RIPE NCC

RIPE NETWORK COORDINATION CENTRE

# IPv6 Security

## RIPE NCC Days - Sofia

June 2023

# Overview

- IPv6 Security vs IPv4 Security
- Reachability of IPv6 Addresses
- Network Scanning in IPv6
- Attacks on IPv6
- IPv6 vs IPv4
- IPv6 Support
- IPv4-Only Networks
- IPv6 Security Resources

# 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.

# Reality

## A change of mindset is necessary

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

# For a Good Level of Security

| | |
|---|---|
| 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<br>IPv6 is also responsible for Internet growth |

# 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.

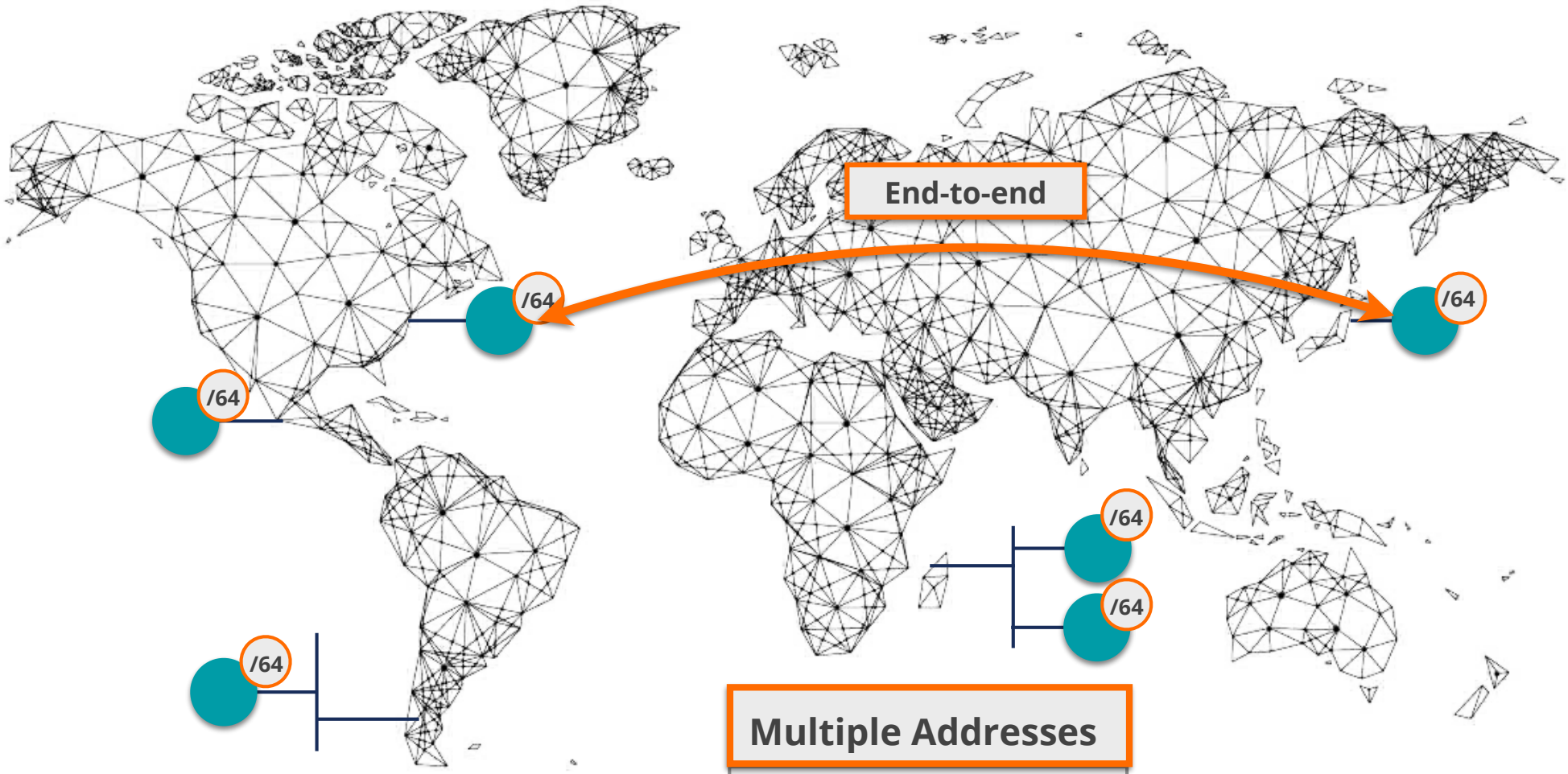
**Reason**:

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

**Reality**:

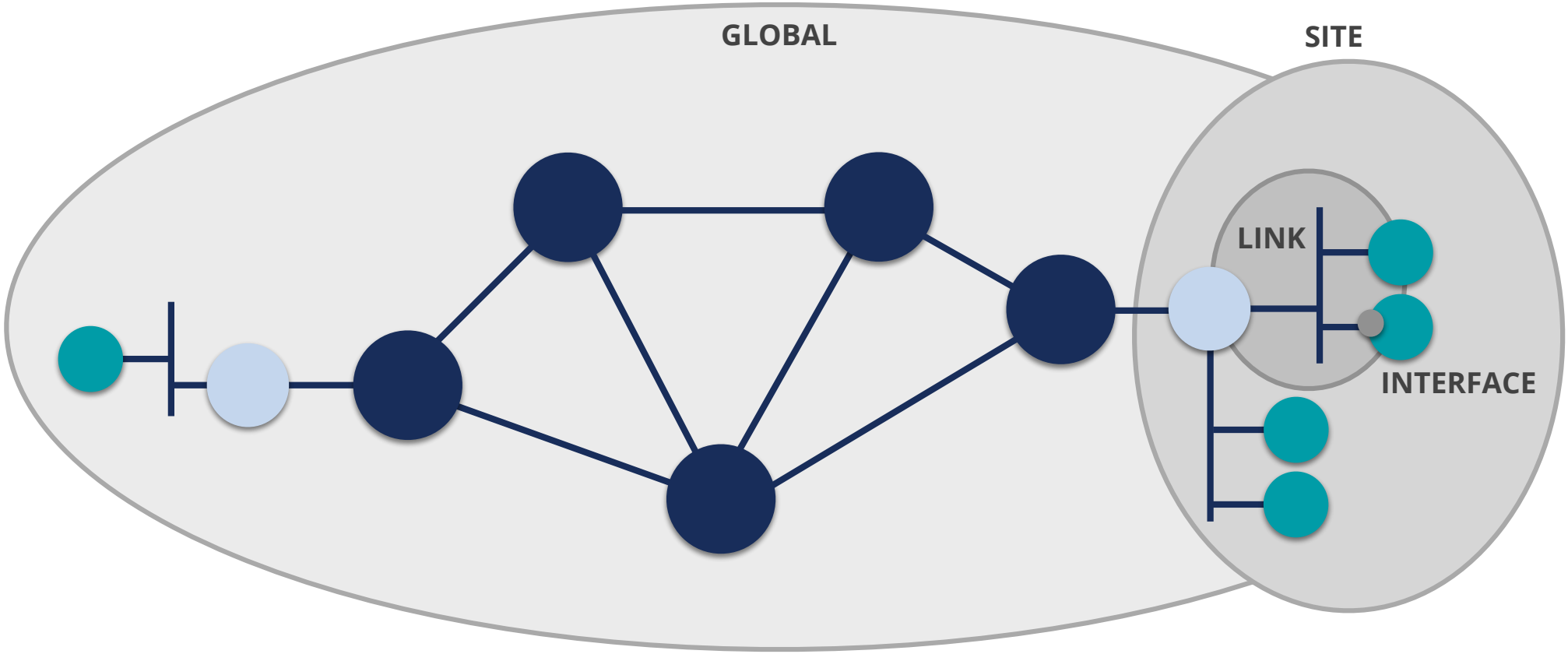
- Global addressing does not imply global reachability.
- You are responsible for reachability (filtering).

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

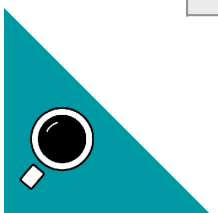
fd00:a:b::100

ff05::1:3

ff02::1

# 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 |

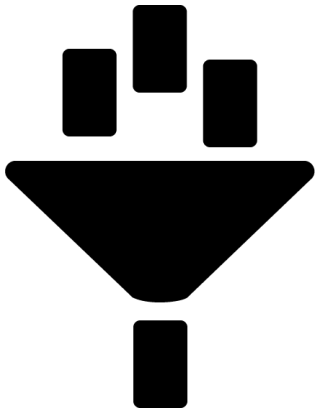


http://www.iana.org/assignments/iana-ipv6-special-registry/

# 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

# Filtering in IPv6 is very Important!

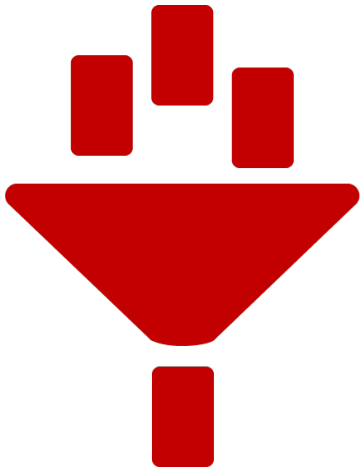


- Global Unicast Addresses
- A good **addressing plan**

**Easier** filtering!

# New Filters to Take Into Account

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



# FILTER ICMPv6 CAREFULLY!

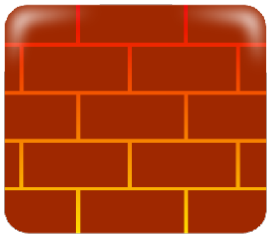
## Used in many IPv6 related protocols

# 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**

+

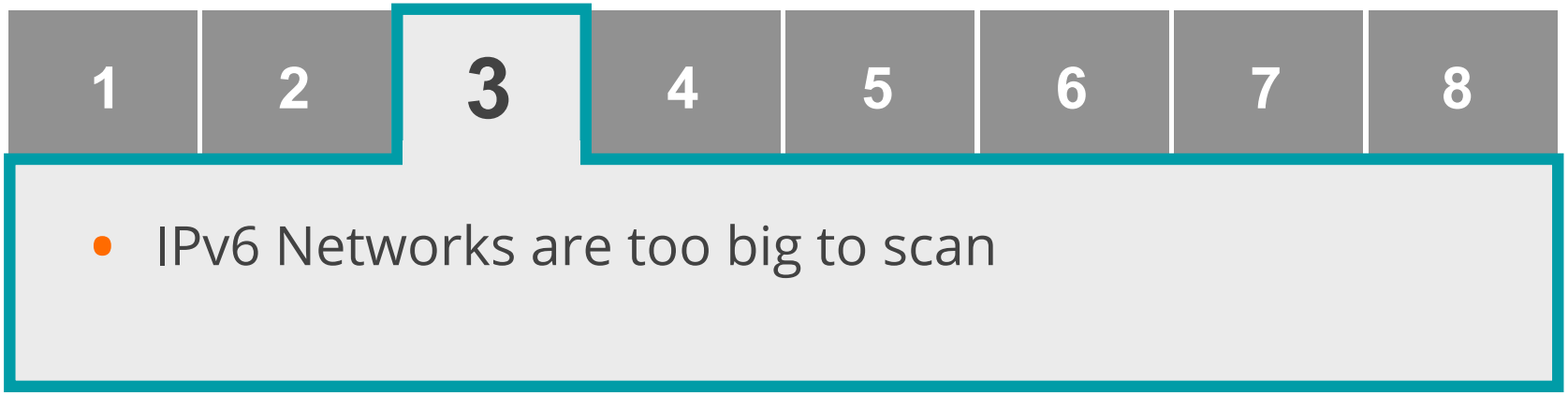
**Common IPv4 Practices**

+

**New IPv6 Considerations**

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

# IPv6 Security Statements



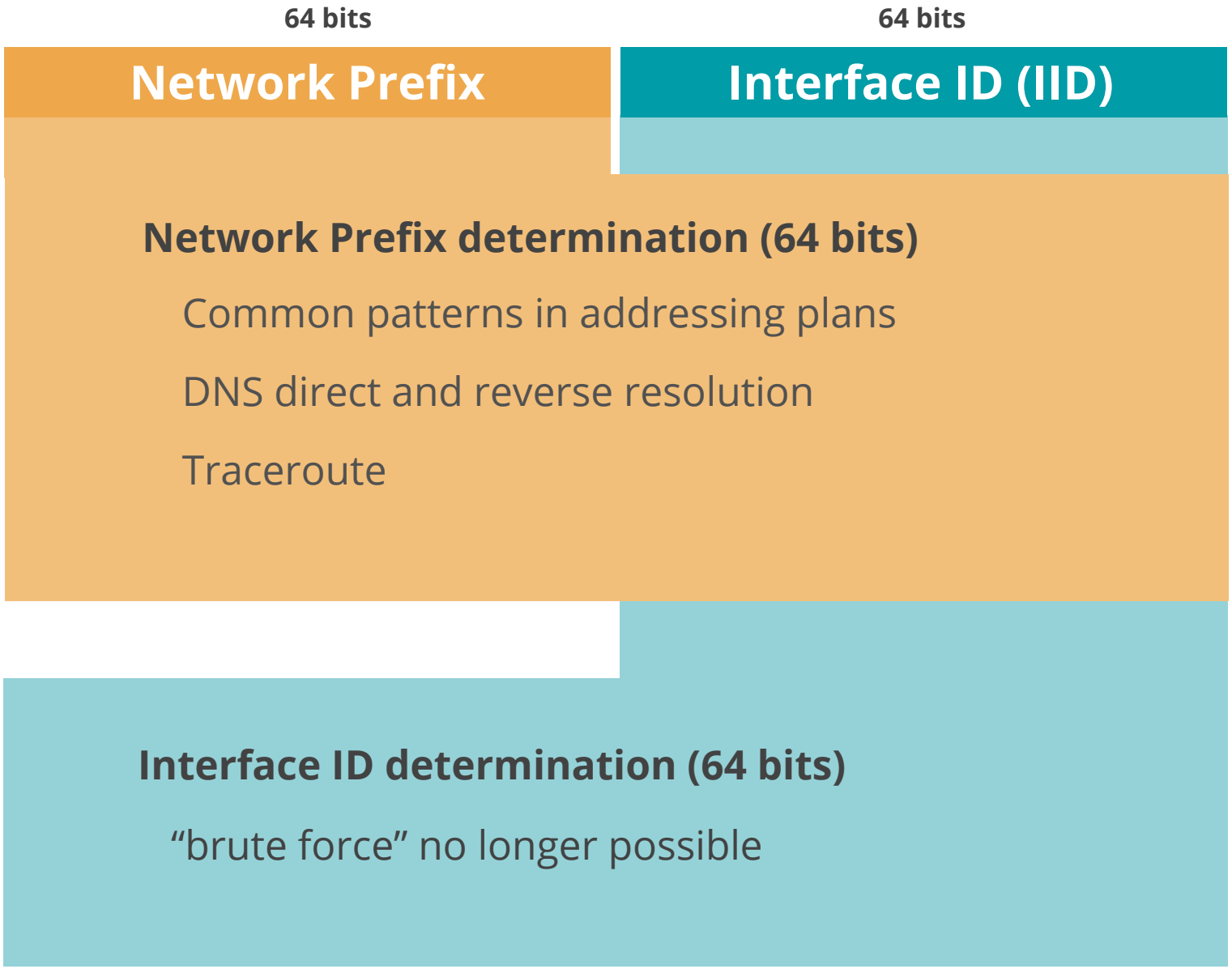

**Reason**:

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

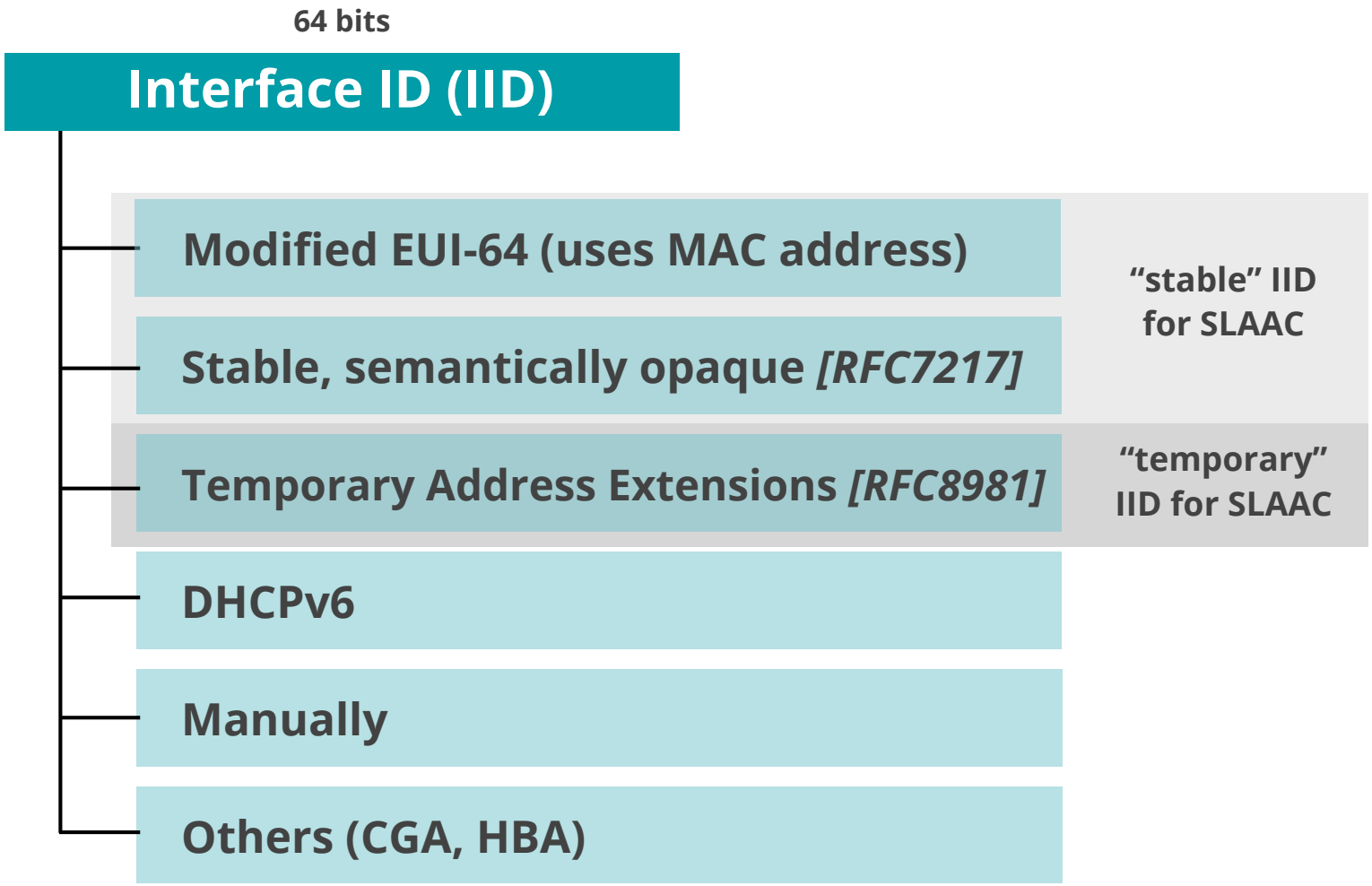
**Reality**:

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

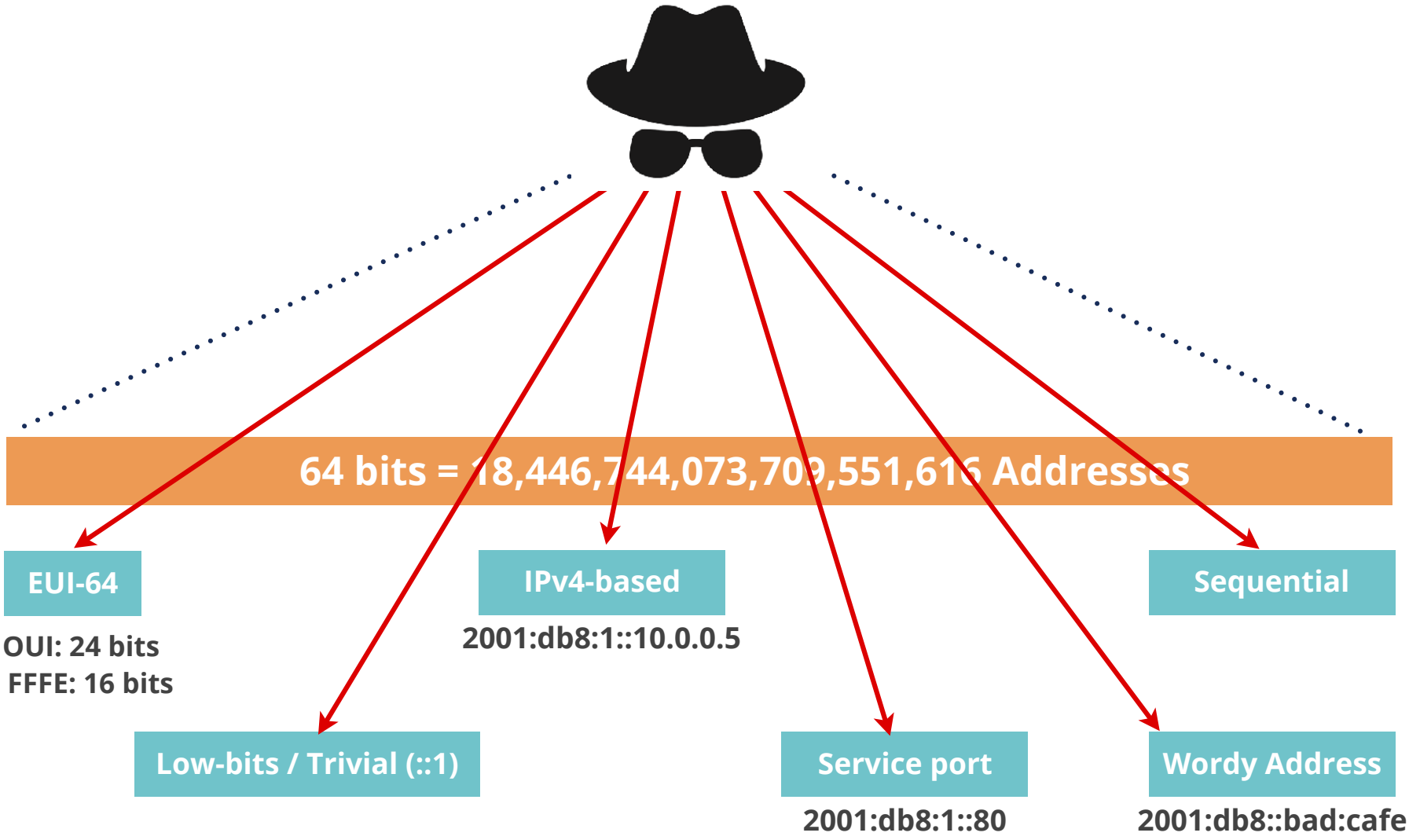
# IPv6 Network Scanning



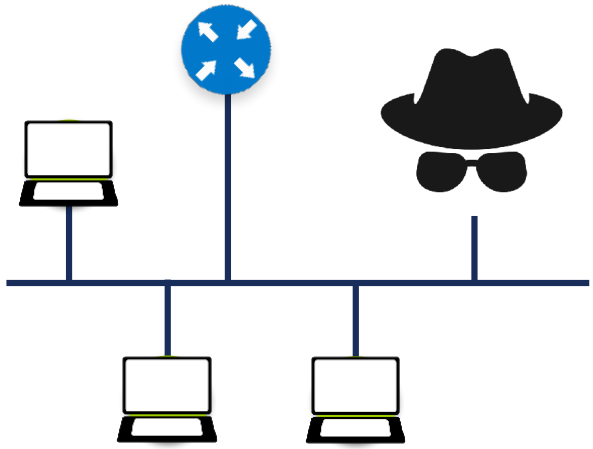
# IID Generation Options



# Guessing IIDs

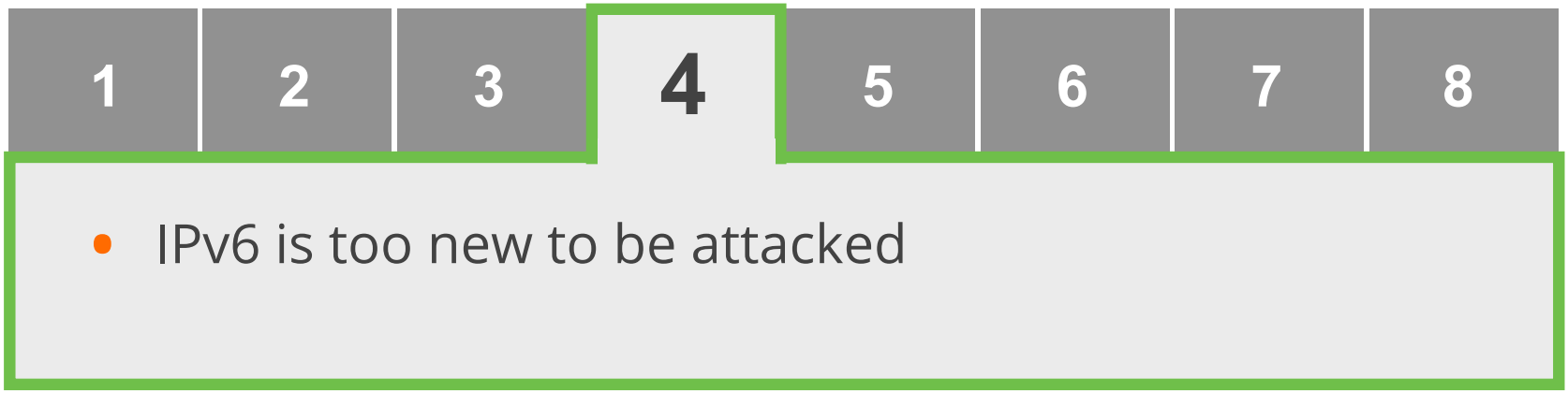


# Locally Scanning IPv6 Networks



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

# IPv6 Security Statements




**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

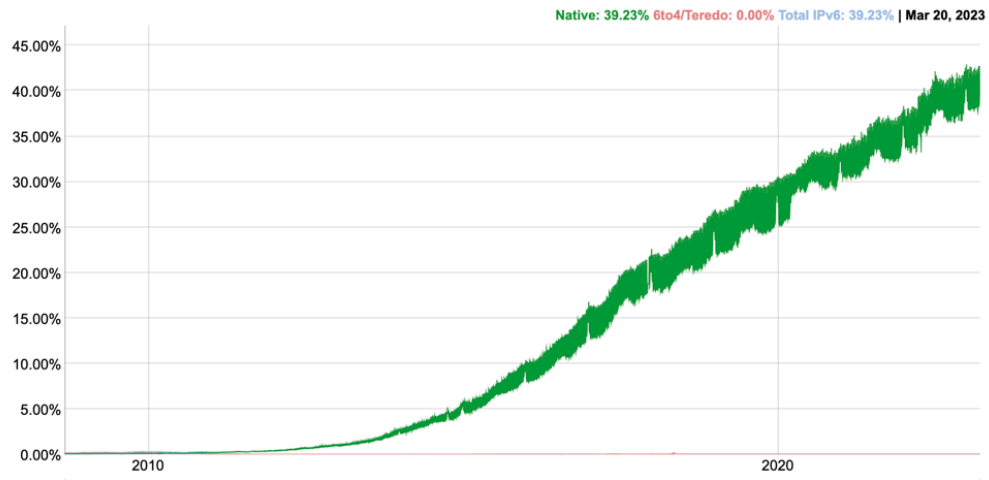
# IPv6 is happening…

| RANK | IPV6% | COUNTRY / REGION |
|---|---|---|
| 1 | 100% | Bahrain |
| 2 | 55.7% | Montserrat |
| 3 | 55.7% | Saudi Arabia |
| 4 | 54.9% | India |
| 5 | 53.9% | Uruguay |
| 6 | 53% | France |
| 7 | 53% | Malaysia |
| 8 | 52.1% | Germany |
| 9 | 50.7% | Greece |
| 10 | 50.4% | United States |
| 11 | 50.1% | Puerto Rico |
| 12 | 50% | Viet Nam |
| 13 | 48.6% | Belgium |
| 14 | 46.4% | Japan |

Show 10 entries Search:

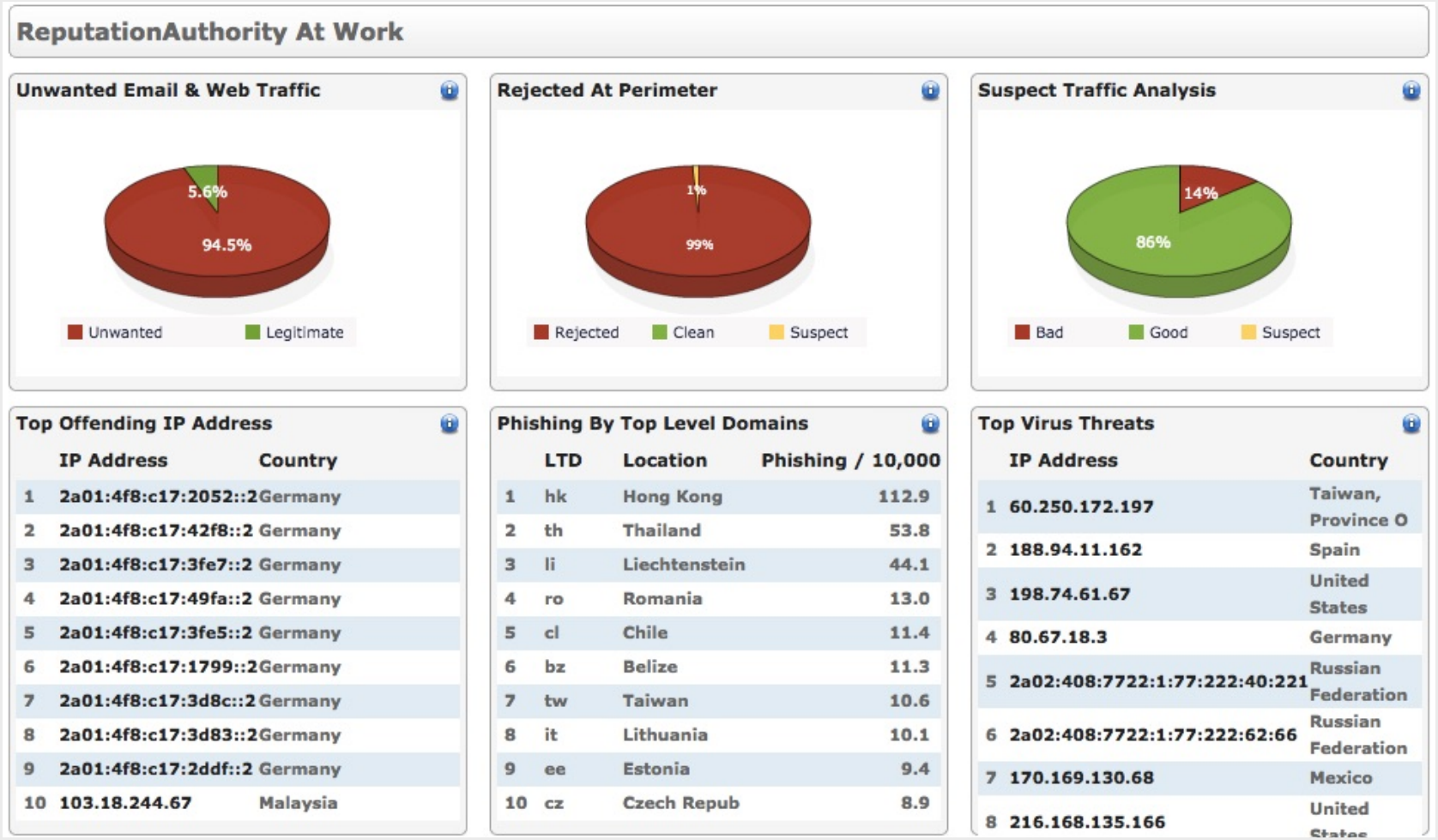
| Rank | Participating Network | ASN(s) | IPv6 deployment |
|---|---|---|---|
| 1 | RELIANCE JIO INFOCOMM LTD | 55836, 64049 | 92.58% |
| 2 | Comcast | 7015, 7016, 7725, 7922, 11025, 13367, 13385, 20214, 21508, 22258, 22909, 33287, 33489, 33490, 33491, 33650, 33651, 33652, 33653, 33654, 33655, 33656, 33657, 33659, 33660, 33661, 33662, 33664, 33665, 33666, 33667, 33668, 36732, 36733 | 73.62% |
| 3 | Combined US Mobile Carriers | 3651, 6167, 10507, 20057, 21928, 22394 | 87.74% |
| 4 | Charter Communications | 7843, 10796, 11351, 11426, 11427, 12271, 20001, 20115, 33363 | 56.41% |
| 5 | ATT | 6389, 7018, 7132 | 72.32% |
| 6 | T-Mobile USA | 21928 | 92.31% |
| 7 | Deutsche Telekom AG | 3320 | 74.48% |
| 8 | Orange Business Services | 3215 | 74.08% |
| 9 | Verizon Wireless | 6167, 22394 | 83.58% |
| 10 | Claro Brasil | 4230, 28573 | 74.53% |

Showing 1 to 10 of 345 entries First Previous 1 2 3 4 5 Next Last




Source: **http://worldipv6launch.org/measurements/ (22/3/2023)**

# … and so are IPv6 Security threats!



# 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**:

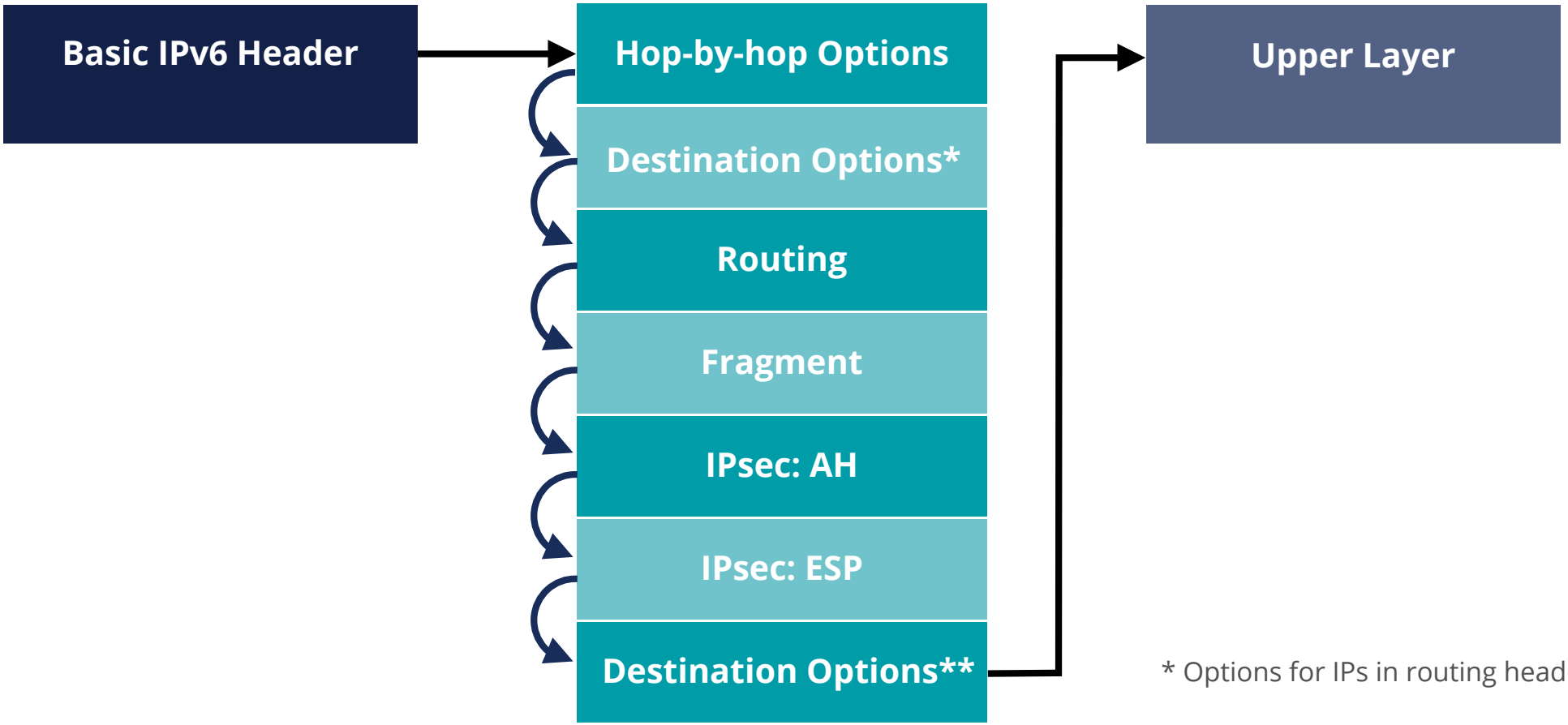
- Whole new addressing architecture
- Many associated new protocols

# IPv6 vs IPv4

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

**No changes with IPv6** | **Changes with IPv6** | **New IPv6 issues**

# IPv6 Extension Headers




* Options for IPs in routing header

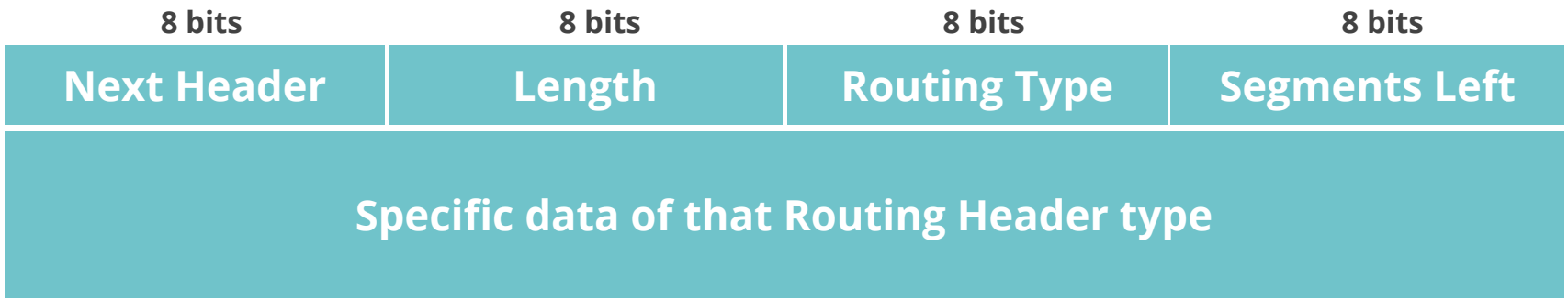
** Options for destination IP

- 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

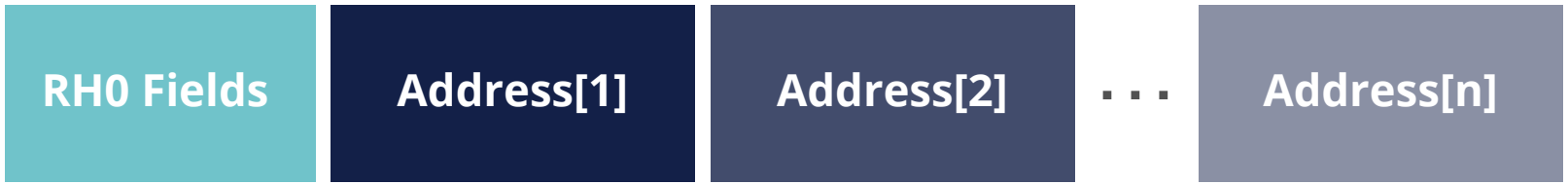
Includes one or more IPs that should be "*visited*" in the path

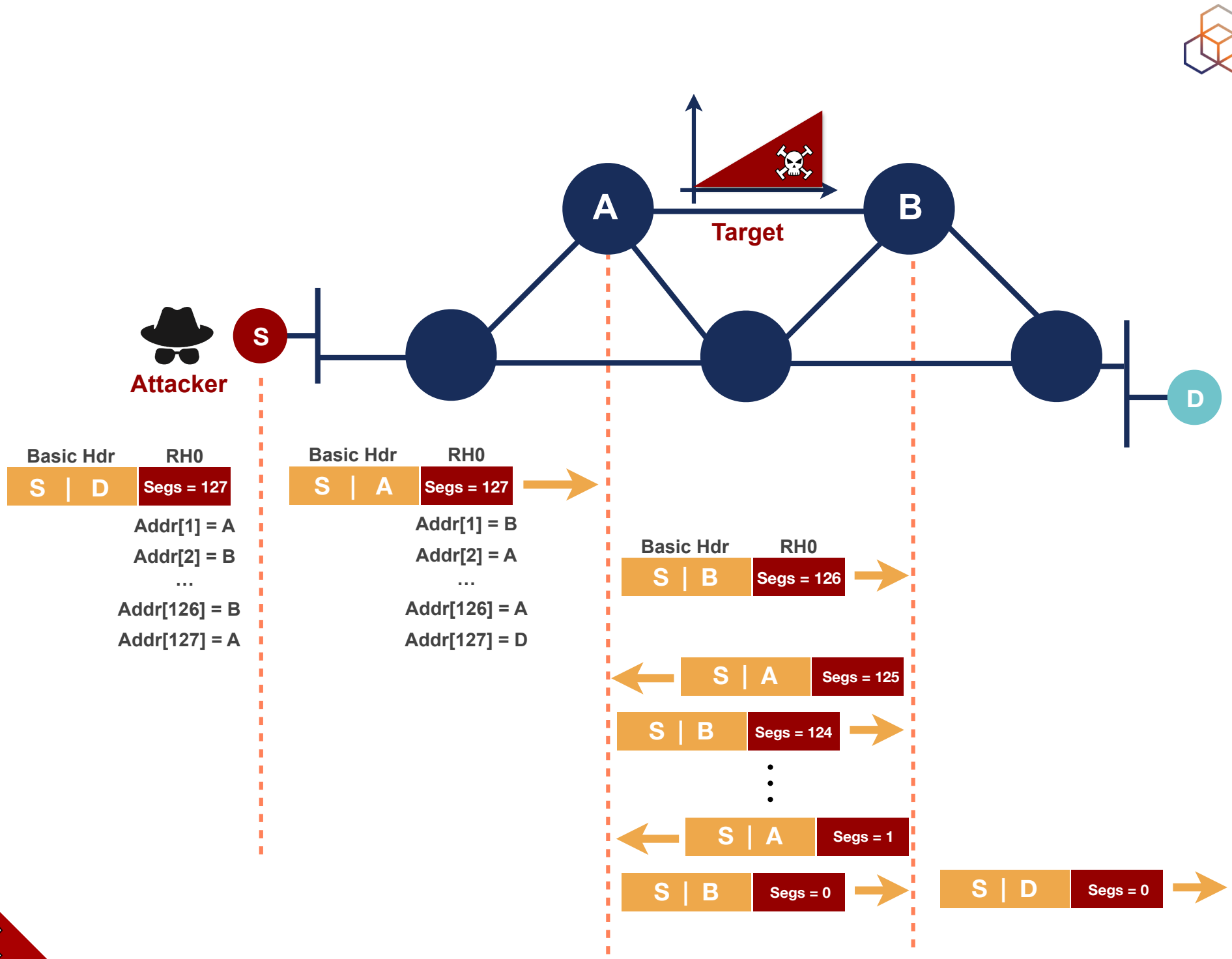
- Processed by the **visited routers**



# 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



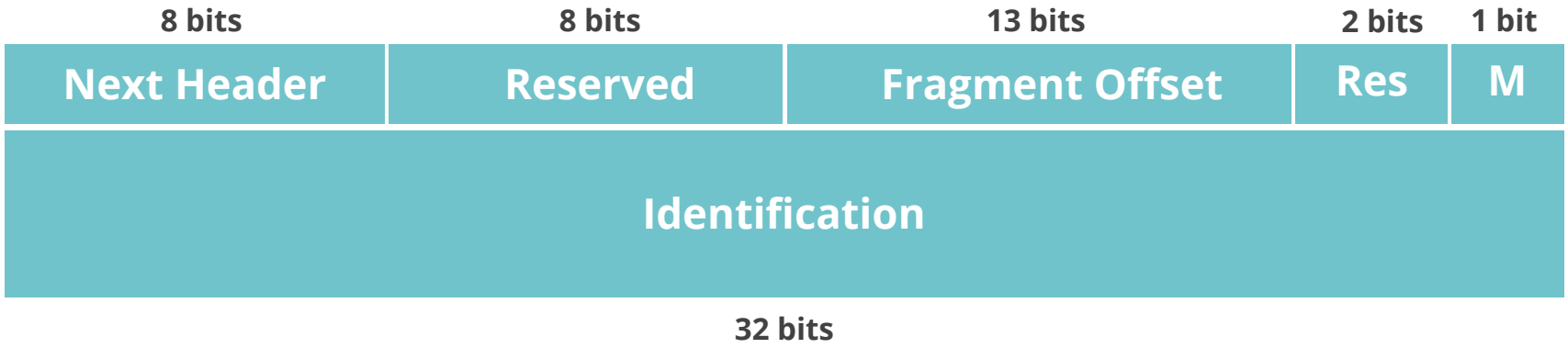

A
B
Target
S
Attacker
D
Basic Hdr
RH0
S | D
Segs = 127
Addr[1] = A
Addr[2] = B
…
Addr[126] = B
Addr[127] = A
Basic Hdr
RH0
S | A
Segs = 127
Addr[1] = B
Addr[2] = A
…
Addr[126] = A
Addr[127] = D
Basic Hdr
RH0
S | B
Segs = 126
S | A
Segs = 125
S | B
Segs = 124
S | A
Segs = 1
S | B
Segs = 0
S | D
Segs =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

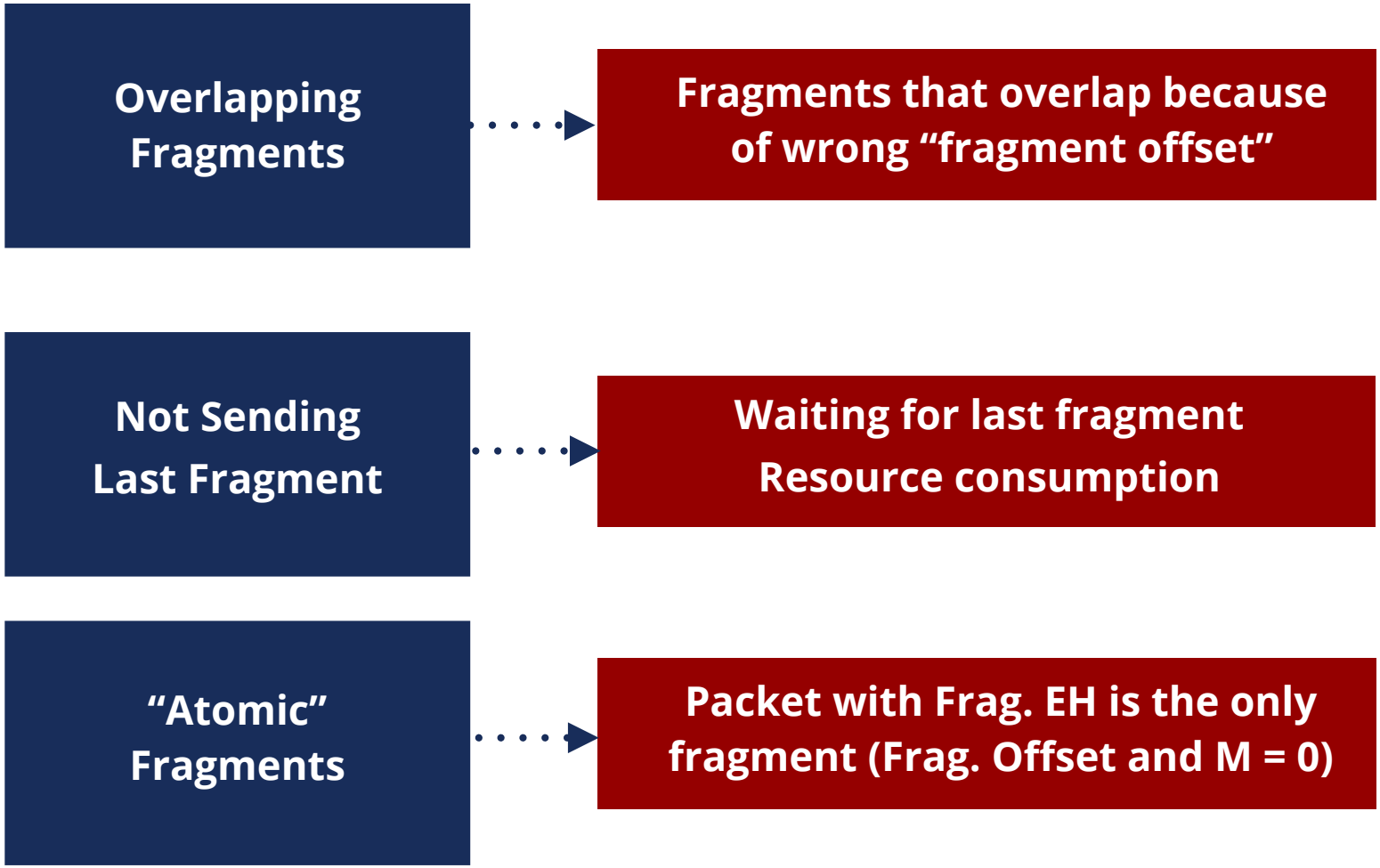



**M Flag**:

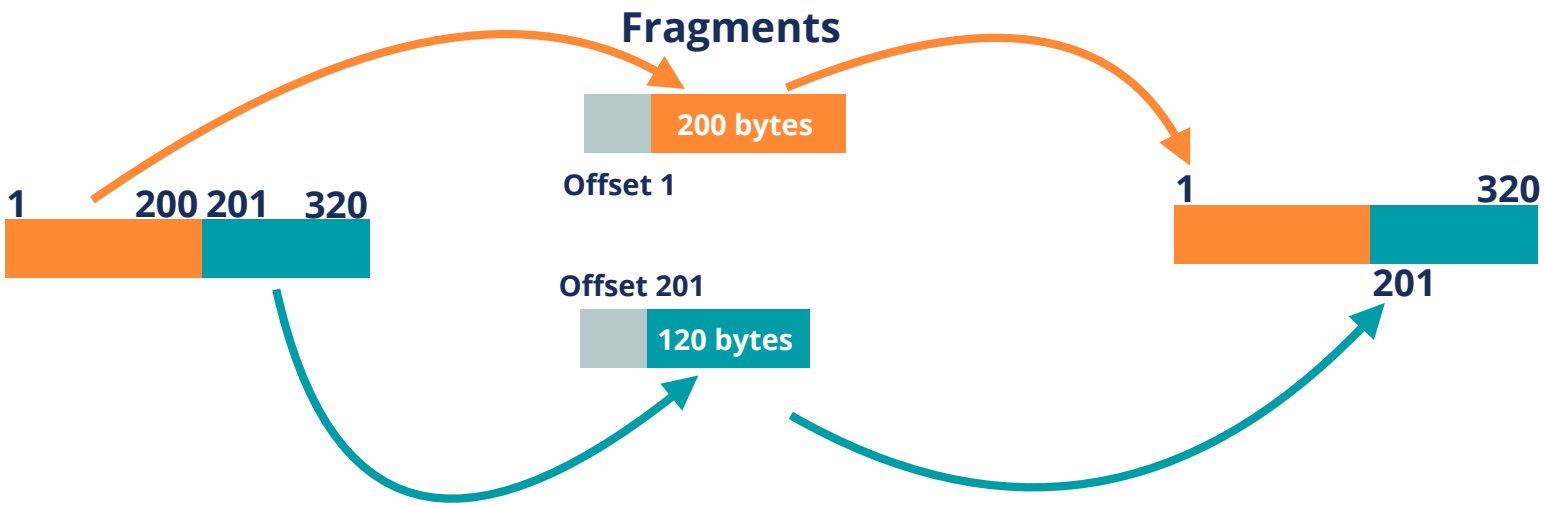
1 = more fragments to come;

0 = last fragment

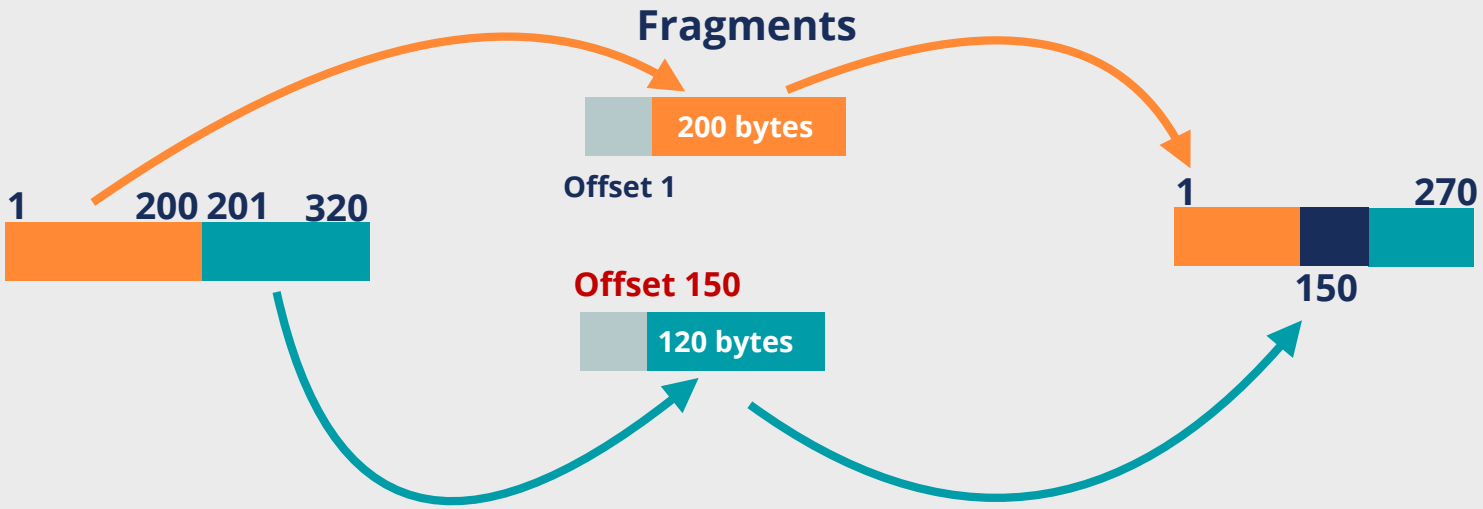
# EH Threats: Fragmentation




# Overlapping Fragments

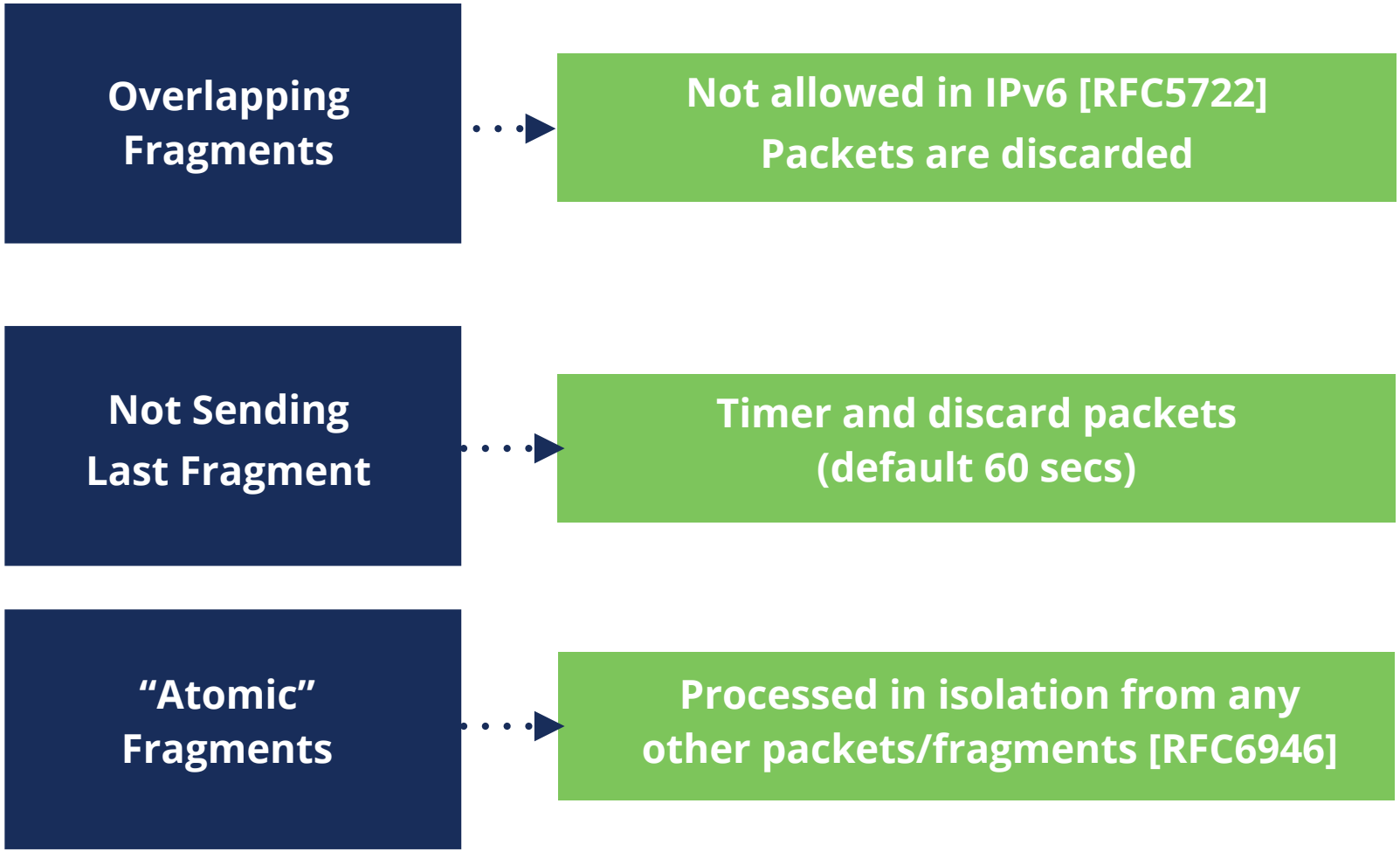



Normal fragments offset say where the data goes




Overlapping fragments have wrong offset values

# EH Solutions: Fragmentation




# 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

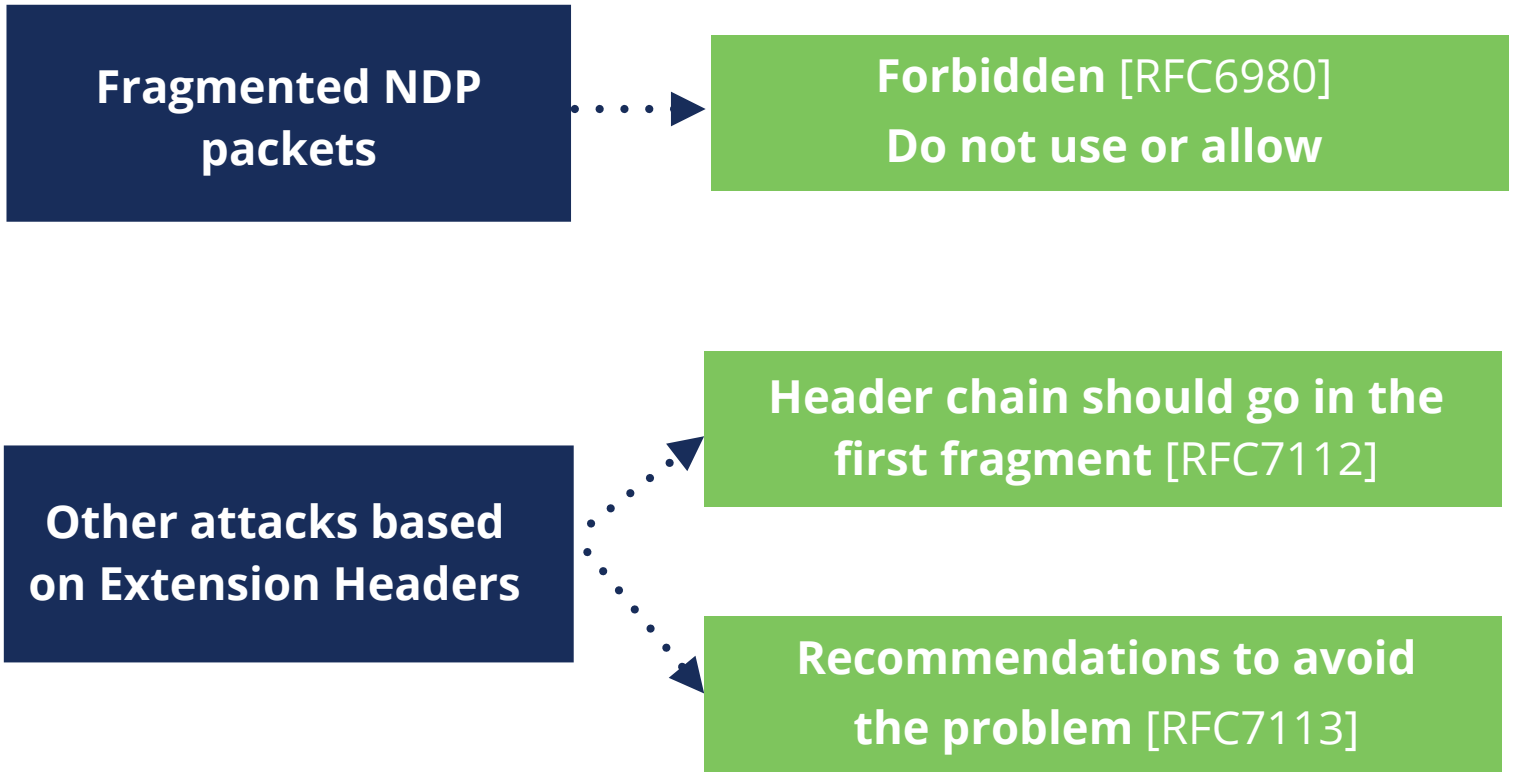
## Using **Fragment** Extension Header

| 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




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

# NDP Features

**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

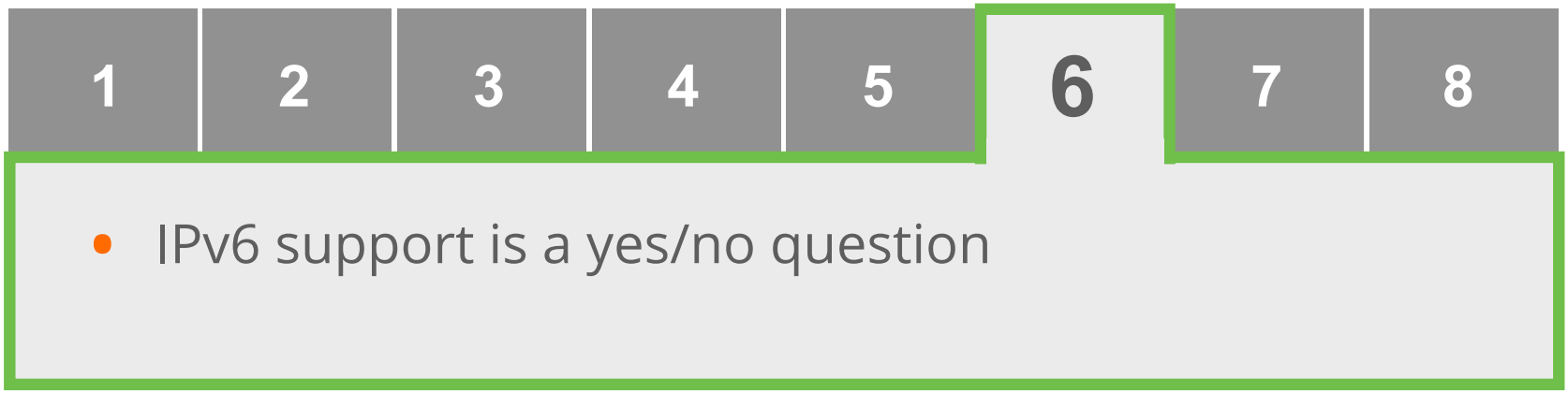
# NDP Threats

- **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 ?

# IPv6 Security Statements




## 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

# 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**

# 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

- 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” |

# 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

# IPv6 vs IPv4

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

**No changes with IPv6** | **Changes with IPv6** | **New IPv6 issues**

# Security Tools

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

# 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)

# 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

# Routing Protocols Authentication

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

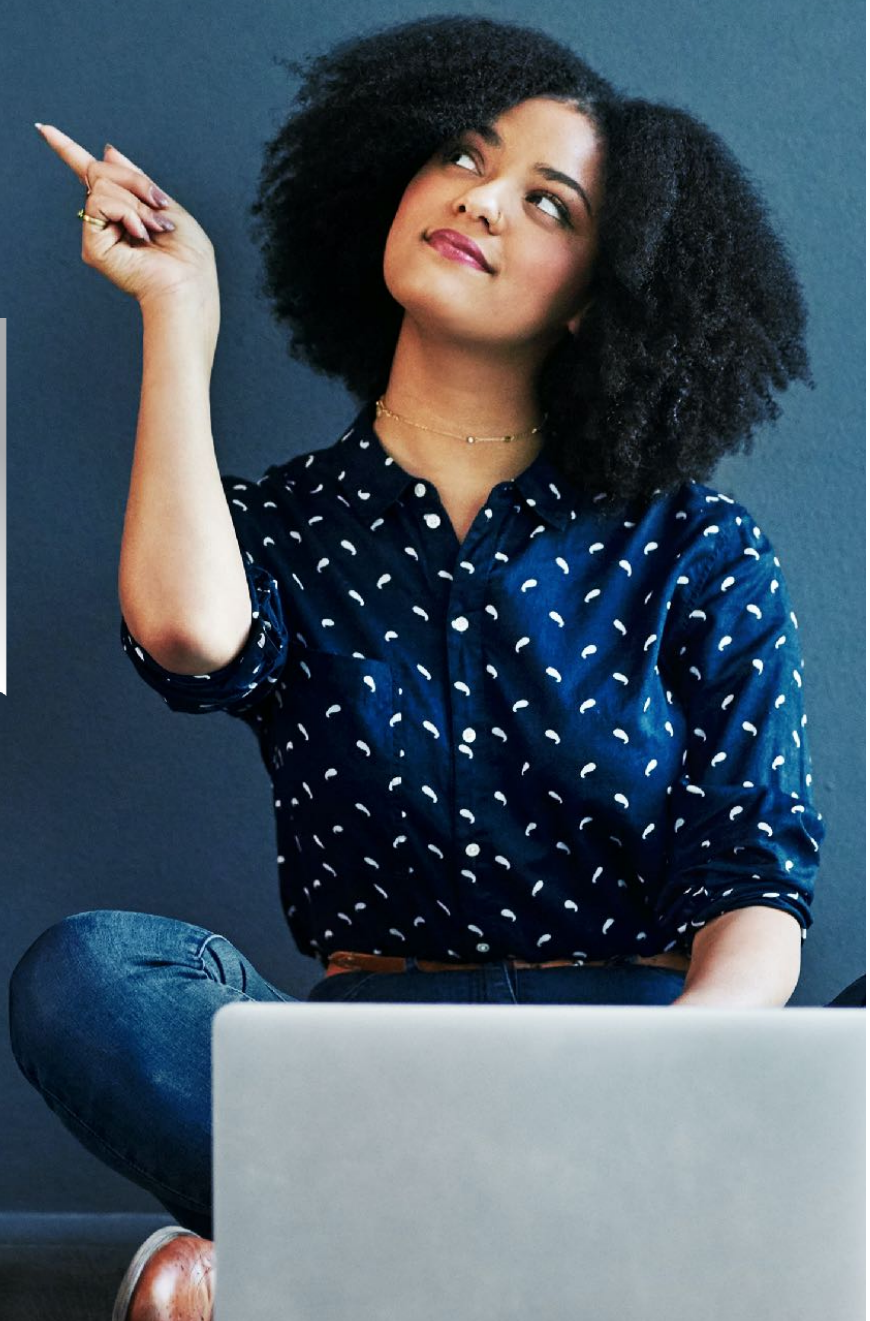
- Other protocols: **No options available**

# 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

# RIPE NCC Certified Professionals


https://getcertified.ripe.net/




Ënn
Соңы
An Críoch
پایان
Y Diwedd
Vége
Endir
Finvezh
վերջ
Ende
Koniec
Son
დასასრული
הסוף
Кінець
Finis
Lõpp
Amaia
Tmiem
Liðugt
Kpaj
Sfârşit
Loppu
Slutt
Fund
Kraj
النهاية
Конец
Konec
Τέλος
Fine
Fin
Fí
Край
Einde
Pabaiga
Slut
Fim
Beigas
E1 N1 D2