RIPE NCC
RIPE NETWORK COORDINATION CENTRE

IPv6 Security Course Preview

SEE 7

Massimiliano Stucchi - Timisoara - 18th June 2018

Overview

IPv6 Security Myths

Basic IPv6 Protocol Security
(Extension Headers, Addressing)

IPv6 Associated Protocols Security
(NDP, MLD)

Legend

Learning/ understanding

Attacker

Protecting

IPv6 Security Myths

IPv6 Security Myths

1 2 3 4 5 6 7 8

- IPv6 is more secure than IPv4
- IPv6 has better security and it’s built in

Reason:

- RFC 4294 - IPv6 Node Requirements: IPsec MUST

Reality:

- RFC 6434 - IPv6 Node Requirements: IPsec SHOULD
- IPSec available. Used for security in IPv6 protocols

IPv6 Security Myths

1 | 2 | 3 | 4 | 5 | 6 | 7 | 8

- IPv6 has no NAT. Global addresses used
- I’m exposed to attacks from Internet

Reason:

- End-2-End paradigm. Global addresses. No NAT

Reality:

- Global addressing does not imply global reachability
- You are responsible for reachability (filtering)

IPv6 Security Myths

1 2 3 4 5 6 7 8

- IPv6 networks are too big to scan

Reason:

- Common LAN/VLAN use /64 network prefix
- 18,446,744,073,709,551,616 hosts

Reality:

- Brute force scanning is not possible [RFC5157]
- New scanning techniques

IPv6 Security Myths

1 2 3 **4** 5 6 7 8

- IPv6 is too new to be attacked

Reason:

- Lack of knowledge about IPv6 (it’s happening!)

Reality:

- There are tools, threats, attacks, security patches, etc.
- You have to be prepared for IPv6 attacks

IPv6 Security Myths

1 2 3 4 **5** 6 7 8

- IPv6 is just IPv4 with 128 bits addresses
- There is nothing new

Reason:

- Routing and switching work the same way

Reality:

- Whole new addressing architecture
- Many associated new protocols

IPv6 Security Myths

1 2 3 4 5 **6** 7 8

- It supports IPv6

Reason:

- Q: “Does it support IPv6?”
- A: “Yes, it supports IPv6”

Reality:

- IPv6 support is not a yes/no question
- Features missing, immature implementations, interoperability issues

IPv6 Security Myths

1 2 3 4 5 6 **7** 8

- My network is IPv4 only
- IPv6 is not a security problem

Reason:

- Networks only designed and configured for IPv4

Reality:

- IPv6 available in many hosts, servers, and devices
- Unwanted IPv6 traffic. Protect your network.

IPv6 Security Myths

1 2 3 4 5 6 7 **8**

- It’s not possible to secure an IPv6 network
- Lack of resources and features

Reason:

- Considering IPv6 completely different than IPv4
- Think there are no BCPs, resources or features

Reality:

- Use IP independent security policies
- There are BCPs, resources and features

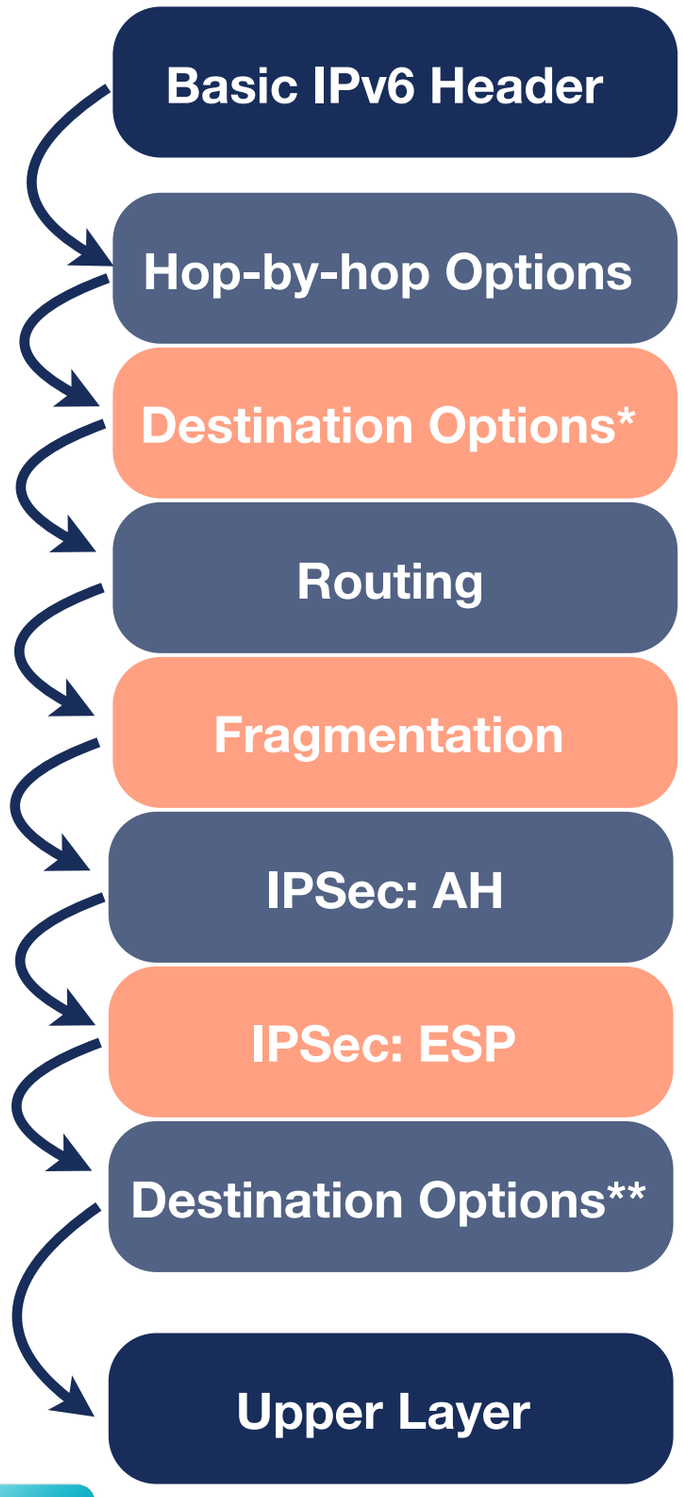
Conclusions

- A change of mindset is necessary
- IPv6 is not more or less secure than IPv4
- Knowledge of the protocol is the best security measure

Basic IPv6 Protocol Security

IPv6 Extension Headers

IPv6 Extension Headers (1)



- Fixed: Types and order
- Flexible use
- Processed only at endpoints
  - Exceptions: Hop-by-hop (and Routing)
- Only appear once
  - Exception: Destination Options

* Options for IPs in routing header

** Options for destination IP

IPv6 Extension Headers (2)

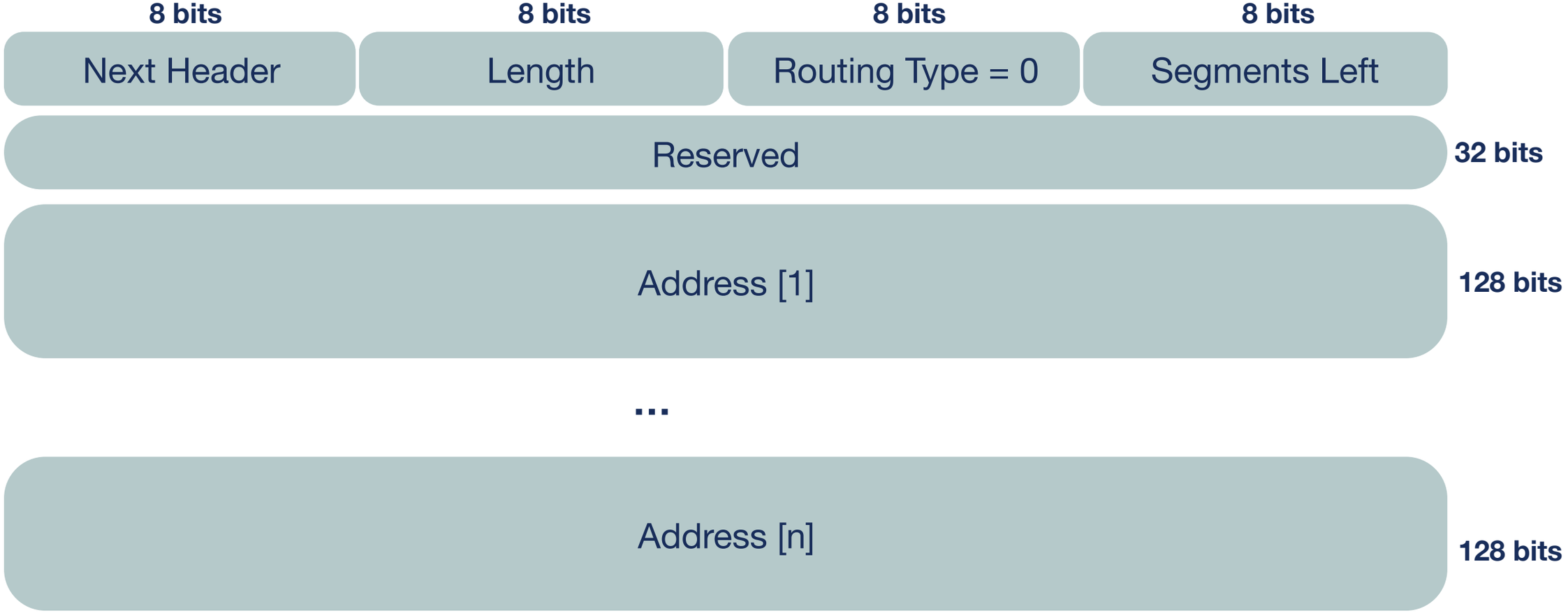
- Flexibility means complexity for security

- Security devices/software should be able to process the full chain of headers

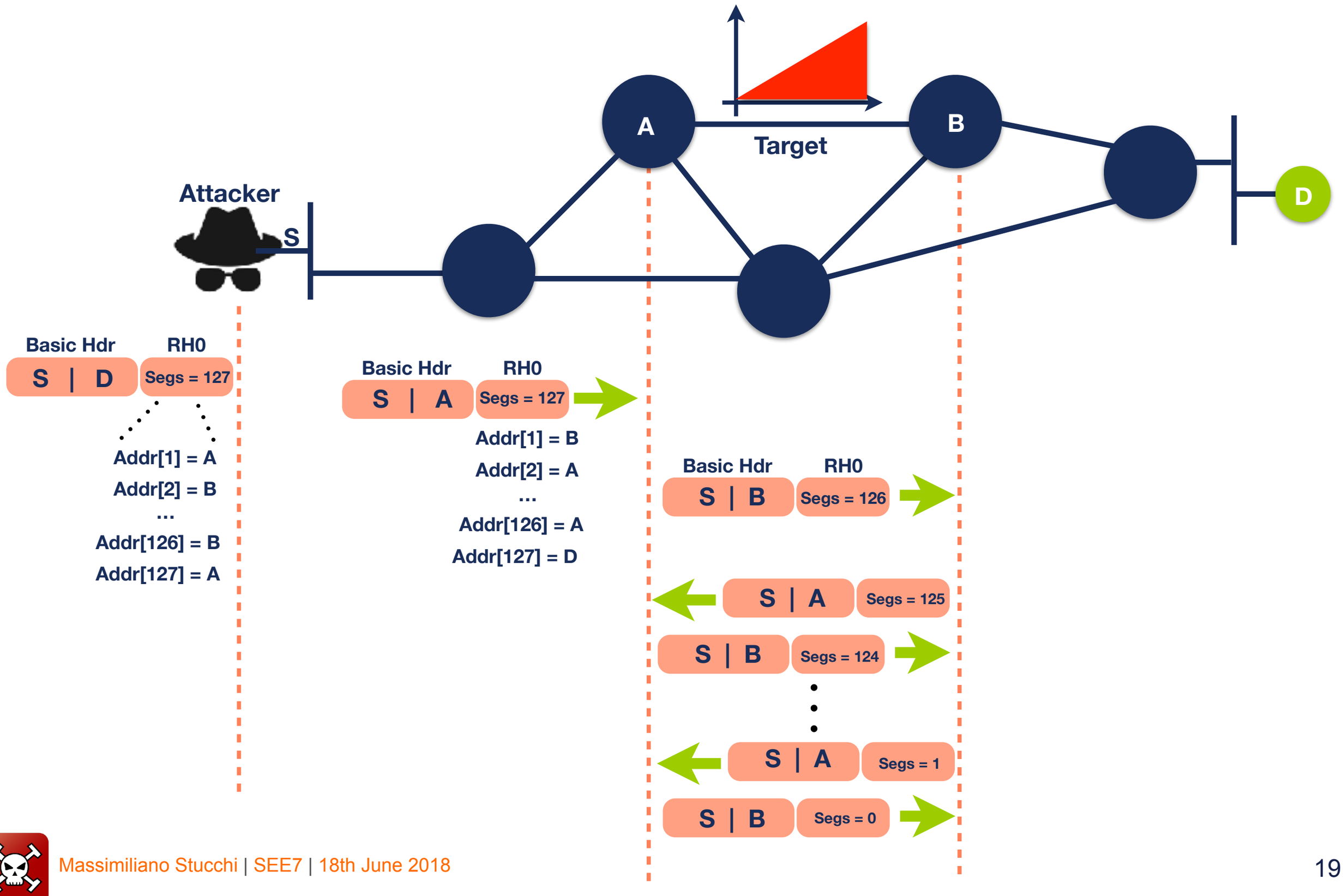
- Firewalls:
  - Must deal with standard EHs
  - Able to filter based on EH

Extension Headers Threats (1)

- **Routing Header** (**Type 0**): RH0 can be used for traffic amplification over a remote path
- **RH0 Deprecated** [RFC 5095]
  - RH1 deprecated, RH2 (MIPv6) & RH3 (RPL) still valid



Extension Headers Threats (2)

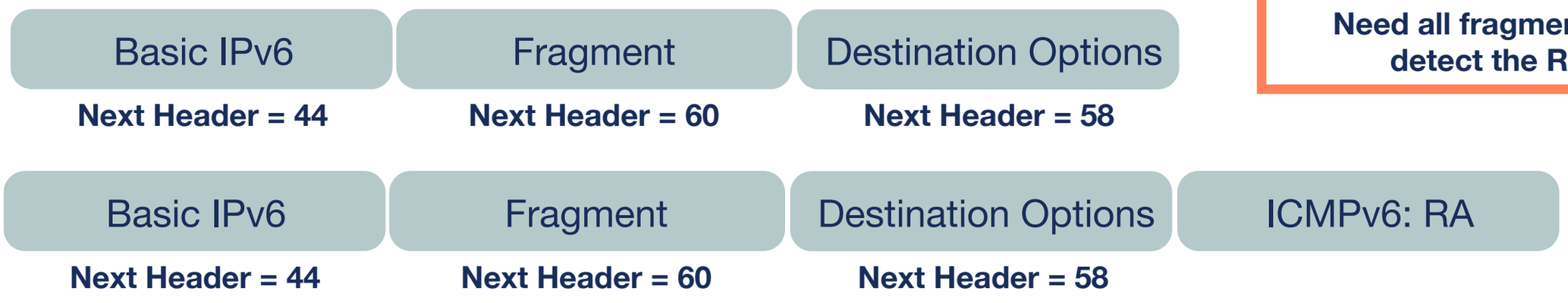


Extension Headers Threats (3)

- Trying to bypass security mechanisms
  - Example: fooling RA filtering (RA-Guard)
- Any EH

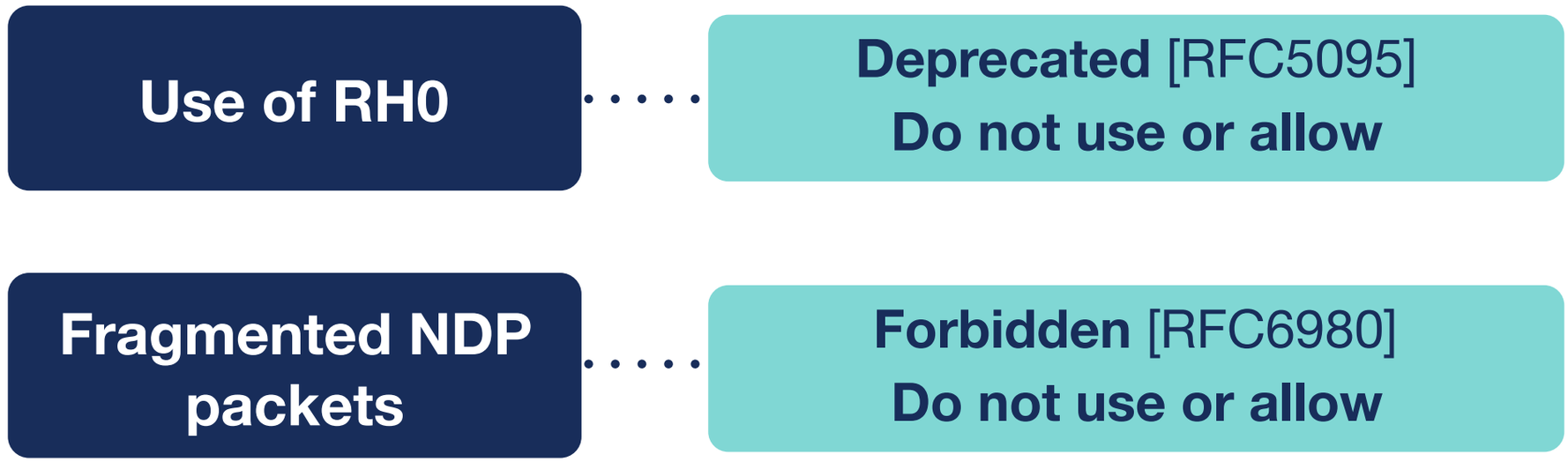
If only looks at Next Header = 60, do not detect the RA

- Fragment EH



Need all fragments to detect the RA

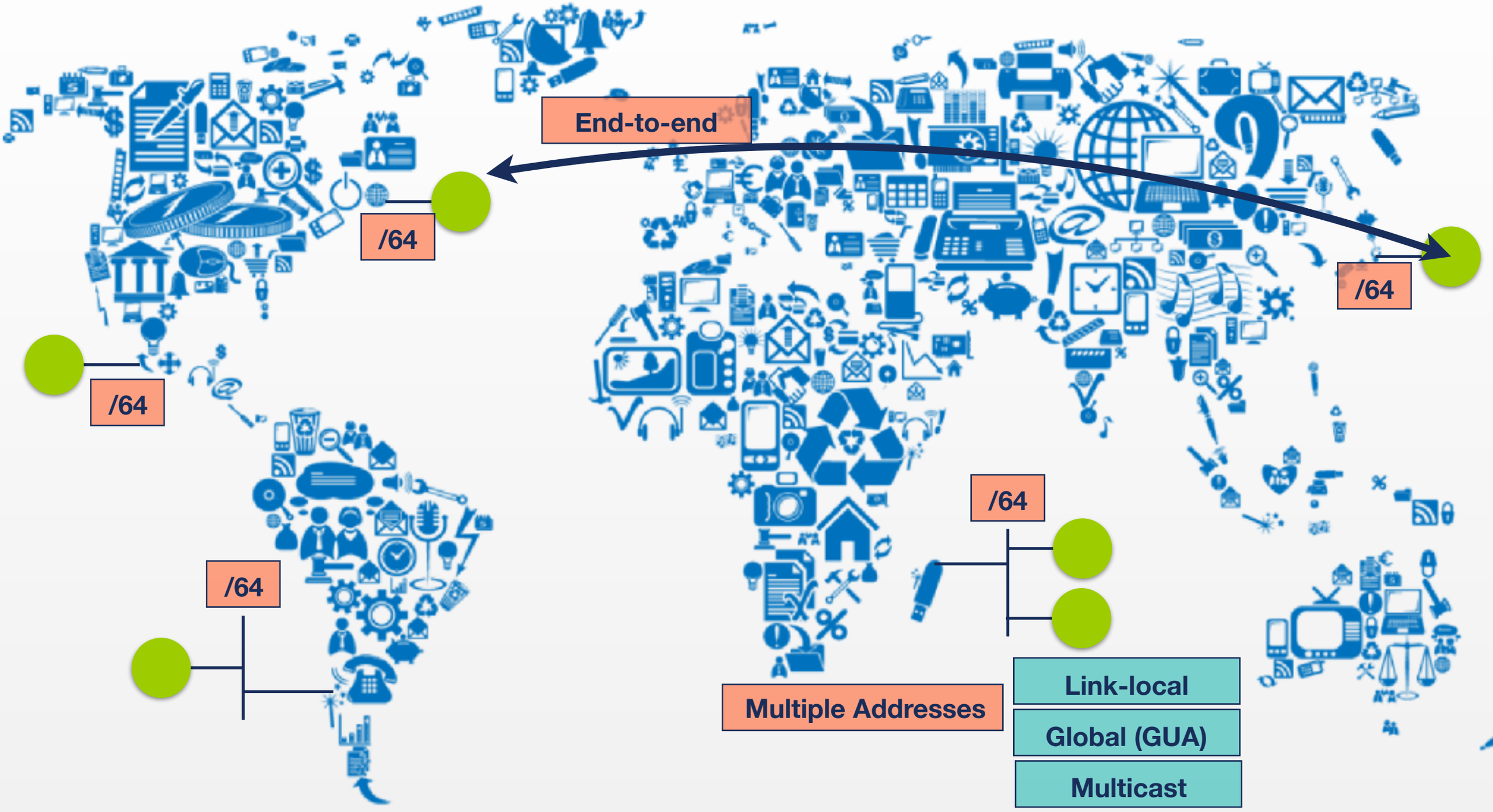
Extension Headers Solutions



- Require security tools to inspect Header Chain properly

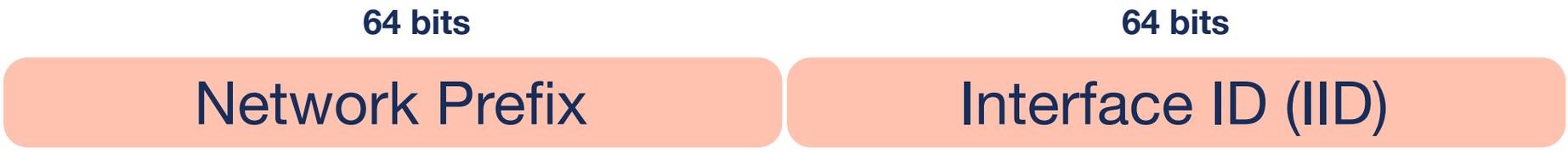
IPv6 Addressing Architecture

Introduction



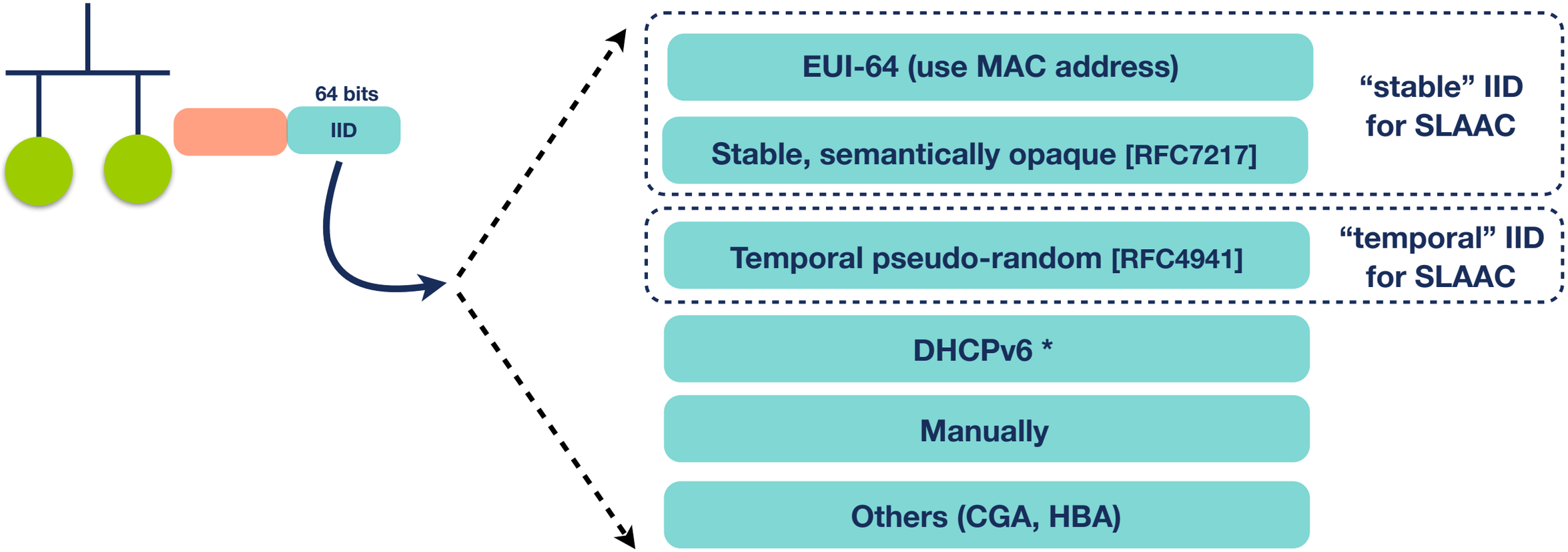
340,282,366,920,938,463,463,374,607,431,768,211,456

IPv6 Network Scanning (1)



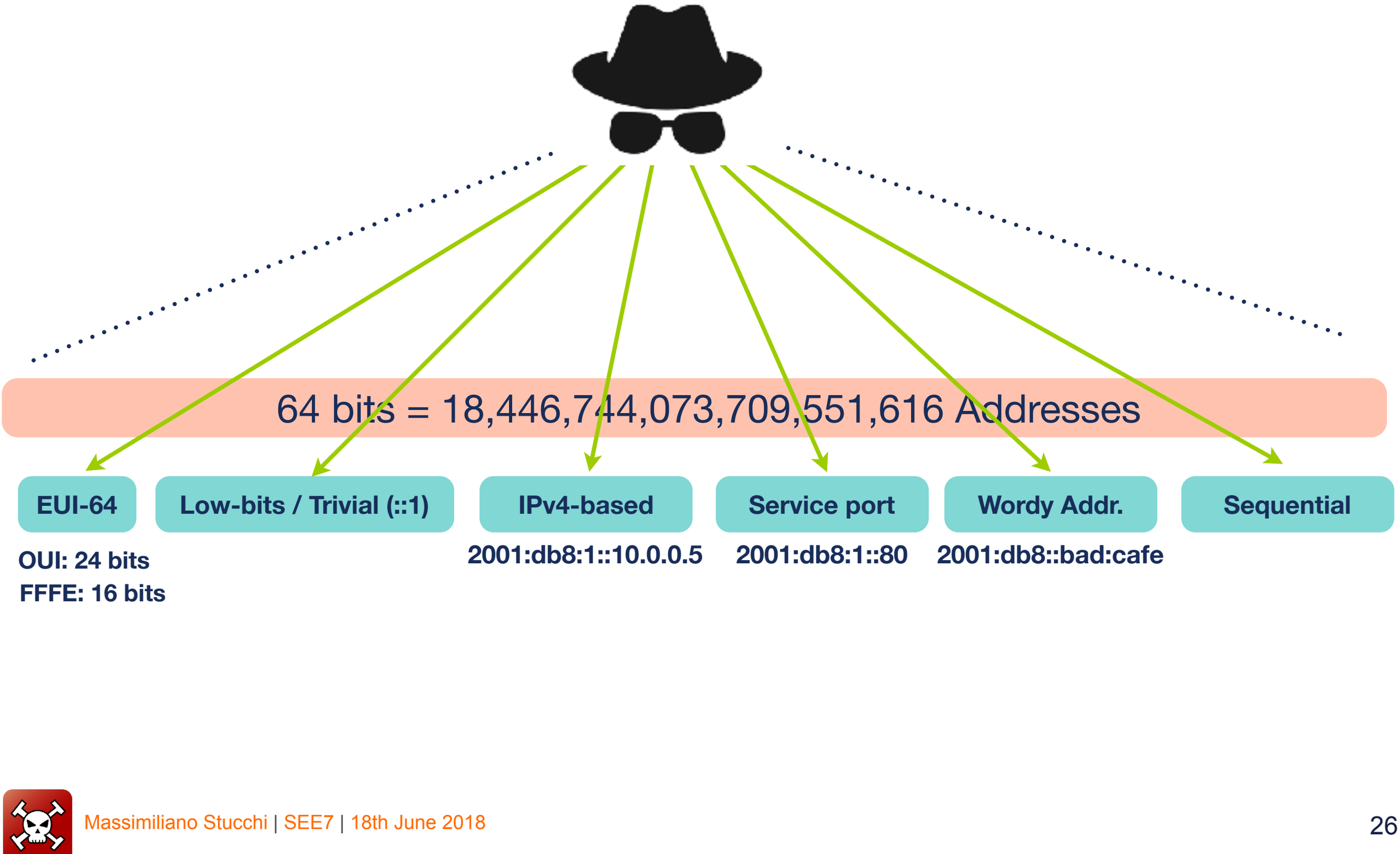
- Network Prefix determination (64 bits)
  - Common patterns in addressing plans
  - DNS direct and reverse resolution
  - Traceroute
- IID determination (64 bits)
  - “brute force” no longer possible

IPv6 Network Scanning (2)



- IID generated by the node (* except DHCPv6)
- Consider IID bits "opaque", no value or meaning [RFC7136]
  - How to generate [RFC7217]
  - This method is widely used and standardised [RFC8064]

IPv6 Network Scanning (3)



Security Tips

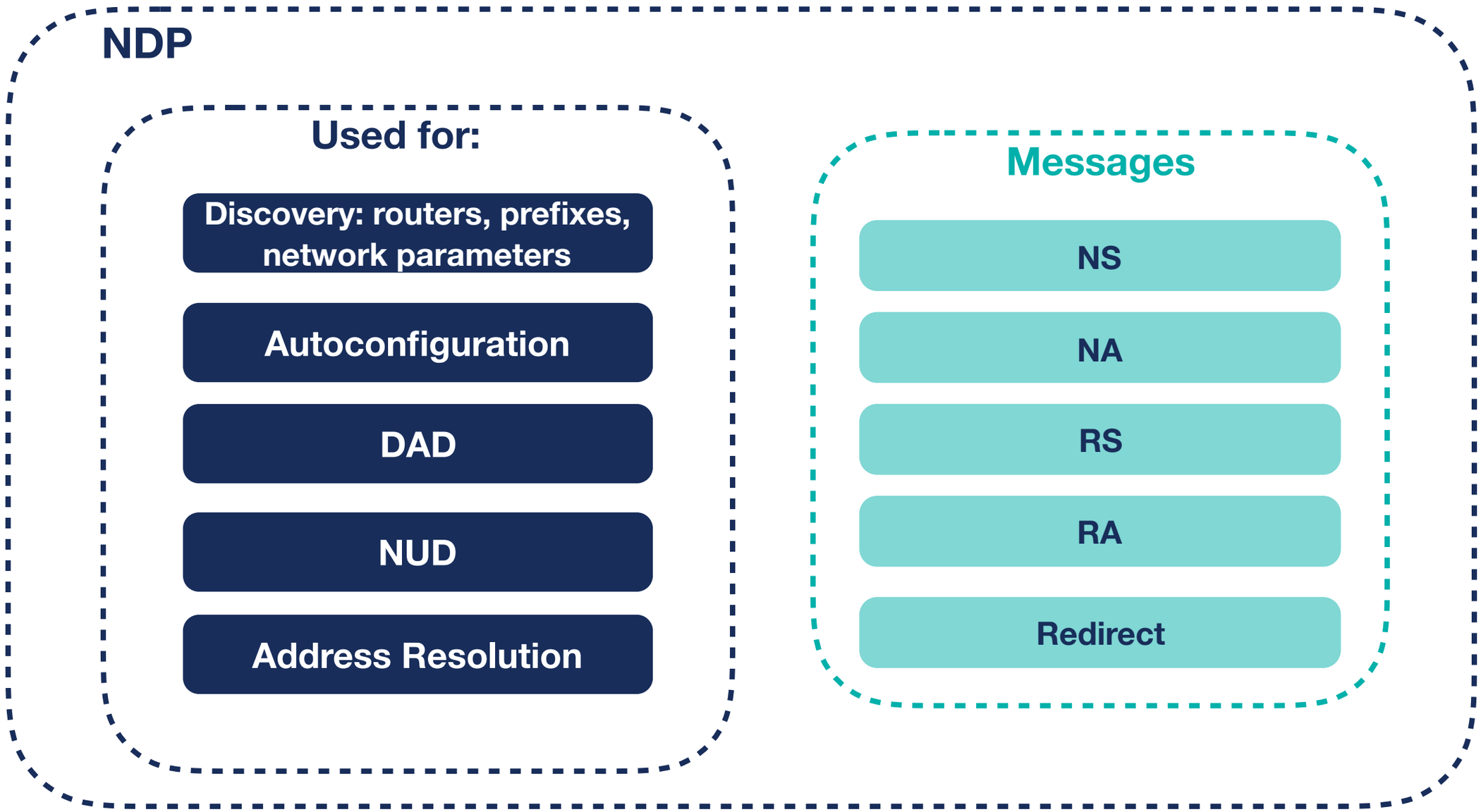
- Use hard to guess IIDs
  - RFC 7217 better than EUI-64
  - RFC 8064 establishes RFC 7217 as the default
- Use IPS/IDS to detect scanning
- Filter packets where appropriate
- Use "default" /64 size IPv6 subnet prefix

IPv6 Associated Protocols Security

NDP

Introduction (1)

- NDP [RFC4861] is used on a link



Introduction (2)

- Hop Limit = 255, if not, discard

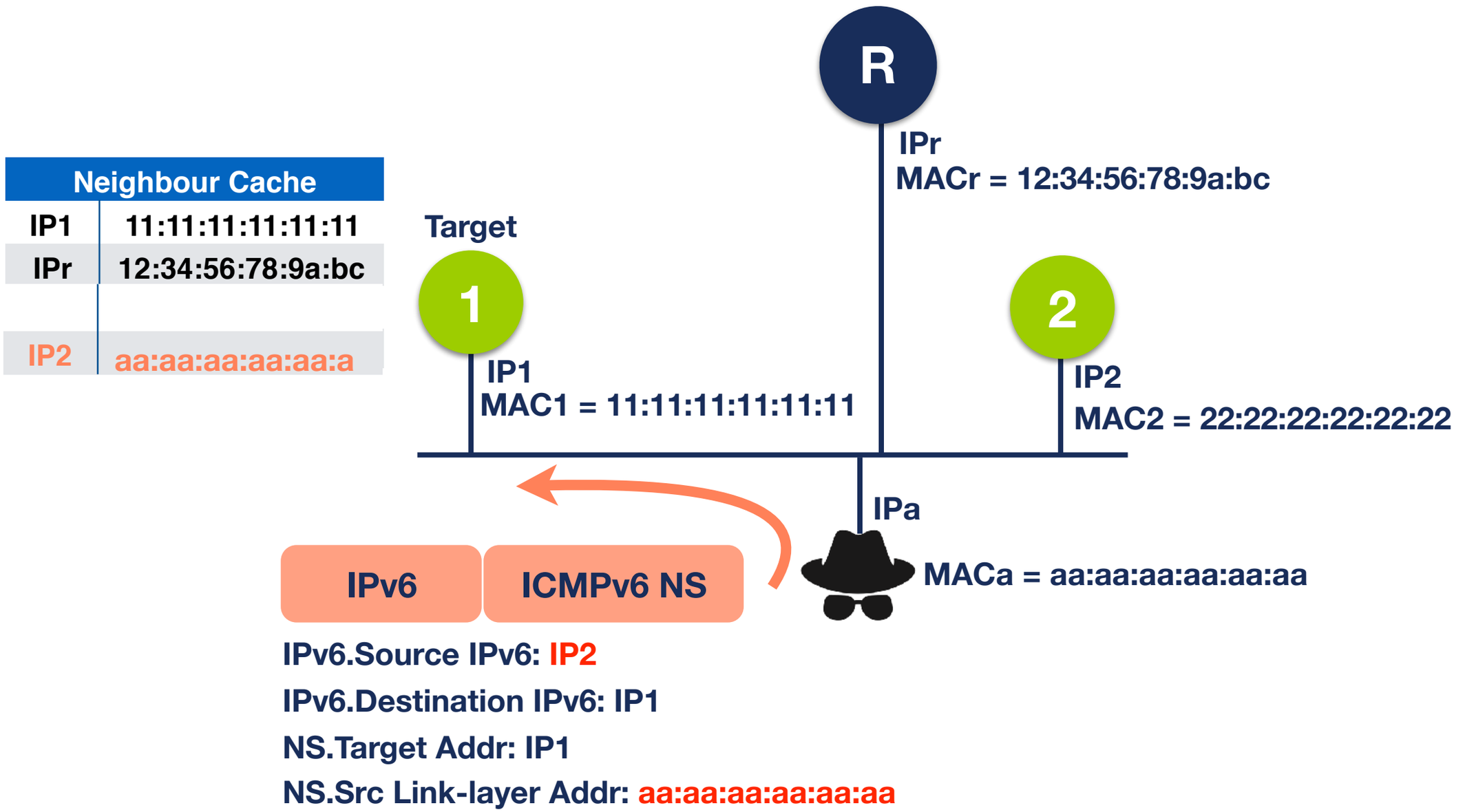
- NDP has vulnerabilities
  - [RFC3756] [RFC6583]

- NDP specification: use IPsec -> impractical, not used

- SEND (SEcure Neighbour Discovery): Not widely available
  - [RFC3971]

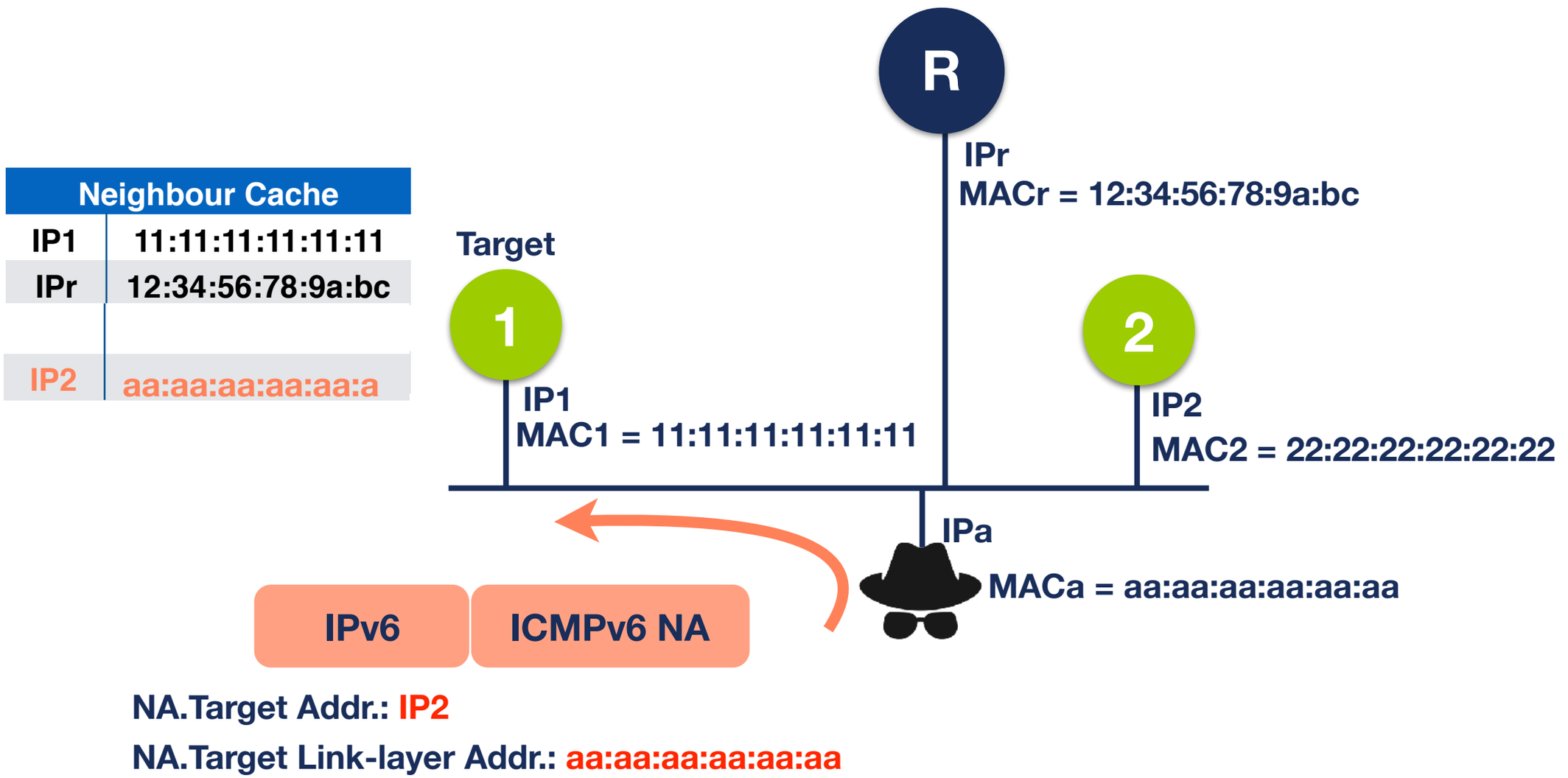
NDP Threats (1)

- NS: Redirection / DoS



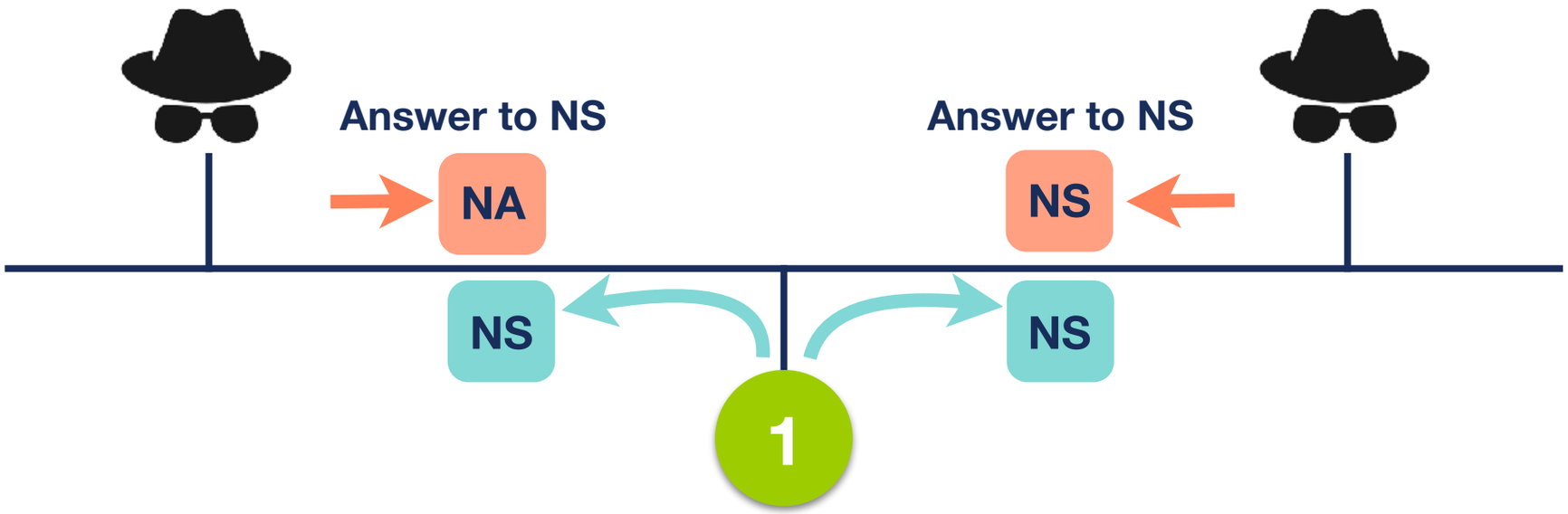
NDP Threats (2)

- Unsolicited NA: Redirection / DoS



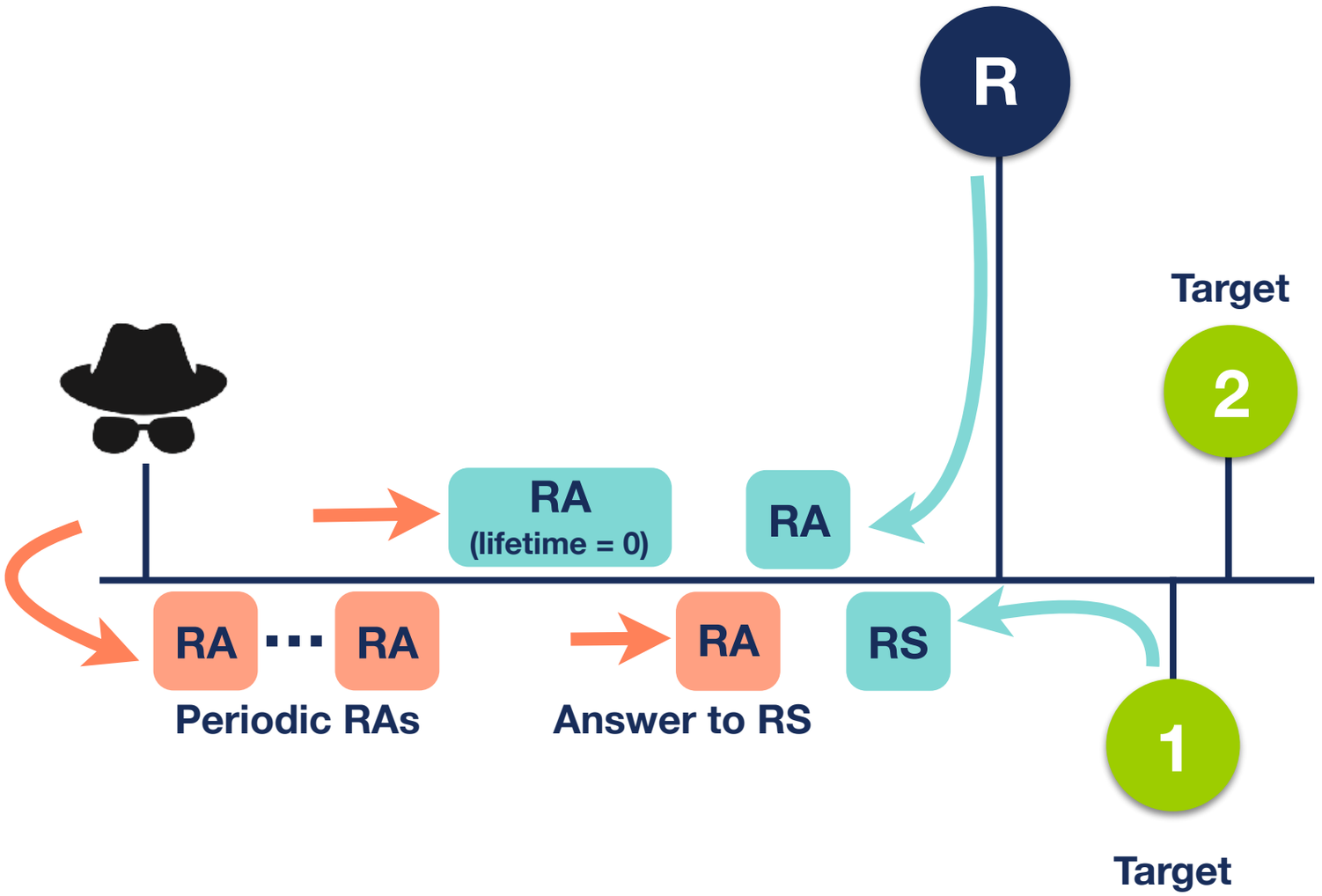
NDP Threats (3)

- DAD DoS Attack



NDP Threats (4)

- Malicious Last Hop Router



NDP Threats (5)

- **Bogus Address Configuration Prefix**

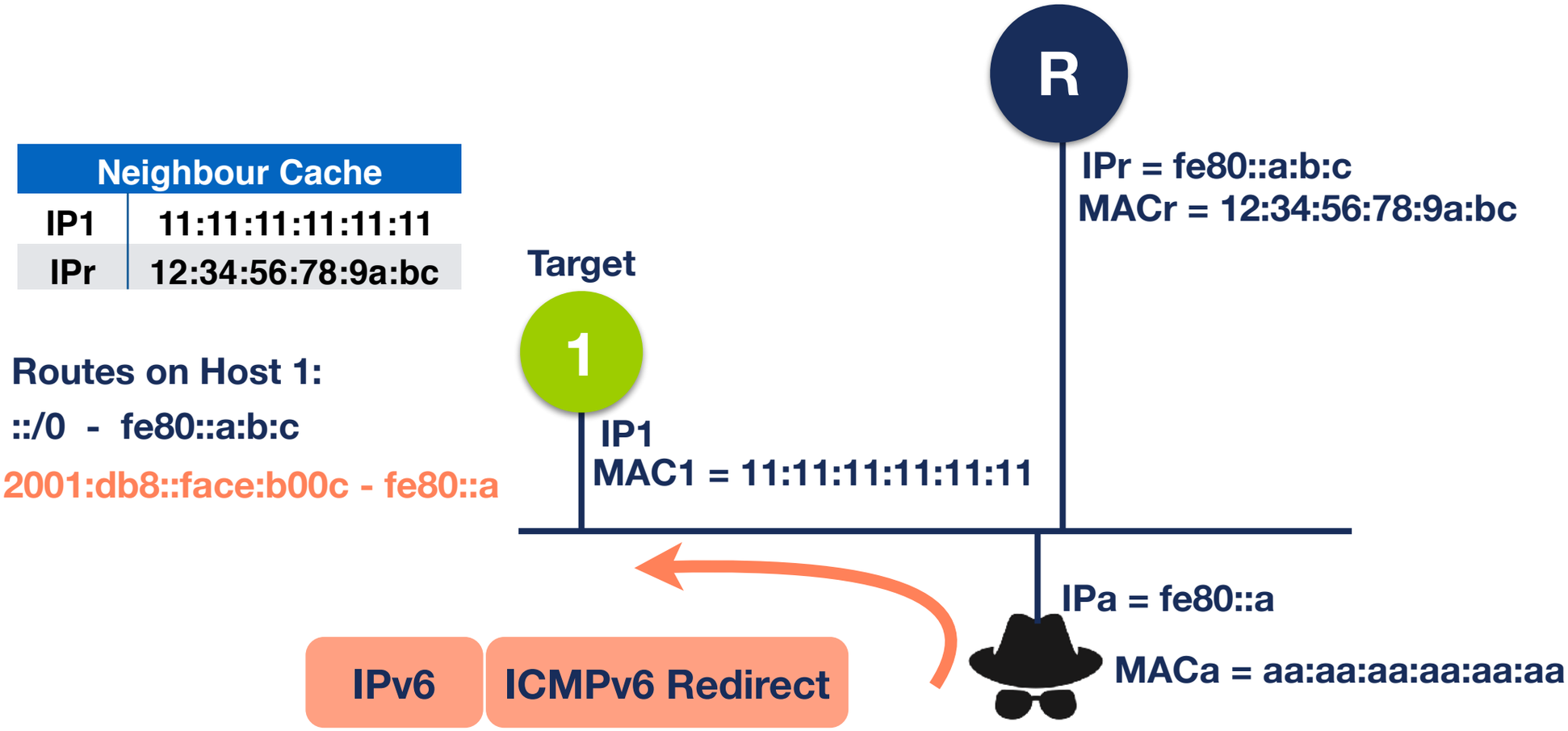
- Attacker sends RA with prefix for SLAAC
- Hosts using SLAAC will auto-configure an address using that prefix

- Return packets never reach the host

- DoS attack

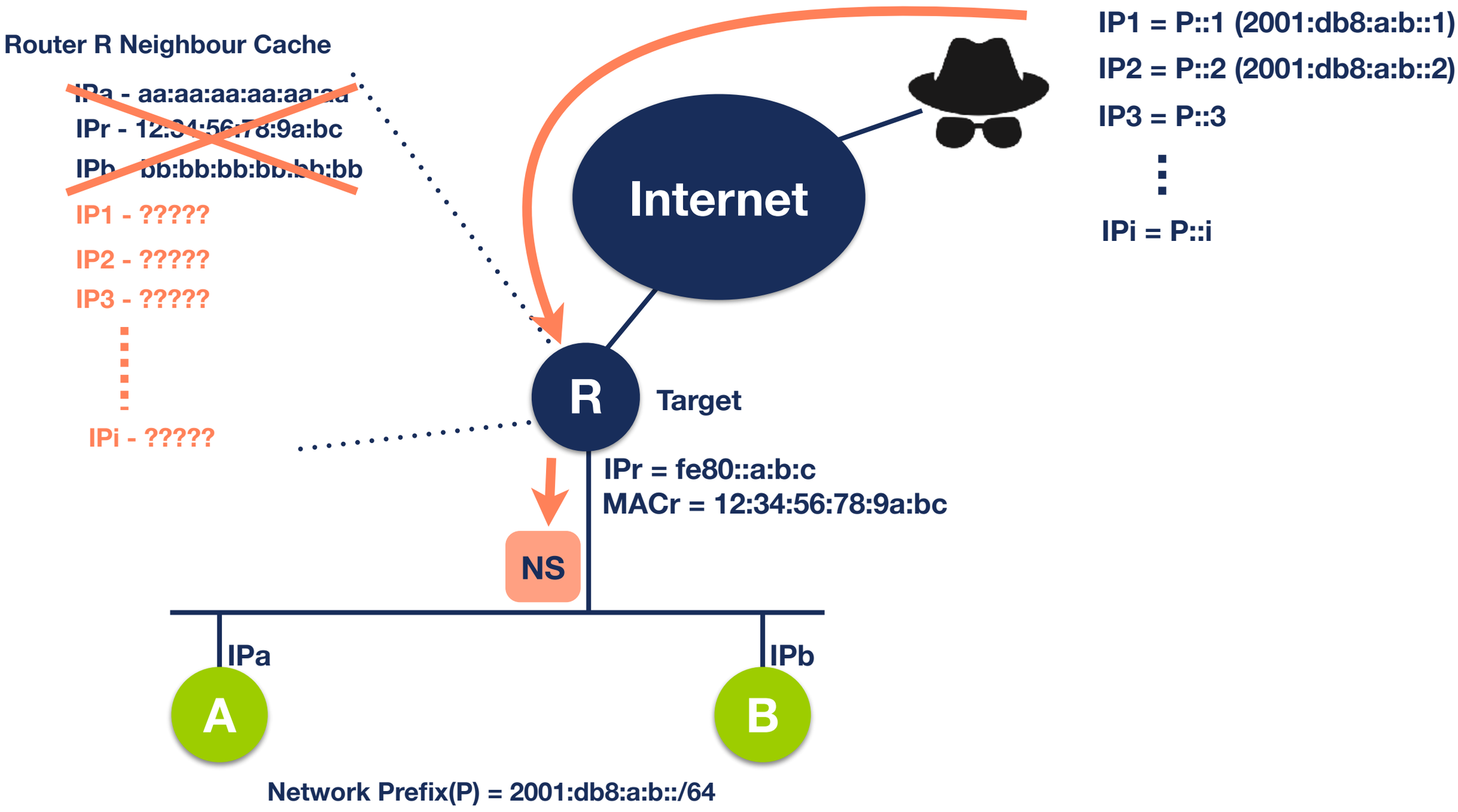
NDP Threats (6)

- Spoofed Redirect Message



NDP Threats (7)

- Neighbour Discovery DoS Attack

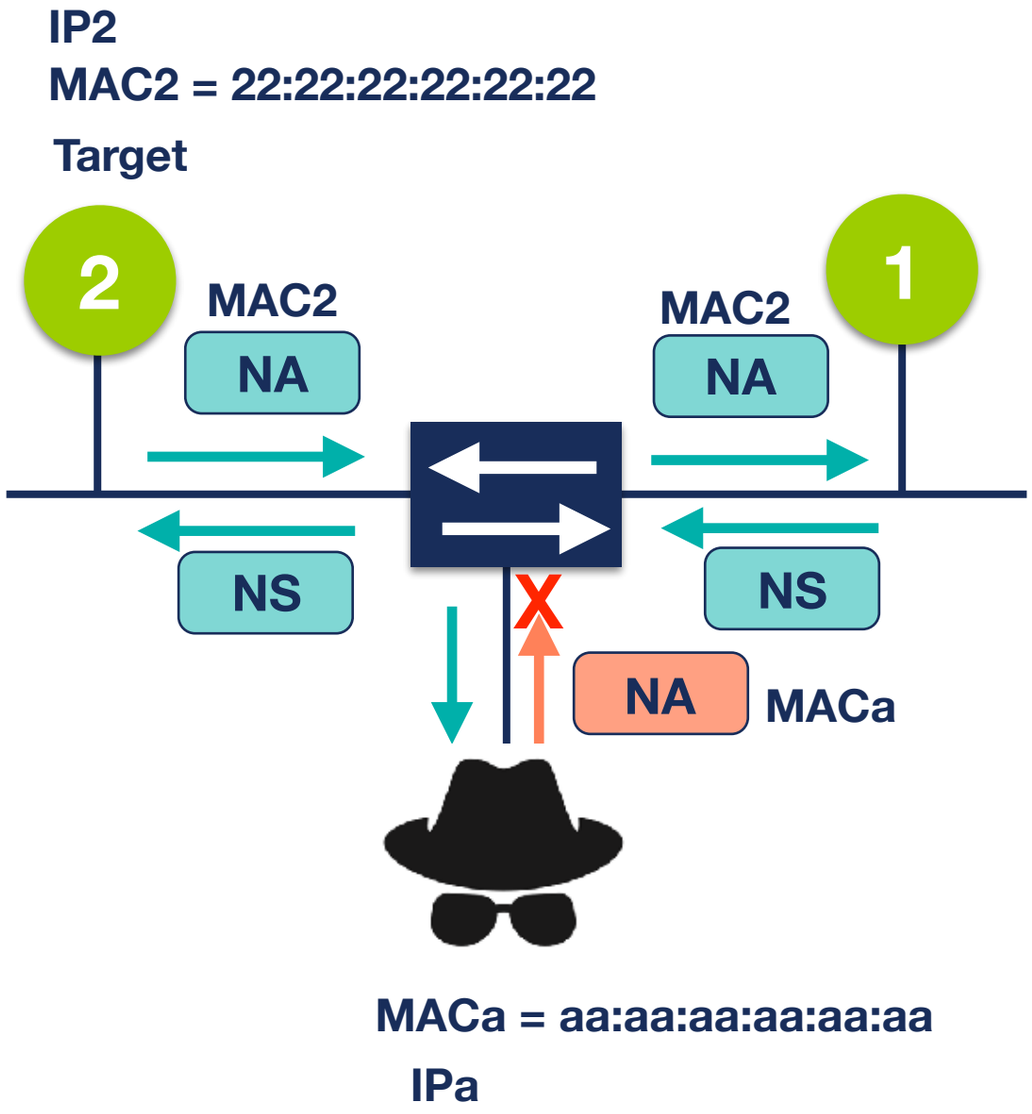


First Hop Security (1)

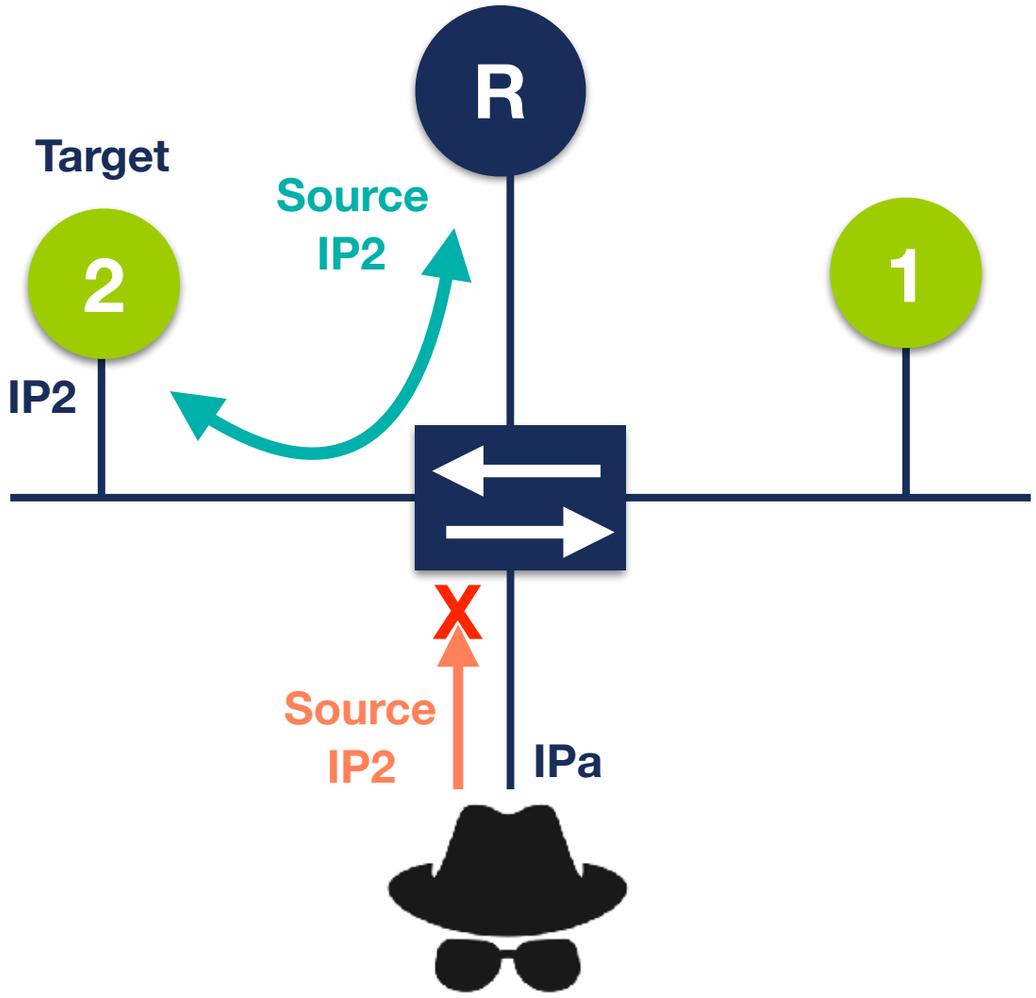
- Security implemented on switches

- There is a number of techniques available:
  - RA-GUARD
  - DHCPv6 Guard
  - IPv6 Snooping (ND inspection + DHCPv6 Snooping)
  - IPv6 Source/Prefix Guard
  - IPv6 Destination Guard (or ND Resolution rate limiter)
  - MLD Snooping

First Hop Security (2)



IPv6 Snooping



IPv6 Source/ Prefix Guard

RA-GUARD

- RA-GUARD [RFC6105] easiest and available solution
- Only allows RAs on legitimate port(s) on L2 switches

Stateless RA-Guard ..... **Decision based on RA message or static configuration**

Stateful RA-Guard ..... **Learns dynamically**

- Requires support on switches
- EHs were used to go through RA-Guard [RFC7113]

Conclusions / Tips

- NDP is an important, powerful and vulnerable protocol

- Some solutions are available to protect NDP

- Recommended: use available ones
  - Check availability and configure them

- Detection (IDS/IPS) could be easier and recommended

Multicast Listener Discovery (MLD)

Introduction

- Multicast Listener Discovery (MLD) is:
  - Multicast related protocol, used in the local link
  - Two versions: MLDv1 and MLDv2
  - Uses ICMPv6
  - Required by NDP and “IPv6 Node Requirements”
- IPv6 nodes use it when joining a multicast group

MLDv1

- Mandatory for all IPv6 nodes (MUST)

QUERY

Router asks for Listeners

General

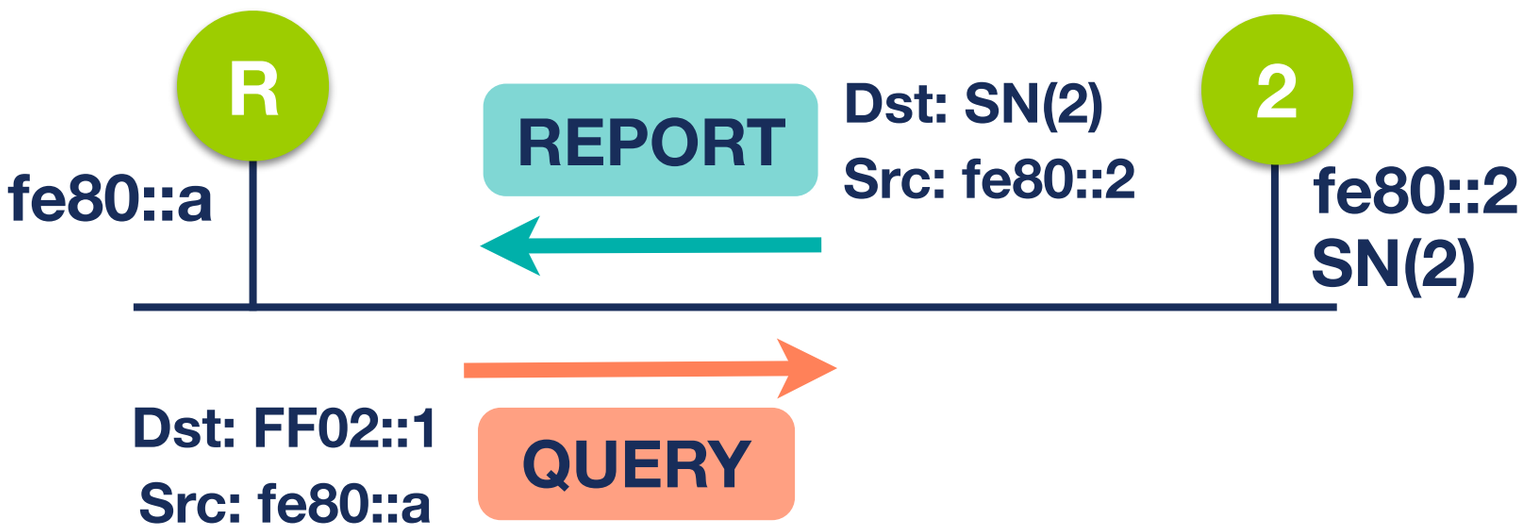
Specific

REPORT

Listeners report themselves

DONE

Listeners indicate they're done



MLDv2

- Strongly recommended for all IPv6 hosts (SHOULD)
- Interoperable with MLDv1
- Adds Source-Specific Multicast filters:
  - Only accepted sources; or
  - All sources accepted except specified ones

QUERY

- **General**
- **Specific**
- **Multicast Address and Source Specific**

REPORT-v2 **Sent to FF02::16**

- **Current State**
- **State Change (filter/sources)**

MLD Threats (1)

- Flooding of MLD messages

Lots of REPORTs

RAM Exhaustion

CPU Exhaustion

Solutions

Rate limit MLD states

Rate limit MLD messages

Disable MLD (if not needed)

- Traffic Amplification

Spoofed QUERY

Hosts send REPORTs

Several for each Addr.

Windows 8.1 = 8 Msgs.

Rate limit MLD messages

MLD Threats (2)

- Network scanning

Passive

Active QUERY

All Hosts (FF02::1)

Routers (FF02::2, FF02::16)

Windows (FF02::1:3, FF02::C)

MLD Solutions (1)

- MLD built-in security

Link-local source address

Hop Limit = 1

Router Alert option in Hop-by-Hop EH

Discard non compliant messages

- MLD Snooping [RFC4541]

Switch listens to REPORTs

MLD Table: maps multicast groups to ports that requested

Only allow multicast traffic on ports with listeners

MLD Solutions (2)

- Only allow QUERIES on router's port
  - Kind of MLD-Guard

```
deny icmp any any mld-query
```

- Protecting routers
  - Rate limit REPORTs from each host
  - Disable multicast/MLD functionality if not using inter-domain multicast routing

IPv6 Security Tips

Introduction

- Best security tool is knowledge
- IPv6 security is a moving target, keep updated
- IPv6 is happening: need to know about IPv6 security
- IPv6 quite similar to IPv4, many reusable practices

Overview: Devices

- Different categories (from RIPE-554):

Host

- **IPSec (if needed)**
- RH0 [RFC5095]
- **Overlapping Frags [RFC5722]**
- **Atomic Fragments [RFC6946]**
- **NDP Fragmentation [RFC6980]**
- **Header chain [RFC7112]**
- **Stable IIDs [RFC8064][RFC7217] [RFC7136]**

Disable if not used: LLMNR, mDNS, DNS-SD, IPv6 DNS Autodiscovery, transition mechanisms

Switch

- **HOST +**
- **IPv6 ACLs**

FHS

- **RA-Guard [RFC6105]**
- **DHCPv6 guard**
- **IPv6 snooping**
- **IPv6 source / prefix guard**
- **IPv6 destination guard**
- **MLD snooping** [RFC4541]
- **DHCPv6-Shield** [RFC7610]

Router

- **HOST +**
- **Ingress Filtering and RPF**
- **DHCPv6 Relay [RFC8213]**

OSPFv3

- **Auth. [RFC4552]**
- **or/and [RFC7166]**

IS-IS

- **[RFC5310]**
- **or, less preferred, [RFC5304]**

MBGP

- **TCP-AO** [RFC5925]
- **Obsoleted** MD5 Signature Option [RFC2385]
- **MBGP Bogon prefix filtering**

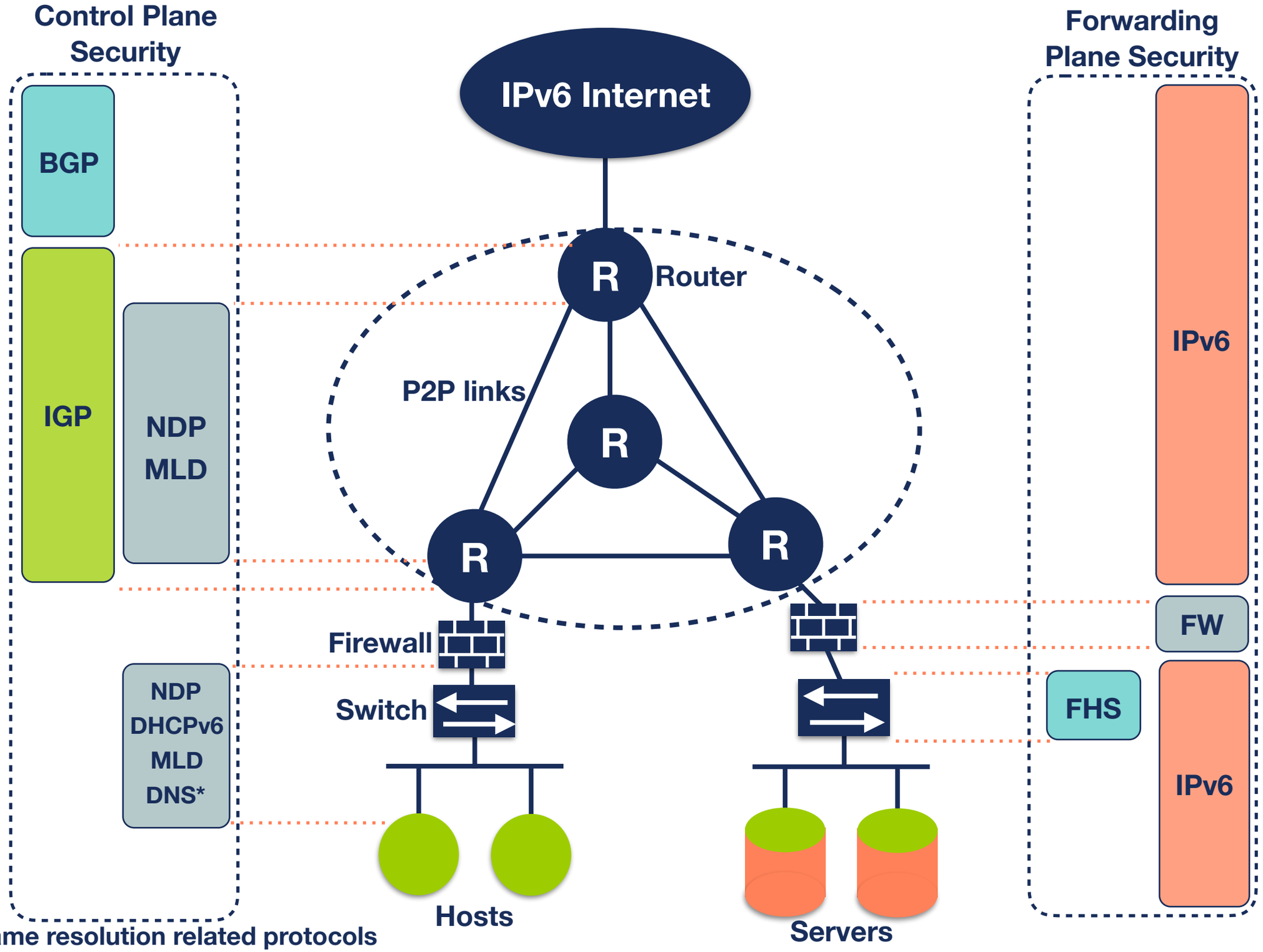
Security Equipment

- **HOST +**
- **Header chain [RFC7112]**
- **Support EHs Inspection**
- **ICMPv6 fine grained filtering**
- **Encapsulated Traffic Inspection**
- **IPv6 Traffic Filtering**

CPE

- **Router**
- **Security Equipment**
- **DHCPv6 Server Privacy Issues**

Overview: Network Example



* All Name resolution related protocols

RIPE NCC Academy

Graduate to the next level!

http://academy.ripe.net

Follow us!

@TrainingRIPENCC

Questions