Capítulo 1

Protocolo de Internet Versión 6

La nueva versión del protocolo de internet tiene características novedosas y actualizaciones con respecto a su versión predecesora que es la que seguimos usando hoy en día. Por lo cual es importante conocer dichas características internas y saber a qué retos se enfrenta este nuevo diseño, por lo cual en este capítulo se hará una exposición del mismo.

Capítulo 1 Protocolo de Internet versión 6 (IPv6)

Esta versión del protocolo de Internet está diseñada para cubrir las actuales limitaciones del protocolo en su versión 4 (*IPv4*) además de proveer mejoras como un mayor espacio para direcciones al pasar de 32 bits en IPv4 a los 128 de IPv6, simplificaciones en los formatos de encabezados, soporte mejorado para el campo de opciones, capacidades nativas de calidad de servicio, servicios de autenticación y cifrados incluidos, auto configuración de direcciones, mejor soporte a la movilidad para dispositivos y usuarios, tráfico multimedia en tiempo real, etcétera.

Además se han desarrollado mecanismos de transición que nos garantizan la coexistencia de ambas versiones del protocolo durante la transición a la última versión.

Actualmente la necesidad de intercambiar información, el crecimiento de la Internet como la red de redes más usada, así como los requerimientos de una mejor seguridad hacen que el uso del IP en su cuarta versión sea cada vez más difícil de manejar. Añadido a esto, la red de redes está inmersa en un medio de una rápida evolución, con tendencia a las modificaciones inmediatas e inseguras, con demandas cada vez más amplias de servicios que garanticen la seguridad y fiabilidad de uso. En nuestros días, donde se garantiza que el agotamiento del espacio disponible de direcciones IPv4 está más cercano, el uso de alternativas, como el *NAT (network addres translation)* y *CIDR (classless inter-domain routing),* además de consideraciones de orden político o de índole económicas no totalmente claras por parte de los actores involucrados en el área de las telecomunicaciones, tanto de la iniciativa privada como de la administración pública han provocado el aplazamiento de dicha transición.

Para propósitos históricos mencionaremos que los principales arquitectos de IPv6 fueron Steve Deering y Robert Hinden.

Un rol importante en el campo del desarrollo e implementación del IPv6 lo han jugado las redes académicas, las cuales han estado generalmente interesadas en el desarrollo y no tanto en las ganancias económicas. Esto ha traído experiencia y recursos humanos capacitados para el desarrollo futuro.

En los últimos años se ha visto un incremento en el número de dispositivos que incluyen capacidades de soporte para el IPv6. Otras regiones del mundo claramente están apoyando el uso de la próxima versión del protocolo, entre ellas Asia y Europa, en la primera región, su tardía inclusión en la red de redes provocó que le fuera asignada una menor cantidad de direcciones en IPv4, lo cual sumado al rápido crecimiento y evolución tecnológica de dicha parte del mundo provoca un agotamiento acelerado de sus direcciones disponibles, y en la segunda región, la Europea, la dorsal (*backbone*) académica del proyecto GÉANT provee soporte oficial para IPv6 desde enero de 2004.

En el mundo existen varias organizaciones que se han encargado del desarrollo del protocolo como son el IPv6 Forum, que es un consorcio formado por proveedores de soluciones, proveedores de servicio de Internet (*ISPs*) además de redes de académicas y de investigación, el cual tiene como misión promover a nivel mundial el uso del IPv6.

En la UNAM existe un grupo de trabajo encargado de promover IPv6, coordinando a su vez a los grupos correspondientes en la Corporación de Universitaria para el desarrollo de Internet (*CUDI*) cuya misión es la de promover y coordinar el desarrollo de redes de telecomunicaciones y cómputo enfocadas al desarrollo científico y educativo en México, así como en la Cooperación Latinoamericana de Redes Avanzadas (*CLARA*) con objetivos similares en toda la región.

En estos momentos IPv6 está siendo considerado clave en el desarrollo de tecnologías como las comunicaciones ubicuas, los servicios multimedia VoIP, las redes punto a punto, etcétera. IPv6 tendrá unos 15 años muy pronto, en los cuales se ha estado robusteciendo y expandiendo sus campos de aplicación hasta abarcar varios como son los ambientes de colaboración a distancia, tecnologías de ubicuidad como los servicios de paquete vía radio[transferencia] (*GPRS*, por sus siglas en inglés), televisión de alta fidelidad (*HDTV*), control remoto de distintos dispositivos, aplicaciones sobre protocolos inalámbricos, enlaces mediante cable eléctrico (*PLC*, por sus siglas en inglés), conexiones domésticas por vía telefónica o fibra, aplicaciones sobre demanda en línea (juegos, colaborativas, etc.), tecnologías always-on (tales como *xDSL*, fibra y más), todo lo anterior son solo algunos de los campos sobre los que se han desarrollado aplicaciones para el protocolo de Internet en sus 2 versiones.

En nuestros días, la primer década del siglo XXI, las redes experimentales han dejado de serlo para volverse redes de producción, madurando la nueva actualización de la pila del protocolo TCP/IP de tal manera que ya se pueden tener una variedad de servicios para astronomía, bibliotecas digitales, educación a distancia, ciencias de la tierra y de la vida, campos colaborativos, laboratorios remotos, robótica, súper cómputo, telemedicina, visualización, cómputo científico y muchos más.

1.1 Datagrama en IPv6

El método por el cual IPv6 encapsula el tráfico recibido a través de los protocolos de las capas inferiores es, básicamente, el mismo que se utiliza para IPv4. Mientras que el uso de datagramas no ha cambiado, para IPv6 se han realizado algunas modificaciones a la estructura y al formato. El incremento de tamaño en las direcciones IP de 32 a 128 bits, llevó a un incremento de información en el encabezado. Todo lo cual condujo a promover el retiro de los campos que en el protocolo eran redundantes o que no eran estrictamente necesarios. Además se introdujeron cambios y nuevas características para mejorar la interacción del protocolo con la interconexión actual. Los cambios más significativos en el encabezado IPv6 son los siguientes:

•Estructura de encabezados múltiples

En vez de contener un solo encabezado que contenga todos los campos para un datagrama (que posiblemente incluyera opciones), el datagrama IPv6 soporta un encabezado principal y encabezados de extensiones para la información adicional, cuando se requiera.

•Formato simplificado de encabezamiento

Algunos campos han sido removidos del encabezado principal para reducir su tamaño y mejorar su eficiencia. Sólo los campos que son requeridos por la mayoría de los datagramas permanecen en el encabezado principal; otros has sido trasladados a los encabezados de extensión y serán utilizados bajo demanda; y otros fueron removidos porque ya no eran necesarios.

•Campos Renombrados

Algunos campos han sido renombrados para reflejar mejor su uso actual en las redes modernas.

•Mayor Flexibilidad

Los encabezados de extensión permiten una mayor cantidad de información adicional cuando sea requerida.

•Eliminación del cálculo de la suma de verificación

Para esta actualización del protocolo ya no se calculará la suma de verificación en el encabezado. Esto ahorra tanto el tiempo de cálculo gastado por cada dispositivo que empaquetaba datagramas IP (hosts y ruteadores) y el espacio que el campo de la suma de verificación ocupaba en el encabezado IPv4.

•Calidad de Servicio mejorada

Un nuevo campo, el campo de flujo, se ha agregado para ayudar en la jerarquización de tráfico.

El encabezado principal en IPv6 contiene información de control y localización que será usada en el procesamiento y ruteo de un datagrama, y su longitud final es de 40 bytes. Los campos que conforman el encabezado principal son los siguientes:

•*Versión (4 bits):* indica la versión IP usada para generar el datagrama.

•*Clase de tráfico(8 bits):* este campo reemplaza al de tipo de servicios (*TOS*) del encabezado IPv4. No se usa de la manera en que se usaba TOS (con precedencia, bits D, T y R), sino usando ahora el método de los servicios diferenciados (*DF)*, definidos en el RFC 2474, para distinguir e identificar entre diferentes clases o prioridades en los paquetes.

•*Etiqueta de flujo (20 bits):* fue creado para proveer soporte adicional para los datagramas que utilizan las características de tiempo real y calidad de servicio.

•*Longitud de la carga útil(16 bits):* mide la longitud de los encabezados de extensión, ya no se toma en cuenta el encabezado principal como en IPv4.

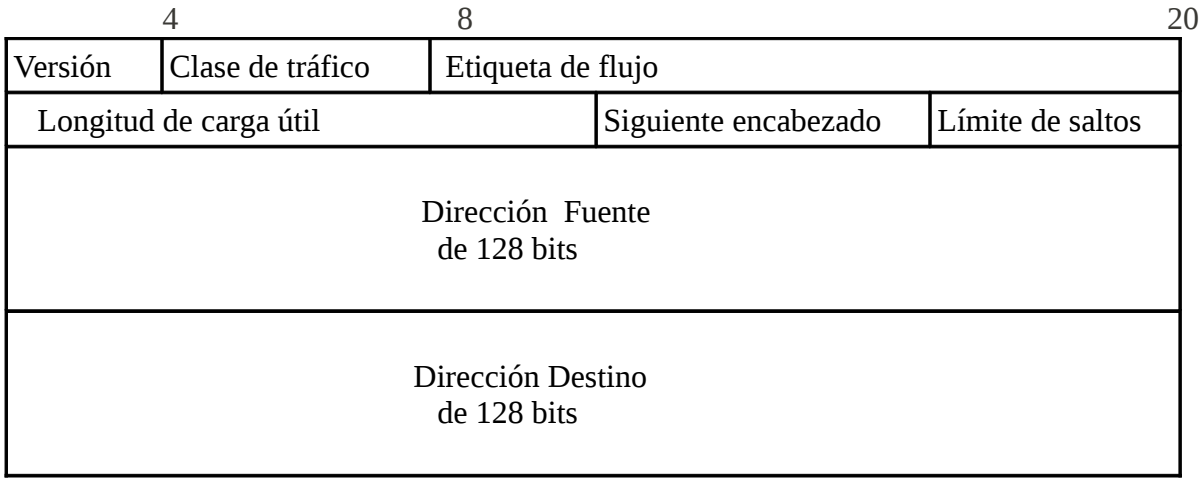
•*Siguiente encabezado(8 bits):* sirve para identificar al siguiente encabezado que sigue al encabezado principal.

•*Límite de saltos(8 bits):*reemplaza al campo *TTL* del encabezado IPv4, con su nueva denominación refleja mejor el objetivo de su trabajo, en tanto que cuenta saltos, no tiempo.

•*Dirección origen(128 bits):* la dirección IPv6 de 128 bits del origen del datagrama.

•*Dirección destino(128 bits)*:la dirección IPv6 de 128 bits del destinatario del datagrama, unicast, multicast o anycast.

Todo lo cual se puede observar en el cuadro 1, la imagen del datagrama que se tiene para IPv6.



Cuadro 1. “Datagrama IPv6”

1.2 Encabezados de IPv6

En esta actualización de la pila del IP, se tiene sólo un encabezado principal y toda la información adicional que requiera un paquete estará contenida en los llamados encabezados de extensión, los cuales fueron creados en un intento de proveer de eficiencia y flexibilidad a los datagramas IPv6. De acuerdo con el RFC 2460 los encabezados de extensión (EH) deberán ir en el siguiente orden y con el código asignado en el encabezado de *siguiente encabezado*. En la Tabla 1, mostramos los encabezados que se están manejando actualmente para IPv6, así como la existencia de

encabezados experimentales.

	Tipo de encabezado	Código asignado.
1	Encabezado principal IPv6.	-
2	Encabezado de opciones salto a salto.	0
3	Encabezado de opciones de destino (con opciones de enrutamiento).	60
4	Encabezado de enrutamiento.	43
5	Encabezado de fragmentación.	44
6	Encabezado de autenticación.	51
7	Encabezado de carga de seguridad de encapsulamiento.	50
8	Encabezado de opciones de destino.	60
	Encabezado de movilidad (*RFC5096 experimental*).	135
	Encabezado de sin siguiente encabezado .	59
9	Encabezado de protocolo de capa superior (TCP, UDP, ICMPv6).	(6, 17, 58)

Tabla 1. “Encabezados en IPv6”

Encabezado de extensión salto a salto

Este encabezado se usa para dar soporte a los jumbo-datagramas o, con la opción de alerta de enrutamiento, en parte integral de la operación MLD (*Multicast Listener Discovery*) RFC2710 MLDv1 1999, RFC3810 MLDv2 2004 y RFC4604 IGMPv3 & MLDv2 2006

Encabezado de opciones de destino

Se usa para la movilidad en IPv6, así como para otras aplicaciones. Únicamente el nodo destino del paquete lo examina y no todos los nodos intermedios en la ruta.

Encabezado de enrutamiento

Se usa en la movilidad IPv6 y en enrutamiento por origen. Podría ser necesario deshabilitar en los enrutadores la opción de enrutamiento por origen IPv6 para proteger contra ataques de denegación [de servicios] distribuida (*DDoS*).

Encabezado de fragmentación

Es fundamental en el uso de comunicaciones que usan paquetes fragmentados (en IPv6, el tráfico origen debe realizar la fragmentación, los nodos intermedios no.)

Encabezado de autenticación

Es similar en formato y uso al encabezado de autenticación usado en IPv4, definido en el RFC2406. No proporciona una garantía de confidencialidad de los datos ya que no provee el cifrado de los mismos, se usa para garantizar la autenticación e integridad, además de la anti-réplica de los paquetes IP.

Encabezado de carga de seguridad de encapsulamiento

Toda la información que lleve el encabezado de seguridad de encapsulamiento (*ESP*) es cifrado y por tal razón es inaccesible para enrutadores intermedios de la red. Se usa para proporcionar confidencialidad, especificando el modo de cifrar los datos y cómo se incluirá el contenido en el paquete IP. También tiene la capacidad de ofrecer autenticación del origen, integridad y anti-réplica de la información contenida.

1.3 Direccionamiento IPv6

Una de las principales motivaciones que llevaron a la creación de IPv6 fue la rectificación de problemas creados por la asignación de direcciones en IPv4.

Se requerían más direcciones, pero mucho más que eso, se deseaba que fuera una manera contemporánea y que reflejara un manejo de redes actuales. En base a esto, no es sorprendente los múltiples cambios que se dieron en el direccionamiento IP. El esquema de direccionamiento es similar en concepto al que se manejó para IPv4, pero fue completamente rediseñado para soportar una red en continuo crecimiento y con nuevas aplicaciones en el porvenir.

Algunos de los aspectos que se conservan, con respecto al modelo anterior, son:

- El ruteo y la identificación de la interfaz de red. El ruteo se lleva a cabo a través de la estructura de direcciones en la red.

- Las direcciones IPv6 están asociadas con la capa de red , del modelo OSI, en las redes TCP/IP, que son distintas de las direcciones físicas de la capa de enlace.

- La interpretación de direcciones y la representación de los prefijos, esto es, las direcciones IPv6 son como las direcciones sin clase (*classsles*) en IPv4, en que son interpretadas con un identificador de red *(NetID)* y un identificador de cliente *(HostID*), un número de prefijo de longitud, usando una notación parecida a la usada en *CIDR* usada para identificar la longitud del identificador de red.

De los cambios que se introdujeron en IPv6, el más celebrado es el incremento en tamaño de las direcciones IP, y por resultado el incremento en el espacio de direcciones disponibles.

En IPv4, las direcciones se componen de 32 bits, los cuales están agrupados en cuatro octetos de bits. El incremento de 32 a 128 bits incrementa este espacio hasta cantidades astronómicas, y con lo cual se pierde la facilidad nemotécnica que se tenia en la versión anterior del IP. Un problema que surge al querer usar la anterior notación , que agrupaba octetos, en notación decimal, es que en esta nueva versión del IP en vez de tener 4 de estos octetos tendríamos 16, con lo que se hace *humanamente* imposible de manejar.

Es por esto que se eligió la notación hexadecimal para la representación de las direcciones IPv6, con lo cual se logra que sean *humanamente* más manejables. En el cuadro 2, se muestran las notaciones existentes y sus variantes.

	0		32		64		96				128
únicamente hexadecimal	805B	2D9D	DC28	0000	0000	FC57	D4C8		1FFF		
ceros suprimidos	805B	2D9D	DC28	0	0	FC57	D4C8		1FFF		
ceros comprimidos	805B	2D9D	DC28	::		FC57	D4C8		1FFF		
notación hibrida	805B	2D9D	DC28	::		FC57	212	200	31	255	

Cuadro 2. “Distintas notaciones existentes para IPv6”

Como se puede apreciar en el cuadro 2, la notación utilizada para las direcciones en IPv6 dista mucho de ser fácilmente manejable, pero ahorrará muchos problemas que se tendrían si se siguiera manejando la notación decimal o binaria. Se muestran las notaciones que se permiten utilizar, los atajos de los que se puede hacer uso si se presentan los casos que correspondan y la última es la notación híbrida que dejaría utilizar la notación decimal habitual en IPv4 embebida en la notación para las direcciones en IPv6.

Los motivos principales que se tomaron en cuenta para dividir el espacio de direcciones en IPv6 fueron asignaciones y ruteo. Esto es, se intento hacer la asignación de direcciones lo mas sencillo posible, ya sea a los proveedores de servicio (*ISP's*), a las organizaciones o a los usuarios finales.

Inicialmente se tenía pensado usar un formato de prefijo (*FP*), se quería dividir el espacio de direcciones IPv6 en bloques variables para diferentes propósitos, aunque rápidamente se dieron cuenta que se empezaría a considerar que el uso de los formatos de prefijo sería el equivalente a las clases de direcciones en IPv4.

Entonces se decidió que los implementadores de hardware con soporte para IPv6 realizarán las decisiones de ruteo en base a los primeros bits de las direcciones. Esto es como IPv6 se suponía que ***no*** debía trabajar, porque se supone que las ubicaciones de estas direcciones están sujetas a cambios y modificaciones. Asi que se decidió remover el término “formato de prefijo” de la norma.

Formato de direcciones IPv6 Unicast Globales

Se anticipaba que las direcciones que más se usarían en IPv6 fueran las direcciones unicast, y es por esta razón que la vasta mayoría del espacio de direcciones IPv6 se dedica a este tipo de direcciones. Un octavo del enorme espacio de direcciones IPv6, las cuales son indicadas por la cadena “001” en los primeros tres bits de la dirección. Surgió la cuestión de como utilizar los 125 bits restantes de las direcciones. Cuando IPv4 fue diseñado, el modelo de asignación de direcciones se basó en una entidad central: la *IANA*. Cualquier organización que deseara obtener un bloque de direcciones se lo tenía que solicitar a esta autoridad central. Pero esto se volvió rápidamente impráctico. Los diseñadores de la nueva versión de la pila de protocolos TCP/IP tuvieron esto en cuenta y se implementaron ventajas en el diseño de las direcciones en IPv6 para reflejar mejor la topología de la red de redes. Algunas de estas fueron:

- Facilidad de ubicación de bloques de direcciones a varios niveles de la jerarquía topológica de Internet.

- Direcciones IP que reflejen automáticamente la jerarquía en que mueven información los enrutadores, permitiendo a los mismos ser facilmente agregables para un ruteo más eficiente.

- Flexibilidad para que las organizaciones, como los proveedores de servicio (*ISP's*), puedan subdividir sus bloques de direcciones para los usuarios.

- Flexibilidad para las organizaciones de usuarios finales para subdividir sus bloques de direcciones para adaptarse a redes internas, tal como hicieron las subredes en IPv4.

- Mayor significado a las direcciones IP, en vez de ser solo una cadena de 128 bits sin significado, es posible observar una dirección y obtener cierta información de ella.

En IPv4, la dirección IP no tiene relación alguna con las tecnologías de red subyacentes de la capa de enlace. Un cliente se puede conectar a una red TCP/IP usando una interfaz de red Ethernet (*NIC*) la cual tiene una dirección física (*MAC*) y una dirección lógica IP, y se puede observar que ambos números no tienen relación alguna de ningún tipo.

Asi con la completa remodelación practicada en las direcciones para IPv6, se aprovechó para poder incluir este nuevo esquema de mapeo de las direcciones físicas como parte de las direcciones lógicas. Con 128 bits, y aún con 45 bits reservados para el prefijo de red y 16 bits para las subredes, quedan 64 bits para usarlos en el identificador de interfaz, análogo este al *hosts ID* bajo IPv4.

Asi como en IPv4 existen direcciones que están reservadas, o son privadas, una pequeña parte del espacio de direcciones IPv6 ha sido designada para direcciones especiales. El propósito de estas direcciones y bloques de direcciones es el de proveer direcciones para propósitos especiales y privados en redes IPv6. Algunos tipos de estas direcciones especiales suelen ser :reservadas, privadas , no específicas y el loopback.

Una porción del espacio de direcciones IPv6 fue reservado por el IETF. A diferencia de IPv4, el cual tiene reservados varios bloques en distintas ubicaciones a lo largo de su espacio de direcciones, en IPv6 el bloque reservado está al principio del espacio de direcciones, aquellos que comienzan con “0000 0000” (o 00 para el primer octeto hexadecimal). Esto representa $\frac{1}{256}$ del total del espacio de direcciones. Las direcciones *IPv4 embebidas* también se encuentran aquí.

IPv6 es compatible con su antecesor IPv4, por ejemplo, para comunicar “islas” de IPv6 con redes IPv4, se pueden emplear túneles. Para soportar la compatibilidad IPv4/IPv6, se desarrolló un esquema para permitir las *direcciones embebidas IPv4* en la estructura de direcciones IPv6. Se usan dos formatos de direcciones embebidas para poder indicarle las capacidades del dispositivo que usa las direcciones embebidas.

Las direcciones IPv4 compatibles con IPv6 son direcciones especiales asignadas a los dispositivos con capacidades IPv6, como aquellos que son de pila doble (*dual stack*) los cuales tienen la capacidad de manejar ambas versiones del protocolo. Asi se podría ver una dirección que se formara con la parte decimal que es la dirección en IPv4 más la parte que se formaría con la dirección en IPv6, como se observa en el cuadro 3.

	0	32	64	96	128
dirección IPv6 en notación hibrida	0 0	0 0	0 0	132.248	59.73
dirección IPv6 en notación comprimida	::132.248.59.73				

Cuadro 3. “Dos formas de notaciones en direcciones IPv6”

Uno de los cambios más significativos en el modelo general de direcciones IPv6 fue la modificación a los tipos básicos de direcciones y como son usadas. Las direcciones *unicast* son la opción para la mayoría de las comunicaciones, así como en IPv4, pero los métodos para las direcciones son diferentes en IPv6. Las direcciones tipo *broadcast* como tipo especial han sido eliminadas. En contraparte, el soporte para las direcciones tipo *multicast* se ha expandido y también aparece un tipo de direcciones nuevo, las direcciones *anycast* que también se pueden usar en IPv4.

Las direcciones tipo *multicast* permiten a un sólo dispositivo mandar datagramas a un grupo de receptores. IPv4 también ofrece soporte a las direcciones tipo *multicast* usando el bloque de direcciones de clase D. En IPv6 este tipo de direcciones se ubican en el bloque *multicast*. Este es $\frac{1}{256}$ del espacio de direcciones que tiene IPv6, que consisten de las direcciones que comienzan con “1111 1111”. Asi cualquier dirección que comience con FF en notación hexadecimal es una dirección *multicast* IPv6.

El formato para las direcciones multicast se observa en la tabla 2.

Campo	Tamaño	Descripción
Indicador	8	Los primeros ocho bits son siempre “1111 1111” para indicar una dirección *multicast*
Banderas	4	Cuatro bits son reservados para el uso de las banderas que pueden indicar la naturaleza de la dirección multicast. En la actualidad los primeros tres de estos bits están en desuso y se ponen en ceros. El cuarto en la bandera “T” (*Transient*). Si está en cero esto indica que la dirección multicast está permanentemente asignada. Si está en uno, significa que una dirección multicast no permanente.
Scope ID	4	Estos cuatro bits permiten tener 16 diferentes valores. Los cuales nos darán una variedad de opciones de alcance, como pueden ser las direcciones globales para toda la Internet o restringidas a una pequeña esfera en particular como pudiera ser una organización.
ID de Grupo	112	Define un grupo en particular

Tabla 2. “Formato para direcciones multicast”

Otra de las características interesantes y de importancia en IPv6, es la capacidad que se le otorga a los dispositivos para autoconfigurarse. En la anterior versión del protocolo, IPv4, es necesaria una configuración manual o en su defecto utilizar mecanismos como DHCP que permiten asignar direcciones, en IPv6 esto se lleva varios pasos más adelante y se permite configurar la dirección IP automáticamente y otros parámetros sin la necesidad de un servidor. También se tiene el mecanismo para reasignar las direcciones (*renumbering*).

Otra de las muchas mejoras introducidas en IPv6 es el mecanismo para administrar dispositivos IP, incluyendo la configuración del cliente. Los dos mecanismos son :

1. ***Autoconfiguración sin estado(stateless)***: un método que permite que el dispositivo se configure así mismo sin intervención de un servidor y mediante un ruteador.

2. ***Autoconfiguración con estado(statefull)***: en este método la configuración del cliente es provista por un servidor.

La *autoconfiguración sin estado (stateless) y la reasignaciones* se define en el RFC 2462, además implementa varias de las nuevas características que trae consigo el IPv6, las cuales incluyen las direcciones locales *(link-local, que es una de los dos tipos de direcciones locales que se tienen), multicast, el protocolo de descubrimiento de vecinos (neighbor discovery [ND] protocol) y la capacidad de generar el identificador de interfaz por medio de la dirección perteneciente a la capa de enlace*, la MAC.

Lo siguiente es un sumario de los pasos tomados cuando se usa la *autoconfiguración sin estado*:

- Generación de direcciones de enlace local (***link-local***): Para el caso de las direcciones de autoconfiguración sin estado estas tienen en sus primero diez bits una cadena del tipo “1111 1110 10”. La dirección generada usa estos diez bits seguidos de 54 ceros y los 64 bits pertenecientes al identificador de interfaz. Usualmente esto se derivará de la capa de enlace, de la dirección MAC o será un “token” generado de alguna otra manera.

- Prueba de unicidad de las direcciones de enlace local (***link-local***): El nodo verifica que la dirección generada no está siendo ocupada por algún otro dispositivo en la red local. Se manda un mensaje de solicitud de vecindad (*neighbor solicitation*) usando el protocolo *neighbor discovery*, el cual escucha por una advertencia de vecindad (*neighbor advertisement*) en respuesta a la verificación que otro dispositivo ya esta usando dicha dirección de enlace local, con lo cual, otra dirección deberá ser generada, o la autoconfiguración falla y otro método deberá ser utilizado.

- Asignación de dirección de enlace local(***link-local***) : asumiendo que se pase una prueba de unicidad de dirección de enlace local, el dispositivo asignará la dirección de liga local a su inetrfaz IP. Esta dirección puede ser usada para comunicación en la red local, pero no hacia la Internet, porque las direcciones de enlace local no son ruteables.

- Enrutador de contacto(***Router Contact)***: el siguiente nodo intentará realizar contacto con el enrutador local para obtener más información acerca de la configuración. Esto se realiza tanto escuchando los mensajes de anuncio de enrutador (*router advertisement*) enviados periódicamente por los enrutadores.

- Enrutador de dirección(***Router Direction***): este enrutador provee de dirección al nodo para proceder con la autoconfiguración, si en esta red se usa la autoconfiguración con estados y/o advertir la dirección del servidor DHCP que si se está usando. Opcionalmente le debe de indicar al cliente como determinar su dirección global de Internet.

- Configuración de la dirección global: asumiendo que la autoconfiguración sin estado esté en uso en la red, el cliente se autoconfigurará con su dirección de Internet global única. Esta dirección está formada por un prefijo de red, que proveerá el ruteador al cliente, combinada con el identificador del dispositivo como se comentó anteriormente.

Este método tiene muchas ventajas sobre las configuraciones manuales o en base a un servidor, y es particularmente útil en el soporte de dispositivos móviles, los cuales se desplazan por varias redes y pueden adquirir direcciones válidas sin necesidad de conocer los servidores locales o prefijos de red.

La reasignación de direcciones (***renumbering***) es un método relacionado con la autoconfiguración. Como la configuración de un cliente, se puede implementar usando protocolos como DHCP, a través del uso de direcciones IP otorgadas temporalmente que expiren después de un tiempo. Bajo IPv6, las redes pueden ser reasignadas teniendo en los enrutadores intervalos que expiren para prefijos de red cuando la auto-configuración este realizada.

Dada la importancia de la pila de protocolos TCP/IP y lo significativos que están siendo los cambios realizados en IPv6, este cambio no está ocurriendo de una una sola vez, se está dando una transición y la coexistencia de ambas versiones del IP.

1.4 Mecanismos de transición de IPv4 a IPv6

Pila Dual (*Dual Stack*):

Este es uno de los mecanismos de transición que se tienen, en el cual se soportan ambas versiones del protocolo tanto IPv4 como IPv6.

Túneles (Tunnels): Para este mecanismo de transición se permiten dos tipos de túnel

- Automáticos

  Las direcciones IPv6 de los hosts alcanzables deben ser compatibles con IPv4. Asi mismo las direcciones IPv4 que se usen para formar direcciones IPv6 deberán ser enrutables. Establecer túneles automáticos entre cualquier par de hosts IPv6, cuyas direcciones IPv6 sean compatibles con IPv4 permite a los hosts el encapsulamiento IPv6 en IPv4 en puntos finales, sin que se requiera a los enrutadores que estén en la ruta que soporten IPv6.

- Manualmente configurados

  Estos túneles son establecidos y configurados manualmente. Los túneles configurados manualmente no requieren de las direcciones compatibles con IPv6 ni compatibilidad con IPv4.

1.5 Ruteo en IPv6

En el enrutamiento en IPv6 es de notar que el anuncio de enrutador (***router advetisement***) es una de las áreas más importantes de la operación del protocolo y que no tiene análogo en IPv4. Es un mecanismo que provee información de configuración a los hosts de la red. Se pueden ajustar algunos parámetros para que respondan a situaciones específicas, como podría ser el uso de dispositivos inalámbricos, donde puede ser deseable el ajuste del tiempo de vida de los prefijos a fin de que pasado un tiempo después de dejarlos de detectar a los primeros, sean dados de baja.

En caso de que se estuvieran usando múltiples enrutadores, pueden surgir algunos problemas ya que dichos enrutadores tratarán de asignarle a un dispositivo distintas direcciones, y a pesar de que se ha implementado la preferencia alta, media y baja para este tipo de situaciones, esto no fue incluido en el *RFC 2461*, y por lo tanto no necesariamente aparecerá implementado como parte del protocolo.

En el caso de los protocolo de enrutamiento, el problema es menor ya que estos protocolos (*BGP, OSPF y demás protocolos*) trabajan de manera similar que en IPv4. Aunque en ocasiones podrían convertirse en una pesadilla los problemas que surgen si es que uno de los protocolos existentes en una red de pila dual, toma decisiones distintas, o podría ser que esto provea una ventaja al ofrecer redundancia a la hora de buscar solución en algún conflicto causado por alguna de las dos versiones.

De momento el uso para el enrutamiento del tipo *multicast,* sigue siendo experimental.

1.6 Seguridad en IPv6

En IPv6, la seguridad es parte del protocolo, en la forma de seguridad IP (***IPSec***). Se había estado buscando un mecanismo que permitiera separar la seguridad de la capa de aplicación, y esta fue la opción que se tomó. En IPv4 no es nativo el soporte, pero para IPv6 esto si lo es.

IPSec es un conjunto de protocolos que son parte de la especificación del IPv6 y dado la fuerte necesidad de seguridad en IPv4 éste fue adaptado al mismo. Aunque el soporte para IPv4 es opcional y las soluciones propietarias son lo que prevalece. Del otro lado en IPv6, IPSec provee la seguridad de punto final a punto final, se define en el *RFC 2401*.

Dicho de otra manera, la seguridad para IPv6 no es diferente de la seguridad para IPv4. Los ataques más conocidos para IPv4 también se pueden llevar a cabo en IPv6, significando esto que el concepto de seguridad es similar.

En las implementaciones nativas de IPv6 en el *RFC 4301* se hace las especificaciones de los requerimientos de IPsec en el IPv6, pero este no cubre como debe ser el intercambio de llaves *PKI*. También introduce nuevos problemas con los IDS/IPS existentes.

Direcciones Privadas

IPv6 ofrece varias opciones para las direcciones ip que pueden ayudar a los arquitectos de seguridad. Las direcciones privadas pueden ser usadas por aplicaciones cliente para inhibir el rastreo a usuarios (*user tracking*), el cual puede ser útil para proteger comunicaciones externas.

De acuerdo al *RFC 4291*, las interfaces que usan las direcciones de autoconfiguración sin estado (*stateless address autoconfiguration*) generan identificadores de interfaz basados en su identificador ***IEEE EUI-64***. Esto provee un fuerte soporte para la diferenciación única (*uniqueness*), pero esto permite rastrear a una interfaz, incluso si esta cambia de una red a otra, o si el prefijo de la red es cambiado.

Considerese, por ejemplo, un dispositivo móvil que se conecte a diferentes redes inalámbricas en diferentes ubicaciones. Usando IPv4, el dispositivo en cuestión usará DHCP en las diferentes redes y recibirá direcciones completamente diferentes. Si este mismo dispositivo usa la autoconfiguración IPv6 , su dirección de interfaz inalámbrica tendría el mismo identificador de interfaz en cada red. Aún más, el identificador ***IEEE EUI-64***, por estar basado en la dirección MAC del hardware, revelaria qué tipo de dispositivo es.

Una interfaz que acepte conecciones entrantes y que tenga una denominación DNS, no puede tener una dirección privada, pero es posible usar diferentes direcciones para las conexiones de salida. Para el *RFC 494*, *Privacy Extensions for Stateless Address Autoconfiguration in IPv6*, se definió la manera de generar y cambiar dichas direcciones temporales. Los requerimientos importantes son que la secuencia de direcciones temporales e interfaces escogidas deben ser impredecibles y tener baja probabilidad de colisiones con las opciones seleccionadas por otras interfaces.

El método recomendado en el *RFC 4941* trabaja aproximadamente como se menciona a continuación:

1. Obtener el identificador de interfaz que será usado sin este esquema.

2. Aplicar una función criptográfica *hash* a éste valor y también a un valor salvado en históricos o a un número de 64 bits escogido añeatoriamente.

3. Use la salida de la función *hash* anterior, para seleccionar el identificador de interfaz y para actualizar el valor de los históricos.

4. Ejecutar la detección de direcciones duplicadas (DAD).

5. Ajuste los tiempos de vida (*lifetime*) apropiados y agregue el nodo de grupo multicast correspondiente al identificador de interfaz.

6. Continúe usando los identificadores de interfaz prioritarios para las conexiones establecidas pero no para las nuevas.

7. Repita este proceso cuando se conecte a una nueva red o cuando los tiempos ajustados en la iteración previa expiren.

Link encap:Ethernet Hwaddr 00:0C:29:6F:8F:98

inet addr: 192.168.1.3 Bcast: 192.168.1.255 Mask:255.255.255.0

inet6 addr: 2002:2::9048:b971:277c:e16c/64 Scope: Global

inet6 addr: 2002:2::20c:29ff:fe6f:8f98/64 Scope: Global

inet6 addr: fe80::20c:29ff:fe6f:8f98/64 Scope: Global

UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1

Cuadro 4 “Ejemplo de direcciones IPv6 privadas. “

En el ejemplo del cuadro 4 se ve una dirección privada IPv4 no ruteable /24, una dirección global enrutable /64 IPv6, una segunda dir. global enrutable /64 IPv6 basada en su dir. IEEE y la dirección local link basada en su dir. IEEE

Por distintas razones, este mecanismo de extensiones privadas deberá ser usado con cuidado si es que se llega a usar. Algunas de las razones son las siguientes:

- Que tanta privacía es provista actualemte es cuestionable. En redes pequeñas que no cambian mucho, cualquiera que pueda observar el tráfico de red podrá correlacionar las actividades con mucha precisión, sin importar si las direcciones cambian periódicamente o no. Un observador podría determinar que tan seguido las interfaces están generando estas nuevas direcciones.
- En algunas redes, los administradores pueden querer tener control de que está conectado y por consiguiente de las direcciones usadas. Las políticas locales de seguridad podrían dictar que para propositos de auditoría o computo forense, todas las direcciones deberán ser asignadas centralizadamente y guardadas en bitácora. En tal caso, es mejor no permitir las direcciones privadas ni la autoconfiguración sin estado de direcciones sino requerir usar *DHCPv6* para la asignación de direcciones.
- En general, las políticas de seguridad empresariales no extienden el privilegio de comunicaciones privadas a usarios que estan en equipos de la empresa o que están accediendo a la red empresarial. En estos casos, la meta del análisis forense y la seguridad pueden ser vistas con más importancia que proteger la privacía del usuario que navega por la Interet. Esta será una decisión que deberá dejarse en manos del departamento encargado.
- Una buena práctica de administración de redes es aplicar filtrado, esto es, no permitir paquetes sin una dirección válida de origen dentro de la red administrada. Algunos ataques distribuidos de denegación de servicios (DDoS) han usado direcciones de origen forjadas con prefijos válidos. Las direcciones privadas pueden ser difícies de distinguir de las direcciones usadas en estos ataques sin medidas adicionales, como la limitación de transferencia o la verificación de ruta en reversa completa.

Direcciones Generadas Criptográficamente

Las direcciones generadas criptográficamente (CGA), también llamadas direcciones basadas en *hash*, proveen un método de comprobar la pertenencia de una dirección de origen en un paquete. La idea se basa en escoger un par de llaves, pública y privada, capaces de crear una firma digital con la llave privada y verificarla con la pública. Entonces, la llave pública (y junto con otros parámetros), es usada para generar un identificador de interfaz, esta llave es insertada dentro del paquete, y el paquete es firmado con la llave privada. A la recibimiento del paquete, la llave pública puede ser usada para verificar la firma y la dirección. Un atacante no puede firmar un paquete forjado sin la llave pública.

Cuatro procesos son necesarios para hacer funcionar esto:

El emisor debe:

1. Generar un par de llaves (pública y privada) y la dirección correspondiente.
2. Insertar la llave pública dentro de un paquete y firmarlo con la llave privada.

El receptor debe:

1. Verificar que la dirección de origen corresponde a la llave pública.
2. Validar la firma con la llave pública.

Notese que usando CGA no se prueba la identidad de uno, pero muestra que la misma entidad (aquella con la llave privada firmante) generó cada paquete y que los paquetes no fueron subsecuentemente modificados por otras entidades. Este punto trata de que nadie sin la llave privada puede usar CGA legitimamente.

CGA ha sido estandarizado como el principal bloque para el aseguramiento del protocolo *RFC 3971* de descubrimiento de vecindad en IPv6 (*IPv6 Secure Neighbor Discovery SEND*), y han sido propuestos para el uso con el protocolo *SHIM6* (*Site Multihoming for IPv6*). En todos los casos el algoritmo hash especificado para CGA es SHA-1, el algoritmo de firma es RSA, y el formato de firma sigue el estandar de cifrado de llave pública (PKCS) #1, versión 1.5, descrito en el *RFC 3447*.

Las CGAs se especificaron en los RFC 3972 y RFC 4581. Las implementaciones necesitan generar y almacenar valores criptograficos seguros para usar estos protocolos con seguridad. Lease el RFC 4086 para una discusión acerca de generar valores pseudo-aleatorios.

Algunas vulnerabilidades en IPv6

La IETF manejo la seguridad como una parte importante en el diseño de los estandares para IPv6. El trabajo para agregar confidencialidad e integridad en IPv4 llevó al desarrollo de IPSec. IPv6 junto con IPSec resuelve este problema, pero IPSec no ha manejado otras debilidades encontrada en la pila del protocolo TCP/IP.

IPv6 no resuelve muchos ataques de capa 2 tradicionales, tales como el sniffeo de tráfico, *traffic flooding*, *man-in-the-middle*, *rogue devices* y ataques de desbordamiento de tabla ARP. Algunos de estos ataques se manejan en IPv6 parcialmente, mientras que otros ataques, similares en naturaleza, eplotan diferentes caracteristicas.

Mientras que la mayoría de los sistemas operativos soportan IPv6 desde 2003, la pila de protocolos de estos sistemas operativos no han sido probados totalmente. Una revisión en la NVD (*National Vulneratibilities Database*) muestra vulnerabilidades en la pila de protocolos de los sistemas operativos mas populares. Cuando las nuevas vulnerabilidades son expuestas, los vendedores realizan actualizaciones. Como cualquier código nuevo, los vendedores necesitan tiempo para estabilizar y *endurecer* (*harden*) el código.

Los ataques de capa 2 y 3 en IPv4 son posibles porque se asumió que todos los nodos de red se comportarían de manera *confiable.* IPv4 usa ARP para asociar las direcciones físicas a las direcciones lógicas. Este presuposición permitió que los ataques interfirieran con la resolución de direcciones IP y la asociación de direcciones lógicas y físicas. IPv6 no usa ARP para mapear direcciones IP con interfaces físicas, en vez de eso usa ICMPv6. IPv6 usa ICMP para el descubrimiento de vecindad (ND) y lel proceso de autoconfiguración de direcciones sin estadoque asocia direcciones físicas y lógicas. Pero IPv6 es aún vulnerable a los ataques de capa 3.

El tamaño de las subredes en IPv6 pueden presentar su propio desafío de seguridad. Estos desafíos se discuten en el *RFC 5157 IPv6 Implications for Network Scanning.* El tamaño de las subredes es mucho mayor de lo que fue en IPv4; una subred por default en IPv6 puede tener 2^{64} direcciones.