RIPE NCC
RIPE NETWORK COORDINATION CENTRE

IPv6 Security

Training Course

February 2024

Copyright Statement

RIPE NCC Training Material

Please find your training material at the following link

https://www.ripe.net/training-material

09:00 - 09:30	Coffee, Tea
11:00 - 11:15	Break
13:00 - 14:00	Lunch
15:30 - 15:45	Break
17:30	End

Introductions

- Name
- Experience with Security and IPv6
- Goals

Introduction

Basic IPv6 Protocol Security

Basic header, Extension Headers, Addressing

IPv6 Associated Protocols Security

ICMPv6, NDP, MLD, DNS, DHCPv6

Internet-wide IPv6 Security

Filtering, DDoS, Transition Mechanisms

Tips and Tools

Up-to-date information, Security Tools, Device features

Legend

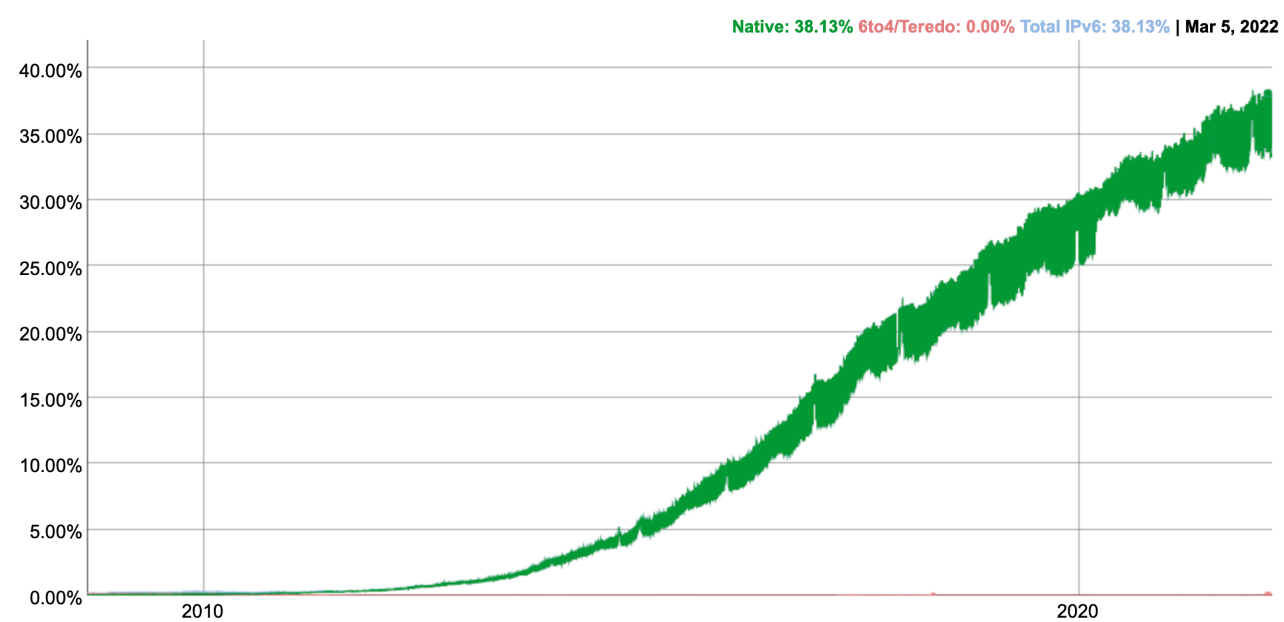
Introduction to IPv6 Security

Section 1

IPv6 is Happening…

RANK	IPV6%	COUNTRY / REGION
1	59.3%	India
2	57.2%	Belgium
3	53.9%	Germany
4	52.1%	Saudi Arabia
5	51%	Montserrat
6	50.5%	Uruguay
7	50.4%	Malaysia
8	49.6%	France
9	48.1%	Viet Nam
10	47.9%	Japan
11	47.8%	Greece
12	46.6%	Luxembourg
13	45.1%	Switzerland
14	43.8%	Mexico

Rank	Participating Network	ASN(s)	IPv6 deployment
1	RELIANCE JIO INFOCOMM LTD	55836, 64049	93.63%
2	Comcast	7015, 7016, 7725, 7922, 11025, 13367, 13385, 20214, 21508, 22258, 22909, 33287, 33489, 33490, 33491, 33650, 33651, 33652, 33653, 33654, 33655, 33656, 33657, 33659, 33660, 33661, 33662, 33664, 33665, 33666, 33667, 33668, 36732, 36733	70.92%
3	Combined US Mobile Carriers	3651, 6167, 10507, 20057, 21928, 22394	87.44%
4	Charter Communications	7843, 10796, 11351, 11426, 11427, 12271, 20001, 20115, 33363	53.56%
5	ATT	6389, 7018, 7132	73.48%
6	T-Mobile USA	21928	92.42%
7	Deutsche Telekom AG	3320	72.69%
8	Orange Business Services	3215	71.28%
9	Claro Brasil	4230, 28573	72.87%
10	Verizon Wireless	6167, 22394	83.10%



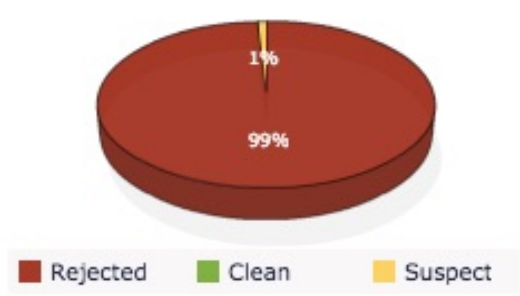
Source: **http://worldipv6launch.org/measurements/ (24/3/2022)**

… and So Are IPv6 Security Threats!

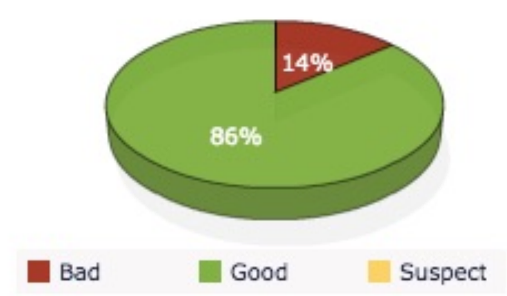
ReputationAuthority At Work

Unwanted Email & Web Traffic

Rejected At Perimeter



Suspect Traffic Analysis



Top Offending IP Address

	IP Address	Country
1	2a01:4f8:c17:2052::2	Germany
2	2a01:4f8:c17:42f8::2	Germany
3	2a01:4f8:c17:3fe7::2	Germany
4	2a01:4f8:c17:49fa::2	Germany
5	2a01:4f8:c17:3fe5::2	Germany
6	2a01:4f8:c17:1799::2	Germany
7	2a01:4f8:c17:3d8c::2	Germany
8	2a01:4f8:c17:3d83::2	Germany
9	2a01:4f8:c17:2ddf::2	Germany
10	103.18.244.67	Malaysia

Phishing By Top Level Domains

	LTD	Location	Phishing / 10,000
1	hk	Hong Kong	112.9
2	th	Thailand	53.8
3	li	Liechtenstein	44.1
4	ro	Romania	13.0
5	cl	Chile	11.4
6	bz	Belize	11.3
7	tw	Taiwan	10.6
8	it	Lithuania	10.1
9	ee	Estonia	9.4
10	cz	Czech Repub	8.9

Top Virus Threats

	IP Address	Country
1	60.250.172.197	Taiwan, Province O
2	188.94.11.162	Spain
3	198.74.61.67	United States
4	80.67.18.3	Germany
5	2a02:408:7722:1:77:222:40:221	Russian Federation
6	2a02:408:7722:1:77:222:62:66	Russian Federation
7	170.169.130.68	Mexico
8	216.168.135.166	United States

IPv6 Security Statements

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 8504 - IPv6 Node Requirements: IPsec **SHOULD**
- IPsec available. Used for security in IPv6 protocols

IPv6 Security Statements

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 Statements

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 Statements

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 Statements

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 Statements

1	2	3	4	5	6	7	8

- IPv6 support is a yes/no question

Reason:

- Question: “Does it support IPv6?”
- Answer: “Yes, it supports IPv6”

Reality:

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

IPv6 Security Statements

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

- IPv6 is not a security problem in my IPv4-only network

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 Statements

1	2	3	4	5	6	7	8

- It is 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

Section 2

IPv6 Basic Header and Extension Headers

Section 2.1

Basic IPv6 Header: Threat #1

Version	Traffic Class	Flow Label
Payload Length	Next Header	Hop Limit
Source Address		
Destination Address		

Basic IPv6 Header: Threat #1

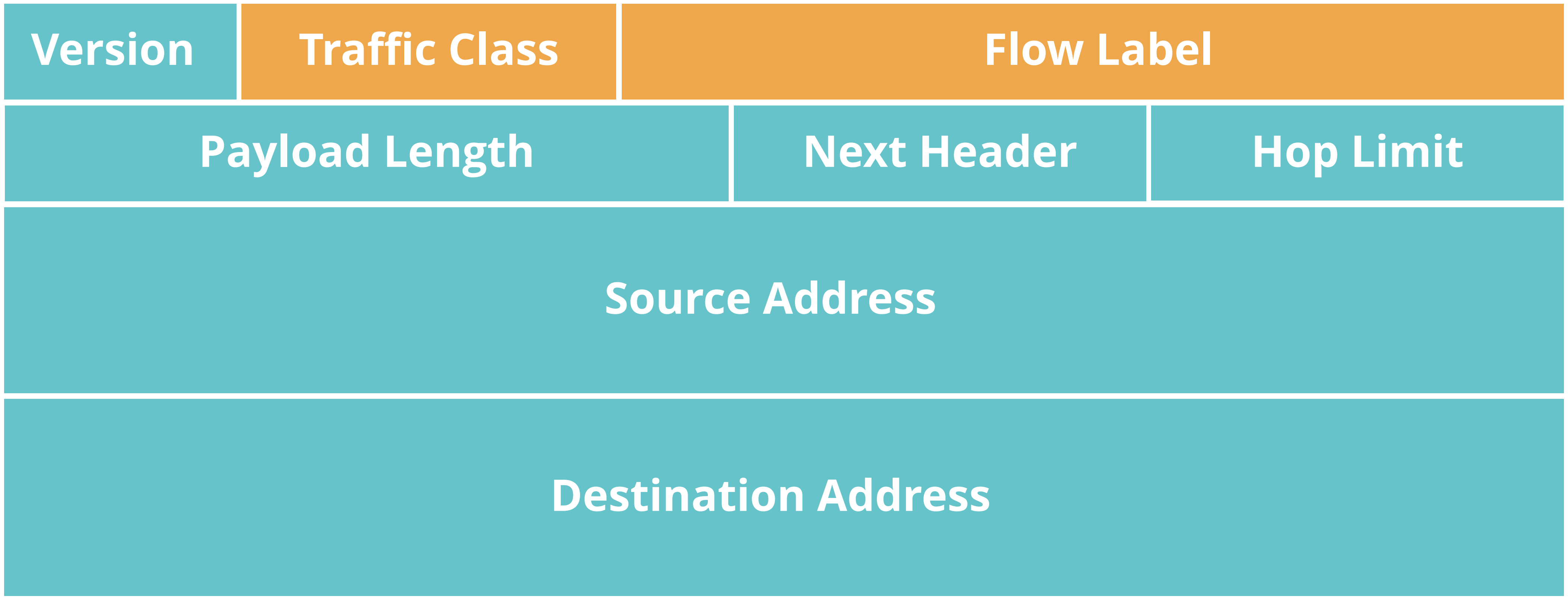
IP spoofing:

Using a fake IPv6 source address

Solution:

ingress filtering and RPF (*reverse path forwarding*)

Basic IPv6 Header: Threat #2



Basic IPv6 Header: Threats #2

Covert Channel:

Using Traffic Class and/or Flow Label

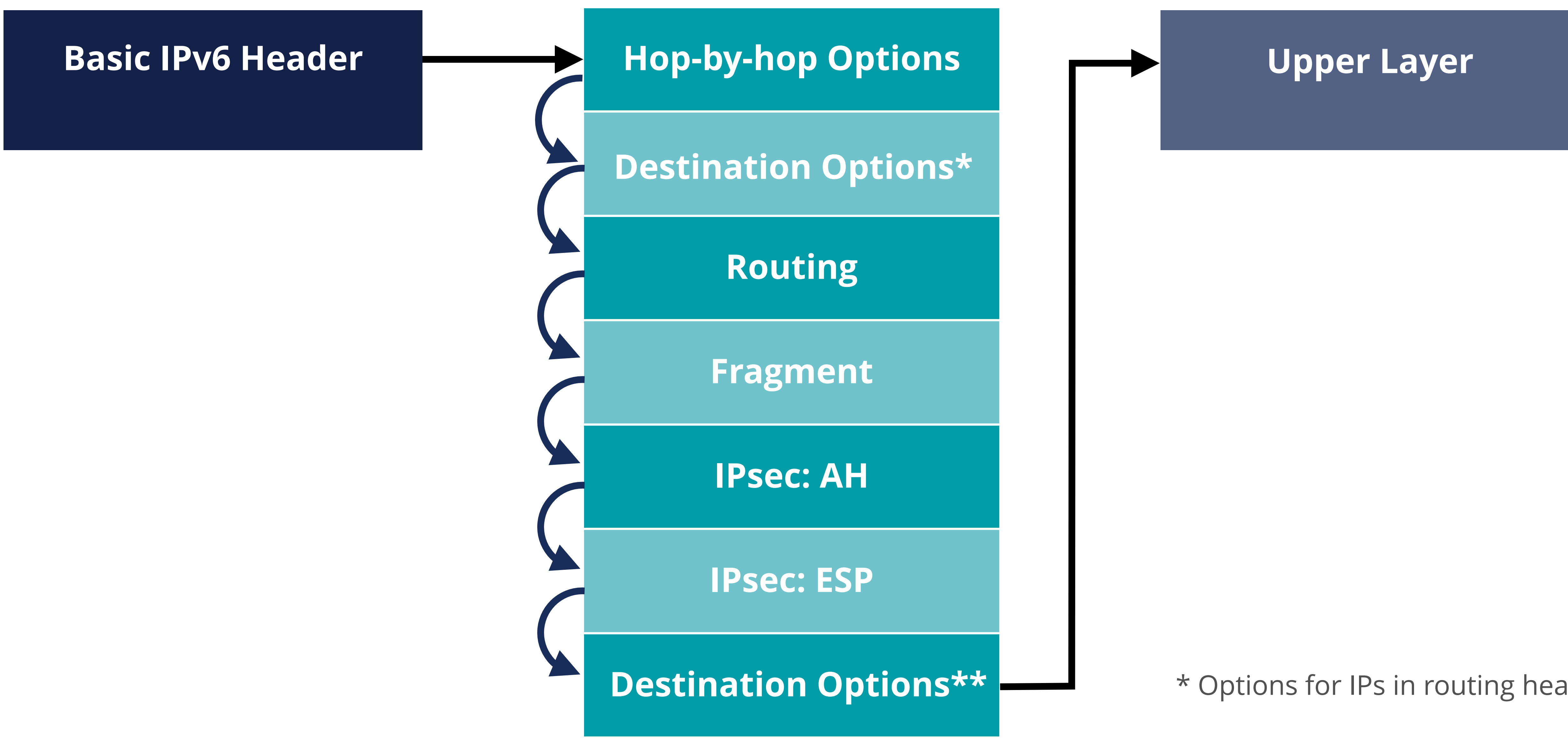
Solution:

Inspect packets (IDS / IPS)

Expected values:

- Traffic Class: 0 (*unless QoS is used*)
- Flow Label: 0

IPv6 Extension Headers



* Options for IPs in routing header

** Options for destination IP

Extension Headers Properties

1	**Flexible** *(use is optional)*
2	**Only appear once** *(except Destination options)*
3	**Fixed** *(types and order)*
4	**Processed only at endpoints** *(except Hop-by-Hop and Routing)*

- Flexibility means **complexity**
- Security devices / software must process the **full chain of headers**
- Firewalls must be able to filter based on **Extension Headers**

Routing Header

Includes one or more IPs that should be "*visited*" in the path

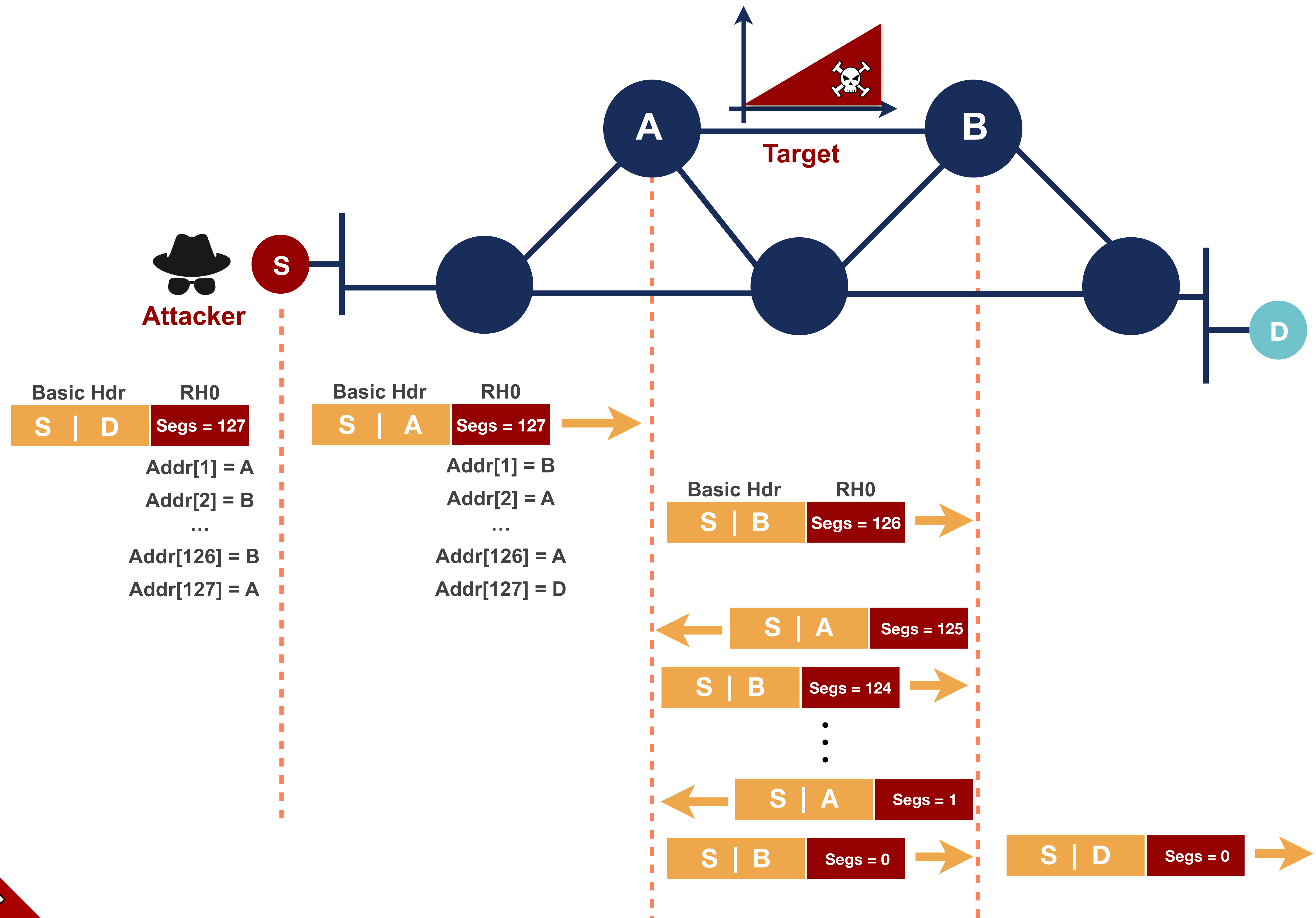
- Processed by the **visited routers**

8 bits	8 bits	8 bits	8 bits
Next Header	Length	Routing Type	Segments Left
Specific data of that Routing Header type			

Routing Header Threat

- **Routing Header** (**Type 0**):
  - RH0 can be used for traffic amplification over a remote path
- **RH0 Deprecated** [*RFC5095*]
  - RH1 deprecated. RH2 (MIPv6), RH3 (RPL) and RH4 (SRH) are valid

RH0 Fields	**Address[1]**	**Address[2]**	...	**Address[n]**


Target
A
B
S
Attacker
D
Basic Hdr
RH0
S | D
Segs = 127
Addr[1] = A
Addr[2] = B
...
Addr[126] = B
Addr[127] = A
Basic Hdr
RH0
S | A
Segs = 127
Addr[1] = B
Addr[2] = A
...
Addr[126] = A
Addr[127] = D
Basic Hdr
RH0
S | B
Segs = 126
S | A
Segs = 125
S | B
Segs = 124
S | A
Segs = 1
S | B
Segs = 0
S | D
Segs = 0

Extension Headers Solutions

Use of RH0 → **Deprecated** [RFC5095]
Do not use or allow

- Require security tools to inspect Header Chain properly

Fragment Header

- Used by IPv6 source node to send a packet **bigger than path MTU**
- **Destination host** processes fragment headers

8 bits	8 bits	13 bits	2 bits	1 bit
Next Header	Reserved	Fragment Offset	Res	M
Identification				
32 bits				

M Flag:

1 = more fragments to come;

0 = last fragment

EH Threats: Fragmentation

Overlapping Fragments	Fragments that overlap because of wrong “fragment offset”
Not Sending Last Fragment	Waiting for last fragment Resource consumption
“Atomic” Fragments	Packet with Frag. EH is the only fragment (Frag. Offset and M = 0)

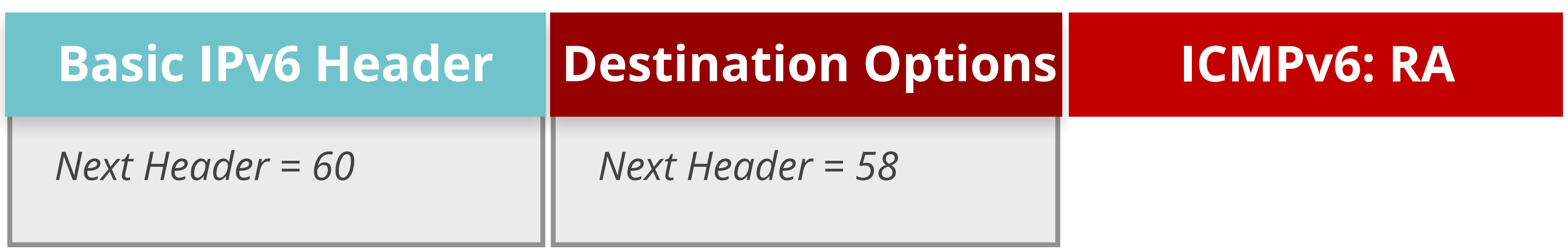
?

EH Solutions: Fragmentation

Overlapping Fragments	Not allowed in IPv6 [RFC5722] Packets are discarded
Not Sending Last Fragment	Timer and discard packets (default 60 secs)
“Atomic” Fragments	Processed in isolation from any other packets/fragments [RFC6946]

Bypassing RA Filtering/RA-Guard

Using **any** Extension Header



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

Bypassing RA Filtering/RA-Guard

Using **Fragment** Extension Header

Basic IPv6 Header	Fragment	Destination Options
Next Header = 44	*Next Header = 60*	*Next Header = 58*

Basic IPv6 Header	Fragment	Destination Options	ICMPv6: RA
Next Header = 44	*Next Header = 60*	*Next Header = 58*	

Needs all fragments to detect the RA

Extension Headers Solutions

Fragmented NDP packets

Forbidden [RFC6980]
Do not use or allow

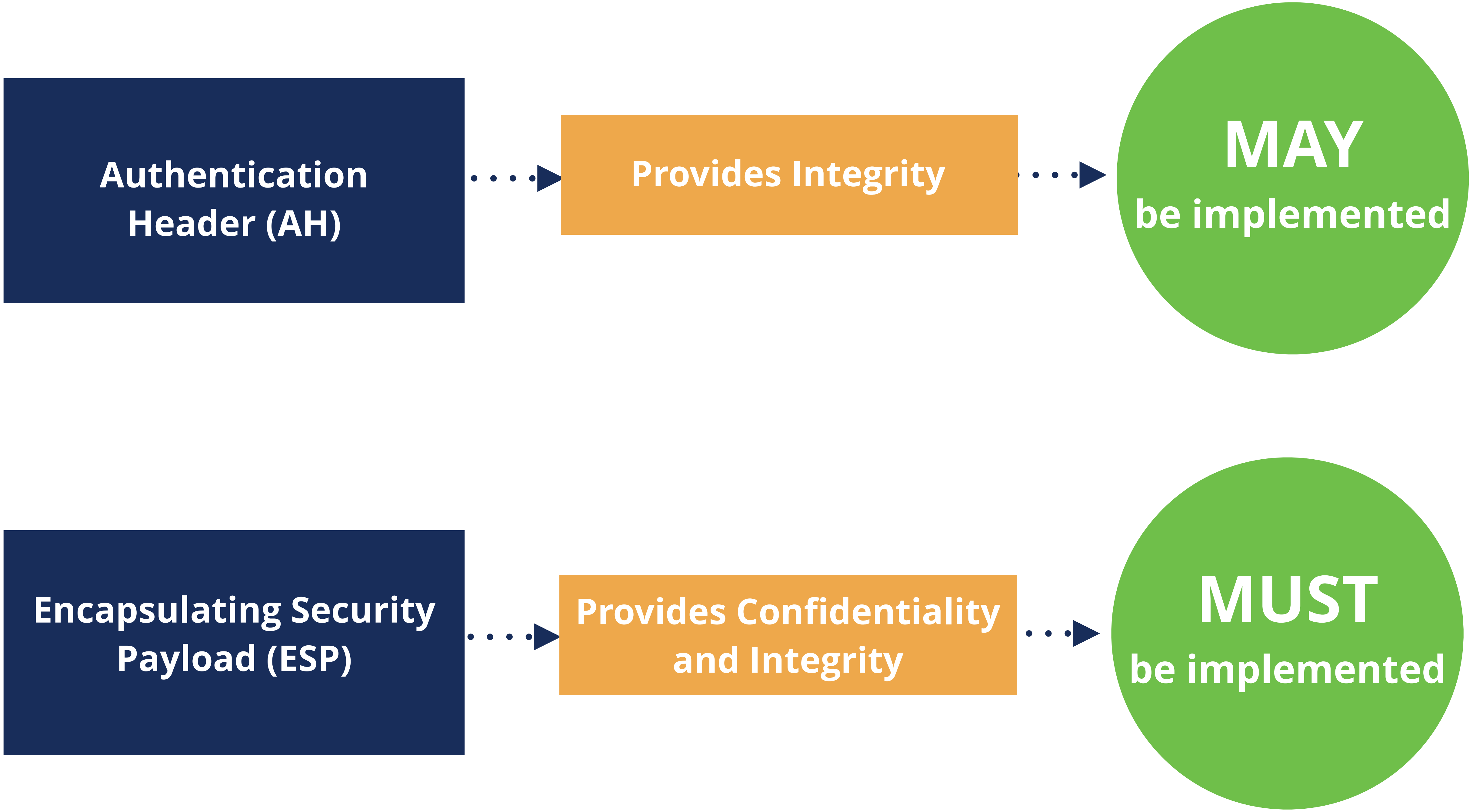
Other attacks based on Extension Headers

Header chain should go in the first fragment [RFC7112]

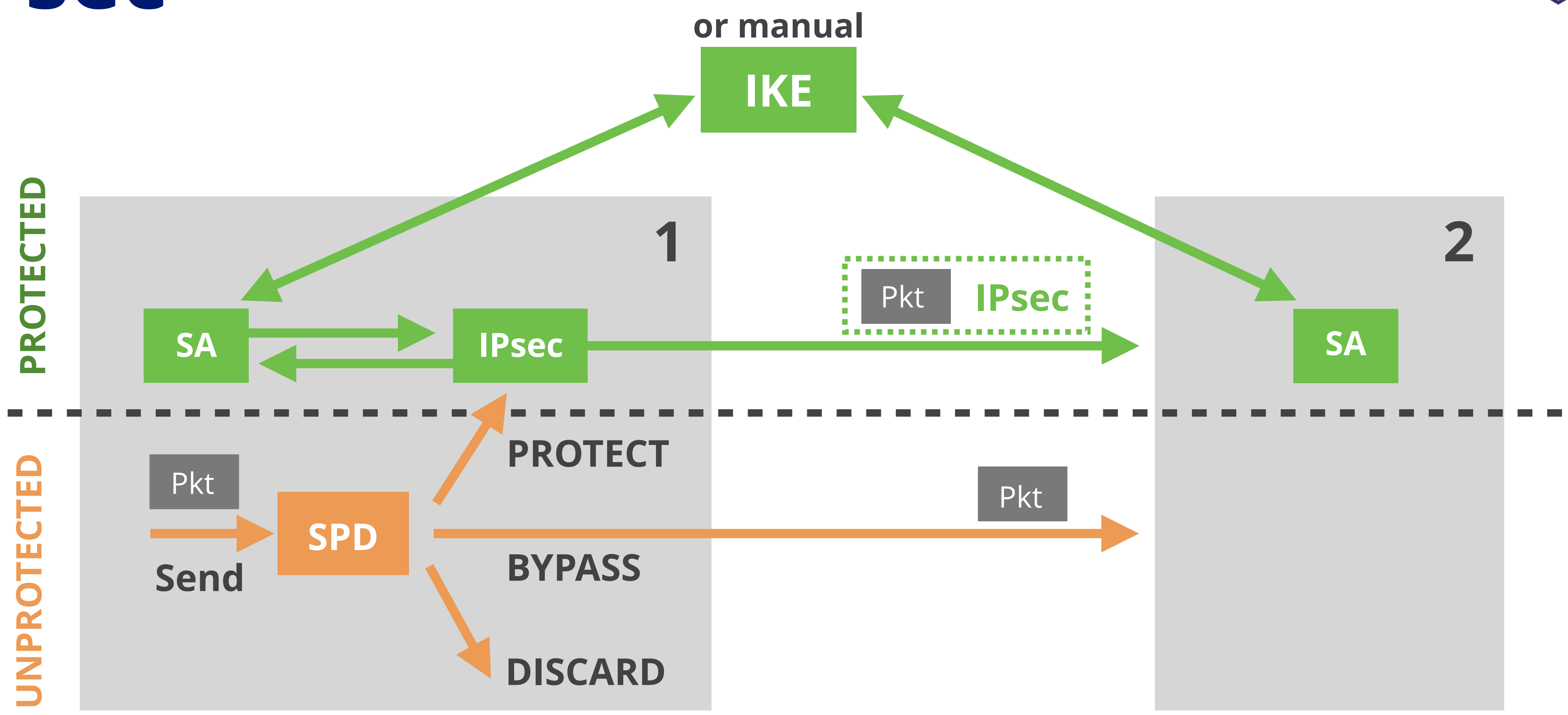
Recommendations to avoid the problem [RFC7113]

- **Require** security tools to inspect Header Chain properly

IPsec - Security Protocols



IPsec



SPD **Security Policy Database** indicates what to do with packets

SA **Security Association:** info needed for IPsec with 1 host, 1 direction

IKE **Internet Key Exchange** allows automatic creation of SAs

IPsec Modes

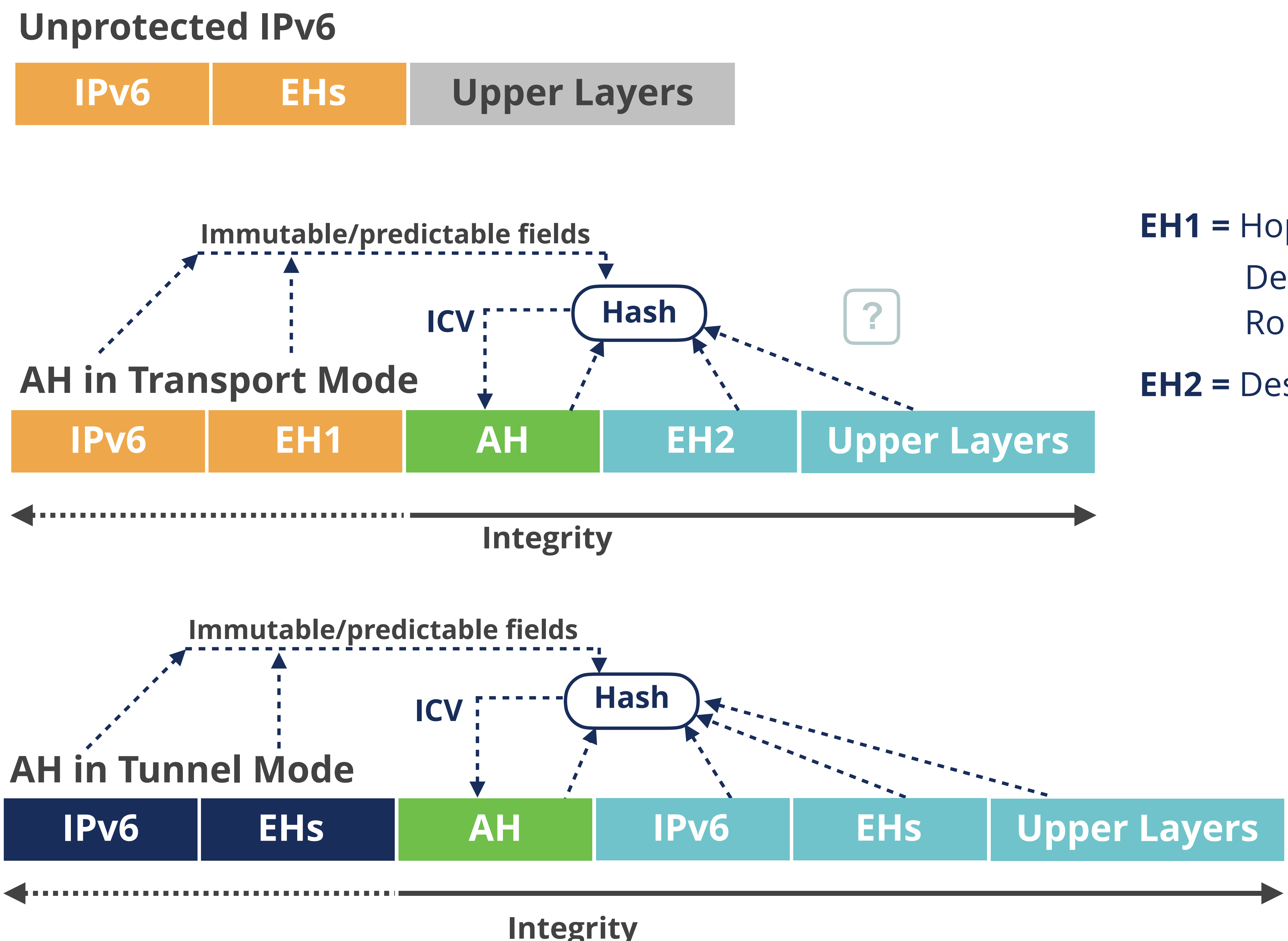
Tunnel Mode

IPv6 | IPsec | IPv6 | Upper Layers

Transport Mode

IPv6 | IPsec | Upper Layers

IPsec: Authentication Header



EH1 = Hop-by-Hop,
Dest. Options*,
Routing, Fragment

EH2 = Destination Options**

* Options for IPs in routing header

** Options for destination IP

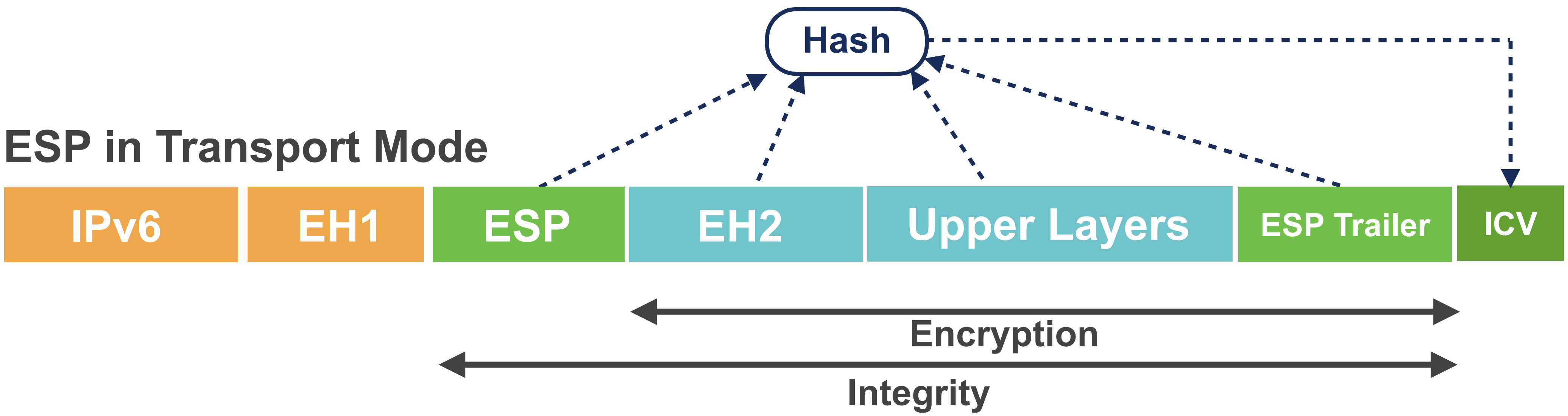
IPsec: ESP

Unprotected IPv6

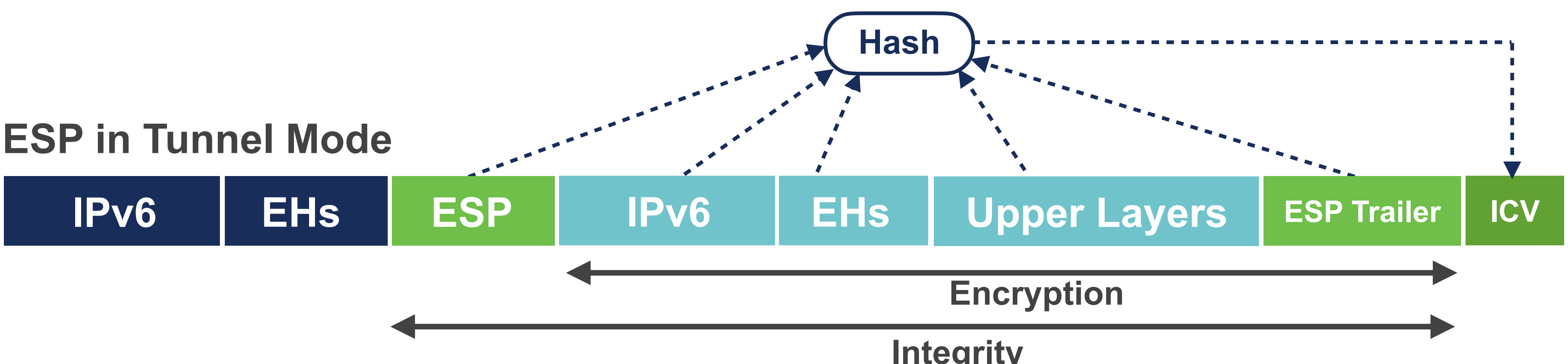
EH1 = Hop-by-Hop,
Dest. Options*,
Routing, Fragment

EH2 = Destination Options**

ESP in Transport Mode



ESP in Tunnel Mode



* Options for IPs in routing header

** Options for destination IP

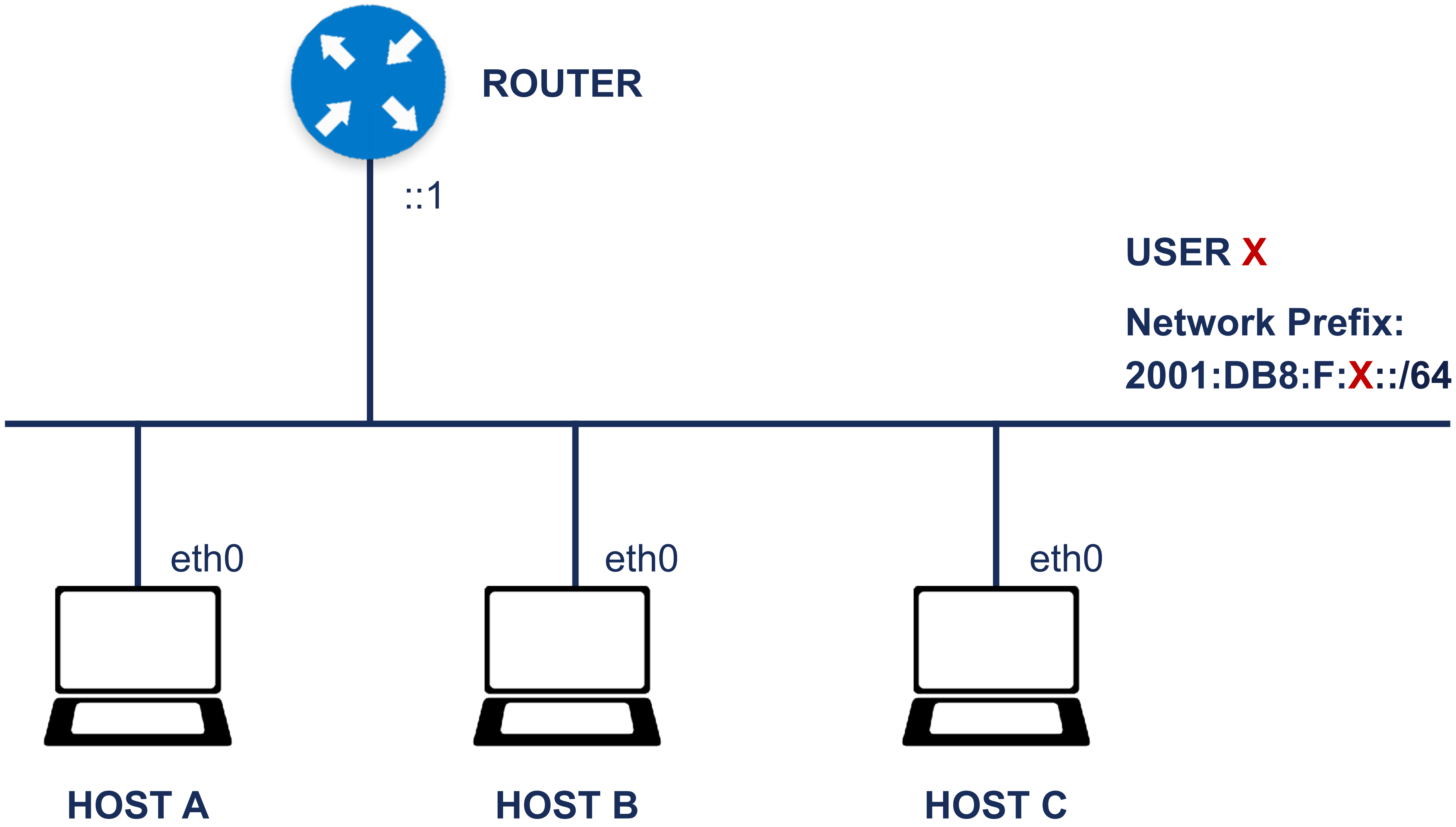
IPv6 Packet Generation

Exercise 2.1

Exercise 2.1: IPv6 Packet Generation

- **Description**: Use Scapy to generate IPv6 packets
- **Goals**:
  - Get familiar with lab environment
  - Learn the basics of Scapy tool
  - Learn to generate tailor made IPv6 packets
- **Time**: 30 minutes
- **Tasks**:
  - Login in to the lab environment
  - Generate IPv6 packets following instructions in Exercise Booklet

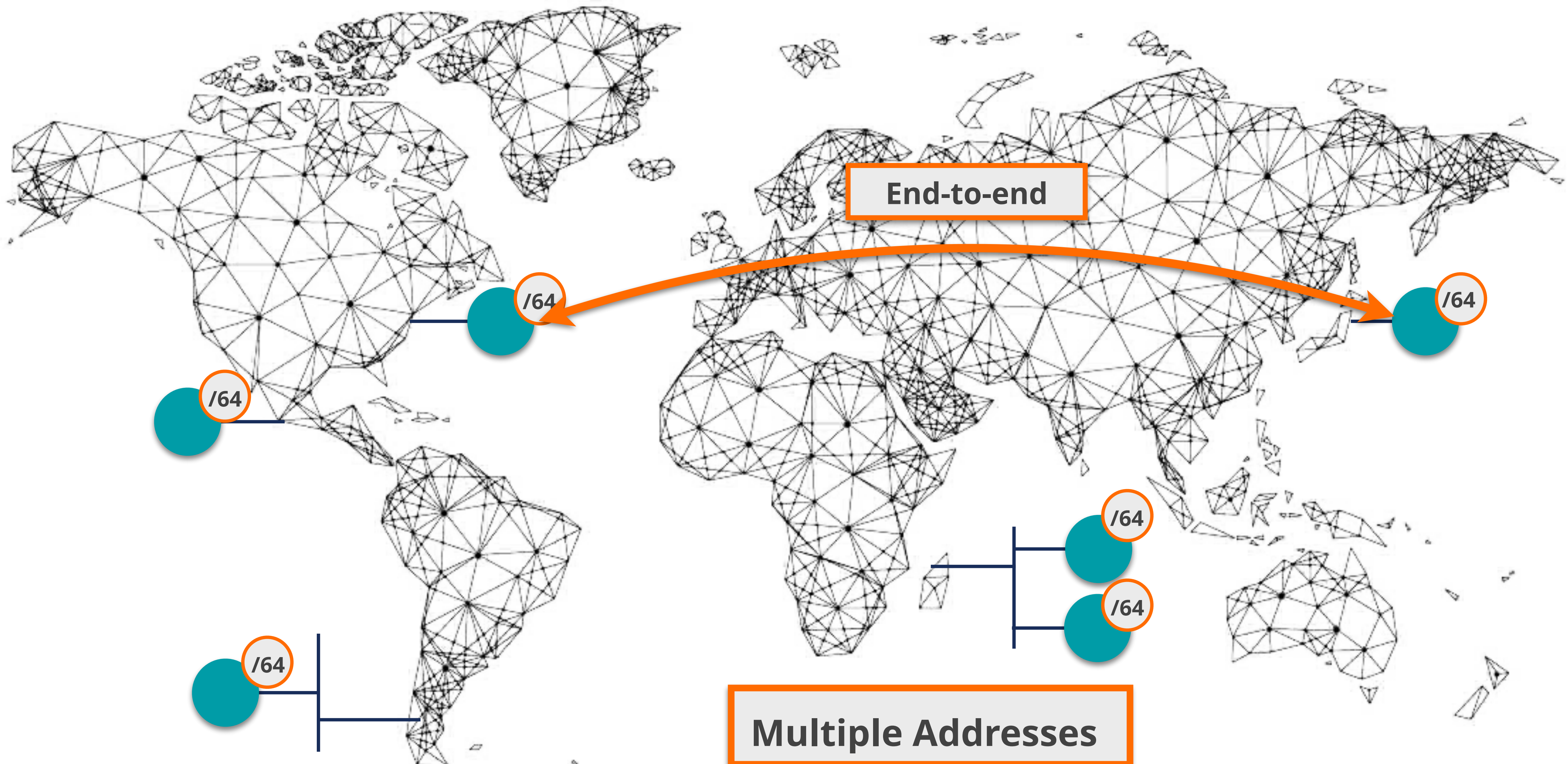
Exercise 2.1: Lab network



IPv6 Addressing Architecture

Section 2.2

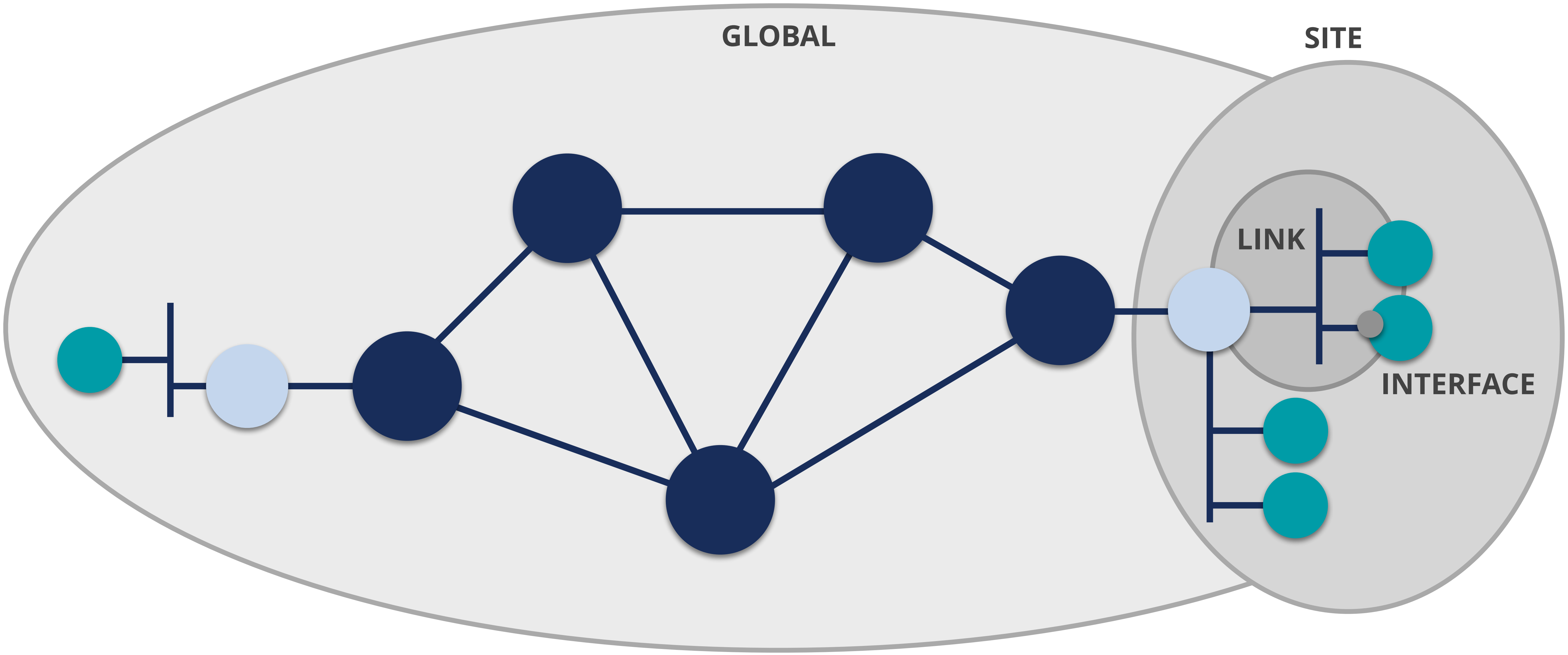
340,282,366,920,938,463,463,374,607,431,768,211,456



Multiple Addresses

Link-local
Global (GUA)
Multicast

IPv6 Address Scope



fe80::a:b:100

ff01::2

2001:67c:2e:1::c1

fd00:a:b::100

ff05::1:3

ff02::1

IPv6 Network Scanning

64 bits	64 bits
Network Prefix	**Interface ID (IID)**

Network Prefix determination (64 bits)

- Common patterns in addressing plans
- DNS direct and reverse resolution
- Traceroute

Interface ID determination (64 bits)

- "brute force" no longer possible

IID Generation Options

64 bits

Interface ID (IID)

Modified EUI-64 (uses MAC address)	"stable" IID for SLAAC
Stable, semantically opaque *[RFC7217]*	
Temporary Address Extensions *[RFC8981]*	"temporary" IID for SLAAC
DHCPv6	
Manually	
Others (CGA, HBA)	

SLAAC IIDs Currently

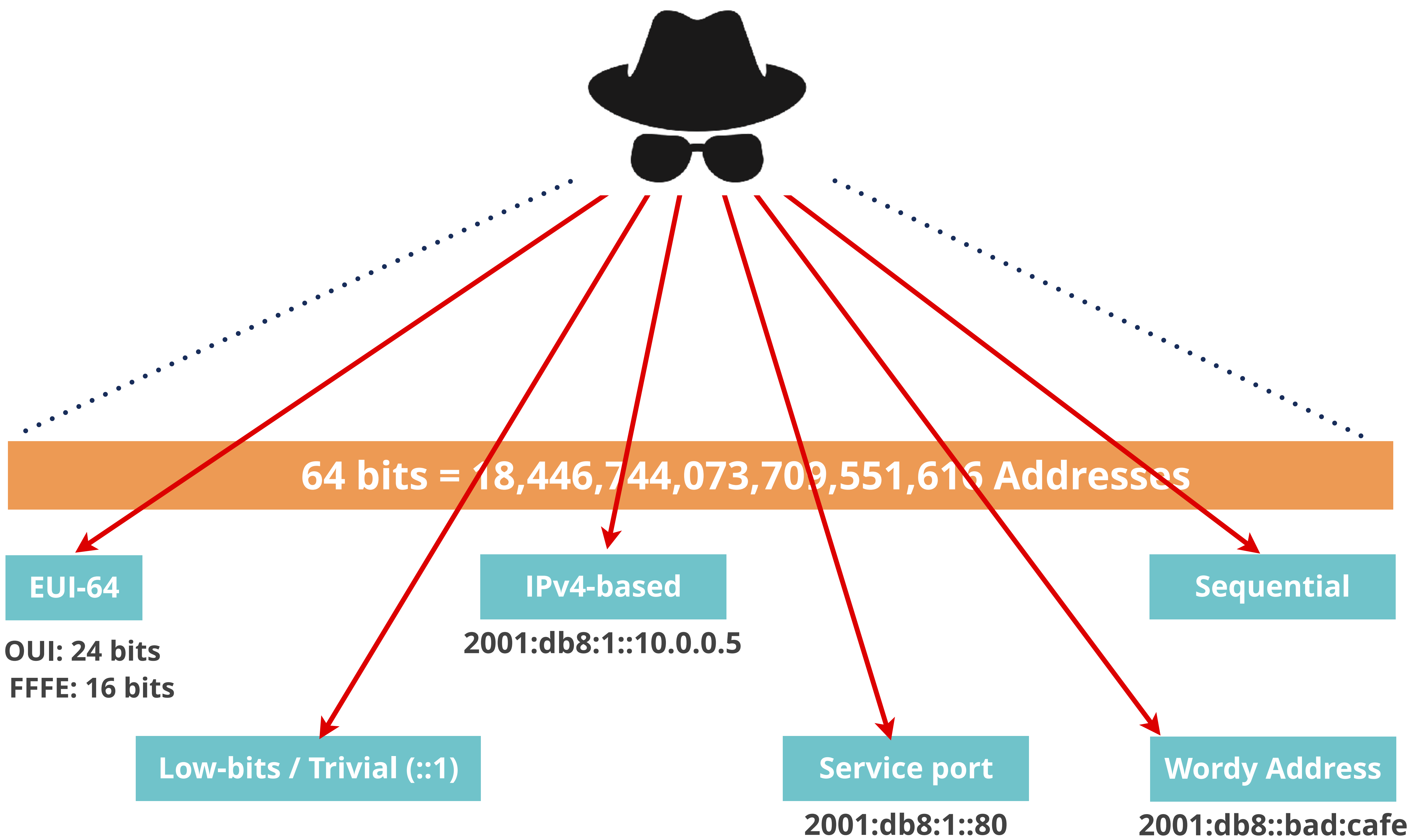
- Consider IID bits "**opaque**", no value or meaning *[RFC7136]*

How to generate IIDs *[RFC7217]*

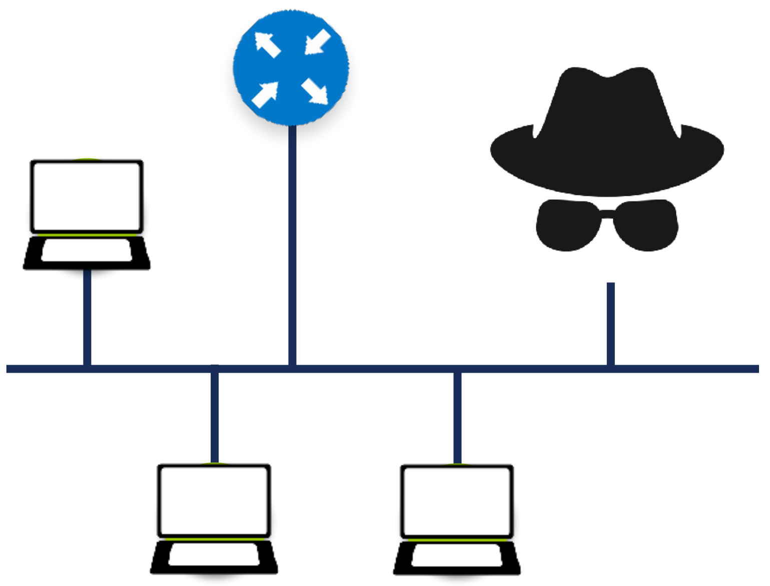
- Different for each interface in the same network prefix
- Not related to any fixed interface identifier
- Always the same when same interface connected to same network

- **Widely used** and **standardised** for "stable" addresses *[RFC8064]*

Guessing IIDs



Locally Scanning IPv6 Networks



- Traffic Snooping
- Dual-stack
- Routing Protocols
- Local Protocols
  - LLMNR [RFC4795]
  - Multicast DNS (mDNS) [RFC6762]
  - DNS Service Discovery (DNS-SD) [RFC6763]
- Local Scanning

Special / Reserved IPv6 Addresses

Name	IPv6 Address	Comments
Unspecified	::/128	When no address available
Loopback	::1/128	For local communications
IPv4-mapped	::ffff:0:0/96	For dual-stack sockets. Add IPv4 address 32 bits
Documentation	2001:db8::/32	RFC 3849
IPv4/IPv6 Translators	64:ff9b::/96	RFC 6052
Discard-Only Address Block	100::/64	RFC 6666
Teredo	2001::/32	IPv6 in IPv4 Encapsulation Transition Mechanism
6to4	2002::/16	IPv6 in IPv4 Encapsulation Transition Mechanism
ORCHID	2001:10::/28	Deprecated RFC 5156
Benchmarking	2001:2::/48	RFC 5180
Link-local	fe80::/10	RFC 4291
Unique-local	fc00::/7	RFC 4193
6Bone	3ffe::/16, 5f00::/8	Deprecated RFC 3701
IPv4-compatible	::/96	Deprecated RFC 5156

http://www.iana.org/assignments/iana-ipv6-special-registry/

Security Tips

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

IPv6 Network Scanning

Exercise 2.2

Exercise 2.2: IPv6 Network Scanning

- **Description**: Use available toolsets to scan a subnet
- **Goals**:
  - Know about two new toolsets: THC-IPV6 and The IPv6 Toolkit
  - Learn how to use them to scan a subnet
- **Time**: 10 minutes
- **Tasks**:
  - Use The IPv6 Toolkit to scan your lab's subnet
  - Use THC-IPV6 to scan your lab's subnet

IPv6 Associated Protocols Security

Section 3

ICMPv6

Section 3.1

ICMPv6 [*RFC4443*] is an integral part of IPv6

Error Messages

- Destination Unreachable
- Packet Too Big
- Time Exceeded
- Parameter Problem

Informational Messages

- Echo Request
- Echo Reply
- NDP
- MLD

ICMPv6 Format

- General Format

8 bits	8 bits	16 bits
Type	**Code**	**Checksum**
Message Body		

- Extended Format [*RFC4884*]

Used by:

- **Destination Unreachable**
- **Time Exceeded**

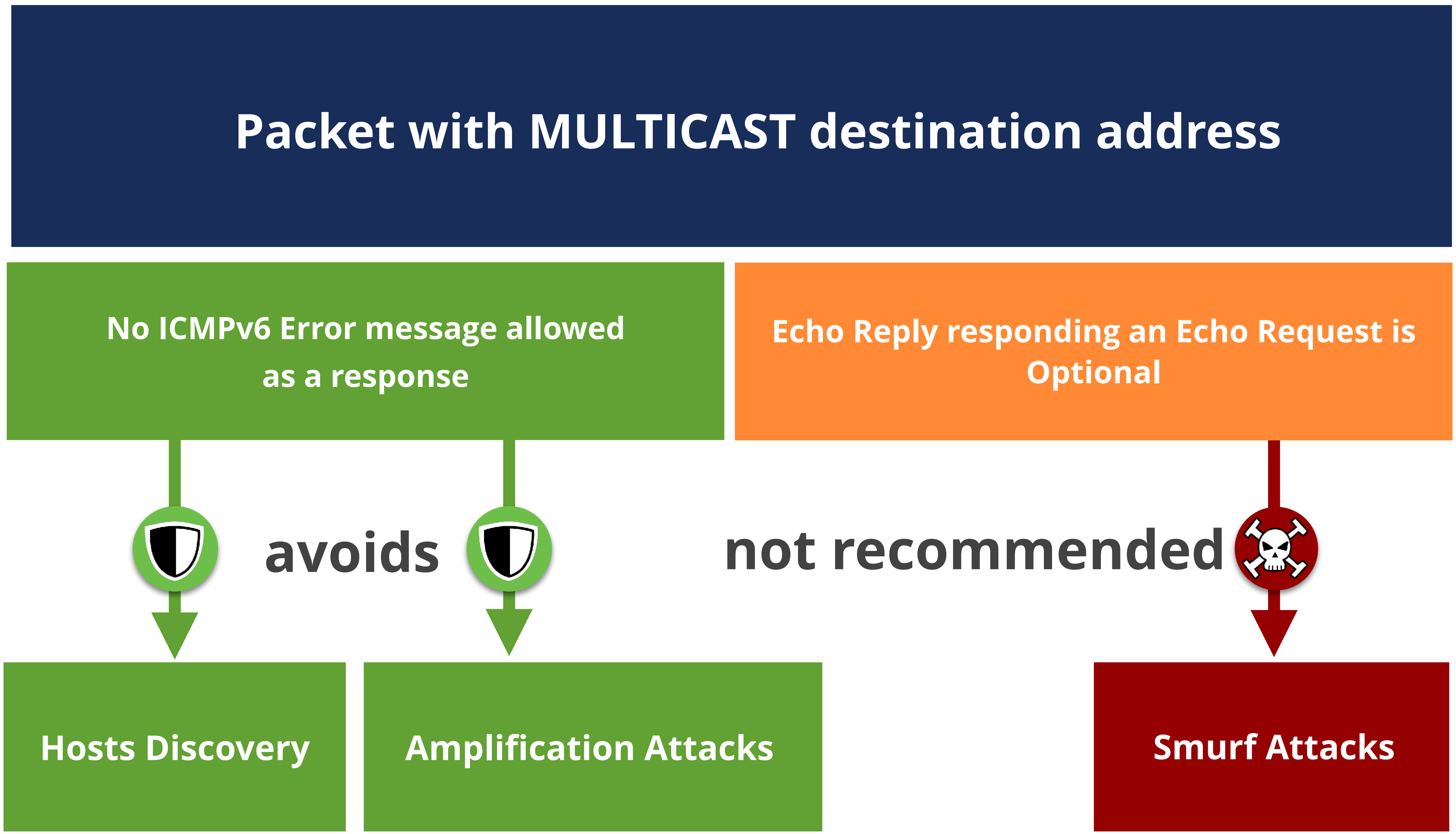
ICMPv6 Error Messages

Type	Code
Destination Ureachable (1)	No route to destination (0)
	Communication with destination administratively prohibited (1)
	Beyond scope of source address (2)
	Address Unreachable (3)
	Port Unreachable (4)
	Source address failed ingress/egress policy (5)
	Reject route to destination (6)
	Error in Source Routing Header (7)
Packet Too Big (2) Parameter = next hop MTU	Packet Too Big (0)
Time Exceeded (3)	Hop Limit Exceeded in Transit (0)
	Fragment Reassembly Time Exceeded (1)
Parameter Problem (4) Parameter = offset to error	Erroneous Header Field Encountered (0)
	Unrecognized Next Header Type (1)
	Unrecognized IPv6 Option (2)
	IPv6 First Fragment has incomplete IPv6 Header Chain (3)

FILTER ICMPv6 CAREFULLY!

Used in many IPv6 related protocols

ICMPv6 Security



NDP

Section 3.2

NDP [*RFC4861*] is used on a link

Messages

- Neighbour Solicitation
- Neighbour Advertisement
- Router Solicitation
- Router Advertisement
- Redirect

Used for:

- Discovery: routers, prefixes, network parameters
- Autoconfiguration
- DAD
- NUD
- Address Resolution

Hop Limit = 255

if not then **discard**

NDP has vulnerabilities

[RFC3756]

[RFC6583]

Specification says to use IPsec

impractical, it's not used

SEND [RFC3971]

(SEcure Neighbour Discovery)

Not widely available

NDP Threats

- **Neighbor Solicitation/Advertisement Spoofing**

- Can be done sending:

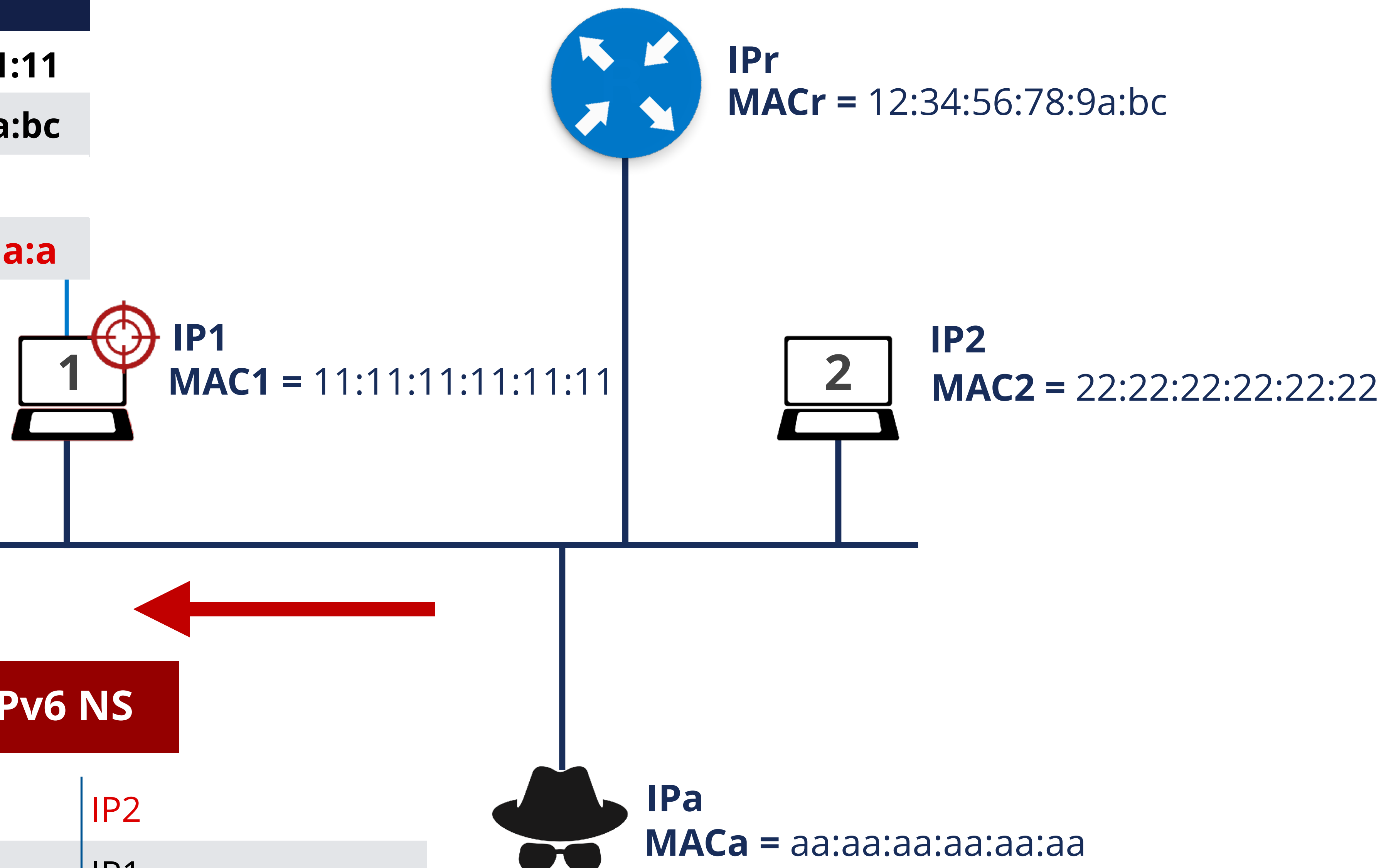
  1. **NS** with "source link-layer" option changed
  2. **NA** with "target link-layer" option changed

     - Can send unsolicited **NA** or as an answer to **NS**

- Redirection/DoS attack
- Could be used for a "**Man-In-The-Middle**" attack ?

NS Spoofing (Redirection / DoS)

Neighbour Cache	
IP1	**11:11:11:11:11:11**
IPr	**12:34:56:78:9a:bc**
IP2	**aa:aa:aa:aa:aa:a**

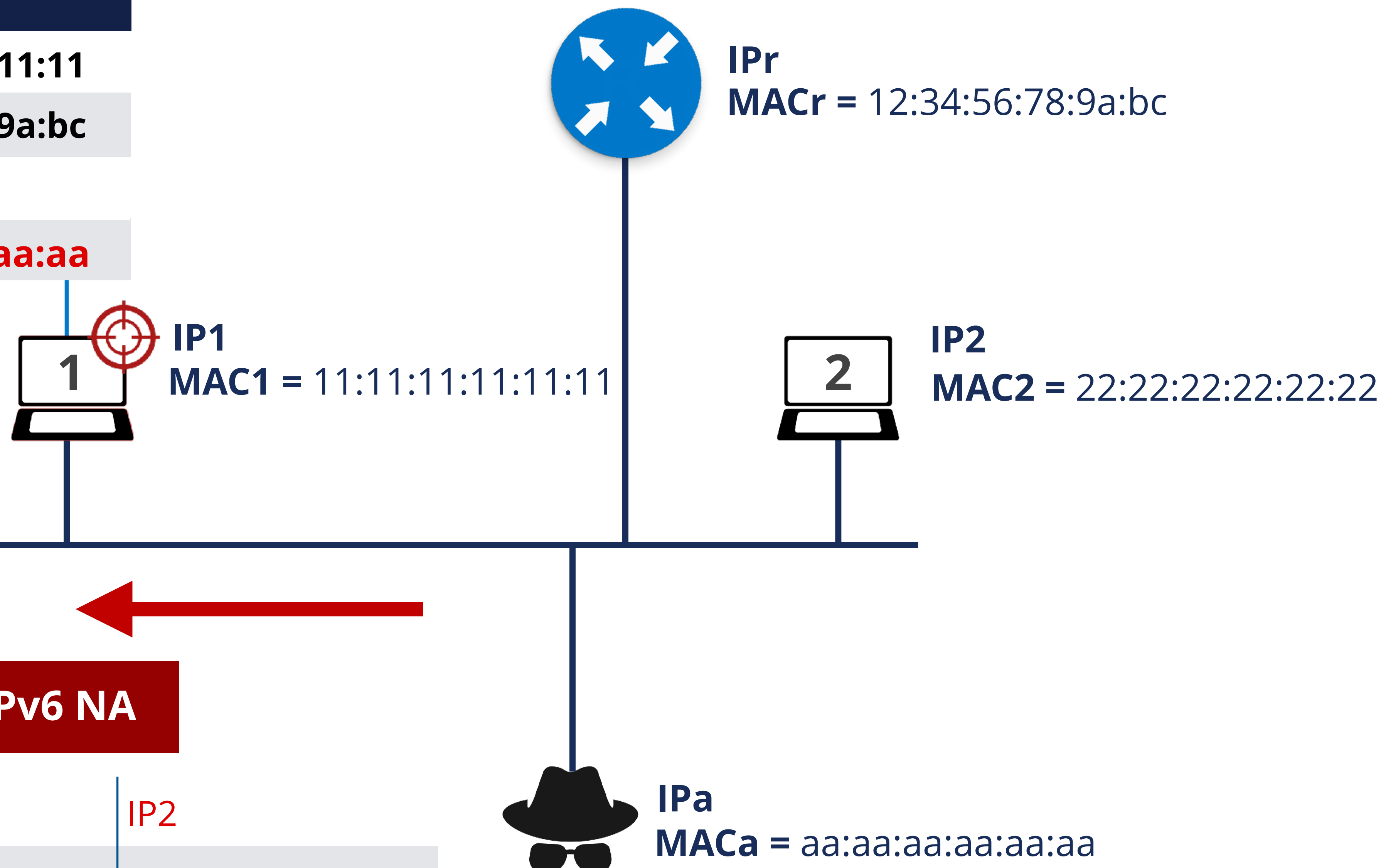


IPv6 | **ICMPv6 NS**

IPv6.Source IPv6	IP2
IPv6.Destination IPv6	IP1
NS.Target Addr	IP1
NS.Src Link-layer Addr	aa:aa:aa:aa:aa:aa

Unsolicited NA (Redirection / DoS)

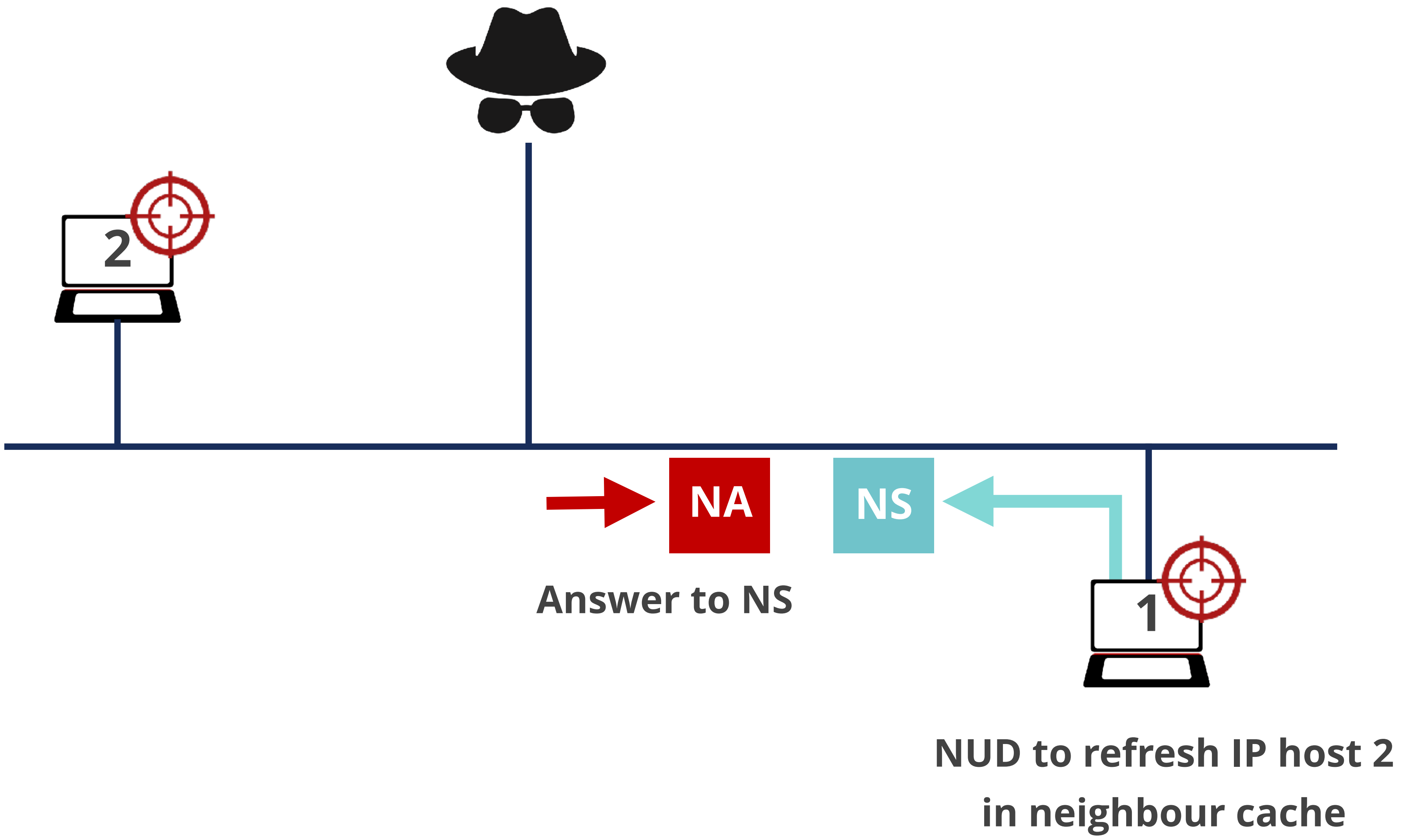
Neighbour Cache	
IP1	**11:11:11:11:11:11**
IPr	**12:34:56:78:9a:bc**
IP2	**aa:aa:aa:aa:aa:aa**



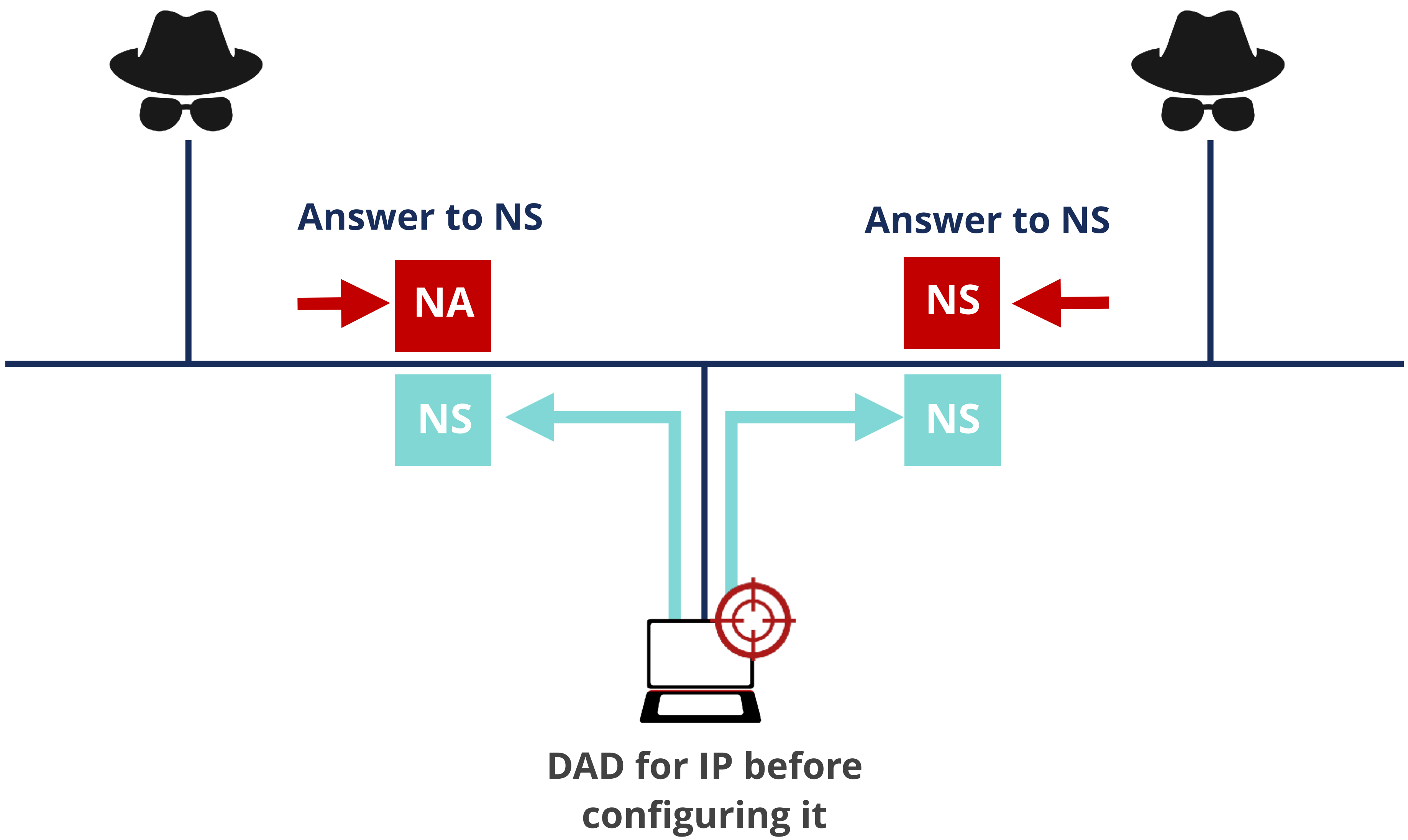
IPv6	ICMPv6 NA

NA.Target Addr	IP2
NA.Target Link-layer Addr	aa:aa:aa:aa:aa:aa

NUD Failure (DoS attack)



DAD (DoS Attack)



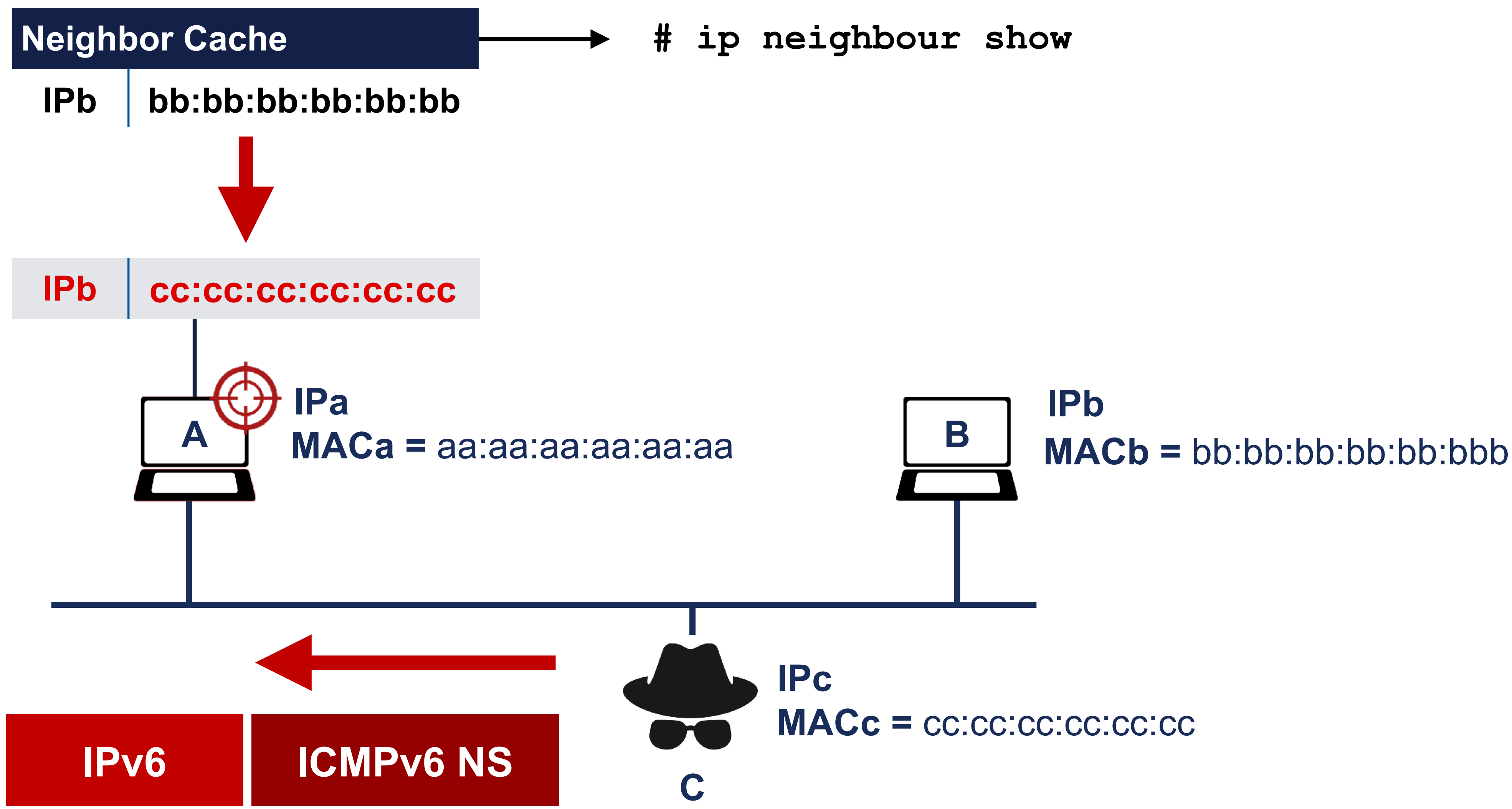
NDP

Exercise 3.2-a

Exercise 3.2-a NDP

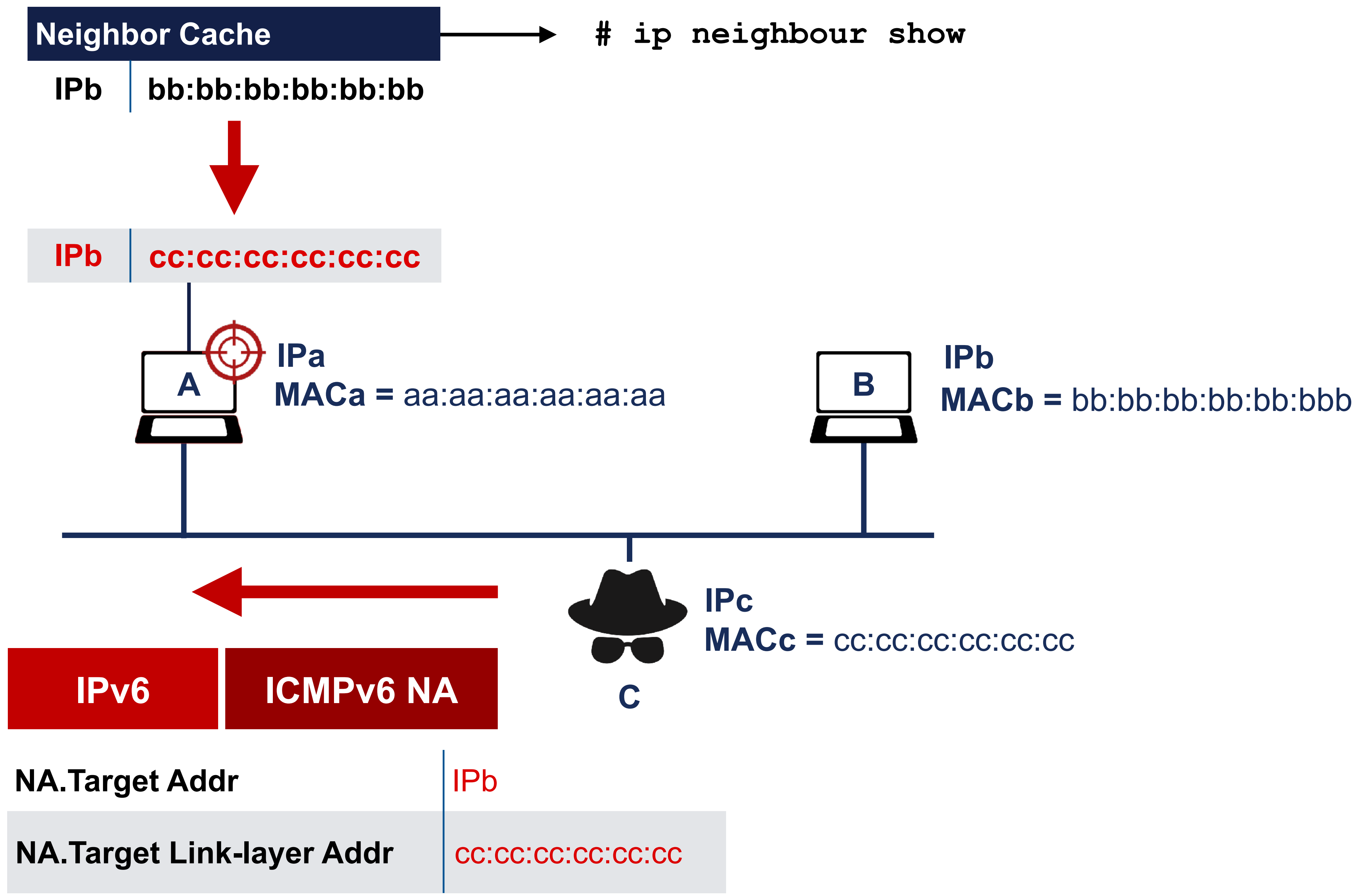
- **Description**: Create packets to poison neighbor cache
- **Goals**:
  - Practice with Scapy tool
  - Learn how to modify the neighbor cache of another host in the same network
- **Time**: 15 minutes
- **Tasks** (at least one of them):
  - Generate NS packets that change other host’s neighbor cache
  - Generate NA packets that change other host’s neighbor cache

3.2-a: Neighbor cache attack using NS

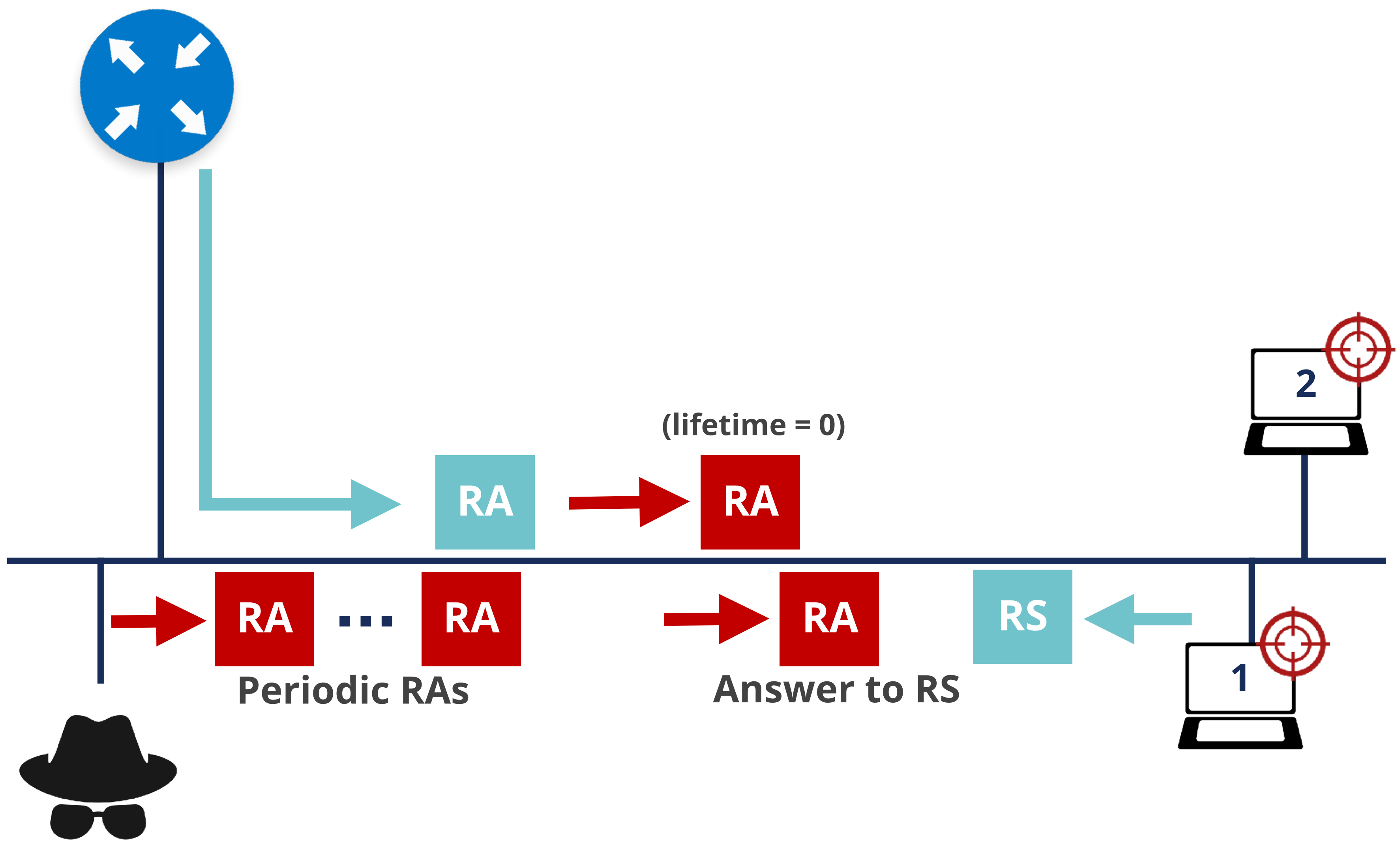


IPv6.Source IPv6	IPb
IPv6.Destination IPv6	IPa
NS.Target Addr	IPa
NS.Src Link-layer Addr	cc:cc:cc:cc:cc:cc

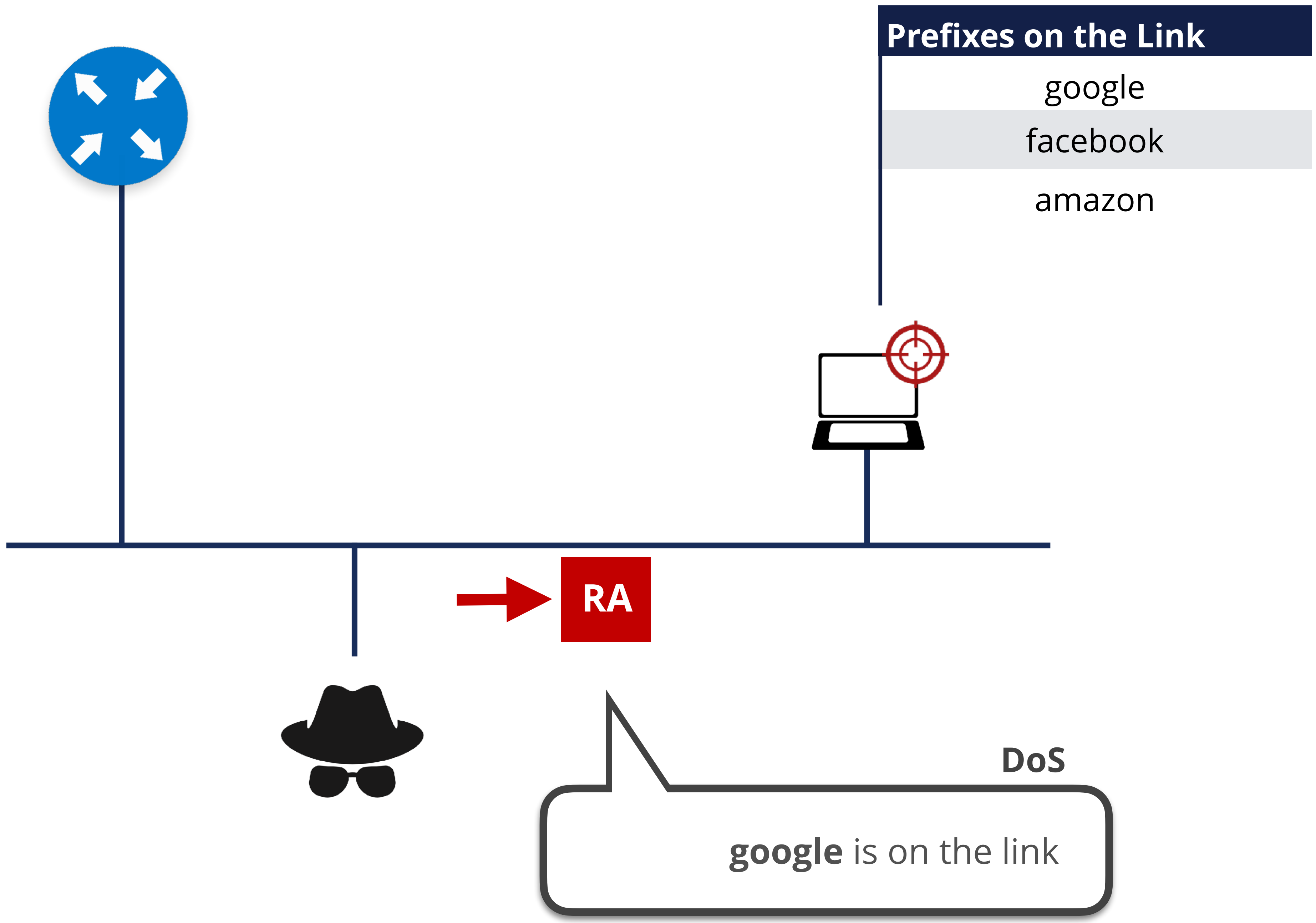
3.2-a: Neighbor cache attack using NA



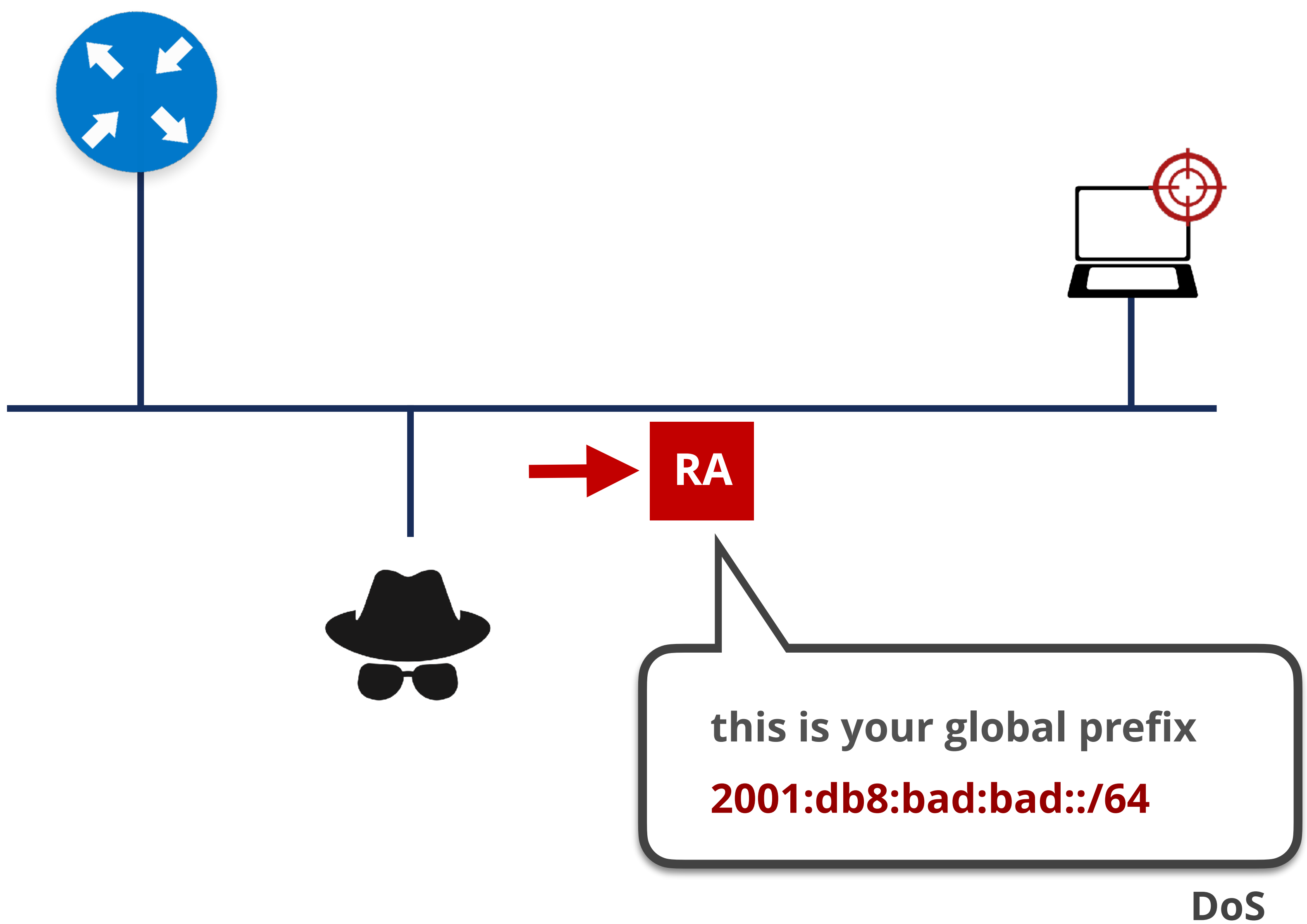
Malicious Last Hop Router



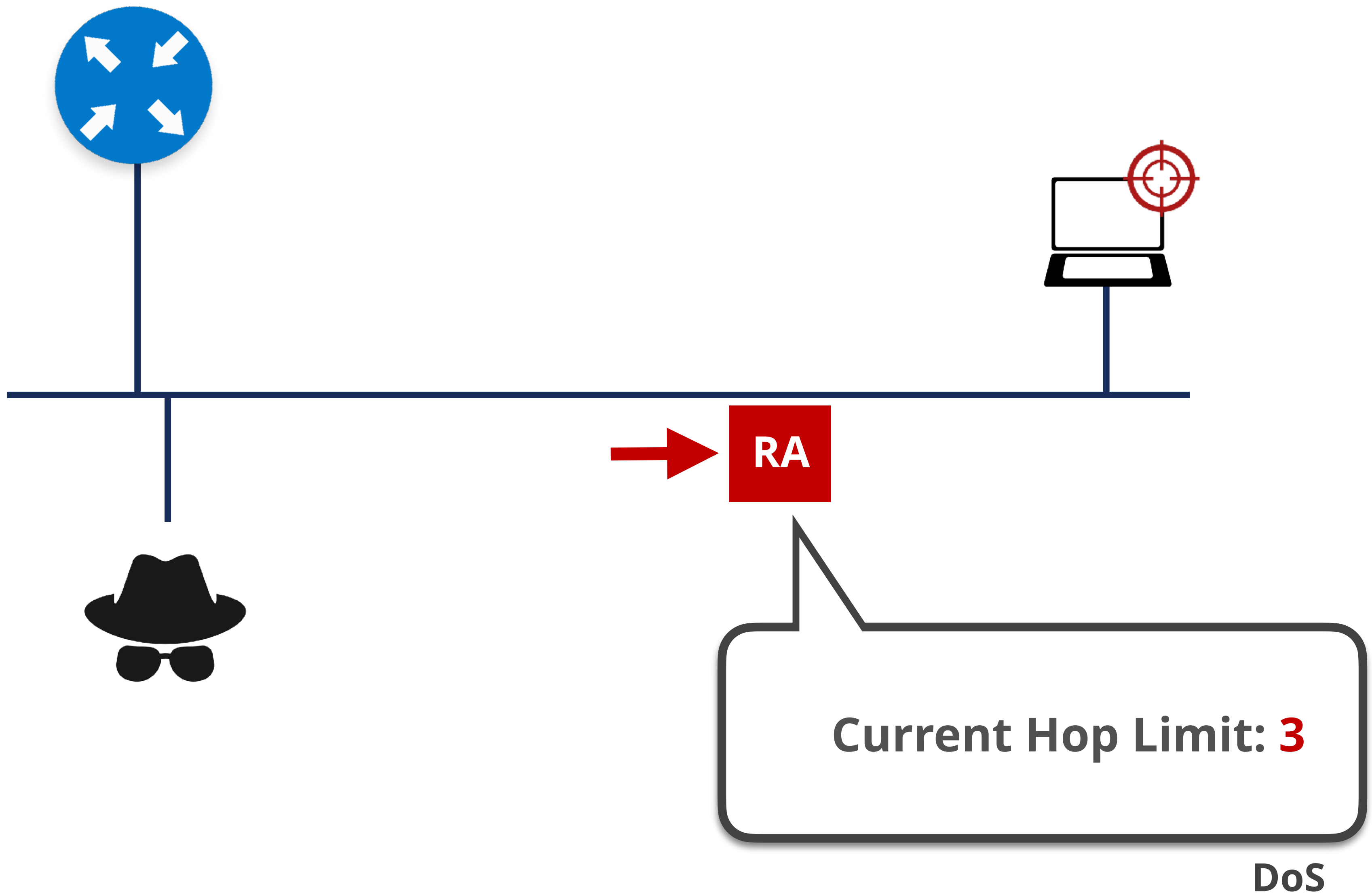
Bogus On-Link Prefix



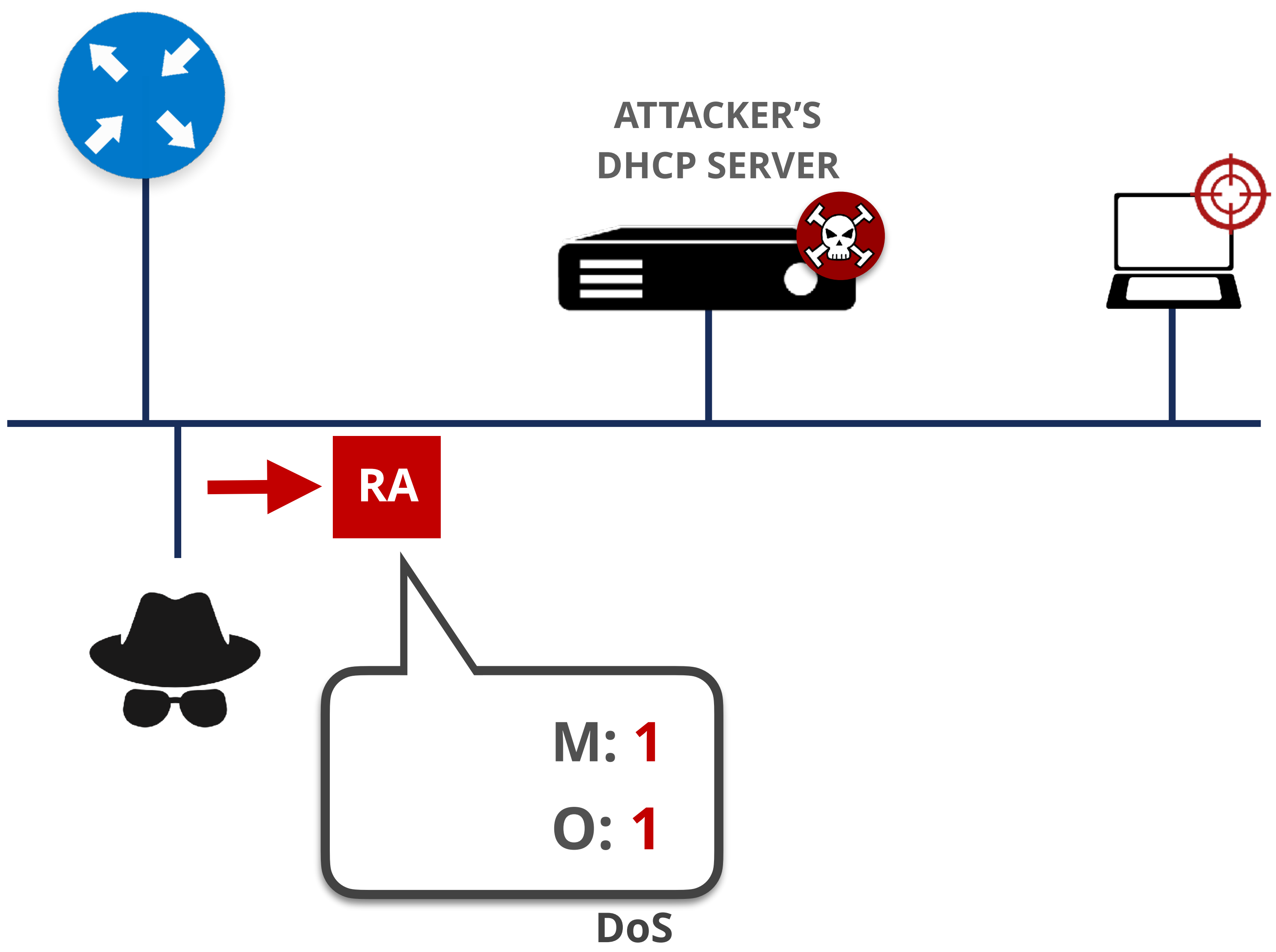
Bogus Address Configuration Prefix



Parameter Spoofing: Hop Limit



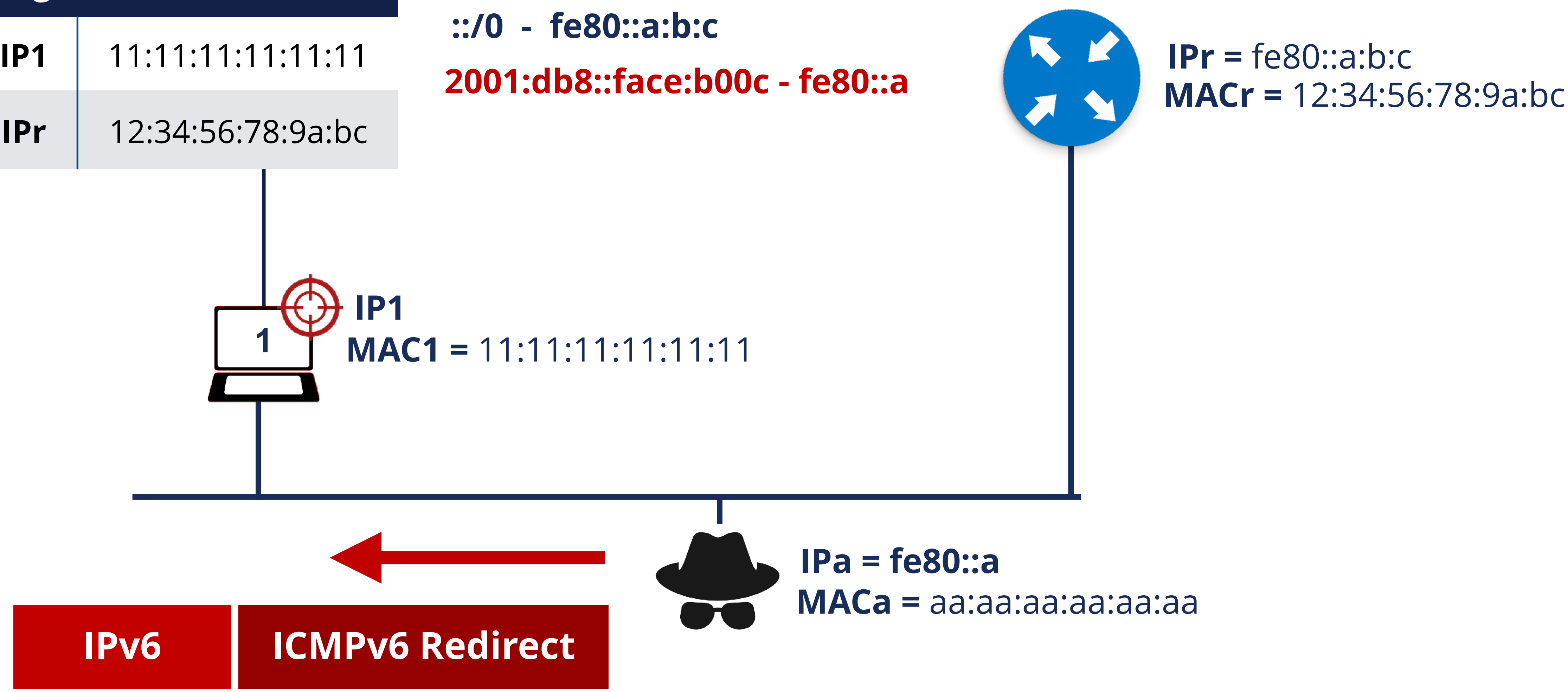
Parameter Spoofing: DHCPv6



Spoofed Redirect Message

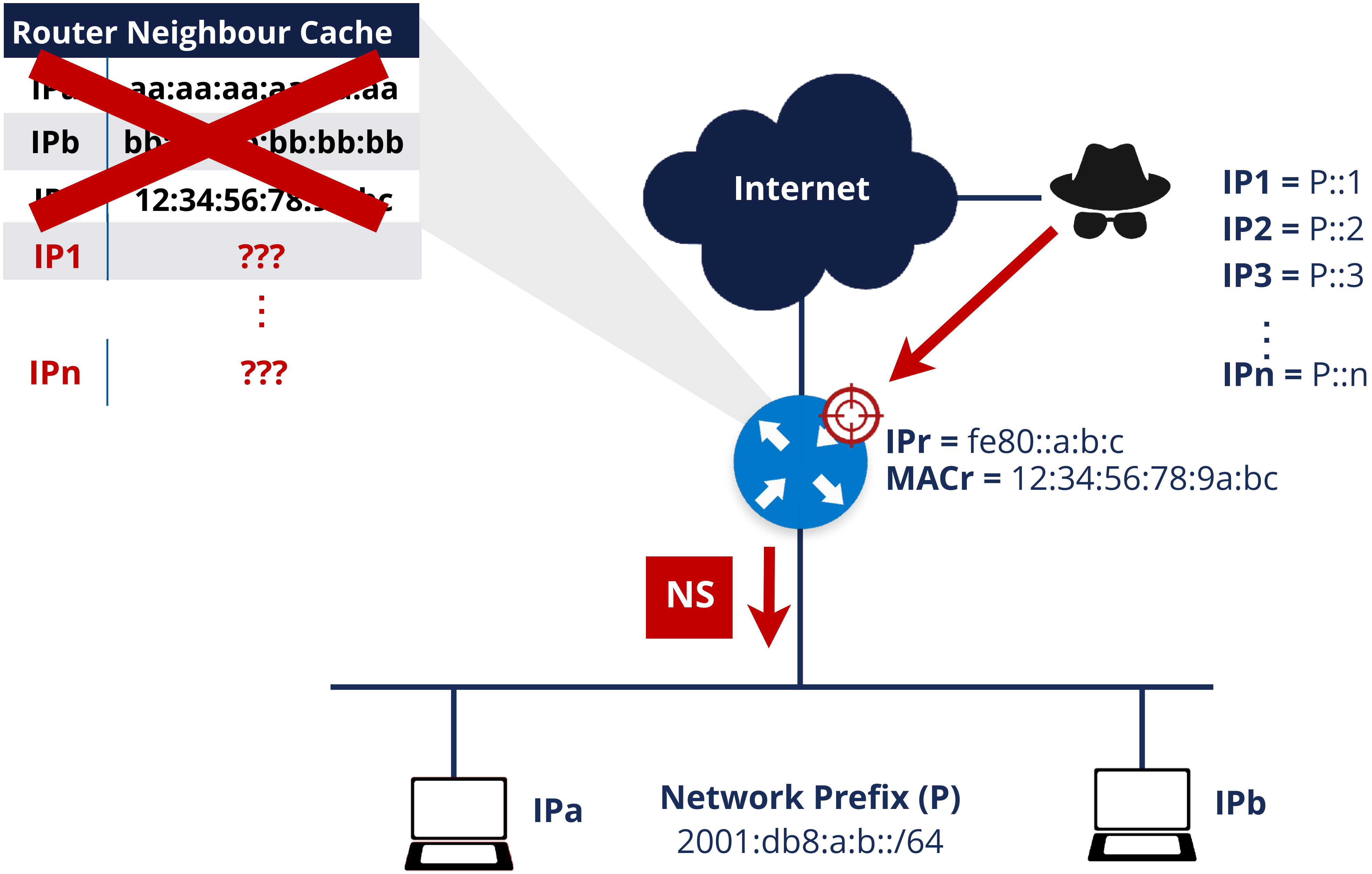
Neighbour Cache	
IP1	11:11:11:11:11:11
IPr	12:34:56:78:9a:bc

Routes on Host 1:
::/0 - fe80::a:b:c
2001:db8::face:b00c - fe80::a



IPv6.Source IPv6	IPr = fe80::a:b:c
IPv6.Destination IPv6	IP1
Redirect.Target Addr	IPa = fe80::a
Redirect.Dst Addr.	2001:db8::face:b00c

Neighbour Discovery DoS Attack



NDP

Exercise 3.2-b

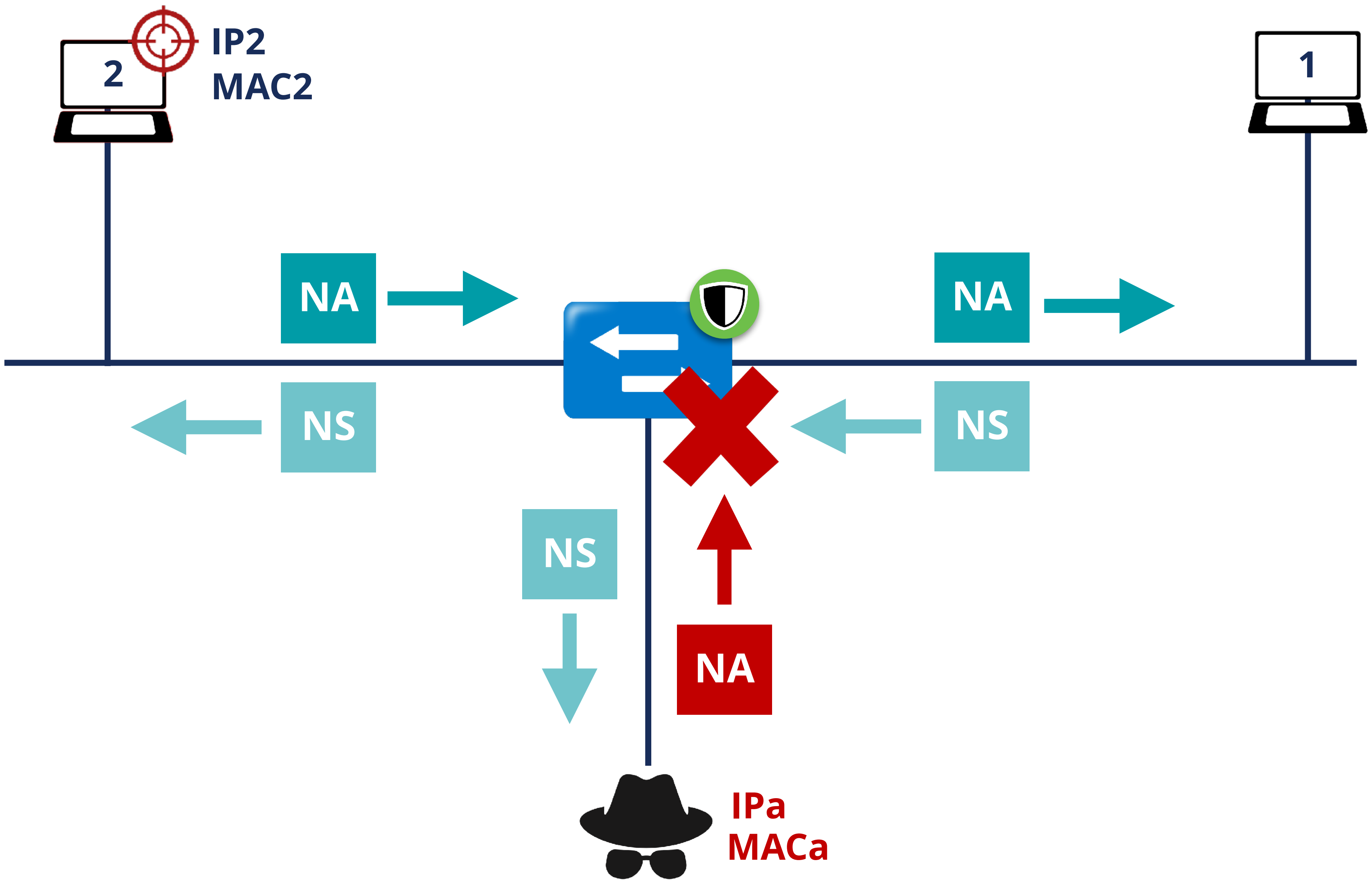
Exercise 3.2-b NDP

- **Description**: Send RA messages to perform attacks
- **Goals**:
  - Practice with Scapy tool
  - Use RA messages to perform attacks on a link
- **Time:** 20 minutes
- **Tasks**:
  - Send RA messages with bogus address configuration prefix

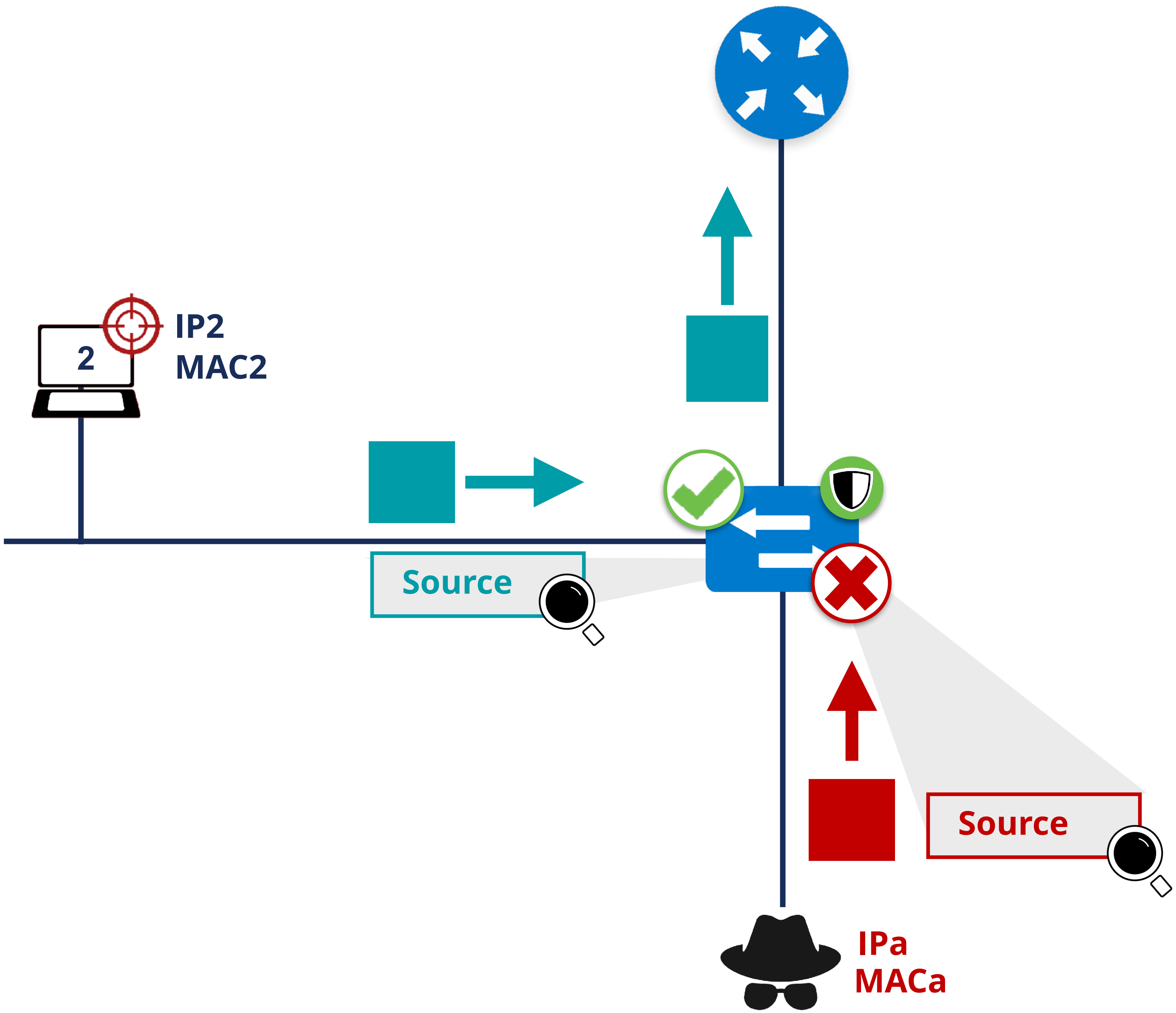
First Hop Security

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

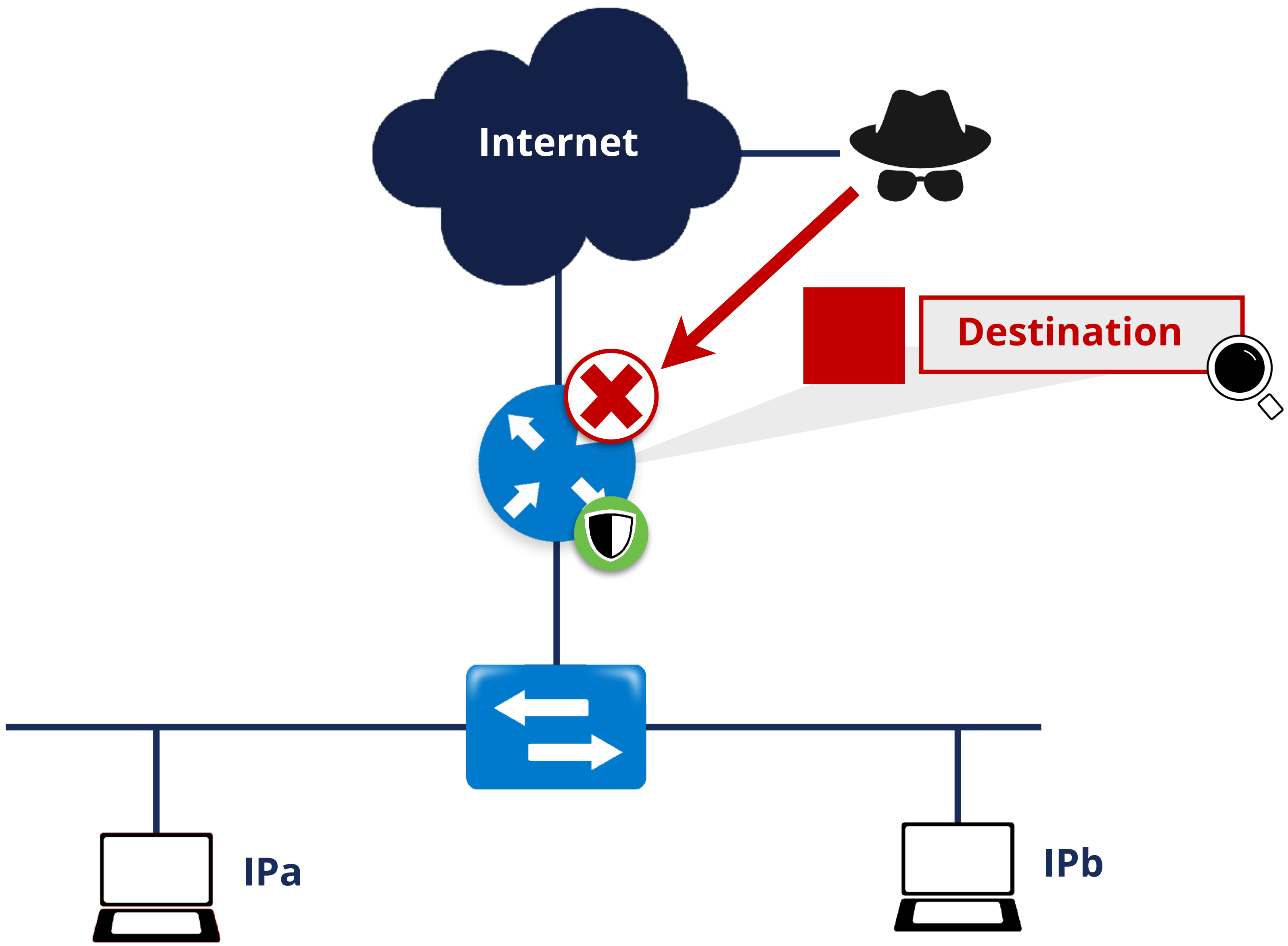
IPv6 Snooping



IPv6 Source / Prefix Guard



IPv6 Destination Guard



Rogue Router Advertisements

RA

Rogue RA Solutions

1 **Link Monitoring**

2 **SEND**

3 **MANUAL CONFIGURATION**
+ Disable Autoconfig

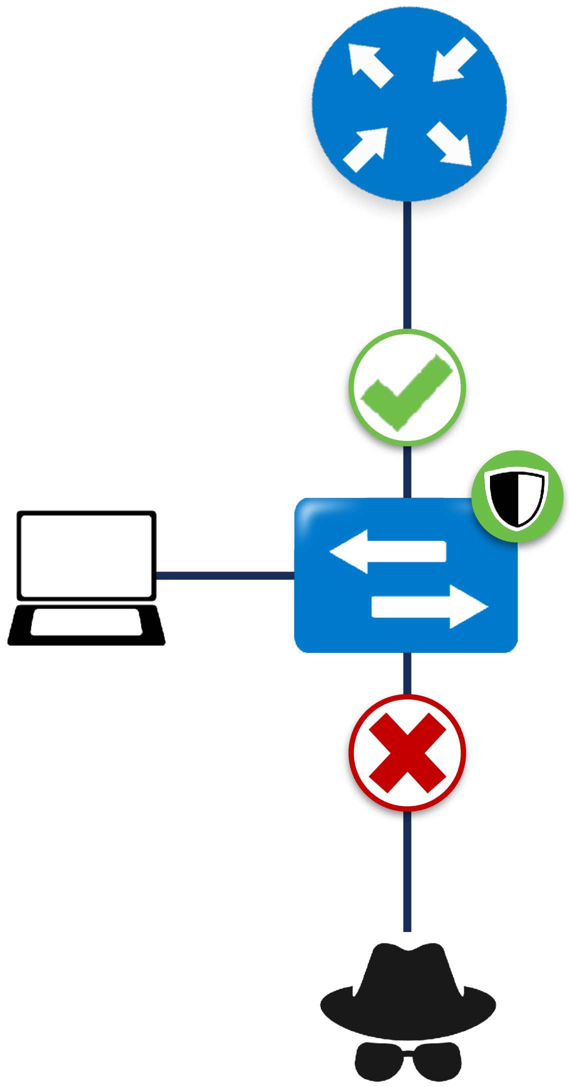
4 **Host Packet Filtering**

5 **Router Preference Option**
[*RFC4191*]

6 **ACLs on Switches**

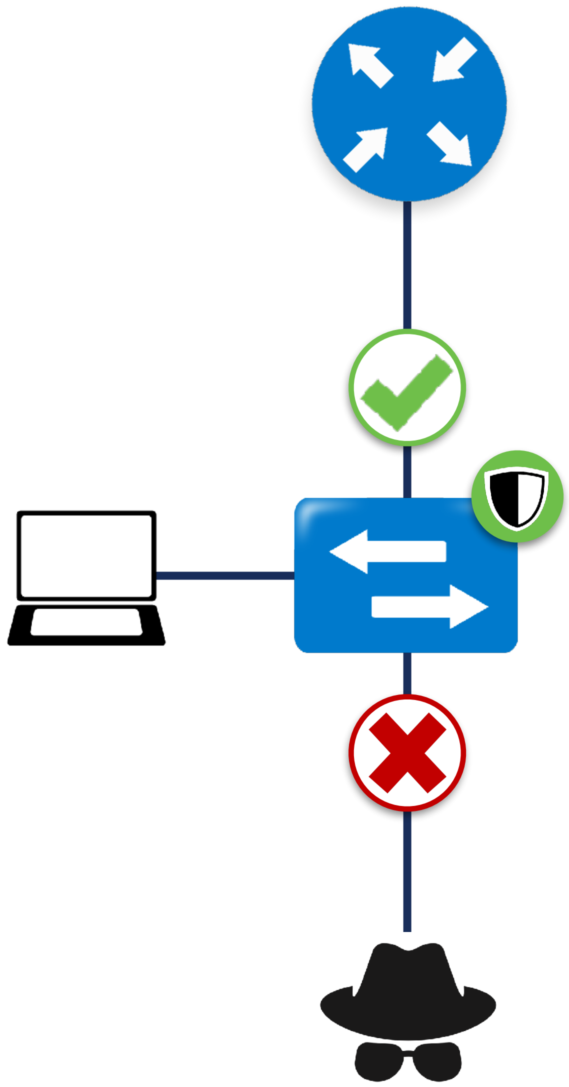
7 **RA Snooping on Switches** (RA GUARD)

RA-GUARD [*RFC6105*]



- Easiest available solution
- Only allows RAs on legitimate ports on L2 switches

Implementing RA-GUARD



Stateless RA Guard

Decision based on RA message or static configuration

Stateful RA Guard

Learns dynamically

Filtering

- Use Access Control Lists (ACLs) in switches

Switches need to understand

Ethernet	IPv6	ICMPv6
Ethertype 0x86DD for IPv6	Version 6	ICMPv6 Type and Code
Source/destination MAC address	Source/destination IPv6 address	
	Next Header	

Filtering Example

```
(config)#ipv6 access-list RA-GUARD
(config-ipv6-acl)#sequence 3 deny icmp any any router-advertisement
(config-ipv6-acl)#sequence 6 permit ipv6 any any

(config-ipv6-acl)#exit

(config)#interface FastEthernet0/5
(config-if)#ipv6 traffic-filter RA-GUARD in
```

Conclusions / Tips

- NDP is an important, powerful and vulnerable protocol
- **Recommended**: use available solutions to protect NDP
- Detection (IDS/IPS) can be easier and recommended

MLD

Section 3.3

- MLD (**Multicast Listener Discovery**) 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

QUERY

Router asks for listeners

General

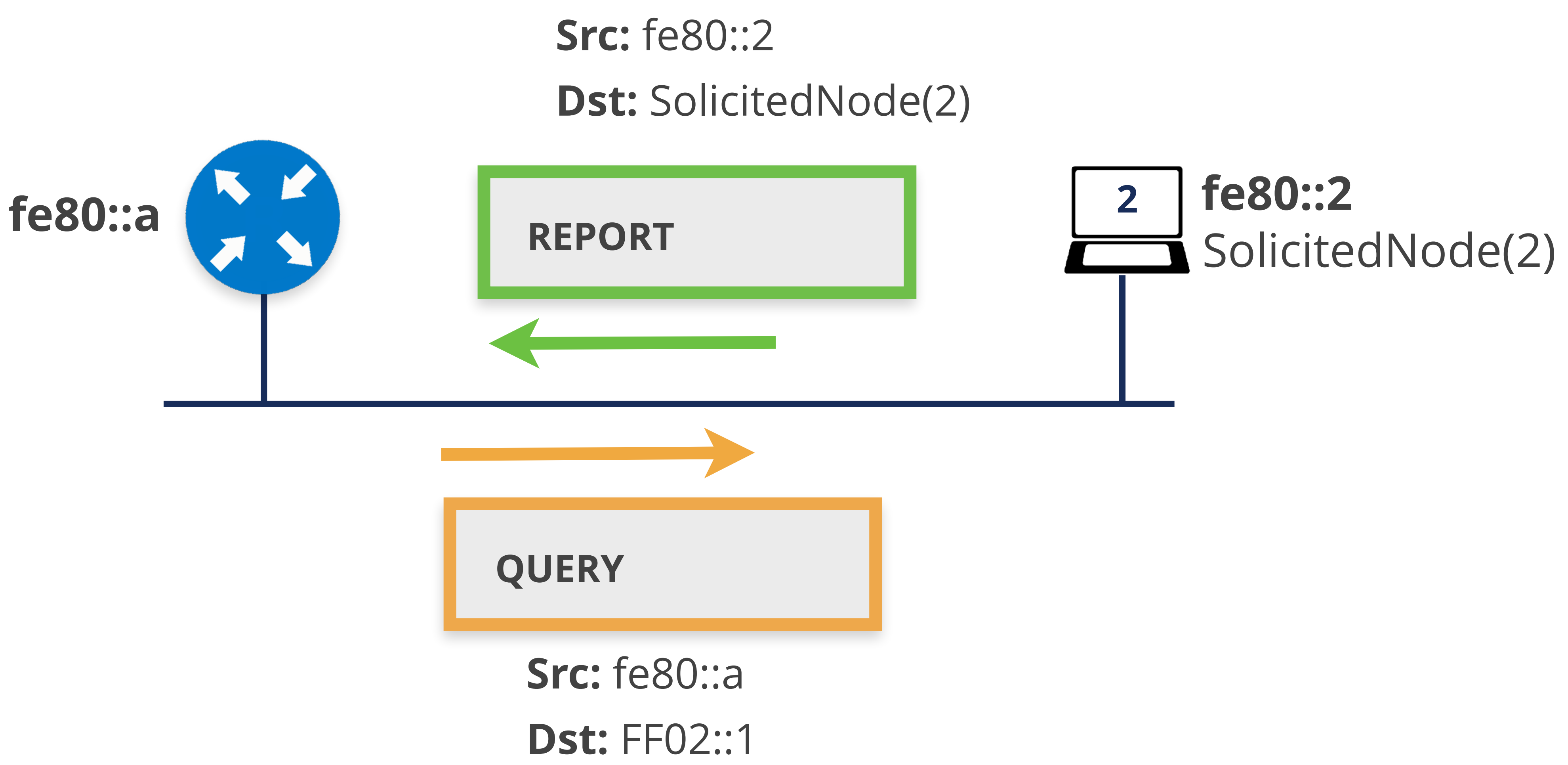
Specific

REPORT

Listeners report themselves

DONE

Listeners indicate that they're done


Src: fe80::2
Dst: SolicitedNode(2)
fe80::a
REPORT
2
fe80::2
SolicitedNode(2)
QUERY
Src: fe80::a
Dst: FF02::1

MLDv2

- Mandatory for all IPv6 nodes (**MUST**) [RFC8504]
- **Interoperable** with MLDv1
- Adds Source-Specific Multicast filters:
  - **Only accepted** sources
  - Or all sources accepted **except** specified ones

MLDv2

QUERY

Router asks for listeners

General

Specific Multicast Address

Specific Multicast Address and Source

REPORT-v2

Current state

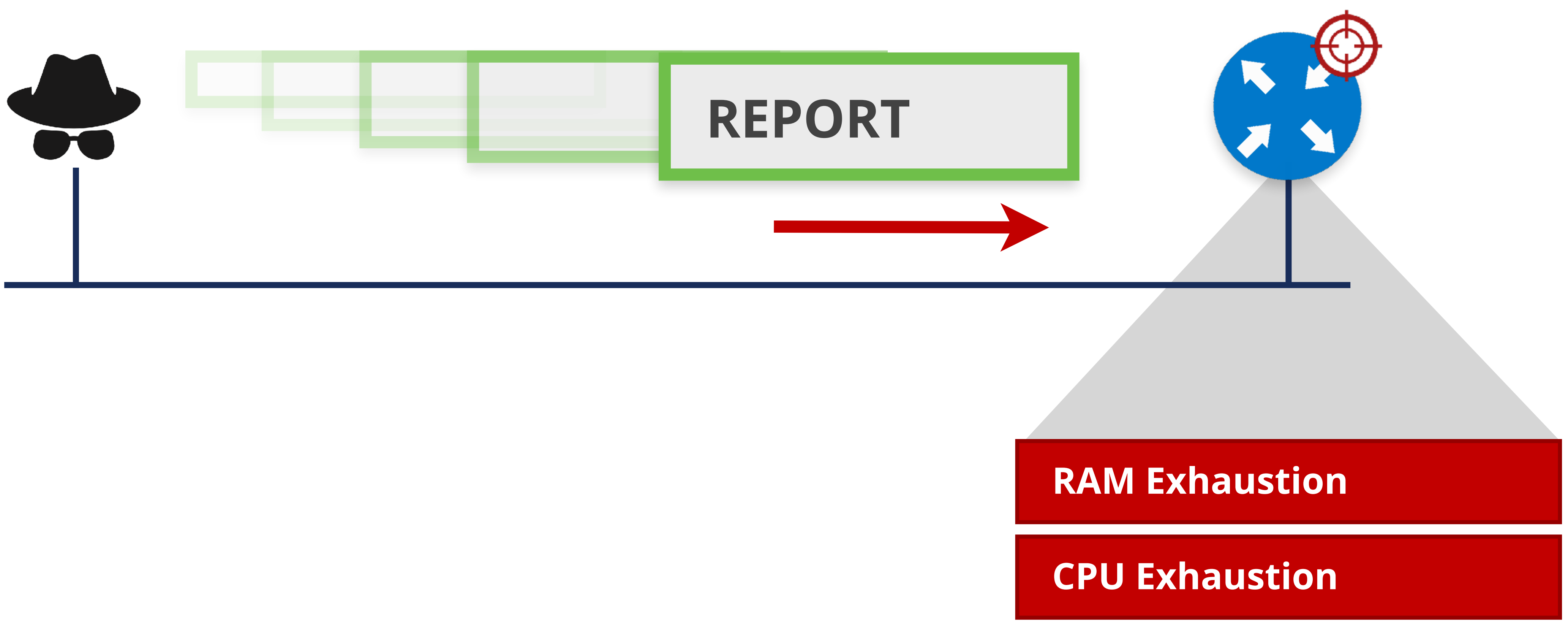
State change (filter/sources)

Sent to FF02::16

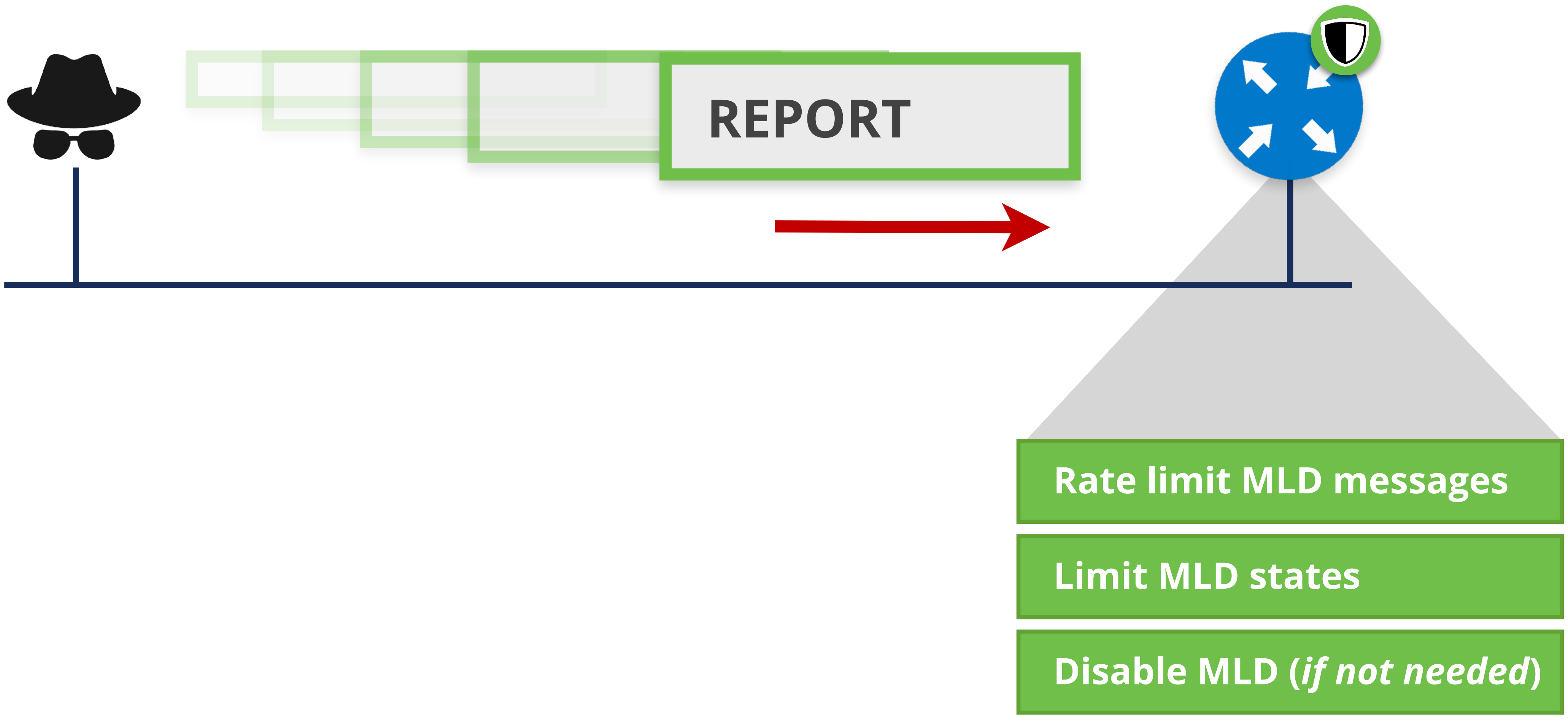
MLD Details

- Nodes **MUST** process QUERY to any of its unicast or multicast addresses
- MLDv2 **needs all nodes** using MLDv2
- **All OSs join** (REPORT) to the Solicited Node addresses

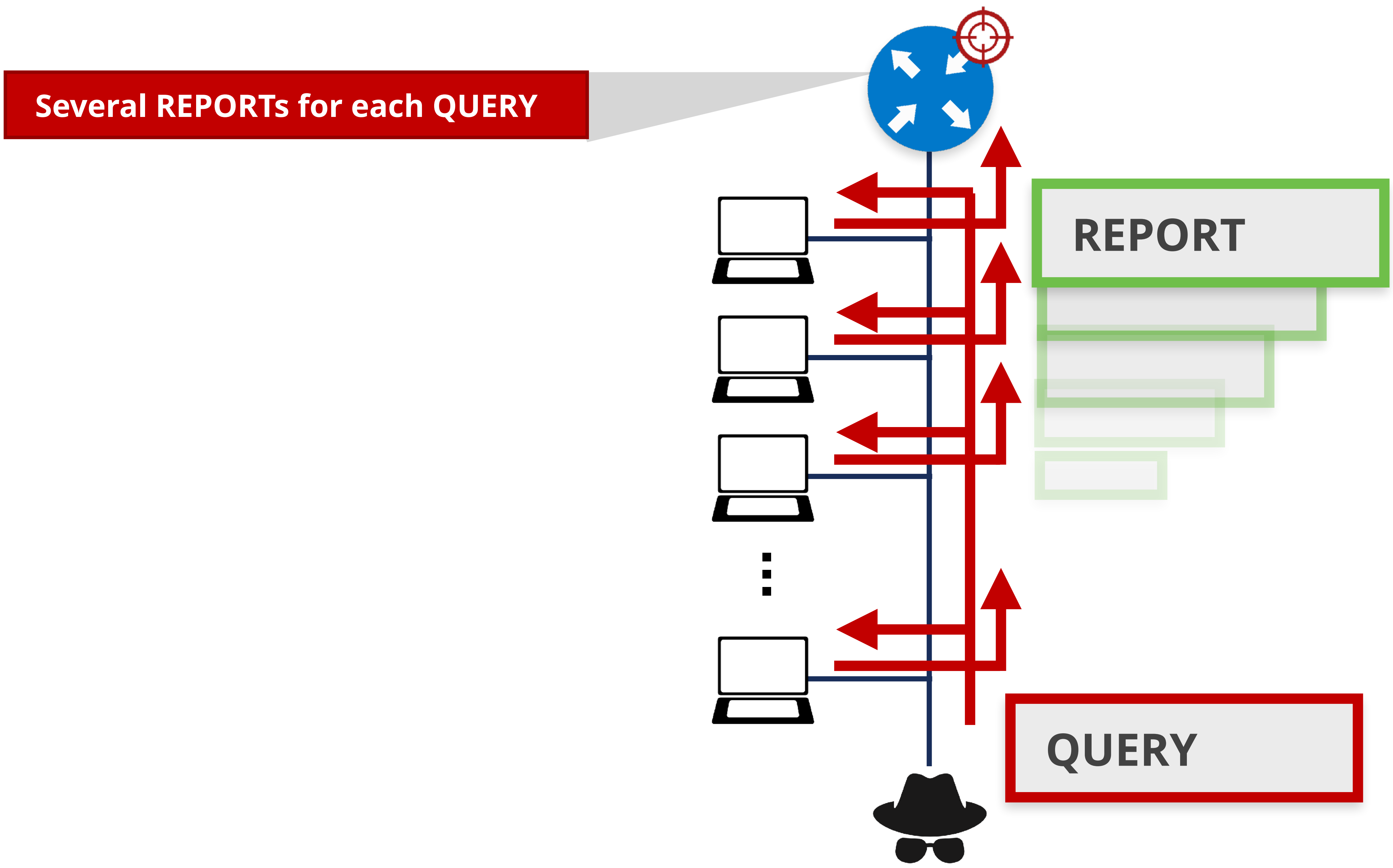
MLD Flooding



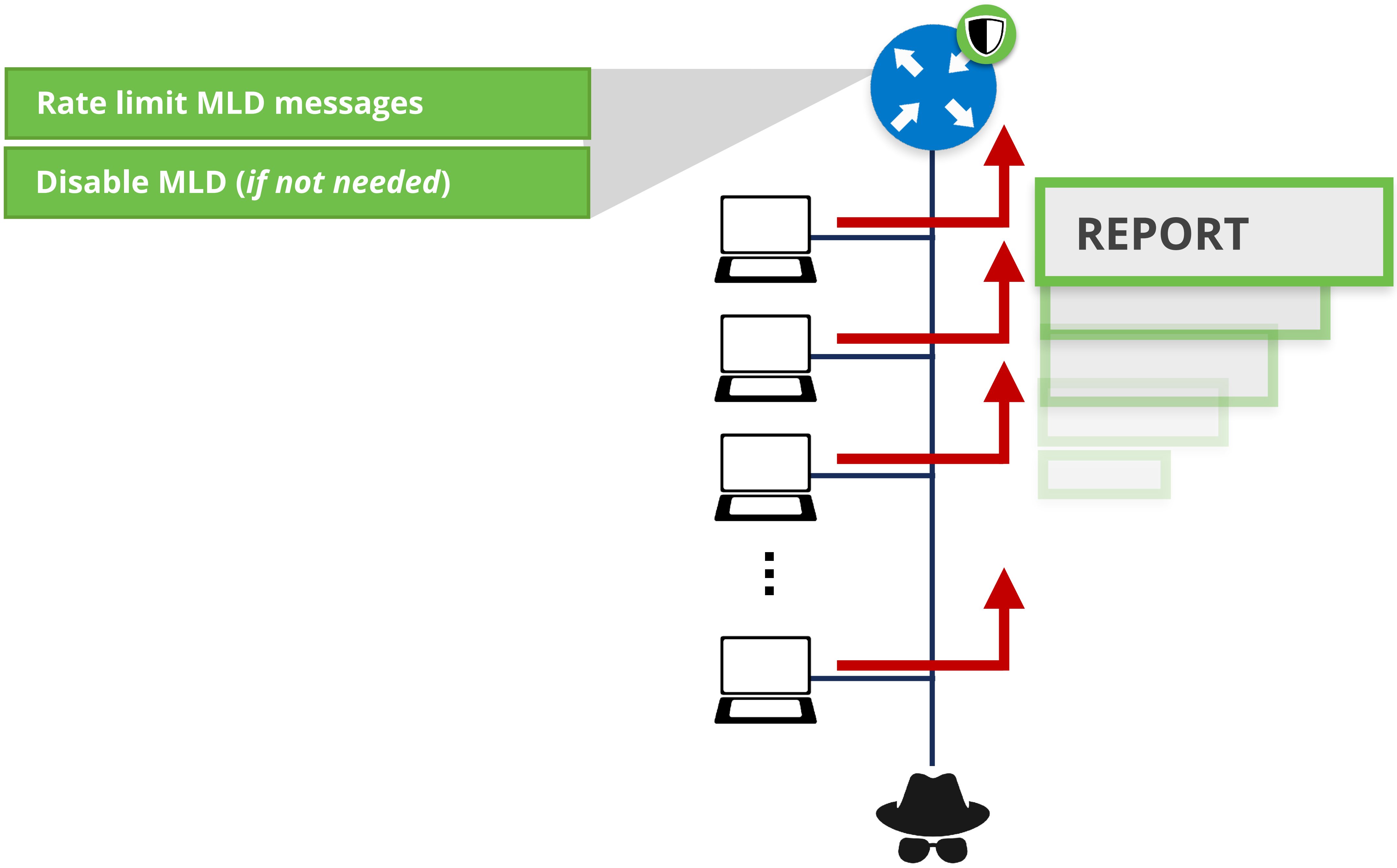
MLD Flooding



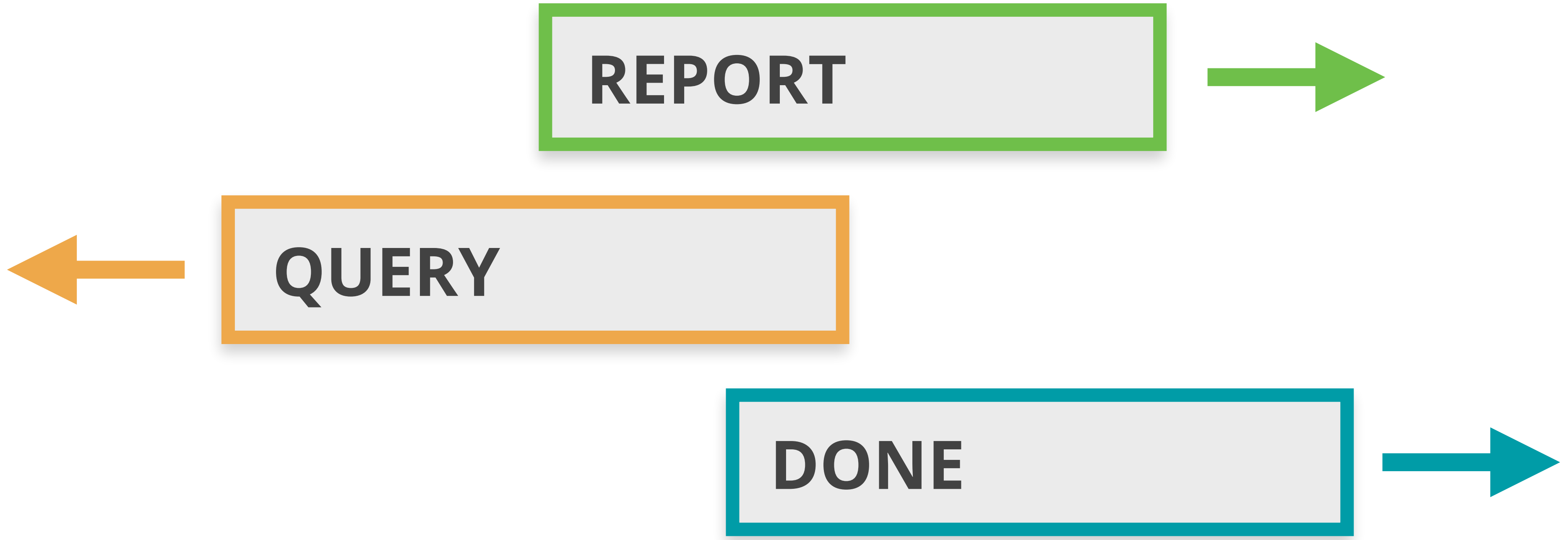
MLD Traffic amplification



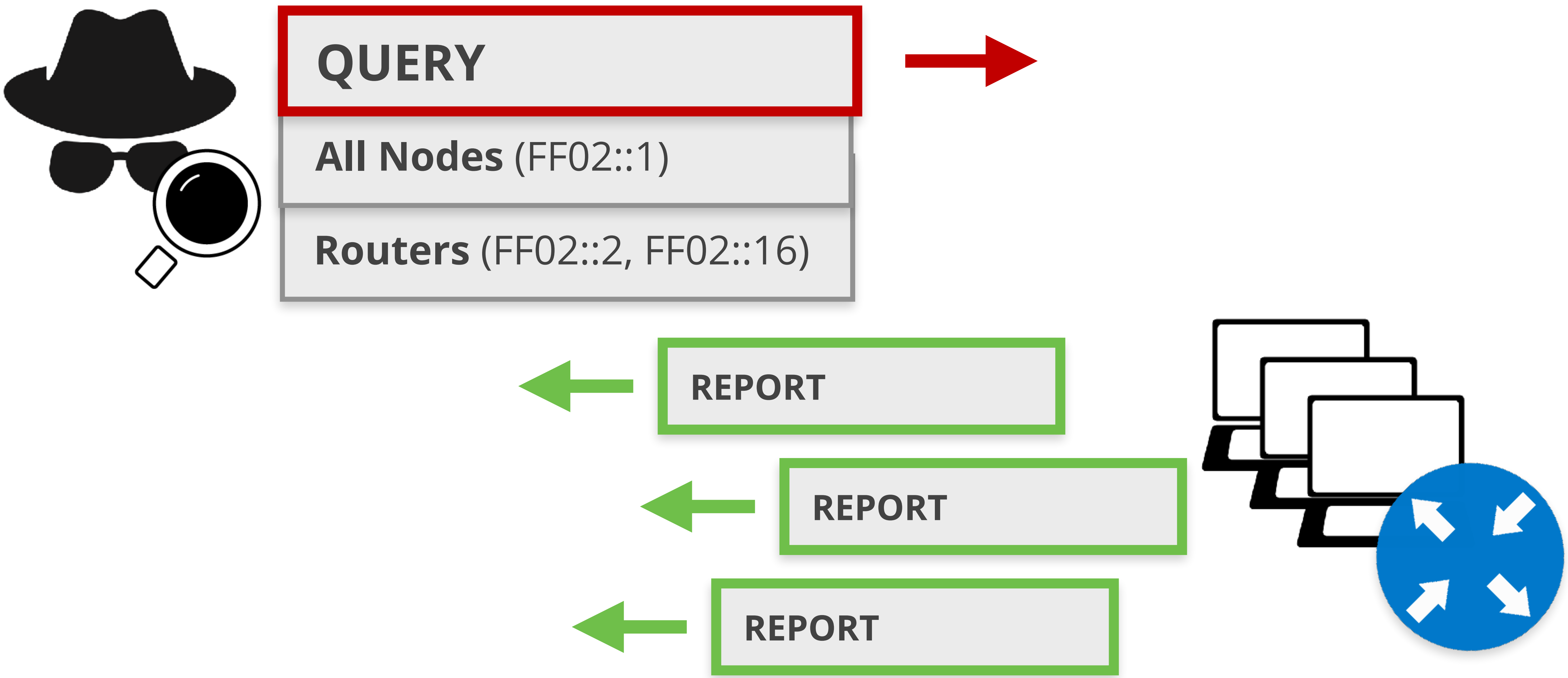
MLD Traffic amplification



Passive MLD Scanning



Active MLD Scanning



Built-in MLD Security

MLD Message

Source: Link local address **only**

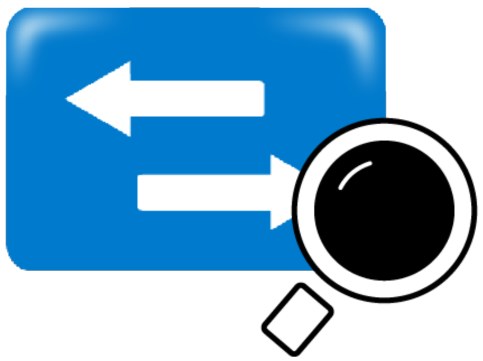
Hop Limit = 1

Router Alert option in Hop-by-Hop EH

Discard non-compliant messages

MLD Snooping

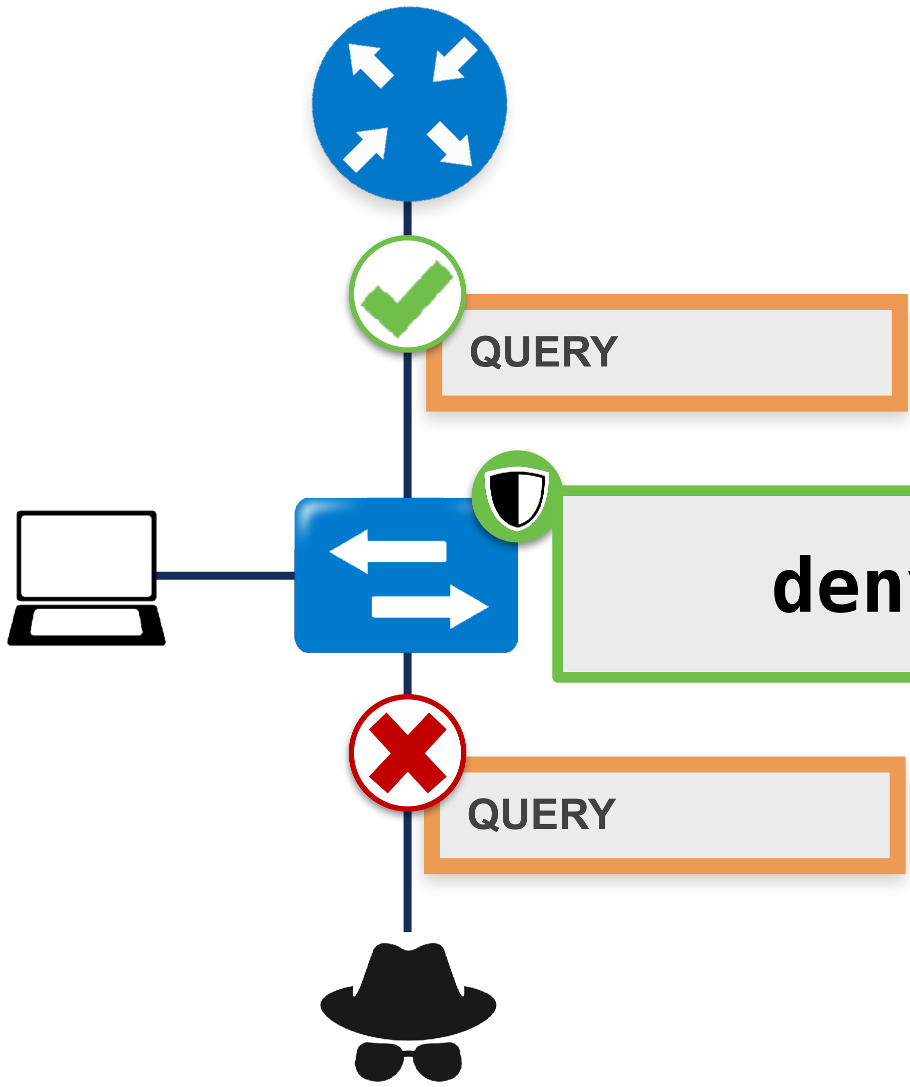
RFC4541



QUERY

Only allow multicast traffic **on ports with listeners**

MLD Protection on Switches



Only allow **QUERIES** on router's port

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

MLD

Exercise 3.3

Exercise 3.3 MLD

- **Description**: Network scanning using MLD
- **Goals**:
  - Know about a new tool: Chiron
  - Learn how to use Chiron to scan a network using MLD
- **Time:** 10 minutes
- **Tasks**:
  - Scan your network using MLD Query message

DNS

Section 3.4

IPv6 DNS Configuration Attacks

Attacker becomes the DNS server of the victim using:

NDP	Autoconfiguration
Man-in-the-Middle	SLAAC
Neighbor Cache Poisoning	DHCPv6

IPv6 DNS Configuration Attacks

Depending on answers to DNS queries

Man-in-the-Middle

DoS Attack

DHCPv6

Section 3.5

Introduction

Similar to IPv4
Client / Server
UDP
Uses Relays

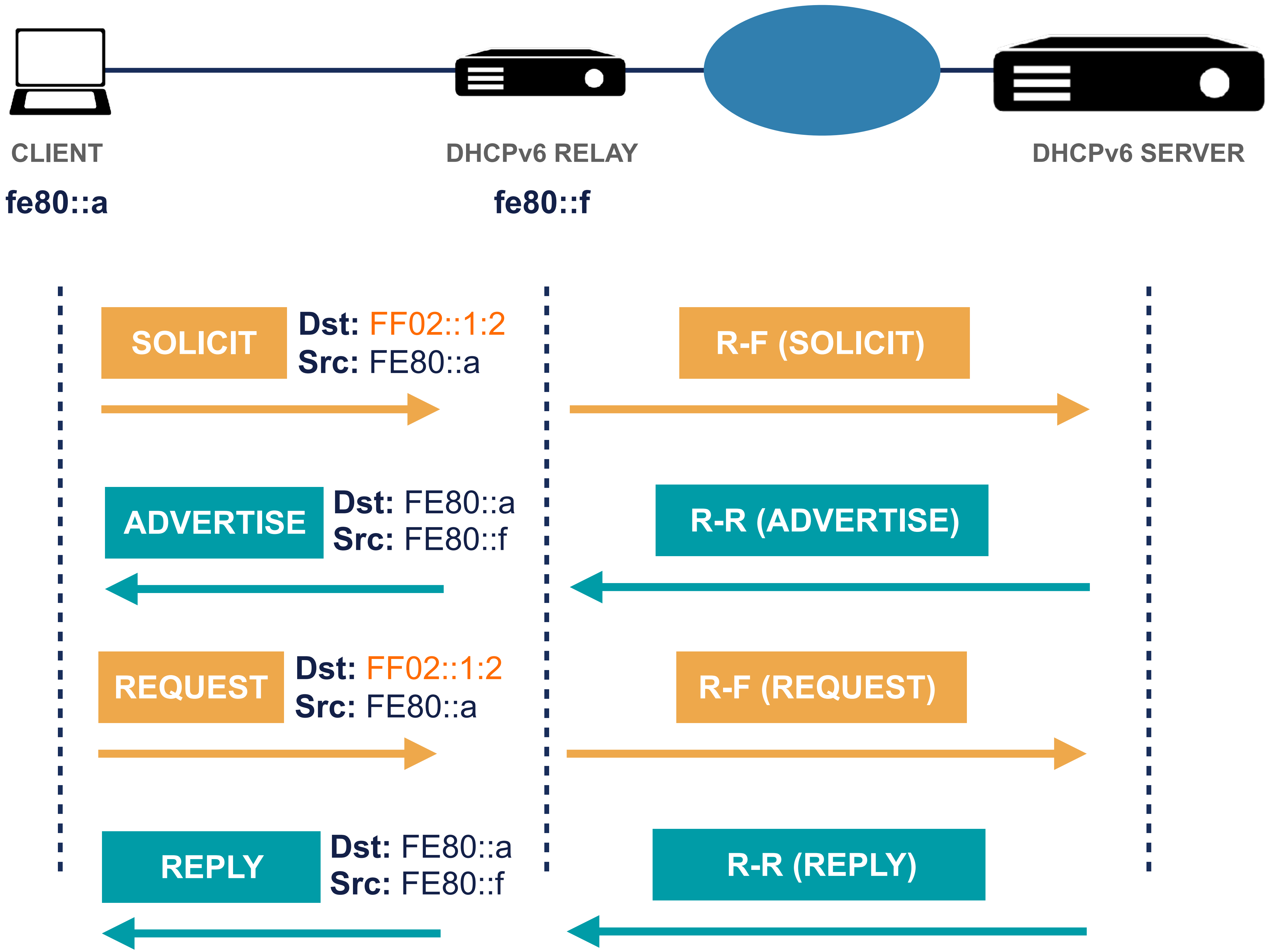
Message names change
SOLICIT
ADVERTISE
REQUEST
REPLY
…

Multicast in DHCPv6

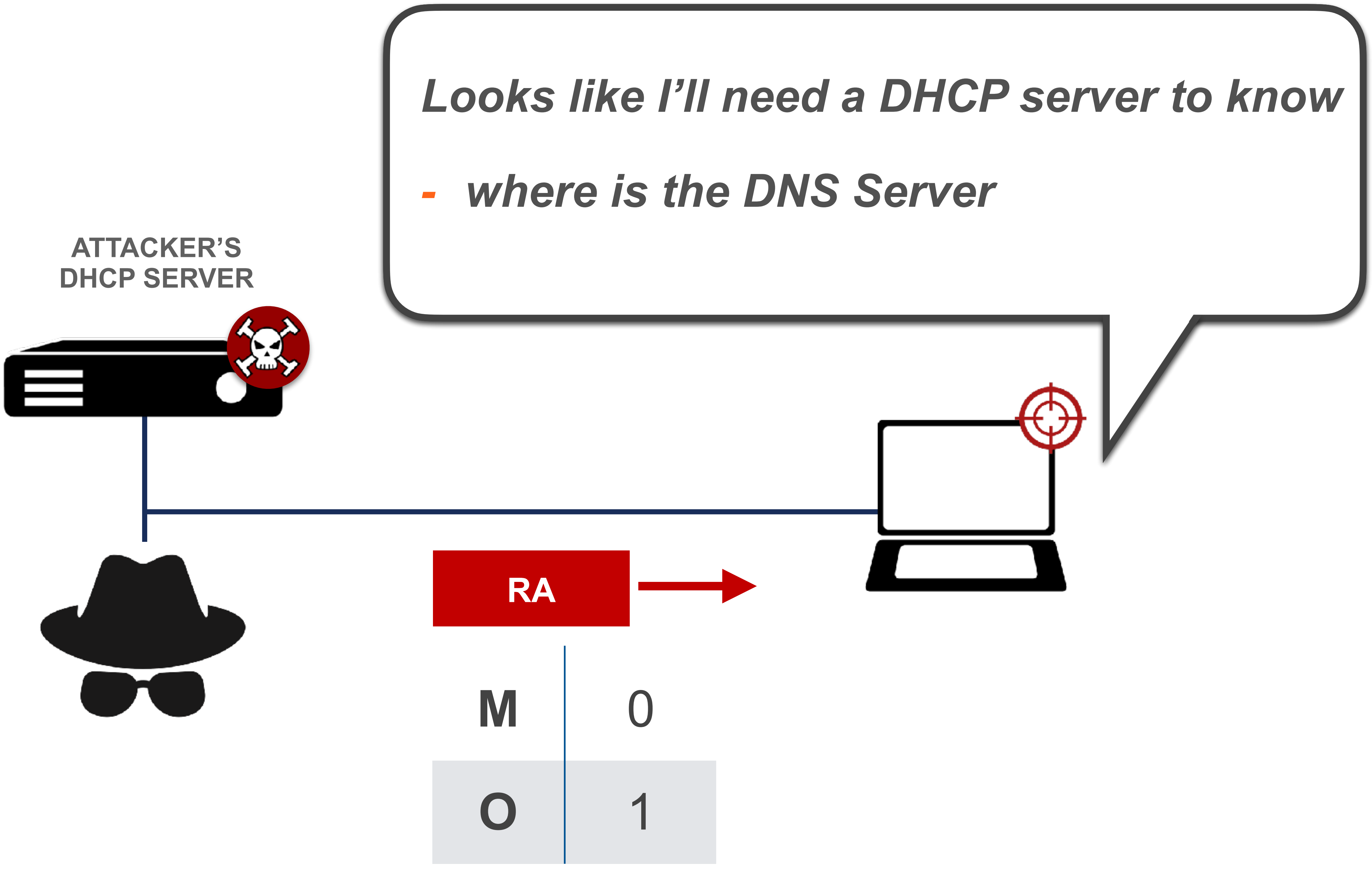
Servers and relays listen on multicast addresses

All DHCP Relay Agents and Servers	FF02::1:2
All DHCP Servers	FF05::1:3

How DHCPv6 works



Triggering the use of DHCP



Privacy Considerations

Client information can be obtained from IDs

like the MAC from Client-ID

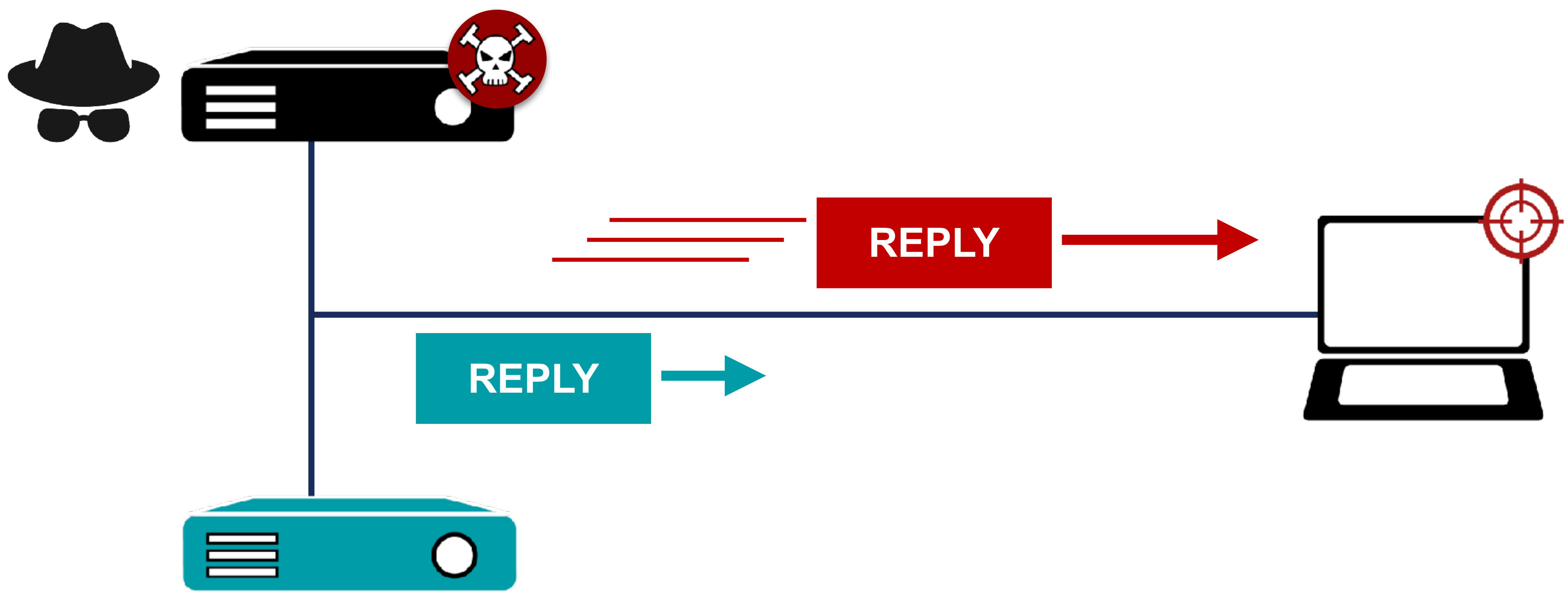
Privacy Considerations

Server address assignment strategies:

- **Iterative:** scanning easier
- **Identifier-based:** easier to track activity
- **Hash:** better, but still allows activity tracking
- **Random:** better privacy

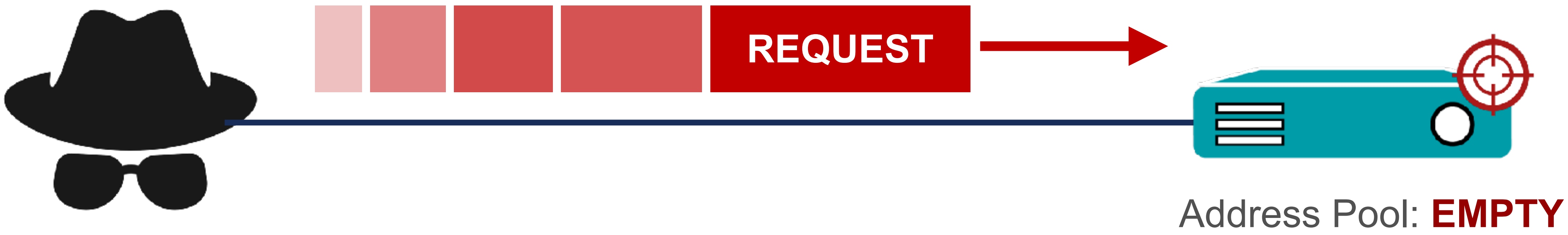
Rogue DHCP Server

Answers before legitimate server

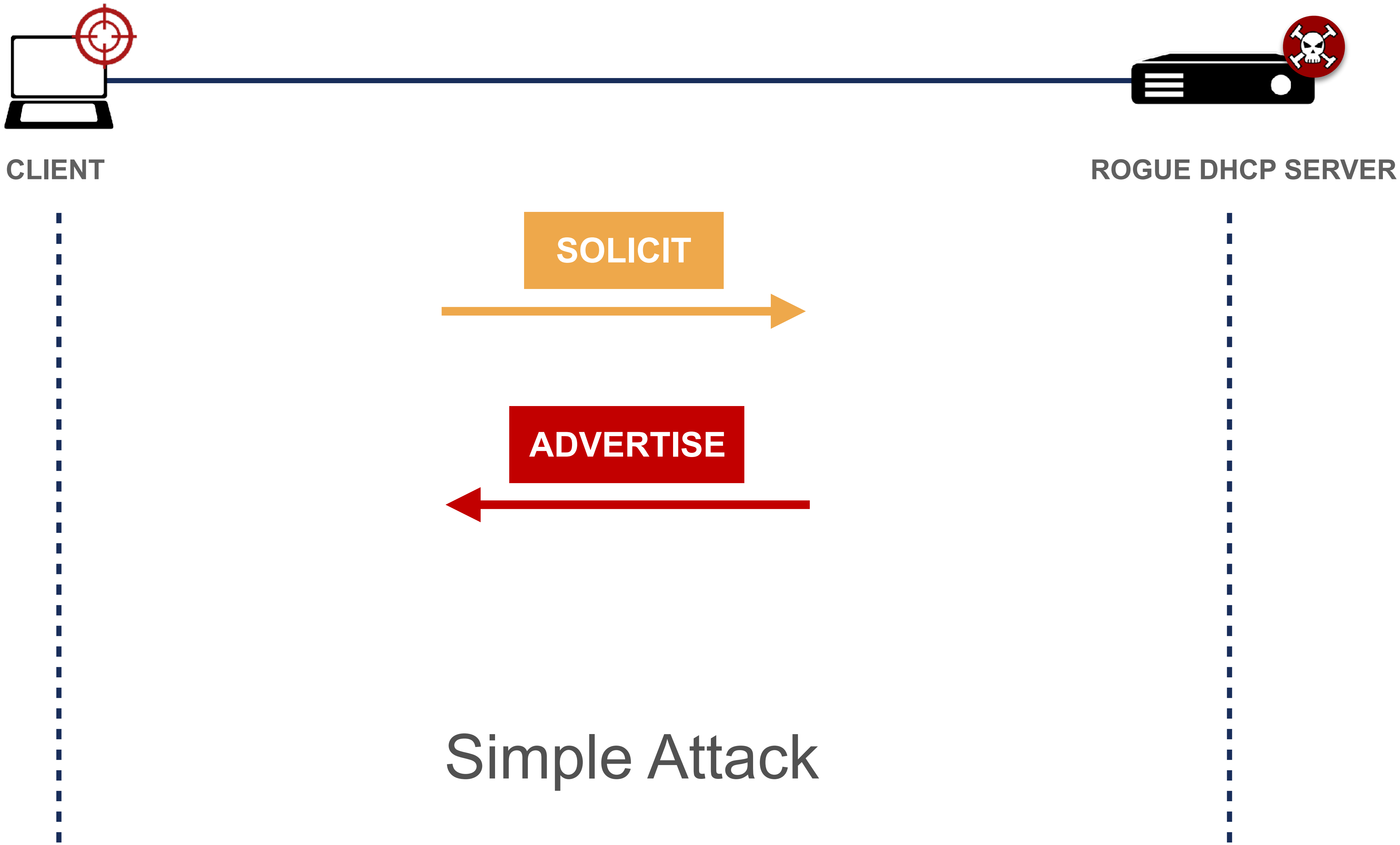


Rogue DHCP Server

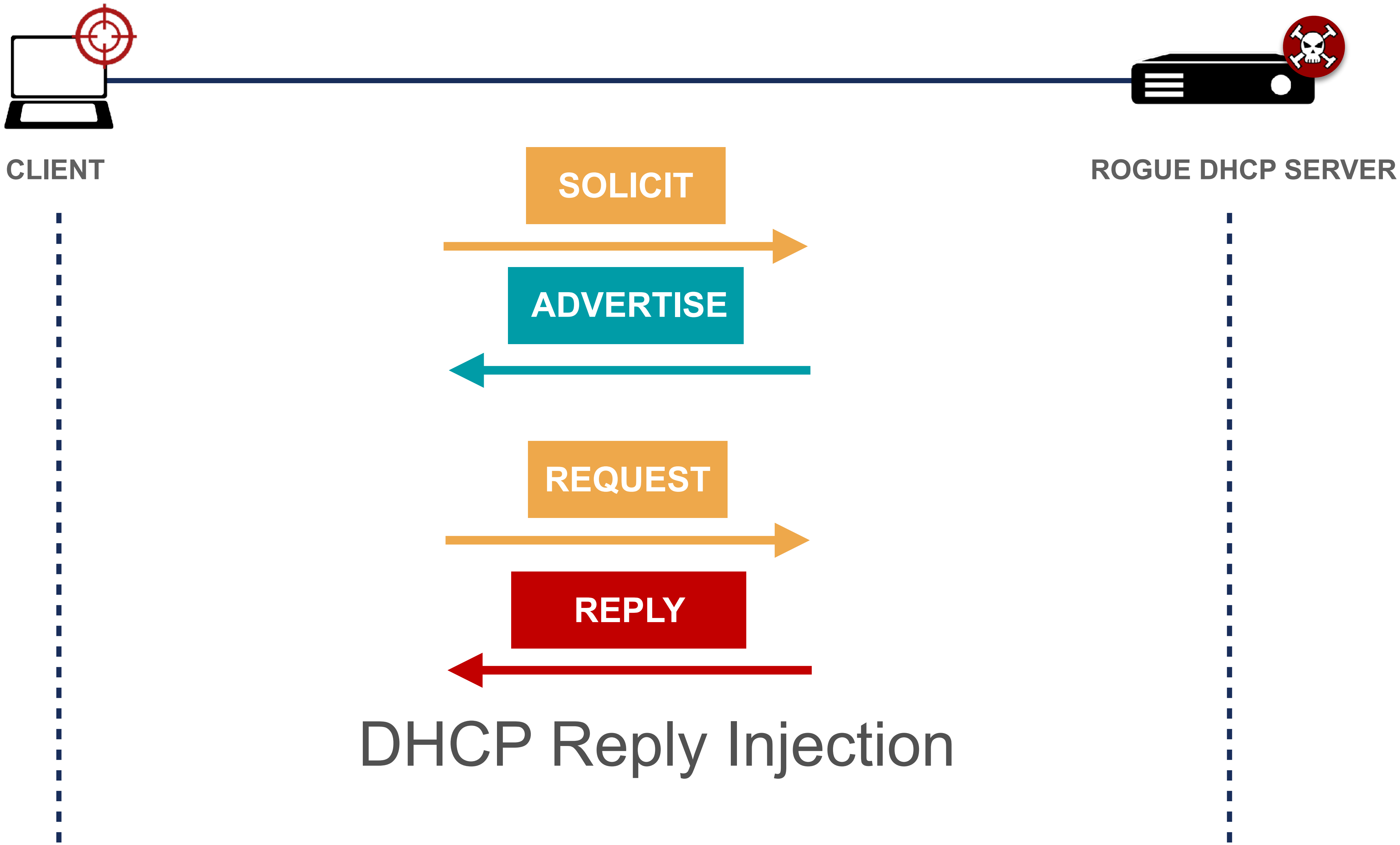
DHCP Exhaustion Attack



Rogue DHCP Server



Rogue DHCP Server

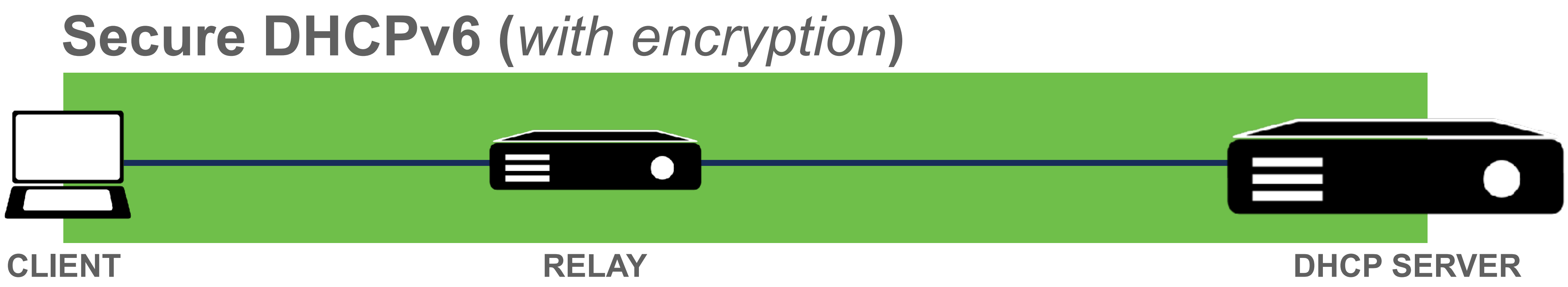


DHCPv6 Solutions

RFC8415 **- Security Considerations**

recommends ***RFC8213*** **- IPSec with Encryption**

DHCPv6 Solutions



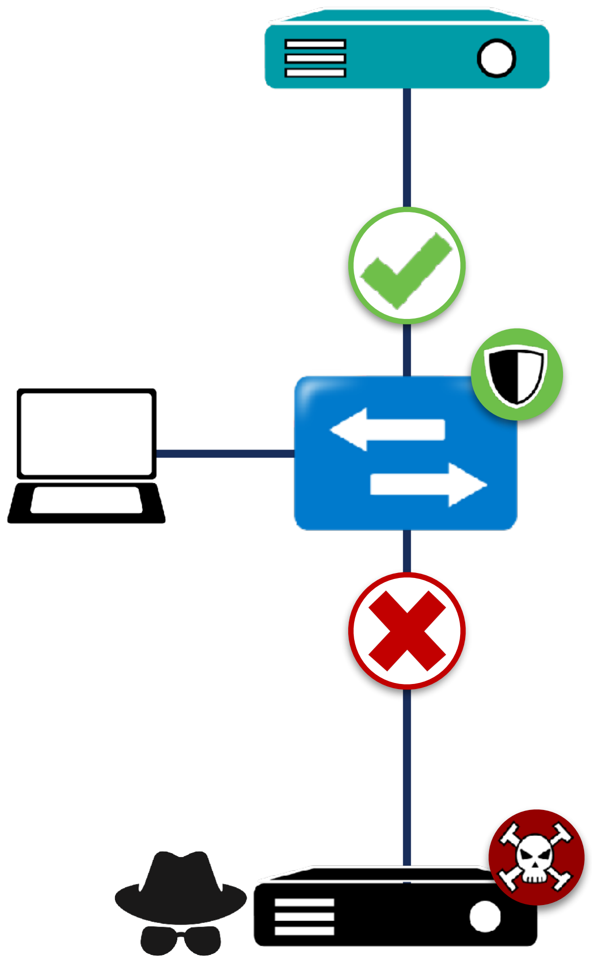
End-to-end encryption

Public key cryptography

Authentication

DHCPv6 Shield

RFC7610



- Protects **clients** only
- Implemented on **L2 switches**
- **DHCPv6 Guard** is vendor implementation

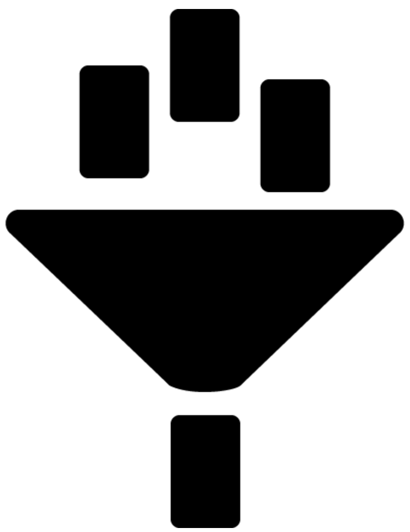
IPv6 Filtering

Section 4

Filtering IPv6 Traffic

Section 4.1

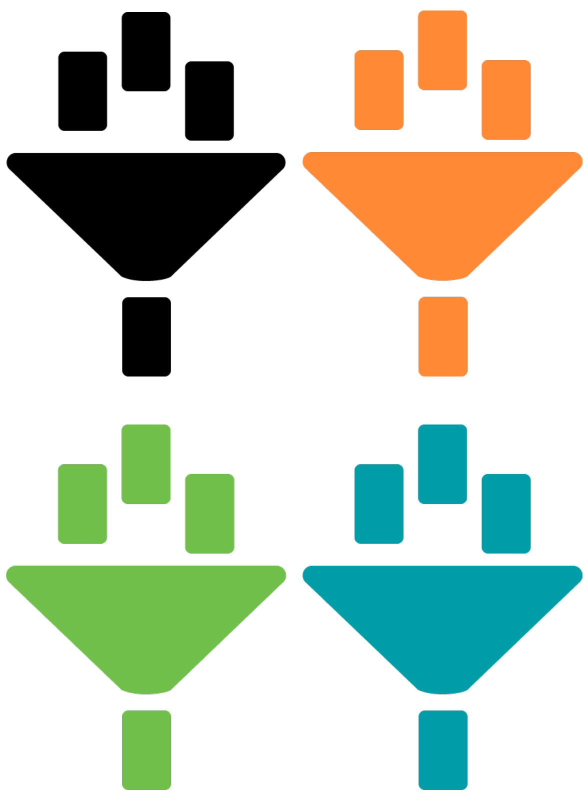
Filtering in IPv6 is very Important!



- Global Unicast Addresses
- A good **addressing plan**

Easier filtering!

New Filters to Take Into Account



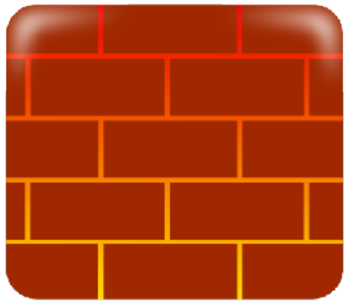
- ICMPv6
- IPv6 Extension Headers
- Fragments Filtering
- Transition mechanisms (TMs) / Dual-Stack

Filtering ICMPv6

Type - Code	Description	Action
Type 1 - all	Destination Unreachable	ALLOW
Type 2	Packet Too Big	ALLOW
Type 3 - Code 0	Time Exceeded	ALLOW
Type 4 - Code 0, 1 & 2	Parameter Problem	ALLOW
Type 128	Echo Reply	ALLOW for troubleshoot and services. Rate limit
Type 129	Echo Request	ALLOW for troubleshoot and services. Rate limit
Types 131,132,133, 143	MLD	ALLOW if Multicast or MLD goes through FW
Type 133	Router Solicitation	ALLOW if NDP goes through FW
Type 134	Router Advertisement	ALLOW if NDP goes through FW
Type 135	Neighbour Solicitation	ALLOW if NDP goes through FW
Type 136	Neighbour Advertisement	ALLOW if NDP goes through FW
Type 137	Redirect	NOT ALLOW by default
Type 138	Router Renumbering	NOT ALLOW

More on RFC 4890 - https://tools.ietf.org/html/rfc4890

Filtering Extension Headers



- **Firewalls** should be able to:
  1. Recognise and filter some **EHs** (example: **RH0**)
  2. Follow the **chain of headers**
  3. Not allow **forbidden combinations** of headers

Filtering Fragments

Upper layer info not in 1st fragment → Creates many tiny fragments to go through filtering / detection

Fragments inside fragments → Several fragment headers

Fragmentation inside a tunnel → External header hides fragmentation

Filtering Fragments

Upper layer info not in 1st Fragment	**All header chain should be in the 1st fragment** [RFC7112]
Fragments inside fragments	**Should not happen in IPv6. Filter them**
Fragmentation inside a tunnel	**FW / IPS / IDS should support inspection of encapsulated traffic**

Filtering TMs / Dual-stack

Technology	Filtering Rules
Native IPv6	EtherType 0x86DD
6in4	IP proto 41
6in4 (GRE)	IP proto 47
6in4 (6-UDP-4)	IP proto 17 + IPv6
6to4	IP proto 41
6RD	IP proto 41
ISATAP	IP proto 41
Teredo	UDP Dest Port 3544
Tunnel Broker with TSP	(IP proto 41) || (UDP dst port 3653 || TCP dst port 3653)
AYIYA	UDP dest port 5072 || TCP dest port 5072

More on RFC 7123 - https://tools.ietf.org/html/rfc7123

IANA Protocol Numbers - https://www.iana.org/assignments/protocol-numbers/protocol-numbers.xhtml

IPv6 Packet Filtering

Much more important in IPv6

+

Common IPv4 Practices

+

New IPv6 Considerations

- End to End needs filtering
- ICMPv6 should be wisely filtered
- Filtering adapted to IPv6: EHs, TMs

Filtering IPv6 Traffic

Exercise 4.1

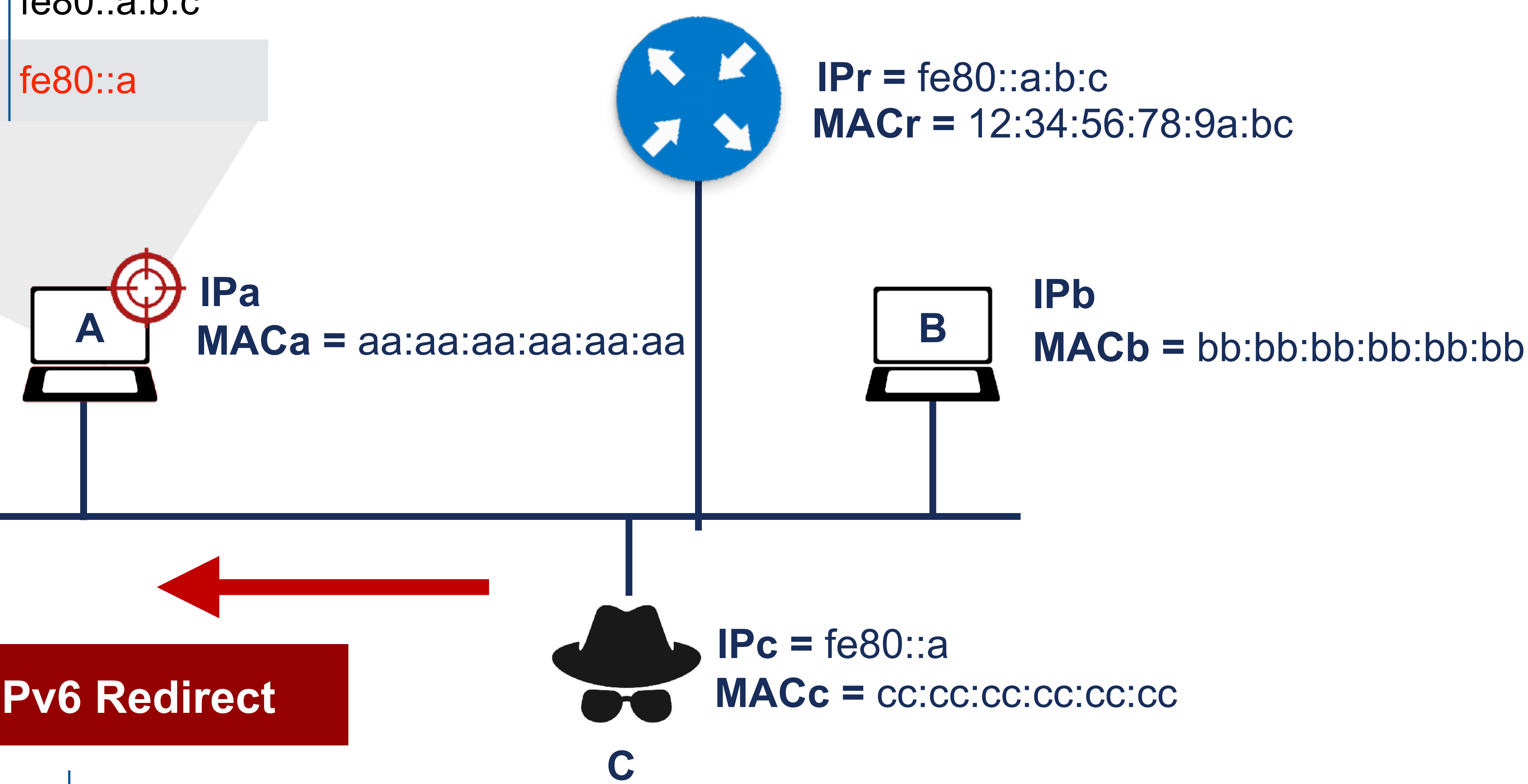
Exercise 4.1 IPv6 Packet Filtering

- **Description**: Configure IPv6 packet filters
- **Goals**:
  - Understand IPv6 packet filtering
  - Learn how to use ip6tables on Linux hosts
- **Time:** 20 minutes
- **Tasks**:
  - Configure IPv6 packet filtering rules

4.1: IPv6 Packet Filtering - Redirect

Routes on Host A	
::/0	fe80::a:b:c
2001:db8:bad:dad::1	fe80::a

```
# ip -6 route show cache
```



IPv6	ICMPv6 Redirect

IPv6.Source	fe80::a:b:c
IPv6.Destination	IPa
Redirect.Target Addr	fe80::a
Redirect.Dst Addr	2001:db8:bad:dad::1

Internet Wide IPv6 Security

Section 5

DDoS

Section 5.1

DDoS attacks in IPv6?

ZDNet

CENTRAL EUROPE MIDDLE EAST SCANDINAVIA AFRICA UK ITALY SPAIN MORE NEWSLETTERS ALL WRITER

JUST IN INTEL CHIP FLAW LETS HACKERS EASILY HIJACK FLEETS OF PCS

First IPv6 Distributed Denial of Service Internet attacks seen

You know IPv6 must finally be making it: The first IPv6 Distributed Denial of Service Internet attacks have been spotted in the wild.

By Steven J. Vaughan-Nichols for Networking | February 20, 2012 -- 14:48 GMT (14:48 GMT) | Topic: Networking

SIGN IN The Register®

{* NETWORKS *}

It's begun: 'First' IPv6 denial-of-service attack puts IT bods on notice

Internet engineers warn this is only the beginning

Kieren McCarthy in San Francisco Sat 3 Mar 2018 // 09:30 UTC

DDoS factors related with IPv6

- Using lots of hosts
- Using outdated firmware
- Poor (or no) security measures

DDoS factors related with IPv6

Filter traffic

Don't allow access to all IPv6 addresses

Update firmware

Use security measures for IPv6

Ingress / Egress filtering and RPF

Hierarchical IPv6 address assignment

IPv6 Transition Mechanisms

Section 5.2

Temporary solution...

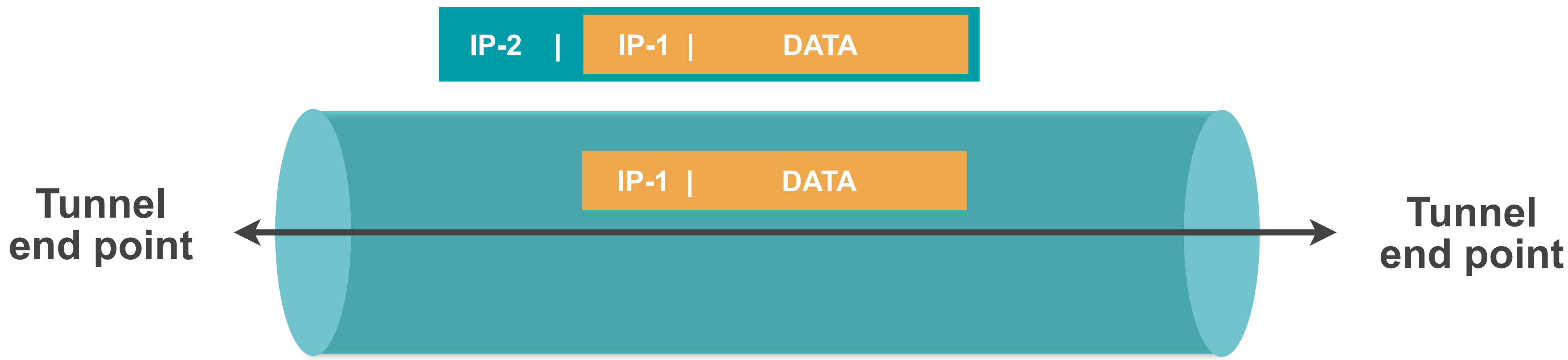
With security risks!

- In IPv4-only infrastructure expect **dual-stack hosts**:
  - VPNs or tunnels
  - Undesired local IPv6 traffic
  - Automatic Transition Mechanisms
  - Problems with rogue RAs

Dual-stack

☠	🛡
Bigger attack surface	Protect IPv6 at the same level as IPv4
GUA Addresses	Filter end-to-end IPv6 properly
Use one IP version to attack the other	Don’t trust “IPv4-only”

Tunnelling



Attackers need knowledge of

- Version of IP-1 and IP-2
- Tunnel end points addresses
- Tunneling protocol

To create tailor-made packets for

- Traffic Injection
- Unauthorised use
- Reflection attack
- Loop attack

Solutions

- Filtering
- Authentication

Translation

IPSec can’t be used end-to-end	
DNSSEC can’t be used with DNS64	
Reflection attack	Must support filtering
IP pool depletion attack	Implementations should protect themselves against exhaustion attacks
ALG (Application Level Gateway) CPU Attack	

IPv6 Security Tips and Tools

Section 6

Introduction

1	Best security tool is knowledge
2	IPv6 security is a moving target
3	IPv6 is happening: need to know about IPv6 security
4	Cybersecurity challenge: Scalability IPv6 is also responsible for Internet growth

Tips

- IPv6 quite similar to IPv4, many reusable practices
- IPv6 security compared with IPv4:

No changes with IPv6	Changes with IPv6	New IPv6 issues

Up to date information

Information category	**Standardisation Bodies**	**Vulnerabilities Databases**	**Security Tools**	**Cybersecurity Organisations**	**Vendors**	**Public Forums**
Sub-categories	IETF, 3GPP, Broadband Forum		Vulnerability Scanners	CSIRTs / CERTs Gov. / LEAs		Mailing Lists Groups of Interest Security Events
Information in this category	Security considerations Protocol updates Security recommendations	Vulnerability ID (CVE-ID, other) Severity (CVSS, other) Description Affected systems Solutions and workarounds	Vulnerability ID (CVE-ID, other) Severity (CVSS, other) Description Affected systems Solutions and workarounds Affected devices in your network	Vulnerability ID (CVE-ID, other) Severity (CVSS, other) Description Affected systems Solutions and workarounds “0 Day” vulnerabilities	Vulnerability ID (CVE-ID, other) Severity (CVSS, other) Description Affected systems Solutions and workarounds “0 Day” vulnerabilities	“0 Day” vulnerabilities News Trends Lessons learned
Examples	RFCs, I-Ds	NVD, CVE	OpenVAS	CERT-EU ENISA EUROPOL/EC3	Cisco, Juniper, MS, Kaspersky, etc.	NOGs, IETF, IPv6 Hackers, Reddit, Troopers, etc.

Examples

Manual

CVE

cve.mitre.org/cve/search_cve_list.html

Search for: **ICMPv6 windows**

NVD

https://nvd.nist.gov/vuln/search

Search for: **CVE-2020-16899**

Go to vendor's link

Automated

OpenVAS

Name ▼	Status	Reports	Last Report	Severity
Windows Workgroup Test	Stopped at 2 %	1		
Windows Domain Test	Stopped at 2 %	1		
DMZ Mail Scan	Container			
EulerOS Scan	Stopped at 22 %	74	Thu, Dec 26, 2019 6:00 AM UTC	10.0 (High)
TLS Map Scan	Done	1	Fri, Dec 27, 2019 1:38 PM UTC	0.0 (Log)
Metasploitable Test - GSM Master	Done	1	Fri, Jan 3, 2020 11:29 AM UTC	10.0 (High)
DMZ Mail Scan 2	New			
system discovery	Done	1	Fri, Dec 20, 2019 10:29 AM UTC	0.0 (Log)

Homework

Go to: cert.europa.eu

Select language filters

Search for IPv6

optional: configure a subscription

Go to NVD: https://nvd.nist.gov/vuln/search

Search for IPv6 + your vendor

Security Tools

Type	Can be used for	Examples
Packet Generators	Assessing IPv6 security Testing implementations Learning about protocols Proof of concept of attacks/protocols	Scapy, nmap, Ostinato, TRex
Packet Sniffers/ Analyzers	Understanding attacks and security measures Learning about protocols and implementations Troubleshooting	tcpdump, Scapy, Wireshark, termshark
Specialised Toolkits	Assessing IPv6 security Learning about protocols and implementations Proof of concept of attacks/protocols Learn about new attacks	THC-IPV6, The IPv6 Toolkit, Ettercap
Scanners	Finding devices and information Proactively protect against vulnerabilities	nmap, OpenVAS
IDS/IPS	Understanding attacks and security measures Learning about protocols and implementations Assessing IPv6 security Learn about new attacks	Snort, Suricata, Zeek

Devices Categories (RIPE-772)

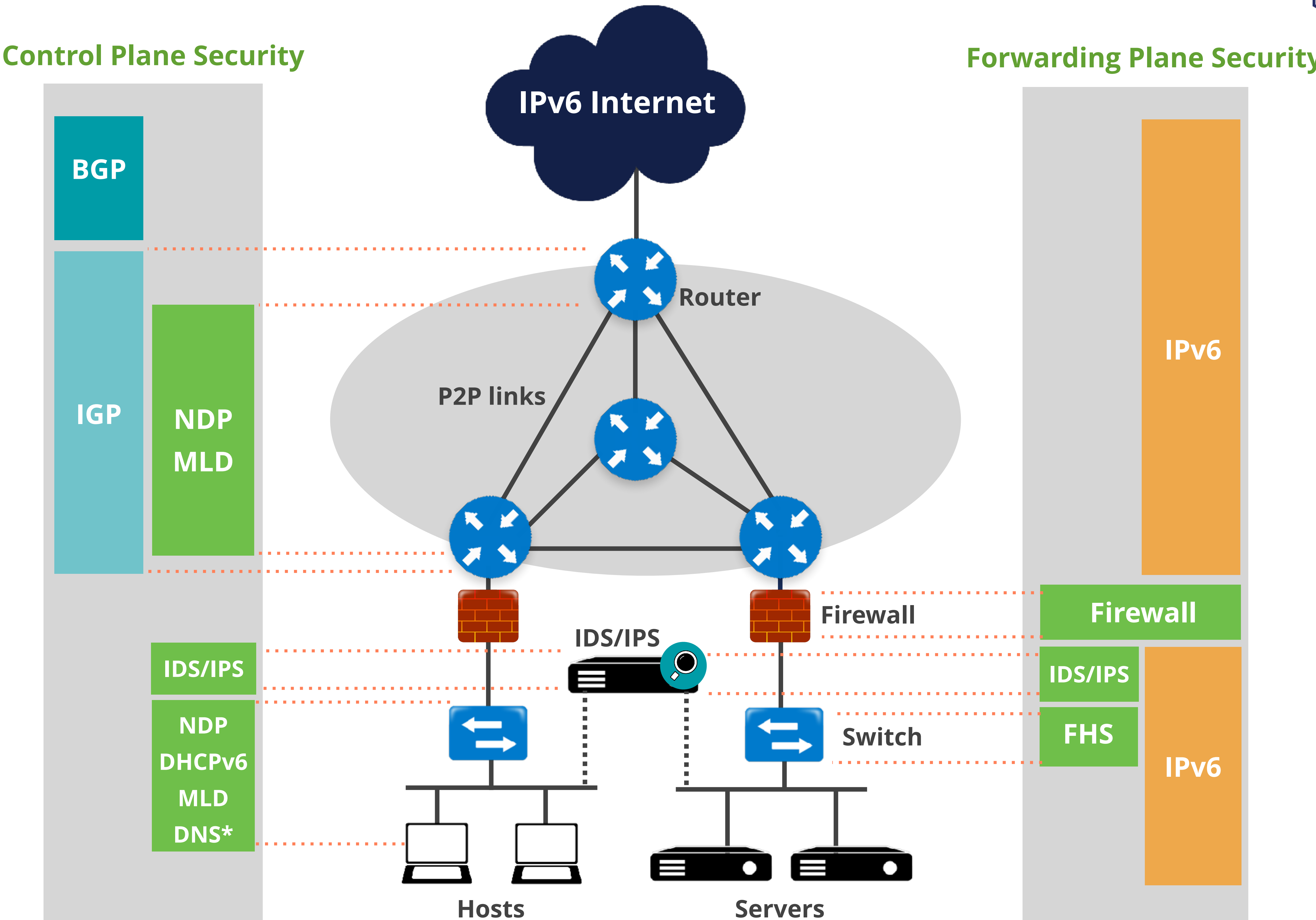
Host
- **IPSec** (if needed)
- **RH0** [RFC5095]
- **Overlapping Frags** [RFC5722]
- **Atomic Fragments** [RFC6946]
- **NDP Fragmentation** [RFC6980]
- **Header chain** [RFC7112]
- **Stable IIDs** [RFC8064][RFC7217][RFC7136]
- **Temp. Address Extensions** [RFC8981]
- **Disable if not used:** LLMNR, mDNS, DNS-SD, 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]
  - **MD5 Signature Option** [RFC2385] *Obsoleted*
  - **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**



* All Name resolution related protocols

What's Next in IPv6

Webinars

Attend another webinar live wherever you are.

- Introduction to IPv6 (2 hrs)
- IPv6 Host Configuration (2 hrs)
- IPv6 Addressing Plan (1 hr)
- Basic IPv6 Protocol Security (2 hrs)
- IPv6 Associated Protocols (2 hrs)
- IPv6 Security Myths, Filtering and Tips (2 hrs)

For more info click the link below

learning.ripe.net

Face-to-face

Meet us at a location near you for a training session delivered in person.

- Basic IPv6 (8.5 hrs)
- Advanced IPv6 (17 hrs)
- IPv6 Security (8.5 hrs)

E-learning

Learn at your own pace at our online Academy.

- IPv6 Fundamentals (15 hrs)
- IPv6 Security (24 hrs)

For more info click the link below

academy.ripe.net

Examinations

Learnt everything you needed? Get certified!

- IPv6 Fundamentals - Analyst
- IPv6 Security - Expert

For more info click the link below

getcertified.ripe.net

We want your feedback!

What did you think about this course?

Take our survey at:

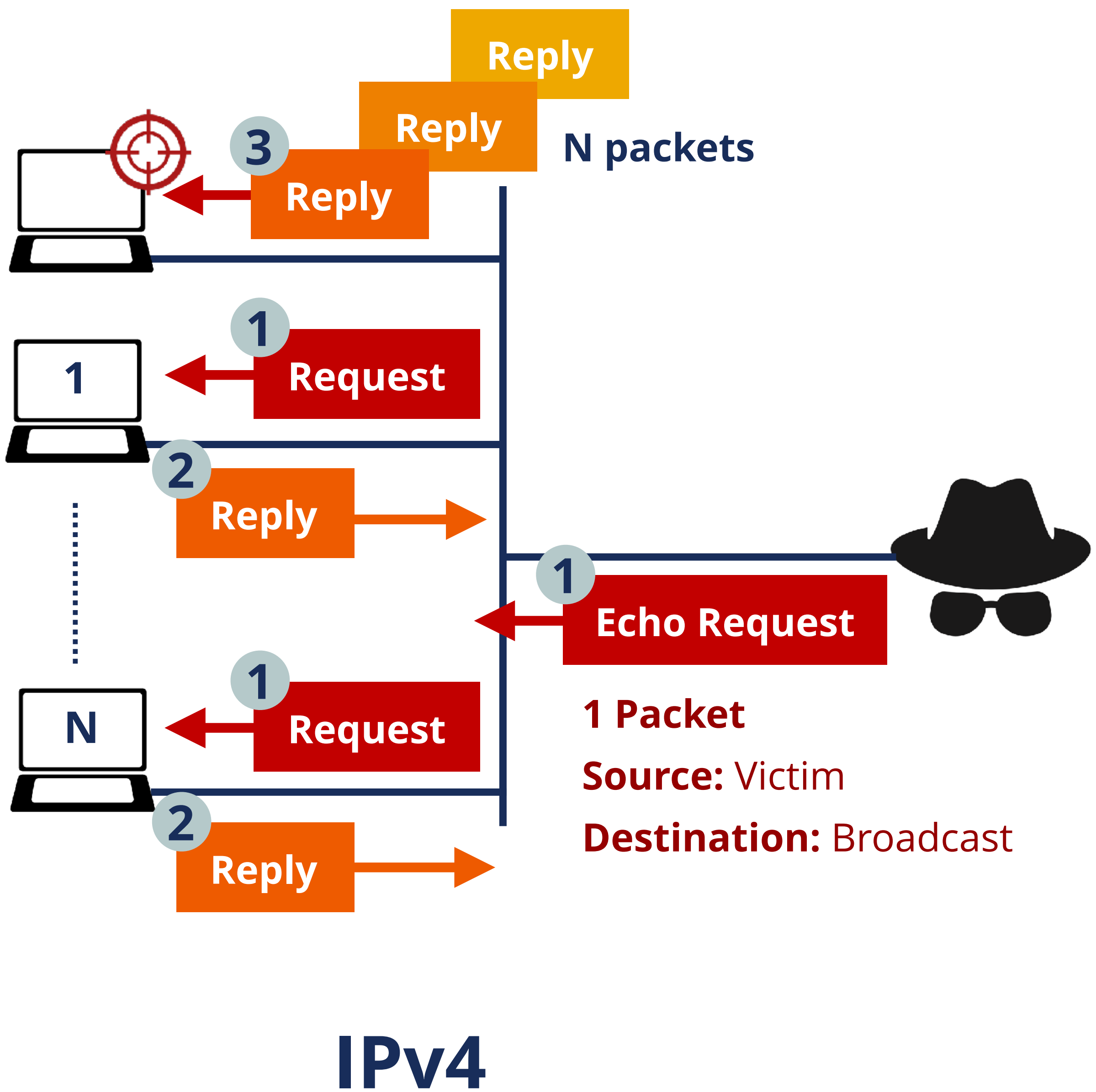
https://www.ripe.net/feedback/v6s/

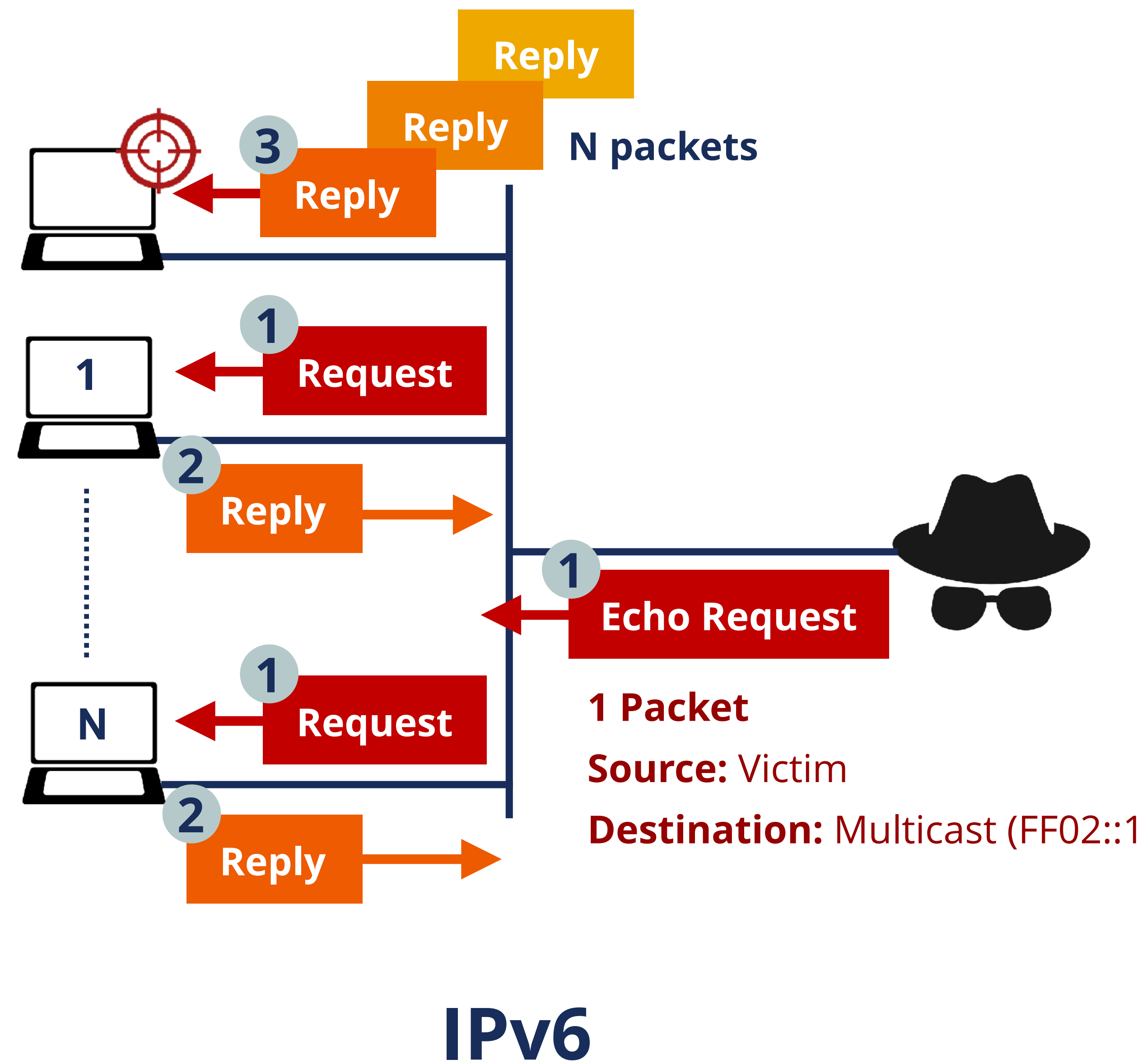

RIPE NCC
Academy
Learn something new today!
academy.ripe.net


RIPE NCC Certified Professionals
RIPE NCC Certified Professionals
IPv6 Fundamentals
Analyst
RIPE NCC Certified Professionals
RIPE Database
Associate
RIPE NCC Certified Professionals
BGP Security
Associate
RIPE NCC Certified Professionals
IPv6 Security
Expert
https://getcertified.ripe.net/

Ënn
Соңы
An Críoch
پایان
Y Diwedd
Vége
Endir
Finvezh
վերջ
Ende
Koniec
Son
დასასრული
הסוף
Tmiem
Кінець
Finis
Lõpp
Amaia
Loppu
Liðugt
Крај
Sfârşit
Slutt
Fund
Kraj
النهاية
Конец
Konec
Fin
Fí
Τέλος
Fine
Einde
Край
Pabaiga
Slut
Fim
Beigas
END

Extra: Smurf Attack



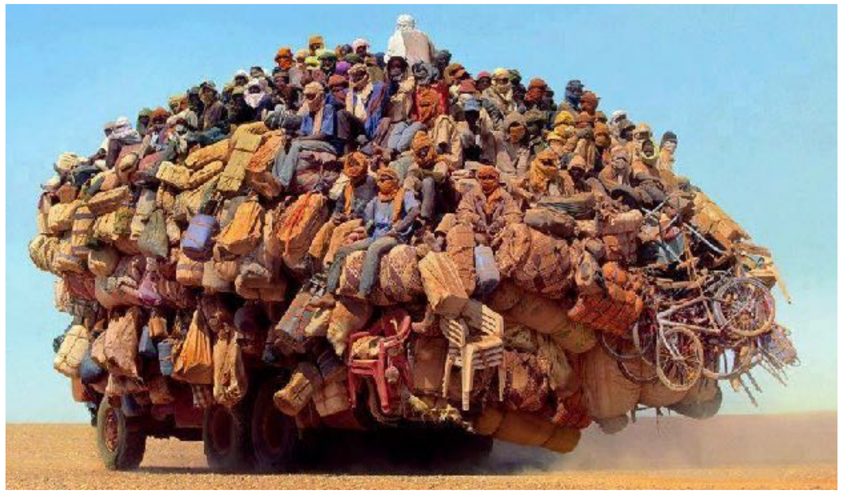


Extra: DoS / DDoS

- **DoS** (Denial of Service): Type of attack that is able to make a service or protocol to stop working.

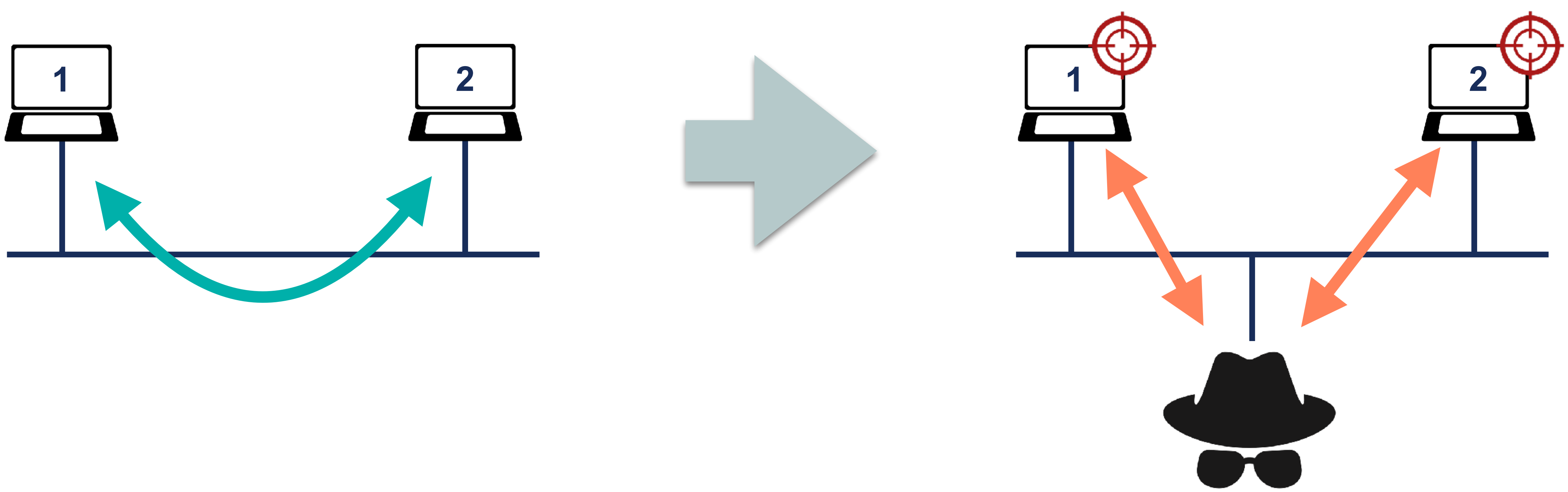
- **DDoS** (Distributed DoS): Is a type of DoS attack that is performed from several devices.

- Example: send too much traffic to a link, so that the routers can't handle it, overloading them



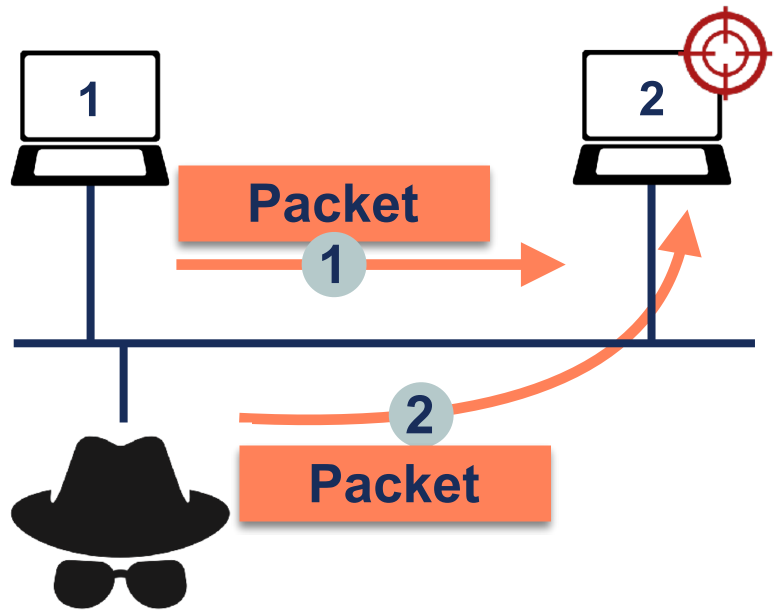
Extra: MITM

- Man-In-The-Middle attack:
  - The attacker is able to be on the path of the packets

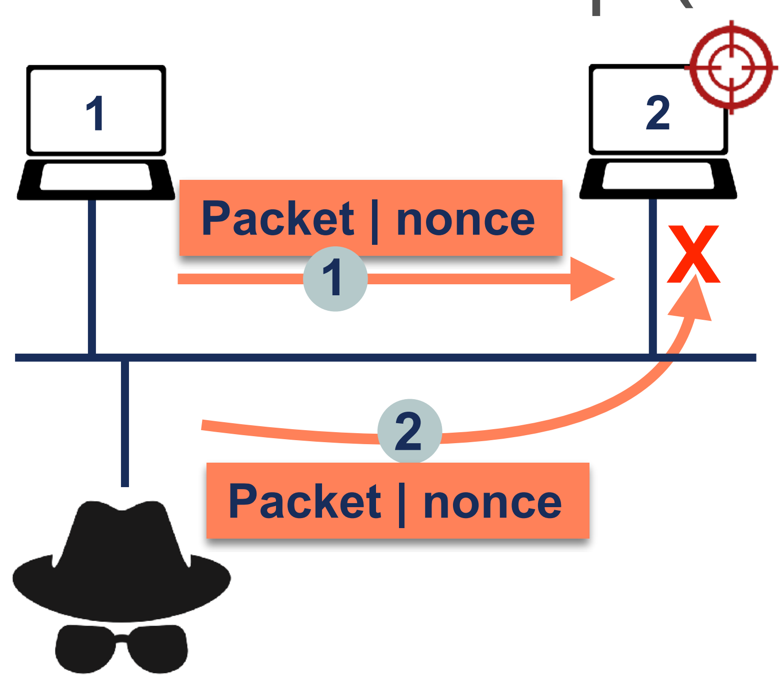


Extra: Replay Attacks

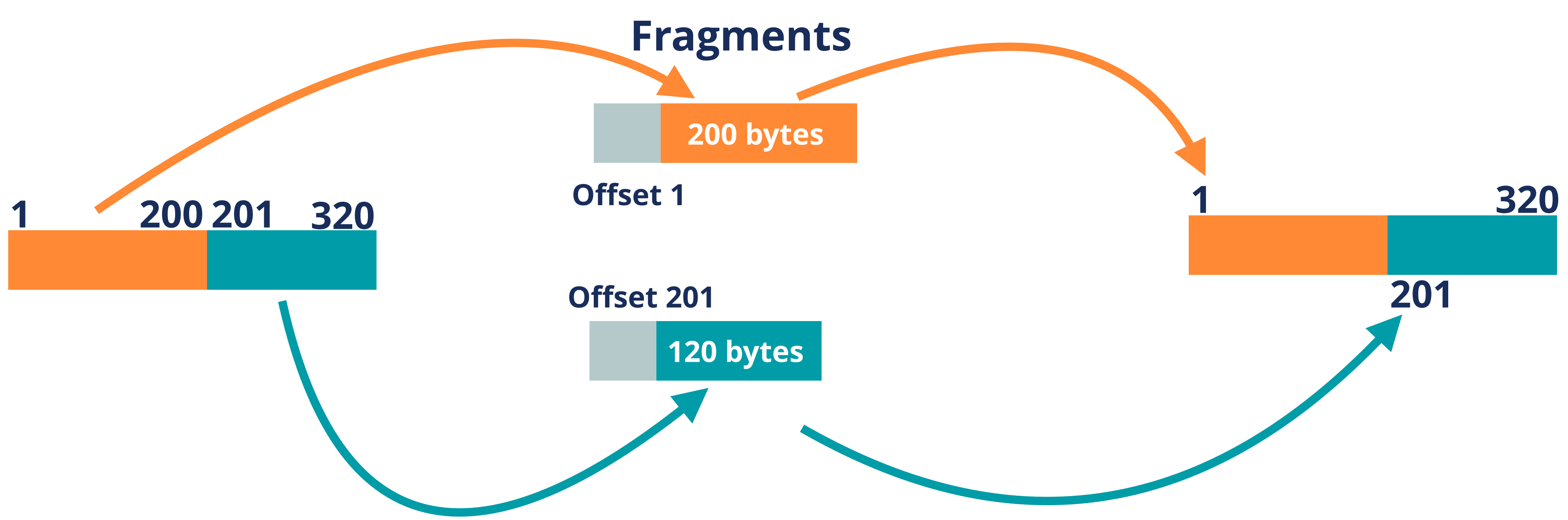
- Replay Attacks consist in sending again a previous packet



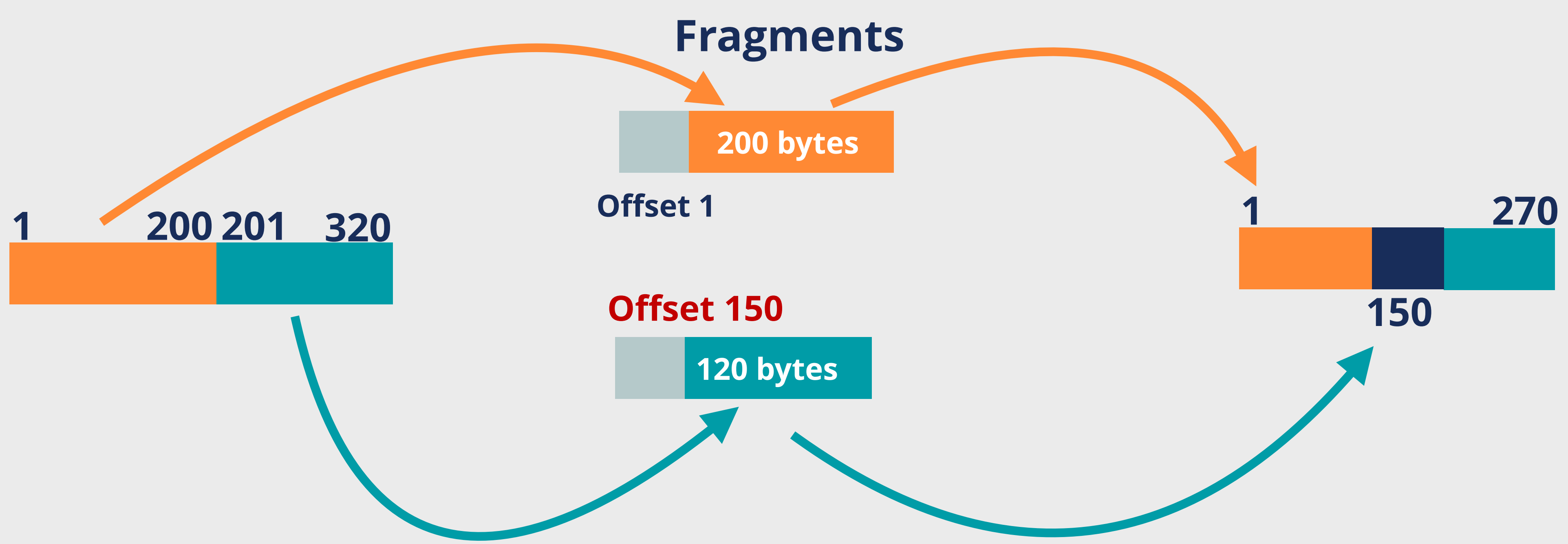
- Solution: nonce or timestamp (makes packet unique)



Extra: Overlapping Fragments



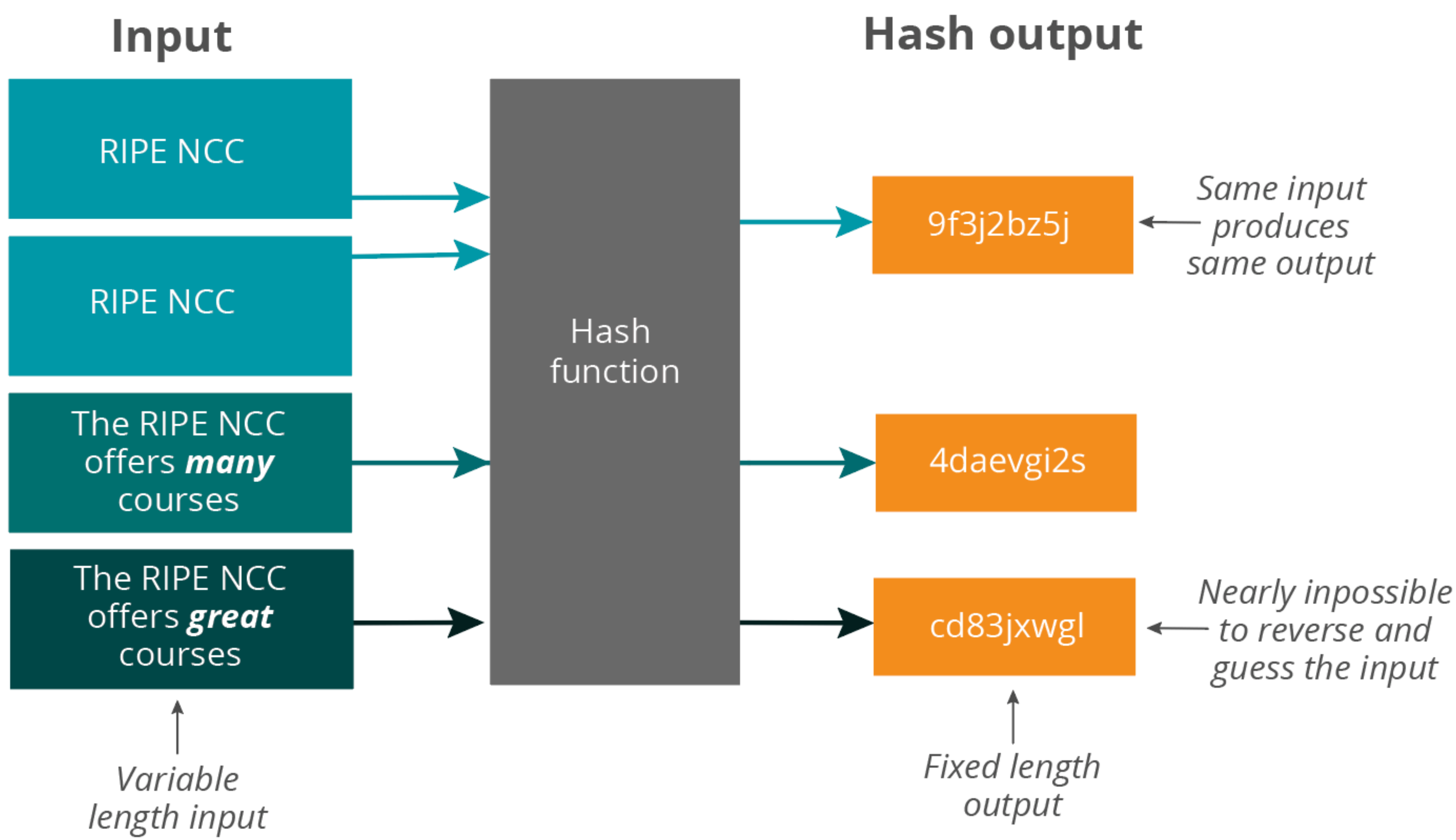
Normal fragments offset say where the data goes



Overlapping fragments have wrong offset values

Extra: Hash Function

- **Input**: Variable length bit string, for example a text
- **Output**: Fixed length bit string, represented by a series of characters



Extra Reference Slides

IPv6 Associated Protocols Security

Section 3

IPv6 Routing protocols

Section 3.6

THIS SECTION	NOT COVERED	SAME AS IPv4
Authentication of neighbors/peers	Route filtering	Router Hardening
Securing routing updates		

Neighbors/Peers Authentication

	Authentication Options	Comments
RIPng	- No authentication - IPsec (general recommendation)	- RIPv2-like MD5 no longer available - IPSec not available in practice
OSPFv3	- IPsec [RFC4552] - Authentication Trailer [RFC7166]	- ESP or AH. Manual keys - Hash of OSPFv3 values. Shared key
IS-IS	- HMAC-MD5 [RFC5304] - HMAC-SHA [RFC5310]	- MD5 not recommended - Many SHA, or any other hash
MBGP	- TCP MD5 Signature Option [RFC2385] - TCP-AO [RFC5925]	- Protects TCP. Available. Obsoleted - Protects TCP. Recommended

Securing Routing Updates

- IPsec is a general solution for IPv6 communication
  - In practice not easy to use

- OSPFv3 specifically states [RFC4552]:
  1. ESP **must** be used
  2. Manual Keying

- Other protocols: **No options available**

Conclusions

- Security options available for IPv6 routing protocols

- Try to use them:
  - Depending on the protocol you use
  - At least at the same level as IPv4

IPv6 Filtering

Section 4

Filtering IPv6 Routing Information

Section 4.2

IPv6 BGP Bogon Prefix Filtering

Use	Prefix
Default	::/0
Unspecified Address	::/128
Loopback Address	::1/128
IPv4-mapped Addresses	::ffff:0.0.0.0/96
IPv4-compatible Addresses (deprecated)	::/96
Link-local Addresses	fe80::/10
Site-local Addresses (deprecated)	fec0::/10
Unique-local addresses	fc00::/7
Multicast Addresses	ff00::/8
Documentation addresses	2001:db8::/32
6Bone Addresses (deprecated)	3ffe::/16, 5f00::/8
ORCHID	2001:10::/28

Team Cymru: https://team-cymru.com/community-services/bogon-reference/

MANRS (www.manrs.org)

- Secure and Resilient Internet is a **collaborative** effort
- **Concrete actions** for: network operators, IXPs, CDN/ Cloud providers
- **IPv6** and **IPv4** BGP

MANRS Network Operators Actions

Facilitate Global Coordination	Keep contact information updated: **RIPE DB, LIR Portal, PeeringDB**	
Facilitate Routing Information Validation	Route Objects	RPKI	Document Policy
Prevent IP Spoofing	uRPF	Ingress Filtering [*RFC2827*][*RFC3704*]
Prevent Incorrect Routing Information	Define Routing Policy	Check BGP Announcements (*RPKI / ROAs*)
	BGP Bogon Filtering	BGPsec (?)

Internet Wide IPv6 Security

Section 5

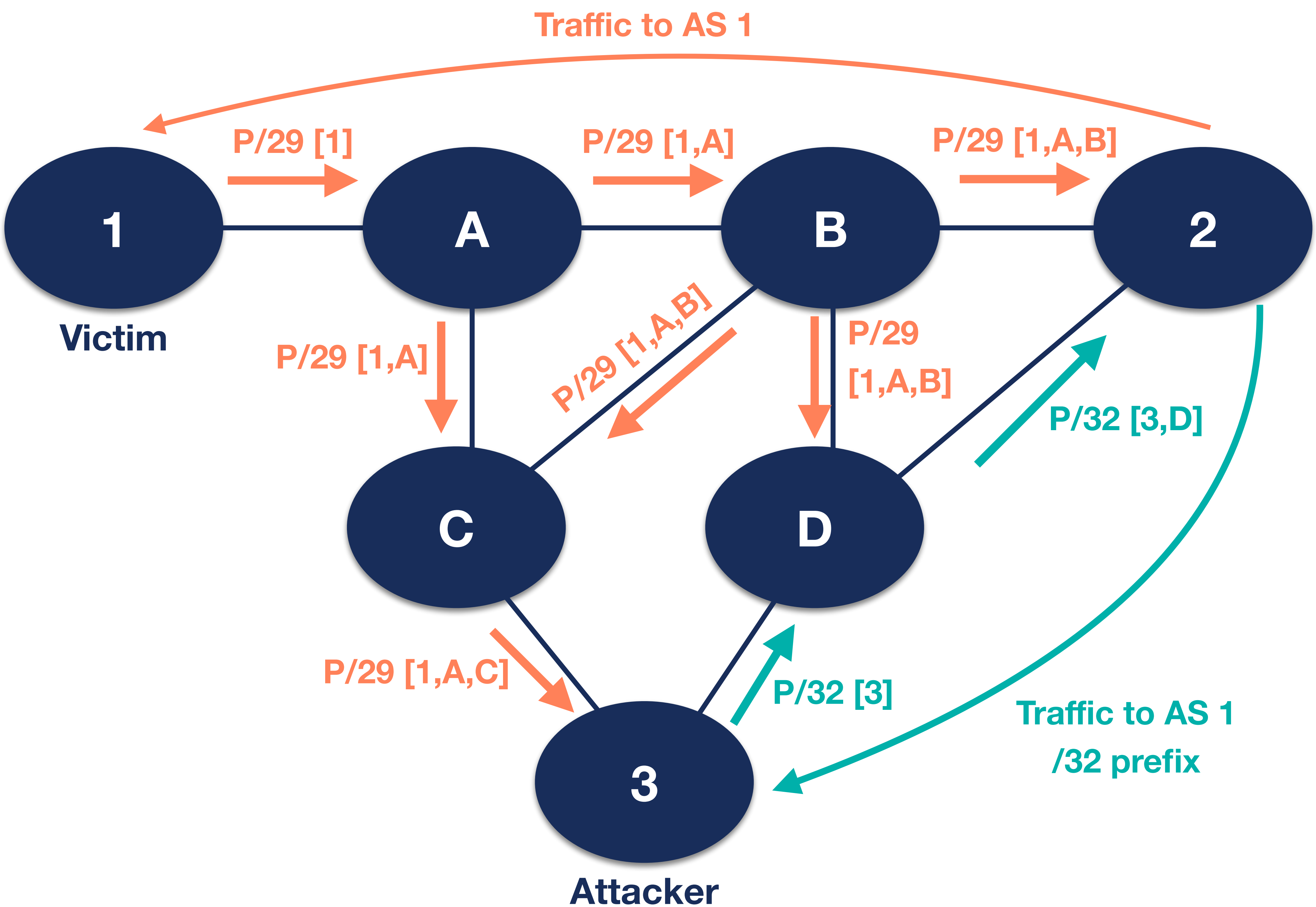
BGP Hijacking

Section 5.3

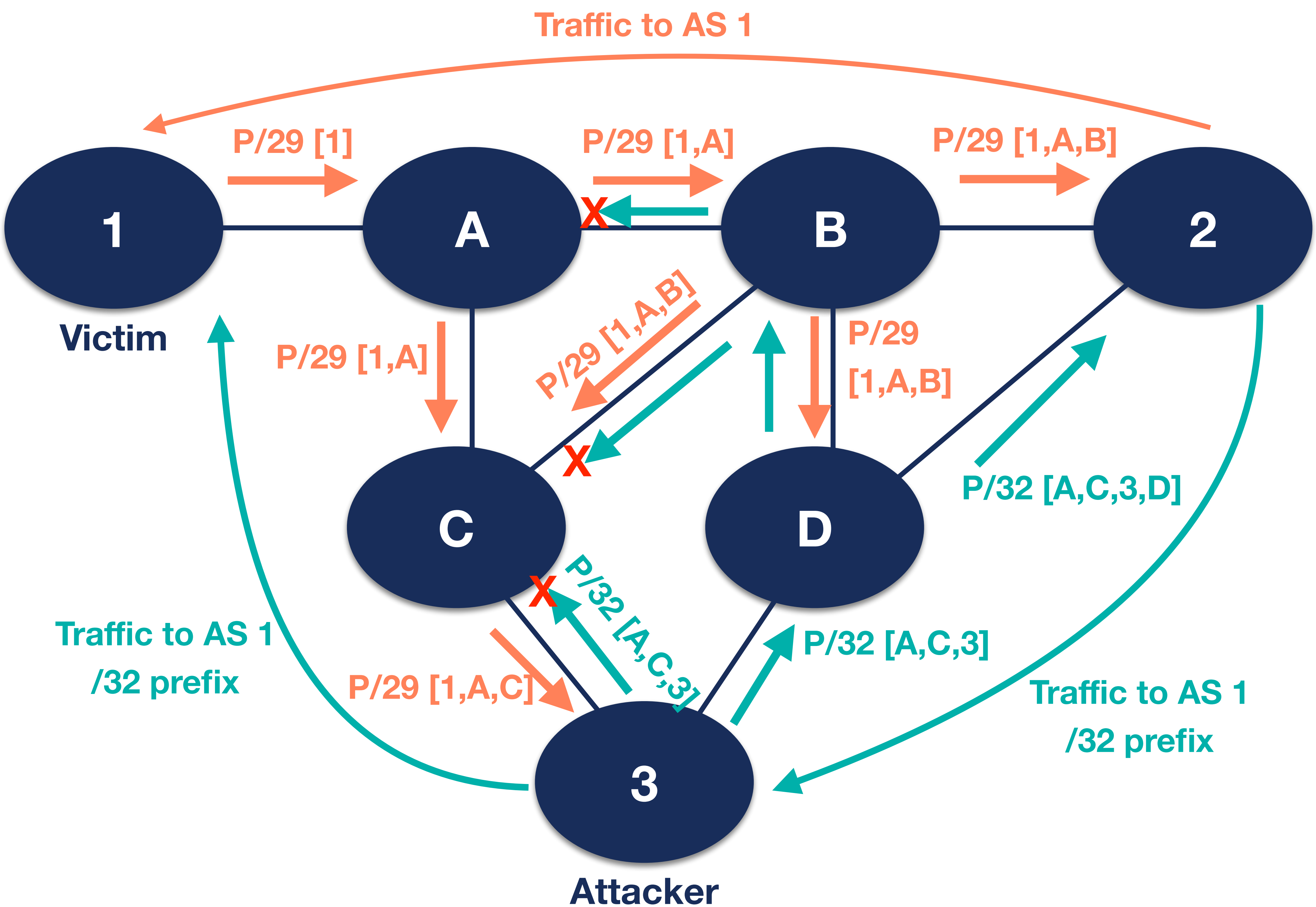
Introduction

- BGP is a control plane protocol (application level)
- Hijack techniques same in IPv6 and IPv4
- Protection techniques as well

BGP Prefix Hijack - Fake Origin



BGP MITM - Fake AS-path



BGP Hijack: Solutions

- To secure BGP for IPv6:

1. Route Filtering
2. RPKI
3. BGPsec (in the future)

- Temporary: More specific announcement