Taller sobre Seguridad IPv6

Fernando Gont

Campus Party 2012
San Pablo, Brasil. Febrero 9, 2012

Acerca de...

- He trabajado en análisis de seguridad de protocolos de comunicaciones para:
  - UK NISCC (National Infrastructure Security Co-ordination Centre)
  - UK CPNI (Centre for the Protection of National Infrastructure)
- Actualmente trabajando para SI6 Networks
- Miembro del grupo CEDI (I+D) de UTN/FRH, Argentina
- Participante activo de la Internet Engineering Task Force (IETF)
- Más información en: http://www.gont.com.ar

Agenda

- Motivación de esta presentación
- Breve comparación entre IPv6/IPv4
- Discusión de aspectos de seguridad de IPv6
- Implicancias de seguridad de los mecanismos de transición/co-existencia
- Implicancias de seguridad de IPv6 en redes IPv4
- Areas en las que se necesita más trabajo
- Conclusiones
- Preguntas y respuestas

Motivación de este taller

Pero... que es todo esto de IPv6?

- Diseñado para solucionar el problema de escasez de direcciones
- Todavía no ha sido amplia/globalmente desplegado
- Soportado por la mayoría de sistemas de propósito general
- Los ISPs y otras organizaciones lo han empezado a tomar más en serio a partir de:
  - Agotamiento del pool central de direcciones IPv4 de IANA
  - Actividades de concientización como el “World IPv6 Day”
  - Inminente agotamiento del pool de direcciones de los RIR
- Parece que IPv6 finalmente va a despegar

Motivación de este taller

- Muchos mitos creados en torno a IPv6:
  - La seguridad fue considerada durante el diseño
  - El paradigma de seguridad cambiará a host-centric
  - Aumentará el uso de IPsec
  - etc.
- Estos mitos tienen y han tenido un impacto negativo
- Este taller intentará:
  - Separar “mito” de “realidad”
  - Influenciar como piensas sobre “seguridad IPv6”
  - Realizar algunos ejercicios prácticos sobre seguridad IPv6

Consideraciones generales sobre seguridad IPv6

Algunos aspectos interesantes...

- Menor experiencia con IPv6 que con IPv4
- Implementaciones de IPv6 menos maduras que las de IPv4
- Menor soporte en productos de seguridad para IPv6 que para IPv4
- La red Internet será mucho mas compleja:
  - Dos protocolos de Internet
  - Mayor uso de NATs
  - Mayor uso de túneles
  - Uso de otras tecnologías de transición co-existencia
- Pocos recursos humanos bien capacitados

... así y todo tal vez sea la única opción para permanecer en el negocio

Breve comparación entre IPv6/IPv4

Breve comparación entre IPv6/IPv4

- Muy similares en *funcionalidad*, pero no así en *mecanismos*

	IPv4	IPv6
Direccionamiento	**32 bits**	**128 bits**
Resolución de direcciones	**ARP**	**ICMPv6 NS/NA (+ MLD)**
Auto-configuración	**DHCP & ICMP RS/RA**	**ICMPv6 RS/RA & DHCPv6 (optional) (+ MLD)**
Aislamiento de fallos	**ICMPv4**	**ICMPv6**
Soporte de IPsec	**Opcional**	**Mandatorio (a "opcional")**
Fragmentación	**Tanto en hosts como en routers**	**Sólo en hosts**

Implicancias de seguridad de IPv6

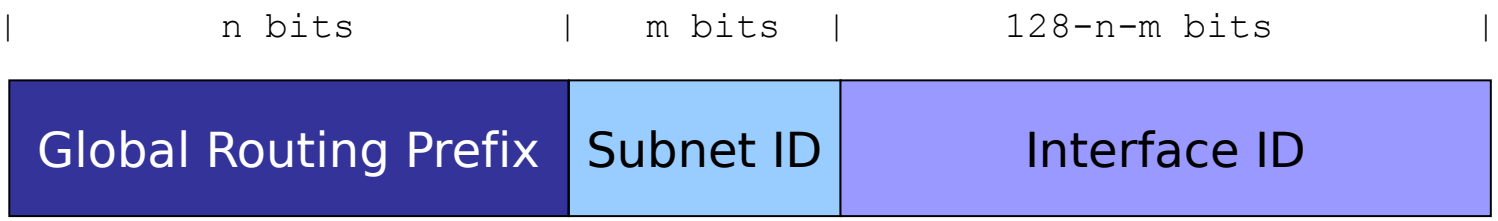
Direccionamiento IPv6
Implicancias en el escaneo de sistemas

SI6 NETWORKS

Breve revisión de direccionamiento IPv6

- El mayor espacio de direcciones es el “motivador” de IPv6
- Se utilizan direcciones de 128 bits
- Semántica muy similar a IPv4:
  - Se agregan direcciones en “prefijos” para el ruteo
  - Existen distintos tipos de direcciones
  - Existen distintos alcances para las direcciones
- Cada interfaz utiliza multiples direcciones, de multiples tipos y alcances:
  - Una dirección link-local unicast
  - Una o mas direcciones global unicast
  - etc.

Direcciones Global Unicast



- El “Interface ID” es en general de 128 bits
- Se puede seleccionar con diferentes criterios:
  - Modified EUI-64 Identifiers
  - Privacy addresses
  - Configurados manualmente
  - De acuerdo a lo especificado por tecnologías de trnasición

Implicancias en escaneo de sistemas

Mito: "*IPv6 hace que los ataques de escaneo de sistemas sean imposibles!*"

- Esto asume que las direcciones IPv6 se generan aleatoriamente
- Malone (*) midió y categorizó las direcciones en:
  - SLAAC (MAC address embebida en el Interface ID)
  - Basadas en IPv4 (2001:db8::192.168.10.1, etc.)
  - "Low byte" (2001:db8::1, 2001:db8::2, etc.)
  - Privacy addresses (Interface ID aleatorio)
  - "Wordy" (2001:db8::dead:beef, etc.)
  - Relacionadas con tecnologias de transición (Teredo, etc.)

(*) Malone, D. 2008. *Observations of IPv6 Addresses*. Passive and Active Measurement Conference (PAM 2008, LNCS 4979), 29–30 April 2008.

Algunos resultados...

- Resultados de [Malone, 2008] (*):

Hosts

Direcciones	Porcentaje
SLAAC	50%
IPv4-based	20%
Teredo	10%
Low-byte	8%
Privacy	6%
Wordy	<1%
Other	<1%

Routers

Direcciones	Porcentaje
Low-byte	70%
IPv4-based	5%
SLAAC	1%
Wordy	<1%
Privacy	<1%
Teredo	<1%
Other	<1%

(*) Malone, D. 2008. *Observations of IPv6 Addresses*. Passive and Active Measurement Conference (PAM 2008, LNCS 4979), 29–30 April 2008.

Algunas conclusiones

- Los ataques de escaneo no son imposibles en IPv6
- Se han econtrado “in the wild”
- Es esperable que no sean de “fuerza bruta”, y aprovechen:
  - Patrones de las direcciones
  - Direcciones multicast, Neighbor discovery, etc. (para ataques locales)
  - “Leaks” de la capa de aplicación
- El **port scanning** no varía
- Recomendaciones:
  - Para servidores, no importa la “predictibilidad” de las direcciones
  - Para clientes, utilizar “privacy addresses”
  - Siempre considerar el uso de firewalls

Ejemplo de scanning por multicast

- All-nodes link-local multicast address
  - ping6 ff02::1%eth0
- All-routers link-local multicast address
  - ping6 ff02::2%eth0

Ej. de leak en protocolo de aplicación

- An e-mail header:

```
X-ClientAddr: 46.21.160.232
Received: from srv01.bbserve.nl (srv01.bbserve.nl [46.21.160.232])
by venus.xmundo.net (8.13.8/8.13.8) with ESMTP id p93Ar0E4003196
for <fernando@gont.com.ar>; Mon, 3 Oct 2011 07:53:01 -0300
Received: from [2001:5c0:1000:a::943]
by srv01.bbserve.nl with esmtpsa (TLSv1:AES256-SHA:256)
(Exim 4.76)
(envelope-from <fgont@si6networks.com>)
id 1RAg8k-0000Qf-Hu; Mon, 03 Oct 2011 12:52:55 +0200
Message-ID: <4E8993FC.30600@si6networks.com>
Date: Mon, 03 Oct 2011 07:52:44 -0300
From: Fernando Gont <fgont@si6networks.com>
Organization: SI6 Networks
User-Agent: Mozilla/5.0 (X11; U; Linux i686; en-US; rv:1.9.2.23)
Gecko/20110922 Thunderbird/3.1.15
MIME-Version: 1.0
To: Fernando Gont <fernando@gont.com.ar>
Subject: Prueba
```

Network Reconnaissance via DNS

- Simplemente peticiona RRs “AAAA” (o “any”)
- Ejemplo:

```
$ dig www.si6networks.com aaaa

; <<>> DiG 9.7.3 <<>> www.si6networks.com aaaa
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 62771
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;www.si6networks.com.     IN   AAAA

;; ANSWER SECTION:
www.si6networks.com.  14400    IN   AAAA2a02:27f8:1025:18::232

;; Query time: 224 msec
;; SERVER: 10.239.1.1#53(10.239.1.1)
;; WHEN: Thu Feb  9 08:31:46 2012
;; MSG SIZE  rcvd: 65
```

Ejemplo de IPv6 port scanning

- Se puede realizar con nmap, mediante:

```
# nmap -6 -p1-10000 -n 2000:db8::1

80/tcp open http
135/tcp open msrpc
445/tcp open microsoft-ds
554/tcp open rtsp
1025/tcp open NFS-or-IIS
1026/tcp open LSA-or-nterm
1027/tcp open IIS
1030/tcp open iad1
1032/tcp open iad3
1034/tcp open unknown
1035/tcp open unknown
1036/tcp open unknown
1755/tcp open wms
9464/tcp open unknown
```

Conectividad Extremo a Extremo

Breve reseña

- La red Internet se basó en el principio de “extremo a extremo”
  - Red tonta, extremos (hosts) inteligentes
  - La comuncación es posible entre cualquier par de nodos
  - La red no examina el contenido de los paquetes IP
- Se suele argumentar que este principio permite la innovación
- Los NATs lo han eliminado de Internet
- Se espera que con IPv6 no existan NATs, y se retorne al principio “extremo a extremo”

IPv6 y el principio “extremo a extremo”

Mito: “*IPv6 devolverá a Internet el principio 'extremo a extremo*'”

- Se asume que el gran espacio de direcciones devolverá este principio
- Sin embargo,
  - Las direcciones globales no garantizan conectividad extremo a extremo
  - La mayoría de las redes no tiene interés en “innovar”
  - Los usuarios esperan en IPv6 los mismos servicios que en IPv4
  - Este principio aumenta la exposición de los sistemas
- En resumen,
  - La conectividad extremo a extremo no necesariamiente es deseable
  - La subred típica IPv6 solo permitirá “trafico saliente” (mediante firewalls)

Resolución de direcciones

Breve reseña

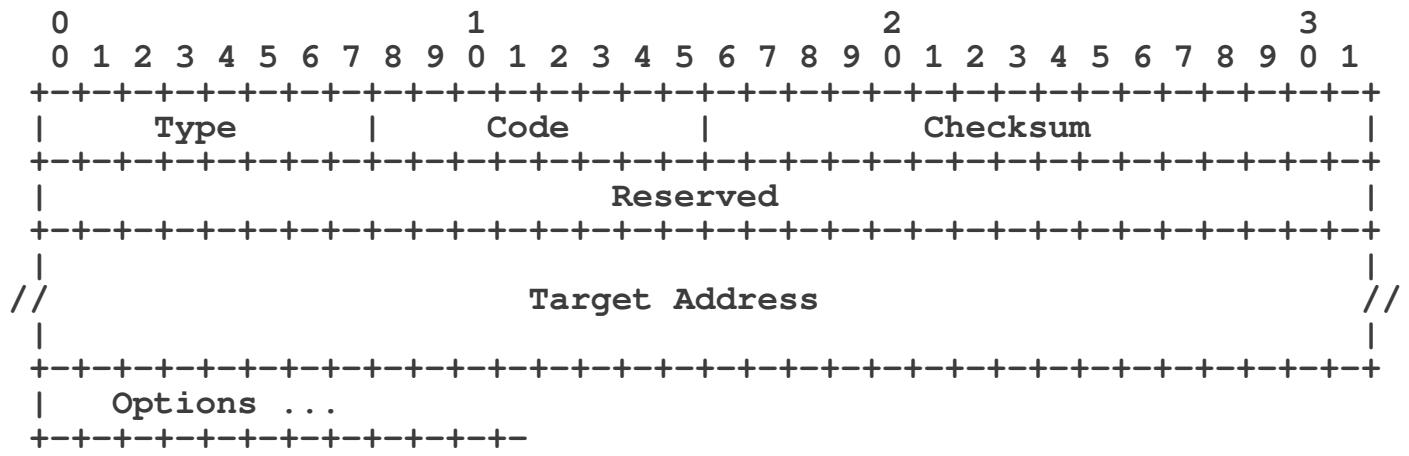
- Resolución de direcciones: IPv6 → capa de enlace
- Realizada en IPv6 por “Neighbor Discovery”:
  - Basado en mesajes ICMPv6 (Neighbor Solicitation y Neighbor Advertisement)
  - Análogo a ARP Request y ARP Reply
  - Implementado sobre IPv6, y **no** sobre la capa de enlace

Operación de Neighbor Discovery

- A grandes rasgos:
  1. El Host 1 envía un NS: “Quién 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

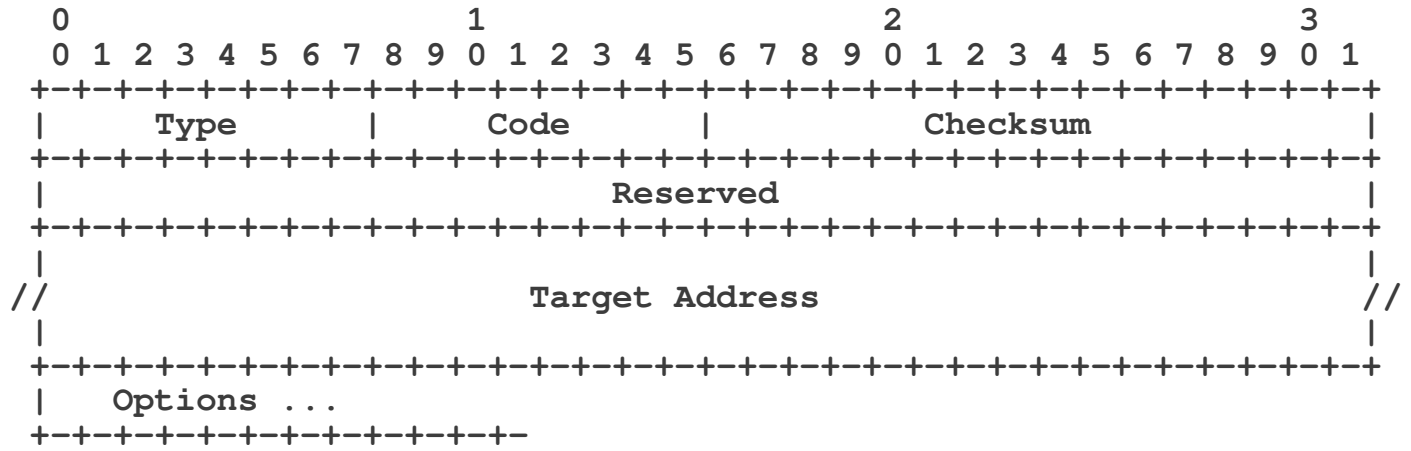
Mensajes Neighbor Solicitation

- Mensajes ICMPv6 de tipo 135, código 0
- Utilizados para solicitar una dirección de capa de enlace
- La única opción permitida es la “Source Link Layer Address”



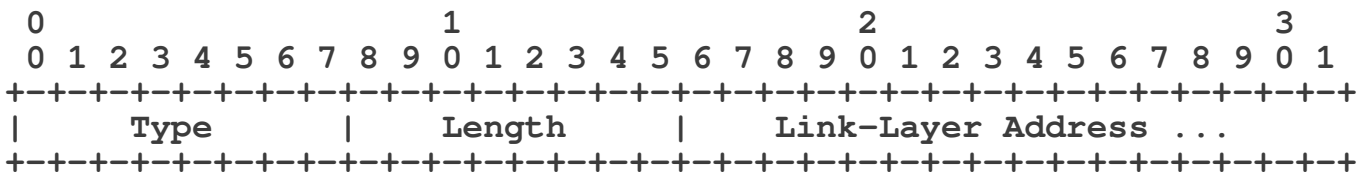
Mensajes Neighbor Advertisement

- Mensajes ICMPv6 de tipo 136, código 0
- Utilizados para informar una dirección de capa de enlace
- La única opción permitida es la “Target Link Layer Address”



Opción Source/Target link-layer address

- SLLA: dirección link-layer de quien envía el paquete
- TLLA: dirección dirección link-layer de la petición



Type:

1: Source Link Layer Address

2: Target Link Layer Address

Neighbor Cache

- Almacena la información de mapeo IPv6 → link-layer
- Cada entrada tiene distintos posibles estados:

NC state	Semantics
INCOMPLETE	Resolución en curso
REACHABLE	Vecino Alcanzable
STALE	Entrada demasiado antigua
DELAY	Se está demorando una prueba
PROBE	Probando el destino

Ejemplo de tráfico Neighbor Discovery

```
% ping6 2004::1

12:12:42.086657 2004::20c:29ff:fe49:ebdd > ff02::1:ff00:1: icmp6: neighbor sol:
who has 2004::1(src lladdr: 00:0c:29:49:eb:dd) (len 32, hlim 255)

12:12:42.087654 2004::1 > 2004::20c:29ff:fe49:ebdd: icmp6: neighbor adv: tgt is
2004::1(SO)(tgt lladdr: 00:0c:29:c0:97:ae) (len 32, hlim 255)

12:12:42.089147 2004::20c:29ff:fe49:ebdd > 2004::1: icmp6: echo request (len
16, hlim 64)

12:12:42.089415 2004::1 > 2004::20c:29ff:fe49:ebdd: icmp6: echo reply (len 16,
hlim 64)
```

ndisc6: Herramienta de Diagnóstico

- Puede enviar NS sobre una dirección en particular
- Ejemplo:

```
$ ndisc6 fc00:1::1 vboxnet0
Soliciting fc00:1::1 (fc00:1::1) on vboxnet0...
Target link-layer address: 08:00:27:F9:73:04
from fe80::a00:27ff:fef9:7304
```

Neighbor Cache (contenido en *BSD)

```
% ndp -a

Neighbor                        Linklayer Address  Netif Expire    S Flags
2004:1::f8dd:347d:8fd8:1d2c     0:c:29:49:eb:e7      em1 permanent R
fe80::20c:29ff:fec0:97b8%em1    0:c:29:c0:97:b8      em1 23h48m16s S R
2004:1::20c:29ff:fe49:ebe7      0:c:29:49:eb:e7      em1 permanent R
fe80::20c:29ff:fe49:ebe7%em1    0:c:29:49:eb:e7      em1 permanent R
2004::1                         0:c:29:c0:97:ae      em0 23h49m27s S R
2004::20c:29ff:fe49:ebdd        0:c:29:49:eb:dd      em0 permanent R
fe80::20c:29ff:fe49:ebdd%em0    0:c:29:49:eb:dd      em0 permanent R
fe80::20c:29ff:fec0:97ae%em0    0:c:29:c0:97:ae      em0 23h48m16s S R
2004::d13e:2428:bae7:5605       0:c:29:49:eb:dd      em0 permanent R
```

Neighbor Cache (contenido en Linux)

```
$ ip -6 neigh show
fe80::a00:27ff:fef9:7304 dev vboxnet0 lladdr 08:00:27:f9:73:04 router STALE
2000::4000 dev vboxnet0 lladdr 11:22:33:44:55:66 PERMANENT
2000:1::1 dev vboxnet0 lladdr 08:00:27:f9:73:04 router REACHABLE
fe80::fc8d:15ed:7f43:68ea dev wlan0 lladdr 00:21:5c:0b:5d:61 router STALE
```

Neighbor Discovery
Algunos ataques...

Vulnerabilidades

- Se pueden portar los ataques “ARP” de IPv4 a IPv6
  - Man in The Middle
  - Denial of Service
- Ataque:
  1. Esperar mensajes NS que “pregunten” por la víctima
  2. Responder con mensajes NA falsificados

Realizando el ataque

- Ejecutar la herramienta na como:

  # na -i IFACE -W VICTIMADDR -E MACADDR -c -o -L

- La víctima enviará ahora sus paquetes a la dirección falsificada
- Puede verificarse mediante tcpdump:

  # tcpdump -i em0 -e -vv ip6

Sniffeando en una red conmutada

- En las redes conmutadas se dificulta el sniffing
- Un truco elegante: mapear la dirección de la víctima a:
  - Dirección Ethernet boradcast (ff:ff:ff:ff:ff:ff)
  - Direcciones Ethernet multicast (por ej., 33:33:00:00:00:01)
- Los paquetes serán enviados a varios sistemas
- Tanto la víctima como el atacante los recibirán

Neighbor Discovery
Posibles contramedidas...

Posibles contramedidas

- Posibles contramedidas:
  - Desplegar SeND
  - Monitorear tráfico de Neighbor Discovery
  - Utilizar entradas estáticas en el Neighbor Cache
  - Restringir el acceso a al red local

SEND (SEcure Neighbor Discovery)

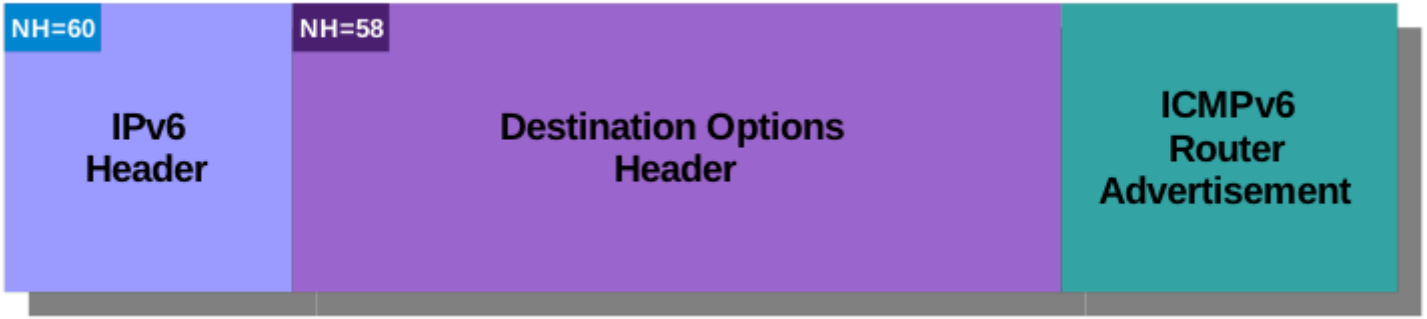
- Utiliza criptografía para mitigar vulnerabilidades en Neighbor Discovery (incluyendo NS falsificados):
  - Direcciones Criptográficamente Generadas (CGAs) para relacionar direcciones IPv6 con un par de llaves asimétricas
  - Firmas RSA para autentificar todos los mensajes de Neighbor Discovery
  - “Caminos certificados” para verificar la autoridad de routers
- SEND es difícil de desplegar:
  - No tiene amplio soporte (por ej., no es soportado por Windows)
  - El requisito de una PKI hace que sea difícil de desplegar para escenarios generales
- SEND es IPR-encumbered (cubierto por patentes)

Monitoreo de tráfico Neighbor Discovery

- Algunas herramientas mantienen un registro de los mapeos (IPv6 -> Ethernet) válidos
- Similar a arpwatch en IPv4
- Sin embargo, típicamente son triviales de evadir:
  - ND “corre” encima de IPv6
  - Los paquetes pueden contener Encabezados de Extensión IPv6
  - Los paquetes pueden fragmentarse
  - Y como es tráfico local, no es posible introducir un MITM para que los “normalice”

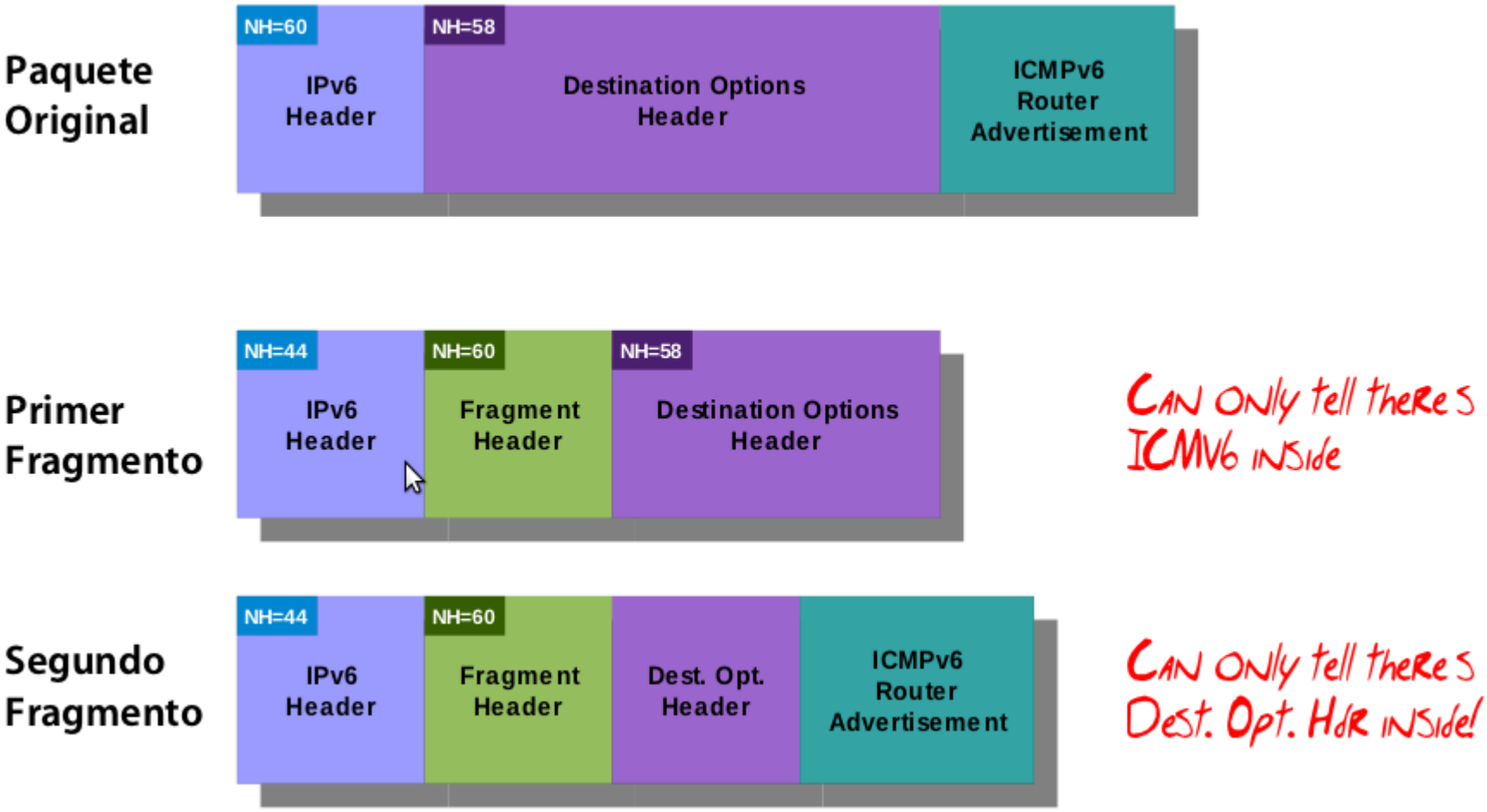
Monitoreo de tráfico ND (II)

- Puede insertarse una cantidad arbitraria de Extension Headers
- La herramienta debe procesar la cadena entera.
- Ejemplo:



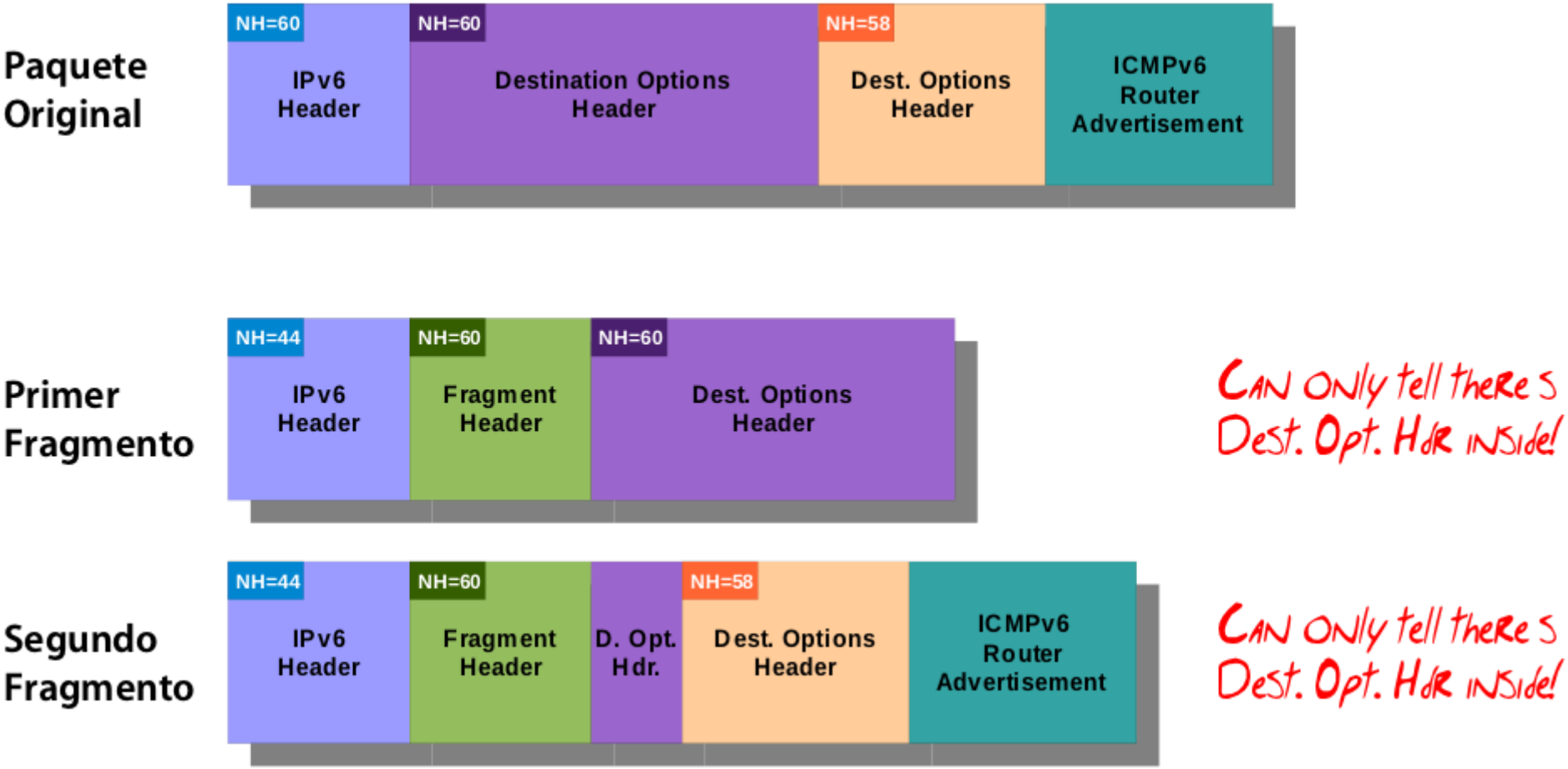
Monitoreo de tráfico ND (III)

- Combinación de Destination Options header y fragmentación:



Monitoreo de tráfico ND (III)

- Dos Destination Options headers, y fragmentación:



Restringir el acceso a la red local

- El tráfico Neighbor Discovery es local a la red
- Separar los nodos en distintas subredes limita el daño que cada nodo puede causar
- No siempre es posible, pero usualmente es deseable

Entradas estáticas en el Neighbor Cache

- Las entradas estáticas evitan intercambiar NS/NA
- Son análogas a las entradas estáticas del ARP cache
- Advertencia: Algunas implementaciones ignoran las entradas estáticas, e intercambian NS/NA!

Entradas estáticas en el NC (II)

- En los *BSD, se crean mediante el comando "ndp"
- Se pueden agregar entradas estáticas así:

  # ndp –s IPV6ADDR MACADDR
- Si IPV6ADDR es una dirección link-local, se debe especificar un “índice de interfaz”:

  # ndp –s IPV6ADDR%IFACE MACADDR
- Se puede verificar el resultado con:

  $ ndp -a

Entradas estáticas en el NC (III)

- En Linux, se manipula el NC con el comando "ip"
- Se pueden agregar entradas estáticas así:

  $ sudo ip neigh add to IPV6ADDR lladdr MACADDR dev IFACE nud permanent

- Se puede verificar el resultado con:

  $ ip -6 neigh show

Conclusiones

- Lamentablemente:
  - SeND es difícil de desplegar
  - Las herramientas de monitoreo son fácilmente evadibles
  - El uso de entradas estáticas “no escala”
  - No siempre es posible restringir el acceso a la red local
- En conclusión,
  - La situación es similar a la de IPv4
  - Tal vez un poco mas complicada

Auto-configuración

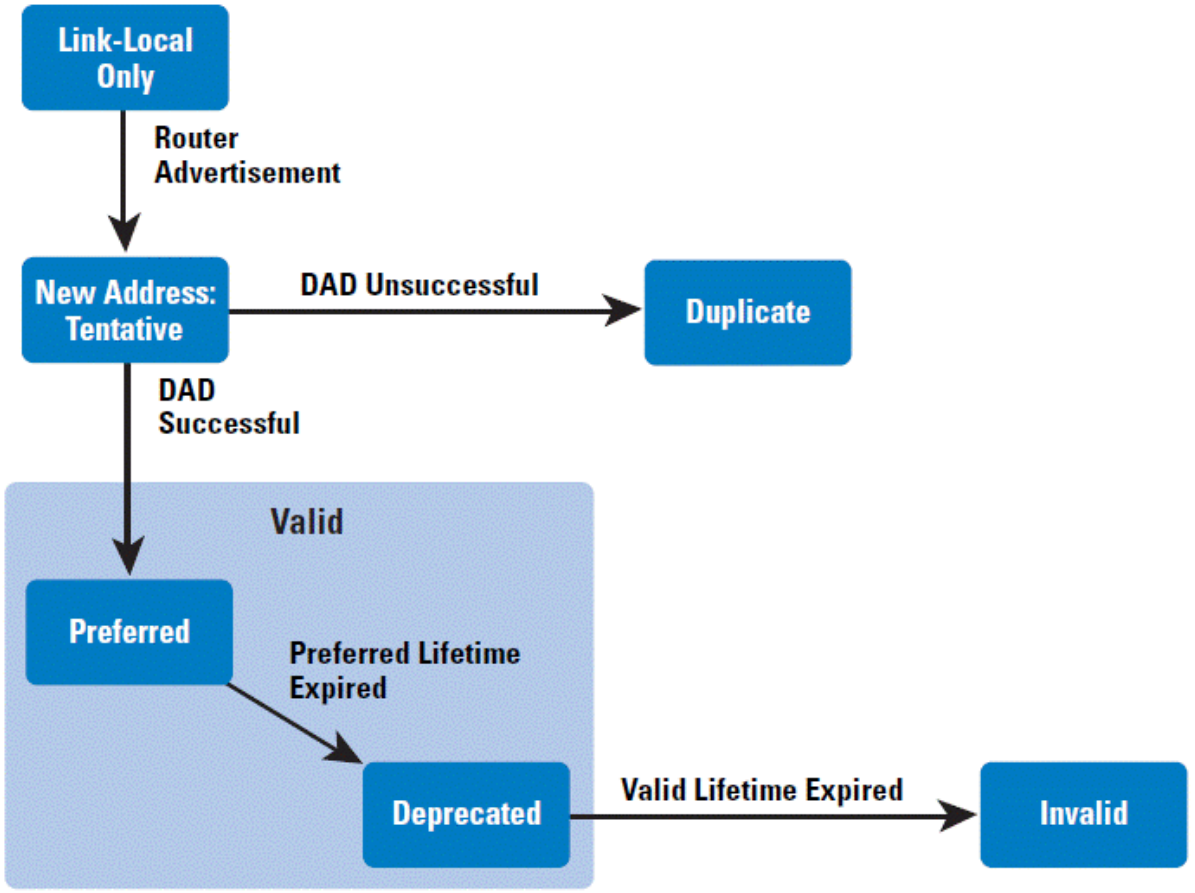
Breve reseña

- Dos mecanismos de autoconfiguración en IPv6:
  - Stateless Address Auto-Configuration (SLAAC)
    - Basado en ICMPv6
  - DHCPv6
    - Basado en UDP
- SLAAC es mandatorio, mientras que DHCPv6 es opcional
- Funcionamiento básico de SLAAC:
  - Los hosts solicitan información mediante ICMPv6 Router Solicitations
  - Los routers responden con Router Advertisements:
    - Prefijos a utilizar
    - Rutas a utilizar
    - Parametros de red
    - etc.

Stateless Address Autoconfiguration

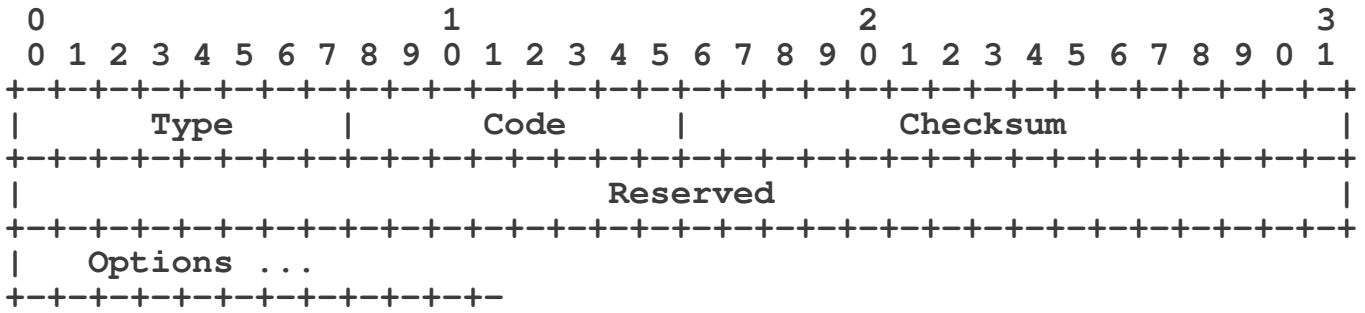
- A grandes rasgos, funciona así:
  1. El host configura una dirección link-local
  2. Chequea que la dirección sea única (DAD)
     - Envia un NS, y ve si se obtiene respuesta
  3. El host envía un mensaje Router Solicitation
  4. Al recibir una respuesta, se configura una dirección IPv6 “tentativa”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

SLAAC: Diagrama de estados



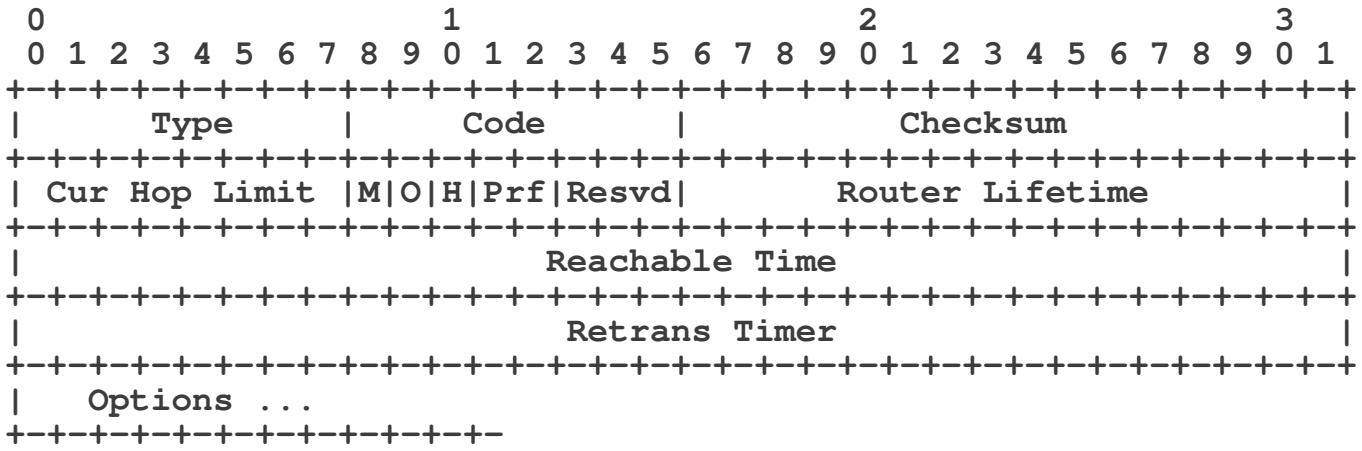
Mensajes Router Solicitation

- Mensajes ICMPv6 de tipo 133, código 0
- Solicitan información de configuración a un router local
- Única opción permitida: Source Link Layer Address



Mensajes Router Advertisement

- Mensajes ICMPv6 de tipo 134, código 0
- Utilizados por routers para enviar información de configuración

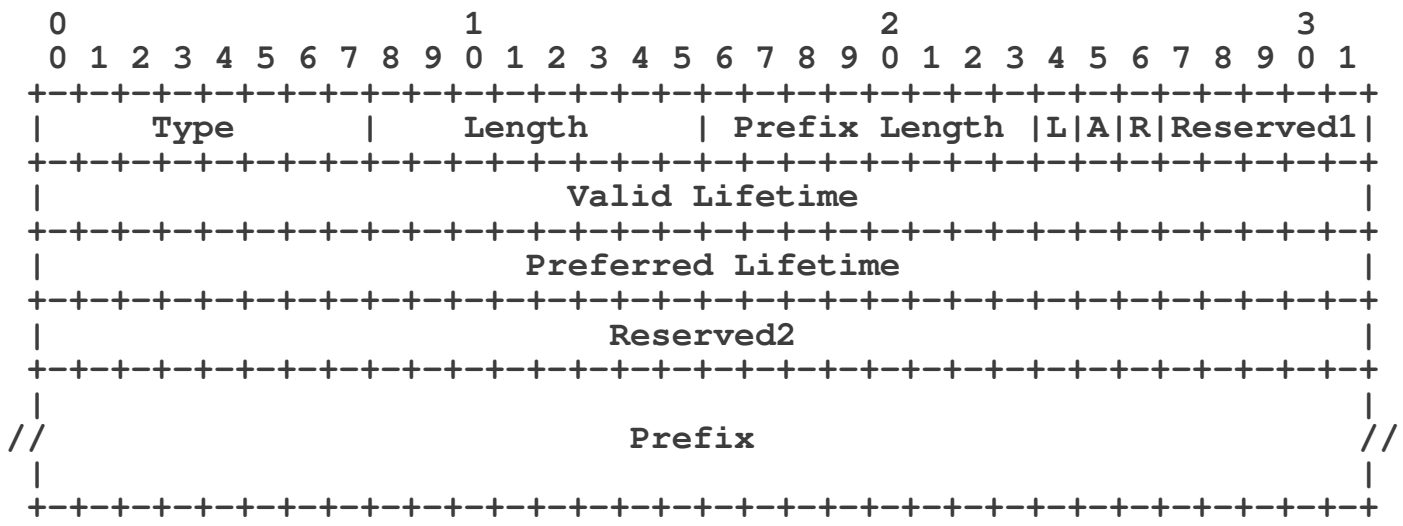


Algunas opciones para RAs

- Los mensajes RA pueden contener:
  - Source Link-layer address option
  - Prefix Information option
  - MTU option
  - Route Information option
  - Recursive DNS Server option
- Usualmente incluyen varias de ellas

Prefix Information Option

- Especifican prefijos “on-link” y prefijos para “auto-configuración”



Ejemplo de tráfico SLAAC

```
17:28:50 :: > ff02::1:ffaf:1958: icmp6: neighbor sol: who has
fe80::20c:29ff:feaf:1958 (len 24, hlim 255)

17:28:52 fe80::20c:29ff:feaf:1958 > ff02::2: icmp6: router solicitation (src
lladdr: 00:0c:29:af:19:58) (len 16, hlim 255)

17:28:52 fe80::20c:29ff:fec0:97b8 > ff02::1: icmp6: router advertisement(chlim=64,
router_ltime=1800, reachable_time=0, retrans_time=0)(src lladdr: 00:0c:29:c0:97:b8)
(prefix info: LA valid_ltime=2592000, preferred_ltime=604800, prefix=2004:1::/64)
(len 56, hlim 255)

17:28:52 :: > ff02::1:ffaf:1958: icmp6: neighbor sol: who has
2004:1::20c:29ff:feaf:1958 (len 24, hlim 255)
```

rdisc6: Herramienta de Diagnóstico

- Envía mensajes RS, y decodifica las respuestas
- Ejemplo:

```
# rdisc6 -v eth0
Soliciting ff02::2 (ff02::2) on eth0...

Hop limit                 :           64 (      0x40)
Stateful address conf.    :           No
Stateful other conf.      :           No
Router preference         :       medium
Router lifetime           :           30 (0x0000001e) seconds
Reachable time            :  unspecified (0x00000000)
Retransmit time           :  unspecified (0x00000000)
 Prefix                   : fc00:1::/64
  Valid time              :      2592000 (0x00278d00) seconds
  Pref. time              :       604800 (0x00093a80) seconds
 Source link-layer address: 00:4F:4E:12:88:0F
 from fe80::24f:4eff:fe12:880f
```

Tabla de “Default Routers” en *BSD

- Ejemplo de salida del comando “ndp -r” (*BSD):

```
% ndp -r
fe80::20c:29ff:fec0:97b8%em1 if=em1, flags=, pref=medium, expire=20m23s
fe80::20c:29ff:fec0:97ae%em0 if=em0, flags=, pref=medium, expire=26m53s
```

Prefijos en uso en *BSD

- Ejemplo de salida de “ndp -p” (*BSD):

```
% ndp -p
2004::/64 if=em0
flags=LAO vltime=2592000, pltime=604800, expire=29d23h57m4s, ref=2
  advertised by
    fe80::20c:29ff:fec0:97ae%em0 (reachable)
2004:1::/64 if=em1
flags=LAO vltime=2592000, pltime=604800, expire=29d23h50m34s, ref=2
  advertised by
    fe80::20c:29ff:fec0:97b8%em1 (reachable)
fe80::%em1/64 if=em1
flags=LAO vltime=infinity, pltime=infinity, expire=Never, ref=0
  No advertising router
fe80::%em0/64 if=em0
flags=LAO vltime=infinity, pltime=infinity, expire=Never, ref=0
  No advertising router
fe80::%lo0/64 if=lo0
flags=LAO vltime=infinity, pltime=infinity, expire=Never, ref=0
  No advertising router
```

Configuración de interfaces

- Ejemplo de salida de “ifconfig -a” en FreeBSD:

```
# ifconfig -a
em0: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> metric 0 mtu 1500
     options=9b<RXCSUM,TXCSUM,VLAN_MTU,VLAN_HWTAGGING,VLAN_HWCSUM>
     ether 00:0c:29:49:eb:dd
     inet 10.0.0.42 netmask 0xffffff00 broadcast 10.0.0.255
     inet6 fe80::20c:29ff:fe49:ebdd%em0 prefixlen 64 scopeid 0x1
     inet6 2004::20c:29ff:fe49:ebdd prefixlen 64 autoconf
     inet6 2004::d13e:2428:bae7:5605 prefixlen 64 autoconf temporary
     nd6 options=23<PERFORMNUD,ACCEPT_RTADV,AUTO_LINKLOCAL>
     media: Ethernet autoselect (1000baseT <full-duplex>)
     status: active
lo0: flags=8049<UP,LOOPBACK,RUNNING,MULTICAST> metric 0 mtu 16384
     options=3<RXCSUM,TXCSUM>
     inet 127.0.0.1 netmask 0xff000000
     inet6 ::1 prefixlen 128
     inet6 fe80::1%lo0 prefixlen 64 scopeid 0x5
     nd6 options=21<PERFORMNUD,AUTO_LINKLOCAL>
```

Stateless Address Autoconfiguration

Algunos posibles ataques...

SI6 NETWORKS

Deshabilitar un router

- Objetivo: Que la víctima descarte a un router como “default router”
- Ataque:
  - Enviar un RA impersonando al router local
  - El RA debe tener un “Router Lifetime” de 0 (u otro valo pequeño)
- Para realizar el ataque con la herramienta ra:

  # ./ra –i IFACE –s ROUTERADDR –d TARGETADDR –t 0 –l 1 –v

  Por ej:

  # ./ra –i eth0 –s fe80::a00:27ff:fef9:7304 -d ff02::1 –t 0 –l 1 –v

Stateless Address Autoconfiguration

Implicancias sobre privacidad...

SI6 NETWORKS

Super cookies

- Las direcciones SLAAC “embeben” la MAC address del host
- Al moverse entre distintas redes, se mantiene la misma MAC address como parte de la dirección IPv6
- Esto equivale a una super-cookie:
- Se vuelve trivial “correlacionar” las actividades de un host

Extensiones de privacidad

- Son direcciones teporales, con el Interface-ID aleatorio
- Se utilizan únicamente para tráfico “saliente”
- Complementan (**no** reemplazan) a las direcciones SLAAC
- En ocasiones fueden dificultar la operación de la red de una organización

Posibles contramedidas

- Posibles contramedidas:
  - Desplegar SeND
  - Monitorear mensajes RS/RA
  - Desplegar Router Advertisement Guard (RA-Guard)
  - Restringir el acceso a la red local

RA-Guard (Router Advertisement Guard)

- Política de filtrado aplicable en switches (layer-2)
- A grandes rasgos:
  - El switch pasa a aceptar RAs solo en determinados puertos
  - Los RAs recibidos en otros puertos son descartados
- RA-Guard **asume** que es posible identificar los RA
- Todas las implementaciones conocidas son evadibles mediante el uso de Extension Headers y/o fragmentación
- Existe una propuesta de mejora, para que RA-Guard sea efectivo (ver <http://blog.si6networks.com>)

Conclusiones

- Lamentablemente,
  - SeND es difícil de desplegar (idem ND)
  - El monitoreo de RS/RA es evadible (idem ND)
  - Las implementaciones de RA-Guard son fácilmente evadibles
  - No siempre se puede limitar el acceso a la red local
- En síntesis,
  - La situación es similar al caso de IPv4
  - Tal vez algo peor

Soporte de IPsec

Breve reseña y consideraciones

Mito: "*IPv6 es mas seguro que IPv4 porque la seguridad fue considerada durante el diseño del protocolo*"

- Debe su origen a que IPsec es **opcional** para IPv4, y **mandatorio** para IPv6
- En la práctica, esto es irrelevante:
  - Es mandatorio el soporte, pero no así su uso
  - Las implementaciones no respetan el estándar
  - Existen en IPv6 los mismos obstaculos para IPsec que en IPv4
- Incluso la IETF reconoció esta situación
- Conclusión:
  - El despliegue de IPv6 no implica un mayor uso de IPsec

Implicancias de seguridad de los mecanismos de transición

Breve reseña

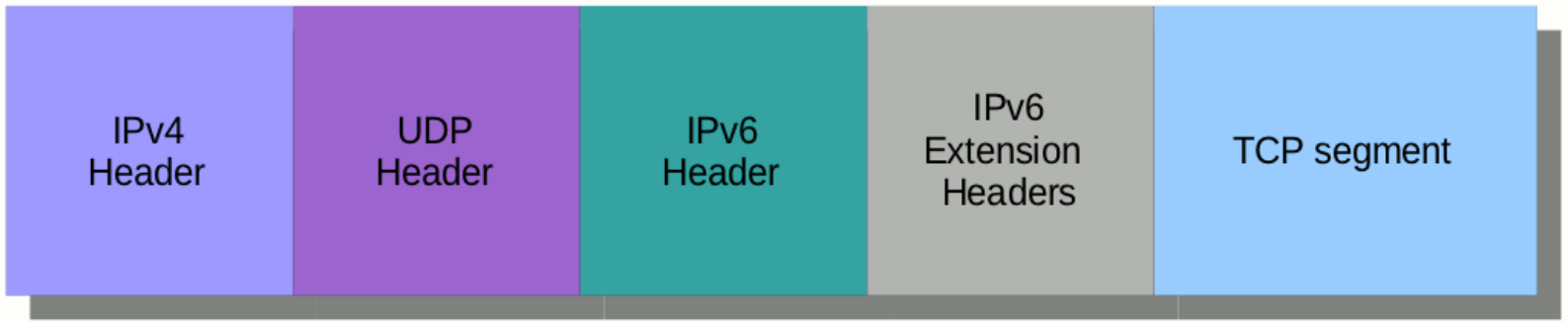
- Plan original de transición: doble pila (dual stack)
  - Desplegar IPv6 en paralelo con IPv4 **antes** de **necesitar** IPv6
  - Este plan **falló**
- La estrategia actual es transición/co-existencia basada en:
  - Doble pila
  - Túneles
    - Automáticos
    - Configurados
  - Traducción
    - CGN
    - NAT64
- La mayoria de los sistemas soportan algunos de estos mecanismos

Consideraciones de seguridad

- Se incrementa la complejidad de la red
- Se introducen “Puntos Únicos de Fallo” (Single Points of Failure)
- Algunas tecnologías tienen implicancias de privacidad:
  - ¿Por dónde circula su tráfico Teredo o 6to4?
  - Esto puede (o no) ser problemático para su organización

Consideraciones de seguridad (II)

- La complejidad del tráfico aumenta notablemente
- Se dificulta la realización de “Deep Packet Inspection”
- Ejemplo: Estructura de un paquete “Teredo”:



- “Ejercicio”: construir filtro libpcap para capturar paquetes destinados al host 2001:db8::1, puerto TCP 25

Implicancias de seguridad de IPv6 en redes IPv4

Breve reseña

- La mayoría de los sistemas tiene algún tipo de soporte IPv6 habilitado “por defecto”
  - Doble pila
  - Teredo
  - ISATAP
  - etc.
- Por ende,
  - La mayoría de las “redes IPv4” tienen al menos un **despliegue parcial de IPv6**

Consideraciones de seguridad

- Se puede habilitar la conectividad IPv6 “durmiente”
  - Enviando Router Advertisements
  - Habilitando tecnologías de transición/co-existencia
- Las tecnologías de transición pueden aumentar la exposición de sistemas
  - Teredo permite el “traspaso” de NATs por sistemas externos
- En conclusión,
  - No existen redes IPv4 “puras”
  - Siempre se deben considerar las implicancias de seguridad de IPv6
  - Si no desea utilizar IPv6, asegurese que ese sea el caso

Áreas en las que se necesita más trabajo

Áreas en las que se necesita mas trabajo

- Seguridad de implementaciones
  - Todavía no han sido foco de ataque
  - Pocas herramientas de auditoria
  - Se descubrirán muchos bugs y vulnerabilidaes
- Soporte de IPv6 en dispositivos de seguridad
  - Se necesita paridad de funcionalidad IPv6/IPv4
  - Caso contrario, no se pueden aplicar las misms políticas de seguridad
- Educación/Entrenamiento
  - Es una locura desplegar IPv6 con “recetas de cocina”
  - Se necesita entrenamiento para todo el personal involucrado
  - Primero entrenarse, luego desplegar IPv6

Algunas conclusiones

Algunas conclusiones....

- Estar atentos al marketing y mitología sobre IPv6
  - Confiar en ellos tiene sus implicancias
- IPv6 provee una *funcionalidad* similar a IPv4
  - Los *mecanismos* utilizados son distintos
  - En dichas diferencias pueden aparecer las “sorpresas”
- La mayoría de los sistemas tiene soporte IPv6
  - Usualmente no existen redes IPv4 “puras”
  - Toda red debe considerar las implicancias de seguridad de IPv6
- Tarde o temprano desplegarás IPv6
  - Es hora de capacitarse y expetimentar con IPv6
  - Sólo después debe desplegarse el mismo

Preguntas?

Gracias!

Fernando Gont

fgont@si6networks.com

IPv6 Hackers mailing-list

http://www.si6networks.com/community/

www.si6networks.com