Universidad Latinoamericana de Ciencia y Tecnología

Facultad de Ingenierías

Escuela de Ingeniería Informática

Trabajo final para optar por el grado de Licenciatura en Ingeniería Informática con énfasis en Redes y Sistemas Telemáticos

Protocolos de Internet: funcionamiento y Beneficios de ipv6

Carlos Cerdas Lazo[1]
Cédula 1 1140 0066

Profesor: Lic. Miguel Pérez M.

Diciembre-2007

[1] Bachiller en Ingeniería Informática. Candidato a Licenciatura en Ingeniería Informática con énfasis en Redes y Sistemas Telemáticos. ULACIT. Correo electrónico: ccerdasl066@yahoo.com

ÍNDICE

Introducción

Actualmente, Internet se ha convertido en una de las herramientas de investigación más importantes en el mundo. Se encuentra poblada por cantidades diferentes de sitios *Web* que proveen de varios tipos de información, los cuales provienen de distintas partes del mundo. Esto convierte a Internet en una biblioteca electrónica mundial muy importante para la humanidad.

Internet no solo crea un impacto informativo, también logra fomentar otro tipo de negociación que tiene un enfoque diferente al que normalmente se conoce como comercio. A este tipo de negocio se le llama comercio electrónico, que es la nueva era de negociación pues, acorta las distancias.

Además, la red global permite aplicar ideas que pretenden economizar inversiones en sectores de la educación, como lo son los sistemas de *e-learning* que fomentan una educación a distancia por medio de herramientas tecnológicas.

Debido a que este mundo se ha convertido en un mundo lleno de avances tecnológicos, Internet necesita valerse de reglas que controlen el flujo de información que se maneja en la *Web*. Por lo tanto, se crean protocolos para cubrir esta función; uno de ellos es el protocolo de Internet (IP).

Protocolo es sinónimo de regla, y el objetivo del protocolo de Internet es exactamente marcar las pautas por seguir para lograr una ordenada comunicación en Internet.

En Tiempos pasados se crea el protocolo de Internet versión 4, que actualmente opera como base de Internet, sin embargo; surgen problemas que crean inconvenientes en un adecuado uso de la red mundial, debido a que este protocolo no cubre las exigentes necesarias en la actualidad. Se crea el protocolo de Internet versión seis, para subsanar las presentes eventualidades.

Tomando en consideración lo expuesto anteriormente. Se presentarán una serie de conceptos y funcionamientos sobre versiones de IP y sus diferencias, con forme se han ido desarrollando a través de los años, pretendiendo mejorías en diferentes sectores importantes dentro de la comunicación de redes de datos.

Concepto de IP

El Protocolo de Internet es un protocolo que no se encuentra orientado a conexión, es utilizado por el emisor tanto como por el relector para lograr enviar paquetes de datos a través de una red conmutada.

Los datos que son enviados por una red con protocolo de Internet son enviados en bloques conocidos como paquetes o datagramas. En IP no es necesaria una configuración previa para lograr enviar un paquete a otro con el que no se había establecido comunicación anteriormente.

El Protocolo de Internet contiene un servicio llamado el mejor esfuerzo *(best effort)* provee un servicio de datagramas no fiable, se intentará hacer lo mejor pero, no será muy eficiente. IP no cuenta con ningún proceso que garantice que los paquetes enviados llegan a alcanzar el destino establecido o no, únicamente proporciona seguridad (mediante *checksums* o sumas de comprobación) de las cabeceras de los paquetes pero, no de los datos dentro del mismo. Por ejemplo, al no garantizar nada sobre la recepción del paquete, éste podría llegar en mal estado, en un orden distinto con base en otros paquetes, duplicado o simplemente no llegar. Si se necesita fiabilidad, esta es proporcionada por los protocolos de la capa de transporte, como TCP.

En la transmisión de los paquetes existe un mecanismo que se realiza en el caso de que los paquetes excedan el tamaño negociado (MTU) en esta situación, podrán ser divididos en paquetes más pequeños, y reensamblados luego, cuando sea necesario.

Las cabeceras IP contienen información valiosa como por ejemplo: las direcciones de origen y de destino, que serán usadas por los conmutadores de paquetes y los *routers* para decidir el camino optimo de red por el que retransmitirán los paquetes.

¿Qué es Ipv4?

El protocolo de Internet versión 4 fue uno de los primeros que se creó para implementarlo de forma global y base para Internet.
Esta versión de protocolo esta constituida por una longitud de 32 bits, que permite tener una cantidad limitada de direcciones ip, es decir; 2 levado a la 32 que da como resultado 4.294.967.296 direcciones únicas.

Direccionamiento

El protocolo de Internet se encarga de la entrega de paquetes en una red. Si el paquete se encuentra en una red origen y debe ser enviado a una red destino. Cada una de las redes debe estar adecuadamente identificada de manera única, este identificador funciona parecido al número de cedula de una persona, y este número es único para este individuo. Cuando cada una de las redes se encuentra identificada el traspaso de paquetes de una red a la otra se realiza.

Al llegar a la entrada de la red destino el paquete será recibido por un router, el cual se encarga de encaminar el paquete al destino correcto.

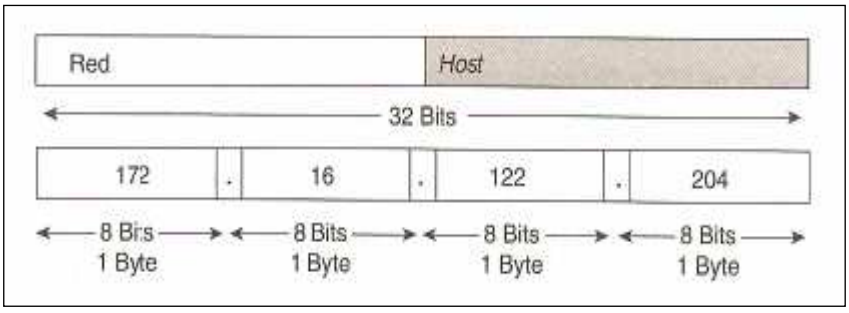
Esto funciona parecido al sistema de correos postales. El paquete es enviado con una dirección destino, luego llega al correo postal y este se encarga de enviar el paquete al destino correcto dentro de su zona. La acción que realiza el correo postal, es la que ejecuta el router en el momento de tener un paquete para su envío.

Un punto muy importante por considerar, es que de acuerdo con lo anterior la red debe estar compuesta por dos partes: una es la identificación de la red a la que se está conectado y otra es lo que se encuentra dentro de dicha red, es decir; el destino específico al que fue enviado el paquete de información.

Clases de Direcciones

En una cantidad tan grande de direccionamiento de redes como lo es 4.294.967.296, debe realizarse una clasificación para lograr un orden de acuerdo con el tamaño de la red que se va ocupar, a esto se le llama direccionamiento de clases, en la que cada dirección de 32 bits se divide en dos partes: *red* y *host*. (Ver gráfico Nº 1)

Gráfico #1. Dirección de red

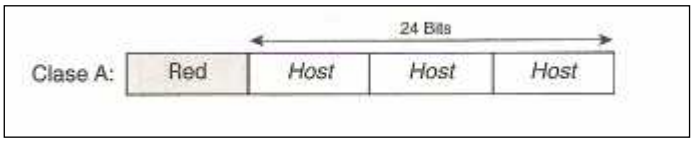


Fuente: Cisco System, Inc, 2004, p.33

Direccionamiento Clase A

Esta clase es para clasificar las direcciones que serán utilizadas para redes de proporciones grandes en tamaño. Además, funcionan en un rango de 0 a 127, y se utiliza el primer octeto para red y los demás para sobrantes para host (Ver gráfico Nº 2)

Gráfico #2. Direcciones de clase A

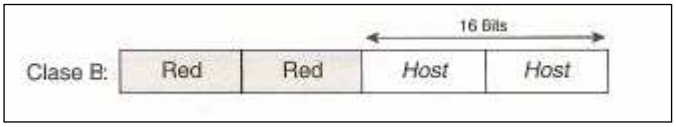


Fuente: Cisco System, Inc, 2004, p.34

Direccionamiento Clase B

Esta clase es para clasificar las direcciones que serán utilizadas para redes de proporciones medianas en tamaño. Además, funcionan en un rango de 128 a 191, y se utiliza los dos primeros octetos para red y los demás sobrantes para host (Ver gráfico Nº 3)

Gráfico #3. Direcciones de clase B

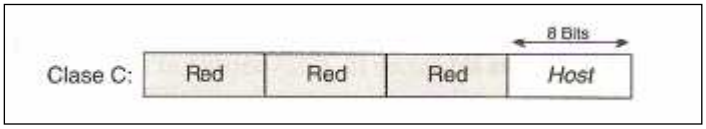


Fuente: Cisco System, Inc, 2004, p.35

Direccionamiento Clase C

Esta clase es para clasificar las direcciones que serán utilizadas para redes de proporciones pequeñas en tamaño. Además, funcionan en un rango de 191 a 223, y se utiliza los tres primeros octetos para red y los demás sobrantes para host (Ver gráfico Nº 4)

Gráfico #4. Direcciones de clase C



Fuente: Cisco System, Inc, 2004, p.36

Subneteo

El subneteo es un proceso que implica la división de la dirección principal de la red en varias otras direcciones para lograr crear otras redes que pertenecen a la misma red, pero que se manejan de forma individual. A estos segmentos de redes que se crean se les llama subredes y en cada una de ellas se definirán los host requeridos.

Desperdicio de direcciones en Ipv4

El desperdicio en esta versión se debe a varios motivos, dentro de los más importantes se destacan:

- No se tuvo en cuenta el inmenso crecimiento en la demanda de Internet a nivel mundial.
- Otro de los casos en los que se presenta el desperdicio de direcciones es en las redes de grandes tamaños por la razón del subneteo, esto implica que en cada subred que se crea con este proceso se desperdician la primera subred y la ultima.
- No todas las subredes que se crean se utilizan, en algunos casos, sobran subredes que son desperdiciadas.
- Por ejemplo, si en una subred se quieren acomodar 80 hosts, se necesita una subred de 128 direcciones (se tiene que redondear a la siguiente potencia de 2); en este ejemplo, las 48 direcciones restantes ya no se utilizan.

Estos puntos anteriormente mencionados crean un estímulo en desarrollar otro tipo de protocolo que cubra estas y otras necesidades, por lo cual, se forma el protocolo de Internet versión 6 que pretende eliminar las debilidades que presenta la versión anterior.

¿Qué es Ipv6?

Es la nueva versión de protocolo de Internet que intenta reemplazar a la versión anterior de forma paulatina. Teniendo una función parecida a su antecesor que era encaminar paquetes a través de la red. Esta nueva versión fue creada por Steve Deering de Xerox PARC y Craig Mudge.

Antecedentes de los cimientos de Ipv6

Dentro de esta temática IPforum México indica lo siguiente:

Para el invierno de 1992 la comunidad del Internet había creado cuatro propuestas diferentes para el IPng que eran: CNAT, IP Encaps, Nimrod y Simple CLNP.

Seguidamente, para diciembre del mismo año, surgieron tres propuestas más el PIP (The P Internet Protocol), el SIP (The Simple Internet Protocol) y el TP/IX.

En la primavera de 1992 el CLNP se desarrolló en el TUBA (TCP and UDP with Bigger Addresses), y el IP Encaps en IPAE (IP Address Encapsulation).

Para el verano de 1993, IPAE se combinó con el SIP aunque mantuvo el nombre SIP, que posteriormente se fusionó con la PIPA, y al grupo de trabajo resultante se le llamó SIPP (Simple Internet Protocol Plus). Casi al mismo tiempo el grupo de trabajo TP/IX cambió su nombre por el de CATNIP (Common Architecture for the Internet).

Posteriormente, en la reunión del IETF del 25 de julio de 1994 en Toronto Canadá, los directores de área del mismo organismo recomendaron el uso del IPng y lo documentaron en el RFC 1752, (la recomendación para el protocolo IP de siguiente generación).

El 17 de noviembre del mismo año fue aprobada esta recomendación por el IESG (Internet Engineering Steering Group) que elaboró una propuesta de estándar.

Motivo de creación de ipv6

Con anterioridad se ha venido mencionando uno de los principales motivos por los cuales se toma la iniciativa de desarrollar un nuevo protocolo como lo es actualmente Ipv6. Esta moción se crea por la falta en cantidad de direcciones que tiene ipv4.

En algunos países asiáticos, en los cuales se muestra una creciente en el número de habitantes. Esta nueva versión de protocolo de Internet viene a solventar el problema de la falta de direcciones ip que presentan estos países debido a su creciente población y por ende una alta tasa de expansión en la demanda de Internet y redes privadas.

Ipv4 tiene un espacio de direcciones de 4.294.967.296, mientras que la Ipv6 cubre un espacio en direccionamiento de 2 elevado a la 128, es decir; 340.228.366.920.938.463.463.374.607.431.768.211.456.

Además del problema de espacio de direcciones nacen otras necesidades que igual la versión 4 no cubre, como por ejemplo:

- 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

- Seguridad: por la cantidad de empresas y usuarios que necesitan la Internet para un correcto funcionamiento de sus actividades.

- Tiempo real. Ipv4 define una red pura orientada a datagramas y, como tal, no existe el concepto de reserva de recursos. Cada datagrama debe competir con los demás y el tiempo de tránsito en la red es muy variable y sujeto a congestión.

- Comunicación móvil: 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.

Características principales de ipv6

Dentro de las principales característica que presenta la nueva versión de protocolo de Internet se muestran las siguientes:

Espacio en direccionamiento

Esta es una de las principales características que define el protocolo de Internet versión seis.

El tamaño del Ipv6 es cuatro veces mayor que la versión 4, es decir que la ipv4 trabajo con un espacio de 32 bits, en cambio ipv6 crea su direccionamiento con un espacio de 128 bits.

En los años 70 no se tenía una visión del crecimiento que se iba tener cuando se diseñó el ipv4. En ese entonces imaginarse que se agotarían las direcciones era insólito. Pero en 1992 se llegó a la conclusión de que

se debía crear un protocolo que permitiera mayor espacio en el direccionamiento, esto debido a que la mala administración en la propagación del direccionamiento y el crecimiento masivo en lo que respecta a la tecnología, lograron agotar el espacio que se había definido.

Ahora, con la creación de ipv6 es más difícil pensar que se agote el espacio en el direccionamiento. Para poder verlo de manera más exacta, el monto de espacio que se tendrá es de 655.570.793.348.866.943.898.599 (6,5 x 1023) direcciones por cada metro cuadrado de la superficie terrestre.

Autoconfiguración

La autoconfiguración es una seria de pasos los cuales un host decide como autoconfigurar sus interfaces en Ipv6. Este mecanismo es el que permite decir que Ipv6 es plug & play.

El proceso incluye la creación de una dirección de enlace local, verificación de que no esta duplicada en dicho enlace y determinación de la información que ha de ser autoconfigurada.

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

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

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

En la autoconfiguración predeterminada, el host obtiene la dirección de

la interfaz o la información y parámetros de configuración desde un servidor. Los servidores mantienen una base de datos con las *direcciones* que han sido asignadas a cada host.

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

El mecanismo de autoconfiguración predeterminada, por el contrario, asegura que cada host tiene una determinada dirección, asignada manualmente.

IPsec

Las redes se diseñan teniendo en cuenta evitar ataques de filtrado desde fuera de la Intranet. Esto se logra cifrando la información que pasa por medios de comunicación públicos.

IPSec tiene como objetivo general lograr prestar seguridad garantizada a las redes y realizar dos de los objetivos específicos que son:

- Proteger la información dentro de los paquetes de ip.
- Defender contra los ataque a la red por medio de filtrado de paquetes.

El funcionamiento de este protocolo de seguridad en forma general se basa en un modelo de seguridad completo, y establece la confianza y la seguridad desde una dirección IP de origen hasta una dirección IP de destino. La dirección IP no se toma como una identidad única, si no que detrás de esta dirección se encuentra un sistema que contiene una llave única que proporciona la identificación del mismo y esta llave se valida por medio de un proceso de autentificación. Es decir Ipsec proporciona una seguridad completa de inicio a fin en lo que respecta al viaje del paquete en un Intranet o extranet, incluidas las comunicaciones entre estaciones de trabajo y servidores, y entre servidores.

Multicast

Este tema es un tanto distinto a el ipv6 con respecto a ipv4, debido un paquete no está dirigido a una red o subred por que estos conceptos no están comprendidos dentro el protocolo de Internet versión seis, si no que esto funciona de manera diferente.

Cuando un paquete se envía de forma multicast, este es encaminado a través de un grupo de nodos definidos con anterioridad, compuesto por cualquier equipo ubicado en cualquier lado de la red.

El nodo que transmite el paquete de forma multicast lo hace como si se tratara de cualquier otro paquete, luego este es procesado por enrutadores intermedios, los cuales contienen tablas que comparan cada dirección de multicast con un conjunto de direcciones reales de nodos, cuando se ubican las direcciones correspondientes, se prepara una copia y esta es retransmitida a los nodos pertinentes.

Anycast

La diferencia que tiene este tema con respecto al anterior es que el paquete es enviado a un destino en concreto no a un grupo.

El funcionamiento de este proceso consiste en que el paquete es enrutado al mejor destino, tomando en cuenta el tipo de topología de la red. Cuando el paquete es encaminado y es captado por los enrutadores intermedios, se encargan te tomar la decisión de cuál es el destino más cercano, desde el punto de vista del tiempo de latencia.

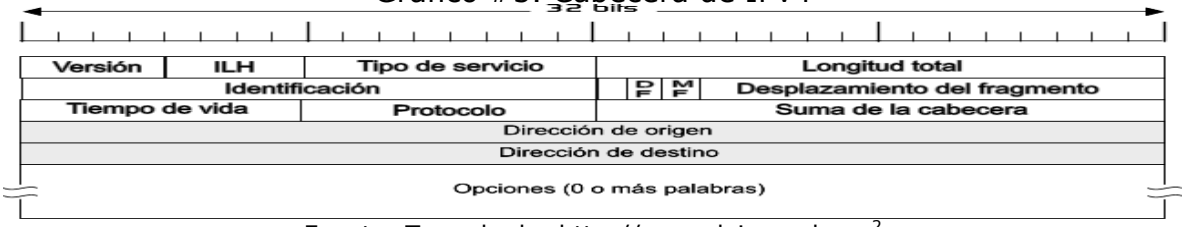
Anycast también, permite el mejoramiento de sistemas existentes como por ejemplo; los DNS, los cuales se encuentran distribuidos geográficamente en distintos lugares y se usa el anycast para lograr una descentralización del servicio y evitar que la carga caiga sobre un único servidor y evitar alguna caída que afecte la navegación por Internet.

Funcionamiento de ipv6

Cabecera de IPv4

La cabecera es una de las partes que componen a un datagrama. En la cabecera existen diferentes tipos de campos:

Gráfico #5. Cabecera de IPv4



Fuente: Tomado de: http://www.dei.uc.edu.py[2]

[2] http://www.dei.uc.edu.py/tai2003/ipv6/cabecera.htm

- **Versión:** Contiene el número de la versión del protocolo a la que pertenece el datagrama.

- **Longitud de la cabecera:** (Internet Header Length, IHL) Está especifica la longitud de la cabecera, aunque esta no tiene una longitud constante.

- **Tipo de servicio:** Este campo se utiliza para definir la importancia o prioridad que tienen los datos que están siendo enviados, y según la prioridad que tengan de esa manera serán tratados en el momento de la transmisión.

- **Longitud total:** Este ofrece la longitud total del datagrama, es decir tomando en cuenta la cabecera y los datos que son enviados. La longitud mayor de un datagrama es de 65.535 bytes, esto quiere decir que el datagrama no podrá ser mayor a este monto, pero ya en la práctica este tamaño es menor.

- **Identificación:** Este valor funciona para identificar a cuál datagrama pertenece un fragmento recién llegado a un host.

- **Fragmentación:** Mantiene un valor que funciona para unir nuevamente los datagramas que hayan sido fragmentados, tomando en cuenta que el valor cero es para el primer fragmento.

- **Tiempo de existencia:** Contiene un valor que cada ves que el paquete atraviesa por un sistema disminuye, en el caso que este número llegue a cero el paquete será eliminado. Esto con un objetivo de seguridad, ya que esto podría producir un bucle infinito, el cual en una red diseñada correctamente no ocurriría, pero aun así se aplica esta medida.

- **Protocolo:** El número utilizado en este campo sirve para indicar a qué protocolo pertenece el datagrama que se encuentra a continuación de la cabecera IP, de manera que pueda ser tratado correctamente cuando llegue a su destino.

- **Suma Comprobación:** El campo de comprobación es necesario para verificar que los datos contenidos en la cabecera IP son correctos. Por razones de eficiencia este campo no puede utilizarse para comprobar los datos incluidos a continuación, sino que estos datos de usuario se comprobarán posteriormente a partir del campo de comprobación de la cabecera siguiente, y que corresponde al nivel de transporte. Este campo debe calcularse de

nuevo cuando cambia alguna opción de la cabecera, como puede ser el límite de existencia.

- **Dirección de origen:** Contiene la dirección del host que envía el paquete.

- **Dirección de destino:** Esta dirección es la del host que recibirá la información. Los routers o *gateways* intermedios deben conocerla para dirigir correctamente el paquete.

- **Opciones IP:** Permite que IP soporte varias opciones, como la seguridad (longitud variable).

- **Relleno:** se agregan ceros adicionales a este campo para garantizar que el encabezado IP siempre sea un múltiplo de 32 bits.

Se ha explicado la función que cumplen cada uno de los campos que componen a la cabecera de un datagrama en el protocolo de Internet versión 4, ahora se dará una explicación de los campos de Ipv6 para posteriormente, lograr hacer una comparación de las diferentes cabeceras que ofrecen estos dos protocolos.

Cabecera de IPv6

La cabecera de ipv6 está dentro de los primeros 40 bytes del paquete. Y Está compuesta por los siguientes campos:

Gráfico #6. Cabecera de IPv6

Fuente: Tomado de: http://www.dei.uc.edu.py[3]

[3] http://www.dei.uc.edu.py/tai2003/ipv6/cabecera.htm

- **Versión:** Este campo ocupa 4 bits, e indica la versión de IP. Para el formato descrito, la versión es la 6, para Ipv6.

- **Prioridad:** Este campo indica la importancia o prioridad que el emisor desea darle a los paquetes enviados respecto a los demás que el mismo ha enviado. Los *rangos* de prioridad se dividen en dos: parte una va de 0 a 7, lo cual significa esperar recibir una respuesta en caso de congestión. Y de 8 a 15 los que no envían respuesta en caso de congestión.

  Cuando se aplica prioridad 8, significa que el emisor está dispuesto a que los paquetes que ha enviado sean descartados en caso de congestión.

- **Etiqueta de flujo***:* Este campo ocupa 24 bits, y es usado por el emisor 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.

- **Longitud de la carga:** Este campo ocupa 16 bits, e indica la longitud del resto del paquete que sigue a la cabecera, en octetos.

- **Siguiente cabecera***:* Este campo ocupa 4 bits, e identifica el tipo de cabecera que sigue a la cabecera IPv6. Es compatible con los valores del campo protocolo en IPv4.

- **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 IPv4.

- **Dirección origen***:* Este campo ocupa 128 bits, y corresponde a la dirección de origen.

- **Dirección destino***:* Este campo ocupa 128 bits, y corresponde a la dirección de destino.

Comparación de cabeceras ipv4 vs. ipv6

Con anterioridad se explicaron los dos tipos de cabeceras de las diferentes versiones de protocolos de Internet, por lo tanto, se puede observar que cada una difiere de la otra tanto en tamaño como en cantidad de campos y funciones de la mayoría de los mismos.

La longitud total de la cabecera en IPv6 es de 40 bytes, cuando en IPv4 era 20 bytes. Además la cabecera IPv6 tiene un tamaño fijo, esto ayuda a los Routers a conmutar el tráfico lo que se traduce en mayores prestaciones.

Además, hay que tener en cuenta que los campos van alineados a 64 bits lo que permite a los nuevos procesadores optimizar el rendimiento.

En la nueva cabecera IPv6 hay muchos campos que son omitidos con respecto a la de IPv4, esto es debido a que se hacen innecesarios por redundancia.

Un ejemplo de campo que ha sido omitido es el campo de Desplazamiento de Fragmentación, es untando distinto, por lo que el proceso por el que se realiza la fragmentación de los paquetes es totalmente modificado en IPv6, lo que implica la total omisión de este campo.

En IPv6 los encaminadores no fragmentan los paquetes, sino que de ser preciso, dicha fragmentación/desfragmentación se produce extremo a extremo es decir, de origen a destino.

Definición de direcciones

Se definen tres tipos de direcciones dentro de este protocolo que son las siguientes:

- Unicast: funciona como un identificador para una interfaz es decir, cuando un paquete es enviado a una dirección unicast, este se entrega a la interfaz que tiene como identificación dicha dirección unicast.

  Dentro de esta definición hay diferentes tipos como lo son:

  - Direcciones mundiales: Este tipo de dirección se identifica por medio del formato de prefijos 001. Además, son creadas

para ser resumidas con el objetivo de hacer más eficiente la infraestructura del enrutamiento.

- Direcciones locales: Estas son utilizadas para lograr una comunicación entre vecinos que se encuentren dentro del mismo enlace con el objetivo de ser conciente de quienes están alrededor. Las direcciones locales son identificadas por el formato de prefijos 1111 1110 10. La dirección siempre comienza con FE80.

- Direcciones especiales: La dirección no especificada, o 0:0:0:0:0:0:0:0: indica la ausencia de una dirección, y por lo general se usa como fuente de dirección para los paquetes que están tratando de verificar la singularidad de una dirección tentativa.

- Direcciones de loopback: La dirección loopback, 0:0:0:0:0:0:0:1, define una interfaz loopback, lo que permite a un nodo enviarse paquetes a sí mismo. Es equivalente a la dirección loopback de IPv4 127.0.0.1.

- Anycast: Esta es aplicada a un conjunto de interfaces, Cuando un paquete es enviado en una dirección anycast se entrega a una interfaz, cualquiera del grupo, tomando en cuenta que dicha interfaz sea la más cercana de acuerdo con las medidas de distancia del protocolo de enrutamiento.

- Multicast: Esta es aplicada a un conjunto de interfaces, cuando un paquete es enviado en una dirección multicast, se entrega a un grupo de interfaces que pueden ser pertenecientes a distintos nodos y que son identificadas como dirección de multicast.

<u>Formato de la dirección ipv6</u>

La representación de las direcciones de ipv6 está compuesta por ocho grupos de cuatro dígitos hexadecimales. Con una longitud de 128 bits.

- Por ejemplo, 1001:0db8:85a3:08c3:1319:8a2e:0370:7334 es una dirección IPv6 correcta.

Si un grupo de cuatro dígitos es cero, como por ejemplo:

- 1001:0db8:85b3:**0000**:1319:8a2d:0370:7344

Si eliminamos esos ceros quedaría de la siguiente manera:

- 1001:0cb8:85b3::1319:8a2f:0370:7344

Los ceros que se encuentran al principio de un grupo de cuatro dígitos pueden ser omitidos:

- 1801:**0**DF8:**0**2ae::**0**f14, al eliminarlos quedaría de la siguiente manera:

- 9101:DF8:2ae::f14

En el caso siguiente que se presenta, que más de dos grupos son nulos de manera consecutivos:

- 8701:0CD8:0000:0000:0000:0000:1638:67ca

Existe la regla que pueden ser eliminados y se representaría de esta manera: 8701: 0CD8::1638:67ca

Diferencias de IPv6 sobre IPv4

A continuación, se presentara un cuadro en el cual se mostrarán las diferencias, de acuerdo con los temas que se consideren de mayor importancia dentro de cada una de las versiones de protocolo de Internet.

Gráfico #7. Diferencias y ventajas entre IPv4 y IPv6

Tema	IPv4	IPv6	Ventajas
Espacio de direccionamiento	2 ^ 32	2 ^ 128	Aumento de 32 bits a 128 con respecto a direcciones IPv4
Configuración	Manual o el uso de DHCP	Autoconfiguración (Play and plug) con o sin DHCP	Gastos menores de operación y tasa menor de errores

Broadcast Multicast	Utiliza ambos	No utiliza Broadcast , pero contiene diferentes formas de Multicast	Se provee un mejor aprovechamiento en el uso de ancho de banda
Anycast	No forma parte del ipv4	Contiene el método anycast	Permite nuevas aplicaciones con respecto a movilidad, y descentralización
Configuración de la red	La mayoría se hace manualmente y eso lo hace más laborioso	Facilita el cambio en la numeración de los host y enrutadores	Facilidad en la migración y menor tasa de gastos de la operación
Calidad de servicios	ToS utilizando DIFFServ	Clase de trafico y flujo etiquetas	Mayor control en la calidad de servicios
Seguridad	IPsec proporciona protección a los paquetes de datos	IPsec protege los datos y el control de los paquetes	Sistema completo de seguridad para proporcionar más seguridad en el entorno computacional
Movilidad	Utilización Móvil de lPv4	Proporciona una rápida entrega, una mejor optimización de enrutador	Mayor calidad y eficiencia en los diferentes servicios y escalabilidad.

Fuente: confeccionado por el autor del artículo

Estado de ipv6 a través del mundo

De acuerdo con IPv6Forum se logran identificar cinco regiones diferentes sobre el estado de ipv6, las cuales son:

a) *Asia:* En esta área, el impacto de la falta de direcciones IPv4 ha sido más obvio, y APNIC, la entidad de registro regional de Internet para esta región (espera agotar su rango de direcciones lPv4 en muy pocos meses. En correspondencia, la presión para encontrar soluciones adecuadas es muy alta, y se han iniciado gran número de actividades, particularmente en Japón: WIDE. KAME y TAHI.

b) *Europa:* La industria de la telefonía móvil es un soporte muy fuerte para la transición a lPv6. En correspondencia, ETSI (European

Telecommunications Standards Institute) y el Foro IPv6 han establecido un acuerdo de cooperación para unir sus fuerzas; este movimiento de ETSI ha sido tildado como impulsado por: "el fuerte deseo de los operadores inalámbricos". Además, de este acuerdo de cooperación con ETSI, el Foro lPv6 ha estrechado fuertes lazos con el Foro UMTS y la Asociación GSM, y hay conversaciones con el grupo 3GPP.

C) *Norteamérica:* Muchas actividades relacionadas con IPv6, tanto en términos de estandarización y despliegue/verificación, tienen sus orígenes en esta región. Muchas de estas actividades pueden ser localizadas en torno al "6bone", la "plataforma de pruebas" internacional de lPv6 (Otras actividades relacionadas con IPv6 que incluyen importante participación norteamericana son 6REN (iniciativa de coordinación para lPv6 en redes de investigación y educación), 6TAP (iniciativa para proporcionar un router lPv6 central en Chicago para facilitar la interconexión entre redes lPv6), y Frente/viagénie (iniciativa de túneles automáticos). En cualquier caso, el despliegue comercial de lPv6 en esta región se ha iniciado muy despacio; solo hay 2 rangos de direcciones lPv6 comerciales (de un total de 22 en todo el mundo) en Norteamérica. Esto refleja la apariencia de que el despliegue operacional de lPv6 "puede no llegar primero a éste área" (tal y como ha sido indicado en el encuentro 46° del IETF, grupo de trabajo lPng), ya que, los problemas de la falta de direcciones lPv4 aun no han emergido como una urgencia en esta región.

d) *Rusia:* Las fuertes relaciones entre el Foro IPv6, el Foro IPv6 local Ruso, y FREEnet (red académica y de investigación Rusa). El objetivo es crear una comunidad rusa de usuarios de lPv6 y proveedores de servicios y soluciones.

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

Implementaciones de IPv6

Este protocolo es aplicado dentro de diferentes tipos de hardware y software. A continuación, se mostrará una lista que muestra algunas de

las tecnologías que están aplicando el protocolo de Internet versión seis, en lo que respecta a host y routers.

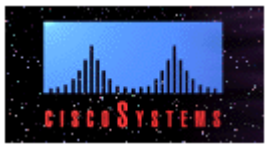
Gráfico #8. Implementaciones de IPv6 en Host

Host	
Tecnologías	**Implementaciones**
Apple Computer	Apple Computer se introduce a IPv6 y IPsec por medio de una implementación de un kit de desarrollo para Mac OS X.
BSD BERKELEY SOFTWARE DESIGN, INC. *Powering the Networked Economy™*	BSDI trabaja sobre una aplicación de Ipv6, además de eso BSDI esta participando en el proyecto 6BONE.
COMPAQ	Compaq Computer Corporation ha puesto en práctica el protocolo de Internet versión seis en las versiones de Alpha Tru64 UNIX y Alpha OpenVMS.
hp invent	Hewlett-Packard ha puesto en marcha HP-UX 11i IPv6 en Agosto del 2001. HP-UX 11i IPv6 es un producto totalmente compatible.
IBM	IBM Contiene muchos proyectos de aplicaciones para host planteados, como: • RS6000: AIX 4.3, Incluye soporte para IPv6 en su base de distribución. • S/390: Un prototipo de IPv6 MVS, esta aplicación está disponible para los mainframe.

Fuente: Playground.Sun.COM[4]

[4] http://playground.sun.com/pub/ipng/html/ipng-implementations.html

Gráfico #9. Implementaciones de IPv6 en Enrutadores

Enrutadores	
Tecnologías	**Implementaciones**
	**3Com Corporation** ha implementado IPv6 en el software para los routers NETBuilderII y PathBuilder S500 desde la versión 11.0 lanzada a finales de 1997.
	Cisco Systems's implementa IPv6 en Cisco IOS 2.2(2)T el 14 de Mayo del 2001. Soporta protocolos de enrutamiento, Unicast, servicios como: DNS, TFTP, etc.
	Nortel Networks' comienza implementando IPv6 en el lanzamiento del software BayRS versión 12.0 en la primera mitad de 1997.
	Teldat es un fabricante español de enrutador y un miembro del IPv6 Forum. Están desarrollando soporte IPv6 para sus enrutadores. La última versión disponible es la versión 1,0 Beta 0
	Zebra desarrollo de IPv6 enrutamiento de software llamado Zebra. Actualmente 2 de 4 conexiones a 6tap es realizada por el software de enrutamiento de Zebra. Se distribuye bajo licencia GNU GPL y funciona en Linux, * BSD, y el apoyo RIPng, BGP - 4 +, OSPFv3

Fuente: Playground.Sun.COM[5]

[5] http://playground.sun.com/pub/ipng/html/ipng-implementations.html

Conclusiones

En la actualidad, las redes de datos no solo son una estrategia de negocio, que brinda ventajas ante competidores, si no que alcanza un nivel de importancia que la hace indispensable para poder sobrevivir en el mundo de los negocios, el cual muestra cada día mayor competitividad y exigencia por parte de los consumidores.

Debido a tal exigencia se hace necesario avanzar en la tecnología y el mundo de la mano con ella. Estas nuevas creaciones permiten más flexibilidad para realizar diferentes actividades de trabajo de forma eficiente y segura.

El desarrollo de IPv6 no escapa al objetivo tecnológico de brindar mayores ventajas innovadoras. Las diferentes actualizaciones que acompañan este protocolo como: El protocolo de mensaje de control de Internet (ICMPv6), el cual es utilizado por IPv6 para mostrar errores que se producen durante el proceso de los paquetes, además, de la realización de diagnósticos por medio del ping a la capa de Internet, El descubrimiento de vecinos (ND) que realiza la función de darle a conocer a un nuevo nodo, los demás existentes dentro de una red. Además, incluye soporte para aplicaciones en tiempo real, selección de proveedores, seguridad extremo-extremo y auto-reconfiguración. Ipv6 está proyectada para correr en redes de alta velocidad y a la vez ser eficiente en redes de ancho de banda bajo.

Gracias a estas innovaciones y entre otras, Ipv6 provee mecanismos flexibles para la transición de la red actual Internet y fue diseñado para manejar los nuevos mercados, tales como los computadores personales nómadas, entretenimiento en redes y dispositivos de control.

El gran objetivo de implementación de este protocolo está enfocado obviamente a países donde no se obtienen direcciones ipv4 o países que están en desarrollo.

Sin embargo; a pesar de las grandes ventajas que conlleva este nuevo protocolo de Internet su implementación mundial llevará algunos años más para que llegue a jugar un papel tan importante, como lo ha hecho su futuro antecesor, además se presentarán algunas barreras que se solucionarán con el paso del tiempo, dentro de la implementación que según IPv6Forum son las siguientes:

- El problema de multi-homing,
- Los “fans” del direccionamiento ajustable en longitud,
- El propio IPv4, de alguna forma, con los “parches” como NAT,
- La falta de soporte real por parte de fabricantes de routers y software “dominantes”.
- La complejidad y costo de la migración/transición.
- Los usuarios necesitan razones comerciales “FORZADAS” para moverse al IPv6.

Como en todo gran proyecto se presentan barreras que retrazan su implementación, pero el momento de transición de un protocolo a otro se dará, debido a que es necesario hacerlo, no solo por el faltante de direcciones ipv4, si no para dar un salto adelante en el mejoramiento de servicios de telecomunicaciones. De esta forma IPv6 se convertirá en “La Internet del Próximo Milenio” según lo describe IPv6Forum.

Referencias bibliográficas

Cisco System, Inc, Academia de Networking de Cisco System (2004). Guía del primer año. CCNA 1 y 2. Person Education, S.A: Madrid, 2004

Cisco System, Inc, Academia de Networking de Cisco System (2004). Guía del primer año. CCNA 3 y 4. Person Education, S.A: Madrid, 2004

RAU, Red Académica Uruguaya (2005). Introducción de ipv6. Recuperado el 27 de Septiembre del 2007 de http://www.rau.edu.uy/ipv6/queesipv6.htm#02

Consultares inteligentes en Telecomunicaciones, ConsulinTel (2003). Situación Mundial de ipv6. Recuperado el 27 de Septiembre del 2007 de http://www.consulintel.es/Html/ForoIPv6/Documentos/Situación%20Mundial%20de%20IPv6.pdf

playground.sun (2003). Ipng-implementations. Recuperado el 27 de Septiembre del 2007 de http://playground.sun.com/pub/ipng/html/ipng-implementations.html

Consultares inteligentes en Telecomunicaciones, ConsulinTel (2003).RFCs de ipv6. Recuperado el 27 de Septiembre del 2007 de http://www.consulintel.es/Html/ForoIPv6/RFCs.htm

Wikipedia, La enciclopedia libre (s.f). Protocolo de Internet versión 6. Recuperado el 27 de Septiembre del 2007 de http://es.wikipedia.org/wiki/Ipv6

ipv6 Forum. (1999). Ipv6 Resources. Recuperado el 27 de Septiembre del 2007 de http://www.ipv6forum.org/modules.php?op=modload&name=Web_Links&file=index

IPv6 México (2007) Historia de ipv6. Recuperado el 27 de Septiembre del 2007 de http://www.ipv6.unam.mx