POTENCIALIDAD DEL PROTOCOLO DE INTERCONEXIÓN DE REDES IP VERSIÓN 6

RUBÉN DARÍO GARCÍA ANAYA
WILMER FABIÁN BARROS GONZÁLEZ

UNIVERSIDAD TECNOLÓGICA DE BOLÍVAR
FACULTAD DE INGENIERÍA DE SISTEMAS
CARTAGENA DE INDIAS D. T. y C.
2004

POTENCIALIDAD DEL PROTOCOLO DE INTERCONEXIÓN DE REDES IP VERSIÓN 6

RUBÉN DARÍO GARCÍA ANAYA
WILMER FABIÁN BARROS GONZÁLEZ

Monografía presentada como requisito parcial para aprobar el Minor en Comunicaciones y Redes

ISAAC ZÚÑIGA SILGADO
Ingeniero de Sistemas
DIRECTOR

UNIVERSIDAD TECNOLÓGICA DE BOLÍVAR
FACULTAD DE INGENIERÍA DE SISTEMAS
CARTAGENA DE INDIAS D. T. y C.
2004

Cartagena de Indias D. T. y C., Noviembre de 2004

Señores:
COMITÉ DE EVALUACIÓN DE PROYECTOS
Universidad Tecnológica de Bolívar
LC.

Respetados Señores:

Con toda atención, nos dirigimos a ustedes, con el fin de presentar a su consideración, estudio y aprobación, el trabajo titulado **"POTENCIALIDAD DEL PROTOCOLO DE INTERCONEXIÓN DE REDES IP VERSIÓN 6"**, como requisito parcial para aprobar el Minor en Comunicaciones y Redes.

Atentamente,

RUBÉN D. GARCÍA ANAYA	**WILMER F. BARROS GONZÁLEZ**
CC. 92.191.148 de San Pedro Sucre	**CC. 9.145.171 de Cartagena de Indias**

AUTORIZACIÓN

Cartagena de Indias D. T. y C., Noviembre 16 de 2004

Yo, **RUBÉN DARÍO GARCÍA ANAYA**, identificado con número de cédula **CC # 92.191.148** de **San Pedro Sucre**, Autorizo a la **UNIVERSIDAD TECNOLÓGICA DE BOLÍVAR** para hacer uso del Trabajo de Grado Titulado **"POTENCIALIDAD DEL PROTOCOLO DE INTERCONEXIÓN DE REDES IP VERSIÓN 6"** y Publicarlo en el Catálogo Online de la Biblioteca.

_____

RUBÉN GARCÍA ANAYA
CC. 92.191.148 de San Pedro Sucre

AUTORIZACIÓN

Cartagena de Indias D. T. y C., Noviembre 16 de 2004

Yo, **WILMER FABIÁN BARROS GONZÁLEZ**, identificado con número de cédula **CC # 9.145.171** de **Cartagena de Indias**, Autorizo a la **UNIVERSIDAD TECNOLÓGICA DE BOLÍVAR** para hacer uso del Trabajo de Grado Titulado **"POTENCIALIDAD DEL PROTOCOLO DE INTERCONEXIÓN DE REDES IP VERSIÓN 6"** y Publicarlo en el Catálogo Online de la Biblioteca.

_____

WILMER BARROS GONZÁLEZ
CC. 9.145.171 de Cartagena de Indias

Cartagena de Indias D. T. y C., Noviembre de 2004

Señores:

UNIVERSIDAD TECNOLÓGICA DE BOLÍVAR.

Comité de Evaluación de Proyectos.

Escuela de Ingenierías.

Ciudad.

Estimados Señores:

Con el mayor agrado me dirijo a ustedes para poner a consideración el trabajo final titulado **"POTENCIALIDAD DEL PROTOCOLO DE INTERCONEXIÓN DE REDES IP VERSIÓN 6",** el cual fue llevado a cabo por los estudiantes RUBÉN DARÍO GARCÍA ANAYA y WILMER FABIAN BARROS GONZALEZ, bajo mi orientación como Asesor.

Agradeciendo su amable atención,

Cordialmente,

_____

ISAAC ZÚÑIGA SILGADO

Ingeniero de Sistemas

ARTÍCULO 107

La UNIVERSIDAD TECNOLÓGICA DE BOLÍVAR se reserva el derecho de propiedad intelectual de todos los trabajos de grado aprobados, y no pueden ser explotados sin la correspondiente autorización.

Nota de Aceptación

_____

_____

_____

_____

Presidente del Jurado

_____

Jurado

_____

Jurado

Cartagena de Indias D. T. y C., Noviembre de 2004

Dedico Esta Obra

A Dios

Por darme la vida, la fortaleza, y la oportunidad de alcanzar mis metas.

A mis Padres

Quienes con su amor y cariño me apoyaron en todos los momentos.

A novia Dina Luz Miranda

Por quererme y aguantarme en esos días que no pude estar con ella.

A mi familia y amigos

Que siempre han compartido y estado conmigo.

Rubén Darío García Anaya

Dedico Esta Obra

A Dios

Quien con su infinita misericordia me acogió en sus brazos no dejándome desfallecer.

A mis padres

Como fruto de su esfuerzo y desvelo.

A Enith

Al final de este camino fuiste la luz.

Solo espero que comprendan que el tiempo que les negué fue para lograr este triunfo

Wilmer Fabián Barros González

Agradecimientos

A Eduardo Gómez Vásquez

Por su valiosa orientación en la selección del tema de monografía

A Isaac Zúñiga Silgado

Por su asesoría y orientación

A Giovanni Vásquez

Por su justa evaluación

A Todos los docentes, quienes hicieron posible nuestro crecimiento personal y apoyaron nuestra formación profesional

...y a todas aquellas personas que de alguna forma aportaron para que este gran sueño se hiciera realidad.

CONTENIDO

2.2.1.8 REPRESENTACIÓN DE LOS TIPOS DE DIRECCIONES

2.2.1.8.1 Direcciones Unicast

2.2.1.8.2 Direcciones Anycast

2.2.1.8.3 Direcciones Multicast

2.2.1.9 DIRECCIONES REQUERIDAS PARA CUALQUIER NODO

2.2.1.10 FORMATO PARA LA REPRESENTACIÓN EN URL'S

2.2.2 ICMP Y LOS MENSAJES DE ERROR

2.2.3 AUTOCONFIGURACION

2.2.3.1 Autoconfiguración Stateless (sin intervención o descubrimiento automático)

2.2.3.2 Autoconfiguración Stateful (predeterminada)

2.2.4 EXTENSIONES DE SEGURIDAD IPSec

2.2.4.1 La seguridad en el protocolo IP

2.2.4.2 Las especificaciones IPsec

2.2.4.2.1 La cabecera de autenticación (ah)

2.2.4.2.2 La cabecera de cifrado de seguridad (esp)

2.2.4.2.3 El protocolo ISAKMP

2.2.4.2.4 El protocolo IKE

2.2.5 CALIDAD DE SERVICIO QoS

2.2.5.1 Arquitecturas de QoS

2.2.5.2 Protocolo de reserva de recursos (RSVP)

2.2.5.3 Protocolos de servicios diferenciados (Diffserv)

2.2.5.4 Soporte de QoS en IPv6

2.2.6 MOVILIDAD

2.2.6.1 Operación

2.2.6.2 Cabeceras adicionales

2.2.6.3 Condiciones de seguridad

2.2.7 MECANISMOS DE MIGRACION DE IPv4 e IPv6

2.2.7.1 Doble pila (Dual Stack)

2.2.7.2 Técnicas basadas en túneles

2.2.7.2.1 Túneles manuales

2.2.7.2.1.1 Túnel Broker

2.2.7.2.1.2 Túnel Server

2.2.7.2.2 Túneles automáticos

2.2.7.2.3 6to4

2.2.7.2.4 6over4

2.2.7.3 Técnicas basadas en traductores

2.2.7.3.1 Stateless IP/ICMP Traslation Algorithm (SIIT)

2.2.7.3.1.1 Traducción de IPv4 a IPv6

2.2.7.3.1.2 Traducción de IPv6 a IPv4

2.2.7.3.1.3 Implicaciones para IPv6

2.2.7.3.2 Network address Traslation-Protocol Traslation (NAT-PT)

2.2.7.3.3 Bump in the Stack (BIS)

2.2.7.3.4 Socks v5

2.3 VENTAJAS E INCONVENIENTES

3. IPv4 VERSUS IPv6

3.1 DIFERENCIAS EN LAS CABECERAS

3.2 CABECERA IPv6

3.2.1 Campos de cabeceras

3.2.2 Campo clase de tráfico

3.2.3 Campo etiqueta de flujo

3.3 CABECERA DE EXTENSION

3.3.1 Cabecera de opciones de salto a salto

3.3.2 Cabecera de encaminamiento

3.3.3 Cabecera de fragmentación

3.3.4 Cabecera de autenticación

3.3.5 Cabecera de encriptación de la carga de seguridad

3.3.6 Cabecera de las opciones para el destino

3.4 DIFERENCIAS EN EL DIRECCIONAMIENTO CON IPv4

3.5 COMPARACIÓN DE LAS CARACTERISTICAS DE IPv4-IPv6

4. SITUACION DE IPv6

4.1 SITUACÍON DE LA DEFINICIÓN DEL PROTOCOLO

4.2 PROBLEMAS DE NORMALIZACIÓN

4.3 COMPETIDORES DE IPv6

4.4 USUARIOS ACTUALES Y FUTUROS

4.5 LUGARES DE PRUEBA E HISTORIAS EXITOSAS

4.6 SITUACIÓN DEL DESPLIEGUE

4.7 ESTADO ACTUAL A LO LARGO DEL MUNDO

4.8 REDES EXPERIMENTALES

4.8.1 6Bone

4.8.2 6Ren

4.8.3 6Tap

4.8.4 IPv6 forum

4.9 ESTADO ACTUAL EN LATINOAMERICA

4.9.1 Red mexicana

4.9.2 Red chilena

CONCLUSIONES

BIBLIOGRAFÍA

ANEXOS

LISTA DE FIGURAS Y TABLAS

pág

GLOSARIO

ACK, acknowledgement (reconocimiento): Carácter de control utilizado en las comunicaciones síncronas binarias. Protocolo para indicar que el bloque de transmisión previo se recibió correctamente y que el receptor está listo para el siguiente bloque.

ARP, address resolution protocol: (protocolo de resolución de dirección): Protocolo de red que permite a un host descubrir la dirección en hardware de un nodo con su dirección IP.

Broadcast (radiodifusión): Método de transmisión utilizado en topologías de red de bus, que envían mensajes a todas las estaciones aún cuando los mensajes sean direccionados a una estación específica.

Cabecera (Header): Información que suele situarse delante de los datos (por ejemplo en una transmisión) y que hace referencia a diferentes aspectos de estos (longitud...).

CRC, cyclic redundant check (revisión de ciclo redundante): Esquema de detección de errores en el cual se genera un carácter de revisión de bloque y se envía sobre el enlace. El CRC se recalcula en el extremo receptor y después se compara con el CRC recibido; si no son iguales el bloque recibido se desecha.

DARPA: Agencia de Proyectos de Investigación Avanzada de la Defensa, (Defense Advanced Research Projects Agency).

Datagrama: Conjunto de estructurado de bytes que forma la unidad básica de comunicación del protocolo IP (en todas sus versiones).

DHCP, Dynamic Host Configuration Protocol: Protocolo de configuración dinámica de host,

DNS, Domain Name System: Sistema de dominio de nombres, sistema utilizado en Internet para controlar los nombres, que convierten direcciones IP en direcciones de dominios.

Encaminamiento (Routing): Procedimiento que consiste en conducir un datagrama hacia su destino a través de INTERNET.

Encapsulamiento: Sistema basado en colocar una estructura dentro de otra formando capas.

Encryption (encriptación): Procedimiento para codificar información de manera que pueda transmitirse son peligro de ser interceptada o alterada antes de que llegue a su destinatario.

Firewall (Cortafuegos): Mecanismo utilizado para proteger una red o computadora conectada a Internet de accesos no autorizados. Un firewall puede construirse con software, con hardware o con una combinación de ambos.

FTP, file transfer protocol (protocolo de transferencia de archivos): Protocolo de compartimiento de archivos que opera en las capas 5 a la 7 del modelo OSI. Permite la transferencia de archivos entre computadoras en una red.

FQND, Fully Qualified Domain Name (FQDN): Nombre de Dominio Totalmente Cualificado. El FQDN es el nombre completo de un sistema y no sólo el nombre del sistema. Por ejemplo, Utb es un nombre de sistema y Utb.edu.co es un FQDN.

Gateway: Equipo que provee interconexión entre dos redes con protocolos de comunicación diferentes; dos ejemplos son los ensambladores/desensambladores de paquetes y conversores de protocolos. Los gateway operan en las capas 4 a la 7 del modelo OSI. Contrasta con puente, enrutador y repetidor.

ICMP (Internet Control Message Protocol): Protocolo encargado de la comunicación de mensajes entre nodos conectados a INTERNET.

IETF, Internet Engineering Task Force (Fuerza de trabajo de Ingeniería en Internet): Organismo encargado de proponer y establecer los estándares en Internet.

INTERNIC, (Internet Network Information Center): Organismo encargado de asignar las direcciones **IP**. Sólo asigna la porción netid para que éstas sean únicas.

IP (INTERNET PROTOCOL): Protocolo no fiable y sin conexión en el que se basa la comunicación por INTERNET. Su unidad es el datagrama.

IPng (IP Next Generation): Abreviatura escogida en IETF, con la que también se denomina la versión 6 del protocolo IP.

IPv6 (IP versión 6): Abreviatura escogida en IETF, con la que se denomina la versión 6 del protocolo IP.

Kernel: Conjunto de servicios básicos que debe ofrecer un sistema operativo para poder funcionar.

LAN (Local Area Network): Red de datos para dar servicio a un área geográfica pequeña, un edificio por ejemplo.

MAC Address: Dirección única que llevan las tarjetas de red grabadas en una ROM para identificarse y diferenciarse de las demás.

MTU (Maximun Transfer Unit): Siglas que denominan el tamaño máximo en unidades de transmisión que se permite en un canal de comunicación.

Multicast (multiemisión): Mensaje enviado por un host a los dispositivos en la red. Generalmente enviado en intervalos específicos para evitar trastornos en la red; en multicast se tiene el nombre del host emisor al igual que la información acerca de los servicios que provee.

NAT, Network Address Traslation: Traducción de direcciones de red, es una tecnología usada ampliamente en la actualidad para permitir el acceso a Internet de varias computadoras a través de una sola conexión y dirección IP externa.

Node (nodo): Punto de interconexión en una red que sirve como punto de terminación para dos o más enlaces.

NTS, (Servidores de Tiempo): suministran el tiempo preciso directamente a la red LAN (WAN). Pueden al mismo tiempo sincronizar el tiempo de todos los servidores, terminales de trabajo y routers que trabajen en la red TCP/IP bajo el control del protocolo NTP.

OSI (Modelo): Modelo teórico propuesto por IEEE que describe cómo deberían conectarse distintos modelos de ordenadores a diferentes tipos de red para poder comunicarse entre sí.

Overhead: Pérdida de rendimiento.

Paquetes: Ver datagrama.

PDU, Unidad de Datos de Protocolo: conjunto de datos especificado en un protocolo de una capa dada y que consta de información de control del protocolo de esa capa, y posiblemente de datos del usuario de esa capa.

Protocolos: Conjunto de reglas que establece cómo debe realizarse una comunicación.

Proxy: Una substitución de direcciones, usado para limitar la información de direcciones disponibles externamente.

QoS, Quality of Service: Calidad de Servicio, conjunto de parámetros y sus valores que determinan las prestaciones de un circuito, red o servicio.

Red: Dispositivo físico que conecta dos o más ordenadores.

RFC (Request For Comments): Documento de especificaciones que se expone públicamente para su discusión.

Router: Dispositivo físico u ordenador que conecta dos o más redes encargado de direccionar los distintos datagramas que le lleguen hacia su destino.

SSL: Secure Sockets Layer. Capa de Socket Segura. Protocolo que ofrece funciones de seguridad a nivel de la capa de transporte para TCP.

Socket: Tupla compuesta por una dirección IP y un número de port.

TCP (Transmission Control Protocol): Protocolo de nivel superior que permite una conexión fiable y orientada a conexión mediante el protocolo IP.

TTL, Time To Live: Tiempo de vida.

Tunneling: Ver encapsulamiento.

Throughput (caudal eficaz).- Indicador de la capacidad de manejo de datos. Mide que tantos datos son procesados como salida de una computadora, dispositivo, enlace, red o sistema.

UDP (User Datagram Protocol): Protocolo no fiable y sin conexión basado en el protocolo IP.

URL, Uniform Resource Locator. Localizador Uniforme de recursos. Sistema de direccionamiento estándar para archivos y funciones de Internet, especialmente en el Word Wide Web. El url esta conformado por el servicio, más el nombre de la computadora, más el directorio y el archivo referido.

VoIP, Voice over IP: Voz sobre IP, término utilizado en la telefonía IP para un conjunto de facilidades para administrar la dotación de voz utilizando el Protocolo Internet (IP).

WAN (Wide Area Network): Red de gran alcance. Este tipo de red suele utilizarse en la unión de redes locales (LAN).

WAP, Wireless Application Protocol: Protocolo de aplicaciones inalámbricas.

RESUMEN

TITULO DE LA MONGRAFÍA

POTENCIALIDAD DEL PROTOCOLO DE INTERCONEXIÓN DE REDES IP VERSIÓN 6

OBJETIVO GENERAL

Introducir al conocimiento de la nueva generación del protocolo IP, haciendo una descripción de la potencialidad que este ofrece a las comunicaciones de hoy en día.

OBJETIVOS ESPECÍFICOS

- Dar a conocer las diferencias entre los protocolos IP versión 4 e IP versión 6 con una comparación minuciosa de cada uno.
- Identificar las principales y las nuevas características que presenta el protocolo IP versión 6 haciendo una descripción detallada.
- Establecer las ventajas y desventajas que abarca esta nueva generación de protocolo IP.
- Dar a conocer el soporte de calidad de servicio (QoS) que ofrece este nuevo protocolo.
- Mostrar los mecanismos de migración de IP versión 4 a IP versión 6 haciendo una descripción de estos.
- Conocer la situación actual de IP versión 6 en el mundo y en Latinoamérica.

BREVE DESCRIPCIÓN DEL PROBLEMA

La Internet de hoy en día, con su protocolo IPv4, fue diseñada para transportar aplicaciones tolerantes al tiempo, donde el tiempo de envío y respuesta no es un problema importante, ejemplos son el Mail, Ftp, Http, Telnet, entre otros.

La visión primaria de dotar de inteligencia a los host extremos en lugar de dotar a los routers de la red con la mínima capacidad de procesamiento, se ha convertido en una visión inadecuada.

Con el surgimiento de nuevas aplicaciones en tiempo real, con la convergencia de aplicaciones de Voz (VoIP), video y datos basado en una infraestructura sobre IP, con la tendencia de aumento de movilidad de los usuarios de las redes entre otros procesos o factores, la actual Internet está empezando hacer obsoleta por no garantizar la calidad de servicio (QoS) adecuada y por no asegurar un espacio de direcciones suficiente.

IPv6 (Internet Protocol version 6), aunque es también conocido comúnmente como IPng (Internet Protocol Next Generation), es el mas reciente desarrollo del protocolo IP; cuyas especificaciones han sido diseñadas por la Fuerza de Tareas de Ingeniería para Internet (IETF).

El protocolo IP es el mecanismo fundamental que se utiliza para desarrollar las comunicaciones en Internet. IPv6 es consecuente con las tecnologías desarrolladas en base al protocolo IPv4, de modo tal que incorpora dichas facilidades (reelaboradas según una nueva filosofía), y direcciona efectivamente las limitaciones nativas del protocolo IPv4.

El IPv6 posibilita e impulsa la construcción de los nuevos servicios y aplicaciones necesarias para satisfacer las demandas presentes y futuras de las redes TCP/IP avanzadas y de Internet.

Viendo la importancia de este tema, esta investigación pretende dar solución a la falta de información y documentación, la cual no existe ninguna en nuestra universidad.

INTRODUCCIÓN

Internet como la conocemos actualmente, está basada en un protocolo que tiene más de 20 años de antigüedad. Este protocolo (IPv4) suplía sin problemas las necesidades que en ese momento existían y ha sido así hasta ahora. Sin embargo, en el momento de su diseño no se previó el crecimiento exagerado que Internet iba a tener en las dos últimas décadas. Este crecimiento desmesurado ha hecho resaltar una de las principales debilidades de diseño del protocolo IPv4: el tamaño del espacio de direcciones es demasiado pequeño y no está en capacidad de suplir la gran demanda que Internet hoy exige.

El número de direcciones IP se está agotando, existen sólo 2^{32} posibles direcciones (pues el tamaño de una dirección es de 32 bits agrupados en 4 grupos de 8 bits), es decir, son **4.294.967.296** direcciones, y podría llegar el momento en que se acaben e Internet por así decirlo colapse al no poder crecer más. El real problema se encuentra es en la asignación de direcciones, a pesar de la implementación de estrategias de direccionamiento como CIDR (encaminamiento entre dominios sin clase) el espacio de direcciones estaba siendo desperdiciado.

Adicional a esto, había una necesidad de extender la funcionalidad de la capa de red con características como QoS, encriptación punto a punto, enrutamiento de origen y autenticación, entre otras, y aparte de esto surgieron otros problemas como:

- Lentitud debido a protocolos de enrutamiento ineficientes, que además hacen que las tablas de enrutamiento sean de gran tamaño y muy difíciles de mantener.
- Falta de seguridad, la imposibilidad de prestar servicios de autenticación, integridad y confidencialidad por sí mismo, sino a través de extensiones al protocolo como lo es IPSec.
- No poder distinguir entre diferentes clases de tráfico para darles un tratamiento especial (QoS).
- El formato de los encabezados es muy grande y complejo.

Por todas estas razones, la **IETF** (**Internet Engineering Task Force**) se ha puesto en la tarea de diseñar una nueva versión de este protocolo (**Versión 6**) que corrija todos los problemas que la versión actual presenta.

Las carencias fundamentales que plantea IPv4 y que podrán ser solucionadas con la nueva versión son las siguientes:

- **Escala**: Cada máquina presente en la red dispone de una dirección IP de 32 bits. Ello supone 4.294.967.296 de máquinas diferentes. Esta cifra, no obstante, es muy engañosa. El número asignado a un ordenador no es arbitrario, sino que depende de una estructura más o menos jerárquica (generalmente, pertenece a una red), lo cual ocasiona que se desperdicie una enorme cantidad de direcciones.

- **Enrutado**: Otro de los grandes problemas del crecimiento de Internet es la capacidad de almacenamiento necesaria en los Routers y el tráfico de gestión preciso para mantener sus tablas de encaminamiento. Existe un límite tecnológico al número de rutas que un nodo puede manejar, y como Internet crece de forma mucho más rápida que la tecnología que la mantiene, se intuye que pronto los Routers alcanzarán su capacidad máxima y empezarán a desechar rutas, con lo que la red comenzará a fragmentarse en subredes sin acceso entre sí.

- **Multiprotocolo**: Cada vez resulta más necesaria la convivencia de diversas familias de protocolos: IP, IPX, OSI. Para comodidad del usuario, se necesitan mecanismos que permitan abstraerle de la tecnología subyacente, de manera que concentre su atención en los aspectos realmente importantes de su trabajo. Se tiende, pues, hacia una red orientada a aplicaciones, más que a una red orientada a protocolos como hasta el momento.

- **Seguridad**: Con la aparición de servicios comerciales y la conexión de numerosas empresas, el enorme incremento en el número de usuarios por todo el planeta y la cantidad de sistemas que necesitan de Internet para su correcto funcionamiento, es

urgente definir unos mecanismos de seguridad para la red. Son necesarios esquemas de autenticación y privacidad, tanto para proteger a los usuarios en sí, como la misma integridad de la red ante ataques malintencionados o errores.

- **Tiempo real**: **IPv4** define una red pura orientada a datagramas y, como tal, no existe el concepto de reserva de recursos. Cada datagrama debe competir con los demás y el tiempo de tránsito en la red es muy variable y sujeto a congestión. Por ello, se necesita una extensión que posibilite el envío de tráfico de tiempo real, y así poder hacer frente a las nuevas demandas en este campo.

- **Tarificación**: Con una red cada día más orientada hacia el mundo comercial, hace falta dotar al sistema de mecanismos que posibiliten el análisis detallado del tráfico, tanto por motivos de facturación, como para poder dimensionar los recursos de forma apropiada.

- **Comunicaciones Móviles**: El campo de las comunicaciones móviles está en auge, y aún lo estará más en un futuro inmediato. Se necesita una nueva arquitectura con mayor flexibilidad topológica, capaz de afrontar el reto que supone la movilidad de sus usuarios. La seguridad de las comunicaciones en este tipo de sistemas se ve además, especialmente comprometida.

Una de las soluciones iniciales al problema de direccionamiento en IPv4 fue conocido como SIPP (Simple IP Plus), donde simplemente se aumentaba el tamaño de las direcciones IP a 64bits y se mejoraban ciertos aspectos de IPv4, como lo eran mejores estrategias de enrutamiento. SIPP era lo más cercano a lo que la Internet necesitaría después de unas modificaciones. Las direcciones pasaron de 64bits a 128 y se le asignó el nombre de IPv6 (IPv5 ya había sido asignado a otro protocolo, conocido como ST-2, que servia para soporte nativo de ATM en Internet).

Las principales características nuevas que aporta el IPv6 frente al IPv4 son:

- **Aumento de las capacidades de direccionamiento**: IPv6 incrementa el tamaño de dirección IP de 32 bits a 128 bits, para dar soporte a más niveles de direccionamiento jerárquico. Estos 128 bits suponen 2^{128}, **3,40282366920938463463374607431768e+38** direcciones con lo que incluso cada grano de arena del planeta podría tener su propia dirección IP.

- **Soporte mejorado para las Extensiones y Opciones**: Los cambios en la manera en que se codifican las opciones de la cabecera IP permiten un reenvío más eficiente, límites menos rigurosos y mayor flexibilidad para introducir nuevas opciones en el futuro.

- **Capacidad de Etiquetado de Flujo**: Se agrega una nueva capacidad para permitir el etiquetado de paquetes que pertenecen a "flujos" de tráfico particulares, para lo cuál, el remitente solicita tratamiento especial, como la calidad de servicio (QoS) no estándar o el servicio en "tiempo real".

- **Capacidades de Autenticación y Privacidad**: En IPv6 se especifican extensiones para utilizar autenticación, integridad de los datos, y confidencialidad de los datos.

- **Autoconfiguración "plug and play", sin necesidad de servidores, y facilidades de reconfiguración**: Los dispositivos pueden configurar sus propias direcciones IPv6 basándose en la información que reciban del router de la red.

- **Mecanismos de movilidad más eficientes y robustos**: Mobile IP soporta dispositivos móviles que cambian dinámicamente sus puntos de acceso a la red, y concretamente Mobile IPv6 permite a un host IPv6 dejar su subred de origen mientras mantiene transparentemente todas sus conexiones presentes y sigue siendo alcanzable por el resto de Internet. Esta característica será de gran importancia cuando entren en funcionamiento las nuevas redes de telefonía con tecnología UMTS.

Puesto que Internet no va a amanecer un día utilizando de repente IPv6 en vez de IPv4, se han debido desarrollar una serie de métodos que permitan la convivencia y comunicación entre nodos, sea cual sea su versión de protocolo IP. Se han desarrollado unos cuantos mecanismos de transición como los túneles y la comunicación entre nodos, cada uno de ellos con sus ventajas e inconvenientes, pero sobre todo pensados en un principio para casos de migración distintos.

CAPÍTULO 1

EL PROTOCOLO INTERNET IP VERSIÓN 4

1.1 GENERALIDADES

1.2 SERVICIOS IP

1.3 CABECERA IPv4

1.4 DIRECCIONES IPv4

1.5 SUBREDES

1.6 ENRUTAMIENTO

1.7 FRAGMENTACIÓN

1.8 REENSAMBLADO

1.9 PROBLEMAS DE IPv4 – LOS MOTIVOS DE IPv6

1.1 GENERALIDADES

El protocolo IP es el más utilizado para la interconexión entre redes y cuando se diseñó ya se tuvo en cuenta la interconexión entre redes. Su trabajo es proporcionar un medio para el transporte de datagramas del origen al destino, sin importar si estas máquinas están en la misma red, o si hay otras redes entre ellas. IP está implementado en todos los computadores y dispositivos de enrutamiento. Se preocupa de la retransmisión de los datos de un computador a otro computador, pasando por uno o varios dispositivos de enrutamiento nodo a nodo. No sabe de que aplicación son los paquetes, únicamente sabe de máquina son.

Este protocolo implementa el mecanismo de entrega de paquetes sin conexión y no confiable (técnica del mejor esfuerzo).

Cubre tres aspectos importantes como:

- Define la unidad básica para la transferencia de datos en una interred, especificando el formato exacto de un Datagrama IP.
- Realiza las funciones de enrutamiento
- Define las reglas para que los Host y Routers procesen paquetes, los descarten o generen mensajes de error.

Como cualquier protocolo estándar, IP se especifica en dos partes:

- La interfaz con la capa superior (por ejemplo TCP), especificando los servicios que proporciona IP.
- El formato real del protocolo y los mecanismos asociados.

Los datos proporcionados por la capa de transporte son divididos en datagramas y transmitidos a través de la capa de red (capa Internet). Durante el camino puede ser fragmentado en unidades más pequeñas si deben atravesar una red o subred cuyo tamaño de

paquete sea más pequeño. En la máquina destino, estas unidades son reensambladas para volver a tener el datagrama original que es entregado a la capa de transporte.

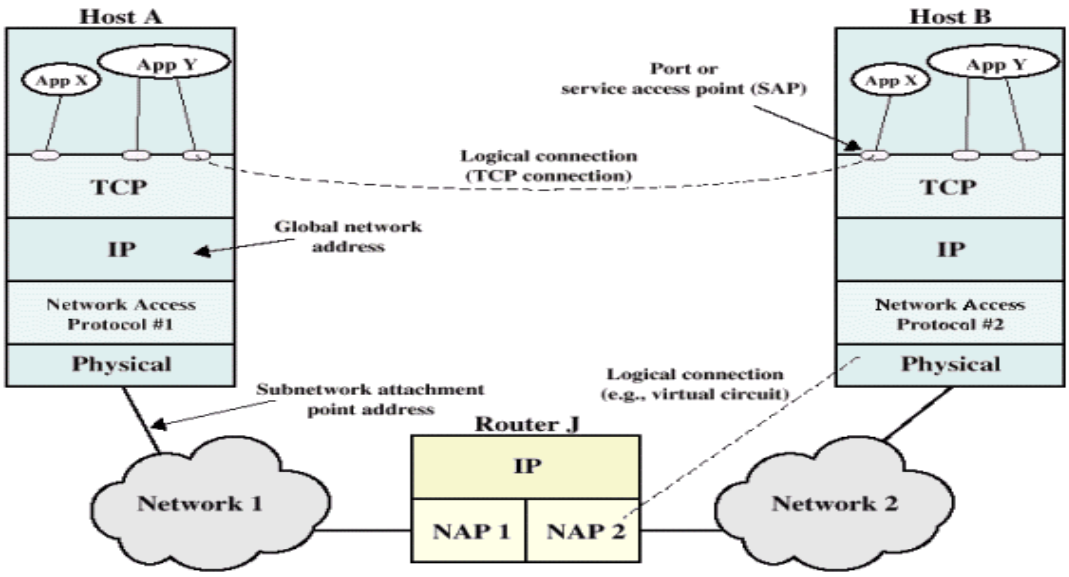


Figura 1 – Conceptos de direccionamiento

1.2 SERVICIOS IP

Los servicios que se van a proporcionar entre las capas de protocolos adyacentes (por ejemplo, entre IP y TCP) se expresan en términos de primitivas y parámetros. Una primitiva especifica la función que se va a ofrecer y los parámetros se utilizan para pasar datos e información de control.

IP proporciona dos primitivas de servicio en la interfaz con la siguiente capa superior.

```
Send {                                  Deliver {
        Dirección de origen                     Dirección de origen
        Dirección destino                       Dirección destino
        Protocolo                               Protocolo
        Indicadores del tipo de servicio        Indicadores del tipo de servicio
        Identificador
        Indicador de fragmentación
        Tiempo de vida
        Longitud de datos                       Longitud de datos
        Datos de opción                         Datos de opción
        Datos                                   Datos
        }                                       }
```

La primitiva **Send** (o envío) se utiliza para solicitar la transmisión de una unidad de datos. La primitiva **Deliver** (o entrega) la utiliza IP para avisar a un usuario la llegada de una unidad de datos.

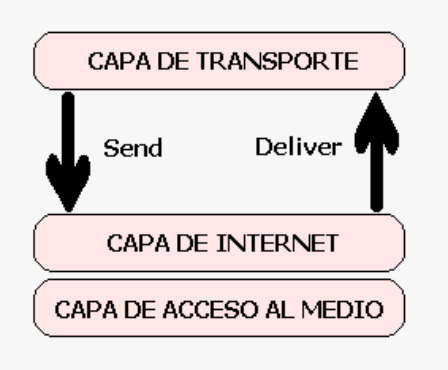


Figura 2 – Funcionamiento de las primitivas

Los parámetros asociados con estas dos primitivas son los siguientes:

- **Dirección de origen**: dirección global de red de la entidad IP que envía la unidad de datos.
- **Dirección destino**: dirección global de red de la entidad IP de destino.
- **Protocolo**: entidad de protocolo recipiente (un usuario IP).
- **Indicadores de tipo de servicio**: utilizado para especificar el tratamiento de la unidad de datos en su transmisión a través de los componentes de las redes.

- **Identificador**: utilizado en combinación con las direcciones origen y destino y el protocolo usuario para identificar de una forma única a la unidad de datos. Este parámetro se necesita para reensamblar e informar de errores.
- **Identificador de no fragmentación**: indica si IP puede segmentar los datos para realizar el transporte.
- **Tiempo de vida**: medida en segundos.
- **Longitud de datos:** longitud de los datos que se transmiten.
- **Datos de opciones**: opciones solicitadas por el usuario IP.
- **Datos:** datos de usuario que se van a transmitir.

En la primitiva Deliver los parámetros identificador, indicador de no fragmentación y tiempo de vida no se encuentran presentes por proporcionar instrucciones IP que no deben ser utilizadas por el receptor.

El emisor puede incluir el campo tipo de servicio para solicitar una calidad de servicio particular. La siguiente tabla muestra las opciones que hay de calidad de servicio:

PRECEDENCIA	Una medida de la importancia relativa del datagrama. Se utilizan ocho niveles de precedencia. IP tratará de proporcionar un tratamiento preferencial a los datagramas con precedencias superiores.
SEGURIDAD	Se puede especificar uno de dos niveles: normal o alta. Un valor alto indica una petición para que se intente minimizar la probabilidad de que este datagrama se pierda o resulte dañado.
RETARDO	Se puede especificar uno de dos niveles: normal o bajo. Un valor bajo indica una petición para minimizar el retardo que experimentará este datagrama.
RENDIMIENTO	Se puede especificar uno de dos niveles: normal o alto. Un valor alto indica una petición para maximizar el rendimiento para este datagrama.

Tabla 1 – Opciones de calidad del servicio IP

Los parámetros de opciones permiten ampliaciones futuras y la inclusión de parámetros que normalmente no se utilizan. Actualmente están definidas las siguientes opciones:

- **Seguridad**: permite que se incorpore una etiqueta de seguridad al datagrama.
- **Enrutamiento por la fuente:** constituye una lista secuencial de direcciones de dispositivos de enrutamiento que se especifica la ruta a seguir.
- **Registro de ruta:** se reserva un campo para registrar la secuencia de dispositivos de enrutamiento visitados por el datagrama.
- **Identificación de secuencia:** identifica recursos reservados utilizados para un servicio de secuencia. Este servicio proporciona un tratamiento especial del tráfico volátil periódico (por ejemplo voz).
- **Marcas de tiempo:** la entidad IP origen y algunos o todos los dispositivos de enrutamiento intermedios incorporan una marca temporal (con una precisión de milisegundos) a las unidades de datos conforme van pasando por ellos.

1.3 CABECERA IPv4

En la cabecera hay una parte fija de 20 bytes y una parte opcional de longitud variable. En la siguiente figura se puede ver el formato de la cabecera IP.

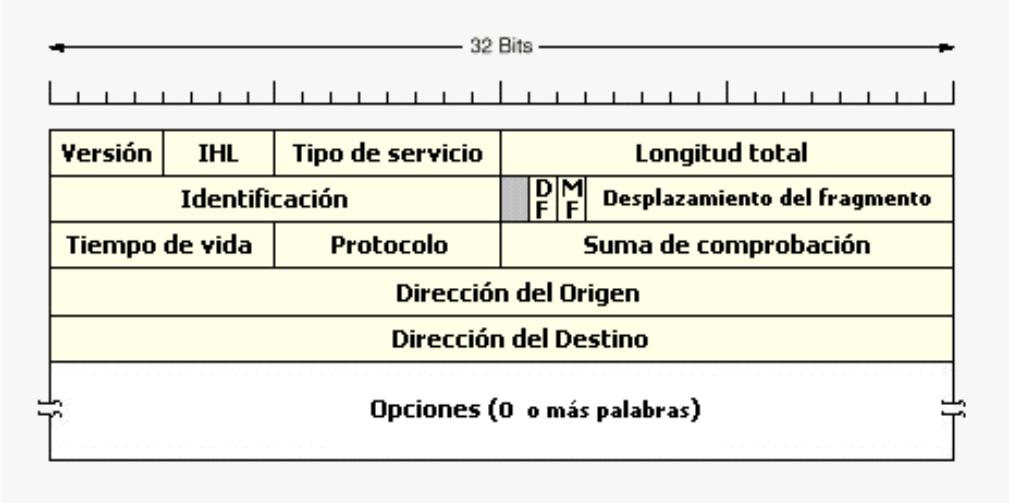


Figura 3 – Cabecera IPv4

A continuación hay una descripción de cada uno de los campos que forman la cabecera:

- **Versión** (4 bits): Indica el número de versión del protocolo al que pertenece el datagrama, lo que permitirá la evolución futura del protocolo y que la transición entre las versiones se pueda hacer ejecutándose en unas máquinas la versión vieja y en otras la versión nueva.

- **IHL** (Internet Header length) (4 bits): Indica la longitud de la cabecera en palabras de 32 bits (4 bytes). El valor mínimo es cinco (20/4=5). Este campo es necesario por no ser constante el tamaño de la cabecera como hemos comentado anteriormente. El valor máximo puede ser 15 (1111) lo que limita la cabecera a 60 bytes (15*4) y en consecuencia el campo de opciones a 40 (60-20). En el caso de que, por ejemplo, se quiera registrar la ruta de un paquete este valor puede ser insuficiente y ser totalmente inútil esta opción.

- **Tipo de servicio** (8 bits): Permite que el host especifique que clase de servicio quiere, pudiéndose combinar confiabilidad y velocidad. Para la voz digitalizada es mas importante realizar la entrega de forma rápida que precisa, mientras que para la transferencia de ficheros no importa a que velocidad se realiza la transferencia pero si que esté libre de errores. De los 8 bits, 3 son para el campo de precedencia que en realidad es una prioridad de 0 (normal) a 7 (para los paquetes de control de red). A continuación aparecen los bits de seguridad (alta o baja), retardo (alto o bajo cuando se intenta minimizar el retardo) y rendimiento (normal o alto cuando se intenta maximizar el rendimiento durante la transmisión del datagrama).

- **Longitud total** (16 bits) en bytes que tendrá todo el datagrama, considerando tanto la cabecera como los datos. Hay que tener en cuenta que el tamaño máximo de un datagrama es de 65535 bytes lo que puede ser insuficiente en las redes de alta velocidad.

- **Identificador** (16 bits): es un número de secuencia que junto a la dirección origen, la dirección destino y el protocolo de usuario, sirven para que la máquina destino determine a que datagrama pertenece el fragmento que ha recibido. Todos los fragmentos de un datagrama contienen el mismo valor en el campo identificador y este número debe ser único para la dirección origen, la dirección destino y el protocolo de usuario durante el tiempo en el que el datagrama permanece en el conjunto de redes.

- **Indicadores** (3 bits): El primer bit no se utiliza actualmente. El indicador de mas fragmentos (**MF**) cuando vale 1 indica que este datagrama tiene mas fragmentos y toma el valor 0 en el último fragmento. El indicador de no fragmentar (**DF**) prohíbe la fragmentación cuando vale 1. Es una orden que se le da a los encaminadores de que no fragmenten el datagrama cuando el destino es incapaz de reensamblarlo. Si este bit vale 1, el datagrama se descartará si se excede el tamaño máximo en una subred de la ruta. Por lo tanto, cuando este bit vale 1, es aconsejable usar enrutamiento por la fuente para evitar subredes cuyo tamaño máximo de paquete sea menor que el tamaño del datagrama.

- **Desplazamiento del fragmento** (13 bits): Indica en que posición del datagrama original, medido en unidades de 8 bytes (64 bits), va el fragmento actual. Debido a esto, todos los fragmentos excepto el último contienen un campo de datos con una longitud múltiplo de 8 bytes. Como se proporcionan 13 bits, puede haber un máximo de 8912 (2**13) fragmentos por datagrama, y por lo tanto el tamaño máximo de un datagrama es de 65536 bytes, uno mas que el campo de longitud total.

- **Tiempo de vida** (8 bits): Es un contador que sirve para limitar la vida de un paquete. Aunque lo lógico sería pensar que cuenta el tiempo en segundos, en realidad lo que cuenta es el número de saltos de dispositivo de enrutamiento que realiza. Cuando el contador llega a cero, el paquete se descarta y se envía de un paquete al computador origen avisándole. Con este mecanismo se consigue que los datagramas no permanezcan indefinidamente en la red si, por ejemplo, se dañan las tablas de enrutamiento.

- **Protocolo** (8 bits): Se utiliza por la capa de red para saber a que protocolo de la capa de transporte le tiene que enviar el datagrama una vez lo ha reensamblado. Existen diferentes protocolos de transporte, entre ellos TCP y UDP.

- **Suma de comprobación** (16 bits): Sirve para verificar el contenido de la cabecera y es útil para la detección de errores generados durante la transmisión del datagrama. Como algunos de los campos de la cabecera pueden cambiar en alguno de los dispositivitos de enrutamiento (por ejemplo, el tiempo de vida y algunos campos relacionados con la segmentación), este valor es verificado y recalculado en cada uno de los dispositivos de enrutamiento. El algoritmo empleado consiste en sumar todas las medias palabras de 16 bits a medida que van llegando, usando la aritmética de complemento a 1, y luego obtener el complemento a 1 del resultado. Se supone que la suma de comprobación de la cabecera es cero cuando llega. Este algoritmo es algo más robusto que una suma normal. Existen algunas técnicas para acelerar el cálculo.

- **Dirección origen** (32 bits): Indica el número de red y el número del computador que envía el datagrama.

- **Dirección destino** (32 bits): Indica el número de red y el número del computador al que se envía el datagrama.

- **Opciones** (variable): Contiene las opciones solicitadas por el usuario que envía los datos y se diseñó para que las versiones posteriores del protocolo pudieran incluir información no considerada originalmente, para que los investigadores pudieran probar cosas nuevas y para que aquellas aquella información que es utilizada pocas veces no tuviera asignada unos bits determinados en la cabecera. Cada una de las opciones empieza en 1 byte que identifica la opción. Algunas de las opciones vienes seguidas de un campo de 1 byte para indicar la longitud de la opción y a continuación uno o más bytes de datos. Hay seis opciones (Seguridad, Enrutamiento estricto desde el origen, Enrutamiento libre desde el origen, Registrar la ruta, Identificación de

secuencia, Marca de tiempo definidas actualmente pero no todas son reconocidas por todos los dispositivos de enrutamiento:

- *Seguridad*: Permite añadir una etiqueta para indicar lo secreta que es la información que contiene el datagrama. Por ejemplo, se podría utilizar para que los dispositivos de enrutamiento no consideren redes en concreto. Pero en realidad esta etiqueta es ignorada y realmente para lo único que sirve es para ayudar a los espías a encontrar con mayor facilidad la información importante.
- *Enrutamiento estricto desde el origen*: Es una secuencia de direcciones IP que sirve para indicar la trayectoria completa que debe seguir el datagrama desde el origen hasta el destino. Esta opción es usada sobre todo cuando los administradores de sistemas envían paquetes de emergencia porque las tablas de enrutamiento se han corrompido o para hacer mediciones de tiempo.
- *Enrutamiento libre desde el origen*: Es una secuencia de direcciones IP que sirve para indicar que el datagrama debe pasar obligatoriamente por esos dispositivos de enrutamiento y en ese orden, pero también puede pasar por otros dispositivos de enrutamiento. Esta opción es útil cuando por diversas consideraciones se deben pasar por algunos dispositivos de enrutamiento en concreto.
- *Registrar la ruta*: Sirve para indicar que los dispositivos de enrutamiento agreguen su dirección IP al campo de opción y de esta manera tener conocimiento de la ruta seguida por el datagrama. Se utiliza, por ejemplo, para poder determinar si los algoritmos de enrutamiento están funcionando correctamente. Los 40 bytes de tamaño máximo que puede tener el campo de opciones sólo permite registrar 9 saltos, lo que puede ser en las redes actuales en muchos casos insuficiente.
- *Identificación de secuencia*. Se utiliza cuando hay recursos reservados para un servicio, por ejemplo voz.
- *Marca de tiempo*: En este caso, además de registrar las direcciones de los dispositivos de enrutamiento como se hacia en la opción registrar la ruta, se utilizan 32 bits para guardar una marca de tiempo expresada en milisegundos.

Esta marca es usada principalmente para buscar fallos en los algoritmos de enrutamiento.

- **Relleno** (variable): El campo de opciones se rellena para que su tamaño sea múltiplo de 32 bits (4 bytes).

1.4 DIRECCIONES IPv4

Cada computador y cada dispositivo de enrutamiento tendrán una dirección única cuya longitud será de 32 bits, que será utilizada en los campos dirección origen y dirección destino de la cabecera. Esta dirección consta de un identificador de red y de un identificador de computador. La dirección, como puede verse en la siguiente figura 1.5, está codificada para permitir una asignación variable de los bits utilizados al especificar la red y el computador. Este formato de direcciones permite mezclar las tres clases de direcciones en el mismo conjunto de redes. La dirección IP más pequeña es la 0.0.0.0 y la mayor es 255.255.255.255. Existen tres clases de redes que se pueden clasificar teniendo en cuenta la longitud del campo de red y del campo computador. La clase a la que pertenece una dirección puede ser determinada por la posición del primer 0 en los cuatro primeros bits. Las direcciones están codificadas para permitir una asignación variable de bits para especificar la red y el computador.

- **Clase A**: Pocas redes, cada una con muchos computadores. 7 y 24 bits (+1). Por ejemplo ARPANET.
- **Clase B**: Un número medio de redes, cada una con un número medio de computadores. 14 y 16 bits (+2).
- **Clase C**: Muchas redes, cada una con pocos computadores. 21 y 8 bits (+3). Por ejemplo una red de área local.
- **Clase D**: Permite hacer multitransmisión (o multicasting) en la cual el datagrama se dirige a múltiples computadores. Podemos enviar un paquete IP a un grupo de máquinas que por ejemplo pueden estar cooperando de alguna manera mediante la utilización de una dirección de grupo.

- **Clase E**: Reservado para el futuro.

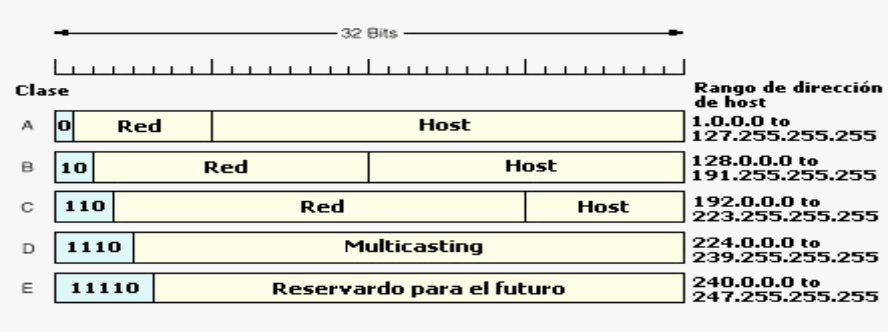


Figura 4 – Formatos de dirección IP

La siguiente tabla muestra el número de redes y de computadores por red en cada una de las tres clases primarias de direcciones IP:

CLASE	BITS EN EL PREFIJO	MAXIMO Nº DE REDES	BITS EN EL SUFIJO	MAXIMO Nº DE COMPUTADORES POR RED
A	7	128	24	16777216
B	14	16384	16	65536
C	21	2097152	8	256

Tabla 2 – Número de redes y computadores por red

Normalmente las direcciones se suelen escribir en notación decimal con puntos. Por ejemplo, la dirección 82CE7C0D (1000 0010 1100 1110 0111 1100 0000 1101 que es de clase B) se escribe como 130.206.124.13.

82 = 8*16 + 2 = 128 + 2 = 130
CE = C*16 + E = 12 * 16 + 14 = 192 + 14 = 206
7C = 7 * 16 + C = 112 + 12 = 124
0D = D = 13

Observando la figura anterior puede verse que no todas las direcciones han sido asignadas a una clase en concreto. Algunas de estas direcciones se utilizan como direcciones especiales:

- **Este computador**: La dirección 0.0.0.0 significa esta red o este computador y únicamente es usada por los computadores cuando son arrancados, sin que se vuelva a utilizar posteriormente. De esta forma las máquinas se pueden referir a su propia red sin saber su número, pero tiene que saber su clase para saber cuantos ceros debe incluir.
- **Un computador de esta red**: Poniendo el campo red todo a ceros (es necesario saber la clase de la red para decidir cuantos ceros se deben poner).
- **Difusión de red local o limitada**: La dirección 255.255.255.255 (todos 1s) se usa como dirección para indicar todos los computadores de la red indicada y es utilizada para hacer difusión.
- **Difusión de una red distante o dirigida**: También se puede hacer difusión a una red distante poniendo la dirección de la red y rellenando el campo computador con 1's.
- **Retrociclo**: Las direcciones 127.xx.yy.zz se reservan para pruebas de realimentación. Los paquetes que tienen esta dirección no son enviados por la red sino que son procesados localmente y se tratan como si fueran paquetes de entrada. Esto permite que los paquetes se envíen a la red local sin que el transmisor conozca su número. Esta característica también se usa para la detección de fallos en el software de red.

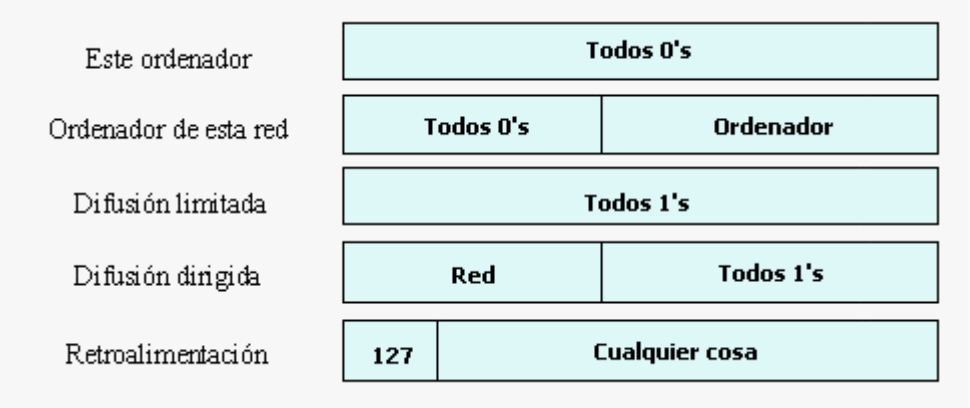


Figura 5 – Direcciones especiales

Para estar seguros de que la dirección Internet es única, todas las direcciones de Internet son asignadas por una autoridad central. El Internet Assigned Number Authority (IANA) tiene el

control sobre los números asignados. Sin embargo, cuando una organización quiere una dirección debe obtenerla de INTERNIC (Internet Network Information Center). La autoridad central solo es necesaria para asignar la porción de la dirección correspondiente a la red, cuando una organización ya tiene su prefijo, puede asignar un único sufijo a cada computador sin contactar con la autoridad central.

1.5 SUBREDES

El que todos los computadores de una red deban tener el mismo número de red puede causar problemas. A medida que aumenta la utilización de las redes locales puede ser interesante considerar que un conjunto de computadores forman una red independiente, pero que externamente se vea a todos los computadores como una sola red. La manera de hacerlo consiste en subdividir el campo correspondiente a la identificación de la máquina en dos subcampos, uno para la subred (por ejemplo de 6 bits) y otro para los computadores (que deberá tener 10 bits).

Antes de continuar es necesario explicar como se realiza el enrutamiento de los paquetes IP. La dirección destino se obtiene gracias a una lista que hay en los dispositivos de enrutamiento en la que pueden haber direcciones IP con el formato (red,0) para llegar a redes distantes y direcciones IP con el formato (esta red, computador) para llegar a los computadores locales. Cuando llega un paquete IP, se busca su dirección de destino en la tabla de enrutamiento. Si es para una red distante, se reenvía al dispositivo de enrutamiento indicado en la tabla. Y si es para un computador local se envía directamente a la máquina. Cuando la red no está en la tabla, el paquete se envía a un dispositivo de enrutamiento predeterminado con tablas más extensas. De esta manera cada dispositivo de enrutamiento sólo debe llevar el control de otras redes y de los computadores locales.

Cuando se utilizan subredes, en las tablas de enrutamiento se agregan entradas de la forma (esta red, subred, 0) y (esta red, esta subred, 0). De esta manera, un dispositivo de enrutamiento de la subred “k” sabe cómo llegar a todas las subredes y a todos los computadores de la subred “k”. No necesita saber nada de los computadores de otras subredes.

Cada enrutador lo que debe hacer es un AND booleano con la máscara de la subred para eliminar el número de host y buscar la información resultante en sus tablas.

En la siguiente tabla se puede ver el siguiente ejemplo. Un paquete dirigido a 130.5.15.6 que llega al dispositivo de enrutamiento de la subred 5 se le hace un AND con la mascara de la subred obteniéndose la dirección 130.50.12.0. Esta es la dirección que se busca en las tablas de enrutamiento para averiguar como se puede llegar a los computadores de la subred 3. De esta manera el dispositivo de enrutamiento de la subred 5 no tiene que mantener un registro de las direcciones de enlace de los computadores que no pertenecen a su subred. Esta jerarquía de tres niveles reduce el tamaño de la tabla de enrutamiento.

Dirección destino	130	5	15	6
(en binario)	10000010	00000101	00001111	00000110
(idem)	10	000010 00000101	000011	11 00000110
MASCARA subred 5	11	111111 11111111	000111	00 00000000
(resultado del AND)	10	000010 00000101	000011	00 00000000
(idem)	10000010	00000101	00001100	00000000
Dirección obtenida	**130**	**5**	**12**	**0**

Figura 6 – Representación punto decimal y binaria de las direcciones IP y las máscaras de subred

1.6 ENRUTAMIENTO

Cuando un paquete llega a un dispositivo de enrutamiento se debe determinar cual es la dirección del siguiente dispositivo de enrutamiento teniendo en cuenta la dirección IP destino que hay almacenada en el campo correspondiente del paquete y de la información que hay almacenada en las tablas de enrutamiento. Hay que tener en cuenta que es necesario realizar una conversión entre la dirección IP y la dirección MAC (cuando el enlace entre los dos

dispositivos de enrutamiento sea una LAN) que se efectúa de manera automática mediante el protocolo ARP.

Esta tabla puede ser estática o dinámica. En el primer caso puede contener rutas alternativas que serán utilizadas cuando algún dispositivo de enrutamiento no esté disponible. Las tablas dinámicas son más flexibles cuando aparecen errores o congestión en la red. Estas tablas también pueden proporcionar servicios de seguridad y de prioridad, por ejemplo, para asegurarse que a ciertos datos no se les permita pasar por determinadas redes.

Otra técnica de enrutamiento es el enrutamiento en la fuente. En este caso, como ya comentamos anteriormente, el computador origen incluye en la cabecera del paquete la dirección de los dispositivos de enrutamiento que debe utilizar el paquete.

1.7 FRAGMENTACIÓN

Cuando tenemos un paquete IP y se va a pasar a la capa de enlace se le añade la cabecera y el campo de CRC. Hay redes que limitan el tamaño máximo de los paquetes que pueden transportar y por este motivo, los paquetes deben ser fragmentados como ilustra la figura 7. Recordar que al hablar de la cabecera de un paquete IP comentamos la existencia del bit de no fragmentación que cuando está activo especifica que el paquete no se puede fragmentar.

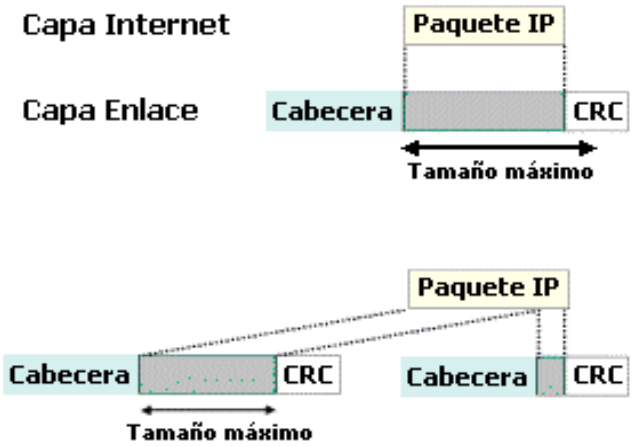


Figura 7 – Fragmentación paquetes

Los campos cuyo valor es modificado debido a la fragmentación son:

- El campo posición o desplazamiento que indica a que byte corresponde el primer byte de datos.
- El Indicador o bit de más datos: Vale 1 en todos los fragmentos excepto en el último. Si un fragmento tiene que volver a ser fragmentado y el bit de más datos ya vale 1, mantendrá este valor en todos los nuevos fragmentos. Si vale 0, tomará el valor 1 excepto en el último fragmento.
- El campo longitud de los datos y el campo checksum es calculado para cada fragmento.
- El identificador de paquete y el resto de campos conservan el valor que tienen antes de ser fragmentado el paquete IP.

1.8 REENSAMBLADO

Como todos los fragmentos de un paquete IP tienen el mismo identificador de paquete y en la cabecera está almacenado el tamaño del fragmento y su desplazamiento dentro del paquete es fácil realizar el reensamblado. De cualquier manera tanto la fragmentación como el

reensamblado consumen bastantes recursos. Además de asignar un buffer en el que se realizará el reensamblado del paquete, también se necesita controlar que fragmentos han llegado y cuando, cual están pendientes de llegar y controlar cuando el paquete ya está completo.

Como no hay manera de saber el tamaño exacto del paquete, el tamaño del buffer tiene que ser de 65535 bytes (exactamente el tamaño máximo del paquete IP) Cuando recibe por primera vez un fragmento de un paquete se pone en marcha un temporizador (tiempo de vida de reensamblaje) y va colocando los diferentes fragmentos que le vayan llegado de ese paquete IP (todos aquellos que tienen el mismo identificador). Si transcurrido el tiempo determinado por el temporizador no se ha podido realizar el reensamblado, se para el proceso de reensamblado y los paquetes recibidos se descartan. Hay que tener en cuenta que el tiempo de vida del datagrama también se va decrementado mientras dura el reensamblado. Como IP no garantiza el servicio, el protocolo de transporte TCP será el encargado de pedir la retransmisión del paquete.

Existen dos posibilidades respecto a donde se debe realizar el reensamblado de los paquetes: en cada uno de los dispositivos de enrutamiento o solo en el destino. Realizar el ensamblado en cada uno de los dispositivos de enrutamiento tiene la ventaja de que se utilizan mejor los recursos del sistema. En cada tramo de red únicamente se transporta el número de paquetes necesario reduciéndose la carga de la red al disminuir el número de paquetes, y por consiguiente de cabeceras, que son transportados. Esta posibilidad tiene el inconveniente de que es necesario reservar memoria en cada uno de los dispositivos de enrutamiento y es necesario un tiempo en cada uno de ellos para realizar el proceso de reensamblado. Además, en este caso, es necesario que todos los fragmentos de un paquete pasen por el mismo dispositivo de enrutamiento y por lo tanto no se podrá hacer enrutamiento dinámico. El protocolo IP realiza el reensamblado en el destino.

En la tabla 3 se puede ver un pequeño resumen de las ventajas e inconvenientes de cada una de las posibilidades:

DISPOSITIVOS DE ENCAMINAMIENTO	• Mejor utilización de los recursos • Se necesitan grandes memorias • Todos los fragmentos deben pasar por el mismo dispositivo de encaminamiento
EN EL DESTINO	• Disminuye la eficiencia • Es más fácil de realizar

Tabla 3 – Ventajas e inconvenientes de los tipos de reensamblado

1.9 PROBLEMAS DE IPv4 – LOS MOTIVOS DE IPv6

El motivo básico por el que surge, en el seno del IETF (Internet Engineering Task Force), la necesidad de crear un nuevo protocolo, que en un primer momento se denominó IPng (Internet Protocol Next Generación, o "Siguiente Generación del Protocolo Internet"), fueron la evidencia de falta de direcciones.

IPv4 tiene un espacio de direcciones de 32 bits, es decir, 2^{32} (4.294.967.296). En cambio, IPv6 nos ofrece un espacio de 2^{128} (340.282.366.920.938.463.374.607.431.768.211.456).

Sin embargo, IPv4 tiene otros problemas o "dificultades" que IPv6 soluciona o mejora.

Adicional a esto, había una necesidad de extender la funcionalidad de la capa de red con características como QoS, encriptación punto a punto, enrutamiento de origen y autenticación, entre otras, y aparte de esto surgieron otros problemas como:

- Lentitud debido a protocolos de enrutamiento ineficientes, que además hacen que las tablas de enrutamiento sean de gran tamaño y muy difíciles de mantener.

- Falta de seguridad, la imposibilidad de prestar servicios de autenticación, integridad y confidencialidad por sí mismo, sino a través de extensiones al protocolo como lo es IPSec.
- No poder distinguir entre diferentes clases de tráfico para darles un tratamiento especial (QoS).
- El formato de los encabezados es muy grande y complejo.

Los creadores de IPv4, a principios de los años 70, no predijeron en ningún momento, el gran éxito que este protocolo iba a tener en muy poco tiempo, en una gran multitud de campos, no sólo científicos y de educación, sino también en innumerables facetas de la vida cotidiana.

Podemos recordar algunas "frases famosas" que nos ayudarán a entender hasta que punto, los propios "precursores" de la revolución tecnológica que se estamos viviendo, no llegaron a prever:

- [1]"Pienso que el mercado mundial de computadores puede ser de cinco unidades".
- [2]"640 Kb, de memoria han de ser suficientes para cualquier usuario".
- [3]"32 bits proporcionan un espacio de direccionamiento suficiente para Internet".

No es que estuvieran equivocados, sino que las Tecnologías de la Información han evolucionado de un modo mucho más explosivo de lo esperado.

Desde ese momento, y debido a la multitud de nuevas aplicaciones en las que IPv4 ha sido utilizado, ha sido necesario crear "añadidos" al protocolo básico.

Entre los "parches" más conocidos, podemos citar medidas para permitir la calidad de servicio (QoS), Seguridad (IPsec), y Movilidad, fundamentalmente.

El inconveniente más importante de estas aplicaciones de IPv4, es que utilizar cualquiera de ellos es muy fácil, pero no tanto cuando pretendemos usar al mismo tiempo dos "añadidos", y

[1] Thomas Watson, Presidente de IBM en 1993
[2] Bill Gates, Presidente de Microsoft, 1981
[3] Dr. Vinton Cerf, padre de Internet, 1977

no digamos que se convierte en casi imposible o muy poco práctico el uso simultaneo de tres o más.

El reducido espacio IPv4, a pesar de disponer de cuatro mil millones de direcciones, junto al hecho de una importante falta de coordinación, durante la década de los 80, en la delegación de direcciones, sin ningún tipo de optimización, dejando incluso grandes espacios discontinuos, nos está llevando a límites no sospechados.

Una solución que se podría considerar como evidente, como sería la remuneración, y reasignación de dicho espacio de direccionamiento. Sin embargo, no es tan sencillo, es incluso impensable que en algunas redes, ya requiere unos esfuerzos de coordinación, a escala mundial, absolutamente impensables.

Además, uno de los problemas de IPv4 permanecería: la gran dimensión de las tablas de encaminado (routing) en le troncal Internet, que la hace ineficaz, y perjudica enormemente los tiempos de respuesta.

La falta de direcciones no es apreciable por igual en todos los puntos de la red, de hecho, no es casi apreciable, por el momento, en Norte América. Sin embargo, en zonas geográficas como Asia (en Japón la situación está llegando a ser critica) y Europa, el problema se agrava.

Algunos Proveedores de Servicios de Internet se ven obligados a proporcionar a sus clientes direcciones IP privadas, mediante mecanismos de NAT (traslación de direcciones, es decir, usar una sola IP pública para toda una red privada).

Pero lo más importante es el imparable crecimiento de aplicaciones que necesitan direcciones IP públicas únicas, globales, válidas para conexiones extremo a extremo, y por tanto encaminables (enrutables): Videoconferencia, voz sobre IP, seguridad, e incluso juegos.

A esto se le suma los innumerables dispositivos que se van creando, o los ya existentes a los que se le dan nuevas o mejoras aplicaciones, mediante conexión a la red, como ejemplo:

- Teléfonos, pues la siguiente generación, sin duda, pasará por tecnología IP (VoIP).
- Televisión y Radio, también basados en tecnología IP.
- Sistemas de seguridad, televigilancia y control.
- Walkman Mp3, que conectados con la red, nos permiten recuperar y almacenar creaciones musicales.
- Nuevas tecnologías emergentes. Como Bluetooth, WAP, redes inalámbricas, redes domesticas, etc.

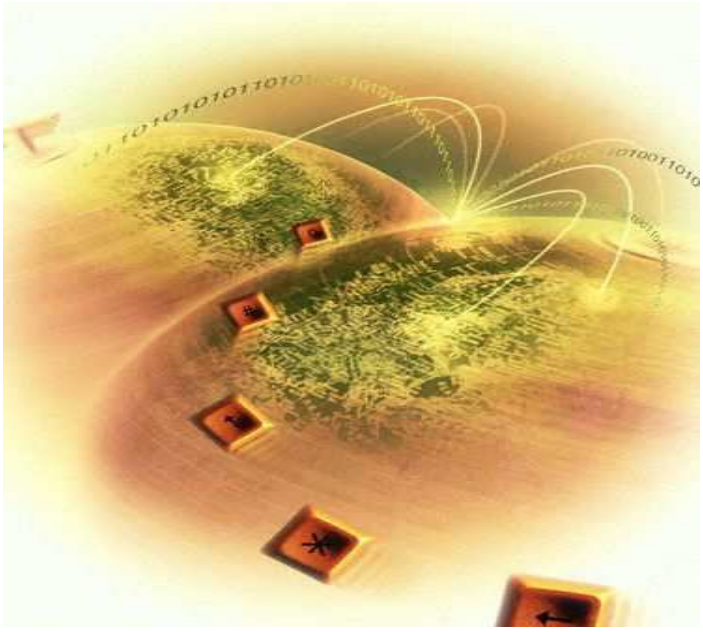
CAPÍTULO 2

EL PROTOCOLO INTERNET IP VERSIÓN 6

2.1 HISTORIA

2.2 CARACTERISTICAS

2.3 VENTAJAS Y DESVENTAJAS



2.1 HISTORIA

IPv6 es la versión nueva del Protocolo de Internet que está diseñada como un paso evolutivo del IPv4. Representa el fruto de muchas propuestas del IETF (Internet Engineering Task Force) y de grupos de trabajo centrados en desarrollar un IPng. Básicamente ha habido tres fases importantes en el desarrollo de IPv6 hasta el momento lo que hoy conocemos como IPv6:

- Para el invierno de 1992 la comunidad del Internet había desarrollado cuatro propuestas diferentes para el IPng que eran: CNAT, IP Encaps, Nimrod y Simple CLNP.
- Después para diciembre del mismo año, aparecieron tres propuestas más el " PIP " (The P Internet Protocol), el " SIP " (The Simple Internet Protocol) y el " TP/IX ".
- En la primavera de 1992 el "Simple CLNP" se desarrolló en el " TUBA" (TCP and UDP with Bigger Addresses" , y el " IP Encaps " en " IPAE " (IP Address Encapsulation)
- Para el verano de 1993, IPAE se combinó con el SIP aunque mantuvo el nombre SIP, que posteriormente se fusionó con la PIPA, y al grupo de trabajo resultante se le llamó "SIPP" (Simple Internet Protocol Plus). Casi al mismo tiempo el grupo de trabajo TP/IX cambió su nombre por el de "CATNIP" (Common Architecture for the Internet)
- Posteriormente, en la reunión del IETF del 25 de julio de 1994 en Toronto Canadá, los directores de área del mismo organismo recomendaron el uso del IPng y lo documentaron en el RFC 1752, (la recomendación para el protocolo IP de siguiente generación)
- El 17 de noviembre del mismo año fue aprobada esta recomendación por el "IESG" (Internet Engineering Steering Group) que elaboró una propuesta de Estándar.

Como fase adicional muy significativa, podemos añadir la constitución oficial, en julio de 1.999, del “IPv6 Forum” o Foro Ipv6, que ha implicado, un importantísimo crecimiento respecto del fomento, promoción, uso y aplicación del protocolo, con adopciones tan importantes como las realizadas por la OTAN, ETSI, UMTS, 3GPP, y la comunidad Europea.

2.2 CARACTERISTICAS

2.2.1 ARQUITECTURA DE DIRECCIONAMIENTO

Diferente a IPv4 que usa 4 octetos separados por puntos en notación decimal, IPv6 al tener que denotar una dirección de 128bits usa 8 campos hexadecimales, de 16 bits cada uno. El uso de hexadecimales en IPv6 sirve para una notoria reducción en el tamaño de la dirección, ya que cada byte se puede denotar en 2 hexadecimales. Por ejemplo una dirección en IPv6 podría verse así: 3FC2:43AB:3240:0000:85E2:0002:2900:00AC, se usan dos puntos (:) para la delimitación de campos.

A veces las direcciones se pueden tornar un poco confusas por ser tan largas, pero se pueden utilizar convenciones adicionales para su reducción.

- Todos los ceros a la izquierda se pueden eliminar.
- Si uno de los campos tiene solo ceros se puede obviar el campo dejándolo vacío.
- Si hay varios campos vacíos, se eliminan los dos puntos de tal modo que solo queden dos consecutivos.

3FFE:43AB:3240:0000:85E2:0002:2900:00AC pasaría a ser:
3FFE:43AB:3240::85E2:2:2900:AC
3FFE:FE34:32AB:0000:0000:0000:0000:0001 podría expresarse como:
3FFE:FE34:32AB::1

Cuando IPv4 surgió, solo se clasificaban las redes de tres maneras (Clase A, B, y C), y la tarea de enrutamiento era muy básica, pero era claro que esta clasificación no era la mas eficiente, y fue cuando estrategias de delegación de redes como [4]"CIDR" (Encaminamiento entre dominio sin clase), que el concepto de clases prácticamente desapareció, permitiendo agregar redes pequeñas en superredes, y partiéndolas en redes mas pequeñas. Este mecanismo mejoró notablemente la distribución del espacio IP pero a su vez trajo una consecuencia, la tarea de enrutamiento. Ya con esto las tablas de enrutamiento crecerían, y la labor de llevar un paquete

[4] Estrategia de direccionamiento que consiste en usar mascaras de bits para asignar una parte variable de la dirección IPv4 de 32 bits a una red, subred, o anfitrión.

a su destino podría costar recursos adicionales, que no fueron previstos cuando se tenía una clasificación de 3 tipos. A pesar de que se solucionó un problema, el de asignación de espacios, pero se originó otro que eran complejas tablas de enrutamiento que podría disminuir la complejidad en la red.

IPv6 debido a esto, trata de establecer ciertas políticas de tal modo que se pueda administrar el nuevo espacio de direcciones con una asignación adecuada, y a su vez que la tarea de enrutamiento sea lo suficientemente eficaz para la transmisión de paquetes.

Una de las ventajas que tiene IPv6 sobre CIDR es que divide la dirección en 6 campos, de tal modo que se pueda identificar la pertenencia de un host a una entidad específica, usando varios bits iniciales para hacer más efectiva la tarea de enrutamiento.

2.2.1.1 DIRECCIONAMIENTO IPv6

Las direcciones IPv6 como ya se ha dicho son identificadores de 128 bits para las interfaces y conjunto de interfaces. Dicha direcciones se clasifican en tres tipos:

- **UNICAST:** identificador para una interfaz. Un paquete enviado a una dirección unicast es entregado ***sólo*** a la interfaz identificada con dicha dirección. Es equivalente a las direcciones IPv4 actuales.

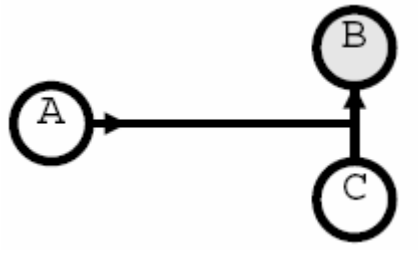


Figura 8 - Comportamiento Unicast

- **ANYCAST:** identificador para un conjunto de interfaces (típicamente perteneciente a diferentes [5]nodos). Ung paquete enviado a un dirección anycast es entregado a ***una*** (cualquiera) de las interfaces identificadas con dicha dirección (la más próxima, de acuerdo a las medidas de distancia del protocolo de encaminamiento). Nos permite crear, por ejemplo, ámbitos de redundancia, de forma que varias máquinas puedan ocuparse del mismo tráfico según un secuencia determinada (por el routing), si la primera cae.

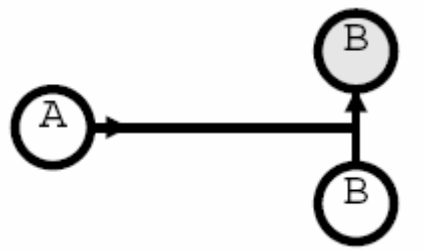


Figura 9 - Comportamiento Anycast

- **MULTICAST:** identificador para un conjunto de interfaces (por lo general perteneciente a diferentes nodos). Un paquete enviado a una dirección multicast es entregado a ***todas*** las interfaces identificadas por dicha dirección. La misión de este tipo de paquete es evidente: aplicaciones de retrasmisión múltiple (broadcast).

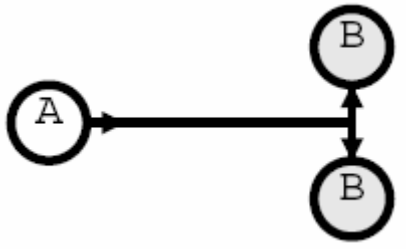


Figura 10 - Comportamiento Multicast

[5] En IPv6, un nodo es cualquier dispositivo que implemente IPv6; esto incluye a los computadores y dispositivos de encaminamiento

2.2.1.2 MODELOS DE DIRECCIONAMIENTO

Cualquier tipo de dirección se asigna a interfaces, no nodos. Es algo importante que no hay que olvidar. Todos las interfaces han de tener, por los menos, una dirección de enlace local (Link-Local) de tipo unicast. Una misma interfaz puede tener asignadas múltiples direcciones de cualquier tipo (unicast, anycast, multicast) o ámbito (scope). Direcciones unicast con ámbito mayor que el de enlace no son necesarias para interfaces que no son usados como origen y destino de paquetes IPv6 hacia o desde no vecinos. Esto significa que para la comunicación dentro de una LAN no nos hacen falta direcciones IPv6 globales, sino que tenemos más que suficiente con direcciones de ámbito local. De hecho, es lo aconsejable para enlaces punto a punto.

Respecto a los prefijos de subred, IPv6 sigue el mismo modelo que IPv4, es decir, un prefijo se asocia a un enlace, pudiendo haber varios prefijos en un mismo enlace.

2.2.1.3 ÁMBITOS

El protocolo IPv6 añade soporte para direcciones de distintos ámbitos, lo que quiere decir que tendremos direcciones globales y no globales. Si bien con IPv4 ya habíamos empleado direccionamiento no global con la ayuda de prefijos de red privados, con IPv6 esta noción forma parte de la propia arquitectura de direccionamiento.

Cada dirección IPv6 tiene un ámbito, que es un área dentro de la cual ésta puede ser utilizada como identificador único de uno o varios interfaces. El ámbito de cada dirección forma parte de la misma dirección, con lo que vamos a poder diferenciarlos a simple vista.

Para las direcciones unicast distinguimos tres ámbitos:

- De enlace local (link-local), para identificar interfaces en un mismo enlace. Empiezan todas por fe80:.

- De sitio local (site-local), para identificar interfaces en un mismo 'sitio'. La definición de 'sitio' es un tanto genérica, pero en principio un 'sitio' es el área topológica de red perteneciente a un edificio o un campus, perteneciente a una misma organización. Empiezan por fec0: .
- Global, para identificar interfaces en toda Internet. Estas comienzan por 2001: o 3ffe:.

En lo que al ámbito se refiere, las direcciones anycast siguen la misma norma que las unicast. Sin embargo, para las direcciones multicast tenemos catorce posibles ámbitos, que identifican desde un interfaz local a una dirección global.

Nodos de un mismo ámbito y visibles entre sí definen una zona. No se permite que un router encamine tráfico entre diferentes zonas (perderían todo el sentido los ámbitos).

Una de las grandes ventajas de los ámbitos es que permitirá la renumeración de prefijos sin mucha dificultad, ya que las direcciones de ámbito no global se mantendrán.

Tenemos que esperar que se produzca alguna renumeración de prefijos globales, ya que según crezca una organización su prefijo se puede quedar pequeño y necesitar más espacio de direcciones. Y como hemos dicho antes, se tratará siempre que sea posible de mantener las tablas de encaminamiento al mínimo.

Lo que sólo se consigue dando un prefijo nuevo mayor e invalidando el anterior, porque lo que seguramente sucederá será que las redes contiguas ya estén asignadas.

2.2.1.4 NOMENCLATURA DE DIRECCIONES IPv6

La representación de las direcciones IPv6 sigue el siguiente esquema:

- X:X:X:X:X:X:X:X donde cada "X" es el valor en hexadecimal de cada grupo de 16 bits de la dirección. No es preciso escribir los ceros a la izquierda de cada campo.
  Ejemplo: FEDC:BA98:7654:3210: FEDC:BA98:7654:3210
  1080:0:0:0:8:800:200C:417A

- Dado que, por el direccionamiento que se ha definido, podrán existir largas cadenas de bits "cero", se permite la escritura de su abreviación, mediante el uso de "::", que representa múltiples grupos consecutivos de 16 bits "cero". Este símbolo solo puede aparecer una vez en la dirección IPv6.

  Ejemplos: las direcciones:

  1080:0:0:0:8:800:200C:417A (una dirección unicast)

  FF01:0:0:0:0:0:0:101 (una dirección multicast)

  0:0:0:0:0:0:0:1 (la dirección loopback)

  0:0:0:0:0:0:0:0 (una dirección no especificada)

  Pueden representarse como:

  1080::8:800:200C:417A (una dirección unicast)

  FF01::101 (una dirección multicast)

  ::1 (la dirección loopback)

  :: (una dirección no especificada)

- Una forma alternativa y muy conveniente, cuando nos hallemos en un entorno mixto IPv4 e IPv6, es X:X:X:X:X:X:d:d:d:d, donde "X" representa los valores hexadecimales de 16 bits (6 porciones de mayor peso), y "d" representa los valores decimales de las 4 porciones de 8 bits de menor peso (representación IPv4 estándar).

  Ejemplos:

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

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

  Pueden representarse como:

  ::13.1.68.3

  :: FFFF:129.144.52.38

2.2.1.5 NOMENCLATURA DE PREFIJOS

La representación de los prefijos de direcciones con IPv6 es similar a la que tenemos con CIDR con IPv4 : dirección-ipv6/tamaño-prefijo.

Donde dirección-ipv6 es alguna de las notaciones vistas en la sección anterior y tamaño-prefijo es un valor decimal que especifica cuantos bits contiguos de la parte izquierda de la dirección corresponden al prefijo.

Por ejemplo, el prefijo de la UJI en hexadecimal es 3FFE33300002, que son 48 bits, lo podemos escribir como:

3FFE:3330:0002:0000:0000:0000:0000:0000/48
3FFE:3330:2:0:0:0:0:0/48
3FFE:3330:2::/48

Si queremos escribir la dirección y el prefijo, no hace falta que escribamos los dos de forma explícita. Por ejemplo, una dirección IPv6 de la misma UJI con su prefijo asociado quedaría 3FFE:3330:2:1:250:BAFF:FE7A:E67E/48.

2.2.1.6 RESERVAS DE ESPACIO DE DIRECCIONAMIENTO

A diferencia de las asignaciones de espacio de direccionamiento que se hicieron en IPv4, en IPv6, se ha reservado, que no "asignado", algo más del 15%, tanto para permitir una fácil transición (caso del protocolo IPX), como para mecanismos requeridos por el protocolo.

De esta forma se permite la asignación directa de direcciones de agregación directa de direcciones de agregación, direcciones locales, y direcciones multicast. Con reservas para OSI NSAP e IPX. El 85% restante queda reservado para uso futuro.

Podemos distinguir las direcciones multicast de las unicast por el valor de octeto de mayor orden de la dirección (FF, o 11111111 en binario, indica multicast). En cambio, en le caso de las anycast, no hay ninguna diferencia, sintacticamente hablando y por lo tanto, son tomadas del espacio de direcciones unicast.

Estado	Prefijo (en binario)	Fracción del Espacio
Reservado	0000 0000	1/256
No Asignado	0000 0001	1/256
Reservado para NSAP	0000 001	1/128
Reservado para IPX	0000 010	1/128
No Asignado	0000 011	1/128
No Asignado	0000 1	1/32
No Asignado	0001	1/16
Direcciones Unicast Globales Agregables	001	1/8
No Asignado	010	1/8
No Asignado	011	1/8
No Asignado	100	1/8
No Asignado	101	1/8
No Asignado	110	1/8
No Asignado	1110	1/16
No Asignado	1111 0	1/32
No Asignado	1111 10	1/64
No Asignado	1111 110	1/128
No Asignado	1111 1110 0	1/512
Direcciones Unicast Locales de Enlace	1111 1110 10	1/1.024
Direcciones Unicast Locales de Sitio	1111 1110 11	1/1.024
Direcciones Multicast	1111 1111	1/256

Tabla 4 - Reservas de direcciones

2.2.1.7 DIRECCIONES ESPECIALES EN IPv6

Se han definido también las direcciones para usos especiales como:

- Dirección de auto-retorno o LoopBack (::1) – No ha de ser asignada a una interfaz física; se trata de una interfaz "virtual", se trata de paquetes que no salen de la máquina que los emite; nos permite hacer un bucle para verificar la correcta inicialización del protocolo (dentro de una misma máquina).

- Dirección no especificada (::) – Nunca debe ser asignada a ningún nodo, ya que se emplea para indicar la ausencia de dirección; por ejemplo, cuando se halla en el campo de dirección fuente, indica que se trata de un host que está iniciándose, antes de que haya aprendido su propia dirección.

- Túneles dinámicos/automáticos de IPv6 sobre IPv4 (::<dirección IPv4>) – se denominan direcciones IPv6 compatibles con IPv4, y permiten la retrasmisión de tráfico IPv6 sobre infraestructuras IPv4, de forma transparente.

80 bits	16 bits	32 bits
0000 ... 0000	0000	dirección IPv4

- Representación automática de direcciones IPv4 sobre IPv6 (::FFFF:<dirección IPv4>) Permite que los nodos que sólo soportan IPv4, puedan seguir trabajando en redes IPv6. Se denominan "direcciones IPv6 mapeadas desde IPv4".

80 bits	16 bits	32 bits
0000 ... 0000	FFFF	Dirección IPv4

2.2.1.8 REPRESENTACIÓN DE LOS TIPOS DE DIRECCIONES

El tipo específico de cada dirección IPv6 viene dado por los primeros bits de ésta, dentro de lo que se llama el campo de formato de prefijo (FP, format prefix). El tamaño de este campo es variable. La asignación de estos prefijos se puede ver en la tabla 4.

Los prefijos desde 001 a 111 tienen la obligación de tener los identificadores de interfaz de 64 bits en formato EUI-64, excepto para las direcciones multicast (1111 1111). Las direcciones unicast se distinguen por el valor del octeto de mayor peso, que tiene algún valor distinto de '1'. Las direcciones anycast se asignan dentro del espacio de las anycast y no son distinguibles entre si observando sus bits.

Como se puede ver, hay mucho espacio no asignado (el 85%), lo que en un futuro permitirá expandir el espacio posible o incluso dar nuevos usos.

2.2.1.8.1 DIRECCIONES UNICAST LOCALES

La direcciones unicast, son agregables con máscaras de bits contiguos, similares al caso de IPv4, con CIDR. Como hemos visto, hay varias formas de asignación de direcciones unicast, y otras pueden ser definidas en el futuro.

Los nodos IPv6 pueden no tener ningún conocimiento o mínimo de la estructura interna de las direcciones IPv6, dependiendo se su misión en la red (por ejemplo, host frente a router). Pero como mínimo, un nodo debe considerar que las direcciones unicast (incluyendo la propia), no tienen estructura:

128 bits
Dirección del nodo

Un host algo más sofisticado, conocería el prefijo de la subred del enlace a que está conectado:

n bits	128-n bits
Prefijo de subred	identificador de interfaz

Dispositivos más sofisticados pueden tener un conocimiento más amplio de la jerarquía de red, sus límites, etc., en ocasiones dependiendo de la posición misma que el dispositivo o host/router, ocupa en la propia red.

El **identificador de interfaz** se emplea, por tanto, para identificar interfaces en un enlace, y deben ser únicos en dicho enlace. En muchos casos también serán únicos en un ámbito más amplio. Por lo general, el identificador de interfaz coincidirá con la dirección de la capa de enlace de dicha interfaz. El mismo identificador de interfaz puede ser empleado en múltiples interfaces del mismo nodo, sin afectar a su exclusividad global en el ámbito IPv6.

Se han definido dos tipos de direcciones unicast de uso local:

- Local de enlace (Link-Local): la direcciones locales de enlace han sido diseñadas para direccional un único enlace para propósitos de auto-configuración (mediante identificadores de interfaz), descubrimiento de vecindario, o situaciones en las que no

hay routers. Por tantos los encaminadores no pueden retransmitir ningún paquete con direcciones fuente o destino que sean locales de enlace (su ámbito está limitado a la red local). Tiene el siguiente formato:

10 bits	54 bits	64 bits
1111111010	0	Identificador de interfaz

Se trata de direcciones FE80::<ID de interfaz>/10

- Local de sitio (Site-Local): las direcciones locales de sitio permiten direccional dentro de un "sitio" local u organización, sin la necesidad de un prefijo global. Se configuran mediante un identificador de subred, de 16 bits. Los encaminadores no deben de retrasmitir *fuera del sitio* ningún paquete cuya dirección fuente o destino sea "Local de sitio" (su ámbito está limitado a la red local o de la organización).

10 bits	38 bits	16 bits	64 bits
1111111011	0	ID de subred	Identificador de interfaz

Se trata de direcciones FEC0::<ID de subred>:<ID de interfaz>/10

2.2.1.8.2 DIRECCIONES ANYCAST

Tal y como se ha indicado antes, las direcciones anycast tienen el mismo rango de direcciones que las unicast.

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

Existe una dirección anycast, requerida para cada subred que se denomina "dirección anycast del router de la subred" (Subnet-router anycast address). Su sintaxis es equivalente al prefijo que especifica el enlace correspondiente de la dirección unicast, siendo el indicador de interfaz igual a cero:

n bits	128-n bits
Prefijo de subred	0000000000000000000

Todos los router han de soportar esta dirección para las subredes a las que están conectados. Los paquetes enviados a la "dirección anycast del router de la subred", serán enviados a un router de la subred.

Una aplicación evidente de esta característica, a demás de la tolerancia a fallos, es la movilidad. Imaginemos nodos que se necesitan comunicarse con un router entre el conjunto de los dispositivos en su subred.

Dentro de cada subred, los 128 valores superiores de identificadores de interfaz están reservados para su asignación como direcciones anycast de la subred.

Las direcciones cuyos tres primeros bits (prefijo de formato) tienen valores entre 001 y 111 (excepto las de multicast, 1111 1111), indican con el bit "universal/local" igual a cero, que el identificador de interfaz tiene 64 bits, y por tanto no es globalmente único (es local). En este caso, las direcciones reservadas anycast de subred se constituyen del siguiente modo:

64 bits	57 bits	7 bits
Prefijo de subred	1111110111 ... 111	ID anycast
	Identificador de interfaz	

En el resto de los casos, el identificador de interfaz puede tener una longitud diferente de 64 bits, por lo que la construcción se realiza según el siguiente esquema:

n bits	121-n bits	7 bits
Prefijo de subred	1111111 ... 1111111	ID anycast
	Identificador de interfaz	

2.2.1.8.3 DIRECCIONES MULTICAST

Una dirección multicast en IPv6, puede definirse como un identificador para un grupo de nodos. Un nodo puede pertenecer a uno o varios grupos multicast.

Las direcciones multicast tienen el siguiente formato:

8	4	4	112 bits
11111111	000T	ámbito	Identificador de Grupo

El bit "T" indica, su valor es cero, una dirección multicast permanente, asignada únicamente por la autoridad de numeración global de Internet. En caso contrario, si su valor es uno, se trata de direcciones multicast temporales. Los 4 bits que le preceden, que por el momento están fijados a cero, están reservados para futuras actualizaciones.

Los bits "ámbito" tienen los siguientes:

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

Tabla 5 - Bits de ámbito

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

Por ejemplo, si asignamos una dirección multicast permanente, con el identificador de grupo 101 (hexadecimal), al grupo de los servidores de tiempo (NTS), entonces:

- FF01::101, significa todos los NTS en el mismo nodo que el paquete origen.
- FF02::101, significa todos los NTS en el mismo enlace que el paquete origen.
- FF05::101, significa todos los NTS en el mismo sitio que el paquete origen.
- FF0E::101, significa todos los NTS en Internet.

Las direcciones multicast no-permanentes, solo tienen sentido en su propio ámbito. Por ejemplo, un grupo identificado por la dirección temporal multicast local sitio FF15::101, no tiene ninguna relación con un grupo usando la misma dirección en otro sitio, ni con otro grupo temporal que use el mismo identificador de grupo (en otro ámbito), ni con un grupo permanente con el mismo identificador de grupos.

Las direcciones multicast no deben ser usadas como dirección fuente en un paquete IPv6, ni aparecer en ninguna cabecera de encaminamiento. Las principales direcciones multicast reservadas son las incluidas rango FF0x:0:0:0:0:0:0:0.

Algunos ejemplos útiles de direcciones multicast, según su ámbito, serían:

- FF01:0:0:0:0:0:0:1 Todos los nodos (ámbito local)
- FF02:0:0:0:0:0:0:1 Todos los nodos (ámbito de enlace)
- FF01:0:0:0:0:0:0:2 Todos los routers (ámbito local)
- FF02:0:0:0:0:0:0:2 Todos los routers (ámbito local)
- FF05:0:0:0:0:0:0:2 Todos los routers (ámbito sitio)

La dirección FF02:0:0:0:0:1:FFxx:xxxx, denominada “Solicited – Node Adress”, o dirección de nodo solicitada, permite calcular la dirección multicast a partir de la unicast o anycast de un determinado nodo. Para ello, se sustituyen los 24 bits de menor peso (“x”) por los mismos bits de la dirección original.

Así, la dirección 4037::01:800:200E:8C6C se convertirá en FF02::1:FF0E:8C6C.

Cada nodo debe calcular y unirse a todas las direcciones multicast que le corresponden para cada dirección unicast y anycast que tiene asignada.

2.2.1.9 DIRECCIONES REQUERIDAS PARA CUALQUIER NODO

Todos los nodos, en el proceso de identificación, al unirse a la red, deben de reconocer como mínimo, las siguientes direcciones:

- Sus direcciones locales de enlace para interfaz
- Las direcciones unicast asignadas
- Las direcciones de loopback
- Las direcciones multicast de todos los nodos
- Las direcciones multicast solicitadas para cada dirección unicast o anycast asignadas.
- Las direcciones multicast de todos los grupos a los que dicho host pertenece.

Además, en el caso de los routers, tienen que reconocer también:

- La dirección anycast del router de la subred, para las interfaces en las que está configurado para actuar como router.
- Todas las direcciones anycast con las que el router ha sido configurado.
- Las direcciones multicast de todos los routers
- Las direcciones multicast de todos los grupos a los que el router pertenece.

Además, todos los dispositivos con IPv6, deben tener, predefinidos los prefijos siguientes:

- Dirección no especificada
- Dirección de loopback
- Prefijo de multicast (FF)
- Prefijos de uso local (local de enlace y local de sitio)
- Direcciones multicast predefinidas
- Prefijos compatibles IPv4

Se deben asumir que todas las demás direcciones son unicast a no se que sean específicamente configuradas (por ejemplo las direcciones anycast).

2.2.1.10 FORMATO PARA LA REPRESENTACIÓN EN URL's

Cuando navegamos, continuamente aludimos a URL's, en muchas ocasiones sin conocer el significado precios de esta abreviatura.

La representación original, que data del año 1988, nos dice que Uniform Resource Locator (Localizador de recursos uniforme), es un medio simple y extensible para identificar un recurso a través de su localización en la red.

Una vez aclarado esto, y de la misma forma que en ocasiones usamos direcciones en formato IPv4 para escribir un URL, se han descrito unas normas para realizar la representación literal de dirección IPv6 cuando se usan herramientas de navegación WWW. El motivo por el que ha sido precio realizar esta definición es bien simple.

Con la anterior especificación no estaba permitido emplear el carácter ":" en una dirección, sino como separador de "Puerto". Por tanto, si se desea facilitar operaciones tipo "cortar y pegar", para trasladar direcciones entre diferentes aplicaciones, de forma rápida, era preciso buscar una solución que evitase la edición manual de direcciones IPv6.

La solución es bien sencilla: el empleo de los corchetes ("[","]") para encerrar la dirección IPv6, dentro de la estructura habitual del URL.

Veamos algunos ejemplos; las direcciones siguientes:

- FEDC:BA98:7654:3210:FEDC:BA98:7654:3210
- 1080:0:0:0:8:800:200C:4171
- 3ffe:2a00:100:7031::1
- 1080::8:800:200C:417ª
- ::192.9.5.5

- :FFFF:129.144.52.38
- 2010:836B:4179::836B:4179

Sería representadas como:

- http://[FEDC:BA98:7654:3210:FEDC:BA98:7654:3210]:80/index.html
- http://[1080:0:0:0:8:800:200C:417A]/index.html
- http://[3ffe:2a00:100:7031::1]
- http://[1080::8:800:200C:417A]/foo
- http://[::192.9.5.5]/ipng
- http://[::FFFF:129.144.52.38]:80/index.html
- http://[2010:836B:4179::836B:4179]

2.2.2 ICMP Y LOS MENSAJES DE ERROR

El protocolo de control de mensajes de INTERNET (INTERNET Control Message Protocol, **ICMP**) ya existía en la versión 4, y su principal objetivo es el de enviar mensajes entre dispositivos de encaminamiento como por los computadores para intercambiar información de miembros de grupo sobre una LAN (por ejemplo mensajes de error como destino desconocido o tiempo de respuestas excedido). También ha sido adaptado a la versión 6 del protocolo IP. Se han suprimido muchos servicios redundantes o no utilizados, se ha impuesto un formato fijo para facilitar su tratamiento por los routers y se le han añadido características como la extensión de las direcciones a 128 bits (ver figura 11). Todo esto lleva a que la nueva revisión del ICMP para la versión 6 del IP (numerada como 2) sea incompatible con la versión anterior (identificada como 1) para IP versión 4. El primer campo de *tipo* (Type) indica la versión del protocolo ICMP, en el caso de ser compatible con la versión 4 es 1, y si es compatible con la versión 6 es 2. El *código* (Code) hace referencia a la naturaleza del mensaje que transporta (ver figura 11). El *checksum* es una suma de control de los datos que se envían, de forma que se pueda verificar que son correctos. Finalmente el mensaje (Body Message) es de longitud variable y contiene los datos.

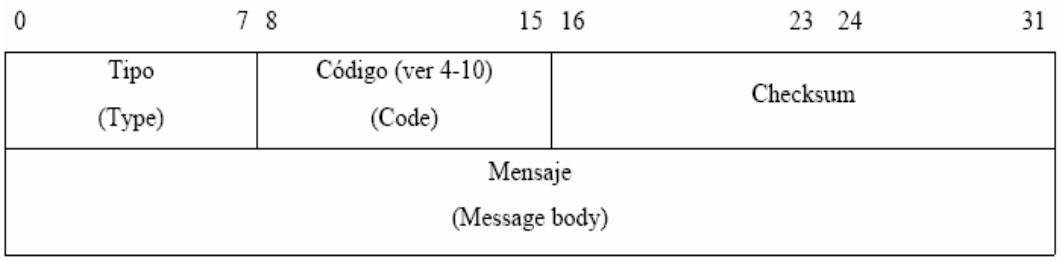


Figura 11 - Formato del ICMP versión 2 compatible con la versión 6 de IP

Codigo	Significado
1	Destino inalcanzable (Destination Unrechable).
2	Datagrama demasiado grande (Packet too big).
3	Tiempo de respuesta agotado (Time Exceeded).
4	Parámetros incorrectos (Parameter Problem).
128	Solicitud de ECHO (ECHO Request).
129	Respuesta a ECHO (ECHO reply).
133	Solicitud de router (Router Solicitation).
135	Solicitud de vecino (Neighbour Solicitation).

Figura 12 - Códigos más relevantes del ICMP versión 2

Tal y como hemos visto en los puntos anteriores, en el caso de que un router descarte un datagrama, envía un mensaje ICMP al propietario del datagrama notificando la causa del error. Los cuatro primeros códigos (ver figura 12) indican los motivos por los cuales un router descarta un datagrama. Esto obliga a que los routers no envíen mensajes ICMP ante datagramas dirigidos a más de un usuario a la vez (*multicast*) para evitar avalanchas de respuestas. De la misma manera tampoco se responde a datagramas de tipo ICMP para evitar bucles infinitos de respuestas de error.

Destacar finalmente que el código de mensaje 2, *datagrama demasiado grande* (Packet too big) es el mecanismo utilizado para el *cálculo del tamaño máximo* de datos (Maximun Transfer Unit, **MTU**) que el router puede soportar. Esto permite saber al emisor cual es el tamaño de datagrama máximo que puede enviar al destino sin peligro de que sea descartado por algún router intermedio, optimizando de esta forma la comunicación entre dos computadores por INTERNET. Como este parámetro depende del camino que tome el datagrama (y por lo tanto de todos y cada uno de los routers intermedios que atraviese) hasta su destino, permite de una forma fácil y eficiente optimizar la comunicación dinámicamente.

2.2.3 AUTOCONFIGURACIÓN

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

El proceso incluye la creación de una dirección de enlace local, verificación de que no está duplicada en dicho enlace y determinación de la información que ha de ser autoconfigurada (direcciones y otra configuración).

Las direcciones puedes obtenerse de forma totalmente manual, mediante **DHCPv6** (Stateful o configuración predeterminada), o de forma automática (Stateless o descubrimiento automático, sin intervención).

Este protocolo define el proceso de generar una dirección de enlace local, direcciones globales y locales de sitio, mediante el procedimiento automático (Stateless). También define el mecanismo para detectar direcciones duplicadas.

La autoconfiguración "Stateless" (sin intervención), no requiere ninguna configuración manual del host, configuración mínima (o ninguna) de Routers, y no precisa servidores adicionales. Permite a un host generar su propia dirección mediante una combinación de información disponible localmente e información anunciada por los Routers. Los Routers anuncian los prefijos que identifican la subred o subredes asociadas con el enlace, mientras el host genera un "identificador de interfaz", que identifica de forma única la interfaz en la subred. La dirección se compone por la combinación de ambos campos. En ausencia de Router, el host sólo puede generar la dirección de enlace local, aunque esto es suficiente para permitir la combinación entre nodos conectados al mismo enlace.

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

Ambos tipos de tipos de autoconfiguración (Stateless y Stateful), se complementan. Un host puede usar autoconfiguración sin intervención (Stateless), para generar su propia dirección, y obtener el resto de parámetros mediante autoconfiguración predeterminada (Stateful).

El mecanismo de autoconfiguración "sin intervención" se emplea cuando no importa la dirección exacta que se asigna a un host, sino tan solo asegurarse que es única y correctamente enrutable.

El mecanismo de autoconfiguración predeterminada, por el contrario, nos asegura que cada host tiene una determinada dirección, asignada manualmente. Cada dirección es cedida a una interfaz durante un tiempo predefinido (posiblemente infinito). Las direcciones tienen asociado un tiempo de vida, que indican durante cuanto tiempo esta vinculada dicha dirección a una determinada interfaz. Cuando el tiempo de vida expira, la vinculación se invalida y la dirección puede ser reasignada a otra interfaz en cualquier punto de Internet.

Para gestionar la expiración de los vínculos, una dirección pasa a través de dos fases diferentes mientras está asignada a una interfaz. Inicialmente, una dirección es "preferred" (preferida), lo que significa que su uso es arbitrario y no está restringido. Posteriormente, la dirección es "deprecated" (desaprobada), en anticipación a que el vínculo con su interfaz actual va a ser anulado.

Mientras está en estado "desaprobado", su uso es desaconsejado, aunque no prohibido. Cualquier nueva comunicación (por ejemplo, una nueva conexión TCP), de usar una dirección "preferida", siempre que sea posible.

Una dirección "desaprobada" debería ser usada tan solo por aquellas aplicaciones que ya la venían utilizando y a las que les es muy difícil cambiar a otra dirección sin interrupción del servicio.

Para asegurarse de que todas las direcciones configuradas son únicas, en un determinado enlace, los nodos ejecutan un algoritmo de detección de direcciones duplicadas, antes de asignarlas a una interfaz. Este algoritmo es ejecutado para todas las direcciones,

independientemente de que hayan sido obtenidas mediante autoconfiguración Stateless o Stateful.

La autoconfiguración está diseñada para host, no para Routers, aunque ello no implica que parte de la configuración de los Routers también pueda ser realizada automáticamente (generación de direcciones de enlace local). Además, los Routers también tienen que aprobar el algoritmo de detección de direcciones duplicadas.

2.2.3.1 AUTOCONFIGURACION STATELESS (SIN INTERVENCIÓN O DESCUBRIMIENTO AUTOMATICO)

El procedimiento de autoconfiguración Stateless (sin intervención o descubrimiento automático), ha sido diseñado con las siguientes premisas:

- Evitar la configuración manual de dispositivos antes de su conexión a la red. Se requiere, en consecuencia, un mecanismos que permita a los host obtener o crear direcciones únicas para cada una de sus interfaces, asumiendo que cada interfaz puede proporcionar un identificador único para si misma (identificador de interfaz). En el caso más simple, el identificador de interfaz consiste en la dirección de la capa de enlace, de dicha interfaz. El identificador de interfaz puede ser combinado con un prefijo, para formar la dirección.

- Las pequeñas redes o sitios, con máquinas conectadas a un único enlace, no deberían requerir la presencia de un servidor "Stateful" o Router, como requisito para comunicarse. Para obtener, en este caso, características "Plug & Play", empleamos las direcciones de enlace local, dado que tienen un prefijo perfectamente conocido que identifica el único enlace compartido, al que se conectan todos los nodos. Cada dispositivo forma su dirección de enlace local a su identificador de interfaz.

- En el caso de redes o sitios grandes, con múltiples subredes y Routers, tampoco se requiere la presencia de un servidor de configuración de direcciones "Stateful", ya que

los host han de determinar, para generar sus direcciones globales o de enlace local, los prefijos que identifican las subredes a las que se conectan. Los Routers generan mensajes periódicos de anunciación, que incluyen opciones como listas de prefijos activos en los enlaces.

- La configuración de direcciones debe facilitar la remuneración de los dispositivos de un sitio, por ejemplo, cuando se desea cambiar de proveedor de servicios. La remuneración se logra al permitir que una misma interfaz pueda tener varias direcciones, que recibe "**en préstamo**". El tiempo del "**préstamo**" es el mecanismo por el por el que se renuevan las direcciones, al expirar los plazos para las viejas, sin que se conceda una prórroga. Al poder disponer de varias direcciones simultáneamente, permite que la transición no sea "disruptora", permitiendo que ambas, la vieja y la nueva dirección den continuidad a la comunicación durante el periodo de transición.

- Sólo es posible utilizar este mecanismo en enlaces capaces de funciones multicast, y comienza, por tanto, cuando es iniciada o activada una interfaz que multicast.

- Los administradores de sistemas necesitan la habilidad de especificar los mecanismos (stateless, stateful, o ambos), deben ser usados. Los mensajes de anunciación de los routers incluyen indicadores para esta función.

Los pasos básicos para la autoconfiguación, una vez la interfaz ha sido activada, serían:

a) Se genera la dirección "tentativa" de enlace local, como se ha descrito antes.
b) Verificar que dicha dirección "tentativa" puede ser asignada (no está duplicada en el mismo enlace).
c) Si está duplicada, la autoconfiguración se detiene, y se requiere un procedimiento manual (por ejemplo, usando otro identificador de interfaz)
d) Si no está duplicada, la conectividad a nivel IP se ha logrado, al asignarse definitivamente dicha dirección "tentativa" a la interfaz en cuestión.
e) Si se trata de un host, se interroga a los posibles routers para indicar al host lo que debe de hacer a continuación.

f) Si no hay routers, se invoca el procedimiento de autoconfiguración "stateful".
g) Si hay routers, estos contestarán indicando fundamentalmente, como obtener las direcciones si se ha utilizar el mecanismo "stateful", u otra información, como tiempos de vida, etc.

2.2.3.2 AUTOCONFIGURACIÓN STATEFUL (PREDETERMINADA)

DHCP para IPv6 es un protocolo UDP cliente/servidor, diseñado para reducir el coste de gestión de nodos IPv6 en entornos donde los administradores precisan un control sobre la asignación de recursos de la red, superior al facilitados por el mecanismo de configuración "statless".

Se pueden utilizar ambos mecanismos pueden usarse de forma concurrente para reducir el coste de propiedad y administración de la red.

Para lograr este objetivo, se centraliza la gestión de los recursos de la red tales como direcciones IP, información de encaminado, información de instalación de Sistemas Operativos, información de servicios de directorios, sobre uno o varios servidores DHCP, en lugar de distribuir dicha información en ficheros de configuración locales en cada nodo.

Además, DHCP ha sido diseñado para ser fácilmente extensible con nuevos parámetros de configuración, a través de "extensiones" que incorporan esta nueva información.
Los objetivos de DHCPv6 son:

- DHCP es un mecanismo, no una política. La política es establecida por el administrador de la red y DHCP le permite propagar los parámetros adecuados, según dicha política.
- DHCP es compatible, lógicamente, con el mecanismo de autoconfiguración.
- DHCP no requiere configuración manual de parámetros de red en clientes DHCP, excepto en casos donde dicha configuración se requiere debido a medidas de seguridad.

- DHCP no requiere un servidor en cada enlace, dado que debe funcionar a través de relés DHCP.
- DHCP, coexiste con nodos configurados estáticamente, así como con implementaciones existentes en la red.
- Los clientes DHCP pueden operar en enlaces donde no hay routers IPv6.
- Los clientes DHCP proporcionan la habilidad de remunerar la red.
- Un cliente DHCP puede hacer múltiples y diferentes peticiones de parámetros de configuración, de uno o varios servidores DHCP simultáneamente. DHCP proporciona suficiente información para permitir a los servidores DHCP el seguimiento del estado de configuración de los clientes.
- DHCP incorpora los mecanismos apropiados de control de tiempo y retrasmisiones para operar eficazmente en entornos con una alta latencia y/o reducido ancho de banda.

Los cambios fundamentales entre DHCPv4 y DHCPv6, están basados en soporte inherente del formato de direccionamiento y autoconfiguración IPv6; son las siguientes:

- La dirección de enlace local permite a un nodo tener una dirección tan pronto como arranca, lo que significa que todos los clientes tienen una dirección IP fuente para localizar un servidor o relé en su mismo enlace.
- Los indicaros de incompatibilidad BOOTP y broadcast han desaparecido.
- El multicast y los ámbitos de direccionamiento permiten el diseño de paquetes de descubrimiento, que definen por si mismos su rango por la dirección multicast, para la función requerida.
- La autoconfiguración stateful ha coexistir e integrarse con la stateless, soportando la detección de direcciones duplicadas y los dos tiempos de vida IPv6, para facilitar la remuneración automática de direcciones y su gestión.
- Se soportan múltiples direcciones por cada interfaz.
- Algunas opciones DHCPv4 ya no son precisas, debido a que los parámetros de configuración se obtienen a través de ND o del producto de localización de servicios.

De esta forma, se soportan las siguientes funciones nuevas:

- Configuración de actualizaciones dinámicas de DNS.

- Desaprobación de direcciones, para renumeración dinámica.
- Relés preconfigurados con direcciones de servidores, o mediante multicast.
- Autenticación
- Los clientes pueden pedir múltiples direcciones IP
- Las direcciones pueden se reclamadas mediante el mensaje de "iniciar-reconfiguración".
- Integración entre autoconfiguración de direcciones "stateless" y "stateful".
- Permitir relés para localizar servidores fuera del enlace.

2.2.4 EXTENSIONES DE SEGURIDAD IPSec

2.2.4.1 LA SEGURIDAD EN EL PROTOCOLO IP

Debido al carácter científico que en un principio tuvo INTERNET, la seguridad no fue contemplada históricamente en ninguna de las capas que forman la estructura TCP/IP. Con el auge de las tecnologías de la información y el aumento de personas y empresas conectadas a INTERNET, la necesidad de seguridad se fue convirtiendo en una necesidad. Además la proliferación de noticias sobre personas sin escrúpulos dedicadas a la piratería en INTERNET, creó un gran malestar social debido a la sensación de inseguridad por los ataques que sufrían tanto las empresas (bancos, universidades e incluso instituciones como la NASA) como los usuarios (utilización ilícita de números de tarjetas de crédito.).

La tardía reacción de las instituciones encargadas de la creación y modificación de los protocolos de INTERNET, propició la aparición de diferentes soluciones comerciales (SSL, SET...) para que los usuarios pudieran disfrutar de una seguridad que INTERNET no proporcionaba.

Aprovechando la necesidad de adaptar los diferentes protocolos al crecimiento de INTERNET, se optó por introducir una serie de especificaciones para garantizar la seguridad como parte implícita de las nuevas especificaciones de los protocolos. Estas especificaciones se conocen como IP Security o **IPSec**.

Una vez que se había consensuado la necesidad de introducir especificaciones de seguridad como parte intrínseca de los protocolos y no como simples extensiones voluntarias para los fabricantes de software (como pasó con la versión 5), se planteó un duro debate sobre que capa sería la idónea para proporcionar esta seguridad. Esta decisión era crítica, ya que en el mercado ya existían diferentes soluciones comerciales (SSL, SET...) que proporcionaban distintos grados de seguridad en la capa de usuario.

Finalmente para evitar duplicidades y asegurar un sistema seguro y auténtico en todas las capas, se optó por incluir las especificaciones en el nivel más bajo de la pila (Stack) de protocolos, en la especificación del protocolo IP versión 6.

2.2.4.2 LAS ESPECIFICACIONES IPSec

Las especificaciones IPSec han sido definidas para trabajar en la capa inferior de la pila (Stack) de protocolos TCP/IP, funcionando por lo tanto en el nivel de datagrama y siendo independientes del resto de protocolos de capas superiores (TCP, UDP...).

La seguridad en IPSec se proporciona mediante dos aspectos de seguridad (Security Payload):

1. **Cabecera de autenticación** (Authentication Header, **AH**). Esta cabecera es la encargada de proporcionar autenticidad a los datos (datagramas) que se reciben en dos aspectos:
   - Los datagramas provienen del origen especificado. Se garantiza la autenticidad del origen de los datos (no pueden ser repudiados).
   - Los datagramas (y por tanto los datos que contienen) no han sido modificados.

2. **Cifrado de seguridad** (Encrypted Security Payload, **ESP**). De esta forma se garantiza que tan sólo el destinatario legítimo del datagrama (datos) pueda descifrar el contenido del datagrama.

La autenticidad y el cifrado de datos (o datagramas) requieren que tanto el emisor como el receptor compartan una clave, un algoritmo de cifrado/descifrado y una serie de parámetros (como el tiempo de validez de la clave) que diferencian una comunicación segura de otra. Estos parámetros conforman la **asociación de seguridad** (Security Association, SA) que permite unir la autenticidad y la seguridad en IPSec.

En un computador con múltiples conexiones (consultar el correo mientras se baja un fichero por FTP y se consulta el saldo bancario...) podemos tener varias asociaciones de seguridad (como mucho una por conexión). Para poder diferenciar entre ellas utilizaremos un **índice de parámetros de seguridad** (Security Parameter Index, SPI) que nos permitirá al recibir un datagrama saber a que asociación de seguridad hace referencia, y de esta forma poder autenticarlo y/o descifrarlo.

Al iniciar una comunicación que utilice los servicios IPSec con un único destino (direcciones unicast) este nos debe comunicar a que índice de parámetros de seguridad (SPI) debemos hacer referencia. Análogamente en una comunicación con varios destinos (direcciones multicast o anycast) todos los destinatarios deben compartir el mismo número de índice (SPI).

AH y ESP permiten dos modos de uso modo de trasporte y modo túnel:

Modo Transporte: se asegura (encripta/autentica) la carga de datos del datagrama (PDU de transporte). Se establece entre nodos extremos de la red.

Modo túnel: se asegura (encripta/autentica) el datagrama completo → Túnel seguro en la red. Se establece entre nodos intermedios/externos de la red. Las direcciones origen y destinos se modifican con las de los nodos intermedios que implementan IPsec.

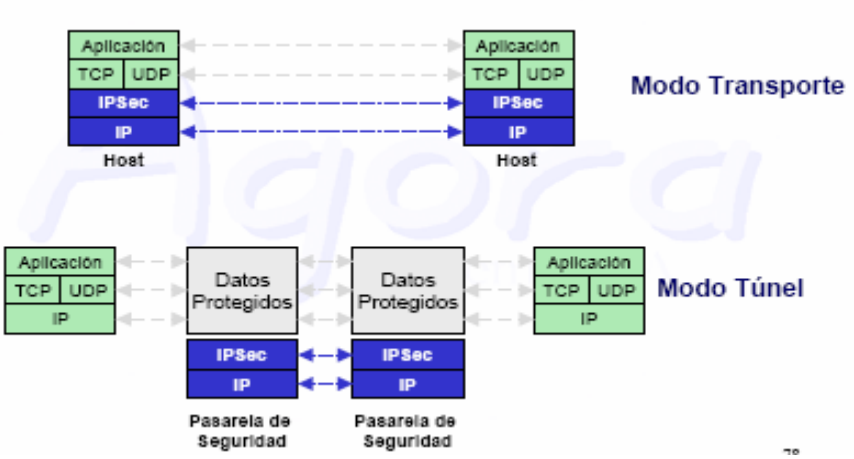


Figura 13 - Modos de Autenticación

2.2.4.2.1 LA CABECERA DE AUTENTICACIÓN (AH)

La **cabecera de autenticación** (Authentication Header, AH) es una cabecera específica de la versión 6 de IP (ver figura 15) y se designa con el número 51 (figura 16). Se suele situar justo antes de los datos, de forma que los proteja de posibles atacantes. No obstante ha sido diseñada de forma muy versátil, pudiendo incluirse antes que otras cabeceras (cabecera de opciones, cabecera de encaminamiento...) para asegurar así que las opciones que acompañan al datagrama son correctas. De esta forma, la presencia de una cabecera de autenticación no modifica el funcionamiento de los protocolos de nivel superior (TCP, UDP...) ni el de los routers intermedios, que simplemente encaminan el datagrama hacia su destino.

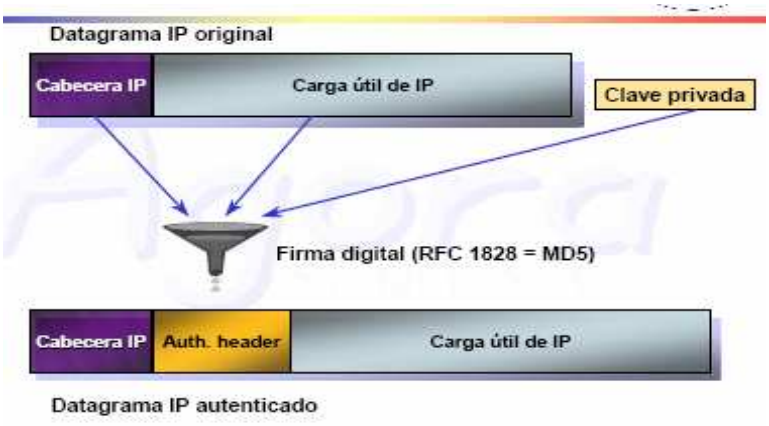


Figura14 - Cabecera de Autenticación AH

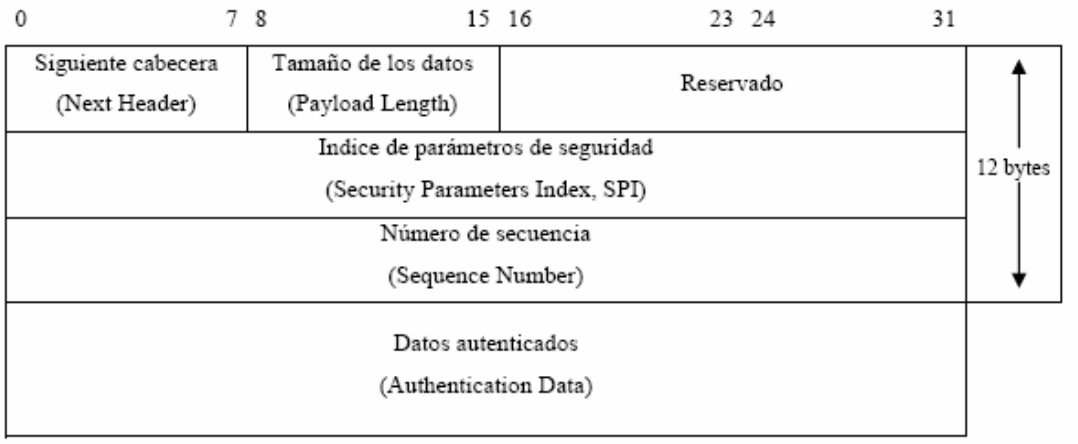


Figura 15 - Esquema de la cabecera de autenticación (AH)

Valor decimal	Abreviatura (keyword)	Descripción
0	HBH	Opciones entre saltos
4	IP	IP en IP (encapsulación en IPv4)
5	ST	Stream
6	TCP	Transmission Control Protocol
17	UDP	User Datagram Protocol
51	AH	Authentication Header
52	ESP	Encrypted Security Payload
59	NULL	No Next Header
60	DO	Destination Options Header
194	JBGR	Jumbogram

Figura 16 - Muestra de algunos valores para los tipos de cabecera en IP versión 6

El **tamaño de los datos** (Payload Length) especifica la longitud de los datos en palabras de 32 bits (4 bytes).

El **índice de parámetros de seguridad** (SPI) es un número de 32 bits, lo que nos permite tener hasta 2^32 conexiones de IPSec activas en un mismo computador.

El **número de secuencia** (Sequence Number) identifica el número del datagrama en la comunicación, estableciendo un orden y evitando problemas de entrega de datagramas fuera de orden o ataques externos mediante la reutilización (Replay Attacks) de datagramas.

Los **datos autenticados** (Authentication Data) se obtienen realizando operaciones (depende del algoritmo de cifrar escogido) entre algunos campos de la cabecera IP, la clave secreta que comparten emisor y receptor y los datos enviados.

El principal problema al autenticar un datagrama es que algunos campos son modificados por los routers intermedios (como el alcance del datagrama, que se va decrementando en una unidad cada vez que pasa por un router para evitar bucles infinitos), esto hace imposible poder autenticar todo el datagrama, ya que durante su camino por INTERNET es modificado. El cálculo de los datos autenticados se realiza mediante un algoritmo de Hash (actualmente se sugiere el algoritmo [6]MD5 que calcula un checksum de 128 bits).

2.2.4.2.2 LA CABECERA DE CIFRADO DE SEGURIDAD (ESP)

La cabecera de autenticación (AH) no modifica los datos que transporta, circulando el texto en claro (Clear Text), simplemente les añade autenticidad (al origen y al contenido). De esta forma, los datos que circulan pueden ser interceptados y visualizados por un eventual atacante.

Esto puede sernos útil por ejemplo cuando consultamos un documento oficial (BOE o las bases de unas oposiciones en la universidad...) ya que debe ser público y no tiene sentido cifrarlo, aunque si es básico que sea auténtico.

En el caso de necesitar confidencialidad (por ejemplo en consultas a un banco, no interesa que una tercera persona tenga acceso a nuestro saldo) se debe utilizar la **cabecera de cifrado de seguridad** (Encrypted Security Payload, **ESP**).

La **cabecera de cifrado de seguridad** (ver figuras 17 y 18) es siempre la última en el sistema de cabeceras en cadena (*Daisy Chain*). Esto es debido a que a partir de ella todo los datos vienen cifrados, con lo que los routers intermedios no podrían procesar las cabeceras posteriores.

[6] Es un algoritmo que utiliza bloques de entrada de 512 bits y retorna una salida de 128 bits.

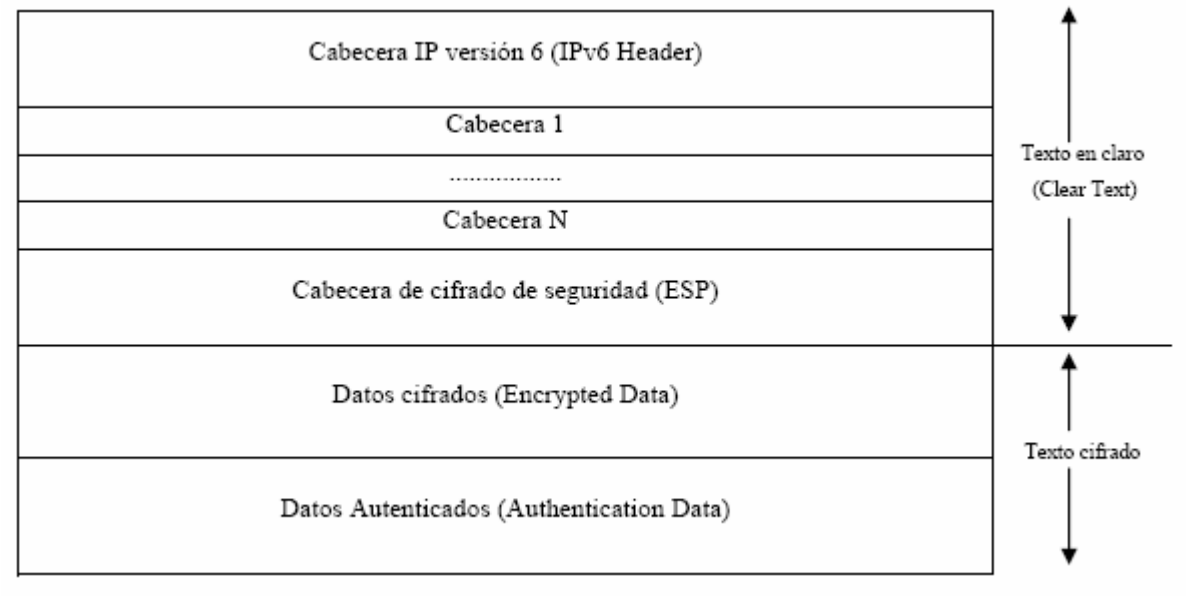


Figura 17 - Situación de la cabecera de cifrado de seguridad (ESP)

Al igual en con la cabecera de autenticación (AH), el algoritmo a utilizar se negocia con el receptor de la información antes de enviar un datagrama cifrado. Actualmente se propone e DES-CBC que es el algoritmo DES funcionado el modo de bloque CBC.

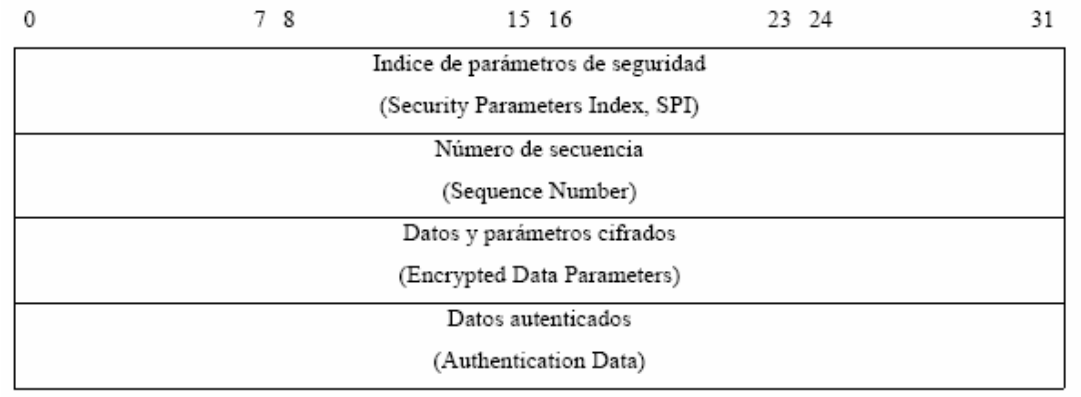


Figura 18 - Esquema de la cabecera de cifrado de seguridad (ESP)

A diferencia de la cabecera de autenticación (AH) no es necesario especificar el tamaño de los datos cifrados, ya que a partir de la cabecera de cifrado hasta el final del datagrama todo esta cifrado.

El **índice de parámetros de seguridad** (SPI) y el **número de secuencia** (Sequence Number) tienen el mismo significado que en la cabecera de autenticación (AH).

Los **datos autenticados** (Authentication Data) aseguran que el texto cifrado no ha sido modificado utilizando un algoritmo de Hash (depende del algoritmo de cifrar escogido).

Debido a que tanto la cabecera de autenticación (AH) como la cabecera de cifrado de seguridad (ESP) pueden ser utilizadas independientemente, se recomienda que en el caso de ser necesario tanto la autenticidad como la privacidad se incluya la cabecera de cifrado tras la de autenticación. De esta forma autenticamos los datos cifrados.

- **Modo transporte ESP:** el modo transporte proporciona protección principalmente a los protocolos de las capas superiores. Es decir. La protección del modo trasporte se extiende sea la carga útil de un paquete IP. Para IPv6 la carga útil son los datos que siguen la cabecera IP y cualquier cabecera de extensión que esté presente, con la posible excepción de la cabecera de las opciones para el destino, que se podría incluir en la protección.

  ESP en modo transporte cifra y opcionalmente autentifica la carga útil de IP pero no la cabecera IP.
  AH en modo trasporte autentifica la carga útil de IP y porciones seleccionadas de la cabecera IP.

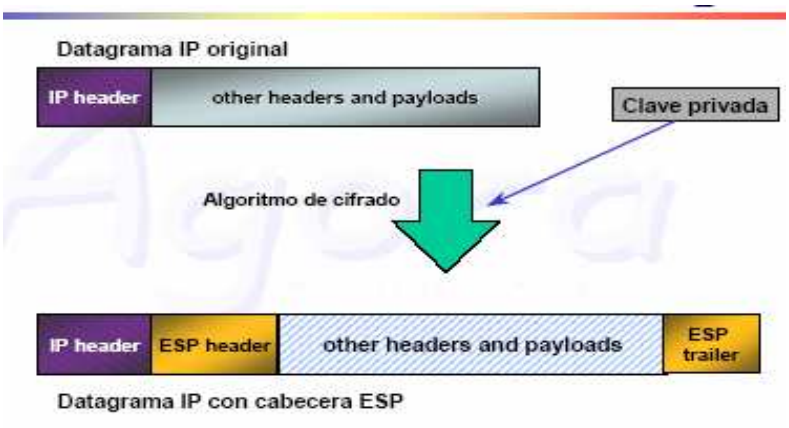


Figura 19 - IPsec ESP en modo transporte

- **Modo Túnel ESP:** el modo túnel proporciona protección al paquete IP entero. Para alcanzar esto, después de que los campos AH o ESP se han incorporado al paquete IP, el paquete entero más un campo de seguridad se tratan como la carga útil de un paquete IP "exterior" nuevo con la cabecera IP exterior nueva. El paquete original entero, o interior, viaja a través del túnel desde el punto de la red IP a otro, ningún dispositivo de encaminamiento a lo largo del camino es capaz de examinar la cabecera IP interior. El modo túnel se utiliza cuando uno o ambos extremos de una SA [7](Security Association), es pasarela (gateway) de seguridad, como un contrafuego (firewall) o un dispositivo de encaminamiento que implementa IPsec.

ESP en modo túnel cifra y opcionalmente autentifica al paquete IP interior completo, incluyendo la cabecera IP interior. AH túnel autentifica al paquete IP interior complejo y porciones seleccionadas de la cabecera IP exterior.

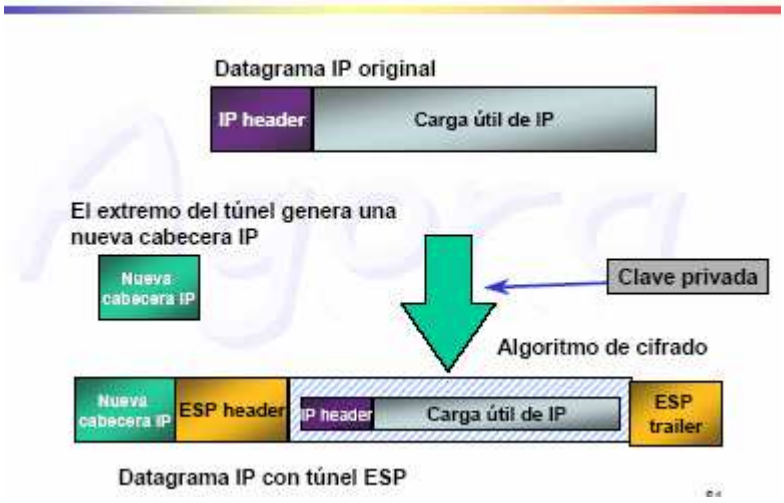


Figura 20 - IPsec ESP modo túnel

[7] Es una relación en un solo sentido entre un emisor y un receptor que proporciona servicios de seguridad al tráfico que se trasporta

2.2.4.2.3 PROTOCOLO ISAKMP

El protocolo **ISAKMP** (INTERNET Security Association Key Management Protocol) parece ser el escogido para el intercambio de claves y parámetros de seguridad en IPSec. No obstante, debido a que aún se encuentra en fase experimental, no se puede asegurar que finalmente este sea el elegido, ya que varios algoritmos han sido propuestos durante los últimos años (SKIP, Phouturis, Oakley...).

ISAKMP es un protocolo que proporciona la infraestructura necesaria para la negociación de asociaciones de seguridad (SA) entre dos usuarios cualesquiera (ver figura 5-4). Definiremos una **transacción de configuración** (Configuration Transaction) como un doble intercambio dónde el emisor realiza un envío/petición (Set/Request) y el receptor contesta mediante un reconocimiento de petición/respuesta (Acknowledge/Reply).

De esta forma a un envío (Set) le corresponde un reconocimiento de envío (Acknowledge) y a una petición (Request) una respuesta (Reply).

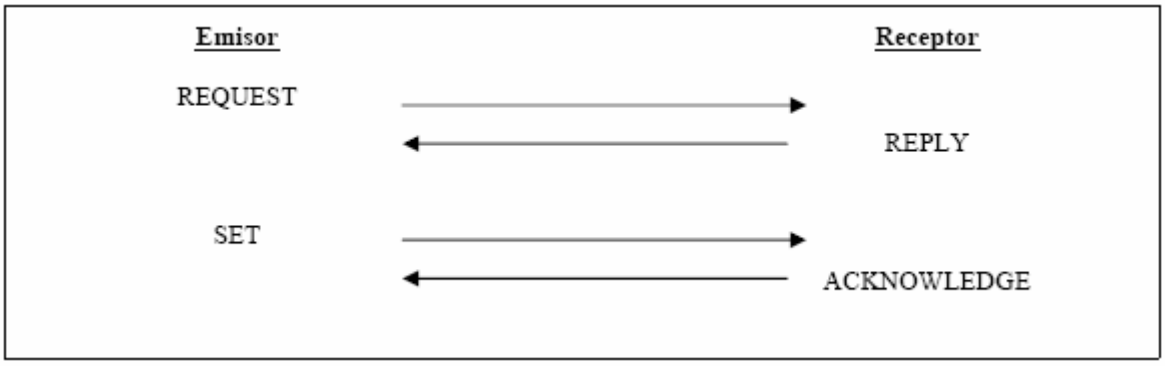


Figura 21 - Esquema de una transacción de configuración

El inicio de la comunicación siempre es precedido de una transacción de configuración dónde se intercambian dos *cookies* (Request/Reply). Este esquema permite evitar ataques de denegación de servicio (DOS) ya que hasta que no recibamos la respuesta el esquema no continúa. Posteriormente se producen los intercambios de información necesarios mediante envíos/reconocimientos de envío (Set/Acknowledge) dónde se negocian los diferentes

parámetros de seguridad (SPI, clave común, tiempo de validez de la clave, algoritmo de cifrado a utilizar...) que gobernaran la comunicación.

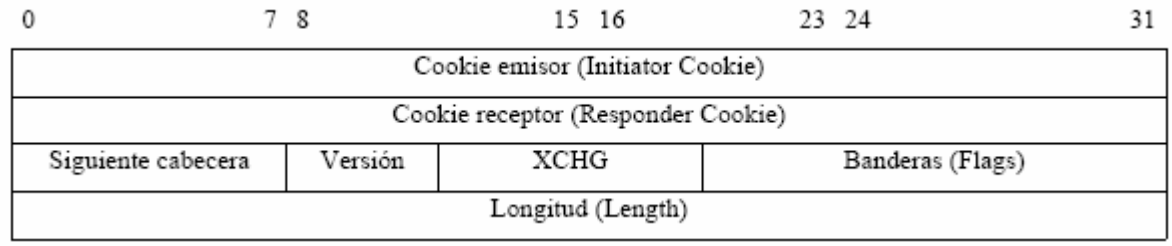


Figura 22 - Formato de la cabecera del ISAKMP

El intercambio de claves entre el emisor y el receptor se realiza utilizando el algoritmo de [8]Diffie-Hellman. En el caso de direcciones multicast (varios emisores/receptores en una misma comunicación) el algoritmo anterior resulta ineficiente, ya que está pensado para un emisor y un receptor. La solución adoptada es la de confiar en computadores servidores de claves.

2.2.4.2.4 EL PROTOCOLO IKE

El protocolo **IKE** (INTERNET Key Exchange) es un protocolo de dos fases para el establecimiento de un canal auténtico y seguro entre dos usuarios (Peers). Este protocolo utiliza la infraestructura de mensajes del protocolo ISAKMP para el intercambio de mensajes.

- **Fase1:** Se negocian las asociaciones de seguridad (SA). Se utiliza el protocolo Diffie-Hellman para el intercambio de una clave común y se establece el algoritmo de cifrado (3DES-CBC...), el algoritmo de Hash (MD5...) y del sistema de autenticación.

- **Fase2:** Una vez establecidos los distintos parámetros iniciales (SA) y aprovechando la seguridad de la fase 1, se inicia un modo rápido (Quick Mode) dónde se vuelven a negociar asociaciones de seguridad (SA) con el objetivo de evitar ataques de reutilización (Replay) de los datagramas de la fase 1 por un atacante.

[8] Algoritmo para el intercambio de una clave entre dos usuarios. Se puede lograr que dos personas compartan una misma clave de forma segura. No proporciona ni autenticación ni cifrado.

Esta combinación de algoritmos permite mantener una comunicación auténtica y privada entre dos usuarios (Peers), el problema principal radica en su complejidad, ya que pese a ser muy flexible (permite distintos métodos de autenticación y utilización de firmas digitales) es difícil su implementación práctica.

Además deja sin resolver el problema de comunicaciones seguras entre varios usuarios, ya que realizar este algoritmo entre todos ellos resulta en un alto coste de intercambio de datagramas.

De esta forma para grupos (multicast o anycast) se debe utilizar un esquema dónde un servidor de claves (que debemos suponer seguro) sincroniza la clave común a todos los componentes del grupo.

2.2.5 CALIDAD DE SERVICIO QoS

Con la implantación de calidad de servicio (QoS), es posible ofrecer más garantía y seguridad para las aplicaciones avanzadas, una vez que el tráfico de estas aplicaciones pasa a tener prioridad en relación con aplicaciones tradicionales.

Con el uso del QoS los paquetes son marcados para distinguir los tipos de servicios y los enrutadores son configurados para crear filas distintas para cada aplicación, de acuerdo con las prioridades de las mismas. Así, una faja de ancho de banda, dentro del canal de comunicación, es reservada para que, en el caso de congestionamiento, determinados tipos de flujos de datos o aplicaciones tengan prioridad en la entrega.

La QoS es una de las claves de Internet 2, porque permitirá, por ejemplo, dar más prioridad a una videoconferencia entre dos médicos que están tratando a un paciente en una complicada operación y tomar menos ancho de banda para el acceso a la Web o el correo electrónico.

Por el momento lo más difícil del reparto de prioridades esta en la tarificación de las mismas, ya que todavía se tiene que desarrollar la forma en que los proveedores de acceso puedan cobrar en un momento dado por coger un ancho de banda más grande y, acto pues, reducir la tarifa porque no se necesita tanto.

Antes de dar una definición de Calidad de servicio veamos los que es las Calidad y los que es el servicio:

- **CALIDAD:** Proceso de entrega de datos de manera fiable y/o "mejor de lo normal". En general hacer un uso eficiente de los recursos de la red.

- **SERVICIO**: Algo ofrecido al usuario final de la red. Por ejemplo la comunicación extremo a extremo, aplicaciones cliente/servidor, transporte de datos, etc.

En términos generales, puede definirse la Calidad del Servicio (QoS) como la capacidad que tiene un sistema de asegurar, con un grado de fiabilidad preestablecido, que se cumplan los

requisitos de tráfico, en términos de perfil y ancho de banda, para un flujo de información dado.

Más específicamente, para el caso de proveedores de red, un Servicio define algunas características significativas de la transmisión de un paquete en una dirección, a través de un conjunto de una o más rutas dentro de la red. Estas características pueden especificarse en términos de caudal (throughput), demora (delay), variación de demora (jitter) y/o pérdidas, o también en términos de alguna prioridad relativa de acceso a los recursos de la red.

2.2.5.1 ARQUITECTURAS DE QoS

Se denominan arquitecturas de QoS a aquellas que la ofrecen. Podemos distinguir dos modelos:

- Arquitectura de Servicios Integrados (ISA): en ella, la aplicación enmarca su solicitud de servicio dentro de un Protocolo de Reserva de Recursos (RSVP), y entonces pasa esta su solicitud a la red. En este modelo, cada estación o router en el camino de los datos debe manejar las peticiones de reservas y luego debe asociar una espera al flujo requiriendo la reserva. Por medio de este método, la QoS puede ser garantizada, pero los "Servicios Integrados" son complejos de implementar y pueden generar mucho tráfico de señalización. Este exceso de tráfico de señalización lleva a una pobre escalabilidad para el modelo de Servicios Integrados.

- Arquitectura de Servicios Diferenciados (DiffServ): se basa en la separación de los conceptos básicos de operación de los encaminadores de reenvío (forwarding) y control (encaminamiento). En el reenvío se realiza un tratamiento diferenciado de los datagramas (PHB), de acuerdo con la clase de tráfico. La interacción entre la red y la aplicación toma la forma de una solicitud de servicio sin negociación previa, en la que la aplicación solicita un servicio marcando cada paquete con un código que indica el servicio deseado. Es más simple que la ISA y se escala mejor.

2.2.5.2 PROTOCOLO DE RESERVA DE RECURSOS (RSVP)

La clave de RSVP es reservar recursos en cada nodo por donde transitarán los paquetes o flujos de datos. Concepto de **soft state.**

El **soft state** son los estados en los router y hosts extremos, refrescados por los mensajes *Path* y *Resv*. Una aplicación solicita participar en una sesión RSVP como emisor, enviando un mensaje *Path* en el mismo sentido que el flujo de datos, por las rutas uni/multicast proporcionadas por el protocolo de routing. A la recepción de este mensaje, el receptor transmite un mensaje *Resv*, dirigido hacia el emisor de los datos, siguiendo exactamente el camino inverso al de los mismos, en el cual se especifica el tipo de reserva a realizar en todo el camino.

En general, sin especificar tipos de QoS un mensaje *Path*, contiene:

- Sender Template: Parámetro por el cual se describe el formato de los paquetes que el emisor generará
- Sender Tspec: Describe el tráfico que la aplicación estima que generará.
- Adspec: Información sobre la QoS y propiedades de la aplicación
- Dirección del PHOP: Necesaria para poder encaminar los mensajes Resv.

Caracteristicas:

- En RSVP, los receptores hacen las reservas de QoS.
- La reserva es realizada por flujo.
- RSVP es un protocolo de **señalización**.
- RSVP debe mantener en cada nodo los requerimientos de reserva. Se define el **soft state.**
- RSVP utiliza un conjunto de mensajes de señalización para mantener el **soft state.**
- Merging: En los diferentes nodos que se van atravesando en la red por el camino de datos, se va realizando un proceso de concentración de los diferentes mensajes de petición de reservas
- Estado de reserva en cada nodo: El estado soft RSVP se crea y refresca periódicamente por mensajes *Path* y *Resv*.

- Estilos de reserva: Una petición de reserva incluye un conjunto de opciones que se conocen como el estilo de reserva. Las distintas combinaciones de estas opciones conforman los tres estilos de reserva en uso, *Wildcar-Filter* (WF), *Fixed-Filter* (FF) y *Shared-Explicit* (SE) (Ver figura 26).

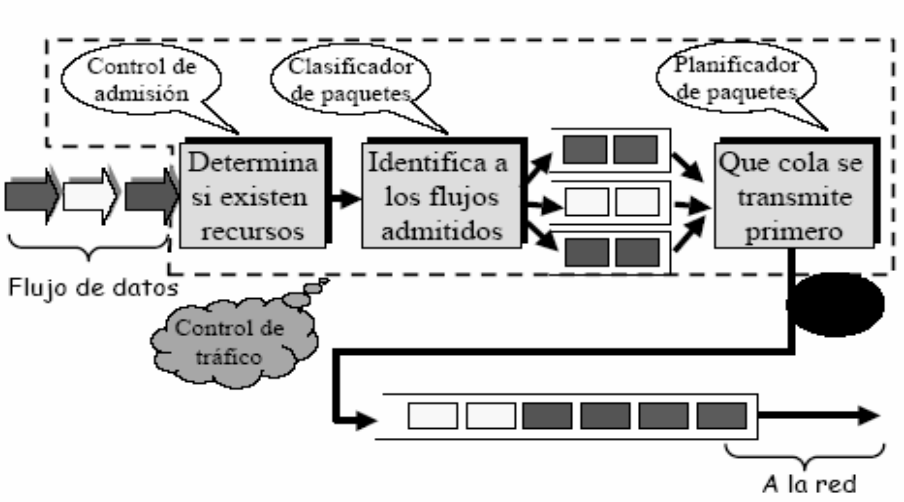


Figura 23 - Idea básica de reserva

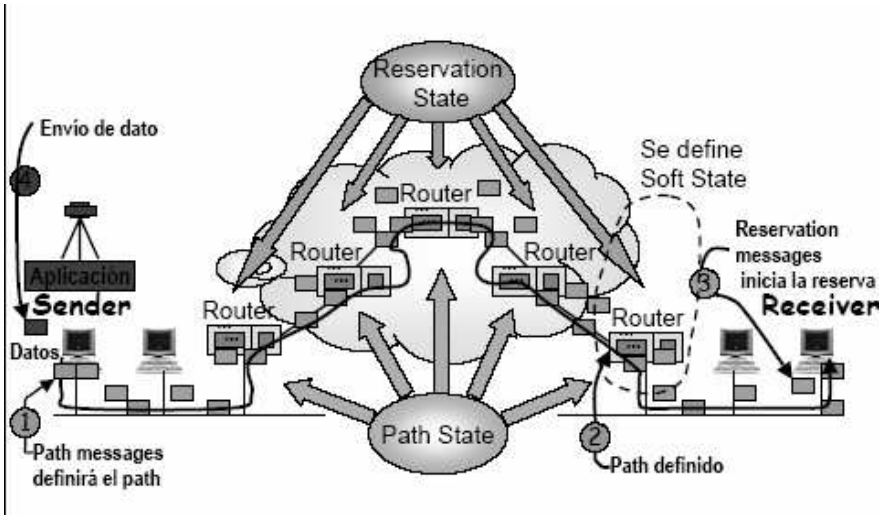


Figura 24 - Reserva en IntServ

Debido a que Internet es una red dinámica, nuevos routers pueden ingresar a la red o algunos dejar de funcionar. Para mantener el soft state es necesario refrescar cada nodo de manera periódica.

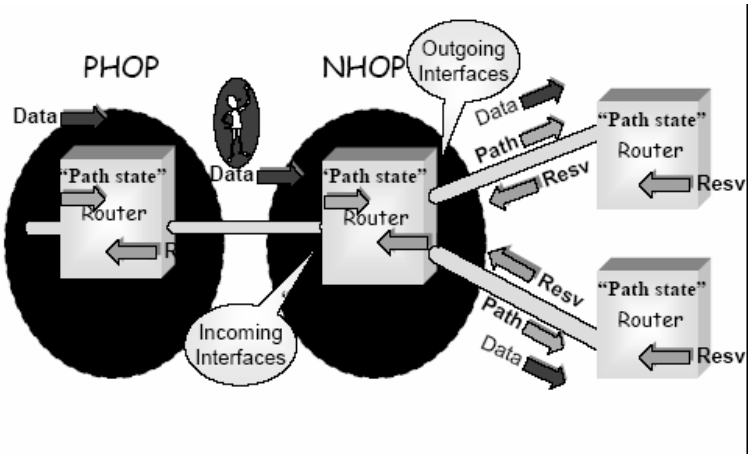


Figura 25 - Mensajes básicos en RSVP

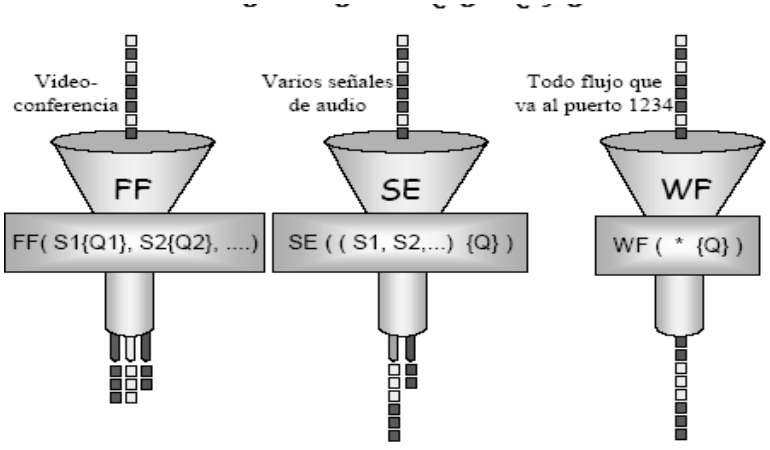


Figura 26 - Estilos de reservas

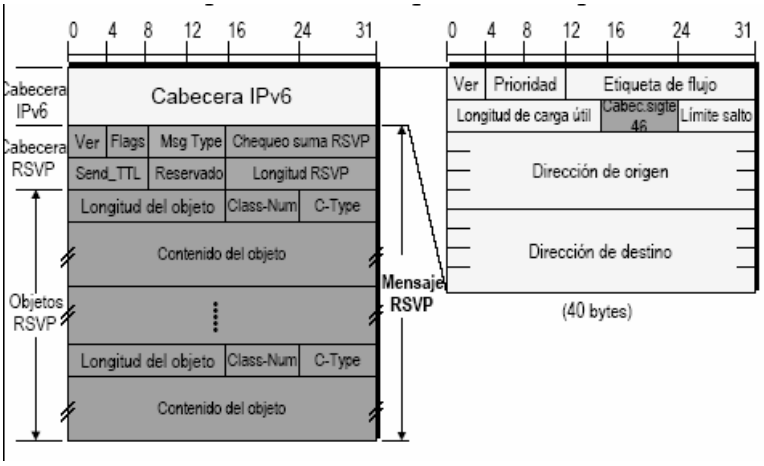


Figura 27 - Formato del protocolo RSVP

- **Campo Ver:** Indica la versión de RSVP. En 1.
- **Campo Flag:** Inicialmente sin definir.
- **Campo Msg Type**: Indica el tipo de mensaje.

Msg Type	Tipo de reserva
1	Path
2	Resv
3	PathErr
4	ResvErr
5	Pathtear
6	Resvtear
7	ResvConf

- **Campo Longitud RSVP:** Tamaño total en bytes.
- **Campo Longitud del objeto:** Longitud total del objeto expresado en bytes.
- **Campo Class-Num y C-Type:** Identifican los diferentes tipos de objetos

Limitaciones de este protocolo:

- Si se hacen dos peticiones seguidas con mucha y poca QoS puede que se rechacen ambas
- Los routers deben comunicarse con los receptores para mantener el soft-state, generando tráfico extra
- Si hay fallos y cambia la ruta, el tráfico se envía como best-effort y se mantiene un tiempo la reserva en la ruta anterior
- Una aplicación debe pedir explícitamente una reserva RSVP
- Dentro de una aplicación todos los miembros deben compartir la misma clase de servicio (aunque se reserven distintos recursos)

2.2.6.3 PROTOCOLO DE SERVICIOS DIFERENCIADOS (DIFFSERV)

El objetivo de una arquitectura DiffServ es implementar una diferenciación de servicios escalable en Internet. Un Servicio define algunas características significativas, características que pueden especificarse en términos de caudal (throughput), demora (delay), variación de demora (jitter) y/o pérdidas (loss), o también en términos de alguna prioridad relativa de acceso a los recursos de la red. Este protocolo se basa en información contenida en la cabecera

de cada paquete, marcada con una determinada prioridad. DiffServ se compone de un número de elementos implementados en los nodos de la red como:

- Per Hop Behaviour (PHB) en el reenvío.
- Funciones de clasificación y agregación de paquetes.
- Funciones de acondicionamiento del tráfico como:
  - Clasificación
  - Marcado
  - Modelado
  - Política de control
- Los paquetes se clasifican y marcan para recibir un tratamiento específico por salto en la ruta.
- Tráfico transportado por marca en la capa IP, utilizando el campo DS (DiffServ). El campo DS constituye una redefinición del campo TOS (Tipo de Servicio) utilizado en los datagramas IP, redefinición cuyo objetivo es unificar los campos similares en IPv4 e IPv6.
- Las operaciones de clasificación, marca, política, y acondicionamiento de tráfico sólo se realizan en los nodos frontera.
- Amplia gama de servicios.
- Establecimiento de un Acuerdo de Nivel de Servicio (SLA, Service Level Agreement).
- Esta arquitectura solo provee diferenciación de servicios en una dirección de flujo del tráfico y es por lo tanto asimétrica.

Los servicios diferenciados (Diffserv) proporcionan mecanismos de calidad de servicio para reducir la carga en dispositivos de la red a través de un mapeo entre flujos de tráfico y niveles de servicio. Los paquetes que pertenecen a una determinada clase se marcan con un código específico (DSCP – Diffserv CodePoint). Este código es todo lo que se necesita para identificar una clase de tráfico. La diferenciación de servicios se logra mediante la definición de comportamientos específicos para cada clase de tráfico entre dispositivos de interconexión, hecho conocido como PHB (Per Hop Behavior).

De esta manera a través de Diffserv planteamos asignar prioridades a los diferentes paquetes que son enviados a la red.

Los nodos intermedios (routers) tendrán que analizar estos paquetes y tratarlos según sus necesidades. Esta es la razón principal por la que Diffserv ofrece mejores características de escalabilidad que Intserv. Dentro del grupo de trabajo de Diffserv de la [9]IETF, se define en el campo DS (Differentiated Services) donde se especificarán las prioridades de los paquetes. En el subcampo DSCP (Differentiated Setvice CodePoint) se especifica la prioridad de cada paquete. Estos campos son validos tanto para IPv4 como IPv6.

En la arquitectura definida por Diffserv (ver figura 28), aparecen nodos extremos DS de entrada y salida, así como nodos DS internos. Este conjunto de nodos definen el dominio Diffserv y presenta un tipo de políticas y grupos de comportamiento por salto (PHB - Per Hop Behavior) que determinarán el tratamiento de los paquetes en la red.

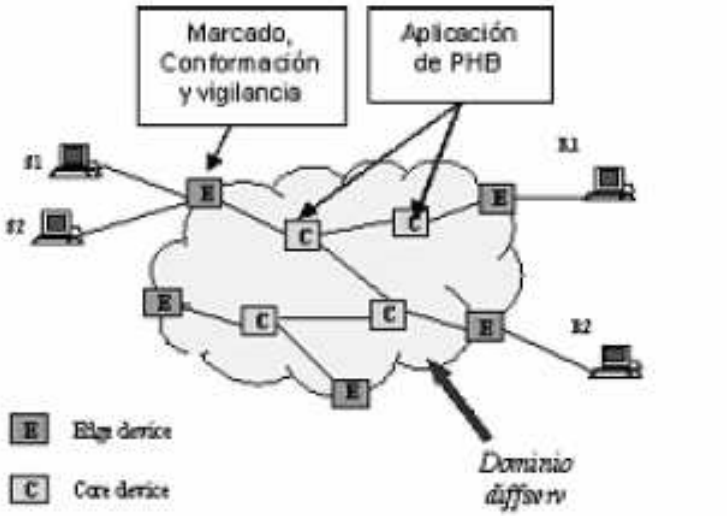


Figura 28 - Arquitectura Diffserv

[9] IETF Diffserv Working Group - http://www.ietf.org/html.charters/diffserv-charter.html

Veamos a continuación las diferentes funciones que deben realizar los nodos DS:

Nodos extremos DS: será necesario realizar diferentes funciones como el acondicionamiento de tráfico entre los dominios Diffserv interconectados. De esta manera debe clasificar y establecer las condiciones de ingreso de los flujos de tráfico en función de: dirección IP y puerto (origen y destino), protocolo de transporte y DSCP, este clasificador se conoce como MF (Multi-Field Classifier).

Una vez que los paquetes han sido marcados adecuadamente, los nodos internos deberán seleccionar el PHB definido para cada flujo de datos.

Los nodos DS de entrada serán responsables de asegurar que el tráfico de entrada cumple los requisitos de algún TCA (Traffic Conditioning Agreement), que es un derivado del SLA, entre los dominios interconectados. Por otro lado los nodos DS de salida deberán realizar funciones de acondicionamiento de tráfico o TC (Traffic Conformation) sobre el tráfico transferido al otro dominio DS conectado.

El campo DS (8 bits) se estructura de la siguiente forma:

- DSCP (Differenciated Services Codepoint) 6 bits
- ECN (Explicit Congestion Notification) 2 bits

El campo DSCP permite definir hasta $2^6 = 64$ posibles categorías de tráfico o clases de servicio, aunque se utilizan bastantes menos.

En DiffServ se definen tres tipos de servicios:

- Servicio Expedited Forwarding: El de mayor calidad (código 101110)

- Servicio Assured Forwarding: Trato preferente. Se definen 4 clases posibles, según los 4 primeros bits del DSCP. Para cada clase se definen 3 categorías de descarte de paquetes (alta media baja) que se indican en los dos bits siguientes.

- Servicio Best Effort: Tiene a 0 los 3 primeros bits. Los 2 bits restantes pueden utilizarse para marcar una prioridad. No ofrece ningún tipo de garantías.

Ventajas:

- Routers más rápidos: se limita la complejidad de clasificación y encolado.
- Menos estados.
- Menos señalización (no hay sobre carga).
- Menos almacenamiento.

Inconvenientes:

- No es extremo a extremo.
- Servicios predictivos.
- Control de acceso de los bordes (bandwidth broker).
- Requiere sobredimensionamineto.

2.2.5.4 SOPORTE DE QoS EN IPV6

- Rendimiento: el formato del paquete IPv6 fue especialmente diseñado para que pudiese ser tratado de manera eficiente por los routers.
  - Tiene menos campos.
  - La etiqueta de flujo está antes que las direcciones, por si se utiliza rutado por flujos (sólo se calcula la ruta por una vez).
  - Un tratamiento eficiente del paquete permite que los paquetes sean procesados con mayor rapidez, disminuyendo el retardo encolado.
  - ICMPv6 es un protocolo más ligero y conciso.
  - Autoconfiguración.
  - Número de saltos y no TTL.

- Flujo: un flujo es tráfico (conjunto de paquetes) con semántica común. Los flujos se usan para que los paquetes correspondientes a él reciban un tratamiento especial. Estos fueron pensados originalmente para ser usados en reserva.

- Etiquetas de flujo: campo de 20 bits en la cabecera IPv6. identifican paquetes IPv6 con el mismo origen y destino con el objetivo de ser tratados de manera especial.
  Evitan inspeccionar el paquete a la vez ---- encriptación Regla:
  - Mismo origen y destino (multidestino).
  - Deben encaminarse al mismo salto siguiente
  - Comparten cabeceras de ruto y salto.
  - Muchos más flujos que parejas origen-destino.
  - No es obligatorio caso (especial en routers)

- Prioridades: campo de 8 bits denominado clase de Tráfico en la cabecera IPv6

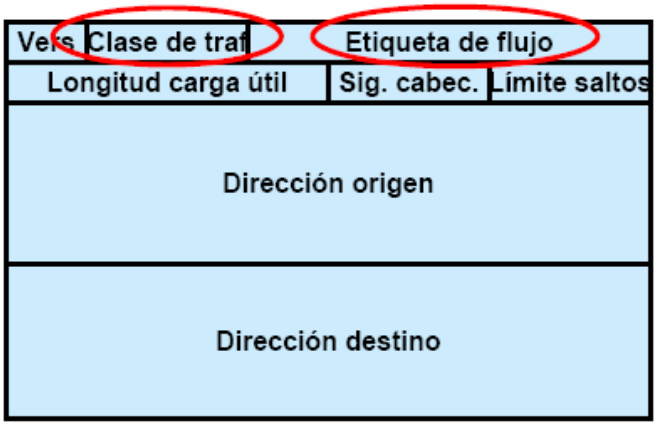


Figura 29 - Campos comprometidos con la QoS

2.2.6 MOVILIDAD

Hoy en día prácticamente todo es móvil, desde el teléfono, al computador, al PDA, algún soporte para la movilidad por parte del protocolo IP no sería nunca mala idea. IPv6 soporta esta característica de serie, sin parches como es necesario con IPv4.

IPv4 tiene dificultades en gestionar computadores móviles, por varios motivos:

- Los computadores móviles necesitan usar una dirección de expedición en cada punto de conexión nuevo a la Internet y con IPv4 no es siempre fácil obtener esta dirección.

- Se necesitan buenos elementos de autenticación, que por lo general no se instalan en nodos IPv4, para informar a cualquier agente en la infraestructura de encaminamiento sobre la nueva localización del nodo móvil.

- En IPv4 puede ser difícil para los nodos móviles de determinar si o no están conectados a la misma red.

- Los nodos móviles en IPv4 no pueden por lo general informar a sus asociados de comunicación sobre un cambio de localización.

Varios aspectos del diseño del protocolo IPv6 son directamente beneficiosos y van más allá de sólo dar apoyo de marcación para, la computación móvil. Un procesamiento mejorado de opciones de destinación, la autoconfiguración, los encabezamientos de encaminamiento, la encapsulación, la seguridad, y las direcciones de difusión a cualquiera contribuyen al diseño lógico de movilidad de IPv6. Tanto es así, de hecho, que una red europea de satélites está ya introduciendo IPv6 como su protocolo principal de comunicación. La ventaja de movilidad de IPv6 puede ser puesta de relieve aún más por la adición de gestión de etiqueta de flujo, lo que da a los nodos móviles una calidad de servicio aún mejor.

En los últimos años ha existido un desarrollo espectacular de:

- Las tecnologías inalámbricas
  - ✓ WLAN (802.11)
  - ✓ Bluetooth
  - ✓ GPRS
  - ✓ UMTS

- Los dispositivos portátiles
  - ✓ PDAs
  - ✓ Computadores portátiles

Existe un gran interés por estar conectado a Internet, de forma inalámbrica y permanente. El objetivo es promover conectividad a Internet a dispositivos móviles inalámbricos, e incluso, que permanezcan conectados mientras se mueven.

Además hay que prever, dada la estructura habitual de las redes inalámbricas (ejemplo muy habitual, la telefonía celular), que un nodo móvil puede estar conectado simultáneamente a varias redes (varias células que se solapan), y debe de ser alcanzable por cualquiera de ellas.

Entenderemos ***movilidad*** como la facilidad para cambiar de red, tanto a nivel físico como a nivel lógico, sin perder el transporte ni las conexiones establecidas por capas de nivel superior al IP. Para que esto sea posible, deberemos mantener una misma dirección IPv6 estemos donde estemos y los paquetes enviados a nosotros tendrían que ser encaminados hacia nosotros estemos donde estemos. Entonces un nodo puede mantener la misma dirección IP, a pesar de su movilidad.

Esta movilidad se puede solucionar de diversas maneras, hacerlo a nivel IP (nivel de red) proporcionará múltiples beneficios:

- Las aplicaciones no se tienen que modificar.
- Proporciona “roaming “.

- Permitirá conectar tecnologías de nivel dos (enlace) heterogéneas (UMTS, WLAN..etc)

2.2.6.1 OPERACIÓN

Todo nodo móvil (**Mobile Node, MN**) tendría una dirección "de casa" (**Home Address, HA**), que seria su dirección en su red origen. Esta dirección se mantendría aunque cambiemos de red.

Los paquetes que se envíen al nodo móvil estando éste en su red origen serían encaminados de forma normal, como si el soporte de movilidad no existiese.

En el momento en que el nodo móvil pasa a una red que no es la suya de origen este es detectado por medio de el descubrimiento del vecindario IPv6 (**Neighbor Discovery**), y por consiguiente obtendría una nueva dirección "de invitado" (**Care-of-Address, CoA**).

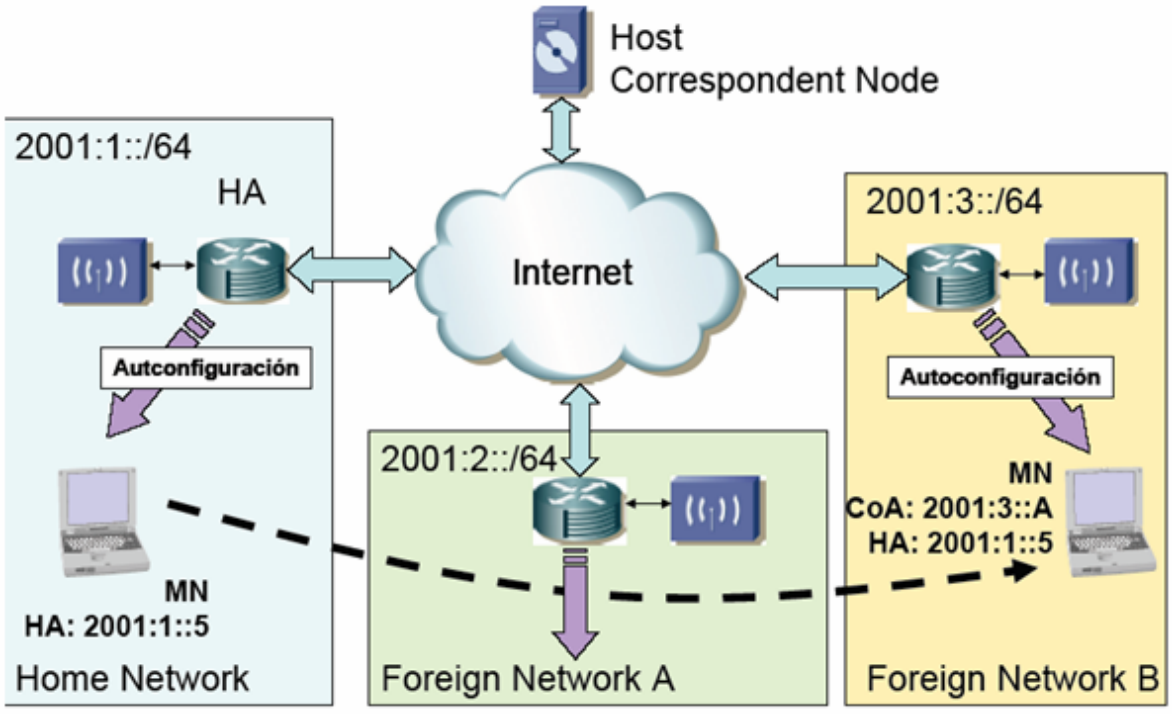


Figura 30 – Móvil que pasa de una red a otra

A partir de ahora el nodo podría ser contactado también a través de esta CoA. Lo siguiente que haría el nodo móvil es contactar con un router de su red origen **(Home Agent, HA)** y comunicarle cual es su CoA actual. De esta forma, cuando un paquete sea enviado a la "dirección de casa", el router sabría que tendría que interceptarlo y entunelarlo con destino a la CoA del nodo móvil.

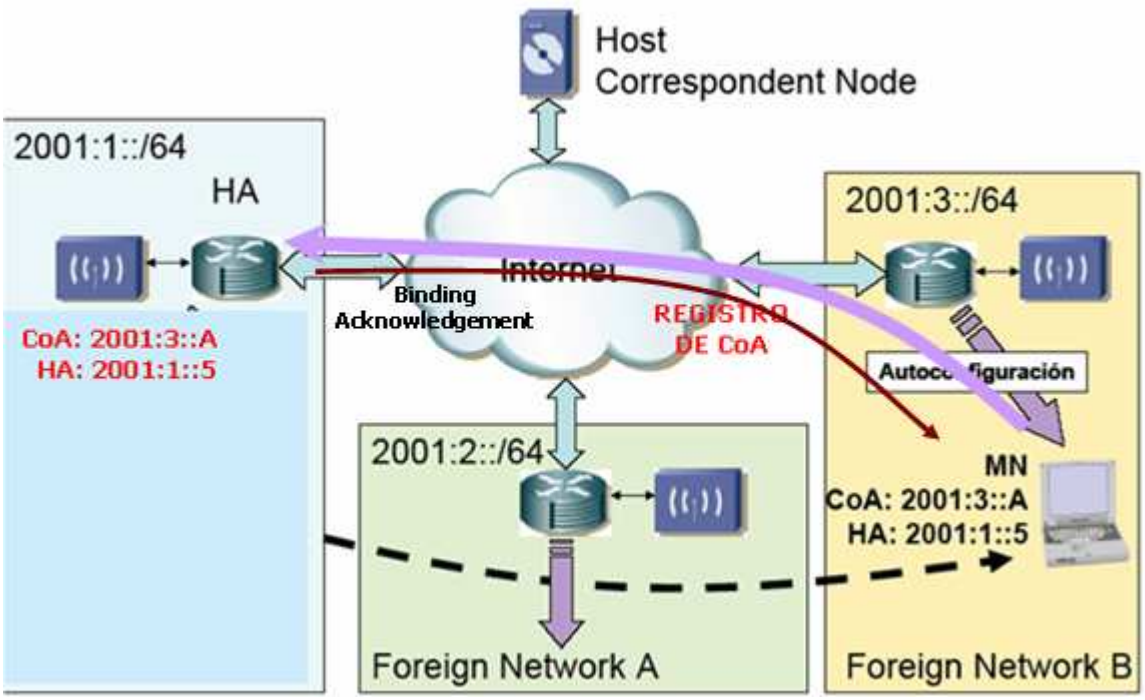


Figura 31 – Registro de dirección de invitado

Lo que en realidad hace el MN cuando se mueve es mandar un mensaje de **Binding Update (BU)** al HA. El BU asocia la CoA con la dirección "de casa" del nodo móvil durante un cierto periodo de tiempo y el Home Agent HA envía un mensaje de reconocimiento **Binding Acknowledgement**. Llamaremos nodo correspondiente **(Correspondent Node, CN)** a cualquier nodo, ya sea fijo o móvil que se comunique con un MN.

Cuando un nodo móvil se comunica con un CN, el MN envía directamente los paquetes utilizando la dirección "de invitado" que ha obtenido en la red que se encuentre. Sin embargo, el CN envía los paquetes a la dirección "de casa" del MN, que serían interceptados por el HA y reenviados a la CoA del nodo móvil.

Se tendría un caso de ruta triangular, que no es ningún problema, pero es ineficiente. Para resolver esto, MobileIPv6 presenta el concepto de optimización de ruta. Este mecanismo permite al MN avisar al CN de que puede enviarle los paquetes directamente a su CoA utilizando para ello mensajes de Binding Úpdate.

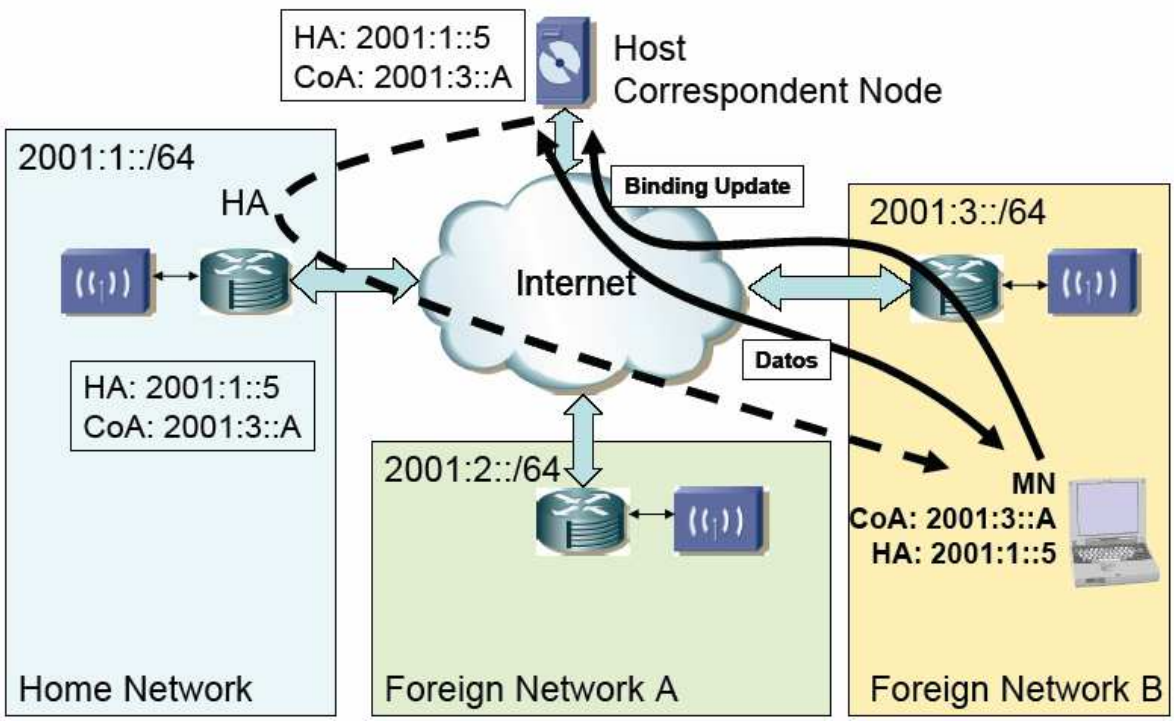


Figura 32 – Comunicación del nodo móvil

2.2.6.2 CABECERAS ADICIONALES

Para conseguir toda esta funcionalidad añadida, MobileIPv6 aprovecha las cabeceras de opción de destino. Esto permite enviar información de señalización en el mismo paquete de datos. Los nuevos tipos de opciones de destino creadas para soportar la movilidad son:

- Home Address Option, indica cual es la dirección "de casa" del nodo móvil cuando éste se encuentra fuera de su red origen.
- Binding Update Option, que sirve para crear, actualizar y eliminar entradas de las asociaciones que se mantienen entre MN y CoA. Un paquete con esta opción haría que

se produzca una asociación en el CN o en el HA entre la dirección origen del paquete y la dirección contenida en el campo de Home Address Option.

- Binding Acknowledgement (BA) Option, que es enviada por el HA y por los CN como respuesta a los BU enviados por el nodo móvil.
- Binding Request (BR) Option, enviada por el CN para solicitar al nodo móvil refrescar su entrada en la lista de asociaciones actual del MN.

2.2.6.3 CONSIDERACIONES DE SEGURIDAD

Tanto los Binding Updates como los Binding Acknowledgements provocan un cambio de estado en los nodos, por lo que deben de ser autenticados. MobileIPv6 utiliza autenticación de cabeceras (Authentication Header, AH) para evitar cualquier ataque.

Sin embargo, la autenticación no es el único problema. La autorización, es decir, que CN puede alterar que asociaciones en la tabla de un MN (que afecta a las tablas de enrutamiento), es el otro.

Para solventar esto se deben incluir mecanismos de protección IPsec, en actualizaciones de los enlaces, utilizar filtrado de entrada utilizando firewall.

2.2.7 MECANISMOS DE MIGRACIÓN DE IPV4-IPV6

Es evidente que son muchas las diferencias entre IPv4 e IPv6 y que tanto los dispositivos actuales como las aplicaciones que los gobiernan y programas de comunicaciones deberán ser actualizados para adaptarse al funcionamiento del nuevo formato. Pero esta actualización no se producirá de un día para otro; es más, IPv6 no implica la desaparición del actual IPv4 sino que ambos protocolos seguirán coexistiendo e ínter operando durante algunos años.

El cambio no debe ser traumático y para ello, los fundadores de IPv6 y sus promotores contemplan todo un programa de acciones que permitan la transición de un protocolo a otro de forma suave y sencilla y que proteja la gran inversión realizada en IPv4.

Uno de los objetivos del proceso de migración a IPv6 es que tanto los routers como los servidores compatibles con el nuevo protocolo sean introducidos en el mercado gradualmente lo que permitirá tanto a fabricantes como a administradores de sistemas y usuarios finales realizar el paso a la nueva versión a su propio ritmo. Una gran ganancia a su favor la encontramos en el propio hecho de que la estructura de direcciones de IPv4 se encuentra incluida dentro de la de IPv6, lo que permite que prácticamente no se necesite realizar ningún trabajo extra en la actualización al nuevo protocolo.

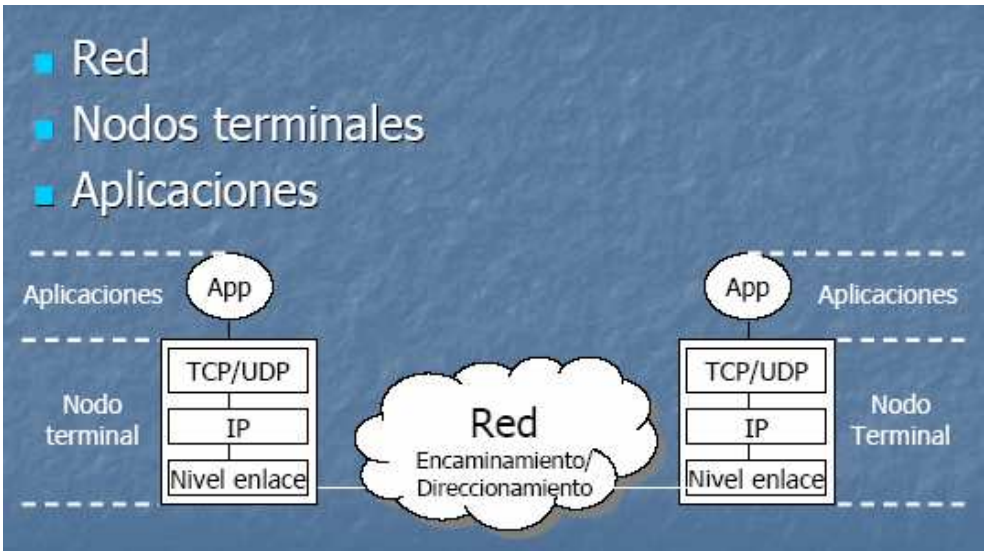


Figura 33 - Arquitectura de Transición

Así, IPv6 puede ser instalado como una actualización de software en los dispositivos de red, siendo totalmente compatible con el actual protocolo.

Durante el periodo de coexistencia de ambos protocolos, los equipos que no hayan sido actualizados todavía podrán seguir trabajando, identificando antes con qué protocolo se realiza la comunicación que recibe en cada momento. Es decir, cada dispositivo deberá leer la cabecera del paquete recibido, en la que un campo de cuatro bits le especificará si el protocolo utilizado es IPv4 o IPv6. Respecto al coste de migrar a la Nueva Internet, se señala [10]que este es mucho menor de lo que pueda pensarse: "el coste en hardware, sistemas operativos o routers, es prácticamente nulo. De hecho, la mayoría de fabricantes no están cobrando por

[10] Palabras de Jordi Palet, Presidente del Grupo de Trabajo de Educación, Promociones y Relaciones Públicas del Foro IPv6

hacer el cambio a IPv6. Lo que sí requerirá una mayor inversión es la migración a IPv6 de todas las redes pero tampoco es un coste descomunal".

Los verdaderos motores de la transición, son, en opinión de Jordi Palet, los propios usuarios. [11]"Son los usuarios finales los que van a tener la necesidad de migrar a IPv6 por que van a ver que les permite nuevas aplicaciones y servicios, más seguridad, mayor calidad de servicio, etc".

La clave para transición es compatibilidad con la base instalada de los dispositivos IPv4. Esta afirmación define un conjunto de mecanismos que los hosts y routers IPv6 pueden implementar para ser compatibles con hosts y routers 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.

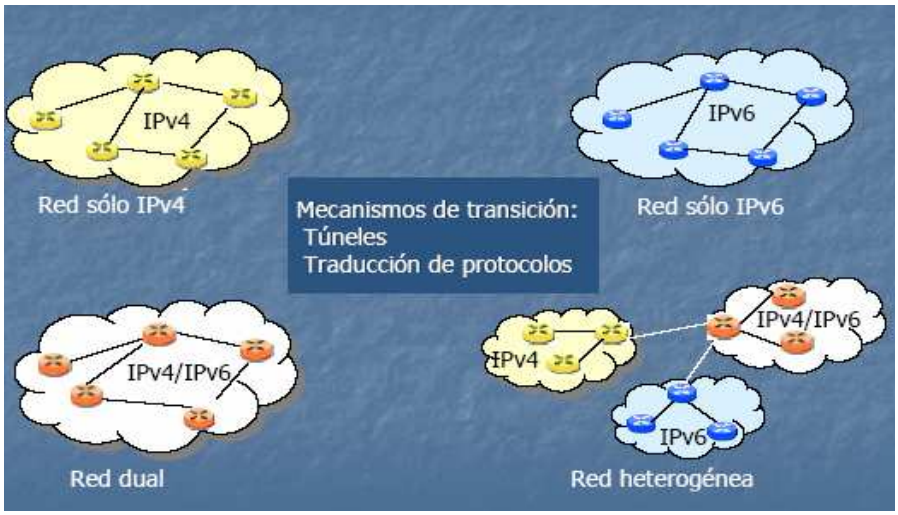


Figura 34 - RED (Encaminamiento/Direccionamiento)

2.2.7.1 DOBLE PILA (DUAL STACK)

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

[11] Jordi Palet señala

IPv6/IPv4". De esta forma, un dispositivo con ambas pilas pueden 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).

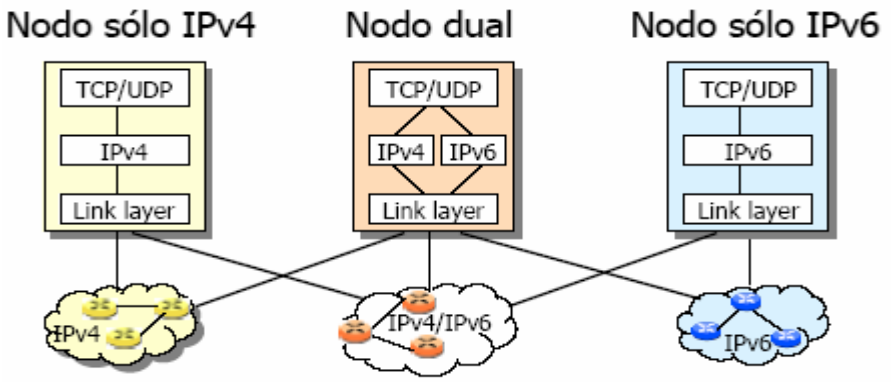


Figura 35 - Nodo (Pila IP)

El DNS podrá devolver la dirección IPv4, la dirección IPv6, o ambas.

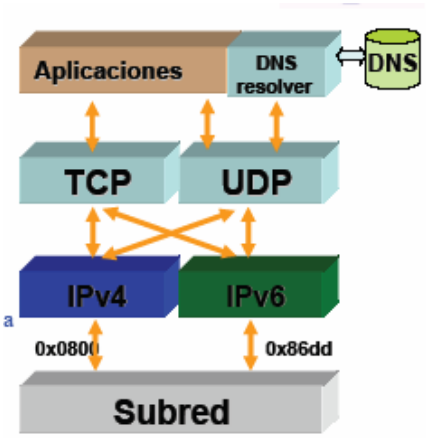


Figura 36 – Doble Pila

Como ya se ha explicado en le apartado de las direcciones especiales IPv6, se pueden emplear la dirección IPv4 (32 bits), anteponiéndose 80 bits con valor cero y 16 bits con valor 1, para crear una dirección IPv6 "mapeada desde IPv4".

Se usa el campo Versión de la cabecera para decidir cual Stack (pila,) debe procesar un paquete que llega.

Ventajas:

- Sencillez.
- Cuando ya no sea necesario el IPv4, se podrá quitar o remover el módulo correspondiente al Sistema Operativo.
- Clientes IPv4 e IPv6 pueden acceder al servicio.
- Se evitan algunos problemas con mecanismos de traducción.

Inconvenientes:

- Necesitaría una completa actualización de software de red.
- Aumento de la carga del procesador y una mayor ocupación de memoria.
- De hecho los routers y los hosts deben tener dos copias de las tablas de encaminamiento y de otros recursos asociados a los protocolos.
- Incremento en la complejidad en el desarrollo de aplicaciones.
- Gestión de dos redes paralelas.

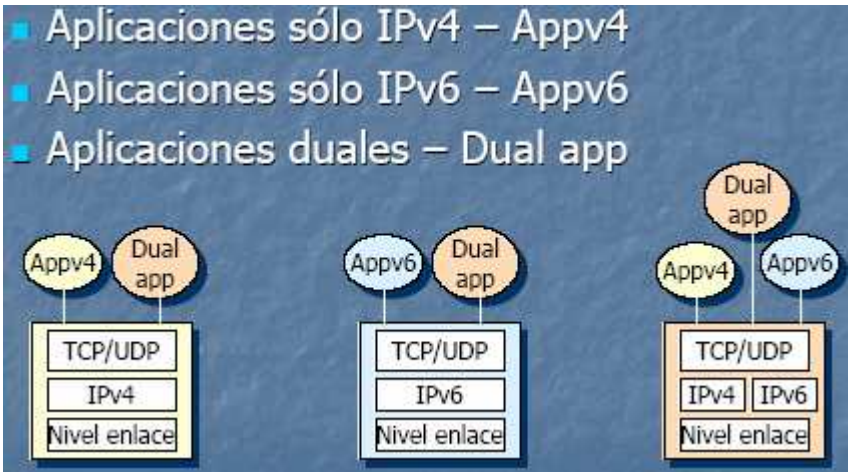


Figura 37 - Aplicaciones (código fuente)

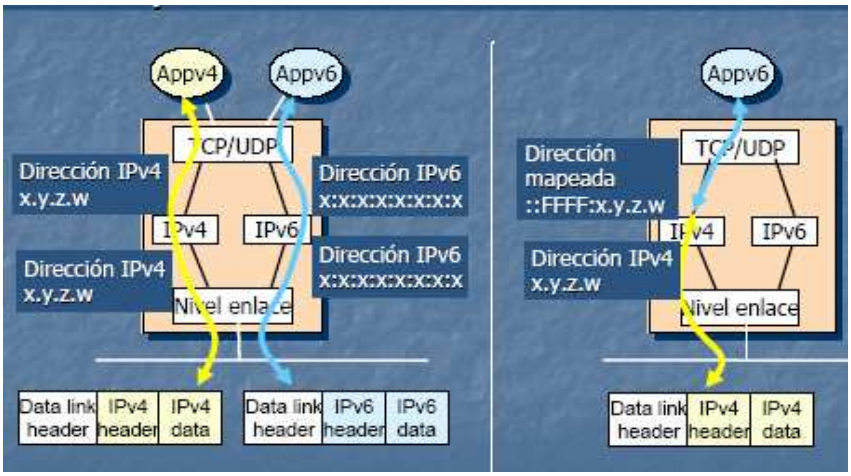


Figura 38 - Aplicaciones (Nodos Duales)

2.2.7.2 TECNICAS BASADAS EN TUNELES

Se basan en encapsular un paquete IP dentro de otro, están enfocados a unir dos nubes o islas IPv6 a través de un océano IPv4 y viceversa.

Figura 39 - Encapsulado en IPv4

Se forma un túnel, que tiene un extremo que se ocupa de encapsular y otro que saque el paquete IPv6 y lo encamine hacia su destino. Existen túneles configurados de manera manual o de tipo automático. El túnel es considerado como un salto único, no hay manera para un host IPv6 de enterarse que el paquete ha sido encapsulado a lo largo de su camino por medio de herramientas como traceroute.

El router a la entrada del túnel decrementa el valor del campo Hop Limit del paquete IPv6 de una unidad y crea un paquete IPv4 con el valor 41 en el campo Protocol Type.

La longitud del paquete es calculada sumando la longitud de la cabecera IPv6, las eventuales cabeceras adicionales y el contenido del paquete. Si necesario el router fragmenta el paquete. El destino del nuevo paquete IPv4 es la salida del túnel.

El router a la salida del túnel recibe el paquete IPv4. Si es fragmentado, espera para todos los fragmentos y los reúne. Luego saca el paquete IPv6 y lo encamina hacía su destino. Al final del túnel hay un host o un router. En ambos casos deben estar capacitados como IPv6 para ser capaces de procesar el paquete después de desencapsularlo. Si al final del túnel hay un host con una dirección IPv4 mapeada como IPv6, el túneling se hace en forma automática extrayendo la dirección IPv4 de la dirección IPv6 para usarla en la cabecera del paquete. Si no es así, el tunneling se debe configurar manualmente. El nodo que encapsula necesita conocer la IP del otro extremo del túnel, ya que no se puede extraer la cabecera.

Desde la perspectiva de IPv6, el otro extremo del túneles visto como un nodo IPv6 normal que está a un salto de distancia, aunque existan muchos saltos en la red IPv4 entre los puntos extremos del túnel.

2.2.7.2.1 TÚNELES MANUALES

La funcionalidad de estos túneles es interconectar islas IPv6 a través de un océano IPv4. Cada extremo es un [12]nodo dual (routers) y en ellos se configuran direcciones IPv4 e IPv6 tanto local como remotas.

[12] Routeres que soportan ambos protocolos IPv4 – Ipv6

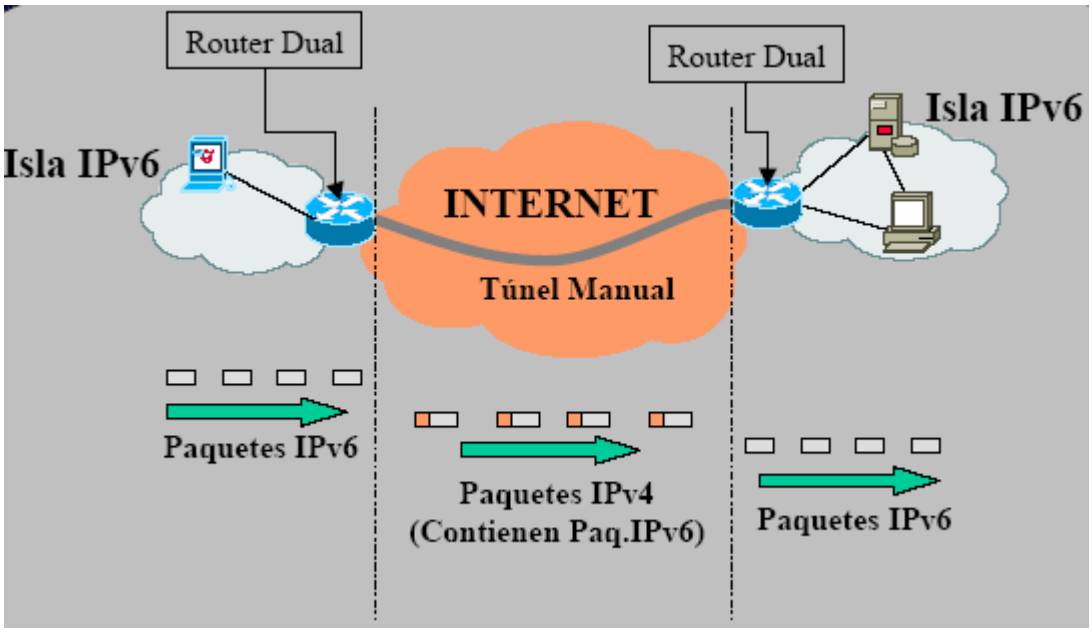


Figura 40 - Funcionamiento de un Túnel Manual

Ventajas:

- Método muy utilizado en el acceso al 6-BONE.
- Disponible en multitud de plataformas (Cisco, Telebit, Linux, Solaris, Windows NT, etc).
- Es un método totalmente transparente respecto al nivel IPv6 y superiores, con lo cual no afecta las aplicaciones.
- No consume excesivos recursos, la MTU se reduce a 20 bytes (cab. IPv4 típica).
- Aplicación principal: conexión con ISP IPv6 remoto a través de Internet.

Inconvenientes:

- No son dinámicos, sino que se establecen manualmente de forma o de forma semiautomática.
- Si se unen N islas y la topología no considera un nodo central o intercambiador, el número de túneles a establecer a cada sitio asciende a N – 1. En el caso de pensar en la conexión entre si de miles de islas IPv6 distribuidas por Internet actual, este método carece de sentido.

2.2.7.2.1.1 TÚNNEL BROKER

El túnel Broker es un lugar WEB 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. Se trata de ISP's IPv6 "virtuales", proporcionando conectividad gratuita y de forma libre a IPv6 a usuarios que ya tienen conectividad IPv4. A diferencia de otros mecanismos es que el "Túnnel Broker" no requiere la configuración del router. Estos mecanismos se hacen indispensables para labores de investigación, dado que se requieren direcciones IPv6 y nombres de dominio DNS.

2.2.7.2.1.2 TÚNNEL SERVER

Es un router con pila doble (IPv4-IPv6), conectado a Internet, que siguiendo órdenes del "Broker" crea, modifica o borra los servicios asociados a un determinado túnel/usuario.

El mecanismo para su configuración es tan sencillo como indicar en un formulario Web, datos relativos al S.O, la dirección IPv4, un "apodo" para maquina, y el país donde está conectada.

El servidor de túneles crea los registros DNS, el extremo final del túnel, y genera un script para la configuración del cliente.

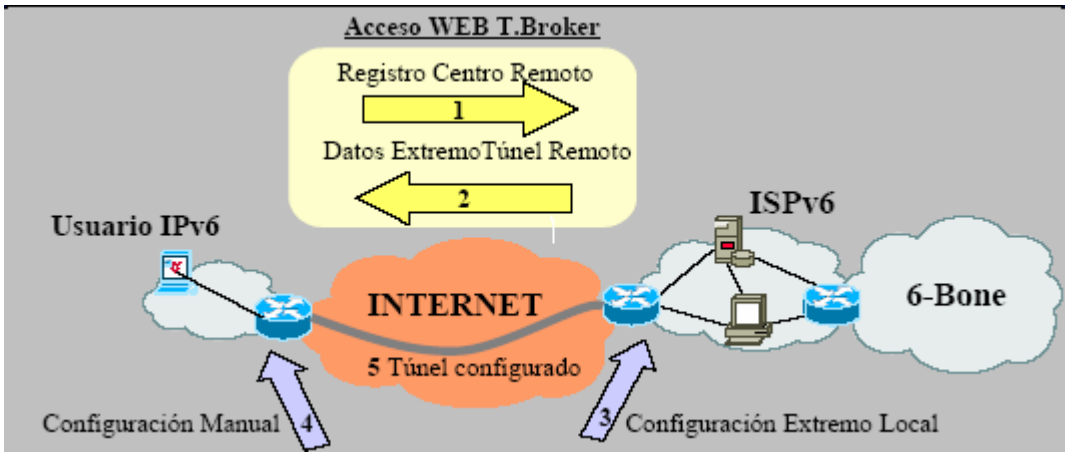


Figura 41- Túnel Broker

2.2.7.2.2 TÚNELES AUTOMÁTICOS

Los túneles automáticos se establecen directamente entre sistemas finales, y como su nombre lo indica no necesitan ser configurados ya que se utilizan conjuntamente con direcciones IPv6 especiales que contienen una dirección IPv4.

Su funcionamiento es muy simple: el sistema origen encapsula directamente los datagramas IPv6 sobre datagramas IPv4 cuya dirección destino se obtiene de la parte final de la dirección IPv6. Estos túneles se utilizan principalmente para comunicar sistemas IPv6 localizados en redes cuyos routers no soportan IPv6 (encapsulación extremo a extremo).

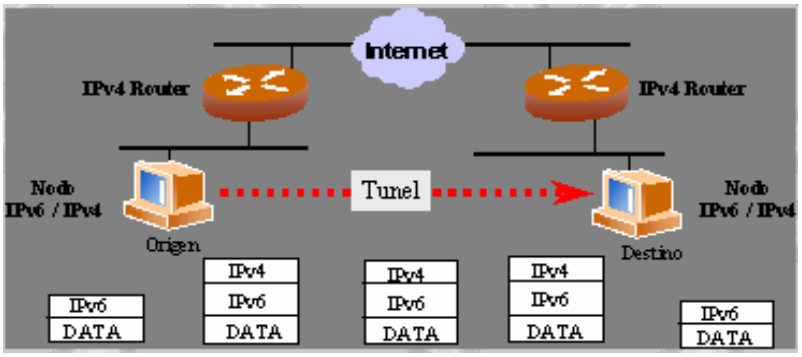


Figura 42 - Túnel automático

- Estos túneles permiten a nodos duales comunicarse a través de una infraestructura IPv4.
- Se utilizan direcciones IPv6 "IPv4 – compatible": Prefijo 0::/96 + Dirección IPv4.
- Se define una interfaz virtual para la dirección "IPv4 compatible".
- Los paquetes destinados a direcciones "IPv4 compatible" se envían por el túnel automático.

Reglas:

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

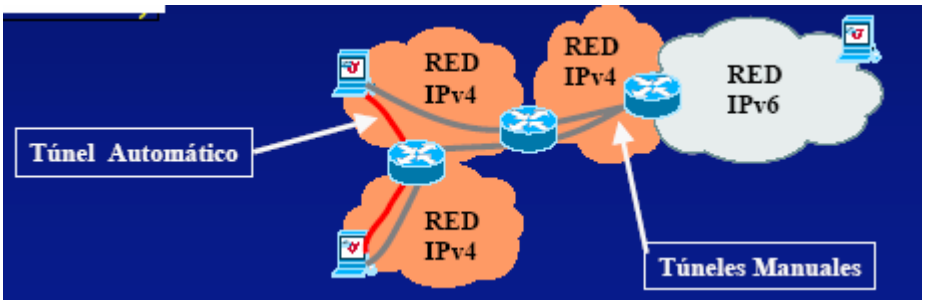


Figura 43 - Uso de Túneles automáticos y túneles manuales (sin routers IPv6)

2.2.7.2.3 TÚNELES 6TO4

Este mecanismo se puede aplicar para comunicar redes IPv6 aisladas por medio de la red IPv4. El router de extremo de la red IPv6 crea un túnel sobre IPv4 para alcanzar la otra red IPv6. Los extremos del túnel son identificados por el prefijo del sitio IPv6.

Este prefijo consiste en 16 bits fijos que indican que estamos utilizando la técnica 6to4 más 32 bits que identifican el router externo del sitio. Un efecto secundario de 6to4 es que deriva automáticamente un prefijo /48 de una dirección IPv4. De esta forma los sitios pueden empezar a utilizar IPv6 sin solicitar nuevo espacio de direccionamiento a la autoridad competente.

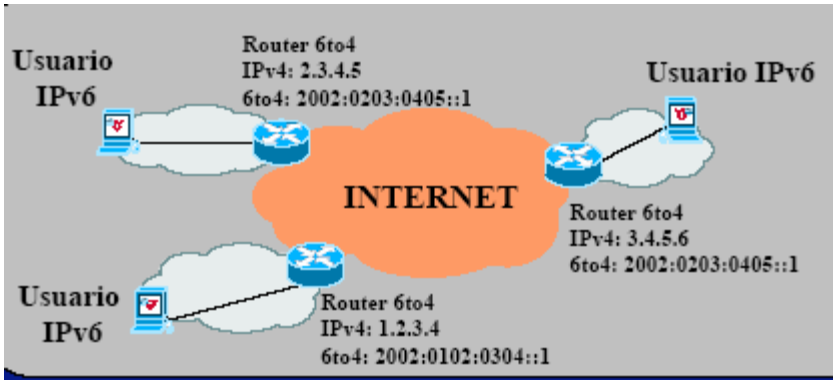


Figura 44 - Túnel 6to4

- Su principal característica es unir islas IPv6 dispersas en un océano IPv4.
- A cada isla IPv6 se le asigna un prefijo IPv6: 2002::/16+Dir IP router de frontera.

- Siguiente salto IPv4 contenido de la dirección IPv6.
- El encaminamiento entre las distintas islas se apoya en el encaminamiento IPv4 subyacente.
- Implementaciones: Windows NT y proyecto KAME: Linux y FreeBSD.

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.
- Dadas N islas IPv6, sólo se establecen los túneles necesarios para las conexiones activas en cada momento.

Inconvenientes:

- Para organizaciones que se conectan a un ISP IPv6 remoto, no es necesario más 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.

2.2.7.2.4 TÚNELES 6OVER4

Con este método podemos comunicar nodos IPv6 aislados dentro de nuestro sitio con el resto de los nodos IPv4. Esta técnica también se emplea en casos en los cuales el router Ipv6 no tiene acceso o permiso para transmitir paquetes IPv6 sobre el enlace. Para esto se emplean enlaces virtuales empleando un grupo multicast IPv4, mapeando las direcciones IPv6 sobre este grupo multicast.

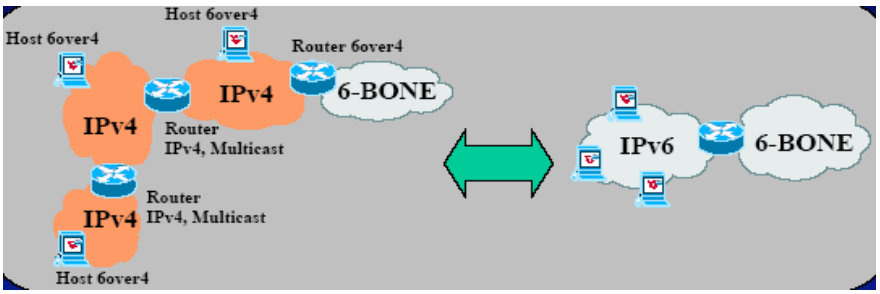


Figura 45 - Túnel 6over4

- Nodos IPv6 dispersos en subredes IPv4 → se forma una "LAN virtual" IPv6.
- Tráfico IPv6 entre nodos encapsulado IPv4. Direcciones IPv4 Multicast.
- Los procesos de Neighbor / Router Discovery se hacen empleando Multicast.
- Router 6over4 con acceso a [13]6-BONE → 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 routers internos.
- Instalado en un solo router el stack IPv6 y conectándolo al 6-BONE se proporciona acceso a dicha red a todos el resto de los nodos IPv6.

Inconvenientes:

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

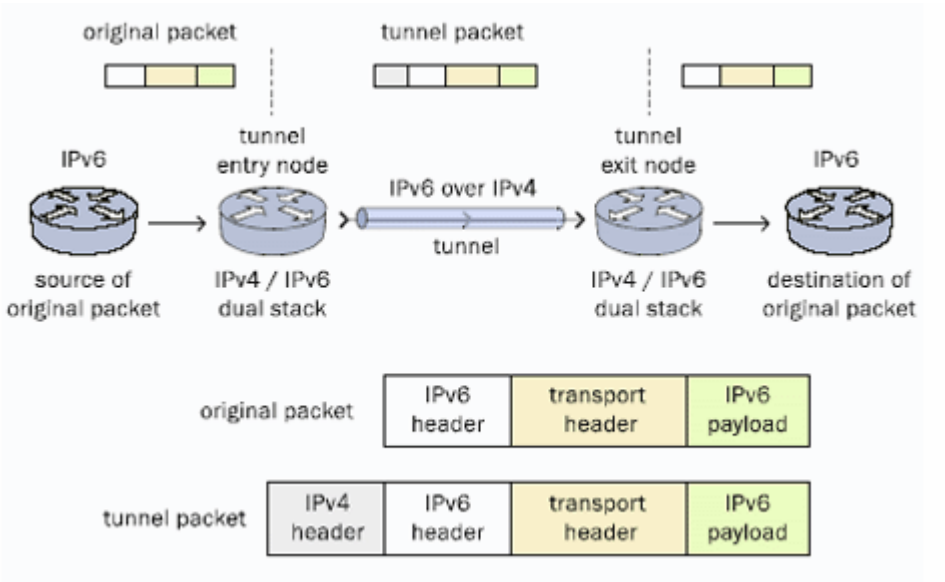


Figura 46 - Funcionamiento Túnel 6over4

[13] Es una red experimental IPv6, informal y cooperativa de alcance mundial. Su función es asistir en la evolución y desarrollo del IPv6

2.2.7.3 TÉCNICAS BASADAS EN TRADUCTORES

Un traductor es un software que se encarga de tomar todos los paquetes que vienen de nodos pertenecientes a una red y que van dirigidos hacia otra, la cual utiliza un protocolo diferente y por consiguiente incompatible, y se encarga de traducir los encabezados y las direcciones contenidas en estos para que los nodos en ambas redes se comuniquen transparentemente.
Existen dos posibles escenarios en donde la traducción de direcciones y protocolos puede ser utilizada:

- Una red IPv6 comunicándose con nodos en una red IPv4. Por ejemplo, una red completamente nueva con nuevos equipos que sólo manejan IPv6 y que necesiten comunicarse con otros nodos que se encuentran en la red IPv4 o en Internet.

- Una red IPv4 comunicándose con nodos en una red IPv6. Por ejemplo, actualizar toda una red IPv4 a IPv6 nodo por nodo necesita que servicios críticos como Web, correo, compartir impresoras o archivos, puedan ser accesibles para todos los nodos, manejen IPv4 o Ipv6.

Este mecanismo es el Traductor de direcciones, que complementado con la utilización de Traductores a nivel de Aplicación (Application Level Gateways o ALG's) para ciertos protocolos que el traductor por sí solo no puede traducir, sería la solución perfecta para este problema de incompatibilidad.

Al quedar colocado como una compuerta (Gateway) entre las redes, permitiría que los equipos de las diferentes redes se comuniquen entre ellos sin que sepan que se encuentran en redes que manejan un protocolo diferente e incompatible.

Otras características:

- Pueden necesitar módulos específicos para algunas aplicaciones
- Problemas de escalabilidad
  - Deben mantener información de los flujos IP
- Utilización recomendada sólo si una aplicación

- No soporta comunicación con ambos protocolos
- O se ejecuta en una máquina con una única pila
- O máquina doble pila pero red sólo soporta uno de los protocolos.

- Dependiendo del servicio
  - Conveniente configurarlo entre servidores. Transparente a usuarios.
  - Usuario6 en servidor6 interactúa con Usuario4 en servidor4
  - Si no es posible lo anterior, lo más cerca posible del servidor
  - Red de usuario lo más simple posible.

2.2.7.3.1 STATELESS IP/ICMP TRASLATION ALGORITHM (SIIT) TRADUCTOR SIN ESTADO

Este algoritmo traduce entre encabezados de paquetes IPv4 e IPv6 (incluyendo los encabezados ICMP). Este nuevo algoritmo puede usarse como parte de una solución que permite a computadores con IPv6 comunicarse con computadores con IPv4.

2.2.7.3.1.1 TRADUCCIÓN DE IPV4 A IPV6

Cuando el traductor recibe un paquete IPv4 y su destino no se encuentra en la red, traduce el encabezado del paquete IPv4 en un encabezado de IPv6. Este es enviado basado en la dirección de destino de IPv6, el encabezado original es eliminado y reemplazado por el encabezado de IPv6, excepto los paquetes de ICMP, el encabezado de la capa de transporte y una porción de los datos quedan inalterados.

Una de las diferencias entre IPv4 e IPv6 es el path IPv6 el descubrimiento de MTU es obligatorio pero el de IPv4 es opcional. Esto implica que los enrutadores no pueden fragmentar el paquete, solo el remitente puede hacer la fragmentación.

Los paquetes de ICMP necesitan una manipulación especial para el manejo de errores y el checksum.

- **Traducción de encabezados IPv4 a encabezados IPv6**
  Si la bandera DF no es fija y el paquete IPv4 produce un paquete IPv6 de más de 1280 bytes, el paquete IPv4 debe ser fragmentado antes de traducirlo.

- **Traducción de UDP sobre IPv4**
  Si un paquete de UDP tiene cero en la suma de comprobación entonces una suma de comprobación válida debe calcularse para traducir el paquete.

- **Traducción de encabezados ICMPv4 en encabezados ICMPv6**
  Todos los paquetes ICMP necesitan tener un valor de traducción y para los mensajes de error incluidos en el encabezado necesitan también traducción.

- **Traducción de mensajes de error ICMPv4 en ICMPv6**
  La traducción de los encabezados puede hacerse con recursividad de la función que tradujo los encabezados exteriores.

2.2.7.3.1.2 TRADUCCIÓN DE IPV6 A IPV4

Cuando el traductor recibe un paquete IPv6 y su destino no se encuentra en la red, traduce el encabezado del paquete IPv6 en un encabezado de IPv4. Este es enviado basado en la dirección de destino de IPv4, el encabezado original es eliminado y reemplazado por el encabezado de IPv4, excepto los paquetes de ICMP el encabezado de la capa de transporte y una porción de los datos quedan inalterados.

2.2.7.3.1.3 IMPLICACIONES PARA IPV6

Un nodo IPv6 que trabaja con SIIT necesita algunas modificaciones más allá de un nodo IPv6 normal. Se debe garantizar que la dirección IPv4 es traducible.

2.2.7.3.2 NETWORK ADDRESS TRASLATION - PROTOCOL TRASLATION NAT-PT

En caso de que se tengan nodos o bien con IPv6 o bien con IPv4 de forma exclusiva, esta puede ser una buena solución. La comunicación se realiza a través de un dispositivo específico (un router que soporte NAT-PT) y que soporta el control de estado de las conexiones. Este método necesita también cambios a nivel de aplicación para controlar las peticiones de resolución de nombre en el DNS.

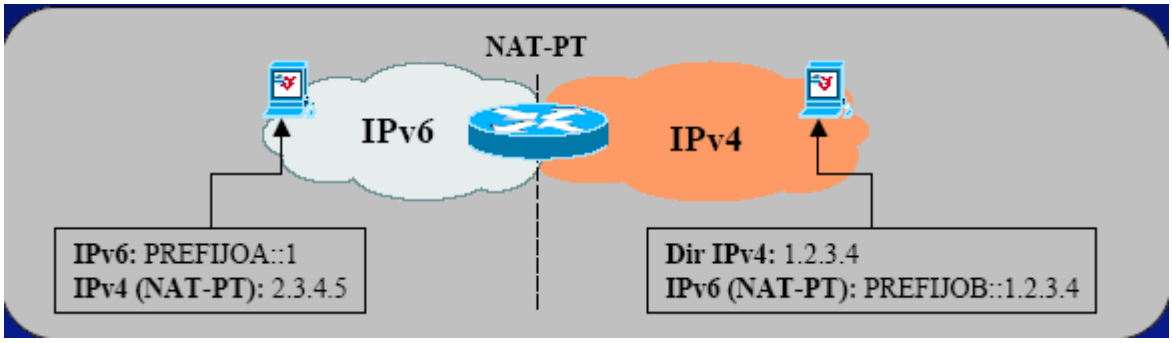


Figura 47 - NAT-TP

Funcionamiento: el NAT-PT asocia los hosts IPv6 direcciones de un conjunto de (ej. 12010.40/24). Los paquetes que llegan desde el host ABCD:EEFF::1234:5678 son traducidos a IPv4 por la dirección fuente 120.10.40.10. El host IPv4 envía a su vez un paquete IPv4 a su destino 120.10.40.10. El NAT-PT se ocupa de construir un paquete IPv6 con dirección destino la del host IPv6.

El NAT-PT tiene que memorizar las asociaciones hechas a lo largo de la sesión.

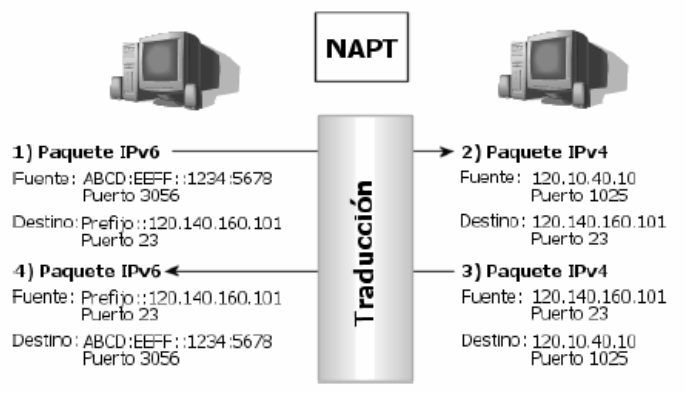


Figura 48 - Traducción NAT

- Básicamente se trata de instalar un NAT gateway que traduzca el tráfico IPv4 a IPv6 y viceversa, de manera transparente.
- NAT tradicional: traduce direcciones (conexiones de redes con dri. IPv4 privado).
- NAT-PT: traducción de direcciones y protocolos.
- Traducción basada en el algoritmo SIIT.
- No es transparente a nivel de aplicación → precisa 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.

Ventajas:

- Comunicación directa entre nodos IPv6 – IPv4
- Muchas redes corporativas poseen experiencia en la gestión / administración de NAT's
- Implementado en la mayor parte de los routers (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 encuenta siempre la carga de tráfico prevista).

Inconvenientes:

- Los NAT's poseen un alto coste de gestión y administración.
- El proceso de traducción es más costoso en recursos que el de entunelar.

- Si la comunicación extremo a extremo es heterogénea (IPvX - IPvY) NAT-PT 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).

2.2.7.3.3 BUMP IN THE STACK (BIS)

Se propone un mecanismo de Dual Stack (pilas duales) en los hosts, usando una técnica llamada "Bump in the Stack". La técnica consiste en el snooping de los datos que fluyen entre un módulo TCP/IPv4 y los módulos del driver de la tarjeta de la red. Se traduce el tráfico IPv4 en IPv6 y viceversa. Esto hace posible que las aplicaciones IPv4 se comuniquen con los hosts IPv6. Tales mecanismos serán necesitados en una fase temprana de la migración, donde no está disponible un sistema completo de los usos IPv6.

Básicamente tres módulos son necesarios para realizar la traducción: (The Extension Name Resolver) **El discernidor de imágenes del nombre de la extensión,** (The Address Mapper) **mapper de la dirección (mapeador), y** (The Translator),**el traductor,** como se describe en la figura 49.

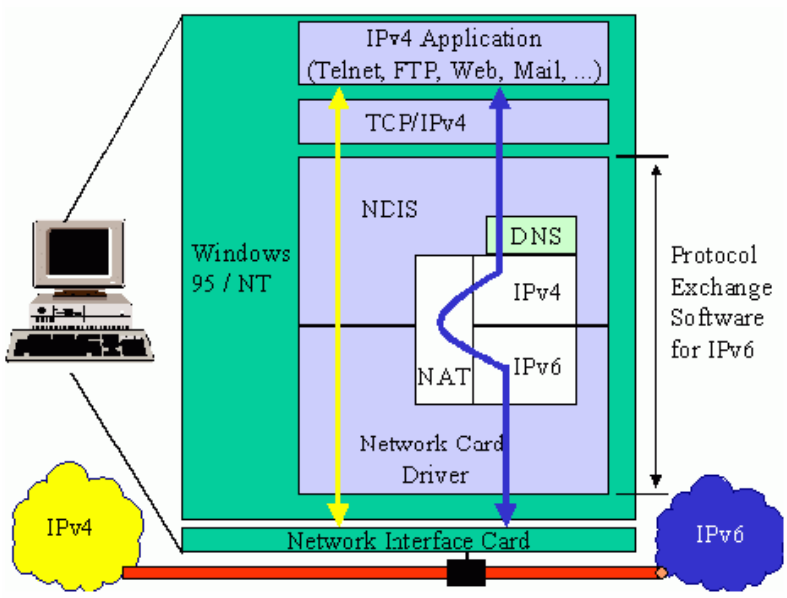


Figura 49 - Traducción BIS

- **Traductor:** Este módulo (NAT) traduce los paquetes IPv4 a los paquetes IPv6 (y viceversa), que usan los algoritmos especificados en el mecanismo de SIIT. Si el traductor recibe un paquete IPv6 de una aplicación, este convierte la cabecera IPv4 en una cabecera IPv6 y da este paquete modificado al IPv6 stack. (Algunas veces el paquete tiene que estar partido en fragmentos primero, porque la cabecera IPv6 es de 20 octetos más grandes que el IPv4, así que el tamaño del paquete puede exceder el tamaño permitido PMTU). Este módulo funciona simétricamente, los paquetes entrantes IPv6 se puede traducir a los paquetes IPv4.

- **Discernidor de imágenes Conocido De la Extensión**: El ENR es implementado como una parte de la pila del DNS de los sistemas del BIS. Este sirve las peticiones del DNS de las aplicaciones. Si recibe una petición del DNS de una dirección IPv4 (registro A), esta genera un pedido del DNS la dirección IPv6 adjunta (registro AAAA). Si las respuestas del servidor del DNS es un registro de A, esta dirección IPv4 se remiten al uso para una conexión de IPv4 solamente. Si la petición del DNS incluye solamente un registro de AAAA, el ENR hace a mapper (convierte) de la dirección, para unir esta dirección IPv6 una dirección temporal IPv4.

- **Mapper De la Dirección:** maneja el espacio de dirección IPv4 del sistema del BIS. Almacena las relaciones entre las direcciones temporales IPv4 y las direcciones IPv6. Es utilizada por el ENR o los traductores en estos casos:

- Si el ENR recibe un registro de AAAA solamente y no existe ninguna relación al registro.

- El traductor recibe un paquete IPv6, para el cual no se encuentra ninguna relación.

Aplicabilidad

Este mecanismo puede ser útil especialmente en la etapa inicial de una migración IPv4/IPv6 donde algunos aplicaciones no se modifican en IPv6. También será provechoso para los

usuarios con las aplicaciones que nunca serán aumentados en IPv6. La técnica permite aplicaciones en los hosts que se pueden comunicar con IPv4 y los hosts IPv6.

Por ejemplo es posible incluirla debajo de Win95 como conductor simple de la red. Este mecanismo se puede combinar con otras técnicas de la migración (e.g. túneles configurados). Se puede utilizar un espacio de dirección privado para las direcciones temporales IPv4, porque estos son usados solamente para el sistema del BIS.

El mecanismo es válido solamente para el tráfico del unicast. No trabajará cuando se utilizan las opciones IPv4 o IPv6. Esto es porque es imposible traducir entre las diversas opciones. Como con otras soluciones NAT, la conversión del IP no puede traducir las direcciones que se encajan en los protocolos de capa de aplicación que se encuentran típicamente en el ftp.

Esto tiene que ser tratado con las entradas específicas de la capa de uso (ALGs) para cada uso. Tiene que haber un algoritmo para lanzar las direcciones temporales del IP para prevenir el desbordamiento del espacio de dirección.

2.2.7.3.4 SOCKS v5

Características principales:

- Uso tradicional Socks v5: conectividad IP directa a Internet en redes con firewall a determinados hosts.
- Servidor Socks v5 dual → Traductor de protocolos (Algoritmo SIIT).
- Traducción IPv-IPv6 y viceversa. Conexiones siempre iniciadas por cliente.
- Dos componentes: servidor SOCKS v5 + Librería SOCKS v5 (Cliente).
- Implementaciones:
  - NEC (www.socks.nec.com)
  - Fujitsu (ftp://ftp.kame.net/pub/kame/misc)

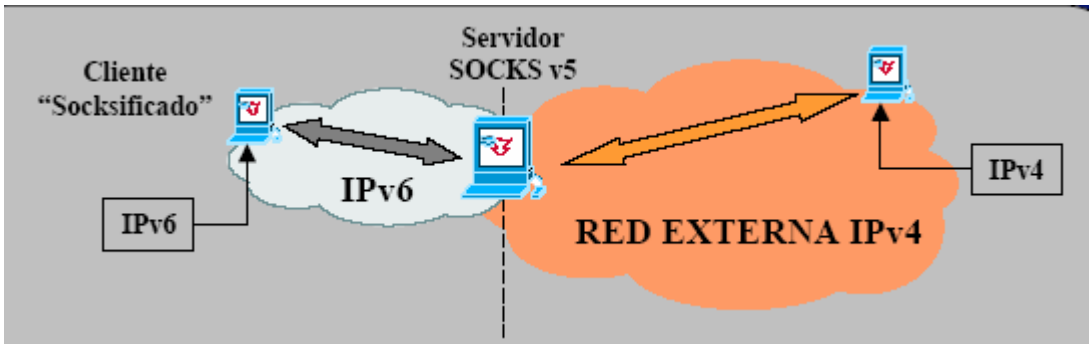


Figura 50 - SOCKS v5

Funcionamiento Detallado: (IPv4 = Red Interna)

- Una aplicación en el nodo cliente inicia una conexión TCP o UDP con un nodo externo empleando el nombre completo FQND (Fully Qualified Domain Name).
- La librería SOCKS v5 en el cliente intercepta la resolución del nombre ("gethostbyname") e inicia una conexión TCP al puerto 1080 del SOCKS v5.
- El servidor SOCKS v5 devuelve al cliente la dirección IPv4 remota falsa ("falke IPv4 address").
- El servidor SOCKS v5 inicia la conexión TCP o UDP con el nodo remoto y hace de Proxy entre el cliente y el nodo externo. Si el nodo externo es IPv6, aplica el algoritmo de traducción SIIT.
- En el cliente, los paquetes con la "fake IPv4 Address" como origen o destino son interceptados y tratados de por las librerías SOCKS v5 que los recibe o envía respectivamente al servidor SOCKS v5.

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 autenticación adecuados para evitar usos indeseados.

Inconvenientes:

- Instalación de librerías SOCKS v5 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).

2.3 VENTAJAS E INCONVENIENTES IPv6

VENTAJAS

- **Escalabilidad:** IPv6 tiene direcciones de 128 bits frente a las direcciones de 32 bits de IPv4. Por tanto el número de direcciones IP disponibles se multiplica por 7,9 * 1028. IPv6 nos ofrece un espacio de 2128 (340.282.366.920.938.463.463.374.607.431.768.211.456). Para hacernos a la idea de lo que esta cifra implica, basta con calcular el número de direcciones IP que podríamos tener por metro cuadrado de la superficie terrestre: Nada más y nada menos que 665.570.793.348.866.943.898.599.
- **Seguridad:** IPv6 incluye seguridad en sus especificaciones como es la encriptación de la información y la autentificación del remitente de dicha información.
- **Aplicaciones en tiempo real:** Para dar mejor soporte a tráfico en tiempo real (i.e. videoconferencia), IPv6 incluye etiquetado de flujos en sus especificaciones. Con este mecanismo los encaminadores o routers pueden reconocer a qué flujo extremo a extremo pertenecen los paquetes que se transmiten.
- **Plug and Play:** IPv6 incluye en su estándar el mecanismo "plug and play", lo cual facilita a los usuarios la conexión de sus equipos a la red. La configuración se realiza automáticamente.
- **Movilidad:** IPv6 incluye mecanismos de movilidad más eficientes y robustos.
- **Especificaciones más claras y optimizadas:** IPv6 seguirá las buenas prácticas de IPv4 y elimina las características no utilizadas u obsoletas de IPv4, con lo que se consigue una optimización del protocolo de Internet. La idea es quedarse con lo bueno y eliminar lo malo del protocolo actual.
- **Direccionamiento y encaminado**: IPv6 mejora la jerarquía de direccionamiento y encaminamiento.

- **Extensibilidad:** IPv6 ha sido diseñado para ser extensible y ofrece soporte optimizado para nuevas opciones y extensiones.
- **El nuevo protocolo Neighbor Discovery** (Descubrimiento de vecinos) para la interacción de nodos vecinos en IPv6 consiste en un conjunto de mensajes del Protocolo de mensajes de control de Internet para IPv6 (ICMPv6) que administran la interacción de nodos vecinos. Este protocolo reemplaza el Protocolo de resolución de direcciones (ARP), el Descubrimiento de enrutadores ICMPv4 y los mensajes de Redirección ICMPv4 por mensajes de multidifusión y unidifusión eficaces.

INCONVENIENTES

Son pocos los inconvenientes pero estos existen:

- El propio IPv4, de alguna forma, con los "parches" como NAT.
- En el Aumento del espacio de direcciones del protocolo IPv6, podemos decir que una "desventaja" de estas nuevas direcciones es su dificultad para recordarlas dado su tamaño 3ffe:3330:2:0:2a0:c9ff:fe10:cb02 podría ser tranquilamente nuestra dirección IPv6. Es de suponer que el servicio DNS tendrá más importancia aún.
- La falta de soporte real por parte de fabricantes de routers y software "dominantes".
- La complejidad de la migración/transición.
- Los usuarios necesitan razones comerciales "FORZADAS" para moverse a IPv6.
- El problema del multi-homing.
- Los "fans" del direccionamiento ajustable en longitud.

CAPÍTULO 3

IPv4 VERSUS IPv6

3.1 DIFERENCIAS EN LAS CABECERAS

Para establecer diferencias de cabeceras primero se describirá la cabecera de un paquete IPv4.

Figura 51 - La cabecera IPv4

Como se puede observar, la longitud mínima de la cabecera IPv4 es de 20 Bytes (cada fila de la tabla supone 4 bytes). A ello hay que añadir las opciones que dependen de cada caso.
Los campos de la cabecera son:

- Version – Versión (4 bits)
- Header – Cabecera (4 bits)
- TOS (Type Of Service) – Longitud total (2 bytes)
- Total Length – Longitud Total (2 bytes)
- Identification – Identificación (2 bytes)
- Flag – Indicador (4 bits)
- Frangment Offset – Desplazamiento de Fragmentación (12 bits – 1.5 bytes)
- TTL (Time To Live) – Tiempo de Vida (1 byte)
- Protocol – Protocolo (1 byte)
- Checksum – Código de Verificación (2 bytes)
- 32 bits Source Address – Dirección Fuente de 32 bits (4 bytes)
- 32 bits Destination Address – Dirección Destino de 32 bits (4 byes)

En la figura anterior, se han, marcado, mediante de color de fondo, los campos que van a desaparecer en Ipv6, y los que son modificados, según el siguiente esquema:

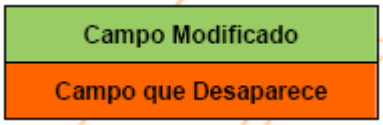


Figura 52 - Campos modificados y que desaparecen

Se ha pasado de tener 12 campos, en IPv4, a tan solo 8 en IPv6. El motivo fundamental de por los que los campos son eliminados, es la innecesaria redundancia. Un caso muy evidente es el checksum o verificación de la integridad de la cabecera: Otros mecanismos de encapsulado ya realizan esta función (IEEE 802 MAC, framing PPP, capa de adaptación ATM, etc.).

El caso del campo de "Desplazamiento de Fragmentación", es ligeramente diferente, dado que el mecanismo por el que se realiza la fragmentación de los paquetes es totalmente modificado en IPv6, lo que implica la total "inutilidad" de este campo. En IPv6 los encaminadores no fragmentan los paquetes, sino que de ser precisa, dicha fragmentación/desfragmentación se produce extremo a extremo.

Algunos campos son renombrados:

- **Longitud Total → longitud de carga útil** (*Payload Length*)
- **Protocolo → Siguiente cabecera (***Next Header***)**
- **Tiempo de Vida → Limites de saltos (*Hop limit*)**

El campo **Versión** queda igual.

Los nuevos campos son:

- **Clase de tráfico** (***Traffic Class***), también denominado **prioridad** (***Priority***), o simplemente **Clase** (***Class***)
- **Etiqueta de flujo** (***Flor Label***)

Estos dos campos son los que nos permiten unas de las características fundamentales e intrínsecas de IPv6: Calidad de Servicio (QoS), Clase de Servicio (CoS), y en definitiva un

poderoso mecanismo de control de flujo, de asignación de prioridades diferenciadas según los tipos de servicios.

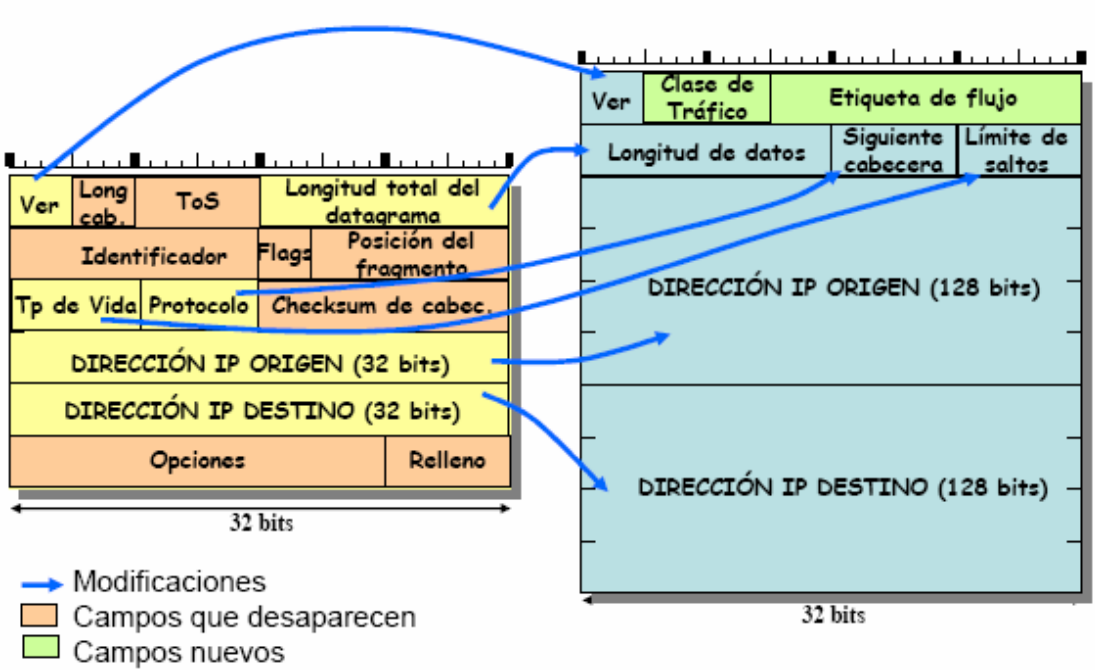


Figura 53 - Cabecera IPv4 Vs IPv6

3.2 CABECERA IPv6

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

Además como ya se ha mencionado, la longitud fija de la cabecera, implica una mayor facilidad para su procesado en routers y conmutadores, incluso mediante hardware, lo que implica unas mayores prestaciones.

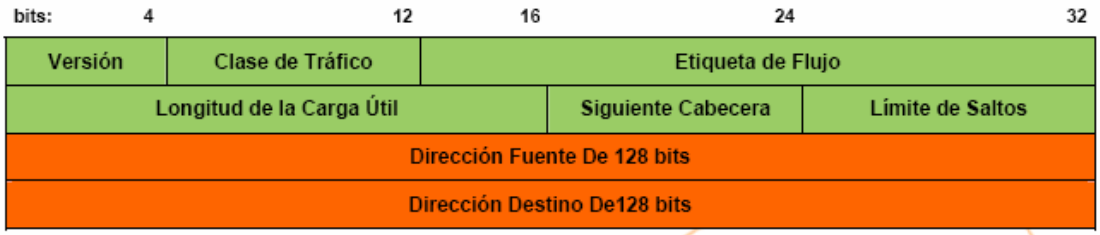


Figura 54 - Cabecera IPv6

3.2.1 CAMPOS DE CABECERA

Estos son los campos que podemos encontrar en una cabecera de IPv6:

- **Versión (*Version*) (4 bits):** Número de la versión de IP; el valor es 6.
- **Clase de tráfico (4 bits):** para poder diferenciar entre servicios sensibles a la latencia, como VoIP, de otros que no necesitan prioridad, como trafico http.
- **Etiqueta de flujo (*Flow label*) (24 bits):** Puede utilizarse por un host para etiquetar aquellos paquetes que requieren un especial manejo dentro de la red por parte de los routers, como veremos más adelante. Longitud de carga útil (*Payload length*) (16 bits): Longitud del resto del paquete IPv6 exceptuando la cabecera, en octetos. Es decir, es la longitud total de las cabeceras extendidas más la PDU del nivel de transporte (a esta porción del paquete es lo que llamaremos *carga útil*).
- **Próxima cabecera (*Next header*) (8 bits):** Como ya hemos mencionado, identifica el tipo de la cabecera inmediatamente siguiente a la cabecera principal.
- **Límite de Saltos (*Hop limit*) (8 bits):** El número restante de saltos permitidos para este paquete. El número máximo de saltos es elegido por la fuente, y ésta pone este campo a ese valor máximo. Este número se decrementa en uno por cada nodo que atraviesa el paquete. El paquete se descarta si el límite de saltos llega a cero. Esta es una simplificación de la idea del campo TTL (*time-to-live*, tiempo de vida) de IPv4. La idea original de este campo era llevar la cuenta del tiempo que esta el paquete en la red, pero el esfuerzo extra que implicaba llevar la cuenta de intervalos de tiempo en IPv4 no añadían una ventaja significativa al protocolo. De hecho los routers IPv4, como norma general, tratan el campo TTL como un campo de límite de saltos. Por ello IPv6 ya parte de esta idea: identificar el tiempo de vida de un paquete con el número de saltos que da dentro de la red, sin dejar espacio a complicadas contabilizaciones de intervalos temporales.
- **Dirección Origen (*Source address*) (128 bits):** La dirección del origen del paquete. Nótese que las direcciones son de 128 bits, no de 32 bits como eran en IPv4. Más adelante veremos esto con mayor profundidad, en el capítulo de direccionamiento.
- **Dirección Destino (*Destination address*) (128 bits):** La dirección del destino deseado del paquete. Esta dirección puede no ser de hecho la del destino último del paquete, si una cabecera de encaminamiento está presente, como veremos más adelante.

3.2.2 CAMPO DE CLASE DE TRÁFICO

Este campo consta de 4 bits que permiten a la fuente identificar la prioridad de un paquete a transmitir respecto a otros paquetes de la misma fuente. De hecho, este campo permite identificar dos prioridades distintas en cada paquete. En primer lugar, los paquetes se clasifican como parte de un tráfico para el cual la fuente esta ofreciendo control de congestión o no; en segundo lugar a cada paquete se le asigna uno de los ocho niveles de prioridad relativa dentro de cada clasificación anterior (con 4 bits tenemos de 0 a 15 etiquetas de prioridad. Las 8 primeras se referirán al primer tipo de tráfico, y las otras al segundo).

Tráfico con Control de Congestión: (*Congestion-Controlled-Traffic*) - se refiere al tráfico para el cual la fuente reacciona a la congestión; un ejemplo es TCP. Veamos lo que esto significa. Si existe congestión en la red, los segmentos TCP tardarán un tiempo mayor que el habitual en llegar a su destino. Como consecuencia de esto los asentimientos de éste también se retrasarán. Según aumenta la congestión, se hace necesario descartar los paquetes en algún punto de su camino: el descarte puede hacerse por un router cuyo buffer se haya desbordado o puede hacerse en una red individual, cuando un nodo de conmutación dentro de la red se congestiona. Ya sea un segmento de datos o bien un asentimiento, el efecto es que la unidad TCP de la fuente no recibe el asentimiento de su segmento transmitido. Entonces TCP responde retransmitiendo el segmento y disminuyendo el flujo de segmentos que genera (para aliviar la congestión).

La naturaleza del tráfico con control de congestión es tal que se acepta una cantidad variable de retardo en el recorrido de los paquetes, e incluso que esos paquetes lleguen fuera de orden. IPv6 define las siguientes categorías de tráfico con control de congestión, en prioridad decreciente (de 7 a 0):

- Tráfico de control de Internet (Internet control traffic): Es el tráfico más importante a distribuir, especialmente en momentos de alta congestión. Por ejemplo protocolos de encaminamiento como OSPF (Open Shortest Path First) y BGP necesitan recibir actualizaciones referentes a las condiciones de tráfico para que puedan ajustar sus rutas para intentar evitar la congestión. Los protocolos de gestión como SNMP (Simple Network Management Protocol) necesitan ser capaces de informar de la congestión a

las aplicaciones de gestión de la red, realizar una reconfiguración dinámica, alterando los parámetros necesarios para hacer frente a esa congestión.

- Tráfico Interactivo (Interactive traffic): Después del tráfico de control de Internet, es el tráfico más importante, como las conexiones en línea usuario-a-host. La eficiencia para el usuario depende críticamente de la velocidad de respuesta de sus sesiones interactivas, por lo que el retardo debe minimizarse.
- Transferencia de muchos datos atendidos (Attended bulk transfer): Son aplicaciones que pueden involucrar la transferencia de gran cantidad de datos; durante éstas, el usuario como norma general está esperando a que se complete la transferencia. Esta categoría se diferencia del tráfico interactivo en que el usuario es consciente de que se producirá un considerable retardo en llegada de los datos que solicitó durante un diálogo interactivo. Un buen ejemplo de esto es la transferencia de ficheros (FTP, File Transfer Protocol). Otro ejemplo puede ser el conocido protocolo de transferencia de hipertexto (HTTP, Hypertext Transfer Protocol), que soporta la interacción servidor-Navegador Web.
- Transferencia de datos desatendididos (Unattended data transfer): Son aplicaciones que el usuario inicia pero que no se espera que se atiendan inmediatamente. Como norma general, el usuario no espera a que se complete la transferencia, sino que realiza otras tareas. El mejor ejemplo de este tipo de tráfico es el correo electrónico.
- Tráfico de relleno (Filler traffic): Es tráfico que de tratará en segundo plano, cuand ya se hayan entregado otras formas de tráfico. Como ejemplo podemos citar los mensajes USENET.
- Tráfico no caracterizado (Uncharacterized traffic): Si la aplicación del nivel superior no le entrega a IPv6 información sobre la prioridad de un tráfico, entonces este es asignado a este valor de prioridad mínimo.

Tráfico sin control de congestión (*Non-Congestion-Controlled Traffic*) - Es tráfico para el cual se desea una tasa de transmisión de datos constante, así como un retardo también constante, o al menos con una variación relativamente pequeña en ambos. Los ejemplos más claros de este tipo de tráfico son las reproducciones de video y/o audio en tiempo real, para los cuales no tiene sentido retransmitir los paquetes descartados. Es más, es importante que se mantenga un flujo de entrega cercano a lo constante. Para este tipo de tráfico se permiten también ocho

niveles de prioridad, que van desde el nivel con prioridad más baja, 8 (en el que más se permite descartar) al de prioridad mayor (menos descartes). En general, el criterio que se sigue es determinar cuanto afectan los paquetes perdidos a la calidad del tráfico recibido. Por ejemplo al sonido de baja fidelidad, (como la voz de una conversación telefónica) se le asignará una alta prioridad, debido a que la pérdida de unos pocos paquetes es apreciable en la línea en forma de clicks y zumbidos. En el otro lado está una señal de video de alta fidelidad, que contiene una considerable cantidad de redundancia, y probablemente no se aprecie tanto la pérdida de algunos paquetes; por ello a este tráfico se le asigna una prioridad relativamente baja.

Es necesario hacer notar que no existe una relación entre las prioridades del tráfico con control de congestión y las del tráfico sin control de congestión. Las prioridades son relativas sólo dentro de cada categoría

3.2.3 CAMPO DE ETIQUETA DE FLUJO

El estándar IPv6 define un flujo (*flow*) como una secuencia de paquetes enviados desde un particular origen a un particular destino (ya sea unicast o multicast), secuencia para la cual la fuente desea un tratamiento especial por parte de los router que intervienen en la comunicación entre origen y destino. Un flujo está unívocamente determinado por la combinación de la dirección de fuente y una etiqueta de flujo de 24 bits distinta de cero. De este modo, todos los paquetes que formen parte del mismo flujo tienen asignada la misma etiqueta de flujo por parte de la fuente.

Desde el punto de vista de la fuente, un flujo será típicamente una secuencia de paquetes generados desde una aplicación de la fuente y que requieren los mismos servicios de transferencia. Un flujo puede constar de una conexión TCP única o incluso múltiples conexiones TCP; un ejemplo de este uso de múltiples conexiones TCP es una aplicación de transferencia de ficheros, que debería tener una conexión de control y múltiples conexiones de datos. Una sola aplicación puede generar un flujo único o múltiples flujos. Nuevamente un ejemplo del uso de múltiples flujos es una conferencia multimedia, la cual debería tener un

flujo para el sonido y otro para las ventanas gráficas, cada uno de los cuales tiene distintos requisitos de transmisión en cuanto a la tasa a la que van los datos, el retardo, la variación del retardo, etc.

Desde el punto de vista del *router*, un flujo es una secuencia de paquetes que comparten ciertos atributos, que afectan al modo en el que el *router* manejará esos paquetes. Estos atributos incluyen el camino, reparto de recursos, requisitos de descarte (cuando debe descartar esos paquetes y cómo), cuenta, y atributos de seguridad. El router puede tratar los paquetes que pertenecen a diferentes flujos de formas muy dispares, entre lo que se incluye almacenarlos en *buffers* de diferentes tamaños, darles diferente prioridad a la hora de reencaminarlos por la red o solicitando para ellos diferentes calidades de servicio de las subredes.

La etiqueta de flujo no tiene un significado especial; en vez de ello la forma especial de manejar los paquetes de ese flujo debe declararse de otra forma. Por ejemplo, una fuente podría negociar o solicitar de los *routers* un trato especial en cuanto al tiempo, por medio de un protocolo de control, o a la vez que se transmite por medio de cierta información en una de las cabeceras extendidas del paquete, como por ejemplo la cabecera de opciones salto a salto. Ejemplos de tratos especiales requeridos para ciertos flujos pueden incluir la petición de alguna clase de calidad de servicio distinta de la predefinida y de alguna forma de servicio en tiempo real.

En un principio, todos los requisitos de un usuario hacia un flujo particular podrían definirse en una cabecera extendida e incluirse en cada paquete. Si se desea dejar el concepto de flujo abierto a la posibilidad de incluir un extensa variedad de requisitos, este diseño desembocaría en cabeceras muy grandes en los paquetes. La alternativa adoptada por IPv6 consiste en la etiqueta de flujo, en la cual los requisitos para un flujo se definen de forma previa al comienzo del flujo, y se asigna una única etiqueta de flujo al mismo. En este caso, el *router* debe guardar la información acerca de los requisitos negociados para cada flujo.

Las siguientes reglas se aplican a la etiqueta de flujo:

- Los *hosts* o *routers* que no soporten o reconozcan el campo de etiqueta de flujo deben poner ese campo a cero cuando originan un paquete, saltarse ese campo sin cambiarlo cuando lo que hacen es reencaminar por la red un paquete e ignorar ese campo cuando reciben un paquete.

- Todos los paquetes que se originan en la misma fuente con la misma etiqueta de flujo (y que ésta sea distinta de cero, obviamente) deben tener la misma dirección de destino, dirección de fuente, prioridad, los mismos contenidos de la cabecera de opciones salto a salto (si esta cabecera está presente) y los mismos contenidos de la cabecera de encaminamiento (si está presente). La intención es que el *router* pueda decidir como encaminar y procesar el paquete simplemente examinando la etiqueta de flujo en una tabla, sin examinar el resto de la cabecera.

- La fuente asigna una etiqueta de flujo a un flujo. Pueden elegirse nuevas etiquetas de flujo de forma (pseudo-) aleatoria y uniforme en el rango 1 a 224 p; 1, sujeto a la restricción que nos dice que una fuente no puede reutilizar una etiqueta de flujo para otro flujo nuevo mientras siga existiendo el flujo actual.

Este último punto requiere una explicación algo más profunda. El *router* debe mantener la información acerca de todos los flujos activos que pueden pasar por él, presumiblemente en alguna clase de tabla. Para que los paquetes puedan reenviarse por la red de una manera eficiente y rápida, el acceso a la información de esa tabla debe ser eficiente. Una alternativa es tener una tabla con 224 (sobre 16 millones) de entradas, una para cada etiqueta de flujo; esto implica una carga de memoria innecesaria en el *router*. Otra alternativa es tener una entrada en la tabla por cada flujo activo, incluir la etiqueta de flujo que le corresponde a cada entrada, obligando de este modo al *router* a buscar por la tabla entera cada vez que llega un paquete. La consecuencia es que se produce un excesivo procesado en el *router*. En lugar de esto, la mayoría de los *routers* se diseñan para utilizar una tabla de tamaño moderado en la que cada entrada se obtiene aplicando un función sobre la etiqueta de flujo. Esta función puede ser simplemente la identidad sobre los bits menos significativos de la etiqueta (unos diez o doce),

es decir, coger los bits menos significativos, o bien puede ser algún tipo de cálculo sobre los 24 bits de la etiqueta. A partir del resultado de aplicar esa función sobre cada etiqueta de flujo obtenemos la entrada a la tabla donde se guarda la información de ese flujo. En cualquier caso la eficiencia de este sistema como norma general depende de que las etiquetas de flujo se distribuyan uniformemente sobre su rango; de ahí el tercer requisito indicado anteriormente.

3.3 CABECERA DE EXTENSIÓN

Como se ha dicho antes, el tamaño de la cabecera IPv6 básica es fijo. Dentro de esta cabecera existe un campo llamado de siguiente cabecera que permite describir con más detalle las opciones del paquete. Esto quiere decir que en realidad tendremos una cabecera de tamaño fijo por norma general y otra cabecera de tamaño variable en caso de que utilicemos alguna de las características avanzadas.

Esta arquitectura es muy flexible, ya que cada cabecera tiene un campo de siguiente cabecera, con lo que podemos tener varias opciones agregadas.

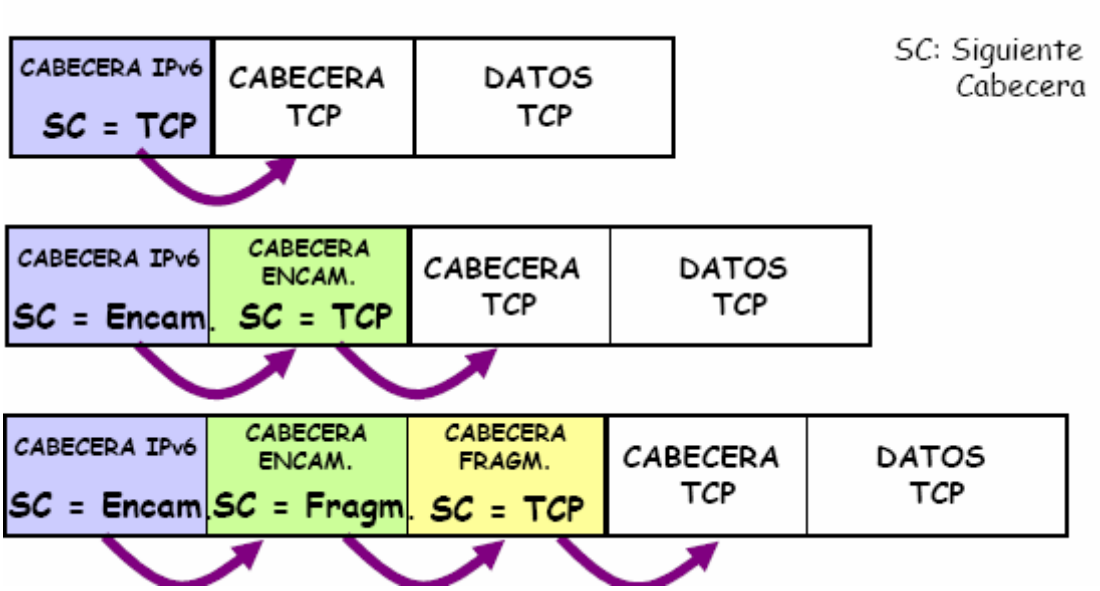


Figura 55 - Diferentes tipos de cabecera de extensión

Se han definido los siguientes 6 tipos de cabecera de extensión:

- **Cabecera con opciones de salto a salto**
- **Cabecera de encaminamiento**
- **Cabecera de fragmentación**
- **Cabecera de autenticación – AH**
- **Cabecera de encapsulamiento de la carga de seguridad**
- **Cabecera de las opciones para el destino**

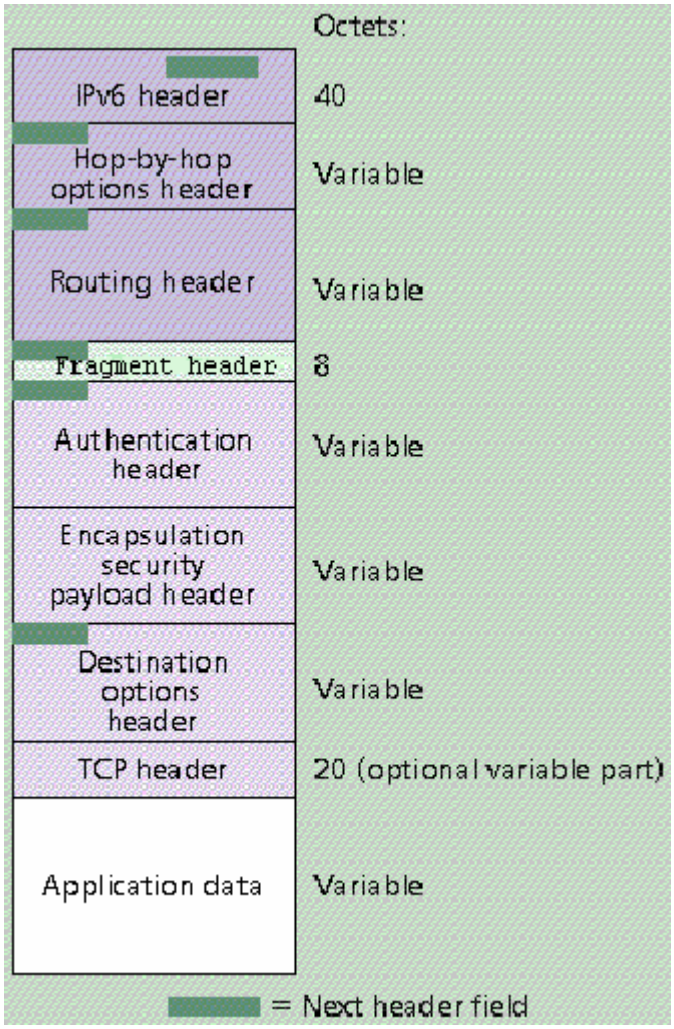


Figura 56 - Paquete IPv6 con las cabeceras de extensión
(Conteniendo un segmento TCP)

3.3.1 CABECERA DE OPCIONES DE SALTO A SALTO

Lleva información adicional que, si está presente, debe ser examinada por cada *router* a lo largo del camino que recorre el paquete. Esta cabecera consiste en (ver figura 2.7):

- Próxima cabecera (*Next Header*): Identifica el tipo de la cabecera inmediatamente siguiente a ésta.
- Longitud de la Cabecera Extendida (*Header extension length*): Longitud de esta cabecera en unidades de 64 bits, sin incluir los primeros 64 bits.
- Opciones (*Options*): Un campo de longitud variable que consta de una o más definiciones de opciones. Cada definición está formada por tres subcampos: tipo de opción (*type opcion*) (8 bits): identifica la opción.
- Longitud (*length*) (8 bits), que especifica la longitud del campo de datos de opción en octetos.
- Datos de opción (*option data*), que consiste en la especificación de la opción (longitud variable).

En realidad son los cinco bits menos significativos del campo tipo de opción los que se usan para especificar una opción particular. Los dos bits más significativo indican la acción que debe llevar a cabo un nodo que no reconoce el tipo de opción, como sigue:

00 - ; Sortear esta opción y continuar procesando la cabecera.

01 - ; Descartar el paquete.

10 - ; Descartar el paquete y mandar un ICMP (*Internet Control Message Protocol*) de *Parameter Problem* (problema con los parámetros), Código 2, esto es un mensaje a la dirección origen del paquete señalando el tipo de opción no reconocido.

11 - ; Descartar el paquete y, solamente si la dirección destino del paquete no es una dirección multicast (esto es, a varias máquinas, ver direccionamiento), mandar un ICMP *Parameter Problem*, Código 2, (mensaje a la dirección origen del paquete, señalando el tipo de opción no reconocido).

El tercer bit más significativo indica si el campo de datos de opción puede cambiar (1) o no (0) en el camino recorrido entre el origen y el destino. Los datos que pueden cambiar deben excluirse del análisis de autenticación que se verá posteriormente.

Estas convenciones para el campo de opción de tipo también pueden aplicarse a la cabecera de opciones de destino.

En el estándar IPv6 sólo una opción está completamente especificada: la opción de los llamados "jumbogramas" (*jumbo payload option*). Esta opción es utilizada para enviar paquetes IPv6 con cargas útiles mayores que 216 (65536) octetos. El campo datos de opción de esta opción es de 32 bits, e indica la longitud del paquete en octetos (excluyendo la cabecera principal). En estos paquetes el campo de longitud de carga útil de la cabecera IPv6 (la principal) debe ponerse a cero, y no tiene que haber cabecera de fragmentación. Los "jumbogramas" tienen una longitud de hasta 4GB, que permiten transferencias más eficientes con pocas interrupciones en la comunicación. Con ello se facilita la transmisión de grandes paquetes de vídeo y permite que IPv6 pueda hacer el mejor uso posible de la capacidad de cualquier medio de transmisión (como puede ser por ejemplo fibra óptica, un medio óptico, medios que por norma general tienen gran capacidad, y en los que interesa que el tamaño del paquete sea mucho mayor para aprovechar mejor las características de los mismos, como se indicó anteriormente).

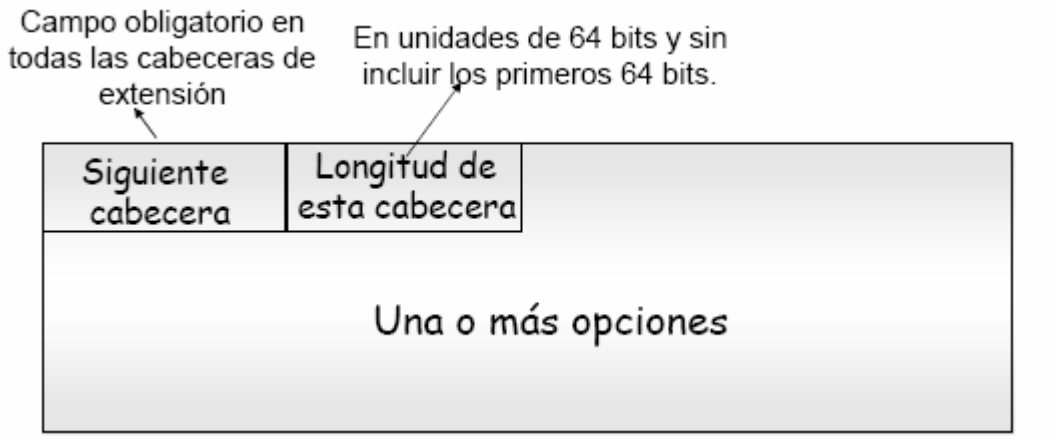


Figura 57 - Cabecera de Opciones Salto a Salto

3.3.2 CABECERA DE ENCAMINAMIENTO

Esta cabecera contiene una lista de uno o más nodos intermedios por los que tiene que pasar el paquete en su camino hacia el nodo destino. Todas las cabeceras de enrutamiento comienzan por un bloque de 32 bits formado por cuatro campos de 8 bits, seguido de los datos específicos de encaminamiento dentro de un tipo de encaminamiento dado. Los campos de 8 bits son los siguientes:

- Próxima cabecera (*Next header*): Como ya hemos comentado varias veces, identifica el tipo de cabecera que sigue.

- Longitud de la cabecera extendida (*Header extension length*): Longitud de esta cabecera en unidades de 64 bits, sin incluir los primeros 64.

- Tipo de encaminamiento (*Routing type*): Identifica una cabecera de encaminamiento particular dentro de las posibles variantes. Si un router no reconoce el valor del tipo de encaminamiento debe descartar el paquete.

- Segmentos restantes (*Segments left*): Número de nodos indicados explícitamente del camino que quedan por visitarse antes de alcanzar el destino final.

Figura 58 - Cabecera de Encaminamiento

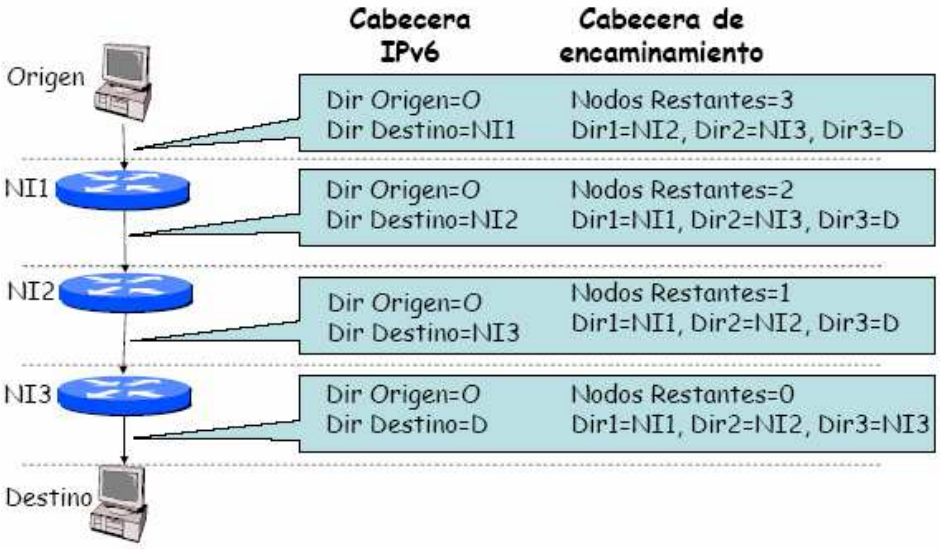


Figura 59 - Funcionamiento Cabecera de Encaminamiento

3.3.3 CABECERA DE FRAGMENTACIÓN

A diferencia de IPv4, en IPv6 la fragmentación sólo puede hacerse en los nodos origen, y no a lo largo de los nodos de la red. Esto tiene la ventaja evidente de que al no fraccionarse los paquetes en la red éstos no se pierden y se evita que un nodo tenga que almacenar muchos fragmentos, y todos los demás problemas derivados de la fragmentación en la red.

Obviamente para realizar la fragmentación desde el nodo fuente, éste deberá implementar un algoritmo descubridor de caminos (algoritmo de encaminamiento) que le permita conocer cual es la unidad de transmisión máxima (MTU) más pequeña de todas las subredes a lo largo de ese camino entre el nodo origen y el nodo destino. Es decir, el algoritmo le permite saber cual es la MTU del cuello de botella del camino (aquel punto donde la MTU es la más pequeña y se van a dar los problemas de fragmentación). Una vez que el nodo fuente sabe esto fragmentará sus paquetes IPv6 como se requiera (con el tamaño de la MTU hallada) para cada destino. Otra posibilidad es que el nodo origen limite todos los paquetes a 576 octetos, que es la mínima MTU que debe soportar cada subred.

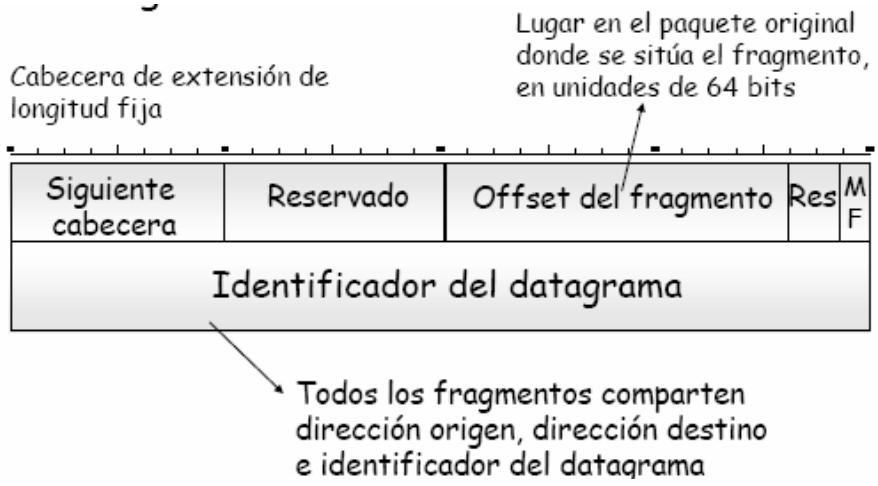


Figura 60 - Cabecera de Fragmentación

La composición de la cabecera de fragmentación y consta de:

- Próxima cabecera (*Next Header*) (8 bits): Identifica el tipo de la cabecera inmediatamente siguiente.
- Reservado (*Reserved*) (8 bits): Para uso futuro.
- Contador de fragmento (*Fragment Offset*) (13 bits): Indica la posición a la que pertenece la carga útil de este fragmento dentro del paquete original. Se mide en unidades de 64 bits. Esto implica que los fragmentos (exceptuando el último) deben contener un campo de datos cuya longitud sea múltiplo de 64 bits Res (2 bits): Reservado para uso futuro. M Flag (1 bit): 1 = más fragmentos; 0 = último fragmento.
- Identificación (*Identification*) (32 bits): Tara de identificar unívocamente al paquete original. Todos los fragmentos que pertenezcan a un mismo paquete deben tener igual el campo de identificación. El identificador debe ser único para un paquete todo el tiempo que ese paquete permanezca en la interred.

El algoritmo de fragmentación es el mismo que el que se utiliza en IPv4

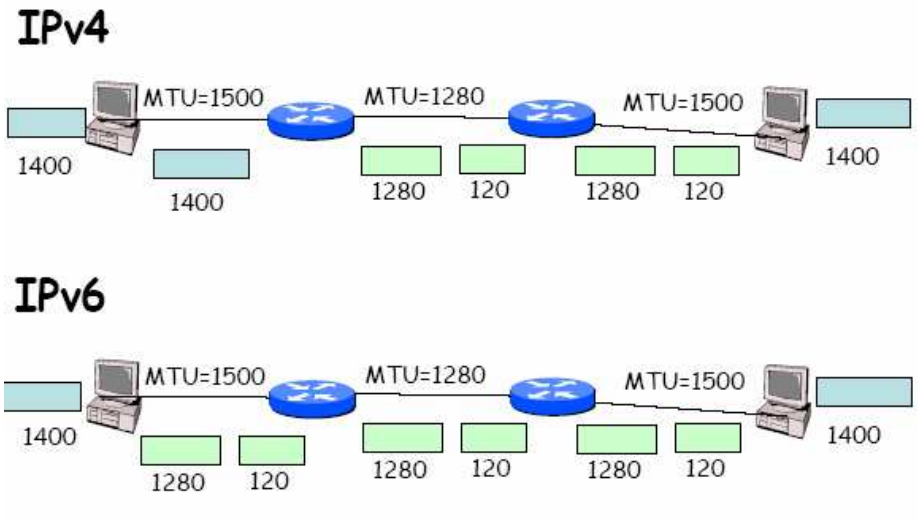


Figura 61 - Fragmentación IPv4 –IPv6

3.3.4 CABECERA DE AUTENTICACIÓN/ENCRIPTACIÓN

Proporciona la integridad del paquete y la autenticación.

Modo Transporte: se asegura (encripta/autentica) la carga de datos del datagrama (PDU de transporte). Se establece entre nodos extremos de la red.

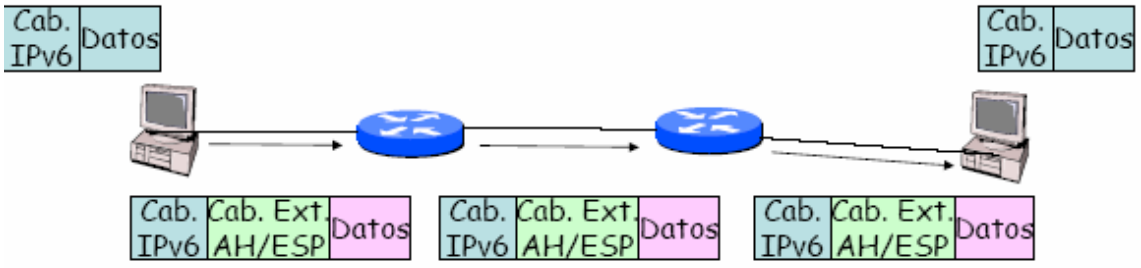


Figura 62 - Modo transporte

Modo túnel: se asegura (encripta/autentica) el datagrama completo → Túnel seguro en la red. Se establece entre nodos intermedios/externos de la red. Las direcciones origen y destinos se modifican con las de los nodos intermedios que implementan IPsec.

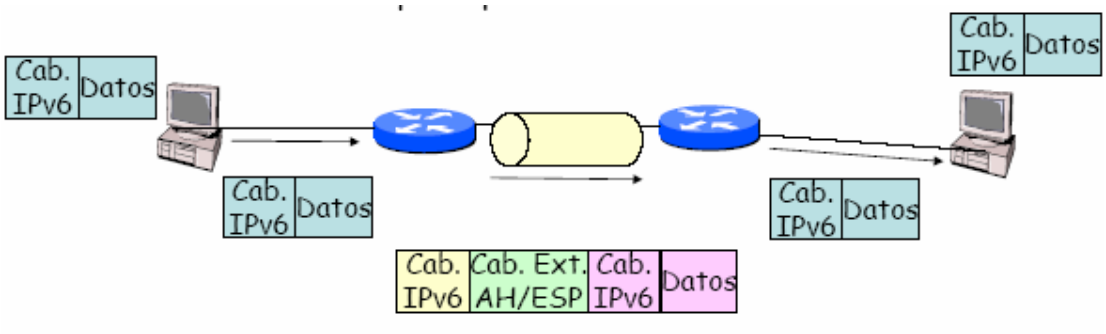


Figura 63 - Modo Túnel

3.3.5 CABECERA DE ENCRIPTACIÓN DE LA CARGA DE SEGURIDAD

Es un valor arbitrario de 32 Bits que usa el receptor para conocer la asociación de seguridad desde la que se ha enviado un paquete entrante. Este campo es obligatorio.

3.3.6 CABECERA DE OPCIONES

La cabecera de opciones de destino lleva información opcional que, en el caso de existir, sólo es examinada por el nodo de destino del paquete. El formato de esta cabecera es el mismo que el de la cabecera de opciones salto a salto.

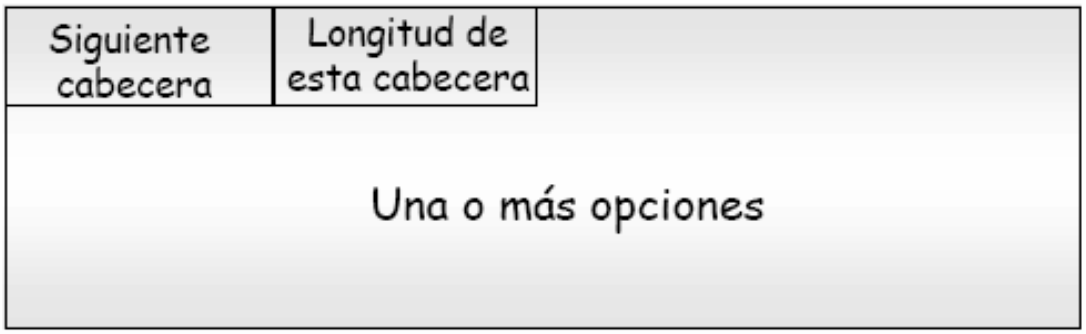
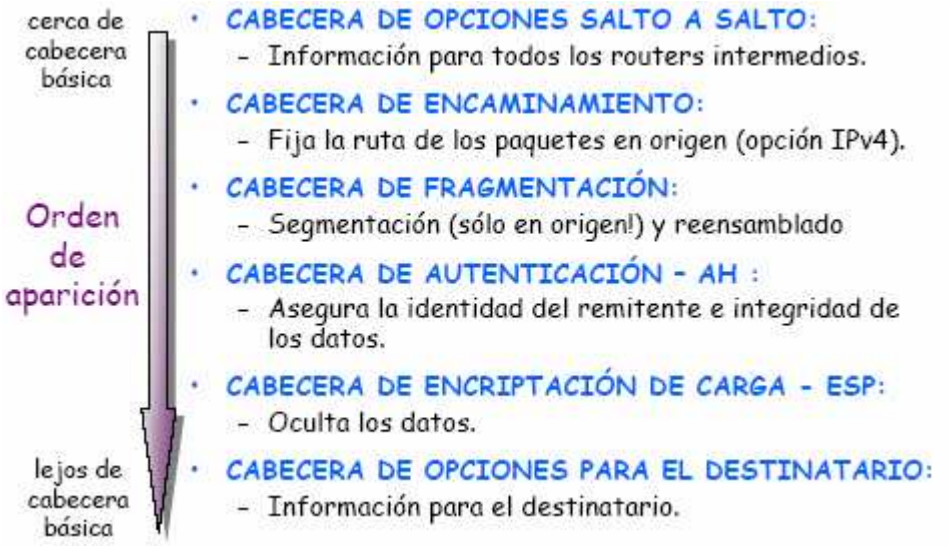


Figura 64 -Cabecera de Opciones



3.4 DIFERENCIAS EN EL DIRECCIONAMIENTO CON IPV4

Hay algunas diferencias importantes en el direccionamiento de IPv6 respecto a IPv4:

- No hay direcciones de broadcast (su función es sustituida por direcciones multicast).
- Los campos de las direcciones reciben nombres específicos; denominados "prefijo" a la parte de la dirección hasta el nombre indicado (incluyéndolo).
- Dicho prefijo nos permite conocer donde está conectada una determinada dirección, es decir, su ruta de encaminado.
- Cualquier campo puede contener sólo ceros unos, salvo que explícitamente se indique lo contrario.
- Las direcciones IPv6, indistintamente de su tipo (unicast, anycast o multicast), son asignadas a interfaces, no nodos. Dado que cada interfaz pertenece a un único nodo, cualquiera de las direcciones unicast de las interfaces del nodo puede ser empleado para referirse a dicho nodo.
- Todas las interfaces han de tener, al menos, una dirección unicast Link-local (enlace local).
- Una única interfaz puede tener también varias direcciones IPv6 de cualquier tipo (unicast, anycast o multicast) o ámbito.

- Una misma dirección o conjunto de direcciones unicast pueden ser asignadas a múltiples interfaces físicas, siempre que la implementación trate dichas interfaces, desde el punto de vista de Internet, como una única, lo que permite balanceo de carga entre múltiples dispositivos.
- Al igual que en IPv4, se asocia un prefijo de subred con un enlace y se pueden asociar múltiples prefijos de subred a un mismo enlace.

3.5 COMPARACIÓN DE LAS CARACTERISTICAS DE IPv4-IPv6

	IPv4	IPv6
Direcciones	Las direcciones de origen y destino tienen una longitud de 32 bits (4 bytes).	Las direcciones de origen y destino tienen una longitud de 128 bits (16 bytes).
IPSec	La compatibilidad es opcional.	La compatibilidad es obligatoria.
Identificación del número de paquetes	No existe ninguna identificación de flujo de paquetes para que los enrutadores controlen la QoS en el encabezado IPv4.	Se incluye la identificación del flujo de paquetes para que los enrutadores controlen la QoS en el encabezado IPv6, utilizando el campo Flow Label (etiqueta de flujo).
Fragmentación	La llevan a cabo los enrutadores y el host que realiza el envío.	No la llevan a cabo los enrutadores, sino únicamente el host que realiza el envío.
Encabezado	Incluye una suma de comprobación.	No incluye una suma de comprobación.
Opciones	El encabezado lo incluye.	Todos se trasladan a los encabezados de extensión IPv6.
Marcos de solicitud ARP	El Protocolo de resolución de direcciones (ARP) utiliza los marcos de solicitud ARP de difusión para resolver una dirección IPv4 como una dirección de capa de vínculo.	Los marcos de solicitud ARP se sustituyen por mensajes de solicitud de vecinos de multidifusión.
Administrar la pertenencia a grupos locales de subred	Se utiliza el Protocolo de administración de grupos de Internet (IGMP).	IGMP se sustituye con los mensajes de Descubrimiento de escucha

		de multidifusión (MLD).
Determinar la dirección IPv4 de la mejor puerta de enlace predeterminada	Se utiliza el Descubrimiento de enrutadores ICMP, y es opcional.	El Descubrimiento de enrutadores ICMP queda sustituido por la Solicitud de enrutadores ICMPv6 y los mensajes de anuncio de enrutador, y es obligatorio.
Direcciones de multidifusión	Se utilizan para enviar tráfico a todos los nodos de una subred.	No hay direcciones de multidifusión IPv6. De forma alternativa, se utiliza una dirección de multidifusión para todos los nodos de ámbito local del vínculo.
Configuración manual	Debe configurarse manualmente o a través de DHCP.	No requiere configuración manual o a través de DHCP.
DNS	Utiliza registros de recurso (A) de dirección de host en el Sistema de nombres de dominio (DNS) para correlacionar nombres de host con direcciones IPv4.	Utiliza registros de recurso (AAA) de dirección de host en el Sistema de nombres de dominio (DNS) para correlacionar nombres de host con direcciones IPv6.
Direcciones IP relacionados con host	Utiliza registros de recurso (A) de puntero en el dominio DNS IN-ADDR. ARPA para correlacionar direcciones IPv4 con nombres de host.	Utiliza registros de recurso (PTR) de puntero en el dominio DNS IPv6.INT para correlacionar direcciones IPv6 con nombres de host.
Tamaño de paquete	Debe admitir un tamaño de 576 bytes (posiblemente fragmentado).	Debe admitir un tamaño de 1280 bytes (sin fragmentación

Tabla 6 - Comparación de las características de IPv4-IPv6

CAPÍTULO 4

SITUACIÓN DE IPv6

4.1 SITUACÍON DE LA DEFINICIÓN DEL PROTOCOLO

4.2 PROBLEMAS DE NORMALIZACIÓN

4.3 COMPETIDORES DE IPv6

4.4 USUARIOS ACTUALES Y FUTUROS

4.5 LUGARES DE PRUEBA E HISTORIAS EXITOSAS

4.6 SITUACIÓN DEL DESPLIEGUE

4.7 ESTADO ACTUAL A LO LARGO DEL MUNDO

4.8 REDES EXPERIMENTALES

4.9 ESTADO ACTUAL EN LATINOAMERICA

4.1 SITUACIÓN DE LA DEFINICIÓN DEL PROTOCOLO IPV6

Según los expertos, en general, el protocolo IPv6 esta bien definido y el núcleo de las especificaciones es muy sólido.

Pero aún existen algunos puntos clave que necesitan trabajos adicionales:

- Problema de Multi-homing. Básicamente el mismo que se tiene en IPv4, y se sigue sobreviviendo. Existen diversas propuestas al respecto, incluyendo el uso de mecanismos de movilidad IP, mecanismos de host, mecanismos de routers, ... En cualquier caso, cualquiera de estas propuestas supone retrasos en el desarrollo e implantación de IPv6.
- Todavía hay quien cuestiona que el direccionamiento de longitud fija sea la alternativa más adecuada. Pero hay que reconocer que el direccionamiento fijo de 128 bits es un límite muy difícil de superar. Actualmente, se está trabajando dentro de este límite con los formatos IPv6 agregables. Ya ha sido mundialmente aceptado, por lo que no hay necesidad de cuestionar de nuevo su redefinición.
- El Grupo de Trabajo DHC del IETF desea verificar que los modelos que están siendo usados como DHCPv6 (la arquitectura es diferente y debe incorporar la RFC 2462 - Stateless Address Configuration) son válidos y trabajarán basándose en los conocimientos adquiridos por las implementaciones DHCPv4. El Grupo de Trabajo IPng quiere extender lo que no se ha podido hacer con DHCPv4 pero sin perder los conocimientos adquiridos en este protocolo. Estos trabajos están siendo finalizados en este momento, y debe de haber un borrador muy sólido en torno a Mayo del 2000, listo para su implementación y para elevarlo a una Propuesta de Norma.
- El uso de ámbitos para unicast de direcciones IPv6, mientras se fijan los procedimientos para su uso y aplicación. Los ámbitos son perfectamente conocidos en IPv6 para unicast de direcciones globales, direcciones de enlace local, y multicast. Se está discutiendo su uso para direcciones locales y como se usarán dentro de la arquitectura, y ello afecta a las implementaciones.
- Aún es precios implementar y comprobar protocolos de Multicast bajo IPv6, dado que, desafortunadamente, aún no han sido lo suficientemente verificados. Existen trabajos en marcha para PIMv6 (Protocol Independent Multicast IPv6), pero no necesitamos

esperar al routing multicast para comenzar la implantación de IPv6. Sería bueno si pudiéramos ver más implementaciones de OSPFv6, dado que tampoco ha sido lo suficientemente verificado en este momento.

- Otra reciente petición ha sido los trabajos para IS-IS para IPv6. IS-IS es un protocolo OSI que puede adaptarse a cualquier otro protocolo mediante su encapsulado. Como IPv4, IPv6, IPX, DecNet, ...

4.2 PROBLEMAS DE NORMALIZACIÓN

La mayor parte de los trabajos han sido definidos como "finalizados" tras el 45° encuentro del IETF en Oslo.

El IESG ha indicado que sólo se requiere algo más de experiencia "en campo", es decir, en aplicaciones reales.

4.3 COMPETIDORES DE IPV6

Hay quien opina que algunas formas de direccionamiento ajustable pueden ser implementadas perfectamente, sin necesidad de mayores modificaciones. Todas las direcciones serían relativas al ámbito de la longitud en la que son usadas.

Es cierto que podría ser una buena solución, sin embargo, el procesado de las opciones de la cabecera sigue siendo una ventaja insuperable de IPv6 sobre cualquier otra solución.

El hecho es que no hay ninguna propuesta real para otros protocolos (fueron rechazadas durante el proceso de selección de IPng). Por tanto, el competidor real puede ser NAT y su descendiente, RSIP.

NAT es casi "transparente" por el hecho de intercambiar espacio de direcciones a costa de la complejidad para su gestión (este punto terminará "matando" este protocolo a largo plazo).

NAT aísla intranets de internet trabajando en contra de la carencia de direcciones. Los esquemas son revisables, dando lugar a múltiples "convertidores" NAT para proporcionar conectividad global. Sin embargo, esta aproximación esta violando el concepto general de Internet: transparencia en el ámbito de la red.

NAT incrementa la complejidad de la configuración y crea puntos únicos de fallo (cuellos de botella) en las conexiones a redes.

NAT rompe el modelo de conexión extremo a extremo (y por tanto rompe el esquema de seguridad extremo a extremo) y predispone a situaciones erróneas (por ejemplo, en la red, lo cual es nefasto para la escalabilidad).

RSIP no es transparente, necesita una actualización para cada aplicación en los nodos extremos (como IPv6) y sólo extiende la longitud real de las direcciones unos pocos bits (lo cual quiere decir que no será suficiente). Por tanto, la única ventaja real de RSIP es ¡su relación con NAT!.

NAT es una ayuda para resolver los problemas de IPv4, pero ha sido comparado con islas fantásticas si pensamos que puede resolver los problemas del núcleo de IPv4 que IPv6 fija definitivamente. NAT es el principal "vendaje" lo que debemos haces es coexistir hasta que IPv6 lo haga innecesario.

4.4 USUARIOS ACTUALES Y FUTUROS DE IPV6.

Obviamente, los mejores objetivos para la aplicación de IPv6 son lugares donde hoy no es posible obtener direcciones IPv4, por añadido, países en desarrollo y crecimiento (dado que los mayores [14]ISP norteamericanos aún mantienen reservas sobre el resto del espacio de direcciones IPv4).

[14] Proveedores de Servicios de Internet

No hay ninguna aplicación "única" para IPv6, sólo resuelve el problema de espacio de direcciones, pero este problema no tiene ninguna otra solución real, y puede evitar que cualquier nueva aplicación con grandes necesidades de espacio de direcciones, como la telefonía IP móvil. Es una realidad, que el número de teléfonos móviles ya ha crecido por encima del número de conexiones a Internet.

Cualquier aplicación que actualmente corre sobre IPv4, lo hará MEJOR sobre IPv6, con muchos recursos adicionales, y ofreciendo mejores métodos para Calidad y Clase de Servicio.

4.5 LUGARES DE PRUEBA E HISTORIAS EXITOSAS DE IPV6

Ya hay cientos de redes funcionando con IPv6, con usuarios reales, corporaciones reales, instituciones de educación y desarrollo, y muchos más preparados para la puesta en marcha. Simplemente dirigiéndonos al Web de 6Bone... podremos descubrir muchos enlaces, a lo largo de todo el planeta. Si esto no es suficiente, como botón de muestra: 6Ren, 6Init, 6Tap, FREEnet, WIDE, US Navy, Eurocontrol.

Probablemente ninguna otra tecnología ha cosechado tantos éxitos en tan poco tiempo como IPv6. Si alguien no lo tiene lo suficientemente claro, basta con leer la prensa especializada desde el momento de la constitución del Foro IPv6.

Por ejemplo:

1. El [15]Dr. Vinton Cerf señala que MCI WorldCom utiliza, en la red vBNS, "IPv6 nativo".

2. NTT ha confirmado que además de haber iniciado servicios públicos IPv6 en Japón, está creando una red mundial basada en IPv6, y ofrecerá, durante un año, servicios gratuitos en la misma, a todos los clientes interesados.

[15] Palabras de el Dr. Vinton Cerf Presidente Honorario del Foro IPv6

4.6 SITUACIÓN DEL DESPLIEGUE DE IPV6

Se ha definido IPv6 como "La Internet del Próximo Milenio", y acabamos de estrenarlo. Desde el comienzo del año 2000 los fabricantes han comenzado a enviar sus propios prototipos y se han comprometido a ellos, e incluso algunos ya tienen productos reales, funcionando perfectamente.

Gran parte de la gente que usa IPv6 lo hace a través de sistemas de túneles. Algunos ya han anunciado ofertas de servicios regulares, nativos IPv6. Han tomado la iniciativa de apostar por el futuro.

Algunos otros grandes ISP esperarán a que los clientes quieran pagar por servicios IPv6 antes de invertir. Es su propia alternativa de negocio.

4.7 ESTADO ACTUAL DE IPV6 A LO LARGO DEL MUNDO

Podemos identificar cinco regiones diferenciadas en lo que al estado de desarrollo de IPv6 se refiere:

1. **Asia:** En esta área, el impacto de la falta de direcciones IPv4 ha sido más obvio, y [16]APNIC, espera agotar su rango de direcciones IPv4 en muy pocos meses. En correspondencia, la presión para encontrar soluciones adecuadas es muy alta, y se han iniciado gran número de actividades, particularmente en Japón: WIDE (http://www.v6.wide.ad.jp)/, KAME (http://www.kame.net/) y TAHI (http://www.tahi.org/).

2. **Europa:** La industria de la telefonía móvil es un soporte muy fuerte para la transición a IPv6. En correspondencia, ETSI (European Telecommunications Standards Institute) y el Foro IPv6 han establecido un acuerdo de cooperación para unificar sus fuerzas; este

[16] Entidad de registro regional de Internet para esta región (http://www.apnic.net/)

movimiento de ETSI ha sido tildado como impulsado por "el fuerte deseo de los operadores inalámbricos".

3. **Norteamérica:** Muchas actividades relacionadas con IPv6, tanto en términos de estandarización y despliegue/verificación, tienen sus orígenes en esta región. Muchas de estas actividades pueden ser localizadas en torno al "6bone", la "plataforma de pruebas" internacional de IPv6 (http://6bone.net/). Otras actividades relacionadas con IPv6 que incluyen importante participación norteamericana son 6REN (http://www.6ren.net/) – iniciativa de coordinación para IPv6 en redes de investigación y educación, 6TAP (http://6tap.net/) – iniciativa para proporcionar un router IPv6 central en Chicago para facilitar la interconexión entre redes IPv6, y Freenet/Viagénie (http://www.freenet6.net y http://www.viagenie.qc.ca/) – iniciativa de túneles automáticos. En cualquier caso, el despliegue comercial de IPv6 en esta región se ha iniciado muy despacio; sólo hay 2 rangos de direcciones IPv6 comerciales en Norteamérica (de un total de 22 en todo el mundo). Esto refleja la apariencia de que el despliegue operacional de IPv6 [17]"puede no llegar primero a éste área", ya que los problemas de la falta de direcciones IPv4 aún no han emergido como una urgencia en esta región.

4. **Rusia:** Las fuertes relaciones entre el Foro IPv6, el Foro IPv6 local Ruso, y FREEnet (red académica y de investigación Rusa). El objetivo es crear una comunidad rusa de usuarios de IPv6 y proveedores de servicios y soluciones.

5. **Resto del Mundo:** A corto plazo, veremos muchos ejemplos, de nuevas actuaciones en México, Corea, India, Australia y Singapur. No es tan extraño dado que son países con alto nivel tecnológico (India) o están situados entre dos grandes áreas de desarrollo (Australia, entre Japón y US). En Singapur la razón es el alto grado de comunicaciones inalámbricas, por medios muy diversos.

[17] Articulo publicado en la pagina IETF (Internet Engineer Task Force) News.

[18]Hay una gran especulación acerca de que esto se convertirá en una gran fuerza según aumente el número de dispositivos de usuario final, como teléfonos móviles y adaptadores de televisión por cable, que requieren direccionamiento IP, lo que obligará a los desarrolladores a escoger IPv6 frente a IPv4 para permitir direcciones únicas para cada dispositivo. Este paso también supondrá, en muchos casos, el uso de NAT's (Network Address Translators), para permitir el transporte de paquetes IPv6 sobre troncales IPv4.

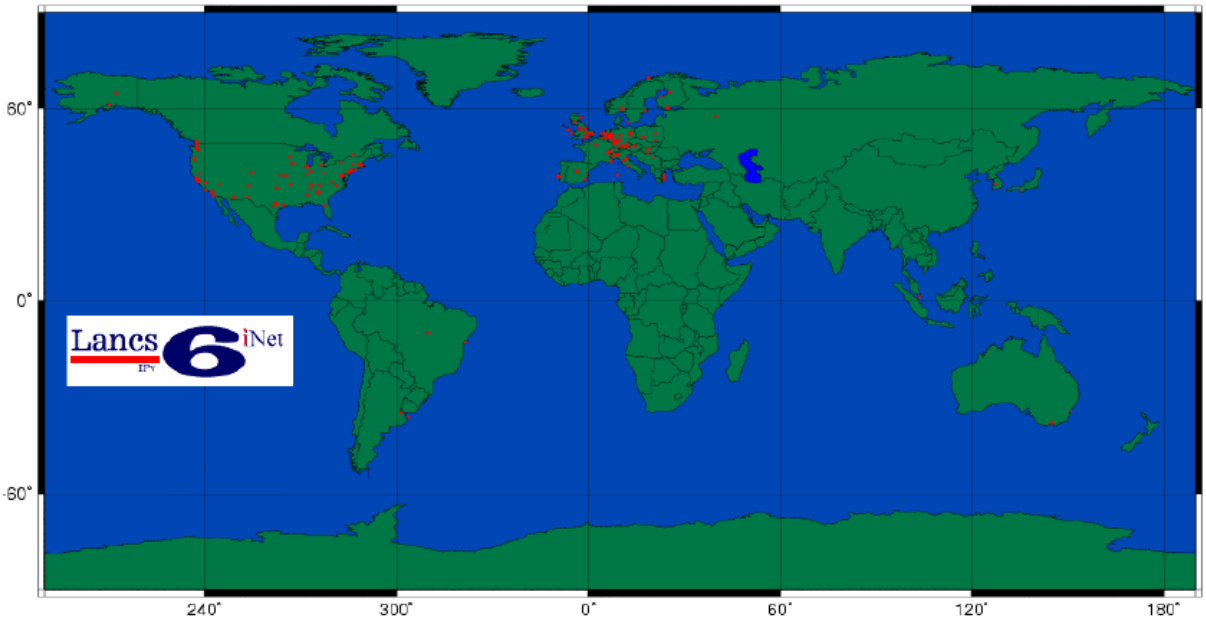


Figura 65 - Concentraciones de nodos en el mundo

En el mundo en 60 países existe un total 1150 &Bone Sites registrados.

4.8 REDES EXPERIMENTALES

4.8.1 6Bone

Derivado del proyecto IPv6 de la IETF nace 6Bone, esta es una red experimental, mundial usada para probar el protocolo IPv6.

[18] Según el Dr. Vinton G. Cerf, Presidente Honorario del Foro IPv6

6Bone actualmente conecta con 57 países participantes, entre ellos Chile y México. La topología de esta red está compuesta por "islas", una isla es un conjunto de equipos y computadores que utilizan el protocolo IPv6 para comunicarse entre sí, unidas por enlaces punto a punto llamados "Túneles IPv6 sobre IPv4", y opera según el esquema de direcciones experimental "IPv6 Testing Address Allocation".

Actualmente se hacen grandes esfuerzos para reemplazar los túneles por links nativos sobre IPv6.

4.8.2 6Ren

En octubre de 1998 la "Energy Science Netword" (ESNET) estableció el proyecto de 6Ren (Red IPv6 para Investigación y Educación), el cual es un proyecto de redes de investigación y educación para proveer servicios de tránsito de IPv6, con el fin de facilitar una alta calidad, alto desempeño y operación robusta en redes de IPv6. el primer paso de 6Ren consistió en establecer interconexiones de IPv6 nativo sobre ATM entre ESNET, Internet2/vBNS, Canarie, Cairn y WIDE.

4.8.3 6Tap

Para facilitar la interconexión de los participantes de 6Ren en E.U.A., Canarie y ESNET patrocinan el proyecto 6Tap que proveerá servicios de ruteo con IPv6, que ayuden en el desarrollo de procedimientos de operación para IPv6.

4.8.4 IPv6 Forum

El IPv6 Forum es un consorcio mundial constituido por proveedores de soluciones de telecomunicaciones, proveedores de servicios de Internet (ISPs) y redes de investigación y educación. El IPv6 Forum se ha impuesto la misión de promover el protocolo de IPv6 para crear la próxima generación de Internet, de mayor calidad y seguridad.

4.9 ESTADO ACTUAL EN LATINOAMERICA

En Latinoamérica existen 57 sitios (redes que trabajan con IPv6) (ver figura 67) (Ver Anexo A)

Los objetivos de estas redes IPv6 son los siguientes:

- Instalar, probar y utilizar la Red Latinoamericana.
- Investigar y probar implementaciones.
- Tener experiencia en IPv6.
- Ayudar en la transición de IPv4 a IPv6.
- Impulsar el desarrollo y el uso de IPv6 y sus aplicaciones.

Figura 66 - Redes IPv6 en Latinoamérica

4.9.1 RED MEXICANA

Los objetivos de esta red son:

- Investigar, probar e implementar el protocolo IPv6 en redes de México.
- Participar en el desarrollo de proyectos de IPv6 nacionales e internacionales.
- Participar en el fortalecimiento y difusión de IPv6 en el mundo y de sus aplicaciones
- Proveer de servicios IPv6 en México y Latinoamérica.
- Instalar y probar distintas aplicaciones IPv6 entre los participantes.

Pruebas:

- Stacks IPv6/IPv4 en distintas plataformas y equipos.
- Aplicaciones IPv6 en diferentes sistemas operativos.
- Herramientas de seguridad con soporte para IPv6.
- IPsec para IPv6 en distintas plataformas y equipos.

Avances:

- Túneles de IPv6 sobre IPv4.
- Túneles de BGP4+ en algunas conexiones.
- Pruebas de IPsec para IPv6.
- Conexiones nativas IPv6.

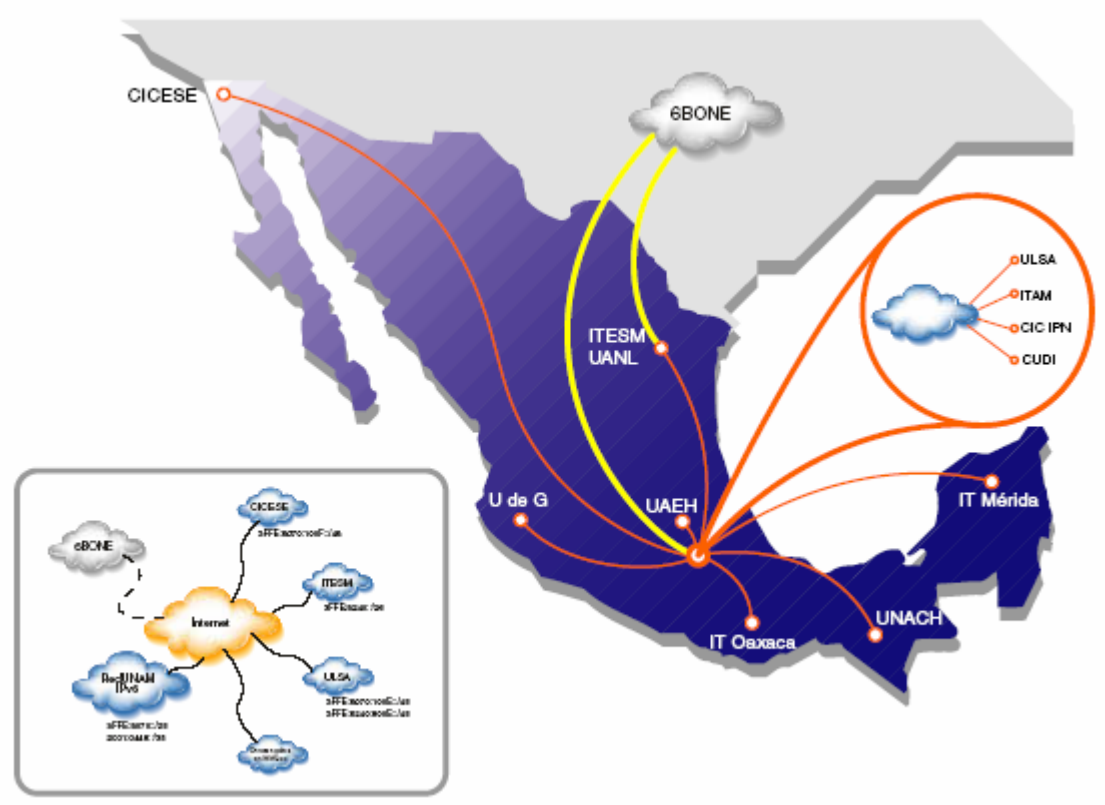


Figura 67 - Red Mexicana IPv6

4.9.2 RED CHILENA

- Propuesta de asignación de direcciones IPv6 para chile.
- Pruebas con herramientas y aplicaciones modificadas con soporte IPv6.
- Colaboración con los demás grupos de trabajo del CUDI (Corporación Universitaria para el desarrollo de Internet).
- Crear un túnel IPv4/IP6 entre la UNAM (Universidad Autónoma de México) y REUNA(a través de la Universidad Austral de Chile).

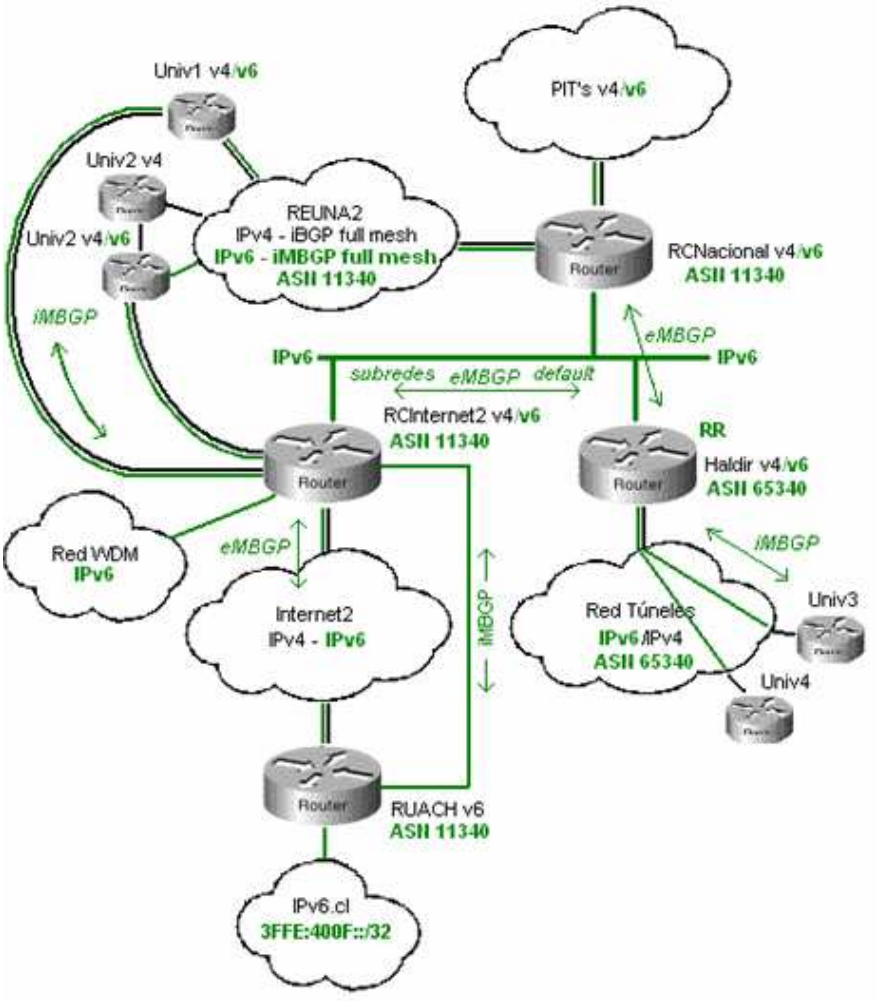


Figura 68 - Diseño de una Red IPv6

CONCLUSIONES

Ipv6 es apropiado para enfrentar los problemas de escalamiento, provee mecanismos flexibles para la transición de la red actual Internet y fue diseñado para manejar los nuevos mercados tales como los computadores personales nómadas, entretenimiento en redes y dispositivos de control.

Ipv6 soporta gran cantidad de direcciones jerárquicas que permiten a la Internet seguir creciendo y proveerla de nuevas capacidades de enrutamiento eficientes. Incluye soporte para aplicaciones en tiempo real, selección de proveedores, seguridad extremo-extremo y auto-reconfiguración.

Ipv6 esta proyectada para correr en redes de alta velocidad y a la vez ser eficiente en redes de ancho de banda bajo, este es un protocolo maduro, aunque existen cuestiones no resueltas todavía, como son: multihoming, anycast, semántica id. Flujo, escenarios de transición, etc.

Este nuevo protocolo mejora el rendimiento de las transmisiones de audio y video en tiempo real. A diferencia de IPv4, IPv6 incluye la información de control de QoS en el encabezado de los paquetes, y así permite la transferencia en tiempo real de audio y video encriptado sin que IPsec afecte la información de control, ya que la encriptación sólo se aplica al cuerpo de los paquetes.

Es evidente que son muchas las diferencias entre IPv4 e IPv6 y que tanto los dispositivos actuales como las aplicaciones que los gobiernan y los programas de comunicaciones deberán ser actualizados para adaptarse al funcionamiento del nuevo formato.

El cambio no debe ser traumático y para ello, los fundadores de IPv6 y sus promotores contemplan todo un programa de acciones que permitan la transición de un protocolo a otro de forma suave y sencilla y que proteja la gran inversión realizada en IPv4.

El camino a IPv4 a IPv6, no es una cuestión de transición ni de migración, sino de evolución, de integración, pero se trata de una evolución disruptora, rompedora y al mismo tiempo necesaria, dicha evolución permitirá un crecimiento escalable y simple.

Este proceso de evolución a IPv6 es que tanto los routers como los servidores compatibles con el nuevo protocolo sean introducidos en el mercado gradualmente lo que permitirá tanto a fabricantes como a administradores de sistemas y usuarios finales realizar el paso a la nueva versión a su propio ritmo.

Llegará el momento en que se de la evolución entre las dos versiones del protocolo. Sin embargo, este cambio va a ser una tarea extremadamente complicada por el gran tamaño que tiene Internet actualmente, y va a ser un proceso de muchos años, complejo y costoso.

Por el momento será necesario que exista convivencia entre los dos tipos de redes y por ende entre los dos tipos de direcciones.

BIBLIOGRAFIA

IPV6: THE NEW INTERNET PROTOCOL, 2nd Edition, Huitema, Christian, Prentice Hall PTR, United States, 1998.

HANDS-ON IPV6, Edition: 1, Goncalves, Marcus, Mc Graw Hill Osborne Media, United States, 1998.

TCP/IP ARQUITECTURA PROTOCOLOS E IMPLEMENTACION CON IPV6 Y SEGURIDAD DE IP. Segunda edición, FEIT, Sidnie, Mc Graw Hill, Madrid, 1998, [Pág. 511-553]

COMUNICACIONES Y REDES DE COMPUTADORES. Sexta edición, STALLINGS, William, Pearson Educación, S.A, Madrid, 2000, [Pág. 510].

REDES GLOBALES E INFORMACION CON INTERNET Y TCP/IP PRINCIPIOS BASICOS. Tercera edición, COMER, Douglas, Prentice-Hall, México, 1996, [Pág. 497-518]

PÁGINAS EN INTERNET

http://www.ipv6.org/

http://www.6bone.net

http://www.ipv6forum.com

http://www.cisco.com/ipv6/

http://www.cu.ipv6tf.org/

http://www.ipv6.unam.mx/historia.html

http://www.ipv6.cl

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

http://www.cs-ipv6.lancs.ac.uk/ipv6/6Bone/Whois/bycountry.html

http://www.aui.es/biblio/libros/mi2000/Jordi%20Pallet.htm

http://www.ipv6.unam.mx/latinoamerica.html

http://www.inforsist.net/articulo.php

http://www.6sos.org/que_es_ipv6.php

http://www.rediris.es/red/reuniones/IPv6practico.pdf

http://www.cisco.com/warp/public/732/Tech/ipv6/

http://mobiquo.dat.escet.urjc.es

http://spisa.act.uji.es/peralta/ipv6

ANEXOS

ANEXO A

SITIOS DE IPv6 EN LATINOAMERICA (REDES EXPERIMENTALES)

ARGENTINA = 14 sitios

AWORLD: Atomic World; Avellaneda_BA, AR
BARRAHOME: Barra Home The Spanish PHP Group
BESOLOCO: Beso Loco, que beso loco.
BOMBI-BOMBI: Bombi-Bombi, Buenos Aires, Argentina.
CENTAURI-AR: Centauri, La Plata, AR
COMPENDIUM-AR: Compendium, Buenos Aires, AR
DIVARSITE: Sitio de experimentación
FIBERTEL: Fibertel TCI Argentina
GEMINIS-AR: Geminis, Buenos Aires, Argentina.
GEMINIS6: Geminis IPV6 test site
IPV6-CCC: Universidad de Buenos Aires- Centro de Comunicación Científica
ORBISTEL: Orbistel, Córdoba, AR
RETINA: Red TeleInformatica Academica
UTN-FRLP: Universidad Tecnologica Nacional - Fac. Reg. La Plata, La Plata / Republica

BRAZIL = 13 sitios

CEFET-BA: CEFET-BA - CENTRO FEDERAL DE EDUCACAO TECNOLOGICA DA BAHIA, FEDERAL CENTER OF TECHNOLOGICAL EDUCATION OF BAHIA
DIVEO-BR: Diveo Brazil Inet6 Site in 6Bone
IAE-SP: Centro Universitário Adventista de São Paulo - Campus 1
IPV6DOBRASIL: IPv6 do Brasil Corporate
PARAISONET: Paraisonet Ltda. (Pegasus Network)
POP-MG: POP Minas Gerais
POP-RN: PoP Rio Grande do Norte
REDEPEGASUS: Rede Pegasus, Pegasus Network Brazil
RNP: RNP - Rede Nacional de Pesquisa, Brazilian National Research Network

SURRIEL: Rik Van Riel's home
UAINET: Uainet Guaxupe Ltda. (Pegasus Network)
UNICAMP: Universidade Estadual de Campinas
UNINCOR: Universidade Vale do Rio Verde - Unincor (Pegasus Network)

 **CHILE = 3**

INF-UTFSM: Universidad Tecnica Federico Santa, Maria - Valparaiso -Chile
UACH: Universidad Austral de Chile(ASN from REUNA), Instituto de Informatica
UACH-IPV6: Universidad Austral de Chile Instituto de Informatica pNLA delegation for the 6bone

 **COLOMBIA = 5**

CORUNIVERSITEC: Corporación Universal de Investigación y Tecnología
EAFIT: Universidad EAFIT
UCAUCA: Universidad del Cauca
UNICAUCA: Universidad del Cauca 6Bone pNLA Site, Popayán(Cauca) - Colombia, Proyecto UniCauca IPv6
UNIMAG: Universidad del Magdalena

 **CUBA = 1 sitio**

CAONAO: Centro de Gestion Tecnologica

 **REPUBLICA DOMINICANA = 3 sitios**

ITHAKA: Ithaka Home Site, Group of I+D on Information Technologies
STON-LOD: Ston´s LinuxOrgDo site
TIGERNET-LOD: TiGeRNeT´s LinuxOrgDo Site, dlsy@linux.org.do

 **MEXICO = 15 sitos**

ASCICESE: CICESE academic member of Red-CUDI (Internet 2 Mexico)
CIC-IPN: Centro de Investigación en Computación, 6Bone Site, Mexico City

CICESE: CICESE academic member of Red-CUDI (Internet 2 Mexico)
CUDI: Corporacion Universitaria para el Desarrollo de Internet (CUDI), IPv6 and Internet2 Testbed
DGSCA: Red para prueba de aplicaciones en IPv6, IPv6 Aplication testing Network
FI-UNAM: Sitio de la Facultad de Ingenieria de la UNAM, IPv6 Testbed
ITAM: Instituto Tecnologico Autonomo de Mexico, 6Bone site, Mexico City
ITESM: ITESM Campus Monterrey, Telecommunications & Networking Department.
ITESM-CCM: Ipv6 ITESM CCM
ITESM-RUV: Tec de Monterrey Virtual University
ITESM-RZN: Tec de Monterrey Rectoria Zona Norte
NIC-MX: ccTLD MX Registry
UDG: Universidad de Guadalajara, Coordinación de Telecomunicaciones y Redes, NOC UDG
ULSA: ULSA academic member of Red-CUDI (Internet 2 Mexico)
UNAM: Universidad Nacional Autonoma de Mexico, 6Bone pTLA Site, Mexico City

PERU = 2 sitios

INICTEL-PE: Instituto Nacional de Investigacion y Capacitacion de Telecomunicaciones. Lima, Peru.
NITCOM: Nucleo de Investigacion Tecnologica Lima-PERU

URUGUAY = 1 sitio

RAU: RAU - Red Académica Uruguaya, SeCIU - Universidad de la Republica, Uruguayan research network

ANEXO B

REDACCIÓN VIRTUAL CISCO SYSTEMS

Diseño de IPv6 atrae a un mayor número de usuarios

El Protocolo de Internet versión 6 (IPv6), es el nuevo protocolo estándar diseñado por la IETF (Internet Engineering Task Force), que permite el crecimiento de Internet de próxima generación al soportar un número creciente de usuarios, aplicaciones mejoradas y la integración de nuevas soluciones tecnológicas.

El Protocolo de Internet versión 6 (IPv6), es el nuevo protocolo estándar diseñado por la IETF (Internet Engineering Task Force), que permite el crecimiento de Internet de próxima generación al soportar un número creciente de usuarios, aplicaciones mejoradas y la integración de nuevas soluciones tecnológicas.

Cisco está tomando un rol activo en definir los estándares de IPv6 y desarrollando productos que soporten este protocolo emergente. Esta semana, se está llevando a cabo el North America Global IPv6 Summit, en San Diego State University, en San Diego, California, en donde Cisco está dando a conocer sus soluciones que soportan IPv6. Redacción Virtual habló con Sangeeta Anand, Vicepresidente de Administración de Producto en la División de Tecnologías de Internet en Cisco Systems, sobre el interés creciente de los clientes en IPv6.

¿Qué es IPv6 y por qué es de interés para los clientes?

Sangeeta Anand: IPv6, o el Protocolo de Internet versión 6, es la próxima generación del protocolo que corre Internet, y es actualmente un conjunto de estándares ensayo de la IETF. IPv6 está diseñado para mejorar el protocolo IPv4 existente, incrementando la escalabilidad

(espacio de direcciones), facilitar configuración y asegurar Internet de próxima generación de alta calidad y segura. Empresas, agencias gubernamentales y proveedores de servicio están mirando IPv6 como un medio para soportar nuevas aplicaciones y servicios, así como nuevos dispositivos. Esto incluye aplicaciones como Telefonía IP, Monitoreo Remoto y Aplicaciones Móviles. Con millones de nuevos dispositivos teniendo en cuenta a IPv6, la necesidad por una conectividad incrementada solo se satisface con la implementación de esta nueva versión del protocolo de Internet.

¿Qué aplicaciones permitirá IPv6?

Sangeeta Anand: Cualquier aplicación que corre sobre IPv4 puede operar sobre IPv6. Sin embargo, IPv6 permite, a través de su espacio de direcciones infinito, despliegue masivo del mercado de aplicaciones y dispositivos IP no tradicionales. Esto incluye dispositivos electrónicos de consumo como DVD players, TVs y cámaras digitales, y equipo residencial de telefonía IP/video conferencia.

¿Qué está haciendo Cisco para soportar IPv6?

Sangeeta Anand: Como líder reconocido en IP Packet Forwarding, Cisco ha ayudado a progresar con rapidez IPv6 por más de una década a través de innovación constante, esfuerzos de estándares y desarrollo de producto. Cisco ha desarrollado software, hardware, servicios y entrenamiento de extremo-a-extremo soportando IPv6 para redes futuras. El software Cisco IOS ofrece la base para la integración y co existencia de IPv6 en Internet. Esto significa que las redes basadas en Cisco son conscientes de IPv6, permitiendo la coexistencia entre IPv4 e IPv6, de manera que los clientes pueden configurar IPv6 cuando se requiera. También permite a nuestros clientes desplegar implementaciones innovadoras como IPv6 sobre MPLS (También conocida como 6PE), y auto configuración CPE a través de DHCPv6 Prefix Delegation. Cisco continuará soportando IPv6 a través de un conjunto superior de funciones planas de control a través de plataformas y ambientes desde redes core a edge, e infraestructuras de acceso de

banda ancha. Para información detallada sobre los esfuerzos de Cisco alrededor de IPv6, ir a http://www.cisco.com/ipv6

¿Qué tipo de organizaciones serán las primeras en desplegar IPv6?

Sangeeta Anand: Las aplicaciones empresariales están conduciendo el despliegue de IPv6. Después de varios años de experimentos, estamos mirando un incremento de las actividades IPv6 para los siguientes mercados: Worldwide National and Research Networks (NRN), y sitios como universidades y laboratorios de investigación que integran IPv6 en sus redes de producción; Proveedores de servicio alrededor del mundo, particularmente en Japón, donde algunos incentivos están conduciendo a su adopción, incluyendo servicios comerciales abiertos IPv6 y ensayos; Proveedores de Servicio Móviles en los Estados Unidos y otras regiones que consideran que los beneficios de IPv6 dan espacio para su modelo de negocio; y Agencias gubernamentales y federales que planean su evolución de infraestructura, y que requieren productos que soportan IPv6.

¿Cual será el impacto de IPv6 en los usuarios finales?

Sangeeta Anand: Debido a que todas las aplicaciones de Internet deberían de correr de manera transparente en IPv4 y IPv6, los usuarios finales no verán ninguna diferencia. Sin embargo, en la medida en que nuevas aplicaciones y dispositivos que corren en IPv6 estén disponibles, el usuario final será capaz de expandir la cantidad de aplicaciones y dispositivos que usa sobre Internet. En el futuro, con IPv6, esperamos que los clientes reciban direcciones IP oficiales, como el número de teléfono de un hogar o la dirección de una calle. Estas direcciones permanentes ofrecerán conectividad constante a Internet, además de eliminar el proceso actual de asegurar una dirección temporal de Internet cada vez que el usuario quiere accesar Internet. Se espera que esas direcciones IP permanentes soporten más fácilmente aplicaciones como juegos distribuidos y Telefonía IP, Fax y Video, así como abrir una variedad de nuevos mercados y aplicaciones innovadoras como e-vehicles.

¿Cuáles son las versiones de Cisco IOS recomendadas para integrar IPv6 en la red del cliente?

Sangeeta Anand: Cisco ha ofrecido soporte para IPv6 desde mayo de 2001 cuando estuvo disponible Cisco IOS 12.2T, para permitir a los clientes comenzar a experimentar con IPv6.

Hoy, IPv6 está disponible en muchas versiones de Cisco IOS. Nuestras recomendaciones sobre las versiones de Cisco IOS para los clientes que están buscando soporte para IPv6, son:

1. Producción General: Cisco IOS 12.3M
2. Core ISP y NREN: Cisco 12.0S en los routers de Cisco de las series 12000 y 10720
3. Infraestructura empresarial e ISP: Cisco IOS 12.2S
4. Acceso de Banda Ancha: Cisco IOS 12.2B
5. Nuevo despliegue tecnológico IPv6: Cisco IOS 12.3T y 12.2S