IPV6 PARA MANEJO DE REDES MULTISERVICIO

GUSTAVO ADOLFO MORALES
LUIS FERNANDO ÁLVAREZ

Monografía para optar al título de
Ingenieros en Electrónica y de Telecomunicaciones

FACULTAD DE INGENIERÍA ELECTRÓNICA Y TELECOMUNICACIONES

POPAYÁN

2003

TABLA DE CONTENIDO

INTRODUCCIÓN ---------- 1

CAPÍTULO 1---------- 4

DESCRIPCIÓN DEL PROTOCOLO IPV6, COMPARACIÓN CON IPV4 Y MECANISMOS DE TRANSICIÓN E INTEGRACIÓN DE IPV4 E IPV6.---------- 4

1.1 Descripción de la cabecera IPv6 y comparación con la cabecera IPv4. ---------- 4

1.2 Formato de la cabecera de IPv6. ---------- 5

1.3 Comparación de las cabeceras básicas de los dos protocolos. ---------- 6

1.4 Encabezados de extensión. ---------- 9

1.5 Fragmentación y ensamblaje en IPv6. ---------- 9
1.5.1 Campos de fragmentación. ---------- 9
1.5.2 Fragmentación extremo a extremo.----------10
1.5.3 Solución del problema del cambio de ruta.----------11

1.6 Mecanismos de transición de IPv4 a IPv6.----------11
1.6.1 Pila dual IPv4 e IPv6. ----------11
1.6.2 Túneles IPv6 sobre IPv4. ----------12
1.6.3 Túneles 6to4.----------15
1.6.4 Transmisión de IPv6 sobre dominios IPv4 (RFC2529). ----------18
1.6.5 Mecanismos de traducción.----------19
1.6.6 “Tunnel server” y “tunnel broker”. ----------21
1.6.7 SIT (Simple Internet Transition). ----------21

1.7 Estrategias de migración.----------22
1.7.1 Estrategia de migración de redes finales (clientes y servidores). ----------22
1.7.2 Estrategias de migración para ISP´s. ----------23
1.7.3 Estrategia de migración de backbones.----------24

CAPÍTULO 2---------- 25

EL USO DE IPV6 PARA COMUNICACIONES MÓVILES---------- 25

2.1 Los problemas de la movilidad. ----------25

2.2 Operación de un nodo móvil en ipv6. ----------27

2.3 Ejemplo de operación de un host móvil en IPv6.----------28

2.4 Opciones de formato.----30
2.4.1 Opción de actualización de los enlaces.----30
2.4.2 La opción de reconocimiento de los enlaces.----32
2.4.3 La opción de demanda de enlaces.----33
2.4.4 La opción dirección local. ----34

2.5 Características de los nodos móviles.----34
2.5.1 Requerimientos generales.----34
2.5.2 Requerimientos del enrutador. ----35
2.5.3 Requerimientos del nodo móvil. ----35

2.6 Transmisión de paquetes hacia un nodo móvil. ----35

2.7 Otras funciones de los nodos móviles.----36
2.7.1 Detección de la movilidad. ----36
2.7.2 Manejando tráfico multicast. ----36
2.7.3 El retorno a la red local.----37

CAPÍTULO 3---------- 38

ENRUTAMIENTO EN IPV6 ---------- 38

3.1 Términos utilizados en este capítulo.----38

3.2 Modelo de red.----39

3.3 Algoritmos de enrutamiento. ----40
3.3.1 Enrutamiento estático.----41
3.3.2 Métrica. ----42
3.3.3 Vector de distancia.----42
3.3.4 Vector de camino.----43
3.3.5 Estado de enlace.----43
3.3.6 Redistribución. ----44
3.3.7 Enrutamiento multiprotocolo. ----44

3.4 Enrutamiento en IPv6.----45
3.4.1 RIPv6. ----45
3.4.2 OSPFv6.----45
3.4.3 IDRPv2. ----46

3.5 Relación entre enrutamiento y direccionamiento.----48
3.5.1 Estructura de Internet. ----48
3.5.2 Problemas IPv4.----49
3.5.3 La solución IPv6. ----49
3.5.4 Desventajas para usuarios.----50
3.5.5 Dominios de enrutamiento con varias direcciones.----50
3.5.6 Túnel.----53
3.5.7 Enlaces privados. ----54

3.6 Enrutamiento multicast. ---- **54**

3.7 Intranets. ---- **55**

CAPÍTULO 4 ---- **57**

SEGURIDAD EN EL PROTOCOLO IP ---- **57**

4.1 Características de seguridad. ---- **58**
4.1.1 Cabecera de autenticación (AH). ---- 58
4.1.2 Técnicas de autenticación. ---- 59
4.1.3 Encrypted Security Payload (ESP). ---- 59

4.2 Gestión de llaves. ---- **61**
4.2.1 Gestión de llaves manual. ---- 62
4.2.2 Gestión de llaves automática. ---- 62

4.3 Aplicación de las características de seguridad en IPv6. ---- **62**
4.3.1 Redes privadas virtuales. ---- 63
4.3.2 Seguridad en el nivel de aplicación. ---- 65
4.3.3 Seguridad de enrutamiento. ---- 65

4.4 Orientación futura. ---- **66**

CAPÍTULO 5 ---- **68**

IMPLEMENTACIÓN DE LA ISLA IPV6 ---- **68**

5.1 Definición de "Isla IPv6". ---- **68**

5.2 Soluciones para la conexión al 6Bone utilizando la topología IPv4 existente. ---- **69**
5.2.1 Solución No. 1: Túneles Configurados manualmente. ---- 69
5.2.2 Solución No. 2: Túneles 6to4. ---- 69

5.3 Objetivos de la transición. ---- **70**

5.4 Solución propuesta para la red de datos de la Universidad del Cauca. ---- **70**
5.4.1 Conexión al 6Bone utilizando túneles 6to4. ---- 70

5.5 Implementación de la isla ipv6 de la Universidad del Cauca y conexión al 6Bone. ---- **79**
5.5.1 Topología de la red implementada. ---- 79
5.5.2 Cómo Trabaja esta Solución. ---- 79
5.5.3 Beneficios. ---- 80
5.5.4 Inconvenientes. ---- 80
5.5.5 Pasos de la Implementación. ---- 81

5.6 Configuración de las interfaces de red de la Isla IPv6. ---- **85**
5.6.1 Equipo con Windows XP con IP de Intranet. ---- 86

5.6.2 Equipo con Windows XP con IP global e IP de Intranet configurado como host 6to4.----------87
5.6.3 Equipo con Windows XP con IP global configurado como enrutador 6to4. ----------88
5.6.4 Equipo con Windows XP que recibe anuncios de enrutador. ----------89

5.7 Descripción de la Topología final. ----------90

5.8 Conclusiones de la implementación y topología final de la Red de Datos de la Universidad del Cauca con la Isla IPv6.----------92

CONCLUSIONES Y RECOMENDACIONES---------- 93

GLOSARIO ---------- 95

BIBLIOGRAFÍA---------- 99

LISTA DE FIGURAS

Figura 1.1 Formato general del paquete IPv6 ---- 4
Figura 1.2 Formato de la cabecera base para IPv6---- 5
Figura 1.3 Formato de la cabecera IPv4.---- 6
Figura 1.4 Comparación gráfica de las dos cabeceras.---- 7
Figura 1.5 Ejemplos de encabezados de extensión. ----10
Figura 1.6 Formato del encabezado de extensión de un fragmento.----10
Figura 1.7 a) Datagrama original IPv6. De b) a d) se muestran los fragmentos resultantes después de que un enrutador encapsula y fragmenta el datagrama. ----11
Figura 1.8 Pila dual, protocolos IPv4 e IPv6. ----12
Figura 1.9 Túnel Configurado o Manual.----13
Figura 1.10 Paquete IPv6 y Paquete IPv6 con cabecera IPv4.----14
Figura 1.11 Túnel Configurado y Túnel Automático. ----15
Figura 1.12 Túnel automático.----15
Figura 1.13 Túnel 6to4.----16
Figura 1.14 Conversión de la dirección IPv4 a una dirección IPv6 para 6to4 ----17
Figura 1.15 Túnel tipo 6over4. ----18
Figura 1.16 Mecanismo de traducción de protocolos. ----19
Figura 1.17 Mecanismo de traducción NAT-PT.----19
Figura 1.18 Mecanismo de traducción SOCKSv5.----20
Figura 1.19 Ejemplo de migración de redes finales (clientes y servidores). A través de mecanismos de traducción.----23
Figura 1.20 Ejemplo de migración de redes finales (clientes y servidores). A través de mecanismos de tipo túnel.----23
Figura 2.1 Red IPv4 Móvil.----26
Figura 2.2 Red IPv6 Móvil.----29
Figura 2.3 Ejemplo de operación de un host móvil en IPv6----29
Figura 2.4 Figura representativa de los campos para las diferentes opciones de enlace. ----32
Figura 2.5 Formato de la opción de reconocimiento ----33
Figura 2.6 Formato de la opción de demanda de enlaces ----34
Figura 2.7 Formato de la opción, dirección local ----34
Figura 2.8 Encabezado de enrutamiento. ----36
Figura 3.1 Modelo de una red IP----40
Figura 3.2 Ejemplo de interconexión entre dos Ass ----40
Figura 3.3 Red con enrutamiento estático y dinámico.----41
Figura 3.4 Ejemplo del uso de OSPF. ----47
Figura 3.5 Interconexión entre ERDs y TRDs.----48
Figura 3.6 Ejemplo de multihomed----52
Figura 3.7 Ejemplos de Túneles ----53
Figura 3.8 Esquema de conexión entre una Intranet e Internet.----55
Figura 4.1 Ejemplo del uso de las cabeceras AH. ----60
Figura 4.2 Estructura de la cabecera AH.----60
Figura 4.3 Estructura de la cabecera DSP, en el caso de utilizar la técnica DES-CBC. ----61
Figura 4.4 Ejemplo de un túnel entre dos firewalls.----64
Figura 4.5 Ejemplo de un túnel entre un firewall y un único host ----64
Figura 5.1 a) Topología inicial de la Intranet de la Universidad del Cauca.----72
Figura 5.1 b) Topología inicial de la Intranet de la Universidad del Cauca simplificada. ----73
Figura 5.2 Topología de la red inicial con la red de prueba adicionada.----75
Figura 5.3 Conectividad establecida desde la red de prueba hasta el ISP 6Bone. ----77
Figura 5.4 Intranet de la Universidad del Cauca con conectividad IPv6 al 6Bone. ----78

Figura 5.5 Topología de la Isla IPv6 implementada en la Universidad del Cauca. ----------79
Figura 5.6 Topología de la red final de la Universidad del Cauca junto con la isla IPv6.----------91

LISTA DE TABLAS

Tabla 1.1 Diferencias de los protocolos IPv4 e IPv6.---------- 9
Tabla 2.1 Posibles valores del campo Estado. ----------33
Tabla 5.1 Conversión de la notación decimal de IPv4 a hexadecimal. ----------82
Tabla 5.2 Hardware y Software usado. ----------86

LISTA DE ANEXOS

Anexo A ICMPv6: Se especifican las características del protocolo de control de mensajes estructurado para IPv6, así como los diferentes formatos de cabeceras que este protocolo maneja.

Anexo B Direcciones IPv6: En este anexo se describen de manera más detallada los diferentes tipos de direcciones y se hace referencia a sus características más importantes.

Anexo C IPv6 sobre ATM: Se describen las definiciones de implementaciones de IP sobre ATM.

Anexo D Prácticas con el protocolo IPv6: Este anexo realiza un importante aporte al trabajo de grado, se describe la realización de prácticas con el protocolo IPv6 utilizando el sistema operativo Windows XP, también se utiliza el software RC-100WL, el cual permite con la visualización de varios ejemplos, tener una mayor comprensión de las tramas como si se estuviera utilizando un analizador de protocolos y de esta manera obtener un mayor entendimiento de los aportes teóricos hechos en el trabajo final

INTRODUCCIÓN

El mundo está a punto de experimentar una nueva generación de Redes que harán más fácil las comunicaciones y los negocios. Estamos cruzando el umbral de una nueva era donde se impone la convergencia de las Telecomunicaciones. Y para ofrecer una respuesta eficaz en este naciente entorno se deben desarrollar redes de próxima generación (*NGN, Next-Generation Networks*), que permitan que los servicios de comunicación, información y entretenimiento. Para lograr una transformación es indispensable la convergencia de las diversas redes actuales, en una red unificada, multiservicio, de datos centralizados, que ofrezca los servicios a diferentes calidades y costos, en plataformas de servicio abiertos.

El ambiente actual de las telecomunicaciones en el mundo está conformado por una amplia variedad de redes. La mayoría de estas redes son altamente especializadas y diseñadas para proveer un servicio específico. Se puede hacer referencia a éstas como “redes integradas verticalmente”. Esta situación multired (“integración vertical”) es el resultado de un proceso de evolución a través de la historia, que dificulta la creación de mecanismos que reduzcan costos de operación, portabilidad del servicio, etc. Estas deficiencias pueden ser remediadas cuando se diseñe una plataforma para el futuro, en donde las líneas divisoras entre las comunicaciones de voz, comunicación de datos y la transmisión de multimedia desaparecerán. Esta tendencia tiene implicaciones importantes para el desarrollo de redes de próxima generación y de esta forma transportar servicios de comunicación, información y entretenimiento a través de una sola red.

Las futuras redes multiservicio harán uso del protocolo IPv6, el cual muchos consideran es la infraestructura subyacente de todos los futuros sistemas de difusión de información. Este debe permitir a las aplicaciones: Una muy alta fiabilidad, una alta capacidad (ancho de banda), soporte de selección de calidad de servicio y herramientas de monitoreo, distribución de cargas y variaciones en rendimiento y planificación dinámicas en función de las aplicaciones. También será necesario añadir nuevas funciones y conceptos para gestionar estas redes con decenas o incluso cientos de millones de usuarios IP.

En este escenario, el protocolo IP soportará el transporte de los distintos tipos de datos y será la base para los nuevos protocolos de control que gestionarán las sesiones multimedia. Sin embargo, estos nuevos conceptos de convergencia y de movilidad han obligado al protocolo IP a evolucionar, bien mediante mecanismos auxiliares a la versión IPv4, o directamente mediante una nueva versión de este protocolo.

Siendo consecuentes con la teoría de que IP es la plataforma de integración para las futuras redes multiservicio surge en el seno de la "Internet Engineering Task Force (IETF)", la organización que desarrolla los protocolos standard para Internet, la nueva versión de este protocolo. La IETF predijo el problema de la disminución de direcciones IP y otros problemas relacionados con la versión 4 de IP (IPv4). Para solucionar estos problemas, la IETF desarrolló la "IP next generation" (IPng), y en Enero de 1995 publicó "The Recommendation for the IP Next Generation Protocol" en su "Request for Comment

RFC 1752" (Todos los RFCs a los que se hace referencia en este trabajo son propuestos por los diferentes grupos de trabajo de la IETF). La IETF se refirió a la nueva generación de IP como "IP versión 6" (IPv6) y desarrolló un amplio conjunto de estándares IPv6 especificando la implementación de IPv6 en Internet. Además de un espacio de direcciones de 128 bits, que resolvería el problema de agotamiento de direcciones, IPv6 usa un esquema de direcciones jerárquico, una cabecera de IP eficaz, calidad de servicio, auto configuración de las direcciones de usuario, autenticación y encriptación. Debido a que IPv6 difiere de manera importante de IPv4, la IETF también creó un mecanismo de transición para facilitar el paso de IPv4 a IPv6.

Los investigadores e ingenieros de las nuevas redes telemáticas y de las aplicaciones inteligentes están construyendo un mundo nuevo, intercomunicado con redes de alta velocidad y al alcance de un número cada vez mayor de individuos, un mundo que será muy diferente al actual. En este aspecto se considera que IPv6 es un activador fundamental para la visión que se tiene de la futura red Multiservicio. Actualmente, el número de teléfonos móviles ya supera con creces el número de terminales fijos de Internet, IPv6 es la única arquitectura viable que puede integrar la nueva ola de dispositivos celulares y las diferentes redes existentes en una única red.

Colombia no puede ser la excepción a este proceso de integración de las diferentes redes en los sistemas de telecomunicaciones, ya que se están presentando varios avances en este ámbito y habrá una avalancha de nuevos servicios y aplicaciones que aumentarán la interacción (Interworking) entre las redes existentes y las futuras. También cabe destacar que la llegada de los PCS impulsará nuevos servicios basados en comunicación de datos, Internet móvil, comercio electrónico móvil, voz sobre IP, por lo que las empresas implicadas en el avance tecnológico de las telecomunicaciones se veran forzadas a crear o subarrendar redes multiservicio. Es aquí donde empieza a tener importancia el concepto de Redes de Próxima Generación NGN y su implementación en Colombia partiendo de las Redes Públicas (Bearer Network) o redes de transporte ya establecidas y las estrategias o fases de migración para llegar a NGN.

La Facultad de Ingeniería Electrónica y Telecomunicaciones de la Universidad del Cauca, pensando en la problemática anteriormente mencionada, y teniendo en cuenta además que Internet tiene grandes posibilidades de continuar siendo a mediano y largo plazo el soporte idóneo sobre el que se construirá la futura Red Global de Información, se ha planteado la necesidad de generar dentro de la institución un ambiente de prueba para IPv6 (Isla IPv6). En donde se asimilarán conceptos tales como: Calidad de servicio, seguridad, autoconfiguración e interoperabilidad de IPv6 con IPv4. A partir de este estudio se quiere impulsar la transición de la actual Red de Datos de la Universidad del Cauca a una red multiservicio desde la nueva versión del Protocolo de Internet. Además servirá como práctica para que los estudiantes se familiaricen con IPv6 y sus características.

Por todo lo anteriormente expuesto se desea con este trabajo de grado, promover dentro de la Universidad del Cauca y en especial en el Departamento de Ingeniería Telemática de la Facultad de Ingeniería Electrónica y Telecomunicaciones, una serie de estudios encaminados al desarrollo de una red multiservicio soportada por el protocolo IPv6.
En los capítulos del uno al cuatro se introducirá de manera gradual en los conceptos básicos de IPv6 como plataforma de las redes de próxima generación, lo que permitirá analizar los mecanismos de transición e integración (interoperabilidad) de IPv4 – IPv6

existentes**.** Además se presentan una serie de recomendaciones sobre la migración a redes multiservicio desde IPv6 y las aplicaciones de este protocolo para comunicaciones móviles.

A través del trabajo final “IPv6 para el manejo de redes multiservicio”, se tratan los aspectos más relevantes del protocolo, aspectos que son los que permiten que IPv6 sea el soporte idóneo para las futuras redes multiservicio, estos aspectos son: transición de IPv4 a IPv6, movilidad, enrutamiento, seguridad y autoconfiguración la cual se observa de manera implícita en el desarrollo de la isla IPv6, tema que se desarrolla en el capítulo final de este trabajo final. En los anexos A, B, C se desarrollan temas igualmente importantes para la comprensión de este protocolo los cuales son: ICMPv6, direccionamiento e IPv6 sobre ATM y finalmente en el anexo D se describen las prácticas implementadas las cuales permitieron desarrollar progresivamente la isla IPv6, en este anexo también se describe el software que se utilizo para el análisis de las tramas IPv6 el cual permite la visualización de los protocolos sin necesidad de utilizar un analizador de protocolos.

Es así como en el primer capítulo de este trabajo de grado, se encuentra una descripción básica de las tramas de IPv6 e IPv4 y su respectiva comparación, además se presentarán los diferentes métodos de transición propuestos por la IETF para migrar del actual protocolo IPv4 a IPv6. En el segundo capítulo se analiza la importancia de IPv6 para las comunicaciones móviles de tercera y cuarta generación. En el tercer capítulo se describe los procedimientos utilizados en cuanto a enrutamiento para IPng. En el cuarto capítulo se desarrolla lo referente a las mejoras en la seguridad en el protocolo (IPsec). Finalmente en el quinto capítulo utilizando toda esta información adquirida a lo largo de todo el proceso de investigación y desarrollo se genera una propuesta de implementación de una Isla IPv6 a partir de la cual se espera que surjan una serie de desarrollos tendientes a integrar la red de datos de la Universidad del Cauca y otras redes en una única red multiservicio soportada por el protocolo IPv6. En la última parte del trabajo final se encuentra un glosario en donde se identifican los diferentes términos utilizados en el desarrollo de este trabajo final, así como una bibliografía de sitios Web, documentos escritos y RFCs de la IETF

CAPÍTULO 1

DESCRIPCIÓN DEL PROTOCOLO IPV6, COMPARACIÓN CON IPV4 Y MECANISMOS DE TRANSICIÓN E INTEGRACIÓN DE IPV4 E IPV6.

A través de este capítulo se mostrarán los mecanismos de transición que son parte del gran esfuerzo para implementar IPv6. Estos mecanismos incluyen la pila dual IPv4/IPv6, encapsulado de IPv6 vía IPv4 y un número de servicios de IPv6 incluyendo IPv6 DNS y otros. Antes de comenzar la descripción de las técnicas de migración se realiza un estudio general de la trama IPv6, con el propósito de dar a conocer sus características se la compara con la IPv4 y se resaltan las principales diferencias y ventajas de nuevo protocolo con respecto a IPv4.

1.1 Descripción de la cabecera IPv6 y comparación con la cabecera IPv4.

Antes de describir las formas de migración e integración de las actúales redes a redes multiservicio basadas en el protocolo IPv6, se hace necesario estudiar la trama IPv6 y sus diferencias con la trama IPv4. En la figura 1.1 se presenta el formato general del paquete IPv6.

Figura 1.1 Formato general del paquete IPv6

Este formato presenta las siguientes características:

- El encabezado base de IPv6 contiene menor información que el encabezado de un datagrama IPv4.
- Las opciones y algunos de los campos fijos del encabezado del datagrama IPv4 han sido movidos hacia los encabezados de extensión de IPv6.
- No hay limitación en el número de opciones en cuanto al número de cabeceras de extensión.
- Mejora en procesamiento del datagrama debido al mejor ordenamiento de las cabeceras.
- Cabeceras procesadas en el destino sin necesitar ningún procesamiento intermedio. Definición precisa del comportamiento frente a opciones desconocidas permitiendo con ello el aprovechamiento del mayor número de datagramas sin que se desechen.

1.2 Formato de la cabecera de IPv6.

En la figura 1.2 se puede apreciar el formato de la cabecera base para IPv6 de 40 octetos.

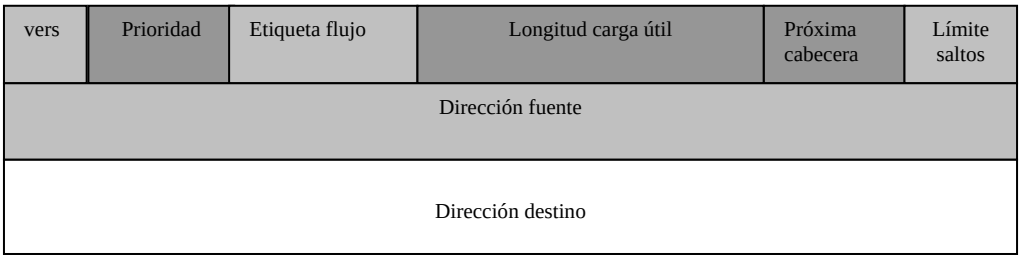


Figura 1.2 Formato de la cabecera base para IPv6

Cada datagrama IPv6 comienza con un encabezado base de 40 octetos que incluye campos para las direcciones IP fuente y destino, el máximo número de saltos, la etiqueta de flujo y el tipo del siguiente encabezado, a continuación se hace una descripción de la totalidad de los campos de la cabecera IPv6.

Versión (Vers): Indica la versión del protocolo 6 para un datagrama IPv6. Esta conformado por 4 bits.

Limite de Saltos (Hop Limit): Análogo al campo TIME-TO-LIVE de IPv4. Representa el número máximo de saltos que un datagrama puede dar antes de ser descartado. Tiene una longitud de 8 bits.

Etiqueta de Flujo (Flow label): Contiene información a ser usada por los enrutadores, como flujo específico y prioridad. Un flujo consiste en un camino a través de Internet, a lo largo del cual enrutadores garantizan una calidad específica de servicio (QoS). Tiene una longitud de 24 bits.

Por ejemplo: Dos aplicaciones que requieren enviar video pueden establecer un flujo en el cual un cierto retardo y ancho de banda es garantizado.

Longitud de carga útil (Payload lenght): Es la longitud de los propios datos y puede ser de hasta 65.536 bytes, tiene una longitud de 16 bits (2 bytes).

Próxima Cabecera (Next header): Dado que en lugar de usar cabeceras de longitud variable se emplean sucesivas cabeceras encadenadas, desaparece el campo de opciones que contenía la cabecera de la versión IPv4. Esta parte es procesada por los enrutadores solo de extremo a extremo, no hay procesamientos intermedios. Existe una única excepción a esta regla, cuando el valor de este campo es cero, lo que indica que se debe examinar de modo “hop by hop” o salto a salto. Son ejemplos de esta excepción: Cabeceras con información de encaminado, fragmentación, opciones de destino, autenticación, encriptación etc, que en cualquier caso han de ser procesadas en el orden riguroso en que aparecen en el paquete. Este campo tiene una longitud de 1 byte.

Prioridad (Priority): También llamado clase de tráfico o simplemente clase, es equivalente al campo ToS (Tipo de Servicio) de IPv4 tiene una longitud de 4 bits.

Dirección Fuente (Source address): Dirección IP de origen. Este campo esta conformado por 128 bits.

Dirección Destino (Destination address): Dirección IP de destino. Este campo esta conformado por 128 bits.

Nota: los diferentes tipos de direcciones IPv6 y sus características se describen en el Anexo B (Direcciones IPv6).

1.3 Comparación de las cabeceras básicas de los dos protocolos.

Algunos de los campos que se nombraron anteriormente, son renombrados de los que utiliza la cabecera de la versión IPv4. Para notar esto y realizar una comparación entre "lo nuevo y lo viejo", se trae a colación la configuración de la cabecera de IPv4 como se ve en la figura 1.3.

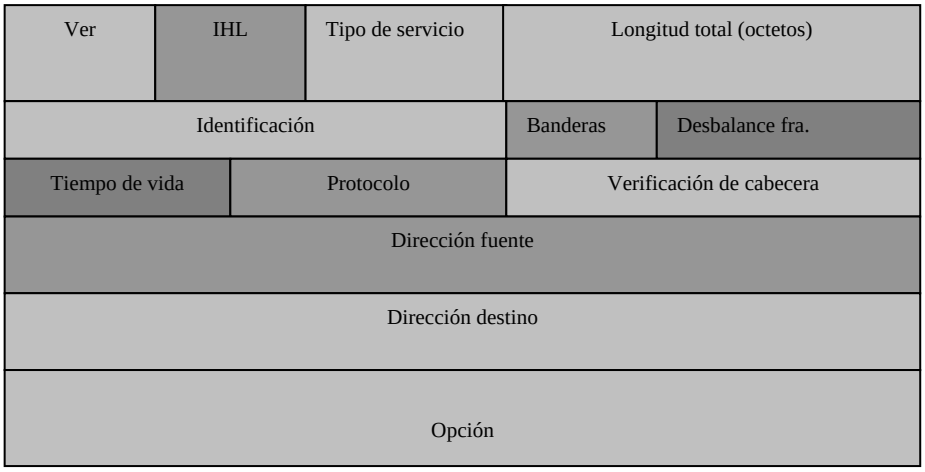


Figura 1.3 Formato de la cabecera IPv4.

Haciendo una breve descripción de esta cabecera se tiene:

Ver: (4 bits): Versión de IP que se emplea para construir el Datagrama. Se requiere para que quien lo reciba lo interprete correctamente.

Ihl: (4 bits): Tamaño de la cabecera en palabras.

Tipo de servicio (Type of service): Determina el tipo de servicio. Conformado por 1 byte. La gran mayoría de los host y enrutadores ignoran este campo.

Longitud total (Total leght): Mide en bytes la longitud de todo el Datagrama. Permite calcular el tamaño del campo de datos.

Identificación (Identification): (16 bits): Número que identifica al Datagrama, que permite implementar números de secuencias y así reconocer los diferentes fragmentos de

un mismo Datagrama, pues todos ellos comparten este número.

Bandera (Flag): (4 bits): Campo de tres bits más uno reservado que permiten indicar si se puede fragmentar el paquete, si es un fragmento y si es el último elemento de éste.

Desbalance de fragmentos (Fragment offset): (12 bits): Este campo indica el tamaño del desplazamiento en bloques de fragmento con respecto al Datagrama original, empezando por el cero.

TTL: (8 bits): Tiempo de Vida del Datagrama, específica el número de segundos que se permite al Datagrama circular por la red antes de ser descartado.

Protocolo (Protocol): Especifica que protocolo de alto nivel se empleó para construir el mensaje transportado en el campo datos de Datagrama IP. Algunos valores posibles son: 1 = ICMP, 6 = TCP, 17 = UDP, etc.

Cheksum: Campo de 16 bits que se calcula a partir de los datos del encabezado, para verificar que estos datos hayan llegado bien.

Dirección fuente (Source address): Dirección IP fuente. Conformado por 32 bits.

Dirección destino (Destination address): Dirección IP de destino de 32 bits.

Como se puede observar en la figura 1.4 se nota que se ha pasado de 13 campos en IPv4 a 8 en IPv6, el motivo principal por la que los campos son eliminados es por la innecesaria redundancia. En IPv4 se esta facilitando la misma información de varias formas. Un caso muy evidente es el checksum o verificación de la integridad de la cabecera. Realizando la comparación entre estas dos cabeceras se tiene:

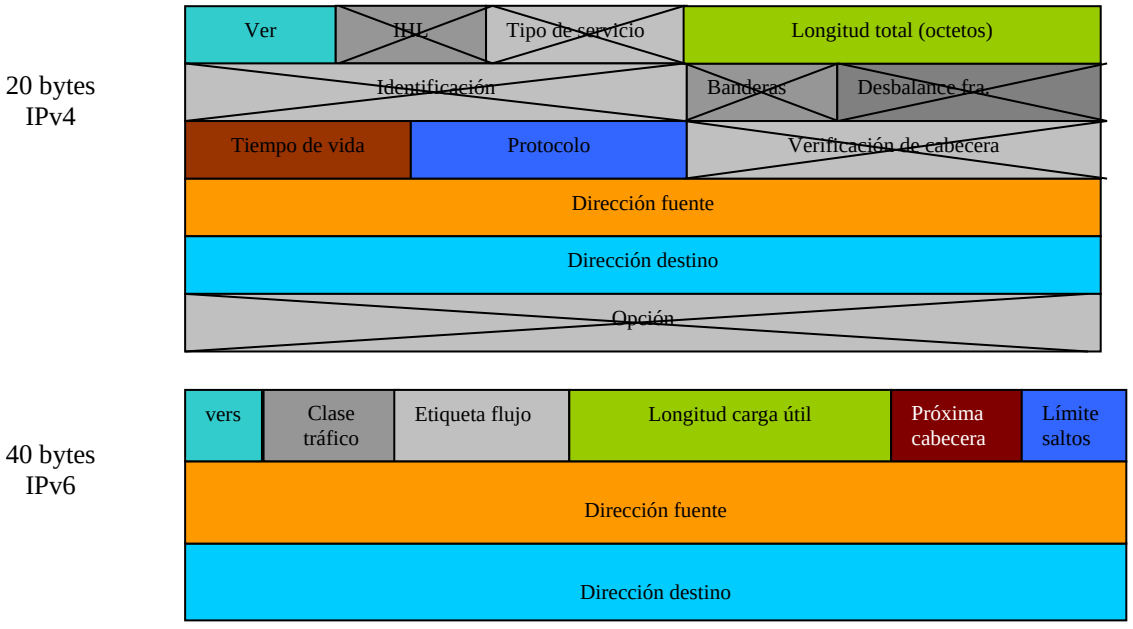


Figura 1.4 Comparación gráfica de las dos cabeceras.

Nota: Una descripción de los campos tanto de la trama IPv4 e IPv6 se realiza mediante el uso de la aplicación RC-100WL (Analizador de Protocolo) en el Anexo D (Prácticas con el Protocolo IPv6).

En el caso del campo de desplazamiento de fragmentación (fragment offset), este es ligeramente diferente, dado a que el mecanismo por el cual se realiza la fragmentación de los paquetes es completamente modificado en IPv6, lo que implica la total inutilidad de este campo. En IPv6 los enrutadores no fragmentan los paquetes, sino que de ser precisa dicha fragmentación / desfragmentación se realiza de extremo a extremo.

Los nuevos campos en la cabecera de IPv6 son: Clase de tráfico (traffic class) y Etiqueta de flujo (flow label). Estos dos campos son los que nos permiten una de las características fundamentales e intrínsecas de IPv6: Calidad de servicio, Clase de servicio, y en definitiva un poderoso mecanismo de control de flujo, de asignación de prioridades diferenciadas según los tipos de servicios.

La longitud de la cabecera de IPv6 es de 40 bytes el doble que en el caso de la cabecera de IPv4, pero con muchas ventajas, al haberse eliminado campos redundantes.

La longitud fija de la cabecera implica un manejo más fácil en el procesamiento por parte de enrutadores y conmutadores. El hecho de que los campos estén alineados a 64 bits permite que las nuevas generaciones de procesadores y microcontroladores de 64 bits puedan procesar mucho más eficazmente la cabecera IPv6.

Las diferencias fundamentales se pueden resumir en:

- El campo *Tamaño de Encabezado* ha sido eliminado y el campo *Tamaño de Datagrama* reemplazado por el campo LONGITUD DE LA CARGA UTIL (*PAYLOAD LENGTH)*.
- El tamaño de los campos de direcciones fuente y destino ha sido incrementados a 16 octetos cada uno.
- La información de fragmentación pasa de ser campo fijo en el encabezado base hacia el encabezado de extensión.
- El campo TIEMPO DE VIDA (*TIME-TO-LIVE)* es reemplazado por el campo LIMITE DE SALTOS (*HOP LIMIT)*.
- El campo TIPO DE SERVICIO (*SERVICE TYPE)* es reemplazado por el campo ETIQUETA DE FLUJO (*FLOW LABEL)*.
- El campo *PROTOCOLO* es reemplazado por un campo que especifica el tipo del siguiente encabezado.

Las ventajas esénciales se resumen en:

- Mejora en la calidad de servicio.
- Soporte de tráfico multimedia en tiempo real.
- Aplicaciones multicast y anycast.
- Facilidad de implementación de los mecanismos de transición e integración de IPv4 a IPv6.

Para mayor facilidad en la comprensión de las diferencias de los dos protocolos ver la tabla 1.1.

IPV6	IPV4
Direcciones de 128 bits	Direcciones de 32 bits
Arquitectura jerárquica	Arquitectura plana
Configuración automática	Configuración manual
Multicast y anycast	Broadcast
Seguridad obligatoria	Seguridad opcional
Identificación calidad de servicio	Sin identificación calidad de servicio

Tabla 1.1 Diferencias de los protocolos IPv4 e IPv6.

1.4 Encabezados de extensión.

Los encabezados de extensión en IPv6 son similares al campo opciones en IPv4. Cada datagrama incluye encabezados de extensión sólo para aquellas facilidades que el datagrama utiliza. Los encabezados de extensión, están definidos por el campo next header de la cabecera básica de IPv6. Se puede extraer, las siguientes características fundamentales:

- Cada encabezado de base y de extensión contiene un campo *NEXT HEADER* para indicar el tipo del siguiente encabezado.
- Extraer toda la información del encabezado de un datagrama IPv6 requiere procesar secuencialmente los encabezados.
- Los enrutadores intermedios no necesariamente requieren procesar todos los encabezados.

En la figura 1.5 se presentan unos ejemplos del uso de los encabezados de extensión.

1.5 Fragmentación y ensamblaje en IPv6.

En IPv6 como en IPv4, el destino final es el encargado del proceso de ensamble de fragmentos. En IPv6 el proceso de fragmentación se lleva a cabo únicamente en la fuente original. Antes de enviar tráfico, la fuente debe de identificar el mínimo MTU (Maximum Transmission Unit) a lo largo de la ruta hacia el destino. El MTU son los paquetes que pueden ser transmitidos en una red. Antes de enviar un datagrama, la fuente fragmenta el datagrama de manera que cada fragmento sea menor que el mínimo MTU. Entonces, el proceso de fragmentación es de extremo a extremo, sin necesidad de que ocurra en enrutadores intermedios.

1.5.1 Campos de fragmentación.

Cuando se requiere fragmentar, la fuente inserta un encabezado de extensión después del encabezado base en cada fragmento. En la figura 1.6 se muestra el formato del encabezado de extensión de un fragmento.

1.5.2 Fragmentación extremo a extremo.

Objetivos de la fragmentación extremo a extremo.

- Liberar al enrutador de la carga de trabajo requerida por el proceso de fragmentación y permitirle atender un mayor número de datagramas por unidad de tiempo.
- En un enrutador convencional, el uso de CPU puede alcanzar hasta un 100% si el enrutador fragmenta muchos o todos los datagramas que recibe.

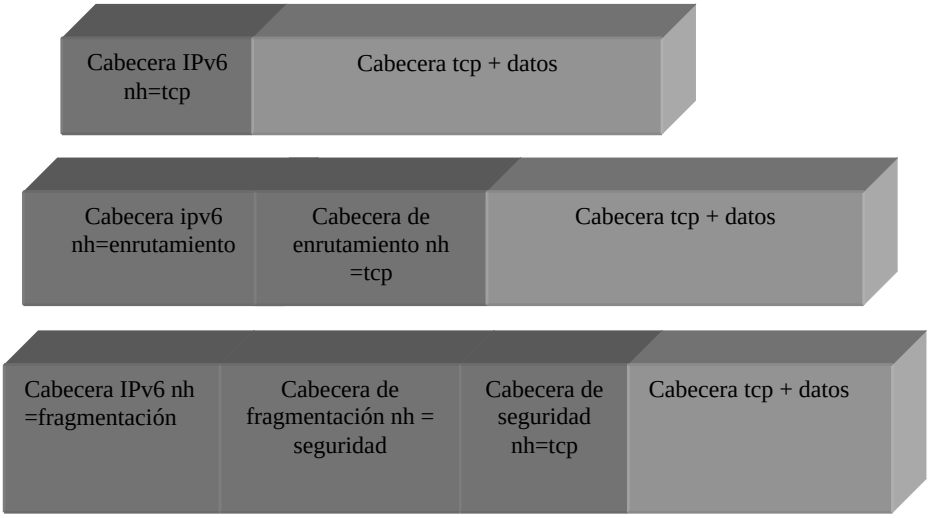


Figura 1.5 Ejemplos de encabezados de extensión.

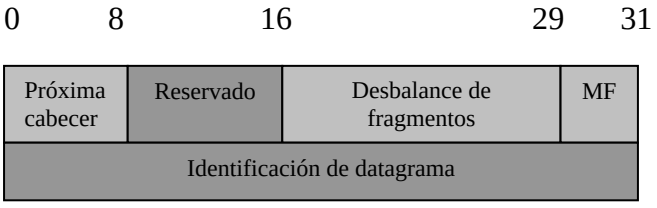


Figura 1.6 Formato del encabezado de extensión de un fragmento.

Consecuencias de la fragmentación extremo a extremo.

- IPv4 fue diseñado para permitir cambios en las rutas en cualquier momento.
- En IPv6, si una ruta es cambiada, puede ocasionar que cambie el mínimo MTU previamente establecido.

El protocolo de Internet con fragmentación de extremo a extremo, requiere que el transmisor descubra el mínimo MTU para cada destino y que fragmente cualquier datagrama que sea mayor que el mínimo MTU en la ruta a seguir. La fragmentación de extremo a extremo no toma en cuenta cambios en la ruta.

1.5.3 Solución del problema del cambio de ruta.

Cuando debido a un cambio en la ruta, el mínimo MTU se ve afectado, un enrutador intermedio que requiera fragmentar, encapsula IPv6 en IPv6 (*"tunneling"*). En la figura 1.7 se muestra este procedimiento.

El encapsulamiento de IPv6 en IPv6 es posible hacerlo de la siguiente manera:

- El enrutador intermedio crea un nuevo datagrama que encapsula el datagrama original en su área de datos.
- El enrutador divide el nuevo datagrama en fragmentos, duplicando el encabezado base e insertando un encabezado de extensión de fragmento en cada fragmento.
- Finalmente, el enrutador envía cada fragmento hacia su destino final.
- En el destino final, el datagrama original es recuperado, recuperando el área de datos del datagrama ensamblado.

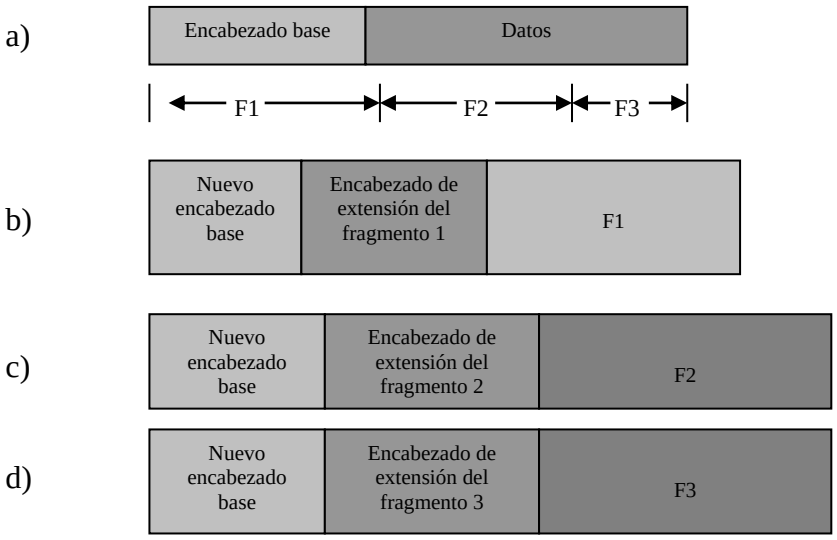


Figura 1.7 a) Datagrama original IPv6. De b) a d) se muestran los fragmentos resultantes después de que un enrutador encapsula y fragmenta el datagrama.

1.6 Mecanismos de transición de IPv4 a IPv6.

La clave para la transición es la compatibilidad con la base instalada de dispositivos IPv4, esta afirmación define un conjunto de mecanismos que los host y enrutadores IPv6 pueden implementar para ser compatibles con host y enrutadores IPv4.

Estos mecanismos permitirán usar infraestructuras IPv4 para IPv6 y viceversa, dado que se prevé que su uso será prolongado, e incluso indefinido en muchas ocasiones.

1.6.1 Pila dual IPv4 e IPv6.

El camino más lógico y evidente es el uso simultáneo de ambos protocolos, en pilas separadas. Los dispositivos con ambos protocolos también se denominan “nodos IPv6/IPv4”.

De esta forma, un dispositivo con ambas pilas puede recibir y enviar tráfico a nodos que sólo soportan uno de los dos protocolos (nodos sólo IPv4 o sólo IPv6).

El dispositivo tendrá una dirección en cada pila. Se pueden utilizar direcciones IPv4 e IPv6 relacionadas o no, y se pueden utilizar mecanismos manuales o automáticos para la asignación de las direcciones (cada una correspondiente al protocolo en cuestión). La dirección podrá devolver la dirección IPv4, la dirección IPv6, o ambas.

Algunas características de IPv6 están explícitamente diseñadas para simplificar la migración. Por ejemplo, las direcciones IPv6 pueden ser automáticamente derivadas de direcciones IPv4, túneles IPv6 pueden construirse sobre redes IPv4, y por lo menos en la fase inicial, todos los nodos IPv6 harán parte de la pila dual; es decir, ellos soportaran ambos protocolos IPv4 e IPv6 al mismo tiempo. La figura 1.8 muestra a nivel de capas como se tendría la pila dual IPv4/IPv6.

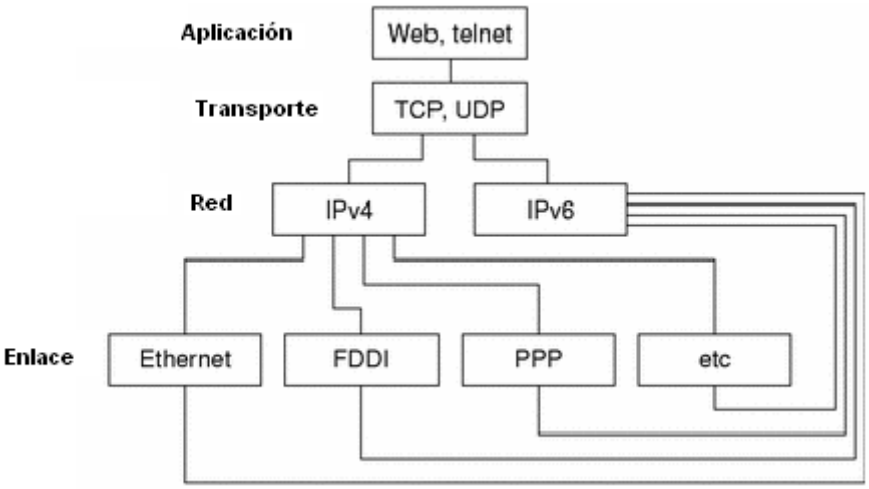


Figura 1.8 Pila dual, protocolos IPv4 e IPv6.

1.6.2 Túneles IPv6 sobre IPv4.

Los túneles proporcionan un mecanismo para utilizar la infraestructura IPv4, mientras la red IPv6 esta siendo implementada. Consiste en enviar datagramas IPv6 encapsulados en paquetes IPv4.

Los extremos finales del túnel siempre son los responsables de realizar la operación de encapsulado del paquete/es IPv6 en IPv4.

Estos túneles pueden ser utilizados de formas diferentes:

- Enrutador a enrutador. Enrutador con pila dual (IPv6/IPv4) se conectan mediante una infraestructura IPv4 y transmiten tráfico IPv6. El túnel comprende un segmento que incluye la ruta completa, extremo a extremo, que siguen los paquetes IPv6.

- Host a enrutador. Hosts con pila dual se conectan a un enrutador intermedio (también con pila dual), alcanzable mediante una infraestructura IPv4. El túnel comprende el primer segmento de la ruta seguida por los paquetes.
- Host a host. Hosts con pila dual interconectados por una infraestructura IPv4. El túnel comprende la ruta completa que siguen los paquetes.
- Enrutador a host. Enrutadores con pila dual que se conectan a hosts también con pila dual. El túnel comprende él último segmento de la ruta.

Los túneles se clasifican según el mecanismo por el que el nodo que realiza el encapsulado determina la dirección del nodo extremo del túnel. En los dos primeros casos (enrutador a enrutador y host a enrutador), el paquete IPv6 es tunelado a un enrutador. El extremo final de este tipo de túnel, es un enrutador intermedio que debe desencapsular el paquete IPv6 y reenviarlo a su destino final. En este caso, el extremo final del túnel es distinto del destino final del paquete, por lo que la dirección en el paquete IPv6 no proporciona la dirección IPv4 del extremo final del túnel. La dirección del extremo final del mismo ha de ser determinada a través de información de configuración en el nodo que realiza el túnel. Es lo que se denomina “túnel configurado”, describiendo aquel tipo de túnel en donde el extremo final de este es explícitamente configurado. Tal como se observa en la figura 1.9 donde cada extremo es un nodo dual y en ellos se configuran las direcciones IPv4 e IPv6 tanto locales como remotas.

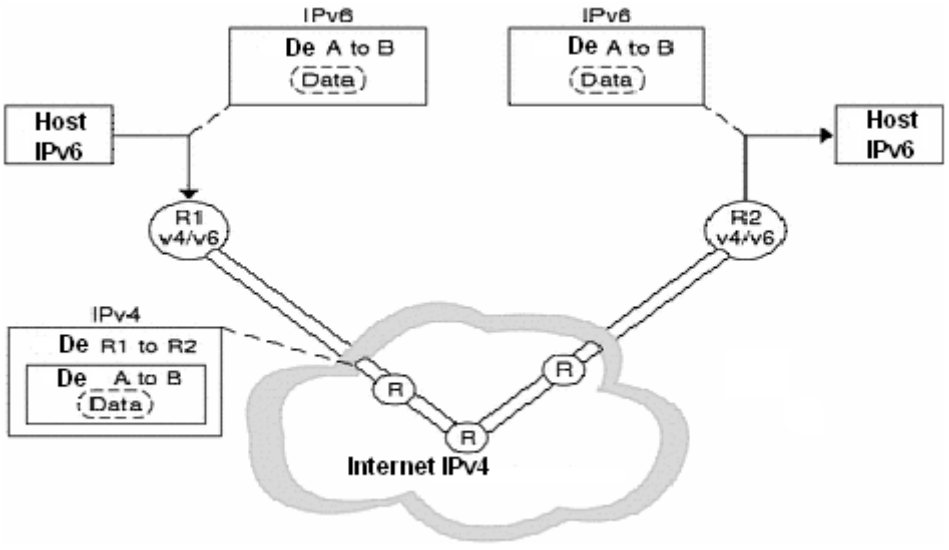


Figura 1.9 Túnel Configurado o Manual.

En los otros dos casos (host a host y enrutador a host), el paquete IPv6 es tunelado, durante todo el recorrido, a su nodo destino. El extremo final del túnel es el nodo destino del paquete, y por tanto, la dirección IPv4 esta contenida en la dirección IPv6. La figura 1.10 muestra como el paquete IPv6 es encapsulado colocándole una cabecera IPv4. Este caso se denomina “túnel automático”.

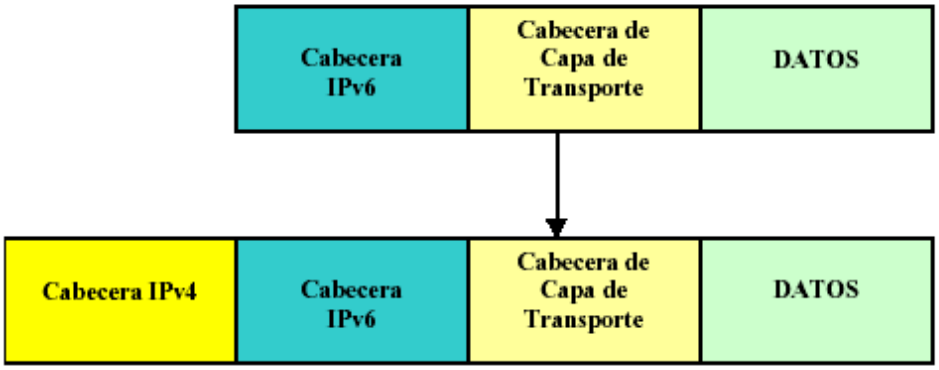


Figura 1.10 Paquete IPv6 y Paquete IPv6 con cabecera IPv4.

El extremo final del túnel, es el encargado de quitar la cabecera IPv4 y mandar el paquete IPv6 a su destino final.

Principales características del túnel automático (El túnel automático se puede observar en la figura 1.11 de color naranja):

- Permitir a nodos duales comunicarse a través de una infraestructura IPv4.
- Dirección IPv6 " IPv4 – compatible": Prefijo 0::/96 + dirección IPv4.
- Se define una interfaz virtual para la dirección "IPv4 compatible".
- Los paquetes destinados a direcciones "IPv4 compatibles" son enviados por el túnel automático siguiendo las siguientes reglas:

    - Dirección origen IPv6: Dirección "IPv4 compatible" local.
    - Dirección destino IPv4: Extraída de la dirección "IPv4 compatible" remota.

En la Figura 1.11 se observa un ejemplo de los dos tipos de túnel, túnel automático y túnel manual en donde se observan host IPv6 aislados (sin enrutadores IPv6 sobre el enlace). De color verde se observa un enlace con un túnel configurado manualmente y de color naranja se observa un túnel automático el cual se establece entre sistemas finales como ya se ha dicho anteriormente.

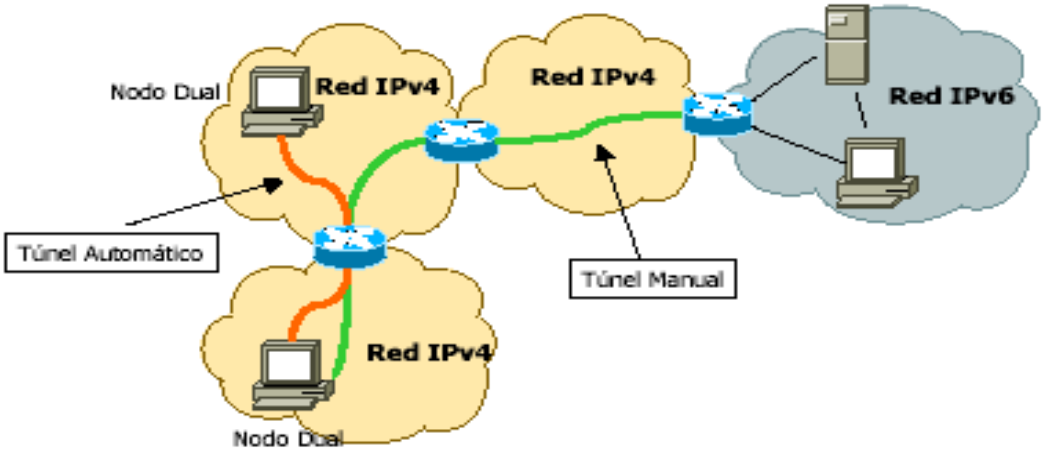


Figura 1.11 Túnel Configurado y Túnel Automático.

Los túneles automáticos se establecen directamente entre sistemas finales y, como su nombre indica, no necesitan ser configurados, ya que se utilizan conjuntamente con direcciones IPv6 especiales que contienen una dirección IPv4 (por ejemplo ::192.168.17.1). Su funcionamiento es simple: el sistema origen encapsula directamente los datagramas IPv6 sobre datagramas IPv4 cuya dirección IPv4 destino obtiene de la parte final de la dirección IPv6. Estos túneles se utilizan principalmente para comunicar sistemas IPv6 localizados en redes cuyos enrutadores no soportan IPv6 (encapsulado extremo a extremo). La figura 1.12 presenta un túnel automático en donde la comunicación se hace entre el origen y el destino.

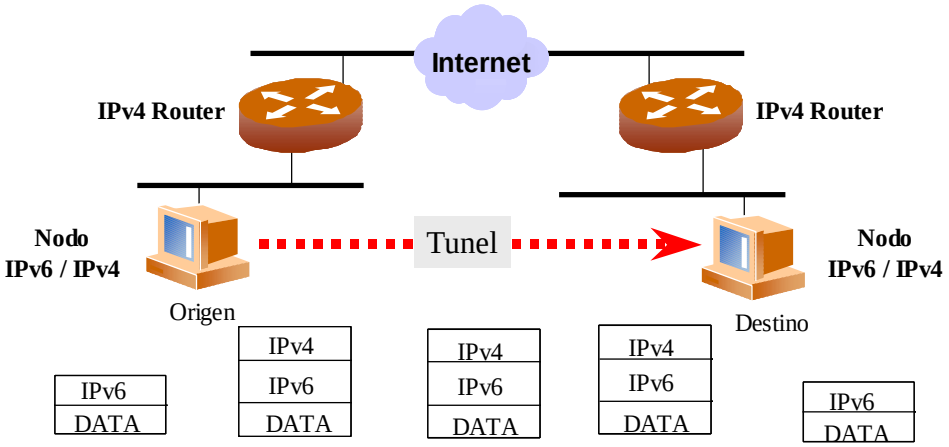


Figura 1.12 Túnel automático.

1.6.3 Túneles 6to4.

6to4 es una manera fácil de obtener conectividad de IPv6 para máquinas que sólo cuentan con una conexión de IPv4. Puede ser usado tanto en máquinas que tienen

asignaciones de IP estáticas como las que tienen direcciones dinámicas, por ejemplo, en escenarios de marcación y conexión vía modem. Cuando se utilizan direcciones dinámicas de IPv4, se debe notar que un cambio dinámico de los números de IP sería un problema para el tráfico que entra, por lo tanto en este tipo de escenario no se podrán correr servidores persistentes.

Este tipo de túnel esta definido en: “Draft-ietf-ngtrans-6to4-06.txt.” sus principales características son:

- Unir islas IPv6 en un océano IPv4.
- A cada isla IPv6 se le asigna un prefijo IPv6: 2002::/16 + Dirección IP del enrutador frontera.
- Siguiente salto IPv4 contenido en la dirección IPv6.
- El encaminamiento entre las distintas islas se apoya en el encaminamiento IPv4 subyacente.

En la figura 1.13 se observa el escenario de un grupo de usuarios IPv6 conectados a través de túneles 6to4 utilizando Internet y sus mecanismos de encaminamiento IPv4 existentes.

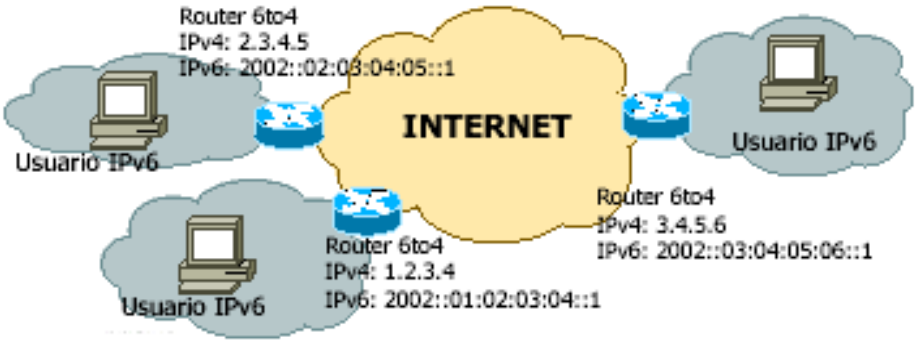


Figura 1.13 Túnel 6to4.

Ventajas:

- Al igual que los túneles manuales, son transparentes a nivel IPv6 y, por tanto, no afectan a las aplicaciones.
- Se trata de túneles establecidos dinámicamente y sin configuración previa.
- Dada N islas IPv6, sólo se establecen los túneles necesarios para las conexiones activas en cada momento.

Inconvenientes:

- Para organizaciones que se conecten a un ISP IPv6 remoto, no es necesario mas que un túnel (o quizá dos por redundancia con otro ISP IPv6), por lo que puede ser suficiente emplear el mecanismo de túneles manuales, que se haya más extendido.

El prefijo de dirección "2002:" del que se habló anteriormente y que se observa en las direcciones de la figura 1.13 es reservado para direcciones basadas en 6to4 (direcciones de IPv6 derivadas de direcciones de IPv4). Los 32 bits siguientes al prefijo de 6to4 corresponden a la dirección de IPv4. Esto da como resultado que se pueda obtener una red /48 que puede utilizar para propósitos propios. Lo que deja un espacio de 16 bits para contar con 2^{16} subredes de IPv6, cada una con 2^{64} direcciones posibles.

La figura 1.14 muestra un ejemplo de como se construye una dirección de IPv6 a partir de la dirección IPv4 200.30.31.72. Los bits menos significativos ":0001::1" fueron escogidos arbitrariamente y pueden contener cualquier otro número que puede determinar según convenga.

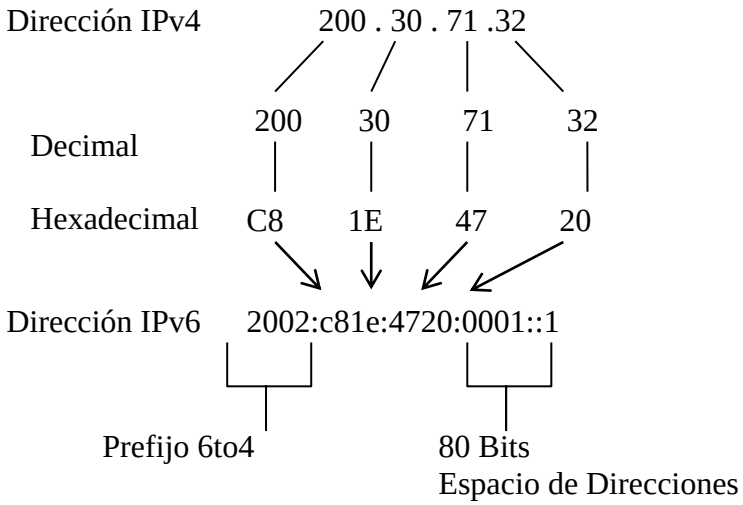


Figura 1.14 Conversión de la dirección IPv4 a una dirección IPv6 para 6to4

Gracias al prefijo de 6to4 y a la dirección de IPv4 única en todo el mundo, este bloque de direcciones es también único, y esta mapeado solo para uso propio.

En contraste con la clásica configuración de "IPv6 sobre un túnel de IPv4", no se tiene que registrar en un gateway de 6bone para conseguir conexión, el cual hará un reenvió de todo el tráfico de IPv6 que se dirija al usuario. En lugar de eso, como la dirección de IPv6 es derivada de la dirección de IPv4, cualquier respuesta puede ser enviada a través de la gateway 6to4 más cercana. El desencapsulado se realiza vía la interfaz 4 de red en Windows XP, la cual también hace el reenvió del paquete IPv6 resultante de acuerdo a la configuración de ruteo (en caso de que se tenga más de una máquina conectada a la red de 6to4 asignada).

Para enviar al exterior paquetes de IPv6, la interfaz de red 4 tomará el paquete v6, y lo encapsulará en un paquete v4. Se debe notar que aún necesitará un “gateway” de 6to4 conectado al 6bone que se encargará de desencapsular los paquetes y reenviarlos al 6bone.

1.6.4 Transmisión de IPv6 sobre dominios IPv4 (RFC2529).

Este mecanismo permite a hosts IPv6 aislados, sin conexión directa a enrutadores IPv6, ser totalmente funcionales como dispositivos IPv6. Para ello se emplean dominios IPv4 que soportan multicast como su enlace local virtual. Es decir, se usa multicast IPv4 como "ethernet virtual". De esta forma, estos hosts IPv6 no requieren direcciones IPv4 compatibles, ni túneles configurados.

Los extremos finales del túnel se determinan mediante ND (neighbor discovery, descubrimiento de vecinos). Es imprescindible que la subred IPv4 soporte multicast. Este mecanismo se denomina comúnmente "6over4".

En la figura 1.15 se puede observar la topología típica de un túnel 6over4 el cual se describe en el RFC 2529 y cuyas principales características son:

- Nodos IPv6 dispersos en subredes IPv4: Se forma una "LAN virtual" IPv6.
- Tráfico IPv6 entre nodos encapsulados en IPv4. Direcciones IPv4 multicast.
- Los procesos de descubrimiento de enrutadores vecinos se hace empleando multicast.
- Los enrutadores 6over4 tienen acceso al 6Bone lo que implica que todos los nodos acceden al 6Bone.

Ventajas:

- Al igual que los túneles anteriores, son transparentes a nivel IPv6 y, por tanto, no afectan a las aplicaciones.
- Se trata de túneles establecidos dinámicamente y sin configuración previa.
- Permite probar IPv6 en algunos nodos de una red IPv4 corporativa sin instalar el "stack" IPv6 en los enrutadores internos.
- Instalado en un solo enrutador el "stack" IPv6 y conectándolo al 6Bone se proporciona acceso a dicha red a todos al resto de nodos IPv6.

Inconvenientes:

- Se trata de un mecanismo adecuado para redes finales únicamente.
- Todavía no esta ampliamente implementado (Windows NT).

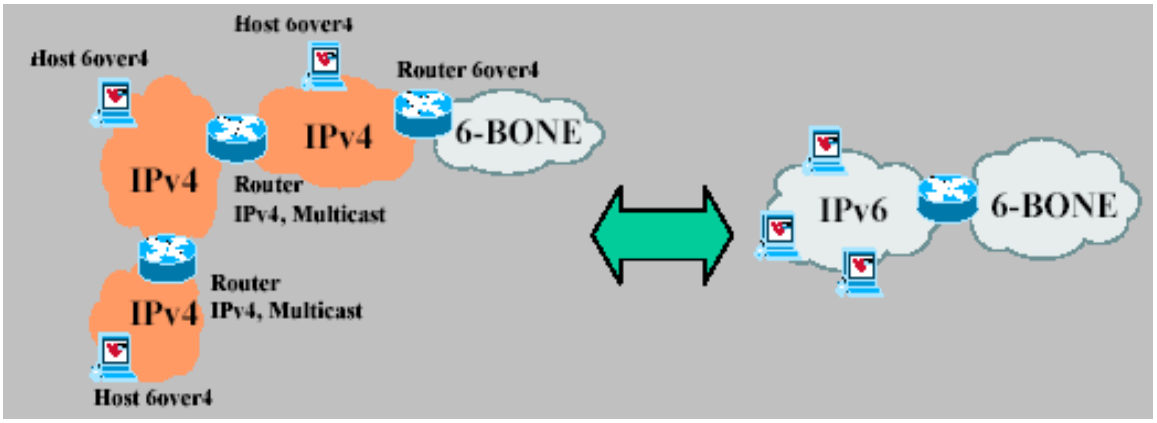


Figura 1.15 Túnel tipo 6over4.

1.6.5 Mecanismos de traducción.

Se basan en traducir, los paquetes de un formato a otro, en un elemento de la red, como se puede observar en la figura 1.16.

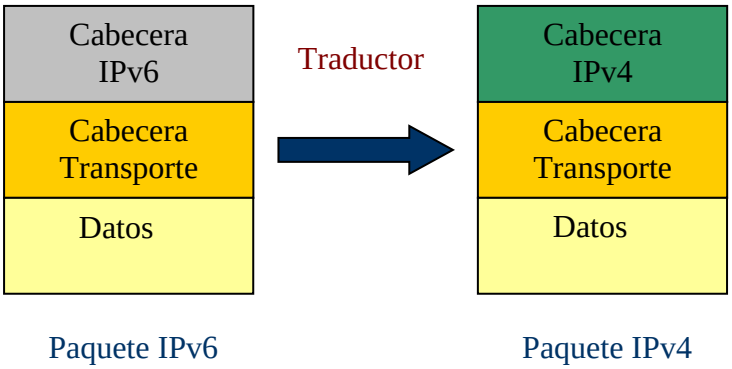


Figura 1.16 Mecanismo de traducción de protocolos.

NAT-PT (RFC 2766): Es una de las especificaciones de IETF (Internet Engineering Task Force) que definen como debe ser un enrutador de extremo para permitir la transición de IPv4 a IPv6. La topología básica de este mecanismo se observa en la figura 1.17 Define la conversión de paquetes IPv4 privados en paquetes IPv6 públicos.

Características principales:

- NAT tradicional: Traduce direcciones (conexión de redes con dirección IPv4 privada).
- NAT-PT: Traducción de direcciones y protocolo.
- Traducción basada en el algoritmo SIIT, de traducción de cabeceras (RFC 2765).
- No es transparente a nivel de aplicación, esto precisa de algunas extensiones.

  - DNS-ALG:Transforma peticiones DNS “A” a peticiones “AAAA”.
  - FTP-ALG:Las conexiones con FTP son problemáticas pues abren dos conexiones TCP intercambiando direcciones IP a nivel de aplicación.

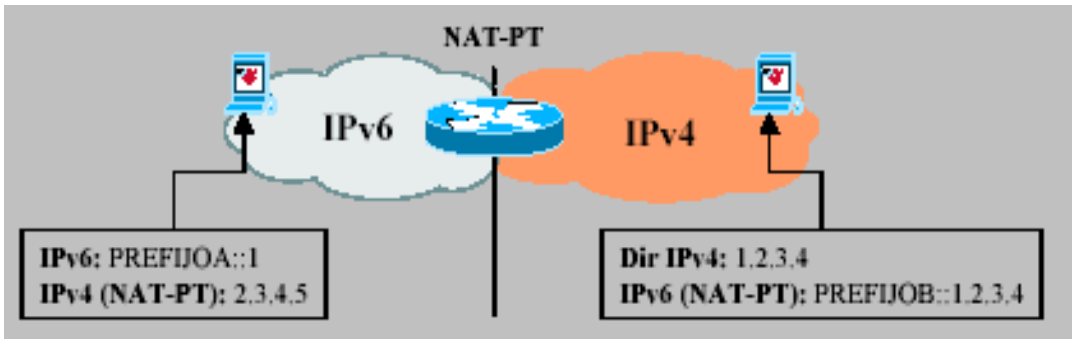


Figura 1.17 Mecanismo de traducción NAT-PT.

Ventajas:

- Muchas redes corporativas poseen experiencia en la gestión/administración de NATs.
- Implementado en la mayor parte de enrutadores (Cisco,Telebit,Linux) y en algunas plataformas habituales en nodos finales(Windows 2000).
- Si la comunicación extremo a extremo es heterogénea (IPvX-IPvY) NAT.PT resulta adecuado (teniendo en cuenta siempre la carga de tráfico prevista).

Inconvenientes:

- Los NATs poseen un alto coste de gestión y administración.
- El proceso de traducción es más costoso en recursos que el de tunelado.
- Si la comunicación extremo a extremo es homogénea (IPvX - IPvX) siempre es preferible emplear túneles a dos sistemas de traducción consecutivos.
- Si en un protocolo de aplicación intercambian direcciones IP (DNS,FTP,etc), es necesario una extensión o módulo que incluya un algoritmo para su tratamiento específico (DNS-ALG,FTP-ALG).

SOCKSv5: Este tipo de mecanismo esta definido en el RFC 1928, la figura 1.18 muestra una red que utiliza este mecanismo. Sus características principales se pueden resumir en:

- Uso tradicional SOCKSv5: conectividad Indirecta a Internet en redes con “firewall” a determinados hosts.
- Servidor SOCKSv5 dual, atizando el traductor de protocolos (Algoritmo SIIT, de traducción de cabeceras).
- Traducción IPv4-IPv6 y viceversa. Conexiones siempre iniciadas por cliente.
- Dos componentes: servidor SOCKSv5 +librería SOCKSv5 (cliente).

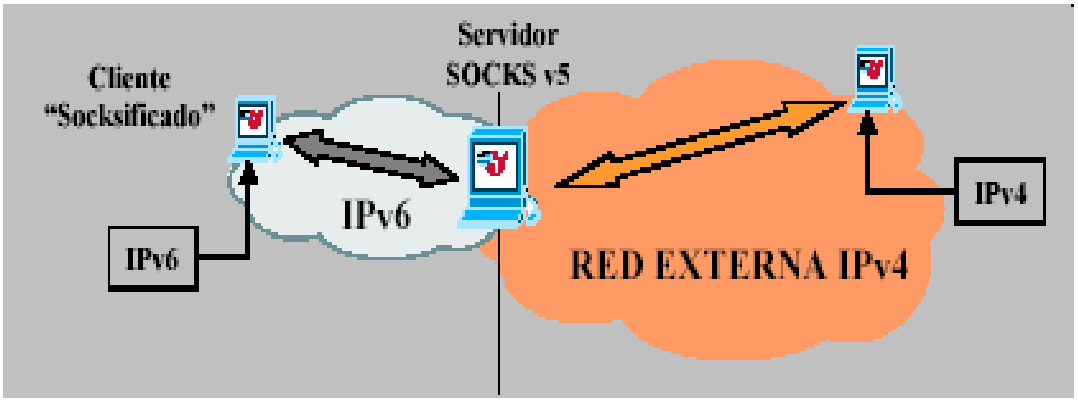


Figura 1.18 Mecanismo de traducción SOCKSv5.

Ventajas:

- Sistema apto actualmente para corporaciones que deseen dar acceso a determinados nodos internos a servicios IPv6 sin probar exhaustivamente el protocolo.
- Provee sistemas de autentificación adecuados para evitar usos indeseados.

Inconvenientes:

- Instalación de librerías SOCKSv5 en todos los clientes a los que se desee dar acceso.
- El proceso de traducción es costoso en cuanto a consumo de recursos en el servidor, por lo que un factor limitante es la carga de tráfico prevista.
- Las conexiones sólo pueden ser iniciadas por los nodos internos, con lo cual no es posible ofrecer servicios al exterior mediante este método.
- Como todos los mecanismos de traducción debe incorporar algoritmos específicos para aquellos protocolos de aplicación que intercambien direcciones IP(FTP).

1.6.6 "Tunnel server" y "tunnel broker".

El documento publicado por la IETF, draft-ietf-ngtrans-broker-02.txt sienta las bases para aplicaciones que permiten utilizar, de forma libre y gratuita, las direcciones IPv4 actuales, sobre las infraestructuras IPv4, para acceder a redes y sitios IPv6.

Estos mecanismos se hacen indispensables para labores de investigación, dado que se requieren direcciones IPv6 y nombres DNS permanentes. La diferencia con el mecanismo "6to4" es que el "Túnel Broker" no requiere la configuración de un enrutador. Se trata de ISP's IPv6 "virtuales", proporcionando conectividad IPv6 a usuarios que ya tienen conectividad IPv4.

El "Túnel Broker" es el lugar donde el usuario se conecta para registrar y activar "su túnel". El "Broker" gestiona (crea, modifica, activa y desactiva) el túnel en nombre del usuario.

El "Túnel Server" es un enrutador con pila doble (IPv4 e IPv6), conectado a Internet, que siguiendo ordenes del "Broker" crea, modifica o borra los servicios asociados a un determinado túnel / usuario.

El mecanismo para la configuración es tan sencillo como indicar, en un formulario WEB, datos relativos al S.O., la dirección IPv4, un "apodo" para la máquina, y el país donde esta conectada. El servidor de túneles crea los registros DNS, el extremo final del túnel, y genera un script para la configuración del cliente.

1.6.7 SIT (Simple Internet Transition).

Un conjunto de mecanismos llamados SIT (Simple Internet Transition) ha sido implementado; Este incluye protocolos y la gestión de las normas para simplificar la migración.

Las principales características de SIT son las siguientes:

- Posibilidad de una progresiva y no traumática transición: Hosts y Erutadores IPv4 pueden actualizarse a IPv6, uno a la vez, sin que otros Hosts o Enrutadores sean actualizados simultáneamente.

- Requisitos mínimos para la actualización: El único requisito para la actualización de los Hosts a IPv6 es la disponibilidad de un servidor DNS para manejar direcciones IPv6. Ningún requisito se necesita para los enrutadores.
- Simplicidad de direccionamiento: Cuando un enrutador o un host son actualizados a IPv6, también puede continuar usando direcciones IPv4.
- Costo inicial Bajo: Ningún trabajo preparatorio es necesario para empezar la migración a IPv6.

Los mecanismos usados por SIT incluyen lo siguiente:

- Una estructura de direcciones IPv6 que permiten la derivación de direcciones IPv6 a partir de direcciones IPv4.
- La disponibilidad de una pila dual en Hosts y en Enrutadores durante la transición, lo que significa, la presencia de ambas pilas IPv4 e IPv6 al mismo tiempo.
- Una técnica para encapsular paquetes IPv6 dentro de paquetes IPv4, llamada "tunneling" para permitir que paquetes IPv6 crucen por redes aún no actualizadas con IPv6.
- Una técnica opcional que consiste en traducir las cabeceras IPv6 en cabeceras IPv4 y viceversa para permitir, en una fase avanzada de la migración, que nodos sólo IPv4 se comuniquen con nodos solo IPv6.

El SIT garantiza que Hosts IPv6 puedan interoperar con Hosts IPv4 inicialmente en la Internet. Cuando la migración se complete, esta interoperabilidad se garantizará localmente durante mucho tiempo. Esta capacidad permite la protección de inversiones hechas durante la existencia de IPv4, dispositivos simples que no pueden ser actualizados a IPv6 por ejemplo, impresoras de red, y los servidores terminales continuaran operando con IPv4 hasta que ellos ya no sean usados.

La posibilidad de una migración gradual les permite a los fabricantes integrar IPv6 en Enrutadores, sistemas operativos, y software de red hasta cuando ellos consideren que las aplicaciones son estables, así los usuarios podrán comenzar la migración una vez ellos lo consideren apropiado.

1.7 Estrategias de migración.

En general, se debería comenzar por migrar los extremos finales de las redes (hosts), continuar con redes finales (LANs) y, según aumente el tráfico IPv6 migrar ISP y Backbones principales.

Recomendaciones para redes finales:

- Servidores "Doble stack": para atender peticiones IPv4 e IPv6.
- Clientes "Doble stack": conectividad con servidores IPv4 e IPv6.

1.7.1 Estrategia de migración de redes finales (clientes y servidores).

- Mediante mecanismos de traducción: como los anteriormente descritos. La figura 1.19 muestra un ejemplo de cómo se haría esta transición de IPv4 a IPv6.

- Mediante mecanismos de tipo túnel: la primera fase de este mecanismo consistiría de la conexión de IPv4 al ISP y entunelar el tráfico IPv6 en IPv4, hasta que el ISP ofrezca conexión con IPv6 nativo. Como se muestra en la figura 1.20

Una segunda fase consistiría en establecer una conexión IPv6 al ISP y túnel IPv4 sobre IPv6 para conectar Internetv4. Este como un caso complementario.

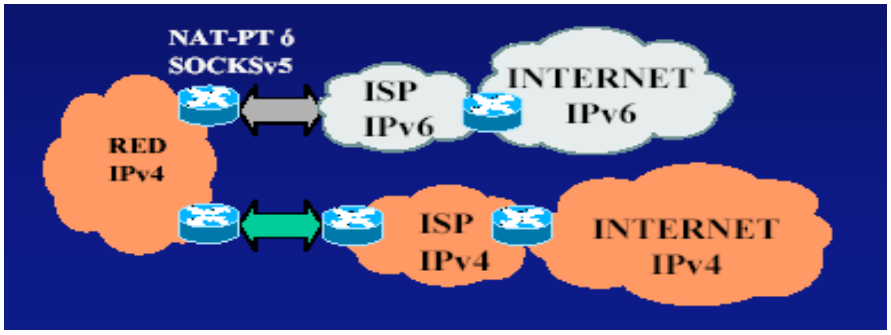


Figura 1.19 Ejemplo de migración de redes finales (clientes y servidores). A través de mecanismos de traducción.

1.7.2 Estrategias de migración para ISP´s.

- Conexión nativa a Backbones IPv4 e IPv6, sin emplear túneles.
- Modos de acceso:

  - ISP IPv4 tradicionales: Acceso IPv4 y tratar de ofrecer acceso a Internetv6 mediante un traductor.
  - Nuevos ISP IPv6: Acceso IPv6 mediante túnel a través de Internet. Ofrecer conectividad a Internetv4 mediante traductores.

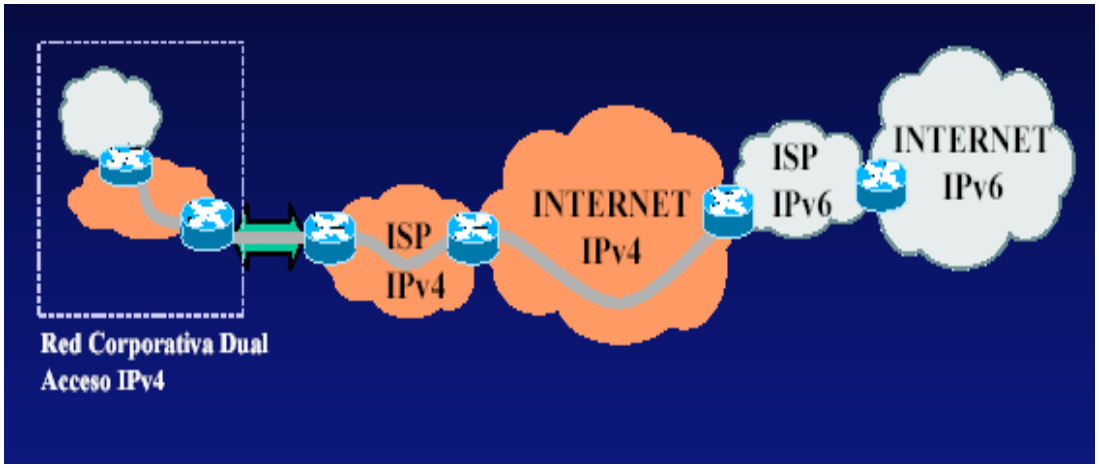


Figura 1.20 Ejemplo de migración de redes finales (clientes y servidores). A través de mecanismos de tipo túnel.

1.7.3 Estrategia de migración de backbones.

- Mantener la configuración actual y migrar cuando el tráfico entunelado sea mayor que el tráfico IPv4.
- Debido a los problemas del número de rutas existente, recomendar y colaborar con los ISP y otros Backbones para evitar una migración “forzosa”.

Finalmente y para concluir este capítulo se tiene que las metas más importantes de la migración son:

- Hosts IPv6 e IPv4 deben interoperar.
- El uso de Host IPv6 y enrutadores debe distribuirse sobre Internet de una manera simple y progresiva, con un poco de interdependencia.
- Administradores de red y usuarios finales deben pensar que la migración es fácil de entender y llevar a cabo.

CAPÍTULO 2

EL USO DE IPv6 PARA COMUNICACIONES MÓVILES

La “informática móvil” es sin duda alguna, uno de los más intrigantes y complejos retos que tienen que afrontar las diferentes redes de telecomunicaciones. En efecto, aunque se afirme, que la necesidad, de la que debe hacerse cargo la informática móvil “acceso a la información, comunicaciones y servicios en cualquier momento y en cualquier lugar” es algo fácil, encontrar soluciones técnicas satisfactorias no es igualmente fácil. De hecho, la informática móvil requiere la generación de infraestructura de comunicación y la modificación de las redes de computadores, sistemas operativos, y programas de aplicación.

IPv6 representa un cambio real para la informática móvil. De hecho, porque IPv6 ha sido completamente rediseñado, desde su concepción se ha previsto la necesidad de apoyar eficazmente la informática móvil y no ha sido limitado, en la opción de soluciones, por requisitos de compatibilidad, con versiones del pasado.

Como se menciono en el Capítulo 1, un número creciente de usuarios de Internet, ya no trabajan en los escritorios de la oficina, pero si trabajan mientras están viajando. Los siguientes casos ocurren más frecuentemente: Primero, cuando los usuarios son empleados de una compañía con varias estaciones de trabajo y ellos desean tener la posibilidad de trabajar de la misma manera en todas las estaciones de trabajo, conectando sus PCs portátiles, a las redes de las diferentes estaciones de trabajo de la compañía o a la red telefónica (en este caso, RDSI) en sus oficinas; el segundo caso pasa cuando los usuarios nómadas (del cual se deriva el término "informática nómada") viajan y trabajan con poca frecuencia en sus oficinas. Claro, suponiendo que ellos aún tengan oficinas. Este segundo tipo de usuario móvil, que es normalmente provisto con un PC móvil y con una placa PCMCIA (asociación internacional de tarjetas de memoria para computadores personales) para un teléfono móvil, se conecta a Internet a través de una red radio móvil pública.

Claramente, el requerimiento de proveer soporte a la movilidad en IPv6 es un asunto de mucha importancia. En Norte América, las estimaciones indican que habrá de 20 a 40 millones de usuarios móviles en el 2007. También, este requerimiento es claramente uno de los más complejos a la hora de ser discutidos, porque ha tratado con una multitud de problemas que van desde aquéllos relacionados a la radio transmisión (fiabilidad, roaming, hand-off), los protocolos IP (identificación, direccionamiento, configuración, encaminamiento) e igualmente los importantes problemas de seguridad.

2.1 Los problemas de la movilidad.

El direccionamiento y los esquemas de enrutamiento, en IPv4 implican que la dirección del nodo depende del punto donde este se conecte a la red. Esto es exactamente lo opuesto de lo que se necesita para la movilidad, porque un nodo móvil frecuentemente

cambia su punto de conexión a la red y por consiguiente debe cambiar su dirección con igual rapidez. En la figura 2.1 se muestra la arquitectura de una red IPv4 móvil.

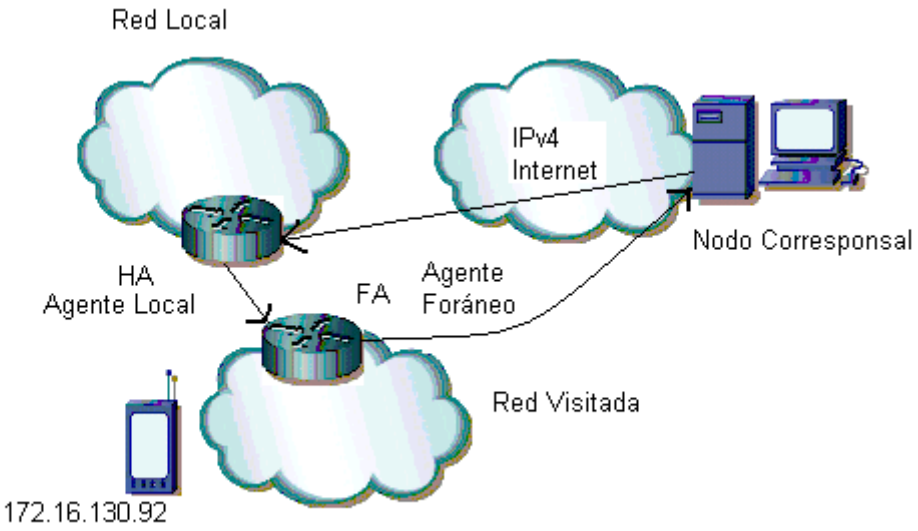


Figura 2.1 Red IPv4 Móvil.

Una primera solución podría manejar la movilidad operando a nivel del DNS (Servicio de Nombre de dominio). El DNS, en IPv6, es el servicio que permite identificar los nodos por nombres, las direcciones son variables en el tiempo y no código mnemotécnico, y los nombres son trasladados a las direcciones por el DNS. Este acercamiento no seria el más adecuado porque el DNS se ha diseñado para minimizar los tiempos de búsqueda de información pero no para actualizarse de inmediato. Es por consiguiente imposible pensar que, cuando un nodo se mueve, propague su nueva dirección a través del DNS, porque actualizarlo podría tardar muchos días, considerando que el nodo debe permitir moverse una vez por segundo.

En general, no es posible pensar que un nodo IP cambie su dirección cuando se mueve. De hecho, la arquitectura de red TCP/IP tiene una estructura de capas imperfecta, en el que TCP no sólo usa los puertos TCP de la fuente y destino sino que también utiliza la dirección IP de la fuente y destino como el identificador de conexión. Esto significa que si la dirección IP de un nodo es cambiada, entonces todas las sesiones de la capa superior de los protocolos relacionados a este nodo serán terminadas. El proceso de direcciones cambiantes normalmente requiere varios días mientras las nuevas y viejas direcciones coexisten.

La situación precedente es un resultado del hecho de que las direcciones IP, en la arquitectura de red TCP/IP, tengan dos propósitos diferentes: identificar las conexiones de los puntos terminales y determinar la ruta del paquete. El hecho que Las direcciones IP identifiquen las conexiones de los puntos terminales significa que estos puntos deben permanecer estables y que un nodo móvil debe identificarse por consiguiente siempre por la misma dirección que esta asociada con el nombre del DNS. Ya que la dirección también se usa para propósitos de enrutamiento, un nodo móvil debe adquirir una o más

direcciones de la red a la que se conecta (red foránea) para ser usados por los paquetes de enrutamiento.

La dirección permanente del nodo, es llamada la "dirección local" (home address), esta es la dirección del nodo cuando se conecta a su red predefinida, la cual es llamada la "red local" (home network). Las direcciones que el nodo móvil adquiere cuando se conecta a una red foránea se llaman "direcciones anfitrionas" (care-of-addresses). La dirección anfitriona es adquirida por el nodo móvil cuando se conecta a una red foránea a través de un procedimiento de auto configuración o a través de DHCP (dynamic host configuration protocol), el cual es un protocolo que permite manejar rangos de direcciones IP de forma dinámica y automatizada.

Los problemas de gestión de la movilidad en IPv6 son por consiguiente problemas de gestión de la relación entre las direcciones locales y las direcciones anfitrionas, y problema del uso del tipo apropiado de dirección en relación al contexto. Es más, cuando el nodo móvil se conecta a una red foránea, debe delegar un enrutador de su red local para “representarlo” mientras está ausente. Este enrutador asume el nombre de “agente local” (home agent).

Un agente local normalmente sirve a todos los nodos móviles de una red local reenviando los mensajes que se dirigieron a ellos. Para hacer esto, el agente local rastrea todos movimientos del nodo móvil y en particular, los almacena en memoria, la cual es llamada "memoria cache de enlace" (binding cache), esto es el mapeo entre las direcciones locales y las direcciones anfitrionas.

De este escenario, se puede ver que IPv6 es conveniente para proporcionar soporte para la movilidad en redes heterogéneas y que puede usarse en ambos casos, para moverse de una red Ethernet a otra y para moverse de una red Ethernet a una red inalámbrica. Es más, note que IPv6 se ha concebido para soportar “macro” movilidad y que es menos conveniente para la “micro” movilidad, en la que, por ejemplo, un nodo se mueve entre dos células de una LAN inalámbrica. En el último caso, la movilidad puede ser más eficazmente llevada a cabo usando mecanismos de la capa de enlace (capa 2 del modelo OSI).

2.2 Operación de un nodo móvil en ipv6.

Cuando un nodo móvil se conecta a una red foránea, decide adquirir una dirección anfitriona (care-of-address) a través de un procedimiento automático o a través de DHCP, sobre la base de mensajes de "Anuncios de enrutador" recibidos.

Cada vez que un nodo móvil cambia su punto de conexión en la capa de enlace de una subred IPv6 a otra subred IPv6, debe adquirir una nueva dirección anfitriona que se vuelve su dirección anfitriona primaria. Otra dirección anfitriona previamente adquirida puede mantenerse para permitirle al nodo continuar recibiendo paquetes dirigidos a la anterior dirección anfitriona. Este procedimiento puede ser útil en el uso de redes de radio en las que un nodo puede decidir configurar él mismo la célula de la que recibe la señal de más alto poder, pero además continuar también recibiendo señal de otras células que previamente le sirvieron.

El mapeo entre la dirección local y la dirección anfitriona primaria es llamado enlace ("binding"). Cada vez que el nodo móvil configura una nueva dirección anfitriona primaria, y por consiguiente un nuevo enlace, debe comunicar la dirección a su agente local a través de una Actualización de enlace. El mensaje de Actualización de enlace también debe enviarse a todos los nodos con los que el nodo móvil tenía un intercambio de paquetes y qué pueden tener información obsoleta en sus memoria cache de enlace. Por esta razón, el nodo móvil mantiene una estructura de datos, llamada una Lista de actualización de enlaces, esta lista contiene direcciones de todos los nodos a los que envió mensajes de Actualización de enlace y el valor temporal de la permanencia relativa.

Un nodo móvil, en un momento cualquiera, puede ser localizado enviando un mensaje a su dirección local. Si el nodo móvil no se conecta a su red local, todos los paquetes remitidos a él serán interceptados por el agente local, qué los transmitirá al nodo móvil a través de un túnel usando la dirección anfitriona primaria.

Cuando un paquete llega al nodo móvil a través de un túnel, el nodo móvil comprende que ha sido reenviado por el agente local y envía un Mensaje de Actualización de enlace al nodo fuente. Cuando el nodo fuente recibe este mensaje, crea en su memoria cache de enlace una entrada que contiene la dirección local y la dirección anfitriona. Esta información permite al nodo fuente directamente reenviar los siguientes paquetes a la dirección anfitriona a través de una cabecera de ruta en lugar de a través de un túnel (una técnica sólo usada por el agente local).

Por consiguiente, sólo el primer paquete de una sucesión de paquetes intercambiados entre un nodo fuente y un nodo móvil atraviesa el agente local como se puede ver en la figura 2.2, considerando que todos los otros paquetes son transmitidos directamente por la fuente al nodo móvil a través de la cabecera de ruta. Este proceso es fundamental para la obtención de una solución escalable, fiable y que minimice la carga de la red.

Cuando el nodo móvil se mueve (cambia su dirección anfitriona), este reenvía un mensaje de Actualización de enlace a todos los nodos en la lista de Actualización de enlaces.

El mensaje de Actualización de enlace debe incluir una Autenticación de cabecera para evitar una situación en la que potenciales hackers pudieran redireccionar el tráfico de alguien más hacia ellos para un uso fraudulento de éstos mensajes.

2.3 Ejemplo de operación de un host móvil en IPv6.

Para entender los temas presentados en la sección anterior, considere el ejemplo mostrado en la Figura 2.3. El nodo Z normalmente se conecta a la subred A que es su red local, Z adquiere de A la dirección A::1 que es su dirección local. (la sintaxis para esta dirección no es correcta, pero servirá de ejemplo). Esta dirección A::1 se relaciona con el nombre Z a nivel del DNS. De la misma manera, el nodo W se conecta a la subred C, y de C, este adquiere la dirección C::5.

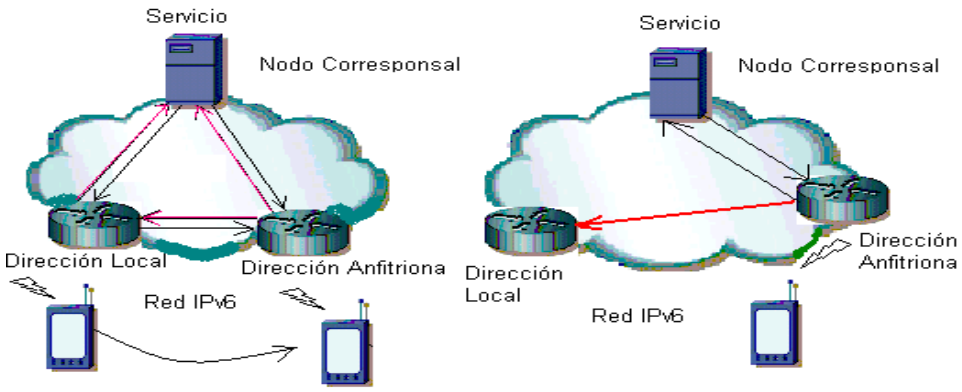


Figura 2.3 Red IPv6 Móvil.

Cuando el nodo W quiere remitirle paquetes a Z, le pregunta al DNS y obtiene la dirección A::1. Entonces W genera paquetes IPv6 cuya dirección de destino es A::1 y la dirección de la fuente es C::5 (2). Estos paquetes se enrutan a través de encaminamiento IPv6 y alcanzan la subred de destino A.

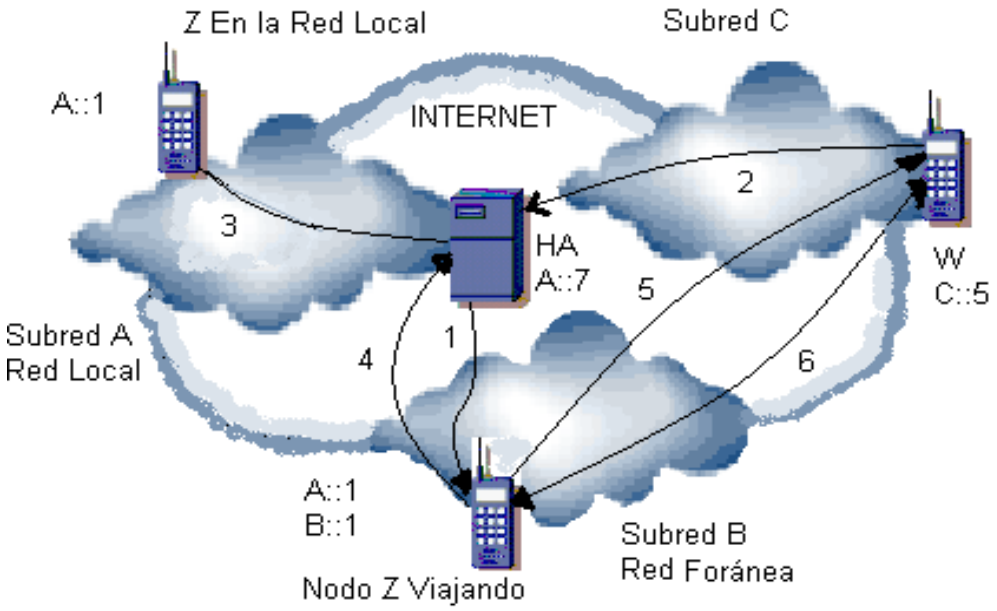


Figura 2.3 Ejemplo de operación de un host móvil en IPv6

A estas alturas, tres situaciones son posibles:

- **El nodo Z esta conectado a su red local:** Los paquetes se entregan a Z usando procedimientos de asignación de ruta clásicos en IPv6 (3).

- **El nodo Z esta conectado a la subred B que actúa como una red foránea:** Z adquiere de B su dirección anfitriona (care-of-address) B::1 que se comunica a través de un mensaje de actualización de enlace (1) a su agente local (home agent, HA). Los paquetes recibidos por el agente local se reenvían a Z a través de un túnel de A::7 a B::1 (4). Cuando B::1 extrae paquetes del túnel, verifica si ellos se dirigen a A::1 es decir, a sí mismo. en este punto, Z envía un mensaje de actualización de enlace a W (5), y W guarda el mensaje en su memoria cache de enlace. De este momento en adelante, W se comunica con Z sin atravesar el agente local, pero envía paquetes a Z a través de la cabecera de encaminamiento eso fuerza a la fuente a que se encamine hacia B::1 (6).

- **La tercera situación posible es que Z no este conectado en ningún lugar:** El enrutador conectado a la subred A intenta localizar a Z en la dirección A::1, y puesto que falla, comunica este fracaso al nodo de la fuente pero usando un mensaje ICMP.

Nota: El protocolo de control de mensajes de Internet versión 6 se describe en el Anexo A (ICMPv6).

Si Z se mueve de la subred B a la subred D, esta adquiere una nueva dirección perteneciente a la subred D (por ejemplo, D::11) esa se vuelve su nueva dirección anfitriona primaria. Esta nueva dirección se comunica a través de un mensaje de actualización de enlace tanto a su agente local como a W.

2.4 Opciones de formato.

La información necesaria para soportar la movilidad de un host IPv6 es intercambiada a través de cuatro opciones llevadas a cabo en la extensión de cabecera **Opción de Destino**. Puesto que la extensión de cabecera **Opción de Destino** puede ser parte de cualquier paquete IPv6, las opciones para la movilidad, pueden asociarse con lo siguiente:

- Paquetes normales IPv6 que contienen cargas útiles tales como TCP o UDP.
- Los paquetes Independientes, conteniendo sólo opciones. En este segundo caso, el siguiente campo de la cabecera Opción de Destino debe ponerse igual al valor 59 para indicar la falta de más cabeceras.
- Las opciones son codificadas según el formato TLV (Tipo, Longitud, Valor).

2.4.1 Opción de actualización de los enlaces.

Esta opción es utilizada por el nodo móvil para comunicarse con su propio agente, o con los nodos a los cuales necesite comunicarse en el proceso.

El campo de 8 bits llamado tipo de opción (*option type)* toma un valor de 192. El campo de 8 bits llamado Longitud del Campo (*Length field)* hace referencia a la longitud en octetos de la opción utilizada. Este campo toma un valor mínimo de 6 si tanto el campo llamado dirección anfitriona (*care of adress)* (C=0) como el campo dirección local del enlace local

(*home link local adress)* (L=0), no están presentes, su máximo valor es de 38, cuando (C=1, L=1), ambos están presentes.

EL campo conocido como A "Reconocimiento" (*Acknowledge*), es utilizado por el nodo fuente para pedirle al nodo que recibe la opción de actualizar el enlace, que envíe un mensaje de reconocimiento de determinado enlace.

El campo conocido como H registró local *(Home Registration),* es utilizado por el nodo fuente para pedirle al nodo que recibe la opción de actualización de enlaces, que trabaje como su propio agente. La dirección de destino del paquete IPv6 contiene esta opción y debe ser equivalente a la del enrutador, cuyo prefijo es el mismo que la dirección del nodo móvil.

El campo conocido como C dirección anfitriona presente (*Care-of Address Present*) es utilizado por el nodo fuente para indicar la utilización de la "dirección anfitriona" en la actualización de los enlaces.

El campo conocido como L *dirección local del enlace local presente (Home Link Local Address Present)* es utilizado por el nodo fuente para indicar la utilización de la "dirección local en el enlace local" en la actualización de los enlaces. También es utilizado por el mismo nodo fuente para pedirle al nodo destino que actúe como un Proxy, esto es que debe participar en el "descubrimiento", de los nodos vecinos en lugar del nodo móvil. Cuando este bit es activado, el campo H también debe ser llenado con un bit.

El campo de 12 bits denominado campo reservado (*Reserved* field) es como su nombre lo indica una reserva para el uso futuro. Debe ser inicializado a cero durante la transmisión e ignorado durante la recepción.

El campo de 16 bits llamado campo de tiempo de vida (*Lifetime field)* hace referencia al intervalo de validación que contiene la información del enlace, es decir cuanto tiempo debe ser considerada valida la información del enlace en la memoria de enlace. Cuando esta en cero dicha información debe ser borrada de la memoria, el valor de *0 * ffff* indica que dicha información debe ser mantenida indefinidamente.

El campo de 16 bits llamado número de secuencia (*Sequence Number)* es utilizado para relacionar los mensajes de actualización de enlaces y los mensajes de reconocimiento del enlace. Cada actualización del enlace enviada por un nodo móvil debe utilizar una secuencia de números más grande que la secuencia enviada en la actualización del enlace previo.

El campo de actualización llamado dirección anfitriona (*Care-of Address)* contiene la dirección IPv6 adquirida del nodo móvil que se encuentra fuera de su red local. Cuando el campo llamado dirección anfitriona tiene un valor igual al campo dirección local. La actualización del enlace indica que es necesario cancelar las asociaciones existentes en la memoria cache de enlace del nodo móvil y no son creadas nuevas asociaciones mediante esta acción.

El campo de 128 bits llamado dirección local del enlace local (*Home Link Local Address)* contiene el enlace local IPv6 utilizado por el nodo móvil durante su última conexión con su red local. Este campo que es opcional, esta presente únicamente si el campo L tiene un valor de 1.

Como en el caso de otras opciones de IPv6, los tres bits más significativos del campo llamado tipo de opción (*Option Type)* tienen un sentido particular. Debido a que el campo toma un valor de 192 (donde los tres bits más significativos son 110, en su representación binaria), esto significa lo siguiente:

- En el caso de los dos bits más significativos que son (11), con esto si el nodo no reconoce la opción, se descarga el paquete y este hecho debe ser comunicado al nodo fuente a través de un parámetro ICMP donde se informa de el problema, claro esto no puede ser utilizado en la forma multicast.
- En el caso del tercer bit más significativo (0), significa que la opción no puede ser modificada en la ruta.

Los campos opcionales que no están definidos pueden ser adicionados después de la opción de la actualización de los enlaces, la presencia de estos campos puede ser detectada del valor del campo llamado: campo longitud de opción (*Option Length field)* como se muestra en la figura 2.4.

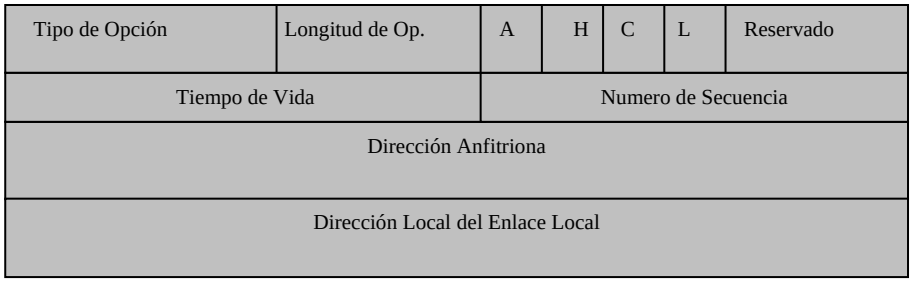


Figura 2.4 Figura representativa de los campos para las diferentes opciones de enlace.

2.4.2 La opción de reconocimiento de los enlaces.

Esta opción se utiliza para confirmar la recepción de la opción de actualización de los enlaces. Es generada únicamente si el nodo móvil explícitamente lo demanda colocando un bit A en la opción actualización de los enlaces. El formato de la opción de reconocimiento de enlaces se muestra en la figura 2.5.

El campo de 8 bits llamado campo tipo de opción (*Option Type* field) toma un valor de 193. El campo de 8 bits llamado longitud de la opción (*Option Length)* contiene la longitud en octetos de determinada opción cuando los dos campos anteriores no se incluyen. Este campo toma un valor de 9. El campo de 8 bits llamado campo estado (*Status* field) puede asumir los valores de la tabla 2.1. Los valores menores de 128

indican que la opción de actualización de enlaces ha sido aceptada, valores mayores o iguales a 128 indican que esta opción ha sido rechazada.

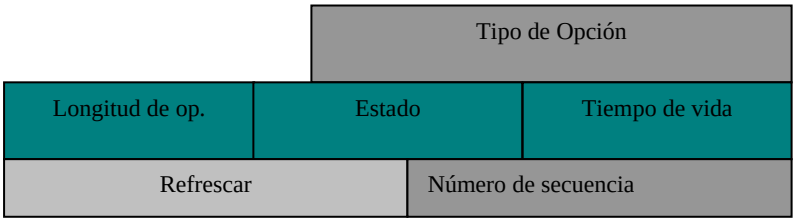


Figura 2.5 Formato de la opción de reconocimiento

Valor	Significado
0	Opción aceptada
128	Opción rechazada: Razón no especificada
129	Opción rechazada: Defectuosa actualización del enlace
130	Opción rechazada: Operación administrativa prohibida
131	Opción rechazada: Recursos insuficientes
132	Opción rechazada: Registro local no soportado
133	Opción rechazada: La red no es la red local
134	Opción rechazada: El valor del campo del número de secuencia es demasiado pequeño
135	Opción rechazada: Hay respuesta de la dirección dinámica del agente local

Tabla 2.1 Posibles valores del campo Estado.

El campo llamado tiempo de vida (*Lifetime)* hace referencia al tiempo en que el nodo mantiene la información de los enlaces. El campo llamado refrescar (*Refresh)* hace referencia al periodo de tiempo después del cual el nodo debe enviar el mensaje de actualización de enlaces para actualizar la información del memoria cache de enlace.

El campo de 16 bits llamado número de secuencia (*Sequence Number)* es usado para establecer una relación entre los mensajes de actualización de enlaces y los mensajes de reconocimiento de enlaces. Los campos opcionales no se encuentran definidos, pueden ser añadidos después de la opción de reconocimiento de enlace, la presencia de estos campos puede ser detectada del valor en la opción longitud (*Length).*

2.4.3 La opción de demanda de enlaces.

Esta opción es utilizada para pedirle al nodo móvil que envíe la actualización de los enlaces. El nodo la activa con una entrada en el memoria cache de enlace, donde la información temporal residente esta a punto de expirar y de ahí que se deba obtener una actualización de la información. Este formato se muestra en la figura 2.6.

El campo de 8 bits llamado tipo de opción (*Option Type)* toma un valor de 194. El campo de 8 bits longitud de la opción (*Option Length)* contiene la longitud de la opción determinada en octetos cuando los campos tipo de opción y longitud de la opción no se incluyen, este campo tiene un valor de cero. Los campos adicionales no se encuentran definidos.

Figura 2.6 Formato de la opción de demanda de enlaces

2.4.4 La opción dirección local.

Esta opción es utilizada en un paquete enviado por el nodo móvil para informar acerca del destino del paquete cuando esta dirigido localmente. Si se incluye este tipo de información en el paquete el nodo que recibe puede sustituir la dirección local del nodo móvil por la dirección de advertencia o de cuidado, así el uso de esta dirección (la de cuidado), es transparente para el nodo que recibe. El formato de la opción, dirección local se muestra en la figura 2.7. El campo de 8 bits llamado tipo de opción tiene un valor de 195. El campo de 8 bits llamado longitud de la opción contiene la longitud de determinada opción en octetos, cuando el campo tipo de opción y longitud de la opción no están incluidos, este campo toma un valor de 8.

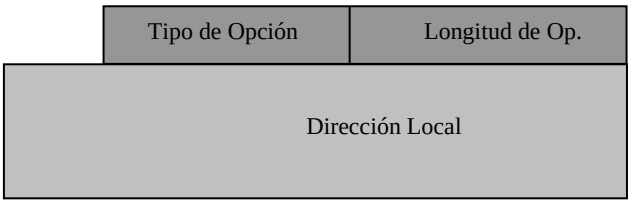


Figura 2.7 Formato de la opción, dirección local

2.5 Características de los nodos móviles.

La movilidad requiere nuevos requerimientos en la arquitectura funcional de los nodos IPv6. En particular, algunos de estos requerimientos deben ser reconocidos por todos los nodos de una red en particular.

2.5.1 Requerimientos generales.

Todos los nodos IPv6 deben de tener en cuenta los siguientes requerimientos:

- Recibir la actualización de enlace y generar el mensaje de reconocimiento de enlace, si este es requerido por otros nodos.
- Administrar la memoria (memoria cache) de información de enlaces, donde los mensajes de enlace son almacenados.

- Administrar la asociación de seguridad para ser usada en conjunto con la cabecera de autenticación de IPv6. De hecho cuando un nodo IPv6 recibe la opción de actualización de enlace debe chequear la identidad del nodo fuente, utilizando la cabecera, si este requerimiento se cumple a cabalidad se almacena la información correspondiente al enlace en el memoria cache.

2.5.2 Requerimientos del enrutador.

Debido a que un enrutador de IPv6 posee información acerca de un equipo móvil en su memoria cache de enlace, todos los enrutadores IPv6 deben poseer las siguientes características:

- Cada enrutador IPv6 tiene que estar en disponibilidad de usar su memoria cache de enlace para enrutamiento de paquetes. Esto significa lo siguiente: si un enrutador tiene en su memoria cache de enlace una entrada relevánte a la dirección destino del paquete que se esta enrutando, debe encapsular ese paquete en un túnel y enviarlo a la llamada dirección anfitriona (*care-of-address).* Es más, para permitir que un nodo móvil deje su red local, al menos un enrutador de esa red local debe poder operar como agente local, para ello debe cumplir con los siguientes requerimientos:

  - Poder administrar un determinado número de nodos para los cuales podrá funcionar como agente local.
  - Poder interceptar paquetes dirigidos a los equipos móviles en su red local, por ejemplo, realizando un procedimiento que permita remplazar a los equipos móviles cercanos. Poder retransmitir paquetes interceptados creando un túnel hacia el móvil utilizando la llamada dirección anfitriona.

2.5.3 Requerimientos del nodo móvil.

Los nodos móviles deben cumplir con las siguientes características:

- Poder recibir paquetes a través del túnel.
- Poder enviar actualizaciones de enlaces y recibir los mensajes de reconocimiento de enlaces.
- Poder administrar una lista de actualizaciones de enlaces para todos los nodos.

2.6 Transmisión de paquetes hacia un nodo móvil.

Se ha visto que el primer paquete que se dirige hacia un equipo móvil que se encuentra en los dominios de una red externa es enrutado hacia la red local, aquí es capturado por el agente local y retransmitido vía "túnel" a la llamada dirección anfitriona. La recepción del paquete por parte del equipo móvil genera la transmisión del mensaje de actualización de enlace hacia el nodo fuente, la información es almacenada por este nodo fuente en la memoria cache de enlace.

En este punto el nodo fuente posee información valida del nodo destino así que puede enviarle la información directamente utilizando la cabecera de enrutamiento.
Por ejemplo, en el caso de que no se necesite utilizar la cabecera de enrutamiento para otros propósitos, el nodo fuente genera un paquete que contiene la dirección anfitriona, que se utiliza como si fuese una dirección de destino IPv6.

En la figura 2.8 se muestra una dirección de destino IPv6 con la cabecera de enrutamiento y esta indica la existencia de un único procesamiento de la información (Segmento Remanente = 1), esta dirección es la dirección local. El paquete IPv6 es enrutado al nodo destino utilizando la información de la dirección destino IPv6 que es llamada dirección anfitriona. Cuando el paquete alcanza el nodo de destino, este procesa la cabecera de enrutamiento y determina que el mismo debe ser enrutado hacia la dirección local, esto es hacia el mismo. Este proceso permite utilizar en los protocolos de la capa superior la dirección local, como si se tratase de la dirección destino por consiguiente es como si no existiese la movilidad.

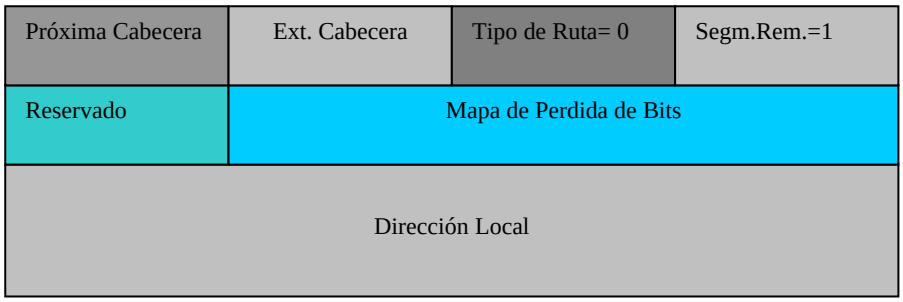


Figura 2.8 Encabezado de enrutamiento.

2.7 Otras funciones de los nodos móviles.

Además de las funciones que se describieron, un equipo móvil tiene que estar listo para detectar su movilidad, para transmitir, para recibir paquetes multicast y volver a su red local.

2.7.1 Detección de la movilidad.

Un equipo móvil puede utilizar todos los mecanismos que tenga a su disposición para detectar su movilidad. El mecanismo maestro para realizar esta labor es el llamado detección de vecinos (*Neighbor Discovery)*. En realidad los equipos móviles deben usar este elemento para localizar la presencia de nuevos enrutadores y nuevos prefijos de red. Es más, el equipo móvil debe usar el procedimiento de detección de proximidad y con ello poder detectar el enrutador que se encuentre en determinado dominio.

2.7.2 Manejando tráfico multicast.

El nodo móvil debe pertenecer a un grupo multicast, para poder recibir el tráfico multicast.

Este tráfico puede ser implementado de las siguientes maneras:

- El equipo móvil puede solicitar al enrutador de determinada red que maneja tráfico que lo adicione al grupo multicast que el maneja.
- El nodo móvil puede solicitarle a su propio enrutador que le asigne al grupo multicast que maneje mediante un túnel bidireccional con su agente local.

Igualmente, un equipo móvil tiene que poder transmitir paquetes multicast de la siguiente manera:

Transmitirla directamente si esta en una red que no es la suya, o transmitirla a su agente local a través de un túnel. Esto debido a que un enrutamiento multicast depende de la fuente de dirección IPv6, en el primer caso, el equipo móvil deberá usar su dirección primaria llamada dirección anfitriona; en el segundo caso, debe utilizar su dirección local. La segunda solución involucra el agente local y el enrutador multicast.

2.7.3 El retorno a la red local.

Un equipo móvil detecta su red local cuando recibe el prefijo de esa red a través de los mensajes que se denominan detección de vecino (*Neighbor Discovery)*. En este punto, el equipo móvil le transmite a su agente local un mensaje de actualización de enlace en el cual la dirección denominada dirección anfitriona es igual a la dirección local, cuando esto sucede el agente local ya no intercepta paquetes direccionados hacia él debido a que el equipo móvil esta nuevamente en la red a la que pertenece. Los mensajes de actualización de enlace deben ser transmitidos con el bit A=1, y repetidos hasta que el agente local envíe un mensaje de reconocimiento de enlace.

El equipo móvil también debe enviar un anuncio de proximidad utilizando la bandera llamada (*override)*. Para solicitarles a todos los equipos en la red local que refresquen la información que tengan en su memoria cache acerca de su vecindad. Esta operación debe ser repetida y limitada en cierto lapso de tiempo tanto para la dirección local como para la dirección de enlace que se utilice en esa localidad.

Finalmente se puede afirmar que las mejoras en el concepto de movilidad en el protocolo IP son notables para su nueva versión IPv6, permitiendo una mejor manejo de la movilidad a través de los procesos de autoconfiguración, con ello se constituye en el protocolo base de las futuras redes móviles habiendo sido este diseñado básicamente para dar soporte a la movilidad.

CAPÍTULO 3

ENRUTAMIENTO EN IPV6

Este capítulo tratará con asuntos concernientes al enrutamiento de paquetes en IPv6. El capítulo analiza la arquitectura de red IPv6, los principales algoritmos utilizados para realizar los cálculos de tablas de enrutamiento, y los protocolos de enrutamiento.

3.1 Términos utilizados en este capítulo.

Con el objeto de hacer uso de ciertas expresiones necesarias para el desarrollo de este capítulo, se incluyen los términos que se van a utilizar y que pueden causar confusión.

- Ruta: Determinación del camino que un paquete IP debe seguir para alcanzar su destino.
- Camino: Un conjunto ordenado de enlaces que conectan una fuente con un destino.
- Subred: Un conjunto de nodos, identificados por direcciones con un prefijo común, los cuales son conectados al mismo enlace físicamente.
- Autónomo: Un conjunto de dominios de rutas gestionados por un único administrador.
- Dominio de ruta: Una partición jerárquica de la red, que contiene un conjunto de hosts y enrutadores, los enrutadores deben compartir la misma ruta. Estos enrutadores son administrados por una autoridad común.
- Enrutador exterior: Un enrutador que maneja conexiones entre diferentes Ass, (los AS´s son los sistemas autónomos).
- Enrutador de frontera: Es un sinónimo de enrutador exterior.
- Enrutador interior: Es un enrutador que maneja conexiones únicamente con un AS.
- Protocolo de compuerta interior (Interior Gateway Protocol IGP): Este es un término genérico aplicado a cada protocolo utilizado para anunciar accesibilidad e información de enrutamiento, de un único AS. El termino gateway, que se esta volviendo obsoleto, es remplazado por enrutador.
- Protocolo de compuerta exterior (Exterior Gateway Protocol EGP): Término genérico aplicado a cada protocolo utilizado para anunciar accesibilidad e información de enrutamiento entre diferentes ASs.
- Camino estático: Técnica en la cual las tablas de enrutamiento son determinadas estadísticamente durante la configuración de la red.
- Camino dinámico: Técnica utilizada para calcular y actualizar las tablas de enrutamiento, en forma dinámica, tomando como referencia la topología y el estado de la red.
- Camino distribuido: La técnica de enrutamiento dinámico en la cual las tablas de enrutamiento son computadas a través de procesos distribuidos en los enrutadores.

- Vector de distancia: Algoritmo de distribución de camino que calcula las tablas de enrutamiento basándose en un intercambio interactivo de dichas tablas con los enrutadores adyacentes.
- Estado de enlace: Algoritmo de distribución de camino para calcular las tablas de enrutamiento, en este caso, un enrutador se comunica a todos los otros enrutadores en la red, el estado del enlace relacionado con él a través de un LSP.
- Paquete de estado de línea (Link State Packet LSP): Paquete generado por un protocolo de estado de enlace para el cálculo de las tablas de enrutamiento. En este caso se tiene una lista de los nodos adyacentes.
- Salto: Se determinará así el cruce de un enlace.
- Costo: Medida asociada con un enlace o un camino.
- Repartición de carga: Pone en equilibrio la carga en caminos paralelos.
- Camino estático: Un acceso en una tabla de enrutamiento, la escribe manualmente el administrador de la red.
- Fin del dominio de ruta (End Routing Domain ERD): Un dominio de ruta en donde las rutas son calculadas ante todo para proveer servicios dentro del dominio.
- Transito de dominio de ruta (Transit Routing Domain TRD): Un dominio de ruta en el cual las rutas son calculadas principalmente para llevar tráfico, esto es tráfico dentro del dominio.
- Dominio de confederación de camino (Routing Domain Confederation): Un conjunto de dominios de enrutamiento que se ven como una única entidad que tiene un único prefijo IPv6.
- Proveedor de servicios de Internet (Internet Service Provider ISP): Una organización pública o privada que suministra servicios, muchas veces se lo denomina proveedor.
- Multicasa (multihome): Una red perteneciente a dos o más dominios de enrutamiento.
- Intranet: Una red privada, basada en el modelo que tiene Internet.

3.2 Modelo de red.

El primer nivel jerárquico en el enrutamiento de paquetes IPV6 es representado por subredes. De hecho los nodos, antes de transmitir paquetes, realizan una prueba, para determinar si el destino esta en modo “on-link” o “off-link”. En el primer caso, los nodos envían un paquete directamente al destino final, en el segundo caso, se utiliza un enrutador que contiene tablas de enrutamiento y con ellas determina cual es el mejor camino hasta el destino. Si se toma en cuenta que las direcciones IP están asociadas con interfaces y no con nodos, el modelo de red resultante es como el que se muestra en la figura 3.1.

Las subredes están agrupadas en sistemas autónomos (Autonomous Systems AS), esto es dentro de grupos de subredes controladas y administradas por una autoridad única.

Los mensajes de enrutamiento de los enrutadores se dirigen dentro del mismo ASs son llamados mensajes de enrutamiento interiores, y los mensajes de enrutamiento entre diferentes ASs son llamados mensajes de enrutamiento exteriores.

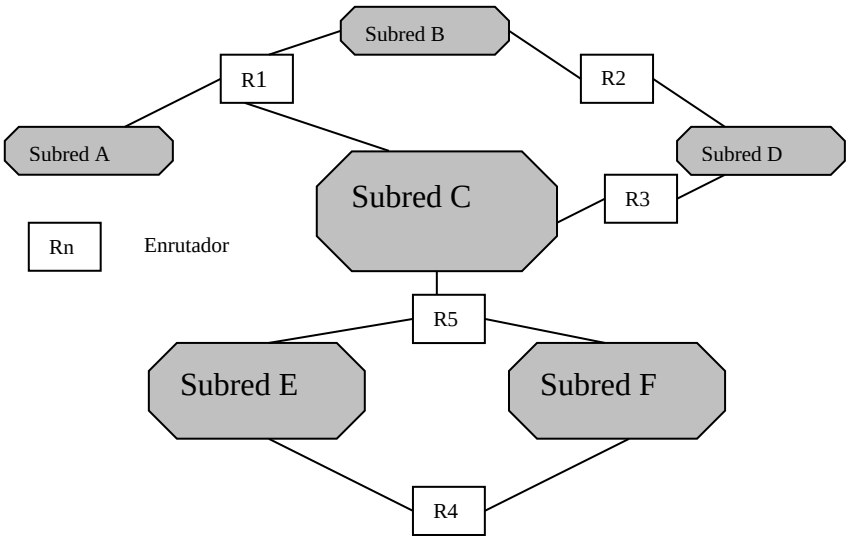
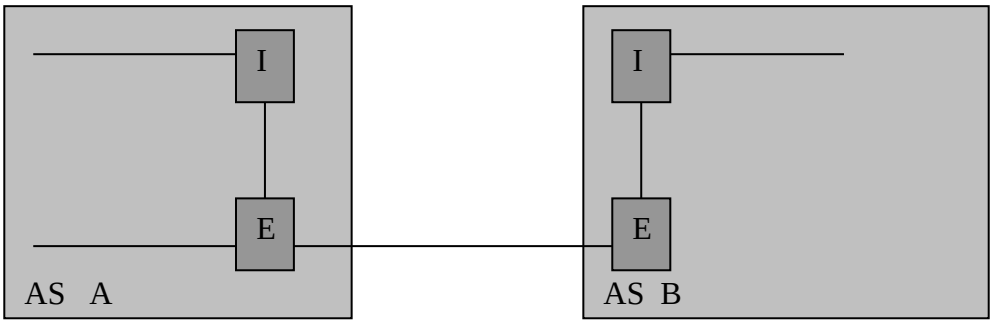


Figura 3.1 Modelo de una red IP

Un ejemplo de interconexión entre dos ASs (indicado por letras A y B) es mostrado en la figura 3.2.

Enrutadores interiores intercambian información de enrutamiento, a través de un protocolo de compuerta interior (Interior Gateway Protocol IGP), mientras que los enrutadores exteriores utilizan un protocolo de compuerta exterior (exterior Gateway Protocol EGP). El mismo IGP es normalmente utilizado en todos los enrutadores en el interior de un AS.



E: Enrutador exterior I: Enrutador interior

Figura 3.2 Ejemplo de interconexión entre dos Ass

3.3 Algoritmos de enrutamiento.

Los enrutadores, no importa si son interiores o exteriores, basan su operación en las tablas de enrutamiento. Las tablas de enrutamiento pueden ser escritas manualmente por el administrador de la red (*Static Routing*) o automáticamente calculadas a través de un

algoritmo dinámico (D*ynamic Routing*), estos algoritmos operan mediante intercambio de información entre enrutadores.

Hoy en día los algoritmos de enrutamiento dinámico (Dynamic Routing Algorithms) son algoritmos de camino distribuido que no poseen un punto central para calcular tablas, debido a esto cada enrutador debe calcular sus propias tablas mediante la interacción con otros enrutadores. En medio de estos tipos de algoritmos las dos familias principales son: algoritmos de vector de distancia y algoritmos de estado de enlace. Los dos enrutamientos, dinámico y estático existen en diferentes regiones de la red por varias razones, como se muestra en la figura 3.3, una porción de la red puede tener enrutamiento dinámico y el resto enrutamiento estático. De hecho, es necesario algoritmos de enrutamiento dinámico para poder tomar ventaja de las redes que utilizan enrutamiento estático, claro esta que el enrutamiento estático es mas sencillo de establecer. El inconveniente del enrutamiento dinámico es en las redes que tienen topología en árbol.

Debido a que las subredes IP están asociadas con redes físicas, cada entrada de las tablas de enrutamiento es independiente del tipo de enrutamiento utilizado.

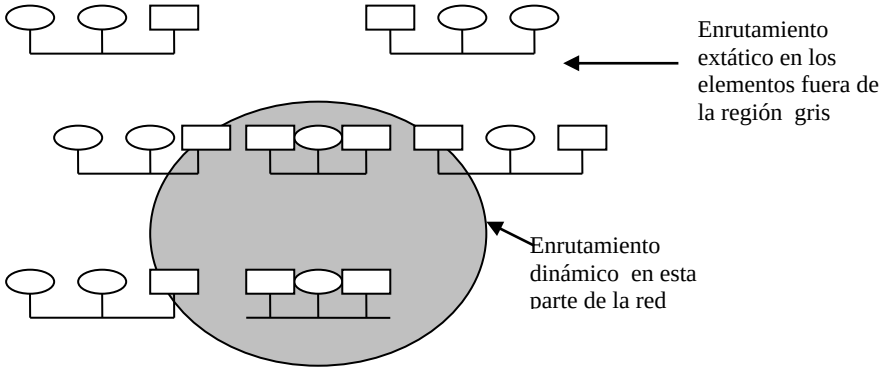


Figura 3.3 Red con enrutamiento estático y dinámico.

En los siguientes numerales se describen aspectos generales de enrutamiento, tenidos en cuenta en todo el nivel IP y no exclusivamente en IPv6.

3.3.1 Enrutamiento estático.

El enrutamiento estático requiere que el administrador de red escriba las tablas de enrutamiento manualmente. El administrador tiene control total del flujo de tráfico en la red, pero la intervención manual es requerida para cambiar la orientación de determinado flujo de datos en caso de un error. Esta aproximación es frecuentemente utilizada en IP en regiones de la red que no están engranadas, en estas regiones no hay rutas alternativas disponibles, y las tablas pueden ser simplificadas utilizando una entrada que indique un camino por defecto para todos los destinos desconocidos. Una entrada estática dentro de una tabla de enrutamiento es llamada camino estático. En redes muy grandes la gestión manual de las tablas puede ser muy complicada. Una entrada en la tabla de

enrutamiento puede ser creada manualmente por medio de un comando como el siguiente: route add 4800:600:0:C00:5/80 4800:600:0:C00:7:800:2B3C:4D5E. Lo anterior especifica que todas las direcciones que comiencen con el prefijo sobre 80 bits 4800:600:0:C00:5 pueden ser alcanzadas por el enrutador conectado al mismo enlace, cuya dirección de interface es 4800:600:0:C00:7:800:2B3C :4D5E.

La entrada por defecto puede ser creada manualmente mediante un comando que especifica el tipo de ruta 4800:600:0:C00:9:800:2B3C:1234. Esto específica que todas las direcciones que no sean concordantes con las existentes en la tabla de enrutamiento pueden ser alcanzadas a través del enrutador cuya dirección de interfaz es 4800:600:0:C00:9:800:2B3C:1234.

Nota: Esas entradas específicas, que se utilizan por defecto en ciertos nodos y enrutadores no son necesario tenerlas. (La introducción manual de parámetros como los anteriores, es de echo necesaria en IPv4), en IPv6, los enrutadores presentan la facultad de aprender automáticamente este tipo de direcciones a través del proceso de descubrimiento de vecindario.

3.3.2 Métrica.

Para implementar los algoritmos de enrutamiento dinámico, la utilización de métricas es esencial. Mediante las métricas se puede medir las características de las rutas a ser utilizadas por los datos. Este proceso es necesario, para clasificar por ejemplo, las rutas y así escoger el mejor camino para el envió de los datos. Las únicas dos metricas aceptadas universalmente son las siguientes:

- El número de saltos: Esto es, el número de enrutadores que existan sobre cierto camino.
- El costo: Esto es la suma de costos de todos los enlaces que componen un camino.

Estos dos parámetros ponen de manifiesto una métrica negativa, debido a que el costo de una línea es asignado de manera inversamente proporcional a la velocidad que la línea maneja, y el conteo del número de saltos indica el conteo de los enrutadores que se cruzan y por lo tanto se puede tener un aumento con este procedimiento del retardo en el recorrido de los datos. Tomando como consideración la carga de la red, es complicado poner las métricas en pleno funcionamiento ya que además de lo anterior, también su uso puede ocasionar inestabilidad en la ruta a seguir. Las técnicas más avanzadas llevan a implementar una carga compartida entre caminos paralelos. Esto también implica la activación de circuitos conmutados, tales como los que se proveen por una RDSI.

3.3.3 Vector de distancia.

El algoritmo llamado vector de distancia es el primer algoritmo de enrutamiento distribuido que a sido implementado. Cada enrutador, además de la tabla de enrutamiento, conserva una estructura de datos, llamada vector de distancia. El vector de distancia contiene una entrada para cada destino, y cada entrada contiene la dirección de destino y las métricas asociadas con determinado camino. El vector de distancia contiene información extraída

de la tabla de enrutamiento del enrutador conectado al otro lado de la línea. Las tablas de enrutamiento son computadas, combinando todos los vectores de distancia asociados con las líneas activas que maneje determinado enrutador. Cada enrutador periódicamente envía su tabla de enrutamiento a otros enrutadores adyacentes, (enrutadores del vecindario), esto lo hace en forma de vectores de distancia. Cuando un enrutador recibe un vector de distancia de otro adyacente, este adiciona las métricas de determinada línea a ese vector recibido, guardando los resultados en su estructura local de datos, además de esto verifica si existe algún cambio comparando el nuevo vector de distancia con el que tenia almacenado anteriormente, si existe un cambio se recomputan las tablas de enrutamiento adjuntando todos los vectores de distancia de las líneas activas que maneje.

La misma operación de recalcular, ocurre cuando una línea va de activada a desactivada o viceversa. Esta asociación de vectores de distancia para calcular tablas de enrutamiento esta basada en un criterio de métricas bajas: Para cada destino, el camino escogido es el que tiene las métricas mas bajas entre todos los demás. Si la tabla de enrutamiento resulta ser otra en comparación con una anterior, el vector de distancia relevante es enviado a los enrutadores adyacentes. El beneficio de esta clase de algoritmos es la facilidad en su implementación. Las desventajas son las siguientes:

- La alta complejidad, exponencial en el peor de los casos y normalmente en el rango comprendido entre n^2 y n^3, donde n es el número de entradas. Esto hace que el uso de este algoritmo no sea adecuado para tablas de enrutamiento con más de 1000 entradas.
- La baja convergencia hacia un enrutamiento estable. El algoritmo converge a una velocidad proporcional a la del enlace más lento y el enrutador más lento de una red.
- La dificultad de entender y anticipar el comportamiento que estos vectores tendrían en redes muy grandes debido a que ningún nodo tiene el mapa de la red.

3.3.4 Vector de camino.

Los algoritmos de vector de camino son similares a los algoritmos de vector de distancia, pero en vez de métricas, ellos anuncian una lista de ASs a ser cruzadas para alcanzar determinado destino. Utilizar una lista de ASs es una manera simple de descubrir lazos en la red e implementar políticas de enrutamiento. Los algoritmos de vector de camino son utilizados en los protocolos EGP.

3.3.5 Estado de enlace.

Los algoritmos de estado de enlace han sido recientemente adoptados. Están basados en la idea de que cada enrutador interactúa con los otros, construyendo así un completo mapa de la red en donde se calculan los caminos óptimos utilizando el algoritmo Dijkstra's o el (Shortest Path First) SPF. Los enrutadores interactúan mediante el intercambio de los LSPs (Link State Packets). A través de los LSPs, cada enrutador comunica a otros enrutadores cuales subredes están directamente conectadas a él. Cada enrutador contiene una base de datos llamada LSP en la cual se almacena las más recientes LSPs generadas por otros enrutadores vecinos. La base de datos LSP es una representación de la red dada como una matriz de redes adyacentes.

Nota: La base de datos LSP es por definición, exactamente idéntica en todos los enrutadores de determinada red. Aun más, una aproximación previa presenta una dualidad: Los enrutadores que utilizan vectores de distancia envían información a las subredes únicamente de los enrutadores vecinos, los enrutadores que utilizan el estado de enlace envían información únicamente a las subredes a las cuales ellos se encuentran conectados directamente, esto suele significar a todos los enrutadores de la red.

La base de datos LSP, representa el mapa de una red con las métricas asociadas, suministra información suficiente para que el enrutador calcule la tabla de enrutamiento.

Una vez más, se nota la diferencia con el vector de distancia: En este caso, los enrutadores cooperan directamente en el cálculo de las tablas de enrutamiento, mientras que estos mantienen la actualización del mapa de la red, con ello cada enrutador coopera con el cálculo automático de sus propias tablas de enrutamiento. El cálculo del algoritmo de estado de línea es igual a (L • log(N)), donde L es el número del enlace y N es el número de nodos. Debido a que las métricas son enteros pequeños, sofisticadas estructuras de datos, que hacen que la complejidad del algoritmo tienda a N, pueden ser implementadas. El algoritmo de estado de enlace puede administrar grandes redes (con 10000 entradas en la tabla de enrutamiento), en este caso rápidamente se converge, y en raros casos se generan lazos en la red, debido a que cada nodo contiene un mapa de la red. Los algoritmos de estado de enlace han sido utilizados en el sistema OSI IS-IS (Intermediate System to Intermediate System).

3.3.6 Redistribución.

Pese a que la definición de AS indica claramente que, dentro de un AS, todos los enrutadores interiores deben usar el mismo IGP, en la práctica esta regla es frecuentemente violada. Muchos ASs usan diferentes IGPs al mismo tiempo, debido a que el software disponible en los enrutadores les permite hacer eso. Por consiguiente existe la necesidad de permitir un IGP #1 que distribuya información de adsequibilidad informándose del IGP #2, y viceversa. Esta operación implica una acertada correspondencia de métricas usadas por los dos IGPs. Esto puede ser fácilmente implementado en partes de la red con una topología de estrella (por ejemplo, redistribución de información de adsequibilidad obtenida de estadísticas), de todas formas se tienen problemas en el enlace de IGP #1 y IGP #2. Esta configuración presenta problemas en la creación de lazos no detectables fácilmente.

3.3.7 Enrutamiento multiprotocolo.

Las redes reales raramente son monoprotocolo, esto es que sólo efectúen sus procesos con un protocolo. Usualmente, las redes LAN transportan simultáneamente varios protocolos, utilizando para ello tramas que pueden acarrear protocolos de diferentes tipos. Los administradores de red algunas veces necesitan transportar varios protocolos al mismo tiempo en cierta parte de la red, para este propósito, son utilizados los enrutadores multiprotocolo. Estos enrutadores calculan tablas de enrutamiento para varios protocolos, este proceso puede ser realizado a través del uso de dos diferentes aproximaciones: Unificada y barcos en la noche. En la aproximación unificada, únicamente un protocolo es utilizado para calcular todas las tablas de enrutamiento. Este resultado es llevado a cabo

habilitando el protocolo para transportar la información de adsequibilidad de varios protocolos al mismo tiempo. En la aproximación: “barcos en la noche”, cada tabla de enrutamiento es calculada para cada protocolo especifico, y los diferentes protocolos viajan de manera paralela, ignorándose el uno del otro como “barcos que pasan en la noche”. La aproximación unificada, es indudablemente muy elegante, pero su implementación es a la vez bastante compleja y menos flexible. Las experiencias de trabajo en red dan como resultado que la aproximación “barcos en la noche”, es la mejor.

3.4 Enrutamiento en IPv6.

Los protocolos principales para el cálculo de las tablas de enrutamiento que son utilizados con IPv6 son RIPv6, OSPFv6, IDRPv2, y probablemente EIGRP y Dual IS-IS. Ninguno de los algoritmos previamente utilizados en IPv4 pueden ser utilizados sin modificaciones en IPv6 debido a que son incapaces de transportar las direcciones del nuevo protocolo con 128 bits.

3.4.1 RIPv6.

El protocolo de información de enrutamiento (The Routing Information Protocol RIP) es originalmente un IGP designado por Xerox para su red XNS, fue introducido en la arquitectura TCP/IP en el año de 1982 en la Universidad de Berkeley en California con el nombre de routed (demonio de encaminamiento), se define en los RFC 1058 en 1988 y se actualizo en el RFC 1388 en 1993. RIP es ampliamente adoptado, principalmente en implementaciones de redes de computadores personales y muchos otros protocolos de enrutamiento son basados en él , como son AppleTalk, Novell, 3Com, Banyan etc.

RIP es un protocolo vector de distancia, en el cual cada enrutador envía su vector de distancia a los enrutadores adyacentes, cada 30 segundos. Las tablas de enrutamiento almacenan únicamente el mejor siguiente salto hacia cada destino. El límite principal de RIP es que permite un máximo de 15 saltos, cada destino que esta mas distante de los 15 saltos es considerado inasequible. En caso de que existan modificaciones de la topología de la red, RIP converge lentamente. Por esta razón, RIP puede ser utilizado únicamente en redes pequeñas.

RIPv6 es la versión de RIP que puede ser utilizada para IPv6. Esta actualización, permite soportar la nueva capacidad de direccionamiento de 128-bits y los prefijos mas relevantes de IPv6. La elección para escoger RIPv6 consiste en mantener la simplicidad y la posibilidad de implementar este proceso en dispositivos muy sencillos en donde la implementación de OSPFv6 podría presentar problemas. RIPv6 tiene únicamente dos tipos de mensajes: Petición y respuesta, estos son transportados en UDP (User Datagram Protocol). En RIPv6 un número limitado de destinos por cada paquete es permitido, el paquete IPv6 no excede el MTU del enlace.

3.4.2 OSPFv6.

El OSPF (The Open Shortest Path First OSPF) es un IGP desarrollado para IP en 1988, en un trabajo de la IETF que tenia el propósito de implementar un protocolo de estado de enlace para IP. OSPF fue definido en el RFC 1247 en 1991 y redefinido en el RFC 1583 en 1994. OSPF esta basado en el concepto de la jerarquía. La raíz de la jerarquía es el

AS el cual puede ser subdividido en áreas, cada una conteniendo un grupo de redes interconectadas. El enrutamiento dentro del área es llamado intra-área, el enrutamiento entre áreas diferentes es llamado inter-área. Cada AS tiene unas áreas de backbone que pueden ser no contiguas, en este caso, la configuración de enlaces virtuales es necesaria para garantizar la cohesión. Todas las otras áreas están conectadas al área del backbone. Los enrutadores OSPF están clasificados en cuatro categorías, que no son exclusivas mutuamente, entre estas tenemos:

- Enrutador interno: Un enrutador conecta subredes, todas pertenecientes a la misma área. Estos enrutadores usan únicamente una instancia del algoritmo. Los enrutadores tienen interfaces únicamente en el backbone que pertenezca a esta categoría.
- Enrutador de borde de área: Un enrutador que conecta al área del backbone a una o más áreas. Estos enrutadores usan varias instancias del algoritmo OSPF: Una instancia para cada área directamente conectada y una instancia para el backbone. Los enrutadores de borde de área acumulan información de acequibilidad de áreas a las cuales ellos están conectados y redistribuye esta información en el backbone para que de esta manera llegue a otras áreas.
- Enrutador del backbone: Es un entutador con una interfaz en el backbone. Esta categoría incluye todos los enrutadores conectados a mas de un área. Todos los enrutadores del backbone con todas las interfaces en el backbone son considerados enrutadores internos.
- Enrutador de frontera AS: Un enrutador que intercambia información con otros enrutadores pertenecientes a otros ASs. Un enrutador de este tipo puede ser un enrutador interno o un enrutador de borde de área.

La figura 3.4 muestra un ejemplo de una AS subdividida en tres áreas OSPF y conectada a otra AS. OSPFv6 es la versión de OSPF utilizada para IPv6; también es un protocolo IGP sugerido para IPv6. Es una implementación estándar para todos los fabricantes de enrutadores, esta hecho para satisfacer grandes redes. OSPFv6, que es una actualización de OSPF, permite transportar direcciones de 128-bits y los prefijos asociados. En OSPFv6, las áreas son identificadas por direcciones de 128-bits, no hay nuevas funciones que hayan sido añadidas debido a que OSPF representa el estado del arte de los protocolos IGP. OSPF para IPv4 y OSPF para IPv6 operan en paralelo, siguiendo el procedimiento de “barcos en la noche”.

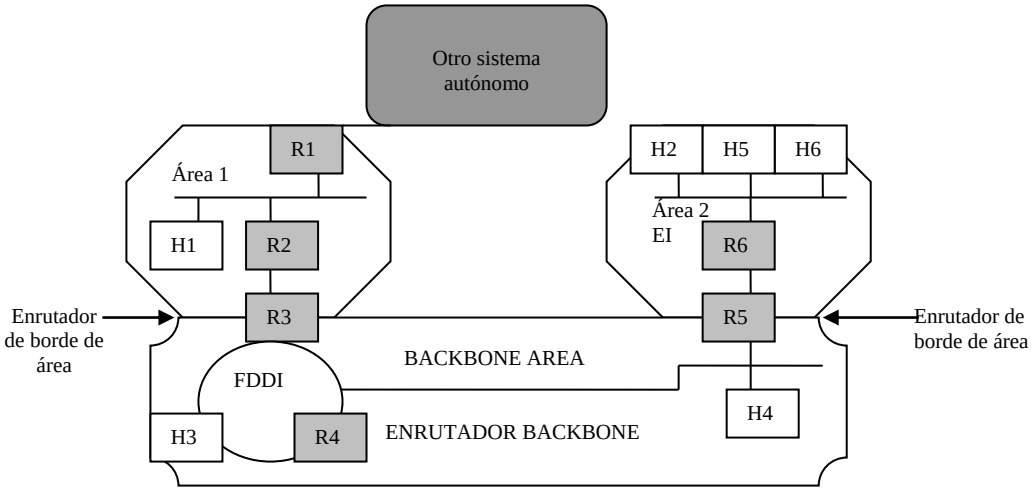
OSPFv6 esta establecido por capas en IPv6, y su cabecera esta identificada por un valor de 89 en decimal, en el campo siguiente cabecera.

3.4.3 IDRPv2.

El protocolo de enrutamiento (IDRP) es un protocolo EGP para ser utilizado con IPv6. El IDRP es un protocolo de vector de camino, diseñado para ser usado en la arquitectura OSI para el protocolo conocido como CLNP ISO 8473 y derivado de el BGP-4 (Border Gateway Protocol versión 4, RFC 1711) que es utilizado como un EGP en la Internet. La versión IDRP que opera para IPv6 es la versión 2 (IDRPv2). IDRPv2 usa el llamado dominio de enrutamiento en lugar de llamar a un sistema autónomo. Un dominio de enrutamiento es identificado por un prefijo IPv6 (direcciones de 128-bits), esta

identificación asigna explícitamente los identificadores para ASs, los cuales en IPv4 son de 16 bits, y que con IPv6 ya no son necesarios. Los dominios de enrutamiento pueden ser agrupados en una confederación de dominios de enrutamiento.

Estas confederaciones son vistas como entidades únicas, y son identificadas también por prefijos IPv6. Las confederaciones de dominios de enrutamiento pueden ser unidas mediante la introducción de un número arbitrario de niveles de jerarquía. IDRP subdivide los dominios de enrutamiento en dos tipos:



Rn: Enrutador
Hn:Host

Figura 3.4 Ejemplo del uso de OSPF.

Dominio de enrutamiento final ERD (end routing domain): Es un dominio de enrutamiento en el cual las rutas son calculadas para proveer servicios de enrutamiento intra dominio.

Dominio de enrutamiento de transito TRD (Transit Routing Domain): Es un dominio de enrutamiento en el cual las rutas son calculadas principalmente para acarrear el transito (esto es, inter-dominio). IDRPv2 ha sido elegido para reemplazar a BGP debido a las siguientes razones:

- Aunque se define en la arquitectura OSI, no presenta ninguna dependencia de dicha arquitectura.
- Ha sido concebido en el principio del enrutamiento multiprotocolo, autorizando varios tipos de direcciones.
- Se incluyen todas las funciones BGP-4, que se basan en la filosofía de utilizar el mismo vector de camino para alcanzar los destinos determinados.
- Cada enrutador calcula el enrutamiento preferido hacia un destino dado y transmite esa información a otros enrutadores IDRP adyacentes. La política para realizar este cálculo es configurable en cada enrutador que utilice IDRP. La cabecera IDRP es identificada con el valor de 45 decimal en el campo siguiente cabecera.

3.5 Relación entre enrutamiento y direccionamiento.

Se hará referencia a la relación existente entre direccionamiento y enrutamiento, este tema se trata con más detalle en el RFC 1887.

3.5.1 Estructura de Internet.

La Internet esta organizada en dominios de enrutamiento para poder intercambiar información entre las redes asequibles que lo conformen. Estos dominios de enrutamiento no tienen igual importancia, como se ha tratado en IDRP, se hace una distinción entre dominio de transito de enrutamiento (Transit Routing Domain, TRD) y dominio final de enrutamiento (End Routing Domain ERD). Un ejemplo de Interconexión entre ERDs y TRDs es ilustrado en la figura 3.5. Los ERDs están asociados con los usuarios finales de la red esto es, para organizaciones conectadas a la Internet, lo hacen usualmente con un TRD. Algunas veces un ERD puede tener conexiones con varios TRDs, en este caso, el ERD es llamado multihome (por ejemplo, en la figura 3.5, el ERD B). Esto, no obstante mantiene su propio ERD lo que significa que no opera como un dominio de transito. Otra posibilidad es que dos ERDs tengan un enlace privado debido a que no tienen que intercambiar largos volúmenes de tráfico, sin que se pase a través de la Internet. Este es el caso de los ERDs F y G en la figura 3.5.

Los TRDs son usualmente asociados con los proveedores de servicio de Internet (Internet Service Providers ISPs), se hará referencia a ellos como proveedores. Estos proveedores pueden ser subdivididos en las siguientes categorías:

Proveedores de servicio directo: Estos proveedores conectan usuarios finales y se conectan a ellos mismos a backbones internacionales. Ejemplos de estos proveedores son America Online y NSFnet.

Proveedores de servicio indirecto: Estos proveedores administran grandes backbones internacionales, conforman el más alto nivel en la jerarquía. Ellos conectan únicamente proveedores de servicio directo y grandes usuarios.

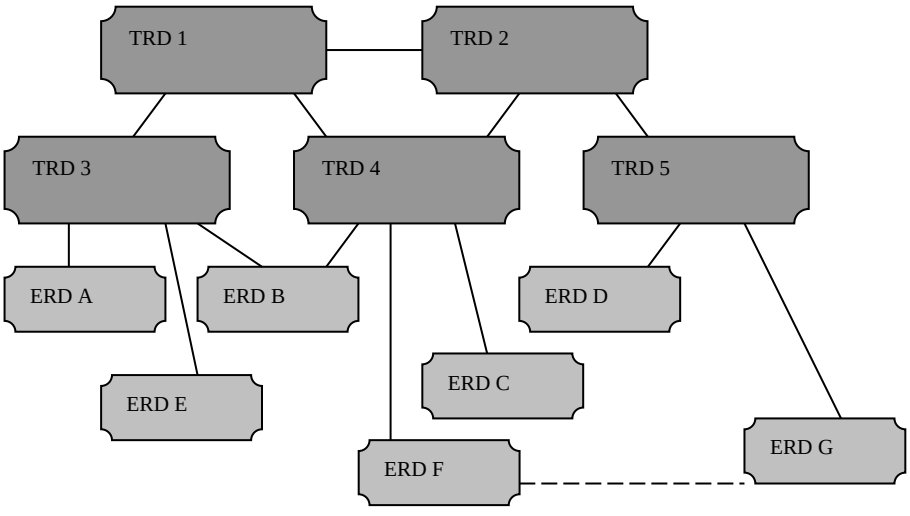


Figura 3.5 Interconexión entre ERDs y TRDs.

3.5.2 Problemas IPv4.

En IPv4, no existe relación entre direcciones y topología. De echo, las direcciones son directamente asignadas a los usuarios finales, incluso si se realiza un esfuerzo para asignar direcciones según las naciones o continentes, este proceso no proporcionara beneficios para el enrutamiento. El Internet, por su misma naturaleza no respeta naciones o fronteras políticas. Por ejemplo, las organizaciones Italianas pueden conectarse a proveedores Italianos y estos a su vez estarán conectados a proveedores Europeos, pero también podrían conectarse a proveedores Americanos. Como resultado las redes Italianas están anunciadas, parte en Europa y parte en Estados Unidos. Esta situación será cada vez más y más complicada con el advenimiento del libre mercado por medio de las telecomunicaciones. Con este hecho, los enrutadores ERD no presentan ningún inconveniente particular, de hecho, es suficiente que mantengan en su tabla de enrutamiento una entrada para cada red dentro del ERD y otra red por defecto para todas las otras redes. Los puntos de entrada por defecto para el TRD del proveedor el cual tiene conexión mediante el ERD.

En el caso de los enrutadores TRD también llamados enrutadores núcleo (core routers) es más complejo. En realidad, estos deben mantener en su tabla de enrutamiento una entrada para cada red conectada a la Internet (esto es sin lugar a duda cierto para los enrutadores de los proveedores de servicio indirecto). Por consiguiente, las tablas de enrutamiento tienden a estallar con el vertiginoso crecimiento de la Internet. Para limitar el crecimiento de las tablas de enrutamiento, el proceso (Classless Inter-Domain Routing CIDR) fue introducido con BGP-4. El CIDR permite el agrupamiento de anuncios de varias redes que tienen direcciones contiguas en una sola entrada. No obstante, el CIDR no puede traer beneficios importantes debido a la filosofía de asignación de las direcciones IPv4. De hecho, no es seguro de que direcciones contiguas sean asignadas a usuarios conectados al mismo TRD y por lo tanto puedan ser agrupados basándose en sus TRDs.

3.5.3 La solución IPv6.

Para resolver los problemas citados en la anterior sección, IPv6 migra de un esquema basado en la asignación de direcciones a los usuarios finales (como se hace en IPv4) a un esquema basado en proveedores. En este nuevo esquema, a cada Proveedor de servicio directo es asignado un grupo de direcciones, el cual, se divide en grupos más pequeños para ser asignados a sus usuarios. Puesto que la dirección IPv6 es más larga que la dirección IPv4, esta puede fácilmente contener este nuevo nivel de jerarquía. Los grupos de direcciones asignados a los usuarios pueden ser agrupados por definición por el proveedor ya que ellos son el resultado de una subdivisión. Para los enrutadores de ERD, la situación permanece inalterable. Ellos continúan teniendo una entrada para cada red dentro del ERD, una entrada predefinida hacia el TRD, y estos anuncian su grupo de direcciones al TRD con sólo una entrada.

Para los enrutadores TRD de Proveedores de Servicio Indirectos, la situación es completamente diferente. De hecho, ahora cada Proveedor de Servicio Directo anuncia todas sus redes con sólo una entrada; por consiguiente, el tamaño de las tablas de asignación de ruta es proporcional al número de proveedores, no al número de redes.

Para los enrutadores TRD del Proveedor de Servicio Directo, la situación puede cambiar significativamente si se hacen muchas conexiones con otros proveedores (Directo o

Indirecto). De hecho, en este caso se anuncian todas las redes asociadas con un proveedor con una sola entrada en las tablas de enrutamiento. Se han propuesto otros posibles esquemas de agregación. Por ejemplo, pueden agregarse proveedores en una base continental, o pueden asignarse grupos de direcciones a proveedores de servicio Indirectos para ser subdivididas asignando las direcciones a proveedores de servicio directo, y los proveedores de servicio directos, en su momento, pueden asignarles las direcciones a los usuarios finales. La utilidad de estos esquemas de enrutamiento es cuestionable. Lo que no es cuestionable, sin embargo, es que la asignación de los proveedores de direcciones a los usuarios finales provoca una contención significante de tablas de enrutamiento (que se pueden estimar en dos órdenes de magnitud). IPv6 seguirán por consiguiente este acercamiento.

3.5.4 Desventajas para usuarios.

La principal desventaja para usuarios sucede cuando estos deciden cambiar de proveedores, esto es, comprar servicios de Internet de otro ISP. De hecho, los usuarios tienen que volver a identificar sus redes. Esta operación es simplificada por los mecanismos de descubrimiento del vecindario que presenta IPv6, de todas formas puede existir cierta ineficiencia. De todas maneras un usuario puede operar con direcciones del proveedor A mientras sigue conectado al proveedor B. En este caso el proveedor B debe conocer las direcciones asignadas al usuario por el proveedor A. Todos los enrutadores de Internet tienen que tener una entrada adicional para indicarle al usuario, que las direcciones del proveedor A pueden ser alcanzadas aun por el usuario a través del proveedor B. Esta situación puede ocurrir por un periodo limitado de tiempo durante una transición que permita al usuario dar otras identificaciones a su red sin la necesidad de quedarse sin servicio, esta deficiencia no puede continuar indefinidamente debido a que rápidamente provocara que las tablas de enrutamiento crezcan.

3.5.5 Dominios de enrutamiento con varias direcciones.

Los conceptos referidos anteriormente se aplican a los ERDs que están conectados a un solo TRD. De todas formas, se puede necesitar un ERD para ser utilizado en el procedimiento llamado multihomed (varias direcciones) esto es, que sea conectado a varios TRDs sin convertirse en un TRD, ejemplos de ERDs en este procedimiento son los dominios de enrutamiento de grandes organizaciones que cubren por ejemplo toda una nación, con ello se debe conectar muchos puntos a la Internet a través de diferentes proveedores, o incluso a una organización internacional que decide conectar su red a la Internet en los lugares donde sus principales subsidiarios se encuentran. Existen muchas razones para tener un ERD multihomed. Las dos principales razones son, la disponibilidad de ancho de banda y la posibilidad de tener caminos alternativos en caso de que se presenten errores y por lo tanto poder tener una red más confiable.

En IPv6, una área entera puede ser multihomed, pero también una sola subred o un solo nodo puede estar dentro del proceso multihomed. Un nodo multihomed puede tener varias direcciones IPv6 asignadas a diferentes interfaces (este caso es común en nodos que deben tener una alta confiabilidad) o también puede ser multihomed por tener varias direcciones asociadas a la misma interfaz (por ejemplo, una LAN con varias interfaces y varios prefijos asociados con diferentes proveedores). Este tópico es el sujeto de debate

en la comunidad de Internet. Se plantean cinco soluciones para conectar un ERD a varios TRDs.

Solución #1: Una organización "multihomed" obtiene un prefijo independientemente de los proveedores con los cuales esta conectada. Esta solución produce una entrada adicional en todos los enrutadores núcleo, y es aceptable sólo para unas pocas organizaciones muy grandes. Esta solución no es apropiada para todas las organizaciones que se conectaran a Internet en un futuro debido a que cientos de miles de organizaciones requerirían tener este proceso y seria muy complejo.

Solución #2: A la organización son asignados varios prefijos tantos como proveedores estén conectados a ella. En cada parte de la red, la organización utilizará un prefijo escogido con base a la distancia de esa parte de la red particular. Por ejemplo, se supone que una organización tiene una red para el cubrimiento de Italia, Francia y España, y se necesita conexión a Internet en estas tres naciones. Para la parte de la red en Italia, se usaran direcciones derivadas del conjunto que se asignó al proveedor Italiano, para la parte Francesa, direcciones del conjunto asignado al proveedor Francés y lo mismo para la parte Española.

Para esta solución, los enrutadores núcleo no necesitan mantener ninguna información adicional para la organización debido a que se trataran estas tres regiones como tres organizaciones separadas que son parte de tres proveedores diferentes. Los enrutadores dentro de la organización pueden ser configurados eficientemente mediante el uso de enlaces privados, sin necesidad de relacionar el ERD a un TRD.

La principal desventaja de esta solución es la carencia de mecanismos de soporte en el caso de que una de las tres conexiones con los proveedores falle. La parte de la red configurada con direcciones de ese proveedor simplemente se convierte en inasequible porque esas direcciones no son públicas para los otros dos proveedores. La promulgación de esas direcciones para que se vuelvan conocidas por los otros proveedores será posible, pero hacerlo será mucho mas costoso en este caso debido a que los enrutadores núcleo deben mantener tres entradas para la organización, una por cada prefijo usado en la red. Por otra parte, si el proveedor es cambiado todas las direcciones asociadas con ese proveedor también deben cambiar. Hay que tener en cuenta, que los paquetes que entren a la organización vía el punto más cercano al nodo fuente (cuya tendencia es a maximizar la carga de la red interna), con la segunda solución, dichos paquetes entran a la organización utilizando el punto que esta mas cercano al nodo destino (cuya tendencia es maximizar la carga en Internet).

Solución #3: Ahora se supone que una segunda organización emplea el prefijo del proveedor A como el prefijo para sus redes debido a que el proveedor A es utilizado como el proveedor por defecto para Internet. Otros TRDs a los cuales la organización esta conectada hace público el prefijo del proveedor A únicamente en áreas controladas. Por ejemplo, suponiendo que esta organización también pertenezca a la red pública Italiana, administrada por el proveedor B. El proveedor hace pública, dentro de la red pública que administra, que esta organización puede ser alcanzada por un conjunto de direcciones provenientes del proveedor A. Esta capacidad demanda que los enrutadores de los TRD

de B tengan una entrada explicita en sus tablas de enrutamiento para la organización, pero no se necesita ninguna entrada adicional en las tablas de los enrutadores núcleo.

Solución #4: La cuarta solución puede ser utilizada cuando dos o más proveedores tienen varios clientes en común. Esta solución es hipotética y se convertirá en un proceso bastante popular cuando la utilización del protocolo IPv6 en redes públicas se vuelva más común. En este caso, los dos proveedores piden un tercer conjunto de direcciones (adicionales a las dos que ya poseen) para ser asignadas a los clientes que tienen en común y están interconectados a sus TRDs. No existe ningún castigo a nivel de los enrutadores núcleo porque todos los usuarios en común entre los dos proveedores están anunciados con una única entrada en las tablas de enrutamiento.

Solución #5: Para la quinta solución, cada estación es asignada a cuanta dirección tengan sus proveedores. Esta situación se ilustra en la figura 3.6, donde la estación X tiene dos direcciones: A::X derivada del proveedor A y B::X derivada del proveedor B. Esta solución no es perfecta. Asumiendo que X establece una sesión Telnet con Y usando sus direcciones A::X, si durante la sesión, el proveedor A se sobrecarga o no puede alcanzar X a través de A, la sesión no puede volver a ser enrutada usando el proveedor B. Esta operación conlleva el uso de direcciones B::X en el paquete IPv6 en lugar de la dirección A::X, pero este uso no es posible. De hecho, la aplicación Telnet coloca en el protocolo de control (TCP), que también utiliza la dirección IPv6 como identificador de conexión, acorde con el RFC 793, esta dirección no puede ser modificada durante el proceso de conexión. Una solución menos pragmática es cerrar la sesión de Telnet y abrir otra, esta vez utilizando la dirección B::X. Una segunda solución, que se encuentra bajo discusión es modificar el protocolo de control TCP permitiendo que las direcciones IPv6 cambien durante la conexión. Una tercera posibilidad es que Y inserte una cabecera de enrutamiento para forzar el paso a través de B::X. de esta forma, la dirección destino en el paquete IPv6 permanece A::X, pero el paquete es entregado a través de B::X, el inconveniente a esta solución esta determinado por la cabecera de enrutamiento (24 octetos en el caso de direcciones intermedias).

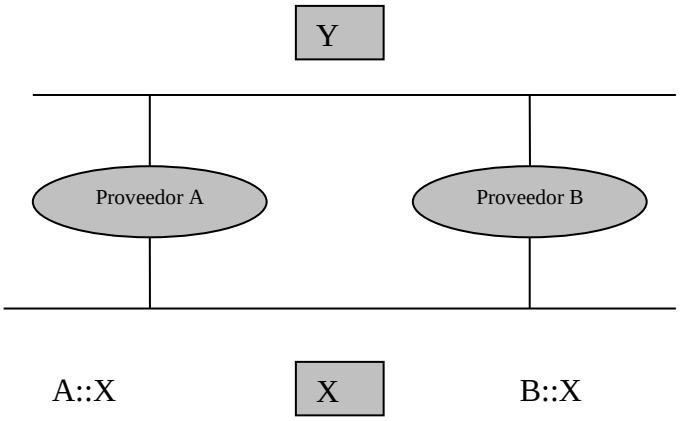


Figura 3.6 Ejemplo de multihomed

3.5.6 Túnel.

En las soluciones descritas en los sub puntos anteriores es frecuentemente referenciada la posibilidad de qué un nodo con múltiples direcciones (multihomed) decida cual dirección va a usar entre muchas direcciones del nodo fuente. Frecuentemente, esto no es posible porque los nodos no tienen suficiente información para decidir correctamente o porque los administradores de la red no quieren que esta situación ocurra.

Los administradores de la red quieren tomar su decisión basados en qué proveedores usar en las fronteras de la red, donde se encuentra, el enrutador de frontera. Una posibilidad esta representada por la creación de túneles, significa transportar paquetes IP dentro de otros paquetes IP.

Lo que corresponde a crear “enlaces virtuales” entre dos nodos IPv6 que ven el túnel como un canal de comunicación en el nivel de enlace de datos, que es un enlace típico. Los dos nodos tienen dos tareas específicas: un nodo encapsula el paquete original y lo transmite en el túnel; y el otro recibe el paquete del túnel, elimina el “encapsulado”, y lo transmite a su destino.

Los túneles son mecanismos unidireccionales; un túnel bidireccional puede ser llevado a cabo usando dos túneles unidireccionales.

Los túneles tienen por lo menos tres aplicaciones importantes:

- Evitar las políticas de enrutamiento de los Proveedores.
- Interconectar Intranets a través de Internet.
- La implementación del 6Bone que es, el primer centro de Internet IPv6.

Los túneles pueden ser simples o enrutados (ver Figura 3.7). En el caso de túneles simples, un paquete IP se transporta dentro de un paquete IP con una cabecera (overhead) de tamaño igual a la cabecera IP (en el caso de IPv6, 40 octetos). En el ejemplo mostrado en Figura 3.7, el túnel simple, permite que el paquete original en la ruta del dominio B localice Y cruzando la ruta del dominio C.

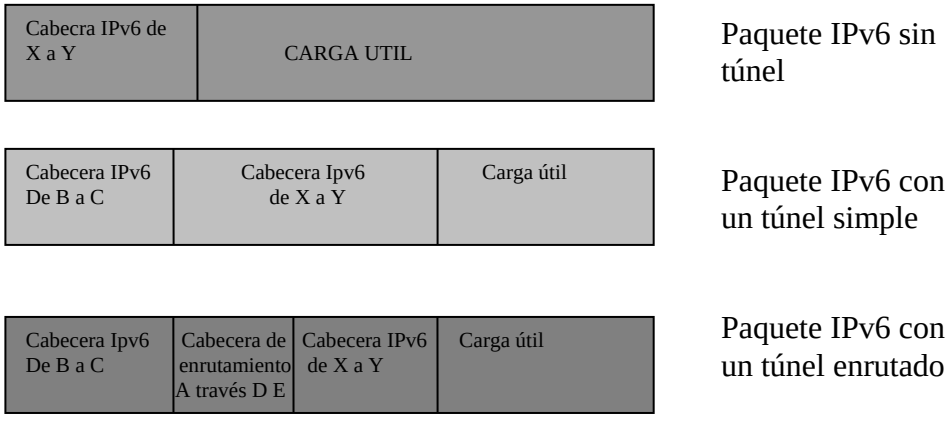


Figura 3.7 Ejemplos de Túneles

En el caso de túneles enrutados, una cabecera de enrutamiento es insertada para especificar otras rutas de dominios que deben cruzarse en el camino hacia el destino. En el ejemplo mostrado en Figura 3.7, el túnel enrutado permite que el paquete original en la ruta de B localice Y cruzando las rutas de los dominios D, E, y C.

3.5.7 Enlaces privados.

Si dos organizaciones X y Y tienen dos ERDs y deciden mejorar el desempeño de su interconexión adquiriendo un enlace punto-a-punto entre los dos ERDs. Este acercamiento no origina ningún problema de enrutamiento en particular en Internet; es un asunto local que es ignorado por el centro de enrutadores. Crear este enlace, agregando una entrada correspondiente a Y en la tabla de enrutamiento del ERD de X es suficiente, y viceversa. Si se conectan otros ERDs de otras organizaciones con las que tiene un intensivo intercambio de información a su ERD, acceder estas organizaciones desde X a través de un enlace privado también es posible, agregando las entradas necesarias en las tablas de enrutamiento.

3.6 Enrutamiento multicast.

El término enrutamiento multicast se refiere a el enrutamiento de paquetes cuya dirección de destino es una dirección multicast, que es, la dirección de un grupo de estaciones. Algunas de estas direcciones multicast son asociadas con grupos predefinidos y tienen sólo significando con respecto al nodo o al enlace; considerando que otros grupos multicast pueden tener miembros en varias partes de Internet, y por consiguiente los paquetes que se dirigen a estos grupos multicast deben ser enrutados por medio de enrutadores.

El problema de enrutamiento multicast en IPv6 es similar al de IPv4, con las siguientes diferencias principales:

- En IPv4, se administran miembros de grupos con un protocolo específico llamado Protocolo de asociación de grupos de Internet (IGMP), qué en IPv6 se integro como parte de ICMPv6 mientras mantiene las mismas funciones.
- En IPv4, los paquetes multicast son enrutados a través de dos protocolos alternativos: el protocolo de enrutamiento multicast de Vector de Distancia (DVMRP) estandarizado en el RFC 1075, o el Multicast OSPF (MOSPF) que consiste de extensiones al protocolo OSPF estandarizado en el RFC 1584 para tratar con paquetes multicast. En IPv6, las extensiones de MOSPF se integran como parte de OSPFv6.

En síntesis, Para enrutar paquetes multicast, se debe crear un árbol de distribución (árbol multicast) para localizar a todos los miembros del grupo. El árbol es claramente dinámico porque nuevos miembros pueden adicionarse en el grupo, y los miembros existentes pueden salirse en cualquier momento. La adición de miembros típicamente induce el crecimiento del árbol. Por consiguiente, los problemas de enrutamiento multicast resultan ser una parte integrada en IPv6 y, en particular, en los protocolos ICMPv6 y OSPFv6.

3.7 Intranets.

Muchas organizaciones, mientras se deciden a implementar redes basadas en el Protocolo IP, no quieren estar interconectadas a Internet o desean tener acceso extremadamente controlado a Internet. Estas organizaciones implementan Intranets que son redes privadas basadas en el modelo de Internet (RFC 1918, lo referente IPv4). La configuración de Intranets esta inmensamente simplificada en IPv6, desde el punto de vista de direccionamiento, porque es suficiente con asignar al sitio direcciones locales en la parte privada de la red. La parte pública tiene, otro tratamiento, las direcciones globales son basadas en proveedores.

La Figura 3.8 muestra un ejemplo de configuración de Internet/Intranet. Para comunicarse entre la parte pública y la parte privada, se usa una solución técnica consolidada; esta proporciona la instalación de gateways de aplicación (por ejemplo, para el correo electrónico) y servidores proxy (por ejemplo, para www, Ftp, y Telnet) en nodos públicos.

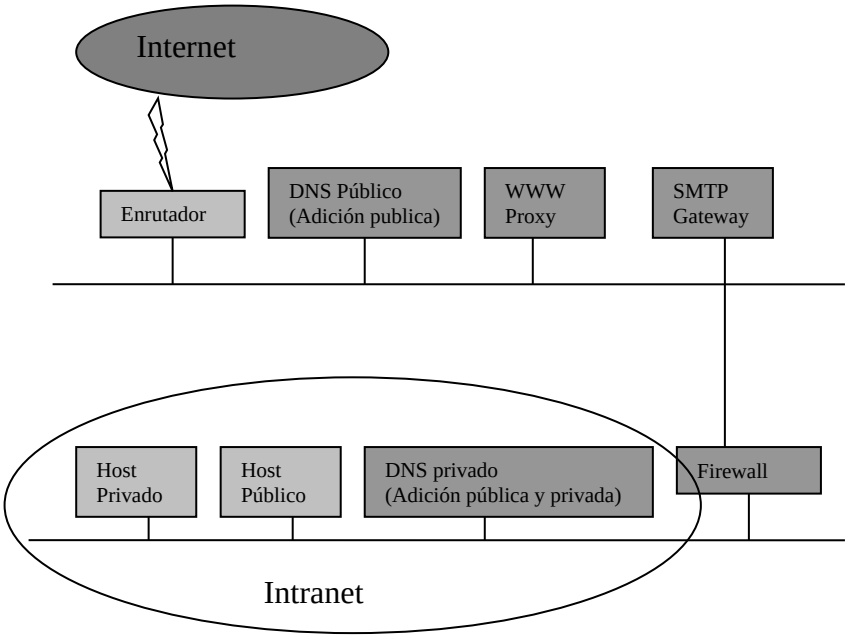


Figura 3.8 Esquema de conexión entre una Intranet e Internet.

Entre la red pública y las redes privadas, ya sea un enrutador, con apropiados filtros de acceso, o un firewall real es insertado para evitar propagar información acerca de la red privada en Internet. Es más, si una compañía implementa muchas intranets, por ejemplo, una para cada sucursal, esta compañía puede interconectar estas Intranets llevando a cabo “túneles” en Internet entre los firewalls de las diferentes sucursales. El paquete IP de la Intranet se encapsula en un paquete IP de Internet.

Un servidor DNS público, conectado a los sistemas de DNS mundiales, debe estar disponible; se usa para definir las direcciones de nodos públicos. Un segundo servidor DNS privado contiene ambas direcciones, la de los nodos públicos y la de los nodos

privados, y usa el DNS público como el remitente hacia el Internet. Todos los nodos (sea público o privado) usan el DNS privado.

Otro método práctico para aumentar la seguridad es adoptar un cableado separado para la parte pública (Internet) y la parte privada (Intranet) de la red. El término cableado separado aquí significa una organización física del cableado en el que, aun si un hacker tiene éxito cargando un programa para la captura de los paquetes de la red en un nodo que puede localizarse en Internet, este programa no puede ver los paquetes de Intranet porque ellos viajan en otros cables.

Como conclusión se tiene que la implementación de nuevos algoritmos de enrutamiento para IPv6, permiten la utilización más efectiva de los diferentes recursos de la red, pero sin olvidar la importancia de la simplicidad de la puesta en marcha de los mismos, esta simplicidad debe al menos no ser menor que la existente en los algoritmos de enrutamiento utilizados para IPv4.

La actualización de los algoritmos de enrutamiento que se utilizan en IPv4, es necesaria para su implementación en IPv6, no sólo para permitir sacar el máximo provecho de las nuevas capacidades de IPv6, sino también por la mayor capacidad de direccionamiento del nuevo protocolo.

CAPÍTULO 4

SEGURIDAD EN EL PROTOCOLO IP

Las redes TCP/IP basadas en el protocolo IPv4 tienen muchos problemas de seguridad, debido a que las mismas han sido diseñadas para trabajar en ambientes amigables respaldadas por conexiones seguras. Cuando este "ambiente amigable" se pierde, como sucede hoy en día, las debilidades en cuanto a seguridad del protocolo IPv4 se vuelven manifiestas y se explotan fácilmente. En general las comunicaciones sobre IP están expuestas a severos tipos de ataque. Entre estos se tiene:

Olfateo de paquetes: Gracias a la topología de red, los paquetes IP enviados por una fuente a un destino específico, pueden ser leídos también por otros nodos que pueden tener acceso a la carga útil del paquete (por ejemplo passwords u otra información).

Engaño IP: Las direcciones IP pueden ser fácilmente engañadas tanto para atacar servicios, los cuales tienen una autenticación basada en la dirección del que envía (como por ejemplo el servicio **rlogin,** o muchos servidores WWW), como para abastecer de información errónea la organización lógica de la red, (por ejemplo, mediante falsificación de mensajes ICMP dando un tipo "dirección inaccesible ").

Conexión pirateada: Todo el conjunto de paquetes IP puede ser falsificado para parecer paquetes legales provenientes de una o dos comunicaciones asociadas e insertar datos erróneos en determinado canal.

Las soluciones para estos y otros ataques no están siempre disponibles. Cuando las contramedidas existen, generalmente están colocadas en el nivel de aplicación. Como consecuencia las soluciones no son ínteroperables, usualmente para proveer una seguridad óptima a nivel de protocolo.

El desarrollo de una nueva versión del protocolo IP ha ofrecido la posibilidad de introducir mecanismos de seguridad a nivel de red. Así que este tipo de seguridad puede estar disponible para todas las aplicaciones. Las técnicas de seguridad adoptadas en el protocolo IPV6 han sido diseñadas para ser insertadas fácilmente en el protocolo IPv4. Se introduce IPSEC, la nueva arquitectura de seguridad genérica a nivel de IP. No obstante debido a que el protocolo IPv4 también padece de otros problemas, es improbable que las redes actuales y sus aplicaciones sean modificadas sólo para implementar IPSEC. De otro lado es muy probable que IPSEC sea implementado en IPV6. Se puede cuestionar si la seguridad a nivel de IP es apropiada, obviamente no existen respuestas definitivas porque generalmente la seguridad de un sistema no esta basada en un solo elemento, más bien es el resultado de una combinación de muchos elementos. El nivel de IP es seguramente una barricada para muchos ataques, como los mencionados al principio de este capítulo, que son los responsables de un gran porcentaje de todos los ataques a la red. De otro lado, IPSEC no es una solución completa cuando las aplicaciones a ser protegidas están orientadas a usuario (como es el caso del correo electrónico) más bien

deben estar orientadas a red. De último pero no menos importante, la seguridad IPv6 esta implementada por cabeceras de extensión.

4.1 Características de seguridad.

Las características de seguridad en IPv6 han sido introducidas por medio, de las cabeceras de extensión: la cabecera de autenticación (AH) y la ESP *Encrypted* Security Payload, con capacidades complementarias.

La cabecera AH fue designada para asegurar la autenticidad e integridad de los paquetes IP. Su presencia es un vigilante contra dos amenazas: Modificación ilegal de los campos invariables y engaño de paquetes. De otro lado, la cabecera ESP provee encapsulamiento de datos con encriptación, para asegurar que únicamente el nodo destino pueda leer la carga útil del paquete IP. Las dos cabeceras pueden ser usadas juntas para cubrir todos los aspectos de seguridad simultáneamente. Ambas AH y ESP sacan provecho del concepto de asociacion de seguridad (AS). En general, cada nodo IPv6 maneja un conjunto de ASs. The Security Parameters Index (SPI) es un parámetro contenido en ambas cabeceras AH y ESP para especificar si SA es utilizada en desepcriptaciòn o autenticación de paquetes.

En las transmisiones unicast, el parámetro SPI es normalmente seleccionado por el nodo destino y vuelto a enviar al transmisor, cuando la comunicación es instalada. En transmisiones multicast, el parámetro SPI debe ser común a todos los miembros del grupo multicast. Cada nodo debe ser capaz de identificar el parámetro AS correctamente mediante la combinación del parámetro SPI con la dirección multicast. La negociación del parámetro AS (y el determinado SPI) es una parte integral del protocolo para el intercambio de las llamadas llaves de seguridad.

4.1.1 Cabecera de autenticación (AH).

La cabecera de autenticación es una de las cabeceras de extensión generales definidas para IPv6, es definida por el valor 51 en el campo próxima cabecera (Next Header). Normalmente es insertada entre la cabecera IPv6 y el nivel superior de la carga útil, el formato de la cabecera AH es simple, esta compuesta por 64 bits fijos seguidos por un grupo variable de 32 bits. La parte fija contiene lo siguiente:

- El valor del próximo tipo de carga útil (8 bits).
- La longitud de la carga útil, esto es la longitud total de los datos de autenticación expresado esto, como un múltiplo de palabras de 32 bits.
- Un campo reservado (16 bits).
- El SPI usado por esta cabecera (32 bits).

La parte variable de la cabecera AH esta compuesta de un grupo variable de 32 bits, el cual contiene los datos de autenticación actual. Se debe a que la longitud de la carga útil esta expresada como un número de 8 bits, un máximo de 1020 bytes pueden ser utilizados en este proceso. Como consecuencia, la longitud exacta de esta cabecera depende del algoritmo de autenticación.

Cuando el nodo de destino recibe un paquete con la cabecera AH, la legitimidad de los paquetes y su integridad pueden ser chequeadas usando este procedimiento. Como paso preliminar, se debe tener cuidado en la normalización del paquete recibido, para eliminar toda la parte variable y calcular correctamente el valor de la autenticación, únicamente se hace utilizando la parte fija. En la figura 4.1 se ilustra un ejemplo del uso de las cabeceras AH, la estructura de la cabecera AH se muestra en la figura 4.2.

4.1.2 Técnicas de autenticación.

La integridad de los datos en un sistema de telecomunicaciones es verificada normalmente por el cálculo y el chequeo de un valor adecuado de los datos, a menudo este proceso es llamado Message Digest (MD). Entre los algoritmos más comunes están: CRC-16 y CRC-32.

Estas funciones realizan efectivamente sus tareas cuando las modificaciones de los datos son causadas por errores aleatorios, pero son completamente inadecuadas para proteger a los paquetes contra modificaciones deliberadas. En este caso una protección razonable puede ser asegurarse utilizando algoritmos específicamente realizados para tal objeto, como lo son: MD54 o SHA5. Se debe tener en cuenta que la integridad de los datos sin autenticación de origen es completamente inservible. Por consiguiente, determinados algoritmos son normalmente aplicados de tal forma que incluyan ciertos parámetros que pueden ser utilizados para proveer comprobación de identidad de los nodos que envían la información en forma simultanea. A menudo este resultado se logra usando una llave pública de encriptación, desafortunadamente este proceso necesita una actividad computacional más pesada que los algoritmos que no cumplen con esta función. Debió a que la velocidad es un factor prepondérate en una red de computadores, la autenticación por defecto hecha para IPSEC es muy simple, y es llamada keyed MD56.

En breve la técnica llamada para el cálculo del algoritmo MD5 en los datos para que estos sean protegidos se precede y se termina por una llave (una cadena secreta de bits). De todas formas el algoritmo MD5 puede ser atacado así que es muy recomendable que en un futuro cercano otras técnicas de autenticación sean estandarizadas para usarlas en IPv6. Por ejemplo la llamada técnica keyed-SHA que *esta* propuesta *en el* RFC 1852, esta basada en el algoritmo SHA5, el cual exhibe mejor seguridad que el MD5 ya que el SHA5 trabaja con una taza de 160 bits.

4.1.3 Encrypted Security Payload (ESP).

El proceso denominado Encrypted Security Payload, que es una de las cabeceras de extensión general definidas en IPv6, esta identificado por el valor de 52 en el campo llamado próxima cabecera del datagrama AH.

Este bloque siempre estará posicionado de último en la cadena de la cabecera, debido a que siempre esta oculto tanto del nivel superior de la carga útil y todas las cabeceras próximas. La forma exacta de la porción encriptada depende del algoritmo de encriptación utilizado. La técnica de encriptación que se utiliza por defecto en IPv6 es la llamada DES-CBC9, la cual aplica el algoritmo DES en el proceso de cifrado de determinado bloque, ha este modo de cifrado del bloque se le denomina *Cipher Block Chaining* (CBC). DES es

una llave de encriptación privada que es normalmente aplicada en bloques de datos de 64 bits. Varias técnicas han sido propuestas para aplicar el algoritmo DES a bloques de datos mayores a 64 bits. El modo CBC divide el flujo de datos en una secuencia de bloques de 64 bits, así que este modo puede ser útil al pensar en el algoritmo DES.

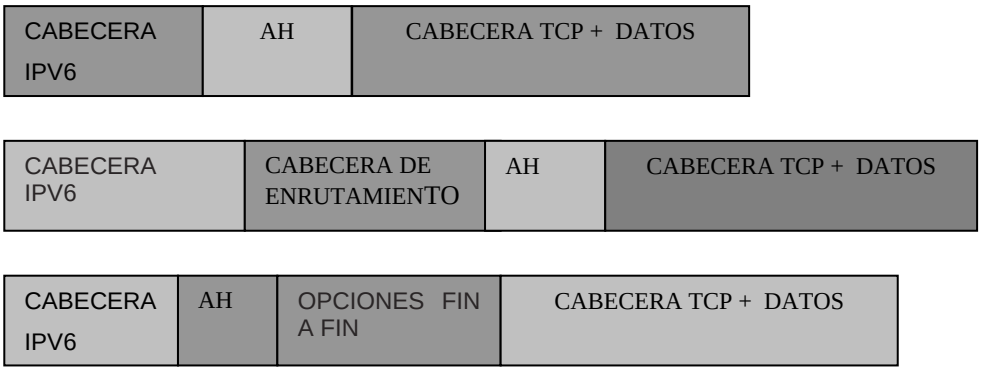


Figura 4.1 Ejemplo del uso de las cabeceras AH.

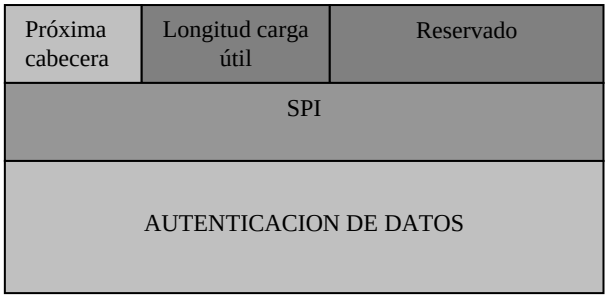


Figura 4.2 Estructura de la cabecera AH.

A cada bloque se le aplica un proceso EX OR, con el resultado de la encriptación previa, antes del mismo proceso que encrípta de una manera más robusta dicho bloque. Con E(d,k) siendo la operación de encriptación aplicada al bloque de datos utilizando la llave k, el modo CBC puede describirse mediante la siguiente transformación.

$$ci = E(di \text{ Å } ci\text{-}1, k)$$

La encriptación del primer bloque de datos d1 requiere un valor inicial c0, comúnmente denominado vector de inicialización (IV). Este vector no debe ser nulo, y debe ser escogido cuidadosamente en el proceso de encriptación para insertar un factor aleatorio. Esto se necesita para eludir ataques “criptográficos”, basados en un conocimiento parcial de los datos que han sido encriptados, tal es el caso de los ataques conocidos como knownplaintext que pueden perjudicar la parte fija de la cabecera de ciertos archivos comunes (por ejemplo: los archivos de datos provenientes de herramientas automáticas de *office*). Normalmente el vector de inicialización tiene valores de 64 bits elegidos en

forma aleatoria. La porción encriptada de la cabecera ESP comienza con el vector de inicialización compuesto por un número entero de 32 bits. En general, la longitud exacta del vector IV depende del nivel de seguridad a ser utilizado, de todas formas el RFC 1829 provee especificaciones únicamente para vectores de 32 a 64 bits.

El vector IV es seguido por la carga útil encriptada, se utilizan bloques de relleno para asegurarse que la dimensión total de la cabecera ESP sea un múltiplo de 64 bits. El último byte contiene el tipo de carga útil transportado. El tamaño de los rellenos suele variar entre 0 y 7 bytes, pero usar tamaños mayores (mayores a 255 bytes) para esconder la longitud real de los datos encripados es legal.

EL algoritmo DES-CBC debe estar disponible en todas las implementaciones estándar IPv6. Debido a que ese algoritmo DES es considerado de mediana dificultad como para ser alterado, es muy probable que en un futuro cercano otros algoritmos sean estandarizados para el uso en IPv6. Por ejemplo, el algoritmo 3DES-CBC propuesto en el RFC 1851. Esta técnica esta basada en una aplicación repetitiva de transformaciones a los bloques de datos pero con la utilización de tres diferentes llaves, trayendo como resultado una protección criptográfica más fuerte. En la figura 4.3 se ilustra la estructura de la cabecera DSP con la técnica DES-CBC.

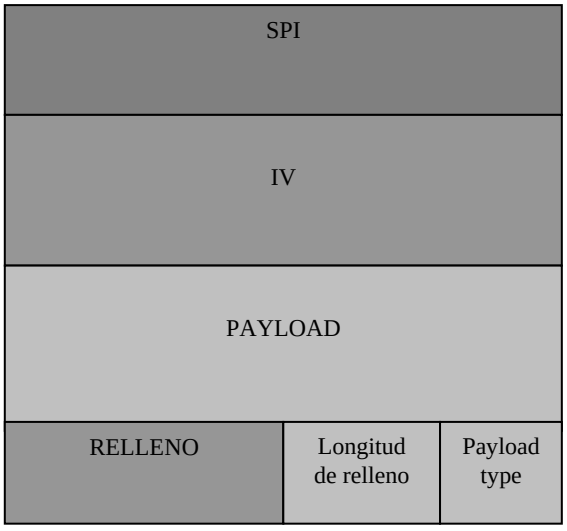


Figura 4.3 Estructura de la cabecera ESP, en el caso de utilizar la técnica DES-CBC.

4.2 Gestión de llaves.

La correcta aplicación de las cabeceras AH y ESP requiere que todas las partes que se comunican estén de acuerdo en una llave común para ser usada en el moldeado y la comprobación de las cabeceras de seguridad. IPv6 autoriza que el uso de la llave de gestión ocurra o no, con protocolos específicos, en un proceso llamado out-of-band. No obstante, el acuerdo entre las partes es difícil de lograr a nivel de una red mundial, no así

en determinados grupos, claro esta, que esos grupos suelen tener necesidades diferentes: rápido intercambio de llaves, fuertes procesos de autenticación, protocolos de fácil procesamiento, y otras. La gestión de llaves es el área más controversial dentro de la arquitectura mundial de IPv6.

4.2.1 Gestión de llaves manual.

IPv6 requiere que cada implementación de llaves de seguridad sea realizada en forma manual. Obviamente, la configuración manual de las llaves es posible únicamente si los operadores de seguridad se han puesto de acuerdo en el proceso de elección de llaves por ejemplo: en una reunión confidencial. Esta solución exhibe costos personales muy altos y no tiene mucha acogida, porque requiere trabajo personal de un operador en cada dispositivo de red que tome parte de un canal seguro. Adicionalmente, esto puede generar un falso sentido de seguridad. Ese nivel de intervención humana no asegura un alto nivel de seguridad, además hay que tener en cuenta los posibles problemas que le sucedan a la integridad del HW y el SW de los dispositivos donde esta la llave.

De todas maneras a pesar de ciertas desventajas la administración manual puede manejar perfectamente aplicaciones en ambientes restringidos, con un número limitado de equipos asegurados, de esa manera este tipo de procedimiento es útil.

4.2.2 Gestión de llaves automática.

Dentro de IPSEC, la gestión de llaves es seguramente el área que esta menos establecida y el área en la que hay mucho trabajo por hacer, ya que el conjunto de protocolos que aseguran por completo a nivel de IP no es consistente. La única decisión que se ha tomado al respecto es la concerniente a, IKMP (key management protocol), que será insertado en el nivel de aplicación, y es independiente de los protocolos de las capas o niveles inferiores. La primera propuesta funcional es la de permitir que IKMP se basa en un conjunto de protocolos como son: El ISAKMP11 y Oakley12. Internet Security Association and Key Management Protocol (ISAKMP) define una arquitectura genérica para autenticación e intercambio de llaves, sin especificar el tipo de algoritmos que serán usados. De esta manera, el ISAKMP puede ser usado con diferentes tipos de llaves. Oakley es un protocolo de intercambio de llaves, basado en una versión modificada de un algoritmo llamado Diffie-Hellman. Actualmente la competencia de la técnica realizada por la simbiosis de ISAKMP Y OAKLEY, es la llamada SKIP (Simple Key-managemen for Internet Protocols), la cual también basa sus procedimientos en el algoritmo Diffie-Hellman. SKIP es un procedimiento simple en comparación con la anterior técnica pero tiene problemas con la gestión de llaves en redes que trabajan a una alta velocidad.

4.3 Aplicación de las características de seguridad en IPv6.

Las cabeceras AH y ESP pueden ser utilizadas de formas diferentes para proteger las comunicaciones IP. Se tratará entonces de repasar algunas de las aplicaciones más interesantes con referencia a las debilidades que se presentan en el protocolo IPv4.

4.3.1 Redes privadas virtuales.

Actualmente, razones técnicas y económicas están impulsando la migración de los enlaces dedicados y redes propietarias a soluciones basadas en enlaces públicos y arquitecturas de red abiertas. Esta migración crea varias ventajas pero actualmente exhibe un serio inconveniente: existe una drástica reducción en el sistema intrínseco de seguridad, debido al uso de canales y dispositivos compartidos. Para mantener el mismo nivel de seguridad en la red con ciertas ventajas económicas ofrecidas por las redes públicas, una organización tiene que tener éxito en separar y proteger sus propios paquetes de datos dentro del conglomerado de paquetes que viajan a través de las redes públicas.

Usualmente este resultado es logrado mediante el establecimiento de una red privada virtual (VPN). En el protocolo IPv4, esto se hace mediente el tunelado sobre IP: los paquetes IP para ser protegidos son envueltos en una cubierta de seguridad y luego se encapsulan sobre paquetes IP normales, este método es utilizado para transportar los paquetes originales a través de las redes públicas hasta su destino final. A menudo, los puntos finales de un túnel IP no son los hosts esperando por el intercambio de datos, más bien se presenta la posibilidad de utilizar dos “firewalls” para proteger determinada LANs de ataques externos. En IPv6, es fácil crear una VPN, incluso mas fácil que en IPv4, gracias a las cabeceras AH y ESP. Como un ejemplo se tiene un canal TCP entre el host H1 en la red N1 y el host H2 en la red N2 deben ser protegidos únicamente contra la manipulación de datos y la falsificación de origen, mientras la privacidad de datos no es requerida. En este caso, la cabecera AH puede ser explotada de la siguiente manera: el “firewall” FW1 obtiene los paquetes y los modifica añadiendo la cabecera AH antes de enviarlas al otro “firewall”, el “firewall” FW2. Cuando este paquete es recibido, chequea la integridad del paquete y la autenticación de origen mediante la utilización de los datos de la cabecera AH. Si el chequeo es exitoso la cabecera IP y la cabecera AH son removidas, y los datos restantes (esto es el paquete original) son enviados al destino final. Si la VPN es implementada usando únicamente la cabecera AH, los atacantes no pueden alterar los paquetes transmitidos ni tampoco insertar paquetes “olvidados” en el canal. De todas formas, los atacantes todavía pueden leer el contenido de los paquetes. Para impedir el descubrimiento de la carga útil la cabecera ESP también debe ser utilizada.

Incluso el uso en conjunción de las dos cabeceras tanto AH como ESP no dan una protección completa al tráfico, los paquetes pueden ser borrados mediante la intermediación de nodos. Estos ataques no pueden ser fácilmente contrarrestados en el nivel de red, defensas apropiadas (como las que utilizan identificadores de paquetes individuales), están por lo general localizadas en un nivel superior en el sistema de red. Una solución parcial en el nivel IP es probablemente ofrecida por el nuevo formato y por los nuevos algoritmos que van a remplazar a los actuales. Comparando este método de la creación de VPN con uno usualmente utilizado en IPv4 que utiliza “firewalls” y tunelado, se puede decir que la arquitectura básica necesaria es la misma que la usada en IPv6, pero debido a que IPv4 no permite la utilización de múltiples cabeceras, el túnel tiene que ser implementado utilizando el encapsulamiento. Obviamente esta solución tiene problemas de compatibilidad entre los “firewalls” de diferentes proveedores así como también acarrea problemas de fragmentación. Si el paquete a ser transmitido tiene la máxima dimensión que soporta un paquete IP, la encapsulaciòn dentro de otro paquete IP no es posible, fragmentación y reensamblaje deben tomar lugar en los dos puntos

extremos del túnel. Como consecuencia el funcionamiento de un canal virtual puede ser degradado por debajo del 50 por ciento del rendimiento normal. El peor caso toma lugar en los paquetes más grandes, los cuales son típicamente utilizados en transferir grandes cantidades de datos, como contraste, no necesitan fragmentación para lograr máxima velocidad. El mejor de los casos ocurre con los paquetes pequeños, como los utilizados en las aplicaciones interactivas. En IPv6, la situación es completamente diferente, debido a la utilización de un tamaño fijo (la dimensión de AH, o inclusive de AH más ESP) es independiente de la dimensión del paquete original, las aplicaciones que sufren la mayor sobrecarga son las interactivas, que son las que manejan las aplicaciones que tienen mejores propiedades de resistencia a ataques.

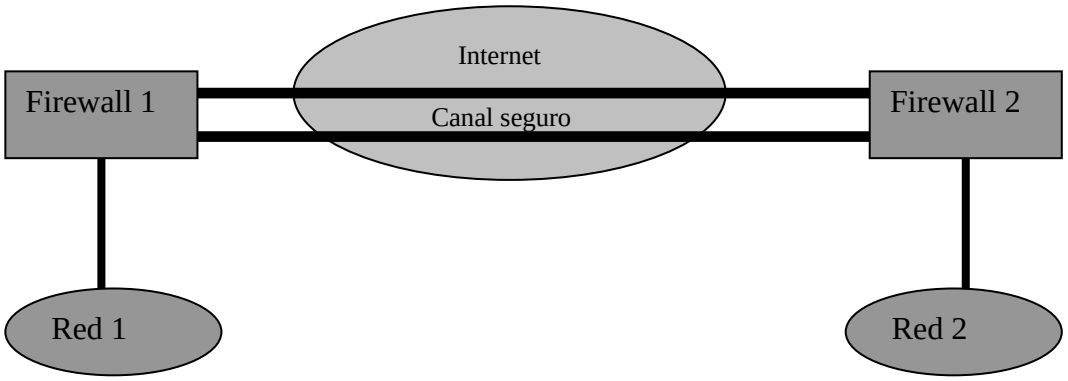


Figura 4.4 Ejemplo de un túnel entre dos firewalls.

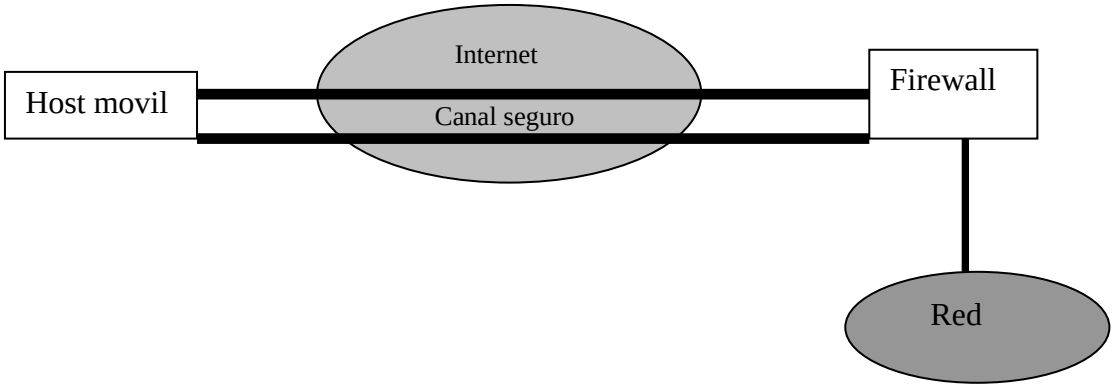


Figura 4.5 Ejemplo de un túnel entre un firewall y un único host

De todas maneras, en los dos casos, el rendimiento es más bajo en la VPN implementada en IPv6 comparada con la que se construye en IPv4. Por último pero no menos importante, es interesante saber que esta técnica de VPN puede ser adoptada incluso entre un "firewall" y un solo host externo. Obviamente, este caso es de una relevancia particular para garantizar seguridad cuando un host móvil es utilizado fuera del parámetro de la red protegida, en este caso el "firewall" actuara como uno de los llamados "home agent". Al "home agent" se le asignaran dos direcciones IP diferentes: una de ellas cuando es conectado dentro del perímetro seguro y la otra cuando esta fuera de ese perímetro. En este último caso, el "firewall" también actuará como un repetidor,

redirigiendo los paquetes provenientes de la red a la que pertenece y que están dirigidos a una dirección externa, todo esto después de haber añadido las cabeceras (AH, o AH + ESP). En la figura 4.4 se ilustra un ejemplo de un túnel entre dos “firewalls” y en la figura 4.5 se muestra un ejemplo de un túnel entre un “firewall” y un host.

4.3.2 Seguridad en el nivel de aplicación.

Las aplicaciones para ser utilizadas en red con IPv6, requieren de un canal de comunicación con características específicas. Para evitar la duplicación de funcionalidad (y consecuentemente la degradación de la funcionalidad), siendo capaz de especificar a la capa de transporte, los atributos de seguridad de determinado canal. En las primeras implementaciones de IPv6 con el sistema operativo UNIX, este efecto podía ser obtenido con el uso apropiado de una opción llamada “**socketoption()”**. De todas maneras, esta solución, no es completa para asegurar el nivel de aplicación debido a que se obtiene únicamente una protección parcial. La cabecera AH provee una autenticación basada únicamente en el host, mientras que las aplicaciones requieren autenticación basada en usuario. Más aún, AH y ESP protegen los datos únicamente durante su transmisión a lo largo del canal. Después de que los datos han sido recibidos no están protegidos de ninguna manera. Este hecho no debería ser relevante si el host que recibe los datos es seguro, pero ahí existe una implicación adicional: que las propiedades de autenticación del origen y la integridad de los datos ya se han perdido. Por consiguiente se debe dar una conclusión de que las características de seguridad en IPv6 no eliminan la necesidad de otros mecanismos de seguridad, que serán mejor recibidos en el nivel de aplicación.

4.3.3 Seguridad de enrutamiento.

Debido a que las direcciones IP en IPv6 son obtenidas en gran parte por asignación dinámica, es de suprema importancia que este proceso sea hecho de una forma segura.

Más aún, con una combinación apropiada de las cabeceras AH y ESP, es recomendable que estas combinaciones sean aplicadas a los mensajes intercambiados por los enrutadores para prevenir ataques que alteren la arquitectura lógica de la red. Los siguientes tipos de comunicaciones deben ser protegidos:

- Los mensajes de aviso de enrutamiento (The routing advertisement messages), para asegurarse que estos son originados por un enrutador autorizado.
- Los mensajes de anuncio de vecindario (The neighbor advertisement messages), para asegurarse de que estos provienen de hosts autorizados y para evitar el riesgo de que alguien añada un nuevo host a la red sin la debida autorización.
- Los mensajes ICMP, compatibles con un host no rastreable o una red no identificada, o cuando se ha escogido una mejor ruta (redireccionamiento), para asegurarse de que esos mensajes provienen del los hosts o los enrutadores autorizados. Asegurar este tipo de mensajes no es algo trivial. Por ejemplo: los mensajes de enrutamiento son enviados a un grupo “multicast”, por consiguiente, todos los enrutadores en determinado grupo deben conocer la llave secreta (común), para ser usada en la verificación y poder desencriptar los mensajes. Lo anterior implica que se podrían falsificar los mensajes y asumir el papel de cualquier enrutador en el grupo.

La protección de los mensajes del vecindario presenta un serio problema, estos mensajes pueden ser protegidos únicamente después de que la asociación de seguridad SA ha sido establecida entre el host y el centro de distribución de direcciones. De otro lado, esta SA puede ser creada únicamente después de que una dirección ha sido asignada al host, así que se puede concluir que este es un problema típico como de quien fue primero el huevo o la gallina, que no tiene solución corriente. Para romper ese circulo vicioso, soluciones parciales son posibles. Por ejemplo: se puede asignar determinada prioridad a la asignación de direcciones, y el estableciemieto del SA se puede permitir únicamente luego de este proceso.

Cada host tiene asignadas un par de llaves (privada y pública) y tiene que preconfigurarse con una llave pública por el encargado de certificar los enrutadores y autorizar los centros de distribución de direcciones. La última alternativa es configurar los enrutadores para que ellos no hagan públicos los prefijos locales, de esta manera cada host es forzado a establecer el contacto con el enrutador.

La protección contra falsos mensajes ICMP requiere la utilización de las cabeceras AH, pero esta aproximación tiene el inconveniente de requerir el establecimiento del SA con cada enrutador y host en el camino entre la fuente y el destino de los paquetes.

Con respecto a la seguridad de los mensajes utilizados por varios protocolos de enrutamiento, ellos deben siempre ser intercambiados únicamente dentro del marco de SA y ser protegidos por la cabecera AH. Esta solución, es altamente preferible en comparación con utilizar mecanismos de autenticación específicos para cada protocolo de enrutamiento. Basándose en el análisis anterior, se puede concluir que la seguridad de enrutamiento es aparentemente un problema en IPv6, pero las oportunidades de resolver este problema son mayores que las oportunidades que se tienen en IPv4.

4.4 Orientación futura.

Actualmente, la utilización de las cabeceras AH y ESP esta siendo modificada teniendo en cuenta los siguientes preceptos:

- La estructura de AH es muy cambiante para permitir la existencia de algoritmos de autenticación nuevos y más fuertes.
- La especificación ESP ha tenido pocos cambios para permitir una mejor ortogonalidad con los algoritmos, esto para simplificar los mecanismos de encriptación. Los beneficios de estos cambios se verán representados en una mayor seguridad a nivel de red, por lo tanto niveles como el de aplicación podrán concentrarse en otros aspectos de seguridad, como la autorización a nivel de usuario.

Por último se puede concluir que: la seguridad es una de las áreas con mayor movimiento en las redes de computadores debido a que la protección de datos y recursos computacionales es vital, más aún con la explotación que esta teniendo el comercio electrónico. La seguridad en IPv6 no es una excepción a la regla, a pesar de que esta área es nueva, se ha investigado lo suficiente como para permitir el logro de ciertos objetivos.

Aunque la implementación de nuevas estructuras para asegurar los datos a nivel de IP como son las cabeceras AH y ESP, se constituyen en un avance importante, no son la panacea de la protección de datos. Se necesita complementar este avance con políticas más seguras a nivel de aplicación, esa es la única forma de brindarles a los usuarios la posibilidad de utilizar los recursos de la red de una manera más confiable.

CAPÍTULO 5

IMPLEMENTACIÓN DE LA ISLA IPV6

El siguiente capítulo se divide en tres partes, en la primera parte se define el concepto de "Isla IPv6", se analizan de forma general dos soluciones posibles para conectarse al 6Bone usando la topología de red IPv4 existente y se establecen unos objetivos económicos. En la segunda parte se describe el mecanismo de túneles 6to4 propuesto para la creación de la Isla IPv6 y la conexión de esta al 6Bone, también se establecen a manera de propuesta unas estrategias a seguir para la implementación de la Isla y se describe paso a paso el ambiente IPv6 utilizando túneles 6to4 más adecuado para conectar la Intranet de la Universidad del Cauca al 6Bone sin tener en cuenta ningún tipo de restricciones. En la parte final se describe de manera precisa la implementación llevada a cabo utilizando túneles 6to4 teniendo en cuenta las restricciones logísticas debidas a los recursos asignados y a restricciones de tipo económico las cuales no permitieron implementar el ambiente ideal para la Intranet de la Universidad.

El desarrollo de esta y otras prácticas se describe de manera detallada en el Anexo D, más las bases conceptuales expuestas a lo largo del trabajo final acerca del protocolo permiten una mejor comprensión de las características que harán de IPv6 un pilar fundamental para el desarrollo de las redes de próxima generación.

5.1 Definición de "Isla IPv6".

Una isla es un conjunto de equipos y computadores que utilizan el protocolo IPv6 para comunicarse entre ellos en lo que se podría definir como un "mar IPv4". Una isla está unida a otras islas usando enlaces punto a punto llamados "túneles IPv6 sobre IPv4". Existen básicamente dos tipos de túneles, los manuales y los automáticos, de los que se hablara más adelante.

La forma más fácil de realizar una isla y conectarla a otras, es participando en el 6bone. El 6bone es una red mundial que utiliza protocolos IPv6. Para realizar la conexión se utilizan túneles, como ya se menciono. El único requisito que debe cumplirse para poder conectarse es disponer de un equipo con capacidad de ruteo IPv6 y que tenga asignada una dirección IPv4 global. A medida que más redes funcionen con IPv6 los túneles dejarán paso a conexiones físicas y el 6bone dejará de llamarse así, y se le dirá sencillamente Internet.

Conectar la red de datos de la Universidad del Cauca a través de una isla IPv6 al 6bone usando túneles, le permitirá a esta comenzar a migrar a una red multiservicio toda IPv6 sin ningún tipo de traumatismos para las aplicaciones y datos que maneja la institución. Brindándole además, beneficios a largo plazo en: costos operativos, mínima gestión de los sistemas servidores y lo más importante, beneficios económicos y académicos ya que le permitirá a la universidad conectarse con instituciones educativas y comerciales con

redes multiservicio que ya operen con IPv6, con las que se podrá intercambiar información en tiempo real (voz sobre IP, video conferencias) tecnología de punta y además realizar negocios que promuevan el desarrollo económico conjunto. Para este propósito a continuación se verán dos soluciones posibles que podrían permitir la conexión de la red de datos de la Universidad del Cauca al 6Bone.

5.2 Soluciones para la conexión al 6Bone utilizando la topología IPv4 existente.

Existen dos posibles maneras de conectar la red de la Universidad del Cauca al 6bone usando la topología IPv4 existente, estas son: túneles configurados manualmente y túneles 6to4 (automaticos). Ambas soluciones requieren que el host o el enrutador en cada extremo del túnel este corriendo la pila dual, esto quiere decir que soporte los dos protocolos IPv4 e IPv6.

5.2.1 Solución No. 1: Túneles Configurados manualmente.

La configuración de túneles manuales, es una técnica en donde una dirección IPv6 se configura manualmente sobre una interfaz del túnel y además las direcciones IPv4 son configuradas manualmente en el origen y en el destino del túnel. Pueden configurarse túneles manualmente entre los enrutadores fronterizos o entre un enrutador fronterizo y un host. Ya que los “túneles manuales” requieren configuración en ambos extremos del túnel, estos precisan de una mayor gestión en las operaciones que llevan a cabo los múltiples túneles, comparado con el uso de túneles 6to4. Debido a que estos se configuran uno a uno entre puntos terminales bien definidos, los túneles configurados manualmente hacen que haya tráfico de información disponible para cada terminal, y proporcionan una mayor seguridad contra el tráfico circundante.

5.2.2 Solución No. 2: Túneles 6to4.

Los túneles 6to4 son una técnica en donde el punto final del túnel es determinado por una dirección IPv4 única global, embebida en una dirección 6to4. Una dirección IPv6 6to4 es una combinación de un único prefijo de ruta 2002::/16 y una única dirección global IPv4 de 32-bits (las direcciones IPv6 compatibles con IPv4 son un formato diferente a las direcciones 6to4. Las direcciones IPv6 compatibles con IPv4 no son usadas en túneles 6to4). Los túneles 6to4 se configuran entre los enrutadores fronterizos, o entre un enrutador fronterizo y un host. Los túneles 6to4 requieren que un sitio de retransmisión 6to4 conectado al 6bone sea identificado para proporcionar el servicio 6to4. El sitio de retransmisión 6to4 configura un enrutador fronterizo con pila dual que se volverá el punto final para el túnel 6to4. Después de esto los sitios de retransmisión 6to4 se preparan para realizar túneles 6to4, su carga de gestión es mínima. En el extremo de origen, una simple configuración del enrutador habilita el acceso al 6bone a través del túnel 6to4.

Además es posible usar túneles 6to4 para interconectar sitios IPv6 dentro de una Intranet lo que permite realizar Islas en entornos corporativos y educativos como en el caso de la Universidad del Cauca, logrando que varios equipos (hosts, servidores, enrutadores) se conecten al 6bone.

5.3 Objetivos de la transición.

Con el propósito de disminuir el impacto en la conectividad, que origina la integración al 6bone, la Facultad de Ingeniería Electrónica y Telecomunicaciones decide extender su conocimiento de IPv6 realizando una Isla IPv6. Teniendo en cuenta el anterior planteamiento se establecen los siguientes objetivos para dar el primer paso en la transición.

- Una inversión mínima, ya que se obtiene experiencia en IPv6 sobre una infraestructura de red IPv6 real (6Bone) ya establecida, usando la topología de la red IPv4 extendida en la Universidad del Cauca.
- Probar los procedimientos de transición y operación en un ambiente IPv6 real antes de implementar IPv6 dentro de la Universidad.
  Los procedimientos de transición son los procedimientos que son necesarios para migrar de IPv4 a IPv6 ya analizados en el capítulo 1. Estos procedimientos incluyen establecer la pila dual en los sistemas finales y enrutadores, mecanismos de túneles, servidores DNS, y, en el futuro, la comprobación del protocolo de traslación de direcciones de red NAT-PT (Network Address Translation-Protocol Translation).
- Probar aplicaciones IPv6 e implementaciones en estaciones de trabajo local.
- Minimizar la gestión en cuanto a costos operativos se refiere, asociados con la conexión al 6Bone.

5.4 Solución propuesta para la red de datos de la Universidad del Cauca.

El mecanismo de túneles 6to4 es la mejor solución con la que se puede implementar la Isla IPv6 utilizando los recursos asignados para el desarrollo de este trabajo de grado y que además permite cumplir con el objetivo de iniciar la transición de la red de datos de la Universidad del Cauca. Aunque el tráfico IPv6 se transporta como la carga de un paquete IPv4, sigue siendo tráfico IPv6 (la infraestructura IPv4 se considera como un nivel de vínculo IPv6). Las aplicaciones que utilizan las direcciones asociadas con este método utilizan las mismas funciones de Windows Sockets que si se utilizaran direcciones IPv6 globales y una infraestructura IPv6. Estos métodos se pueden utilizar para comprobar la funcionalidad IPv6 en las aplicaciones sin tener que implementar enrutadores IPv6 en la Universidad, además sin el requisito de obtener un prefijo de dirección global IPv6 de un proveedor de servicios de Internet (ISP).

5.4.1 Conexión al 6Bone utilizando túneles 6to4.

La figura 5.1 a) muestra la topología actual de la red IPv4 de la Universidad del Cauca, y la figura 5.1 b) muestra esta misma topología de una manera simplificada, para propósitos ilustrativos, en las figuras 5.1 a y 5.1 b se puede observar la red con una conexión IPv4 permanente a Internet en donde un proveedor de servicio (ISP), en este caso Orbitel, proporciona conectividad externa.

Partiendo de la topología actual de la Universidad del Cauca, se describe en esta sección de manera general el mecanismo de túneles 6to4 seleccionado para la implementación de la Isla IPv6 como un ambiente de prueba, se establece una estrategia a seguir y se

definen tres ambientes IPv6 de prueba, de los cuales se describe de forma detallada y a manera de propuesta el ambiente más conveniente para la Intranet de la Universidad.

Se seleccionó este ambiente para describirlo ya que brinda una solución más completa, ideal para el correcto funcionamiento de la red en el proceso de transición de IPv4 a IPv6 de la Intranet de la Universidad del Cauca. Al ser este el ambiente más completo, los otros dos ambientes se encuentran de manera implícita en la implementación del mismo.

Nota: El ambiente implementado, no es el mismo que se describe en esta sección, la diferencia entre uno y otro es mínima y radica en la separación de la red de prueba IPv6 y de la Intranet a través de un "firewall" implementado para impedir que el tráfico IPv6 fluya libremente por la red IPv4 de la Universidad.

Descripción general del mecanismo 6to4.
6to4 es una técnica de túnel que se describe en el documento RFC 3056 de la IETF. Cuando se utiliza 6to4, el tráfico IPv6 se encapsula con un encabezado IPv4 antes de enviarse a través de un conjunto de redes IPv4, como Internet.

6to4 utiliza el prefijo de dirección global de 2002:*WWXX*:*YYZZ*::/48, en donde *WWXX*:*YYZZ* es a la vez la parte Agregador de siguiente nivel (NLA, Next Level Aggregator) de una dirección global y la representación hexadecimal con dos puntos de una dirección IPv4 pública (w.x.y.z) que está asignada al sitio o host. La dirección 6to4 completa de un host 6to4 es 2002:*WWXX*:*YYZZ*:[Id. de SLA]:[Id. de interfaz].

En el documento RFC 3056 se definen los términos siguientes:

- Host 6to4.
  Host IPv6 que está configurado con al menos una dirección 6to4.
- Enrutador 6to4.
  Enrutador IPv4 o IPv6 que reenvía el tráfico con direcciones 6to4 entre los hosts 6to4 de un sitio y otros enrutadores 6to4 o enrutadores de retransmisión 6to4 en un conjunto de redes IPv4, como Internet.
- Enrutador de retransmisión 6to4.
  Enrutador IPv4 o IPv6 que reenvía tráfico con direcciones 6to4 entre enrutadores 6to4 en Internet y hosts en el 6bone.

Cuando se utilizan hosts 6to4, una infraestructura de enrutamiento IPv6 en sitios 6to4, un enrutador 6to4 en los límites del sitio y un enrutador de retransmisión 6to4, son posibles los tipos de comunicación siguientes:

- Un host 6to4 se puede comunicar con otro host 6to4 en el mismo sitio. Este tipo de comunicación está disponible mediante la infraestructura de enrutamiento IPv6, que proporciona accesibilidad a todos los hosts del sitio.

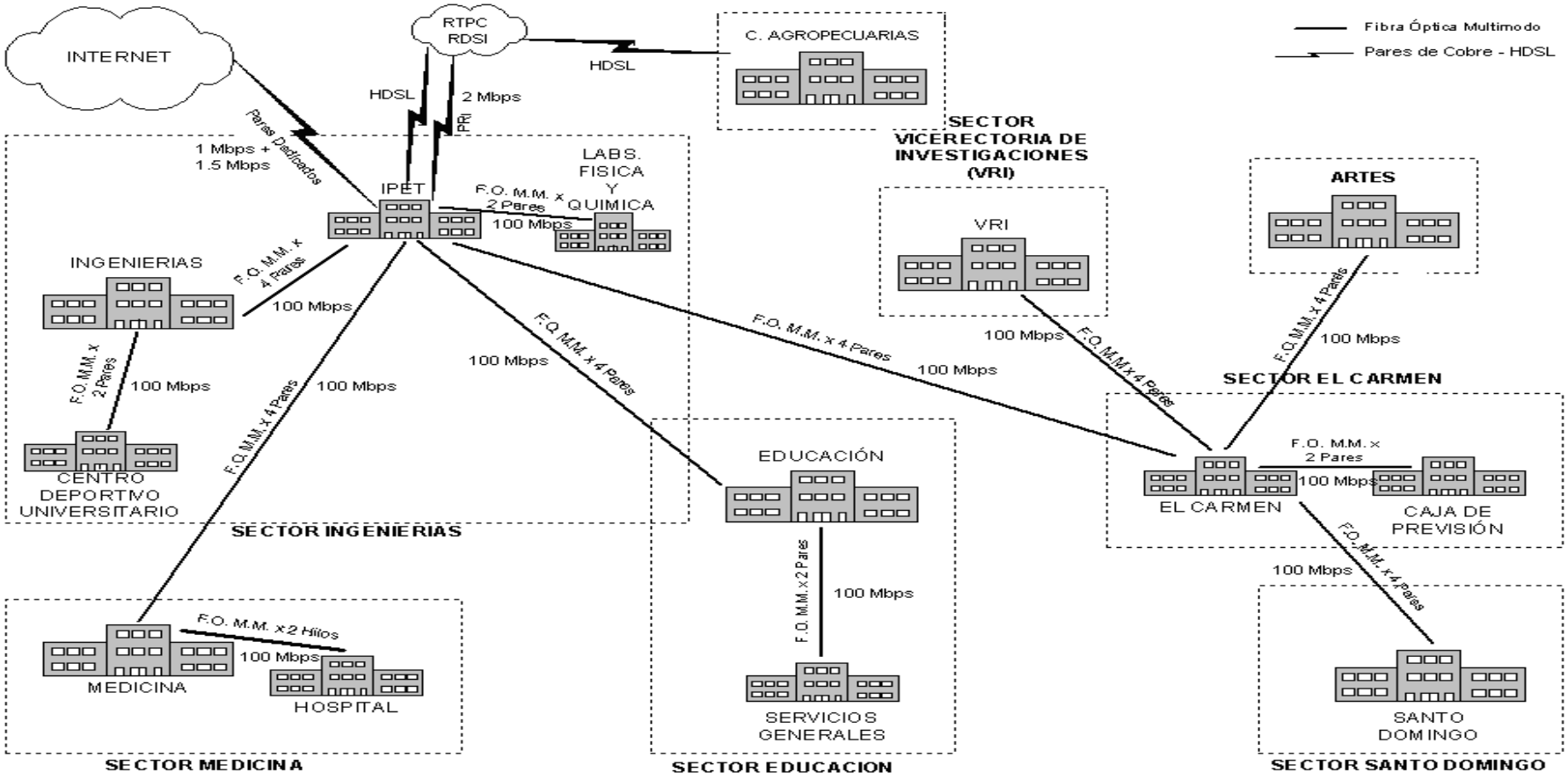


Figura 5.1 a) Topología inicial de la Intranet de la Universidad del Cauca.

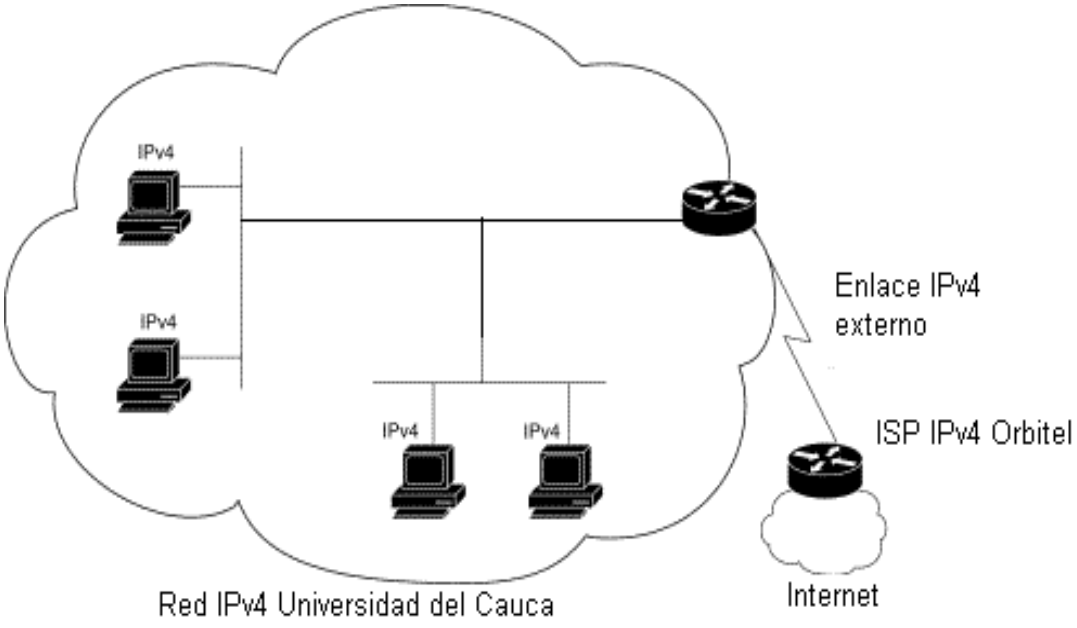


Figura 5.1 b) Topología inicial de la Intranet de la Universidad del Cauca simplificada.

- Un host 6to4 se puede comunicar con hosts 6to4 de otros sitios de la red Internet IPv4. Este tipo de comunicación se produce cuando un host 6to4 reenvía al enrutador 6to4 del sitio local el tráfico IPv6 que está destinado a un host 6to4 de otro sitio. El enrutador 6to4 del sitio local encapsula el tráfico IPv6 con un encabezado IPv4 y lo envía al enrutador 6to4 del sitio de destino en Internet. El enrutador 6to4 del sitio de destino quita el encabezado IPv4 y reenvía el paquete IPv6 al host 6to4 correcto mediante la infraestructura de enrutamiento IPv6 del sitio de destino.
- Un host 6to4 se puede comunicar con hosts de 6bone. Este tipo de comunicación se produce cuando un host 6to4 reenvía al enrutador 6to4 del sitio local el tráfico IPv6 que está destinado a un host de 6bone. El enrutador 6to4 del sitio local encapsula el tráfico IPv6 con un encabezado IPv4 y lo envía a un enrutador de retransmisión 6to4 que está conectado a la red Internet IPv4 y al 6bone. El enrutador de retransmisión 6to4 quita el encabezado IPv4 y reenvía el paquete IPv6 al host de 6bone correcto mediante la infraestructura de enrutamiento IPv6 de 6bone.

Todos estos tipos de comunicación utilizan tráfico IPv6 sin el requisito de obtener una conexión directa al 6bone o un prefijo de dirección global IPv6 de un proveedor de servicios de Internet (ISP).

Los túneles 6to4 proveen un mecanismo para acceder al 6bone y a través de este, a sitios IPv6 finales, utilizando túneles sobre Internet IPv4. Para prevenir interferencia con la red

actual, la solución debe ser inicialmente desplegada en una red aislada (Isla), como un ambiente de prueba.

Estrategia.
La idea es empezar con una red IPv4 que tenga una conexión IPv4 externa a un ISP, en el caso de la Universidad del Cauca será Orbitel en Medellín. Se requiere una conexión IPv4 porque el túnel al 6bone que se establecerá usará IPv4 para transportar el tráfico IPv6.

Selección del Ambiente IPv6 inicial de Prueba.
Se debe elegir cual de los tres ambientes siguientes es más conveniente para el proyecto de llevar a cabo la conexión inicial al 6bone:

- Una red de prueba completamente separada, como un laboratorio.
- Una red de prueba que se conecta al resto de la red, pero que este aislada por un "firewall" que no deje pasar el tráfico IPv6.
- Una red de prueba integrada al resto de la red con el tráfico IPv6 fluyendo libremente por toda la red.

Una vez seleccionado el ambiente más adecuado se debe empezar el proceso de implementación, llevando a cabo etapa por etapa para lograr una transición adecuada sin que esta ocasione problemas operacionales dentro de la red de datos de la Universidad del Cauca.

A continuación se describe el ambiente más completo como ya se mencionó anteriormente, no siendo este, el ambiente implementado finalmente debido a la limitación de recursos.

Aprovisionar la Red IPv6 de Prueba.
Se Instalan los dispositivos que se usarán en la red IPv6 de prueba. La figura 5.2 muestra una red de prueba IPv6 que se aísla de la red IPv4 de la Universidad del Cauca por un "firewall" que se configura para bloquear tráfico IPv6. Todos los enrutadores en la red de prueba se configuran para ejecutar la pila dual IPv4/IPv6.

Nota: el proceso de instalación y de configuración de todos los dispositivos utilizados para esta y otras prácticas se encuentra de manera detallada en el Anexo D.

Identificar el enrutador para Conectarse al 6bone.
En la red IPv6 de prueba, se identifica un enrutador fronterizo que se usará para conectarse al "6bone ISP". Este enrutador fronterizo debe ser un enrutador con pila dual que se configurará con el túnel para pasar el tráfico IPv6 sobre Internet IPv4.

En la actualidad muchas empresas dedicadas al desarrollo de este tipo de dispositivos como Cisco Systems, 3Com entre otras ya cuentan con dispositivos que soportan los dos protocolos IPv6 e IPv4 y se pueden configurar para funcionar ya sea para funcionar con uno solo o con los dos (Pila Dual). Así como sistemas operativos que soportan enrutamiento a nivel de software como Linux y FreeBSD ambos con Zebra que instalado actúa como un enrutador dedicado y Windows XP/2000 que también se puede configurar como enrutador habilitándole ICS (Conexión compartida a Internet).

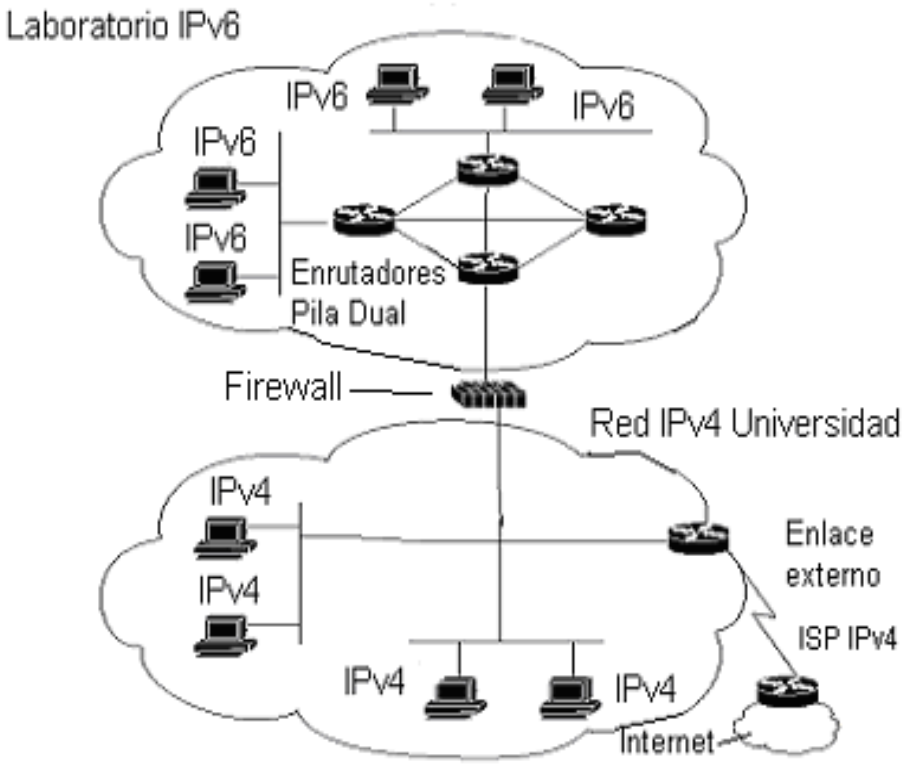


Figura 5.2 Topología de la red inicial con la red de prueba adicionada.

Nota: La configuración de Windows XP como enrutador se describe de manera detallada en el Anexo D.

Recibir Información de la dirección IPv4 del 6bone ISP.

Se le pide al "6bone ISP" que configure su extremo del túnel, y entonces se obtiene de este la dirección IPv4 del enrutador que se usará para el acceso al 6bone. El 6Bone ISP es el enrutador de retransmisión más cercano o el seleccionado por defecto como en el caso del enrutador de retransmisión de Microsoft que es el enrutador por defecto para los equipos con Windows XP. El enrutador de retransmisión no es el mismo enrutador fronterizo seleccionado para la Intranet.

Ya que se estará configurando un túnel 6to4 al 6bone, la dirección IPv6 (global) del enrutador fronterizo será la dirección IPv4 concatenada al prefijo 6to4 2002::/16.

El proveedor de servicio de Internet (ISP) que usa la Isla para conectarse al 6bone no puede ser el mismo ISP que se usa para la conectividad IPv4. El "6bone ISP" debe ser el enrutador más cercano que proporcione un servicio de retransmisión 6to4 como se mencionó anteriormente, así no se restringe la conexión al ISP local.

Configurar el enrutador fronterizo.
Usando la dirección IPv4 del "6bone ISP", se configura el enrutador fronterizo designado para ejecutar la pila dual, con un túnel 6to4 que se conecta al 6bone. Se recomienda que cada sitio tenga una única dirección 6to4 asignada a la interfaz externa del enrutador. Todos los sitios necesitan ejecutar un protocolo IPv6 de enrutamiento interior tal como el Protocolo de Información de Ruta (RIPng) para el enrutamiento IPv6 dentro del sitio, pero el enrutamiento exterior es manejado por el protocolo correspondiente a IPv4. Se consigue así conectividad al 6bone desde la red de prueba, como se muestra en la figura 5.3.

Nota: la configuración del enrutador fronterizo utilizando Windows XP se encuentra de manera detallada en el Anexo D.

Conectar la Red (Isla) de la Universidad del Cauca al 6bone.
Cuando se este listo para desplegar IPv6 en la red de la Universidad, la conexión al "6bone ISP" será hecha a través de su ISP IPv4. Se configura el enrutador fronterizo para que se una al ISP IPv4 y para correr la pila dual con un túnel 6to4 al "6bone ISP". La dirección IPv4 del enrutador fronterizo que se une al ISP IPv4 cambiará según la dirección que el ISP IPv4 le proporcione. Se Identifican otros enrutadores y hosts en la red que deseen tener conectividad IPv6. Se necesitará configurar cada uno de estos dispositivos para ejecutar la pila dual de protocolos.

Se puede quitar el firewall entre la red de la Universidad y el laboratorio para permitir que el tráfico IPv6 fluya a lo largo de la red, y se puede mantener una porción de la red como IPv4 solamente hasta que se esté listo para desplegar IPv6 en toda la red. La Figura 5.4 muestra la red de la Universidad con conectividad IPv6 al 6bone a través de un túnel 6to4 vía su ISP IPv4.

Las dos siguientes figuras muestran la topología de una red como la de la Universidad del Cauca en donde se ha implementado un ambiente de prueba IPv6 adecuado para mantener la red de prueba aislada inicialmente a través de un firewall como se observa en la figura 5.3 y conectada al 6Bone a través del "6Bone ISP" que en este caso es el enrutador de retransmisión más cercano.

En la figura 5.4 se observa la misma red pero esta vez la red de prueba IPv6 se ha integrado a toda la red, en donde además se ha comenzado a migrar la mayoría de equipos (host, enrutadores, servidores, etc.) a direcciones IPv6 con el prefijo 6to4 (2002:) pero conservando también la dirección IPv4 a lo que se le llama "Pila Dual".

La topología mostrada en la figura 5.4, se conecta al 6Bone a través del proveedor de servicio de Internet IPv4 utilizando un túnel IPv6 sobre IPv4 (6to4). Dentro de esta red se conserva una pequeña porción de la red con equipos soló IPv4 (la red soló IPv4 se observa en la parte inferior de la figura 5.4) conectados a un enrutador con pila dual, con el propósito de seguir utilizando aquellos equipos que aun no soportan el protocolo IPv6.

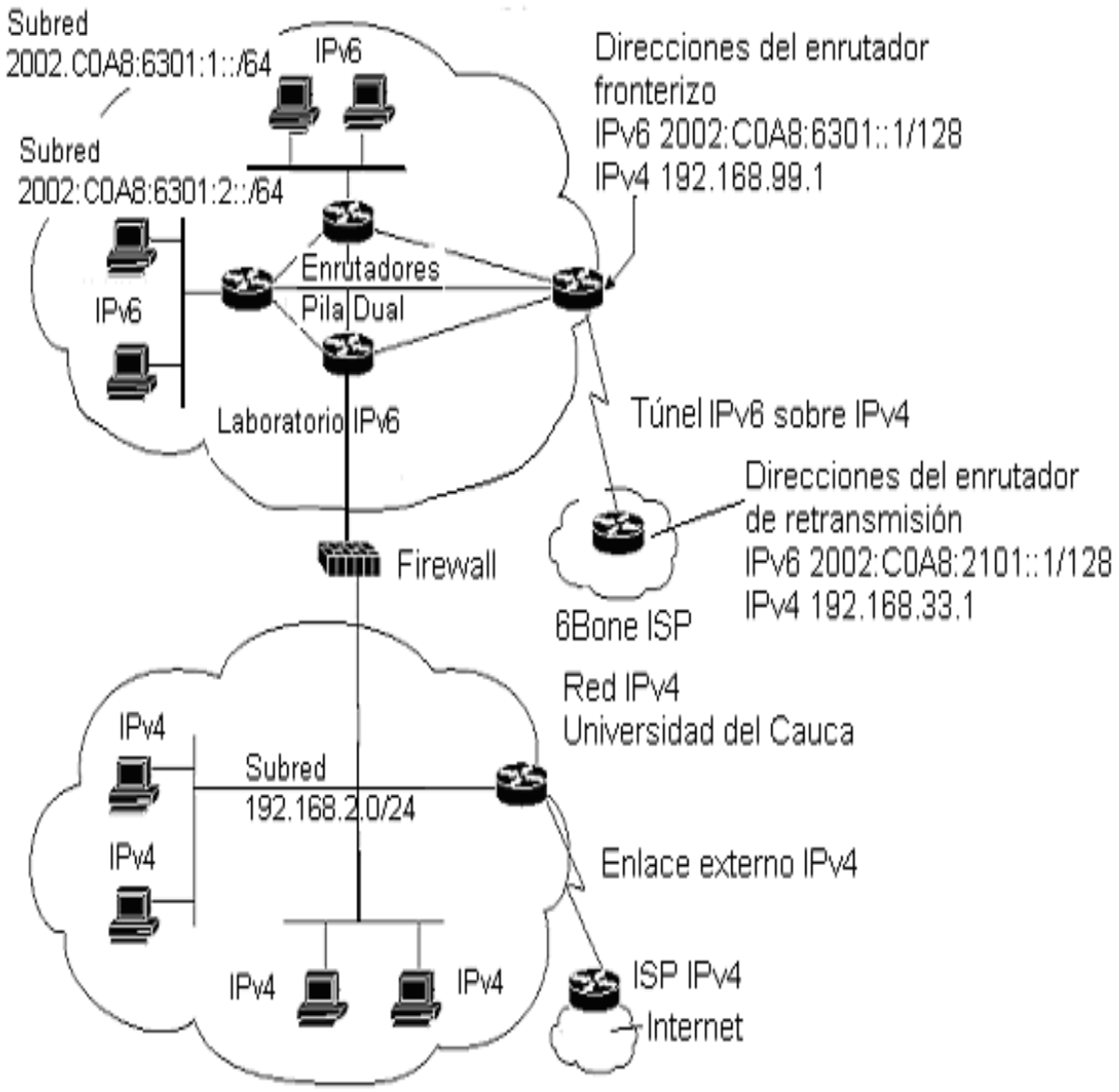


Figura 5.3 Conectividad establecida desde la red de prueba hasta el ISP 6Bone.

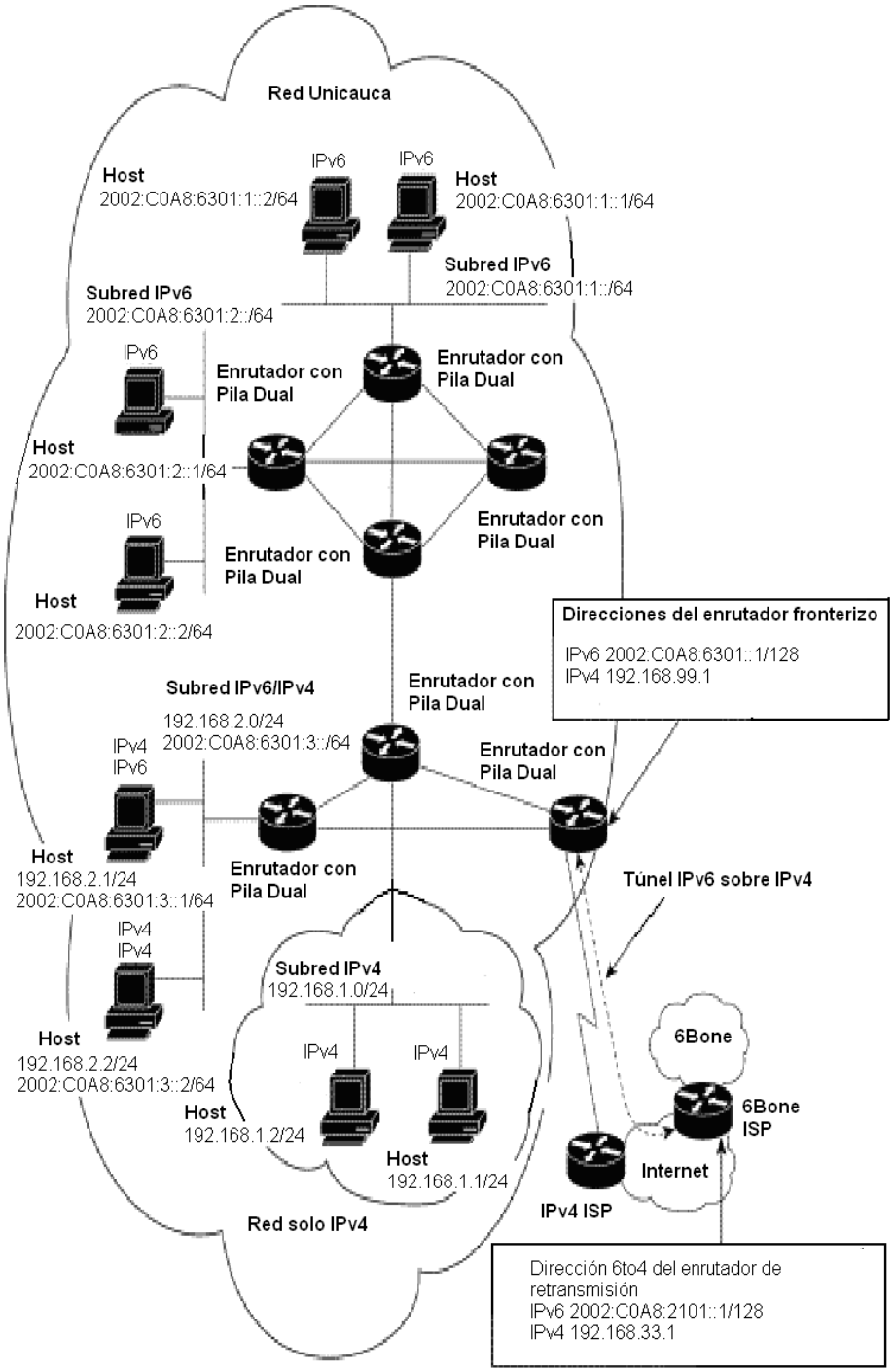


Figura 5.4 Intranet de la Universidad del Cauca con conectividad IPv6 al 6Bone.

5.5 Implementación de la isla ipv6 de la Universidad del Cauca y conexión al 6Bone.

5.5.1 Topología de la red implementada.

La figura 5.5 muestra la topología de la isla IPv6 de la Universidad del Cauca usando un túnel 6to4 al 6bone a través del enrutador de retransmisión 6to4 de Microsoft.

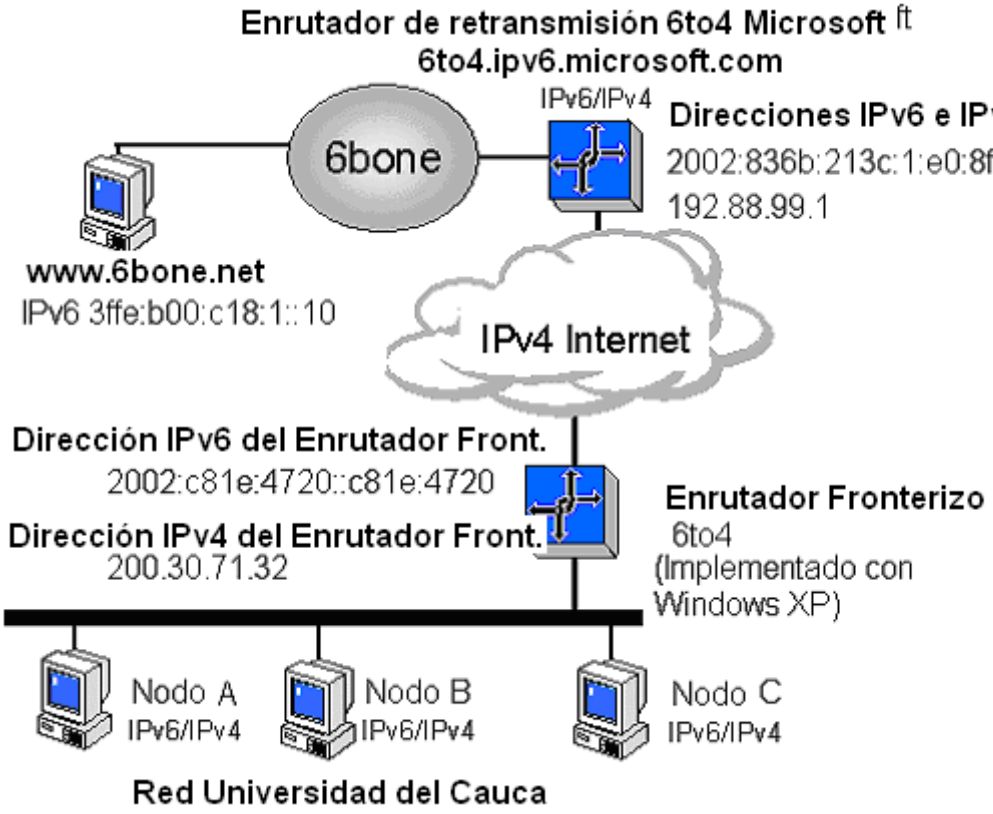


Figura 5.5 Topología de la Isla IPv6 implementada en la Universidad del Cauca.

5.5.2 Cómo Trabaja esta Solución.

Un túnel 6to4 se configura en un enrutador fronterizo con pila dual, el cual es el computador asignado para el desarrollo de este trabajo de grado, al que se le instaló el sistema operativo Windows XP y se configuró para funcionar como enrutador (la configuración de este equipo se encuentra de manera detallada en el Anexo D). Todo el tráfico IPv6 dirigido hacia el 6bone es enrutado sobre IPv4 a través del túnel 6to4 hasta el enrutador de retransmisión 6to4 del "6bone ISP" (Enrutador de retransmisión 6to4 de Microsoft el cual es el 6bone ISP por defecto para los equipos con Windows XP)). El tráfico dirigido desde el 6bone hacia la Isla IPv6 de la Universidad, es enrutado sobre IPv4

a través del túnel 6to4 hacia el enrutador fronterizo con pila dual de la Universidad del Cauca, y desde este, al host IPv6 de destino.

Los equipos que se encuentran en la parte inferior de la figura 5.5 se encuentran dentro de la red de la Universidad del Cauca y pertenecen a la Isla IPv6, ya que se les ha instalado el protocolo IPv6 y se han configurado automáticamente con una direccion IPv6 con el prefijo 2002:c81e:4720::/48 al recibir anuncios de enrutador desde el enrutador fronterizo de la Universidad.

Cada nodo dentro de la Isla IPv6 se configura con una dirección IPv6 y mantiene su dirección IPv4 de Intranet asignada para permitirle a este host seguir manejando tráfico IPv4 y a la vez acceder a sitios Web IPv6 que se encuentren conectados al 6Bone como en el caso de la figura 5.5, los host con pila dual IPv6/IPv4 acceden al sitio Web IPv6 del 6Bone (www.6bone.net) con una dirección IPv6 3ffe:b00:c18:1::10.

5.5.3 Beneficios.

Los beneficios para la Universidad al usar túneles 6to4 son los siguientes:

- Los túneles 6to4 son soportados por muchos de los sistemas operativos y aplicaciones actuales con los que cuenta la Universidad como Windows 2000/XP, Linux Red Hat 7.3/8.0, Internet Explorer, cliente ftp, telnet entre otras. No teniendo así que adquirir nuevos sistemas operativos.
- La configuración del host del usuario final es simple y requiere una gestión operativa mínima.
- El túnel es automático; ninguna configuración específica se requiere en el sitio de retransmisión 6to4.
- Los túneles 6to4 son escalables. Ya que a partir de estos se puede empezar un proceso de transición que lleve a la Universidad a contar con una red toda IPv6.
- Esta solución se acomoda a direcciones IP dinámicas.
- El túnel 6to4 sólo existe durante la sesión. Porque no es una carga permanente para el tráfico de la red de datos de la Universidad del Cauca.

5.5.4 Inconvenientes.

Los inconvenientes al usar túneles 6to4 son los siguientes:

- Independientemente de cómo se haga el manejó de NAT Network Address Translation (Traducción de Direcciones de Red), no es permitido a lo largo del camino del túnel.
- El mecanismo de túnel 6to4 proporciona un bloque de dirección /48; ninguna dirección más está disponible.
- Ya que el prefijo IPv6 de direcciones de 6to4 de la Universidad es determinado por la dirección IPv4 y depende de esta, la migración a una red IPv6 nativa requiere el renumerando de toda la red.
- Esta solución es limitada para enrutamiento estático o BGP4+.

5.5.5 Pasos de la Implementación.

Esta sección describe el proceso de implementación de la Isla IPv6 de la Universidad del Cauca y la conexión al 6bone utilizando un túnel 6to4.

Contiene las siguientes secciones:

- Requisitos previos y consideraciones de diseño.
- Pasos del proceso de implementación para la Universidad del Cauca.
- Características de dispositivos.
- Archivos de Configuración comentados.

Requisitos previos y Consideraciones de diseño.

Antes de que se lleve a cabo un túnel 6to4 al 6bone, se deben realizar las siguientes tareas:

Nota: Cuando se configuran túneles 6to4 en los enrutadores fronterizos, se debe usar direcciones IPv4 globalmente ruteables. Las direcciones IPv4 que se usaron en las configuraciones del ejemplo en este documento no son globalmente ruteables ni son direcciones reales de la Universidad del Cauca y sólo se usan con propósitos ilustrativos.

- Identificar el enrutador fronterizo del sitio, el cual se configurará para ejecutar la pila dual. Este enrutador debe tener una dirección IPv4 estática, globalmente ruteable. Para este trabajo de grado se utilizo un equipo Dell/Pentium 3 con Windows XP y con ICS (conexión compartida a Internet) habilitada para funcionar como enrutador.
- Del “6bone ISP”, se obtiene la dirección IPv4 haciendo un ping a la dirección DNS (6to4.ipv6.microsoft.com) del enrutador de retransmisión 6to4 que se usará para el acceso al 6bone.
- Cerciorarse que la aplicación actual de la pila dual en los equipos esta corriendo, permitiendo que aplicaciones como TFTP, ping, Telnet, y traceroute corran sobre IPv4 o sobre IPv6.
- Seleccione un protocolo de enrutamiento IPv6 interior, como RIPng que sea apropiado para la configuración de la red. La solución presentada en este documento usa una ruta estática. El protocolo de enrutamiento exterior es manejado por el protocolo de enrutamiento IPv4 correspondiente.
- Se configuran todos los enrutadores con pila dual para usar RIP.

Nota: la configuración de los enrutadores con RIP, la forma de obtener la dirección IPv4 del enrutador de retransmisión así como la forma de cerciorarse que la pila dual corre en cada equipo se encuentra detallada en el Anexo D.

Pasos del proceso de implementación de la Isla para la Universidad del Cauca.

Después de haber instalado el protocolo IPv6 en todos los equipos y de cerciorarse que están corriendo la pila dual y el protocolo de enrutamiento RIP se procede con la configuración de las direcciones y el establecimiento del túnel.

Partiendo de la dirección IPv4 global, asignada para la implementación de la isla la cual es 200.30.71.32. Se deriva el prefijo 6to4 convirtiendo los componentes decimales de la dirección IPv4 al hexadecimal y añadiendo el prefijo “2002” al número hexadecimal resultante. Así el prefijo 6to4 de los nodos en la red IPv6 de la Universidad serán 2002:c81e:4720::/48 según la tabla 5.1.

La parte de la dirección IPv6 (c81e:4720) se forma de la dirección IPv4 convirtiendo cada octeto de la notación decimal punteada a su equivalente hexadecimal, como se muestra en la tabla 5.1.

Decimal	Hexadecimal
200	C8
30	1E
71	47
32	20

Tabla 5.1 Conversión de la notación decimal de IPv4 a hexadecimal.

El “6bone ISP” de Microsoft proporciona la dirección IPv4 del enrutador de retransmisión 6to4: 192.88.99.1. Usando la dirección del enrutador de retransmisión, se configura un túnel 6to4 en el enrutador fronterizo con pila dual de la Isla IPv6 de la Universidad del Cauca. Utilizando un equipo con Windows 2000 se deberán introducir los siguientes comandos:

Nota: El mismo proceso lo realiza Windows XP de forma automática, pero para propósitos ilustrativos se explica con Windows 2000, al que además hay que instalarle el stack del protocolo IPv6 ya que este no lo trae.

ipv6 rtu 2002::/16 2

El comando ipv6 rtu realiza una actualización en la tabla de enrutamiento, este puede ser usado para adicionar, remover o actualizar una ruta, en este caso habilita 6to4.

El argumento 2002::/16 es el prefijo de la ruta, especifica el único prefijo 6to4.

El argumento 2 especifica la interfaz del enlace para este prefijo. la Interfaz #2 es la "pseudo-interfaz" usada para los túneles configurados, túneles automáticos, y 6to4. Cuando una dirección de destino IPv6 corresponde al prefijo 2002::/16, los 32 bits que le siguen al prefijo en la dirección de destino son extraídos para formar una dirección IPv4 de destino. El paquete se encapsula con una cabecera IPv4 y se envía a la dirección IPv4 de destino.

ipv6 adu 2/2002:c81e:4720::c81e:4720

El comando ipv6 adu realiza una actualización de una dirección. Puede usarse para agregar, remover, o puede actualizar una dirección en una interfaz. En este caso, este configura la dirección 6to4 del computador.

El argumento 2/2002:c81e:4720::c81e:4720 especifica la interfaz y " la dirección. Este configura la dirección 2002:c81e:4720::c81e:4720 en la interfaz #2. La dirección es creada usando el prefijo de sitio 2002:c81e:4720::/48, la subred 0 da un prefijo de subred 2002:c81e:4720::/64, y un identificador de interfaz de 64-bits.

Las dos órdenes anteriores son suficientes para permitir comunicación con otros sitios 6to4. Por ejemplo, se puede probar haciendo ping al sitio 6to4 de Microsoft 6to4:

ping6 2002:836b:9820::836b:9820

Nota: Al utilizar la configuración automática del servicio 6to4, un host que ejecute el protocolo IPv6 en Windows XP y esté configurado con una dirección IPv4 pública se configurará automáticamente. Un host 6to4 puede crear su propio túnel para alcanzar hosts 6to4 de otros sitios o hosts del 6bone.

Para habilitar comunicación con el 6bone, se debe crear un túnel configurado por defecto a un enrutador de retransmisión 6to4. Se puede usar el enrutador de retransmisión 6to4 de Microsoft, 192.88.99.1:

ipv6 rtu:: /0 2/::192.88.99.1 pub life 1800

El comando ipv6 rtu realiza una actualización de la tabla de enrutamiento y establece, en este caso, una ruta predefinida al sitio de retransmisión 6to4.

El argumento :: /0 es el prefijo de la ruta. El prefijo de longitud cero indica que es una ruta predefinida.

El argumento 2/::192.88.99.1 especifica el próximo salto de vecino para este prefijo. Precisa que paquetes coincidentes con este prefijo sean enviados a la dirección ::192.88.99.1 usando la interfaz #2. Reenviando cada paquete a la dirección ::192.88.99.1 en la interfaz #2 causando que este sea encapsulado con una cabecera v4 y enviado a la dirección 192.88.99.1.

El argumento pub hace de esta, una ruta publicada. Ya que esto es sólo pertinente para los enrutadores, no tiene efecto hasta que la ruta se habilita. De igual forma, el tiempo de vida de 30 minutos sólo se aplica si la ruta se habilita.

Con los anteriores comandos ya existe un túnel 6to4 al 6Bone, y a través de este se puede acceder a sitios del 6Bone también como a sitios 6to4. Para probar esto se usa el siguiente comando:

ping6 3ffe:1cff:0:f5::1

El paso final es habilitar el enrutamiento en el equipo 6to4. Para este procedimiento la interfaz #4 en la computadora es una interfaz Ethernet y la interfaz #3 es 6to4. Cada computadora podría numerar sus interfaces de forma diferente. Los siguientes dos comandos asignan los prefijos de subred a los dos enlaces. Los prefijos de subred se derivan del prefijo 6to4 del sitio 2002:c81e:4720::/48:

Nota: Este procedimiento es el mismo para Windows XP. Al habilitar ICS se puede utilizar un equipo que ejecute el protocolo IPv6 como enrutador 6to4, que es capaz de encapsular y reenviar el tráfico 6to4 a otros hosts o sitios 6to4 de Internet, y reenviar el tráfico de 6bone a un enrutador de retransmisión 6to4 de Internet.

ipv6 rtu 2002:c81e:4720:1::/64 3 pub life 1800
ipv6 rtu 2002:c81e:4720:2::/64 4 pub life 1800

El comando ipv6 rtu especifica que el prefijo 2002:c81e:4720:1::/64 activa un enlace en la interfaz #3. Este configura el primer prefijo de subred en la interfaz Ethernet. La ruta se publica con un tiempo de vida de 30 minutos.

De igual manera, el prefijo 2002:c81e:4720:2::/64 se configura en la interfaz 6over4.

Los próximos tres comandos habilitan el equipo 6to4 para que funcione como un enrutador:

ipv6 ifc 2 forward
ipv6 ifc 3 forward
ipv6 ifc 4 advertises forward

Los comandos ipv6 ifc controlan los atributos de una interfaz. Un enrutador envía paquetes y envía anuncios de enrutador. En la implementación IPv6 de Microsoft, este par de atributos son controlados separadamente.

En la interfaz #3 no se necesita anuncios de enrutador porque es una pseudo-interfaz.

Si una computadora tiene interfaces adicionales, ellas también deberían configurarse para estar reenviando paquetes y anuncios de enrutador.

Después de ejecutar estos comandos, el protocolo IPv6 de Microsoft configurará las direcciones automáticamente en las interfaces #3 y #4 usando el respectivo prefijo de subred y las dos interfaces empezarán a enviar anuncios de enrutador aproximadamente a intervalos de 3 a 10 minutos.

Los host que reciben estos anuncios de enrutador se configurarán automáticamente con una ruta predefinida y una dirección 6to4 derivada del prefijo de subred del enlace. Estos tendrán comunicación a otros sitios 6to4 y el 6bone a través de la computadora que sirve como enrutador.

Si la Conexión compartida a Internet (ICS, Internet Connection Sharing) está habilitado en una interfaz que tiene asignada una dirección IPv4 pública, el servicio 6to4 lleva a cabo las acciones siguientes:

- Habilita el enrutamiento en la interfaz privada.
- Envía anuncios de enrutador que contienen prefijos de direcciones 6to4 basados en la dirección IPv4 pública de la interfaz pública. El Id. de SLA del prefijo de la dirección 6to4 se establece como el Id. de la interfaz en la que se envían los anuncios.

Los equipos host que ejecutan Windows XP en los segmentos de la red privada reciben el anuncio de enrutador que envía el enrutador 6to4 de su sitio y que contiene un prefijo de dirección 6to4. El resultado es que dos hosts 6to4 se pueden comunicar mediante direcciones 6to4 a través de Internet.

Aunque 6to4 se diseñó principalmente para permitir la comunicación entre sitios independientes habilitados para IPv6, los hosts 6to4 que utilicen el protocolo IPv6 de Windows XP pueden utilizar también direcciones 6to4 y túneles 6to4 para comunicarse en un conjunto de redes IPv4 o en Internet.

En todos los casos anteriores, aunque el tráfico IPv6 se transporta como la carga de un paquete IPv4 (la infraestructura IPv4 se considera como un nivel de vínculo IPv6), sigue siendo tráfico IPv6. Las aplicaciones que utilizan las direcciones asociadas con estos métodos utilizan las mismas funciones de Windows Sockets que si se utilizaran direcciones IPv6 globales y una infraestructura IPv6. Estos métodos se pueden utilizar para comprobar la funcionalidad IPv6 en las aplicaciones sin tener que implementar enrutadores IPv6 en la organización.

Características de los dispositivos.
La tabla 5.2 describe los dispositivos usados para esta solución.

5.6 Configuración de las interfaces de red de la Isla IPv6.

Esta sección muestra las configuraciones para cada interfaz en un host con el sistema operativo Windows XP y con las direcciones IPv4 privada y publica 172.16.130.92 y 200.30.71.32 respectivamente. Se pueden ver estas configuraciones usando el comando ipv6 if en el símbolo del sistema, la salida que genera este comando para la configuración del host 6to4 y del enrutador fronterizo 6to4 mostrado en la figura 5.5 se pueden ver a continuación:

Nota: En el anexo D (Practicas con el Protocolo IPv6) se encuentran de manera detallada los pasos a seguir para la configuración de esta y otras prácticas.

	Enrutador fronterizo Universidad del Cauca	6Bone ISP (Enrutador de retransmisión de Microsoft)
Nombre del host	IPv6 Unicauca	Enrutador de retransmisión 6to4 de Microsoft
Tipo de equipo	Dell OptiPlex GX 110 / pentium III	Microsoft (desconocido)
Interfaz fisica	Controlador Fast Ethernet integrado 3Com 3C920 (compatible 3C905C-TX)	Microsoft (desconocida)
Software utilizado	Windows 2000/XP	Windows (desconocido)
Memoria	128 MB RAM	
Direcciones IP	Ethernet: Ipv4 200.30.71.32 Tunel 2002: 2002:c81e:4720::1/128	Ethernet: Ipv4 192.88.99.1 Tunel2002: 2002:836b:213c::1/128

Tabla 5.2 Hardware y Software usado.

5.6.1 Equipo con Windows XP con IP de Intranet.

```
C:\>ipv6 if
Interfaz 4: Ethernet: Conexión de área local
{1704FC14-119A-43CB-AEB7-DD8E45A1E950}
 usa unidad de detección de equipos cercanos (Neighbor Discovery)
 utiliza descubrimiento de enrutador
 dirección de capa de vínculo: 00-b0-d0-c2-93-80
  preferred link-local fe80::2b0:d0ff:fec2:9380, duración infinite
  multidifusión interface-local ff01::1, 1 referencias, no se puede informar
  multidifusión link-local ff02::1, 1 referencias, no se puede informar
  multidifusión link-local ff02::1:ffc2:9380, 1 referencias, último informe
 vínculo MTU 1500 (vínculo MTU verdadero 1500)
 limite de saltos actual 128
 tiempo accesible 32500ms (base 30000ms)
 intervalo de retransmisión 1000ms
 transmisiones DAD 1
Interfaz 3: Seudo interfaz de túnel 6to4
{A995346E-9F3E-2EDB-47D1-9CC7BA01CD73}
  no usa unidad de detección de equipos cercanos (Neighbor Discovery)
  no utiliza descubrimiento de enrutador
  preferencia de enrutamiento 1
  vínculo MTU 1280 (vínculo MTU verdadero 65515)
  limite de saltos actual 128
  tiempo accesible 29000ms (base 30000ms)
  intervalo de retransmisión 1000ms
  transmisiones DAD 0
Interfaz 2: Seudo interfaz de túnel automático
{48FCE3FC-EC30-E50E-F1A7-71172AEEE3AE}
  no usa unidad de detección de equipos cercanos (Neighbor Discovery)
  no utiliza decubrimiento de enrutador
  preferencia de enrutamiento 1
  Dirección IPv4 con EUI-64 incrustado: 0.0.0.0
  Dirección de capa de enlace del enrutador: 0.0.0.0
    preferred link-local fe80::5efe:172.16.130.92, duración infinite
```

```
  vínculo MTU 1280 (vínculo MTU verdadero 65515)
  limite de saltos actual 128
  tiempo accesible 40500ms (base 30000ms)
  intervalo de retransmisión 1000ms
  transmisiones DAD 0
Interfaz 1: Seudo interfaz de bucle invertido
{6BD113CC-5EC2-7638-B953-0B889DA72014}
  no usa unidad de detección de equipos cercanos (Neighbor Discovery)
  no utiliza decubrimiento de enrutador
  dirección de capa de vínculo:
    preferred link-local ::1, duración infinite
    preferred link-local fe80::1, duración infinite
  vínculo MTU 1500 (vínculo MTU verdadero 4294967295)
  limite de saltos actual 128
  tiempo accesible 24000ms (base 30000ms)
  intervalo de retransmisión 1000ms
  transmisiones DAD 0
```

5.6.2 Equipo con Windows XP con IP global e IP de Intranet configurado como host 6to4.

```
C:\>ipv6 if
Interfaz 4: Ethernet: Conexión de área local
{1704FC14-119A-43CB-AEB7-DD8E45A1E950}
  usa unidad de detección de equipos cercanos (Neighbor Discovery)
  utiliza descubrimiento de enrutador
  dirección de capa de vínculo: 00-b0-d0-c2-93-80
    preferred link-local fe80::2b0:d0ff:fec2:9380, duración infinite
    multidifusión interface-local ff01::1, 1 referencias, no se puede informar
    multidifusión link-local ff02::1, 1 referencias, no se puede informar
    multidifusión link-local ff02::1:ffc2:9380, 1 referencias, último informe
  vínculo MTU 1500 (vínculo MTU verdadero 1500)
  limite de saltos actual 128
  tiempo accesible 32500ms (base 30000ms)
  intervalo de retransmisión 1000ms
  transmisiones DAD 1
Interfaz 3: Seudo interfaz de túnel 6to4
{A995346E-9F3E-2EDB-47D1-9CC7BA01CD73}
  no usa unidad de detección de equipos cercanos (Neighbor Discovery)
  no utiliza decubrimiento de enrutador
  preferencia de enrutamiento 1
    preferred global 2002:c81e:4720::c81e:4720, duración infinite
  vínculo MTU 1280 (vínculo MTU verdadero 65515)
  limite de saltos actual 128
  tiempo accesible 29000ms (base 30000ms)
  intervalo de retransmisión 1000ms
  transmisiones DAD 0
Interfaz 2: Seudo interfaz de túnel automático
{48FCE3FC-EC30-E50E-F1A7-71172AEEE3AE}
  no usa unidad de detección de equipos cercanos (Neighbor Discovery)
  no utiliza decubrimiento de enrutador
  preferencia de enrutamiento 1
  Dirección IPv4 con EUI-64 incrustado: 0.0.0.0
  Dirección de capa de enlace del enrutador: 0.0.0.0
    preferred link-local fe80::5efe:172.16.130.92, duración infinite
    preferred link-local fe80::5efe:200.30.71.32, duración infinite
  vínculo MTU 1280 (vínculo MTU verdadero 65515)
  limite de saltos actual 128
```

```
  tiempo accesible 40500ms (base 30000ms)
  intervalo de retransmisión 1000ms
  transmisiones DAD 0
Interfaz 1: Seudo interfaz de bucle invertido
{6BD113CC-5EC2-7638-B953-0B889DA72014}
  no usa unidad de detección de equipos cercanos (Neighbor Discovery)
  no utiliza decubrimiento de enrutador
  dirección de capa de vínculo:
    preferred link-local ::1, duración infinite
    preferred link-local fe80::1, duración infinite
  vínculo MTU 1500 (vínculo MTU verdadero 4294967295)
  limite de saltos actual 128
  tiempo accesible 24000ms (base 30000ms)
  intervalo de retransmisión 1000ms
  transmisiones DAD 0
```

5.6.3 Equipo con Windows XP con IP global configurado como enrutador 6to4.

```
C:\>ipv6 rtu 2002:c81e:4720:1::/64 3 pub life 1800
C:\>ipv6 rtu 2002:c81e:4720:2::/64 4 pub life 1800
C:\>ipv6 ifc 4 forwards advertises
C:\>ipv6 ifc 3 forwards
C:\>ipv6 ifc 2 forwards
C:\>ipv6 if
Interfaz 4: Ethernet: Conexión de área local
{1704FC14-119A-43CB-AEB7-DD8E45A1E950}
  usa unidad de detección de equipos cercanos (Neighbor Discovery)
  utiliza descubrimiento de enrutador
  envía anuncios de enrutador
  retransmite paquetes
  dirección de capa de vínculo: 00-b0-d0-c2-93-80
    preferred global 2002:c81e:4720:2:28ed:caa2:2cf2:d829, duración 29m53s
(anónimo)
    preferred global 2002:c81e:4720:2:2b0:d0ff:fec2:9380, duración 29m53s
(público)
    preferred link-local fe80::2b0:d0ff:fec2:9380, duración infinite
    multidifusión interface-local ff01::1, 1 referencias, no se puede informar
    multidifusión link-local ff02::1, 1 referencias, no se puede informar
    multidifusión link-local ff02::1:ffc2:9380, 2 referencias, último informe
    multidifusión interface-local ff01::2, 1 referencias, no se puede informar
    multidifusión link-local ff02::2, 1 referencias, último informe
    multidifusión site-local ff05::2, 1 referencias, último informe
    multidifusión link-local ff02::1:fff2:d829, 1 referencias, último informe
    cualquier difusión global 2002:c81e:4720:2::
    multidifusión link-local ff02::1:ff00:0, 1 referencias, último informe
  vínculo MTU 1500 (vínculo MTU verdadero 1500)
  limite de saltos actual 128
  tiempo accesible 32500ms (base 30000ms)
  intervalo de retransmisión 1000ms
  transmisiones DAD 1
Interfaz 3: Seudo interfaz de túnel 6to4
{A995346E-9F3E-2EDB-47D1-9CC7BA01CD73}
  no usa unidad de detección de equipos cercanos (Neighbor Discovery)
  no utiliza descubrimiento de enrutador
  retransmite paquetes
  preferencia de enrutamiento 1
    preferred global 2002:c81e:4720::c81e:4720, duración infinite
  vínculo MTU 1280 (vínculo MTU verdadero 65515)
```

```
  limite de saltos actual 128
  tiempo accesible 29000ms (base 30000ms)
  intervalo de retransmisión 1000ms
  transmisiones DAD 0
Interfaz 2: Seudo interfaz de túnel automático
{48FCE3FC-EC30-E50E-F1A7-71172AEEE3AE}
  no usa unidad de detección de equipos cercanos (Neighbor Discovery)
  no utiliza descubrimiento de enrutador
  retransmite paquetes
  preferencia de enrutamiento 1
  Dirección IPv4 con EUI-64 incrustado: 0.0.0.0
  Dirección de capa de enlace del enrutador: 0.0.0.0
    preferred link-local fe80::5efe:172.16.130.92, duración infinite
    preferred link-local fe80::5efe:200.30.71.32, duración infinite
  vínculo MTU 1280 (vínculo MTU verdadero 65515)
  limite de saltos actual 128
  tiempo accesible 40500ms (base 30000ms)
  intervalo de retransmisión 1000ms
  transmisiones DAD 0
Interfaz 1: Seudo interfaz de bucle invertido
{6BD113CC-5EC2-7638-B953-0B889DA72014}
  no usa unidad de detección de equipos cercanos (Neighbor Discovery)
  no utiliza descubrimiento de enrutador
  dirección de capa de vínculo:
    preferred link-local ::1, duración infinite
    preferred link-local fe80::1, duración infinite
  vínculo MTU 1500 (vínculo MTU verdadero 4294967295)
  limite de saltos actual 128
  tiempo accesible 24000ms (base 30000ms)
  intervalo de retransmisión 1000ms
  transmisiones DAD 0
```

5.6.4 Equipo con Windows XP que recibe anuncios de enrutador.

```
C:\>ipv6 if
Interfaz 4: Ethernet: Conexión de área local
{24194D6F-C305-49C0-BB42-A0851D27511B}
  usa unidad de detección de equipos cercanos (Neighbor Discovery)
  utiliza descubrimiento de enrutador
  dirección de capa de vínculo: 00-06-5b-76-05-a6
   preferred global 2002:c81e:4720:2:f0e4:8a9f:24f9:6a, duración 28m54s (anónimo)
   preferred global 2002:c81e:4720:2:206:5bff:fe76:5a6, duración 28m54s (público)
   preferred link-local fe80::206:5bff:fe76:5a6, duración infinite
    multidifusión interface-local ff01::1, 1 referencias, no se puede informar
    multidifusión link-local ff02::1, 1 referencias, no se puede informar
    multidifusión link-local ff02::1:ff76:5a6, 2 referencias, último informe
    multidifusión link-local ff02::1:fff9:6a, 1 referencias, último informe
  vínculo MTU 1500 (vínculo MTU verdadero 1500)
  limite de saltos actual 128
  tiempo accesible 42000ms (base 30000ms)
  intervalo de retransmisión 1000ms
  transmisiones DAD 1
Interfaz 3: Seudo interfaz de túnel 6to4
{A995346E-9F3E-2EDB-47D1-9CC7BA01CD73}
  no usa unidad de detección de equipos cercanos (Neighbor Discovery)
  no utiliza decubrimiento de enrutador
  preferencia de enrutamiento 1
  vínculo MTU 1280 (vínculo MTU verdadero 65515)
```

```
  limite de saltos actual 128
  tiempo accesible 25000ms (base 30000ms)
  intervalo de retransmisión 1000ms
  transmisiones DAD 0
Interfaz 2: Seudo interfaz de túnel automático
{48FCE3FC-EC30-E50E-F1A7-71172AEEE3AE}
  no usa unidad de detección de equipos cercanos (Neighbor Discovery)
  no utiliza decubrimiento de enrutador
  preferencia de enrutamiento 1
  Dirección IPv4 con EUI-64 incrustado: 0.0.0.0
  Dirección de capa de enlace del enrutador: 0.0.0.0
    preferred link-local fe80::5efe:172.16.70.68, duración infinite
  vínculo MTU 1280 (vínculo MTU verdadero 65515)
  limite de saltos actual 128
  tiempo accesible 28500ms (base 30000ms)
  intervalo de retransmisión 1000ms
  transmisiones DAD 0
Interfaz 1: Seudo interfaz de bucle invertido
{6BD113CC-5EC2-7638-B953-0B889DA72014}
  no usa unidad de detección de equipos cercanos (Neighbor Discovery)
  no utiliza decubrimiento de enrutador
  dirección de capa de vínculo:
    preferred link-local ::1, duración infinite
    preferred link-local fe80::1, duración infinite
  vínculo MTU 1500 (vínculo MTU verdadero 4294967295)
  limite de saltos actual 128
  tiempo accesible 24000ms (base 30000ms)
  intervalo de retransmisión 1000ms
  transmisiones DAD 0
```

5.7 Descripción de la Topología final.

La topología fínal de la Intranet de la Universidad del Cauca junto con la Isla IPv6 Unicauca se puede observar en la figura 5.6 en donde se puede observar la red de la Universidad del Cauca Integrada con la Isla IPv6 y conectada al 6Bone utilizando un túnel 6to4 (línea punteada de color rojo), este túnel se hace a través del enrutador de la Universidad con dirección 200.30.71.254 cuyo proveedor de servicio de Internet es Orbitel, la dirección IPv4 del extremo del túnel que le corresponde a la Universidad es 200.30.71.32 que le pertenece al enrutador fronterizo 6to4 que es el encargado de enrutar el tráfico de la Isla IPv6 a través del túnel mencionado anteriormente, la dirección IPv4 del extremo del túnel del enrutador de retransmisión es la dirección 192.88.99.1 de Microsoft.

Se observan en la figura 5.6 las siguientes partes:

- Isla IPv6 de la Universidad del Cauca, Nodos A, B, C, con Pila Dual (1).
- Intranet de la Universidad del Cauca, Nodos D, E,….,N, Host IPv4 (2).
- Enrutador de Retransmisión 6to4, equipo asignado para el trabajo de grado con direccion global 200.30.71.32 y sistema operativo Windows XP configurado para funcionar como enrutador (3).
- Túnel 6to4 entre la Isla IPv6 de la Universidad del Cauca y el 6Bone (4).
- Enrutador de la Universidad del Cauca, 200.30.71.254 ISP Orbitel (5).
- ISP IPv4 Orbitel (6).

- Enrutador de Retransmisión 6to4, 6to4.ipv6.microsoft.com, ISP 6Bone (7).
- 6Bone (8).
- Sitio IPv6 del 6Bone www.6bone.net al que se puede acceder a través del túnel 6to4 (9).

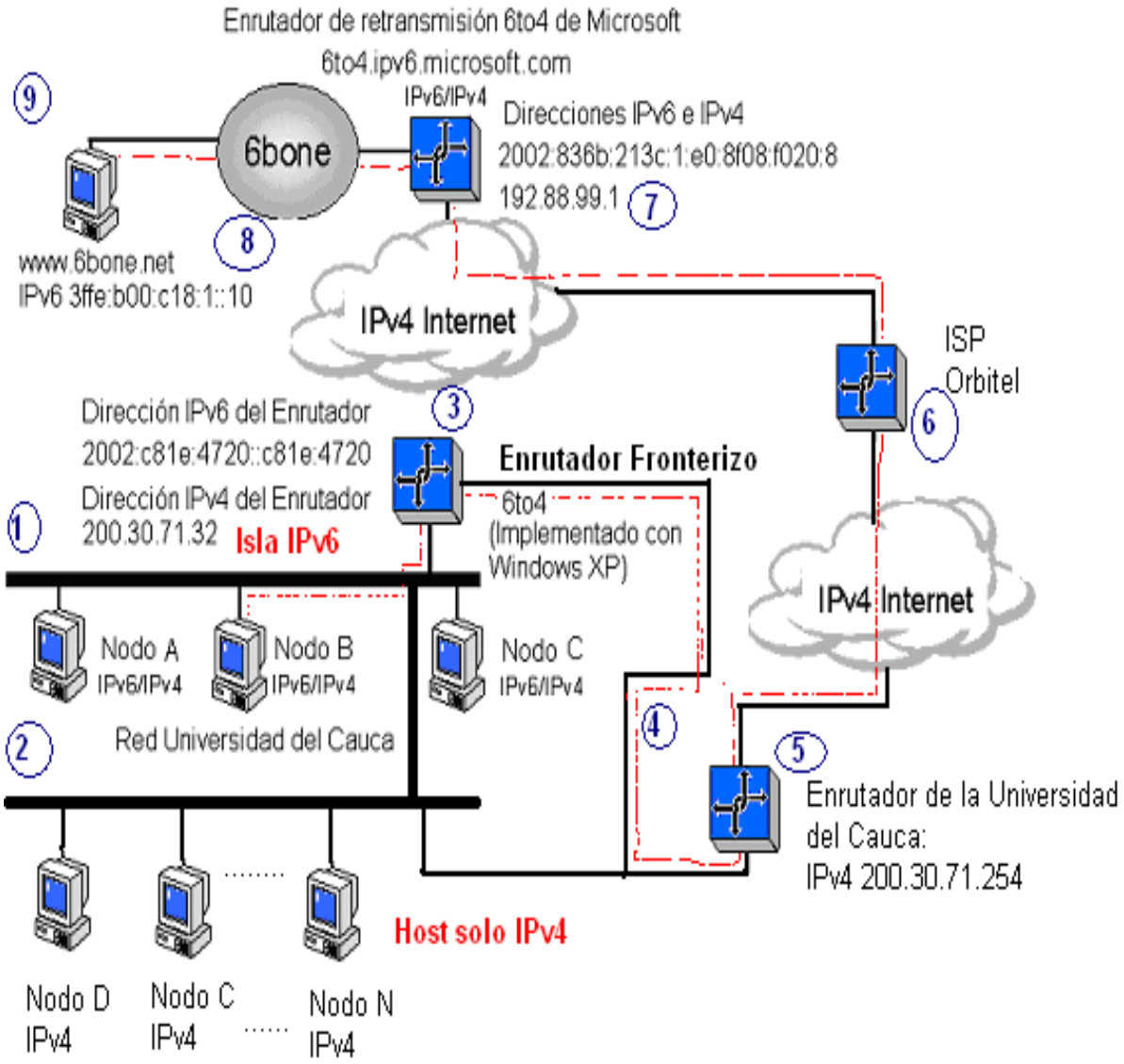


Figura 5.6 Topología de la red final de la Universidad del Cauca junto con la isla IPv6.

5.8 Conclusiones de la implementación y topología final de la Red de Datos de la Universidad del Cauca con la Isla IPv6.

La implementación llevada a cabo permite realizar un estudio más práctico de las características de IPv6 como protocolo clave en el desarrollo de las redes de próxima generación. La isla es implementada como un laboratorio de pruebas del protocolo utilizando el mecanismo de túneles 6to4 con un host corriendo el sistema operativo Windows XP Profesional al que además se le habilita la Conexión compartida a Internet (ICS) para que funcione como enrutador y así poder conectar otros equipos de la Intranet de la Universidad del Cauca al 6Bone. La arquitectura final de la red de datos de la Universidad del Cauca junto con la Isla IPv6 implementada se puede observar en la figura 5.6.

Una implementación real debería utilizar equipos especializados como por ejemplo enrutadores de la serie Cisco 3640, Cisco 2621 y Cisco 7507 que soportan el protocolo IPv6. A través de la configuración de estos equipos con la pila dual IPv6/IPv4 realizar la conexión al 6Bone a través de túneles 6to4 e ir migrando en la medida que se requiera, servidores DNS, Telnet, FTP y HTTP, así como las diferentes aplicaciones cliente servidor que se utilicen dentro de la Universidad.

Finalmente se puede concluir que el mecanismo de conexión podría no ser el mejor pero si es el que más se adecua a los recursos disponibles y a los requerimientos actuales de la Intranet de la Universidad del Cauca. Entonces se puede decir que el mecanismo seleccionado dependerá de la capacidad económica y de las características actuales de la red.

CONCLUSIONES Y RECOMENDACIONES

IPv6 no esta lejos de una cobertura total. Con más de diez años de desarrollo sólido, soporte de casi todos los nuevos proveedores de tecnologías de Internet en el mundo, y la cooperación de gobiernos y de los cuerpos gobernantes de Internet, IPv6 ya no sufre los problemas de una tecnología adolescente. Se ha convertido en un protocolo robusto y maduro que brinda revitalización e innovación al estancado y cansado Internet.

Está claro que el protocolo de hoy ya no puede soportar la voracidad continua del mundo para los servicios y aplicaciones actuales. El mundo busca perfección en las comunicaciones, mejora en la seguridad de los datos, y superior calidad en el entretenimiento, el protocolo actual de Internet empieza a mostrar su edad y cierta incapacidad para adaptarse a las nuevas tecnologías. IPv6 ofrece a los usuarios finales y a las empresas una oportunidad de evolucionar mas allá de su interacción actual, reforzando con ello el intercambio comercial.

- Con el estudio teórico de este trabajo de grado se dio a conocer y se espera robustecer el conocimiento teórico del protocolo IPv6 como soporte de las nuevas tecnologías de telecomunicaciones, dentro de la Universidad del Cauca.
- Las bases teóricas adquiridas con la realización de este trabajo de grado son suficientes para impulsar en la FIET futuros desarrollos de aplicaciones que saquen provecho de las nuevas características de IPv6 tanto en calidad de servicio, movilidad y características para el manejo de aplicaciones en tiempo real, que no se tenían en IPv4.
- Gracias a los conceptos teóricos adquiridos a través del desarrollo de este proyecto, se pudieron implementar varias prácticas en donde se pueden observar de una manera más tangible las características de IPv6.
- Fue posible la conexión con el 6bone utilizando varios mecanismos como son: túneles 6to4 y el protocolo TSP descrito en el RFC 2026.
- Se logró configurar el servidor apache para su funcionamiento con IPv6, realizando la primera página exclusiva para IPv6 de la Universidad del Cauca.
- A través de la utilización de un equipo con Windows XP configurado como enrutador 6to4, fue posible permitir que otros equipos de la red pudieran acceder al 6bone y a través de este a otros equipos con IPv6 en el mundo, estableciéndose así una isla IPv6 dentro de la red de la Universidad del Cauca.
- Con el desarrollo de las prácticas se toma confianza en la comprensión y la aplicación de los procesos de transición hacia las nuevas tecnologías, procesos que debido a la formación académica impartida son posibles de entender y de llevar acabo.
- La migración hacia las redes multiservicio basadas en el protocolo IPv6 no es capricho sino una necesidad. Con la elaboración de este trabajo de grado se da el primer paso en ese camino que culminara con la implementación de una red toda IPv6.

- Después de desarrollar las diferentes practicas, entre ellas la implementación de la primera Isla IPv6 dentro de la Universidad del Cauca se concluye que la mejor forma para iniciar la transición dentro de esta institución debido a las ventajas en cuanto costo, eficiencia y menor impacto en cuanto a compatibilidad con IPv4 es el mecanismo de túneles ya sea estos automáticos o manuales.

Para finalizar se recomienda para futuros trabajos de grado:

- La realización de una isla IPv6, utilizando sistemas operativos distintos de Windows, como por ejemplo: Linux, Unix, Solaris así como la utilización de equipos de internetworking como enrutadores que soporten el nuevo protocolo configurado con direcciones IPv6 asignadas por un proveedor de servicio (ISP IPv6).
- Desarrollo de nuevas aplicaciones cliente/servidor y la migración de software existente que trabaje en base a sockets.
- Establecer un grupo de investigación y desarrollo que se dedique al estudio y al desarrollo de IPv6 para el manejo de redes multiservicio dentro de la Universidad del Cauca.
- Realizar un estudio de integración de las dos tecnologías de más proyección para las redes corporativas como son ATM e IPv6.

GLOSARIO

ANYCAST: La dirección unicast de un grupo de interfaces pertenecientes a diferentes nodos. Un paquete que es enviado a una dirección anycast es entregado únicamente a una interfaz del grupo (el más cercano a la fuente, coherentemente con las métricas de enrutamiento).

CABECERA DE AUTENTICACION (Autentication header)**(AH):** Cabecera con la función de garantizar la autenticidad e integridad de un paquete. Esto garantiza que el paquete no ha sido modificado durante la transmisión.

CARGA ÚTIL ENCRIPTADA Y ASEGURADA (Encrypted Security Payload**) (ESP):** Técnica de encapsulación usando encriptación para garantizar que únicamente el receptor pueda leer el campo de datos.

CRC (Cyclic Redundancy Check, chequeo cíclico redundante): Cadena binaria calculada en un paquete para probar su integridad durante la fase de recepción.

DES (Data Encryption Standard, estándar de encriptación de datos): Algoritmo de encriptación utilizado para el cifrado de datos.

DES-CBC (DES Cipher Block Chaining, encadenado de cifrado de bloques DES): Uso particular del estándar DES.

DHCP (Dynamic Host Configuration Protocol, protocolo de configuración dinámica de los host): Protocolo basado en servidores, para la configuración automática de las redes (por ejemplo: direcciones y prefijos).

DIRECCION IPv4: Dirección de 32-bits asignada a la interfaz de un host o un enrutador que están dispuestos en la arquitectura de red de IPv4, escrita en formato decimal punteado.

DIRECCION IPv6: Dirección de 128-bits, asignada a las interfaces de un host o un enrutador, utilizada en la arquitectura de red IPv6, escrita como 8 dígitos hexadecimales separados por : .

DIRECCIÓN IPv6 COMPATIBLE CON IPv4: Una dirección IPv6 algoritmicamente derivada de una dirección IPv4.

DIRECCION MAC: Dirección de capa de enlace de datos, usada en LANs, con 48 bits de largo, y asignada por determinado proveedor, es escrita como seis parejas hexadecimales divididas por un carácter.

DNS: (Domain Name Server, servidor de nombres de dominio): Servicio para la traducción de nombres en direcciones y viceversa en la arquitectura de una red TCP/IP, basada en bases de datos distribuidas.

DVMRP (Distance Vector Multicast Routing Protocol): Protocolo de enrutamiento para tráfico multicast IP, basado en la filosofía de vector de distancia y utilizado en Mbone.

ETHERNET: Red local CSMA/CD, algunas veces es utilizada para una red LAN IEEE 802.3.

FTP (File Transfer Protocol, protocolo de transferencia de archivos): Protocolo de aplicación, parte del conjunto de protocolos de TCP/IP, utilizado para la transferencia de archivos entre nodos de la red.

FIREWALL: Un computador o un enrutador designado como un buffer entre cualquier conexión con la red pública y la red privada, esto con el propósito de implementar seguridad.

HOME AGENT (agente local): Es una respuesta del enrutador a los mensajes de descubrimiento de vecindario, en representación de otro nodo (por ejemplo: el caso de los nodos móviles).

HOST: En la aquitectura de una red IP, cada nodo que no es un enrutador.

ICMP (Internet Control Message Protocol, protocolo de control de mensajes en Internet): En la arquitectura de una red TCP/IP, un protocolo de capa de red utilizado para reportar errores y proveer información relevante al procesamiento de paquetes.

ICMPv6 (ICMP versión 6): Versión 6 del protocolo ICMP, para ser usado por IPv6.

IGMP (Internet Group Management Protocol, protocolo de gestión de grupos en Internet): Protocolo utilizado en IPv4 para gestión de grupos multicast. En IPv6, las funciones IGMP están incluidos en ICMPv6.

INTRANET: La red privada de una empresa basada en el modelo de Internet.

INITIALIZATION VECTOR (IV, vector de inicialización): Cadena binaria utilizada en asociación con DES-CBC para introducir un factor de facilidad en el proceso de encriptación.

IKMP (internet key management protocol, protocolo de gestión de llaves en Internet): Protocolo para la encriptación y la gestión de llaves.

IP:(Internet Protocol, protocolo de Internet): En la arquitectura de una red TCP/IP, es la capa de protocolo de datos de la red.

IPv4 (IP versión 4): El único protocolo IP utilizado hasta 1996.

IPv6 (IP versión 6): La nueva versión de IP.

LAN (Local Area Network, red de área local): Red de alta velocidad, baja taza de errores, que cubre una área geográfica relativamente pequeña (hasta unos cientos de metros). Las LAN conectan: estaciones de trabajo, componentes, terminales, y otros dispositivos en un solo edificio o zona geográfica limitada.

LINK (enlace): Un canal de comunicación, sobre el cual, los nodos pueden transmitir utilizando la capa 2 de OSI, o sea la capa de datos. Son ejemplos de esto: Ethernet, PPP, X.25, Frame Relay, y ATM, también túneles en protocolos como IPv4 o IPv6.

MAC (Medium Access Control, control de acceso al medio): La más baja de las dos subcapas de la capa enlace de datos, determina el acceso a un medio compartido, la subcapa MAC provee un control de enlace lógico con servicios no orientados a la conexión.

MOSPF (Multicast OSPF): Extensión de OSPF para manejar paquetes multicast IP.

MULTICAST: Una única dirección para un conjunto de interfaces pertenecientes a diferentes nodos. Un paquete enviado a una dirección multicast es entregado a todas las interfaces pertenecientes al conjunto.

NODE: Un dispositivo que utiliza el protocolo IP.

OFF-LINK: Una dirección IPv6 no asignada a ninguna interfaz conectada al enlace.

ON-LINK: Una dirección IPv6 asignado a una interfaz conectada a un enlace.

OSI (Open System Interconnect, interconexión de sistemas abiertos): Estándar internacional creado por la ISO para desarrollar estándares para datos que circulan por determinada red facilitando la interoperabilidad de equipos de diferentes vendedores. Contiene 7 capas: física, enlace de datos, red, transporte, sesión, presentación y aplicación. Este estándar es descrito en el documento de la ISO 7498.

OSPF (Open Shortest Path First): Protocolo de estado de enlace, que calcula tablas de enrutamiento usadas en la arquitectura de red TCP/IP.

OUT OF BAND (fuera de banda): La técnica para la distribución y encriptación de llaves fuera de los canales normalmente utilizados para la transferencia de información.

PC: Computador personal.

PROXY: Una entidad que participa con protocolos en el beneficio de otra entidad.

RDSI: (Red digital de servicios integrados): Es una evolución de la red telefónica, basada en tecnología digital, esto conlleva a que las redes telefónicas transporten además de voz datos y otras fuentes de datos desde 64 Kbps a 2 Mb/s.

RFC (Request For Comments): Series de documentos utilizados como medios primarios para comunicar información acerca de la Internet. Algunos RFCs son designados como estandares en la arquitectura de red TCP/IP.

RIP (Routing Information Protocol, protocolo de información de enrutamiento): Protocolo que calcula las tablas de enrutamiento, adecuado para redes pequeñas.

SA (Security Association, asociación segura): Acuerdo entre dos o más nodos acerca de los algoritmos de seguridad y otros parámetros utilizados en el intercambio de paquetes. Cada SA es identificado por un SPI.

SPI (Security Parameter Index): El SA ha ser usado en un intercambio de paquetes. Utilizado tanto por AH como por ESP.

SUBRED: Una subred de nodos identificada por direcciones con un prefijo común el cual corresponde a un segmento de red física independiente.

TCP (Transmission Control Protocol, protocolo de control de transmisión): En la arquitectura de una red TCP/IP, es una conexión orientada a la capa de protocolo de transporte que provee una transmisión de datos de manera confiable, full-duplex. TCP es parte del conjunto TCP/IP.

TCP/IP (Transmission Control Protocol/Internet Protocol, protocolo de control de transmisión/protocolo de Internet): La arquitectura de red desarrollada en los años 70 para el apoyo en la construcción de redes mundiales, mejor conocida como Internet, prácticamente se a convertido en un estándar por defecto.

TELNET: En la arquitectura de red TCP/IP, es un protocolo estándar de emulación, utilizado para la conexión remota de un terminal, permitiendo a los usuarios entrar en sistemas remotos y usar recursos como si estuvieran conectados al sistema local.

UNICAST: La dirección de una sola interfaz. Un paquete enviado a una dirección unicast es entregado únicamente a la interfaz identificada por esa dirección.

VPN (Virtual Private Network, red privada virtual): Frecuentemente implementada por medio de túneles en IP.

WWW (World Wide Web): Servicio utilizado para proveer información con la técnica de hipertexto en la Internet.

BIBLIOGRAFÍA

Referencias Electrónicas.

Direcciones IPv4.

- Foro IPv6.
  www.ipv6forum.com
- IPv6 News & Links.
  http://www.hs247.com/
- 6Bone.
  http://www.6bone.net
- Ethereal.
  http://www.ethereal.com/
- MSDN Online – Technology Preview.
  http://msdn.microsoft.com/downloads/sdks/platform/tpipv6/start.asp
- Microsoft.
  http://www.research.microsoft.com/research/os/
- Apache 2.0.44 (2003/01/26)
  http://www.apache.com
- httpd-2.0.44-win32-ipv6.zip: IPv6 enabled Apache 2.0.44.
  http://win6.jp/Apache2/index.html
- Freenet6, Conectividad Ipv6 gratis.
  http://www.freenet6.net
- Configuring 6to4 Connectivity with MSR IPv6.
  http://research.microsoft.com/msripv6/docs/6to4.htm
- IETF, The Internet Engineering Task Force Home Page.
  http://www.ietf.org/
- 6WIND.
  http://www.6wind.com/
- RFC's.
  http://www.ietf.org/rfc.html
- IPv6.org.
  http://www.ipv6.org/
- Cisco Systems.
  http://www.cisco.com/ipv6
- IPv6 Mexico.
  http://www.ipv6.unam.mx/
- Proyecto IPv6 en la RAU.
  http://www.rau.edu.uy/ipv6/
- Google.
  http://www.google.com/IPv6

Direcciones IPv6.

- Foro IPv6.
  http://www.ipv6forum.com
- 6Bone.
  http://www.6bone.net
- 6Wind.
  http://www.ipv6.6wind.com/

Referencias Impresas.

- Silvano Gai. “Internetworking IPv6 with Cisco Routers”.
  McGraw-Hill Computer Communications Series, 1998.
- Mark A. Millar, P.E. “Implementing IPV6: Supporting the Next Generation Internet Protocols” Second Edition.
  The M&T IP Library,

RFC’s.

[RFC 1719] A Direction for IPng.

[RFC 1726] Technical Criteria for Choosing IP The Next Generation (IPng).

[RFC 1752] The Recommendation for the IP Next Generation Protocol.

[RFC 1809] Using the Flow Label Field in IPv6.

[RFC 1881] IPv6 Address Allocation Management.

[RFC 1887] An Architecture for IPv6 Unicast Address Allocation.

[RFC 1888] OSI NSAPs and IPv6.

[RFC 1981] Path MTU Discovery for IP version 6.

[RFC 2126] ISO Transport Service on top of TCP (ITOT).

[RFC 2170] Application REQuested IP over ATM (AREQUIPA).

[RFC 2185] Routing Aspects Of IPv6 Transition.

[RFC 2292] Advanced Sockets API for IPv6.

[RFC 2373] IP Version 6 Addressing Architecture.

- Obsoleto: RFC 1884.

[RFC 2374] An IPv6 Aggregatable Global Unicast Address Format.

- Obsoleto: RFC 2073.

[RFC 2375] IPv6 Multicast Address Assignments.

[RFC 2401] Security Architecture for the Internet Protocol.

[RFC 2450] Proposed TLA and NLA Assignment Rules.

[RFC 2452] IP Version 6 Management Information Base for the Transmission Control Protocol.

[RFC 2454] IP Version 6 Management Information Base for the User Datagram Protocol.

[RFC 2460] Internet Protocol, Version 6 (IPv6) Specification.

- Obsoleto: RFC 1883.

[RFC 2461] Neighbor Discovery for IP Version 6 (IPv6).

- Obsoleto: RFC 1970.

[RFC 2462] IPv6 Stateless Address Autoconfiguration.

- Obsoleto: RFC 1971.

[RFC 2464] Transmission of IPv6 Packets over Ethernet Networks.

- Obsoleto: RFC 1972.

[RFC 2465] Management Information Base for IP Version 6: Textual Conventions and General Group.

[RFC 2467] Transmission of IPv6 Packets over FDDI Networks.

- Obsoleto: RFC 2019.

[RFC 2470] Transmission of IPv6 Packets over Token Ring Networks.

[RFC 2471] IPv6 Testing Address Allocation.

- Obsoleto: RFC 1897.

[RFC 2472] IP Version 6 over PPP.

- Obsoleto: RFC 2023.

[RFC 2473] Generic Packet Tunneling in IPv6 Specification.

[RFC 2474] Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers.

[RFC 2475] An Architecture for Differentiated Services.

[RFC 2491] IPv6 over Non-Broadcast Multiple Access (NBMA) networks.

[RFC 2492] IPv6 over ATM Networks.

[RFC 2497] Transmission of IPv6 Packets over ARCnet Networks.

[RFC 2507] IP Header Compression.

[RFC 2508] Compressing IP/UDP/RTP Headers for Low-Speed Serial Links.

[RFC 2526] Reserved IPv6 Subnet Anycast Addresses.

[RFC 2529] Transmission of IPv6 over IPv4 Domains without Explicit Tunnels.

[RFC 2553] Basic Socket Interface Extensions for IPv6.

- Obsoletos: RFC 2133.

[RFC 2590] Transmission of IPv6 Packets over Frame Relay Networks Specification.

[RFC 2675] IPv6 Jumbograms.

- Obsoleto: RFC 2147.

[RFC 2711] IPv6 Router Alert Option.

[RFC 2732] Format for Literal IPv6 Addresses in URL's.

[RFC 2765] Stateless IP/ICMP Translation Algorithm (SIIT).

[RFC 2766] Network Address Translation - Protocol Translation (NAT-PT).

[RFC 2767] Dual Stack Hosts using the "Bump-In-the-Stack" Technique (BIS).

[RFC 2780] IANA Allocation Guidelines For Values In the Internet Protocol and Related Headers.

[RFC 2874] DNS Extensions to Support IPv6 Address Aggregation and Renumbering.

[RFC 2893] Transition Mechanisms for IPv6 Hosts and Routers.

- Obsoleto: RFC 1933.

[RFC 2928] Initial IPv6 Sub-TLA ID Assignments.

[RFC 3041] Privacy Extensions for Stateless Address Autoconfiguration in IPv6.

[RFC 3053] IPv6 Tunnel Broker.

[RFC 3056] Connection of IPv6 Domains via IPv4 Clouds.

[RFC 3111] Service Location Protocol Modifications for IPv6.

[RFC 3142] An IPv6-to-IPv4 Transport Relay Translator.

[RFC 3146] Transmission of IPv6 Packets over IEEE 1394 Networks.

[RFC 3178] IPv6 Multihoming Support at Site Exit Routers.

[RFC 3306] Unicast-Prefix-based IPv6 Multicast Addresses.

[RFC 3307] Allocation Guidelines for IPv6 Multicast Addresses.

[RFC 3314] Recommendations for IPv6 in Third Generation Partnership Project (3GPP) Standards.

[RFC 3484] Default Address Selection for Internet Protocol version 6 (IPv6).

RFC's obsoletos:

[RFC 1883] Internet Protocol, Version 6 (IPv6) Specification.

[RFC 1884] IP Version 6 Addressing Architecture.

[RFC 1897] IPv6 Testing Address Allocation.

[RFC 1933] Transition Mechanisms for IPv6 Hosts and Routers.

[RFC 1970] Neighbor Discovery for IP Version 6 (IPv6).

[RFC 1971] IPv6 Stateless Address Autoconfiguration.

[RFC 1972] A Method for the Transmission of IPv6 Packets over Ethernet Networks.

[RFC 2019] A Method for the Transmission of IPv6 Packets over FDDI Networks.

[RFC 2023] IP Version 6 over PPP.

[RFC 2073] An IPv6 Provider-Based Unicast Address Format.

[RFC 2133] Basic Socket Interface Extensions for IPv6.

[RFC 2147] TCP and UDP over IPv6 Jumbograms.