RIPE NCC
RIPE NETWORK COORDINATION CENTRE

IPv6 & Security

March 2023

Today & Tomorrow

Reaching the next billion: w/ IPv4?

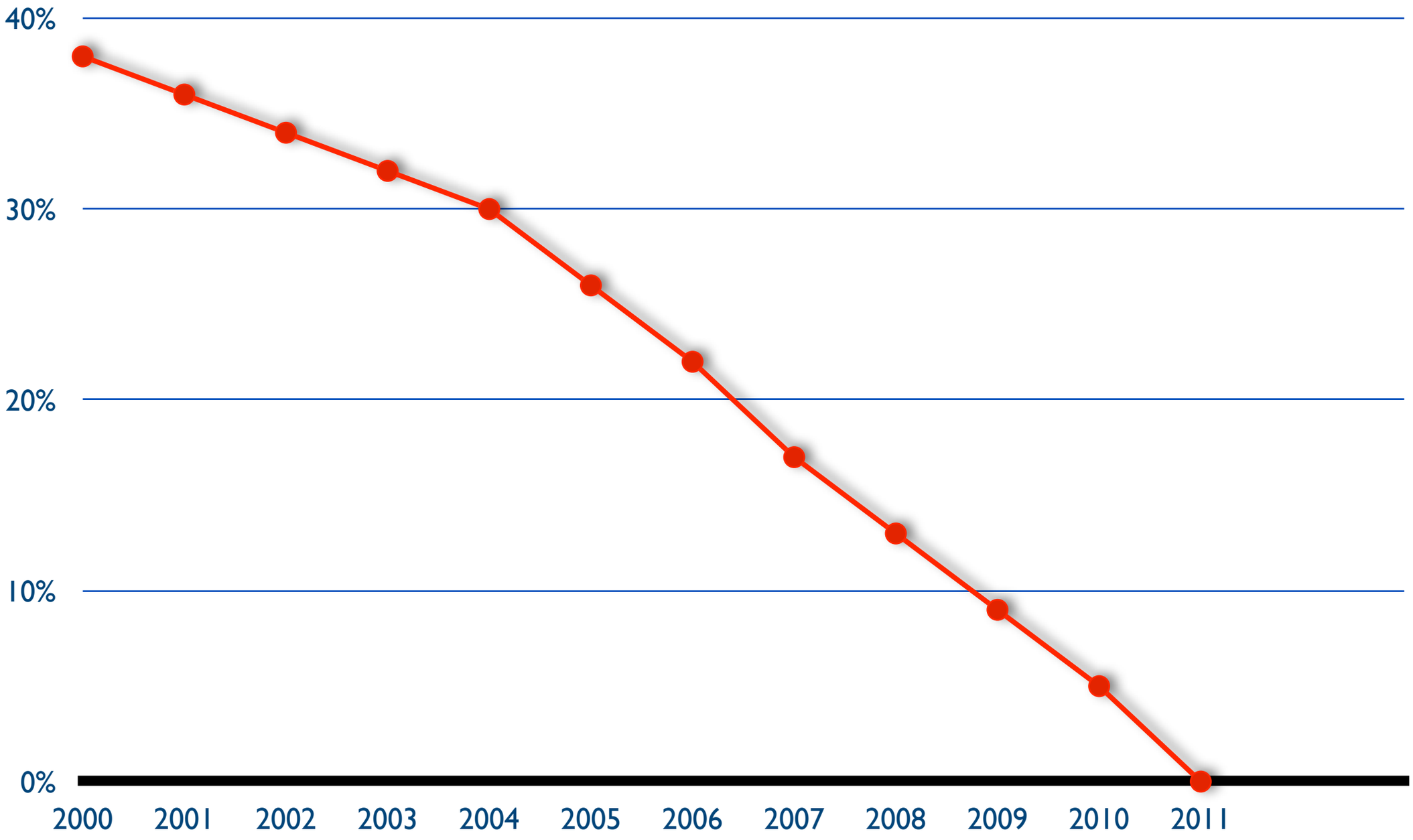
- Around 5,168 billion Internet users now
  - around 65.6 % of all people in the world
- Phones, IP Cameras, “Smart” devices / Gateways are Internet devices
- The Internet of Things
  - How will the Internet look like in 5 - 10 years?

The Internet of Things

Libelium Smart World

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 form at the LIR Portal (/24)
2. Wait

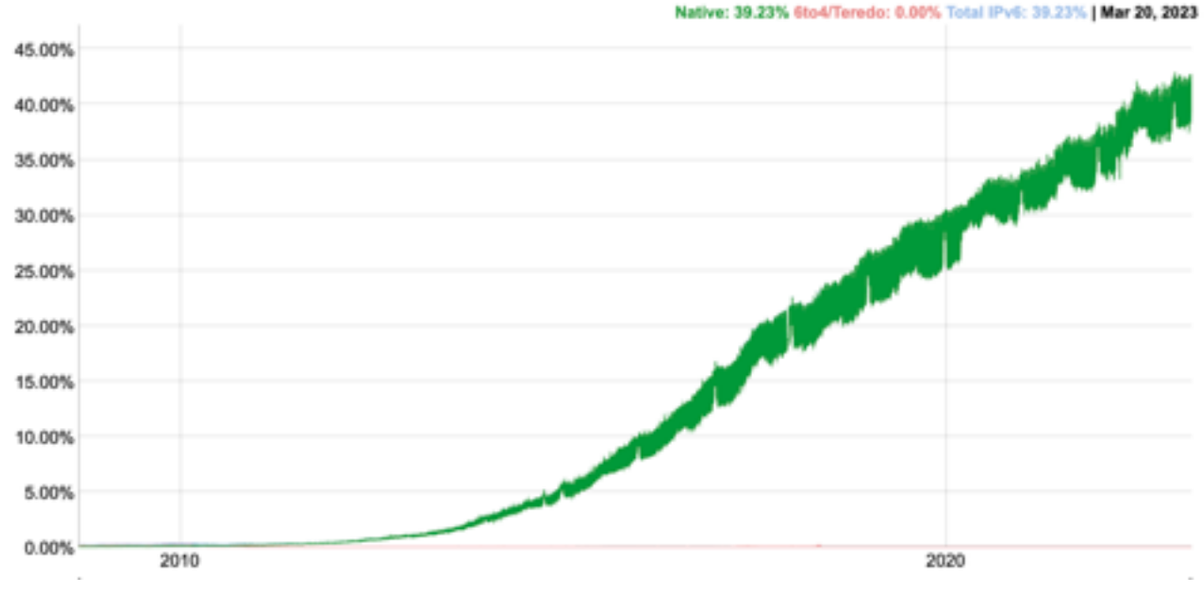
IPv6 is Happening…

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!

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:c17:3fc5::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

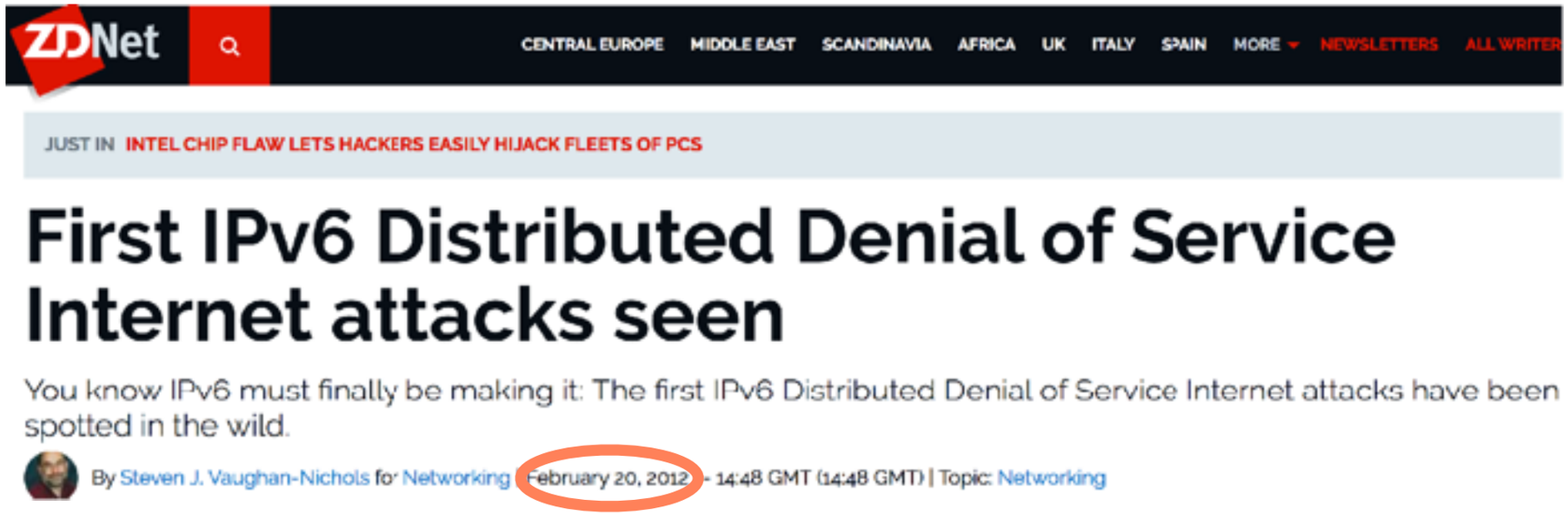
Phishing By Top Level Domains

	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	lt	Lithuania	10.1
9	ee	Estonia	9.4
10	cz	Czech Repub	8.9

Top Virus Threats

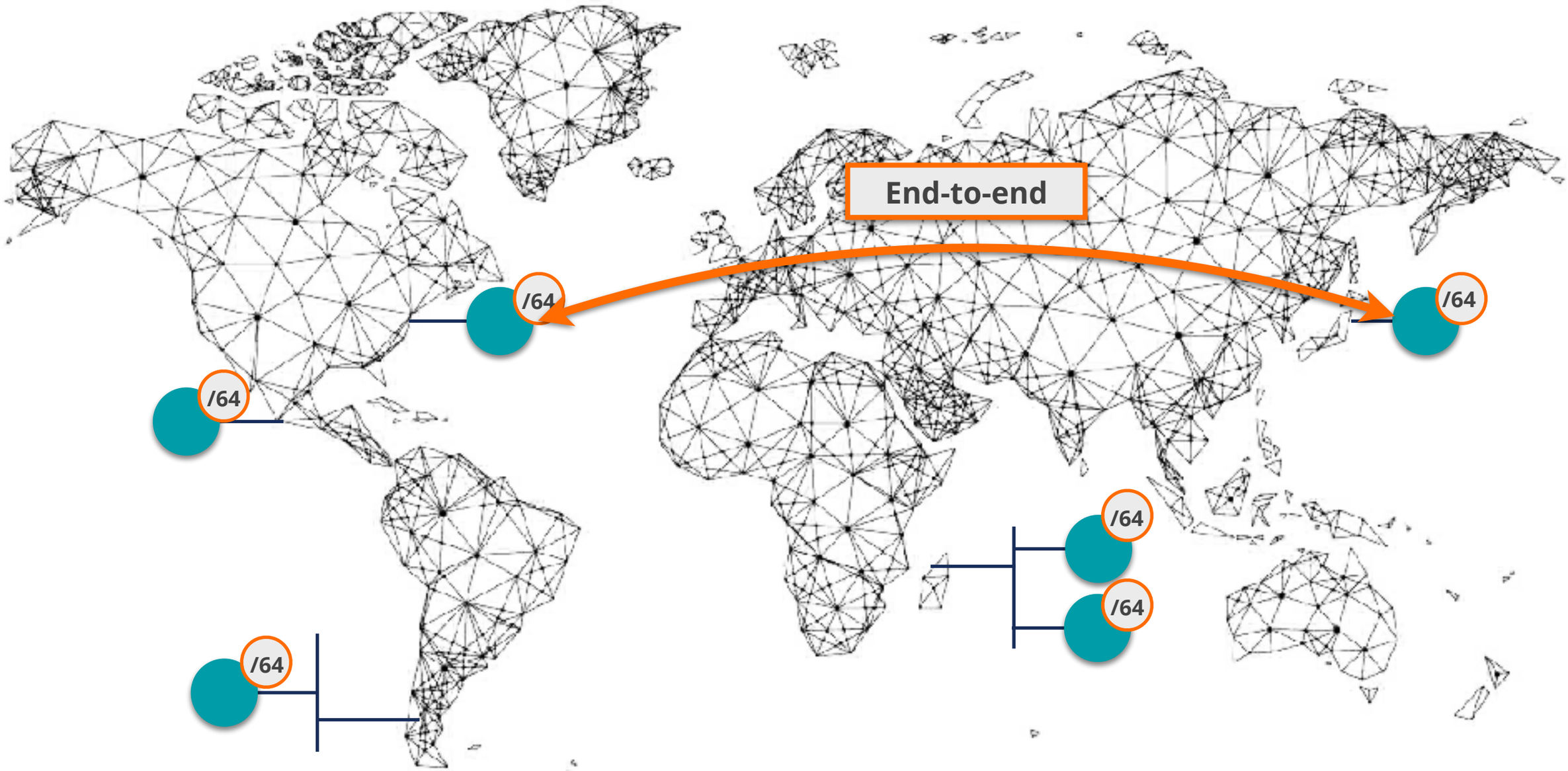
	IP Address	Country
1	60.250.172.197	Taiwan, Province O
2	188.94.11.162	Spain
3	198.74.61.67	United States
4	80.67.18.3	Germany
5	2a02:408:7722:1:77:222:40:221	Russian Federation
6	2a02:408:7722:1:77:222:62:66	Russian Federation
7	170.169.130.68	Mexico
8	216.168.135.166	United States

DDoS attacks in IPv6?



IPv6 Concepts and Investment

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



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 the current deployments support IPv6 already
- Network operators will need to have a **IPv4/IPv6 feature parity check.**
- No NAT; **Firewalls are needed**
- FHS features may be needed for switches in the LANs
- The best investment is for **knowledge!**

How to Deploy & Secure IPv6?

Justification of IPv6 deployment

- Actual price of the new IPv4 (needed for new projects ie. Network expansion)
- CAPEX&OPEX for NAT
- Hidden costs of NAT (ie. troubleshooting, keeping logs)
- Cost of postponing the unavoidable transition
- Potential price of the existing IPv4 base (ie. It can be sold)

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
  - face first
  - core
  - customers

Don’ts for Deployment

- Don't separate IPv6 features from IPv4
- Don't do everything in one go
- Don't appoint an IPv6 specialist
  - do you have an IPv4 specialist?
- Don't see IPv6 as a product
  - the Internet is the product!

For good level of IPv6 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 IPv6 is also responsible for Internet growth

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.

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
- Knowledge of the protocol is the best security measure

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
վերջ
Ende
Koniec
Son
დასასრული
הסוף
Кінець
Finis
Lõpp
Amaia
Tmiem
Liðugt
Kpaj
Sfârşit
Loppu
Slutt
Fund
Kraj
النهاية
Конец
Konec
Τέλος
Fin
Fine
Fí
Край
Einde
Pabaiga
Slut
Fim
Beigas
E1 N1 D2