

# **Cuando implante IPv6... ¿se acabaron los problemas de seguridad?**



---

# Javier Prieto

---

Profesor Redes, Seguridad y Alta Disponibilidad  
- CFGS ASIR - IES Picasso (Chiclana de la Frontera, Cádiz)

Licenciado en Ciencias Físicas Universidad Sevilla

@jprietove

[www.jprietove.com](http://www.jprietove.com)



---

1

# Introducción

Seguridad en IPv6

*Entre los objetivos de diseño  
principales de IPv6 se encuentran  
la seguridad y la  
auto-configuración*



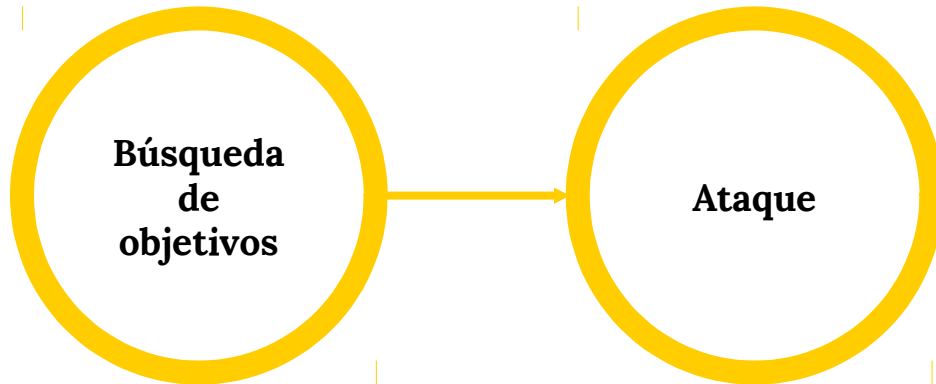
“



# ¿Cómo es un ataque?



## Fases de un Ataque



---

2

# Búsqueda de objetivos

¿Es fácil encontrar equipos con IPv6?



## Búsqueda de objetivos

---

Scan ICMPv6





## Búsqueda por ICMP en IPv4

- En IPv4 una búsqueda de equipos en una red /24 tarda...

¡menos de 10 segundos!

```
javi@jprieto:~$ sudo nmap -sP 140.36.234.0/24
[sudo] contraseña para javi:

Starting Nmap 7.60 ( https://nmap.org ) at 2018-08-30 10:54 CEST
Nmap scan report for 140.36.234.0
Host is up (0.36s latency).
Nmap scan report for 140.36.234.1
Host is up (0.059s latency).
Nmap scan report for 140.36.234.2
Host is up (0.066s latency).
Nmap scan report for 140.36.234.3
Host is up (0.084s latency).
Nmap scan report for 140.36.234.4
Host is up (0.066s latency).
Nmap scan report for 140.36.234.252
Host is up (0.36s latency).
Nmap scan report for 140.36.234.253
Host is up (0.36s latency).
Nmap scan report for 140.36.234.254
Host is up (0.36s latency).
Nmap scan report for 140.36.234.255
Host is up (0.36s latency).
Nmap done: 256 IP addresses (247 hosts up) scanned in 6.70 seconds
javi@jprieto:~$
```



## Búsqueda por ICMPv6

$$2^{64} = 18 \cdot 10^{18}$$

¡Número de Hosts en una red /64!

244.000 años



# Pero...

Entre los objetivos de diseño  
principales de IPv6 se encuentran  
la seguridad y la  
**auto-configuración**

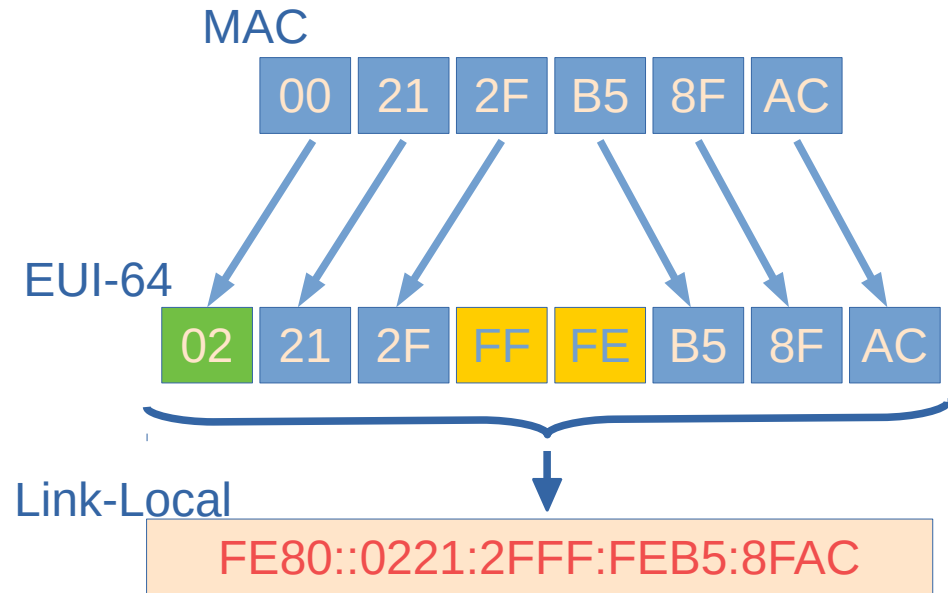


“



## EUI-64

- El Identificador de Interfaz se genera a partir de la dirección MAC
- La dirección Link-Local y SLAAC se genera a partir del Identificador de Interfaz





## Descubriendo Equipos con Dual Stack

- A partir de una búsqueda en IPv4, hallamos las direcciones IPv6

```
javi@jprieto:~$ sudo nmap -sP 192.168.1.0/24

Starting Nmap 7.60 ( https://nmap.org ) at 2018-08-31 10:08 CEST
Nmap scan report for _gateway (192.168.1.1)
Host is up (0.0014s latency).
MAC Address: CC:2D:E0:50: (Unknown)
Nmap scan report for 192.168.1.2
Host is up (0.0016s latency).
MAC Address: 64:D1:54:F7: (Routerboard.com)
Nmap scan report for 192.168.1.3
Host is up (0.0023s latency).
MAC Address: 4C:5E:0C:32: (Routerboard.com)
Nmap scan report for 192.168.1.51
Host is up (-0.093s latency).
MAC Address: B0:E2:35:32: (Xiaomi Communications)
Nmap scan report for 192.168.1.60
Host is up (-0.069s latency).
MAC Address: 00:FC:8B:38: (Amazon Technologies)
Nmap scan report for jprieto (192.168.1.40)
Host is up.
Nmap done: 256 IP addresses (6 hosts up) scanned in 4.36 seconds
javi@jprieto:~$ ping6 fe80::b2e2:35ff:fe32: %wlp3s0
PING fe80::b2e2:35ff:fe32:84a2%wlp3s0(fe80::b2e2:35ff:fe32: %wlp3s0) 56
64 bytes from fe80::b2e2:35ff:fe32: %wlp3s0: icmp_seq=1 ttl=64 time=19.
64 bytes from fe80::b2e2:35ff:fe32: %wlp3s0: icmp_seq=2 ttl=64 time=3.
^C
--- fe80::b2e2:35ff:fe32: %wlp3s0 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 3.191/98.187/193.184/94.997 ms
javi@jprieto:~$ ping6 fe80::2fc:8bff:fe38: %wlp3s0
PING fe80::2fc:8bff:fe38:d31f%wlp3s0(fe80::2fc:8bff:fe38: %wlp3s0) 56
64 bytes from fe80::2fc:8bff:fe38: %wlp3s0: icmp_seq=1 ttl=64 time=1.9
64 bytes from fe80::2fc:8bff:fe38: %wlp3s0: icmp_seq=2 ttl=64 time=55.
^C
--- fe80::2fc:8bff:fe38: f%wlp3s0 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 1.995/28.635/55.275/26.640 ms
```



**¿Qué podemos hacer para no ser descubiertos?**



## Dificultando el escaner de red

---

### RFC 7707

Método para generar un identificador de interfaz para SLAAC estable en una subred, pero que varía al cambiar de una red a otra

### Filtrar ICMPv6 Echo Request

... con cuidado, pues perdemos una gran herramienta de diagnóstico



## RFC 7707: Reconocimiento de Redes en IPv6

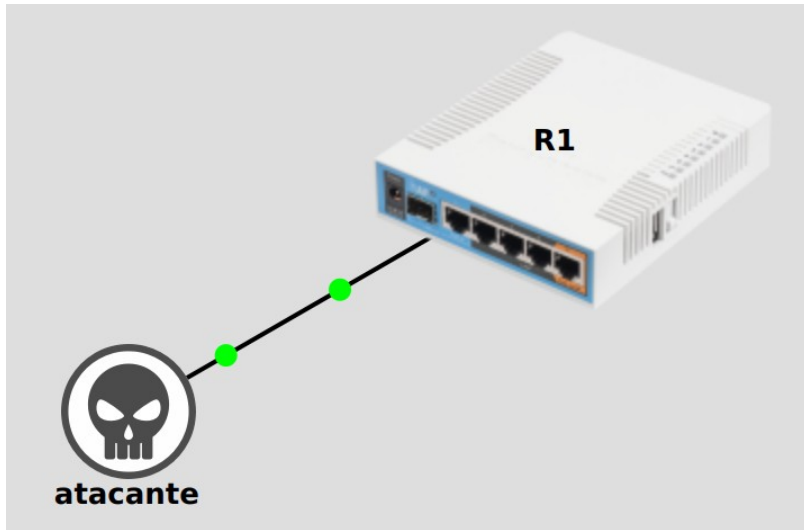
- Utilizar IID según RFC 7217
- IPS en el perímetro
- En VM configurar direcciones MAC manualmente
- Servidores DHCPv6 evitar asignación secuencial. RFC 7217
- Evitar direcciones manualmente configuradas (::0, ::1, ::2) que sean predecibles en la forma de ser asignadas
- Usar el tamaño de prefijo por “defecto” /64





# Evitando PING

Usando ping sin reglas de FW



```
root@atacante:/thc-ipv6# ping6 fe80::e40:14ff:fedb:f400%eth0
PING fe80::e40:14ff:fedb:f400%eth0(fe80::e40:14ff:fedb:f400%eth0) 56 data bytes
64 bytes from fe80::e40:14ff:fedb:f400%eth0: icmp_seq=1 ttl=64 time=0.919 ms
64 bytes from fe80::e40:14ff:fedb:f400%eth0: icmp_seq=2 ttl=64 time=0.954 ms
64 bytes from fe80::e40:14ff:fedb:f400%eth0: icmp_seq=3 ttl=64 time=0.718 ms
64 bytes from fe80::e40:14ff:fedb:f400%eth0: icmp_seq=4 ttl=64 time=0.871 ms
64 bytes from fe80::e40:14ff:fedb:f400%eth0: icmp_seq=5 ttl=64 time=0.982 ms
64 bytes from fe80::e40:14ff:fedb:f400%eth0: icmp_seq=6 ttl=255 time=0.905 ms
^C
--- fe80::e40:14ff:fedb:f400%eth0 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5050ms
rtt min/avg/max/mdev = 0.718/0.891/0.982/0.090 ms
root@atacante:/thc-ipv6#
```





# PING: Filtrado

New Firewall Rule

General | Advanced | Extra | Action | Statistics

Chain: input

Src. Address: [ ]

Dst. Address: [ ]

Protocol:  icmpv6

OK

Cancel

Apply

New Firewall Rule

General | Advanced | Extra | Action | Statistics

Src. Address List: [ ]

Dst. Address List: [ ]

Content: [ ]

TCP Flags: [ ]

ICMP Options: [ ]

ICMP Type:  echo request

ICMP Code: [ ]

enabled

OK

New Firewall Rule

General | Advanced | Extra | Action | Statistics

Action: drop

Log

Log Prefix: [ ]

OK

Cancel

Apply

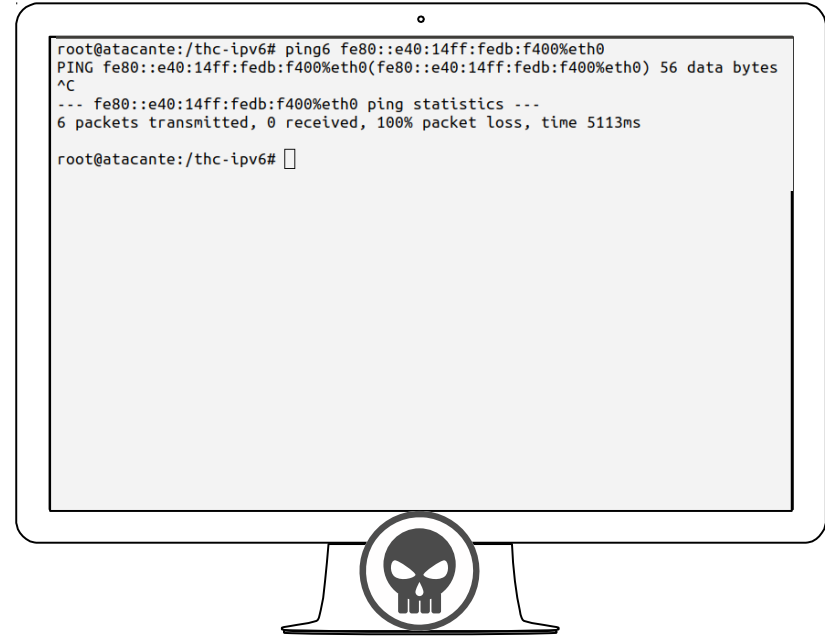
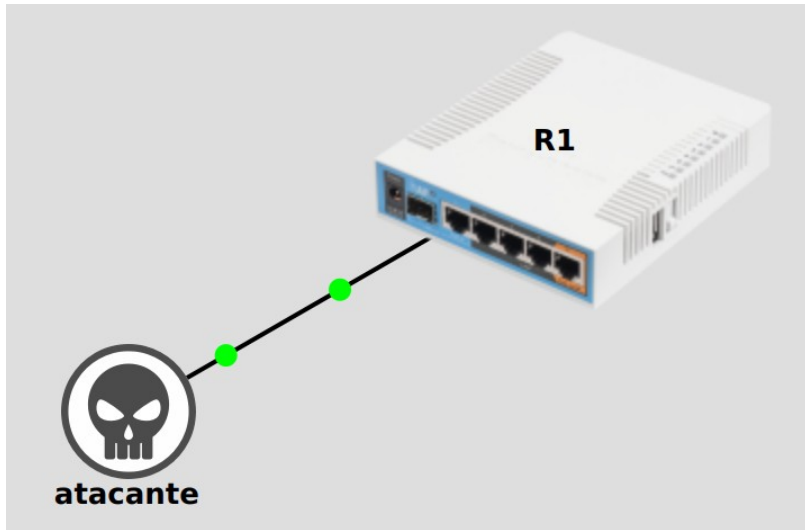
Disable

enabled



## Evitando PING

Usando ping con reglas de FW





## Búsqueda de objetivos

ICMPv6

Direcciones  
Multicast



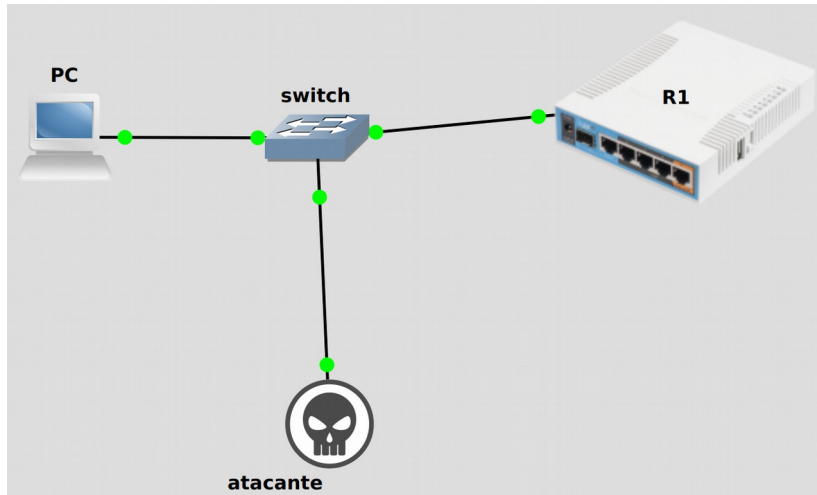
## Direcciones Multicast

Dirección	Descripción
FF02::1	Todos los nodos de la red
FF02::2	Routers en la Subred Local
FF02::5	Routers OSPF
FF02::6	Routers OSPF Designados (DR)
FF02::9	Routers RIP
FF02::D	Routers PIM
FF02::1:2	Agentes DHCP



# Encontrando nodos

## Usando ping y alive6



```
root@atacante:/thc-ipv6# ping ff02::1%eth0
PING ff02::1%eth0(ff02::1%eth0) 56 data bytes
64 bytes from fe80::24ec:bcff:fe35:b437%eth0: icmp_seq=1 ttl=64 time=0.024 ms
64 bytes from fe80::aca8:3aff:fe5f:2981%eth0: icmp_seq=1 ttl=64 time=0.281 ms (DUP!)
64 bytes from fe80::e77:27ff:fe87:eb00%eth0: icmp_seq=1 ttl=255 time=0.594 ms (DUP!)
64 bytes from fe80::24ec:bcff:fe35:b437%eth0: icmp_seq=2 ttl=64 time=0.034 ms
64 bytes from fe80::aca8:3aff:fe5f:2981%eth0: icmp_seq=2 ttl=64 time=0.372 ms (DUP!)
64 bytes from fe80::e77:27ff:fe87:eb00%eth0: icmp_seq=2 ttl=255 time=0.891 ms (DUP!)
64 bytes from fe80::24ec:bcff:fe35:b437%eth0: icmp_seq=3 ttl=64 time=0.051 ms
64 bytes from fe80::aca8:3aff:fe5f:2981%eth0: icmp_seq=3 ttl=64 time=0.599 ms (DUP!)
64 bytes from fe80::e77:27ff:fe87:eb00%eth0: icmp_seq=3 ttl=255 time=1.11 ms (DUP!)
^C
--- ff02::1%eth0 ping statistics ---
3 packets transmitted, 3 received, +6 duplicates, 0% packet loss, time 2032ms
rtt min/avg/max/mdev = 0.024/0.439/1.111/0.369 ms
root@atacante:/thc-ipv6# alive6 eth0 ff02::1
Alive: fe80::aca8:3aff:fe5f:2981 [ICMP echo-reply]
Alive: fe80::e77:27ff:fe87:eb00 [ICMP echo-reply]

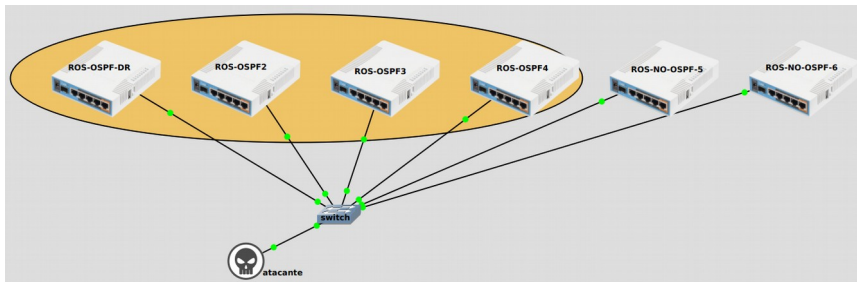
Scanned 1 address and found 2 systems alive
root@atacante:/thc-ipv6#
```





# Encontrando routers

## Usando ping y alive6



```
root@atacante:/thc-ipv6# alive6 eth0 ff02::2
Alive: fe80::eff:40ff:fe6c:6500 [ICMP echo-reply]
Alive: fe80::eff:40ff:fe89:9300 [ICMP echo-reply]
Alive: fe80::eff:40ff:fecc:7700 [ICMP echo-reply]
Alive: fe80::eff:40ff:fe39:e400 [ICMP echo-reply]
Alive: fe80::eff:40ff:fe28:8300 [ICMP echo-reply]
Alive: fe80::eff:40ff:fe4b:5800 [ICMP echo-reply]

Scanned 1 address and found 6 systems alive
root@atacante:/thc-ipv6# alive6 eth0 ff02::5
Alive: fe80::eff:40ff:fecc:7700 [ICMP echo-reply]
Alive: fe80::eff:40ff:fe89:9300 [ICMP echo-reply]
Alive: fe80::eff:40ff:fe39:e400 [ICMP echo-reply]
Alive: fe80::eff:40ff:fe28:8300 [ICMP echo-reply]

Scanned 1 address and found 4 systems alive
root@atacante:/thc-ipv6# alive6 eth0 ff02::6
Alive: fe80::eff:40ff:fecc:7700 [ICMP echo-reply]
Alive: fe80::eff:40ff:fe89:9300 [ICMP echo-reply]

Scanned 1 address and found 2 systems alive
root@atacante:/thc-ipv6#
```





**¿Cómo impedimos que nos encuentren?**





# Multicast: Filtrado de Echo Request

The image displays three overlapping screenshots of the Mikrotik WinBox Firewall Rule configuration interface for rule <ff02::5>.

- Top Window (General tab):** Shows the rule configuration with Chain: `input`, Src. Address: (empty), Dst. Address: `ff02::5`, and Protocol: (empty). Buttons for OK, Cancel, Apply, and Disable are visible.
- Middle Window (Advanced tab):** Shows the ICMP Options section with ICMP Type: `128 (echo request)` and ICMP Code: (empty). Buttons for OK, Cancel, Apply, and Disable are visible.
- Bottom Window (Action tab):** Shows the Action: `drop` and Log: . A Log Prefix field is also present. Buttons for OK, Cancel, Apply, and Disable are visible.



## Búsqueda de objetivos

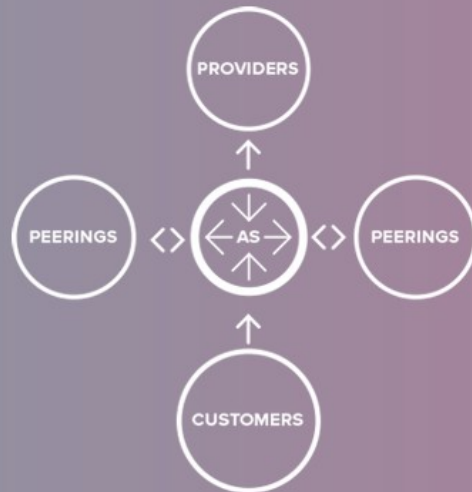
ICMPv6

Direcciones  
Multicast

Buscadores  
y DNS

# AS Relation Model

Our portal represents various analytical data regarding the relation types between autonomous systems (AS). For each AS we openly display its current links as well as the dynamics of their changes. This information is updated daily.



<	AS Relation Model	Radar Monitor	Reverse LG	AS Rating	>
---	-------------------	---------------	------------	-----------	---

CONTACT US



# AS16509

AMAZON-02

Amazon.com, Inc.

35th place in IPv4 connectivity rating

↓ Last month: -5 positions

40th place in IPv6 connectivity rating

↑ Last month: +11 position

Overview

Graph

CURRENT (742)

NEW (59)

LEFT (7)

RETURNING (49)

Prefix	ROA	
2400:6500::/32	Valid	✓
2400:6500:ff00::/48	Valid	✓
2400:6700::/32	Valid	✓
2400:6700:ff00::/48	Valid	✓
2403:b300::/32	Valid	✓
2403:b300:ff00::/48	Valid	✓
2406:da00:2000::/40	Valid	✓
2406:da00:6000::/40	Valid	✓

---

3

# Ataques en IPv6

Sacando partido a la información obtenida

---



## IPv6. Consideraciones de Seguridad\*

### Eavesdropping (escuchas)

Elementos en el camino pueden observar los paquetes

### Replay (repetición)

Un atacante puede grabar una secuencia de paquetes y volver a transmitirlos al destinatario

### Inserción de paquetes

El atacante crea un paquete con un conjunto de propiedades seleccionadas y los inyecta en la red

### Borrado de paquetes

El atacante elimina paquetes del canal

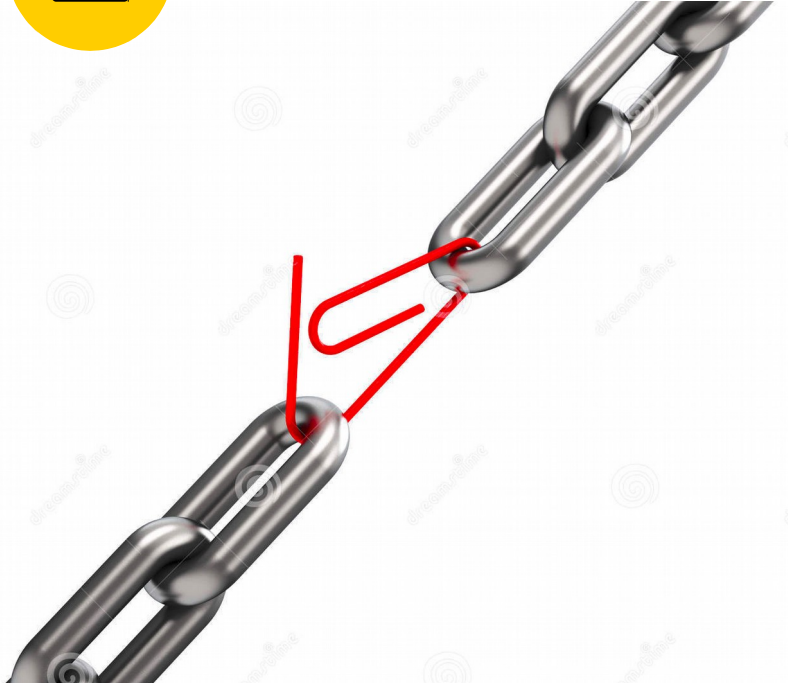
### Modificación de paquetes

El atacante elimina paquetes del canal, los modifica y los reinyecta a la red

### Man in The Middle

El atacante modifica la comunicación para aparecer como receptor al emisor y viceversa

\*RFC 8200-IPv6 Specification



**¿Son realmente importantes estas consideraciones de seguridad?**



## ICMPv6

---

### **NS: Neighbor Solicitation**

ICMPv6 tipo 135

Sirve para preguntar la dirección  
MAC de una determinada IPv6

### **NA: Neighbor Advertisement**

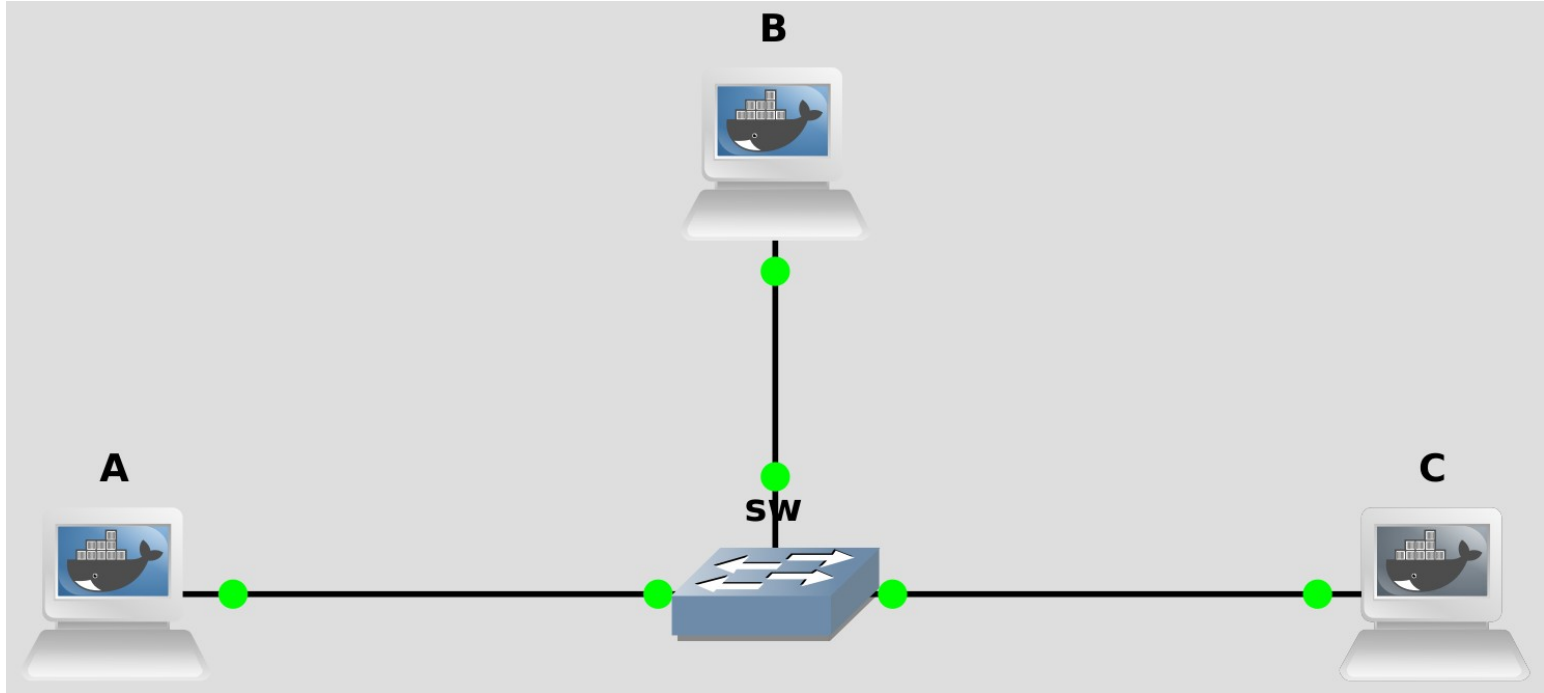
ICMPv6 tipo 136

Sirve para publicar la dirección  
MAC de una determinada IPv6



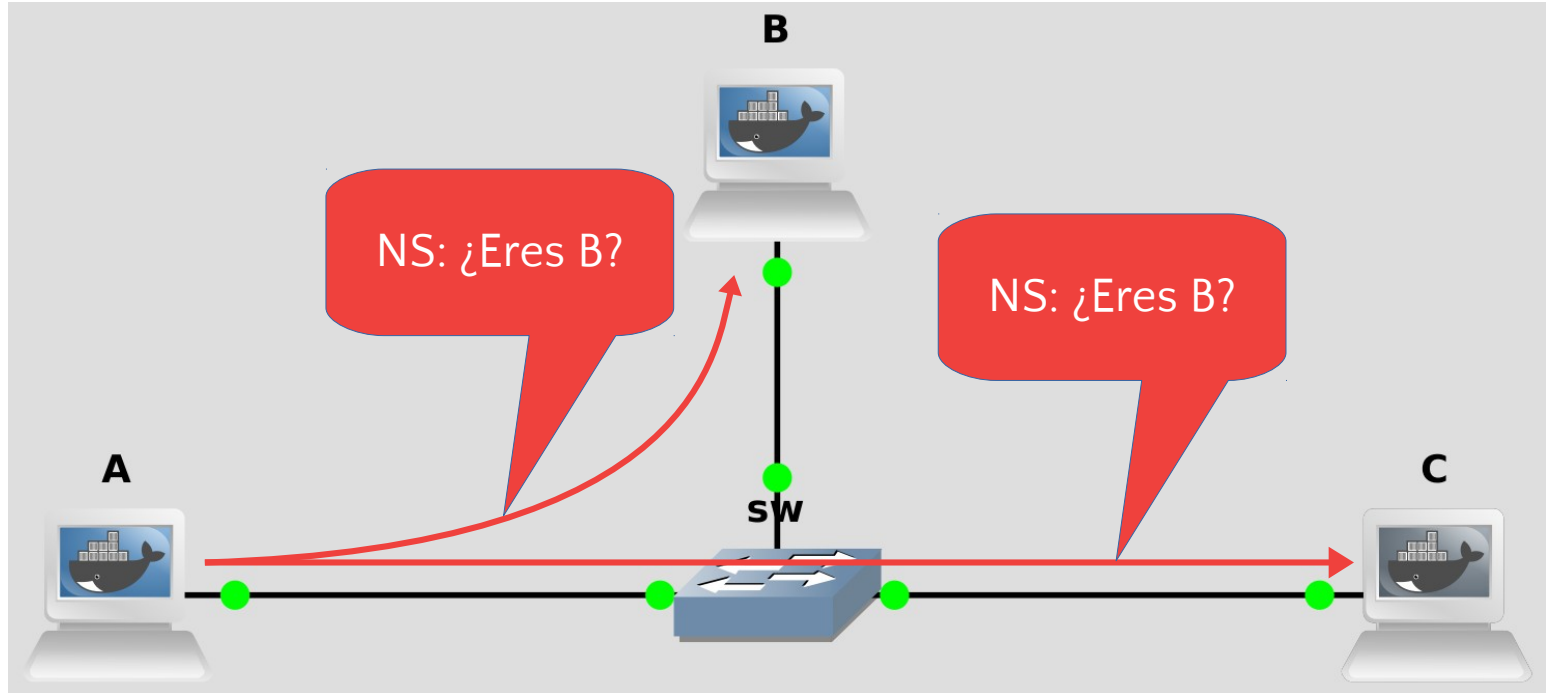


# ICMPv6 NS y NA



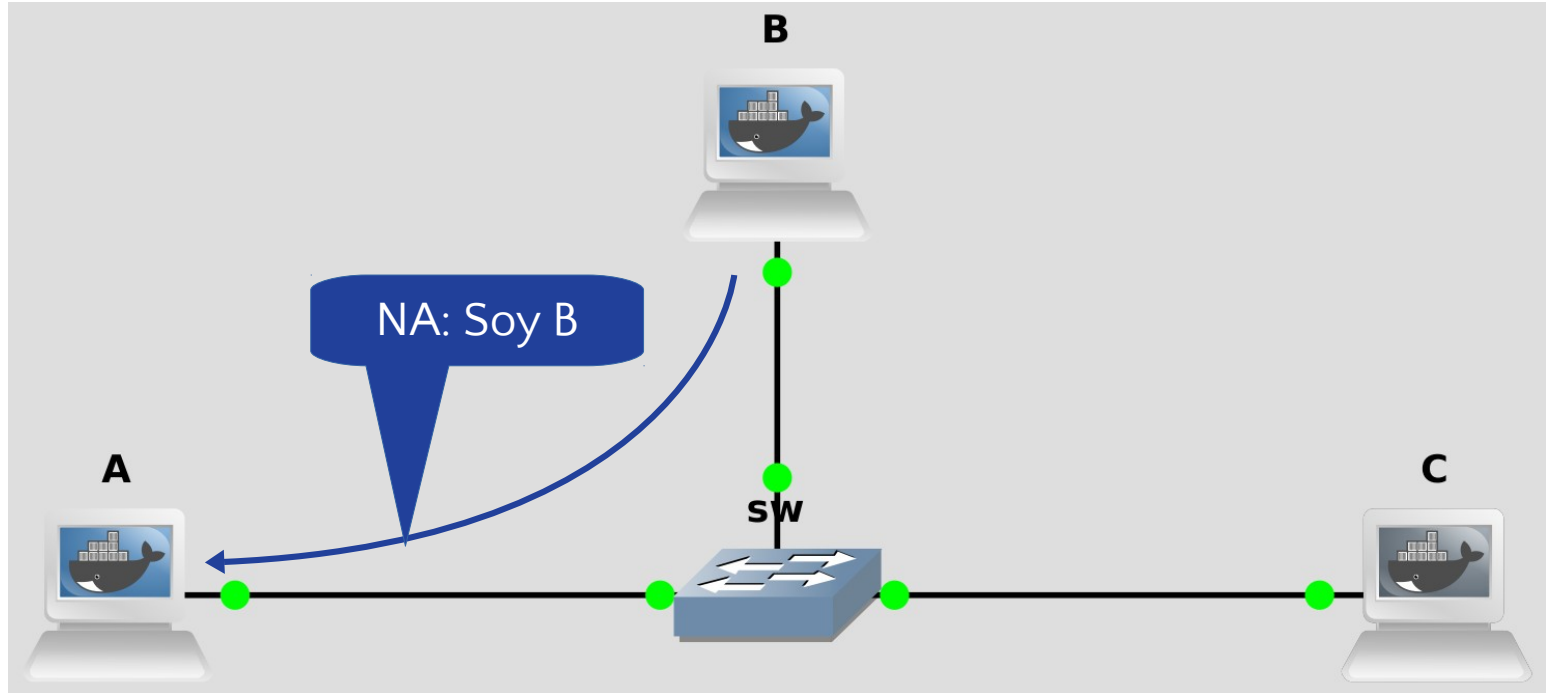


## ICMPv6 NS y NA



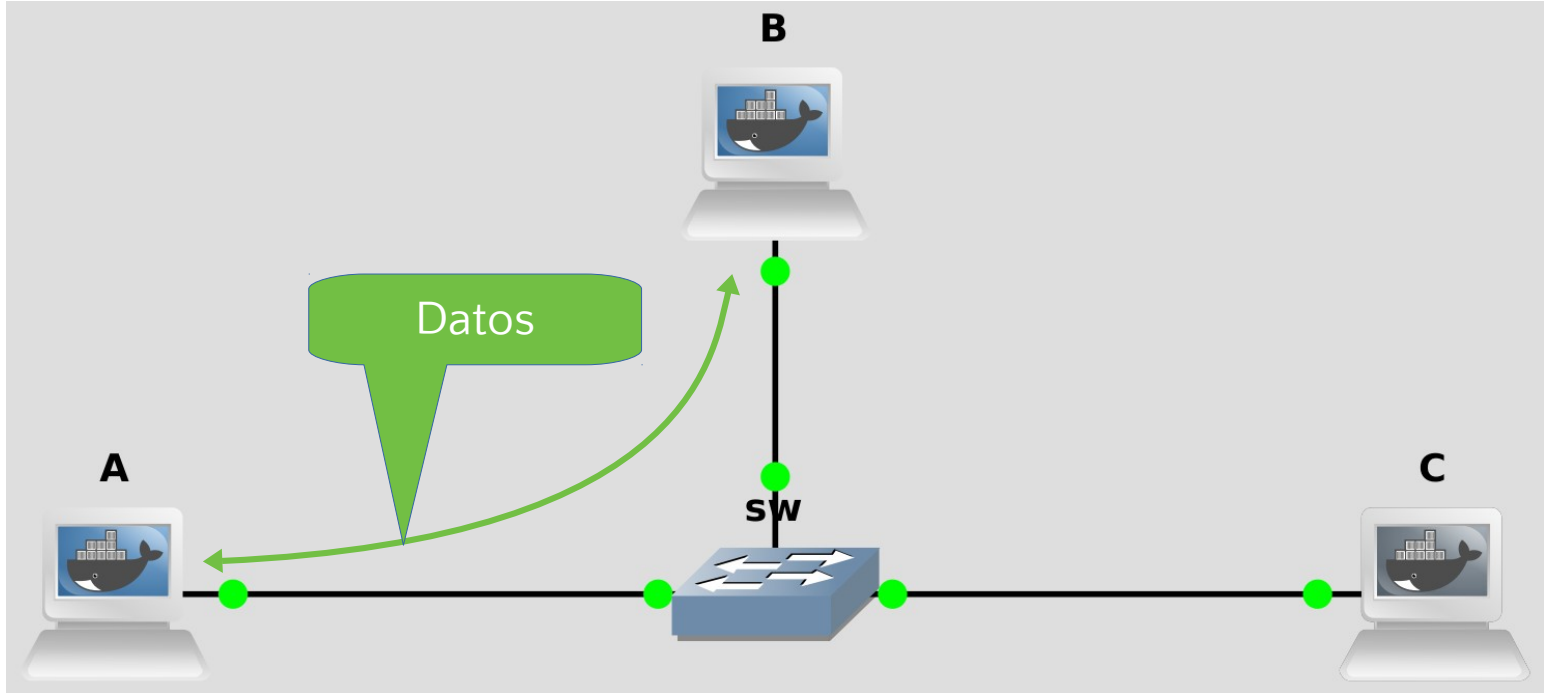


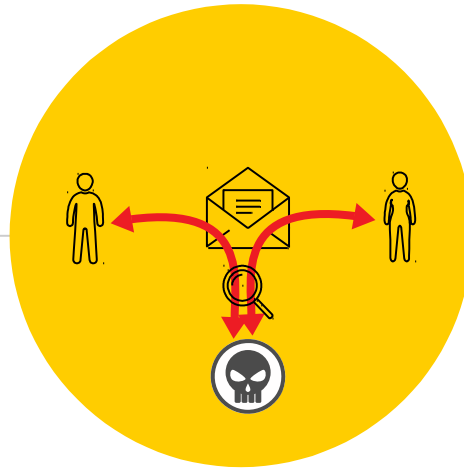
## ICMPv6 NS y NA





# ICMPv6 NS y NA



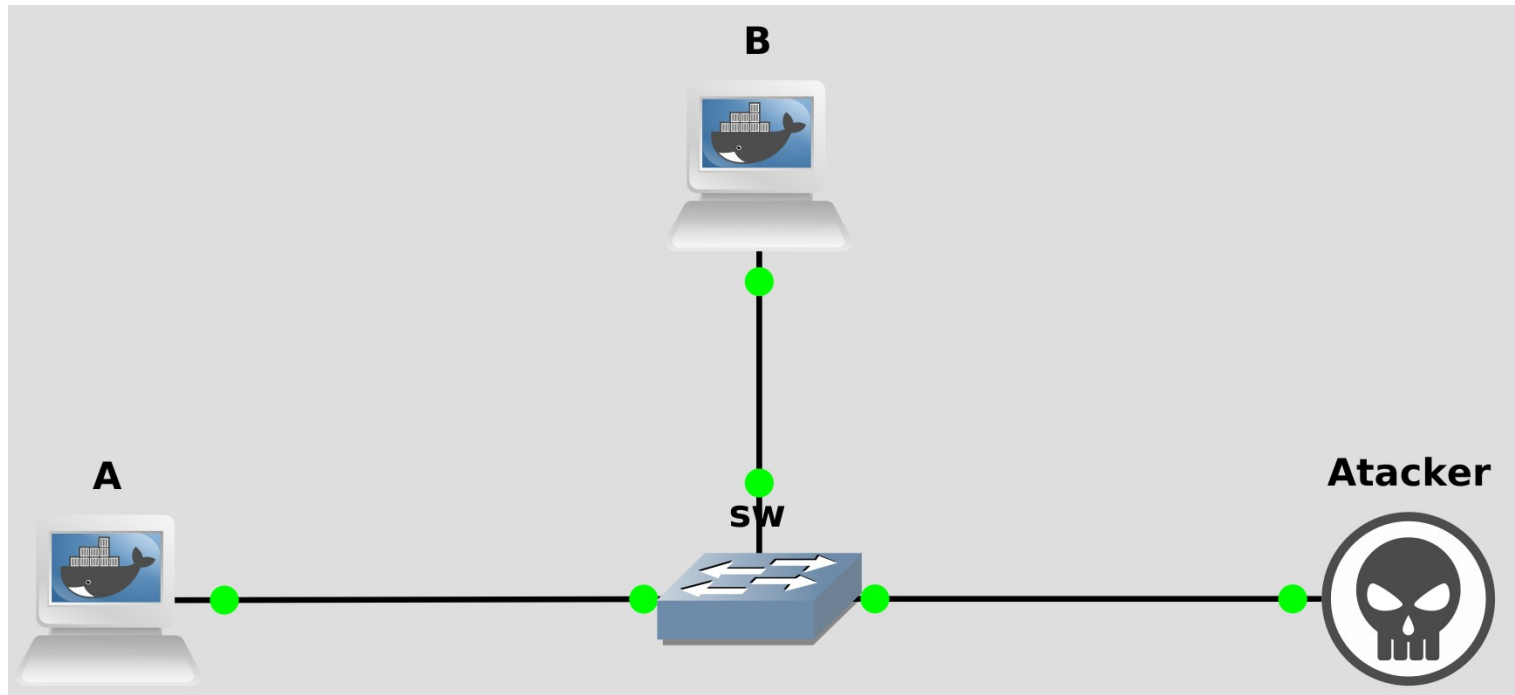


# Ataque MitM

Falsificación de ICMPv6 NA

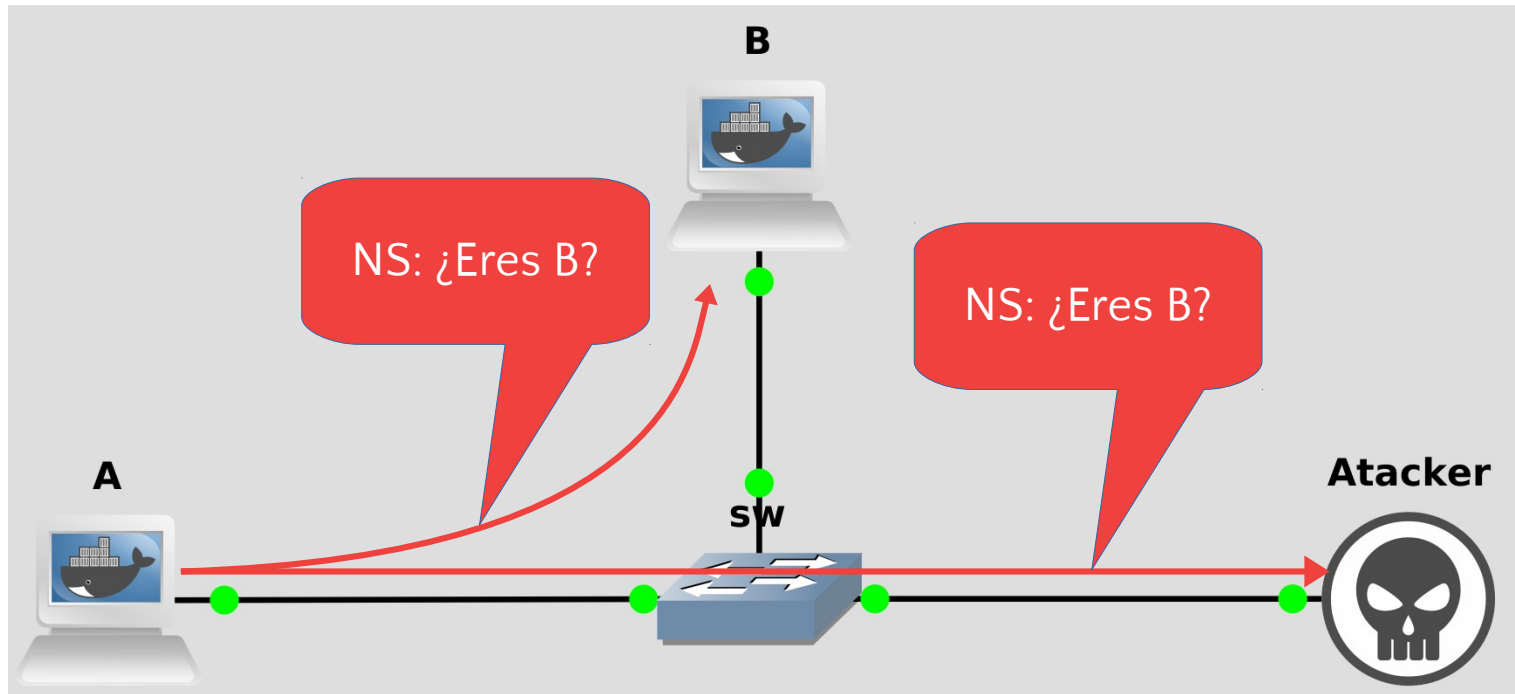


## MitM falsificando ICMPv6 NA



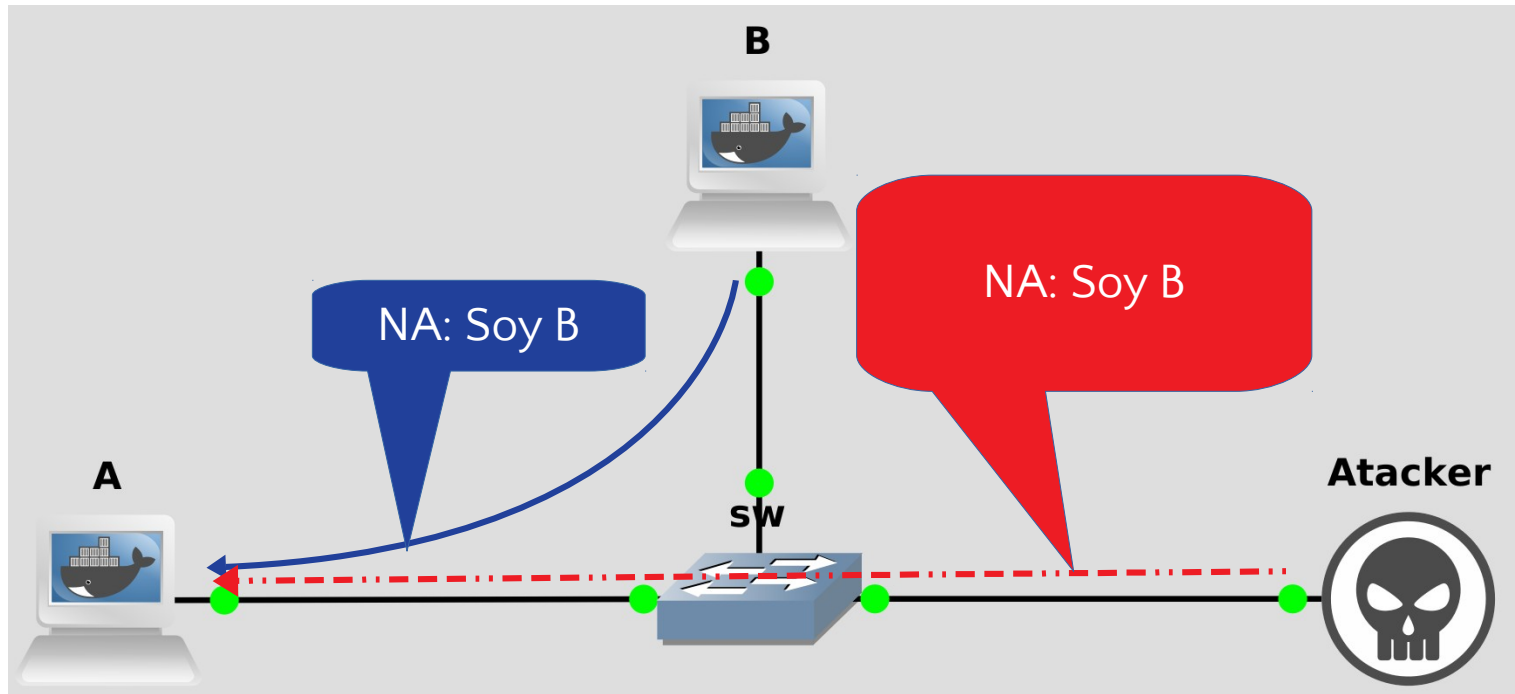


## MiTM falsificando ICMPv6 NA





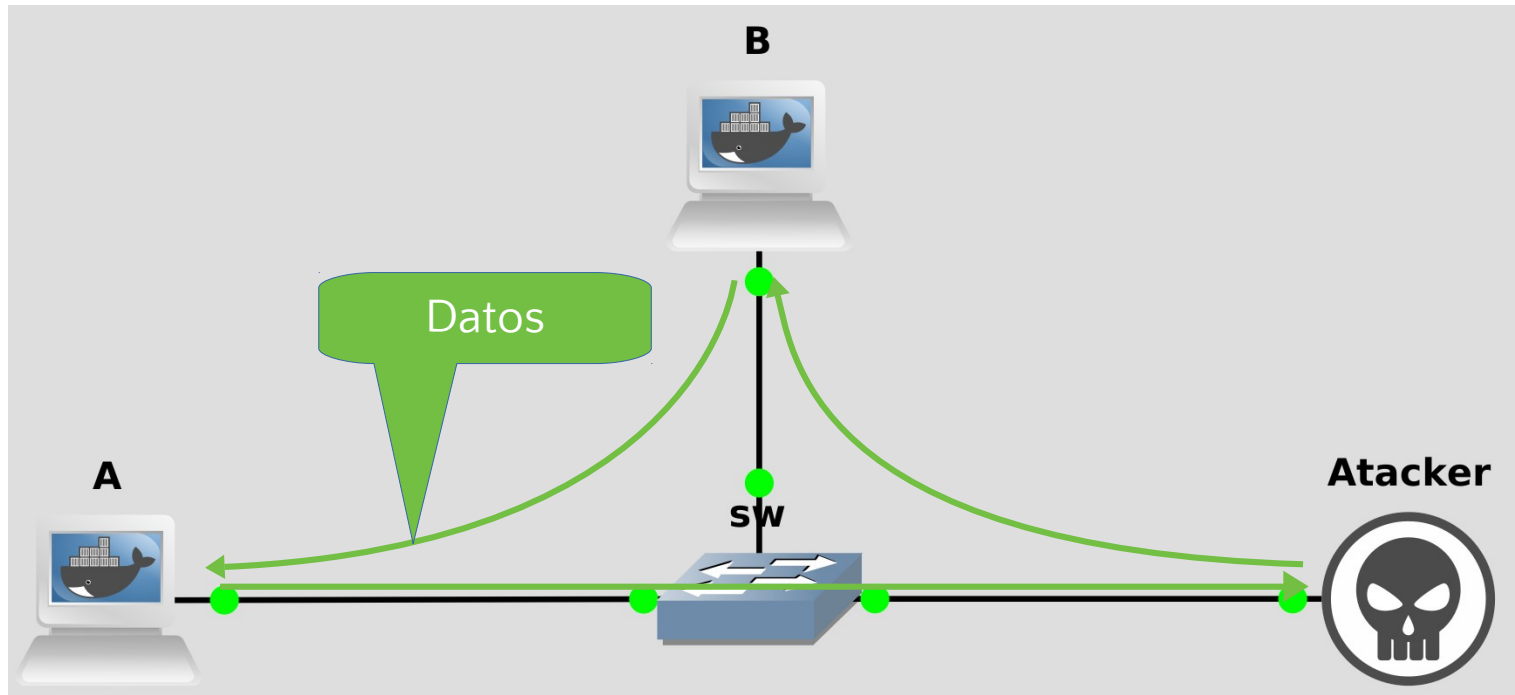
## MiTM falsificando ICMPv6 NA





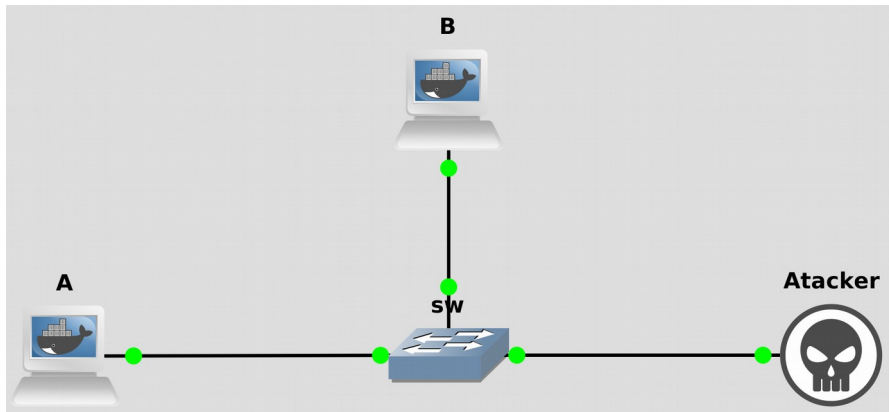


## MiTM falsificando ICMPv6 NA





## MiTM falsificando NA



```
root@Atacker:/thc-ipv6# parasite6 eth0 -l
Remember to enable routing, you will denial service otherwise:
=> echo 1 > /proc/sys/net/ipv6/conf/all/forwarding
Remember to prevent sending out ICMPv6 Redirect packets:
=> iptables -I OUTPUT -p icmpv6 --icmpv6-type redirect -j DROP
Started ICMP6 Neighbor Solicitation Interceptor (Press Control-C to end) ...
Spoofed packet to fe80::7835:58ff:fe86:b2ff as fe80::58b1:b4ff:fe09:d25b
Spoofed packet to fe80::a43e:c5ff:fe0b:1e6b as fe80::58b1:b4ff:fe09:d25b
Spoofed packet to fe80::58b1:b4ff:fe09:d25b as fe80::a43e:c5ff:fe0b:1e6b
Spoofed packet to fe80::a43e:c5ff:fe0b:1e6b as fe80::58b1:b4ff:fe09:d25b
```





## ICMPv6

---

### **RS: Router Solicitation**

ICMPv6 tipo 133

Sirve para solicitar un router en la red

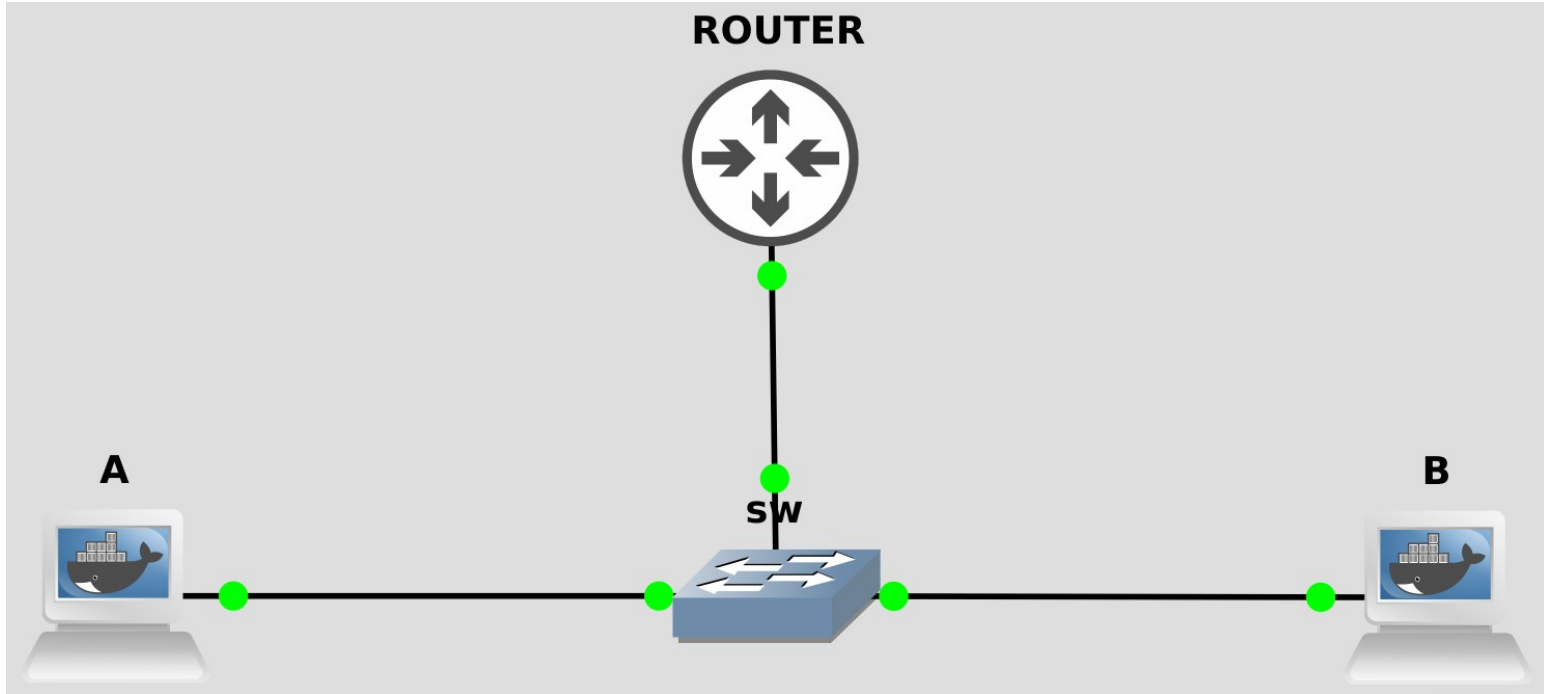
### **RA: Router Advertisement**

ICMPv6 tipo 134

Sirve para que un router publique opciones de autoconfiguración IPv6

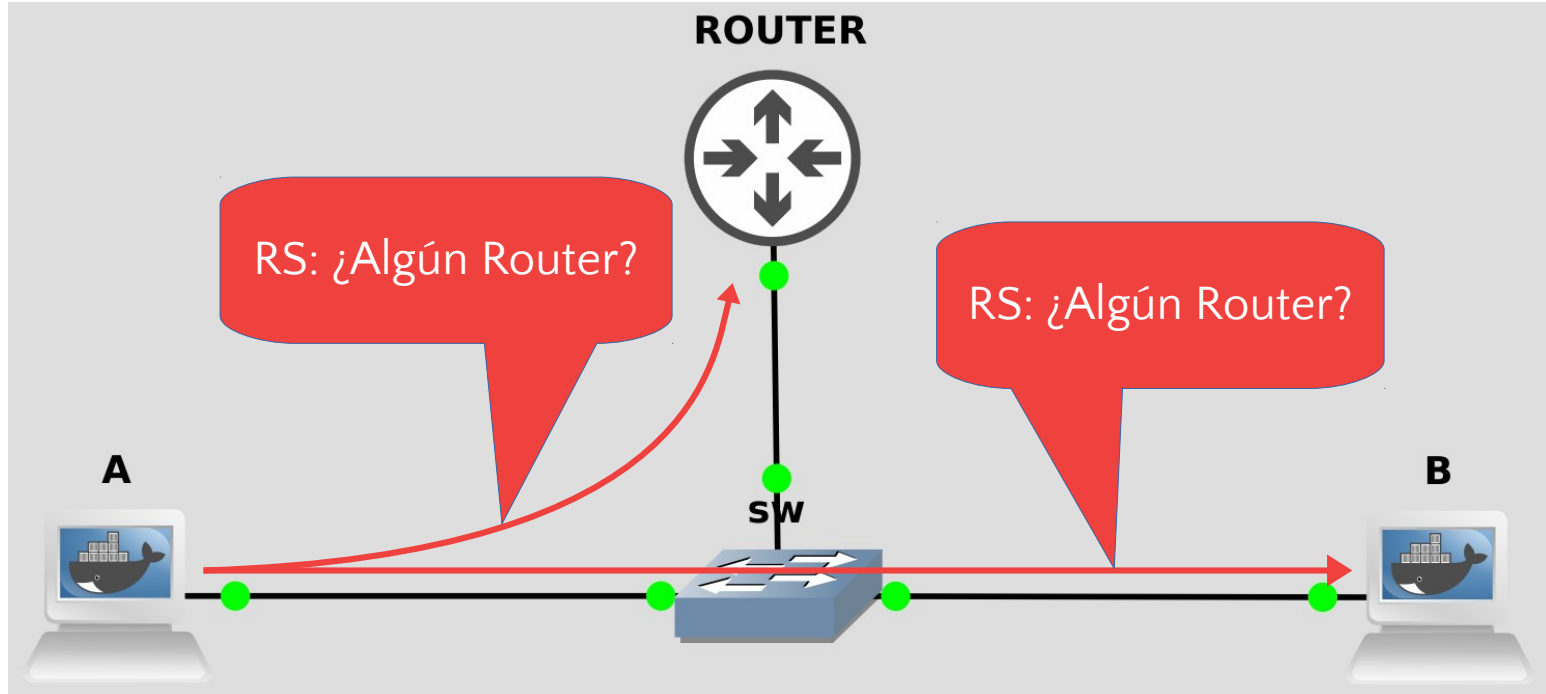


# ICMPv6 RS y RA



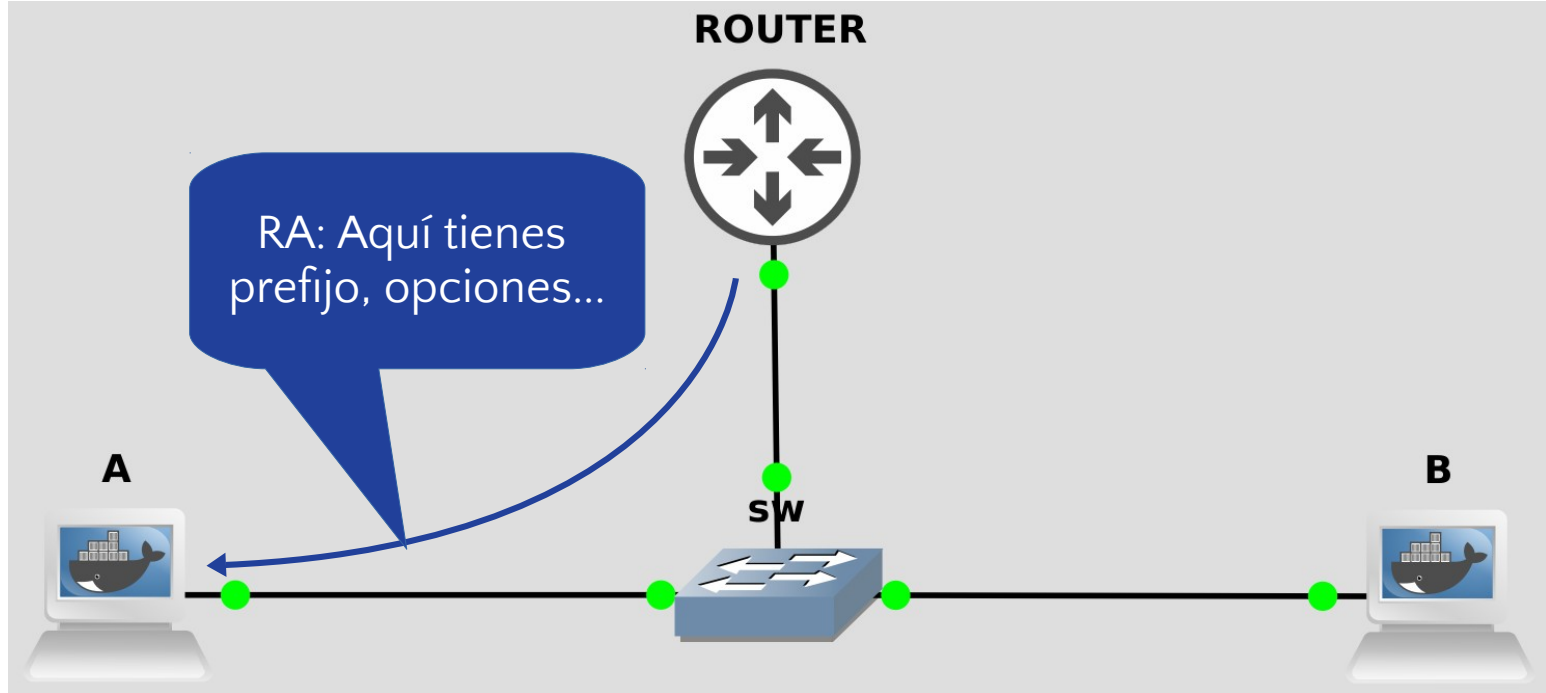


## ICMPv6 RS y RA



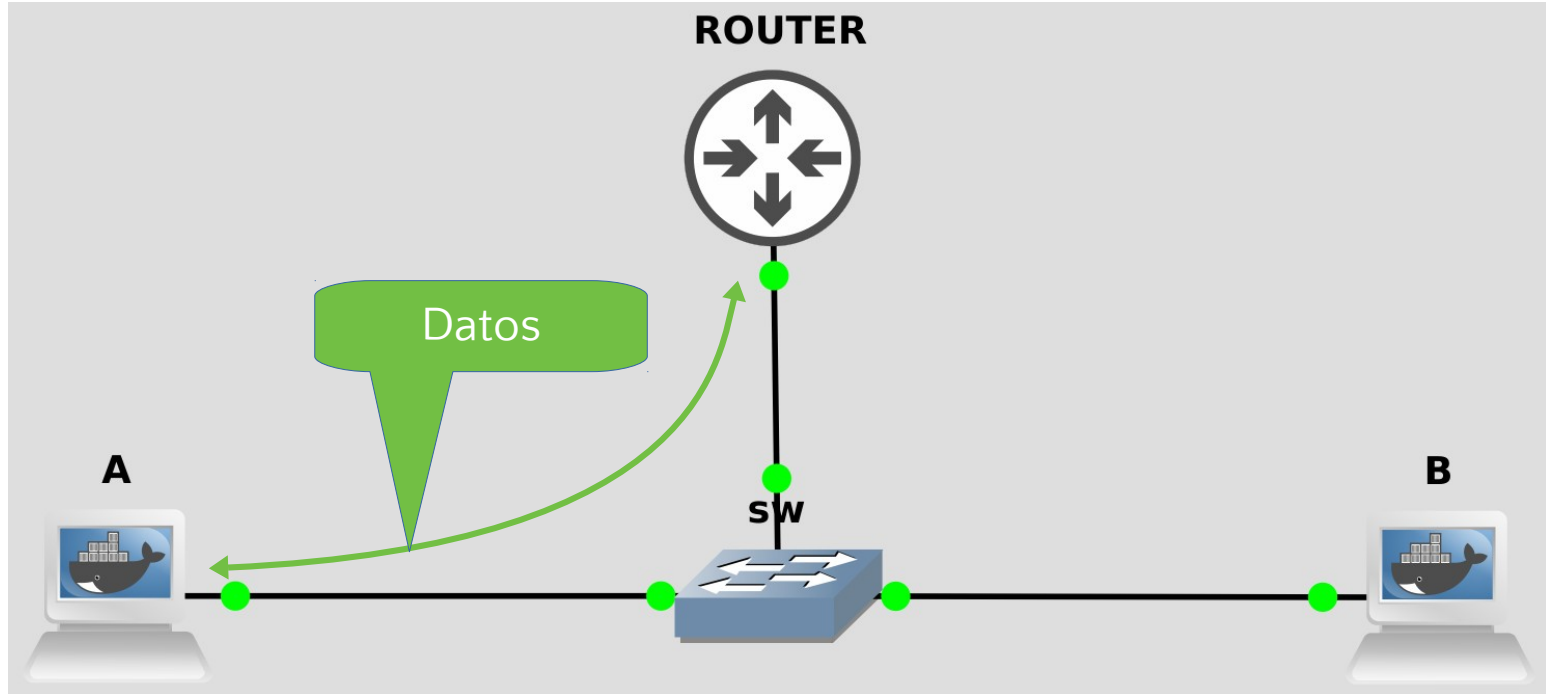


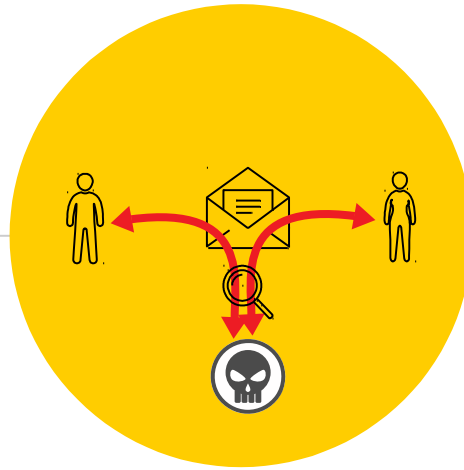
## ICMPv6 RS y RA





## ICMPv6 RS y RA



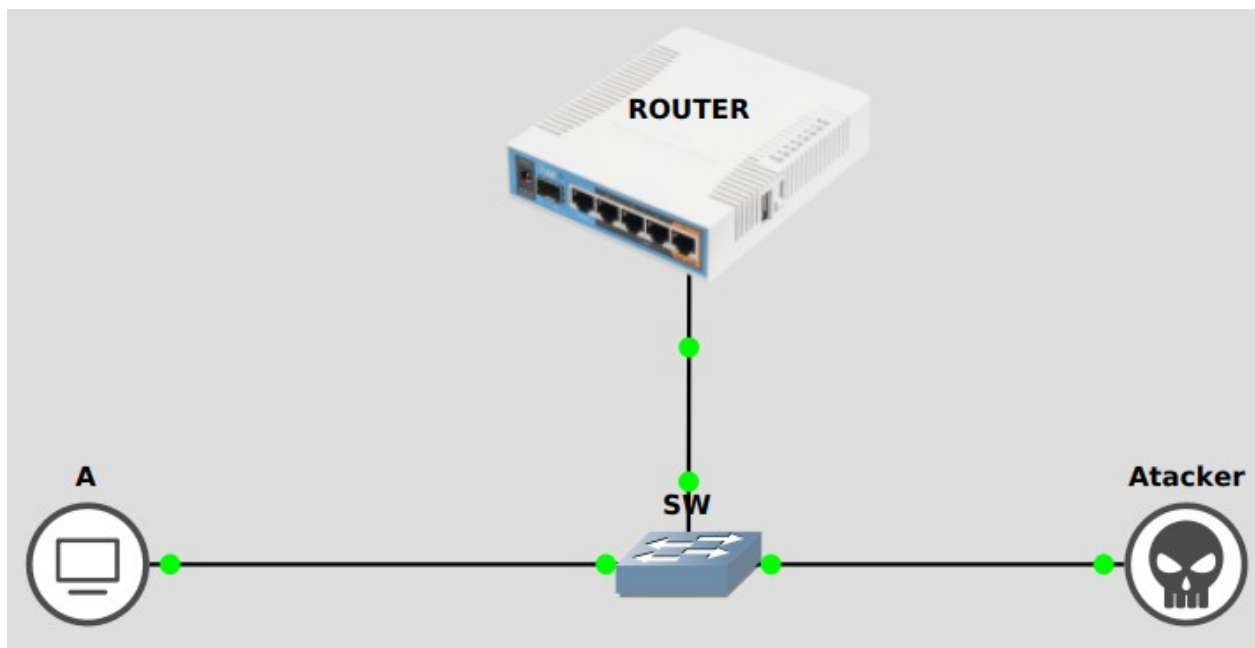


# Ataque MitM

Falsificación de ICMPv6 RA

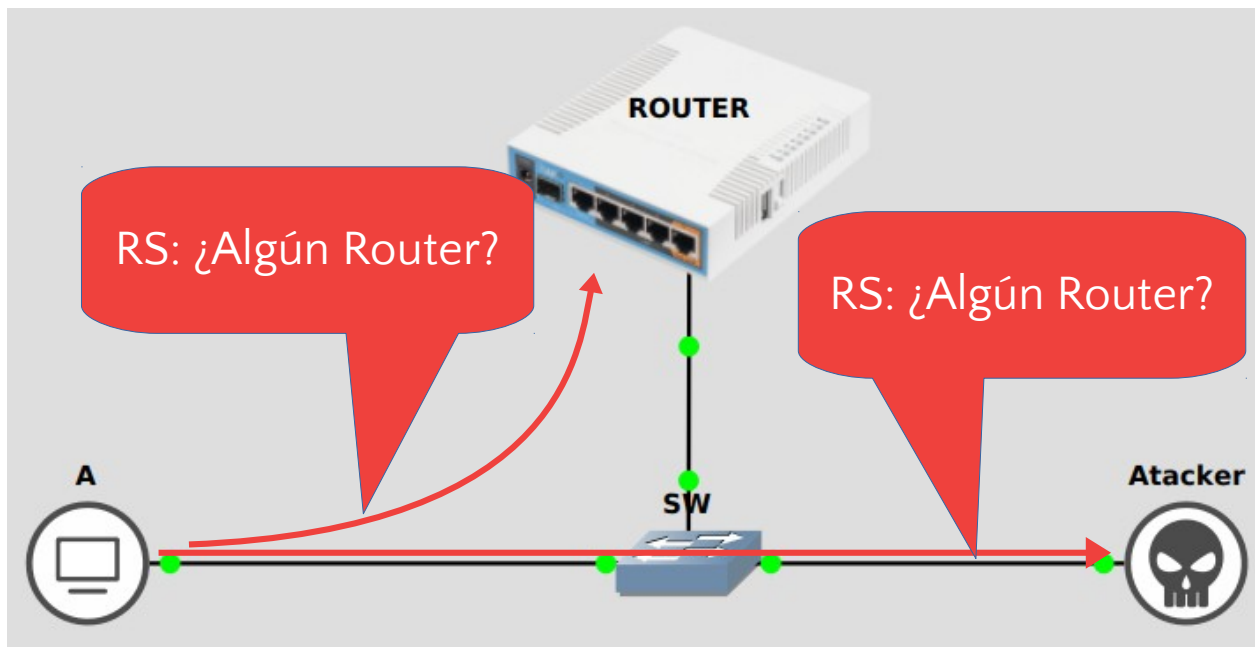


## MiTM falsificando ICMPv6 RA



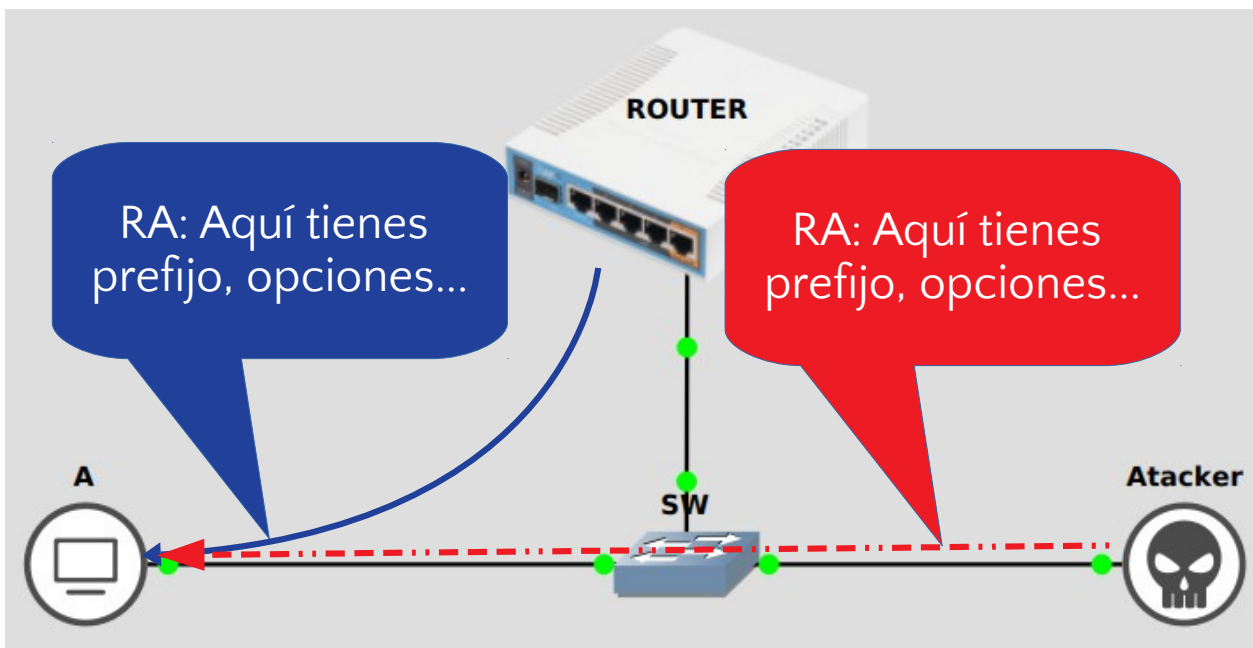


## MiTM falsificando ICMPv6 RA

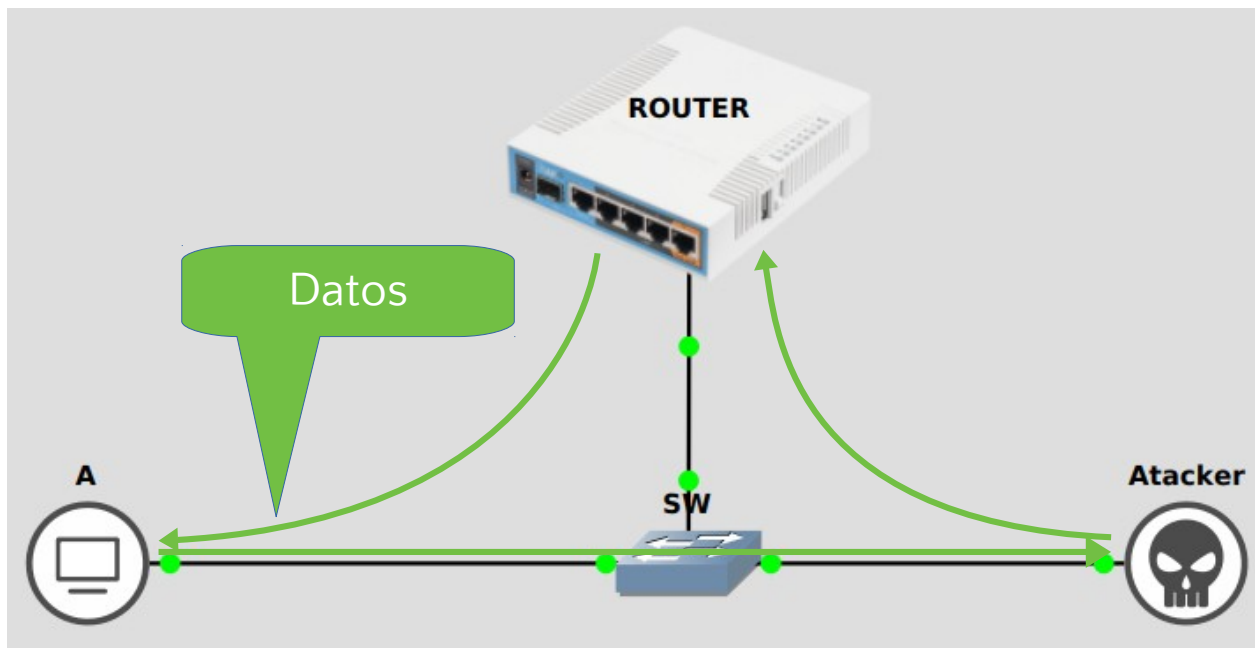




## MiTM falsificando ICMPv6 RA



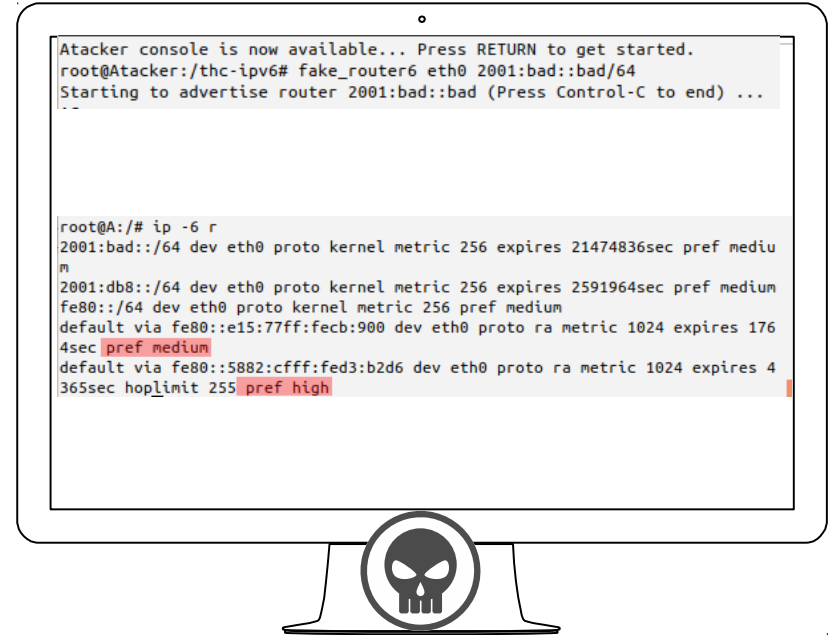
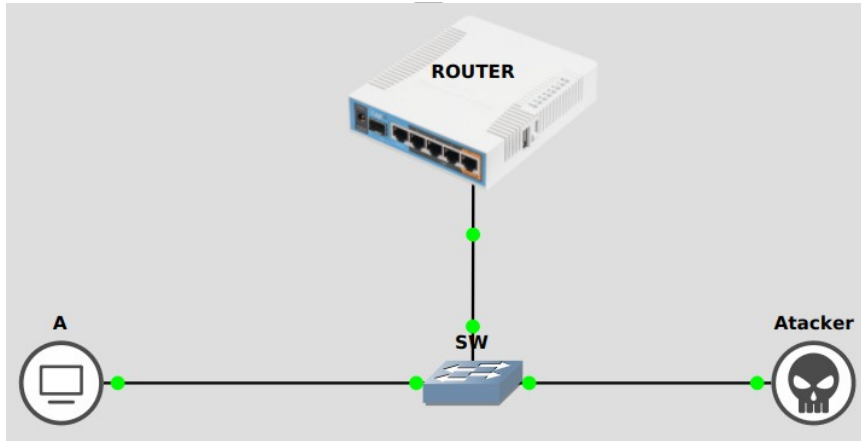
## MiTM falsificando ICMPv6 RA





## MiTM falsificando RA

Usando fake\_router6



# ¿Qué pasa con...

Entre los **objetivos** de diseño principales **de IPv6** se encuentran la **seguridad** y la auto-configuración



“



## Requisitos Nodo IPv6

**Año 2006  
RFC4294  
IPv6 DEBE  
soportar  
IPSec**



## IPSec\*

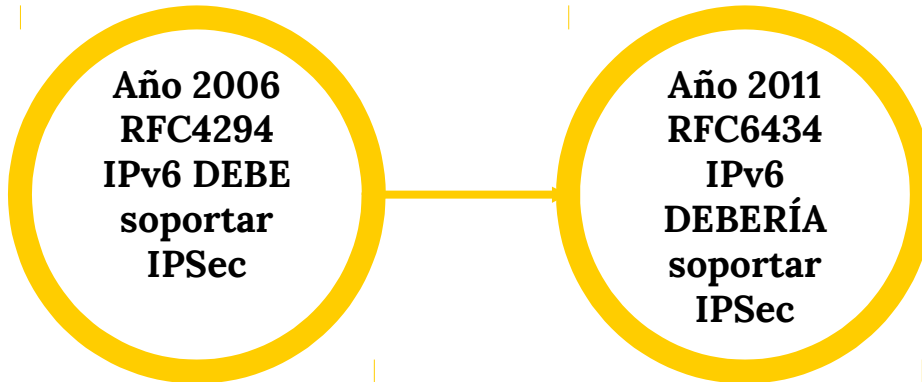
- Control de acceso
- Integridad
- Autenticación del origen de los datos
- Detección y eliminación de repeticiones
- Confidencialidad

\*RFC 4301–Security Architecture for the Internet Protocol





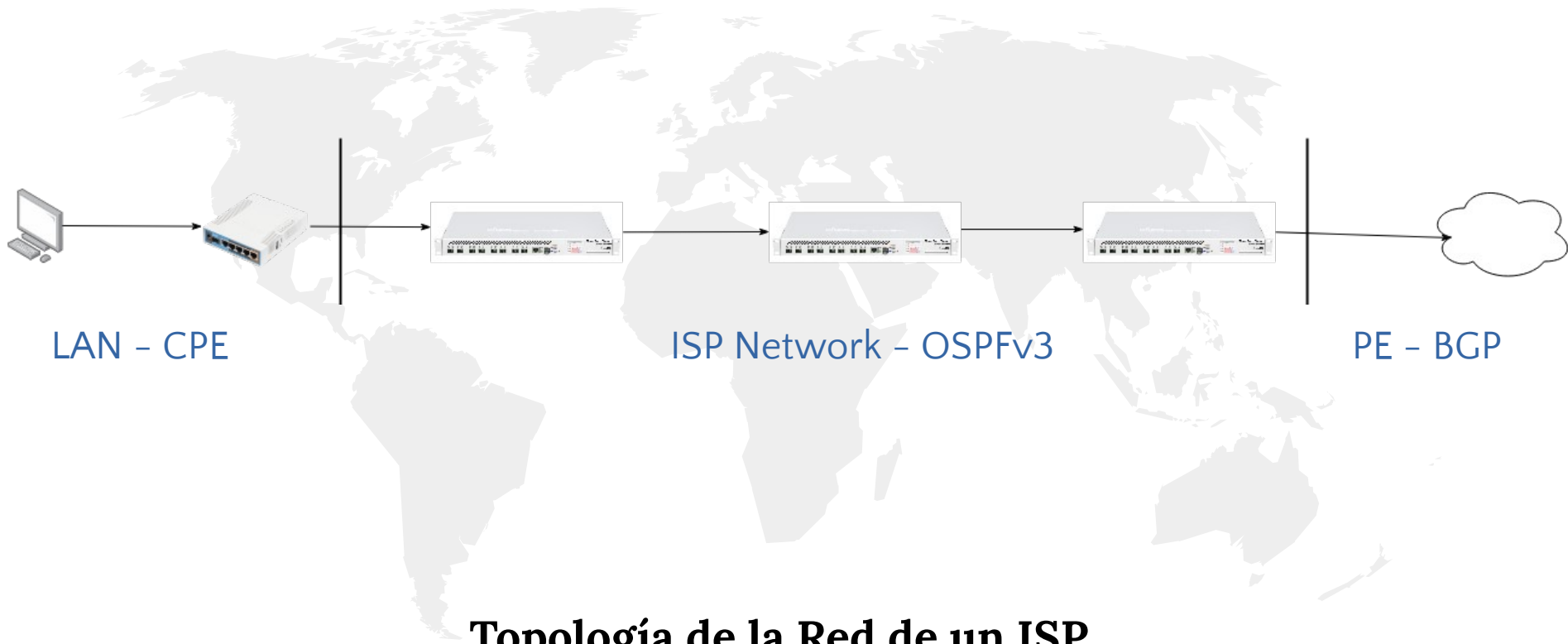
## Requisitos Nodo IPv6



4

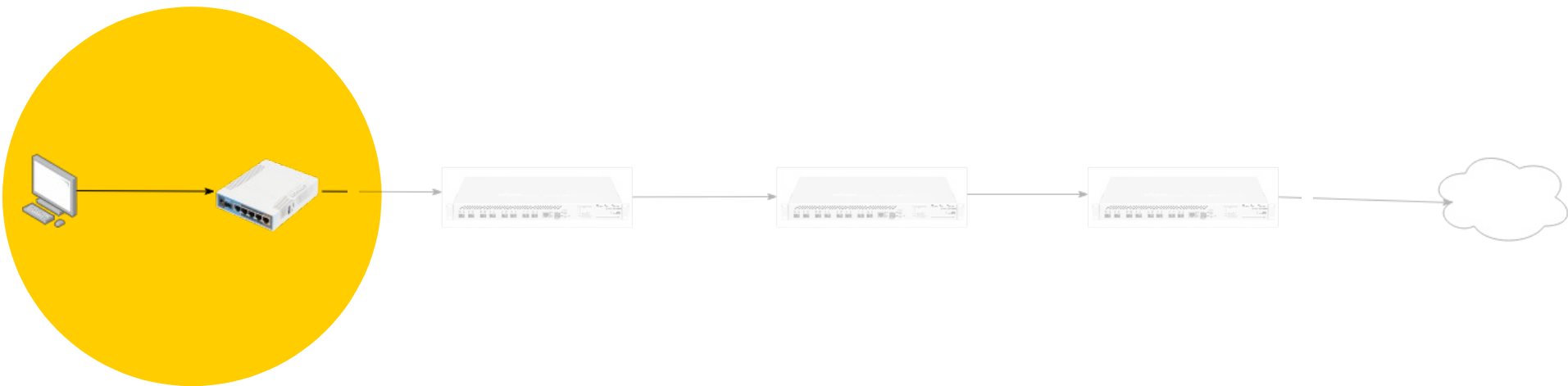
# Seguridad en la red

Cómo proteger las distintas capas de la red



## Topología de la Red de un ISP





# Seguridad en el CPE



## ¿Echaremos de menos NAT?

- NAT se inventó para prolongar la vida de IPv4
- “Falsa sensación de seguridad”
- NAT requiere “connection-tracking”



## Filtrado para CPE (sustituir NAT)

- Permitir sólo conexiones originadas por cliente
  - Permitir sólo direcciones IPv6 del cliente
  - Denegar todo el tráfico multicast in/out
  - Filtrar ICMPv6 (selectivamente)
- 
- RFC 6092, Recommended Simple Security in CPE for Residential IPv6



## Filtrado para CPE

IPv6 Firewall

Filter Rules Mangle Raw Connections Address Lists

+ - ✓ ✕ [Filter Icon] 00 Reset Counters 00 Reset All Counters Find all

#	Action	Chain	Src. Address	Dst. Address	Protocol	Src. Port	Dst. Port	In. In
;;; PERMITIR CONEXIONES ORIGINADAS POR CLIENTE								
0	✓ acc...	forward						
;;; PERMITIR SOLO DIRECCIONES IPv6 DEL CLIENTE								
1	✓ acc...	forward		2001:db8:1234::/64				
;;; DENEGAR MULTICAST								
2	✕ drop	forward						
;;; ICMP ECHO REPLY								
3	✓ acc...	forward			58 (icmpv6)			
;;; ICMP DESTINATION UNREACHABLE								
4	✓ acc...	forward			58 (icmpv6)			
;;; ICMP PACKET TOO BIG								
5	✓ acc...	forward			58 (icmpv6)			
;;; ICMP LIMIT EXCEED								
6	✓ acc...	forward			58 (icmpv6)			
;;; ICMP BAD HEADER								
7	✓ acc...	forward			58 (icmpv6)			
;;; DENEGAR WAN->LAN								
8	✕ drop	forward						

9 items



# Filtrado CPE: Conexiones Originadas por el Cliente

New Firewall Rule

General Advanced Extra Action Statistics

Chain **forward**

Src. Address

Dst. Address

Protocol

Src. Port:

Dst. Port:

Any. Port:

In. Interface

Out. Interface

In. Interface Lis  WAN

Out. Interface Lis

Packet Mark

Connection Mar

Connection Type

Connection Stat  invalid  established  related  new  untracked

New Firewall Rule

General Advanced Extra Action Statistics

Action **accept**

Log

Log Prefix





## Filtrado CPE: Sólo Direcciones del Cliente

New Firewall Rule

General | Advanced | Extra | Action | Statistics

Chain: forward

Src. Address: [Empty]

Dst. Address:  2001:db8:1234::/64

Protocol: [Empty]

Src. Port: [Empty]

Dst. Port: [Empty]

Any. Port: [Empty]

In. Interface: [Empty]

Out. Interface: [Empty]

In. Interface Lis:  WAN

Out. Interface Lis: [Empty]

Packet Mark: [Empty]



## Filtrado CPE: Denegar Tráfico Multicast

IPv6 Firewall

Filter Rules Mangle Raw Connections Address

+ - ✓ ✗ 📁 🏠

Name	Address	Time
MULTICAST	ff02::1	
MULTICAST	ff02::2	
MULTICAST	ff02::5	
MULTICAST	ff02::6	
MULTICAST	ff02::9	
MULTICAST	ff02::d	
MULTICAST	ff02::1:2	

New Firewall Rule

General Advanced Extra Action Statistics

Chain forward

Src. Address

Dst. Address New Firewall Rule

Protocol General Advanced Extra Action Statistics

Src. Address Lis

New Firewall Rule

General Advanced Extra Action Statistics

Action drop

Log

Log Prefix



# Filtrado CPE: Filtrado selectivo de ICMPv6

New Firewall Rule

General | Advanced | Extra | Action | Statistics

Chain: forward

Src. Address:

Dst. Address:

Protocol:  icmpv6

Src. Port:

Dst. Port:

Any. Port:

In. Interface:

Out. Interface:

In. Interface List:  WAN

Out. Interface List:

New Firewall Rule

General | Advanced | Extra | Action | Statistics

Src. Address List:

Dst. Address List:

New Firewall Rule

General | Advanced | Extra | Action | Statistics

Action: accept

Log

Log Prefix:

ICMP Options

ICMP Type:  echo reply

ICMP Code:

ICMP Options

ICMP Type:  destination unreachable

ICMP Code:

ICMP Options

ICMP Type:  packet too big

ICMP Code:

ICMP Options

ICMP Type:  limit exceeded

ICMP Code:

ICMP Options

ICMP Type:  bad header

ICMP Code:



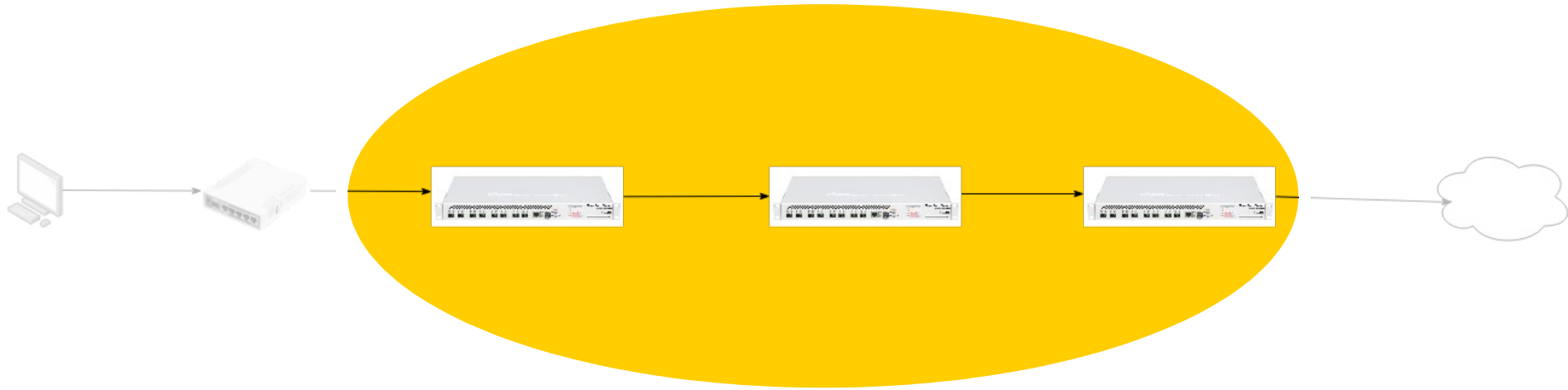
# Filtrado CPE: Filtrado selectivo de ICMPv6

The screenshot displays the Mikrotik WinBox interface for configuring a new firewall rule. The main window is titled "New Firewall Rule" and has tabs for General, Advanced, Extra, Action, and Statistics. The "General" tab is active, showing the following configuration:

- Chain: forward
- Src. Address: (empty)
- Dst. Address: (empty)
- Protocol:  icmpv6
- Src. Port: (empty)
- Dst. Port: (empty)
- Any. Port: (empty)
- In. Interface: (empty)
- Out. Interface: (empty)
- In. Interface List:  WAN
- Out. Interface List: (empty)
- Packet Mark: (empty)

Overlaid on the main window are two smaller windows showing the "Advanced" and "Action" tabs of the same rule configuration:

- The middle window shows the "Advanced" tab with "ICMP Options" expanded, where "ICMP Type" is set to "echo request" and "ICMP Code" is empty.
- The right window shows the "Action" tab where the action is set to "drop", "Log" is unchecked, and "Log Prefix" is empty.



# Seguridad en la red ISP - OSPFv3



## Ataques sobre OSPFv3

### Rogue Router

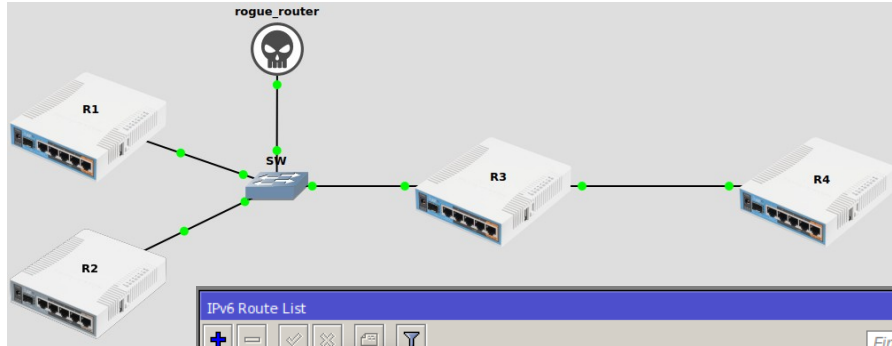
Un atacante con acceso a la red conecta un dispositivo y modifica la topología OSPFv3

### Router comprometido

Se altera la configuración de un Router legítimo que ha sido comprometido, alterando la información de enrutamiento



# Rogue OSPF-v3



IPv6 Route List

Dst. Address	Gateway	Distance
DAo ▶ ::/0	fe80::e79:d4ff:feac:9000%ether2 reachable	110
DAC ▶ 2001:db8::/64	ether1 reachable	0
DAC ▶ 2001:db8:34::/64	ether2 reachable	0
DAo ▶ 2001:db8:beef::/64	fe80::e79:d4ff:feac:9000%ether2 reachable	110
DAo ▶ 2001:db8:cafe::/64	fe80::e79:d4ff:feac:9000%ether2 reachable	110
DAo ▶ 2001:1234::/64	fe80::e79:d4ff:feac:9000%ether2 reachable	110
DAo ▶ 2001:abcd::/64	fe80::e79:d4ff:feac:9000%ether2 reachable	110

7 items

IPv6 Route List

Dst. Address	Gateway	Distance
DAo ▶ ::/0	fe80::e79:d4ff:feac:9000%ether2 reachable	110
DAC ▶ 2001:db8::/64	ether1 reachable	0
DAC ▶ 2001:db8:34::/64	ether2 reachable	0
DAo ▶ 2001:db8:beef::/64	fe80::e79:d4ff:feac:9000%ether2 reachable	110
DAo ▶ 2001:db8:cafe::/64	fe80::e79:d4ff:feac:9000%ether2 reachable	110
DAo ▶ 2001:1234::/64	fe80::e79:d4ff:feac:9000%ether2 reachable	110
DAo ▶ 2001:abcd::/64	fe80::e79:d4ff:feac:9000%ether2 reachable	110
DAo ▶ baca::/16	fe80::e79:d4ff:fe05:9900%ether1 reachable	110
DAo ▶ dead::/16	fe80::e79:d4ff:fe05:9900%ether1 reachable	110
DAo ▶ f0ca::/16	fe80::e79:d4ff:fe05:9900%ether1 reachable	110

10 items





# Autenticación en OSPF v2 y v3

## OSPFv2

- Autenticación

New OSPF

General Status

Interface: all

Cost: 10

Priority: 1

Authentication: none

Authentication Key: none

Authentication Key 1: 1

Network Type: broadcast

Instance ID: 0

Passive

Use BFD

Retransmit Interval: 5 s

Transmit Delay: 1 s

Hello Interval: 10 s

Router Dead Interval: 40 s

enabled passive State: down

## OSPFv3

- ¡Sin autenticación!

New OSPFv3

General Status

Area: backbone

Interface: all

Cost: 10

Priority: 1

Network Type: default

Instance ID: 0

Passive

Use BFD

Retransmit Interval: 5 s

Transmit Delay: 1 s

Hello Interval: 10 s

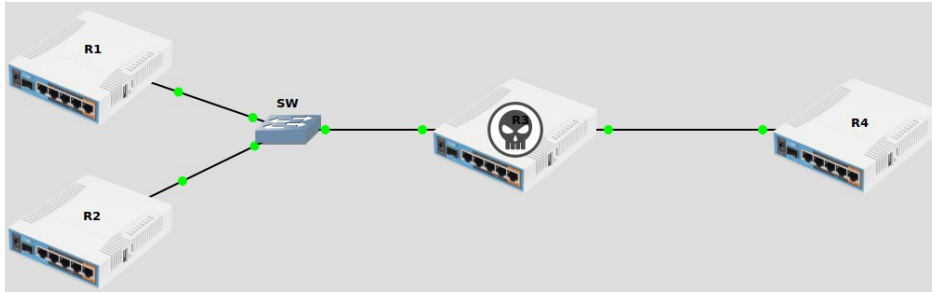
Router Dead Interval: 40 s

enabled passive inactive State: down





# Router Comprometido



IPv6 Route List

	Dst. Address	Gateway	Distance
DAo	::/0	fe80::e79:d4ff:feac:9000%ether2 reachable	110
DAC	2001:db8::/64	ether1 reachable	0
DAC	2001:db8:34::/64	ether2 reachable	0
DAo	2001:db8:beef::/64	fe80::e79:d4ff:feac:9000%ether2 reachable	110
DAo	2001:db8:cafe::/64	fe80::e79:d4ff:feac:9000%ether2 reachable	110
DAo	2001:1234::/64	fe80::e79:d4ff:feac:9000%ether2 reachable	110
DAo	2001:abcd::/64	fe80::e79:d4ff:feac:9000%ether2 reachable	110

7 items

IPv6 Route List

	Dst. Address	Gateway	Distance
DAo	::/0	fe80::e79:d4ff:feac:9000%ether2 reachable	110
DAC	2001:db8::/64	ether1 reachable	0
DAC	2001:db8:34::/64	ether2 reachable	0
DAo	2001:db8:beef::/64	fe80::e79:d4ff:feac:9000%ether2 reachable	110
DAo	2001:db8:cafe::/64	fe80::e79:d4ff:feac:9000%ether2 reachable	110
DAo	2001:1234::/64	fe80::e79:d4ff:feac:9000%ether2 reachable	110
DAo	2001:abcd::/64	fe80::e79:d4ff:feac:9000%ether2 reachable	110
DAo	baca::/16	fe80::e79:d4ff:fe05:9900%ether1 reachable	110
DAo	dead::/16	fe80::e79:d4ff:fe05:9900%ether1 reachable	110
DAo	f0ca::/16	fe80::e79:d4ff:fe05:9900%ether1 reachable	110

10 items



## Seguridad OSPF-v3

---

- Desactivar la instancia si no se utiliza
- Todos los interfaces **passive**
- Sólo interfaces necesarios **active**



## Protección de OSPF-v3

- Proteger la capa 2
- Aceptar multicast a FF02:5 y FF02:6 sólo desde IP conocidas
- Utilizar IPSec



# Filtrado Multicast OSPF-v3

IPv6 Firewall

Filter Rules Mangle Raw Connection: Address Lists

Name	Address	Timeout
OSPF_ROUTERS	fe80::e79:d4ff:fee8:df00	
OSPF_ROUTERS	fe80::e79:d4ff:fefc:9c00	

Firewall IPv6 Address List <OSPF\_ROUTERS>

Name: OSPF\_ROUTERS

Address: fe80::e79:d4ff:fefc:9c00

Timeout: [ ]

2 items (1 selected) enabled

IPv6 Firewall

Filter Rules Mangle Raw Connections Address Lists

#	Action	Chain	Src. Address	Dst. Ad
0	drop	input		ff02::5
1	drop	input		ff02::6

2 items (1 selected)

Firewall Rule <ff02::5>

General Advanced Extra Action Statistics

Chain: input

Src. Address: [ ]

Dst. Address: ff02::5

OK Cancel Apply Disable

Firewall Rule <ff02::5>

General Advanced Extra Action Statistics

Src. Address List: OSPF\_ROUTERS

OK Cancel

Firewall Rule <ff02::5>

General Advanced Extra Action Statistics

Action: drop

Log

Log Prefix: [ ]

OK Cancel Apply Disable Comment



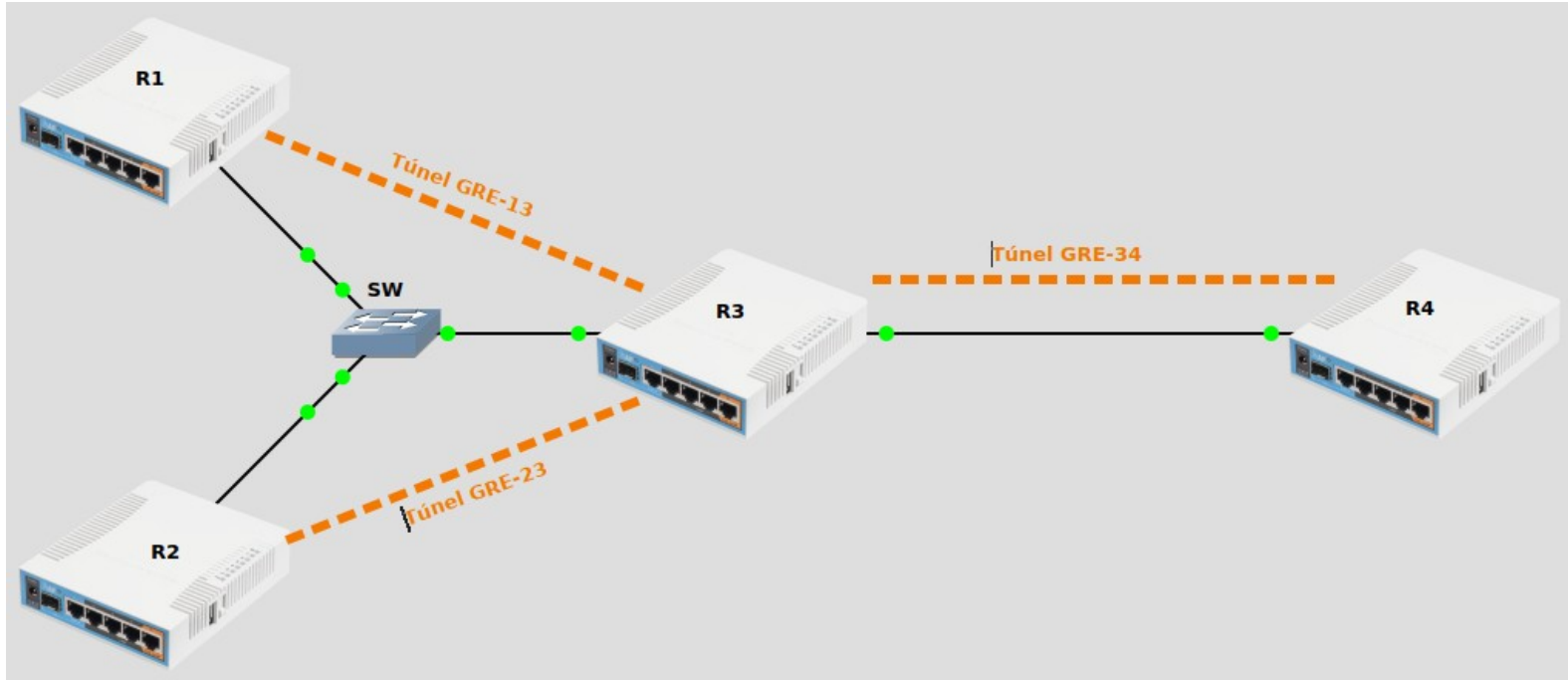
## IPSec en OSPF-v3

---

- ⦿ IPSec no puede transmitir tráfico multicast
- ⦿ OSPF-v3 no puede utilizarse directamente sobre IPSec
- ⦿ Pueden usarse túneles GRE6

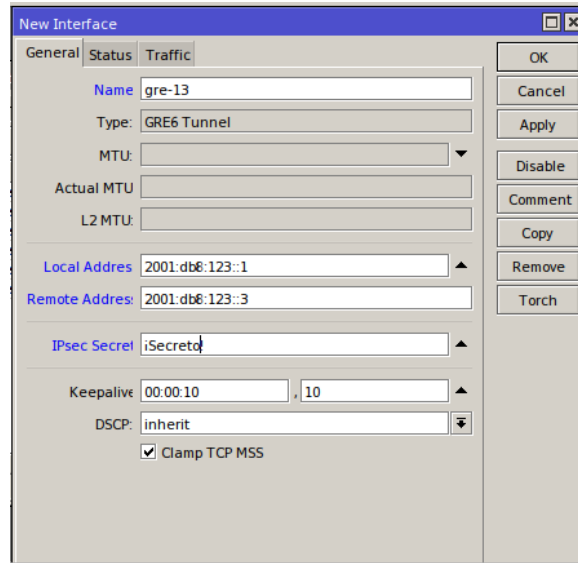
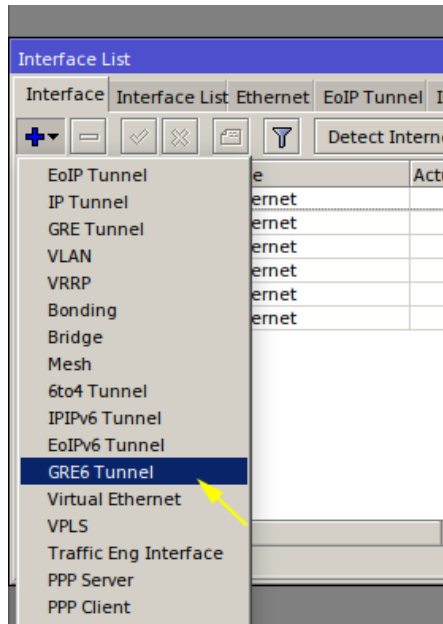


## IPSec en OSPF-v3: How To

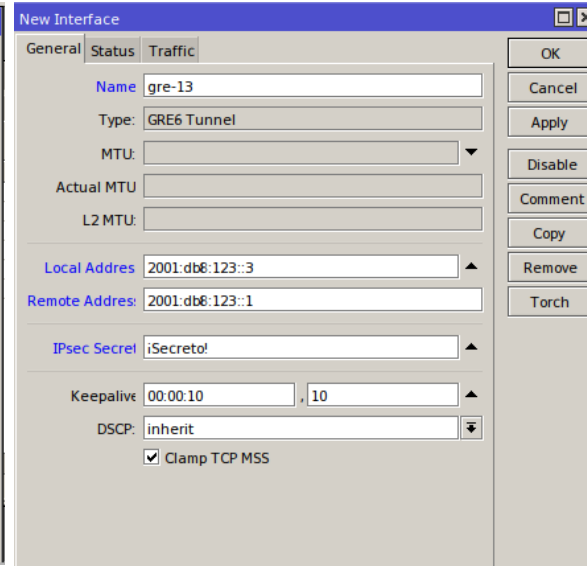




# IPSec en OSPF-v3: Túnel GRE



Router R1



Router R3



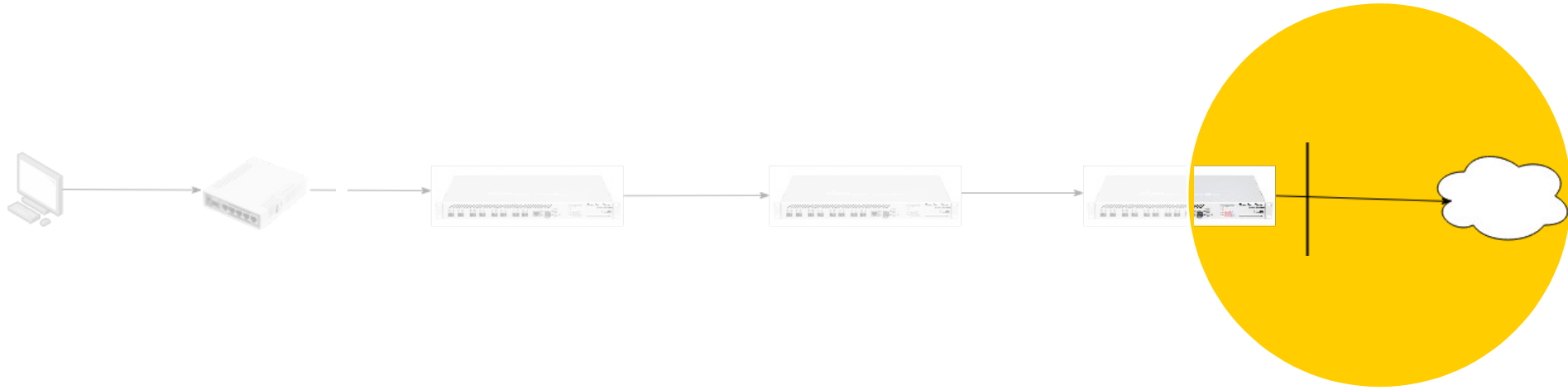
## IPSec en OSPF-v3: Interfaces

The screenshot displays the Mikrotik WinBox interface for configuring OSPFv3. The main window is titled 'New OSPFv3' and is currently on the 'General' tab. The configuration is for the 'backbone' area on the 'gre-13' interface. The network type is set to 'point to point'. The instance ID is 0, and the 'Passive' and 'Use BFD' options are unchecked. The following table summarizes the configuration parameters:

Parameter	Value
Area	backbone
Interface	gre-13
Cost	10
Priority	1
Network Type	point to point
Instance ID	0
Passive	<input type="checkbox"/>
Use BFD	<input type="checkbox"/>
Retransmit Interval	5 s
Transmit Delay	1 s
Hello Interval	10 s
Router Dead Interval	40 s

The status bar at the bottom of the dialog indicates 'State: down'. The background shows the 'OSPFv3' configuration page with a table for 'Area' and 'Interface' columns, currently empty (0 items).

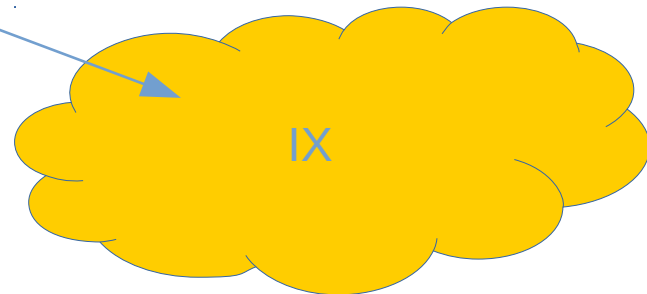
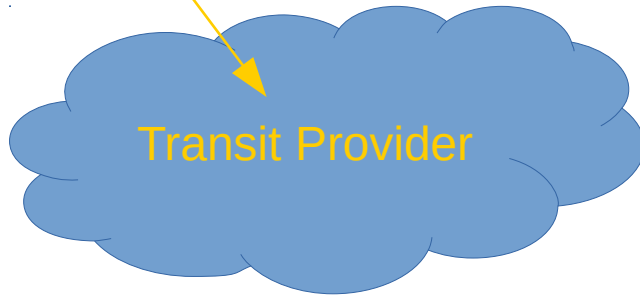




# Seguridad en el PE



## Amenazas





## Amenazas

---

- BGP no protegido
- Tráfico entrante/saliente bogons/martians
- Tráfico no deseado RFC 4890



## Proteger el PE

BGP

Bogons &  
Martians

Tráfico no  
deseado



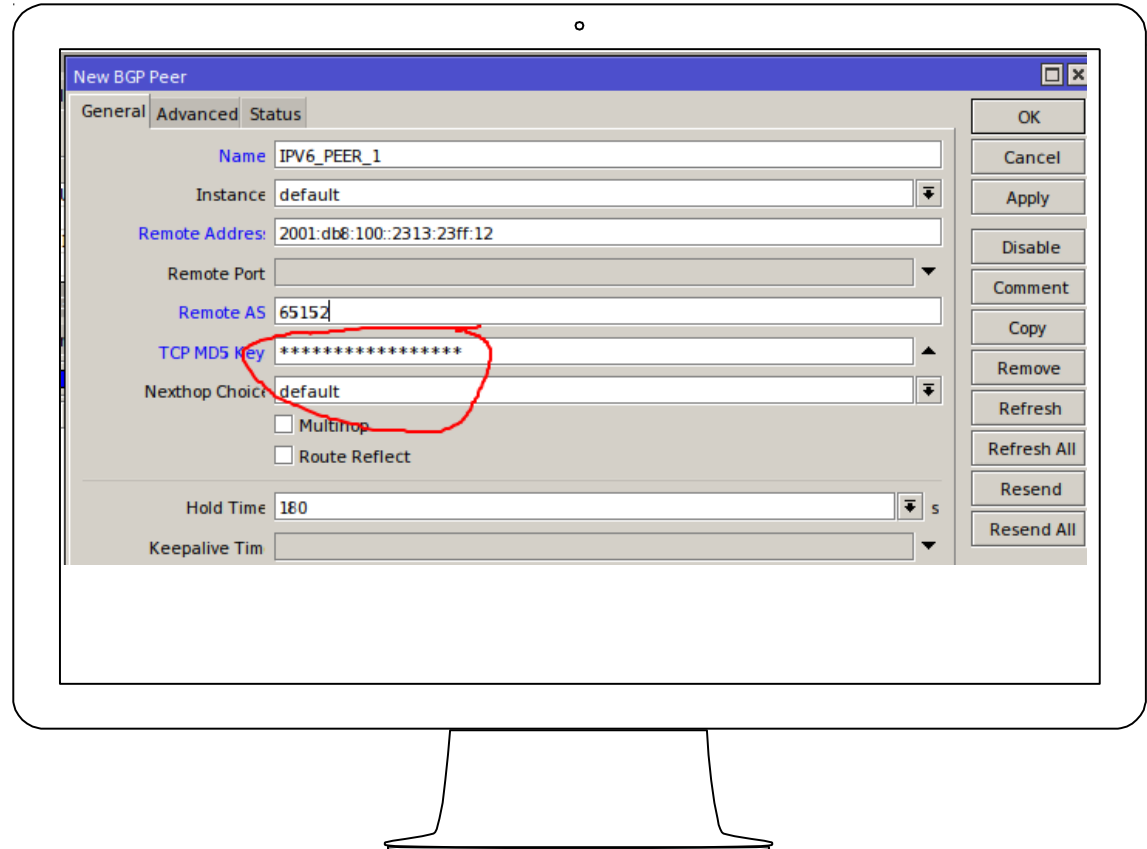
## Fortificar BGP

---

- Desactivar la instancia si no se utiliza
- Utilizar clave MD5
- Filtros en Firewall para PEERS



# BGP: MD5





# Filtrado Peers

**New Firewall Rule**

General | Advanced | Extra | Action | Statistics

Chain

Src. Address

Dst. Address

Protocol  6 (tcp)

Src. Port:

Dst. Port:  179

Any. Port:

In. Interface:

**New Firewall Rule**

General | Advanced | Extra | Action | Statistics

Action

Log

Log Prefix

**New Firewall Rule**

General | Advanced | Extra | Action | Statistics

Src. Address Lis !

Dst. Address List

Content

**IPv6 Firewall**

Filter Rules | Mangle | Raw | Connections | Address Lists

+ - ✓ ✕ 📄 🔍

Name contains BGP\_PEER

Name	Address	Timeout
🟢 BGP_PEER	2001:db8:10::123f:ab...	
🟢 BGP_PEER	2001:db8:18::abc:123..	



## Proteger el PE

BGP

Bogons &  
Martians

Tráfico no  
deseado





## Prefijos a filtrar

- Martians: prefijos no válidos para su uso en Internet
- Bogons: prefijos válidos sin asignar por IANA a RIR
- Full-bogons: prefijos asignados a RIR pero no a ISP

**¡Se usan como dirección origen de ataques!**



## Martians & Bogons

Direcciones a bloquear	Descripción
::	Dirección no especificada
::1	Dirección de Loopback
::/96	Direcciones IPv4-compatibles
::ffff:0.0.0.0/96	Direcciones IPv4-mapeadas (obsoletas)
::0.0.0.0/96	Direcciones de túneles (obsoletas)



## Martians & Bogons (2)

Direcciones a bloquear	Descripción
Fe80::/10	Direcciones de enlace local
Fec0::/10	Direcciones site-local (obsoletas)
Fc00::/7	Direcciones unique-local
Ff00::/8	Direcciones multicast (sólo como origen)
2001:db8::/32	Dirección de documentación



## Martians & Bogons (3)

Direcciones a bloquear		Descripción
<code>::224.0.0.0/100</code> <code>::127.0.0.0/104</code>	<code>::0.0.0.0/104</code> <code>::255.0.0.0/104</code>	Otras direcciones compatibles
<code>2002:e000::/20</code> <code>2002:7f00::/24</code> <code>2002:0a00::/24</code> <code>2002:ac10::/28</code>	<code>2002::/24</code> <code>2002:ff00::/24</code> <code>2002:c0a8::/32</code>	Direcciones falsas 6to4



# Lista Completa: Bogons

<https://www.team-cymru.org/Services/Bogons/fullbogons-ipv6.txt>



# Bogons: Filtrado

New Firewall Rule

General Advanced Extra Action ...

Chain **forward**

Src. Address **New Firewall Rule**

Dst. Address **General Advanced Extra Action Statistics**

Protocol **Src. Address List** **MARTIANS**

Src. Port **Dst. Address List**

Dst. Port **Content**

Any. Port **Connection Bytes**

In. Interface **Connection Data**

Out. Interface

New Firewall Rule

General Advanced Extra Action Statistics

Action **drop**

Log

Log Prefix

OK

Cancel

Apply

Disable

Comment

IPv6 Firewall

Filter Rules Mangle Raw Connections Address List

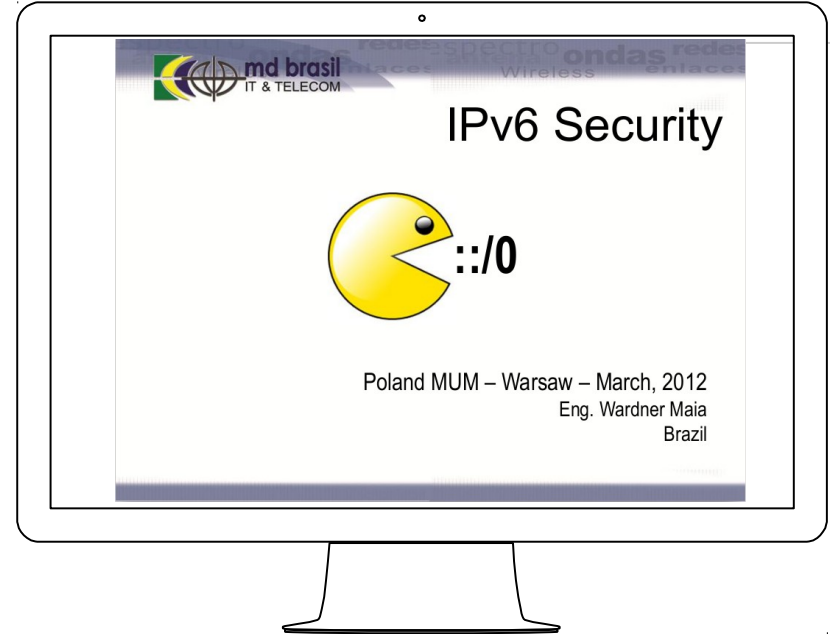
+ - ✓ ✗ 📁 🗑️

Name	Address	Timeout
MARTIANS	::/0	
MARTIANS	::1	
MARTIANS	::/96	
MARTIANS	::ffff:0:0:0:0/0	
MARTIANS	fe80::/10	
MARTIANS	fec0::/10	
MARTIANS	0000::/10	
MARTIANS	0000::/8	



## Bogons: Filtrado

- BGP Peering con Cymru
  - Filtrado automático de B&M
- Script Address List de B&M Cymru
  - Filtrado FW entrante





## Proteger el PE

BGP

Bogons &  
Martians

Tráfico no  
deseado





## RFC 4890: Recomendaciones filtros ICMPv6 en FW

● Reglas para:

- FW de tránsito (**chain=forward**)
- Interfaces del FW (**chain=input**)



## **RFC 4890: Recomendaciones filtros ICMPv6 en FW**

- ◎ Categorías de Reglas para los mensajes:
  - No deben ser bloqueados
  - No deberían ser bloqueados
  - Deben ser bloqueados
  - Los administradores deben decidir si bloquear
  - Los administradores deben considerar bloquear



## **RFC 4890: ICMPv6 que no debe eliminarse**

Mensajes de error esenciales:

- Destination Unreachable (Tipo 1) – todos los códigos
- Packet Too Big (Tipo 2)
- Time Exceeded (Tipo 3) sólo código 0
- Parameter Problem (Tipo 4) sólo códigos 1 y 2



## **RFC 4890: ICMPv6 que no debe eliminarse (2)**

Mensajes de comprobación de conectividad:

- Echo Request (Tipo 128)
- Echo Response (Tipo 129)



## **RFC 4890: ICMPv6 normalmente no debe eliminarse**

Otros mensajes de error

- Time Exceeded (Tipo 3) código 1
- Parameter Problem(Tipo 4) código 0



## **RFC 4890: ICMPv6 normalmente no debe eliminarse (2)**

Mensajes para asistencia en movilidad:

- Home Agent Address Discovery Request (Tipo 144)
- Home Agent Address Discovery Reply (Tipo 145)
- Mobile Prefix Solicitation (Tipo 146)
- Mobile Prefix Advertisement (Tipo 147)



## **RFC 4890: ICMPv6 normalmente se elimina**

Mensajes Address Conf. Y Router Sel. (deben recibirse con hop limit = 255)

- Router Solicitation (Tipo 133)
- Router Advertisement (Tipo 134)
- Neighbor Solicitation (Tipo 135)
- Neighbor Advertisement (Tipo 136)



## **RFC 4890: ICMPv6 normalmente se elimina (2)**

- Redirect (Tipo 137)
- Inverse Neighbor Discovery Solicitation (Tipo 141)
- Inverse Neighbor Discovery Advert. (Tipo 142)





## **RFC 4890: ICMPv6 normalmente se elimina (3)**

Link-local multicast receiver notification messages  
(deben recibirse con dirección de origen link-local)

- Listener Query (Tipo 130)
- Listener Report (Tipo 131)
- Listener Done (Tipo 132)
- Listener Report v2 (Tipo 143)



## **RFC 4890: ICMPv6 normalmente se elimina (4)**

Mensajes de notificación SEND Certificate Path (deben recibirse con hop limit = 255)

- Certificate Path Solicitation (Tipo 148)
- Certificate Path Advertisement (Tipo 149)



## **RFC 4890: ICMPv6 normalmente se elimina (5)**

Mensajes Multicast Router Discovery (deben recibirse con hop limit = 1 y dirección de origen link-local)

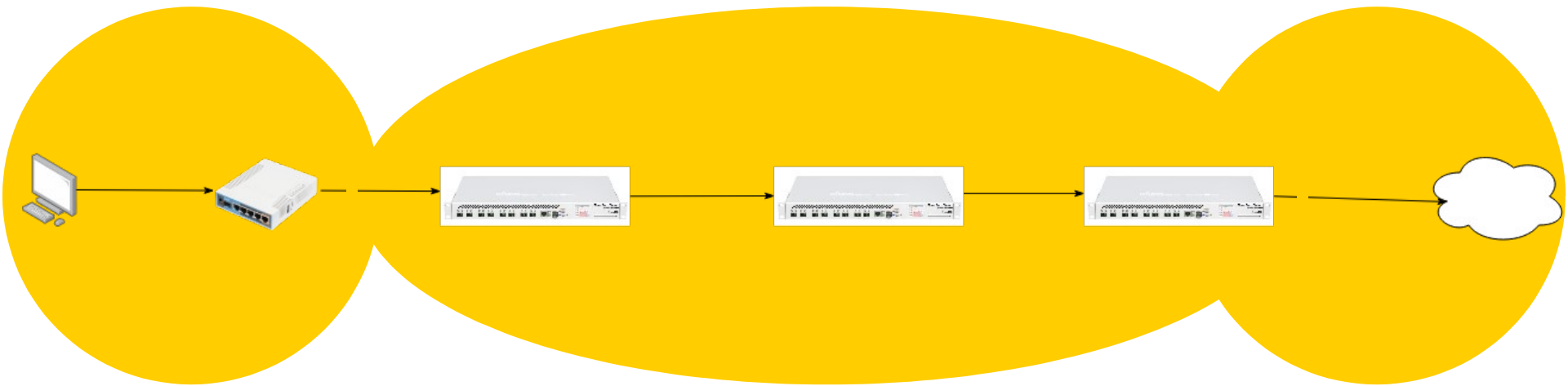
- Multicast Router Advertisement (Tipo 151)
- Multicast Router Solicitation (Tipo 152)
- Multicast Router Termination (Tipo 153)



# RFC 4890

The screenshot shows the IPv6 Firewall configuration interface in WinBox. The 'Filter Rules' tab is active, displaying a list of rules for the 'rfc4890' chain. Each rule is associated with a specific ICMPv6 error code and has an 'accept' action. The table below represents the data shown in the screenshot.

#	Action	Chain	Protocol	ICMP Options/ICMP Type	ICMP Options...	Limit/Rate	Limit/Burst
;;; DESTINATION UNREACHABLE							
0	✓ accept	rfc4890	58 (icmpv6)	1 (destination unreacha...			
;;; PACKET TOO BIG							
1	✓ accept	rfc4890	58 (icmpv6)	2 (packet too big)			
;;; TIME EXCEED							
2	✓ accept	rfc4890	58 (icmpv6)	3 (limit exceeded)		0	
;;; PARAMETER PROBLEM							
3	✓ accept	rfc4890	58 (icmpv6)	4 (bad header)		1-2	
;;; ECHO REQUEST							
4	✓ accept	rfc4890	58 (icmpv6)	128 (echo request)		3/sec	5
;;; ECHO REPLY							
5	✓ accept	rfc4890	58 (icmpv6)	129 (echo reply)		3/sec	5
;;; TIME EXCEED (code 1)							
6	✓ accept	rfc4890	58 (icmpv6)	3 (limit exceeded)		1	
;;; PARAMETER PROBLEM (code 0)							
7	✓ accept	rfc4890	58 (icmpv6)	4 (bad header)		0	
;;; HOME AGENT ADDRESS DISCOVERY REQUEST							
8	✓ accept	rfc4890	58 (icmpv6)	144			
;;; HOME AGENT ADDRESS DISCOVERY REPLY							



# Seguridad en la Red



---

# Entonces...

*...¿se acabaron los  
problemas de  
seguridad?*



## La Seguridad...

- ⦿ No es un producto, sino un proceso
- ⦿ Debe ser, principalmente, proactiva...  
... y no reactiva
- ⦿ No tiene por qué ser complicada



## Si van a implantar IPv6

- Asesórense
- Fórmense
- Tengan en cuenta las RFC
  
- Traten de hacerlo seguro desde el inicio





# Recuerden...





# ¡Gracias!

## ¿Preguntas?

Puedes contactar conmigo en

- @jprietove
- info@jprietove.com



## Bibliografía y Referencias

- Maia, Wardner; IPv6 Security, Poland MUM Marzo 2012; <http://bit.ly/IPv6Maia>
- García Rambla, Juan Luis; Ataques en redes de datos IPv4 e IPv6, Ed.OxWord; <http://bit.ly/IPv6IPv4Ataques>
- Grundemann, Chris; Security in an IPv6 World, Myths & Reality; <http://bit.ly/IPv6Myths>
- ISP Workshops; Hardening IPv6 Network Devices; <http://bit.ly/IPv6HardDevice>
- Gont, F; Chown, T; Network Reconnaissance in IPv6 Networks IETF Draft; <http://bit.ly/IPv6ScanDraft>
- THC-IPv6-Attack-Toolkit, <http://bit.ly/IPv6THC>
- RFC 4301 Security Architecture for the Internet Protocol, <http://bit.ly/IPv6RFC4301>
- RFC 4890 Recommendations for Filtering ICMPv6 Messages in Firewalls, <http://bit.ly/IPv6RFC4890>
- RFC 6092 Recommended Simple Sec. Cap. in CPE for Residential IPv6, <http://bit.ly/IPv6RFC6092>
- RFC 7217 A method for generating semantically opaque IID with IPv6 SLAAC, <http://bit.ly/IPv6RFC7217>
- RFC 7707 Network Reconnaissance in IPv6 Networks, <http://bit.ly/IPv6RFC7707>
- RFC 8200 Internet Protocol, Version 6 (IPv6) Specification, <http://bit.ly/IPv6RFC8200>

---

5

# Anexos

---



## Reglas Filtrado Evitar Ping

### Pág. 18

- /ipv6 firewall filter  
add action=drop chain=input icmp-options=128:0-255 protocol=icmpv6



## Reglas Filtrado Ping Multicast Pág. 25

- `/ipv6 firewall address-list`
- `add address=ff02::1/128 list=MULTICAST`
- `add address=ff02::2/128 list=MULTICAST`
- `add address=ff02::5/128 list=MULTICAST`
- `add address=ff02::6/128 list=MULTICAST`
- `add address=ff02::9/128 list=MULTICAST`
- `add address=ff02::d/128 list=MULTICAST`
- `add address=ff02::1:2/128 list=MULTICAST`
- `/ipv6 firewall filter`
- `add action=drop chain=input dst-address-list=MULTICAST icmp-options=128:0-255 \`  
`protocol=icmpv6`



## Reglas Filtrado CPE Pág. 63. (1 de 2)

- /ipv6 firewall filter
- add action=accept chain=forward comment=\
- "PERMITIR CONEXIONES ORIGINADAS POR CLIENTE" connection-state=\
- established,related,untracked in-interface-list=WAN
- add action=accept chain=forward comment=\
- "PERMITIR S\D3LO DIRECCIONES IPv6 DEL CLIENTE" dst-address=\
- 2001:db8:1234::/64 in-interface-list=WAN
- add action=drop chain=forward comment="DENEGAR MULTICAST" dst-address-list=\
- MULTICAST
- add action=accept chain=forward comment="ICMP ECHO REPLY" icmp-options=\
- 129:0-255 in-interface-list=WAN protocol=icmpv6



## Reglas Filtrado CPE Pág. 63. (2 de 2)

- `add action=accept chain=forward comment="ICMP DESTINATION UNREACHABLE" \`  
  `icmp-options=1:0-255 in-interface-list=WAN protocol=icmpv6`
- `add action=accept chain=forward comment="ICMP PACKET TOO BIG" icmp-options=\`  
  `2:0-255 in-interface-list=WAN protocol=icmpv6`
- `add action=accept chain=forward comment="ICMP LIMIT EXCEED" icmp-options=\`  
  `3:0-255 in-interface-list=WAN protocol=icmpv6`
- `add action=accept chain=forward comment="ICMP BAD HEADER" icmp-options=\`  
  `4:0-255 in-interface-list=WAN protocol=icmpv6`
- `add action=drop chain=forward comment="DENEGAR WAN->LAN" in-interface-list=\`  
  `WAN`





## Reglas Filtrado OSPF-v3

### Pág. 76.

- /ipv6 firewall filter
- add chain=input dst-address=ff02::5 src-address-list=!OSPF\_ROUTERS action=drop
- add chain=input dst-address=ff02::6 src-address-list=!OSPF\_ROUTERS action=drop



## IPSec en OSPF-v3. Túnel Gre. Pág. 79

- `## Router 1`
- `/interface gre6`
- `add ipsec-secret="\A1Secreto!" local-address=2001:db8:123::1 name=gre-13 \`
- `remote-address=2001:db8:123::3`
- `/routing ospf-v3 interface`
- `add area=backbone interface=gre-13 network-type=point-to-point`
- 
- `## Router 3`
- `/interface gre6`
- `add ipsec-secret="\A1Secreto!" local-address=2001:db8:123::3 name=gre-13 \`
- `remote-address=2001:db8:123::1`
- `/routing ospf-v3 interface`
- `add area=backbone interface=gre-13 network-type=point-to-point`



## Regla de Filtrado BGP Peer. Pág. 87

- `/ipv6 firewall filter add chain=input protocol=tcp dst-port=179 src-address-list=!BGP_PEER action=drop`



## Regla de Filtrado Bogons. (1 de 2). Pág. 94

- `/ipv6 firewall address-list`
- `add list=MARTIANS`
- `add address>::1/128 list=MARTIANS`
- `add address>::/96 list=MARTIANS`
- `add address>::ffff:0.0.0.0/96 list=MARTIANS`
- `add address=fe80::/10 list=MARTIANS`
- `add address=fec0::/10 list=MARTIANS`
- `add address=fc00::/10 list=MARTIANS`
- `add address=ff00::/8 list=MARTIANS`
- `add address=2001:db8::/32 list=MARTIANS`
- `add address>::224.0.0.0/100 list=MARTIANS`
- `add address>::127.0.0.0/104 list=MARTIANS`
- `add address>::/104 list=MARTIANS`



## Regla de Filtrado Bogons. (2 de 2). Pág. 94

- /ipv6 firewall address-list
- add address=::255.0.0.0/104 list=MARTIANS
- add address=2002:e000::/20 list=MARTIANS
- add address=2002:7f00::/24 list=MARTIANS
- add address=2002:a00::/24 list=MARTIANS
- add address=2002:ac10::/28 list=MARTIANS
- add address=2002::/24 list=MARTIANS
- add address=2002:ff00::/24 list=MARTIANS
- add address=2002:c0a8::/32 list=MARTIANS



## RFC 4890. (1 de 7). Pág. 108

- /ipv6 firewall filter
- add action=accept chain=rfc4890 comment="DESTINATION UNREACHABLE" \  
icmp-options=1:0-255 protocol=icmpv6
- add action=accept chain=rfc4890 comment="PACKET TOO BIG" icmp-options=2:0-255 \  
protocol=icmpv6
- add action=accept chain=rfc4890 comment="TIME EXCEED" icmp-options=3:0 \  
protocol=icmpv6
- add action=accept chain=rfc4890 comment="PARAMETER PROBLEM" icmp-options=\  
4:1-2 protocol=icmpv6



## RFC 4890. (2 de 7). Pág. 108

- /ipv6 firewall filter
- add action=accept chain=rfc4890 comment="ECHO REQUEST" icmp-options=128:0-255 \  
limit=3,5:packet protocol=icmpv6
- add action=accept chain=rfc4890 comment="ECHO REPLY" icmp-options=129:0-255 \  
limit=3,5:packet protocol=icmpv6



## RFC 4890. (4 de 7). Pág. 108

- /ipv6 firewall filter
- add action=accept chain=rfc4890 comment=\
- "HOME AGENT ADDRESS DISCOVERY REQUEST" icmp-options=144:0-255 protocol=\
- icmpv6
- add action=accept chain=rfc4890 comment="HOME AGENT ADDRESS DISCOVERY REPLY" \
- icmp-options=145:0-255 protocol=icmpv6
- add action=accept chain=rfc4890 comment="MOBILE PREFIX SOLICITATION" \
- icmp-options=146:0-255 protocol=icmpv6
- add action=accept chain=rfc4890 comment="MOBILE PREFIX ADVERTISEMENT" \
- icmp-options=147:0-255 protocol=icmpv6





## RFC 4890. (5 de 7). Pág. 108

- /ipv6 firewall filter
- add action=drop chain=rfc4890 comment="ROUTER SOLICITATION" icmp-options=\
- 133:0-255 protocol=icmpv6
- add action=drop chain=rfc4890 comment="ROUTER ADVERTISEMENT" icmp-options=\
- 134:0-255 protocol=icmpv6
- add action=drop chain=rfc4890 comment="NEIGHBOR SOLICITATION" icmp-options=\
- 135:0-255 protocol=icmpv6
- add action=drop chain=rfc4890 comment="NEIGHBOR ADVERTISEMENT" icmp-options=\
- 136:0-255 protocol=icmpv6



## RFC 4890. (6 de 7). Pág. 108

- /ipv6 firewall filter
- add action=drop chain=rfc4890 comment=REDIRECT icmp-options=137:0-255 \  
protocol=icmpv6
- add action=drop chain=rfc4890 comment=\  
"INVERSE NEIGHBOR DISCOVERY SOLICITATION" icmp-options=141:0-255 \  
protocol=icmpv6
- add action=drop chain=rfc4890 comment=\  
"INVERSE NEIGHBOR DISCOVERY ADVERTISEMENT" icmp-options=142:0-255 \  
protocol=icmpv6



## RFC 4890. (7 de 7). Pág. 108

- `/ipv6 firewall filter`
- `add action=drop chain=rfc4890 comment="LISTENER QUERY" icmp-options=130:0-255 \`
- `protocol=icmpv6`
- `add action=drop chain=rfc4890 comment="LISTENER REPORT" icmp-options=\`
- `131:0-255 protocol=icmpv6`
- `add action=drop chain=rfc4890 comment="LISTENER DONE" icmp-options=132:0-255 \`
- `protocol=icmpv6`
- `add action=drop chain=rfc4890 comment="LISTENER REPORT V2" icmp-options=\`
- `143:0-255 protocol=icmpv6`
- `/ipv6 firewall filter`
- `add action=drop chain=rfc4890 comment="DROP THE REST OF ICMPv6" protocol=\`
- `icmpv6`