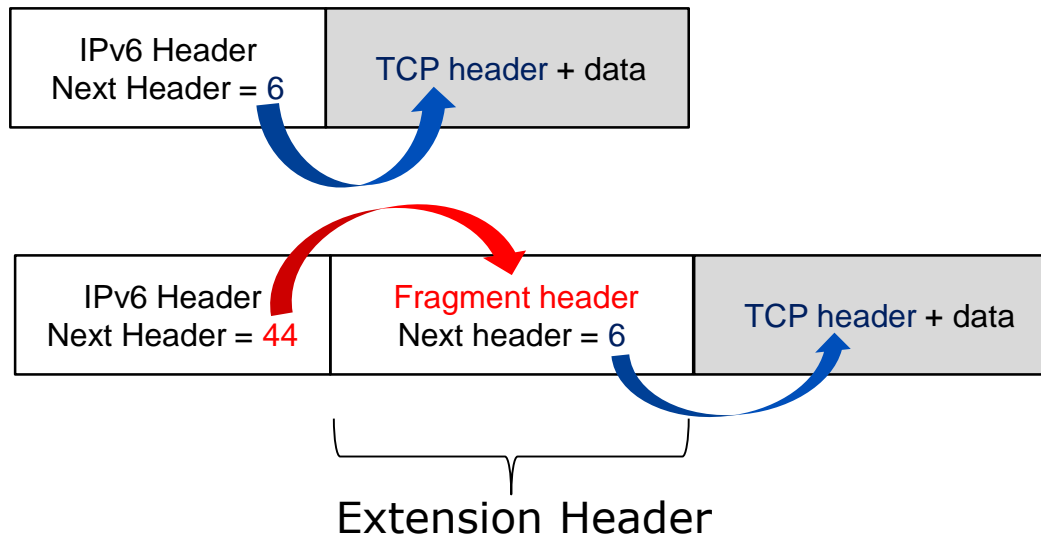


# IPv6 Security

# Remember Extension Headers?

- IPv6 allows an optional *Extension Header* in between the IPv6 header and upper layer header
  - Allows adding new features to IPv6 protocol without major re-engineering



## Next Header values:

- 0 Hop-by-hop option
- 2 ICMP
- 4 SRH
- 6 TCP
- 17 UDP
- 43 Source routing (**RFC5095**)
- 44 Fragmentation
- 50 Encrypted security payload
- 51 Authentication
- 59 Null (No next header)
- 60 Destination option

# Extension Headers

Next Header Value	Name	Function	Remarks
0	Hop-by-Hop	To carry additional information (Ex: RSVP)	Must be examined by every node along the path
43	Routing Header	List nodes to be visited on its way to the destination	<b><i>Deprecated by RFC 5095</i></b>
44	Fragment Header	To fragment packets that do not fit the path MTU	By the source node
60	Destination Options	To carry optional information	Examined only by destination node

# EHs - security nightmare?

- **RFC8200** states:
  - “Extension headers (except for Hop-by-Hop Options header) are **not processed, inserted, or deleted by any node along a packet's delivery path**, until the packet reaches the node”
    - **Firewalls (stateful/stateless) should not inspect them?**
  - But destination nodes **must accept and process EH...**
    - “**any order** and occurring **any number** of times in the same packet”

# EHs - security nightmare?

- The number of EH is **NOT** limited
- The number of options within an Options header (*Hop-by-hop* and *Destinations*) is **NOT** limited
- The order of EH is **NOT** defined (only a recommendation)
  - RFC2460/8200 "it is **recommended** that those headers appear in the following order"

# Possible EH threat – covert channel

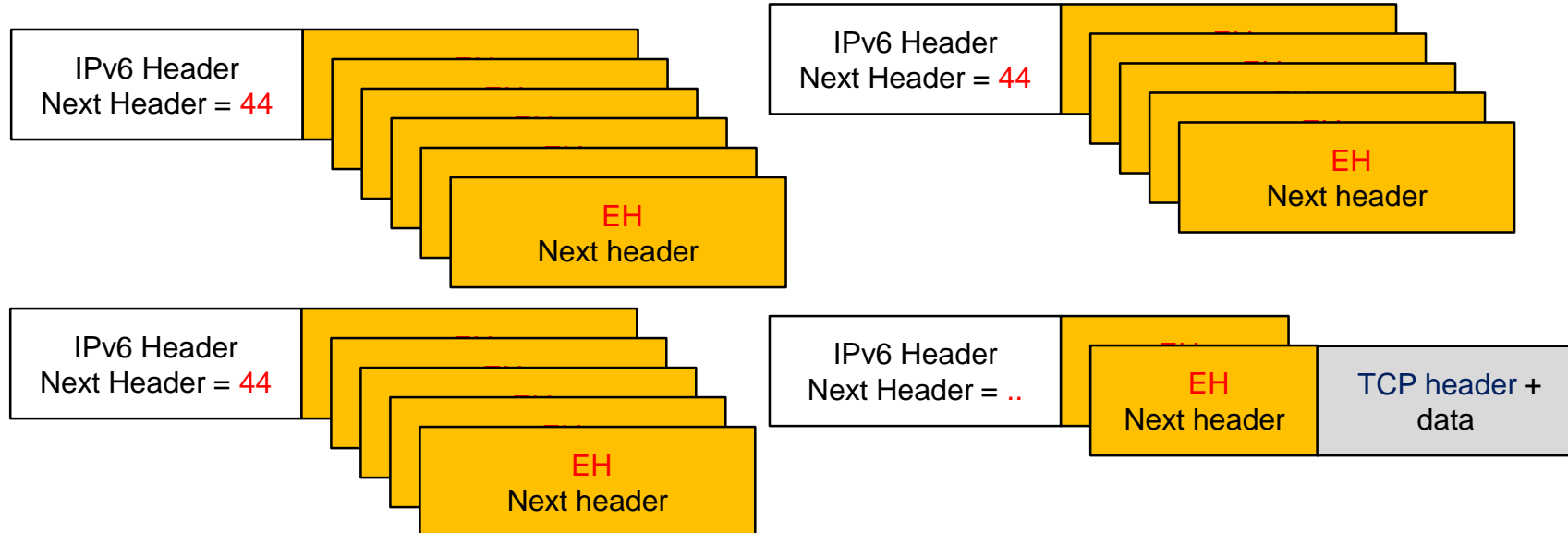
- Use the EH as a covert channel to exchange information (payload) undetected



- Mitigation:
  - **Drop** unknown EH
  - Which means you need to inspect EH

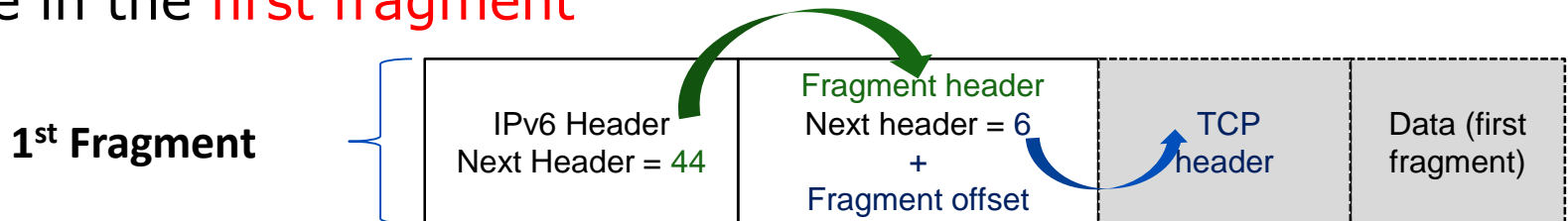
# Possible EH threat – Unlimited EHs

- Send packets with huge number of EH
  - EH chain itself is fragmented (L4 info could appear in N<sup>th</sup>-fragment)
  - Overwhelm the destination node (DOS)
  - Evade IPS/IDS/Firewall



# EH and Fragments

- Should we **DROP** all IPv6 fragments?
  - How does services like DNSSEC work?
- **RFC7112**
  - “When a host **fragments** an IPv6 datagram, it **MUST** include the entire IPv6 Header Chain in the **First Fragment**”
    - **inspect and drop**
- **RFC8200:**
  - “**Extension headers**, if any, and **Upper-Layer** headers **MUST** be in the **first fragment**”





# EH and Fragments

- If you don't want stateful inspection, you can use proprietary solutions
  - **undetermined-transport** (Cisco)
    - Drop fragments that do not have upper-layer headers in the first fragment (**satisfies RFC7112/8200**)  
`deny any any [undetermined-transport]`

# ICMPv6 is important!

## ICMPv6 Message Types

### Error-Messages (1-127)

1:Destination Unreachable 2:Packet too big (PMTUD)  
3:Time Exceeded (Hop Limit) 4:Parameter Problem

### Info-Messages (Ping)

128:Echo Request 129:Echo Reply

### Multicast Listener Discovery (MLD, MLD2)

130:Multicast Listener Query 131/143:Multicast Listener Report/2  
132:Multicast Listener Done

### Neighbor Discovery (NDP), **Stateless Autoconfiguration (SLAAC)**

133:Router Solicitation 134:**Router Advertisement**  
135:**Neighbor Solicitation (DAD)** 136:Neighbor Advertisement (DAD)  
137:Redirect Message

### Other (Router Renumbering, Mobile IPv6, Inverse NS/NA,...)

138-153

<http://www.iana.org/assignments/icmpv6-parameters/icmpv6-parameters.xhtml>

# Filtering ICMPv6 (perimeter)

- Filtering ICMPv6 is not straight forward
  - You block ICMPv6 => you break IPv6!
- **RFC4890**: “ICMPv6 Filtering Recommendations”
  - **Permit** Error messages
    - Destination Unreachable (Type 1) - All codes
    - Packet Too Big (Type 2)
    - Time Exceeded (Type 3) - Code 0 only
    - Parameter Problem (Type 4) - Codes 1 and 2 only
  - **Permit** Connectivity check messages
    - Echo Request (Type 128)
    - Echo Response (Type 129)

# Filtering ICMPv6 (perimeter)

- Some also recommend rate limiting ICMPv6

```
ipv6 access-list ICMPv6
 permit icmp any any
 !
class-map match-all ICMPv6
 match protocol ipv6
 match access-group name ICMPv6
 !
policy-map ICMPv6_RATE_LIMIT
 class ICMPv6
  police 100000 200000 conform-action transmit exceed-action drop
 !
interface fa0/0
 service-policy input ICMPv6_RATE_LIMIT
```

# IPv6 Bogons

- IPv6 has bogons too... filter them!

```
no ipv6 prefix-list v6-IN-FILTER
ipv6 prefix-list v6-IN-FILTER deny 2001::/32 le 128           ! Teredo subnets
ipv6 prefix-list v6-IN-FILTER deny 2001:db8::/32 le 128     ! Documentation
ipv6 prefix-list v6-IN-FILTER deny 2002::/16 le 128         ! 6to4 subnets
ipv6 prefix-list v6-IN-FILTER deny <your::/32> le 128       ! Your prefix
ipv6 prefix-list v6-IN-FILTER deny 3ffe::/16 le 128         ! Old 6bone
ipv6 prefix-list v6-IN-FILTER deny fc00::/7 le 128          ! ULA
ipv6 prefix-list v6-IN-FILTER deny fe00::/9 le 128          ! Reserved IETF
ipv6 prefix-list v6-IN-FILTER deny fe80::/10 le 128         ! Link-local
ipv6 prefix-list v6-IN-FILTER deny fec0::/10 le 128         ! Link-local
ipv6 prefix-list v6-IN-FILTER deny ff00::/8 le 128          ! Link-local
ipv6 prefix-list v6-IN-FILTER permit 2000::/3 le 48         ! Global Unicast
ipv6 prefix-list v6-IN-FILTER deny ::/0 le 128
```

# Aside - Bogons

- Not all IP (v4 and v6) are allocated by IANA
- Addresses that should not be seen on the Internet are called "**Bogons**" (also called "**Martians**")
  - RFC1918s + Reserved space
- IANA publishes list of number resources that have been allocated/assigned to RIRs/end-users
  - <https://www.iana.org/assignments/ipv6-unicast-address-assignments/ipv6-unicast-address-assignments.xhtml>
  - <https://www.iana.org/assignments/ipv4-address-space/ipv4-address-space.xhtml>

# Bogons

- Commonly found as source addresses of DDoS packets
- We should have ingress and egress filters for bogon routes
  - Should not route them nor accept them from peers
- We could manually craft prefix filters based on the bogon list from IANA
  - But bogon list is dynamic
  - New allocations made out of reserved blocks frequently

# Bogon Route Server Project

- In comes the Bogon Route Server project by Team Cymru
  - Provides dynamic bogons information using eBGP multihop sessions
  - Traditional bogons (AS65333)
    - martians plus prefixes not allocated by IANA
  - Full-bogons (AS65332)
    - above plus prefixes allocated to RIRs but not yet assigned to ISPs/end-users by RIRs
- For details:
  - <http://www.team-cymru.org/bogon-reference-bgp.html>





# Peering- Bogon Route Servers

- To peer with bogon route servers
  - Write to [bogonrs@cymru.com](mailto:bogonrs@cymru.com)
- You should provide:
  - Your ASN
  - Which bogons you wish to receive
  - Your peering addresses
  - MD5 for BGP?
  - PGP public key (optional)
- It is recommended to have at least 2 (two) peering sessions for redundancy

# Source IP spoofing – Defense

- **BCP38** (RFC2827)
  - Since **1998!**
  - <https://tools.ietf.org/html/bcp38>
- Only allow traffic with valid source addresses to
  - Leave your network
    - Only packets with source address from your own address space
  - To enter/transit your network
    - Only source addresses from downstream customer address space

# uRPF – Unicast Reverse Path

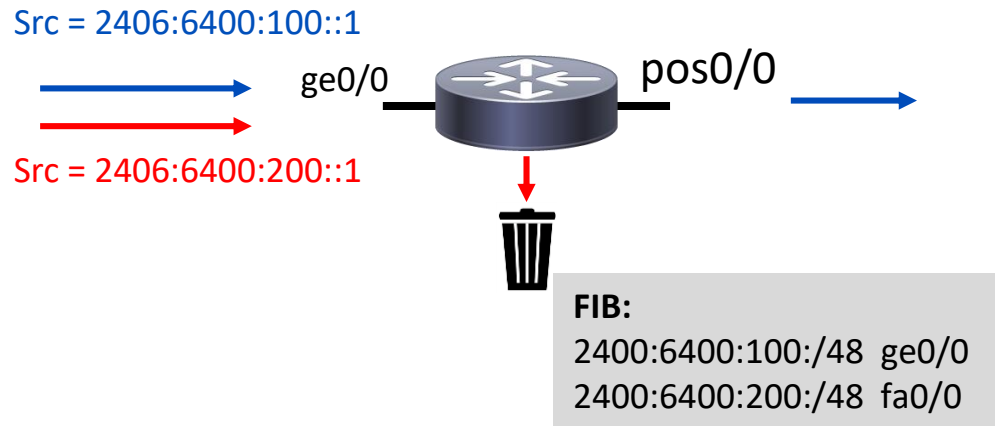
- Unicast Reverse Path Forwarding (uRPF)
  - Router verifies if the source address of packets received is in the FIB table and reachable (routing table)
    - Else **DROP!**
  - ***Recommended on customer facing interfaces***

```
(config-if)#ipv6 verify unicast source reachable-via {rx|any}
```

# uRPF – Unicast Reverse Path

- Modes of Operation:

- Strict: verifies both source address and incoming interface with FIB entries



- Loose: verifies existence of route to source address

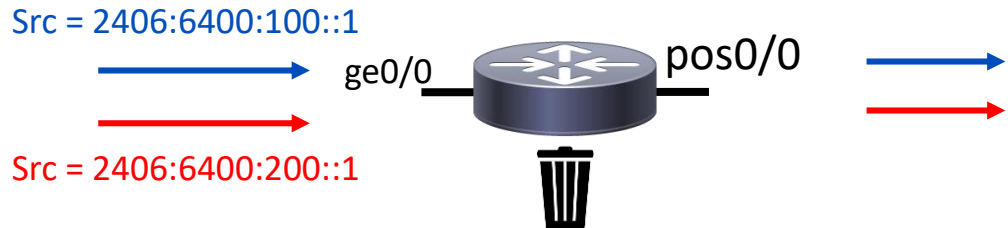
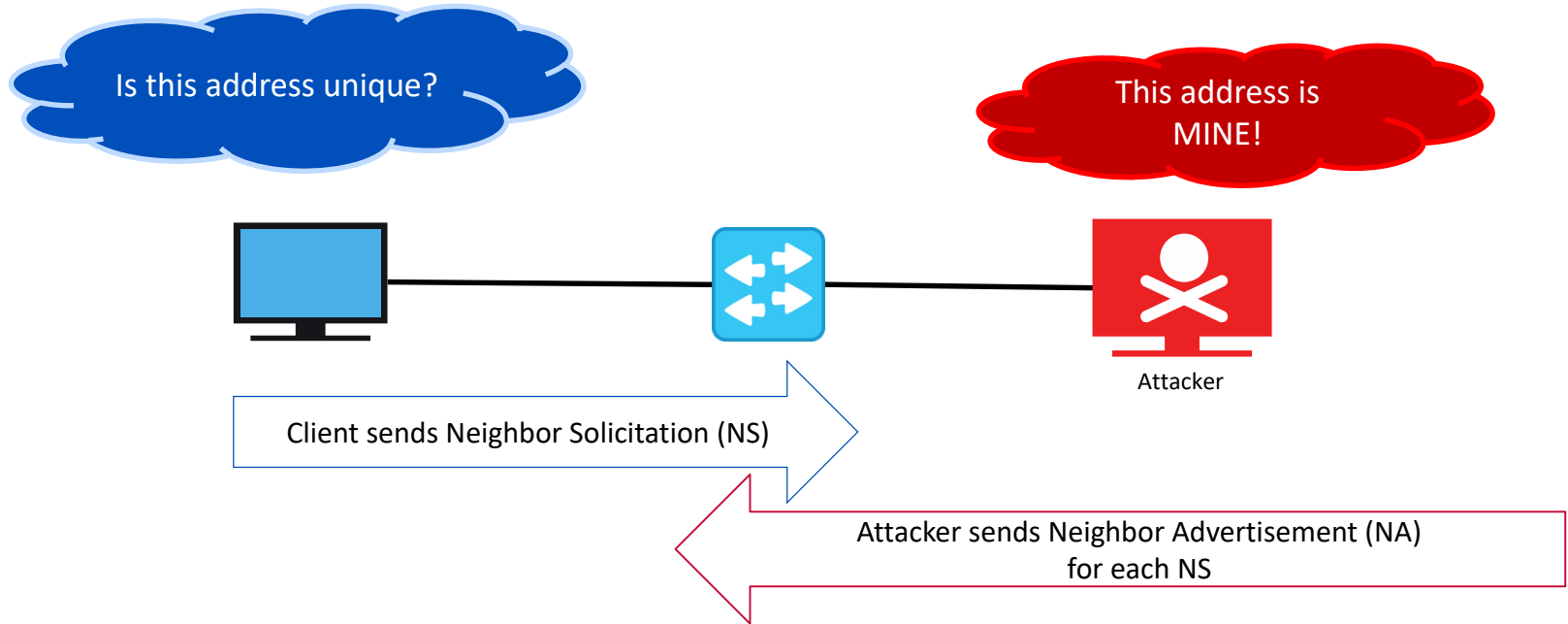


Image source: "Cisco ISP Essentials", Barry Greene & Philip Smith 2002

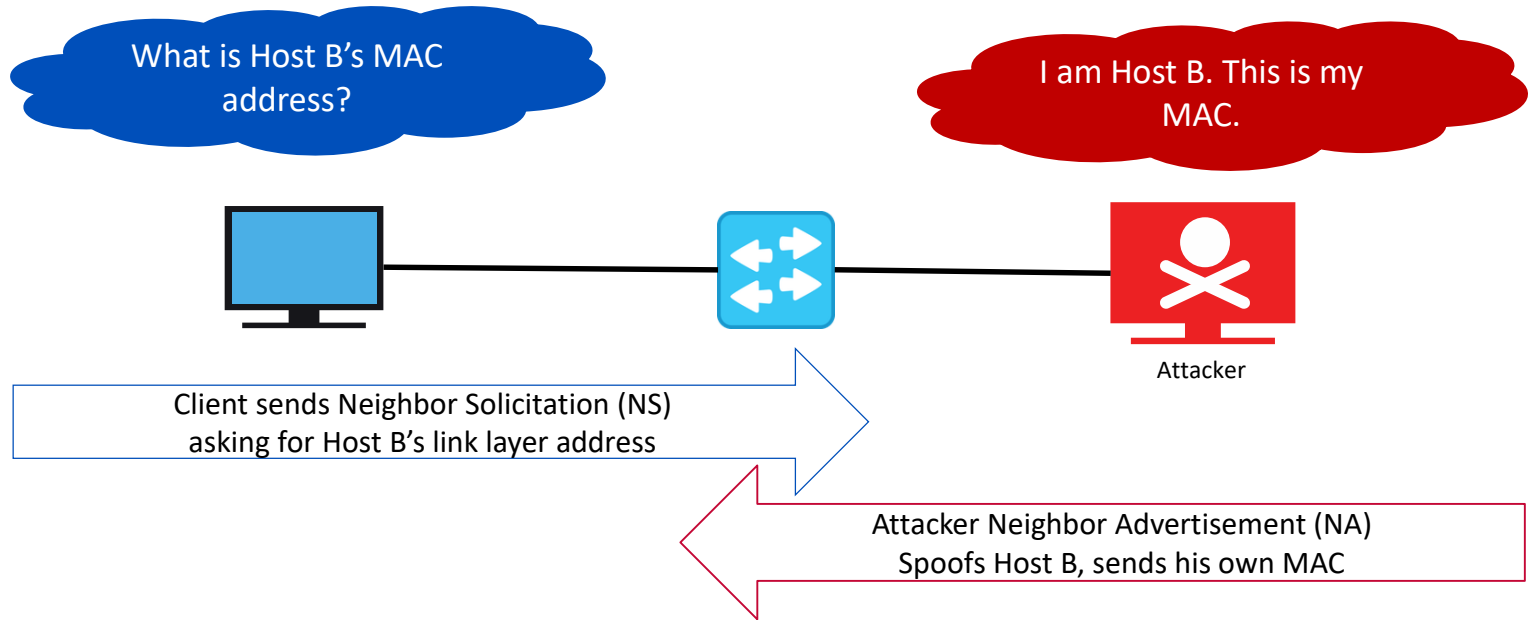
# ICMPv6 Attack Tools

- THC-IPv6
  - <https://www.thc.org/thc-ipv6/>
- SI6 Networks IPv6 Toolkit
  - <http://www.si6networks.com/tools/ipv6toolkit/>
- Chiron
  - <http://www.secfu.net/tools-scripts/>

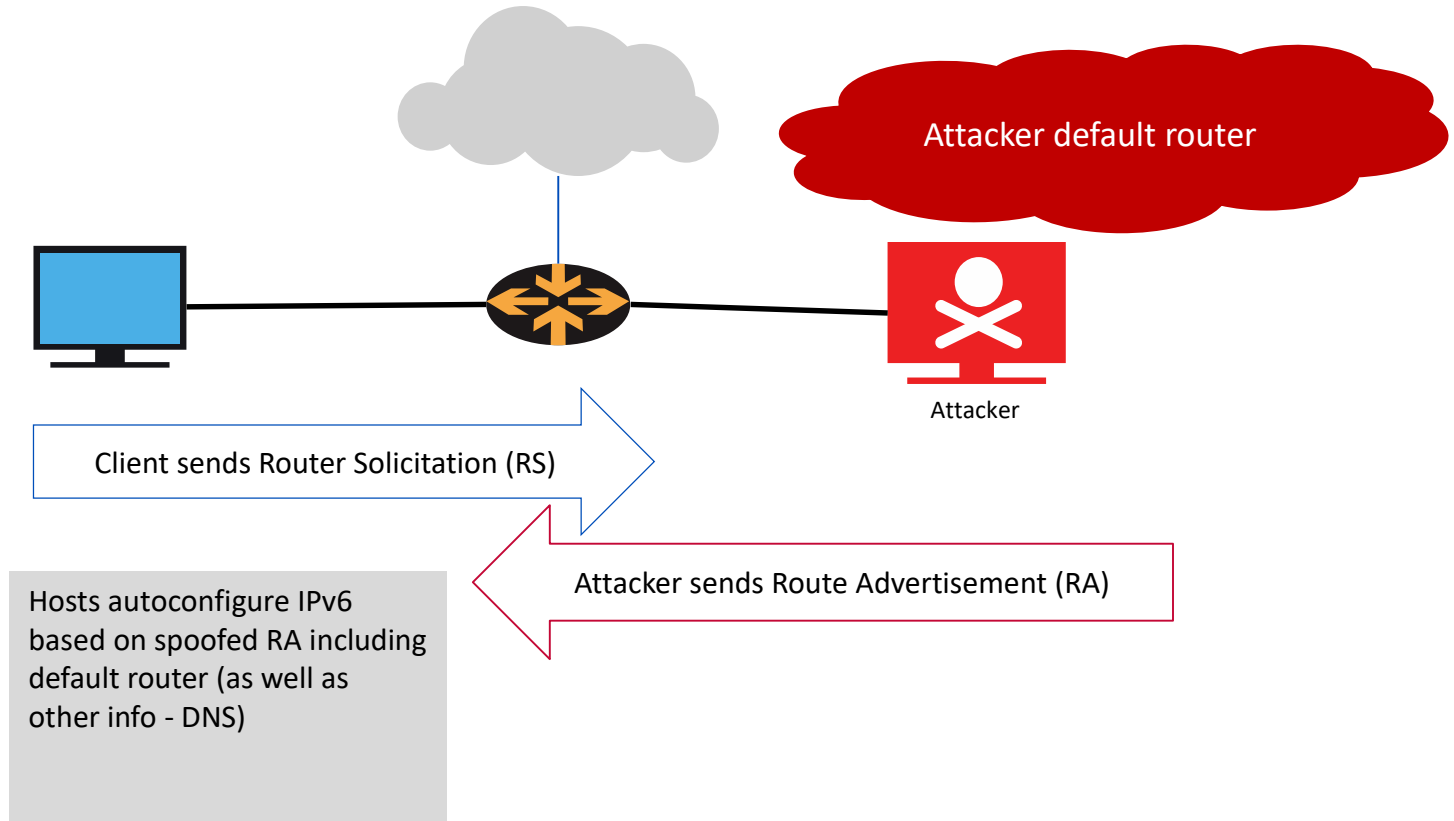
# DAD - DOS



# ND Spoofing

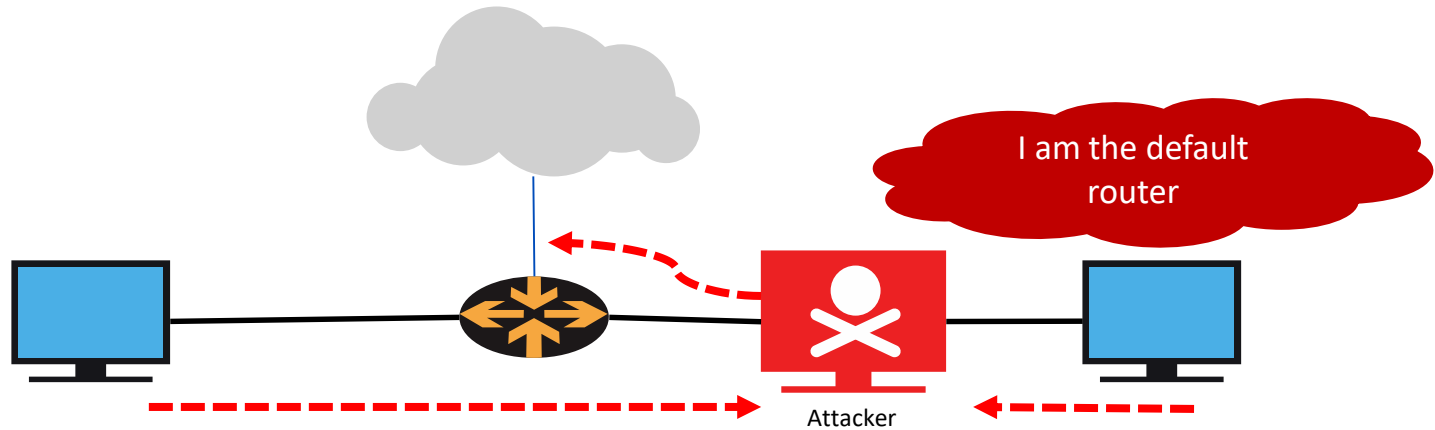


# Rogue RA





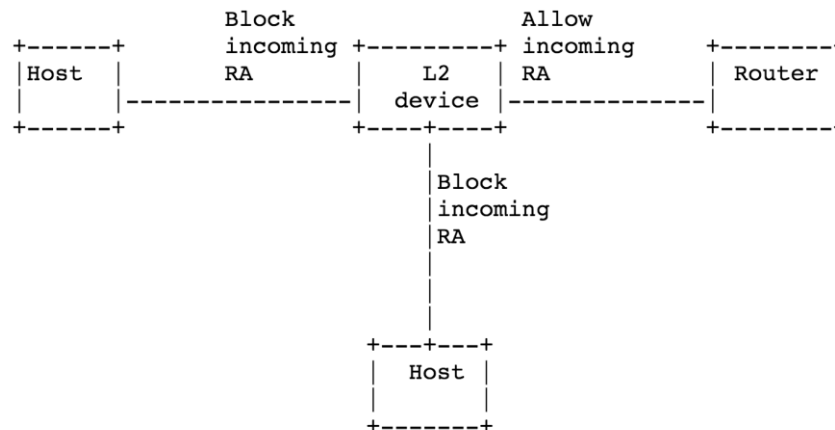
# Rogue RA



- Attacker can now intercept, listen and modify the packets coming from Host A and B – MITM
- Or redirect to a site they control

# Mitigation tools

- RA Guard (RFC6105/7113)
  - messages between IPv6 devices traverse the controlled L2 networking device
  - first-hop security
- Allow or drop RA messages based on policies



# Mitigation tools

- SEND (RFC3971)
  - Uses crypto to secure NDP messages
    - Uses CGA and a set of NDP options
- CGA (crypto-generated address):
  - CGA associates a public key with a IPv6 address
    - RSA signature option
  - Node computes interface-ID
    - Using hash-function of the node's public key
  - and appends to the IPv6 prefix - CGA

# Mitigation tools

- SEND (RFC3971)
  - The receiver recomputes the hash and compares with the interface-ID
    - Verifies the public key binding
  - Messages sent from a CGA address can be protected by attaching the public key and signing the message with private key.

# References:

- [https://www.first.org/resources/papers/conf2015/first\\_2015-herberg-frank\\_ipv6-security\\_20150618.pdf](https://www.first.org/resources/papers/conf2015/first_2015-herberg-frank_ipv6-security_20150618.pdf)
- <https://tools.ietf.org/html/rfc2460>
- <https://tools.ietf.org/html/rfc7112>
- <https://tools.ietf.org/html/rfc7113>
- <https://tools.ietf.org/html/rfc8200>



# Questions

