Tutorial de IPv6: INTRODUCCION

Jordi Palet
Presidente del Grupo de Trabajo
de Educación, Promoción
y Relaciones Públicas
del *IPv6 Forum*

La Internet Actual

- Falta de Direcciones IPv4 Clase B
- Demasiados Sistemas Conectados
- Demasiadas entradas en las tablas de routing
- Incremento progresivo del tiempo de búsqueda, DNS, etc.
- Situación salvada temporalmente con NAT

¿Porqué IPv6?

- Evitar los parches de IPv4
  - Solución al problema de direcciones: 128 bits
- Todos los dispositivos conectados
  - QoS, IPsec, Movilidad
- Desarrollo de Internet e Internet Móvil
  - UMTS, xDSL, Cable

Características de IPv6

- 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**.

Introducción a IPv6

- Expansión de las Capacidades de Routing y Direccionamiento
  - Solución al problema de direcciones: 128 bits

    (340.282.366.920.938.463.463.374.607.431.768.211.456 = 10^{38} = 2^{128})

    665.570.793.348.866.943.898.599 / m^2 en la tierra
  - Soporte de mejores estructuras jerárquicas
  - Direcciones Unicast, Anycast y Multicast
  - No hay BROADCAST
- Cabecera de 40 bytes
  - 64 bits+128 bits (origen y destino)
  - Proceso más eficiente

Historia de IPv6

- 1.992 - TUBA
  - Mecanismos para usar TCP y UDP sobre direcciones mayores
  - Se emplea ISO CLNP (Connection-Less Network Protocol)
  - Se descarta
- 1.993 - SIPP
  - Proyecto Simple IP Plus
  - Mezcla de SIP y PIP (dos tentativas anteriores para sustituir a IPv4)
- 1.994 – IPng
  - Se adopta SIPP
  - Se cambia el tamaño de direcciones a 128 bits
  - Se renombre como IPv6

Historia de IPv6 Forum

- Julio de 1.999
  - Constitución del IPv6 Forum
- Acuerdo de compra del 75% de Telebit por Ericsson
- Acuerdos y adopciones de IPv6 por:
  - OTAN, ETSI, UMTS Forum, 3GPP, UE, etc.
- Confirmación de otros fabricantes:
  - Sun, Nortel, 3Com, Microsoft, Cisco, ...

Tendencias Conductoras de la Necesidad de IPv6

- Creciente movilidad de los usuarios de Internet
- Necesidad de más de 1 IP por persona
- Redes domésticas, Domótica y otras redes similares
- Redes inalámbricas
- Servicios “siempre conectado”
- Convergencia de voz, vídeo, y datos en infraestructuras basadas en IP

El Desafío de IPv6

- No es técnico
- Es la educación de los usuarios finales
- Es el desarrollo de los casos de negocio
- No hay una única “aplicación definitiva”

RFC2460

Especificaciones

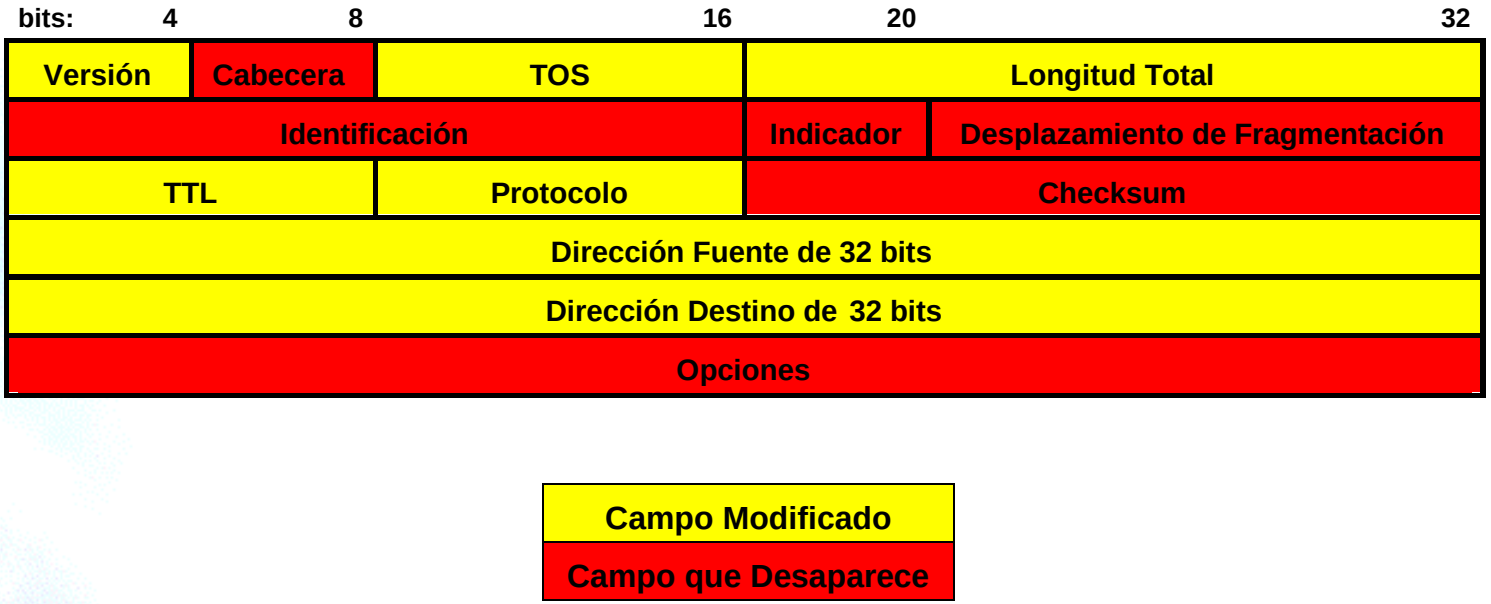
Básicas

de

IPv6

Cabecera IPv4 (I)

- 20 bytes + opciones



Cabecera IPv4 (II)

- 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)

Cabecera IPv6 (I)

- Pasamos de 12 a 8 campos

bits: 4	12	16	24	32
Versión	Clase de Tráfico	Etiqueta de Flujo		
Longitud de la Carga Útil			Siguiente Cabecera	Límite de Saltos
Dirección Fuente De 128 bits				
Dirección Destino De 128 bits				

  - Evitamos redundancia (checksum)
  - Fragmentación extremo a extremo

Cabecera IPv6 (II)

- 40 bytes

- Longitud Fija
- Campos alineados a 64 bits

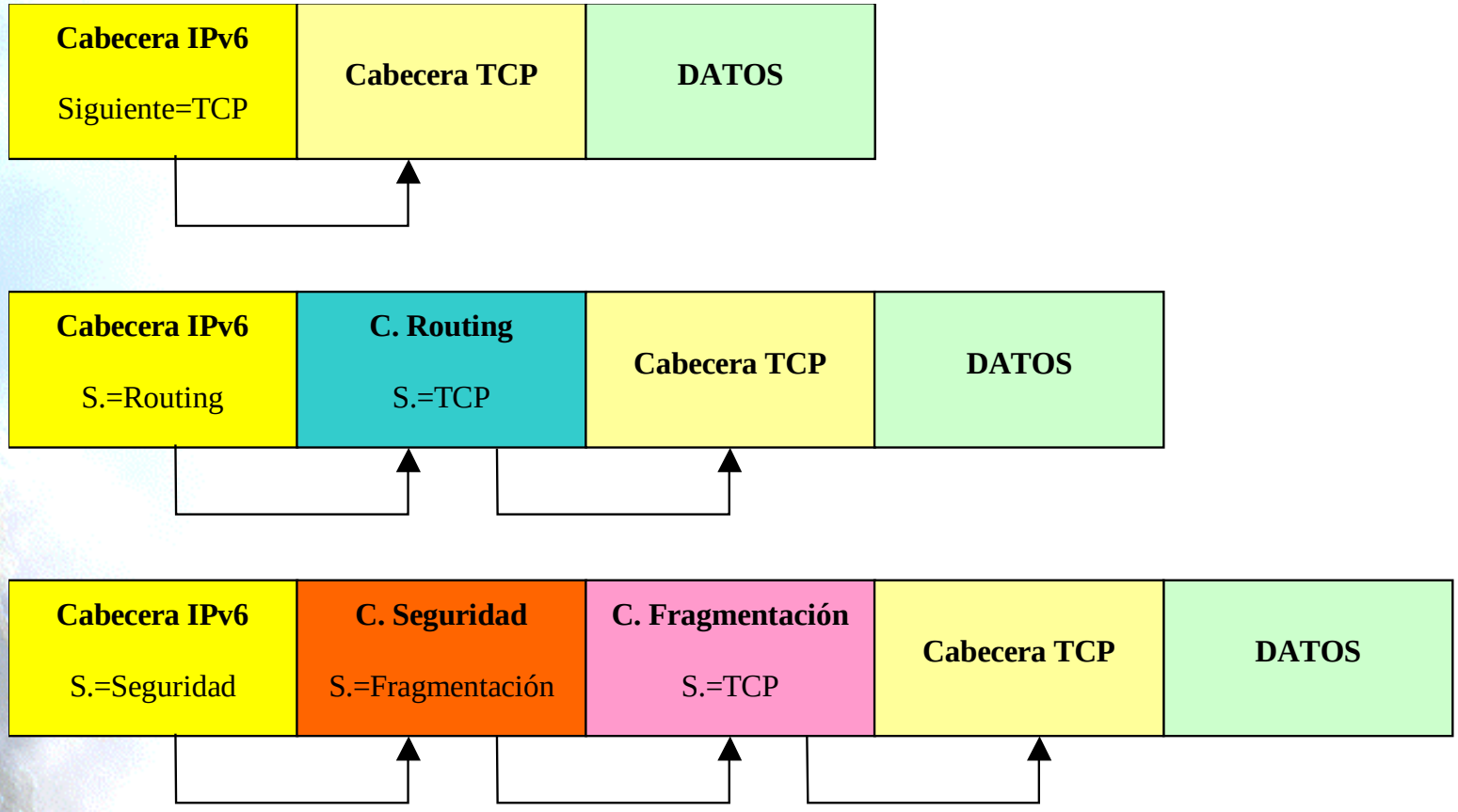
- MTU mínimo de 1.280 bytes, recomendado +1.500 bytes
- Cabeceras de Extensión

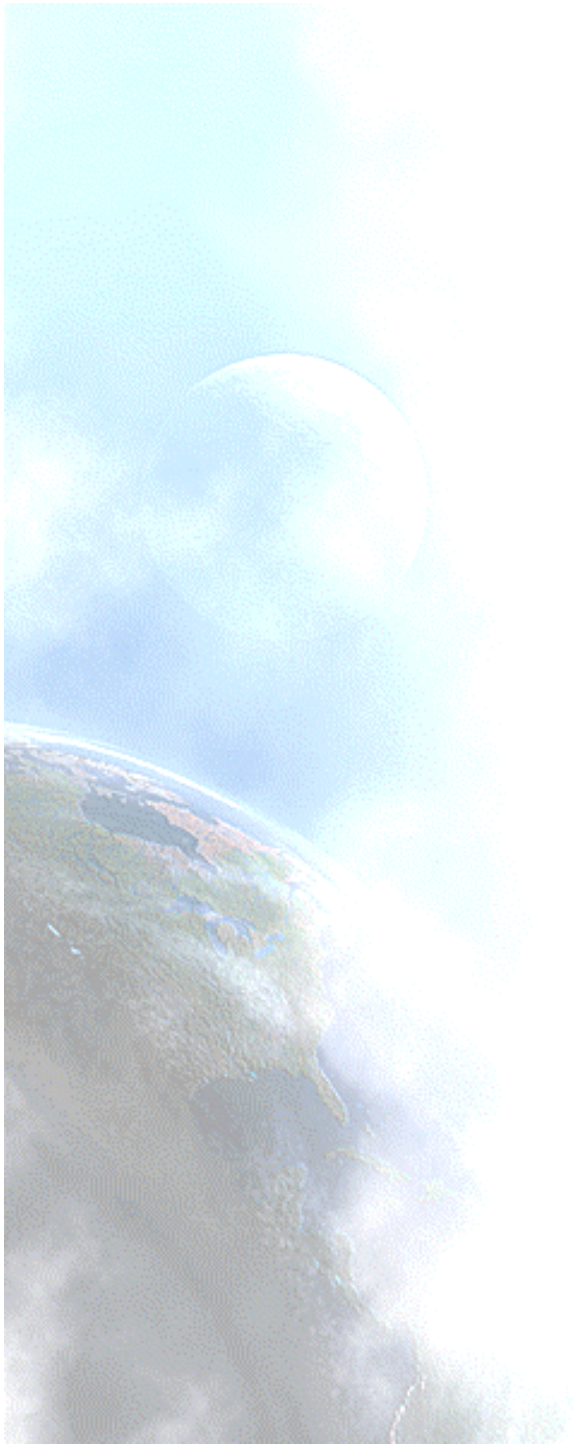
Cabecera IPv6 (III)

- Campos 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).
- Nuevos Campos
  - 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.

Cabeceras de Extensión

- Campo “Siguiente Cabecera”





RFC2373

Direcciones

y

Direccionamiento

en

IPv6

Espacio de Direcciones IPv6

- $2^{128} = 3{,}40E38$
  (340.282.366.920.938.463.463.374.607.431.768.211.456)
- 665.570.793.348.866.943.898.599 IP's por m^2 de la superficie terrestre
- Las direcciones IPv6 son identificadores de 128 bits para interfaces y conjuntos de interfaces

Tipos de Direcciones IPv6

- Unicast: Identificador para una única interfaz. Paquetes entregados únicamente a la interfaz identificada, como en IPv4
- Anycast: Identificador para un conjunto de interfaces. Paquetes entregados a cualquiera de las interfaces identificadas (ámbitos de redundancia)
- Multicast: Identificador para un conjunto de interfaces. Paquetes entregados a todas las interfaces identificadas (broadcast).

Direccionamiento IPv4 vs. IPv6

- No hay broadcast -> Multicast
- Organización en Campos -> Prefijos
- El prefijo indica donde esta conectada una dirección -> Su Ruta
- Los campos pueden ser todo 0’s o 1’s
- Direcciones asignadas a interfaces, no nodos
- Cada interfaz tiene al menos una dirección unicast de enlace local
- Una única interfaz puede tener varias direcciones
- Una misma dirección o direcciones unicast pueden ser asignadas a varias interfaces (balanceo de carga)

Reservas de Espacio IPv6

- Espacio Reservado vs. Espacio Asignado
- Aproximadamente el 15%
- Para facilitar la transición
- Mecanismos y desarrollo del propio protocolo
- Facilidad de distinción de direcciones multicast
  (valor del octeto superior = FF)
- No hay diferencia entre unicast y anycast
- ¡ 85% libre para uso futuro !

Tabla de Reservas de Direcciones

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

Direcciones Especiales IPv6

- Auto-retorno (loopback) -> ::1
  Interfaz “virtual”, paquetes que no salen del nodo que los envía, para verificación del protocolo
- No Especificada -> ::
  Ausencia de dirección, no ha de ser usada nunca. Puede indicar un host iniciándose
- Túneles Dinámicos/Automáticos de IPv6 sobre IPv4 -> ::<dirección IPv4>
  Direcciones IPv6 compatibles con IPv4

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

- Representación Automática de IPv4 sobre IPv6 -> ::FFFF:<dirección IPv4>
  Para que nodos “sólo IPv4” puedan trabajar en redes IPv6

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

Representación de Direcciones

- **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
- **Abreviación**: 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:
  - 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)

Direcciones IPv4

- 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

Prefijos

- dirección-IPv6/longitud-del-prefijo
  - 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

Identificador de Interfaz

- El “identificador de interfaz” se emplea, para identificar interfaces en un enlace
- Debe 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.

Direcciones Unicast Locales

- Son agregables, con máscaras de bits contiguos, al modo de CIDR (Classless Interdomain Routing) en IPv4.
- Los nodos verán las direcciones en función de su “inteligencia”.
  - Nodos IPv6 “poco inteligentes”:

128 bits
Dirección del nodo

  - Nodos IPv6 “más sofisticados”:

n bits	128-n bits
Prefijo de subred	identificador de interfaz

Tipos de Direcciones Unicast

- Local de Enlace (Link-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).

10 bits	54 bits	64 bits
1111111010	0	Identificador de interfaz

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

- Local de Sitio (Site-Local)
  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

Direcciones Requeridas

- 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/anycast
  - Las direcciones multicast de todos los grupos a los que dicho host pertenece
- 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

Prefijos requeridos para un Dispositivo IPv6

- 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).

RFC2732

Formato

para

la

Representación

en URL’s

Representación de URL's

- RFC2396: 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.
- De la misma forma que en ocasiones usamos direcciones en formato IPv4 para escribir un URL, se han descrito unas normas para realizar la representación literal de direcciones IPv6 cuando se usan herramientas de navegación WWW.
- 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: empleo de los corchetes ("[","]") para encerrar la dirección IPv6, dentro de la estructura habitual del URL.

URL's - Ejemplos:

- Las direcciones:
  - 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:
  - 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]

Direccionamiento IPv6: Resumiendo

RFC2450

y

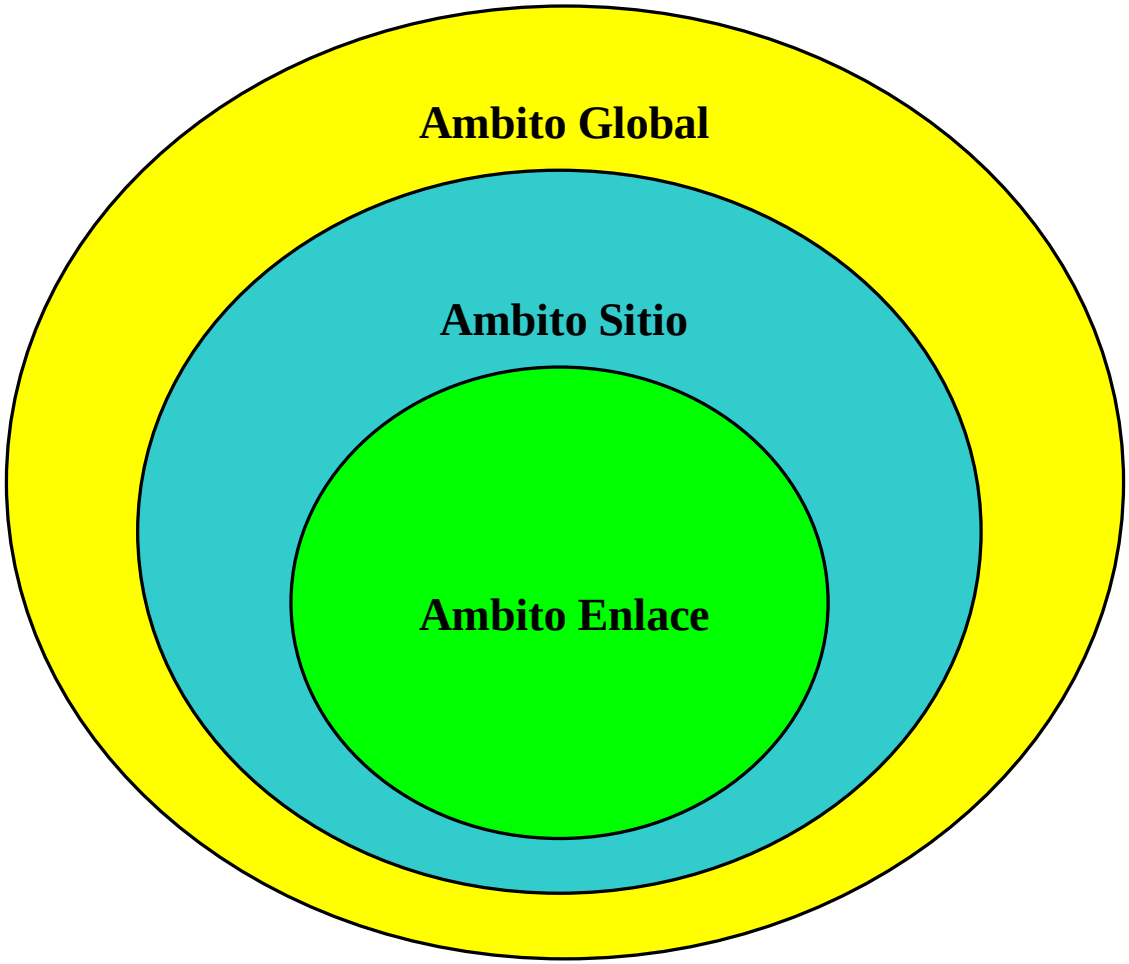
otras

Recomendaciones

Direccionamiento IPv6

- Esquema muy simple y sobre todo, muy eficiente.
- Resultados:
  - 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).
  - Las interfaces pueden tener múltiples direcciones.
  - Las direcciones tienen ámbito (Global, Sitio, Enlace).
  - Las direcciones, al estar compuestas por un prefijo y un identificador de interfaz, nos permiten separar “quién es” de “donde esta conectado”:
  - Además, las direcciones tienen un período de vida (de validez).

Ambitos



RFC2450

- Propone las reglas para la administración de los TLA's y NLA's.
- http://www.arin.net/regserv/ipv6/IPv6.txt -> más información al respecto de las normas para registros IPv6
- http://www.ripe.net/ripencc/about/regional/maps/ipv6policy-draft-090699.html
- http://www.apnic.net/drafts/ipv6/ipv6-policy-280599.html
- Máxima autoridad competente es IANA (Internet Assigned Numbers Authority).

RFC2463

ICMPv6

Internet Control Message Protocol

- Protocolo de Mensajes de Control de Internet: RFC792 para IPv4.
- Modificación para IPv6: ICMPv6
- Valor 58, para el campo de “siguiente cabecera”.
- 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”).

Formato de ICMPv6

bits 8	16	32
Tipo	Código	Checksum
Cuerpo del Mensaje		

- “tipo” -> tipo de mensaje; su valor determina el formato del resto de la cabecera.
- “código” -> depende del tipo de mensaje; se emplea para crear un nivel adicional de jerarquía para la clasificación del mensaje.
- “checksum” o código de redundancia -> permite detectar errores en el mensaje ICMPv6.
- Los mensajes ICMPv6 se agrupan en dos clases:
  - Mensajes de Error. Tienen cero en el bit de mayor peso del campo “tipo” (valores 0-127).
  - Mensajes Informativos. Entre 128 y 255.

Mensajes ICMPv6

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)	

Nuevos Mensajes ICMPv6

- 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).

RFC2461

Neighbor

Discovery

El “ARP” de IPv6

- El protocolo equivalente a ARP, es el “descubrimiento del vecindario”.
- Incorpora también la funcionalidad de otros protocolos IPv4, como “ICMP Router Discovery” e “ICMP Redirect”.
- Es 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.
- ND (“Neighbor Discovery”), 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, y detectar cualquier cambio.
- ND emplea los mensajes ICMPv6, incluso a través de mecanismos de multicast en la capa de enlace, para algunos de sus servicios.

Base de la Autoconfiguración

- ND es completo y sofisticado: 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.
- El RFC 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, de un documento clave para la correcta interpretación de IPv6, cuando se trata de aplicarlo a su uso por parte de desarrolladores.

Nuevos mensajes ICMPv6

- Solicitud de Router (Router Solicitation) – generado por interfaces cuando se activan, para pedir a los routers que se “anuncien” inmediatamente. Tipo ICMPv6 = 133.
- Anunciación de Router (Router Advertisement) – generado por 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 y otros parámetros de enlace e Internet (prefijos, tiempos de vida, configuración de direcciones, límite de salto sugerido, etc.). Fundamental para permitir la renumeración. Tipo ICMPv6 = 134.
- Solicitud de Vecino (Neighbor Solicitation) – generado por nodos para determinar la dirección en la capa de enlace de sus vecinos, o para verificar que el nodo vecino sigue activo (es alcanzable), y para detectar las direcciones duplicadas. Tipo ICMPv6 = 135.
- Anunciación de Vecino (Neighbor Advertisement) – generado por nodos como respuesta a la “solicitud de vecino”, o para indicar cambios de direcciones en la capa de enlace. Tipo ICMPv6 = 136.
- Redirección (Redirect) – generado por routers para informar a los host de un salto mejor para llegar a un determinado destino. Equivalente, a “ICMP redirect”. Tipo ICMPv6 = 137.

Ventajas de ND vs. IPv4 (I)

- 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 232 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.

Ventajas de ND vs. IPv4 (II)

- 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.

Ventajas de ND vs. IPv4 (III)

- 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.

RFC2462

Autoconfiguración

en

IPv6

¿Qué es la Autoconfiguración?

- Conjunto de pasos por los cuales un host decide como autoconfigurar sus interfaces en IPv6.
- Mecanismo 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) y el mecanismo para detectar direcciones duplicadas.

Tipos de Autoconfiguración

- 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.

Complementariedad

- 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.

Caducidad de las Direcciones

- Cada dirección es cedida a una interfaz durante un tiempo predefinido (posiblemente infinito).
- El tiempo de vida, indica durante cuanto tiempo esta vinculada dicha dirección a una determinada interfaz.
- Cuando expira, la vinculación se invalida y la dirección puede ser reasignada a otra interfaz en cualquier punto de Internet.
- Una dirección pasa a través de dos fases diferentes:
  - 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.
- En estado “desaprobado”, su uso es desaconsejado, no prohibido. Cualquier nueva comunicación (una nueva conexión TCP), debe usar una dirección “preferida”.
- 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.

Detección de Direcciones Duplicadas

- 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.

Autoconfiguración Stateless

Procedimiento

Las Premisas (I)

- 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.

Las Premisas (II)

- 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.

El Mecanismo

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

Autoconfiguración Stateful

DHCPv6

draft-ietf-dhc-dhcpv6-15.txt

DHCPv6

- 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.

Objetivos de DHCPv6

- DHCP es un mecanismo, no una política. La política es establecida por el administrador de la red y DHCP permite propagar los parámetros.
- DHCP es compatible, con el mecanismo de autoconfiguración “stateless”.
- DHCP no requiere configuración manual de parámetros de red.
- DHCP no requiere un servidor en cada enlace (relés DHCP).
- DHCP coexiste con nodos configurados estáticamente.
- 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.

DHCPv4 vs. DHCPv6

- 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).

Nuevas Funciones con DHCPv6

- 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.

RFC2464

IPv6

sobre

Ethernet

Ejemplo Clásico

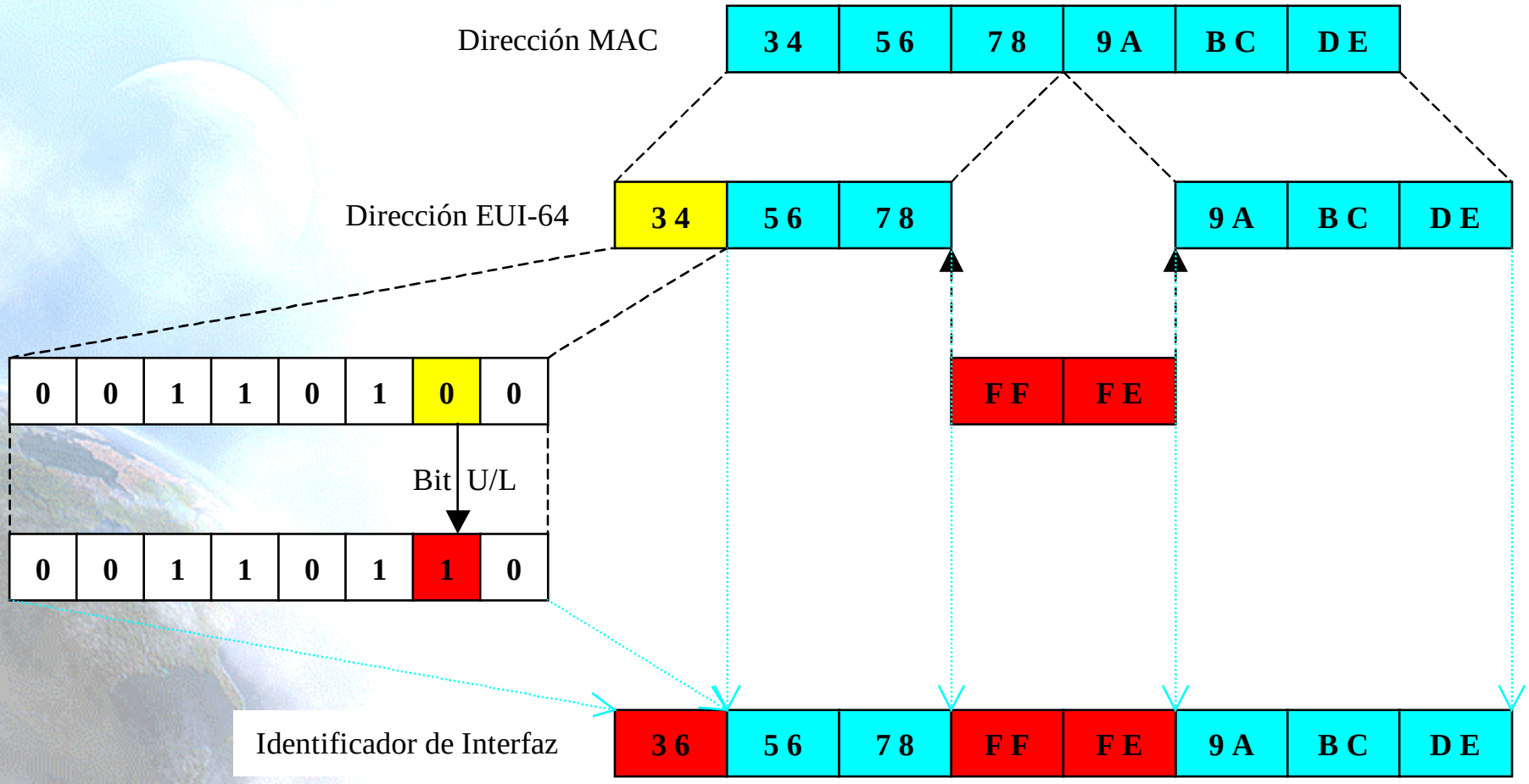
- Ya han sido definidos protocolos para permitir el uso de IPv6 sobre cualquier tipo de red o topología (Token Ring, FDDI, ATM, PPP, ...).
- IPv6 sobre Ethernet es un ejemplo habitual y básico.
- Los paquetes IPv6 se transmiten sobre tramas normalizadas Ethernet.
- La cabecera Ethernet contiene las direcciones 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.
- 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).

Formato de la trama

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

- Para obtener el identificador de interfaz, de una interfaz Ethernet, para la autoconfiguración stateless, nos basamos en la dirección MAC de 48 bits (IEEE802).
- A los 3 primeros bytes (los de mayor orden), se les agrega “FFFE” (hexadecimal)
- Se continúa con 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.

EUI-64


Dirección MAC
3 4
5 6
7 8
9 A
B C
D E
Dirección EUI-64
3 4
5 6
7 8
9 A
B C
D E
F F
F E
0 0 1 1 0 1 0 0
Bit U/L
0 0 1 1 0 1 1 0
Identificador de Interfaz
3 6
5 6
7 8
F F
F E
9 A
B C
D E

Identificador de Interfaz

- El identificador de interfaz se obtiene, 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.
- 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”.