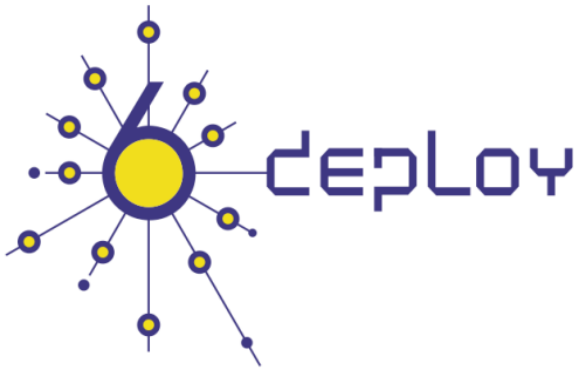
WALC2011
Track 2: Despliegue de IPv6
Día -1
Guayaquil - Ecuador
10-14 Octubre 2011



Alvaro Vives (alvaro.vives@consulintel.es)

4. ICMPv6, Neighbor Discovery y DHCPv6

4.1 ICMPv6

4.2 Neighbor Discovery

4.3 Autoconfiguración

4.4 DHCPv6

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.

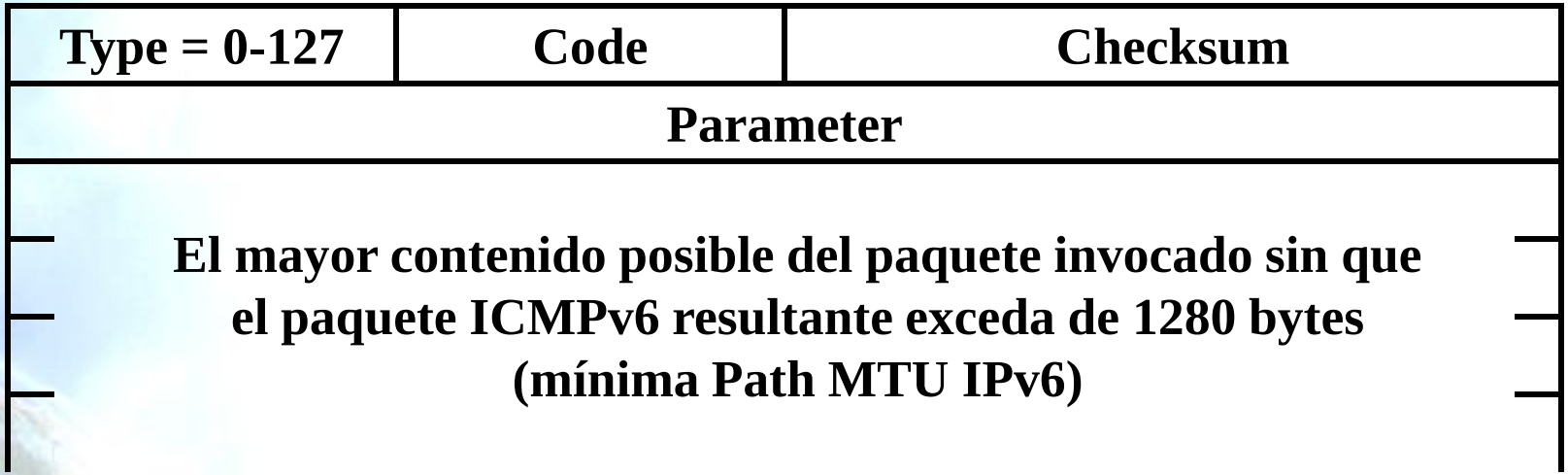
Mensajes ICMPv6

- 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.

Mensaje ICMP de Error



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.

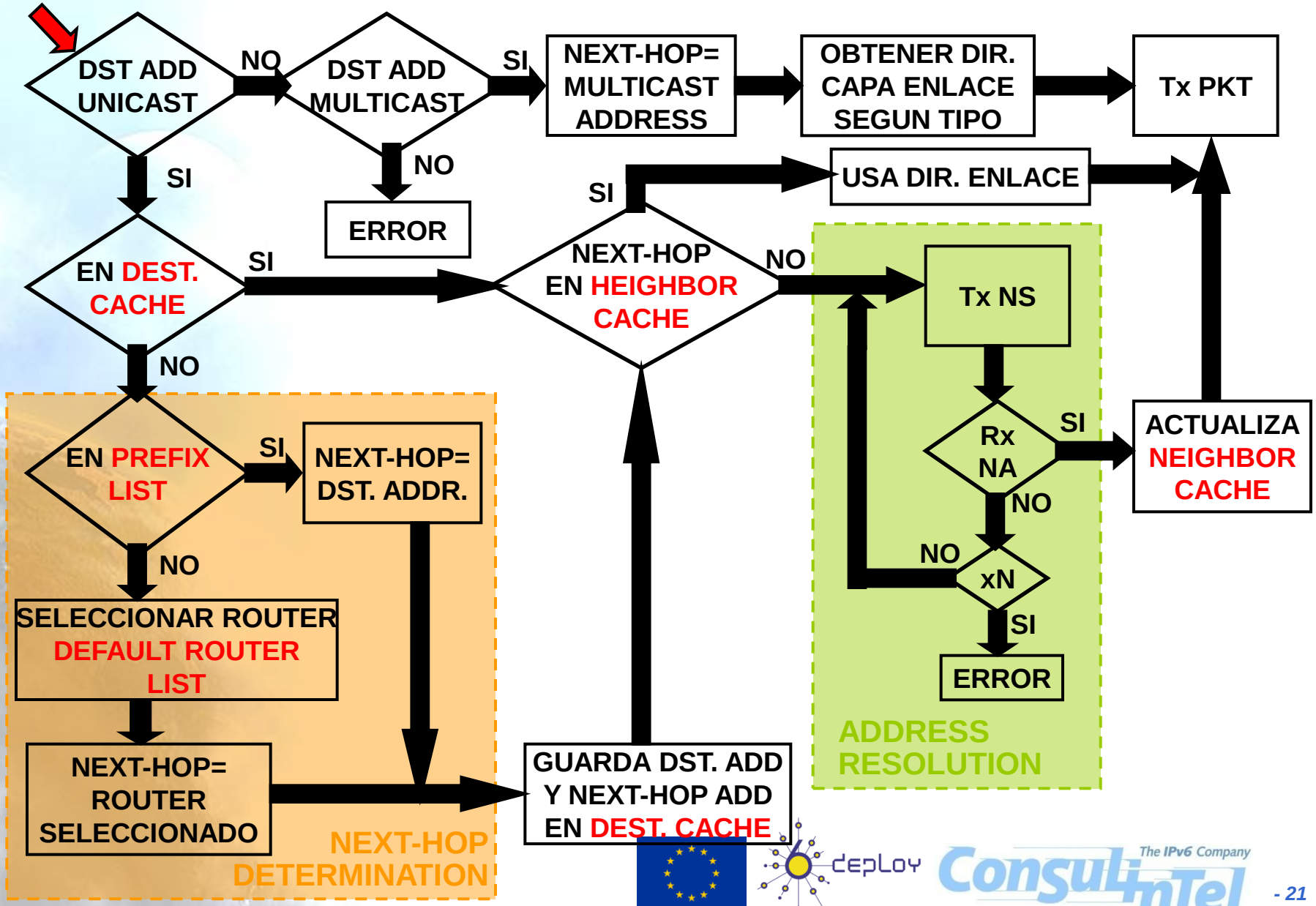
Bits 8	16	32
Type = 137	**Code = 0**	**Checksum**
Reserved = 0		
Target Address		
Destination Address		
Options …		

- 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



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” (SLAAC) no precisa de configuración manual en el host, mínima (si acaso alguna) configuración de encaminadores y ningún servidor adicional

RA: Flags M y O

- Los flags M y O de los RA indican cómo deben comportarse los hosts con respecto a la autoconfiguración de los parámetros de red
- M indica como configurar la dirección IP
- O indica cómo configurar otros parámetros: DNS, etc.

Dir. / Otros	M	O	Comentario
SLAAC / SLAAC	0	0	Si dual-stack, se puede usar IPv4 para DNS
SLAAC / DHCPv6	0	1	DHCPv6 Stateless
DHCPv6 / SLAAC	1	0	Si dual-stack, se puede usar IPv4 para DNS
DHCPv6 / DHCPv6	1	1	El gateway se aprende del RA

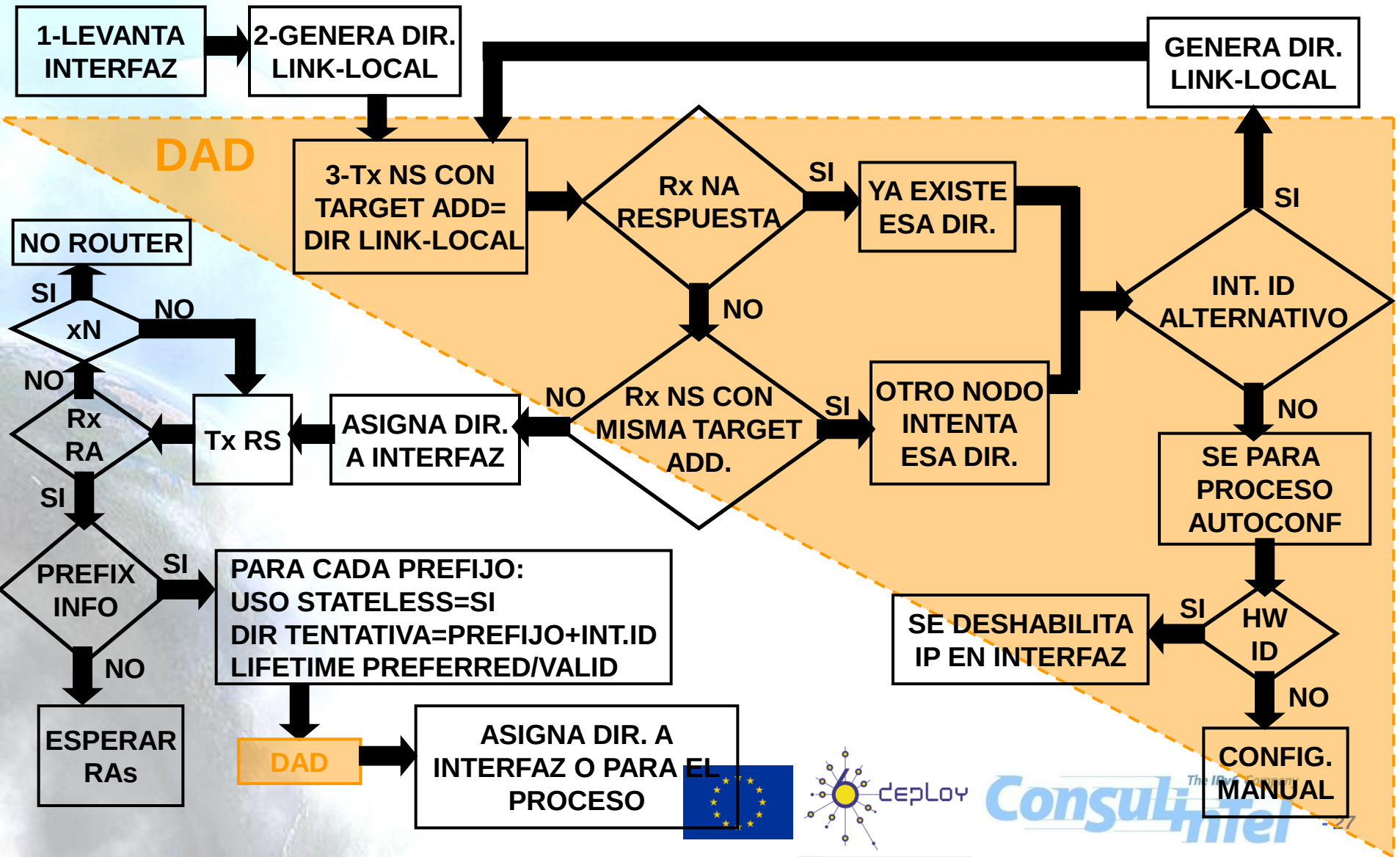
Autoconfiguración Stateless o Serverless (RFC4862)

- 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 (64 bits)
- 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 (64 bits)
- 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

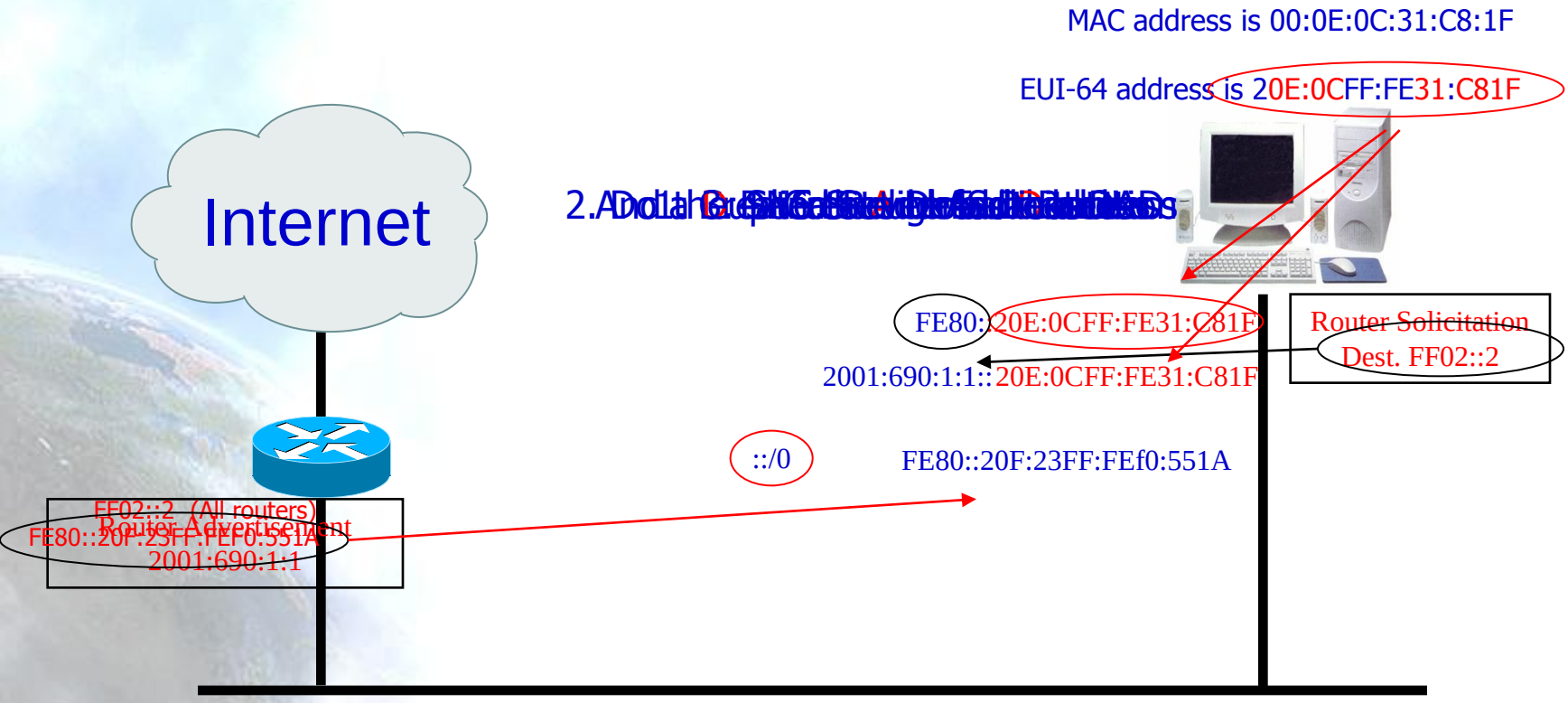
Funcionamiento de la Autoconfiguración Stateless



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

Autoconfiguración Stateless



Configurar el Servidor DNS con Autoconfiguración Stateless (1)

- Hay dos maneras de configurar el servidor DNS en un nodo:
  - Manualmente
  - Con DHCPv6 o DHCPv4 (en caso de nodos dual-stack)
- Puede ser un problema en algunos entornos:
  - Necesidad de usar dos protocolos en IPv6 (Stateless Autoconfguration y DHCPv6)
  - Retardo al obtener el servidor DNS cuando se usa DHCP
  - En entornos wireless, donde el nodo cambia de red frecuentemente, no es posible usar configuración manual o el retardo del DHCP puede ser demasiado
- Una nueva forma de configurar servidores DNS sedefine en el RFC5006, la opción Recursive DNS Server (RDNSS) para los RA
  - Se puede usar conjuntamente con DHCPv6

Configurar el Servidor DNS con Autoconfiguración Stateless (2)

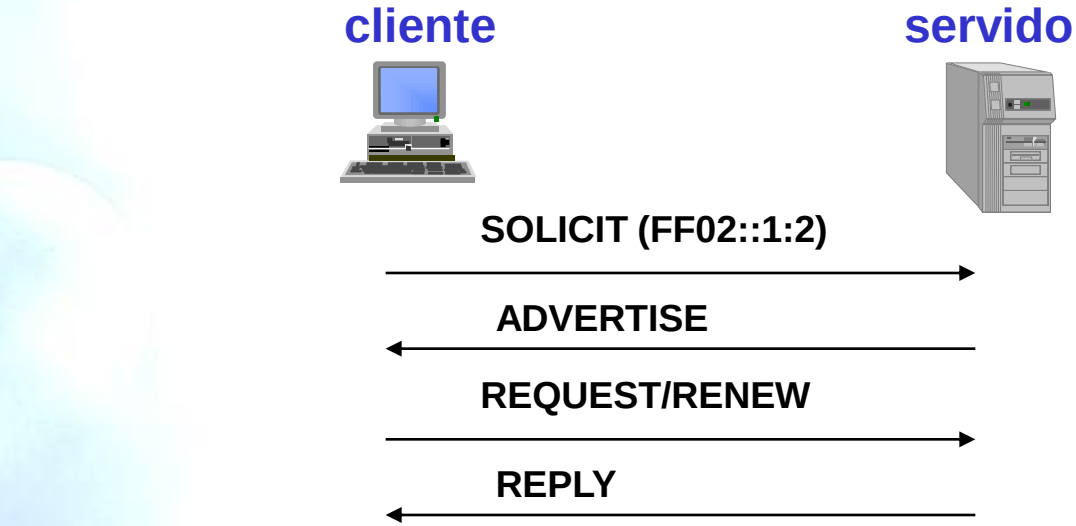
- Funciona de la misma manera en que se aprenden los prefijos y routers usando ND: IPv6 Sateless Address Autoconfiguration [RFC4862]
- Con la opción RDNSS el nodo aprende, con solo un mensaje:
  - Prefjo para usar en la autoconfiguración
  - Gateway IP
  - Servidores DNS Recursivos
- Si, además de la opción RDNSS, se usa DHCPv6, se debe activar el flag “O” en el RA
- Dos opciones para configurar la opción RDNSS en los routers:
  - Manualmente
  - Automaticamente, siendo un cliente DHCPv6

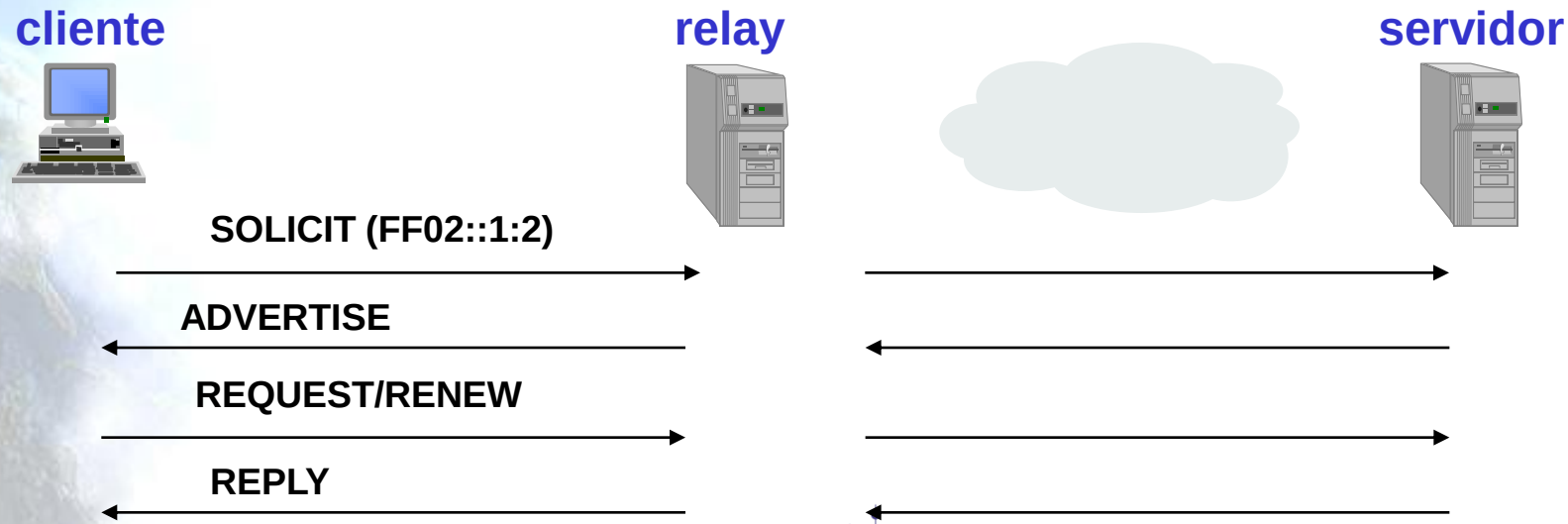
4.4 DHCPv6

DHCPv6

- DHCPv6 [RFC3315] se usa cuando:
  - No hay router
  - Lo indica el RA (ManagedFlag y OtherConfigFlag)
- Modelo cliente servidor sobre UDP, que proporciona al cliente una dirección IPv6 y otros parámetros (Servidor DNS, etc.)
- No proporciona Puerta de enlace (Default Gateway)
- Utiliza direcciones multicast conocidas: All_DHCP_Relay_Agents_and_Servers (FF02::1:2), All_DHCP_Servers (FF05::1:3)
- También hay un DHCPv6 stateless, definido en [RFC3736]

Ejemplo Básico de DHCPv6





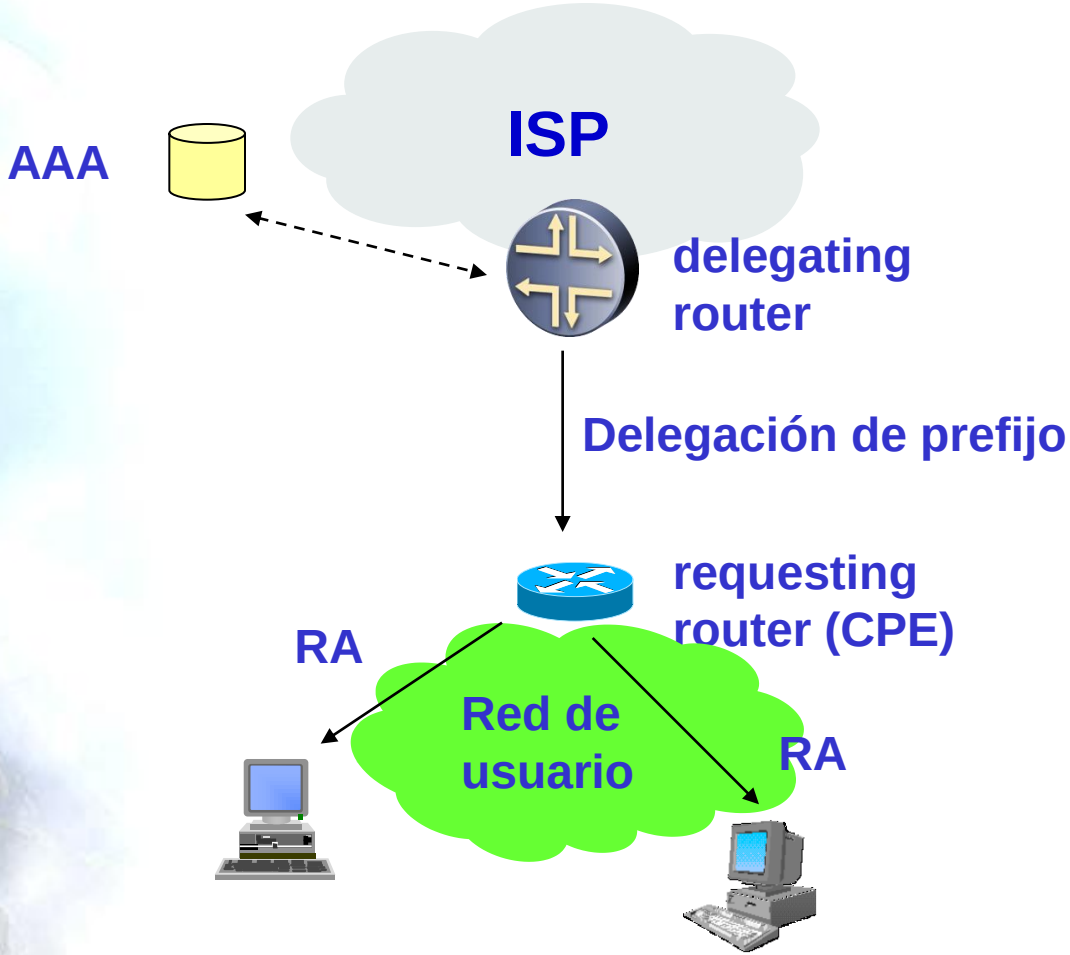
DHCPv6-PD (RFC3633)

- 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

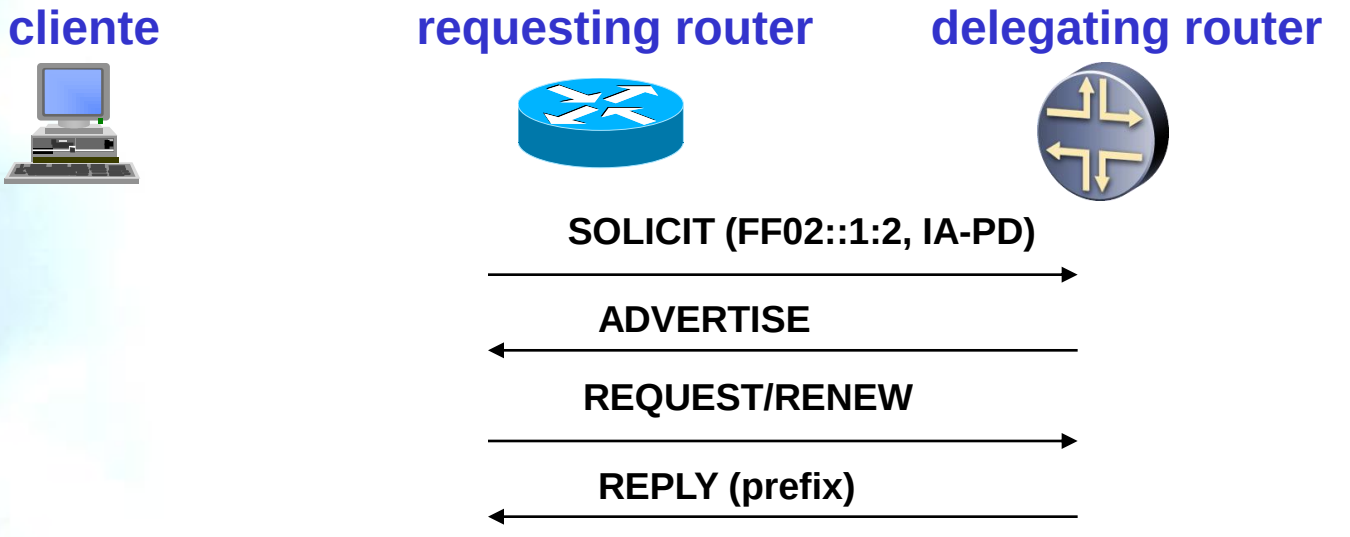
Detalles de DHCPv6-PD

- 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



Gracias !!

Contacto:

- Alvaro Vives (Consulintel): alvaro.vives@consulintel.es