The Layer-2 Security Issues and the Mitigation Techniques

Eric Vyncke

Cisco

Distinguished Engineer

evyncke@cisco.com Eric.Vyncke@ipv6council.be Eric.Vynce@ulg.ac.be

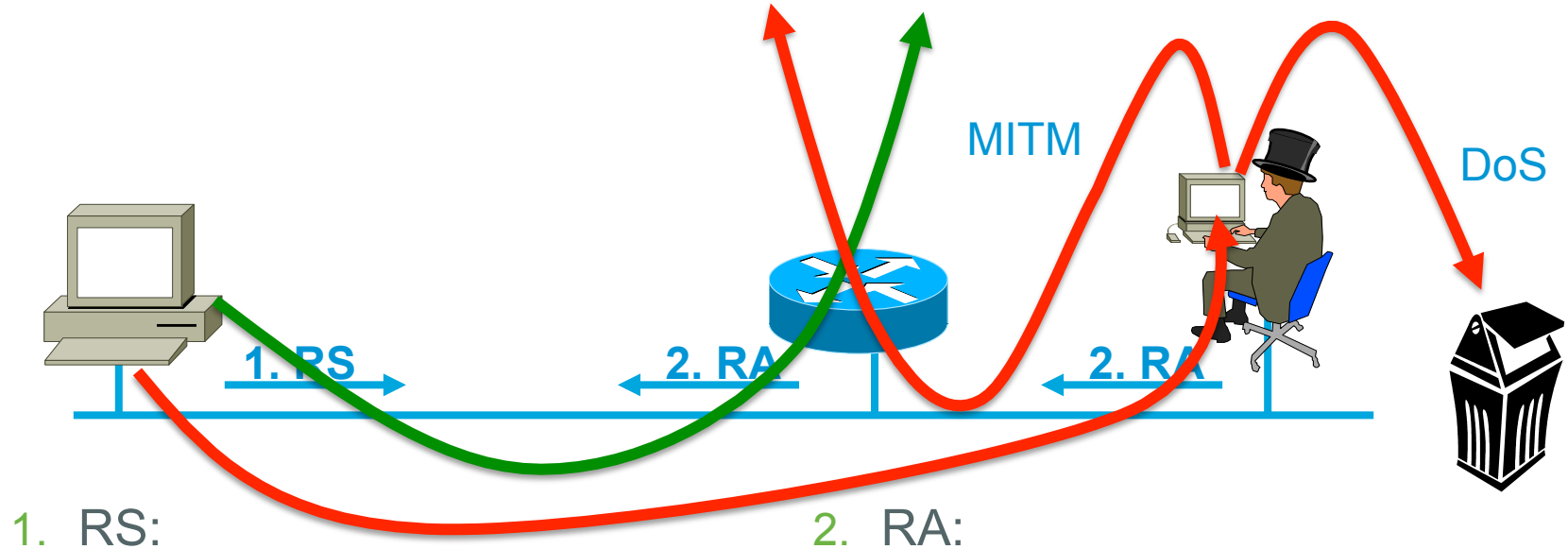
Networks are Sand Castles…

Courtesy of Curt Smith

Rogue Router Advertisement

Router Advertisements contains:
-Prefix to be used by hosts
-Data-link layer address of the router
-Miscellaneous options: MTU, DHCPv6 use, …

RA w/o Any Authentication Gives Exactly Same Level of Security as DHCPv4 (None)



1. RS:

Data = Query: please send RA

2. RA:

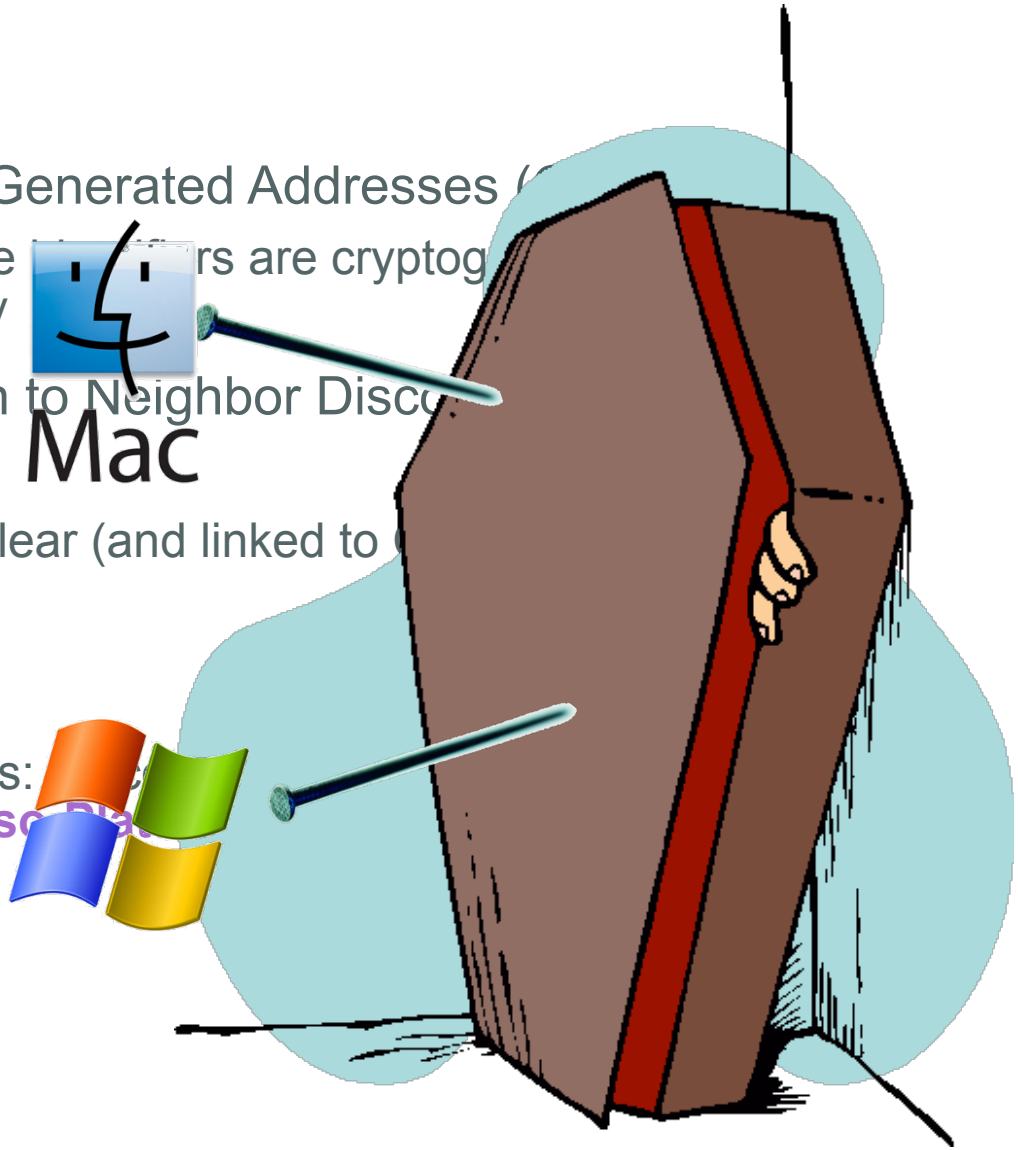
Data= options, **prefix**, lifetime, A+M+O flags

Rogue RA – Mitigation Techniques

Where	What
Routers	Increase “legal” router preference
Hosts	Disabling Stateless Address Autoconfiguration
Routers & Hosts	SeND “Router Authorization”
Switch (First Hop)	Host isolation
Switch (First Hop)	Port Access List (PACL)
Switch (First Hop)	RA Guard

Secure Neighbor Discovery (SeND) RFC 3971

- RFC 3972 Cryptographically Generated Addresses (
  - IPv6 addresses whose interface rs are cryptog
    generated from node public key
- SeND adds a signature option to Neighbor Disco
  - Using node private key
  - Node public key is sent in the clear (and linked to
- Very powerful
  - If MAC spoofing is prevented
  - But, not a lot of implementations:
    party for Windows (from Hasso



Clipart from Clipartheaven.com

Mitigating Rogue RA: Host Isolation

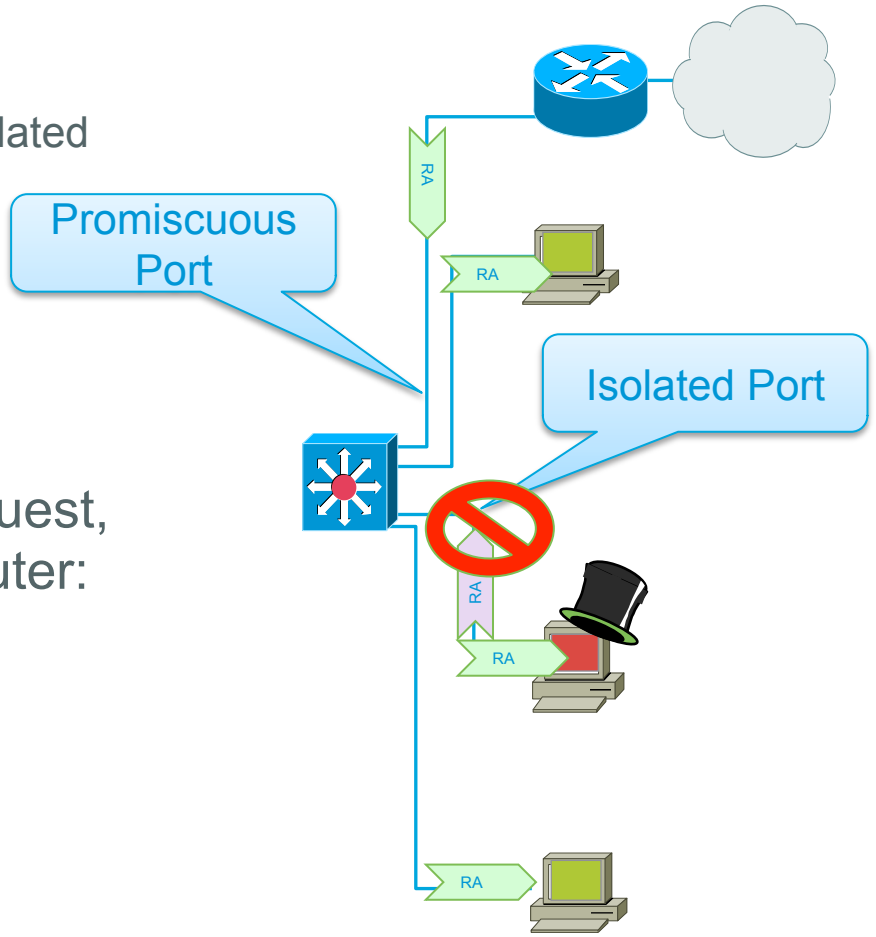
- Prevent Node-Node Layer-2 communication by using:

  Private VLANs (PVLAN) where nodes (isolated port) can only contact the official router (promiscuous port)

  WLAN in ‘AP Isolation Mode’

  1 VLAN per host (SP access network with Broadband Network Gateway)

- Link-local multicast (RA, DHCP request, etc) sent only to the local official router: no harm



Mitigating Rogue RA: RFC 6105

- **Port ACL** blocks all ICMPv6 RA from hosts

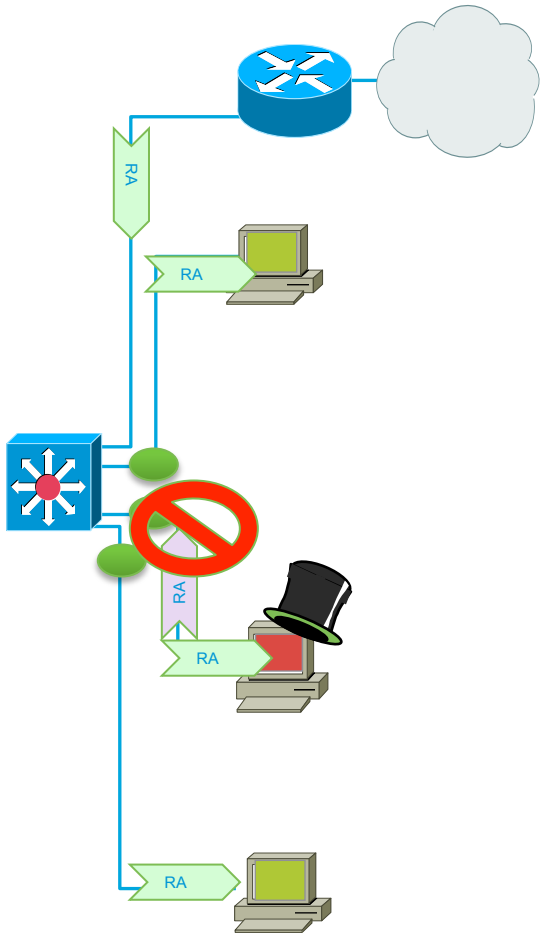
```
interface FastEthernet0/2
  ipv6 traffic-filter ACCESS_PORT in
  access-group mode prefer port
```

- **RA-guard lite** (12.2(33)SXI4 & 12.2(54)SG): also dropping all RA received on this port

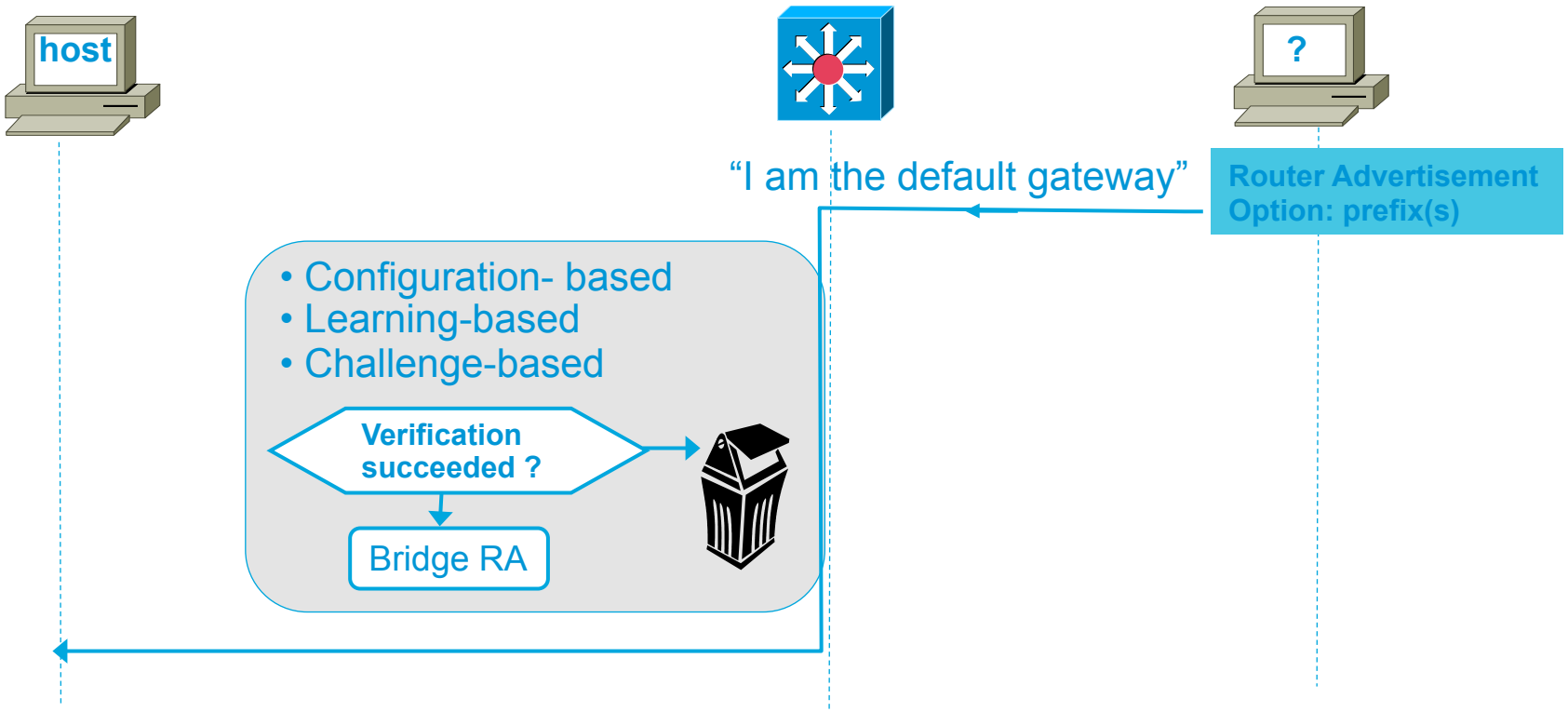
```
interface FastEthernet0/2
  ipv6 nd raguard
  access-group mode prefer port
```

- **RA-guard** (12.2(50)SY)

```
ipv6 nd raguard policy HOST device-role host
ipv6 nd raguard policy ROUTER device-role router
ipv6 nd raguard attach-policy HOST vlan 100
interface FastEthernet0/0
  ipv6 nd raguard attach-policy ROUTER
```



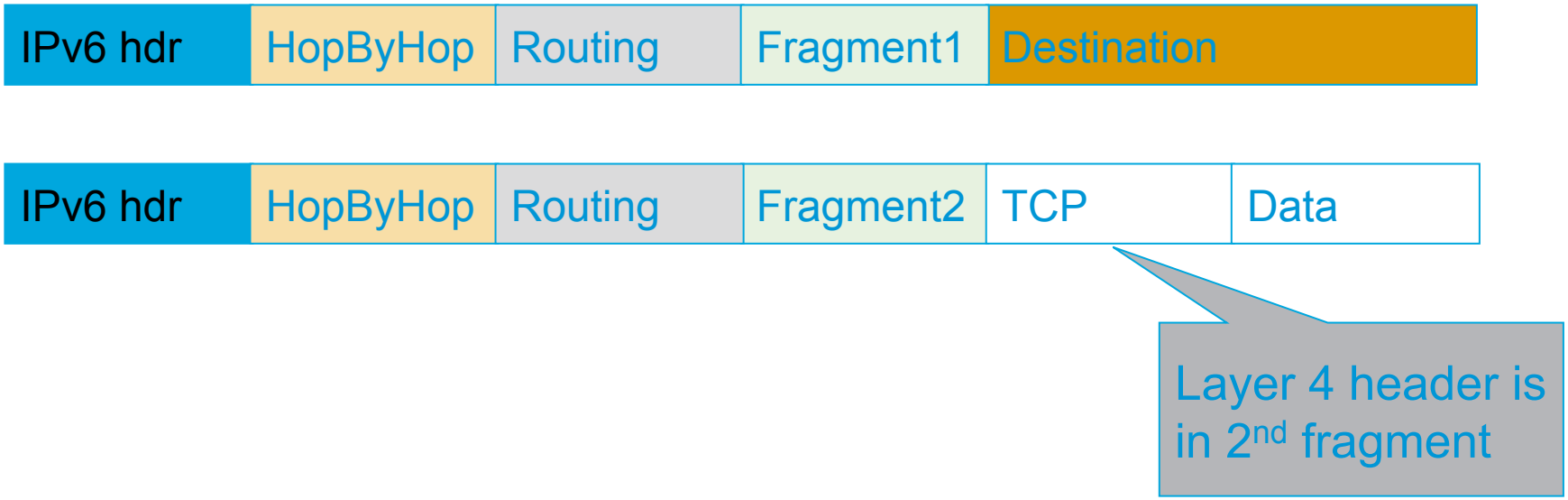
RA-Guard (RFC 6105)



- Switch selectively accepts or rejects RAs based on various criteria's
- Can be ACL based, learning based or challenge (SeND) based.
- Hosts see only allowed RAs, and RAs with allowed content

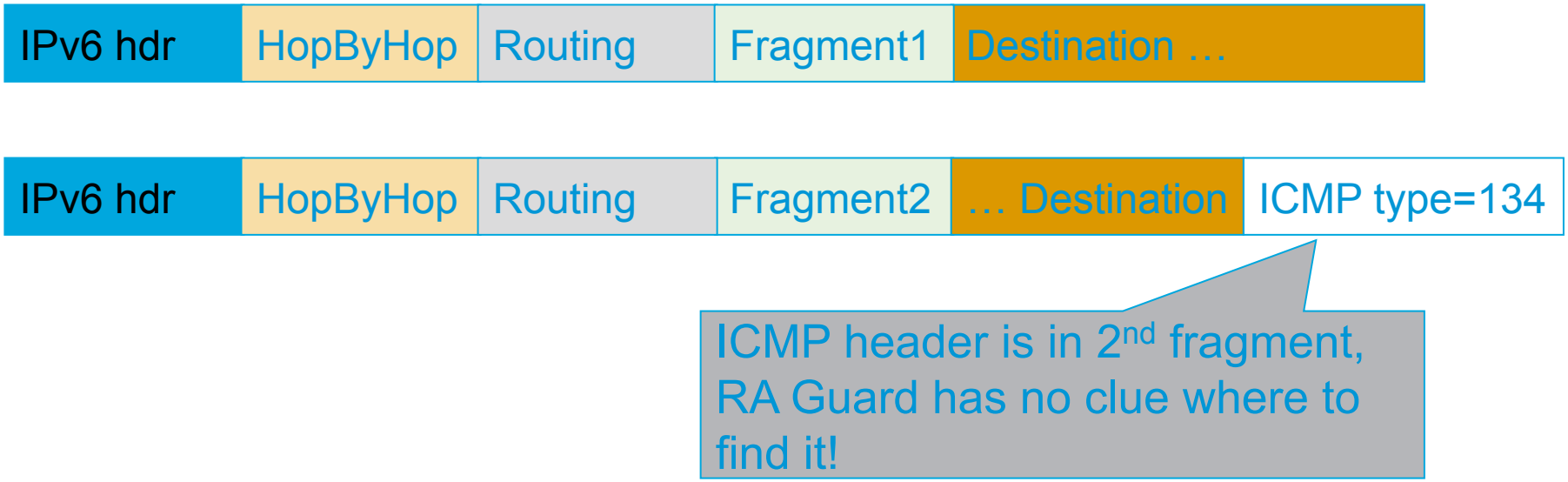
Here comes Fragmentation…

- Extension headers chain can be so large than it is fragmented!
- RFC 3128 is not applicable to IPv6
- Layer 4 information could be in 2nd fragment



Parsing the Extension Header Chain Fragments and Stateless Filters (RA Guard)

- RFC 3128 is not applicable to IPv6, extension header can be fragmented
- ICMP header could be in 2nd fragment after a fragmented extension header
- RA Guard works like a stateless ACL filtering ICMP type 134
- THC fake_router6 –FD implements this attack which bypasses RA Guard
- ***Partial work-around: block all fragments sent to ff02::1***
  - ***'undetermined-transport' is even better***
  - ***Does not work in a SeND environment (larger packets) but then no need for RA-guard ☺***



Attacking Neighbor Discovery with NDP Spoofing

Neighbor Advertisement can be Spoofed

- Pretty much like RA: no authentication
  - Any node can ‘steal’ the IP address of any other node
  - Impersonation leading to denial of service or MITM
- Requires layer-2 adjacency
- IETF SAVI Source Address Validation Improvements (work in progress)

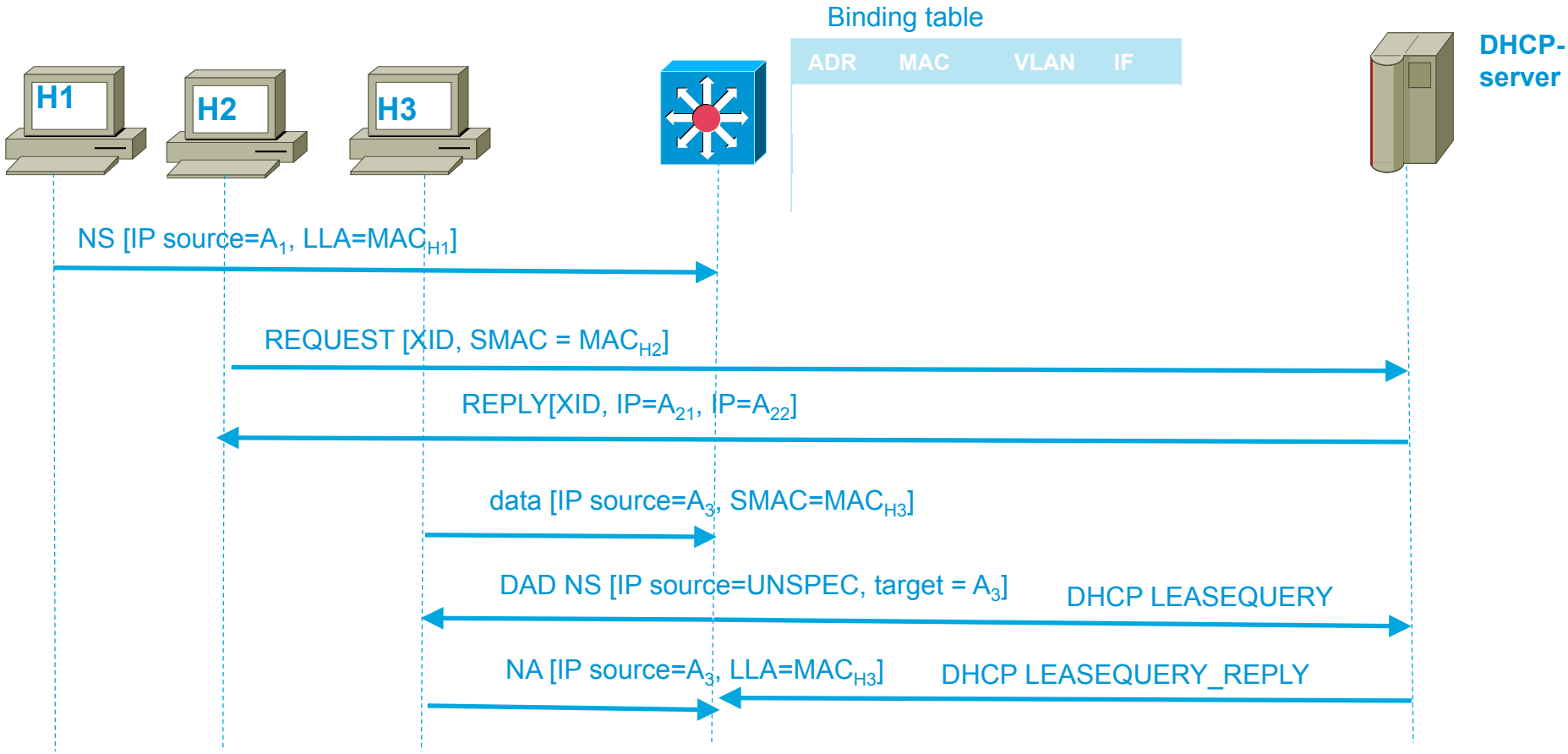
NDP Spoofing Mitigations

Where	What
Routers & Hosts	configure static neighbor cache entries
Routers & Hosts	Use CryptoGraphic Addresses (SeND CGA)
Switch (First Hop)	Host isolation
Switch (First Hop)	Address watch • Glean addresses in NDP and DHCP • Establish and enforce rules for address ownership

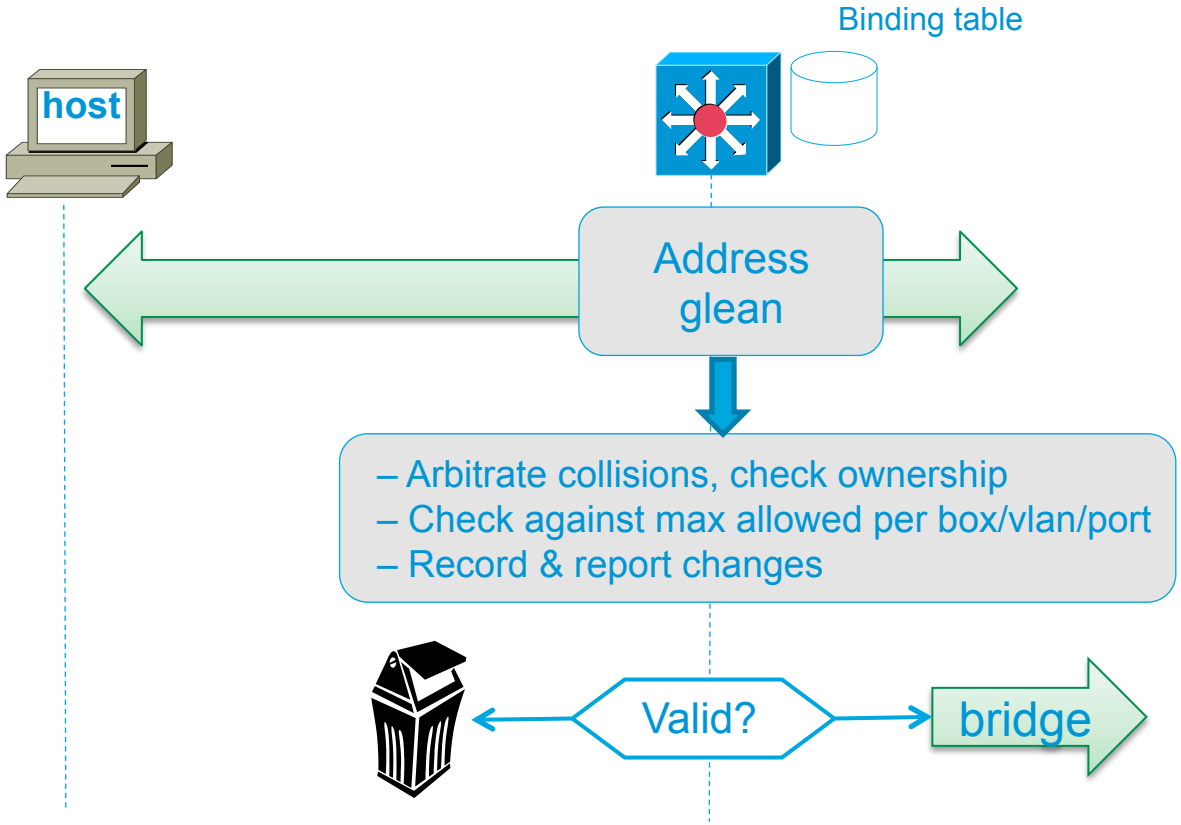
SAVI: How to Learn?

- If a switch wants to enforce the mappings < *IP address, MAC address*> how to learn them?
- Multiple source of information
  - SeND: verify signature in NDP messages, then add the mapping
  - DHCP: snoop all messages from DHCP server to learn mapping (same as in IPv4)
  - NDP: more challenging, but '*first come, first served*'
    - The first node claiming to have an address will have it

NDP Spoofing – Mitigation: Binding Integrity at the First Hop



NDP Spoofing – Mitigation: Address Watch at the First Hop



- Preference is a function of: configuration, learning method, credential provided
- Upon collision, choose highest preference (for instance static, trusted, CGA, DHCP preferred over dynamic, not_trusted, not_CGA, SLACC)
- For collision with same preference, choose First Come, First Serve

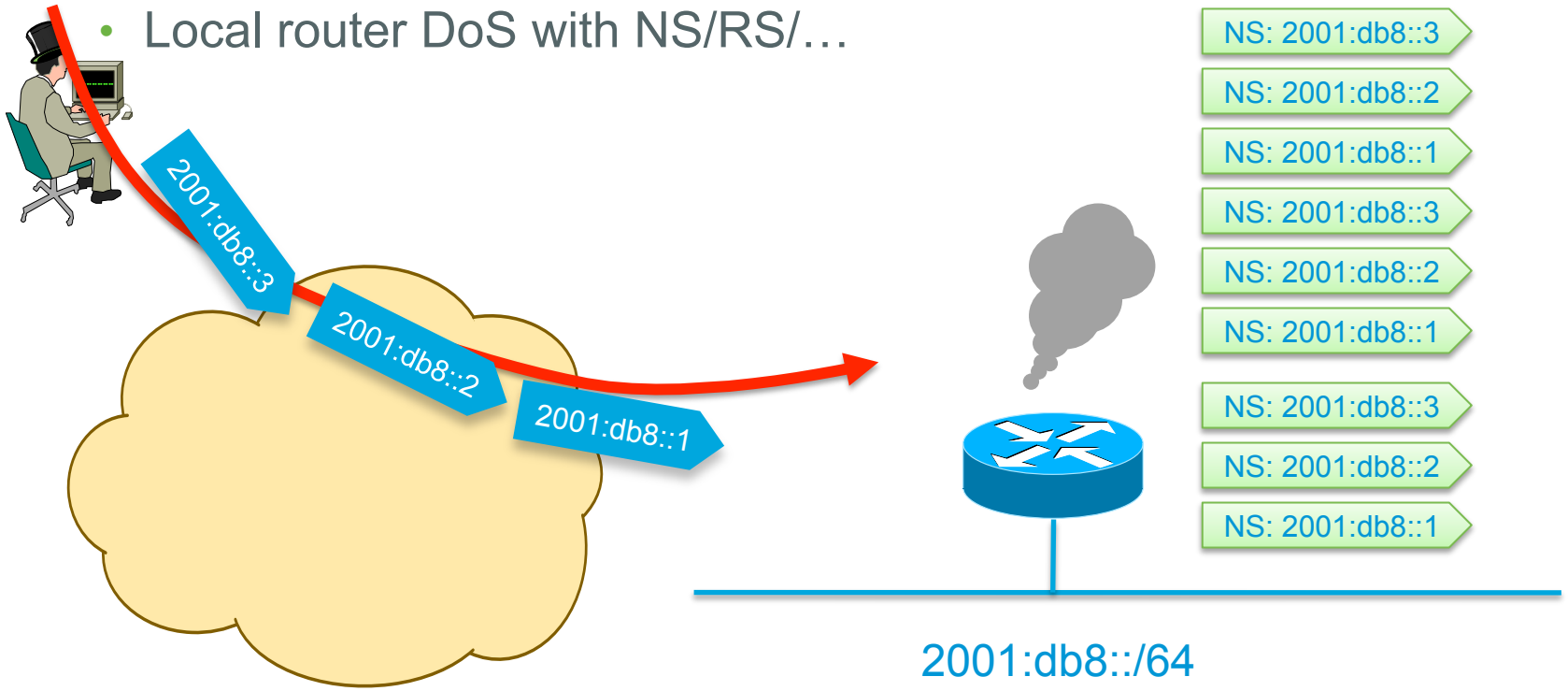
Exhausting the Neighbor Cache

Scanning Made Bad for CPU
Remote Neighbor Cache Exhaustion

- Remote router CPU/memory DoS attack if aggressive scanning

  Router will do Neighbor Discovery... And waste CPU and memory

- Local router DoS with NS/RS/…

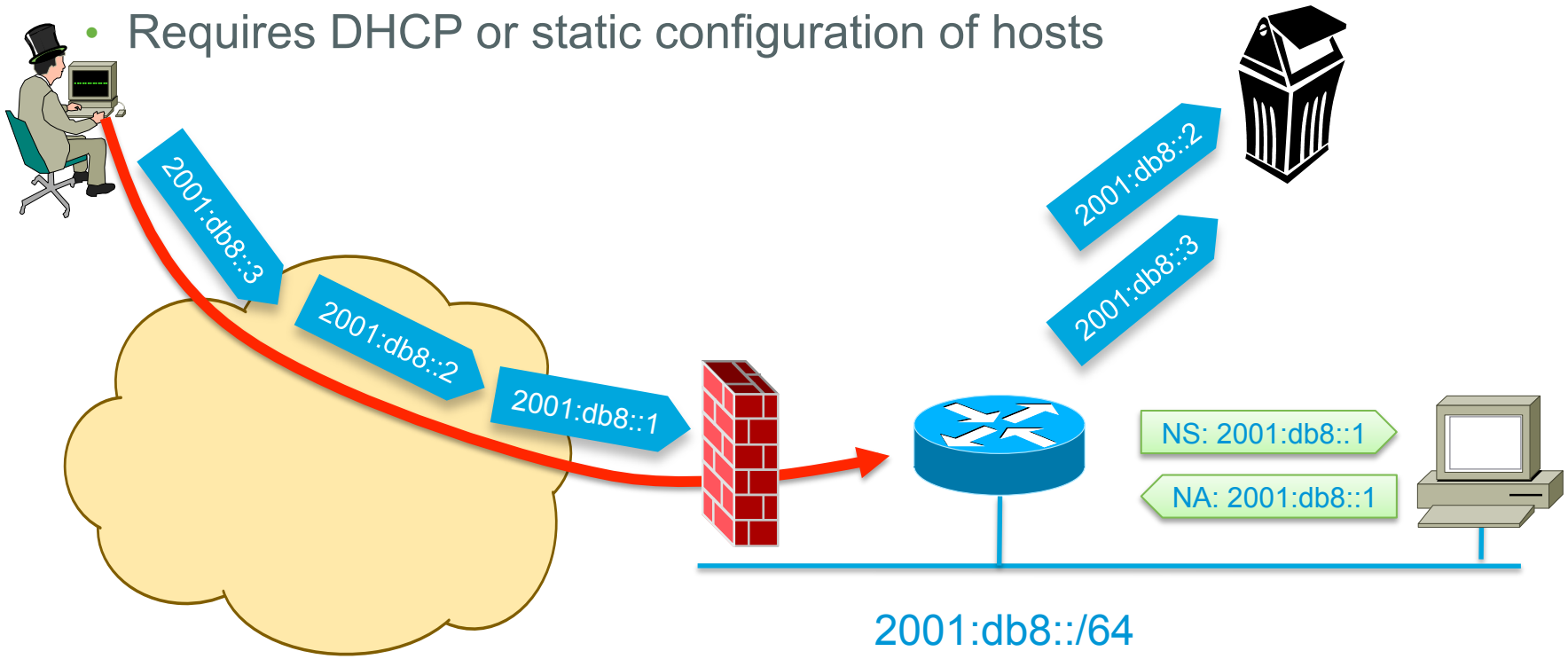


Mitigating Remote Neighbor Cache Exhaustion

- Mainly an implementation issue
  - Rate limiter on a global and per interface
  - Prioritize renewal (PROBE) rather than new resolution
  - Maximum Neighbor cache entries per interface and per MAC address
- **Internet edge/presence**: a target of choice
  - Ingress ACL permitting traffic to specific statically configured (virtual) IPv6 addresses only
  - ⇒Allocate and configure a /64 but uses addresses fitting in a /120 in order to have a simple ingress ACL
- Using a /64 on **point-to-point links** => a lot of addresses to scan!
  - Using /127 could help (RFC 6164)

Simple Fix for Remote Neighbor Cache Exhaustion

- Ingress ACL allowing only valid destination and dropping the rest
- NDP cache & process are safe
- Requires DHCP or static configuration of hosts



Addressing the Attendees-Exhaustion with Summary

Summary

- Without a secure layer-2, there is no upper layer security
- Rogue Router Advertisement is the most common threat
- Mitigation techniques
  - Host isolation
  - Secure Neighbor Discovery: but not a lot of implementations
  - SAVI-based techniques: discovery the ‘right’ information and dropping RA/NA with wrong information
  - Last remaining issue: (overlapped) fragments => drop all fragments…
- Neighbor cache exhaustion
  - Use good implementation
  - Expose only a small part of the addresses and block the rest via ACL
- Products are now available implementing the techniques ;-)

First Hop Security in September 2012

For Your Reference

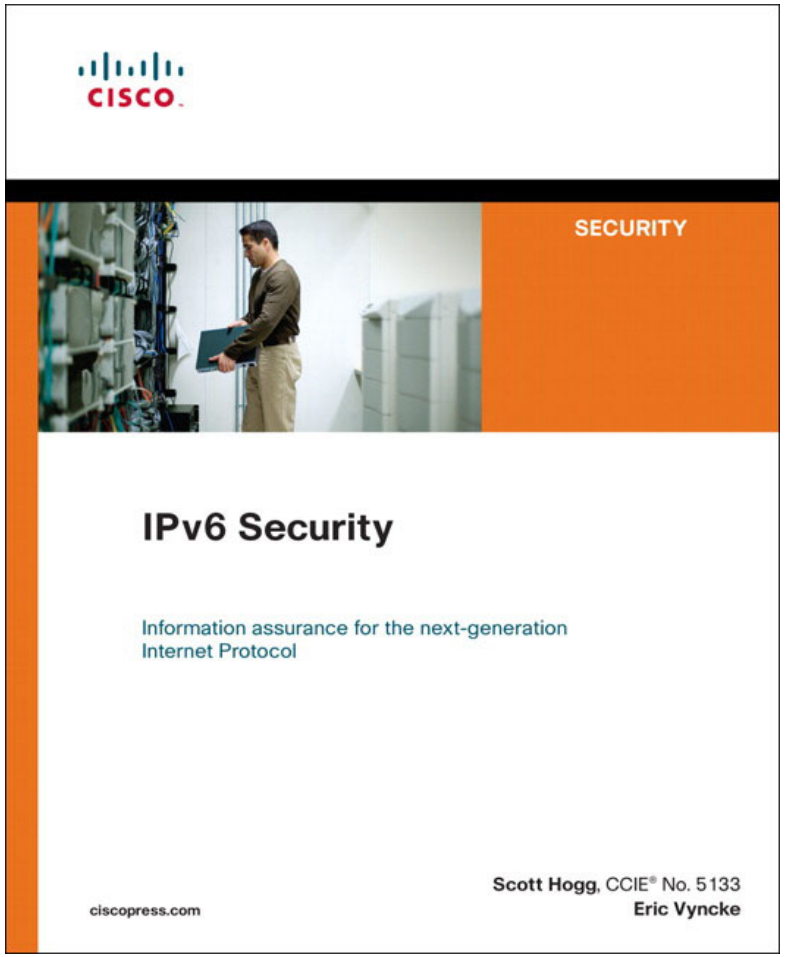
- IPv6 VLAN ACL & RA-Guard lite: 12.2(54)SG, 3.2.0SG, 15.0(2) SG, 12.2(33)SXI4

- NDP inspection & RA-Guard:
  - Cat 6K Sup 2T: 12.2(50)SY and 15.0(1)SY
  - WLC: 7.2
  - 7600: XE 7.0
  - Cat 2K/3K: 15.0(2)SE

For more Information:
http://www.cisco.com/en/US/docs/ios/ipv6/configuration/guide/ip6-roadmap.html
http://www.cisco.com/en/US/docs/ios-xml/ios/ipv6/configuration/15-2mt/ip6-first-hop-security.html

Any Question?

- And a shameless plug



Thank you.