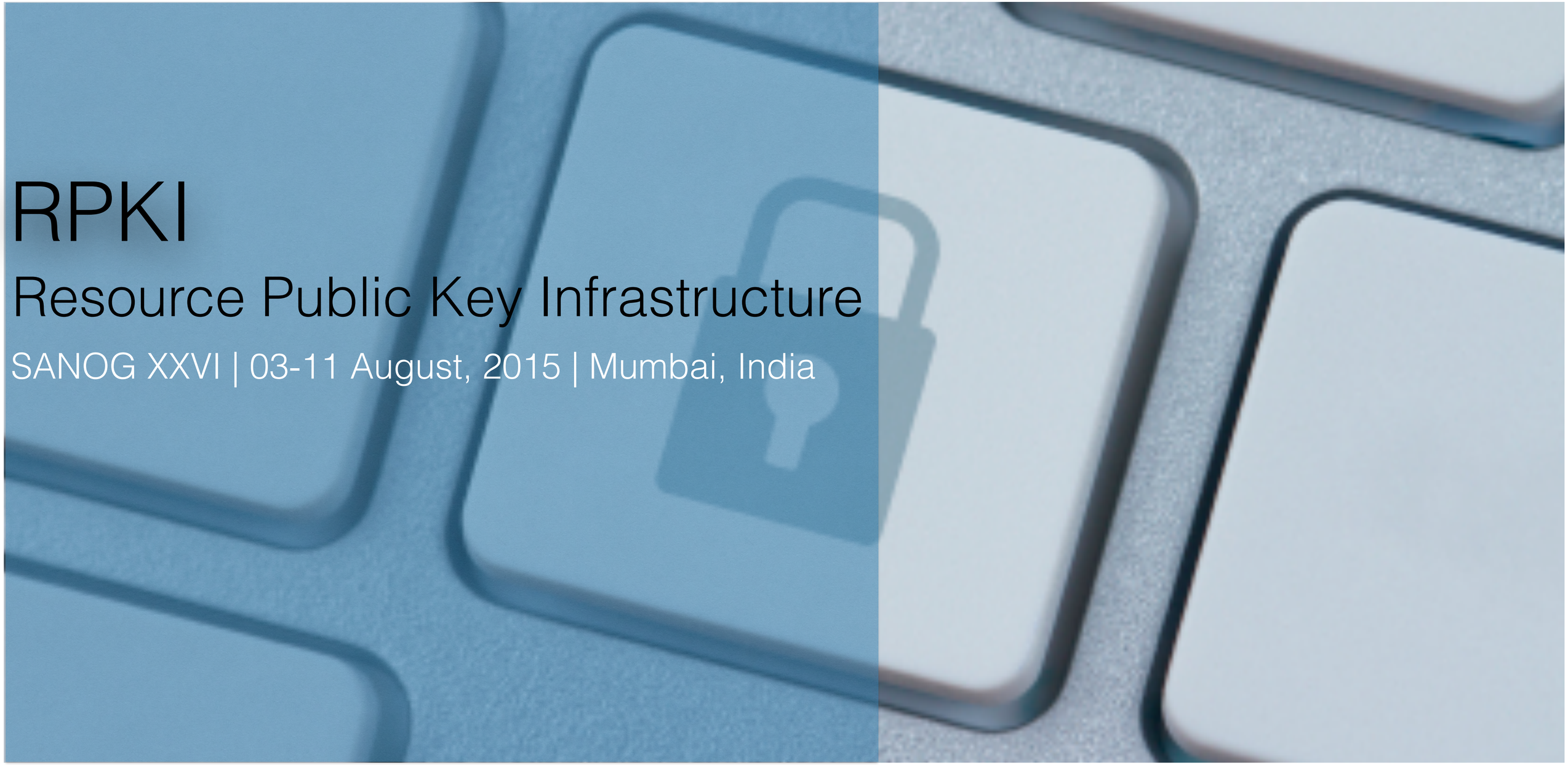


RPKI

Resource Public Key Infrastructure

SANOG XXVI | 03-11 August, 2015 | Mumbai, India

Fakrul Alam fakrul@bdhub.com http://bd.linkedin.com/in/fakrulalam https://twitter.com/rapappu

Target Audience

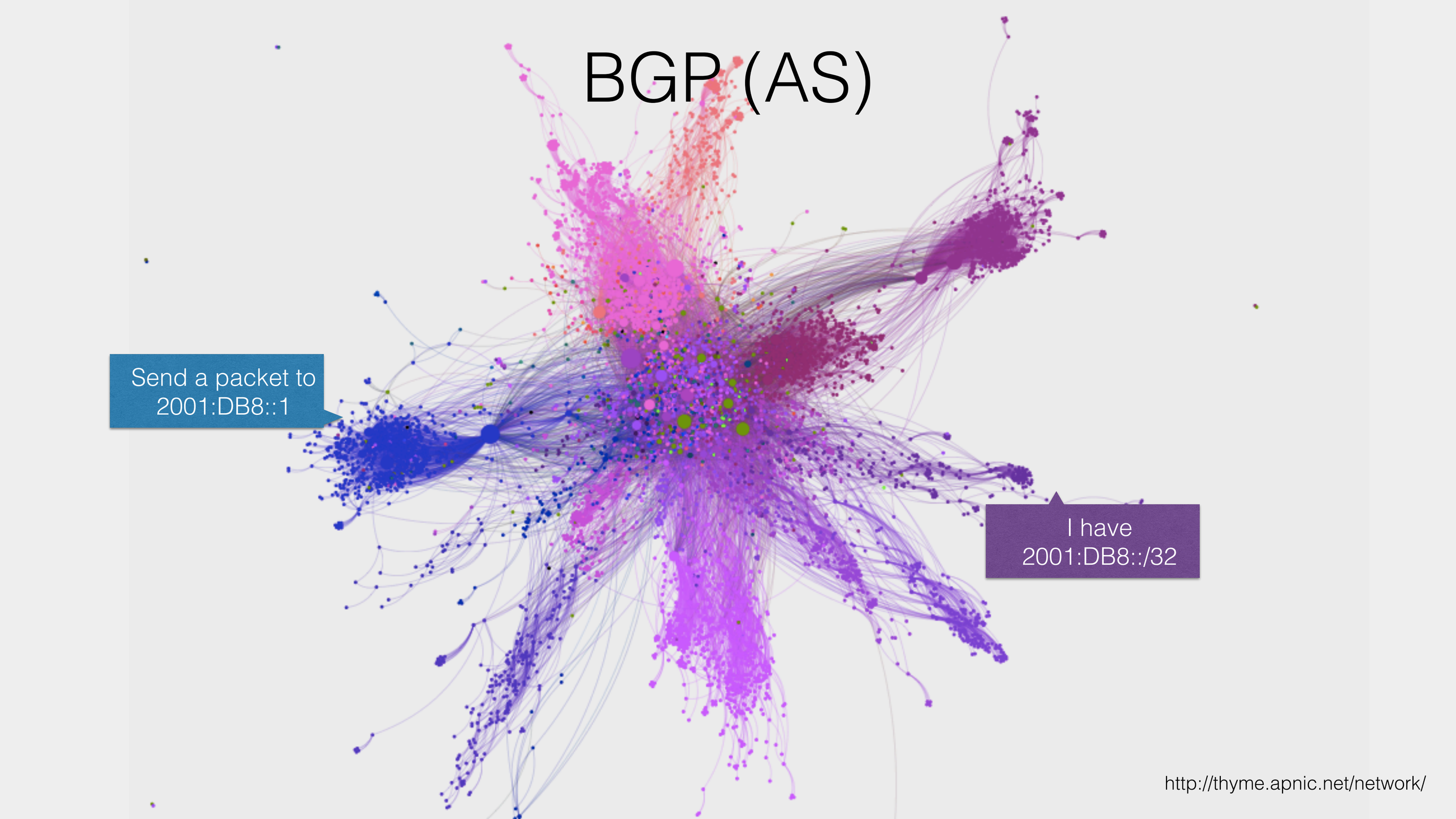
- Knowledge of Internet Routing(specially BGP)
- Familiar with any IRR Database
- No need to know Cryptography
- Basic knowledge of PKI(Public Key Infrastructure)

Agenda

- BGP / RPKI
- Configuration
- Hands-on Lab (Juniper)

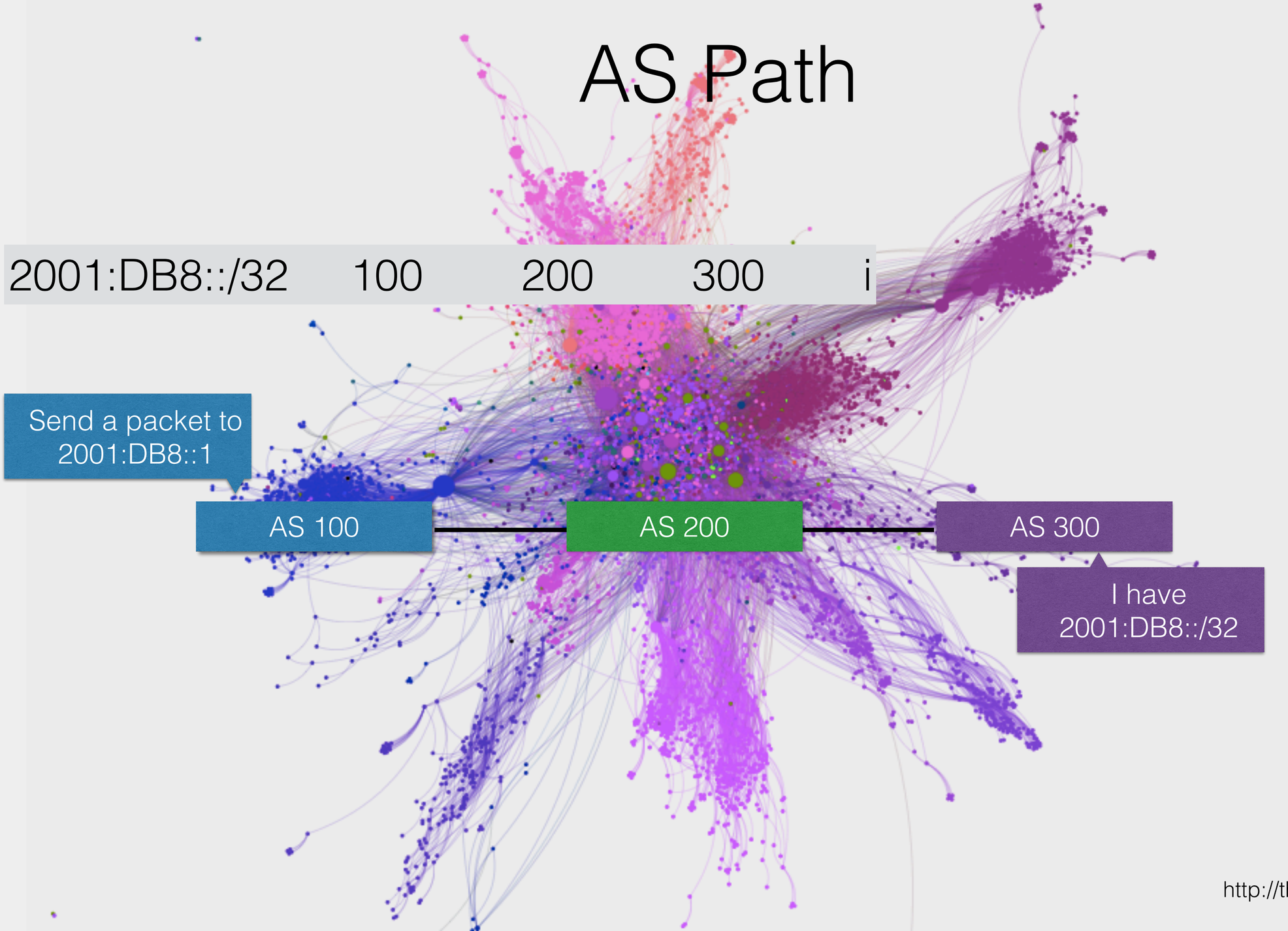
BGP

BGP (AS)



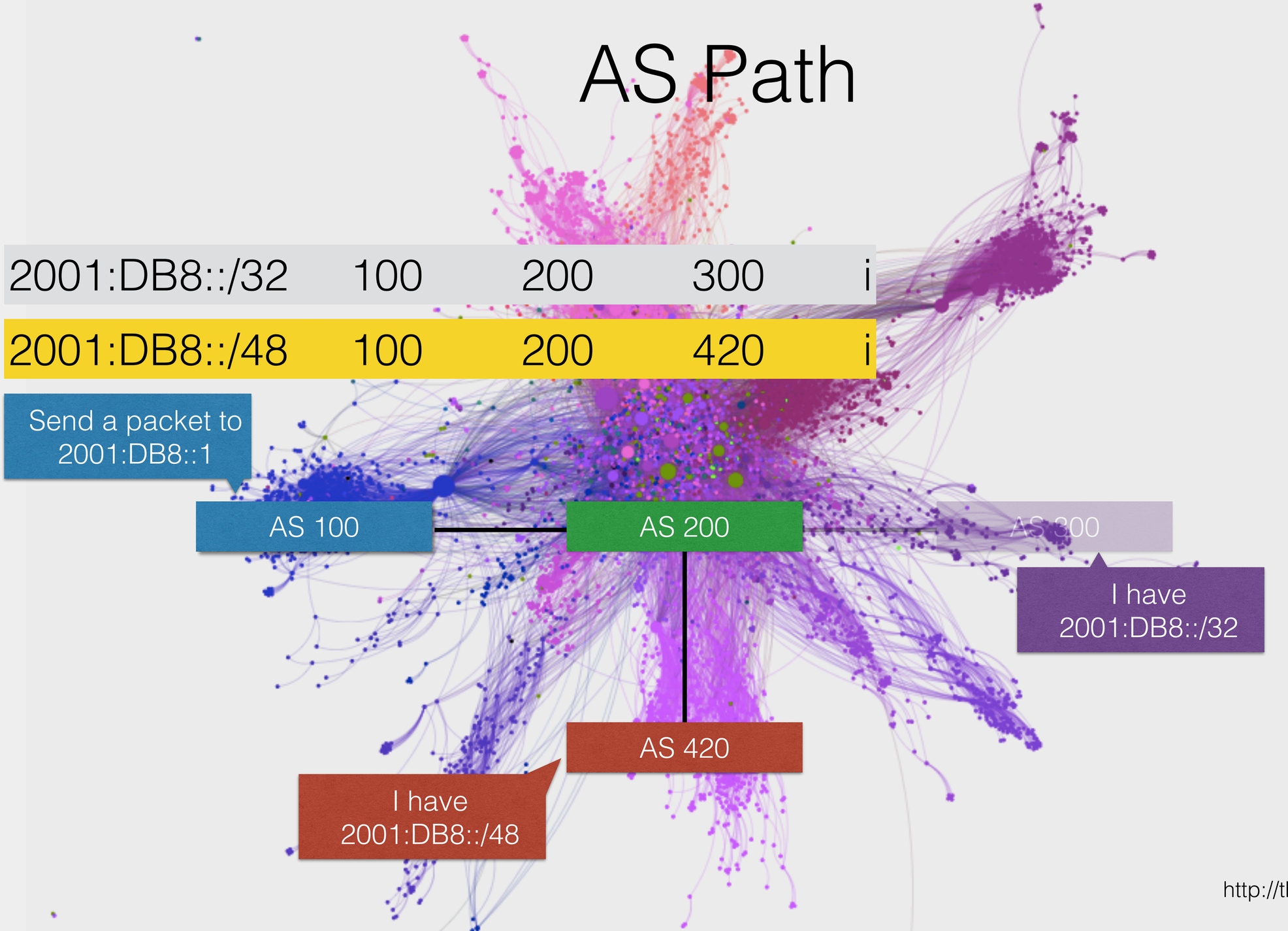
http://thyme.apnic.net/network/

AS Path



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

AS Path



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

Historical Incident

- April 1997: The "AS 7007 incident" UU/Sprint for 2 days
- February 24, 2008: Pakistan's attempt to block YouTube access within their country takes down YouTube entirely.[6]
- November 11, 2008: The Brazilian ISP CTBC - Companhia de Telecomunicações do Brasil Central leaked their internal table into the global BGP table.
- April 8, 2010: China Telecom originated 37,000 prefixes not belonging to them in 15 minutes, causing massive outage of services globally.

source : http://en.wikipedia.org/wiki/IP_hijacking

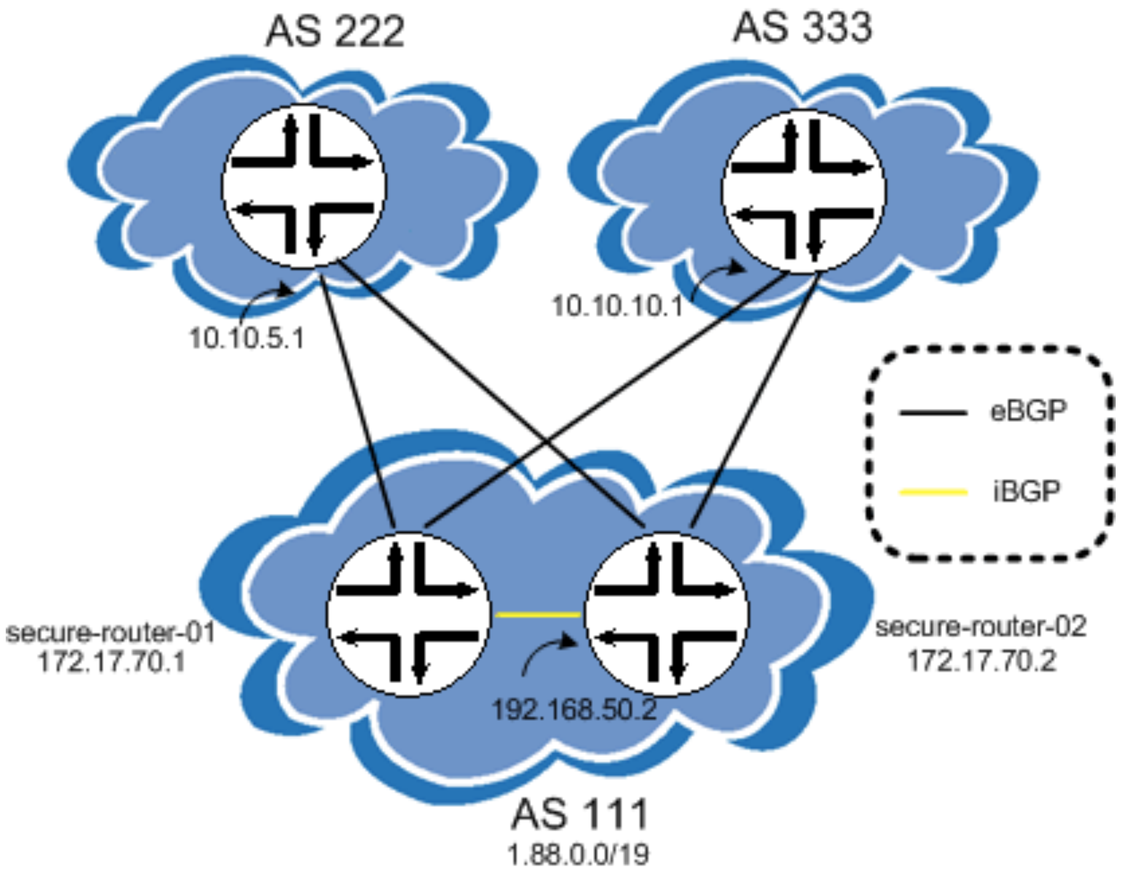
Historical Incident

- For theory of positivity lets call all these as Mis-Origination
- Traffic Hijacking or Prefix Hijacking assumes Negative intent

Current Trend

- 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

Filter Where?



- Secure BGP Templates
  - http://www.cymru.com/gillsr/documents/junos-bgp-template.htm
  - https://www.team-cymru.org/ReadingRoom/Templates/secure-bgp-template.html

Internet Registry (IR)

- Maintains Internet Resources such as IP addresses and ASNs, and publish the registration information
  - Allocations for Local Internet Registries
  - Assignments for end-users
- APNIC is the Regional Internet Registry(RIR) in the Asia Pacific region
  - National Internet Registry(NIR) exists in several economies

The Eco-System

Internet Assigned Numbers Authority

Regional IR (RIR)

National IR (NIR)

Internet Service Provider

End User

Routing Policy Specification Language (RPSL)

- Maintains routing policy database
  - RADB is the most popular service, though some RIRs also provide similar services
  - Routing policy information is expressed in a series of objects
  - On RADB, a registered user can register any object
- route and route6 objects are used to indicate route origination
  - Prefix and origin AS

Still not enough
IRR is useful, but it’s not perfect

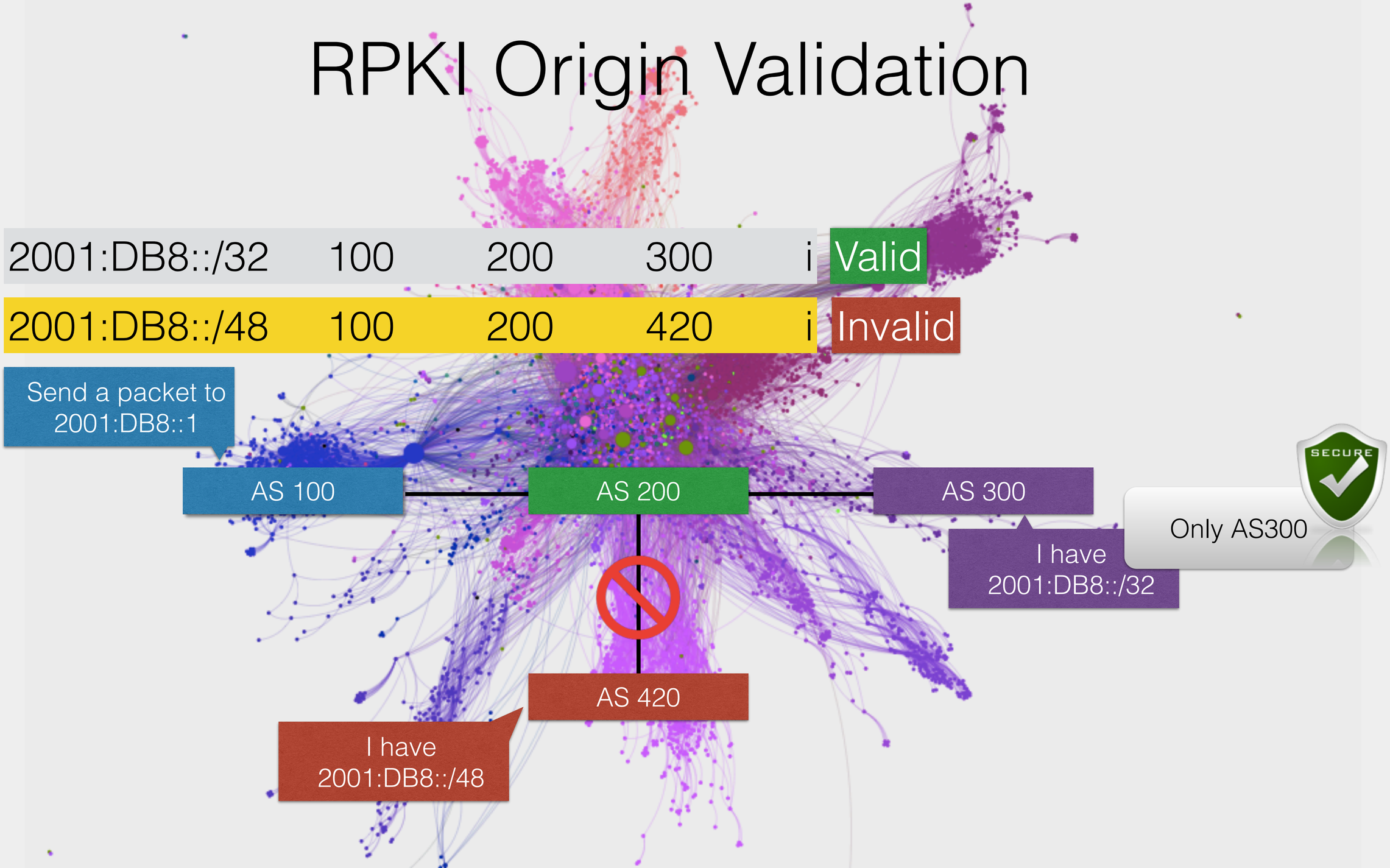
RPKI

Resource Pubic Key Infrastructure

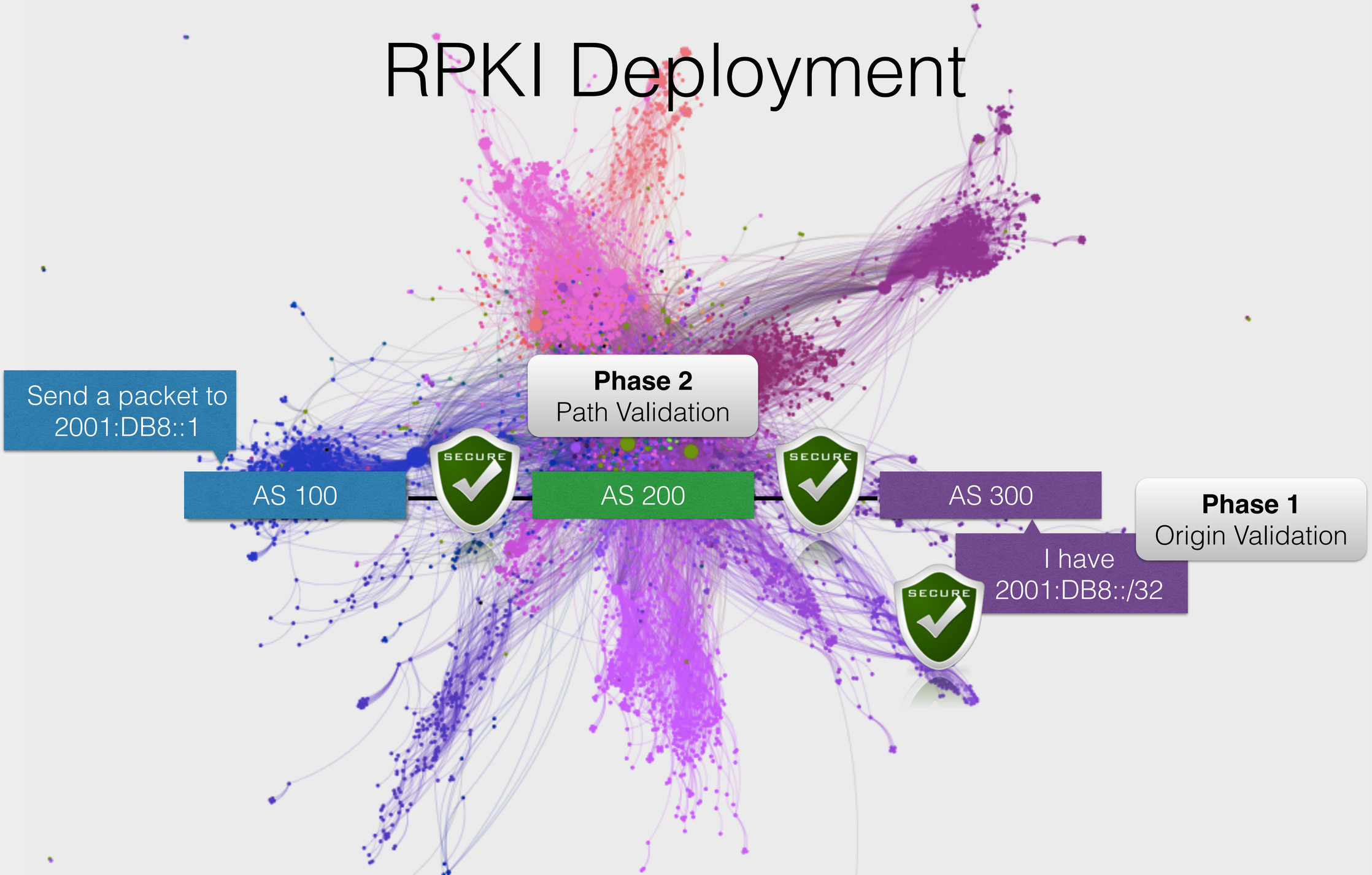
IP Address & AS Numbers

Digital Certificate

RPKI Origin Validation



RPKI Deployment



Goals of RPKI

- Able to authoritatively prove who owns an IP Prefix and what AS(s) may Announce It
  - Reducing routing leaks
  - Attaching digital certificates to network resources (AS Number & IP Address)
- Prefix Ownership Follows the Allocation Hierarchy IANA, RIRs, ISPs, …

RPKI Implementation

- Two RPKI implementation type
  - **Delegated**: Each participating node becomes a CA and runs their own RPKI repository, delegated by the parent CA.
  - **Hosted**: The RIR runs the CA functionality for interested participants.

RPKI Building Blocks

- Trust Anchors (RIR's)
- Route Origination Authorizations (ROA)
- Validators

Let’s discuss these building blocks in details

PKI & Trust Anchors

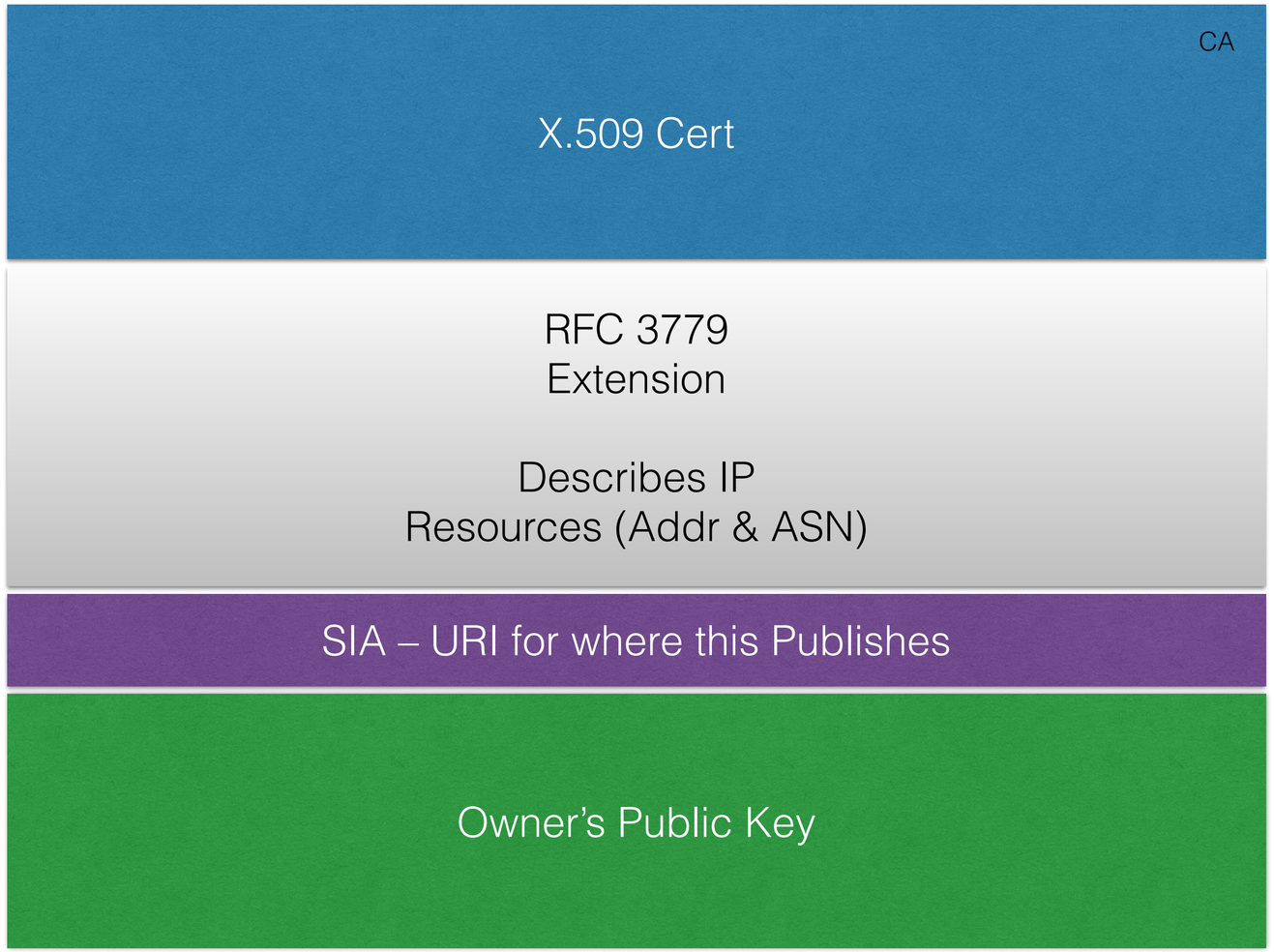
Public Key Concept

- **Private key**: This key must be known only by its owner.
- **Public key**: This key is known to everyone (it is public)
- **Relation between both keys**: What one key encrypts, the other one decrypts, and vice versa. That means that if you encrypt something with my public key (which you would know, because it's public :-), I would need my private key to decrypt the message.
- Same alike http with SSL aka https

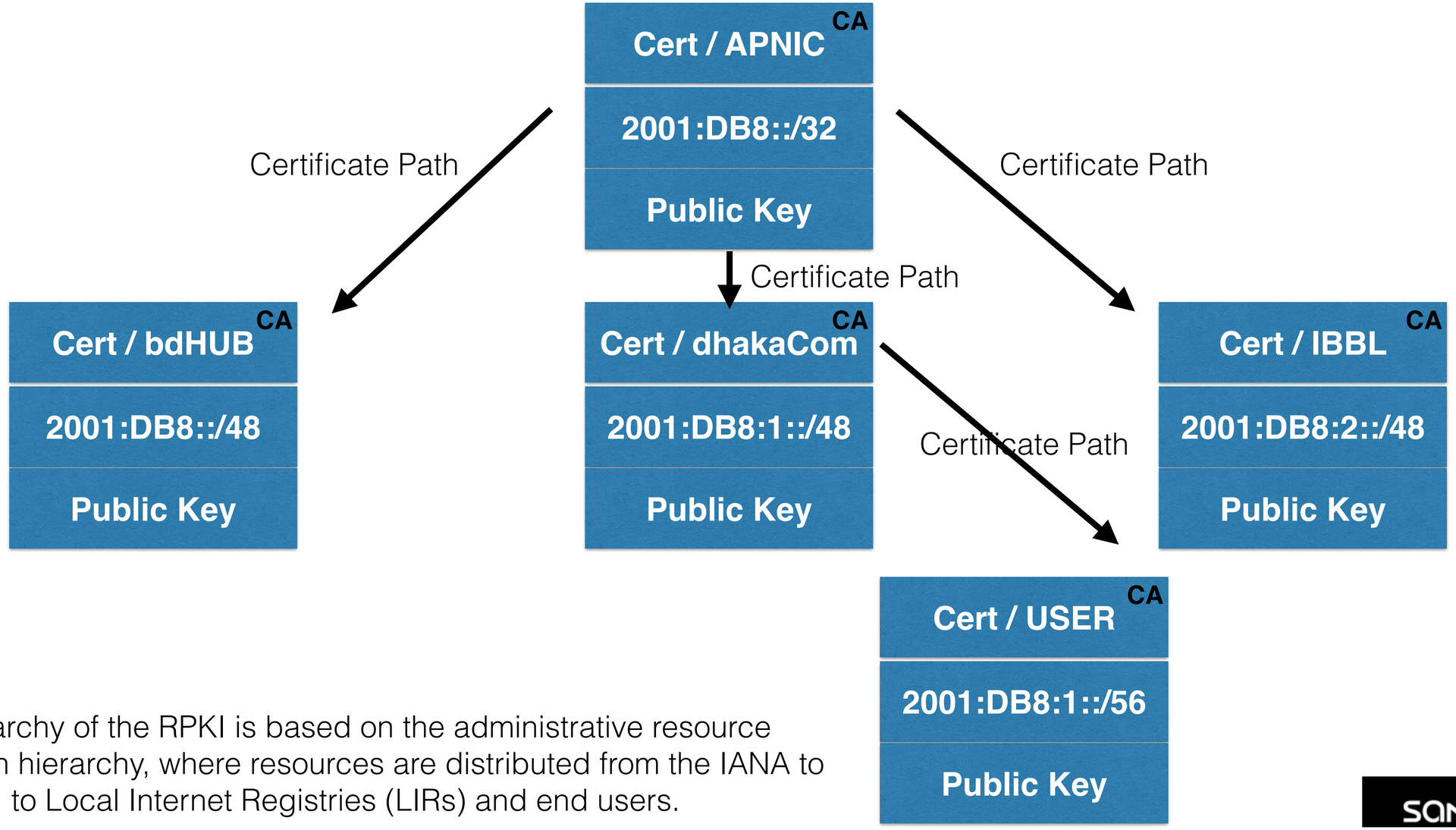
X.509 Certificates 3779 EXT

Signed by Parent's Private Key

Certificates are X.509 certificates that conform to the PKIX profile [PKIX]. They also contain an extension field that lists a collection of IP resources (IPv4 addresses, IPv6 addresses and AS Numbers) [RFC3779]



Trust Anchor



The hierarchy of the RPKI is based on the administrative resource allocation hierarchy, where resources are distributed from the IANA to the RIRs, to Local Internet Registries (LIRs) and end users.

Trust Anchor Locator (TALs)

- In cryptographic systems with hierarchical structure, a Trust anchor is an authoritative entity for which trust is assumed and not derived.
- In X.509 architecture, a root certificate would be the trust anchor from which whole chain of trust is derived. The trust anchor must be in possession of the trusting party beforehand to make any further certificate path validation possible.
- RPKI uses Internet Assigned Numbers Authority(IANA) as the trust anchor, and Regional Internet Registries(RIR) as immediately subordinate nodes to that anchor.

PKI in IRR

- The RIRs hold a self-signed root certificate for all the resources that they have in the registry
  - They are the trust anchor for the system
- That root certificate is used to sign a certificate that lists your resources
- You can issue child certificates for those resources to your customers
  - When making assignments or sub allocations

ROA
Route Origin Authorizations

Route Origination Authorizations (ROA)

A ROA is a **digitally signed object** that provides a means of **verifying** that an **IP address block holder** has **authorized** an **Autonomous System (AS)** to originate routes to one or more **prefixes** within the address block.

With a **ROA**, the **resource holder is attesting** that the **origin AS** number is **authorized** to **announce** the **prefix(es)**. The attestation can be verified cryptographically using RPKI.

Route Origination Authorizations (ROA)

- Next to the prefix and the ASN which is allowed to announce it, the ROA contains:
  - A minimum prefix length
  - A maximum prefix length
  - An expiry date
  - Origin ASN
- Multiple ROAs can exist for the same prefix
- ROAs can overlap

Validators

Origin Validation

- Router gets ROA information from the RPKI Cache
  - RPKI verification is done by the RPKI Cache
- The BGP process will check each announcement with the ROA information and label the prefix

Result of Check

- **Valid** – Indicates that the prefix and AS pair are found in the database.
- **Invalid** – Indicates that the prefix is found, but either the corresponding AS received from the EBGP peer is not the AS that appears in the database, or the prefix length in the BGP update message is longer than the maximum length permitted in the database.
- **Not Found / Unknown**– Indicates that the prefix is not among the prefixes or prefix ranges in the database.

Valid > Unknown > Invalid

ROA Example

Prefix: 10.0.0.0/16
ASN: 65420

	Origin AS	Prefix	Max Length
ROA	65420	10.0.0.0/16	/18
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	

Local Policy

- You can define your policy based on the outcomes
  - Do nothing
  - Just logging
  - Label BGP communities
  - Modify preference values
  - Rejecting the announcement

RPKI Support in Routers

- The RPKI-RTR Protocol is an IETF Internet Draft
- Production Cisco Support:
  - ASR1000, 7600, ASR903 and ASR901 in releases 15.2(1)S or XE 3.5
  - Cisco Early Field Trial (EFT):
  - ASR9000, CRS1, CRS3 and c12K (IOS-XR 4.3.2)
- Juniper has support since version 12.2
- Quagga has support through BGP-SRX

RPKI Caveats

- When RTR session goes down, the RPKI status will be not found for all the bgp route after a while
  - Invalid => not found
  - we need several RTR sessions or care your filtering policy
- In case of the router reload, which one is faster, receiving ROAs or receiving BGP routes?
  - If receiving BGP is match faster than ROA, the router propagate the invalid route to others
  - We need to put our Cache validator within our IGP scope

Who do we trust?

- Can we trust the *IR for hosting our Private Keys?

Two digital certificates have been mistakenly issued in Microsoft's name that could be used by virus writers to fool people into running harmful programs, the software giant warned Thursday.

According to Microsoft, someone posing as a Microsoft employee tricked VeriSign, which hands out so-called digital signatures, into issuing the two certificates in the software giant's name on Jan. 30 and Jan. 31.

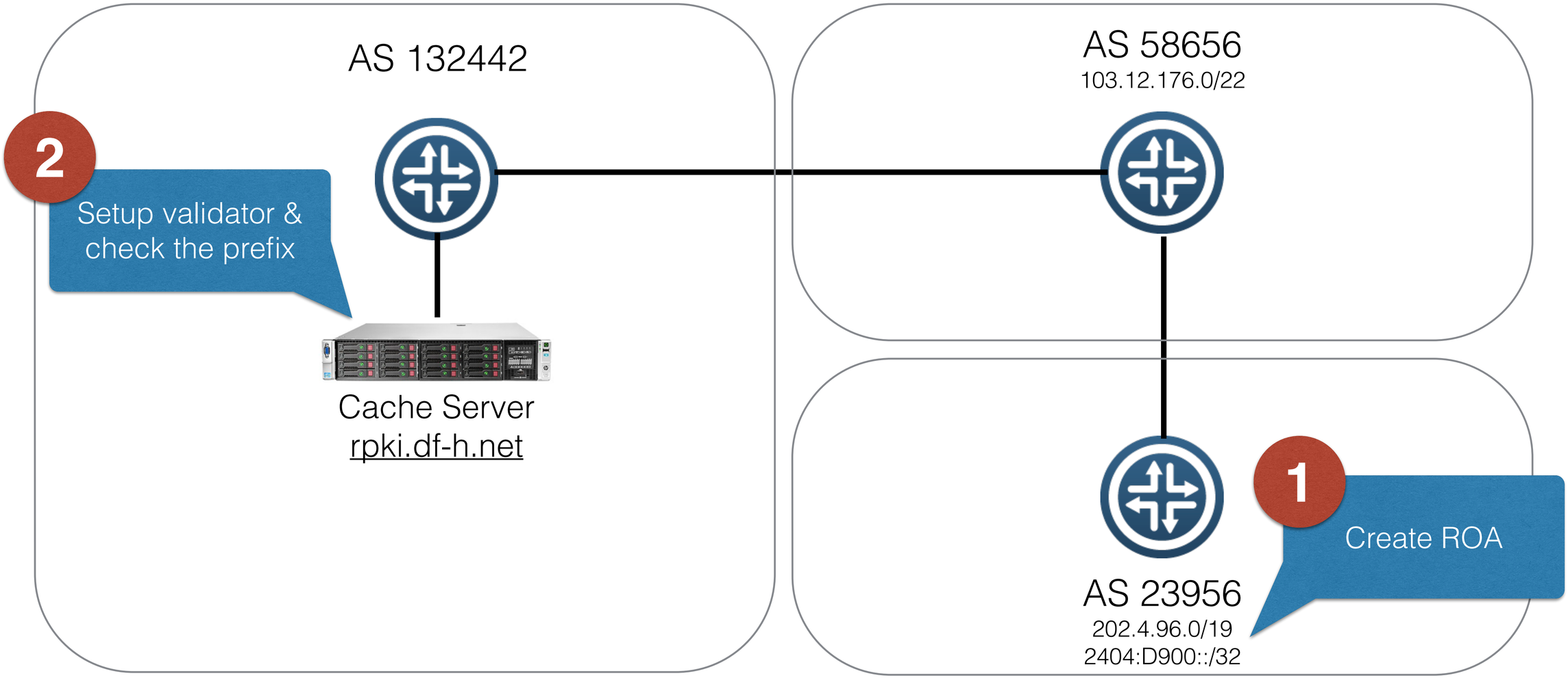
Such certificates are critical for businesses and consumers who download patches, updates and other pieces of software from the Internet, because they verify that the software is being supplied from a particular company, such as Microsoft.

RPKI Further Reading

- RFC 5280: X.509 PKI Certificates
- RFC 3779: Extensions for IP Addresses and ASNs
- RFC 6481-6493: Resource Public Key Infrastructure

RPKI Configuration

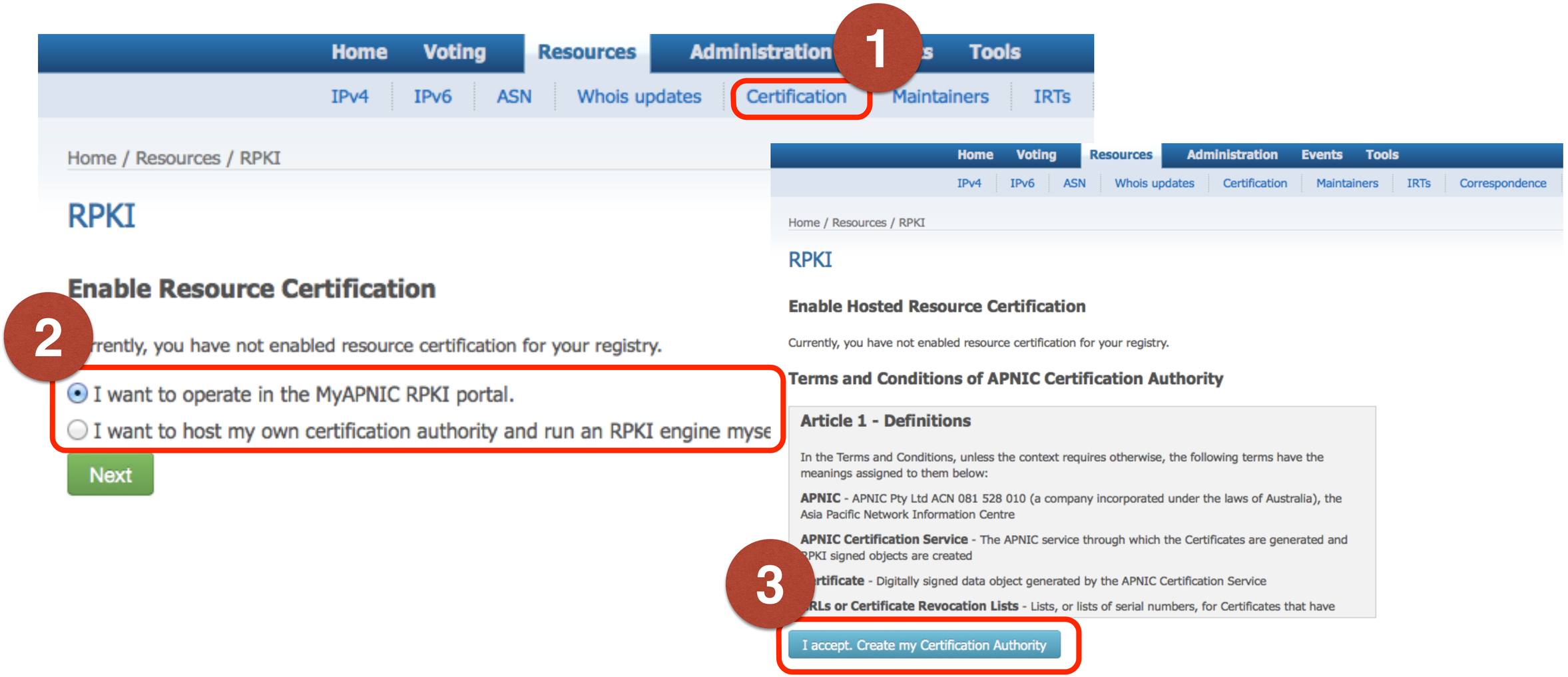
Topology for Origin Validation



Phase I - Publishing ROA

- Login to your MyAPNIC portal
- Required valid certificate
- Go to Resources > Certification Tab

Phase I - Publishing ROA



Phase I - Publishing ROA

RPKI

BGP Route Validity

All

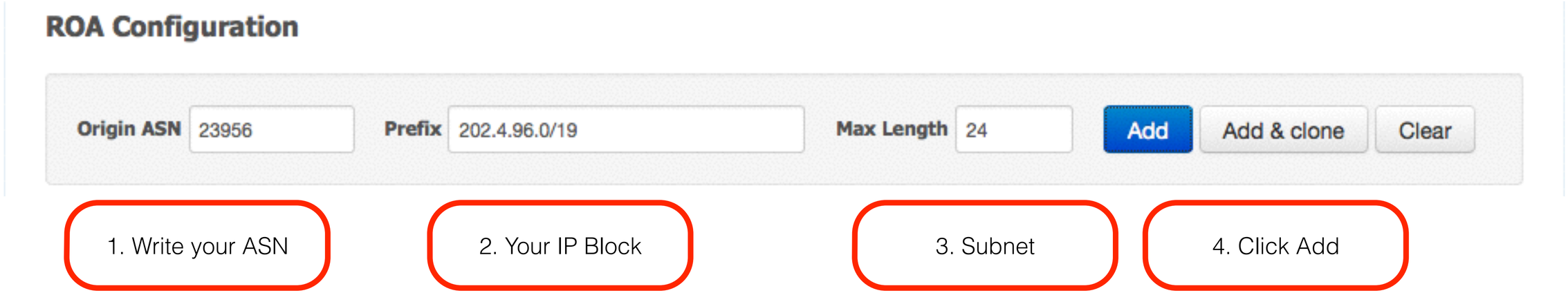
Items per page 10

Search by AS or IP...

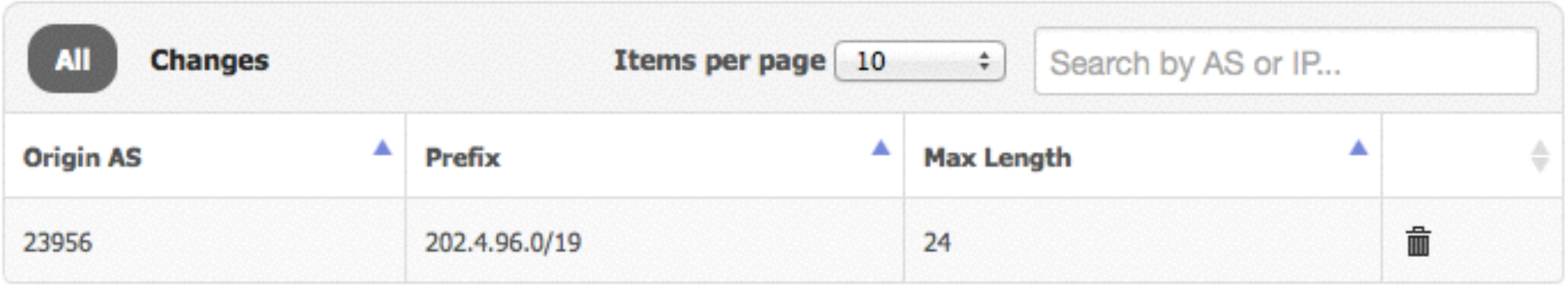
	Origin AS	Prefix
☐	23956	118.179.192.0/19
☐	23956	202.4.96.0/19
☐	23956	2405:7600::/32

- Show available prefix for which you can create ROA

Phase I - Publishing ROA - IPv4

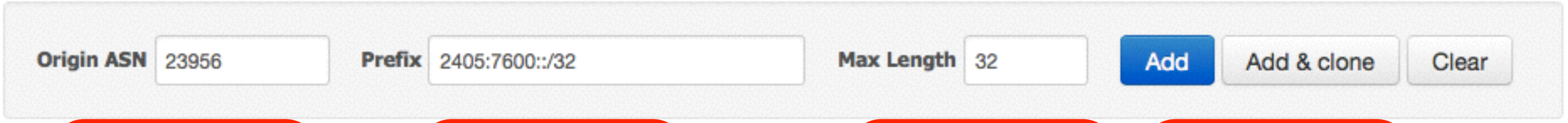


- Create ROA for smaller block.



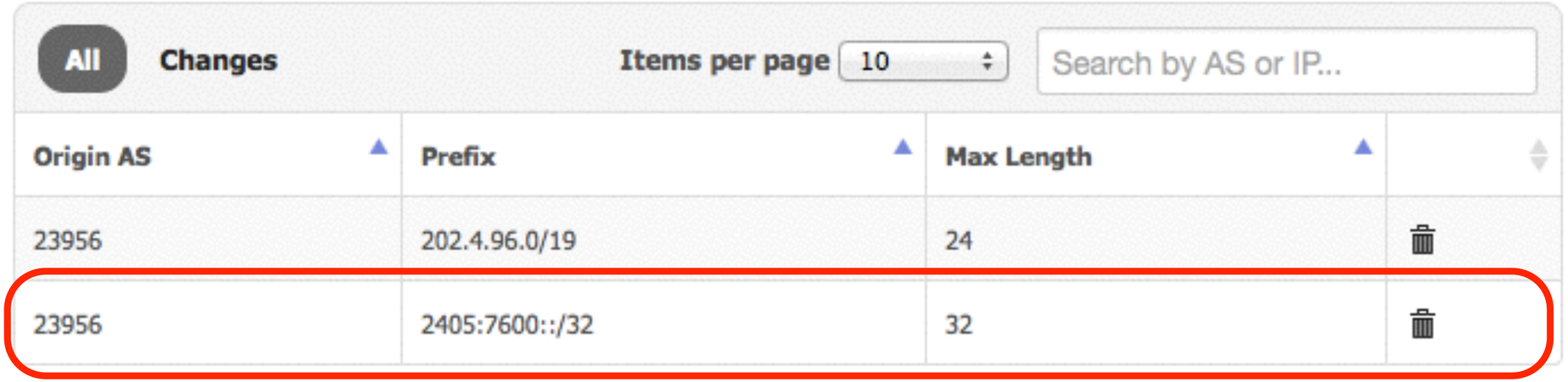
Phase I - Publishing ROA - IPv6

ROA Configuration



1. Write your ASN
2. Your IP Block
3. Subnet
4. Click Add

- ROA for your IPv6 prefix



Phase I - Check your ROA

```
fakrul@access ~> whois -h whois.bgpmon.net 202.4.96.0/24

Prefix:                 202.4.96.0/24
Prefix description:     APT (Dhakacom)
Country code:           BD
Origin AS:              23956
Origin AS Name:         DHAKACOM-BD-AS dhakaCom Limited,BD
RPKI status:            ROA validation successful
First seen:             2013-12-23
Last seen:              2015-07-10
Seen by #peers:         221
```

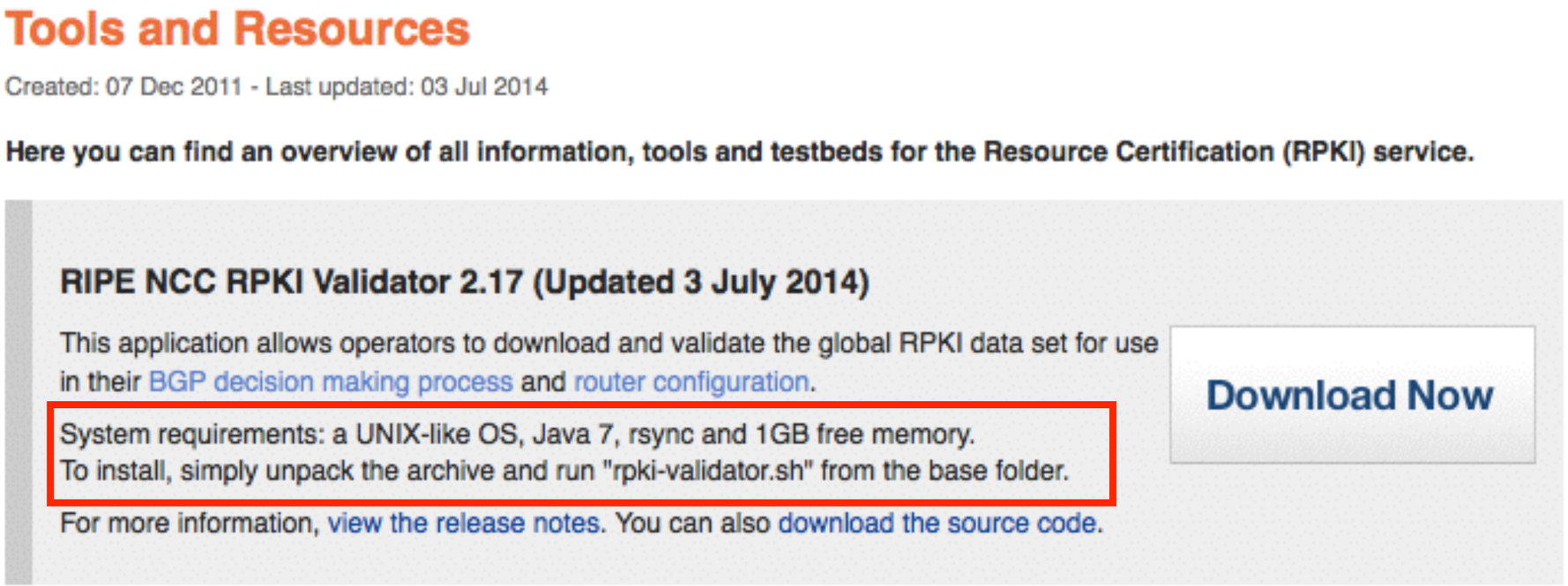
Phase I - Check your ROA

```
fakrul@access ~> whois -h whois.bgpmon.net " --roa 23956 202.4.96.0/24"

0 - Valid
-------------------------
ROA Details
-------------------------
Origin ASN:       AS23956
Not valid Before: 2014-10-21 02:40:16
Not valid After:  2015-12-30 00:00:00  Expires in 172d6h6m23s
Trust Anchor:     rpki.apnic.net
Prefixes:         202.4.96.0/19 (max length /24)
                  2405:7600::/32 (max length /32)
```

Phase II - RPKI Validator

- Download RPKI Validator

http://www.ripe.net/lir-services/resource-management/certification/tools-and-resources

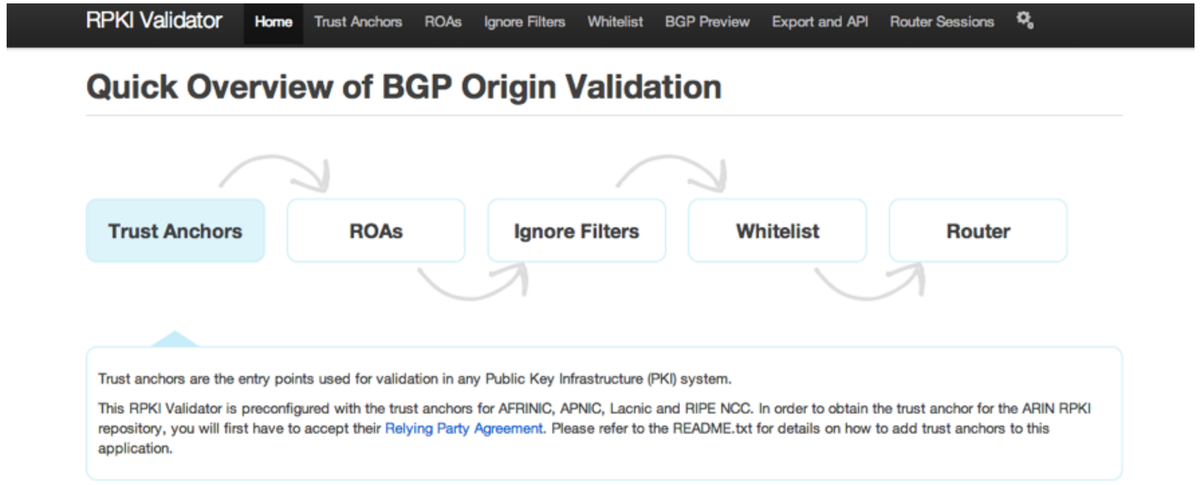


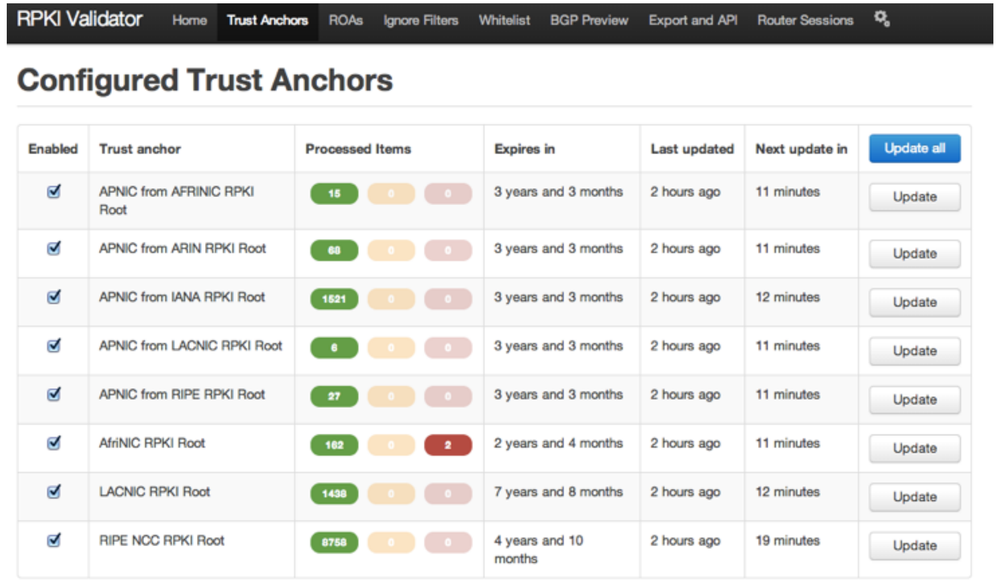
Phase II - RPKI Validator

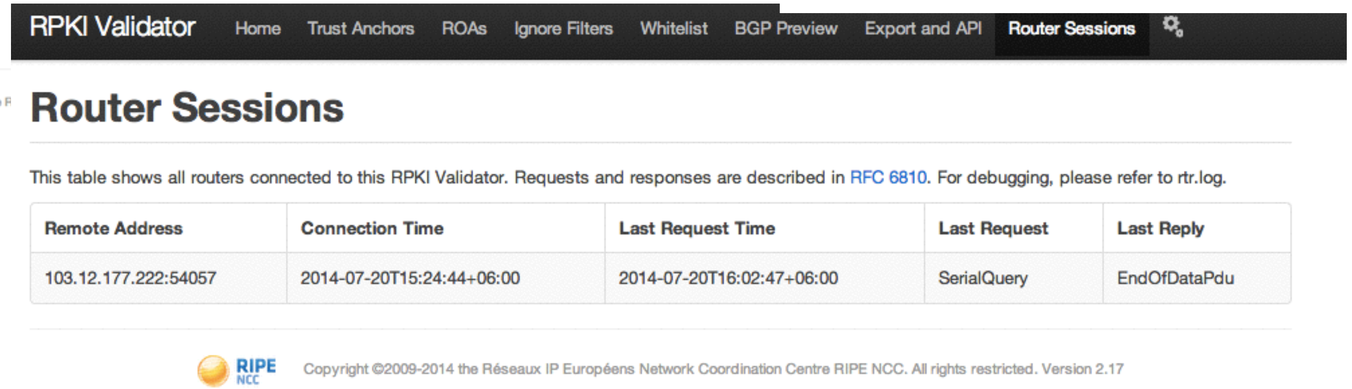
```
# tar -zxvf rpki-validator-app-2.17-dist.tar.gz

# cd rpki-validator-app-2.17

# ./rpki-validator.sh start
```

Phase II - RPKI Validator

http://ip-address:8080







Phase III - Router Configuration

1. Establish session with RPKI Validator

JunOS

```
routing-options {
    validation {
        group RPKI {
            session 103.21.75.10 {
                refresh-time 120;
                hold-time 180;
                port 8282;
                local-address 103.12.75.1;
            }
        }
    }
}
```

Cisco IOS

```
router bgp 64500
  bgp log-neighbor-changes
  bgp rpki server tcp 103.21.75.10 port
8282 refresh 120
```

Phase III - Router Configuration (JunOS)

2. Configure policy to tag ROA

```
policy-options {
    policy-statement ROUTE-VALIDATION {
        term valid {
            from {
                protocol bgp;
                validation-database valid;
            }
            then {
                local-preference 110;
                validation-state valid;
                accept;
            }
        }
        term invalid {
            from {
                protocol bgp;
                validation-database invalid;
            }
            then {
                local-preference 90;
                validation-state invalid;
                accept;
            }
        }
        term unknown {
            from {
                protocol bgp;
                validation-database unknown;
            }
            then {
                local-preference 100;
                validation-state unknown;
                accept;
            }
        }
    }
}
```

Phase III - Router Configuration (Cisco IOS)

2. Configure policy to tag ROA

```
!
route-map ROUTE-VALIDATION permit 10
 match rpki invalid
 set local-preference 90
!
route-map ROUTE-VALIDATION permit 20
 match rpki not-found
 set local-preference 100
!
route-map ROUTE-VALIDATION permit 30
 match rpki valid
 set local-preference 110
```

Phase III - Router Configuration

3. Push policy to the BGP neighbour

JunOS

```
protocols {
    bgp {
        log-updown;
        import ROUTE-VALIDATION;
        group EBGP {
            type external;
            ! other configurations
        }
    }
}
```

Cisco IOS

```
router bgp 64500
  bgp log-neighbor-changes
  !other neighbour related configuration
  neighbor 10.1.1.2 route-map ROUTE-
VALIDATION in
```

Check your prefix

```
fakrul@core01.bdhub.com> show route protocol bgp 202.4.96.0/24

inet.0: 549862 destinations, 549874 routes (549862 active, 0 holddown, 1
hidden)
+ = Active Route, - = Last Active, * = Both

202.4.96.0/24          *[BGP/170] 2d 07:54:43, localpref 110
                          AS path: 58587 58656 23956 I, validation-state: valid
                        > to 103.229.83.9 via ge-1/0/1.0
```

Command

```
fakrul@core01.bdhub.com> show validation session detail

Session 103.21.75.10, State: up, Session index: 2
  Group: RPKI, Preference: 100
  Local IPv4 address: 103.21.75.1, Port: 8282
  Refresh time: 120s
  Hold time: 180s
  Record Life time: 3600s
  Serial (Full Update): 6717
  Serial (Incremental Update): 6717
    Session flaps: 0
    Session uptime: 1w1d 11:36:48
    Last PDU received: 00:00:40
    IPv4 prefix count: 14755
    IPv6 prefix count: 2153
```

Command

```
fakrul@core01.bdhub.com> show validation statistics

Total RV records: 16908
Total Replication RV records: 16908
  Prefix entries: 16304
  Origin-AS entries: 16908
Memory utilization: 3280312 bytes
Policy origin-validation requests: 31825409
  Valid: 784332
  Invalid: 677941
  Unknown: 30363136
BGP import policy reevaluation notifications: 85447
  inet.0, 85447
  inet6.0, 0
```

Command

```
fakrul@core01.bdhub.com> show validation database

RV database for instance master

Prefix                  Origin-AS Session                                   State
41.73.32.0/19-24            37105 103.21.75.10                              valid
41.77.152.0/22-22           32653 103.21.75.10                              valid
41.77.156.0/23-23           32653 103.21.75.10                              valid
41.77.158.0/23-23           37394 103.21.75.10                              valid
41.78.188.0/22-22           37271 103.21.75.10                              valid
41.79.148.0/22-22           37403 103.21.75.10                              valid
41.86.32.0/19-19            36958 103.21.75.10                              valid
2001:43f8:90::/48-128       37708 103.21.75.10                              valid
2001:43f8:92::/48-128       37301 103.21.75.10                              valid
2001:43f8:110::/48-128       37181 103.21.75.10                             valid
```

Command

```
fakrul@core01.bdhub.com> show route protocol bgp validation-state valid

inet.0: 549890 destinations, 549902 routes (549890 active, 0 holddown, 1 hidden)
+ = Active Route, - = Last Active, * = Both

2.0.0.0/16          *[BGP/170] 1d 06:25:16, localpref 110
                       AS path: 58587 6453 5511 3215 I, validation-state: valid
                     > to 103.229.83.9 via ge-1/0/1.0
2.1.0.0/16          *[BGP/170] 1d 06:25:16, localpref 110
                       AS path: 58587 6453 5511 3215 I, validation-state: valid
                     > to 103.229.83.9 via ge-1/0/1.0
2.2.0.0/16          *[BGP/170] 1d 06:25:16, localpref 110
                       AS path: 58587 6453 5511 3215 I, validation-state: valid
                     > to 103.229.83.9 via ge-1/0/1.0
2.3.0.0/16          *[BGP/170] 1d 06:25:16, localpref 110
                       AS path: 58587 6453 5511 3215 I, validation-state: valid
                     > to 103.229.83.9 via ge-1/0/1.0
```

Command

```
fakrul@core01.bdhub.com> show route protocol bgp validation-state invalid

inet.0: 549895 destinations, 549907 routes (549895 active, 0 holddown, 1 hidden)
+ = Active Route, - = Last Active, * = Both

5.152.160.0/24     *[BGP/170] 4d 07:18:39, localpref 90
                      AS path: 58587 9498 20804 59472 I, validation-state: invalid
                    > to 103.229.83.9 via ge-1/0/1.0
5.152.161.0/24     *[BGP/170] 4d 07:18:40, localpref 90
                      AS path: 58587 9498 20804 59472 ?, validation-state: invalid
                    > to 103.229.83.9 via ge-1/0/1.0
5.152.163.0/24     *[BGP/170] 4d 07:18:40, localpref 90
                      AS path: 58587 9498 20804 59472 ?, validation-state: invalid
                    > to 103.229.83.9 via ge-1/0/1.0
5.152.164.0/24     *[BGP/170] 4d 07:18:39, localpref 90
                      AS path: 58587 9498 20804 59472 I, validation-state: invalid
                    > to 103.229.83.9 via ge-1/0/1.0
```

!Caution!

- Make sure that your router IOS is bug free for RPKI; other wise….

```
CMD: 'show ip bgp ' 18:26:21 BDT Mon Mar 17 2014

CMD: 'show ip bgp ' 18:26:34 BDT Mon Mar 17 2014

CMD: 'show ip bgp ' 18:27:55 BDT Mon Mar 17 2014

CMD: 'show ip bgp ' 18:29:20 BDT Mon Mar 17 2014

CMD: 'show ip bgp rpki table ' 18:29:31 BDT Mon Mar 17 2014

CMD: 'show ip bgp rpki servers ' 18:29:34 BDT Mon Mar 17 2014

CMD: 'show ip bgp rpki table ' 18:29:49 BDT Mon Mar 17 2014

Exception to IOS Thread:
Frame pointer 0x7F3A8AA51EE0, PC = 0x8DA4DA

UNIX-EXT-SIGNAL: Segmentation fault(11), Process = BGP Router
-Traceback= 1#270a78af3c82800fb448b5d32a66d575  :400000+4DA4DA :400000+73AB56B :4000(
400000+4980EA :400000+4A64DD :400000+496ED5

Fastpath Thread backtrace:
-Traceback= 1#270a78af3c82800fb448b5d32a66d575  c:7F3B7C28C000+BDDD2

Auxiliary Thread backtrace:
-Traceback= 1#270a78af3c82800fb448b5d32a66d575  pthread:7F3B774EB000+A7E9

RAX = 0000000000000008  RBX = 00007F3A8AA520A0
RCX = 8039F30F00000000  RDX = 0000000000000000
RSP = 00007F3A8AA51EE0  RBP = 00007F3A8AA51FE0
RSI = A020A58A3A7F0000  RDI = D8803CB53A7F0000
R8  = A020A58A3A7F0000  R9  = 00007F3AB53C80D8
R10 = 00007F3A83A6B221  R11 = 0000000000000001
R12 = 00007F3AB53C80D8  R13 = 00007F3A8AA52110
R14 = FFF7000600000000  R15 = 00007F3A8AA52094
RFL = 0000000000010293  RIP = 00000000008DA4DA
CS = 0033  FS = 0000  GS = 0000
ST0 = 0000 0000000000000000  ST1 = 0000 0000000000000000
ST2 = 0000 0000000000000000  ST3 = 0000 0000000000000000
ST4 = 0000 0000000000000000  ST5 = 0000 0000000000000000
ST6 = 0000 0000000000000000  ST7 = 0000 0000000000000000
X87CW = 037F  X87SW = 0000  X87TG = 0000  X87OP = 0000
X87IP = 0000000000000000  X87DP = 0000000000000000
XMM0  = A81F718A3A7F00009802598A3A7F0000
```

Check your prefix

Cisco (hosted by the RIPE NCC)

Public Cisco router: rpki-rtr.ripe.net

Telnet username: ripe / No password

Juniper (hosted by Kaia Global Networks)

Public Juniper routers: 193.34.50.25, 193.34.50.26

Telnet username: rpki / Password: testbed

source : http://www.ripe.net/lir-services/resource-management/certification/tools-and-resources

Configuration - Reference Link

Cisco

http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_bgp/command/irg-cr-book/bgp-m1.html#wp3677719851

Juniper

http://www.juniper.net/techpubs/en_US/junos12.2/topics/topic-map/bgp-origin-as-validation.html


READY TO
ROA
http://www.apnic.net/roa
APNIC

RPKI Demo