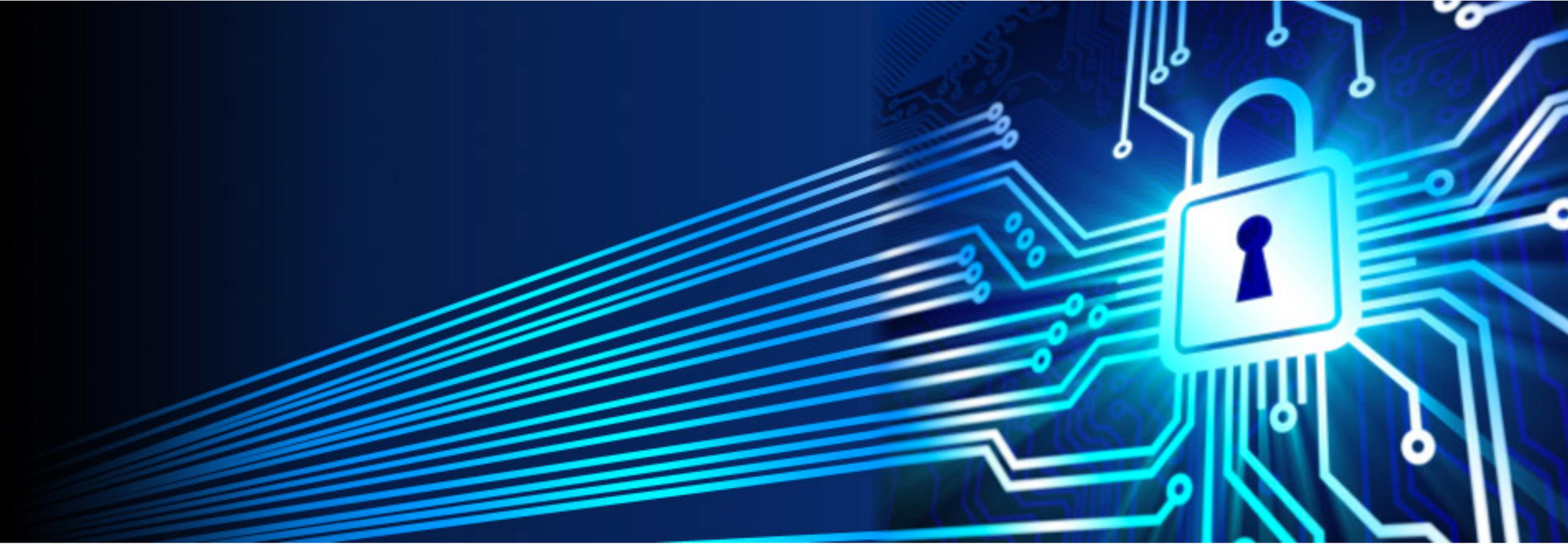
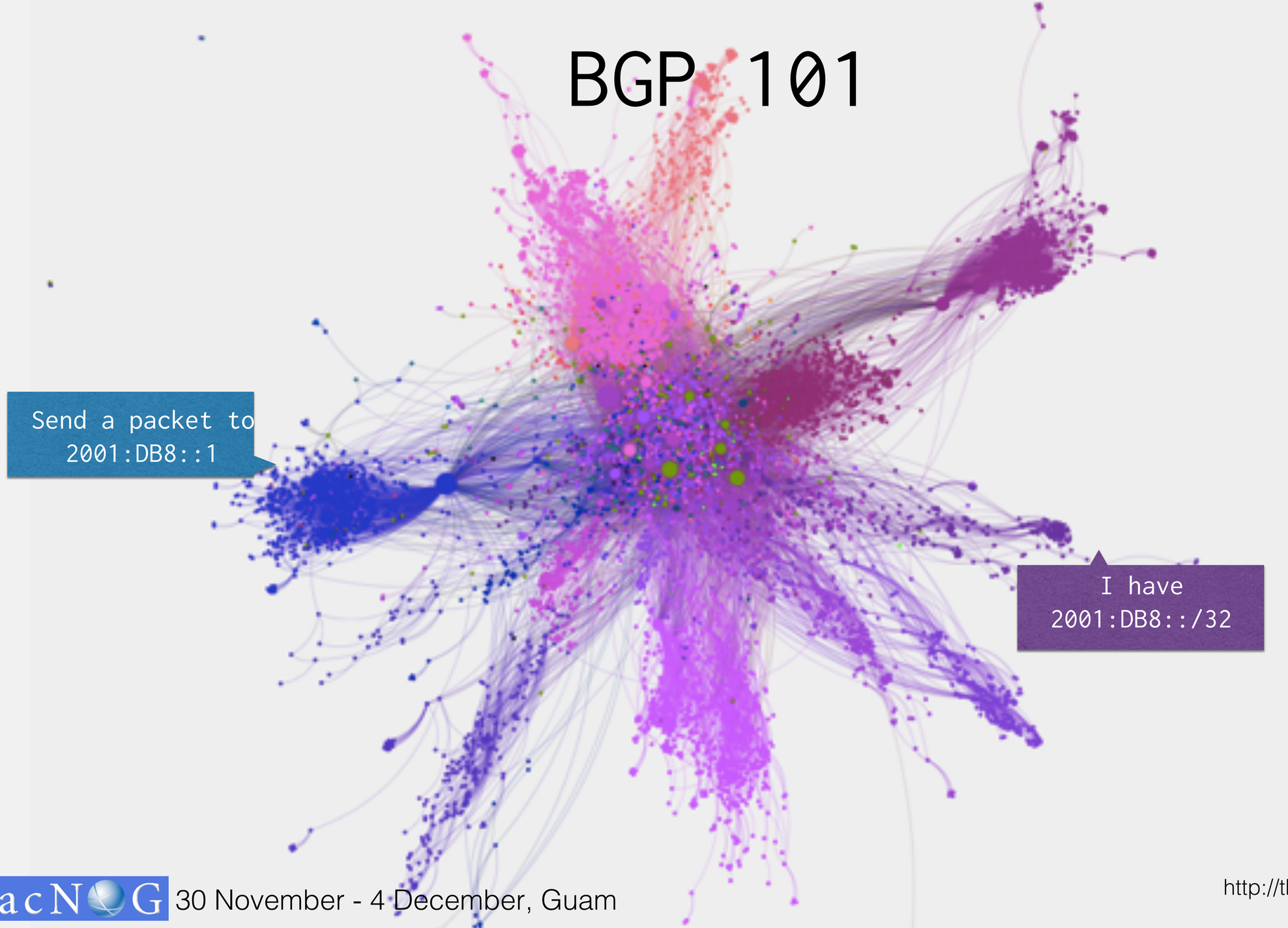


A week with analysing RPKI status: Internal Story

Fakrul Alam
Senior Training Officer, APNIC
fakrul@apnic.net

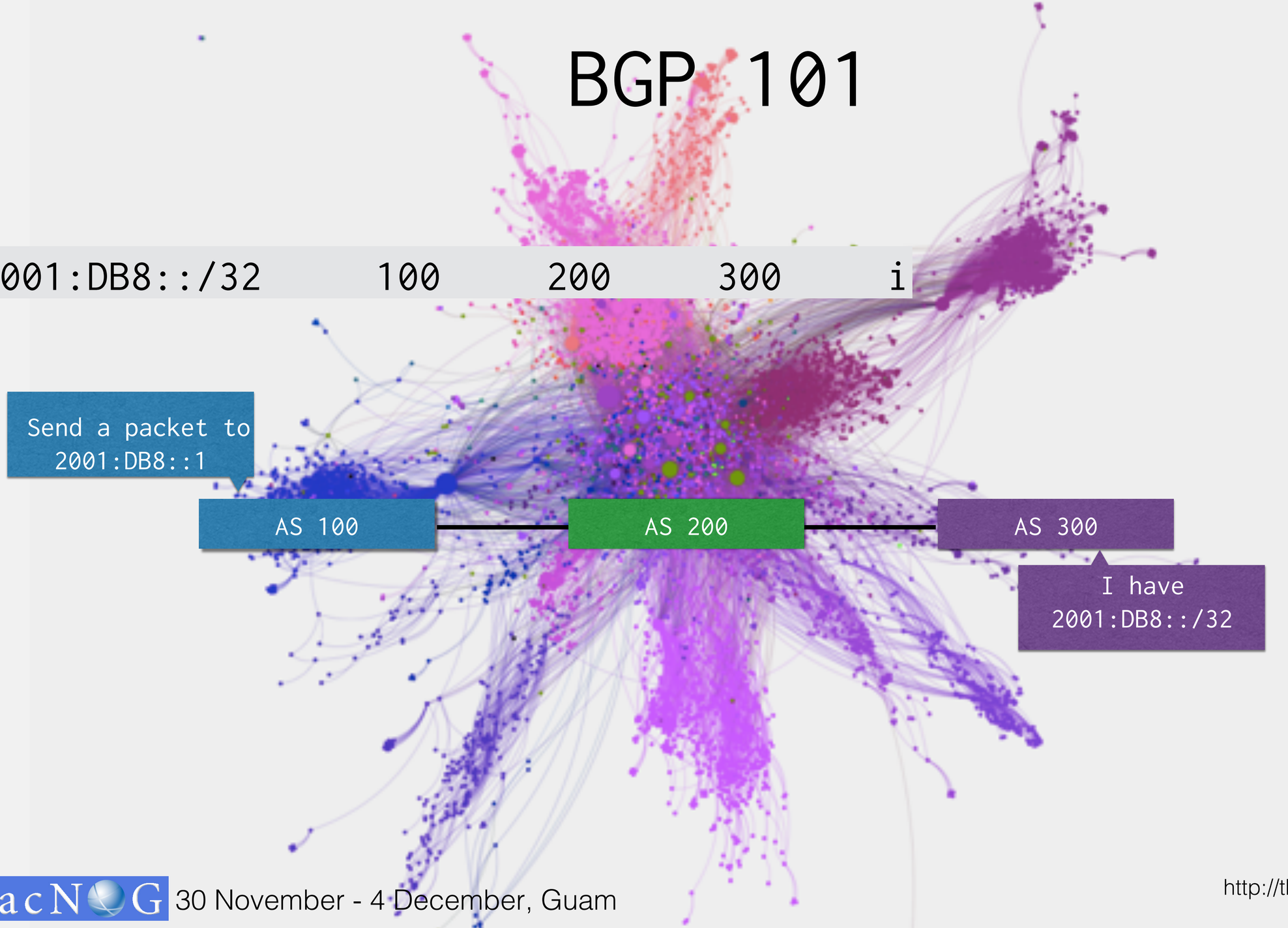
BGP 101



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

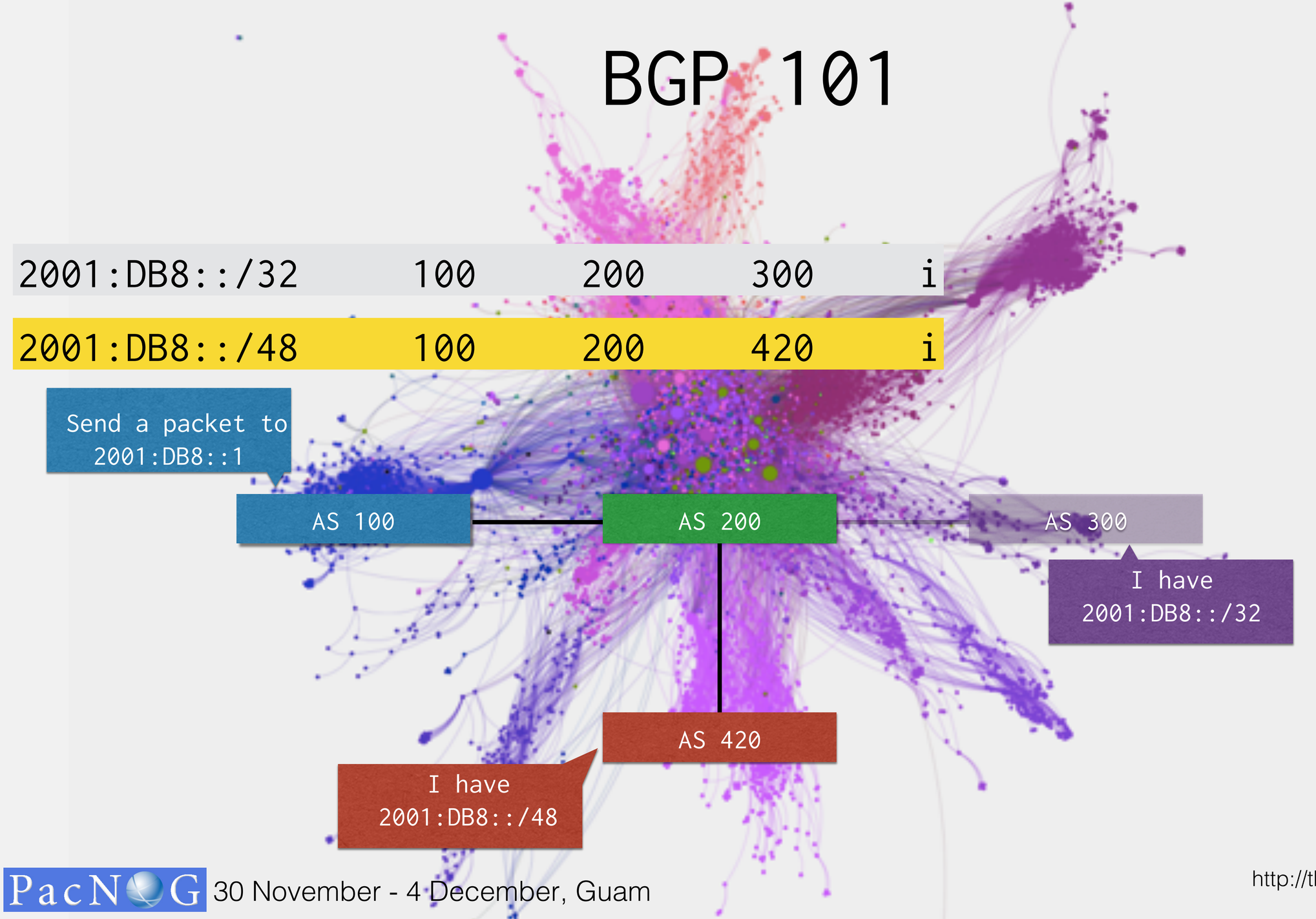
BGP 101

2001:DB8::/32 100 200 300 i



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

BGP 101



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

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

RPKI

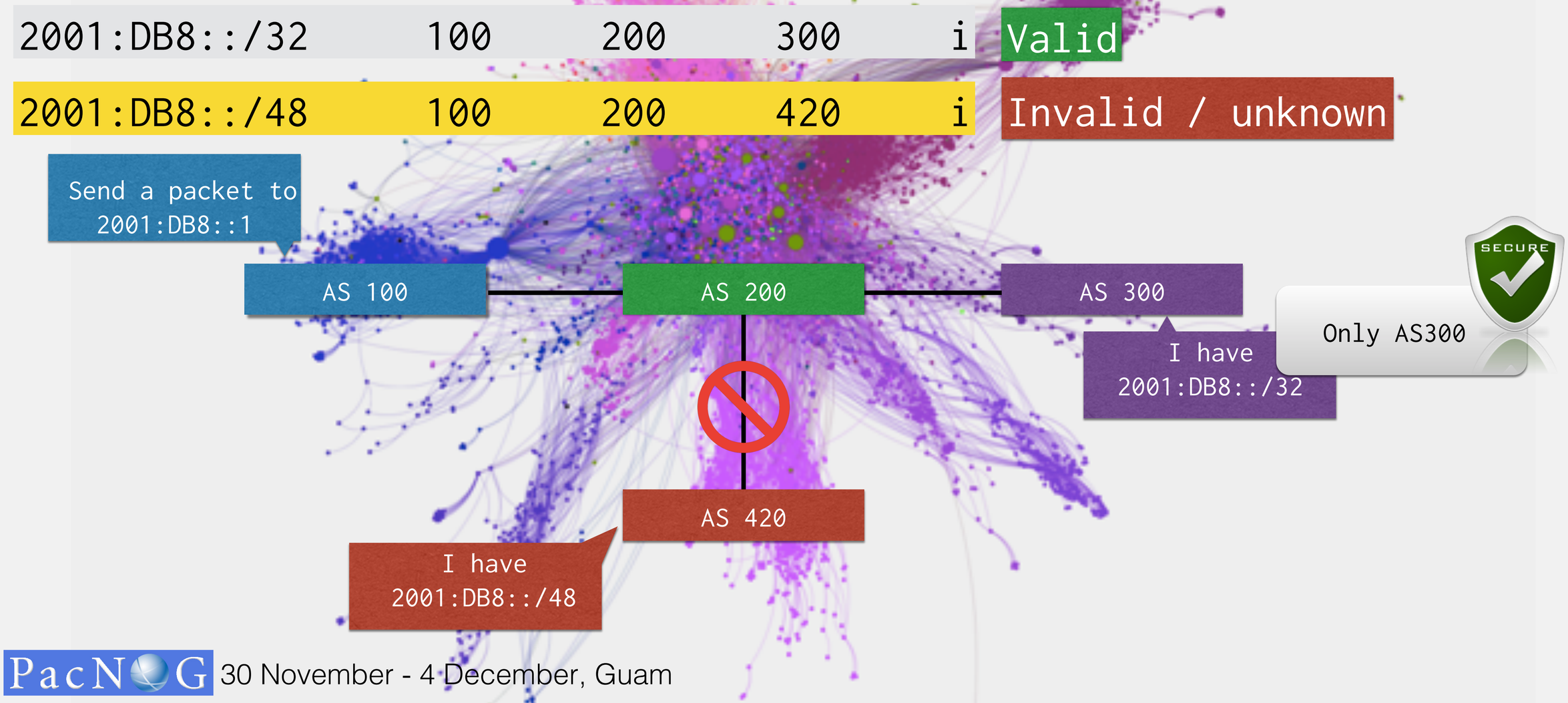
Resource Public Key Infrastructure

IP Address & AS Numbers

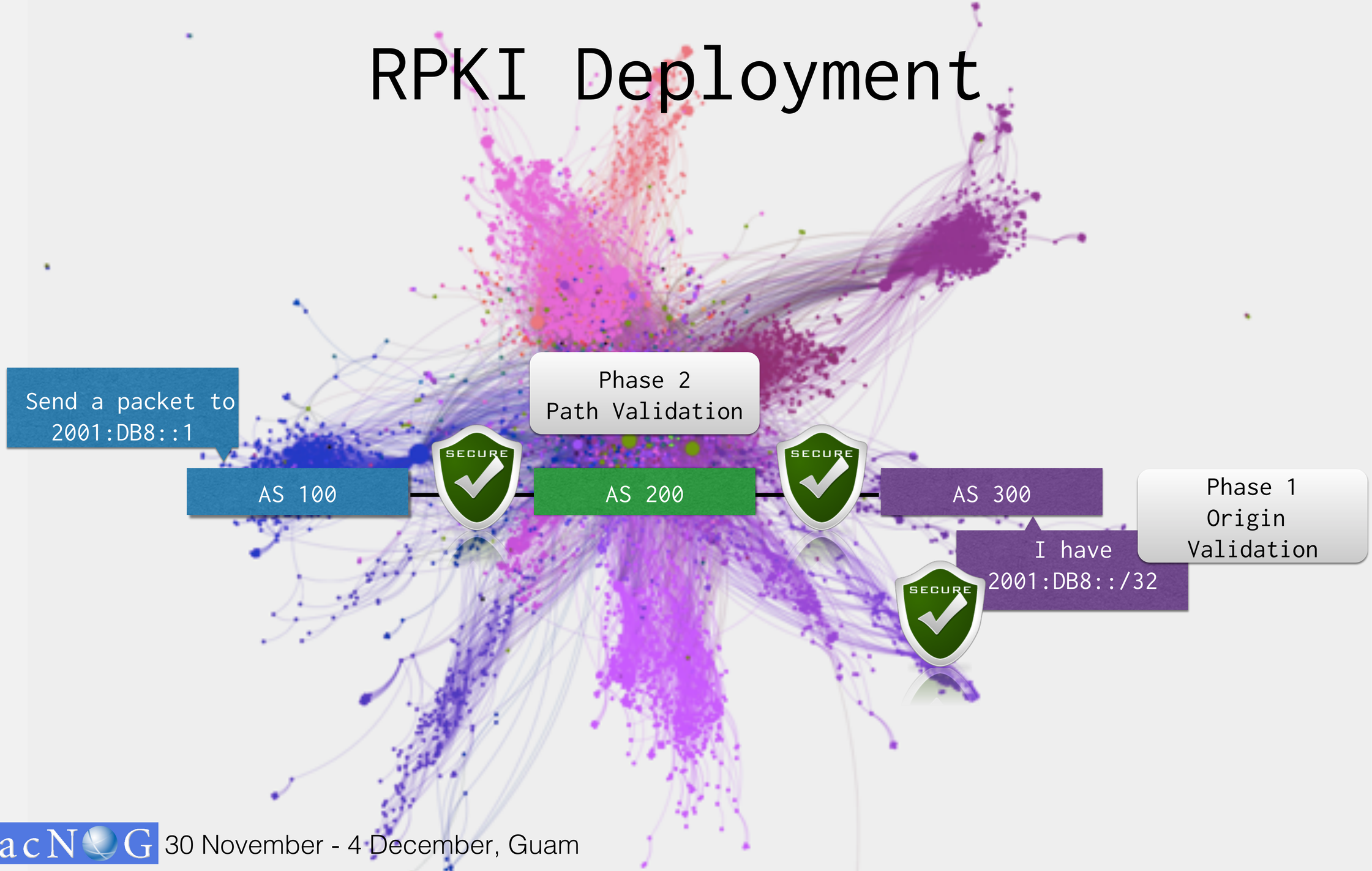
Digital Certificate

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

RPKI Origin Validation



RPKI Deployment



RPKI Building Blocks

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

Primary Goal

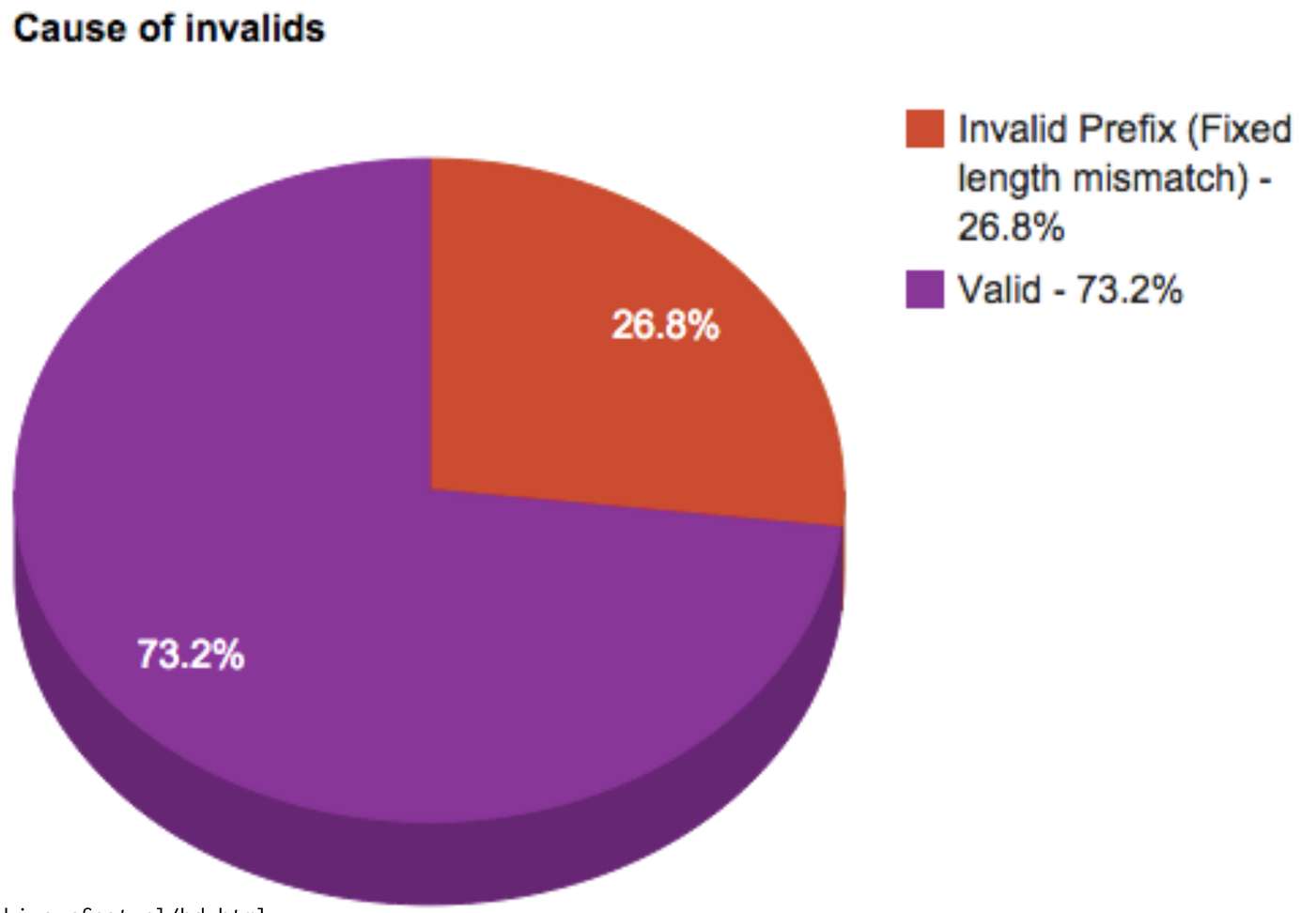
RPKI adoption rate / deployment status

RPKI Breakdown

November 2014	Total Prefix	Valid	Invalid	Unknown	Accuracy	RPKI Adoption Rate
APNIC	135876 (100%)	581 (0.43%)	684 (0.5%)	134611 (99.07%)	45.93%	0.93%
BD	2079 (100%)	71 (3.42%)	26 (1.25%)	1982 (95.33%)	73.2%	4.67%

source : http://rpki.surfnet.nl/perrir.html & http://rpki.surfnet.nl/country.php

Invalid Prefix



source : http://rpki.surfnet.nl/bd.html

All Invalid prefixes from BD

Prefix	ASN	IP Version	Validity	
116.212.184.0/24	38556	4	Invalid	
116.212.185.0/24	38556	4	Invalid	
116.212.186.0/23	38556	4	Invalid	
116.212.187.0/24	38556	4	Invalid	
116.212.188.0/24	38556	4	Invalid	
116.212.189.0/24	38556	4	Invalid	
116.212.190.0/24	38556	4	Invalid	Show details
116.212.191.0/24	38556	4	Invalid	Show details

ROAs

AS	Prefix	Max length
38556	116.212.184.0/21	21

Fixed length mismatch

ASN from Whois DB

38556
38556

source : http://rpki.surfnet.nl/bd.html

All Invalid prefixes from BD

Prefix	ASN	IP Version	Validity	Ir
103.15.244.128/29	58717	4	Invalid	
103.15.244.136/29	58717	4	Invalid	
103.15.244.144/29	58717	4	Invalid	
103.15.244.160/29	58717	4	Invalid	
103.15.244.176/28	58717	4	Invalid	
103.15.244.192/29	58717	4	Invalid	
103.15.244.200/29	58717	4	Invalid	
103.15.244.208/29	58717	4	Invalid	
103.15.244.216/29	58717	4	Invalid	
103.15.244.232/29	58717	4	Invalid	Show details

Showing 1 to 10 of 26 entries

← Previous 1 2 3 Next →

ROAs

AS	Prefix	Max length
58717	103.15.244.0/22	22
58717	103.15.244.0/24	24

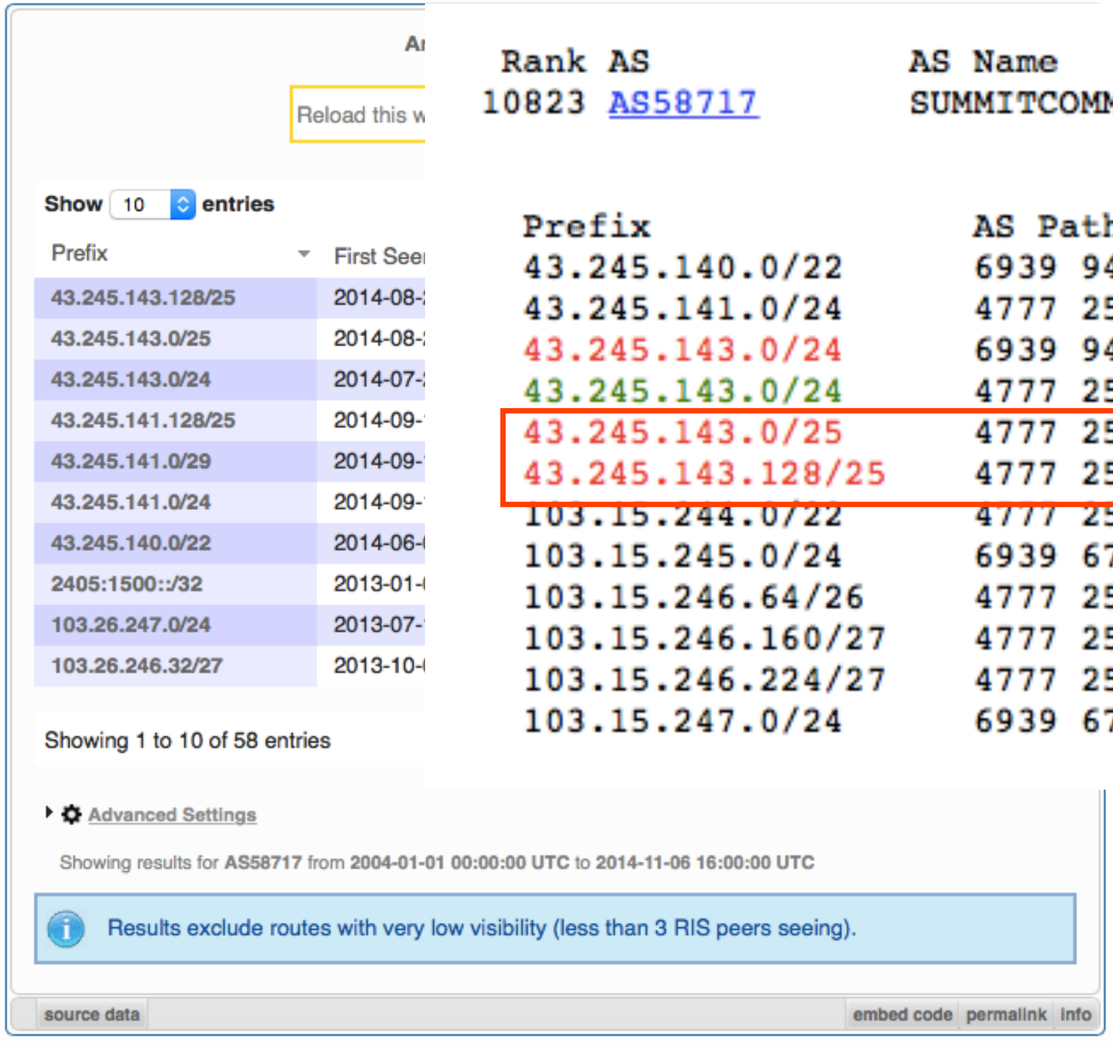
Fixed length mismatch

ASN from Whois DB

58717

source : http://rpki.surfnet.nl/bd.html

Something more serious




```
 Rank AS            AS Name                                          Current  Wthdw  Aggte
10823 AS58717       SUMMITCOMMUNICATIONS-BD Summit Communications       11      3      1

 Prefix              AS Path                                  Aggregation Suggestion
 43.245.140.0/22     6939 9498 132884 58717
 43.245.141.0/24     4777 2516 6453 132884 58717
 43.245.143.0/24     6939 9498 132884 58717 - Withdrawn - matching aggregate 43.245.
 43.245.143.0/24     4777 2516 6762 132602 58717 + Announce - aggregate of 43.245.14
 43.245.143.0/25     4777 2516 6762 132602 58717 - Withdrawn - aggregated with 43.24
 43.245.143.128/25   4777 2516 6762 132602 58717 - Withdrawn - aggregated with 43.24
 103.15.244.0/22     4777 2516 6453 132884 58717
 103.15.245.0/24     6939 6762 132602 58717
 103.15.246.64/26    4777 2516 6762 132602 58717
 103.15.246.160/27   4777 2516 6762 132602 58717
 103.15.246.224/27   4777 2516 6762 132602 58717
 103.15.247.0/24     6939 6762 132602 58717
```

source : http://www.cidr-report.org/cgi-bin/as-report?as=as58717&view=2.0

source : https://stat.ripe.net/widget/announced-prefixes#w.resource=58717

Secondary Goal

Clients are announcing > /24

and some upstream is allowing them!!

Secondary Goal

Who are they & how to get all those prefixes!!

Solution

ExaBGP + GIXLG

ExaBGP

- sql backed looking glasses with prefix routing visualisation
service high availability automatically isolating dead servers / broken services
DDOS mitigation solutions
anycasted services

source : https://github.com/Exa-Networks/exabgp

GIXLG

```
mysql> desc prefixes;
+--------------------+---------------------+------+-----+---------------------+-----------------------------+
| Field              | Type                | Null | Key | Default             | Extra                       |
+--------------------+---------------------+------+-----+---------------------+-----------------------------+
| neighbor           | varchar(39)         | NO   | PRI | NULL                |                             |
| type               | tinyint(3) unsigned | NO   |     | NULL                |                             |
| prefix             | varchar(43)         | NO   | PRI | NULL                |                             |
| length             | tinyint(3) unsigned | NO   |     | NULL                |                             |
| ip_start           | decimal(39,0)       | NO   |     | NULL                |                             |
| ip_end             | decimal(39,0)       | NO   |     | NULL                |                             |
| ip_poly            | polygon             | NO   | MUL | NULL                |                             |
| aspath             | varchar(500)        | NO   | MUL | NULL                |                             |
| nexthop            | varchar(39)         | NO   |     | NULL                |                             |
| community          | text                | NO   |     | NULL                |                             |
| extended_community | text                | NO   |     | NULL                |                             |
| origin             | varchar(10)         | NO   |     | NULL                |                             |
| originas           | int(10) unsigned    | NO   |     | NULL                |                             |
| time               | timestamp           | NO   |     | 0000-00-00 00:00:00 | on update CURRENT_TIMESTAMP |
+--------------------+---------------------+------+-----+---------------------+-----------------------------+
```

```
select prefix, length, aspath,
origin from prefixes where length >
'24';
```

Result

Total Prefix 97

Originating AS

PREFIX	LENGTH	AS PATH	ORIGIN
196.10.97.128/26	26	58656 132602 6762 8452 37664	igp
177.221.194.176/30	30	58656 132602 6762 4230 52682	igp
177.221.194.144/30	30	58656 132602 6762 4230 52682	igp
121.100.54.60/30	30	58656 132602 6762 38742	igp
186.233.141.0/25	25	58656 132602 6762 4230 262991 262991 262991	igp
177.221.197.120/30	30	58656 132602 6762 4230 52682	igp
41.209.195.128/25	25	58656 132602 6762 8452 8452 8452 20484	igp
177.221.194.112/30	30	58656 132602 6762 4230 52682	igp

prefix/length

Something even more serious!

```
whois -h whois.cymru.com 180.149.11.67/32
AS      | IP                | AS Name
45904   | 180.149.11.67     | BANGLALION-WIMAX-BD
Banglalion Communications Ltd,BD
```

```
whois -h whois.cymru.com as132602
AS Name
BANGLADESH-AS-AP Bangladesh Submarine Cable
Company Limited (BSCCL),BD
```

177.221.194.104/30	30	58656 132602 6762 [illegible] 52682	igp
180.149.11.67/32	32	58656 132602	igp
93.186.133.80/31	31	58656 132602	incomplete
93.186.133.82/31	31	58656 132602	incomplete
177.221.197.[illegible]/30	30	58656 132602 6762 4230 52682	igp
177.221.197.168/[illegible]	30	58656 132602 6762 4230 52682	igp
[illegible]	[illegible]	58656 132602 6762 4230 52682	igp

```
whois -h whois.cymru.com 213.144.176.128/31
AS      | IP                | AS Name
6762    | 213.144.176.128   | SEABONE-NET
TELECOM ITALIA SPARKLE S.p.A.,IT
```

Encourage resource owner to create ROA and start doing RPKI validation

RPKI Status : Bangladesh

	Total Prefix	Valid	Invalid	Unknown	Accuracy	RPKI Adoption Rate
Nov 2014	2079 (100%)	71 (3.42%)	26 (1.25%)	1982 (95.33%)	73.2%	4.67%
Feb 2015	2295 (100%)	137 (5.97%)	9 (0.39%)	2149 (93.64%)	93.84%	6.36%

source : http://rpki.surfnet.nl/perrir.html & http://rpki.surfnet.nl/country.php

RPKI Breakdown - APNIC

Year	Total Prefix	Valid	Invalid	Unknown	Accuracy	RPKI Adoption Rate
November 2014	135876 (100%)	581 (0.43%)	684 (0.5%)	134611 (99.07%)	45.93%	0.93%
November 2015	154338 (100%)	3078 (1.99%)	1123 (0.73%)	150137 (97.28%)	73.27%	2.72%

source : http://rpki.surfnet.nl/perrir.html & http://rpki.surfnet.nl/country.php


READY TO
ROA
www.apnic.net/roa
APNIC

Special thanks to

Jac Kloots
SURFnet
http://rpki.surfnet.nl/index.html

Thomas Mangin
Exa-Networks : ExaBGP
https://github.com/Exa-Networks/exabgp

Daniel Piekacz
GIXtools Project : GIXLG
https://gixtools.net

Thank You