RIPE NCC
RIPE NETWORK COORDINATION CENTRE

IPv6 Security

Training Course

December 2017

Schedule

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
- Number in the list
- Experience with Security and IPv6
- Goals

Overview

Intro

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)

Legend

Learning/
understanding

Attacker

Protecting

Introduction to IPv6 Security

Section 1

IPv6 Security Myths (1)

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 (2)

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 (3)

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 (4)

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 (5)

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 (6)

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 (7)

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 (8)

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

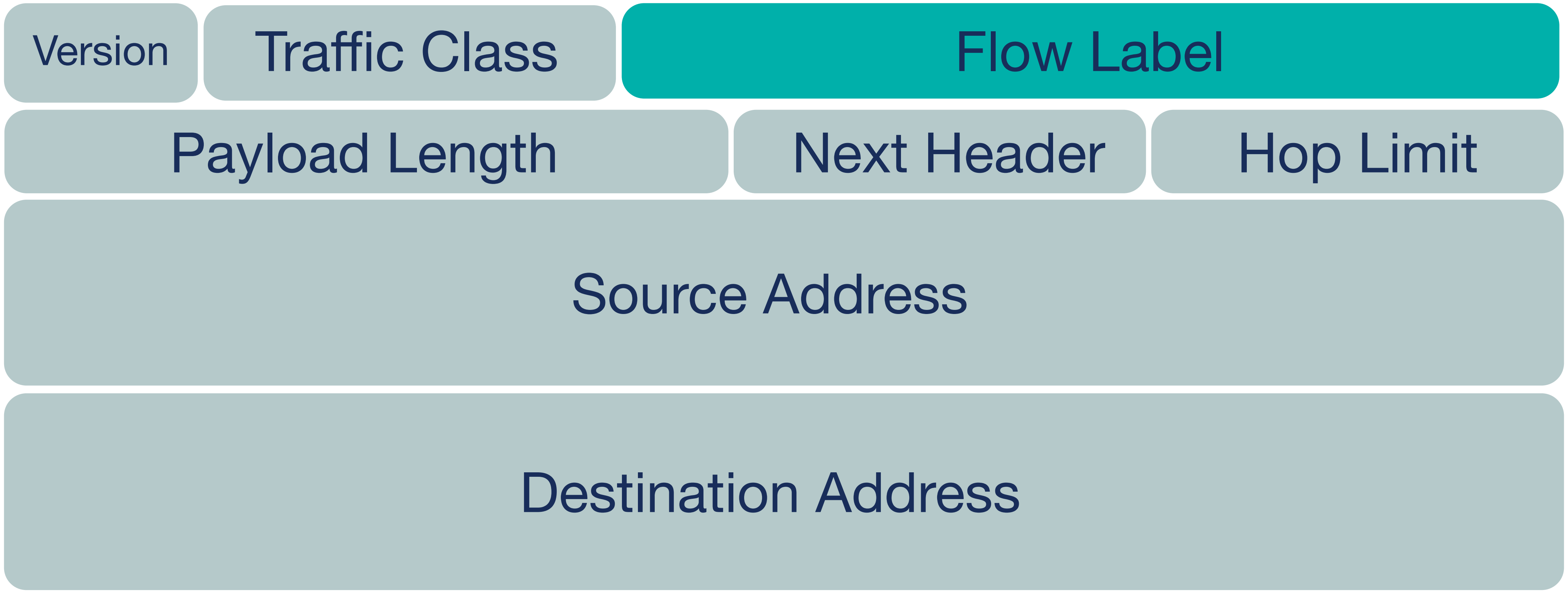
Basic IPv6 Protocol Security

Section 2

IPv6 Basic Header and Extension Headers

Section 2.1

Basic IPv6 Header



Version

Traffic Class

Flow Label

Payload Length

Next Header

Hop Limit

Source Address

Destination Address

- Simplified
- Fixed length (40 bytes)
- Aligned to 64 bits
- New field: Flow Label

Basic IPv6 Header: Threats (1)

- **IP spoofing**: Using a fake IPv6 source address

- Solution: ingress filtering and RPF (reverse path forwarding)

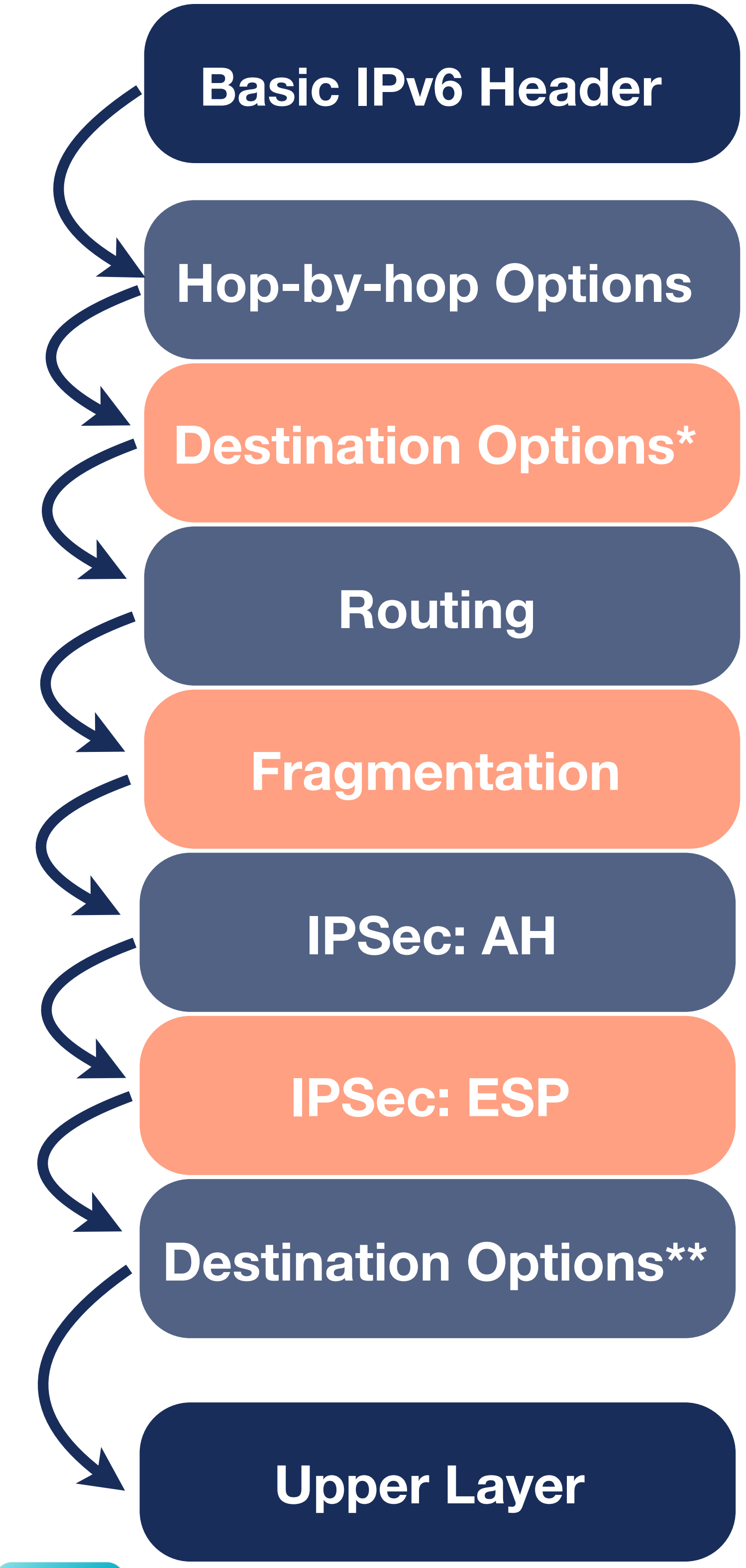
Basic IPv6 Header: Threats (2)

- **Covert Channel**
  - Example: Using Traffic Class and/or Flow Label

- These values should be expected
  - Traffic Class: 0 unless QoS is used
  - Flow Label: 0

- Solution: inspect packets (IDS / IPS)

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)

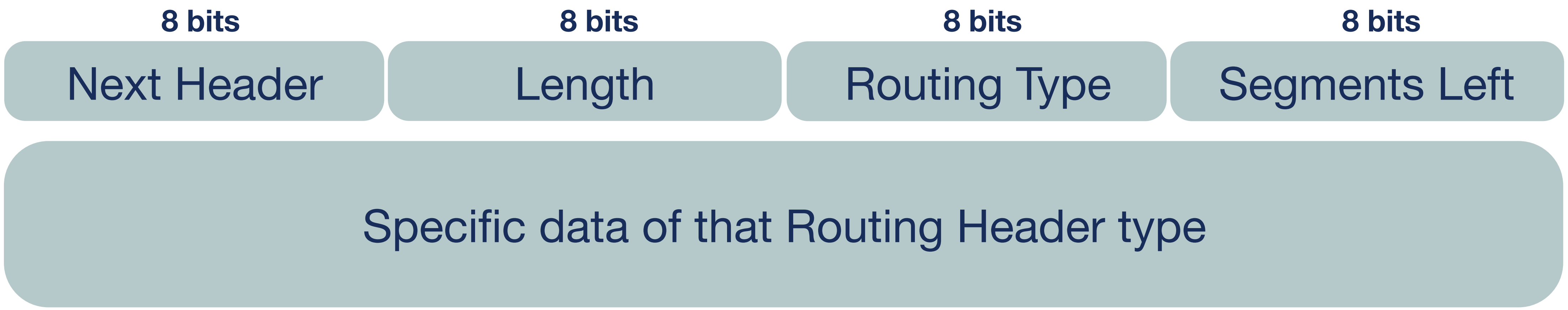
- Flexibility means complexity for security

- 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

IPv6 Extension Headers (3)

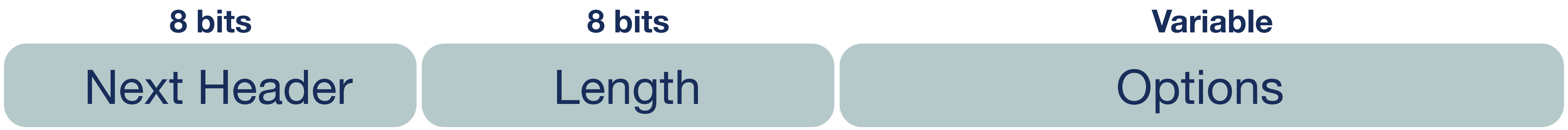
- **Routing** (43): indicates one or more IPs that should be “visited” in the path
  - Processed by the visited routers



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

IPv6 Extension Headers (4)

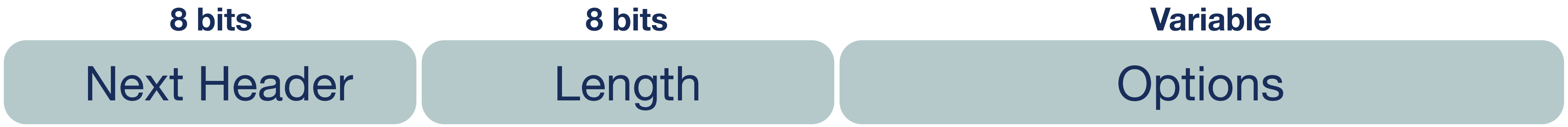
- **Hop-by-Hop Options** (0): processed by each node in the path
  - If used, goes just after the basic IPv6 header
  - Contains one or more options



8 bits	8 bits	Variable
Next Header	Length	Options

IPv6 Extension Headers (5)

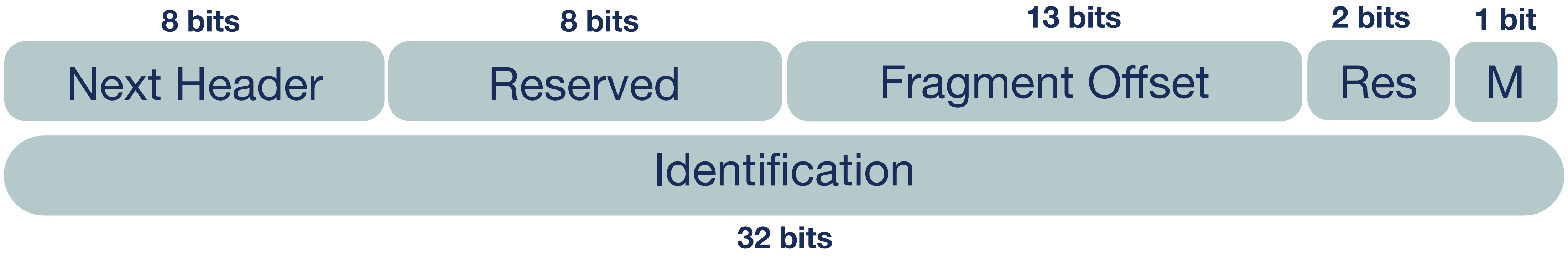
- **Destination Options** (60): To send optional information to the destination host
  - Contains one or more options
  - Could be used twice: routing and destination host



8 bits	8 bits	Variable
Next Header	Length	Options

IPv6 Extension Headers (6)

- **Fragment** (44): Used by the IPv6 source node to send a packet bigger than the 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				

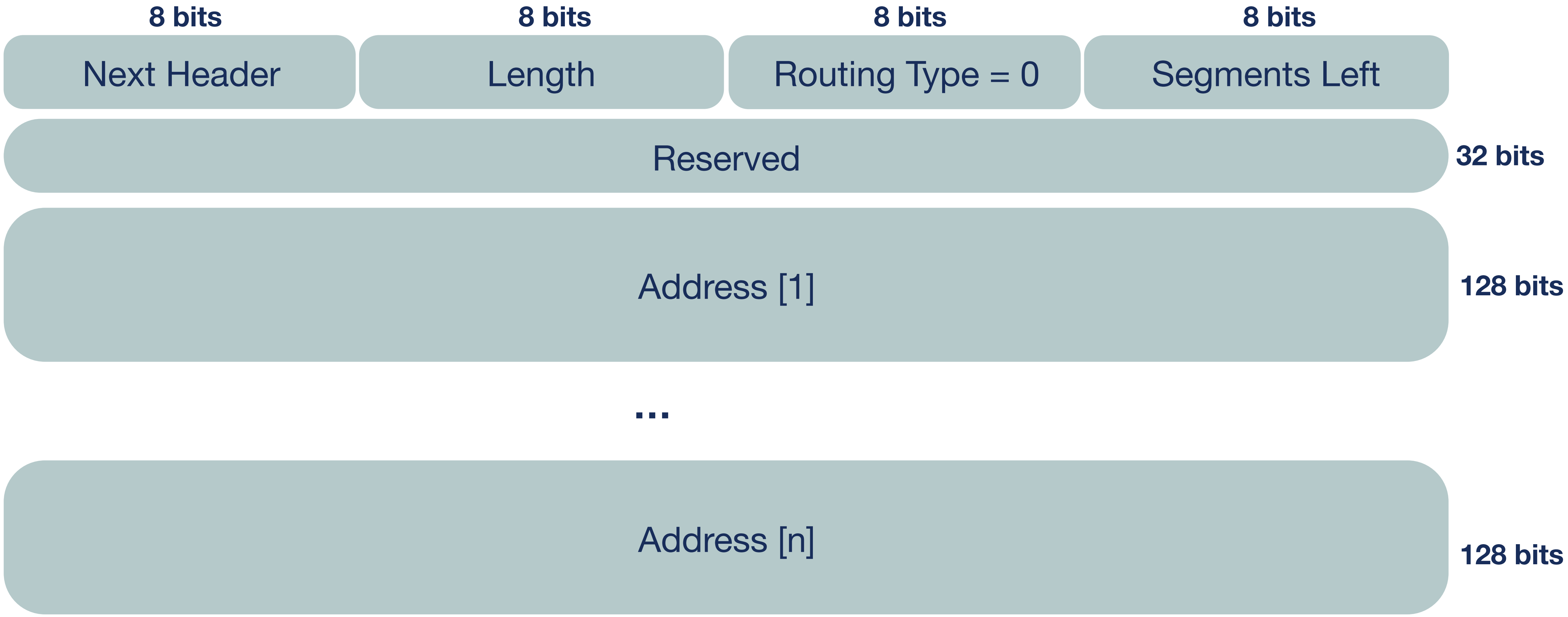
M Flag: 1 = more fragments to come; 0 = last fragment

IPv6 Extension Headers (7)

- Other next header values:
  - IPsec: ESP (50) and AH (51)
  - No Next Header (59)
  - Others: Mobility Header (135), HIP (139), and SHIM6 (140), Experimental (253, 254)
  - Upper layer: TCP (6), UDP (17), IPv6 (41), ICMPv6 (58)

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



8 bits | 8 bits | 8 bits | 8 bits

Next Header | Length | Routing Type = 0 | Segments Left

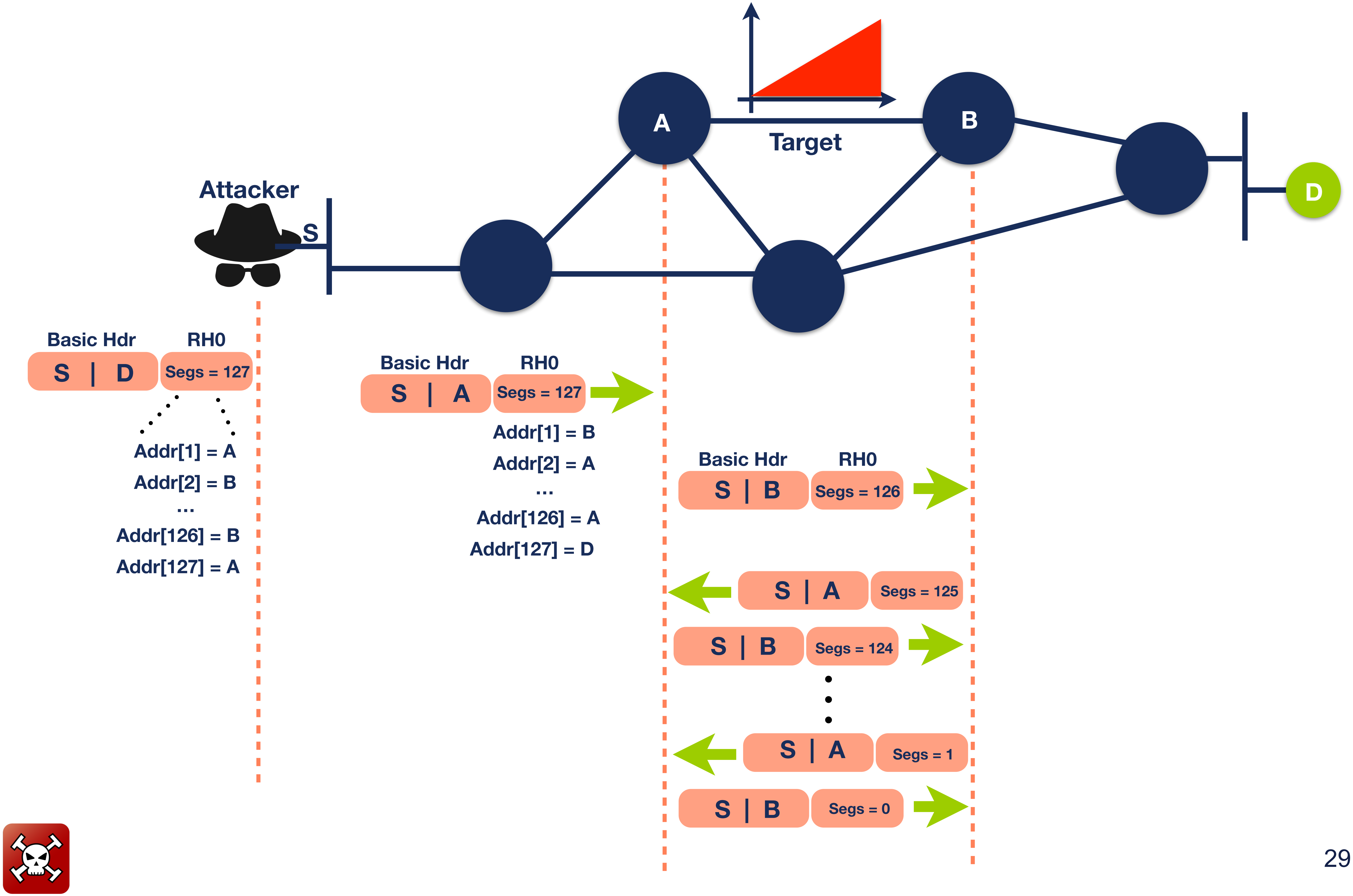
Reserved — 32 bits

Address [1] — 128 bits

...

Address [n] — 128 bits

Extension Headers Threats (2)



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

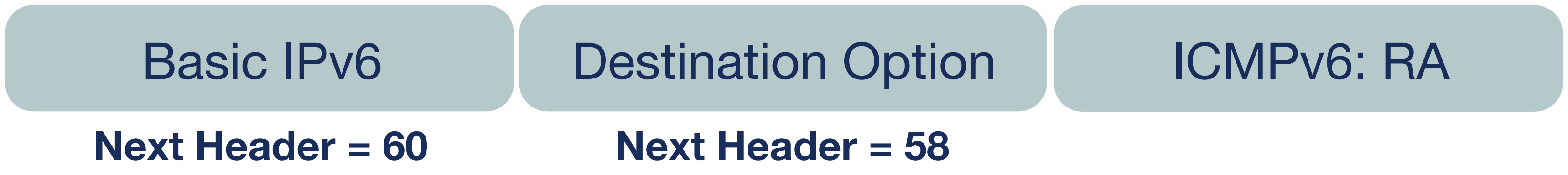
S | B | Segs = 124

S | A | Segs = 1

S | B | Segs = 0

Extension Headers Threats (3)

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

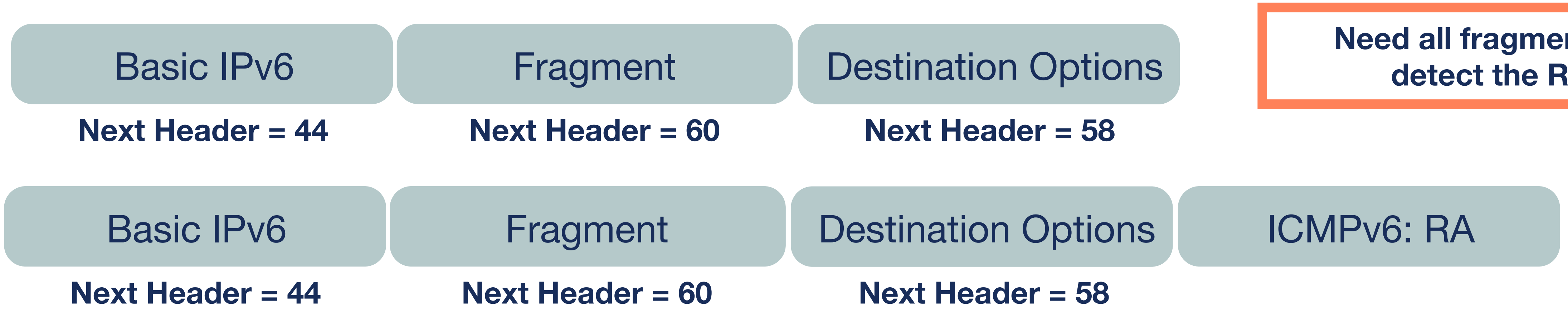


Basic IPv6 | Destination Option | ICMPv6: RA

Next Header = 60 | Next Header = 58

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

- Fragment EH



Basic IPv6 | Fragment | Destination Options

Next Header = 44 | Next Header = 60 | Next Header = 58

Basic IPv6 | Fragment | Destination Options | ICMPv6: RA

Next Header = 44 | Next Header = 60 | Next Header = 58

Need all fragments to detect the RA

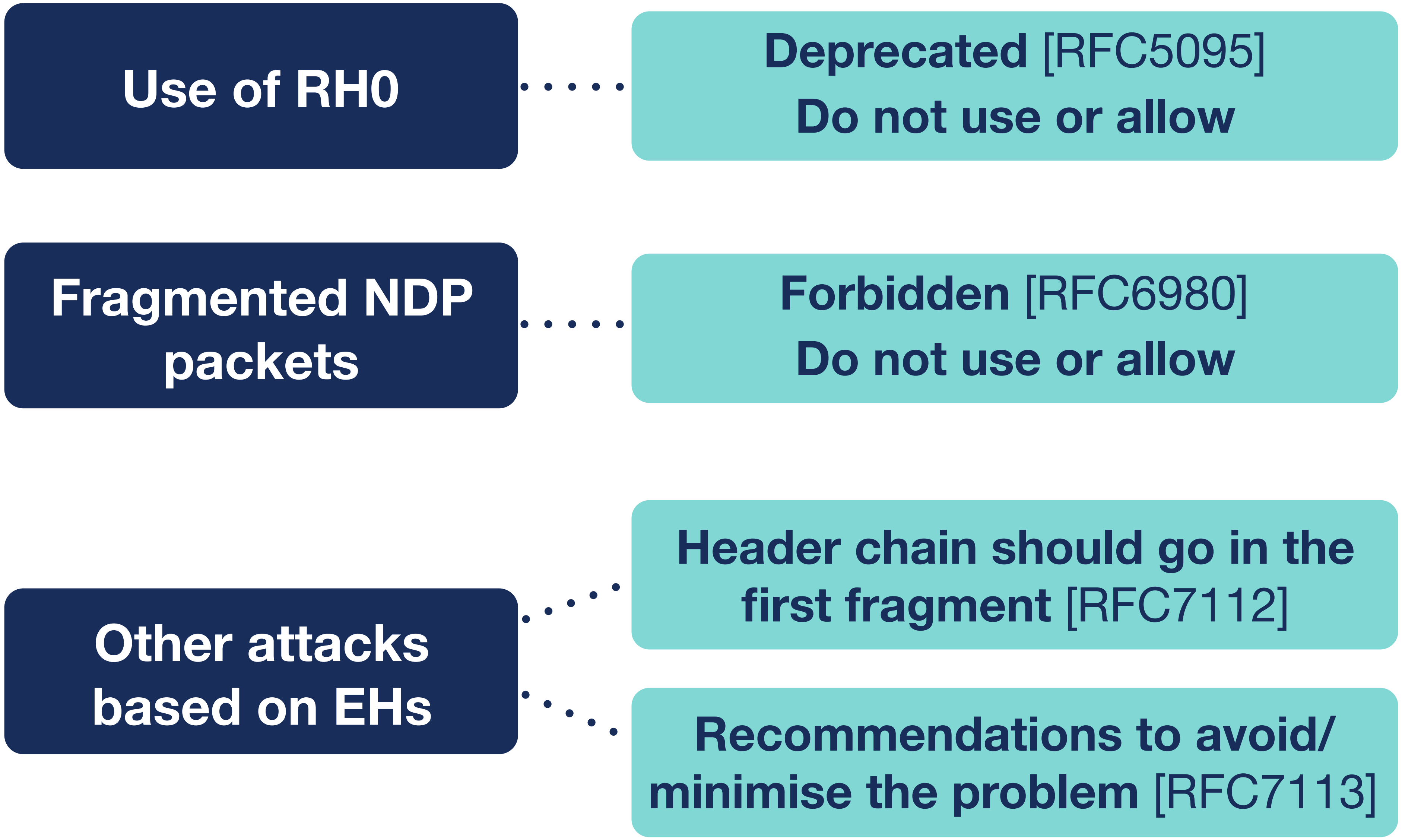
Extension Headers Threats: Fragmentation

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

Extension Headers 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]

Extension Headers Solutions



Use of RH0

Deprecated [RFC5095]
Do not use or allow

Fragmented NDP packets

Forbidden [RFC6980]
Do not use or allow

Other attacks based on EHs

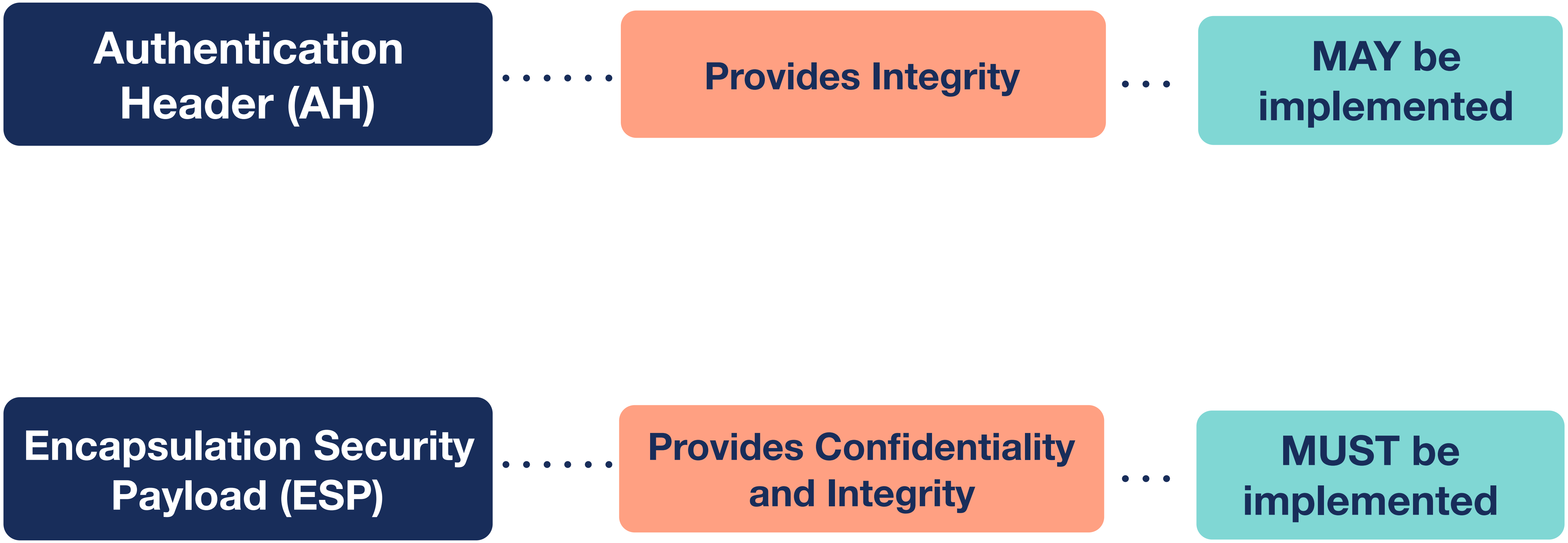
Header chain should go in the first fragment [RFC7112]

Recommendations to avoid/minimise the problem [RFC7113]

- Require security tools to inspect Header Chain properly

IPsec

- IPSec in IPv6 uses two Security Protocols (EHs):



Authentication Header (AH)

Provides Integrity

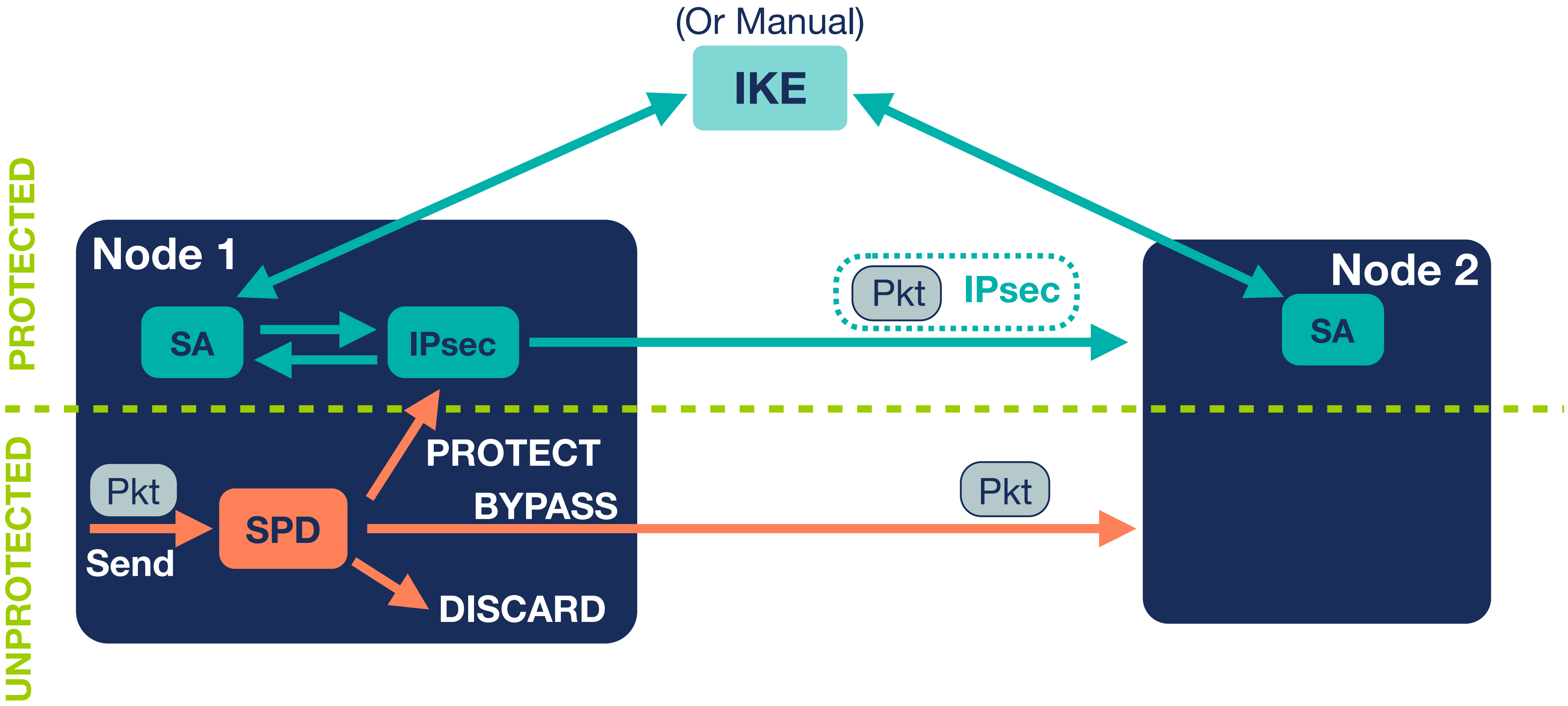
MAY be implemented

Encapsulation Security Payload (ESP)

Provides Confidentiality and Integrity

MUST be implemented

IPsec Explained



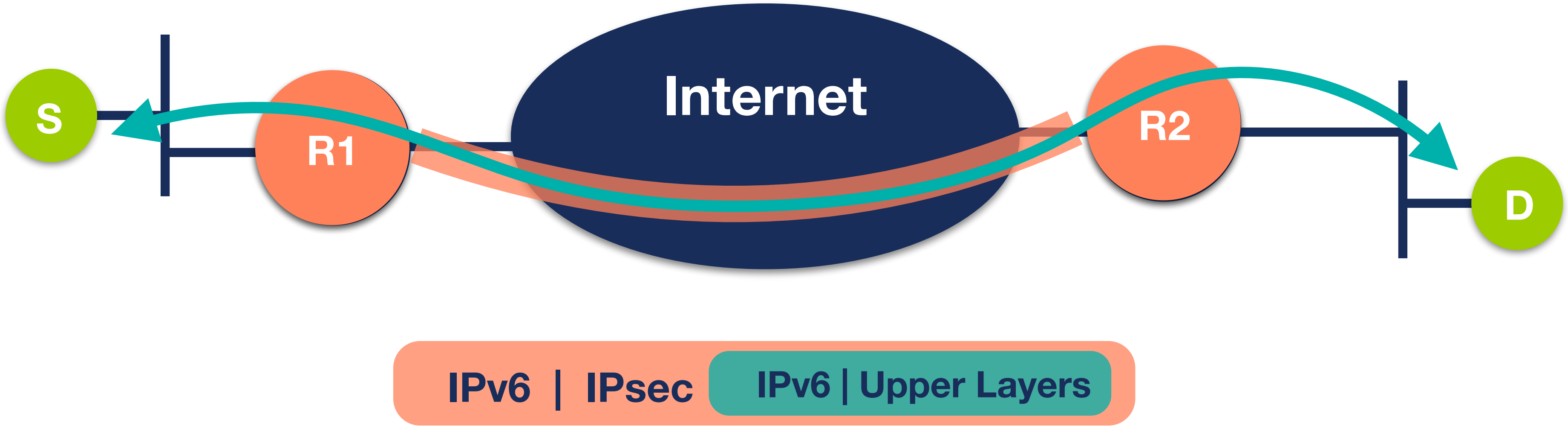
SPD Security Policy Database indicates what to do with packets

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

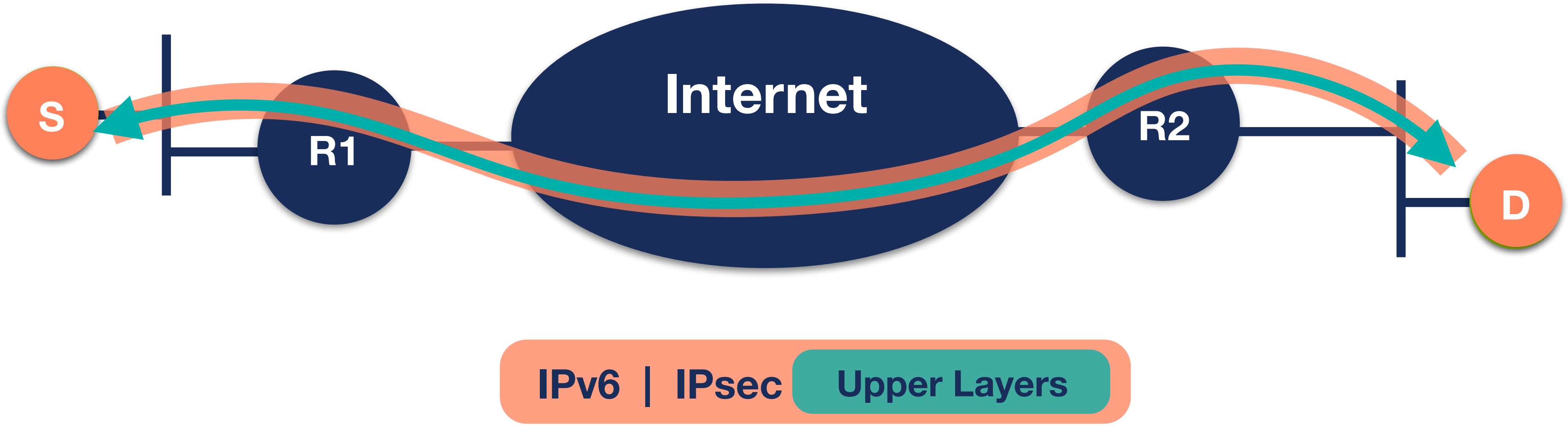
IKE Internet Key Exchange allows automatic creation of SAs

IPsec Modes

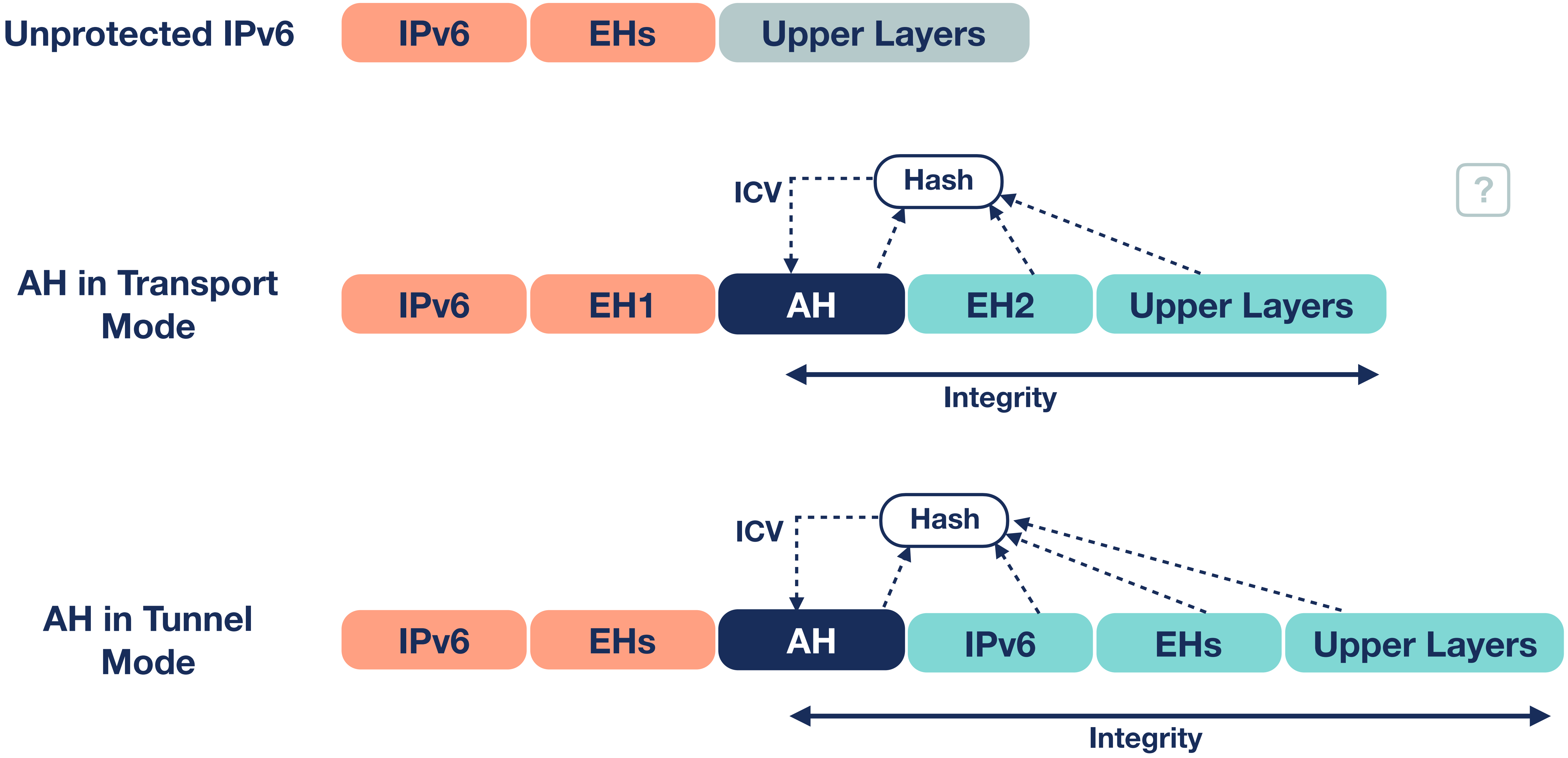
Tunnel Mode



Transport Mode



IPsec: Authentication Header



Unprotected IPv6

IPv6 | EHs | Upper Layers

AH in Transport Mode

ICV | Hash

IPv6 | EH1 | AH | EH2 | Upper Layers

Integrity

AH in Tunnel Mode

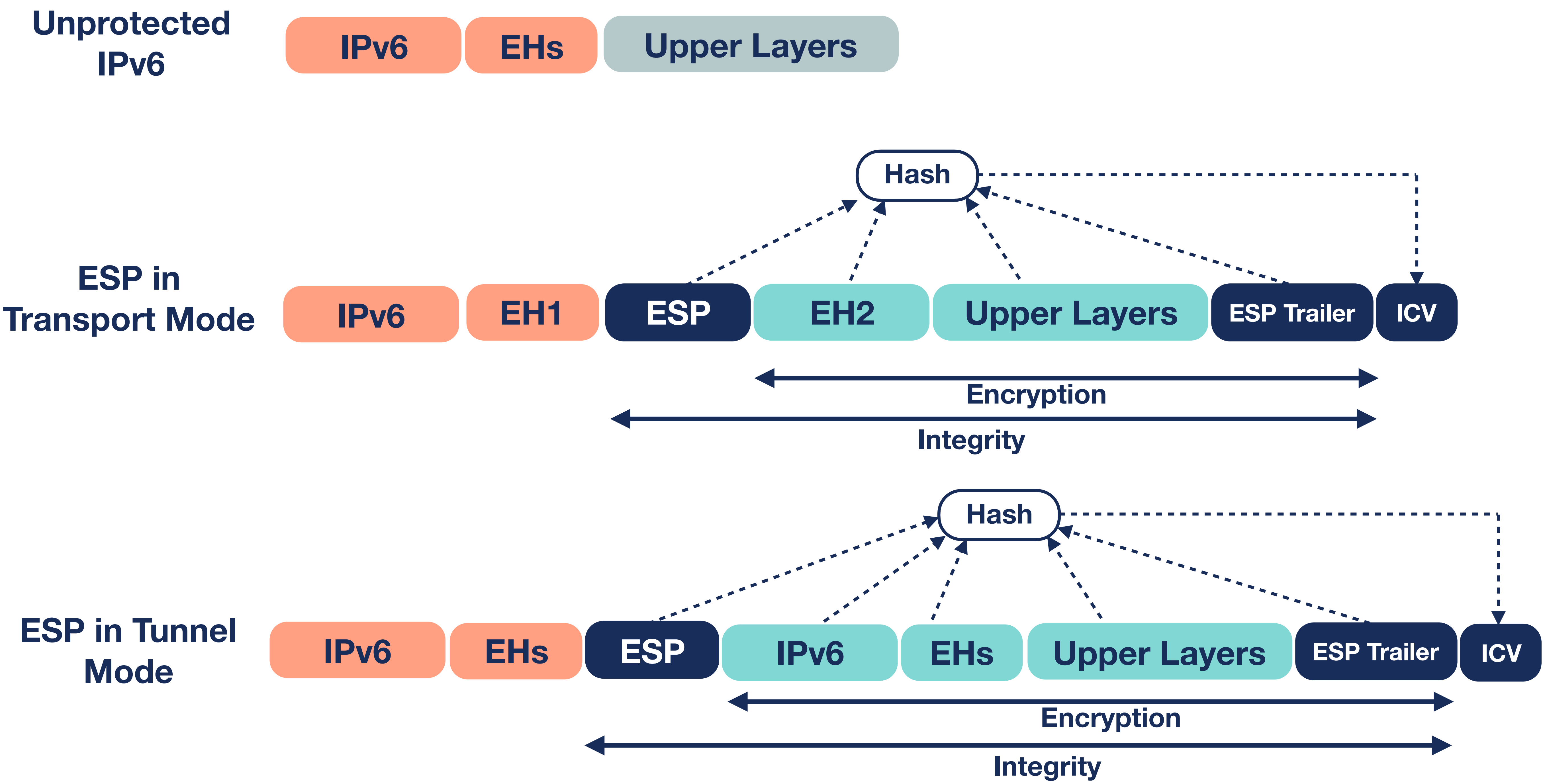
ICV | Hash

IPv6 | EHs | AH | IPv6 | EHs | Upper Layers

Integrity

EH1 = Hop-by-Hop, Routing, Fragmentation | EH2 = Destination Options

IPsec: ESP



EH1 = Hop-by-Hop, Routing, Fragmentation | EH2 = Destination Options

IPv6 Packet Generation

Exercise 2.1

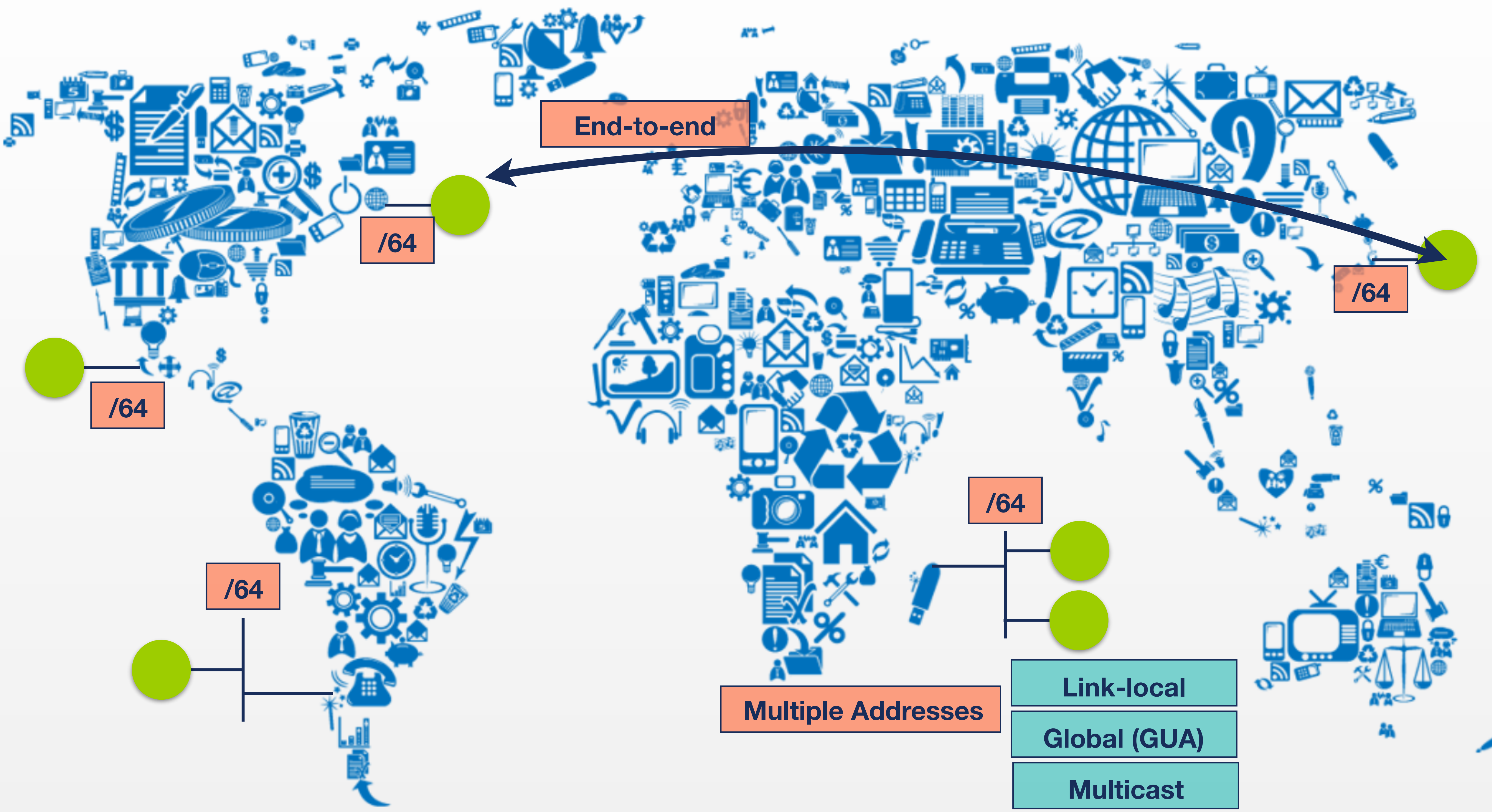
Exercise 2.1: IPv6 Packet Generation

- **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**: 20 minutes
- **Tasks**:
  - Login in the lab environment
  - Generate IPv6 packets following instructions in Exercise Booklet

IPv6 Addressing Architecture

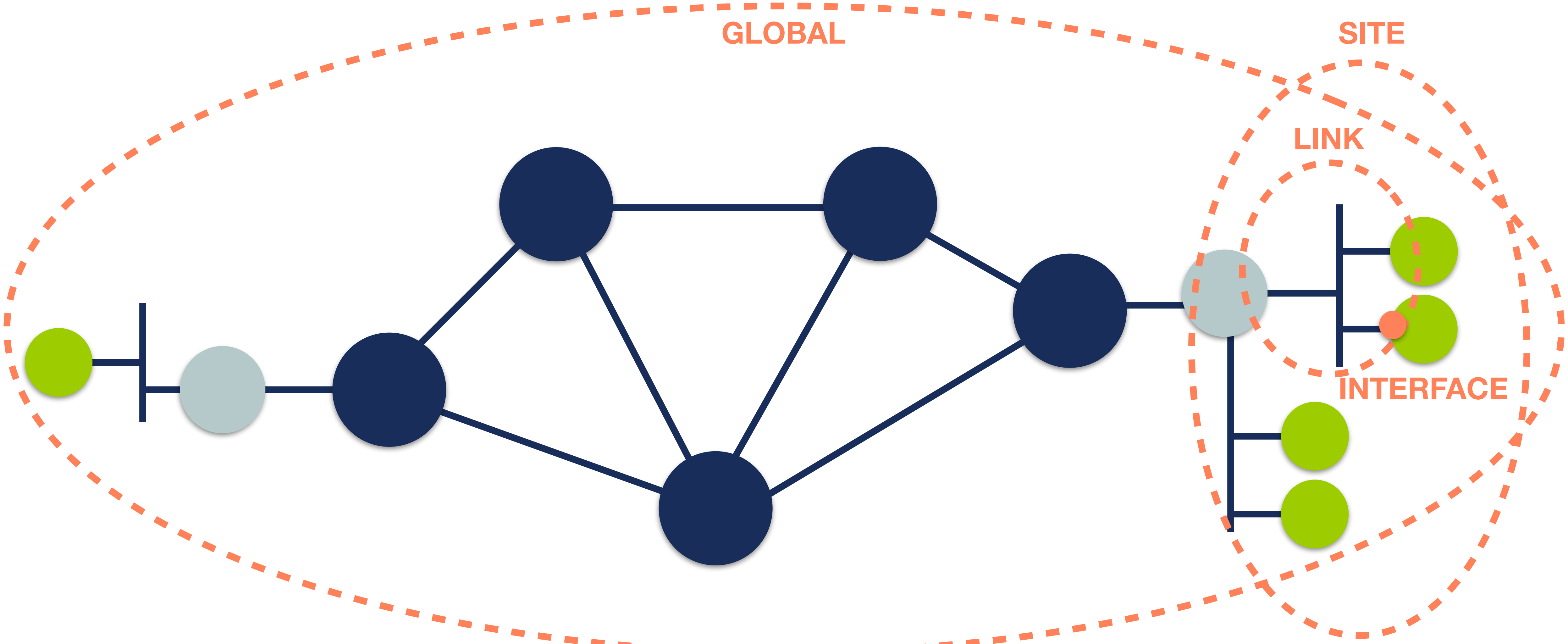
Section 2.2

Introduction



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

IPv6 Address Scope



fe80::A:b:100

ff01::2

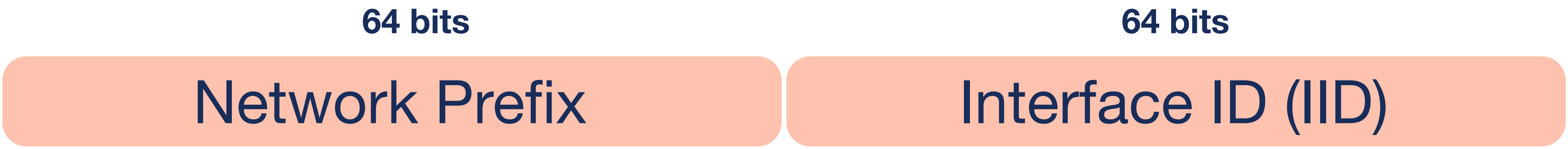
2001:67c:2e:1::c1

FD00:A:B::100

FF05::1:3

ff02::1

IPv6 Network Scanning (1)



64 bits

Network Prefix

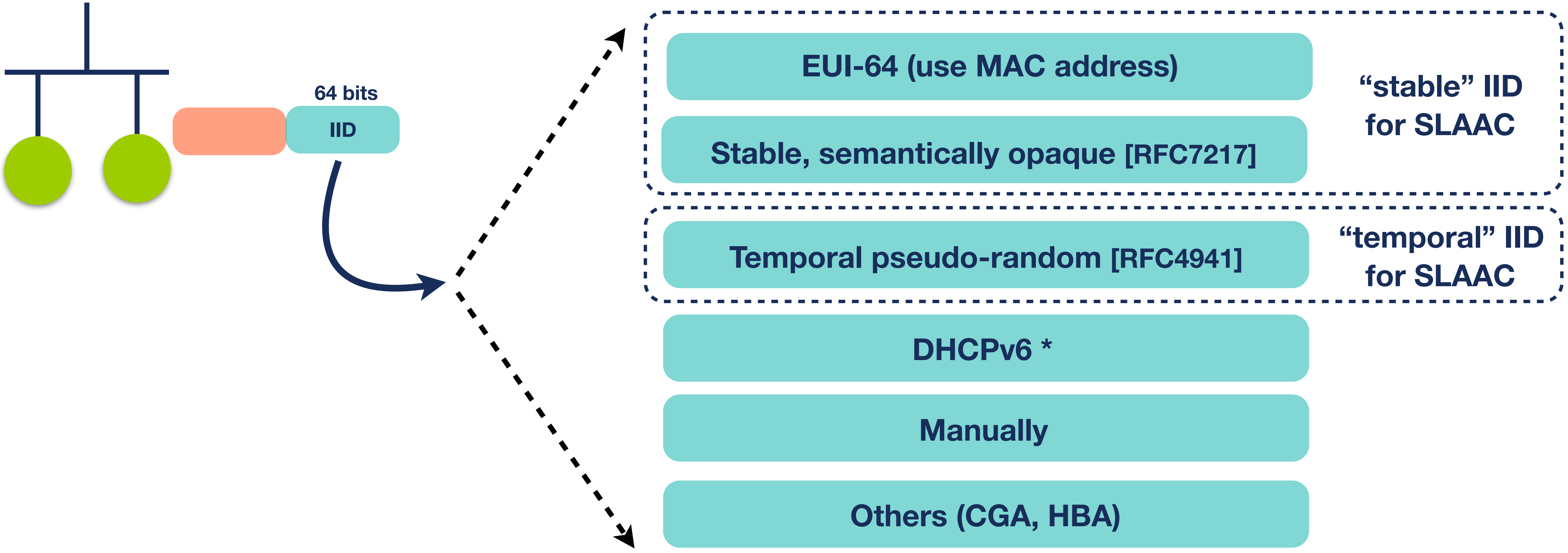
64 bits

Interface ID (IID)

- Network Prefix determination (64 bits)
  - Common patterns in addressing plans
  - DNS direct and reverse resolution
  - Traceroute

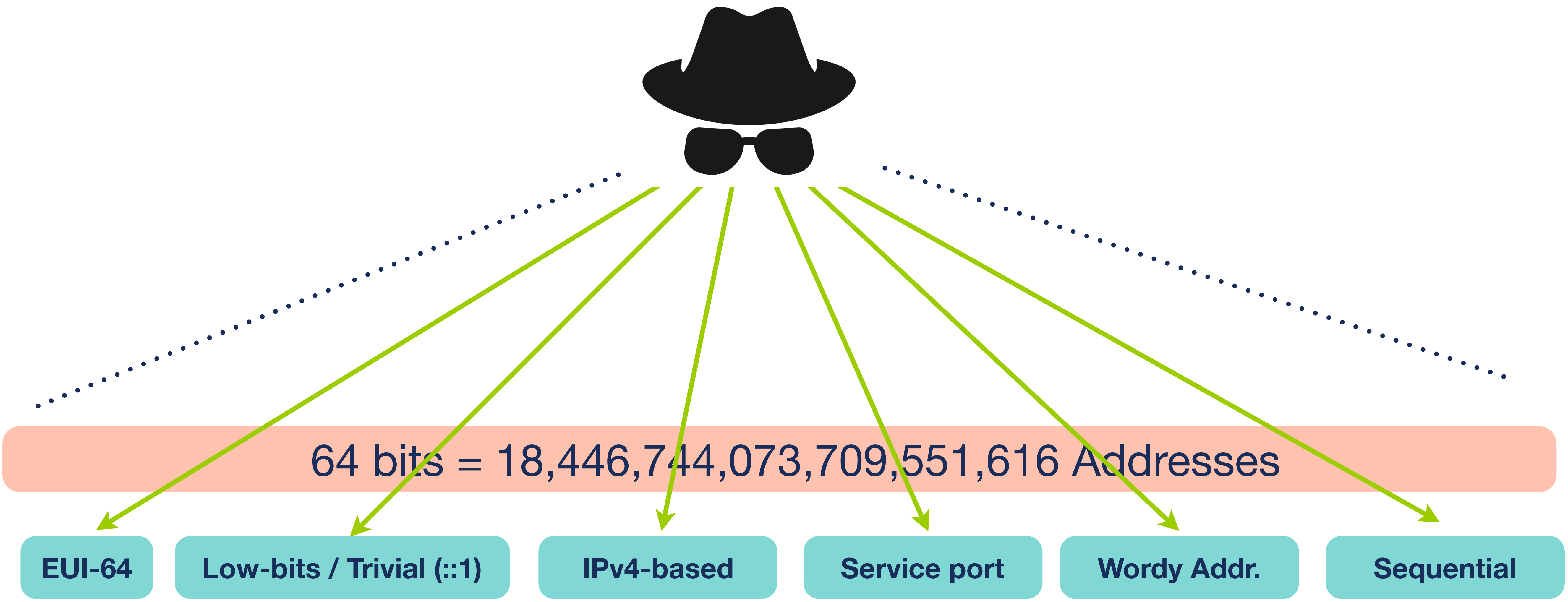
- IID determination (64 bits)
  - “brute force” no longer possible

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)



64 bits = 18,446,744,073,709,551,616 Addresses

EUI-64

Low-bits / Trivial (::1)

IPv4-based

Service port

Wordy Addr.

Sequential

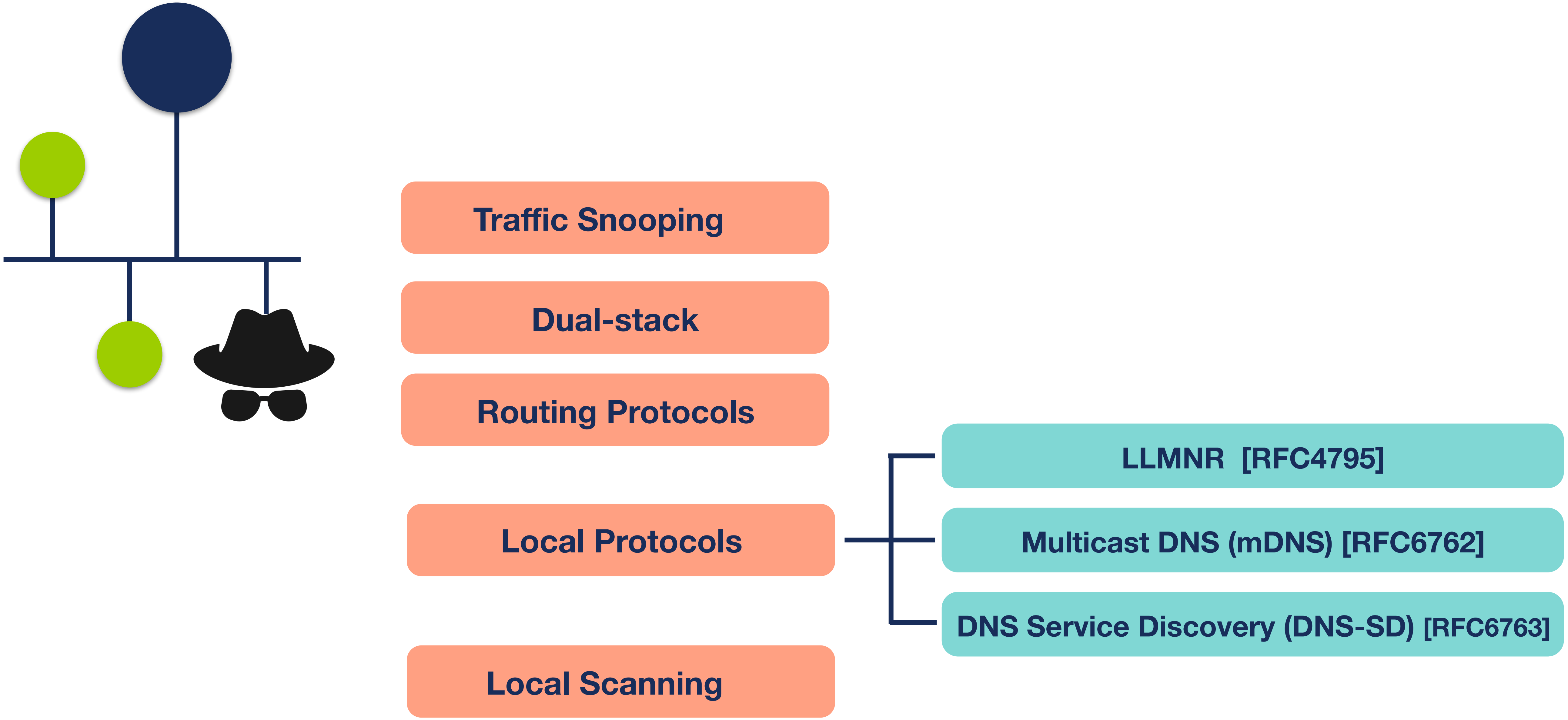
OUI: 24 bits
FFFE: 16 bits

2001:db8:1::10.0.0.5

2001:db8:1::80

2001:db8::bad:cafe

IPv6 Network Scanning (4)



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
IPv6-mapped	::ffff:0:0/96	Used by Transition mechanisms. 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
Benchmarking	2001:2::/48	

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

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
- 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**: 15 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

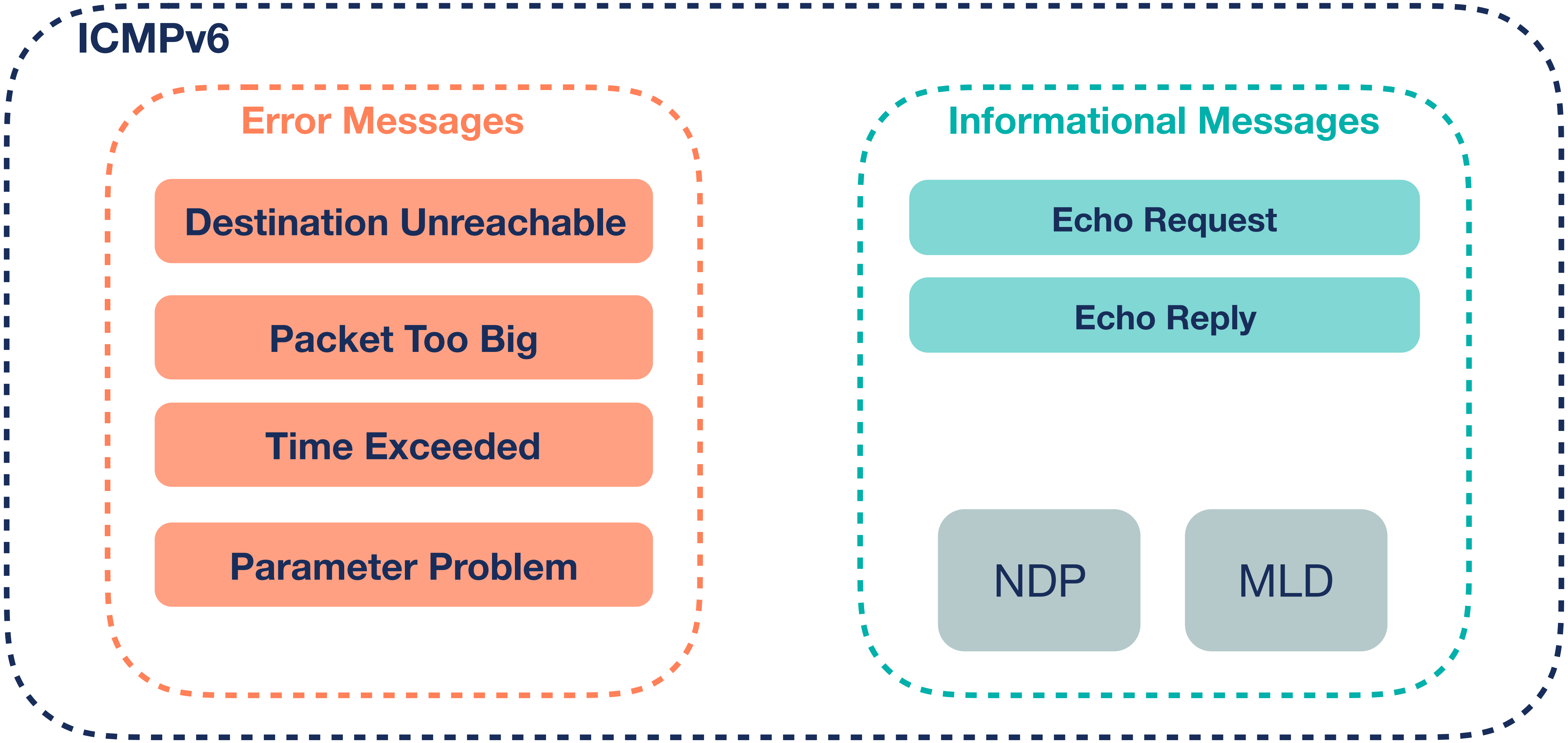
Section 3

ICMPv6

Section 3.1

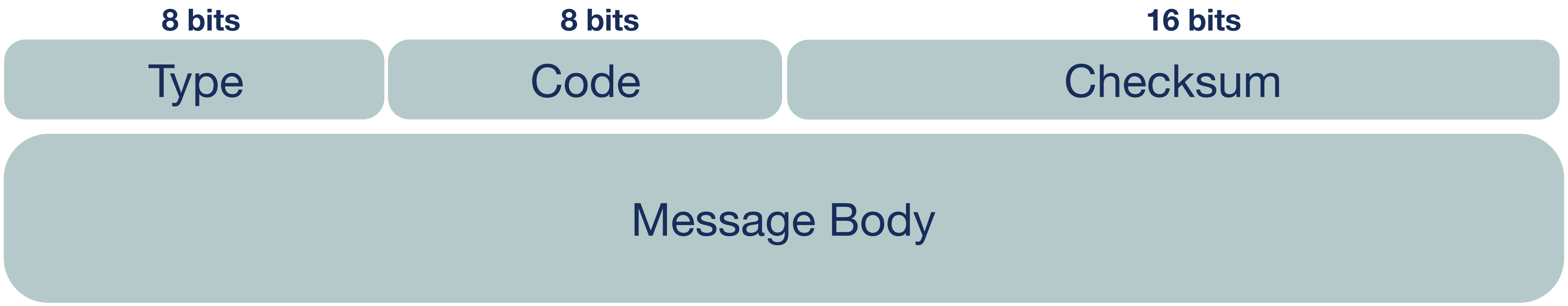
Introduction

- ICMPv6 [RFC4443] is an integral part of IPv6



ICMPv6 Format

- General Format



8 bits

8 bits

16 bits

Type

Code

Checksum

Message Body

- Extended Format [RFC4884]
  - Adds a length field
  - For Destination Unreachable, and Time Exceeded

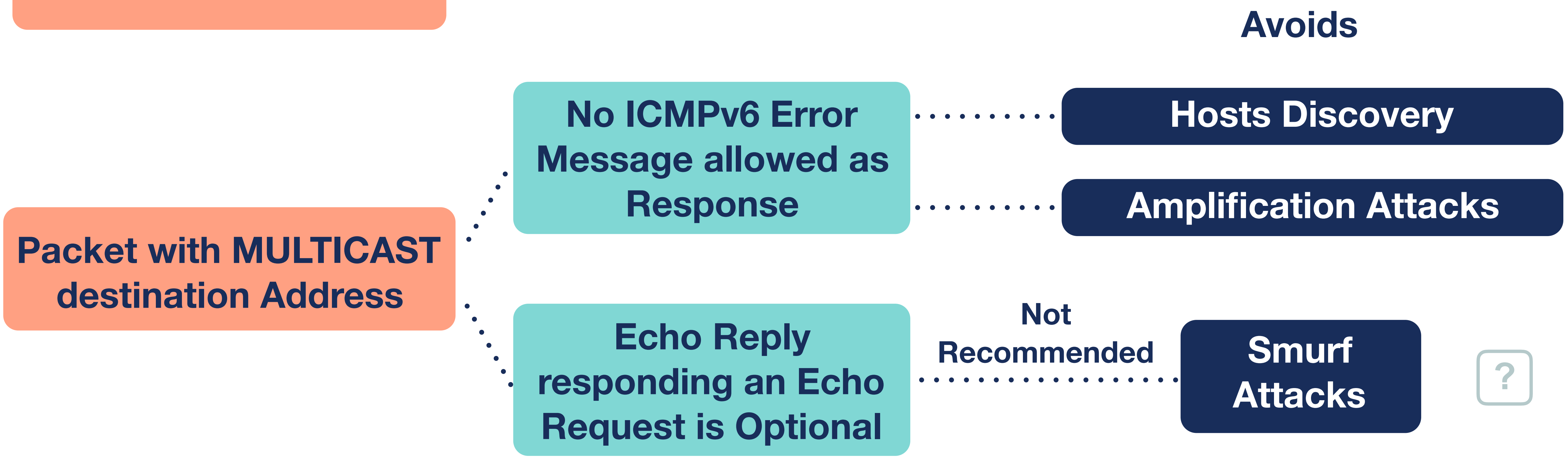
ICMPv6 Error Messages

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)

ICMPv6 security

- Security point of view:

FILTER CAREFULLY



Avoids

Packet with MULTICAST destination Address

No ICMPv6 Error Message allowed as Response

Hosts Discovery

Amplification Attacks

Echo Reply responding an Echo Request is Optional

Not Recommended

Smurf Attacks

?

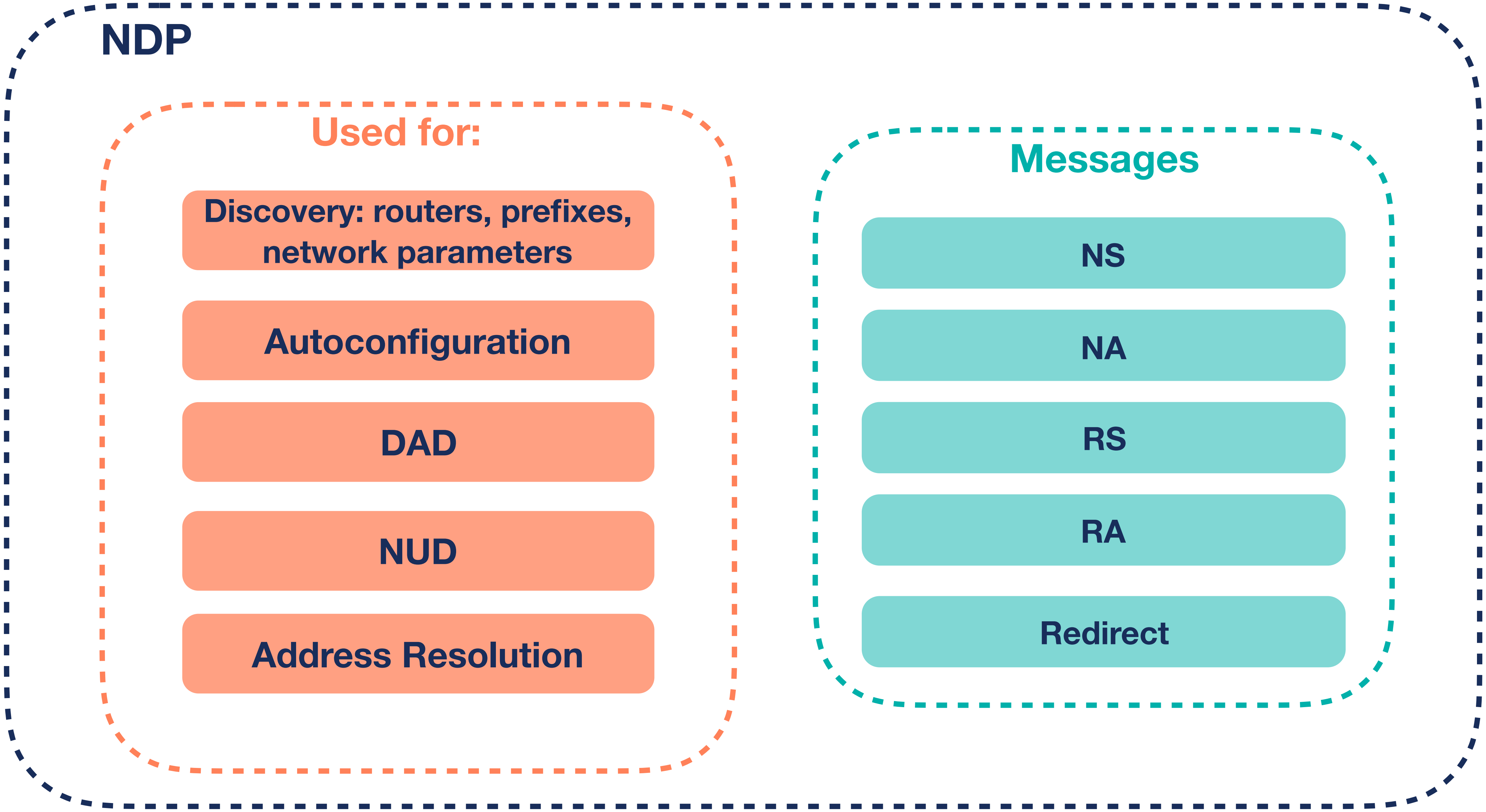
Used in many IPv6-related protocols

NDP

Section 3.2

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)

- **Neighbor Solicitation/Advertisement Spoofing**

- Can be done:

1. Sending NS with “source link-layer” option changed
2. Sending NA with “target link-layer” option changed
   - Can send unsolicited NA or as an answer to NS

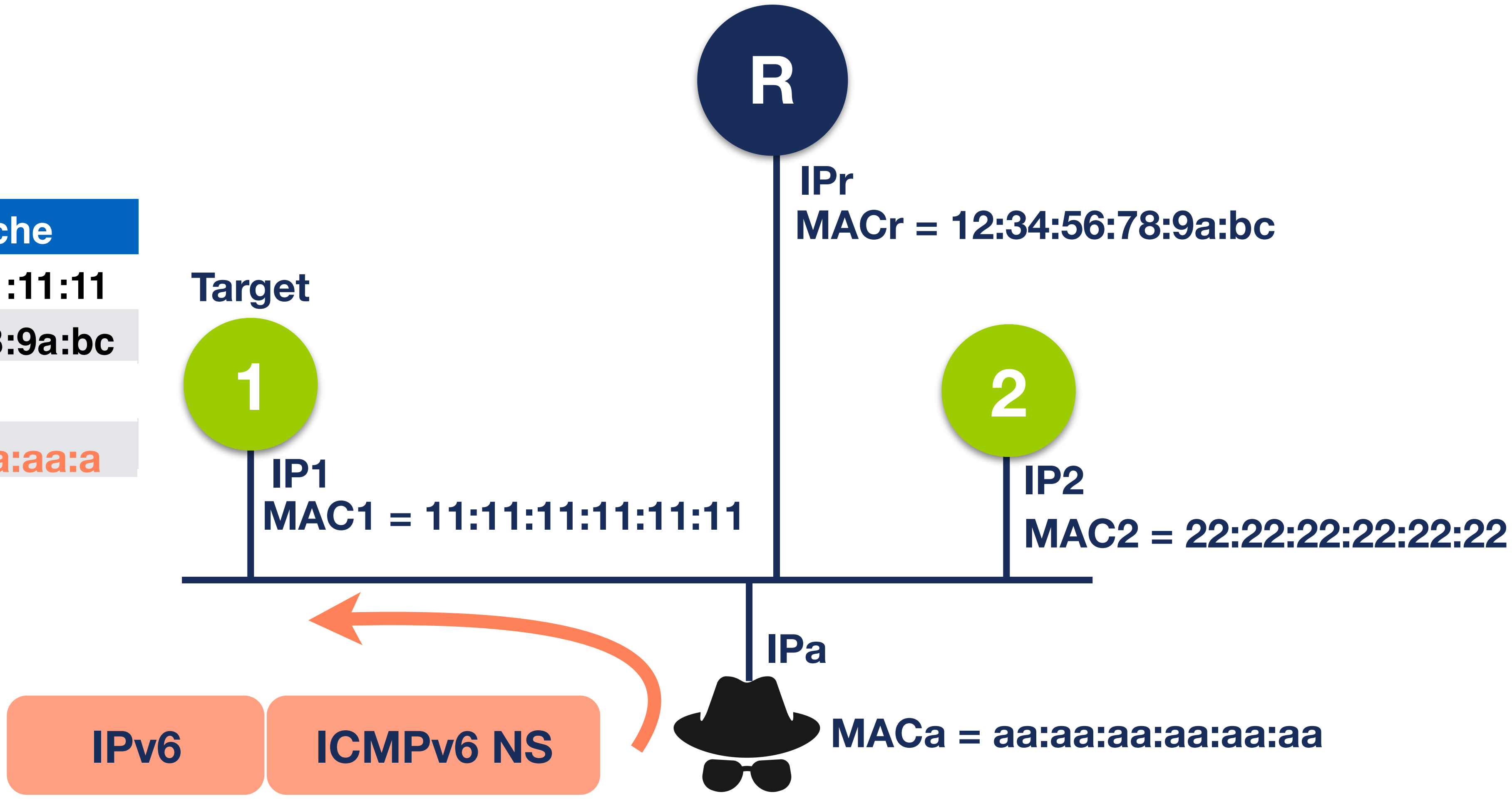
- This is a redirection/DoS attack
- Could be used for a “Man-In-The-Middle” attack

?

NDP Threats (2)

- NS: 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.Source IPv6: IP2

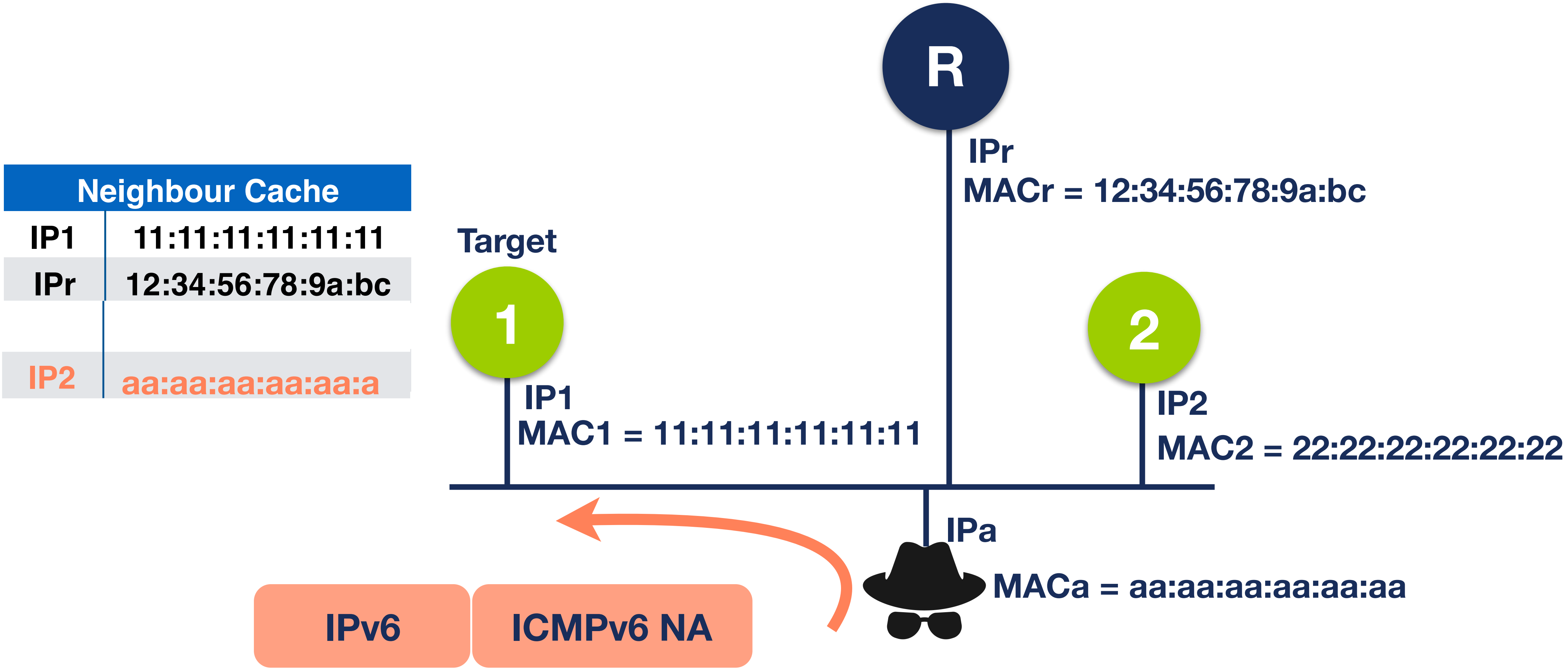
IPv6.Destination IPv6: IP1

NS.Target Addr: IP1

NS.Src Link-layer Addr: aa:aa:aa:aa:aa:aa

NDP Threats (3)

- 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:a

NA.Target Addr.: IP2

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

NDP Threats (4)

- **NUD Failure**
- A malicious node keeps sending fake NAs in response to NUD NS messages
- DoS Attack

NDP Threats (5)

- **DAD DoS Attack**
- Attacking node responds all DAD attempts made by a host. Two options:

1. **Sending NS**: simulating it’s trying DAD with the same address
2. **Sending NA**: simulating it’s using the same address

- Result: host can’t configure the address

NDP

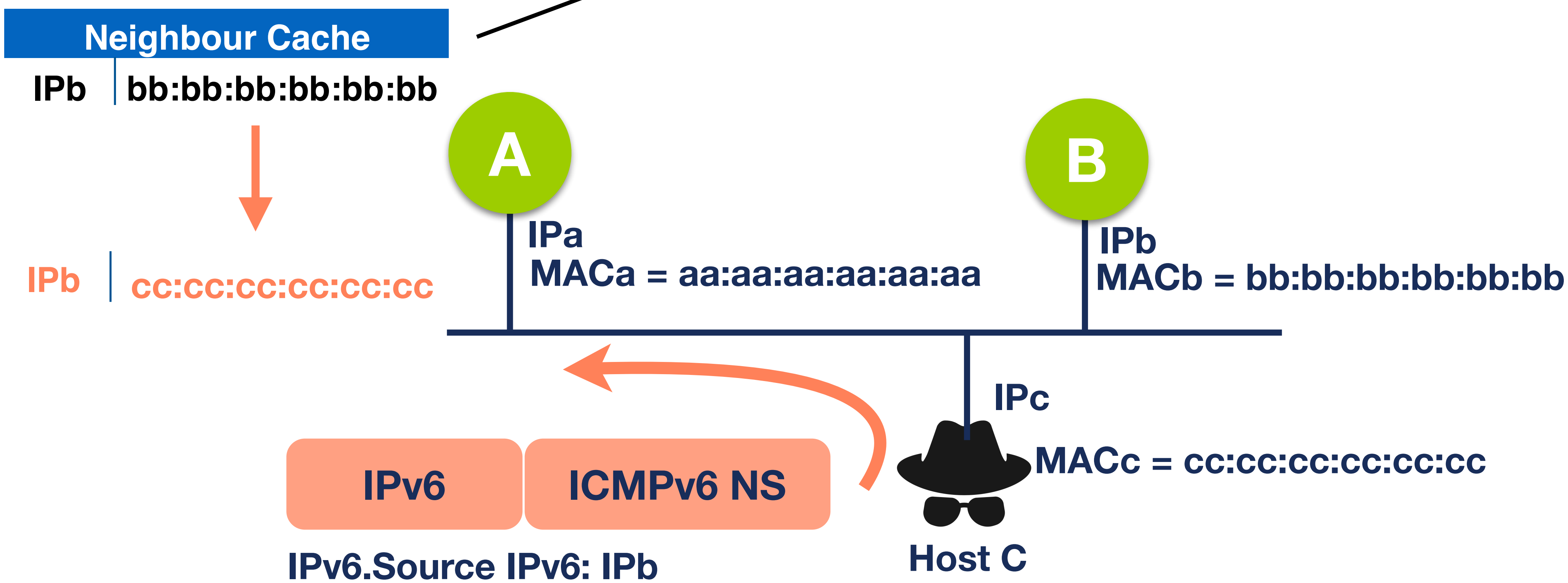
Exercise 3.2-a

Exercise 3.2-a NDP

- **Description**: Create packets to poison neighbour cache
- **Goals**:
  - Practice with Scapy tool
  - Learn how to modify the neighbour 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 neighbour cache
  - Generate NA packets that change other host's neighbour cache

3.2-a: Neighbour cache attack using NS

```
# ip neighbour show
```



Neighbour Cache

IPb	bb:bb:bb:bb:bb:bb
IPb	cc:cc:cc:cc:cc:cc

A

IPa
MACa = aa:aa:aa:aa:aa:aa

B

IPb
MACb = bb:bb:bb:bb:bb:bb

IPc
MACc = cc:cc:cc:cc:cc:cc

Host C

IPv6 | ICMPv6 NS

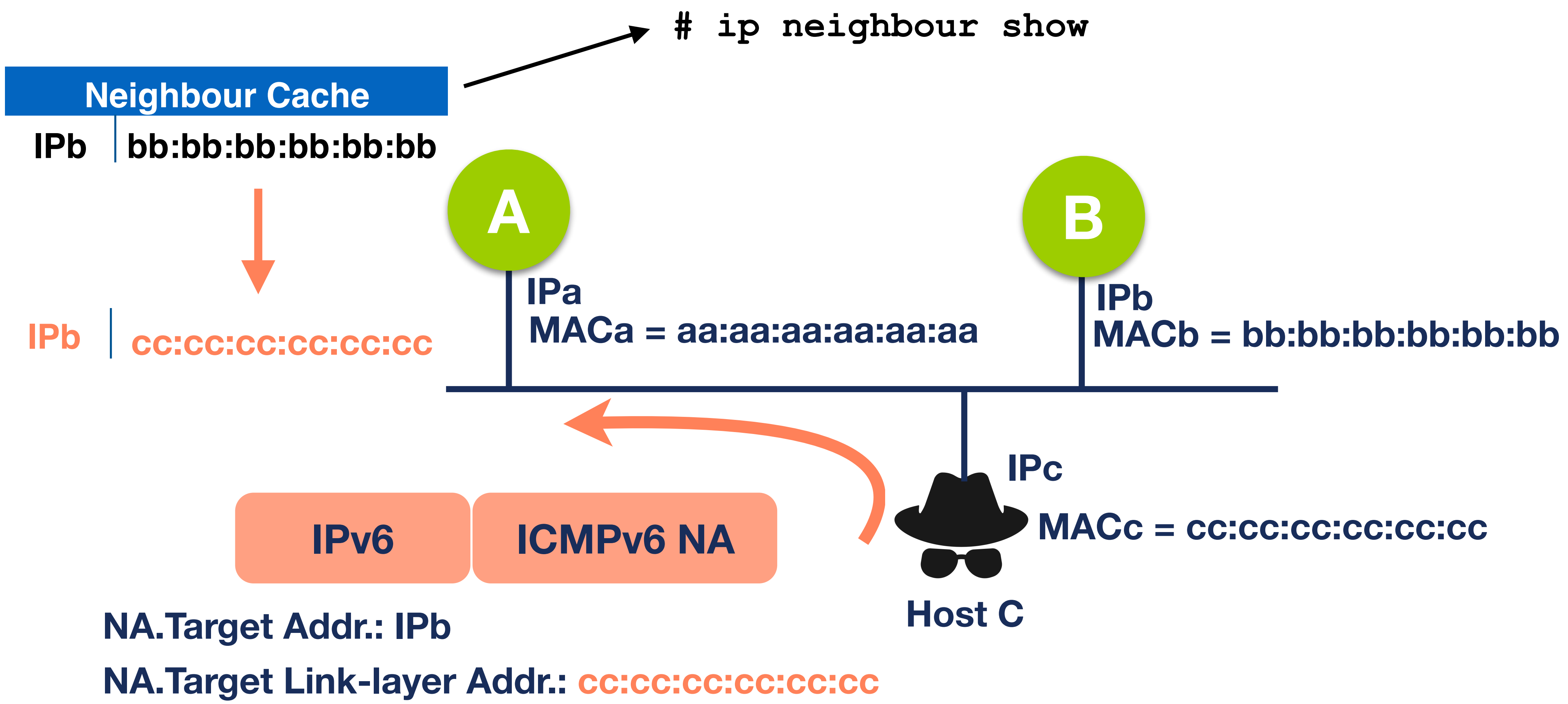
IPv6.Source IPv6: IPb

IPv6.Destination IPv6: IPa

NS.Target Addr: IPa

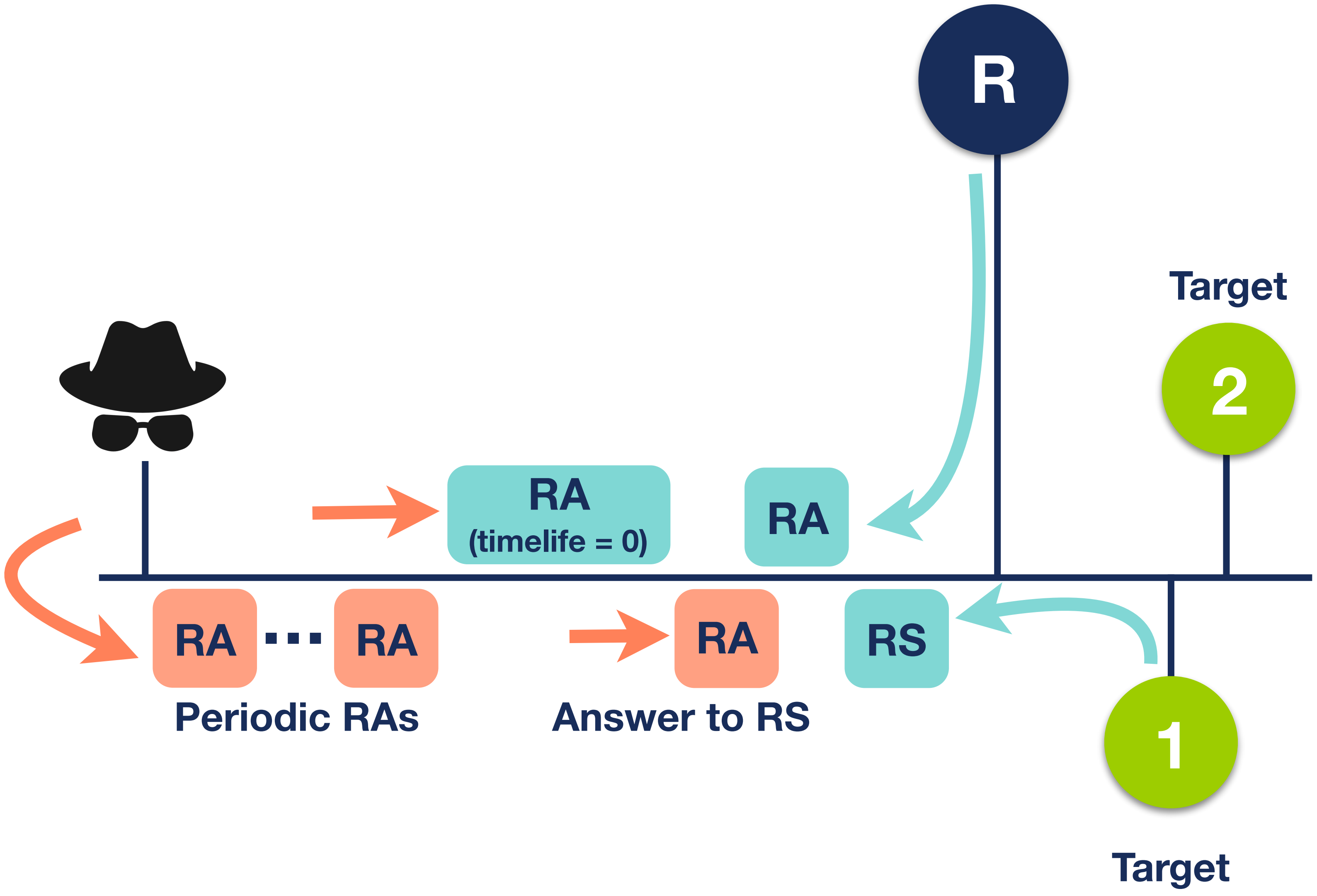
NS.Src Link-layer Addr: cc:cc:cc:cc:cc:cc

3.2-a: Neighbour cache attack using NA



NDP Threats (6)

- Malicious Last Hop Router



NDP Threats (7)

- **Bogus On-Link Prefix**
- Attacker sends RA with on-link prefix
- Hosts sending packets to addresses on that prefix don't use a gateway
- DoS attack
  - Can be extended to redirection / MITM

NDP Threats (8)

- **Bogus Address Configuration Prefix**
- Attacker sends RA with prefix for SLAAC
- Hosts using SLAAC will autoconfigure an address using that prefix
- Return packets never reach the host
- DoS attack

NDP Threats (9)

- **Parameter Spoofing**

- Attacker replicates valid RAs but with changed parameters
- Examples:

1. Current Hop Limit: small value
2. M/O flags set to one (stateful). Pretend DHCPv6

- DoS attack

NDP Threats (10)

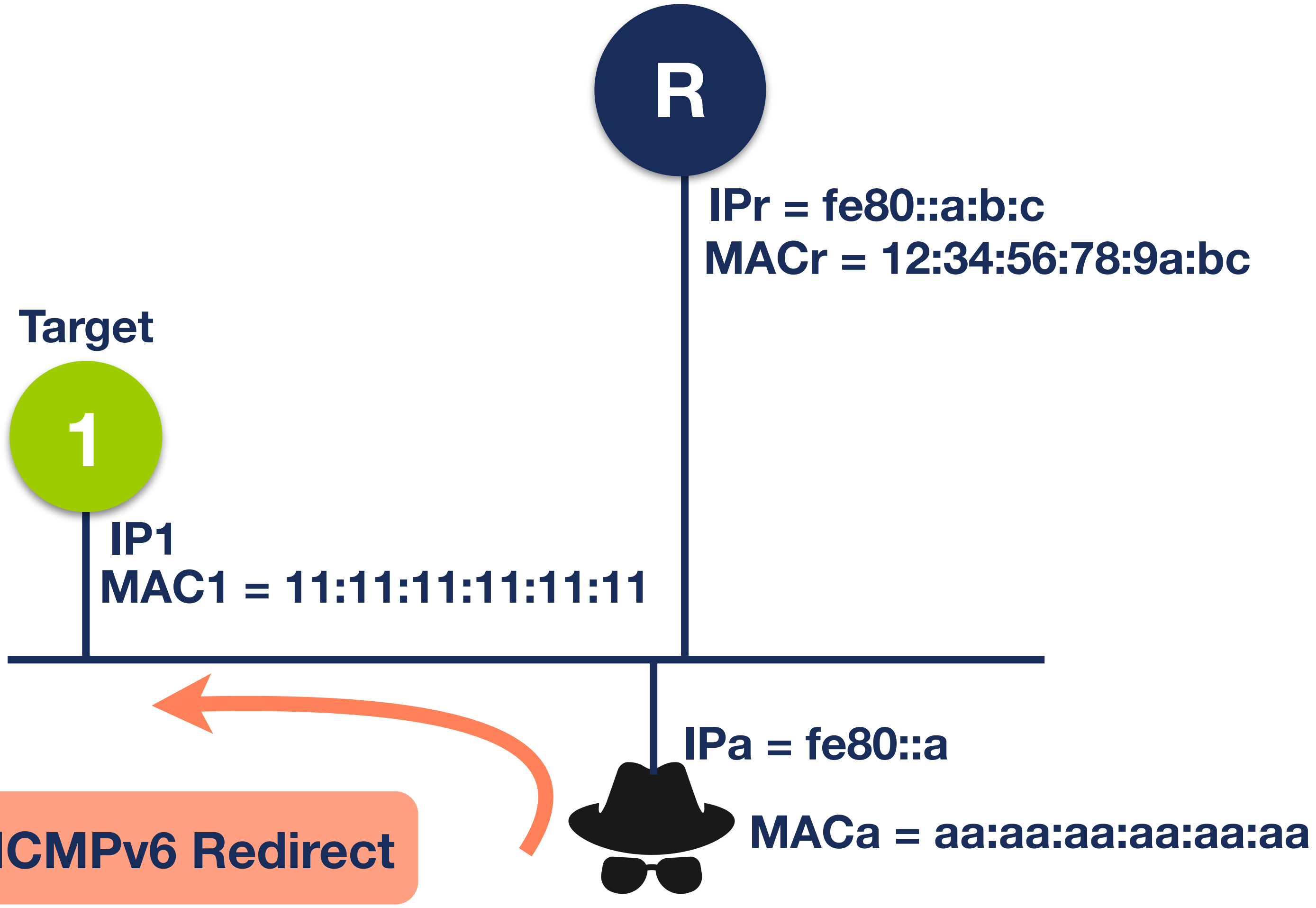
- Spoofed Redirect Message

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: IPr = fe80::a:b:c

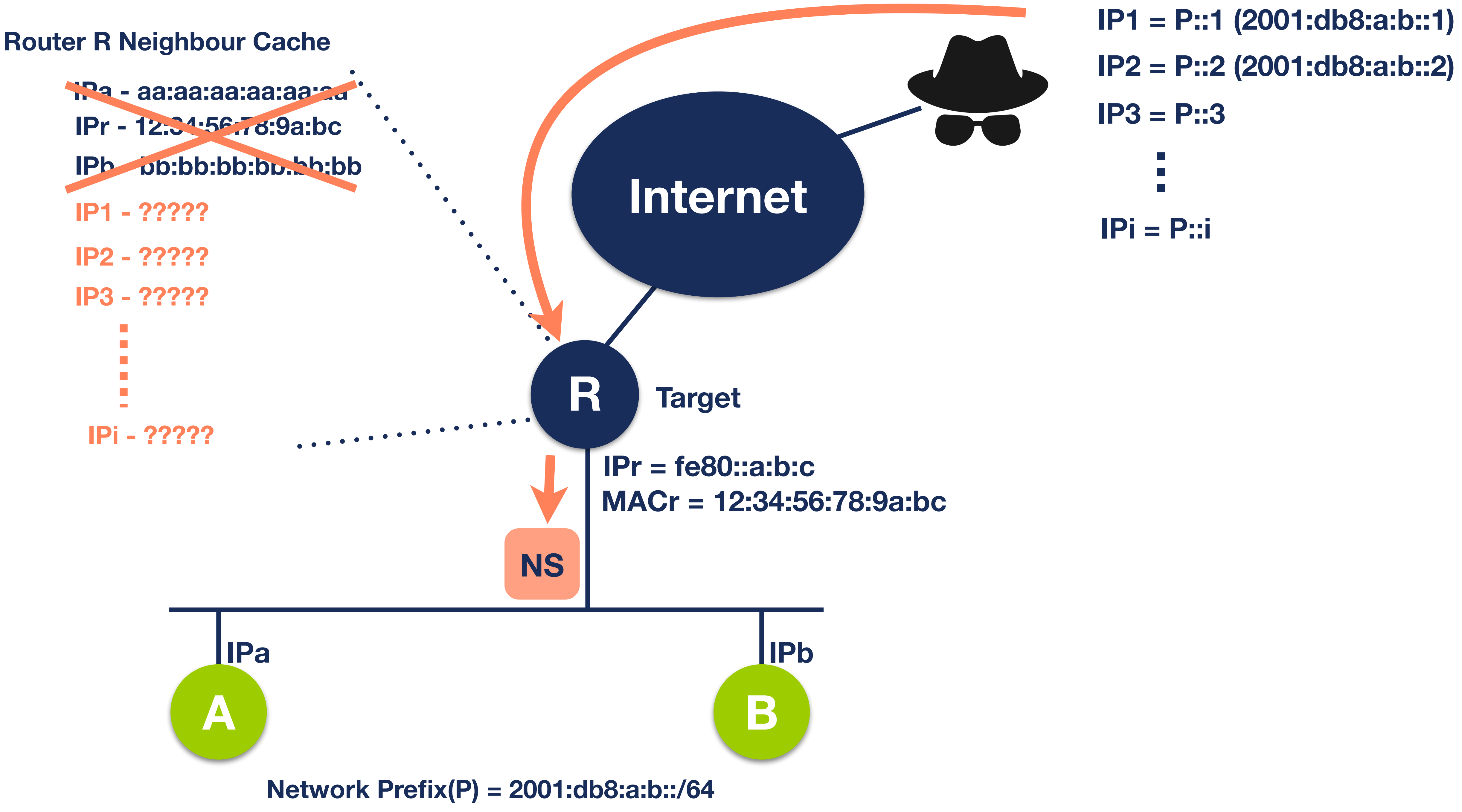
IPv6.Destination: IP1

Redirect.Target Addr.: IPa = fe80::a

Redirect.Dst Addr.: 2001:db8::face:b00c

NDP Threats (11)

- Neighbour Discovery DoS Attack


Router R Neighbour Cache
~~IPa - aa:aa:aa:aa:aa:aa~~
~~IPr - 12:34:56:78:9a:bc~~
~~IPb - bb:bb:bb:bb:bb:bb~~
IP1 - ?????
IP2 - ?????
IP3 - ?????
IPi - ?????
IP1 = P::1 (2001:db8:a:b::1)
IP2 = P::2 (2001:db8:a:b::2)
IP3 = P::3
IPi = P::i
Internet
R
Target
IPr = fe80::a:b:c
MACr = 12:34:56:78:9a:bc
NS
IPa
IPb
A
B
Network Prefix(P) = 2001:db8:a:b::/64

NDP

Exercise 3.2-b

Exercise 3.2-b NDP

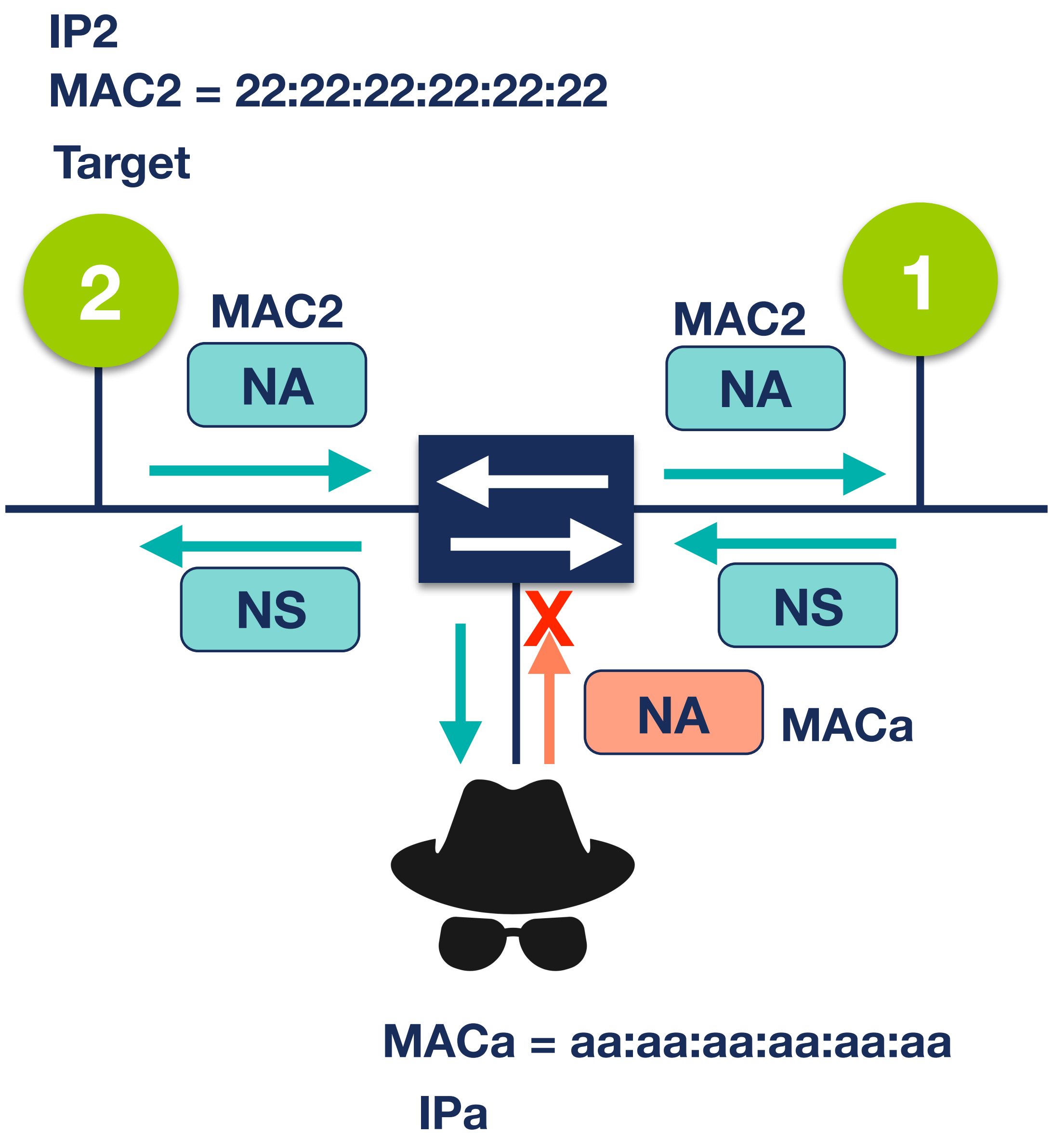
- **Description**: Send RA messages to perform attacks
- **Goals**:
  - Practice with Scapy tool
  - Use RA messages to perform attacks on a link
- **Time:** 20 minutes
- **Tasks**:
  - Send RA messages with bogus address configuration prefix

First Hop Security (1)

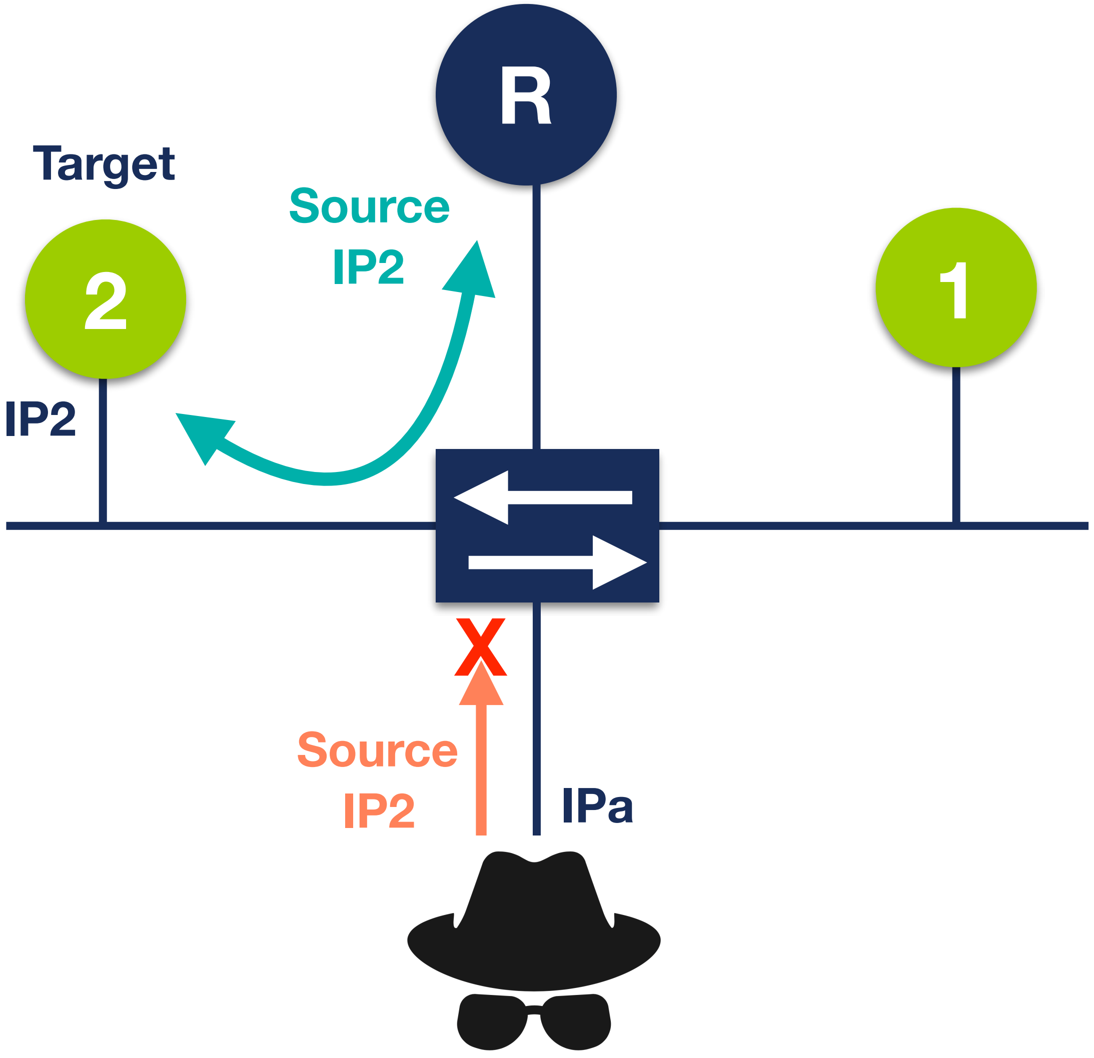
- Security implemented on switches

- 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)

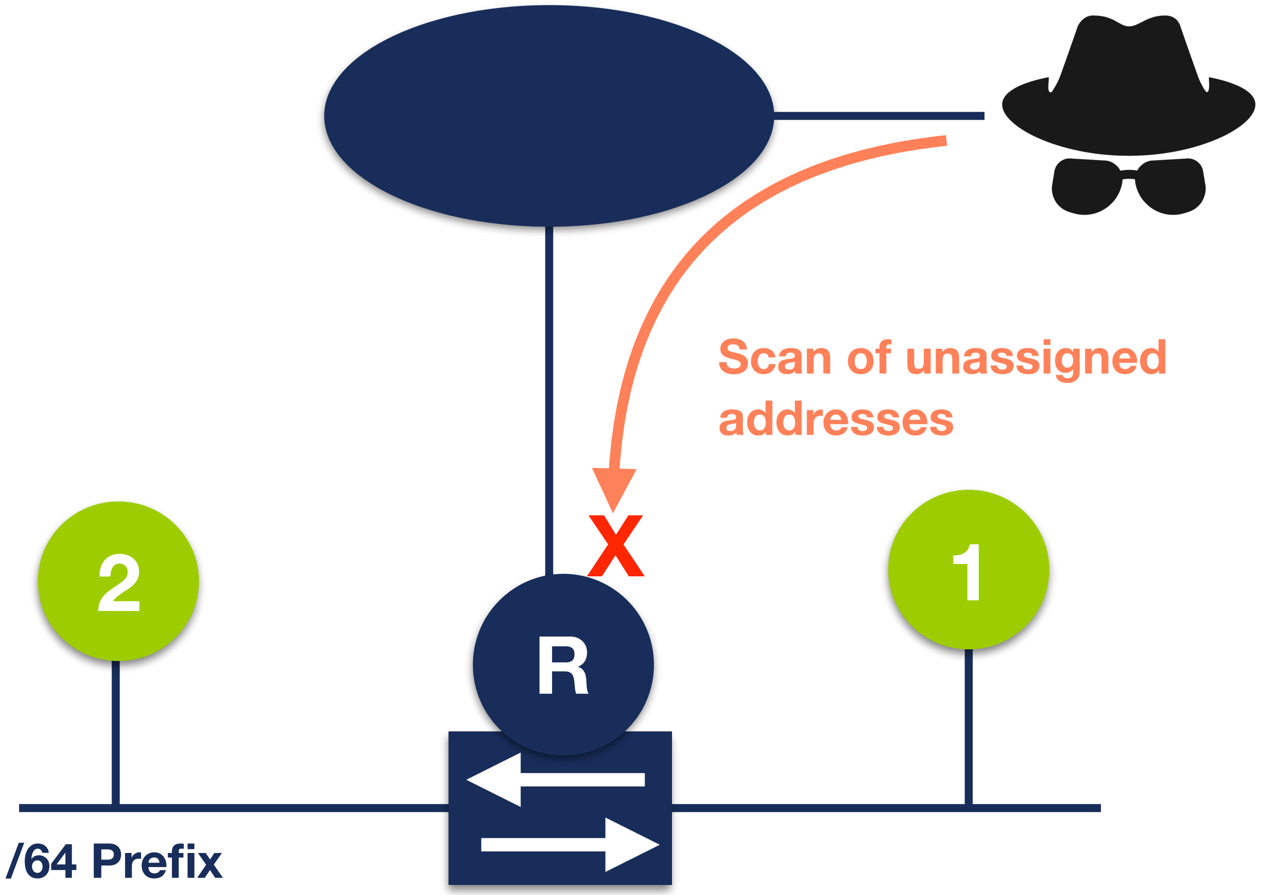


IPv6 Snooping



IPv6 Source/ Prefix Guard

First Hop Security (3)



IPv6 Destination Guard

Rogue RA Solutions

- Rogue RA could be a big problem
- How to protect:

Manual Configuration
+
Disable autoconfig

ACLs on switches

RA Snooping on switches
(RA-GUARD)

SEND

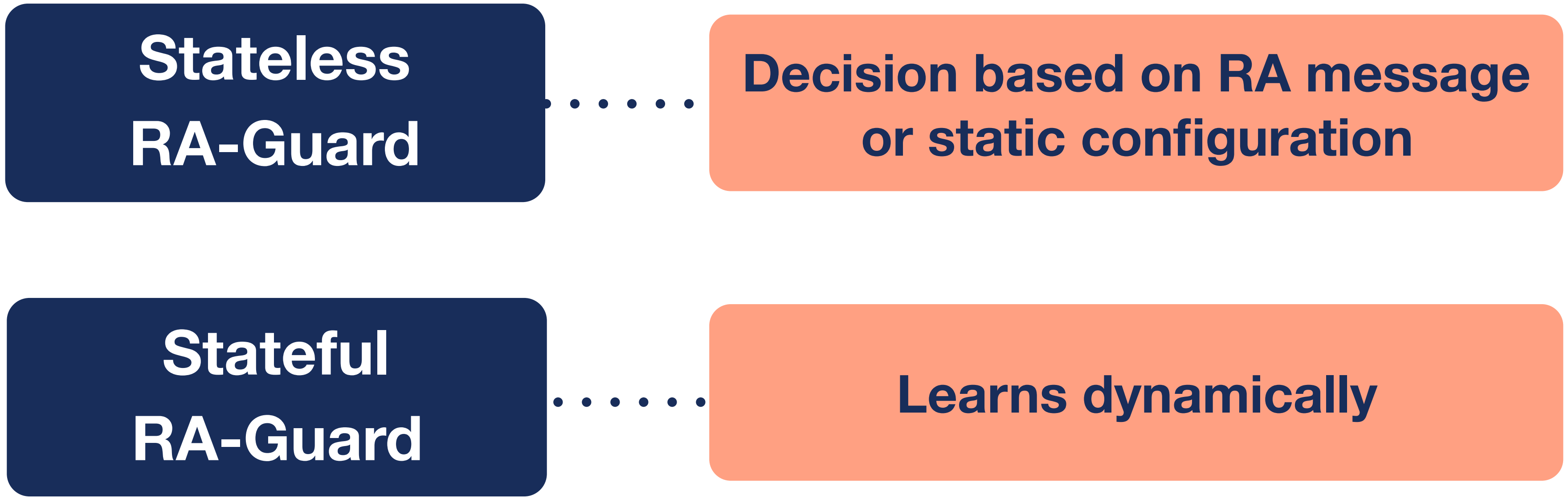
Router Preference
Option [RFC4191]

Host packet filtering

Link Monitoring

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

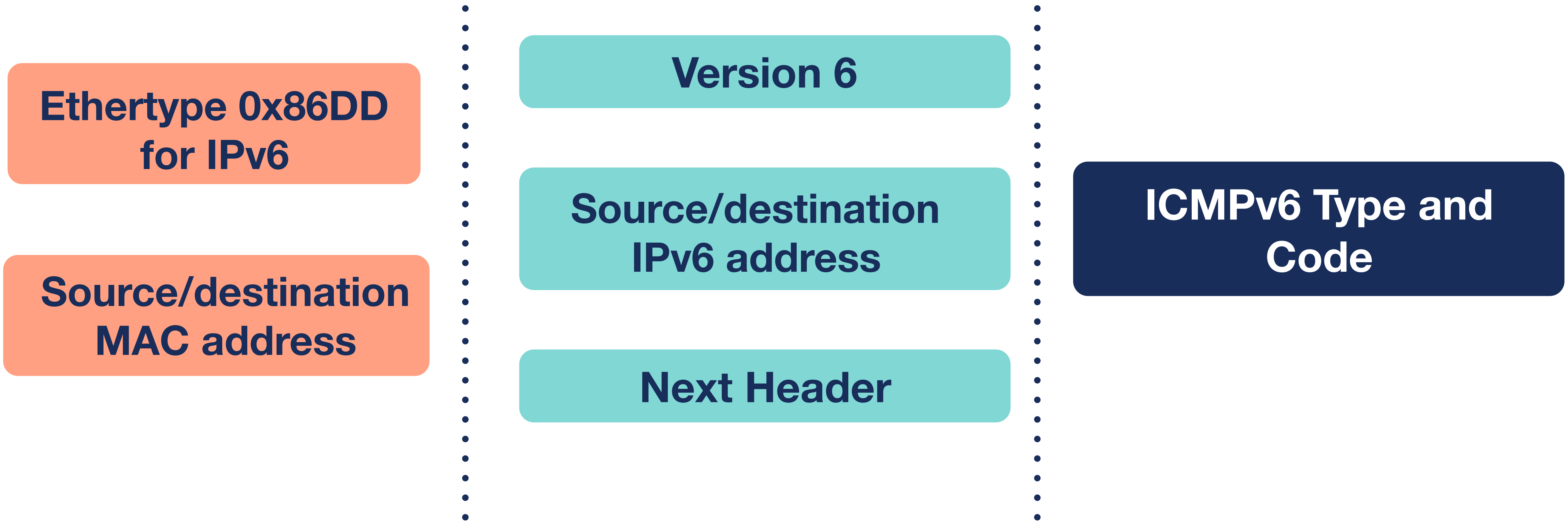
Stateful RA-Guard

Learns dynamically

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

Filtering

- ACLs in switches can protect NDP
- Switches should understand Ethernet, IPv6 and ICMPv6:



Ethertype 0x86DD for IPv6

Source/destination MAC address

Version 6

Source/destination IPv6 address

Next Header

ICMPv6 Type and Code

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
- Some solutions are available to protect NDP
- Recommended: use available ones
    - Check availability and configure them
- Detection (IDS/IPS) could be easier and recommended

MLD

Section 3.3

Introduction

- 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

- Mandatory for all IPv6 nodes (MUST)

QUERY

Router asks for Listeners

General

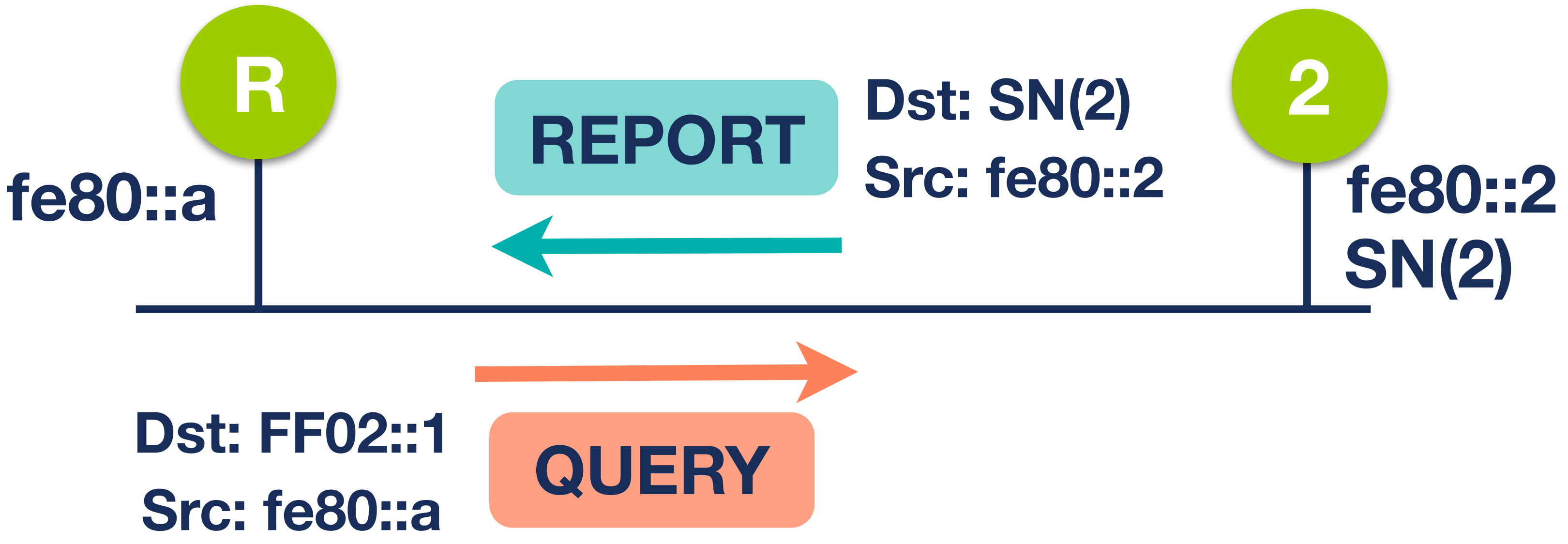
Group Specific

REPORT

Listeners report themselves

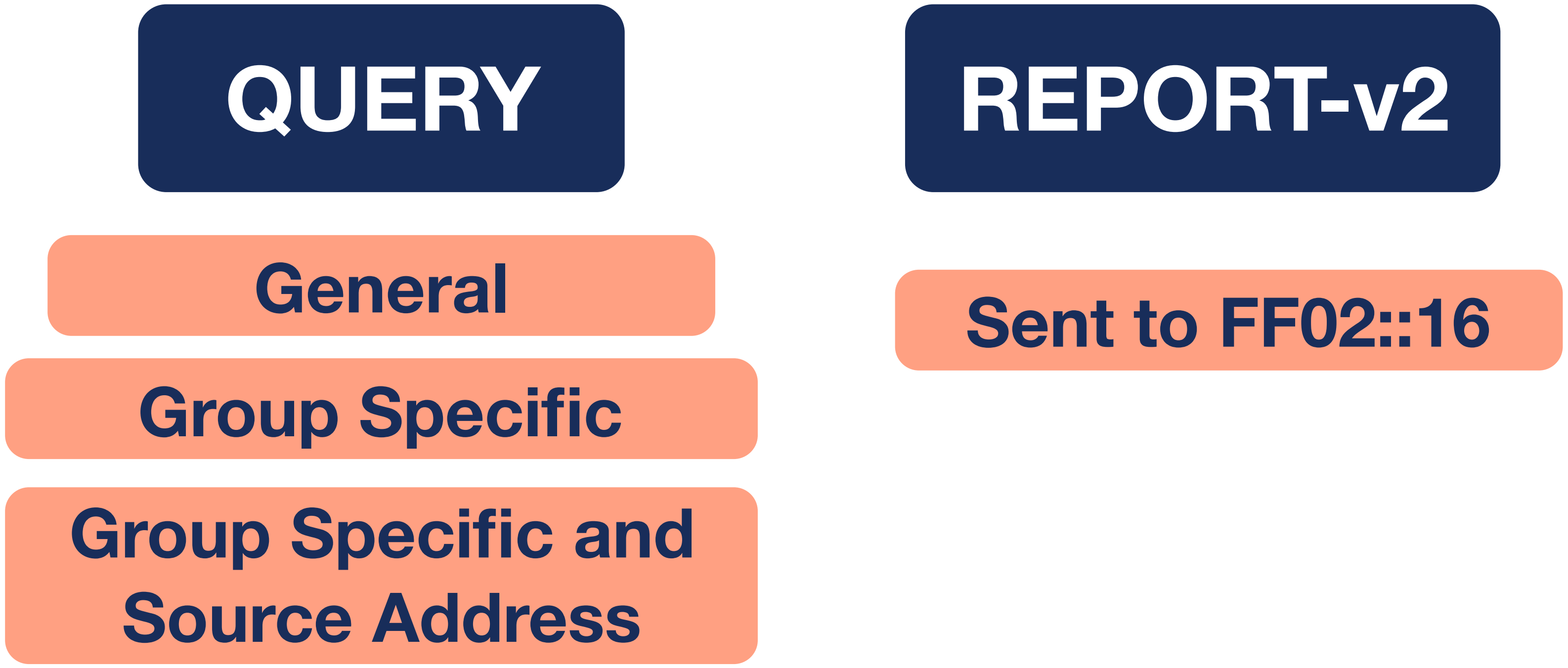
DONE

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

Group Specific

Group Specific and Source Address

REPORT-v2

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
- GUA accepted as destination for QUERY => allows direct interaction with listeners
- GUA accepted as source of REPORT => allows remote interaction with routers

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

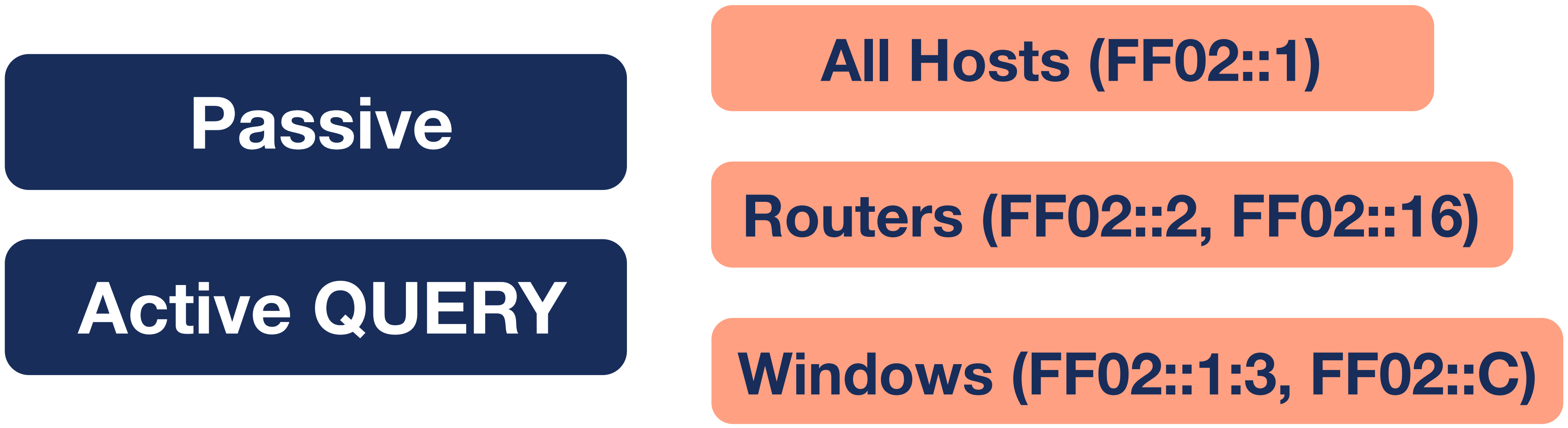
Several for each Addr.

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

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:** 20 minutes
- **Tasks**:
  - Scan your network using MLS Query message

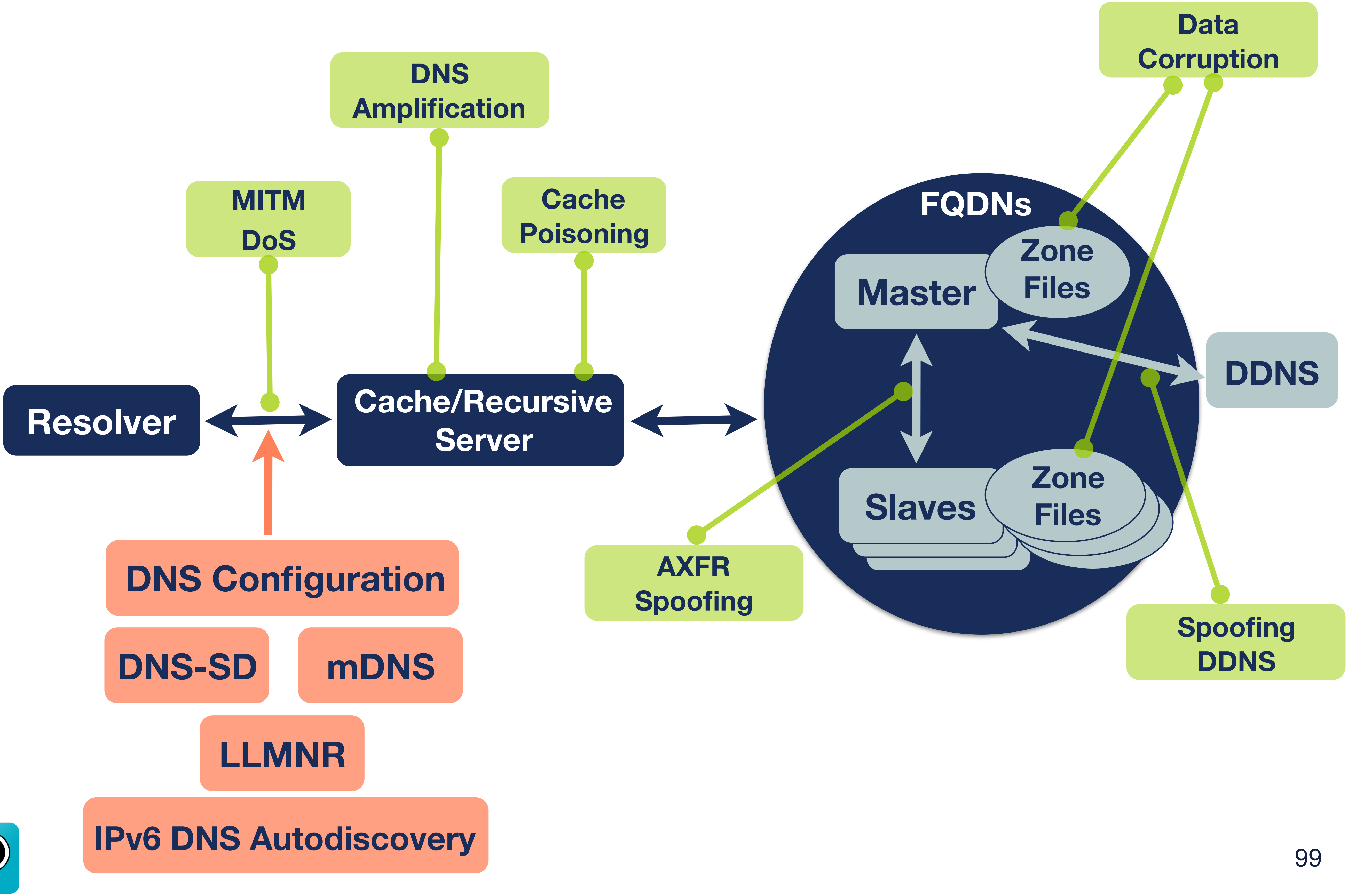
DNS

Section 3.4

Introduction (1)

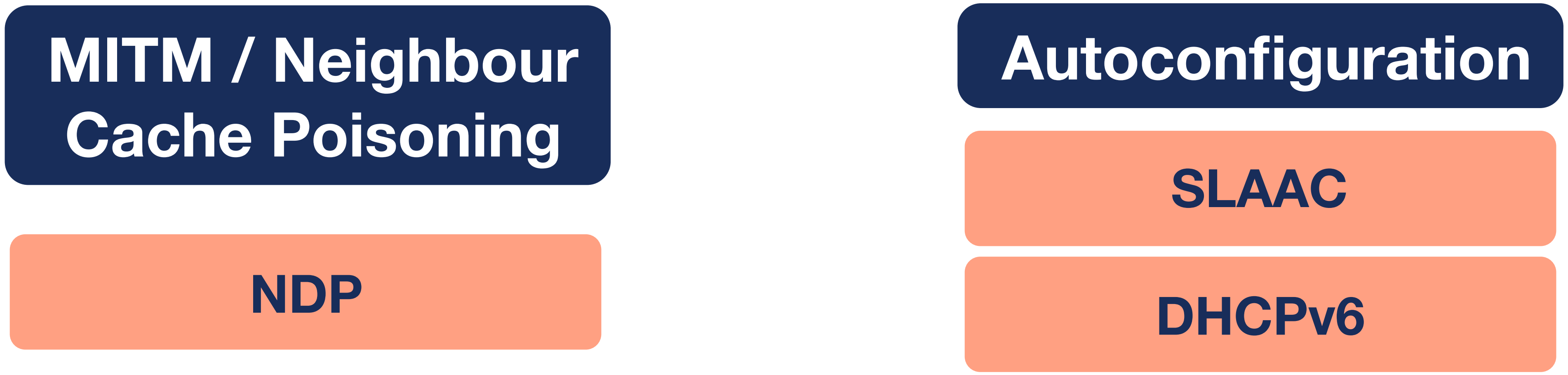
- IPv6 and IPv4 have same DNS vulnerabilities
- IPv6 support added in:
  - Communications between elements
  - Stored information (AAAA, PTR)
- Dual-stack means bigger attack surface
  - Protect DNS for IPv4 and IPv6
- Vulnerabilities come from:
  - DNS-related protocols
  - Implementation specifics

Introduction (2)



IPv6 DNS Configuration Attacks

- Attacker becomes the DNS server of the Victim



MITM / Neighbour Cache Poisoning

NDP

Autoconfiguration

SLAAC

DHCPv6

- Depending on answers to DNS queries:

MITM Attack

DoS Attack

DHCPv6

Section 3.5

Introduction

- Pretty similar to DHCPv4

Client-Server | UDP | Relay

- Message names change

SOLICIT | ADVERTISE | REQUEST | REPLY | Others…

- Servers/relays listen on multicast addresses

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

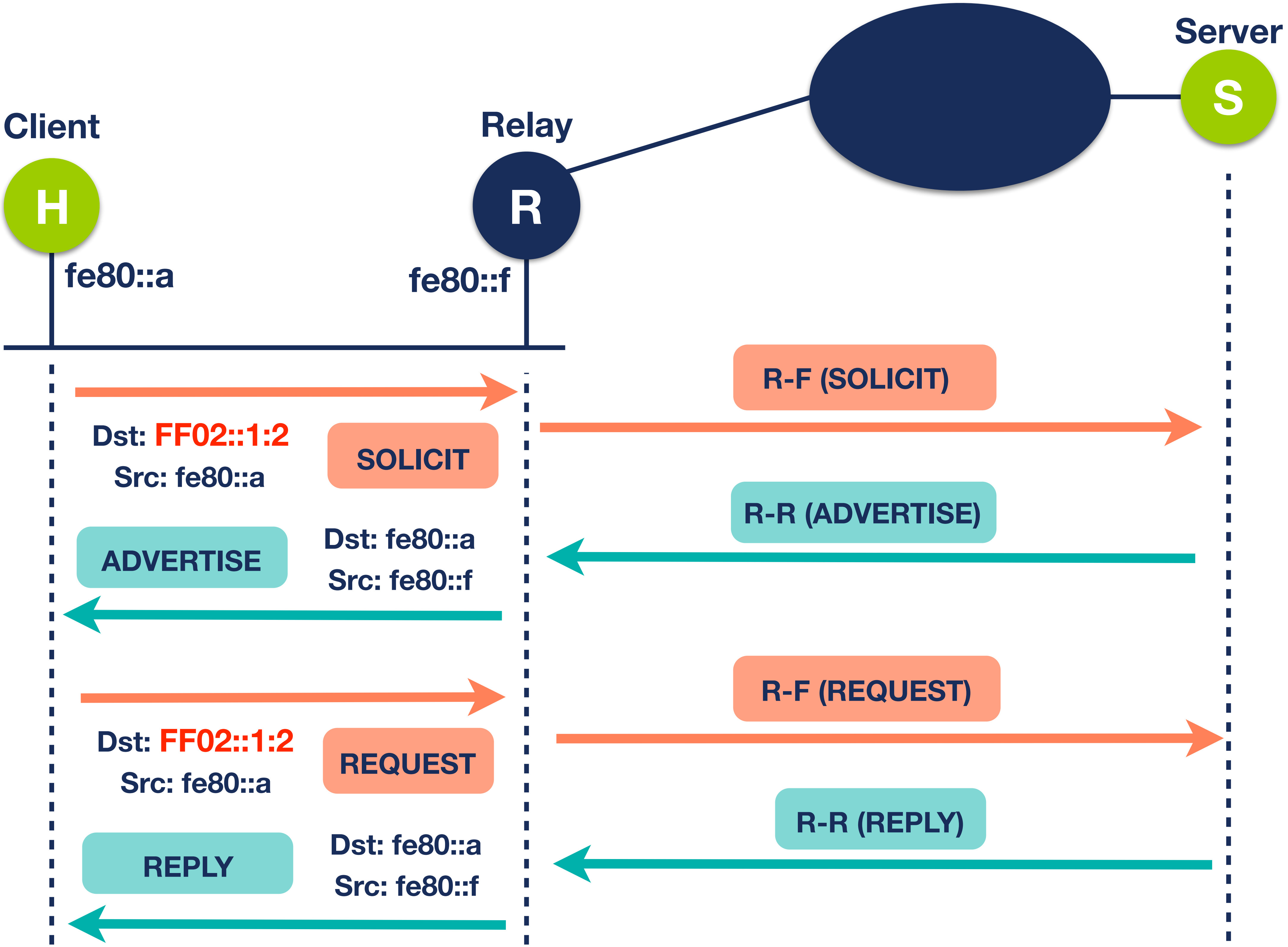
FF05::1:3
All DHCP Servers

DHCPv6 Details (1)

- How to trigger the use of DHCPv6?

		Attacker
RA with M = 1	Host asks for Address and DNS	DHCPv6 Server
RA with M = 0 / O = 1	Host asks for DNS	Stateless DHCPv6

DHCPv6 Details (2)



DHCPv6 Threats (1)

Privacy considerations:

- Client information can be obtained from IDs used (like the MAC from Client-ID)
- Server address assignment:
  - Iterative allocation: scanning easier
  - Identifier-based allocation: easier to track activity
  - Hash allocation: better, still allows activity track
  - Random allocation: better privacy

DHCPv6 Threats (2)

- **Rogue Server**: answer before legitimate server
- DHCPv6 Exhaustion attack can be used beforehand
- Two types:
  1. Simple: ADVERTISE answering to SOLICIT
  2. Reply Injection: Sending REPLY
- DNS Spoofing: sending wrong DNS server address
- IP Spoofing
- NOT Possible to send wrong Default Gateway

DHCPv6 Solutions

DHCPv6 [RFC3315] — **IPsec between Relays and Servers**

IPsec ESP [RFC8213] — **Recommends encryption to secure relay-to-relay and relay-to-server communication**

Secure DHCPv6 (I-D) — **Public Key Crypto** — **Client-Server authentication** — **Client-Server encryption**

DHCPv6-Shield [RFC7610] — **Protects Clients** — **Layer 2 ports**

DHCPv6 Guard — **Vendor's implementation of DHCPv6-Shield**

IPv6 Routing protocols

Section 3.6

Introduction

- We will cover:

1. Authentication of neighbours/peers
2. Securing routing updates

- Route filtering in next section

- Device hardening: same as in IPv4
  - More attention to bugs/updates

Neighbours/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 Traffic

Section 4.1

Introduction

- Filtering IPv6 traffic is important: GUA
- Good addressing plan means easier filtering
- Many things still the same
- New ones to take into account:
  1. ICMPv6
  2. IPv6 Extension Headers
  3. Fragments Filtering
  4. Transition mechanisms/dual-stack

Filtering ICMPv6

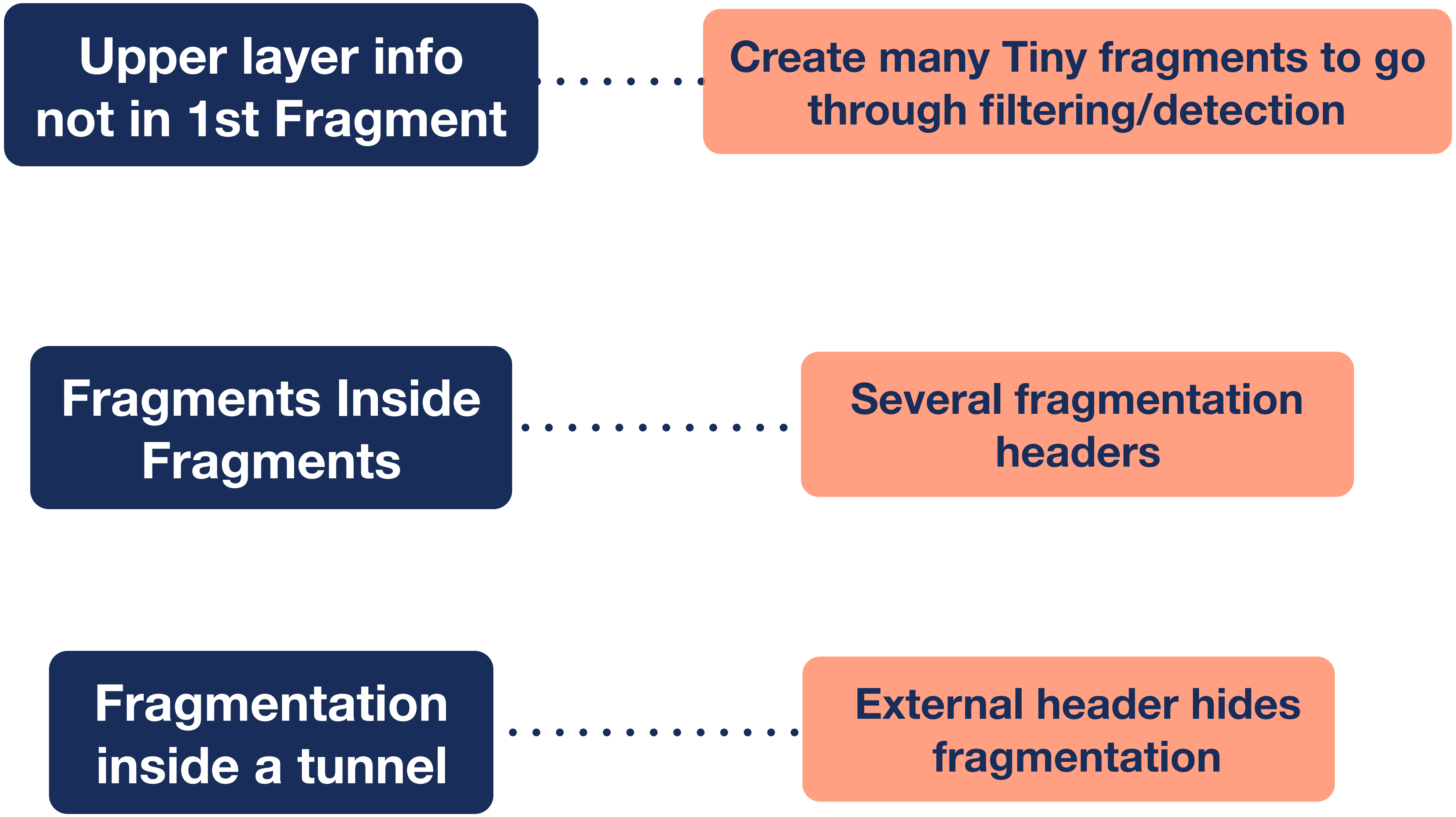
Type - Code	Description	Action
Type 1 - all	Destination Unreachable	ALLOW
Type 2	Packet Too Big	ALLOW
Type 3 - Code 0 & 1	Time Exceeded	ALLOW
Type 4 - Code 0, 1 & 2	Parameter Problem	ALLOW
Type 128	Echo Reply	ALLOW for troubleshoot and services. Rate limit
Type 129	Echo Request	ALLOW for troubleshoot 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

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: Threats



Upper layer info not in 1st Fragment — Create many Tiny fragments to go through filtering/detection

Fragments Inside Fragments — Several fragmentation headers

Fragmentation inside a tunnel — External header hides fragmentation

Filtering Fragments: Solutions

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

Fragmentation inside a tunnel

FW/IPS/IDS should support inspection of encapsulated traffic

Transition Mechanisms/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) ll (UDP dst port 3653 ll TCP dst port 3653)
AYIYA	UDP dest port 5072 ll TCP dest port 5072

Conclusions

- Packet filtering:
  - Powerful tool to protect your IPv6 network
  - Common practices, same as with IPv4
  - Some new considerations about IPv6

End-to-End needs filtering

ICMPv6 should be wisely filtered

Filtering adapted to IPv6: EHs, TMs

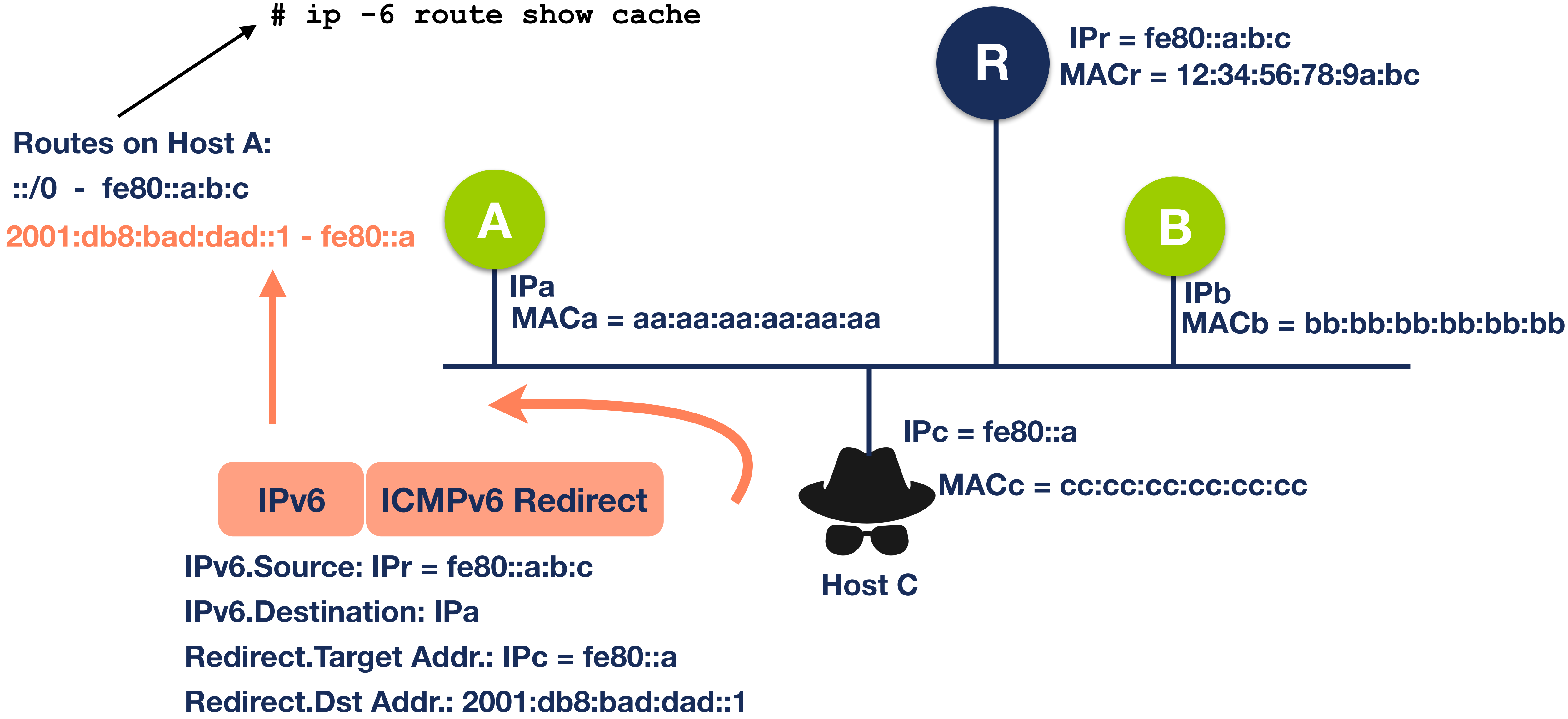
Filtering IPv6 Traffic

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:** 15 minutes
- **Tasks**:
  - Configure IPv6 packet filtering rules

4.1: IPv6 Packet Filtering - Redirect



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

Routes on Host A:

::/0 - fe80::a:b:c

2001:db8:bad:dad::1 - fe80::a

IPv6.Source: IPr = fe80::a:b:c

IPv6.Destination: IPa

Redirect.Target Addr.: IPc = fe80::a

Redirect.Dst Addr.: 2001:db8:bad:dad::1

Filtering IPv6 Routing Information

Section 4.2

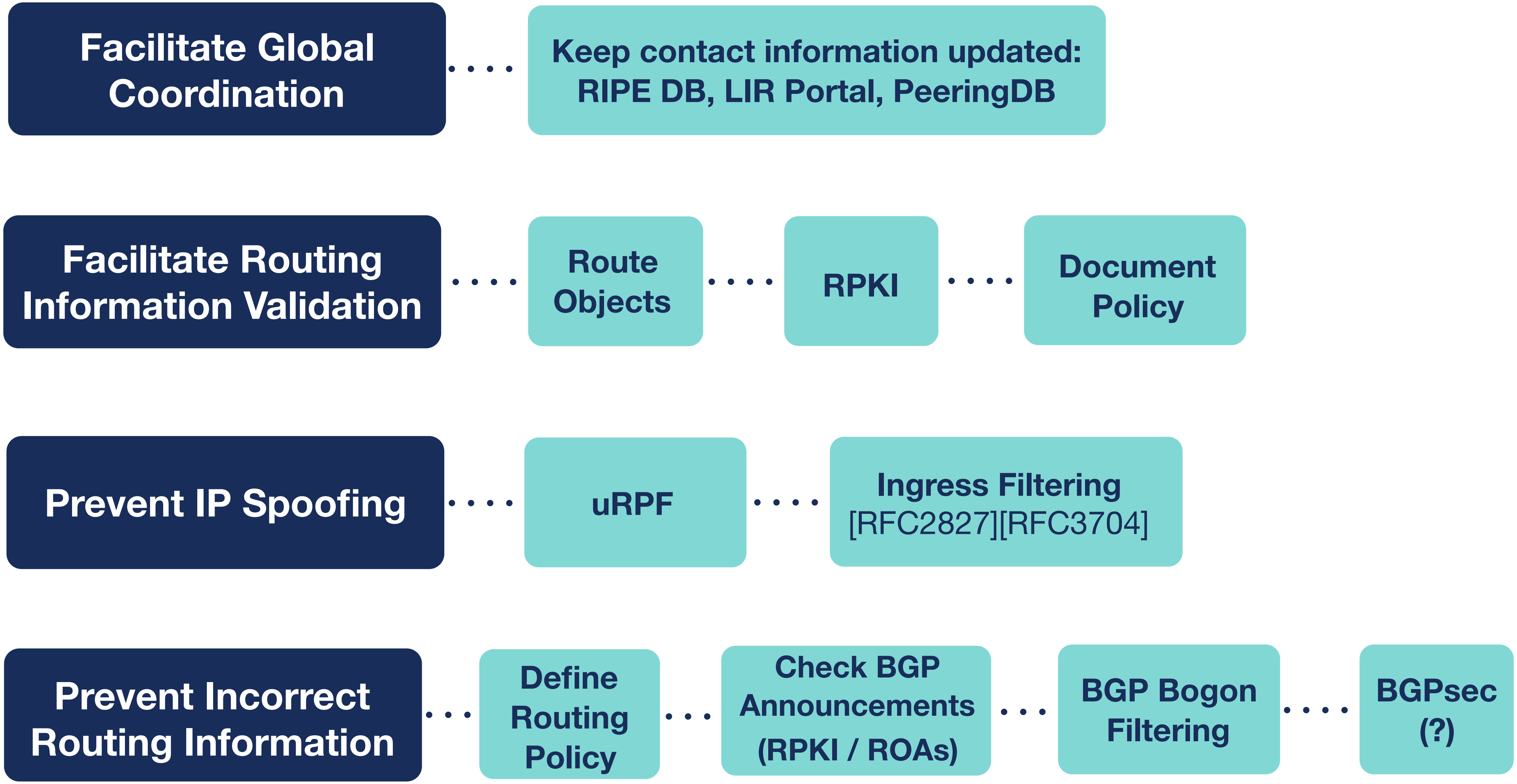
Introduction

- The ideas are the same as with IPv4

- MANRS (www.routingmanifesto.org)
  - Secure and Resilient Internet is a **collaborative** effort
  - 4 concrete actions for network operators
  - IPv6 and IPv4 BGP

- Good addressing plan, makes route filtering easier within a network

MANRS 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 (?)

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 or longer
Site-local Addresses (deprecated)	fec0::/10 or longer
Unique-local addresses	fc00::/7 or longer
Multicast Addresses	ff00::/8 or longer
Documentation addresses	2001:db8::/32 or longer
6Bone Addresses (deprecated)	3ffe::/16, 5f00::/8
ORCHID	2001:10::/28

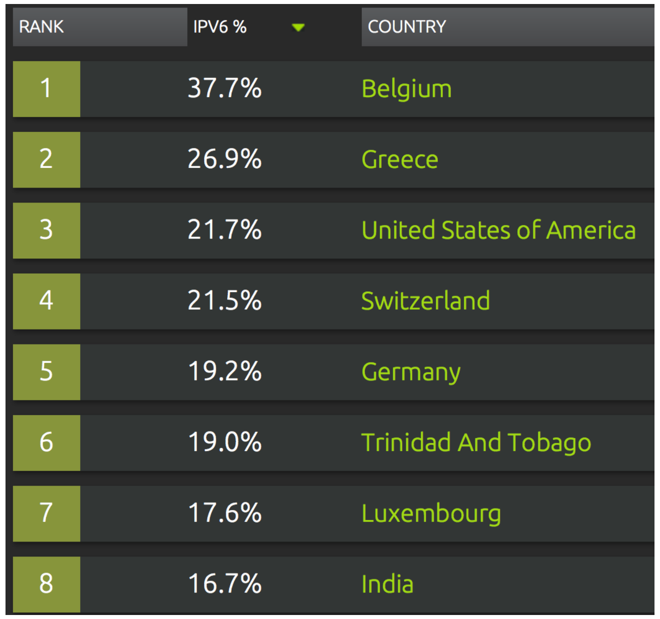
- Team Cymru http://www.team-cymru.org/bogon-reference-bgp.html

Internet Wide IPv6 Security

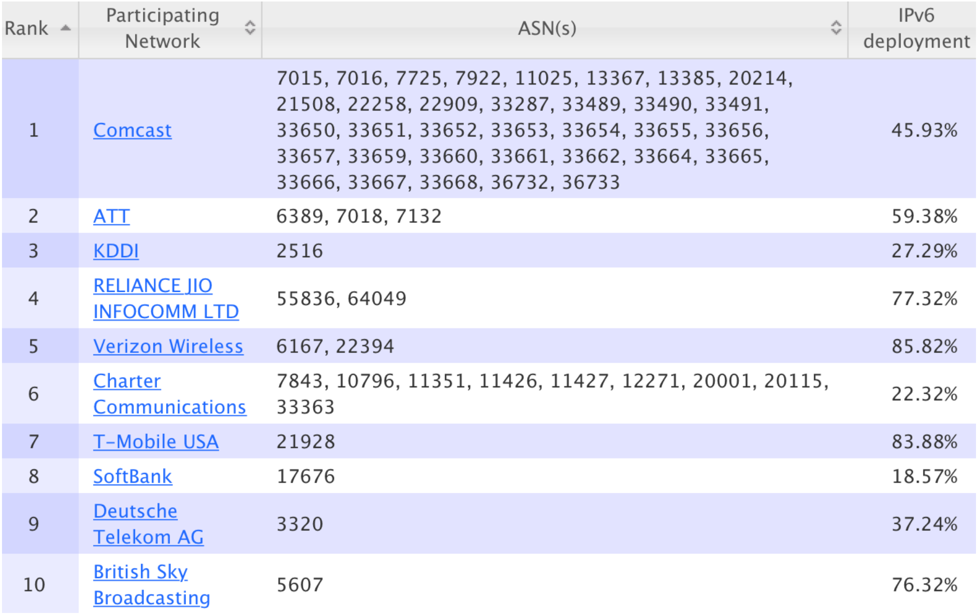
Section 5

Introduction (1)

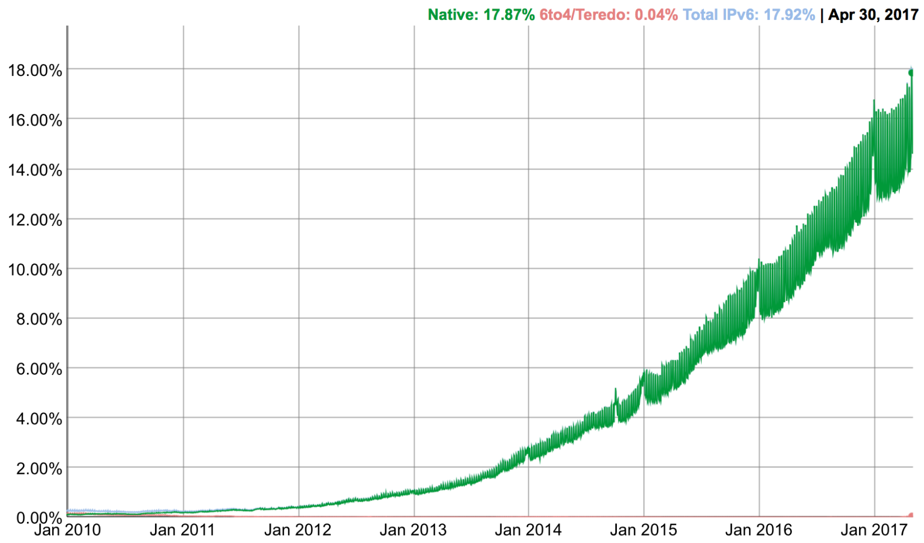
- IPv6 is happening! …



RANK	IPV6 %	COUNTRY
1	37.7%	Belgium
2	26.9%	Greece
3	21.7%	United States of America
4	21.5%	Switzerland
5	19.2%	Germany
6	19.0%	Trinidad And Tobago
7	17.6%	Luxembourg
8	16.7%	India



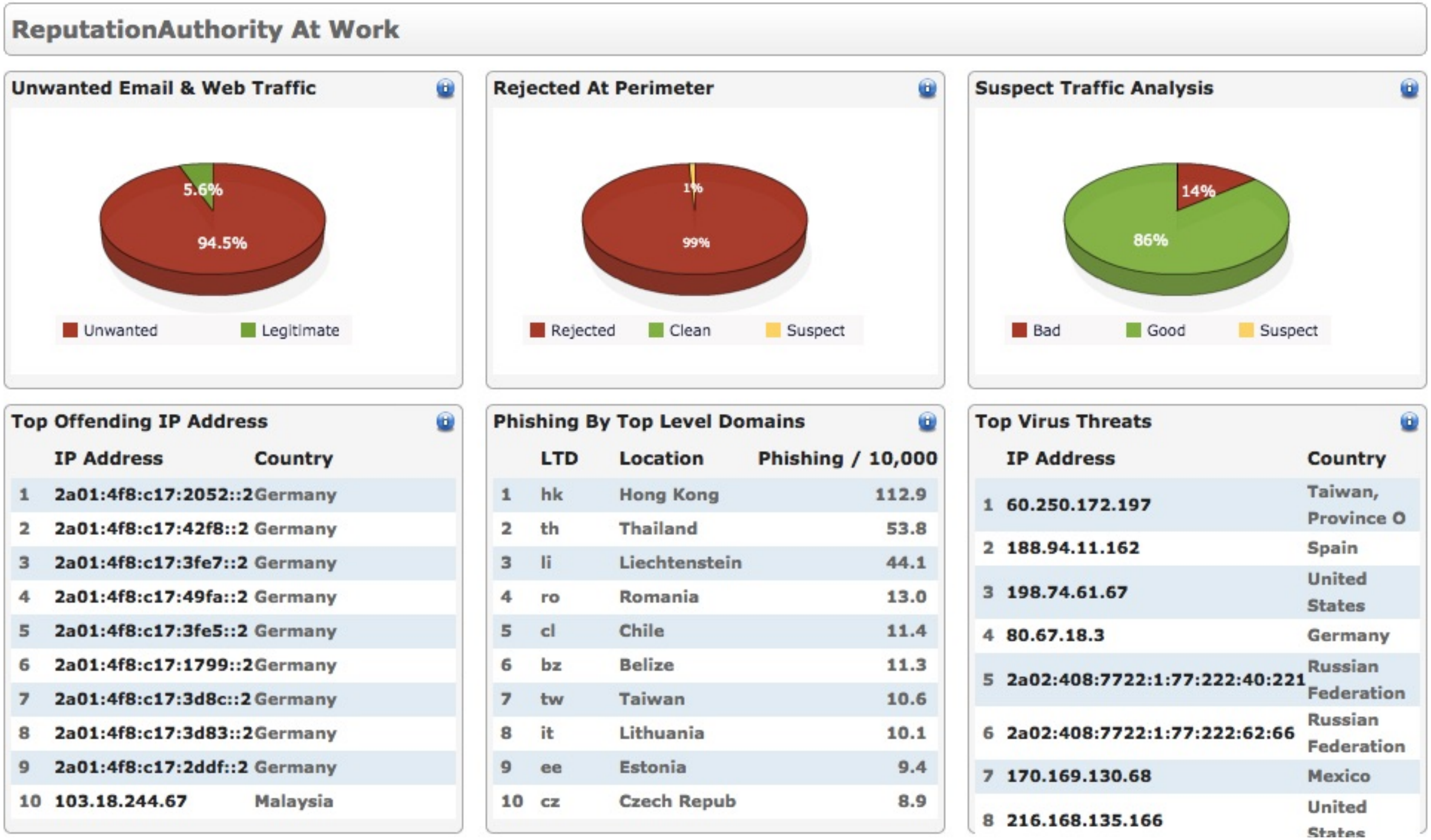
Rank	Participating Network	ASN(s)	IPv6 deployment
1	Comcast	7015, 7016, 7725, 7922, 11025, 13367, 13385, 20214, 21508, 22258, 22909, 33287, 33489, 33490, 33491, 33650, 33651, 33652, 33653, 33654, 33655, 33656, 33657, 33659, 33660, 33661, 33662, 33664, 33665, 33666, 33667, 33668, 36732, 36733	45.93%
2	ATT	6389, 7018, 7132	59.38%
3	KDDI	2516	27.29%
4	RELIANCE JIO INFOCOMM LTD	55836, 64049	77.32%
5	Verizon Wireless	6167, 22394	85.82%
6	Charter Communications	7843, 10796, 11351, 11426, 11427, 12271, 20001, 20115, 33363	22.32%
7	T-Mobile USA	21928	83.88%
8	SoftBank	17676	18.57%
9	Deutsche Telekom AG	3320	37.24%
10	British Sky Broadcasting	5607	76.32%



Source: http://worldipv6launch.org/measurements/ (10/5/2017)

Introduction (2)

- … 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

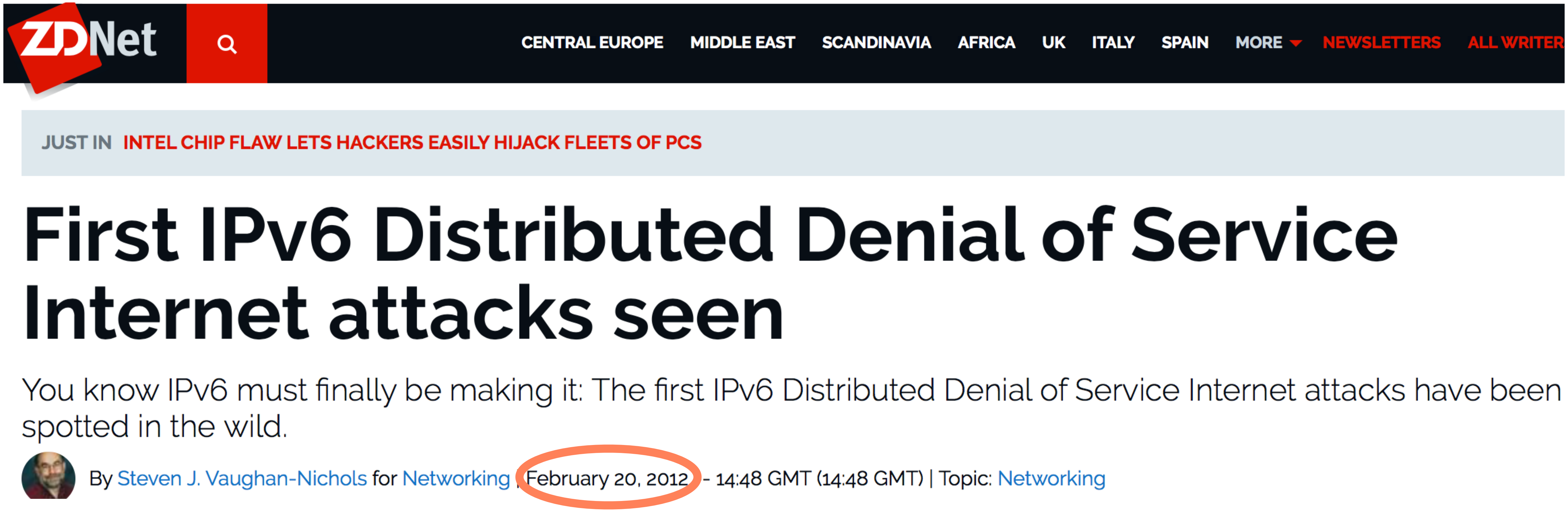
Source: http://www.borderware.com

DDoS

Section 5.1

Introduction

- DDoS attacks in IPv6?



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

DDoS with IPv6 (1)

- DDoS attacks makes use of many factors

- Related with IPv6:

1. Using lots of hosts
2. Using outdated firmware
3. Lacking/poor security measures

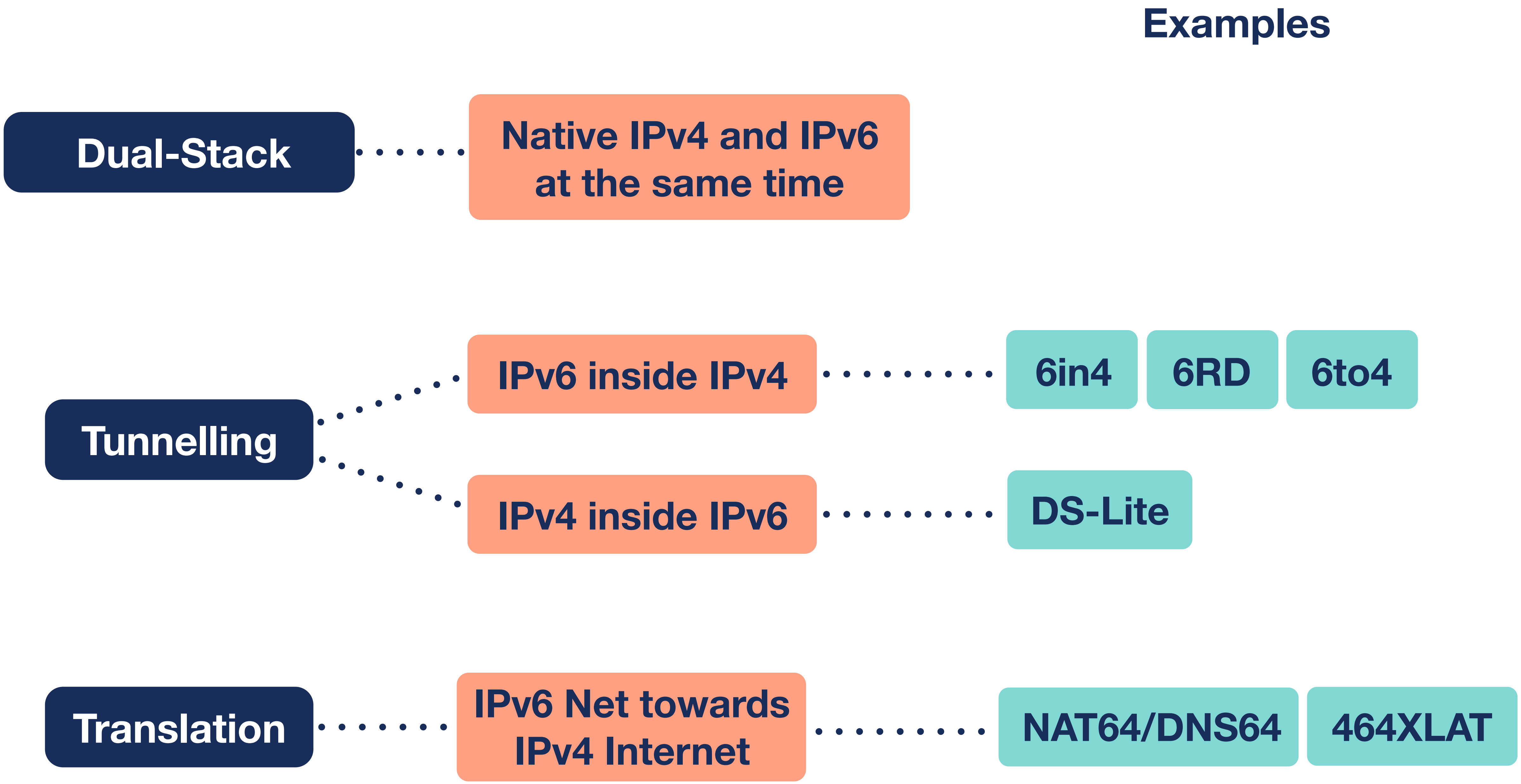
DDoS with IPv6 (2)

- Filter traffic, don’t allow free access to all IPv6 addresses
- Update firmware/SW
- Use security measures for IPv6 (this course is a good starting point :-)
- Ingress/egress filtering and RPF
- Hierarchical IPv6 address assignment helps

IPv6 Transition Mechanisms

Section 5.2

Introduction



Examples

Dual-Stack

Native IPv4 and IPv6 at the same time

Tunnelling

IPv6 inside IPv4

6in4 | 6RD | 6to4

IPv4 inside IPv6

DS-Lite

Translation

IPv6 Net towards IPv4 Internet

NAT64/DNS64 | 464XLAT

Dual-stack: Threats

- Makes attack surface bigger
- IPv6 nodes (commonly) have GUA
- One IP version could be used to attack the other
- Be careful with “IPv4 only” networks …

IPv4-only Networks (1)

- Different scenarios depending on version used:

IPv4-only

Dual-stack

IPv6-only

- From two points of view:

Infrastructure ········ Data service, configuration and network services

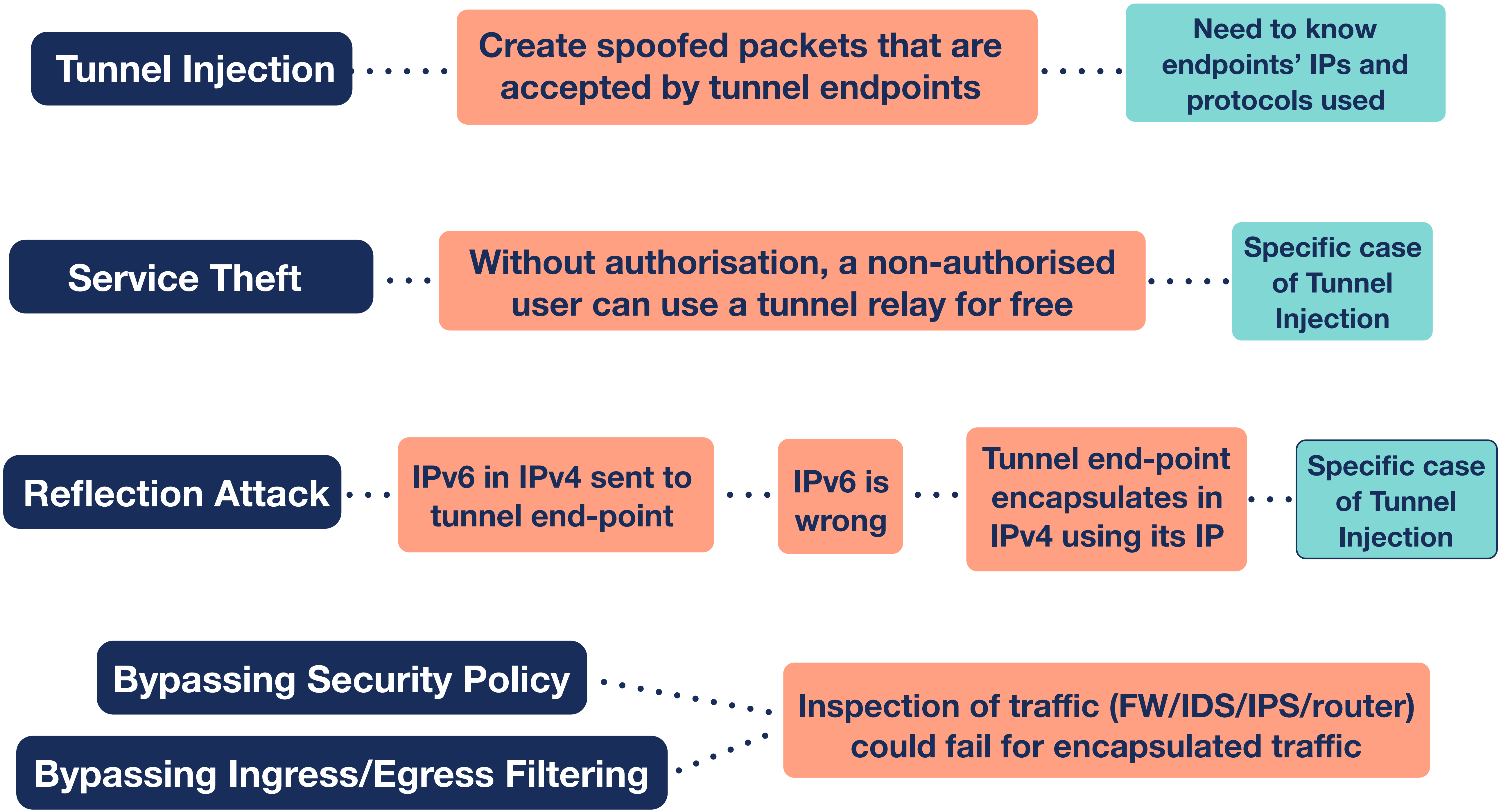
Network hosts ······· Devices connected to the network

IPv4-only Networks (2)

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

- IPv6-only hosts:
  - Avoids the use of IPv4 for finding IPv6 hosts

Tunnelling Threats



Tunnel Injection

Create spoofed packets that are accepted by tunnel endpoints

Need to know endpoints' IPs and protocols used

Service Theft

Without authorisation, a non-authorised user can use a tunnel relay for free

Specific case of Tunnel Injection

Reflection Attack

IPv6 in IPv4 sent to tunnel end-point

IPv6 is wrong

Tunnel end-point encapsulates in IPv4 using its IP

Specific case of Tunnel Injection

Bypassing Security Policy

Bypassing Ingress/Egress Filtering

Inspection of traffic (FW/IDS/IPS/router) could fail for encapsulated traffic

Translation Threats

- IPsec can’t be used end-to-end
- DNSSEC can’t be used with DNS64

- Possible attacks:

Reflection Attack

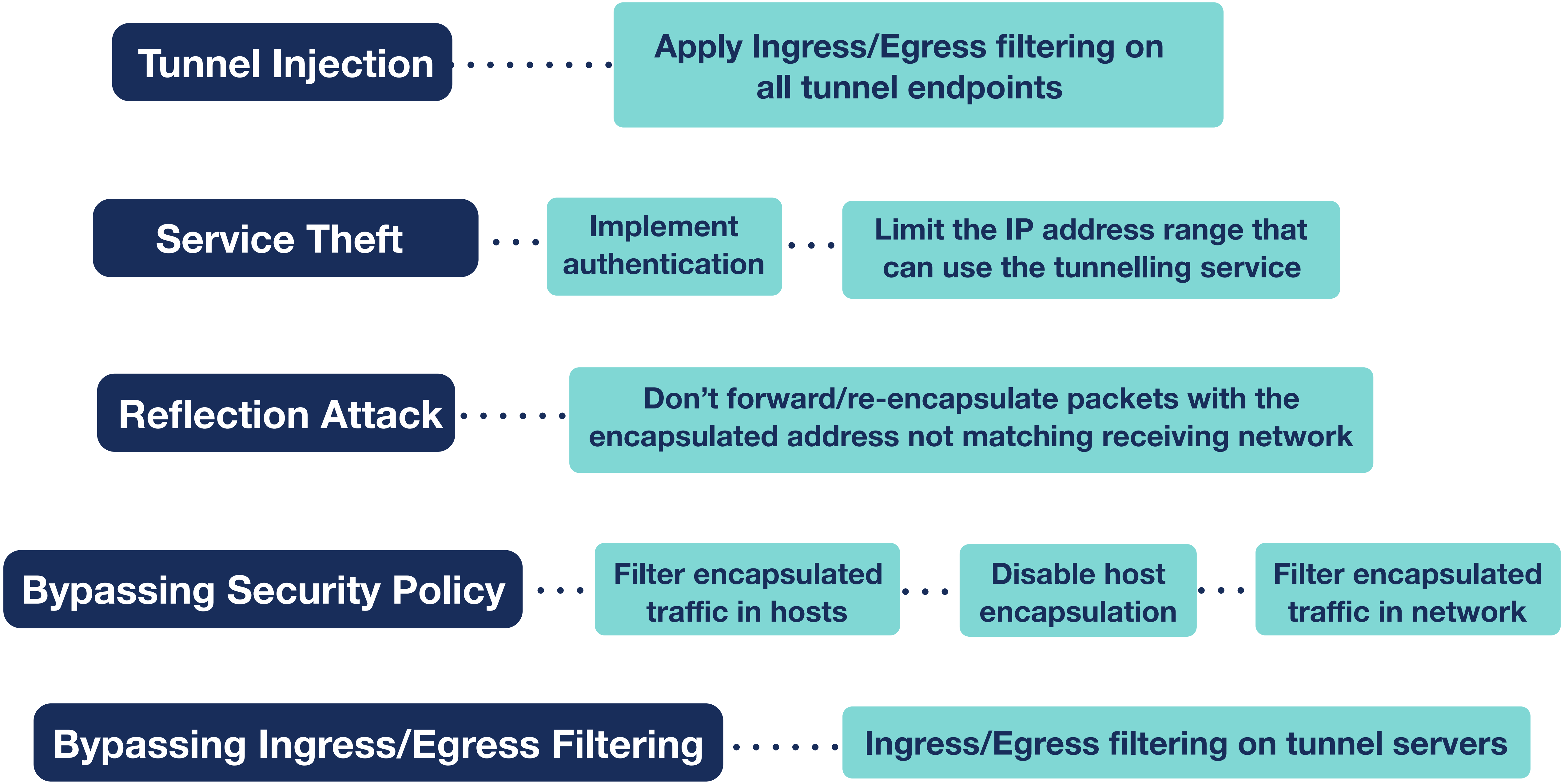
Pool Depletion Attack

ALG CPU Attack

Dual-stack Solutions

- Protect IPv6 at the same level as IPv4
- Filter end-2-end IPv6 traffic properly
- Don’t trust on “IPv4-only” networks

Tunnelling Solutions



Tunnel Injection — Apply Ingress/Egress filtering on all tunnel endpoints

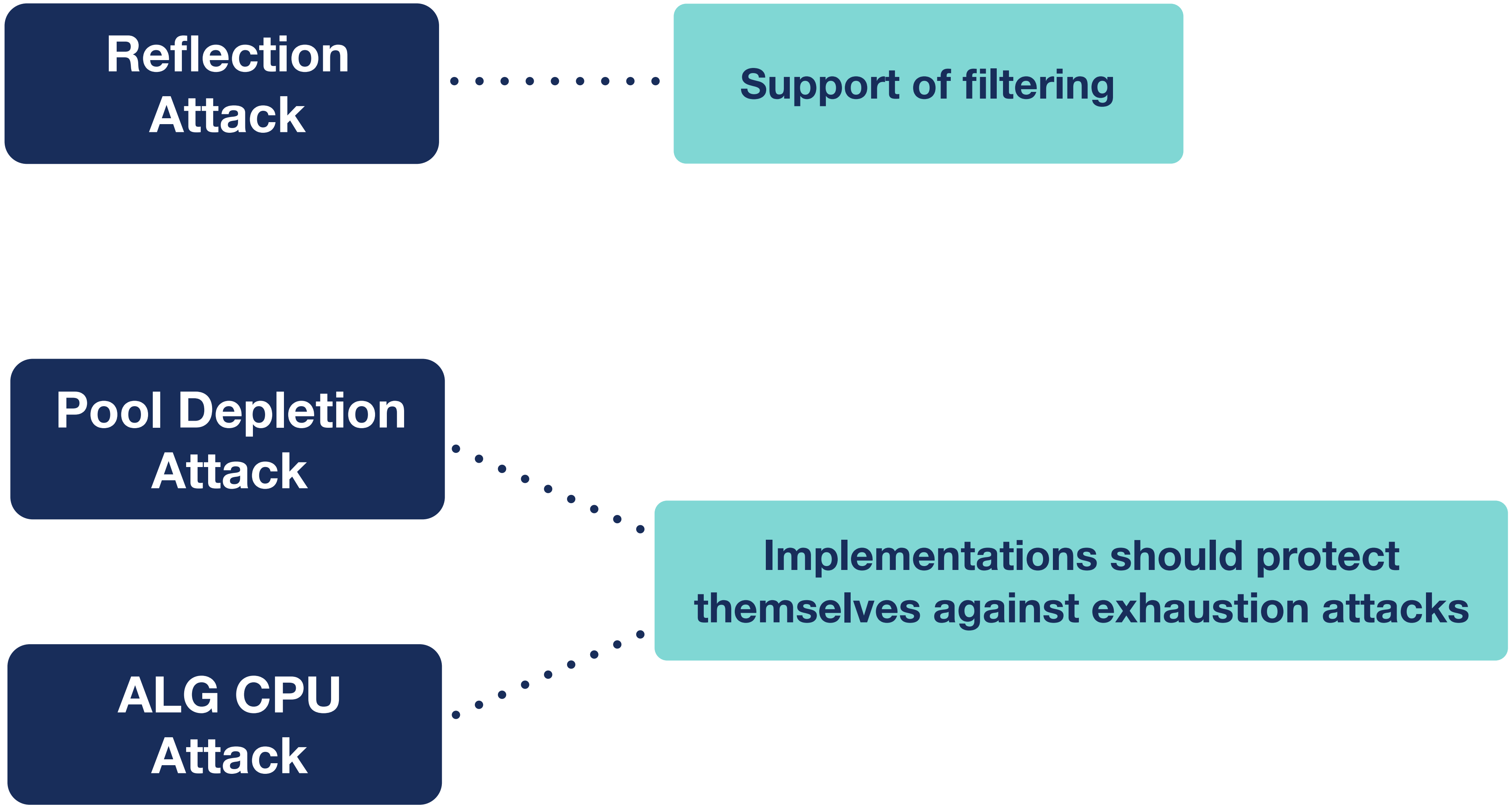
Service Theft — Implement authentication — Limit the IP address range that can use the tunnelling service

Reflection Attack — Don't forward/re-encapsulate packets with the encapsulated address not matching receiving network

Bypassing Security Policy — Filter encapsulated traffic in hosts — Disable host encapsulation — Filter encapsulated traffic in network

Bypassing Ingress/Egress Filtering — Ingress/Egress filtering on tunnel servers

Translation Solutions



Reflection Attack

Support of filtering

Pool Depletion Attack

ALG CPU Attack

Implementations should protect themselves against exhaustion attacks

IPv6 Security Tips and Tools

Section 6

Introduction

- Best security tool is knowledge
- IPv6 security is a moving target, keep updated

- IPv6 is happening: need to know about IPv6 security

- Cybersecurity challenge: Scalability
  - IPv6 is also responsible for Internet growth
  - IPv6 security knowledge needed to tackle the scalability issue

Tips

- IPv6 quite similar to IPv4, many reusable practices

- IPv6 security compared with IPv4:

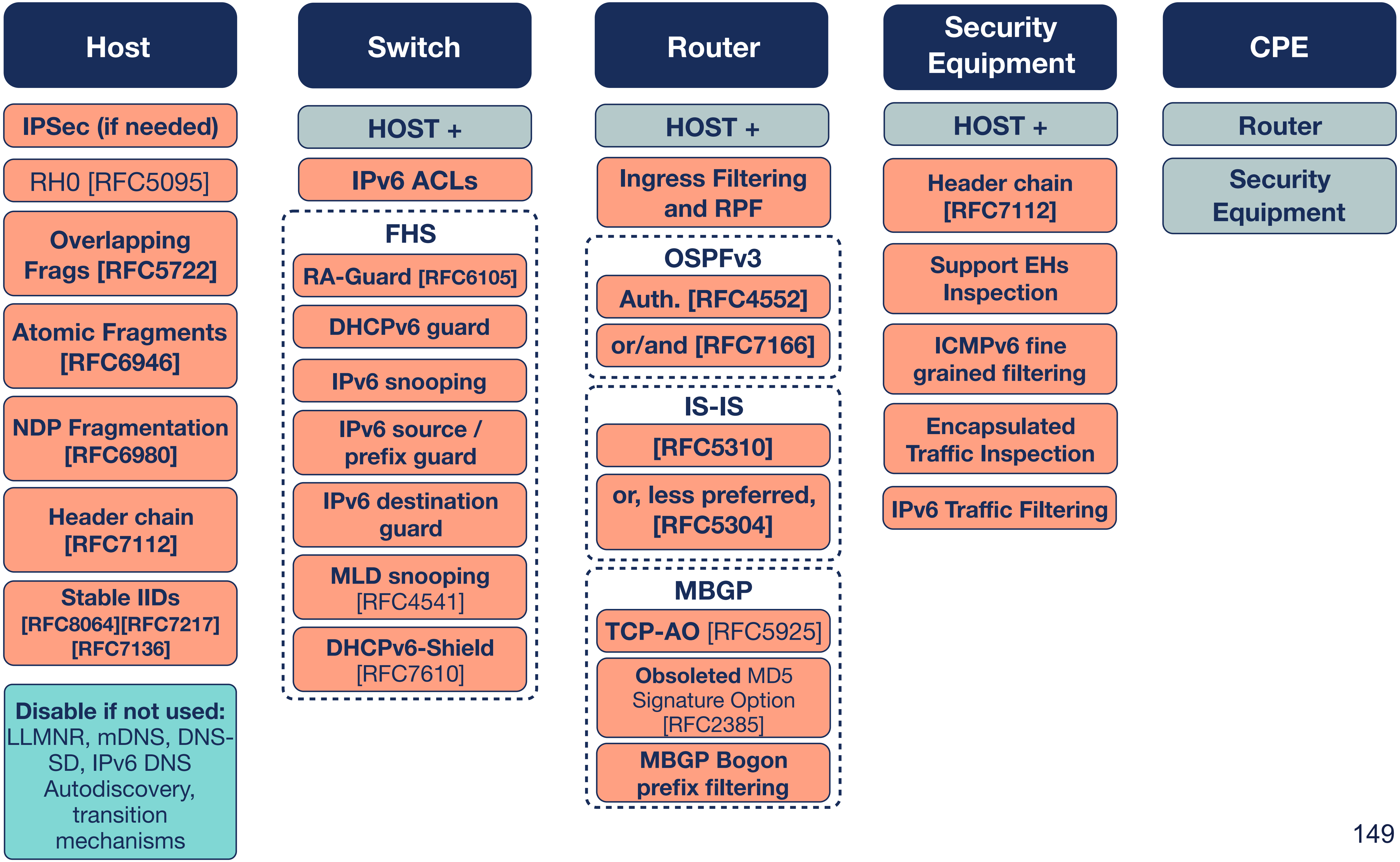
No changes with IPv6

Changes with IPv6

New IPv6 issues

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
- 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

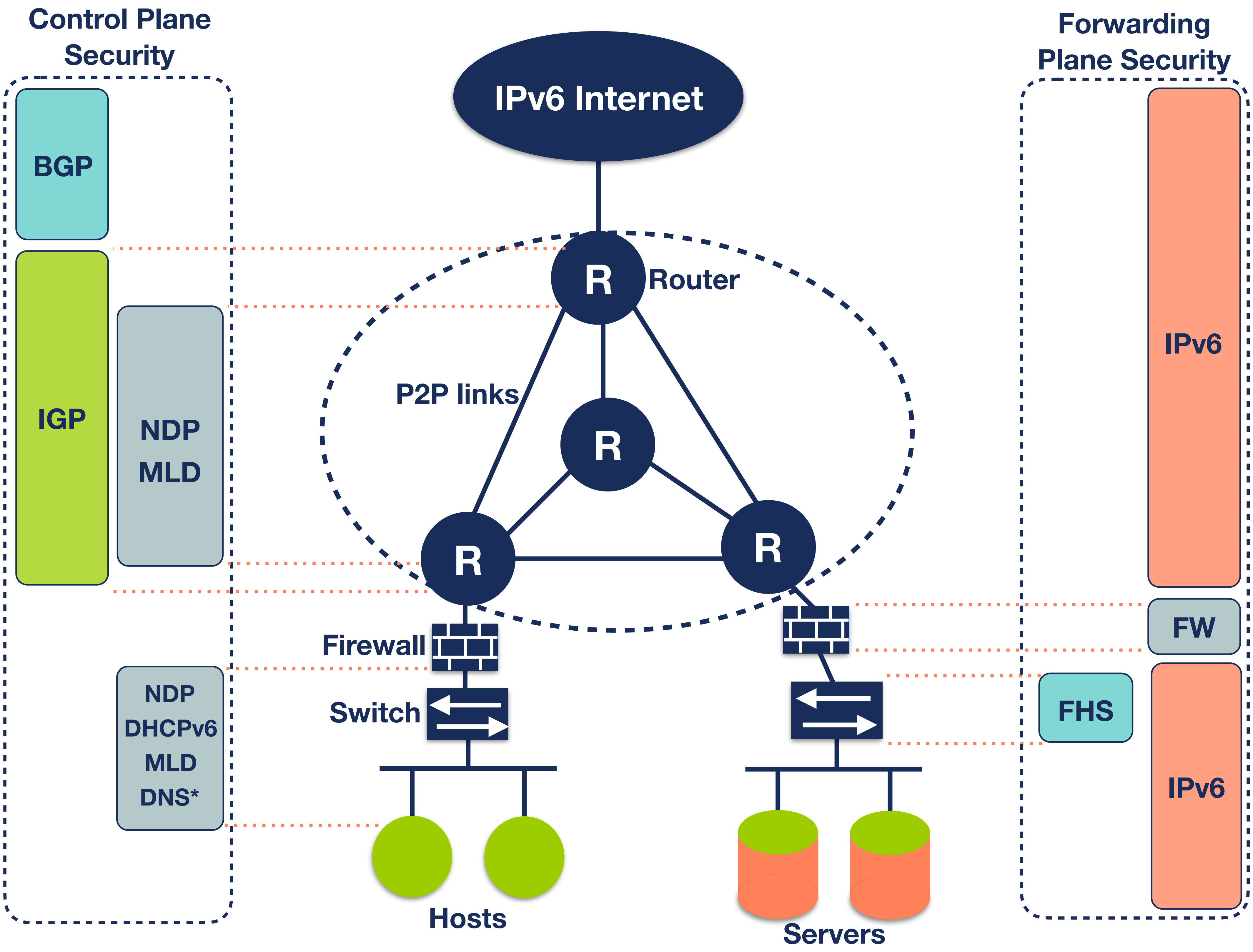
Security Equipment

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

CPE

- Router
- Security Equipment

Overview: Network Example



* All Name resolution related protocols

IPv6 Support

- IPv6 support is not a yes/no question

- List the features you need
  - Security features **are important**

- Check if IPv6 is supported for your specific needs

Security Tools

- Many existent software/vendors support IPv6

Wireshark

The IPv6 Toolkit

THC-IPV6

Nmap

Scapy

Ettercap

Chiron

Pholus

Feedback!

https://www.ripe.net/training/ipv6security/survey

RIPE NCC Academy

RIPE NCC

Academy

Graduate to the next level!

http://academy.ripe.net

Follow us!

@TrainingRIPENCC

The End!

Край

Y Diwedd

Fí

Finis

النهاية

Соңы

Վերջ

Liðugt

Ende

Finvezh

Кінець

Konec

Kraj

Ënn

Fund

پایان

Крај

Lõpp

Beigas

Vége

Son

An Críoch

הסוף

Endir

Fine

Sfârşit

Fin

Τέλος

Einde

Конец

Slut

Slutt

დასასრული

Pabaiga

Fim

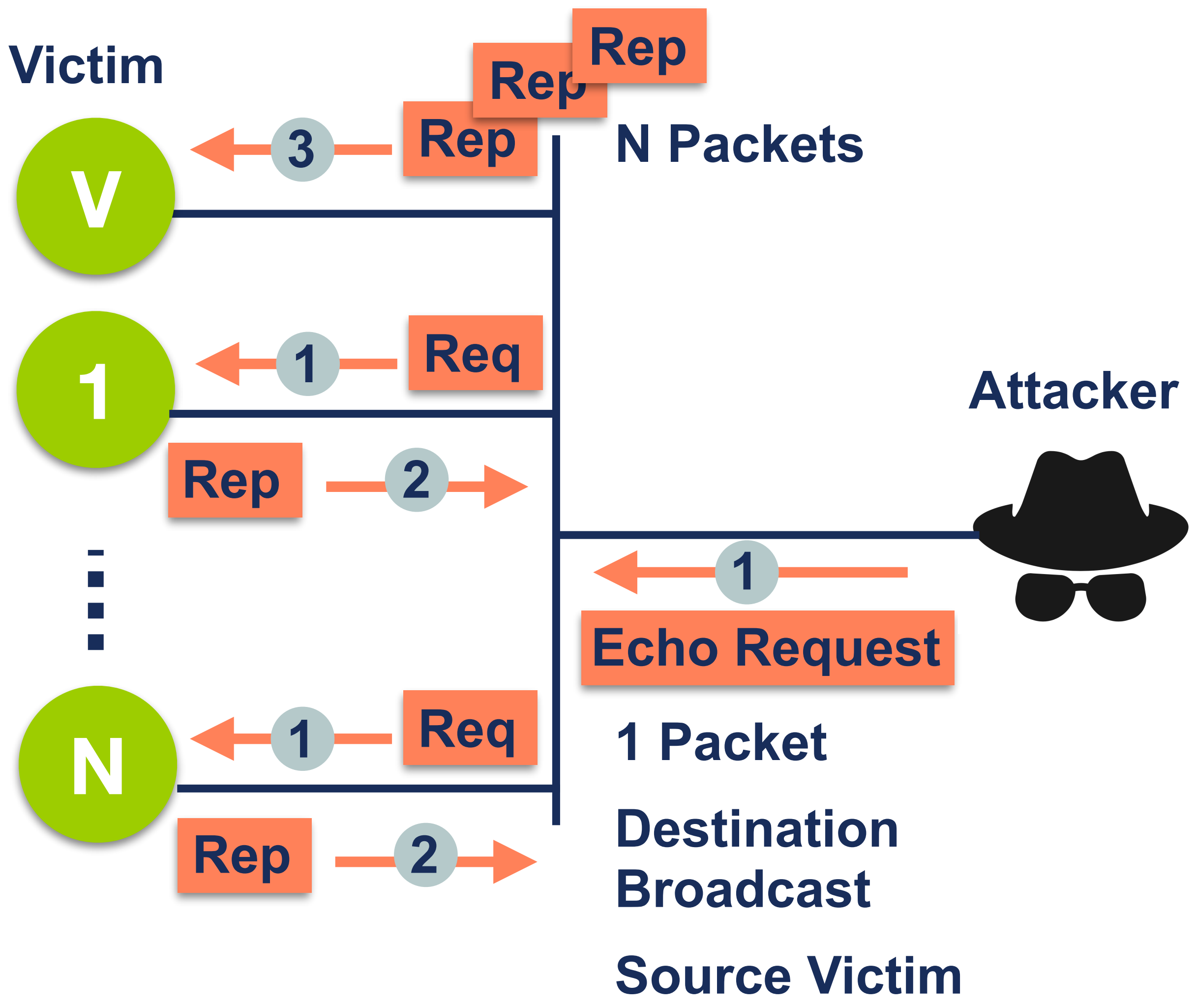
Amaia

Loppu

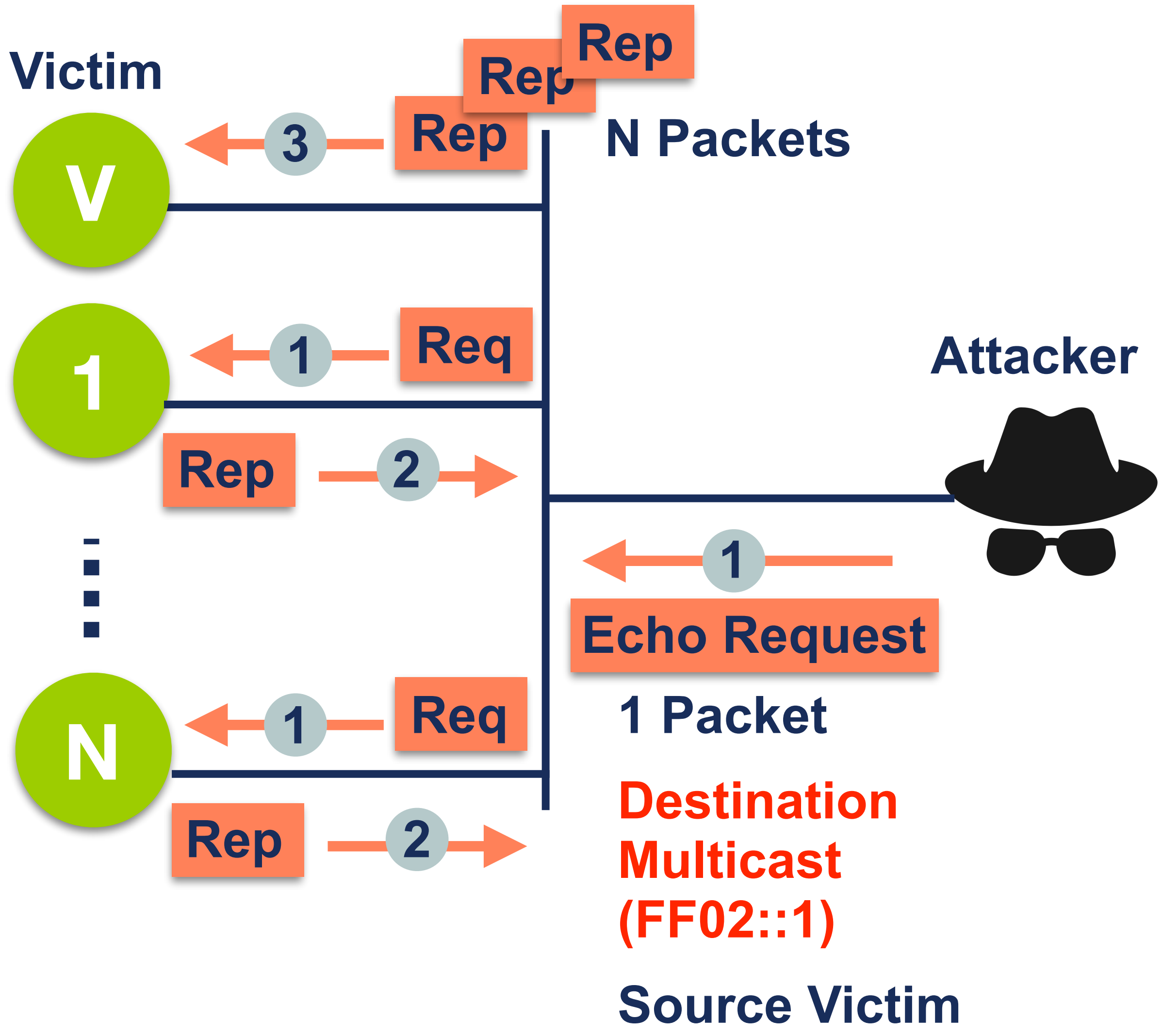
Tmiem

Koniec

Extra: Smurf Attack



IPv4 Smurf Attack



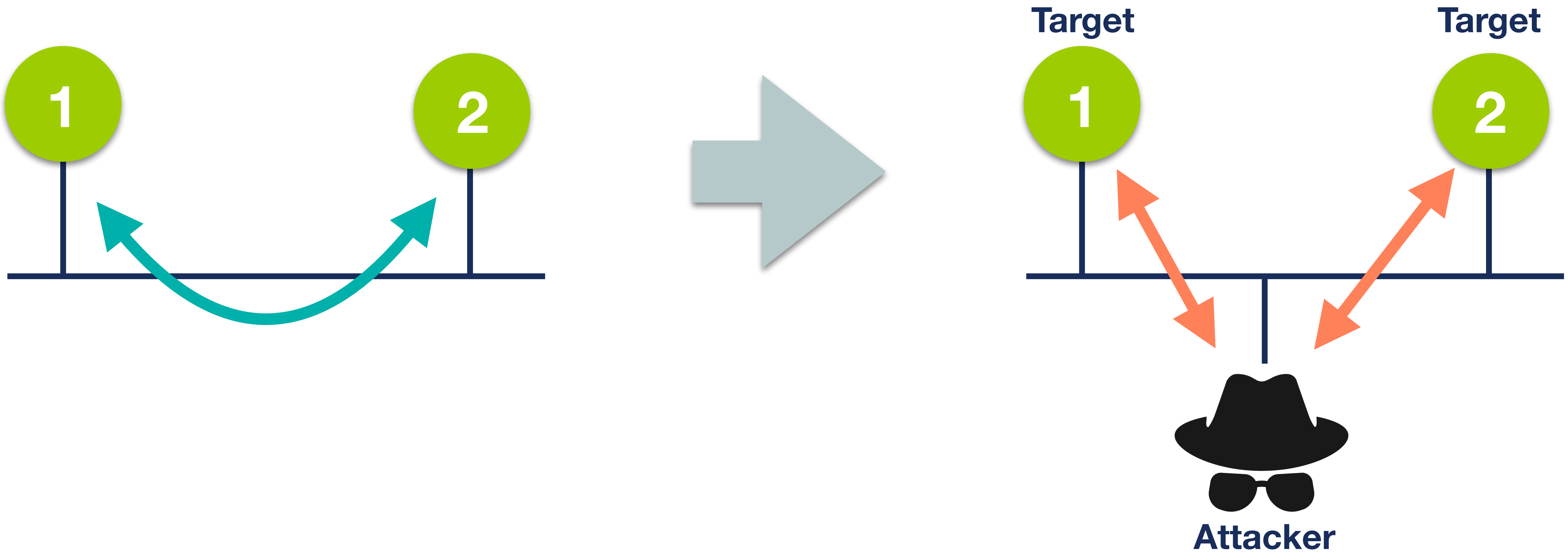
IPv6 Smurf Attack

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

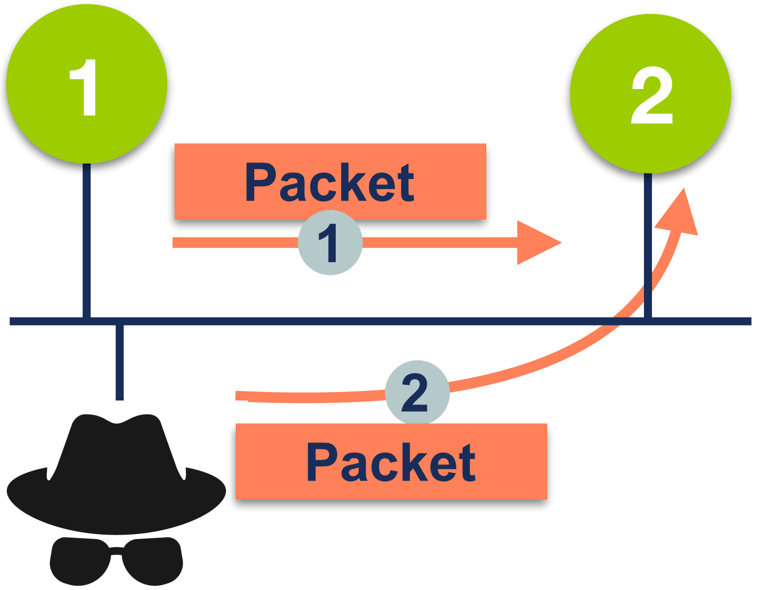
Extra: MITM

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

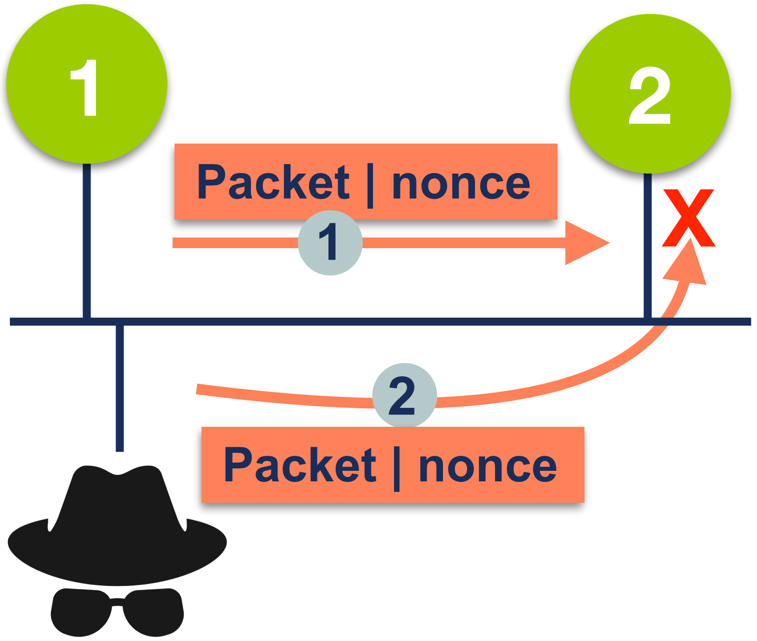


Extra: Replay Attacks

- Replay Attacks consist in sending again a previous packet

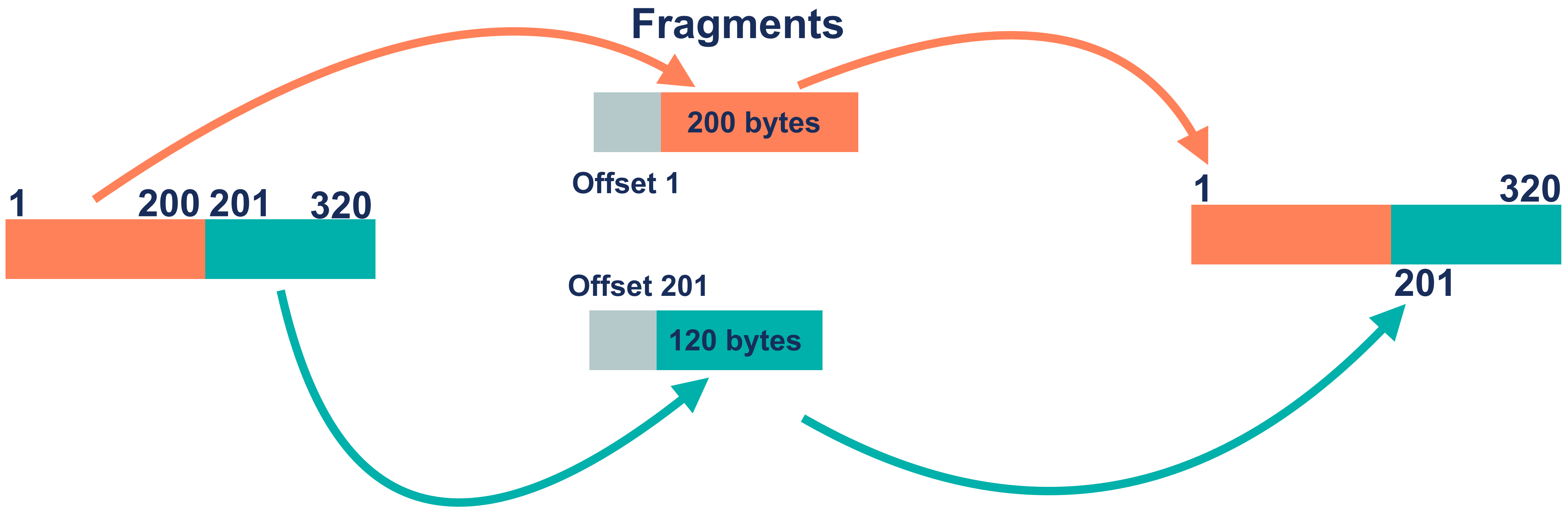


- Solution: nonce or timestamp (makes packet unique)

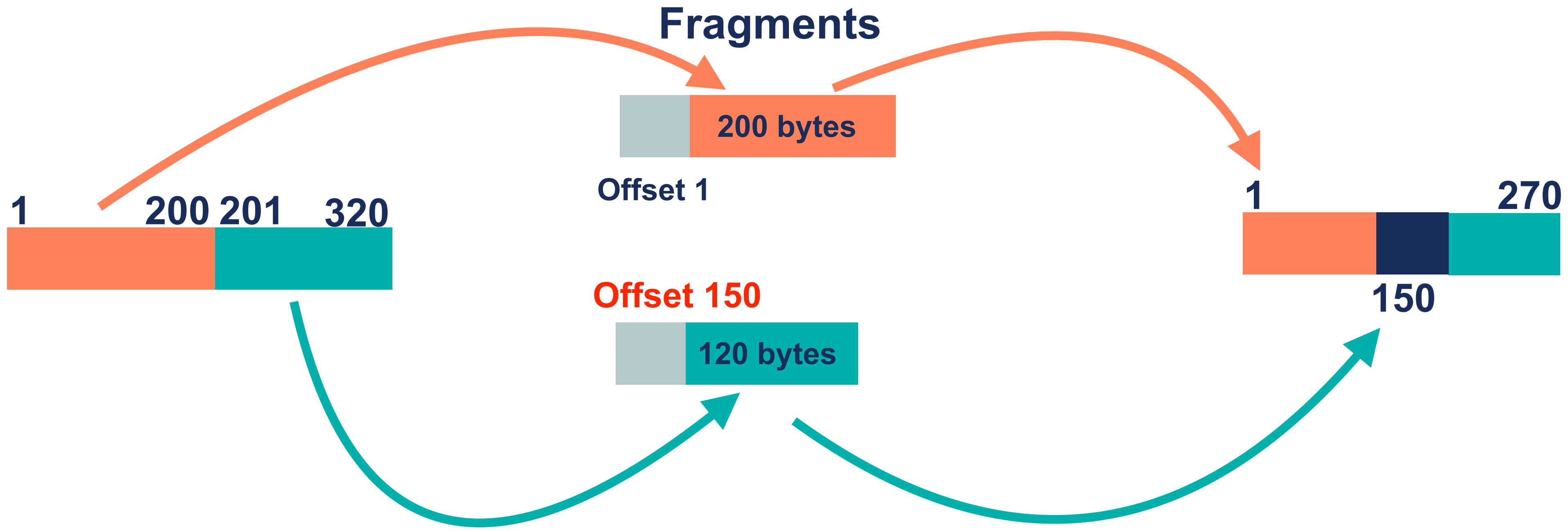


Extra: Overlapping Fragments

- Normal fragments offset say where the data goes:

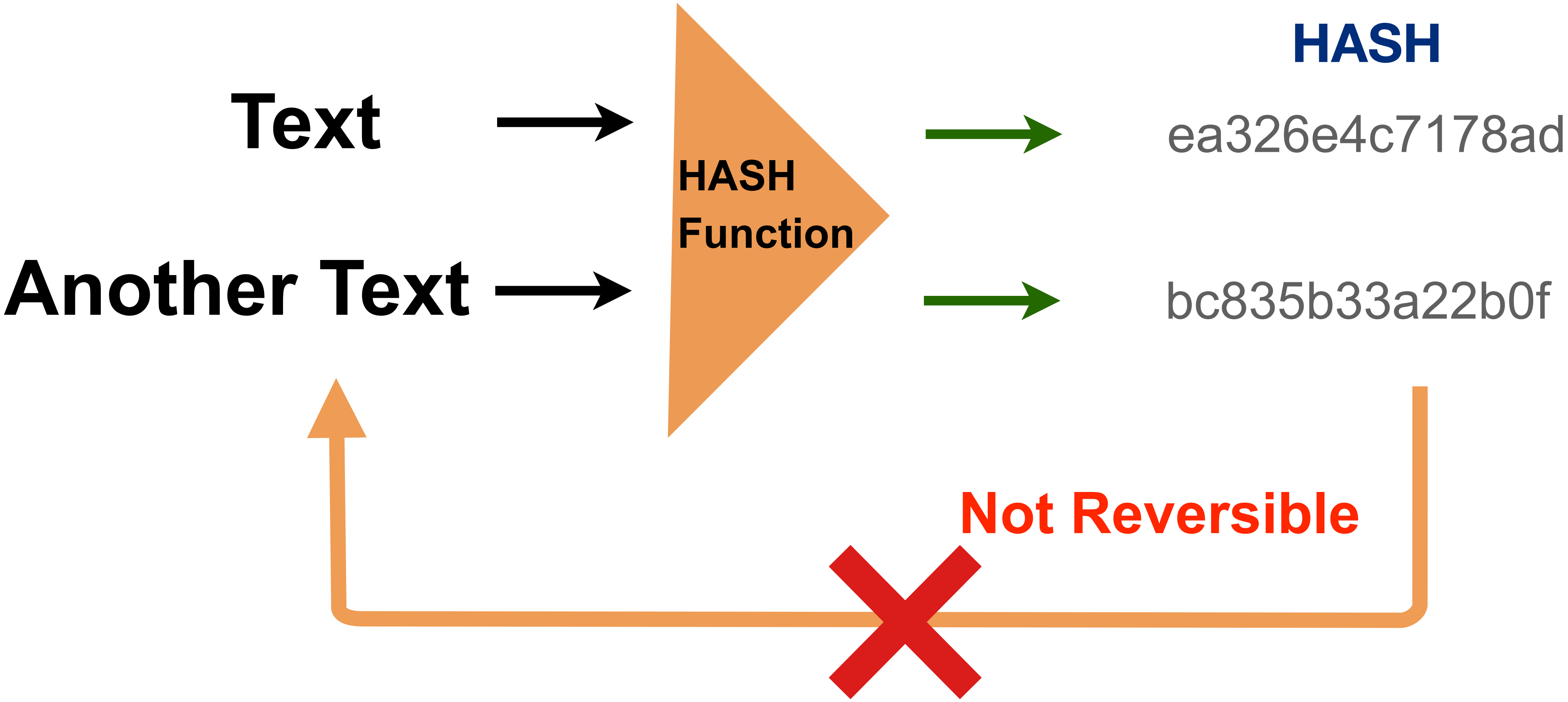


- Overlapping fragments have wrong offset values:



Extra: Hash Function

- Input: String
- Output: Fixed length series of characters


HASH
Text
ea326e4c7178ad
HASH
Function
Another Text
bc835b33a22b0f
Not Reversible