RIPE NCC
RIPE NETWORK COORDINATION CENTRE

Basic IPv6 Protocol Security

Webinar

RIPE NCC Learning & Development

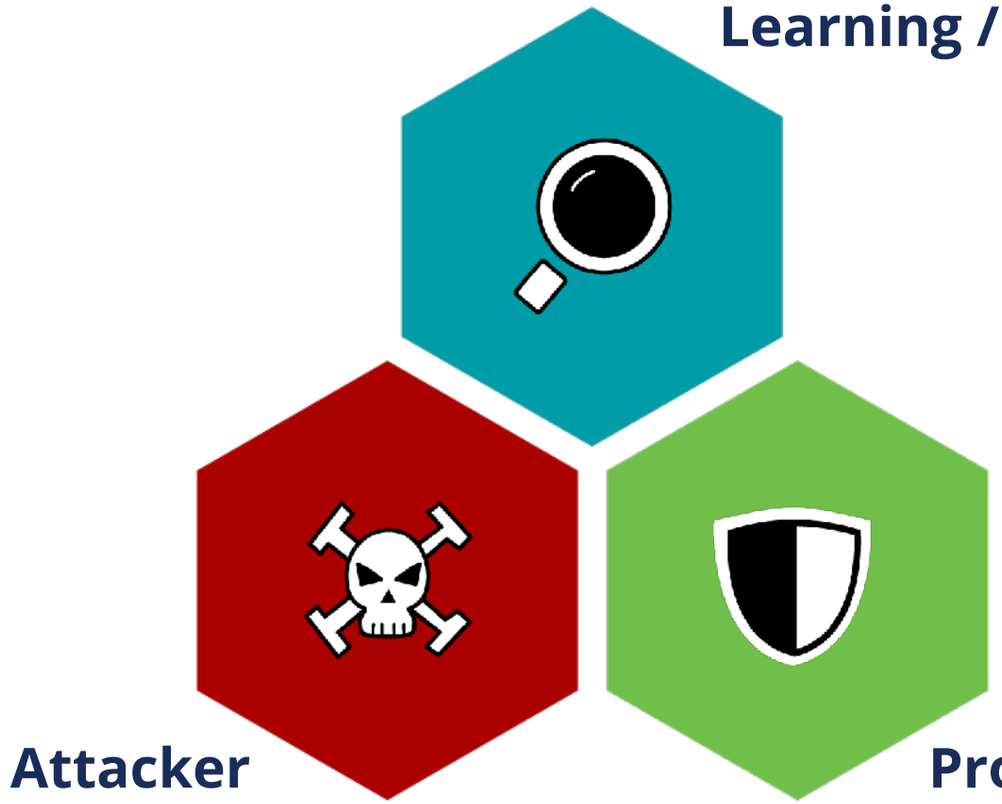
This webinar is being recorded

Basic IPv6 Protocol Security

IPv6 Basic header and Extension Headers

IPSec

IPv6 Security Addressing Architecture


Learning / Understanding
Attacker
Protecting

Tell us about you!

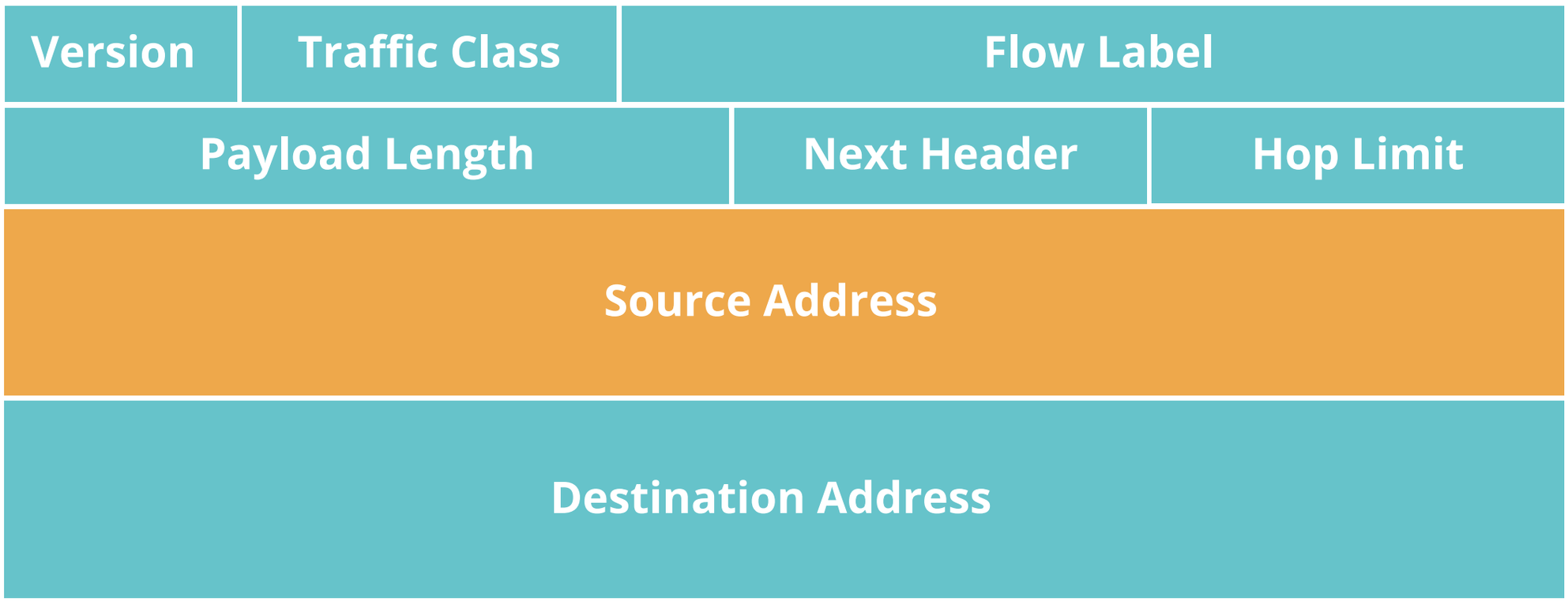
Please answer the polls

2 min.

IPv6 Basic Header and Extension Headers

Section 1

Basic IPv6 Header: Threat #1



Basic IPv6 Header: Threat #1

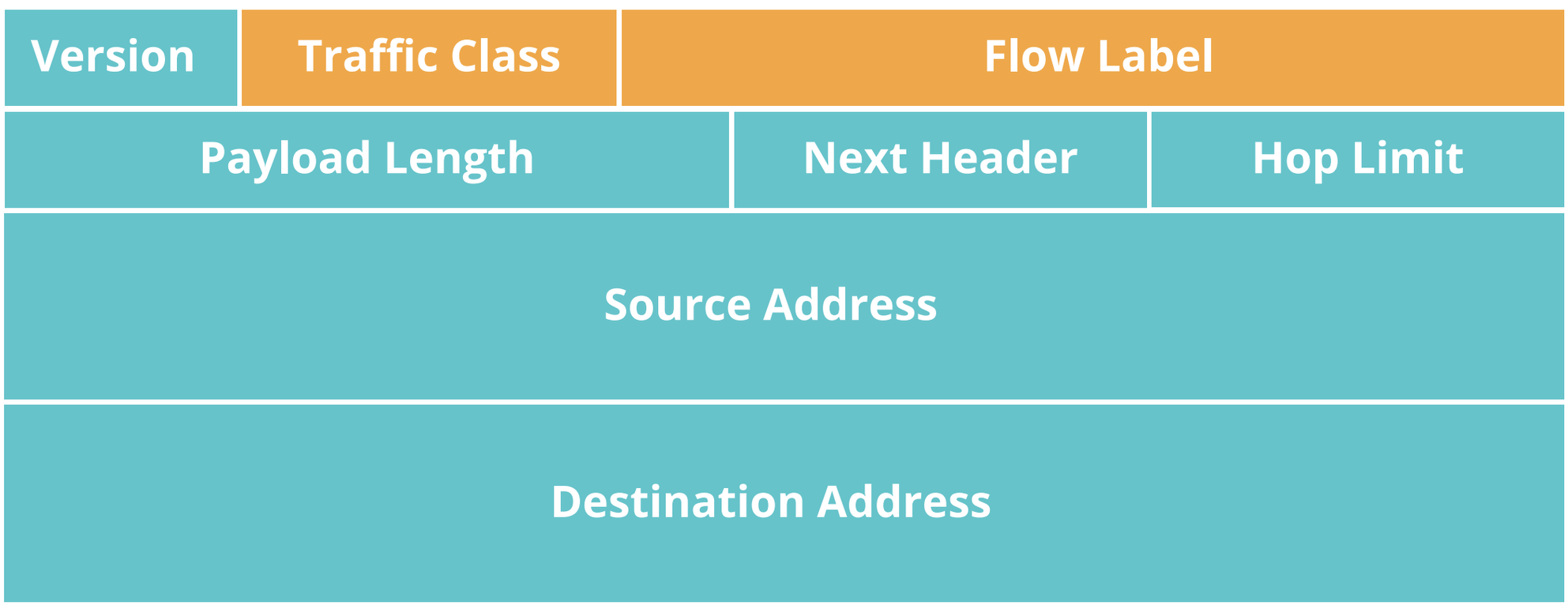
IP spoofing:

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

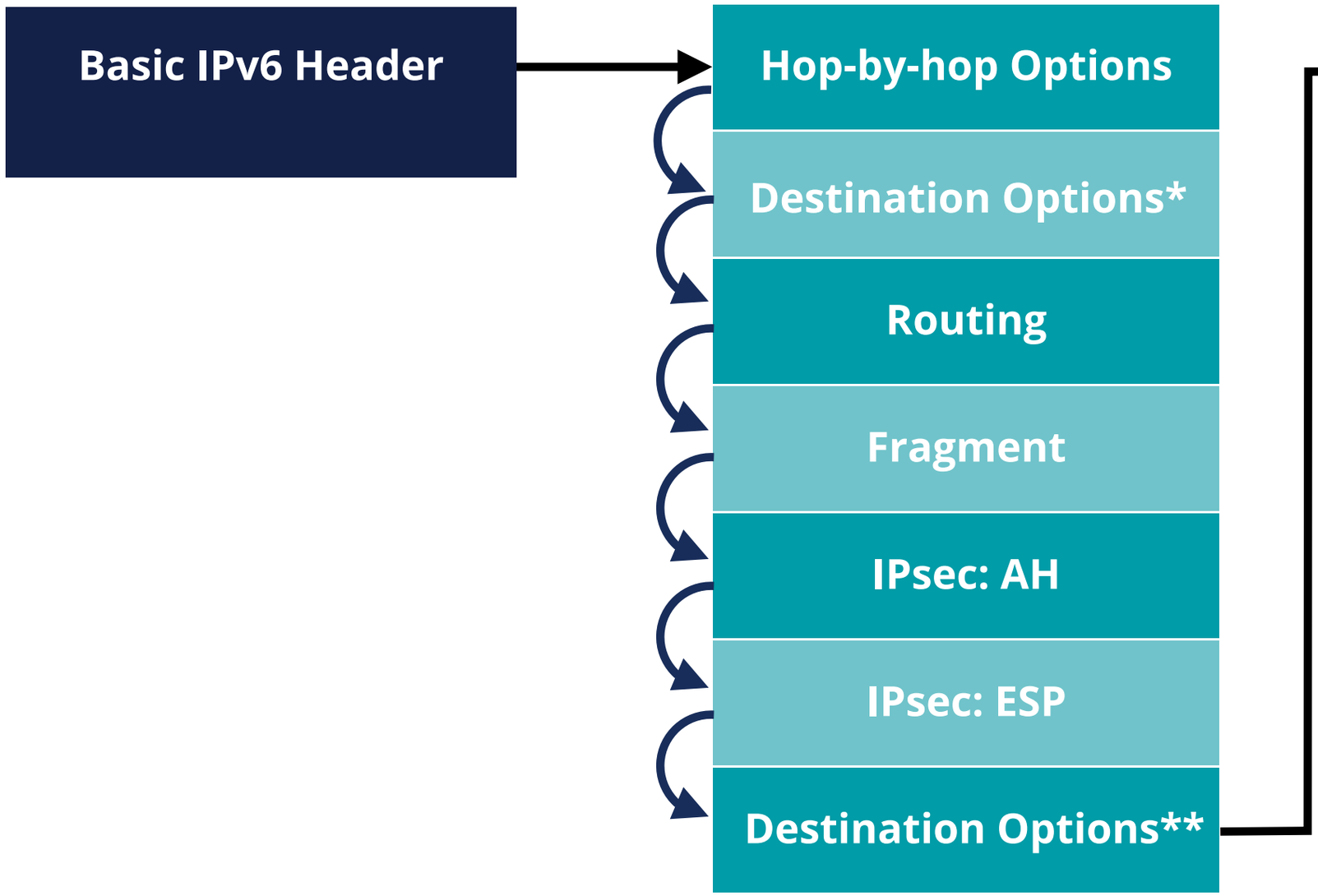
Solution:

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**

Questions

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

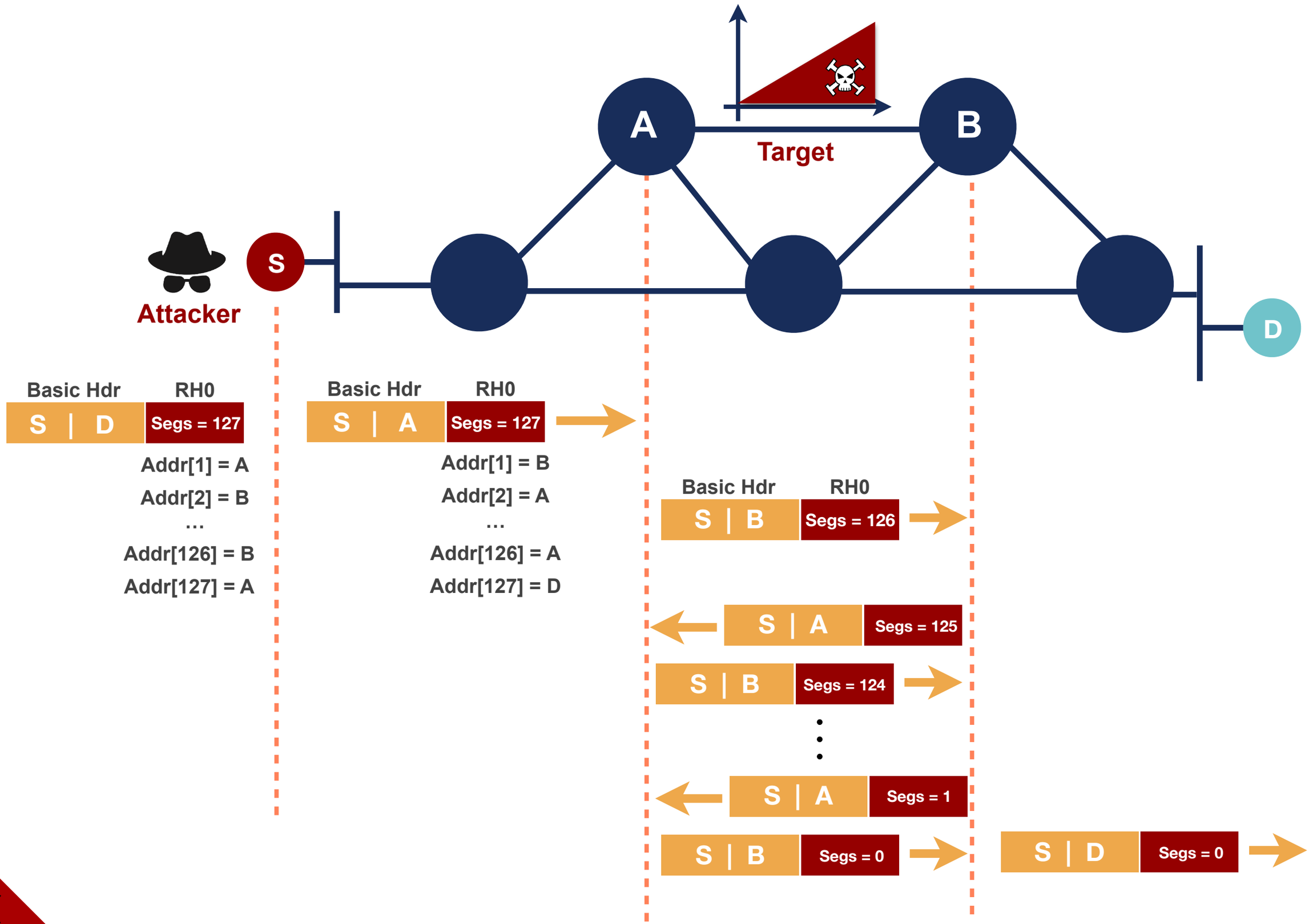
- **Routing Header** (**Type 0**):
  - RH0 can be used for traffic amplification over a remote path
- **RH0 Deprecated** [*RFC5095*]
  - RH1 deprecated. RH2 (MIPv6), RH3 (RPL) and RH4 (SRH) are valid

Take the poll!

What can **RH0** be used for?

Something bad?

2 min.

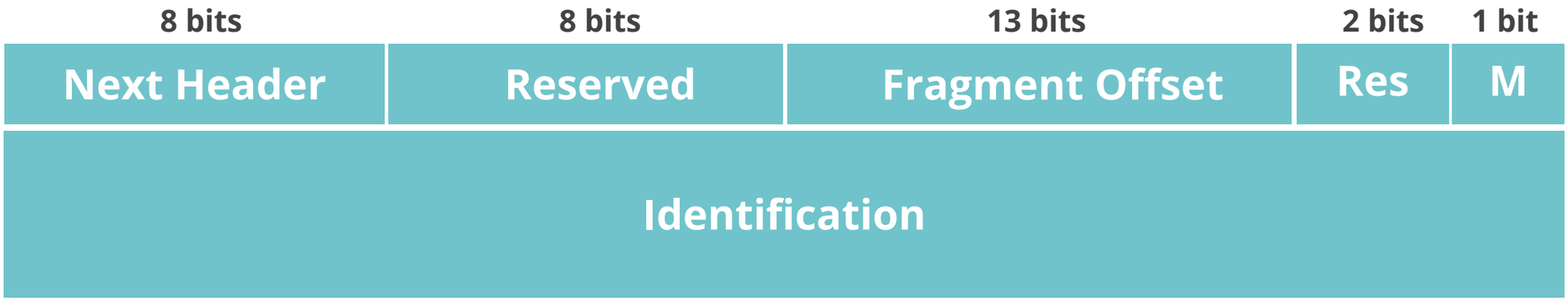

A
B
Target
S
Attacker
D
Basic Hdr
RH0
S | D
Segs = 127
Addr[1] = A
Addr[2] = B
...
Addr[126] = B
Addr[127] = A
Basic Hdr
RH0
S | A
Segs = 127
Addr[1] = B
Addr[2] = A
...
Addr[126] = A
Addr[127] = D
Basic Hdr
RH0
S | B
Segs = 126
S | A
Segs = 125
S | B
Segs = 124
S | A
Segs = 1
S | B
Segs = 0
S | D
Segs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

Extension Headers Solutions

- 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



M Flag:

1 = more fragments to come;

0 = last fragment

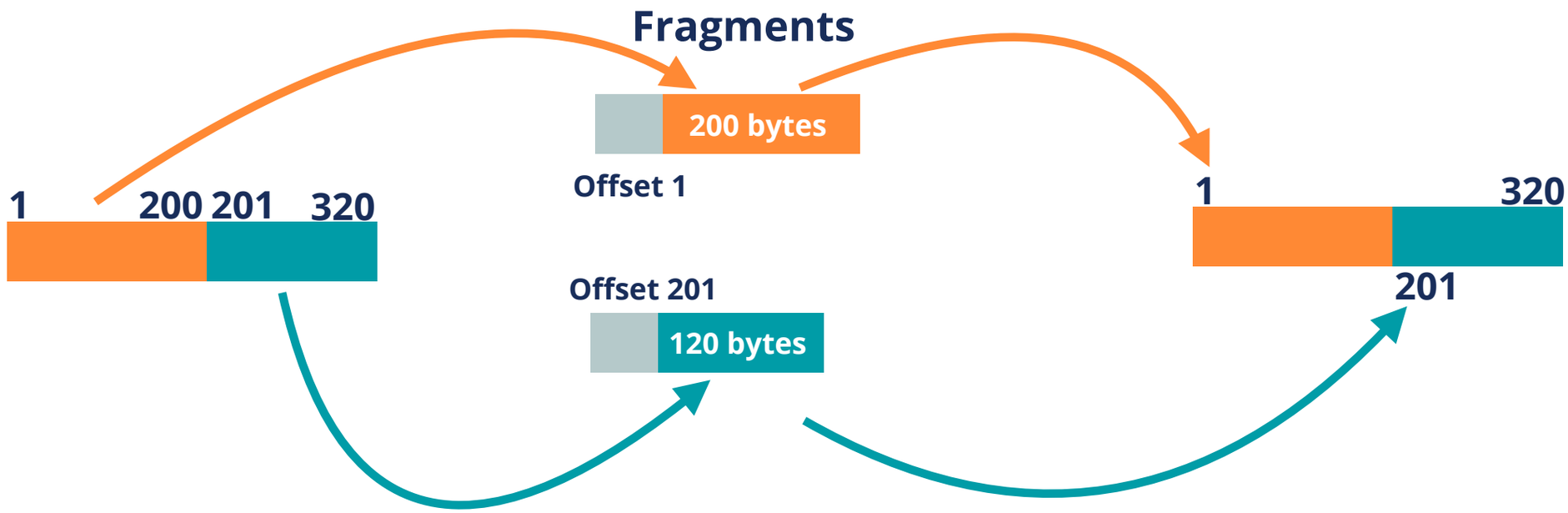
EH Threats: Fragmentation

Take the poll!

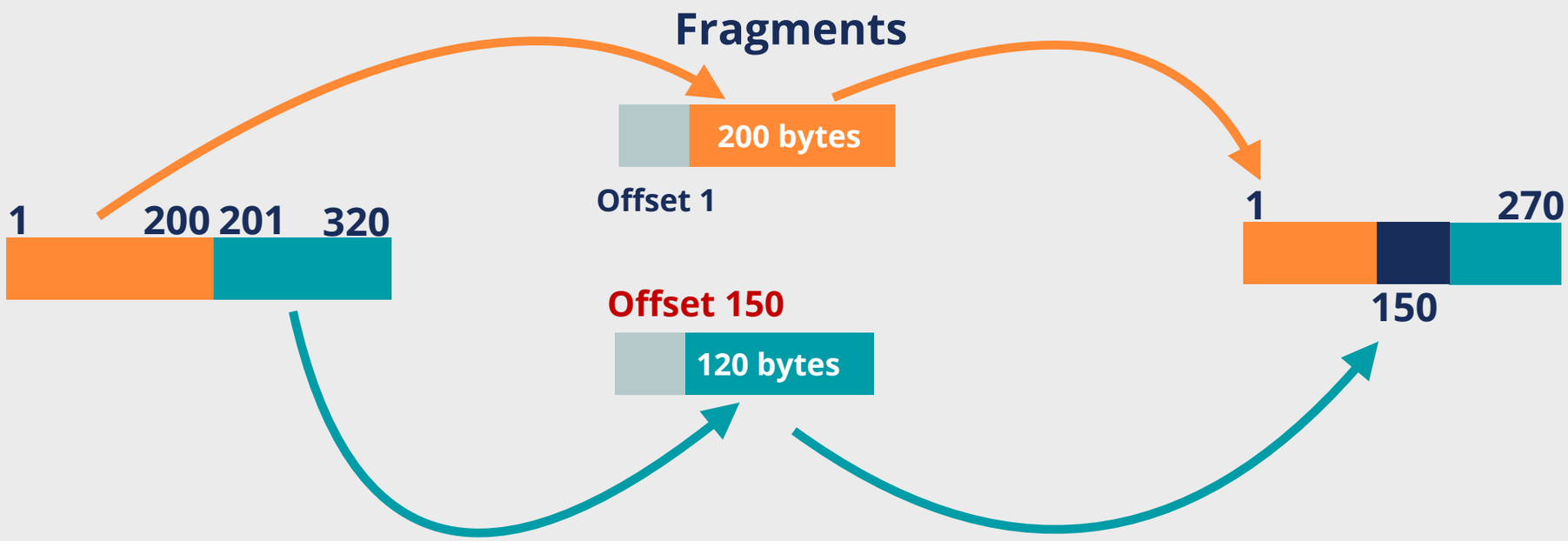
Do you know how **Overlapping Fragments** works?

2 min.

Overlapping Fragments

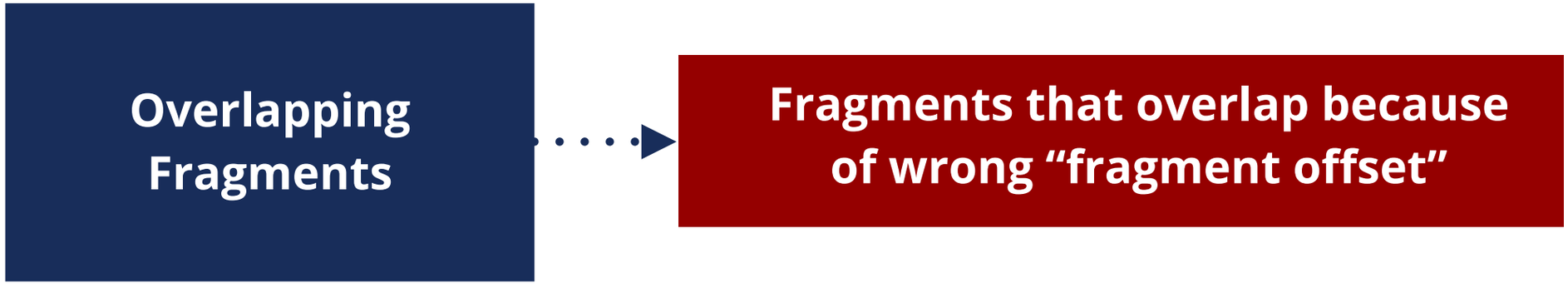


Normal fragments offset say where the data goes



Overlapping fragments have wrong offset values

EH Threats: Fragmentation



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]**

Take the poll!

For what other malicious attacks can **Extension Headers** be used for?

2 min.

Bypassing RA Filtering/RA-Guard

Using **any** Extension Header

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

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*	

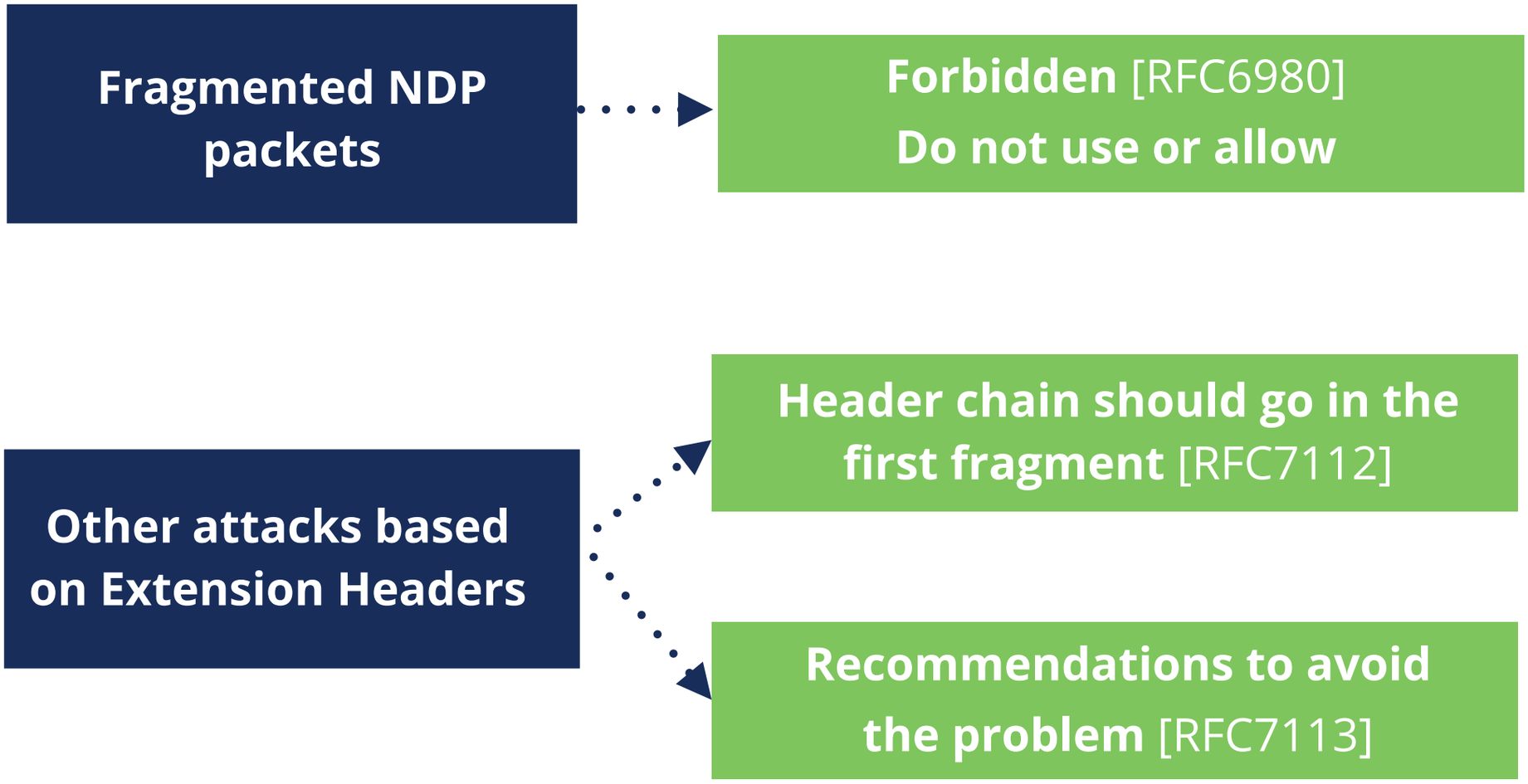
Needs all fragments to detect the RA

Take the poll!

How would you change IPv6 to **avoid** the **bypass using fragment header**?

2 min.

Extension Headers Solutions



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

Questions

- Is it possible to **generate** all those weird packets?

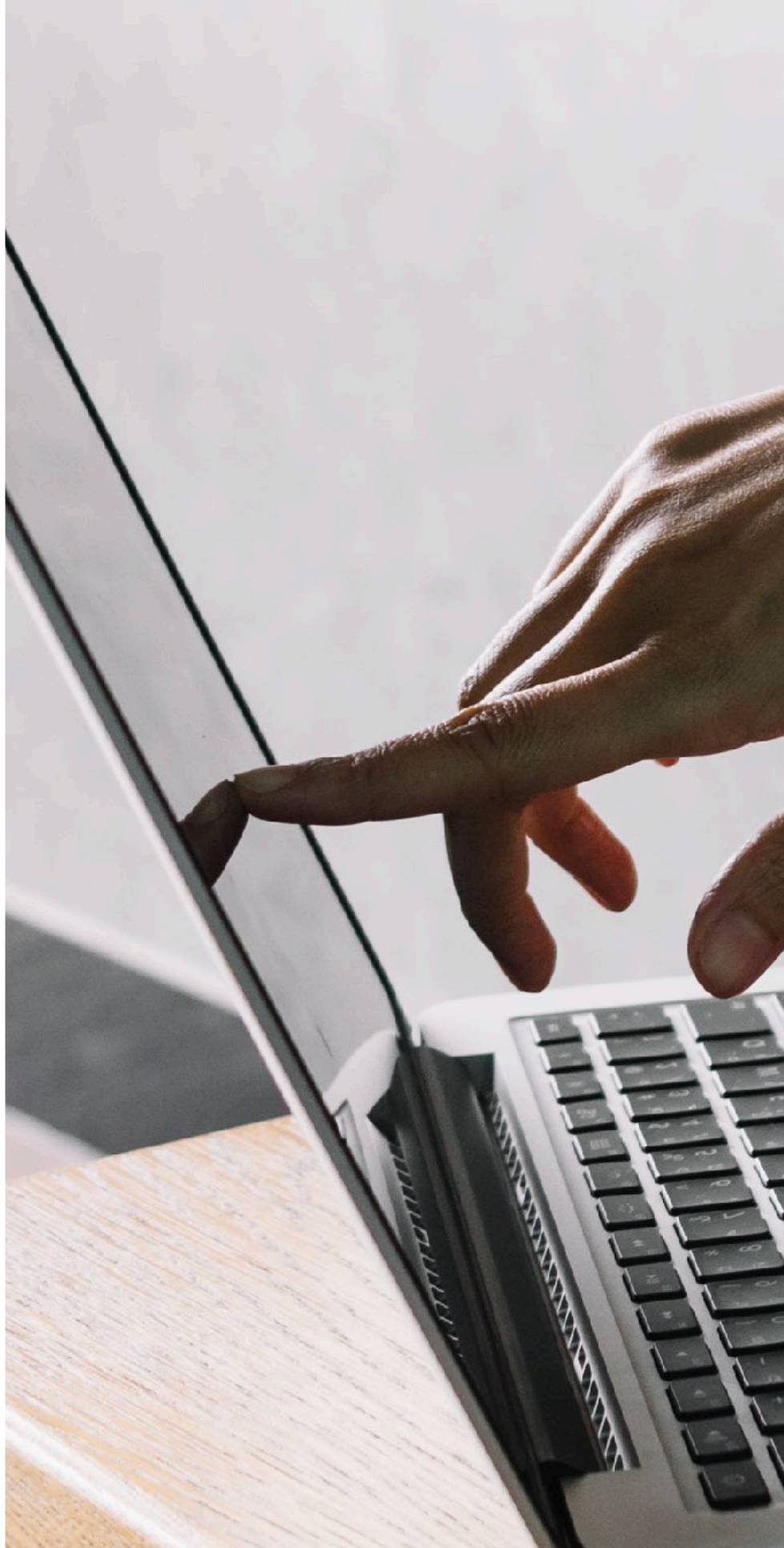
- How can I check if my devices/ software are **ready to resist** specific attacks? (Security assessment)?

Demo 1

IPv6 Packet Generation

Demo time!

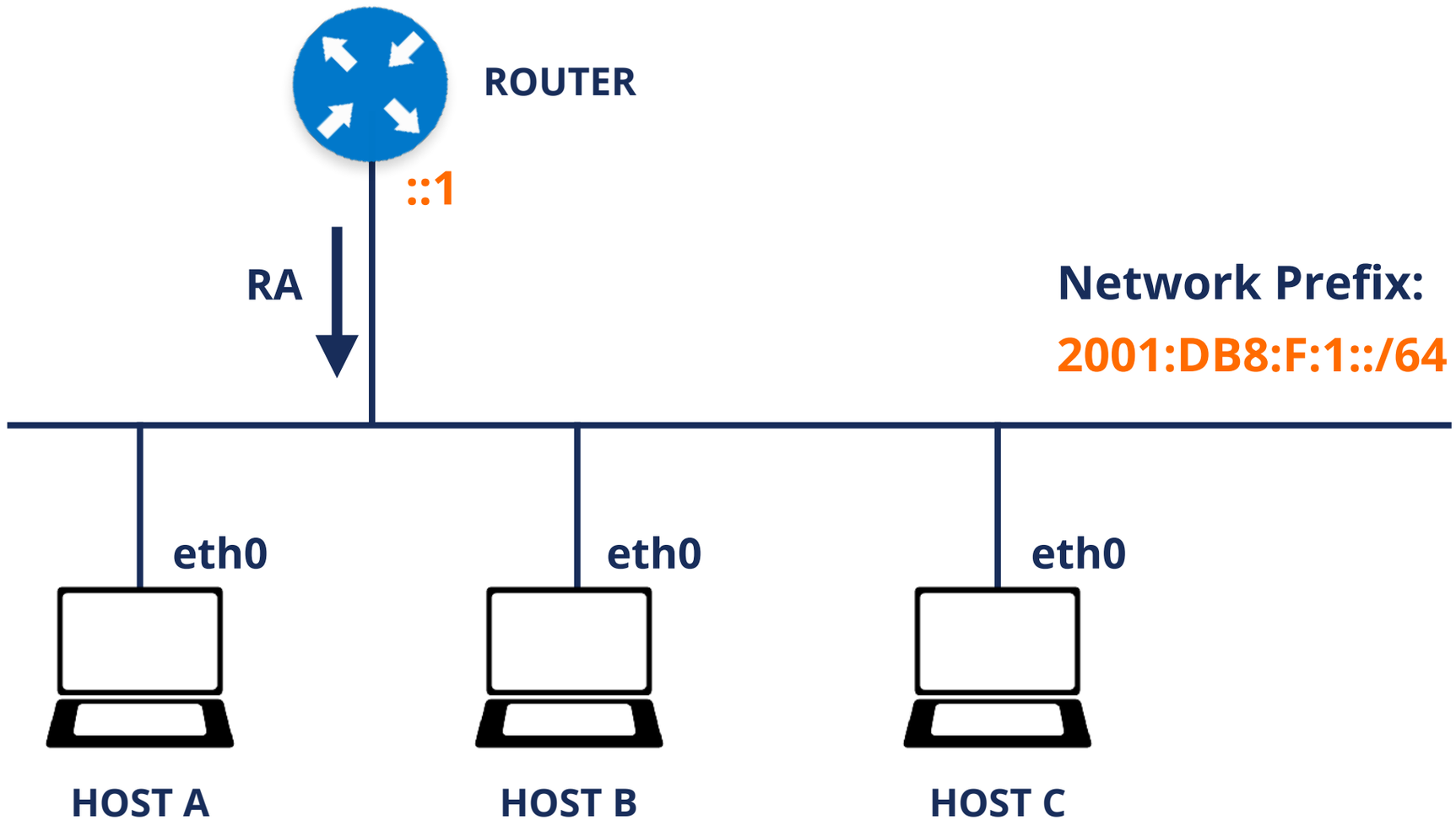
We will demo the activity on the screen.
Watch what we do.



Demo 1: IPv6 Packet Generation

- **Description**: Use **Scapy** to generate IPv6 packets
- **Goals**:
  - Know about the Scapy tool (http://secdev.org/projects/scapy/)
  - Learn about some of the capabilities of Scapy
- **Time**: 10 minutes
- **Demo**:
  - Generate IPv6 packets
  - Send and receive IPv6 packets

Demo 1 Lab Network



Network Prefix:

2001:DB8:F:1::/64

Questions

Let’s take a **5 minutes** break!

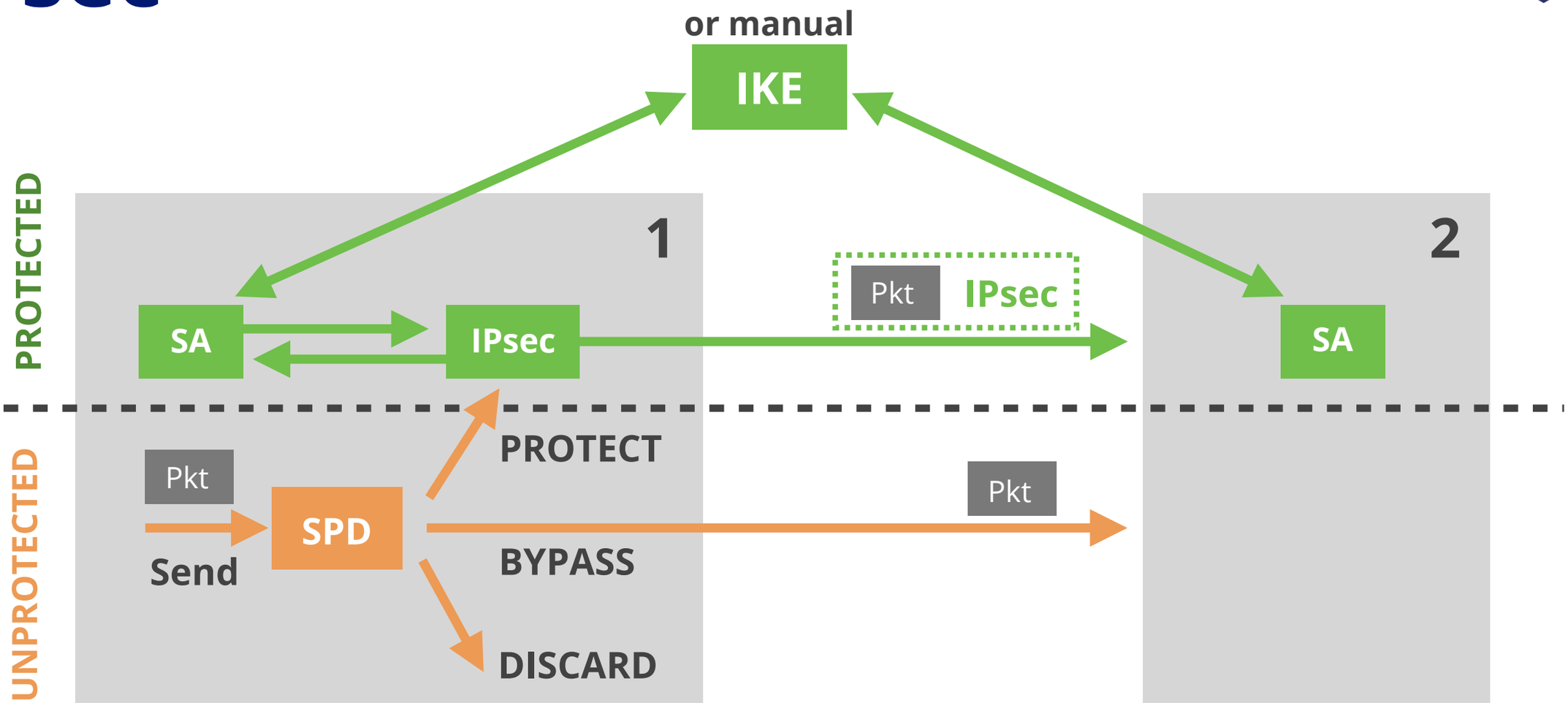

WELCOME
WE ARE
OPEN
PLEASE COME IN

IPSec

Section 2

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

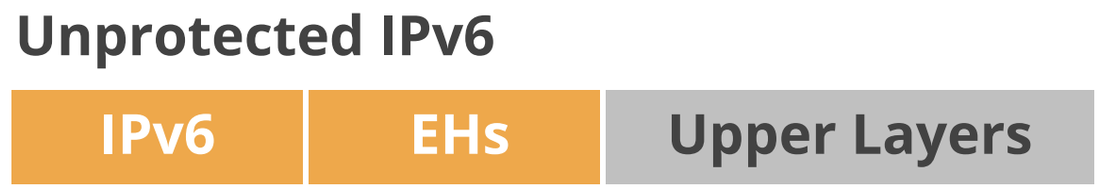
IKE **Internet Key Exchange** allows automatic creation of SAs

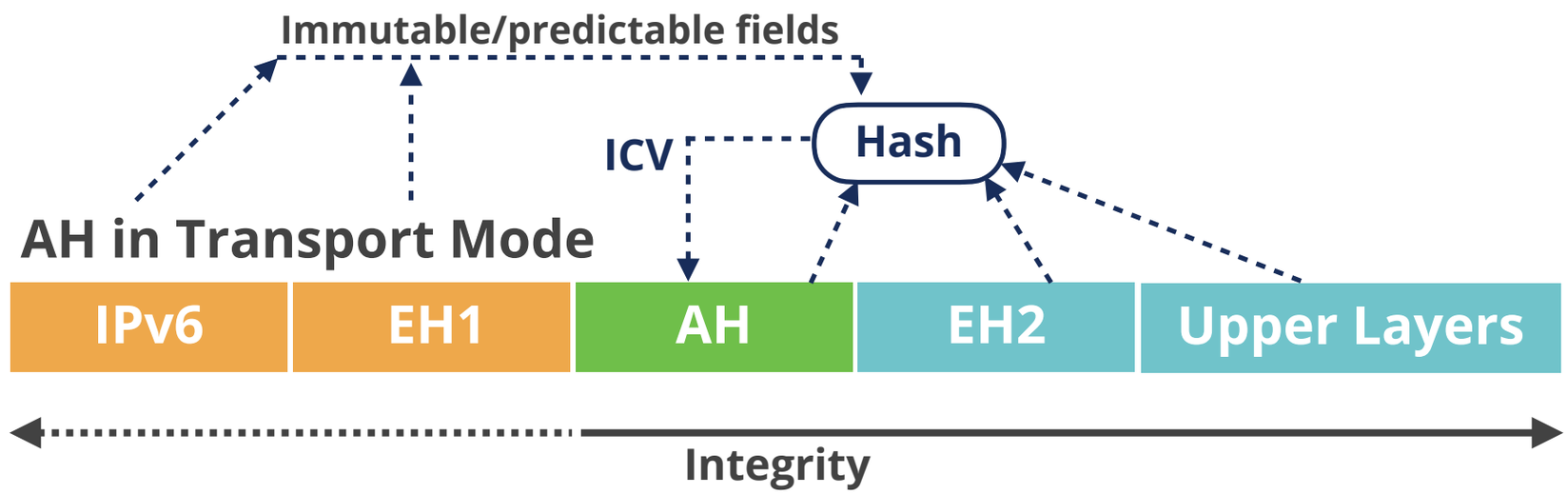
IPsec Modes

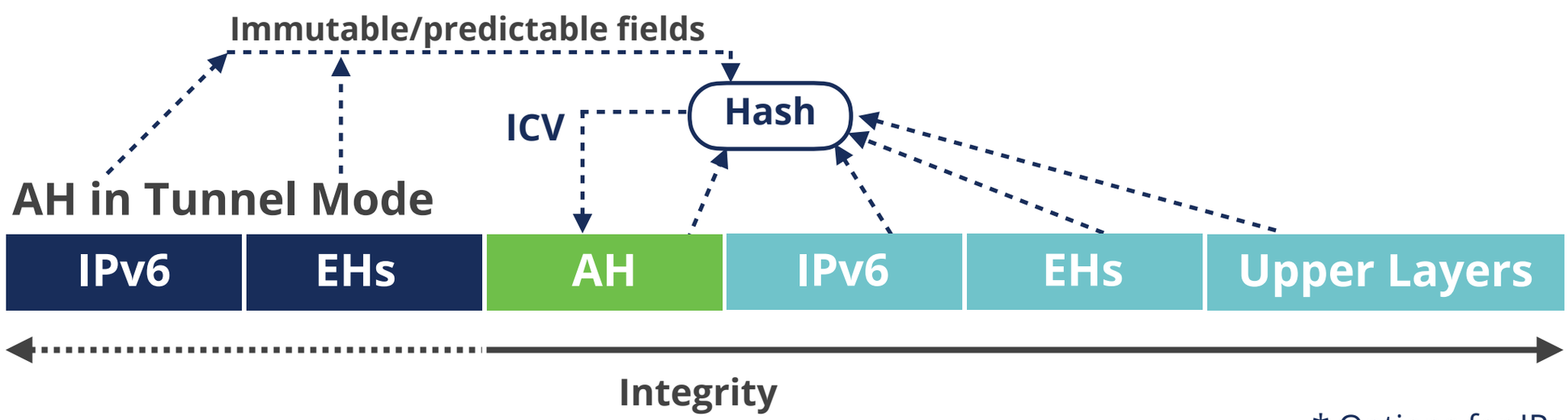
Tunnel Mode

Transport Mode

IPsec: Authentication Header







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

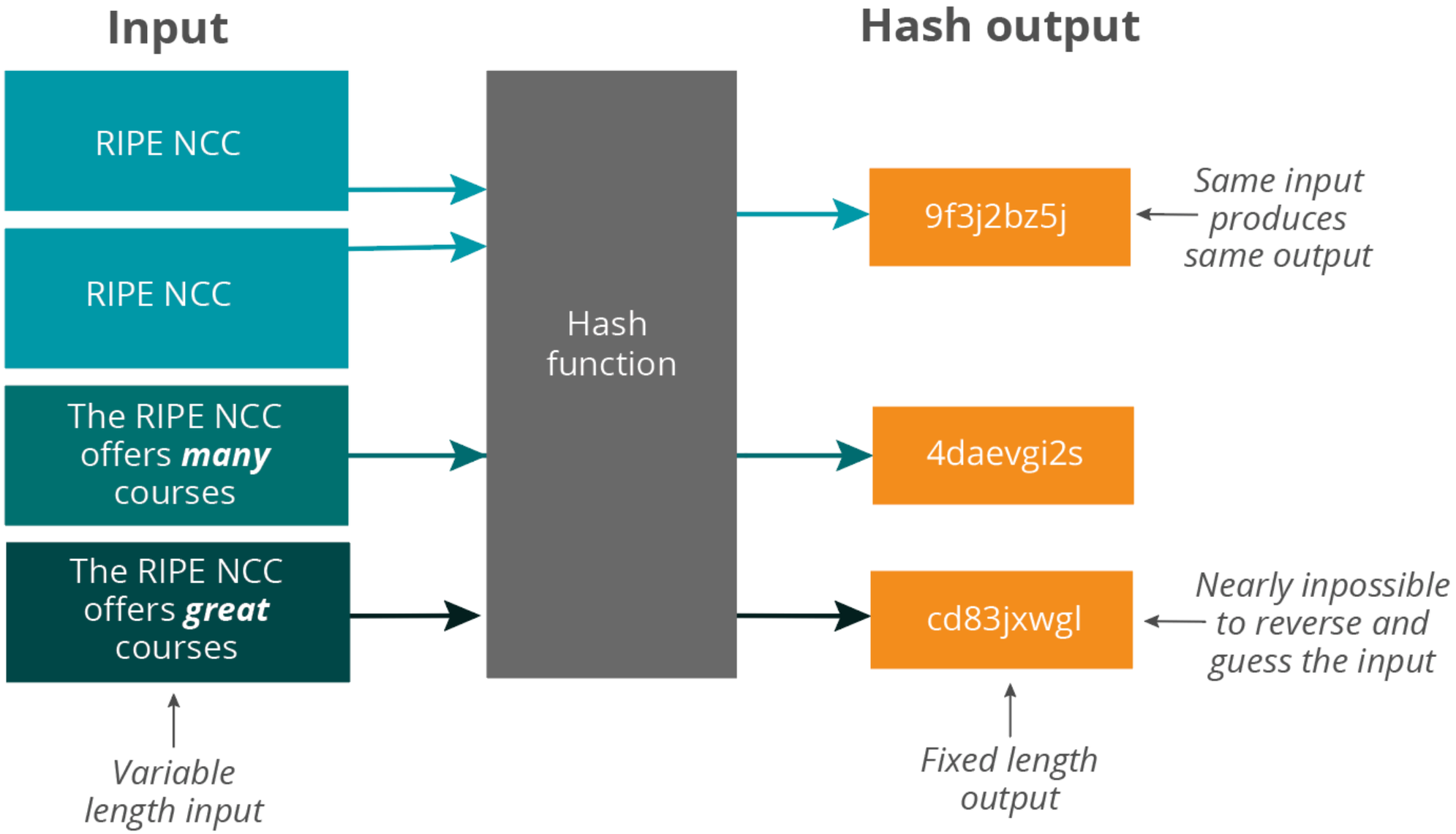
EH2 = Destination Options**

* Options for IPs in routing header

** Options for destination IP

Hash Function

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



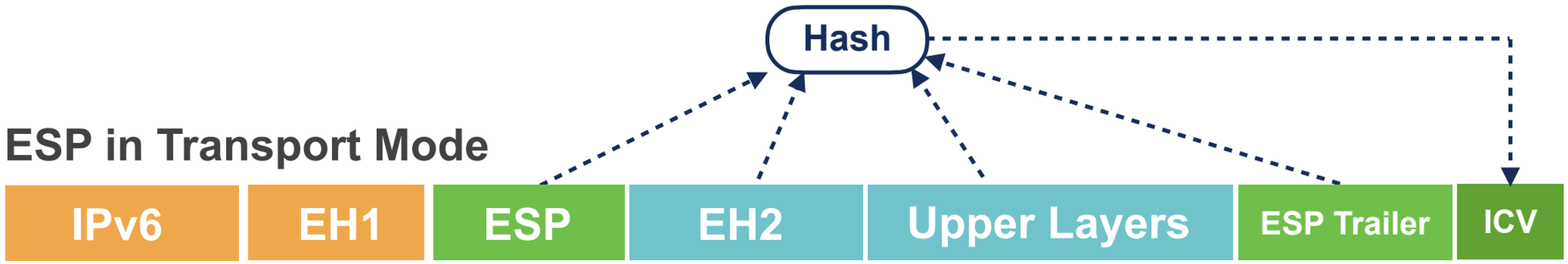
IPsec: ESP

Unprotected IPv6

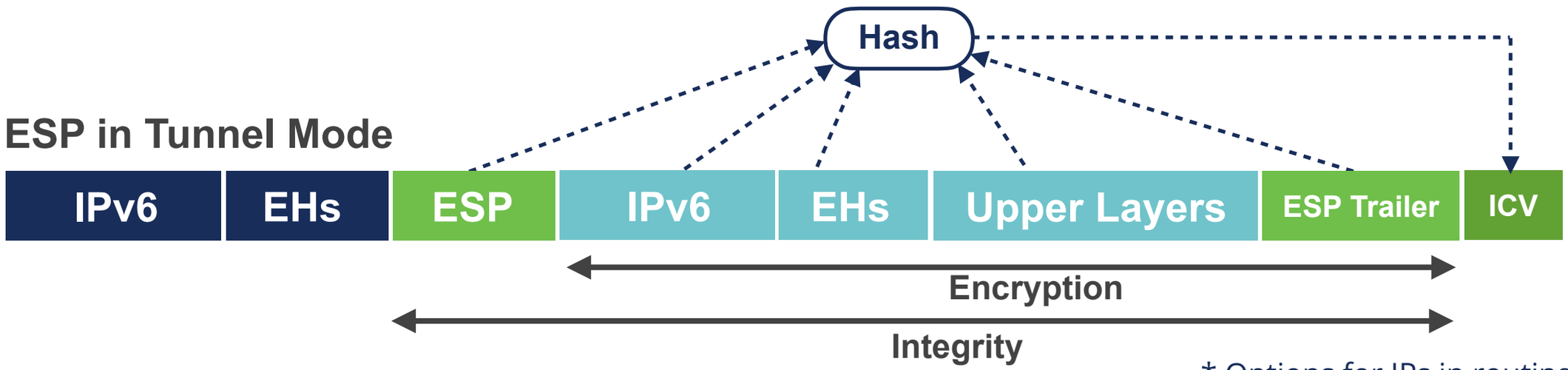
EH1 = Hop-by-Hop,
Dest. Options*,
Routing, Fragment

EH2 = Destination Options**

ESP in Transport Mode



ESP in Tunnel Mode



* Options for IPs in routing header

** Options for destination IP

Take the poll!

How is the **ICV** (**Integrity Check Value**) used in **IPsec** to provide integrity?

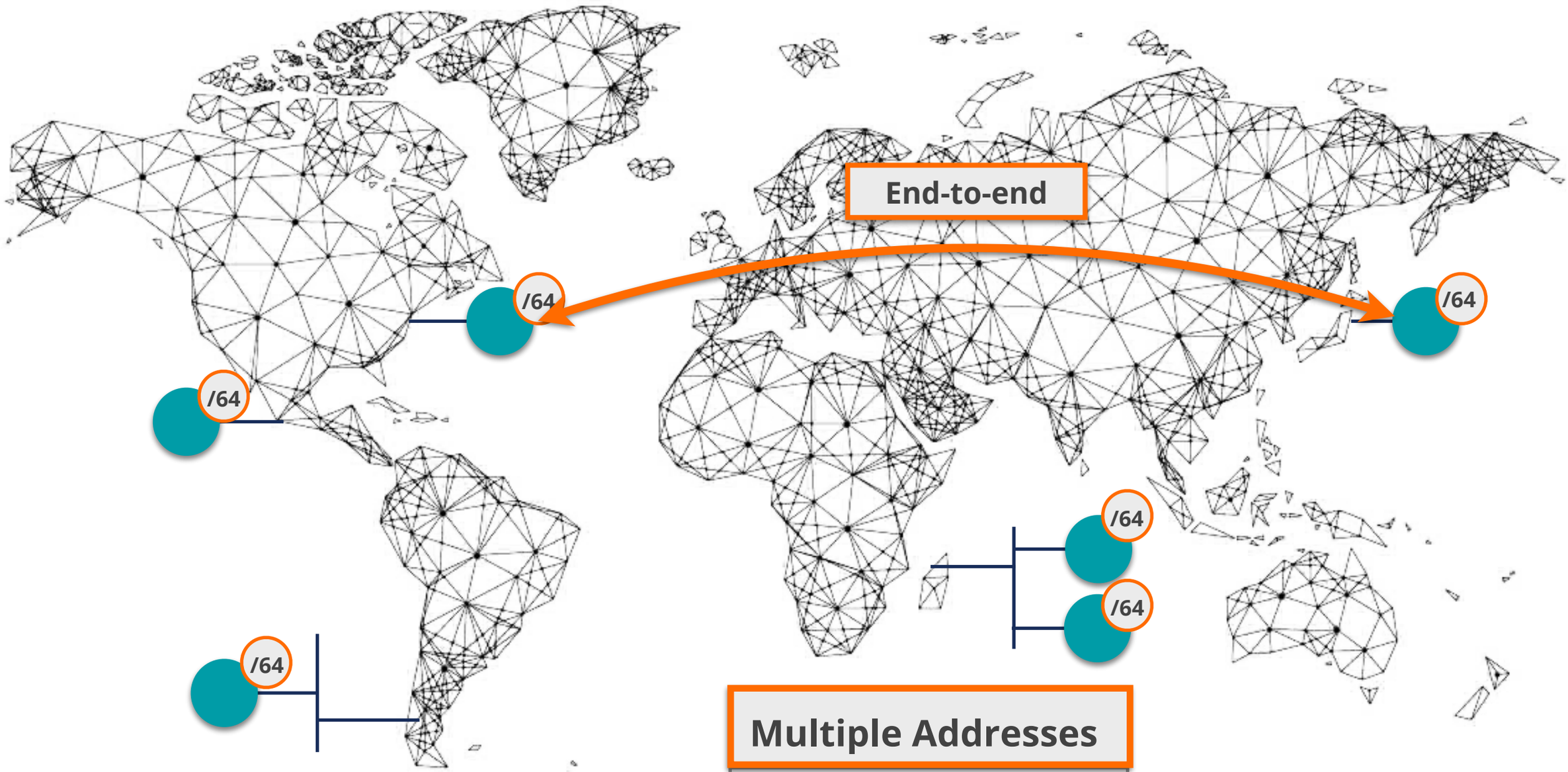
2 min.

Questions

IPv6 Addressing Architecture

Section 3

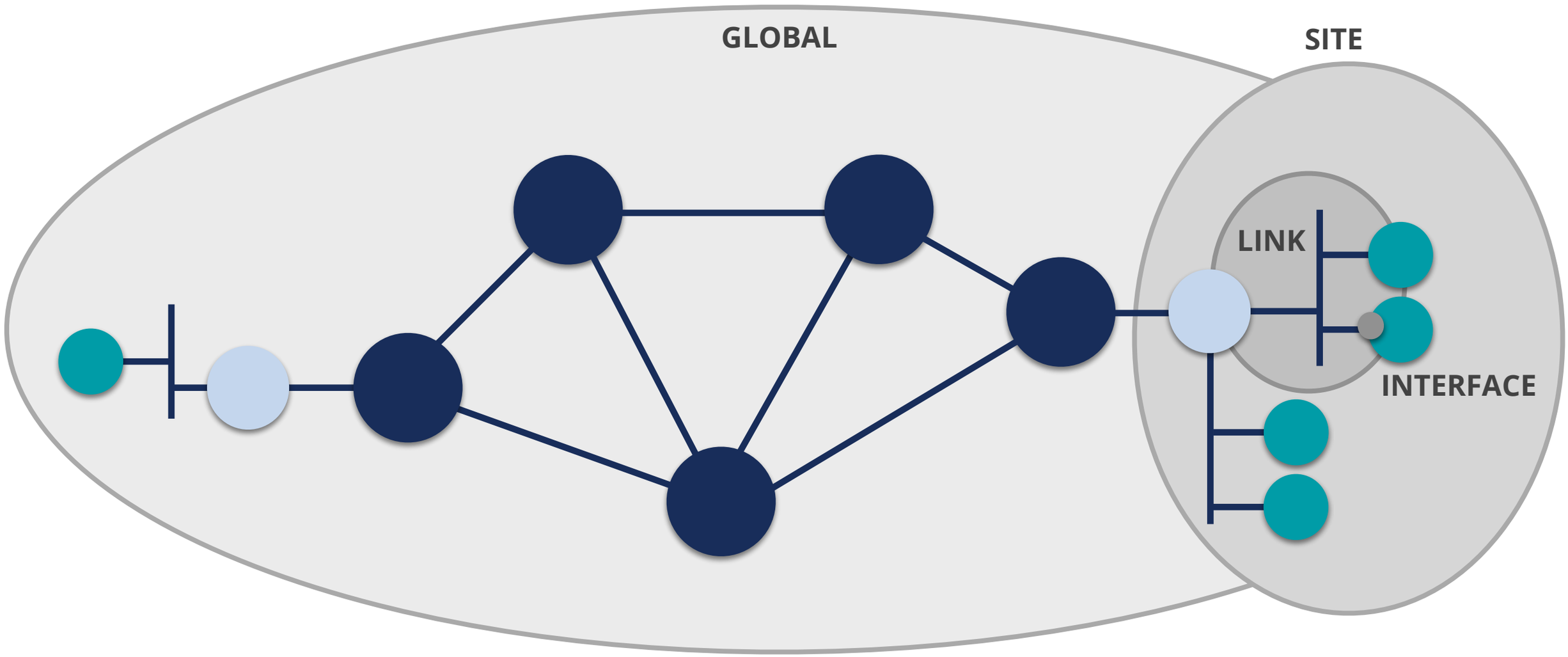
340,282,366,920,938,463,463,374,607,431,768,211,456



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

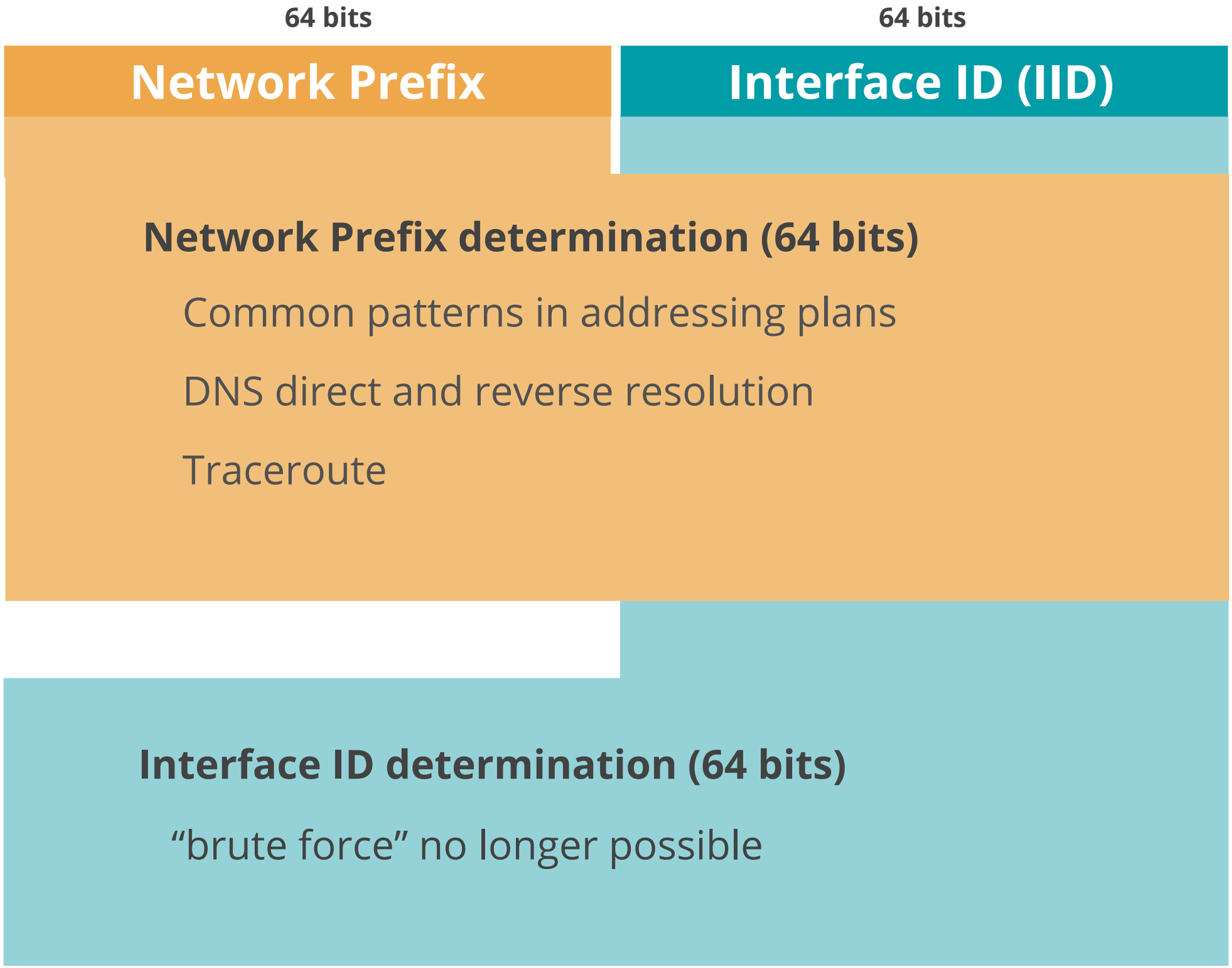
Take the poll!

What is the **scope** of the following IPv6 address?

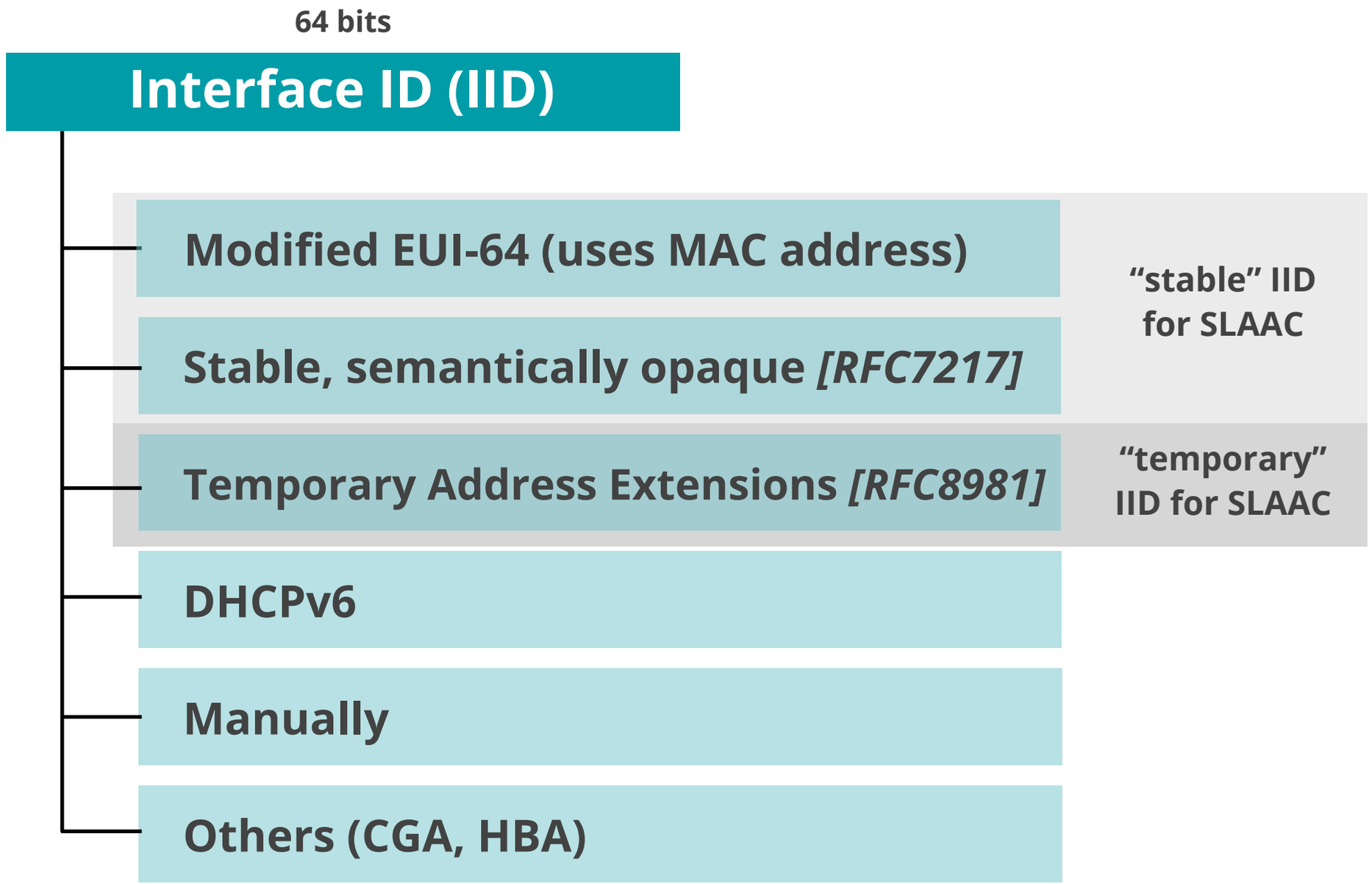
fe80::0123:aff:ad34

2 min.

IPv6 Network Scanning



IID Generation Options



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

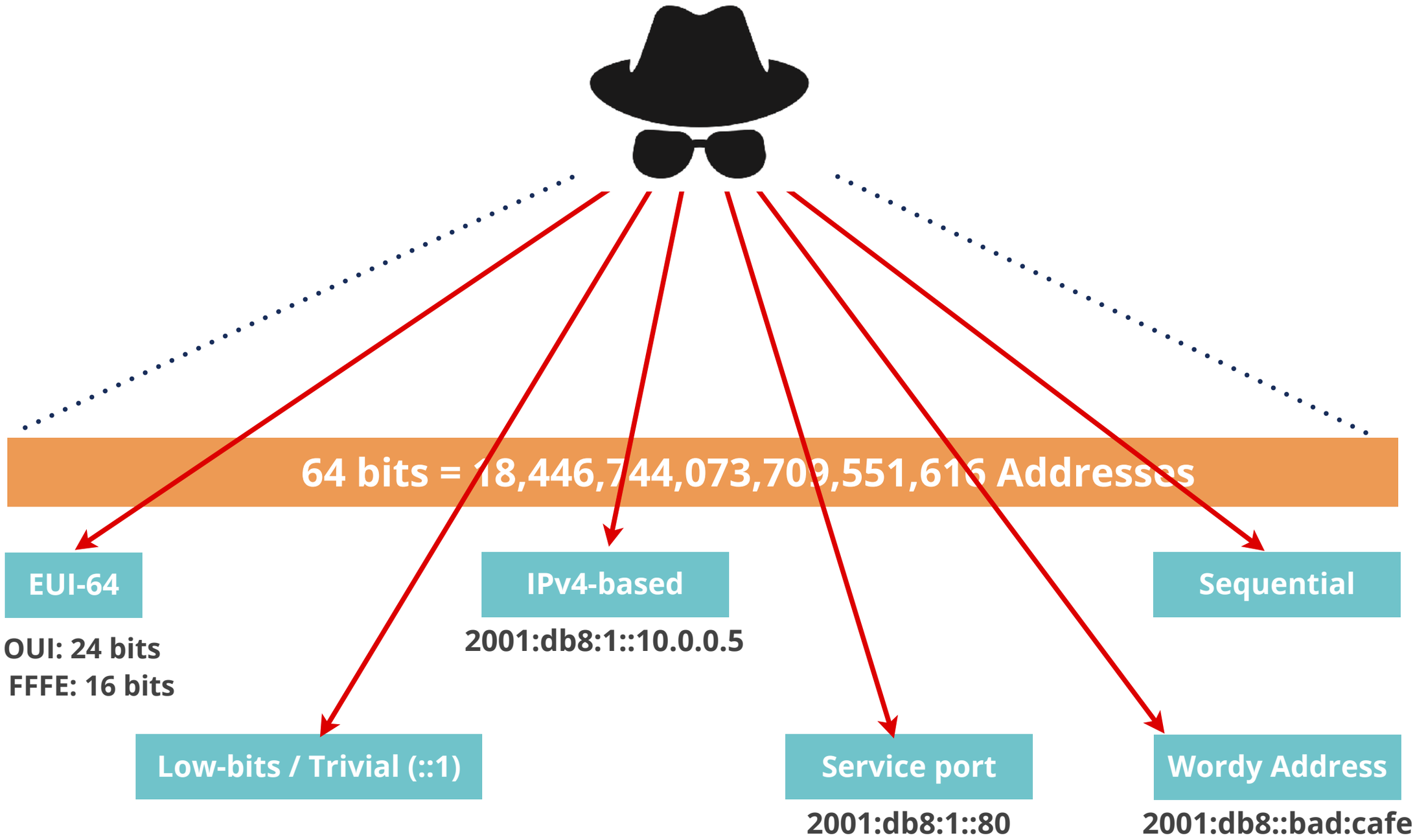
- **Widely used** and **standardised** for “stable” addresses *[RFC8064]*

Take the poll!

How can the **EUI-64** make it easier to guess an **IID**?

2 min.

Guessing IIDs

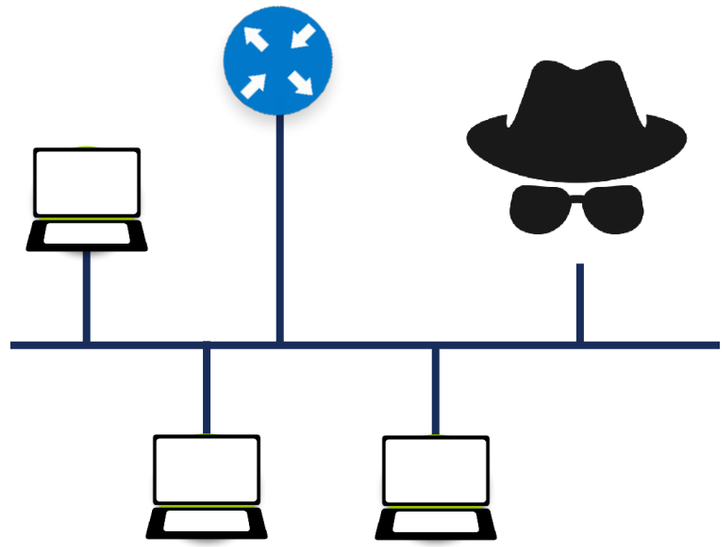


Take the poll!

Why is a **Dual-Stack network** easier to scan?

2 min.

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 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

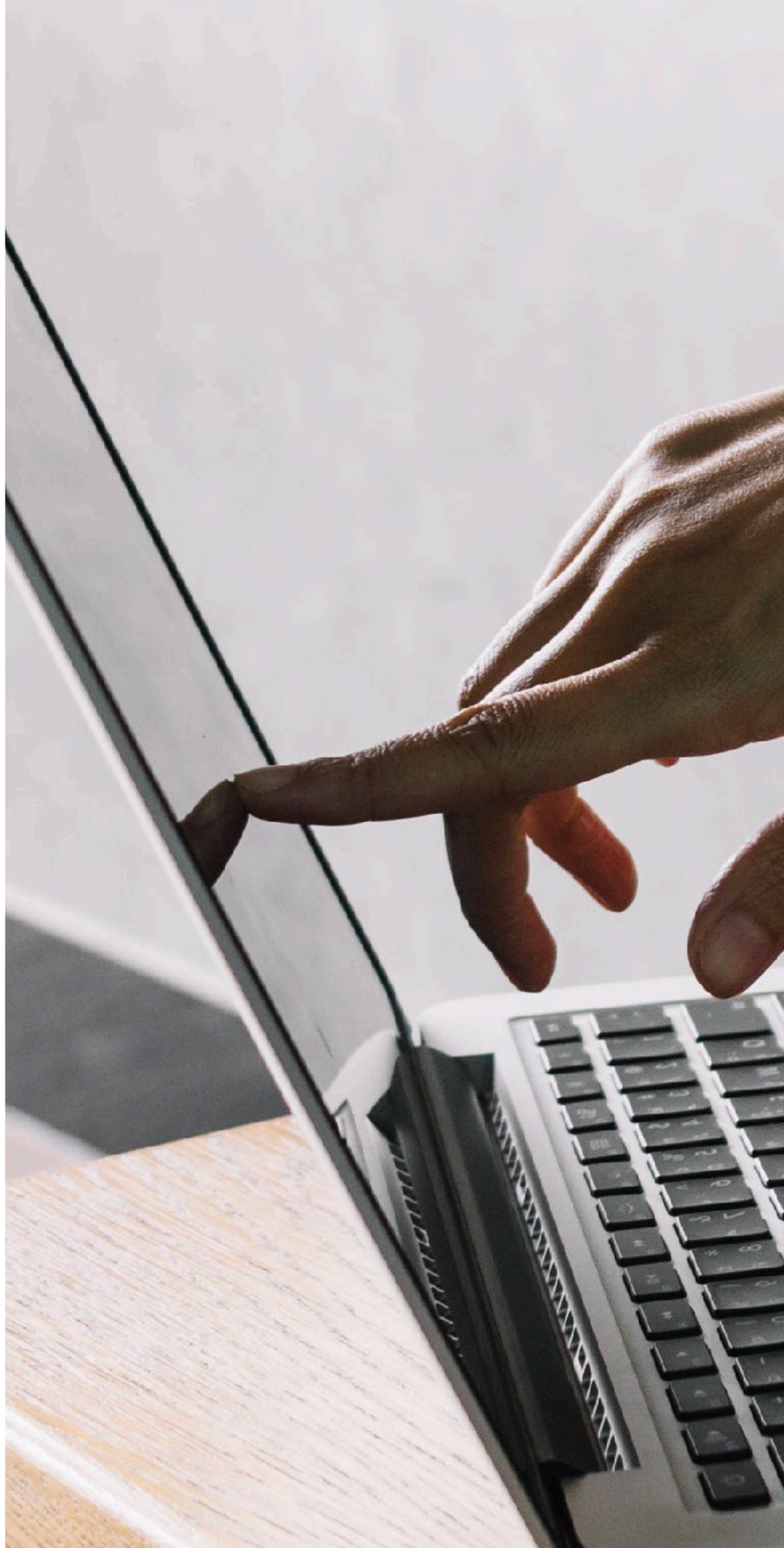
- Is it easy to **scan** an IPv6 network?

Demo 2

IPv6 Network Scanning

Demo time!

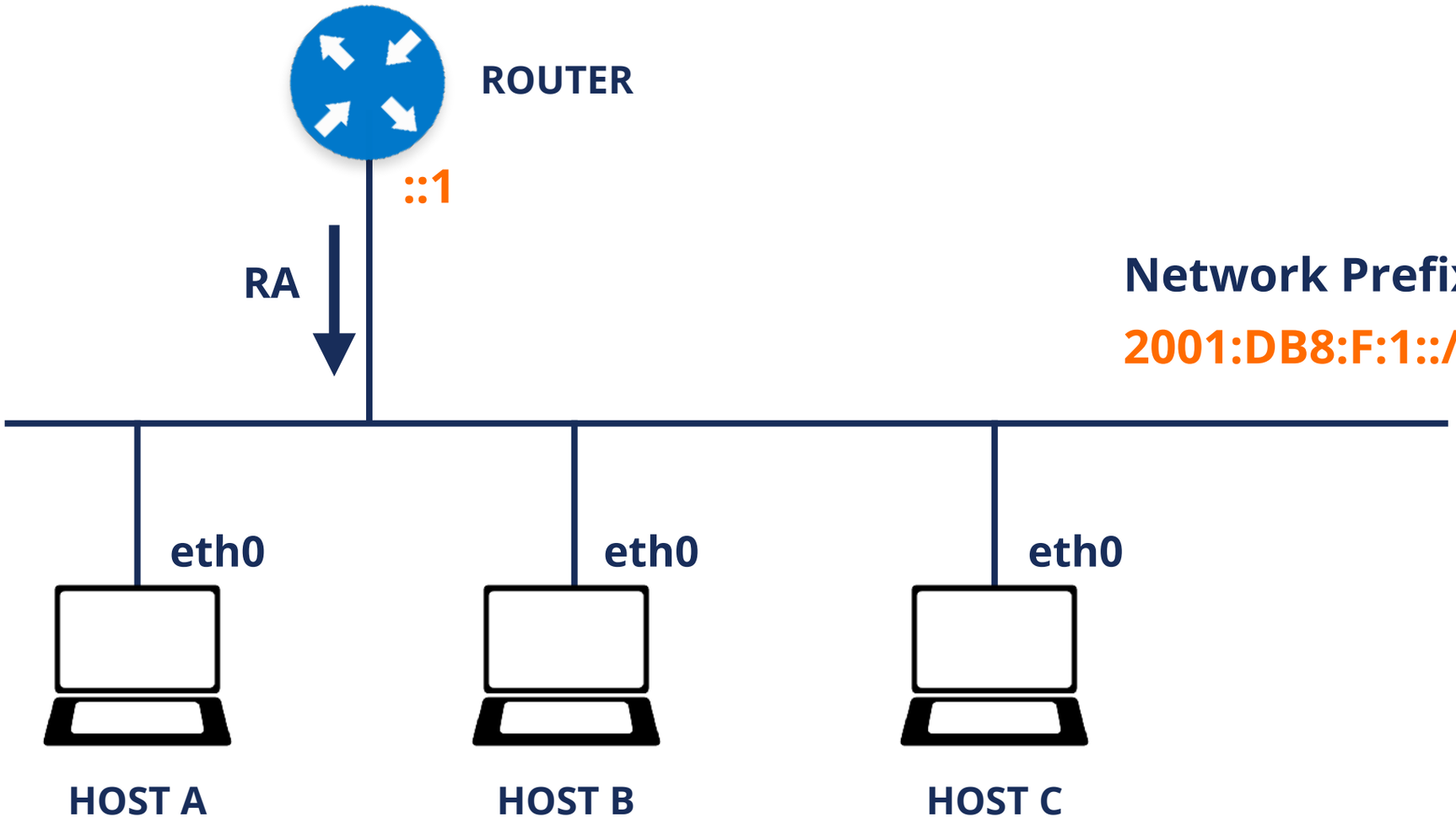
We will demo the activity on the screen.
Watch what we do.



Demo 2: IPv6 Network Scanning

- **Description**: Use available toolsets to scan a subnet
- **Goals**:
  - Know about two toolsets:
  - **THC-IPV6** (https://github.com/vanhauser-thc/thc-ipv6)
  - **The IPv6 Toolkit** (https://www.si6networks.com/tools/ipv6toolkit/)
  - Learn which tool they have to scan a link
- **Time**: 5-10 minutes
- **Demo**:
  - Use The IPv6 Toolkit to scan a subnet
  - Use THC-IPV6 to scan a subnet

Demo 2 Lab network



Network Prefix:

2001:DB8:F:1::/64

Take the poll!

Why do you think **alive6** only finds **global** addresses and **scan6** also finds the **link-local** addresses?

2 min.

What Have We Seen?

Basics of IPv6 brings some security considerations

- **Same as in IPv4: IP spoofing, covert channel, or even IPsec**
- **New in IPv6: Extension headers, new addressing scheme, new scanning techniques**

There are tools that allow security assessment of IPv6 networks

- **Scapy**
- **THC-IPV6**
- **The IPv6 Toolkit**

Take the poll!

Think of what you learned in this webinar.

What things can you apply or use in **your own network**?

2 min.

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 webinar?

Take our survey at:

https://www.ripe.net/feedback/ipv6s1

RIPE NCC
Academy

Learn something new today!

academy.ripe.net

RIPE NCC Certified Professionals

https://getcertified.ripe.net/


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

Copyright Statement

[...]

The RIPE NCC Materials may be used for **private purposes, for public non-commercial purpose, for research, for educational or demonstration purposes**, or if the materials in question specifically state that use of the material is permissible, and provided the RIPE NCC Materials are not modified and are properly identified as RIPE NCC documents. Unless authorised by the RIPE NCC in writing, any use of the RIPE NCC Materials for advertising or marketing purposes is strictly forbidden and may be prosecuted. The RIPE NCC should be notified of any such activities or suspicions thereof.

[...]

Find the full copyright statement here:
https://www.ripe.net/about-us/legal/copyright-statement