RIPE NCC
RIPE NETWORK COORDINATION CENTRE

IPv6 Security

Second SEE Roundtable Meeting for Governments and Regulators

Alvaro Vives | Budva, Montenegro| 28 Sept 2023

IPv6 is real

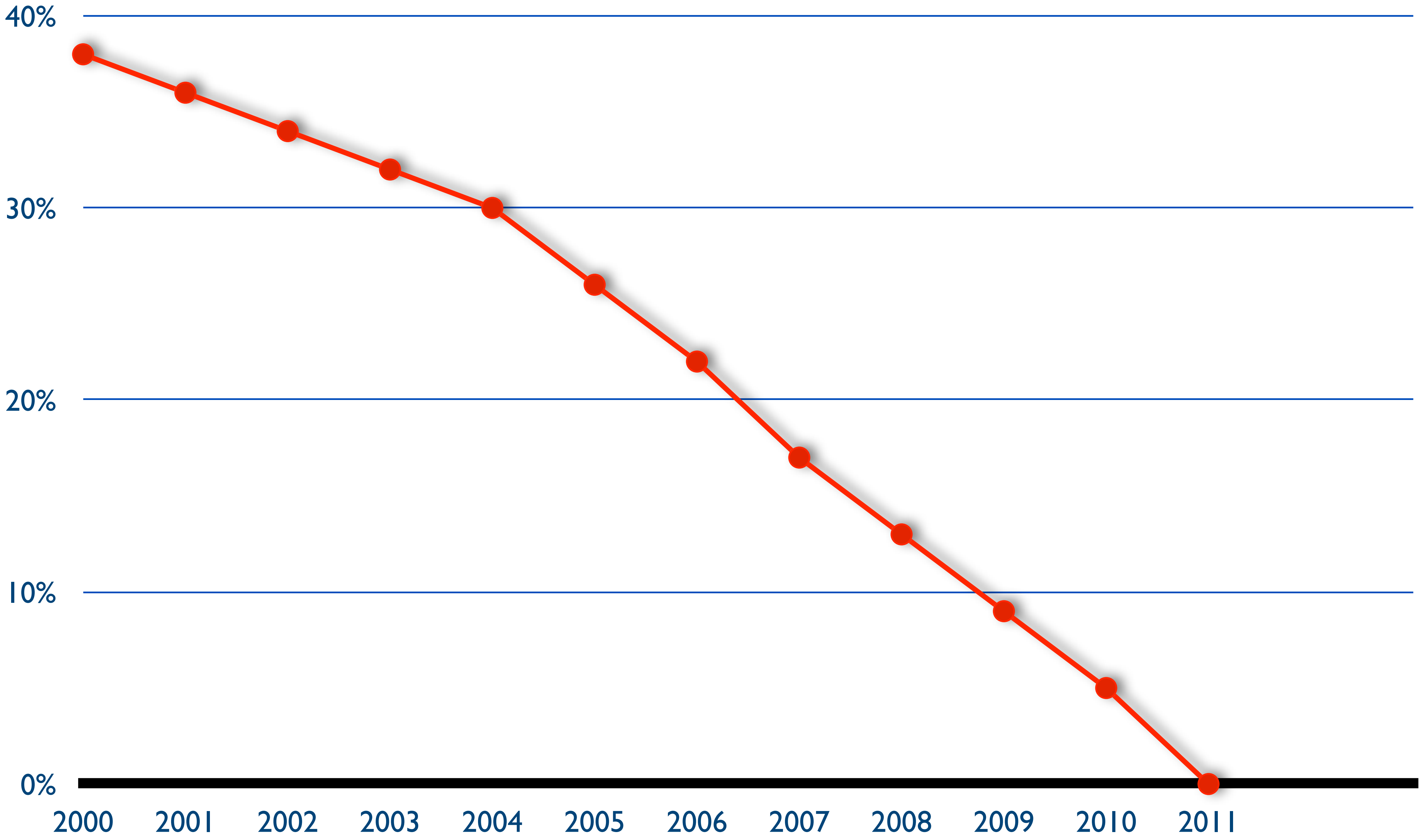
Internet is everywhere…

Libelium Smart World

libelium
www.libelium.com

http://www.libelium.com/top_50_iot_sensor_applications_ranking

IANA IPv4 Pool



IPv4 run-out

“Today, at 15:35 (UTC+1) on 25 November 2019, we made our final /22 IPv4 allocation from the last remaining addresses in our available pool. We have now run out of IPv4 addresses.”

Our Reality: The Waiting List

1. Submit the IPv4 allocation request (/24)

2. Wait: 1080 LIRs waiting, 1st LIR's been waiting for 441 days

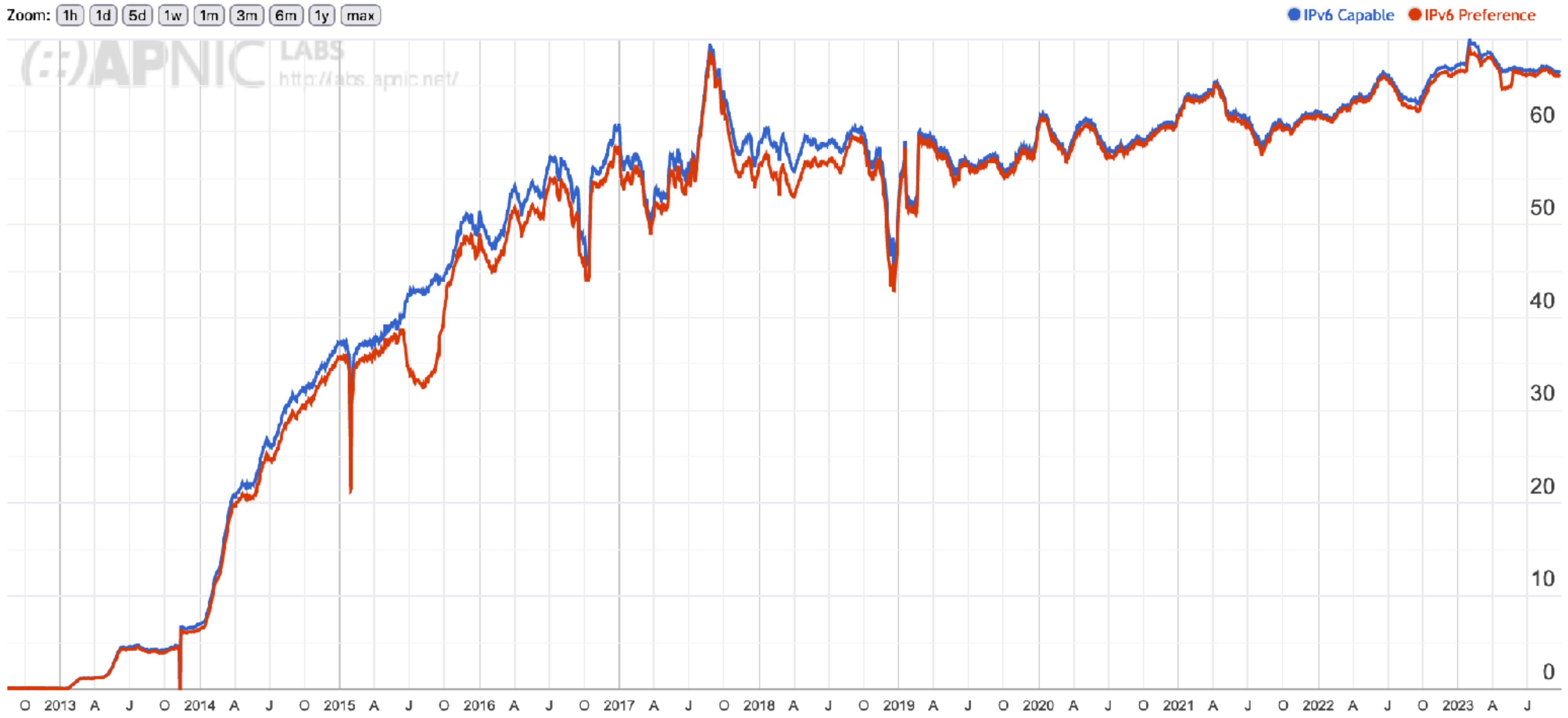
IPv4 waiting list: https://www.ripe.net/manage-ips-and-asns/ipv4/ipv4-waiting-list

IPv4 is the “killer application”

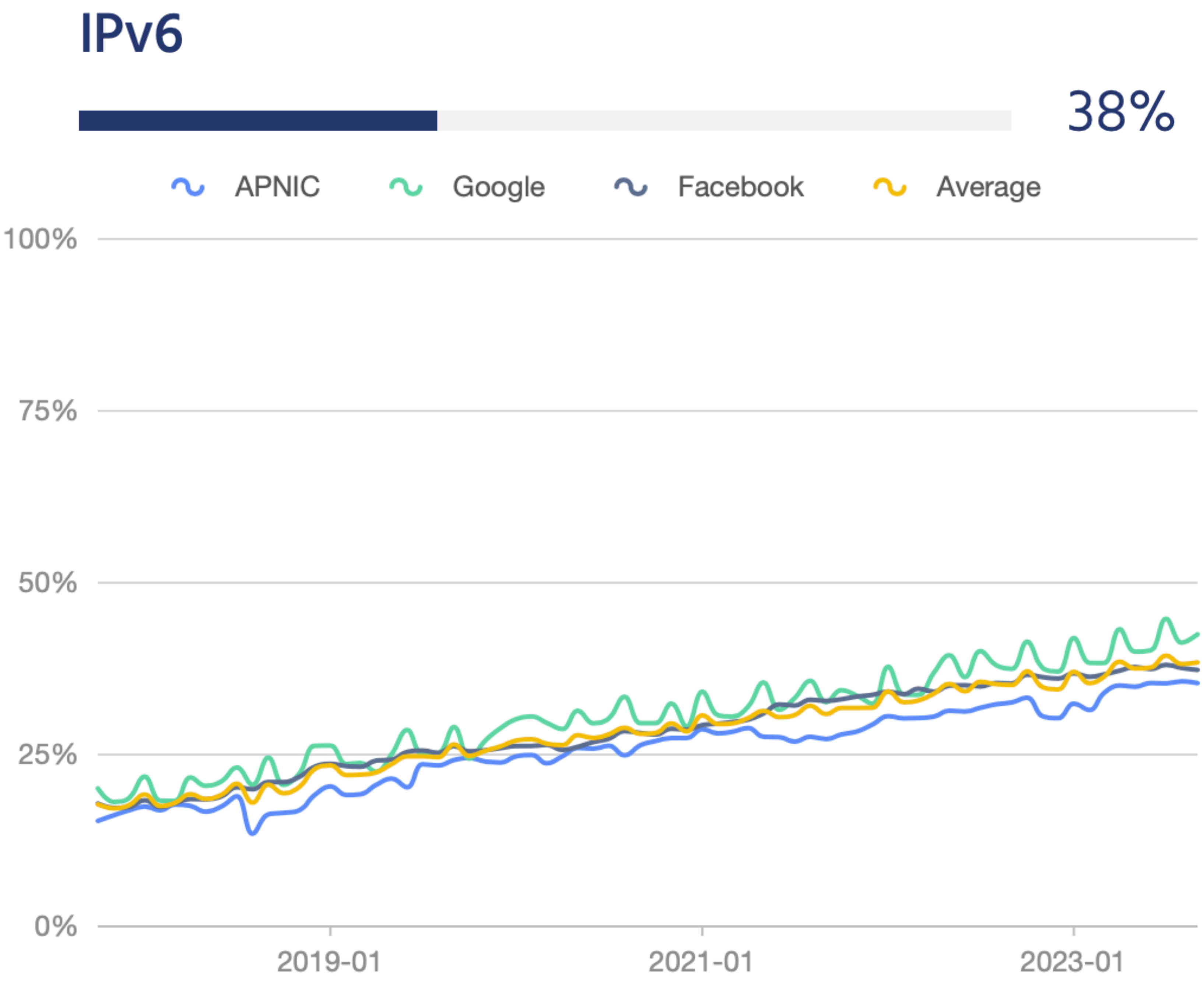
- High price of new IPv4 (needed for new projects i.e. Network expansion)
- CAPEX & OPEX for NAT
- Hidden costs of NAT (ie. troubleshooting, keeping logs) and sub-optimal connectivity
- Cost of postponing the unavoidable transition
- Potential price of own IPv4 (i.e. it can be sold)

Belgium and CGNATs

- Regulated/facilitated and agreement: limit in the number of users per IP using CGNAT (1 IP max 16 users) - **2012**
- To avoid poor service for users and comply with law
- Operators saw it cheaper and easier to move to IPv6



IPv6 is Happening...



Global IPv6 deployment (data sources: APNIC, Facebook and Google)

IPv6

46%

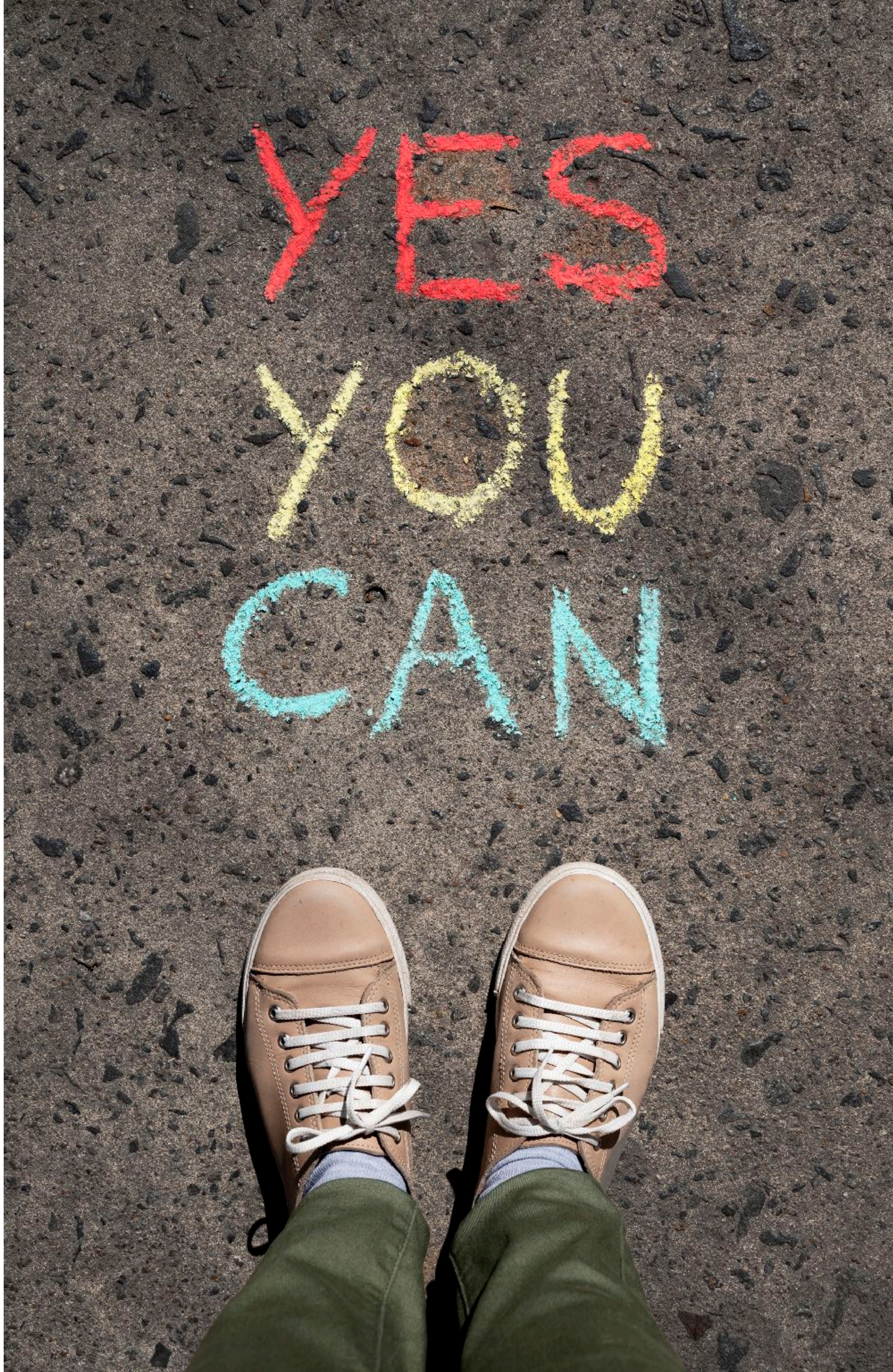
Current percentage of top 1000 websites globally that support IPv6.

Source: https://pulse.internetsociety.org/technologies

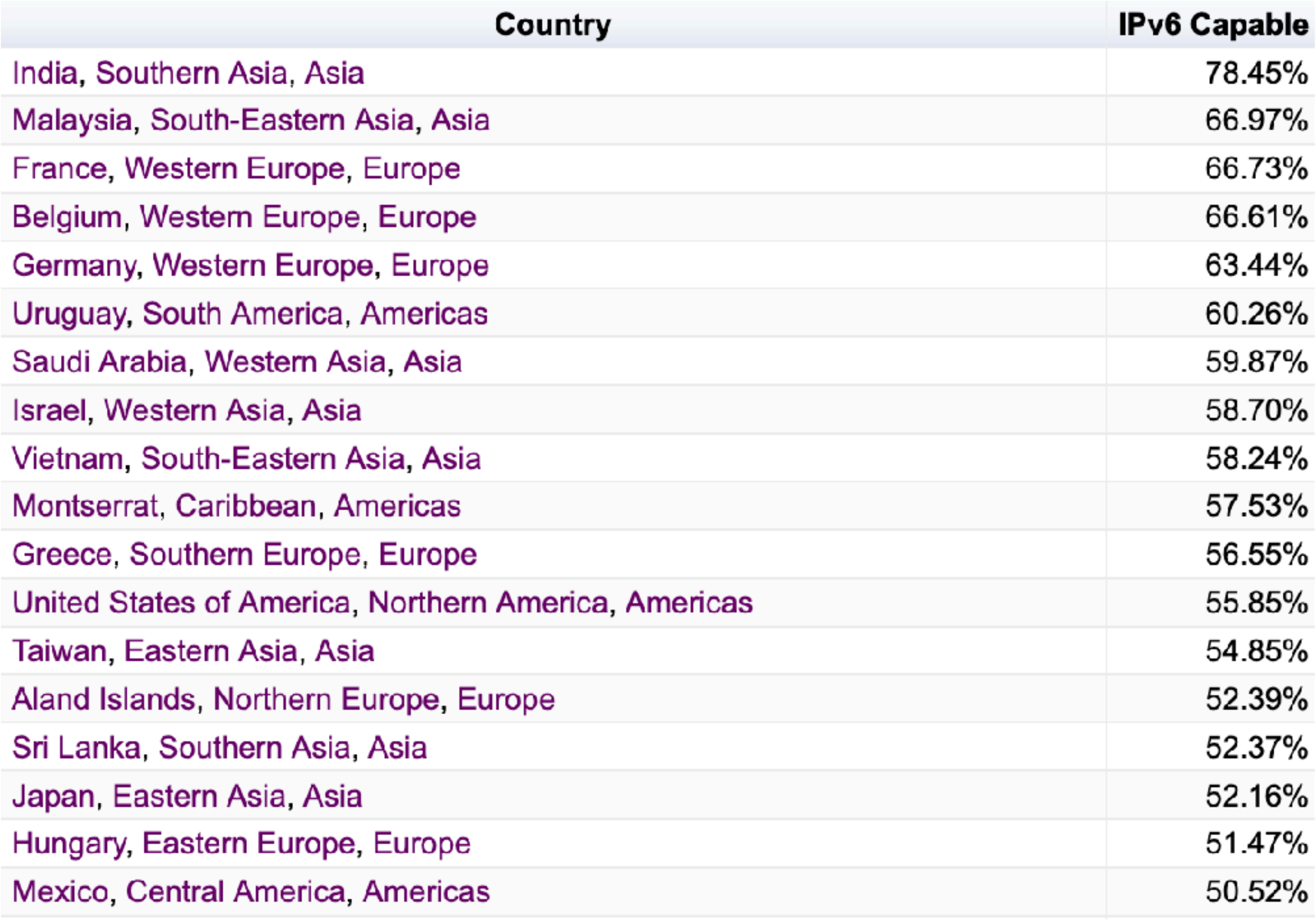
Number of users?

Estimations are well above **1.1 billion users!**

Source: https://stats.labs.apnic.net/v6pop



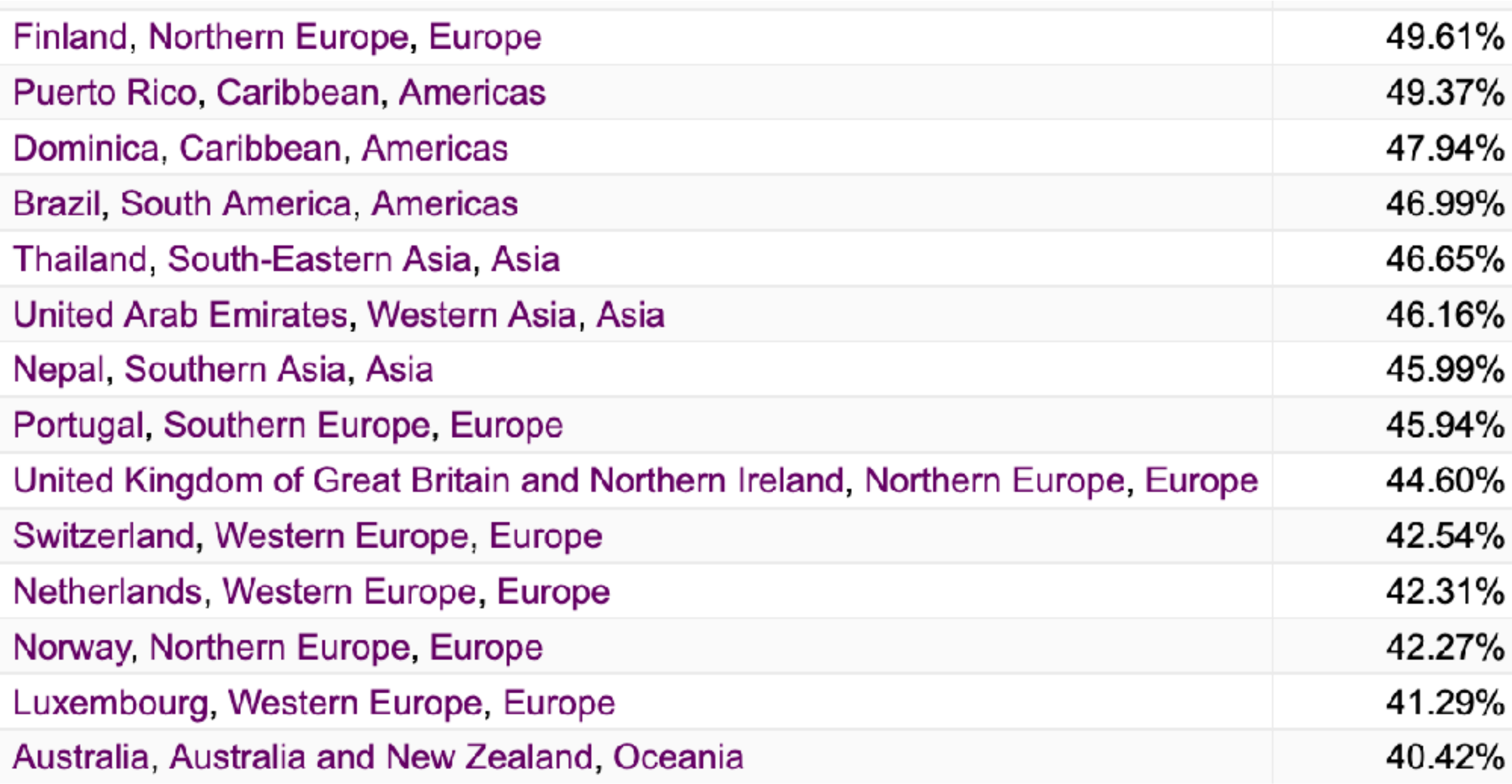
IPv6 is Happening…



Country	IPv6 Capable
India, Southern Asia, Asia	78.45%
Malaysia, South-Eastern Asia, Asia	66.97%
France, Western Europe, Europe	66.73%
Belgium, Western Europe, Europe	66.61%
Germany, Western Europe, Europe	63.44%
Uruguay, South America, Americas	60.26%
Saudi Arabia, Western Asia, Asia	59.87%
Israel, Western Asia, Asia	58.70%
Vietnam, South-Eastern Asia, Asia	58.24%
Montserrat, Caribbean, Americas	57.53%
Greece, Southern Europe, Europe	56.55%
United States of America, Northern America, Americas	55.85%
Taiwan, Eastern Asia, Asia	54.85%
Aland Islands, Northern Europe, Europe	52.39%
Sri Lanka, Southern Asia, Asia	52.37%
Japan, Eastern Asia, Asia	52.16%
Hungary, Eastern Europe, Europe	51.47%
Mexico, Central America, Americas	50.52%

Source: https://stats.labs.apnic.net/ipv6/XA

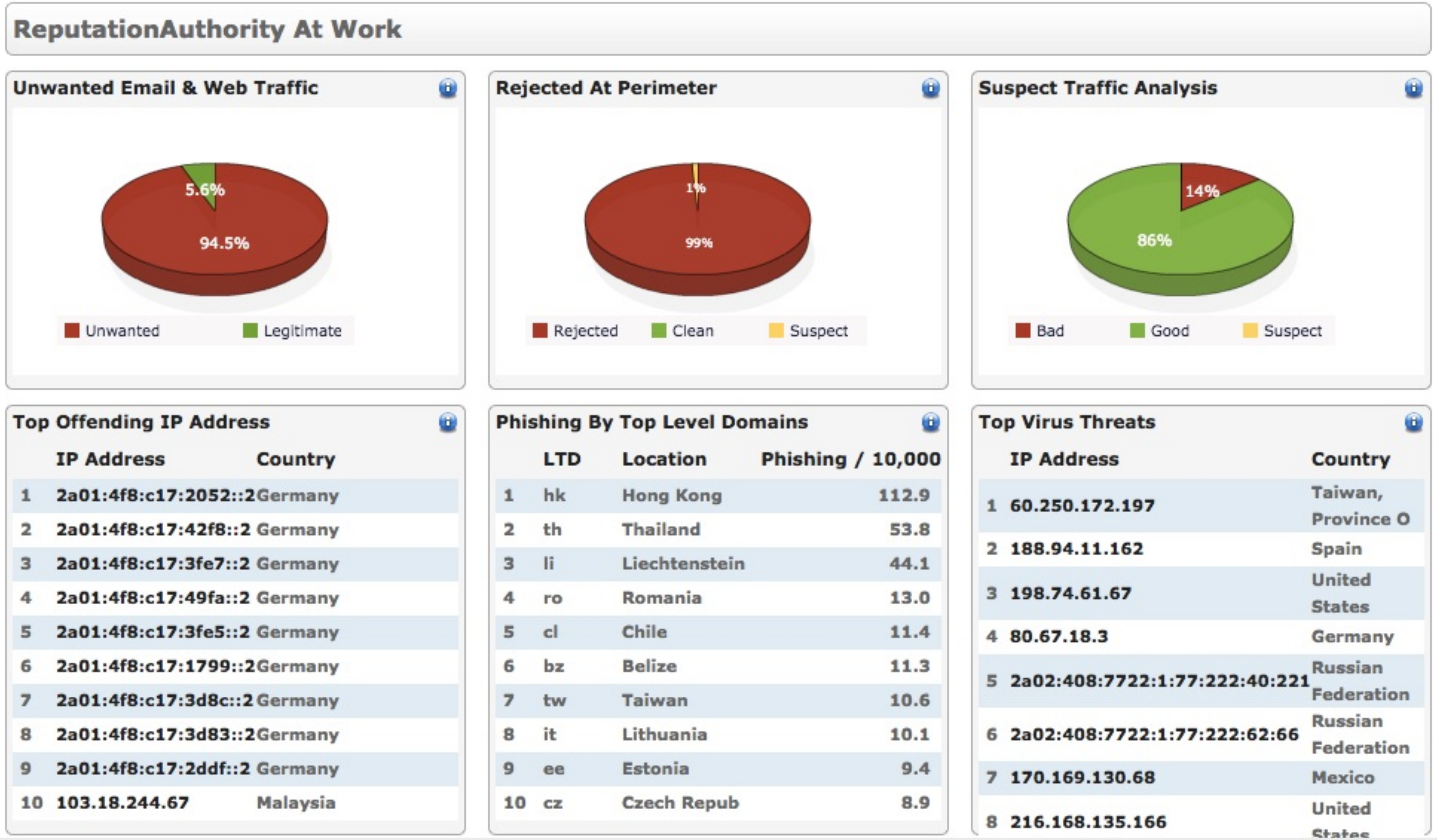
IPv6 is Happening...



Finland, Northern Europe, Europe	49.61%
Puerto Rico, Caribbean, Americas	49.37%
Dominica, Caribbean, Americas	47.94%
Brazil, South America, Americas	46.99%
Thailand, South-Eastern Asia, Asia	46.65%
United Arab Emirates, Western Asia, Asia	46.16%
Nepal, Southern Asia, Asia	45.99%
Portugal, Southern Europe, Europe	45.94%
United Kingdom of Great Britain and Northern Ireland, Northern Europe, Europe	44.60%
Switzerland, Western Europe, Europe	42.54%
Netherlands, Western Europe, Europe	42.31%
Norway, Northern Europe, Europe	42.27%
Luxembourg, Western Europe, Europe	41.29%
Australia, Australia and New Zealand, Oceania	40.42%

Source: https://stats.labs.apnic.net/ipv6/XA

… 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

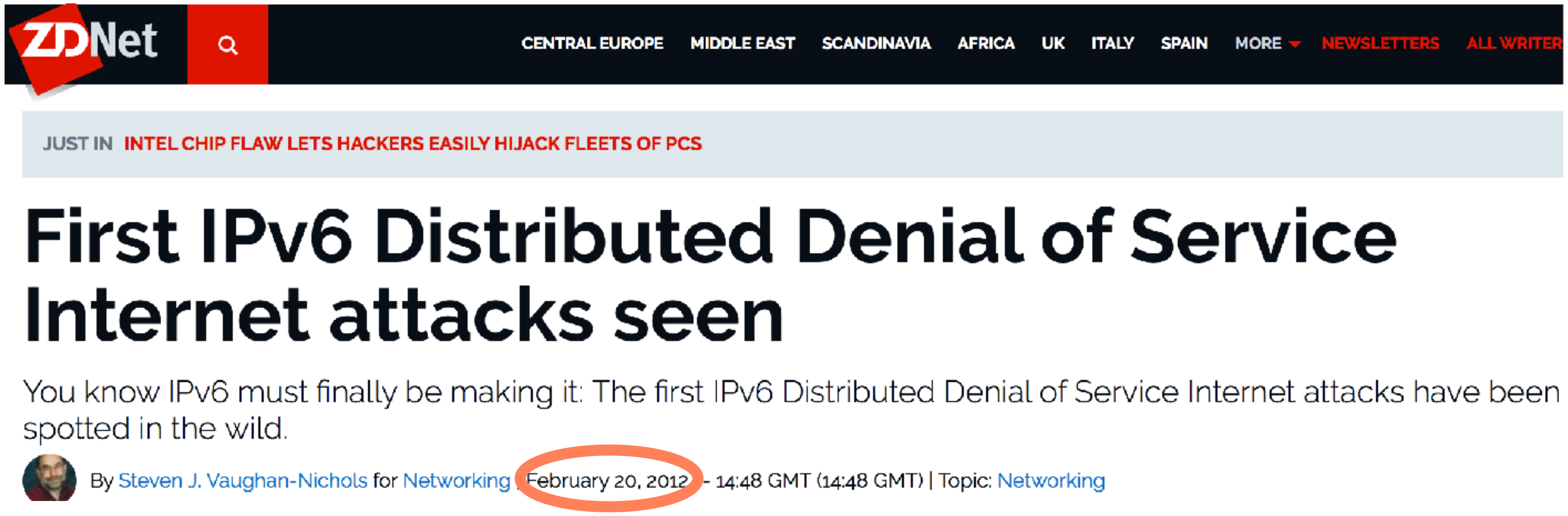
Phishing By Top Level Domains

	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

DDoS attacks in IPv6?

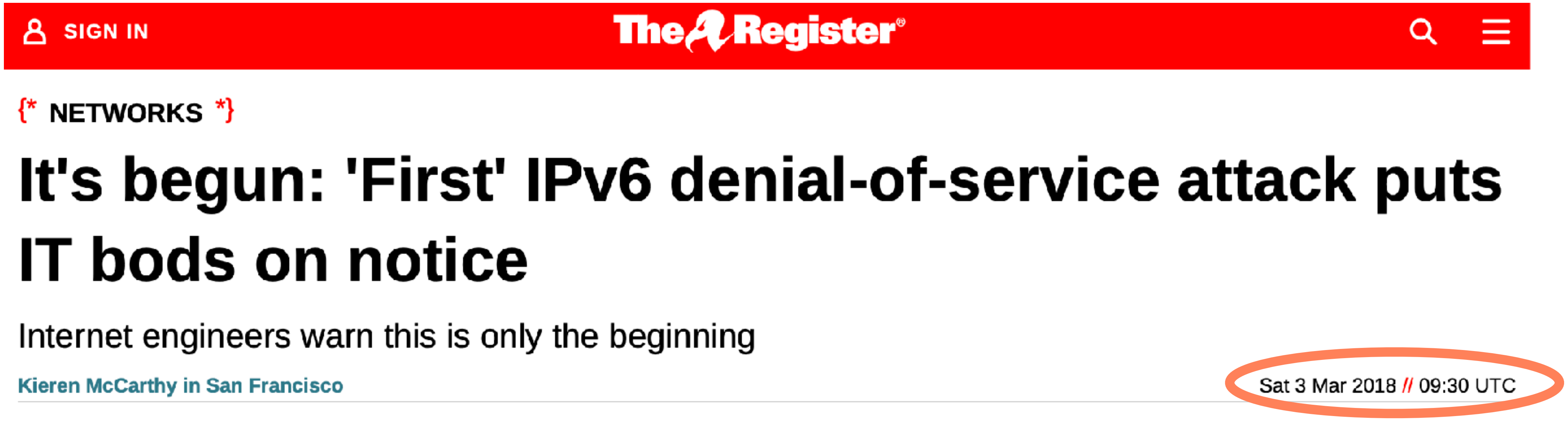


JUST IN INTEL CHIP FLAW LETS HACKERS EASILY HIJACK FLEETS OF PCS

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



{* NETWORKS *}

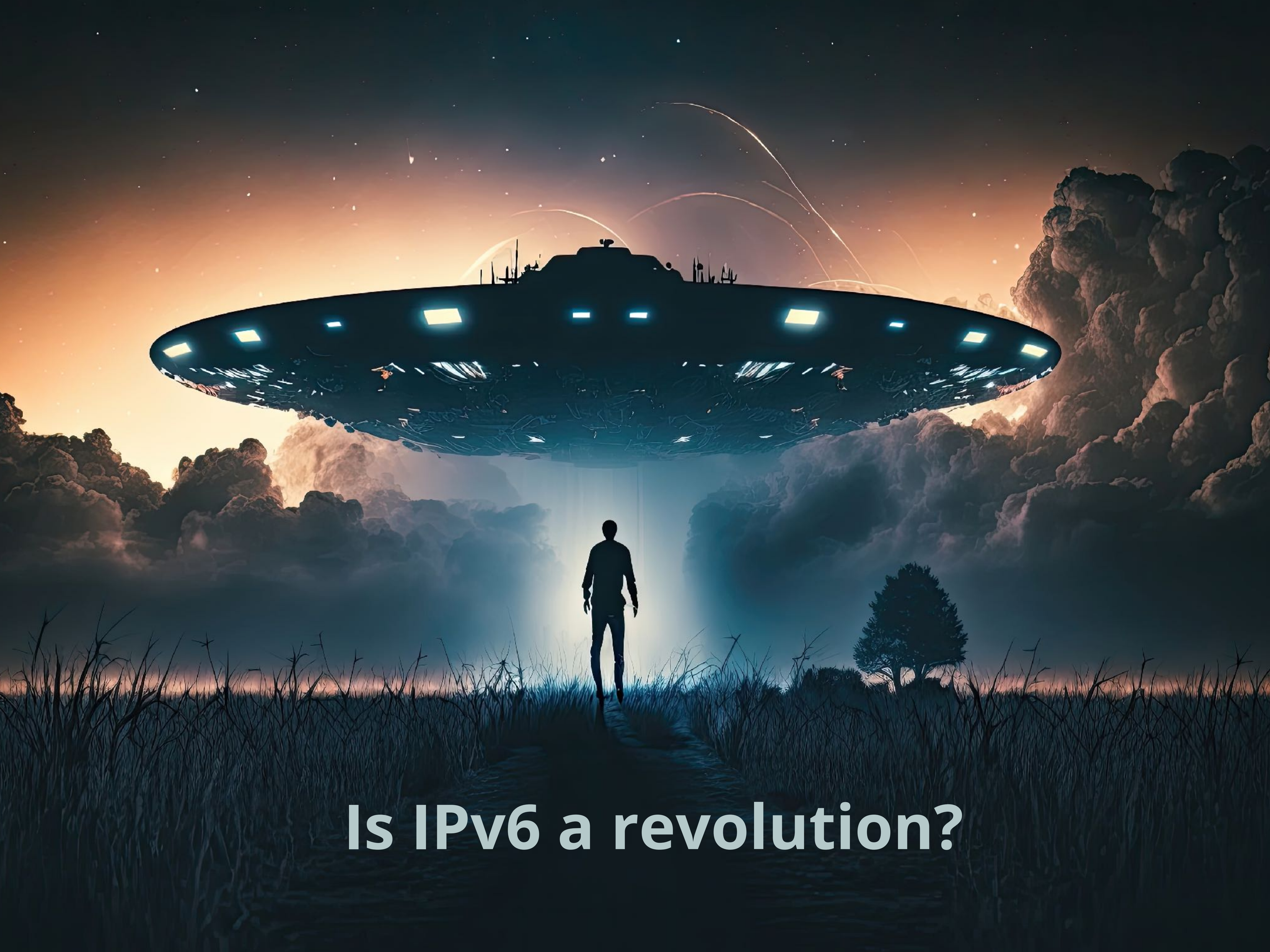
It's begun: 'First' IPv6 denial-of-service attack puts IT bods on notice

Internet engineers warn this is only the beginning

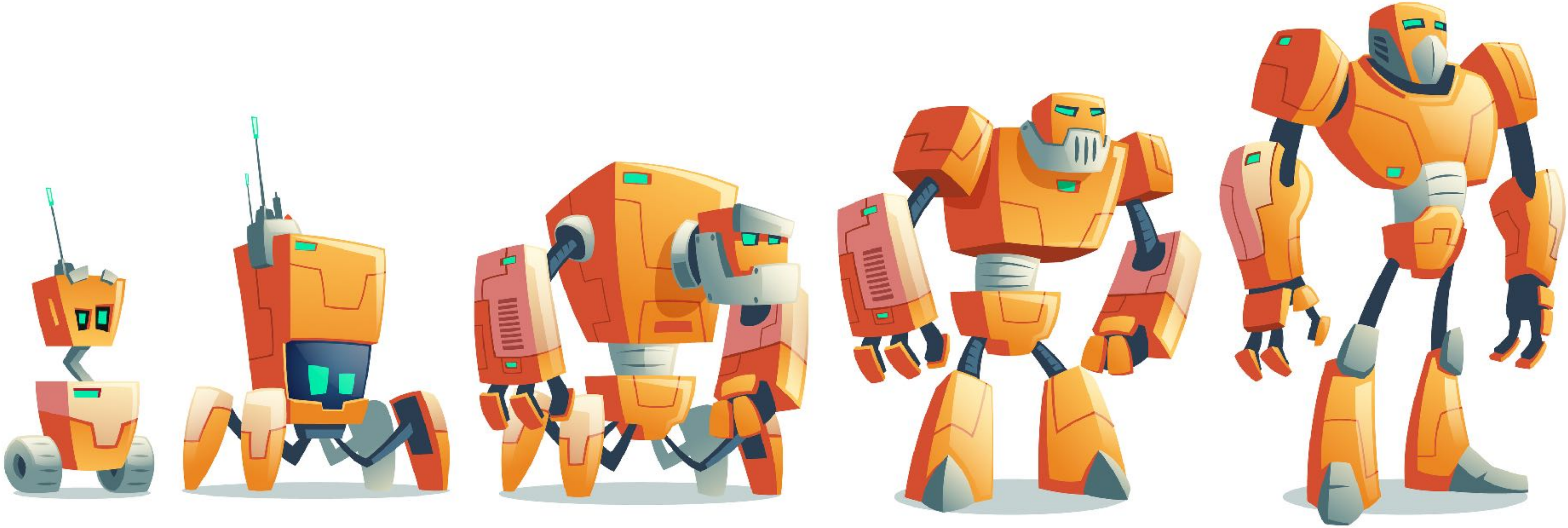
Kieren McCarthy in San Francisco   Sat 3 Mar 2018 // 09:30 UTC

IPv6 is here and is mature.

Is ***security*** *a reason to not implement IPv6?*



Is IPv6 a revolution?



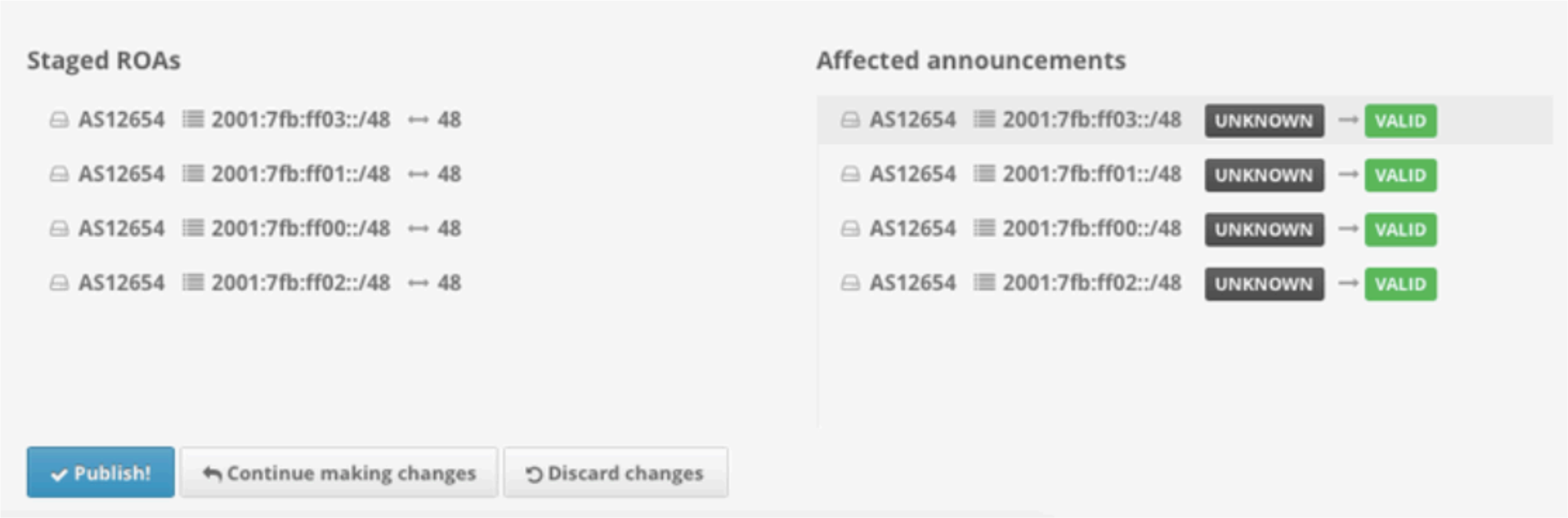
No, IPv6 is an Evolution!

Meaning that...

- Only layer 3/network changes
- Security frameworks, techniques, tools and knowledge can be re-used
- Lot of IP agnostic cybersecurity: based on profiling, identity management, authentication, micro segmentation, etc.
- IPv6 security is just **a piece of the puzzle** in the whole picture

Example: RPKI

- Service offered by RIRs to protect the Internet’s routing (BGP)
- Allows to cryptographically verify if a network (AS) can announce addresses as being used



Staged ROAs

AS12654	2001:7fb:ff03::/48	↔ 48
AS12654	2001:7fb:ff01::/48	↔ 48
AS12654	2001:7fb:ff00::/48	↔ 48
AS12654	2001:7fb:ff02::/48	↔ 48

Affected announcements

AS12654	2001:7fb:ff03::/48	UNKNOWN	→ VALID
AS12654	2001:7fb:ff01::/48	UNKNOWN	→ VALID
AS12654	2001:7fb:ff00::/48	UNKNOWN	→ VALID
AS12654	2001:7fb:ff02::/48	UNKNOWN	→ VALID

Same principles, tools and interface for v4/v6

Managing ROAs:
https://www.ripe.net/manage-ips-and-asns/resource-management/rpki/resource-certification-roa-management

But also…

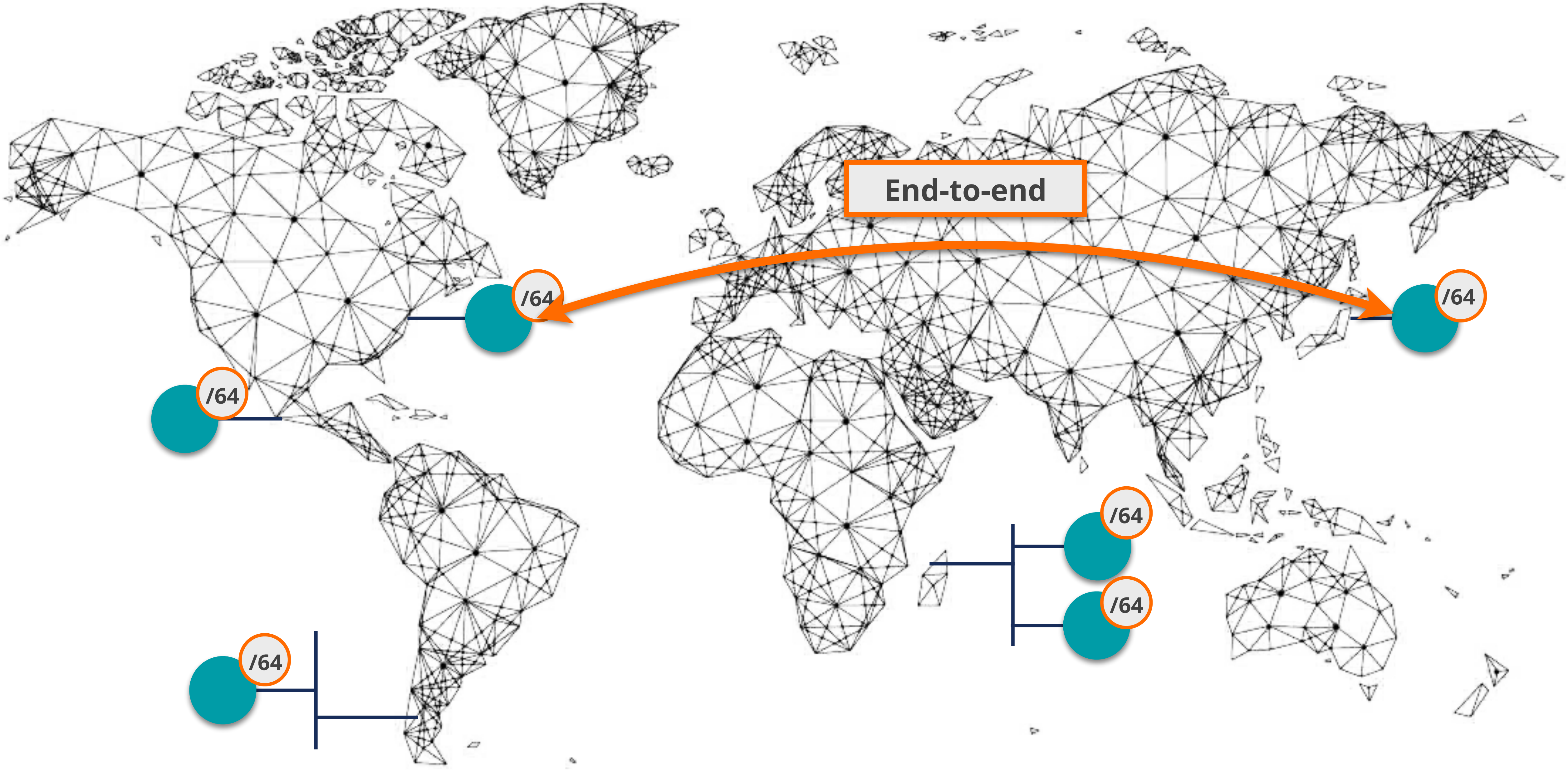
- IPv6 introduces its own new elements that need to be learnt, and taken into account

- IPv6 is not more or less secure than IPv4, is **different**

- You need to design your networks with the appropriate security **for IPv6**

A change of mindset is needed

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



Several changing addresses + more options for autoconfiguration

IPv6 uses some new protocols

- Need to be known, properly configured/used and secured
  - **NDP** (Neighbour Discovery Protocol)
  - **MLD** (Multicast Listener Discovery)

- They have their own **threats** and **security measures**

Transition Mechanisms

Temporary solution with security risks!

Filtering in IPv6 is very Important!

- Global Unicast Addresses
- No NAT anymore, **Firewalls are needed**
- **Good news;** most of the **existing firewalls** support IPv6 already
- A good **addressing plan** → **Easier** filtering!

Investment for IPv6 (Security)

- Most of current deployments support IPv6 already
- Look for **IPv4/IPv6 feature parity check**
  - IPv6 support is not a yes or no question
- No NAT means **firewalls are needed**
- Specific security features may be needed for **switches**/ LANs

- The best investment is in **knowledge!**

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.

How to get started

- Change purchasing procedure (feature parity)
  - Vendors and system integrators must have engineers knowledgeable about IPv6
- Check your current hardware and software
- Plan every step and test
- One service at a time
- Phased approach: face/core/customers
- IPv4 phase out? Dual-stack = bigger attack surface

RIPE-772 Document

- “Requirements for IPv6 in ICT Equipment”
  - Best Current Practice describing what to ask for when requesting IPv6 Support
  - Useful for tenders and RFPs
  - Original version was ripe-554
  - Ripe-554 Originated by the Slovenian Government
  - Adopted by various others (Germany, Sweden)

Link to the document:

https://www.ripe.net/publications/docs/ripe-772

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**

Conclusions

A change of mindset is necessary

- IPv6 is not more or less secure than IPv4
- **Up to date knowledge** is the best security measure
- IPv6 is **mature** and used by more than a billion users
- IPv6 Security should not be a reason to not deploy IPv6

Questions