Tutorial de IPv6

1. Los motivos de IPv6

El motivo básico por el que surge, en el seno del IETF (Internet Engineering Task Force), la necesidad de crear un nuevo protocolo, que en un primer momento se denominó IPng (Internet Protocol Next Generation, o "Siguiente Generación del Protocolo Internet"), fue la evidencia de la falta de direcciones.

IPv4 tiene un espacio de direcciones de 32 bits, es decir, 2^{32} (4.294.967.296).

En cambio, IPv6 nos ofrece un espacio de 2^{128} (340.282.366.920.938.463.463.374.607.431.768.211.456).

Sin embargo, IPv4 tiene otros problemas o "dificultades" que IPv6 soluciona o mejora.

Los creadores de IPv4, a principio de los años 70, no predijeron en ningún momento, el gran éxito que este protocolo iba a tener en muy poco tiempo, en una gran multitud de campos, no sólo científicos y de educación, sino también en innumerables facetas de la vida cotidiana.

Podemos recordar algunas "famosas frases" que nos ayudarán a entender hasta que punto, los propios 'precursores' de la revolución tecnológica que estamos viviendo, no llegaron a prever:

- ✓ "Pienso que el mercado mundial de ordenadores puede ser de cinco unidades", Thomas Watson, Presidente de IBM en 1.943
- ✓ "640 Kbps. de memoria han de ser suficientes para cualquier usuario", Bill Gates, Presidente de Microsoft, 1.981
- ✓ "32 bits proporcionan un espacio de direccionamiento suficiente para Internet", Dr. Vinton Cerf, padre de Internet, 1.977

No es que estuvieran equivocados, sino que las Tecnologías de la Información han evolucionado de un modo mucho más explosivo de lo esperado. Además, ¿no dice el dicho "es de sabios rectificar"?

Desde ese momento, y debido a la multitud de nuevas aplicaciones en las que IPv4 ha sido utilizado, ha sido necesario crear "añadidos" al protocolo básico. Entre los "parches" más conocidos, podemos citar medidas para permitir la Calidad de Servicio (QoS), Seguridad (IPsec), y Movilidad, fundamentalmente.

El inconveniente más importante de estas ampliaciones de IPv4, es que utilizar cualquiera de ellos es muy fácil, pero no tanto cuando pretendemos usar al mismo tiempo dos "añadidos", y no digamos que se convierte en casi imposible o

muy poco práctico el uso simultáneo de tres o más, llegando a ser un auténtico malabarismo de circo.

2. ¿Porqué IPv6?

Como decía en párrafos anteriores, la ventaja fundamental de IPv6 es el espacio de direcciones.

El reducido espacio de IPv4, a pesar de disponer de cuatro mil millones de direcciones (4.294.967.296), junto al hecho de una importante falta de coordinación, durante la década de los 80, en la delegación de direcciones, sin ningún tipo de optimización, dejando incluso grandes espacios discontinuos, nos esta llevando a límites no sospechados en aquel momento.

Por supuesto, hay una solución que podríamos considerar como evidente, como sería la renumeración, y reasignación de dicho espacio de direccionamiento. Sin embargo, no es tan sencillo, es incluso impensable en algunas redes, ya que requiere unos esfuerzos de coordinación, a escala mundial, absolutamente impensables.

Además, uno de los problemas de IPv4 permanecería: la gran dimensión de las tablas de encaminado (routing) 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 (en Japón la situación esta llegando a ser crítica), y Europa, el problema se agrava.

Como ejemplos, podemos citar el caso de China que ha pedido direcciones para conectar 60.000 escuelas, 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.

Tanto en Japón como en Europa el problema es creciente, dado al importante desarrollo de las redes de telefonía celular, inalámbricas, módems 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 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, podemos ver dispositivos “siempre conectados”, con lo que fácilmente un usuario podría tener, en un futuro no muy lejano, hasta 50 o 100 IP’s (1:50 o 1:100).

Algunos Proveedores de Servicios Internet se ven incluso obligados a proporcionar a sus clientes direcciones IP privadas, mediante mecanismos de NAT (traslación de direcciones, es decir, usar una sola IP pública para toda una red privada). De hecho, casi todos los PSI’s se ven obligados a delegar tan sólo 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 quedan relegadas a su uso en Intranets, dado que muchos protocolos son incapaces de atravesar los dispositivos NAT:

- RTP y RTCP ("Real-time Transport Protocol" 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.
- IPsec 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.

3. Cifras: el crecimiento de Internet

Las cifras de "internautas", esperadas en los próximos años, avalan lo expuesto:

- Africa: 800.000.000 (sólo 3.000.000 sin NAT)
- América Central y del Sur: 500.000.000 (sólo 10.000.000 sin NAT)
- 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)

Pero lo más importante es el imparable crecimiento de aplicaciones que necesitan direcciones IP públicas únicas, globales, válidas para conexiones extremo a extremo, y por tanto encaminables (enrutables): Videoconferencia, Voz sobre IP, seguridad, e incluso juegos.

Veamos más cifras. Sólo en Estados Unidos de América, el mercado potencial de aplicaciones susceptibles de ser conectadas a la red, según Driscol & Associates, en un estudio del año 1.995, era:

MERCADO VERTICAL	EJEMPLOS DE APLICACIÓN	TAMAÑO DEL MERCADO
Lectura de Contadores	Lectura de consumos de agua, gas, electricidad, etc.	242.000.000
Seguridad	Sistemas de alarma, incendios, etc., tanto residenciales como comerciales	24.000.000
Posicionamiento de Vehículos/flotas e información de condiciones	Seguimiento automático de vehículos Seguimiento de inventarios Diagnóstico y seguridad de vehículos	15.000.000
Monitorización	Máquinas de venta automática (vending) Buzones de correo Gas e irrigación	7.900.000
	Total	**288.900.000**

En 1.997, el mercado de dispositivos con aplicaciones capaces de conectarse a Internet (sin incluir terminales ni ordenadores, tan sólo WebTV, agendas electrónicas, teléfonos con acceso a Internet, y consolas de juegos), era de 3.000.000. En el año 1.998, este se duplica hasta llegar a los 6.000.000, y las previsiones de crecimiento para el 2.002, según IDC, son de 56.000.000.

Sólo contabilizando el crecimiento de la nueva generación de telefonía móvil (UMTS), en el año 2.003 se prevén cifras del orden de los 1.000.000.000 de usuarios, la misma cifra que para la telefonía fija y que para el número de usuarios "fijos" de Internet. En ese momento, los usuarios móviles con conexión a Internet se acercarán a los 400.000.000.

El mismo Foro UMTS/GSM prevé unas necesidades de direcciones IP para los dispositivos de la red (no para los dispositivos de los usuarios), para el año 2.005, de 3,2 millones, y de 6,3 para el 2.010. Según el mismo informe, en el 2.005, se requerirían un total de 20.000.000.000 de direcciones IP para los dispositivos de los usuarios.

A esto hemos de sumar los innumerables dispositivos que vamos creando, o los ya existentes a los que damos nuevas o mejoradas aplicaciones, mediante su conexión a la red, valgan como ejemplos:

- Teléfonos, pues la siguiente generación, sin duda, pasara por tecnologías IP (VoIP).
- Televisión y Radio, también basados en tecnologías IP.
- Sistemas de seguridad, televigilancia y control.
- Frigoríficos que evalúan nuestros hábitos de consumo y nos dan la opción de a) imprimir la lista de la compra, b) hacer el pedido en el supermercado para que nos sea entregado automáticamente, c) hacer el pedido para que pasemos a recogerlo decidiendo "in situ" el resto de la compra, d) navegar por un supermercado virtual y permitirnos llenar el carro según nuestros hábitos añadiendo nuestros caprichos ocasionales.
- Despertadores, que conocen nuestros tiempos de desplazamiento habituales a nuestro lugar de trabajo, y con motivo de un accidente o gran nevada, de los que son informados mediante los servicios de la red, calculan el tiempo adicional que necesitamos y nos levantan con la anticipación precisa, ¡aún a riesgo de que los destrocemos al arrojarlos contra la pared!
- Walkman MP3, que conectados a la red, nos permiten recuperar y almacenar creaciones musicales.

Nuevas tecnologías emergentes, como Bluetooth, WAP, redes inalámbricas, redes domésticas, etc., hacen más patente esta necesidad de crecimiento, al menos, en los que al número de direcciones se refiere.

Por ejemplo, la última tendencia es la de permitir a cualquier dispositivo serie, ser conectado a una LAN o WAN, y por que no a Internet. Este tipo de "convertidores", denominados "Universal Device Server", o Servidor de Dispositivos Universal, permite que aplicaciones impensables por las limitaciones de los cableados serie, se realicen remotamente a través de redes, o incluso que un sistema de alarmas, que antes requería un módem dedicado para la conexión con la central de recepción de alarmas, pueda ahora enviar un e-mail, ¡con todo lujo de detalles!.

Podríamos hablar, en general, de casi cualquier dispositivo tanto doméstico como industrial, integrado en la gran red, pero también en dispositivos de control médico, marcapasos, etc.

4. Conclusión

Me permito reflejar aquí una conclusión de una importante compañía de ingeniería y consultoría Canadiense, “Viagénie”, también miembro del Foro IPv6, que copreside el directorado técnico:

“La verdadera cuestión no es si necesitamos y creemos en IPv6, sino ¿estamos interesados en una red que permita a cualquier dispositivo electrónico IP comunicarse transparentemente con otros, independientemente de su localización, en LA red global?”

Mi propia conclusión, extendiendo la frase anterior, a la que me adhiero categóricamente, es:

“El camino de IPv4 a IPv6 no es una cuestión de transición ni de migración, sino de evolución, de integración, pero se trata de una evolución disruptora, rompedora, y al mismo tiempo necesaria. IPv6 nos permitirá un crecimiento escalable y simple, principales handicaps actuales de IPv4. Preparemos y mejoremos nuestras redes, las de nuestros clientes, las de nueva implantación, con dispositivos, sistemas operativos y aplicaciones que estén realmente listos o en camino de cumplir las especificaciones de IPv6, sin por ello dejar de ser válidos en IPv4. Hay que asegurar el futuro, no hipotecarlo, frente al inevitable *comercio electrónico móvil* (m-commerce), por la salud de la red global. Seamos y estemos ¡IPv6 READY!”

5. Características principales de IPv6

Si resumimos las características fundamentales de IPv6 obtenemos la siguiente relación:

- Mayor espacio de direcciones.
- “Plug & Play”: Autoconfiguración.
- Seguridad intrínseca en el núcleo del protocolo (IPsec).
- Calidad de Servicio (QoS) y Clase de Servicio (CoS).
- Multicast: Envío de UN mismo paquete a un grupo de receptores.
- Anycast: Envío de UN paquete a UN receptor dentro de UN grupo.
- Paquetes IP eficientes y extensibles, sin que haya fragmentación en los encaminadores (routers), alineados a 64 bits (preparados para su procesado óptimo con los nuevos procesadores de 64 bits), y con una cabecera de longitud fija, más simple, que agiliza su procesado por parte del encaminador (router).
- Posibilidad de paquetes con carga útil (datos) de más de 65.535 bytes.
- Encaminado (enrutado) más eficiente en el troncal (backbone) de la red, debido a una jerarquía de direccionamiento basada en la agregación.
- Renumeración y “multi-homing”, que facilita el cambio de proveedor de servicios.
- Características de movilidad.

Pero hay que insistir, de nuevo, en que estas son las características básicas, y que la propia estructura del protocolo permite que este crezca, o dicho de

otro modo, sea escalado, según las nuevas necesidades y aplicaciones o servicios lo vayan precisando.

Precisamente, la escalabilidad es la baza más importante de IPv6 frente a IPv4.

6. Un poco de "historia"

Básicamente ha habido tres fases importantes en el desarrollo de IPv4 hasta lo que hoy conocemos como IPv6:

- 1.992 – TUBA
  - Implementación de mecanismos para usar TCP y UDP sobre mayores direcciones.
  - Se emplea ISO CLNP (Connection-Less Network Protocol, "protocolo de redes sin conexión").
  - Se descarta.
- 1.993 – SIPP
  - Proyecto "Simple IP Plus".
  - Mezcla de SIP y PIP (dos tentativas anteriores para sustituir IPv4).
  - Direcciones de 64 bits.
- 1.994 – IPng
  - Se adopta SIPP.
  - Se cambia el tamaño de las direcciones a 128 bits.
  - Se renombra como IPv6.

Como fase adicional, muy significativa, podemos añadir la constitución oficial, en Julio de 1.999, del "IPv6 Forum" o Foro IPv6, que ha implicado, en un plazo de tan solo seis meses, un importantísimo crecimiento respecto del fomento, promoción, uso y aplicación del protocolo, con adopciones tan importantes como las realizadas por la OTAN, ETSI, UMTS, 3GPP, o la Comunidad Europea.

Por último, en el momento en que estas líneas están siendo escritas, entre el 13 y el 16 de Marzo de 2.000, en Telluride (Colorado – US), una pequeña población, antigua colonia minera fundada por Españoles, convertida ahora en un importante completo turístico dedicado al esquí, mientras se celebraba el 1er Congreso Internacional de IPv6 en Norteamérica (Global IPv6 Summit), organizado por el Foro IPv6, se ha producido un importante acontecimiento, de gran relevancia para IPv6.

La apertura del ciclo de conferencias ha incluido la presentación magistral de Judy Estrin, CTO (Chief Technology Officer) y Vice-Presidente Senior de Cisco Systems, y miembro de las juntas directivas de importantes empresas como Sun Microsystems, Walt Disney y Federal Express. En su cargo es responsable de la planificación de tecnologías estratégicas y desarrollo del negocio, incluyendo inversiones y adquisiciones, ingeniería de consultoría, proyectos avanzados de Internet, así como de asuntos legales y con el gobierno. Fue una de las personas

involucradas en los primeros desarrollos del protocolo TCP/IP, desde la Universidad de Stanford.

En su conferencia resaltó frases tan significativas como “Cisco esta comprometido con IPv6, pero estamos comprometidos con la integración, no con la transición”, y urgió a la comunidad IPv6 a proporcionar herramientas y técnicas de gestión que faciliten la integración de IPv6 con IPv4, indicando que “debemos traer IPv6 junto a IPv4, como dos afluentes que convergen para crear un río más poderoso”. Reconoció que Cisco ha percibido un creciente interés en IPv6, lo que les ha obligado, en los últimos seis meses, a tomar alternativas al respecto, con importantes esfuerzos de desarrollo al respecto.

Además, citó las siguientes tendencias como conductoras de la necesidad de IPv6:

- La creciente movilidad de los usuarios de Internet: los usuarios desean poder acceder a los mismos servicios Internet, tanto desde el trabajo, como desde su casa, como desde el coche, lo que crea la necesidad de más de una IP por persona.
- Redes domésticas: con la venida al hogar de accesos a Internet de gran ancho de banda, y oferta de servicios “siempre conectado”, los consumidores desean conectar a la red dispositivos de seguridad, al igual que otros muchos.
- La convergencia de voz, vídeo y datos, en infraestructuras basadas en IP: lo que implica el movimiento hacia la arquitectura ofrecida por IPv6, más simple, escalable y más fiable.

Judy Estrin remarcó que la infraestructura actual de IPv4 está extendida, y que el mayor espacio de direcciones de IPv6 ofrece ventajas y eficacias, pero que los métodos de implementación han de asegurar una integración suave, entre IPv4 e IPv6.

Según Judy, los desafíos para la implantación de IPv6 no son técnicos, sino de educación de los usuarios finales, y del desarrollo de casos de negocio para la tecnología. No debemos ilusionarnos sólo por una única aplicación definitiva.

Pocas horas después, dos relevantes proveedores de la industria de las Tecnologías de la Información, Cisco y Microsoft, han anunciado sus planes inmediatos de soportar “oficialmente” IPv6. Se puede encontrar más información al respecto se hallan en: http://www.networkworld.com/news/2000/0314ciscoipv6.html y http://www.microsoft.com/presspass/press/2000/Mar00/IPv6PR.asp.

Se trata de los último “gigantes” en confirmar su apoyo incondicional a IPv6, pues previamente, durante un evento similar, celebrado en Diciembre del pasado año, en Berlín, el resto de los fabricantes habían hecho similares anuncios.

De hecho, incluso antes de dicho encuentro, todos los fabricantes tenían versiones beta, para algunos de sus productos. En concreto, uno de ellos, Ericsson Telebit, dispone de productos comerciales con IPv6 desde hace varios años, y diversas plataformas UNIX también ofrecen dicho soporte.

Por otro lado, Sun Microsystems, anunciaba también la disponibilidad actual de la nueva versión de su Sistema Operativo Solaris 8, que YA incluye IPv6. Más información en http://www.sun.com/solaris/ipv6.

Además, Nokia y Cernet (red de educación e investigación China), anuncian la implantación mediante encaminadores (routers) de Nokia, de una nueva e importante red, dentro del programa "Internet 6", basada en este protocolo. La noticia completa esta disponible en http://www.businesswire.com/webbox/bw.031300/200731676.htm.

Por si no fuera suficiente, NTT Multimedia Communications Laboratories (MCL), subsidiaria de NTT Communications, anuncia la creación del primer nodo neutro de intercambio de tráfico Internet basado en IPv6, en Norteamérica, disponible en el mes de Abril próximo. Información completa disponible en http://www.businesswire.com/webbox/bw.031300/200730477.htm. En Berlín, durante otra de las conferencias del Foro IPv6, NTT hizo un anuncio similar, para el ámbito Europeo, incluso con ofertas de conexión gratuita, a dicho servicio, durante el primer año.

Se trata de un complejo e inesperado cúmulo de noticias al respecto de IPv6 que hacen prever una avalancha de otras nuevas, de similar índole, y que auguran un desarrollo mucho más rápido de los inicialmente previsto para IPv6.

Se dispone de un resumen actualizado de las noticias más relevantes respecto de IPv6 en http://www.ipv6forum.com/navbar/ipv6forum/pressroom.htm.

7. Los cimientos de IPv6

Los criterios que se han seguido a lo largo del desarrollo de IPv6 han sido fundamentales para obtener un protocolo sencillo y al mismo tiempo extremadamente consistente y escalable.

Son de destacar, entre estos criterios, además de todo lo dicho hasta el momento (número de direcciones, seguridad, movilidad y autoconfiguración) la especial aptitud para ser soportado por plataformas existentes, y una evolución que permite su uso concurrente con IPv4: No es necesario realizar un cambio "instantáneo en una fecha X", sino que el cambio es transparente.

Estos criterios se han alcanzado en gran medida por la ortogonalidad y simplificación de la cabecera de longitud fija, lo que redunda en la eficacia de su encaminado (enrutado), tanto en pequeños encaminadores como en los más grandes, con soportes de ancho de banda muy superiores a los 100 Gbytes con los dispositivos actuales.

Los equipos actuales, a pesar de sus tremendas capacidades de procesamiento de paquetes, no serían capaces de acometer la misma tarea, ni de ofrecer soluciones a todas las necesidades emergentes, con la estructura de la cabecera IPv4, sin contar la imposibilidad de gestionar las tablas de encaminado de los troncales, si siguen creciendo al ritmo actual.

8. Especificaciones básicas de IPv6 (RFC2460)

Veamos, en primer lugar, la descripción de la cabecera de un paquete IPv4:

bits: 4	8	16	20	32
Versión	Cabecera	TOS	Longitud Total	
Identificación			Indicador	Desplazamiento de Fragmentación
TTL		Protocolo	Checksum	
Dirección Fuente de 32 bits				
Dirección Destino de 32 bits				
Opciones				

Como vemos, la longitud mínima de la cabecera IPv4 es de 20 bytes (cada fila de la tabla supone 4 bytes). A ello hay que añadir las opciones, que dependen de cada caso.

En la tabla anterior hemos usado abreviaturas, en aquellos casos en los que son comunes. En el resto, nuestra "particular" traducción de la nomenclatura original anglosajona, cuya "leyenda de equivalencias" indicamos a continuación:

- Version – Versión (4 bits)
- Header – Cabecera (4 bits)
- TOS (Type Of Service) – Tipo de Servicio (1 byte)
- Total Length – Longitud Total (2 bytes)
- Identification – Identificación (2 bytes)
- Flag – Indicador (4 bits)
- Fragment Offset – Desplazamiento de Fragmentación (12 bits – 1.5 bytes)
- TTL (Time To Live) – Tiempo de Vida (1 byte)
- Protocol – Protocolo (1 byte)
- Checksum – Código de Verificación (2 bytes)
- 32 bit Source Address – Dirección Fuente de 32 bits (4 bytes)
- 32 bit Destination Address – Dirección Destino de 32 bits (4 bytes)

En la tabla anterior, hemos marcado, mediante el color de fondo, los campos que van a desaparecer en IPv6, y los que son modificados, según el siguiente esquema:

Campo Modificado
Campo que Desaparece

Hemos pasado de tener 12 campos, en IPv4, a tan solo 8 en IPv6.

El motivo fundamental por el que los campos son eliminados, es la innecesaria redundancia. En IPv4 estamos facilitando la misma información de varias formas. Un caso muy evidente es el checksum o verificación de la integridad de la cabecera: Otros mecanismos de encapsulado ya realizan esta función (IEEE 802 MAC, framing PPP, capa de adaptación ATM, etc.).

El caso del campo de “Desplazamiento de Fragmentación”, es ligeramente diferente, dado que el mecanismo por el que se realiza la fragmentación de los paquetes es totalmente modificado en IPv6, lo que implica la total “inutilidad” de este campo. En IPv6 los encaminadores no fragmentan los paquetes, sino que de ser precisa, dicha fragmentación/desfragmentación se produce extremo a extremo.

Algunos de los campos son renombrados:

- Longitud total ➔ longitud de carga útil (payload length), que en definitiva, es la longitud de los propios datos, y puede ser de hasta 65.536 bytes. Tiene una longitud de 16 bits (2 bytes).
- Protocolo ➔ siguiente cabecera (next header), dado que en lugar de usar cabeceras de longitud variables se emplean sucesivas cabeceras encadenadas, de ahí que desaparezca el campo de opciones. En muchos casos ni siquiera es procesado por los encaminadores, sino tan sólo extremo a extremo. Tiene una longitud de 8 bits (1 byte).
- Tiempo de vida ➔ límite de saltos (Hop Limit). Tiene una longitud de 8 bits (1 byte).

Los nuevos campos son:

- Clase de Tráfico (Traffic Class), también denominado Prioridad (Priority), o simplemente Clase (Class). Podría ser más o menos equivalente a TOS en IPv4. Tiene una longitud de 8 bits (1 byte).
- Etiqueta de Flujo (Flow Label), para permitir tráficos con requisitos de tiempo real. Tiene una longitud de 20 bits.

Estos dos campos, como se puede suponer, son los que nos permiten una de las características fundamentales e intrínsecas de IPv6: Calidad de Servicio (QoS), Clase de Servicio (CoS), y en definitiva un poderoso mecanismo de control de flujo, de asignación de prioridades diferenciadas según los tipos de servicios.

Por tanto, en el caso de un paquete IPv6, la cabecera tendría el siguiente formato:

El campo de versión, que es igual a 6, lógicamente, tiene una longitud de 4 bits.

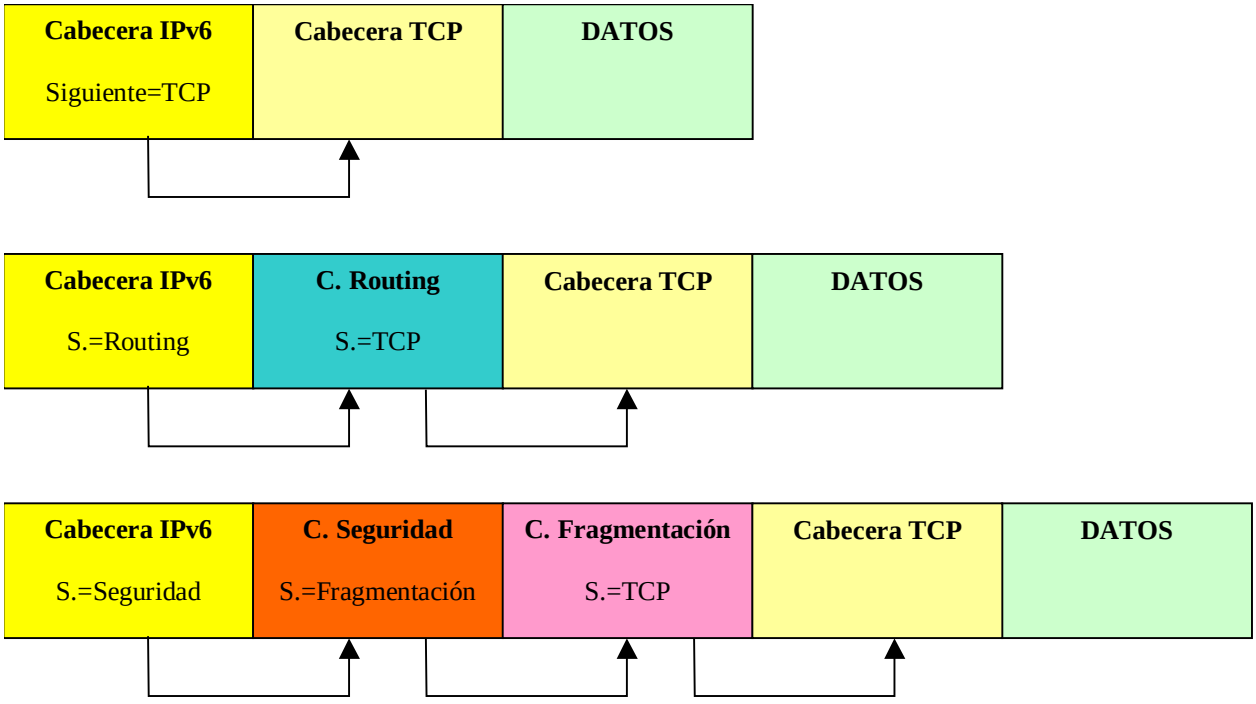
La longitud de esta cabecera es de 40 bytes, el doble que en el caso de IPv4, pero con muchas ventajas, al haberse eliminado campos redundantes.

Además, como ya hemos mencionado, la longitud fija de la cabecera, implica una mayor facilidad para su procesado en routers y conmutadores, incluso mediante hardware, lo que implica unas mayores prestaciones.

A este fin coadyuva, como hemos indicado anteriormente, el hecho de que los campos están alineados a 64 bits, lo que permite que las nuevas generaciones de procesadores y microcontroladores, de 64 bits, puedan procesar mucho más eficazmente la cabecera IPv6.

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, sino sólo en el nodo o nodos destino finales. Hay una única excepción a esta regla: cuando el valor de este campo es cero, lo que indica opción de examinado y proceso “salto a salto” (hop-by-hop). Así tenemos, por citar algunos ejemplos, cabeceras con información de encaminado, fragmentación, opciones de destino, autenticación, encriptación, etc., que en cualquier caso, han de ser procesadas en el orden riguroso en que aparecen en el paquete.

Sin entrar en más detalles, véanse a continuación los siguientes ejemplos gráficos del uso del concepto de las “cabeceras de extensión” (definidas por el campo “siguiente cabecera”), mecanismo por el que cada cabecera es “encadenada” a la siguiente y anterior (si existen):



El MTU (Unidad Máxima de Transmisión), debe de ser como mínimo, de 1.280 bytes, aunque se recomiendan tamaños superiores a 1.500 bytes. Los nodos descubren el valor MTU a través de la inspección de la ruta. Se prevé así una optimización de los paquetes y del número de cabeceras, dado el continuo crecimiento de los anchos de banda disponibles, así como del incremento del propio tráfico.

Dado que IPv6 no realiza verificación de errores de la cabecera, en tráfico UDP, se requiere el empleo del su propio mecanismo de checksum.

9. Direcciones y direccionamiento en IPv6 (RFC2373)

Ya hemos dicho que IPv6 nos aporta, como principio fundamental, un espacio de 2^{128} direcciones, lo que equivale a 3,40E38 (340.282.366.920.938.463.463.374.607.431.768.211.456).

Hagamos una cuenta "rápida", para hacernos a la idea de lo que esta cifra "impronunciable" implica. Calculemos el número de direcciones IP que podríamos tener por metro cuadrado de la superficie terrestre: ¡nada más y nada menos que 665.570.793.348.866.943.898.599!

Indudablemente, hay cabida para todos los dispositivos que podamos imaginar, no solo terrestres, sino interplanetarios. Aunque, por el momento, no podemos asegurar que tenga capacidad para los dispositivos "intergalácticos".

9.1. Definición de dirección en IPv6

Las direcciones IPv6 son identificadores de 128 bits para interfaces y conjuntos de interfaces. Dichas direcciones se clasifican en tres tipos:

- *Unicast*: Identificador para una única interfaz. Un paquete enviado a una dirección unicast es entregado sólo a la interfaz identificada con dicha dirección. Es el equivalente a las direcciones IPv4 actuales.
- *Anycast*: Identificador para un conjunto de interfaces (típicamente pertenecen a diferentes nodos). Un paquete enviado a una dirección anycast es entregado en una (cualquiera) 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 routing), si la primera "cae".
- *Multicast*: Identificador para un conjunto de interfaces (por lo general pertenecientes a diferentes nodos). Un paquete enviado a una dirección multicast es entregado a todas las interfaces identificadas por dicha dirección. La misión de este tipo de paquetes es evidente: aplicaciones de retransmisión múltiple (broadcast).

9.2. Diferencias con IPv4

Hay algunas diferencias importantes en el direccionamiento de IPv6 respecto de IPv4:

- 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.

- Cualquier campo puede contener sólo ceros o sólo unos, salvo que explícitamente se indique lo contrario.
- Las direcciones IPv6, indistintamente de su tipo (unicast, anycast o multicast), son asignadas a interfaces, no nodos. Dado que cada interfaz pertenece a un único nodo, cualquiera de las direcciones unicast de las interfaces del nodo puede ser empleado para referirse a dicho nodo.
- Todas las interfaces han de tener, al menos, una dirección unicast link-local (enlace local).
- Una única interfaz puede tener también varias direcciones IPv6 de cualquier tipo (unicast, anycast o multicast) o ámbito.
- Una misma dirección o conjunto de direcciones unicast pueden ser asignados a múltiples interfaces físicas, siempre que la implementación trate dichas interfaces, desde el punto de vista de internet, como una única, lo que permite balanceo de carga entre múltiples dispositivos.
- Al igual que en IPv4, se asocia un prefijo de subred con un enlace, y se pueden asociar múltiples prefijos de subred a un mismo enlace.

9.3. Reservas de espacio de direccionamiento en IPv6

A diferencia de las asignaciones de espacio de direccionamiento que se hicieron en IPv4, en IPv6, se ha reservado, que no "asignado", algo más del 15%, tanto para permitir una fácil transición (caso del protocolo IPX), como para mecanismos requeridos por el propio protocolo.

Estado	Prefijo (en binario)	Fracción del Espacio
Reservado	0000 0000	1/256
No Asignado	0000 0001	1/256
Reservado para NSAP	0000 001	1/128
Reservado para IPX	0000 010	1/128
No Asignado	0000 011	1/128
No Asignado	0000 1	1/32
No Asignado	0001	1/16
Direcciones Unicast Globales Agregables	001	1/8
No Asignado	010	1/8
No Asignado	011	1/8
No Asignado	100	1/8
No Asignado	101	1/8
No Asignado	110	1/8
No Asignado	1110	1/16
No Asignado	1111 0	1/32
No Asignado	1111 10	1/64
No Asignado	1111 110	1/128
No Asignado	1111 1110 0	1/512
Direcciones Unicast Locales de Enlace	1111 1110 10	1/1.024
Direcciones Unicast Locales de Sitio	1111 1110 11	1/1.024
Direcciones Multicast	1111 1111	1/256

De esta forma se permite la asignación directa de direcciones de agregación, direcciones locales, y direcciones multicast, con reservas para OSI NSAP e IPX. El 85% restantes queda reservado para uso futuro.

Podemos distinguir las direcciones multicast de las unicast por el valor del octeto de mayor orden de la dirección (FF, o 11111111 en binario, indica multi-

cast). En cambio, en el caso de las anycast, no hay ninguna diferencia, sintácticamente hablando, y por tanto, son tomadas del espacio de direcciones unicast.

9.4. Direcciones especiales en IPv6

Se han definido también las direcciones para usos especiales como:

- Dirección de auto-retorno o Loopback (::1) – No ha de ser asignada a una interfaz física; se trata de una interfaz "virtual", pues se trata de paquetes que no salen de la máquina que los emite; nos permite hacer un bucle para verificar la correcta inicialización del protocolo (dentro de una determinada máquina).
- Dirección no especificada (::) – Nunca debe ser asignada a ningún nodo, ya que 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.
- Túneles dinámicos/automáticos de IPv6 sobre IPv4 (::<dirección IPv4>) – Se denominan direcciones IPv6 compatibles con IPv4, y permiten la retransmisión de tráfico IPv6 sobre infraestructuras IPv4, de forma transparente.

80 bits	16 bits	32 bits
0000 ... 0000	0000	dirección IPv4

- Representación automática de direcciones IPv4 sobre IPv6 (::FFFF:<dirección IPv4>) – permite que los nodos que sólo soportan IPv4, puedan seguir trabajando en redes IPv6. Se denominan "direcciones IPv6 mapeadas desde IPv4".

80 bits	16 bits	32 bits
0000 ... 0000	FFFF	Dirección IPv4

9.5. Representación de las direcciones IPv6

La representación de las direcciones IPv6 sigue el siguiente esquema:

a) x:x:x:x:x:x:x:x, donde "x" es un valor hexadecimal de 16 bits, de la porción correspondiente a la dirección IPv6. No es preciso escribir los ceros a la izquierda de cada campo. Ejemplos:
   FEDC:BA98:7654:3210:FEDC:BA98:7654:3210
   1080:0:0:0:8:800:200C:417A

b) Dado que, por el direccionamiento que se ha definido, podrán existir largas cadenas de bits "cero", se permite la escritura de su abreviación, mediante el uso de "::", que representa múltiples grupos consecutivos de 16 bits "cero". Este símbolo sólo puede aparecer una vez en la dirección IPv6. Ejemplos:
   Las direcciones:
   1080:0:0:0:8:800:200C:417A (una dirección unicast)
   FF01:0:0:0:0:0:0:101 (una dirección multicast)
   0:0:0:0:0:0:0:1 (la dirección loopback)
   0:0:0:0:0:0:0:0 (una dirección no especificada)
   Pueden representarse como:

1080::8:800:200C:417A (una dirección unicast)
FF01::101 (una dirección multicast)
::1 (la dirección loopback)
:: (una dirección no especificada)

c) Una forma alternativa y muy conveniente, cuando nos hallemos en un entorno mixto IPv4 e IPv6, es x:x:x:x:x:x:d:d:d:d, donde "x" representa valores hexadecimales de 16 bits (6 porciones de mayor peso), y "d" representa valores decimales de las 4 porciones de 8 bits de menor peso (representación estándar IPv4). Ejemplos:
   0:0:0:0:0:0:13.1.68.3
   0:0:0:0:0:FFFF:129.144.52.38
   Pueden representarse como:
   ::13.1.68.3
   ::FFFF:129.144.52.38

La representación de los prefijos IPv6 se realiza del siguiente modo:

dirección-IPv6/longitud-del-prefijo

donde:

- dirección-IPv6 = una dirección IPv6 en cualquiera de las notaciones válidas
- longitud-del-prefijo = valor decimal indicando cuantos bits contiguos de la parte izquierda de la dirección componen el prefijo

Por ejemplo, las representaciones válidas del prefijo de 60 bits 12AB00000000CD3, son:

12AB:0000:0000:CD30:0000:0000:0000:0000/60
12AB::CD30:0:0:0:0/60
12AB:0:0:CD30::/60

Por tanto, para escribir una dirección completa, indicando la subred, podríamos hacerlo como:

12AB:0:0:CD30:123:4567:89AB:CDEF/60

9.6. Direcciones unicast locales

Las direcciones unicast, son agregables con máscaras de bits contiguos, similares al caso de IPv4, con CIDR (Class-less Interdomain Routing). Como hemos visto, hay varias formas de asignación de direcciones unicast, y otras pueden ser definidas en el futuro.

Los nodos IPv6 pueden no tener ningún conocimiento o mínimo de la estructura interna de las direcciones IPv6, 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., en ocasiones dependiendo de la posición misma que el dispositivo o host/router, ocupa en la propia red.

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. Por lo general, el identificador de interfaz coincidirá con la dirección de la capa de enlace de dicha interfaz. El mismo identificador de interfaz puede ser empleado en múltiples interfaces del mismo nodo, sin afectar a su exclusividad global en el ámbito IPv6.

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

Las 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:

10 bits	54 bits	64 bits
1111111010	0	Identificador de interfaz

Se trata de direcciones FE80::<ID de interfaz>/10.

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).

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

Se trata de direcciones FEC0::<ID de subred>:<ID de interfaz>/10.

9.7. Direcciones anycast (RFC2526)

Tal y como hemos indicado antes, 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 IPv6 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	

9.8. Direcciones multicast (RFC2375)

Una dirección multicast en IPv6, puede definirse como un identificador para un grupo de nodos. Un nodo puede pertenecer a uno o varios 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 Local de Organización
9	No asignado
A	No asignado
B	No asignado
C	No asignado
D	No asignado
E	Ambito Global
F	Reservado

El “Identificador 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
- FF0E::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 di-

rección 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 IPv6, 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.

9.9. Direcciones Requeridas para cualquier nodo

Todos los nodos, en el proceso de identificación, al unirse a la red, deben de reconocer como mínimo, las siguientes direcciones:

- Sus direcciones locales de enlace para cada interfaz
- Las direcciones unicast asignadas
- La dirección de loopback
- Las direcciones multicast de todos los nodos
- Las direcciones multicast solicitadas para cada dirección unicast o anycast asignadas
- Las direcciones multicast de todos los grupos a los que dicho host pertenece

Además, en el caso de los routers, tienen que reconocer también:

- La dirección anycast del router de la subnet, para las interfaces en las que esta configurado para actuar como router
- Todas las direcciones anycast con las que el router ha sido configurado
- Las direcciones multicast de todos los routers
- Las direcciones multicast de todos los grupos a los que el router pertenece

Además, todos los dispositivos con IPv6, deben de tener, predefinidos, los prefijos siguientes:

- Dirección no especificada
- Dirección de loopback
- Prefijo de multicast (FF)
- Prefijos de uso local (local de enlace y local de sitio)
- Direcciones multicast predefinidas
- Prefijos compatibles IPv4

Se debe de asumir que todas las demás direcciones son unicast a no ser que sean específicamente configuradas (por ejemplo las direcciones anycast).

9.10. Direcciones unicast globales agregables (RFC2374)

Dado que uno de los problemas que IPv6 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 IPv6, permiten su continuidad. Pero además, se incorpora 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.

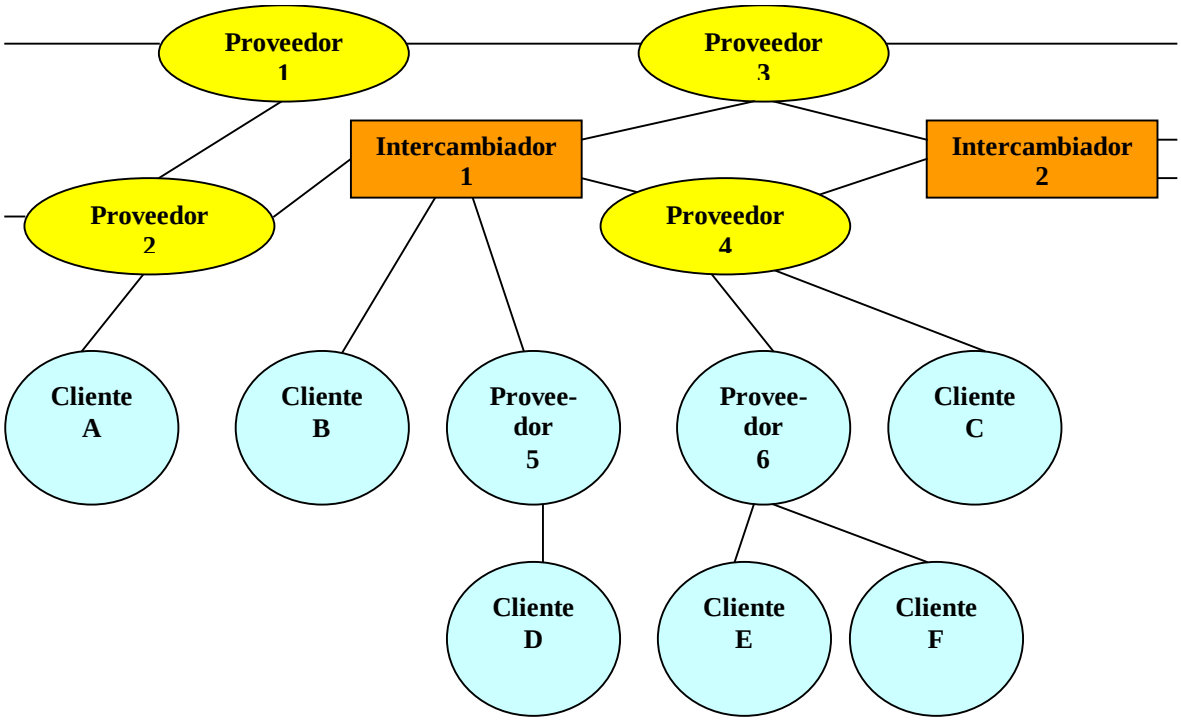
Se trata de una organización basada en tres niveles:

- 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”.
- Identificador de Interfaz: identifican interfaces de enlaces.

En la figura adjunta, el formato de direcciones agregables ha sido diseñado para soportar proveedores de larga distancia (identificados como Proveedor 1-4), intercambiadores (Intercambiador 1 y 2), proveedores de niveles inferiores (podrían ser ISP’s, identificados como Proveedor 5 y 6), y Clientes (Cliente A-F).

A diferencia de lo que ocurre actualmente, los intercambiadores también proporcionarán direcciones públicas IPv6. 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 IPv6.



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.

9.10.1. Estructura de direcciones unicast globales agregables

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 →

Donde:

FP	Prefijo de Formato (001) - Format Prefix
TLA ID	Identificador de Agregación de Nivel Superior - Top-Level Aggregation Identifier
Res.	Reservado para uso futuro
NLA ID	Identificador de Agregación de Siguiente Nivel - Next-Level Aggregation Identifier
SLA ID	Identificador de Agregación de Nivel de Sitio - Site-Level Aggregation Identifier
Interfaz ID	Identificador de Interfaz

El campo Reservado 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.

9.10.2. Identificador 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.

Esta estructura de direccionamiento permite 8.192 (2^{13}) identificadores de TLA. Se prevé su crecimiento haciendo que este campo crezca hacia la derecha en el espacio reservado para el futuro, o usando este mismo formato/estructura para prefijos de formato (FP) adicionales.

9.10.3. Identificador 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.

n	24-n bits	16	64 bits
NLA1	Site ID	SLA ID	Interfaz ID

Dado que cada organización que recibe un TLA dispone de 24 bits de espacio NLA, permite proporcionar servicio aproximadamente al número total de direcciones IPv4 soportadas actualmente.

Las organizaciones que reciben un TLA pueden soportar varios NLA en su propio espacio de direccionamiento (Site ID). Esto permite que sirvan tanto a clientes directos (suscriptores) como a otras organizaciones proveedoras de servicios públicos de tránsito. Y así sucesivamente, como se muestra en la siguiente figura:

n	24-n bits			16	64 bits
NLA1	Site ID			SLA ID	Interfaz ID
	m	24-n-m bits		16	64 bits
	NLA2	Site ID		SLA ID	Interfaz ID
		o	24-n-m-o bits	16	64 bits
		NLA3	Site ID	SLA ID	Interfaz ID

El diseño del espacio NLA de cada organización es libre para cada TLA asignado, y así sucesivamente con los niveles inferiores. Sin embargo, se recomienda seguir los procedimientos del RFC2050.

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.

9.10.4. Identificador 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 IPv4, 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, según la figura adjunta:

n	16-n bits		64 bits
SLA1	Subred		Interfaz ID
	m	16-n-m bits	64 bits
	SLA2	Subred	Interfaz ID

Una gran compañía podría necesitar varios identificadores SLA. Como es lógico, cada caso dependerá de cómo están conectadas sus diversas delegaciones.

9.11. Formato para la representación en URL’s (RFC2732)

Cuando navegamos, continuamente aludimos a URL, en muchas ocasiones sin conocer el significado precios de esta abreviatura.

La especificación original (RFC2396), que data del año 1.988, nos dice que Uniform Resource Locator (Localizador de Recurso Uniforme), es un medio simple y extensible para identificar un recurso a través de su localización en la red.

Una vez aclarado esto, y de la misma forma que en ocasiones usamos direcciones en formato IPv4 para escribir un URL, se han descrito unas normas pa-

ra realizar la representación literal de direcciones IPv6 cuando se usan herramientas de navegación WWW.

El motivo por el que ha sido preciso realizar esta definición es bien simple. Con la anterior especificación no estaba permitido emplear el carácter ":" en una dirección, sino como separador de "puerto". Por tanto, si se desea facilitar operaciones tipo "cortar y pegar" (cut and paste), para trasladar direcciones entre diferentes aplicaciones, de forma rápida, era preciso buscar una solución que evitase la edición manual de las direcciones IPv6.

La solución es bien sencilla: el empleo de los corchetes ("[","]") para encerrar la dirección IPv6, dentro de la estructura habitual del URL.

Veamos algunos ejemplos; las direcciones siguientes:

- FEDC:BA98:7654:3210:FEDC:BA98:7654:3210
- 1080:0:0:0:8:800:200C:4171
- 3ffe:2a00:100:7031::1
- 1080::8:800:200C:417A
- ::192.9.5.5
- ::FFFF:129.144.52.38
- 2010:836B:4179::836B:4179

Serían representadas como:

- http://[FEDC:BA98:7654:3210:FEDC:BA98:7654:3210]:80/index.html
- http://[1080:0:0:0:8:800:200C:417A]/index.html
- http://[3ffe:2a00:100:7031::1]
- http://[1080::8:800:200C:417A]/foo
- http://[::192.9.5.5]/ipng
- http://[::FFFF:129.144.52.38]:80/index.html
- http://[2010:836B:4179::836B:4179]

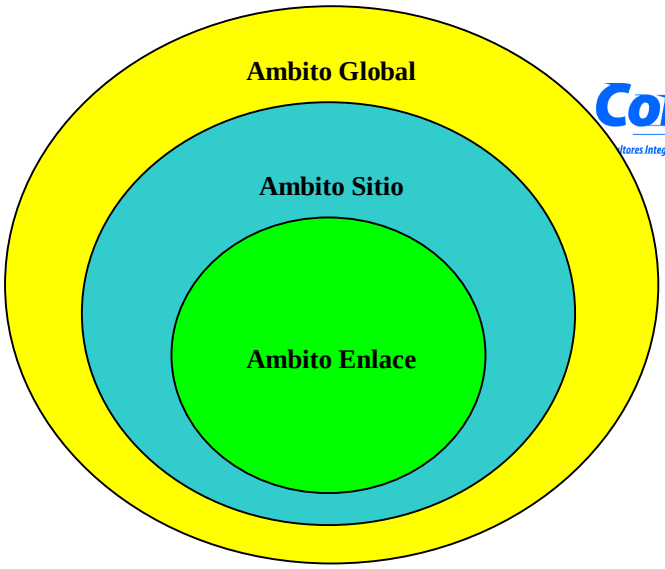
Hemos añadido alguna "complicación", para que el propio lector descubra el uso del separador de puertos.

9.12. Resumiendo

Puede parecerle, al lector, un esquema muy complejo, pero en realidad es muy simple y sobre todo, muy eficiente.

Los resultados de este esquema son:

a) Las direcciones siguen siendo asignadas por el proveedor, pero al cambiar de proveedor, sólo cambia el prefijo, y la red se "renumera" automáticamente (routers, sitios y nodos finales – dispositivos – servidores).



b) Las interfaces pueden tener múltiples direcciones.

c) Las direcciones tienen ámbito (Global, Sitio, Enlace).

d) Las direcciones, al estar compuestas por un prefijo y un identificador de interfaz, nos permiten separar “quién es” de “donde esta conectado”:

e) Además, las direcciones tienen un período de vida (de validez).

El RFC2450 propone las reglas para la administración de los TLA’s y NLA’s. Además, en http://www.arin.net/regserv/ipv6/IPv6.txt, podemos encontrar más información al respecto de las normas para registros IPv6, del mismo modo que en http://www.ripe.net/ripencc/about/regional/maps/ipv6policy-draft-090699.html, o en http://www.apnic.net/drafts/ipv6/ipv6-policy-280599.html. En todos los casos, la máxima autoridad competente es IANA (Internet Assigned Numbers Authority).

10. ICMPv6 (RFC2463)

El Protocolo de Mensajes de Control de Internet (Internet Control Message Protocol), descrito originalmente en el documento RFC792 para IPv4, ha sido actualizado para permitir su uso bajo IPv6.

El protocolo resultante de dicha modificación es ICMPv6, y se le ha asignado un valor, para el campo de “siguiente cabecera”, igual a 58. ICMPv6 es parte integral de IPv6 y debe ser totalmente incorporado a cualquier implementación de nodo IPv6.

ICMPv6 es empleado por IPv6 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 ICMPv6 es el siguiente:

bits 8	16	32
Tipo	Código	Checksum
Cuerpo del Mensaje		

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 ICMPv6.

Los mensajes ICMPv6 se agrupan en dos tipos o clases: mensaje de error y mensajes informativos. Los mensajes de error tienen 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 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)	

Se esta trabajando en nuevos tipos de mensajes, siendo el más interesante de ellos el definido en un borrador de IETF (draft-ietf-ipngwg-icmp-name-lookups-05.txt), que permitirá solicitar a un nodo información completa como su “nombre de dominio completamente cualificado” (Fully-Qualified-Domain-Name).

Por razones de seguridad, las cabeceras ICMPv6 pueden ser autenticadas y encriptadas, usando la cabecera correspondiente. El uso de este mecanismo permite, además, la prevención de ataques ICMP, como el conocido “Negación de Servicio” (DoS o Denial of Service Attack).

11. Neighbor Discovery (RFC2461)

En IPv6, el protocolo equivalente, en cierto modo, a ARP en IPv4, es el que denominamos “descubrimiento del vecindario”. Sin embargo, incorpora también la funcionalidad de otros protocolos IPv4, como “ICMP Router Discovery” y “ICMP Redirect”.

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 Discovery”), 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 alternativas funcionales.

ND emplea los mensajes de ICMPv6, incluso a través de mecanismos de multicast en la capa de enlace, para algunos de sus servicios.

El protocolo ND es bastante completo y sofisticado, ya que es la base para permitir el mecanismo de autoconfiguración en IPv6.

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.

ND define cinco tipos de paquetes ICMPv6:

- Solicitud de Router (Router Solicitation) – generado por una interfaz cuando es activada, para pedir a los routers que se “anuncien” inmediatamente. Tipo en paquete ICMPv6 = 133.
- Anunciación de Router (Router Advertisement) – generado por los routers periódicamente (entre cada 4 y 1800 segundos) o como consecuencia de una “solicitud de router”, a través de multicast, para informar de su presencia así como de otros parámetros de enlace y de Internet, como prefijos (uno o varios), tiempos de vida, configuración de direcciones, límite de salto sugerido, etc. Es fundamental para permitir la renumeración. Tipo en paquete ICMPv6 = 134.
- Solicitud de Vecino (Neighbor Solicitation) – generado por los nodos para determinar la dirección en la capa de enlace de sus vecinos, o para verificar que el nodo vecino sigue activo (es alcanzable), así como para detectar las direcciones duplicadas. Tipo en paquete ICMPv6 = 135.
- Anunciación de Vecino (Neighbor Advertisement) – generado por los nodos como respuesta a la “solicitud de vecino”, o bien para indicar cambios de direcciones en la capa de enlace. Tipo en paquete ICMPv6 = 136.

- Redirección (Redirect) – generado por los routers para informar a los host de un salto mejor para llegar a un determinado destino. Equivalente, en parte a “ICMP redirect”. Tipo en paquete ICMPv6 = 137.

El protocolo ND, frente a los mecanismos existentes en IPv4, reporta numerosas ventajas:

- El descubrimiento de routers es parte de la base del protocolo, no es preciso recurrir a los protocolos de encaminado.
- La anunciación de router incluye las direcciones de la capa de enlace, no es necesario ningún intercambio adicional de paquetes para su resolución.
- La anunciación de router incluye los prefijos para el enlace, por lo que no hay necesidad de un mecanismo adicional para configurar la máscara de red.
- La anunciación de router permite la autoconfiguración de direcciones
- Los routers pueden anunciar a los host del mismo enlace el MTU (tamaño máximo de la unidad de transmisión).
- Se extienden los multicast de resolución de direcciones entre 2^{32} direcciones, reduciendo de forma importante las interrupciones relativas a la resolución de direcciones en nodos distintos al objetivo, y evitando las interrupciones en nodos sin IPv6.
- Las redirecciones contienen la dirección de la capa de enlace del nuevo salto, lo que evita la necesidad de una resolución de dirección adicional.
- Se pueden asignar múltiples prefijos al mismo enlace y por defecto los host aprenden todos los prefijos por la anunciación de router. Sin embargo, los routers pueden ser configurados para omitir parte o todos los prefijos en la anunciación, de forma que los host consideren que los destinos están fuera del enlace; de esta forma, enviarán el tráfico a los routers, quién a su vez lo redireccionará según corresponda.
- A diferencia de IPv4, en IPv6 el receptor de una redirección asume que el siguiente salto esta en el mismo enlace. Se prevé una gran utilidad en el sentido de no ser deseable o posible que los nodos conozcan todos los prefijos de los destinos en el mismo enlace (enlaces sin multidifusión y media compartida).
- La detección de vecinos no alcanzables es parte de la base de mejoras para la robustez en la entrega de paquetes frente a fallos en routers, particiones de enlaces, nodos que cambian sus direcciones, nodos móviles, etc.
- A diferencia de ARP, en ND se puede detectar fallos de la mitad del enlace, es decir, con conectividad en un sólo sentido, evitando el tráfico hacia ellos.
- A diferencia de IPv4, no son precisos campos de preferencia (para definir la “estabilidad” de los routers). La detección de vecinos no alcanzables sustituirá los caminos desde routers con fallos a otros activos.
- El uso de direcciones de enlace local para identificar routers, permite a los hosts que mantengan su asociación con los mismos, en el caso de que se realice una renumeración para usar nuevos prefijos globales.

- El límite de saltos es siempre igual a 255, lo que evita que haya envíos accidentales o intencionados desde nodos fuera del enlace, dado que los routers decrementan automáticamente este campo en cada salto.
- Al realizar la resolución de direcciones en la capa ICMP, se independiza el protocolo del medio, permitiendo mecanismos de autenticación y seguridad normalizados.

En este RFC se describe, además, el "modelo conceptual" de las estructuras de datos y su manipulación, que un dispositivo (host o router) requeriría para cumplir los protocolos IPv6. Se trata, pues, de un documento clave para la correcta interpretación de IPv6, cuando se trata de aplicarlo a su uso por parte de desarrolladores.

En resumen, ND reemplaza, con grandes mejoras e importantes ventajas, a ARP.

12. Autoconfiguración en IPv6 (RFC2462)

La autoconfiguración es el conjunto de pasos por los cuales un host decide como autoconfigurar sus interfaces en IPv6. Este mecanismo es el que nos permite afirmar que IPv6 es "Plug & Play".

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

En la autoconfiguración "stateful" (predeterminada), el host obtiene la dirección de la interfaz y/o la información y parámetros de configuración desde un servidor. Los servidores mantienen una base de datos con las direcciones que han sido asignadas a cada host.

Ambos tipos de autoconfiguración (stateless y stateful), se complementan. Un host puede usar autoconfiguración sin intervención (stateless), para generar

su propia dirección, y obtener el resto de parámetros mediante autoconfiguración predeterminada (stateful).

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

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

Cada dirección es cedida a una interfaz durante un tiempo predefinido (posiblemente infinito). Las direcciones tienen asociado un tiempo de vida, que indican durante cuanto tiempo esta vinculada dicha dirección a una determinada interfaz. Cuando el tiempo de vida expira, la vinculación se invalida y la dirección puede ser reasignada a otra interfaz en cualquier punto de Internet.

Para gestionar la expiración de los vínculos, una dirección pasa a través de dos fases diferentes mientras está asignada a una interfaz. Inicialmente, una dirección es “preferred” (preferida), lo que significa que su uso es arbitrario y no está restringido. Posteriormente, la dirección es “deprecated” (desaprobada), en anticipación a que el vínculo con su interfaz actual va a ser anulado.

Mientras esta en estado “desaprobado”, su uso es desaconsejado, aunque no prohibido. Cualquier nueva comunicación (por ejemplo, una nueva conexión TCP), debe usar una dirección “preferida”, siempre que sea posible.

Una dirección “desaprobada” debería ser usada tan solo por aquellas aplicaciones que ya la venían utilizando y a las que les es muy difícil cambiar a otra dirección sin interrupción del servicio.

Para asegurarse de que todas las direcciones configuradas son únicas, en un determinado enlace, los nodos ejecutan un algoritmo de detección de direcciones duplicadas, antes de asignarlas a una interfaz. Este algoritmo es ejecutado para todas las direcciones, independientemente de que hayan sido obtenidas mediante autoconfiguración stateless o stateful.

La autoconfiguración esta diseñada para hosts, no para routers, aunque ello no implica que parte de la configuración de los routers también pueda ser realizada automáticamente (generación de direcciones de enlace local). Además, los routers también tienen que “aprobar” el algoritmo de detección de direcciones duplicadas.

12.1. Autoconfiguración Stateless

El procedimiento de autoconfiguración stateless (sin intervención o descubrimiento automático), ha sido diseñado con las siguientes premisas:

- Evitar la configuración manual de dispositivos antes de su conexión a la red. Se requiere, en consecuencia, un mecanismo que permita a los host obtener o crear direcciones únicas para cada una de sus interfaces, asumiendo que cada interfaz puede proporcionar un identificador único para si misma (identificador de interfaz). En el caso más simple, el identificador de interfaz consiste en la dirección de la capa de enlace, de dicha

interfaz. El identificador de interfaz puede ser combinado con un prefijo, para formar la dirección.

- Las pequeñas redes o sitios, con máquinas conectadas a un único enlace, no deberían requerir la presencia de un servidor “stateful” o router, como requisito para comunicarse. Para obtener, en este caso, características “plug & play”, empleamos las direcciones de enlace local, dado que tienen un prefijo perfectamente conocido que identifica el único enlace compartido, al que se conectan todos los nodos. Cada dispositivo forma su dirección de enlace local anteponiendo el prefijo de enlace local a su identificador de interfaz.
- En el caso de redes o sitios grandes, con múltiples subredes y routers, tampoco se requiere la presencia de un servidor de configuración de direcciones “stateful”, ya que los host han de determinar, para generar sus direcciones globales o de enlace local, los prefijos que identifican las subredes a las que se conectan. Los routers generan mensajes periódicos de anunciación, que incluyen opciones como listas de prefijos activos en los enlaces.
- La configuración de direcciones debe de facilitar la renumeración de los dispositivos de un sitio, por ejemplo, cuando se desea cambiar de proveedor de servicios. La renumeración se logra al permitir que una misma interfaz pueda tener varias direcciones, que recibe “en préstamo”. El tiempo del “préstamo” es el mecanismo por el que se renuevan las direcciones, al expirar los plazos para las viejas, sin que se conceda una prórroga. Al poder disponer de varias direcciones simultáneamente, permite que la transición no sea “disruptora”, permitiendo que ambas, la vieja y la nueva dirección den continuidad a la comunicación durante el período de transición.
- Sólo es posible utilizar este mecanismo en enlaces capaces de funciones multicast, y comienza, por tanto, cuando es iniciada o activada una interfaz que permite multicast.
- Los administradores de sistemas necesitan la habilidad de especificar que mecanismo (stateless, stateful, o ambos), deben ser usados. Los mensajes de anunciación de los routers incluyen indicadores para esta función.

Los pasos básicos para la autoconfiguración, una vez la interfaz ha sido activada, serían:

a) Se genera la dirección “tentativa” de enlace local, como se ha descrito antes.
b) Verificar que dicha dirección “tentativa” puede ser asignada (no esta duplicada en el mismo enlace).
c) Si esta duplicada, la autoconfiguración se detiene, y se requiere un procedimiento manual (por ejemplo, usando otro identificador de interfaz).
d) Si no esta duplicada, la conectividad a nivel IP se ha logrado, al asignarse definitivamente dicha dirección “tentativa” a la interfaz en cuestión.
e) Si se trata de un host, se interroga a los posibles routers para indicar al host lo que debe de hacer a continuación.
f) Si no hay routers, se invoca el procedimiento de autoconfiguración “stateful”.

g) Si hay routers, estos contestarán indicando fundamentalmente, como obtener las direcciones si se ha de utilizar el mecanismo “stateful”, u otra información, como tiempos de vida, etc.

Hay algunos detractores de este mecanismo, ya que implica que cualquier nodo puede ser identificado en una determinada red si se conoce su identificador IEEE (dirección MAC). Por ello, para permitir que la dirección no sea estática, se esta trabajando en el documento draft-ietf-ipngwg-addrconf-privacy-01.txt.

12.2. Autoconfiguración Stateful – DHCPv6 (draft-ietf-dhc-dhcpv6-15.txt)

DHCP para IPv6 es un protocolo UDP cliente/servidor, diseñado para reducir el coste de gestión de nodos IPv6 en entornos donde los administradores precisan un control sobre la asignación de los recursos de la red, superior al facilitados por el mecanismo de configuración “stateless”.

Como ya hemos indicado, ambos mecanismos pueden usarse de forma concurrente para reducir el coste de propiedad y administración de la red.

Para lograr este objetivo, se centraliza la gestión de los recursos de la red, tales como direcciones IP, información de encaminado, información de instalación de Sistemas Operativos, información de servicios de directorios, sobre uno o varios servidores DHCP, en lugar de distribuir dicha información en ficheros de configuración locales en cada nodo.

Además, DHCP ha sido diseñado para ser fácilmente extensible con nuevos parámetros de configuración, a través de “extensiones” que incorporan esta nueva información. Al respecto es fundamental el documento dhc-v6exts-12.txt.

Los objetivos de DHCPv6 son:

- DHCP es un mecanismo, no una política. La política es establecida por el administrador de la red y DHCP le permite propagar los parámetros adecuados, según dicha política.
- DHCP es compatible, lógicamente, con el mecanismo de autoconfiguración “stateless”.
- DHCP no requiere configuración manual de parámetros de red en clientes DHCP, excepto en casos donde dicha configuración se requiere debido a medidas de seguridad.
- DHCP no requiere un servidor en cada enlace, dado que debe funcionar a través de relés DHCP.
- DHCP coexiste con nodos configurados estáticamente, así como con implementaciones existentes en la red.
- Los clientes DHCP pueden operar en enlaces donde no hay routers IPv6.
- Los clientes DHCP proporcionan la habilidad de renumerar la red.
- Un cliente DHCP puede hacer múltiples y diferentes peticiones de parámetros de configuración, de uno o varios servidores DHCP simultáneamente. DHCP proporciona suficiente información para permitir a los servidores DHCP el seguimiento del estado de configuración de los clientes.

- DHCP incorpora los mecanismos apropiados de control de tiempo y retransmisiones para operar eficazmente en entornos con una alta latencia y/o reducido ancho de banda.

Los cambios fundamentales entre DHCPv4 y DHCPv6, están basados en el soporte inherente del formato de direccionamiento y autoconfiguación IPv6; son las siguientes:

- La dirección de enlace local permite a un nodo tener una dirección tan pronto como arranca, lo que significa que todos los clientes tienen una dirección IP fuente para localizar un servidor o relé en su mismo enlace.
- Los indicadores de compatibilidad BOOTP y broadcast han desaparecido.
- El multicast y los ámbitos de direccionamiento permiten el diseño de paquetes de descubrimiento, que definen por si mismos su rango por la dirección multicast, para la función requerida.
- La autoconfiguración stateful ha de coexistir e integrarse con la stateless, soportando la detección de direcciones duplicadas y los dos tiempos de vida de IPv6, para facilitar la renumeración automática de direcciones y su gestión.
- Se soportan múltiples direcciones por cada interfaz.
- Algunas opciones DHCPv4 ya no son precisas, debido a que los parámetros de configuración se obtienen a través de ND o del protocolo de localización de servicios (RFC2165).

De esta forma, se soportan las siguientes funciones nuevas:

- Configuración de actualizaciones dinámicas de DNS.
- Desaprobación de direcciones, para renumeración dinámica.
- Relés preconfigurados con direcciones de servidores, o mediante multicast.
- Autenticación.
- Los clientes pueden pedir múltiples direcciones IP.
- Las direcciones pueden ser reclamadas mediante el mensaje de “iniciar-reconfiguración”.
- Integración entre autoconfiguración de direcciones “stateless” y “stateful”
- Permitir relés para localizar servidores fuera del enlace.

12.3. Renumeración

En los párrafos anteriores ya hemos descrito el mecanismo básico de renumeración, basado en el “préstamo” o alquiler de direcciones, en las fases de “preferida” y “desaprobada”, y en el tiempo de vida de las mismas.

En cualquier caso, podemos describir el mecanismo de forma sencilla, como consistente en disminuir el tiempo de vida del prefijo en los paquetes de anunciación del router, de forma que las direcciones pasen a ser desaprobadas, frente a las nuevas, que pasan a ser preferidas.

Sin embargo, este mecanismo está básicamente diseñado para los host. En el caso de los routers, se trabaja en un nuevo documento “draft-ietf-ipngwg-router-renum-10.txt”, que permitirá mecanismos similares y más adecuados.

13. IPv6 sobre Ethernet (RFC2464)

Aunque ya han sido definidos protocolos para permitir el uso de IPv6 sobre cualquier tipo de red o topología (Token Ring, FDDI, ATM, PPP, ...), como ejemplo mucho más habitual y básico, centraremos este apartado en Ethernet (CSMA/CD y tecnologías full-duplex basadas en ISO/IEC8802-3). Mas adelante, en este mismo documento, citaremos los protocolos adecuados para cada una de las otras tecnologías.

Los paquetes IPv6 se transmiten sobre tramas normalizadas Ethernet. La cabecera Ethernet contiene las direcciones fuente y destino Ethernet, y el código de tipo Ethernet con el valor hexadecimal 86DD.

El campo de datos contiene la cabecera IPv6 seguida por los propios datos, y probablemente algunos bytes para alineación/relleno, de forma que se alcance el tamaño mínimo de trama para el enlace Ethernet.

48 bits	48 bits	16 bits	
Dirección Ethernet Destino	Dirección Ethernet Fuente	1000011011011101 (86DD)	Cabecera y datos IPv6

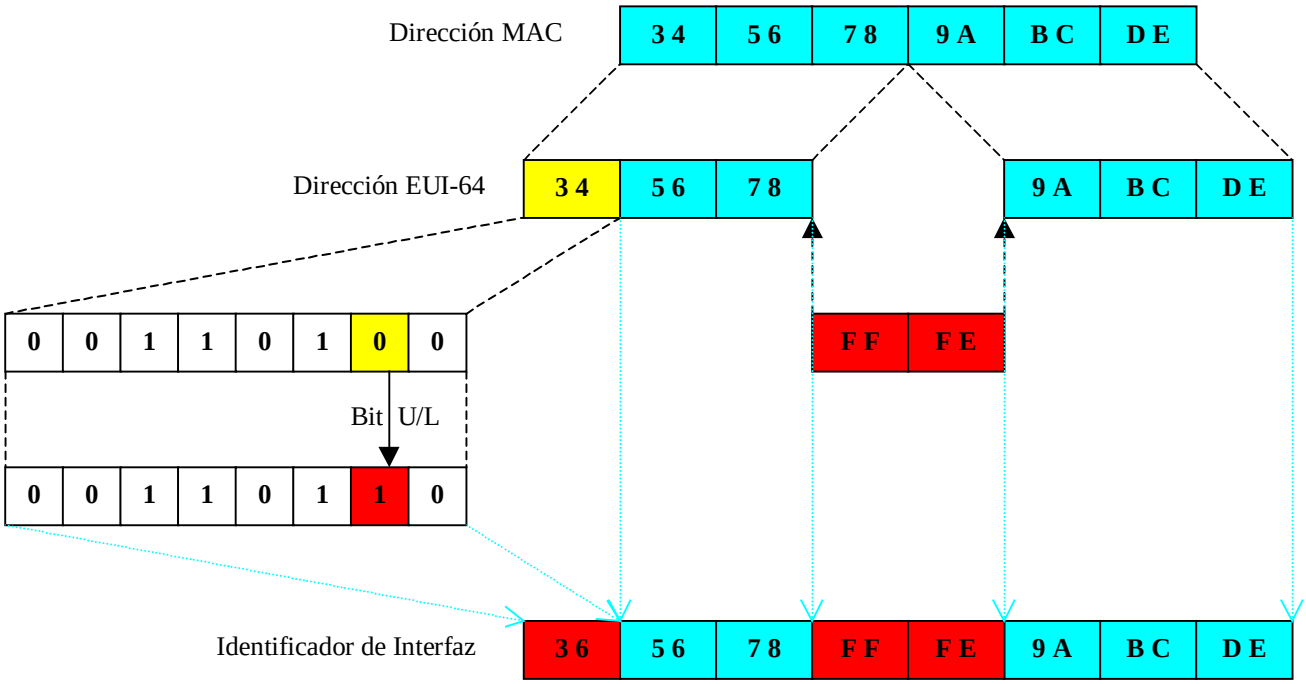
El tamaño máximo de la unidad de transmisión (MTU), para IPv6 sobre Ethernet, es de 1.500 bytes. Evidentemente, este puede ser reducido, manual o automáticamente (por los mensajes de anunciación de routers).

Para obtener el identificador de interfaz, de una interfaz Ethernet, para la autoconfiguración stateless, nos basamos en la dirección MAC de 48 bits (IEEE802). Tomamos los 3 primeros bytes (los de mayor orden), y les agregamos “FFFE” (hexadecimal), y a continuación, el resto de los bytes de la dirección MAC (3 bytes). El identificador así formado se denomina identificador EUI-64 (Identificador Global de 64 bits), según lo define IEEE.

El identificador de interfaz se obtiene, a continuación, partiendo del EUI-64, complementando el bit U/L (Universal/Local). El bit U/L es el siguiente al de menor valor del primer byte del EUI-64 (el 2º bit por la derecha, el 2º bit de menor peso). Al complementar este bit, por lo general cambiará su valor de 0 a 1; dado que se espera que la dirección MAC sea universalmente única, U/L tendrá un valor 0, y por tanto se convertirá en 1 en el identificador de interfaz IPv6.

Una dirección MAC configurada manualmente o por software, no debería ser usada para derivar de ella el identificador de interfaz, pero si no hubiera otra fórmula, su propiedad debe reflejarse en el valor del bit U/L.

Véase el esquema siguiente:



Para mapear direcciones unicast IPv6 sobre Ethernet, se utilizan los mecanismos ND para solicitud de vecinos.

Para mapear direcciones multicast IPv6 sobre Ethernet, se emplean los 4 últimos bytes de la dirección IPv6, a los que se antepone “3333”.

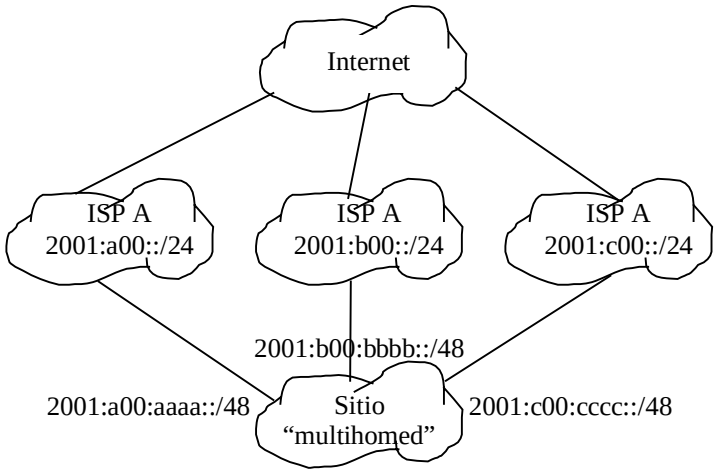
14. Multi-homing

Como venimos viendo, el mecanismo de asignación de direcciones IPv6 es totalmente jerárquico.

El multi-homing (“múltiples hogares”) es el mecanismo por el cual un determinado sitio o red puede estar conectado a otros por múltiples caminos, por razones de seguridad, redundancia, ancho de banda, balanceo de carga, etc.

Dado que un determinado sitio utiliza el prefijo de su ISP, o proveedor de nivel superior, un sitio puede ser “multi-homed” simplemente teniendo varios prefijos. Frecuentemente, cada prefijo estará asociado a diferentes conexiones físicas, aunque no necesariamente, dado que se puede tratar de una sola conexión física y diversos túneles o conexiones virtuales.

La problemática se plantea por la dificultad de que un host decida, en una red “multi-homed”, que dirección fuente utilizar.



Algunos de los documentos sobre los que se está trabajando en este campo son:

- Default Address Selections for IPv6 (draft-ietf-ipngwg-default-addr-select-00.txt).
- IPv6 Multi-homing with Route Aggregation (draft-ietf-ipngwg-ipv6multihome-with-aggr-00.txt).
- Multi-homed Routing Domain Issues for IPv6 (draft-ietf-ipngwg-multi-isp-00.txt).

15. IPsec

Una de las grandes ventajas de IPv6 es, sin duda, la total integración de los mecanismos de seguridad, autenticación y confidencialidad (encriptación), dentro del núcleo del protocolo.

Se trata por tanto de algo obligatorio, y no adicional ni “añadido” como en IPv4. Para ello, la siguiente cabecera puede tener valores AH (autenticación – “Authentication Header”) y ESP (encriptación – “Encapsulation Security Payload”), que permiten, básicamente, emplear las mismas extensiones de protocolo empleadas en IPv4, y que de hecho, al haber sido desarrolladas con posterioridad al inicio de los trabajos de IPv6, ya lo contemplan.

Dado que los mecanismos asociados ya han sido descritos, simplemente citamos las normas básicas que son aplicables: RFC2401 al RFC2412 y RFC2451.

16. Movilidad

La posibilidad de que un nodo mantenga la misma dirección IP, a pesar de su movilidad, es otra de las motivaciones básicas de IPv6. Como no, ya se han iniciado trabajos al respecto en IPv4, pero las complicaciones para usar la movilidad en este caso son enormes.

El documento base de estos trabajos es draft-ietf-mobileip-ipv6-12.txt. La idea básica permite identificar a un nodo móvil por su dirección de partida ("home address"), independientemente de su punto de conexión a Internet en cada momento dado. Por supuesto, cuando no esta en su punto de origen o de partida, también esta asociado con la información que permite identificar su posición o dirección actual ("care-of-address"). Los paquetes enviados a un nodo móvil (a su dirección de origen), son transparentemente encaminados a su "dirección actual".

El protocolo también permite que los nodos IPv6 almacenen la información de vinculación entre la dirección de partida y la posición actual, a modo de caché, y por tanto sean capaces de enviar los paquetes destinados al nodo móvil, directamente a su "dirección actual".

Para ello, el protocolo define nuevas opciones de destino, una de las cuales ha de ser soportada incluso en paquetes recibidos por todos los nodos (aunque no sean móviles).

Además, hay que prever, dada la estructura habitual de las redes inalámbricas (ejemplo muy habitual, la telefonía celular), que un nodo móvil puede estar conectado simultáneamente a varias redes (varías células que se solapan), y debe de ser alcanzable por cualquiera de ellas.

Los trabajos iniciales están documentados en el RFC2002 (soporte de movilidad en IP) y sucesivos. Además, se han publicado ya las especificaciones para túneles inversos en redes IP móviles (RFC2344), en cuya actualización se esta trabajando (draft-ietf-mobileip-rfc2344-bis-01.txt).

Se trabaja también en apartados como los requisitos de autenticación, autorización y facturación (draft-ietf-mobileip-aaa-reqs-03.txt), comúnmente denominadas AAA (Authentication, Authorization and Accounting), las extensiones de autenticación (draft-ietf-mobileip-challenge-09.txt), las claves de registro AAA (draft-ietf-mobileip-aaa-key-01.txt), la optimización de rutas (draft-ietf-mobileip-optim-09.txt), claves de registro para la optimización de rutas (draft-ietf-mobileip-regkey-01.txt), registros regionales (draft-ietf-mobileip-reg-tunnel-02.txt), entre otros.

17. DNS (RFC1886)

El mecanismo fundamental por el cual nos referimos a direcciones IP para la localización de un host, es el uso de literales (URL), como ya hemos anticipado en apartados anteriores.

Sin embargo, para que este mecanismo funcione, a más bajo nivel existe un protocolo denominado "Sistema de Nombres de Dominio" (Domain Name System o DNS).

Este mecanismo, definido para IPv4 (RFC1034 y RFC1035), fue actualizado por el RFC1886, básicamente incluyendo un nuevo tipo de registro para almacenar las direcciones IPv6, un nuevo dominio para soportar las "localizaciones" (lookups) basadas en IPv6, y definiciones actualizadas de tipos de consultas existentes que devuelven direcciones Internet como parte de procesos de secciones adicionales.

Las extensiones han sido diseñadas para ser compatibles con las aplicaciones existentes y, en particular, con las implementaciones del propio DNS.

El problema del sistema de DNS existente es fácilmente comprensible: Al hacer una consulta, las aplicaciones asumen que se les devolverá una dirección de 32 bits (IPv4). Para resolverlo, hay que definir las siguientes extensiones, antes indicadas:

- Un nuevo tipo de registro de recurso para mapear un nombre de dominio con una dirección IPv6: Es el registro AAAA (con un valor de tipo 28, decimal).
- Un nuevo dominio para soportar búsquedas basadas en direcciones. Este dominio es IP6.INT. Su representación se realiza en orden inverso de la dirección, separando los nibbles (hexadecimal) por puntos (“.”), seguidos de “.IP6.INT”. Así, la búsqueda inversa de la dirección 4321:0:1:2:3:4:567:89ab, seria “b.a.9.8.7.6.5.0.4.0.0.0.3.0.0.0.2.0.0.0.1.0.0.0.0.0.0.0.1.2.3.4.IP6.INT”
- Redefinición de las consultas existentes, que localizan direcciones IPv4, para que puedan también procesar direcciones IPv6. Ello incluye TODAS las consultas, lógicamente (NS, MX, MB, ...).

Además, para soportar la agregación de direcciones IPv6, la renumeración y el multi-homing, se trabaja en un nuevo documento (draft-ietf-ipngwg-dns-lookups-07.txt), que incluye un nuevo tipo de registro de recurso (A6) para almacenar las direcciones IPv6 de forma que se agilice la renumeración de la red. Se prevé que este documento sustituya al RFC1886.

Otros documentos relevantes son: RFC2181 (clarificaciones a las especificaciones DNS), RFC2535 (extensiones de seguridad para DNS), RFC2672 (redirección de árboles DNS), RFC2673 (etiqueta binarias en DNS).

18. Protocolos de Routing

Básicamente se adoptan los mismo protocolos de encaminado que los existentes en las redes IPv4: RIP, OSPF y BGP. Pero además se está trabajando en IDRP (ISO Inter-Domain Routing Protocol) e IS-IS (Intermediate System to Intermediate System).

18.1. RIPng (RFC2080 y RFC2081)

La especificación del Protocolo de Información de Rutas (RIP – “Routing Information Protocol”) para IPv6, recoge los cambios mínimos e indispensables al RFC1058 y RFC1723 para su adecuado funcionamiento.

RIPng es un protocolo pensado para pequeñas redes, y por tanto se incluye en el grupo de protocolos de pasarela interior (IGP – “Interior Gateway Protocol”), y emplea un algoritmo denominado “Vector-Distancia”. Se basa en el intercambio de información entre routers, de forma que puedan calcular las rutas más adecuadas, de forma automática.

RIPng sólo puede ser implementado en routers, donde requerirá como información fundamental, la métrica o número de saltos (entre 1 y 15), que un pa-

quete ha de emplear, para llegar a determinado destino. Cada salto supone un cambio de red, por lo general atravesando un nuevo router.

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

Estos parámetros han de ser configurados por el administrador de la red.

El router incorporará, en la tabla de encaminado, una entrada para cada destino accesible (alcanzable) por el sistema. Cada entrada tendrá como mínimo, los siguiente parámetros:

- El prefijo IPv6 del destino.
- La métrica (número de saltos entre este router y el destino).
- La dirección IPv6 del siguiente router, así como la ruta para llegar a él.
- Un indicador relativo al cambio de ruta.
- Varios contadores asociados con la ruta.

Además se podrán crear rutas internas (saltos entre interfaces del propio router), o rutas estáticas (definidas manualmente).

RIPng es un protocolo basado en UDP. Cada router tiene un proceso que envía y recibe datagramas en el puerto 521 (puerto RIPng).

El inconveniente de RIPng, al igual que en IPv4, siguen siendo, además de su orientación a pequeñas redes (diámetro de 15 saltos como máximo), en que su métrica es fija, es decir, no puede variar en función de circunstancias de tiempo real (retardos, fiabilidad, carga, etc.).

18.2. OSPFv6 (RFC2740)

El protocolo de encaminado “Abrir Primero el Camino más Corto” (OSPF – “Open Shortest Path First”), es también un protocolo IGP (para redes autónomas), basado en una tecnología de “estado de enlaces” (“link-state”).

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

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

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

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

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

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

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

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

OSPFv6 mantiene los mecanismos fundamentales de la versión para IPv4, pero se han tenido que modificar ciertos parámetros de la semántica del protocolo, así como el incremento del tamaño de la dirección. OSPFv6 se ejecuta basado en cada enlace, en lugar de en cada subred.

Además, ha sido necesario eliminar la autenticación del protocolo OSPFv6, dado que IPv6 incorpora estas características (AH y ESP).

A pesar de la mayor longitud de las direcciones, se ha logrado que los paquetes OSPFv6 sean tan compactos como los correspondientes para IPv4, eliminando incluso algunas limitaciones y flexibilizando la manipulación de opciones.

18.3. BGP4+ (RFC2283, RFC2545)

El Protocolo de Pasarelas de Frontera (BGP – "Border Gateway Protocol") es un protocolo de encaminado para la interconexión de sistemas autónomos, es decir, para el enrutado entre diferentes dominios.

Frecuentemente se emplea para grandes corporaciones y para la conexión entres proveedores de servicios (como ISP's).

Su principal función es, por tanto, el intercambio de información de disponibilidad o alcance entre varios sistemas BGP, incluyendo información de los sistemas autónomos que contienen, permitiendo así construir las rutas más adecuadas y evitar bucles de tráfico.

BGP4 incorpora mecanismos para soportar enrutado entre dominios sin clases ("classless interdomain routing"), es decir, el uso de prefijos, agregación de rutas, y todos los mecanismos en los que se basa IPv6.

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

BGP usa TCP como protocolo de transporte, a través del puerto 179.

BGP4+ añade a BGP (RFC1771), extensiones multiprotocolo, tanto para IPv6 como para otros protocolos, como por ejemplo IPX.

19. Estrategias de Transición (RFC1933)

La clave para la transición es la compatibilidad con la base instalada de dispositivos IPv4. Esta afirmación define un conjunto de mecanismos que los hosts y routers IPv6 pueden implementar para ser compatibles con host y routers IPv4.

Estos mecanismos permitirán usar infraestructuras IPv4 para IPv6 y viceversa, dado que se prevé que su uso será prolongado, e incluso indefinido en muchas ocasiones.

19.1. Doble pila (IPv4 e IPv6)

El camino más lógico y evidente de transición es el uso simultáneo de ambos protocolos, en pilas separadas. Los dispositivos con ambos protocolos también se denominan “nodos IPv6/IPv4”.

De esta forma, un dispositivo con ambas pilas pueden recibir y enviar tráfico a nodos que sólo soportan uno de los dos protocolos (nodos sólo IPv4 o sólo IPv6).

El dispositivo tendrá una dirección en cada pila. Se pueden utilizar direcciones IPv4 e IPv6 relacionadas o no, y se pueden utilizar mecanismos manuales o automáticos para la asignación de las direcciones (cada una correspondiente al protocolo en cuestión).

El DNS podrá devolver la dirección IPv4, la dirección IPv6, o ambas.

Como ya hemos explicado en el apartado de direcciones especiales IPv6, se pueden emplear la dirección IPv4 (32 bits), anteponiéndole 80 bits con valor cero y 16 bits con valor 1, para crear una dirección IPv6 “mapeada desde IPv4”.

19.2. Túneles IPv6 sobre IPv4

Los túneles proporcionan un mecanismo para utilizar las infraestructuras IPv4 mientras la red IPv6 esta siendo implantada. Este mecanismo consiste en enviar datagramas IPv6 encapsulados en paquetes IPv4.

Los extremos finales del túnel siempre son los responsables de realizar la operación de encapsulado del paquete/es IPv6 en IPv4.

Estos túneles pueden ser utilizados de formas diferentes:

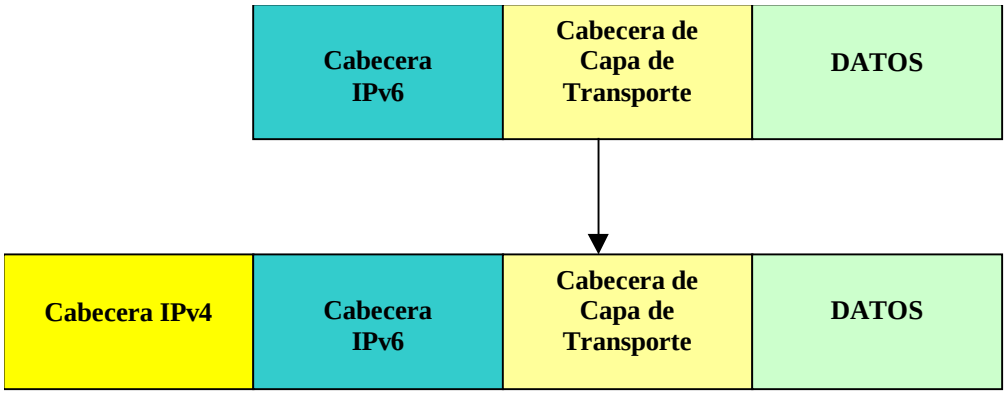
- Router a router. Routers con doble pila (IPv6/IPv4) se conectan mediante una infraestructura IPv4 y transmiten tráfico IPv6. El túnel comprende un segmento que incluye la ruta completa, extremo a extremo, que siguen los paquetes IPv6.
- Host a router. Hosts con doble pila se conectan a un router intermedio (también con doble pila), alcanzable mediante una infraestructura IPv4.

El túnel comprende el primer segmento de la ruta seguida por los paquetes.

- Host a host. Hosts con doble pila interconectados por una infraestructura IPv4. El túnel comprende la ruta completa que siguen los paquetes.
- Router a host. Routers con doble pila que se conectan a hosts también con doble pila. El túnel comprende el último segmento de la ruta.

Los túneles se clasifican según el mecanismo por el que el nodo que realiza el encapsulado determina la dirección del nodo extremo del túnel. En los dos primeros casos (router a router y host a router), el paquete IPv6 es tunelizado a un router. El extremo final de este tipo de túnel, es un router intermedio que debe desencapsular el paquete IPv6 y reenviarlo a su destino final. En este caso, el extremo final del túnel es distinto del destino del destino final del paquete, por lo que la dirección en el paquete IPv6 no proporciona la dirección IPv4 del extremo final del túnel. La dirección del extremo final del túnel ha de ser determinada a través de información de configuración en el nodo que realiza el túnel. Es lo que se denomina “túnel configurado”, describiendo aquel tipo de túnel donde el extremo final del túnel es explícitamente configurado.

En los otros dos casos (host a host y router a host), el paquete IPv6 es tunelizado, durante todo el recorrido, a su nodo destino. El extremo final del túnel es el nodo destino del paquete, y por tanto, la dirección IPv4 está contenida en la dirección IPv6. Este caso se denomina “túnel automático”.



El “desencapsulado”, en el extremo final del túnel, realiza la función opuesta, lógicamente.

19.3. Transmisión de IPv6 sobre dominios IPv4 (RFC2529)

Este mecanismo permite a hosts IPv6 aislados, sin conexión directa a routers IPv6, ser totalmente funcionales como dispositivos IPv6.

Para ello se emplean dominios IPv4 que soportan multicast como su enlace local virtual. Es decir, usamos multicast IPv4 como su “ethernet virtual”.

De esta forma, estos hosts IPv6 no requieren direcciones IPv4 compatibles, ni túneles configurados.

Los extremos finales del túnel se determinan mediante ND. Es imprescindible que la subred IPv4 soporte multicast.

Este mecanismo se denomina comúnmente “6 over 4”.

19.4. Conexión de dominios IPv6 sobre redes IPv4

El documento draft-ietf-ngtrans-6to4-04.txt nos indica un mecanismo comúnmente denominado “6 to 4”, para asignar un prefijo de dirección IPv6 a cualquier sitio que tenga al menos una dirección IPv4 pública.

De esta forma, dominios o hosts IPv6 aislados, conectados a infraestructuras IPv4 (sin soporte de IPv6), pueden comunicar con otros dominios o hosts IPv6 con una configuración manual mínima.

Este mecanismo funciona aún cuando la dirección IPv4 global (pública) es única y se accede a la red mediante mecanismos NAT (Network Address Translation), que es el caso más común en las redes actuales para el acceso a Internet a través de ISP’s.

19.5. “Tunnel Server” y “Tunnel Broker”

El documento draft-ietf-ngtrans-broker-02.txt sienta las bases para aplicaciones que permiten utilizar, de forma libre y gratuita, nuestras direcciones IPv4 actuales, sobre las infraestructuras IPv4, para acceder a redes y sitios IPv6.

Estos mecanismos se hacen indispensables para labores de investigación, dado que se requieren direcciones IPv6 y nombres DNS permanentes.

La diferencia con el mecanismo “6to4” es que el “Tunnel Broker” no requiere la configuración de un router.

Se trata de ISP’s IPv6 “virtuales”, proporcionando conectividad IPv6 a usuarios que ya tienen conectividad IPv4.

El “tunnel broker” es el lugar donde el usuario se conecta para registrar y activar “su túnel”. El “broker” gestiona (crea, modifica, activa y desactiva) el túnel en nombre del usuario.

El “tunnel server” es un router con pila doble (IPv4 e IPv6), conectado a Internet, que siguiendo órdenes del “broker” crea, modifica o borra los servicios asociados a un determinado túnel/usuario.

El mecanismo para su configuración es tan sencillo como indicar, en un formulario Web, datos relativos al S.O., la dirección IPv4, un “apodo” para la máquina, y el país donde esta conectada. El servidor de túneles crea los registros DNS, el extremo final del túnel, y genera un script para la configuración del cliente.

Se pueden hallar ejemplos de estos sistemas en http://www.freenet6.net y http://carmen.cselt.it/ipv6/download.html.

19.6. Otros mecanismos de transición

Estas técnicas pueden ser utilizadas incluso de forma combinada.

Se esta trabajando en varios mecanismos alternativos y modificaciones a los aquí expuestos, a través de los borradores draft-ietf-ngtrans-mech-06.txt, draft-ietf-ngtrans-translator-03.txt, draft-ietf-ngtrans-socks-gateway-04.txt, draft-ietf-ngtrans-dstm-01.txt, draft-ietf-ngtrans-tcpudp-relay-00.txt, draft-ietf-ngtrans-hometun-00.txt y draft-ietf-ngtrans-ipv4survey-00.txt.

Un documento introductorio completo a todos los mecanismos es draft-ietf-ngtrans-introduction-to-ipv6-transition-03.txt.

20. Situación del estándar: RFC's y borradores

Los RFC's existentes son los siguientes:

	Documento	Título
Especificaciones Básicas	RFC2460	Especificaciones del Protocolo Internet Versión 6 (IPv6)
	RFC2461	Descubrimiento del Vecindario para IPv6 (ND)
	RFC2462	Autoconfiguración de Direcciones “stateless” IPv6
	RFC2463	Protocolo de Mensajes de Control de Internet para IPv6 (ICMPv6)
	RFC1981	Descubrimiento del MTU de la ruta para IPv6
	RFC1809	Uso del campo “Etiqueta de Flujo” en IPv6
Direccionamiento	RFC2373	Arquitectura de Direccionamiento en IPv6
	RFC1887	Arquitectura para la Asignación de Direcciones Unicast IPv6
	RFC2374	Formato de Direcciones Unicast Agregables Globales
	RFC2450	Propuesta de normas de asignación de TLA y NLA
Routing	RFC2080	RIP para IPv6
	RFC2081	Aplicabilidad de RIPng para IPv6
	RFC2283	Extensiones Multiprotocolo para BGP-4
	RFC2545	Uso de las Extensiones Multiprotocolo de BGP-4 para Routing entre dominios para IPv6
	RFC2740	OSPF para IPv6
DNS	RFC1886	Extensiones DNS para soportar IPv6
IPv6 sobre ...	RFC2464	Transmisión de paquetes IPv6 sobre redes Ethernet
	RFC2467	Transmisión de paquetes IPv6 sobre redes FDDI
	RFC2470	Transmisión de paquetes IPv6 sobre redes Token Ring
	RFC2472	IPv6 sobre PPP
	RFC2491	IPv6 sobre redes de Acceso Múltiple Sin Broadcast
	RFC2492	IPv6 sobre redes ATM
Seguridad	RFC2401	Arquitectura de Seguridad para IP
	RFC2402	Cabecera de Autenticación IP
	RFC2406	Encriptación de datos en IP (ESP)
	RFC2408	Asociaciones de Seguridad y Protocolo de Gestión de Claves en Internet (ISAKMP)
Multicast	RFC2375	Asignación de Direcciones Multicast
	RFC2710	Descubrimiento de nodos que desean recibir Multicast para IPv6
	RFC2776	Protocolo de Anunciación de Zonas de Ambito Multicast (MZAP)
Anycast	RFC2526	Direcciones de Subredes para Anycast en IPv6
Multi-Homing	RFC2260	Soporte Escalable de Multi-homing para Conectividad Multi-Proveedor
	RFC2497	Transmisión de paquetes IPv6 sobre redes ARCnet
Transición	RFC1933	Mecanismos de Transición para Routers y Hosts IPv6
	RFC2185	Aspectos de Routing de la Transición IPv6
	RFC2473	Especificaciones Genéricas de Tunelización de Paquetes en IPv6
	RFC2529	Transmisión de IPv6 sobre Dominios IPv4 sin Túneles Explícitos
	RFC2765	Algoritmo de Traslación Stateless IP/ICMP (SIIT)
	RFC2766	Protocolo de Traslación – Traslación de Dirección de Red
	RFC2767	Doble Pila en Hosts usando la Técnica “Bump-In-the-Stack” (BIS)
API	RFC2292/bis	Advanced Sockets API para IPv6
	RFC2553/bis	Basic Socket API para IPv6
MIB	RFC2452	Base de Información de Gestión para IPv6: TCP
	RFC2454	Base de Información de Gestión para IPv6: UDP
	RFC2465	Base de Información de Gestión para IPv6: Convenciones Textuales y Grupo General
	RFC2466	Base de Información de Gestión para IPv6: ICMPv6
Otros	RFC1881	Gestión de la Asignación de Direcciones IPv6
	RFC1924	Representación Compacta de Direcciones IPv6
	RFC2147	TCP y UDP sobre Jumbogramas IPv6
	RFC2428	Extensiones FTP para IPv6 y NAT
	RFC2471	Plan de Asignación de direcciones IPv6 para Pruebas
	RFC2474	Definición del Campo de Servicios Diferenciados (DS) en Cabeceras IPv4 e IPv6
	RFC2546	Prácticas de Routing en 6Bone
	RFC2663	Consideraciones y Terminología de IP NAT
	RFC2732	Formato para la representación literal de direcciones IPv6 en URL’s
	RFC2772	Guías de Routing en el troncal 6Bone
	RFC2775	Transparencia de Internet

Pero además, se esta trabajando en los siguientes documentos (drafts):

	Borrador IETF	Título
Direccionamiento	ipngwg-iana-tla-03.txt	Asignaciones Iniciales de Identificadores sub-TLA IPv6
	ipngwg-site-prefixes-04.txt	Prefijos de Sitios en ND
	ipngwg-esd-analysis-05.txt	Análisis de propuesta de direccionamiento GSE para IPv6
	ipngwg-scopedaddr-format-02.txt	Extensión de formato para Ambitos de Direcciones en IPv6
	ipngwg-scoping-arch-01.txt	Arquitectura de Ambitos de Direcciones en IPv6
	ipngwg-addr-arch-v3-00.txt	Arquitectura de Direccionamiento en IPv6
Routing	ipngwg-router-renum-10.txt	Renumeración de Routers para IPv6
	ipngwg-scoped-routing-04.txt	Routing de Ambitos de Direcciones en IPv6
DNS	ipngwg-dns-lookups-08.txt	Extensiones DNS para soportar Agregación y Renumeración en IPv6
ICMP	ipngwg-icmp-name-lookups-05.txt	Peticiones de información a nodos en IPv6
ND	ion-ipv6-ind-03.txt	Extensiones a ND en IPv6 para descubrimiento inverso
Movilidad	mobileip-ipv6-12.txt	Soporte de Movilidad en IPv6
	mobileip-challenge-12.txt	Extensiones de Desafío/Respuesta en movilidad IP
	mobileip-aaa-reqs-03.txt	Requisitos de Autenticación, Autorización y Contabilidad (AAA) en movilidad IP
	mobileip-rfc2344-bis-01.txt	Revisión de Túneles Inversos para movilidad IP
DHCP	dhc-dhcp-dns-12.txt	Interacción entre DHCP y DNS
	dhc-autoconfig-04.txt	Opción DHCP para desactivar la autoconfiguración stateless en clientes IPv4
	dhc-dhcpv6-15.txt	Protocolo de Configuración Dinámica de Host para IPv6 (DHCPv6)
	dhc-v6exts-12.txt	Extensiones para DHCPv6
Seguridad	ipngwg-addrconf-privacy-01.txt	Extensiones de Privacidad para Autoconfiguración de Direcciones Stateless en IPv6
Multi-Homing	ipngwg-default-addr-select-00.txt	Selección de Direcciones por Defecto para IPv6
	ipngwg-ipv6multihome-with-aggr-00.txt	Multi-Homing en IPv6 con Agregación de Rutas
	ipngwg-multi-isp-00.txt	Problemática de dominios con Routing Multi-Homing en IPv6
Transición	ngtrans-translator-03.txt	Técnicas de Transición para comunicación entre IPv6 e IPv4
	ngtrans-mech-06.txt	Mecanismos de Transición para Host y Routers IPv6
	ngtrans-6to4-06.txt	Conexión de dominios IPv6 a través de redes IPv4 sin túneles explícitos
	ngtrans-broker-02.txt	Tunnel Broker para IPv6
	ngtrans-introduction-to-ipv6-transition-03.txt	Guía para la introducción de IPv6 en el mundo IPv4
	ngtrans-socks-gateway-04.txt	Mecanismos de Pasarela IPv6/IPv4 basados en SOCKS
	ngtrans-6bone-6papa-01.txt	Pre-cualificación para asignación de prefijos de direcciones en 6Bone (6PAPA)
	ngtrans-dstm-01.txt	Mecanismo de Transición de doble pila (DSTM)
	ngtrans-tcpudp-relay-01.txt	Traductor de relé de transporte IPv6-IPv4
	ngtrans-hometun-00.txt	Túneles IPv6 sobre IPv4 para acceso doméstico a Internet
	ngtrans-ipv4survey-00.txt	Inspección de direcciones IPv4 en normas actuales IETF
MIB	ipngwg-mld-mib-03.txt	Base de Información de Gestión para Multicast Listener Discovery Protocol en IPv6
Otros	pim-ipv6-03.txt	Protocolo de Routing Multicast Independiente en IPv6
	pim-v2-sm-01.txt	Protocolo de Routing Multicast Independiente en Modo Esparcido (PIM-SM)

Autor: Jordi Palet Martínez (jordi@consulintel.es)

- Director de Producto de Consulintel
- Presidente del Grupo de Trabajo de Educación, Promoción y Relaciones Públicas del Foro IPv6
- Ex-Presidente y Ex-Vicepresidente de @asLAN