UNIVERSIDAD NACIONAL AUTONOMA DE MEXICO

FACULTAD DE INGENIERIA

VOZ SOBRE REDES DE TERCERA GENERACION

QUE PARA OBTENER EL TITULO DE INGENIERO EN TELECOMUNICACIONES

PRESENTA

ARTURO GALLARDO CELIS

DIRECTOR DE TESIS

MIGUEL MOCTEZUMA FLORES

CIUDAD UNIVERSITARIA, 2012

1

Introducción

Voz sobre IP es una tecnología para trasmitir voz sobre paquetes de datos utilizando el protocolo IP, pero varios protocolos de paquetes han sido propuestos, probados y desarrollados durante años, incluyendo redes de Voz sobre X.25 (VoX25), voz sobre Frame Relay (VoFR), voz sobre ATM (VoATM), voz sobre IP (VoIP), voz sobre WiFi, y voz sobre MPLS (VoMPLS). De estas VOIP ha sido la cual ha penetrado con mayor fuerza en el mercado en los recientes años y será este quien reemplazara la tradicional conmutación de circuitos de la red pública conmutada (PSTN). Esta tecnología ha sido estudiada desde finales de los años 70's, la realidad es que hasta finales de los 90's se ha implementado con mayor afluencia en redes corporativas principalmente, inicialmente utilizada como una solución media para descargar archivos de audio y video, como es la transmisión de radio por Internet. En estos momentos existe una transición en la industria hacia la convergencia de servicios plenamente multimedia, desarrollo de infraestructura para la comunicación basada en paquetes y en tiempo real para redes empresariales y para empresas prestadoras de servicios, con el objetivo de ofrecer video y voz de forma comercial. Las redes convergentes permitirán entregar en cualquier momento, en cualquier parte del mundo y en cualquier dispositivo de comunicación conectado a la red IP la entrega de audio, video e imágenes.

Con la aparición de los DPS (Digital Signal Processing) a principios de los años 80's, la compresión de voz y datos tuvo el impulso para proporcionar servicios multimedia sobre paquetes. Los servicios y tecnologías de VOIP comerciales comenzaron aparecer a principios del nuevo siglo con la primera generación de redes (1G), desde entonces las redes comerciales, proveedores de servicio celular, proveedores de voz sobre cable, proveedores de "triple play" y proveedores tradicionales de voz todos están migrando a VoIP, lo cual representa la segunda generación de tecnología, la siguiente generación (3G) está en proceso diseño para aparecer en un par de años, sin embargo en pases Asiáticos a es un hecho.

Una buena aceptación está causando VoIP en medianas y grandes empresas por el ahorro de dinero en comparación con la comunicación de voz tradicional. Las grandes empresas están utilizando esta herramienta para soportar movilidad y presencia para sus usuarios finales, les permite desarrollar nuevas aplicaciones como la mensajera unificada, y el roaming para teléfonos celulares entre redes locales y redes prestadoras de servicios. Las empresas transportadoras están desplegando estos servicios para generar nuevo ingresos y sustituir los basados en TDM y, entrar a nuevo mercados (como ofrecer servicios de voz, banda ancha y televisión de paga).

La expansión de VoIP ha sido de gran éxito, pero se tienen dos problemas fundamentales que pueden impedir su escalabilidad, la primera de ellas es la baja calidad de servicio en redes IP desplegadas en todo el mundo, tanto en nivel de transporte como a nivel empresarial. El segundo problema se refiere al trasporte de la señalización y el estableciendo de la ruta de VoIP, concretamente a que los paquetes de VoIP tienen problemas para ser transportados a través de dispositivos de seguridad en redes como el firewall, no solo por las particularidades de protocolo, sino por los problemas de traducción de direcciones. Además se pueden presentar problemas de seguridad en las conexiones, como la escucha y el Hawking. La tercera generación de redes (3G) pretende dar solución a estos problemas, concretamente a la escalabilidad y fiabilidad comercial, basándose en IPv6.

IPv6 ofrece el potencial de lograr la escalabilidad, la fiabilidad, conectividad extremo a extremo, calidad de servicio y la robustez necesaria a VoIP para sustituir a través del mundo la telefonía conmutada en circuitos, específicamente IPv6 trata los problemas relacionados con calidad de servicio y traducción de direcciones. IPV6 es considerado para ser el protocolo de la próxima generación de Internet. La actual versión de Internet, IPv4, ha sido utilizada por más de 30 años y exhibe retos emergentes con el espacio de direccionamiento, movilidad y seguridad. IPv6 es una versión mejorada del protocolo de Internet que esta diseño para coexistir con IPv4 y eventualmente mejores capacidades de interconexión que IPv4. La gama de aplicaciones que se pueden desarrollar con este protocolo no solo incluye VoIP, también redes WiFi, 3G y 4G para telefonía móvil, televisión sobre demanda y seguridad por mencionar algunas.

IPv6 fue inicialmente desarrollado en los principios de los años 90's por la IETF denominado como IPng y liberado en septiembre de 1995, originado por la anticipada necesidad de direcciones por el crecimiento exponencial de Internet, como es el desarrollo de teléfonos celulares, PDA y el incremento de usuarios conectados a la red por ciertos países del mundo, como es el caso de India y China. Las tecnologías nuevas como VoIP, acceso siempre a Internet, Ethernet en casa y nuevas aplicaciones de computación aumentan la necesidad de conectividad en los años próximos.

Ante este actual estado de crecimiento una solución acorto plazo es NAT, la cual proporciona un método de traducción de direcciones y de puertos. El NAT básico traduce direcciones locales a direcciones globales y viceversa, las cuales están almacenadas y relacionadas en una tabla de traducción de direcciones. Esto, sin embargo, afecta la accesibilidad, el alcance y la individualidad de los dispositivos conectados a la red global. El NATP ofrece una traducción donde muchas direcciones de red y puertos son traducidas a una sola. La implementación de NAT ofrece ahorro de dinero para las empresas y usuarios que no tienen las suficientes direcciones publicas en su red, sin embargo no es totalmente compatible con VoIP.

La expectativa con el nuevo protocolo de IP es bajar los costos de cada dispositivo de red, más poderosos y con un menos consumo de energía, el problema de energía no solo importa por razones ambientales, sino que también mejora la

operatividad (por ejemplo mayor batería en dispositivos portátiles, como son los teléfonos celulares). Ipv6 puede mejorar el Internet o una Intranet, como por ejemplo:

- Mejora las capacidades de direccionamiento.
- Configuración y autoconfiguración sin servidores.
- Mecanismos de de movilidad más eficientes y robustos
- Seguridad punto a punto, con encriptación y autentificación de la capa IP.
- Mejor soporte para tráfico multicast y calidad de servicio.

En el sector gubernamental y corporativo podrán alcanzar un número de mejoras en sus redes con la implementación de IPv6, mientras que la función básica de los protocolos de Internet es mover información a través de las redes, IPv6 tiene más capacidades incorporadas que IPv4, por ejemplo el aumento significativo del espacio de direccionamiento. Los usuarios buscan simplicidad de autoconfiguración, colaboración y movilidad. IPv6 es un protocolo convergente para el mundo IP del mañana, como se muestra en la figura 1.1.

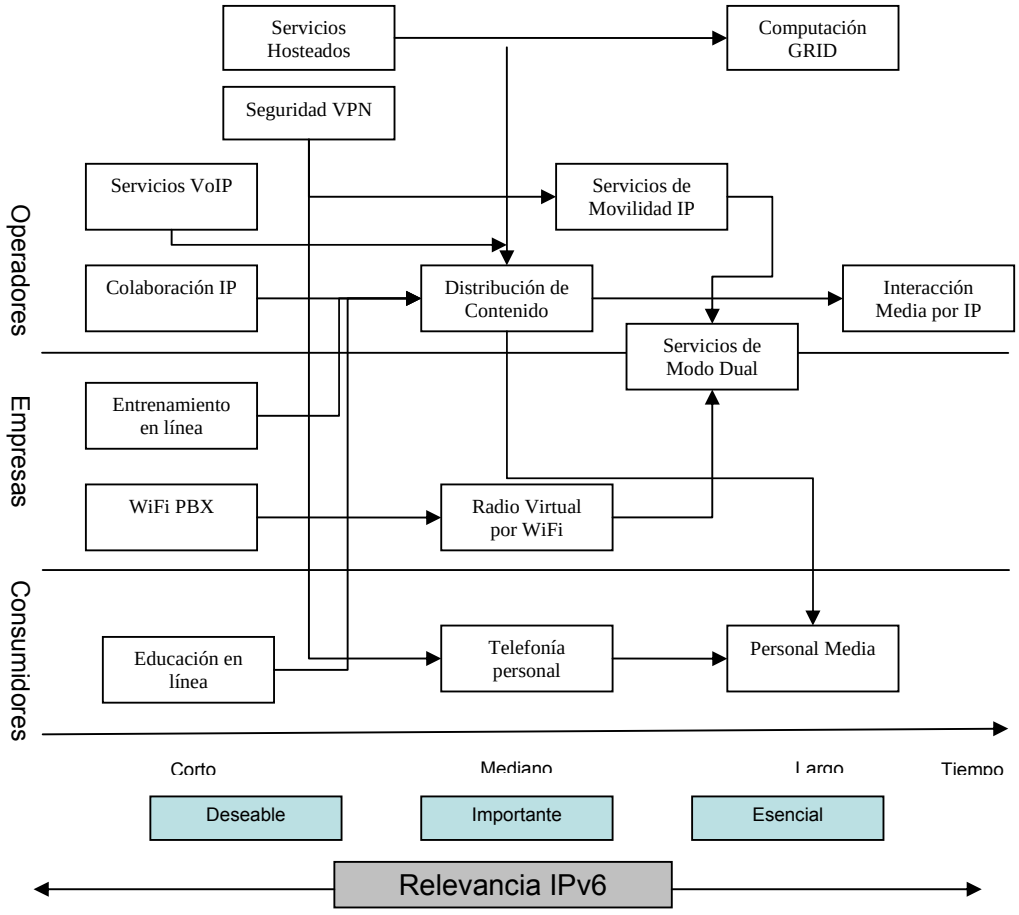


Figura 1.1 Convergencia de IPv6.

En un ambiente IPv6 cada dispositivo tiene una dirección IP única y global, por lo que puede ser localizado, mientras que hoy en día cada dispositivo tiene una dirección física irrepetible. En IPv6 el espacio de direccionamiento extendido suministra una dirección única a cada dispositivo de red. Ipv6 ofrece más seguridad en

la red que el protocolo actual IPv4, también cuenta con mecanismos de autoconfiguración automática, sustituyendo técnicas con el DHCP para IPv4.

Las áreas de crecimiento en las telecomunicaciones a corto y mediano plazo se encuentran además de VoIP, wíreless, IPv6 y nanotecnología. IPv6 ya es implementado en algunas partes del mundo; en Asia debido a la alta demanda de direcciones IP y el poco espacio de direccionamiento organizaciones como WIDE, KAME y TAHI encuentran en IPv6 una solución adecuada a este problema; en Europa el desarrollo de la telefonía móvil es soporte para la transición a IPv6, la ETSI (Europan Telecomunications Standards Intitute) ha sido una precursora a la redes de la siguiente generación basada en IPv6; en Norteamérica es donde muchos términos de estandarización y despliegue de tecnología tiene origen, las cuales son localizadas en torno al 6bone, que es la plataforma de pruebas para IPv6, el avance comercial es lento, debido a la cantidad de direcciones IPv4 asignadas a esta zona, para lo que la IETF ha publicado que el despliegue operacional puede no llegar primero en esta área.

Los sistemas de VoIP, y aun mas los dispositivos móviles, requieren interconexión punto a punto entre entidades como son elementos de red VoIP/ gatekeepers / gateways / Servidores SIP / Proxys / Servidores de Registro, Redes LAN inalámbricas 802.11, Firewalls, Gateways de aplicación, dispositivos IPsec, nodos VPN, servidores de DCHP, servidores DNS, sistemas y aplicaciones de escritorio. Algunos de estos elementos no trabajan correctamente en un ambiente IPv6. Estos elementos aplican para redes puramente IP en un ambiente empresarial VoIP o un ISP (Prestador de Servicio de Internet). Un gran número de instituciones han o un amiente hibrido, utilizando comúnmente un PBX o un multilíneas para comunicarse con la red PSTN y una interface física a la red IP para servicios de VoIP, limitando los recursos de movilidad, presencia, productividad y mejoras que ofrece esta tecnología en un ambiente puramente IP, sin embargo la transición solo será cuestión de tiempo.

1.1.- Introducción IPv6.

IP fue diseñado en los años 70's con el propósito de conectar computadoras que estuvieran en lugares geográficos diferentes. Las computadoras estaban conectadas entre sí a través de redes locales, pero estas redes locales estaban aisladas. El departamento de defensa de los EUA desarrollo la pila de protocolos TCP/IP con el propósito de conectar esas islas de maquinas entre sí con un lenguaje común. La aplicación práctica del protocolo IP es el Internet, que se define como red de redes o bien la conexión entre redes. En sus inicios solo tenía un uso militar pero las redes de universidades, usuarios y empresariales fueron pronto añadidos por su necesidad de intercambiar información.

El protocolo de Internet utiliza direcciones lógicas para identificar y localizar a - cada dispositivo conectado a la red. En una red los elementos que forman parte de la red, como son servidores, routers, computadoras personales, puertas de enlace, etc, se comunican entre ellos utilizando su dirección IP como identificador, de tal forma que se requiere que cada dispositivo se alcanzado desde cualquier punto de Internet.

La versión actual de IP es antigua. La versión 4 del Protocolo de Internet se normalizo en septiembre de 1981 por el IETF. IPv4 ha demostrado, por largo de su larga vida, ser un mecanismo fiable y de gran alcance. El crecimiento desmedido del Internet causo a los desarrolladores darse cuenta que las necesidades de comunicación en el siglo XXI requieren un nuevo protocolo con nuevas funciones y

capacidades, mientras que al mismo tiempo conserve las características útiles del protocolo existente. En 1992, la normalización de una nueva generación del Protocolo de Internet (IP), con frecuencia denominado IPng, fue soportada por el Grupo de Ingeniería de Internet (IETF). IPng se conoce ahora como Protocolo de Internet versión 6 (IPv6). IPv6 está definido en el RFC 2460. Los problemas específicos que se descubrieron con IPv4 que motivaron el desarrollo de un nuevo protocolo de Internet son el agotamiento de las direcciones de red IPv4 y el incremento rápido y sustancial de tamaño de las tablas de enrutamiento de Internet debido al crecimiento de este ultimo.

Durante las últimas dos décadas, se han desarrollado numerosas extensiones para IPv4 específicamente diseñadas para mejorar la eficacia con que puede utilizarse el espacio de direcciones de 32 bits. Mientras tanto, se ha definido y desarrollado una versión de IP más extensible y escalable que utiliza128 bits en lugar de los 32 bits actualmente utilizados por IPv4. IPv6 utiliza numerosos hexadecimales para representar los 128 bits. Proporciona 16 mil millones de direcciones de IP, lo que representa suficientes direcciones para las necesidades futuras de comunicación.

IPv6 mejora en áreas de enrutamiento autoconfiguración y seguridad sobre una red. Los nuevos dispositivos conectados al Internet serán dispositivos “plug-and-play”, es decir auto configurables. Con IPv6 no requiere configuración de dirección IP, puerta de enlace y mascara de red de forma manual, solo será requerido conectarse a la red y el equipo automáticamente cargara su perfil de red.

Las redes IPv6 tienen una gran cantidad de aplicaciones en diferentes tipos de redes, entre otras, intranets corporativas, redes institucionales y extranets, redes de movilidad, redes 3G inalámbricas, redes de gobierno, el Internet y la red VoIP, esta última tecnología es el motivo de estudio del presente trabajo de investigación. IPv6 será el protocolo para desarrollar nuevos servicios para el mercado de las telecomunicaciones, en conjunto con tecnologías ya establecidas como Wi-Fi, por ejemplo se pretende ofrecer Voz sobre Wi-Fi (VoWi-Fi). Los prestadores de servicio intentan añadir la movilidad a servicios de voz ya existentes y ampliar servicios calificados más allá de sus áreas e cobertura. Las nuevas aplicaciones incluyen cubrir servicios en edificios blindados, tarjeta virtual de llamada, llamadas desviadas, roaming fuera de a red, movilidad en servicios multimedia, entre otras.

1.2.- Introducción de VoIP

La tecnología para redes de datos basadas sobre paquetes, en particular IP, han progresado hasta el punto que ahora soportan aplicaciones multimedia y transporte de voz en tempo real sobre estas redes. Las redes empresariales, las celulares, las redes de VoIP, redes de triple play y aun las redes tradicionales se están migrando rápidamente al mundo de VoIP, con la meta de establecer redes integradas. No solo las grandes empresas se están empezando a habituar con las nuevas tecnologías, sino también los usuarios residenciales se comunican entre si a través de algún programa conectado a Internet, como es el caso de Skype, el Messenger de Microsoft. Además, los gigantes de Internet, como AOK, Google, MSN y Yahoo, se han embarcado en una carrera por ofrecer servicios de voz sobre IP gratuitos, que les permitirá aumentar su base de usuarios y elevar sus ingresos por publicidad.

El transporte de voz sobre el protocolo IP se ha convertido en una manera muy popular de de ahorro en las comunicaciones, ya que resultan muy baratas y, en muchas ocasiones, incluso gratis al hacer uso de las redes de transporte de datos

para la transmisión de la voz, lo que está haciendo que la telefonía tradicional pierda terreno entre aquellos clientes que se adaptan bien a las nuevas tecnologías, pues todo lo que requiere es una conexión a una red IP, como puede ser Internet, y una computadora personal con una tarjeta de sonido y con el software adecuado, o un teléfono IP.

La tecnología de voz sobre IP, que solo en los últimos tiempos ha alcanzado una calidad aceptable y resuelto algunos problemas de interoperabilidad, se considera un servicio indispensable para el crecimiento de usuarios en los operadores de Internet, ofreciendo servicios de banda ancha con tarifa plana.

De igual forma que las telecomunicaciones, VOIP ha experimentado procesos de cambios intensos y decisivos. Después de la desregulación, de la modernización y de las privatizaciones que se iniciaron en todo el mundo desde mediados de los ochenta, las telecomunicaciones alcanzaron un momento de crisis a principios del nuevo siglo. Un nuevo factor de crisis comenzó aparecer en las grandes empresas, este factor es la evolución tecnológica. A esta evolución se le conoce como las Redes de Próxima Generación (RPG) o Redes de Nueva Generación (RNG)

Actualmente la red básica consta de tres redes interconectadas, las cuales son:

La Red de Telefonía Pública Conmutada (PSTN) o red telefónica tradicional, con líneas dedicadas, centrales de conmutación telefónica, el nodo telefónico como núcleo de la red y un sistema universal de numeración. Estos componentes tenderán a desaparecen como tales con la evolución tecnológica. El sistema de numeración puede cambiar de acuerdo a las necesidades de cada país o continente.

La segunda red es la inalámbrica, encabezada por la telefonía celular. Sin embargo, nuevas tecnologías inalámbricas (entre las que despuntan el WiFi y el WiMax) anticipan un desarrollo creciente del inalámbrico. Lo que ha sucedido con la telefonía móvil celular puede ser un anuncio de este proceso. En los últimos quince años, la red de telefonía móvil celular ha tenido un avance espectacular marcado por cuatro generaciones tecnológicas (primera generación analógica, segunda generación digital sistema GSM, segunda generación y media: sistemas GPRS, Edge bluetooth y actualmente la cuarta generación teniendo como núcleo a IP).

La tercera generación es el Internet diseñada para transmitir datos sobre toda una gama de medios de comunicación.

El valor de la PSTN puede quedar reducido a cero, a menos que esta red evolucione rápida, eficiente y competitivamente para convertirse en una red de próxima generación. Este es uno de los desafíos más importantes que enfrentan las empresas telefónicas tradicionales, cuya red, desde el punto de vista de los clientes, se convertirá en una de varias para acceder a los nuevos servicios. Para VoIP el auge comenzó a partir que apareció la primera generación, la segunda y finalmente se desarrolla la tercera generación.

1.2.1.- Primera Generación de redes VoIP.

A lo largo de los años se ha logrado alcanzar la integración de servicios multimedia, el único mecanismo viable para alcanzar la integración son las redes basadas en IP. Sin embargo, la investigación de Redes de Servicios Integrados (ISDN) comenzó en Japón con la idea de desarrollar e implementar redes Integradas. La

meta principal era soportar voz y datos sobre redes TDM. La idea de trasportar voz sobre redes de datos ha recibido una considerable atención comercial desde hace más de 10 años. Se ha transportado la voz sobre diferentes tipos de redes basadas en ATM, FDDI y redes LAN.

La primera generación (1G) de productos VoIP empezaron aparecer a mediados de los años 90's. Estos productos eran rudimentarios y típicamente solo soportaban servicios de telefonía básica: por ejemplo tono de invitación a marcar desde la intranet y conexiones a la PSTN. Además de no tener una amplia gama de funciones en los dispositivos de voz, esta generación de productos careció de confiabilidad comercial y tenia capacidades muy limitadas de señalización. Los equipos no soportaban la calidad de servicio, proporcionando una calidad de audio bastante deficiente, no contaban con energía en línea y servicios de emergencia.

1.2.2.- Segunda Generación de redes VoIP

Los productos de segunda generación (2G) fueron introducidos al mercado a principios del año 2000. Estos dispositivos comenzaron a soportar servicios de telefonía más avanzados; por ejemplo la conferencia, menor costo de enrutamiento, calidad de servicio y algunas características inalámbricas y de seguridad. La confiabilidad y administración mejoraron. Los dispositivos VoIP comenzaron a soportar la señalización de una manera más intrínseca y con protocolos más maduros (por ejemplo SIP y H.323). La energía en línea y servicios de emergencia eran ya soportados en este generación. Sin embargo la integración con los servicios de correo electrónico seguían siendo una problemática, así como la mensajería unificada y los directorios centralizados.

Muchos organismos, empresas y otras entidades han empezado a publicar especificaciones del protocolo VoIP en los recientes años y una serie de equipos de red de voz sobre datos ha aparecido y está apareciendo en el mercado con un constante movimiento. Por ejemplo la plataforma de teléfonos IP para áreas empresariales y puertas de enlace de la red IP a la red pública han sido introducidas en el mercado, algunos ejemplos se presentan en la figura 1.2. Grandes empresas como Cisco, Avaya, Siemens, Panasonic, Alcatel y empresas libres desarrollan nuevo hardware para VoIP.

Figura 1.2 Teléfonos VoIP.

El desafío mayor es que las redes IP públicas y las redes empresariales no soportan aun características de calidad de servicio (aunque actualmente la calidad de servicio se construye en el dispositivo final). También, se cuentan con problemas de seguridad con dispositivos, como el firewall, problemas de traducción de direcciones y traducción de puertos.

Considerando la base de equipos instalados en el mercado, el de mayor auge es el PBX tradicional, llega a ser imprescindible que alguno nuevo sistema basado en IP deba integrar con eficacia las soluciones ya existentes y facilitar la inflexión hacia soluciones más maduras. La interconectividad que ofrece IP permitirá a los sistemas de telefonía de la siguiente generación ser diseñados con arquitecturas descentralizadas, como antes no era posible. En VoIP, la red IP por si mismo se convierte en equipo de conmutación, con el procesamiento de llamadas y aplicaciones distribuidas en diferentes servidores conectados a través de la red.

Las principales arquitecturas alternativas desarrolladas a nivel comercial para una red 2G son las siguientes:

- Troncales VoIP, como son troncales tipo TIE contratadas con proveedores de Internet.
- Un PBX tradicional con interfaces IP.
- Sistemas híbridos TDM/IP.
- Sistemas solamente IP basados en servidores.

La evolución a la siguiente generación de VoIP en una plataforma IPv6 será gradual, pero en el mercado empresarial se tienen diferentes escenarios de transición. Inicialmente las grandes empresas pueden integrar a sus sistemas de telefonía tradicional interfaces IP las cuales deberán estar conectadas a su red, estas interfaces tendrán la función de convertir la voz en paquetes de datos para ser transmitidos por un protocolo de red. Sin embargo, es posible actualizar su PBX para soportar IP, lo cual tiene como desventaja el costo económico que esto implica. Finalmente, la migración de mayor costo es reemplazar el sistema de voz por un sistema puramente IP. La transición permitirá converger a una red VoIPv6.

1.2.3.- Tercera Generación de redes VoIP

La siguiente generación de VoIP tendrá como características las siguientes:

- Conexión punto a punto basada en IPv6.
- Accesibilidad desde cualquier punto del mundo para usuarios VoIP.
- Señalización basada en SIP.
- Integración con redes corporativas desde una perspectiva de seguridad y de protocolo.
- Calidad de servicio en un ambiente inalámbrico.
- Integración con sistemas celulares de 3G.
- Niveles de servicio, fiabilidad y seguridad en servicios comerciales.
- Calidad de servicio en conexiones punto a punto a través de redes públicas.
- Soporte de baja tasa de bits en video y videoconferencia.
- Soporte de nuevas funciones, por ejemplo presencia y colaboración.
- Integración con otros sistemas para soportar mensajería unificada.

Algunas estrategias para la transición a VoIPv6, se describen en la figura 1.3. El tercer método de transición es el más costoso y probablemente no se aplique en un par de años, debido a que el cambio de tecnología es muy radical. El segundo método no es tan costeable como el anterior, sin embargo actualmente no se tiene desplegado a nivel comercial una ambiente IPv6. El primer método es el más razonable y el más

usado en las redes comerciales, ya que el cambio es gradual desde una red hibrida TDM/IP hasta un ambiente IPv6 extremo a extremo.

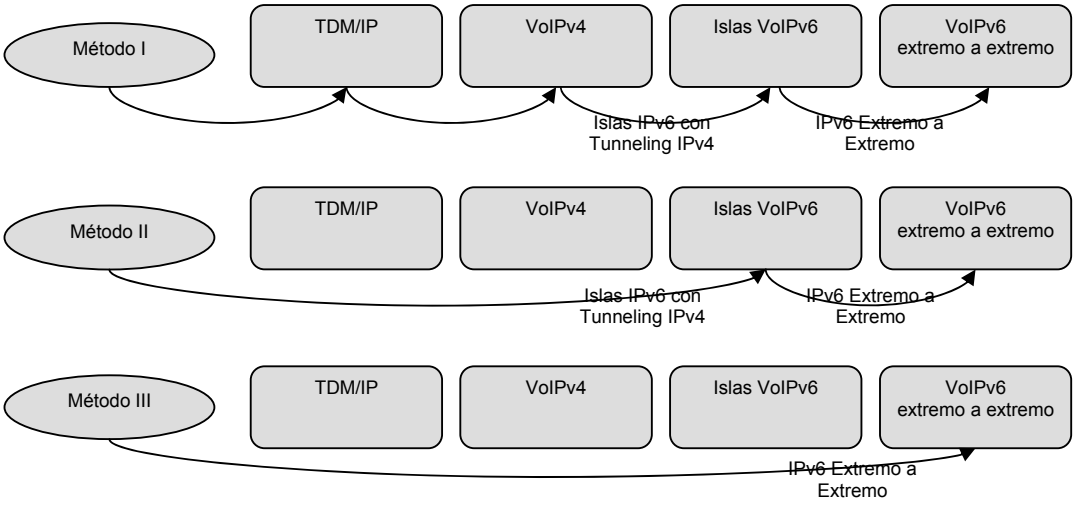


Figura 1.3 Estrategias de transición.

VoIPv6 ofrecerá nuevos servicios, no solo a las grades empresas, sino también a usuarios finales, los cuales no se han podido desarrollar por diferentes problemas con el actual protocolo de Internet. Las redes actuales deberán converger hacia redes inteligentes para no quedar atrás de esta evolución tecnológica, con una inversión inicial fuerte, pero con grandes recursos para su desarrollo. Durante los próximos años los operadores de servicios de telecomunicaciones tendrán que actualizarse para tener una competencia comercial y tener ingresos en nuevas áreas de desarrollo que proporciona VoIPv6.

1.3 Objetivos.

Investigar, analizar y proponer las bases para el desarrollo de Redes de Tercera Generación en la transmisión de información en tiempo real sobre él protocolo de Internet versión 6. Examinar los diferentes protocolos de comunicación, métodos de compresión y optimización de ancho de banda que intervienen en cada etapa de la transmisión de los paquetes sobre una red de datos. Describir la evolución de las redes de voz, el marco teórico de VoIP e IPv6 para tecnologías de networking involucradas para aumentar la calidad de servicio. Proponer escenarios sencillos para la transición a VoIPv6 basándose en los recursos ya desarrollados en la actualidad. Finalmente, mostrar casos de éxitos y procedimientos para adoptar los pasos necesarios para la explotación de VoIPv6 en países desarrollados.

1.4 Definición del problema.

En la actualidad el mercado de la Telecomunicaciones está en constante crecimiento, demandando seguridad, transparencia, eficacia y efectividad en sus comunicaciones, el constante aumento en dispositivos que requieren estar conectados en cualquier momento y en cualquier lugar, exige nuevas tecnologías

capaces de cubrir estas necesidades. El futuro de las comunicaciones se perfila al desarrollo de diferentes aplicaciones para soportar transferencia de voz, datos y video sobre un mismo dominio de red. El presente trabajo pretende esbozar la base de conocimientos sobre de VoIP e IPv6 y sentar las bases de la transición a VoIPv6.

Esta tesis tendrá como alcance plantear y presentar la transición a VoIPv6 en un esquema teórico basado en estándares mundiales, trabajos realizados por organismos independientes y empresas líderes en el mercado de las telecomunicaciones en el desarrollo de tecnologías de la información.

1.5 Esquema de análisis.

La tesis se basa en el método de investigación y se apoya en fuentes de información abiertas publicadas por organizaciones internacionales de regularización, informes técnicos, libros especializados, normas mundiales de telecomunicaciones, folletos relacionados con el tema y manuales de administración de productos que se encuentran en el mercado. Los capítulos presentados están ordenados de forma jerárquica con el fin de llegar al tema final con los fundamentos necesarios para presentar la solución efectiva a la transición de VoIPv6. La información contenida en cada tema tiene la directriz de hacer simple y clara la explicación al lector.

1.6 Aportación de la tesis.

El estudio pretende proporcionar un marco teórico para el desarrollo de redes de próxima generación para el transporte de datos en tiempo real sobre redes corporativas y empresariales, conociendo sus orígenes, situación actual y visión a largo plazo de su implementación. Esbozar un panorama general en la convergencia y aplicación de herramientas que permitan el establecimiento de redes siguiente generación basadas en la arquitectura actualmente desplegada para VoIP.

2

Conceptos de VoIP

Desde hace ya más de un cuarto de siglo se ha mostrado gran interés en la transmisión de paquetes de voz sobre las redes de datos ya implementadas. Se han desarrollado, propuesto y probado varias tecnologías para soportar voz, la idea principal era transformar la voz en paquetes de información manejables por un protocolo de red, tales es el caso de X.25, Frame Relay, ATM, IP, WiFi y MPLS. Sin embargo, el crecimiento y fuerte implantación de las redes IP, el desarrollo de técnicas avanzadas de digitalización de voz, mecanismos de control y priorización de tráfico, protocolos de transmisión en tiempo real, nuevos estándares que permiten la calidad de servicio en redes IP, han creado un ambiente donde es posible transmitir voz sobre IP.

Voz sobre Protocolo de Internet, también llamado Voz IP, VozIP, VoIP, es un grupo de recursos que hacen posible que la señal de voz viaje a través de Internet empleando un protocolo IP (Protocolo de Internet). Esto significa que se envía la señal de voz en forma digital, en paquetes, en lugar de enviarla en forma digital o analógica, a través de circuitos utilizables sólo para telefonía como una compañía telefónica convencional o PSTN. Actualmente, nuevas facilidades del protocolo IP, por ejemplo QoS, permite garantizar al usuario final fiabilidad en la calidad de audio que se presenta en las llamadas establecidas.

La asimilación de VoIP en la transmisión de voz mediante Internet, no es la única establecida, existen diferentes tipos de redes IP, entre las que podemos encontrar son la Red IP Publica, la cual se refiere a la red que ofrece un prestador de servicios de Internet y la principal diferencia es la calidad de servicio y la seguridad; y la Intranet, la cual es la red IP implementada a nivel empresarial.

El objetivo de VoIP es reemplazar la ya establecida Red Publica Telefónica Conmutada (PSTN por siglas en ingles), desde inicios del presente siglo la voz sobre Internet ha tenido mayor auge a nivel interracial, en comparación con TDM, la telefonía tradicional, el trafico por minutos alrededor del mundo ha incrementado notablemente sobre VoIP, tal como se muestra en la tabla 2.1.

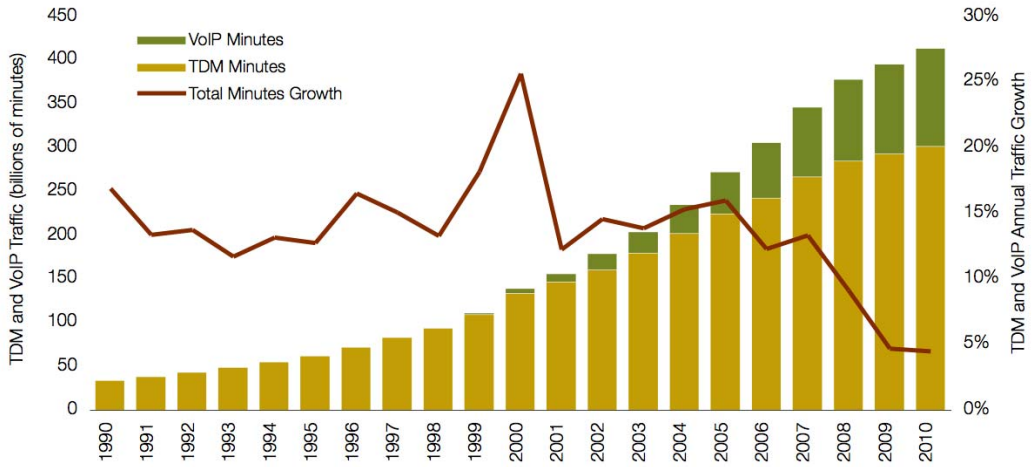


Tabla 2.1 Trafico VoIP

El protocolo de VoIP ofrece diferentes ventajas contra un servicio telefónico convencional. La ventaja más importante es el costo de las llamadas internacionales, debidas a que se utiliza la misma red de datos para transportar voz, especialmente cuando los usuarios no explotan toda la capacidad de su arquitectura de red. El desarrollo de nuevas técnicas de conexión a Internet, como ADSL, a nivel domestico disminuye los cargos en llamadas de larga distancia. Otra ventaja de este nuevo servicio es su portabilidad., permitiendo hacer y recibir llamadas de voz sobre IP donde quiera que haya una conexión rápida de Internet, entrando en tu cuenta de VOIP. Las terminales VoIP se pueden integrar con otros servicios existentes en Internet, como video, mensajería, intercambio de datos, etc., en forma. Los servicios de identificación de llamadas, Servicio de llamada en espera, trasferencia de llamadas, remarcación de llamada, desvío de llamadas y otras características que ofrecen por una tarifa extra los proveedores de telefonía ya están incluidos en esta tecnología.

Para conocer el desarrollo de VoIP es necesario entender conceptos que maneja este protocolo y durante este capítulo se presentaran dicho términos, así como el proceso de la digitalización de la voz y las ventajas de su implementación.

2.1. Digitalización de la voz.

El mecanismo natural de comunicación de los seres vivos es la voz, la cual es producida por las cuerdas vocales, debido a un acoplamiento y modulación del flujo de aire que pasa a través de ellas, generando su movimiento. Las cuerdas vocales vibran a una velocidad llamada frecuencia fundamental. La señal de voz es continua en el tiempo y en amplitud, de tal forma se considera analógica, la vibración de las cuerdas da lugar a la onda de voz con un contenido espectral en banda base, el conjunto de frecuencias audibles del ser humano comprenden entre los 20 Hz y 20 KHz, mientras

que el rango de frecuencias legibles por el oído humano se encuentra entre los 200 Hz y los 3400Hz, lo que constituye un canal telefónico, como se muestra en la figura 2.1.

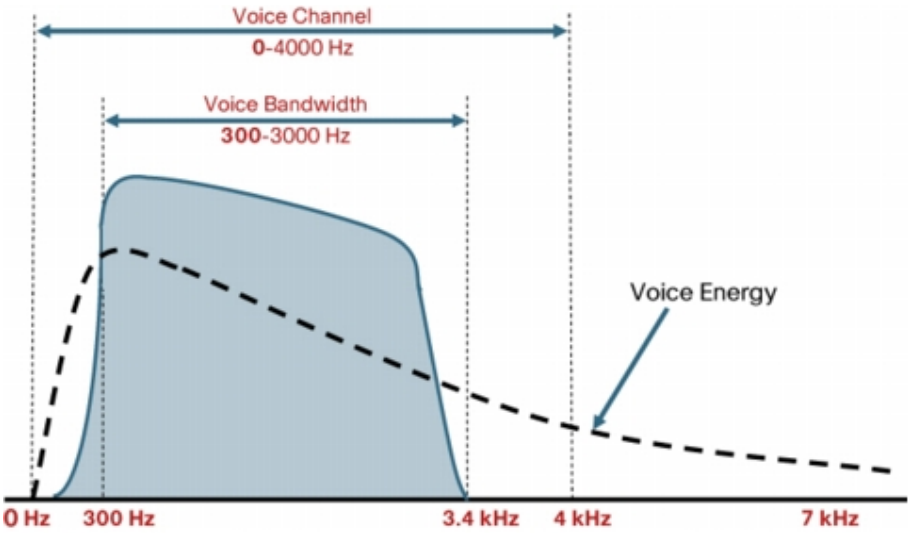


Figura 2.1 Canal Telefónico.

Existen varias desventajas en la transmisión de señales analógicas en banda base, por ejemplo la transmisión de voz de forma natural, tales como vulnerabilidad al ruido, la interferencia, costos de propagación, la dificultad del manejo de la información, incluso no es posible aplicar técnicas de seguridad, por lo tanto es necesario convertir las señales analógicas a digitales, reduciendo el ancho de banda para transmitir estas señales.

Los rápidos avances en la electrónica, particularmente en las técnicas de fabricación de circuitos integrados, ha desarrollado tecnologías como VLSI/LSI, que permiten el despliegue de computadoras digitales más potentes, pequeñas, rápidas y baratas, lo que ha hecho posible construir sistemas digitales altamente sofisticados. Entre los avances en la fabricación de circuitos integrados se encuentra el DSP (Digital Signal Processor). Un procesador digital de señales o DSP es un sistema basado en un procesador o microprocesador que posee un juego de instrucciones matemáticas, algoritmos de procesamiento, un hardware y un software para procesar señales en tiempo real. Los DSPs se encargan de transformar una señal analógica a una señal digital, pueden estar alojados en una terminal VoIP o en Gateway.

El proceso de conversión analógico-digital se lleva a cabo dentro del DSP, tal objetivo se realiza con el muestreo, la cuantificación y codificación de la señal de entrada, obteniendo a la salida una señal digital, el procedimiento se describe a continuación:

Muestreo. Consiste en tomar valores representativos instantáneos en el tiempo de una señal analógica, la información muestreada permite reconstituir más o menos una representación de la forma original de la señal de voz, para que dicho proceso tenga utilidad práctica es necesario elegir la tasa o frecuencia de muestreo adecuada, de modo que la secuencia de valores muestreados identifiquen la forma original de la señal. De acuerdo al teorema de Nyqust la frecuencia de muestreo debe ser mayor al doble del ancho de banda para que se pueda reconstruir una señal. En el caso de un canal telefónico, teóricamente 4 KHz, la frecuencia de muestreo debe ser 8 KHz.

El muestreo periódico de una señal, en el dominio de la frecuencia, se observa una repetición de dicha señal cada periodo de tiempo, si la fs, frecuencia de muestreo, es menor al doble de ancho de banda se produce un traslape ente versiones de la señal, haciendo imposible su reconstrucción, tal fenómeno es llamado aliasing (Figura 2.2).

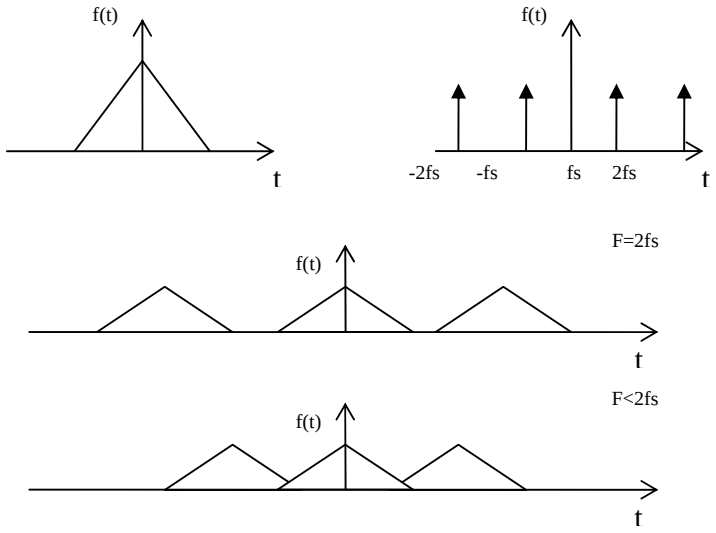


Figura 2.2 Aliasing

Cuantificación. Es la conversión discreta en amplitud de la señal, permite representarla en un número finito de bits (N), hasta 2N-1 valores diferentes. La característica entrada/salida de un cuantificador tiene forma de escalera (Figura 2.3). El resultado será la representación digital de la señal. En la telefonía se utiliza un cuantificador escalar de niveles fijos no uniforme con 128 niveles para asegurar la cantidad aceptable. El equiespaciamiento entre niveles origina en telefonía, por ejemplo, que una persona que habla en voz muy baja no sea escuchada claramente, por lo que este sistema ha causado una cuantificación no uniforme o logarítmica es decir los niveles de cuantificación varían, y tiene mayor sensibilidad para amplitudes bajas.

La cuantificación logarítmica equivale a una compresión de la señal, una cuantificación uniforme de la señal comprimida y una posterior expansión en el otro extremo, utilizando la misma ley empleada en transmisión. Esta ley recibe el nombre de ley de compansión, formado por los procesos de compresión y expansión. Existen dos métodos de compresión analógicos que se aproximan a una función logarítmica, y son conocidos como Ley μ y Ley A. En EUA y Japón se usa la ley μ, mientras que en Europa se usa la ley A, esta última estandarizada por la ITU en G.711.

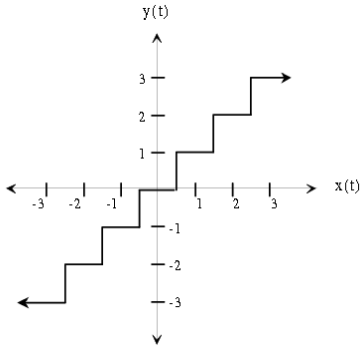


Figura 2.3 Cuantificación

Codificación. El siguiente paso para la conversión de la voz a una señal digital es adaptar la señal para que sus características sean las idóneas a la hora de transmitirla por un canal de comunicaciones concreto con la mayor calidad posible, la codificación consiste en asignar un código binario a cada uno de los valores discretos de la señal.

Tradicionalmente en entornos telefónicos se ha utilizado la modulación por codificación de pulsos o PCM, en la que la voz se representa por 8 bits, resultando un ancho de banda de 64 Kbps con una frecuencia de muestreo de 8000 Hz, que coincide con canal de voz tradicional.

El ancho de banda, cantidad de información en bits que se puede transmitir en un instante de tiempo, está en función de la frecuencia de muestreo (fs) y del número de bits (N) empleados para codificar cada muestra:

BW= fs . N

En la práctica, el ancho de banda es un recurso limitado y costoso, por lo que la necesidad de un buen codificador que ofrezca calidad y mayor tasa de transmisión es primordial para cualquier red.

Existen varios vocoders (codificadores de voz) que nos permiten cuantificar con un número menor de bits empleados para reducir el ancho de banda, por ejemplo, codificando la diferencia entre muestras sucesivas (DPCM, Diferencial PCM) o adaptando que el tamaño del paso de cuantificación varíe a lo largo del rango dinámico de la señal (ADPCM Adaptive Diferencial PCM). Codificadores de este tipo son el G.721 y G.726 que pertenecen a los codificadores de onda, es decir, los que codifican directamente los valores que toma la señal en el dominio temporal.

Otra manera de reducir la utilización del BW es reducir las frecuencias de muestreo menores a la de Nyquist. Para resolver la distorsión energética, se utilizan procedimientos más complejos, tales como la interpolación y la predicción lineal que tratan de estimar tramas anteriores y posteriores a la actual mediante varias técnicas.

El precio de la disminución del ancho de banda es un aumento del retardo y una disminución en la calidad de voz, además la compresión implica un procedimiento adicional de la muestras de voz que tiene por objetivo eliminar o al menos reducir la información de redundancia presente en la señal de voz. Este procedimiento consume ciclos de CPU del DSP del codificador e introduce un retardo CPU que puede causar que la voz no se ha entendible en valores considerablemente altos.

2.1.1 CODES

La conversión de la voz de analógica a digital se lleva a cabo en un equipo único, un codificador-decodificador (CODEC), el cual lleva acabo la traducción A/D, comprime la secuencia de datos, proporciona la cancelación del ECO y otros suprimen el silencio producido en una llamada normal. Las características de calidad y retardo varían según cada implementación y no hay una clase predominante. Los codecs realizan esta tarea de conversión tomando muestras de la señal de voz miles de veces por segundo. Un códec convierte las señales analógicas en un flujo de bits digitales, y otro códec idéntico en el otro extremo de la comunicación convierte el flujo de bits digital a una señal analógica y finalmente es reproducida por un dispositivo de audio. En el mundo de VoIP, los codecs se utilizan para codificar la voz para su transmisión a través de redes IP.

Los codecs operan usando algoritmos avanzados que les permiten tomar las muestras, comprimir y empaquetar los datos. La unión internacional de telecomunicaciones ha estandarizado diferentes métodos de compresión, las cuales se describen en la tabla 2.2.

Codec	Técnica de compresión	Ancho de banda
G.711	PCM	64
G.726	ADPCM	32,24,16
G.728	LD-CELP	16
G.729 A/B	CS-ACELP	8
G.723	ACELP	6.3,5.3

Tabla 2.2 Codecs

G.711. Este codec utiliza la técnica de compresión PCM; es implementado tanto para la ley μ y la ley A. Se utiliza en conexiones para una red LAN y desarrolla una excelente calidad de voz, sin embargo el ancho de banda utilizado que se consume es alto para conexiones de Internet de pequeños recursos.

G.726. Comprime con el algoritmo ADPCM, tiene menor consumo de ancho de banda por usar 4,3 o 2 bits para cada muestra. Es recomendado para utilizarlo con conexiones con poco ancho de banda, su calidad de voz no es tan buena como el codec anterior.

G.728. Es un codec CELP, tiene más alta carga de procesamiento y calidad media de la voz, consume 16 kbps de ancho de banda utilizando 10 bits por muestra.

G.729. Es un tipo de codec CS-ACELP en sus dos variantes A y B, el cual ofrece el mejor balance entre la calidad de voz y el ancho de banda, por lo cual es implementado en redes WAN. Este vocodec utiliza Voice Activity Detection (VAD) en su versión G.729B, mientras que la versión G.729A es más susceptible a problemas con la red, tales como perdida de paquetes y retardo.

G.723. Codificador del tipo MPMLQ, implementado cuando la calidad de voz no es requerida.

2.2 Calidad de voz y factores influyentes.

Las redes implementadas están orientadas tradicionalmente al tráfico de datos y presentan exigencias de calidad y prestaciones diferentes a las de las redes de voz sobre paquetes. Las aplicaciones para la transmisión de voz son muy sensibles al retardo y perdidas de paquetes, por lo que se requiere de algoritmos que permitan diferenciar tipos de tráfico y proporcionen un especial servicio a los usuarios finales en la transmisión de la información durante una llamada VoIP.

La calidad de voz está determinada por varios factores tanto subjetivos como objetivos. Para definir el concepto de calidad de voz, desde una visión cercana al usuario, seria la fidelidad con la que se escucha la voz en el otro extremo, dependiera concretamente de la calidad de la red para soportar el flujo normal de la conversación.

La telefonía tradicional utiliza tecnología de conmutación de circuito mientras que VoIP utiliza conmutación de paquetes. En las redes de conmutación de circuitos, los recursos de la red están dedicados al circuito durante todo el tiempo, y los datos transmitidos siguen la misma trayectoria. En las redes de conmutación de paquetes, el mensaje es dividido en paquetes, cada uno de los cuales pueden tomar diferente ruta a su destino y finalmente es reconstruido en el destino. Esta diferencia en el transporte de la información es reflejada en la calidad de la conversación. La calidad de servicio o Quality of Service (QoS) es la capacidad de la red para ofrecer mejoras en el servicio de cierto tipo de tráfico, asegurando al usuario un nivel aceptable en la legibilidad de la voz.

Las consideraciones generales sobre la evaluación de la calidad del servicio telefónico se detallan en la recomendación de la ITU-T E.420, describe los aspectos generales que mayor influencia ejercen sobre la percepción de la calidad del servicio telefónico en los usuarios finales. Entre los más importantes se encuentran:

Tasa de conectividad. Es la probabilidad con la que la red dispondrá de recursos para una llamada establecida.

Inteligibilidad de la voz. Es necesario que dentro de un canal de comunicación en ambos extremos sean capaces de entender claramente las palabras de su interlocutor, lo que depende en gran medida de la claridad de la voz.

Codificación de la voz. Una vez establecida la llamada y una vez que la voz en el otro extremo puede entenderse con claridad el siguiente paso es codificar la voz, transmitirla a través de la red y ver qué tal se escucha. El resultado final está influenciado por la teórica de codificación utilizada, lo que depende en gran medida de la tasa binaria, como se muestra en la figura 2.4, entre mayor es la tasa binaria, mayor es la calidad de la codificación, el incremento de la tasa de error es mayor cuando menos es la tasa binaria.

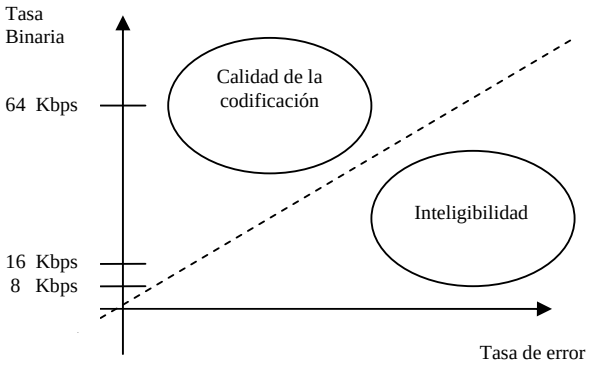


Figura 2.4 Tasa Binaria vs Tasa de Error

En las redes de conmutación de circuitos se establece un circuito virtual, que tiene un ancho de banda reservado y una sola ruta, por lo que la información llega en el mismo orden en que se genera, en cambio las redes de computación de paquetes no hay un canal de transmisión reservado, cada paquete de datos puede tener un camino diferente a su destino, por lo que existe la posibilidad que los paquetes se pierdan y lleguen en desorden, deteriorando la calidad de voz en el extremo del canal de comunicación. En el caso de la VoIP se pretende ofrecer la misma calidad de audio que en una red de conmutación de circuitos, sin embargo hay factores que influyen directamente en la calidad de voz tales como la disponibilidad, la pérdida de paquetes, el jitter, el retardo y la latencia del ancho de banda y compresión de voz. Estos factores se describen en la presente sección.

Disponibilidad. Es la probabilidad de tiempo que el servicio es ofrecido al usuario, se obtiene del cociente entre el tiempo de uso efectivo y el tiempo de uso fatal. La red voz tradicional, PSTN, ofrece una disponibilidad de 99.999, lo que significa 5 minutos y 5 segundos fuera de servicio al año, una probabilidad difícil de alcanzar para redes de datos, debido a fallas con dispositivos, software, aplicaciones y por los usuarios. Para el caso de VoIP los componentes críticos son los servidores, el Call Agent, las puertas de enlace, los Gatekeeper, las terminales de usuario e incluso el Internet. Las empresas prestadoras de servicio de Internet ofrecen hasta 99.99 % de disponibilidad, lo que significa 8 segundos fuera de servicio por día.

La clave de la tolerancia a fallos es la renuncia, cuyo principio es que cualquier punto de la red que resulte vulnerable a fallas debe ser respaldada en recursos físicos y lógicos que proporcionen el mismo servicio, sin embargo económicamente no es viable respaldar todos los equipos de red, por lo que solo se respaldan aquellos equipos que realmente son críticos para el servicio, generalmente los servidores encargados del control de llamadas, la señalización y los gateway de voz. Por otra parte, los usuarios finales son configurados de tal manera que se asegure la salida de llamadas, por la red pública, lo que se conoce como ruta de backup o de respaldo.

El backup también incluye el sistema eléctrico que alimenta a todos los servidores, para tal motivo se recomienda el uso de UPS (sistemas de alimentación interrumpida) que reducen el impacto de los cortes de suministro eléctrico.

Jitter. Es la variación en el retardo de los paquetes recibidos causada por congestión de red, perdida de sincronización o por las diferentes rutas seguidas por los paquetes para llegar al destino, es decir la diferencia entre el tiempo en que llega un paquete y el tiempo que se cree que llegara el paquete en el destino. El trafico de voz es muy sensible a las variaciones del retardo, en redes de paquetes no es posible garantizar que todos los paquetes sigan el mismo camino, como consecuencia cada

paquete llegará al destino atravesando un número distinto de dispositivos de red, y por tanto alcanzaron su objetivo en diferentes intervalos de tiempo, originado el jitter, tal ejemplo se muestra en la figura 2.5.

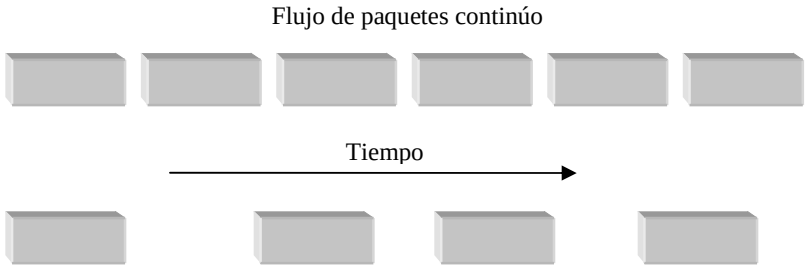


Figura 2.5 Jitter

El Jitter produce espacios en la conversación debido al flujo desigual de datos. Por ejemplo, si del origen se transmite: "José, ven aquí. Quiero." El destino en presencia de Jitter se reciben: "Jo.. s..e, ven aquí. Quie….ro". El arribo de paquetes en el destino causa los espacios y el retardo de la conversación. Algunos factores que contribuyen al Jitter son:

- El desempeño de la red durante condiciones "pico".
- Los dispositivos de red.
- Velocidad de los enlaces.
- Tamaño de los paquetes de voz y datos.
- Tamaño de los buffer en los routers.

Para absorber las variaciones de arribo se utilizan los buffer de supresión de Jitter. La supresión consiste en almacenar los paquetes durante el tiempo suficiente para que los paquetes se puedan reordenar y reenviar en el orden correcto. La cantidad de buffer puede ser dinámica o estáticamente asignada en los dispositivos de red. Los valores recomendados para el jitter entre el punto inicial y final de la comunicación debieran ser inferiores a 100 ms.

Delay. El retardo o latencia es el tiempo que tarda en viajar la señal de voz desde el origen al destino. Esto puede dar como resultado una pobre calidad de voz, también incrementa considerablemente el impacto negativo del eco. Existen dos tipos de retardos:

1) Retardo Fijo. Los componentes de red de retardo fijo son predecibles y suman directamente al total de retardo en la conexión. Los retardos fijos son:

- Codificación. Es el tiempo que toma en transformar la señal analógica a digital y depende del codec.

- Empaquetamiento. Es el tiempo utilizado en empaquetar la señal digital en paquetes de datos, la cual varía de acuerdo al codec. En la tabla 2.3 se muestra algunos retardos dependiendo del codec utilizado.

	G.711	G.729	G.723.1
Tasa binaria (Kbps)	64	8	6.3/5.3
Retardo de Codificación (ms)	0.125	15	37.5

Muestreo (tiempo entre paquetes)	20	20	20
Retardo de empacamiento (ms)	1,5	15	37.5

Tabla 2.3 Tiempo de Retardo por Empaquetamiento

- Serialización. Es el tiempo en que el dispositivo de red invierte en transmitir los paquetes de voz a través de una interface de red, el cual depende de la velocidad de la interface y del tamaño del paquete, y está directamente relacionado con la tasa de reloj de la transmisión.

- Propagación. Es el tiempo en que tarda el paquete en alcanzar su destino. Depende de las características del medio físico de transmisión, de la velocidad de la luz, en caso de una señal óptica, por lo que suele ser despreciable, en caso de una señal eléctrica su velocidad promedio es de 4 a 6 ms/Km; de tal forma que depende de la distancia geográfica.

2) Retardo Variable. Estos retardos no son predecibles y se deben al encolamiento de paquetes y al buffer de almacenamiento en las interfaces de red conectada a la WAN. Por ejemplo el retardo de encolamiento, se define como el tiempo variable que permanecen los paquetes retenidos en los dispositivos de red antes de ser transmitidos debido a una congestión sobre la interface de salida. En la figura 2.6 se aprecian diferentes tipos de retardos al transmitir paquetes.

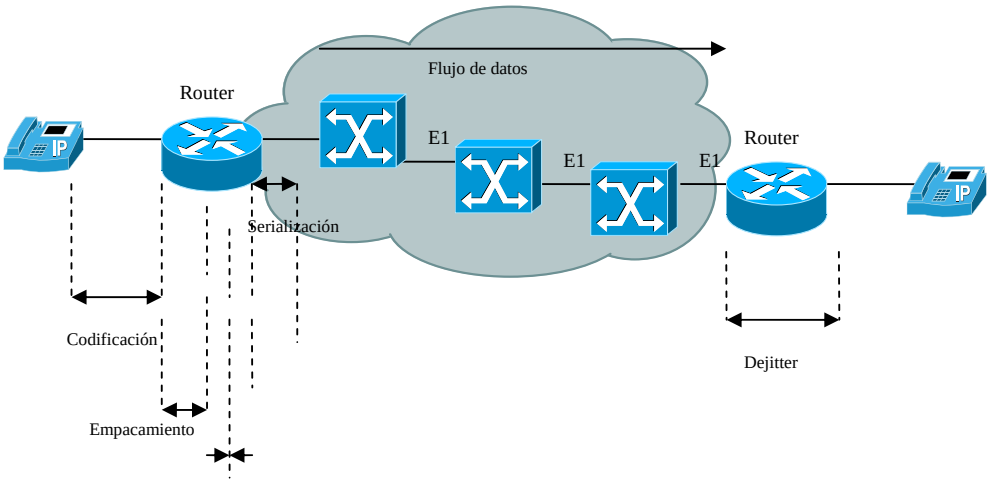


Figura 2.6 Tipos de Retardo

En la recomendación de la International Telecommunication Union (ITU) G.114 se establecen umbrales aceptables de retardo, como se muestra en la tabla 2.4.

Rango (ms)	Descripción
0-150	Excelente. Válida para las aplicaciones más comunes.
150-40	Bueno-Pobre. Aceptable, teniendo en cuenta que un administrador de red conozca las necesidades del usuario.
Sobre 400	Inaceptable para la mayoría de las aplicaciones de red, sin embargo puede ser excedido en algunos casos aislados.

Tabla 2.4 Umbrales aceptables de retardo

Algunos estudios muestran que un retardo superior a 150 ms ya es percibido por el oído humano, por lo que es una cantidad máxima que se debe considerar en el diseño de una red. A continuación se muestra un ejemplo de valores aceptables de retardo en un diseño de red en la tabla 2.5:

Retardo	Fijo	Variable
Codificación	18	
Empaquetamiento	30	
Encolamiento		8
Serialización (64 Kbps)	5	
Propagación (Retardo de Red)	40	25
Dejitter buffer	45	
Total	138	33

Tabla 2.5 Valores aceptables de retardo

El aumento de ancho de banda, configuración de la calidad de servicio, la capacidad de los equipos en la Internet son factores que se pueden manipular para controlar el retardo. La principal causa de la latencia es la congestión de la red.

Perdida de paquetes. En una red de datos los paquetes perdidos son recuperables solicitando una retransmisión, sin embargo en el caso de la transmisión de voz no es práctica la retransmisión debido a que se trata de tráfico en tiempo real, además de ocasionar retardos adicionales. La perdida de paquetes en redes de datos es esperada y común, es resultado del descarte de paquetes que se produce en los nodos de red como consecuencia de una red inestable, congestión de red y retardos variables.

El efecto de pérdidas de paquetes es una disminución de la calidad de voz, puesto que falta información al momento de reconstruir el mensaje, como se muestra en la figura 2.7. La disminución de la calidad es mayor tanto mayor sea la tasa de compresión del codec. En una conversación que experimenta perdida de paquetes, el efecto se escucha inmediatamente, si el origen del mensaje es: “José, ven aquí. Quiero”, el destino obtendrá. “Jo…, ven aquí. ….ro”.

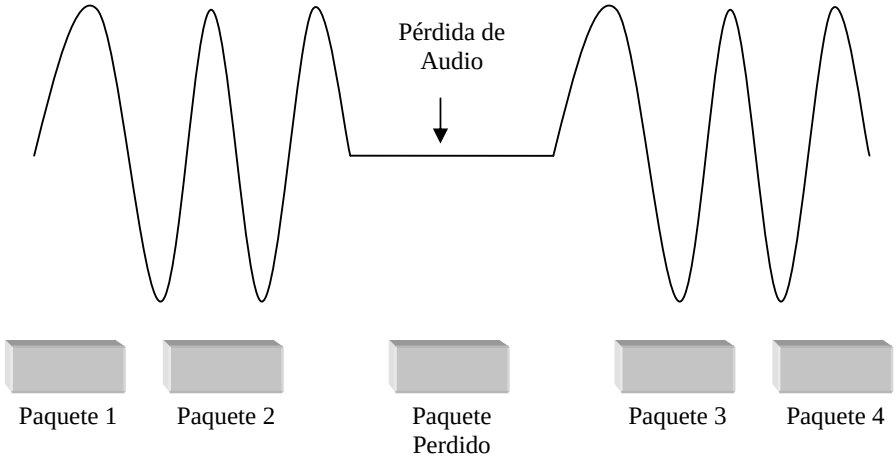


Figura 2.7 Perdida de paquetes.

La solución inmediata es incrementar los recursos de red, pero económicamente no es práctico, una vez que se presente mas tráfico se volverá a presentar el mismo problema. De tal manera, que requieren otro tipo de técnicas para atenuar este efecto para lo que se conocen las siguientes técnicas.

- Forward Error Control (Corrección de errores). En los paquetes se incluye información de redundancia que permite recuperar el valor del paquete perdido. Su principal inconveniente es el retardo, puesto que para decodificar un paquete son necesarios paquetes vecinos.

- Distribución de Errores. Consiste en aleatorizar las pérdidas para dispersar sus efectos, su inconveniente es el retardo adicional que introducen y el mayor consumo de ancho de banda.

- Packet Loss Concealment (recuperación de errores). Consiste en sustituir el paquete perdido por otro. Existen varias posibilidades en esta técnica, ya sea sustituir un paquete perdido por un ruido blanco, un silencio o bien un paquete que se obtiene con una técnica de predicción a partir de paquetes anteriores y posteriores; sin embargo entre mayor complejidad se requiere mayor procesamiento y se produce mayor retardo.

En la recomendación de la ITU-T G.113 apéndice 1 se provee una planificación en el efecto de pérdidas de paquetes con relación a los codec utilizados y al factor de deterioro (Le), lo cual se encuentra en la tabla 2.6.

Codec	Le (0% perdidas)	Le (2% perdidas)	Le (3% perdidas)
G.711 sin PLC	0	35	55
G.711 con PLC	0	7	15
G.729 A	11	19	26
G.723 I	15	24	32

Tabla 2.6 Relacion Codec vs Le

Eco. El eco consiste en la superposición de una señal con ella misma retardada un tiempo, que para ser perceptible para el oído humano ha de superar los 70 ms para voz o los 10 ms si se trata de música. Este fenómeno normalmente se presenta en redes de circuitos, pero también se presenta en voz sobre paquetes. Físicamente se detecta cuando el emisor escucha parte de su propia voz junto con la voz del receptor o en ausencia de ella. Existen varios tipos de Ecos, entre los cuales se mencionan:

- Acústico. Es el producido por la retroalimentación de la señal de voz sobre la línea de transmisión y se debe al acoplamiento entre el micrófono y el auricular del teléfono, se considera en teléfonos, manos libres o teléfonos inalámbricos y se soluciona con terminales de mayor calidad.

- Eléctrico o Híbrido. Producido por el desacoplamiento en la conversión de 2 pares de hilos, utilizado por la central telefónica, a 1 par de hilos en el nodo terminal, esta operación se realiza a cabo en un dispositivo denominado bobina híbrida, como se describe en la figura 2.8. En la conversión 2H/4H se produce una desadaptación de impedancias que

refleja parte de la señal incidente y que viajara tanto con la voz al otro extremo, donde da lugar al fenómeno del eco.

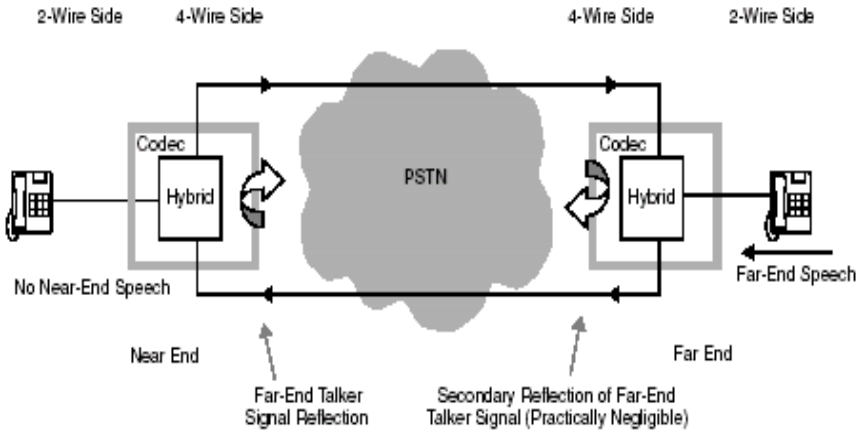


Figura 2.8 Eco Eléctrico o Hibrido.

En redes telefónicas convencionales si la amplitud es suficientemente baja y el retardo en un solo sentido es menor de 50 ms, el eco queda enmascarado por la conversación normal, si el retardo de extremo a extremo es corto, cualquier eco que es generado por el circuito de voz regresara al abonado llamante muy rápidamente y no será percibido. En la recomendación de la ITU G. 168 establece que la magnitud de la señal reflejada recibe el nombre de ERL (Echo Return Loss) y se define como:

ERL=Amplitud de la señal fuente- Amplitud del eco

y debe ser mayor de 55 dB.

En el escenario de VoIP se debe considerar que el eco se produce en los segmentos analógicos de la red y no en los digitales, cuando una conversación puramente IP no se produce este fenómeno. Para disminuir el eco, algunas técnicas se pueden implementar mediante hardware y otros por software, en el caso de un Gateway, los DSP se encargan de la cancelación del eco, esto también se lleva a cabo en algunos teléfonos IP (Figura 2.9).

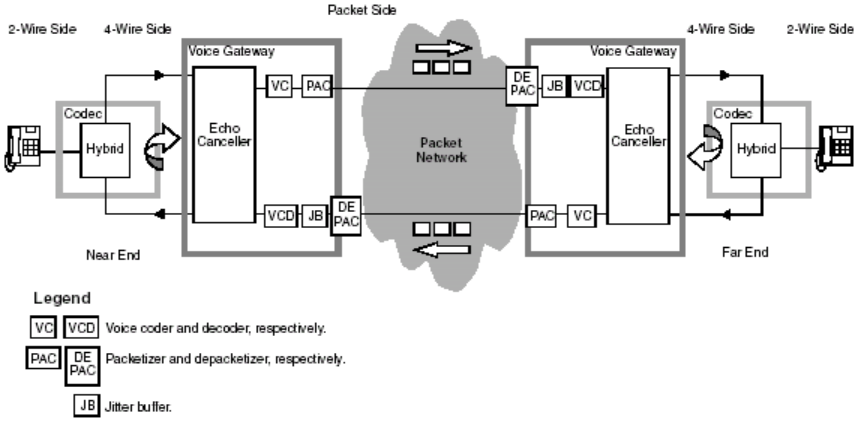


Figura 2.9 Cancelación de ECO en DSP

Existen dos formas de resolver el problema del eco: con supresores de eco o con canceladores de eco. Los supresores de eco funcionan suprimiendo la señal de voz del extremo con menos intensidad, haciendo que la comunicación se vuelva half-duplex. Los canceladores de eco, son dispositivos más complejos, la idea es sintetizar una réplica del eco y restarla a la señal que retoma.

Ancho de Banda. Es la cantidad de información que puede fluir de un punto a otro en un periodo de tiempo específico. En los sistemas digitales, la unidad básica son los bits por segundo (bps) normalmente se utilizan múltiplos de bps. Una comunicación de voz sin comprimir consume 64 Kbps. Es un recurso finito y está determinado por limitaciones del medio de transmisión, método de señalización y recursos de la red. Los sistemas de telefonía IP requieren mayor ancho de banda para proporcionar mejor calidad de voz, reduciendo la pérdida de paquetes y el retardo en sus transmisiones.

El ancho de banda en telefonía IP esta directamente asociada al tamaño de las muestras de la voz, la cual es una variable asignada por cada administrador de red. El tamaño de la muestra es proporcional al tamaño de los paquetes de voz, para el caso de voz el tráfico es altamente sensible al tiempo, por lo que si el tiempo de empaquetamiento es muy largo las llamadas no son enviadas rápidamente a la red. El tamaño del paquete de VoIP es la carga útil (payload) medida en bytes que equivale al tiempo de duración del paquete en el canal expresado en milisegundos calculando a una determinada tasa de envió de paquetes.

El tiempo de duración del paquete de voz está relacionado a la cantidad de muestras, por lo que al aumentarla es equivalente a incrementar la carga útil, por lo que podremos tomar más muestras mejorando la calidad de voz, pero se elevara el retardo de transmisión provocando pérdidas de paquetes. En la tabla 2.7 se ilustra la relación de las muestras de voz, la carga útil y el codec.

Codec	**G.711**			**G.729**		
Ancho de Banda (kbps)	64			8		
Muestras (ms)	10	20	30	10	20	30
Carga útil (bytes)	80	160	240	10	20	30

Tabla 2.7 Relación entre Ancho de banda-Muestra-Carga útil.

El Payload es la carga útil del paquete de voz, está definido como:

Payload=tamaño de la muestra */Ancho de banda del Codec/8

En la tabla 2.8 se muestra el número de paquetes por segundo que se transmiten en el canal de transmisión dependiendo del tamaño de la muestra y el ancho de banda.

CODEC	**Ancho de Banda (bps)**	**Tamaño de la muestra (Bytes)**	**Paquetes**
G.711	64,000	240	33
G.711	64,000	160	50
G.726r32	32,000	120	33
G.726r32	32,000	80	50
G.726r24	24,000	80	25

CODEC	Ancho de Banda (bps)	Tamaño de la muestra (Bytes)	Paquetes
G.726r24	24,000	60	33
G.726r16	16,000	80	25
G.726r16	16,000	40	50
G.728	16,000	80	13
G.728	16,000	40	25
G.729	8000	40	25
G.729	8000	20	50
G.723r63	6300	48	16
G.723r63	6300	24	33
G.723r53	5300	40	17
G.723r53	5300	20	33

Tabla 2.8 Paquetes por segundo.

Para reducir el ancho de banda se utiliza técnicas como la supresión de cabeceras y se selecciona el codec adecuado que permita una excelente relación entre el consumo del ancho de banda y la calidad de voz.

VAD. Es una aplicación por software que trata de aprovechar el hecho de que en una conversión normalmente el 60% del tiempo lo ocupan los silencios debidos a las pausas para respirar y a la espera del tema en la comunicación. El ancho de banda desperdiciado en transmitir paquetes sin información se puede utilizar para introducir otro tipo de tráfico.

VAD trabaja detectando la magnitud de la voz en dB y decide cuando no empaquetar la voz. Típicamente, cuando se detecta una caída en la amplitud del habla, espera una cantidad de tiempo fija antes de detener la salida de paquetes de voz, la cantidad de tiempo es aproximadamente de 200ms. Esta aplicación tiene problemas de interferencia al detectar la voz del ruido de fondo que se presenta en una conversación, para lo que se detecta un umbral de señal-ruido para hacer la diferencia. En caso de que el ruido no se pueda diferenciar de la voz VAD se deshabilita por si solo al inicio de la llamada. También el fenómeno del clipping, mutilación de la voz, es problema que se introduce con VAD.

Para evitar que el interlocutor piense que se ha cortado la comunicación durante los intervalos de silencio la ITU-T especifica dos posibles soluciones: 1) Enviar periódicamente paquetes de silencio (SID, Silence Insertion Description) durante la pausa. Estos paquetes proporcionan una indicación del nivel de ruido que existe en el origen para que el receptor lo simule en el terminal remoto mediante un algoritmo de CNG (Comfort Noise Generation) o generador de ruido. 2) Para evitar el envío de paquetes SID es posible marcar el bloque generado como NOTX (No Transmission). En el receptor se genera ruido ambiente a partir de una señal de ruido blanco o del muestreo del auricular.

Se debe de tener en cuenta que los CODECS están disponibles con y sin VAD, por ejemplo G.729 A/B soporta VAD, pero G.711 no. En general con esta aplicación se alcanza un ahorro de 30 a 50 % de ancho de banda.

2.3 Medidas de la calidad de voz.

Para que la tecnología VoIP pueda ser utilizada en forma masiva y comercial, es esencial garantizar una calidad de voz aceptable. Para ello se han desarrollado métodos para medirla. Estos métodos se dividen en subjetivos y objetivos. Los métodos subjetivos de medida de la calidad de servicio, se basan en conocer directamente la opinión de los usuarios, por lo que las medidas no son tan exactas, sin embargo se efectúan en tiempo real mientras que el sistema sigue en explotación sin interferir en las llamadas existentes. Además, típicamente resultan en un promedio de opiniones. Métodos subjetivos son las escalas MOS y el modelo E. Los métodos objetivos miden propiedades físicas en la red para proveer o estimar el rendimiento paralelo a los usuarios. A su vez se subdividen en intrusivos, donde se inyecta una señal de voz conocida en el canal y se estudia su degradación a la salida, por ejemplo PESQ, y no intrusivos los cuales monitorean ciertos parámetros en un punto de la red y en base a estos permite establecer en tiempo real la calidad que percibiría un usuario.

2.3.1 Métodos subjetivos.

MOS. Es un sistema de medida para la calidad de voz, se trata de un conjunto de técnicas subjetivas de la medida de la calidad de voz que recibe el nombre de test ACR (Absolute Category Rerting), donde la calidad es evaluada directamente y tienen el mismo esquema general; se reúne a una muestra de usuarios a los que se les pide que opinen sobre la calidad que en algún aspecto concreto ofrece un determinado sistema de transmisión de la voz. Las escalas MOS están estandarizadas en la recomendación ITU-TP.800, el resultado obtenido se califica con valores entre 1 y 5, siendo 5 “excelente” y 1 “malo”. La serie de preguntas en la prueba que se realiza al grupo de personas seleccionado para medir la calidad de audio, se presenta en la figura 2.10.

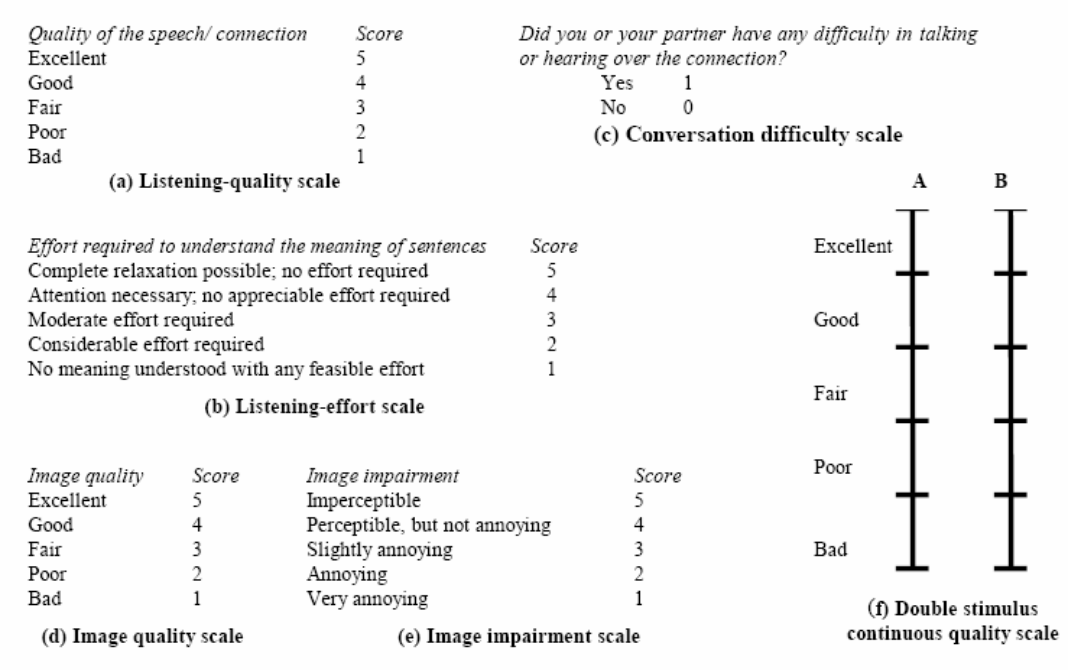


Figura 2.10 MOS.

Existen otros aspectos que evalúan las escalas MOS, son muy variados, entre ellos está la calidad de voz y el esfuerzo requerido para entender el significado del mensaje pronunciado por el otro extremo, tal como se muestra en la tabla 2.9.

Puntuación	Calidad
5	Excelente
4	Buena
3	Aceptable
2	Pobre
1	Mala

Puntuación	Esfuerzo
5	Relajación completa: no es necesario ningún esfuerzo.
4	Necesario prestar atención: no se requiere esfuerzo apreciable
3	Esfuerzo moderado
2	Esfuerzo considerable
1	Imposible de entender

Tabla 2.9 Aspectos de evaluación MOS.

Un factor directamente influenciable en la calidad del audio es la tasa de compresión, directamente proporcional al CODEC seleccionado, en la tabla 2.10 se muestra la puntuación en escala MOS de algunos de los estándares de codificación más habituales en voz sobre paquetes.

Codec	Valor MOS
G.711	4.4
G.726	3.8
G.728	3.6
G.729	3.7
G.723.1	3.9

Tabla 2.10 Puntación MOS de Codecs.

MODELO E. El modelo E es una aproximación matemática a la medida de la calidad de voz para relacionar los parámetros de red medibles con el MOS. La ITU ha recomendado el modelo E, el cual ha sido adaptado por la ETSI y por la TIA,

organismos internacionales de normalización, y es el modelo más ampliamente difundido. El resultado es una cuantificación escalar de la calidad de audio que se estima percibirá un usuario. Una característica fundamental del modelo es la utilización de factores de degradación de la transmisión que reflejan los efectos de los dispositivos de procesamiento de señales, cuyo objetivo es predecir la calidad de la voz en función del retardo, el jitter, las pérdidas y otras características de la red.

El modelo E esta especificado en la recomendación ITU-T G.107 y estipula que la calidad de la voz puede evaluarse a través del parámetro R (factor de determinación de índice de la calidad) que puede relacionarse con el MOS de acuerdo a la figura 2.11.

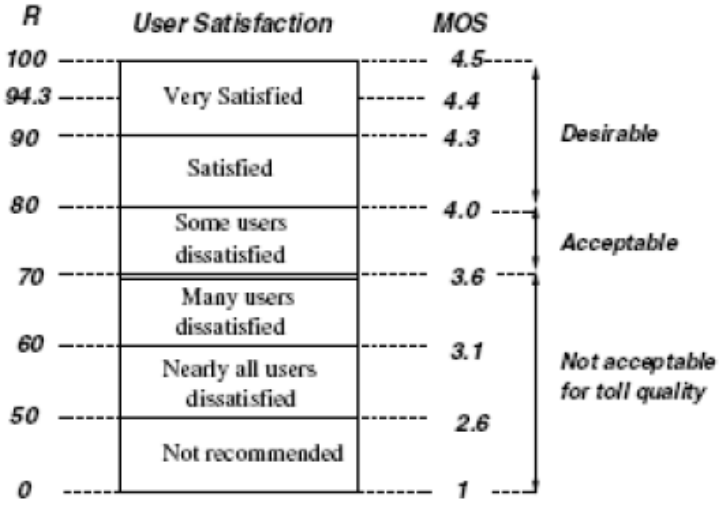


Figura 2.11 Modelo E.

Definido como:

$$R = Ro - Is - Id - Ie + A$$

El termino Ro es el efecto de ruido medido obtenido de la relación señal a ruido, Is modela la degradación que sufre la señal como consecuencia de su conversión a un formato adecuado para su transmisión por la red, Id modela las degradaciones producidas por los retardos y el eco, mientras que Ie representa las degradaciones producidas por las pérdidas de paquetes; finalmente A es el margen de seguridad, el cual es un factor de ventaja que significa que el usuario aceptaría una degradación en la calidad a cambio de facilidad de acceso. Los parámetros anteriores se calculan de los parámetros de transmisión que sirven en la figura 2.12.

El retardo es uno de los factores más importantes a considerar, su impacto en el modelo E está representado por el parámetro Id que en redes IP es función del retardo extremo a extremo

$$Id = 0.024.d + 0.11.(d - 117.3) \,.\, H(d - 117.3)$$

Donde H(x) es la función de Hearyside:

$$H(x) = \begin{cases} 0 & x < 0 \end{cases}$$

1 x >= 0

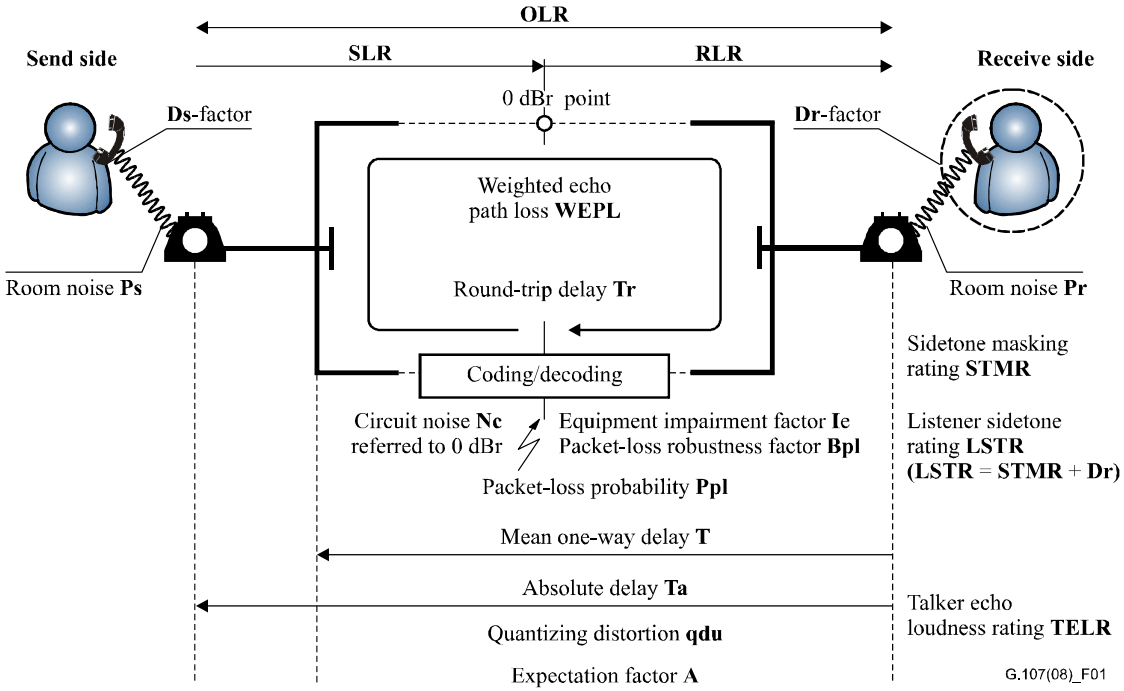


Figura 2.12 Factor de determinación de índice de calidad.

Si se representa gráficamente esta relación, como se muestra en la figura 2.13, se concluye que entorno a los 175 ms un aumento del retardo supone una disminución drástica de la calidad de voz, algo que concuerda con la recomendación ITU-TU G.114 en la que se aconseja que los valores del retardo en un solo sentido no superen los valores comprendidos entre 150 ms y 200 ms.

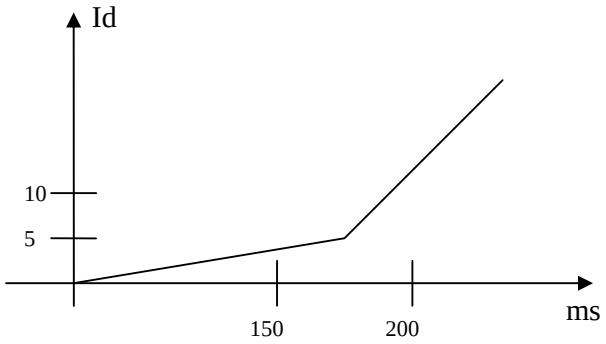


Figura 2.13 Id vs Retardo en ms

El factor de determinación de índice de transmisión R puede variar entre 0 y 100, donde R = 0 representa una calidad extremadamente mala y R = 100 representa una calidad muy alta, la salida del modelo E, R, a partir del cual se puede obtener un valor en la escala MOS de la calidad de voz. Se puede obtener medidas MOS en la escala de 1 a 5 utilizando las formulas

$$MOS = \begin{cases} 1 & R = 0 \\ 1 + 0.035R + 7R\,(R-60)\,(100-R).10^{-6} & 0 < R < 100 \\ 4.5 & R > 100 \end{cases}$$

donde se obtiene la figura 2.14.

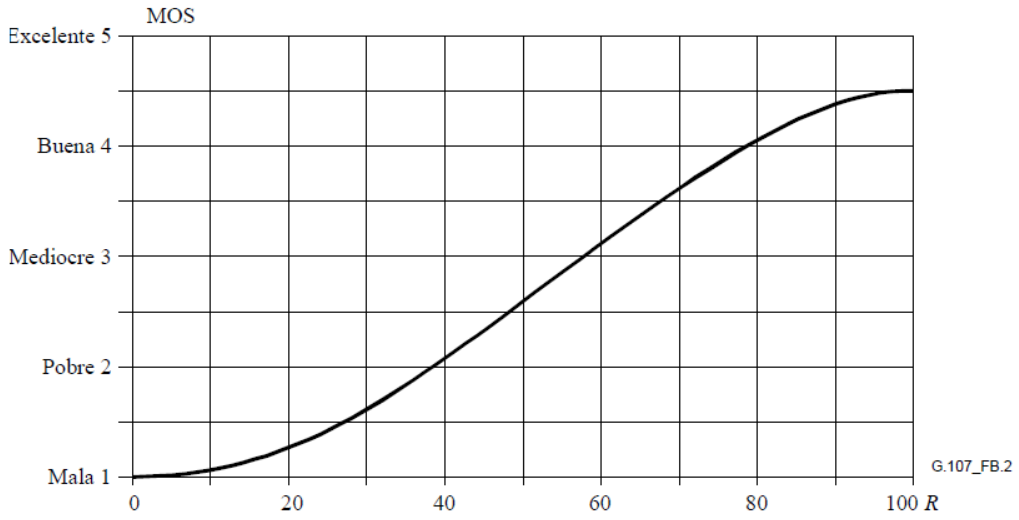


Figura 2.14 Medidas MOS.

A partir de la gráfica anterior se deduce que el valor máximo de R es 94.2, la calidad nunca podrá ser mayor de 4.4 y cualquier procedimiento de la voz produce una degradación de la calidad.

PSQM (Perceptual Speech Quality Mesaure). Es un algoritmo utilizado en señales telefónicas estandarizado en la recomendación ITU-T P.861, considera los efectos psicoacústicos en la percepción de la calidad del sonido. La finalidad es imitar la percepción del sonido experimentada en conversaciones reales, el experimento consta en juzgar la calidad de los codecs comparando una señal codificada a una señal fuente.

En la medida en que la PSQM es una fiel representación de los procesos de percepción audibles, las diferencias inaudibles entre la señal de entrada y de salida recibirán la misma nota PSQM. Los parámetros de esta prueba son el nivel de escucha, la ponderación en intervalos de silencio, ruido ambiental en el lado de recepción, características del umbral de audición, características de emisión y recepción del micro teléfono. Dado que la relación entre los valores MOS y PSQM no son necesariamente la misma para los diferentes idiomas, ni siquiera para distintas pruebas subjetivas con un mismo idioma, es difícil determinar una función única que transforme el valor PSQM al valor MOS estimado. En la práctica es necesario obtener con anticipación dichas funciones de transformación para cada idioma y para cada prueba subjetiva. En la figura 2.15 se muestra el diagrama del experimento PSQM.

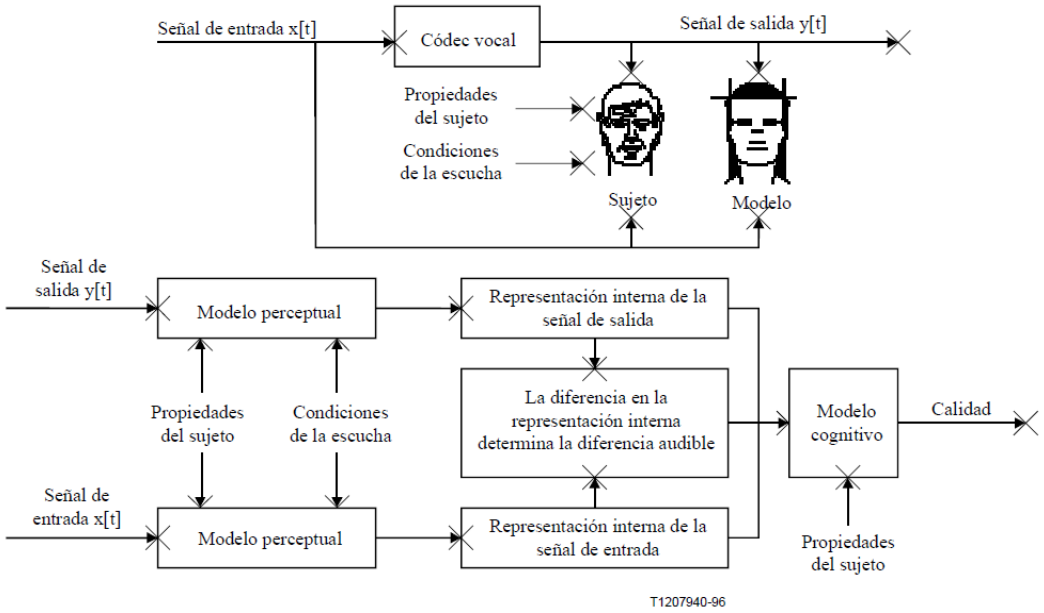


Figura 2.15 PSQM.

La figura 2.16 resume de manera general el procedimiento de medición objetiva utilizando PSQM.

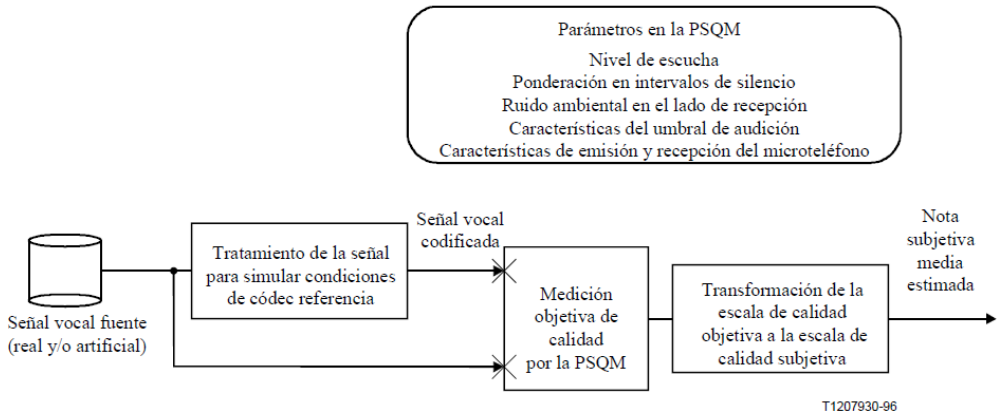


Figura 2.16 Procedimientos de medición PSQM.

PESQ. (Perceptual Evaluation of Speech Quality). Desarrollado originalmente por BT (British Telecomunication) y la KPN (Research in the Netherlonds) y recomendado por la ITU-T en P.862, es un método objetivo para predecir la calidad subjetiva de la voz telefónica utilizando los codecs mas comunes. PESQ compone una señal inicial X(t) con una señal degradada Y(t) que se obtiene como resultado de la transmisión de X(t) através de un sistema de comunicaciones. La salida de PESQ es una predicción de la calidad percibida por los sujetos en una prueba de escucha subjetiva y que sería atribuida a Y(t). El primer paso de PESQ consiste en una alineación temporal entre las señales inicial X(t) y degradada Y(t). Para cada intervalo de señal se calcula un punto de arranque y un punto de parada correspondientes. Una vez alineadas, PESQ, compara la señal (entrada) inicial con la salida degradada alineada, utilizando un modelo de percepción, como el que se presenta en la figura 2.17.

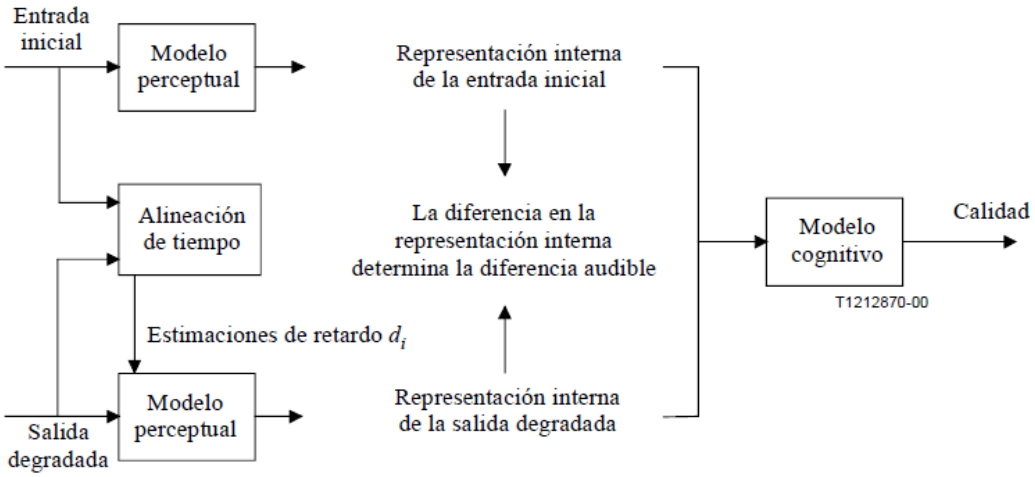


Figura 2.17 PESQ.

Lo esencial del proceso es la transformación de la señal inicial y la degradada, en una representación interna que intenta reproducir la representación psicoacustica de señales de audio en el sistema auditivo humano, teniendo en cuanta la frecuencia por percepción (Bark) y la sonoridad (Sone).

PESQ toma en cuenta problemas de una red IP como lo son el jitter, retardo, errores de codificación y filtrado. Su principal inconveniente es que no está diseñado para aplicaciones de streaming. El modelo PESQ termina brindando una comparación entre la señal vocal inicial y la señal vocal degradada, la que corresponde a su vez con una predicción de la MOS subjetiva. La nota PESQ corresponde a una escala similar a la de MOS, un número único en una escala de -0.5 a 4.5, aunque en la mayoría de los casos la gama de las salidas estará entre 1.0 y 4.5 que es la gama normal de los valores MOS.

C.ITU-T P.563. Es un algoritmo aplicable a la predicción de la calidad vocal sin una señal de referencia independiente, por tal motivo, se recomienda para la evaluación no intrusiva de la calidad vocal y para la supervisión y evaluación con la red en funcionamiento, empleando en el extremo lejano de una conexión telefónica fuentes de señal vocal desconocidas.

El enfoque utilizado en P.563 puede visualizarse como un experto que escucha una llamada real con un dispositivo de prueba, tal como un micro teléfono convencional conectado en paralelo a la línea. Esta visualización permite explicar la principal aplicación y permite al usuario clasificar las puntuaciones obtenidas mediante P.563. La puntuación de calidad que se predice mediante P.563 está relacionada con la calidad percibida en extremo receptor.

En la figura 2.18 se muestran algunas diferencias entre la recomendación ITU-T P.862 y P.563.

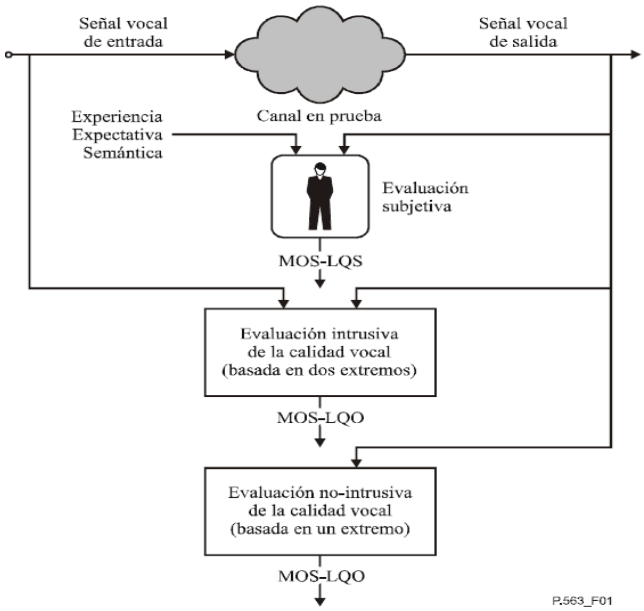


Figura 2.18 Diferencias entre T.P862 y P.563.

La señal vocal que debe evaluarse se analiza de varias formas, que detectan un conjunto de parámetros de señal característicos. En base a un conjunto restringido de parámetros clave, se establece la asignación a una clase de distorsión principal.

La parametrización de la señal del algoritmo P.563 puede dividirse en tres bloques funcionales independientes que se corresponden con las tres clases de distorsión principales, las que corresponden con el análisis del tracto vocal y desnaturalización de la voz, el análisis de un ruido adicional intenso y las interrupciones, silenciamientos y recorte temporal. El modelo de calidad vocal de P.563 se compone de tres bloques principales: 1) Decisión sobre la clase de distorsión de que se trata. 2) Evaluación de la calidad vocal intermedia para la correspondiente clase de distorsión. 3) Cálculo global de la calidad vocal.

La calidad vocal definida se calcula combinado los resultados de calidad vocal intermedia con algunas características adicionales a la señal.

2.3.2 Comparación de métodos objetivos.

En la tabla 2.11 se muestran algunas ventajas y desventajas de los métodos objetivos. Sin embargo, ningún método es 100% exacto, pero cada algoritmo presenta las siguientes ventajas y desventajas.

Algoritmo	Ventajas	Desventajas
PSQM	Bajo costo	-Sensible al delay -Sensible al procesamiento -Requiere señal de referencia -No se puede probar el jilter de extremo a extremo, ni paquetes

		perdidos
PESQ	Bajo costo Alta confiabilidad Se puede probar el Jitter y la pérdida de paquetes	-Sensible al delay -Requiere señal de referencia -Sensible al procesamiento -No diseñado para aplicaciones de streaming
P.563	No intrusivo Solo aplica en puntos finales de la red	-Inexacto -Complejo
E Model	No afecta al desempeño de la red Muy bajo costo	-Solo palabras son conocidas por los codecs -Muchos problemas de red no son contemplados -La combinación de varios problemas de red son difíciles de predecir

Tabla 2.11 Métodos Objetivos.

En resumen, de acuerdo a las características anteriores se recomienda utilizar el algoritmo PESQ para medir la calidad de voz en una red de comunicación.

2.3.3 Aportes recientes.

La ITU-T esta estandarizado una metodología de medición de calidad de voz basado solamente en información de los paquetes IP, asumiendo un payload de voz genérico. Será el estándar P.VTQ. Es una herramienta no intrusiva ya que no ocupa el canal. Servirá para monitorear en tiempo real la calidad de la transmisión. Permitirá a un proveedor conocer la calidad de voz que está ofreciendo en un momento concreto a un cliente para realizar una gestión dinámica de la red.

Una de las herramientas candidatas para el estándar es PsyVoIP, opera monitoreando en tiempo real llamadas VoIP de clientes para determinar la calidad de voz brindada por una red VoIP. La punta de prueba PsyVoIP captura los datos de una llamada específica como se muestra en la figura 2.19.

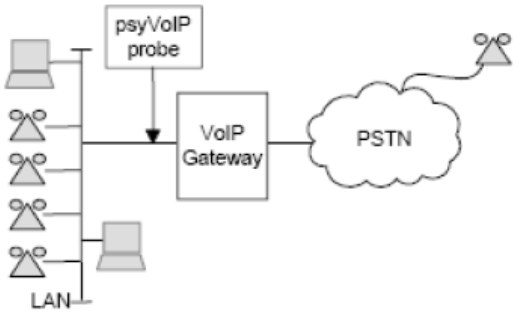


Figura 2.19. PsyVoIP.

PsyVoIP clasifica y caracteriza los distintos gateways y teléfonos IP ya que se comprobó que dan distinta calidad ante las mismas condiciones de red.

Otra propuesta de medición no intrusiva se presenta en la figura 2.20. Se propone tomar los paquetes recibidos, extraer su encabezamiento y sustituir el "payload" de voz con una señal conocida. De esa forma se obtiene una señal sustituta

conocida, con la misma distorsión que la recibida. Luego se puede aplicar cualquiera de las herramientas objetivas que precisan de la señal original (PESQ, PQSM) y obtener un MOS.

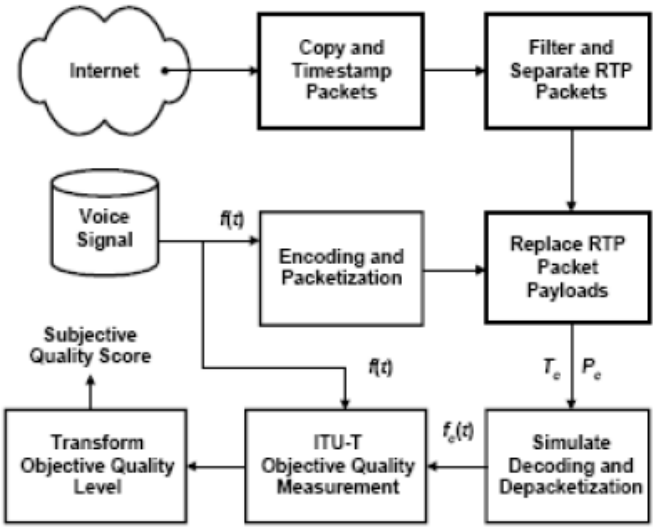


Figura 2.20 Medición no Intrusiva.

3

Protocolos de señalización VoIP.

De la misma forma que en una red de datos, las redes de voz sobre paquetes requieren de una serie de normas que especifiquen las funcionalidades y servicios que este tipo de redes deben proveer a los usuarios. Estas normas son los protocolos, un aspecto muy importante es que deben ser abiertos e internacionalmente aceptados con la finalidad de garantizar la interoperabilidad entre productos de distintos fabricantes, facilitando la elección de los usuarios y disminuyendo los procesos de los equipos al fabricarse estos en mejor escala. Un protocolo es una convención o estándar que controla o permite la conexión, comunicación, y transferencia de datos entre dos puntos finales. Los protocolos de VoIP definen la manera en que dispositivos deben establecer la comunicación entre sí, además de incluir especificaciones para codecs de audio para convertir una señal auditiva a una digitalizada compresa y viceversa, como se observa en la figura 3.1.

En redes telefónicas convencionales, una llamada consta de varios pasos, sin embargo se resume en: establecimiento, comunicación y desconexión. Durante el establecimiento se reservan los recursos necesarios para que en la fase de comunicación, la información pueda fluir libremente entre los dos extremos. Finalmente, en la desconexión se liberan los recursos que previamente, se habían reservado y se pasa la información necesaria para que pueda ser costeable la llamada (tarificada). Tradicionalmente, se ha venido distinguido tres grupos de protocolos que pueden ir bien sobre TCPVo UDP, y ambos sobre IP. En el presente capitulo se detalla los protocolos utilizados en VoIP divididos en:

Protocolos de señalización. El objetivo es establecer un canal de comunicación a través del cual fluya la información de usuario y liberar el canal cuando finalice la comunicación. Para ello, debe existir un dialogo entre los componentes de la red y las

terminales de usuario. Son protocolos de señalización el H.323, SIP y MGCP, entre los más importantes.

Protocolos de transporte. Son las normas que definen como debe realizarse la comunicación entre los extremos por un canal de comunicaciones previamente establecidos. Los protocolos de transporte más empleados son RTP y RTCP.

Protocolos de Gestión. Cuando el tamaño de las redes aumenta se convierte en un entramado muy complejo de hardware y software y, si no se toman las medidas oportunas, se corre el riesgo de volverse inmanejables. Esto es lo que pretende evitar el sistema de gestión y mantenimiento. El protocolo de gestión RTCP XR es lo comúnmente utilizado por los diseñadores de red.

Con el crecimiento de Internet la preocupación por la seguridad en redes es una preocupación continua, y las redes de voz sobre paquetes no son la excepción, para ello se han desarrollado protocolos de seguridad en ámbitos como la voz, señalización y control de llamadas. Sin embargo, VoIP es una tecnología que ha de apoyarse necesariamente en muchas otras capas y protocolos ya existentes de las redes de datos, utilizando como base la teoría ya establecida para estas redes, no es prioridad para este trabajo la explicación de las seguridad en redes VoIP versión 4.

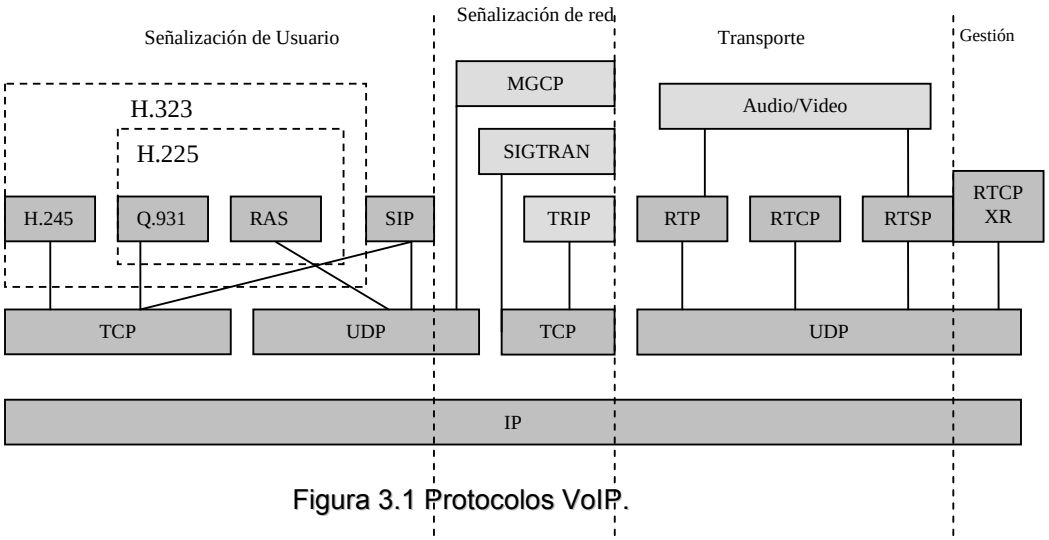


Figura 3.1 Protocolos VoIP.

Los protocolos de señalización en redes de voz realizan el establecimiento de sesiones, señales de progreso de llamadas, gestión de participantes, apartan recursos necesarios en la red. Por otra parte, las expectativas de calidad del usuario exigen una red de señalización de altas prestaciones, pues la disponibilidad debe ser similar a la de la PSTN (99.999%). Esta es la razón por la que la fiabilidad no solo deba residir en los elementos de la red sino también en la arquitectura de señalización empleada.

En VoIP se tienen protocolos de señalización entre terminales y protocolos de señalización en la red IP, los protocolos de señalización entre terminales son comunes a cualquier tipo de comunicaciones multimedia (voz, video y audio) a través de las redes de paquetes. Aplicados a la voz sobre paquetes, tienen como objetivo mantener la interfaz con el usuario típica de las redes telefónicas, es decir, generar los tonos y señales necesarios para que el usuario no perciba que la tecnología de soporte de las

llamadas telefónicas ha cambiado. Los protocolos más destacados son el H.323, SIP, MEGACO y otros no más populares.

3.1 H.323

Es un conjunto de protocolos que definen los componentes y los medios de interacción entre los mismos elementos de red que deben cumplirse para soportar comunicaciones multimedia sobre redes de paquetes sin conexión, ni garantía de calidad de servicio, como el caso de las redes de voz sobre IP. Este protocolo fue desarrollado y estandarizado por la ITU desde 1996, originalmente desarrollado para soportar conferencias multimedia sobre redes LAN, aunque actualmente se aplica a voz sobre paquetes, por lo que permite la transmisión en tiempo real de video y audio por una red de paquetes.

El protocolo H.323 es una suite de protocolos de audio y video preparada para compartir aplicaciones, la arquitectura de este protocolo se muestra en la figura 3.2. Los protocolos cubren los distintos aspectos de la comunicación en la red, desde el direccionamiento y la señalización de las llamadas, tal como se describe continuación.

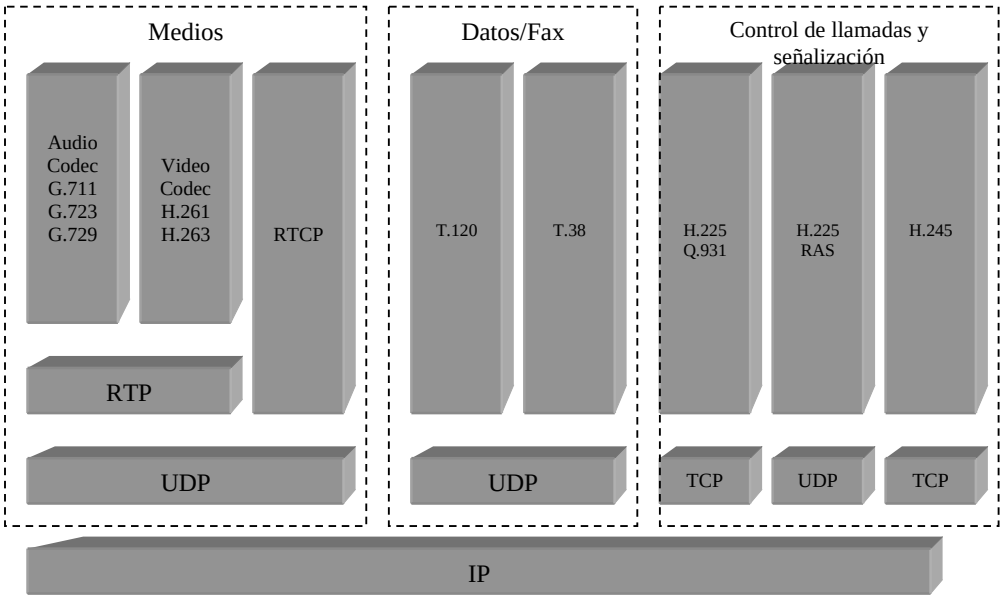


Figura 3.2 Arquitectura H.323.

H.225. Este protocolo permite empaquetar, sincronizar e iniciar las llamadas usando mensajes de señalización, como es el establecimiento, control y finalización de una llamada H.323. La señalización H.225.0 está basada en los procedimientos de establecimiento de llamada de RDSI, Recomendación Q.931. Define la señalización RAS (Registration Admission and Status). Este protocolo permite registrar el control de admisión, control del ancho de banda, estado de llamada y desconexión de las terminales. Permite el dialogo entre terminales H.323 y el Gatekeeper, los cuales se describen mas adelante, cuya finalidad es el registro de una terminal con el servidor.

Q.931. Este protocolo maneja la inicialización y fin de las llamadas, además se utiliza para señalización de llamada en la red IP, es decir desde la puerta de enlace a

la terminal. En un protocolo de control de conexiones utilizado en ISDN. No provee control de flujo ni realiza retransmisiones.

H.245. Tiene la capacidad de transmitir y proporcionar la información necesaria para la comunicación multimedia, tal como la codificación, el control de flujo, la gestión del jitter, el procedimiento de apertura y cierre de los canales lógicos para transmitir el flujo de datos. Define las capacidades de envió y recibo de información, y los métodos para enviar estos detalles a otros dispositivos que soporten H.323.

H.235. Es una recomendación de la ITU para seguridad en sistemas H.323. El estándar aborda la autentificación mediante diferentes algoritmos y privacidad en conexiones punto a punto y multipunto, la privacidad proporciona el cifrado de la sesión.

3.1.1 Componentes de una red H.323.

Una red H.323 está compuesta por terminales, Gateway, controladores de acceso (MC) y unidades de multiconferencia (MCU). Dichos componentes se comunican mediante la transmisión de trenes de información.

Terminales. Son los equipos utilizados por los usuarios finales y abarcan desde teléfonos tradicionales hasta teléfonos IP, PCs y sistemas de conferencia. En la figura 3.3 se muestra un ejemplo de una Terminal H.323.

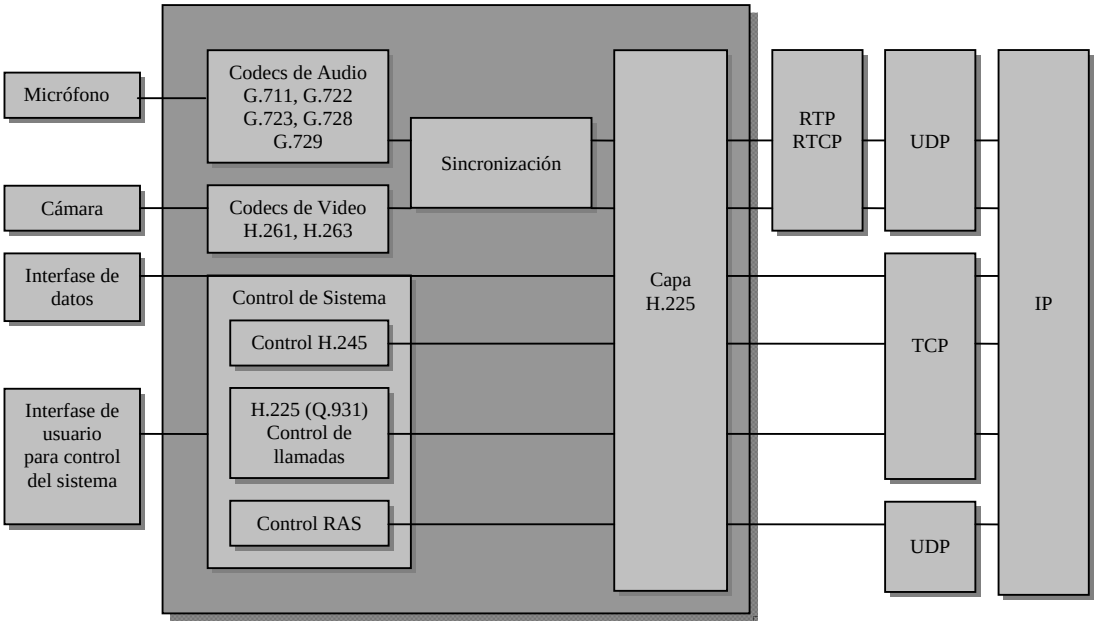


Figura 3.3 Terminal H.323 y su Arquitectura.

En el diagrama se muestran las interfaces del equipo del usuario, el codec del video, el codec de audio, el equipo telefónico, la capa H.225.0, las funciones de control del sistema y la interfaz con la red de paquetes. Todas las terminales H.323 tienen una unidad de control del sistema, capa H.225.0, interfaz de red y unidad de codec de audio.

La comunicación bajo H.323 contempla las señales de audio y video. La señal de audio se digitaliza y se comprime bajo uno de los algoritmos soportados como, G.711 y G.723, y la señal de video (opcional) se trata con la norma H.261 o H.263. Los datos (opcional) se manejan bajo estándar T.120 que permite la comparación de aplicaciones en conferencias punto a punto y multipunto.

Gateway. Se encarga de proporcionar la conversión adecuada entre formatos de transmisión y entre procedimientos de comunicaciones. Además lleva acabo el establecimiento y la liberación de la llamada en el lado de la red y en el lado de la PSTN. La conversión entre formatos de video, audio y datos también puede efectuarse en el Gateway. Son elementos opcionales cuando las comunicaciones multimedia se establecen entre equipos de una misma red local. En este dispositivo se cuenta con una interface IP hacia la red VoIP y otra interface hacia una red diferente, como puede ser la red de telefonía convencional.

Gatekeeper. El Gatekeeper es un controlador de acceso, es opcional en una red H.323, presta servicios de control de llamada a los puntos extremos H.323. Además facilita el control del ancho de banda utilizado y localiza los distintos Gateways y MCU's cuando se necesita Puede haber más de uno en la red. Este elemento presta los siguientes servicios:

- Conversión de dirección. Efectúa la conversión de dirección alias a dirección de transporte, utilizando un cuadro de conversión que se actualiza mediante mensajes de registro.

- Control de admisiones. Controla el acceso a la red utilizando mensajes H-225.0. La autorización de acceso puede basarse en la autorización de la llamada, en el ancho de banda o en algún otro criterio.

- Control de ancho de banda. Soporta mensajes de señalización para asignar o negar el ancho de banda

- Gestión de zona. Gestiona la zona configurada a cada elemento de la red. Una zona es una colección de nodos H.323 como es el Gateway, MCU, terminales, registrados por un Gatekeeper. Por zona solo se tiene configurado un solo Gatekeeper (figura 3.4).

- Señalización de control de llamada, autorización de llamada , gestión de anchura de banda, gestión de llamada, modificación del alias de dirección, conversión de los dígitos marcados, estructura de datos de información de gestión del controlador de acceso y servicio de directorio.

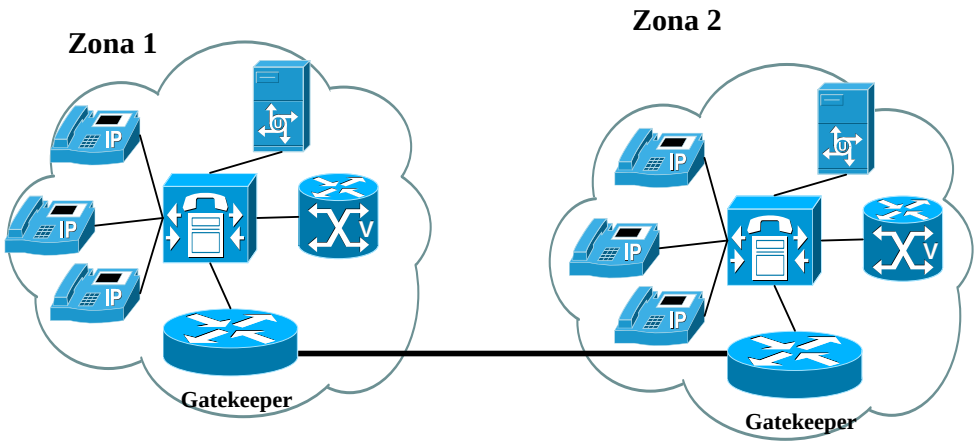


Figura 3.4 Gestión de Zona.

MC. El controlador multipunto proporciona funciones de control para soportar conferencias entre tres o más puntos externos de una conferencia multipunto. Este dispositivo lleva acabo el intercambio de capacidades con cada uno de los puntos externos de una conferencia multipunto y envía un conjunto de capacidades a los puntos externos de la conferencia indicando los modos de funcionamiento en los que pueden transmitir, de esta manera determina el modo de comunicación seleccionado para la conferencia.

MCU. Es un punto externo que da soporte a conferencias multipunto y deberá estar formada por un MC y un procesador multipunto. Este elemento utiliza los mensajes y procedimientos H.245 para implementar características similares a H.243. Se encarga de mezclar los flujos de audio y video y distribuir dichos flujos entre todos los participantes.

3.1.1.2 Señalización.

La señalización consiste en los mensajes y procedimientos utilizados para establecer una comunicación, pedir cambios de ancho de banda, obtener el estado de los puntos externos y desconectar la llamada. El establecimiento de la comunicación se efectúa utilizando mensajes de control de llamada con la recomendación H.225 RAS. El dialogo entre terminales y el Gatekeeper tiene como finalidad el registro, la admisión y el control del estado de una Terminal de usuario en la misma red H.323. En la fase de registro la terminal indica al Gatekeeper su dirección IP para que se mantenga el vínculo entre la dirección lógica y el usuario. Para cada llamada se establece un canal de señalización entre el Terminal y el Gatekeeper, un canal de señalización entre los terminales y un canal lógico de control entre los terminales con H.245. El establecimiento de la llamada en H.323 se lleva a cabo en tres fases y se muestra en la figura 3.5

1. RAS. Es el intercambio de mensajes entre el Gatekeeper y la terminal., para la traducción de direcciones, autorización de llamadas y gestión del ancho de banda.
2. Q.931. Es el intercambio de mensajes entre terminales para el establecimiento de conexiones lógicas.

3. H.245. Es el intercambio de mensajes entre terminales para acordar en intercambio de información de usuario.

El paso previo al establecimiento de una comunicación entre dos terminales es la resolución de la dirección IP del destinatario de la llamada a través del Gatekeeper, el cual si el proceso de registro es satisfactorio, el control de acceso dará de alta la IP del usuario y será enviada a la entidad llamante, los mensajes para este proceso se basan en H.225 y se transportan por UDP.

Una vez conocido el destino final y autorizado por el Gatekeeper, el llamante establece un canal de comunicación por una conexión TCP con el destino. Cuando el llamante recibe la solicitud de conexión, este le pide autorización al Gatekeeper, ya autorizado envía al llamante un mensaje Q.931 notificando que ha aceptado la solicitud de llamada. Esta negociación se lleva a cabo mediante el intercambio de mensajes H.245 sobre datagramas TCP. Finalmente, la comunicación queda establecida cuando ambos extremos se informan mutuamente de los puertos UDP de los canales RTP por los que fluirán los datos de cada extremo.

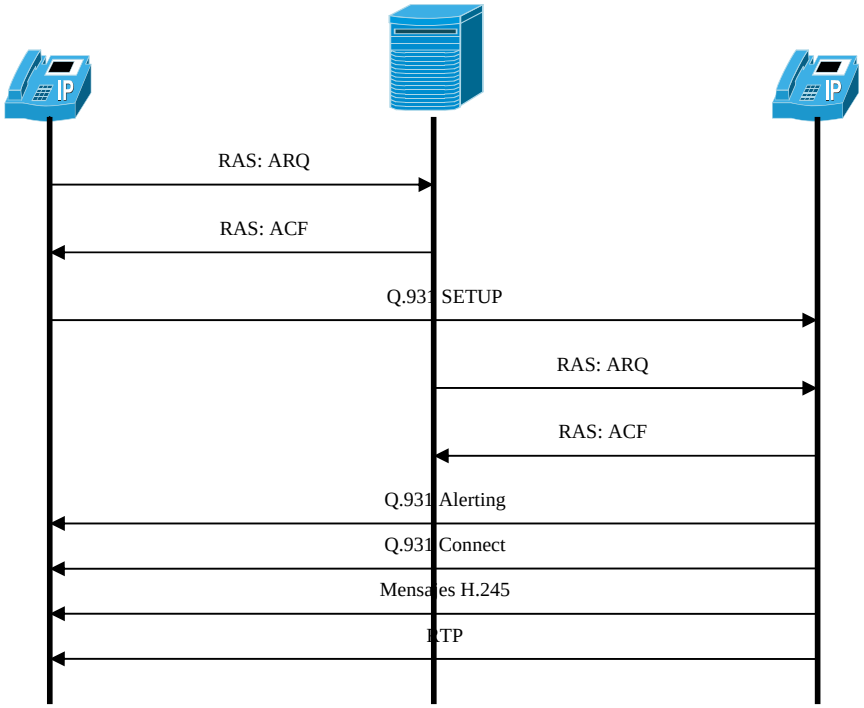


Figura 3.5 Establecimiento de una llamada H.323.

3.2 SIP

Es un protocolo de control en la capa de aplicación, define como iniciar, establecer, modificar o finalizar una sesión entre dos o más extremos en una red SIP. En Noviembre del año 2000, SIP fue aceptado como el protocolo de señalización de 3GPP y elemento permanente de la arquitectura IMS (IP Multimedia Subsystem). Definido por la Internet Engineering Task Force (IETF) como un protocolo de señalización en su recomendación RFC 2543 y aclarado en el RFC 3261.El protocolo H.323 es utilizado en redes corporativas, mientras que SIP es un protocolo basado en http, solo se definen los elementos que participan en un entorno SIP y el sistema de

mensajes que intercambian. Utiliza el protocolo SMTP (Simple Mail Transfer Protocol) para transmitir mensajes electrónicos y el direccionamiento utiliza el concepto de "Uniform Resource Locutor" o URL, el cual es parecido como una dirección de e-mail (userID@host), por lo que cada participante en una red SIP es alcanzable vía una dirección o por nombre de dominio, utiliza ambos protocolos con la el fin de que la telefonía se despliegue de forma más sencilla sobre el Internet, convirtiéndola en un servicio más. El SIP es un protocolo basado en texto que utiliza la codificación Utf-8. La conexión es por medio de TCP para clientes SIP y UDP para conectar con los servidores. Las aplicaciones SIP usan el puerto 5060 por default para ambos UDP y TCP. El tipo de sesión a establecer está definida por SDP (Session Description Protocol), que describe el contenido multimedia de la sesión. Una vez la sesión está establecida, los participantes de la sesión intercambian directamente su tráfico audio/video a través del protocolo "Real Time Transport Protocol" (RTP).

SIP no es un protocolo de reservación de recursos, y en consecuencia, no puede asegurar la calidad de servicio. Se trata de un protocolo de control de llamada y no de control del medio. SIP está basado en una arquitectura cliente-servidor en el cual los clientes inician las llamadas y los servidores responden las llamadas. Es un protocolo abierto basado en estándares, es ampliamente soportado y no es dependiente de un solo fabricante.

Para la telefonía IP la gran ventaja de SIP es que el proceso de establecimiento de llamada es más simple que H.323 reduciendo de 1.5 a 5 el número de mensajes. Otra ventaja es la flexibilidad para soportar servicios, ha sido adoptado por 3GPP (3rd Generation Partnership Project) para soportar servicios multimedia de tercera generación en las redes móviles. SIP también implementa muchas de las más avanzadas características del procesamiento de llamadas de SS7, Sistema de Señalización de Canal número 7 para comunicación entre centrales telefónicas, aunque los dos protocolos son muy diferentes.

3.2.1 Componentes de red.

La arquitectura de una red SIP es muy similar a la de http, está compuesto por clientes y servidores, figura 3.6, las solicitudes del cliente son enviadas a un servidor, este las procesa y envía una respuesta al cliente. Está modelado entre agentes de usuario clientes y servidores de red, los cuales se describen en esta sección.

Agentes de usuario (UA, User Agent). Son terminales o puntos extremos de la red donde se originan las solicitudes para iniciar una nueva sesión o de terminar una sesión en curso. Los UA consisten en dos componentes funcionales a nivel lógico: 1) User Agent Client (UAC) encargado de iniciar solicitudes SIP, y 2) User Agent Server (UAS) es un servidor de aplicación que responde las solicitudes SIP para aceptar el establecimiento de una sesión. Ambas partes pueden terminar una sesión en curso. Los UA pueden ser teléfonos IP, softphones y gateway. Los UA´s deben implementar el transporte tanto sobre TCP como sobre UDP. Los UAC´s y UAS´s pueden, por si solos y sin los servidores de red, ser capaces de soportar una comunicación básica

Los servidores de red actúan como intermediarios en las comunicaciones entre los agentes de usuario y se clasifican en los siguientes tipos:

Servidor Proxy. Es un componente intermedio que recibe solicitudes SIP desde un cliente, actúa como servidor y un cliente, las solicitudes las reenvía en nombre del cliente al siguiente servidor SIP en la red. El siguiente servidor puede ser otro Proxy Server. Este elemento puede proporcionar funciones como son autentificación, autorización, control de acceso a la red, direccionamiento, confiabilidad en la transmisión de solicitudes y seguridad.

Servidor de Redirección. Se trata de un servidor quien acepta solicitudes SIP, traduce la dirección SIP de destino en una o varias direcciones de red y las devuelve al cliente. De manera contraria al Servidor Proxy, este servidor no encamina las solicitudes SIP. En el caso de una respuesta de una sesión devuelve el número de reenvío al cliente origen quien se encarga de establecer una sesión hacia este nuevo destino, además no pueden aceptar o terminar sesiones como ocurre con los UAS.

Servidor de Registro. Se trata de un servidor que acepta las solicitudes de registro de los usuarios, quienes envían un mensaje a este servidor con la dirección donde es localizable, como es la dirección IP o su dominio de red. El servidor actualiza una base de datos de localización por cada evento de registro. El registrador es una función asociada a otros servidores de red, frecuentemente el servidor de localización. Un mismo usuario puede registrarse sobre distintas UAS SIP:

Servidor de Localización. Proporciona información acerca de la localización del usuario, proporciona la resolución de direcciones a servidores Proxy y servidores de redirección. Si un usuario A desea comunicarse con un usuario B, A necesita descubrir la localización de B en la red, con el fin de que la petición de establecimiento de sesión pueda llegarle, por lo que primero se solicita al localizador por medio de un mensaje donde se encuentra el destino B, el localizador responde el mensaje y el usuario B ya conoce el lugar de su destino.

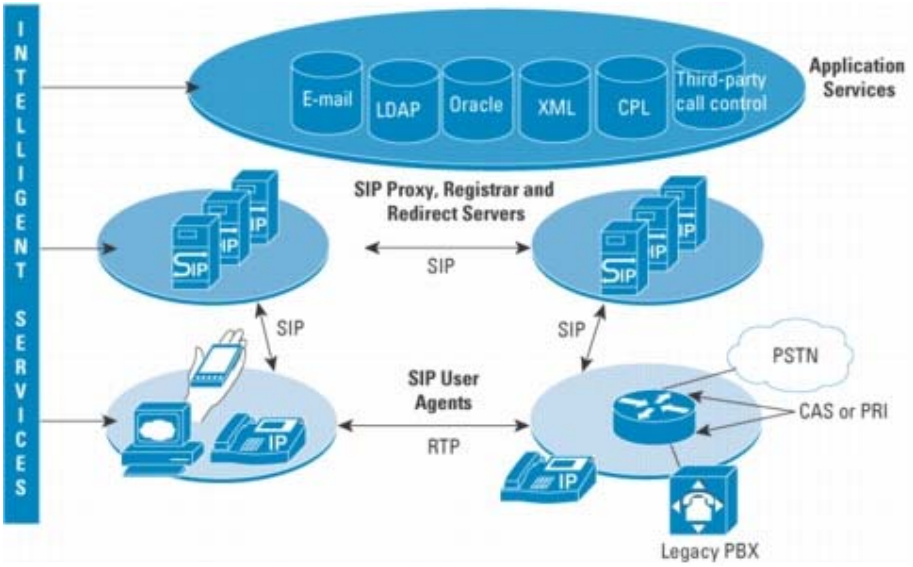


Figura 3.6 Elementos de una red SIP.

Tanto H.323 como SIP son consideradas arquitecturas punto a punto o descentralizadas, además, gran parte de la inteligencia en ambas arquitecturas reside en las terminales.

3.2.2 Señalización

La comunicación entre los componentes SIP es por peticiones y respuestas. Las peticiones o respuestas son enviadas en mensajes entre clientes y servidores, los mensajes están compuestos por una línea de comienzo, una o varias cabeceras, una línea vacía que indica el final de las cabeceras y un cuerpo de mensaje. La línea de comienzo nos informa del tipo de mensaje y la versión del protocolo, puede ser una línea de solicitud indicando el usuario o servicio al cual ha sido dirigido el mensaje, o una línea de estado (respuesta) informando el estado con un código basado en texto. SIP define 4 tipos de encabezado: un encabezado general, un encabezado de entidad, un encabezado de petición y un encabezado de respuesta. Las cabeceras son utilizadas para transportas atributos del mensaje y para modificar el significado del mensaje, son muy parecidas en sintaxis y semántica a los campo de la cabecera HTTP. Los campos en las cabeceras son los siguientes:

Via: Indica el transporte usado para el envío e identifica la ruta de la solicitud, por ello cada proxy añade una línea a este campo.
From: Indica la dirección del origen de la petición.
To: Indica la dirección del destinatario de la petición.
Call-Id: Identificador único para cada llamada y contiene la dirección de la entidad SIP. Debe ser igual para todos los mensajes dentro de una transacción.

Cseq: Se inicia con un número aleatorio e identifica de forma secuencial cada petición.
Contact: Contiene una o más direcciones que pueden ser usada para contactar con el usuario.
User Agent: Contiene el Agent Client que realiza la comunicación.

Finalmente, el cuerpo del mensaje es usado para describir la sesión a ser iniciada o alternativamente puede ser usada para contener información binaria o en texto relacionada de alguna forma con la sesión. SIP hace una clara distinción entre la información de señalización, transportada en la línea de comienzo y en las cabeceras, y la información de descripción de la sesión, el cual está fuera del alcance de SIP. Todos los mensajes SIP son basados en texto y descritos en la RFC 822.

Los mensajes de solicitud indican la acción a ser tomada por los servidores y son los siguientes:

INVITE. Mensaje inicial de invitación a iniciar una conexión, enviado por el extremo llamante, este mensaje contiene información sobre el que genera la llamada y el destinatario, así como el tipo de flujos que serian intercambiados (voz y video/audio).
ACK. Es la respuesta de agente llamante ante el mensaje de aceptación de la llamada por parte del destino.
BYE. Señal de terminación de la sesión por parte de uno de los participantes.
CANCEL. Cancela una solicitud pendiente. No termina las llamadas/sesiones que han sido aceptadas.
REGISTER. Informa a un servidor de registro sobre la ubicación actual del usuario dentro del dominio.
OPTIONS. Consulta a un agente de usuario acerca de sus capacidades. Se utiliza antes de iniciar la llamada a fin de averiguar si este agente tiene la capacidad de transmitir distintos tipos de flujos.
INFO. Contiene información fuera de banda, como dígitos DTMF.

Los mensajes de respuesta son enviados en respuesta a una solicitud e indica la interpretación y ejecución de la solicitud. Estos mensajes toman tres posibles posturas: exitoso, falla o provisional, están compuestos por:

1xx. Es un mensaje de información e indica que la solicitud esta aun siendo procesada.
2xx. Éxito. Indica que la solicitud ha sido completa y exitosa.
3xx. Mensaje de desvío. Indica que el solicitante necesita una acción más lejana.
4xx. Error en la petición. Indica que la solicitud del cliente fallo o es imposible de ser completada.
5xx. Error en el servidor. Indica que la solicitud es válida pero el servidor fallo para completarla.
6xx. Error general. Indica que la solicitud no puede ser completada por algún servidor.

3.2.3 Establecimiento de una sesión.

El establecimiento de una sesión depende del tipo de conexión, si un User Agent (UA) reconoce el destino del User Agent Server (UAS), el cliente se comunica directamente con el servidor. En situaciones en el cual el cliente es incapaz de establecer una relación directa, el cliente solicita la asistencia de un servidor de red, el cual puede ser un servidor Proxy o un servidor de re direccionamiento.

Los pasos básicos implicados en el manejo de sesiones SIP son los siguientes y se describen en la figura 3.7:

- Registro, iniciación y localización del usuario.
- Descripción de la sesión multimedia que se pretende establecer
- Aceptación de la petición de conexión del otro extremo
- Establecimiento de la sesión
- Comunicación
- Terminación de la sesión

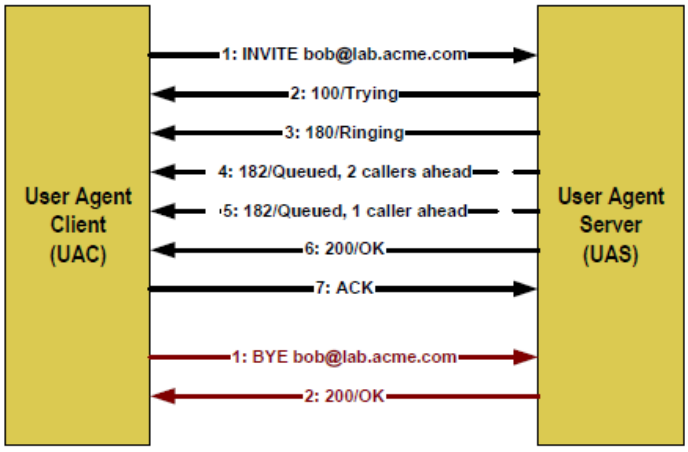


Figura 3.7 Establecimiento de una sesión SIP.

Los mensajes SIP se transportan utilizando UDP o TCP, aunque la IETF tiene su protocolo, SCTP (Stream Control Transport Protocol), para un transporte fiable de señalización sobre IP. SDP (Session Description Protocol) se encarga de la descripción de las características de la sesión entre los extremos. Su objetivo es proporcionar información acerca de los flujos de datos a los respectivos receptores; SDP no es exclusivo de SIP, sino que también se emplea con otros protocolos. Por otra parte, SAP (Session Announcement Protocol) es utilizado para la publicación de sesiones multicast mediante el envío periódico de un paquete de anuncio que contiene una dirección y un puerto multicast conoce dos.

3.3 MGCP

Este protocolo se desarrolló principalmente para atender las demandas basadas en redes de telefonía IP. MGCP es un protocolo complementario, tanto para H.323 y SIP. Es un protocolo de control de dispositivos desarrollado por la IETF en el RFC3435, define la comunicación entre elementos que controlan una llamada denominados MGC (Media Gateway Controller), MG (Media Gateway) y un SG (Signaling Gateway),y por medio de mensajes de texto crear, administrar y terminar comunicaciones multimedia en un sistema de comunicaciones centralizado. Diseñado para redes grandes, permite a un componente de control central, también llamado Call Agent, administrar remotamente varios dispositivos, especificando que los Gateway esclavos (MG) son controlados por un maestro (MGC). El encargado de describir el tipo de sesión a iniciar es SDP, documentado en el RFC2327.

3.3.1 Arquitectura.

En una red con un protocolo MGCP implementado, la arquitectura física define un número de componentes y se ejemplifica en la figura 3.8, los cuales se detallan a continuación:

Media Gateway. Es típicamente un elemento de la red que proporciona la conversión entre la señal de audio transportada sobre redes de circuitos y paquetes de datos sobre Internet o sobre otras redes de paquetes. Ejemplos de algunos Media Gateway son: Gateway de Troncales, Gateway ATM, Gateway Residencial, Gateway de Acceso, entre otros.

Media Gateway Controller. También llamado Call Agent, puede crear, modificar y borrar conexiones entre MG; se encarga del registro, administración y control de los recursos en los puntos finales.
Signaling Gateway. Es una puerta de enlace cuando una red MGCP se conecta a la PSTN.

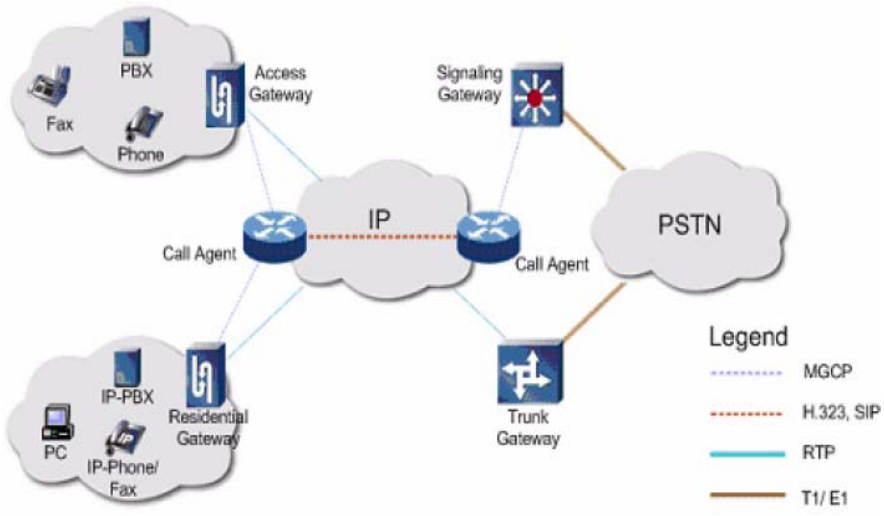


Figura 3.8 Arquitectura MGCP

El protocolo MGCP adopta un modelo donde los componentes básicos son las conexiones y los puntos finales o Endpoint. Las conexiones son agrupadas en llamadas. Una o más conexiones pueden pertenecer a una llamada. Los Endpoints representan el punto de interconexión entre la red de paquetes y la red tradicional de telefonía, son fuentes de datos y pueden ser virtuales o físicos, se presentan las siguientes variantes de este elemento:

DS0. Representa un canal digital y soporta más de una conexión.
Línea Analógica. Representa la interface final del servicio a la red tradicional de telefonía.
Servidor de Anuncios. Es un punto de acceso aun servidor de anuncios.
IVR. Representa un punto de acceso a un servidor de respuesta de voz i nteractiva.
Bridge de Conferencia. Representa el acceso a una conferencia específica.
Packet Relay. Representa el acceso de un bridge sobre dos conexiones para interconectar Gateways incompatibles o retransmitirlas en un firewall.
Troncal ATM. Representa una instancia de un canal de audio en una red ATM.

El nombre de endpoints se identifican por dos partes, un nombre local en contexto del gateway y el nombre de dominio del mismo Gateway que lo administra, las dos partes son separadas por un @ (local-endpoint-nameadomain-name), pero también se puede representar el nombre de dominio como una IPv4 o IPv6. El nombre del dominio es definido en la RFC 1034

MGCP simplifica las gateways al máximo, limitando sus funciones a la interconexión con redes de conmutación de circuitos, la notificación a los MGC de los eventos que ocurren en los terminales y la ejecución de comandos procedentes de los MGC. La inteligencia de control de llamadas se ubica en los Call Agent, el cual envía mensajes a las pasarelas que están bajo su control. El Call Agent usa su propio directorio de endpoint y la relación que cada uno tiene con el plan de marcación para determinar el direccionamiento de la llamada. La comunicación entre los MGC y los gateways se basa en el intercambio de comandos y la recepción de señales, son trasportados por UDP/IP, por la misma red de transporte IP con seguridad IPsec. De tal manera que el gateway solo realizara funciones de conversión vocal y genera una ruta RTP entre extremos, el MGC regula y administra la comunicación entre entidades de la red MGCP. El flujo de una llamada se muestra en la figura 3.9.

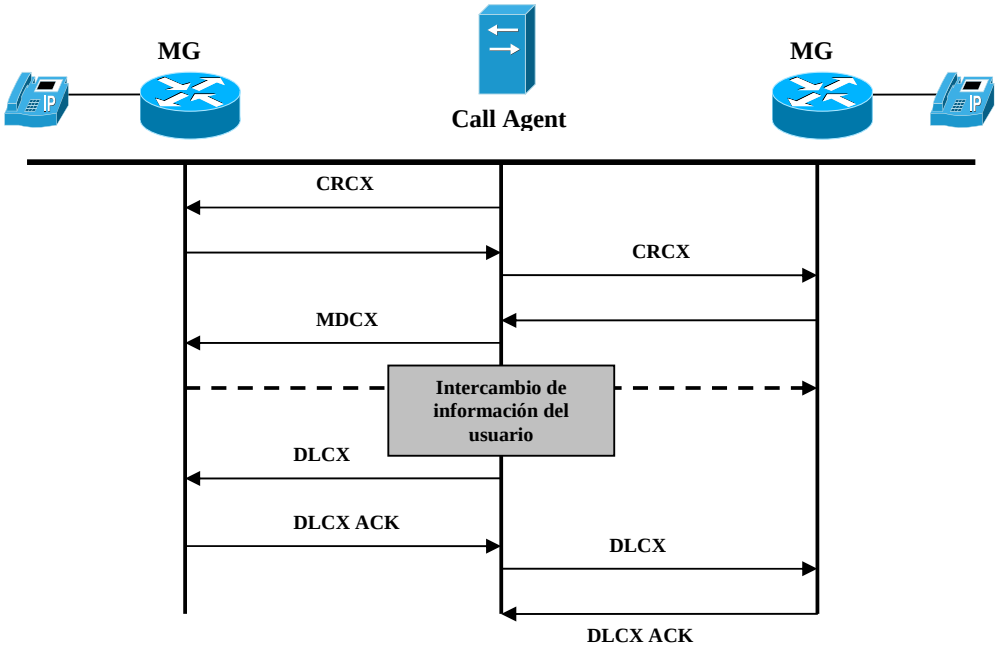


Figura 3.9 Conexiones y llamadas MGCP

Los mensajes se dividen en comandos y señales, los que se describen a continuación:

Comandos

ENDPOINTCONFIGURATION (EPCF). Configura las características de la línea del puerto (ley M o leyA).
NOTIFICATIONREQUEST (RQNT). Solicitud de notificación de eventos.
POLLNOTIFY (NTFY). Comprobación de la notificación de eventos.
CREATECONNECTION (CRCX). Crea una conexión que termina en un endpoint.
MODIFICONNECTION (MDCX). Modifica los parámetros de una conexión existente.
DELETE CONECTION (DLCX). Libera una conexión.
AUDITENDPOINT (AVEP). Recoge la configuración y la información de estado de un punto final.
AUDITCONECTION (AUCX). Recoge la información de estado de una conexión.
RESTARTINGPROGRESS (RSIP). Usado por os Gateway para señalar que un endpoint esta en servicio o fuera de servicio.

Señales.

NOTIFY (TFY). Indica que ha ocurrido algún evento.
DELECONECTION (DLCX). Informa que ha liberado una conexión.
RESTARTIN PROGRESS (RSIA). Uno o más puntos finales están siendo puestos fuera de servicio.

3.3.2. Establecimiento de una llamada.

El Call Agent envía un comando a cada Gateway, RQNT, para que cada uno espere cuando un endpoint descuelgue, cuando esto suceda el Gateway proporciona el tono de marcado, envía un mensaje de NOTIFY al Call Agent, el MG recoge los números marcados y los envía al MGC quien se encarga, a través de mensajes CRCX, de crear la conexión con el punto remoto. Si el destino descuelga los MG comienzan a negociar capacidades para después establecer el flujo RTP. Cuando el usuario llamante cuelga, se genera el comando NTFY al Call Agent (MGC), y este envía un DLCX para eliminar la conexión a los dos Gateway. En la figura 3.10 se muestra el flujo de mensajes en una llamada por MGCP.

Las sesiones punto a punto son establecidas por la conexión de dos o más terminales. En el establecimiento de una llamada, el Call Agent instruye al Gateway, asociado con cada endpoint, para hacer una conexión con un endpoint especifico o un endpoint de un tipo en particular, cada Gateway envía los parámetros de sesión al Call Agent, mientras que el Call Agent envía a cada Gateway el fin de la sesión por flujos RTP.

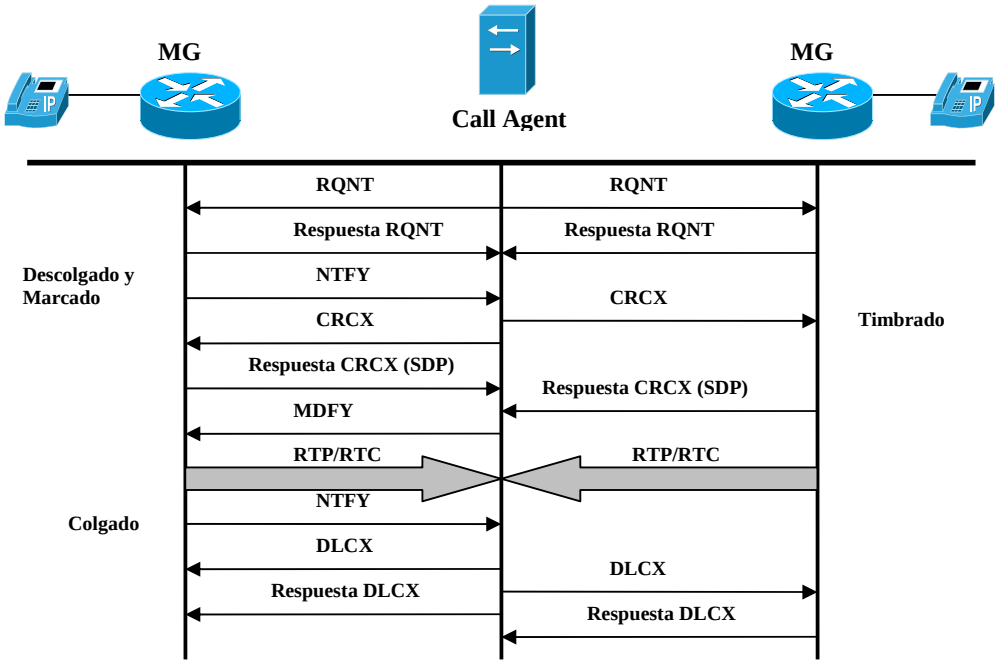


Figura 3.10 Establecimiento de una llamada MGCP

3.4 Comparación de Protocolos.

En las tablas 3.1 y 3.2 se comparan las modelos de control de llamada en arquitectura, características y servicios de H.323, SIP y MGCP.

Componentes y Servicios			
	H.323	**SIP**	**MGCP**
Componentes de control común (Señalización y control de una sesión	Gatekeeper	Servidor Proxy Servidor de Redireccionamiento, Localización, Registro.	MGC
Endpoint	Gateway Terminal	Teléfonos IP Gateway	MG Endpoint
Administración de la llamada	Gateway	Gateway Servidor Proxy	MGC
Estado de una sesión	Gateway Gatekeeper	Gateway	MGC
Direccionamiento	Gatekeeper	Servidor de Localización y Servidor de Registro.	MGC
Control de Admisión	Gatekeeper	No soportado	MGC

Tabla 3.1 Comparación de Protocolos.

Características			
	H.323	**SIP**	**MGCP**
Organismo de Estandarización	ITU	IETF	IETF
Arquitectura	Distribuida	Distribuida	Centralizada
Versión Actual	H.323v5	SIPv2.0	MGCPv10
Señalización	TCP/UDP	TCP/UDP	UDP
Soporte multada	Sí	Sí	Sí
Escalabilidad	Buena	Pobre	Moderada
Trasporte de audio	RTP	RTP	RTP
Codificación	ASN.1	Texto	Texto
Control de Transporte de audio	RTCP	RTCP	RTCP
Complejidad	Baja	Alta	Alta
Costo	Bajo	Alto	Moderado
Servicios Suplemnarios	En Endpoint o Gateway	Endpoint o Gateway	MGC

Tabla 3.2 Características de Protocolos VoIP.

En el área de las telecomunicaciones se pueden tener diferentes tipos de escenarios, recursos y necesidades de implementación en una red VoIP, dependiendo de estos puntos se puede seleccionar el protocolo más adecuado (MGCP, SIP, H.323). H.323 ha sido por largo periodo de tiempo una opción viable en VoIP por ser un protocolo maduro, escalable y adaptable a varios tipos de redes ya implementadas, este protocolo funciona correctamente en redes grandes por administrar localmente la

red, operación y mantenimiento del control de llamadas. SIP es popular por sus aplicaciones de internet, permite construir redes escalables y redundantes, proporciona mecanismos de interconexión con otros protocolos. Finalmente, MGCP nos proporciona la posibilidad de administrar redes de mayor rango por un solo dispositivo, haciendo fácil de administrar y escalable, es fácil de implementar y administrar de forma central el plan de marcación.

3.5 Protocolos de transporte

Los protocolos de transporte se encargan de asegurar que todos los datos hayan llegado intactos desde el origen al destino, cumpliendo con los requerimientos de calidad de servicio y ancho de banda adecuados. Los protocolos empleados en comunicaciones de audio y video en tiempo real y serán definidos en la RFC 1889, se define RTP (Real Time Protocol) para el intercambio de la información y RTCP (Real Time Control Protocol) para el control de dicho intercambio. Aunque la norma no lo indica explícitamente, tanto RTP como RTCP suelen emplearse sobre UDP ya que posee menor retardo que TCP, ya que no envía retransmisiones de datos, por lo que se gana velocidad a cambio de sacrificar la confiabilidad de TCP.

En una comunicación de voz sobre paquetes, cada canal de comunicaciones está compuesto por un flujo RTP y un flujo RTCP(Figura 3.11), cuyos puertos UDP se eligen independientemente en cada extremo de la comunicación, el cual deben notificarlo mutuamente utilizando algún mecanismo de señalización. El único requisito es que el puerto UDP asociado al flujo RTP sea par y el puerto UDP asociado al flujo RTCP sea el impar inmediatamente superior al del flujo RTP.

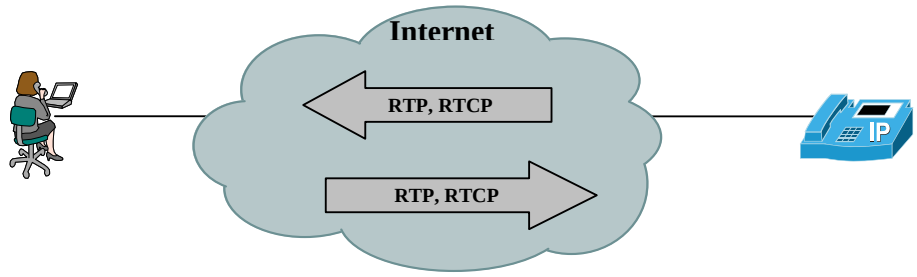


Figura 3.11 Flujo RTP/RTCP.

3.5.1 RTP

Es un protocolo de transporte de la IETF, definido en la RFC 3550 para tráfico sensible a perdidas de paquetes y retardo en la transmisión de datos. Permite comunicaciones de audio y video en tiempo real sobre redes IP. RTP no garantiza la entrega de todos los paquetes, ni la llegada de estos en el instante adecuado. La aplicación superior debe encargarse de solucionar las fallas. Suministra funciones de transporte extremo a extremo y ofrece servicios tales como identificación de tipo de carga, numeración de secuencia, timestamping (marcación del tiempo), identificación de la fuente, etc. No garantiza la entrega de tráfico en tiempo real pero si suministra los recursos para que este se entregue de manera sincronizada datos multimedia desde diferentes aplicaciones.

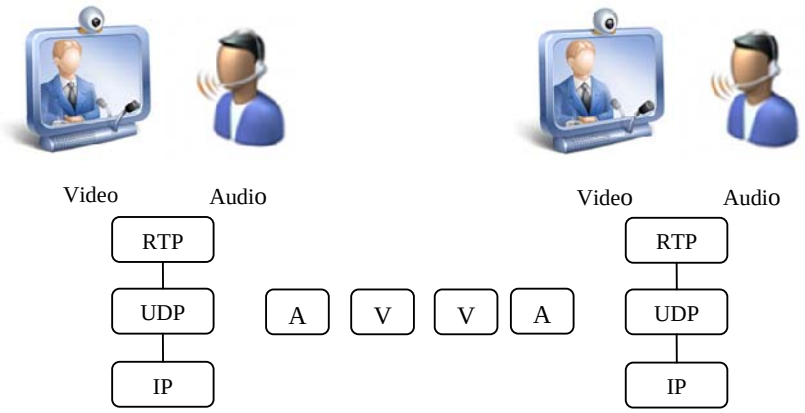


Figura 3.12 Multiplexación por RTP.

La función de RTP es multiplexar varios flujos de datos en tiempo real en un solo flujo de paquetes UDP, figura 3.12. Los paquetes son enumerados, se les asigna a cada paquete un número mayor que su antecesor. Esto es útil para la aplicación final conozca si ha fallado algún paquete o no en la transmisión. Permite identificar el tipo de información transportada, añadir marcas temporales (timestamp), números de secuencia y controlar la llegada de los paquetes. Toda esta información es utilizada por los receptores para reconstruir el flujo de paquetes que género el receptor, eliminando en la medida de lo posible los efectos de las perdidas, el retardo y el jitter.

El encabezado de RTP consiste en tres palabras de 32 bits y algunas extensiones, como se muestra en la figura 3.13.

bit offset	0-1	2	3	4-7	8	9-15	16-31
0	Version	P	X	CC	M	PT	Sequence Number
32	Timestamp						
64	SSRC identifier						
96	CSRC identifiers ...						
96+32×CC	Profile-specific extension header ID						Extension header length
128+32×CC	Extension header ...						

Figura 3.13 Encabezado RTP.

Primera palabra.

V (Versión): Campo de versión, la versión actual es la 2, ocupa 2 bits.
P (Padding): 1 bit, indica si el paquete se ha rellenado aún múltiplo de 4 bytes. El último byte de relleno indica cuantos bytes se agregaron.
X (Extensión): 1 bit. Si el bit de extensión está colocado, entonces el encabezado fijo es seguido por una extensión del encabezado.

CSRC (Conteo CSRC): 4 bit. El número de identificadores CSRC que sigue el encabezado fijo. Si la cuanta es cero, entonces la fuente de sincronización es la fuente de la carga util.
M (Marcador): 1 bit. Es un marcador específico de la aplicación, normalmente un marcador de inicio.
PT (tipo de carga): indica cual es el algoritmo de codificación que se ha utilizado.
Número de secuencia: 16 bit. El número del paquete es incrementado en uno para cada paquete enviado.

Segunda palabra.

Timestamp (Marca de tiempo). 32 bits. Refleja el instante de muestreo del primer byte en la carga útil. El valor inicial es aleatorio. Varios paquetes consecutivos pueden tener la misma marca si son lógicamente generados en el mismo tiempo, por ejemplo si son todo parte del mismo frame de video.

Tercera palabra.

Identificador de SSRC: 32 bits. Identifica la fuente de sincronización. Es un valor aleatorio que debe de llevar todos los paquetes RTP procedentes de una misma fuente de sincronización. El receptor debe agrupar todos los paquetes en el mismo SSCR para reproducirlos.
Lista CSRC. Contiene los SSRC de las fuentes que contribuyen al payload del paquete

El ancho de banda es un recurso limitado, por tal razón se requiere ahorrar este recurso por diferentes técnicas de compresión, RTP no es la excepción. En algunos casos para disminuir el flujo de datos transportados se ofrece la posibilidad de comprimir las cabeceras utilizando una versión comprimida de RTP, denominada cRTP figura 3.14. En un paquete de 40 bytes con encabezados IP/UDP/RTP se logra reducir hasta 2 a 4 bytes. Sin embargo, el principal problema es la introducción de retardo como consecuencia del proceso de compresión.

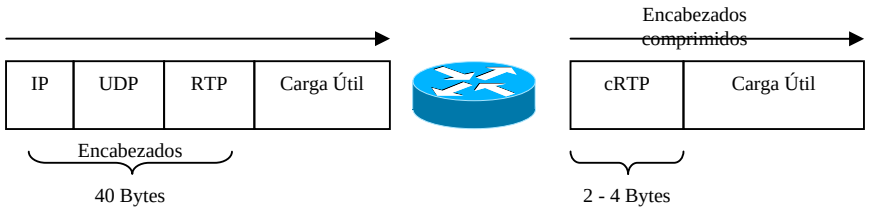


Figura 3.14 cRTP.

3.5.2 RTCP.

Es un protocolo de control definido en la RFC 3550 por la IETF, es complementario de RTP y utiliza UDP, utiliza el puerto adyacente siguiente al puerto que se utiliza para RTP. Proporciona información de control asociado al flujo de datos de una aplicación multimedia. Su función principal es informar la calidad de servicio proporcionada en una sesión RTP, se encarga de recolectar estadísticas de la conexión e información, por ejemplo los bytes enviados, paquetes enviados, paquetes perdidos, retardo o jitter, entre otros, y en base a ellos determina si la sesión puede continuar activa.

Describe el intercambio de mensajes de control relacionados con la calidad de servicio, los mensajes que se incluyen los siguientes:

Informes de Emisor (SR). Permiten al emisor activo en una sesión informar sobre estadísticas de recepción y transmisión.
Informes de Receptor (RR). Los utilizan los receptores que no son emisores para enviar estadísticas para la recepción.
Descripción de la fuente (SDES). Proporciona un identificador de nivel de transporte denominado CNAME (Canonical Name).
Goodbye(BYE). Indica el final de la participación en una sesión.
Paquetes definidos de la aplicación (APP). Usados para aplicaciones específicas.

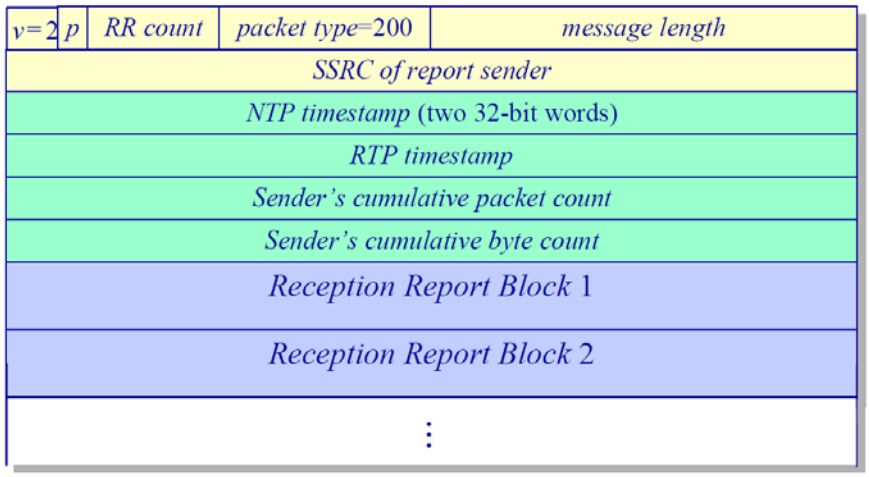


Figura 3.15 Paquete RTCP.

El encabezado del paquete de RTCP está compuesto por la Versión (2 bits), relleno (1 bit), Cuenta (5 bits), Tipo de paquete (8 bits) y la longitud del paquete (16 bits), y por último la información adicionada por cada mensaje, figura 3.15.

3.5.3 RTSP.

Es un protocolo de flujo de datos en tiempo real, definido por la IETF en el RFC2326, establece y controla uno o muchos flujos sincronizados de datos, ya sea audio o video. Actúa como un mando a distancia mediante la red de servidores multimedia. Es un protocolo no orientado a conexión, el servidor mantiene una sesión asociada a un identificador, en la mayoría de los casos usa TCP para datos de control y UDP para los datos de audio y video, aunque también puede usar TCP en caso de ser necesario. El protocolo es similar en sintaxis y operación a HTTP, emplea URLs para su transmisión, está basado en texto, permite recuperar un determinado medio de un servidor, invitar un servidor de medios a una multiconferencia y grabar una multiconferencia. Está basado en peticiones y generalmente son enviadas del cliente al servidor, el flujo de una sesión se especifica en la figura 3.16, las típicas son:

SETUP. El servidor asigna recursos y establece una sesión RTSP.
PLAY. Empieza la transmisión de datos.
PAUSE. Detiene temporalmente la transmisión.
TEARDOWN. Libera recursos y termina la sesión.

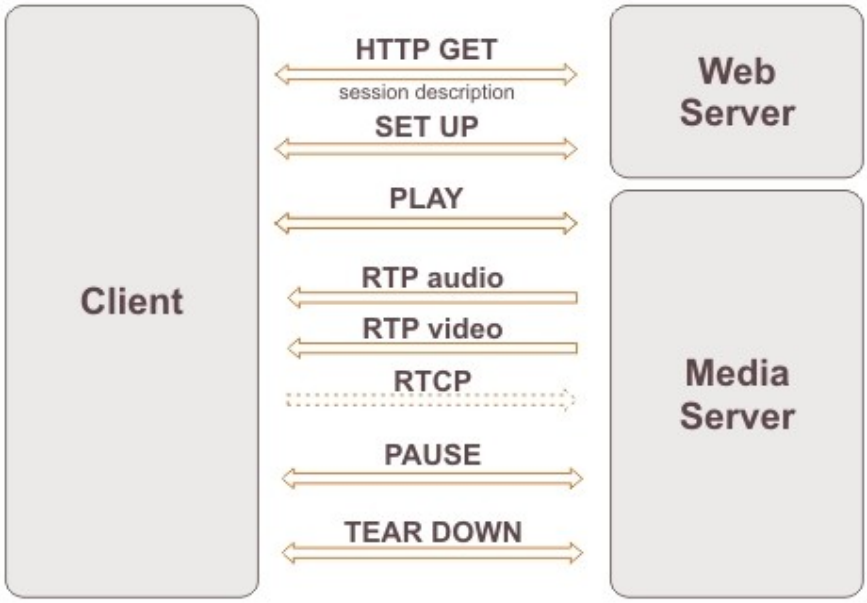


Figura 3.16 RTSP.

3.6 Arquitecturas de Red.

Las arquitecturas en una red VoIP se dividen en tres modelos que permiten la flexibilidad y capacidad de administración y control. En la redes convencionales de voz la arquitectura utilizada se basa en un equipo de conmutación central encargado de proporcionar el servicio de telefonía, los teléfonos son controlados por centrales telefónicas centralizadas. Uno de los beneficios de la tecnología VoIP es permitir a las redes ser construidas usando una arquitectura centralizada o distribuida. Estas arquitecturas permiten a las compañías construir redes caracterizadas por una administración simplificada.

3.6.1 Centralizada.

Es una arquitectura asociada a protocolos como MGCP, donde se definen tres elementos principales: MGC, MG y un enlace a través de Internet, el cual es proporcionado por empresas prestadoras del servicio de Internet, en México es el caso de UNINET de Telmex. En una topología de red centralizada, como se puede ver en la figura 3.17, el componente de procesamiento de las llamadas suele estar ubicado en un punto central o más grande. Este componente ofrece el servicio de administración y control a todos los teléfonos conectados a esa red.

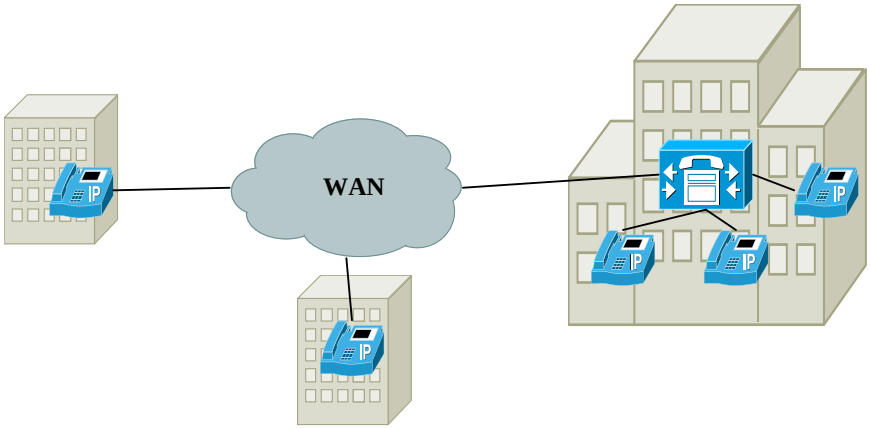


Figura 3.17 Esquema Centralizado

En un esquema centralizado uno de los sitios almacena una única instancia el componente de procesamiento de llamada, y el reste de los sitios se conectan a él a través de la red IP existente entre ellos. Las aplicaciones como el correo de voz o IVRs son centralizadas, reduciendo el costo de operación y administración. Una desventaja es cuando el enlace WAN falla entre el sitio central y los remotos, ya que los teléfonos no podrán hacer llamadas.

3.6.2 Distribuida.

Principalmente asociada con los protocolos H.323 y SIP. Este esquema es aplicado principalmente en una red con varias localizaciones geográficas, es posible que cada sitio pueda controlar las llamadas y las terminales. La inteligencia de la red es distribuida, es decir cada punto establece, define características, encamina, procesa, factura y cualquier otro manejo de las llamadas. En estos entornos, cada sitio dispone de un servidor de procesamiento de llamadas, como se muestra en la figura 3.18.

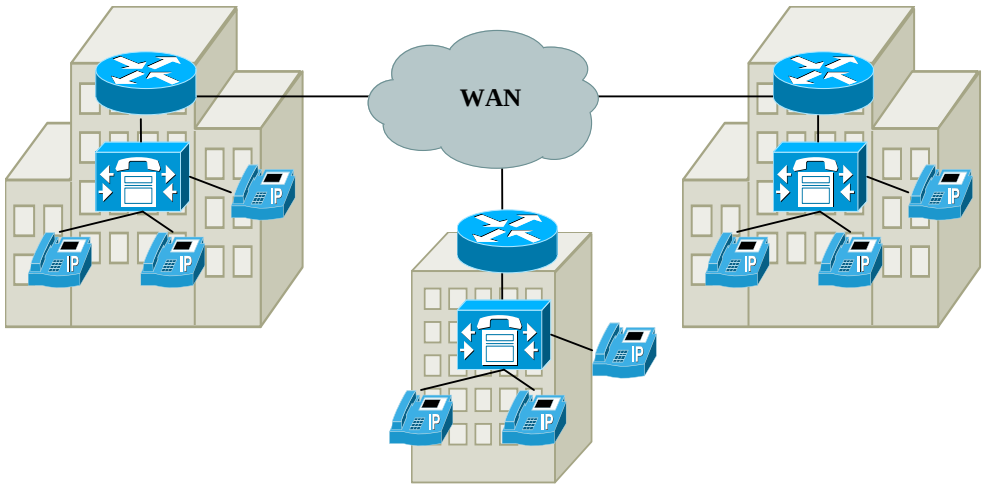


Figura 3.18 Esquema Distribuido.

El tipo de arquitectura de red tiene redundancia implícita, ya que cada sitio cuenta con un componente de procesamiento de llamadas. El modelo distribuido también lleva implícito la escalabilidad en la capacidad de las llamadas y el balanceo de tráfico.

3.3.3 Híbrida.

En la realidad la mayoría de las redes imposibilita un modelo totalmente centralizado o distribuido. Por el contrario muchas redes son un hibrido de ambos métodos. Una red de gran extensión suele contar con un importante número de sitios remotos que no son lo suficientemente grandes como para invertir económicamente en un procesador de llamadas. Las restricciones de fiabilidad y disponibilidad también hacen que una red netamente centralizada no sea una lección acertada, ya que el fallo del único componente de procesamiento significa la caída completa de la red. Un pequeño número de servidores de procesamiento de llamadas repartidos por los enlaces fundamentales ofrece una flexibilidad, cobertura y escalabilidad mucho mayor en redes grandes. Este tipo de red híbrida incluye las siguientes características de cada uno de los modelos de procesamiento de llamada individual:

Centralizado. Los sitios remotos obtienen los servicios de procesamiento de llamada a trabes de la red de un procesador central.

Distribuido. Varios sitios disponen de servidores de procesamiento de llamada.

4

Fundamentos de IPv6

El protocolo actual de Internet fue normalizado en septiembre de 1981 por el programa de Internet de la DARPA (Defense Advanced Research Projects Agency) del Departamento de Defensa de USA, diseñado inicialmente para tener sistemas interconectados de redes de comunicación de computadoras ubicadas en distintas localidades, su propósito era enviar paquetes de datos en cualquier momento, bajo cualesquiera condiciones y desde un punto a otro. Durante esa época las computadoras eran conectadas unas a otras, lo que conocemos ahora como una red local, pero con el crecimiento de esta tecnología fue creciendo el número de redes locales ubicadas en diferente localidad, creando islas separadas entre sí. La palabra Internet es el resultado de la unión de dos términos: Inter, que hace referencia a conexión y Net palabra inglesa con traducción red, que significa interconexión de redes. En un principio el protocolo de Internet tenía un uso militar pero usuarios de universidades, residenciales y empresariales fueron incluidos posteriormente. El Internet como red de información mundial es el resultado del uso práctico del protocolo IP. La versión actual del protocolo de Internet es la 4 y forma parte del modelo TCP/IP.

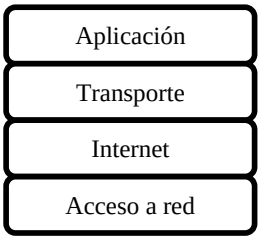


Figura 4.1 Modelo TCP/IP

Para que dos sistemas cualesquiera se comuniquen, deben de ser capaces de identificarse y localizarse entre sí. Una dirección IP es un identificador que esta asignada a cada dispositivo conectado a una red IP, el problema consiste si un dispositivo puede tener un identificador dedicado, permanente y globalmente único. Por una fácil comprensión humana las direcciones son representadas por una cadena de números separados por puntos, por ejemplo: 192.124.145.10. Inicialmente se creía que con ese número de identificadores sería suficiente para abarcar cualquier necesidad posterior de conexión a Internet, actualmente las redes de telecomunicaciones crecen cada vez más rápido conforme servicios de red convergen entre sí, tal es el caso de la telefonía, video y transmisión de datos, estos servicios requieren acceso alambrico e inalámbrico y conexión permanente, teniendo la necesidad de siempre estar localizables.

En 1992, la normalización de una nueva generación del Protocolo de Internet, con frecuencia conocido como IPng, fue soportada por el Grupo de ingeniería de Internet (IETF), definida en la RFC 2460 y con el fin de cubrir las limitaciones del protocolo de IPv4. IPng se conoce ahora como el Protocolo de Internet versión 6 y será el tema a desarrollar en el presente apartado.

4.1 Limitaciones de IPv4.

La apertura comercial del Internet ha provocado un crecimiento exponencial en la demanda de usuarios que se desean conectar a la red, cada dispositivo conectado requiere una dirección IP para poder ser alcanzado desde cualquier parte del mundo.

Actualmente no es suficiente el espacio de direcciones a 32 bits, lo que representa 4.2 millones de direcciones, debido a nuevas tecnologías introducidas al mercado, como es el caso de la conexión a Internet por medio de XDSL, el agotamiento de direcciones IP esta por alcanzarse, según predicciones realizadas por la IANA el primer semestre del 2012 todo el pool de direcciones libres habrá sido agotado. Este tema se ha ido controlando con técnicas que originalmente no se tenían diseñadas en el protocolo de Internet inicial, tales como el NAT.

Los diseñadores de Internet imaginaron que las redes se construirían de diferentes tamaños, dependiendo del número de dispositivo en la red, por lo que dividieron las direcciones IP en clases A, B, C, D con el fin de definir la dimensión de una red, sin embargo la asignación de direcciones es ineficaz. Las direcciones de Clase A y Clase B representan el 75% del espacio de direcciones, las direcciones Clase C son más numerosas que las direcciones de Clase A y Clase B, tal como se observan en la tabla 4.1.

Clase de dirección	Numero de Redes	Nodos por Red
A	126	16 777 216
B	16 384	65 535
C	2 097 152	254
D	-	-

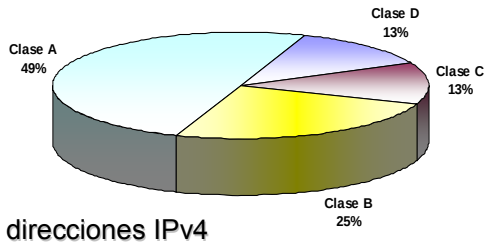


Tabla 4.1 Numero de direcciones IPv4

Algunas organizaciones con un gran número de nodos adquieren una dirección IP clase A, pero algunas empresas pequeñas deben de adquirir una dirección clase B o C desperdiciando algunas direcciones IP. Por desgracia, las direcciones C tienes solo 254 nodos, lo cual no reúne las necesidades de grandes empresas que no pueden adquirir una dirección clase A con mayor costo.

El incremento rápido y sustancial del tamaño de las tablas de enrutamiento de Internet debido al crecimiento de este último, es uno de los problemas por el cual el procesamiento de los enrutadores dentro de la nube de Internet se ha quedado obsoleto. Debido a la multitud de nuevas aplicaciones en las que IPv4 es utilizado, ha sido necesario agregar nuevas funcionalidades al protocolo básico, lo que genera complicaciones en su escalabilidad, entre las características que han sido añadidas se encuentran la Calidad de Servicio (QoS), Seguridad (IPsec) y movilidad. En respuesta de estos problemas se ha creado el nuevo protocolo de Internet.

4.2 Desarrollo de IPv6

A comienzos de 1992 en la reunión de la Sociedad de Internet en Kobe, Japón, circulaban varios mecanismos para mejorar e intentar suplir los defectos del protocolo de Internet versión 4, la IETF anunció el llamado para la creación de grupos de trabajo de IP de próxima generación, el consejo fue llamado IPng. La comunidad del Internet había desarrollado cuatro propuestas diferentes que eran: CNAT, IP Encaps, Nimrod y Simple CLNP. Después, aparecieron tres propuestas más: PIP (The P Internet Protocol), SIP (The Simple Internet Protocol) y el TP/IX. En la primavera de 1992 el Simple CLNP se desarrolló en TUBA (TCP and UDP with Bigger Addresses) definido en el RFC 1347, 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) definido en el RFC1752. Casi al mismo tiempo el grupo de trabajo TP/IX cambió su nombre por el de CATNIP (Common Architecture for the Internet) definido en el RFC1707. La propuesta recomendada fue SIPP con un direccionamiento de 128 bits, su principal autor fue Steve Deering. En 1996 se publica el RFCs2460 definiendo IPv6. Este nuevo protocolo es la versión 6, la versión 5 no pudo ser usado debido a su anterior asignación a un protocolo experimental desarrollado en paralelo al IP.

4.3 Beneficios de IPv6

El protocolo IPv6 resuelve los problemas de IPv4 y proporciona nuevos beneficios: nuevo formato de encabezado, mayor espacio de direccionamiento, alcance global al tener una dirección globalmente única, escalabilidad, niveles de direccionamiento jerárquico, direcciones múltiples, autoconfiguración, al transición a IPv6 es transparente por los usuarios por la técnica de renumeración, uso de multicast, eficiencia del encabezado, diferenciación de tráfico, flexibilidad, movilidad y seguridad. La siguiente parte de este apartado examina algunas de estas funciones y revisa las ventajas sobre el protocolo anterior.

Los criterios que sea han utilizado para el desarrollo de IPv6 han sido primordiales para obtener un protocolo sencillo y al mismo tiempo consistente y escalable. El protocolo puede ser soportado por las plataformas existentes y permite una evolución gradual y sencilla de IPv4 a IPv6.

4.3.1 Mayor espacio de direccionamiento

La disponibilidad de casi un número ilimitado de direcciones IP es el mayor forzamiento de implementar redes IPv6. Comparado a IPv4, IPv6 incrementa el número de bits en un factor de 4, de 32 bits a 128 bits. Los 128 bits proporcionan 4,294,967,296 nodos posibles, lo que representa aproximadamente 5 x 1028 direcciones por habitante en el mundo de acuerdo a la población hasta 2008. Sin embargo como en cualquier esquema de direccionamiento, como es el caso de IPv4 y sistemas de telefonía, no todas las direcciones pueden ser usada, pero habrá las suficientes para cubrir cualquier tipo de uso. El incremento del número de bits también representa el incremento en el tamaño de la cabecera del paquete IP. Debido a que cada IP contiene una dirección fuente y destino, el tamaño de los campos de cabecera para IPv4 es 64 bits y 256 para IPv6.

Comparando el modelo de referencia OSI de IPv4 a IPv6, en el protocolo nuevo de Internet solo representa un cambio en la capa 3. Las demás capas son ligeramente modificadas. Este fue una importante consideración durante la plantación de IPv6. Las otras capas del modelo OSI son las mismas, lo que significa que protocolo como TCP y UDP, para el caso de transporte de paquetes de voz, son compatibles sobre IPv6.

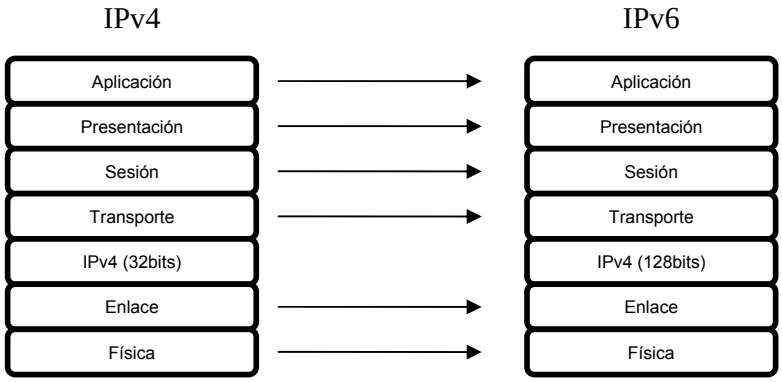


Figura 4.2 Protocolo IPv4 vs IPv6

4.3.2 Alcance Global.

El problema importante por el cual inicio IPv6 fue el agotamiento de direcciones, IPv6 proporciona una única dirección global a cada dispositivo conectado a la Internet. Usando un espacio de direccionamiento mayor a IPv4, Ipv6 permite el uso de una dirección única y accesible para cada casi tipo de dispositivo: computadoras, Teléfonos, Fax sobre IP, Televisión, cámaras, PDAs, celulares, dispositivos 802.11b, vehículos y redes caseras.

Intentar acceder a estos dispositivos de forma global con el actual direccionamiento es prácticamente imposible. Tener una dirección única para cada dispositivo permitiría ser alcanzado desde cualquier punto, lo cual no es posible con técnicas actuales como NAT. La accesibilidad punto a punto es especialmente importante para la seguridad de llamadas VoIP.

4.3.3 Niveles de Direccionamiento Jerárquico

Un espacio de direccionamiento mucho más grande permite el uso de niveles de jerarquía dentro del espacio de direccionamiento, como se muestra en la figura siguiente cada nivel ayuda a agregar su espacio IP de direccionamiento y mejora la función de asignación. Los proveedores de Internet y Organizaciones pueden tener un espacio de direcciones jerárquico y administrado.

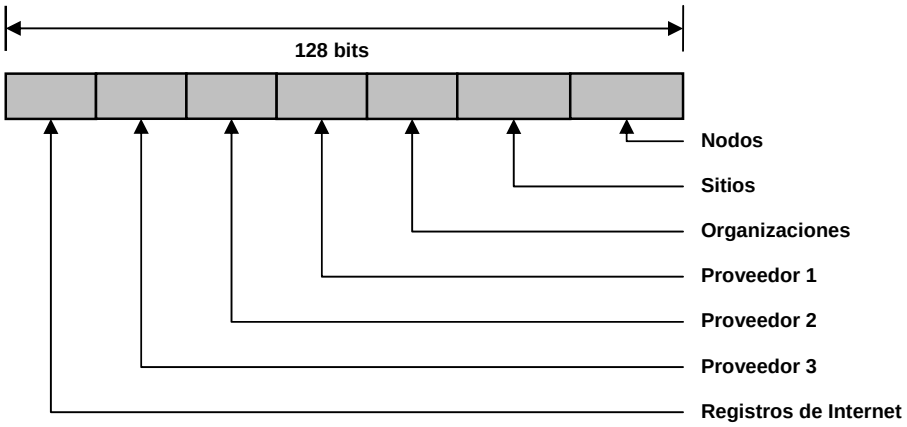


Figura 4.3 Direccionamiento Jerárquico.

El gran espacio de direccionamiento de IPv6 permite la asignación de grandes bloques de direcciones a los ISP (Internet Service Providers) y a otras organizaciones, esta asignación permite a los ISPs agregar un prefijo a todos sus clientes y anunciarlo a Internet 6 como una sola red. El uso de múltiples niveles de jerarquía ayuda a agregar el tráfico en ese nivel y a realizar la asignación de direcciones en un formato jerárquico.

Usando niveles múltiples en la jerarquía proporciona flexibilidad y nuevas funcionalidades al protocolo. Una arquitectura de direccionamiento flexible es la llave de éxito para un protocolo de red. En la versión 4 de IP, el pequeño espacio de direccionamiento de 32 bits es una importante limitación que no permite el uso de varios niveles de jerarquía. Una arquitectura de red jerárquica permite agregar prefijos de redes de forma más eficiente y ayuda a reducir rutas dentro de Internet.

4.3.4 Multihoming

Es una técnica que permite a una red estar conectada a dos o más ISPs incrementando la confiabilidad, redundancia, la tolerancia a fallos y permite balanceo de tráfico sobre la conexión a Internet, es complicado conectar a una red con dos proveedores en IPv4. Una forma para tener multihoming es tener un espacio de direccionamiento independiente de registros regionales de Internet, pero no es económicamente viable, y se anunciarían dos redes distintas, la manera de tener multihoming es anunciar el mismo prefijo de red a Internet, sin embargo en la tabla de ruteo global rompería con cualquier tipo de agregación. Las capacidades y el uso de esta técnica se encuentran bajo estudio, sin embargo se ha creado un protocolo llamado Shim6, documentado en el RFC 5533, donde los nodos que emplean este protocolo usan múltiples prefijos de direcciones IPv6 gracias al gran espacio de direccionamiento.

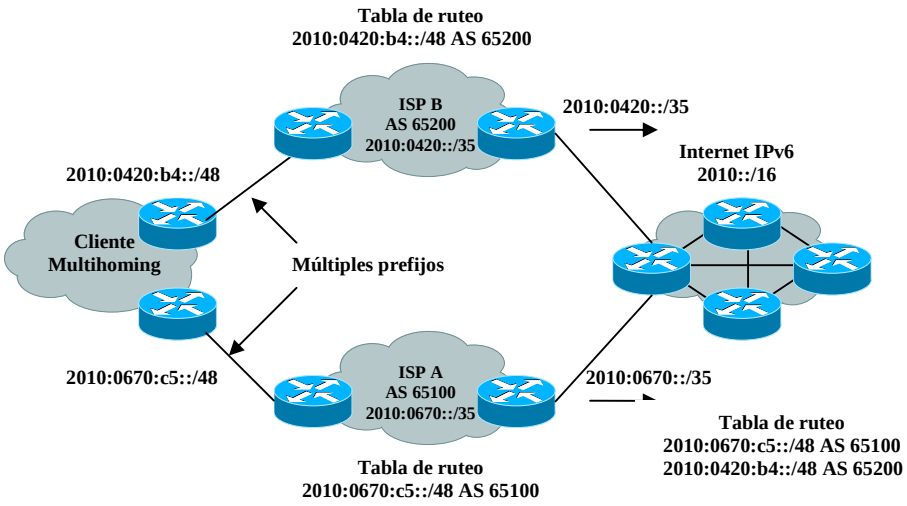


Figura 4.4 Multihoming.

El multihoming es posible en IPv4 pero el tamaño de la tabla de enrutamiento global se incrementa notablemente, porque el mismo prefijo puede ser anunciado por dos diferentes sistemas autónomos, una de las metas de IPv6 es mantener esta tabla lo más compacta posible.

El concepto de múltiples direcciones implica que cada interface de red pueda tener múltiples direcciones unicast globales en mismo intervalo de tiempo. Teniendo direcciones múltiples los nodos deben de seleccionar que conexión a Internet deben de usar, la selección de origen es un mecanismo por el cual los nodos selección o son forzados un prefijo de red cuando se tienen varios disponibles.

4.3.5 Auto configuración

La autoconfiguración es nueva función en IPv6 y está documentada en el RFC 2462, también llamada descubrimiento automático. La autoconfiguración evita la configuración manual de los nodos, gracias al gran espacio de direccionamiento el nodo puede tener una dirección única para cada una de sus interfaces, asumiendo que cada interface cuenta con su identificador único de dirección en capa 2, su dirección MAC. Como se muestra en la figura 4.4, un router IPv6 sobre un mismo enlace local manda información del tipo de red como es el prefijo de red y el router de default, todos los nodos conectados a su interface escuchan esta información y pueden configurar esta información por ellos mismos, incluyendo la dirección IPv6, esta función será de gran importancia para la movilidad en teléfonos IP.

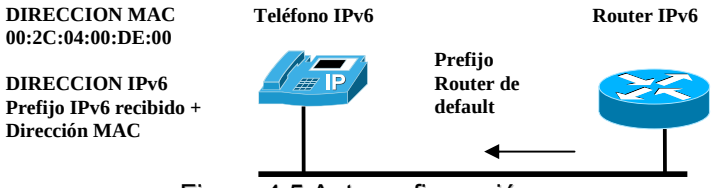


Figura 4.5 Autoconfiguración.

Los 128 bits de direccionamiento por nodo proporcionados por la técnica de autoconfiguración aseguran una dirección única, porque los 48 bits de la direccion MAC es una combinación 24 del vendedor del producto y 24 bits por cada interfase.

La autoconfiguración permite el Plug and Play, conocida como PnP, permite conectar a los dispositivos a la red sin ninguna configuración o los servidores tales como servidores del DHCP. Esto es una característica dominante para permitir el despliegue de nuevos dispositivos en mismo un gran escala en el Internet tal como teléfonos celulares, dispositivos inalámbricos, aparatos electrodomésticos, y redes caseras. La frase plug-and-play se traduce como enchufar y usar. No obstante, esta tecnología en la mayoría de los casos se describe mejor por la frase apagar, enchufar, encender y listo.

4.3.6 Renumeración

La renumeración es una facilidad que proporciona el nuevo protocolo de internet, está definida en el RFC 2894 y RFC 4192. La renumeración o de cambio de numeración de red es el cambio de un prefijo de red existente a u nuevo prefijo en una red. Al igual que la configuración de los nodos de red, este método puede utilizar mecanismos como el DHCP con el uso de direcciones IPv6 que expiran en un periodo de tiempo. En IPv6 las redes pueden ser renumeradas por medio de routers que especifican un intervalo de expiración para los prefijos de red cuando se hace la autoconfiguración; más tarde, pueden enviar un nuevo prefijo para pedirle a los dispositivos de la red que renueven su dirección IP. Los dispositivos pueden mantener el viejo prefijo durante algún tiempo y después moverse al nuevo prefijo que definirá el segmento de red.

4.3.7 Uso de Multicast

Una de las características de IPv6 es que no utiliza la difusión por mensajes broadcast. Las funciones previamente soportadas por broadcast de IPv4 como el descubrimiento de dispositivos ahora son soportadas por mensajes de difusión multicast de IPv6, sin embargo la multidifusión es ligeramente distinta en IPv6. Un paquete multicast, por ejemplo un stream de video o audio, no está dirigido necesariamente a una red o subred, concepto que no existe en IPv6, sino a un grupo de nodos predefinido compuesto por cualquier equipo en cualquier parte de la red.

El nodo origen emite su paquete a una dirección de multidifusión como si se tratase de cualquier otro paquete. Dicho paquete es procesado por diversos dispositivos de ruteo. Estos ruteadores utilizan una tabla de correspondencia que asocia cada dirección de multidifusión con un conjunto de direcciones reales de nodos. Una vez determinadas dichas direcciones, retransmite una copia del paquete a cada uno de los nodos interesados.

Las direcciones de multidifusión comienzan por FF00 (en hexadecimal). A diferencia de IPv4, la implementación de la multidifusión es obligatoria para los roteadores. Su aplicación práctica está en la videoconferencia y telefonía. La multidifusión mejora la eficacia de una red limitando las peticiones broadcast a un número más pequeño de nodos. Así, el multicast IPv6 previene los problemas causados por las tormentas broadcast en las redes IPv4.

4.3.8 Eficiencia del encabezado.

Aunque el incremento en el número de bits en el espacio de direcciones de IPv6 resulto un incremento en el tamaño de la cabecera, el formato de la cabecera del paquete de IPv6 es más simple que IPv4. El tamaño básico del encabezado de IPv4 es solo 20 octetos, pero la longitud variable del campo de opciones añade el resto del tamaño del paquete. El paquete IPv6 tiene un tamaño fijo de 40 octetos. Aunque 6 de los 12 campos de IPv4 han sido removidos in IPv6, algunos campos de IPv4 han sido conservados con nombres modificados, y algunos nuevos campos han sido adicionados para mejor la eficiencia e introducir nuevas funciones.

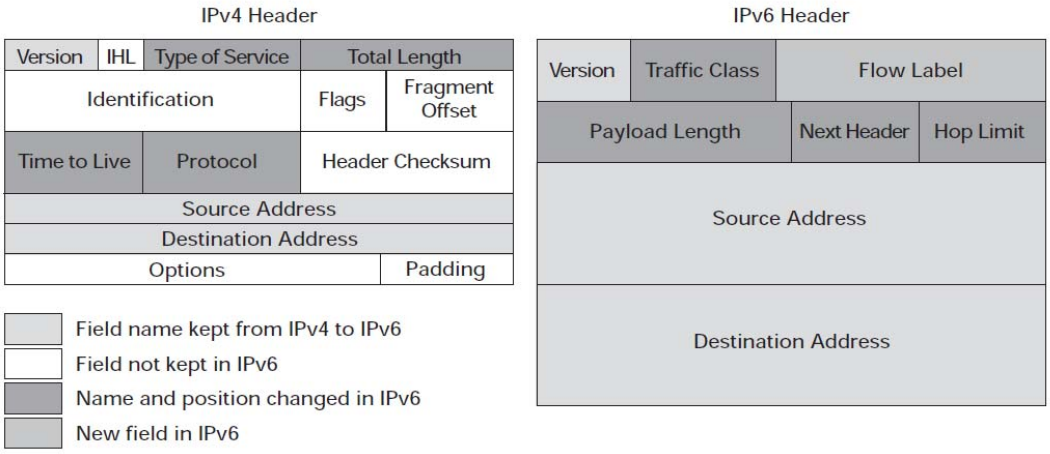


Figura 4.6 Eficiencia del encabezado.

La fragmentación es ahora manejada de forma distinta y no requiere campos en el encabezado IP. Los routers no hacen más la fragmentación en IPv6, reduciendo el alto procesamiento que consume este proceso en cada dispositivo de red. Debido a que le campo de comprobación de errores ha sido eliminado y los routers a los largo de una trayectoria IPv6 no necesitan recalcular los errores producidos en el camino, la eficiencia en el encaminamiento en IPv6 ha mejora notablemente. La detección de errores será labor de la capa superior e inferior, tecnologías de acceso al medio y de transporte. En redes de la próxima generación, la fragmentación es manejada por el dispositivo fuente con la ayuda del protocolo MTU.

Los campos de Opciones han cambiado en IPv6 con respecto a IPv4, ahora son administrados por un campo de extensión de opciones. Además de un número menor de campos, la cabecera de 64 bits permite un mejor procesamiento en los actuales equipos de red.

Un factor de mejora de la eficiencia de IPV6 a resaltar es el uso de etiquetas de flujo. En estas etiquetas se puede colocar cualquier requerimiento referente a un servicio especial, tal como prioridad, retardo o ancho de banda. Todos los paquetes que estén en secuencia llevan los mismos detalles de esta información en la etiqueta de flujo a fin de asegurar el tipo de servicio que ellos necesitan de los routers intermedios. Este campo será utilizado por aplicaciones de telefonía IPv6 con el fin de proporcionar una calidad en la transmisión de paquetes de voz sobre Internet.

En IPv4 el campo de opciones se limita a 40 bytes, pero en IPv6 el tamaño puede ser arbitrario, las opciones se colocan en encabezados de extensión independientes que se ubican entre el encabezado de IPv6 y el encabezado de capa de transporte de un paquete. Ningún ruteador procesa ni examina la mayoría de los encabezados de extensión de IPv6 durante el recorrido de distribución del paquete

hasta que éste llega a su destino. En IPv4, la presencia de cualquier opción hace que el enrutador examine todas las opciones, pero en IPv6 la memoria utilizada para este proceso puede ser utilizada para distintos fines. Para mejorar el rendimiento al controlar los encabezados de opciones, así como el protocolo de transporte que va después, las opciones de IPv6 siempre son un múltiplo entero de 8 octetos. El múltiplo entero de 8 octetos mantiene la alineación de los encabezados subsiguientes.

4.3.9 Movilidad

La movilidad es una característica altamente importante y deseable para compañías, organizaciones y empleados quienes requieren estar conectados a su correo, al Internet o a la Intranet. Mobile IPv6 es un estándar de la IETF permitiendo a los dispositivos móviles desplazarse sin perder la conexión existente. Actualmente cuando un dispositivo se desplaza viajando por diferentes redes (roaming), cada una de las redes por las que se mueve tiene un identificador de red distinto, proporcionando una dirección IP nueva en cada red, por lo que el usuario no puede mantener una sesión de aplicación abierta durante su movimiento. Lo que implicaría para una sesión de VoIP que se cortara la comunicación.

Mobile IPv6 es una solución que requiere una infraestructura adicional, conocida como Home Agent, diseñado para transmitir paquetes entre el nodo móvil y su red origen. El nodo móvil tiene asignada una dirección IP pública en la red origen que utilizará como identificador invariante para establecer todas las conexiones de transporte y comunicarse con otros nodos. Cuando el nodo móvil cambia su punto de conexión a la red actualiza a su agente enviándole la nueva dirección disponible, de modo que éste puede interceptar los datagramas enviados al nodo móvil y retransmitírselos.

Para el uso de Mobile IPv6 se requieren los siguientes elementos: a) Mobile Node, es el dispositivo que se encuentra en movimiento; b) Home Agent, es el encargado de reenviar los paquetes al Mobile node; y c) El Nodo correspondiente, es un nodo que se encuentra en cualquier punto de Internet y donde se encuentra el Mobile node. El funcionamiento básico se muestra en la figura 4.5, cuando el dispositivo móvil se encuentra en una red visitada envía un mensaje de señalización para notificar su ubicación, es decir envía su dirección IPv6 que se tiene en ese momento, el Home Agente mantiene el registro de la dirección actual con la dirección origen. Cuando el nodo correspondiente debe transmitir o recibir un paquete, el Home Agent actúa como puesta de enlace entre ambos dispositivos.

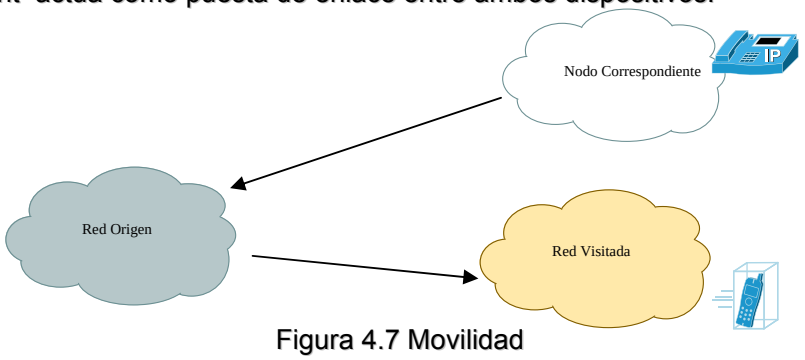


Figura 4.7 Movilidad

4.3.10 Seguridad

Mientras el uso de IPsec es opcional en protocolo de Internet versión 4, para la versión 6 se incluye explícitamente la posibilidad de usarlo, por lo tanto los diseñadores de red pueden habilitar IPsec en cada dispositivo de la red, haciendo la red más segura. IPv6 proporciona encabezados de extensión en seguridad, haciendo fácil de implementar la autentificación, la integridad y confidencialidad a las comunicaciones extremo a extremo, encriptación y establecimiento de VPNs. Debido a que IPv6 ofrece una dirección global y seguridad, también ofrece servicios de seguridad como control de acceso y la integridad de datos.

IPsec es un conjunto de protocolos abiertos que tienen como fin proporcionar seguridad en las comunicaciones de la capa de red del modelo OSI (a la que pertenece el protocolo IPv6), y de ese modo, a todos los protocolos de capas superiores. IPv6 habilita la posibilidad de usar IPsec, y no los mecanismos de cifrado y autenticación propios de IPsec.

Por el momento, el número de problemas de seguridad y ataques sobre IPv6 es pequeño debido a que no está desplegado aún a gran escala. Pero, se espera que la tendencia cambie a medida que los operadores y proveedores de contenidos lo implementen en sus redes y servicios. Los principales aspectos relacionados con la seguridad del protocolo que se debe de tener en cuenta son de Aspectos técnicos, consideraciones de gestión y estructura o características propias del protocolo.

4.4 Encabezado IPv6.

El encabezado de IPv6 es más simple y eficiente que IPv4, lo que ayuda a procesar de forma más rápida los paquetes de IPv6 en los dispositivos de red. Tal y como se define por la IETF en el RFC 2460, un paquete de Internet versión 6 consiste principalmente de una cabecera y extensiones de cabecera, como se muestra en la figura 4.6.

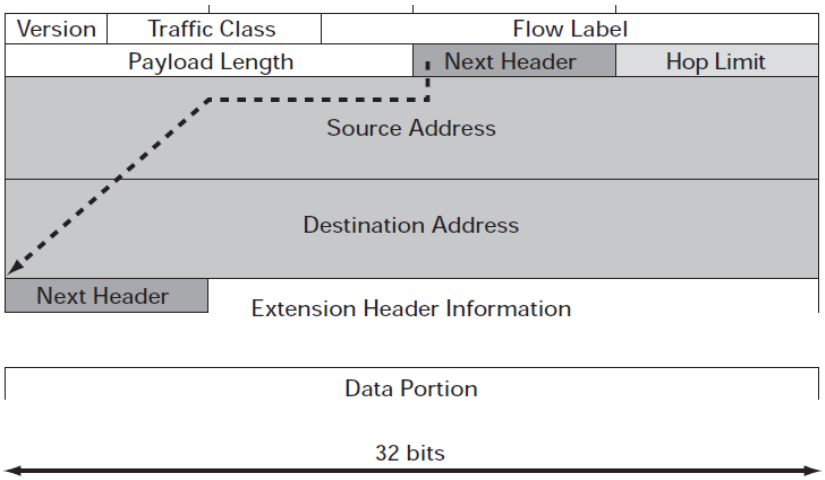


Figura 4.8 Encabezado IPv6.

La cabecera se compone por los siguientes campos:

Versión: Es un campo de 4 bits de largo e identifica la versión del protocolo, para este caso la versión 6.

Traffic Class. Este campo tiene 8 bits de largo y reemplaza el campo de tipo de servicio de IPv4, también denominado Prioridad o simplemente clase, facilita la manipulación de datos en tiempo real y algún otro tipo de datos que requieran un tratamiento especial, en los nodos origen y los nodos de reenvío permite identificar y distinguir entre diferentes clases o prioridades de paquetes de datos.

Los siguientes requerimientos generales aplican a este campo:

- ➔ Para paquetes que son originados en un nodo por un protocolo de capa más alta, ese protocolo de capa más alta especificaría el valor de los bits del campo Traffic Class, el valor por default es cero.

- ➔ Nodos que soportan una función particular que usa bits de Traffic Class pueden cambiar los valores de los bits en paquetes que ellos originan, reenvían o reciban, como sea especifico en ese uso. Sin un nodo no soporta esa función particular, no debe cambiar ninguno de los bits de traffic class.

- ➔ Los protocolos de capa más alta no deben asumir que los valores de los bits de Traffic Class en un paquete recibido son los mismos valores que fueron originalmente transmitidos.

Se asignan prioridades de 0 a 7 a fuentes que pueden disminuir su velocidad en caso de congestión. Se asignan valores de 8 a 15 al tráfico en tiempo real (datos de audio y video incluidos) en donde la velocidad es constante.

Flow Label. El campo de Flow Label es de 20 bits, y puede ser usado por un nodo para solicitar un manejo especial para ciertos paquetes, como es el caso de tráfico en tiempo real. Todos los paquetes pertenecientes al mismo flujo deben contener la misma dirección fuente, dirección destino y el mismo Flow label.

EL RFC 1809, “Usando el campo Flow Label en IPv6”, describe algunas de las características de este campo. El flow label es un número entre el 1 y el FFFFFH (donde H denota notación hexadecimal), la cual es elegida de forma seudo aleatoria y uniforme, este número es utilizado como una clave hash para buscar el estado asociado con el flujo, el cual es único cuando se combina con la dirección de la fuente. El cero se reserva para decir que no se utiliza este campo o bien dispositivos que no soportan estas funciones.

Payload length. Es un entero no asignado de 16 bits que indica la longitud en octetos de la parte de datos del paquete. Los encabezados de extensión opcional son considerados parte de la carga, junto con cualquier protocolo de capa más alta, como TCP, UDP, etc.

La carga útil del paquete puede tener un tamaño de hasta 64 KB en modo normal, o mayor con una opción de carga jumbo (jumbo payload) en el encabezado opcional Hop-By-Hop, para indicar una carga jumbo, el valor de Payload Length está fijado en cero.

Next Header. Tiene 8 bits de longitud y determina el tipo de información siguiente del paquete IPv6, si es que existe. Si en cambio no existiera ningún otro encabezamiento el campo identifica el protocolo de la capa superior de transporte (es

decir, TCP o UDP). En este caso, la identificación es la misma que tenía el campo Protocolo en el IP tradicional. La tabla 4.2 muestra algunos ejemplos del siguiente encabezado.

Valor	Encabezado
0	Opciones de Hop-by-hop
1	ICMPv4
4	IP en IP (encapsulación)
6	TCP
17	UDP
43	Ruteo
44	Fragmentación
50	Encapsulación de seguridad en la carga útil
51	Autentificación
58	ICMPv6
59	Ninguna
60	Opciones de Destino

Tabla 4.2 Next Header.

Un paquete IPv6, que se compone en un encabezado más la carga útil, puede consistir de cero, uno o más encabezados de extensión. Los encabezados de extensión se encuentran entre el encabezado de IPv6 y el encabezado del protocolo de capa superior. Cada encabezado de extensión es identificado por el campo de next header en el encabezado precedente.

Los encabezados de extensión son examinados o procesados solamente por el nodo identificado en el campo de dirección destinación del encabezado de IPv6. Si la dirección en el campo de dirección de destinación es una dirección del tipo multicast, los encabezados de extensión son examinados y procesados por todos los nodos que pertenecen a ese grupo multicast, como es el caso de audio o video conferencias en transmisión de paquetes en tiempo real. Hay una excepción a la regla que solamente el nodo destino procesara el encabezado de extensión. Si el encabezado de extensión es un encabezado de Opción Hop-by-Hop, la información es examinada y procesada por cada nodo a lo largo de la trayectoria del paquete.

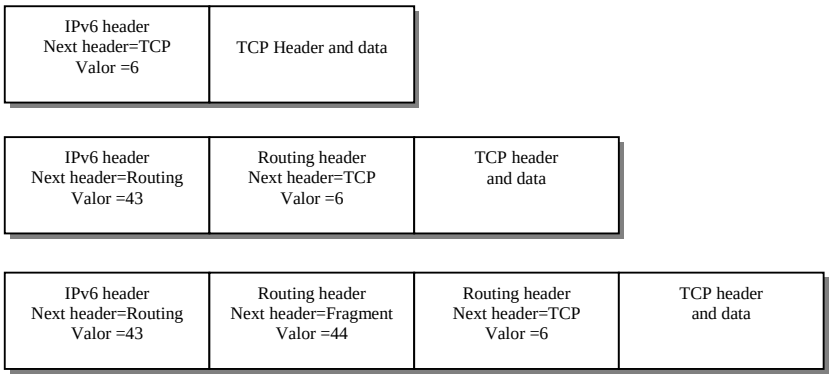


Figura 4.9 Uso del encabezado siguiente.

Hop Limit. Identifica el número de segmentos de red, también conocidos como enlaces o subredes, sobre el cual el paquete de IPv6 debe de ser transmitido antes de ser descartado. Es un campo de 8 bits y va decreciendo en 1 por cada nodo que reenvía el paquete, cuando la cuenta llega a cero es cuando el paquete es descartado

y se retorna un mensaje de error. Este campo es manipulado por cada nodo, también se utiliza para evitar la circulación indefinida de paquetes por una red, especialmente en las de cierta complejidad. Este campo reemplaza el campo TTL de IPv4, con la diferencia que en lugar de especificar tiempos en segundos, ahora se va contando el número de saltos

Source Address. Es un campo de 128 bits o de 16 octetos que identifica en nodo origen del paquete IPv6. Se define ampliamente en el RFC 2373.

Destination Address. Es un campo de 128 bits o de 16 octetos que identifica en nodo destino del paquete IPv6. Se define ampliamente en el RFC 2373.

Extension Header. Las opciones de IPv6 se colocan en encabezados de extensión independientes que se ubican entre el encabezado de IPv6 y el encabezado de capa de transporte de un paquete. Ningún dispositivo de red de capa 3 procesa ni examina la mayoría de los encabezados de extensión de IPv6 durante el recorrido de distribución del paquete hasta que éste llega a su destino. Este diseño simplifica el encabezado existente de IPv4 colocando muchos de los campos existentes en encabezados opcionales, la presencia de cualquier opción hace que el enrutador examine todas las opciones, sin embargo en IPv6 solo en nodo destino examina los campos opcionales.

A diferencia de las opciones de IPv4, los encabezados de extensión de IPv6 pueden tener un tamaño arbitrario. Asimismo, la cantidad de opciones que lleva un paquete no se limita a 40 bytes. Aparte de la forma de procesar las opciones de IPv6, esta función permite que las opciones de IPv6 se apliquen a funciones que no resultan viables en IPv4.

Para mejorar el rendimiento al controlar los encabezados de opciones subsiguientes, así como el protocolo de transporte que va después, las opciones de IPv6 siempre son un múltiplo entero de 8 octetos. El múltiplo entero de 8 octetos mantiene la alineación de los encabezados subsiguientes. Para óptimo desempeño del protocolo, estos encabezados de extensión son colocados en un orden específico. La RFC 2460 recomienda que los encabezados de extensión sean colocados en el paquete IPv6 en un orden en particular, mas aun cuando más de una extensión de encabezado es usada en el mismo paquete, se recomienda que esos encabezados aparezcan en el siguiente orden:

- Hop-by-hop options header
- Destination options header
- Routing header
- Fragment header
- Authentication header
- Encapsulating security payload header
- Upper-layer header

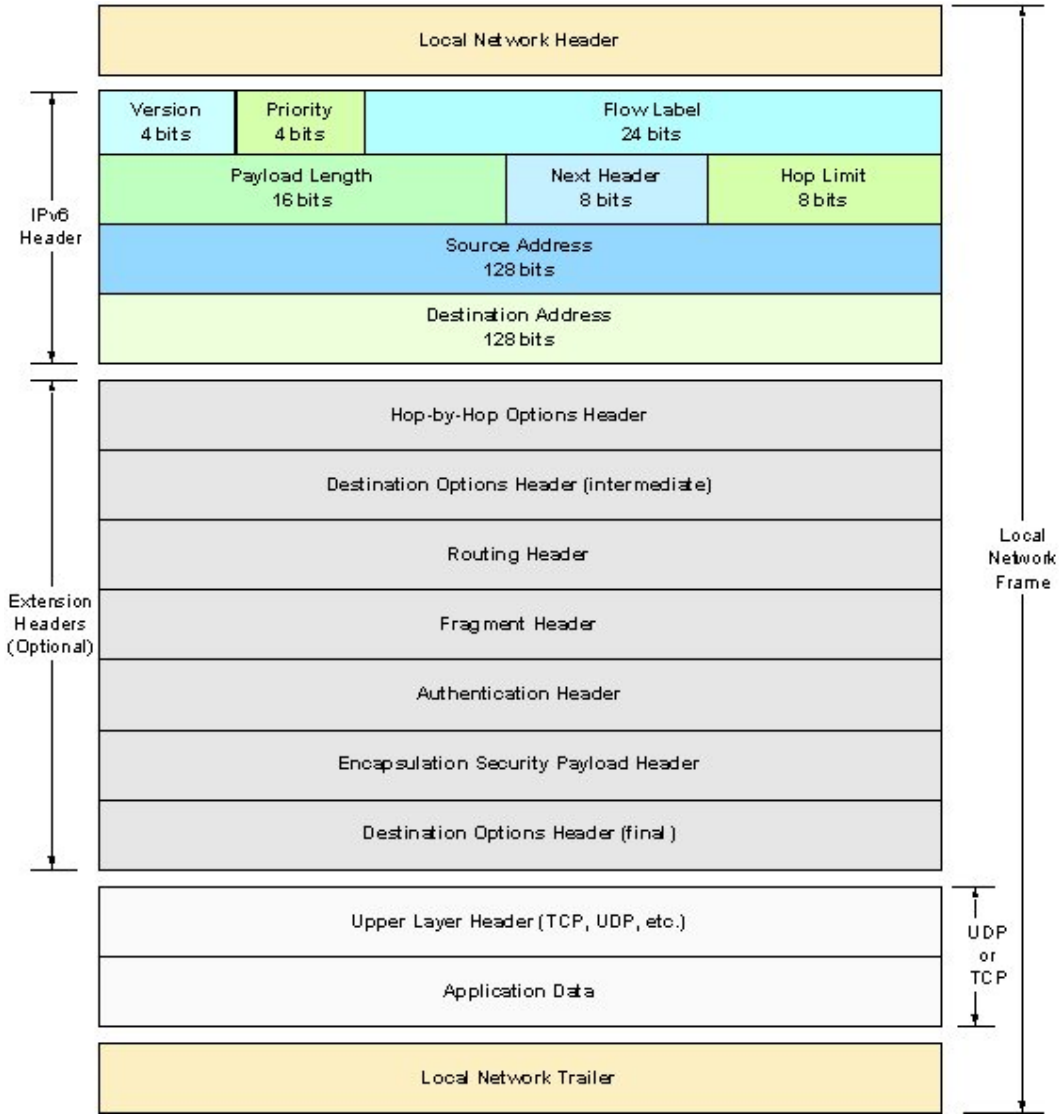


Figura 4.10 Extension Header.

Cada cabecera de extensión debe ocurrir en más de una vez, a excepción de la cabecera de opción de destino, la cual debería de ocurrir dos veces (una vez del Routing Header y otra después de la Upper-layer Header

Dos de los encabezados de extensión, Hop-by-hop y Destination Options, pueden cargar una o más opciones que identifican más allá de los parámetros de operación de red. Estas opciones son codificadas usando el formato TLV (Tipo-Longitud-Valor) que es especificado por el lenguaje de descripción de mensajes ASN1. La opción del formato incluye un campo Option Type de 8 bits que identifica la longitud del campo Option Data dada en octetos; y un campo Option Data de longitud variable.

Los dos bits de orden más alto del campo Option Type, especifican como tener opciones que son irreconocibles en el nodo de procesamiento IPv6 y sus valores se despliegan en la tabla 4.3.

Valor	Acción
00	Salta la opción y continúa procesando el encabezado.
01	Descarta el paquete
10	Descarta el paquete, sin importar que la dirección destino haya sido Multicast o no, envía un Problema de parámetro de ICMP ala fuente (Tipo de opción irreconocible)
11	Descarta el paquete y envía un mensaje ICMP problema de parámetro (Tipo de Opción irreconocible), solo si el destino no era Mulitcast.

Tabla 4.3 Option Type

El tercer bit de orden más alto del campo Option Type especifica si el Option Data de esa opción pueda cambiar en ruta el destino final del paquete o no y sus valores se ven a continuación.

Valor	Acción
0	Option data no cambia el valor de su ruta
1	Option data no puede cambiar la ruta

Tabla 4.4 Option Type.

Además, hay dos opciones que son usadas, como necesarios, para rellenar las opciones de forma que el encabezado de extensión contenga un múltiplo de 8 octetos. Pad1 Option es usado para insertar un octeto de relleno en el área de opciones en el encabezado. Lo que representa un caso especial (notado por Type = 0) que no tiene campos Opt Data Len o Option Data.

PadN Option es usada para insertar 2 o más octetos de relleno en el área Options de un encabezado. Identificada con el campo Type=1. Si el relleno deseado fuera n octetos, el campo Opt Data Len contendría el valor n-2 octetos de valor cero.

Hop-by-hop options header. Este encabezado se utiliza para información y debe ser examinado por cada nodo que se encarga de direccionar los paquetes IPv6. Este tipo de cabecera se encuentra en aquellos paquetes de IPv6 que indican en el campo cabecera siguiente. El formato sería el que se muestra en la figura 4.9. Siguiente:

Figura 4.11. Hop-by-hop Option Header.

- Cabecera siguiente: 8 bits: Indica la siguiente cabecera.
- Longitud cabecera de extensión: 8 bits: Longitud de la cabecera en octetos, no incluye el primer octeto.

- Opciones: Tamaño variable: Debe de tener un tamaño que permita la alineación del paquete, para ello se podrá utilizar Pad1 y PadN.

La presencia de este encabezado es identificada por un valor 0 en campo Next Header.

Destination Options Header. Carga información que debe ser examinada por los nodos que el paquete de IPv6 tenga que saltar en su ruta para alcanzar el destino. La presencia de este encabezado es identificada por el valor 60 en el campo Next Header del encabezado precedente. Este encabezado contiene 2 campos más el campo de opciones. El encabezado Extension Length es de 8 bits de longitud, y mide la longitud del encabezado Destination Option en unidades de 8 octetos, sin contar con los primeros 8 octetos.

El campo Option es variable en longitud y es un entero múltiple de 8 octetos de longitud. Solo dos opciones son definidas en el RFC 2460, la opción Pad1, usada para insertar un octeto de relleno en el área Options de un encabezado, y el PadN, usada para insertar 2 o más octetos de relleno en el área Options del encabezado.

Routing Header. El encabezado lista uno o más nodos intermediarios que son visitados durante el camino hasta el destino. Es identificado en el campo de Next Header por el valor 43. El campo Next Header tiene 8 bits de longitud, e identifica el encabezado que continua inmediatamente al encabezado Routing. Este campo usa los mismos valores que el campo Protocolo de IPv4. Este encabezado está compuesto por el campo de Next Header, Extension Header, Rounting Type, el campo Segments Left y el campo Type-specific. El formato de esta cabecera se muestra en la figura 4.10.

Next Header	Extension Header	Type	Segments Left
Type-specific data			

Figura 4.12 Routing Header.

El campo Next Header tiene 8 bits de longitud, e identifica el encabezado que continua inmediatamente al encabezado Routing. Este campo usa los mismos valores que el campo de Protocolo de IPv4.

El campo Header Extension Length tiene 8 bits de longitud, y mide la longitud del encabezado Routing en unidades de 8 octetos, sin contar los primeros 8 octetos.

El campo de Routing Type tiene 8 bits de longitud e identifica una variable particular del encabezado de Rounting. El RFC 2460 define una variante simple, el encabezado Routing Type 0, que contiene una lista ordenada de direcciones que serán visitadas durante la ruta del paquete.

El campo Segments Left tiene 8 bits de longitud, e identifica el numero de segmentos de ruta que quedan, o en otras palabras, el numero de nodos intermedios explícitamente listados que todavía serán visitados antes de alcanzar el destino final.

El campo Type-Specific es variable en longitud, con un formato definido por la variante particular Routing Type.

Fragment Header. Este encabezado maneja la fragmentación de una manera parecida al de IPv4. El encabezado contiene el identificador del datagrama, el número de fragmento y un bit que indica si seguirán más fragmentos. A diferencia de IPv4, en Ipv6 solo el host origen puede fragmentar un paquete, lo que permite acelerar el procesamiento de los equipos ruteadores. Si un paquete demasiado grande para un nodo intermedio no puede ser procesado, lo descarta y devuelve un paquete ICMP al origen. Esta información permite que el host de origen fragmente el paquete en pedazos más pequeños usando este encabezado y lo intenta nuevamente. La presencia del encabezado es identificada por el número 44 en el campo de Next Header en el encabezado precedente. La cabera de Fragmentación contiene 6 campos, como se muestra en la figura 4.11.

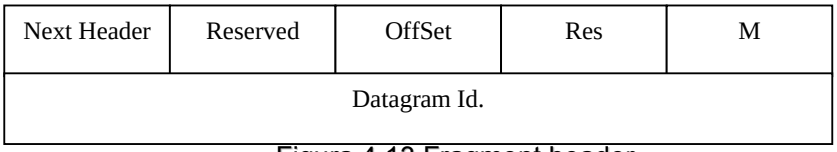


Figura 4.13 Fragment header.

El campo Next Header tiene 8 bits de largo e identifica el encabezado que continua inmediatamente al header fragment. Este campo tiene los mismos valores que el campo Protocolo de IPv4.

El campo Reserved tiene 8 bits de largo y está reservado para uso futuro. Este campo es iniciado en cero para la transmisión e ignorado en la recepción.

El campo Fragment Offset es un entero sin signo de 13 bits que mide la compensación, en unidades de 8 octetos, de los datos que continúan este encabezado, relativo al comienzo de la parte fragmentable del paquete original.

El campo reservado tiene 2 bits de largo, y está reservado para uso futuro. Este campo es inicializado en cero para la transmisión e ignorado en la recepción.

La bandera M es de 1 bit de longitud y determina si mas fragmentos vienen (M=1) o si este es el ultimo fragmento (M=0).

El campo de identificación es de 32 bits de largo y únicamente identifica el o los paquetes fragmentados durante el proceso de re-ensamblaje. Este campo es generado por el nodo fuente.

Cada paquete original consiste de dos partes: una parte no fragmentable y una parte fragmentable. La parte no fragmentable incluye el encabezado IPv6, más cualquier encabezado de extensión que debe ser procesado en una ruta destino. Este puede incluir un encabezado Hop-by-Hop y un encabezado Routing. La parte fragmentable es el balance del paquete, que puede incluir cualquier encabezado de extensión que es procesado al final del nodo destino, los encabezados de capa más alta, y los datos de aplicación.

La parte fragmentable del paquete original está dividida en fragmentos que son íntegros múltiplos de 8 octetos. Cada paquete fragmentado consiste de tres partes: la parte no fragmentable, un encabezado de fragmentación y un fragmento de datos. La

parte no fragmentable de cada fragmento contiene un campo de Payload Length revisado que hace juego con la longitud de este fragmento y un campo Next Header igual a 44.

Authentication header. Este encabezado proporciona un mecanismo mediante el cual el receptor de un paquete puede estar seguro de quien lo envió. La carga útil de seguridad encriptada posibilita cifrar el contenido de un paquete de modo que solo el receptor pretendido pueda leerlo. La presencia de este encabezado es identificada por un valor de 51 en el campo de Next Header en el encabezado precedente. Este encabezado contiene 6 campos, figura 4.12.

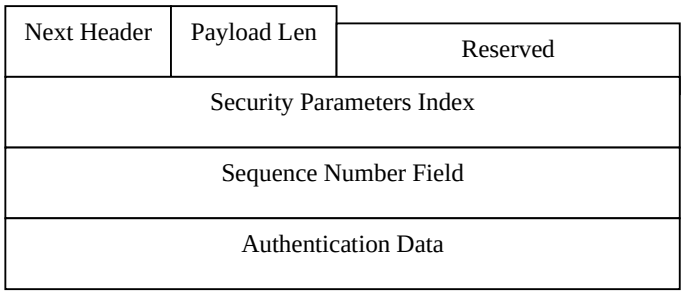


Figura 4.14 Authentication Header.

El campo Next Header tiene 8 bits de largo e identifica el encabezado que continua inmediatamente al encabezado Authentification. Este campo usa los mismos valores que el campo Protocolo IPv4.

El campo Payload Length tiene 8 bits de longitud y provee la longitud del encabezado Authentification en palabra de 32 bits, menos 2. El valor mínimo es 1, que consiste en el valor de autentificación de 96 bits, menos el valor 2. Este mínimo es solo usado en el caso de un algoritmo de autentificación nulo, empleado para procesos de depuración.

El campo Reserved tiene 16 bits de longitud y es reservado para uso futuro, es inicializado en cero para la transmisión. Está incluido en el cálculo Authentification Data, pero sino es ignorado en la recepción.

El campo Security Parameters Index (SPI) es un valor arbitrario de 32 bits que identifica la asociación de seguridad (SA) para este datagrama, relativo a la dirección contenida en el encabezado de IP al que este encabezado de seguridad es asociado, y relativo al protocolo de seguridad empelado. La asociación de seguridad, como se define en el RFC 2401, es una conexión simple y lógica que es creada para propósitos de seguridad. Todo trafico que atraviesa SA tiene el mismo proceso de seguridad. SA puede comprimir muchos parámetros, incluyendo el algoritmo Authentification, calves del algoritmo de autentificación y otros. Según el RFC 2402, el valor de SPI = 0 puede ser usado para propósitos locales, de implementación especificas. Otros valores, en el rango 1 – 255, son reservados para uso futuro por la IANA.

El campo Sequence Number contiene un número de 32 bits que crece monotónicamente. Tanto el contador del que envía como el contador del que recibe son iniciados en cero cuando una asociación de seguridad es establecida.

Authentification Data es un campo de longitud variable que contiene el Valor de Chequeo de Integridad (ICV) y debe ser un múltiplo integral de 32 bits de longitud. El tamaño del campo depende de la función de autentificación que es seleccionada. Este campo es opcional, y es incluido solo si esa asociación de seguridad ha seleccionado servicio de autentificación.

Encapsulating security payload header. Este encabezado llamado ESP por sus siglas en ingles, es definido en el RFC 2406, se emplea para proporcionar confidencialidad, autentificación de datos en origen, integridad sin conexión, servicio de anti-repetición y confidencialidad del flujo de tráfico. El encabezado ESP es identificado por un valor de 50 en el campo de Next Header del encabezado precedente. Este encabezado contiene 7 campos, algunos obligatorios y algunos otros opcionales dependiendo de la asociación de seguridad.

El campo Security Parameters Index (SPI) es un valor arbitrario de 32 bits, en conjunto con la dirección IP destino y el protocolo de seguridad ESP identifica la asociación de seguridad para este datagrama, es un campo Obligatorio.

El campo Sequence Number con 32 bits contiene un valor que incrementa monotónicamente. Es un campo obligatorio. El contador del que envía y el contador del que recibe son inicializados en cero cuando una asociación de seguridad es establecida.

El campo Payload Data es de longitud variable que contiene datos descritos por el campo Next Header. Este campo es obligatorio y es un número integral de bytes en longitud.

El campo Padding puede opcionalmente contener 0 – 255 octetos de información de relleno, como requerido por la implementación de seguridad. Debido a que vario algoritmos criptográficos necesitan como entrada de datos bloques de tamaño definido, para completar y alcanzar el tamaño de dichos bloques se utiliza el campo Padding o relleno. Este campo es obligatorio

El campo Pad Length es de 8 bits e indica en bytes el tamaño del campo Padding. Siempre está presente y si el valor es 0 indica que no hay relleno. Este campo es obligatorio.

El campo Next Header es de 8 bits, indica el tipo de datos que es transportado en el campo Payload y es obligatorio.

El campo Authentication Data es un campo de longitud variable que contiene un valor de chequeo de integridad (Integrity Check Value. CVI). La longitud de este campo depende de la función de autentificación que es seleccionada. El campo es opcional y es incluido solo si esa asociación de seguridad ha seleccionado el servicio de autentificación.

5

Diseño de IPv6

El espacio de direccionamiento de IPv6 es definido por varias clases de direcciones, tal y como se presento con el Protocolo de Internet versión 4, definen un identificador de sitio, un identificador de host y múltiples prefijos de dirección. El diseño de IPv6 ha sido diseñado para ser compatible e interoperable con la red actual de Internet con la finalidad de que ambas arquitecturas de red puedan coexistir. Tal como se discutió en el capitulo anterior, IPv6 no solo soluciona el agotamiento de direcciones, sino que también mejora funciones de IPv4. Ipv6 mejora el enrutamiento y el direccionamiento, mientras que de igual simplifica el encabezado. Las características de IPv6 ofrecen una gran escalabilidad y un diseño jerárquico, el cual permite un enrutamiento más eficiente ya que reduce las tablas de enrutamiento. Durante este apartado se describirá el tipo de direcciones: unicast, anycast y multicast; la representación de las direcciones IPv6 y su estructura. Se describirá el diseño propuesto de IPv6 al Sistema de Nombres de dominio y sus características. Se explicara los mensajes que utilizan el protocolo ICMPv6 y su funcionalidad.

5.1 Direccionamiento.

La dirección IP identifica de manera lógica y jerárquica a un dispositivo de red. Las direcciones IPv6 son cuatro veces más grandes que las direcciones del protocolo de internet versión 4. Su representación es diferente a la versión anterior. Una dirección de IPv6 esta constituida por 128 bits de longitud, lo que se traduce en 340 282 366 920 938 463 374 607 431 768 211 456 direcciones. Según cifras proyectadas por la International Data Base de los Estados Unidos, la población mundial alcanzara la cifra de 9 256 342 700 habitantes, lo que representaría 3 676 2075 254 726 519 953 002 021 784 direcciones por habitante en el planeta. De acuerdo con la Universidad de Hawaii existen 7,500,000,000,000,000,000 granos de arena en el mundo, lo que representaría 45 370 982 256 125 128 461 direcciones por grano. Las analogías salen

fuera de cualquier intento de comparación. De tal forma que el gran espacio de direccionamiento resuelve por varios años un posible agotamiento de direcciones.

5.1.1 Representación de direcciones IPv6.

De acuerdo al RFC 2373 llamado IP Version 6 Addressing Architecture, RFC 2374 An IPv6 Aggregatable Global Unicast Address Format y redefinidas en el RFC 3513 Internet Protocol Version 6 (IPv6) Addressing Architecture, hay tres tipos de formas para representar las direcciones IPv6. La dificultad de memorizar las direcciones ha propiciado a utilizar diferentes métodos de representar las direcciones. La forma preferida es el método más largo, representado por 32 caracteres hexadecimales, la notación hexadecimal es representada usando dígitos del 0-9 o letras de a-f. El siguiente formato es la representación compacta de una dirección IPv6, que permite simplificar la dirección IPv6 cuando se presenta un valor de cero. Por último, el tercer método para representar una dirección está relacionado a los métodos de transición, donde una dirección IPv4 esta embebida en una dirección IPv6, la cual está limitada solo a redes que reutilizaran su direccionamiento. La representación de cada método se detalla a continuación.

Método Preferido. Como se muestra en la figura 5.1, este método, también conocido como la forma completa de una dirección IPv6 está compuesta por 8 campos hexadecimales de 16 bits separados por dos puntos (:) . Cada campo de 16 bits es representado por cuatro caracteres hexadecimales, lo que significa de cada campo de 16 bits puede tener los valores hexadecimales de 0X0000 hasta F:FFFF.

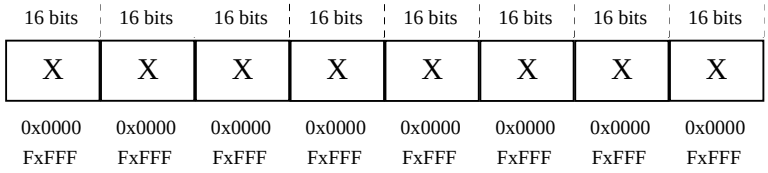


Figura 5.1 Método Preferido.

Este formato es la representación más larga de una dirección IPv6. Un total de 32 caracteres hexadecimales puede ser representado in esta forma. En comparación con una dirección IPv4 que tiene cuatro campos decimales de 8 bits separados por un punto, para un posible total de 12 caracteres decimales.

Método compacto. En IPv6 es común el uso de direcciones que contienen una cadena de ceros , para escribir este tipo de direcciones de forma más practica y sencilla, una sintaxis especial puede ser utilizada para abreviar las direcciones en dos situaciones: campos sucesivos de 16 bits con el valor cero y si los campos iniciales también son ceros.

En el caso de uno o varios campos sucesivos compuestos por una cadena de ceros es posible representarlos como (::). Sin embargo, solo un :: es permitido por dirección. Este método permite reducir considerablemente las direcciones IPv6. La representación compacta de la dirección IPv6 puede también significar varias

representaciones de una misma dirección. En la tabla 5.1 se muestran algunos ejemplos de este método.

Formato Preferido	Formato compacto
0000:0000:0000:0000:0000:0000:0000:0000	::
0000:0000:0000:0000:0000:0000:0000:0001	::0001
2001:0410:0000:1234:FB00:1400:5000:45FF	2001:0410::1234:FB00:1400:5000:45FF
3FFE:0000:0000:0000:1010:2A2A:0000:0001	3FFE::1010:2A2A:0000:0001
FE80: 0000:0000:0000:0000:0000:0000:0009	FE80::0009

Tabla 5.1 Método compacto.

Campos iniciales en ceros. El siguiente método para comprimir direcciones es aplicable para cada campo hexadecimal cuando uno o más ceros iniciales en cada campo se encuentran presentes. Este tren de ceros puede ser simplemente removido para simplificar la longitud de la dirección. Sin embargo, si cada carácter hexadecimal de un campo de 16 bits es cero, al menos un carácter debe ser mantenido. La tabla 5.2 contiene algunos ejemplos de este método.

Formato Preferido	Formato compacto
0000:0000:0000:0000:0000:0000:0000:0000	0:0:0:0:0:0:0:0
0000:0000:0000:0000:0000:0000:0000:0001	0:0:0:0:0:0:0:1
2001:0410:0000:1234:FB00:1400:5000:45FF	2001:0410:0:1234:FB00:1400:5000:45FF
3FFE:0000:0000:0000:1010:2A2A:0000:0001	3FFE:0:0:0:1010:2A2A:0000:0001
FE80: 0000:0000:0000:0000:0000:0000:0009	FE80:0:0:0:0:0:0:0009

Tabla 5.2 Campos iniciales en cero.

Ambos métodos pueden ser utilizados o bien pueden ser combinados en la representación de las direcciones IPv6.

Dirección IPv6 con una dirección IPv4 embebida. La tercera representación de una dirección IPv6 es para usar una dirección IPv4 embebida dentro de una dirección IPv6. La primera parte de la dirección IPv6 usa una representación hexadecimal, mientras que la dirección IPv4 usa una notación decimal. Esta es una representación específica de una dirección IPv6 usada por métodos de transición. En la figura 5.2 se muestra el formato de una dirección IPv6 usando una dirección IPv4 embebida.

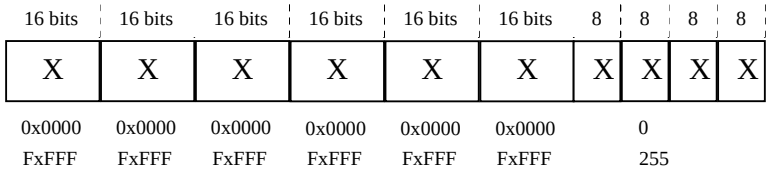


Figura 5.2 Dirección IPv6 con una dirección IPv4 embebida.

La tabla 5.3 muestra algunos ejemplos de esta representación de este método y también demuestra que se puede utilizar la representación del método compacto.

Formato Preferido	Formato compacto
0000:0000:0000:0000:0000:0000:206.123.31.2	0:0:0:0:0:0:206.123.31.2 o ::206.123.31.2
0000:0000:0000:0000:0000:0000:ce7b:1f01	0:0:0:0:0:0:ce7b:1f01 o ::ce7b:1f01
0000:0000:0000:0000:0000:FFFF:206.123.31.2	0:0:0:0:0:FFFF:206.123.31.2 o ::FFFF:206.123.31.2
0000:0000:0000:0000:0000:FFFF:ce7b:1f01	0:0:0:0:0:FFFF:ce7b:1f01 o ::FFFF:ce7b:1f01

Tabla 5.3 Dirección IPv6 con una dirección IPv4 embebida.

5.1.2 Tipos de direcciones.

Independientemente del tipo de representación, diferentes tipos de direcciones son definidas para el Protocolo de Internet versión 6, como se muestra en la figura 5.3 hay tres tipos de direcciones: Unicast, Anycast y Multicast. Cada una de ellas tiene su tipo de direcciones. Unicast tiene direcciones del tipo link-local, site-local, global, loopback, sin especificar y direcciones compatibles con IPv4. Anycast tiene direcciones globales, site-local y link-local. Multicast tiene asignadas y de nodo solicitado.

Las direcciones Unicast identifican un única interface de un nodo de red en IPv6. Un paquete enviado a una dirección unicast es entregado al interfaz identificado por dicha dirección. La dirección Anycast es asignada a múltiples interfaces, normalmente de distintos nodos. Un paquete enviado a una dirección anycast es entregado a uno de los interfaces identificados con dicha dirección. Una dirección multicast identifica a un grupo de interfaces, típicamente pertenecientes a diferentes nodos. Un paquete enviado a una dirección multicast es entregado a todos los interfaces que tengan asignada dicha dirección.

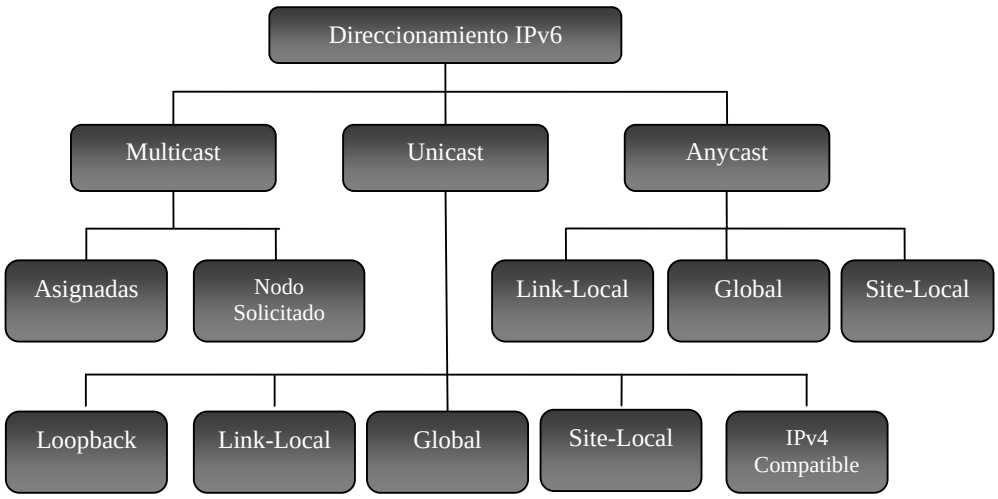


Figura 5.3 Direcciones IPv6

Dirección Link-Local. La dirección local de enlace, por su traducción en español, es usada solo entre nodos conectados en un mismo enlace local, ofrece

funciones como la autoconfiguración de direcciones, neighbor discovery o para permitir la comunicación entre nodos cuando no existe un dispositivo de capa 3. La dirección Link local tiene el siguiente formato:

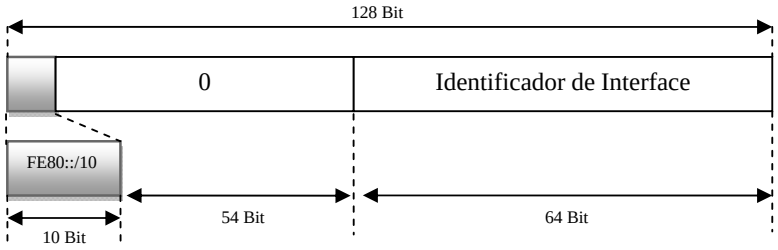


Figura 5.4 Dirección Link-Local

Como se observa en la imagen 5.4, el prefijo usado para identificar estas direcciones es FE80 y se usa un identificador de interface con el formato EUI-64 en los 64 bits de menor orden. Los siguientes bits después del prefijo están configurados en 0. Estas direcciones son representadas en el formato compacto como FE80::/10.

Dirección Site-Local. Las direcciones de uso local son definidas para ser utilizadas dentro de una red local con diferentes enlaces. Esta dirección es similar al espacio de direccionamiento privado en IPv4, puede ser usada por organizaciones las cuales no han obtenido una dirección global dentro de su organización. Este tipo de direcciones no debe de ser anunciada al Internet. La dirección es constituida por un prefijo FEC0::/10, un campo de 54 bits llamada Identificador de Subred y un identificador de interface en un formato EUI-64 en los 64 bits de menor orden.

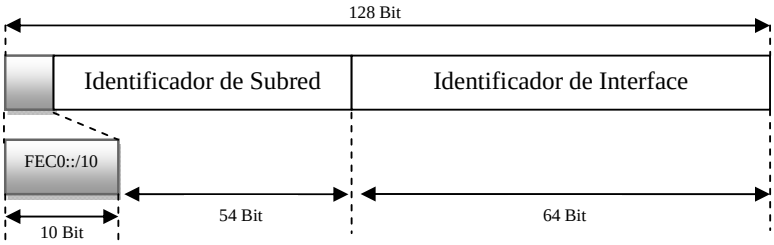


Figura 5.5 Dirección Site-Local.

Dirección Global Unicast. Es una dirección usada para el tráfico genérico de IPv6 sobre el Internet IPv6. Son similares a las direcciones unicast para la comunicación usada a través de IPv4. La estructura de esta dirección hablita una estricta agregación de prefijos de rutas para limitar el tamaño de las tablas de ruteo de Internet. El formato general para las direcciones global unicast está en la siguiente figura.

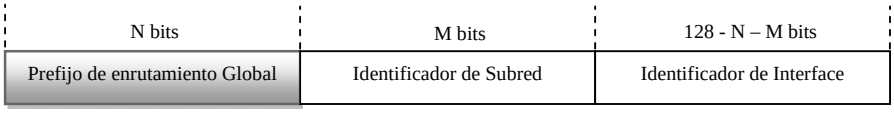


Figura 5.6 Dirección Global Unicast

donde el prefijo de enrutamiento global (global routing prefix) es un valor asignado a un sitio, un conjunto de subredes o enlaces, el campo Identificador de Subred es el identificador de cada unade las subredes dentro del sitio, y el Identificador de Interface es el identificador de una interface. El prefijo de enrutamiento global ha sido diseñado para ser estructurado jerárquicamente por los Proveedores de Servicio, mientras que el identificador de subred es asignado de manera jerárquica por los administradores de la red. Todas las direcciones global unicast que no empiecen con el prefijo 000 tienen un identificador de interface de 64 bits, mientras que las que las que empiezan por 000 no tienen ninguna restricción sobre la longitud de dicho identificador.

Dirección Loopback. La dirección 0:0:0:0:0:0:0:1 es llamada dirección Loopback, sirve para enviar un paquete de IPv6 de un nodo a sí mismo. No puede ser asignada a ninguna interface físico, sino que debe entenderse como la dirección link-local asignada a una interface virtual. La dirección de loopback no puede ser usada como dirección origen en paquete salientes, y si un paquete tiene la dirección de loopback como destino no debe ser enviado fuera del nodo ni debe ser direccionado por los routers.

Dirección IPv6 con dirección IPv4 embebida. Existen dos tipos de estas direcciones. La primera utilizada en mecanismos de transición de IPv6, donde los nodos utilizan los últimos 32 bits para encaminar paquetes sobre redes IPv4. Los nodos IPv6 que utilizan esta técnica son asignados con una dirección Unicast especial que transporta una dirección IPv4 global en sus últimos 32 bits de menor orden, denominada “IPv4- compatible IPv6 address” y su formato se presenta en la figura 5.7.

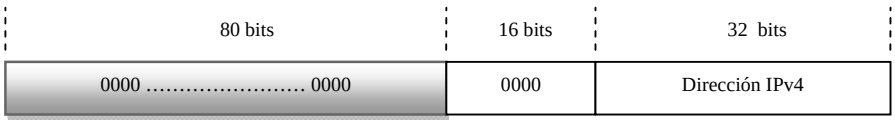


Figura 5.7 Dirección IPv6 con dirección IPv4 embebida

El segundo tipo de direcciones IPv6 que contienen direcciones IPv4, son las que representan las direcciones de nodos que sólo soportan IPv4 en formato IPv6. Este tipo de direcciones es conocida como “IPv4-mapped IPv6 address” y su formato se presenta en la figura 5.8.

Figura 5.8 Dirección IPv6 con dirección IPv4 embebida

Dirección Anycast. Una dirección Anycast es una dirección asignada a más de un interfaces, con el propósito de que un paquete que sea enviado a una dirección anycast sea encaminado hasta la interface más cercana que responda a esa dirección. Las direcciones anycast son asignadas del espacio de direcciones Unicast , usando alguno de los formatos definidos para estas direcciones. Así, una dirección anycast es sintácticamente indistinguible de una dirección unicast. Cuando una dirección unicast es asignada a más de un interfaz se convierte inmediatamente en

anycast, y los nodos a los que se les asigna deben ser explícitamente configurados para saber que se trata de una dirección anycast. Para cada dirección anycast, hay un prefijo largo P de la dirección, que identifica la región topológica en la que residen todos los interfaces con una dirección anycast concreta. Dentro de la región identificada con P, la dirección anycast se debe de mantener como una entrada diferente en el sistema de enrutamiento; fuera de la región P, las direcciones anycast deben ser agregadas en las entradas de rutas bajo el prefijo P.

Un uso esperado de las direcciones anycast es identificar conjuntos de routers pertenecientes a una organización que provea servicios de Internet. Estas direcciones podrán ser usadas como direcciones intermedias en una Cabecera de ruteo IPv6, para provocar que los paquetes sean encaminados a través de un ISP particular o una secuencia proveedores. Otro posible uso es para identificar el conjunto de routers unidos a una determinada subred o un conjunto de routers proporcionando entradas a un dominio de ruteo particular.

Una dirección anycast no debe ser usada como una dirección fuente de un paquete IPv6. Una dirección anycast no debe ser asignada a un nodo IPv6, es decir, puede ser asignada un router IPv6 solamente. Las direcciones anycast pueden ser usadas como direcciones Site-Local o Link-Local.

Direcciones Multicast. Una dirección multicast en IPv6 identifica a un grupo de interfaces. Además, una interface puede pertenecer a cualquier número de grupos multicast. Estas direcciones tienen el siguiente formato:

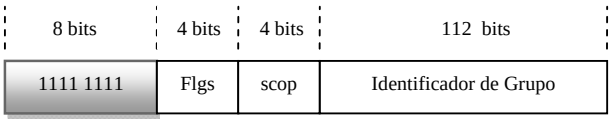


Figura 5.9 Dirección Multicast.

donde el prefijo 11111111 ó 0xFF identifica la dirección como multicast, el campo flag es un conjunto de 4 banderas,

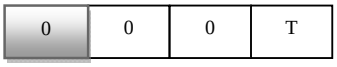


Figura 5.10 Dirección Multicast campo flag.

donde las banderas de mayor orden están reservadas y deben estar configuradas en cero. T=0 indica que la dirección es permanente y es asignada por la IANA, si T=1 indica que la dirección es dinámica.

El campo scope de 4 bits indica el alcance de cada dirección multicast y tiene los siguientes valores:

0-Reservado.
1-Interfaz de ámbito local.
2-Ámbito de enlace local.
3-Reservado.
4-Ámbito de administración local.
5-Ámbito de sitio local.

6-(sin asignar).
7-(sin asignar).
8-Ámbito de organización local.
9-(sin asignar).
A-(sin asignar).
B-(sin asignar).
C-(sin asignar).
D-(sin asignar).
E-Ámbito global.
F-Reservado.

El Identificador de Grupo identifica al grupo multicast, tanto el permanente o el dinámico. Las direcciones multicast no pueden aparecer como dirección origen en un paquete, y tampoco pueden ser utilizadas en el campo “Cabecera de encaminamiento” comentado para las direcciones anycast.

Las direcciones multicast “well-known” o dinamicas dentro del rango FF00:: a FF0F:: son reservadas y nunca serán asignadas a un grupo multicast. IPv6 sustituye el uso de direcciones broadcast por direcciones multicast, dentro del RFC 3513 se definen direcciones especificas para grupos multicast predefinidos.

Dirección Multicast	Descripción
FF01::1	Todos los nodos en la interface
FF02::1	Todos los nodos en el enlace
FF01::2	Todos los routers en un nodo local
FF02::2	Todos los routers en el enlace
FF05::2	Todos los routers en el sitio

Tabla 5.4 Direcciones Multicast Well-Know.

Para realizar la asociación entre direcciones de capa 2 y direcciones IPv6 se utilizan las direcciones “Solicited-Node”o en su traducción de nodo solicitado. Es una dirección calculada a partir de una dirección unicast (oanycast). Se toman los últimos 24 bits de la dirección y se añaden al prefijo FF02:0:0:0:0:1:FF00:0/104, resultando en direcciones con el rango FF02::1:FF00:0000 a FF02::1:FFFF:FFFF.

Las direcciones IPv6 que difieren en los bits de alto orden, quedarán asociados a una única dirección multicast, reduciendo el número de grupos a los que el nodo deberá unirse. Los nodos están obligados a unirse a todas las direcciones solicited-node multicast asociadas a las direcciones unicast (o anycast) que le han sido asignadas.

Direcciones requeridas para cualquier nodo. Todos los nodos en proceso de identificación en la red deben de reconocer las siguientes direcciones:

- Sus direcciones locales de enlace para cada interface.
- Las direcciones adicionales unicast o anycast asignadas.
- La dirección 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 nodo pertenece.

- Los routers deben reconocer:
- 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.

5.2 Arquitectura de direccionamiento IPv6.

IPv6 tiene un espacio de direccionamiento que parecería difícil de ocupar porque utiliza 128 bits en sus direcciones lógicas, gran parte de este direccionamiento es usado por funciones del protocolo por sí mismo como las direcciones de sitio local, direcciones multicast, direcciones de nodo solicitado, direcciones lookback, direcciones sin especificar y direccionesIpv4 compatibles con IPv6, del total del espacio de direccionamiento solo menos del 2% es reservado para estas funciones.

La tabla 5.5 representa un resumen del espacio de IPv6 asignado. La primera columna especifica el prefijo en binario de los 16 bits de orden mayor, la siguiente columna es el rango de valores hexadecimales asignados. Las últimas columnas muestran la proporción de cada prefijo con respecto al espacio completo de direcciones.

Prefijo en Binario	Rango Hexadecimal	Proporción	Descripción
0000 0000		1/256	Sin Asignar
0000 0001	0100 – 01FF	1/256	Sin Asignar
0000 001	0200 – 03FF	1/128	Reservado para NSAP
0000 01	0400 – 05FF	1-64	Sin Asignar
0000 1	0800 – 0FFF	1-32	Sin Asignar
0001	1000 – 1FFF	1/16	Sin Asignar
001	2000 – 3FFF	1/8	Unicast Global
010	4000 – 5FFF	1/8	Sin Asignar
011	6000 – 7FFF	1/8	Sin Asignar
100	8000 – 9FFF	1/8	Sin Asignar
101	A000 – BFFF	1/8	Sin Asignar
110	C000 – DFFF	1/8	Sin Asignar
1110	E000 – EFFF	1/16	Sin Asignar
1111 0	F000 – F7FF	1/32	Sin Asignar
1111 10	F800 – FBFF	1/64	Sin Asignar
1111 110	FC00 – FDFF	1/128	Sin Asignar
1111 1110 0	FE00 – FE7F	1/512	Sin Asignar
1111 1110 10	FE80 – FEBF	1/1024	Unicast de Enlace Local
1111 1110 11	FEC0 – FEFF	1/1024	Unicast de Sitio Local
1111 1111 11	FFFF – FFFF	1/256	Multicast

Tabla 5.5 Espacio de Direcciones IPv6.

Las asignaciones que resaltan del espacio de direccionamiento son las siguientes:

- 00::/8 o ::/8 es el rango reservado para direcciones sin especificar (::), loopback (::1) y compatibles con IPv4. Estas asignaciones representan el 0.38 % del espacio de direccionamiento.
- 200::/7 está reservado para Puntos de Acceso al Servicio de Red (NSAP). Lo que representa un 0.77 % del espacio.
- 2000::/3 está reservado para direcciones unicast globales agregables, lo que representa el 12.5 % del espacio total. Estas direcciones contienen un rango de /16 de 8192.
- FE80::/10 es para direcciones de enlace local, el cual usa el 0.1 % del espacio de direccionamiento.
- FEC0::/10 es para direcciones de sitio local, usa solo el 0.1 % del espacio general.
- FF00::/8 utilizado para direcciones multicast, representa el 0.38 % del espacio.

5.3 DNS.

Internet está construido con un esquema de direccionamiento jerárquico. El problema al que un usuario se enfrenta es asociar la dirección correcta con el sitio de Internet adecuado. Para asociar los contenidos de un sitio con sus direcciones, se desarrollo un sistema de denominación de dominios. DNS es un sistema usado en Internet para traducir nombres de dominio en sus correspondientes direcciones IP. Recordemos que un dominio es un grupo de computadoras que están agrupadas por su localización geográfica o su tipo de negocio y que están inidentificadas con una cadena de caracteres y / o números. El DNS es un dispositivo de red que responde a una petición realizada por clientes y que traduce un nombre de dominio en la dirección IP asociada.

IPv6 introduce un nuevo tipo de registro para almacenar las direcciones IPv6, un nuevo dominio para soportar las localizaciones (lookups) basadas en IPv6, y definiciones actualizadas de tipos de consultas existentes que devuelven direcciones Internet como parte de secciones adicionales.

El problema del sistema de DNS existente consiste en esperar una dirección de 32 bits al realizar cualquier consulta. Para resolverlo se definieron nuevos métodos, un nuevo tipo de registro para mapear una dirección de 128 bits, el registro AAAA es definido por la IETF en el RFC 3596 , los registros A6 definido en el RFC 2874, un nuevo dominio para soportar búsquedas basadas en direcciones, y redefinición de consultas existentes.

Los registros AAAA sustituyen los registros A en el IPv4 y mapean una dirección IPv6 a un nombre de host. Este registro tiene el siguiente formato:

<nombrehost> EN AAAA <direcciónIPdehost>

por ejemplo, Maquina2 En AAAA 3FFE:8071:10F9:E00:1234::33. En caso de cambiar de proveedor o de dominio se introdujo un sistema dinámico de traducción, para lo que se crearon los registros A6.

Cuando un nodo necesita la dirección IP de otro nodo (www.abc.test), este envía una solicitud AAAA al DNS para conocer cómo llegar a él. EL DNS responde con la dirección IPv6 solicitada, por ejemplo 3FFE:0B00:0C18:0001:0290:27FF:FE17:FC1D. El registro AAAA almacena una dirección IPv6 simple. Un nodo con más de una dirección puede tener más de un registro en la base de datos del servidor DNS.

Los registros A6 este tipo de registro permiten que una consulta pueda ser de forma recursiva, es decir, que la consulta pueda dividirse en varias subconsultas. Este registro se encuentra como experimental por la IETF y tiene el siguiente formato:

a.b.c A6 <NN> <address-suffix> <name>

donde a.b.c es el nombre del dominio que se quiere resolver, NN es el largo del prefijo, o sea, 128; el <address-suffix> es la parte de la dirección que resuelve este registro. Y el campo Name es el próximo registro que resuelve la otra parte de la dirección, siendo nulo si NN igual a cero.

La operación más habitual con el DNS es obtener la dirección IP correspondiente a un nombre de nodo. Sin embargo, a veces queremos hacer la operación opuesta, para lo que se utiliza la resolución inversa, y la usan diversas aplicaciones para comprobación de identidad. El registro que nos permite el mapeo inverso es conocido como PRT definido en el RFC 1035, el registro especifica la dirección IPv6 al nombre del nodo. Finalmente, los registros DNAME y etiquetas binarias permiten que la remuneración sea fácil de obtener.

Actualmente en nuestro país, NIC México (Network Information Center México) es responsable de administrar los nombres de dominio .MX en Internet, así como de la asignación de direcciones de IP en el país y ha desplegado el primer nodo de DNS sobre IPv6 en el país.

5.4 ICMPv6.

Ligado al nuevo protocolo IPv6 aparecen nuevas versiones de protocolos usados con IPv4 como es el caso de ICMPv6 (Internet Control Message Protocol Versión 6). ICMP es el componente del conjunto de protocolos TCP/IP que se encarga del fallo de IP para asegurar la entrega de datos. ICMP simplemente envía mensajes de error al emisor de los datos, indicando que se han producido problemas en la entrega de los datos.

Este protocolo se ubica en la capa de Internet del modelo TCP/IP. Define mensajes para el diagnostico, información y para propósitos de administración de red. En esta versión los servicios ofrecidos por ICMP han sido ampliados e incluyen funcionalidades ofrecidas anteriormente por IGMP (Internet Group Management Protocol) y ARP (Address Resolution Protocol) además de nuevas funcionalidades como el descubrimiento de máximo MTU del camino. El RFC 2463 específica los tipos de mensajes en ICMPv6 y los cuales se muestran en la tabla 5.6.

Mensaje	Numero de tipo	Tipo de Mensaje	Definición
Destino inalcanzable	1	Error	Indica al nodo que no es posible entregar el datagrama.
Paquete demasiado grande	2	Error	El paquete es más grande que el MTU del enlace de salida.
Tiempo Excedido	3	Error	Indica que el tiempo de vida TTL ha caducado y el paquete es descartado.
Solicitud de Eco	128	Informativo	Determina si está disponible un nodo IP en la red.
Respuesta de Eco	129	Informativo	Responde a una solicitud de eco de ICMP.

Tabla 5.6 Mensajes ICMPv6.

Un valor de 58 en el campo de siguiente cabecera identifica un paquete ICMPv6. IPv6 considera un paquete de ICMPv6 ser un protocolo de capa superior. Por tanto, los mensajes ICMP contienen la cabecera IP básica, posibles cabeceras de extensión y el mensaje ICMP cuya inmediata predecesora la identifica con el campo siguiente cabecera igual a 0x58. El formato del mensaje ICMPv6 se muestra en la figura.

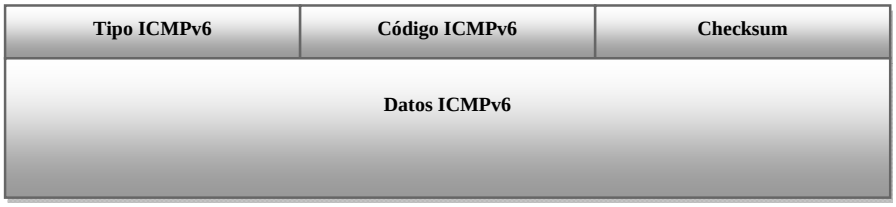


Figura 5.11 Mensaje ICMPv6.

El campo Tipo indica el tipo de mensaje, este valor determina el formato de la información a recibir, ejemplos de estos mensajes se encuentran en la tabla superior. El campo Código depende del tipo de mensaje y es usado para crear un nuevo subnivel de clasificación de los mensajes. El campo Checksum es usado para detectar la corrupción de los datos en los mensajes ICMPv6 y en parte de las cabeceras IPv6. El campo de datos de ICMPv6 puede ser o no utilizado, dependiendo del tipo de mensaje. Cuando es usado, este campo proporciona información al nodo destino.

Los paquetes ICMP en IPv6 son usados en el protocolo llamado Neighbor Discovery, en el descubrimiento del valor más grande de MTU (PMTUD), remuneración de Prefijos, detección de direcciones duplicadas y mecanismos usados para reemplazar ARP en IPv4.

5.5.- Protocolo Neighbord Discovery.

En IPv6, los nodos de una red usan un nuevo protocolo denominado Neighbor Discovery o descubrimiento de vecinos para determinar las direcciones de enlace de los nodos que residen en su mismo enlace, denominados vecinos, y para eliminar rápidamente los valores almacenados en caché que queden invalidados. Este protocolo es equivalente a ARP en IPV4 y es definido en el RFC 2461. Tal como su

traducción indica consiste en descubrir los nodos que conforman la red, determinar sus direcciones de la capa de enlace y mantener la información de conectividad. Este protocolo proporciona además un mecanismo a los hosts que les permite encontrar los routers que han de encaminar sus paquetes, por lo que, teniendo en cuenta su facultad de seguimiento de estado del enlace, serán capaces de encontrar nuevas rutas ante fallos de enlaces o routers. Este protocolo es la base del mecanismo de autoconfiguración de IPv6.

El protocolo ND (Neighbord Discovery) define cinco mecanismos que hacen uso de los nuevos mensajes de ICMPv6.

Mensaje	Tipo de ICMPv6	Descripción
Solicitud de Router	133	Son peticiones que utilizan los routers.
Aviso de Router	134	Enviado por los routers periódicamente y en respuesta de una solicitud de router.
Solicitud de Vecino	135	Son peticiones a los nodos.
Aviso de Vecino	136	Es la respuesta a un mensaje de solicitud de vecino, o también cuando un nodo cambio de dirección de enlace.
Redirección	137	Utilizados por los routers para informas de mejores rutas a los nodos.

Tabla 5.7 Protocolo ND.

Las funcionalidades cubiertas por ND son bastante amplias, entre ellas se encuentran el descubrimiento de routers vecinos por parte de los nodos, subredes, parámetros de enlace, autoconfiguración de dirección de las interfaces de los nodos, resolución de la dirección de enlace de los vecinos a partir de su dirección IP, construcción de tablas de siguiente salto mapeando las direcciones IP de los destinos con las de los vecinos para enviar el trafico saliente, detección de vecinos inalcanzables, direcciones duplicadas, redirección de paquetes provenientes de un nodo hacia otro mejor primer salto, actualización de direcciones invalidas.

El protocolo ND corresponde a una combinación de protocolos de IPv4 como ARP, ICMP Router Discovery e ICMPv4 Redirect. Las mejoras de ND ante el conjunto de protocolos de IPv4 utilizados para funciones parecidas son descritas en el RFC 2461 y se listan a continuación:

- Router Discovery es parte del protocolo, por lo que no es necesario que los nodos tengan ningún conocimiento de los protocolos de enrutamiento.
- Los mensajes Router Advertisement contienen información acerca de sus direcciones de enlace, por lo que no son necesarios intercambios adicionales de paquetes.
- La información sobre el prefijo del enlace que contienen estos mismos mensajes evitan tener que implementar otros mecanismos para configurar las máscaras de la red.
- Estos mensajes proporcionan también servicios de autoconfiguración de dirección.
- Los routers pueden indicar la MTU a los hosts del enlace, asegurándose así de que todos los nodos usen el mismo valor de MTU en enlaces que no tengan una MTU bien definida.
- Se extienden los multicast de resolución de direcciones entre 232 direcciones, reduciendo de forma importante las interrupciones relativas a la resolución de

direcciones en nodos distintos al objetivo, y evitando las interrupciones en nodos IPv6.

- Las redirecciones contienen la dirección de la capa de enlace del nuevo salto, lo que evita la necesidad de una resolución de dirección adicional.
- Un mismo enlace puede ser asociado a múltiples prefijos. Por defecto, los nodos aprenden todos los prefijos del enlace al que están conectados a partir de los Router Advertisement. En algunos casos, los routers pueden estar configurados para omitir algunos de los prefijos (o todos) en sus avisos, de manera que los nodos asuman que destinos no se encuentran en su enlace y manden el tráfico a través de los routers, que serán los encargados de redireccionarlos apropiadamente.
- El receptor de un paquete de Redirección asume que el nuevo Next-Hop pertenece al enlace. En IPv4, los hosts ignoraban los paquetes de redirección si consideraban que el siguiente salto no estaba en el enlace, basándose en su máscara.
- El algoritmo "Neighbor Unreachability Detection" es también parte del protocolo, lo que aumenta la robustez del reparto de paquetes frente a fallos de routers o cambios de direcciones de enlace por parte de los nodos. Esto permite, por ejemplo, que nodos móviles puedan cambiar de red (abandonando el vecindario)sin perder conectividad como ocurría con las cachés de ARP.
- El uso de direcciones link-local para identificar unívocamente los routers hace posible que los hosts mantengan las asociaciones de los routers en el caso de que se establezca un nuevo prefijo global.
- ND es inmune a los ataques por parte de usuarios no pertenecientes al enlace que envíen, accidental o intencionadamente, mensajes de ND con el campo Hop-Limit igual a 255 (debido a que los mensajes deberán proceder de direcciones de alcance local). En IPv4 estos eran capaces de enviar tantos mensajes ICMP de redirección como Avisos de Router.

5.6 Enrutamiento y Administración de las rutas

El enrutamiento es una función de capa 3 y funciona de forma jerárquica permitiendo agrupar direcciones individuales para ser tratadas como una sola unidad hasta que se necesiten esas direcciones individuales para una distribución final de los datos. El enrutamiento es el proceso que consisten en encontrar la ruta más eficaz desde un dispositivo a otro. Para ayudar en el proceso de determinación de la ruta, los protocolos de enrutamiento construyen y mantienen tablas de enrutamiento, que contienen información de rutas, la cual varía de acuerdo al protocolo utilizado. Los nodos IPv6 utilizan una tabla de enrutamiento para mantener información acerca de otras redes y nodos IPv6. Los segmentos de red se identifican mediante un prefijo de red IPv6 y una longitud de prefijo. Además, las tablas de enrutamiento proporcionan información importante a cada host local respecto a cómo deben comunicarse con redes y hosts remotos.

Una de las ventajas de IPv6 es el mecanismo de enrutamiento flexible. Debido a la forma en que los Identificadores de red de IPv4 se asignaban y se asignan, los principales enrutadores de Internet deben mantener grandes tablas de enrutamiento. Estos enrutadores deben conocer todas las rutas para poder reenviar los paquetes que se dirigen potencialmente a cualquier nodo de Internet. Con su capacidad de agregar direcciones, IPv6 permite direcciones flexibles y reduce drásticamente el tamaño de las tablas de enrutamiento. En esta nueva arquitectura de direccionamiento, los enrutadores intermedios sólo deben mantener el seguimiento de la parte local de su red para reenviar los mensajes de forma adecuada.

Antes de enviar un paquete IPv6, el equipo inserta la dirección IPv6 de origen y la dirección IPv6 de destino (para el destinatario) en el encabezado IPv6. A continuación, el equipo examina la dirección IPv6 de destino, la compara con una tabla de enrutamiento IPv6 mantenida localmente y realiza la acción adecuada. Las tablas de enrutamiento pueden ser creadas manualmente (encaminamiento estático) o bien automáticamente con algún algoritmo apropiado (encaminamiento dinámico). Estos algoritmos funcionan con un intercambio de información entre los routers de la red. Actualmente los algoritmos más usados son los algoritmos de encaminamiento distribuido, las dos principales familias son los algoritmos de vector distancia y los algoritmos de estado de enlace.

El enrutamiento estático requiere que el administrador de la red cree las tablas de enrutamiento manualmente en los routers. El administrador tiene el control total del tráfico que transmite por la red, pero en caso de falla o error se requiere re-encaminar el flujo de datos. Una entrada estática en la tabla de enrutamiento se llama ruta estática.

Para utilizar algoritmos de encaminamiento dinámico, la introducción del concepto de métrica es esencial. Las métricas de enrutamiento se utilizan para determinar la conveniencia de una ruta. Existen dos métricas universalmente aceptadas: Numero de saltos y costo. El costo es directamente asociado a la velocidad de los enlaces, mientras que el número de saltos indica el número de dispositivos que se atraviesan en la red.

El método de enrutamiento por vector distancia determina la dirección (vector) y la distancia (cuenta de saltos) a cualquier enlace de la red. Estos algoritmos envían periódicamente todo o una porción de su tabla de enrutamiento a sus vecinos adyacentes. Los protocolos de estado de enlace responden rápidamente a los cambios de la red, envían actualizaciones solo cuando se ha producido un cambio en la red., y envían actualizaciones periódicas a intervalos largos de tiempo.

Los principales protocolos de encaminamiento en IPv6 son básicamente los mismos que IPv4: RIPv6 , OSPFv6, BGP4, IDRPv2 y IS-IS, a continuación se detallan los más comunes:

RIPng (RIP next generation). Está basado en protocolos y algoritmos usados en RIP y RIP2 para IPv4 en los RFC1058 y RFC1723. Es un protocolo de vector de distancia que debe ser implementado solo en routers IPv6. Este protocolo está diseñado para redes pequeñas y se incluye en protocolos IGP, emplea un algoritmo Vector Distancia, se basa en el intercambio de información entre routers, de modo que se calculen las rutas más adecuadas de forma automática. El problema de este protocolo es que tiene una métrica fija y no puede variar por problemas de retardo o jitter.

OSPFv6 (Open Shortest Path First) es un protocolo IGP para redes autónomas, basado en una tecnología de estado de enlaces y definido en el RFC2740. Distribuye información entre routers pertenecientes al mismo sistema autónomo, escrito para hacer frente las redes grandes y escalables. Mantiene los mecanismos fundamentales de la versión para IPv4, pero se han modificado ciertos parámetros, así como el incremento del tamaño de la dirección, se ejecuta basado en cada enlace, en lugar de cada subred.

BGP4. Es un protocolo para la interconexión de sistemas autónomos, es decir para el enrutamiento de diferentes dominios. Frecuentemente usado para grandes corporaciones y para la conexión entre proveedores de servicio. La información de enrutamiento de BGP-4 es usada para crear un árbol lógico que describe a las conexiones entre los diferentes sistemas autónomos. La información del árbol se la utiliza para la creación de rutas libres de lazos en las tablas de los routers. Los mensajes de BGP-4 son enviados por el puerto TCP 179. BGP4 añade a BGP en el RFC1771 extensiones multiprotocolo, tanto para IPv6 como para otros protocolos.

IDRPv2. Es un protocolo EGP para ser usado con IPv6. Fue creado originalmente como un protocolo de red no orientado a la conexión y al igual BGP-4 fue también diseñado para permitir la comunicación entre distintos sistemas autónomos. IDRPv2 es un mejor protocolo de enrutamiento que BGP-4 ya que en lugar de utilizar identificadores para los sistemas autónomos, en los dominios de enrutamiento IDRP se los identifica mediante un prefijo IPv6; además los dominios de enrutamiento pueden agruparse en confederaciones de enrutamiento las cuales también son identificadas por el prefijo, para crear una estructura jerárquica y así resumir el enrutamiento.

IS-IS. También conocido como doble IS, es un protocolo de enrutamiento de estado de enlace muy similar a OSPF. IS-IS soporta IPv4 y es orientado a no conexión, usa direcciones multicast, permite dos niveles de escala jerárquica, mientras que OSPF solo permite una.

6

IPv4/IPv6: Estrategias coexistencia e integración.

El protocolo IPv6 has sido diseñado desde el inicio de su diseño con una transición y compatibilidad completa con IPv4, en la actualidad millones de usuarios, aplicaciones, y servidores están interconectados a través de Internet usando IPV4, lo que hace imposible a mediano plazo un cambio de tecnología a la nueva versión de Internet de forma inmediata, por lo que la transición será un proceso largo y gradual, facilitado en un primer momentos la interconexión de nodos IPv6 con nodos IPv4. Por lo anterior habrá un lógico periodo de transición, durante el cual ambos protocolos de Internet deberán coexistir.

La migración al nuevo IP en tan corto periodo de tiempo requeriría la redefinición de un plan de direccionamiento IPv6 mundial, la instalación del protocolo en cada router y nodo, y la modificación de las aplicaciones actuales para que puedan soportarlo. Un proceso caro, sin duda, y que podría causar interrupciones del servicio inaceptables. No hay una regla universal que pueda ser aplicada al proceso de transición de IPv4 a IPv6. En algunos casos, adoptar directamente, sin pasos previos, el nuevo IP será la única solución. En Asia, por ejemplo, las autoridades políticas están impulsando fuertemente IPv6 a fin de sostener el crecimiento económico de la zona, garantizando a cada ciudadano un número suficiente de direcciones IP. Pero otros planes de transición habrán de asegurar una inter operatividad gradual entre IPv4 y IPv6 a medida que evoluciona la transición. Es obvio que los ISP y las empresas preferirán preservar las grandes inversiones realizadas en redes IPv4.

Algunos estudios pronostican que el periodo de transición finalizará entre 2030-2040; en algún momento de esa década, las redes IPv4 deberían haber desaparecido totalmente. Una historia realmente larga comparada con el rápido crecimiento

experimentado por Internet. La línea de tiempo en la transición se muestra en la figura 6.1.

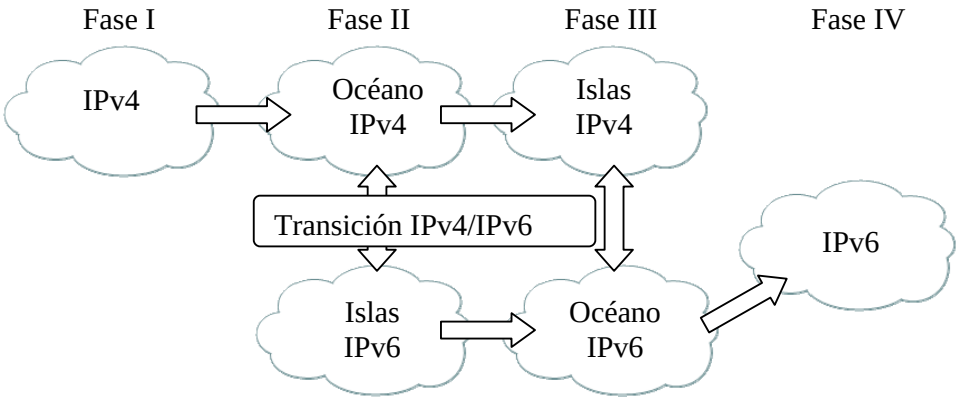


Figura 6.1 Línea de tiempo Transición IP4/IPv6

En general, las aplicaciones legadas por IPv4 necesitaran ser rescritas para soportar redes IPv6, incluyendo dispositivos y elementos de VOIP, por ejemplo Servidores Proxy, terminales, teléfonos, Gateway, gatekeeper y otros equipos utilizados para trasmitir voz sobre paquetes; esto requerirá cambios en las aplicaciones tanto del cliente como del servidor. El Internet es un conglomerado de protocolos globales y estandarizados, por lo que la implementación será progresiva, al principio solo existirán "islas" de redes IPv6 conectadas entre sí, pero será necesario implementar algunos métodos que colaboren con la transición. Para que dicha transición sea exitosa es necesario que exista compatibilidad con los nodos y routers basados en IPv4, de tal forma que sea imperceptible su conexión. La conexión entre redes aplica a todos los tipos de redes basados en IPv4 e IPv6 incluyendo VoIP.

Durante el proceso de migración es importante mantener bajo control la transición para evitar el despliegue de dos infraestructuras Internet paralelas. Los mecanismos aquí descritos implican la utilización de herramientas de ingeniería necesarias para definir estrategias de evolución. Elegir los mecanismos más convenientes, y decidir dónde y cómo desplegarlos no es un proceso sencillo, es preciso definir pautas y directrices que orienten al usuario durante el proceso de transición, en el siguiente apartado se estudian ventajas y desventajas de los métodos de transición. Además se dará una visión global de las técnicas de integración y estrategias de coexistencia definidos por la IETF y otras instituciones de normalización.

6.1 Mecanismos de transición.

La transición a IPv6 no es completamente transparente a lo que se refiere a las capas superiores de IP. Las direcciones son más largas que las direcciones IPv4, lo que requiere de un cambio en la aplicación de las estructuras de los datos más que en la asignación de direcciones, como consecuencia, las interfaces programadas en las aplicaciones finales deben ser extendidas para dar soportar tanto a IPv4 como IPv6, así como la habilidad de seleccionar el protocolo apropiado para cada comunicación entre usuarios. Se debe proveer que este proceso de transición

evolucionara y tomara la forma de modos duales, en los cuales cada modo de Internet puede ser tanto IPv4 como IPv6.

Una de las principales preocupaciones durante el período de transición es la interoperabilidad entre las aplicaciones ya existentes y las nuevas desarrolladas para IPv6. En la mayoría de los casos la interoperabilidad de aplicaciones se consigue utilizando nodos que implementen ambos protocolos, es decir, nodos duales que puedan comunicarse utilizando tanto IPv4 como IPv6. Los nodos con pila dual proporcionan un mecanismo para permitir a las aplicaciones IPv4 comunicarse con aplicaciones IPv6 utilizando el protocolo IPv4 para el intercambio de paquetes entre los nodos finales. Sin embargo, en los escenarios en los que la conectividad entre los nodos origen y destino sólo es posible utilizando IPv6, la pila dual no será suficiente para establecer la comunicación y se necesitará algún mecanismo de transición adicional. En aplicaciones de movilidad se exigen mayores características IP, las cuales no son satisfechas con IPv4, como una mayor disponibilidad en el número de direcciones y la facilidad de configuración a usuarios.

La clave del éxito en la transición a IPv6 está en la compatibilidad con la larga base instalada de nodos y routers IPv4. La IETF define en la RFC 2893 un grupo de mecanismos donde los nodos y routers en IPv6 pueden implementar mecanismos de traducción, compatibilidad e interconectividad con nodos y Routers de IPv4. Este documento especifica los mecanismos compatibles con IPv4 que pueden ser ejecutados por nodos IPv6, donde se incluye implementaciones completas de las dos versiones de Internet, y un desarrollo de túneles para transmitir paquetes IPv6 sobre IPv4. Están diseñadas para permitir a los nodos IPv6 mantener una compatibilidad total con IPv4, que mejoraran notablemente el despliegue de IPv6 sobre Internet y facilitar la eventual transición de toda la Internet a la siguiente generación de redes.

Ambos protocolos se estima que convivirán unos 20 a 30 años para que finalmente se tenga una transición completa a IPv6. Sin embargo, el cambio de IPv4 a IPv6 ya es una actualidad en países de Europa y Asia, pero no tiene el impacto necesario como EUA y parte de América, debido al espacio de direccionamiento otorgado por la IANA y técnicas como NAT. El desarrollo de IPv6 en Latinoamérica es para redes académicas e investigación.

Los métodos que permitirán la convivencia y la migración progresiva tanto de las redes como de los dispositivos que integran dicha red, se agrupan en tres componentes mayores:

- Doble Pila.
- Tunales.
- Traductores de protocolos.

La decisión de que método de transición elegir depende de las necesidades de la implementación, de la infraestructura de red y los recursos al alcance del diseño. La RFC 2893 nos proporciona un set de mecanismos de transición iniciales, pero no se espera que estas técnicas sean las únicas disponibles, adicionales técnicas de transición y compatibilidad son esperadas a ser desarrolladas en un futuro, con nuevas RFCs de la IETF y su respectiva documentación, mientras tanto se da un panorama de las técnicas más utilizadas en este momento.

6.1.1 Doble Pila.

La manera más sencilla para que los nodos IPv6 sigan siendo compatibles con nodos IPv4 es mediante el suministro de una completa aplicación IPv4, para lo que la IETF en el RFC 2893 define como método de transición a Dual Stack o Doble Pila, el cual es usado por nodos, servidores y routers, incluyendo tecnologías de VoIP para operar y usar los protocolos IPv4 e IPv6 simultáneamente. Esta técnica fue satisfactoriamente aplicada en transiciones de protocolos pasados, especialmente para el desarrollo de IPv4 dentro de redes IPX de Novel y redes basadas en DECnet y Apple-Talk. En este esquema el nodo de red tiene las dos pilas de protocolo IPv4 e IPv6 operando en el mismo tiempo y se conoce como nodo IPv4/IPv6, tienen la capacidad de enviar y recibir paquetes IPv4 e IPv6. Pueden interoperar con nodos IPv6 usando paquetes IPv4 y también interoperar directamente con nodo solo IPv6 utilizando paquetes IPv6.

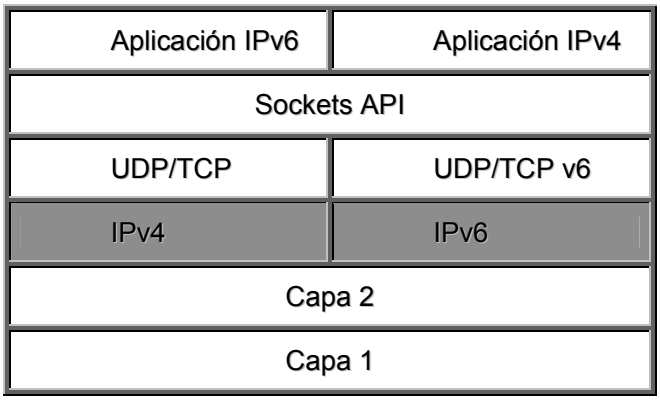


Figura 6.2 Doble Pila.

A pesar de que un nodo pude ser equipado para ambos protocolos, una o otra pila pueden ser deshabilitados por razones de operación. Así nodos IPv4/IPv6 pueden operar de las siguientes formas:

- Con pila IPv4 habilitada y su pila IPv6 deshabilitada.
- Con pila IPv6 habilitada y su pila IPv4 deshabilitada.
- Con ambas pilas habilitadas.

Los nodos con su pila IPv6 deshabilitada operan como nodos IPv4, de forma similar cuando la pila IPv4 es deshabilitada. La Pila Doble puede o no ser usada en conjunto con técnicas de Túnel IPv6 sobre IPv4. Un nodo IPv6/IPv4 tiene tres métodos de soportar túneles:

- Nodos IPv6/IPv4 que no realizan túnel.
- Nodos IPv6/IPv4 que realizan túnel configurado.
- Nodos IPv6/IPv4 que realizan túnel automático y configurado.

El Dual Stack significa que en una instancia de red, como un Servidor Proxy o teléfono IP, puedan establece comunicación en ambos protocolos de Internet. Una aplicación de usuario sobre UDP deberá decidir si usar IPv4 o IPv6. El beneficio de esta herramienta es que los protocolos de la capa de transporte, por ejemplo TCP/UDP, son los mismos para ambas versiones de Internet. Actualmente terminales de usuario con telefonía IP son capaces de soportar ambas pilas de protocolos en el mismo tiempo, en la figura 6.2 se muestra un sistema operando.

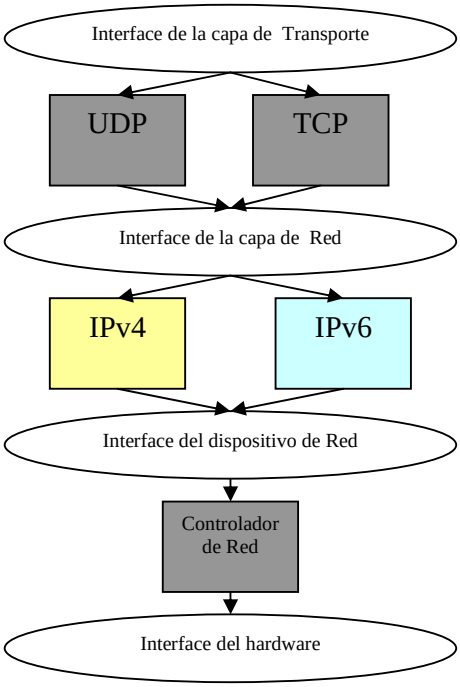


Figura 6.3 Sistema Operando con Dual Stack.

Un equipo que ha implementado el mecanismo de transición Dual Stack tiene la desventaja de necesitar dos direcciones de red, una para IPv4 y otra para IPv6. En el caso de VoIP se puede aplicar este método dentro de la interface de red de cada teléfono IP o en los elementos de control de llamada y señalización. Esta herramienta de coexistencia no puede decidir por sí mismo que pila de protocolo utilizar para comunicarse con otros nodos. Existen métodos para forzar a un nodo usar el protocolo IPv4 cuando la conexión IPv6 esté disponible o viceversa.

Debido a que la pila dual soporta ambos protocolos, cada nodo IPv4/IPv6 debe ser configurado con dos direcciones, una dirección de Internet versión 4 y otra versión 6, para la configuración de las direcciones IPv4 se utilizan mecanismos como DHCP, mientras que para IPv6 se utilizan mecanismo diferentes, por ejemplo la autoconfiguración o configuración compatibles con ambas versión de Internet.

Un nodo IPv4/IPv6 con una dirección IPv4 compatible utiliza esa misma dirección como una dirección IPv6 incluyéndola en los últimos 32 bits y se representa de la siguiente forma:

X:X:X:X:X:X:d.d.d.d

donde X representa valores hexadecimales de las primeras seis partes mas significativas , de 16 bits cada una y d son valores decimales de las 4 partes menos significativas, cada uno de 8 bits, y que corresponde a los octetos de una dirección IPv4 estándar.

Un nodo dual debe de adquirir su dirección tipo compatible vía cualquier mecanismo de adquisición, una característica de estas direcciones es su prefijo nulo de 96 bits: 0:0:0:0:0:0. Basándonos en la RFC 2893, se define los siguientes mecanismos para obtener una dirección IPv4 compatible con IPv6:

- DHCP.

- BOOTP.
- Configuración manual.
- Algún otro mecanismo, el cual incluye en el nodo la ya existente IPv4.

Esencialmente el objetivo de este mecanismo es que un nodo IPv6 obtenga su dirección IPv4 para establecer comunicación con un nodo que maneje solo direcciones IPv4. Permite ejecutar aplicaciones IPv4 sin modificación alguna y solo se puede aplicar dentro de una red IPv6. Se compone de dos métodos: a) La asignación de direcciones IPv4 a nodos IPv6, b) Una interface DTI (Dynamic Tunneling Interface), diseñada para encapsular paquetes IPv4 dentro de paquetes IPv6. Por otra parte, la arquitectura, como se muestra en la figura 6.4, está constituida por tres elementos:

1) DSTM Client. El cual es un nodo de red IPv6 con Dual Stack.

2) DSTM Server. Es un servidor que proporciona un grupo de direcciones IPv4 como respuesta a la solicitud de una dirección IPv4 de un DSTM Client y guarda el mapeo de IPv6 a IPv4 en su memoria local. Las direcciones asignadas son temporales y generalmente el servidor se utiliza DHCPv6.

3) DSTM TEP (Tunnel End Point). Es un router frontera con una interface DSTM TEP configurada. Este equipo comunica el dominio IPv6 aun dominio exterior o al Internet, se encarga de desencapsular el trafico IPv4 en el trafico IPv6 recibido desde los nodos IPv6 y reenvía los paquetes a la red IPv4. También desencapsula trafico IPv4 desde un nodo IPv4 y reenvía estos paquetes al nodo IPv6 destino.

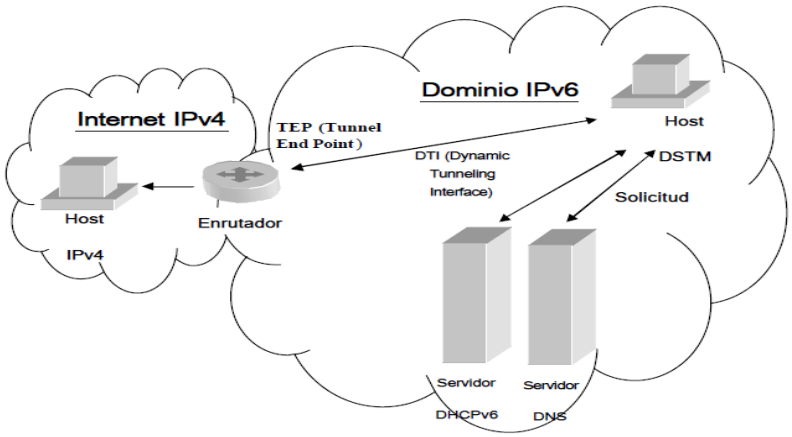


Figura 6.4 Arquitectura Dual-Stack.

El funcionamiento parte del nodo DSTM, el cual se hace una solicitud de dirección IPv4 el servidor de direcciones, para establecer una comunicación con un nodo fuera de la red, para la comunicación con un nodo dentro de la misma red no es necesario solicitar una dirección IPv4.

El servidor de direcciones le asigna una dirección IPv4 temporalmente al nodo de doble pila. El tiempo de esa asignación debe ser indicado en la respuesta del servidor al nodo, así como la dirección IPv6. Si un nodo requiere más tiempo, deberá realizar una nueva solicitud al servidor de direcciones. Este servidor se encargara de mapear las direcciones IPv4 asignadas a la dirección IPv6 correspondiente, es decir, relacionar ambas direcciones. Como una extensión del proceso de asignación de direcciones, el servidor puede asignar un rango de puertos a utilizar por el nodo. Esto permitirá que solo una dirección IPv4 pueda ser utilizada por varios nodos al mismo

tiempo, evitando que los puertos se traslapen. Con la dirección IPv6 del TEP, el nodo se encargara de configurar una interface DTI hacia el TEP, encapsulando los paquetes IPv4 dentro de paquetes IPv6. Si la interface no ha sido configurada, es decir que no tiene asignada una dirección IPv4, el proceso deberá detenerse hasta obtener una dirección IPv4 del servidor de direcciones. Todo el trafico IPv4 puede ser dirigido a esta interface por medio de una entrada en la tabla de enrutamiento del nodo. Una vez que la dirección IPv4 ha sido asignada, es utilizada como dirección fuente para todos los paquetes que sean enviados desde esa interface.

Por último, el nodo manda los paquetes encapsulados hacia el TEP, generalmente el enrutador frontera, quien se encarga de desencapsular los paquetes y reenviarlos hacia la red exterior o el Internet, de modo que lleguen al nodo solicitado por el nodo con doble pila.

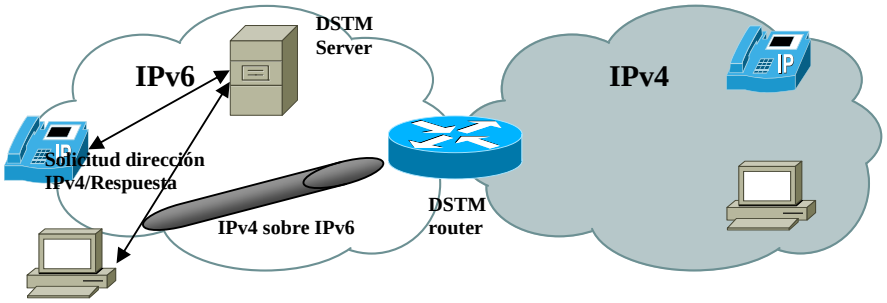


Figura 6.5 Flujo de Dual-Stack.

La doble pila es un mecanismo bidireccional, permite que un nodo Dual Stack dentro de un dominio IPv6 se comunique con un nodo exclusivamente IPv4, o en caso contrario que un nodo IPv4 se pueda comunicar con un nodo Dual Stack dentro de un dominio IPv6. En el primer caso, el nodo DSTM solicitara una resolución de dirección de tipo AAAA para el nodo con el que quiere establecer comunicación, debido a que el nodo no es IPv6, el servidor DNS le devolverá un error de resolución, es entonces cuando el nodo solicitara una dirección IPv4 para poder establecer la comunicación. En el segundo caso, cuando el nodo es IPv4 y desea establecer un canal de comunicación con un nodo IPv6, el nodo IPv4 solicitara una resolución de dirección de tipo A para el nodo DSTM al servidor DNS dentro de su red IPv4. El servidor DNS se comunica con el router DSTM, el cual solicita al servidor de direcciones de dominio IPv6 que se le asigne temporalmente una dirección IPv4 al nodo solicitado para entablar la comunicación.

El nodo IPv4/IPv6 debe de ser capaz de interoperar directamente con nodos IPv4 e IPv6, de tal manera que se debe proporcionar recursos capaces de tratar con registros A para IPv4 y registros AAAA para nodos IPv6, cuando se resuelve una solicitud del registro A o AAAA a una dirección IPv6, la respuesta que se entrega a la aplicación esta influenciada en el orden a la versión de paquetes IP usados para comunicarse con el nodo, se tiene tres alternativas:

- Regresar solo la dirección IPv6 a la aplicación.
- Regresar solo la dirección IPv4 a la aplicación o
- Regresar ambas direcciones a la aplicación.

Si se regresa solo la dirección IPv6 la aplicación se comunicara con un nodo IPv6, si se regresa solo la dirección IPv4 la aplicación se comunicara con un nodo IPv4, pero si se regresan ambas direcciones la aplicación decidirá que dirección usar y

que versión de protocolo IP empleara. En el último caso, la aplicación decide el orden de las direcciones entregadas.

6.1.2 Tunneling.

El uso de la pila dual limita el aprovechamiento de todo el campo de direccionamiento que ofrece IPv6, ya que para hacer "compatibles" estos protocolos se utilizan direcciones IPv4 compatibles. Según el RFC 2473 define el IPv6 tunneling como una técnica para establecer enlaces virtuales entre dos nodos IPv6 para transmitir paquetes de datos como la carga útil de paquetes IPv4. Desde el punto de vista de un nodo, este enlace virtual es lo que se conoce como túneles IPv6 y actúan como un enlace punto a punto, donde IPv6 actúa como un protocolo de capa de enlace. Los dos nodos tienen un papel especifico, uno de ellos encapsula los paquetes recibidos de otros nodos y reenviarlos por el túnel, el otro nodo funciona como desencapsulador y reenvía el paquete original a su destino final. El nodo encapsulador es llamado nodo de entrada o entrada del túnel, mientras que el nodo desencapsulador es llamado nodo de salida o destino del túnel.

Un túnel IPv6 es un mecanismo unidireccional, el flujo de paquetes tiene lugar solo en una dirección entre el nodo de entrada y el nodo de salida. Si desea un mecanismo bidireccional es necesario fusionar dos mecanismos unidireccionales, configurando dos túneles, cada uno en dirección opuesta al otro, el nodo de entrada de un túnel es el nodo de salida del otro túnel. Esta técnica es recomendada para comunicar redes IPv6 a través de una red IPv4.

Este método permite encapsular trafico IPv6 dentro de paquetes IPv4 utilizando las infraestructura de IPv4, permitiendo que sistemas finales de IPv6 aislados, terminales (teléfonos IP), servidores (Proxy Servers) o routers se comuniquen sin necesidad de actualizar los elementos de red IPv4 existentes, como se muestra en la figura 6.6 un túnel esta desarrollado entre dos islas compuestas de nodos IPv6 sobre una red IPv4 como lo es el Internet.

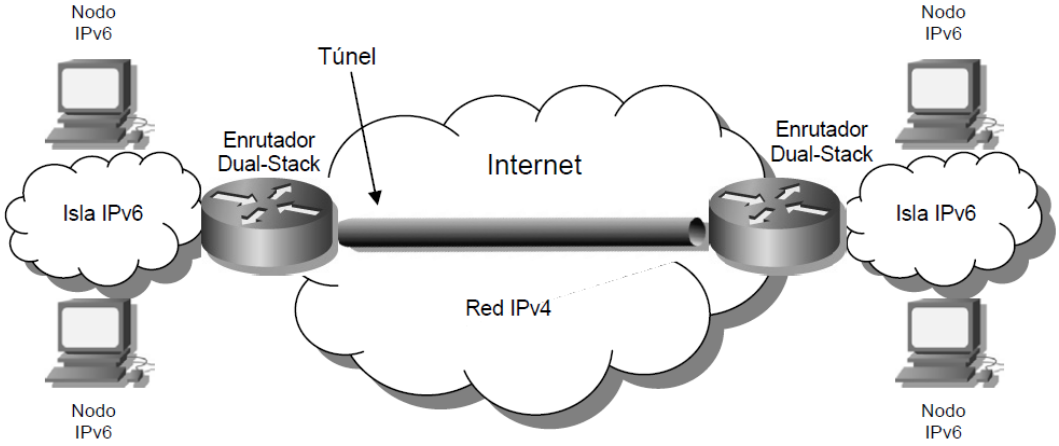


Figura 6.6 Tunneling.

En la RFC 2893, IPv6 Transition Mechanisms, el numero de protocolo asignado a la encapsulación de paquetes IPv6 en IPv4 es el numero 41, este valor es utilizado en el encabezado del paquete IPv4 dentro del campo Numero de protocolo para especificar la encapsulación de un paquete IPv6 sobre un paquete IPv4. Existen cuatro escenarios para la creación de un túnel, los cueles se describen a continuación:

Router-Router. Los routers IPv6/IPv4 son interconectados através de una infraestructura IPv4 para intercambiar paquetes IPv6 entre si. El túnel abarca un segmento del trayecto que toma el paquete IPv6, cada router debe de tener configurado la doble pila y son utilizados para interconectar islas IPv6.

Nodo-Router. Los nodos IPv6/IPv4 pueden intercambiar paquetes IPv6 por un router IPv6/IPv4 intermediario que sea alcanzable por a infraestructura IPv4. Este tipo de túnel abarca el primer segmento del trayecto del paquete. El router puede tener conectividad IPv6 nativa por otra interfase, permitiendo el establecimiento de sesiones IPv6 extremo a extremo entre cualquier nodo de la isla IPv6.

Nodo-Nodo. Los nodos IPv6/IPv4 interconectados con una infraestructura IPv4 pueden intercambiar paquetes IPv6 entre sí. En ese caso, el túnel abarca el recorrido completo que toman los paquetes, ambos nodos debes de tener la doble pila configurada.

Router-Nodo. Los routers IPv6/IPv4 pueden intercambiar paquetes IPv6 hasta el nodo IPv6/IPv4 destinatario. Este túnel abarca el último recorrido del segmento de red.

En la figura 6.7 se muestran tres de los cuatro escenarios para emplear el mecanismo de Tunneling, en el primer caso se muestra la generación de un túnel nodo-nodo; el segundo caso presenta la generación de un túnel nodo-router, el último caso muestra la generación de un túnel router-router.

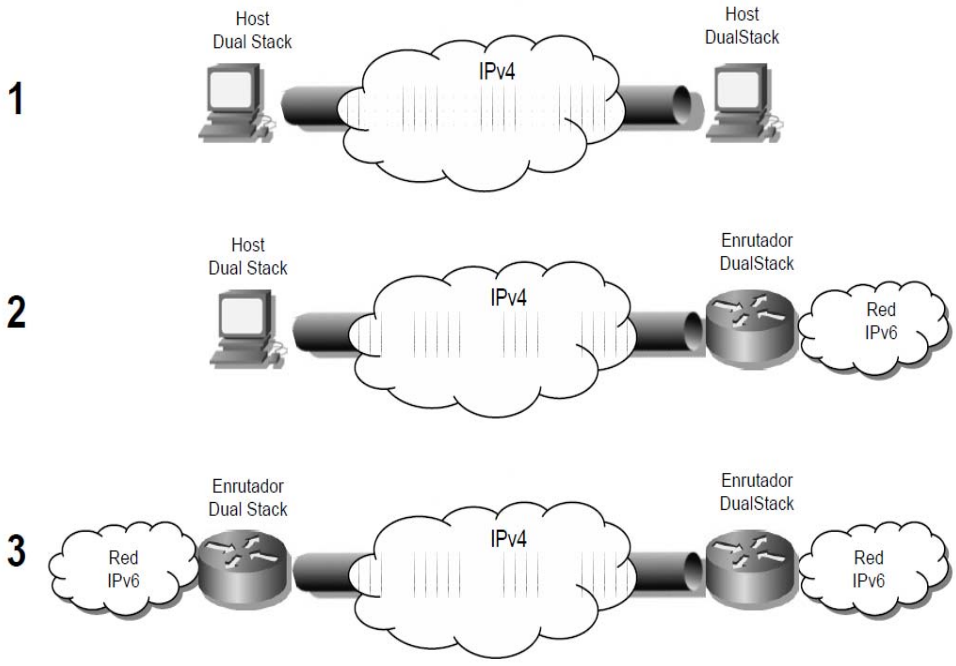


Figura 6.7 Escenarios del Tunneling.

Las técnicas de tunneling se clasifican según el mecanismo por el cual el nodo de encapsulamiento determina la dirección del nodo al final de túnel. En los primeros dos casos (Router-Router y Nodo-Router) el paquete IPv6 es enviado a un router. El punto final de este tipo de túneles es un router intermediario, el cual debe desencapsular el paquete IPv6 y reenviarlo a su destino final. Cuando se envían los

paquetes a un router, el punto final del túnel es distinto del destino final del paquete que se está enviando. Así, la dirección del paquete IPv6 que se envía no provee la dirección IPv4 del punto final del túnel, de tal forma que dicha dirección deberá obtenerse de la información de configuración en el nodo que ejecuta el tunneling. Por lo tanto, se utiliza el término "tunneling configurado" para describir el tipo de túneles donde el punto final esta explícitamente configurado.

En los dos últimos casos (Nodo-Nodo y Router-Nodo) el punto final del túnel es el nodo al cual el paquete IPv6 esta direccionado. Por lo tanto, el punto final puede ser determinado por la dirección IPv6 de destino que contiene el paquete. Si dicha dirección es una dirección IPv6 compatible con IPv4, entonces los últimos 32 bits especifican la dirección del nodo de destino y se puede usar como dirección del punto final el túnel. De esta manera se evita configurar explícitamente de la dirección del punto final. Esta técnica es llamada túnel automático.

Las técnicas de tunneling se diferencian principalmente en cómo se valen para determinar la dirección del punto final del túnel, los escenarios son:

- El nodo de entrada del túnel (nodo de encapsulamiento) crea un paquete IPv4 en el que encapsula el paquete IPv6 y lo transmite encapsulado.

- El nodo de salida del túnel (nodo de desencapsulamiento) recibe el paquete encapsulado, reensambla el paquete si es necesario, elimina la cabecera IPv4, actualiza la cabecera IPv6 y procesa el paquete IPv6 recibido.

- El nodo encapsulador puede necesitar mantener información por cada túnel grabado, por ejemplo el MTU de cada túnel para procesar los paquetes IPv6 reenviados dentro del túnel.

Los tipos de túneles están determinados por la IETF, quien definió protocolos y técnicas para establecer túneles entre nodos con doble pila, específicamente para el protocolo IPv6; la siguiente lista proporciona información de los protocolos y técnicas que están diseñados para el establecimiento de túneles en una red.

- Túnel Configurado.
- Túnel Broker.
- Túnel Server.
- Túnel GRE.
- 6to4.
- ISATAP.
- Túnel Automático con direcciones IPv4 compatibles.

Todas estas técnicas requieren que los puntos finales del túnel soporten direcciones IPv4 e IPv6 y deben estar configurados con Pila dual. Los routers con Dual Stack tienen configurados ambos protocolos simultáneamente y pueden interoperar directamente con sistemas, nodos y dispositivos de red finales en IPv4 o IPv6.

Túnel configurado. Los túneles configurados son habilitados y configurados estáticamente sobre nodos con doble pila. Debido a que esta técnica fue uno de os primeros mecanismos de transición soportados por IPv6, este es el más soportado por todas las implementaciones IPv6 disponibles. En cada extremo de un túnel

configurado las direcciones IPv4 e IPv6 deben ser asignados manualmente para configurar la interese del túnel. Las direcciones asignadas a la interfaz del túnel pueden ser:

- IPv4 Local. Es una dirección IPv4 por el cual el nodo local con doble pila puede ser alcanzado sobre la red IPv4. la dirección local IPv4 es usada como dirección IPv4 origen para el tráfico de salida.
- IP del oro extremo. Es una dirección IPv4 por el cual el otro nodo con pila dual puede ser alcanzado sobre una red IPv4. la dirección IPv4 del extremo es usada como el destino IPv4 para tráfico de salida.
- IPv6 Local. La dirección es asignada localmente a la interface del túnel.

Un túnel configurado equivale a un enlace permanente entre dos dominios IPv6 sobre una infraestructura IPv4, por lo que se considera como un enlace punto a punto. También, ofrece seguridad entre los nodos debido a que las direcciones origen y destino son bien conocidos y por lo tanto se pueden habilitar reglas de seguridad en un equipo de red, como el firewall o un router.

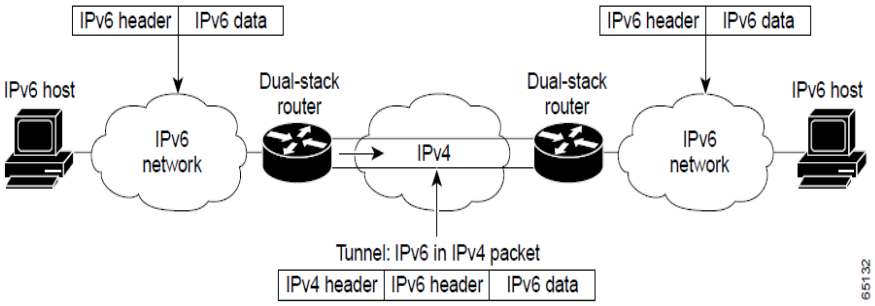


Figura 6.8 Túnel Configurado.

Túnel Broker. La EITF definió este mecanismo para facilitar el desarrollo de túneles configurados sobre redes IPv4, ya que mediante este tipo de túnel no se tiene que configurar manualmente cada extremo. Tal como está establecido en el RFC 3053 "IPv6 Tunnel Broker", este túnel es un servicio extremo-extremo que actúa como un servidor sobre IPv4 y recibe peticiones de nodos con doble pila para configurar túneles automáticamente, funcionando como un modelo cliente-servidor. Estas peticiones son enviadas vía HTTP sobre IPv4 por el nodo que desea configurar dicho túnel. El túnel Broker envía información de vuelta al nodo-cliente, tal como la dirección IPv4 del servidor túnel, la dirección IPv6 del servidor, la nueva dirección IPv6 que será asignada a este nodo con pila dual y las rutas IPv6 de default para la configuración del túnel. Algunos túneles broker ya proporcionan scripts de configuración para los nodos de los clientes. Finalmente, aplica comandos de manera remota sobre un router con pila dual y que esté conectado a un dominio IPv6 para habilitar el túnel configurado.

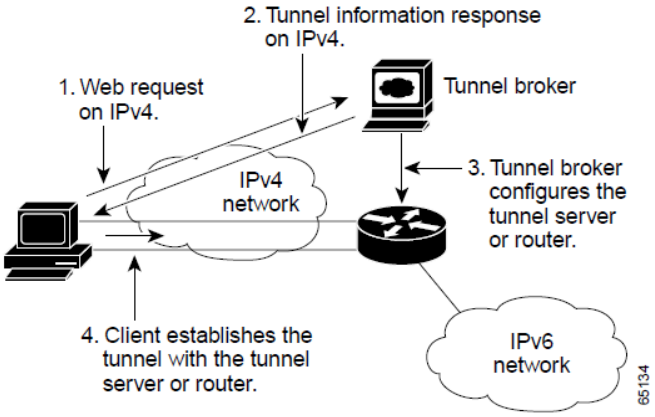


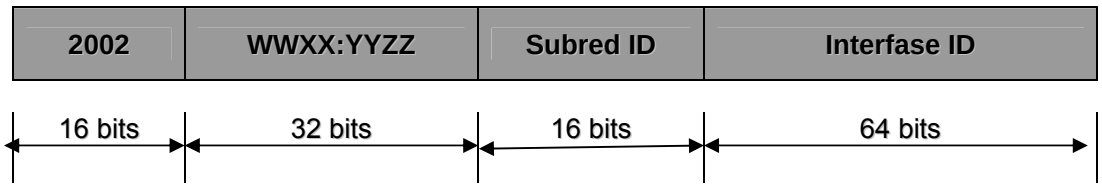
Figura 6.9 Túnel Broker.

Los túneles broker ofrecen un servicio de manera gratuita, el único requisito es registrarse mediante un pequeño formulario sobre servidores de la WEB. La desventaja e esta técnica es que en los sistemas finales o routers aceptan un cambio de configuración desde un servidor remoto con las implicaciones de seguridad que esto implica.

Túnel Server. El servidor de túnel es un modelo simplificado del túnel Broker. El servidor de túnel combina el router broker y el router con doble pila en la misma entidad. La forma de solicitar un túnel configurado es generalmente la misma como con el Túnel Broker. Debido a que el router Broker y el de doble pila se encuentran dentro del mismo dispositivo, el servidor de túnel es considerado un modelo abierto que puede permitir el desarrollo de nuevos protocolos de control y señalización para el establecimiento de túneles configurados.

El Túnel Broker y el Túnel Server son mecanismos para automatizar el despliegue de túneles configurados para nodos con doble pila sobre dominios de ruteo IPv4 sin operación manual.

6to4. La EITF define oro mecanismo llamado &to4 para facilitar el despliegue de redes IPv6 sobre IPv4 a través de túneles. Este mecanismo es una asignación de direcciones y una tecnología de túnel automático para escenario s Router-Router, Nodo-Router y Router-nodo definido en el RFC 3056, es usado para proporcionar conectividad unycast IPv6 entre sitios IPv6 y nodos a través del Internet IPv4. Permite que dominios aislados IPv6 se comuniquen con otros dominios IPv6 con una mínima configuración. Un túnel 6to4 utiliza un prefijo asignado por la IANA para designar los sitios participantes. Las direcciones 6to4 consisten de lo siguiente:



donde:

- El espacio reservado para túneles 6to4 es 2002::/16.

- WWWW:YYZZ es una representación hexadecimal de una dirección publica IPv4 asignada para un nodo o sitio sobre Internet IPv4.
- Subred ID es usado dentro de una red privada para enumerar subredes individuales.
- Interface ID identifica a un nodo sobre una subred dentro de una red privada.

Un sitio IPv6 aislado se asignara así mismo una dirección global con un prefijo 2002:ADDR-IPv4::/48, donde el prefijo tiene el mismo formato que un prefijo normal /48, y por ello permite a un dominio IPv6 usarlo como cualquier otro prefijo, /48 valido. Es un escenario en donde dominios 6to4 quisieran comunicarse entre sí, no es necesaria la configuración explicita de los túneles. Las direcciones IPv4 en los extremos del túnel son determinados al extraerlos del prefijo global IPv6 de la dirección destino del paquete IPv6 a transmitir. Los routers 6to4 no necesitan utilizar ningún protocolo de enrutamiento IPv6, pues el enrutamiento IPv4 es el encargado de realizar esta tarea, lo anterior descrito se ve en la figura 6.10.

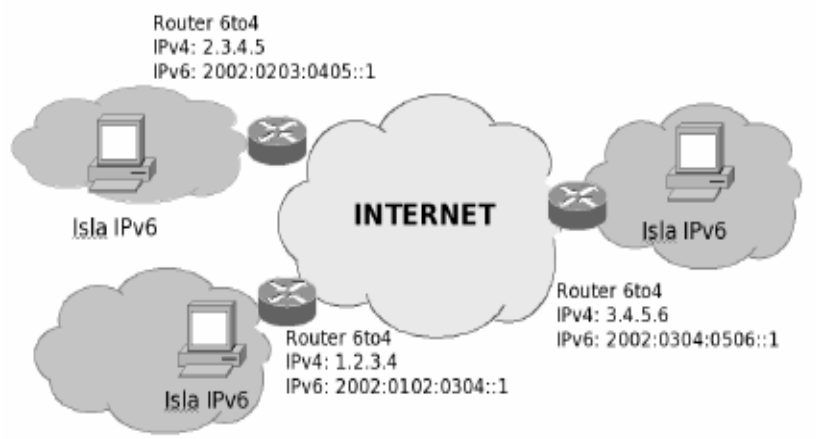


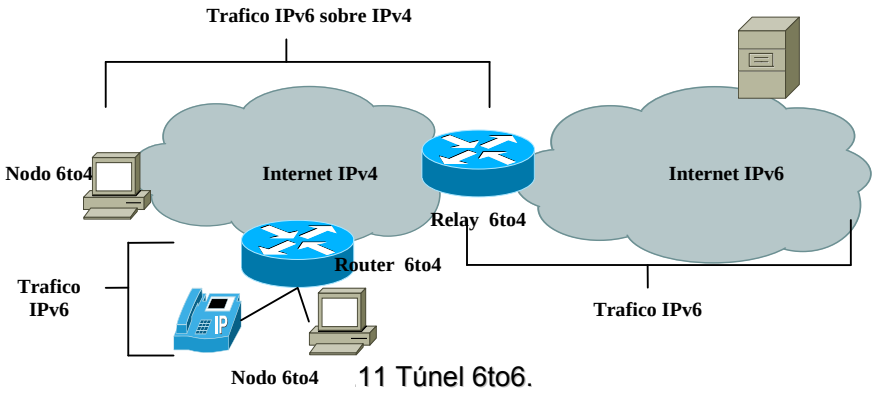
Figura 6.10 6to4.

Los componentes que constituyen un túnel 6to6 son nodos 6to4, routers 6to4 y routers relay, los cuales se describen a continuación:

1. Nodo 6to4. Es un nodo IPv6 nativo que es configurado con por lo menos una dirección 6to4. Un nodo 6to4 no tiene una interface 6to4 y no realiza tunneling.

2. Router 6to4. Es un router IPv6/IPv4 que usa una interface de túnel 6to4 para reenviar trafico 6to4 entre los nodos dentro de una red, entre otros routers 6to4 o routers relay 6to4 a través de Internet versión 4.

3. Router Relay 6to4. Es un router IPv6/IPv4 que reenvía trafico 6to4 entre routers 6to4 y nodos sobre IPv4 y a nodos sobre IPv6. Este router tiene al menos una interface 6to4 y otra interface de IPv6 nativa.



11 Túnel 6to6.

Cuando los dominios 6to4 desean comunicarse con dominios IPv6 nativos, la conectividad es manejada por medio de routers relay, el cual debe usar un protocolo de enrutamiento exterior IPv6. Un Router Relay publica el prefijo 2002::/16 en su ruteo IPv6 nativo y adicionalmente puede publicar rutas IPv6 nativas en su interfase 6to4.

Existen varios inconvenientes en esta técnica, una de las es que solo se permite enviar trafico IPv6 entre nodos con prefijos de enrutamiento 2002::/16. Además, el uso de direcciones como 10.0.0.0/8, 172.0.0.0/12 y 192.168.0.0/16 están prohibidas para el desarrollo de un router 6to4 sobre Internet; sin embargo, el uso más común de 6to4 es para routers de frontera.

Tunel GRE. Esta técnica fue desarrollada originalmente por CISCO para transportar trafico multicast sobre redes unicast y protocolos como IPX y AppleTalk sobre IP, pero también puede transportar tráfico IPv6 sobre redes IPv4. En cada extremo del túnel no mantienen ningún tipo de información sobre el estado o la disponibilidad del extremo del túnel remoto. GRE no utiliza TCP o UDP, en su lugar trabaja directamente con la capa IP y utiliza el número de protocolo 47. Incluye sus propios mecanismos para verificar la entrega e integridad de los paquetes. La carga de un paquete GRE incluye un paquete de capa 3 completo con su encabezado y carga intactos. El enrutador en la entrada del túnel GRE toma los paquetes IP y los envuelve en un nuevo paquete con un encabezado GR, después los envía por la red hasta que alcanzan el router de la salida del túnel. El router de salida extrae el paquete contenido dentro del paquete GRE y lo entrega l nodo destino. Esta herramienta de transición está definido en el RFC 1701-2, 2460 y 2784 de la EITF. Un paquete GRE encapsulado tiene la forma que se muestra en la figura 6.12.

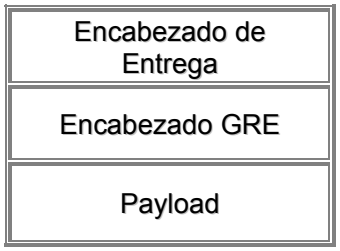


Figura 6.12 Paquete GRE.

ISTAP (Intra-Site Automatic Tunnel Addressing Protocol). Es un mecanismo de transición de IPv6 para transmitir paquetes de IPv6 entre nodos con doble pila sobre redes IPv4, creando una red virtual IPv6 sobre una red IPv4. Es un protocolo de asignación de direcciones y creación de túneles automáticos definido en

la RFC 4214, ofrece conexiones unicast IPv6 entre nodos IPv6/IPv4 a través de una red IPv4. La dirección asignada a nodos y routers ISATAP se determina mediante la concatenación del prefijo IPv6 FE(=::5EFE con los 32 bits de la dirección IPv4. Las direcciones IPv4 deben ser únicas y si es usada para acceder a Internet deberá ser global. Los nodos ISATA deben configurar una lista de routers posibles (PRL Potencial Routers List), los cuales son sondeados por un mensaje ICMPv6 de descubrimiento de router. Como la dirección IPv4 siempre esta embebida dentro de la dirección IPv6, la resolución de direcciones es trivial. Se debe de tener en cuenta que para que funcione la solicitud de Routers, los nodos deben de haber aprendido de alguna manera las direcciones IPv4 de los posibles Routers ISATAP, por ejemplo DCHP, DNS o configuración manual. El Router siempre envía mensajes de anuncio de manera unicast y solo enviara regularmente solicitudes a los routers ISATAP que conozca.

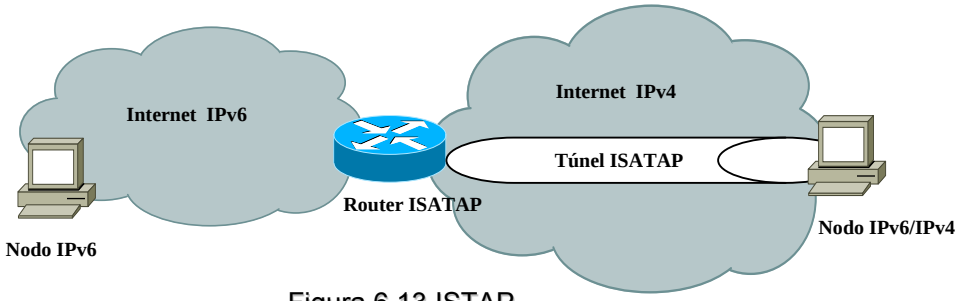


Figura 6.13 ISTAP.

Túnel automático con direcciones Ipv4 compatibles. Es otra técnica para transportas paquetes IPv6 sobre redes IPv4, fue uno de los primeros mecanismos de transición definido por la IETF. Este túnel debe ser configurado entre routers frontera o bien entre routers frontera y sistemas finales. Cada punto final del túnel, ya sea router o sistemas, deben de tener implementada la doble pila. En un este tipo de túnel el nodo origen y el nodo destino son automáticamente determinados por las direcciones IPv4. La dirección IPv6 es tiene como característica que los bits de mayor orden son determinados por el prefijo 0:0:0:0:0:0 y los últimos 32 bits menor orden es la dirección IPv4; por lo tanto, los 32 bits de bajo orden de las direcciones IPv6 origen y destino representan direcciones IPv4 origen y destino de los puntos finales del túnel.

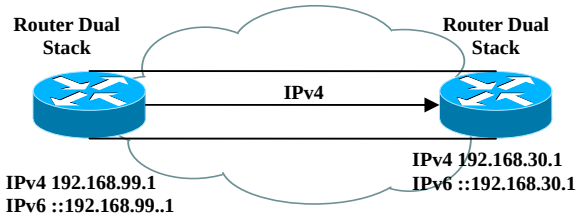


Figura 6.14 Túnel automático con direcciones Ipv4 compatibles

Aunque es una manera fácil de crear túneles para IPv6 sobre IPv4, es un mecanismo que no es escalable para grandes redes, porque cada nodo requiere una dirección IPv4 y una IPv6 disponibles para determinar los puntos finales del túnel, lo que limita el espacio de direccionamiento, además todas las comunicaciones son entre direcciones IPv4 compatibles.

6.1.3.- Traductores

Los mecanismos de traducción se refieren a la conversión directa de los protocolos IPv4 a IPv6 de manera bidireccional y puede incluir una transformación tanto del encabezado como de la carga efectiva del protocolo. La traducción puede ocurrir en diferentes capas de la pila de protocolos, incluyendo la capa de red, transporte y aplicación (Figura 6.15).

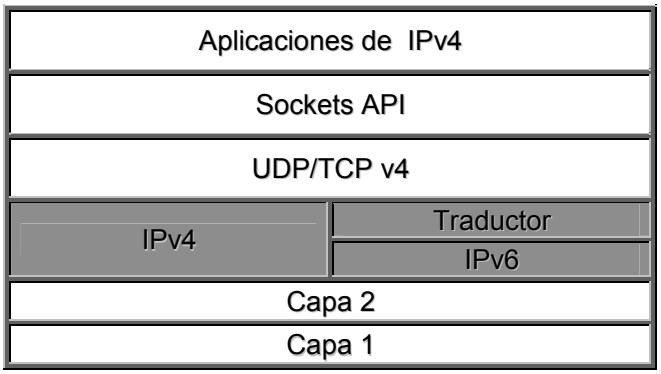


Figura 6.15 Mecanismos de Traducción.

Los traductores empleados en los nodos finales pueden resolver los problemas de interoperabilidad, los cuales son relativamente fáciles de implementar, pero son difíciles de manejar a gran escala. Los traductores propuestos para explicar durante este trabajo son NAP-PT y SIIT.

NAP-PT. Es una técnica de transición que permite a nodos IPv6 nativos comunicarse con nodos IPv4 nativos a través de Internet versión 4. Está definido en la RFC 2766 y es definido como un tipo de NAT que traduce direcciones IPv6 a direcciones IPv4 y viceversa. Está basado en el algoritmo SIIT, el cual traduce el encabezado del paquete IPv4 a IPv6, incluyendo las cabeceras ICMP. Utiliza un grupo de direcciones IPv4, únicas globalmente y no privadas, para ser asignadas dinámicamente a los nodos IPv6 cuando estos inicien una sesión para establecer comunicación con algún otro nodo y no requieren tener la pila dual configurada. Todos los paquetes pertenecientes a una sesión deberán pasar por el mismo router NAP-PT, el cual publica el prefijo ::/96 en el dominio de red para ser identificado. El prefijo es un valor predeterminado que identifica un número de direcciones del mismo tipo.

Una parte fundamental de NAP-PT son los ALGs (Application Level Gateways), opera en la capa de aplicación del modelo OSI y activamente inspecciona el contenido de los paquetes que se transmiten a través de la puerta de enlace. Se utiliza cuando se manejan direcciones IP dentro de la carga de datos del paquete para realizar la traducción. El ALG mas importante es el DNS-ALG, el cual se encarga de mapear las direcciones IPv4 asignadas a un nodo IPv6. Un ALGes una aplicación que permite la traducción de ciertos paquetes que contienen información de direcciones IP y no pueden ser precedidos por el traductor.

Una de las ventajas de NAP-PT es que no requiere cambios en los nodos existentes de la red, debido a que la configuración se realiza en un router, llamado router NAP-PT. En este router se configura un grupo de direcciones IPv4 para ser traducidas, si ese grupo es igual o mayor al número de nodos IPv6, entonces cada nodo IPv6 tendrá una IPv4; si el grupo de direcciones es menor al número de nodos, entonces las direcciones tendrán que ser asignadas dinámicamente. NAP-PT se pueden configurar de las siguientes formas:

NAP-PT Estático. El modo estático proporciona una traducción uno a uno entre direcciones IPv6 y direcciones IPv4. En el router NAP-PT la traducción es similar a NATv4.

IPv6	Traducción	IPv4
2001:a:b:c::1/64	➔	192.168.40.1
2001:a:b:c::2/64	➔	192.168.40.2
2001:a:b:c::3/64	➔	192.168.40.3

Tabla 6.1 NAT-PT Estático.

NAP-PT Dinámico. El modo dinámico permite múltiples mapeos NAP-PT en la asignación de direcciones desde un grupo de direcciones. En el inicio de una sesión NAP-PT una dirección temporal es dinámicamente asignada desde un grupo de direcciones, la cantidad disponible de direcciones determina el número máximo de sesiones al mismo tiempo. El router NAP-PT archiva cada mapeo entre direcciones en una tabla dinámica, la cual se actualiza en cada evento nuevo.

IPv6	Traducción	IPv4
2001:a:b:c::/64	➔	192.168.40.1
	➔	192.168.40.2
	➔	192.168.40.3

Tabla 6.2 NAT-PT Dinámico.

En la figura 6.16 se muestra el proceso de traducción de un paquete enviado desde un nodo IPv6, el cual llega al router NAP-PT y se encarga de traducir el paquete de protocolo y de dirección, y es entregado al nodo IPv4, este proceso se repite cuando el paquete es contestado, pero en proceso inverso.

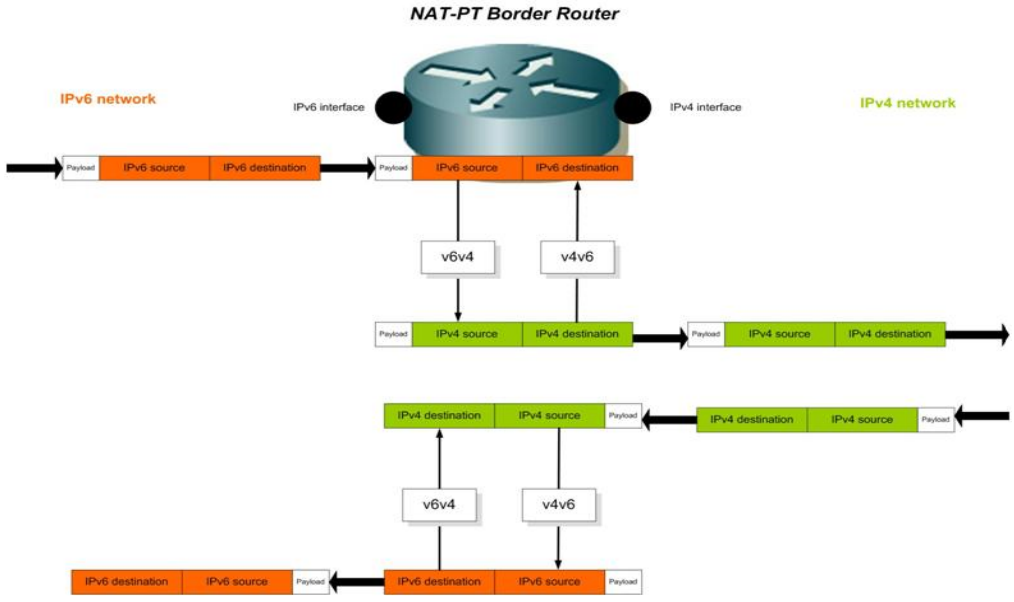


Figura 6.16 Traducción de paquetes en NAP-PT

NAP-PT proporciona un mapeo dinámico entre múltiples direcciones IPv6 en el router NAP-PT y una dirección de IPv4 fuente. Esta traducción es realizada simultáneamente en la capa 3 y en capas superiores. Permite que múltiples nodos IPv6 se comuniquen con nodos IPv4 utilizando una sola dirección IPv4. NAT-PT tiene

varias limitaciones bien conocidas, por ejemplo tiene un punto vulnerable a fallas en el router, no soporta multicast y no proporciona seguridad punto a punto.

SIIT. Es un mecanismo que especifica la traducción de encabezados IP/ICMP entre IPv6 e IPv4, documentado en la RFC 2765 por la IETF, no tienen en cuenta el estado del paquete, por lo que la traducción se realiza por casa paquete. Básicamente, se encarga de traducir las cabeceras entre IPv4 e IPv6, permite la comunicación entre nodos IPv6 e IPv4. El nodo IPv6 obtiene una dirección IPv4 temporal y enmedio e enrutamiento para los paquetes. La dirección IPv4 temporal será utilizada como una dirección IPv6 llamada IPv4-traducida. Después los paquetes pasaran por un traductor SIIT encargado de traducir las cabeceras IPv4 e IPv6 y las direcciones de red. En la RFC la IETF define el método de traducción de paquetes de IPv4 a IPv6, la traducción de encabezados de IPv4 a IPv6, la traducción de IPv6 a IPv4 y la traducción de cabeceras IPv6 a IPv4, los cuales se describe en esta sección.

Traducción de IPv4 a IPv6. Cuando el traductor recibe un datagrama IPv4 que contiene una dirección destino que esta fuera de la red IPv4, entonces traduce el encabezado de ese datagrama por uno IPv6 y lo reenvía basándose en la dirección IPv6 destino. Una descripción básica y rápida de esta traducción consiste en que el encabezado IPv4 del paquete es memorizado y reemplazado por uno IPv6.

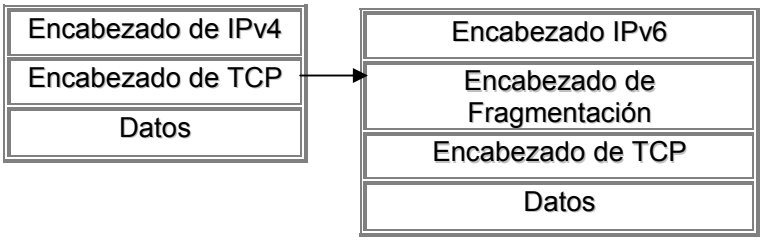


Figura 6.17 Traducción de IPv4 a IPv6

Este proceso de traducción se debe de tomar en cuenta que para IPv6 la detección del camino por MTU es obligatoria, pero para IPv4 es opcional, por lo que la fragmentación, si es necesaria, se haga desde el nodo fuente y se especifique en el nuevo encabezado de IPv6.

Traducción de encabezados de IPv4 e IPv6. Basándose en la RFC 2765, para efectuar la traducción de encabezados de IPv4 a IPv6, los campos de cabecera IPv6 se establecen de la siguiente manera:

Versión	6
Clase de tráfico	Se copian los 8 bits de forma idéntica.
Etiqueta de flujo	Todos los bits en cero.
Longitud total	Se establece restando el valor de la longitud total del encabezado de IPv4 con el tamaño del encabezado de IPv4
Limite de salto	Copiado del valor TTL
Dirección fuente	La dirección fuente IPv4 es colocada en los últimos 32 bits, mientras que los 96 bits de mayor orden restantes son sustituidos por un prefijo ::FFFF:0:0/96
Dirección destino	Se realiza la misma operación que con la dirección fuente, solo que esta vez se utiliza la dirección destino y se utiliza un prefijo diferente

Si la bandera DF (Don't Fragment) en el encabezado IPv4 es cero y el tamaño de paquete es mayor a 1280 bytes el paquete IPv4 debe fragmentarse antes de hacer la traducción. Debido a que los paquetes con DF igual a cero siempre resultaran en un encabezado fragmentado, el paquete IPv4 debe fragmentarse de tal manera que su extensión debe ser al menos 1232 bytes. Si el bit DF esta en uno, el paquete no está fragmentado y no hay necesidad de agregar un encabezado de fragmentación.

Traducción de IPv6 a IPv4. Cuando el traductor recibe un datagrama IPv6 destinado a una dirección IPv4 mapeada, el encabezado IPv6 se traduce a un encabezado IPv4. El encabezado original IPv6 es removido y sustituido por un encabezado IPv4; excepto por paquetes ICMP, el encabezado de la capa de transporte y la porción de datos del paquete se dejan sin cambios.

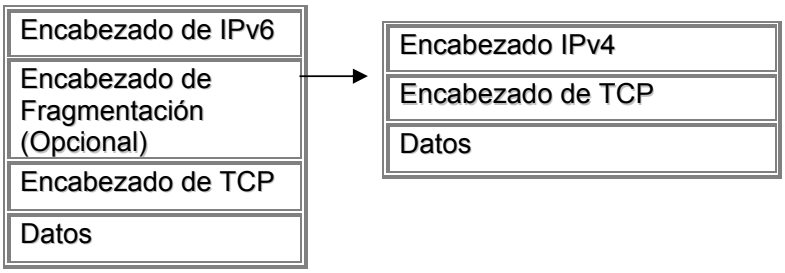


Figura 6.18 Traducción de IPv6 a IPv4.

Existen diferencias entre la fragmentación IPv6 e IPv4 y el mínimo MTU efectúa la traducción. Un paquete IPv6 tiene un MTU mínimo de 1280 bytes. El limite correspondiente para IPv4 es e 68 bytes.

Traducción de cabeceras de IPv6 a IPv4. Cuando el encabezado del paquete IPv6 no está fragmentado, los campos del encabezado IPv4 son configurados de la siguiente forma:

Versión	4
Longitud del encabezado	5
Tipo de Servicio y Procedencia	Copiado directamente del encabezado de clase de Trafico, los 8 bits completos. La semántica utilizada para IPv4 e IPv6 es la misma.
Longitud total	El valor se obtiene sumando la longitud total del encabezado IPv6 más el tamaño del encabezado IPv4.
Identificación	Todos los bits en cero.
Banderas	Las banderas de fragmentación M se configura en 0 y DF en 1.
Offset	Todos los bits en cero
TTL	Copiado del campo limite de salto de IPv6.
Protocolo	Copiado del valor del encabezado siguiente.
CHECKSUM	Calculado una vez que el encabezado IPv6 ha sido creado.
Dirección Fuente	Si la dirección origen es una dirección IPv4 traducida, se toman los últimos 32 bits de la dirección IPv6 fuente y se copian directamente.
Dirección Destino	Los paquetes IPv6 que son traducidos tienen una dirección IPv4 mapeada por dirección destino, los últimos 32 bits son copiados directamente en el campo de dirección destino.

Si el paquete IPv6 contiene un encabezado fragmentado los campos son configurados como se en la parte superior con los las siguientes excepciones:

Longitud total	Se configura como la longitud total del encabezado IPv6 meno 8, correspondiente al encabezado de fragmentación, mas el tamaño del encabezado IPv4.
Identificación	Se copian los últimos 16 bits del campo de identificación del encabezado del paquete fragmentado.
Banderas	La bandera M (Mas Fragmentos) se configura con l valor e la bandera M de IPv6, la bandera DF (No Fragmentado) se configura con 0, permitiendo que los paquetes sean fragmentados por IPv4.
Offset	Se copia del campo Offset del encabezado de fragmentación.
TTL	Copiado del campo limite de salto de IPv6.
Protocolo	Valor del siguiente encabezado copiado desde el encabezado de fragmentación.

6.2 Otros mecanismos de transición.

La EITF ha definido otros mecanismos de transición adicionales a los ya descritos en este capítulo, con el objetivo de que nodos IPv6 intercambien paquetes con nodos IPv4, los descritos en esta sección son BIS, BIA y SOCKS64.

BIS (The Bum-In-the Stack). Este mecanismo es diseñado para trabajar con nodos Dual Stack, utiliza el algoritmo SIIT para traducir paquetes IPv4 a IPv6 y viceversa. Un software es añadido sobre los nodos con doble pila para interceptar y traducir paquetes entre las capas de aplicación y red, cuando recibe paquetes IPv4 desde aplicaciones, IPv4 BIS convierte los paquetes IPv4 a IPv6 y los envía a la red IPv6 usando el protocolo IPv6. BIS es definido en la RFC 2767. Este documento especifica que BIS tiene tres módulos, el primero se encarga de la resolución de Nombre, el segundo es un mapeador de direcciones y el tercero es el traductor de direcciones IPv4 a IPv6.

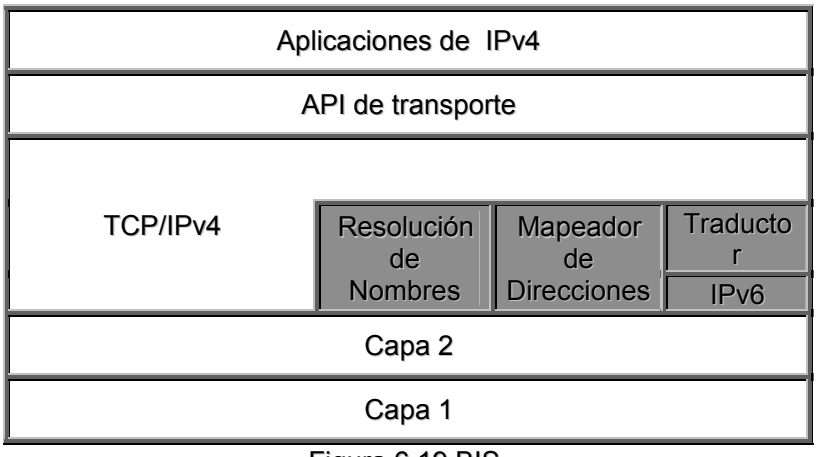


Figura 6.19 BIS.

Este mecanismo es válido para comunicaciones unicast, para sesiones multicast se requiere de otro mecanismo. No puede traducir aplicaciones IPv4 que usen el campo de opciones.

BIA (Bump-In-the-API). Define un mecanismo de transición para permitir a aplicaciones IPv4 don doble pila comunicarse usando IPv6. Es muy similar a BIS, pero la traducción se realiza antes de construir el paquete en la interface de programación de aplicaciones (API). El mecanismo BIA permite que las aplicaciones IPv4 sigan funcionando normalmente sobre una red IPv6, sin que haya que modificar el código fuente, ni recompilarlo. Proporciona direcciones ficticias IPv4 a la aplicación para que sea transparente el hecho de que los nodos remotos son solo alcanzados mediante IPv6. BIA se encarga de mantener la correspondencia entre las direcciones IPv4 ficticias y las direcciones IPv6 reales, su arquitectura consiste de una resolución de nombres un mapeador de direcciones y un mapeador de aplicaciones.

Este mecanismo es válido para comunicaciones unicast, para sesiones multicast se deben considerar una aplicación extra en el modulo de mapeo de direcciones.

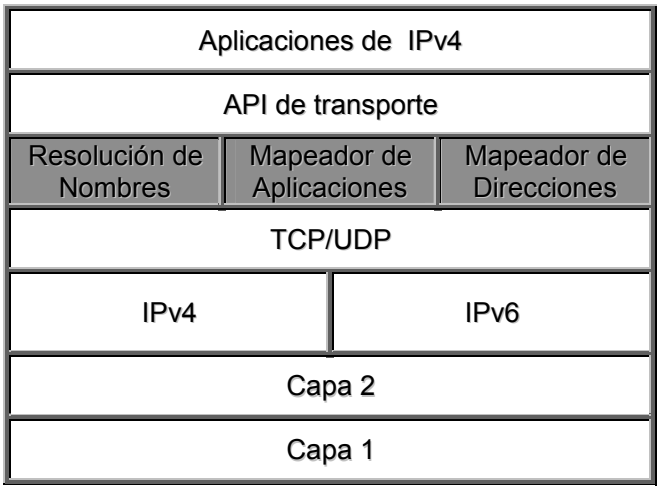


Figura 6.20 BIA.

SOCKS64. Definido en la RFC3089 (A SOCKS-Based IP6/IPv4 Gateway Mechanism), es un mecanismo que permite la comunicación entre nodos IPv6 y nodos IPv4, utiliza un router tipo SOCKS64 con pila dual y aplicaciones con características tipo SOCKS, utilizando una librería especial SOCKS64 que reemplaza APIs y DNS. Esta librería intercepta las sesiones de inicio de búsqueda de DNS a partir de aplicaciones en el sistema final y responde con direcciones ficticias para la sesión solicitada. Es un ambiente Cliente-Servidor, los nodos IPv4 actúan como clientes para comunicarse con servicios IPv6 y viceversa dentro de un servidor de pila dual, en este caso un router.

Para permitir la comunicación, se basa en 2 componentes que deben ser agregados, los componentes son una librería sock y un servidor SOCK. La librería sock es agregada al nodo interno de la red, que desea la comunicación con otros nodos externos. Dentro de esta librería existe una dirección especial denominada "dirección IP falsa", así como una tabla de mapeo. El Servidor sock es el encargado de permitir la comunicación entre el nodo interno de la red y otro nodo externo, es un intermediario entre ambos nodos. Básicamente es un nodo dual que tiene una pila para el protocolo IPv4 y otra para el IPv6.

La dirección "IP falsa" es usada como una dirección IP destino virtual por una aplicación en el nodo interno de la red. Esta dirección es brindada a la aplicación, que se ejecuta en el nodo interno por la librería sock, como supuesta dirección destino del nodo externo con el que desea la comunicación. Esta dirección nunca es utilizada en la comunicación real. Dentro de la librería sock se mantiene un vínculo entre la

dirección real y el nombre lógico del nodo externo. Dicho vínculo es almacenado en la tabla de mapeo existente dentro de la librería sock.

7

Usando IPv6 para soportar 3G VoIP: Arquitectura.

La figura 7.1 muestra los elementos de una red típica en un ambiente empresarial, muchos de los cuales aparecen en una red VoIP. Un número de estos dispositivos requerirán soportar IPv6, especialmente aquellos que se encuentran en la capa 3 del modelo de referencia OSI, cuya función es proporcionar conectividad y una selección de ruta entre dispositivos ubicados en diferente posición geográfica, además del direccionamiento lógico. La simbología utilizada en este trabajo se basa en la tecnología desarrollada por CISCO.

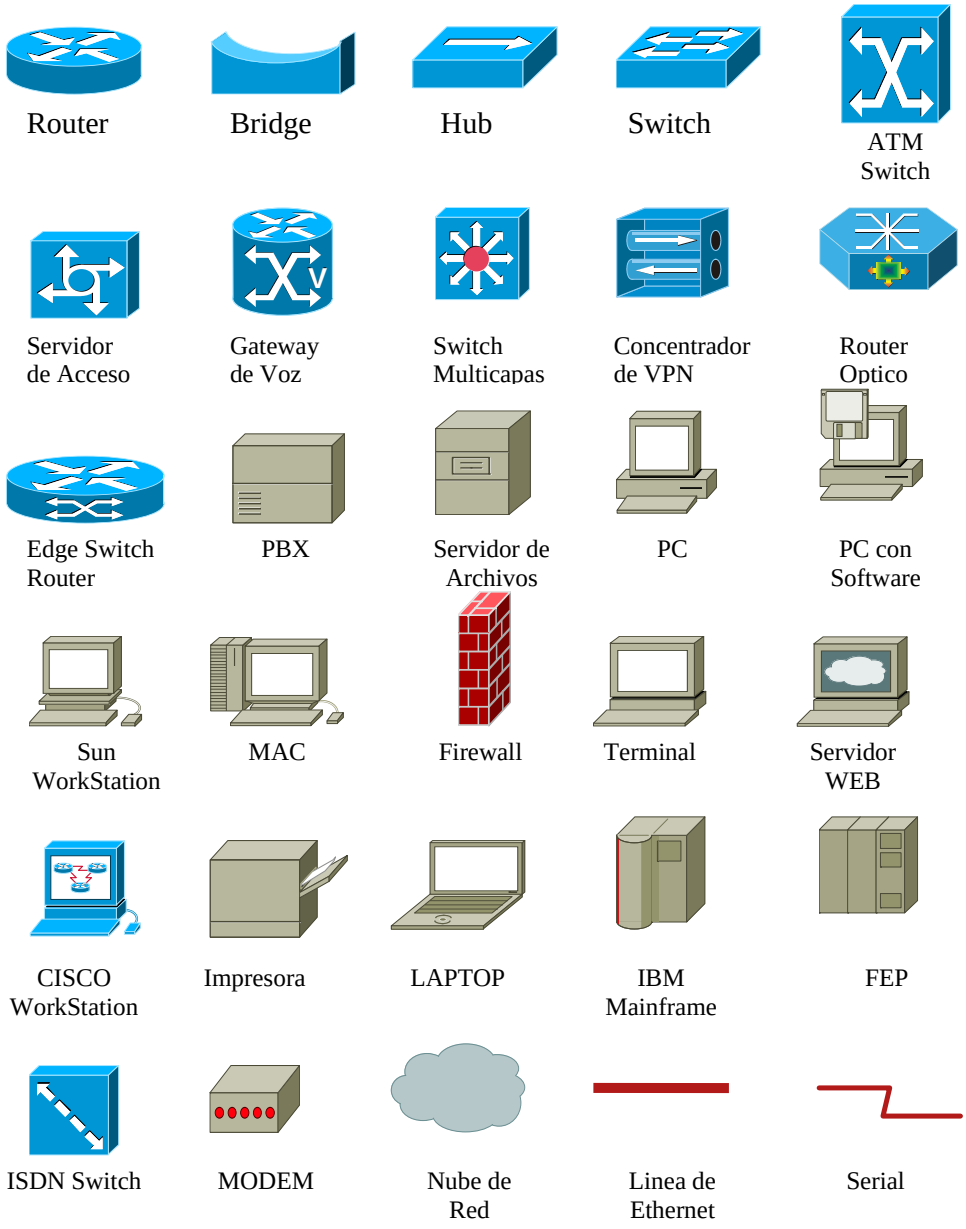


Figura 7.1 Elementos de una red VoIPv6

La figura 7.2 muestra los elementos de una red VoIPv6 implementados en un ambiente empresarial y comercial. La tendencia actual es que cualquier dispositivo en cualquier punto pueda ser alcanzado, no importando el dominio o tipo de red en el que se encuentre. En la actualidad la movilidad es fundamental para cualquier usuario, lo que requiere mayor infraestructura en las redes para soportar la densidad de usuarios que necesitan una conexión a Internet para estar siempre conectados. Todas las aéreas de telefonía serán conectadas atreves de servidores y Gateway que permitan ubicarse en al menos una frontera con algún tipo red, como lo es la PSTN, IPv4, el extinto IPx, IPv6, la red GSM, SS7, Dispositivos WiFI o Otra tecnología Celular.

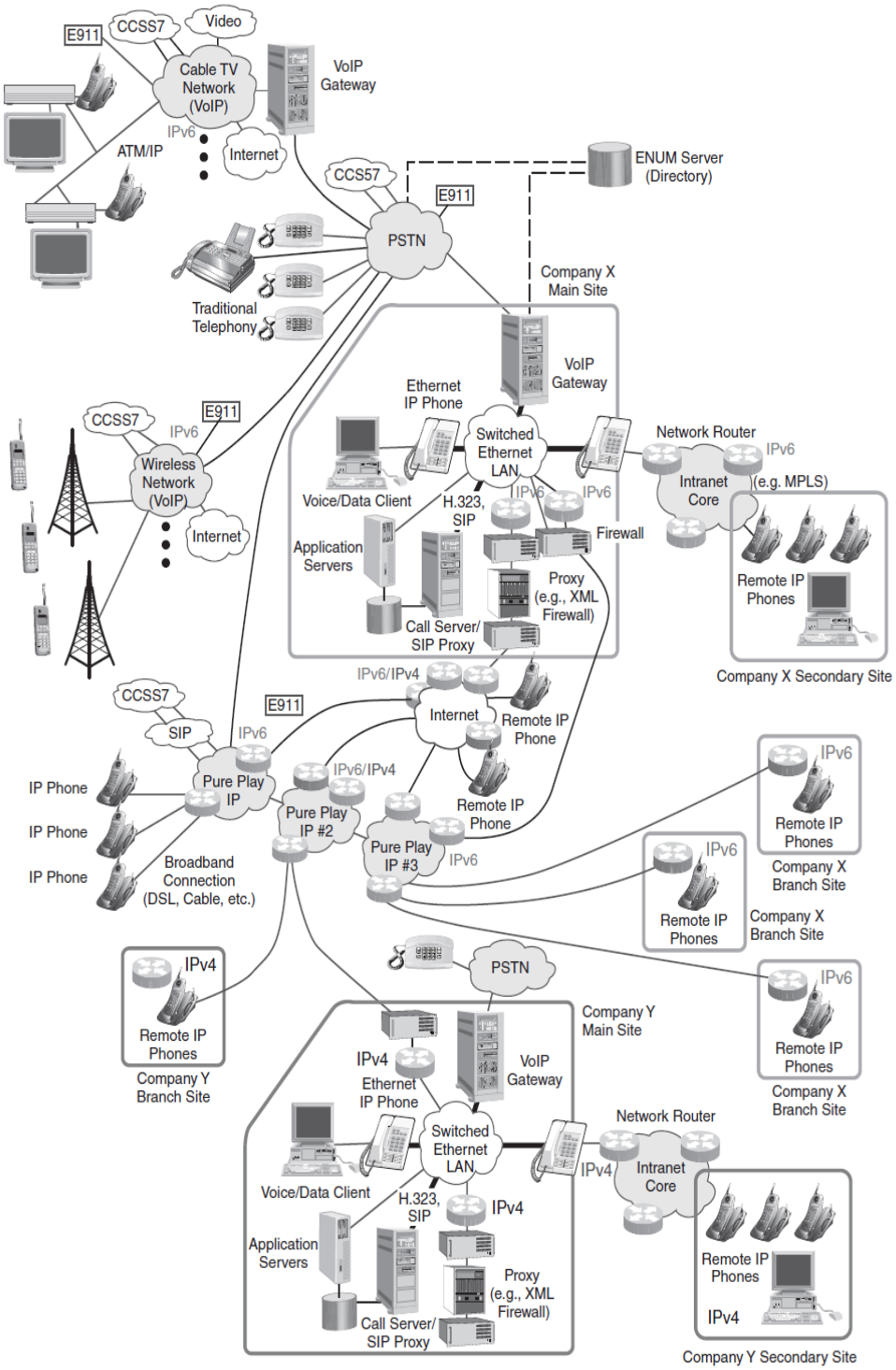


Figura 7.2 Arquitectura VoIPv6

La idea principal es que cada dispositivo conectado a la red pueda libremente, de forma segura y fiable comunicarse con cualquier otro dispositivo conectado a la red en cualquier punto y en cualquier momento; y siempre que sea posible, una llamada deberá tomar una ruta puramente IP, si esta existe, pero los elementos que no tengan opción deberán utilizar un segmento de la red tradicional de voz, la PSTN.

En la figura 7.2 se muestra como operara una red 3G VoIP basada en IPv6. Muchos de los elementos conectados deberán ser actualizados para soportar IPv6 o bien soportar ambos protocolos de Internet con diferentes estrategias de coexistencia o integración, las cuales ya fueron discutidas en el capitulo anterior. Así como, cualquier protocolo de transporte que incluya direcciones en su campo de cabecera deberá ser modificado para utilizar VoIPv6, para incluir los 128 bits de una dirección IPv6 en lugar de 32 bits que utiliza el protozoo de Internet versión 4.

El stock de protocolos de VoIP para IPv6 será básicamente los mismos que para IPv4, tal como SIP, H.323, MGCP y SSCP. SIP es compatible con IPv6, de tal forma que es posible operar con SIP en un ambiente puramente IPv6, o bien coexistir en un ambiente dual. SIP e IPv6 serán la clave tecnológica para la siguiente generación de comunicaciones. Los elementos de una red SIP, como son los UA, Proxy Server, Servidores de Localización pueden tener una dirección IPv4 e IPv6 de al forma que se podrán comunicar entre ellos ya sea en versión 4 o versión 6 o através de una comunicación mixta. Para el protocolo de VoIP H.323 los elementos como son el gatekeeper, gateway y terminales ya soportan IPv6 y técnicas de integración como el dual stack. Para el caso de MGCP y SCCP son protocolos que soportan IPv6.

7.1 Infraestructura IPv6 para VoIP.

La unidad de datos de protocolo (PDU) de IPv6 consiste de una cabecera y e una carga útil, como se muestra en la figura 7.3

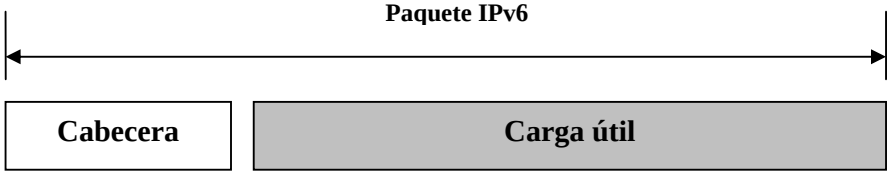


Figura 7.3 Unidad de datos.

La cabecera de IPv6 está compuesta por dos partes, tal como se ha explicado en este trabajo: la cabecera base de IPv6 y el encabezado de tipo opcional. El encabezado de tipo opcional es considerado como parte de la carga útil del paquete IPv6, como son los paquetes tipo TCP/UDP/RTP (incluyendo el flujo de voz). IPv6 e IPv4 no son interoperables, de tal forma que los dispositivos de red, como el router, operando en una arquitectura mixta deberán soportar ambas versiones de Internet; este es el caso de VoIP que soporta ambas arquitecturas, sin olvidar los ambientes de transición. En la figura 7.4 se muestra el flujo de paquetes de VoIP en una red VoIPv6.

IPv6 permite un espacio de direccionamiento de 2128 o 3.4 x 108 posibles direcciones. Como se menciono en un anterior capitulo, el largo espacio de direccionamiento permite que sea subdividido en dominios jerárquicos de ruteo que es soportado en la red de Internet actual. El uso de 128 bits proporciona múltiples niveles de jerarquía y flexibilidad en el diseño de direccionamiento y ruteo jerárquico. En VoIP es indispensable una conexión extremo a extremo fiable y con la jerarquía de IPv6 se puede soportar esta característica. Se debe de tener en cuenta que la red global de voz, la PSTN, está organizada en un modelo jerárquico por razones administrativas, ruteo, facturación, etc.

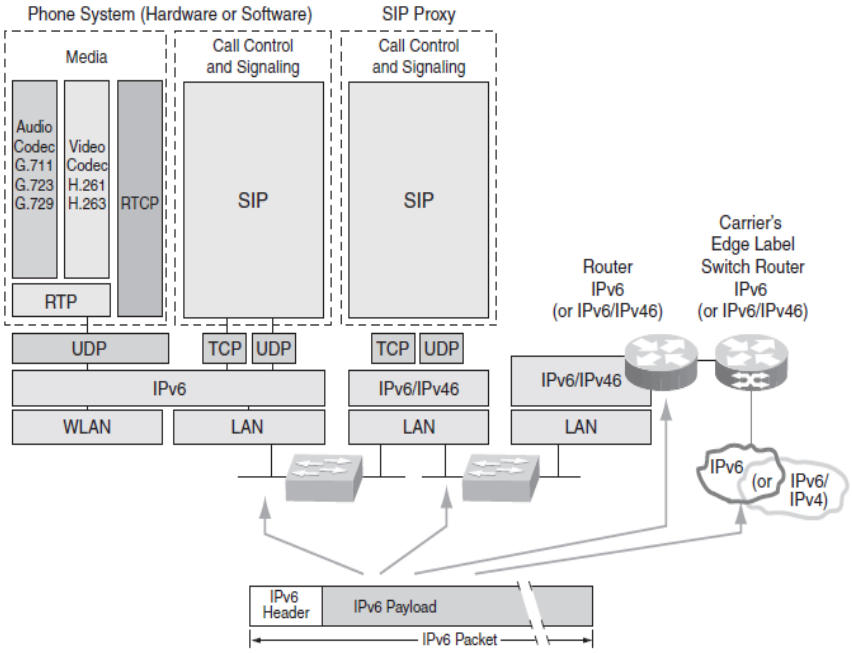


Figura 7.4 Flujo de un paquete en IPv6

Dos mecanismos de soporte son de interés para soluciones con problema de voz: (a) Un mecanismo para reportar problemas de transmisión con la comunicación, y (b) un mecanismo para soportar multicast.

ICMPv6 (Internet Control Message Protocol, como se trato en el capítulo 5, está diseñado para realizar funciones tales como detectar errores encontrados en la interpretación de paquetes, realizar diagnósticos, realizar funciones como Neighbor Discovery y detectar direcciones IPv6 multicast. Los mensajes de ICMPv6 son transportados en la carga útil del PDU de IPv6, como se muestra en la figura 7.5. Este protocolo servirá de herramienta para resolver problemas en los sistemas 3G de VoIP.

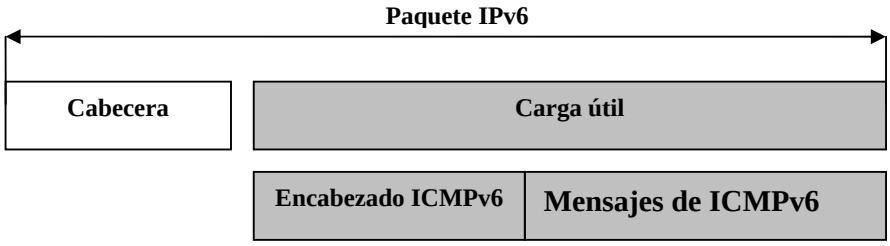


Figura 7.5 Paquete ICMPv6

El protocolo Neighbor Discovery (ND) es equivalente al protocolo ARP (Address Resolution Protocol), Consiste en un mecanismo con el cual un nodo que se acaba de incorporar a una red, descubre la presencia de otros nodos en el mismo enlace, además de ver sus direcciones IP. Emplea los mensajes de ICMPv6, y es la base para permitir el mecanismo de autoconfiguración en IPv6. Elementos de una red VoIP como Servidores Proxy en SIP, terminales H.323, Gateway y Gatekeeper hacen uso de ND para descubrir los routers vecinos, direcciones IP, prefijos de dirección y otros parámetros de configuración.

Una función soportada por IPv6 es el multicast. Es un método para transmitir datagramas IP a un grupo de receptores interesados. Además es soportado por una

variedad de protocolos como es ND y MLD. Las aplicaciones de multicasting son variadas, por ejemplo los operadores de TV de paga, algunas instituciones educativas ofrecen streaming de vídeo y audio a alta velocidad a un gran grupo de receptores. También hay algunos casos en que se ha utilizado para transmitir videoconferencias. Otro uso que se le ha dado, también a nivel comercial, es el de distribuir archivos. Particularmente para ofrecer imágenes de arranque de sistemas operativos. Respecto a los sistemas tradicionales permite un menor uso del ancho de banda de la red. Para una red VoIPv6 el multicasting es una herramienta para audioconferencias, videoconferencias, sistemas de voceo, música en espera, operadoras automáticas, entre otros.

El trafico multicast es reconocido por utilizar una dirección, pero es procesada por múltiples nodos. Las direcciones multicast en IPv6 tienen un prefijo 0xFF. La lista de miembros en un grupo multicast es dinámica, permitiendo a los nodos unirse y dejar el grupo en cualquier momento y en cualquier tiempo. En el caso de VoIPv6, un servidor Proxy o un Gatekeeper H.323 pueden enviar tráfico a un grupo de direcciones sin pertenecer al grupo multicast. Para unirse a un grupo multicast, el nodo (por ejemplo un teléfono IP) debe enviar un mensaje de solicitud. Los routers multicast sondean el estado de grupo de multicast. Cada grupo multicast es identificado por su dirección IPv6 tipo multicast, por lo que reciben y envían mensajes sobre la misma dirección de red.

7.2 Direccionamiento IPv6 sobre nodos VoIP.

De acuerdo a la RFC 1884 existen tres tipos de direcciones, tal como se vio en el capítulo 5, las cuales serán utilizadas por diferentes dispositivos y escenarios en una red VoIPv6, por ejemplo:

Unicast. Definidas en el RFC 1887 [12] identifican una sola interfaz. Cuando un paquete es enviado a una dirección unicast, este solamente es entregado a la interfaz que tenga dicha dirección. Este tipo de direcciones pueden ser un teléfono VoIP en un ambiente VoIPv6. Existen diferentes tipos de direcciones Unicast y estos son:

Global. Las direcciones Unicast Globales son direcciones de Internet, es decir, tienen significado y pueden ser enrutadas por Internet, ya sea de manera nativa si así lo permite la infraestructura de red, ó por medio de túneles. Usada en un ambiente VoIPv6 para conectar un teléfono VoIP através de la red de Internet.
Local. Este tipo de direcciones sirven para identificar una interfaz únicamente dentro de un mismo segmento de red (LAN), fuera de él pierden totalmente su valor. Para VoIPv6 este tipo de dirección será utilizada para comunicar un teléfono IP sobre una misma red LAN.

Sitio local. Este tipo de direcciones identifica una interfaz dentro de un dominio IPv6, pero no pueden ser enrutadas fuera de él, ya que pierden significado. Una dirección de sitio local permite alcanzar un teléfono VoIP en un ambiente VoIPv6 dentro de una red corporativa.

Multicast. Identifica a un conjunto de interfaces. Este tipo de direcciones son muy parecidas a las direcciones de difusión que maneja IPv4, es decir, un paquete que es enviado a una dirección Multicast es entregado a todas las interfaces identificadas por dicha dirección. El tráfico multicast permite enviar un solo flujo de paquetes para un grupo de usuarios, de forma que todos escuchan el mismo grupo multicast, y aceptan los mismos paquetes, tal es el caso de una videoconferencia o

audioconferencia VoIPv6, donde varios teléfonos IP intervienen en la misma conversación. Los protocolos de VoIP H.323 y SIP utilizan envíos multicast para el descubrimiento del gatekeeper en el primer caso y en el segundo através de mensajes de grupo INVITEs.

Anycast. Identifica a un conjunto de interfaces. A diferencia de las direcciones multicast, un paquete que es enviado a una dirección anycast es entregado a una de las interfaces identificadas por dicha dirección. Esta puede ser usada, por ejemplo, por grupos e distribución de un correo de voz en un ambiente IPv6.

En contraste a un IPv4 en donde un nodo con un su adaptador de red tiene asignada una dirección IPv4, en IPv6 un nudo tiene múltiples direcciones IPv6, tal es el caso de un Servidor Proxy, El uso de una dirección Ipv6 en un nodo router es como sigue:

Nodo (Teléfono IP). Típicamente los nodos IPv6 tienen a las menos dos direcciones con las cuales pueden recibir un PDU. Cada nodo tiene asignado una dirección local para el tráfico local, una dirección global y una dirección loopback, como se menciono en otro capítulo es una dirección que puede usar un nodo para enviarse paquetes a sí mismo.

Router (Gateway de voz). Un router IPv6 tiene asignado direcciones locales, globales y de tipo loopback.

7.3 Métodos de Configuración en VoIPv6.

Como se vio en el capítulo 5, el protocolo IPv6 puede utilizar dos métodos de configuración: (a) Configuración automática mediante direcciones sin estado, y (b) Configuración manual. El RFC2462 define el conjunto de pasos por los cuales un nodo decide como autoconfigurar sus interfaces en IPv6 de forma automática, lo que nos permite afirmar que IPv6 es “Plug&Play”. Este proceso incluye la creación de una dirección local, verificando que no esté duplicada en ese segmento de red y determina el perfil del nodo que ha de ser configurada. Las direcciones configuradas automáticamente tienen varios estados, como son: Tentativo, Preferido, Desaconsejado, Valido y No Valido, como se muestra en la figura 7.7

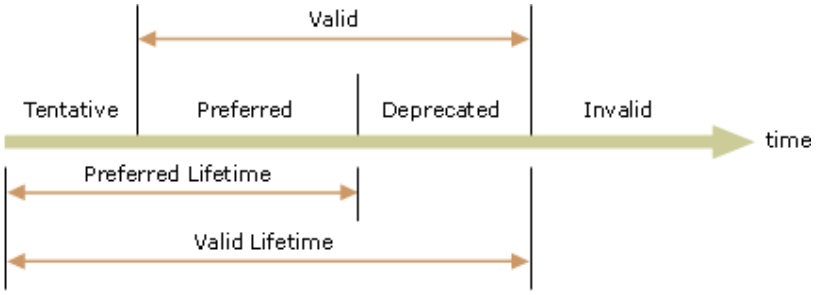


Figura 7.6 Direcciones Automáticas.

Existen tres tipos de configuración automática:

- Sin estado. La configuración de direcciones se basa en la recepción de mensajes de anuncio de enrutador. Estos mensajes contienen prefijos de direcciones sin estado y requieren que los nodos no utilicen un protocolo de configuración de direcciones con estado.

- Con estado. La configuración se basa en el uso de un protocolo de configuración de direcciones con estado, como DHCPv6, para obtener las direcciones y otras opciones de configuración. Un nodo utiliza la configuración de direcciones con estado cuando recibe mensajes de anuncio de enrutador que no incluyen prefijos de direcciones y requieren que el nodo utilice un protocolo de configuración de direcciones con estado. Un nodo también utilizará un protocolo de configuración de direcciones con estado cuando no haya routers presentes en el vínculo local.

- Ambos. La configuración se basa en la recepción de mensajes de anuncio de enrutador. Estos mensajes contienen prefijos de direcciones sin estado y requieren que los nodos utilicen un protocolo de configuración de direcciones con estado.

El proceso de configuración automática de direcciones en un nodo IPv6 o bien un teléfono VoIPv6 se produce de la manera siguiente:

1.- Se deriva una dirección local del vínculo tentativa, basada en el prefijo local del vínculo de FE80::/64 y el identificador de interfaz de 64 bits.

2.- Se lleva a cabo la detección de direcciones duplicadas para comprobar la exclusividad de la dirección local del vínculo tentativa.

3.- Si se produce un error en la detección de direcciones duplicadas, se debe realizar la configuración manual en el nodo.

4.-Si la detección de direcciones duplicadas tiene éxito, la dirección local del vínculo tentativa se considera única y válida. La dirección local del vínculo se inicializa para la interfaz. La dirección correspondiente de nivel de vínculo de multidifusión para el nodo solicitado se registra en el adaptador de red.

En un nodo IPv6 como puede ser un Servidor SIP, la configuración automática de direcciones continúa de la forma siguiente:

1.- El nodo envía un mensaje de solicitud de enrutador.

2.- Si no se reciben mensajes de anuncio de enrutador, el nodo utilizará un protocolo de configuración de direcciones con estado para obtener las direcciones y otros parámetros de configuración.

3.- Si se recibe un mensaje de anuncio de enrutador, se establece en el nodo la información de configuración incluida en el mensaje.

4.-En cada uno de los prefijos de direcciones de configuración automática con estado que se incluyen:

El prefijo de dirección y el identificador de interfaz de 64 bits correspondiente se utilizan para derivar una dirección tentativa.

Se utiliza la detección de direcciones duplicadas para comprobar la exclusividad de la dirección tentativa.

Si la dirección tentativa está en uso, no se inicializa para la interfaz. Si la dirección tentativa no está en uso, se inicializa. Esto incluye la configuración de la duración válida y la duración preferida en función de la información contenida en el mensaje de anuncio de enrutador. Si se especifica en el mensaje de anuncio de enrutador, el host utilizará un protocolo de configuración de direcciones con estado para obtener direcciones adicionales o parámetros de configuración.

7.4 Problemas de desarrollo a VoIPv6

La adaptación de VoIP sobre IPv6 se centra en el desarrollo de aplicaciones y componentes físicos que soporten ambos dominios de red, sin embargo se deben de considerar los cambios en los encabezados de los protocolos de transporte, protocolos de señalización y resolución de nombres cuando inicie intercambio de información entre distintas versiones de internet para establecer un canal de comunicación. Los problemas a resolver son los siguientes:

Señalización. Un escenario con IPv4 nativo o IPv6 nativo no requiere de una adaptación o modificación adicional, el reto sin embargo es la interconexión de IPv4 e IPv6. Los protocolos de señalización de voz sobre IP se encargan del establecimiento de una llamada o sesión entre dos puntos finales, en la versión 6 de Internet la suite protocolos de VoIP para el intercambio de mensajes de establecimiento de canal se agrupa entre SIP y H.323 por sus características y penetración en el mercado, para lo que será necesario de un elemento de red que pueda entender las dos nubes de red, capaz de traducir las cabeceras de SIP y H.323 hacia los nodos destino. Dependiendo del protocolo de señalización se han propuesto por distintas entidades internacionales crear gateways o servidores proxy con dicha cualidad, ambas soluciones plantean que exista un solo dispositivo para que lo mensajes de señalización atraviesen el mismo elemento. Con la penetración de IPv6 al Internet, cada nodo deberá de entender el protocolo de red sin importar la longitud de las direcciones origen y destino, los métodos de transición a IPv6 descritos en el anterior capitulo deberán adaptarse a cada dispositivo de voz o al que se encuentre en el borde de cada protocolo de internet, pero dependerá cada escenario que se implemente VoIPv6.

DNS. En general, el DNS es usado para resolver nombres de dominio fuera y dentro de los servidores Proxy con sus correspondientes direcciones IP. Hay dos formas de obtener las direcciones IP de un servidor Proxy: por un registro A o AAAA para IPv6 y un registro SRV para SIP. Para soportar SIP en IPv6, la dirección IPv6, la dirección del Servidor Proxie deben de ser registrada en la base de datos del DNS, lo que requiere que los DNSs estén actualizados con nuevos registros, además de soportar ambos protocolos de red con algún método de transición, como es el caso del Dual-Stack.

Transmisión. En el mensaje de establecimiento de sesión, SIP transporta un encabezado de SDP para negociar los atributos de la sesión de media, incluyendo los codecs, dirección de transporte y protocolos. Con el fin de intercambiar paquetes de media, los puertos lógicos de transporte son indispensables para realizar la conexión entre nodos y deben de poder viajar por cualquiera de las redes de internet. El protocolo de transporte no es afectado mientras se entregan los paquetes de voz o video, los puertos son negociados por los nodos finales, los call servers o los

Servidores Proxie. En el caso de H.323 el encargado de negociar los codecs, puertos y direcciones de transporte será el protocolo H.245.

El éxito de VoIPv6 dependerá de las propuestas de transición y el método de resolver los problemas que se presenten al interconectar los dos protocolos de internet, sin embargo el mercado demanda una solución rápida, transparente y eficaz a las necesidades de los usuarios.

7.5 H.323 e IPv6.

H.323 está diseñado para iniciar, controlar y terminar sesiones entre dos nodos IP que hablen este protocolo, sin importar la versión de internet, basta con conocer la dirección IP destino. Un canal de transmisión está definido por dos punto finales: un origen y un destino y son identificados por una dirección de red. H.323 es un protocolo robusto, antiguo y actualmente reemplazado por SIP, sin embargo un protocolo integro y especialmente usado en muchas empresas como herramienta de transición entre el medio digital y transmisión de paquetes por IP, de tal forma que la infraestructura actual debe ser la base para la evolución de VoIPv6. En general es posible realizar una comunicación entre puntos finales de distinto dominio de red utilizando direcciones IP embebidas, Dual Stack o algún otro mecanismo de transición. Los componentes de una red H.323 como son los Gatekeeper, Gateway, aplicaciones de voz y teléfonos IPv4/IPv6 que se encuentren en ambas redes deberán hablar ambos protocolos, para ello existen diferentes posibilidades para implementar IPv6 en el trasporte de voz.

Una primera solución sería implementar Dual Stack en el Gatekepeer y tener la habilidad de resolver los mensajes que sean transmitidos en IPv6 a IPv4 y viceversa por Gateway o teléfonos. Esta propuesta está sujeta a la disponibilidad a que el sistema operativo del Gatekeeper soporte IPv6 y traducción de direcciones con NAT-PT. Para usar NAP-TP se ha de implementar un Aplication Level Gateway H.323 que convierta el tráfico en la versión IP correcta, sabiendo que el protocolo H.323 tiene algunas características específicas, como el uso de puertos dinámicos. Los problemas se presentan cuando una llamada se desea establecer entre dos nodos de diferente dominio, para lo que es posible asignar técnicas de transición en teléfonos o gateways. Cuando teléfono IP se enciende se abre un puerto de comunicación sobre el cual recibe la información de media, en un escenario con IPv4 e IPv6 y Dual Stack se recibirán dos puertos al mismo tiempo. Por otra parte, si un teléfono se debe de comunicar con un Gatekeeper, se debe de tomar la decisión y especificar una dirección de red. El Gatekeeper pude registrar un Gateway con una dirección IPv4 y/o IPv6. La interconexión de mensajes en tiempo real entre nodos H.323 puede establecerse entonces diferentes sentidos en solo IPv6, IPv6 a IPv4, IPv4 a IPv6 o solo IPv4., para lo que se

Una segunda solución es aplicar direcciones IPv4 sobre direcciones IPv6 en los routers que se encuentren en la frontera de ambas redes, sin embargo no es una solución definitiva por el espacio limitado de direcciones en la versión 4 de Internet, además los mensajes de H.225 en la capa de aplicación intercambian direcciones IPvx. Una tercera solución es aplicar DSTM en el router de extremo, que funciona como un Termination End Point, y el cliente (con el cliente DSTM instalado). Esta segunda parte podría ser un problema porque el cliente DSTM ha de estar disponible bajo el entorno del host. Hay que desplegar además un servidor (DHCPv6) y un protocolo de asignación de direcciones IPv4 que proporcione la dirección IPv4 durante

la sesión H.323.

En general no existe una solución para implementar H.323 en una red VoIPv6, esto dependerá de las necesidades técnicas de la red.

7.6 SIPv6.

El protocolo SIP es un protocolo de VoIP inicialmente creado para IPv4, está diseñado de la misma forma que HTTP y SMTP, se encarga de iniciar, modificar y finalizar sesiones multimedia. Es un protocolo que debido a su arquitectura fácil de comprender, implementar y desarrollo se postula en un futuro como el más importante de su clase. Los estudios más relevantes del desarrollo de VoIPv6 se basan en SIP, la facilidad de funciones como Presencia, Mensajería Unifica y Comunicaciones Unificadas actualmente se inclinan por SIP. Una solución completa para la transición a IPv6 requiere que la capa de señalización y media puedan ser transportadas por diferentes redes. Aunque SIP pueda manejar redes heterogéneas en las capas mencionadas los servidores Proxy, DNS, User Agents o Gateway deben de ser configurados de tal forma que puedan soportan los intercambios de mensajes de distintos elementos en diferentes redes.

Los User Agents típicamente envían trafico SIP a un servidor Proxy, el cual se dedica a direccionarlo al destino final. Con el fin de soportar nodos IPv6, IPv4 o mixtos se puede adoptar el mecanismo de transición Dual-Stack en los servidores Proxy o un Servidor Proxy-IPv4 y otro IPv6, además de existir un servidor DNS en cada dominio o con Dual-Stack que permite resolver direcciones con nombres de dominio. La conexión entre SIP Proxys puede ser basada sobre DNS, si una solicitud de registro AAA para el nombre de destino SIP puede ser resuelta, la dirección IPv6 del Proxy destino puede ser alcanzada, en caso contrario, si una solicitud de dominio IPv6 no es posible, entonces un registro tipo A es devuelto y la dirección IPv4 del destino es usada para la conexión entre Proxys.

En el intercambio de paquetes de media se requiere realizar la traducción de IPv4 a IPv6 y viceversa, el protocolo SDP contiene algunos campos que deberán de ser modificados, tales como los campos que contienen direcciones IP e información del puerto de transporte. El dispositivo encargado de traducir esta direcciones es un Gateway de aplicación, la traducción sucede cuando un user agent trata de realizar una conexión con otro user agent, el elemento de la capa de aplicación se encarga de modificar los encabezados de SIP y los paquetes de RTP son traducidos en la capa de red, ya que no utilizan una dirección IP en su carga útil no es necesario realizar ninguna operación con las cabeceras.

7.6.1 Elementos de Red.

En IPv6 se requiere que los elementos de la red SIP puedan establecer una sesión con distintos nodos en diferentes dominios, para lo que en una arquitectura con IPv4 e IPv6 se pueden presentar los siguientes elementos de red:

- User Agent Solo IPv4. Un usuario solo IPv4 que soporta señalización SIP y media solo en red IPv4.

- User Agent Solo IPv6. Un usuario solo IPv6 que soporta señalización SIP y media solo en red IPv6.

- Nodo Solo IPv4. Un nodo que implementa solo IPv4 y que no soporta IPv4.

- Nodo Solo IPv6. Un nodo que implementa solo IPv6 y que no soporta IPv4.

- Nodo IPv4/IPv6. Un nodo que implementa tanto como IPv4 como IPv6, también conocido como nodo dual-stack.

- User Agent IPv4/IPv6. Un usuario que soporta señalización SIP y media en ambas redes IPv4/IPv6.

- Proxy IPv4/IPv6. Un servidor proxy que soporta señalización SIP sobre IPv4 e IPv6.

- SER. El SIP Express Router es un servidor que actúa como SIP Register, Servidor Proxy o Redirect que soporta ambos protocolos.

- MiniSIP Proxy. Recibe y modifica mensajes SIP, instala mapas de UDP para la comunicación RTP y reenvía los mensajes SIP a otro Proxy. Está compuesto por un Proxy IPv6 y un Proxy IPv4. Si una solicitud es recibida por la interface IPv4 se envía por IPv6 y viceversa, para ello se deben de modificar los siguientes campos en el encabezado de SIP:

- Contact Header. Este campo es modificado sustituyendo el encabezado de contacto original con el URI del SIP Gateway frontera entre IPv6 e IPv4 con un parámetro adicional que refleja la dirección original de contacto.

- Request URI. Solo se debe modificar si la solicitud URI tiene un parámetro Real-URI.

- SDP Header. Los campos a modificar son el origen (o=), contacto (c=) y la descripción de media (m=), los cuales mantienen la dirección o puertos y debe ser modificados con el protocolo de red a usar.

- Longitud de Contenido. Cuando se modifica el campo de SDP, la longitud del contenido debe ser recalculada.

- VIA. Un encabezado VIA es insertado en mensajes de solicitud y son eliminados desde los mensajes de respuesta.

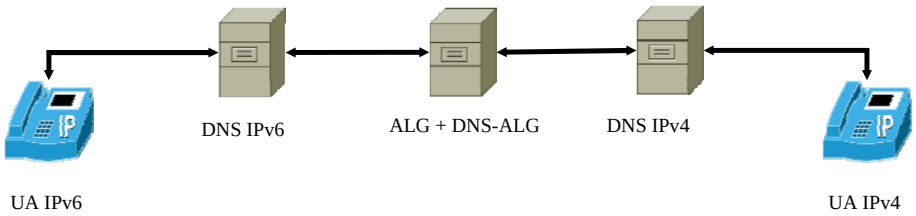
- ALG. Es un Gateway a nivel de aplicación para soportar la interconexión entre IPv4 e IPv6 para aplicación es SIP. Este elemento es necesario para manejar la traducción de SIP y UDP, la traducción de mensajes para DNS

Dependiendo de las necesidades técnicas y diseño de una red IPv6 que soporte VoIP se podrán desarrollar diferentes escenarios de VoIPv6, por lo que no todos los elementos mencionados pueden estar presentes al mismo tiempo. La traducción de protocolos en la capa de aplicación será manejada por un Gateway en la capa de aplicación y la traducción en la capa de red será manejada por un Gateway que soporte NAT-PT. En la actualidad se desarrollan nuevos dispositivos capaces de

traducir a IPv6, sin embargo la base de los dispositivos se han mencionado en este trabajo.

7.6.2 Flujo de llamada SIPv6

En la Figura 7.8 se presenta un escenario de VoIPv6 entre dos UA, un UA solo IPv6 y otro UA solo IPv4 y un ALG como traductor de protocolos. Cuando el UAv6 intenta iniciar una sesión con el UAv4 vía la dirección URI (username@domain), el UAv6 manda una solicitud a un Servidor DNS para resolver la dirección IPv6, ya que el DNS no encontrara un registro correcto para resolver la solicitud, reenviara vía su Default Gateway a él DNS en el dominio IPv4 con la dirección origen y destino IPv6. El NAT-PT revisará los encabezados de las capas de red y de transporte de la solicitud del servidor de DNS y las reenviara a él DNS-ALG para convertir el registro AAAA a registro A, quien regresara al NAP-PT para traducir la dirección IPv6 a IPv4 a través de una dirección IPv4 embebida por ejemplo. La solicitud al DNS del dominio IPv4 es enviada. EL DNS de IPv4 resuelve con la dirección IPv4 y regresa la respuesta al DNS IPv6. EN el DNS-ALG se traduce el registro A a AAAA, el NAT-PT traduce de IPv4 a IPv6 la dirección destino y la respuesta al DNS IPv6 es entregada al UA solo IPv6 por lo que se puede iniciar a establecer el canal de comunicación, no sin antes traducir los puertos lógicos de UDP por el ALG.



7.7 Sesión SIPv6

El ejemplo anterior nos permite tener un panorama del un escenario simple para implementar SIPv6, sin embargo en la figura 7.9 se pueden observar más posibilidades. En cada escenario se requiere de un elemento para traducir los paquetes IPv6, en este caso el Gateway de aplicación, él cual recibe una solicitud y responde en una o más ocasiones, lo que se conoce como transacción. Esta transacción es iniciada por un iniciador. El objetivo de la transacción puede o no ser el destinatario de la solicitud. Considerando un mensaje SIP enviado de un UA1 a un UA2 en el escenario uno, donde el iniciador es el UA1 y el objetivo es el UA2. En la tabla 7.1 se presenta como ejemplo las direcciones de los UA.

Nodo	IPv4	IPv6	Nombre de Dominio	Num. Telf
UA1	10.10.10.10	3ffe:3600:1::3	ua1.ipv6.unam.ing.mx	1234
UA2	10.10.10.20	3ffe:3600:2::10.10.10.20	ua2.ipv4.unam.ing.mx	4321
SIPv4 Server	10.10.20.40	3ffe:3600:2::10.10.20.40	sip.ipv4.unam.ing.mx	No especificado
NAT-PT/SIP-ALG	10.10.20.50	3ffe:3600:1::1	NO especificado	NO especificado

Tabla 7.1 Ejemplo de direcciones de UAs.

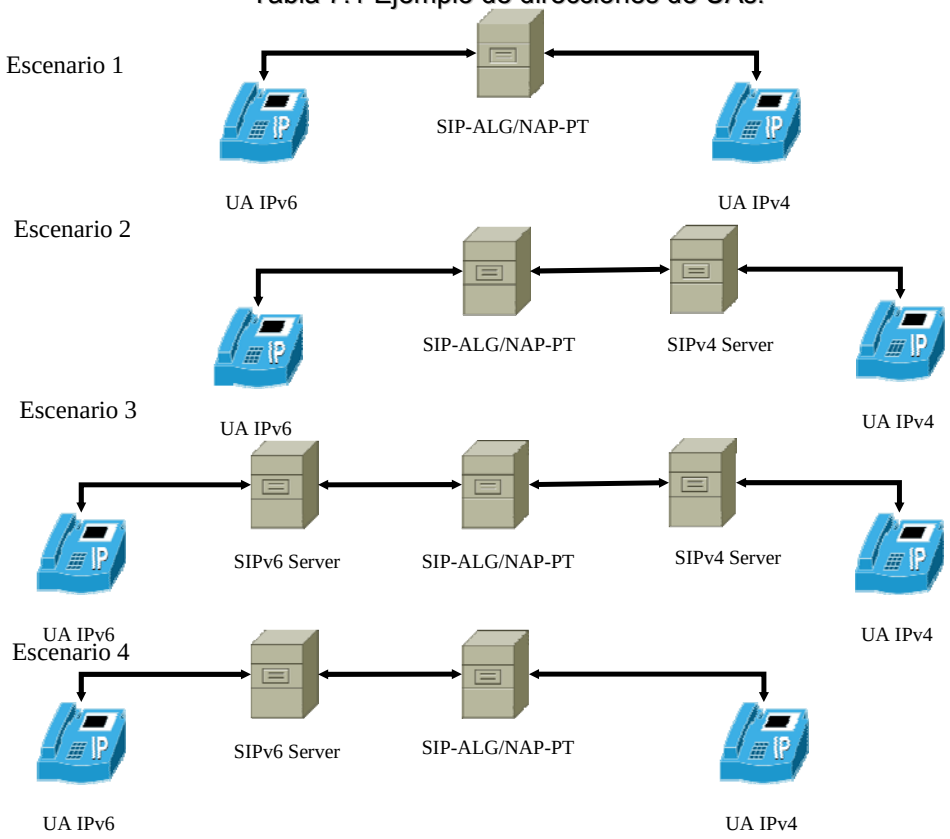


Fig 7.8 Escenario de desarrollo para SIPv6

Inicialmente los UAs se registran con el Registration Server, que puede estar físicamente en el mismo dispositivo que el Servidor Proxie y el Location Server, proporcionando su localización con una dirección IPv6, IPv4 o con un sufijo numérico en la dirección URI para conocer su ubicación, lo que permite, en una red como IPv6, la movilidad para dispositivos móviles que requieren los usuarios.

Una vez registrados los puntos finales, el flujo de una sesión SIP del el UA2 al UA2, en el escenario 2 de la figura 7.9, será el siguiente:

- 1. El UA2 manda un mensaje de INVITE a él Servidor SIPv4. En este mensaje, el mensaje de solicitud URI es sip:1234@ sip.ipv4.unam.ing.mx y el campo de vía es SIP/2.0/UDP 10.10.10.20:5060. EL campo de Contacto es sip:5678@ sip.ipv4.unam.ing.mx. En la porción de SDP, el campo o es 5678 “ID” in IPv4 10.10.10.20, el campo c es IN IPv4 10.10.10.20 y el campo m es audio “Port ID” RTP/AVP 0. El UA2 recupera el destino del siguiente salto (en este ejemplo sip.ipv4.unam.ing.mx para el Servidor SIPv4) desde el mensaje de solicitud URI. El dominio recuperado es traducido a la dirección IPV4 10.10.20.40 a través de la resolución del DNS. Entonces este mensaje es enviado al Servidor SIPv4.
- 2. Una vez recibido el mensaje de INVITE, el servidor SIPv4 utiliza el número de teléfono 123 en el mensaje de solicitud URI para recuperar la dirección IP/numero de puerto del UA1 (10.10.10.10:5061). La solicitud URI es

modificada como sip:1234@10.10.10.10:5061. El servidor SIPv4 agrega su dirección en el segundo campo via SIP/2.0/UDP 10.10.20.40:5060. El campo de contacto y la parte de SDP no son modificados. En el encabezado de IP, la dirección fuente es 10.10.20.40 (para el servidor SIPv4), y la dirección destino es 10.10.10.10 (de la solicitud URI). EL mensaje es direccionado al NTP-PT.

- 3. El NAT-PT pasa el mensaje INVITE a él SIP-ALG. El SIP-ALG traduce la solicitud URI a el formato de IPv6 (sip:(1234@3ffe:3600:1::3):5060), basado en el mapa que NAT-PT crea de la dirección IPv4:puerto a IPv6:puerto. EL SIP-ALG traduce el segundo campo via a SIP/2.0/UDP (3ffe:3600:2::10.10.10.30):5060. En el cuerpo de SDP, el SIP-ALG traduce el campo c IN IPv4 10.10.10.30 en un formato de IPv6 (IN IP6 3ffe:3600:2::10.10.10.20). El campo o y m no son cambiados. El NAT-PT traduce la dirección IPv4 fuente a un formato de IPv6 (3ffe:3600:2::10.10.10.30). La dirección destino es traducida a 3ffe:3600:1::3. Entonces el mensaje es enviado al UA1.
- 4. Suponiendo que la llamada es aceptada por el punto destino después que los mensajes 100 Trying y 180 Ringing han sido enviados. El UA1 envía el mensaje 200 OK a el UA2. Los campos To,From,Via son directamente copiados del mensaje de INVITE. El campo Contact es 1234@ sip.ipv4.unam.ing.mx. En la parte de SDP, el campo o es 1234 “ID” IN IP6 3ffe:3600:1::3, el campo c es IN IP6 3ffe:3600:1::3, y el campo m es audio “Port ID” RTP/AVP 0. Desde el segundo campo via, UA1 obtiene la dirección IPv6/puerto ((3ffe:3600:2::10.10.10.30):5060) del siguiente salto. Basándose en esta dirección, el mensaje 200 OK es direccionado al NAP-PT.
- 5. Cuando el NAT-PT recibe el mensaje 200 OK, este es direccionado al SIP-ALG, quien traduce el campo c de SDP a IN IPv4 10.10.10.10. Para el campo m, el número de puerto 9000 es reemplazado por 9002 para evitar que múltiples SIPv6 UAs usen la misma dirección y el mismo número de puerto. El servidor SIP-ALG construye el mapa de puerto RTP/RTCP para la siguiente sesión de voz o datos. El campo o no es cambiado. El servidor SIP-ALG traduce el segundo campo via a un formato de IPv4 10.10.20.40:5060, la cual es el siguiente salto para el servidor SIPv4. El NAT-PT traduce la fuente y destino IPv6 al dominio IPv4 10.10.10.10 y 10.10.20.40. Entonces el mensaje es enviado al servidor SIPv4.
- 6. Una vez recibido el mensaje 200 OK, el servidor SIPv4 elimina el segundo campo via, y recupera la direccion IP4 y el puerto (10.10.10.20:5060) del primer campo de via. El mensaje es enviado a UA2.
- 7. Cuando el UA2 recibe el mensaje 200 OK, comienza la transmisión de paquetes RTP/RTCP. Por lo tanto, UA2 regresa el mensaje ACK a el UA1.

En la figura 7.9 se puede observar de manera grafica el flujo descrito anteriormente.

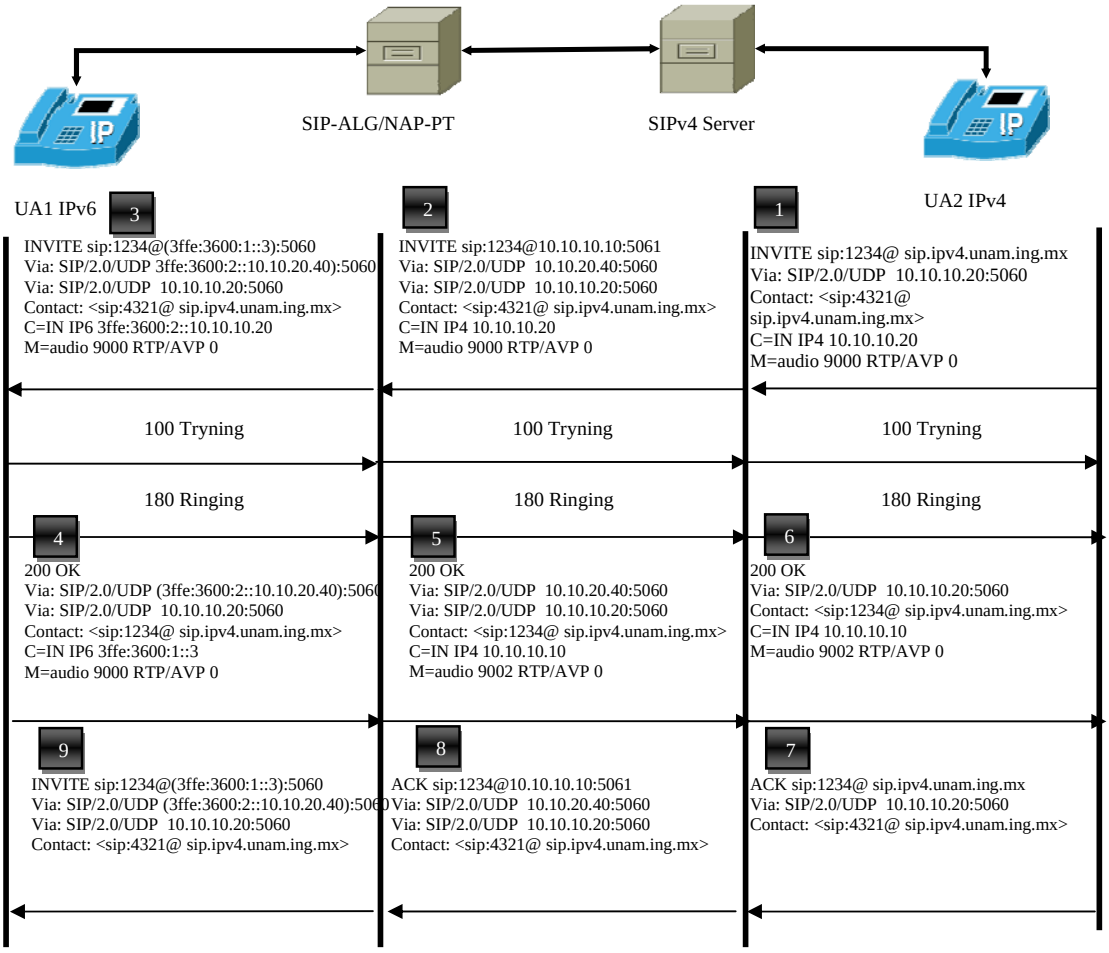


Figura 7.9 Flujo de una llamada SIPv6

7.7 Transición a VoIPv6.

En un ambiente VoIP los elementos de la red deberán ser actualizados en hardware o software para soportar el protocolo de Internet versión 6, inicialmente las redes IPV6 se encuentran aisladas, como en el caso de CLARA para Latinoamérica. El objetivo de VoIPv6 es interconectar las redes actualmente instaladas, como los son la PSTN, Internet versión 4, Internet versión 6 la red inalámbrica, entre las más comerciales, con el fin de poder conectar cualquier teléfono a cualquier parte del mundo, sin importar la red en que se encuentre.

Las redes VoIPv6 deberán utilizar técnicas de transición como es la doble pila y túneles para comunicarse con otro tipo de redes basadas en IPv4, aunque no son las únicas posibilidades de transición, si las más viables; sin embargo la traducción de paquetes de tiempo real ya ha sido un desarrollo constante, especialmente para SIPv6. De tal forma que redes SIP y H.323, serán soportadas en una red IPv6, sin

cambiar sus principales características. Pero, el escenario más estudiado es con SIP sobre IPv6, lo que lo que representa la plataforma a desarrollar para VoIPv6.

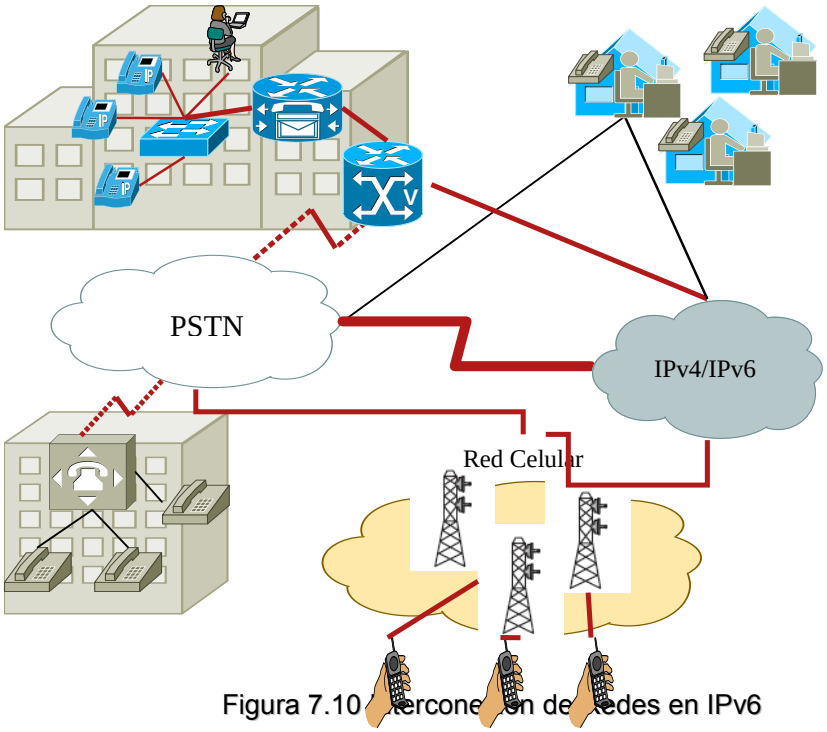


Figura 7.10 Interconexión de redes en IPv6

El despliegue del protocolo IPv6 inició en 1999. Para soportar un despliegue exitoso de IPv6 la infraestructura de red, las aplicaciones, programas intermedios, la seguridad, la administración para proveedores, empresas, consumidores de red y los usuarios finales deben ser primero desarrollados. La planeación y análisis operacional para desarrollar VoIPv6 en un red requiere ser probada y planeada. El despliegue de VoIP sobre Internet versión 6 requiere de planeación y una serie de pasos para implementar esta tecnología, existen casos como Corea y Holanda en el despliegue de IPv6 donde se planifico una política de implantación, como se muestra en la tabla 7.2

Caso Corea	Caso Holanda
Los tres planes de política en torno al IPv6 son: 1.- Plan sobre la infraestructura de las redes de siguiente generación. (2000-2004). Objetivo: Llevar a cabo pruebas, creación de negocios de IPv6 en los sectores público y privado, así como difundir el conocimiento en el público sobre el Ipv6 2.- Plan sobre la promoción de IPv6 (2004-2006). Objetivo: Definir los obstáculos para el desarrollo de los servicios IPv6 en los hogares, oficinas, etc., incrementar comercialmente equipos	Los planes de desarrollo para IPv6 consisten: 1.- Creación del IPv6 Task Force. 2.- Desarrollo de un Plan de Proyecto con la finalidad de: a) Expectativas estratégicas: Identificar las necesidades y posibilidades del IPv6. b) Establecer ruta crítica, enfoque y urgencia. c) Formular un plan de integración de alto nivel. d) Formulación, implementación y expansión de fases. 3.- Posibles medidas de la Administración pública de Holanda:

IPv6 y Acuerdo de servicio. 3.- Plan II sobre la promoción de IPv6 (2007-2011) Objetivo: Ofrecer el servicio de VoIPv6 a usuarios del sector público, establecer como modelo de referencia la VoIPv6 en 16,000 agencias gubernamentales, incrementar usuarios e instituciones del IPv6 y desarrollo de la red	• Hacer que los portales del gobierno estén listos para IPv6 • Exponer casos de estudio en comunicación con las organizaciones

Tabla 7.2 Despliegue de IPv6

Para el caso del desarrollo de VoIPv6 es indispensable el desarrollo de IPv6 en nuestro país, de acuerdo a la LACNIC (Registros de Direcciones de Internet para Latinoamérica y el Caribe), quien administra las Direcciones IP versión 4 y versión 6, Números de Sistemas Autónomos, DNS Reverso, y otros recursos de red para la región; hasta Febrero de 2010 la distribución de las direcciones IPv6, en número de /32, ya asignadas entre los países de la región se muestran en la figura 7.11.

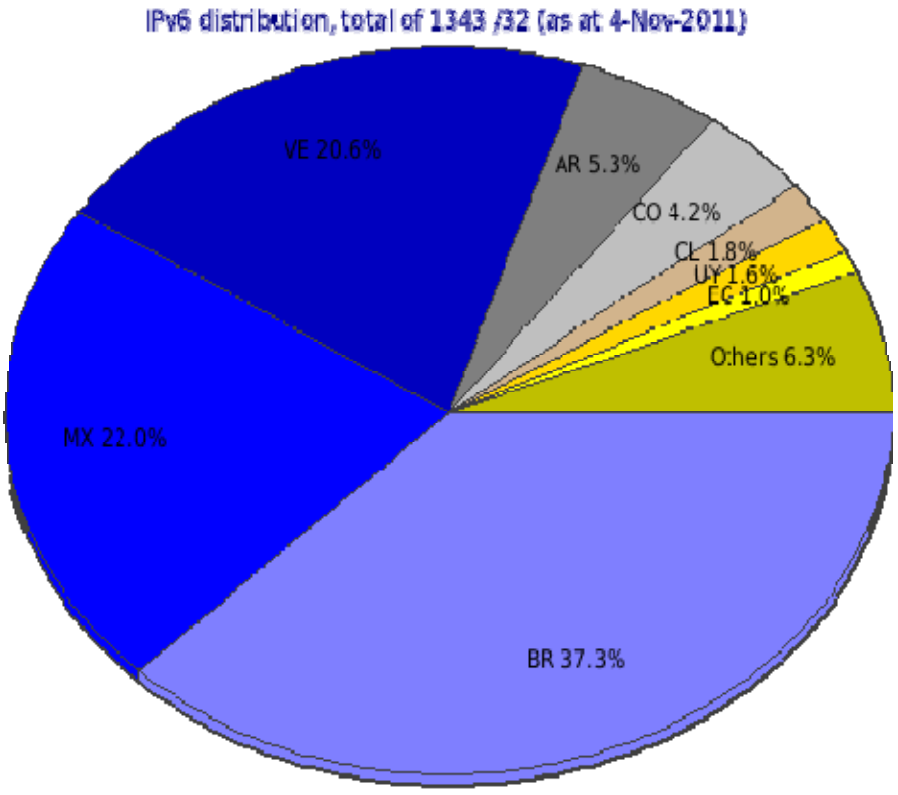


Figura 7.11 Distribución de IPv6

La cantidad de solicitudes para recursos Internet (IPv4, IPv6, ASN) recibidas por LACNIC a cada mes se refleja en la figura 7.12. Y también se muestra un comparativo con los años anteriores.

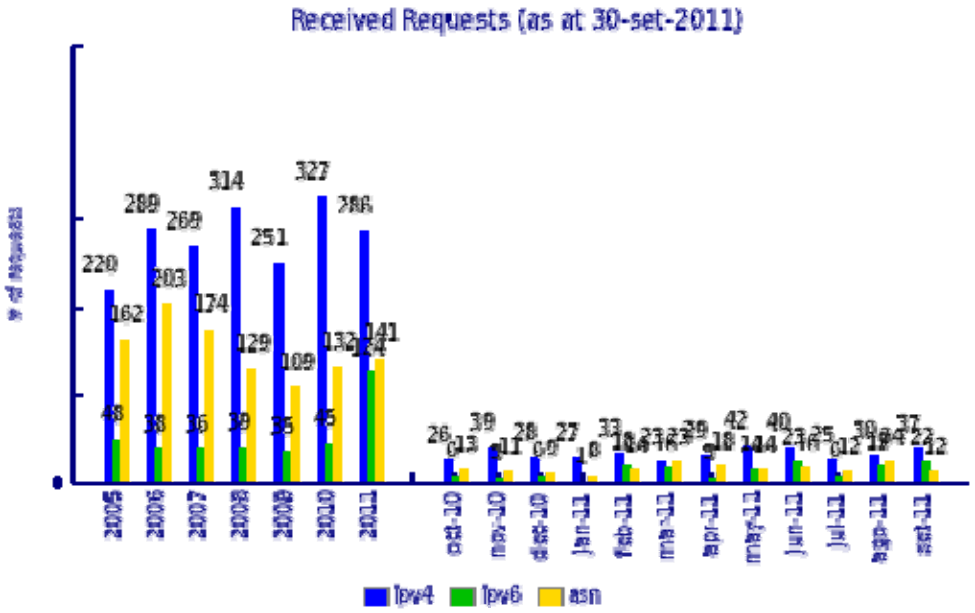


Figura 7.12 Solicitudes IPv6

La figura 7.13 indica la cantidad de direcciones IPv6 asignadas por LACNIC a organizaciones de la región. Dichas asignaciones están representadas en bloques de prefijo /32.

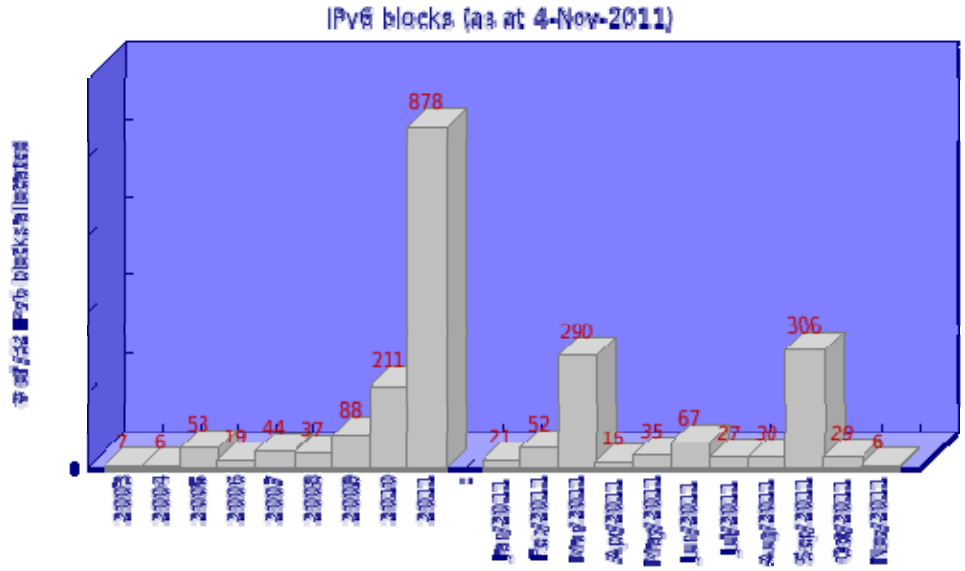


Figura 7.13 Numero de Bloques de /32 de Ipv6 asignados.

Las redes piloto de IPv6 están probando diferentes modelos de despliegue: (1) IPv6 soportado sobre el core de Internet, (2) IPv6 soportado en los equipos frontera del cliente y del proveedor, y, (3) IPv6 soportado en las redes finales del cliente. Dentro de estos modelos el primer modelo es el más difícil de probar en la transición a IPv6 directamente, debido a costo y el nivel de servicios implementados actualmente sobre la versión de Internet 4. Inicialmente el Internet transportara paquetes de IPv6 por la infraestructura de IPv4 de forma transparente por túneles, encapsulando paquetes versión 6 sobre IPv4 o el uso de MPLS. En el segundo modelo se están probando redes IPv6 nativas y redes IPv6 sobre IPv4, implementando túneles al router frontera del proveedor en el caso de redes nativas y aplicando mecanismos de transición en redes IPv6 sobre IPv4. En el último modelo la vista escasa del despliegue es que solamente los nodos o las redes que requieren IPv6 serán aumentados para utilizar IPv6.

La demanda creciente de conexión a Internet crea el escenario perfecto para impulsar servicios de redes de tercera generación, por lo que IPv6 será la base para el futuro de las telecomunicaciones.

CONCLUSIONES

La evolución de internet durante sus primeros años de vida ha sido sorprendente, la proyección en utilización de esta tecnología ha sido rebasada debido al crecimiento sostenido de computadoras, móviles, servidores, cámaras de vigilancia, dispositivos de rastreo y otros dispositivos con conexión de internet. En la actualidad es sumamente sencillo iniciar una conversación en tiempo real o bien una video llamada, la VoIP nos permite acortar distancias entre regiones lejanas y reducir costos en comunicaciones cotidianas, este impacto se registra en varios sectores de negocios y en la sociedad en general, por ejemplo en los negocios es posible ofrecer mayor seguridad a un bajo costo, mayores servicios de telecomunicaciones y mejor calidad; la oferta a los usuarios permite tener precios más competitivos y una gama de diversa de nuevas funcionalidades; para los proveedores de servicio disminuye el costo de operación y permite el desarrollo de nuevos productos.

La Voz sobre IP está creciendo de manera acelerada a nivel mundial y seguirá creciendo pues los servicios y la innovación que ofrece son altamente mayores a la tecnología actual de comunicación telefónica que gradualmente irá desapareciendo hasta lograr una transformación total en la manera de comunicarse. La VoIP reduce el costo de las comunicaciones telefónicas, lo cual atrae de manera impetuosa a los clientes que buscan economía y calidad en el servicio al momento de comunicarse con personas dentro y fuera de su empresa así como también a nivel mundial.

La VoIP se ofrecerá bajo un conjunto de estándares internacionales y protocolos aceptados por la mayoría de los operadores a nivel internacional, lo que facilitará la integración entre diferentes tecnologías y plataformas. La segunda generación de redes VoIP permitirá reafirmar nuevos conceptos como el servicio de telefonía hosteado, los contact center virtuales, presencia, comunicaciones unificadas, telepresencia, un número único y seguridad integrada. Esta generación solventa los problemas de calidad de servicio en las redes actualmente implementadas y la seguridad en el transporte de datos, con la ayuda del nuevo protocolo de internet IPv6 que incluye en su estructura nuevos campos en su cabecera. Se resuelven dificultades con la actual versión de IPv4, como es el agotamiento de direcciones, obteniendo una verdadera Movilidad para todo aquel dispositivo que se conecte a la Internet con una dirección globalmente única. La mejora de IPv6 en cuanto a los campos introducidos en relación con la cabecera IPv4 como lo son: Clase de tráfico y etiquetado de flujo garantizan la calidad de servicio para aplicaciones con requerimientos de tiempo real como lo es VoIP. El simple y eficiente encabezado de IPv6 facilita el procesamiento de paquetes a transmitir y el ahorro de recursos de memoria en los elementos de red cuya responsabilidad será elegir la mejor ruta para llegar al destino.

La evolución hacia la versión 6 del protocolo de internet hasta el momento ha sido gradual y lenta, sin embargo la nueva tecnología en las redes de comunicaciones ya están adecuadas para convivir con ambas redes. La transición requerirá el desarrollo de nuevas aplicaciones para soportar redes de IPv4/IPv6, incluyendo dispositivos de red y elementos de red VoIP. Durante el periodo de transición será imperativo utilizar técnicas de compatibilidad como es la doble pila, los túneles o los traductores de protocolo. La manera más sencilla para que los nodos sigan siendo compatibles es la utilización de ambos protocolos de internet es diseñando una interface lógica o física para cada uno, como lo propone el mecanismo de doble pila.

En una red VoIP el Call Server, el Media Gateway o las terminales deben soportar los protocolos de internet simultáneamente. Los mecanismos de tunneling no se hacen viables, debido a que deben utilizar direcciones IPv4 del espacio de direccionamiento ya agotado, pero es una opción para proveedores del servicio que cuenten con un segmento de red lo bastante amplio para asignar estas direccionas a los dispositivos que así lo requieran. Finalmente, los traductores de protocolo pueden resolver problemas de interoperabilidad, son fáciles de implementar, pero difíciles de gestionar a gran escala.

Las redes VoIP de siguiente generación estarán basadas en SIP e IPv6, debido a que la sintaxis de las operaciones de SIP se asemeja a las de HTTP y SMTP, protocolos utilizados en los servicios de páginas WEB y la distribución de correos respectivamente, por lo que SIP facilitara la integración con Internet. Es un protocolo que debido a su arquitectura fácil de comprender, implementar y desarrollo se postula en un futuro como el más importante de su clase. La adaptación de VoIP sobre IPv6 se centra en el desarrollo de aplicaciones y componentes físicos que soporten ambos dominios de red, sin embargo se deben de considerar los cambios en los encabezados de los protocolos de transporte, protocolos de señalización y resolución de nombres cuando inicie intercambio de información entre distintas versiones de internet para establecer un canal de comunicación. En el intercambio de paquetes de media se requiere realizar la traducción de IPv4 a IPv6 y viceversa, el protocolo SDP contiene algunos campos que deberán de ser modificados, tales como los campos que contienen direcciones IP e información del puerto de transporte.

La explotación de VoIPv6 tiene como base el desarrollo de redes IPv4/IPv6 de pequeña, media o grandes dimensiones, sin embargo hasta el momento solo se tiene una red IPv6 con fines de estudio ya implementada en México. La comercialización de productos y servicios por parte de los proveedores de Internet, difusión de contenidos y desarrollo de productos que utilicen VoIPv6, creación de patentes de productos y servicios permitirán la adaptación de esta nueva tecnología que representa el futuro de las telecomunicaciones.

Bibliografía.

1. Daniel Minoli (2006), Voice Over IPv6 Architectures for Next Generation VoIP Networks, Editorial Elsevier, EUA.

2. Jose Manuel Huidobro Moya y David Roldan Martinez (2006), Tecnología VoIP y Telefonía IP. Primera Edición. México. Editorial Alfaomega Grupo Editor.

3. Cisco Systems, Inc (2004), Guía del segundo año. CCNA 1 Y 2, Tercera Edición. España Ed. Pearson Educación, S.A.

3.1 Guía del segundo año. CCNA 3 Y 4, Tercera Edición. España Ed. Pearson Educación, S.A.

3.2 Manual Cisco Voice Over IP . Volumen I y II (2004).

3.3 Manual Cisco Ip Telephony . Volumen I y I (2008).

3.4 Quality of Service for Voice over IP.

3.5 Implementing NAT-PT for IPv6.

3.6 The ABCs of IP Version 6.

3.7 SIP Messages and Methods Overview.

3.8 Implementing VoIP for IPv6.

3.9 IPv6 Deployment Strategies.

3.10 Cisco IP Communications Express: CallManager Express con Cisco Unity Express. España, Ed. Pearson Educación, S.A.

3.11 Session Initiation Protocol Gateway Call Flows and Compliance Information.

4. Allan Reid, Jim Lorenz y Cheryl Schmidt (2008), Introducción al enrutamiento y la conmutación en la empresa. Unica edición. Ed. España Ed. Pearson Educación, S.A.

5. Ciprian Popoviciu, Eric Levy-Abegnoli, Patrick Grossetete (2006), Deploying IPv6 Networks. Ed Cisco Press, EUA.

6. Björn Karlsson (2003), Cisco Self-Study: Implementing IPv6 Networks (IPV6). Ed Cisco Press, EUA.

7. David Malone, Niall Murphy (2005), IPv6 Network Administration, Ed. O'Reilly, EUA.

8. Iljitsch Van Beijnum (2006), Running IPv6, Ed Apress. EUA.

9. Nortel Networks Corporation (2002), Voice Fundamentals Reference Guide . EUA .

10. Advance VoIP Technologies for Desing And Support (2006).
11. Henning Schulzrinne y Jonathan Rosenberg (1998). A Comparison of SIP and H.323 for Internet Telephony , Colombia University, EUA.

12. Wenyu Jiang y Henning Schulzrinne (2003), Assessment of VoIP Service Availability in the Current Internet, Colombia University, EUA.

13. Ismail Dalgic y , Hanlin Fang (1999), Comparison of H.323 and SIP for IP Telephony Signaling, EUA.

14. Héctor Kaschel C y Enrique San Juan U (2003), Consideraciones Técnicas para Elaborar un Estándar Definitivo VoIP, Universidad de Chile.

15. Tutorial: El Estándar VoIP: Redes y servicios de banda ancha.

16. IP-Telephony (Protocols), http:// www.rares.com.ar/PDF.

17. Recomendación ITU P.800, Métodos de determinación subjetiva de la Calidad de transmisión.

18. Recomendación ITU G.10, El modelo E, un modelo informático para utilización en planificación de la transmisión.

19. Recomendación ITU P.862. Evaluación de la calidad vocal por percepción: Un método objetivo para la evaluación de la calidad vocal de extremo a extremo de redes telefónicas de banda estrecha y códecs vocales.

20. Recomendación ITU P.861 .Evaluación de la calidad vocal por percepción: Un método objetivo para la evaluación de la calidad vocal de extremo a extremo de redes telefónicas de banda estrecha y códecs vocales.

21. Tommi Koistinen, Protocol overview: RTP and RTCP, Nokia Telecommunications.

22. Jose Ignacio Moreno, Ignacio Soto, David Larrabeiti, Protocolos de Señalización para el transporte de Voz sobre redes IP, Madrid, España.

23. José Joskowicz y Rafael Sotelo, Medida de la calidad de voz en redes IP, Universidad de Montevideo, Uruguay.

24. James Wright, MSc, Session Description Protocol, KONNETICSIP & IMS .NET development.

25. RADVISION (2001), SIP: Protocol Overview.

26. Simon ZNATY, Jean-Louis DAUPHIN y Roland GELDWERTH EFFORT, SIP : Session Initiation Protocol, Publicado por http://www.efort.com.

27. Simon ZNATY, Jean-Louis DAUPHIN y Roland GELDWERTH, SIP: Session Initiation Protocol, http://www.efort.com.

28. Spirent Communications, Inc (2001), Voice over IP (VoIP).

29. Tim Rooney, IPv4-to-IPv6 Transition Strategies.

30. Carlos Taffernaberry, Gustavo Mercado, Alejandro Dantiacq, Santiago Pérez y Raúl Moralejo (2008), Transició,. Implementación de Túnel 6to4, Argentina.

31. Eva M. Castro, Jesús González, Gregorio Robles, Tomás de Miguel, Interoperabilidad de aplicaciones IPv4 e IPv6, Universidad Rey Juan Carlos de Madrid, España.

32. Technology Guide (2004), Media Gateway Control Protocol (MGCP) Technology, Publicado por www.ixiacom.com.

33. Axel Ernesto Moreno Cervantes (2004), IPv6 Interoperabilidad y robustez, IPN, México.

34. Joseph Davies (2008), Understanding IPv6, Segunda Edición, Publicado por Microsoft Press, EUA.

35. Jenny Almeida, María Intriago, Talina Velasteguí, Iván Masapanta y Santiago Mosquera (2005), Protocolos de enrutamiento para IPv6, Publicado por http://www.ipv6forum.org/.

36. P.O'Hanlon, S.Varakliotis, R.Ruppelt y J.Fiedler (2005). Realisation of IPv6/IPv4 VoIP Integration Scenarios, Publicado por http://www.6net.org/.

37. FhG FOKUS (2003), Report on Integration of SIP and IPv6, Publicado por http://www.6net.org/.

38. Haidong Xia, Yanick Pouffarny y Jim Bound, The Evaluation of DSTM: An Transition mechanism.

39. Tutorial de IPv6, Publicado por IPv6 Forum, http://www.ipv6forum.org/.

40. Recommendations on the use of IPv6 in the Session Initiation Protocol (SIP) (2005), http://www.ietf.org/.

41. Hugo Oliveira, António Pereira, Mário Antunes y Nuno Fonseca (2006). VoIP over IPv6.

42. Escuela Superior de Tecnología e Gestão de L-eiria.

43. Richard Menedetter, Thomas Hoeher and Slobodanka Tomic. SIP collides with IPv6. IEEE.

44. Antonio Cuevas, Carlos García, José Ignacio Moreno y Ignacio Soto. Los pilares de las redes 4G: QoS, AAA y Movilidad. Universidad Carlos III de Madrid. España.

45. Anto K Davis, Kashyap Vasudevan, Joy Kuri y Haresh Dagale. IPv4-IPv6 Translator for VoIP and Video Conferencing. Center for Electronics Design and Technology, Indian Institute of Science, Bangalore.

46. Armin Brunner (2004), Interoperability between IPv4 and IPv6 SIP User Agent, Swiss Federal Institute of Technology Zürich.

47. Lambros Lambrinos y Peter Kirstein (2007), Integrating Voice over IP services in IPv4 and IPv6 networks, Publicado por IEEE.

48. Thomas Hoeher, Martin Petraschek, Slobodanka Tomic, Y Michael Hirschbichler (2007), Evaluating Performance Characteristics of SIP over IPv6, Publicado por IEEE.

49. Ch. Bouras, A. Gkamas, S. Josset y K. Stamos, Adding IPv6 support to H323: Gnomemeeting/openH323 port.

50. V. Gurbani (2008), Session Initiation Protocol (SIP) Torture Test Messages for Internet Protocol Version 6 (IPv6). RFC 5118.

51. G. Camarill (2007, IPv6 Transition in the Session Initiation Protocol (SIP). RFC 6157.

52. David H. Crocker(1982), Standard for the format of ARPA Internet text messages. RFC 822.

53. P. Mockapetris (1987), Domain Names - Concepts and Facilities, RFC 1034 y RFC 1035.

54. C. Hedrick (1988), Routing Information Protocol, RFC 1058.

55. Ross Callon (1992), TCP and UDP with Bigger Addresses (TUBA), A Simple Proposal for Internet Addressing and Routing, RFC 1347.

56. S. Hanks (1994), Generic Routing Encapsulation (GRE), RFC 1701.

57. M. McGovern (1994), CATNIP: Common Architecture for the Internet, RFC 1707.

58. G. Malkin (1994), RIP Version 2, Carrying Additional Information, RFC 1723.

59. S. Bradner (1995), The Recommendation for the IP Next Generation Protocol, RFC 1752.

60. Y. Rekhter (1995), A Border Gateway Protocol 4 (BGP-4), RFC 1771.

61. C. Partridge (1995), Using the Flow Label Field in IPv6, RFC 1809.

62. R. Hinden y Ipsilon Networks (1995), IP Version 6 Addressing Architecture, RFC 1884.

63. Y. Rekhter (1995), An Architecture for IPv6 Unicast Address Allocation, RFC 1887.

64. H. Schulzrinne, S. Casner, R. Frederick y V. Jacobson (1996), RTP: A Transport Protocol for Real-Time Applications, RFC 1889.

65. H. Schulzrinne (1998), Real Time Streaming Protocol (RTSP), RFC 2326.

66. M. Handley (1998), SDP: Session Description Protocol, RFC 2327.

67. R. Hinden (1998), IP Version 6 Addressing Architecture, RFC 2373.

68. S. Kent (1998), Security Architecture for the Internet Protocol, RFC 2401.
69. S. Kent (1998), IP Authentication Header, RFC 2402.

70. S. Kent (1998), IP Encapsulating Security Payload (ESP), RFC 2406.

71. S. Deering Y R. Hinden (1998), Internet Protocol, Version 6 (IPv6) Specification, RFC 2460.

72. T. Narten, E. Nordmark y W. Simpson (1998), Neighbor Discovery for IP Version 6 (IPv6), RFC 2461.

73. S. Thomson y T. Narten (1998), IPv6 Stateless Address Autoconfiguration, RFC 2462.

74. Conta, Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification, RFC 2463.

75. Conta y S. Deering (1998), Generic Packet Tunneling in IPv6 Specification, RFC 2473.

76. M. Handley, H. Schulzrinne, E. Schooler y J. Rosenberg (1999), SIP: Session Initiation Protocol, RFC 2543.

77. R. Coltun, D. Ferguson Y J. Moy (1999), OSPF for IPv6, RFC 2740.

78. E. Nordmark (2000), Stateless IP/ICMP Translation Algorithm (SIIT), RFC 2765.

79. G. Tsirtsis y P. Srisuresh (2000), Network Address Translation - Protocol Translation (NAT-PT), RFC 2766.

80. K. Tsuchiya y Y. Atarashi (2000), Dual Stack Hosts using the "Bump-In-the-Stack" Technique (BIS), RFC 2767.

81. D. Farinacci, S. Hanks y D. Meyer (2000), Generic Routing Encapsulation (GRE), RFC 2784.

82. M. Crawford y C. Huitema (2000), DNS Extensions to Support IPv6 Address Aggregation and Renumbering, RFC 2874.

83. R. Gilligan y E. Nordmark (2000), Transition Mechanisms for IPv6 Hosts and Routers, RFC 2893.

84. M. Crawford (2000), Router Renumbering for IPv6, RFC 2894.

85. Durand, P. Fasano y I. Guardini (2001), IPv6 Tunnel Broker, RFC 3053.

86. Carpenter y K. Moore (2001), Connection of IPv6 Domains via IPv4 Clouds, RFC 3056.

87. H. Kitamura (2001), A SOCKS-based IPv6/IPv4 Gateway Mechanism, RFC 3089.

88. J. Rosenberg, H. Schulzrinne, G. Camarillo, A. Johnston, J. Peterson, R. Sparks, M. Handley y E. Schooler, SIP: Session Initiation Protocol, RFC 3261.

89. D. Lawrence (2002), Obsoleting IQUERY, RFC 3425.
90. R. Hinden y S. Deering (2003), Internet Protocol Version 6 (IPv6) Addressing Architecture, RFC 3513.

91. H. Schulzrinne, S. Casner, R. Frederick y V. Jacobson (2003), RTP: A Transport Protocol for Real-Time Applications, RFC 3550.

92. S. Thomson, C. Huitema, V. Ksinant y M. Souissi (2003), DNS Extensions to Support IP Version 6, RFC 3596.

93. F. Baker, E. Lear y R. Droms (2005), Procedures for Renumbering an IPv6 Network without a Flag Day, RFC 4192.

94. F. Templin, T. Gleeson, M. Talwar y D. Thaler (2005), Intra-Site Automatic Tunnel Addressing Protocol (ISATAP), RFC 4214.

95. E. Nordmark y M. Bagnulo (2009), Shim6: Level 3 Multihoming Shim Protocol for IPv6, RFC 5533.

96. http://www.plusformacion.com/Recursos/r/Estandar-VoIP-Redes-servicios-banda-ancha.

97. http://www.itu.int/rec/T-REC-Y/s.

98. http://www.cudi.edu.mx/primavera_2007/presentaciones/Convergencia_IPv6-Azael.pdf.

99. http://www.ipv6.unam.mx/documentos/IPv6-Realidad.pdf.

100. http://www.ipv6.unam.mx/.

101. http://www.ipv6summit.com.mx/documentos/JordiPalet_Consulintel.pdf.

102. http://portalipv6.lacnic.net/.