IPv6

Siguiente Generación del Protocolo Internet

Por Antonio Rodríguez López

Ampliación de Automatización Industrial

3º Ingeniería Técnica Industrial

E.P.S. La Rábida, Huelva 01/05/02

INTRODUCCIÓN

Los protocolos se inventaron debido a que los datos no se pueden enviar por un cable directamente, porque los ordenadores conectados a la red no tendrían modo de saber a cuál de ellos se dirigen o cuál es su contenido. La solución la basamos en un conjunto de mensajes que se envían por la red junto con los datos, y que traducidos al lenguaje humano representan el equivalente a los saludos y notificaciones que no aportan información.

En la actualidad la red Internet funciona gracias a un protocolo general para redes de ordenadores llamado TCP/IP (*Transfer Control Protocol / Internet Protocol*), en concreto la versión 4, o IPv4, sistema que tiene casi 20 años de antigüedad. Con el paso de los años el protocolo IPv4 empieza a mostrar serias deficiencias. La más importante es la escasez de direcciones IP libres.

La organización conocida como IETF (*Internet Engineering Task Force*, Comando de Ingeniería de Internet) ha desarrollado un nuevo protocolo llamado IP Next Generation (IPng) o IPv6, que soluciona el problema de la limitación de direcciones y mejora otros aspectos técnicos como en enrutamiento y la autoconfiguración.

El reducido espacio de lPv4, impensable hace varios años, junto al hecho de una importante falta de coordinación en la asignación de direcciones, sin ningún tipo de optimización, dejando incluso grandes espacios discontinuos, nos esta llevando a lo que podríamos llamar un “colapso”.

Una solución posible solución sería la renumeración, y reasignación de dicho espacio de direccionamiento. Sin embargo esto no es tan sencillo e incluso impensable en algunas redes, ya que requiere unos esfuerzos enormes de coordinación a escala mundial que lo hacen inviable. Además seguiríamos teniendo uno de los problemas de lPv4 como es la gran dimensión de las tablas de encaminado (routing) en el troncal de lntemet, haciéndolo ineficaz, y entorpeciendo los tiempos de respuesta.

Por otra parte, la falta de direcciones no es apreciable en todas las zonas de la geografía mundial. En EEUU y Canadá apenas tienen necesidad de aumentar el número de direcciones IP. Sin embargo, en otras zonas como Asia y Europa, el problema se agrava.

Tenemos el caso de China que ha pedido direcciones para conectar 60.000 escuelas y tan sólo 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.

En poco tiempo estamos pasando de 10 usuarios por cada 1 dirección IP, a 1 usuario por cada IP. Se estima que, dentro de unos años, esta tendencia se invertirá pasando a ser de 50 a 100 direcciones IP por cada usuario. Esto estará motivado por el incremento de dispositivos denominados "siempre conectados". Actualmente algunos Proveedores de Servicios Internet se ven incluso obligados a proporcionar a sus clientes direcciones lP privadas, mediante mecanismos de NAT (traslación de direcciones, es decir, usar una sola lP pública para toda una red privada). Cada ordenador conectado a Internet debe tener su propia dirección IP, sea un servidor de páginas web o un ordenador doméstico que se conecta temporalmente a la red mediante un módem. En este último caso se asigna una IP dinámica, que cuando ya no esté en uso puede asignarse a otro usuario.

Existen una serie de protocolos como pueden ser RTP, RTCP, autenticación Kerberos, IPsec, etc. que son incapaces de atravesar los dispositivos NAT, debido a que sus cabeceras son modificadas.

Como ejemplo de estas necesidades podemos ver las previsiones en cuanto al número de internautas para los próximos años.

América del Norte..... 500.000.000 (sólo 125.000.000 sin NAT)
Asia..... 2.500.000.000 (sólo 50.000.000 sin NAT)
Europa Occidental..... 250.000.000 (sólo 50.000.000 sin NAT)
Africa..... 800.000.000 (sólo 3.000.000 sin NAT)
América Central y del Sur.... 500.000.000 (sólo 10.000.000 sin NAT)

A menudo, cuando hablamos de dispositivos conectados a la red, tendemos a pensar exclusivamente en un determinado número de ordenadores o terminales domésticos, en empresas, etc. pero nos olvidamos

de toda una serie de dispositivos, algunos conocidos y otros aún por conocer, que poco a poco nos van siendo familiares, están cada vez más presentes y que por supuesto también hacen uso de la red al igual que un ordenador doméstico pero dirigidos hacia diversas aplicaciones. A continuación se expone una breve lista de dispositivos o aplicaciones que necesitarán direcciones IP públicas únicas y por lo tanto ser integrados en la gran red.

Teléfonos de nueva generación.
Sistemas de seguridad, televigilancia y control.
Seguimiento automático de vehículos.
Diagnóstico y seguridad de vehículos.
Lectura de contadores de agua, luz, gas, etc.
Maquinas de venta automáticas.
Televisión y Radio.
Walkman MP3.
Electrodomésticos (Domótica, frigoríficos, despertadores, etc.)
Dispositivos de control médico (marcapasos, etc.)
Consolas de juegos, agendas electrónicas, etc.

Todo esto sin olvidar las nuevas tecnologías emergentes como Bluetooth, WAP, redes inalámbricas, redes domésticas, etc., la necesidad existente de mejorar las aplicaciones de videoconferencia, seguridad, juegos, etc. y la creciente necesidad de movilidad por parte de los usuarios ya que queremos estar conectados desde cualquier sitio.

CARACTERISTICAS PRINCIPALES DE IPv6

A continuación se exponen, a groso modo, aquellas características que resaltan en esta nueva versión del protocolo IPv.

- Un mayor espacio de direcciones.
- Autoconfiguración (Plug & Play)
- Paquetes IP eficientes y extensibles.
- Paquetes con carga útil de más de 65535 bytes.

- Anycast y Multicast.
- Renumeración y multi-homing.
- Seguridad Intrínseca (IPsec).
- Calidad de servicio y Clase de servicio.
- Enrutado más eficiente.
- Características de movilidad.
- Escalabilidad

Especificaciones básicas de IPv6

Para comenzar a entender las mejoras introducidas en este nuevo protocolo, estudiaremos las dos cabeceras de un paquete IPv4 e IPv6. Empezaremos por la cabecera Ipv4:

Bits: 4 8 16 20 32

VERSIÓN	**CABECE**	**TOS**	**LONGITUD TOTAL**	
IDENTIFICACIÓN			**INDICAD**	**DESP. DE FRAGMENTACIÓN**
TTL		**PROTOCOLO**	**CHECKSUM**	
DIRECCIÓN FUENTE DE 32 BITS				
DIRECCIÓN DESTINO DE 32 BITS				
OPCIONES				

Equivalencias en ambos idiomas y longitud de cada campo:

ESPAÑOL	INGLÉS	LONGITUD
Versión	Version	4 bits
Cabecera	Header	4 bits
TOS (tipo de servicio)	TOS (Type Of Service)	8 bits
Longitud Total	Total Length	16 bits
Identificación	Identification	16 bits
Indicador	Flag	4 bits

Desplazamiento de Fragmentación	Fragment Offset	12 bits – 1.5 bytes
Tiempo de vida	TTL (Time To Live)	8 bits
Protocolo	Protocol	8 bits
Código de verificación	Checksum	16 bits
Dirección fuente de 32 bits	32 bits Source Address	32 bits
Dirección destino de 32 bits	32 bits Destination Address	32 bits

Los campos marcados con color de fondo amarillo desaparecen en IPv6 y el resto de campos son renombrados y/o modificados en cada caso. Como se puede observar, la longitud mínima de la cabecera es de 20 bytes. A estos 20 bytes hay que añadirles las opciones que dependan de cada caso. Debido a la multitud de nuevas aplicaciones en las que IPv4 ha sido utilizado, se crearon "añadidos" o también llamados "parches" al protocolo básico como son la Calidad de Servicio (QoS), Seguridad (Ipseg) y Movilidad por citar los más conocidos. Todos estos parches son los que van en el campo *Opciones*.

En la nueva versión, 6 campos desaparecen por motivos de redundancia ya que se estaría facilitando la misma información varias veces. Tal es el caso del campo ***Checksum*** que sirve para verificar la integridad de la cabecera y que otros mecanismos de encapsulado ya realizan esta función. El campo Desplazamiento de Fragmentación también se suprime ya que en IPv6 los enrutadores no fragmentan los paquetes sino que de ser precisa esta se produce extremo a extremo.

La siguiente tabla recoge de manera esquemática los campos que han sido eliminados y aquellos que son modificados:

CAMPO	LONGITUD IPv4	LONGITUD IPv6	DESCRIPCIÓN
Cabecera	DESAPARECEN		
Identificación			
Indicador			
Desplazamiento de fragmentación			
Checksum			
Opciones			
Versión	4 bits	4 bits	Contiene el número (6) de la nueva versión

Longitud Total	16 bits	16 bits	Es la longitud de los propios datos (hasta 65.536 bytes)
Tiempo de vida (TTL)	8 bits	8 bits	Límite de saltos (Hop Limit)
Protocolo	8 bits	8 bits	Indica cual es la siguiente cabecera ya que se emplean sucesivas cabeceras encadenadas en lugar de usar una sola de longitud variable. Por este motivo se elimina el campo Opciones.
Clase de Tráfico		8 bits	También se denomina Prioridad (Priority) o Clase (Class). Equivale a TOS (Tipo de Servicio) de IPv4.
Etiqueta de flujo		20 bits	Para permitir tráficos con requisitos de tiempo real.
Direcciones	32 bits	128 bits	2 campos de 128 bits: Dirección fuente y destino.

Los campos Clase de Tráfico y Etiqueta de Flujo son los que permiten una de las características fundamentales de IPv6: Calidad de Servicio (QoS), Clase de Servicio (CoS). Constituyen un buen mecanismo de control de flujo y de asignación de prioridades en función de los tipos de servicios.

Con todos los datos anteriores ya podemos darle forma a la nueva cabecera IPv6:

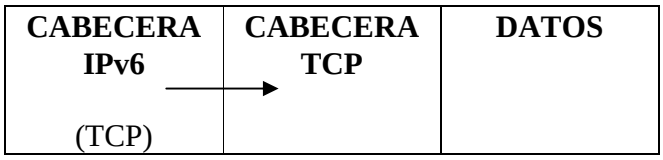
Bits: 4 12 16 24 32

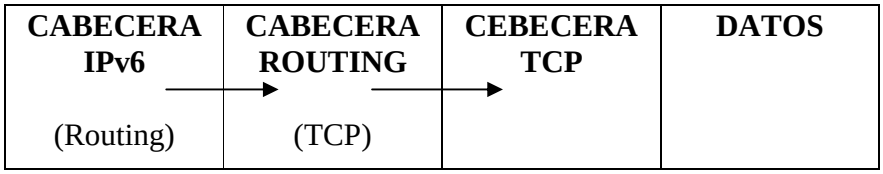
VERSIÓN	**CLASE DE TRÁFICO**	**ETIQUETA DE FLUJO**		
LONGITUD DE LA CARGA UTIL		**SIG. CABECERA**	**LÍMITE DE SALTOS**	
DIRECCIÓN FUENTE DE 128 BITS				
DIRECCIÓN DESTINO DE 128 BITS				

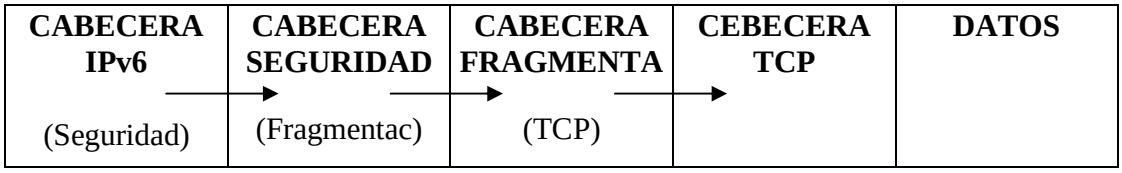
- Como primera conclusión nótese que hemos pasado de tener 12 campos + Opciones en IPv4 ha tener tan solo 8 en IPv6.
- La longitud de la cabecera es de 20 bytes en IPv4 y esta pasa ha ser de 40 bytes en IPv6. Las ventajas radican en el hecho de la eliminación de los campos redundantes y en la longitud fija de la cabecera que facilita su procesado en routers y conmutadores.
- Los campos están alineados a 64 bits para su procesamiento óptimo en procesadores y microcontroladores de 64 bits

El valor del campo "siguiente cabecera", indica cual es la siguiente cabecera y así sucesivamente. Las sucesivas cabeceras, no son examinadas en cada nodo de la ruta de manera que solo son examinadas en el nodo o nodos destino finales. La única excepción ocurre cuando el valor de este campo es cero, lo que indica opción de examinado. Las cabeceras han de ser procesadas en el mismo orden en que aparecen en el paquete.

Se introduce por tanto un nuevo concepto llamado "cabeceras de extensión" mecanismo por el que cada cabecera es "encadenada" a la siguiente y anterior. La figura ilustra lo anteriormente explicado:







Definición de dirección en lPv6

Como ya sabemos, el principal motivo por el cual se hace necesario un cambio progresivo hacia a Ipv6 es por la actual falta de direcciones IP y la creciente demanda de las mismas.

lPv4 tiene un espacio de direcciones de 32 bits, es decir, 4.294.967.296 direcciones. En cambio, lPv6 nos ofrece un espacio de direcciones de 128 bits, en total:
340.282.366.920.938.463.463.374.607.431.768.211.456 direcciones.

Del total de direcciones disponibles, tan solo algo más del 15% están reservadas para un uso de corto a medio plazo (una vez instaurado el nuevo protocolo). El 85% restante queda reservado para uso futuro.

Por otra parte hay que señalar algunas diferencias importantes en el direccionamiento de lPv6 respecto de lPv4:

→ No hay direcciones broadcast (su función es sustituida por direcciones multicast).
→ Los campos de las direcciones reciben nombres específicos; denominamos "prefijo" a la parte de la dirección hasta el nombre indicado (incluyéndolo).
→ Dicho prefijo nos permite conocer donde esta conectada una determinada dirección, es decir, su ruta de encaminado.

En IPv6 existen principalmente 3 tipos de direcciones. Cada una constituye un identificador para una o varias interfaces:

- **Unicast**: ldentificador para una única interfaz. El paquete es entregado sólo a la interfaz identificada con dicha dirección. Es el tipo de dirección que se usa actualmente en IPv4.

- **Anycast**: ldentificador para un conjunto de interfaces. El paquete es entregado a una sola de las interfaces identificadas con dicha dirección (la más próxima, de acuerdo a las medidas de distancia del protocolo de encaminado). Nos permite crear, por ejemplo, ámbitos de redundancia, de forma

que varias máquinas puedan ocuparse del mismo tráfico según una secuencia determinada por el enrutado, si la primera "cae".

- **Multicast:** ldentificador para un conjunto de interfaces. El paquete es entregado a todas las interfaces identificadas por dicha dirección. Sirve por tanto para aplicaciones de retransmisión múltiple (broadcast en IPv4).

También existen otros tipos de direcciones denominadas “especiales”:

- **Túneles dinámicos / automáticos de lPv6 sobre lPv4** (::<dirección lPv4>). Son direcciones lPv6 compatibles con infraestructuras lPv4.

- **Direcciones lPv6 mapeadas desde lPv4** (::FFFF:<dirección lPv4>). Permite que los nodos que sólo soportan lPv4, puedan seguir trabajando en redes lPv6.

- **Loopback** o **Dirección de auto-retorno** (::1). No ha de ser asignada a una interfaz física ya que se trata de una interfaz "virtual" (paquetes que no salen de la máquina que los emite) y que nos permite hacer un bucle para verificar la correcta inicialización del protocolo dentro de una determinada máquina.

- **Dirección no especificada** (::). No es asignada a ningún nodo. Se emplea para indicar la ausencia de dirección; por ejemplo, cuando se halla en el campo de dirección fuente, indica que se trata de un host que esta iniciándose, antes de que haya aprendido su propia dirección.

Algunos ejemplos de direcciones:

Unicast:	1080:0:0:0:8:800:200C:417A
Multicast:	FF01:0:0:0:0:0:0:101
Loopback:	0:0:0:0:0:0:0:1
Dirección no especificada:	0:0:0:0:0:0:0:0

La nueva ortografía IP

Con un octeto (ocho bits de la forma 00010111) se pueden representar los números de 0 a 255. Por tanto las direcciones IPv4 se componen de cuatro octetos decimales, o 32 bits, lo cual genera los cuatro millones y pico de direcciones antes mencionadas. En el siguiente ejemplo cada X representaría un octeto:

Dirección IPv4 → X . X . X . X
Ejemplo: 23 . 103 . 5 . 255

En IPv6 las direcciones se componen de 16 octetos hexadecimales, es decir 128 bits. Esto daría lugar a más o menos 340 sextillones de direcciones posibles. No obstante, esta cifra no se alcanza, ya que parte de los dígitos identifican el tipo de dirección, con lo que se quedan en 3800 millones. En cualquier caso se garantiza que no se acabarán en un plazo razonable. Esta sería su ortografía:

Dirección IPv6 → X : X : X : X : X : X: X : X
Ejemplo: FEDC:BA98:7654:3210:FEDC:BA98:7654:3210

Para representar las direcciones IPv6 como cadenas de texto (en lugar de ceros y unos) hay diferentes reglas:

- **Preferred form** y consiste en listar la dirección completa como 8 números hexadecimales de cuatro cifras (8 paquetes de 16 bits):

  FEDC:2A5F:709C:216:AEBC:97:3154:3D12
  1030:2A9C:0:0:0:500:200C:3A4

- **Compressed form** o forma comprimida, en la que las cadenas que sean cero se sustituyen por un par de dos puntos "::" que indican que hay un grupo de ceros teniendo en cuenta que solo se puede hacer una sola vez. Por ejemplo:

FF08:0:0:0:0:0:209A:61 → FF08::209A:61

0:0:0:0:0:0:0:1 → ::1

- Por último se pueden escribir en **forma mixta**, con las primeras cifras en hexadecimal y las últimas (las correspondientes a IPv4) en decimal. Hay que tener en cuenta que ahora existen 10 porciones, 2 mas debido a que las cuatro últimas son de 8 bits por lo que cada una de ellas ocupa la mitad de una porción de 16 bits :

  Dirección en forma mixta → X : X : X : X : X : X: d : d : d : d

  Ejemplo: 0:0:0:0:0:0:193.136.239.163 o bien ::193.136.239.163

Direcciones Unicast

Las direcciones Unicast se dividen en dos tipos:

- **Direcciones Unicast Globales Agregables**.
- **Direcciones Unicast Locales**, que a su vez estas se subdividen en:
  - **Local de Enlace** (Link-Local)
  - **Local de Sitio** (Site-Local)

Direcciones Unicast Globales Agregables

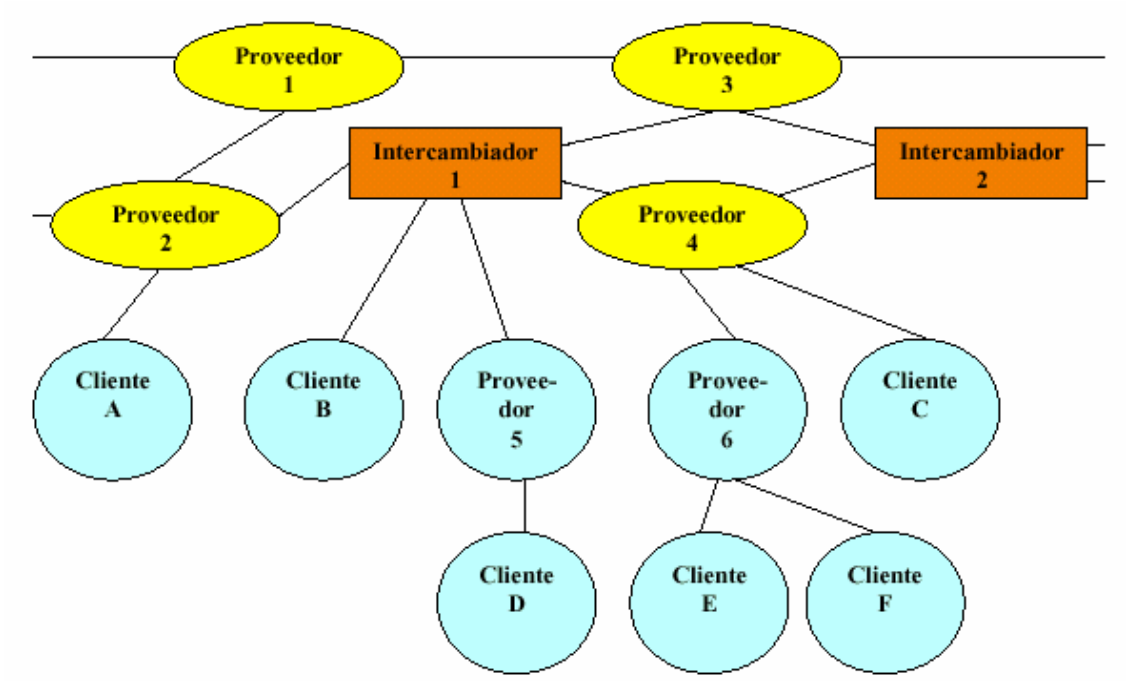
Dado que uno de los problemas que lPv6 resuelve es la mejor organización jerárquica del routing en las redes públicas (globales), es indispensable el concepto de direccionamiento "agregable".

En la actualidad ya se emplea este tipo de direcciones, basadas en la agregación por parte de los proveedores del troncal Internet, y los mecanismos adoptados para lPv6, permiten su continuidad. Pero además, se incorporó un mecanismo de agregación basado en "intercambios". La combinación de ambos es la que permite un encaminamiento mucho más eficiente, dando dos opciones de conectividad a unas u otras entidades de agregación.

Se trata de una organización basada en tres niveles:

- Topología Pública: conjunto de proveedores e "intercambiadores" que proporcionan servicios públicos de tránsito Internet.
- Topología de Sitio: redes de organizaciones que no proporcionan servicios públicos de tránsito a nodos fuera de su propio "sitio".
- ldentificador de Interfaz: identifican interfaces de enlaces.

En la figura adjunta, el formato de direcciones agregables ha sido diseñado para soportar proveedores de larga distancia (1-4), intercambiadores (1 y 2), proveedores de niveles inferiores (5 y 6), y clientes (A-F).



A diferencia de lo que ocurre actualmente, los intercambiadores también proporcionarán direcciones públicas lPv6. Las organizaciones conectadas a dichos intercambiadores también recibirán servicios de conectividad directos, indirectamente a través del intercambiador, de uno o varios proveedores de larga distancia.

De esta forma, su direccionamiento es independiente de los proveedores de tráfico de larga distancia, y pueden, por tanto, cambiar de proveedor sin necesidad de renumerar su organización. Este es uno de los objetivos de lPv6. Además, una organización puede estar suscrita a múltiples proveedores (multi-homing o "multi-localización"), a través de un intercambiador, sin necesidad de tener prefijos de direcciones de cada uno de los proveedores.

El formato de las direcciones Unicast Globales Agregables es el siguiente:

3	13	8	24	16	64 bits
FP	**TLA ID**	**RES.**	**NLA ID**	**SLA ID**	**INTERFAZ ID**
Topología Pública			Topología de Sitio		Identificador de Interfaz

FP	Prefijo de formato
TLA ID	Identificador de agregación de Nivel Superior
RES.	Reservado para uso futuro
NLA ID	Identificador de agregación de siguiente Nivel
SLA ID	Identificador de agregación de Nivel de Sitio
Interfaz ID	Identificador de interfaz

TLA ID (ldentificador de Agregación de Nivel Superior):

Se trata del nivel superior en la estructura jerárquica de enrutado. Los routers situados en este nivel tienen, en la tabla de encaminado, una entrada para cada TLA ID activo, y probablemente entradas adicionales relativas al propio TLA ID donde están físicamente situados. Podrían tener otras entradas, para su optimización, dependiendo de su topología, pero siempre pensando en que se minimice la tabla.

RES

El campo *Reservado* (RES) permitirá, en el futuro, ampliaciones "organizadas" del protocolo, por ejemplo ampliar el número de bits de los campos TLA y NLA. Por el momento contiene ceros.

NLA ID. (ldentificador de Agregación de Siguiente Nivel)
Es empleado por organizaciones a las que se ha asignado un TLA, para crear una estructura jerárquica de direccionamiento, acorde con su propia red, y para identificar los "sitios" u organizaciones que de ella dependen. Pueden reservar los bits superiores para la diferenciación de la estructura de su red, en función a sus propias necesidades.

Dado que cada organización que recibe un TLA dispone de 24 bits de espacio NLA, permite proporcionar servicio aproximadamente al número total de direcciones lPv4 soportadas actualmente.

En cualquier caso es fundamental apreciar el balance entre eficacia de encaminado agregable y flexibilidad. Las estructuras más jerárquicas permiten una mejor agregación, y por tanto reducen las tablas de encaminado. Por el contrario asignaciones más planas del espacio NLA proporcionan mejor flexibilidad en la conexión (crecimientos no previstos en un determinado espacio), resultando en tablas de encaminado mayores, y por tanto menos eficaces.

SLA. (ldentificador de Agregación de Nivel de Sitio)
El SLA es usado por organizaciones "finales" para crear su propia estructura jerárquica de direcciones e identificar sus subredes. Es equivalente al concepto de subred en lPv4, con la muy apreciable diferencia de que cada corporación tiene un mayor número de subredes (16 bits proporcionan capacidad para 65.535).

Del mismo modo que en el caso del NLA, se puede escoger entre una estructura "plana", o crear varios niveles. Una gran compañía podría necesitar varios identificadores SLA. Como es lógico, cada caso dependerá de cómo están conectadas sus diversas delegaciones.

Direcciones Unicast Locales

Los nodos lPv6 pueden no tener ningún conocimiento o mínimo de la estructura interna de las direcciones lPv6, dependiendo de su misión en la red (por ejemplo, host frente a router). Pero como mínimo, un nodo debe considerar que las direcciones unicast (incluyendo la propia), no tienen estructura:

128 bits
Dirección del nodo

Un host algo más sofisticado, conocería el prefijo de la subred del enlace al que esta conectado:

n bits	128–n bits
Prefijo de subred	**Identificador de interfaz**

Dispositivos más sofisticados pueden tener un conocimiento más amplio de la jerarquía de la red, sus límites, etc.

El "identificador de interfaz" se emplea, por tanto, para identificar interfaces en un enlace, y deben de ser únicos en dicho enlace. En muchos casos también serán únicos en un ámbito más amplio. El mismo identificador de interfaz puede ser empleado en múltiples interfaces del mismo nodo, sin afectar a su exclusividad global en el ámbito lPv6.

Se han definido dos tipos de direcciones unicast de uso local: **Local de Enlace** (Link-Local) y **Local de Sitio** (Site-Local).

Direcciones locales de enlace

Han sido diseñadas para direccionar un único enlace para propósitos de auto-configuración (mediante identificadores de interfaz), descubrimiento del vecindario, o situaciones en las que no hay routers.
Por tanto, los encaminadores no pueden retransmitir ningún paquete con direcciones fuente o destino que sean locales de enlace (su ámbito esta limitado a la red local). Tienen el siguiente formato:

FE80::<lD de interfaz>/10.

10 bits	54 bits	64 bits
1111111010	**0**	**Identificador de interfaz**

Las direcciones locales de sitio permiten direccionar dentro de un "sitio" local u organización, sin la necesidad de un prefijo global. Se configuran mediante un identificador de subred, de 16 bits. Los encaminadores no deben de retransmitir fuera del sitio ningún paquete cuya dirección fuente o destino sea "local de sitio" (su ámbito esta limitado a la red local o de la organización).

FECO::<lD de subred>:<lD de interfaz>/10.

10 bits	38 bits	16 bits	64 bits
1111111011	**0**	**ID de subred**	**Identificador de interfaz**

Direcciones Anycast

Las direcciones anycast tienen el mismo rango de direcciones que las unicast. Cuando una dirección unicast es asignada a más de una interfaz, convirtiéndose en una dirección anycast, los nodos a los que dicha dirección ha sido asignada, deben ser explícitamente configurados para que reconozcan que se trata de una dirección anycast.

Existe una dirección anycast, requerida para cada subred, que se denomina "dirección anycast del router de la subred" (subnet-router anycast address). Su sintaxis es equivalente al prefijo que especifica el enlace correspondiente de la dirección unicast, siendo el indicador de interfaz igual a cero:

n bits	128-n bits
Prefijo de subred	**0000000000000000000**

Todos los routers han de soportar esta dirección para las subredes a las que están conectados. Los paquetes enviados a la "dirección anycast del router de la subred", serán enviados a un router de la subred.

Una aplicación evidente de esta característica, además de la tolerancia a fallos, es la movilidad. Imaginemos nodos que necesitan comunicarse con un router entre el conjunto de los disponibles en su subred.

Dentro de cada subred, los 128 valores superiores de identificadores de interfaz están reservados para su asignación como direcciones anycast de la subred.

La construcción de una dirección reservada de anycast de subred depende del tipo de direcciones lPv6 usadas dentro de la subred.

Las direcciones cuyos tres primeros bits (prefijo de formato) tienen valores entre 001 y 111 (excepto las de multicast, 1111 1111), indican con el bit "universal/local" igual a cero, que el identificador de interfaz tiene 64 bits, y por tanto no es globalmente único (es local). En este caso, las direcciones reservadas anycast de subred se construyen del siguiente modo:

64 bits	57 bits	7 bits
Prefijo de subred	**1111110111 ... 111**	**ID anycast**
	Identificador de Interfaz	

En el resto de los casos, el identificador de interfaz puede tener una longitud diferente de 64 bits, por lo que la construcción se realiza según el siguiente esquema:

n bits	121-n bits	7 bits
Prefijo de subred	**1111111...1111111**	**ID anycast**
	Identificador de Interfaz	

Direcciones Multicast

Una dirección multicast en lPv6, puede definirse como un identificador para un grupo de nodos. Un nodo puede pertenecer a uno o vados grupos multicast. Las direcciones multicast tienen el siguiente formato:

8	4	4	112 bits
11111111	**000T**	**Ámbito**	**Identificador de Grupo**

El bit "T" indica, si su valor es cero, una dirección multicast permanente, asignada únicamente por la autoridad de numeración global de Internet. En caso contrario, si su valor es uno, se trata de direcciones multicast temporales. Los 4 bits que le preceden, que por el momento están fijados a cero, están reservados para futuras actualizaciones.

Los bits "ámbito" tienen los siguientes significados:

0	**Reservado**
1	**Ambito Local de Nodo**
2	**Ambito Local de Enlace**
3	**No asignado**
4	**No asignado**
5	**Ambito Local de Sitio**
6	**No asignado**
7	**No asignado**
8	**Ambito Loc. de Organización**
9	**No asignado**
A	**No asignado**
B	**No asignado**
C	**No asignado**
D	**No asignado**
E	**Ambito Global**
F	**Reservado**

El "ldentificador de Grupo", identifica, como cabe esperar, el grupo de multicast concreto al que nos referimos, bien sea permanente o temporal, dentro de un determinado ámbito.

Por ejemplo, si asignamos una dirección multicast permanente, con el identificador de grupo 101 (hexadecimal), al grupo de los servidores de tiempo (NTS), entonces:

FF01::101 significa todos los NTS en el mismo nodo que el paquete origen

FF02::101 significa todos los NTS en el mismo enlace que el paquete origen
FF05::101 significa todos los NTS en el mismo sitio que el paquete origen
FFOE::101 significa todos los NTS en Internet

Las direcciones multicast no permanentes, sólo tienen sentido en su propio ámbito. Por ejemplo, un grupo identificado por la dirección temporal multicast local de sitio FF15::101, no tiene ninguna relación con un grupo usando la misma dirección en otro sitio, ni con otro grupo temporal que use el mismo identificador de grupo (en otro ámbito), ni con un grupo permanente con el mismo identificador de grupo.

Las direcciones multicast no deben ser usadas como dirección fuente en un paquete lPv6, ni aparecer en ninguna cabecera de encaminado.

Las principales direcciones multicast reservadas son las incluidas en el rango FF0x:0:0:0:0:0:0:0.

Algunos ejemplos útiles de direcciones multicast, según su ámbito, serían:

FF01:0:0:0:0:0:0:1 - todos los nodos (ámbito local)
FF02:0:0:0:0:0:0:1 - todos los nodos (ámbito de enlace)
FF01:0:0:0:0:0:0:2 - todos los routers (ámbito local)
FF02:0:0:0:0:0:0:2 - todos los routers (ámbito de enlace)
FF05:0:0:0:0:0:0:2 - todos los routers (ámbito de sitio)

La dirección FF02:0:0:0:0:1:FFxx:xxxx, denominada "Solicited-Node Address", o dirección de nodo solicitada, permite calcular la dirección multicast a partir de la unicast o anycast de un determinado nodo. Para ello, se sustituyen los 24 bits de menor peso (“x”) por los mismos bits de la dirección original. Así, la dirección 4037::01;800:200E:8C6C se convertiría en FF02::1:FF0E:8C6C.

Cada nodo debe de calcular y unirse a todas las direcciones multicast que le corresponden para cada dirección unicast y anycast que tiene asignada.

Otros protocolos

En Internet existen otros protocolos encargados de funciones diversas. Por su especial relevancia podemos comentar el **ICMPv6** (Protocolo de Mensajes de Control de Internet) y el **ND** (Neighbor Discovery) o "descubrimiento del vecindario".

Protocolo ICMPv6

El Protocolo de Mensajes de Control de Internet (Internet Control Message Protocol), descrito originalmente en el documento RFC792 para lPv4, ha sido actualizado para permitir su uso bajo lPv6.

El protocolo resultante de dicha modificación es lCMPv6, y se le ha asignado un valor, para el campo de "siguiente cabecera", igual a 58. lCMPv6 es parte integral de lPv6 y debe ser totalmente incorporado a cualquier implementación de nodo lPv6.

lCMPv6 es empleado por lPv6 para reportar errores que se encuentran durante el procesado de los paquetes, así como para la realización de otras funciones relativas a la capa "Internet", como diagnósticos (ping).

El formato genérico de los mensajes lCMPv6 es el siguiente:

Bits	8	16	32
Tipo	**Código**	**Checksum**	

El campo "tipo" indica el tipo de mensaje, y su valor determina el formato del resto de la cabecera.

El campo "código" depende del tipo de mensaje, y se emplea para crear un nivel adicional de jerarquía para la clasificación del mensaje.

El "checksum" o código de redundancia nos permite detectar errores en el mensaje lCMPv6.

Los mensajes lCMPv6 se agrupan en dos tipos o clases: **mensajes de error** y **mensajes informativos**. Los mensajes de error tienen un cero en el bit de mayor peso del campo "tipo", por lo que sus valores se sitúan entre 0 y 127. Los valores de los mensajes informativos oscilan entre 128 y 255.

Los mensajes definidos por la especificación básica (se esta trabajando en nuevos tipos de mensajes) son los siguientes:

Mensajes de error ICMPv6		
Tipo	Descripción y Códigos	
1	Destino no alcanzable (Destination Unreachable)	
	Código	Descripción
	0	Sin ruta hacia el destino
	1	Comunicación prohibida administrativamente
	2	Sin asignar
	3	Dirección no alcanzable
	4	Puerto no alcanzable
2	Paquete demasiado grande (Packet Too Big)	
3	Tiempo excedido (Time Exceeded)	
	Código	Descripción
	0	Límite de saltos excedido
	1	Tiempo de desfragmentación excedido
4	Problema de parámetros (Parameter Problem)	
	Código	Descripción
	0	Campo erróneo en cabecera
	1	Tipo de "cabecera siguiente" desconocida
	2	Opción IPv6 desconocida
Mensajes informativos ICMPv6		
Tipo	Descripción	
128	Solicitud de eco (Echo Request)	
129	Respuesta de eco (Echo Reply)	

Protocolo ND

En lPv6, el protocolo equivalente, en cierto modo, a ARP en lPv4, es el que denominamos "descubrimiento del vecindario". Sin embargo, incorpora también la funcionalidad de otros protocolos lPv4, como "ICMP Router Discovery" y "ICMP Redirect".

El protocolo ND es bastante completo y sofisticado, ya que es la base para permitir el mecanismo de autoconfiguración en lPv6.

Tal como indica esta "traducción", consiste en el mecanismo por el cual un nodo que se incorpora a una red, descubre la presencia de otros, en su mismo enlace, para determinar sus direcciones en la capa de enlace, para localizar los routers, y para mantener la información de conectividad ("reachability") acerca de las rutas a los "vecinos" activos.

El protocolo ND (abreviatura común de "Neighbor Discoverf'), también se emplea para mantener limpios los "caches" donde se almacena la información relativa al contexto de la red a la que esta conectado un nodo (host o router), y por tanto para detectar cualquier cambio en la misma. Cuando un router, o una ruta hacia él, falla, el host buscará altemativas funcionales.

ND emplea los mensajes de lCMPv6, incluso a través de mecanismos de multicast en la capa de enlace, para algunos de sus servicios.

Define, entre otros, mecanismos para descubrir routers, prefijos y parámetros, autoconfiguración de direcciones, resolución de direcciones, determinación del siguiente salto, detección de nodos no alcanzables, detección de direcciones duplicadas o cambios, redirección, balanceo de carga entrante, direcciones anycast, y anunciación de proxies.

La **autoconfiguración** es el conjunto de pasos por los cuales un host decide como autoconfigurar sus interfaces en lPv6. Este mecanismo es el que nos permite afirmar que lPv6 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 (direcciones y otra información).

Las direcciones pueden obtenerse de forma totalmente manual, mediante DHCPV6 (**stateful** o configuración predeterminada), o de forma automática (**stateless** o 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 (stateless). También define el mecanismo para detectar direcciones duplicadas.

La autoconfiguración "stateless" (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 combinación 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 por 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.

Bibliografía

Direcciones Web de interés:

- http://www.ipv6.itesm.mx/
- http://www.consulintel.es/
- http://www.rau.edu.uy/ipv6/
- http://www.baquia.com/com/legacy/8364.html
- http://www.ipv6-taskforce.org/e-index.html