RIPE NCC
RIPE NETWORK COORDINATION CENTRE

IPv6 Security Myths, Filtering and Tips

Webinar

RIPE NCC Learning & Development

This webinar is being recorded

IPv6 Security Myths

Filtering IPv6 Traffic

IPv6 Security Tips

Legend

Learning / Understanding

Attacker

Protecting

Tell us about you!

Please answer the polls

2 min.

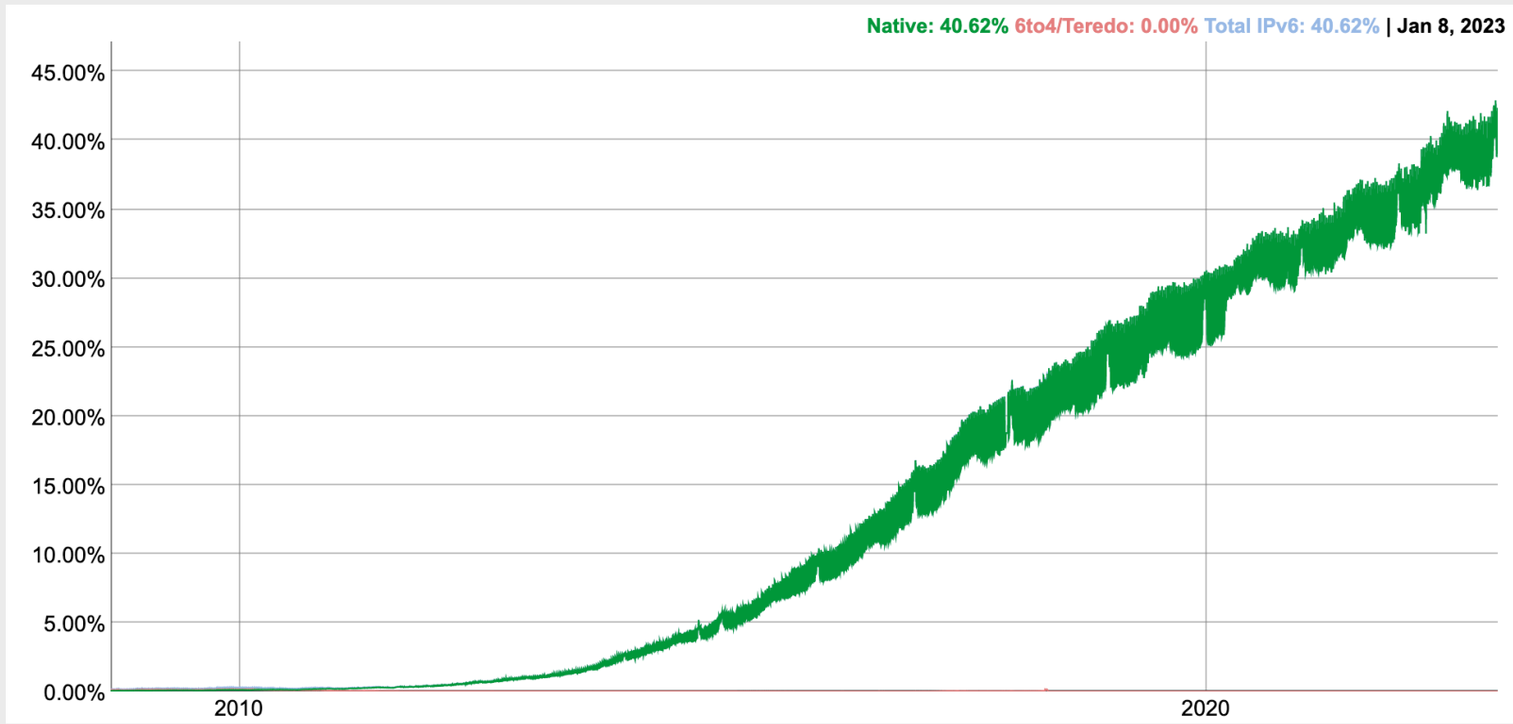
IPv6 Security Myths

Section 1

IPv6 is Happening…

RANK	IPV6%	COUNTRY / REGION
1	100%	Bahrain
2	59.8%	Montserrat
3	58.5%	Belgium
4	56.8%	France
5	55.9%	Germany
6	55.3%	Uruguay
7	54.6%	Saudi Arabia
8	53.4%	Greece
9	52.4%	United States
10	52%	Puerto Rico

Rank	Participating Network	ASN(s)	IPv6 deployment
241	CNGI-CERNET2/6IX	23910, 23911	100.00%
323	Sauk Valley Community College	13953	96.12%
1	RELIANCE JIO INFOCOMM LTD	55836, 64049	92.58%
6	T-Mobile USA	21928	92.31%
25	Chunghwa Telecom (Mobile)	17421	91.37%
182	Virginia Tech	1312	88.67%
327	mc.net	6479	88.23%
252	Gustavus Adolphus College	17234	88.07%
19	Free	12322	88.00%
3	Combined US Mobile Carriers	3651, 6167, 10507, 20057, 21928, 22394	87.74%



Source: **http://worldipv6launch.org/measurements/ ; Google; Akamai**

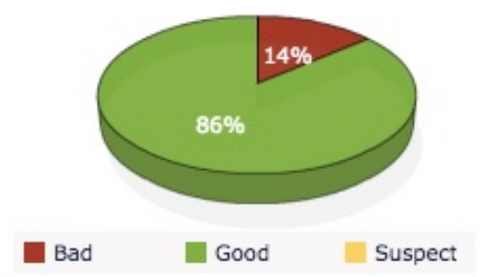
… and So Are IPv6 Security Threats!

ReputationAuthority At Work

Unwanted Email & Web Traffic

Rejected At Perimeter

Suspect Traffic Analysis



Top Offending IP Address

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

Phishing By Top Level Domains

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

Top Virus Threats

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

We need you to participate!

Please answer the questions on the chat

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**

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**

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

IPv6 Security Statements

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

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

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

IPv6 Security Statements

1	2	3	4	5	6	7	8

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

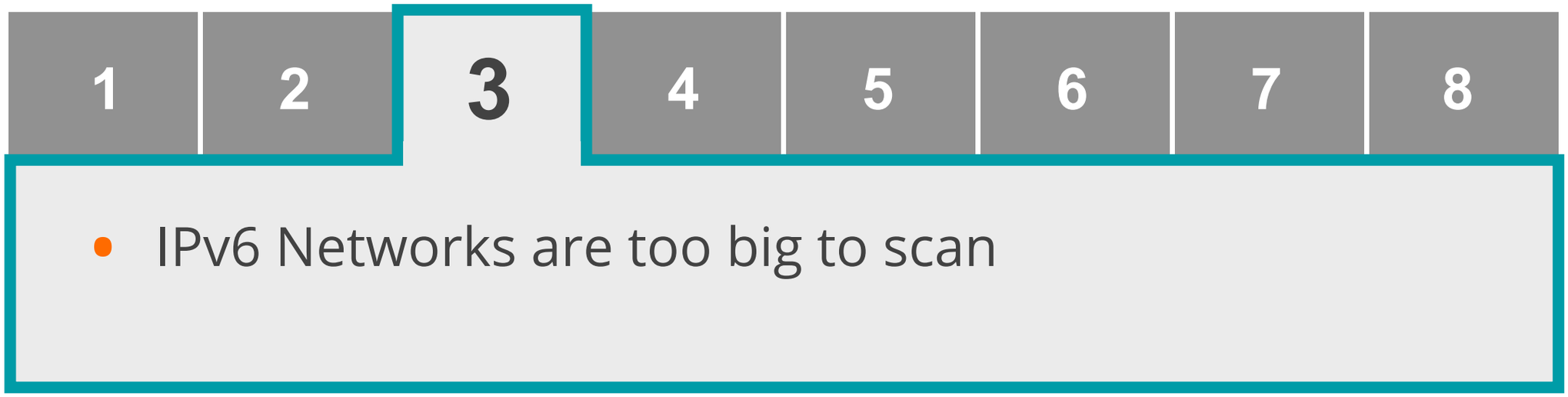
Reason:

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

Reality:

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

IPv6 Security Statements



IPv6 Security Statements

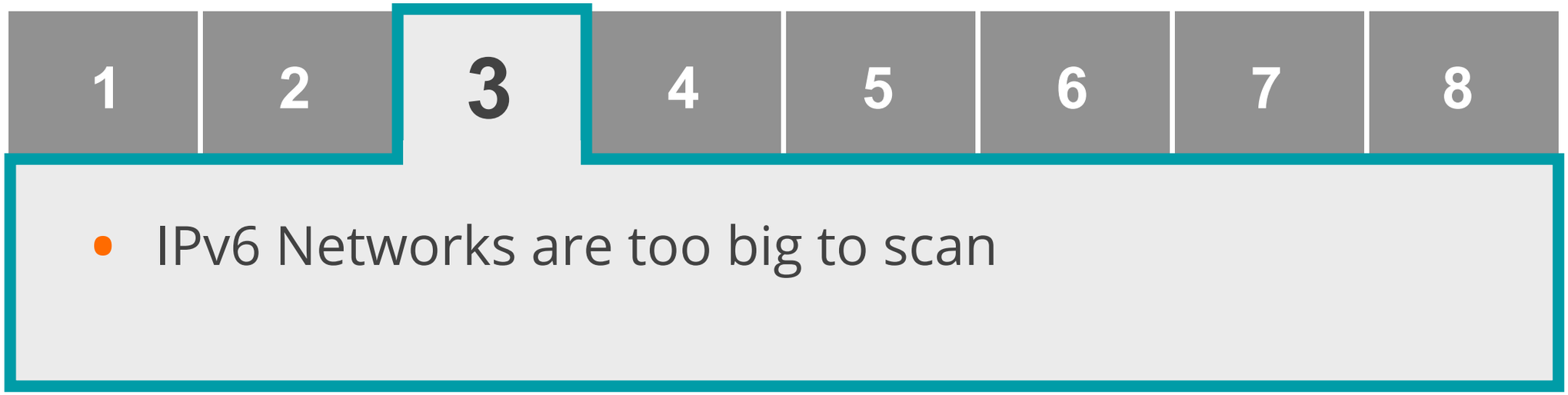
1	2	3	4	5	6	7	8

- IPv6 Networks are too big to scan

Reason:

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

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 Security Statements

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

- IPv6 is too new to be attacked

IPv6 Security Statements

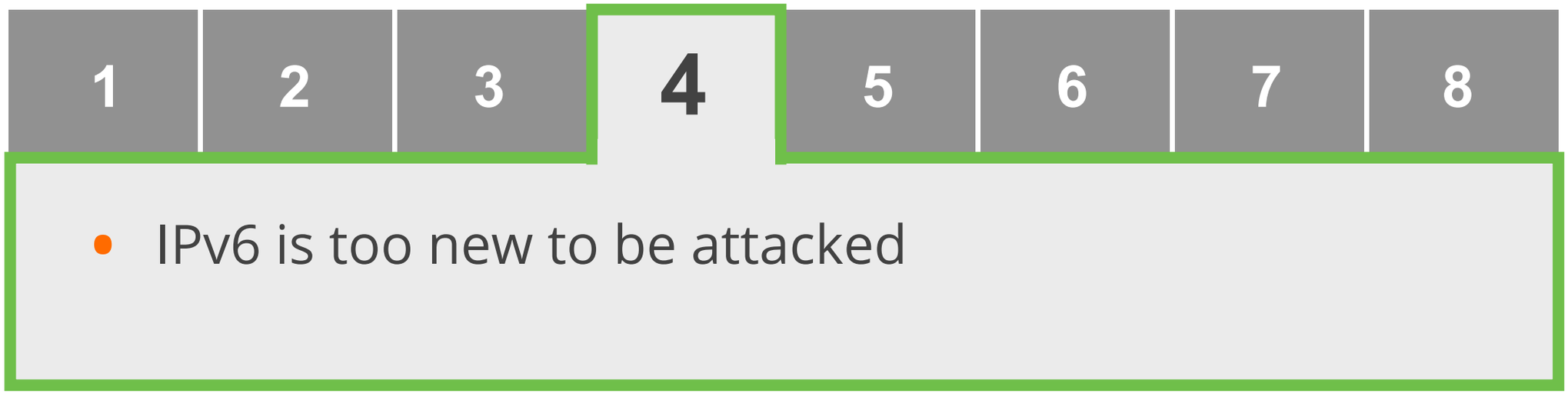
1	2	3	**4**	5	6	7	8

- IPv6 is too new to be attacked

Reason:

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

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 Security Statements

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

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

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

IPv6 Security Statements

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

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

Reason:

- Routing and switching work the same way

Reality:

- Whole new addressing architecture
- Many associated new protocols

IPv6 Security Statements

1	2	3	4	5	6	7	8

- IPv6 support is a yes/no question

IPv6 Security Statements

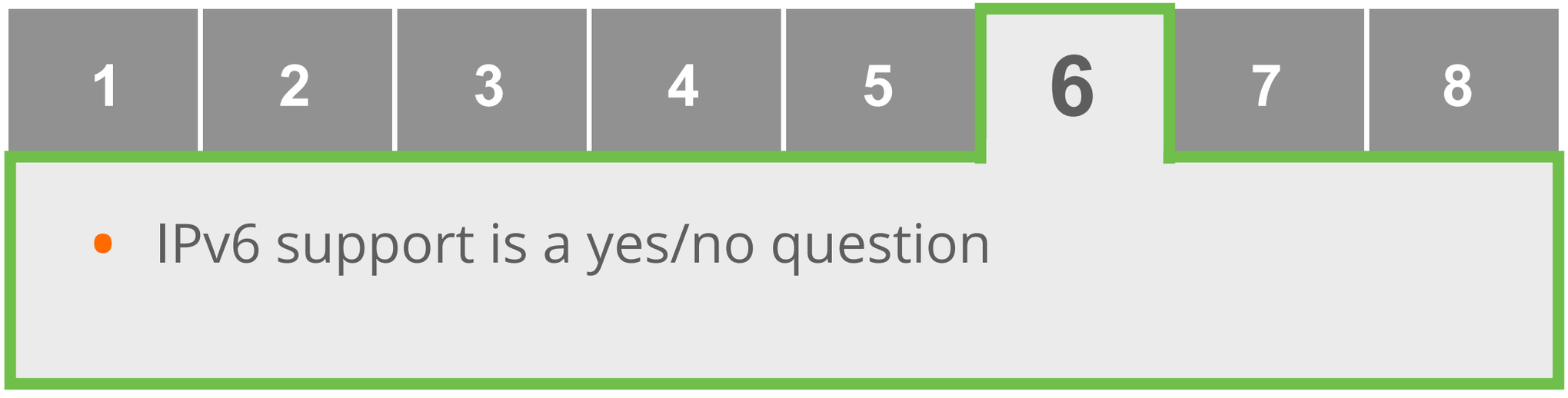
1	2	3	4	5	6	7	8

- IPv6 support is a yes/no question

Reason:

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

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

IPv6 Security Statements

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

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

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

IPv6 Security Statements

1	2	3	4	5	6	7	8

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

Reason:

- Networks only designed and configured for IPv4

Reality:

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

IPv6 Security Statements

1	2	3	4	5	6	7	8

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

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

IPv6 Security Statements

1	2	3	4	5	6	7	8

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

Reason:

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

Reality:

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

Conclusions

A change of mindset is necessary

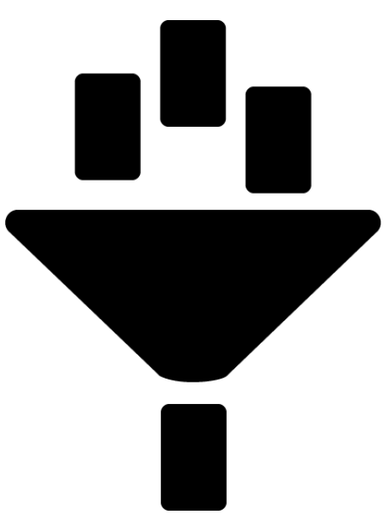
- IPv6 is not more or less secure than IPv4
- Knowledge of the protocol is the best security measure

Questions

Filtering IPv6 Traffic

Section 2

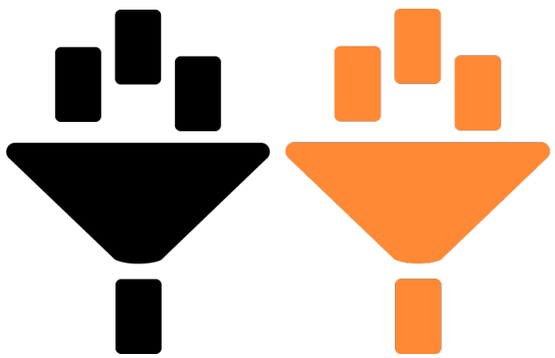
Filtering in IPv6 is very Important!



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

Easier filtering!

New Filters to Take Into Account



- ICMPv6
- IPv6 Extension Headers

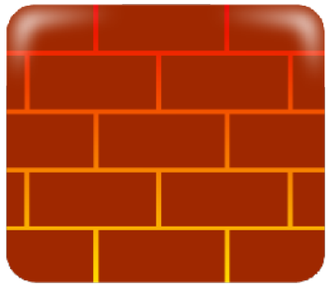
- Fragments Filtering
- Transition mechanisms (TMs) / Dual-Stack

Filtering ICMPv6

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

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

Filtering Extension Headers



- **Firewalls** should be able to:

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

Filtering Fragments

Upper layer info not in 1st fragment	Creates many tiny fragments to go through filtering / detection
Fragments inside fragments	Several fragment headers
Fragmentation inside a tunnel	External header hides fragmentation

Filtering Fragments

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

Take the poll!

Is it recommended to configure **filtering in an IPv6 host** to drop all **NS** and **NA** messages?

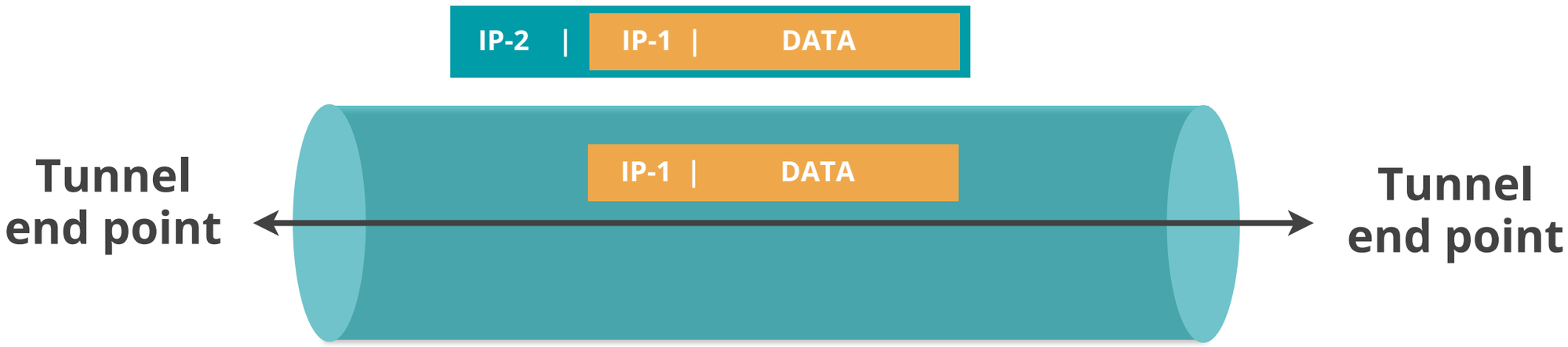
2 min.

Transition Mechanisms (TMs)

Temporary solution…

With security risks!

Tunnelling



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

Take the poll!

Are you using **Transition Mechanisms** in your network?

2 min.

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

Questions

Let’s take a **5 minutes** break!


WELCOME
WE ARE
OPEN
PLEASE COME IN

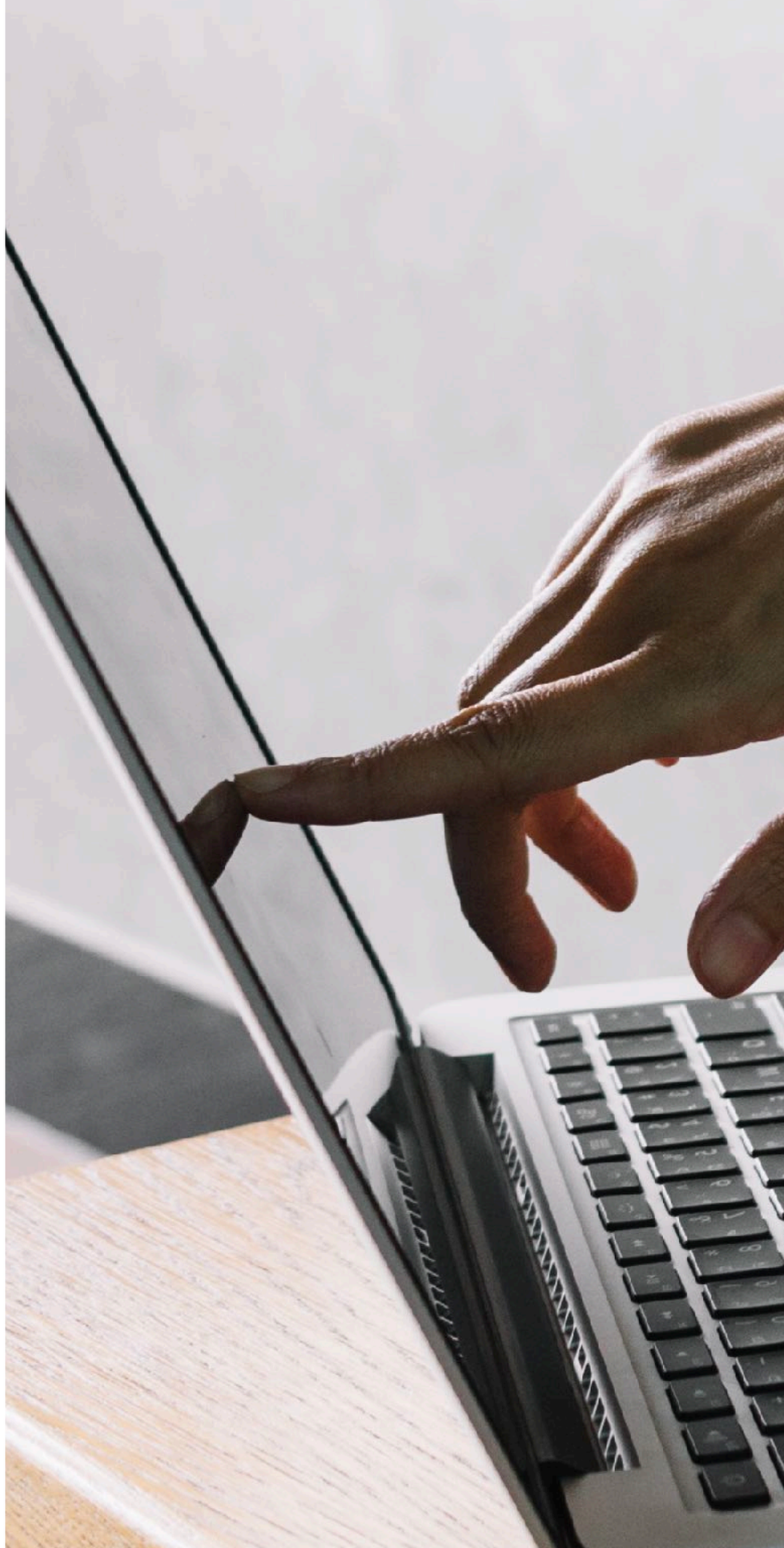
- How can you **protect** your IPv6 Host if the attack comes from the **same link**?

Demo 1

IPv6 Packet Filtering

Demo time!

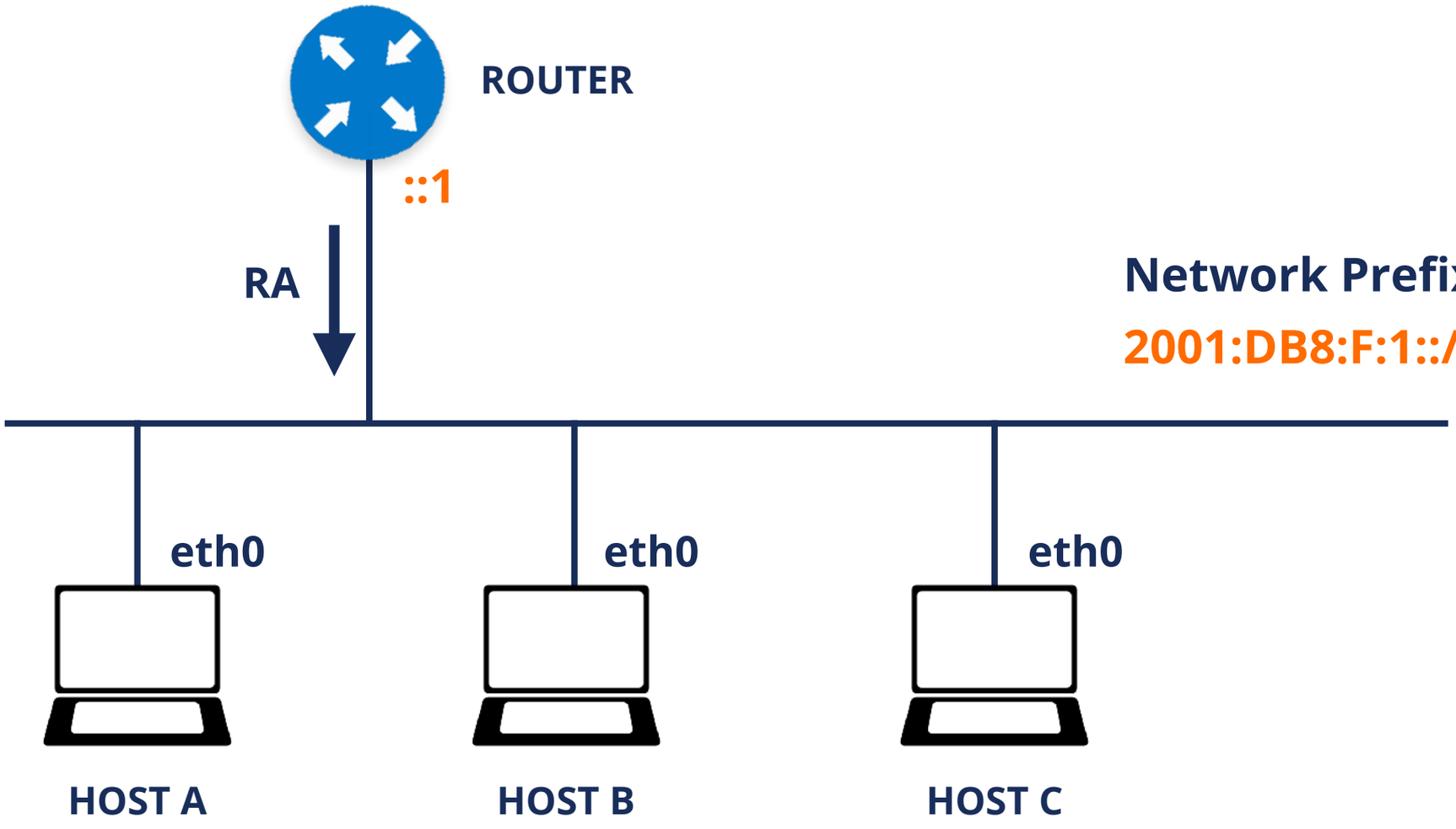
We will demo the activity on the screen.
Watch what we do.



Demo 1: IPv6 Packet Filtering

- **Description**: Configure a packet filter for NDP Redirect messages
- **Goals**:
  - Understand how easy it is to filter unwanted messages
- **Time**: 15 minutes
- **Demo**:
  - Generate Redirect packets that change other host's routes (using a toolkit)
  - Filter out Redirect messages in a host (using ip6tables)

Demo 1: Lab Network



Network Prefix:

2001:DB8:F:1::/64

Demo 1: IPv6 Packet Filtering

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

IPv6	ICMPv6 Redirect
IPv6.Source	fe80::a:b:c
IPv6.Destination	IPa
Redirect.Target Addr	fe80::a
Redirect.Dst Addr	2001:db8:bad:dad::1

Take the poll!

Think of the use of **IPv6 packet filtering in the host** as a protection tool.

Which of the following statements are **true**?

2 min.

Questions

IPv6 Security Tips

Section 3

Take the poll!

Which **IPv6 security tips** can you already **share** with others in this webinar?

2 min.

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

Tips

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

No changes with IPv6

Changes with IPv6

New IPv6 issues

Up to date information

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

Examples

Manual

CVE

cve.mitre.org/cve/search_cve_list.html

Search for: **ICMPv6 windows**

NVD

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

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

Go to vendor’s link

Automated

OpenVAS

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

Homework

Go to: cert.europa.eu

Select language filters

Search for IPv6

optional: configure a subscription

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

Search for IPv6 + your vendor

Security Tools

Type	Can be used for	Examples
Packet Generators	Assessing IPv6 security	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	

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**

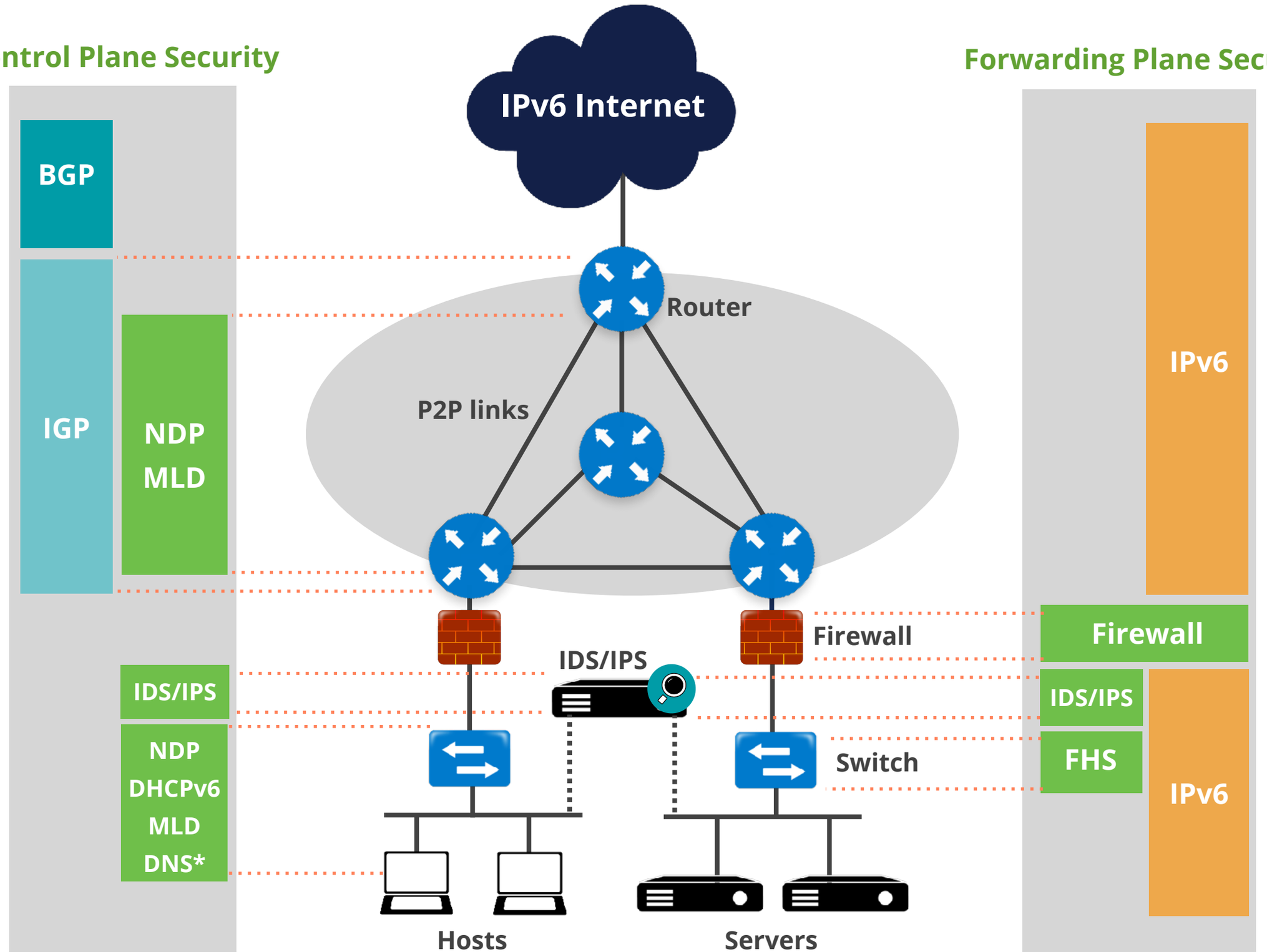
CPE

Router

Security Equipment

- **DHCPv6 Server Privacy Issues**

Control Plane Security



Forwarding Plane Security

* All Name resolution related protocols

IPv6 security myths

- Change your mindset
- IPv6 no more/less secure than IPv4

Filtering IPv6 Traffic

- Very important because of Global Addresses

Tips

- Features per device
- Features by context

Questions

Take the poll!

Think of everything you've 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/ipv6s3

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