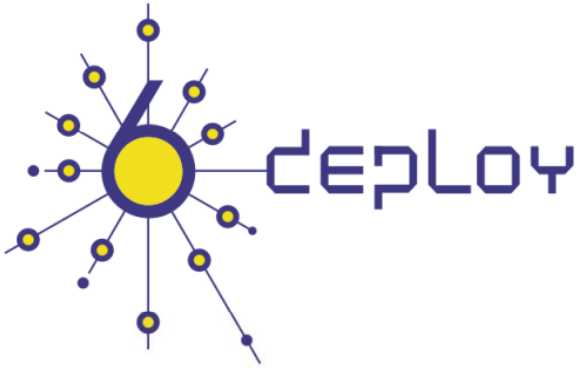
Curso IPv6

WALC 2009

Bogotá – Colombia

21 al 25 Septiembre 2009



César Olvera (cesar.olvera@consulintel.es)

Alvaro Vives (alvaro.vives@consulintel.es)

deploy

Consulintel

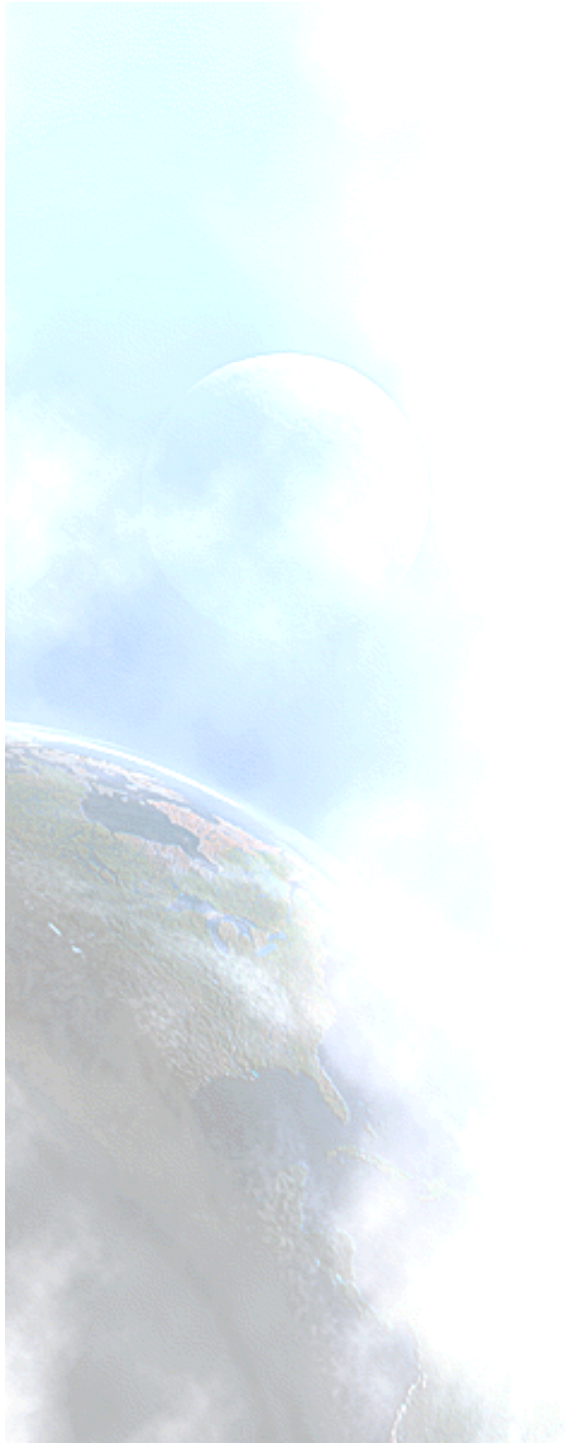
Consultores Integrales en Telecomunicaciones

Contenido del curso (1)

- **Bloque 1. Tutorial IPv6**
  1. Introducción a IPv6
  2. Formatos de cabeceras y tamaño de paquetes
  3. Direccionamiento IPv6
  4. ICMPv6, Neighbor Discovery y DHCPv6
  5. Seguridad IPv6
  6. Encaminamiento con IPv6
  7. Mecanismos de Transición
  8. Movilidad IPv6

Contenido del curso (2)

- **Bloque 2. Otros Aspectos Avanzados**
  9. Calidad de Servicio (QoS)
  10. Multicast
  11. Multi-homing
  12. Porting de aplicaciones
  13. Gestión SNMP sobre IPv6
  14. IPv6 sobre MPLS
  15. DNS IPv6

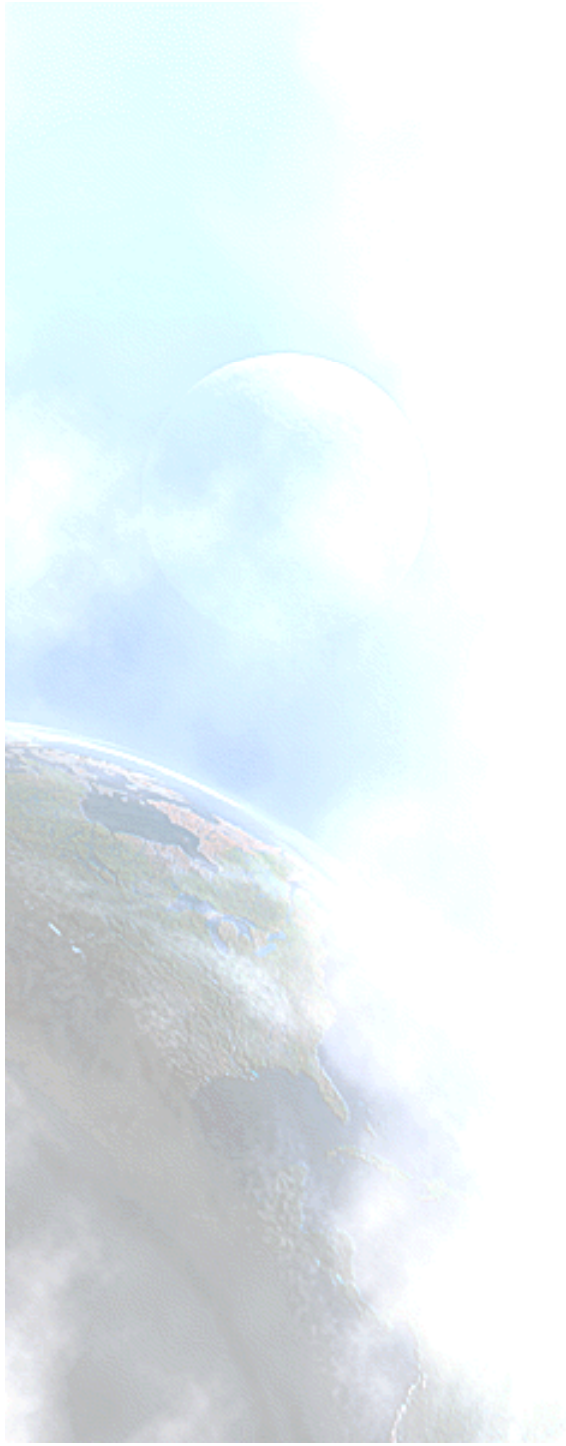


Bloque 1

Tutorial IPv6

4. ICMPv6, Neighbor Discovery y DHCPv6

4.1 ICMPv6
4.2 Neighbor Discovery
4.3 Autoconfiguración
4.4 DHCPv6
4.5 Secure Neighbor Discovery
4.6 Router Renumbering



4.1 ICMPv6

ICMPv6 (RFC4443)

- IPv6 emplea el Internet Control Message Protocol (ICMP) como se define en IPv4 (RFC792)
- Aunque se introducen algunos cambios para IPv6: ICMPv6.
- Valor Next Header = 58.
- Se emplea ICMPv6 en los nodos IPv6 para reportar errores encontrados durante el procesamiento de los paquetes y para realizar otras funciones de la capa de Red, tales como diagnósticos (ICMPv6 "ping").
- ICMPv6 es una parte integral de IPv6 y DEBE ser completamente implementado por cada nodo IPv6.

Mensajes ICMPv6

- Agrupados en dos clases:
  - Mensajes de error
  - Mensajes informativos

bits 8	16	32
Type	Code	Checksum
Message Body		

- Los mensajes de error tienen un cero en el bit de mayor orden del valor del campo Type. Por tanto el valor del campo Type es de 0 a 127.
- Los mensajes informativos tienen valores para el campo Type de 128 a 255.

Determinación de la Dirección Origen del Mensaje

- Un nodo que envía un mensaje ICMPv6 tiene que determinar las direcciones IPv6 origen y destino de la cabecera IPv6 antes de calcular el checksum.
- Si el nodo tiene más de una dirección unicast la dirección origen del mensaje la elige de la siguiente forma:

a) Si el mensaje es como respuesta a un mensaje enviado a una de las direcciones unicast del nodo, entonces Dirección Fuente Respuesta = Misma Dirección

b) Si el mensaje es como respuesta a un mensaje enviado a una dirección multicast o grupo anycast del cual el nodo es miembro, en ese caso Dirección Fuente Respuesta = dirección unicast perteneciente a la interfaz que recibió el paquete multicast o anycast.

c) Si el mensaje es como respuesta a un mensaje enviado a una dirección que no pertenece al nodo, entonces Dirección Fuente = Dirección unicast perteneciente al nodo que sirva de más ayuda en el diagnóstico del error.

d) En cualquier otro caso se debe examinar la tabla de encaminamiento del nodo para determinar que interfaz se va a usar para transmitir el mensaje a su destino, Dirección Fuente = Dirección unicast perteneciente a esa interfaz.

Mensaje ICMP de Error

Type = 0-127	Code	Checksum
Parameter		
El mayor contenido posible del paquete invocado sin que el paquete ICMPv6 resultante exceda de 1280 bytes (mínima Path MTU IPv6)		

Tipos de mensajes de error ICMPv6

- Destino Inalcanzable (tipo = 1, parámetro = 0)
  - No hay ruta al destino (código = 0)
  - Comunicación con el destino prohibida administrativamente (código = 1)
  - Más allá del ámbito de la dirección origen (código = 2)
  - Dirección Inalcanzable (código = 3)
  - Puerto Inalcanzable (código = 4)
  - Dirección origen falló política ingress/egress (código = 5)
  - Ruta a destino rechazada (código = 6)
- Paquete demasiado grande (tipo = 2, código = 0, parámetro = next hop MTU)
- Tiempo Excedido (tipo = 3, parámetro = 0)
  - Límite de saltos excedidos en tránsito (código = 0)
  - Tiempo de reensamblado de fragmentos excedido (código = 1)
- Problemas de parámetros (tipo = 4, parámetro = offset to error)
  - Campo de cabecera erróneo (código = 0)
  - Tipo no reconocido de “Next Header” (código = 1)
  - Opción IPv6 no reconocida (código = 2)

Mensajes ICMP Informativos

- Echo Request (tipo =128, código = 0)
- Echo Reply (tipo = 129, código = 0)

Type = 128-255	Code	Checksum
Maximum Response Delay		Reserved
Multicast Address		

- Mensajes MLD (Multicast Listener Discovery):
  - Query, report, done (como IGMP para IPv4):

4.2 Neighbor Discovery

ND (RFC4861)

- Define el protocolo Neighbor Discovery (ND) (Descubrimiento de Vecinos) en IPv6.
- Los nodos usan ND para determinar la dirección de la capa de enlace de los nodos que se sabe que están en el mismo segmento de red y para purgar rápidamente los valores almacenados inválidos.
- Los hosts también usan ND para encontrar encaminadores vecinos que retransmitirán los paquetes que se les envíen.
- Los nodos usan el protocolo para tener conocimiento de los vecinos que son alcanzables y los que no y para detectar cambios de sus direcciones en la capa de enlace.
- ND habilita el mecanismo de autoconfiguración en IPv6.

Interacción Entre Nodos

- Define el mecanismo para solventar:
  - Descubrimiento de encaminadores
  - Descubrimiento de prefijos de red
  - Descubrimiento de parámetros
  - Autoconfiguración de direcciones
  - Resolución de direcciones
  - Determinación del “Next-Hop”
  - Detección de Vecinos Inalcanzables (NUD).
  - Detección de Direcciones Duplicadas (DAD).
  - Redirección del “First-Hop”.

Nuevos Tipos de Paquetes ICMP

- ND define 5 tipos de paquetes:
  - "Router Solicitation" (RS)
  - "Router Advertisement" (RA)
  - "Neighbor Solicitation" (NS)
  - "Neighbor Advertisement" (NA)
  - "Redirect"

Router Advertisements

- En una red (link) con capacidad broadcast, cada encaminador envía periódicamente paquetes multicast RA.
- Un host recibe los RAs de todos los encaminadores, construyendo una lista de encaminadores por defecto.
- El algoritmo de Neighbor Unreachability Detection (NUD) detecta si existen problemas en alcanzar los encaminadores.
- Los RAs contienen una lista de prefijos usados por los hosts para determinar si una dirección destino de un paquete pertenece a dicho link y para la autoconfiguración de direcciones.
- Los RAs y los 'Flags' asociados a cada prefijo permiten a los encaminadores indicar a los hosts como realizar la autoconfiguración (stateless o DHCPv6).

Comparación con IPv4

- IPv6 ND equivaldría a ARP, ICMP Router Discovery e ICMP Redirect en IPv4, con algunas cosas más (NUD).
- ND supone mejoras en muchos aspectos sobre los protocolos usados en IPv4, entre otras:
  - RAs llevan la dirección de la capa de enlace del encaminador, no es necesario resolverla.
  - RAs llevan los prefijos de un enlace, no es necesario un mecanismo para conocer la máscara de red.
  - RAs permiten la Autoconfiguración de direcciones.
  - REDIRECTS llevan la dirección de la capa de enlace del nuevo 'first hop', no es necesario resolverla.
  - El uso de direcciones de enlace local para identificar a los encaminadores, hace que los hosts 'resistan' una renumeración de la red.
  - Usando un 'Hop Limit' de 255 ND es inmune a mensajes ND de fuera del enlace. En IPv4 podían enviar de fuera Redirects y RAs.

Formato Router Advertisement

Bits 8	16			32
Type = 134	**Code = 0**			**Checksum**
Cur Hop Limit	**M**	**O**	**Reserved = 0**	**Router Lifetime**
Reachable Time				
Retrans Timer				
Options …				

- Cur Hop Limit: valor predeterminado que debería ponerse en el campo Hop Count de la cabecera IPv6 de los paquetes que van a ser enviados
- M: 1-bit "Managed address configuration" flag
- O: 1-bit "Other configuration" flag
- Router Lifetime: entero sin signo de16-bits
- Reachable Time: entero sin signo de 32-bits
- Retrans Timer: entero sin signo de 32-bits
- Possible Options: Source LinkLayer Address, MTU, Prefix Information, Flags Expansion (RFC5175)

Formato Router Solicitation

- Cuando arrancan los hosts envían RSs para indicar a los encaminadores que generen un RA inmediatamente.
- Se envía a la dirección multicast que engloba a todos los encaminadores del segmento de red.

Bits 8	16	32
Type = 133	**Code = 0**	**Checksum**
Reserved = 0		
Options …		

- Opciones Posibles: Source Link-Layer Address.

Formato Neighbor Solicitation

- Los nodos envían NSs para obtener la dirección MAC del nodo con el que se pretende comunicar, a la vez que se proporciona la propia dirección MAC del nodo solicitante.
- Los paquetes NSs son multicast cuando el nodo precisa resolver una dirección y unicast cuando el nodo pretende averiguar si un vecino es alcanzable.

Bits 8	16	32
Type = 135	**Code = 0**	**Checksum**
Reserved = 0		
Target Address		
Options …		

- Target Address: La dirección IPv6 objetivo de la solicitud. No debe ser una dirección multicast.
- Opciones Posibles : Source Link-Layer Address.

Formato Neighbor Advertisement

- Un nodo envía NAs como respuesta a un NS y envía NAs no solicitados para propagar nueva información rápidamente.

Bits	8	16	32
Type = 136		**Code = 0**	**Checksum**
R	**S**	**O**	**Reserved = 0**
Target Address			
Options …			

- Flags:
  - **R**: **Router Flag**=1 indica que el que envía en un encaminador.
  - **S**: **Solicited Flag**=1 indica que se envía como respuesta a un NS.
  - **O**: **Override Flag**=1 indica que deben actualizarse las caches.
- Para NA solicitados, igual al campo “Target Address” del NS. Para un NA no solicitado, la dirección cuya MAC ha cambiado. No puede ser una dirección multicast.
- Posibles Opciones: Target Link-Layer Address (MAC del Tx).

Formato Redirect

- Los encaminadores envían paquetes Redirect para informar a un host que existe otro encaminador mejor en el camino hacia el destino final.
- Los hosts pueden ser redireccionados a otro encaminador mejor pero también pueden ser informados mediante un paquete Redirect que el destino es un vecino.

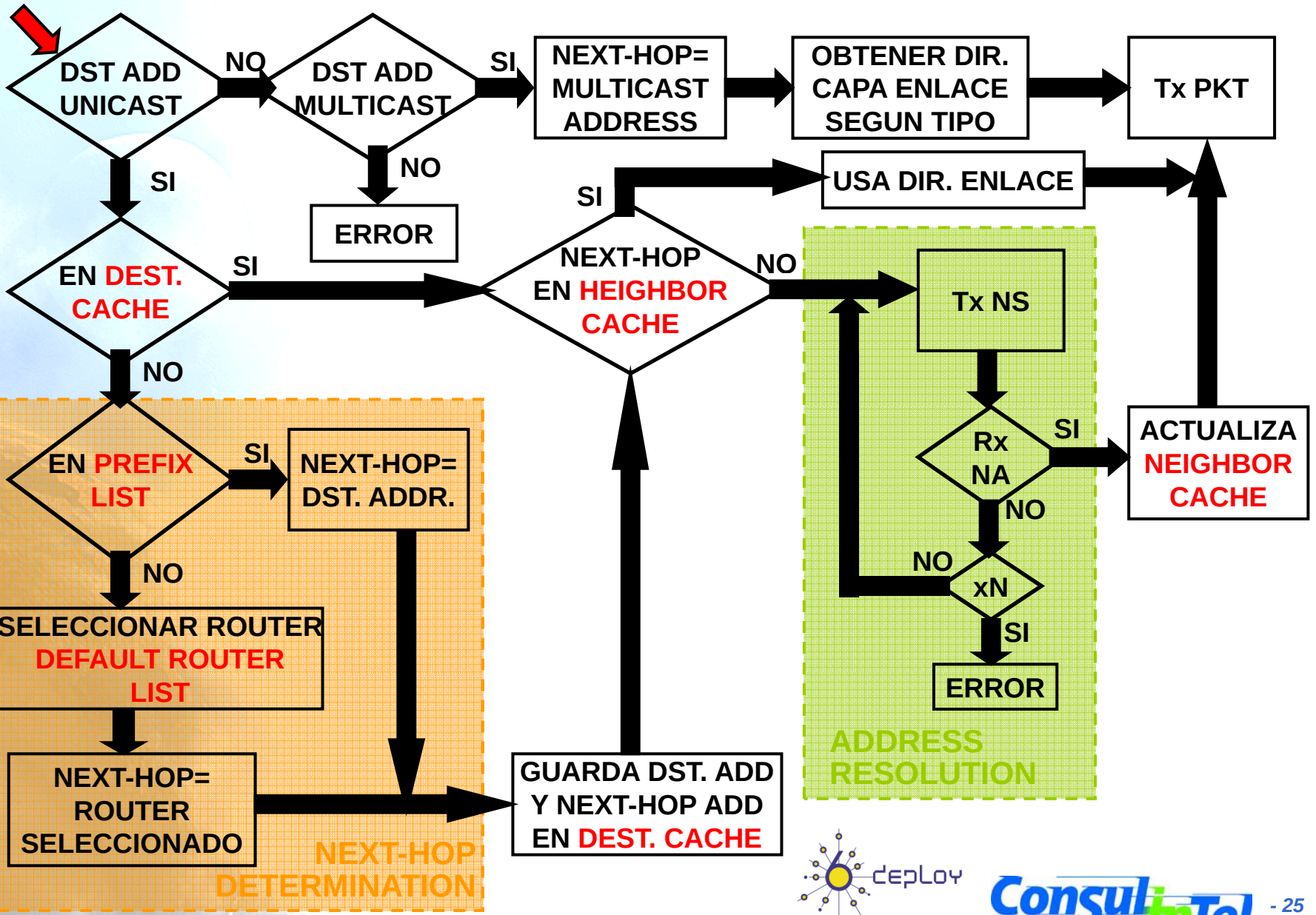
Bits 8	16	32
Type = 137	**Code = 0**	**Checksum**
Reserved = 0		
Target Address		
Destination Address		
Options …		

- Target Address: La dirección IPv6 del ‘first hop’ que es mejor usar para llegar al ‘Destination Address’ del paquete ICMPv6
- Destination Address: La dirección IPv6 de destino que es redireccionada al ‘target address’ del paquete ICMPv6

Ejemplo Funcionamiento (1)

- **Neighbor Cache**: Vecinos a los que se les ha enviado tráfico recientemente. Se indexa por la ‘on-link unicast IP address’. Cada entrada contiene: dir. capa enlace, si es router/host, información de NUD (reachability state, etc.).
- **Destination Cache**: Mapea IP destino con ‘next hop’. Direcciones a las que se ha enviado recientemente.
- **Prefix List**: Contiene los prefijos del enlace. Se basa en los RAs, de donde se saca también el tiempo de validez.
- **Default Router List**: Lista de routers a donde los paquetes ‘off-link’ deben ser enviados. Cada entrada apunta a una entrada en la Neighbor Cache y tiene un tiempo de validez obtenido del RA (router lifetime).

Ejemplo Funcionamiento (2): Envío



Preferencias Encaminador por Defecto y Rutas Más Específicas (RFC4191)

Bits 8	16			32
Type = 134	**Code = 0**			**Checksum**
Cur Hop Limit	**M**	**O**	**H| PRF| Rsvd**	**Router Lifetime**
Reachable Time				
Retrans Timer				
Options …				

- RFC4191 describe una extensión opcional para los RAs para que los encaminadores comuniquen a los hosts preferencias para los encaminadores por defecto y rutas más específicas.
- PRF (Default Router Preference) = 01 Alta
  = 00 Meda (Por defecto)
  = 11 Baja
  = 10 Reservada (NO SE DEBE usar)
- También se define la **Route Information Option**, también con PRF (Route Preference) de 2-bits (entero con signo) (mismos valores).

4.3 Autoconfiguración

Autoconfiguración

- El estándar especifica los pasos que un host debe seguir para decidir cómo auto-configurar sus interfaces de red en IPv6
- El proceso de auto-configuración incluye la creación de una dirección IPv6 de ámbito local (link-local) y la verificación de que no está duplicada en el mismo segmento de red, determinando qué información debería ser auto-configurada y en el caso de direcciones, si estas deberían obtenerse mediante “stateful”, “stateless” o ambos
- IPv6 define tanto un mecanismo de auto-configuración de direcciones de tipo “stateful” como “stateless”
- La auto-configuración “stateless” (SAAC) no precisa de configuración manual en el host, mínima (si acaso alguna) configuración de encaminadores y ningún servidor adicional

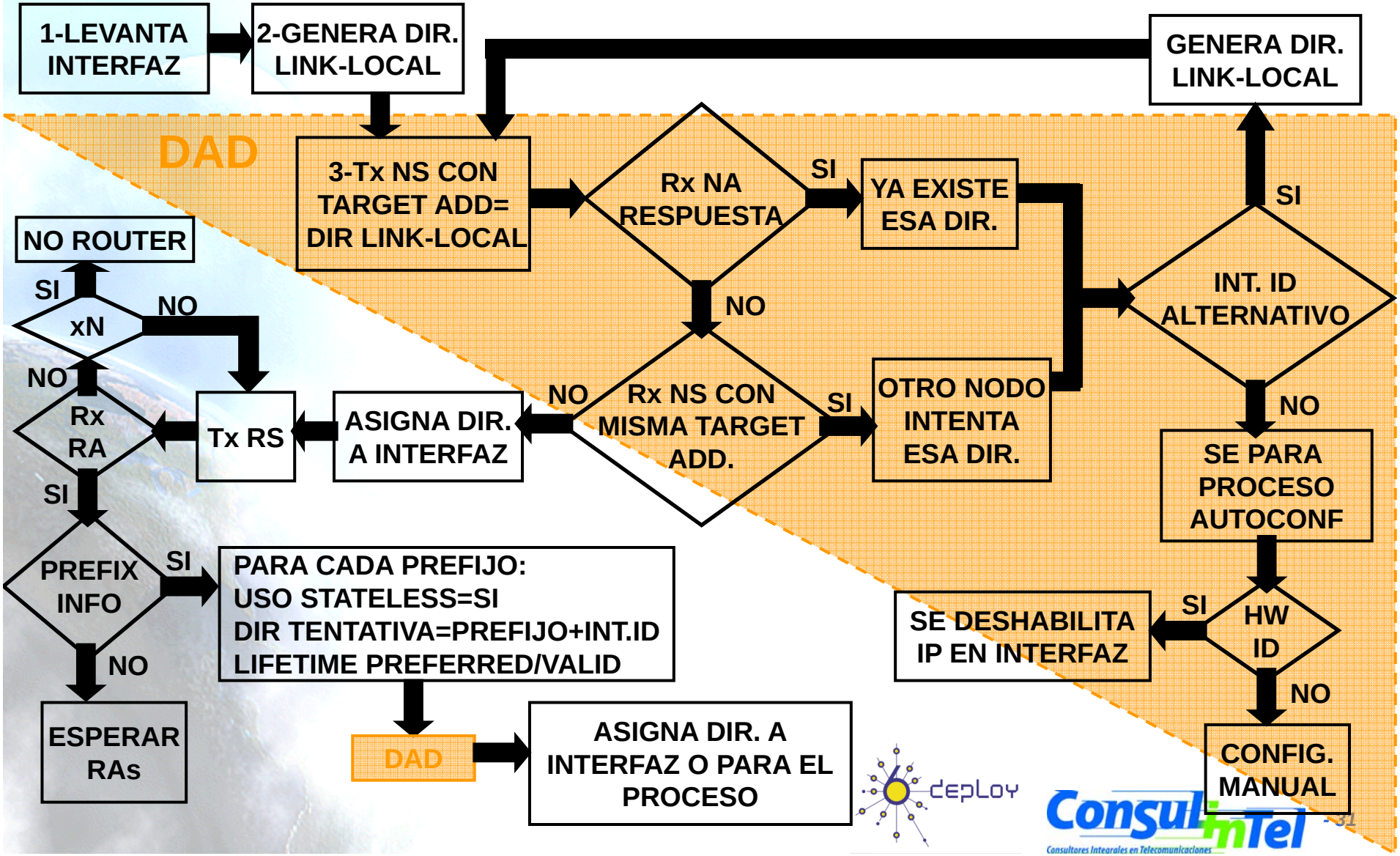
Autoconfiguración Stateless o Serverless (RFC4862)

- El mecanismo “stateless” permite a un host generar su propia dirección usando una combinación de información localmente disponible y de información proporcionada por los encaminadores
- Los **encaminadores anuncian los prefijos de red** que identifican la sub-red asociada a un determinado segmento de red
- Los **hosts generan un identificador de interfaz** que lo identifica de manera única en la subred. Dicho identificador se genera localmente, por ejemplo a partir de la dirección MAC
- Una dirección IPv6 se forma mediante la combinación de ambas informaciones
- En la ausencia de encaminadores, un host puede generar solo las direcciones IPv6 de ámbito local (link-local)
- Las direcciones link-local son suficiente para permitir la comunicación IPv6 entre nodos que están conectados en el mismo segmento de red

Ventajas/Beneficios de la Autoconfiguración Stateless

- La configuración manual de cada máquina antes de conectarla a la red no es necesaria
- Los sitios pequeños compuesto de pocas máquinas conectadas al mismo segmento no necesitarían de un servidor DHCPv6 ni de un encaminador para comunicarse, usarían direcciones link-local
- Un sitio grande con varias subredes no necesitaría de un servidor DHCPv6 para la configuración de direcciones
- Facilita el cambio de prefijo de una sitio mediante el uso de varias direcciones por interfaz y tiempo de vida

Funcionamiento de la Autoconfiguración Stateless



Formato Prefix Information Option

Bits 8	16	24	32		
Type = 3	**Length = 4**	**Prefix Length**	**L**	**A**	**Reserved1 = 0**
Valid Lifetime					
Preferred Lifetime					
Reserved2 = 0					
Prefix					

- **L**(1bit): **on-link flag**=1 indica que el prefijo se puede usar para la determinación ‘en-enlace’.
- **A**(1bit): **autonomous address-configuration flag**=1 indica que este prefijo puede usarse para SAAC.
- **Valid Lifetime**: Tiempo en segs. que el prefijo es valido para determinación ‘en-enlace’. También usado en SAAC.
- **Preferred Lifetime**: Tiempo en segundos que la dirección generada con SAAC permanece como ‘preferred’.
- **Prefix** (128 bits): Dirección IP o prefijo de una dirección.

Autoconfiguración Stateful o DHCPv6 (RFC3315)

- Los hosts obtienen las direcciones de la interfaz de red y/o información de configuración desde un servidor
- Los servidores mantienen una base de datos que actualizan con las direcciones que han sido asignadas y con información de a qué hosts se han asignado
- La auto-configuración “stateless” y la “stateful” se complementan una a la otra
- Ambos tipos de auto-configuración se pueden usar de forma simultánea
- El administrador de red especifica qué tipo de auto-configuración se usa, por medio de la configuración de los campos adecuados de los mensajes RAs

Tiempo de Validez de las Direcciones

- Las direcciones IPv6 se asignan a un interfaz por un tiempo determinado (posiblemente infinito) que indica el periodo de validez de la asignación
- Cuando el tiempo de asignación expira, la asignación ya no es válida y la dirección puede ser reasignada a otra interfaz de red en cualquier otra red dentro de Internet
- Con el fin de gestionar de una manera adecuada la expiración de las direcciones, una dirección pasa por dos fase distintas mientras está asignada a una interfaz.
  - Inicialmente una dirección es la preferida (preferred), lo cual significa que su uso en una comunicación arbitraria no está restringida
  - Más tarde, una dirección se convierte en “deprecada” anticipándose al hecho de que su asignación al interfaz de red será inválido en breve

Detección de Direcciones Duplicadas

- Para asegurarse de que todas las direcciones configuradas son únicas en un determinado segmento de red los nodos ejecutan el algoritmo DAD (Duplicate Address Detection) antes de que la asignación de las direcciones a una interfaz de red sea definitiva
- El algoritmo DAD se realiza para todas las direcciones, independientemente de si se obtienen mediante auto-configuración “stateless” o “stateful”
- El procedimiento para detectar las direcciones duplicadas emplea mensajes NS y NA
- Ya que la auto-configuración de los hosts usa la información anunciada por los encaminadores, estos necesitan ser configurados por algún otro medio. Sin embargo, los encaminadores deben generar las direcciones de ámbito local (link-local) usando el mismo mecanismo
- De este modo los encaminadores también deben pasar adecuadamente el algoritmo de DAD en todas las direcciones antes de asignarlas a sus respectivas interfaces

Configuración DNS usando Autoconfiguración Stateless (1)

- Tradicionalmente la configuración del servidor DNS en los nodos IPv6 se ha hecho por medio de:
  - Configuración manual
  - DHCPv6 o DHCPv4 (en el caso de nodos de Doble Pila)
- Sin embargo esto plantea algunos inconvenientes en ciertos entornos:
  - Necesidad de ejecutar dos protocolos en IPv6 (Auto-configuración Stateless –RA-, DHCPv6)
  - Retardo en la obtención de la dirección del servidor DNS cuando se emplea DHCP
  - Inviabilidad de la configuración manual y/o retardo por DHCP en entornos inalámbricos en los que el nodo cambia de red de manera contínua
- Se puede emplear la configuración DNS basada en RA de forma alternativa para proporcionar la dirección de uno o varios servidores DNS
  - Se emplea una opción específica en el paquete RA
    - Recursive DNS Server (RDNSS)
  - Se puede emplear de forma conjunta con DHCPv6

Configuración DNS usando Autoconfiguración Stateless (2)

- El funcionamiento es el mismo que el que usan los nodos para aprender los encaminadores o el prefijo IPv6 /64 en una red, especificado en RFC4862: IPv6 Stateless Address Autoconfiguration
- Por medio de la opción RDNSS, los nodos aprenden con un solo intercambio de paquetes:
  - Configuración relativa a la red (prefijo /64)
  - Servidores DNS más próximos
- Si además de proporcionar la dirección de los servidores DNS por medio de la opción RDNSS se va a emplear DHCPv6, entonces hay que activar el Flag “O” del paquete RA
- La configuración de la opción RDNSS en los encaminadores se realiza:
  - de forma manual
  - de forma automática mediante DHCPv6 (cliente)

4.4 DHCPv6

DHCPv6 (RFC3315 - RFC4361)

- DHCP para IPv6 (DHCPv6) es un protocolo UDP cliente/servidor diseñado para reducir el coste de la gestión de nodos IPv6 en entornos donde los administradores de red precisan de más control sobre la asignación de direcciones IPv6 y la configuración de los parámetros de red que el ofrecido por la auto-configuración de tipo “stateless”
- DHCPv6 reduce el coste de la asignación de direcciones centralizando la gestión de los recursos de red en vez de distribuir dicha información en ficheros de configuración local entre cada nodo de la red
- DHCPv6 se ha diseñado para ser extendida fácilmente para transportar parámetros nuevos de configuración añadiendo nuevas opciones DHCP definidas para dichas necesidades

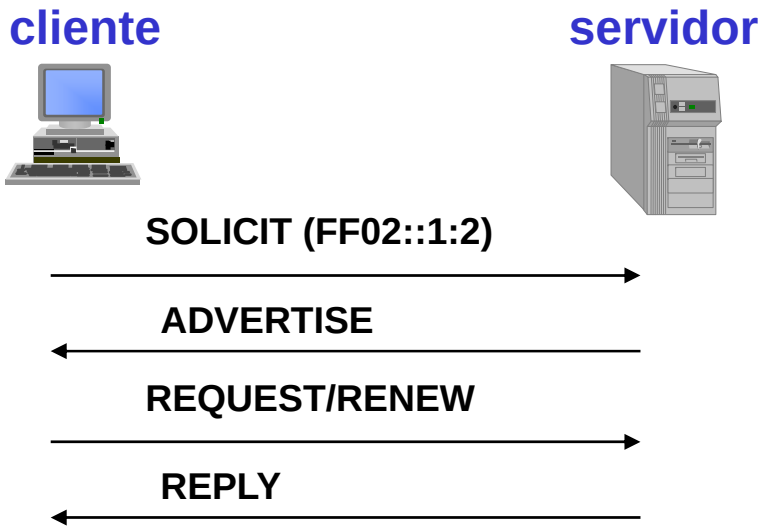
Objetivos de DHCPv6

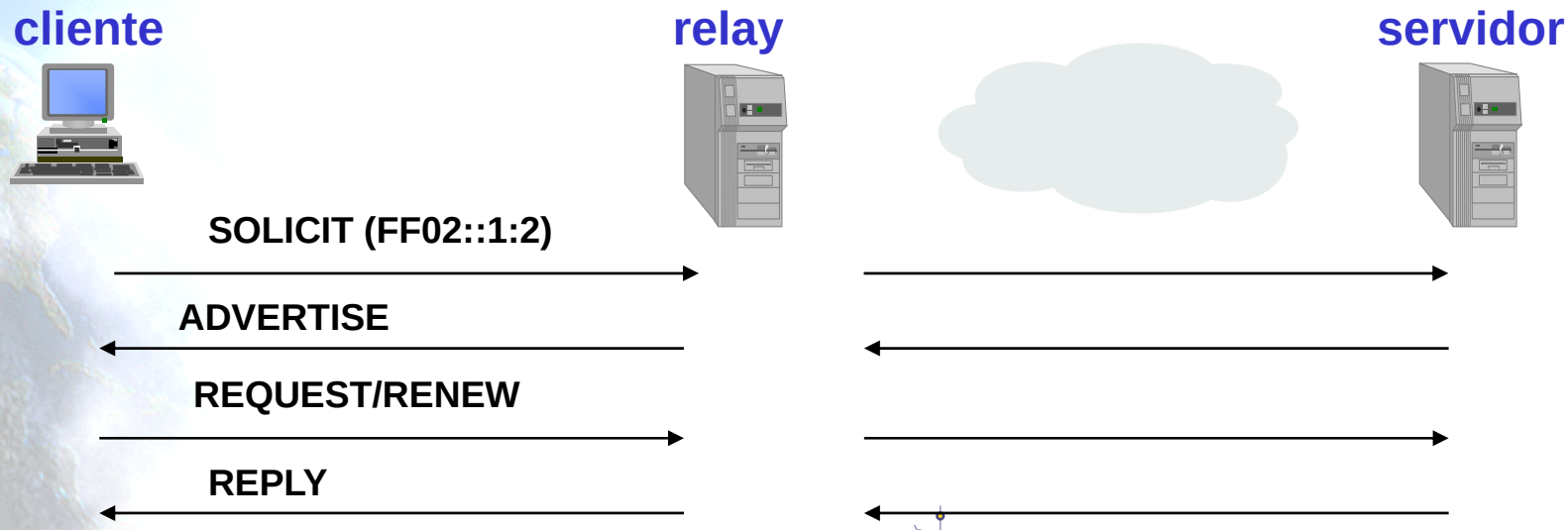
- Es un mecanismo, no una política de asignación
- Es compatible con la auto-configuración IPv6 “stateless”
- No requiere configuración manual de parámetros de red en los clientes DHCP
- No requiere un servidor en cada segmento de red
- Coexiste con nodos configurados estáticamente, nodos no participantes y con otras implementaciones de protocolos de red existentes
- Los clientes DHCP pueden operar en un segmento de red sin que estén presentes encaminadores IPv6
- DHCP proporciona la capacidad de renumeración de las redes
- Un cliente DHCP puede hacer peticiones diferentes y múltiples
- DHCP contiene temporizadores y mecanismos de retransmisión para funcionar de forma eficiente en entornos con alta latencia y bajo ancho de banda

Detalles de DHCPv6

- Los puertos UDP son
  - Clientes escuchan en el 546
  - Servidores y relays escuchan en el 547
- Direcciones para servidores DHCPv6 y relays
  - FF02::1:2 (link local scope)
  - FF05::1:3 (site scope only for servers)
- Mensajes DHCP
  - SOLICIT
  - ADVERTISE
  - REQUES
  - CONFIRM
  - RENEW
  - REBIND
  - REPLY
  - RELEASE
  - DECLINE
  - RECONFIGURE
  - INFORMATION-REQUEST
  - RELAY-FORW
  - RELAY-REPL
- Cada mensaje puede transportar una o más opciones DHCP
  - Domain-list
  - DNS-server
  - IA-NA, etc.
- Identificador Único DHCP (DHCP Unique Identifier, DUID)
  - Los servidores usan DUIDs para identificar a los clientes para la selección de unos determinados parámetros de configuración
  - Los clientes usan los DUIDs para identificar un servidor en aquellos mensajes en los que el servidor necesita ser identificado

Ejemplo Básico de DHCPv6





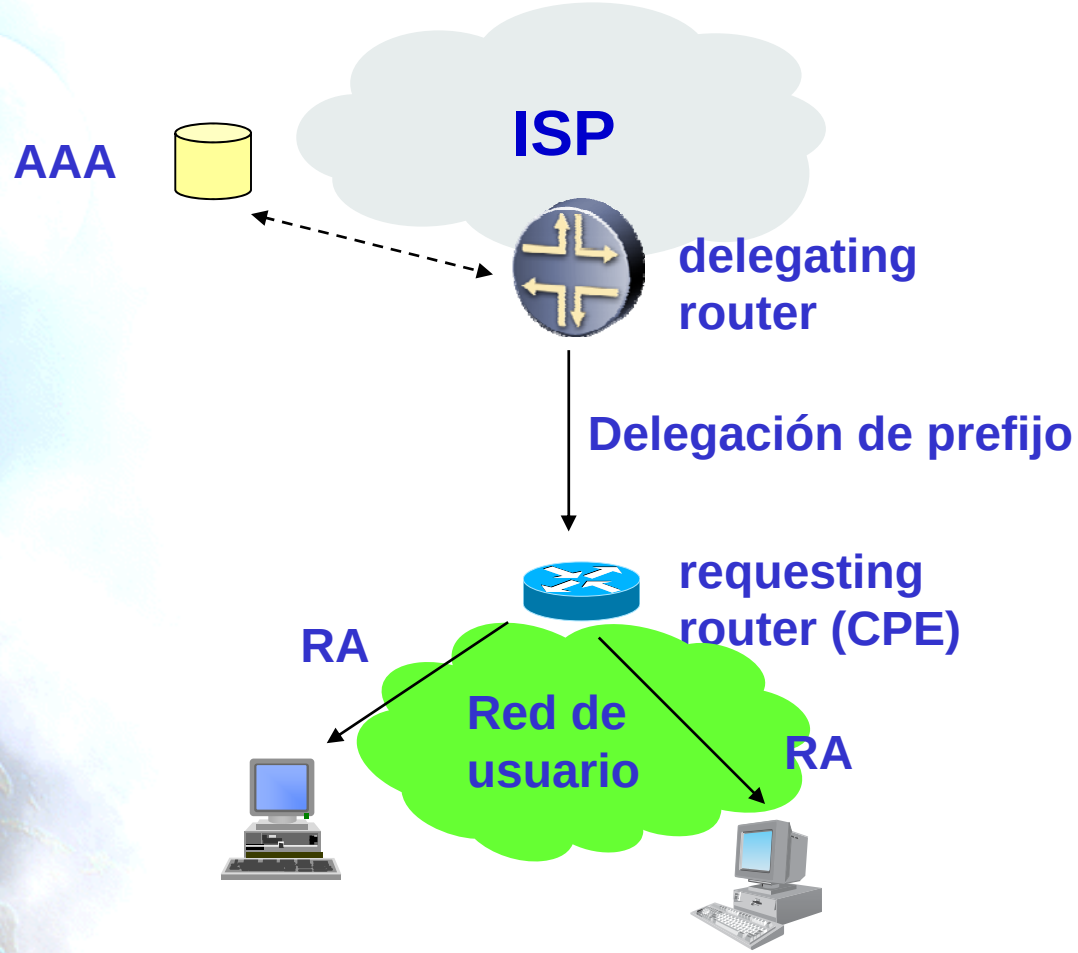
DHCPv6-PD (RFC3633)

- Proporciona a los encaminadores autorizados que lo necesiten un mecanismo automatizado para la delegación de prefijos IPv6
- Los encaminadores que delegan no necesitan tener conocimiento acerca de la topología de red a la que están conectados los encaminadores solicitantes
- Los encaminadores que delegan no necesitan ninguna información aparte de la identidad del encaminador que solicita la delegación de un prefijo
  - un ISP que asigna un prefijo a un CPE que actúa como encaminador

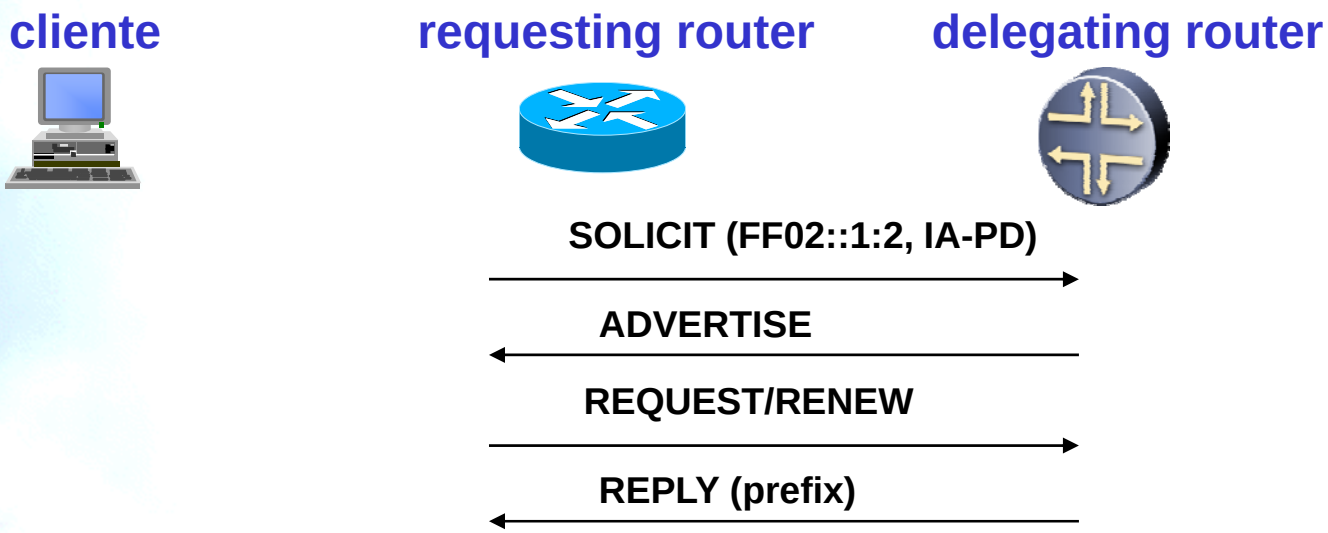
Detalles de DHCPv6-PD

- El encaminador que solicita la delegación (Requesting Router, RR) necesita autenticación
- El perfil de un RR se puede almacenar en un servidor AAA
- El prefijo delegado se puede extraer de:
  - Perfil del cliente almacenado en el servidor AAA
  - Lista de prefijos (prefix pool)
- Los prefijos delegados tienen cierto período de validez, al igual que las direcciones IPv6 en DHCPv6
- Lo que DHCPv6-PD no hace es proporcionar un método para propagar el prefijo delegado a través de la red del usuario
  - Todos los prefijos ::/64 que se pueden extraer de un prefijo delegado se asignan en el RR de acuerdo a las políticas que tengan configuradas
- Se pueden usar los DHCPv6 relays en DHPv6-PD de igual forma que en DHCPv6

Arquitectura de Red para DHCPv6-PD



Ejemplo Básico de DHCPv6-PD



Nuevas Características de Usuario con DHCPv6

- Configuración de actualizaciones dinámicas de servidores DNS
- Deprecación de direcciones para la renumeración dinámica
- Los “relays” se pueden configurar con direcciones de servidor o usar multicast
- Autenticación
- Los clientes pueden pedir múltiples direcciones IPv6
- Las direcciones pueden ser reclamadas usando mensajes “Reconfigure-init”
- Integración entre auto-configuración de tipo “stateful” y “stateless”
- Habilitando “relays” para localizar servidores no alcanzables

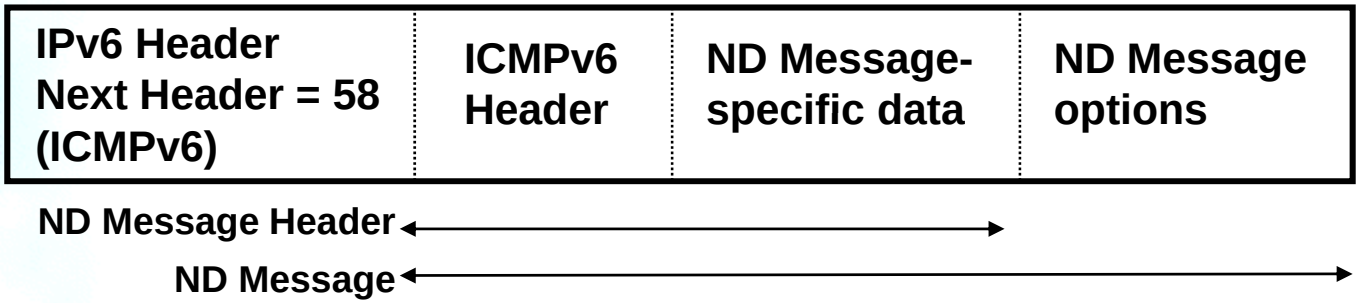
4.5 Secure Neighbor Discovery

Secure Neighbor Discovery - SEND (RFC3971)

- Los nodos IPv6 usan NDP (Neighbor Discovery Protocol) para:
  - Descubrir otros nodos en el segmento de red o enlace
  - Determinar su dirección de nivel de enlace
  - Mantener información para saber si los vecinos siguen activos
- NDP es vulnerable a varios ataques si no se asegura
- El RFC3971 especifica ciertos mecanismos de seguridad para NDP
  - Estos mecanismos no usan IPSec, a diferencia de las especificaciones originales de NDP
  - SEND se aplica en entornos donde la seguridad física del enlace no está asegurado (como por ejemplo redes inalámbricas)
- De momento solo hay implementaciones de SEND para linux y *BSD
  - P.e. http://www.docomolabs-usa.com/lab_opensource.html

Elementos de SEND

- Un mensaje NDP sigue el mismo formato que los mensajes ICMPv6
- Un mensaje NDP real incluye:
  - Cabecera del mensaje NDP
    - Cabecera ICMPv6
    - Datos específicos del mensaje ND
  - y cero o más opciones NDP, las cuales siguen el formato “Type-Length-Value”



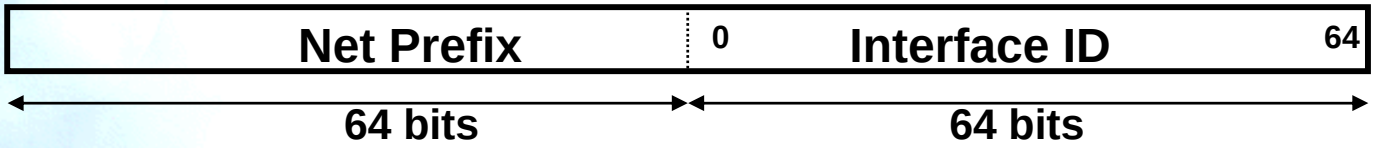
- Se definen una serie de nuevas opciones ND para asegurar NDP y proteger sus mensajes
- El RFC3971 introduce
  - Opciones de SEND para Neighbor Discovery
  - Un proceso de descubrimiento de delegación de autorización
  - Un mecanismo para probar la propiedad de una dirección
  - Y los requisitos para el uso de estos componentes en NDP

Funcionamiento de SEND y CGAs

- SEND se basa en el uso de CGAs (Cryptographically Generated Addresses)
- Una CGA es una dirección IPv6 que se ha formado con un mecanismo especial definido en RFC3972
  - El RFC3972 describe un método para ligar una clave pública a una dirección IPv6 en el contexto de SEND
  - Para ello, se genera un par de claves pública-privada en el nodo que usa SEND
  - Partiendo de un ID de interfaz, una clave pública y de ciertos parámetros auxiliares, se construye un nuevo ID de interfaz mediante una función hash criptográfica univoca
  - Las CGAs son direcciones IPv6 para las que el ID de interfaz se genera por medio de dicho método
  - La relación entre la clave pública y la dirección se puede verificar re-calculando el valor hash y comparándolo con el ID de interfaz
  - La protección así definida funciona sin necesidad de una autoridad certificadores ni una infraestructura de seguridad añadida
  - Los nodos que usen SEND DEBEN usar CGAs
- La autenticidad del nodo que use una CGA viene dada por la acción conjunta de
  - El uso de su clave publica para generar la CGA
  - La firma del mensaje con su clave privada

Formato de CGAs IPv6

- RFC3972 considera
  - Dirección IPv6: leftmost 64 bits = subnet prefix, rightmost 64 bits = ID de interfaz
  - Los bits ID de interfaz se numeran empezando desde el bit cero que está a la izquierda
  - Una CGA tiene un parámetro de seguridad (Sec) que determina su fortaleza frente a ataques de fuerza bruta
    - Sec es un parámetro entero sin singo de 3 bits codificado en los tres bits mas a la izquierda del ID de interfaz (bits 0 - 2)
    - Sec = (ID de interfaz & 0xe000000000000000) >> 61



- La CGA se asocia a una serie de parámetros que consisten en una clave pública y parámetros auxiliares
  - Se calculan dos valores hash a partir de esos parámetros: Hash1 (64 bits) y Hash2 (112 bits)
- La CGA satisface las dos condiciones siguientes:
  - El valor hash1 es igual al ID de interfaz de la dirección. Los bits 0, 1, 2, 6 y (parámetro Sec y bits "u" y "g" del formato de una dirección IPv6 estándar) se ignoran en la comparación
  - Los 16*Sec bits de la izquierda del segundo valor hash (Hash2) son cero
  - La definición anterior se puede establecer en los términos de las dos máscaras siguientes :
    Mask1 (64 bits) = 0x1cffffffffffffff
    Mask2 (112 bits) = 0x00000000000000000000000000 if Sec=0,
    0xffff0000000000000000000000 if Sec=1,
    0xffffffff00000000000000000000 if Sec=2,
    0xffffffffffff000000000000000000 if Sec=3,
    0xffffffffffffffff0000000000000000 if Sec=4,
    0xffffffffffffffffff00000000 if Sec=5,
    0xffffffffffffffffffffff0000 if Sec=6, y
    0xffffffffffffffffffffffffff if Sec=7

- Luego una CGA es un dirección IPv6 para las que se cumplen las dos ecuaciones siguientes:
  Hash1 & Mask1 == ID de interfaz & Mask1
  Hash2 & Mask2 == 0x00000000000000000000000000

Opciones de SEND para Neighbor Discovery (1)

- La opción CGA (Cryptographically Generated Addresses) para transportar la clave pública y los parámetros asociados necesarios para verificar que la CGA es correcta
  - Si el nodo usa SEND, la opción CGA es obligatoria y asegura que el remitente de un mensaje ND es el propietario de la dirección que dice tener
  - Un par de claves publica-privada deben generarse por todos los nodos antes de poder reclamar una dirección
  - El RFC3971 también permite a un nodo usar direcciones que no son CGA, sino que son aseguradas por medio de certificados, aunque los detalles en este caso quedan fuera de la especificación
- Formato:

Bits 8	Bits 16	24	32
Type = 11	**Length**	**Pad Length**	**Reserved**
CGA Parameters			
Padding			

Opciones de SEND para Neighbor Discovery (2)

- La opción de firma RSA (RSA Encryption Standard) se usa para proteger todos los mensaje relacionados con ND y RD
  - Las firmas con claves privada protegen la integridad de los mensajes y autentican la identidad del remitente
  - Esta opción permite añadir una firma RSA al mensaje NDP
  - Es sólo opcional, pero recomendable para verificar la autenticdad del remitente

- Formato:

Bits 8	Bits 16	32
Type = 12	**Length**	**Reserved**
Key Hash (128-bit)		
Digital Signature (PKCS#1 v1.5 signature)		
Padding		

Opciones de SEND para Neighbor Discovery (3)

- Las opciones “Timestamp” y “Nonce” sirven para prevenir ataques de réplica
  - La opción “Timestamp” ofrece protección frente a reenvío de paquetes aprendidos (ataque de réplica) sin necesidad de usar números de secuencia ni establecimiento de estados. Sirve de gran utilidad por ejemplo, para mensajes ND y RD enviados a direcciones multicast
  - La opción “Nonce” protege los pares de mensajes de solicitación y anuncio de vecinos
    - El “nonce” es un número aleatorio o pseudo-aleatorio impredecible y generado y usado solo una vez por un nodo. En SEND estos números se usan para asegura que un anuncio particular se refiere a la solicitud que lo ha generado

Proceso de “Authorization Delegation Discovery” (1)

- Planteamiento del problema
  - NDP permite a un nodo autoconfigurarse basándose en la información recibida de la red
  - Es muy fácil configurar un nodo como encaminador “maligno” en un enlace de red que no sea seguro y por contra muy difícil para el nodo recién conectado distinguir entre fuentes de información de red válidas o inválidas
    - El nodo necesita precisamente esa información para poder comunicar
  - Puesto que el nodo recién conectado no se puede comunicar con otros nodos fuera del link, no puede ser responsable de buscar información que le ayude a validar al encaminador que le envía información sobre la red
  - Sin embargo, si existe un “certification path” el nodo puede concluir que un determinado encaminador es una fuente autorizada o no
  - In the typical case, a router already connected beyond the link can communicate if necessary with off-link nodes and construct a certification path
- Certification path
  - SEND hace obligatorio el uso de
    - Un formato para el certificado
    - Dos nuevos mensajes ICMPv6 usados entre nodos y encaminadores
  - Ambas cosas permite que el nodo conozca el camino de certificación con la ayuda del encaminador

Proceso de “Authorization Delegation Discovery” (2)

- Modelo para la autorización
  - Para proteger el RD, SEND requiere que los encaminadores sean autorizados a actuar como tal
  - Esta información se proporciona tanto a los encaminadores como a los nodos
  - Una autoridad de confianza proporciona certificados a los encaminadores y a los nodos se les configura esa autoridad de confianza para autorizar a los encaminadores
  - Este modelo es específico de SEND y no asume que los certificados que ya estén desplegados para otros propósitos sean usados para SEND
- La autorización para los encaminadores es doble:
  - Los encaminadores son autorizados a actuar como encaminadores
    - Solo si el encaminador pertenece al conjunto de encaminadores autorizados por la autoridad de confianza
  - Opcionalmente, a los encaminadores también se les puede autorizar a anunciar un conjunto de prefijos de red
    - A un encaminador específico se le autoriza a anunciar un determinado conjunto de prefijos mientras que a otros encaminadores se les autoriza a anunciar un conjunto de prefijos diferente

Formato del Certificado (1)

- El camino de certificación de un encaminador acaba en un Certificado de Autorización de Encaminador el cual autoriza a un nodo IPv6 específico a actual como encaminador
  - Dado que los caminos de autorización no son muy comunes en la práctica en Internet, el camino DEBE estar compuesto de Certificados de Clave Pública estándar (Public Key Certificates, PKC)
  - El camino de certificación DEBE comenzar en la autoridad de confianza compartida entre el nodo y el encaminador.
  - Una autoridad de confianza puede emitir multitud de certificados
- Certificado de Autorización de Encaminador
  - Son certificados X.509v3 (RFC3280)
  - DEBEN incluir al menos una instancia de una extensión X.509 para direcciones IP (RFC3779)

Formato del Certificado (2)

- Ejemplo de camino de certificación
  - Supongamos que isp_group_example.net es la autoridad de confianza. El nodo tendrá el siguiente certificado:

Certificate 1:
Issuer: isp_group_example.net
Validity: Jan 1, 2004 through Dec 31, 2004
Subject: isp_group_example.net
Extensions:
IP address delegation extension:
Prefixes: P1, ..., Pk
... possibly other extensions ...
... other certificate parameters ...

  - Cuando un nodo se conecta a la red servida por router_x.isp_foo_example.net, recibe el siguiente camino de certificación:

Certificate 2:
Issuer: isp_group_example.net
Validity: Jan 1, 2004 through Dec 31, 2004
Subject: isp_foo_example.net
Extensions:
IP address delegation extension:
Prefixes: Q1, ..., Qk
... possibly other extensions ...
... other certificate parameters ...

Certificate 3:
Issuer: isp_foo_example.net
Validity: Jan 1, 2004 through Dec 31, 2004
Subject: router_x.isp_foo_example.net
Extensions:
IP address delegation extension:
Prefixes R1, ..., Rk
... possibly other extensions ...

... other certificate parameters ...

4.6 Router Renumbering

Router Renumbering (RFC2894)

- ND y la auto-configuración de direcciones IPv6 hacen la asignación inicial de los prefijos y de las direcciones de red a los diversos hosts
- Gracias a estos dos mecanismos, el procedimiento de reconfiguración de hosts es extremadamente sencillo cuando los prefijos de una red cambian
- El mecanismo de renumeración de encaminadores (Router Renumbering, "RR“) permite configurar y reconfigurar los prefijos de direcciones en los encaminadores tan fácilmente como funciona la combinación de ND y la auto-configuración de direcciones en los hosts
- Proporciona un medio para que el administrador de la red haga actualizaciones en los prefijos usados y que se anuncian por medio de los encaminadores IPv6 a toda una red

Funcionamiento

- Los paquetes “Router Renumbering Command” contiene una secuencia de operaciones de control de prefijos (Prefix Control Operations, PCO)
- Cada PCO especifica una operación, un prefijo-plantilla y cero o más prefijos de uso
- Un encaminador procesa cada PCO, comprobando cada una de sus interfaces para una dirección o prefijo que concuerda con el prefijo-plantilla
- Se aplica a cada interfaz en la que el prefijo-plantilla concuerda
- La operación puede ser: ADD, CHANGE, o SET-GLOBAL para respectivamente instar al encaminador a añadir un prefijo de uso, para configurar prefijos, quitar un prefijo y reemplazarlo con el prefijo de uso, o reemplazar todos los prefijos de ámbito global con los prefijos de uso

Gracias !!

Contacto:

- Cesar Olvera (Consulintel): cesar.olvera@consulintel.es
- Alvaro Vives (Consulintel): alvaro.vives@consulintel.es

6DEPLOY Project: http://www.6deploy.org

The IPv6 Portal: http://www.ipv6tf.org