**ESCUELA POLITÉCNICA DEL EJERCITO**

**FACULTAD DE INGENIERÍA ELECTRÓNICA**

# PROYECTO DE GRADO PARA LA OBTENCIÓN DEL TÍTULO EN INGENIERÍA ELECTRÓNICA

## IP-V6 BAJO LA INFRAESTRUCTURA DE ANDINANET

**LUIS GERMÁN OJEDA MENDIETA**

**QUITO – ECUADOR**

**2005**

# CERTIFICACIÓN

Certificamos que el presente proyecto titulado:

**"IP-V6 BAJO LA INFRAESTRUCTURA DE ANDINANET"**

Ha sido desarrollado en su totalidad, por el señor: **LUIS GERMÁN OJEDA MENDIETA** con **C.I. 110341103-7** bajo nuestra dirección.

| | |
|---|---|
| Ing. Fabián Sáenz | Ing. Darwin Aguilar |
| DIRECTOR | CODIRECTOR |

# AGRADECIMIENTO

Agradezco a Dios por haberme permitido culminar mi carrera con el desarrollo del presente proyecto, ya que me ha sabido guiar en cada paso del mismo.

Un agradecimiento muy sincero al Ing. Fabián Sáenz y al Ing. Darwin Aguilar director y codirector de mi tesis respectivamente, al Ing. David Guerrero Jefe del Departamento de Producción de ANDINANET, quienes me supieron brindar todo el apoyo y la colaboración durante el proceso de desarrollo del proyecto.

A todos y a cada uno de los Docentes de la Escuela Politécnica de Ejercito, en especial a los de la Facultad de Ingeniería Electrónica quienes me impartieron sus conocimientos en las aulas para mi formación profesional.

A mis Padres quienes me supieron guiar con sus consejos, a mis compañeros y amigos que siempre estuvieron dándome su apoyo en todo momento.

*Luis G. Ojeda Mendieta*

# DEDICATORIA

Dedico este proyecto a toda mi familia, quienes me han sabido dar su amor, cariño y todo su apoyo para salir siempre adelante en cada una de mis metas, llenando mi vida de sabios consejos que me han permitido ser una persona de bien para la sociedad.

En especial dedico este proyecto a una persona muy importante en mi vida "Mi Padre" que en paz descansa, y quien ansiaba con mucho orgullo que termine él proyecto con éxito.

A mi Madre, Hermanas, Sobrinos y Hermanos Políticos quienes han sido y serán por siempre parte de mi vida.

A mi Novia quien me ha sabido también dar su apoyo y todo su amor y mucho valor para terminar mi proyecto de tesis.

A cada uno de las personas que me apoyaron con el desarrollo del proyecto.

*Luis G. Ojeda Mendieta*

# PROLOGO

IP-V6 es el futuro del Internet, con nuevas miras para cada uno de los usuarios, como es: rapidez y seguridad en cada uno de los paquetes enviados por todo el mundo. El principio de la conmutación de paquetes es la piedra angular de las redes de datos modernas. IP-V6 permite una ampliación de direccionamiento IP, es decir millones de millones de usuarios en toda una red de redes como lo es Internet.

Es por estos motivos que para un crecimiento de ANDINANET S.A. se ha desarrollado el estudio de la implementación de IP-V6 sobre IP-V4, aspirando a ser uno de los líderes del mercado de IP-V6 en Ecuador y en Latinoamérica, con un servicio electrónico muy dinámico y proporcionándonos numerosas ventajas de gran utilidad para los usuarios finales.

# ÍNDICE

## CAPITULO I:

**INTRODUCCIÓN**



## CAPITULO II:

**PROTOCLOLO IP-V6**

## CAPITULO III:

**MECANISMOS DE TRANSICIÓN, TRADUCCIÓN, SEGURIDAD Y SERVICIOS EN IP-V6**

## CAPITULO IV:

**INTERACCIONES ENTRE IP-V4 E IP-V6, IMPLEMENTACIÓN Y CONFIGURACIÓN IP-V6.**



## CAPITULO V:

**ANÁLISIS DE COSTOS Y BENEFICIOS**



## CAPITULO VI:

**CONCLUSIONES Y RECOMENDACIONES**

# CAPÍTULO I

# INTRODUCCIÓN

## 1.1. INTRODUCCIÓN

IP son las siglas de **"Internet Protocol"**. El protocolo fue diseñado en los años 70 con el fin de interconectar ordenadores que estuviesen en redes separadas. Hasta entonces los equipos informáticos se conectaban entre sí mediante redes locales, pero éstas estaban separadas entre sí formando islas de información.

El nombre Internet para designar el protocolo, y posteriormente la red mundial de información, significa justamente "Inter. Red", es decir, conexión entre redes. Al principio el protocolo tuvo un uso exclusivamente militar pero rápidamente se fueron añadiendo ordenadores de universidades y posteriormente usuarios particulares y empresas.

La Internet como red mundial de información es el resultado de la aplicación práctica del protocolo IP, es decir, el resultado de la interconexión de todas las redes de información que existen en el mundo.

Cuando IP-V4 (Internet Protocol Versión 4) se estandarizó, nadie pudo imaginar que se convertiría en lo que es hoy: una arquitectura de cobertura mundial, con un número de usuarios superior al centenar de millones y con una tasa de crecimiento exponencial.

Aquella primera "Internet" fundada, sobre todo, con fines de investigación científico-técnicos y con objetivos militares, ya no se parece en nada a la actual.

Hoy, al hablar de Internet, nos referimos a una estructura de red que es la columna vertebral de las comunicaciones, una herramienta imprescindible en el mundo científico-técnico, empresarial y gubernamental.

El protocolo IP-V4 (Internet Protocol) fue diseñado para interconexión de redes. IP-V4 se ocupa de la transmisión de bloques de datos, llamados datagramas de origen a destino, donde orígenes y destinos son *hosts* identificados por direcciones de una longitud fija. De la misma manera IP-V4 también se encarga de la fragmentación de datagramas. En la actualidad el protocolo IP-V4 implementa dos funciones básicas: direccionamiento y fragmentación.

El Protocolo de Internet actualmente en uso, denominado IP-V4, ha llegado a sus limites de utilización. Problemas tales como dificultad de configuración, escasez de números IP, dificultades de transporte de datos con Calidad de Servicio y excesivo retardo en el ruteo de datagramas los mismos que en la actualidad son muy comunes.

Debido al imparable crecimiento del Internet, IP-V4 se está quedando obsoleta. Por ello, el IETF (Internet Engineering Task Force, organización encargada de la evolución de la arquitectura en la Red) ha diseñado una nueva interpretación, denominada IP-V6 (Internet Protocol Version 6). Este nuevo modelo es el sucesor de la versión 4 puesto que resuelve sus deficiencias y aporta nuevas funciones acordes a la evolución actual de la red.

De todas estas razones, la única que no tiene alternativa sobre IP-V4 es el agotamiento de direcciones: en la práctica las 232 direcciones quedan restringidas a la configuración flexible de las subredes.

Los constantes parches desarrollados durante todos estos años han permitido que la versión 4 (IP-V4) llegue a nuestros días. Aunque no se puede obviar que el principal déficit que presenta esta versión es la escasez de direcciones posibles y el bajo nivel de seguridad que ofrece.

Si bien los parches mencionados han solucionado parte del problema, estos distan mucho de ser una solución eficiente de cara a la permanente evolución que sufre la red. Estas limitaciones han incentivado al desarrollo de pruebas con una nueva versión del Protocolo de Internet (IP-V6), tendientes a la búsqueda de subsanar las deficiencias mencionadas y optimizar el uso de la red.

En nuestro país ANDINANET S.A. ha iniciado tareas de estudio, investigación y desarrollo en este campo. Como primer medida se ha tomado contacto con el área de producción para realizar un convenio de cooperación. Este convenio permitirá el estudio para la implementación del protocolo IP-V6 y su conexión con la red global de ANDINANET S.A.

El nacimiento de este nuevo protocolo (IP-V6) no ha venido solo propiciado por la escasez de direcciones IP-V4 en la actualidad, sino que además se añaden nuevas características y se mejoran las existentes. Sobre IP-V4 las tablas de rutas de los routers se están haciendo gigantescas. Las nuevas necesidades del usuario no pueden ser satisfechas de forma sencilla: seguridad, movilidad y calidad de servicio (QoS) entre otras.

Para tomar referencia sobre los problemas descriptos, podemos analizar lo mencionado sobre las limitaciones en las cantidades de direcciones IP que podemos lograr con la versión 4. La identificación de los sitios en Internet, como así también de cada uno de los usuarios, se realiza mediante un valor numérico de cuatro bytes escrito en formato decimal.

Un ejemplo de esto es la dirección 63.84.236.46 que corresponde a mail.andinanet.net. Las asignaciones de direcciones pueden ser relativas o absolutas y también varían en cuanto a su duración en el tiempo. Estas direcciones están compuestas por 4 bytes que equivalen a 32 bits. De este modo la cantidad de direcciones posibles es de $2^{32}$, es decir 4.294.967.296 de direcciones.

Debido al elevado número de servidores, computadoras, nodos, teléfonos celulares, etc. que interactúan en la Internet actual, se hacen insuficiente la cantidad de direcciones que soporta el protocolo IP-V4.

En cambio, las direcciones en el IP-V6, tienen un espacio de 16 bytes equivalentes a 128 bits. Lo que permitiría elevar la posibilidad de direcciones a $2^{128}$, es decir 3.40282366921E38 de direcciones, con lo cual el espectro de direcciones posibles se incrementaría de tal modo, que aun cuando en el futuro se conectaran a la red otros dispositivos no tradicionales como heladeras, microondas, televisores, etc., todavía sobrarían direcciones.

El nuevo direccionamiento IP establecerá las siguientes características:

**Escala.** Cada máquina presente en la red dispone de una dirección IP de 32 bits. Ello supone 4.300 millones de máquinas diferentes. Esta cifra, no obstante, es muy engañosa. El número asignado a un ordenador no es arbitrario, sino que depende de una estructura más o menos jerárquica (generalmente, pertenece a una red), lo cual ocasiona que se desperdicie una enorme cantidad de direcciones. En el año 2002 en ANDINANET S.A. se vio claramente que con el crecimiento exponencial sostenido de Internet hasta aquel momento conducía al agotamiento casi inminente del espacio de direcciones.

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

**Aumento del espacio de direcciones.** El protocolo IP-V4 que forma la Internet de hoy en día está basado en una arquitectura que utiliza direcciones de 32 bits. Con la nueva versión del protocolo, las direcciones constan de 128 bits. Esto significa, entre otras cosas, que soluciones al agotamiento de direcciones IP-V4, como el NAT, no serán necesarias.

**Multiprotocolo*:*** Cada vez resulta más necesaria la convivencia de diversas familias de protocolos: IP, OSI, IPX. Para comodidad del usuario, se necesitan

mecanismos que permitan abstraerle de la tecnología subyacente. Se tiende, pues, hacia una red orientada a aplicaciones, más que a una red orientada a protocolos como hasta el momento tiene ANDINANET S.A.

**Seguridad.** Con la aparición de servicios comerciales y la conexión de numerosas empresas, el enorme incremento en el número de usuarios por todo el planeta y la cantidad de sistemas que necesitan de Internet para su correcto funcionamiento, es urgente definir unos mecanismos de seguridad para la red. Son necesarios esquemas de autenticación y privacidad, tanto para proteger a los usuarios en sí, como la misma integridad de la red ante ataques mal intencionados o errores.

**Tiempo real.** IP-V4 define una red pura orientada a datagramas y como tal, no existe el concepto de reserva de recursos. Cada datagrama debe competir con los demás y el tiempo de tránsito en la red es muy variable y sujeto a congestión. Por ello, se necesita una extensión que posibilite el envío de tráfico de tiempo real, y así poder hacer frente a las nuevas demandas en este campo.

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

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

Lentamente, los usuarios de Internet de ANDINANET S.A. estarían adoptando como algo natural la utilización de la red, para las actividades básicas de su vida cotidiana: el trabajo, la educación o el ocio.

Podemos decir que una "desventaja" de estas nuevas direcciones es su dificultad para recordarlas dado su tamaño. Es de suponer que el servicio DNS tendrá más importancia aún.

Las principales nuevas características que aporta el IP-V6 frente al IP-V4 son:

- ✓ ***Aumento de las capacidades de direccionamiento***. IP-V6 incrementa el tamaño de dirección IP de 32 bits a 128 bits, para dar soporte a más niveles de direccionamiento jerárquico. Estos 128 bits suponen 340 cuatrillones de direcciones con lo que incluso cada grano de arena del planeta podría tener su propia dirección IP.
- ✓ ***Soporte mejorado para las Extensiones y Opciones***. Los cambios en la manera en que se codifican las opciones de la cabecera IP permiten un reenvío más eficiente, límites menos rigurosos y mayor flexibilidad para introducir nuevas opciones en el futuro.
- ✓ ***Capacidad de Etiquetado de Flujo.*** Se agrega una nueva capacidad para permitir el etiquetado de paquetes que pertenecen a "flujos" de tráfico particulares, para lo cuál, el remitente solicita tratamiento especial, como la calidad de servicio no estándar o el servicio en "tiempo real".
- ✓ ***Capacidades de Autenticación y Privacidad***. En IP-V6 se especifican extensiones para utilizar autenticación, integridad de los datos, y confidencialidad de los datos.
- ✓ ***Auto-configuración "plug and play",*** sin necesidad de servidores, y facilidades de re-configuración. Los dispositivos pueden configurar sus propias direcciones IP-V6 basándose en la información que reciban del router de la red.
- ✓ ***Mecanismos de movilidad más eficientes y robustos***. Mobile IP soporta dispositivos móviles que cambian dinámicamente sus puntos de acceso a la red, y concretamente Mobile IP-V6 permite a un host IP-V6 dejar su subred de origen mientras mantiene transparentemente todas sus conexiones presentes y sigue siendo alcanzable por el resto de Internet.

IP-V6 es un activador fundamental para la visión que tenemos de la Sociedad de Información Móvil. Actualmente, el número de teléfonos inalámbricos ya supera con creces el número de terminales fijos de Internet. En estos momentos, IP-V6 se perfila como la única arquitectura viable que puede acomodar la nueva ola de dispositivos celulares capaces de soportar Internet.

Además, IP-V6 permite la oferta de servicios y prestaciones demandadas por las infraestructuras móviles (GPRS, UMTS), redes de banda ancha, electrónica de consumo, terminales, y la subsecuente interoperatibilidad/gestión.

IP-V6 en la actualidad es la Segunda Generación, como una iniciativa de alta tecnología tiene el mismo tipo de desarrollo que Internet tuvo en sus inicios, es decir en los círculos académicos, militares y de gobierno para pronto ampliarse al público que demanda aplicaciones que se caracterizan por requerir de banda ancha, para lo cual se requiere ampliar el ya casi agotado recurso de direcciones IP de IP-V4.

El direccionamiento IP tal como se lo ha conocido y estudiado hasta ahora (IP-V4), pronto será reemplazado por la versión IP-V6, en la practica no existió IP-V5. El nuevo esquema de direccionamiento nos permite, en principio, nada menos que 2 elevado a la 96 (por diferencia entre 128 y 32) veces más direcciones (casi 80,000 cuatrillones).

Con semejante magnitud, aunque lo seleccionado no fuera lo mejor, se podría augurar que probablemente IP-V6 tendrá una supervivencia de varias décadas, en todo caso, las limitaciones provendrán de otras necesidades que puedan ir surgiendo, pero no originadas con el direccionamiento en sí.

La estructura del nuevo direccionamiento permite identificar regiones, ISP (Proveedores de Servicios de Internet), empresa o corporación, subredes, oficinas, etc. Con el nuevo formato, incluso, se puede asignar más de una dirección a la misma interfaz de una organización.

Las otras características que distinguen al protocolo IP-V6 tienen que ver especialmente con la calidad y seguridad de los servicios, estamos refiriéndonos por ejemplo, al encriptado, autenticación, manejo de tráfico en tiempo real, sensibilidad a los retardos por medio de un método de prioridades, mejoras en el proceso de enrutado, soporte de equipos móviles y configuración automática.

También se ha ampliado la longitud máxima de los paquetes, mucho más allá del límite de 64 Kb del IP-V4. Los paquetes manejados por IP-V6 se componen de un encabezamiento principal, seguido, opcionalmente, por uno o más encabezamientos extendidos y por la PDU (Unidad de Datos de Protocolo) correspondiente a la capa de Transporte.

Desde Julio del 99, se puede afirmar que IP-V6 no es una teoría, sino un hecho. La lista de corporaciones involucradas en este proyecto de migración de protocolo IP-V4 a protocolo IP-V6 es explosiva, incluyendo fabricantes, instituciones de Investigación y Desarrollo, organizaciones de Educación, Operadores de Telecomunicaciones, Empresas de Consultoría, entre otros.

Debido al auge de Internet que hemos vivido durante la última década, el espacio de direcciones IP-V4 se ha ido agotando gradualmente. ANDINANET S.A. ante este problema, que amenaza el crecimiento de la Red de redes ha iniciado el estudio para la migración hacia IP-V6.

La característica más llamativa de IP-V6, es su superior espacio de direcciones (128 bits) en comparación con el rango más modesto que su predecesor que maneja (32 bits). Durante todos estos años, los distintos problemas que han surgido con la escasez de direcciones se han ido resolviendo con el uso generalizado del NAT, y los espacios de direccionamiento privado.

Sin embargo, con la llegada de la era de la movilidad (PDAs, UMTS, edificios inteligentes, etc.), la necesidad de direcciones IP crecerá de forma exponencial, y esta vez no parece que haya ningún remedio a medio y largo plazo capaz de asegurar el desarrollo de las nuevas tecnologías basadas en Internet.

Además, IP-V6 no solo ofrece una solución al problema del agotamiento de direcciones, sino que también establece unas bases para permitir el crecimiento de forma escalable y organizada (RTP, RTPC, QoS, CoS, Kerberos, IPSec, Multicast, etc.) de una Internet en el que haya millones (sino billones) de elementos conectados, con los servicios actuales y con otros nuevos aún no imaginados, de forma más segura y flexible.

La migración de este protocolo de comunicaciones IP-V6, infinitamente más robusto y potente que su predecesor, va a convulsionar el mundo del networking desde sus cimientos al proporcionar, entre otras cosas, una provisión de direcciones IP casi ilimitada.

La capacidad de ANDINANET S.A. de ofrecer nuevos servicios, en el futuro será necesidad, a sus clientes y a sus empleados, haciéndoles más competitivos en el futuro. ANDINANET S.A. será cada vez más importante, y la adopción de IP-V6 asegura el crecimiento de cualquier organización que use Internet.

En Alhambra-Eidos, desde hace más de cuatro años, se encuentran trabajando en la adopción de IP-V6. Actualmente tienen toda la red y servicios adaptados a IP-V6, y continúan examinando de cerca el desarrollo de este nuevo protocolo, probando nuevos servicios y aplicativos, siempre con la mente puesta en cubrir las ¿futuras? (quizás ya presentes) necesidades para los clientes.

Orientado y guiado de diferentes ISP's de otros países y de acuerdo a las necesidades y al crecimiento de clientes Banda Ancha ANDINANET S.A. se encuentra en la actualidad realizando el estudio para la migración hacia el nuevo protocolo IP-V6 para de esta forma brindar un servicio mucho más confiable y seguro al usuario.

Para garantizar su correcto funcionamiento, todos los sistemas que se encuentran integrados en una red deben de tener una identificación ante esta y el resto de los dispositivos. En el caso del protocolo IP que se emplea en la actual

Internet (IP-V4) se utilizan 32 bits en bloques de 4 bytes, de forma que cada elemento de la red dispone de una dirección que debe ser única.

Un problema del actual protocolo IP viene provocado por el hecho de que Internet necesita de unos equipos llamados routers que dirigen el trafico que se genera en la red a partir de unas tablas de re-direccionamiento. Por desgracia, a medida que las direcciones IP van creciendo, estas tablas se hacen más grandes, incrementando la sensación de colapso que actualmente sentimos cuando accedamos a Internet.

Con el protocolo IPV6, las cabeceras donde se encuentra la información de control para el paquete durante su viaje a través de las redes que conforman Internet han visto reducido al mínimo sus parámetros, lo que descarga de trabajo a los routers y agiliza de esta manera el trafico de paquetes.

Continuando con las ventajas del nuevo Protocolo IP-V6, no podemos olvidarnos de las etiquetas de flujo para requerimientos de calidad de servicio. Este aspecto es fundamental ya que actualmente toda la información que circula por la red recibe la misma prioridad, mientras que gracias a la llamada garantía de calidad de servicios (QoS o Quality of service guarante) las aplicaciones podrán solicitar por si mismos una cantidad determinada de ancho de banda o una prioridad especifica.

La QoS es una de las claves de IP-V6 porque permitirá, por ejemplo, dar mas prioridad a una videoconferencia entre dos médicos que están tratando a un paciente en una complicada operación y tomar menos ancho de banda para el acceso a la Web o el correo electrónico. Por el momento lo más difícil del reparto de prioridades esta en la tarifación de las mismas, ya que todavía se tiene que desarrollar la forma en que ANDINANET S.A. pueda cobrar en un momento dado por coger un ancho de banda más grande y reducir la tarifación.

# CAPÍTULO II

# PROTOCOLO IP–V6

## 2.1. INTRODUCCIÓN

El nacimiento de este nuevo protocolo no ha venido solo propiciado por la escasez de direcciones IP-V4 en estos momentos, sino que además se añaden nuevas características y se mejoran las existentes. Sobre IP-V4 las tablas de rutas de los routers se están haciendo gigantescas. Las nuevas necesidades de los usuarios de ANDINANET S.A. no pueden ser satisfechas de forma sencilla: seguridad, movilidad y calidad de servicio (QoS) entre otras. De todas estas razones, la única que no tiene alternativa sobre IP-V4 es el agotamiento de direcciones: en la práctica las 232 direcciones quedan restringidas a la configuración flexible de las subredes con lo que el número de direcciones asignado de forma eficiente se queda en tan solo 200 millones.

Los beneficios derivados de un protocolo nuevo deben ser equilibrados por los costos asociados a la transición del sistema existente. Los desarrolladores de IP-V6 reconocieron que no todos los sistemas se actualizaran de IP-V4 a IP-V6 en el futuro inmediato y que para algunos otros sistemas, tomará algunos años.

La mayoría de las redes son sistemas heterogéneos, con diversos routers, equipos, etc. fabricados por empresas diferentes. Otro punto de traba (mucho más grande) seria la ***Word Wide Internet***, que opera a través de 24 zonas diferentes de tiempo. Actualizar este sistema en un proceso único sería aun más difícil. Dado las dificultades antes mencionadas en contraste, llega a ser necesario desarrollar estrategias que permitan la coexistencia de IP-V4 e IP-V6.

El proceso de transición a IP-V6 será muy largo, y muy probablemente nunca termine (IP-V4 no desaparecerá). Linux posee uno de los mejores *stacks* de IP-V6. MS Windows XP profesional posee un buen soporte de IP-V6, pero ha tardado mucho en llegar y a nivel de aplicaciones el soporte es muy escaso. Para la migración de ANDINANET S.A. los estudios sobre IP-V6 deben portar las aplicaciones existentes y diseñar las nuevas aplicaciones con soporte IP-V6

## 2.2. EL PROTOCOLO IP-V6

En 1992, el IETF (The Internet Engineering Task Force - Fuerza de Tarea de Ingeniería de Internet) llegó a la conclusión de que haría falta un sustituto del IP-V4 y formó un grupo de trabajo con el nombre de ***IPng*** (IP Next Generation o Siguiente Generación) que tendría la misión de desarrollar la siguiente generación del protocolo IP. De las distintas propuestas, el IETF escogió el Protocolo IP versión 6, que más tarde sería *Draft Standard*.

Llegará un momento en el que cada vehículo, electrodoméstico o instrumento existente esté conectado y controlado a través de Internet, contando con su propia dirección particular (IP).

Internet Protocol Version 6 (IP-V6) llamado también "***Ipng"*** desarrollado mediante una serie de especificaciones por la IETF ha sido creado para reemplazar la actual versión del protocolo de Internet IP-V4 e introducir mejoras significantes como cambiar las direcciones IP de 32 a 128 bits con lo que se corrige ya la actual escasez de direcciones de red.

El espectacular crecimiento del tráfico en Internet y la tan ansiada convergencia de voz, datos e imagen en una única red, hacen necesaria la evolución de las comunicaciones que van de la mano de las siglas IP. El Internet Protocol (IP), es el lenguaje en el que "habla" la Red, aparece ahora también como el elemento integrador, capaz de hacer converger todas las necesidades de comunicación de compañías y usuarios, en una misma infraestructura.

El principal problema de IP-V4 es su espacio de direcciones, de tan solo 32 bits (que teniendo en cuenta el ruteo jerárquico y las políticas de asignación de direcciones limitan la cantidad de direcciones disponibles a mucho menos que los 4 mil millones que supuestamente debería proveer). Las estimaciones actuales calculan que entre el 2004 y el 2008 se acabaran las direcciones.

IP-V6 modifica las direcciones de modo que ahora son de 128 bits, particionados en 64 para la red y 64 para el equipo (esto, permite 18446744073709551616 redes cada una con una cantidad a los efectos prácticos infinita de equipos conectados) .

Pese a ser este el principal motivo por el que se necesita IP-V6 se aprovecha el rediseño del protocolo para atender a otras necesidades:

- ✓ No solo crece la cantidad de direcciones, sino que también lo hace la cantidad de rutas en la red. Este crecimiento limita a los routers de backbone y evita que se puedan alcanzar mejores velocidades.
- ✓ IP-V6 propone un mecanismo de agregación estricta que evita ese crecimiento indiscriminado de entradas en las tablas de rutas.
- ✓ IP-V6 reestablece el modelo de conexión entre extremos, quebrado por los NAT. Para salvar el problema de la falta de direcciones muchas organizaciones emplean sistemas de traducción de direcciones llamados NAT. Estos sistemas evitan la conectividad directa entre equipos que estén tras un traductor. IP-V6 permite eliminar los NAT, ya que dejan de hacer falta.
- ✓ IP-V6 provee un conjunto de métodos que permiten la configuración automática de las redes (incluyendo la facilidad para renumerar las redes), es así que los clientes Banda Ancha que tiene ANDINANET S.A. se verán beneficiados en cuanto a calidad y servicio.

- ✓ Seguridad. IPSec es parte de las especificaciones de IPV6.

Estas son las principales características de IP-V6.

IP-V6, sucesor del actual IP-V4, implicará un aumento formidable de las direcciones disponibles, al tratarse de un sistema de 128 bits, contra los 32 bits de su predecesor. Esto quiere decir que IP-V6 usará 128 bits para cada dirección, lo que a su vez implica que la cantidad teórica de nuevas direcciones será una cifra con 39 ceros.

IP-V6 también incorporará mejores sistemas de seguridad, además de soporte para aplicaciones QoS (Quality of Service).

Los objetivos principales de ANDINANET S.A. para la implementación del protocolo IP-V6 bajo su plataforma es el aumento del espacio de direcciones ya que para a mediados de este año se pretende tener una masificación de clientes con servicio ADSL, con el aumento del espacio de direcciones se achica el tamaño de las tablas de ruteo simplificando el protocolo para poder enrutar más rápido, con mayor seguridad, mejor calidad de servicio, soporte para multicast (uno a muchos) y anycast (al más cercano de un grupo).

La mayor parte de las descripciones del futuro de la Internet ponen de relieve el ancho de banda. Pero la Internet de próxima generación IP-V6 se trata de mucho más que redes de alta velocidad, en la figura 2.2 (a), se muestra que el asunto verdadero no es lo que puede hacer la tecnología, sino lo que nosotros podemos hacer con la tecnología.

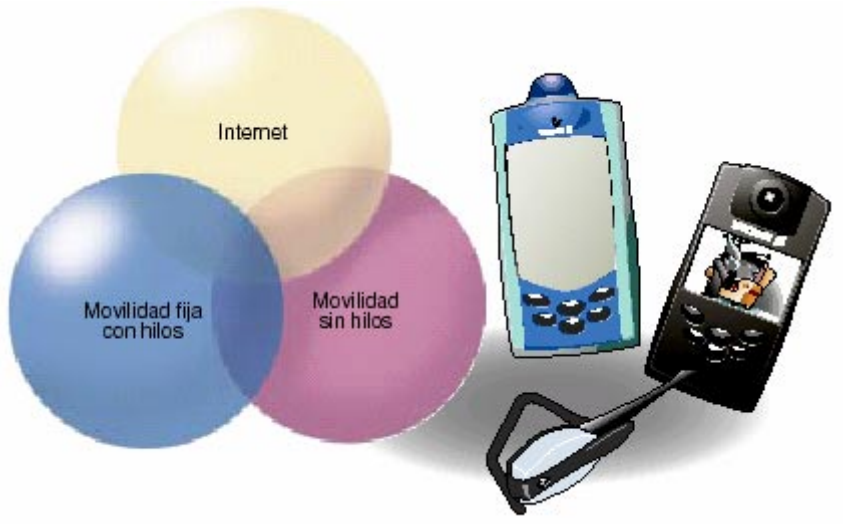



**Figura. 2.2. (a). IP-V6 y el futuro**

Es así que IP-V6 ofrece procesamiento superior de opciones de destinación, auto configuración, encabezamientos de encaminamiento, encapsulación, seguridad, y direcciones de difusión a cualquiera como se indica en la figura 2.2. (b).

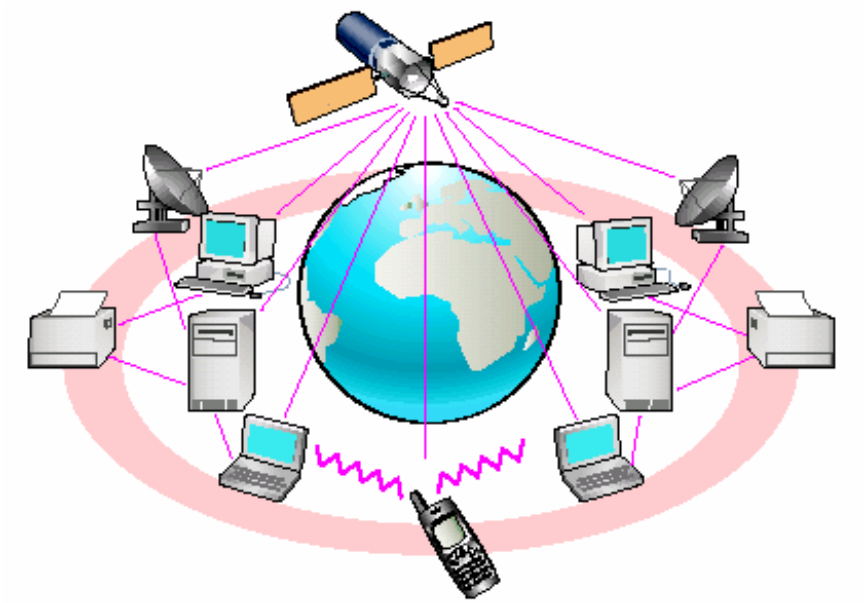


**Figura. 2.2. (b). IP-V6 y el futuro**

Una característica importante de IP-V6 es su configuración y reconfiguración que es Plug and Play con lo cual la asignación de direcciones es dinámica, así los hots pueden construir su propia dirección.

IP-V6 define tanto el mecanismo de auto configuración con control de estado como el de sin control de estado. En el caso de sin control de estado, la configuración necesaria es nula en los nodos y prácticamente nula en los routers. El mecanismo permite al host obtener una dirección a partir de información local (el identificador de interfaz) e información anunciada por los routers (el prefijo de subred). En caso de que no haya routers en la red, los hosts pueden generar sus propias direcciones de enlace local (link-local). Suficiente para comunicarse entre sí. En el caso de auto configuración con control de estado, los hosts obtienen sus direcciones y otra información de algún servidor. Este servidor puede mantener un control preciso de qué direcciones han sido asignadas a cada host. Se ha

desarrollado una versión específica de DHCP para IP-V6 llamada DHCP-V6 para tal efecto.

Cuando un nodo se conecta a la red, éste recibe los datos necesarios para empezar a comunicarse por parte del router: dirección IP-V6, máscara de red y rutas. Hay que recordar que este nuevo protocolo trata de simplificar. Con IP-V4 tenemos el DHCP (Dynamic Host Configuration Protocol, Protocolo de Configuración Dinámica de Nodo) para conseguir algo equivalente.

La movilidad es otro factor importante dentro de IP-V6. Con esta funcionalidad podremos "saltar" de una red a otra sin apenas percibir ningún cambio. Si bien esto ya es posible con IP-V4 de una manera más bien ardua, en IP-V6 es uno de los requerimientos de diseño. Esta característica será de gran importancia cuando entren en funcionamiento las nuevas redes de telefonía con tecnología UMTS.

La seguridad es otro de los requerimientos de diseño del nuevo protocolo: todas las aplicaciones se deben beneficiar de las facilidades de autenticación y encriptación de datos de forma transparente. El estándar escogido para esto es IPSec.

Así mismo el encaminamiento bajo IP-V6 es bastante similar al de IP-V4 con CIDR, es decir, jerárquico y sin clases. Con esto se pretende conseguir que las entradas en las tablas de rutas en los backbones no abunden más de lo necesario. Al mismo tiempo, se consigue simplificar el enrutamiento esperando así que los routers sean más rápidos.

Otra característica importante es el Multi-Homing. Esta funcionalidad se consigue con direcciones anycast. Una dirección anycast identifica a un conjunto de distintos interfaces, encontrándose estos, por norma general, en distintos nodos. Un paquete a una dirección anycast será entregado a un solo miembro del conjunto. En principio, el paquete será entregado al miembro más cercano según el concepto de cercano de los protocolos de encaminamiento.

Por último la Calidad de Servicio (QoS) si bien con IP-V4 se tienen bits para el control del tipo de servicio, ToS, con IP-V6 se podrá disponer de campos más amplios para definir la prioridad y flujo de cada paquete. Según el contenido de este campo, el router deberá darle un trato más o menos especial.

### 2.2.1. SIGLAS IP

Existe, como vemos, una gran coincidencia en señalar a IP como el elemento que permite hacer realidad la integración de voz, datos y contenidos multimedia en una única red. Pero, ¿cuáles son las razones que le hacen merecedor de tanta confianza?

Según la consultora Yankee Group, “las redes IP son abiertas, flexibles, robustas y estandarizadas y constituyen la única base posible sobre la que apoyar la continua innovación y el desarrollo de aplicaciones de valor añadido”.

Entre las ventajas que presenta IP, se destaca la posibilidad de integrar diversos servicios en una única red, una mejor interoperabilidad entre equipos y la posibilidad de ofrecer nuevos servicios, entre los que podemos destacar servicios multimedia basados en H.323 o SIP.

Por su parte, se apunta la eficiencia en el transporte de la información como la más importante ventaja que presenta IP. "La principal ventaja es la mayor eficiencia en el transporte de todo tipo de información, lo cual implica un significativo abaratamiento del soporte y operación de redes.

En cuanto a los nuevos servicios que permite ofrecer, aparte de los ya conocidos como multiconferencia o videoconferencia, podemos citar los servicios que surgen combinando la telefonía y la información web y otras nuevas posibilidades que surgen de combinar la telefonía y la mensajería instantánea.

Sin embargo, durante bastante tiempo, IP se ha visto acompañada de cierta incertidumbre respecto a la calidad del servicio y la seguridad de transmisión. Sin ir más lejos, en los inicios de la VoIP, la transmisión de la voz a través de Internet, no faltaron las voces críticas que aseguraban la pobre calidad y los retardos en el servicio. Ambos aspectos parecen haber sido solucionados.

"La calidad y seguridad de las redes IP están garantizadas desde hace mucho tiempo, ya que los operadores IP utilizan redes IP gestionadas (no públicas), con todos los requerimientos para asegurar la fiabilidad en las comunicaciones y en la calidad de la voz. No obstante, aún pueden encontrarse operadores que utilizan redes públicas y aún así confiesan un alto grado de satisfacción entre sus clientes".

Por lo que respecta a la seguridad de las comunicaciones, IP Security (IPSec) es la respuesta. "IPSec es un conjunto de recomendaciones y protocolos definidos para proteger intercambios de datos sobre IP, mediante encriptación de red, que proporciona seguridad extremo a extremo. El entorno de seguridad incluye soporte de servicios de confidencialidad (encriptación), autenticación (garantía de la identidad del emisor), integridad (garantía de que el contenido no ha sido modificado), así como una serie de metodologías para el intercambio de claves de encriptación".

#### 2.2.1.1. PROTOCOLO H.323

H.323 es el protocolo más utilizado para la telefonía IP. Es un estándar publicado por la ITU, organismo responsable de estandarizar muchos sistemas de comunicación a nivel internacional.

La recomendación H.323 cubre los requerimientos técnicos para los servicios de comunicaciones entre Redes Basadas en Paquetes (PBN) que pueden no proporcionar calidad de servicio (QoS).

Estas redes de paquetes pueden incluir Redes de Área Local (LAN's), Redes de Área Extensa (WAN), Intra-Networks y Inter-Networks (incluyendo Internet). También incluye conexiones telefónicas o punto a punto sobre RTC o ISDN que usan debajo un transporte basado en paquetes como PPP. Esas redes pueden consistir de un segmento de red sencillo, o pueden tener topologías complejas que pueden incorporar muchos segmentos de red interconectados por otros enlaces de comunicación.

La recomendación que describe los componentes de un sistema H.323 son: Terminales, Gateways, Gatekeepers, Controladores Multipunto (MC), Procesadores Multipunto (MP) y Unidades de Control Multipunto (MCU)

#### 2.2.1.1.1. TERMINALES

Los terminales son puntos finales de la comunicación. Proporcionan comunicación en tiempo real bidireccional. Para permitir que cualesquiera terminales ínter operen se define que todos tienen que tener un mínimo denominador que es; soportar voz y con un codec G.711. De esta manera el soporte para video y datos es opcional para un terminal H.323.

Todos los terminales deben soportar H.245, el cual es usado para negociar el uso del canal y las capacidades. Otros tres componentes requeridos son: Q.931 para señalización de llamada y configuración de llamada, un componente llamado RAS (Registrantion/Admisión/ Status), este es un protocolo usado para comunicar con el Gatekeeper; y soporte para RTP/RTCP para secuenciar paquetes de audio y video.

Otros componentes opcionales de los terminales H.323 son: los codec de video, los protocolos T.120 para datos y las capacidades MCU.

#### 2.2.1.1.2. GATEWAYS

El Gateway (o Pasarela) es un elemento opcional de una conferencia H.323. Es necesario solo si necesitamos comunicar con un terminal que está en otra red (por ejemplo RTC).

Los Gateways proporcionan muchos servicios, el más común es la traducción entre formatos de transmisión (por ejemplo H.225.0 a H.221) y entre procedimientos de comunicación (por ejemplo H.245 a H.242). Además el Gateway también traduce entre los codecs de video y audio usados en ambas redes y procesa la configuración de la llamada y limpieza de ambos lados de la comunicación.

El Gateway es un tipo particular de terminal y es una entidad llamable (tiene una dirección).

En general, el propósito del Gateway es reflejar las características del terminal en la red basada en paquetes en el terminal en la Red de Circuitos Conmutados (SCN) y al contrario. Las principales aplicaciones de los Gateways son:

- ✓ Establecer enlaces con terminales telefónicos analógicos conectados a la RTB (Red Telefónica Básica).
- ✓ Establecer enlaces con terminales remotos que cumple H.320 sobre redes RDSI basadas en circuitos conmutados (SCN).

- ✓ Establecer enlaces con terminales remotos que cumple H.324 sobre red telefónica básica (RTB).

Los Gateways no se necesitan si las conexiones son entre redes basadas en paquetes.

Muchas funciones del Gateway son dejadas al diseñador. Por ejemplo, el número de terminales H.323 que pueden comunicar a través del Gateway no es asunto de estandarización. De la misma manera el número de conexiones con los circuitos conmutados (SCN), el número de conferencias individuales soportadas, las funciones de conversión de audio/video/datos, y la inclusión de funciones multipuntos son dejadas al diseñador. Debido a la incorporación de los Gateways a la especificación H.323, la ITU posicionó H.323 como el pegamento que junta todos los terminales para conferencias funcionando juntos.

#### 2.2.1.1.3. GATEKEEPERS

Son un elemento opcional en la comunicación entre terminales H.323. No obstante, son el elemento más importante de una red H.323. Actúan como punto central de todas las llamadas dentro de una zona y proporcionan servicios a los terminales registrados y control de las llamadas. De alguna forma, el gatekeeper H.323 actúa como un conmutador virtual.

Los Gatekeepers proporcionan dos importantes funciones de control de llamada:

- ✓ Traducción de direcciones desde alias de la red H.323 a direcciones IP o IPX, tal y como está

especificado en RAS (Registrantion/Admisión/ Status).

- ✓ Gestión de ancho de banda, también especificado en RAS. Por ejemplo, si un administrador de red a especificado un umbral para el número de conferencias simultáneas, el Gatekeeper puede rechazar hacer más conexiones cuando se ha alcanzado dicho umbral. El efecto es limitar el ancho de banda total de las conferencias a alguna fracción del total existente para permitir que la capacidad remanente se use para e-mail, transferencias de archivos y otros protocolos.

A la colección de todos los Terminales, Gateways y MCU's gestionados por un gatekeeper se la conoce como Zona H.323.

Una característica opcional, pero valiosa de los gatekeepers es la habilidad para enrutar llamadas. Si se enruta la llamada por un gatekeeper, esta puede ser controlada más efectivamente. Los proveedores de servicio necesitan esta característica para facturar por las llamadas realizadas a través de su red. Este servicio también puede ser usado para re-enrutar una llamada a otro terminal en caso de estar no disponible el llamado.

Además con esta característica un gatekeeper puede tomar decisiones que involucren el balanceo entre varios gateways. Por ejemplo, si una llamada es enrutada por un gatekeeper, ese gatekeeper puede re-enrutar la llamada a uno de varios gateways basándose en alguna lógica de enrutamiento propietaria.

Mientras que un Gatekeeper está lógicamente separado de los extremos de una conferencia H.323, los fabricantes pueden elegir incorporar la funcionalidad del Gatekeeper dentro de la implementación física de Gateways y MCU's.

A pesar de que el Gatekeeper no es un elemento obligatorio, si existe, los terminales deben usarlo. RAS (Registrantion/Admisión/ Status), define para estos la traducción de direcciones, control de admisión, control de ancho de banda y gestión de zonas.

Los Gatekeepers juegan también un rol en las conexiones multipunto. Para soportar conferencias multipunto, los usuarios podrían emplear un Gatekeeper para recibir los canales de control H.245 desde dos terminales en una conferencia punto-punto. Cuando la conferencia cambia a multipunto, el Gatekeeper puede redireccionar el Canal de Control H.245 a un controlador multipunto, el MC. El Gatekeeper no necesita procesar la señalización H.245, solo necesita pasarla entre los terminales o entre los terminales y el controlador multipunto.

Las redes que posean un Gateway pueden también tener un Gatekeeper para traducir llamadas entrantes E.164 (número de teléfono convencionales) a direcciones de transporte. Debido a que una Zona está definida por su Gatekeeper, las entidad H.323 que contengan un Gatekeeper interno necesitan de un mecanismo para desactivar su funcionamiento cuando hay varias entidades H.323 que contiene un Gatekeeper dentro de la red, las entidades pueden ser configuradas para estar en la misma Zona.

Existen dos formas para que un terminal se registre en un gatekeeper, sabiendo su IP y enviando entonces un mensaje de registro Unicast a esta dirección o bien enviando un mensaje Multicast de descubrimiento del gatekeeper (GRQ) que pregunta ¿quién es mi gatekeeper?.

#### 2.2.1.1.4. UNIDADES CONTROL MULTIPUNTO (MCU)

No trata directamente con ningún flujo de datos, audio o video. Esto se lo deja a el procesador multipunto, este mezcla, conmuta y procesa audio, video y/o bits de datos. Las capacidades de los controladores multipunto y los procesadores multipunto pueden estar implementadas en un componente dedicado o ser parte de otros componentes H.323, en concreto puede ser parte de un Gatekeeper, un Gateway, un terminal o una MCU. La MCU soporta conferencias entre tres o mas extremos.

En terminología H.323, la unidad de control multipunto se compone de: Controlador Multipunto (MC) que es obligatorio, y cero o más Procesadores Multipunto (MP). El Controlador Multipunto gestiona las negociaciones H.245 entre todos los terminales para determinar las capacidades comunes para el procesado de audio y video. El Controlador Multipunto también controla los recursos de la conferencia para determinar cuales de los flujos, si hay alguno, serán multicast. Las capacidades son enviadas por el Controlador Multipunto a todos los extremos en la conferencia indicando los modos en los que pueden transmitir. El conjunto de capacidades puede variar como resultado de la incorporación o salida de terminales de la conferencia.

El Controlador Multipunto no trata directamente con ningún flujo de datos, audio o video. Esto se lo deja a el Procesador Multipunto, este mezcla, conmuta y procesa audio, video y/o bits de datos. Las capacidades del Controlador Multipunto y el Procesador Multipunto pueden estar implementadas en un componente dedicado o ser parte de otros componentes H.323, en concreto puede ser parte de un Gatekeeper, un Gateway, un terminal o una Unidad de Control Multipunto.

El Procesador Multipunto recibe flujos de audio, video o datos desde los extremos, estos pueden estar involucrados en una conferencia centralizada, descentralizada o híbrida. El Procesador Multipunto procesa esos flujos y los devuelve a los extremos.

La comunicación entre el Controlador Multipunto y el Procesador Multipunto no es asunto de estandarización.

#### 2.2.1.2. PROTOCOLO SIP

SIP (Session Initiation Protocol) es un protocolo de señalización para conferencia, telefonía, presencia, notificación de eventos y mensajería instantánea a través de Internet. Fue desarrollado inicialmente en el grupo de trabajo IETF MMUSIC (Multiparty Multimedia Session Control) y, a partir de Septiembre de 1999, pasó al grupo de trabajo IETF SIP.

SIP (Session Initiation Protocol) es para el web, el comercio electrónico, los centros de contacto, los directorios telefónicos interempresariales, las bases de datos compartidas, la telefonía IP, el transporte de imágenes, etc. “Quizás en este momento los beneficios son inasibles, porque quienes lo aprovecharán, al menos en América

Latina, atraviesan la etapa de la convergencia de red", elemento indispensable para la señalización del protocolo.

SIP (Session Initiation Protocol) es un protocolo de señalización para conferencia, telefonía y mensajería instantánea a través de internet. Utiliza protocolos de internet como HTTP (HyperText Transfer Protocol) y SMTP (Simple Mail Transfer Protocol). También usa una estructura de direcciones URL. Estas direcciones (tipo correo electrónico) permiten identificar a los usuarios en vez de reconocer dispositivos. De esta forma, SIP no depende del dispositivo y no hace distinción alguna entre voz y datos, teléfono o computadota.

Como aplicaciones diseñadas para SIP se tienen las siguientes:

- ✓ ***Call back*** (devolución de llamada). Mediante SIP, los usuarios pueden indicar su presencia en una red. Puesto que SIP usa una dirección independiente de la ubicación, es posible encontrar un individuo en la red, sin importar si está en una PC o en un teléfono móvil, y pedirle que devuelva la llamada.
- ✓ ***Conference on demand*** (Conferencia por demanda). Usando la información de presencia, puede contactarse a un individuo e introducirlo en conferencias multimodo. Los participantes pueden usar distintos dispositivos que están funcionando en redes diferentes.
- ✓ ***Servicios de traducción.*** Los correos electrónicos o de voz pueden traducirse automáticamente al idioma preferente predefinido por un usuario con base en un perfil controlado dinámicamente.
- ✓ ***Call re-routing*** (Re-enrutamiento automático de llamadas).

En resumen, SIP, como evolución del protocolo H.323, es un vehículo para transmitir aplicaciones de voz, datos o video en tiempo real, y sin importar la marca de los dispositivos ni la ubicación del destinatario.

Aunque ya se hacen pruebas piloto en Europa y Estados Unidos, en ninguna parte del mundo SIP opera como tal. El estándar todavía no está completamente definido.

La mayoría de los enlaces actuales entre empresas se hacen a través de la red pública tradicional e Internet Dedicado, ADSL o Dial-up, apoyados en correo electrónico, chat y soporte telefónico.

En un escenario con señalización SIP, la comunicación e interacción se ofrece en tiempo real y con transparencia entre emisor y receptor.

El SIP es un protocolo de señalización que ha surgido como estándar para establecer, enrutar, modificar y terminar llamadas o comunicaciones a través de las redes IP. Esa tecnología (la cual puede funcionar en cualquier tipo de red) se perfila para convertirse en el protocolo de la próxima generación de comunicaciones multimedia en Internet, incluyendo telefonía IP y comunicación unificada.

## 2.3. DIRECCIONAMIENTO IP-V6

IP-V6 ha incrementado el espacio de direccionamiento para que sea suficiente para los próximos 30 años, de tal modo que se de soporte a dispositivos móviles (pda´s, teléfonos, coches, etc.) redes residenciales HAN (Home Area Networks) y servicios de datos inalámbricos, entre otros.

ANDINANET S.A., dentro de los estudios previstos de transición de IP-V4 a IP-V6 existe una técnica que permite a los hosts y routers entunelar

dinámicamente paquetes IP-V6 sobre la infraestructura IP-V4 existente. Los nodos que vayan a utilizar esta técnica recibirán una dirección unicast IP-V6 un tanto especial: los 32 bits más bajos serán la dirección IP-V4. A este tipo de direcciones se las llama direcciones IP-V6 compatibles con IP-V4. También existe otro tipo de dirección IP-V6 que contiene a una IP-V4 y se utiliza para representar aquellos nodos que solo disponen de pila IP-V4. En este caso los 32 bits más bajos serán iguales que en el caso anterior (la dirección IP-V4), pero los 16 bits siguientes por delante serán todos 1. Este tipo de direcciones recibe el nombre de direcciones IP-V6 mapeadas en IP-V4.

El método de configuración sin control de estado se diseño con los siguientes objetivos:

- ✓ No debe ser necesaria la configuración manual de los hosts para poder comunicarse a través de la red. Un nodo debe de ser capaz de generar una dirección para cada interfaz. El mecanismo asume que cada interfaz tiene al menos un identificador único. Un identificador y un prefijo permiten obtener una dirección.
- ✓ "Sitios" de tamaño pequeño no deben de necesitar ni un servidor ni un router para comunicarse entre sí. Con las direcciones de enlace local (link local) se consigue esto. Estas se obtienen añadiendo el identificador de interfaz al prefijo de enlace local.
- ✓ "Sitios" grandes no deben necesitar un servidor de auto configuración con control de estado si no lo desean. Los routers han de ser capaces de anunciar los datos necesarios para obtener una dirección correcta, no duplicada y encaminable a través de Anuncios de Router (Router Advertisements, RA).

En la creación de las direcciones de enlace local (link local) un nodo construye una dirección de enlace local cuando alguno de sus interfaces se activa. Se considera que un interfaz se activa cuando:

- ✓ El interfaz se levanta al arrancar el sistema.
- ✓ El interfaz es reiniciado después de haber sido desactivado.

- ✓ El interfaz se engancha al enlace por primera vez.

La dirección de enlace local (link local) se construye añadiendo el identificador de interfaz al prefijo FE80::0 (del tamaño adecuado). Si el identificador de interfaz tiene una longitud de N bits, el identificador reemplazará los N bits más a la derecha del prefijo. En caso de que el identificador de interfaz sea mayor de 118 bits, el mecanismo de auto configuración falla y requerirá intervención manual. Por norma general, esto no sucederá ya que el identificador de interfaz seguirá la norma EUI-64 y tendrá un tamaño de 64 bits.

La creación de direcciones globales y de "sitio" local (site local) se construyen a partir de un prefijo anunciado en los RA y el identificador del interfaz. Los routers mandan de forma periódica RA a la dirección multicast predefinida de "Todos los nodos". Si un nodo desea recibir un RA más pronto puede enviar uno o más RS. Para saber si hay o no hay routers en el enlace, un nodo debe haber enviado varios RS y no haber obtenido ningún RA en un periodo razonable de tiempo. En este caso el nodo debe probar autoconfigurarse con el mecanismo de control de estado. Estos son los pasos a seguir por un nodo a la hora de procesar las opciones de información de prefijo de cada Anuncio de Router:

- ✓ Si el prefijo es el de enlace local (link local), debe descartarlo de forma silenciosa.
- ✓ Si el tiempo de vida del prefijo es mayor que el tiempo válido de vida, debe ignorar la información del prefijo de forma silenciosa.
- ✓ Si el prefijo anunciado tiene un tiempo válido de vida mayor que 0 y no ha formado ya una dirección a partir de este prefijo, debe construirla y añadirla.
- ✓ Si el prefijo anunciado coincide con alguno a partir del cual hemos construido alguna dirección las acciones a tomar dependerán del tiempo válido de vida del prefijo.

Para IP-V6 se utilizan 128 bits en lugar de los 32 bits que se utilizan en IP-V4, siendo los tipos de direcciones los siguientes:

- ***Direcciones UNICAST***. Son direcciones asignadas a un único interfaz. Se han definido direcciones especiales.

Existen varios tipos de direcciones unicast en IP-V6, como las globales agregables, las site local, las link local, las IPX jerárquicas, la NSAP, y las compatibles IP-V4. Más tipos de direcciones pueden ser definidos en el futuro. Ver tabla 2.3.

| Asignación | Prefijo |
|---|---|
| Reservado | 0000 0000 |
| No asignado | 0000 0001 |
| Reservado para asignación NSAP | 0000 001 |
| Reservado para asignación IPX | 0000 010 |
| No asignado | 0000 011 |
| No asignado | 0000 1 |
| No asignado | 0001 |
| Direcciones Unicast Globales Agregables | 001 |
| No asignado | 001 |
| No asignado | 010 |
| No asignado | 011 |
| No asignado | 100 |
| No asignado | 101 |
| No asignado | 110 |
| No asignado | 1110 |
| No asignado | 1111 0 |
| No asignado | 1111 10 |
| No asignado | 1111 110 |
| No asignado | 1111 1110 0 |
| Direcciones Unicast Link-Local | 1111 1110 10 |
| Direcciones Unicast Site-Local | 1111 1111 11 |
| Direcciones Multicast | 1111 1111 |

**Tabla. 2.3. Direcciones Unicast**

Las direcciones especiales definidas para Unicast son:

1. ***Dirección loopback [::1]:*** se asigna a una dirección virtual a la que el host puede enviar paquetes. La dirección unicast 0:0:0:0:0:0:0:1 recibe el nombre de *loopback* y su equivalente en IP-V4 es 127.0.0.1. Se utiliza para la comunicación entre servicios de un mismo nodo y nunca se debe mandar un paquete con esta dirección

tanto de origen como destino sobre un medio físico. Con esto queda claro que no se puede asignar a interfaces reales, sino a interfaces virtuales (como el interfaz de loopback).

2. ***Dirección inespecífica:*** esta dirección se utiliza como dirección de fuente durante el proceso de autoconfiguración. Equivale a la dirección 0.0.0.0 de IP-V4. Para IP-V6 será la dirección 0:0:0:0:0:0:0:0. Esta nunca debe ser asignada a ningún nodo y sólo se permite su uso en casos bien contados, como en el campo de dirección origen cuando un interfaz no conoce todavía la suya. Bajo ningún concepto se debe usar esta dirección como dirección destino de un paquete IP-V6 o en la cabecera de encaminamiento.
3. ***Direcciones compatibles [::<dirección IP-V4>***): se utilizan cuando se necesita enviar tráfico IP-V6 a través de redes IP-V4 mediante túneles. Los puntos finales de estos túneles pueden ser host o routers. Las direcciones de este tipo se forman añadiendo 96 bits a ´0´ delante de una dirección válida IP-V4. Este tipo de direcciones compatibles se recomienda para ANDINANET.SA.
4. ***Direcciones mapeadas a IP-V4 [::HF<dirección IP-V4>]:*** estas direcciones se utilizan cuando un host IP-V6 se quiere comunicar con un host IP-V4. Esto requiere una pila doble de protocolos en el host o en el router para la traducción de cabeceras. Este tipo de direcciones sería otra alternativa de direccionar a los clientes de ANDINANET S.A..
5. ***Direcciones de ámbito local***: pueden utilizarse únicamente dentro de la red física a la que la interfaz del host está conectada.
6. ***Direcciones de ámbito privado:*** estas direcciones no pueden ser enrutadas a través de Internet. Las direcciones equivalentes en IP-V4 son: 10.0.0.0, 176.16.0.0 - 176.31.0.0, 192.168.0.0 - 192.168.255.0.
7. ***Direcciones unicast globales:*** se espera que lleguen a ser el formato de dirección predominante para la conexión de los nodos a Internet.

En la figura 2.3 (a) se puede ver un ejemplo de comunicación entre tres nodos con direcciones A, B y C. Y su comportamiento:

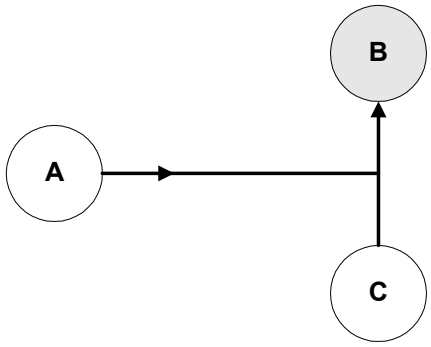



**Figura. 2.3. (a). Ejemplo comportamiento Unicast**

- ***Direcciones MULTICAST:*** son identificadores asignados a un conjunto de interfaces en múltiples hosts. Los paquetes que se envían a una de estas direcciones se hacen llegar a todas las interfaces que tienen asignada esta dirección. No hay direcciones de broadcast en IP-V6, ya que su funcionalidad queda asumida por las direcciones multicast. Algunas direcciones de propósito especifico son:

  1. ***FF01::1:*** todas las interfaces del host.
  2. ***FF02::1:*** todos los sistemas del ámbito local.
  3. ***FF01::2:*** todos los routers locales a un host dado.
  4. ***FF02::2:*** todos los routers que pertenecen a la misma red de área local.
  5. ***FF05::2:*** todos los routers dentro de un mismo ámbito privado.
  6. ***FF02::B:*** agentes móviles dentro de la misma red de área local.
  7. ***FF02::1:2:*** todos los agentes DHCP dentro de una misma red de área local.
  8. ***FF05::1:3:*** todos los servidores DHCP dentro de un mismo ámbito privado.

  En la figura 2.3 (b) se puede ver un ejemplo de comunicación entre nodos con direcciones A, B y los distintos comportamientos de comunicación.

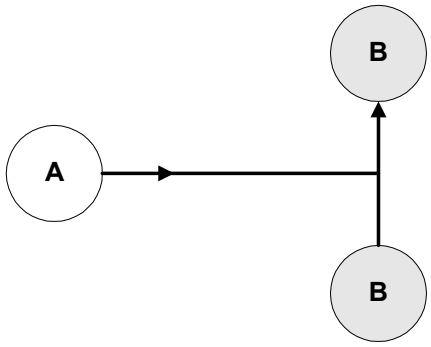



**Figura. 2.3. (b). Ejemplo comportamiento Multicast**

- ***Direcciones ANYCAST:*** son un tipo especial de direcciones *unicast* que se asignan a interfaces en múltiples hosts. Los paquetes que se envían a esta dirección se hacen llegar a la interfaz más cercana que tenga esta dirección. Son direcciones experimentales. Este tipo de direcciones pueden ser asignadas a distintas interfaces de uno o varios nodos, de forma que un paquete enviado a una dirección *anycast* llegará a uno y sólo a uno de las interfaces. Sintácticamente, las direcciones *anycast* no pueden ser distinguidas de las *unicast*. En la actualidad, se tiene poca experiencia con las direcciones *anycast* por lo que se han impuesto las restricciones:

  1. No se puede enviar un paquete con dirección origen que sea de tipo *anycast*.
  2. Una dirección *anycast* no puede ser asignada a un host, sólo a routers.

  A pesar de las restricciones, las direcciones *anycast* ya se están utilizando por ejemplo para que un nodo móvil contacte con alguno de sus routers en su red de casa.

  En la figura 2.3 (c) se puede ver un ejemplo de comunicación entre nodos con direcciones A, B y los distintos comportamientos de comunicación.

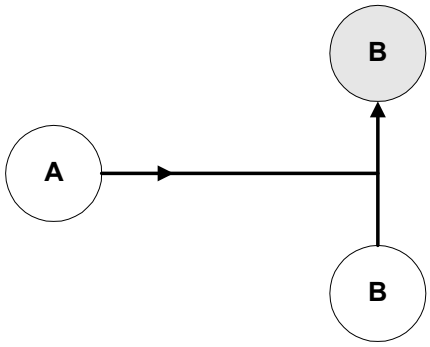


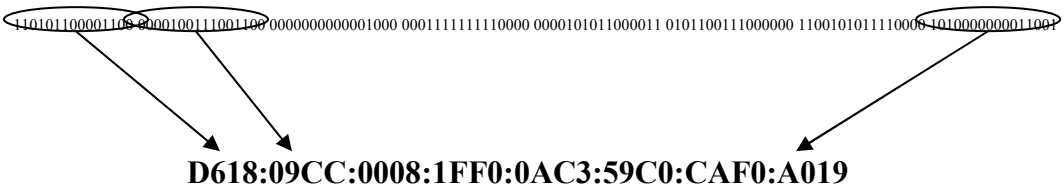

**Figura. 2.3. (c). Ejemplo comportamiento Anycast**

Las direcciones IP-V6 se representan como series de campos hexadecimales de16 bits separados por "**:**", con un formato ***X:X:X:X:X:X:X:X***, mientras que para IP-V4 se mantiene con un formato ***X.X.X.X***.

El direccionamiento para IP-V6 implica 128 bits (16 bytes) mientras que para IP-V4 se tienen 32 bits (4 bytes). Al direccionamiento IP-V6 se lo expresa en notación hexadecimal con dos puntos.

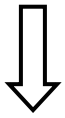
Así los 128 bits se dividen en 8 secciones, de 2 bytes (16 bits) de longitud. Los 2 bytes se expresan con 4 dígitos hexadecimales, por tanto, la dirección IP consta de 32 dígitos hexadecimales, con cada 4 dígitos separados por dos puntos.

Un *ejemplo* de cómo quedaría una dirección IP-V6 es:




El direccionamiento IP-V6 también se lo puede realizar con direcciones abreviadas. Normalmente, en una dirección IP hay muchos dígitos que son 0, en esos casos, se puede abreviar la dirección. Es así que los 0's al inicio de una sección de pueden omitir. *Ejemplo:*

**D618 : 09CC : 0008 : 1FF0 : 0AC3 : 59C0 : CAF0 : A019**



**D618:9CC:8:1FF0:AC3:59C0:A019**

Además, si hay secciones consecutivas que son todos 0's, se pueden eliminar y poner dos puntos seguidos (solo una vez por dirección). Por ejemplo:

**D618:09CC:0000:0000:0AC3:0000:CAF0:A019**

**D618:9CC:0::AC3:0:CAF0:A019**

Al direccionamiento en IP-V6 se lo hace por categorías como se describió anteriormente:

- ✓ ***UNICAST (Unidestino).-*** se refieren a un único nodo de la red (dirección de interfaz de la red).
- ✓ ***MULTICAST (Multidestino).-*** se refiere a un conjunto de nodos de red. Un paquete dirigido a una dirección multidestino debe ser entregado a todos los nodos del grupo.
- ✓ ***ANYCAST (A cualquier destino).-*** también se refiere a un conjunto de nodos en la red. Un paquete dirigido a una dirección "a cualquier destino" debe ser entregado *"solamente a uno"* de los nodos del grupo. Por ejemplo: conexión de una estación móvil al router más cercano de entre un conjunto de ellos.

### 2.3.1. NOTACIÓN DE LAS DIRECCIONES IP-V6

Formas de representar las direcciones IP-V6:

- ✓ Ocho enteros de 16 bits en hexadecimal separados por "**:**" *Ejemplo:*

ABCD:0000:0000:0000:9ABC:0700:C035:0453
ABCD:0:0:0:9ABC:700:C035:453

- ✓ Simplificación de cadenas de ceros: *Ejemplo:*

ABCD::9ABC:700:C035:453
El loopback (0:0:0:0:0:0:0:1) quedaría 1.

- ✓ Para entornos mixtos IP-V4 e IP-V6 se pueden representar los últimos 4 bytes en "dotted-decimal". *Ejemplo:*

ABCD::9ABC:700:**63.81.237.1**

### 2.3.1.1. ESTRUCTURA DE LAS DIRECCIONES UNICAST GLOBALES AGREGABLES

El la figura 2.3.1.1 se indica como esta establecida la estructura para las direcciones *unicast* globales agregables.

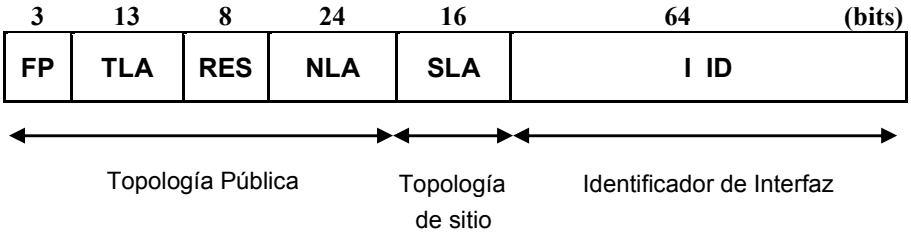



**Figura. 2.3.1.1. Estructura de direcciones Unicast**

- FP: Format Prefix (001).
- TLA: Top-Level Aggregation Identifier.
- RES: Reservado (0's).
- NLA: Next-Level Aggregation Identifier.
- SLA: Site-Level Aggregation Identifier.
- I ID: Interface Identifier.

1. Los campos TLA y NLA permiten asignación jerárquica en base a dos niveles de proveedor.
2. El campo SLA posibilita la división en subredes dentro de un sitio.
3. El campo I ID se puede generar a partir de un identificador de la interfaz o de la máquina.
4. Se utiliza el formato EUI-64 y una forma usada es generarlo a partir de la dirección MAC (Ethernet) de 48 bits de la interfaz.

### 2.3.2. ASIGNACIÓN DEL ESPACIO DE DIRECCIONES

Las direcciones IP se dividen en dos partes como se indica en la figura 2.3.2.. La primera es el prefijo de tipo la misma que es de longitud variable, determina el objetivo de la dirección y los valores de los códigos se determinan de manera que ningún código sea igual que la parte inicial de cualquier código.

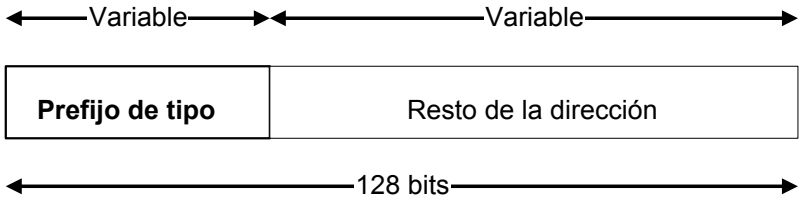



**Figura. 2.3.2. Asignación del espacio de direcciones**

### 2.3.3. PREFIJOS PARA LAS DIRECCIONES IP-V6

| Prefijo | Tipo | Fracción | Prefijo | Tipo | Fracción |
|---|---|---|---|---|---|
| 0000 0000 | Resevado | 1/256 | 011 | Reservado | 1/8 |
| 0000 0001 | Resevado | 1/256 | 100 | Dirección unidestino geográfica | 1/8 |
| 0000 001 | Punto de Acceso a servicio de red (NSAP) | 1/128 | 101 | Reservado | 1/8 |
| 0000 010 | IPX (Novell) | 1/128 | 110 | Reservado | 1/8 |
| 0000 011 | Resevado | 1/128 | 1110 | Reservado | 1/16 |
| 0000 100 | Resevado | 1/128 | 1111 0 | Reservado | 1/32 |
| 0000 101 | Resevado | 1/128 | 1111 10 | Reservado | 1/64 |
| 0000 110 | Resevado | 1/128 | 1111 110 | Reservado | 1/128 |
| 0000 111 | Resevado | 1/128 | 1111 1110 0 | Reservado | 1/512 |
| 0001 | Resevado | 1/16 | 1111 1110 10 | Dirección local de enlace | 1/1024 |
| 001 | Resevado | 1/8 | 1111 1110 11 | Dirección local de enlace | 1/1024 |
| 010 | Dirección unidestino basada en proveedor | 1/8 | 1111 1111 | Dirección multidestino | 1/256 |

**Tabla. 2.3.3. Prefijos IP-V6**

### 2.3.4. DIRECCIONES UNICAST BASADAS EN ANDINANET

Son el tipo de direcciones que se emplearán para identificar un nodo de red. El formato de la dirección se indica en la figura 2.3.4:

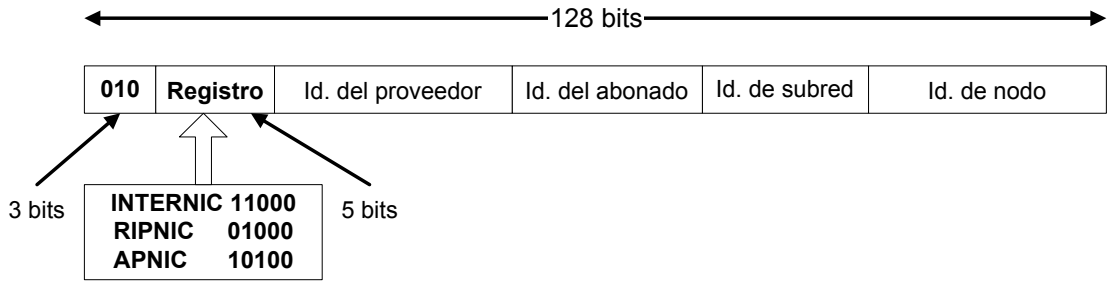
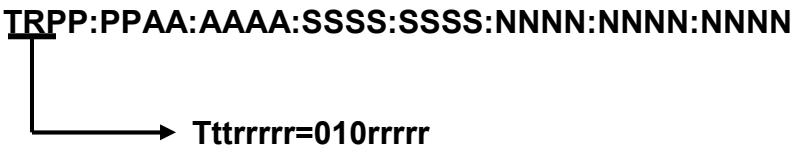



**Figura. 2.3.4. Formato de dirección IP-V6**

Los diferentes campos de la dirección estaría denotada de la siguiente forma:

- ✓ Identificador de tipo (010)
- ✓ Identificador de registro (5 bits): agencia que ha registrado la dirección INTERNIC para Norteamérica, RIPNIC para Europa, APNIC para Asia y Pacífico.
- ✓ Identificador de proveedor: proveedor de acceso a Internet en este caso ANDINANET S.A.. Se recomiendan 16 bits.
- ✓ Identificador de abonado: identificador que se asigna a una organización que se conecta a Internet. Se recomiendan 24 bits.
- ✓ Identificador de subred: define una subred especifica bajo el dominio del abonado. Se recomiendan 32 bits.
- ✓ Identificador de nodo: define la identidad del nodo conectado a la subred. Se recomiendan 48 bits, para que sea compatible con las direcciones Ethernet.
- ✓ El esquema jerárquico de direccionamiento quedaría denotado de la siguiente manera:




### 2.3.5. DIRECCIONES IP-V4 MAPEADAS EN DIRECCIONES IP-V6

Dentro de los mecanismos previstos de transición de IP-V4 a IP-V6, existe una técnica que permite a los hots y routers entunelar dinámicamente paquetes IP-V6 sobre la infraestructura IP-V4 existente y con la cual se encuentra ANDINANET S.A. Los nodos que vayan a utilizar está técnica recibirán una dirección *Unicast* IP-V6 donde los 32 bits más bajos serán la dirección IP-V4. Por *ejemplo*:

4818:9CC::1FF0:AC3:0:3F54:ED1 ⇨ 4818:9CC::1FF0:AC3:0:63.84.237.1

Este tipo de direcciones son direcciones IP-V6 compatibles con IP-V4, donde la dirección 63.84.237.1 pertenece a uno de los ruteadores principales de ANDINANET S.A..

Hay otro tipo de dirección IP-V6 que contiene a una IP-V4 y se emplea para representar aquellos nodos que solo disponen de pila IP-V4. En este caso los 32 bits más bajos serán iguales que en el caso anterior (la dirección IP-V4), pero los 16 bits siguientes por delante serán todos 1. Por *ejemplo*:

4818:9CC::1FF0:AC3:HF: 3F54:ED1

⇩

4818:9CC::1FF0:AC3:FFFF:63.84.237.1

A este tipo de direcciones se las denomina direcciones IP-V6 mapeadas en IP-V4.

### 2.3.6. FORMATO DEL PAQUETE IP-V6

El formato del paquete para IP-V6 se forma de dos partes como se indica en la figura 2.3.6:

1. Cabecera base obligatoria (40 bytes)
2. Carga:

   - ✓ Cabeceras de ampliación (opcionales)
   - ✓ Datos del nivel superior

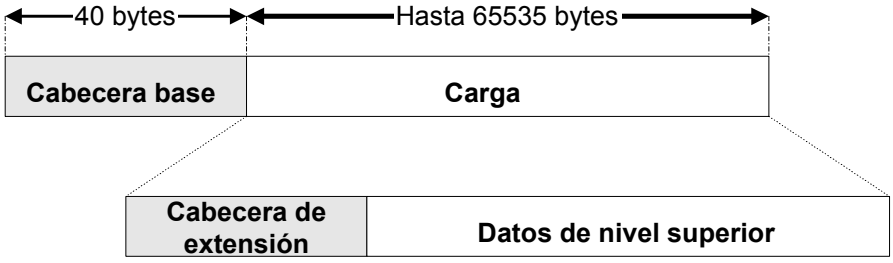



**Figura. 2.3.6. Formato del paquete IP-V6**

### 2.3.6.1. CABECERA BASE

- ✓ Versión (VER): número de versión de IP. Misma posición y formato que el campo de IP-V4.
- ✓ Prioridad (PRI): define la prioridad del paquete
- ✓ Etiqueta de flujo: permite ofrecer un tratamiento especial a los paquetes de un flujo de datos.
- ✓ Longitud de la carga: longitud total del datagrama, excluyendo la cabecera base.
- ✓ Cabecera siguiente: define la cabecera que sigue a la cabecera base. Puede ser una cabecera de ampliación de IP, o una cabecera con información del nivel superior (TCP, UDP). Todas las cabeceras de ampliación contienen este campo. Equivale al campo protocolo de la cabecera de IP-V4.

En la figura 2.3.6.1 se muestra la distribución de bits para cada una de las partes de la cabecera base.


**Figura. 2.3.6.1. Cabecera Base**

| Código | Cabecera siguiente |
|---|---|
| 0 | Opción salto a salto |
| 2 | ICMP |
| 6 | TCP |
| 17 | UDP |
| 43 | Encaminamiento origen |
| 44 | Fragmentación |
| 50 | carga de seguridad cifrada |
| 51 | Autenticación |
| 59 | Nula |
| 60 | Opción destino |

**Tabla. 2.3.6.1. Códigos de la Cabecera Siguiente**

- ✓ Límite de salto: equivale al campo TTL de la cabecera IP-V4
- ✓ Dirección origen: dirección del emisor del datagrama
- ✓ Dirección destino. Normalmente, identifica al destino final del datagrama. Si se emplea encaminamiento fuente, este campo contiene la dirección del siguiente encaminador.

#### 2.3.6.1.1. CABECERA BASE. Prioridad

El valor del campo prioridad define la prioridad de cada datagrama en relación a otros paquetes con el mismo origen. IP-V6 divide el tráfico en dos amplias categorías:

- ✓ Tráfico con control de congestión.
  - El emisor adapta su tasa de emisión de paquetes a la carga de la red. *Ejemplo:* Protocolo TCP.
  - A los datos de este tipo de tráfico se les asigna prioridades entre 0 (más baja) y 7 (más alta)

- ✓ Tráfico sin control de congestión.

  - Los datos de este tipo de tráfico esperan un retardo mínimo.
  - No es deseable el descarte de paquetes.
  - No es viable la retransmisión de los datos. *Ejemplo:* audio o vídeo en tiempo real.
  - La prioridad en este caso es una indicación de cuánto afecta la pérdida de información a la calidad de los datos recibidos. Valores entre 8 (más baja, datos con más redundancia) y 15 (más alta, datos con menos redundancia)

Prioridad del tráfico con control de congestión, ver tabla 2.3.6.1.1.:

| PRI | Tipo de tráfico | Significado |
|---|---|---|
| 0 | Ningún tráfico específico | Prioridad no definida |
| 1 | Tráfico de fondo | Ejemplo: noticias |
| 2 | Tráfico de datos no esperados | El receptor no sabe que le va a llegar la información, y un poco de retardo no importa. Ejemplo: correo electrónico |
| 3 | Reservado | |
| 4 | Tráfico de gran cantidad de datos separados | Transferencia de grandes volúmenes de datos mientras el usuario espera. Ejemplo: HTTP, FTP |
| 5 | Reservado | |
| 6 | Tráfico interactivo | Ejemplo: TELNET |
| 7 | Tráfico de control | Ejemplo: Protocolos de Encaminamiento (RIP, IGRP, OSPF...) y gestión (SNMP) |

**Tabla. 2.3.6.1.1. Prioridad Cabecera Base**

### 2.3.6.1.2. CABECERA BASE. Etiquetas de Flujo

Flujo es la secuencia de paquetes enviados desde un emisor determinado a un destino que necesita acciones especiales en los encaminadores.

Desde el punto de vista del encaminador, un flujo es una secuencia de paquetes que comparten las mismas características, como la circulación por el mismo camino, uso de los mismos recursos, mismo tipo de seguridad, etc..

Un encaminador que soporte el manejo de etiquetas de flujo mantiene una tabla con dichas etiquetas; una entrada por cada etiqueta activa, cada entrada define los servicios requeridos por los paquetes que lleven la etiqueta de flujo correspondiente.

Cuando llega un paquete al encaminador, éste busca en su tabla de etiquetas la entrada correspondiente para la etiqueta del paquete, y le aplica los servicios descritos en dicha entrada.

Los servicios de definen mediante las opciones salto a salto, o protocolos de nivel superior. La forma más sencilla de emplear las etiquetas de flujo es para acelerar el procesamiento de los paquetes dentro del encaminador. Para obtener el siguiente salto, es más eficiente consultar la tabla de etiquetas que ejecutar el algoritmo de encaminamiento.

Otro uso posible es ayudar a la reserva de recursos a lo largo de una ruta para las trasmisiones de audio y video lo mismo que sirve de soporte a otros protocolos de nivel superior.

Las reglas de uso de las etiquetas de flujo son:

1. Número aleatorio [1 .. $2^{24} - 1$]
2. Un origen no debe reutilizar una etiqueta de flujo para un nuevo flujo ya existente esté todavía activo.

3. Si un nodo no soporta las etiquetas de flujo, pone ese campo a cero. Si un encaminador no soporta el campo, lo ignora.
4. Todos los paquetes del mismo flujo deben tener el mismo origen, destino, prioridad y opciones.

#### 2.3.6.1.3. COMPARATIVAS DE LAS CABECERAS IP-V4 E IP-V6

En la tabla 2.3.6.1.3. se describe las comparativas que existe entre las cabeceras IP-V4 e IP-V6:

| Campo IP-V4 | Equivalente IP-V6 |
|---|---|
| Longitud de cabecera | Eliminado (cabecera de tamaña fijo) |
| Tipo de servicio (TOS) | Reemplazado por Prioridad + Etiqueta de flujo |
| Longitud total | Reemplazado por Longitud de la carga |
| Identificador, flags, y desplazamiento de fragmento | Se trasladan a la cabecera de ampliación de fragmentación |
| TTL | Límite de saltos |
| Protocolo | Cabecera siguiente |
| Checksum cabecera | No existe (la proporcionan protocolos de nivel superior) |
| Opciones IP-V4 | Cabeceras de ampliación |

**Tabla. 2.3.6.1.3. Cabeceras IP-V4 e IP-V6**

#### 2.3.6.1.4. CABECERAS DE AMPLIACIÓN

La longitud de la cabecera base de un datagrama IP-V6 es siempre de 40 bytes. La cabecera base puede ser seguida por hasta 6 cabeceras de ampliación las mismas que proporcionan mas funcionalidad al datagrama IP. Los 6 tipos de cabeceras son como se describe a continuación en la tabla 2.3.6.1.4:

| Código | Significado |
|---|---|
| 0 | Opción salto a salto |
| 43 | Encaminamiento origen |
| 44 | Fragmentación |
| 50 | Carga de seguridad cifrada |
| 51 | Autenticación |
| 60 | Opción destino |

**Tabla. 2.3.6.1.4. Cabeceras de ampliación**

En la figura 2.3.6.1.4. se indica los diferentes saltos de las cabeceras de amplificación:

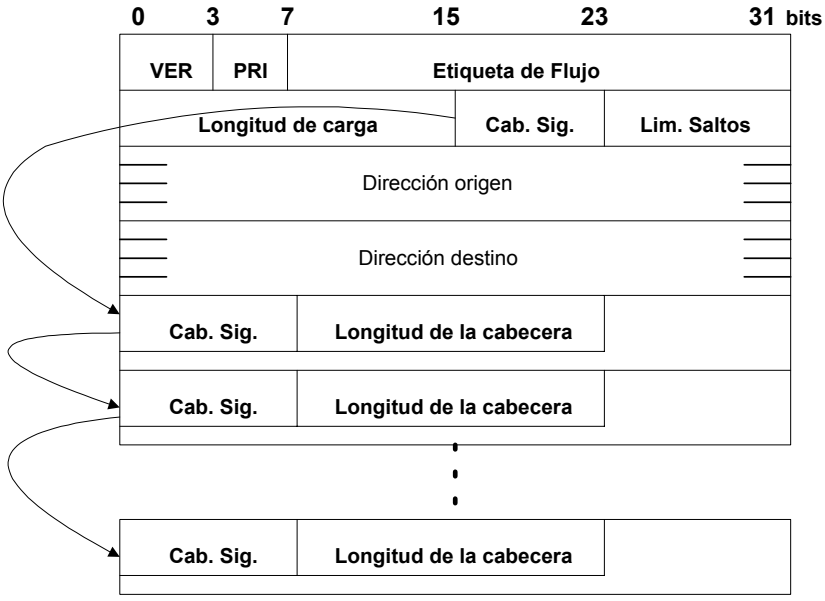



**Figura. 2.3.6.1.4. Cabecera de ampliación**

### 2.3.6.1.5. DATAGRAMA IP-V6

El datagrama para el protocolo IP-V6 se encuentra formado como se describe en la figura 2.3.6.1.5.

En el datagrama se explica la funcionalidad de cada uno de los componentes del mismo:

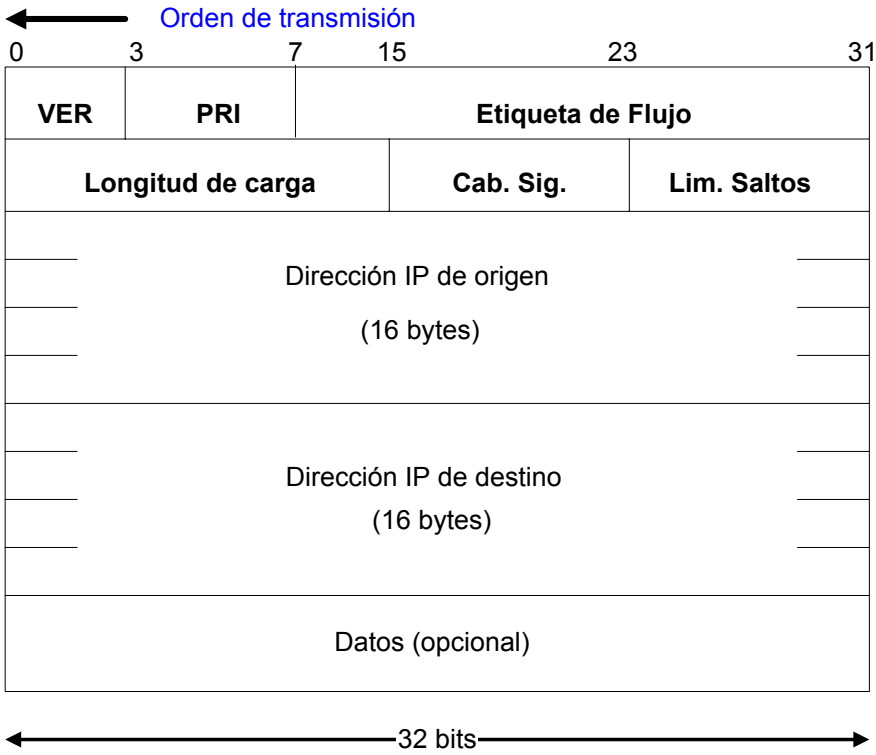



**Figura. 2.3.6.1.5. Datagrama IP-V6**

### 2.3.6.1.5.1. VERSIÓN (VER)

Este campo ocupa 4 bits, e indica la versión de IP. Para el formato descrito, la versión es la 6, para IP-V6. Ver figura 2.3.6.1.5.1..

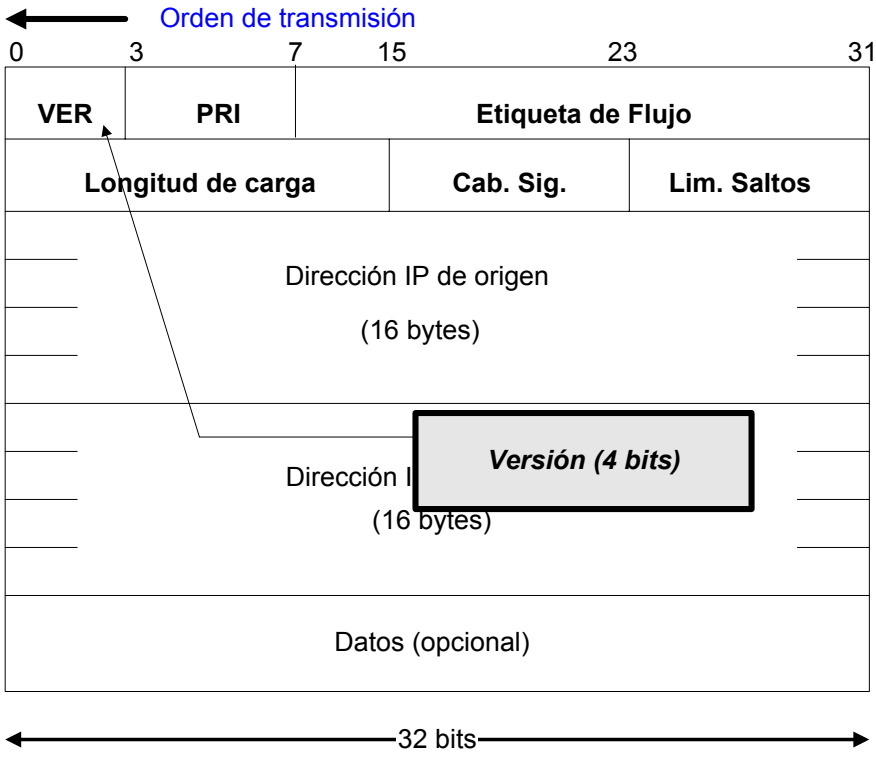



**Figura. 2.3.6.1.5.1. Datagrama IP-V6 "VER"**

### 2.3.6.1.5.2. PRIORIDAD (PRI)

Este campo ocupa 4 bits, e indica la prioridad que el remitente desea para los paquetes enviados, respecto a los demás paquetes enviados por él mismo. Los valores de prioridad se dividen en dos rangos, de 0 a 7, paquetes para los cuales el remitente espera una respuesta en caso de congestión (tráfico TCP). Y de 8 hasta 15, paquetes que no deben ser respondidos en caso de congestión, el valor más bajo (8), se usaría cuando el remitente está dispuesto a que sus paquetes sean descartados en caso de congestión (video en alta calidad). Y el valor más alto (15), cuando el remitente está muy poco dispuesto a que algún paquete sea descartado (Audio de baja calidad). Ver figura 2.3.6.1.5.2.

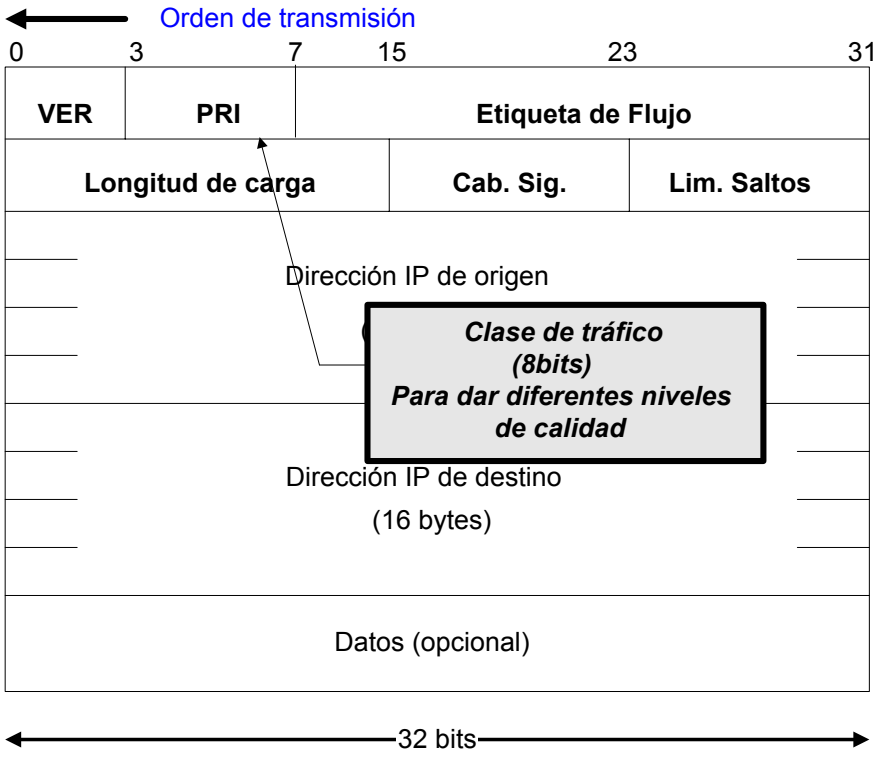



**Figura. 2.3.6.1.5.2. Datagrama IP-V6 "PRI"**

### 2.3.6.1.5.3. ETIQUETA DE FLUJO

Este campo ocupa 24 bits, y es usado por el remitente para indicar que sus paquetes sean tratados de forma especial por los routers, como en servicios de alta calidad o en tiempo real. En este punto, se entiende el flujo como un conjunto de paquetes que requieren un tratamiento especial.

Todos los paquetes pertenecientes al mismo flujo deben tener valores similares en los campos dirección origen, dirección destino, prioridad, y etiqueta de flujo. Ver figura 2.3.6.1.5.3..

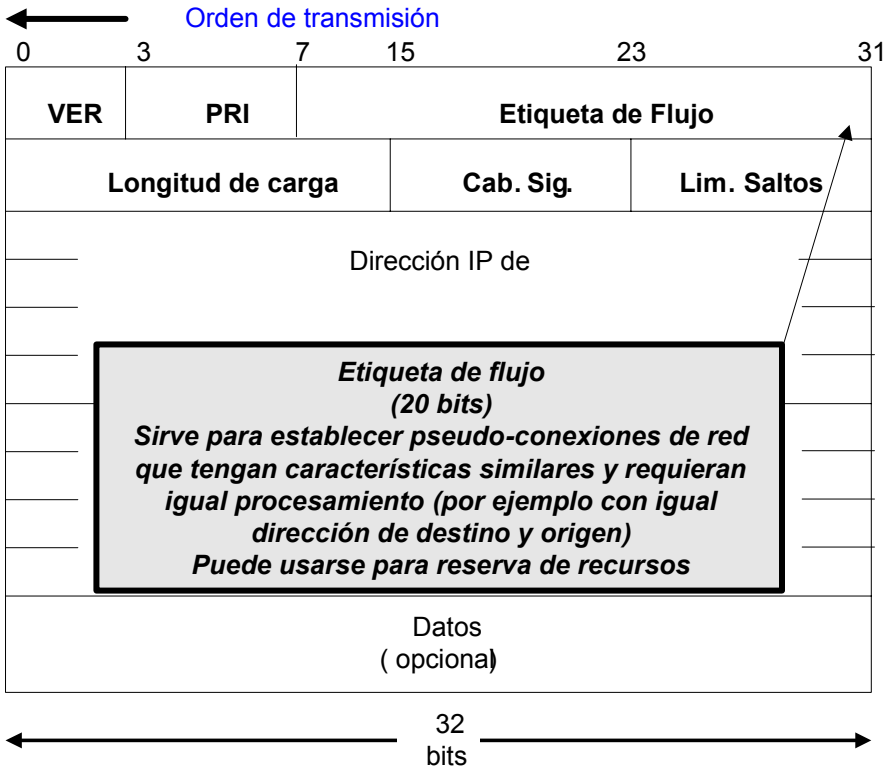



**Figura. 2.3.6.1.5.3. Datagrama IP-V6 "Etiqueta de Flujo"**

### 2.3.6.1.5.4. LONGITUD DE CARGA

Este campo ocupa 16 bits, e indica la longitud del resto del paquete que sigue a la cabecera, en octetos. Si su valor es cero, indica que el tamaño de la carga vendrá especificado como "Carga Jumbo", en una opción "salto a salto". Ver figura 2.3.6.1.5.4..

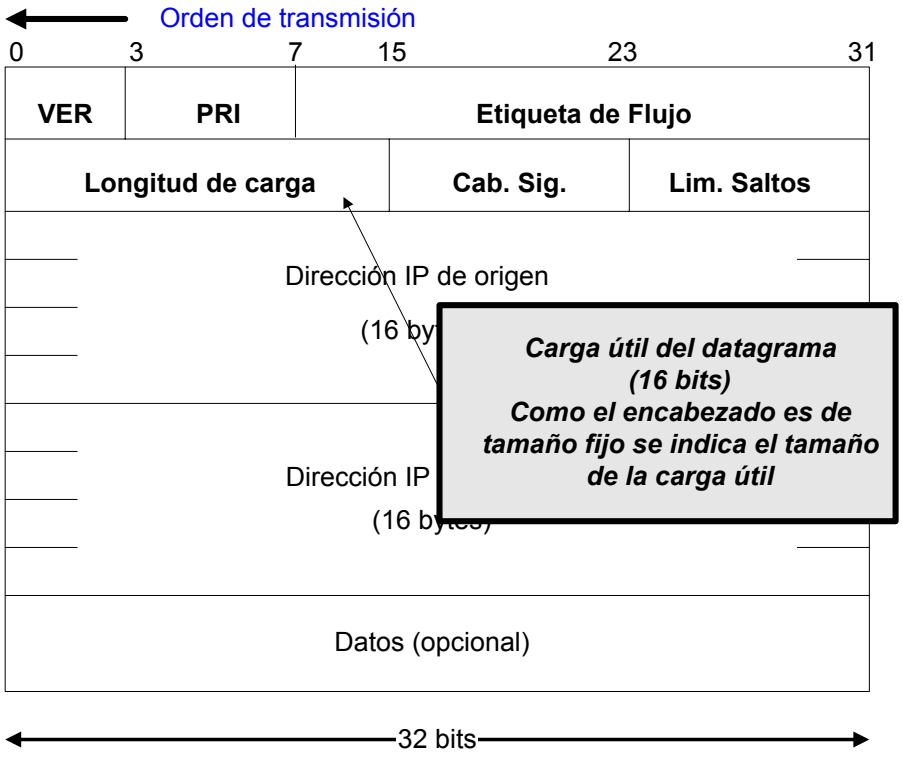



**Figura. 2.3.6.1.5.4. Datagrama IP-V6 "Longitud de carga"**

### 2.3.6.1.5.5. CABECERA SIGUIENTE

Este campo ocupa 4 bits, e identifica el tipo de cabecera que sigue a la cabecera IP-V6. Es coherente con los valores del campo protocolo en IP-V4. Ver figura 2.3.6.1.5.5..

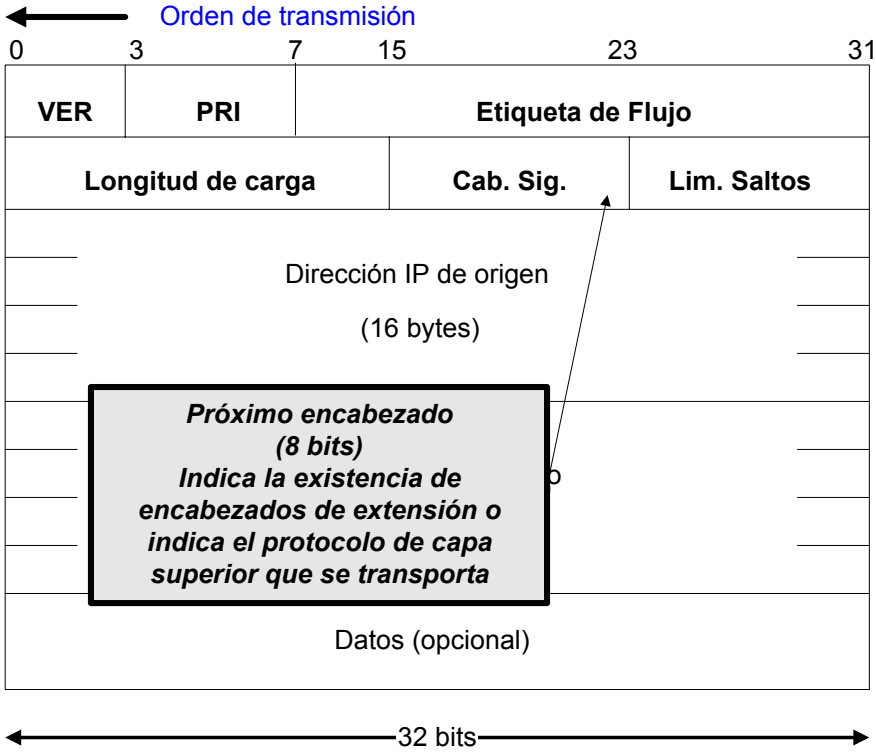



**Figura. 2.3.6.1.5.5. Datagrama IP-V6 "Cabecera Siguiente"**

### 2.3.6.1.5.6. LÍMITE DE SALTOS

Este campo ocupa un octeto. Es decrementado en una unidad por cada nodo que redirige el paquete hacia su destino. El paquete es descartado si el valor del campo llega a cero. Este campo sustituye al campo tiempo de vida, de IP-V4. Ver figura 2.3.6.1.5.6..

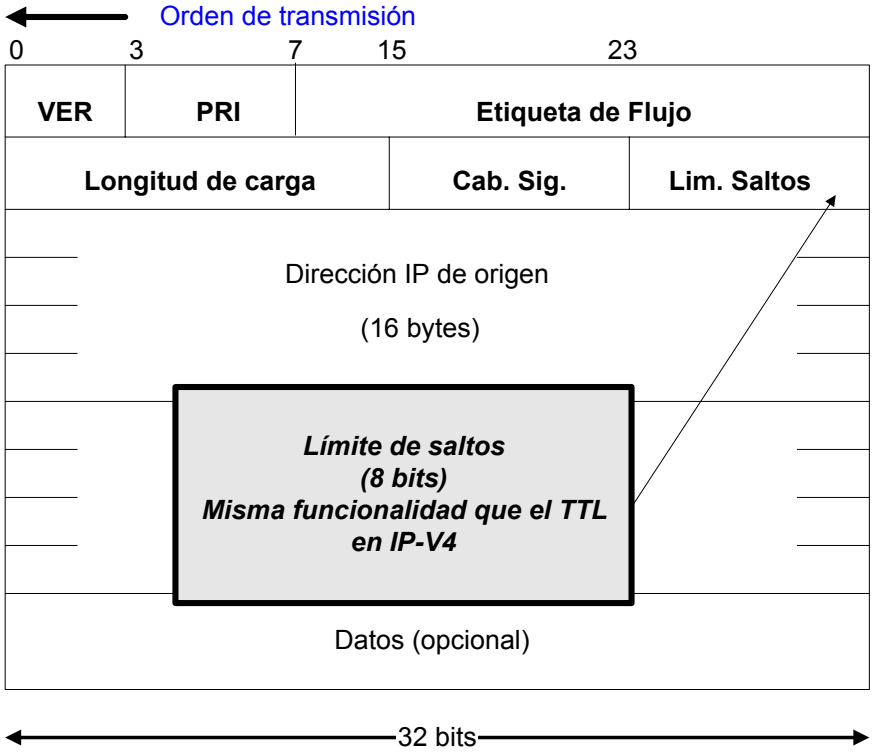



**Figura. 2.3.6.1.5.6. Datagrama IP-V6 "Limite de saltos"**

### 2.3.6.1.5.7. DIRECCIÓN DE ORIGEN

Este campo ocupa 128 bits, y corresponde a la dirección de origen. Ver figura 2.3.6.1.5.7..

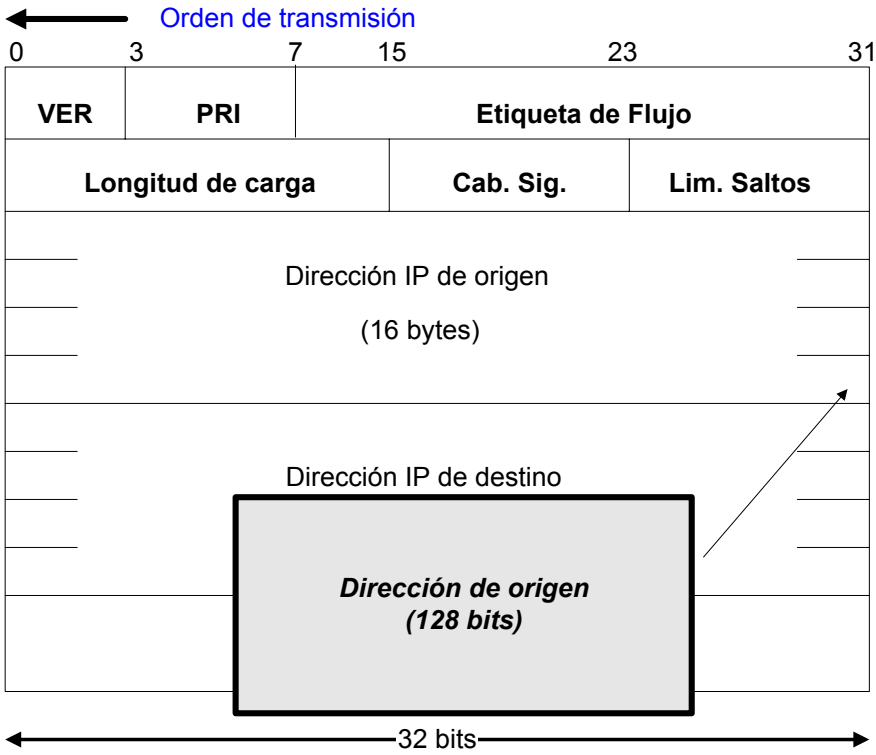



**Figura. 2.3.6.1.5.7. Datagrama IP-V6 "Dirección de origen"**

### 2.3.6.1.5.8. DIRECCIÓN DE DESTINO

Este campo ocupa 128 bits, y corresponde a la dirección de destino. Ver figura 2.3.6.1.5.8. (a) y (b).

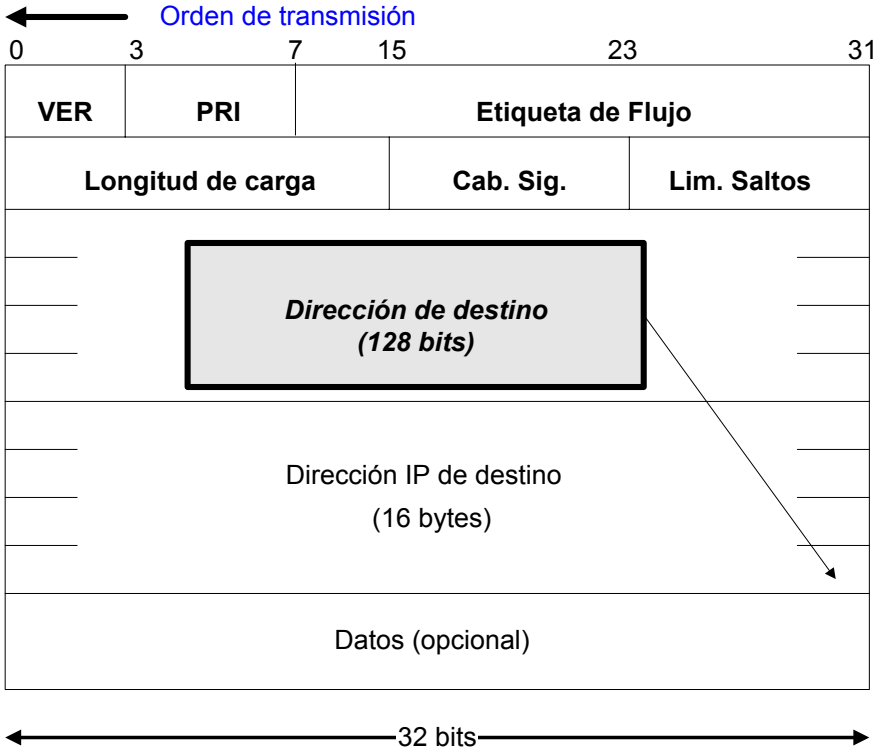



**Figura. 2.3.6.1.5.8. (a). Datagrama IP-V6 "Dirección de destino"**

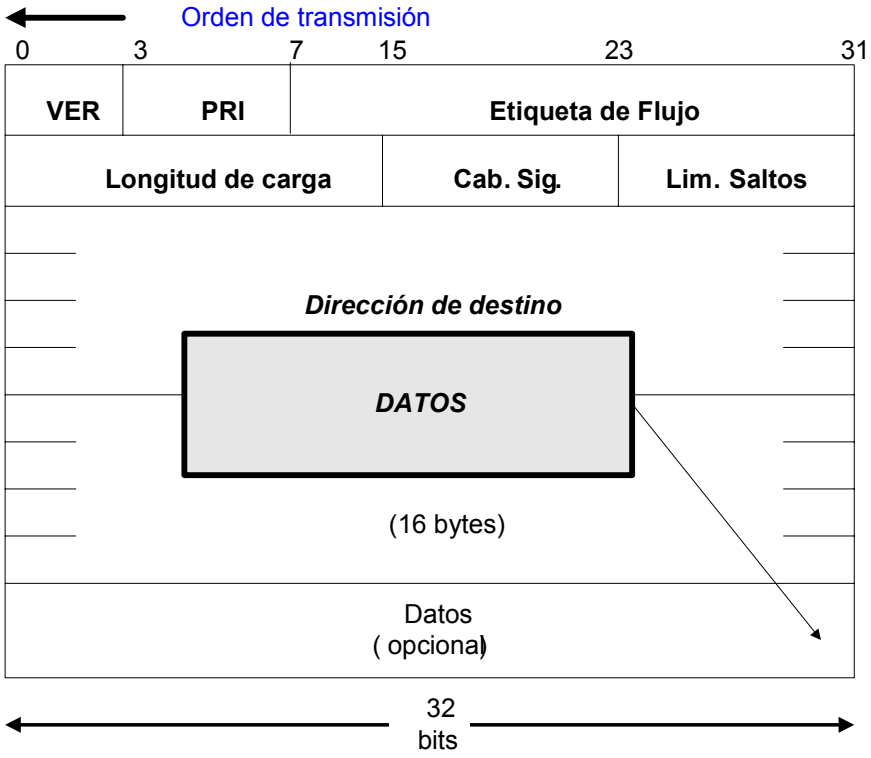



**Figura. 2.3.6.1.5.8. (b). Datagrama IP-V6 "Datos"**

## 2.4. PROTOCOLOS DE ENCAMINAMIENTO

IP-V6 para su encaminamiento se basa en los mismos protocolos de encaminamiento empleados por IP-V4 con ciertas modificaciones. Dentro de los protocolos de encaminamiento principales que emplea IP-V4 son TCP (Transfer Control Protocol) y UDP (User Datagram Protocol).

Normalmente, los paquetes IP transportan TPDUs (Transport Protocol Data Unit) o segmentos TCP o UDP, que son los dos protocolos de transporte utilizados en TCP/IP. Sin embargo, existen otros posibles contenidos para un paquete IP, en el que los datos que pueden transportarse son mensajes de los distintos protocolos de control de IP.

El protocolo actual de encaminamiento para IP-V4 es el TCP/IP mediante un servicio no orientado a conexión. IP-V6 tiene como futuro protocolo de encaminamiento TCP/IP así mismo mediante un servicio no orientado a conexión (no hay control de errores ni de flujo).

La adaptación del protocolo IP-V4 a IP-V6 es:

1. Incrementar el espacio de direcciones IP a 16 octetos
2. Agilizar el encaminamiento
3. La transmisión de audio y video en tiempo real
4. Transmisiones seguras

IP-V4 utiliza protocolos de encaminamiento interno y externo. Dentro de los protocolos de encaminamiento interno se tiene RIP, OSPF, IS-IS y como protocolos de encaminamiento externo el protocolo BGP. Otro protocolo de encaminamiento para IP-V4 es el ICMP el mismo que para IP-V6 es el protocolo ICMPV6.

IP-V6 para su encaminamiento emplea protocolos como RIPng o RIPV6, OSPFV6, BGP4+, BGP5.

## 2.4.1. PROTOCOLOS DE ENCAMINAMIENTO INTERNO

### 2.4.1.1. ROUTING INFORMATION PROTOCOL "RIP"

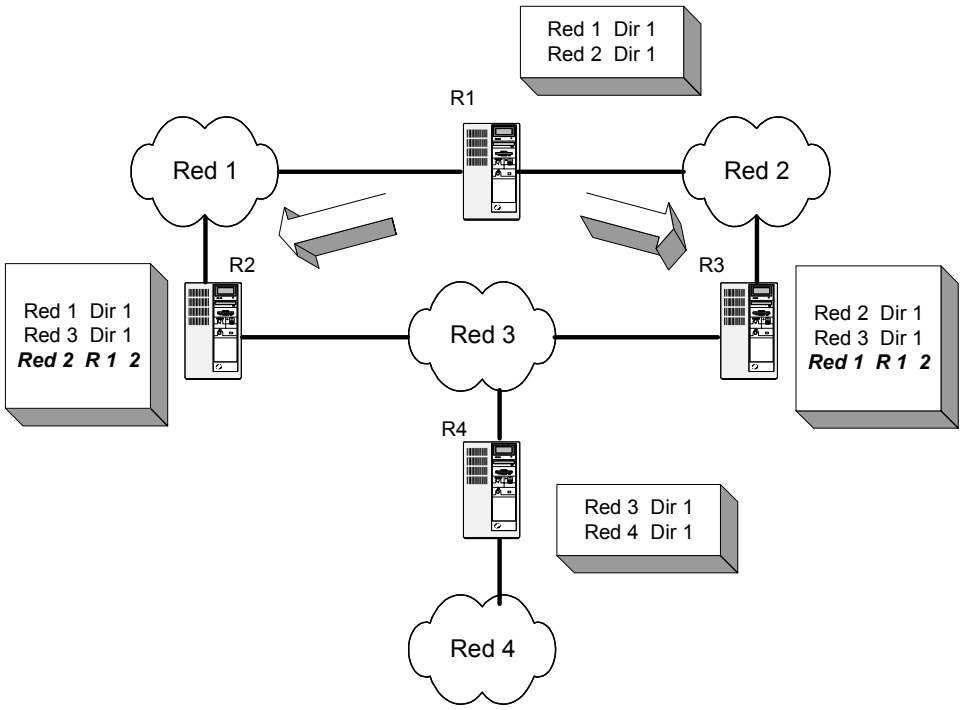



**Figura. 2.4.1.1. Protocol RIP**

Uno de los protocolos de routing más antiguos es el Routing Informacition Protocol o más comúnmente llamado RIP como se indica en la figura 2.4.1.1.. RIP utiliza algoritmos de vector distancia para calcular sus rutas. Este tipo de algoritmos para calcular rutas fueron utilizados durante décadas en sus distintas variantes. De hecho los algoritmos de vector distancia utilizados por RIP están basados en aquellos algoritmos utilizados por ARPANET en el año 1969.

RIP es un protocolo de routing de vector distancia muy extendido en todo el Mundo por su simplicidad en comparación a otros protocolos como podrían ser OSPF, IS-IS o BGP. RIP se trata de un protocolo abierto a diferencia de otros protocolos de routing

como por ejemplo IGRP y EIGRP propietarios de Cisco Systems o VNN propietario de Lucent Technologies.

RIP está basado en el algoritmo de Bellman Ford y busca su camino óptimo mediante el conteo de saltos, considerando que cada router atravesado para llegar a su destino es un salto.

RIP, al contar únicamente saltos, como cualquier protocolo de vector distancia no tiene en cuenta datos tales como por ejemplo ancho de banda o congestión del enlace.

RIP emplea los siguientes campos:

- ✓ Dirección de destino
- ✓ Siguiente salto
- ✓ Interfaz de salida del router
- ✓ Métrica
- ✓ Temporizador

Para obtener esta tabla, el protocolo de routing RIP utiliza el siguiente procedimiento para mantener actualizada la tabla de routing de cada uno de los nodos o routers de la red:

- ✓ Mantener una tabla con una entrada por cada posible destino en la red. La entrada debe contener la distancia D al destino, y el siguiente salto S del router a esa red. Conceptualmente también debería de existir una entrada para el router mismo con métrica 0, pero esta entrada no existirá.
- ✓ Periódicamente se enviará una actualización de la tabla a cada uno de los vecinos del router mediante la dirección de broadcast. Esta actualización contendrá toda la tabla de routing.

- ✓ Cuando llegue una actualización desde un vecino S, se añadirá el coste asociado a la red de S, y el resultado será la distancia D'. Se comparará la distancia D' y si es menor que el valor actual de D a esa red entonces se sustituirá D por D'.

#### 2.4.1.1.1. DIRECCIÓN DE DESTINO

La dirección de destino en la tabla de routing de RIP será la red de destino, es decir, la red final a la que se desea acceder, esta red en la versión 1 del protocolo RIP tendrá que ser obligatoriamente clasfull, es decir tendrá que tener en cuenta la clase, es decir, no se permite el subneting en RIP versión 1. Por ejemplo si la red de destino es la 192.168.4.0, sabemos que al ser RIP classfull la red de destino tiene 256 direcciones, de las cuales 254 son útiles, una vez descontada la dirección de red y la dirección de broadcast, ya que la red 192.168.4.0 es de clase C, es decir que los 24 primeros bits de la dirección IP identifican la red y los 8 últimos identifican los hosts de dentro de la red.

#### 2.4.1.1.2. SIGUIENTE SALTO

El siguiente salto se define como el siguiente router por el que el paquete va a pasar para llegar a su destino, este siguiente salto será necesariamente un router vecino del router origen.

#### 2.4.1.1.3. INTERFAZ DE SALIDA DEL ROUTER

La interfaz de salida del router es al interfaz al cual está conectado su siguiente salto.

#### 2.4.1.1.4. MÉTRICA

La métrica utilizada por RIP consiste en el conteo de saltos, como métrica se considera cada salto como una única unidad, independientemente de otros factores como tipo de interfaz o congestión de la línea. La métrica total consiste en el total de saltos desde el router origen hasta el router destino, con la limitación que 16 saltos se considera destino inaccesible, esto limita el tamaño máximo de la red.

#### 2.4.1.1.5. TEMPORIZADOR

El temporizador indica el tiempo transcurrido desde que se ha recibido la última actualización de esa ruta. RIP utiliza dos tiempos importantes, el tiempo de actualización que se estable en 30 segundos, el tiempo de desactivación que se establece en 180 segundos y el tiempo de borrado se establece en 300 segundos.

El tiempo de actualización se considera al tiempo máximo a transcurrir entre el envío de los mensajes de actualización de los vecinos.

El tiempo de desactivación se considera al tiempo máximo que puede esperar un router sin recibir actualizaciones de vecino, una vez pasado este tiempo, el vecino que no ha enviado la actualización se considera que ha caído y con lo cual el router no está activo en la red, se establece la métrica a valor 16, es decir destino inalcanzable.

El tiempo de borrado implica que una vez transcurrido ese tiempo todas las rutas de ese router supuestamente caído son eliminadas de la tabla de routing.

### 2.4.1.2. ROUTING INFORMATION PROTOCOL V6 "RIPV6"

El continuo desarrollo de Internet requiere que toda la arquitectura envuelva un acomodo de las nuevas tecnologías que soporta un incremento en el número de usuarios, aplicaciones y servicios. El protocolo Internet version 6 (IP-V6) esta diseñado para habilitar la expansión de Internet. Al hablar de IP-V6, se encuentran involucrados aspectos importantes inherentes a este concepto. Y uno de los mas importantes a nivel de direccionamiento de Routers es el Protocolo de Información de Ruteo (RIP). El cual varía con esta nueva versión de IP. Es importante destacar el uso de protocolos y algoritmos que están siendo utilizados actualmente en IP-V4, esto demuestra la compatibilidad existente entre ambas versiones.

Ripngd soporta el protocolo RIPng, el cual esta descrito en la RFC2080. Este protocolo es la adaptación del protocolo RIP a IP-V6.

RIPng (RFC2080 y RFC2081) es la especificación del Protocolo de Información de Rutas (RIP) para IP-V6 recoge los cambios mínimos e indispensables al RFC1058 y RFC1723 para su adecuado funcionamiento.

RIPng es un protocolo pensado para pequeñas redes, y, por tanto, se incluye en el grupo de protocolos de pasarela interior IGP (Interior Gateway Protocol), y emplea un algoritmo denominado "Vector - Distancia". Se basa en el intercambio de información entre routers, de forma que puedan calcular las rutas más adecuadas, de forma automática. RIPng sólo puede ser implementado en routers, donde requerirá, como información fundamental, la métrica o número de saltos (entre 1 y 15) que un paquete ha de emplear, para llegar a determinado destino. Cada salto supone un cambio de red, por lo general atravesando un nuevo router.

Además de la métrica, cada red tendrá un prefijo de dirección destino y la longitud del propio prefijo.

Además se podrán crear rutas internas (saltos entre interfaces del propio router), o rutas estáticas (definidas manualmente). RIPng es un protocolo basado en UDP. Cada router tiene un proceso que envía y recibe datagramas en el puerto 521 (puerto RIPng).

El inconveniente de RIPng, al igual que en IP-V4, siguen siendo, además de su orientación a pequeñas redes (diámetro de 15 saltos como máximo), en que su métrica es fija, es decir, no puede variar en función de circunstancias de tiempo real (retardos, fiabilidad, carga, etc.).

RIP es extendido para permitir a los routers intercambiar información para redes de computadoras a través de una red basada en IP-V6. RIPng es un protocolo de vector de distancia. RIPng debe ser implementado solo en Routers: IP-V6 provee otros mecanismos para descubrimiento de rutas. En cualquier router que usa RIPng se asume que tiene interfaz para una o más redes, de otra forma esto no es realmente un router. Esto esta referido a sus redes conectadas directamente.

El protocolo cuenta sobre el acceso de cierta información acerca de cada una de esas redes, de lo cual lo más importante es su métrica. La métrica RIP de una red es un entero entre 1 y 15, inclusive. Esto es establecido en alguna forma no especificada en este protocolo; sin embargo, dado el máximo número de saltos es de 15, usualmente es usado un valor de 1. Las implementaciones deben permitir al administrador del sistema establecer la métrica de cada red. En adición a la métrica, cada red tendrá un prefijo de dirección destino y la longitud del prefijo asociado a este. Estos son establecidos por el administrador del sistema de una manera no especificada en este protocolo.

Cada router que implementa RIP es asumido que tiene una tabla de ruteo. Esta tabla tiene una entrada para cada destino que es asequible desde todas partes por el Sistema Operativo RIP. Cada entrada contiene al menos la siguiente información:

- ✓ El prefijo IP-V6 del destino.
- ✓ Una métrica, la cual representa el costo total de obtener un datagrama desde el router a este destino. Esta métrica es la suma de los costos asociados con las redes que serian recorridas para obtener el destino.
- ✓ La dirección IP-V6 del próximo router pertenece al camino del destino. Si el destino esta sobre una de las redes directamente conectadas, este punto no es necesario.
- ✓ Una bandera para indicar que la información acerca de la ruta, ha cambiado recientemente.
- ✓ Varios timers asociados con la ruta.

Las entradas para las redes directamente conectadas son establecidas por el router usando información recolectada que en ningún caso es especificada en este protocolo. La métrica para una red directamente conectada es establecer el costo de esta red.

ANDINANET S.A. puede también permitir al Administrador del Sistema introducir rutas adicionales. Esto seria mas parecido a rutear hosts o redes fuera del alcance del Sistema de ruteo. Esto es referido como “Rutas Estáticas”. Las entradas para otros destinos que son inicialmente son sumadas y actualizadas por ciertos algoritmos.

La distinción entre red, subred y rutas de host no necesitan ser hechas para RIPng porque un prefijo de dirección IP-V6 es ambigua.

Cualquier prefijo con una longitud de prefijo de cero es usado para diseñar una ruta por defecto. Es sugerible que el prefijo 0:0:0:0:0:0:0:0 sea usado cuando se especifica la ruta por defecto, pero sin embargo el prefijo es esencialmente ignorado.

Una ruta por defecto es usada cuando no es conveniente listar todas las posibles redes en la actualización RIPng, y cuando uno o más routers en el sistema están preparados para manejar trafico en las redes que no están explícitamente listadas.

Estos "Routers por Defecto" usan la ruta por defecto como un camino para todos los datagramas para los cuales ellos no tienen ruta explícita. La decisión de cómo un Router llega a ser un Router por Defecto es dejada al implementador. En general, el sistema administrador estará provisto con una forma de especificar cual routers debe crear y anunciar las entradas de las rutas por defecto. Si este mecanismo es usado, la implementaron debe permitir al sistema administrador seleccionar la métrica asociada con el anuncio de las rutas por defecto. Esto hará posible establecer una precedencia entre múltiples routers por defecto.

Las entradas de rutas por defecto son manejadas por RIPng en exactamente la misma manera de cómo fuese para otro prefijo destino. Los administradores del sistema deben tener cuidado de asegurarse que las rutas por defecto no propagaran mas allá de lo entendido. generalmente, cada administrador de sistema tiene su propio router por defecto ya seleccionado.

### 2.4.1.3. OPEN SHORTEST PATH FIRSHT "OSPF"

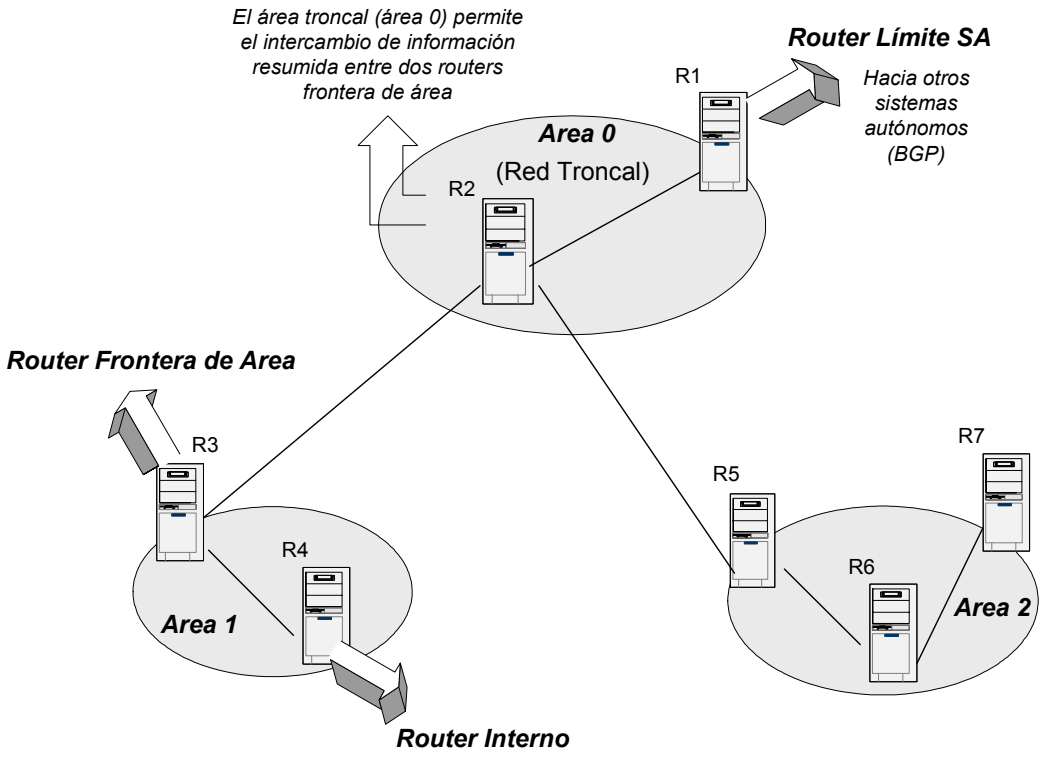



**Figura. 2.4.1.3. Protocolo OSPF**

OSPF es un protocolo de encaminamiento para redes IP que se basa en las especificaciones de RFC. En la década de los 90 OSPF fue recomendado como un protocolo de encaminamiento estándar. Ver figura 2.4.1.3..

El protocolo OSPF propone el uso de rutas más cortas y accesibles mediante la construcción de un mapa de la red y mantenimiento de bases de datos con información sobre sistemas locales y vecinos, de esta manera es capaz de calcular la métrica para cada ruta, entonces se eligen las rutas de encaminamiento más cortas. En este proceso se calculan tanto las métricas de estado del enlace como de distancia, en el caso de RIP se calcula sólo la distancia y no el trafico del enlace, por esta causa OSPF es un protocolo de encaminamiento diseñado para redes con crecimiento constante y capaz de manejar una tabla de encaminamiento

distribuida y de rápida propagación, entre las características más resaltantes de OSPF están:

- ✓ Rápida detección de cambios en la topología y restablecimiento muy rápido de rutas sin bucles.
- ✓ Poca sobrecarga, usa actualizaciones que informan de los cambios de rutas.
- ✓ División de tráfico por varias rutas equivalentes.
- ✓ Encaminamiento según el tipo de servicio.
- ✓ Uso de multienvio en las redes de área local.
- ✓ Mascaras de subred y superred.
- ✓ Autentificación.

El encaminamiento dentro de un área se basa en un mapa completo de estado de enlace del área. OSPF se diseñó para que admitiera el crecimiento de la red porque un encaminador necesita conocer la topología detallada e información de métricas sólo de un área a la que pertenece.

Un encaminador usa su base de datos para construir un árbol de caminos más cortos poniéndose a sí mismo en la raíz. Este árbol se usa para construir la tabla de encaminamiento. Si se dispone de encaminamiento por tipo de servicio en el área, se construye un árbol separado y un conjunto de rutas para cada tipo de servicio.

Todos los encaminadores de OSPF tiene una base de datos detallada con la información necesaria para construir un árbol de encaminamiento del área, con la descripción de:

- ✓ Todas las interfaces, conexiones y métricas de los encaminadores.
- ✓ Todas las redes de multiacceso y una lista de todos los encaminadores de la red.

¿Cómo consigue un encaminador esta información?. Pues empieza descubriendo quienes son sus vecinos mediante un mensaje de saludo (*Hello*).

En los mensajes de saludo todos los encaminadores están configurados con un identificador único que se usa en los mensajes. Habitualmente, la parte menor de la dirección de IP de encaminador se usa como identificador único.

Los encaminadores multienvían periódicamente mensajes de saludo (*Hello*) en una red multienvio, como puede ser EtherNet, Token Ring, o interfaz de datos distribuidos por fibra ( *FDDI* ), para que el resto de los encaminadores sepan que siguen activos. También envían mensajes de saludo al otro extremo de un enlace punto a punto o un circuito virtual para que estos vecinos sepan que siguen atentos.

Una de las rezones por la que funcionan los mensajes de saludo es que un mensaje contiene la lista de todos los identificadores de los saludos cuyos vecinos escucharan el emisor, así los encaminadores conocen si se les está escuchando en la red.

Existen diferentes tipos de mensajes OSPF, de los cuales los cinco tipos de mensajes del protocolo OSPF que se han descrito son:

- ✓ **Saludo.-** Se usa para identificar a los vecinos, es decir, encaminadores adyacentes en un área para elegir un encaminador designado para una red multienvio, para encontrar un encaminador designado existente y para enviar señales de "*Estoy aquí*".
- ✓ **Descripción de la base de datos.-** Durante la inicialización, se usa para intercambiar información de manera que un encaminador puede descubrir los datos que le faltan en la base de datos.

- ✓ **Petición del estado del enlace.-** Se usa para pedir datos que un encaminador se ha dado cuenta que le faltan en su base de datos o que están obsoletos.
- ✓ **Actualización del estado del enlace.-** Se usa como respuesta a los mensajes de Petición del estado del enlace y también para informar dinámicamente de los cambios en la topología de la red.
- ✓ **ACK de estado del enlace.-** Se usa para confirmar la recepción de una Actualización del estado del enlace. El emisor retransmitirá hasta que se confirme.

#### 2.4.1.4. OPEN SHORTEST PATH FIRSHT V6"OSPFV6"

OSPFV6 con RFC2740. El protocolo de rouitng "Abrir Primero el Camino más Corto" OSPF (Open Shortest Path First), es también un protocolo IGP (para redes autónomas) basado en una tecnología de "estado de enlaces" ("link-state").

Se trata de un protocolo de routing dinámico que detecta rápidamente cambios de la topología (como un fallo en un router o interfaz) y calcula la siguiente ruta disponible (sin bucles), después de un corto período de convergencia con muy poco tráfico de routing.

Cada router mantiene una base de datos que describe la topología del sistema autónomo (de la red), y es lo que denominamos base de datos de "estado de enlaces". Todos los routers del sistema tienen una base de datos idéntica, indicando el estado de cada interfaz y de cada "vecino alcanzable".

Los routers distribuyen sus "estados locales" a través del sistema autónomo (la red) por medio de desbordamientos ("flooding").

Todos los routers utilizan el mismo algoritmo en paralelo y construyen un árbol de las rutas más cortas, como si fueran la raíz del sistema. Este árbol de "rutas más cortas" proporciona la ruta a cada destino del sistema autónomo.

Si hubiera varias rutas de igual coste a un determinado destino, el tráfico es distribuido equilibradamente entre todas. El coste de una ruta se describe por una métrica simple, sin dimensión.

Se pueden crear áreas o agrupaciones de redes, cuya topología no es retransmitida al resto del sistema, evitando tráfico de routing innecesario.

OSPF permite el uso de máscaras diferentes para la misma red ("variable length subnetting"), lo que permite el encaminado a las mejores rutas (las más largas o más específicas).

Todos los intercambios de protocolo OSPF son autenticados, y, por tanto, sólo pueden participar los routers verificados ("trusted").

OSPFV6 mantiene los mecanismos fundamentales de la versión para IP-V4, pero se han tenido que modificar ciertos parámetros de la semántica del protocolo, así como el incremento del tamaño de la dirección. OSPFV6 se ejecuta basado en cada enlace, en lugar de en cada subred.

Además, ha sido necesario eliminar la autenticación del protocolo OSPFV6, dado que IP-V6 incorpora estas características (AH y ESP).

A pesar de la mayor longitud de las direcciones, se ha logrado que los paquetes OSPFV6 sean tan compactos como los

correspondientes para IP-V4, eliminando incluso algunas limitaciones y flexibilizando la manipulación de opciones.

#### 2.4.1.5. INTERMEDIATE SYSTEM "IS-IS"

Este protocolo permite el intercambio de información de routing entre sistemas intermedios (intradomain). Corresponde a la norma ISO-10747. Está basado en un desarrollo original de DECnet. Desde el punto de vista de las funciones es similar a OSPF (pero no son compatibles); ambos son del tipo estado de enlace (*Link State*).

IS-IS permite funciones no soportadas en RIP, como: jerarquías de routing, separación de trayectos, tipo de servicio ToS, soporta la autentificación, soporta una máscara de subred de longitud variable. El protocolo que permite el routing interdomain es el **IDRP** (*Interdomain Routing Protocol*) que es similar al BGP. Los IS-IS y IDRP trabajan sobre el protocolo de red CLNP.

Utiliza una métrica con valor máximo de 1024; es arbitraria y es asignada por el administrador de red. Un enlace simple puede tener un valor máximo de 64. La longitud del enlace es calculada por la suma de las ponderaciones individuales. Otras métricas adicionales son: retardo del enlace, costos de expensas asociado al enlace y errores en el enlace. Un mapa de estos 4 tipos de métrica permite formar la QoS en el encabezado del paquete **CLNP** (protocolo de capa 3 en el modelo ISO) y computar la tabla de rutas de la internetwork.

Existen 3 tipos básicos de paquetes en IS-IS: el *Hello* para el IS-IS; el paquete de *Link State* y el paquete de número secuencial. El formato de los paquetes es complejo y contiene en esencia 3 diferentes partes lógicas. El formato común se enumera a continuación:

- ✓ **OH.-** 8 Bytes de *OverHead.* Encabezado común contiene un byte para cada uno de los siguientes mensajes.
- ✓ **IDE.-** Identificador del protocolo IS-IS (corresponde a 1 Byte con valor 131).
- ✓ **LEN.-** Longitud del encabezado (corresponde a los 8 Bytes de longitud).
- ✓ **PRO.-** Versión del protocolo.
- ✓ **ID.-** Identifica la longitud de la porción de dominio ID en la dirección NSAP.
- ✓ **PAC.-** Tipo de paquete: hello, link state o numeración secuencial.
- ✓ **VRS.-** Versión del protocolo (repetición).
- ✓ **RSV.-** 1 Byte Reservado (todos ceros).
- ✓ **AR.-** Dirección de área máxima: número máximo de direcciones en el área.

## 2.4.2. PROTOCOLOS DE ENCAMINAMIENTO EXTERNO

### 2.4.2.1. BORDER GATEWAY PROTOCOL "BGP"

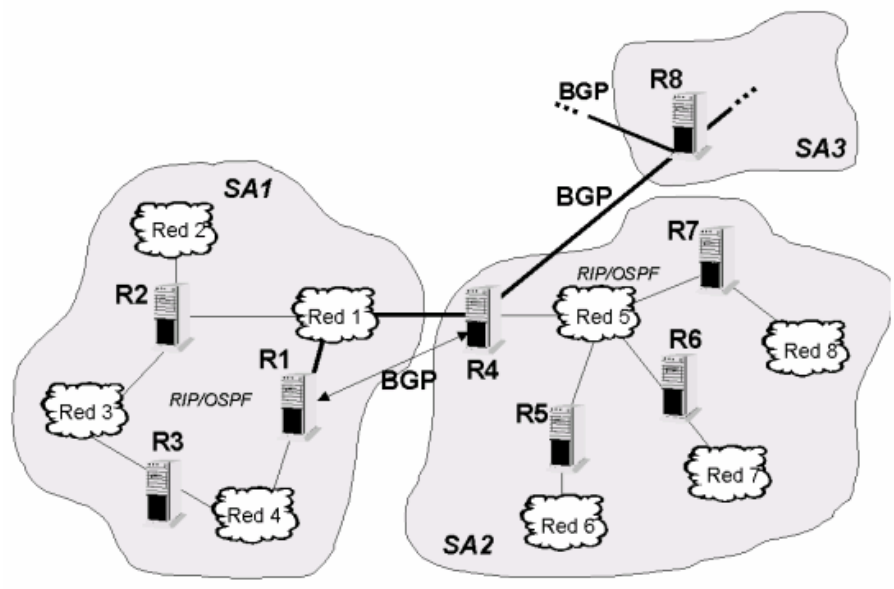



**Figura. 2.4.2.1. Protocolo BGP**

El protocolo de pasarela frontera BGP (Border Gateway Protocol) se encarga de mover paquetes de una red a otra pero en algunos casos debe preocuparse de otras cuestiones que no tienen porque estar relacionadas con el objetivo de mover los paquetes de la forma mas eficiente posible. Es posible que se deban considerar algunas restricciones relacionadas con cuestiones comerciales o políticas. Ver figura 2.4.2.1..

Los diferentes dispositivos de encaminamiento BGP se comunican entre sí estableciendo conexiones TCP. El protocolo BGP es fundamentalmente un protocolo de vector distancia en el que cada dispositivo de encaminamiento mantiene el coste a cada destino y la trayectoria seguida. Estos valores son dados periódicamente a cada uno de los vecinos enviando mensajes. La esencia de BGP es el intercambio de información de encaminamiento entre dispositivos de encaminamiento. La información de encaminamiento actualizada se va propagando a través de un conjunto de redes.

BGP involucra tres procedimientos funcionales, que son:

#### 2.4.2.1.1. ADQUISICIÓN DE VECINO

Dos dispositivos de encaminamiento son vecinos si están conectados a la misma subred y se han puesto de acuerdo en que ambos quieren intercambiar regularmente información de encaminamiento. Para llevar a cabo la adquisición de vecino, un dispositivo de encaminamiento envía a otro un mensaje OPEN. Si el dispositivo destino acepta la solicitud, devuelve un mensaje KEEPALIVE (la vecindad se mantiene viva) como respuesta.

#### 2.4.2.1.2. DETECCIÓN DE VECINO ALCANZABLE

Una vez establecida la relación de vecino, para mantener la relación se realiza la detección de vecino alcanzable enviándose periódicamente mensajes KEEPALIVE.

#### 2.4.2.1.3. DETECCIÓN DE RED ALCANZABLE

Para la detección de red alcanzable es necesario que cada dispositivo de encaminamiento tenga una base de datos con todas las redes que puede alcanzar y la mejor ruta para alcanzarla. Cuando se realiza un cambio en la base de datos es necesario enviar un mensaje UPDATE por difusión a todos los dispositivos de encaminamiento que implementan BGP para que puedan acumular y mantener la información necesaria.

Todos los mensajes BGP tienen una cabecera de 19 bytes que consta de tres campos:

- ✓ **Marcador**.- sirve de autentificación, es decir, para que el receptor pueda verificar la identidad del emisor.
- ✓ **Longitud**.- indica el tamaño del mensaje en bytes.
- ✓ **Tipo**.- Open, Update, Notification y Keepalive.

Además de la cabecera alguno de estos mensajes pueden tener unos campos adicionales:

- ✓ El mensaje **Open** incluye la dirección IP del dispositivo de encaminamiento que envía el

mensaje, un identificador de la red a la que pertenece y un temporizador como propuesta del tiempo que puede pasar sin recibir un Keepalive o un Update. Para indicar que acepta la solicitud envía un Keepalive pudiendo poner en el temporizador un valor menor.

- ✓ El mensaje **Keepalive** consta solamente de la cabecera.
- ✓ El mensaje **Update** facilita dos tipos de información que incluso pueden enviarse en el mismo mensaje: la de una ruta particular a través del conjunto de redes y una lista de rutas previamente anunciadas por este dispositivo para que sean anuladas.
- ✓ El mensaje **Notification** se envía cuando se detecta una condición de error: error en la cabecera del mensaje, error en el mensaje Open, error en el mensaje Update, tiempo de mantenimiento expirado, error en la máquina de estados finitos y cese para cerrar una conexión con otro dispositivo en ausencia de cualquier error.

#### 2.4.2.2. BORDER GATEWAY PROTOCOL 4+ "BGP4+"

El Protocolo de Pasarelas de Frontera BGP (Border Gateway Protocol) es un protocolo de encaminado para la interconexión de sistemas autónomos, es decir, para el routing entre diferentes dominios. Frecuentemente se emplea para grandes corporaciones y para la conexión entres proveedores de servicios (como ISP ANDINANET S.A.).

Su principal función es, por tanto, el intercambio de información de disponibilidad o alcance entre varios sistemas BGP,

incluyendo información de los sistemas autónomos que contienen, permitiendo así construir las rutas más adecuadas y evitar bucles de tráfico.

BGP4 incorpora mecanismos para soportar routing entre dominios sin clases ("classless interdomain routing"), es decir, el uso de prefijos, agregación de rutas y todos los mecanismos en los que se basa IP-V6.

BGP se basa en que un dispositivo sólo informa a los otros dispositivos que se conectan a él acerca de las rutas que el mismo emplea. Es decir, es una estrategia de "salto a salto". La implicación es la simplicidad de Internet, pero la desventaja es que este mecanismo impide políticas complejas, que precisan de técnicas como el routing de fuente ("source routing").

BGP usa TCP como protocolo de transporte a través del puerto 179. BGP4+ añade a BGP (RFC1771), extensiones multiprotocolo, tanto para IP-V6 como para otros protocolos, como por ejemplo IPX.

### 2.4.3. PROTOCOLO DE CONTROL DE MENSAJES INTERNET "ICMP"

El protocolo ICMP hace referencia a Internet Control Message Protocol. ICMP utiliza el soporte básico de IP como si se tratara de un protocolo de nivel superior.

ICMP es un protocolo que se utiliza entre computadoras, hosts y bridges por diversas razones:

- ✓ Cuando no se pueden enviar los mensajes.
- ✓ Para que los bridges encaminen el tráfico por rutas más cortas.
- ✓ Cuando un bridge no dispone de suficiente capacidad de almacenamiento para detener y enviar unidades de datos.

- ✓ Para descartar los datagramas por expiración del TTL o imposibilidad de reensamblar los datagramas.

Este protocolo notifica a la computadora origen si el destino no se pudo alcanzar. Crea y gestiona un mensaje de tiempo en el caso de que expire el tiempo de vida del mensaje. También determina si la cabecera de IP es errónea.

El servicio de ping está implementado sobre ICMP.

ICMP es un protocolo robusto encargado de generar mensajes de error en caso de fallas durante el transporte de los datos por el cable. La notificación de errores no depende de un centro de gestión de red central. ICMP envía los mensajes de error a todos los host.

Existen situaciones en que se descartan los datagramas de IP. Por ejemplo; puede que no se llegue a un destino porque el enlace se ha caído. Puede que halla expirado el contador del tiempo de vida o que sea imposible que un encaminador envíe un datagrama muy grande porque no permite la fragmentación. En fin, todas éstas representan posibles causas de error para el protocolo ICMP.

ICMP notificará el error de manera inmediata a los sistemas en línea. Para realizar esta tarea, ICMP utiliza un estándar de mensajes de error conocidos como se indica en la tabla 2.4.3.

| MENSAJE | DESCRIPCIÓN |
|---|---|
| Destino inalcanzable (destino unrreachable) | Un datagrama no puede llegar a su host, utilidad o aplicación de destino. |
| Plazo superado (Time exceeded) | El tiempo de vida ha expirado en un encaminador o el plazo de reensamblado en un host de destino. |
| Problema de los Parámetros (Parameter Problen) | Existe un parámetro erróneo en la cabecera de IP |
| Acallado de origen (Source Quench) | Un encaminador o un destino están congestionado. Se recomienda que los sistemas no envíen mensajes de acallado. |
| Redirigir (redirect) | Un host ha enviado un datagrama al encaminador local equivocado. |

**Tabla. 2.4.3. Mensajes de error ICMP**

### 2.4.4 PROTOCOLO DE CONTROL DE MENSAJES INTERNET V6 "ICMPV6"

En plena "construcción" del protocolo IP-V6, aparece ICMP y dice "Yo no quiero ser menos", con lo que aparece también la versión 6 del protocolo ICMP. Dicha versión conserva muchas de las funciones de la versión que se ha descrito anteriormente, pero se destacan algunos cambios importantes. Entre las nuevas ventajas del protocolo ICMPV6 podemos encontrar las siguientes funciones, que no se encuentran en la versión 4 de este protocolo.

- ✓ Funciones que intentan substituir al protocolo ARP.
- ✓ Mas facilidades a la hora de descubrir el MTU de una ruta (si no sabe de que va lee un poco mas arriba).
- ✓ Deja de existir los ICMP_SOURCE_QUENCH.
- ✓ Funciones para el multienvío.
- ✓ Ayuda para la configuración automática de direcciones.
- ✓ Ayuda para detectar gateways fuera de servicio

ICMPV6 tiene el mismo formato de cabecera, 8 octetos (tipo (1), código (1), suma de comprobación (2) y parámetros (4)), así mismo el tamaño máximo de los mensajes incluyendo cabeceras de 576 octetos (generalmente 36 octetos en IP-V4). Mensajes de error: Destino inalcanzable, Paquete demasiado grande, Tiempo excedido, Problemas de parámetros

El Internet Control Messages Protocol (56 en el campo de Next Header), tiene el mismo uso que su antepasado, el ICMPV4. La misión de un ICMP, es sobre todo la de informar. Sobre que informa, como y de que forma, cada uno de estos pasos se describen a continuación.

Los ataques producidos por los ICMP enviados de forma masiva, generalmente para provocar un DOS (Denial of Service) y/o la caída de un nodo de una red y/o de una conexión, son lo suficientemente conocidos como para no tener que volver a explicarlos.

El protocolo IP-V6, implementa medios de autentificación que pueden evitar los mas comunes:

- ✓ Caída por recepción de envíos masivos de ICMP.
- ✓ Desconexión de un host, por el envió de un atacante al servidor, de ICMP con mensages de error.
- ✓ Falsificación de ICMP.

Todos estos problemas, están descritos en el RFC 2463, así como sus posibles soluciones mediante aplicaciones de métodos autentificadores a nivel de trasporte IP y/o mediante el chesum de control.

### 2.4.4.1. TIPOS DE ICMPV6 Y FORMATO

Los mensages de ICMP, se han dividido en 2 clases, los que comunican errores, y los que piden/dan información sobre un nodo. Para diferenciarlos, se han adjudicado una numeración del 0 al 127 a

los mensages que contienen información y del 128 al 255, sobre los que informan de algún tipo de error de una petición.

Un paquete ICMPV6, esta formado por una cabecera IP-V6, y es precedido inmediatamente por una cabecera con valor 58 en el campo next header como se puede ver en la figura 2.4.4.1.

| | |
|---|---|
| IP-V6 Header<br>Next Header = 58 | ICMP header + data |

**Figura. 2.4.4.1. Next Header "Formato ICMPV6"**

Este procedimiento es diferente al de IP-V4, y que un ICMP puede ser insertado en cualquier tipo de paquetes.

### 2.4.4.2. TIPOS DE ICMPV6 DE INFORMACIÓN

Los mensajes de información, pueden ser del tipo: Echo Request (Type 128). Un nodo, puede enviar un ICMP Echo Request (Mas conocidos como pings), para saber el tiempo de respuesta de otro host. El formato se indica en la figura 2.4.4.2 (a).:

| | | |
|---|---|---|
| Type | Code | Checksum |
| Identifier | | Sequence Number |
| Data..... | | |

**Figura. 2.4.4.2. (a). Información en ICMPV6**

- Type: 128
- Code: 0
- Checksum: Suma de control, para la comprobación de la información.

- Identifier: Identificador para contrastar los ICMP Echo Reply de respuesta.
- Sequence Number: Secuencia de numeros, para contrastar los ICMP Echo Reply de respuesta en orden.
- Data: Datos aleatorios o ceros de relleno.

La recepción de ICMP Echo Request, debe ser comunicada a la capa superior de trasporte. Echo Reply (Type 129). El ICMP Echo Reply, es enviado como respuesta a un ICMP Echo Request. El ICMP Echo Reply debe ser trasportado al proceso que origino el ICMP Echo Request. El formato se indica en la figura 2.4.4.3:

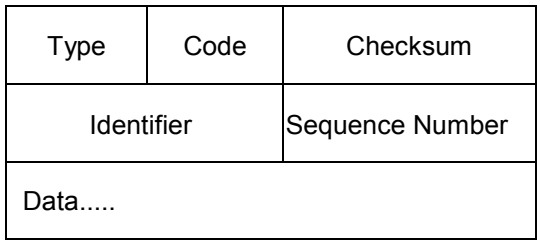



**Figura. 2.4.4.2. (b) Información en ICMPV6**

- Type: 129
- Code: 0
- Checksum: Suma de control, para la comprobación de la información.
- Identifier: Identificador que debe contrastar con los ICMP Echo request que se han recibido.
- Sequence Number: Secuencia de números, que debe contrastar con los ICMP Echo request que se han recibido en el mismo orden.
- Data: Datos aleatorios o ceros de relleno.

### 2.4.4.3. TIPOS DE ICMPV6 DE ERROR

Destination Unreachable (Type 1) Un ICMP Destination Unreachable es mandado por un router, o por cualquier nodo, para informar de la imposibilidad de que un paquete llegue a su destino. No se deberían mandar ICMPV6, si son ocasionados por problemas de congestión de la red.

Estos ICMP se dividen en subclases, según el tipo de problema que halla ocasionado su emisión:

- ✓ Si el error es ocasionado por un envió de un paquete al nodo erróneo, este enviara un ICMPV6 con código 0.
- ✓ Si el error es ocasionado por un envió hacia un destino cerrado por causas administrativas (Un firewall por ejemplo), se debe enviar un ICMP de código 1.
- ✓ Si el error es ocasionado por la imposibilidad de resolver la dirección IP de un link, se enviara un ICMPV6 con código 3.
- ✓ Si el error es ocasionado por un fallo en la capa de trasporte si el puerto esta indisponible para la misma se enviara un ICMP con código 4. Por ejemplo, un paquete TCP enviado a un puerto UDP.

Un nodo que ha recibido un ICMPV6 Destination Unreachable, debe comunicarlo a la capa superior del proceso.

El formato seria como se indica en la figura 2.4.4.3.(a):

| Type | Code | Checksum |
|---|---|---|
| Unused | | |
| La máxima cantidad posible de datos del paquete originario del error, sin exceder el tamaño del MTU. | | |

**Figura. 2.4.4.3. (a). Error ICMPV6**

- Type: 0
- Code: 0 no route to destination, 1 communication with destination administratively prohibited, 2 (not assigned), 3 address unreachable, 4 port unreachable.
- Unused: Campo sin uso, que debe ser inicializado a 0 por el emisor e ignorado por el destino.
- Checksum: Suma de control, para la comprobación de la información.

Packet Too Big (Type 2). Un ICMP Packet Too Big , es enviado cuando el tamaño máximo de un paquete es superior a la MTU del interfaz de red al que se ha enviado. También es enviado por un router, si el siguiente salto tiene un MTU inferior al tamaño del paquete. Este ICMP, puede ser usado para saber el MTU de un path.

El formato se indica en la figura 2.4.4.3 (b):

| Type | Code | Checksum |
|---|---|---|
| MTU | | |
| La máxima cantidad posible de datos del paquete originario del error, sin exceder el tamaño del MTU. | | |

**Figura. 2.4.4.3. (b). Error ICMPV6**

- Type: 2
- Code: 0 (Inicializado a 0 por el origen, ignorado por el destino)
- Checksum: Suma de control, para la comprobación de la información.
- MTU: MTU del siguiente salto.

Time Exceeded (Type 3). Si un router recibe un paquete con el Hop limit a 0 o si es el quien lo tiene que poner a 0, el paquete es descartado y se envía un ICMPV6 Time Exceeded. Si un host, no puede ensamblar un paquete en un tiempo *x*, descartara todos los fragmentos recibidos y también enviara un ICMP de esta clase. La llegada de un ICMPV6, debe ser notificada a la capa superior de trasporte.

El formato queda como se indica en la figura 2.4.4.3. (c):

| Type | Code | Checksum |
|---|---|---|
| | | Unused |
| La máxima cantidad posible de datos del paquete originario del error, sin exceder el tamaño del MTU. | | |

**Figura. 2.4.4.3. (c). Error ICMPV6**

- Type: 3
- Code: 0 - hop limit exceeded in transit (Rebasado el limite de saltos) 1 - fragment reassembly time exceeded (Rebasado el tiempo de ensamblado en destino).
- Unused: Campo inicializado a 0 en origen, e ignorado por destino.
- Checksum: Suma de control, para la comprobación de la información.

Parameter Problem (Type 4). Si un nodo IP-V6, al procesar un paquete, encuentra un error en uno de los parámetros de sus campos, enviara un ICMP Parameter Problem informando al destino de la situación del error en el paquete.

El formato se indica en la figura 2.4.4.3. (d)

| Type | Code | Checksum |
|---|---|---|
| | | Pointer |
| La máxima cantidad posible de datos del paquete originario del error, sin exceder el tamaño del MTU. | | |

**Figura. 2.4.4.3. (d). Error ICMPV6**

- Type: 4
- Code: 0 erroneous header field encountered (Error en la cabecera), 1 unrecognized Next Header type encountered (Numero de Next Header desconocido), 2 unrecognized IP-V6 option encountered (Opción desconocida en el paquete IP-V6).
- Checksum: Suma de control, para la comprobación de la información.
- Pointer: Contiene un offset, para la localización del parámetro que origino el error. El offset, es el byte donde se encuentra el dato erróneo dentro del paquete.

### 2.4.5. PROTOCOLO "TCP/IP"

Cuando se habla de TCP/IP , se relaciona automáticamente como el protocolo sobre el que funciona la red Internet . Esto , en cierta forma es cierto , ya que se le llama TCP/IP , a la familia de protocolos que nos permite estar conectados a la red Internet . Este nombre viene dado por los dos protocolos estrella de esta familia:

- ✓ El protocolo TCP, funciona en el nivel de transporte del modelo de referencia OSI, proporcionando un transporte fiable de datos.
- ✓ El protocolo IP, funciona en el nivel de red del modelo OSI, que permite encaminar los datos hacia otras maquinas.

Pero un protocolo de comunicaciones debe solucionar una serie de problemas relacionados con la comunicación entre ordenadores, además de los que proporciona los protocolos TCP e IP.

Para poder solucionar los problemas que van ligados a la comunicación de ordenadores dentro de la red Internet, se tienen que tener en cuenta una serie de particularidades sobre las que ha sido diseñada TCP/IP:

- ✓ Los programas de aplicación no tienen conocimiento del hardware que se utilizara para realizar la comunicación (módem, tarjeta de red...).
- ✓ La comunicación no esta orientada a la conexión de dos maquinas, eso quiere decir que cada paquete de información es independiente, y puede viajar por caminos diferentes entre dos maquinas.
- ✓ La interfaz de usuario debe ser independiente del sistema, así los programas no necesitan saber sobre que tipo de red trabajan.
- ✓ El uso de la red no impone ninguna topología en especial (distribución de los distintos ordenadores).

De esta forma, se puede decir, que dos redes están interconectadas, si hay una maquina común que pase información de una red a otra. Además, también podremos decir que una red Internet virtual realizara conexiones entre redes, que ha cambio de pertenecer a la gran red, colaboraran en el trafico de información procedente de una red cualquiera, que necesite de ella para acceder a una red remota. Todo esto independiente de las maquinas que implementen estas funciones, y de los sistemas operativos que estas utilicen.

La arquitectura TCP/IP esta hoy en día ampliamente difundida, a pesar de ser una arquitectura de facto, en lugar de ser uno de los estándares definidos por la ISO, IICC, etc... Esta arquitectura se empezó a desarrollar como base de la ARPANET (red de comunicaciones militar del gobierno de los EE.UU), y con la expansión de la INTERNET se ha convertido en una de las arquitecturas de redes más difundida.

Así como el modelo de referencia OSI posee siete niveles (o capas), la arquitectura TCP/IP viene definida por 4 niveles : el nivel de subred [enlace y físico], el nivel de interred [Red, IP], el protocolo proveedor de servicio [Transporte, TCP o UDP] , y el nivel de aplicación.

Para la configuración del protocolo TCP/IP es importante contar con la siguiente información:

- ✓ Dirección IP asignada por ANDINANET S.A.
- ✓ El Gateway asignado por ANDINANET S.A.
- ✓ Los DNS administrados por ANDINANET S.A. 63.84.236.33 y 63.84.233.34

Bajo el protocolo TCP/IP el usuario final, luego de contar con una instalación Banda Ancha instalada por ANDINANET S.A., establece la comunicación entre su PC, el Router y finalmente el ISP para la conexión a Internet.

TCP/IP es el protocolo común de comunicaciones utilizado en Internet (E-mail, FTP, WWW). El protocolo TCP envía la información fragmentada en paquetes "IP", permite el redireccionamiento por los “Routers”, verifica que los datos llegan al destino y reunifica los paquetes en perfecto orden en el destino. El IP da un tamaño determinado y etiqueta a cada paquete con un número “IP”.

### 2.4.6. PROTOCOLO UDP

Este protocolo es no orientado a la conexión, y por lo tanto no proporciona ningún tipo de control de errores ni de flujo, aunque si que utiliza mecanismos de detección de errores. Cuando se detecta un error en un datagrama en lugar de entregarlo a la aplicación se descarta.

Este protocolo se ha definido teniendo en cuenta que el protocolo del nivel inferior (el protocolo IP) también es no orientado a la conexión y puede ser interesante tener un protocolo de transporte que explote estas características.

Como el protocolo es no orientado a la conexión cada datagrama UDP existe independientemente del resto de datagramas UDP.

El protocolo UDP es muy sencillo y tiene utilidad para las aplicaciones que requieren pocos retardos o para ser utilizado en sistemas sencillos que no pueden implementar el protocolo TCP.

Las características del protocolo UDP son:

- ✓ No garantiza la fiabilidad. No podemos asegurar que cada datagrama UDP transmitido llegue a su destino. Es un protocolo del tipo best-effort porque hace lo que puede para transmitir los datagramas hacia la aplicación pero no puede garantizar que la aplicación los reciban.
- ✓ No preserva la secuencia de la información que proporciona la aplicación. La información se puede recibir desordenada (como ocurre en IP) y la aplicación debe estar preparada por si se pierden datagramas, llegan con retardo o llegan desordenados.

La figura 2.4.6 muestra los campos de un datagrama UDP y como se forma el datagrama IP.

| Puerto de origen | Puerto de destino |
|---|---|
| Longitud | Suma de comprobación |

**Figura. 2.4.6. Datagrama UDP**

Un datagrama consta de una cabecera y de un cuerpo en el que se encapsulan los datos. La cabecera consta de los siguientes campos:

- ✓ Los campos puerto origen y puerto destino son de 16 bits e identifican las aplicaciones en la máquina origen y en la máquina destino.
- ✓ El campo longitud es de 16 bits e indica en bytes la longitud del datagrama UDP incluyendo la cabecera UDP. En realidad es la longitud del datagrama IP menos el tamaño de la cabecera IP. Como la longitud máxima del datagrama IP es de 65.535 bytes y la cabecera estándar de IP es de 20 bytes, la longitud máxima de un datagrama UDP es de 65.515 bytes.
- ✓ El campo suma de comprobación (checksum) es un campo opcional de 16 bits que, a diferencia del campo equivalente de la cabecera IP que solo protegía la cabecera, protege tanto la cabecera como los datos.

Como el protocolo UDP no está orientado a la conexión y no envía ningún mensaje para confirmar que se han recibido los datagramas, su utilización es adecuada cuando se quiere transmitir información en modo multicast (a muchos destinos) o en modo broadcast (a todos los destinos) pues no tiene sentido esperar la confirmación de todos los destinos para continuar con la transmisión. También es importante tener en cuenta que si en una transmisión de este tipo los destinos enviarán confirmación, fácilmente el emisor se vería colapsado, pues por cada paquete que envía recibiría tantas confirmaciones como destinos hayan recibido el paquete.

Lo que realmente proporciona UDP respecto a IP es la posibilidad de multiplexación de aplicaciones. La dirección del puerto permite identificar aplicaciones gracias a la dirección del puerto.

# CAPÍTULO III

# MECANISMOS DE TRANSICIÓN, TRADUCCIÓN, SEGURIDAD Y SERVICIOS EN IP-V6

## 3.1. INTRODUCCIÓN

Este capítulo tiene por objetivo realizar el estudio para poder implementar los mecanismos de transición de IP-V4 a IP-V6 donde coexistirán redes y host que funcionen con uno u otro protocolo. Este mecanismo se basa en Nodos, Routers, Servidores de Nombre Dual-IP, Tunneling IP-V6 sobre IP-V4, los nodos pueden ser actualizados parcialmente a IP-V6, siendo mejor actualizar los routers antes de hacerlo con los nodos. Al conjunto de modos de migración de IP-V4 a IP-V6 se los suele denominar SIT (Simple Internet Transition). Esta transición emplea los siguientes mecanismos:

- ✓ Implementación de una pila nula de IP-V4 e IP-V6 para los host y routers que deben de interpolar.
- ✓ Encapsulamiento de las direcciones IP-V4 en IP-V6. Los hosts serán asignados a direcciones IP-V6 interoperables con IP-V4 y los hosts con direcciones IP-V4 serán mapeados a direcciones IP-V6.
- ✓ Mecanismos de Tunneling para transportar paquetes IP-V6 sobre redes IP-V4. Estos túneles pueden ser automáticos (con direcciones IP-V6 compatibles con IP-V4) o manuales.
- ✓ Traducción de cabeceras IP-V4/IP-V6 realizada por los routers. Esta técnica debe ser utilizada cuando la implementación de IP-V6 este muy avanzada y queden pocos sistemas IP-V4.

Dentro de las principales actividades para la migración e implementación de túneles, seguridades y servicios se deben definir escenarios de interoperabilidad entre IP-

V4 e IP-V6 y estrategias de transición. Así mismo se debe evaluar las distintas tecnologías de acceso y transporte y su interacción con el protocolo IP-V6. También se debe evaluar los nuevos servicios en redes de próxima generación como seguridades y servicios.

Las aplicaciones clásicas en Internet están dirigidas para usuarios estáticos permitiendo realizar trasferencia de archivos: FTP, Telnet y/o Web. Con las nuevas aplicaciones se pueden establecer conexiones interactivas mediante acceso remoto siendo en tiempo real y necesitando grandes recursos de la red manipulando así grandes volúmenes de tráfico y gran ancho de banda, es decir; las redes deben de ofrecer alta calidad se servicio (QoS: Quality of Service) y una alta seguridad.

Para lograr el potencial completo de la nueva Internet, los usuarios finales deben poder confiar en la información y las transacciones en línea. A medida que la información digital va llegando a ser un artículo importante, ésta debe ser protegida y autenticada. Lo que vemos debe ser lo mismo que fue enviado y lo que recibimos. Se debe poder controlar los datos y proteger lo secreto en el ciberespacio. Esto exige mecanismos fáciles de usar, pocos costos y universalmente disponibles para la seguridad y autenticación. En particular, se necesitan de medios libres de fallos para:

- ✓ Asegurar la confidencialidad de datos enviados por la Internet;
- ✓ Probar que los datos privados seguirán siendo privados;
- ✓ Verificar que un mensaje fue enviado y recibido en forma correcta;
- ✓ Autenticar a individuos e información en la Web;
- ✓ Probar que alguien firmo un documento electrónico; y
- ✓ Certificar que se llevo a cabo una transacción a un tiempo dado.

Así mismo la mayor parte de los usuarios de Internet de hoy pasan gran parte de su tiempo en línea no haciendo otra cosa que esperar, esperar para ser conectado a un sitio Web, esperando para que se carguen páginas y esperando para bajar software. Como contraste la próxima generación de Internet nos dará la velocidad que necesitamos.

Los servicios de difusión son otra innovación de la especificación de IP-V6 que no se encuentra en IP-V4. IP-V6 ofrece procesamiento superior de opciones de destinación, autoconfiguración, encabezamientos, encapsulación, seguridad y direcciones de difusión.

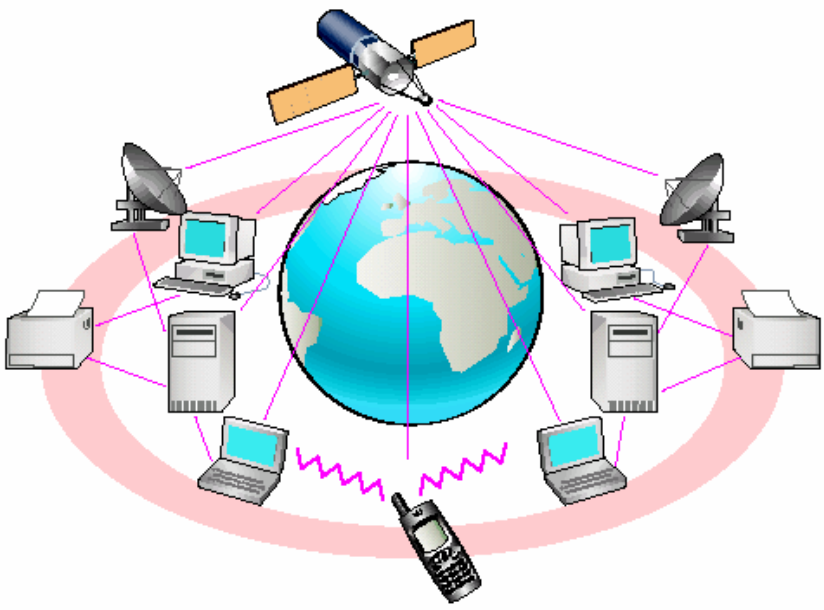


**Figura. 3.1. Servicios de difusión de la especificación IP-V6 que no se encuentra en IP-V4.**

IP-V6 significa redes más seguras y robustas de extremo a extremo que las que ofrece NAT con IP-V4, mientras que teóricamente brinda direcciones IP gratuitas para todos los usos imaginables, accesibles para todos en línea y fuera de línea. Esto, en sí mismo, puede contribuir significativamente tanto al desarrollo sostenible como a la reducción de la brecha digital tal como la conocemos hoy.

La seguridad es otro de los requerimientos del diseño del nuevo protocolo: todas las aplicaciones se deben beneficiar de las facilidades de autenticación y encriptación de datos de forma transparente. El estándar escogido para esto es IpSec.

## 3.2. MECANISMOS DE TRANSICIÓN

EL mecanismo se basa en Nodos, Routers, Servidores de Nombre Dual-IP, Tunneling IP-V6 sobre IP-V4. Los nodos pueden ser actualizados parcialmente a IP-V6, siendo mejor actualizar los routers antes de hacerlo con los nodos. En la figura 3.2 se indica un diagrama del mecanismo de transición entre IP-V4 e IP-V6

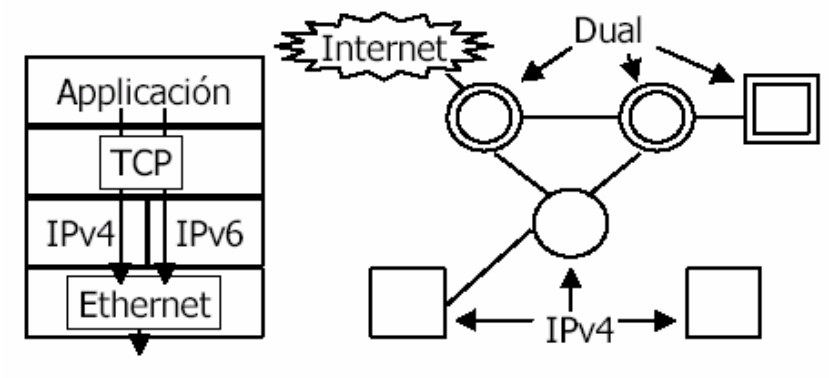



**Figura. 3.2. Mecanismo de Transición**

En la capa de Aplicación de debe tener en cuenta las siguientes consideraciones;

- ✓ La mayor parte de los protocolos de aplicación deberán ser actualizados, estos protocolos son: FTP, SMTP, Telnet, Rlogin.
- ✓ 27 de los 51 Full Internet Standards, 6 de los 20 Draft Starndards, 25 de los 130 Proposed Standards serán revisados para IP-V6.
- ✓ No hay checksum, El checksum en los niveles superiores es obligatorio, incluso en UDP.
- ✓ Los estándares no IETF: X-Open, Kerberos, deben ser actualizados y
- ✓ Se deben crear nuevos registros DNS.

## 3.3. TUNNELIG EN IP-V6

Puesto que Internet no va a amanecer un día utilizando de repente IP-V6 en vez de IP-V4, se han debido desarrollar una serie de métodos que permitan la convivencia y comunicación entre nodos, sea cual sea su versión de protocolo IP.

Encapsular un paquete IP dentro de otro es un mecanismo conocido y se usa en la actualidad sobre todo para crear redes privadas virtuales. La utilidad que le daremos aquí es para enlazar nubes o islas IP-V6 en una Internet basada en su totalidad en IP-V4.

Existen varios tipos básicos de túneles: Túneles Manuales o Estáticos (host-host, router-router, host-router) este tipo de túneles permiten atravesar nubes IP-V4 desde entidades IP-V6/IP-V4, Túneles Automáticos o Dinámicos donde la dirección destino es compatible con IP-V4, Túneles 6to4 donde este tipo de túnel permite tener direcciones IP-

V6 globales en redes solo IP-V6 donde hay un router frontera dual-stack encargado de dar salida al exterior y último tipo de Túnel es 6over4. IP-V4 actual se encuentra formado en su mayoría por túneles estáticos.

Los mecanismos de Tipo Túnel se basan en encapsular. Están enfocados en unir dos islas IP-Vx a través de un océano IP-Vy. Ver figura 3.3.

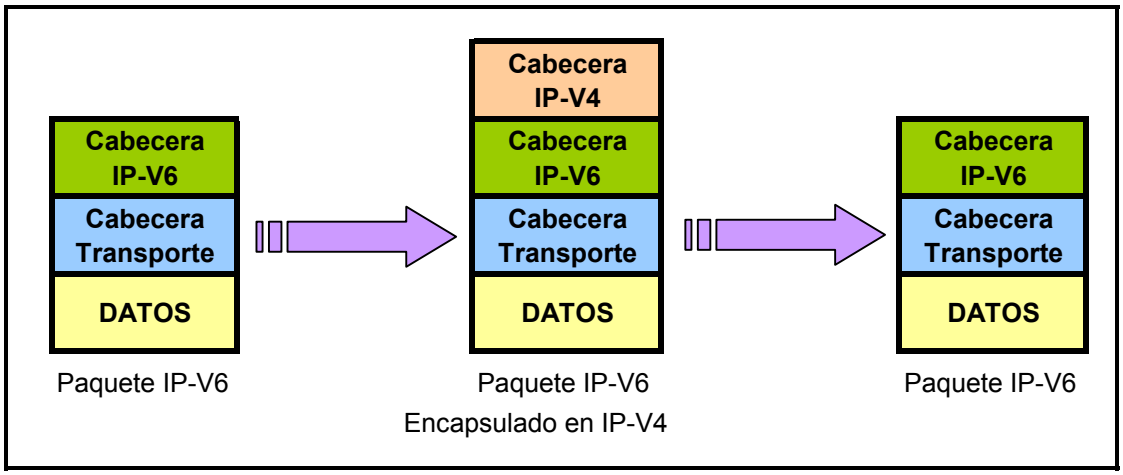



**Figura. 3.3. Mecanismos de Tipo Túnel**

Se debe tener en cuenta que IP-V4 e IP-V6 son incompatibles a nivel de paquete ya que los nodos finales actuales de Internet no generan ni reconocen IP-V6 y los routers IP actuales de Internet descartan paquetes IP-V6.

Cabe notar que si se realiza la migración de IP-V4 a IP-V6 la principal dificultad es migrar a la red Internet actual ya que durante la etapa de transición, a nivel lógico, habrá Internet IP-V4 e IP-V6 es por estas dificultades que se han desarrollado los diferentes tipos de mecanismos de transición de IP-V4 a IP-V6 los mismos que permiten la integración y/o interacción de sistemas IP-V4 e IP-V6.

### 3.3.1. TÚNELES MANUALES

Esta es la solución más sencilla y la menos intrusiva si queremos tener acceso tanto a IP-V6 como a IPV4. El caso más común será un host con IP-V4 que desee tener acceso a la red IP-V6 existente. Para ello se debe crear un túnel con un router a través de IP-V4 que tenga tanto acceso a IP-

V6 como a IP-V4. Un caso un poco menos común para el usuario es en el que se deseen unir "islas" IP-V6, es decir; unir redes IP-V6, utilizando para ello la infraestructura IP-V4 existente.

Este método se está utilizando en la actualidad por parte de algunos proveedores de servicios para que cualquiera pueda tener acceso a la red IP-V6. Dentro de esta categoría podemos considerar también la de los servidores de túneles, que en estos momentos son interfaces Web que permiten la creación de túneles bajo demanda a cualquier usuario.

Este tipo de túnel esta definido en la RFC 2893 bajo las siguientes características principales (Ver figura 3.3.1 (a)):

- ✓ Funcionalidad: interconectar islas IP-V6 a través de un océano IP-V4.
- ✓ Cada extremo es un nodo dual y en ellos se configura las direcciones IP-V4 e IP-V6 tanto local como remotas

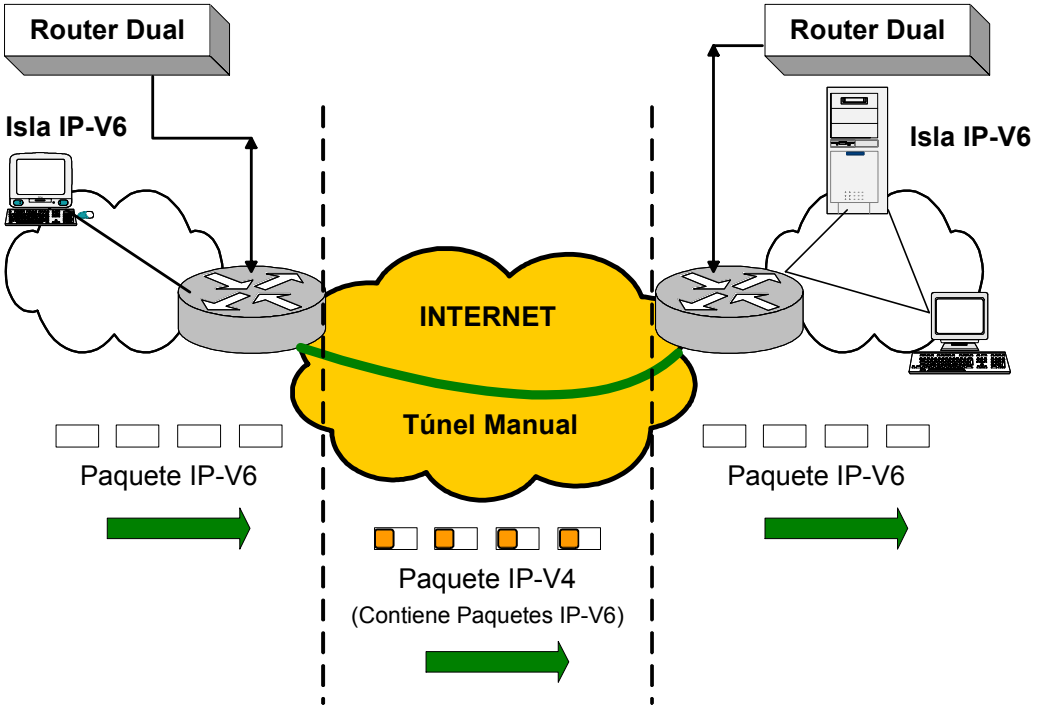



**Figura. 3.3.1. (a). Túnel Manual**

Las ventajas de este sistema de túneles manuales son:

- ✓ Método muy utilizado en el acceso al 6-Bone
- ✓ Disponible en multitud de plataformas (Cisco, Telebit, Linux, Solares, Windows NT, etc)
- ✓ Es un método totalmente transparente respecto al nivel IP-V6 y superiores, con lo cual no afecta a las aplicaciones.
- ✓ No consume excesivos recursos, la MTU se reduce a 20 bytes.
- ✓ Aplicación Principal: Conexión con ISP IP-V6 remoto a través de Internet

Así como tiene sus ventajas, existen los inconvenientes dentro de este tipo de túnel como:

- ✓ No son dinámicos, sino que establecen manualmente o de forma semi-automática.
- ✓ Si se unen N islas y la topología no considera un nodo central o intercambiador, el número de túneles a establecer en cada sitio asciende a N-1. En el caso de pensar en la conexión entre sí de miles de islas IP-V6 distribuidas por la Internet actual, este método carece de sentido.

La herramienta de Gestión para el establecimiento de los Túneles Manuales es el *Túnel-Broker* el mismo que ha sido definido en "Draft-ietf-ngtrans-broker". Estas herramientas se establecen bajo los siguientes parámetros:

- ✓ Sistema de Alta de Túneles con interfaz WEB.
- ✓ ISP-V6 proporcionan acceso al 6-Bone y son accesibles por Internet.
- ✓ Datos Usuario (Usuario).
- ✓ Datos Usuario y Configuración Local (Administrador Sistema).

El esquema para todos estos parámetros se indica en la figura 3.3.1 (b):

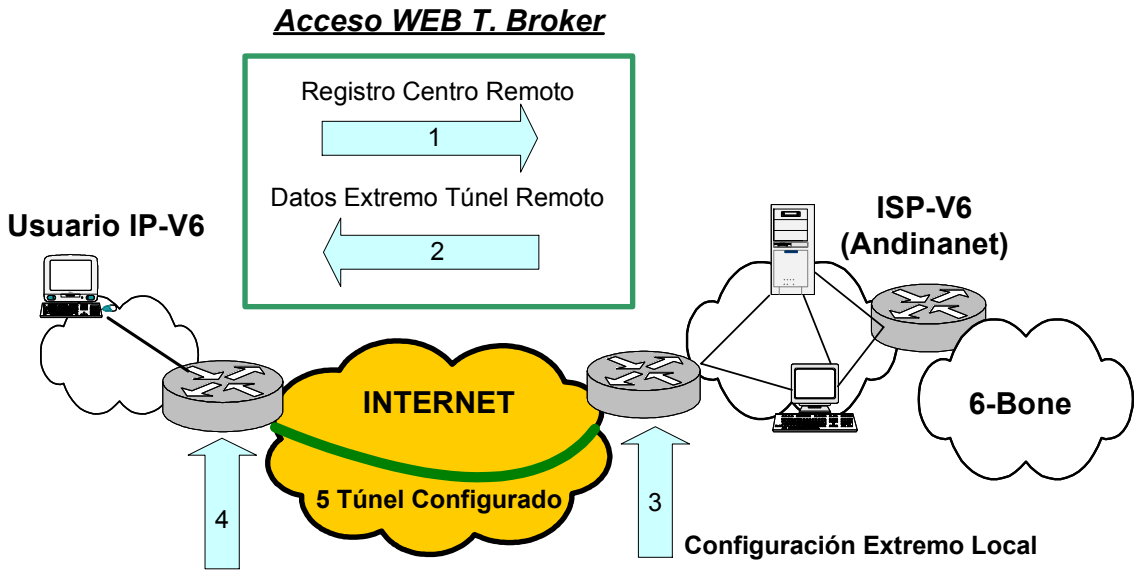



**Figura. 3.3.1. (b). Acceso WEB Túnel-Broker**

### 3.3.2. TÚNELES AUTÓNOMOS

Este tipo de túnel esta definido en la RFC 2893 bajo las siguientes características principales: (Ver figura 3.3.2)

- ✓ Permite a nodos duales comunicarse a través de una infraestructura IP-V4.
- ✓ Direcciones IP-V6 "IP-V4 Compatible": Prefijo 0::/96 + Dirección IP-V4.
- ✓ Se define una interfaz virtual para la dirección "IP-V4 Compatible".
- ✓ Los paquetes destinados a direcciones "IP-V4 Compatibles" se envían por el túnel automático bajo las siguientes reglas:

  - o Dirección origen IP-V6: Dirección "IP-V4 Compatible" local.
  - o Dirección destino IP-V4: Extraída de la dirección "IP-V4 Compatible" remota.

- ✓ Uso de Túneles Automáticos y Túneles Manuales: Hosts IP-V6 aislados (sin routers IP-V6 on-link)

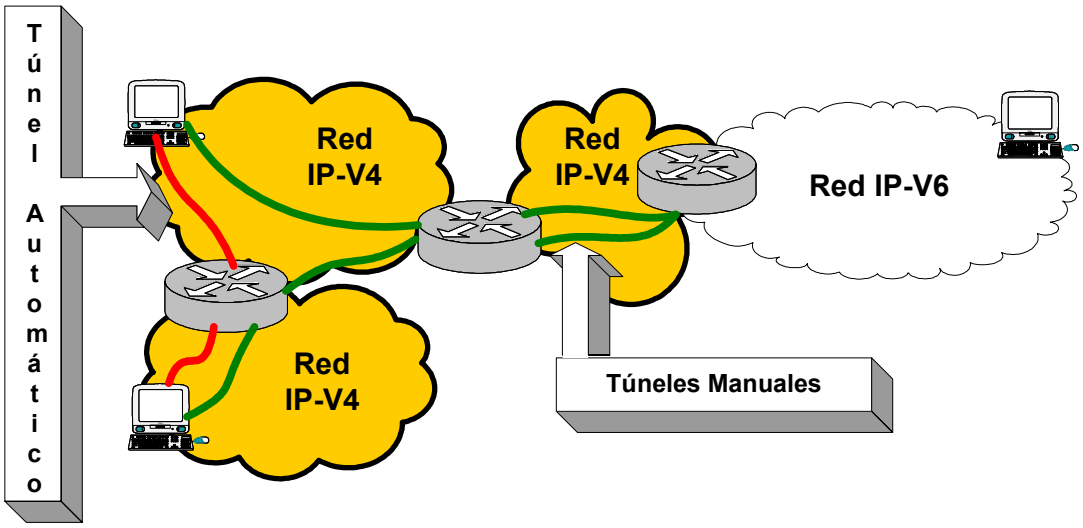



**Figura. 3.3.2. Túnel Automático**

### 3.3.3. TÚNELES 6to4

Este mecanismo se puede aplicar para comunicar redes IP-V6 aisladas por medio de la red IP-V4. El router extremo de la red IP-V6 crea un túnel sobre IP-V4 para alcanzar la otra red IP-V6. Los extremos del túnel son identificados por el prefijo del sitio IP-V6. Este prefijo consiste en 16 bits fijos que indican que se esta utilizando la técnica 6to4 más 32 bits que identifican al router externo del "sitio".

Un efecto secundario de 6to4 es que deriva automáticamente un prefijo /48 de una dirección IP-V4. De esta forma, los "sitios" pueden empezar a utilizar IP-V6 sin solicitar nuevo espacio de direccionamiento a la autoridad competente.

Este tipo de túnel esta definido en "Draft-ietf-ngtrans-6to4-06.txt" bajo las siguientes características principales: (Ver figura 3.3.3)

- ✓ Su principal aplicación es unir islas IP-V6 dispersas en un océano IP-V4.

- ✓ A cada isla IP-V6 se le asigna un prefijo: 2002::/16 mas la dirección IP del Router Frontera.
- ✓ Siguiente salto IP-V4 contenido en la dirección IP-V6
- ✓ El encaminamiento entre las distintas islas se apoya en el encaminamiento IP-V4 subyacente.
- ✓ Implementaciones: Windows NT y Proyecto KAME: Linux y FreeBSD

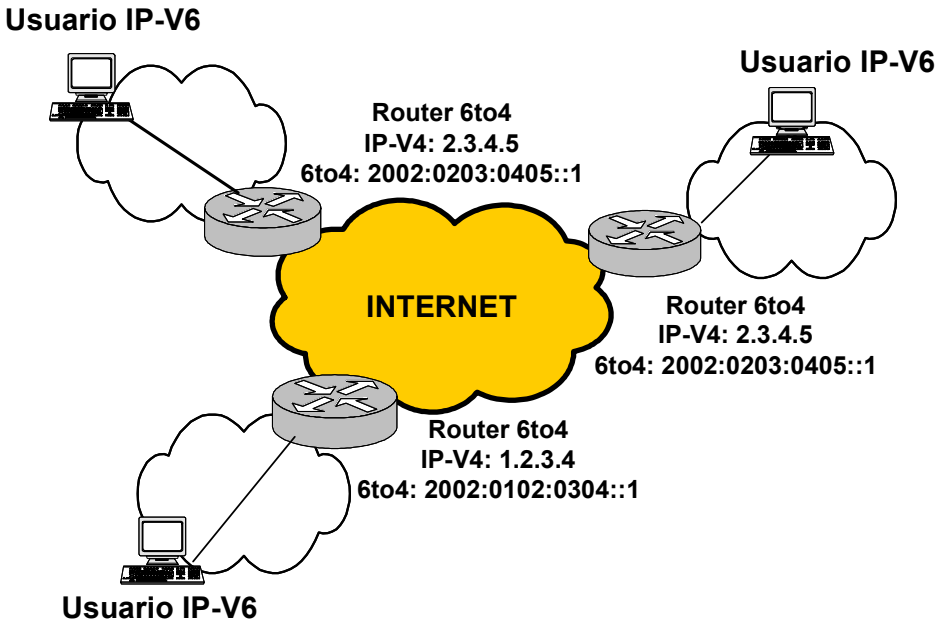



**Figura. 3.3.3. Túneles 6t04**

Las ventajas de este sistema de túneles 6to4 son:

- ✓ Al igual que los túneles manuales, son transparentes a nivel IP-V6 y, por tanto, no afectan a las aplicaciones.
- ✓ Se trata de túneles establecidos dinámicamente y sin configuración previa.
- ✓ Dadas N islas IP-V6, solo se establecen los túneles necesarios para las conexiones activas en cada momento.

Así como tiene sus ventajas, existen los inconvenientes dentro de este tipo de túnel como:

- ✓ Para organizaciones que se conecten a un ISP IP-V6 remoto, no es necesario más que un túnel (o quizá dos por redundancia con otro ISP IP-V6), por lo que puede ser suficiente emplear el mecanismo de Túneles Manuales, que se haya más extendido.

### 3.3.4. TÚNELES 6over4

Puede que no tengamos una red de sitio homogénea en el aspecto de que todos los nodos puedan comunicarse entre sí con la misma versión de protocolo IP. Con este método se puede comunicar nodos IP-V6 aislados dentro de un "sitio" con el resto de nodos IP-V4. Esta técnica también se emplea en casos en los cuales el router IP-V6 no tiene acceso o permiso para transmitir paquetes IP-V6 sobre el enlace. Para salvar este escollo se crea un enlace virtual utilizando un grupo multicast IP-V4, mapeando las direcciones IP-V6 sobre este grupo multicast.

Este tipo de túnel esta definido en la RFC 2529 bajo las siguientes características principales: (Ver figura 3.3.4)

- ✓ Nodos IP-V6 dispersos en subredes IP-V4 formándose una "LAN virtual" IP-V6.
- ✓ Tráfico IP-V6 entre nodos encapsulado en IP-V4. Direcciones IP-V4 Multicast.
- ✓ Los procesos de Neighbor/Router Discovery se hacen empleando Multicast.
- ✓ Router 6over4 con acceso 6-BONE, donde todos los nodos acceden al 6-BONE.

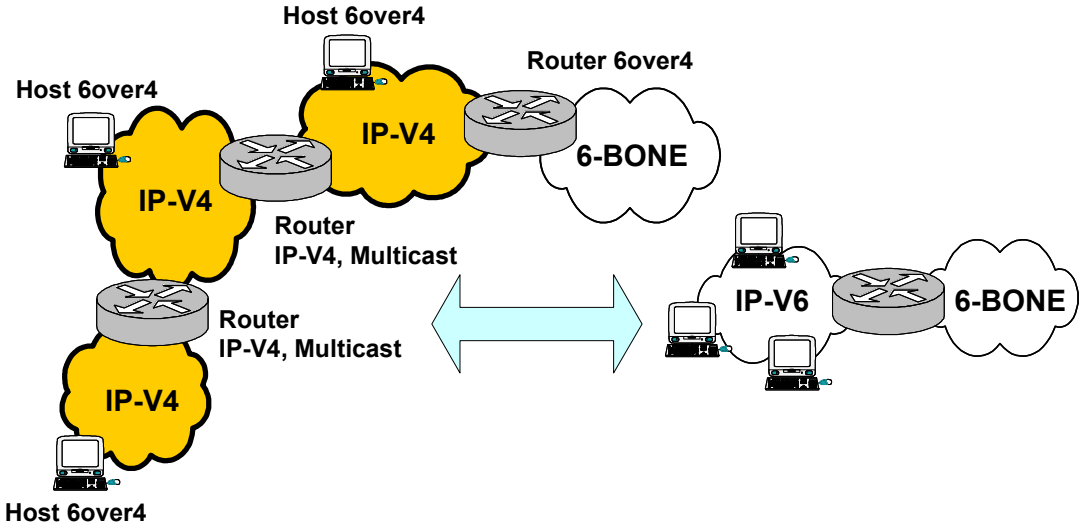



**Figura. 3.3.4. Túnel 6over4**

Las ventajas de este sistema de túneles 6over4 son:

- ✓ Al igual que los túneles anteriores, son transparentes a nivel IP-V6 y, por tanto, no afectan a las aplicaciones.
- ✓ Se trata de túneles establecidos dinámicamente y sin configuración previa.
- ✓ Permite probar IP-V6 en algunos nodos de una red IP-V4 corporativa sin instalar el snack IP-V6 en los routers internos.
- ✓ Instalando en un solo router el snack IP-V6 y conectándolo al 6-Bone se proporciona acceso a dicha red a todo el resto de nodos IP-V6.

Así como tiene sus ventajas, existen los inconvenientes dentro de este tipo de túnel como:

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

## 3.4. MECANISMOS DE TRADUCCIÓN

Adicionalmente dentro de los mecanismos de transición también tenemos los Mecanismos de Traducción los mismos que se basan en traducir un elemento de red, los paquetes de un formato a otro. Dentro de este tipo de mecanismos tenemos: NAT-PT, SOCKSv5, BIS (Bump in the Snack). Ver figura 3.4

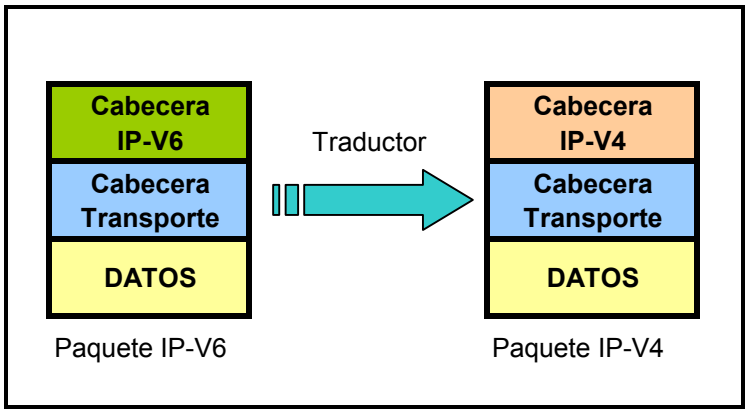



**Figura. 3.4. Mecanismos de Traducción**

### 3.4.1. NAT-PT

Este tipo de mecanismo de traducción esta definido en la RFC 2766 bajo las siguientes características principales: (Ver figura 3.4.1)

- ✓ NAT Tradicional: Traduce direcciones (conexión de redes con direcciones IP-V4 privado).
- ✓ NAT-PT: Traducción de direcciones y protocolo.
- ✓ Traducción basada en el algoritmo SIIT (RFC 2765).
- ✓ No es transparente a nivel de aplicación, para lo cual se precisa algunas extensiones:

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

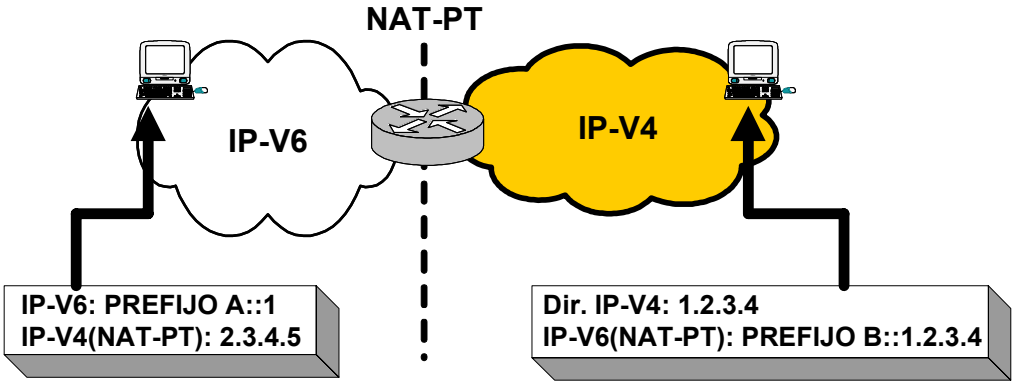



**Figura. 3.4.1. NAT-PT**

Las ventajas de este sistema de Mecanismo de Traducción son:

- ✓ Muchas redes corporativas poseen experiencia en la gestión/administración de NATs.
- ✓ Implementando en la mayor parte de los routers (Cisco, Telebit, Linux) y en algunas plataformas habituales en nodos finales (Windows 2000).
- ✓ Si la comunicación extremo a extremo es heterogénea (IP-Vx – IP-Vy) NAT-PT resulta adecuado (teniendo en cuenta siempre la carga de tráfico prevista).

Así como tiene sus ventajas, existen los inconvenientes dentro de este tipo de mecanismo de traducción como:

- ✓ Los NATs poseen un alto coste de gestión y administración.
- ✓ El proceso de traducción es mas costoso en recursos que el de entunelar.
- ✓ Si la comunicación extremo a extremo es homogénea (IP-Vx – IP-Vy) siempre es preferible emplear túneles a dos sistemas de traducción consecutivos.
- ✓ Si en un protocolo de aplicación intercambian direcciones IP (DNS, FTP, etc.), es necesario una extensión o módulo que

incluya un algoritmo para su tratamiento específico (DNS-ALG, FTP-ALG).

### 3.4.2. SOCKSv5

Este tipo de mecanismo de traducción esta definido en la RFC 1928, "Draft-ietf-ngtrans-socks-gateway-05" bajo las siguientes características principales: (Ver figura 3.4.2)

- ✓ Uso tradicional SOCKSv5: conectividad IP directa al Internet en redes con Firewall a determinados hosts.
- ✓ Servidor SOCKSv5 dual, siendo un traductor de protocolos (Algoritmo SIIT).
- ✓ Traducción IP-V4 – IP-V6 y viceversa. Conexiones SIEMPRE iniciadas por cliente.
- ✓ Dos componentes: Servidor SOCKSv5 + Librería SOCKSv5 (cliente).
- ✓ Implementaciones:
  - o NEC (www.socks.nec.com)
  - o Fujitsu (ftp://ftp.kame.net/pub/kame/misc)

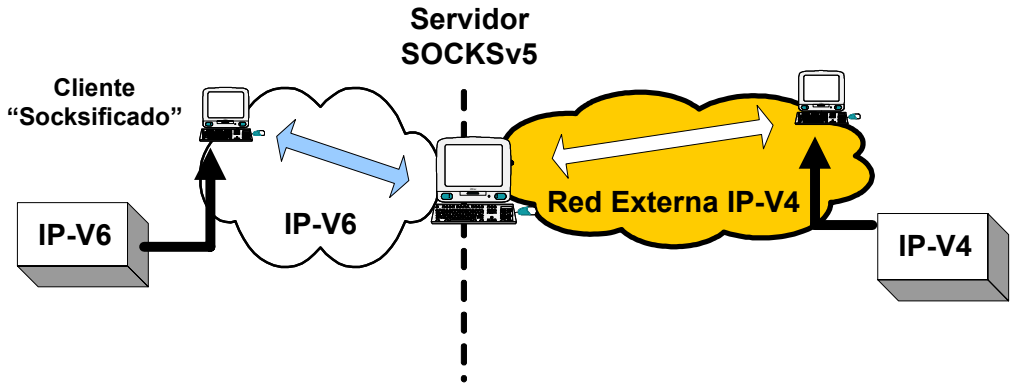



**Figura. 3.4.2. Socksv5**

El funcionamiento detallado para este mecanismo de traducción es: (Red IP-V4 = Red Interna)

- ✓ Uso aplicación en el nodo cliente inicia una conexión TCP o UDP con un nodo externo empleando el nombre completo (FQDN).
- ✓ La librería SOCKSv5 en el cliente intercepta la resolución del nombre ("gethostbyname") e indica una conexión TCP al puerto 1080 del servidor SOCKSv5.
- ✓ El servidor SOCKSv5 devuelve al cliente una dirección IP-V4 remota falsa ("fake IP-V4 address").
- ✓ El servidor SOCKSv5 inicia la conexión TCP o UDP con el nodo remoto y hace de proxy entre el cliente y el nodo extremo. Si el nodo extremo es IP-V6, aplica además el algoritmo de traducción SIIT (RFC 2765).
- ✓ En el cliente, los paquetes con la "fake IP-V4 address" como origen o destino son interceptados y tratados por las librerías SOCKSv5 que los recibe o envía respectivamente al servidos SOCKSv5.

Las ventajas de este sistema de Mecanismo de Traducción son:

- ✓ Sistema apto actualmente para corporaciones que deseen dar acceso a determinados nodos internos a servicios IP-V6 sin probar exhaustivamente el protocolo.
- ✓ Provee sistemas de autenticación adecuados para evitar usos indeseados.

Así como tiene sus ventajas, existen los inconvenientes dentro de este tipo de mecanismo de traducción como:

- ✓ Instalación de las librerías SOCKSv5 en todos los clientes a los que se desee dar acceso.
- ✓ El proceso de traducción es costoso en cuanto a consumo de recursos en el servidor, por lo que un factor limitante es la carga de tráfico prevista.

- ✓ Las conexiones solo pueden ser iniciadas por los nodos internos, con lo cual no es posible ofrecer servicios al exterior mediante este método.
- ✓ Como todos los mecanismos de traducción debe incorporar algoritmos específicos para aquellos protocolos de aplicación que intercambien direcciones IP (FTP).

## 3.5. ESTRATEGIAS DE MIGRACIÓN

Para poder realizar la migración del protocolo IP-V4 a IP-V6 se debe considerar las siguientes características:

- ✓ IP-V4 e IP-V6 son incompatibles a nivel de paquete debido a que:
  - o Los nodos finales actuales de Internet bajo la infraestructura de ANDINANET S.A. no generan ni reconocen IP-V6.
  - o Los routers IP actuales de Internet descartan los paquetes IP-V6.
- ✓ La principal dificultad es migrar la red de Internet:
  - o Durante la etapa de transición, a nivel lógico habrá Internet IP-V4 e IP-V6 (Ver figura 3.5 (a))

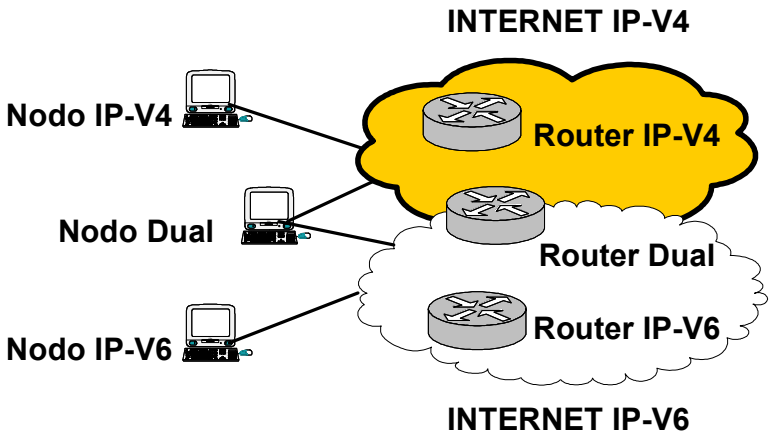



**Figura. 3.5. (a). Etapa de Transición**

Debido a este tipo de inconvenientes en ANDINANET S.A. se esta planteando un estudio para así poder establecer un mecanismo de transición de IP-V4 a IP-V6 permitiendo así la integración y/o interacción de sistemas IP-V4 e IP-V6.

La migración del protocolo IP-V4 a IP-V6 significa un cambio a nivel de BackBone, Plataforma, Infraestructura para un ISP, para el caso del desarrollo de este proyecto de ANDINANET S.A. Si fuere el caso de querer realizar la migración de IP-V4 a IP-V6 se deben considerar los siguientes parámetros:

- ✓ Redes Finales
- ✓ ISP y Backbones principales

Antes de considerar estos parámetros para la migración de protocolo, se debe tener en cuenta las siguientes recomendaciones:

- ✓ Servidores "Doble stack": para atender peticiones IP-V4 e IP-V6.
- ✓ Clientes "Doble stacks": conectividad con servidores IP-V4 e IP-V6

Una estrategia de Migración de Redes Finales (clientes y servidores) es mediante mecanismos de Traducción los mismos que se fueron detallados anteriormente. (Ver figura 3.5 (b)).

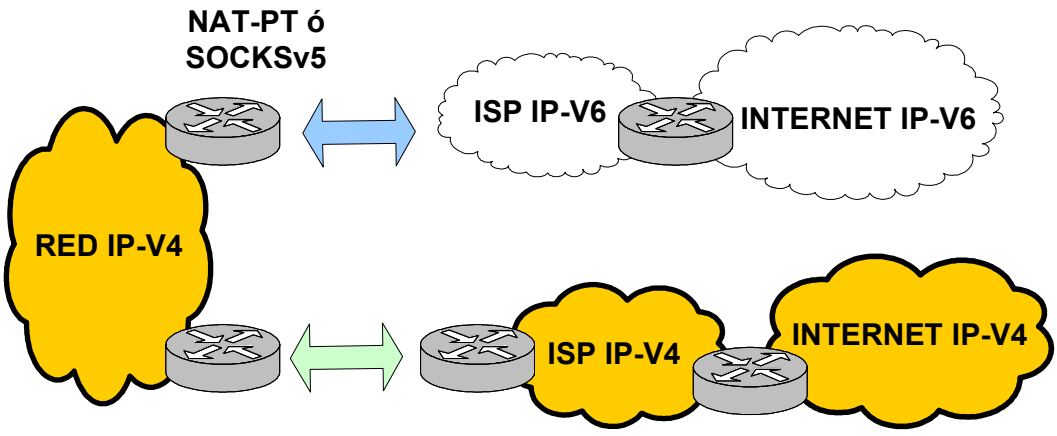



**Figura. 3.5. (b). Migración de Redes Finales**

Otro tipo de estrategia para la Migración es mediante los mecanismos de tipo Túnel bajo dos fases:

- ✓ ***Primera Fase:*** conexión IP-V4 al ISP (ANDINANET S.A.) y entunelar el tráfico IP-V6 en IP-V4, hasta que el ISP ofrezca conexión con IP-V6 Nativo. (Ver figura 3.5 (c)).
- ✓ ***Segunda Fase:*** conexión IP-V6 al ISP y túnel IP-V4 sobre IP-V6 para conectar Internet IP-V4 (caso complementario).

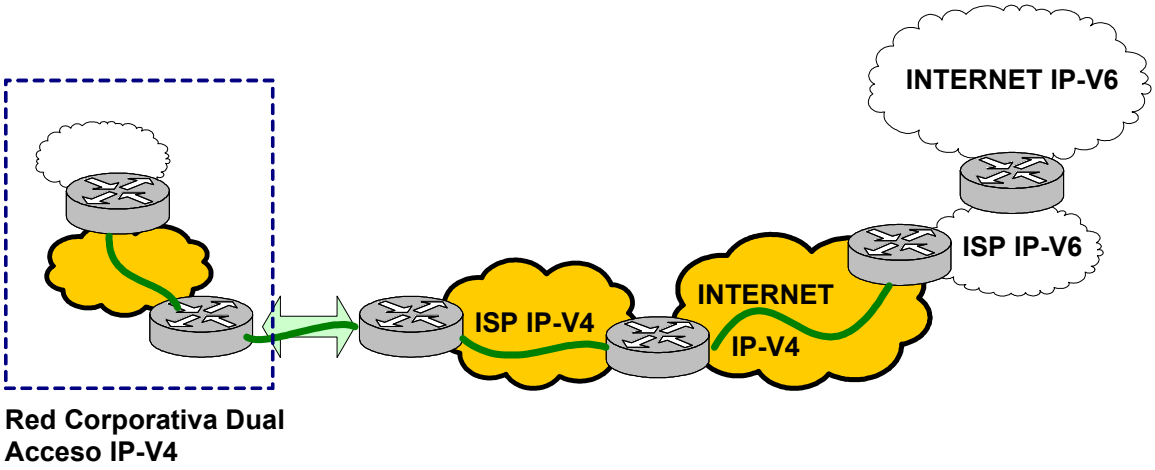



**Figura. 3.5. (c). Mecanismo de Tipo Túnel**

También existe otro tipo de estrategia para la migración del protocolo IP-V4 a IP-v6 la misma que es para ISPs. Esta estrategia se basa en dos Modos de Acceso que son:

- ✓ ***ISP IP-V4 Trasicionales:*** Acceso IP-V4 y tratar de ofrecer acceso a Internet IP-V6 mediante un traductor.
- ✓ ***Nuevos ISP IP-V6:*** Acceso IP-V6 y mediante túnel a través de Internet ofrecer conectividad a Internet IP-V4 mediante traductores.

Por último dentro de las estrategias para la migración del protocolo IP-V4 a IP-V6 se tiene la Estrategia de Migración de Backbones donde se debe mantener la configuración actual y migrar cuando el trafico entunelado sobre tráfico IP-V4. Debido a los problemas del número de rutas existente se debe recomendar y colaborar con los ISP y otros Backbones para evitar así una migración "forzosa".

## 3.6. LUZ AL FINAL DEL TÚNEL IP-V6

Algunas expectativas en el despliegue pueden llevar más tiempo que el previsto. La seguridad, exigida para IP-V6, ofrece tanto robustez como espacio infinitamente escalable de direcciones IP, no disponibles con IP-V4.

Realizar la migración del protocolo IP-V4 a IP-V6 para la plataforma que tiene actualmente ANDINANET S.A. no es factible debido a que en nuestro medio los usuarios finales no tienen equipos y software para soportar el mismo. Para la implementación del protocolo IP-V6 en ANDINANET S.A. se recomienda realizarla mediante Túneles ya sea Manual o Automático obteniéndose así tener direcciones IP-V6 más IP-V4 en los routers principales y una dirección IP-V4 donde el cliente, ganando espacio de direcciones para la masificación de ANDINANET S.A. y poder prestar a los clientes los diferentes servicios bajo buenos niveles de seguridad que se manejan bajo IP-V6.

## 3.7. SEGURIDAD EN IP-V6

En IP-V4 la seguridad se consigue mediante técnicas de criptografía en la capa de aplicación, mientras que en IP-V6 la seguridad se puede conseguir a nivel de la capa de red (Protocolo IP), y se implementa en los routers. En IP-V6 la seguridad se implementa mediante la extensión de cabeceras diseñadas específicamente para dicho propósito (como es el caso de la cabecera de autentificación y cifrado de la carga).

IPSec es un conjunto de estándares abiertos desarrollados por el *Internet Enginnering Task Force* (IETF) que ofrece protección en la transmisión de información sensible sobre redes inseguras tal como es la propia Internet, así IPSec actúa en la capa de Red, protegiendo y autentificando paquetes IP entre los dispositivos principales.

IPSec tiene tres componentes principales:

- ✓ Authentication Header (AH).
- ✓ Encapsulating Security Payload (ESP)
- ✓ Internet Key Exchange (IKE)

Cada uno de estos componentes forman parte de la Estructura IPSec teniendo así interoperabilidad, siendo independiente de algoritmos criptográficos actuales. IPSec soporta tanto IP-V4 como IP-V6 siendo una componente obligada en IP-V6. la arquitectura para IPSec se indica en la figura 3.7

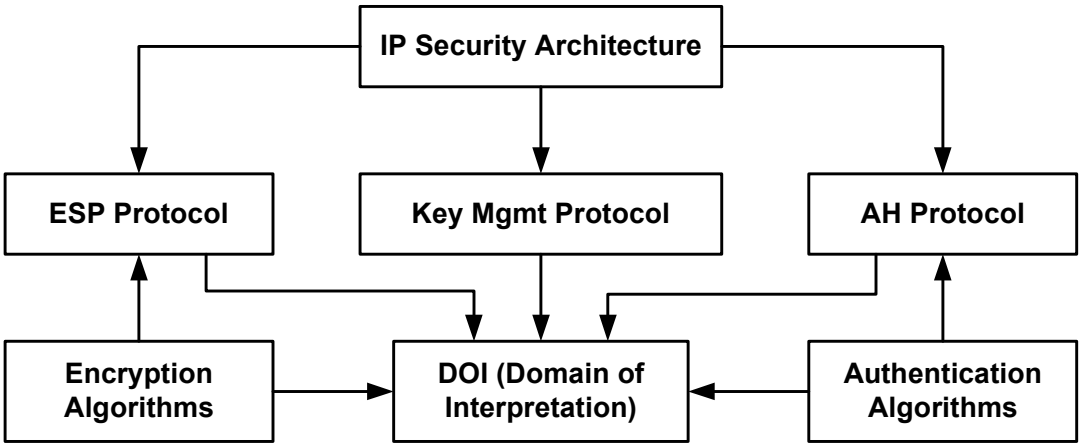



**Figura. 3.7. Arquitectura IPSec**

IPSec tiene los siguientes beneficios:

- ✓ Herencia de niveles de seguridad
- ✓ Transparencia en las aplicaciones
- ✓ Transparencia respecto a usuarios finales
- ✓ Seguridad a nivel individual.

IPSec asegura paquetes de bajo nivel creando redes seguras sobre canales inseguros, asegurando así una red completa mientras que SSL actualmente empleado opera en la capa de transporte y no necesita estar en la misma red segura, SSL asegura los aplicaciones a través de una red pública.

Dentro de las aplicaciones que brinda IPSec tenemos:

- ✓ IPSec brinda privacidad, integridad y autentificación para el comercio electrónico.
- ✓ Satisface rigurosos requerimientos para la transmisión de información sensible en Internet.

- ✓ Al implementarse sobre las redes no se afecta a la base instalada.

### 3.7.1. TIPOS DE SEGURIDADES

#### 3.7.1.1. SEGURIDAD NODO A NODO

Ver figura 3.7.1.1

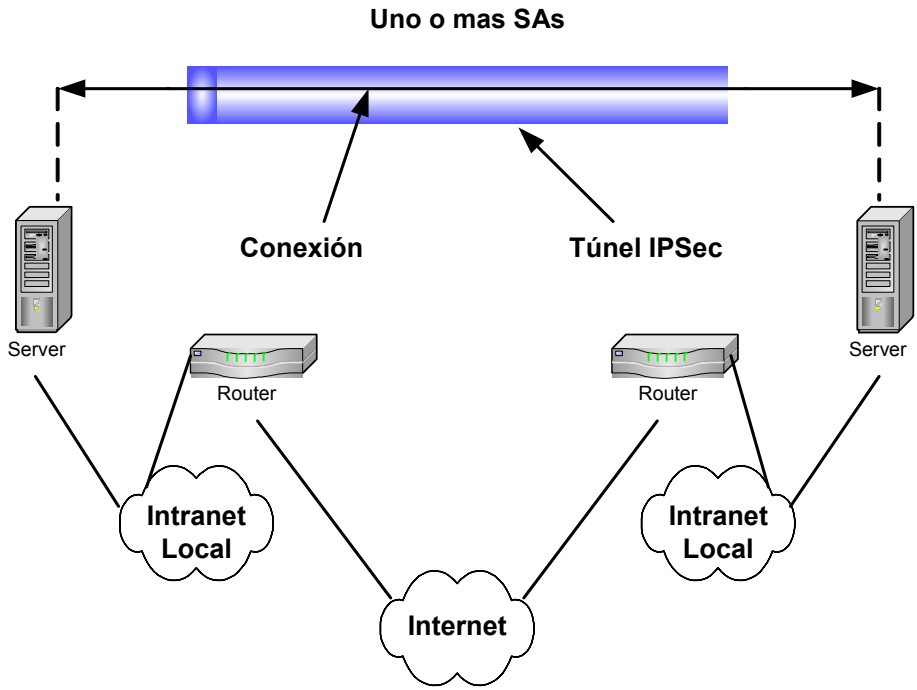



**Figura. 3.7.1.1. Seguridad Nodo a Nodo**

#### 3.7.1.2. SOPORTE BÁSICO VPN

Ver figura 3.7.1.2

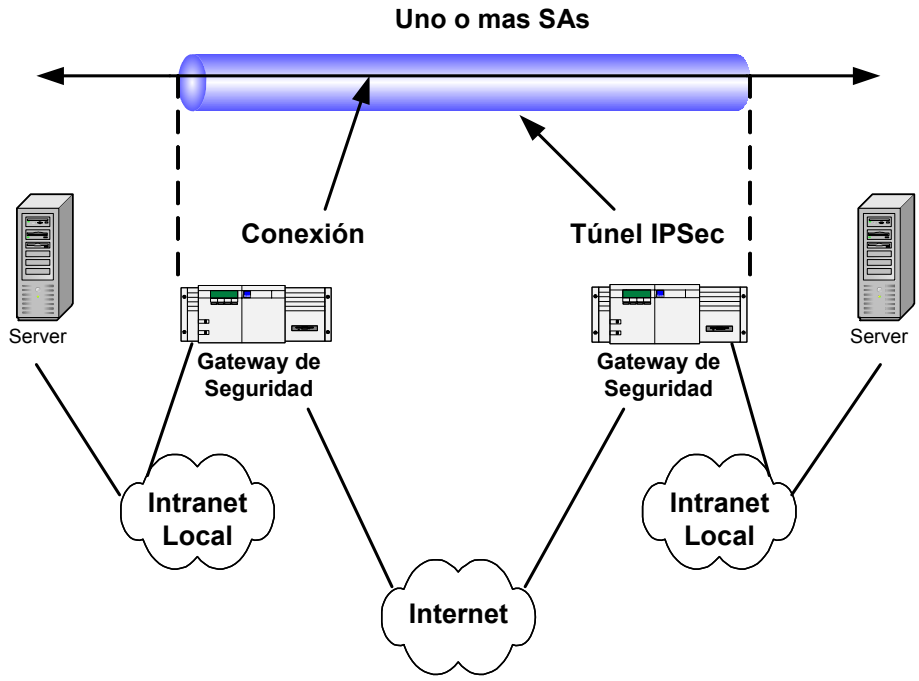



**Figura. 3.7.1.2. Soporte Básico VPN**

### 3.7.1.3 SEGURIDAD NODO A NODO CON SOPORTE VPN

Ver figura 3.7.1.3

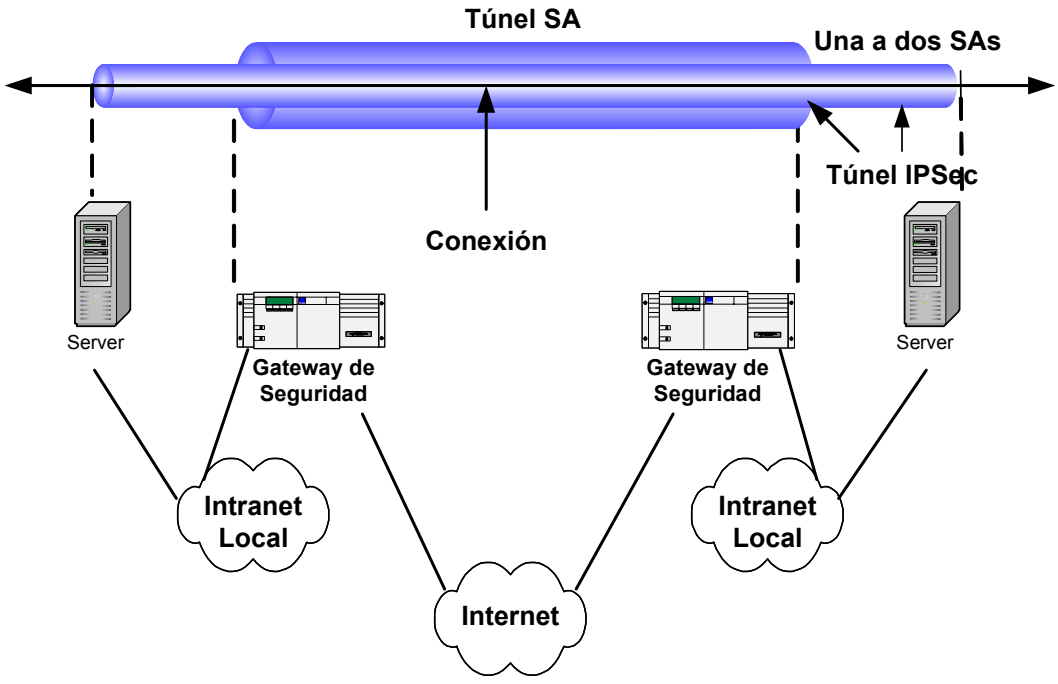



**Figura. 3.7.1.3. Seguridad Nodo a Nodo con Soporte VPN**

### 3.7.1.4. ACCESO REMOTO

Ver figura 3.7.1.4

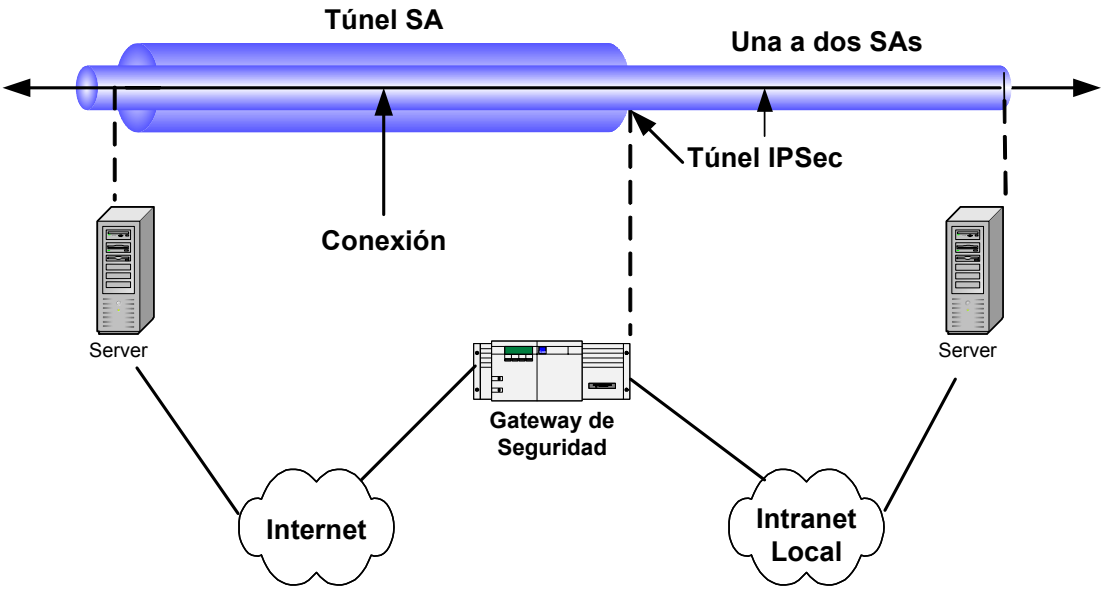



**Figura. 3.7.1.4. Acceso Remoto**

Para lograr el potencial completo de la nueva Internet, los usuarios finales de ANDINANET S.A. deben poder confiar en la información y las transacciones en línea tanto como o más que lo que confían en documentos en copia impresa. A medida que la información digital va llegando a ser un artículo importante, este debe ser protegida y autentificada. Lo que vemos debe ser lo mismo que fue enviado y lo que recibimos. Debemos poder controlar nuestros datos y proteger nuestro secreto en el ciberespacio, es por esto que se emplean y se exponen mecanismos fáciles de usar, poco costosos y universalmente disponibles para la seguridad y la autentificación. En particular se necesitan medios libres de fallos para:

- ✓ Asegurar la confidencialidad de datos enviados por la Internet;
- ✓ Probar que los datos privados seguirán siendo privados;
- ✓ Verificar que un mensaje fue enviado y recibido en forma correcta;
- ✓ Autenticar a individuos e información en la Web;
- ✓ Probar que alguien firmo un documento electrónico; y,
- ✓ Certificar que se llevo a cabo una transacción a un tiempo dado.

## 3.8. CALIDAD Y SERVICIOS EN IP-V6

La mayor parte de los usuarios de ANDINANET S.A. pasan una gran parte de su tiempo en línea no haciendo otra cosa que esperar, esperar para ser conectado a un sitio Web, esperando para que se carguen páginas y esperando para bajar software. Como contraste, la próxima generación de Internet nos brindara la velocidad que necesitamos.

IP-V4 lleva un byte de servicios diferenciados e IP-V6 lleva un byte de clase de tráfico equivalente, destinado para el apoyo de servicios simples diferenciados. IP-V4 e IP-V6 pueden apoyar cada uno el protocolo de reservación de recursos (RSVP) para implementaciones QoS mas complejas. El formato de paquete IP-V6 contiene un nuevo campo de identificación de flujo de tráfico de 24 bit que será de gran valor para los vendedores que implementan funciones de red de calidad de servicio. Aún cuando estos productos se encuentran todavía en la fase de planificación. IP-V6 sienta las bases, permitiendo que se haga disponible una amplia gama de funciones QoS (inclusive reservación de ancho de banda y límites de retardo) de una manera abierta e interoperable.

Un beneficio adicional para QoS en IP-V6 es que se puede usar una etiqueta de flujo (asignada dentro del encabezamiento de IP-V6) para distinguir flujos de tráfico para obtener un encaminamiento optimizado. Además se puede usar la etiqueta de flujo para identificar flujos aún cuando la carga útil esta encriptada. El encaminamiento basado influjo puede dar a las redes internas algunas de las características determinativas asociadas con la tecnología de conmutación orientada en conexiones y circuitos virtuales. Las etiquetas de flujo se pueden usar también para dar a flujos de tráfico un nivel específico de seguridad, retardo de propagación, o costo.

Hoy en día cuando entramos a un hogar o una oficina, vemos típicamente uno o más ordenadores. Se puede imaginar de entrar a un hogar y ver docenas o hasta cientos de ordenadores, PDAs y otros dispositivos todos conectados al Internet. Se puede imaginar un mundo en el casi cualquier cosa contenga una pequeña tarjeta inteligente que puede comunicarse por medio de un enlace sin hilos a la Internet.

Varios aspectos del diseño del protocolo IP-V6 son directamente beneficiosos a, y van mas allá de solo dar apoyo de marcación para, la computación móvil. Un

procesamiento mejorado de opciones de destinación, la autoconfiguración, los encabezamientos de encaminamiento, la encapsulación, la seguridad y las direcciones de difusión a cualquiera contribuyen al diseño lógico de movilidad de IP-V6. La ventaja de la movilidad de IP-V6 puede ser puesta de relieve aún mas por la adicción de gestión de etiqueta de flujo, lo que da a los nodos móviles una calidad de servicio aún mejor.

Uno de los requisitos comerciales de más rápido crecimiento para redes internas es la capacidad de transmitir una corriente de video, audio, noticias, datos financieros, u otros datos sobre tiempo a un grupo de estaciones extremas funcionalmente relacionadas pero geográficamente dispersas. La mejor manera de lograr esto es por medio de técnicas de multidifusión de capa de red.

Los servicios de difusión a cualquiera son otra innovación de la especificación IP-V6 que no se encuentra en IP-V4. La difusión a cualquiera es conceptualmente un cruce entre unidifusión y multidifusión: dos o más interfases en un número arbitrario de nodos son designados como un grupo de difusión a cualquiera.

Hoy, toda la información que circula en la Red recibe la misma prioridad; eso significa que compiten por el mismo ancho de banda un correo electrónico, un archivo que se descarga de un servidor FTP y una video conferencia. La implantación de la QoS permitirá a las aplicaciones solicitar por si mismas una cantidad determinada de ancho de banda o una prioridad específica. Esto lograría que los computadores que estuviesen procesando una aplicación como la teleinmersión o la video conferencia se pudiesen comunicar entre sí a la alta velocidad requerida para las interacciones correspondientes, “en tiempo real”.

Dentro de las aplicaciones mas relevantes, que utiliza IP-V6 como infraestructura para su funcionamiento, son:

- ✓ Videoconferencia Multimedia y Videoconferencia Teleinmersiva
- ✓ Telemedicina
- ✓ Bibliotecas Digitales Multimedia
- ✓ Laboratorios Virtuales.

Cada una de estas aplicaciones serían posibles con la tecnología del Internet de hoy.

Para promover el desarrollo de IP-V6 en ANDINANET S.A. y en el Ecuador, por iniciativa de diversas Universidades Politécnicas, en el año 2002 se conformó la denominada COEDI2 (Corporación para el Desarrollo de Internet 2) en la que también participan instituciones como CONATEL (Consejo nacional de Telecomunicaciones) y FUNDACYT (Fundación para la Ciencia y Tecnología), además de empresas estatales como ANDINATEL y PACIFICTEL.

La intención de todos estos actores es participar activamente en el desarrollo del nuevo Internet IP-V6 en el Ecuador. Esto incluye:

- ✓ Infraestuctura física y lógica: redes, enlaces, sistemas, equipos de alto rendimiento, protocolos y procedimientos adecuados de los mismos que ANDINANET S.A. cuenta al momento,
- ✓ Aplicaciones que incluyan el aprovechamiento de las posibilidades de IP-V6.
- ✓ Recursos Humanos, capaces de desarrollar IP-V6.

### 3.8.1. VIDEOCONFERENCIA MULTIMEDIA Y TELEINMERSIVA

La videoconferencia multimedia interactiva permite que los usuarios geográficamente distantes puedan compartir e intercambiar información a través de voz, video y datos, "en tiempo real". Los anchos de banda de IP-V6 permiten asegurar la calidad de esa interacción. Ver figura 3.8.1 (a).


**Figura. 3.8.1. (a). Videoconferencia Multimedia**

La "Teleinmersión" por su parte, es un tipo avanzado de videoconferencias, en tres dimensiones, que permite que gente geográficamente apartada se encuentre en una sala de conferencias virtual. Ver figura 3.8.1 (b)

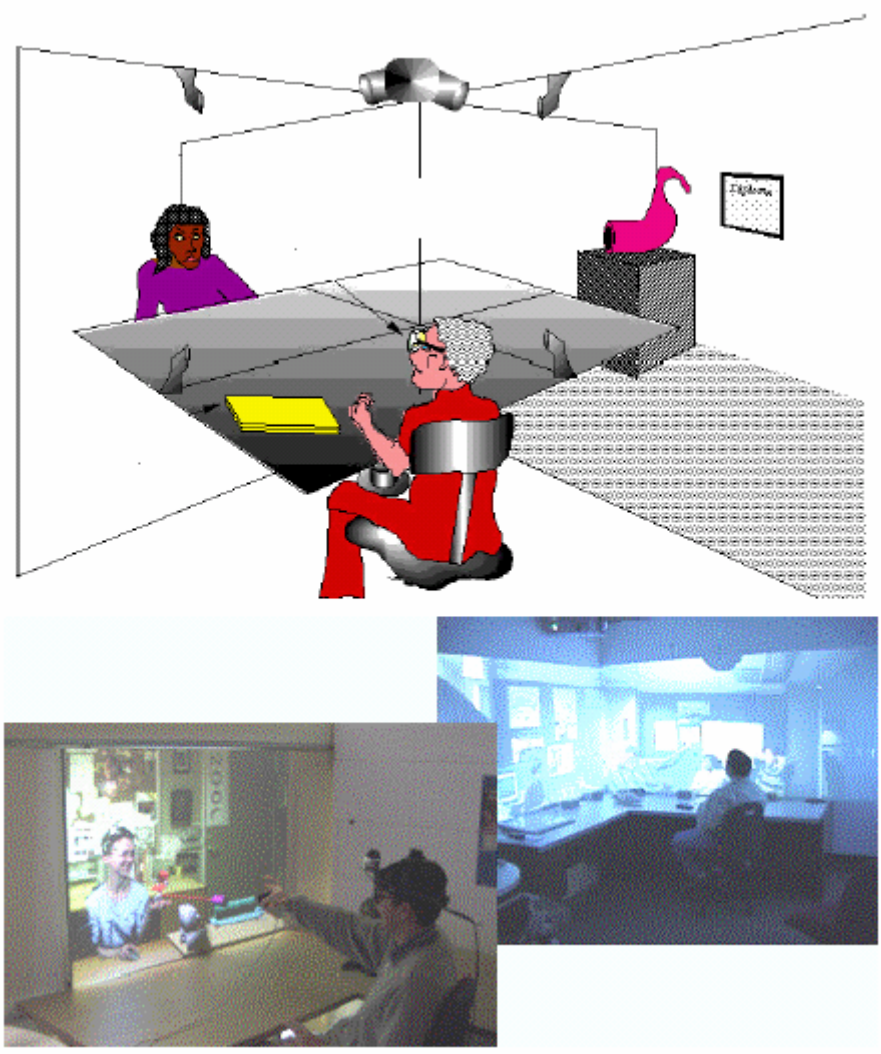


**Figura. 3.8.1. (b). La Teleinmersión**

La Teleinmersión podría ir más lejos al permitir a sus participantes compartir un entorno de realidad virtual que les permitiera la comunicación humana de forma natural y la interacción dentro de una aplicación común.

En una red como Internet 2, la experiencia del video streaming puede desarrollarse a varias decenas de Mbps, con un sistema de sonido envolvente (sound surround) y megapantallas de alta definición.

Para la mayoría de los usuarios de Internet, una transmisión de audio y video (multimedia) significa soportar un sonido que se entrecorta y una imagen que se detiene y pierde sincronía con el sonido, desplegándose sobre

una pequeña ventana dentro de la pantalla de una PC. Con IP-V6 la historia es muy diferente.

### 3.8.2. TELEMEDICINA

Por definición, "Telemedicina" es la provisión de cuidados de salud y de educación médica, a distancia, utilizando tecnologías de información y de comunicaciones.

La Telemedicina (también conocida como telesalud o e-salud) permite a los profesionales del cuidado de la salud, utilizar dispositivos médicos "conectados" a las redes telefónicas o a redes de datos (alambicas e inalámbricas), en la evaluación, diagnóstico y tratamiento de pacientes localizados en sitios diferentes al del profesional médico. Estos dispositivos mejoran su rendimiento mediante el uso de tecnología de telecomunicaciones, computación en red, sistemas de videoconferencia y sistemas de codificación-decodificación. El software de aplicación especializado, los dispositivos de almacenamiento de bases de datos, y los dispositivos médicos capaces de recolectar datos electrónicos, almacenar y transmitir son componentes claves de la infraestructura de Telemedicina. Ver figura 3.6.2

**Figura. 3.8.2. Telemedicina**

La telemedicina usa normalmente dos métodos para transmitir imágenes, datos y sonido:

- ✓ Transmisiones en vivo, en las que el profesional médico participa en el examen del paciente mientras la información de diagnóstico es recolectada y transmitida por las redes, desde el sitio en el que está el paciente hasta el sitio en que se encuentra el médico.
- ✓ Transmisión basada en almacenamiento y envió, en el que el profesional médico revisa la información posteriormente a la recolección de datos.

Muchos programas y sistemas utilizan ambos tipos de transmisión, para maximizar el uso eficiente de recursos apropiados para los servicios médicos que se proveen, dependiendo de la infraestructura disponible.

Las redes privadas de telemedicina son una tecnología disponible en los mejores hospitales del mundo; sin embargo, su elevado costo ha impedido un uso mas amplio de estos servicios.

En la actualidad la disponibilidad tecnológica es cada vez un problema menos importante en telemedicina.

### 3.8.3. BIBLIOTECAS DIGITALES MULTIMEDIA

Desde el punto de vista del aprendizaje, un vídeo bien realizado fácilmente puede convertirse en una herramienta mucho más efectiva que el simple texto. Las bibliotecas digitales que contienen este tipo de material se conocen como Bibliotecas Digitales Multimedia.

Las prestaciones que ofrece IP-V6 le convierten en el medio ideal para difundir este tipo de servicios, que en el Internet tradicional ha logrado sólo un mínimo desarrollado. Ver figura 3.8.3


**Figura. 3.8.3. Biblioteca Digital Multimedia**

Esta categoría de aplicación, combinada con tecnologías de reconocimiento de voz y procesamiento de lenguaje natural permitirán la catalogación automática, la búsqueda inteligente y la recuperación selectiva de información.

### 3.8.4. LABORATORIOS VIRTUALES

En principio, un Laboratorio Virtual es una infraestructura de experimentación o de pruebas que no existe físicamente en el sitio en que se encuentran los realizadores de esos experimentos, pero puede existir en otro lugar del planeta, o haber sido creado electrónicamente dentro de un sistema computacional.

Existen dos enfoques bajo los que se desarrolla la tecnología de los Laboratorios Virtuales:

- ✓ Laboratorios Virtuales por simulación
- ✓ Laboratorios Virtuales por acceso remoto

En el primer caso, se utiliza software y hardware que permite la posibilidad de modelar experimentos y experiencias (simulación), con interactividad gráfica apropiada.

En el segundo caso, se accede a equipos y dispositivos reales ubicados en sitios diferentes a aquellos en que se encuentran quienes realizan los experimentos (acceso remoto).

La infraestructura tecnológica de los laboratorios virtuales generalmente tiene algunos o todos los componentes siguientes:

- ✓ Servidores de computación capaces de manejar reducciones de datos y simulaciones a gran escala.
- ✓ Bases de datos que contengan información específica para aplicaciones, tales como simulación inicial y condición límite, observaciones experimentales, requerimientos de clientes, restricciones de fabricación: así como recursos distribuidos específicos de las aplicaciones, tales como las bases de datos del genoma humano.
- ✓ Instrumentos científicos conectados a la red.
- ✓ Herramientas de colaboración, que a veces incluye la teleinmersión.
- ✓ Software especializado para simulación, análisis de datos, descubrimiento, reducción y visualización. Ver figura 6.8.4.

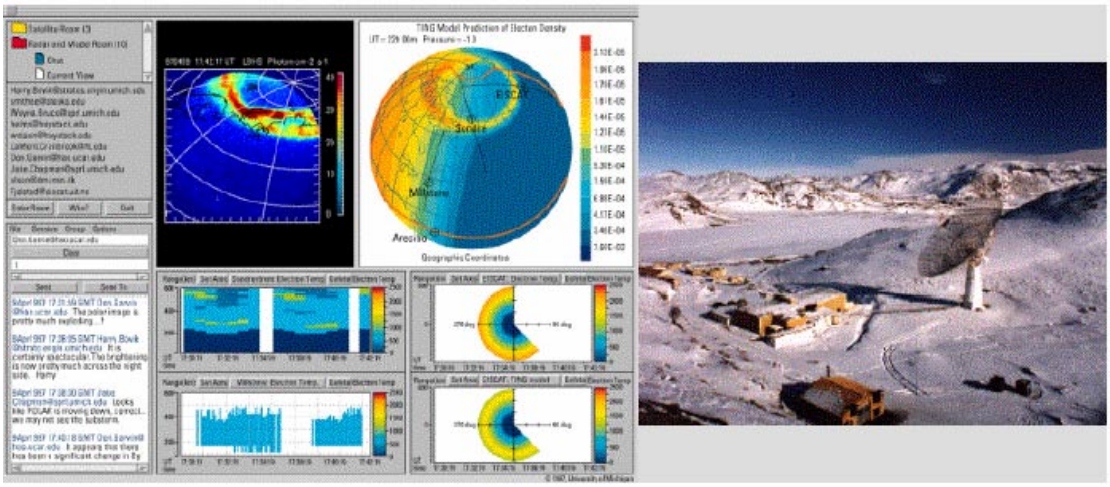


**Figura. 3.8.4. Laboratorios Virtuales**

Es importante mencionar que aun deben surgir nuevas aplicaciones, mas sofisticadas, que aprovecharán de mejor manera toda la capacidad del Internet IP-V6.

Quizás las más apasionadas posibilidades son las que aún no imaginamos, pero que se desarrollarán durante la vida de IP-V6.

Los esfuerzos de desarrollo de red para crear una nueva generación de Internet en ANDINANET S.A. donde existan aplicaciones que exploten totalmente las capacidades de las redes de gran ancho de banda como integración de medios, interactividad, colaboración en tiempo real.

# CAPÍTULO IV

# INTERACCIONES ENTRE IP-V4 E IP-V6, IMPLEMENTACIÓN Y CONFIGURACIÓN IP-V6

## 4.1. INTRODUCCIÓN

Para ANDINANET S.A. migrar al sistema IP-V6 en un simple proceso seria muy difícil, en contraste se hace necesario desarrollar estrategias para que IP-V4 coexista con IP-V6. Este capitulo esta orientado ha desarrollar el estudio para que IP-V4 e IP-V6 puedan coexistir entre sí. Para la interacción entre IP-V4 e IP-V6 actualmente existen dos mecanismos; Una ley Dual IP, y por Entubamiento.

Este capitulo también tiene por objetivo mostrar el mundo de las nuevas tecnologías como son ATM e IP-V6 siempre muy unidas. Mediante ellas el mundo de la información a adoptado una nueva dimensión en cuanto a la capacidad y fiabilidad de la transmisión de información con ATM y en cuanto al aumento de números de usuarios y facilidad de uso con el protocolo de la próxima generación IP-V6.

La implementación de IP-V6 sobre IP-V4 implica una modificación de Computadores, Routers (Sistemas Encaminadores) e, incluso en las aplicaciones, en una interacción que no será sencilla; no obstante lo cual el usuario no tendrá que cambiar su direccionamiento de correo electrónico o el URL de un Servicio de Información Web, puesto que los cambios se producen a nivel de los dominios del sistema que actualmente tiene ANDINANET S.A..

Cualquier aplicación que corre sobre IP-V4 puede operar sobre IP-V6. Sin embargo, IP-V6 permite a través de su espacio de direcciones infinito un despliegue masivo del mercado de aplicaciones y dispositivos IP no tradicionales. Esto incluye

dispositivos electrónicos de consumo como DVD players, TVs, Cámaras Digitales y equipo residencial de telefonía IP (video conferencia).

Debido a que todas las aplicaciones de Internet deberían de correr de manera transparente en IP-V4 e IP-V6, los usuarios finales no verán ninguna diferencia. Sin embargo, en la medida en que las nuevas aplicaciones u dispositivos que corren en IP-V6 estén disponibles, el usuario final será capaz de expandir la cantidad de aplicaciones y dispositivos que usa sobre Internet. En el futuro, ANDINANET S.A. espera que los clientes reciba direcciones IP oficiales, como el número de teléfono de un hogar o la dirección de una calle. Estas direcciones permanentes ofrecerán conectividad constante a Internet, además de eliminar el proceso actual de asegurar una dirección temporal de Internet cada vez que el usuario accede a la red. Se espera que estas direcciones IP permanentes soporten mas fácilmente aplicaciones como juegos distribuidos y telefonía IP, Fax y Video, así como abrir una variedad de nuevos mercados y aplicaciones innovadoras.

La forma más directa para poder realizar la interacción para los nodos IP-V6 de ser compatibles con nodos IP-V4 es proveyendo una implementación completa de IP-V4. Los nodos IP-V6 que proveen una implementación completa de IP-V4 son llamados como nodos “IP-V4/IP-V6”. Estos nodos tienen la habilidad de enviar y recibir paquetes IP-V6 e IP-V4, pudiendo así interpolar directamente con nodos IP-V4, y también operar con nodos IP-V6 usando paquetes IP-V6.

El primer paso hacia la migración del protocolo IP-V6 es la interacción entre los dos protocolos IP-V4 e IP-V6. La nueva versión del Protocolo de Internet sustituirá progresivamente a IP-V4, ya que brinda mejores características entre las que se destacan: espacio de direcciones prácticamente infinito, posibilidad de autoconfiguración de computadoras y ruteadores; soporte para seguridad, computación móvil , calidad de servicios, un mejor diseño para el transporte de tráfico multimedia en tiempo real, aplicaciones anycast y multicast; así como la posibilidad de transición gradual de IP-V4 a IP-V6.

## 4.2. INTERACCIÓN ENTRE IP-V4 E IP-V6

Para poder realizar la interacción entre los dos protocolos, primero pensemos en los posibles escenarios en los que se podría llegar a utilizar un traductor de direcciones IP-V6/IP-V4 para lidiar con el problema de la incompatibilidad de protocolos a la hora de hacer una migración hacia la nueva versión del protocolo IP. Existen dos posibles escenarios en donde la traducción de direcciones y protocolos puede ser utilizada:

- ✓ Una red IP-V6 comunicándose con nodos en una red IP-V4. Por ejemplo, una red completamente nueva con nuevos equipos que solo manejan IP-V6 y que necesiten comunicarse con otros nodos que se encuentran en la red IP-V4 o en Internet.
- ✓ Una red IP-V4 comunicándose con nodos de una red IP-V6. Por ejemplo, actualizar toda una red IP-V4 a IP-V6 nodo por nodo necesita que servicios críticos como Web, correo, compartir impresoras o archivos, puedan ser accesibles para todos los nodos, manejen IP-V4 o IP-V6

A partir de estos dos puntos importantes se plantea como una solución a implementarse en futuro en ANDINANET S.A., la interacción de los dos protocolos. Para que puedan coexistir e interaccionar estos dos protocolos actualmente hay dos mecanismos:

1. Una Ley Dual IP, haciendo un túnel de IP-V6 sobre IP-V4.
2. Entubamiento

### 4.2.1. LEYES DE IP DUAL

El mecanismo para que IP-V4 e IP-V6 coexistan, es que el snack de ambos protocolos sean implementados en un mismo dispositivo (Router, Pc o Servidor), el cual esta referido como un nodo IP-V6/IP-V4.

El nodo IP-V6/IP-V4 tiene la capacidad de enviar y recibir ambos tipos de paquetes IP-V4 e IP-V6 y puede interoperar con un dispositivo IP-V4 y con un dispositivo IP-V6 usando paquetes IP-V6. El nodo IP-V6/IP-V4 puede ser

configurado con direcciones soportadas en ambos protocolos, como un protocolo de configuración dinámica (DHCP), conjuntamente con un protocolo de inicio (BOOTP) y el sistema de Nombre de Dominio (DNS), los cuales deben ser involucrados en este proceso. Ver figura 4.2.1..

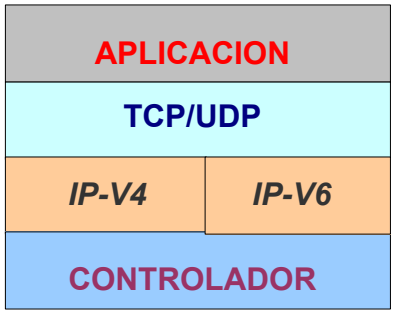



**Figura. 4.2.1. Ley de IP Dual**

### 4.2.2. ENTUBAMIENTO

Entubamiento es el proceso por el cual la información de un protocolo es encapsulado dentro del Frame de otro protocolo o sistema, poniendo disponible la data original para ser cargada sobre el otro protocolo. Los escenarios para entubar IP-V6/IP-V4 fueron designados para poder utilizar la infraestructura existente de IP-V4 para que cargue paquetes IP-V6 encapsulado la información IP-V6 dentro del paquete IP-V4.

Del Proceso de encapsulamiento resulta un paquete IP-V4 que contiene ambos encabezados de IP-V6 y el de IP-V4. El encapsulamiento incluye tres pasos:

- ✓ Encapsulamiento,
- ✓ Desencapsulamiento y
- ✓ Manejo de Túnel o Tubo

En el nodo encapsulador (emisor o punto de entrada del túnel) el encabezado IP-V4 es creado y encapsulado el paquete a transmitir, en el nodo desencapsulador (receptor o salida del túnel) el encabezado IP-V4 es removido y el paquete IP-V6 es procesado. En adición el nodo encapsulador puede mantener la

información de configuración considerando el túnel establecido con un máximo tamaño de unidad de referencia soportada por el túnel (MTU).

RFC-1993 definió cuatro posibles configuraciones de Túneles que pueden ser establecidos entre routers y equipos:

- ✓ Routers a Routers: Routers IP-V6/IP-V4 que están separados por una infraestructura IP-V4 con un túnel IP-V6 entre ellos mismos, en este caso el túnel puede ser colocado sobre un segmento del camino end to end del paquete.
- ✓ Host a Router: Un Host IP-V6/IP-V4 hace un túnel de un paquete IP-V6 hacia un Router IP-V6/IP-V4 en el cual es alcanzable por una infraestructura IP-V4, en este el túnel se puede colocar en el primer segmento del camino end to end del paquete.
- ✓ Host a Host: Un Host IP-V6/IP-V4 que esta interconectado por una infraestructura puede hacer un túnel del paquete IP-V6 a través de la infraestructura IP-V4 en este caso, el Túnel se coloca en el camino entero end to end del paquete.
- ✓ Router a Host: Un Router IP-V6/IP-V4 puede entregar paquetes IP-V6 para un equipo IP-V6/IP-V4 el cual es el destino final. En este caso el túnel se deberá colocar al final del segmento del camino end to end del paquete.

Para que un túnel este operativo, las direcciones de ambos extremos del túnel y los destinos del paquete deben ser conocidos, y estas dos direcciones no necesariamente son las mismas, la manera en la cual la dirección al final del túnel es determinada define los tipos de túneles, que pueden ser automático o configurado.

IP-V6 de punto a punto necesitará tunelización a través de redes IP-V4 hasta que los proveedores de servicios construyan principales IP-V6 y ofrezcan servicios IP-V6. Esto se lleva a cabo encapsulando un paquete IP-V6 a la carga útil de un paquete IP-V4. Un nodo IP-V6 origina los paquetes IP-V6, que son encapsulados en IP-V4 y enviados por la red IP-V4. El nodo al final del túnel desconecta el

paquete IP-V4, exponiendo el paquete IP-V6 para la entrega al nodo de destinación. Ver figura 4.2.2..

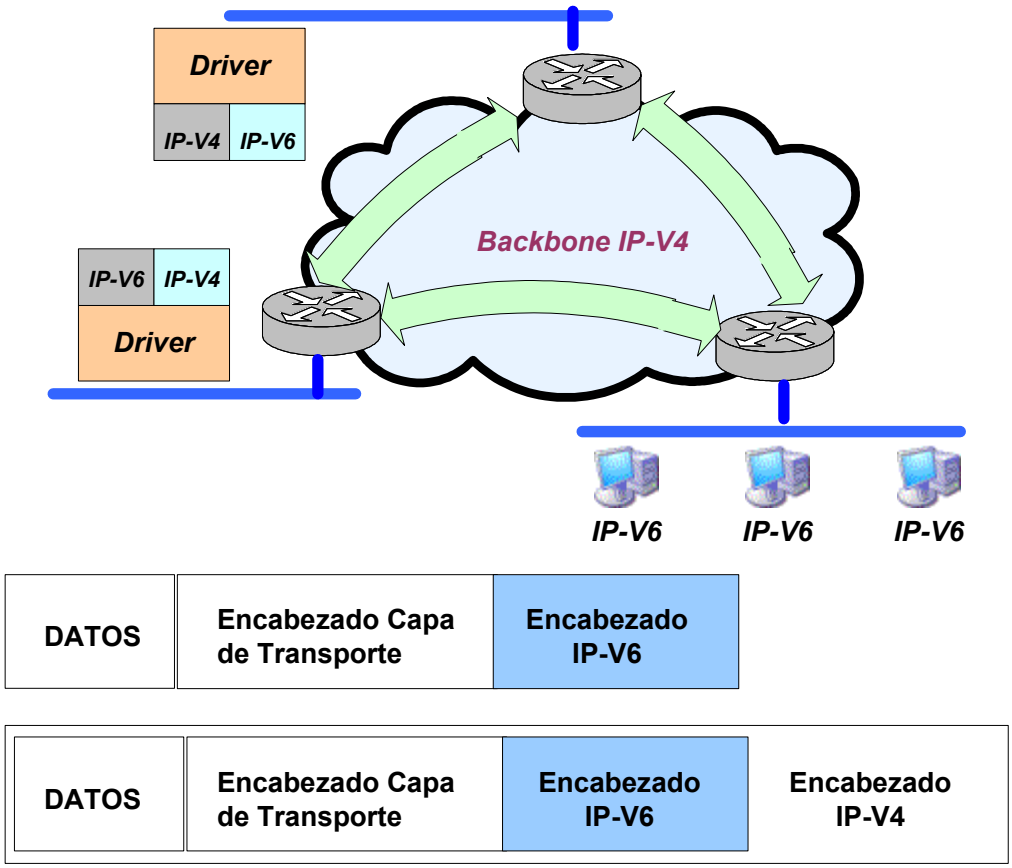



**Figura. 4.2.2. Entubamiento**

## 4.3. IMPLEMENTACIÓN Y CONFIGURACIÓN IP-V6

### 4.3.1. IMPLEMENTACIONES DE IP-V6

A continuación se describen las características necesarias para la implementación de IP-V6 sobre IP-V4:

- ✓ BSD (FreeBSD 4.0, KAME, NRL's IP-V6, IP-V6 DRET)
- ✓ COMPAQ (Tru64, OpenVMS)
- ✓ FTP/NetManage (OnNet Host Suite)
- ✓ HITACHI (Toolnet6, GR2000 Gigabit Router, NR60 Router)
- ✓ HP (HP/UX 11.0)
- ✓ IBM (AIX 4.3, OS/390)

- ✓ Integrated Systems Inc (ISI) (IP-V6 in embedded systems)
- ✓ LINUX (IP-V6 How To, Debian IP-V6 Project, Linux IP-V6 RPM Project)
- ✓ MICROSOFT (Windows NT stack MSR 1.1 – 1.4, Windows 2000)
- ✓ MENTAT (Mentat TCP)
- ✓ SCO (UnixWare 7)
- ✓ SUN (Solaris 2.5, Solaris 7, Solaris 8)
- ✓ TRUMPET (Winsock 5.0)
- ✓ 3Com (NetBuilder, PathBuilder)
- ✓ CISCO (c1000, c1005, c1600, c2500, c2600, c3620, c3660, c4000, c4500, c5200, c7200, c5rsm)
- ✓ ERICSSON TELEBIT (Router RXI 820)
- ✓ GateD CONSORTIUM (GateD 1.0)
- ✓ Multi-threaded Routing Toolkit (MRT) (MRT 2.2.0A)
- ✓ NORTEL Networks (ARN, ASN, BLN, Passport 2430 y 5430)
- ✓ SUMITOMO (Suminet 3700)
- ✓ THOMSON CSF Detexis
- ✓ ZEBRA (Zebra 0.84)

### 4.3.2. CONFIGURACIONES DE IP-V6

Dentro de las configuraciones de IP-V6 se las destaca en computadores y en ruteadores:

- ✓ IP-V6 en Windows NT 4.0 y 2000
- ✓ IP-V6 en Solaris 2.5 – 8
- ✓ IP-V6 en Linux RedHat
- ✓ IP-V6 en ruteadores 3Com
- ✓ IP-V6 en ruteadores Nortel
- ✓ IP-V6 en ruteadores Cisco.

### 4.3.2.1. IP-V6 EN COMPUTADORAS

Para los diferentes sistemas operativos que existen se han elaborado nuevas versiones, versiones que permiten soportar IP-V6. Dentro de estos sistemas operativos tenemos los siguientes que en la actualidad ya tienen la capacidad de permitir realizar sus configuraciones de IP-V6:

- ✓ ***En WINDOWS***
  - o Stack MSR IP-V6 ver. 1.4, para Win NT 4.0 y SP 4
  - o Windows 2000 preview version, para Win 2000

La instalación de IP-V6 en Windows NT se la realice de la siguiente forma: Ver figura 4.3.2.1(a).


**Figura. 4.3.2.1. (a). Configuración en Windows de IP-V6**

Dentro de las características del MRS IP-V6 r1.4 se tiene:

- Se puede iniciar o detener el Snack sin reiniciar
- Soporte para APIs (Interfaz de programación de aplicaciones)
- Protocolo Parser IP-V6 (monitoreo de paquetes)
- Traductor IP-V6/IP-V4
- No tiene soporte para Encriptación y Movilidad

#### 4.3.2.1.1. COMANDOS IP-V6 EN WINDOWS NT

- ✓ ipv6 if
- ✓ ipv6 adu
- ✓ ipv6 nc
- ✓ ipv6 rc
- ✓ ipv6 bc
- ✓ ipv6 spt
- ✓ ipv6 rt
- ✓ ipv6 spu
- ✓ ipv6 rtu
- ✓ ping6
- ✓ tracert6
- ✓ ttcp
- ✓ 6to4cfg
- ✓ Net: Inicia o Detiene el stack IP-V6 (net stop tcpip6 – net start tcpip6)

#### 4.3.2.1.2. CONFIGURACIÓN DE TÚNELES

Para la configuración de un túnel de IP-V6 sobre IP-V4 se debe realizar los siguientes pasos:

1. Configurar la dirección IP-V4 remota del túnel (ipv6 rtu ::/0 2/::"dir IP-V4 Destino" pub)

2. Configurar la dirección IP-V6 local de la interfaz (ipv6 adu 2/dir IP-V6 Origen)

✓ ***En WINDOWS 2000***

- Snack MSR IP-V6 ver 1.4
- IP-V6 Technology Preview (marzo 2000) (No funciona con versions Beta – Inicia o Detiene el stack IP-V6 (net stop tcpip6 –net Stara tcpip6))

Las características del IP-V6 Technology Preview son las siguientes:

- Se puede iniciar o detener el stack sin reiniciar
- Soporte para APIs
- Configuración automatica bajo 6to4
- Direccionamiento Local (Intranets)
- No soporta direcciones IP-V4 mapeadas

✓ ***En SUN***

- Solaris 2.5
- Solaris 7
- Solaris 8

✓ ***INSTALACIÓN SOLARIS 2.5 - 2.5.1***

Para la configuración de IP-V6 en Solaris 2.5 - 2.5.1 se procede de la siguiente forma para la instalación:

- Versión de Solaris 2.5 o 2.5.1 sin parches
- Bajar el parche IP-V6
- Descomprimirlo e instalarlo
- Ejecutar /usr/ipv6/etc/conf_ipv6
- Reiniciar el equipo.

Para el sistema Solaris se tienen algunos módulos del Kernel como:

- /kernel/drv/ip
- kernel/drv/tcp
- kernel/drv/udp
- kernel/drv/icmp

Así mismo se tienen algunos comandos para Solaris agregados como:

- /kernel/drv/atun → Driver para túneles
- /usr/ipv6/sbin → Para IP-V4/IP-V6
- usr/ipv6/bin

El sistema Solaris permite aplicar las siguientes aplicaciones para IP-V6:

- ifconfig
- telenet/in.telnetd
- ping
- snoop
- route
- rdist
- rlogin/in.rlogind
- rsh/in.rshd
- tftp/in.tftpd
- inetd
- traceroute
- netstat
- finger/in.fingerd
- mconnect
- sendmail
- DNS

- Rcp
- RIPng

✓ ***INSTALACIÓN SOLARIS 7***

Para la instalación del sistema Solaris 7 se deben considerar los siguientes puntos:

- Versión FCS de Solaris 7, es decir; aquella que no tiene parches
- Contar 25 MB (Sparc) o 11MB (x86)
- Instalar el paquete: 107788-01 (Sparc) / 107916-01 (x86)
- Reiniciar el equipo
- Crear /etc/hostname6<interface>

Igual que el sistema Solaris 2.5, el sistema Solaris 7 presenta las siguientes aplicaciones para IP-V6:

- Ifconfig
- Ping
- telnet/in.telnetd
- snoop
- rdist
- route
- traceroute
- rlogin/in.rlogind
- netstat
- rsh/in.rshd
- tftp/in.tftpd
- inetd
- rcp
- finger/in.fingerd
- mconnect

- sendmail
- DNS

A diferencia del sistema Solaris 2.5, el sistema Solaris 7 permite tener Servicios de Nombres como:

- NIS
- NIS+
- DNS
- /etc/inet/ipnodes
- /etc/nswitch.conf
- /etc/hostname6.*
- /etc/hostname6.ip.t

✓ ***INSTALACIÓN SOLARIS 8***

El sistema Solaris 8 es diferente a los sistemas Solaris antes presentados 2.5 – 7. La instalación del sistema Solaris 8 para IP-V6 presenta un ambiente gráfico. Ver figura 4.3.2.1(b)

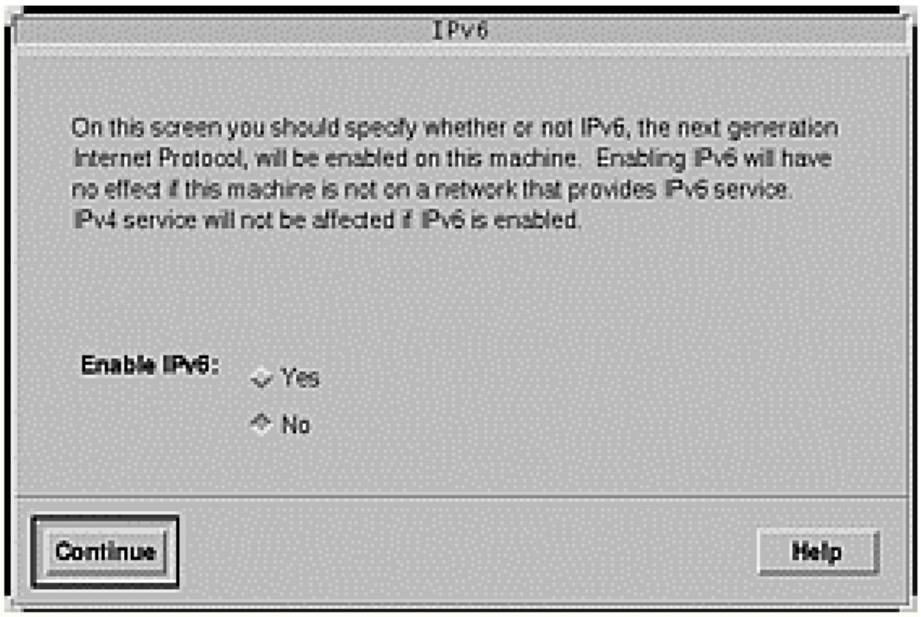



**Figura. 4.3.2.1. (b). Instalacion Sistema Solaris 8**

Igual que el sistema Solaris 7, el sistema Solaris 8 presenta las siguientes aplicaciones para IP-V6:

- Ifconfig
- Ping
- telnet/in.telnetd
- snoop
- rdist
- route
- traceroute
- rlogin/in.rlogind
- netstat
- rsh/in.rshd
- tftp/in.tftpd
- inetd
- rcp
- finger/in.fingerd
- mconnect
- sendmail
- DNS

El sistema Solaris 8 también permite tener Servicios de Nombres como:

- NIS
- NIS+
- DNS
- Getent
- In.named
- nslookup

El sistema Solaris 8 permite la configuración de un túnel de IP-V6 sobre IP-V4, los pasos para poder realizar esta configuración son los siguientes:

1. Configurar las direcciones IP-V4 fuente y destino tsrc "dir.IP-V4 Origen" tdst "dir.IP-V4 Destino" up.
2. Agregar una interfaz lógica para las direcciones IP-V6 addif "dir.IP-V6 Origen" "dir.IP-V6 Destino" up.

El sistema Solaris 8 igual que los sistemas anteriores presenta los siguientes Archivos de configuración:

- hostname6.hme0
- /etc/hostname6.ip.tun#
- /etc/inet/ndpd.conf

✓ ***En LINUX***

- RedHat

Para el sistema LINUX para poder realizar la instalación del mismo se debe verificar los siguientes puntos:

- Versión RedHat 6.0 o superior
- Contar un Kernel 2.2.x
- Compilar el Kernel
- Configurar el LILO
- Reiniciar la computadora

Al momento de realizar la compilación del Kernel se debe tomar en cuenta en las opciones de RedHat activar o verificar:

- Packet socket
- Unix domain sockets
- The IP-V6 protocol
- IP-V6: enable EUI-64 token format
- IP-V6: disable provider based address.

Si se actualice el Kernel, no se debe remover el anterior.

El sistema LINUX también permite la creación de Túneles en donde la configuración que se realiza del túnel es de IP-V6 sobre IP-V4 tomando en cuenta los siguientes pasos:

1. Configurar la dirección IP-V4 remóta en el túnel: tunnel "dir. IP-V4 Destino"
2. Configurar la dirección IP-V6 local de la interfaz: add "dir. IP-V6 Origen" / "prefijo".

#### 4.3.2.2. IP-V6 EN RUTEADORES

Los ruteadores desempeñan un papel muy importante en un ISP, permiten la interconexión entre el usuario, el ISP y el mundo del Internet. Los diferentes proveedores han realizado nuevas versiones de software que permite soportar IP-V6:

- ✓ ***EN 3Com:***

  - NetBuilderII
  - PathBuilder S500

Para los ruteadores 3Com el sistema operativo debe ser:

  - Enterprise OS Software 11 – 11.3E y 11.4

En este tipo de ruteadores la habilitación de IP-V6 se la debe realizar por Menús o por Comandos:

1. En un puerto: (setdefault ¡puerto –ipv6 control=route)
2. Configuración de una dirección IP-V6 estática (add ¡puerto –ipv6 netaddr dir.IP-V6)

Así mismo para la configuración de Túneles en ruteadores 3Com se debe realizar la configuración de un túnel de IP-V6 sobre IP-V4:

1. Configurar interfaz, túnel (setd ¡puerto –ipv6 tunnel= "dir. IP-V4 Ori." "dir. IP-V4 Dest."
2. Asignar una dirección IP-V6 al puerto (setd !puerto – ipv6 control=route ) (add ¡puerto –ipv6 netaddr "dir. IP-V6")

Los ruteadores 3Com también permiten el manejo de Otros Comandos como:

- Añadir o borrar una ruta estática
  - ✓ add ¡puerto –ipv6 route dir.IP-V6 [<gateway>]<metríca>
  - ✓ delete –ipv6 route dir.IP-V6 [<gateway>]
- Utilizar del protocolo "Neighbor Discovery"
  - ✓ Set ¡puerto –ipv6 NbrDiscovery = ([Valores])
- Otros Comandos que se pueden emplear para los ruteadores 3Com son:
  - ✓ ipv6 ping "dirección IP-V6"
  - ✓ ipv6 traceroute6 "dirección IP-V6"
  - ✓ show –ipv6 address
  - ✓ show –ipv6 conf
  - ✓ show –ipv6 allroute
  - ✓ show –ipv6 tunnel
  - ✓ show –sys statistics –ipv6 | -bgp | -ripng

✓ ***EN NORTEL:***

Dentro de los ruteadores Bay Networks que presenta Nortel tenemos:

- ARN, ASN, BLN
- Passport 2430 y 5430

Los ruteadores Nortel igual que los 3Com presenta su propio sistema operativo el mismo BayRS Release 12 –13.20. Adficional a su sistema operativo cuenta con un Site Manager, GUI para configuración.

Otra característica importante que presentan los ruteadores NORTEL es la Habilitación de IP-V6 Globalmente y En una interfaz:

1. Globalmente:
   - ✓ Configuration Manager
     - Protocols
     - IP-V6
     - IP-V6 Global Enable
2. En una interfaz
   - ✓ Configuration Manager
     - Protocols
     - IP-V6
     - Edit IP-V6 Interfaces Enable

Una de las características principales de este tipo de ruteadores es permitir la configuración de un túnel de IP-V6 sobre IP-V4 bajo los siguientes puntos:

1. Configurar interfaz, tunel y token (Protocols > IP-V6 > Interfaces > Add Túnel)
2. Configurar Prefijo (Protocols > IP-V6 > Prefix)

- ***EN CISCO:***

  - c1000 – c1005 – c1600 – c2500 – c2600 – c3620 – c3660 – c4000 – c4500 – c5200 – c7200 – c5rsm

Los ruteadores CISCO es uno de los mas empleados por ANDINANET S.A. CISCO al igual que los ruteadores antes estudiados presenta su propio sistema operativo:

  - 11.3(5)T
  - 12.0T

Así mismo los ruteadores CISCO permiten habilitar IP-V6 bajo los siguientes parámetros:

  - Habilitación de IP-V6 en una interfase (ipv6 enable)
  - Configuración de una dirección IP-V6 en una interfase (ipv6 address prefijo/long-prefijo EUI-64)
  - Configuración del protocolo “Neighbor Discovery” (ipv6 nd aviso de prefijo >prefijo de ruteo>/<long><tiempo de vida>[onlink | autoconfig]

ANDINANET S.A. cuenta como uno de sus ruteadores principales un CISCO de la Serie 7000, el mismo que permite la configuración de un túnel de IP-V6 sobre IP-V4 empleando los siguientes comandos:

  - host(config)#interface tunnel 1
  - host(config-if)#description TUNEL 1
  - host(config-if)#tunnel source ethernet 0/1
  - host(config-if)#tunnel destination dd.dd.dd.dd
  - host(config-if)#no ip address
  - host(config-if)#ipv6 address ee:ee:ee:ee:ee:ee:ee:ee/p
  - host(config-if)#tun mode ipv6ip

Dentro de otros comandos empleados en la configuración de ruteadores CISCO son:

- ping ipv6 “dirección IP-V6”
- traceroute ipv6 “dirección IP-V6”
- show ipv6 tunnel
- show ipv6 interface
- show ipv6 route
- show ipv6 bgp

Los ruteadores CISCO tiene una característica principal en comparación con los antes mencionados ya que permite la configuración de RIPng. Para este tipo de configuración se debe considerar los siguientes comandos:

- ipv6 rip <tag> enable
- ipv6 rip <tag> summary-address <prefijo>/<long.>
- ipv6 rip <tag> filtro in|filtro out <nombre>
- ipv6 rip <tag> redistribute static

Así mismo ANDINANET S.A. actualmente en sus configuraciones principales para dar servicio IP-V4 tiene configurado en sus ruteadores principales el protocolo BGP, de la misma forma para poder dar servicio de IP-V6 este tipo de ruteadores permite la configuración del protocolo BGP+ que es empleado por IP-V6. Para la configuración de este protocolo se deben considerar los siguientes puntos:

- Definición de un vecino: (ipv6 bgp neighbor dir. IP-V6 remore-as <#sis.auto.>)
- Filtración de las actualizaciones recibidas: (ipv6 bgp neighbor dir. IP-V6 route-map <nombre> in)
- Filtración de las actualizaciones enviadas : ipv6 bgp neighbor dir. IP-v6 route-map <nombre> out

Para poder brindar el servicio de IP-V6 ANDINANET S.A. no tendrá que realizar una inversión costosa en ruteadores, ya que cuenta con ruteadores CISCO. Lo único que se debe realizar es la actualización en la configuración del sistema operativo para que permita soportar IP-V6 sobre IP-V4 ganando así direccionamiento IP para la masificación de clientes.

Para establecer la conectividad IP-V6 desde una de las maquinas de la red. Debe tener la interfaz del túnel (sit1) la misma que funcionará de router para la red LAN. Una de las grandes ventajas que tiene IP-V6 es la gran cantidad de direcciones que se pueden conseguir, lo cual hace recurrir al NAT, y se puede dar una dirección de ámbito publico a cada uno de los nodos de la red LAN. Si a esto se une la gran ventaja de la autoconfiguración que incluye IP-V6 hace que se requiera de DHCP para asignar direcciones IP-V6 validas a los nodos de la red.

Esto se lo puede hacer por medio de un RAD (Router Advertisement Daemon), se trata de un daemon que envía periódicamente Anuncios de Router (RA) a los nodos de la red.

## 4.4. APLICACIONES EN IP-V6

- ✓ Chat
  - o IRC: cliente BitchX
  - o RAT y SDR

- ✓ Correo

Exim

  - o Qmail
  - o Public Sendmail
  - o WIDE Sendmail

- ✓ DNS
  - o BIND 9 Beta 2
  - o Totd

- ✓ Firewalls
  - o ipfilter
  - o IPFW

- ✓ FTP
  - o LFTP
  - o NcFTP (Windows)
  - o NcFTP (BSD)

- ✓ Java
  - o IP-V6 Java (Windows)

- ✓ Herramientas de Monitores
  - o ASPath-tree
  - o Link View

- ✓ Noticias
  - o INN v2.2.2
  - o Mnews

- ✓ Parches
  - o Linux
  - o KAME
  - o WIDE

- ✓ Software para Sockets
  - o IP-V6 socket 1.1
  - o Trumpet winsock

- ✓ Traductor IP-V6/IP-V4
  - o Toolnet6
  - o Traductor IP-V6/IP-V4 (Windows)

- ✓ Para Túneles

- BT Ultima IP-V6 Access
- CSELT Tunnel Broker
- V6tun

✓ WWW

- Apache (Linux)
- Apache (BSD)
- Fnord (Windows)
- lynx v2.8.2
- mini_hhtpd
- Mozilla

Aunque pocos, (quizá un 1%) hay servidores en Internet que permiten conexión a través de IP-V6. Uno de ellos es el que alberga la pagina web del diario El Mundo, pero hay muchos otros mas. Ver figura 4.4(a).

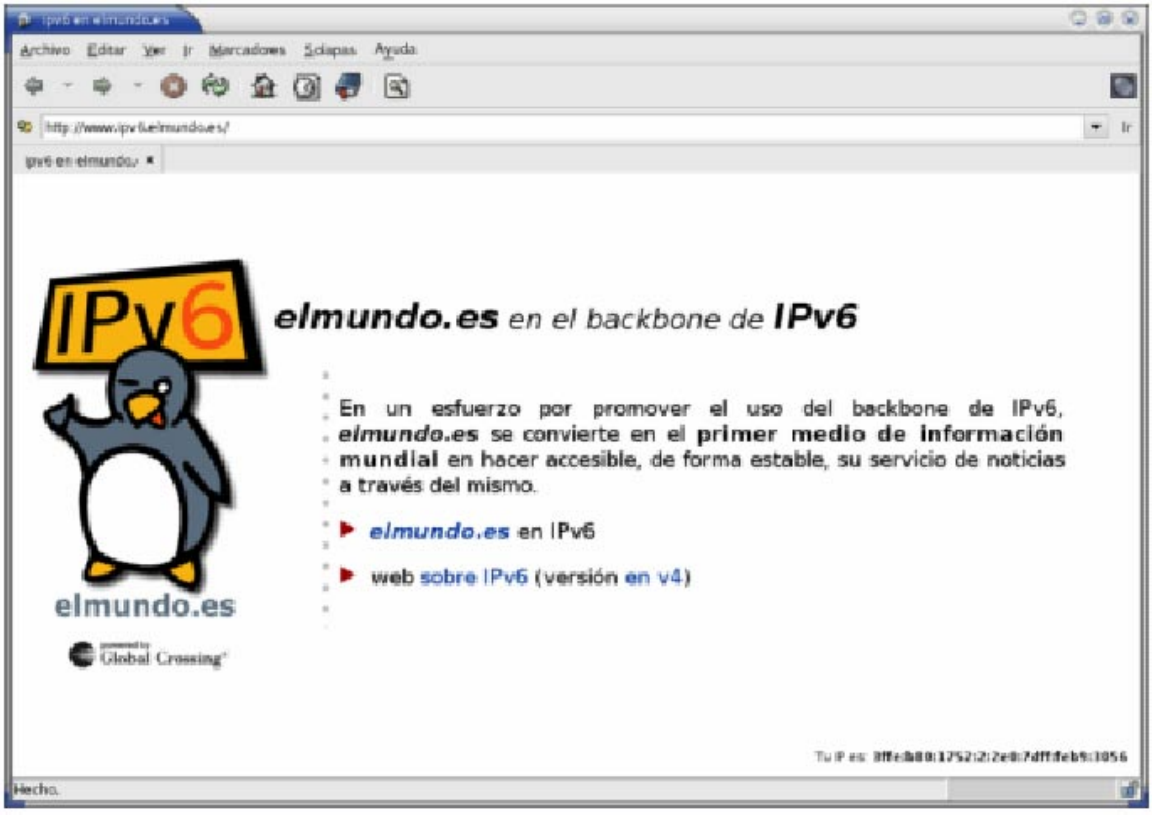



**Figura. 4.4. (a). Navegador WEB**

✓ Juegos

- Quakeforge

✓ Analizador de Protocolos

- Link View (Reconoce paquetes IP-V6)

Uno de las aplicaciones mas empleadas por ANDINANET S.A. y por los clientes es el comando de traceroute, para el cual al momento de verificar la conectividad del cliente con una conexión IP-V6 se vería como se muestra en la figura 4.4.(b):

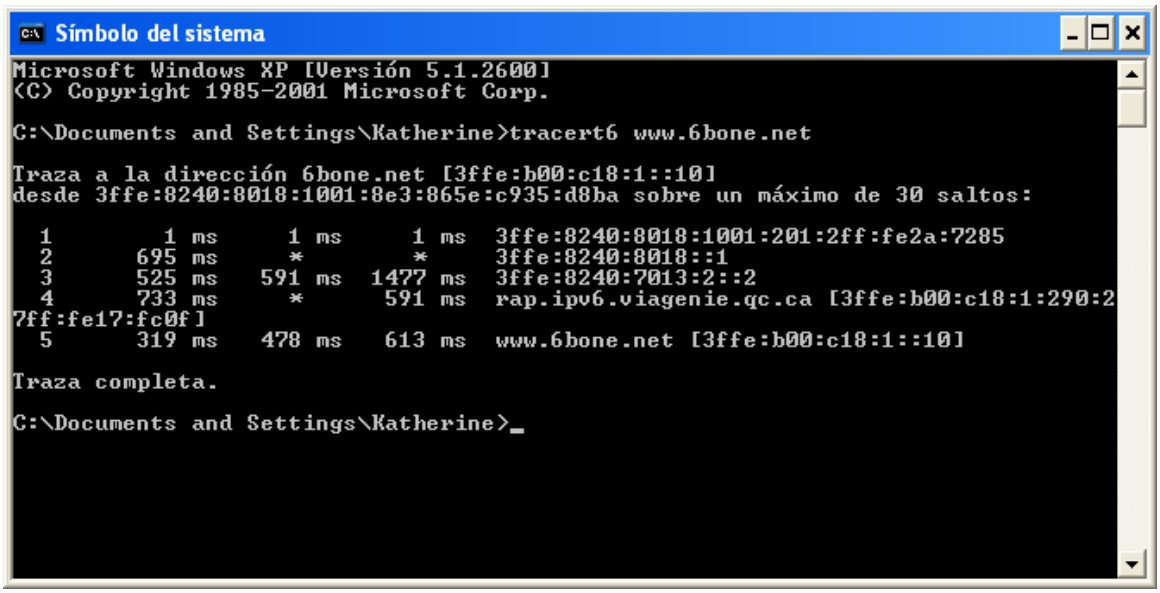



**Figura. 4.4. (b). Monitoreo mediante comando traceroute6**

# CAPÍTULO V

# ANÁLISIS DE COSTOS Y BENEFICIOS

## 5.1. INTRODUCCIÓN

Aquella primera "Internet" fundada, sobre todo, con fines de investigación científico-técnicos y con objetivos militares, ya no se parece en nada a la actual. Hoy, al hablar de Internet, nos referimos a una estructura de red que es la columna vertebral de las comunicaciones, una herramienta imprescindible en el mundo científico-técnico, empresarial y gubernamental.

Cuando IP-V4 se estandarizó, nadie pudo imaginar que se convertiría en lo que es hoy: una arquitectura de cobertura mundial, con un número de usuarios superior al centenar de millones y con una tasa de crecimiento exponencial.

El nacimiento del nuevo protocolo IP-V6, no ha venido solo propiciado por la escasez de direcciones IP-V4 en la actualidad, sino que además se añaden nuevas características y se mejoran las existentes. En principio la migración de IP-V4 a IP-V6 es costoso, razón por la cual uno de los primeros pasos que ANDINANET S.A. debe realizar es que los dos protocolos IP-V4 e IP-V6 vayan juntos de la mano, teniendo así costos mas bajos, de aquí las ventajas que aporta el nuevo protocolo, permitir amortizar la inversión en poco tiempo.

El beneficio derivado de un nuevo protocolo debe ser balanceado por el costo asociado al realizar la transición del sistema actual.

Sin embargo y pese a que la versión mejorada del protocolo de Internet, está completamente desarrollada y dispuesta para su utilización, aspectos comerciales

hacen que ésta no sea una realidad inmediata. "La tecnología está preparada" pero, lastimosamente, los aspectos comerciales hasta ahora han pesado más.

Los grandes fabricantes no han ayudado mucho a que IP-V6 se implante porque comercialmente aún había mucho que vender con IP-V4, muchos productos, servicios, aplicaciones y protocolos que no eran precisos con IP-V6.

Afortunadamente, ANDINANET S.A. ha empezado a dar un importante giro con el estudio para su migración de protocolo y seguir siendo el proveedor líder de Internet en el Ecuador y llegar a ser uno de los primeros en proveer servicios de Internet sobre IP-V6 a nivel de Latinoamérica.

Todo apunta, por tanto, a que la plena adopción de IP-V6 no se hará de esperar demasiado, permitiendo así la calidad y seguridad necesarias que conviertan a IP en el protocolo de las redes del futuro. La tecnología IP hará realidad la convergencia de voz, datos y contenidos multimedia en una misma red, que ofrecerá nuevos y más completos servicios.

## 5.2. PLATAFORMA DE ANDINANET

En la actualidad ANDINANET S.A. cuenta con una plataforma nueva con la capacidad de poder proveer los servicios de Internet a nivel Nacional. Gracias a que ANDINANET S.A. cuenta con esta nueva plataforma los costos de inversión para la implementación de IP-V6 no tendría un costo elevado ya que cuenta con RTU's Cisco.

Los tipos de RTU's que tiene ANDINANET son de los siguientes modelos:

- ✓ 3 RTU's Cisco 7513
- ✓ 1 RTU Cisco 7507

Los RTU's antes nombrados tienen un IOS que permite soportar IP-V4. Para la implementación de IP-V6 sobre IP-V4 ANDINANET S.A. seguirá

manteniendo sus propios equipos y el único cambio que se hará es la versión del IOS. El IOS que mantienen estos equipos es el siguiente:

- ✓ Cisco 7513 (Denominado como Router DS-3): rsp-isv-mz.122-16c.bin.
- ✓ Cisco 7513 (Denominado como Router Q1): rsp-isv-mz.122-16c.bin
- ✓ Cisco 7507 ( Denominado como Router de PROVINCIAS y CLIENTES): rsp-isv-mz.121-5.T10.bin
- ✓ Cisco 7513 (Denominado como Router ANDINADATOS): rsp-isv-mz.121-5.T10.bin

Básicamente a todos estos RTU's los podemos considerar como el cerebro principal de ANDINANET S.A., ya que en ellos se encuentra la configuración y el enrutamiento para que cada uno de los nodos y clientes tenga acceso al servicio de Internet bajo el protocolo IP-V4

En cuanto a sus DSLAM, ANDINANET S.A. no necesita hacer ninguna migración. La conexión física y la adecuación de la LP sigue siendo la misma.

Una vez que se adquiera la nueva versión de IOS, ANDINANET S.A., debe también realizar un cambio en sus equipos que desempeñan la función de servidores. En la actualidad ANDINANET S.A. cuenta con varios servidores de diferentes características y con una función diferente, estos son:

- ✓ DELL POWEREDGE 2650 Intel(R) Xeon(TM). (Denominado PICHINCHA.ANDINANET.NET), bajo tecnología LINUX y su función es ser ***DNS Primario***.
- ✓ DELL POWEREDGE 2650 Intel(R) Xeon(TM). (Denominado TUNGURAHUA.ANDINANET.NET), bajo tecnología LINUX y su función es ser ***DNS Secundario***.
- ✓ DELL POWEREDGE 2650 Intel(R) Xeon(TM). (Denominado QUILOTOA.ANDINANET.NET), bajo tecnología LINUX y su función es ser ***DNS Tercero***.

- ✓ COMPAQ PROLIANT ML350 Intel(R) Pentium(R) III. (Denominado WEBMAIL.ZONA-ANDINA.NET), bajo tecnología LINUX y su función es ser ***Webmail***.
- ✓ COMPAQ PROLIANT 1850R Pentium II. (Denominado IMBABURA.ANDINANET.NET), bajo tecnología MICROSOFT y su función es ser ***Hosting.***
- ✓ HP ML370 Intel(R) Xeon(TM). (Denominado WEB-LINUX), bajo tecnología LINUX y su función es ser ***Hosting.***
- ✓ COMPAQ EVO Pentium III. (Denominado PROXY-ANDINANET), bajo tecnología LINUX y su función es ser ***Proxy.***
- ✓ COMPAQ ALPHA SERVER DS20 Alpha microprocessor. (Denominado SANGAY.ANDINANET.NET), bajo tecnología UNIX y su función es ser ***Sistema de gestión comercial.***
- ✓ COMPAQ ALPHA SERVER DS10 Alpha microprocessor. (Denominado CHIMBORAZO.ANDINANET.NET), bajo tecnología UNIX y su función es se ***Radius.***
- ✓ COMPAQ PROLIANT ML350 Intel(R) Pentium(R) III. (Denominado FIREWALL), bajo tecnología LINUX y su función es se ***Firewall.***
- ✓ COMPAQ PROLIANT 1850R Pentium II. (Denominado REVENTADOR.ANDINANET.NET), bajo tecnología MICROSOFT y su función es ser ***Hosting.***
- ✓ HP ML370 Intel(R) Xeon(TM). (Denominado REVENTADORUIO.ANDINANET.NET (RESPALDO)), bajo tecnología MICROSOFT y su función es ser ***Hosting Principal Backup.***
- ✓ HP ML370 Intel(R) Xeon(TM). (Denominado REVENTADORUIO.ANDINANET.NET (PRINCIPAL)), bajo tecnología MICROSOFT y su función es ser ***Hosting Principal.***
- ✓ Server Supermicro SuperServer 6013P-i Intel Pentium IV Xeon (Denominado SRV1), bajo tecnología LINUX y su función es ser ***SMTP, POP3, HTTP.***
- ✓ Server Supermicro SuperServer 6013P-i Intel Pentium IV Xeon (Denominado SRV2), bajo tecnología LINUX y su función es ser ***SMTP, POP3, HTTP.***

- ✓ Server Supermicro SuperServer 6013P-i Intel Pentium IV Xeon (Denominado SRV3), bajo tecnología LINUX y su función es ser ***SMTP, POP3, HTTP.***
- ✓ Server Supermicro SuperServer 6013P-i Intel Pentium IV Xeon (Denominado SRV4), bajo tecnología LINUX y su función es ser ***SMTP, POP3, HTTP.***
- ✓ Server Supermicro SuperServer 6013P-i Intel Pentium IV Xeon (Denominado SRV5), bajo tecnología LINUX y su función es ser ***SMTP, POP3, HTTP.***
- ✓ Server Supermicro SuperServer 6013P-i Intel Pentium IV Xeon (Denominado SRV6), bajo tecnología LINUX y su función es ser ***SMTP, POP3, HTTP.***
- ✓ Server Supermicro SuperServer 6013P-i Intel Pentium IV Xeon (Denominado SRV7), bajo tecnología LINUX y su función es ser ***SMTP, POP3, HTTP.***
- ✓ Server Supermicro SuperServer 6013P-i Intel Pentium IV Xeon (Denominado SRV8), bajo tecnología LINUX y su función es ser ***SMTP, POP3, HTTP.***
- ✓ Server Supermicro SuperServer 6013P-i Intel Pentium IV Xeon (Denominado SRV9), bajo tecnología LINUX y su función es ser ***SMTP, POP3, HTTP.***
- ✓ Server Supermicro SuperServer 6013P-i Intel Pentium IV Xeon (Denominado NAS), bajo tecnología LINUX y su función es ser ***Almacenamiento Correo.***
- ✓ Sun Ultra 60 Ultra Sparck. (Denominado MONITOREO), bajo tecnología SOLARES y su función es ser ***Gestión de Red.***
- ✓ NORTEL ALTEON 2216 (Denominado ALTEON NORTEL NETWORKS), la función es ser ***Balanceo de cargas.***

ANDINANET S.A al momento cuenta con todos los equipos antes mencionados como los son los RTU's y los diferentes servidores. Básicamente su gran mayoría de servidores son nuevos con año de fabricación 2004. De los servidores antes citados 7 tienen como años de fabricación 1999, 2001, 2002 y 2003. Estos 7 servidores son: COMPAQ ALPHA SERVER DS20, COMPAQ

ALPHA SERVER DS10, COMPAQ PROLIANT ML350, COMPAQ PROLIANT ML1850R, HP ML370, COMPAQ EVO.

Los costos que ANDINANET S.A. tendrá que realizar son la compra de nuevos equipos para remplazar los antes mencionados, costos que no serán representativos teniendo en cuenta los beneficios que tendrá. Uno de los primeros beneficios será, un mayor incremento de sus clientes, clientes que en la actualidad buscan seguridad y rapidez, características que solo IP-V6 nos puede brindar.

## 5.3. ANÁLISIS DE COSTOS

Una vez realizado el estudio de los equipos con los cuales cuenta ANDINANET S.A. y cuales deben ser remplazados se procede a detallar los costos que representarían los mismos.

El listado de los requerimientos que se necesitan para poder brindar el servicio de IP-V6 son:

- ✓ IOS para RTU's CISCO que soporte IP-V6
- ✓ 7 Servidores que serán remplazados
- ✓ Sistemas Operativos que soporte IP-V6.

El Protocolo de Internet IP-V6, es el nuevo protocolo estándar diseñado por la IETF (Internet Engineering Task Force), que permite el crecimiento de Internet de próxima generación al soportar un número creciente de usuarios, aplicaciones mejoradas y la integración de nuevas soluciones tecnológicas.

Cisco está tomando un rol activo en definir los estándares de IP-V6 y desarrollando productos que soporten este protocolo emergente. Cisco ha ofrecido soporte para IP-V6 desde mayo de 2001 cuando estuvo disponible Cisco IOS 12.2T, para permitir a los clientes comenzar a experimentar con IP-V6. Hoy, IP-V6 está disponible en muchas versiones de Cisco IOS. Nuestras recomendaciones sobre las versiones de Cisco IOS para los clientes que están buscando soporte para IP-V6, son:

- ✓ Producción General: Cisco IOS 12.3M.
- ✓ Core ISP y NREN: Cisco 12.0S en los routers de Cisco de las series 12000 y 10720.
- ✓ Infraestructura empresarial e ISP: Cisco IOS 12.2S Acceso de Banda Ancha: Cisco IOS 12.2B
- ✓ Nuevo despliegue tecnológico IP-V6: Cisco IOS 12.3T y 12.2S

Luego de un programa beta que incluyó a varios centenares de clientes, Cisco ofrece ahora la solución de enrutamiento IP-V6 más avanzada, amplia e integral en la industria. Previendo que los requerimientos del mercado continuarán madurando, Cisco planifica ofrecer próximamente otras aplicaciones y soluciones complementarias, que cumplen con los estándares de la industria y que pueden ser utilizadas en múltiples plataformas.

Hoy en día la disponibilidad y solución IP-V6 de Cisco está disponible en ***software IOS versión 12.2(1)T***. Soporta, entre otras, las siguientes plataformas: Cisco 800 Series Routers; Cisco 1400 Series Routers; Cisco 1600 Series Routers; Cisco 1700 Series Routers; Cisco 2500 Series Routers; Cisco 2600 Series Routers; Cisco 3600 Series Routers; Cisco 4500 and 4700 Series Routers; Cisco AS5300 y AS5400 Universal Access Servers; ***Cisco 7100, 7200 y 7500 Series Routers.***

Así mismo se debe definir las características de los equipos que van a ser empleados como servidores, los mismos que van a reemplazar a los 7 servidores antes mencionados.

Existen múltiples razones por las cuales ANDINANET S.A. debería emprender una adopción de IP-V6 para su Red. El potencial tecnológico e intelectual que radica en su estructura, hace de ANDINANET S.A. sea el punto estratégico para el País, con un compromiso de fomentar el desarrollo de los ciudadanos con la aplicación de la tecnología y contribuir a la construcción de la *Sociedad del Conocimiento.*

Otra razón fuerte para la implementación de IP-V6 en la infraestructura de ANDINANET S.A., es el beneficio de ubicarse como el ISP pionero a nivel Nacional, en el estudio de esta tecnología.

Debemos tomar en cuenta que la implementación no busca reemplazar servicios IP-V4 existentes. La adopción exitosa de cualquier tecnología, depende de la fácil integración con la infraestructura existente sin interferir significativamente en los servicios actuales.

Este proyecto de implementación esta enfocado en mantener una plataforma dual sobre IP-V4 e IP-V6, por ello será necesaria la adopción de los mecanismo de coexistencia e interoperatividad definidos entre protocolos IP-V4 e IP-V6. Entre ellos contamos con:

- ✓ Stack IP Dual
- ✓ Túneles IP-V6 sobre IP-V4 o viceversa. (túneles manuales, túneles automáticos)
- ✓ Mecanismos de traducción.

De aquí una vez analizado y recordado que mecanismos se van a emplear para la implementación de IP-V6, podemos definir el Sistema Operativo con Soporte IP-V6. Ya que el Sistema Operativo es pieza fundamental para el soporte de IP-V6, las casas de software han reestructurado los stack para soportar eventualmente IP-V6.

- ✓ Linux Kernel 2.0 o más recientes
- ✓ Solaris 8
- ✓ Tru64 UNIX 4.0D (de Compaq)
- ✓ Tru64 UNIX 5.1 (de Compaq)
- ✓ Windows 2000
- ✓ Windows XP.

En cuanto a las características de los equipos que soportaran estos Sistemas Operativos podrían ser los mismos, pero debido a que se tiene 2 de los 7 servidores

de características Pentium II los cuales la única función es de Hosting podrían se reemplazados por 2 servidores nuevos, abaratando así aún mas los costos de inversión para la implementación del protocolo IP-V6.

A continuación se presentan las tablas 5.3.(a) y 5.3. (b). de costos de los pocos requerimientos que le hacen falta a ANDINANET S.A. para la implementación de IP-V6:

| HARDWARE | CARACTERISTICAS | COSTO USD |
|---|---|---|
| **COMPAQ Tru64 UNIX 4.0F** | **Compaq AlphaServer ES40 Model 2** | |
| Sistema Operativo | Compaq Tru64 UNIX 4.OF | |
| Procesador | Alpha 21264 667 MHz | |
| Procesador Qty. | 1 | |
| Memoria Instalada | 2 GB (SDRAM) | |
| Plataforma | UNIX | **11325.00** |
| **COMPAQ Tru64 UNIX 5.1A** | **Compaq AlphaServer ES45** | |
| Sistema Operativo | Compaq Tru64 UNIX 5.1A | |
| Procesador | Alpha 21264 667 MHz | |
| Procesador Qty. | 1 | |
| Memoria Instalada | 2 GB (SDRAM) | |
| Plataforma | UNIX | **17995.00** |
| | **TOTAL** | **29320.00** |

**Tabla. 5.3. (a). Análisis Costos Hardware**

| SOFTWARE | COSTO USD |
|---|---|
| Linux Kernel 2.0 | 79.00 |
| Solaris 8 | 443.99 |
| Windows 2000 Terminal Server | 419.00 |
| Windows XP Special Edition Full Version | 238.00 |
| IOS Cisco Versión 12.2 | 1175.98 |
| **TOTAL** | **2355.97** |

**Tabla. 5.3. (b). Análisis Costos Software**

El costo total que le representará a ANDINANET S.A. para la implementación de IP-V6 en su plataforma es de **31675.97 UDS.** Como se puede ver la cantidad de inversión es baja frente al crecimiento de clientes que tendrá con esta nueva plataforma y la recuperación de la inversión será en plazo de pocos cortos meses, teniendo luego mejores ingresos para ANDINATEL S.A.

## 5.4 BENEFICIOS

Una vez realizado el análisis del requerimiento de equipos y sus costos, podemos ver que la cifra calculada de inversión es baja debido a que ANDINANET. S.A. ha venido constantemente actualizando sus equipos y plataforma.

Los beneficios que obtendrá ANDINANET S.A. con la implementación del protocolo IP-V6 se verá reflejado en el notable crecimiento de clientes que abarcara en poco tiempo, ya que en la actualidad el servicio de Internet por conexión Dial-UP esta siendo reemplazada por conexiones xDSL. En Ecuador los usuarios buscamos mayores velocidades de navegación y de descargas.

Actualmente ANDINANET S.A cuenta con aproximadamente 3000 clientes con conexiones xDSL y con un crecimiento diario del 0.66%, lo que significa que al mes se tiene un crecimiento del 13.33%. Se estima que con la implementación del protocolo IP-V6 este crecimiento se duplique al 26% tendiendo a seguir creciendo.

Con este factor de crecimiento, la inversión que ANDINANET S.A. realizaría se vería recuperada en pocos meses y produciendo mayores ingresos para ANDINATEL S.A., y convirtiéndose en el ISP líder de Ecuador y de Latinoamérica.

# CAPÍTULO VI

# CONCLUSIONES Y RECOMENDACIONES

## 6.1. CONCLUSIONES

- ✓ En los años 70 la principal finalidad del IP fue interconectar redes locales entre sí, para posteriormente llegar a formarse en una red mundial de información estandarizándose como IP-V4 V4 (Internet Protocol Versión 4) y convirtiéndose en una arquitectura de cobertura mundial y llegar a ser la columna vertebral de las comunicaciones.
- ✓ En la actualidad el protocolo IP-V4 implementá dos funciones básicas: direccionamiento y fragmentación.
- ✓ El número de direcciones IP con el protocolo IP-V4 ha llegado a sus límites de utilización, presentado ya dificultades de transporte de datos con Calidad de Servicio y provocando un excesivo retardo en el ruteo de datagramas.
- ✓ ANDINANET. S.A ha iniciado la investigación y desarrollo en la implementación del nuevo protocolo (IP-V6) bajo la infraestructura que en la actualidad cuenta. Con esta implementación no se tendrá el agotamiento de direcciones IP por varios años.
- ✓ El nacimiento del protocolo IP-V6 añaden al protocolo IP-V4 nuevas características mejorando las existentes como son seguridad, movilidad y calidad de servicio (QoS) entre otras.
- ✓ En IP-V4 las direcciones están compuestas por 4 bytes que equivalen a 32 bits teniéndose como direcciones IP posibles $2^{32}$, es decir 4.294.967.296 de direcciones., mientras que con IP-V6 se tiene un espacio de 16 bytes equivalentes a 128 bits. Lo que permitiría elevar la posibilidad de direcciones a $2^{128}$, es decir 3.40282366921E38 de direcciones.

- ✓ Debido al elevado número de servidores, computadoras, nodos, teléfonos celulares, etc. que interactúan en la Internet actual, se hacen insuficiente la cantidad de direcciones que soporta el protocolo IP-V4.
- ✓ El nuevo direccionamiento IP también establecerá características como es la escala, enrutado, aumento del espacio de direcciones, multiprotocolo, seguridad, tiempo real, tarificación y comunicaciones moviles.
- ✓ Se puede decir que una desventaja de este tipo de nuevas direcciones es su dificultad para recordarlas dado su tamaño, siendo así el servicio DNS el que tendrá mas importancia aún.
- ✓ Dentro de las principales características que aporta IP-V6 frente a IP-V4 es el aumento de las capacidades de direccionamiento, un soporte mejorado para las extensiones y opciones, capacidad de etiquetado de flujo, capacidades de autentificación y privacidad, auto-configuración Plug and plan y mecanismos de movilidad mas eficientes y robustos.
- ✓ IP-V6 es un activador fundamental para la visión que tenemos de la Sociedad de Información Móvil. Actualmente, el número de teléfonos inalámbricos ya supera con creces el número de terminales fijos de Internet. En estos momentos, IP-V6 se perfila como la única arquitectura viable que puede acomodar la nueva ola de dispositivos celulares capaces de soportar Internet.
- ✓ La estructura del nuevo direccionamiento permite identificar regiones, ISP (Proveedores de Servicios de Internet), empresa o corporación, subredes, oficinas, etc. Con el nuevo formato, incluso, se puede asignar más de una dirección a la misma interfaz de una organización.
- ✓ Desde Julio del 99, se puede afirmar que IP-V6 no es una teoría, sino un hecho. La lista de corporaciones involucradas en este proyecto de migración de protocolo IP-V4 a protocolo IP-V6 es explosiva, incluyendo fabricantes, instituciones de Investigación y Desarrollo, organizaciones de Educación, Operadores de Telecomunicaciones, Empresas de Consultoría, entre otros.
- ✓ Debido al auge de Internet que hemos vivido durante la última década, el espacio de direcciones IP-V4 se ha ido agotando gradualmente. ANDINANET S.A. ante este problema, que amenaza el crecimiento de la Red de redes ha iniciado el estudio para la migración hacia IP-V6.
- ✓ IP-V6 ofrece también establecer bases para permitir el crecimiento de forma escalable y organizada (RTP, RTPC, QoS, CoS, Kerberos, IPSec, Multicast,

etc.) de una Internet en el que haya millones (sino billones) de elementos conectados, con los servicios actuales y con otros nuevos aún no imaginados, de forma más segura y flexible.

- ✓ La capacidad de ANDINANET S.A. de ofrecer nuevos servicios, en el futuro será necesidad, a sus clientes y a sus empleados, haciéndoles más competitivos en el futuro.
- ✓ Los beneficios derivados de un protocolo nuevo deben ser equilibrados por los costos asociados a la transición del sistema existente.
- ✓ El espectacular crecimiento del tráfico en Internet y la tan ansiada convergencia de voz, datos e imagen en una única red, hacen necesaria la evolución de las comunicaciones que van de la mano de las siglas IP.
- ✓ Una característica importante de IP-V6 es su configuración y reconfiguración que es Plug and Play con lo cual la asignación de direcciones es dinámica, así los hots pueden construir su propia dirección.
- ✓ La movilidad es otro factor importante dentro de IP-V6. Con esta funcionalidad podremos "saltar" de una red a otra sin apenas percibir ningún cambio. Si bien esto ya es posible con IP-V4 de una manera más bien ardua, en IP-V6 es uno de los requerimientos de diseño. Esta característica será de gran importancia cuando entren en funcionamiento las nuevas redes de telefonía con tecnología UMTS.
- ✓ La seguridad es uno de los requerimientos de diseño del nuevo protocolo: todas las aplicaciones se deben beneficiar de las facilidades de autenticación y encriptación de datos de forma transparente.
- ✓ SIP, como evolución del protocolo H.323, es un vehículo para transmitir aplicaciones de voz, datos o video en tiempo real, y sin importar la marca de los dispositivos ni la ubicación del destinatario. SIP es un protocolo de señalización que ha surgido como estándar para establecer, enrutar, modificar y terminar llamadas o comunicaciones a través de las redes IP.
- ✓ Existe una técnica que permite a los hosts y routers entunelar dinámicamente paquetes IP-V6 sobre la infraestructura IP-V4 existente. Los nodos que vayan a utilizar esta técnica recibirán una dirección unicast IP-V6 un tanto especial: los 32 bits más bajos serán la dirección IP-V4. A este tipo de direcciones se las llama direcciones IP-V6 compatibles con IP-V4.

- ✓ Otro tipo de dirección IP-V6 que contiene a una IP-V4 y se utiliza para representar aquellos nodos que solo disponen de pila IP-V4. En este caso los 32 bits más bajos serán iguales que en el caso anterior (la dirección IP-V4), pero los 16 bits siguientes por delante serán todos 1. Este tipo de direcciones recibe el nombre de direcciones IP-V6 mapeadas en IP-V4.
- ✓ Las direcciones IP-V6 se representan como series de campos hexadecimales de16 bits separados por ":", con un formato X:X:X:X:X:X:X:X, mientras que para IP-V4 se mantiene con un formato X.X.X.X. Así los 128 bits se dividen en 8 secciones, de 2 bytes (16 bits) de longitud. Los 2 bytes se expresan con 4 dígitos hexadecimales, por tanto, la dirección IP consta de 32 dígitos hexadecimales, con cada 4 dígitos separados por dos puntos.
- ✓ El direccionamiento IP-V6 también se lo puede realizar con direcciones abreviadas. Normalmente, en una dirección IP hay muchos dígitos que son 0, en esos casos, se puede abreviar la dirección. Es así que los 0's al inicio de una sección de pueden omitir. Además, si hay secciones consecutivas que son todos 0's, se pueden eliminar y poner dos puntos seguidos (solo una vez por dirección).
- ✓ Al direccionamiento en IP-V6 se lo realiza por categoría como son: UNICAST (unidestino), MULTICAST (multidestino) y ANYCAST (a cualquier destino).
- ✓ Las direcciones IP se dividen en dos partes. la primera que es el prefijo de tipo, la misma que es de longitud variable y que determina el objetivo de la dirección y los valores de los códigos se determinan de manera que ningún código sea igual que la parte inicial de cualquier código, y la segunda parte es el resto de la dirección.
- ✓ Dentro de los mecanismos previstos de transición de IP-V4 a IP-V6, existe una técnica que permite a los hots y routers entunelar dinámicamente paquetes IP-V6 sobre la infraestructura IP-V4 existente y con la cual se encuentra ANDINANET S.A. Los nodos que vayan a utilizar está técnica recibirán una dirección Unicast IP-V6 donde los 32 bits más bajos serán la dirección IP-V4.
- ✓ Otro tipo de dirección IP-V6 que contiene a una IP-V4 y se emplea para representar aquellos nodos que solo disponen de pila IP-V4. En este caso los 32 bits más bajos serán iguales que en el caso anterior (la dirección IP-V4), pero los 16 bits siguientes por delante serán todos 1.

- ✓ IP-V6 para su encaminamiento se basa en los mismos protocolos de encaminamiento empleados por IP-V4 con ciertas modificaciones. Dentro de los protocolos de encaminamiento principales que emplea IP-V4 son TCP (Transfer Control Protocol) y UDP (User Datagram Protocol).
- ✓ IP-V4 utiliza protocolos de encaminamiento interno y externo. Dentro de los protocolos de encaminamiento interno se tiene RIP, OSPF, IS-IS y como protocolos de encaminamiento externo el protocolo BGP. Otro protocolo de encaminamiento para IP-V4 es el ICMP el mismo que para IP-V6 es el protocolo ICMPV6. IP-V6 para su encaminamiento emplea protocolos como RIPng o RIPV6, OSPFV6, BGP4+, BGP5.
- ✓ La implementación de mecanismos de transición de IP-V4 a IP-V6 donde coexistirán redes y host que funcionen con uno u otro protocolo se basa en Nodos, Routers, Servidores de Nombre Dual-IP, Tunneling IP-V6 sobre IP-V4, los nodos pueden ser actualizados parcialmente a IP-V6, siendo mejor actualizar los routers antes de hacerlo con los nodos. Al conjunto de modos de migración de IP-V4 a IP-V6 se los suele denominar SIT (Simple Internet Transition).
- ✓ Dentro de las principales actividades para la migración e implementación de túneles, seguridades y servicios se debe definir escenarios de interoperabilidad entre IP-V4 e IP-V6 y estrategias de transición. Así mismo se debe evaluar las distintas tecnologías de acceso y transporte y su interacción con el protocolo IP-V6. También se debe evaluar los nuevos servicios en redes de próxima generación como seguridades y servicios.
- ✓ Para lograr el potencial completo de la nueva Internet, los usuarios finales deben poder confiar en la información y las transacciones en línea. A medida que la información digital va llegando a ser un artículo importante, ésta debe ser protegida y autenticada.
- ✓ IP-V6 significa redes más seguras y robustas de extremo a extremo que las que ofrece NAT con IP-V4, mientras que teóricamente brinda direcciones IP gratuitas para todos los usos imaginables, accesibles para todos en línea y fuera de línea. Esto, en sí mismo, puede contribuir significativamente tanto al desarrollo sostenible como a la reducción de la brecha digital tal como la conocemos hoy.

- ✓ Existen varios tipos básicos de túneles: Túneles Manuales o Estáticos (host-host, router-router, host-router) este tipo de túneles permiten atravesar nubes IP-V4 desde entidades IP-V6/IP-V4, Túnenles Automáticos o Dinámicos donde la dirección destino es compatible con IP-V4, Túneles 6to4 donde este tipo de túnel permite tener direcciones IP-V6 globales en redes solo IP-V6 donde hay un router frontera dual-stack encargado de dar salida al exterior y último tipo de Túnel es 6over4. IP-V4 actual se encuentra formado en su mayoría por túneles estáticos.
- ✓ Así mismo dentro de los mecanismos de transición también tenemos los Mecanismos de Traducción los mismos que se basan en traducir un elemento de red, los paquetes de un formato a otro. Dentro de este tipo de mecanismos tenemos: NAT-PT, SOCKSv5, BIS (Bump in the Snack).
- ✓ La migración del protocolo IP-V4 a IP-V6 significa un cambio a nivel de BackBone, Plataforma, Infraestructura para un ISP, para el caso del desarrollo de este proyecto de ANDINANET S.A.
- ✓ Dentro de las estrategias para la migración del protocolo IP-V4 a IP-V6 se tiene la Estrategia de Migración de Backbones donde se debe mantener la configuración actual y migrar cuando el trafico entunelado sobre tráfico IP-V4. Debido a los problemas del número de rutas existente se debe recomendar y colaborar con los ISP y otros Backbones para evitar así una migración "forzosa".
- ✓ En IP-V4 la seguridad se consigue mediante técnicas de criptografía en la capa de aplicación, mientras que en IP-V6 la seguridad se puede conseguir a nivel de la capa de red (Protocolo IP), y se implementa en los routers. En IP-V6 la seguridad se implementa mediante la extensión de cabeceras diseñadas específicamente para dicho propósito.
- ✓ La mayor parte de los usuarios de ANDINANET S.A. pasan una gran parte de su tiempo en línea no haciendo otra cosa que esperar, esperar para ser conectado a un sitio Web, esperando para que se carguen páginas y esperando para bajar software. Como contraste, la próxima generación de Internet nos brindara la velocidad que necesitamos.
- ✓ Un beneficio adicional para QoS en IP-V6 es que se puede usar una etiqueta de flujo (asignada dentro del encabezamiento de IP-V6) para distinguir flujos de

tráfico para obtener un encaminamiento optimizado. Además se puede usar la etiqueta de flujo para identificar flujos aún cuando la carga útil esta encriptada.

- ✓ Uno de los requisitos comerciales de más rápido crecimiento para redes internas es la capacidad de transmitir una corriente de video, audio, noticias, datos financieros, u otros datos sobre tiempo a un grupo de estaciones extremas funcionalmente relacionadas pero geográficamente dispersas. La mejor manera de lograr esto es por medio de técnicas de multidifusión de capa de red.
- ✓ Para ANDINANET S.A. migrar al sistema IP-V6 en un simple proceso seria muy difícil, en contraste se hace necesario desarrollar estrategias para que IP-V4 coexista con IP-V6.
- ✓ El mecanismo para que IP-V4 e IP-V6 coexistan, es que el snack de ambos protocolos sean implementados en un mismo dispositivo (Router, Pc o Servidor), el cual esta referido como un nodo IP-V6/IP-V4.
- ✓ Para que un túnel este operativo, las direcciones de ambos extremos del túnel y los destinos del paquete deben ser conocidos, y estas dos direcciones no necesariamente son las mismas, la manera en la cual la dirección al final del túnel es determinada define los tipos de túneles, que pueden ser automático o configurado.
- ✓ Para poder brindar el servicio de IP-V6 ANDINANET S.A. no tendrá que realizar una inversión costosa en ruteadores, ya que cuenta con ruteadores CISCO. Lo único que se debe realizar es la actualización en la configuración del sistema operativo para que permita soportar IP-V6 sobre IP-V4 ganando así direccionamiento IP para la masificación de clientes.
- ✓ En la actualidad ANDINANET S.A. cuenta con una plataforma nueva con la capacidad de poder proveer los servicios de Internet a nivel Nacional. Gracias a que ANDINANET S.A. cuenta con esta nueva plataforma los costos de inversión para la implementación de IP-V6 no tendría un costo elevado ya que cuenta con RTU's Cisco.
- ✓ Uno de los primeros beneficios será, un mayor incremento de sus clientes, clientes que en la actualidad buscan seguridad y rapidez, características que solo IP-V6 nos puede brindar.
- ✓ Existen múltiples razones por las cuales ANDINANET S.A. debería emprender una adopción de IP-V6 para su Red. El potencial tecnológico e intelectual que radica en su estructura, hace de ANDINANET S.A. sea el punto estratégico

para el País, con un compromiso de fomentar el desarrollo de los ciudadanos con la aplicación de la tecnología y contribuir a la construcción de la *Sociedad del Conocimiento.*

- ✓ Los beneficios que obtendrá ANDINANET S.A. con la implementación del protocolo IP-V6 se verá reflejado en el notable crecimiento de clientes que abarcara en poco tiempo, ya que en la actualidad el servicio de Internet por conexión Dial-UP esta siendo reemplazada por conexiones xDSL. En Ecuador los usuarios buscamos mayores velocidades de navegación y de descargas.

## 6.2. RECOMENDACIONES

- ✓ Un problema del actual protocolo IP viene provocado por el hecho de que Internet necesita de unos equipos llamados routers que dirigen el trafico que se genera en la red a partir de unas tablas de re-direccionamiento. Por desgracia, a medida que las direcciones IP van creciendo, estas tablas se hacen más grandes, incrementando la sensación de colapso que actualmente sentimos cuando accedamos a Internet, por lo cual se debe optar por la migración de protocolo a IP-V6.
- ✓ Realizar la migración del protocolo IP-V4 a IP-V6 para la plataforma que tiene actualmente ANDINANET S.A. no es factible debido a que en nuestro medio los usuarios finales no tienen equipos y software para soportar el mismo. Para la implementación del protocolo IP-V6 en ANDINANET S.A. se recomienda realizarla mediante Túneles ya sea Manual o Automático obteniéndose así tener direcciones IP-V6 más IP-V4 en los routers principales y una dirección IP-V4 donde el cliente, ganando espacio de direcciones para la masificación de ANDINANET S.A. y poder prestar a los clientes los diferentes servicios bajo buenos niveles de seguridad que se manejan bajo IP-V6.
- ✓ Para lograr el potencial completo de la nueva Internet, los usuarios finales de ANDINANET S.A. deben poder confiar en la información y las transacciones en línea tanto como o más que lo que confían en documentos en copia impresa. A medida que la información digital va llegando a ser un artículo importante, este debe ser protegida y autentificada. Lo que vemos debe ser lo mismo que fue enviado y lo que recibimos.

- ✓ Debemos poder controlar nuestros datos y proteger nuestro secreto en el ciberespacio, es por esto que se emplean y se exponen mecanismos fáciles de usar, poco costosos y universalmente disponibles para la seguridad y la autentificación.
- ✓ Toda la información que circula en la Red recibe la misma prioridad; eso significa que compiten por el mismo ancho de banda un correo electrónico, un archivo que se descarga de un servidor FTP y una video conferencia. La implantación de la QoS permitirá a las aplicaciones solicitar por si mismas una cantidad determinada de ancho de banda o una prioridad específica. Esto lograría que los computadores que estuviesen procesando una aplicación como la teleinmersión o la video conferencia se pudiesen comunicar entre sí a la alta velocidad requerida para las interacciones correspondientes, "en tiempo real".

# REFERENCIAS BIBLIOGRÁFICAS


http://www.diarioti.com/noticias/1999/jul99/15192163.htm, Protocolo IP-V6.

http://canales.laverdad.es/cienciaysalud/7_1_36.html, Protocolo IP-V6.

http://www.alhambra-eidos.com/ipv6/NIPv6.html, Protocolo IP-V6.

http://www.argo.es/~jcea/proyecto/ip6.htm, Protoclo IP-V6.

http://www.die.udec.cl/~redes/apuntes/myapuntes/node233.html, Protocolo UDP.

http://bulma.net/body.phtml?nIdNoticia=1840, Configuración IP-V6.

http://imasd.elmundo.es/imasd/ipv6/cfg/router-freebsd.html, Configuración de túneles.

http://www.wl0.org/~sjmudd/wireless/network-structure/html/x78.html, Direccionamiento IP.

http://www4.ipv6.frlp.utn.edu.ar/direcciones-utn.html, Túneles.

http://www.die.udec.cl/~redes/apuntes/myapuntes/node184.html, Encabezado IP-V6.

http://www.merlinux.org/traductor/justi.html, Enrutamiento IP-V6/IP-V4.

http://www.arsys.es/empresa/idc/ipv6.htm, Formato de las direcciones IP.

http://www.canal-ar.com.ar/Noticias/NoticiaMuestra.asp?Id=419, Aplicaciones IP-V6.

http://www.rau.edu.uy/ipv6/queesipv6.htm, Representación de direcciones IP-V6, Mecanismos de Transición.

http://www.linups.org/modules/doc/documentos/ipv6/ipv6.html, Navegador de Internet.

http://club.telepolis.com/jlrosalesf/FUNDAMENTOS%20DEL%20TCP%20-4-.htm, Direccionamiento IP-V6.

http://fmc.axarnet.es/tcp_ip/tema-03/tema-03-m.htm, Direcciones Unicast, Anycast y Multicast.

http://pegaso.ls.fi.upm.es/arquitectura_redes/transparencias/APDO_11_14/, Protocolo RIP, BGP y OSPF.

http://www.geocities.com/ricardodp/nt_internet.htm, Formato de Cabecera IP-V6.

http://www.die.udec.cl/~redes/apuntes/myapuntes/node157.html, Protocolo ICMP.

http://www.rediris.es/gt/iris-ipv6/rtiris-1198.es.html, Transición de IP-V6 a IP-V4.

http://www.windowstimag.com/atrasados/2001/57_oct01/articulos/IPv6_1.asp, El protocolo IP-V6 en Windows.

http://www.eduangi.com/quagga/quagga-es-9.html, Encaminamiento IP-V6.

http://revista.robotiker.com/articulos/articulo71/pagina1.jsp, Historia de IP-V6.

http://www.aui.es/biblio/libros/mi2000/Jordi%20Pallet.htm, Definición del Protocolo IP-V6.

http://www.alhambra-eidos.com/ipv6/NIPv6.html, Migración de IP-V4 a IP-V6.

http://www.itlp.edu.mx/publica/revistas/revista_isc/actual/ipv6.html, El Futuro de IP-V6.

http://neutron.ing.ucv.ve/revista-e/No5/WOrtega.htm, Capacidades de IP-V6.

http://www.rediris.es/mmedia/Arquitectura.es.html, H.323, Terminales, Gateways, Gatekeepes, Unidades de Control (MCU),

http://www.netmedia.info/business/articulos.php?id_sec=29&id_art=4037&num_page=14000, SIP a las redes IP.

B. A., Forouzan, *Transmisión de datos y redes de comunicaciones*, 1, 2ª edición, Editorial McGraw-Hill, 2002, Apéndice H.

E. Kaufman, A. Newman, *Implementing Ipsec*, 3, 2ª edición, Editorial John Wiley & Sons, 2003, Página 183.

DOUGLAS E. Comer, *Internetworking with TCP/IP, 3*ª Edición, McGraw-Hill, 2001. Página 89.

# ÍNDICE DE FIGURAS

# ÍNDICE DE TABLAS

# GLOSARIO

**AH.-** Authentication Header

**BGP**.- Border Gateway Protocol

**BIS.-** Bump in the Snack

**DOS.-** Denial of Service

**DHCP**.- Dynamic Host Configuration Protocol

**ESP.-** Encapsulating Security Payload

**FP.-** Format Prefix

**HAN**.- Home Area Networks

**HTTP.-** HyperText Transfer Protocol

**ICMP.-** Internet Control Message Protocol

**ICMPV6.-** Internet Control Message Protocol V6

**IDRP.-** Interdomain Routing Protocol

**IETF.-** Internet Engineering Task Force

**I ID**.- Interface Identifier

**IKE.-** Internet Key Exchange

**IP**.- Internet Protocol

**Ipng**.- IP Next Generation o Siguiente Generación

**IP-V4.-** Internet Protocol Versión 4

**IP-V6.-** Internet Protocol Versión 6

**ISP.-** Proveedores de Servicios de Internet

**MC.-** Controladores Multipunto

**MCU.-** Unidades de Control Multipunto

**MP.-** Procesadores Multipunto

**NLA**.- Next-Level Aggregation Identifier

**OSPF**.- Open Shortest Path Firsht

**OSPFV6**.- Open Shortest Path Firsht V6.

**PBN.-** Redes Basadas en Paquetes

**PDU.-** Unidad de Datos de Protocolo

**PRI.-** Prioridad

**QoS.-** Quality of service

**RAS**.- Registrantion Admisión Status

**RTB.-** Red Telefónica Básica

**RIP.-** Routing Information Protocolo

**RIPV6.-** Routing Information Protocolo V6.

**SIP.-** Session Initiation Protocol

**SLA.-** Site-Level Aggregation Identifier

**SMTP**.- Simple Mail Transfer Protocol

**TCP.-** Transfer Control Protocol

**TLA**.- Top-Level Aggregation Identifier.

**TPDUs.-** Transport Protocol Data Unit

**UDP.-** User Datagram Protocol

**VER.-** Versión

**VoIP.-** Voz a través de Internet

.

# FECHA DE ENTREGA

El proyecto de grado fue entregado a la Facultad de Ingeniería Electrónica y reposa en la Escuela Politécnica del Ejercito desde:

Sangolquí, a_____del 2005.

_____

Xavier Martinez C.

TCRL. DE E.M.

Decano de la Facultad de Ingeniería Electrónica

_____

Dr. Jorge Carvajal

Secretario Académico

_____

Luis Germán Ojeda Mendieta

Autor