Initiatives from Korea to lessen cybersecurity divide in the developing countries

Dr. Lee Jeong Min
Korea Internet and Security Agency
Republic of Korea

Korea Internet & Security Agency

Established with the vision of creating a safe Internet environment (July, 2009)

Information Security

Information Security Countermeasure Development
Personal Information Protection

KISC
KrCERT/CC
KOREA INTERNET SECURITY CENTER

Korea Internet & Security Agency
한국인터넷진흥원

Internet Promotion

New Internet Industry Promotion Support
Internet Address Resources Activation

International Cooperation

Overseas Expansion of the Internet Industry
Global Collaboration on Internet Security

ACT ON PROMOTION OF INFORMATION AND COMMUNICATIONS NETWORK UTILIZATION AND INFORMATION PROTECTION, ETC.

Global Cybersecurity Center for Development(GCCD)

GCCD
Global Cybersecurity Center for Development

START

- ✓ Established in 2015 under KISA

Target

- ✓ Public officials in emerging economies and our partners

Mission & Vision

- ✓ To enhance information security capacity of emerging economies.

Programs

- ✓ Joint seminar, Invitation-based training.

Objective

- ✓ Supporting Cyber Capacity Building for Global Community
- ✓ Sharing Practical Cyber Security Knowledge & Experiences

Framework

- ✓ Positioning : A global institute in charge of enhancing national cyber security capabilities
- ✓ Formation : Established as a virtual organization within the KISA at the moment

Major Role

Education

- Invitation-based Training & Joint Local Seminars
- Online Hacking Simulation Test

Consultation

- Establishment of Cybersecurity Master Plan
- Consulting Cybersecurity Policy & Strategies
- Diagnosis of Critical Information Infrastructure Protection

Networking

- Partnership with International Organizations
- Hosting Global Conference and forum

Program List

- The programs of GCCD can be divided into three categories of education, assessment and networking. The followings are the draft program of GCCD. The target participants are from the OECD DAC list of ODA recipients.
- http://www.oecd.org/dac/stats/daclist.htm

1. Invitation-based training and Seminar (in Korea)

- ✓ The GCCD will provide a one-week long invitation-based training course or 2-3 day seminars to support the member countries to respond to cyber incidents and establish cyber protection policies. Internally developed curriculum and training materials will be used to show differences from the existing training programs.

2. Co-hosting Joint Seminar (in a local country)

- ✓ Cybersecurity Joint Seminar will cover various themes requested by an applying country which needs assistance. The GCCD will design a tailored program based on the requests from the country and its level of expertise and knowledge.

3. Consulting

- The assessment will be carried out in a particular public information asset unit level. The range of the assessment is for information management composed of policy, organization, and incident responses. Through this assessment, the recipient country will be able to understand the current status of their cybersecurity competency and guide themselves where to make the right investment and the area where needs further development.

Lesson Learned

- ✓ Need more frequently contact
  - ✓ Communication and sharing Channel
- ✓ Build up successful story for Trust building
  - ✓ Start from low level cooperation to higher level.

2016-2018 GCCD Joint Seminar Programs

Year	Country	Main Topic	Co-host
2016	Montenegro	Critical Information Infrastructure Protection (CIIP)	Ministry for Information Society and Telecommunications (MIST)
2016	Moldova	Information Security Management System (ISMS)	Ministry of Informational Technologies and Communications (MITC)
2016	Guatemala	Cybersecurity Incident Response	Ministerio de Gobernacion(MINGOB)
2016	Bolivia		Cybersecurity Incident ResponseMinisterio de Obras Publicas, Servicios y Vivienda, Autoridad de Regulación y Fiscalización de Telecomunicaciones y Transporte(ATT)
2016	Indonesia	Information Security Manpower Training and Cyber Crime Response	Desk Cyberspace National (DCN)
2017	Ghana	National Cybersecurity Framework	Ministry of Communications(MoC)
2018	Serbia	Cybersecurity policy and CERT operation	Ministry of Interior(MoI)

CMM Follow-up Training

YEAR	Countryw
2017	Kyrgyzstan
2018	FYR Macedonia
2018	Bosnia and Herzegovina
2018	Albania

Cybersecurity Alliance for Mutual Progress(CAMP)

Introduction

START

- ✓ CAMP was officially launched on July 11, 2016 in Korea with 40 organizations from 29 countries to serve as a platform for the members to enhance their cybersecurity capacity.

Mission & Vision

- ✓ CAMP will serve as a network platform to lift up the overall level of cybersecurity of the members.
- ✓ The members will share development experiences and trends of cybersecurity to catalyze mutual growth as well as contribute to development of global cybersecurity for large.

Membership

55 Organizations from 41 Countries

Membership

55 Organizations from 41 Countries

-	AICTO	Kenya	ICT Authority	Peru	CAEN
-	CEABAD	Korea	MSIT	Philippines	DOST-ICTO
-	ECOWAS	Korea	KISA	Senegal	MPT
Azerbaijan	CSC	Kosovo	MED	Rwanda	RDB
Bangladesh	MPTIT	Laos	LaoCERT	Rwanda	RNP
Bangladesh	BDCERT	Laos	MOST	Sierra Leone	MIC
Brazil	NTA	Malaysia	CSM	Sri Lanka	Sri Lanka CERT/CC
Cambodia	MPTC	Malaysia	MCMC	Taiwan	NCCST;TWNCERT
Costa Rica	MICITT	Mauritius	CERT-MU	Tanzania	TCRA
Cote D'Ivoire	MIC	Mauritius	MTCI	Thailand	EGA
Estonia	ISA	Moldova	MITC	Thailand	ETDA
Ethiopia	INSA	Mongolia	CITA	Turkey	ICTA
Gabon	ANINF	Montenegro	MIST	Uganada	NITA-U
Ghana	NITA	Morocco	DGSSI	Uganada	UICT
Guatemala	MINGOB	Nepal	NID	Uzbekistan	ISC
Haiti	CONATEL	Nepal	NITC	Uzbekistan	CoM
Indonesia	BSSN	Nigeria	MIC	Vietnam	VNCERT
Indonesia	Id-SIRTII/CC	Oman	ITA		
Iran	CERT/CC IR	Paraguay	CONATEL		

2018-19 Program of Work

Regional Forums

- Inter-regional forum
- Collaboration with regional and international organizations

Info Sharing

- International cybersecurity conference
- Online Communication

Capacity Building

- Joint workshops & Seminars
- Joint research & survey

Collaboratively increasing the resilience of critical services in the Netherlands through a national DDoS clearing house

Internet Infrastructure Security Day at APRICOT2019
February 23, 2019
Daejeon, South Korea

Cristian Hesselman (SIDN)

A few DDoS trends

- Volume at 1+ Tbps, likely going up (Dyn 1.2 Tbps, GitHub 1.3 Tbps)
- Many widely distributed sources (Mirai 600K, Hajime 400K)
- High propagate rates (e.g., Mirai from 42K to 71K bots in 1 hour)
- Complex traffic (e.g., bot churn, volumetric/TCP state exhaustion)
- Easier to launch through booters/stressers (Mirai)
- Reflection attacks possible (e.g., Mirai and Reaper botnets)

➔ At the same time, our societies increasingly depend on network services!

- Antonakakis, T. April, M. Bailey, M. Bernhard, E. Bursztein, J. Cochran, Z., Durumeric, J. A. Halderman, L. Invernizzi, M. Kallitsis, D. Kumar, C. Lever, Z. Ma, J. Mason, D. Menscher, C. Seaman, N. Sullivan, K. Thomas, and Y. Zhou, "Understanding the Mirai Botnet", 26th USENIX Security Symposium, 2017
- S. Herwig, K. Harvey, G. Hughey, R. Roberts, and D. Levin, "Measurement and Analysis of Hajime, a Peer-to-peer IoT Botnet", Network and Distributed Systems Security (NDSS) Symposium 2019, San Diego, CA, USA, February 2019

Netherlands critical infrastructure

- Services whose “failure or disruption … would result in severe social disruption and poses a threat to national security” (NL gov’t)
- Providers protect their services through (3rd party) DDoS mitigation systems (e.g., scrubbing)
- Limited DDoS information sharing, focus on person-to-person comms during attacks (reactive)
- Trigger to change: estimated 40 Gbps DDoS attacks in January 2018, resulting in various service outages

NOS Nieuws Sport Uitzendingen TELEBLIK AEX 423 km

Na banken nu ook Belastingdienst en DigiD slachtoffer DDoS-aanvallen

MA 29 JANUARI, 10:50 AANGEPAST MA 29 JANUARI, 17:37 BINNENLAND, ECONOMIE

DigiD *Je eigen inlogcode voor de hele overheid*

Home Nieuws Over DigiD Machtigen Veiligheid Vraag en antwoord zoek Sitemap Lees voor

DigiD

Houd uw burgerservicenummer en uw mobiele telefoon bij de hand. Begin de aanvraag

DigiD aanvragen
DigiD activeren
Machtiging regelen
Inloggen Mijn DigiD

Handige links
- Wachtwoord vergeten?
- Nieuw mobiel nummer opgeven?
- Herstelcode ontvangen?

9 januari 2013 - DigiD is op dit moment niet beschikbaar. Naar verwachting kunt u morgenochtend weer gebruikmaken van DigiD. Onze excuses voor het ongemak.

Laatste nieuws
- Waarschuwing valse e-mails DigiD
- Veranderingen in nieuwe versie DigiD
- Is uw computersysteem geschikt voor DigiD?

DigiD
Met uw persoonlijke DigiD (een gebruikersnaam en wachtwoord) kunt u zich identificeren op websites van de overheid en van organisaties die

Waar u kunt inloggen
U kunt uw DigiD gebruiken bij ruim 500 organisaties.

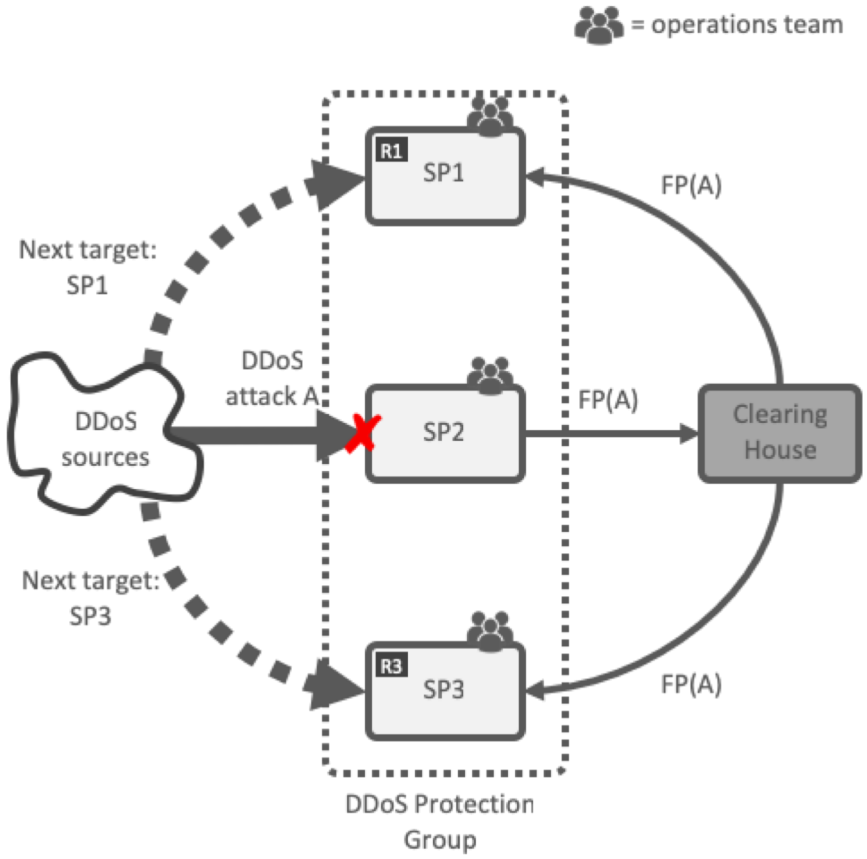
undefined ANP

De golf van DDoS-aanvallen op Nederlandse instellingen houdt aan. Vandaag is de Belastingdienst tweemaal getroffen, en sinds 15.45 uur heeft ook DigiD last van een DDoS-aanval waardoor de site slecht bereikbaar is.

Volgens een woordvoerder van DigiD “gebeurt een aanval wel vaker, maar dit is wel zwaar”. Er wordt hard gewerkt aan een oplossing. Hoelang dat nog gaat duren, kan de woordvoerder niet zeggen.

New: DDoS information sharing in NL

- Continuous and automatic sharing of “DDoS fingerprints” buys providers time (proactive)
- Extends DDoS protection services that critical service providers use and does not replace them
- Improves attribution, allowing for better prosecution and increased deterrent effects
- Open to all critical providers in the Netherlands (Internet, financial, energy, water, etc.)



DDoS fingerprints

- Summary of DDoS traffic
  - Domain names used
  - Source IP addresses
  - Protocol
  - Packet length
  - No victim IP addresses!
- Created from network measurements
  - Examples: PCAP files, Netflow, IPFIX, sFlow, and Logfile
- Fingerprint extension records (optional)
  - Device-specific packet filter rules that ops teams used
  - Suspected type of DDoS attack (e.g., Mirai or Hajime-powered)
  - Contact details of ops team
- Challenge: creation at high speed (10s of Gbps)

Status

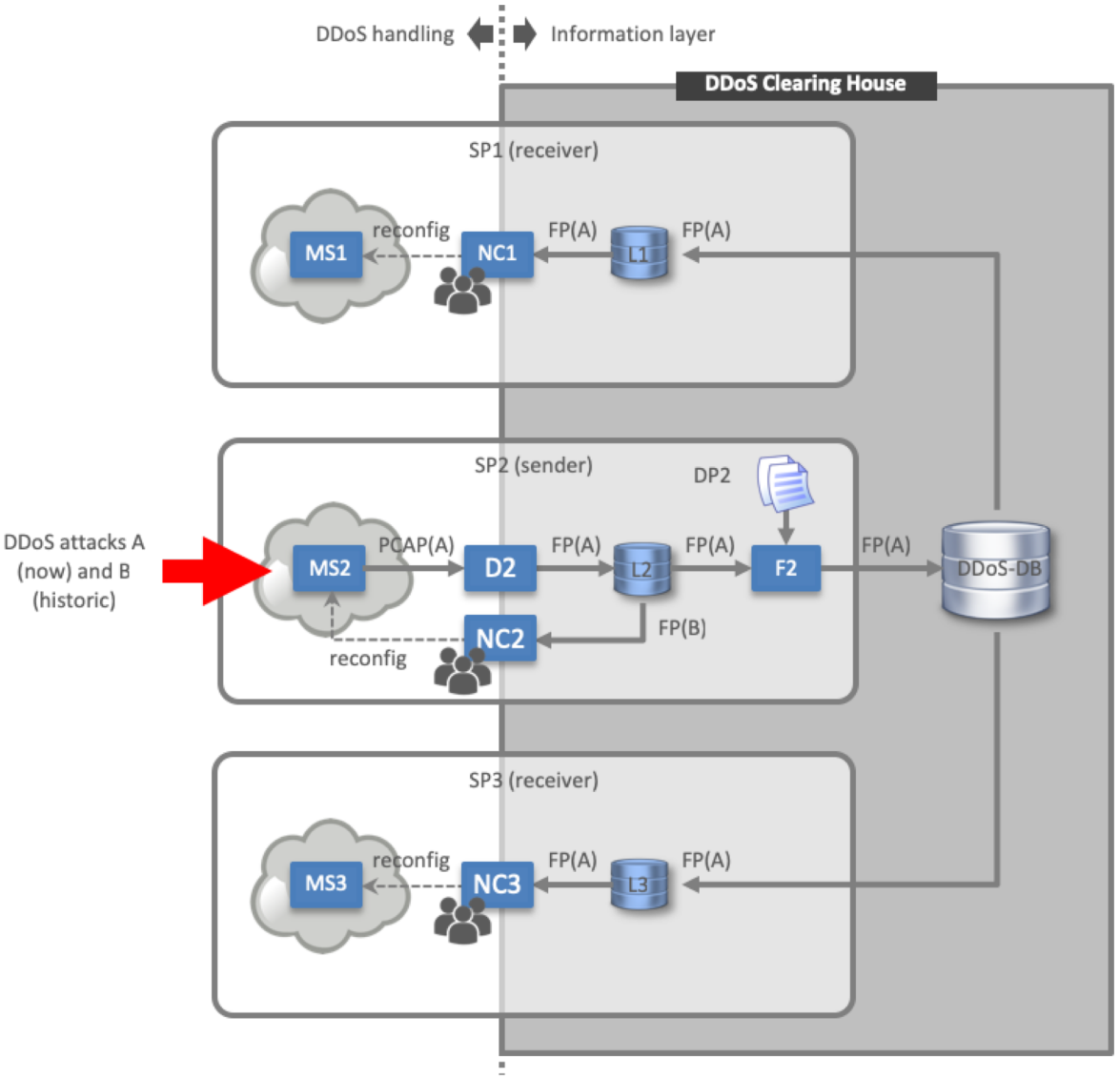
- Embraced by a coalition of 25 players from industry (ISPs, xSPs, IXPs, banks, not-for-profit DPS) and gov't (ministries and agencies)

- Including various existing collaborative anti-DDoS initiatives, such as the Dutch Continuity Board (DCB), NoMoreDDoS, and NaWas

- Working groups:
  - **Clearing house**
  - Cross-industry information sharing
  - Outreach
  - Ground rules and incident response
  - Exercises

- Facilitated by Dutch National Cyber Security Centre (NCSC-NL)

Clearing house overall architecture (DRAFT)



Clearing house pilot

- Netherlands
  - Approach: start small and iteratively scale up to more partners
  - Infra operators: NBIP, KPN, VodafoneZiggo, NL-ix, SIDN
  - Government: THTC, NCSC-NL
  - Financial: Dutch Payment Association
  - Research: University of Twente
- European Union
  - Part of CONCORDIA project (www.concordia-h2020.eu)
  - Development of a “cookbook” to run system in multiple member states
  - Use cases are pilot in the Netherlands and a second one in Italy
- Develop clearing house
  - Extend and improve existing components
  - DDoS-DB of the University of Twente (ddosdb.org)
  - NBIP’s DDoS pattern recognition system (ddos-patterns.net)

Next steps

- Initial version of NL pilot
  - Setting up joint development and experimentation environment
  - First share pre-generated fingerprints, then on-the-fly generated prints
- Agree on and flesh out charter/manifesto
  - WG Ground rules and incident response
- Envisioned growth paths
  - Netherlands → Europe → global (e.g., through CONCORDIA)
  - Extend to “non-critical” service providers

Q&A

Cristian Hesselman
Director SIDN Labs
+31 6 25 07 87 33
cristian.hesselman@sidn.nl
@hesselma

The development of the Dutch national DDoS clearing house is a joint effort of NBIP, KPN, THTC, NCSC-NL, Dutch Payment Association, VodafoneZiggo, NL-ix, SIDN, and the University of Twente (WG clearing house). SIDN and the University of Twente were partly funded by the European Union's Horizon 2020 Research and Innovation program under Grant Agreement No 830927.

IGF Internet Governance Forum

IoT Global Good Practice
www.iot-dynamic-coalition.org

APRICOT 2019, DAEJEON

Building Global Trust in the Internet of Things

THE IGF DYNAMIC COALITION ON IOT BRINGS TOGETHER STAKEHOLDERS FROM ALL OVER THE WORLD TO ENGAGE IN A DIALOGUE ON "GOOD PRACTICE" IN IOT, WITH THE INTENT TO FIND A REALISTIC AND ETHICAL WAY FORWARD

Benefits … and challenges

- New technologies bring us ways to respond to todays' challenges that never existed before … and come with new challenges
- Technologies are not good or bad in themselves – it is how we use them.

Societal challenges

Healthcare; Independent living; Secure society; Sustainable society

Economic challenges

Innovation; growth; profit

Environmental challenges

Scarce resources; waste reduction; environmental monitoring

Governance

Global standards, open standards, multistakeholder involvement, ethical IoT

Privacy and data collection

Big data issues, cloud issues (location, jurisdiction, accountability), digital literacy

Security

Access,Autonomous systems, cyber attacks on new end points

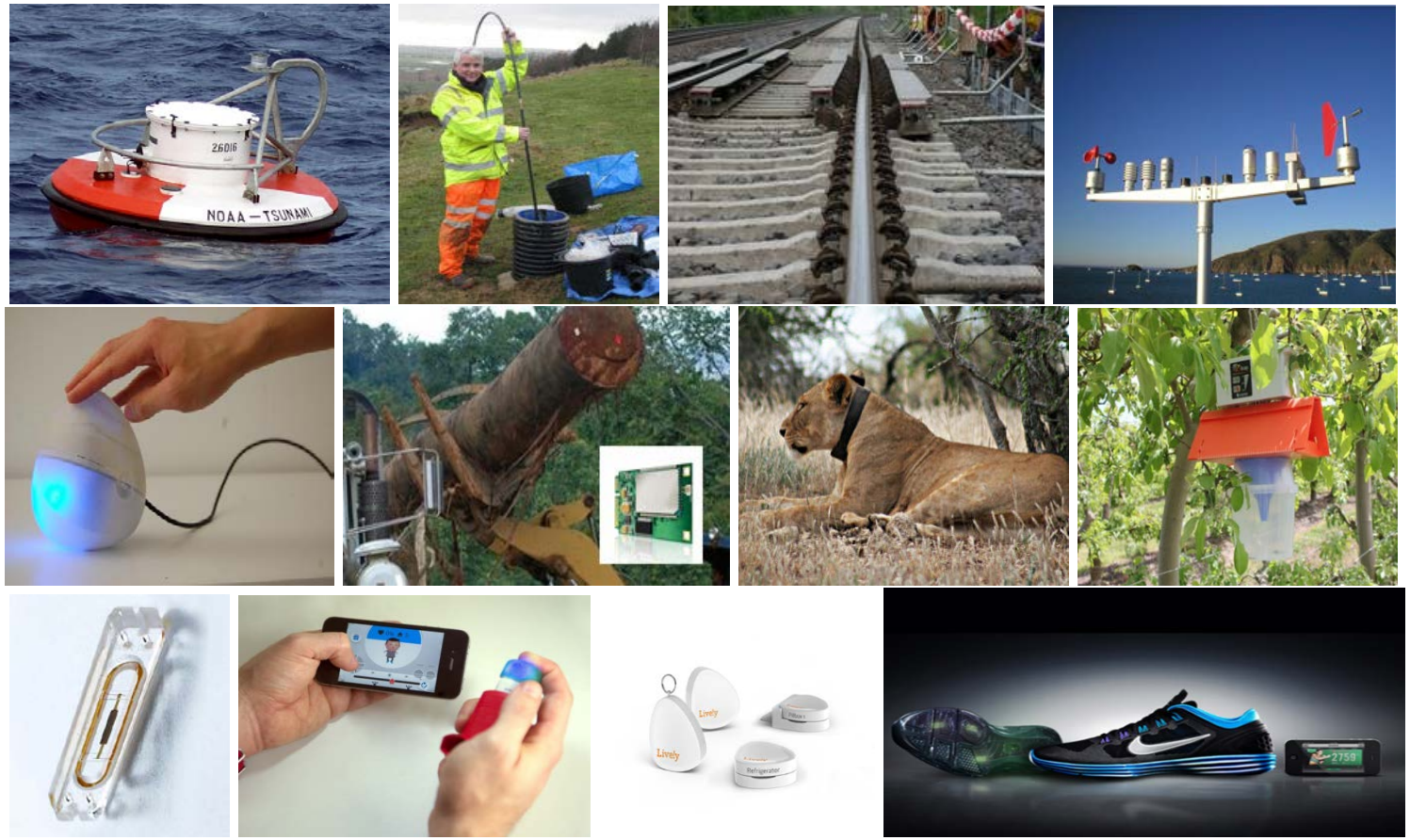
Source: GNKS 2014

Address specific societal issues

- Connected technologies are a necessity to addressing multiple societal challenges in a doable way.
- It requires sharing global knowledge about solutions, and local knowledge and action to make things happen.

Many applications...

- Ranging from:
  - industrial IoT to Consumer IoT;
  - connected emergency warning systems to traffic management systems;
  - Health monitoring and enhancing systems to agriculture applications;
  - Wildlife tracking to security enhacing;
  - Autonomous systems to tools that enhance our human abilities;
  - and much more ....



Global approach towards IoT

IGF AND THE DYNAMIC COALITION ON IOT

IoT is part of Internet

1. IoT is merely a specific aspects of the Internet, just like social media, communication and access to information
2. IoT has specific characteristics that will co-determine the development of future networks. This includes;
   - Collecting, storing and providing access to many data related on observations by sensors;
   - Autonomous networks with actuators that take action following receipt of specific data according to pre-programmed decision models, learning, or external interventions;
   - The possibility to “weaponize” IoT devices to attack third parties.

Dynamic Coalition on IoT

- Set up in Hydrabad (IGF, 2008) and active ever since during IGF and regional meetings
- Aim is to develop a shared understanding
  - on Global Good Practice
    - with regards to the Internet of Things
- most IoT dialogues take place in silos with single stakeholders – in DC IoT ***multi- stakeholders meet on equal terms at global level***

Internet of Things **Good Practice Principle**

- *Internet of Things Good Practice aims at developing IoT systems, products, and services **taking ethical considerations into account from the outset**, both in the development, deployment and use phases of the life cycle, **thus to find an ethical, sustainable way ahead** using IoT to help to **create a free, secure and enabling rights-based** environment: a future we want.*

(IGF Dynamic Coalition on IoT: "IoT Good Practice policies")

IGF DC IoT thinking in summary

Embrace IoT to address societal challenges in an ethical way

- We need IoT to keep this world manageable

Create an IoT environment that encourages investments

- Involve all stakeholders
- Create ecosystem
- Stimulate awareness and feedback
- Provide legal clarity and review the legal mechanisms

Ensure emergence of a trusted IoT environment

- Meaningful transparency
- Clear accountability
- Real choice

Examples from other countries

- Canada
- Netherlands
- United Kingdom

CANADIAN MULTISTAKEHOLDER PROCESS

ENHANCING IOT SECURITY

The Canadian approach

- All stakeholders bear a responsibility and opportunity for the safety and resiliency of the Internet.
- We need urgent and collective action now if we are to make an increasingly-connected world a safe place for users and society-at-large.
- No single stakeholder can solve this alone, and users need to be at the center of solutions. An inclusive and collaborative approach is needed for long-lasting, efficient and flexible solutions.
- The complexity of IoT security necessitates such a bottom-up, organic process to ensure the outcomes address all existing and potential challenges and issues.
- Informed by global experiences.

Initiative focus

- The following three thematic areas have been identified and working groups created for each:

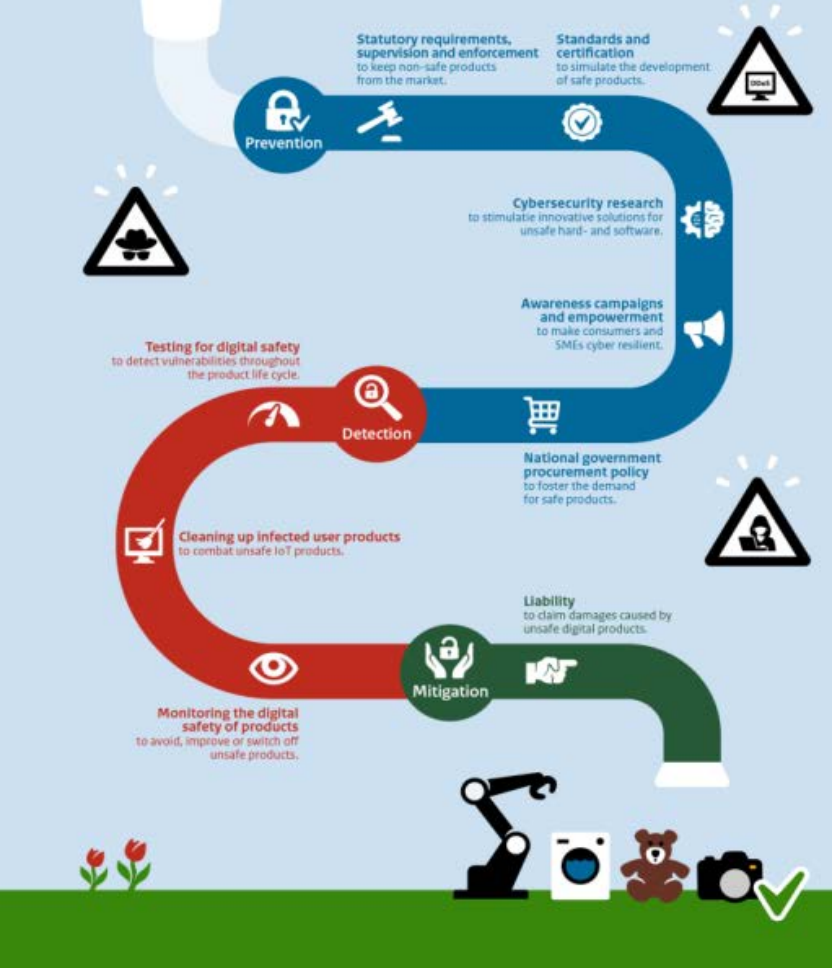
1. **Consumer Education:** the aim of this working group is to establish an education and awareness framework to create a more security-conscious public.
2. **Labelling:** the goal of this group is to scope out possible labelling regimes that could be applied and/or enhanced in the Canadian landscape.
3. **Network Resiliency:** the purpose of this group is to develop a set of recommendations to protect the Internet from things and protect things from the Internet. Thus far, this has coalesced in the form of a secure home gateway which leverages Manufacturers Use Description (MUD).

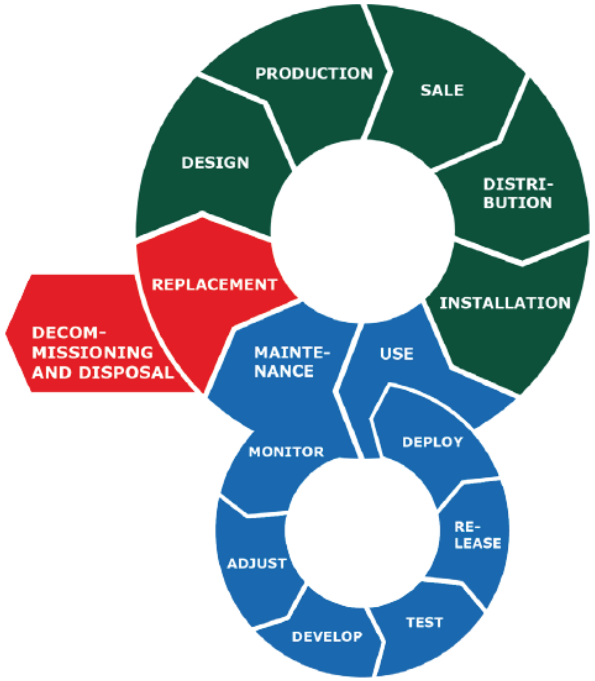
Roadmap

Digital Hard- and Software Security

1. Product life-cycle approach
2. Joint responsibility
3. Balancing public values
4. Portfolio approach
5. Options for a complementary / differentiated approach

Ever more devices are digitally connected to each other and with the Internet. This so-called "Internet of Things" (IoT) makes our lives easier and more fun. But it also leads to new forms of insecurity, precisely because the digital and the 'real' world become intertwined. Vulnerabilities can have major consequences for you and for society as a whole. The measures of this Roadmap provide citizens, businesses and government with a good point of departure to work towards digitally safe products.





Product life cycle approach

Balancing public interest

Joint responsibility

Portfolio approach

Dutch Roadmap Digital Hardware and Software Security:

a complementary approach

Standards and certification

Monitoring digital security

Cleaning up infected products

Testing digital security

Cybersecurity research

Liability

Statutory requirements, supervision and enforcement

Awareness campaigns and empowerment

National goverment procurement policy

UK Government approach

2017 -2018: Cooperation with industry, academia, consumer associations and international partners

March 2018: Policy report

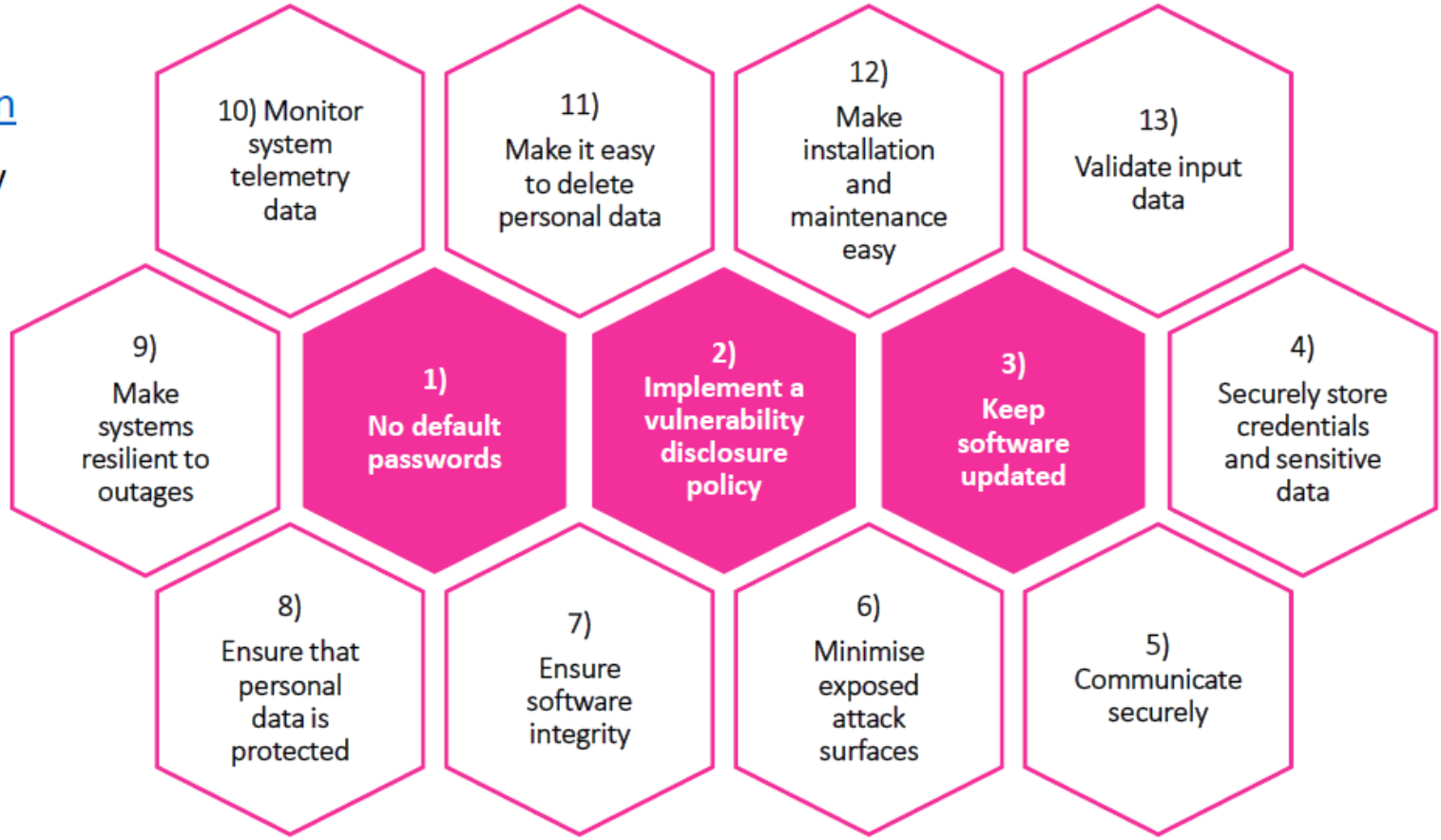
October 2018: Code of Practice for Consumer IoT Security

Mapping of the Code to existing recommendations https://iotsecuritymapping.uk

Consumer guidance https://www.gov.uk/government/publications/secure-by-design

Code of Practice for Consumer IoT Security

- Published in October 2018 in 8 languages: gov.uk/government/publications/secure-by-design
- To help manufacturers protect consumers' privacy and online security.
- Brings together what is widely considered good practice in 13 high-level guidelines.
- Focuses on what matters most.
- Mapped against existing standards and recommendations from 50+ organisations: iotsecuritymapping.uk.



Considerations

- What can we learn from the Canadian approach
  - Use a multistakeholder approach to kick off a flywheel of action
    - Action both in technical community; government units; consumer organisations; kick-off joint position
- What can we learn from the Dutch approach?
  - Complementary measures:
    - Liability (stick behind the door); Government procurement (backing up development of standards); Reviewing legislation (statutory requirements supervision and enforcement); Cleaning up infected products (joint LEA – industry action?)
- What can we learn from the British approach?
  - Working towards a Code of Practice for industry?
    - Adopting the British one – or at least use it for discussion with industry and other stakeholders
- ***Keep an eye on global developments! To learn, and to tack on as IoT goes across borders, as well***

Global Action

IN SUPPORT OF LOCAL ACTION

IoT Global Good Practice
www.iot-dynamic-coalition.org

Search

IGF Dynamic Coalition on the Internet of Things

Welcome to the Dynamic Coalition on Internet of Things (DC IoT)

The Internet of Things (IoT) has been an emerging technology that is now rapidly coming to fruition, recognized by Gartner in 2014 to come to the top of the technology hype cycle … and staying there in 2015.

"Networked technology is spreading rapidly from traditional devices to everyday items, and even to the spaces in which we live. Before long, online functionality will be ubiquitous in the most commonplace objects, allowing them to identify, communicate and cooperate with one another."

As was recognized during the World Economic Forum in January 2015, the "phenomenon known as the Internet of Things'" will touch all. And whereas this brings many promises for a future that is yet to unfold, it also comes with challenges to all stakeholders, in particular related to dealing with security, safety, and governance, and related to the trust of people from different regions and


Internet of Things (IoT)
Read the Online Trust Alliance (OTA) IoT Framework

INTERNET OF THINGS

Internet of Things: Standards and Guidance from the IETF

By: Ari Keränen, Carsten Bormann

Date: April 17, 2016

A true Internet of Things (IoT) requires “things” to be able to use Internet Protocols. Various “things” have always been on the Internet, and general-purpose computers at data centers and homes are usually capable of using the Internet protocols as they have been defined for them. However, there is considerable value in extending the Internet to more constrained devices that often need optimized versions or special use of these protocols.

RELATED ARTICLES

Rough Guide to IETF 103: Internet of Things

Rough Guide to IETF 102: Internet of Things

Managing the Internet of Things – It’s All About

Study Group 20 at a glance

ITU-T

ITU-T in brief

The framework of ITU-T

ITU-T Study Groups

Standards development

Standards approval

ITU-T Study Group 20 - Internet of Things, smart cities and communities

- Homepage of ITU-T Study Group 20

Study Group 20 is working to address the standardization requirements of Internet of Things (IoT) technologies, with an initial focus on IoT applications in smart cities and communities (SC&C).

SG20 develops international standards to enable the coordinated development of IoT technologies, including machine-to-machine communications and ubiquitous sensor networks. A central part of this study is the standardization of end-to-end architectures

Newsfeed | Study Groups

Future Networked Cars: Saving millions of lives, wirelessly
Published Fri, 22 Feb 2019

The opportunity of 5G for the automotive sector: Q&A with Audi's Matthias Schneider
Published Thu, 21 Feb 2019

How ITU and NGMN are promoting a 'level playing field' for 5G intellectual property licensing

https://iot.ieee.org

IEEE Internet of Things

IEEE

Search IEEE IOT

Search

Join the IoT Technical Community

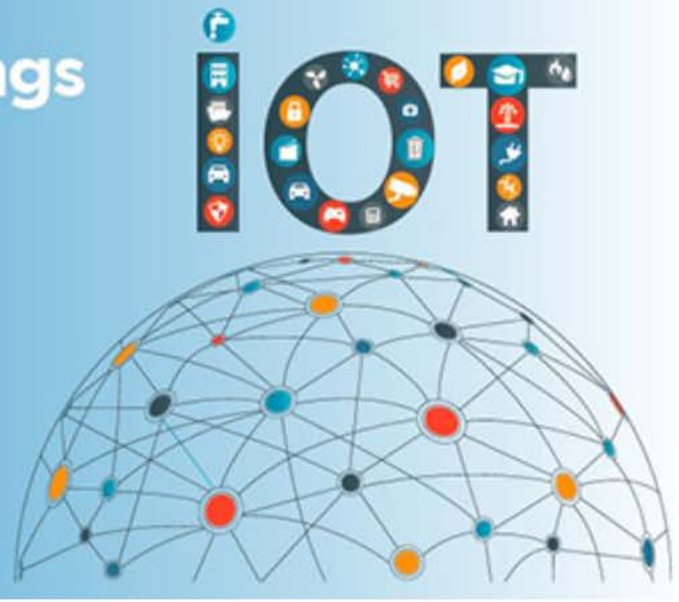
Home | About | What's New | Conferences & Events | IoT Magazine | Newsletter | Publications | Standards | Scenarios | Define IoT | Education

Now Available: IEEE Guide to the Internet of Things

Meet your CEU and PDH requirements with these new courses from IEEE IoT.

- What is the Internet of Things?
- IoT Software: Fundamental Concepts and State of the Art
- Exploring IoT Industry Applications in Healthcare
- Social Internet of Things Platforms, Reference Architecture, Use Cases

Learn more



ENG 23:24 22/02/2019

Back

ETSI releases first globally applicable standard for consumer IoT security

ETSI RELEASES FIRST GLOBALLY APPLICABLE STANDARD FOR CONSUMER IOT SECURITY

Sophia Antipolis, 19 February 2019

The ETSI Technical Committee on Cybersecurity (TC CYBER) has just released ETSI TS 103 645, a standard for cybersecurity in the Internet of Things, to establish a security baseline for internet-connected consumer products and provide a basis for future IoT certification schemes.

As more devices in the home connect to the internet, the cyber security of the Internet of Things (IoT) is becoming a growing concern. People entrust their personal data to an increasing number of online devices and services. In addition, products and appliances that have traditionally been offline are now becoming connected

We create the world of tomorrow with the choices and actions of today …

More information

- Internet Society activities:
- http://www.internetsociety.org
- IGF DC IoT activities:
- http://www.iot-dynamic-coalition.org/
- IEEE new standard for IoT Security
- IETF work on MUD

IoT Global Good Practice

www.iot-dynamic-coalition.org

IPv6: Deployment Status, Standards and Best Practices

February 2019

Daejeon, South Korea

@JordiPalet

(jordi.palet@theipv6company.com)

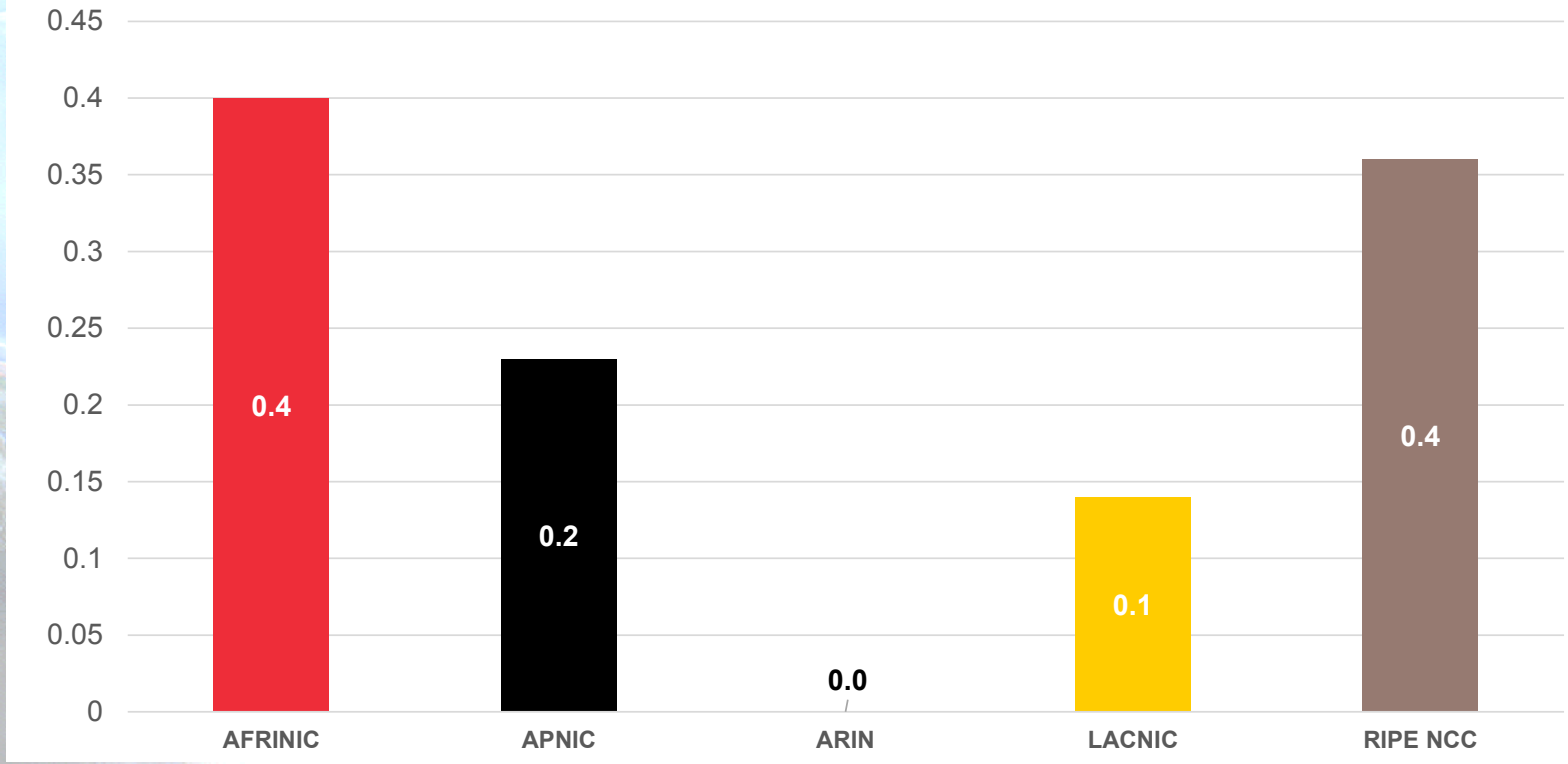
IPv4 is gone! IPv6 was born!

- In 1992 IETF realized that IPv4 is not sufficient
- Work started for IPng
- IPv6 specs:
  - RFC1883 (1995)
  - RFC2460 (1998)
  - RFC8200/STD86 (2017)
- Other (main) specs:
  - RFC8201/STD87 (PMTUD)
  - RFC3596/STD88 (IPv6 DNS extensions)
  - RFC4443/STD89 (ICMPv6)
  - RFC4291 (Addressing Architecture)

Available IPv4

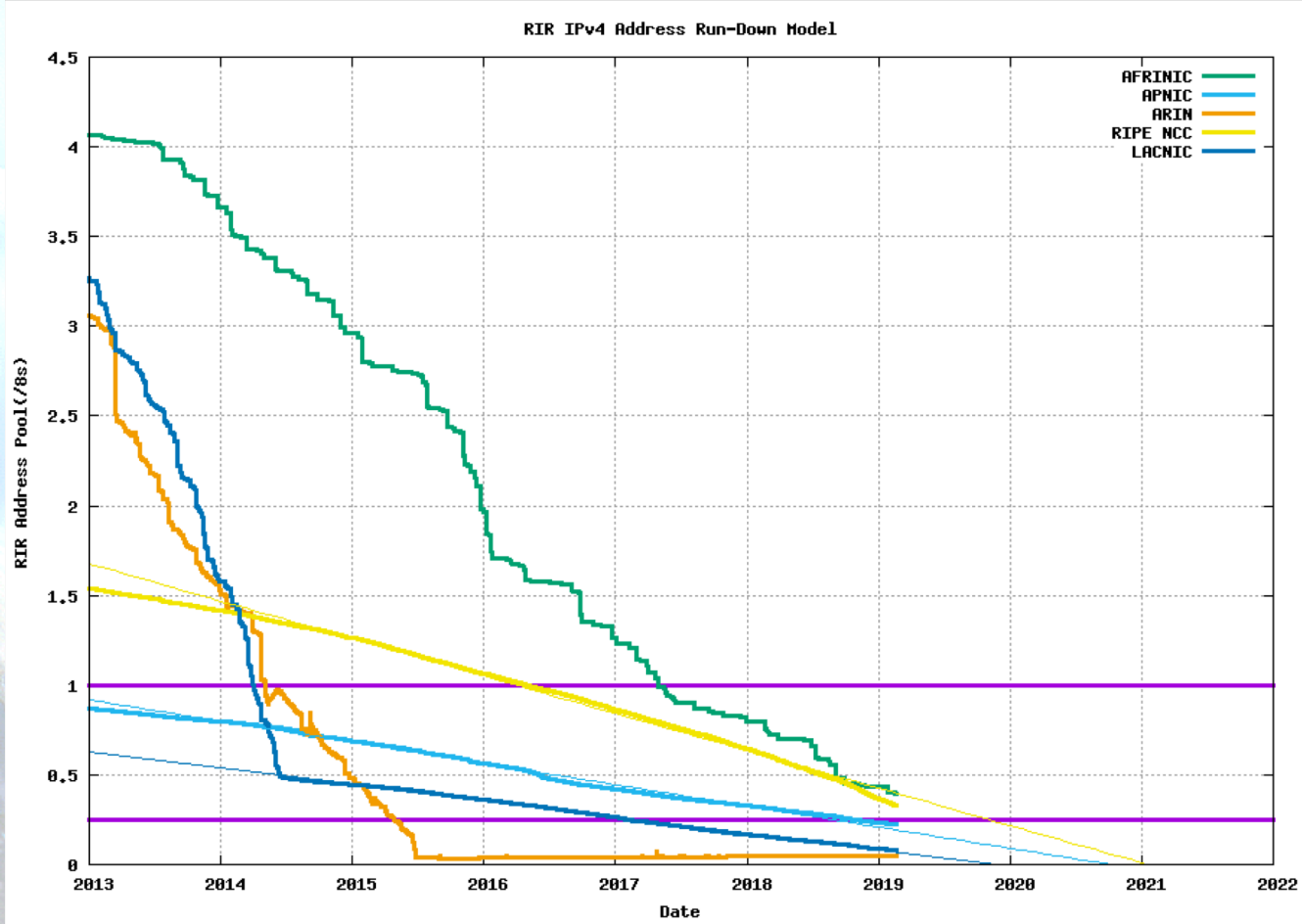
In terms of /8s

Note: Each /8, in IPv4, is a block of 16.777.216 addresses



* NRO, December 2018

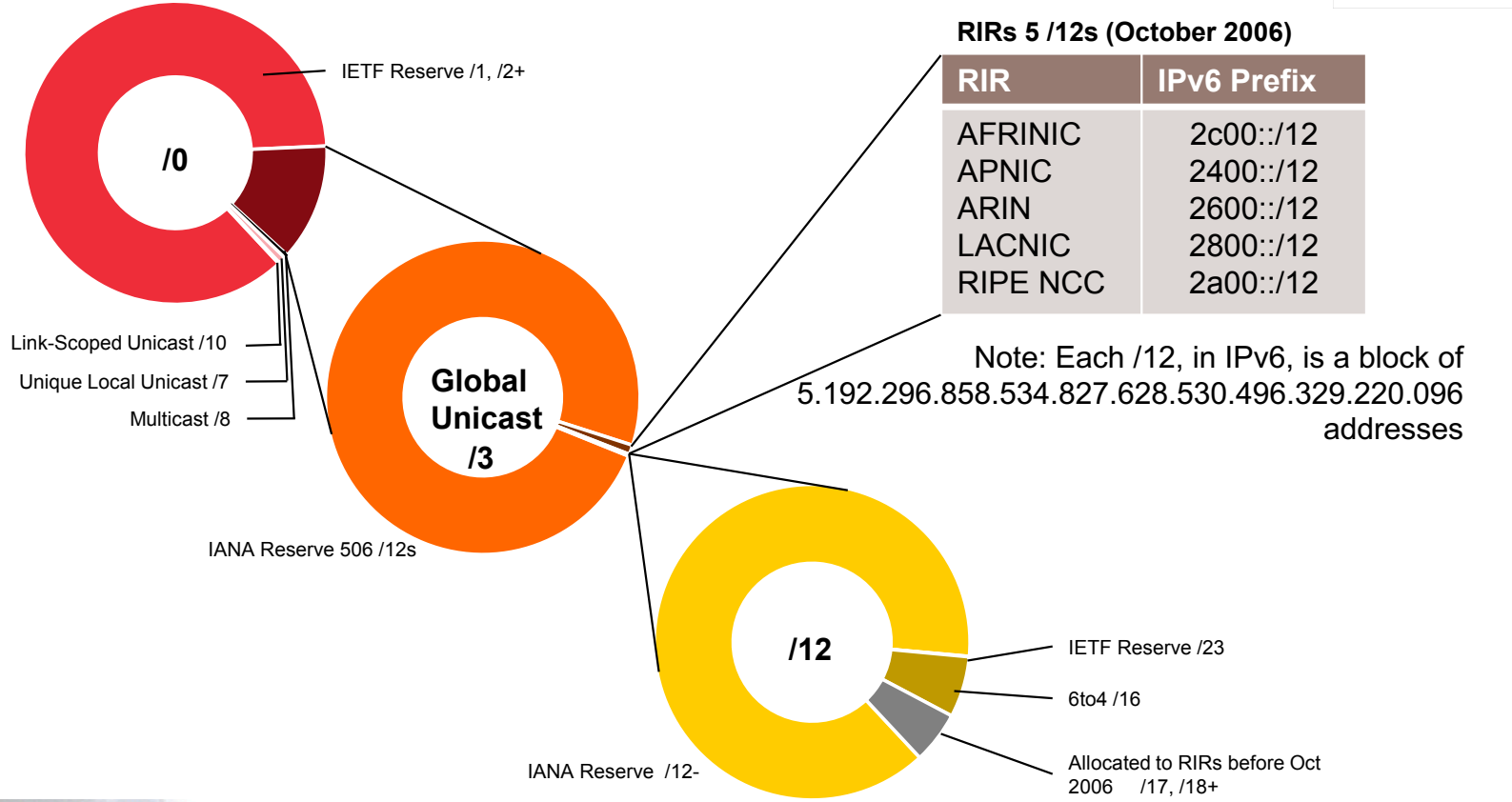
RIR IPv4 Run-Down



* http://www.potaroo.net/tools/ipv4/rir.jpg - February 2019

IPv6 Addressing Space

How much has been allocated to the RIRs?



RIRs 5 /12s (October 2006)

RIR	IPv6 Prefix
AFRINIC	2c00::/12
APNIC	2400::/12
ARIN	2600::/12
LACNIC	2800::/12
RIPE NCC	2a00::/12

Note: Each /12, in IPv6, is a block of 5.192.296.858.534.827.628.530.496.329.220.096 addresses

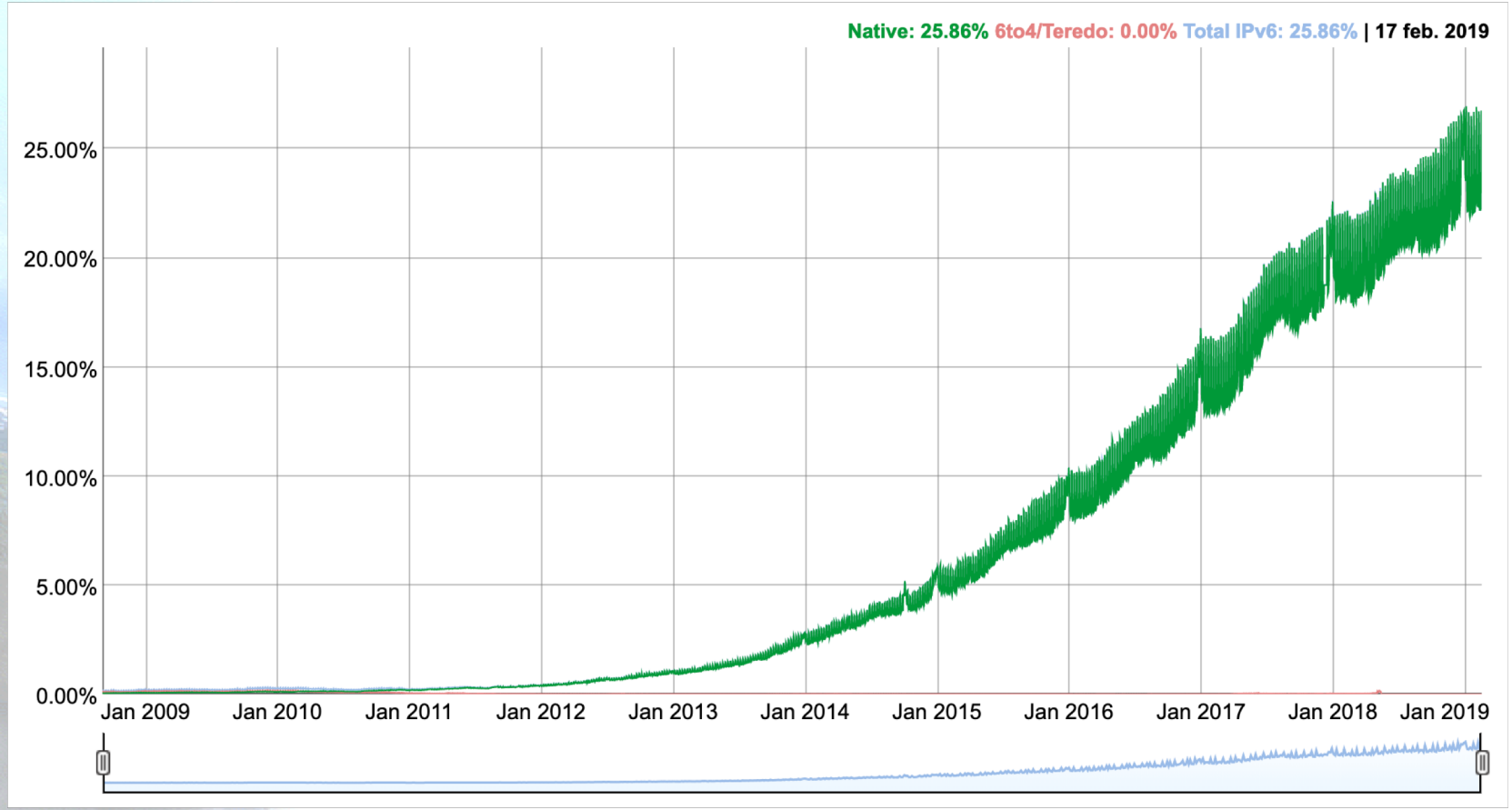
* NRO, December 2018

IPv6 is Mandatory

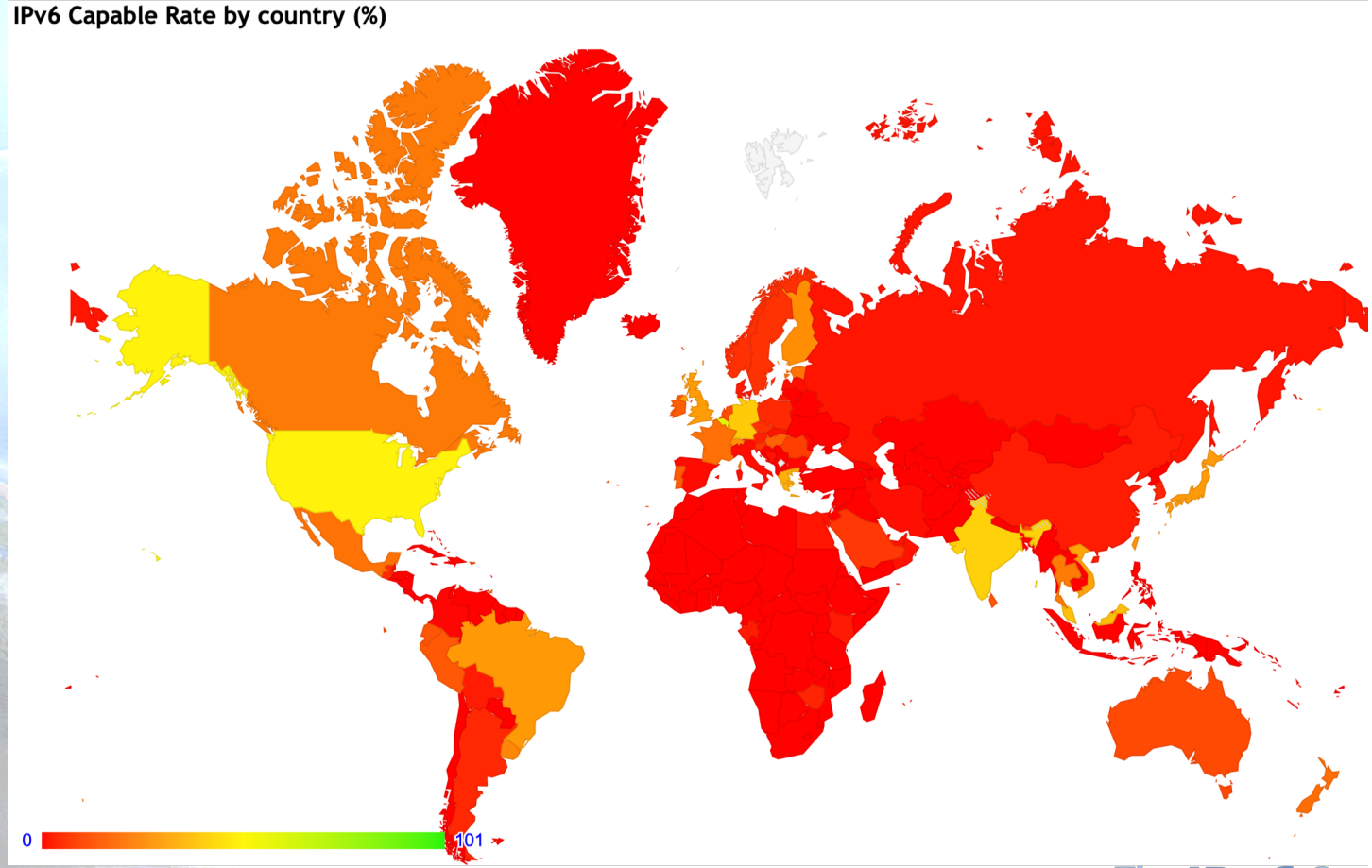
- Since 2012, IETF requires IPv6 support:
  - New implementations
  - Updates
  - Same or higher quality and functionality as IPv4
  - Must support dual-stack, but also work in IPv6-only

- On-going work to make IPv4 “historic”
  - Sleeping now, but it will happen

Global IPv6 Deployment (Google)



IPv6 World



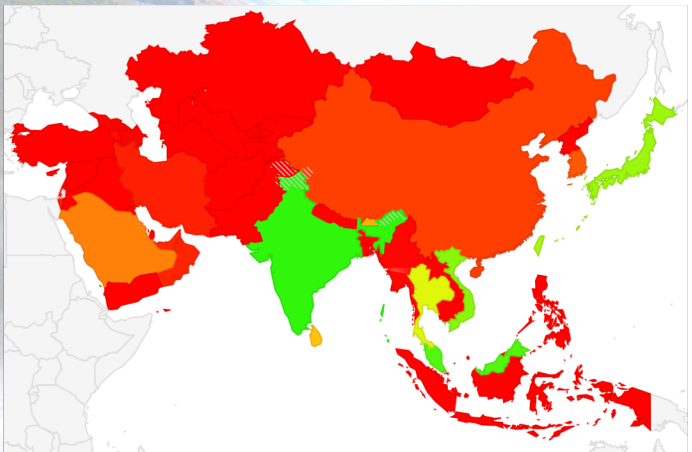
APNIC, 20th February 2019

IPv6 by Regions

Code	SubRegion	IPv6 Capable	IPv6 Preferred
XQ	Northern America, Americas	47.11%	46.43%
XT	Southern Asia, Asia	35.24%	34.86%
QO	Western Europe, Europe	32.13%	31.62%
QM	Northern Europe, Europe	25.06%	24.62%
XP	South America, Americas	19.62%	19.35%
XO	Central America, Americas	19.25%	19.04%
QP	Australia and New Zealand, Oceania	16.68%	15.19%
XU	South-Eastern Asia, Asia	15.90%	15.54%
XS	Eastern Asia, Asia	9.55%	8.50%
QN	Southern Europe, Europe	5.91%	5.83%
XW	Eastern Europe, Europe	5.68%	5.55%
XN	Caribbean, Americas	4.21%	4.12%
XH	Eastern Africa, Africa	2.92%	2.86%
XV	Western Asia, Asia	2.32%	2.26%
XJ	Northern Africa, Africa	1.75%	1.66%
XK	Southern Africa, Africa	0.52%	0.50%
QQ	Melanesia, Oceania	0.16%	0.03%
XI	Middle Africa, Africa	0.08%	0.08%
XL	Western Africa, Africa	0.05%	0.04%
XR	Central Asia, Asia	0.01%	0.01%
QR	Micronesia, Oceania	0.00%	0.00%
QS	Polynesia, Oceania	0.00%	0.00%

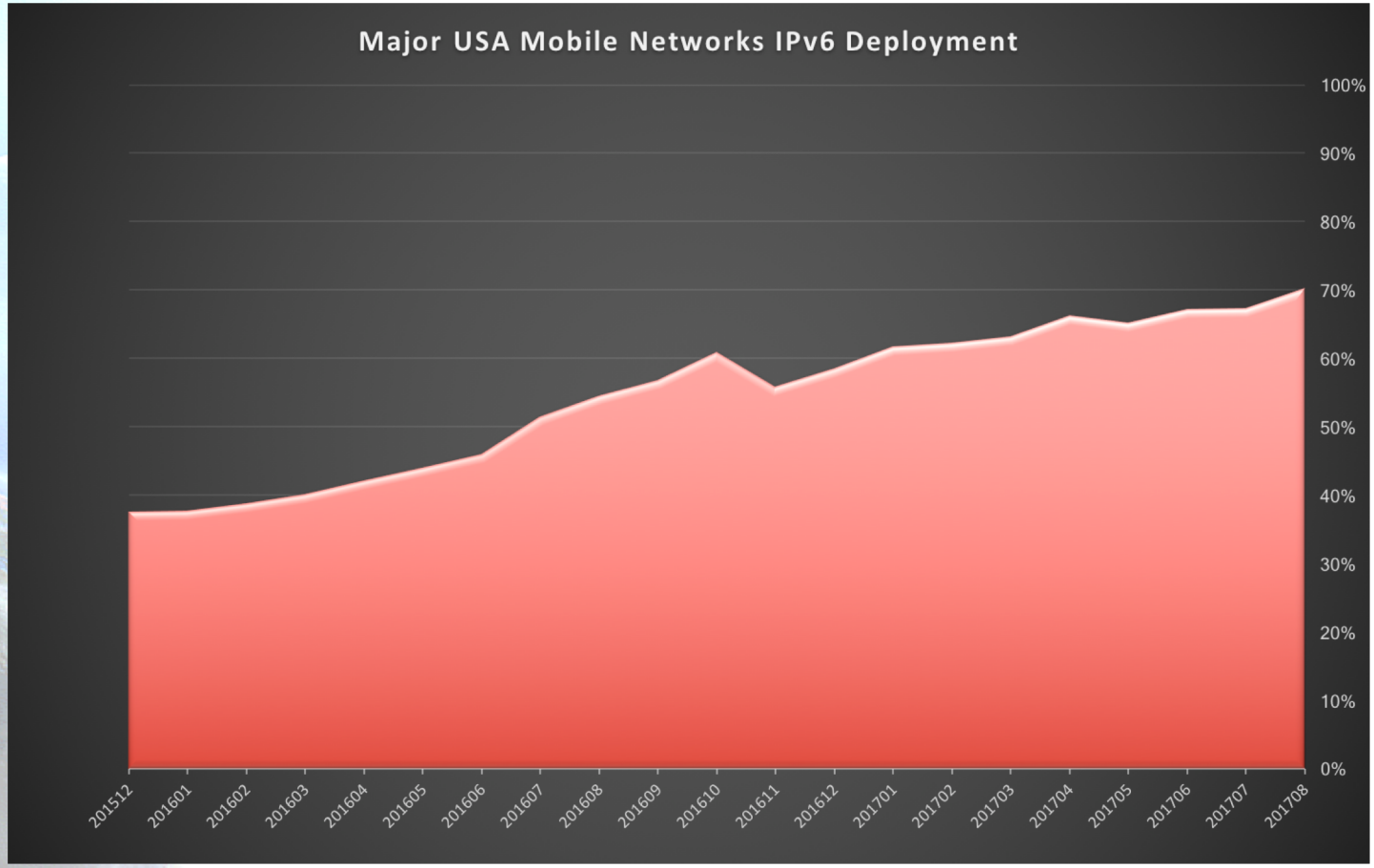
Asia

CC	Country	IPv6 Capable	IPv6 Preferred
IN	India, Southern Asia, Asia	43.04%	42.57%
MY	Malaysia, South-Eastern Asia, Asia	39.49%	39.07%
VN	Vietnam, South-Eastern Asia, Asia	33.83%	32.75%
JP	Japan, Eastern Asia, Asia	31.85%	30.70%
TW	Taiwan, Eastern Asia, Asia	30.47%	29.95%
TH	Thailand, South-Eastern Asia, Asia	25.15%	24.86%
LK	Sri Lanka, Southern Asia, Asia	17.37%	17.02%
BT	Bhutan, Southern Asia, Asia	15.77%	15.69%
SA	Saudi Arabia, Western Asia, Asia	11.55%	11.25%
SG	Singapore, South-Eastern Asia, Asia	10.82%	10.16%
MO	Macao Special Administrative Region of China, Eastern Asia, Asia	9.47%	9.38%
KR	Republic of Korea, Eastern Asia, Asia	7.93%	7.88%
CN	China, Eastern Asia, Asia	5.67%	4.57%
AE	United Arab Emirates, Western Asia, Asia	3.49%	3.45%
OM	Oman, Western Asia, Asia	3.21%	3.16%
IR	Iran (Islamic Republic of), Southern Asia, Asia	2.79%	2.73%
IL	Israel, Western Asia, Asia	2.48%	2.45%
AM	Armenia, Western Asia, Asia	1.08%	1.07%



APNIC, 20th February 2019

IPv6 Cellular/US



*ISOC/World IPv6 Launch data

Spanish Government Plan

BOLETÍN OFICIAL DEL ESTADO

Núm. 147 Martes 21 de junio de 2011 Sec. I. Pág. 65329

I. DISPOSICIONES GENERALES

MINISTERIO DE LA PRESIDENCIA

10786 *Orden PRE/1716/2011, de 9 de junio, por la que se publica el Acuerdo de Consejo de Ministros de 29 de abril de 2011, por el que se aprueba el Plan de fomento para la incorporación del protocolo IPv6 en España.*

El Consejo de Ministros, en su reunión de 29 de abril de 2011 y a propuesta del Vicepresidente Tercero y Ministro de Política Territorial y Administración Pública y del Ministro de Industria, Turismo y Comercio ha adoptado un Acuerdo por el que se aprueba el Plan de fomento para la incorporación del protocolo IPv6 en España.

Para general conocimiento se dispone su publicación como anexo a la presente orden.

Madrid, 9 de junio de 2011.–El Ministro de la Presidencia, Ramón Jáuregui Atondo.

ANEXO

Acuerdo de Consejo de Ministros por el que se aprueba el Plan de fomento para la incorporación del protocolo IPv6 en España

Las tecnologías de la información y de las comunicaciones, en especial Internet, se extienden cada vez con mayor amplitud en nuestra sociedad, produciendo la transformación de los procesos económicos y actividades sociales y configurando lo que se ha denominado sociedad de la información o del conocimiento. Son, asimismo, piedra angular de la modernización de nuestras Administraciones Públicas y del modelo de relación entre estas y los ciudadanos.

Las direcciones IP constituyen el sistema de identificación que permite que diferentes

Colombia Government Plan

Ministerio de Tecnologías de la Información y las Comunicaciones
República de Colombia

Prosperidad para todos

Código TRD:

CIRCULAR NÚMERO ____ 000002

PARA : **RAMA EJECUTIVA SECTOR CENTRAL, ENTIDADES TERRITORIALES, ENTIDADES DESCENTRALIZADAS, ENTIDADES DE LA ADMINISTRACIÓN PÚBLICA Y DEMÁS RAMAS Y ORGANISMOS DEL ESTADO, SECTOR DE TIC Y LA SOCIEDAD EN GENERAL**

DE : **MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES**

FECHA: 06 JUL 2011

ASUNTO : **PROMOCIÓN DE LA ADOPCIÓN DEL IPv6 EN COLOMBIA.**

Con el fin de lograr la prestación de servicios eficientes[1] a los ciudadanos, las entidades públicas deberán adoptar todas las medidas necesarias para garantizar el máximo aprovechamiento de las Tecnologías de la Información y las Comunicaciones en el desarrollo de sus funciones y el Gobierno Nacional debe fijar los mecanismos y condiciones, para garantizar el desarrollo de los principios orientadores[2] de la Ley 1341 de 2009.

En este sentido, es función del Ministerio de Tecnologías de la Información y las Comunicaciones, diseñar[3], adoptar y promover las políticas, planes, programas y proyectos del sector de las Tecnologías de la Información y las Comunicaciones; así como, preparar y expedir los actos administrativos[4] para el cumplimiento de los fines de intervención del Estado en materia de TIC.

Por otra parte, el Estado debe garantizar la libre adopción de tecnologías teniendo en cuenta recomendaciones, conceptos y normativas de los organismos internacionales competentes e idóneos en la materia que permitan fomentar la eficiente prestación de servicios, contenidos y

[1] En consonancia con la estrategia de Masificación del Gobierno en Línea.
[2] Ley 1341 de 2009 Art. 2.
[3] Ley 1341 de 2009 Art.18 numeral 1 y 2.
[4] Ley 1341 de 2009 Art.18 numeral 19

Edificio Murillo Toro, Carrera 8a, entre calles 12 y 13
Código Postal: 117711 . Bogotá, Colombia
T.: +57 (1) 3443460 Fax: 57 (1) 344 2248
www.mintic.gov.co
www.vivedigital.gov.co

vive digital Colombia

provea y/o fabrique sobre IPv6, con total compatibilidad y soporte IPv4, demostrable mediante los RFCs concretos del IETF y demás normas que determinan esta compatibilidad.

De otro lado, se hace un llamado a las instituciones de educación formal y no formal, públicas y privadas, para que promuevan y divulguen la adopción del IPv6 en Colombia, a través de la apropiación e inclusión de dicha temática, en sus cursos regulares y escenarios de formación en TIC.

Por último, es importante generar espacios de concertación entre la academia, los usuarios, el sector de TIC, los entes regulatorios de índole nacional e internacional, la sociedad y el gobierno; para impulsar la masificación del uso del Internet y lograr en el menor tiempo posible la adopción del IPv6 en Colombia.

Atentamente,

DIEGO MOLANO VEGA
MINISTRO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES

Elaboró: Dr. Ing. Rafael Ignacio Sandoval Morales
Asesor de la Dirección de Comunicaciones – SITIC.
Revisó: Ing. Miguel Felipe Anzola
Director de Comunicaciones
Ing. Mirvan Campo Ayala
Subdirectora Para la Industria de TIC
Dr. Alejandro Delgado R.
Asesor Despacho de la Viceministra de TIC.
Dr. Javier Ortiz Muñoz
Asesor Despacho del Ministro
Asesoró Jordi Palet
Gerente Consultintel

Edificio Murillo Toro, Carrera 8a, entre calles 12 y 13
Código Postal: 117711 . Bogotá, Colombia
T.: +57 (1) 3443460 Fax: 57 (1) 344 2248
www.mintic.gov.co
www.vivedigital.gov.co

vive digital Colombia

AAR-TIC-FM-011. V2.

Ecuador Government Plan

mintel
Ministerio de Telecomunicaciones y de la Sociedad de la Información

ACUERDO N° 007-2012

ING. HÉCTOR VICENTE MOYA UNDA

MINISTRO DE TELECOMUNICACIONES Y DE LA SOCIEDAD DE LA INFORMACIÓN (ENCARGADO)

CONSIDERANDO:

Que, el numeral 1 del Art. 154 de la Constitución de la República del Ecuador, dispone que a las ministras y ministros del Estado, además de las atribuciones establecidas en la ley, les corresponde ejercer la rectoría de las políticas públicas del área a su cargo y expedir los acuerdos y resoluciones administrativas que requiera su gestión;

Que, el Art. 313 de la Constitución de la República del Ecuador dispone: "El Estado se reserva el derecho de administrar, regular, controlar y gestionar los sectores estratégicos, de conformidad con los principios de sostenibilidad ambiental, precaución, prevención y eficiencia. Los sectores estratégicos, de decisión y control exclusivo del Estado, son aquellos que por su trascendencia y magnitud tienen decisiva influencia económica, social, política o ambiental, y deberán orientarse al pleno desarrollo de los derechos y al interés social. Se consideran sectores estratégicos la energía en todas sus formas, las telecomunicaciones, los recursos naturales no renovables, el transporte y la refinación de hidrocarburos, la biodiversidad y el patrimonio genético, el espectro radioeléctrico, el agua, y los demás que determine la ley" ;

Que, mediante Decreto Ejecutivo N° 8, de 13 de agosto de 2009, publicado en el Registro Oficial N° 10, de 24 de agosto de 2009, el Presidente Constitucional de la República resolvió crear el Ministerio de Telecomunicaciones y de la Sociedad de la Información, como órgano rector del desarrollo de las tecnologías de la información y comunicación, que incluye las telecomunicaciones y el espectro radioeléctrico;

Que, el numeral 1 del artículo 2 del Decreto Ejecutivo antes referido, faculta al Ministerio de Telecomunicaciones y de la Sociedad de la Información a ejercer la representación del Estado, en materia de Sociedad de la Información y Tecnologías de la Información y Comunicación;

Que, con Decreto Ejecutivo N° 311, de 5 de abril de 2010, publicado en el Registro Oficial Suplemento N° 171, de 14 de abril de 2010, el Presidente Constitucional de la República designó al Ing. Jaime Guerrero Ruiz, Ministro de Telecomunicaciones y de la Sociedad de la Información;

Que, mediante Acuerdo Ministerial N° 035, de 6 de abril de 2010, el Ing. Jaime Guerrero Ruiz, asumió las funciones de Ministro de Telecomunicaciones y de la Sociedad de la Información;

Que, con fecha 8 de Octubre de 2009 se realizó la reunión constitutiva de la fuerza de trabajo (Task Force) IPv6– Ecuador, en la cual participaron delegados del Gobierno Ecuatoriano, representantes del sector de Telecomunicaciones, Entidades Educativas de nivel superior, miembros de la sociedad en general y expertos internacionales;

mintel
Ministerio de Telecomunicaciones y de la Sociedad de la Información

incorporación y correcto funcionamiento del protocolo IPv6 en el sistema de nombres de dominio bajo el código de país .ec, la misma calidad que los servicios ofrecidos con IPv4, y sin incremento de costes para los usuarios.

Artículo 3.- Requerir a la Secretaría Nacional de Telecomunicaciones SENATEL, que ejecute las acciones y procedimientos administrativos y normativos necesarios con el fin de que los Proveedores de Servicio de Internet ISPs y portadores nacionales, admitan en sus redes, plataformas y sistemas el curso normal de tráfico de IPv6 en coexistencia con IPv4.

Artículo 4.- Requerir a la Secretaría Nacional de Telecomunicaciones SENATEL, que ejecute las acciones necesarias con el fin de que los Proveedores de Servicios de Internet (ISPs), establezcan sus planes de direccionamiento, y en función de los mismos, inicien los trámites para la solicitud de recursos de direccionamiento (direcciones IP) IPv6.

DISPOSICIÓN TRANSITORIA

ÚNICA.- En el plazo de 90 días contados a partir de la publicación del presente acuerdo, el Ministerio de Telecomunicaciones y de la Sociedad de la Información publicará un plan de compras de equipamiento ICT con soporte IP para las entidades del sector público, el cual servirá como marco de referencia en los procesos de adquisiciones de infraestructura para garantizar el adecuado soporte de IPv6.

Este Acuerdo Ministerial entrará en vigencia a partir de la presente fecha.

Dado en Quito, Distrito Metropolitano, a dieciocho de enero de dos mil doce.

Ing. Héctor Vicente Moya Unda
MINISTRO DE TELECOMUNICACIONES Y DE LA SOCIEDAD DE LA INFORMACIÓN (ENCARGADO)

JT/OC/bc

Perú Government Plan

PRESIDENCIA DEL CONSEJO DE MINISTROS

Decreto Supremo que aprueba la formulación de un Plan de Transición al Protocolo IPV6 en las entidades de la Administración Pública

DECRETO SUPREMO
Nº 081-2017-PCM

EL PRESIDENTE DE LA REPÚBLICA

CONSIDERANDO:

Que, la Ley Nº 27658 - Ley Marco de Modernización de la Gestión del Estado, declara al Estado Peruano en proceso de modernización en sus diferentes instancias, dependencias, entidades, organizaciones y procedimientos, con la finalidad de mejorar la gestión pública y contribuir en el fortalecimiento de un Estado moderno, descentralizado y con mayor participación del ciudadano; por lo que deviene en necesario mejorar la gestión pública a través del uso de nuevas tecnologías que permitan brindar mejores servicios a los ciudadanos;

Que, el Decreto Legislativo Nº 604, Ley de Organización y Funciones del Instituto Nacional de Estadística e Informática, crea el Sistema Nacional de Informática, el cual tiene por finalidad asegurar que sus actividades se desarrollen en forma integrada, coordinada, racionalizada y bajo una normatividad técnica común, contando con autonomía técnica y de gestión; teniendo como competencia la instrumentalización jurídica y de mecanismos técnicos para el ordenamiento de los recursos de cómputo y de la actividad informática del Estado, entre otros;

Que, de acuerdo a lo establecido en el artículo 47 del Reglamento de Organización y Funciones de la Presidencia del Consejo de Ministros, aprobado mediante Decreto Supremo Nº 022-2017-PCM, la Secretaría de Gobierno Digital es el órgano de línea, con autoridad técnico normativa a nivel nacional, responsable de formular y promover políticas nacionales y sectoriales, planes nacionales, normas, lineamientos y estrategias en materia de Informática y Gobierno Electrónico; asimismo, es el órgano rector del Sistema Nacional de Informática y brinda asistencia técnica en la implementación de los procesos de innovación tecnológica para la modernización del Estado;

Que, la Política Nacional de Gobierno Electrónico, aprobada mediante Decreto Supremo Nº 081-2013-PCM, prevé determinados lineamientos estratégicos para el Gobierno Electrónico en el Perú, entre otros, el relacionado con la Infraestructura, el mismo que busca contar con una red informática que integre a todas las dependencias y a sus funcionarios públicos, incluyendo hardware, software, sistemas, bases de datos, entre otros;

Que, el Plan de Desarrollo de la Sociedad de la Información en el Perú – La Agenda Digital Peruana 2.0, aprobada mediante Decreto Supremo Nº 066-2011-PCM, establece en su Objetivo 1, "Asegurar el acceso inclusivo y participativo de la población de áreas urbanas y rurales a la Sociedad de la Información y del Conocimiento", disponiendo a su vez, en su Estrategia 7, "Proponer e implementar servicios públicos gubernamentales que utilicen soluciones de comunicación innovadoras la comunicación entre dispositivos, acceso a servicios a través de Internet u otros, y conforme a lo manifestado por el Registro de Direcciones de Internet para América Latina y el Caribe- (LACNIC por sus siglas en inglés) sobre el agotamiento de la cantidad de direcciones de IPv4, emerge el uso de las direcciones basadas en el protocolo IPv6, como mecanismo para asegurar la provisión y acceso a servicios digitales basados en IPv6;

Que, para que las computadoras, servidores de datos, laptops, tabletas, teléfonos móviles multimedia (smartphones) y otros dispositivos se conecten a través del Internet, requieren de una dirección IP – Internet Protocol, provista por un Proveedor de Servicio de Internet;

Que, mediante la Resolución Nº 180 correspondiente a la Conferencia de Plenipotenciarios de la Unión Internacional de Telecomunicaciones (UIT), detallada en el documento "Actas Finales de la Conferencia de Plenipotenciarios, Guadalajara, 2010", se invita a los Estados Miembros a elaborar políticas nacionales para fomentar la actualización tecnológica de los sistemas, a fin de asegurar que los servicios públicos ofrecidos a través del Protocolo de Internet (IP), la infraestructura de comunicaciones y las aplicaciones correspondientes, sean compatibles con IPv6;

Que, en la mencionada Resolución, también se invita a los Estados Miembros, a garantizar que, en las acciones que lleven a cabo en relación con los equipos de comunicaciones e informáticos, se tomen las medidas necesarias para que los equipos cuenten con capacidad de IPv6, tomando en consideración un periodo de transición necesario para pasar del IPv4 al IPv6;

Que, el Registro de Direcciones de Internet para América Latina y el Caribe (LACNIC por sus siglas en inglés) es la organización responsable de la asignación y administración de los recursos de numeración de Internet conocidos como IPv4 e IPv6, entre otros, en la región;

Que, LACNIC señala que el agotamiento de las direcciones IPv4 en América Latina y el Caribe se encuentra en su tercera y última fase, debiendo los gobiernos priorizar el despliegue del protocolo IPv6, quienes deben asegurar que las acciones que se lleven a cabo garanticen que los nuevos recursos TIC cuenten con capacidad IPv6, tomando en consideración un periodo de transición necesario para pasar del IPv4 al IPv6, ello conforme con lo dispuesto en la Resolución Nº 180 correspondiente a la Conferencia de Plenipotenciarios de la Unión Internacional de Telecomunicaciones;

Que, se hace necesario que el Perú propicie un entorno que garantice la adopción del protocolo IPv6 por parte de las entidades de la Administración Pública ante el inminente agotamiento de las direcciones IPv4, de tal manera que se asegure la comunicación y accesibilidad a dispositivos o servicios que utilizan el sistema de direccionamiento IPv6;

De conformidad con lo establecido en la Ley Nº 27658 - Ley Marco de Modernización de la Gestión del Estado; la Ley Nº 29158 - Ley Orgánica del Poder Ejecutivo; el Decreto Legislativo Nº 604; y, el Decreto Supremo Nº 022-2017-PCM, que aprueba el Reglamento de Organización y Funciones de la Presidencia del Consejo de Ministros;

DECRETA:

Artículo 1º.- Objeto
Disponer la formulación de un Plan de Transición al Protocolo IPV6, a implementarse de manera progresiva en toda la infraestructura tecnológica, software, hardware, servicios, entre otros, en las entidades de la Administración Pública.

Artículo 2º.- Alcance
El presente Decreto Supremo es de alcance obligatorio a todas las entidades de la Administración Pública comprendidas en el Artículo I del Título Preliminar del Texto

Who is first, why?

- IPv6 deployment is not related to rich or poor
- Neither to ISPs with more users or growing faster
- Or to specific countries
- Etc …

- It is related to when in a country ONE ISP deploys it, the others follow …

- Related talk:
  - https://conference.apnic.net/46/assets/files/APNC402/An-IPv6-Update.pdf

IPv6 and Security

- IPv6 is NOT more secure than IPv4
- It depends on how you deploy it
- Non-experts will replicate IPv4 knowledge, which is a terrible mistake
- You need to unlearn IPv4 to correctly deploy IPv6

IPv6 and Government/Enterprise

- Do not follow IPv4 bad practices …
- Start with good training
- You need your own BGP and DNS
  - addresses & ASN from the RIR
- Governments may need to consider a nation wide network to connect all the public administration units
  - Huge savings!
- There is no NAT
  - security and address planning, IPAM
- Long-term strategy is not dual-stack (wrong way), it must be “IPv6-only”
  - Make sure to check apps

*12 steps for IPv6 deployment in governments and enterprises

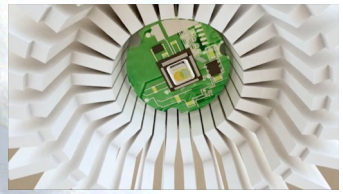
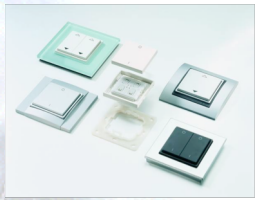
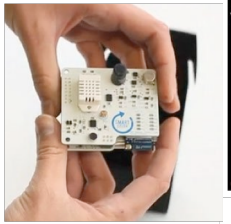
IPv6 for ISPs

- Too late for dual-stack
- Don’t buy Carrier Grade NAT (CGN)
  - You will need to invest in more IPv4 addresses
- IPv6-only is a MUST *NOW*
  - Both fix and cellular networks
- You probably want to have CEs supporting IPv6 with IPv4-as-a-Service:
  - draft-ietf-v6ops-transition-ipv4aas-15 (soon RFC)
  - draft-palet-v6ops-nat64-deployment

*12 steps to enable IPv6 in an ISP network

Secure IoT and SmartCities

- In all the cases, deploy IoT
  - only with IPv6
- Security is a must
  - You don't want your network to be used for DDoS




Thanks !!

Contact:

@JordiPalet (The IPv6 Company):
jordi.palet@theipv6company.com

Value of ROA/RPKI and preparing for its deployment

GFCE Triple-I Daejeon Korea

16 February 2019

Taiji Kimura, JPNIC

Contents

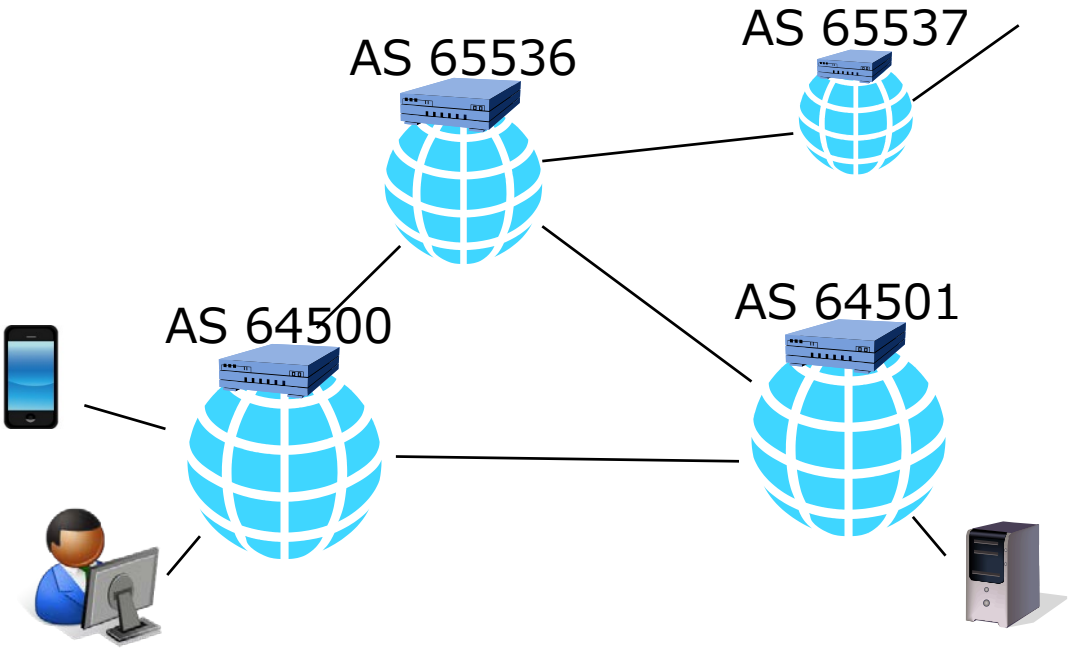
- What is RPKI and ROA
- Why ROA/RPKI is being deployed
- Origin validation - What will happen with it
- How to prepare for deployment
- What we can do

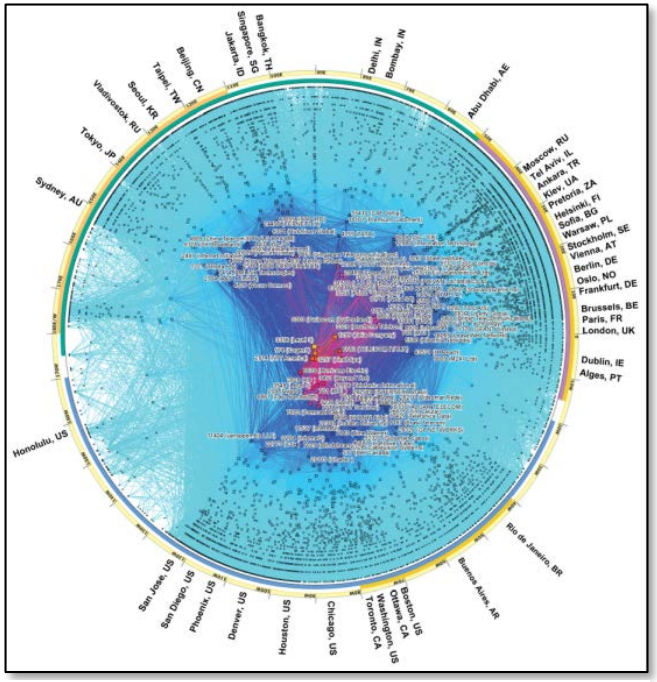
What is RPKI and ROA

BGP - Autonomous System's network

Allocated ASN 102,398

The 32-bit AS Number Report
http://www.potaroo.net/tools/asn32/





CAIDA's IPv6 AS Core AS-Level Internet Graph
http://www.caida.org/research/topology/as_core_network/

To find mis-originating routes, BGP operators need correct data

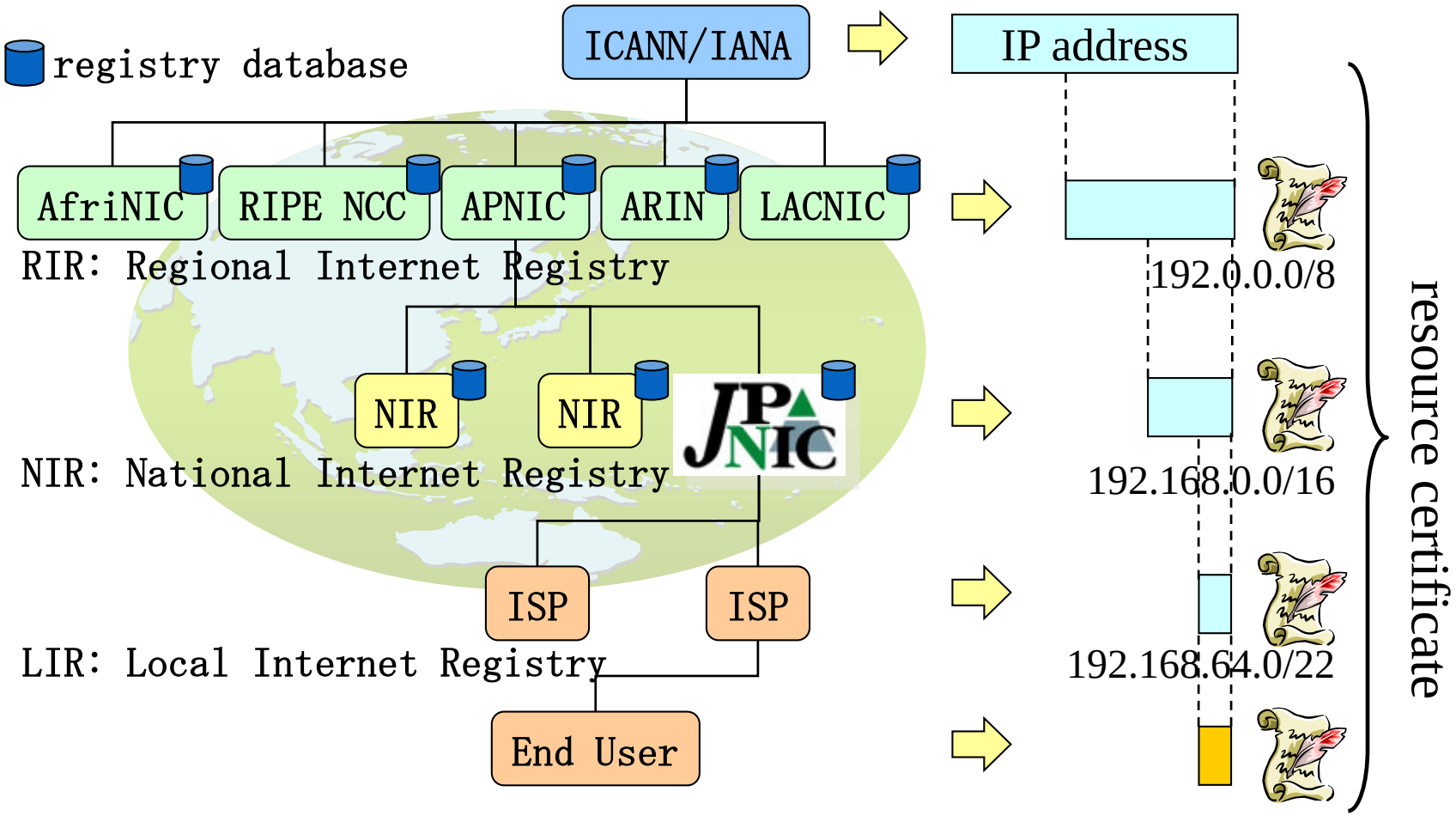
Recent incident

- MyEtherWallet.com
  - What observed
    - AWS Route 53's prefix originally /23 was announced as /24
    - A DNS server in the prefix made forged DNS response for MyEtherWallet.com
    - The web server has self-signed certificate (EV SSL certificate is used on the original server)
  - What happened
    - $150,000 in Ethereum was sent abnormally

Mis-originated BGP prefix was used to redirect to a phishing site.

- MyEtherWallet、DNSサーバーにハッキング、15万ドル分のETH盗難か
  https://jp.cointelegraph.com/news/myetherwallet-warns-that-a-couple-of-its-dns-servers-have-been-hacked
- AWS DNS network hijack turns MyEtherWallet into ThievesEtherWallet - The Register, 2018/4/24
  https://www.theregister.co.uk/2018/04/24/myetherwallet_dns_hijack/

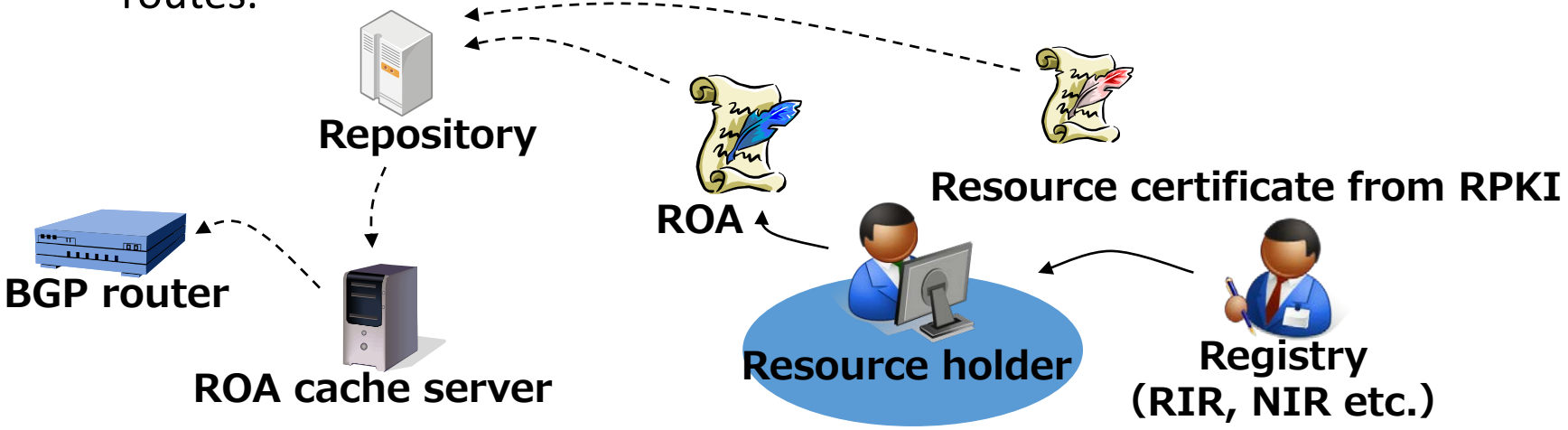
Resource Public-Key Infrastructure



Lower certificate have small range of IP address.

RPKI and ROA

- Resource Public-Key Infrastructure
  - A PKI for certify number resource allocations
- Route Origination Authorization
  - Signed object expressing an AS is authorized by resource holder to announce specific prefixes.
  - ROA can be used to compare BGP route to find mis-originated routes.



Why ROA/RPKI is being deployed

Why ROA/RPKI is getting deployed

- Global BGP routes can be unsecure without tools
- DNS servers, Web sites and other IP nodes on Internet could be controlled their connectivity by mis-originated BGP routes
- Route Origination Authorization(ROA) - showing correct AS number specified by IP holders. It could be used to find if a route is correct or not.

Origin validation - What will happen with it

Origin validation - What will happen with it

- Origin validation is done by ROA validating server and BGP router (could be very far from IP holders)
- Invalid routes could be dropped or filtered
- Unreachable when BGP route is dropped because being different from ROA (but only BGP operators can know the reason)

How to prepare for its deployment

- for helping Internet reliable -

How to prepare for its deployment

- Try and know what will happen when using ROA/RPKI

- When unreachable for some specific routes, remember to investigate origin validation state

- Consider communication in different NOG

  "Be conservative in what you do, be liberal in what you accept" - Jon Postel

What we can do

What we can do

- Understand adoption rate is not only the indication of security
- Encourage communicating between engineers and between tech and non-tech persons (includes customer supporting staff)
- Spread culture of "mutual help" in BGP and Internet without making tie in the rule

Who we are?

- Online service provider
- ISP
- Government
- End user
- Engineer
- Researcher
- Developer
- Leader?

Conclusion

- Dropping invalid routes using origin validation with ROA/RPKI can make unreachable IP networks
- To ease recovery from mis-configured routes or ROAs, communication between tech and non-tech people will be important
- Encouraging "mutual help" is essential for global Internet