



## IP VERSI N 6: LA NUEVA GENERACI N IP

Edgar F. Pinillos T.

Desde los comienzos de la Internet ha sido muy r pida la evoluci n de este medio de comunicaci n de masas hasta llegar a la popularidad con que cuenta hoy en d a. Lo que comenz  como una red sobre todo, con fines experimentales, cient fico-t cnicos y, por supuesto, con objetivos militares en los Estados Unidos, ha terminado convirti ndose en uno de los m s populares sistemas de comunicaci n en el  mbito mundial del momento. Esto a creado una serie de nuevos desaf os que la comunidad tecnofila ha tenido que afrontar.

### UN POCO DE HISTORIA

A principios de los a os 70, dos cient ficos visionarios llamados Vinton G. Cerf y Robert E. Kahn, que trabajaban para la DARPA (Advanced esearch Projects Agency) del Departamento de Defensa de los Estados Unidos, fueron los encargados de liderizar un proyecto para interconectar los computadores de cierto n mero de Universidades repartidas por el pa s que realizaban proyectos cient ficos inform ticos de inter s para la Advanced Research Projects Agency (DARPA), llamado ARPANET.

Este proyecto dio inicio al desarrollo de la Arquitectura Base y los protocolos que hoy por hoy gobiernan la Internet. Teor as como la conmutaci n de paquetes, manejo de redes heterog neas y enrutamientos sin conexiones, comenzaron a sucumbir entre los investigadores debido a las grandes bondades y potencialidades que estas caracter sticas generaban.

Para el a o 1974, el dise o b sico Cerf – Kahn, del protocolo Internet (IP) fue publicado, convirti ndose en conjunto con un protocolo de capa superior llamado TCP, en el punto de partida para la explotaci n y uso de las redes de interconexi n. No fue sino hasta inicios de la d cada de los 90, que la Internet y su protocolo base TCP/IP, inici  su proliferaci n y uso masivo, cuando por primera vez inician operaciones dos compa as llamadas UUnet y Psinet como ISP (Internet Service Provider) en los Estados Unidos, consiguiendo la tecnolog a, crecimientos exponenciales nunca previstos en tan poco tiempo.

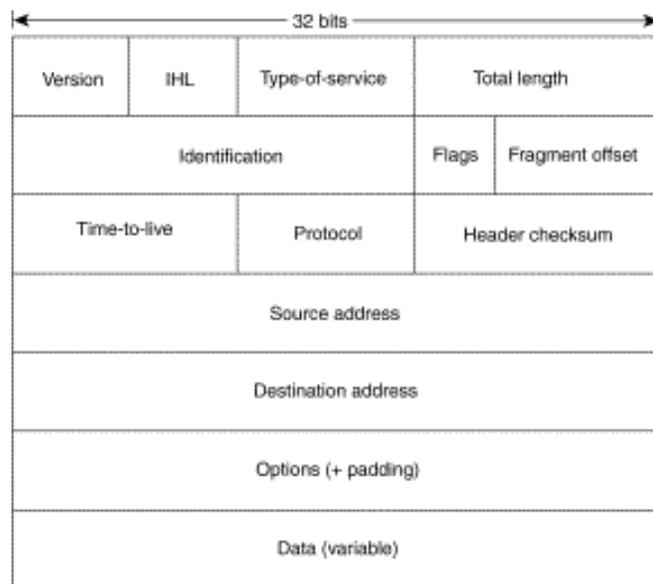
Desde entonces el Protocolo IP en su versi n actual 4 (IPv4), ha sido muy exitoso, por su dise o flexible y poderoso. Ha permitido que la Internet

maneje redes Heterogéneas, cambios bruscos en las tecnologías de hardware y aumentos enormes de escala.

De igual manera, con la multitud de nuevas aplicaciones en las que IPv4 a sido utilizado, sé a presentado la necesidad de desarrollar extensiones o añadidos al protocolo original, como lo son fundamentalmente medidas para permitir: Calidad de Servicio (QoS), Seguridad (IPSec) y movilidad.

Pero con el transcurrir del tiempo, la tecnología de redes a madurado considerablemente, han surgido nuevas aplicaciones y nuevos protocolos. De tal manera, que el protocolo IP (IPv4), sé esta quedando corto en el alcance de soportar estas nuevas tendencias tecnológicas.

Tanto es así, que ya se están presentando algunas limitaciones al funcionamiento de las redes actuales, como lo es fundamentalmente la inminente saturación del espacio de direcciones IP, por el abrupto crecimiento de la Internet, limitando el crecimiento de la misma; soporte inadecuado de las nuevas aplicaciones, ya que son más demandantes de factores como: tiempos de respuestas y disponibilidad de ancho de banda; y por último, la inminente necesidad de manejar altos grados de seguridad, pero de manera nativa, ya que IPv4 para manejar seguridad, se basa en protocolos (Patches) como IPSec (IP Security Protocol), SSL (Secure Sockets Layer), SHTTP (Secure HyperText Transfer Protocol), los cuales ninguno es un estándar.



*Formato de un Datagrama Ipv4*



Viendo esto, como un gran problema para el futuro de Internet y de las redes en general, la Organizaci n IETF (Internet Engineering Task Force) cre  un proyecto para la nueva generaci n del protocolo IP, llamado IPng (IP Next Generation) tambi n llamado IPv6, el cual se ha convertido en un est ndar para el sucesor de IPv4, desde que por primera vez la IETF se pronunciara el 25 de Julio de 1994, con su documento RFC 1752 "The Recommendation for the IP Next Generation". Recomendaci n que fue aprobada el 17 de Noviembre del mismo a o.

Este nuevo Protocolo de Internet (IPv6), se convierte en una evoluci n natural del protocolo anterior (IPv4), m s no es un cambio abrupto del mismo, ya que funciones que serv an en IPv4 se mantuvieron y mejoraron en IPv6, y funciones que no serv an se eliminaron, produciendo una serie de caracter sticas determinantes en la mejora del protocolo anterior.

### **PORQUE IPV6?**

Uno de los mayores desaf os, aunque no es el  nico, es el crecimiento abrupto a la que esta sometida la Internet. En los actuales momentos son ya m s de 200 millones de personas que acceden a este medio de comunicaci n y esto no representa m s del 2 por ciento de la poblaci n mundial, lo que nos indica que este dato crecer  de forma impresionante en los pr ximos a os.

El reducido espacio de las direcciones de Ipv4 ( $2^{32}$  bits), a pesar de disponer de cuatro mil millones de direcciones (4.294.967.296), junto al hecho de una importante falta de coordinaci n, durante la d cada de los 80, en la delegaci n de direcciones, sin ning n tipo de optimizaci n, dejando incluso grandes espacios discontinuos, nos esta llevando a limites no sospechados en aquel momento.

Por supuesto se podr a pensar en una soluci n que podr amos considerar como evidente, como ser a la reenumeraci n, y reasignaci n de dicho espacio de direccionamiento. Sin embargo, no es tan sencillo, es incluso impensable en algunas redes, ya que requiere unos esfuerzos de coordinaci n, a escala mundial, absolutamente impensable.

Adem s, uno de los problemas de Ipv4 permanecer a: la gran dimensi n de las tablas de enrutamiento en el troncal de Internet, que la hace ineficaz, y perjudica enormemente los tiempos de respuesta.



La falta de direcciones no es apreciable por igual en todos los puntos de la red, de hecho, no es casi apreciable, por el momento, en Norte América. Sin embargo, en zonas geográficas como Asia, y Europa, el problema se agrava.

Como ejemplos podemos citar el caso de China que ha pedido direcciones para conectar 60.000 escuelas, tan solo ha obtenido una clase B (65.535 direcciones), o el de muchos países Europeos, Asiáticos y Africanos, que solo tienen una clase C (255 direcciones) para todo el país.

Tanto en Japón como en Europa el problema es creciente, dado al importante desarrollo de las redes de telefonía celular, inalámbricas, modems de cable, xDSL, etc., que requieren direcciones Ip fijas para aprovechar al máximo sus posibilidades e incrementar el número de aplicaciones en las que pueden ser empleados.

La razón de la utilización de las direcciones IP por parte de los usuarios, esta pasando en pocos meses de 10:1 a 1:1, y la tendencia se invertirá. En pocos meses, podremos ver dispositivos siempre conectados, con lo que fácilmente un solo usuario podría tener, en un futuro no muy lejano, hasta 50 ó 100 Ip's (1:50 ó 1:100).

Algunos proveedores de Internet se ven incluso obligados a proporcionar a sus clientes direcciones IP privadas, mediante mecanismos NAT (traslación de direcciones, es decir, usar una sola IP pública para toda una red privada). De hecho, casi todos los ISP's se ven obligados a delegar tan solo reducidos números de direcciones IP públicas para sus grandes clientes corporativos.

Como ya he apuntado, la solución, temporalmente, es el uso de mecanismos NAT. Desafortunadamente, de seguir con Ipv4, esta tendencia no sería temporal, sino invariablemente permanente. Ello implica la imposibilidad práctica de muchas aplicaciones, que queden relegadas a su uso en intranets, dado que muchos protocolos son incapaces de atravesar los dispositivos NAT:

- RTP y RTCP (Real-time Transport Protocolo y Real-time Control Protocol) usan UDP con asignación dinámica de puertos (NAT no soporta esta traslación).
- La autenticación Kerberos necesita la dirección fuente, que es modificada por NAT en la cabecera IP.



- Ipv6 pierde integridad, debido a que NAT cambia la dirección en la cabecera IP.
- Multicast, aunque es posible, técnicamente, su configuración es tan complicada con NAT, que en la práctica no se emplea.

Por otro lado, factores como el desarrollo de nuevas aplicaciones de la Internet, que necesitan capacidades de direccionamiento y de enrutamiento más complejas. Como por ejemplo, aplicaciones que entregan audio y video, que necesitan hacerlo a intervalos regulares, es decir, entregar audio y video en tiempo real y, tendencias en surgimientos de interés por tecnologías de colaboración que ofrezcan comunicaciones entre grupo de colegas, parecida a una llamada telefónica en conferencia. Para todo esto, el protocolo actual no define servicios para tal fin, ni mecanismos que permitan tales funciones.

### **CARACTERÍSTICAS DE IPV6**

El nuevo protocolo IPv6, trae consigo características interesantes que resuelven muchos de los problemas del protocolo anterior. Pero en sí, conserva su esencia, ya que no es una sustitución completa del protocolo solo una evolución del mismo.

Por lo tanto, IPv6 conserva muchas de las características de diseño que hicieron a IPv4 tan exitoso. Como el IPv4, el IPv6 opera sin conexiones (cada datagrama tiene una dirección de destino y se enruta independientemente). Como el IPv4, la cabecera de cada datagrama tiene una cantidad máxima de saltos que pueden hacerse antes de descartarlo. De esta manera, otras características son conservadas y mejoradas, además de poseer nuevas características que los diferencian.

A continuación se describen las características más importantes de IPv6.

### **DIRECCIONAMIENTO**

Con un campo de dirección de 32 bits, es posible conseguir  $2^{32}$  direcciones, por lo que estaríamos hablando de aproximadamente unas 4 billones de direcciones. Esto para los años ochenta no era un problema, mucho menos el protocolo. Pero fue ya para los inicios de los años noventa, cuando comenzó la explosión de Internet, que se comenzó a vislumbrar, que bastarían esos 4 billones de direcciones. Por ende, unas de las características principales del nuevo IPv6, es el tamaño de campo para direccionar o identificar dispositivos.



Este campo es de 128 bits ( $2^{128}$ ), que proveen el espacio de direcciones lo suficientemente grande para manejar el crecimiento continuo de la Internet mundial durante muchas d cadas. Con esto se maneja un factor de  $2^{96}$  superior de lo que se tiene hoy en d a; lo suficiente para soportar hasta las ineficientes asignaciones que se pudieran dar en el transcurso del tiempo, tal cual como sucede hoy en d a.

## RENDIMIENTO

Hoy en d a, las redes LANs y WANs, est n progresando con respecto a las ratas de transmisi n que manejan, eso indica que ya se esta teniendo capacidad para utilizar ratas de cientos de megabits por segundo, con la tendencia de llegar hasta los varios gigabits por segundo. Todo esto, como respuesta a la mejora en las tecnolog as y las necesidades de ancho de banda por parte de los nuevos servicios y aplicaciones que est n surgiendo, en especial aplicaciones basadas en gr ficos. Algo que no se escapa de la Internet.

Con estas velocidades inmensas e incremento de carga, los Routers, deben de tener la capacidad de afrontar estas funciones lo m s r pido y eficiente posible, donde se pueda procesar y reenviar datagramas IP de manera r pida tanto para enlaces de alta velocidad como tambi n enlaces de baja velocidad, manteniendo siempre el buen desempe o.

Para conseguir este tipo de elementos es necesario manejar plataformas de hardware robustas, as  como tambi n juega un rol cr tico el dise o IP que se tenga.

Por tal raz n IPv6, trae consigo tres aspectos de dise o que contribuye a mejorar el rendimiento en las interredes:

- La simplificaci n de la cabecera Ip, reduciendo los trece campos que estaban en IPv4, a solo 7 campos. El n mero de opciones se ponen en cabeceras separadas. La mayor a de estas cabeceras opcionales no son examinadas ni son procesadas por cualquier enrutador en el camino del paquete. Esto simplifica y acelera el procesamiento de los paquetes IPv6 comparado con los datagramas IPv4.
- La cabecera del paquete IPv6 es de longitud fija mientras que la cabecera IPv4 es de longitud variable. Una vez m s el dise o IPv6 simplifica el proceso.



- La fragmentación no está permitida en los Routers IPv6. La fragmentación solo puede ser realizada por el origen.

### **SERVICIOS DE RED**

El manejo de tráfico multimedia, es vagamente soportado con IPv4 con su campo Tipo de Servicio. Para las aplicaciones de hoy en día se requiere mucho más. Por esto IPv6, incluye un mecanismo que permite a un transmisor y un receptor establecer una trayectoria de alta calidad por la red y asociarle los datagramas, garantizando el alto desempeño a aplicaciones de audio y video en tiempo real.

IPv6 permite el etiquetado de los paquetes que pertenecen a un flujo de tráfico en particular para la cual el origen solicita un manejo especial.

### **CAPACIDAD DE SEGURIDAD**

En la Internet se presentan un gran número de problemas de seguridad, y una carencia de políticas efectivas y mecanismos de autenticación confiables.

IPv4 por si solo no provee capacidades de seguridad, se tiene que complementar con servicios como IP-Sec, para proveer niveles de seguridad sin que la aplicación posea capacidad de seguridad.

Para remediar esta situación IPv6 proporciona soporte nativo para seguridad basándose en sus cabeceras de extensión. Por medio de las cabeceras de autenticación y la cabecera de encapsulamiento seguro, se logra proveer diferentes niveles de seguridad para diferentes usuarios. Esto es muy importante ya que diferentes comunidades de usuarios tienen diferentes necesidades de seguridad.

El primer mecanismo, llamado Cabecera de Autenticación, es una cabecera de extensión que provee de autenticación e integridad a los datagramas IPv6, ya que se asegura que un paquete este viniendo realmente de un emisor indicado en la dirección de origen del datagrama. Esta autenticación es especialmente útil para asegurarse contra intrusos que configuran un equipo principal para generar los paquetes con direcciones de origen forzadas. El algoritmo propuesto para trabajar con esta cabecera de extensión es el MD5, para ayudar a asegurar la interoperabilidad con la Internet mundial.



La segunda cabecera de extensión llamada, cabecera de encapsulamiento seguro, provee mecanismos de integridad y confidencialidad end-to-end para datagramas IPv6, de manera flexible e independiente del algoritmo. Esta cabecera de extensión proporciona campos que llevan llaves de encriptación y otras informaciones relevantes, permitiendo el cifrado interoperable de paquetes IP.

### **CALIDAD DE SERVICIO**

La calidad de servicio en IPv6, es un servicio más robusto que el provisto por datagrama llamados, Prioridad (priority –4 bits-) y Etiqueta de Flujo (Flow Label –24 bits-). Estos, son usados para que un host pueda identificar los paquetes, para el cual se requiere un manejo especial por parte de los routers IPv6. Esta capacidad es importante, para el momento de soportar aplicaciones que requieren el menor grado de retardos, delay o alteraciones en el flujo. Estos tipos de aplicaciones son comúnmente descritas como aplicaciones multimedia o de tiempo real.

El enrutamiento basado en flujo, le podría dar a las interredes algunas de las características determinísticas asociadas con tecnologías de conmutación orientadas a conexión y circuitos virtuales telefónicos.