

En la figura 3.58 se muestra la comprobación de la conectividad desde una máquina situada en la sala UNO a otras máquinas de la misma sala, a la dirección de enlace de la UGI y a las máquinas que se encuentran en las diferentes salas, siguiendo los siguientes pasos:

1. Se ejecuta el comando *ipconfig* para visualizar las direcciones asignadas.
2. Se ejecuta el comando *ping* a la dirección de la propia máquina.
3. Se ejecuta el comando *ping* a la dirección de enlace.
4. Se ejecuta el comando *ping* a direcciones de otras máquinas.



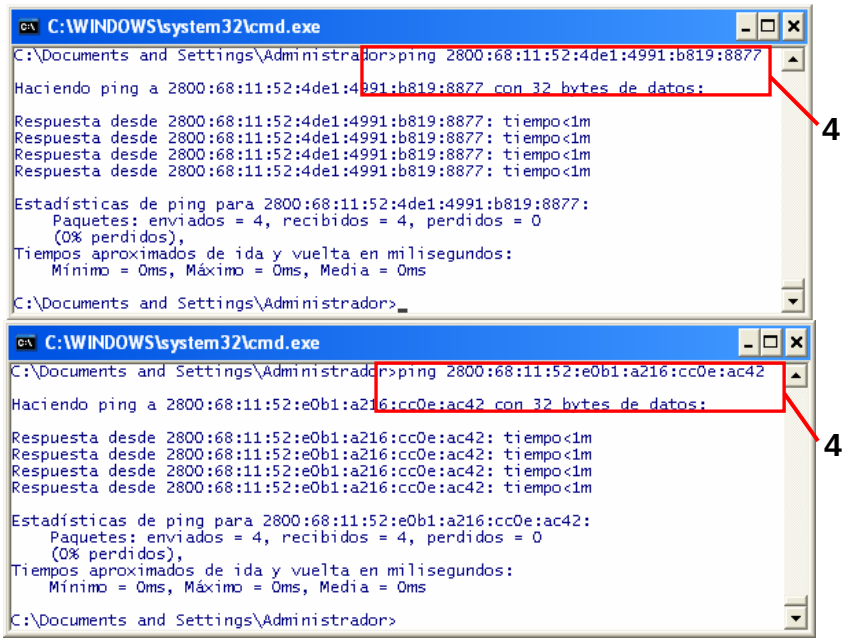
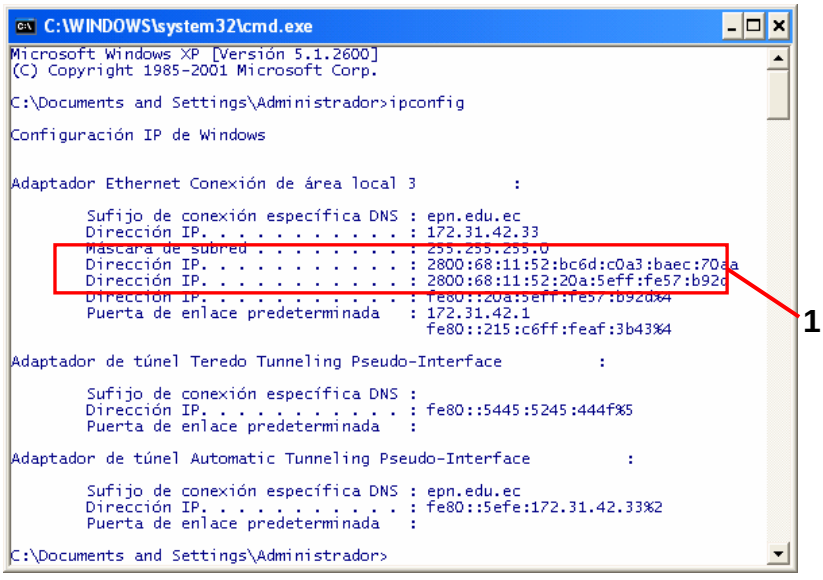


Fig. 3.58 Conectividad desde la sala uno

En la figura 3.59 se muestra la comprobación de la conectividad desde una máquina situada en la sala DOS a otras máquinas de la misma sala, a la dirección de enlace de la UGI y a las máquinas que se encuentran en las diferentes salas, siguiendo los pasos anteriormente mencionados:



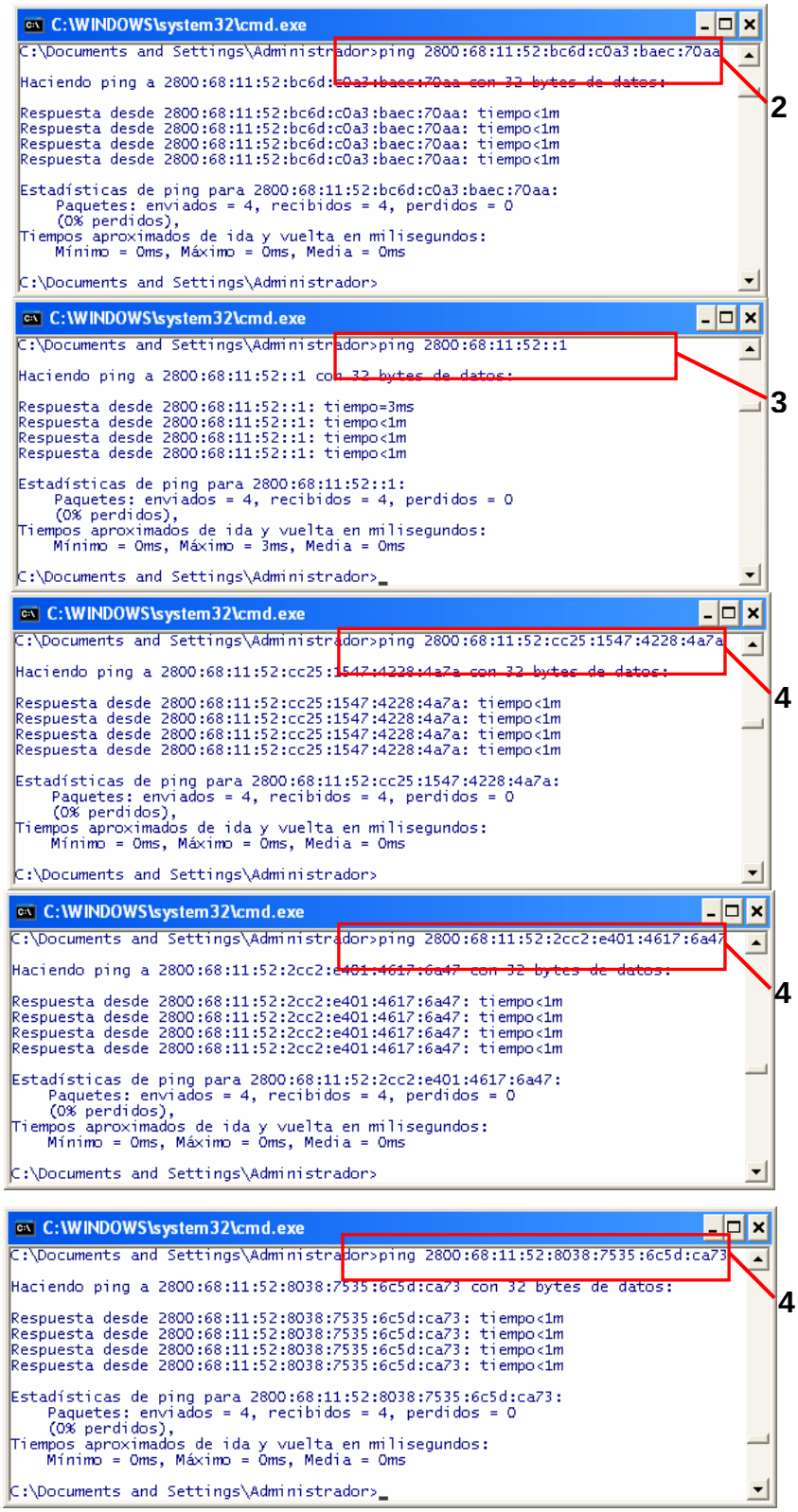
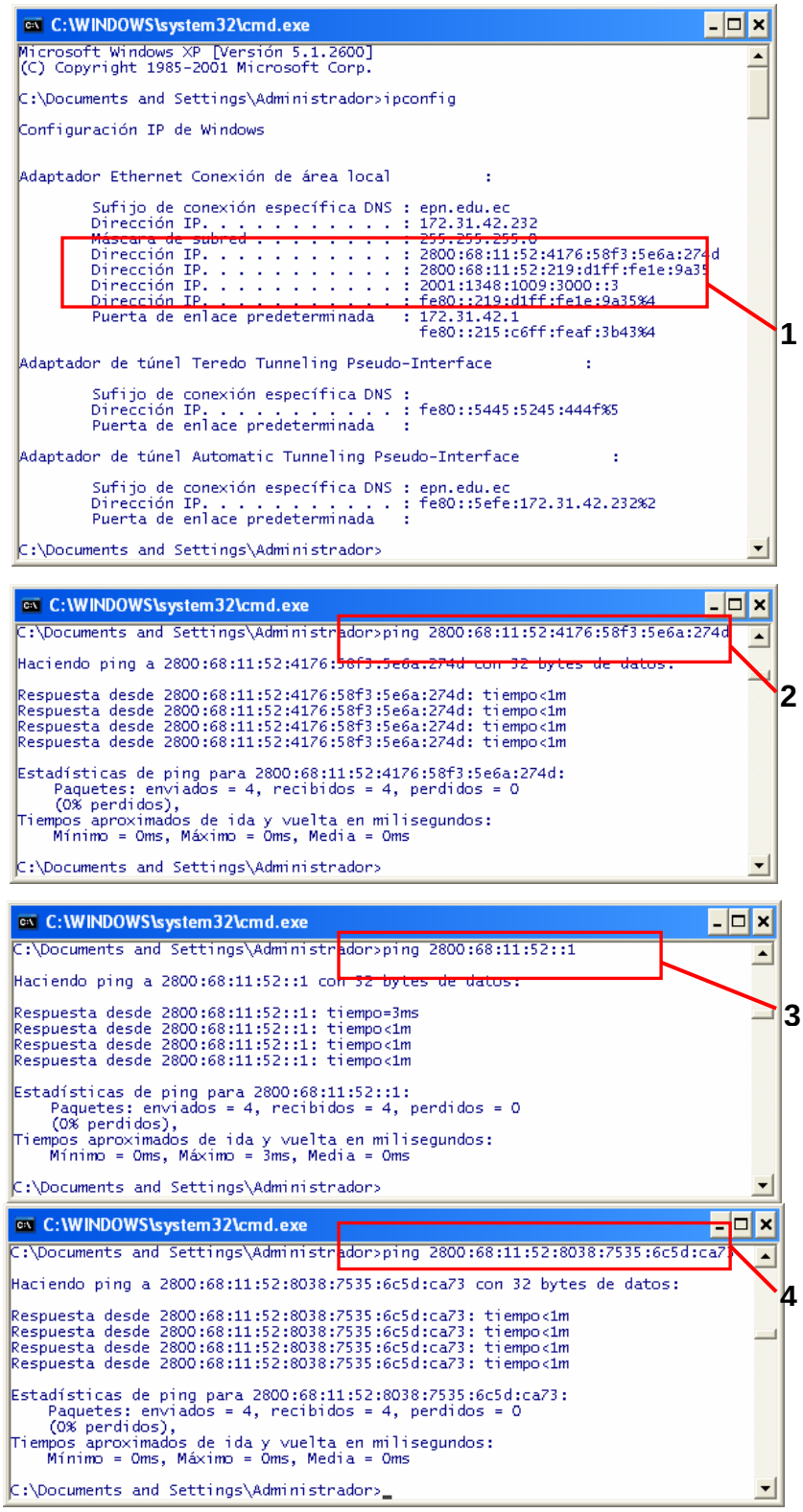


Fig. 3.59 Conectividad desde la sala dos

En la figura 3.60 se muestra la comprobación de la conectividad desde una máquina situada en la sala TRES a otras máquinas de la misma sala, a la

dirección de enlace de la UGI y a las máquinas que se encuentran en las diferentes salas, siguiendo los pasos mencionados anteriormente:



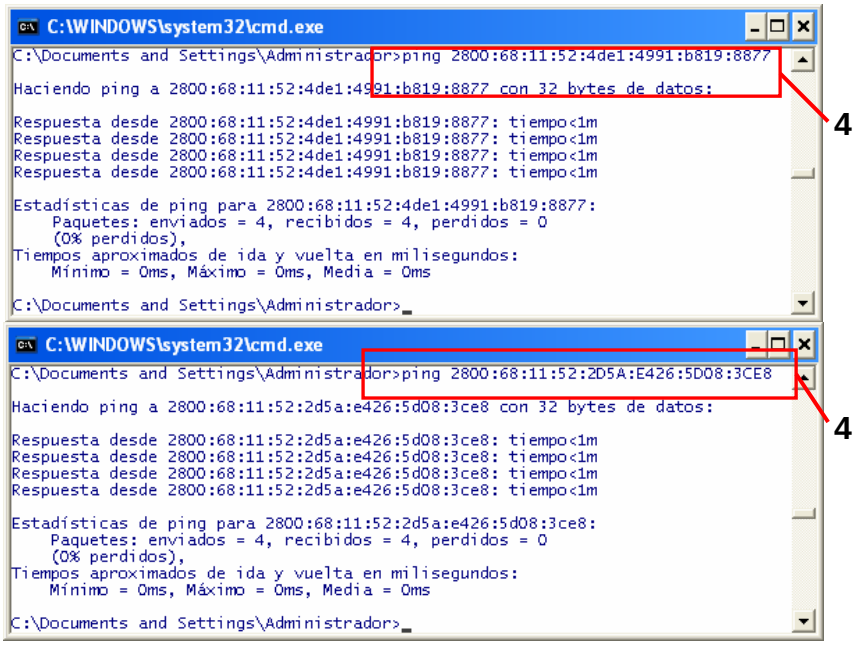
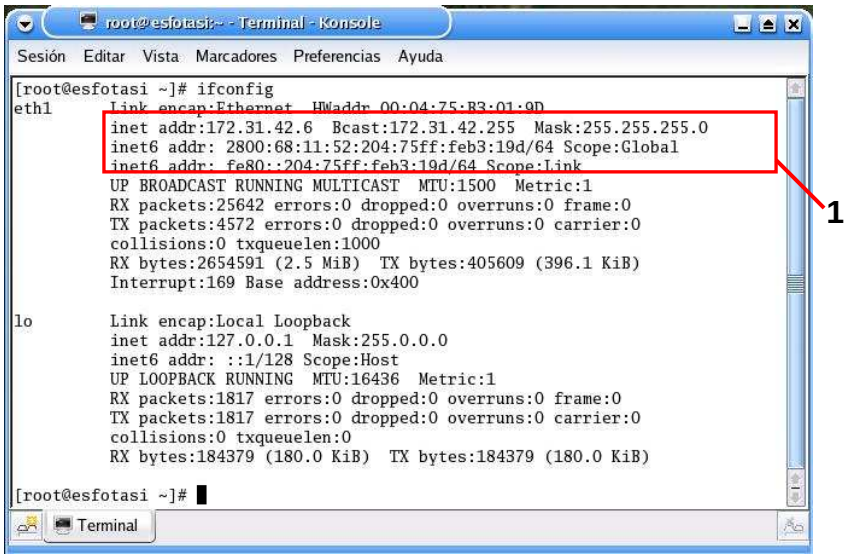


Fig. 3.60 Conectividad desde la sala tres

En la figura 3.61 se muestra la comprobación de la conectividad de los servidores entre sí situados en la sala de SERVIDORES y a otras máquinas de las diferentes salas, siguiendo los siguientes pasos:

1. Se ejecuta el comando *ipconfig* para visualizar las direcciones asignadas.
2. Se ejecuta el comando *ping* a la dirección de la propia máquina.
3. Se ejecuta el comando *ping* a direcciones de otros servidores.
4. Se ejecuta el comando *ping* a direcciones de otras máquinas



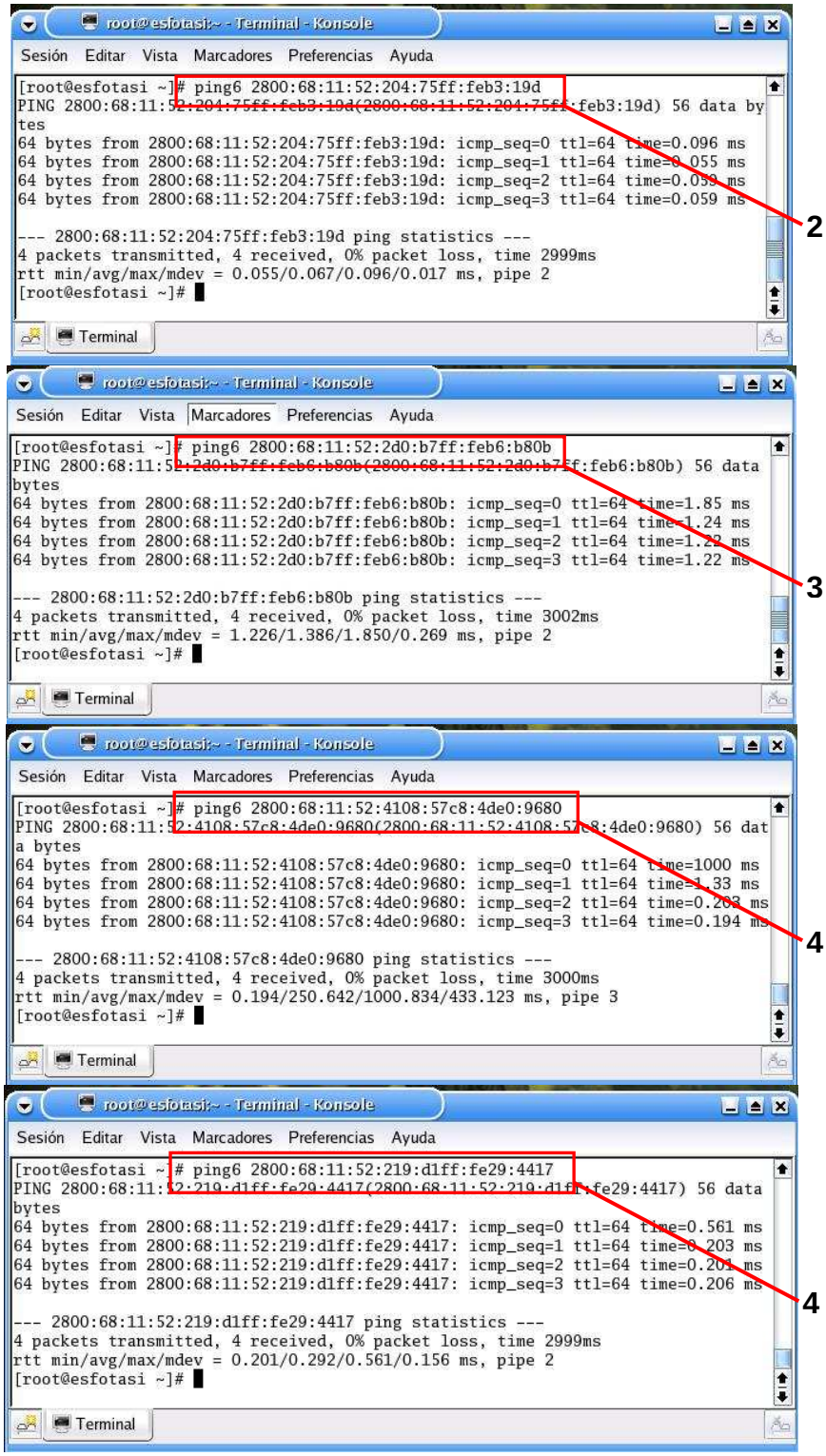


Fig. 3.61 Conectividad desde la sala de Servidores

Comprobación de la Conectividad con Internet

Para comprobar la conectividad con Internet en la figura 3.62 se muestra el acceso al sitio Web de la Escuela Politécnica Nacional mediante el protocolo IPv6 mediante el URL *www2.epn.edu.ec,* en este caso en la parte superior de la pagina web nos muestra la dirección de la máquina de la cual estamos accediendo al sitio web la cual es *2800:68:11:52:f90a:de40:90b2:c8d4*.

Fig. 3.62 Conectividad con Internet

3.3 OBTENCION DE DIRECCIONES IPV6

Los RIRs *(Registradores de Internet Regional)* se establecieron durante 1990 como organizaciones sin fines de lucro, y son los encargados de asignar los recursos de números de Internet como son las direcciones IP y de los sistemas autónomos dentro de sus regiones, los cuales son requeridos por los ISPs *(Proveedores de Servicio de Internet)* y de usuarios finales para identificar los elementos de la infraestructura de Internet.

ICANN.- Responsable por la administración global de los recursos de Internet (Direcciones IP, ASN). Su autoridad proviene a través del Departamento de Comercio de los Estados Unidos. IANA es una parte del ICANN.

Existen varios RIRs como:

Internet Registry (IR): Responsable de la distribución de espacios de direcciones IP y registración de esa distribución.

Regional Internet Registry (RIR): Representan, administran y distribuyen a grandes regiones geográficas (ARIN, APNIC, RIPE, LACNIC, AFRINIC)

National Internet Registry (NIR): Asigna espacio de direcciones a sus miembros, generalmente ISP a nivel nacional y a sus usuarios finales.

Estos NIR existen mayormente en la región de Asia Pacífico y en Latinoamérica son México y Brasil.

Local Internet Registry (LIR) o ISP: Asigna espacio de direcciones a los usuarios de sus servicios de red los cuales son generalmente ISPs cuyos clientes son *usuarios finales* u otros ISPs

3.3.1 JERARQUIA DE LAS DELEGACIONES

Las direcciones IP's son administradas por diversas entidades según el orden de jerarquía presentado en la figura 3.63.

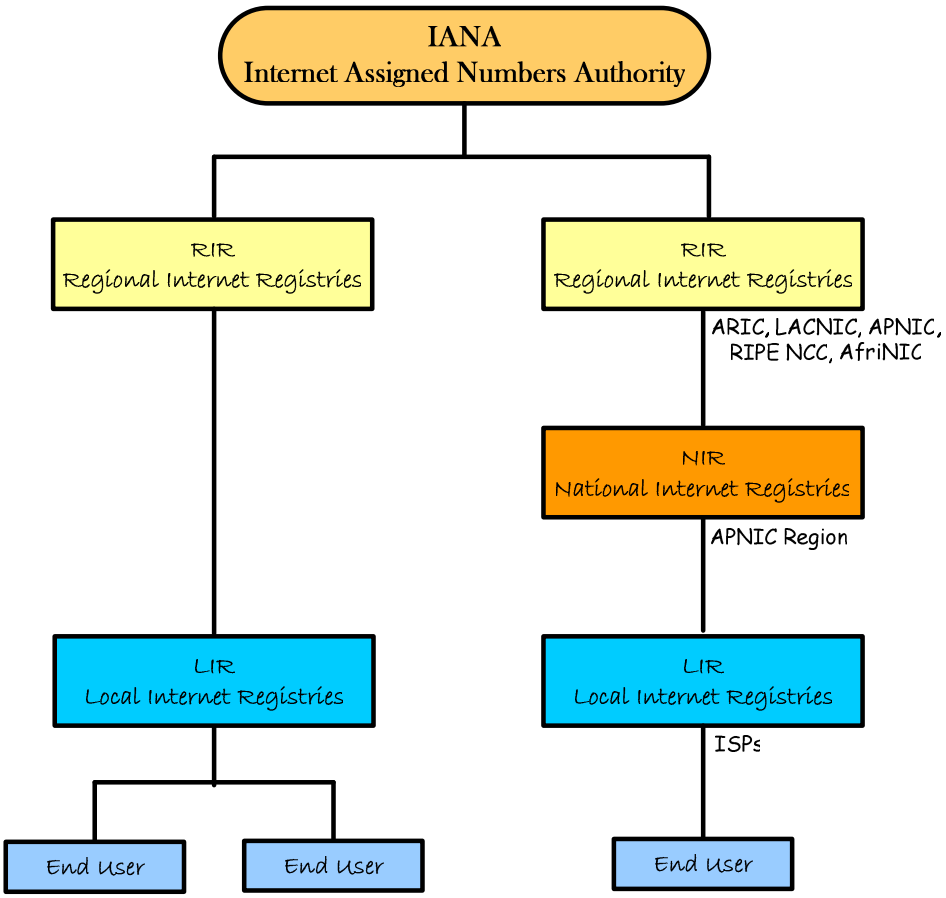
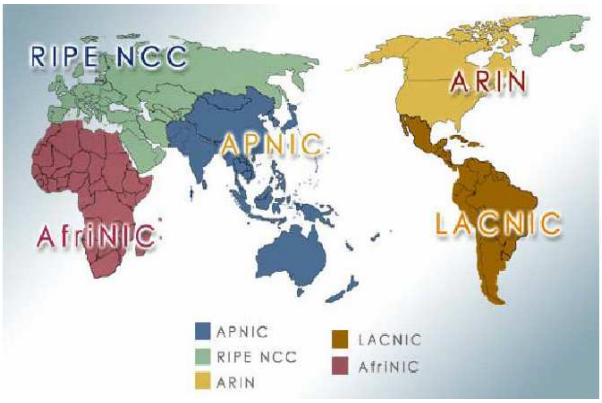


Fig. 3.63 RIRs en el mundo

IANA *(Internet Assigned Number Authority)* es la entidad de máxima jerarquía y se encarga de distribuir las IP en Internet a nivel mundial. IANA no otorga IP's a cualquier persona o empresa, sino que lo hace a través de otras entidades con jerarquía de segundo nivel y estas están repartidas por regiones:

APNIC - Registro de IP's para la región Asia Pacífico.
ARIN - Registro de IP's para América del Norte.
LACNIC - Registro de IP's para Latinoamérica y las islas del Caribe.
RIPE - Registro de IP's para Europa, Oriente Medio, Asia Central y países africanos del hemisferio norte.
AfriNIC – Registro de IP's para África

La figura 3.64 muestra la ubicación de varios registros regionales existentes a nivel mundial.



RIR	Office Location	Year established
APNIC	Brisbane, Australia	1993
ARIN	Chantilly, Virginia, USA	1997 (InterNIC established in 1993)
LACNIC	Montevideo, Uruguay	2002
RIPE NCC	Amsterdam, The Netherlands	1992
AfriNIC	Port-Louis, Mauritius	Emerging RIR

Fig. 3.64 Registros regionales **[15]**

En el tercer nivel de jerarquía se encuentran los Sistemas Autónomos y son quienes reciben los rangos de IP directamente de la entidad de su región. Los sistemas Autónomos tienen sus propias redes y conectividad.

Dattatec.com se encuentra en el tercer nivel de jerarquía y es un Sistema Autónomo que dispone de su propio bloque de IP's.

En el cuarto nivel se encuentran los ISP y la mayoría de las empresas de hosting que revenden los servicios de proveedores mayoristas.

Por último y en el quinto nivel están los usuarios finales que reciben una IP a la hora de conectarse a Internet o adquirir un servicio de hosting.

LACNIC fundada en 1999 es una organización sin fines de lucro reconocida como Organismo Internacional por el Gobierno, establecida en Uruguay.

Es la encargada de administrar los recursos de direccionamiento de Internet tanto como para América Latina como el Caribe asegurando equidad en el acceso de los recursos y con criterio de servicio de comunidad.

LACNIC se transformó en el cuarto RIR el 31 de Octubre del 2002 por resolución de la ICANN

Sus políticas se basan en un proceso “bottom-up” y membrecía abierta.

LACNIC basa su operación en tres objetivos fundamentales como la gestión de las direcciones IP aplicadas globalmente por los otros Registros de Internet:

- ✓ Agregación
- ✓ Conservación
- ✓ Registración

LACNIC brinda sus servicios en 29 territorios de América Latina y el Caribe, donde están incluidos:

- ✓ Antillas Holandesas
- ✓ Argentina
- ✓ Aruba
- ✓ Belice
- ✓ Bolivia
- ✓ Brasil
- ✓ Chile
- ✓ Colombia
- ✓ Costa Rica
- ✓ Cuba
- ✓ ***Ecuador***
- ✓ El Salvador
- ✓ Guyana Francesa
- ✓ Guatemala
- ✓ Guyana
- ✓ Haití
- ✓ Honduras
- ✓ Islas Falkland (Malvinas)
- ✓ México
- ✓ Nicaragua
- ✓ Panamá
- ✓ Paraguay
- ✓ Perú
- ✓ República Dominicana
- ✓ South Georgia and The South Sandwich Islands
- ✓ Suriname
- ✓ Trinidad y Tobago
- ✓ Uruguay
- ✓ Venezuela

LACNIC asigna bloques de direcciones IP en base a límites soportado por el esquema CIDR.

Asignaciones /24 en Ecuador

Las estadísticas de la asignación de direcciones IPv4 hasta el 29 de Junio de 2004, el cual fue de un total de 645 direcciones se muestra en la figura 3.65.

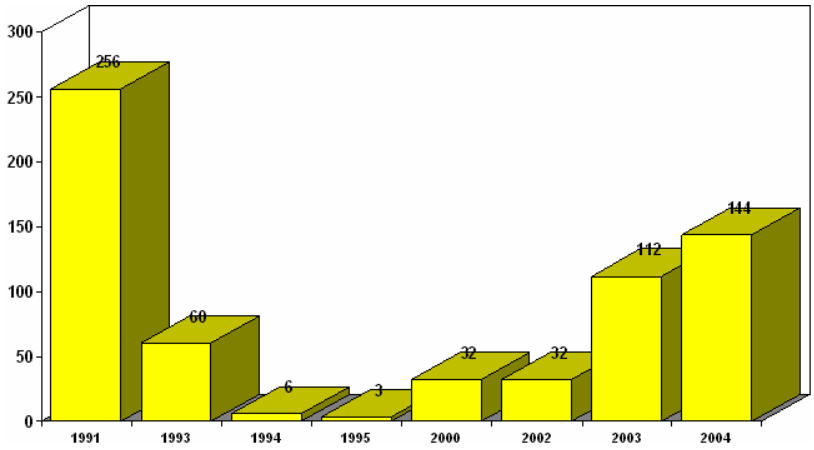


Fig. 3.65 Direcciones en Ecuador **[15]**

Hasta el 15 de Mayo del mismo año se realizaron 21 asignaciones de direcciones IPv6, pero inicialmente reciben una asignación de /32.

Las direcciones IP son válidas mientras se mantengan los objetivos de exclusividad, conservación, ruteabilidad e información. Estas asignaciones son renovadas cada año, en la figura 3.66 se muestra el proceso de asignación de las direcciones IP.

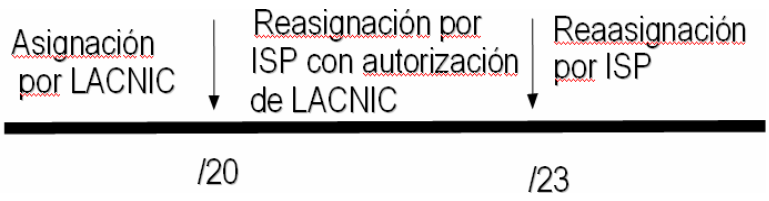


Fig. 3.66 Asignación de Direcciones IP **[15]**

Para la obtención un rango de direcciones IP se presenta la solicitud correspondiente y seguir el proceso mostrado en la figura 3.67

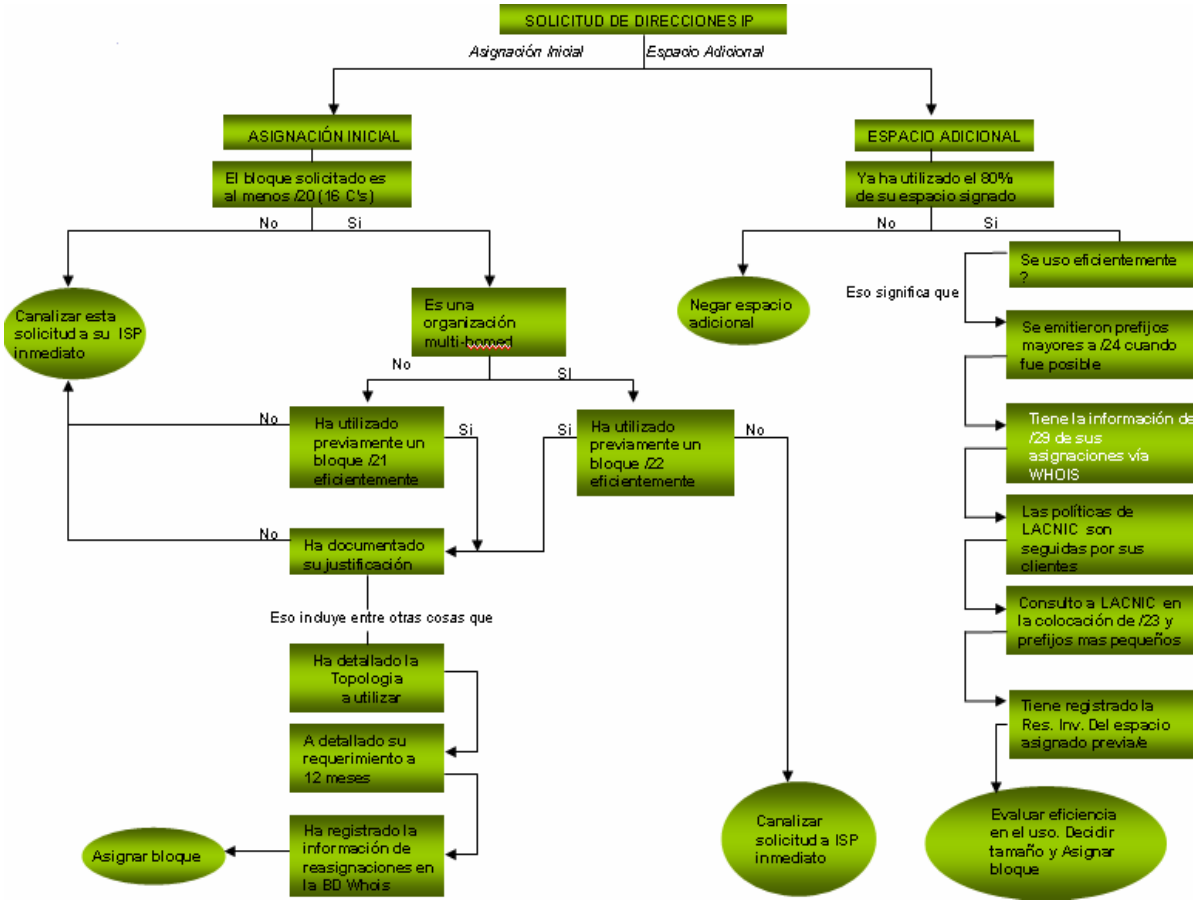


Fig. 3.67 Solicitud para la Adquisición de Direcciones **[15]**

CAPITULO 4: CONCLUSIONES Y RECOMENDACIONES

4.1 CONCLUSIONES

Luego del trabajo realizado en este proyecto, a continuación se muestra una serie de conclusiones respecto al protocolo IPv6 las cuales han sido ordenadas de acuerdo a las siguientes referencias: la cantidad de direcciones, a la migración hacia el nuevo protocolo, a las formas de configuración, a los servicios disponibles, a las aplicaciones, a la calidad de servicio y a la seguridad.
Esto con el objetivo de organizar de mejor manera las conclusiones.

Con respecto a las Direcciones.-

- √ La diferencia entre el protocolo IPv4 e IPv6 esta marcada por su capacidad. IPv4 usa solo 32 bits para su direccionamiento y esto es equivalente a (2^{32} = 4294967294) direcciones, mientras el protocolo IPv6 utiliza 128 bits (2^{128} = $3.4x10^{38}$) direcciones para cada nodo de una red, debido a esta gran cantidad de direcciones se podría decir que aproximadamente se pueden tener 10^{30} direcciones por cada habitante en el mundo. De lo cual se puede concluir que hay suficientes direcciones IPv6 para satisfacer las necesidades requeridas por los usuarios.

- √ El organismo encargado de distribuir las direcciones IPv6 a nivel mundial es IANA *(Internet Assigned Numbers Authority)*, para el caso de Latinoamérica la entidad encargada es LACNIC la cual distribuye direcciones IPv6 a las entidades nacionales como *CEDIA* y esta a las organizaciones académicas.

- √ A la E.P.N., se le ha asignado una dirección con prefijo de 48 bits, lo que significa que con los 80 bits restantes se puede disponer de 2^{80} = 1208925819614629174706176 direcciones. Lo que quiere decir que hay gran cantidad de direcciones para las aplicaciones y servicios requeridos.

- √ Por la cantidad de direcciones disponibles, ya no es necesario mantener el concepto de subneting y de traducción de direcciones (NAT). El proceso de traducción de direcciones NAT es utilizado para convertir una dirección privada a pública en el caso de IPv4, pero en IPv6 este proceso no es necesario realizarlo ya que desaparece el concepto de direcciones públicas y direcciones privadas.

- √ Debido a la gran cantidad de direcciones IPv6 se han incorporado nuevos servicios como:

    - o *Servicios Basados en la Web.-* transmite resultados de servicios y estadísticas mediante la web.
    - o *Servicios de Difusión.-* permite la difusión de frecuencias de radio y televisión en equipos móviles.
    - o *VoIP.-* permite la transmisión de voz en tiempo real.
    - o *Servicios de Monitorización.-* permite monitorear el tráfico en una red, trazar rutas de red, procesos de producción, etc.
    - o *Servicios de Red.-* permite la implementación de servidores públicos de NTP *(Network Time Protocol)*.
    - o *Servicios de Vigilancia.-* permite la vigilancia de diferentes lugares como: casas, oficinas, etc.
    - o *Movilidad.-* permite a un nodo móvil ser accesible desde su dirección principal, sin importar donde se encuentre físicamente.

- √ Debido a que una dirección IPv6 consta de 128 bits, ha sido conveniente representarla mediante valores hexadecimales. Adicionalmente para la separación de cada valor compuesto de 2 octetos *(16 bits)* se utiliza dos puntos ***(:)***.

- √ La dirección de loop back del protocolo IPv4 es *127.0.0.1*, mientras que en el protocolo IPv6 es *::1.*

- √ Cuando se instala el protocolo IPv6 se crea automáticamente una dirección IPv6 a la cual se la conoce como dirección de enlace local la misma que hace referencia al host, esta dirección es de tipo *fe80:xxxx:xxxx:xxxx (x=dirección física de la máquina).*

- √ Para saber a que red pertenece una dirección IPv4 es necesario conocer la mascara de red, en cambio en IPv6 se utilizan prefijos de red de longitud única para cada dirección de red.

Con respecto a la Migración.-

- √ Para migrar de una red IPv4 a una red IPv6 se tiene que considerar los siguientes factores:

    - o *Hardware*.- dispositivos que forman una red como los routers y hosts.
    - o *Software*.- versiones para la implementación de:
        - Servicios de Red tales como DNS, DHCP;
        - Aplicaciones de Red tales como FTP, HTTP;
        - Sistemas Operativos tales como Windows XP, Windows 2003, Windows Vista, Distribuciones de Linux;

- √ Una de las alternativas más utilizadas para la migración hacia el protocolo IPv6 es la coexistencia entre el protocolo IPv4 e IPv6 mediante la configuración dual stack, aunque adicionalmente existen otros mecanismos como: túneles sobre IPv4 y túneles sobre IPv6. En la E.P.N. se ha optado por el mecanismo dual.

- √ La configuración dual stack permite a una red comunicarse con otras redes que están configuradas solo con IPv4 ó solo con IPv6, o con ambos.

- √ La implementación del protocolo IPv6 puede ser un proceso largo y complejo de acuerdo al nivel de conocimiento que se tenga de IPv6.

Con respecto al Costo.-

- √ La implementación de IPv6 lleva consigo un costo, el cual depende de los siguientes factores:

    - o *Equipamiento.-* principalmente de los equipos de interconexión a usarse.
    - o *Capacitación del personal técnico.-* en el caso de ser requerida.
    - o *Aplicaciones.-* las requeridas para trabajar con IPv6.
    - o *Direcciones.-* es costo depende de la institución que la solicite, para el caso de las instituciones académicas el costo es menor.

Con respecto a la Configuración.-

- √ Las formas de configuración del protocolo IPv6 más utilizadas son: la autoconfiguración *(de enlace local y con anuncio de prefijos)* y la configuración manual, las cuales han sido adoptadas por la UGI.

- √ Para la implementación del prototipo mencionado en la sección 3.1.7 se ha hecho uso de los Routers Cisco modelo 2600, para los cuales solo se necesito actualizar la versión del IOS que tiene como nombre *tanabata,* el cual no tiene ningún costo.

- √ En los Routers solo se puede realizar la configuración manual, y mediante este dispositivo se puede hacer la autoconfiguración con anuncio de prefijo a los hosts que se encuentran conectados a el.

- √ Para el caso de los Hosts se puede utilizar la autoconfiguración mediante la instalación del protocolo IPv6 y mediante la conexión con el router. Adicionalmente pueden ser configurados manualmente.

- √ Muchos sistemas operativos tienen a IPv4 como protocolo de red predeterminado y están incorporando a IPv6 como protocolo de red

adicional, pero en el futuro todos los sistemas operativos tendrán a IPv6 como protocolo predeterminado para sus configuraciones de red. En la siguiente tabla se puede visualizar el uso de las versiones del protocolo IP por los diferentes sistemas operativos

Tabla 4.1: Protocolos IP

	S. O.	Protocolo Predeterminado	Protocolo Adicional
Windows	Win 98	IPv4	IPv6
	Win NT	IPv4	IPv6
	Win XP	IPv4	IPv6
	Win 2003	IPv4	IPv6
	Win Vista	IPv6	IPv4
Linux	Centos 4	IPv4	IPv6
	Centos 5	IPv6	IPv4
	Ubuntu 6.10	IPv4	IPv6
	Mandriva 10.1	IPv4	IPv6
	Mandriva 2007.2	IPv6	IPv4

Nota: Todas las distribuciones de Linux han venido trabajando para hacer de IPv6 un protocolo de red predeterminado:

Con respecto a los Servicios de Red.-
(Ver definición en Glosario)

- √ Existen muchos servicios que todavía no están adaptados para el protocolo IPv6, los cuales son:
  - o *Servidor DHCP.*

- *Servidor Samba.*
- *Servidor Wins, etc*.

√ Uno de los servicios ya desarrollados y adaptados al nuevo protocolo son los siguientes:

- *Servidor de Dominio de Nombres (DNS).-* su utilidad esta definida en cuanto a que las direcciones IPv6 son extensas, entonces la asignación de un nombre a los host facilita su administración y retentiva por parte de los usuarios.
- *Ping6.-* es el más utilizado por los administradores de red para comprobar la conectividad de la red.
- *Tracert6.-* no es muy utilizado.
- *Otros.*

√ Las direcciones IPv6 en la configuración de un servidor DNS son denominadas como direcciones de registro cuádruples *(AAAA).*

√ Los mensajes que presentan los protocolos ICMPv4 e ICMPv6 son similares, ambos presentan mensajes de error pero lo que les diferencia es que en ICMPv6 se agrega un nuevo mensaje que es el de *Descubrimiento de Vecinos*.

Con respecto a las Aplicaciones.-
(Ver definición en Glosario)

√ Con la llegada de este nuevo protocolo serán posibles varias aplicaciones de software como:

- *FTP.-* permite la transferencia de datos de un host a otro dentro de una red.
- *Telnet.-* permite acceder mediante la red a otra máquina mediante modo terminal, para así poder manipular determinado equipo. Esta

aplicación es poco recomendable ya que carece de autentificación que permita asegurar la transmisión de los datos.

- *IExplorer.-* esta aplicación es la más utilizada por los usuarios por que permite la publicación y acceso a sitios web creados sobre IPv6 mediante el protocolo HTTP.

Muchas de estas aplicaciones aún no pueden ser implementadas, por que todavía se están probando.

√ Por la incorporación de nuevos servicios en la red Internet actual como es el: e-comerce, e-business, etc., se requieren mayor seguridad, como la que esta incorporada en este nuevo protocolo.

√ La necesidad de tener una red exclusiva para la investigación, ha hecho que se cree una nueva red conocida como Internet2 *(Redes Avanzadas)* mediante el protocolo http2.

Con respecto a la Estructura de la Trama IP.-

√ Al reducir la longitud de los campos en la cabecera del paquete IP, se puede concluir que el paquete puede transmitir más datos y ser más flexible. Los campos en la cabecera del protocolo IPv4 son 13 y en el protocolo IPv6 llagan a 8 campos.

√ Uno de los campos más importantes dentro de la cabecera del protocolo IPv6 son las *Cabeceras de Extensión* las cuales son utilizadas de acuerdo al tipo de aplicación y no hay la necesidad de especificar que extensión se utilizará ya que el protocolo reconoce la aplicación y asigna la cabecera de extensión adecuada.

√ La existencia del campo *Clase de Tráfico* dentro del encabezado IPv6 logra que el paquete se adapte al tráfico creado por las diferentes aplicaciones.

- √ Mediante este nuevo formato es posible aumentar la carga útil del paquete, llegando a transmitir datagramas de mayor tamaño, conocidos como Jumbogramas los cuales superan los 64 kbytes.

- √ El protocolo IP sigue siendo un protocolo no orientado a la conexión y poco confiable, aunque en la nueva versión del protocolo IP se incluya al protocolo IPSec de forma nativa.

Con respecto a la Seguridad.-

- √ El protocolo IPSec es un conjunto de algoritmos que fue creado como parte de la seguridad en el protocolo IPv6, pero como la implementación de este protocolo no se dio oportunamente, entonces fue adaptado para el protocolo IPv4 como un servicio adicional.

- √ La seguridad en la capa de internet se lo hace mediante el uso del protocolo IPSec el cual garantiza la protección de las comunicaciones privadas y proporciona las siguientes características:

    - o Confiabilidad en los datos.
    - o Autentificación en los datos.
    - o Integridad en los datos.

- √ La seguridad mediante el protocolo IPSec es proporcionada mediante dos aspectos principales como son:

    - o *Cabeceras de Autentificación.-* se encargan de la autenticidad de los datos que son recibidos.
    - o *Cifrado de Seguridad.-* garantiza que solo el destinatario sea capaz de descifrar el contenido de los datagramas.

Con respecto a la Calidad de Servicio.-

- √ La calidad de servicio *(QoS)* en IPv6 garantiza menos retardo en la transmisión de paquetes, mejor distribución del ancho de banda, recuperación de los datos perdidos y mejor administración de trafico en la red; mediante los dos campos en la cabecera IP.

- √ La clase de servicio *(CoS)* es parte de la calidad de servicio y principalmente hace referencia al la clase de tráfico cuya información sirve para definir la prioridad en el envió de paquetes de acuerdo al tipo de aplicación.

- √ Las aplicaciones que son realizadas en tiempo real son beneficiadas por estos dos factores, las cuales son:

    - o *VoIP.-* Voz sobre IP
    - o *IPTV.-* Televisión sobre IP
    - o *Radio sobre IP.*

4.2 RECOMENDACIONES

Las recomendaciones que se presentan a continuación pueden ser tomadas en cuenta en el ámbito de redes académicas y corporativas. Adicionalmente se presentan recomendaciones relativas al funcionamiento de la red LTI.
A primera instancia se presentan las recomendaciones generales.

De Nivel General.- las siguientes recomendaciones están orientadas al ámbito técnico.

- √ Para la implementación de la nueva tecnología es necesario contar con el equipamiento básico de una red como son: Routers y Hosts que sean capaces de soportar esta tecnología.

- √ Instalar en los hosts las nuevas versiones de los sistemas operativos; como por ejemplo Windows XP, Windows Vista, Windows 2003, y las distribuciones de Linux como Centos 5.0, Ubuntu.

- √ Hasta que el servidor DHCPv6 esté aprobado completamente y listo para su implementación, es recomendable aplicar la autoconfiguración con anuncio de prefijos. Estos dos métodos facilitan una adecuada administración en la red.

- √ El uso de un servidor de dominio de nombres permite conocer a un host por su nombre en lugar de su dirección, debido a que las direcciones IPv6 son más difíciles de recordar y manipular.

- √ La implementación Dual Stack puede ser aprovechada por una red *(como la Polired)* para comunicarse con redes que respectivamente trabajan con los protocolos IPv4 ó Ipv6, si es que están conectadas directamente. Para el caso de la Polired, se muestra los casos que pueden presentarse (ver figura 4.1).

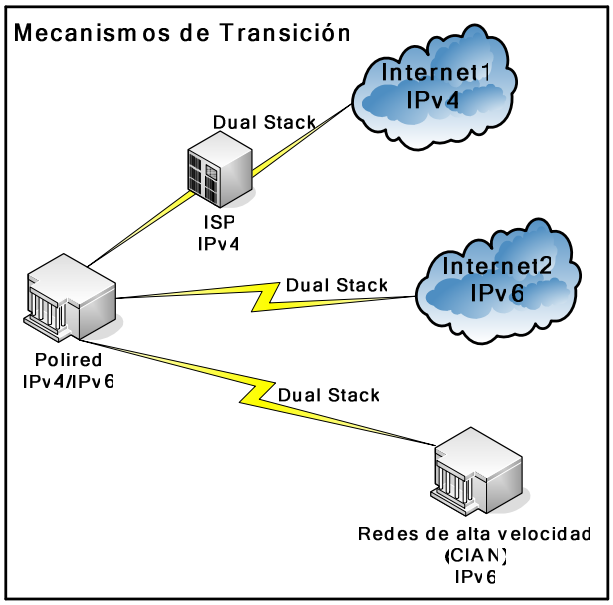


Fig. 4.1 Comunicación de la Polired

√ Cuando dos redes se comunican a través de otra red *(como la de un ISP),* se pueden presentar los siguientes escenarios (ver tabla 4.1):

Tabla 4.2: Mecanismos de Transición

Escenario	***Origen***	***ISP***	***Destino***	***Mecanismo de Transición***
1ro	IPv4	IPv4	IPv4	Dual Stack
2do	IPv6	IPv6	IPv6	Dual Stack
3ro	IPv6	IPv4	IPv6	Túneles IPv4
4to	IPv4	IPv4/IPv6	IPv6	Servidor de Túneles
5ro	IPv4	IPv6	IPv4	Túneles IPv6

√ Para el primer y segundo escenario, la comunicación se realiza directamente debido a que cada red trabaja con el mismo protocolo (ver figura 4.2).

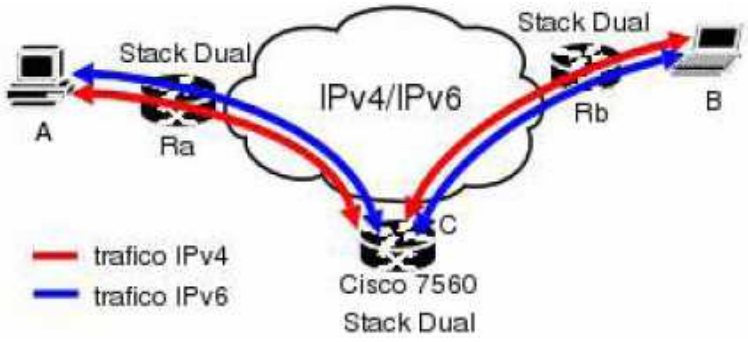


Fig. 4.2 Mecanismo Dual **[16]**

√ Para el tercer escenario, se tiene que utilizar la denominada Técnica de Tunelización.

√ En el cuarto escenario (ver figura 4.4), los paquetes viajan normalmente a través de la red IPv4 hasta lograr alcanzar a los servidores de Túneles. Estos encapsulan los paquetes IPv4 dentro de paquetes IPv6 y así llegar a su destino. Este escenario puede utilizarse de manera invertida para proporcionar la comunicación del protocolo IPv6 a IPv4.

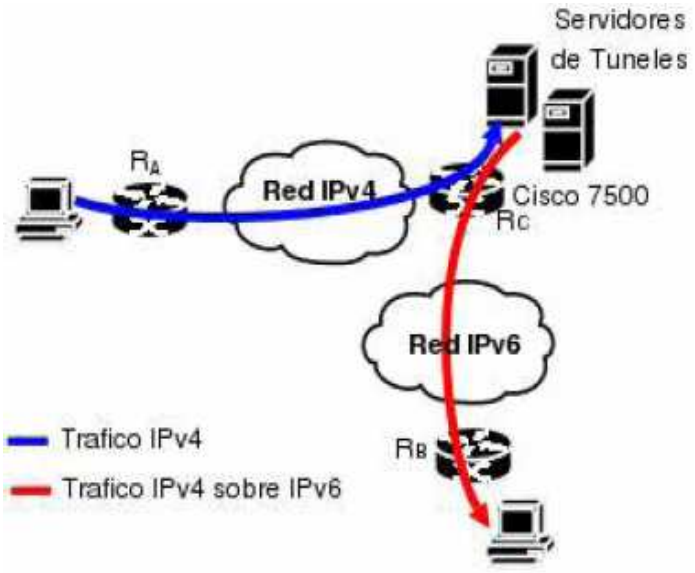


Fig. 4.3 Mecanismo de Tunelización **[16]**

√ El quinto escenario, en la práctica no se da, pues generalmente una red intermedia que trabaje con el protocolo IPv6 también puede trabajar con el protocolo IPv4.

De carácter Administrativo.-

- √ Se recomienda que la Polired mantenga por lo menos un segmento de red IPv6 permanente y un equipo de profesionales dedicados a investigar, desarrollar, probar e implementar las nuevas aplicaciones del protocolo IPv6.

- √ Se debería dar una mayor difusión acerca del protocolo IPv6 en la comunidad académica para así realizar proyectos con esta nueva tecnología.

- √ Capacitar al personal encargado de la administración de la red con el protocolo IPv6 para obtener un mejor uso de las aplicaciones que se ejecutan sobre este nuevo protocolo y administrar de manera adecuada la red.
- √ Mantener un plan de direccionamiento para el buen uso de las direcciones IPv6; que sea flexible, perdurable y seguro de manera que permita la conexión a otras redes.

- √ Implementar el protocolo IPv6 en toda la red, ya que así podemos aprender acerca de su funcionamiento, su configuración y poder realizar pruebas.

- √ Es recomendable instalar los servicios y aplicaciones de red, tales como DNS, HTTP2 para obtener sus beneficios.

Recomendaciones Orientadas al LTI.-

Las recomendaciones presentadas a continuación son de carácter técnico y académico.

De carácter Técnico.-

- √ Debido a que la UGI es la encargada de la administración de la Polired y como el LTI forma parte de esta, se recomienda mantener instalado el

protocolo IPv6 en los hosts para que estos puedan ser utilizados en comunicaciones a través de aplicaciones compatibles con el protocolo IPv6.

√ Actualizar el sistema operativo IOS para el caso de los routers.

√ Actualizar los hosts de manera que las características técnicas permitan la instalación del sistema operativo que funcione directamente con el protocolo IPv6.

√ Debido al avance tecnológico se recomienda la adquisición de nuevos equipos de interconexión de red para implementar de mejor manera la nueva tecnología.

De carácter Académico.-

√ Incorporar el tema del protocolo IPv6 en el pensum de estudio de la carrera de A.S.I., principalmente en la materia TCP/IP de manera que los estudiantes conozcan y apliquen esta nueva tecnología.

√ Mantener prototipos de red para pruebas, para que así los estudiantes de la carrera puedan determinar los inconvenientes y beneficios de una red con el protocolo IPv6.

√ Incentivar y apoyar a los estudiantes a realizar proyectos de comunicación basados en el protocolo IPv6, principalmente sobre la aplicación HTTP2.

4.3 REFERENCIA BIBLIOGRÁFICA

[1] Transmisión de datos y Redes de Comunicaciones, segunda edición, Behrouz A. Forouzan, Mc Graw Hill

[2] http://dgti.salud.gob.mx/capacitacion/manuales_pdf/Linux%20Redes.pdf

[3] El Protocolo IPv6, Documento Teórico, 6SOS http://www.6sos.org

[4] http://es.wikipedia.org/wiki/Cabecera_IP

[5] http://www.rfc-editor.org/cgi-bin/rfcsearch.pl

[6] http://www.microsoft.com/technet/prodtechnol/windowsserver2003/es/library/ServerHelp/7deed46e-5b5e-4253-b89d-33e129e0eca3.mspx?mfr=true

[7] http://internetng.dit.upm.es/ponencias-jing/2001/david-fernandez.PDF

[8] http://www.cu.ipv6tf.org/conf/conferencia_ipv6_janios.ppt

[9] http://www.dte.us.es/ing_inf/inge_prot/docs/tema2.pdf

[10] http://www.consulintel.es/Html/ForoIPv6/Documentos/Tutorial%20de%20IPv6.pdf

[11] Unidad de Gestión de la Información de la E.P.N.

[12] http://es.wikipedia.org/wiki/Algoritmo_de_los_C%C3%B3digos_de_Redundancia_C%C3%ADclica

[13] http://www.consulintel.es/Html/ForoIPv6/Documentos/Tutorial%20de%20IPv6.pdf

[14] http://halley.ls.fi.upm.es/~jyaguez/pdfs/TRANSCUARTOtransiipv4v6febrero2007.pdf

[15] http://lacnic.net/en/ipv6.html

[16] http://www.nic.ve/view/docs/CNTI_IPv6.pdf

GLOSARIO

Ancho de Banda.- Término técnico que determina el volumen de información que puede circular por un medio físico de comunicación de datos, es decir, la capacidad de una conexión. A mayor ancho de banda, mejor velocidad de acceso y mayor tráfico o cantidad de personas.

Aplicaciones de Red.- Son aplicación realizadas por el usuario dentro de una red.

ARPANET.- Red de la agencia de proyectos de investigación avanzada, es una red de los Estados Unidos encargada para la investigación de las nuevas tecnologías.

CISCO.- Cisco System, es una empresa principalmente dedicada a la fabricación. Venta, mantenimiento y consultoría de equipos de telecomunicaciones.

CoS.- Clase de Servicio, este protocolo trabaja conjuntamente con QoS.

CSMA/CD.- Carrier Sense Multiple Access/Collision Detect, es un protocolo que permite detectar la colisión en la transmisión de datos.

DARPA.- Es una agencia de proyectos de investigación avanzada del departamento de defensa de los Estados Unidos que se encarga de la investigación para el avance de proyectos.

Datagramas.- Son paquetes sencillos enrutados en una red sin reconocimiento

DHCP.- Dynamic Host Configuration Protocol, es un servidor que asigna dinámicamente direcciones a los hosts que se encuentren conectados dentro de organización de red. Este servidor permite a los administradores de red supervisar y distribuir las direcciones IP desde un punto central. Cada vez que se enciende una maquina, esta recibe una dirección diferente desde el servidor.

DNS.- Domain Named System, es un servidor que permite asignar un nombre a una determinada dirección para facilitar su uso par ala comprobación de la conectividad, para el caso de la direcciones IPv6 que son mas grandes facilita al administrador su reconocimiento.

EPN.- Escuela Politécnica Nacional.

ID.- Es el identificadores que posee una máquina dentro de una red.

IETF.- Internet Engineering Task Force, es una organización encargada de la evolución de la arquitectura de la red.

Internet2.- Esta red se diferencia con la red Internet por ser únicamente una red educacional. Esta red sirve solo para la comunicación con universidades que se encuentran dentro de un mismo país o de otros países.

IP.- Protocolo de Internet, es el protocolo que permite el acceso al Internet**.**

IPSec.- Internet Protocol Security, es una extensión del protocolo IP que sirve para la seguridad añadiendo cifrado para permitir servicios de autenticación, de esta manera se aseguran las comunicaciones. Este protocolo fue desarrollado para el nuevo protocolo IPv6 y posteriormente fue adaptado para IPv4.

IPv4.- Es una de las versiones del protocolo de Internet, esta versión fue la primera en implementarse extensamente y forma la base para el acceso al Internet.
IPv4 usa 32 bits para la asignación de sus direcciones IP, lo que equivale a 2^{32} = 4.294.967.296 direcciones posibles.

IPv6.- Es la nueva versión del protocolo de Internet. IPv6 utiliza 128 bits para asignar sus direcciones IP, lo que equivale a 2^{128} = 3,40282366920938463463374607431768e+38 direcciones posibles.

IPng.- Protocolo de Internet de nueva generación, así fue llamado antes de ser IPv6.

ISO.- International Organization of Standarization, esta organización se encarga de la estandarización de los protocolo.

Jumbograms.- Son datagramas de gran tamaño que viajan en una red, su tamaño superan los 64 kbytes.

LAN.- Son las siglas de una red de área local, son redes pequeñas de hasta 10 Km.

LTI.- Laboratorio de Tecnologías de la Información, es el laboratorio de la carrera de Análisis de Sistemas informáticos.

MTU.- Es el tamaño máximo de la unidad de trasmisión, para el caso de IPv6 el tamaño es de 1500 bytes sobre redes Ethernet.

Multihoming.- Se denomina Multihoming a los hosts que se conectan a Internet a través de dos o más ISPs.

Multicast.- Es la comunicación de un sólo emisor y varios receptores dentro de una red

NAT.- Network Address Translation, este proceso de traducción se usa cuando se requiere la comunicación entre diferentes redes. Esto permite la duplicación de la dirección IP para acceder a dicha red.

OSI.- Open System Interconnection, fue la primera pila de protocolos para la comunicación de datos.

Plug & Play.- esta tecnología permite a un dispositivo informático ser conectado a un ordenador sin tener que configurarlo, para que eso sea posible el sistema

operativo con el que funciona el ordenador debe tener soporte para dicho dispositivo.

Protocolo.- Conjunto de comandos que permite que dos computadoras se comuniquen entre si.

QoS.- Quality of Service o Calidad de Servicio, garantiza la transmisión de los datos en un tiempo dado, dentro de IPv6 se puede definir la prioridad y flujo de cada paquete que se transmite y según el contenido de estos campos el router debe darles un trato adecuado.

RFC.- Corresponde a Request for Commentes, son documentos cuyo contenido es una propuesta oficial para un nuevo protocolo de la red Internet, los cuales explican con detalle para que casos deben ser aceptados para su implementación.
Cada uno de los RFC tienen asignado un título y un número, que no pueden repetirse ni eliminarse aunque ya sean documentos obsoletos.

Servicios de Red.- Son los servicios que se presta dentro de una red principalmente hacia hosts que se encuentran dentro de la misma red.

TCP.- Protocolo de control de la transmisión

TCP/IP.- Es un conjunto de protocolos de red que implementa la pila de protocolos en la que se basa el Internet y que permite la transmisión de datos entre redes de computadoras.

Unicast.- Comunicación establecida entre un solo emisor y un solo receptor en una red.

VLAN.- Son las siglas de una red virtual de área local, es una red lógicamente independiente. En un switch pueden existir muchas VLANs, una de las ventajas de este tipo de red surge cuando se traslada físicamente una computadora a otra

ubicación ya que puede permanecer en la misma VLAN sin la necesidad de realizar ninguna reconfiguración en el hardware.

WAN.- Es una red de gran tamaño, son capaces de cubrir de 100 a 1000Km de distancia.

W3C.- Word Wide Web Consortium, es el consorcio encargado de la red Internet.

ANEXOS

ANEXO 1: ALGORITMO DE LOS CÓDIGOS DE REDUNDANCIA CÍCLICA

El algoritmo utilizado por el control de redundancia cíclica es el siguiente:

Se añaden **r** bits "0" a la derecha del mensaje (esto es, se añaden tantos ceros como grado tenga el polinomio generador).

Se divide el polinomio obtenido por el polinomio generador. La división se realiza en módulo 2, que es igual que la división binaria, con dos excepciones:

1 + 1 = 0 (no hay acarreo) y 0 - 1 = 1 (no hay acarreo)

Y se añade el resto de la división al polinomio original.

La elección del polinomio generador es esencial si queremos detectar la mayoría de los errores que ocurran.

Uno de los polinomios generadores que más se suelen utilizar es el estándar CCITT: $\mathbf{x^{16} + x^{12} + x^5 + 1}$.

Este polinomio permite la detección de:

- 100% de errores simples.
- 100% de errores dobles.
- 100% de errores de un número impar de bits.
- 100% de errores en ráfagas (en una serie sucesiva de bits) de 16 o menos bits.
- 99.99% de errores en ráfagas de 18 o más bits. **[12]**

ANEXO 2: GUIA DE CONFIGURACION DE TCP/IP CON IPv4

En la figura que se muestra más abajo se describe el prototipo a utilizarse para la configuración del protocolo IPv4 en el LTI.

El protocolo TCP/IP puede ser configurado en servidores y host con Windows mediante los siguientes métodos: **[6]**

- Configuración automática
- Configuración dinámica
- Configuración alternativa
- Configuración manual

2.1 CONFIGURACIÓN AUTOMÁTICA

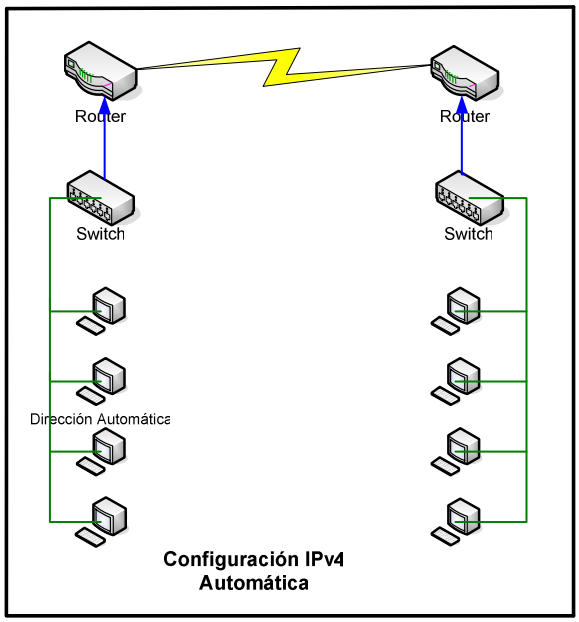


Fig. A.1 Asignación de direcciones Automáticas

Pasos de configuración de TCP/IP para direccionamiento automático

1. Abrir Conexiones de red.

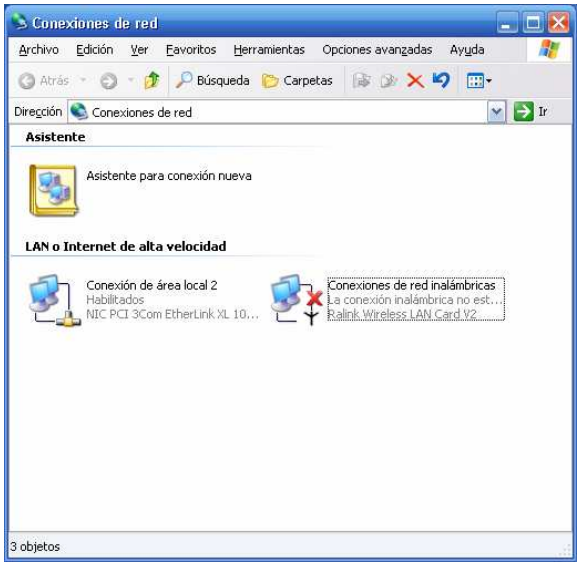


Fig. A.2 Conexiones de Red

2. Haga clic con el botón secundario del mouse en la conexión de red que desee configurar y, a continuación, haga clic en Propiedades.

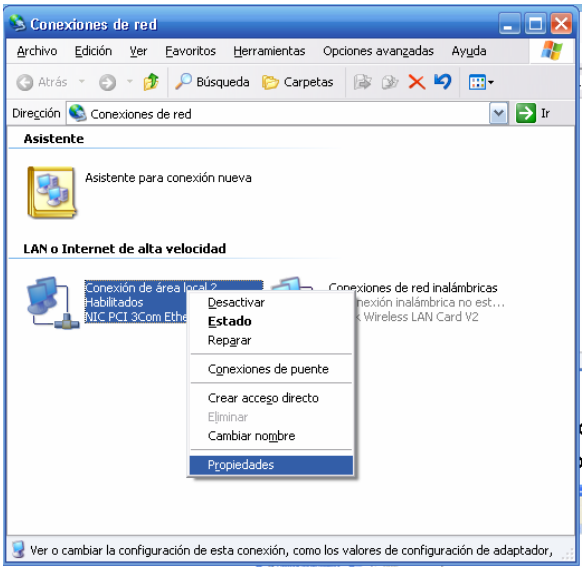


Fig. A.3 Propiedades de la Red

3. En la pestaña General, haga clic en Protocolo Internet (TCP/IP) y, a continuación, en Propiedades.

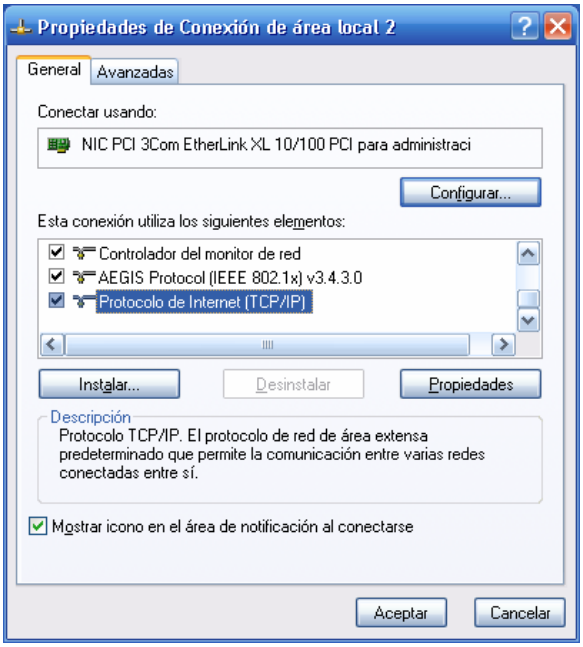


Fig. A.4 Propiedades de la Tarjeta de Red

4. Haga clic en Obtener una dirección IP automáticamente y, después, haga clic en Aceptar.

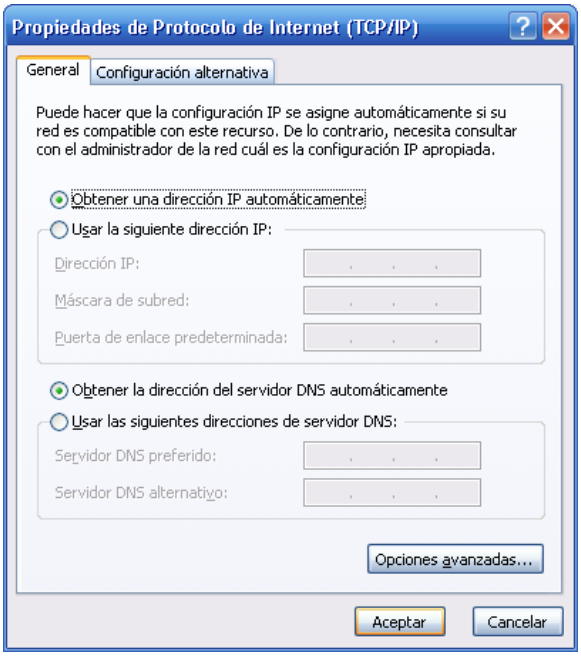


Fig. A.5 Opciones de Configuración

2.2 CONFIGURACIÓN DINÁMICA

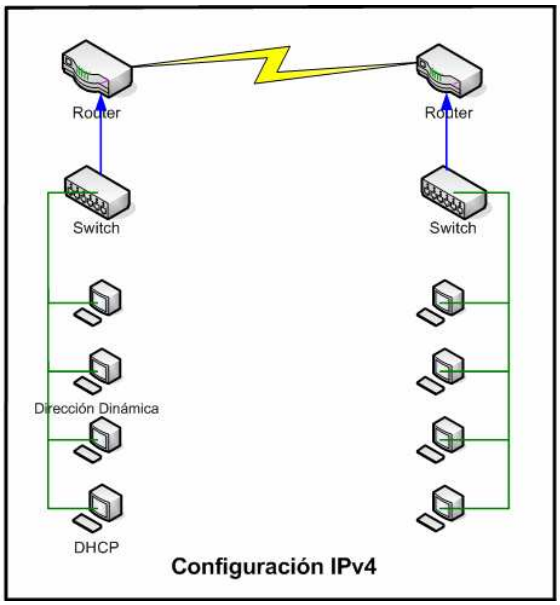


Fig. A.6 Asignación de direcciones Dinámicas

Pasos para la configuración del servidor DHCP

1. Hacemos clic en inicio/programas/Herramientas administrativas/DHCP.

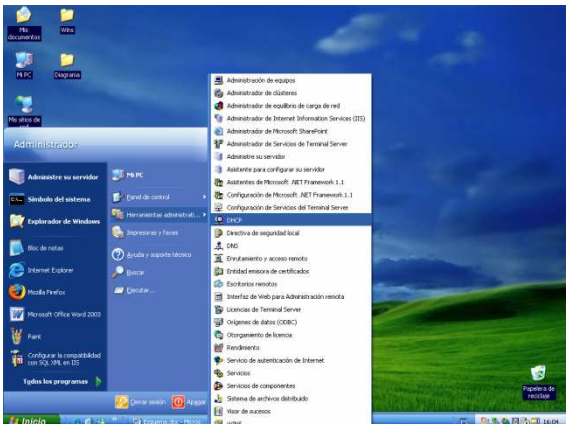


Fig. A.7 Administración del DHCP

2. Hacemos clic en el botón secundario del mouse en el Servidor/Ámbito Nuevo.

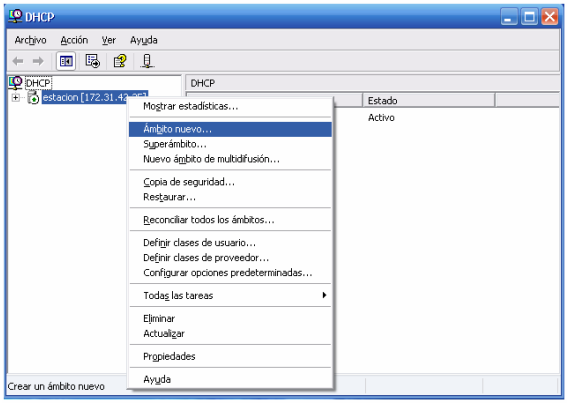


Fig. A.8 Configuración del Servidor DHCP

3. Escribimos en Nombre del ámbito con el que vamos a trabajar y una corta descripción.

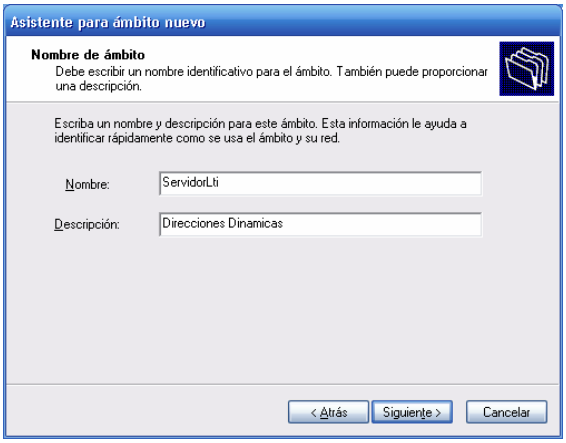


Fig. A.9 Ámbito del servidor DCHP

4. Ingresamos un rango de direcciones.

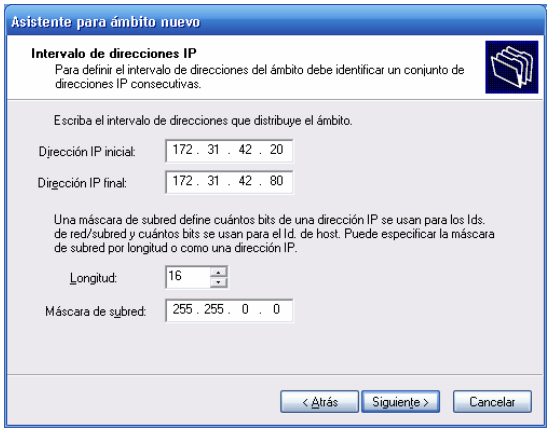


Fig. A.10 Rango de direcciones del DHCP

5. Describimos un intervalo de direcciones el cual no va ha ser utilizado en nuestra red.

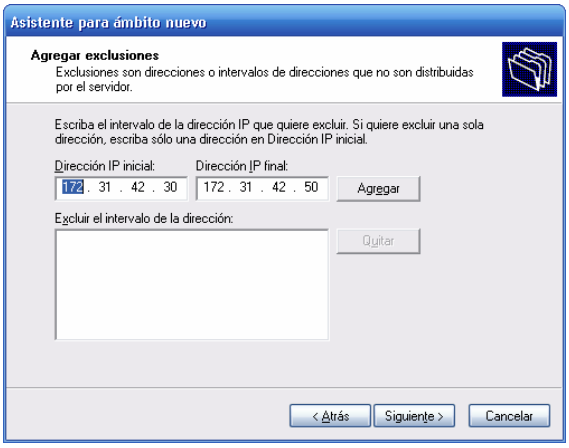


Fig. A.11 Exclusión de direcciones del DHCP

6. Determinamos un tiempo para la duración de la concesión.

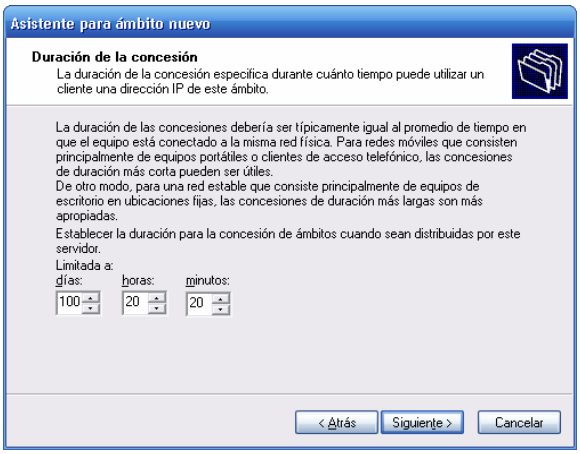


Fig. A.12 Tiempo de Concesión

7. Escogemos a nuestra conveniencia una de las opciones de la configuración del DHCP.

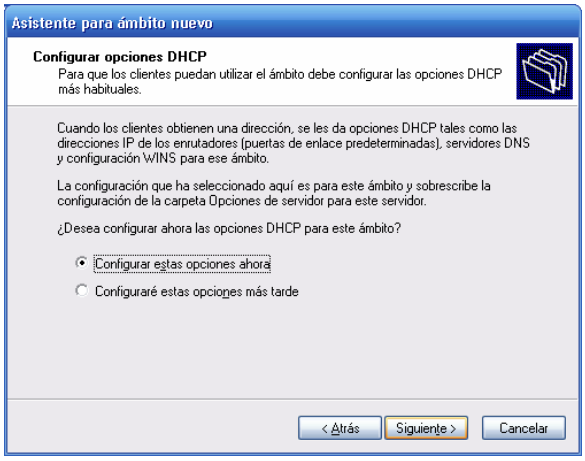


Fig. A.13 Configuración de opciones del DHCP

8. Ingresamos la dirección de la puerta de enlace con la que vamos acceder a la red.

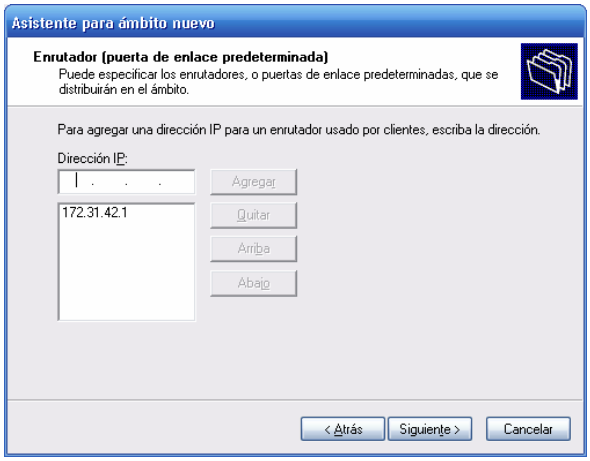


Fig. A.14 Asignación de Puerta de Enlace

9. Asignamos un dominio y un servidor de dominio.

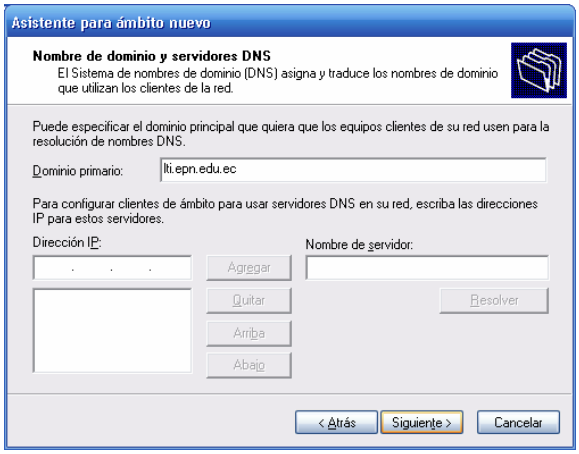


Fig. A.15 Asignación de Dominio

10. Esta es una opción que la podemos evadir.

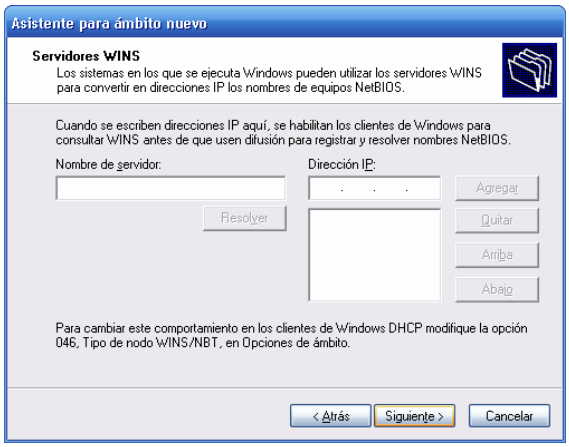


Fig. A.16 Servidores Wins

11. Podemos escoger una de estas opciones de acuerdo a nuestras necesidades de activación del ámbito.

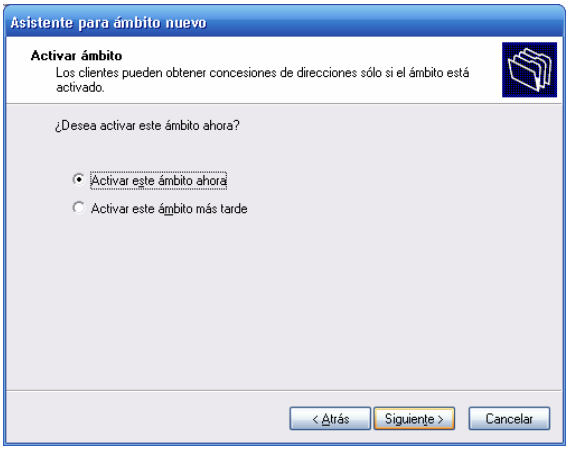


Fig. A.17 Activación del servicio

12. Finalizamos la configuración y listo.

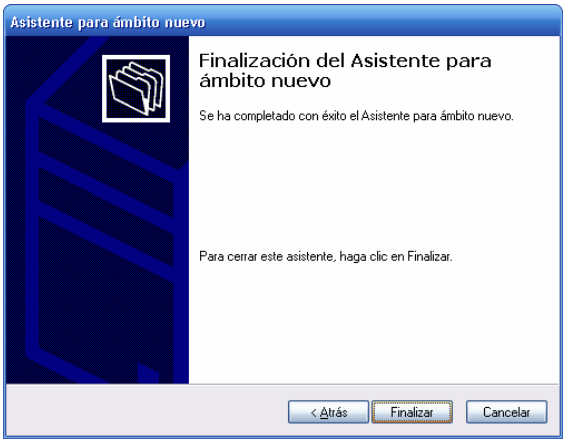
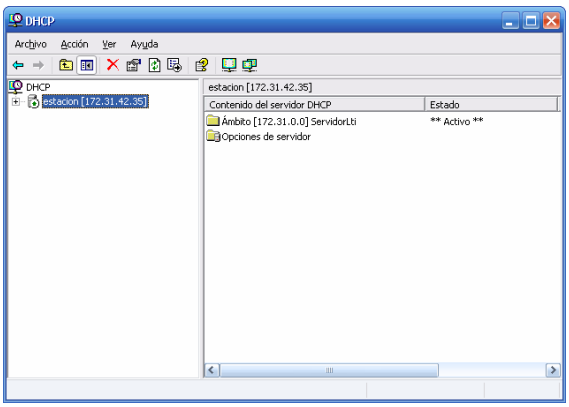


Fig. A.18 Finalización de configuración

13. Para comparar entramos de nuevo (mediante el primer paso) a la presentación inicial del DHCP.



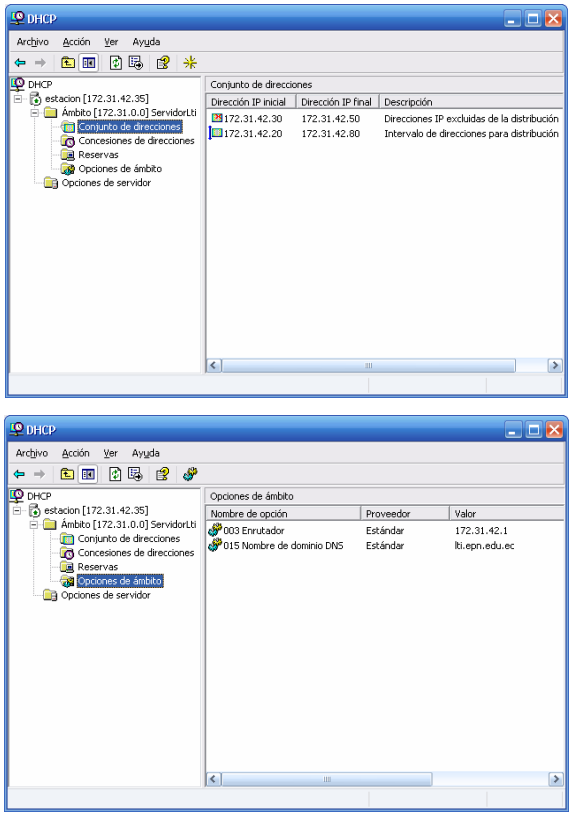


Fig. A.19 Comprobación de la creación del servicio

Verificación de la Configuración del Servidor DHCP

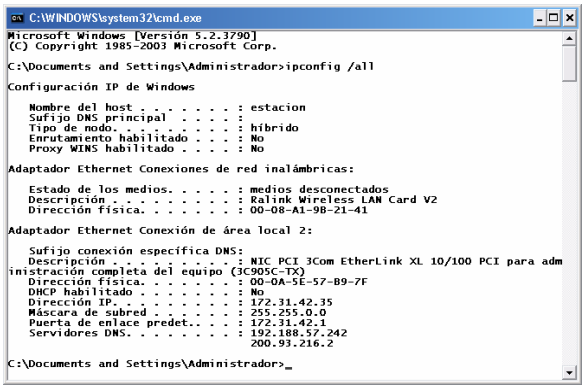


Fig. A.20 Verificación del servicio

Pasos de configuración de TCP/IP para direccionamiento dinámico

Repetir los pasos 1 hasta 4 de la Configuración Automática.

Verificación de la asignación de direcciones a las estaciones por el Servidor DHCP

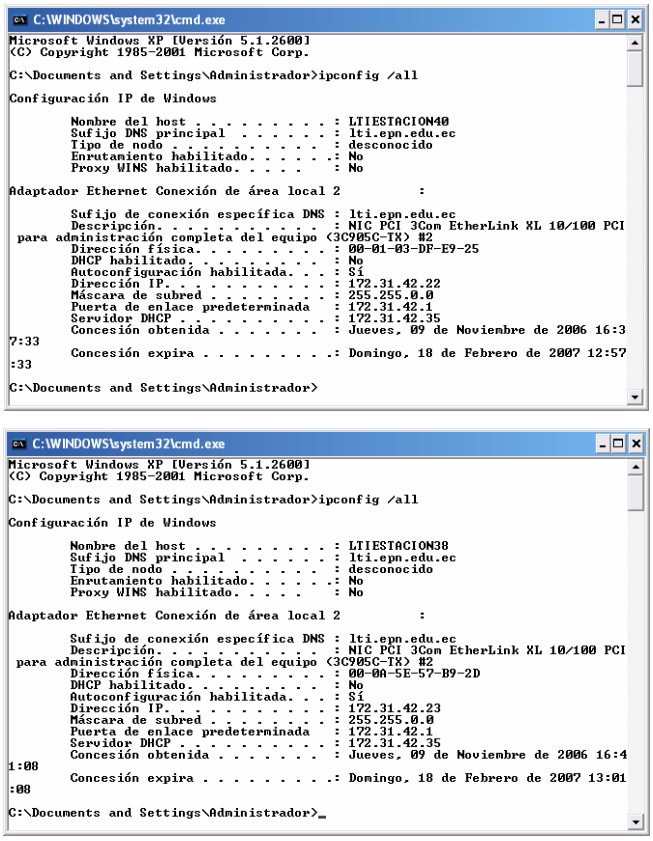


Fig. A.21 Verificación de la existencia del servidor en las estaciones

2.3 CONFIGURACIÓN ALTERNATIVA

Pasos de configuración de TCP/IP para direccionamiento alternativa

Repetir los pasos 1 hasta 4 de la Configuración Automática.

5. En la pestaña Configuración alternativa, haga clic en Configurada por el usuario y, a continuación, escriba los valores apropiados para lo siguiente:
    - Dirección IP
    - Máscara de subred
    - Puerta de enlace predeterminada
    - Servidor DNS preferido y alternativo
    - Servidor WINS preferido y alternativo

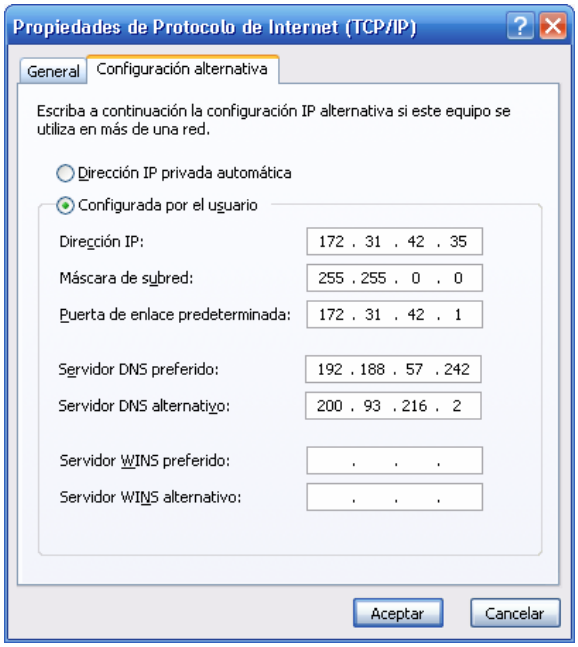


Fig. A.22 Asignación de dirección

2.4 CONFIGURACIÓN MANUAL

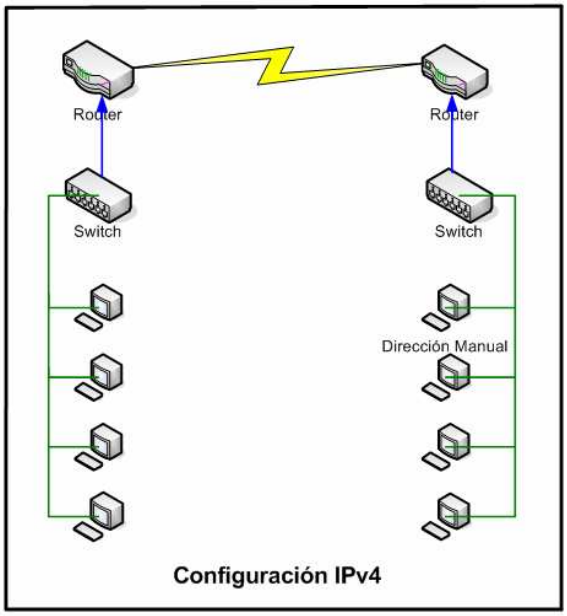


Fig. A.23 Asignación de dirección Manual

Pasos de configuración de TCP/IP para direccionamiento estático

Repetir los pasos 1 hasta 3 de la Configuración Automática.

4. Haga clic en Utilizar la siguiente dirección IP y elija una de las opciones siguientes:
    - Para una conexión de área local, en Dirección IP, Máscara de subred y Puerta de enlace predeterminada, escriba la dirección IP, la máscara de subred y las direcciones de puerta de enlace predeterminadas.
    - Para las demás conexiones, escriba la dirección IP en Dirección IP.

5. Haga clic en Usar las siguientes direcciones de servidor DNS. En Servidor DNS preferido y en Servidor DNS alternativo, escriba las direcciones de los servidores DNS principal y secundario.

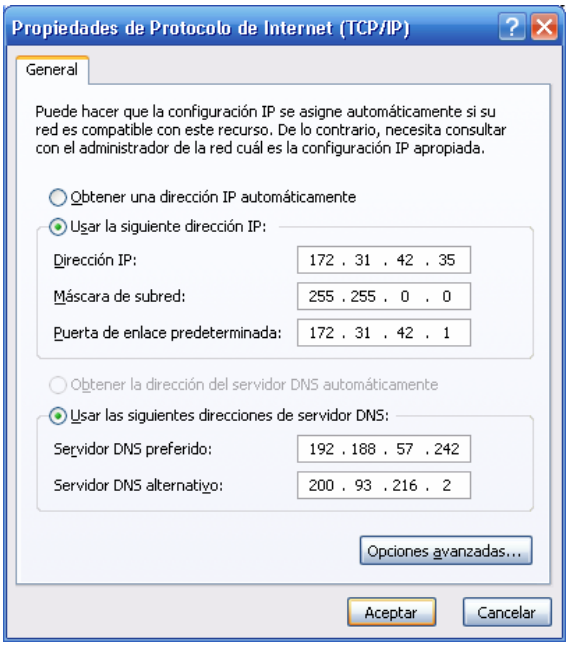


Fig. A.24 Opciones de configuración

Para configurar las opciones avanzadas de direcciones estáticas de una conexión de área local, haga clic en Configuración avanzada y siga uno o varios de los pasos siguientes:

Para configurar direcciones IP:

1. En la pestaña Configuración de IP, en Direcciones IP, haga clic en Agregar.

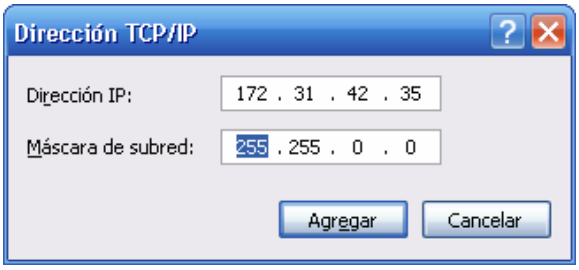


Fig. A.25 Asignación de dirección

2. En Dirección TCP/IP, escriba una dirección IP en Dirección IP y una máscara de subred en Máscara de subred y, a continuación, haga clic en Agregar.

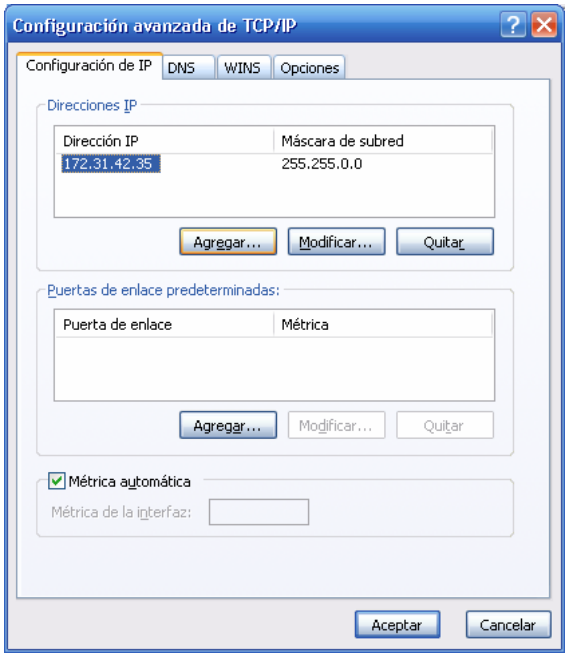


Fig. A.26 Opciones de configuración Avanzada

3. Repita los pasos 1 y 2 para cada dirección IP que desee agregar y, a continuación, haga clic en Aceptar.

Para configurar puertas de enlace predeterminadas adicionales:

Para un host específico, la dirección IP del router que se encuentra en el mismo segmento que el host recibe el nombre de la puerta de enlace predeterminada del host. Toda la información que el host necesite enviar a segmentos distintos, es enrutada a través de la puerta de enlace predeterminada. Como un host y su

puerta de enlace predeterminada se encuentran en el mismo segmento, tienen el mismo ID de red pero diferentes IDs de host.

1. En la ficha Configuración de IP, en Puertas de enlace predeterminadas, haga clic en Agregar. Con los pasos anteriores hasta la configuración de Opciones Avanzadas.

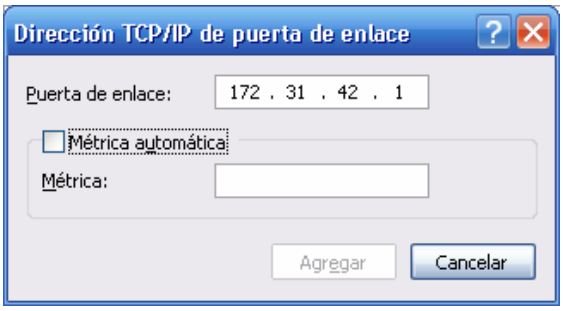


Fig. A.27 Asignación de dirección

2. En Dirección TCP/IP de puerta de enlace, escriba la dirección IP de la puerta de enlace predeterminada en Puerta de enlace. Para configurar manualmente una métrica de ruta predeterminada, desactive la casilla de verificación Métrica automática y escriba una métrica en Métrica.

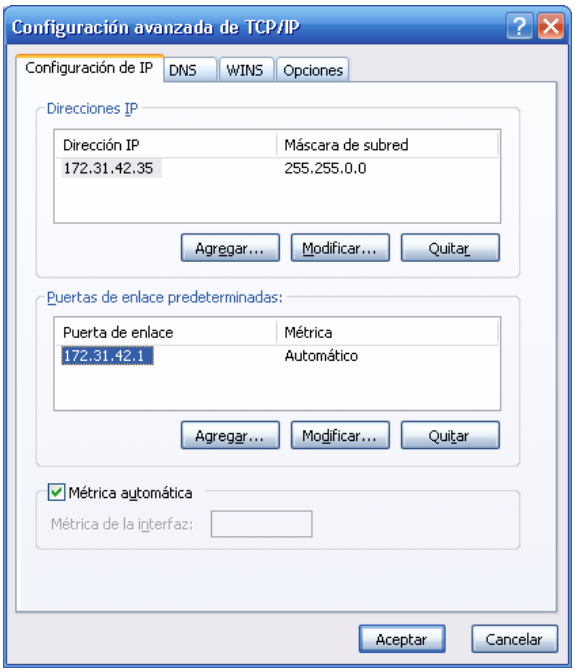


Fig. A.28 Configuración de Métrica

3. Haga clic en Agregar.

4. Repita los pasos del 1 al 3 para cada puerta de enlace predeterminada que desee agregar y, a continuación, haga clic en Aceptar.

ANEXO 3: RFC`s

Los RFC`s existentes en el desarrollo de IPv6 son los siguientes: **[13]**

	Documento	Título
Especificaciones Básicas	RFC2460	Especificaciones del Protocolo Internet Versión 6 (IPv6)
	RFC2461	Descubrimiento del Vecindario para IPv6 (ND)
	RFC2462	Autoconfiguración de Direcciones "stateless" IPv6
	RFC2463	Protocolo de Mensajes de Control de Internet para IPv6 (ICMPv6)
	RFC1981	Descubrimiento del MTU de la ruta para IPv6
	RFC1809	Uso del campo "Etiqueta de Flujo" en IPv6
Direccionamiento	RFC2373	Arquitectura de Direccionamiento en IPv6
	RFC1887	Arquitectura para la Asignación de Direcciones Unicast IPv6
	RFC2374	Formato de Direcciones Unicast Agregables Globales
	RFC2450	Propuesta de normas de asignación de TLA y NLA
Routing	RFC2080	RIP para IPv6
	RFC2081	Aplicabilidad de RIPng para IPv6
	RFC2283	Extensiones Multiprotocolo para BGP-4
	RFC2545	Uso de las Extensiones Multiprotocolo de BGP-4 para Routing entre dominios para IPv6
	RFC2740	OSPF para IPv6
DNS	RFC1886	Extensiones DNS para soportar IPv6
IPv6 sobre ...	RFC2464	Transmisión de paquetes IPv6 sobre redes Ethernet
	RFC2467	Transmisión de paquetes IPv6 sobre redes FDDI
	RFC2470	Transmisión de paquetes IPv6 sobre redes Token Ring
	RFC2472	IPv6 sobre PPP
	RFC2491	IPv6 sobre redes de Acceso Múltiple Sin Broadcast
	RFC2492	IPv6 sobre redes ATM
Seguridad	RFC2401	Arquitectura de Seguridad para IP
	RFC2402	Cabecera de Autenticación IP
	RFC2406	Encriptación de datos en IP (ESP)
	RFC2408	Asociaciones de Seguridad y Protocolo de Gestión de Claves en Internet (ISAKMP)
Multicast	RFC2375	Asignación de Direcciones Multicast
	RFC2710	Descubrimiento de nodos que desean recibir Multicast para IPv6
	RFC2776	Protocolo de Anunciación de Zonas de Ambito Multicast (MZAP)
Anycast	RFC2526	Direcciones de Subredes para Anycast en IPv6
Multi-Homing	RFC2260	Soporte Escalable de Multi-homing para Conectividad Multi-Proveedor
	RFC2497	Transmisión de paquetes IPv6 sobre redes ARCnet
Transición	RFC1933	Mecanismos de Transición para Routers y Hosts IPv6
	RFC2185	Aspectos de Routing de la Transición IPv6
	RFC2473	Especificaciones Genéricas de Tunelización de Paquetes en IPv6
	RFC2529	Transmisión de IPv6 sobre Dominios IPv4 sin Túneles Explícitos
	RFC2765	Algoritmo de Traslación Stateless IP/ICMP (SIIT)
	RFC2766	Protocolo de Traslación – Traslación de Dirección de Red

	RFC2767	Doble Pila en Hosts usando la Técnica "Bump-In-the-Stack" (BIS)
API	RFC2292/bis	Advanced Sockets API para IPv6
	RFC2553/bis	Basic Socket API para IPv6
MIB	RFC2452	Base de Información de Gestión para IPv6: TCP
	RFC2454	Base de Información de Gestión para IPv6: UDP
	RFC2465	Base de Información de Gestión para IPv6: Convenciones Textuales y Grupo General
	RFC2466	Base de Información de Gestión para IPv6: ICMPv6
Otros	RFC1881	Gestión de la Asignación de Direcciones IPv6
	RFC1924	Representación Compacta de Direcciones IPv6
	RFC2147	TCP y UDP sobre Jumbogramas IPv6
	RFC2428	Extensiones FTP para IPv6 y NAT
	RFC2471	Plan de Asignación de direcciones IPv6 para Pruebas
	RFC2474	Definición del Campo de Servicios Diferenciados (DS) en Cabeceras IPv4 e IPv6
	RFC2546	Prácticas de Routing en 6Bone
	RFC2663	Consideraciones y Terminología de IP NAT
	RFC2732	Formato para la representación literal de direcciones IPv6 en URL's
	RFC2772	Guías de Routing en el troncal 6Bone
	RFC2775	Transparencia de Internet

	Borrador IETF	**Título**
Direccionamiento	ipngwg-iana-tla-03.txt	Asignaciones Iniciales de Identificadores sub-TLA IPv6
	ipngwg-site-prefixes-04.txt	Prefijos de Sitios en ND
	ipngwg-esd-analysis-05.txt	Análisis de propuesta de direccionamiento GSE para IPv6
	ipngwg-scopedaddr-format-02.txt	Extensión de formato para Ambitos de Direcciones en IPv6
	ipngwg-scoping-arch-01.txt	Arquitectura de Ambitos de Direcciones en IPv6
	ipngwg-addr-arch-v3-00.txt	Arquitectura de Direccionamiento en IPv6
Routing	ipngwg-router-renum-10.txt	Renumeración de Routers para IPv6
	ipngwg-scoped-routing-04.txt	Routing de Ambitos de Direcciones en IPv6
DNS	ipngwg-dns-lookups-08.txt	Extensiones DNS para soportar Agregación y Renumeración en IPv6
ICMP	ipngwg-icmp-name-lookups-05.txt	Peticiones de información a nodos en IPv6
ND	ion-ipv6-ind-03.txt	Extensiones a ND en IPv6 para descubrimiento inverso
Movilidad	mobileip-ipv6-12.txt	Soporte de Movilidad en IPv6
	mobileip-challenge-12.txt	Extensiones de Desafío/Respuesta en movilidad IP
	mobileip-aaa-reqs-03.txt	Requisitos de Autenticación, Autorización y Contabilidad (AAA) en movilidad IP
	mobileip-rfc2344-bis-01.txt	Revisión de Túneles Inversos para movilidad IP
DHCP	dhc-dhcp-dns-12.txt	Interacción entre DHCP y DNS
	dhc-autoconfig-04.txt	Opción DHCP para desactivar la autoconfiguración stateless en clientes IPv4
	dhc-dhcpv6-15.txt	Protocolo de Configuración Dinámica de Host para IPv6 (DHCPv6)
	dhc-v6exts-12.txt	Extensiones para DHCPv6
Seguridad	ipngwg-addrconf-privacy-01.txt	Extensiones de Privacidad para Autoconfiguración de Direcciones Stateless en IPv6
Multi-Homing	ipngwg-default-addr-select-00.txt	Selección de Direcciones por Defecto para IPv6
	ipngwg-ipv6multihome-with-aggr-00.txt	Multi-Homing en IPv6 con Agregación de Rutas
	ipngwg-multi-isp-00.txt	Problemática de dominios con Routing Multi-Homing en IPv6
Transición	ngtrans-translator-03.txt	Técnicas de Transición para comunicación entre IPv6 e IPv4
	ngtrans-mech-06.txt	Mecanismos de Transición para Host y Routers IPv6
	ngtrans-6to4-06.txt	Conexión de dominios IPv6 a través de redes IPv4 sin túneles explícitos
	ngtrans-broker-02.txt	Tunnel Broker para IPv6
	ngtrans-introduction-to-ipv6-transition-03.txt	Guía para la introducción de IPv6 en el mundo IPv4
	ngtrans-socks-gateway-04.txt	Mecanismos de Pasarela IPv6/IPv4 basados en SOCKS
	ngtrans-6bone-6papa-01.txt	Pre-cualificación para asignación de prefijos de direcciones en 6Bone (6PAPA)
	ngtrans-dstm-01.txt	Mecanismo de Transición de doble pila (DSTM)

	ngtrans-tcpudp-relay-01.txt	Traductor de relé de transporte IPv6-IPv4
	ngtrans-hometun-00.txt	Túneles IPv6 sobre IPv4 para acceso doméstico a Internet
	ngtrans-ipv4survey-00.txt	Inspección de direcciones IPv4 en normas actuales IETF
MIB	ipngwg-mld-mib-03.txt	Base de Información de Gestión para Multicast Listener Discovery Protocol en IPv6
Otros	pim-ipv6-03.txt	Protocolo de Routing Multicast Independiente en IPv6
	pim-v2-sm-01.txt	Protocolo de Routing Multicast Independiente en Modo Esparcido (PIM-SM)

Fig. A.29 Descripción de RFCs