Internet Infrastructure Initiative

Triple I: a GFCE Capacity-building project

@INSIG, Kolkata, India, 14 November 2019

Global Risks Report 2018

"… this generation enjoys unprecedented technological, scientific, and financial resources, which we should use to chart a course towards a more sustainable, equitable and inclusive future.

At the same time, the risks are greater than ever, with an important role for disruptive technologies that may be used to affect societies in good and bad ways, and with cyberattacks amongst today's biggest threats to disrupt society."

WORLD
ECONOMIC
FORUM

Internet Infrastructure Initiative

- Aim: to help build a robust, transparent and resilient internet infrastructure.
- Rationale: A robust, open and resilient internet infrastructure is key to counter infringements and threats to the cyber domain, and:
  - diminishes the chances and impact of cyber-attacks (like DDoS) and cybercrime (hacking malware, phishing, botnets) and SPAM.
  - enables the public to maintain confidence and trust;
  - is a precondition for the use of the internet as a means to boosting innovative and economic activities.
- Offering: this Initiative seeks to deepen and broaden the know-how in locally applying, testing and monitoring compliance with widely agreed open internet standards.
  - Key elements include national internet infrastructure protection, internet exchange points, registries, open source software, email security and routing security.

Supported by global and regional stakeholders

- GFCE members
  - Governments
  - International Organisations
  - Businesses
- Regional Internet Registries
  - All regions
- Internet Society
  - Global office
  - Local chapters
- NL Ministry of Economic Affairs

Internet Society

GFCE

lacnic

AFRINIC

APNIC

RIPE NCC
RIPE NETWORK COORDINATION CENTRE

AfricaCERT
United in promoting cyber security in Africa

ICANN

LACTLD
Latin American and Caribbean ccTLDs Organization

Ministerie van Economische Zaken

Aim of the Capacity building events

- Targeted at regions that are catching up
- Bringing together regional stakeholders
- Awareness raising on Open Internet Tools
- Inspiration through Good Practice Examples (mix local/global)
- Impact through joint commitment for action

GFCE

GFCE TRIPLE - I

From State-of-Practice to State-of-the-Art, together

Joint priority setting and action planning

La Paz, 5 August 2019

LACTLD
Latin American and Caribbean
ccTLDs Organization

lacnic

ICANN

Internet Society

Internet Society
Capítulo Bolivia

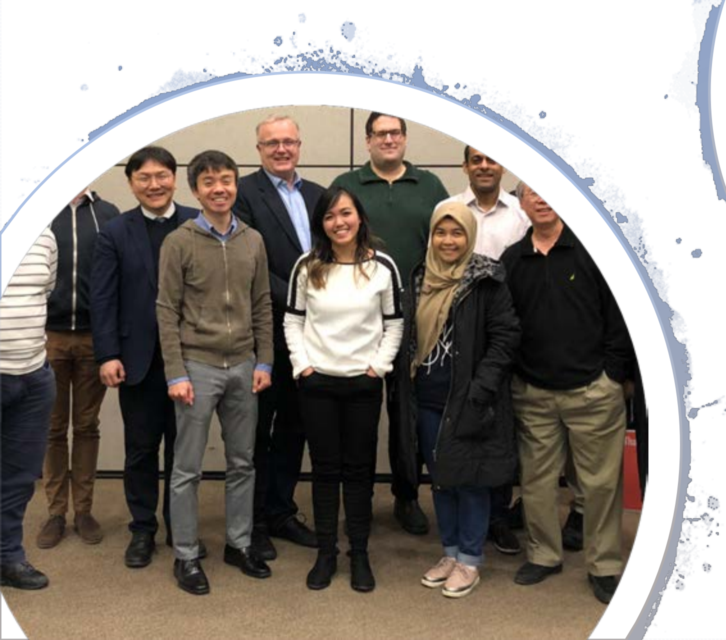
Ministry of Economic Affairs
and Climate Policy

"What to do to improve justified trust in using the Internet and email in the region"

Purpose of the Day

GFCE Triple-I agenda for today

09:00	Opening, intent
09:30	Block I: Better Use of Today’s Open Internet Standards
11:30	Block II: Inspiration from Good Practice Actions - 1
12:30	Lunch
13:30	Block II: Inspiration from Good Practice Actions - 2
16:00	Block III: Action Planning for a More Trusted Internet
17:30	Conclusions and Closing Remarks



6 events so far

- Dakar, Senegal, hosted by the African Internet Summit, supported by AfricaCERT/AfriNIC/ISOC 2019, 7 May 2018
- Almaty, Kazachstan, hosted by RIPE NCC, supported by RIPE NCC/ISOC/Kazachstan Telecom, 25 September 2018
- Delhi, India, hosted by Indian Summerschool for Internet Governance, supported by ISOC/APNIC/Indian Govt, 12 October 2018
- Daejeon, Korea, hosted by APRICOT2019,supported by APNIC/ISOC/dotASIA, 23 February 2019
- Kampala, Uganda, hosted by the African Internet Summit, supported by AfricaCERT, AfriNIC, WACREN, ISOC, ICANN, 27 June 2019
- La Paz, Bolivia, hosted by LACIGF, supported by LACTLD, LACNIC, ISOC, ICANN, CGI.br, 5 August 2019

Plans for next year

GFCE TRIPLE - I

- GFCE is planning to support additional events in 2020. For more information, email to the GFCE Secretariat at:

<contact@thegfce.com>

Triple I is a GFCE project

www.thegfce.com

GFCE

For more information about this workshop contact:

Maarten Botterman: maarten@gnksconsult.com
Arnold van Rhijn: A.C.F.vanRhijn@minez.nl

About Maarten Botterman

- More than 25 years experience with work “in the public interest”: where connected technologies touch society - internationally
- Independent analyst, strategic advisor, moderator and chairman, see for more: www.gnksconsult.com
- Currently chairing: IGF Dynamic Coalition on Internet of Things (www.iot-dynamic-coalition.org/); PICASSO Policy Expert Group (www.Picasso-project.eu), and Supervisory Board of NLnet Foundation (www.nlnet.nl.)
- ICANN Board Member (www.icann.org)
- Full CV: https://www.linkedin.com/in/botterman
- Email: maarten@gnksconsult.com

Internationalized Domain Names and Universal Acceptance Program & Confusability

GFCE

//*.*/

Dr. Ajay Data
Chair – Universal Acceptance Steering Group
Member – ccNSO Council (NomCom Appointed)

ICANN

IDN Program Objective

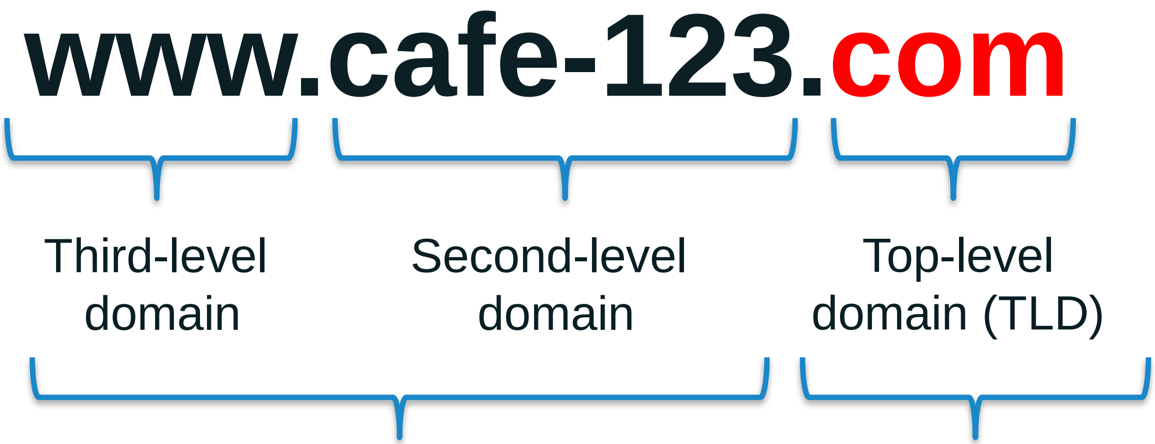
Enable deployment of domain names

in the local languages and scripts

used by the communities globally

in a secure and stable manner.

ASCII Domain Name Label



www.cafe-123.com

Third-level domain

Second-level domain

Top-level domain (TLD)

② **Forming ASCII Labels**

Use **LDH**

- **L**etters [a-z]
- **D**igits [0-9]
- **H**yphen [H]

Label length = 63

Other constraints (e.g. on hyphen)

① **Forming ASCII Labels**

Use only Letters

- **L**etters [a-z]

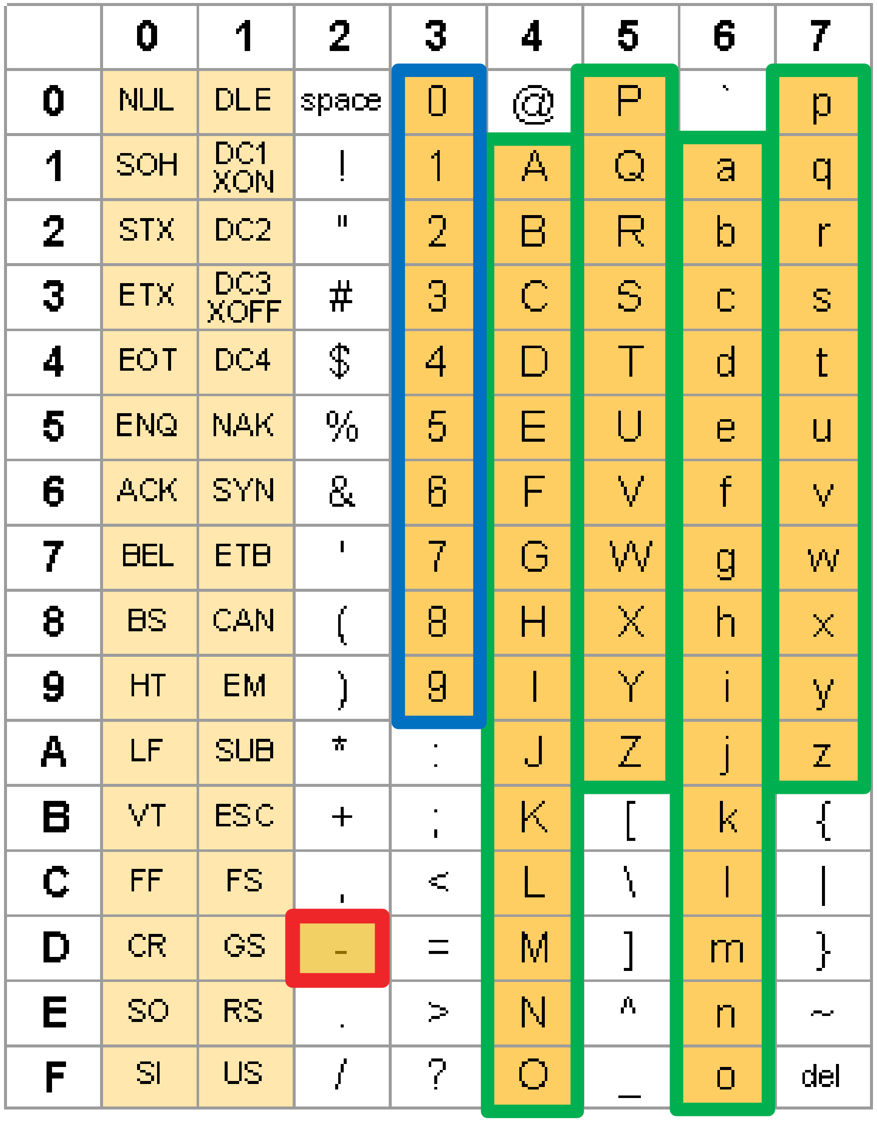
Label length = 63

Domain Name Mnemonics in ASCII

Using LDH

- Letters [a-z]
- Digits [0-9]
- Hyphen (H)

②



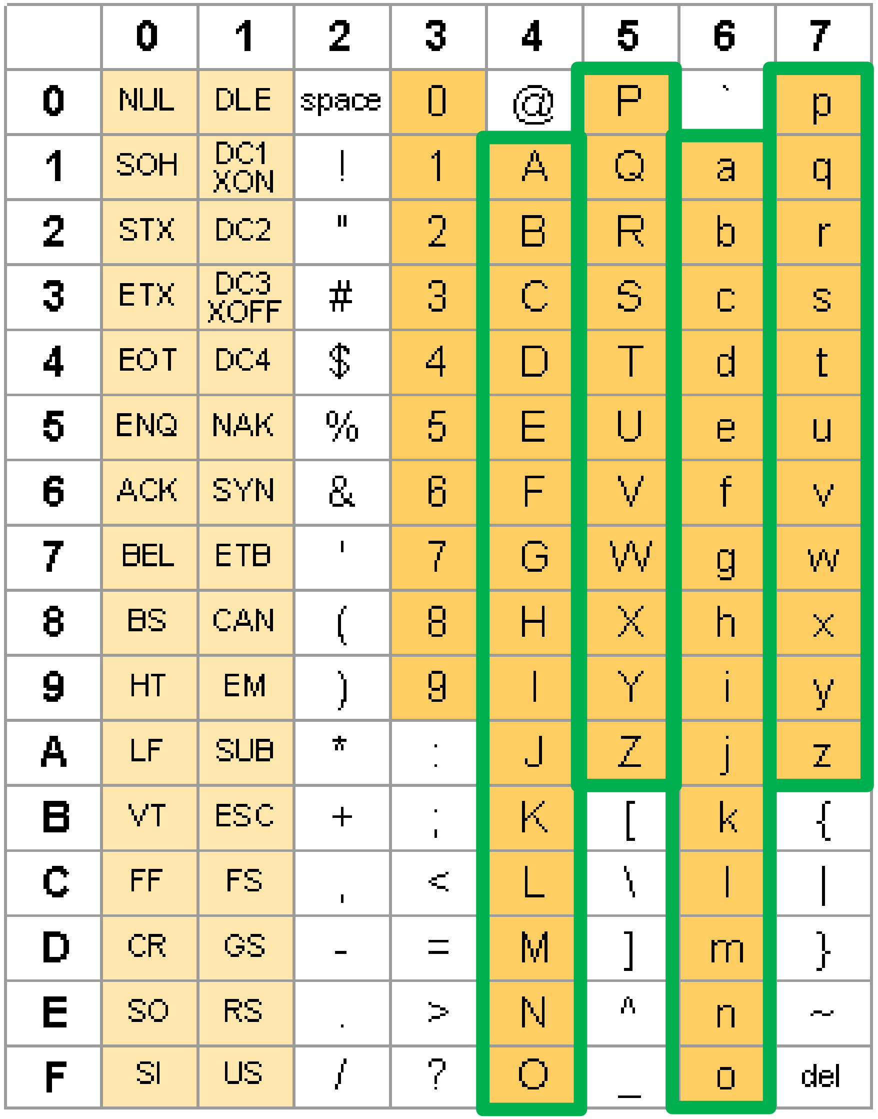
	0	1	2	3	4	5	6	7
0	NUL	DLE	space	0	@	P	`	p
1	SOH	DC1 XON	!	1	A	Q	a	q
2	STX	DC2	"	2	B	R	b	r
3	ETX	DC3 XOFF	#	3	C	S	c	s
4	EOT	DC4	$	4	D	T	d	t
5	ENQ	NAK	%	5	E	U	e	u
6	ACK	SYN	&	6	F	V	f	v
7	BEL	ETB	'	7	G	W	g	w
8	BS	CAN	(	8	H	X	h	x
9	HT	EM	)	9	I	Y	i	y
A	LF	SUB	*	:	J	Z	j	z
B	VT	ESC	+	;	K	[	k	{
C	FF	FS	,	<	L	\	l	|
D	CR	GS	-	=	M	]	m	}
E	SO	RS	.	>	N	^	n	~
F	SI	US	/	?	O	_	o	del

Top-level Domain Name Mnemonics in ASCII

Using Letters only

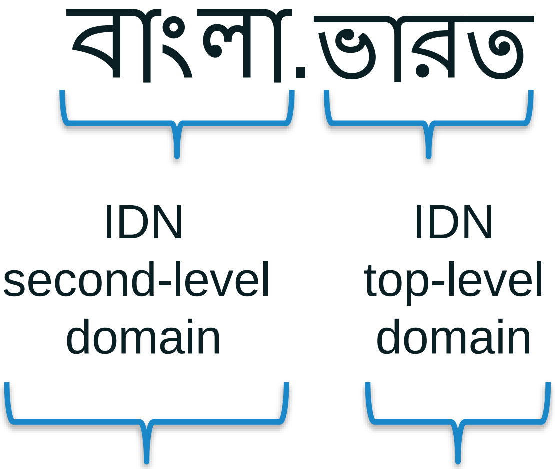
- Letters [a-z]
- ~~Digits [0-9]~~
- ~~Hyphen (H)~~

①



	0	1	2	3	4	5	6	7
0	NUL	DLE	space	0	@	P	`	p
1	SOH	DC1 XON	!	1	A	Q	a	q
2	STX	DC2	"	2	B	R	b	r
3	ETX	DC3 XOFF	#	3	C	S	c	s
4	EOT	DC4	$	4	D	T	d	t
5	ENQ	NAK	%	5	E	U	e	u
6	ACK	SYN	&	6	F	V	f	v
7	BEL	ETB	'	7	G	W	g	w
8	BS	CAN	(	8	H	X	h	x
9	HT	EM	)	9	I	Y	i	y
A	LF	SUB	*	:	J	Z	j	z
B	VT	ESC	+	;	K	[	k	{
C	FF	FS	,	<	L	\	l	|
D	CR	GS	-	=	M	]	m	}
E	SO	RS	.	>	N	^	n	~
F	SI	US	/	?	O	_	o	del

Internationalized Domain Name (IDN) Labels



বাংলা.ভারত

IDN
second-level
domain

IDN
top-level
domain

<u>Syntax of IDN Labels</u>

Valid U-Label: Unicode code points as constrained by the “LDH” scheme within IDNA 2008

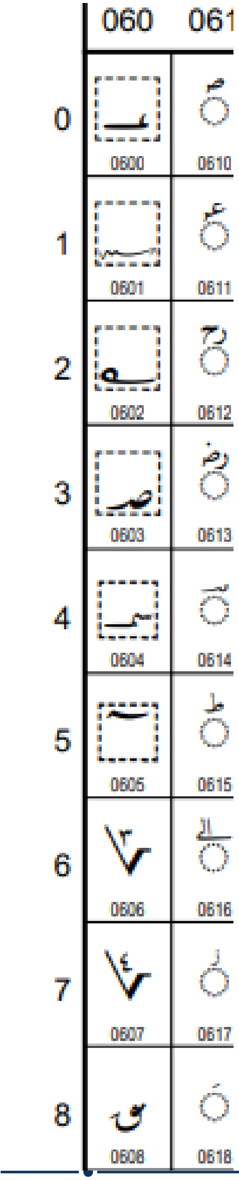
②

<u>Syntax of IDN Labels</u>

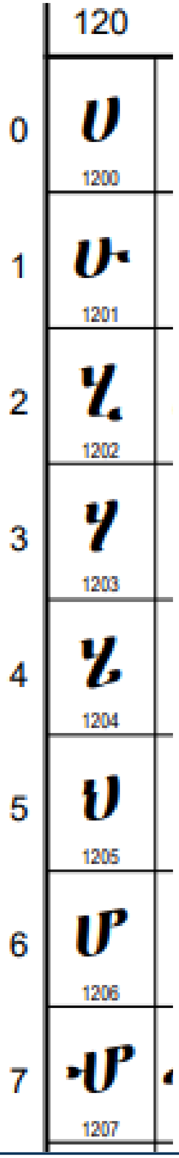
Valid U-label, further constrained by the “letter” principle for TLDs

①

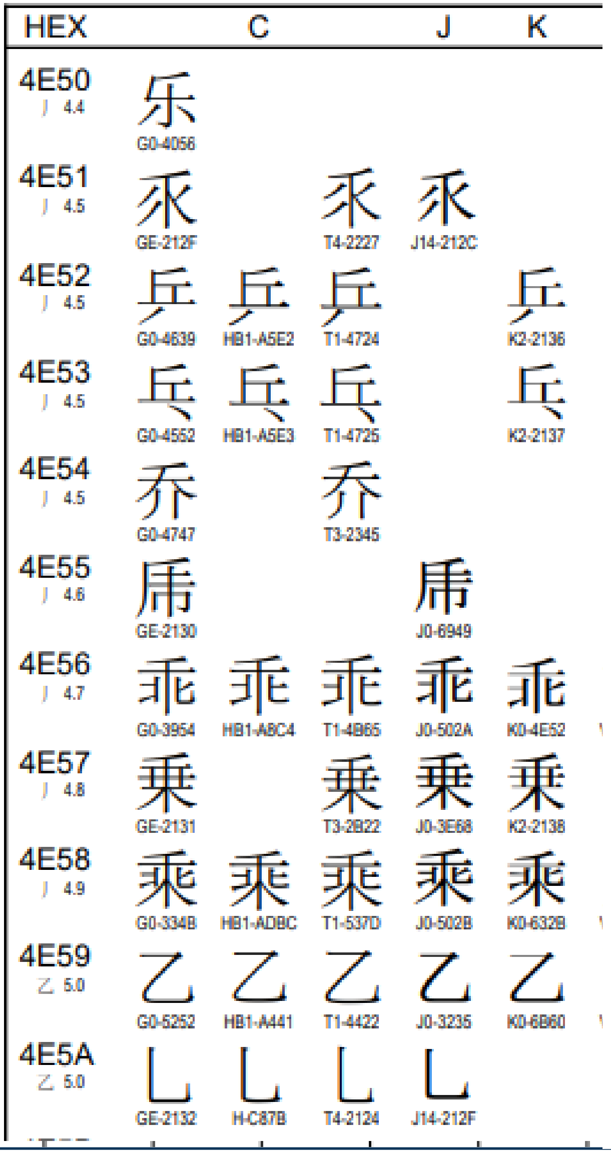
IDN Mnemonics



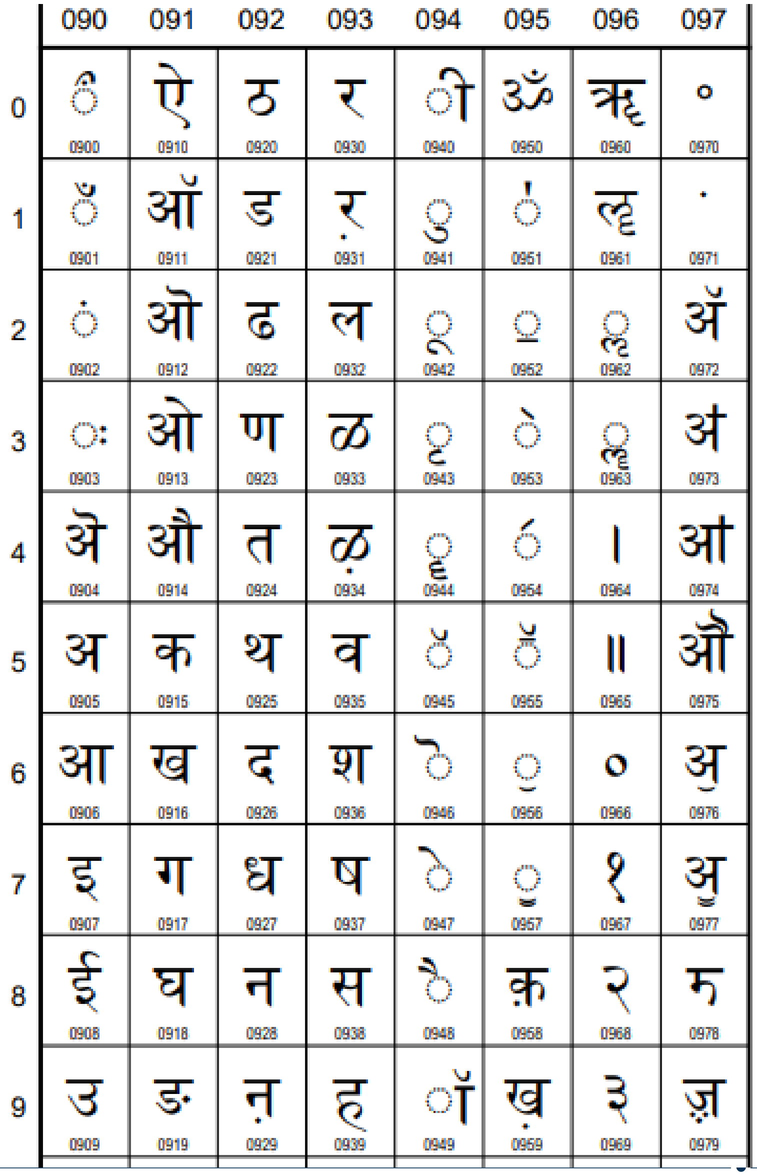
	060	061
0	؀ 0600	◌ؐ 0610
1	؁ 0601	◌ؑ 0611
2	؂ 0602	◌ؒ 0612
3	؃ 0603	◌ؓ 0613
4	؄ 0604	◌ؔ 0614
5	؅ 0605	◌ؕ 0615
6	؆ 0606	◌ؖ 0616
7	؇ 0607	◌ؗ 0617
8	؈ 0608	◌ؘ 0618



	120
0	ሀ 1200
1	ሁ 1201
2	ሂ 1202
3	ሃ 1203
4	ሄ 1204
5	ህ 1205
6	ሆ 1206
7	ሇ 1207

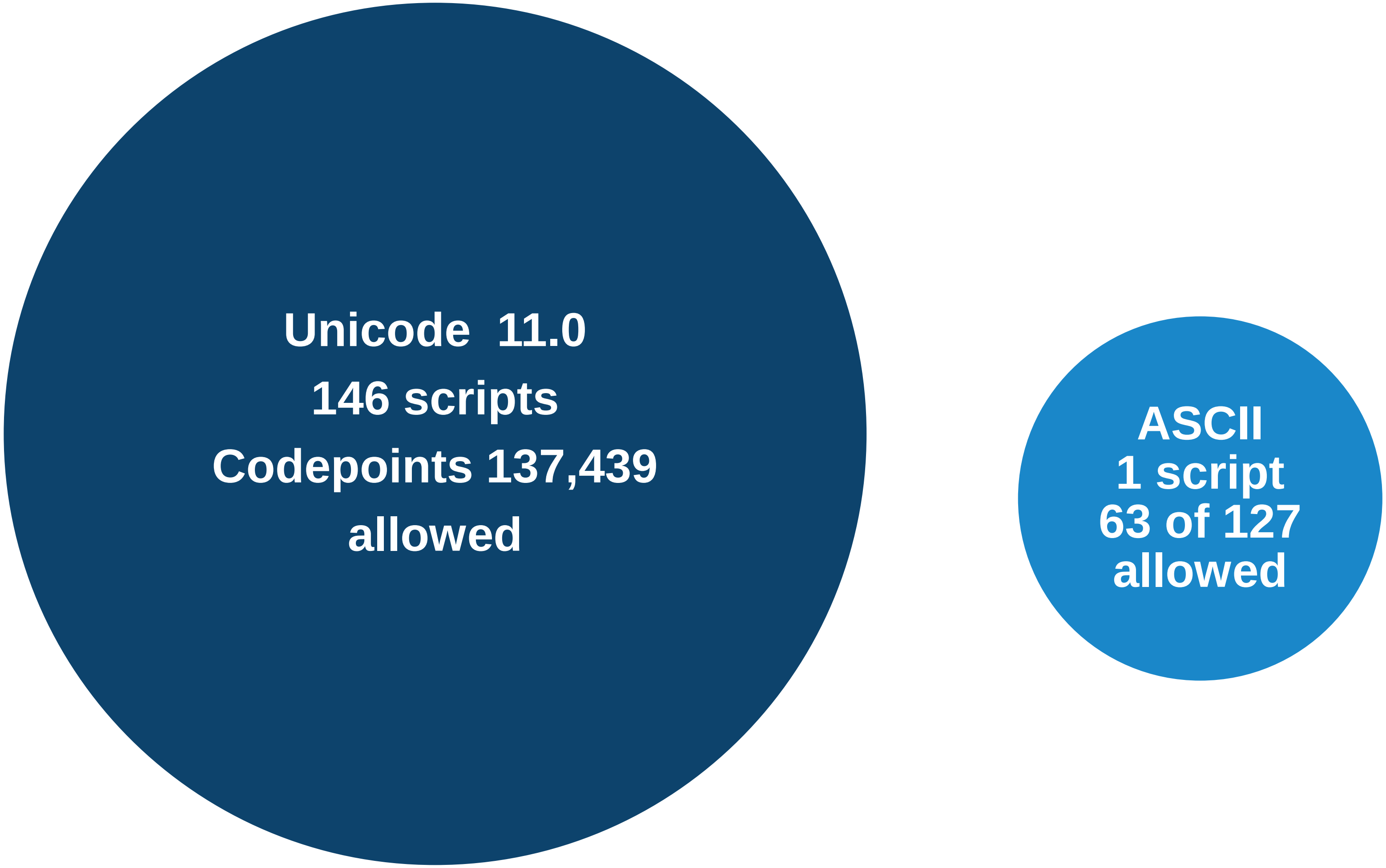


HEX	C			J	K
4E50 丿 4.4	乐 G0-4056				
4E51 丿 4.5	乑 GE-212F		乑 T4-2227	乑 J14-212C	
4E52 丿 4.5	乒 G0-4639	乒 HB1-A5E2	乒 T1-4724		乒 K2-2136
4E53 丿 4.5	乓 G0-4552	乓 HB1-A5E3	乓 T1-4725		乓 K2-2137
4E54 丿 4.5	乔 G0-4747		乔 T3-2345		
4E55 丿 4.6	乕 GE-2130			乕 J0-6949	
4E56 丿 4.7	乖 G0-3954	乖 HB1-A8C4	乖 T1-4B65	乖 J0-502A	乖 K0-4E52
4E57 丿 4.8	乗 GE-2131		乗 T3-2B22	乗 J0-3E68	乗 K2-2138
4E58 丿 4.9	乘 G0-334B	乘 HB1-ADBC	乘 T1-537D	乘 J0-502B	乘 K0-632B
4E59 乙 5.0	乙 G0-5252	乙 HB1-A441	乙 T1-4422	乙 J0-3235	乙 K0-6B60
4E5A 乙 5.0	乚 GE-2132	乚 H-C87B	乚 T4-2124	乚 J14-212F	



	090	091	092	093	094	095	096	097
0	◌ऀ 0900	ऐ 0910	ठ 0920	र 0930	◌ी 0940	ॐ 0950	ॠ 0960	॰ 0970
1	◌ँ 0901	ऑ 0911	ड 0921	ऱ 0931	◌ु 0941	◌॑ 0951	ॡ 0961	ॱ 0971
2	◌ं 0902	ऒ 0912	ढ 0922	ल 0932	◌ू 0942	◌॒ 0952	◌ॢ 0962	ॲ 0972
3	◌ः 0903	ओ 0913	ण 0923	ळ 0933	◌ृ 0943	◌॓ 0953	◌ॣ 0963	ॳ 0973
4	ऄ 0904	औ 0914	त 0924	ऴ 0934	◌ॄ 0944	◌॔ 0954	। 0964	ॴ 0974
5	अ 0905	क 0915	थ 0925	व 0935	◌ॅ 0945	◌ॕ 0955	॥ 0965	ॵ 0975
6	आ 0906	ख 0916	द 0926	श 0936	◌ॆ 0946	◌ॖ 0956	० 0966	ॶ 0976
7	इ 0907	ग 0917	ध 0927	ष 0937	◌े 0947	◌ॗ 0957	१ 0967	ॷ 0977
8	ई 0908	घ 0918	न 0928	स 0938	◌ै 0948	क़ 0958	२ 0968	ॸ 0978
9	उ 0909	ङ 0919	ऩ 0929	ह 0939	◌ॉ 0949	ख़ 0959	३ 0969	ॹ 0979

Code Point Repertoires



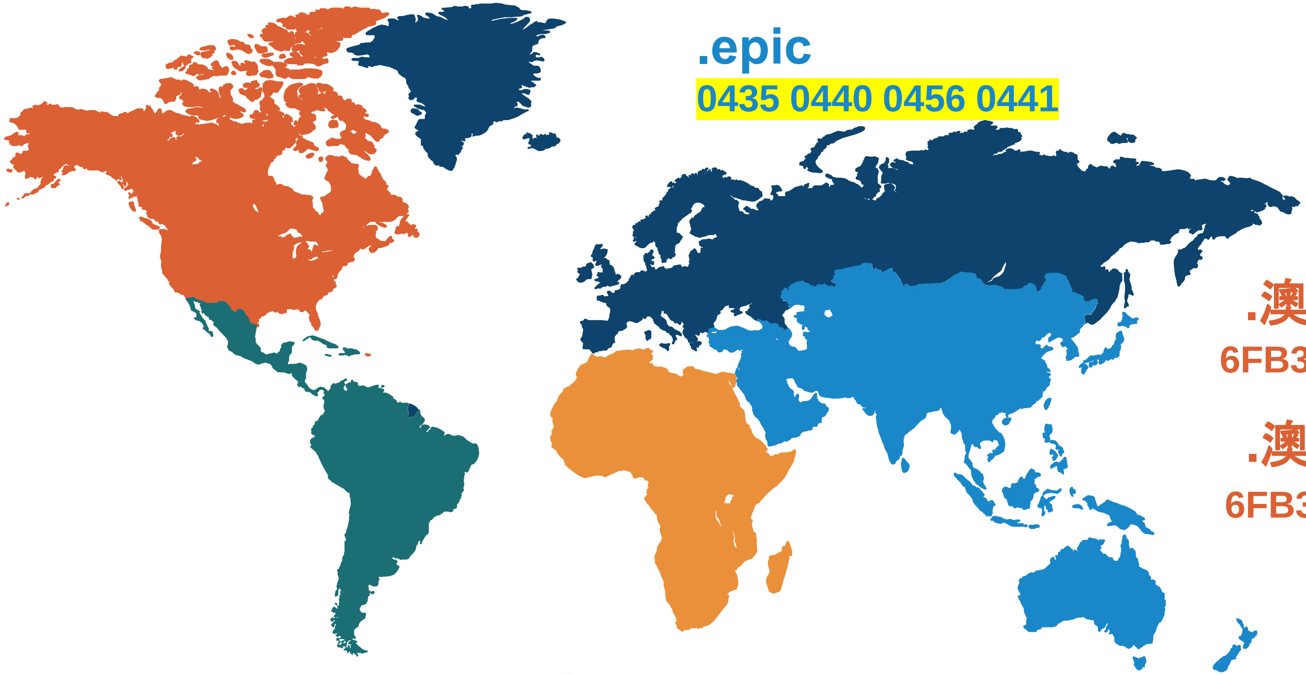
Unicode 11.0
146 scripts
Codepoints 137,439
allowed

ASCII
1 script
63 of 127
allowed

*IDNA2008 expects registries at all levels will reduce opportunities for confusion by **restricting characters** or **using variant techniques**.*

Understanding IDN Variant TLDs

- Security
- Usability



.epic
0065 0070 0069 0063

.еріс
0435 0440 0456 0441

.澳门
6FB3 95E8

.澳門
6FB3 9580

.السعودية
0627 0644 0633 0639 0648 062F 064A 0629

.السعودیۃ
0627 0644 0633 0639 0648 062F 06CC 06C3

Which Scripts Have Variant Code Points?

- Arabic
- Armenian
- Bengali
- Cyrillic
- Devanagari
- Ethiopic
- Georgian
- Greek
- Gujarati
- Gurmukhi
- Han
- Hebrew
- Japanese
- Kannada
- Khmer
- Korean
- Lao
- Latin
- Malayalam
- Myanmar
- Oriya
- Sinhala
- Tamil
- Telugu
- Thaana
- Tibetan
- Thai

🟥	Variant code points
🟩	No variant code points
⬛	Work in progress

① Root Zone Label Generation Rules Procedure

Generation Panels

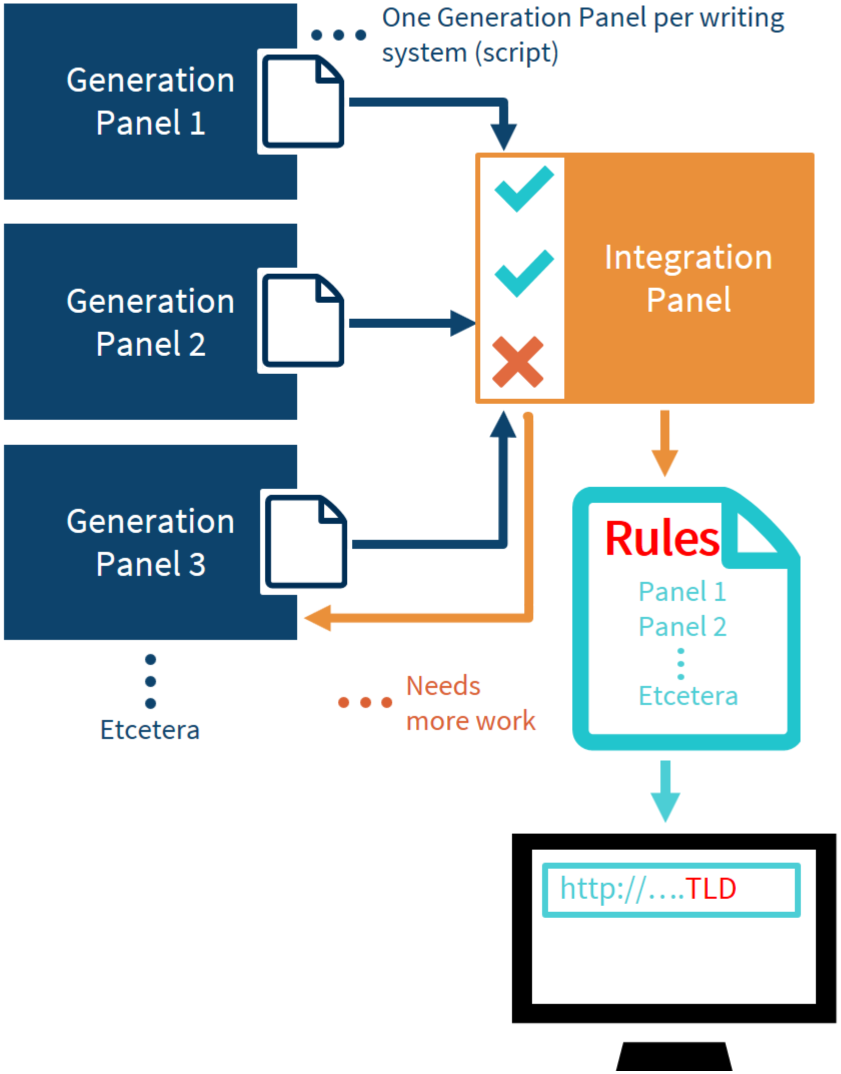
– Generate proposals for script specific LGRs, based on community expertise and linguistic, security, and stability requirements.

Integration Panel

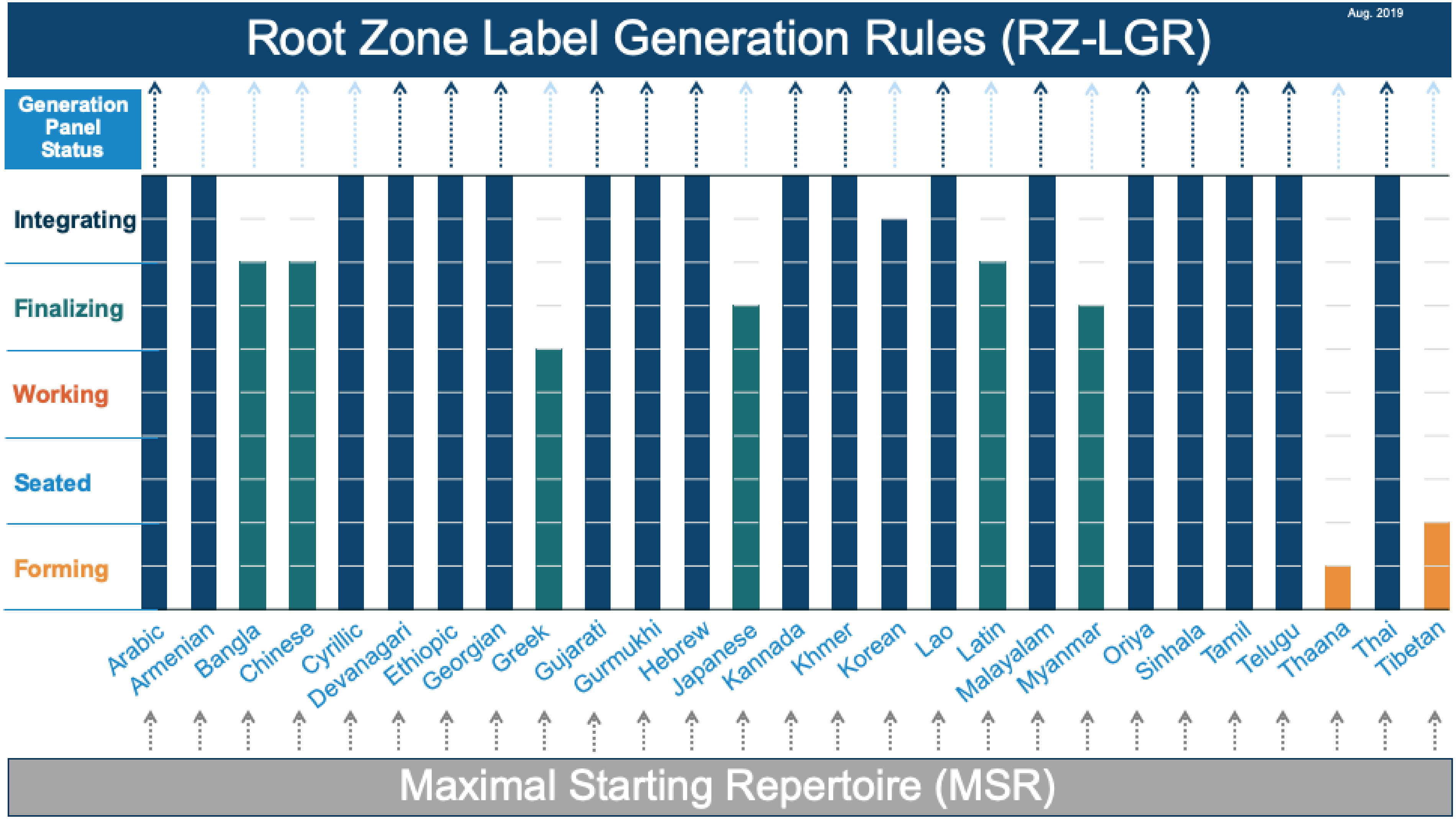
– Integrates them into common Root Zone LGR while minimizing the risk to Root Zone as shared resource.

Label Generation Rules (LGR)

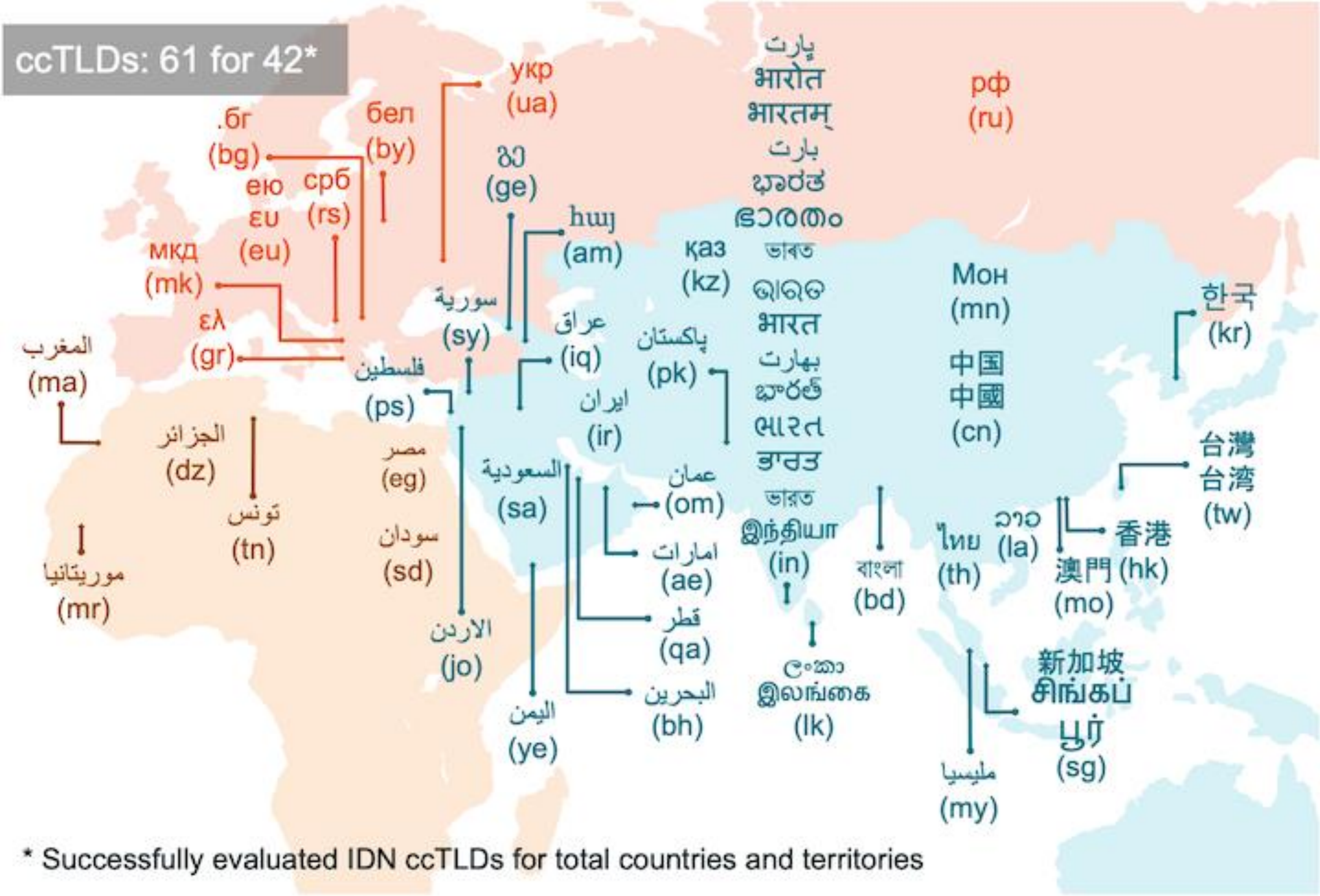
– Which labels are permissible?
– Which variant labels exist?
– Are there any more constraints?



Generation Panels Status



IDN Country Code Top-level Domains



ccTLDs: 61 for 42*

* Successfully evaluated IDN ccTLDs for total countries and territories

Confuability / Security Issue

✗ **paypal**

(0070 0061 0079 0070 0430 006C)

✓ **paypal**

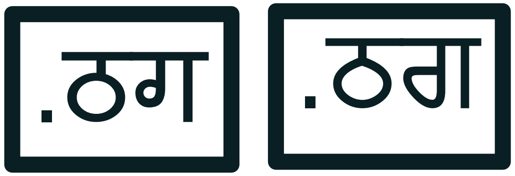
TLD - Variant example for Devanagari

.ठग

TLD - Variant example for Gurmukhi

.ਠਗ

TLD - Variant example for Devanagari and Gurmukhi



Universal Acceptance of Domain Names and email addresses

https://www.uasg.tech

Universal Acceptance Steering Group

Universal Acceptance (UA) Initiative

Vision

All domain names and email addresses work in all software applications.

Mission

To mobilize the software application developers to get their products UA-ready by providing encouragement, documentation, case studies, tools, and measures to deliver the right user experience to the end user.

Impact

Promote consumer choice, improve competition, and provide broader access to end users.

Categories Affected by UA Issues

- **Newer top-level domain names:** example.sky
- **Longer top-level domain names:** example.photography
- **Internationalized Domain Names:** البحرين.مثال
  - Rendering problems
    - Displaying A-label: xn--mgbh0fb.xn--mgbcpq6gpa15g
    - Ordering right-to-left scripts: should be مثال.البحرين
- **Internationalized email addresses:** अजय@डाटा.भारत (Hindi email)
  - Available standards are not implemented by all email software and service providers making email delivery unreliable.
    - Test if your email is compliant: https://uasg.tech/eai-check/

Five Actions for UA-readiness

Applications should be able to do the following for all domain names and email addresses:

- **Accept**
- **Validate**
- **Store**
- **Process**
- **Display**

Moving Forward

- Test your own email address
- Secure an EAI address

    - Use DataMail or

    Install DataMail App to get EAI address

    Get your own systems evaluated and fixed

    - Use UASG Blueprint for CIOs as a guide
- Get your tendering and contracts to include UA Readiness Clauses

    - Use UASG Quick Guide to Tendering clauses
- Report UA problems with other applications

    - UASG Issue Logging
- Participate in the UASG Discussions

    - Join the UA Discuss Mailing List

Universal Acceptance Steering Group

- To address the Universal Acceptance of domain names and email addresses, the Universal Acceptance Steering Group (UASG) was organized as a community initiative.

- UASG has produced documentation to define and address challenges, and share progress, available at https://UASG.tech.
  - Quick Guide to Universal Acceptance
  - Quick Guide to Email Address Internationalization
  - UA Case Study: Government of Rajasthan, India
  - Quick Guide to Tendering and Contractual Documents

- UASG is actively engaged in disseminating the information to relevant stakeholders.

Thank You

Dr. Ajay Data

ajay@data.in

अजय@डाटा.भारत

অজয়ডাটা@ডাটামেল্.ভারত

Internet Governance Forum

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

GFCE Triple-I @INSIG2019, Kolkata, India, 14 November 2019

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

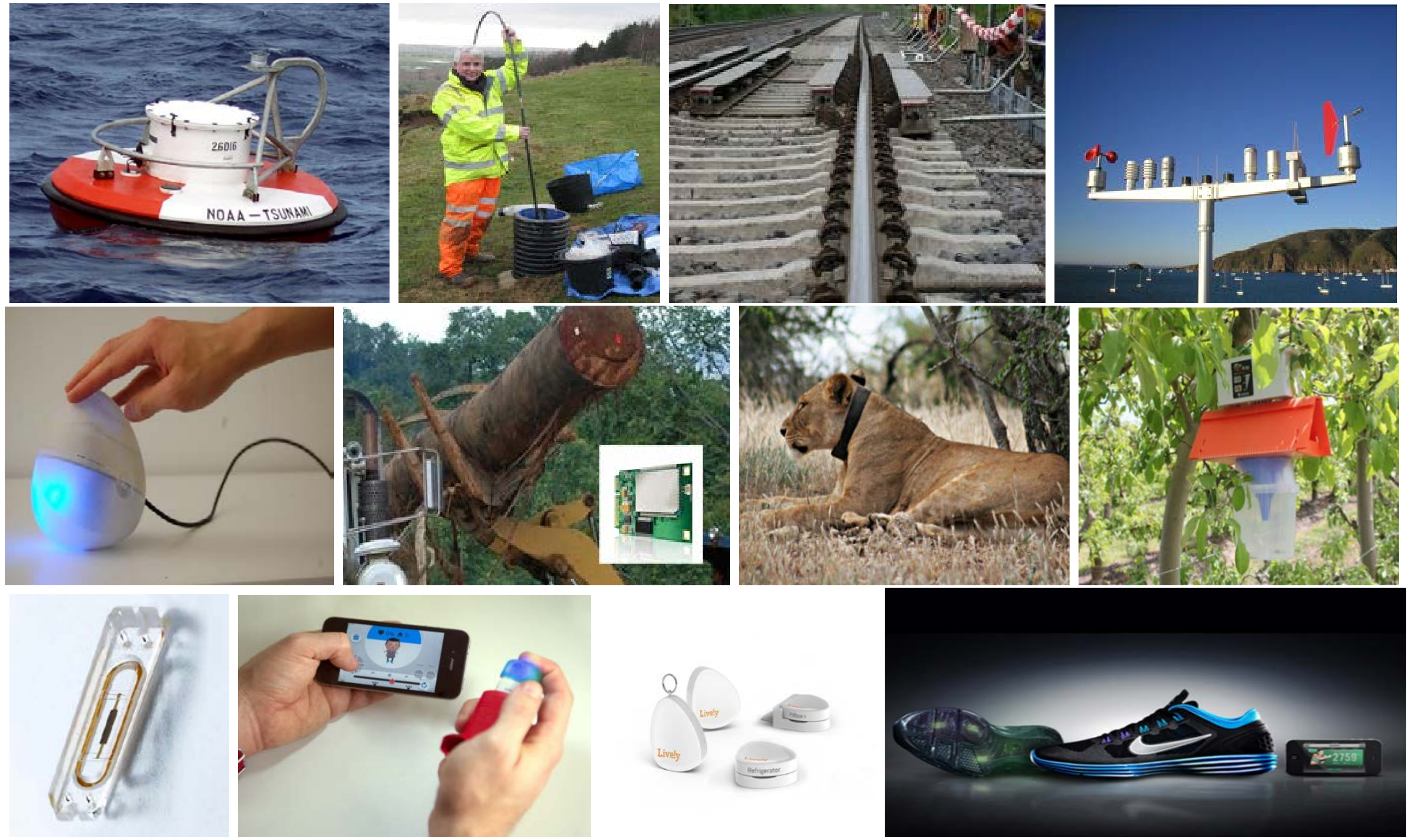
Address specific societal issues

- 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.

1 NO POVERTY
2 ZERO HUNGER
3 GOOD HEALTH AND WELL-BEING
4 QUALITY EDUCATION
5 GENDER EQUALITY
6 CLEAN WATER AND SANITATION
7 AFFORDABLE AND CLEAN ENERGY
8 DECENT WORK AND ECONOMIC GROWTH
9 INDUSTRY, INNOVATION AND INFRASTRUCTURE
10 REDUCED INEQUALITIES
11 SUSTAINABLE CITIES AND COMMUNITIES
12 RESPONSIBLE CONSUMPTION AND PRODUCTION
13 CLIMATE ACTION
14 LIFE BELOW WATER
15 LIFE ON LAND
16 PEACE, JUSTICE AND STRONG INSTITUTIONS
17 PARTNERSHIPS FOR THE GOALS
INTERNET OF THINGS AND THE SUSTAINABLE DEVELOPMENT GOALS

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 ....



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

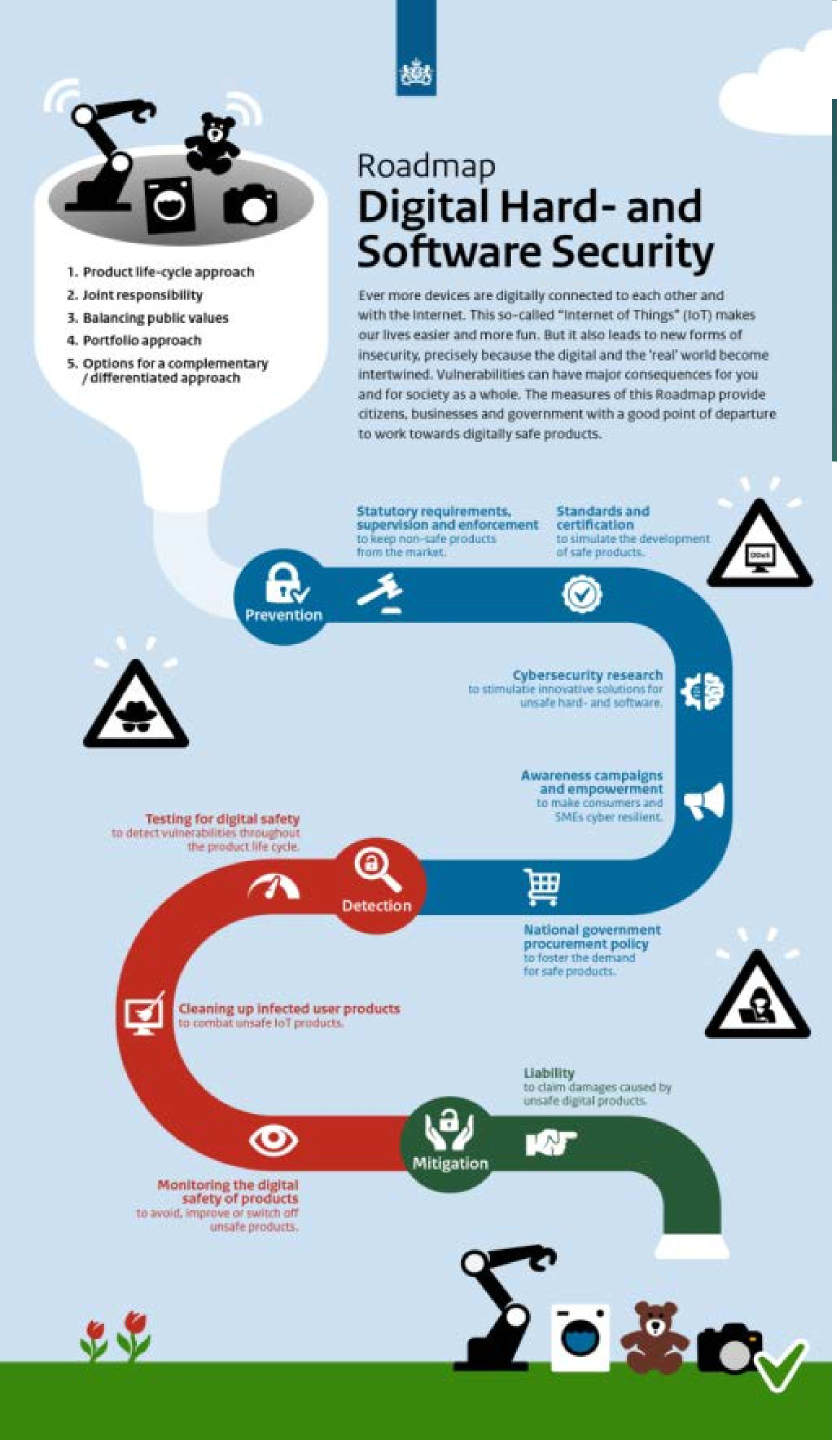
The Canadian approach

- 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.

Statutory requirements, supervision and enforcement to keep non-safe products from the market.

Standards and certification to simulate the development of safe products.

Cybersecurity research to stimulatie innovative solutions for unsafe hard- and software.

Awareness campaigns and empowerment to make consumers and SMEs cyber resilient.

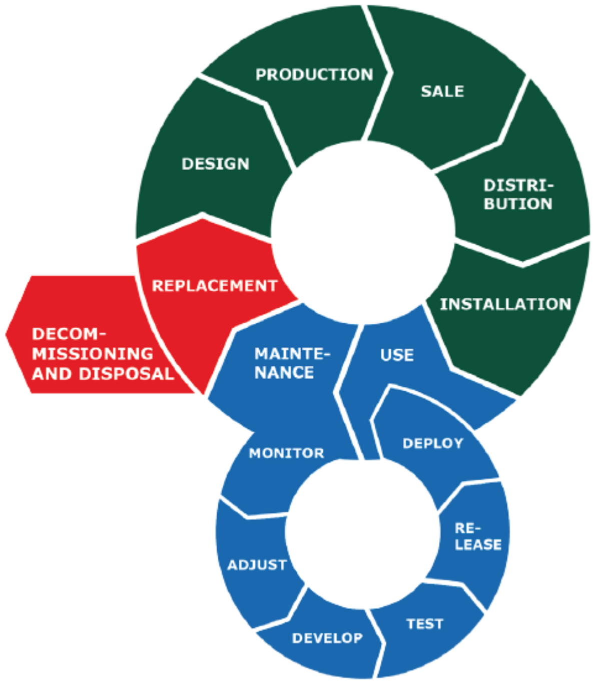
National government procurement policy to foster the demand for safe products.

Testing for digital safety to detect vulnerabilities throughout the product life cycle.

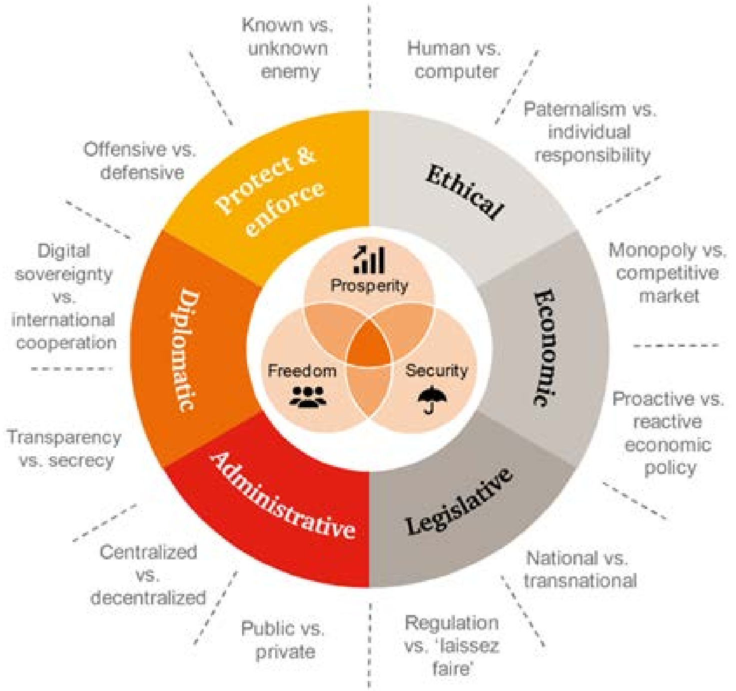
Cleaning up infected user products to combat unsafe IoT products.

Monitoring the digital safety of products to avoid, improve or switch off unsafe products.

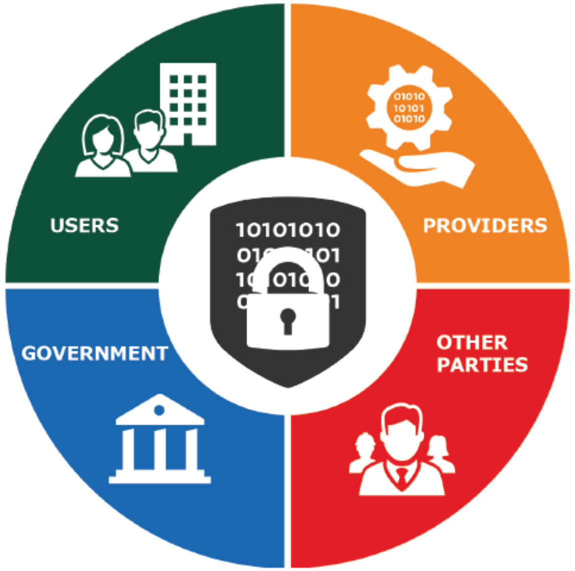
Liability to claim damages caused by unsafe digital products.



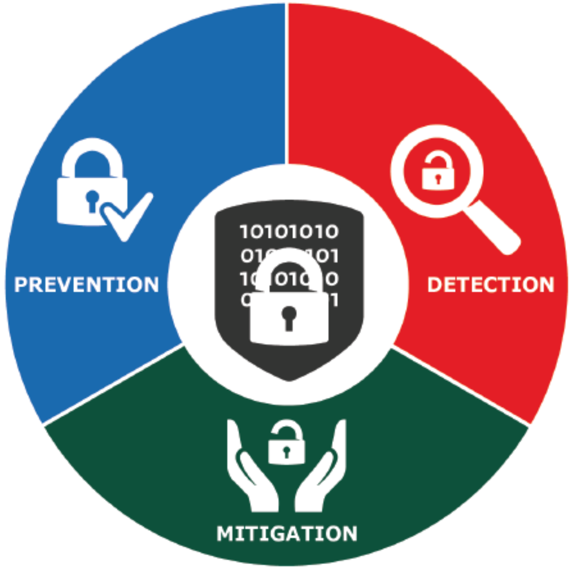
Product life cycle approach


Known vs. unknown enemy
Human vs. computer
Paternalism vs. individual responsibility
Monopoly vs. competitive market
Proactive vs. reactive economic policy
National vs. transnational
Regulation vs. 'laissez faire'
Public vs. private
Centralized vs. decentralized
Transparency vs. secrecy
Digital sovereignty vs. international cooperation
Offensive vs. defensive
Protect & enforce
Ethical
Economic
Legislative
Administrative
Diplomatic
Prosperity
Freedom
Security

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

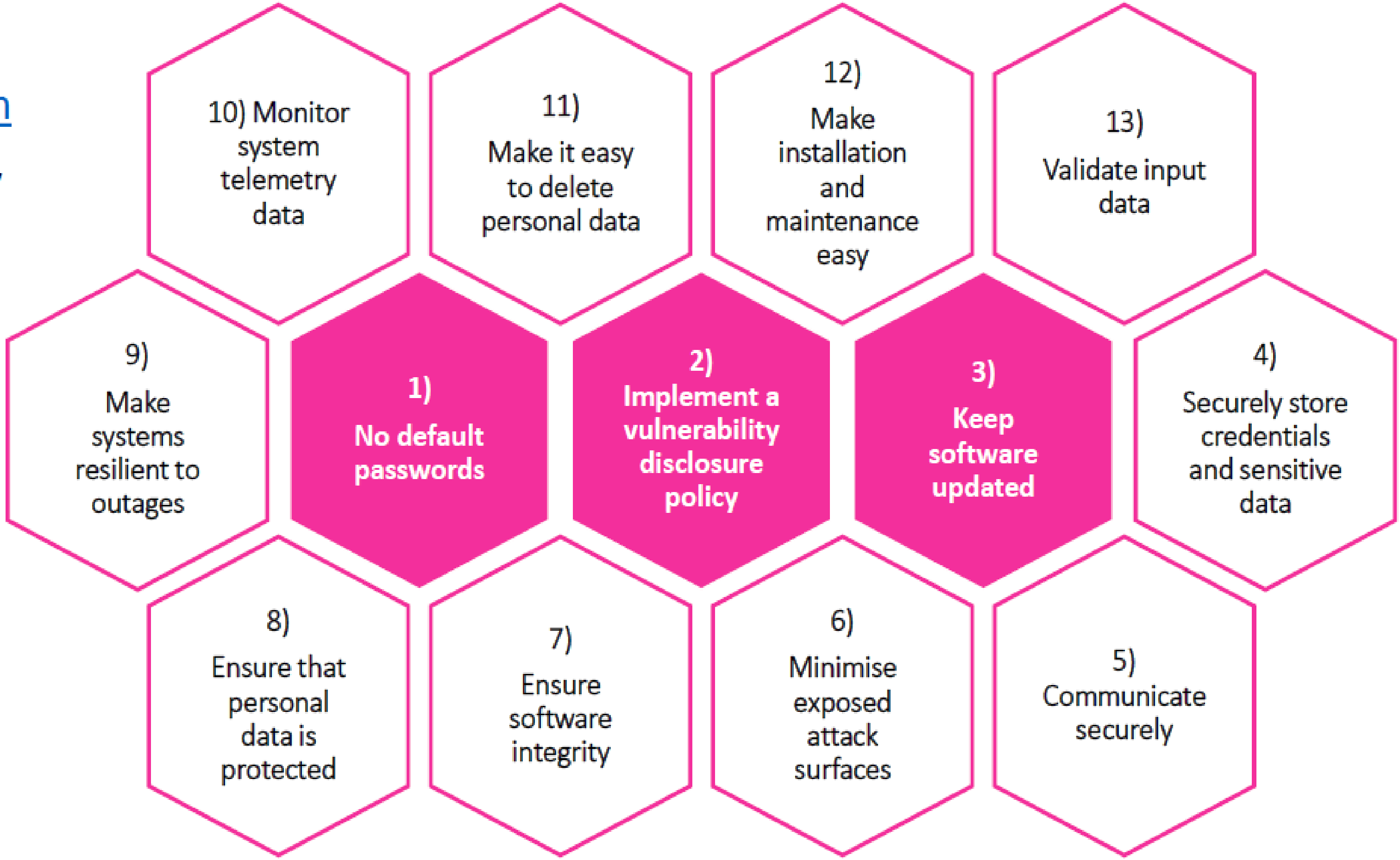
October 2018: Code of Practice for Consumer IoT Security

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.



1) No default passwords

2) Implement a vulnerability disclosure policy

3) Keep software updated

4) Securely store credentials and sensitive data

5) Communicate securely

6) Minimise exposed attack surfaces

7) Ensure software integrity

8) Ensure that personal data is protected

9) Make systems resilient to outages

10) Monitor system telemetry data

11) Make it easy to delete personal data

12) Make installation and maintenance easy

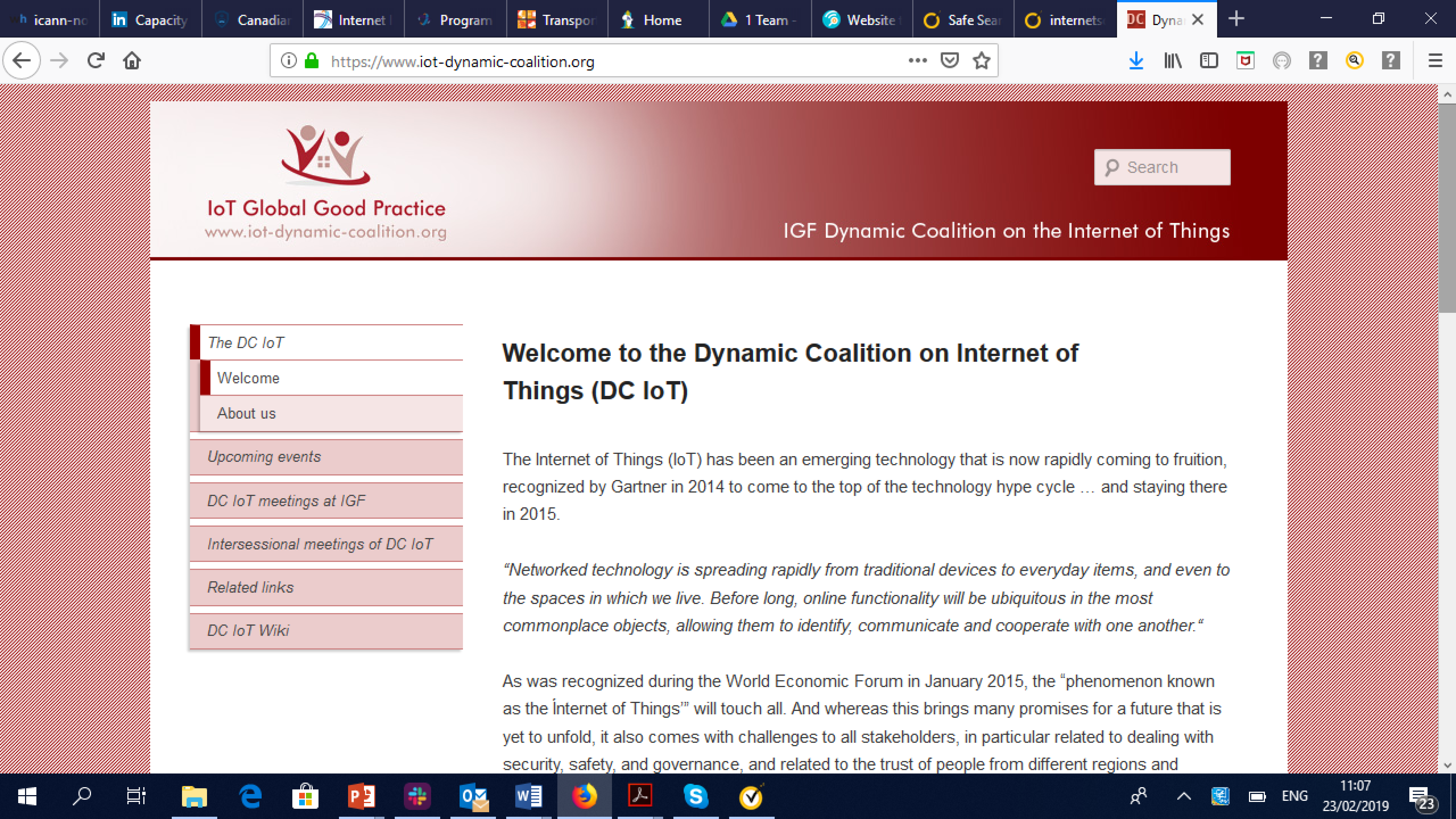
13) Validate input data

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

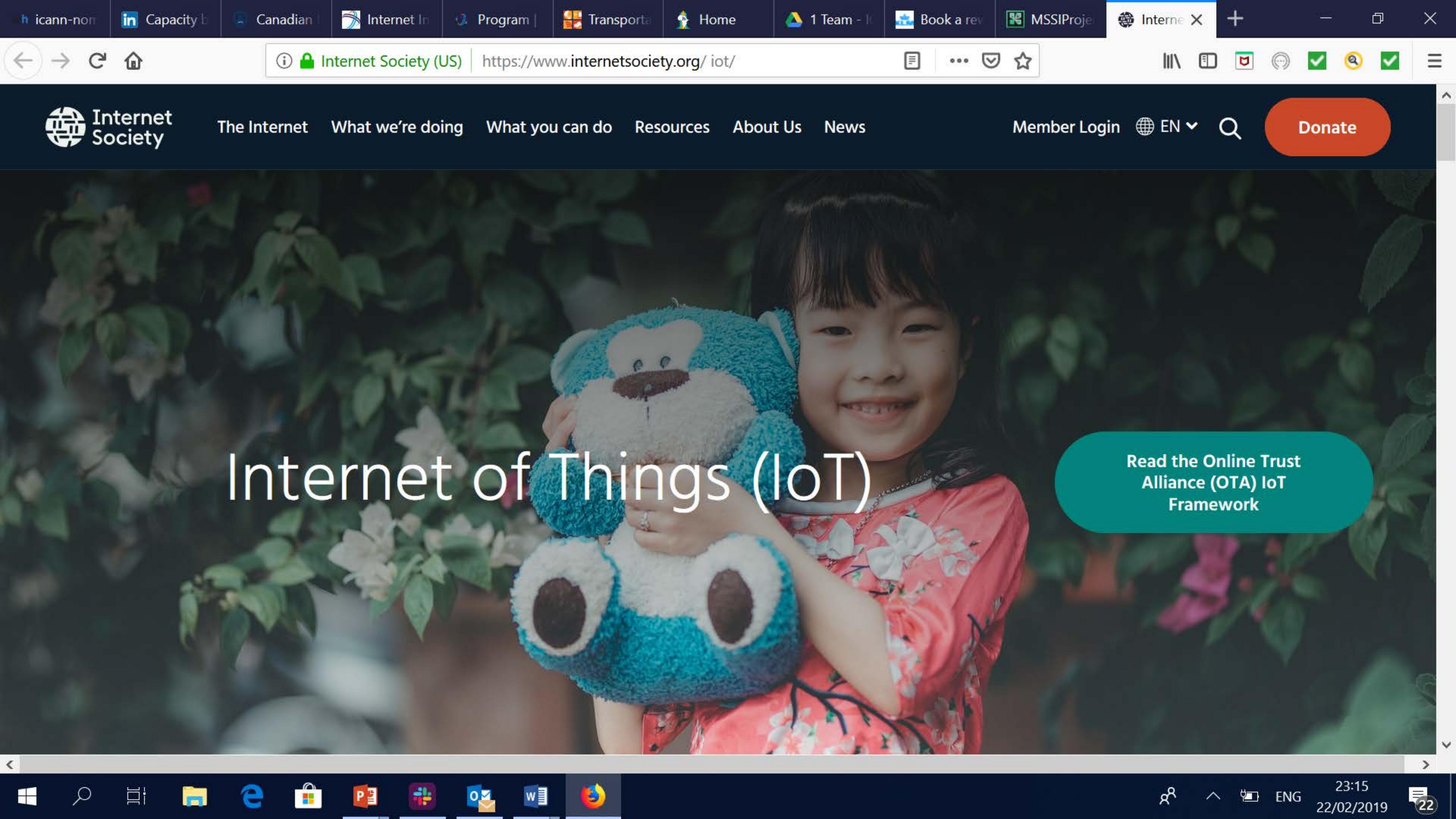


Welcome to the Dynamic Coalition on Internet of Things (DC IoT)

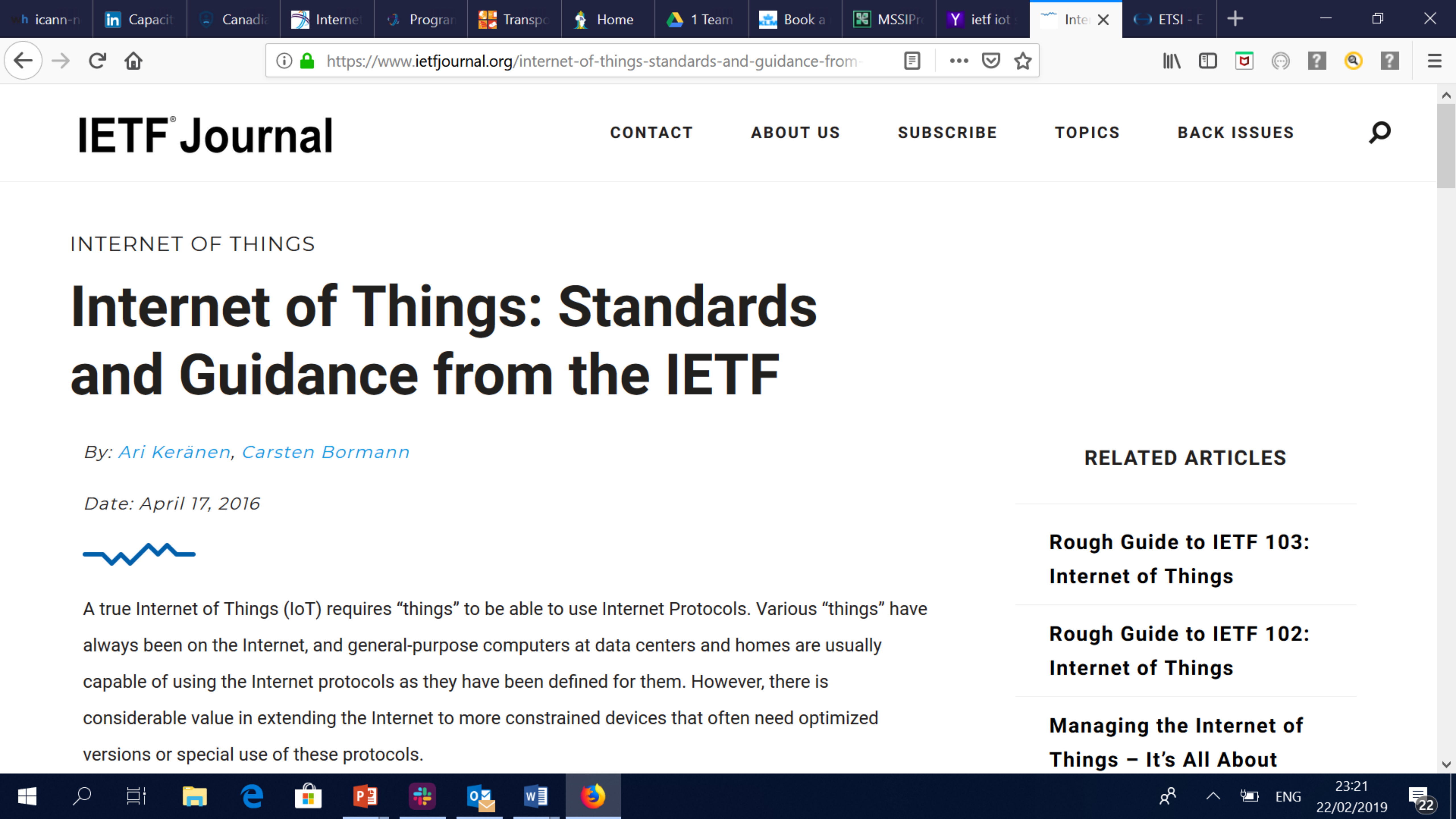
The Internet of Things (IoT) has been an emerging technology that is now rapidly coming to fruition, recognized by Gartner in 2014 to come to the top of the technology hype cycle … and staying there in 2015.

"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)



IETF® Journal

INTERNET OF THINGS

Internet of Things: Standards and Guidance from the IETF

By: Ari Keränen, Carsten Bormann

Date: April 17, 2016

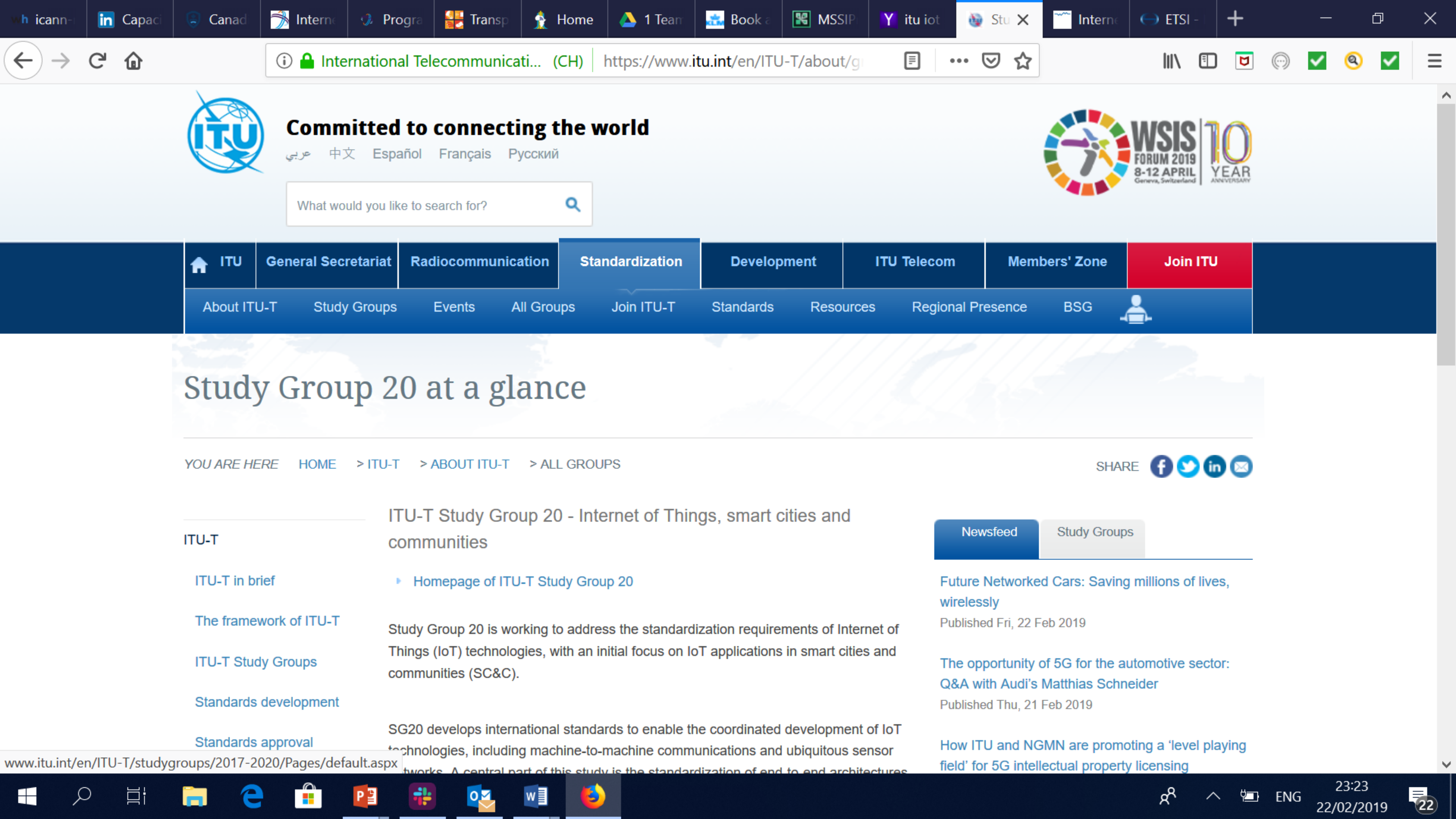
A true Internet of Things (IoT) requires "things" to be able to use Internet Protocols. Various "things" have always been on the Internet, and general-purpose computers at data centers and homes are usually capable of using the Internet protocols as they have been defined for them. However, there is 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 Study Group 20 - Internet of Things, smart cities and communities

- Homepage of ITU-T Study Group 20

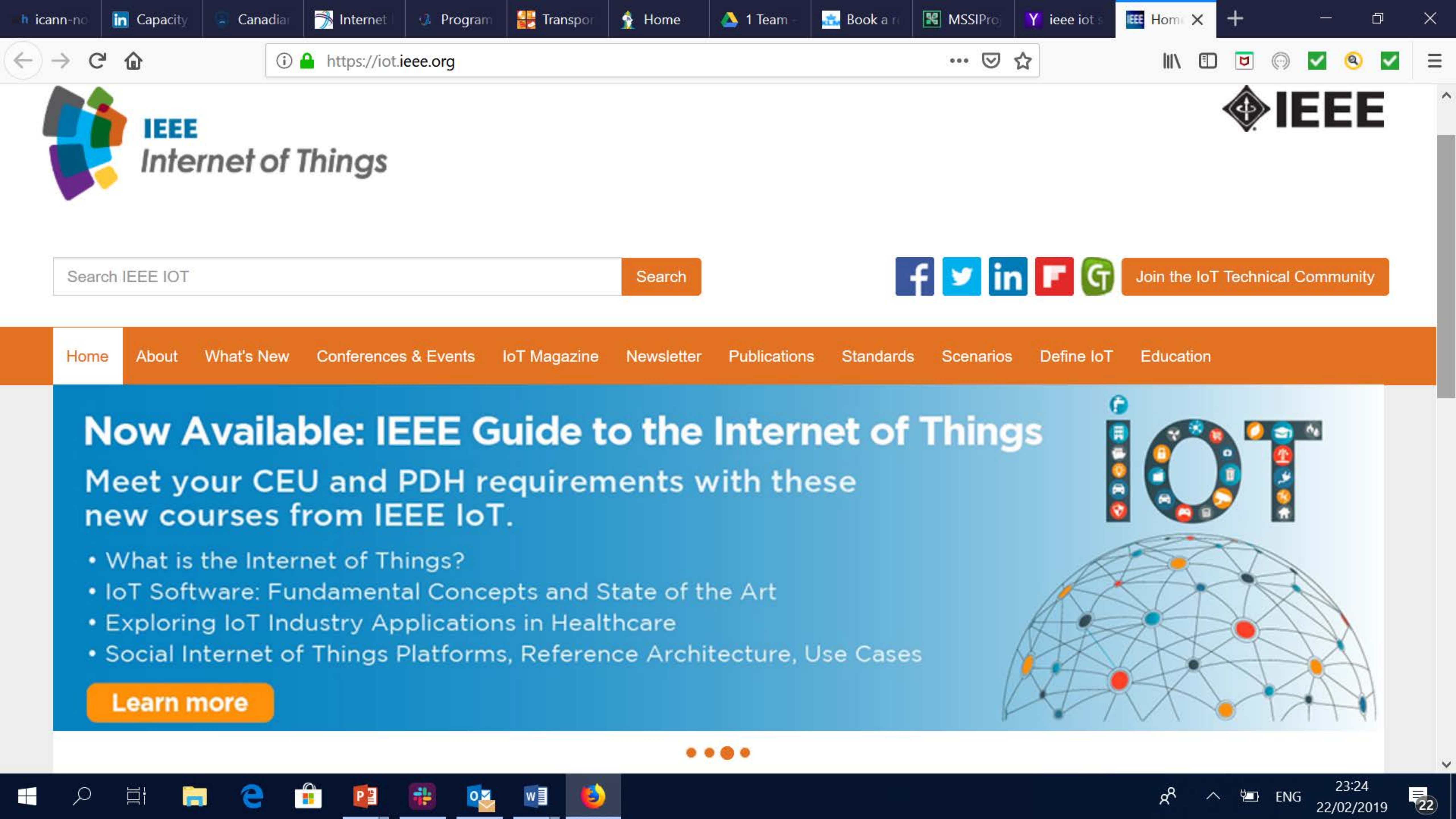
Study Group 20 is working to address the standardization requirements of Internet of Things (IoT) technologies, with an initial focus on IoT applications in smart cities and communities (SC&C).

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

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



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

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

Better routing security through concerted action

SIMON SOHEL BAROI
Fiber@Home Global Limited.

GFCE Triple-I Day @INSIG2019
Thursday 14 November, 2019
Kolkata, India

Routing Incidents Cause Real World Problems

Event	Explanation	Repercussions	Example
Prefix/Route Hijacking	A network operator or attacker impersonates another network operator, pretending that a server or network is their client.	Packets are forwarded to the wrong place, and can cause Denial of Service (DoS) attacks or traffic interception.	*The 2008 YouTube hijack* *April 2018 Amazon Route 53 hijack*
Route Leak	A network operator with multiple upstream providers (often due to accidental misconfiguration) announces to one upstream provider that is has a route to a destination through the other upstream provider.	Can be used for a MITM, including traffic inspection, modification and reconnaissance.	*November 2018. Google faced a major outage in many parts of the world thanks to a BGP leak. This incident that was caused by a Nigerian ISP MainOne.* *June 2019. Allegheny leaked routes from another provider to Verizon, causing significant outage.*
IP Address Spoofing	Someone creates IP packets with a false source IP address to hide the identity of the sender or to impersonate another computing	The root cause of reflection DDoS attacks	*March 1, 2018. Memcached 1.3Tb/s reflection-amplification attack reported by Akamai*

We Are In This Together

Network operators have a collective responsibility to ensure a globally robust and secure routing infrastructure.

Your network’s safety depends on a routing infrastructure that mitigates incidents from bad actors and accidental misconfigurations that wreak havoc on the Internet.

Security of your network depends on measures taken by other operators.

The more network operators work together, the fewer incidents there will be, and the less damage they can do.

Mutually Agreed Norms for Routing Security

MANRS provides baseline recommendations in the form of Actions

- Distilled from common behaviors – BCPs, optimized for low cost and low risk of deployment
- With high potential of becoming norms

MANRS builds a visible community of security minded operators

- Social acceptance and peer pressure

MANRS

MANRS for Network operators

Filtering

Prevent propagation of incorrect routing information

Ensure the correctness of your own announcements and announcements from your customers to adjacent networks with prefix and AS-path granularity

Anti-spoofing

Prevent traffic with spoofed source IP addresses

Enable source address validation for at least single-homed stub customer networks, their own end-users, and infrastructure

Coordination

Facilitate global operational communication and coordination between network operators

Maintain globally accessible up-to-date contact information in common routing databases

Global Validation

Facilitate validation of routing information on a global scale

Publish your data, so others can validate

MANRS for IXPs

Action 1

Prevent propagation of incorrect routing information

This mandatory action requires IXPs to implement filtering of route announcements at the Route Server based on routing information data (IRR and/or RPKI).

Action 2

Promote MANRS to the IXP membership

IXPs joining MANRS are expected to provide encouragement or assistance for their members to implement MANRS actions.

Action 3

Protect the peering platform

This action requires that the IXP has a published policy of traffic not allowed on the peering fabric and performs filtering of such traffic.

Action 4

Facilitate global operational communication and coordination

The IXP facilitates communication among members by providing necessary mailing lists and member directories.

Action 5

Provide monitoring and debugging tools to the members.

The IXP provides a looking glass for its members.

MANRS for CDN&Cloud - a draft action set

Action 1

Prevent propagation of incorrect routing information

Egress filtering

Ingress filtering – non-transit peers, explicit whitelists

Action 2

Prevent traffic with illegitimate source IP addresses

Anti-spoofing controls to prevent packets with illegitimate source IP address

Action 3

Facilitate global operational communication and coordination

Contact information in PeeringDB

and relevant RIR databases

Action 4

Facilitate validation of routing information on a global scale

Publicly document ASNs and prefixes that are intended to be advertised to external parties.

Action 5

Encourage MANRS adoption

Actively encourage MANRS adoption among the peers

Action 6

Provide monitoring and debugging tools to peering partners

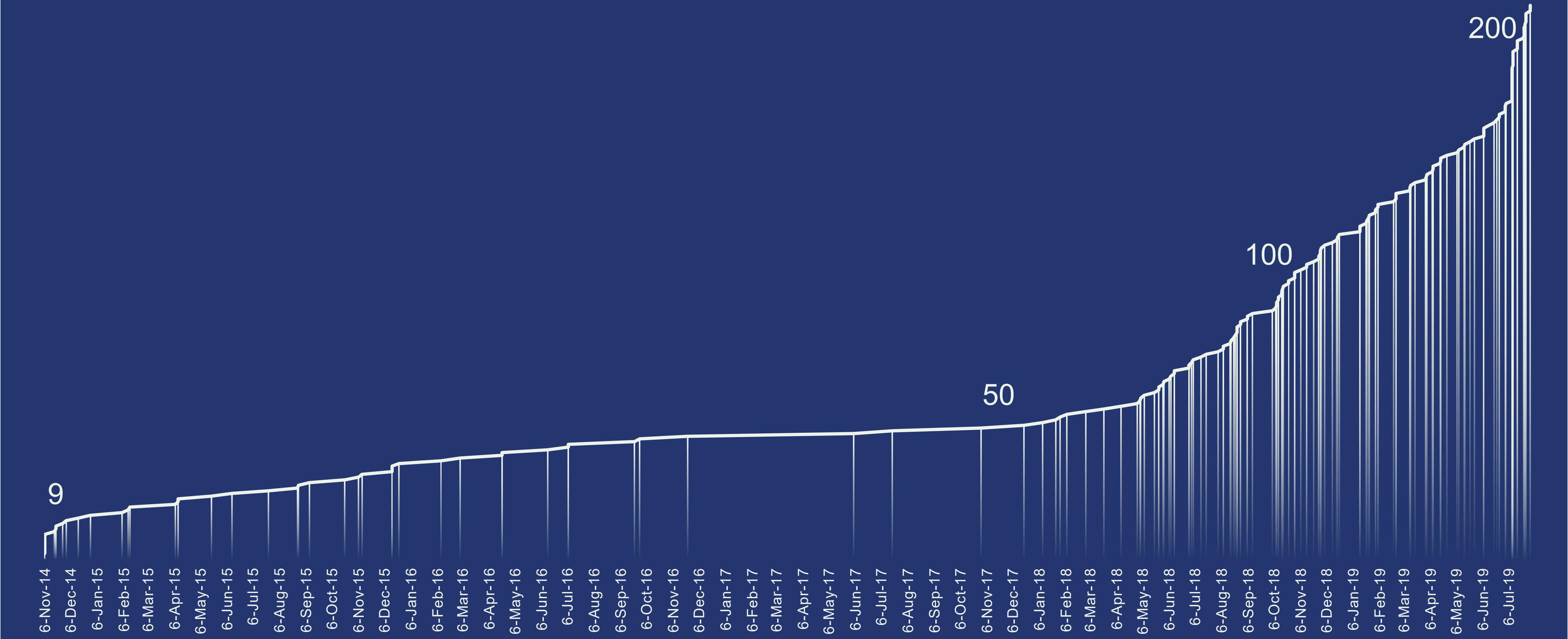
Provide monitoring tools to indicate incorrect announcements from peers that were filtered by the CDN&Cloud operator.

MANRS – increasing adoption

228 ISPs

41 IXPs

GROWTH OF THE MANRS MEMBERSHIP (NETWORK OPERATORS)

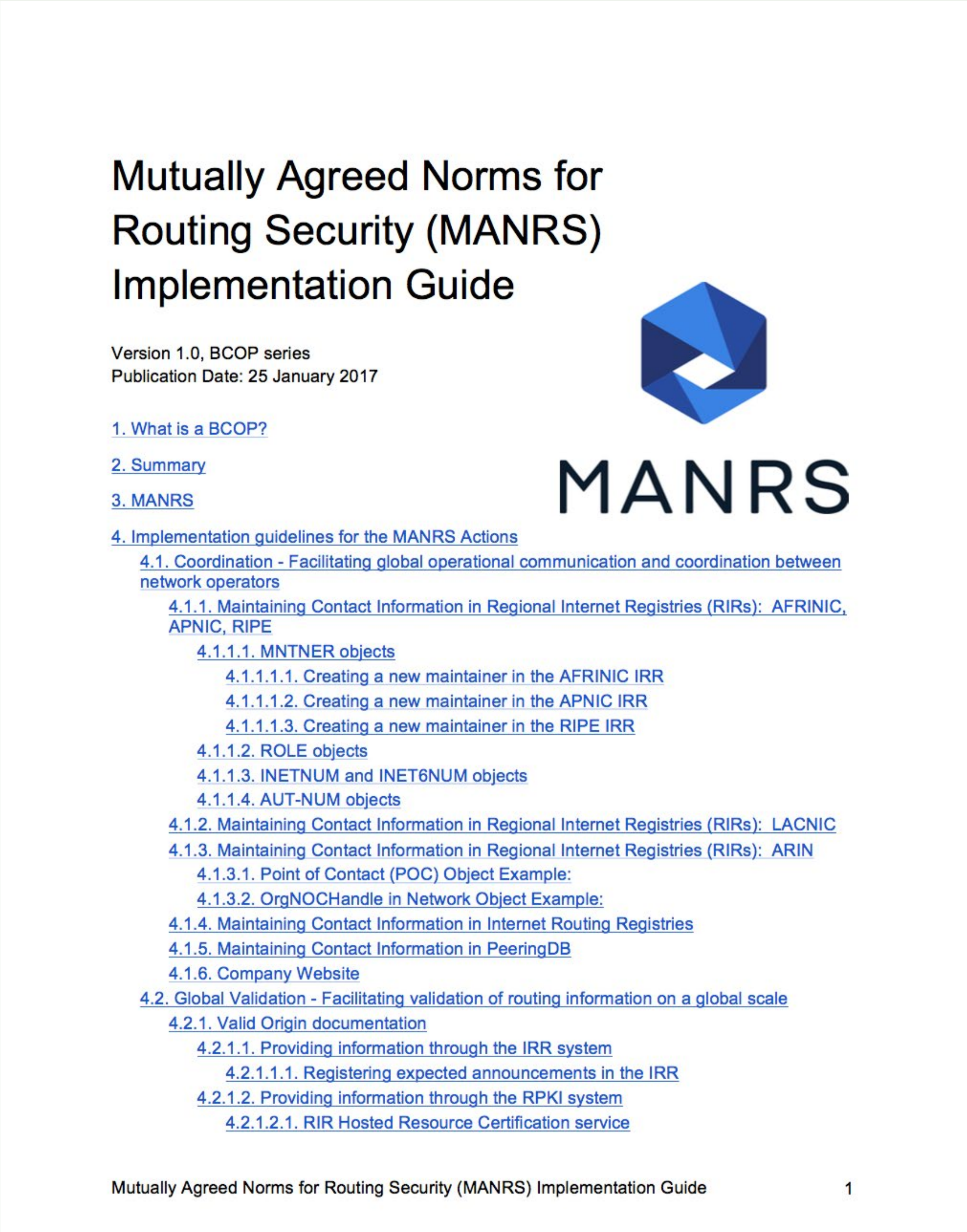


MANRS – capacity building

MANRS Implementation Guide

A resource to help Operators implement MANRS Actions.

- Based on Best Current Operational Practices deployed by network operators around the world
- https://www.manrs.org/bcop/
- Has received recognition from the RIPE community by being published as RIPE-706



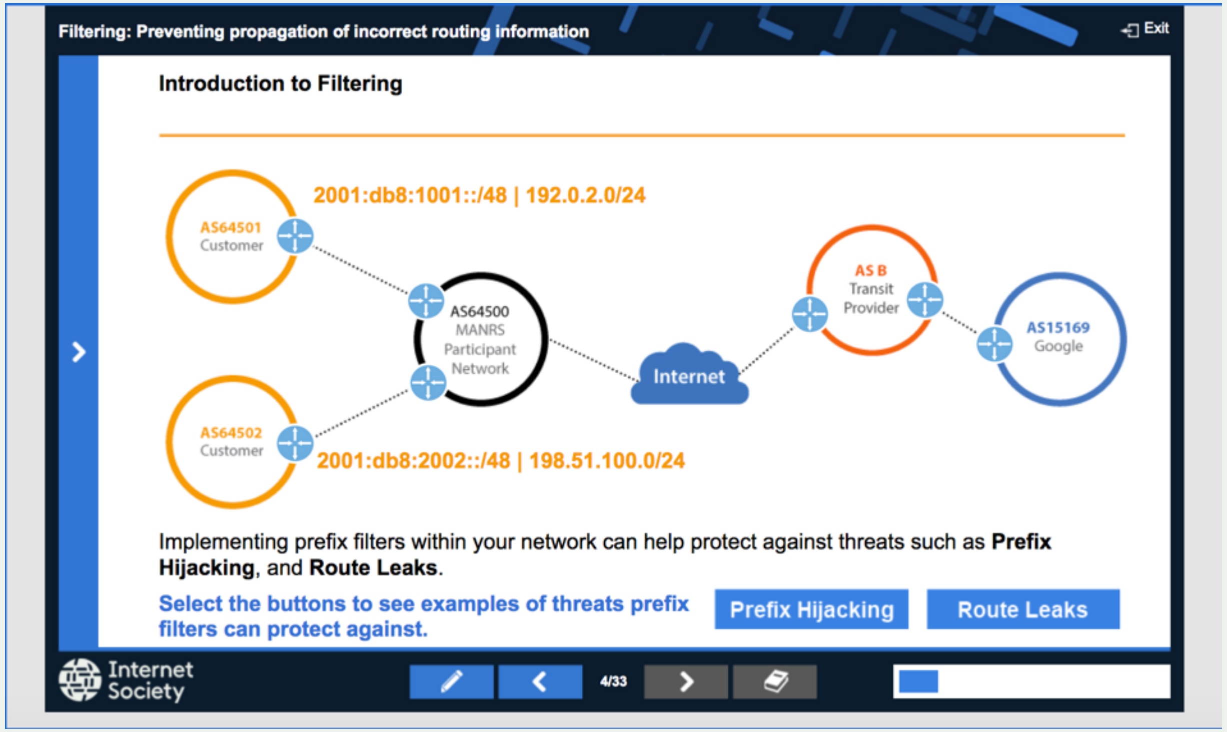
Mutually Agreed Norms for Routing Security (MANRS) Implementation Guide

Version 1.0, BCOP series
Publication Date: 25 January 2017

MANRS Training Tutorials

6 training tutorials based on information in the Implementation Guide. A test at the end of each tutorial. https://www.manrs.org/tutorials

About to begin training moderators for online classes (43 applications received!)



Filtering: Preventing propagation of incorrect routing information

Introduction to Filtering

Implementing prefix filters within your network can help protect against threats such as **Prefix Hijacking**, and **Route Leaks**.

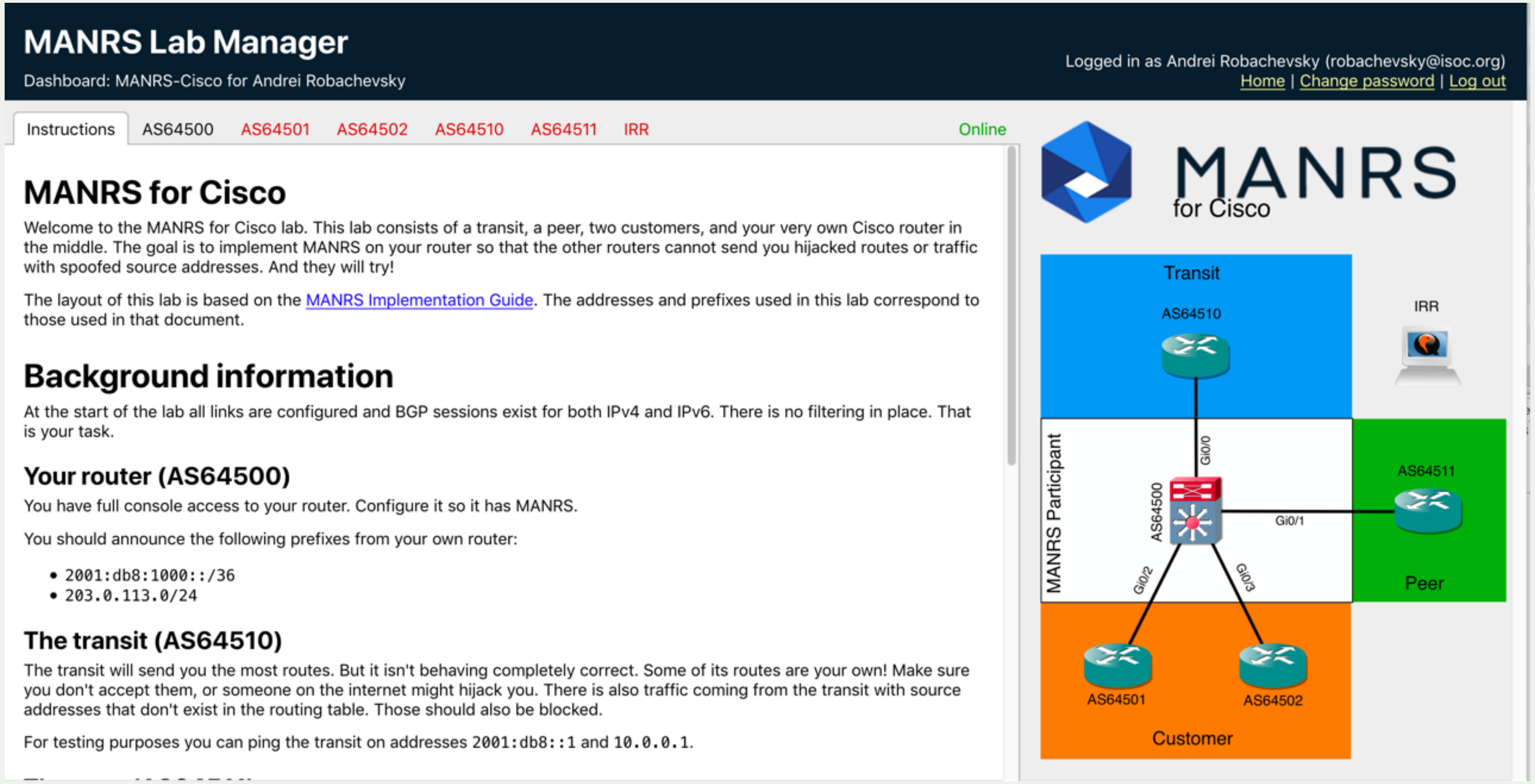
Select the buttons to see examples of threats prefix filters can protect against.

MANRS Hands-on Lab

The prototype lab is ready, finalizing the production version.

- Cisco
- Juniper
- Mikrotik

Can be used as a standalone lab or as an end-exam



MANRS Lab Manager

Dashboard: MANRS-Cisco for Andrei Robachevsky

Logged in as Andrei Robachevsky (robachevsky@isoc.org)
Home | Change password | Log out

MANRS for Cisco

Welcome to the MANRS for Cisco lab. This lab consists of a transit, a peer, two customers, and your very own Cisco router in the middle. The goal is to implement MANRS on your router so that the other routers cannot send you hijacked routes or traffic with spoofed source addresses. And they will try!

The layout of this lab is based on the MANRS Implementation Guide. The addresses and prefixes used in this lab correspond to those used in that document.

Background information

At the start of the lab all links are configured and BGP sessions exist for both IPv4 and IPv6. There is no filtering in place. That is your task.

Your router (AS64500)

You have full console access to your router. Configure it so it has MANRS.

You should announce the following prefixes from your own router:

- `2001:db8:1000::/36`
- `203.0.113.0/24`

The transit (AS64510)

The transit will send you the most routes. But it isn't behaving completely correct. Some of its routes are your own! Make sure you don't accept them, or someone on the internet might hijack you. There is also traffic coming from the transit with source addresses that don't exist in the routing table. Those should also be blocked.

For testing purposes you can ping the transit on addresses `2001:db8::1` and `10.0.0.1`.

Measuring MANRS Readiness

Motivation

Inform MANRS members about their degree of commitment

- Improve reputation and transparency of the effort
- Facilitate continuous improvement and correction

Provide a factual state of routing security as it relates to MANRS

- Support the problem statement with data
- Demonstrate the impact and progress
- Network, country, region, over time

Improve robustness of the evaluation process

- Make it more comprehensive and consistent
- Reduce the load
- Allow preparation (self-assessment)

Measurement framework

- Passive
- Based on third party open data sources

Data sources and caveats

Action	Measurement	Data source	Caveats
Filtering	Route hijacks and leaks	BGPStream.com	False positives, obscure algorithms, vantage points
Filtering	“Bogon” announcements	CIDR report	Limited vantage points
Anti-spoofing	Negative tests	CAIDA Spoofer	Sparse, active
Coordination	Registered contacts	RIRs Whois DBs	Stale/non-responsive contacts not detected
Global validation	Coverage of routing announcements	IRRs, RPKI	

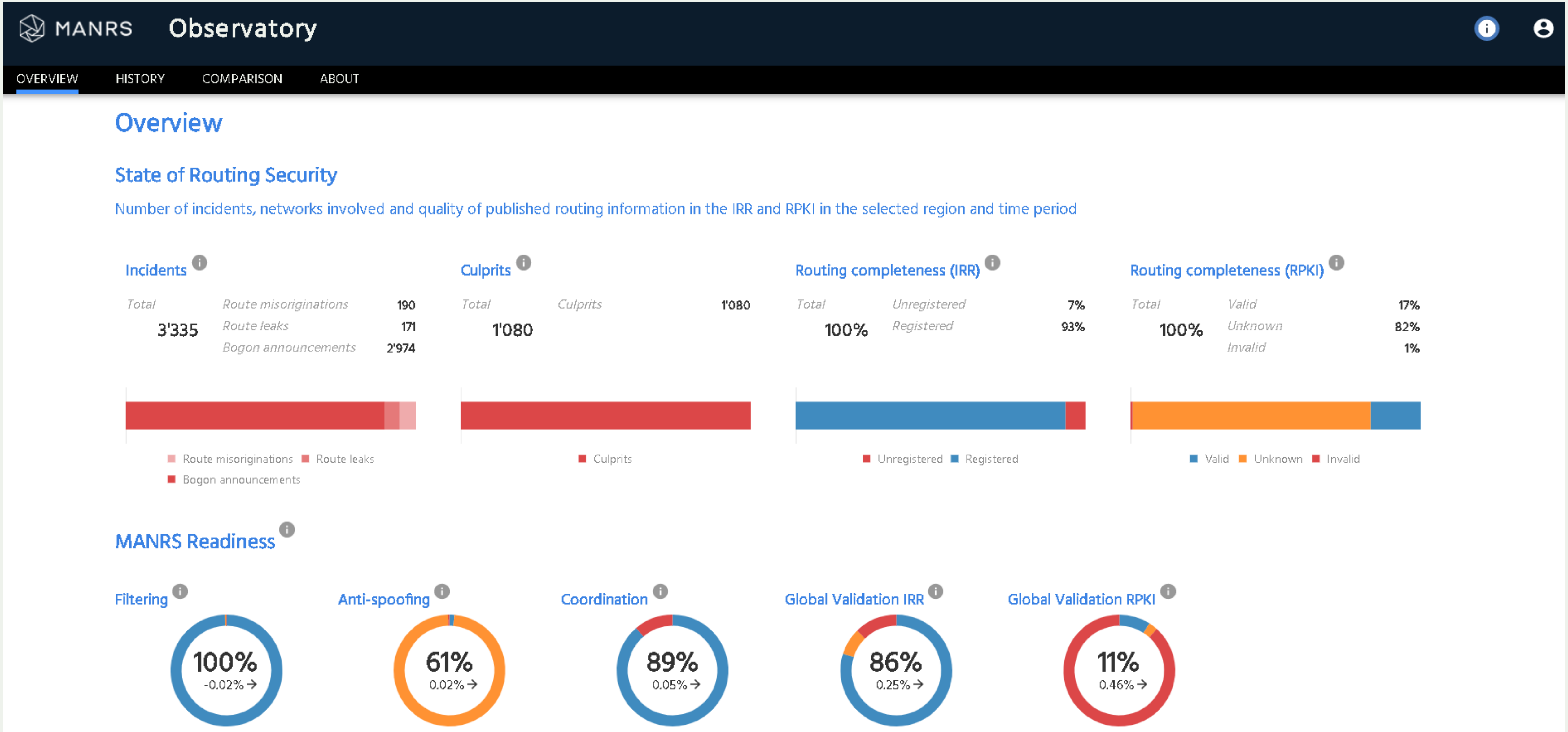
2 views of the Observatory

Public view – granularity: region, economy, pre-defined groups (e.g. MANRS)

Private view – granularity: region, economy, ASN

2 views of the Observatory

Public view



MANRS Observatory

OVERVIEW HISTORY COMPARISON ABOUT

Overview

State of Routing Security

Number of incidents, networks involved and quality of published routing information in the IRR and RPKI in the selected region and time period

Incidents

Total		
3'335	*Route misoriginations*	190
	Route leaks	171
	Bogon announcements	2'974

Culprits

Total		
1'080	*Culprits*	1'080

Routing completeness (IRR)

Total		
100%	*Unregistered*	7%
	Registered	93%

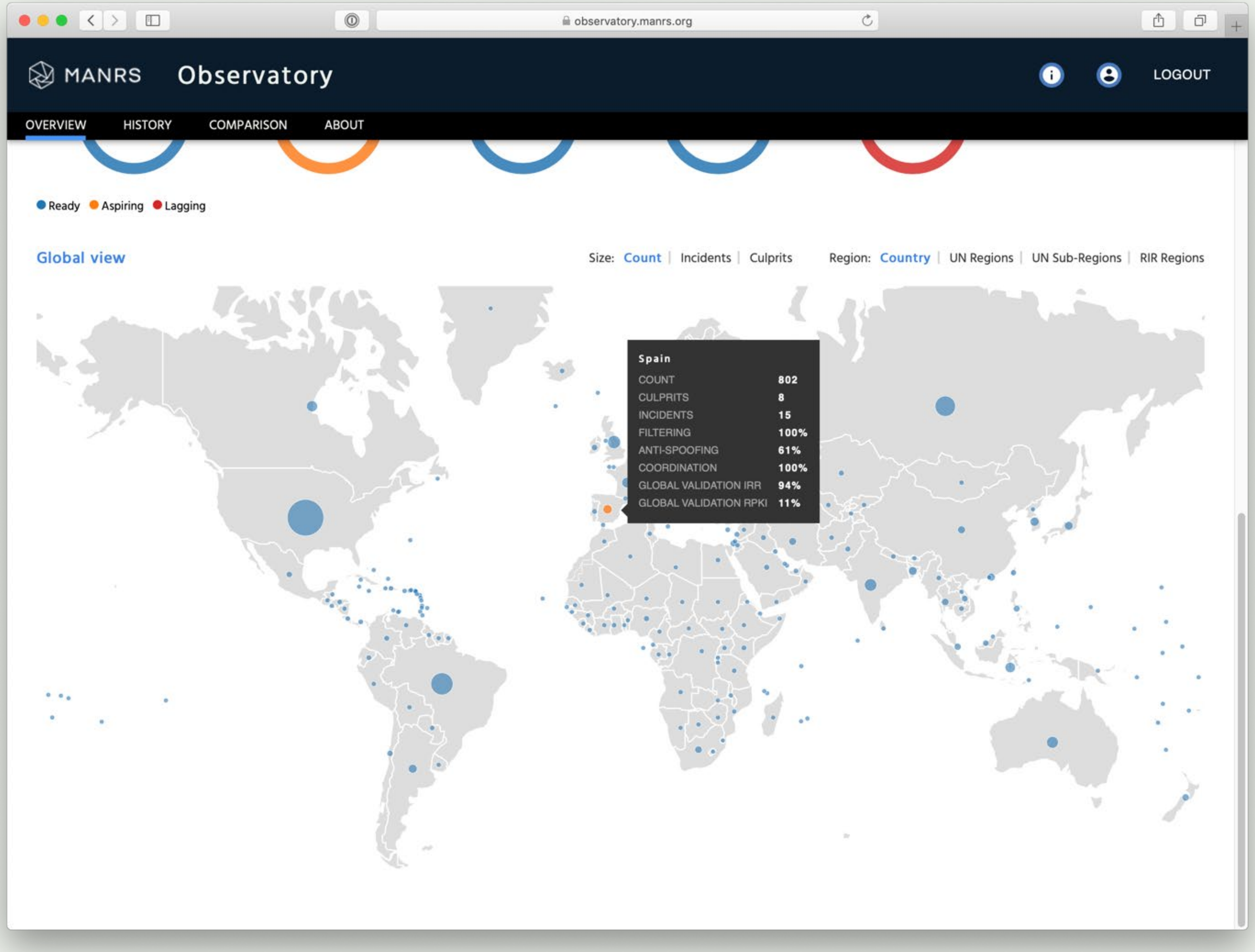
Routing completeness (RPKI)

Total		
100%	*Valid*	17%
	Unknown	82%
	Invalid	1%

MANRS Readiness

Filtering	Anti-spoofing	Coordination	Global Validation IRR	Global Validation RPKI
100% -0.02% →	61% 0.02% →	89% 0.05% →	86% 0.25% →	11% 0.46% →

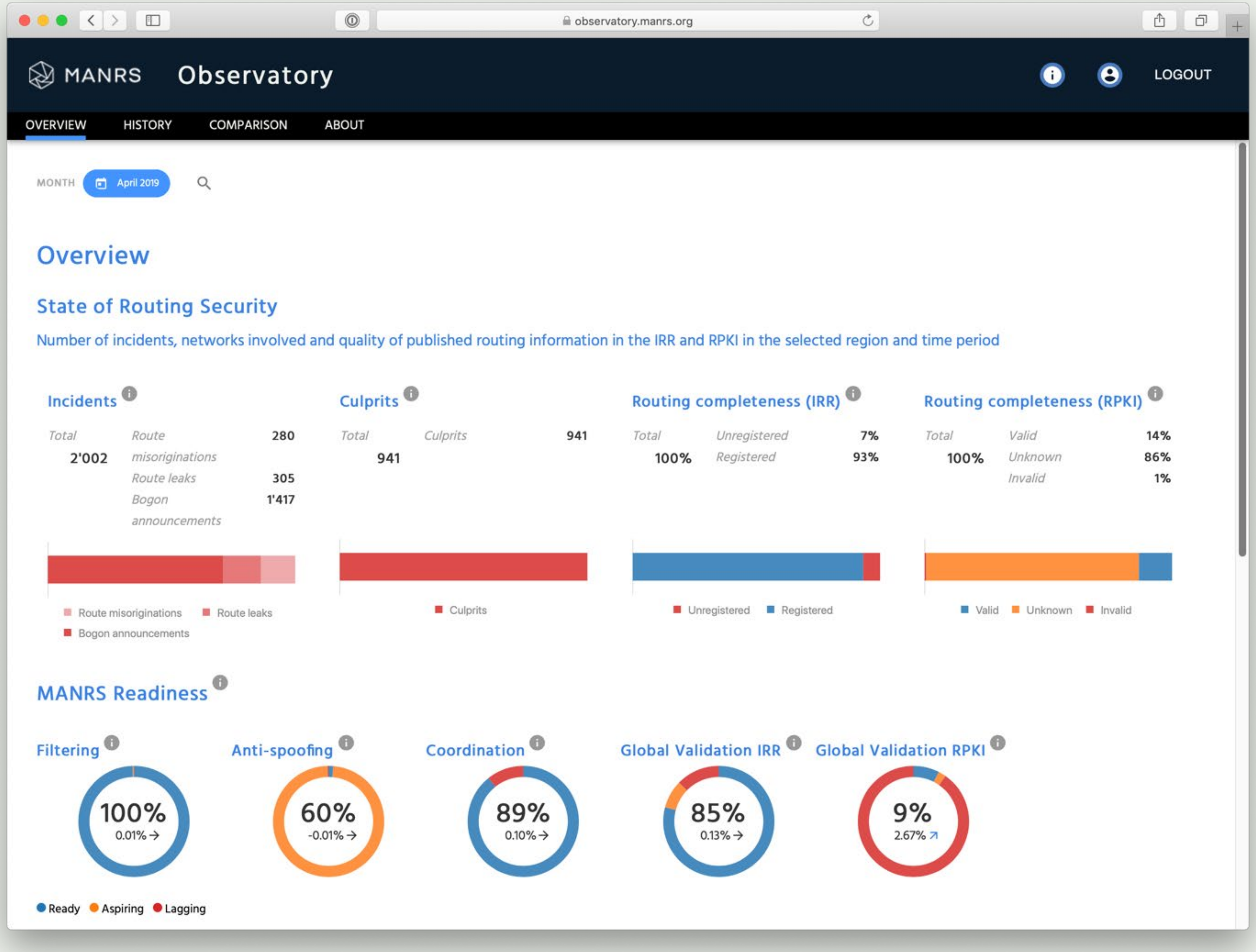
MONTH October 2019



Global view

Size: Count | Incidents | Culprits   Region: Country | UN Regions | UN Sub-Regions | RIR Regions

Spain	
COUNT	802
CULPRITS	8
INCIDENTS	15
FILTERING	100%
ANTI-SPOOFING	61%
COORDINATION	100%
GLOBAL VALIDATION IRR	94%
GLOBAL VALIDATION RPKI	11%



Overview

State of Routing Security

Number of incidents, networks involved and quality of published routing information in the IRR and RPKI in the selected region and time period

Incidents

Total 2'002

Route misoriginations	280
Route leaks	305
Bogon announcements	1'417

Culprits

Total 941

Culprits	941

Routing completeness (IRR)

Total 100%

Unregistered	7%
Registered	93%

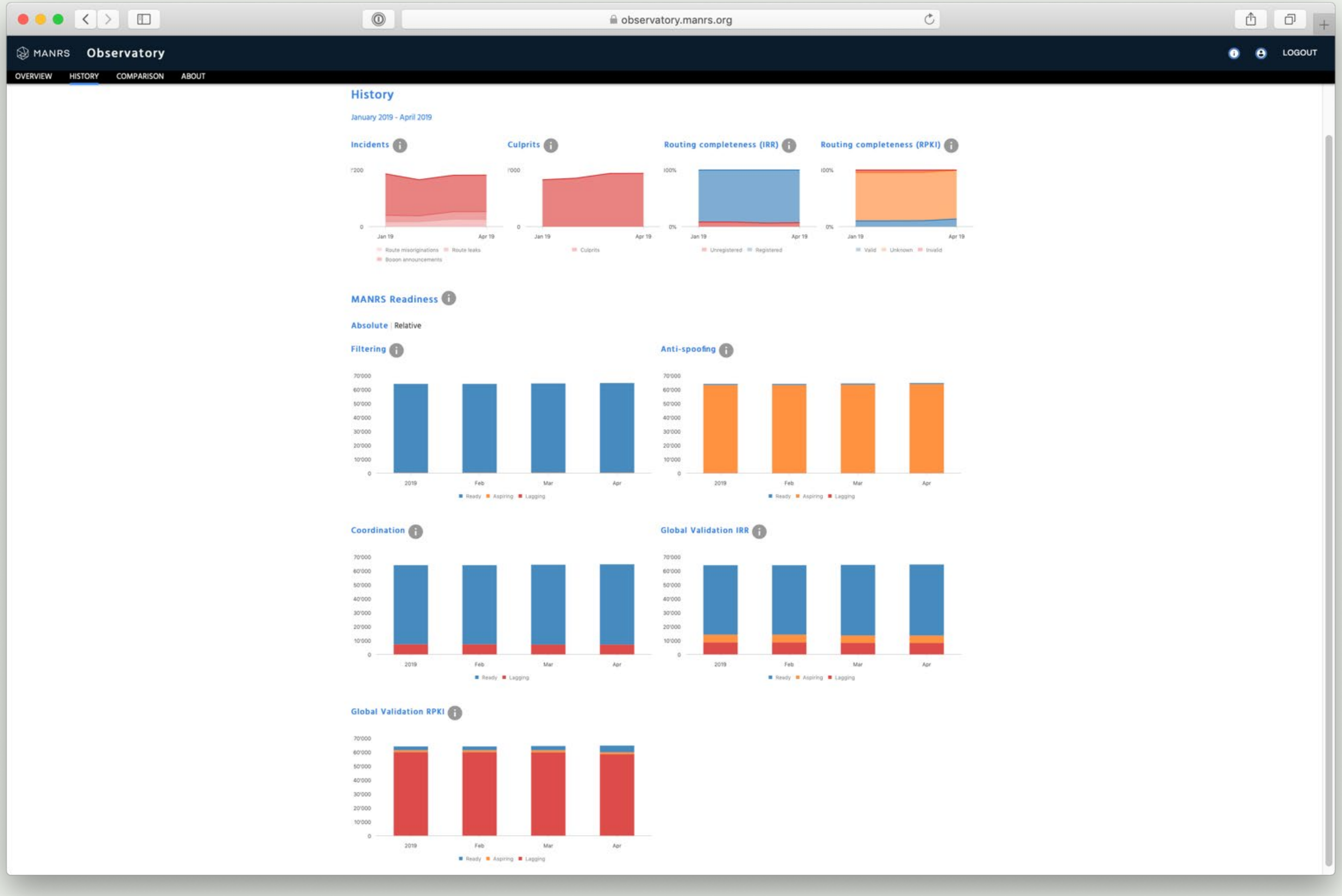
Routing completeness (RPKI)

Total 100%

Valid	14%
Unknown	86%
Invalid	1%

MANRS Readiness

Filtering	Anti-spoofing	Coordination	Global Validation IRR	Global Validation RPKI
100%	60%	89%	85%	9%
0.01% →	-0.01% →	0.10% →	0.13% →	2.67% ↗

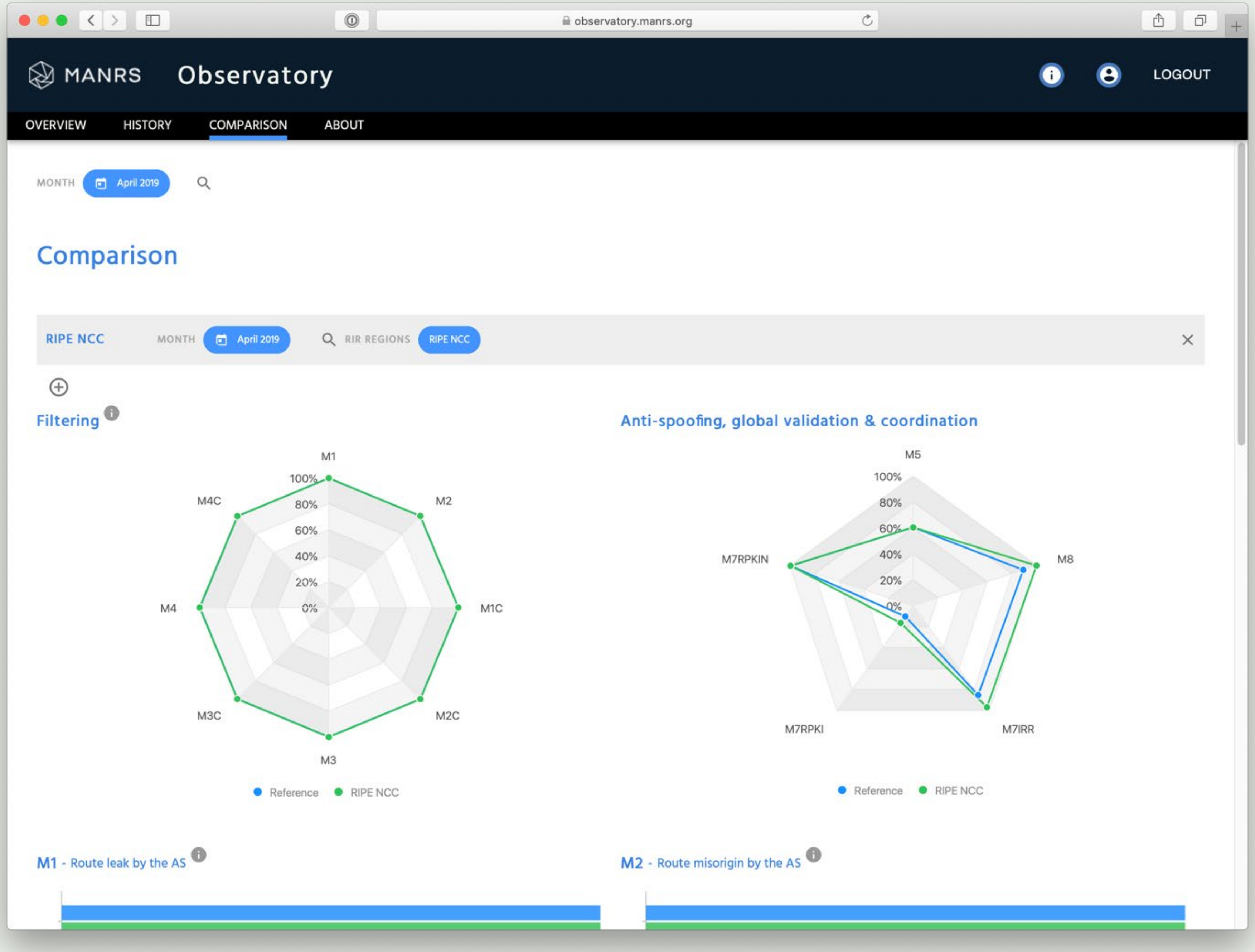


History

January 2019 - April 2019

MANRS Readiness

Absolute | Relative



observatory.manrs.org

MANRS Observatory

LOGOUT

OVERVIEW HISTORY COMPARISON ABOUT

MONTH April 2019

Comparison

RIPE NCC MONTH April 2019 RIR REGIONS RIPE NCC

Filtering

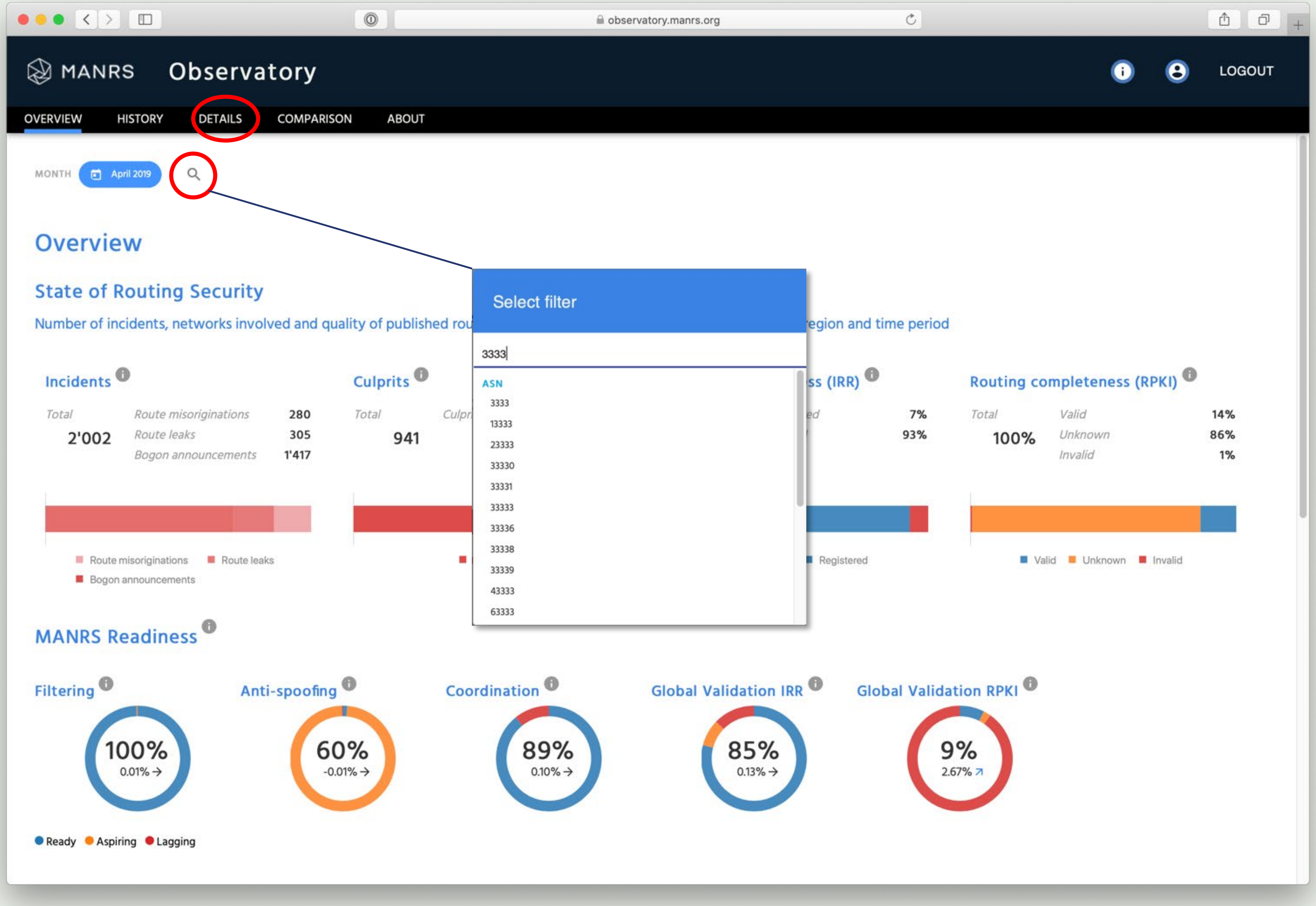
Anti-spoofing, global validation & coordination

M1 - Route leak by the AS

M2 - Route misorigin by the AS

2 views of the Observatory

Private view



Overview

State of Routing Security

Number of incidents, networks involved and quality of published rou… …egion and time period

Incidents

Total		
2'002	Route misoriginations	280
	Route leaks	305
	Bogon announcements	1'417

Culprits

Total 941

Culpr…

…ss (IRR)

…ed 7%

93%

Routing completeness (RPKI)

Total		
100%	Valid	14%
	Unknown	86%
	Invalid	1%

Select filter

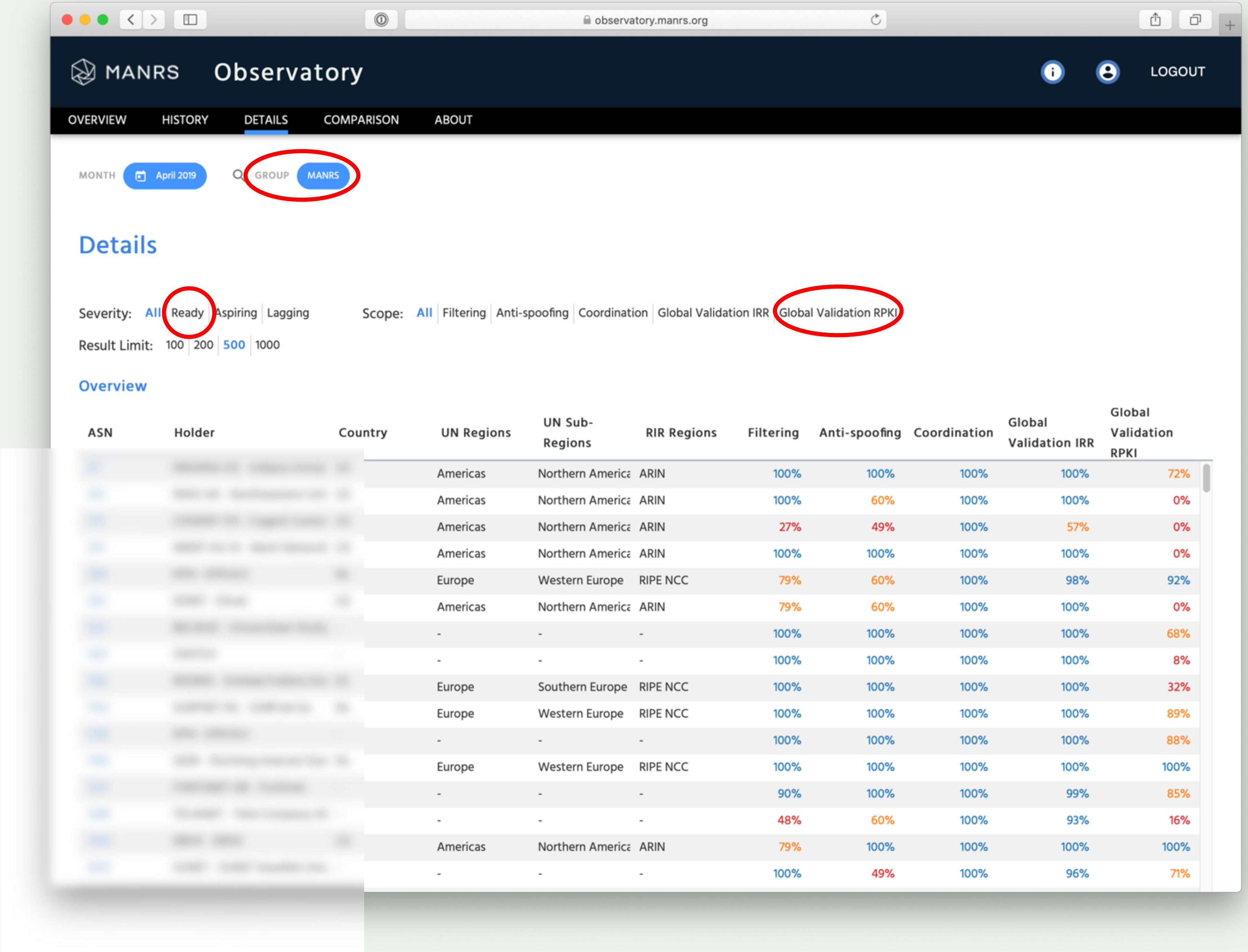
3333

ASN

3333
13333
23333
33330
33331
33333
33336
33338
33339
43333
63333

MANRS Readiness

Filtering	Anti-spoofing	Coordination	Global Validation IRR	Global Validation RPKI
100%	60%	89%	85%	9%
0.01% →	-0.01% →	0.10% →	0.13% →	2.67% ↗



MONTH April 2019 GROUP MANRS

Details

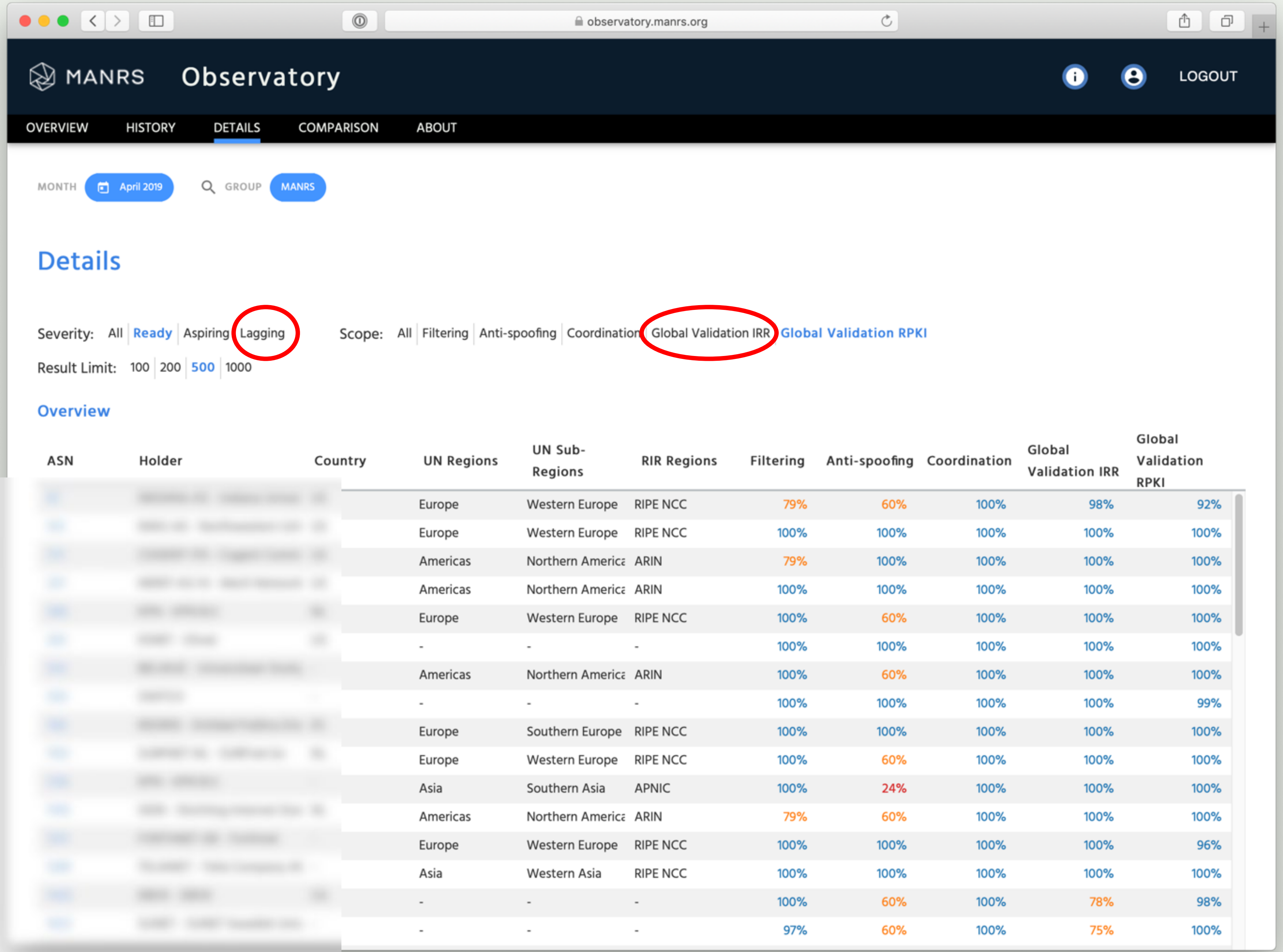
Severity: All | Ready | Aspiring | Lagging

Scope: All | Filtering | Anti-spoofing | Coordination | Global Validation IRR | Global Validation RPKI

Result Limit: 100 | 200 | 500 | 1000

Overview

ASN	Holder	Country	UN Regions	UN Sub-Regions	RIR Regions	Filtering	Anti-spoofing	Coordination	Global Validation IRR	Global Validation RPKI
[redacted]	[redacted]	[redacted]	Americas	Northern Americ	ARIN	100%	100%	100%	100%	72%
[redacted]	[redacted]	[redacted]	Americas	Northern Americ	ARIN	100%	60%	100%	100%	0%
[redacted]	[redacted]	[redacted]	Americas	Northern Americ	ARIN	27%	49%	100%	57%	0%
[redacted]	[redacted]	[redacted]	Americas	Northern Americ	ARIN	100%	100%	100%	100%	0%
[redacted]	[redacted]	[redacted]	Europe	Western Europe	RIPE NCC	79%	60%	100%	98%	92%
[redacted]	[redacted]	[redacted]	Americas	Northern Americ	ARIN	79%	60%	100%	100%	0%
[redacted]	[redacted]	[redacted]	-	-	-	100%	100%	100%	100%	68%
[redacted]	[redacted]	[redacted]	-	-	-	100%	100%	100%	100%	8%
[redacted]	[redacted]	[redacted]	Europe	Southern Europe	RIPE NCC	100%	100%	100%	100%	32%
[redacted]	[redacted]	[redacted]	Europe	Western Europe	RIPE NCC	100%	100%	100%	100%	89%
[redacted]	[redacted]	[redacted]	-	-	-	100%	100%	100%	100%	88%
[redacted]	[redacted]	[redacted]	Europe	Western Europe	RIPE NCC	100%	100%	100%	100%	100%
[redacted]	[redacted]	[redacted]	-	-	-	90%	100%	100%	99%	85%
[redacted]	[redacted]	[redacted]	-	-	-	48%	60%	100%	93%	16%
[redacted]	[redacted]	[redacted]	Americas	Northern Americ	ARIN	79%	100%	100%	100%	100%
[redacted]	[redacted]	[redacted]	-	-	-	100%	49%	100%	96%	71%



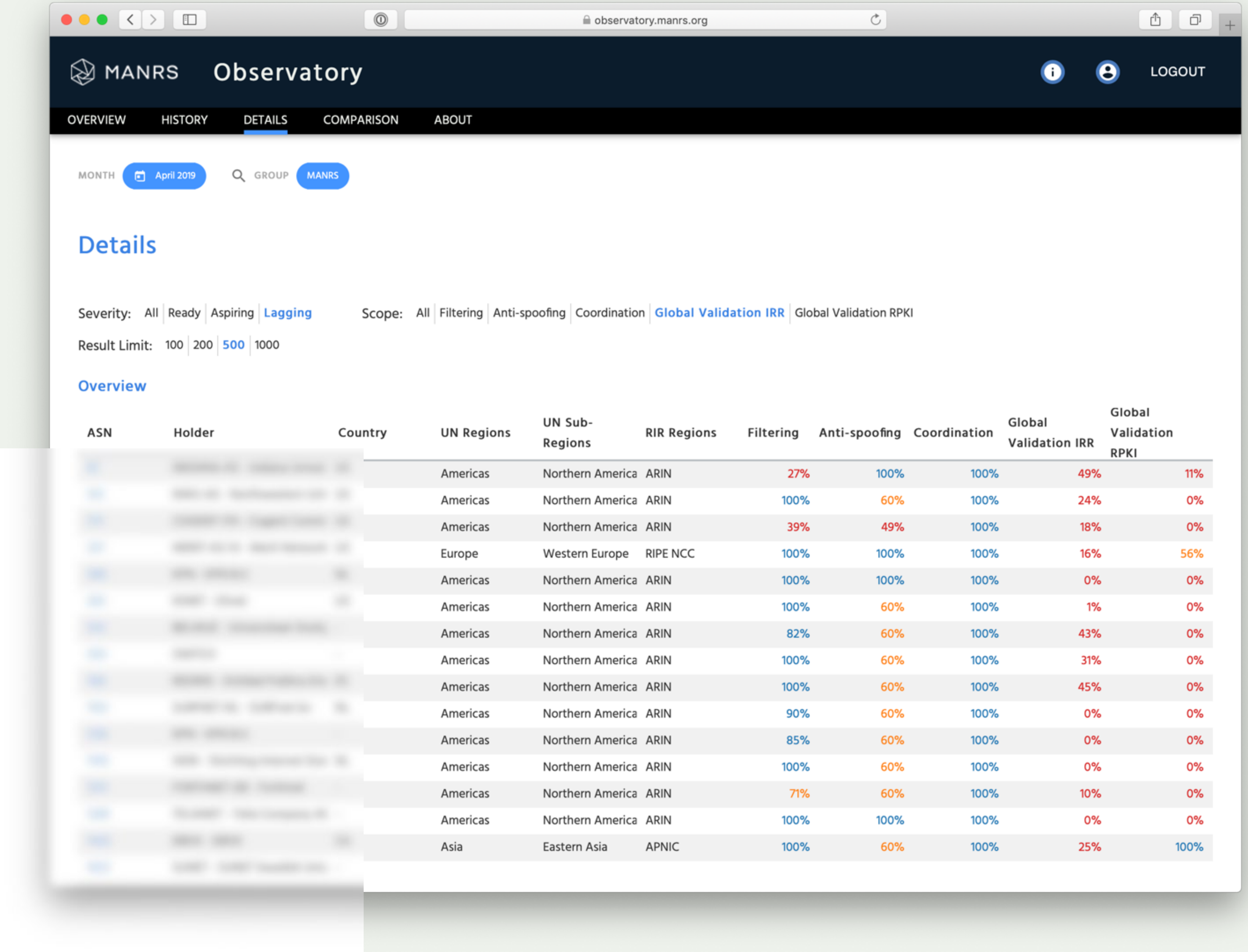
Details

Severity: All | Ready | Aspiring | Lagging Scope: All | Filtering | Anti-spoofing | Coordination | Global Validation IRR | Global Validation RPKI

Result Limit: 100 | 200 | 500 | 1000

Overview

ASN	Holder	Country	UN Regions	UN Sub-Regions	RIR Regions	Filtering	Anti-spoofing	Coordination	Global Validation IRR	Global Validation RPKI
[redacted]	[redacted]	[redacted]	Europe	Western Europe	RIPE NCC	79%	60%	100%	98%	92%
[redacted]	[redacted]	[redacted]	Europe	Western Europe	RIPE NCC	100%	100%	100%	100%	100%
[redacted]	[redacted]	[redacted]	Americas	Northern Americ	ARIN	79%	100%	100%	100%	100%
[redacted]	[redacted]	[redacted]	Americas	Northern Americ	ARIN	100%	100%	100%	100%	100%
[redacted]	[redacted]	[redacted]	Europe	Western Europe	RIPE NCC	100%	60%	100%	100%	100%
[redacted]	[redacted]	[redacted]	-	-	-	100%	100%	100%	100%	100%
[redacted]	[redacted]	[redacted]	Americas	Northern Americ	ARIN	100%	60%	100%	100%	100%
[redacted]	[redacted]	[redacted]	-	-	-	100%	100%	100%	100%	99%
[redacted]	[redacted]	[redacted]	Europe	Southern Europe	RIPE NCC	100%	100%	100%	100%	100%
[redacted]	[redacted]	[redacted]	Europe	Western Europe	RIPE NCC	100%	60%	100%	100%	100%
[redacted]	[redacted]	[redacted]	Asia	Southern Asia	APNIC	100%	24%	100%	100%	100%
[redacted]	[redacted]	[redacted]	Americas	Northern Americ	ARIN	79%	60%	100%	100%	100%
[redacted]	[redacted]	[redacted]	Europe	Western Europe	RIPE NCC	100%	100%	100%	100%	96%
[redacted]	[redacted]	[redacted]	Asia	Western Asia	RIPE NCC	100%	100%	100%	100%	100%
[redacted]	[redacted]	[redacted]	-	-	-	100%	60%	100%	78%	98%
[redacted]	[redacted]	[redacted]	-	-	-	97%	60%	100%	75%	100%



MONTH April 2019 GROUP MANRS

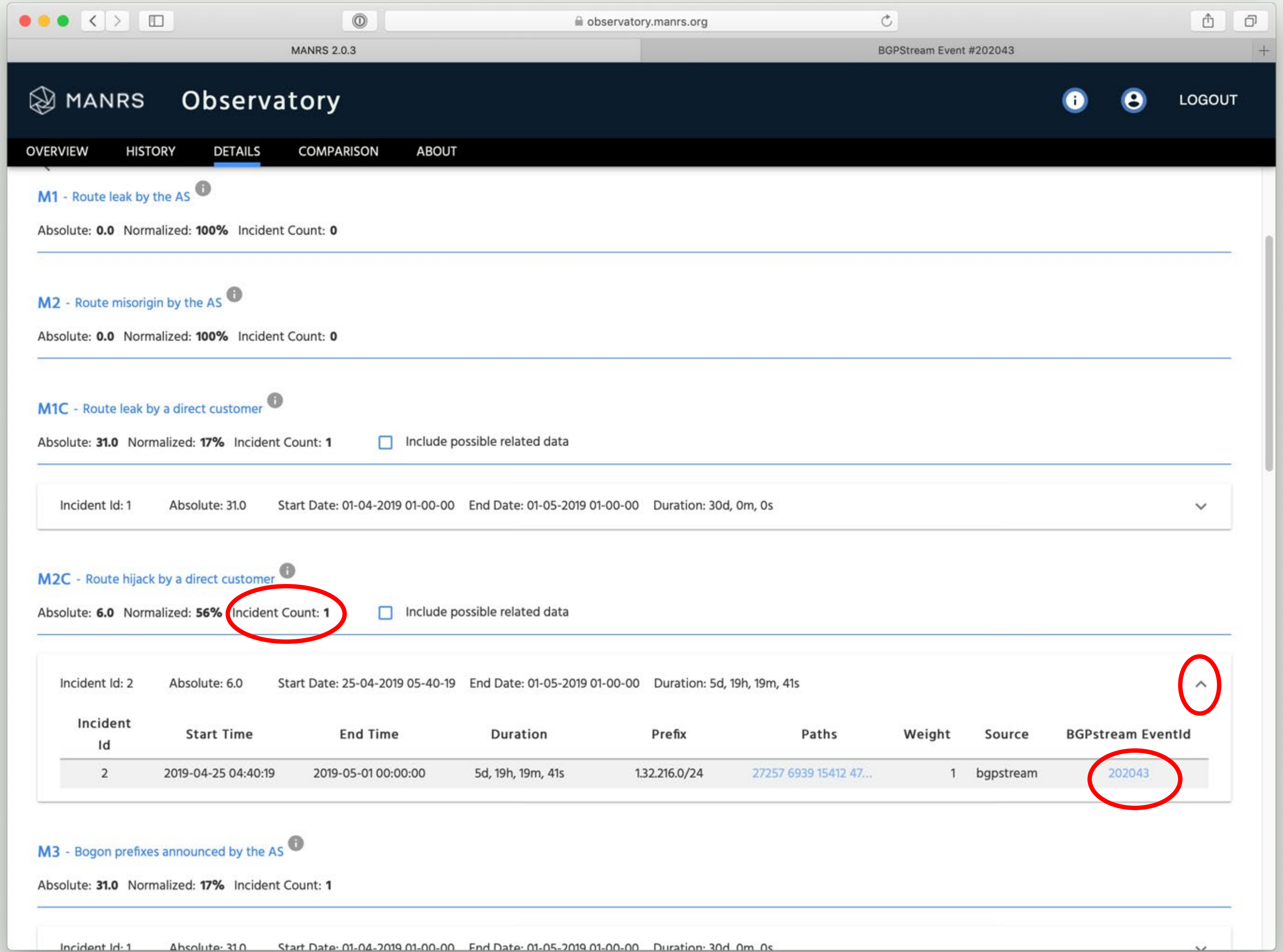
Details

Severity: All | Ready | Aspiring | **Lagging**   Scope: All | Filtering | Anti-spoofing | Coordination | **Global Validation IRR** | Global Validation RPKI

Result Limit: 100 | 200 | **500** | 1000

Overview

ASN	Holder	Country	UN Regions	UN Sub-Regions	RIR Regions	Filtering	Anti-spoofing	Coordination	Global Validation IRR	Global Validation RPKI
[redacted]	[redacted]	[redacted]	Americas	Northern America	ARIN	27%	100%	100%	49%	11%
[redacted]	[redacted]	[redacted]	Americas	Northern America	ARIN	100%	60%	100%	24%	0%
[redacted]	[redacted]	[redacted]	Americas	Northern America	ARIN	39%	49%	100%	18%	0%
[redacted]	[redacted]	[redacted]	Europe	Western Europe	RIPE NCC	100%	100%	100%	16%	56%
[redacted]	[redacted]	[redacted]	Americas	Northern America	ARIN	100%	100%	100%	0%	0%
[redacted]	[redacted]	[redacted]	Americas	Northern America	ARIN	100%	60%	100%	1%	0%
[redacted]	[redacted]	[redacted]	Americas	Northern America	ARIN	82%	60%	100%	43%	0%
[redacted]	[redacted]	[redacted]	Americas	Northern America	ARIN	100%	60%	100%	31%	0%
[redacted]	[redacted]	[redacted]	Americas	Northern America	ARIN	100%	60%	100%	45%	0%
[redacted]	[redacted]	[redacted]	Americas	Northern America	ARIN	90%	60%	100%	0%	0%
[redacted]	[redacted]	[redacted]	Americas	Northern America	ARIN	85%	60%	100%	0%	0%
[redacted]	[redacted]	[redacted]	Americas	Northern America	ARIN	100%	60%	100%	0%	0%
[redacted]	[redacted]	[redacted]	Americas	Northern America	ARIN	71%	60%	100%	10%	0%
[redacted]	[redacted]	[redacted]	Americas	Northern America	ARIN	100%	100%	100%	0%	0%
[redacted]	[redacted]	[redacted]	Asia	Eastern Asia	APNIC	100%	60%	100%	25%	100%
[redacted]	[redacted]	[redacted]								



M1 - Route leak by the AS

Absolute: **0.0** Normalized: **100%** Incident Count: **0**

M2 - Route misorigin by the AS

Absolute: **0.0** Normalized: **100%** Incident Count: **0**

M1C - Route leak by a direct customer

Absolute: **31.0** Normalized: **17%** Incident Count: **1** □ Include possible related data

Incident Id: 1 Absolute: 31.0 Start Date: 01-04-2019 01-00-00 End Date: 01-05-2019 01-00-00 Duration: 30d, 0m, 0s

M2C - Route hijack by a direct customer

Absolute: **6.0** Normalized: **56%** Incident Count: **1** □ Include possible related data

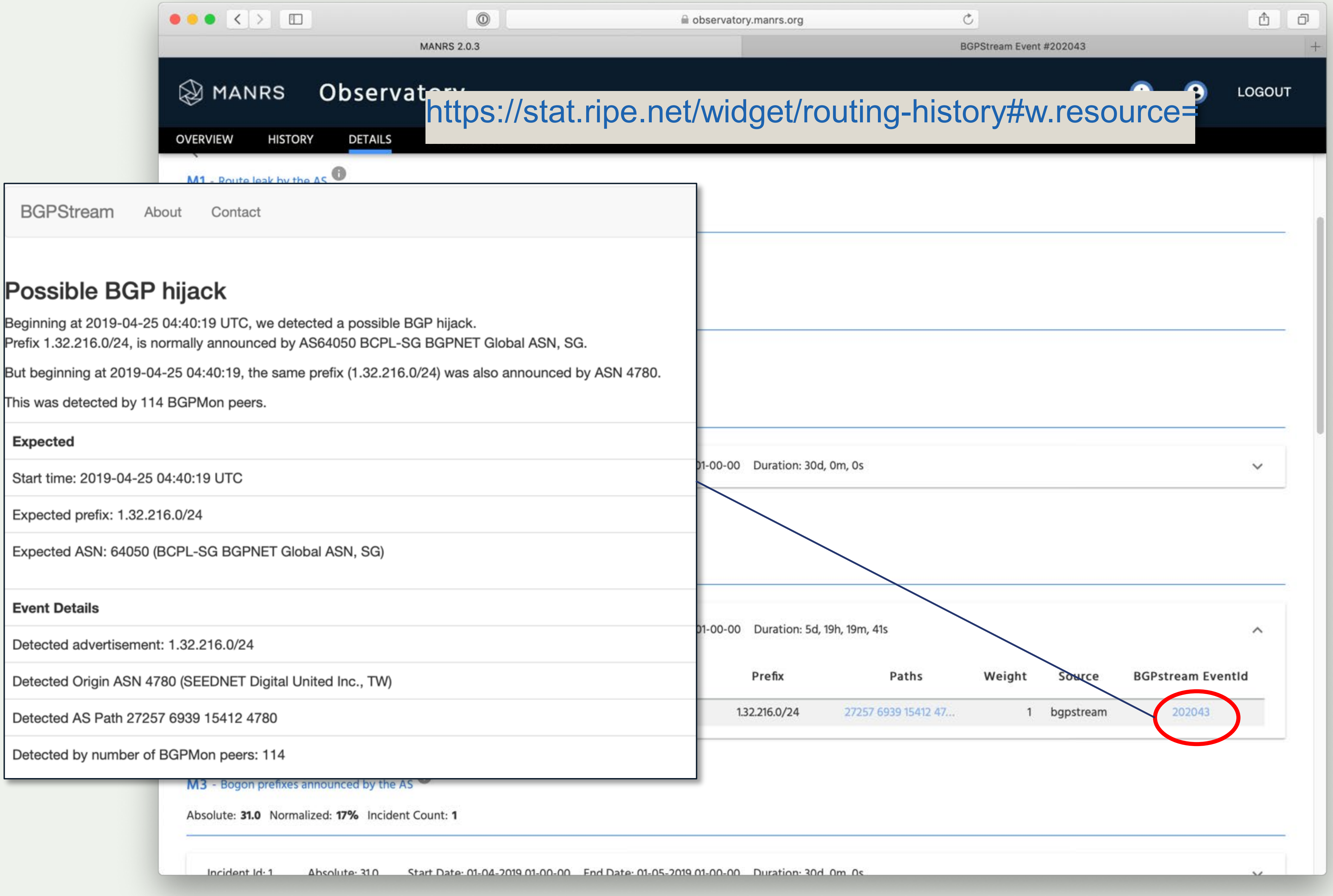
Incident Id: 2 Absolute: 6.0 Start Date: 25-04-2019 05-40-19 End Date: 01-05-2019 01-00-00 Duration: 5d, 19h, 19m, 41s

Incident Id	Start Time	End Time	Duration	Prefix	Paths	Weight	Source	BGPstream EventId
2	2019-04-25 04:40:19	2019-05-01 00:00:00	5d, 19h, 19m, 41s	1.32.216.0/24	27257 6939 15412 47...	1	bgpstream	202043

M3 - Bogon prefixes announced by the AS

Absolute: **31.0** Normalized: **17%** Incident Count: **1**

Incident Id: 1 Absolute: 31.0 Start Date: 01-04-2019 01-00-00 End Date: 01-05-2019 01-00-00 Duration: 30d, 0m, 0s



https://stat.ripe.net/widget/routing-history#w.resource=

Possible BGP hijack

Beginning at 2019-04-25 04:40:19 UTC, we detected a possible BGP hijack.
Prefix 1.32.216.0/24, is normally announced by AS64050 BCPL-SG BGPNET Global ASN, SG.

But beginning at 2019-04-25 04:40:19, the same prefix (1.32.216.0/24) was also announced by ASN 4780.

This was detected by 114 BGPMon peers.

Expected

Start time: 2019-04-25 04:40:19 UTC

Expected prefix: 1.32.216.0/24

Expected ASN: 64050 (BCPL-SG BGPNET Global ASN, SG)

Event Details

Detected advertisement: 1.32.216.0/24

Detected Origin ASN 4780 (SEEDNET Digital United Inc., TW)

Detected AS Path 27257 6939 15412 4780

Detected by number of BGPMon peers: 114

01-00-00 Duration: 30d, 0m, 0s

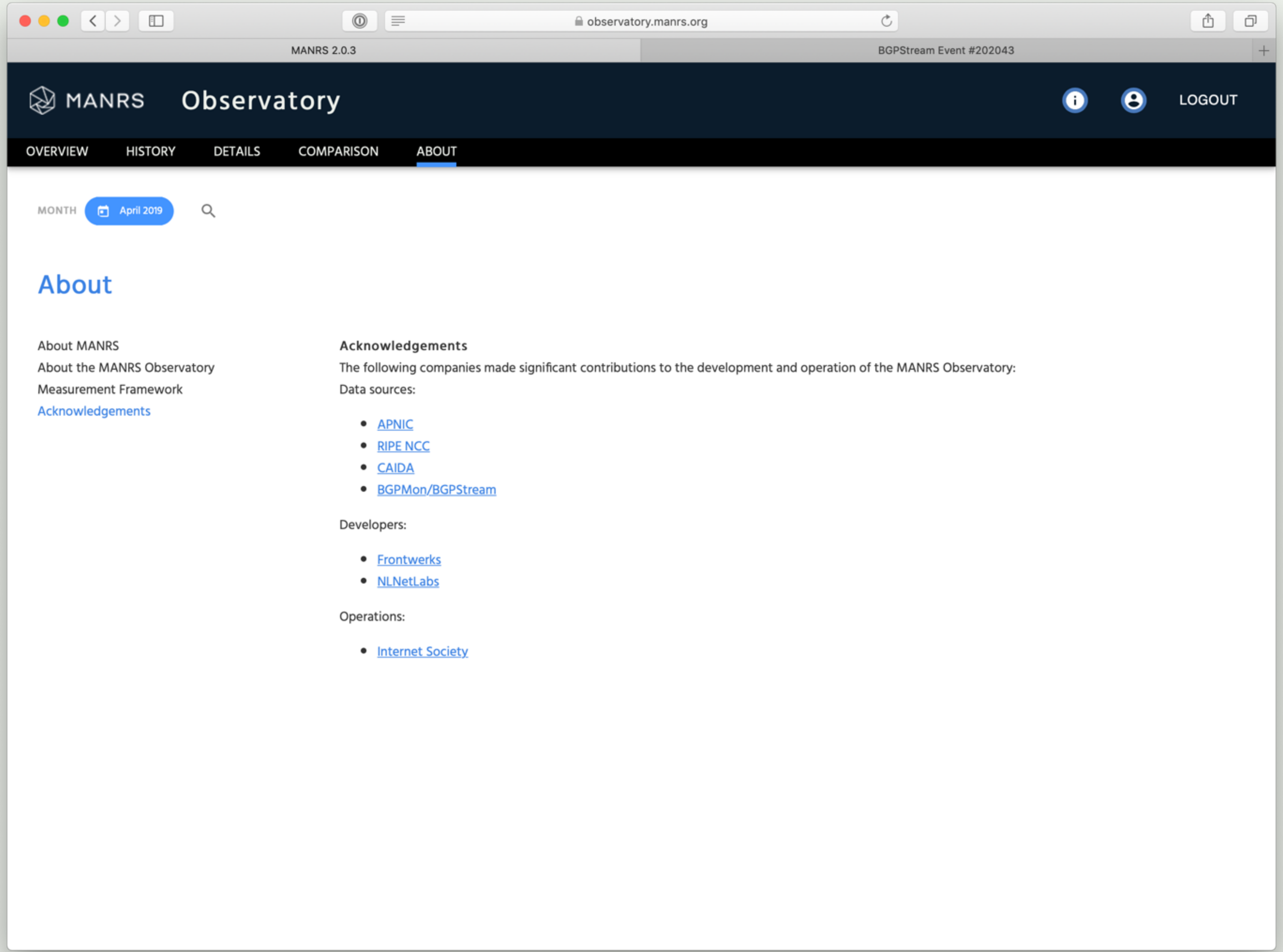
01-00-00 Duration: 5d, 19h, 19m, 41s

Prefix	Paths	Weight	Source	BGPstream EventId
1.32.216.0/24	27257 6939 15412 47...	1	bgpstream	202043

M3 - Bogon prefixes announced by the AS

Absolute: **31.0** Normalized: **17%** Incident Count: **1**

Incident Id: 1 Absolute: 31.0 Start Date: 01-04-2019 01-00-00 End Date: 01-05-2019 01-00-00 Duration: 30d, 0m, 0s



About

- About MANRS
- About the MANRS Observatory
- Measurement Framework
- Acknowledgements

Acknowledgements

The following companies made significant contributions to the development and operation of the MANRS Observatory:

Data sources:

- APNIC
- RIPE NCC
- CAIDA
- BGPMon/BGPStream

Developers:

- Frontwerks
- NLNetLabs

Operations:

- Internet Society

Why join MANRS?

- Improve your security posture and reduce the number and impact of routing incidents
- Demonstrate that these practices are reality
- Join a community of security-minded operators working together to make the Internet better
- Use MANRS as a competitive differentiator

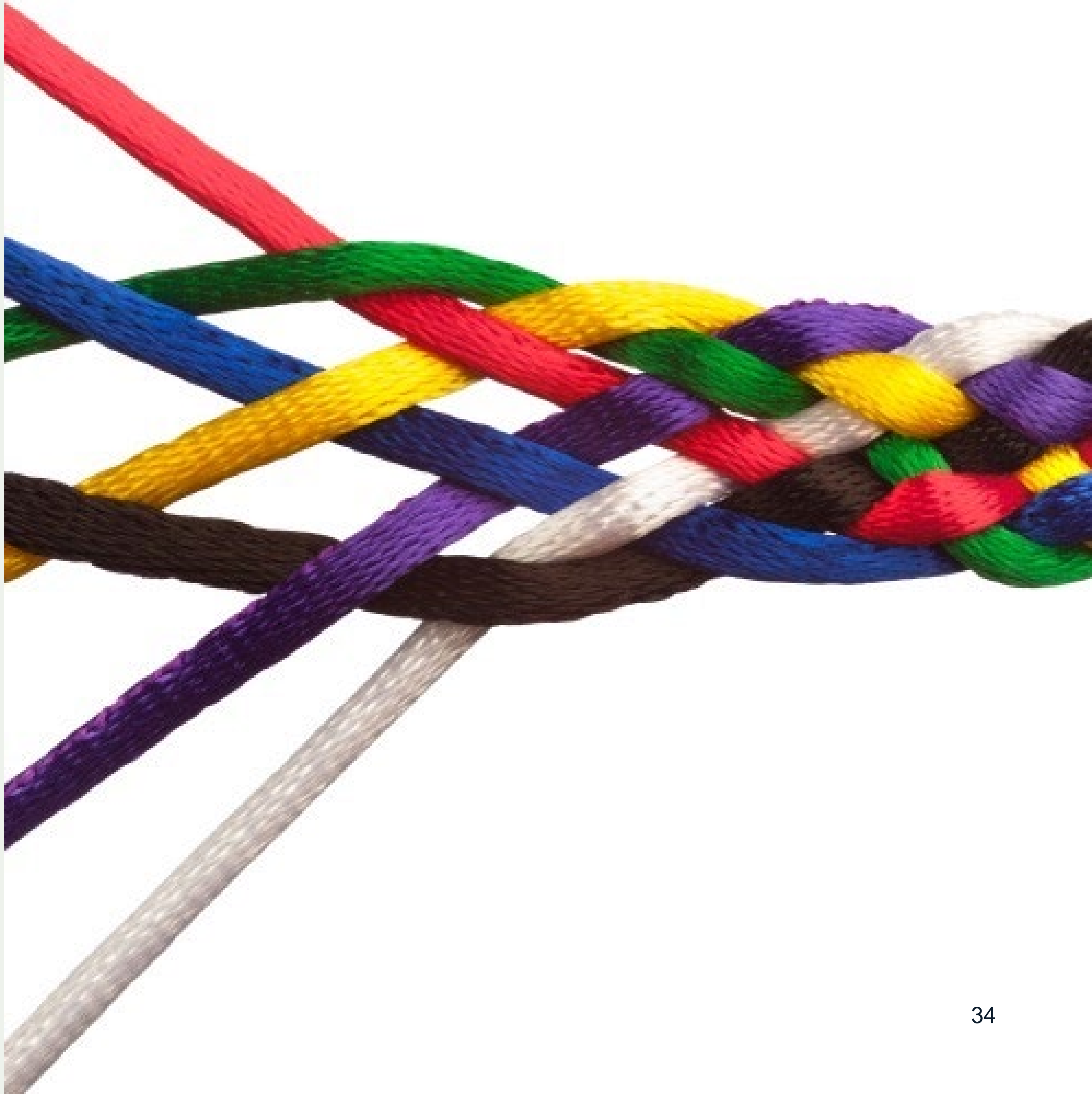
Join MANRS

Visit https://www.manrs.org

- Fill out the sign up form with as much detail as possible.
- We may ask questions and request tests

Get Involved in the Community

- Participants support the initiative and implement the actions in their own networks and encouraging MANRS adoption
- Participants are engaged in substantive activities – developing MANRS requirements and guidance, assisting with capacity and awareness building activities



MANRS

manrs.org

#ProtectTheCore

MANRS Observatory:

https://observatory.manrs.org

SIMON SOHEL BAROI

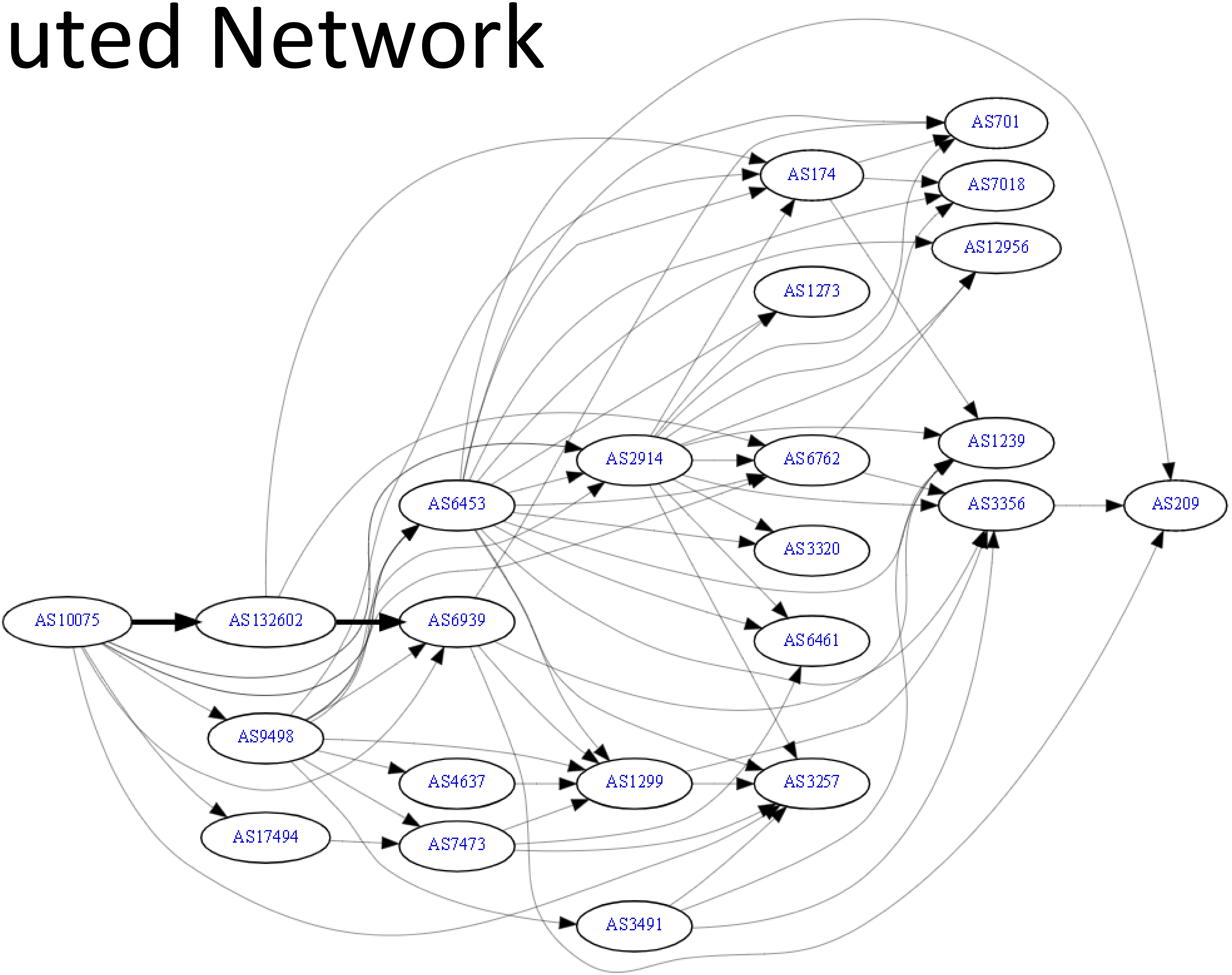
Fiber@Home Global Limited.

GFCE Triple-I Day @INSIG2019

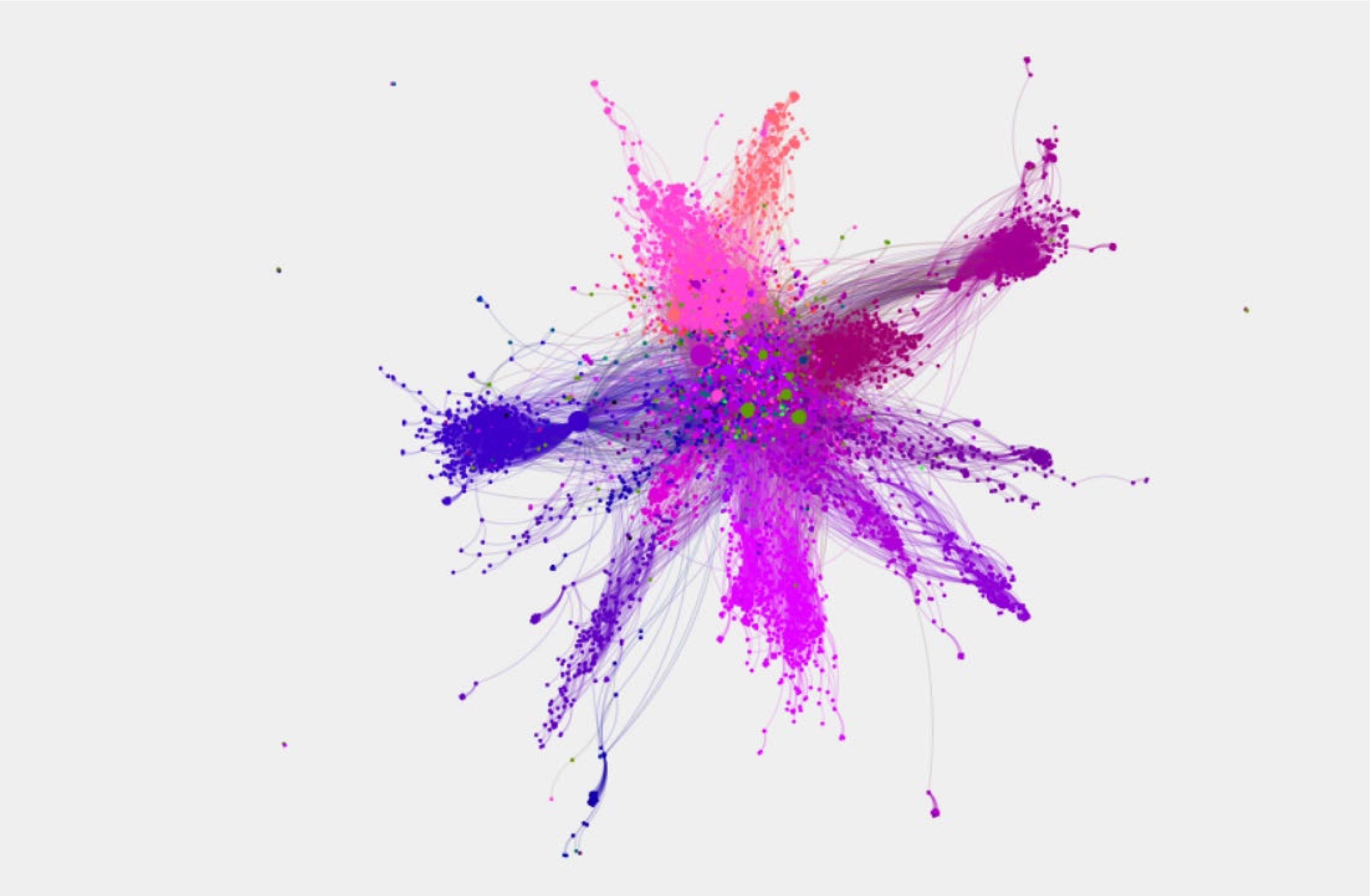
Thursday 14 November, 2019

Kolkata, India

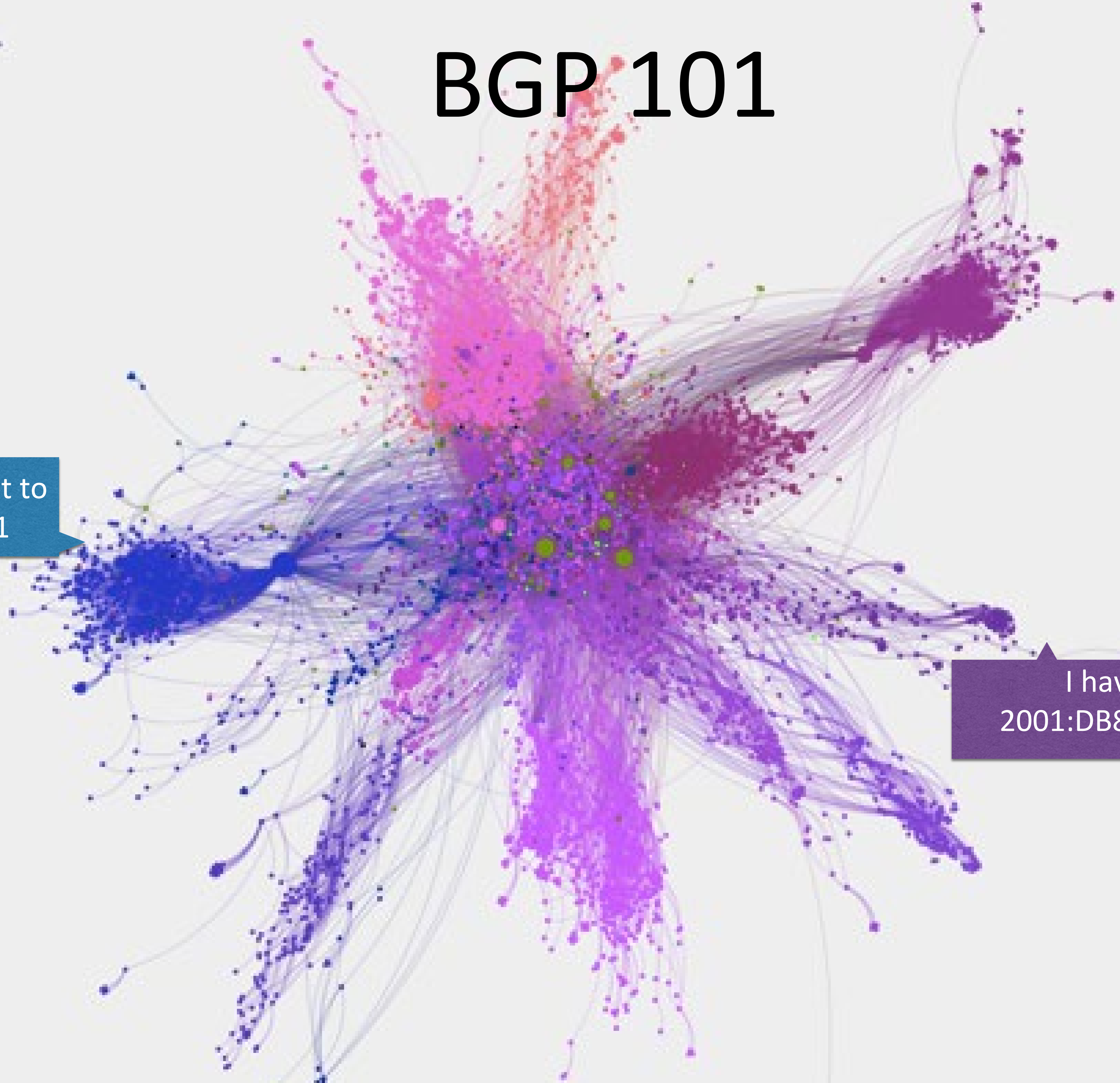
Routed Network



Routed Network



BGP 101

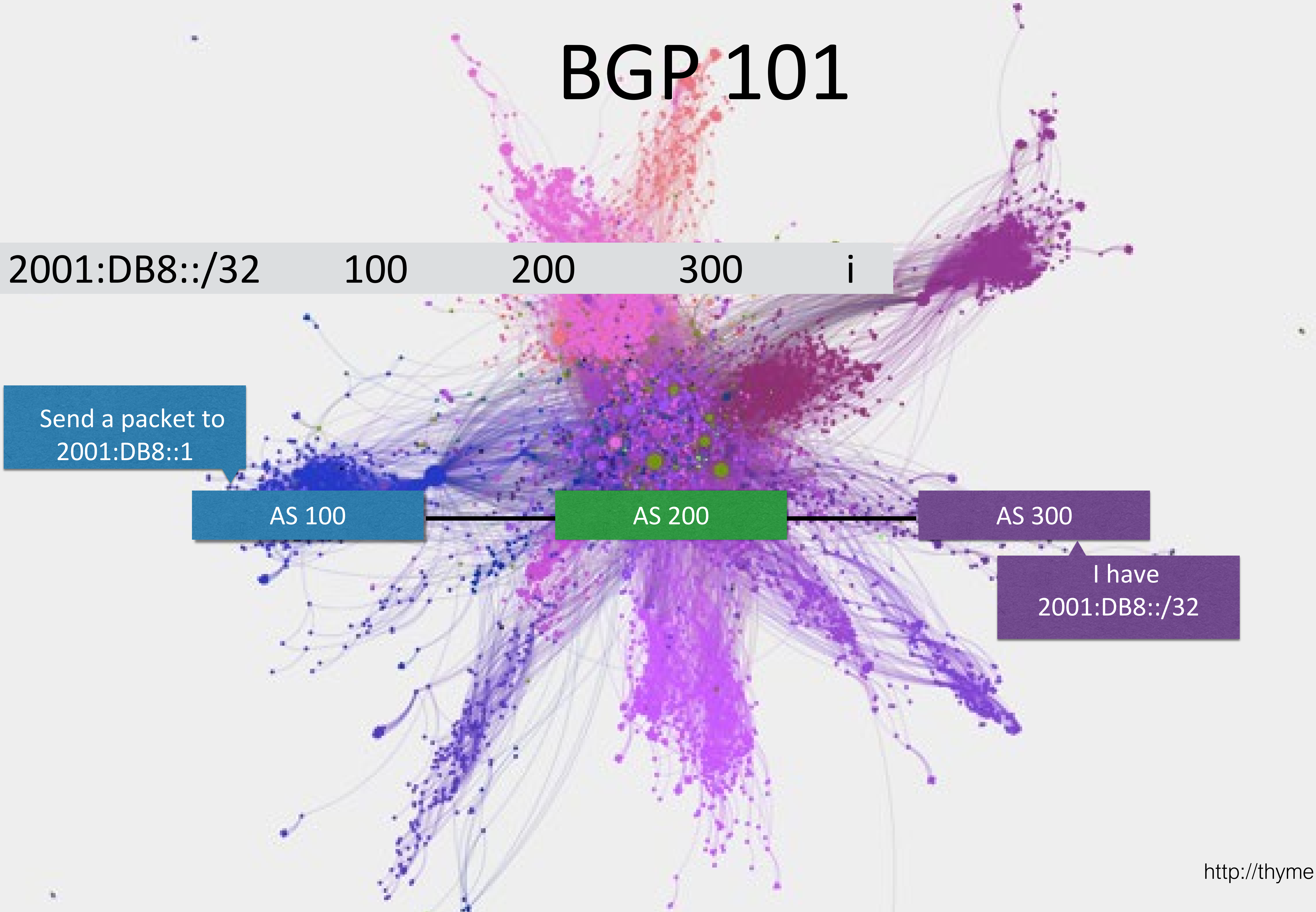


Send a packet to
2001:DB8::1

I have
2001:DB8::/32

http://thyme.apnic.net/network/

BGP 101



2001:DB8::/32 100 200 300 i

Send a packet to 2001:DB8::1

AS 100

AS 200

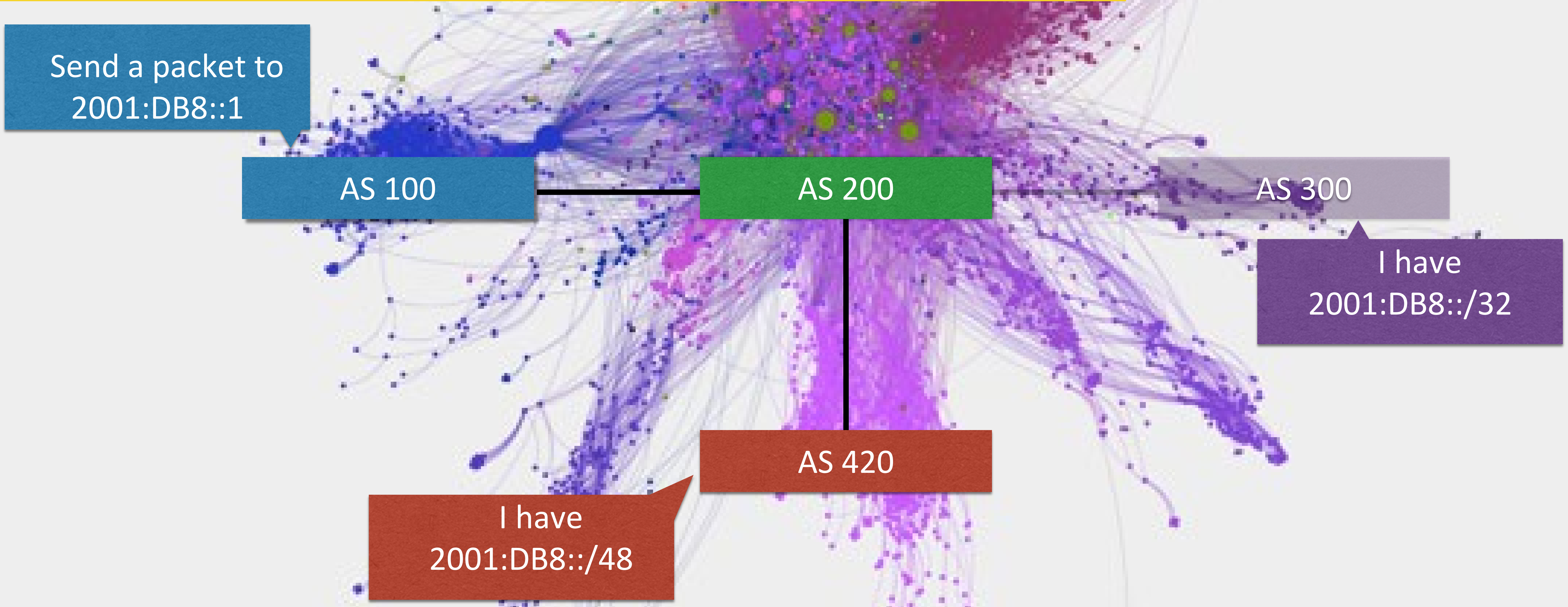
AS 300

I have 2001:DB8::/32

http://thyme.apnic.net/network/

BGP 101

2001:DB8::/32	100	200	300	i
2001:DB8::/48	100	200	420	i



http://thyme.apnic.net/network/

Caveats in Current Trends

- Filtering limited to the edges facing the customer

- Filters on peering and transit sessions are often too complex or take too many resources

- Check prefix before announcing it

- RPSL to automate it

What is RPKI ?

- A robust security framework for verifying the association between **resource holders** and **their Internet resources**
- Uses x.509 certificates with RFC3779 extensions
- Collaborative effort by all RIRs to help secure Internet routing by validating routes

RFC 6810 / 6480 / 6481 / 6491 / 6493 / 6487

RPKI

Resource Public Key Infrastructure

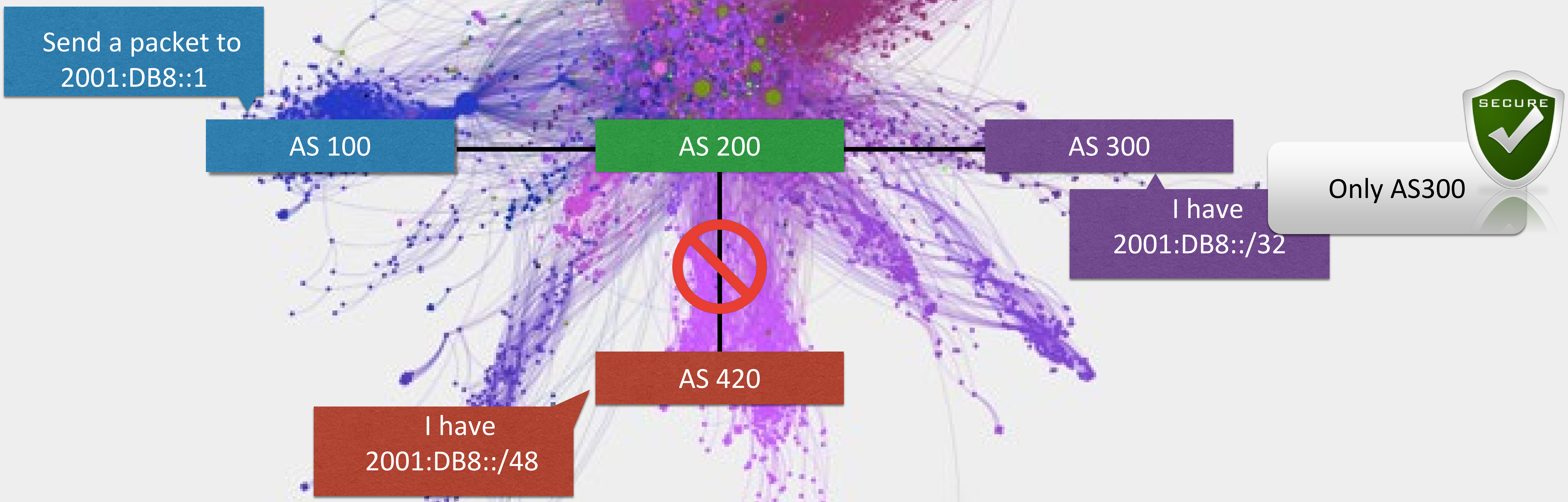
IP Address & AS Numbers

Digital Certificate

public key infrastructure framework designed to secure the Internet's routing infrastructure

RPKI Origin Validation

2001:DB8::/32	100	200	300	i	Valid
2001:DB8::/48	100	200	420	i	Invalid / unknown



Send a packet to 2001:DB8::1

AS 100

AS 200

AS 300

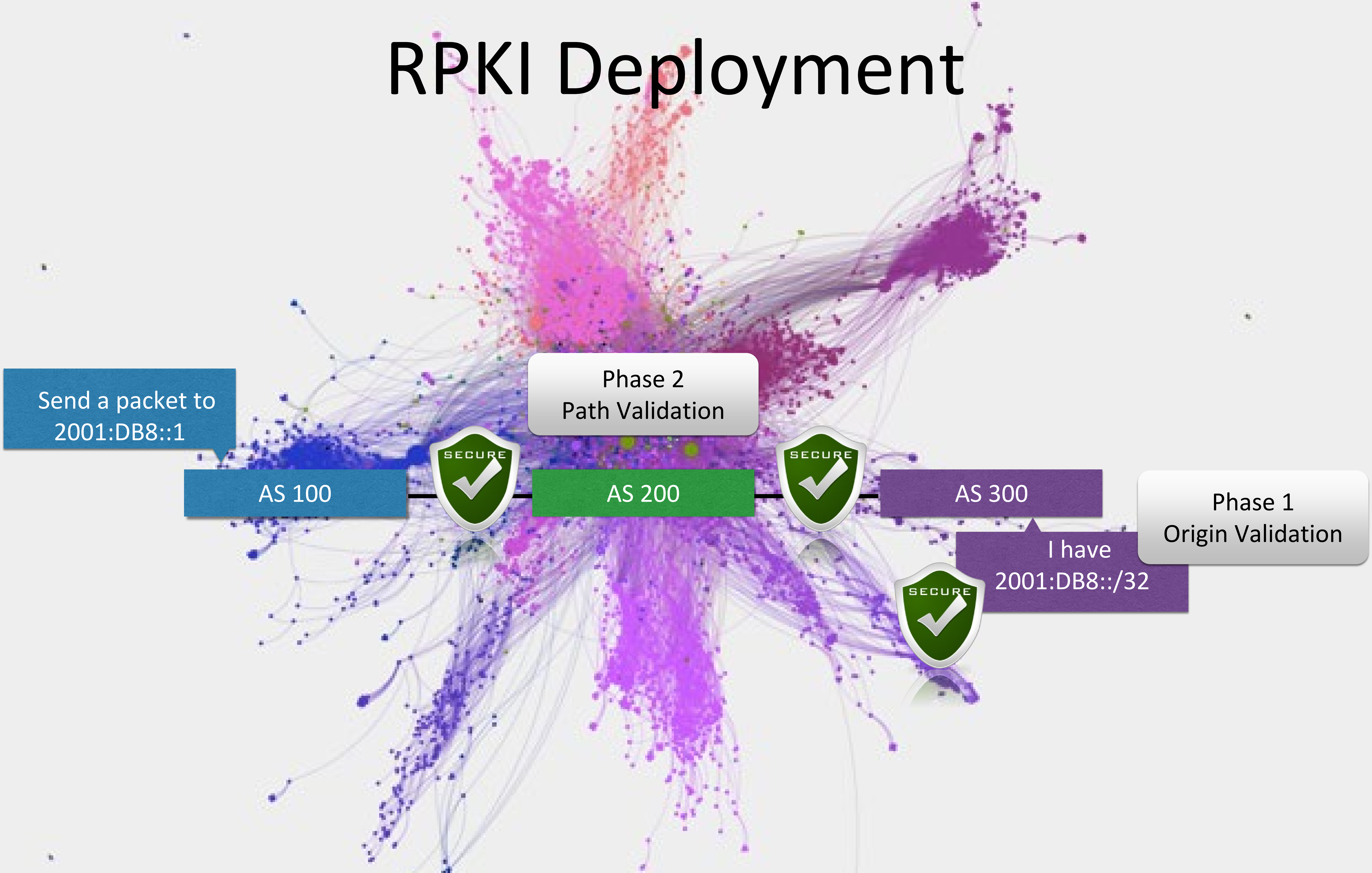
AS 420

I have 2001:DB8::/32

Only AS300

I have 2001:DB8::/48

RPKI Deployment



Send a packet to 2001:DB8::1

Phase 2
Path Validation

AS 100

AS 200

AS 300

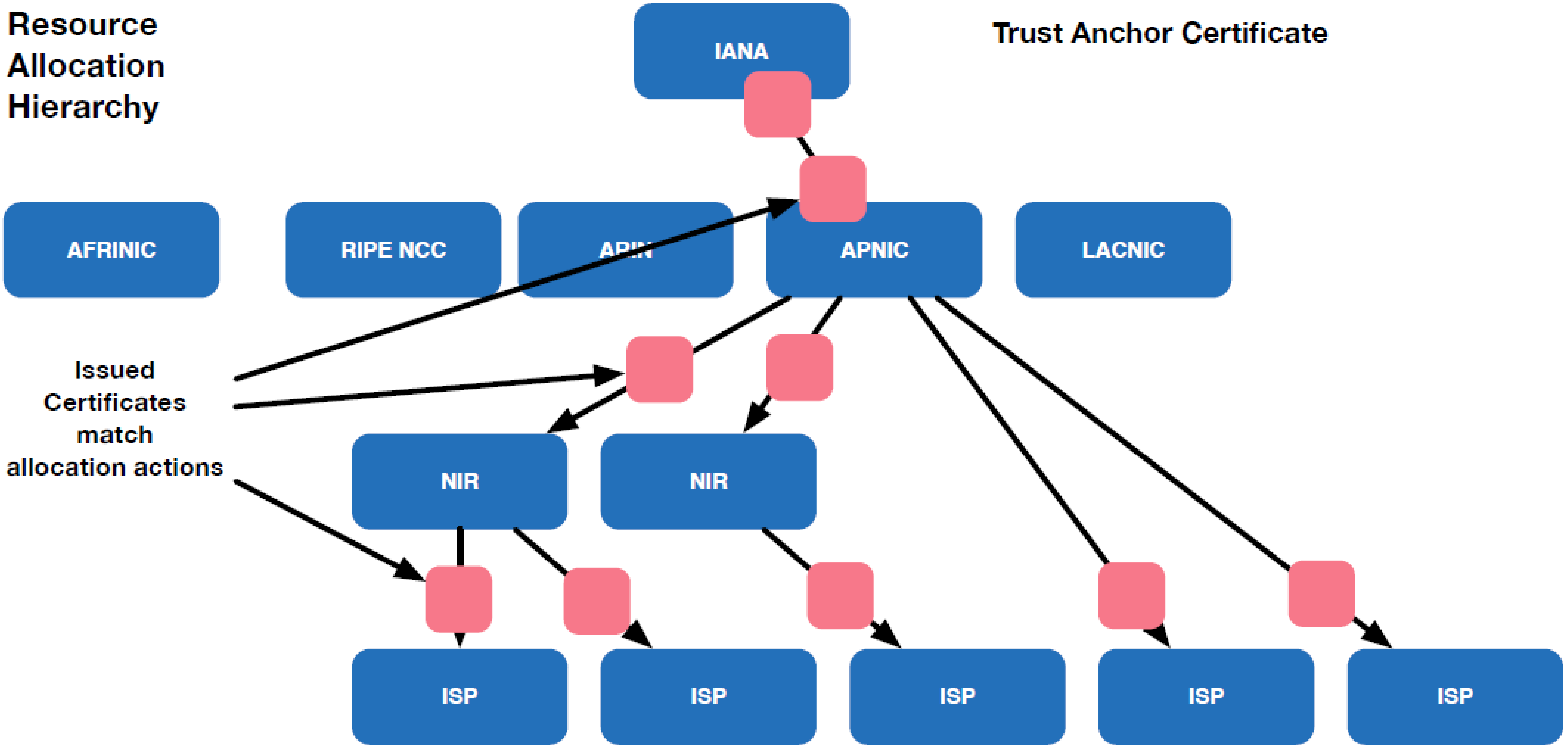
I have 2001:DB8::/32

Phase 1
Origin Validation

RPKI Building Blocks

1. Trust Anchors (RIR’s)
2. Route Origination Authorizations (ROA)
3. Validators

Trust Anchors (RIR's)



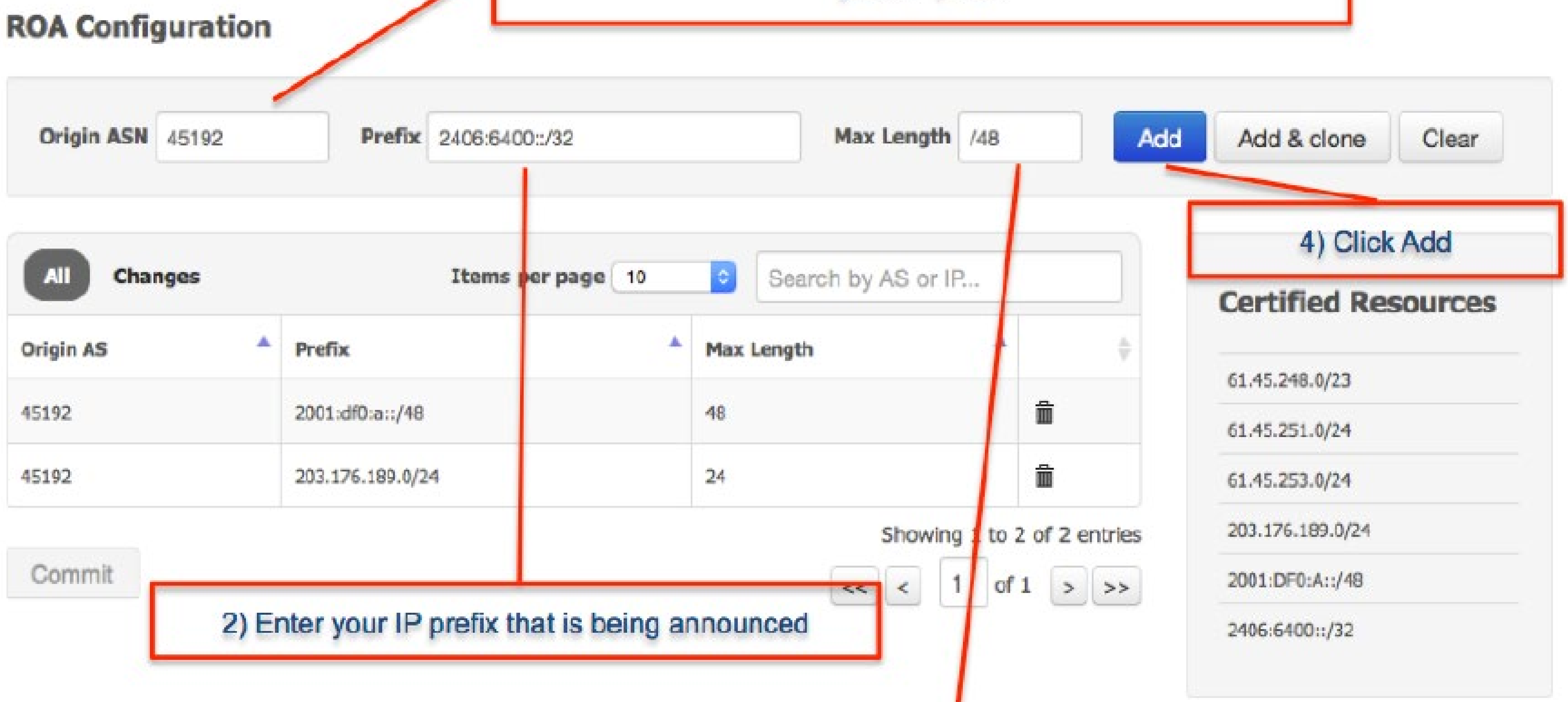
Route Origination Authorizations (ROA)

What’s contained in a ROA

- The AS number you have authorized
- The prefix that is being originated from it
- The most specific prefix (maximum length) that the AS may announce

*For example: “**AS58587** originates a route for the prefix **2001:DB8::/32** with a maximum prefix length of **/40)**”*

Creating ROA



ROA Configuration

Origin ASN: 45192 | Prefix: 2406:6400::/32 | Max Length: /48

Items per page: 10

Search by AS or IP...

Origin AS	Prefix	Max Length	
45192	2001:df0:a::/48	48	🗑
45192	203.176.189.0/24	24	🗑

Showing 1 to 2 of 2 entries

Certified Resources

61.45.248.0/23
61.45.251.0/24
61.45.253.0/24
203.176.189.0/24
2001:DF0:A::/48
2406:6400::/32

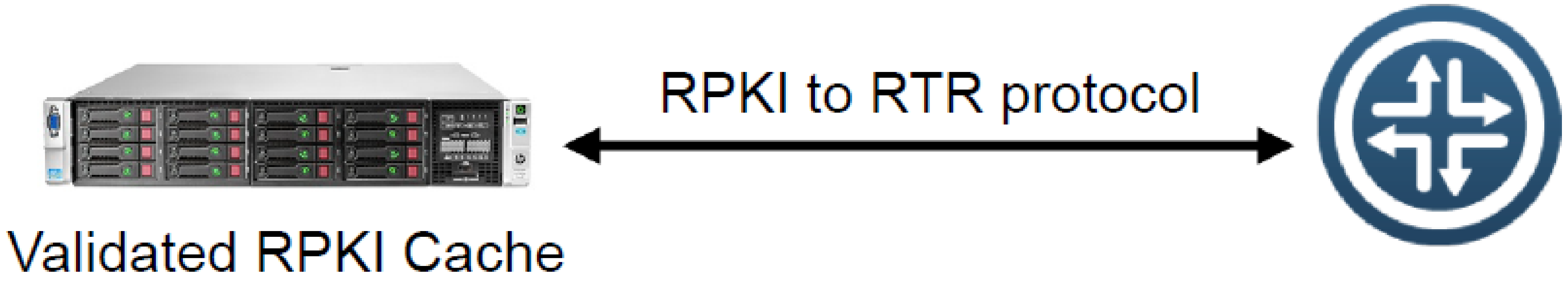
1) Enter the Origin ASN you authorize to announce routes for your IP prefix

2) Enter your IP prefix that is being announced

3) Enter the Max Length of prefix that you authorize for this ROA

4) Click Add

Validator Integration



RPKI to RTR protocol

Validated RPKI Cache

The BGP Process will check each announcement with ROA information and label the prefix.

Invalid

Unknown

Valid

Prefix: 10.0.0.0/16
ASN: 65420

ROA	65420	10.0.0.0/16	/18
	Origin AS	**Prefix**	**Max Length**
VALID	AS65420	10.0.0.0/16	
VALID	AS65420	10.0.128.0/17	
INVALID	AS65421	10.0.0.0/16	
INVALID	AS65420	10.0.10.0/24	
UNKNOWN	AS65430	10.0.0.0/8	

Now What ?

Take Action

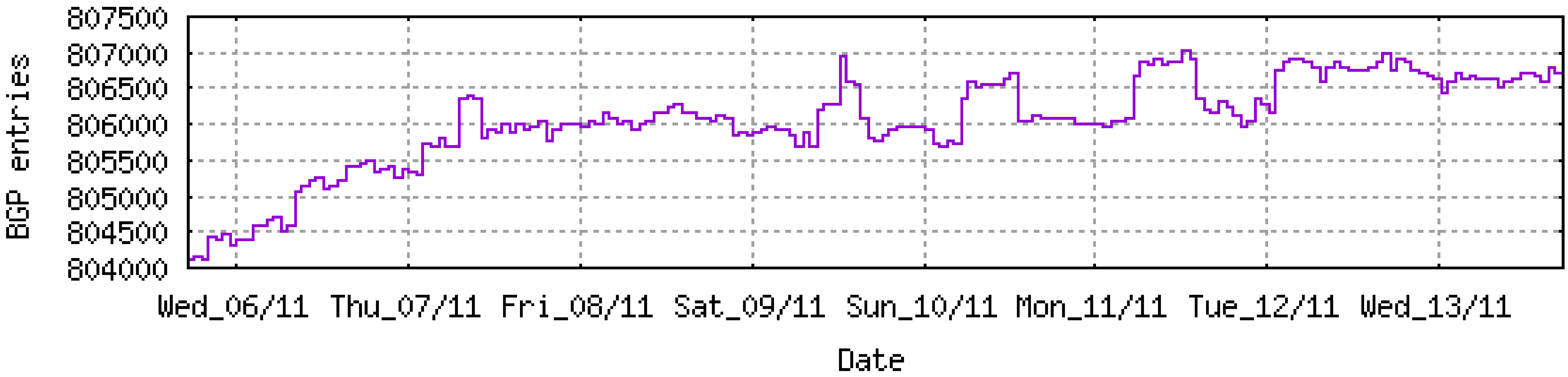
Invalid

Unknown

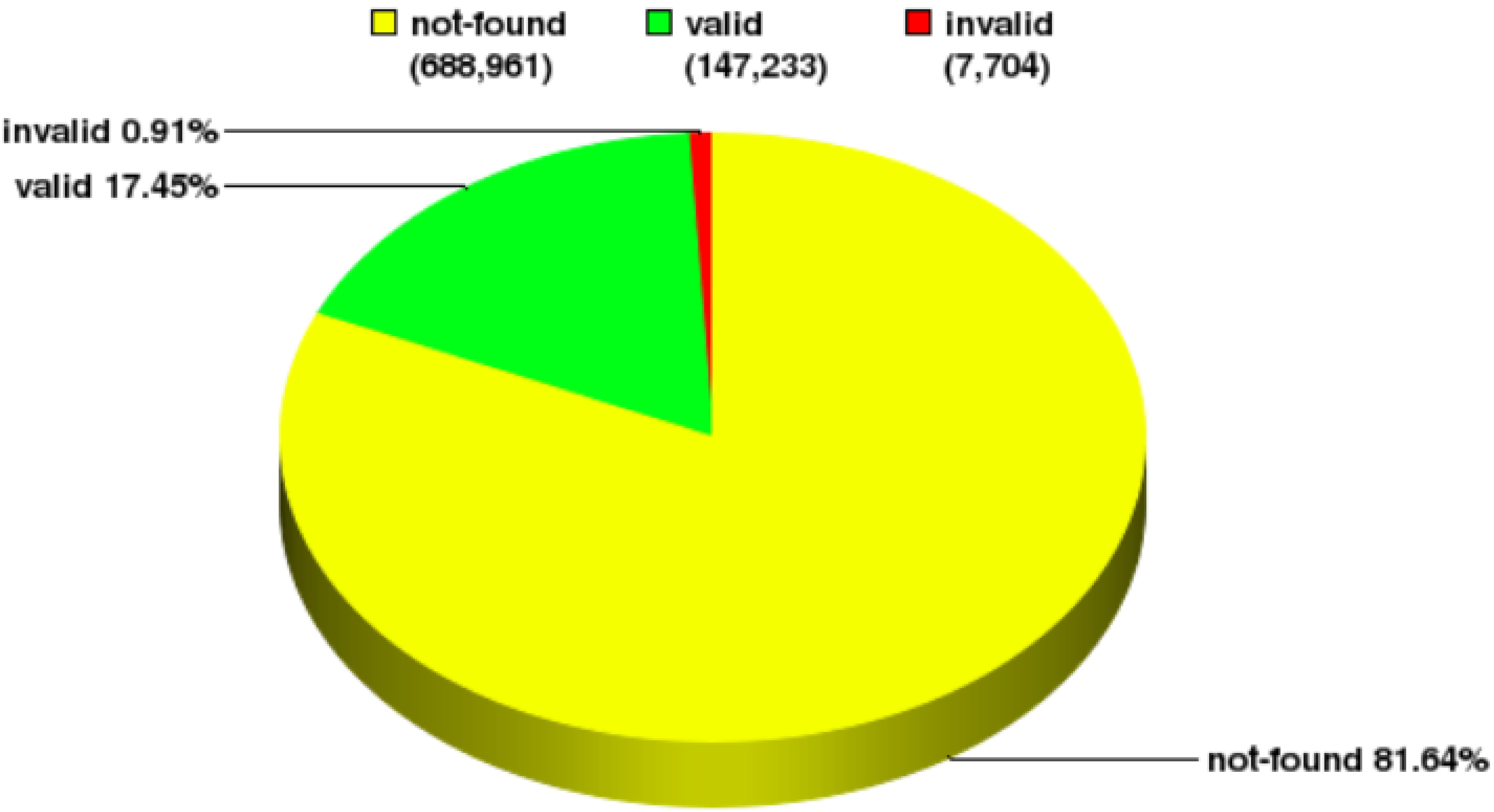
Valid

- Do Nothing
- Just Log it
- Play with BGP Community
- Modify the Preference Value
- Reject the announcement

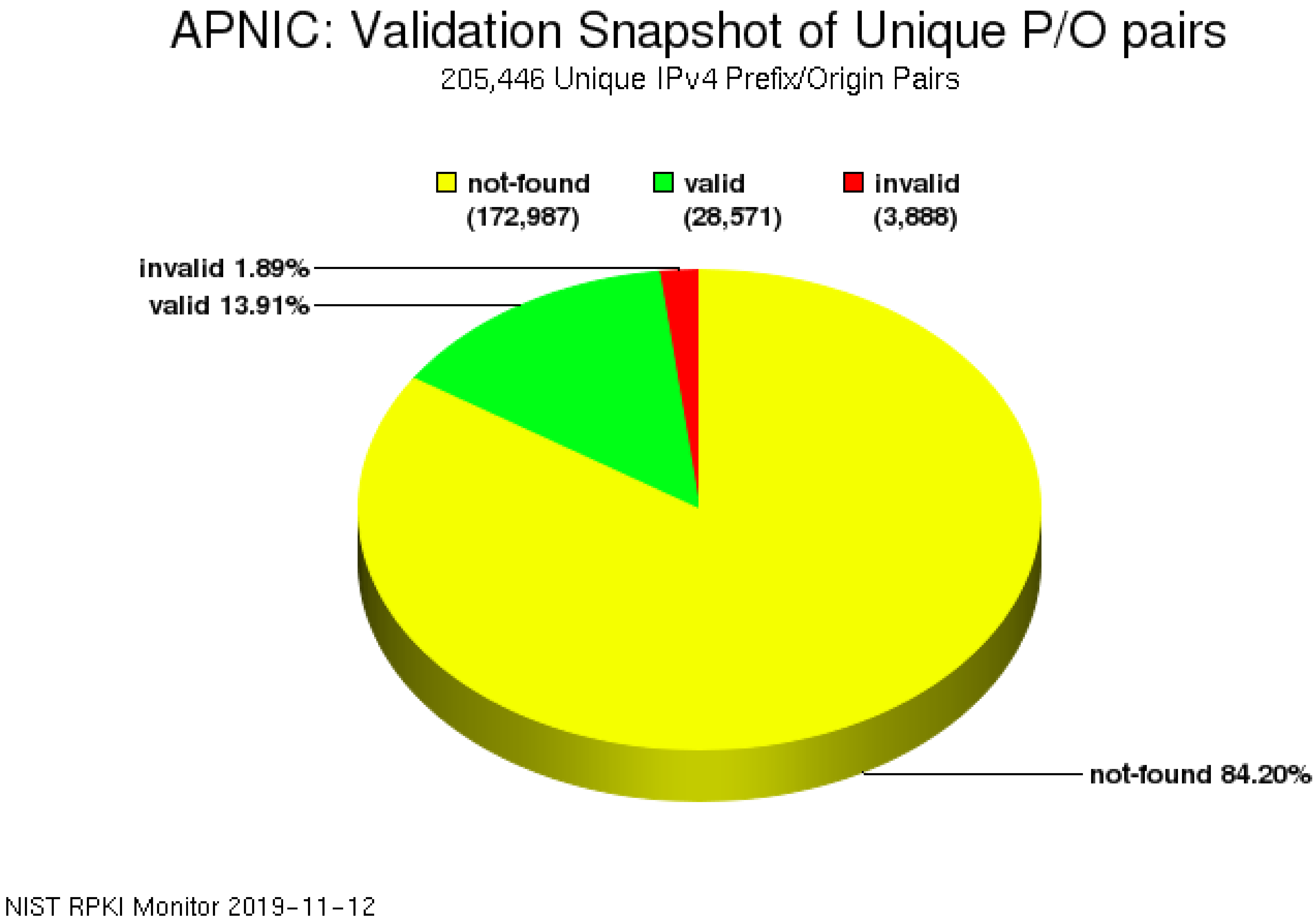
RPKI adoption rate / deployment status



https://www.cidr-report.org/as2.0/



https://rpki-monitor.antd.nist.gov/



APNIC: Validation Snapshot of Unique P/O pairs

205,446 Unique IPv4 Prefix/Origin Pairs

NIST RPKI Monitor 2019-11-12

https://rpki-monitor.antd.nist.gov/?p=3&s=0

Some Activity in APNIC Region :

- ❑ ROA Signing Ceremony
- ❑ Routing Security/RPKI/* SIG
- ❑ prop-132: RPKI ROAs for unallocated and unassigned APNIC address space (was: AS0 for Bogons)

Special thanks to

Fakrul Alam, Dimension Data
Aftab Siddiqui, ISOC
Zobair Khan, Fiber@Home
Vivek Nigam, APNIC
Anupam Agrawal, ISOC Kolkata

ধন্যবাদ

SIMON SOHEL BAROI
Fiber@Home Global Limited.
simon.baroi@fiberathome.net