Análisis de Seguridad de "Descubrimiento de Vecinos" (Neighbor Discovery) para IPv6

Fernando Gont

proyecto realizado para

UK Centre for the Protection of National Infrastructure

Cisco Academy Conference

20-21 de Mayo de 2011. Arequipa, Perú

Agenda

- Breve descripción del trabajo realizado para UK CNI
- Introducción al “Descubrimiento de Vecinos” (Neigbor Discovery) en IPv6
- Mecanismo de resolución de direcciones en IPv6
- Ataques contra el mecanismo de resolución de direcciones en IPv6
- IPv6 Stateless Address Auto-Configuration (SLAAC)
- Ataques contra SLAAC
- Evasión de Router Advertisement Guard (RA-Guard)
- Conclusiones
- Preguntas y respuestas

Trabajo actual sobre seguridad IPv6 en UK CPNI

Trabajo actual sobre seguridad IPv6 en CPNI

- El UK CPNI (Centro para la Protección de la Infraestructura Nacional del Reino Unido) está trabajando actualmente en un análisis de seguridad de la suite de protocolos IPv6
- La metodología de trabajo es similar a la utilizada años atras para el caso de TCP e IPv4:
  - Hacer un análisis de seguridad de las especificaciones correspondientes
  - Hacer un análisis de seguridad de implementaciones de los protocolos
  - Producir herramientas de auditoría/prueba de concepto
  - Publicar documentos con recomendaciones
- Actualmente estamos trabajando en conjunto con distintos fabricantes y otras organizaciones

Descubrimiento de Vecinos en IPv6

Descubrimiento de vecinos en IPv6

- Se utiliza principalmente para:
  - Resolución de direcciones
  - Autoconfiguración sin estado (StateLess Address AutoConfiguration)
- Está basado en mensajes ICMPv6
- Provee en IPv6 una funcionalidad análoga a la provista en IPv4 por ARP y DHCPv4

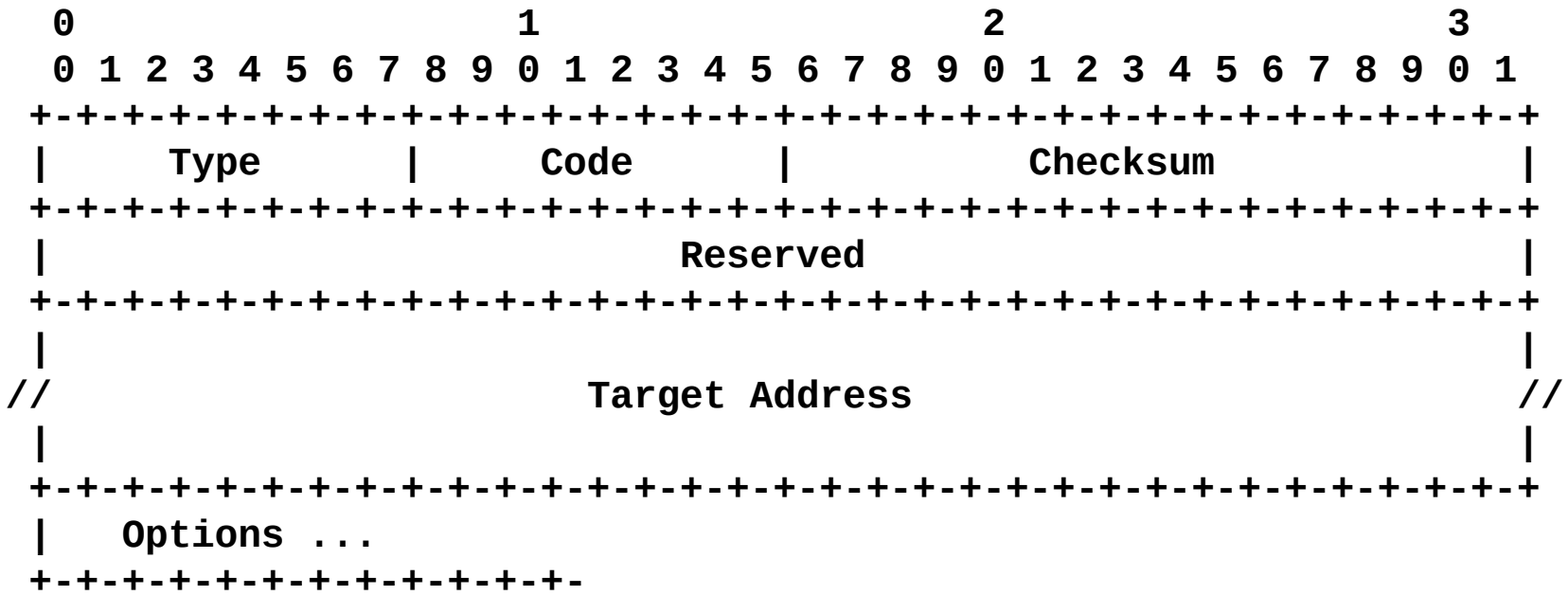
Resolución de Direcciones en IPv6

Resolución de Direcciones en IPv6

- Utiliza mensajes ICMPv6 Neighbor Solicitation y Neighbor Advertisement
- El proceso es simple:
  1. El Host 1 envía un NS: Quien tiene la dirección IPv6 2001:db8::1?
  2. El Host 2 responde con una NA: Yo tengo la dirección 2001:db8::1, y la MAC address correspondiente es 06:09:12:cf:db:55.
  3. El Host 1 “cachea” la informacíón recibida en el “Neighbor Cache” durante un tiempo (esto es una optimización similar al ARP cache)
  4. El Host 1 puede ahora enviarle paquetes al Host 2

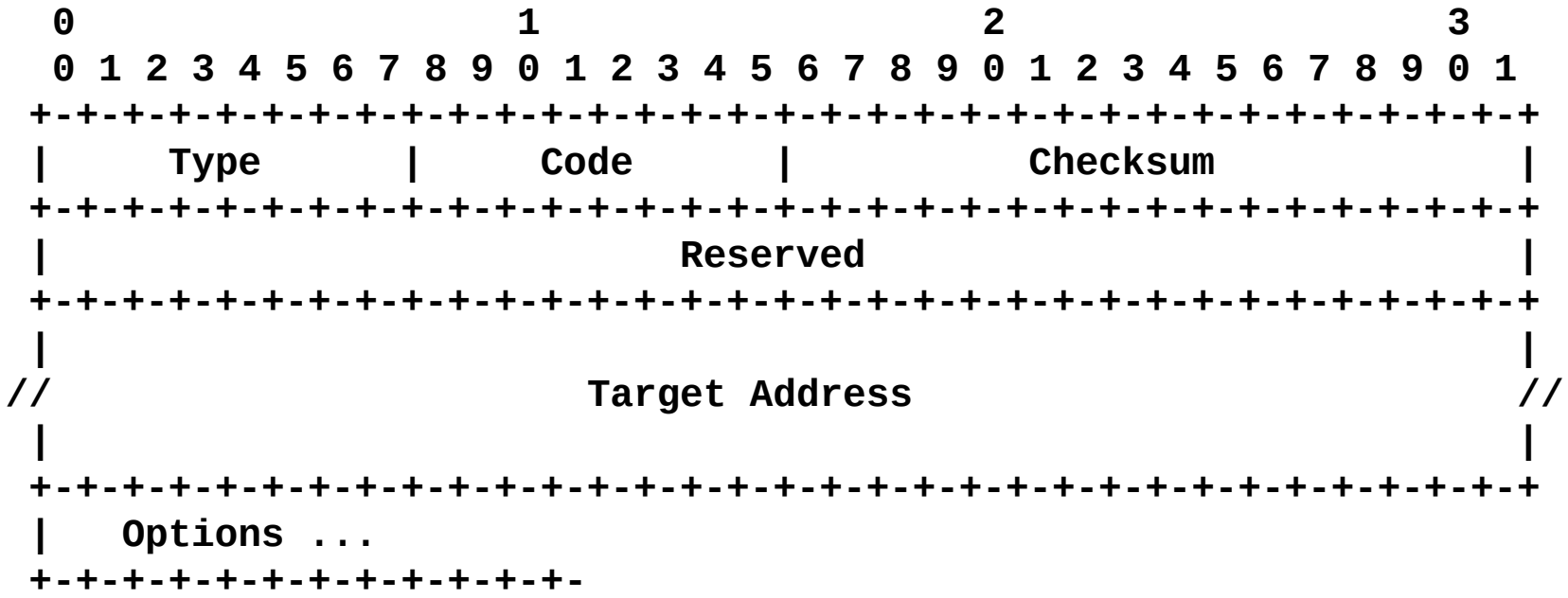
Mensajes Neighbor Solicitation

- Son mensajes ICMPv6 de Tipo 135, Código 0
- Utilizados para solicitar la dirección de capa de enlace correspondiente a una dirección IPv6
- La única opción permitida en ellos es la “Source Link-layer address”



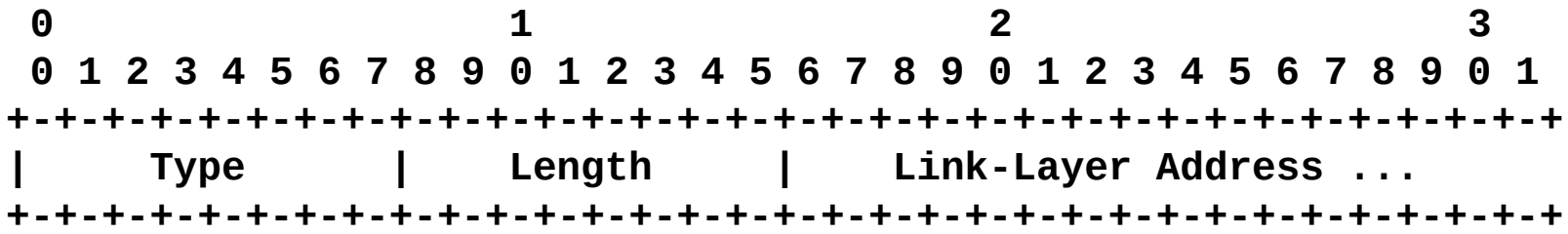
Neighbor Advertisement messages

- Son mensajes ICMPv6 de Tipo 136, Código 0
- Utilizados para informar la dirección de capa de enlace correspondiente a una dirección IPv6
- La única opción permitida en ellos es la "Target Link-layer address"



Opción Source/Target Link-layer address

- La opción Source Link-layer Address contiene la dirección de capa de enlace correspondiente a la dirección origen del paquete IPv6
- La opción Target Link-layer address contiene la dirección de capa de enlace correspondiente a la "Target Address" del mensaje Neighbor Solicitation



Type: 1 para Source Link-layer Address
2 para Target Link-layer Address

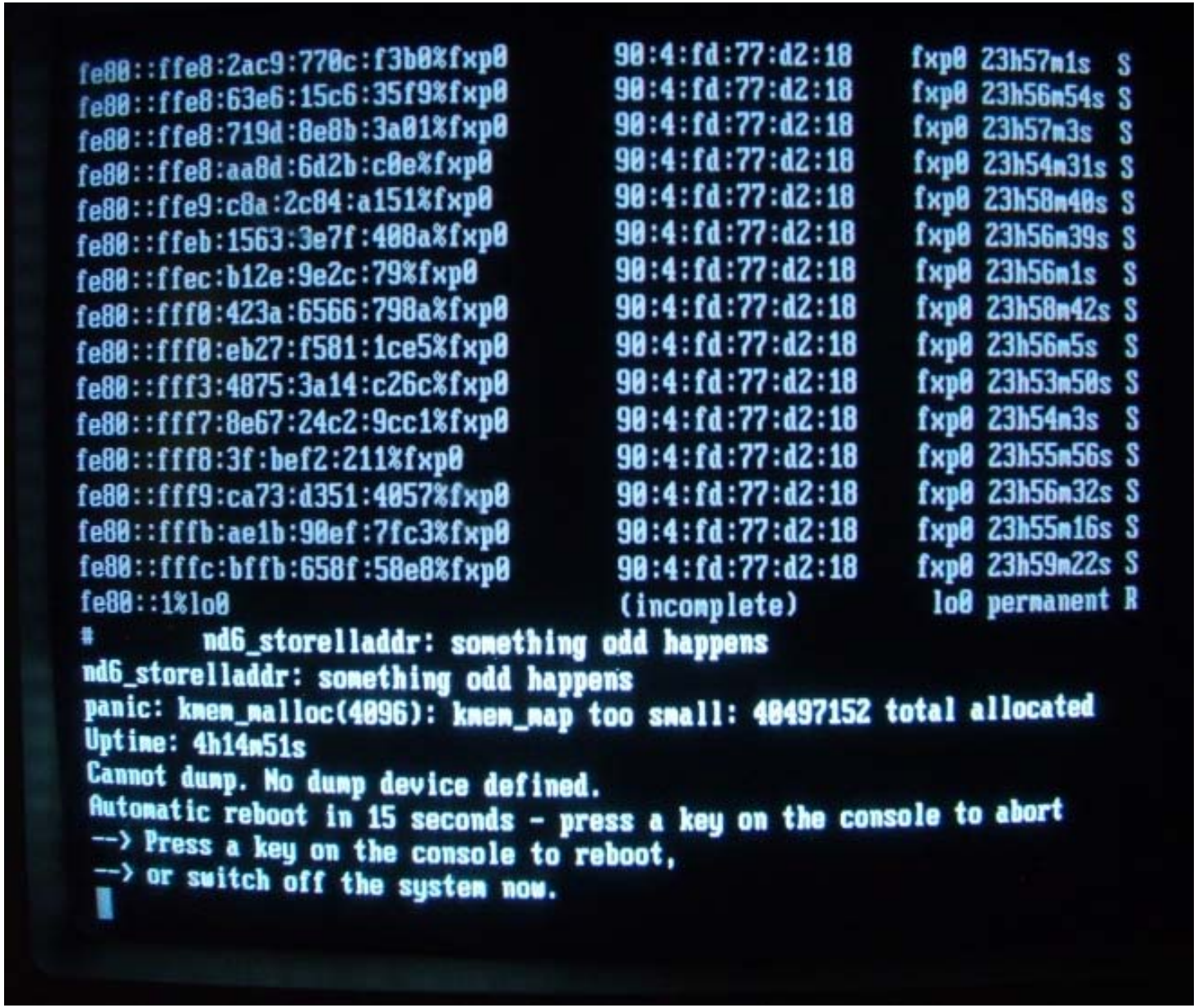
Resolución de Direcciones en IPv6

(un ejemplo de ataque…)

Desbordando el Neighbor Cache

- Algunas implementaciones no imponen límites en el número de entradas máxima que admiten en el Neighbor Cache.
- Ataque:
  - Enviar una gran cantidad de mensajes Neighbor Solicitation que incluyan la opción Source Link-layer address
  - Por cada paquete enviado, al víctima agregará una entrada en el Neighbor Cache
  - Y si se agregan entradas a mayor velocidad de lo que se eliminan las entradas “viejas” del Neighbor Cache....

Desbordando el Neighbor Cache (II)



“Hombre en el Medio” ó Denegación de Servicio

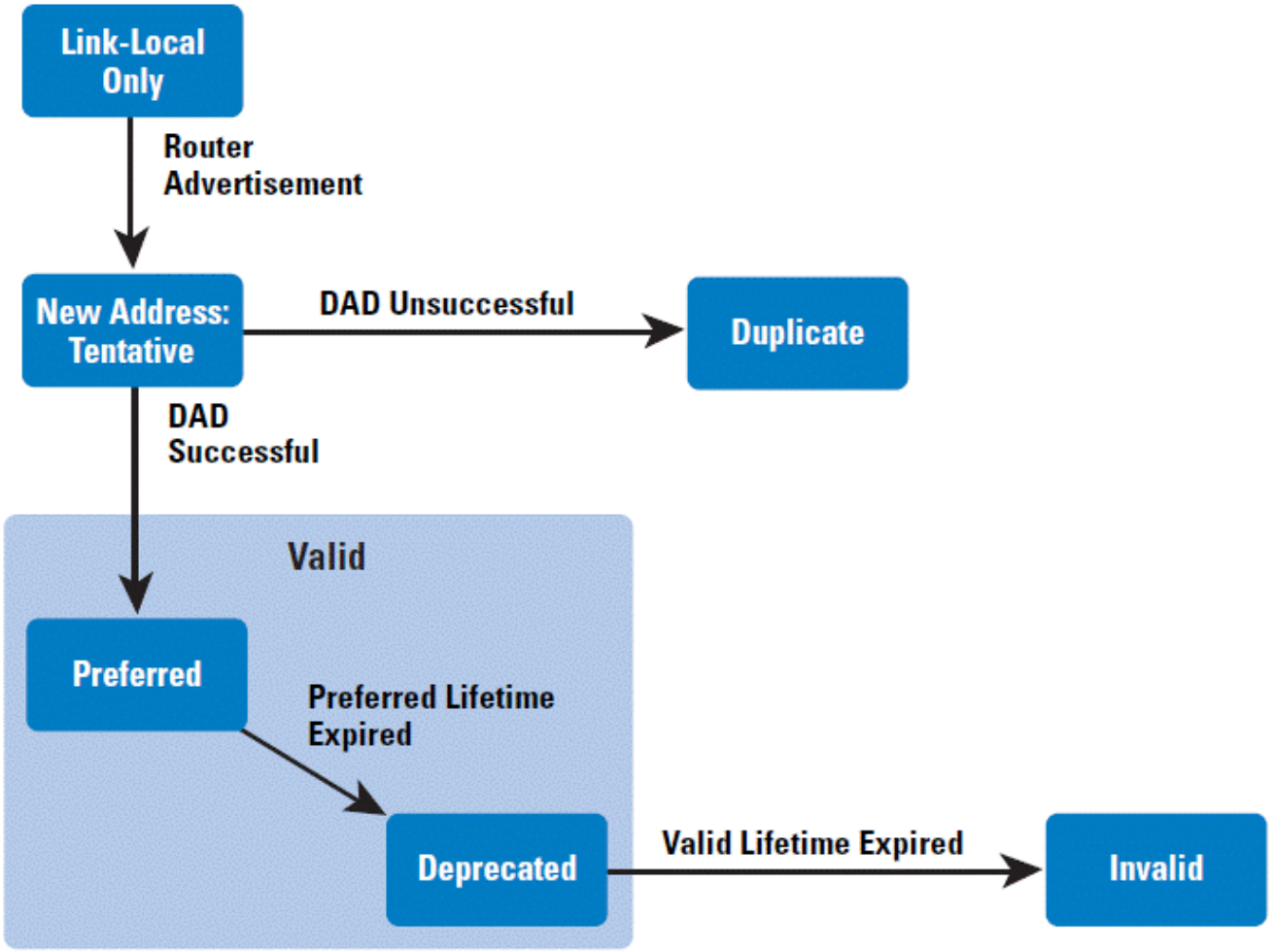
- Sin el uso apropiado de mecanismos de autentificación, resulta trivial para un atacante falsificar mensajes de Descubrimiento de Vecinos
- Ataque:
  - “Escuchar” en la red el envío de mensajes Neighbor Solicitation con una “Target Address” correspondiente a la víctima
  - Al recibir un NS, enviar un Neighbor Advertisement falsificado
- Si la “Target Link-layer address” anunciada no existe, el tráfico termina siendo descartado, y se logra una Denegación de Servicio (DoS)
- Si la “Target Link-layer address” anunciada se corresponde con la del atacante, entonces se puede lograr un ataque de tipo “Hombre en el Medio” (Man In the Middle)

Stateless Address Autoconfiguration en IPv6

Stateless Address Autoconfiguration

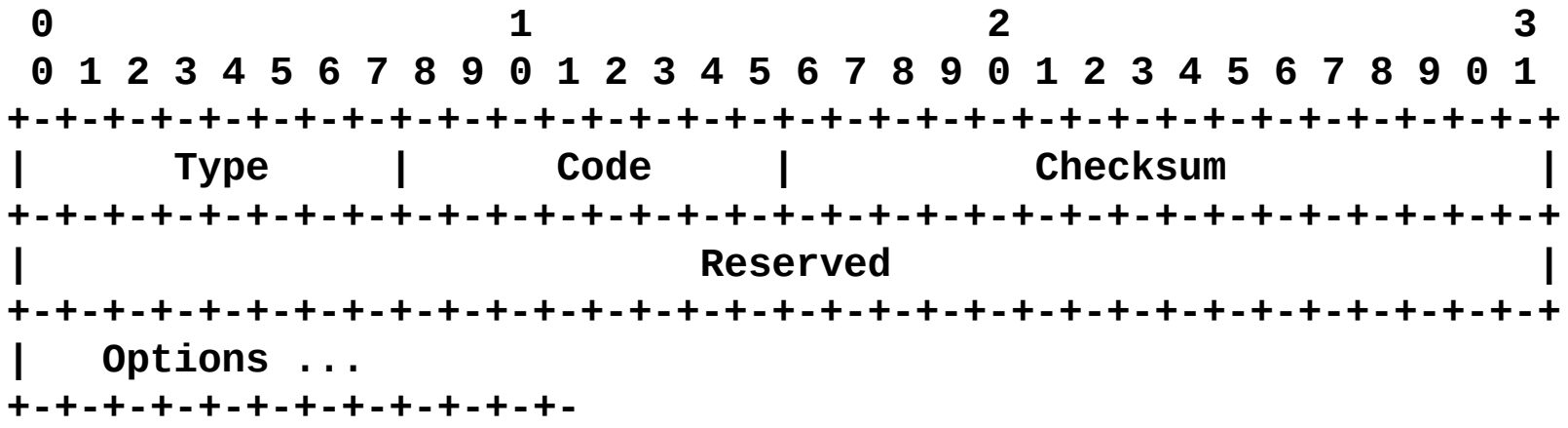
- A grandes rasgos, funciona así:
  1. El host configura una dirección link-local
  2. Chequea que la dirección sea única – es decir, realiza el procedimiento de Detección de Dirección Duplicada (DAD)
     - Enviar un NS, y ver si se obtiene respuesta
  3. El host envía un mensaje Router Solicitation
  4. Al recibir una respuesta, se configura una dirección IPv6 “tentativa”
  5. Chequea que la dirección sea única – es decir, realiza el procedimiento de Detección de Dirección Duplicada (DAD)
     - Enviar un NS, y ver si se obtiene respuesta
  6. Si es única, la dirección “tentativa” se convierte en una dirección valida

Diagrama de flujos de SLAAC



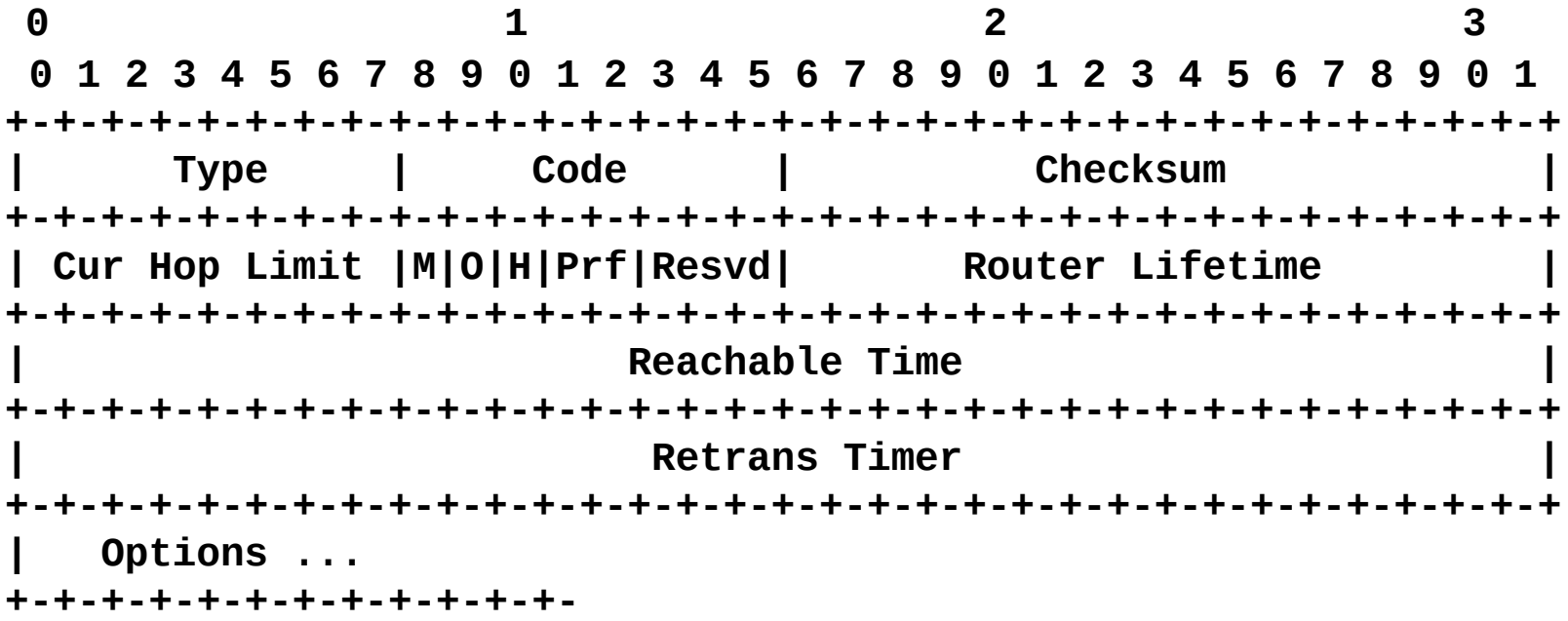
Mensajes Router Solicitation

- Son mensajes ICMPv6 They are ICMPv6 con Tipo 133, Código 0
- Utilizados para solicitar a un router local información de configuración de red
- La única opción actualmente permitida en estos mensajes es la Source Link-layer Address



Mensajes Router Advertisement

- Son mensajes ICMPv6 de Tipo 134, código 0
- Utilizados para anunciar información de configuración de red

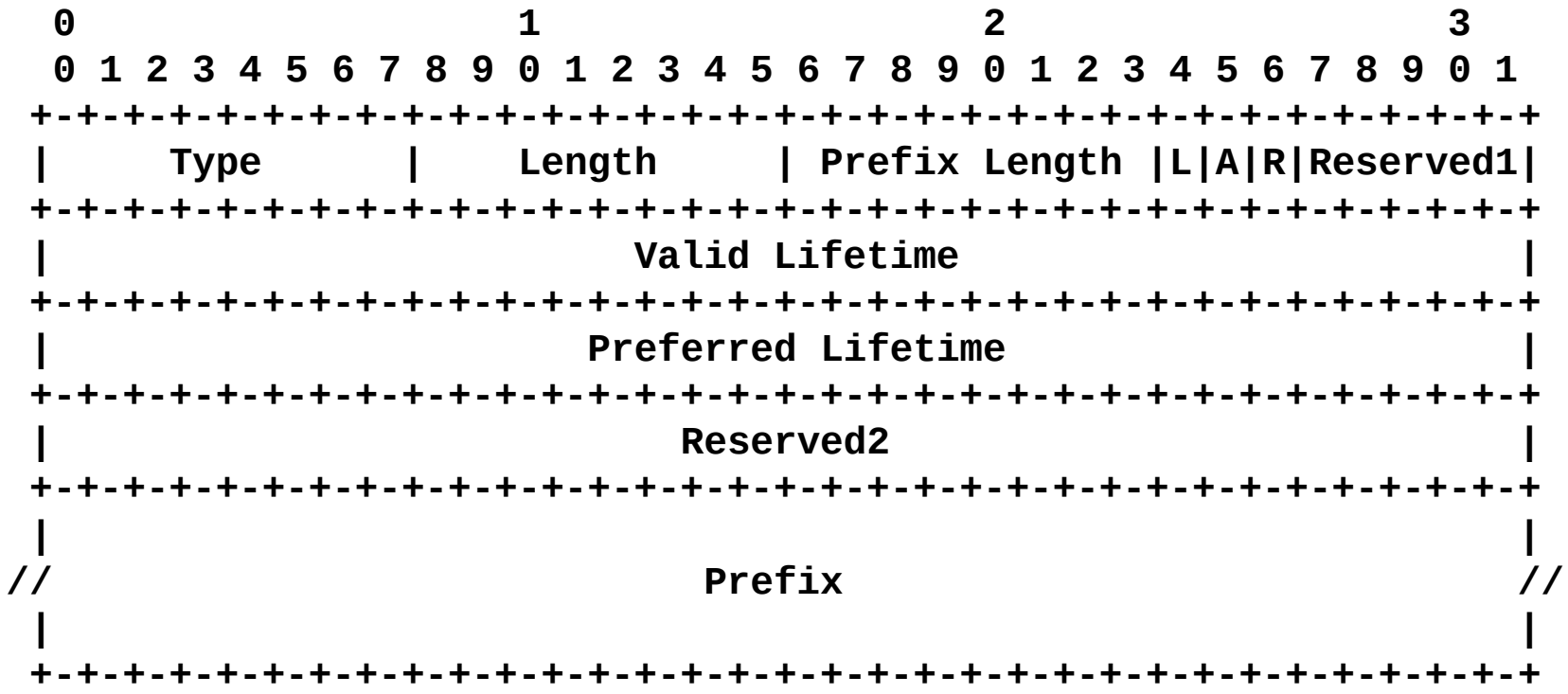


Opciones permitidas en los mensajes RA

- Los mensajes RA pueden contener cualquiera de las siguientes opciones:
  - Source Link-layer address
  - Prefix Information
  - MTU
  - Route Information
  - Recursive DNS Server
- Usualmente, incluyen varias de ellas

Opción Prefix Information

- Utilizada para especificar prefijos “on-link” y prefijos para auto-configuración



SLAAC en IPv6

algunos ataques de ejemplo…

Denegación de Servicio

- Explotar el mecanismo de Detección de Direcciones Duplicadas (DAD)
  - Esperar la recepción de mensajes Neighbor Solicitation que utilicen la dirección IPv6 "no-especificada" (::) como dirección IPv6 Origen.
  - Cuando se recibe tal mensaje, responder con un Neighbor Advertisement
  - Como resultado, se considerará que la dirección "tentativa" no era única, y por ende DAD fallará.

- "Deshabilitar" un router ya existente
  - Falsificar un mensaje Router Advertisement pretendiendo ser el router local, especificando un "Router Lifetime" igual a cero (o a otro valor pequeño)

Router Advertisement Guard (RA-Guard)

SegURIdad PlacebO

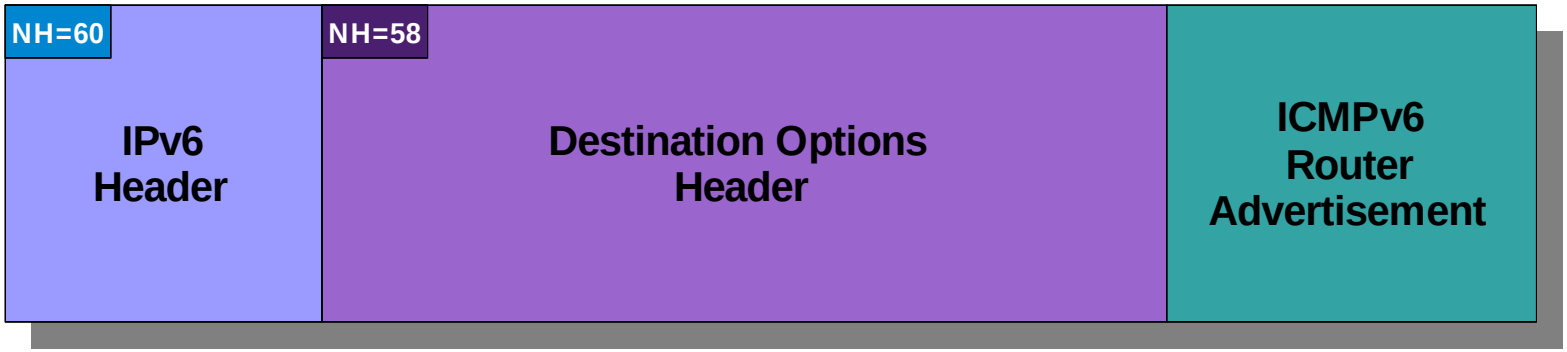
Router Advertisement Guard

- Muchas organizaciones utilizan como “primer linea de defensa” contra ataques de Descubriimiento de Vecinos, el mecanismo conocido como “Router Advertisement Guard”
- RA-Guard funciona, a grandes rasgos, así:
  - Se configura un dispositivo de capa 2 de modo tal que se permitan los mensajes Router Advertisement únicamente si los mismos llegan en un puerto determinado
  - Cualquier mensaje RA recibido en otro puerto, es descartado
- El mecanismo RA-Guard depnde de la capacidad de dicho dispositivo de identificar los mensajes Router Advertisement

Evasión de Router Advertisement Guard

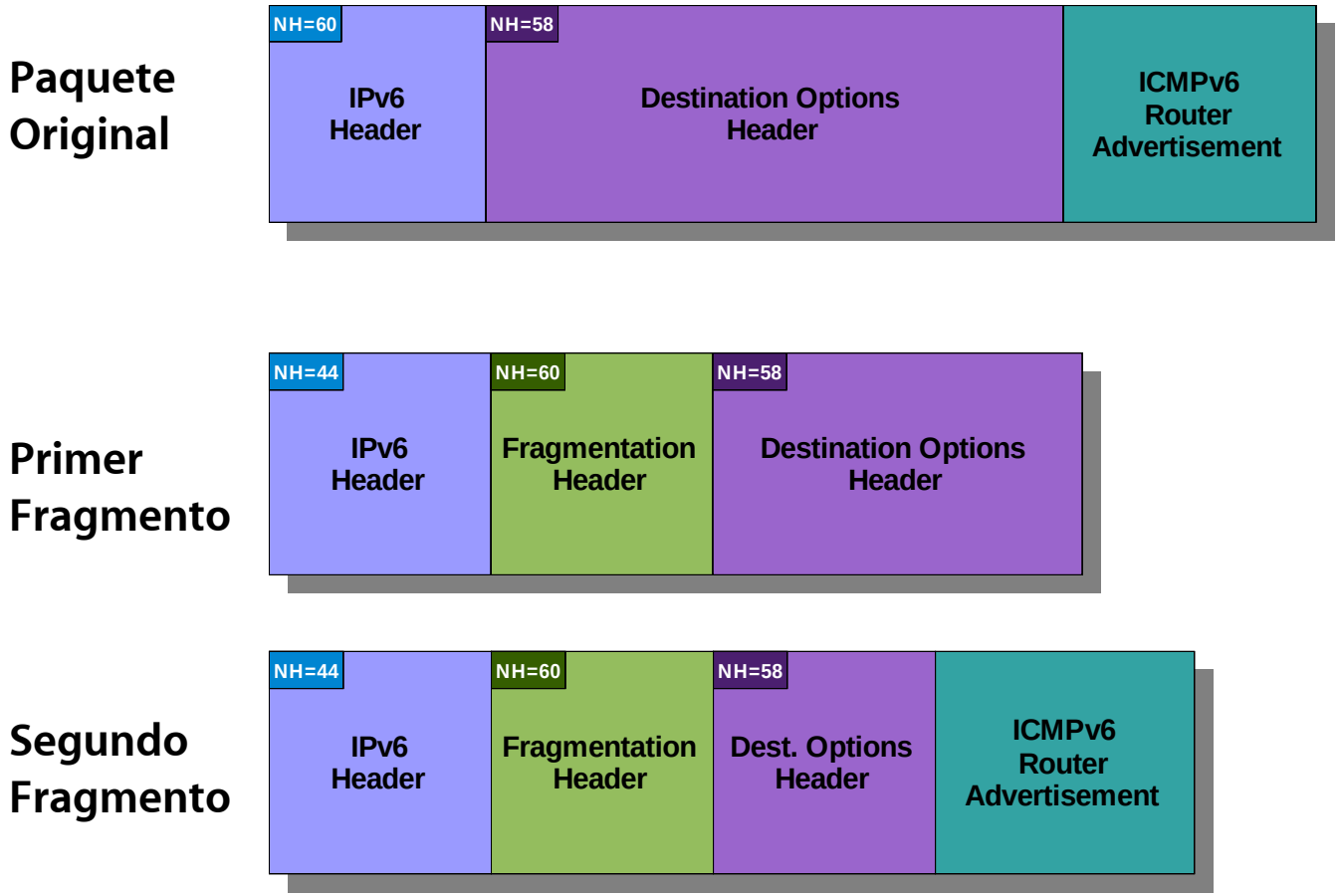
Enunciado del problema

- Las especificaciones de IPv6 permite (y las distintas implementaciones lo soportan) el uso de múltiples encabezados de extensión – inclusive múltiples instancias del mismo tipo de encabezado de extensión.
- Asi, la estructura resultante de los paquetes puede resultar compleja, a tal punto que puede dificultar el filtrado de paquetes.
- Por ejemplo:



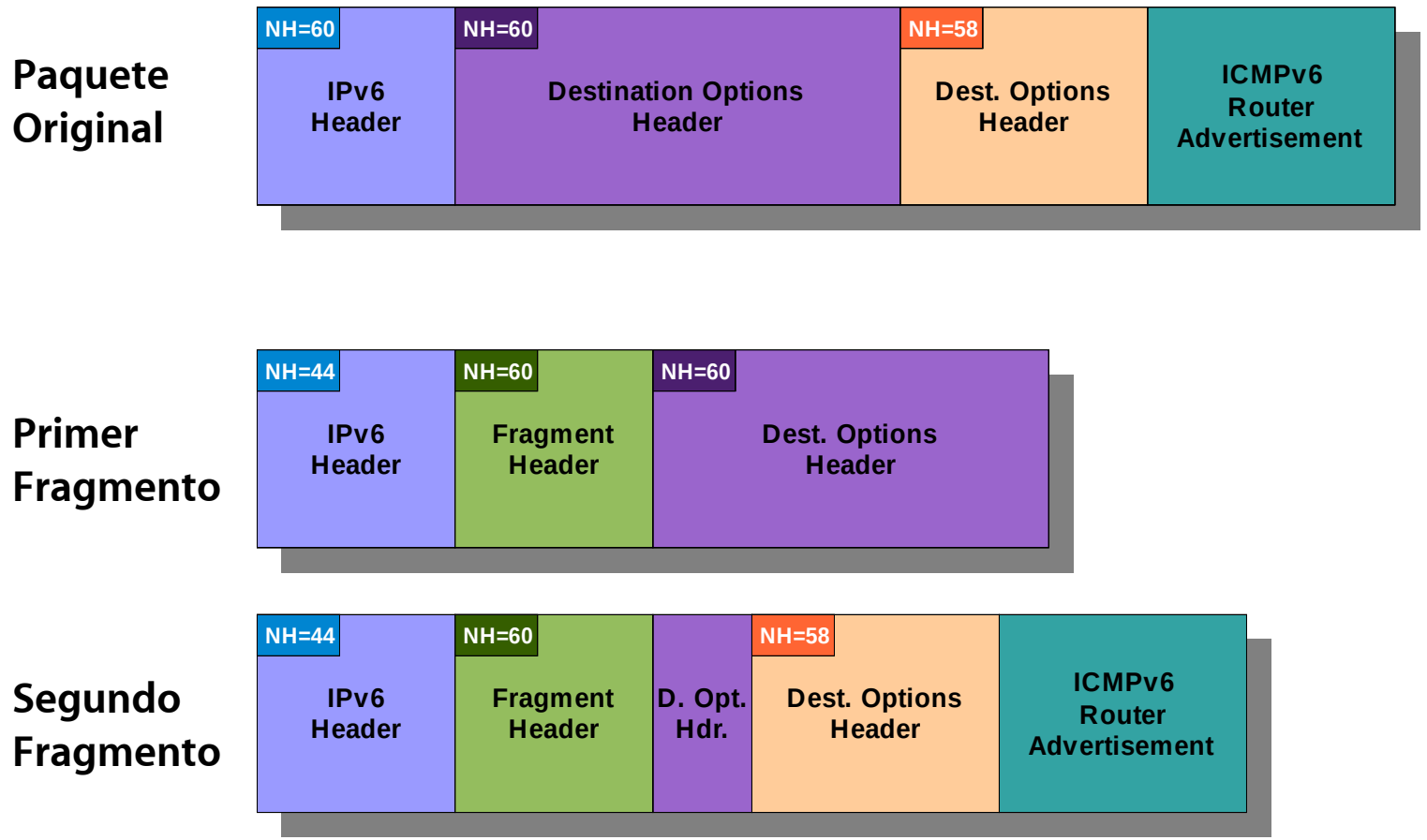
Enunciado del problema (II)

- Combinación de un encabezado de Destination Options header y el uso de fragmentación:



Enunciado del problema (III)

- Otro ejemplo: Dos encabezados de Destination Options, y uso de fragmentación:



Resultados

- Incluso un simple encabezado de “Destination Options” es suficiente apra evadir implementaciones de RA-Guard.
- La combinación de fragmentación con varios encabezados de destindo hace imposible que un dispositivo de capa 2 pueda detectar que un mensaje Router Advertisement está atravesando el dispositivo.

Conclusiones

- Es evidente que llevará un tiempo considerable hasta que la madurez de las implementaciones de IPv6 sea comparable con al de la de las implementaciones de IPv4.
- Es peligroso que las organizaciones desplieguen tecnologías y “mitigaciones” sin un sólido conocimiento de las mismas.

Preguntas?

Agradecimientos

- CNPI, organizadores de este evento, y Uds., los asistentes

Fernando Gont

fernando@gont.com.ar

http://www.gont.com.ar