IPv6 Day

Seguridad

Alejandro Acosta
LACNIC
alejandro @ lacnic dot net

@ITandNetworking

2019

Contenido

- Introducción a Seguridad con IPv6
- Amenazas de Seguridad IPv6
- Firewalling y Switching
- Recomendaciones de Seguridad IPv6

Mitos de Seguridad IPv6

- Primero
  - No olvidar
    - Seguridad es un campo MUY complejo
  - Nos centraremos en IPv6

- Mitos de Seguridad
  - Yo solo uso IPv4, no tengo que preocuparme de IPv6
  - IPv6 es más seguro que IPv4
  - Estoy expuesto: sin NAT ni direcciones privadas
  - IPv6 es algo muy nuevo para ser atacado

IPv6 desde el Punto de Vista de Seguridad

- No es más ni menos seguro que IPv4
- IPsec no es obligatorio (nunca lo fue !)
- End-to-end posible pero no obligatorio
- Menos maduro que IPv4: capacitación, implementaciones, buenas prácticas
- Impacta (potencialmente) a todo lo que lleve IP
- Soporte IPv6 desigual
- Muchas cosas en común con IPv4
- Presenta novedades a tener en cuenta
- No es la causa de todos los males, hay otras capas

Clasificación Amenazas IPv6 (I)

- Tres categorías para amenazas seguridad IPv6:

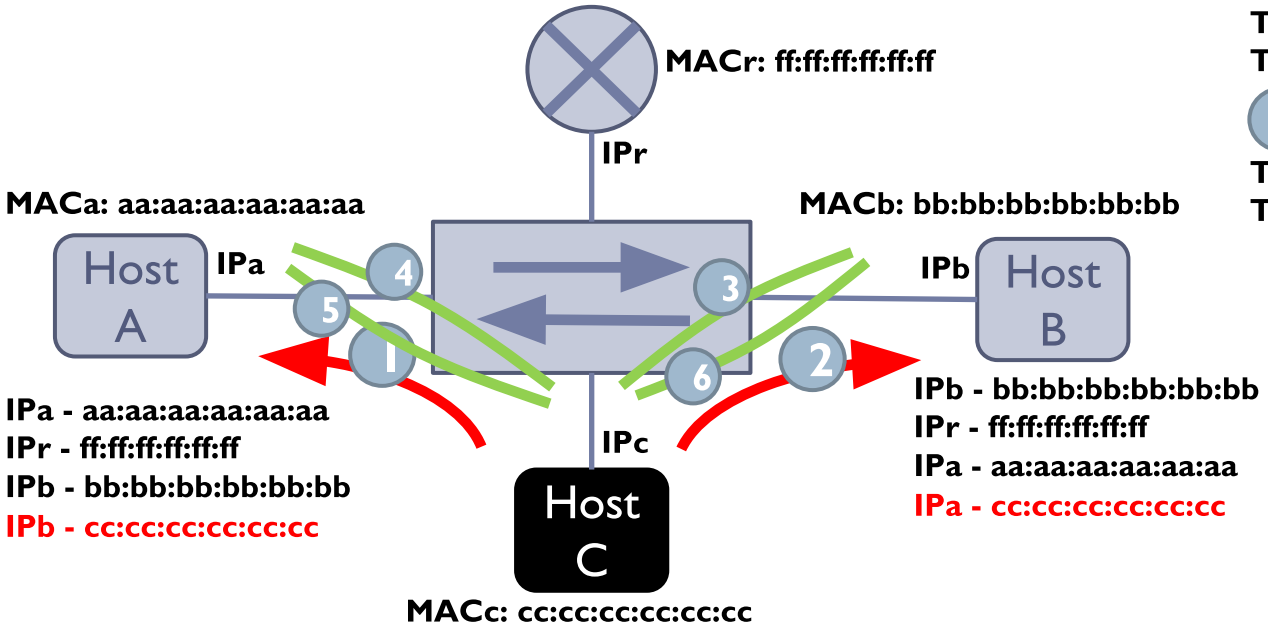
1. Ya existían con IPv4 y se comportan similar con IPv6
   - Ejemplos: sniffing, ataques a otras capas, flooding
2. Ya existían con IPv4 y se comportan distinto con IPv6
   - Ejemplos: escaneo de red, amplificación (smurf)
3. Nuevas amenazas que aparecen con IPv6
   - Ejemplos: amenazas a NDP, Routing Header tipo 0, cabeceras de extensión

Amenazas NDP (I)

- Neighbor Discovery Protocol (NDP) [RFC4861] es vulnerable a diversos ataques [RFC3756][RFC6583]
- La especificación original define el uso de IPsec para proteger los mensajes de ND. Por diversas razones en la práctica esta no es una solución
- SEcure Neighbor Discovery (SEND) [RFC3971] tiene como objetivo proteger ND

Amenazas NDP (II)

- Neighbor Advertisement no solicitado: MITM



1 IPv6 | ICMPv6: NA
Target Addr.: IPb
Target Link-layer Addr.: cc:cc:cc:cc:cc:cc

2 IPv6 | ICMPv6: NA
Target Addr.: IPa
Target Link-layer Addr.: cc:cc:cc:cc:cc:cc

3 IPv6 | Ethernet
Src = IPb
Dst = IPa
Src = MACb
Dst = MACc

4 IPv6 | Ethernet
Src = IPb
Dst = IPa
Src = MACc
Dst = MACa

5 IPv6 | Ethernet
Src = IPc
Dst = IPc
Src = MACa
Dst = MACc

6 IPv6 | Ethernet
Src = IPc
Dst = IPb
Src = MACc
Dst = MACb

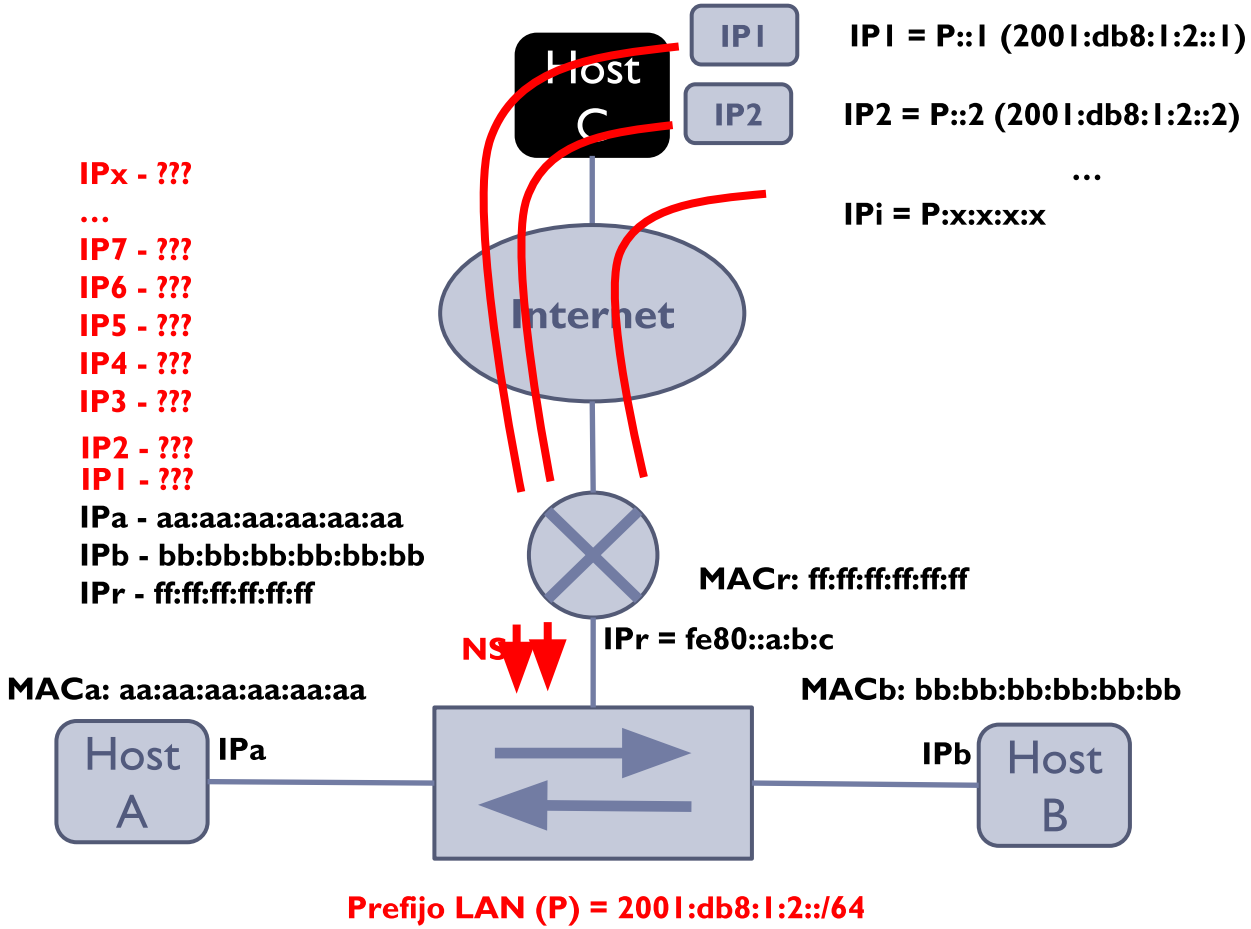
Amenazas NDP (III)

- Ataques usando RAs:

1. Atacante se hace pasar por router (Redir./Dos)
2. Prefijo falso en el enlace (DoS)
3. Prefijo falso para configurar dirección (DoS)
4. Parámetros falseados (DoS)

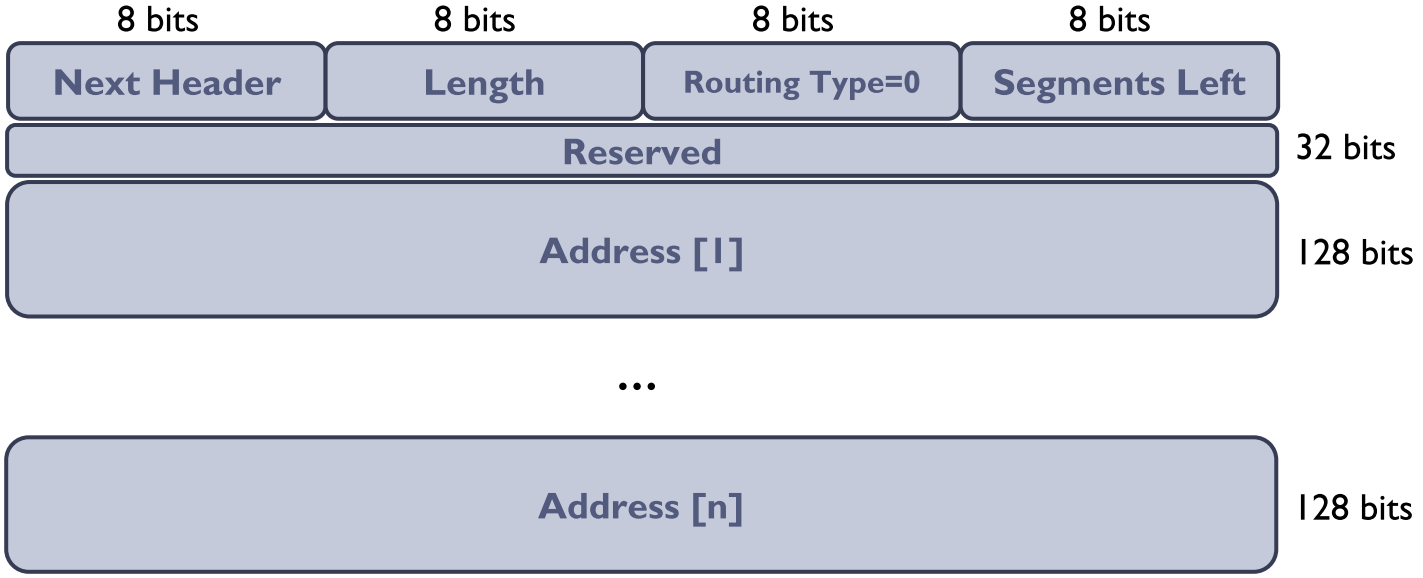
Amenazas NDP (IV)

- Neighbor Cache Exhaustion: DoS

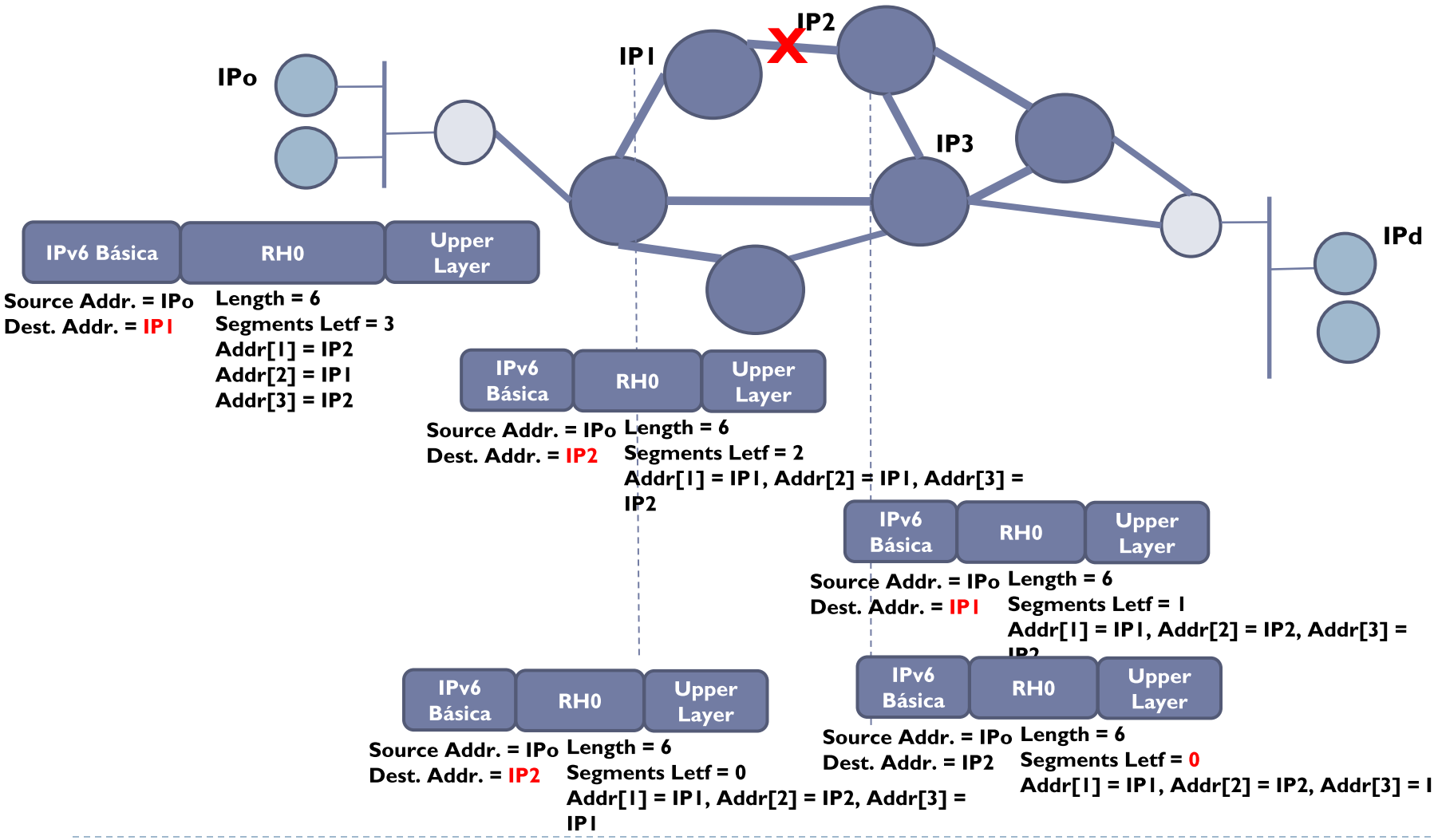


RH0 (I)

- Routing Header (Type 0) puede ser usada para acumular tráfico sobre un camino remoto con el propósito de degradar el tráfico o DoS
- Amenaza grave: Se prohibió su uso [RFC5095]
  - Sólo afecta a EH Routing Type 0.
  - Type 2 usada en MIPv6 [RFC6275], Type 3 usada en RPL [RFC6554] siguen siendo válidas



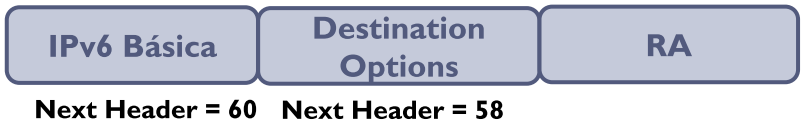
RH0 (II)


IPo
IP1
IP2
IP3
IPd
IPv6 Básica
RH0
Upper Layer
Source Addr. = IPo
Dest. Addr. = IP1
Length = 6
Segments Letf = 3
Addr[1] = IP2
Addr[2] = IP1
Addr[3] = IP2
IPv6 Básica
RH0
Upper Layer
Source Addr. = IPo
Dest. Addr. = IP2
Length = 6
Segments Letf = 2
Addr[1] = IP1, Addr[2] = IP1, Addr[3] = IP2
IPv6 Básica
RH0
Upper Layer
Source Addr. = IPo
Dest. Addr. = IP1
Length = 6
Segments Letf = 1
Addr[1] = IP1, Addr[2] = IP2, Addr[3] =
IPv6 Básica
RH0
Upper Layer
Source Addr. = IPo
Dest. Addr. = IP2
Length = 6
Segments Letf = 0
Addr[1] = IP1, Addr[2] = IP2, Addr[3] = IP1
IPv6 Básica
RH0
Upper Layer
Source Addr. = IPo
Dest. Addr. = IP2
Length = 6
Segments Letf = 0
Addr[1] = IP1, Addr[2] = IP2, Addr[3] = IP1

Cabeceras de Extensión

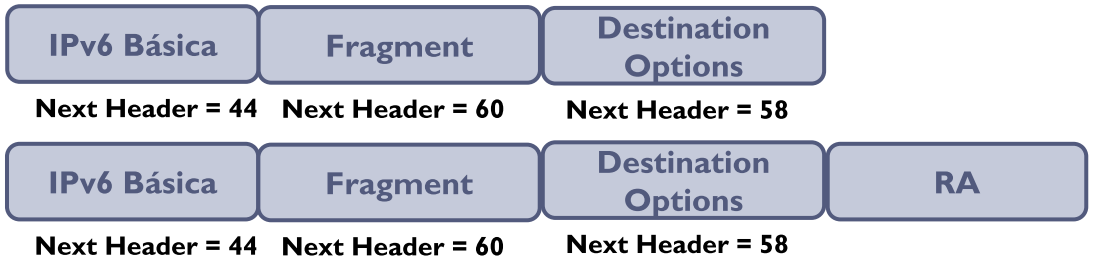
Saltarse medidas de seguridad: RA-Guard

- Usando Cabeceras de extensión



- Si solo mira Next Header = 60 no detecta RA

- Fragmentando



- Si no reensambla no puede saber el tipo de paquete.
- **Puede saber que es RA por Next Header = 58 en ambos fragmentos**
  - **Atentos a evasiones (implementar ACLs)**

- [RFC7113] Recomendaciones implementación para evitarlo o minimizarlo
- [RFC7112] La cadena de cabeceras (Básica + EHs + Upper Layer) deben ir en el primer fragmento

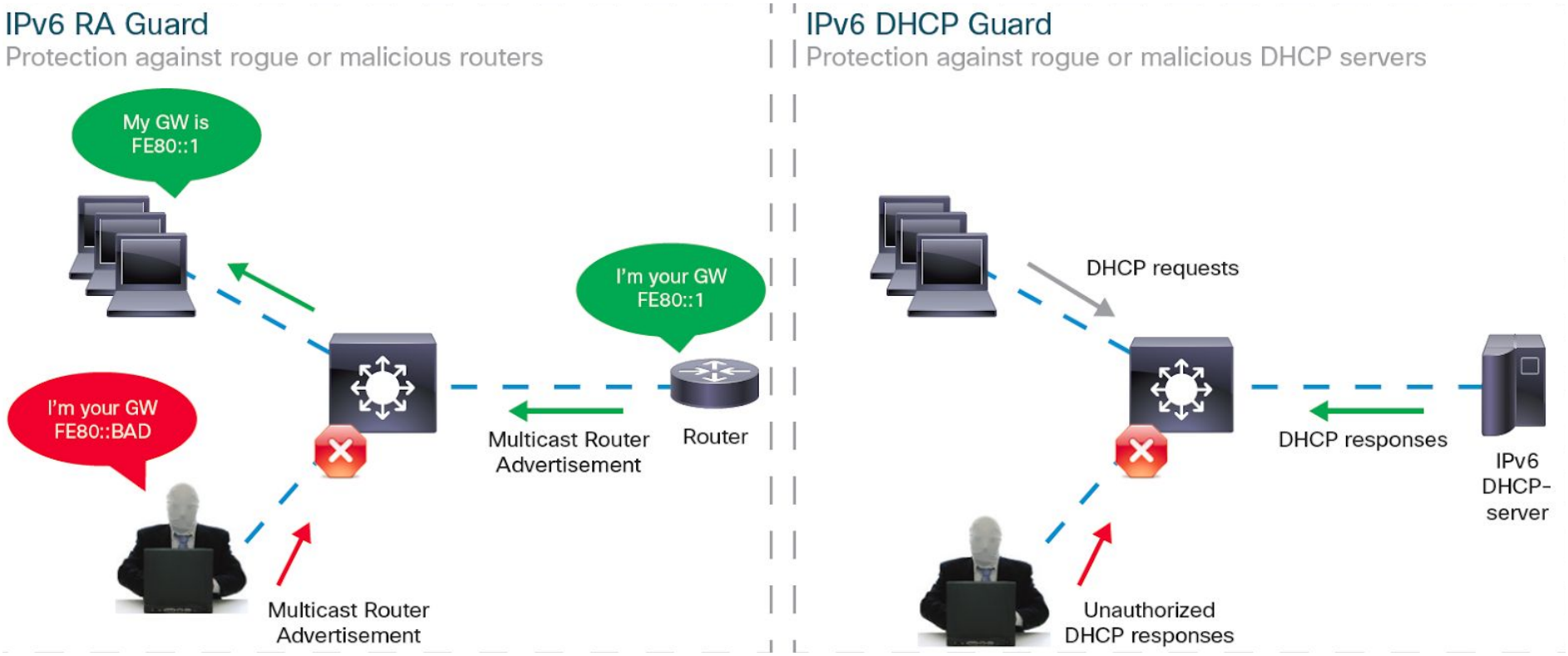
FHS (I)

- FHS (First Hop Security): asegurar y optimizar la operación de los nodos en un enlace
- Existen varias técnicas o herramientas para IPv6:
  - RA-GUARD
  - DHCP Guard
  - IPv6 Snooping (ND inspection + DHCPv6 Snooping)
  - Source/Prefix Guard
  - IPv6 Destination Guard (o ND Resolution rate limiter)
  - MLD Snooping

FHS (II)

- RA-GUARD

DHCPv6 Guard

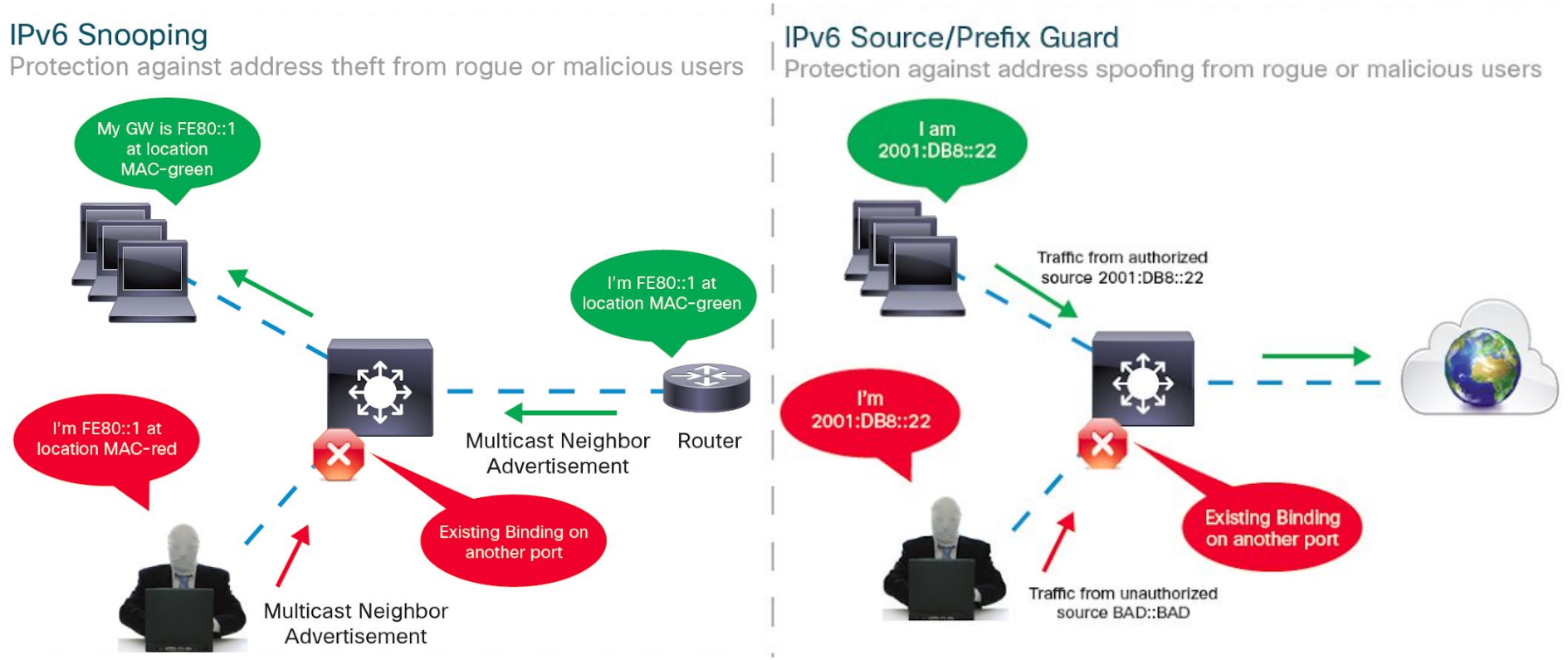


Fuente: http://www.cisco.com/c/en/us/products/ios-nx-os-software/ipv6-first-hop-security-fhs/index.html

FHS (III)

- IPv6 Snooping

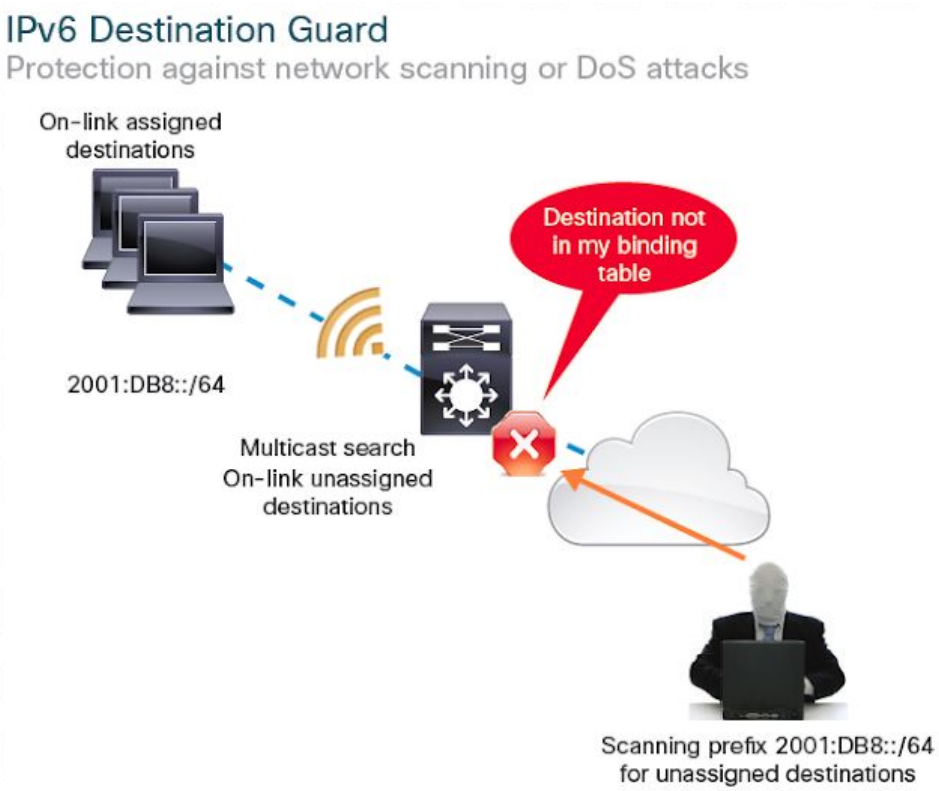
Source/Prefix Guard



Fuente: http://www.cisco.com/c/en/us/products/ios-nx-os-software/ipv6-first-hop-security-fhs/index.html

FHS (IV)

- IPv6 Destination Guard (o ND Resolution rate limiter)



Fuente: http://www.cisco.com/c/en/us/products/ios-nx-os-software/ipv6-first-hop-security-fhs/index.html

JUNE 6th IPv6 Day

lacnic webinars

Firewalling

Introducción a Firewalling con IPv6

- Introducción:
  - En esta oportunidad se mencionan algunos aspectos importantes que no se deben olvidar durante una implementación de IPv6 que contenga *firewalls*.

Firewalling con IPv6

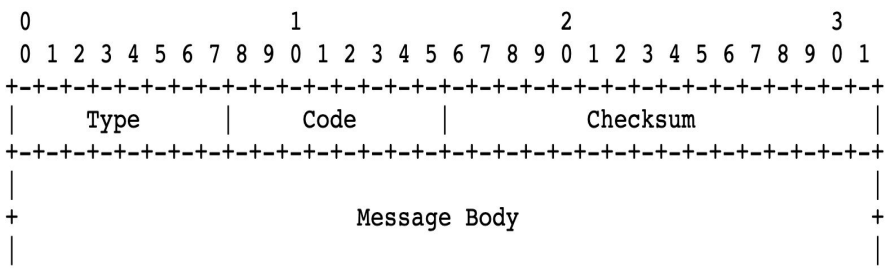
- Tener en cuenta: No se pueden replicar ligeramente las reglas de IPv4 en IPv6
  - Se pueden replicar pero el trabajo no termina aquí !!

Firewalling con IPv6 (II)

- Prestar atención si es un *firewall* de borde o un *firewall* en el mismo equipo. Lo que vayamos a hacer puede ser diferente. Por ejemplo, en un *firewall* sobre el mismo dispositivo se debe permitir RS/RA, NS/NA.
- En los firewalls es muy importante permitir paquetes ICMPv6 Packet Too Big (PTB). *De hecho, al momento de haber un problema de conectividad, los primeros pasos para resolver la situación es estar seguros si el PMTUD funciona correctamente (sin ICMPv6 PTB esto no funcionaría).*
- Probablemente interese bloquear túneles automáticos (por seguridad).

Firewalling – Filtrado de ICMPv6 (i)

- Filtrado ICMPv6 comúnmente permitido (recordar que todas las redes son diferentes)
  - En base a la lámina anterior, importante NO bloquear todo el tráfico ICMPv6. Recordar que ICMPv6 va muy de la mano con IPv6.
  - Probablemente se desee permitir:
    - Destination Unreachable (Type 1, todos los códigos)
    - Time Exceeded (type 3, código 0)
    - Packet Too Big (Type 2)
    - Parameter problems
    - Echo Request
    - Echo Reply



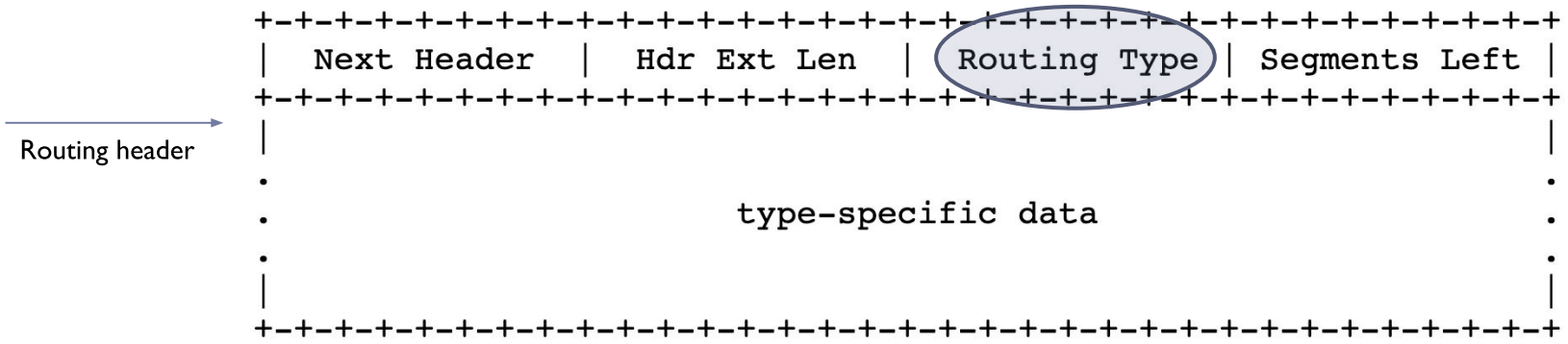
Cabecera ICMPv6

Firewalling – Filtrado de ICMPv6 (ii)

- Filtrado ICMPv6 no tan comúnmente permitido
  - Home Agent Address Discovery Request (Type 144)
  - Home Agent Address Discovery Reply (Type 145)
  - Mobile Prefix Solicitation (Type 146)
  - Mobile Prefix Advertisement (Type 147)

Firewalling – Filtrado de cabeceras

- Filtrado de cabeceras de extensión
  - Una cabecera que muy probablemente se desee filtrar sea RH tipo 0 (Routing Header) – esto a pesar de ya haber sido depreciada en el RFC 5095.
    - No bloquear todo RH0, solo ciertos tiempos de RH0



  - Bloquear RH Tipo 2 (mobilidad).

Firewalling – Filtrado de Tuneles

- Filtrado de túneles automáticos
  - 6to4 (bloquear prefijo 2001::/16)
  - Teredo (bloquear prefijo 2001::/32)

- Filtrado de túneles manuales
  - Bloquear protocolo 41 – IPv6 in IPv4

JUNE 6th
IPv6 Day
lacnic webinars

Switching

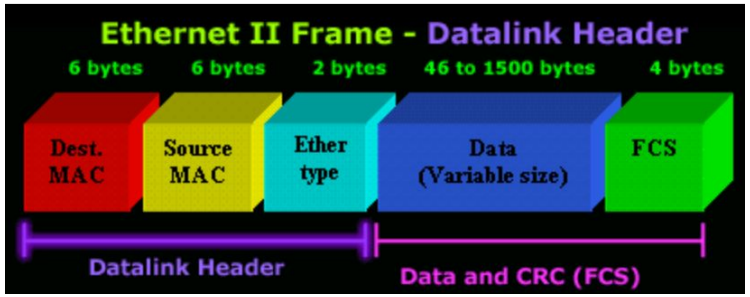
Introducción a Switching e IPv6

- Pensamiento general:
  - *"Los LAN Switches son equipamientos capa 2, no importa que protocolo IP vaya sobre estos."*
  - ¡¡ NO TAN RÁPIDO !!

Switching e IPv6

- Hay que estar seguro que el LAN Switch (y cualquier equipo de capa 2) pueda en realidad "mover" paquetes IPv6.
  - ¿Por qué?
    - Algunos dispositivos capa 2 prestan atención (y pueden descartar) algunos ethertype. No se va a profundizar mucho, pero se repasarán los siguientes ethertypes conocidos:
      - 0x8000 → IPv4
      - 0x0806 → ARP
      - 0x86DD → IPv6
      - 0x8100 → 802.1q

802.3 Ethernet II



¿Qué pasaría si el dispositivo no conmuta paquetes 0x86DD?. Adiós IPv6

Recomendaciones de Seguridad

Soluciones Estandarizadas

- Soluciones de Seguridad IPv6 Estandarizadas
  - Extensiones de Privacidad [RFC4941]
  - IPsec [RFC4301, 4302, 4303, 4307, 7296, 7321]
  - SEND [RFC3971, 3972]
  - RA-GUARD [RFC6104, 6105, 7113]
  - RA-MON
  - DHCPv6-Guard
  - Firewalling

Configuración Direcciones IPv6

- De más a menos nivel de control y seguimiento, métodos de configuración de direcciones:
  - Direcciones estáticas
  - Autoconfiguración con DHCPv6
  - SLAAC: Identificador de interfaz a partir de la dirección MAC
  - SLAAC: Identificador de interfaz utilizando las extensiones de privacidad o aleatorios
- Será normal tener varias direcciones IPv6 un una interfaz
- También deben elegirse direcciones difíciles de "adivinar", ya que los patrones de escaneo han cambiado para IPv6

JUNE 6th IPv6 Day

lacnic webinars

¿Preguntas /Dudas ?

Alejandro Acosta
alejandro at lacnic dot net
@ITandNetworking