

RPKI

Resource Public Key Infrastructure

SANOG XXV | 16-24 January, 2015 | Kandy, Sri Lanka



Fakrul Alam



fakrul@bdhub.com



<http://bd.linkedin.com/in/fakrulalam>



<https://twitter.com/rapappu>

Target Audience

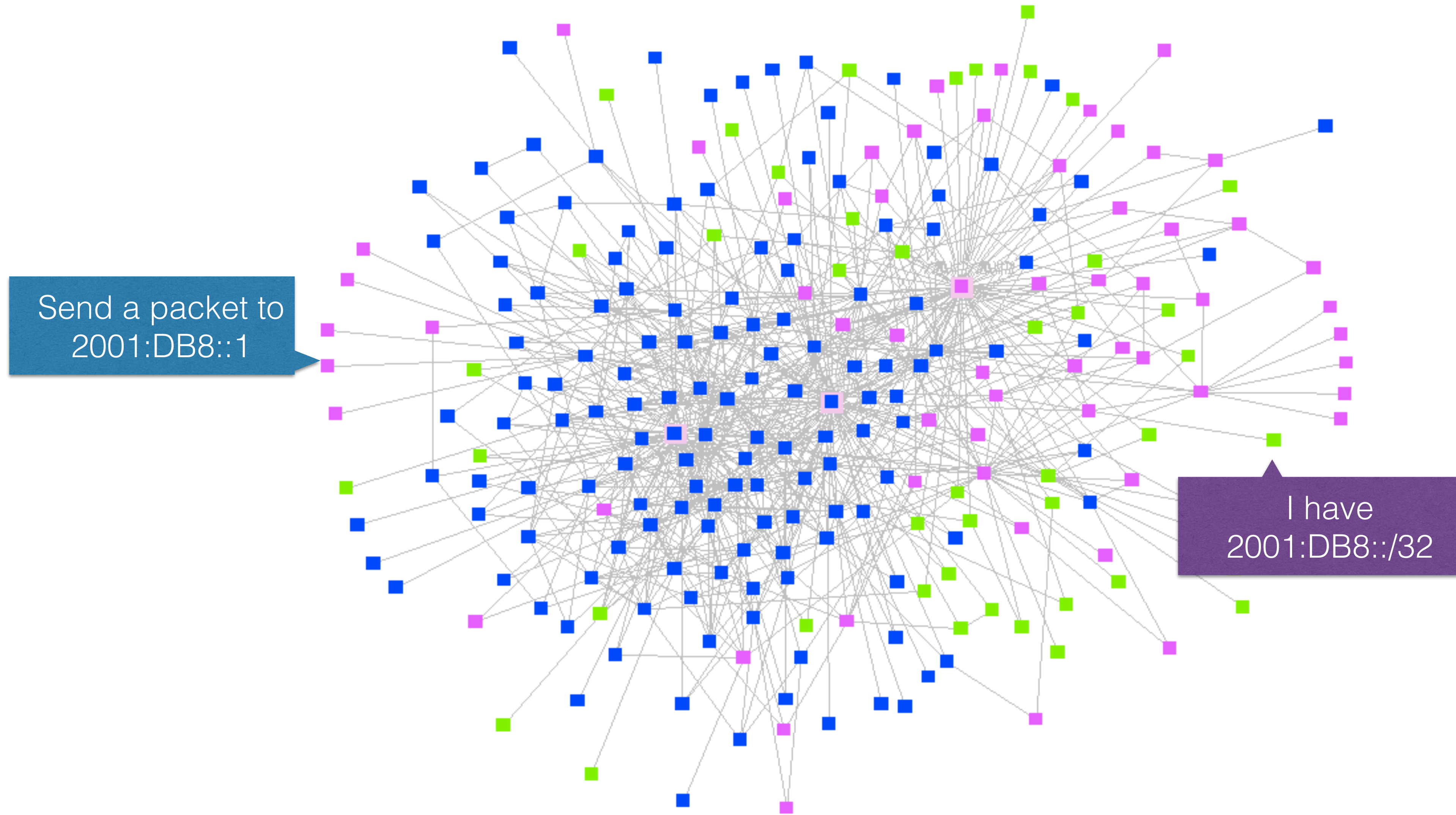
- Knowledge of Internet Routing(specially BGP)
- Familiar with any IRR Database
- No need to know Cryptography
- Basic knowledge of PKI(Public Key Infrastructure)

Agenda

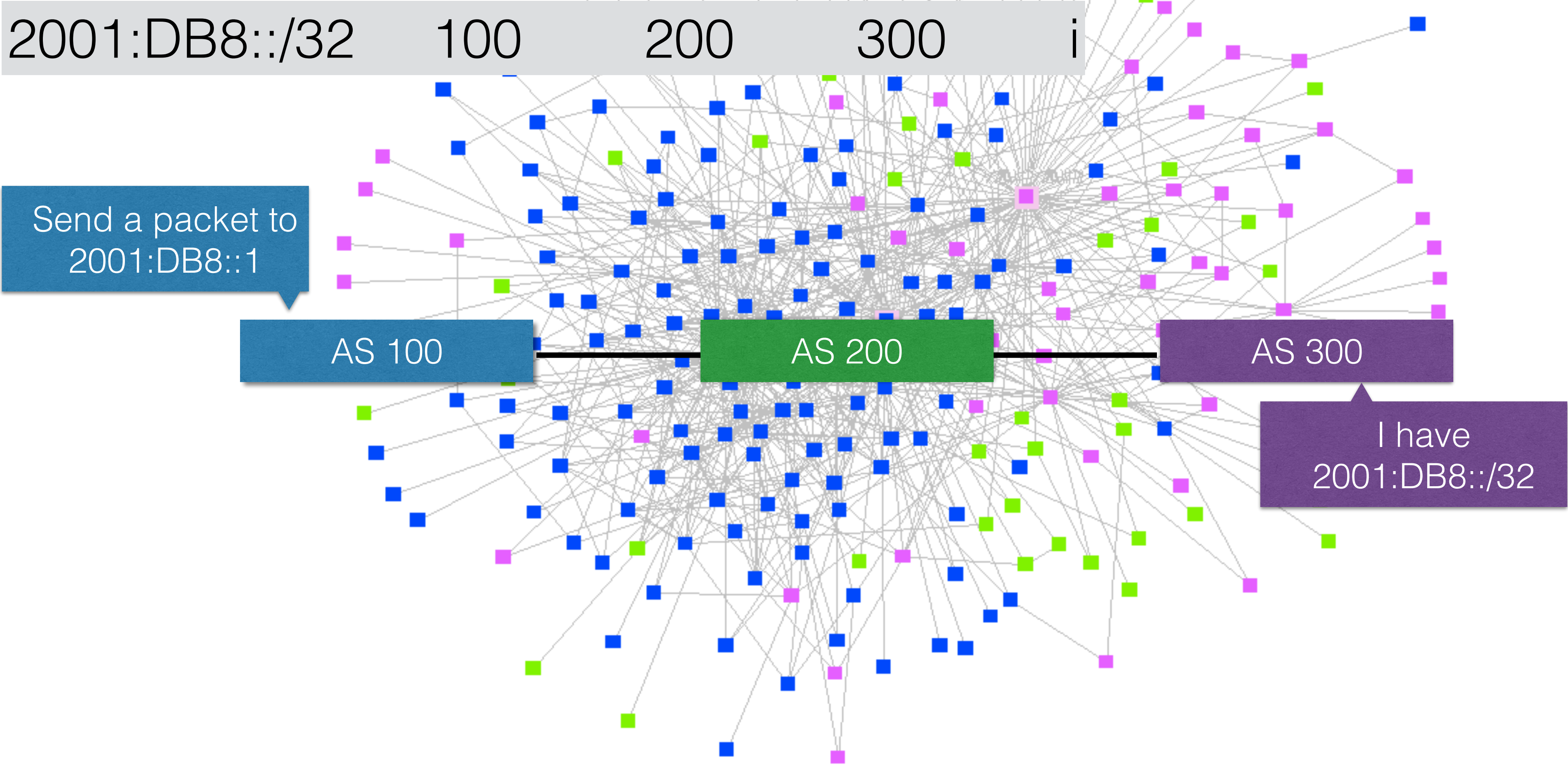
- BGP / RPKI
- Configuration
- Hands-on Lab (Juniper)

BGP

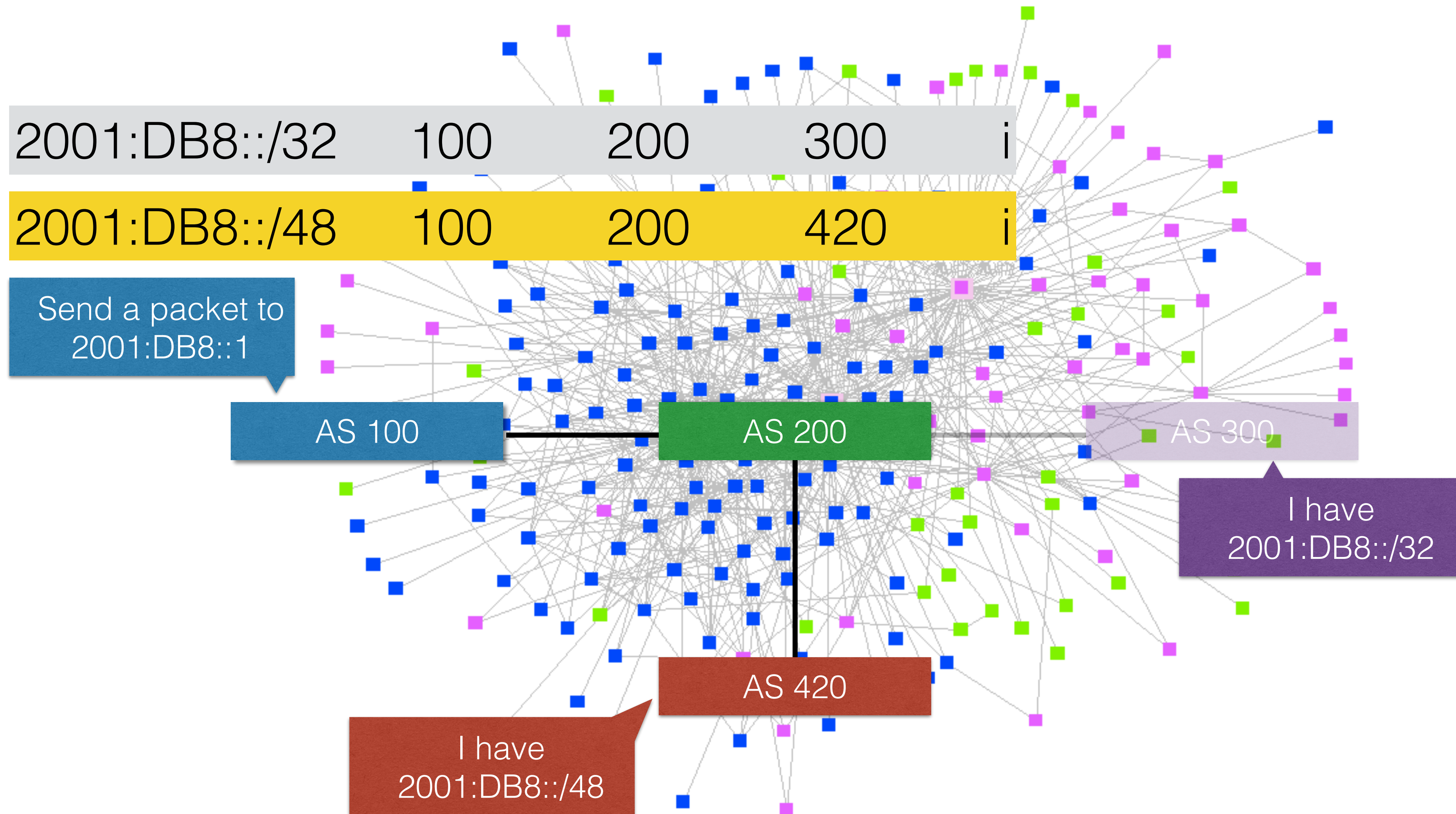
BGP (AS)



AS Path



AS Path



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

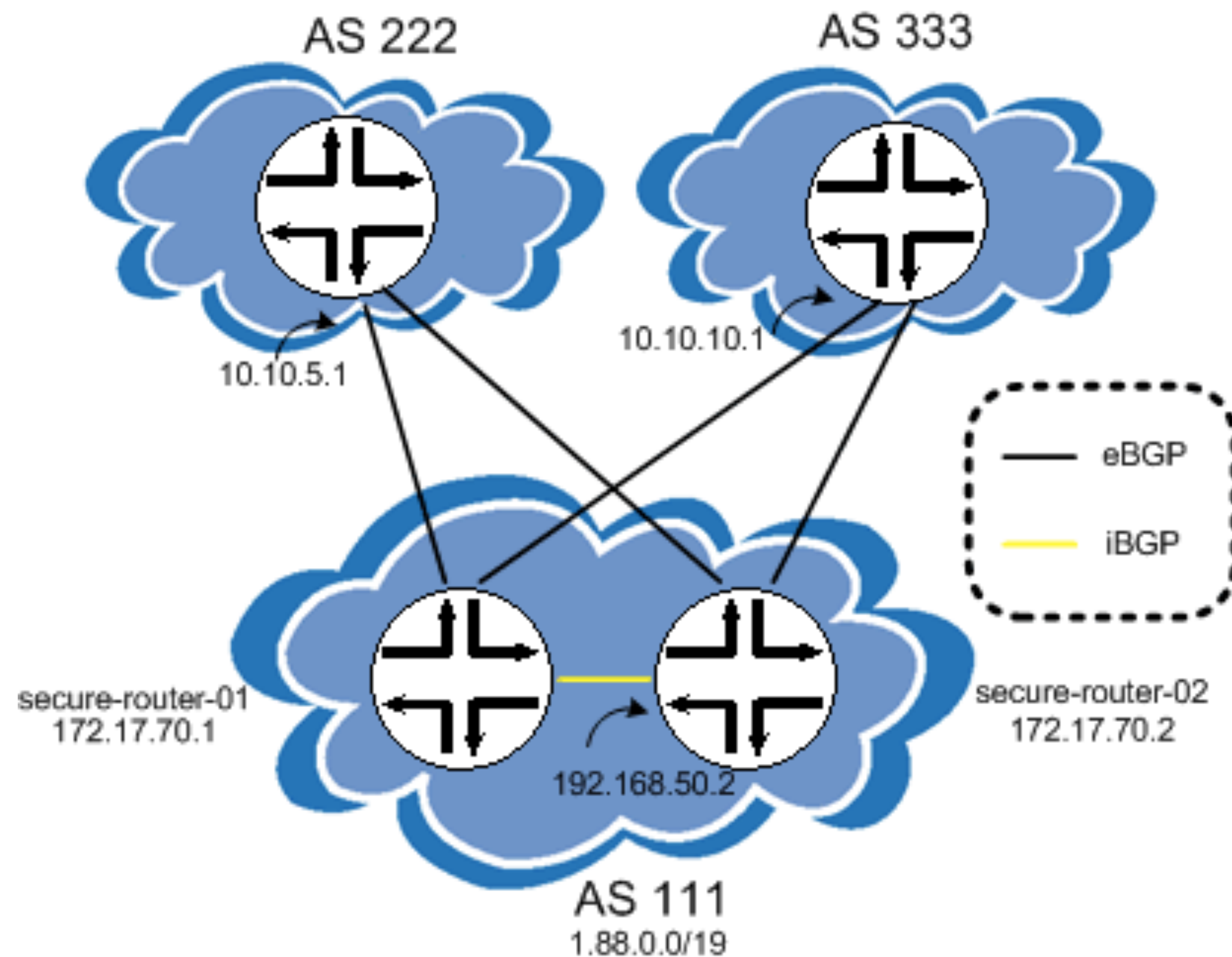
Historical Incident

- 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

Internet Routing Registry

- 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

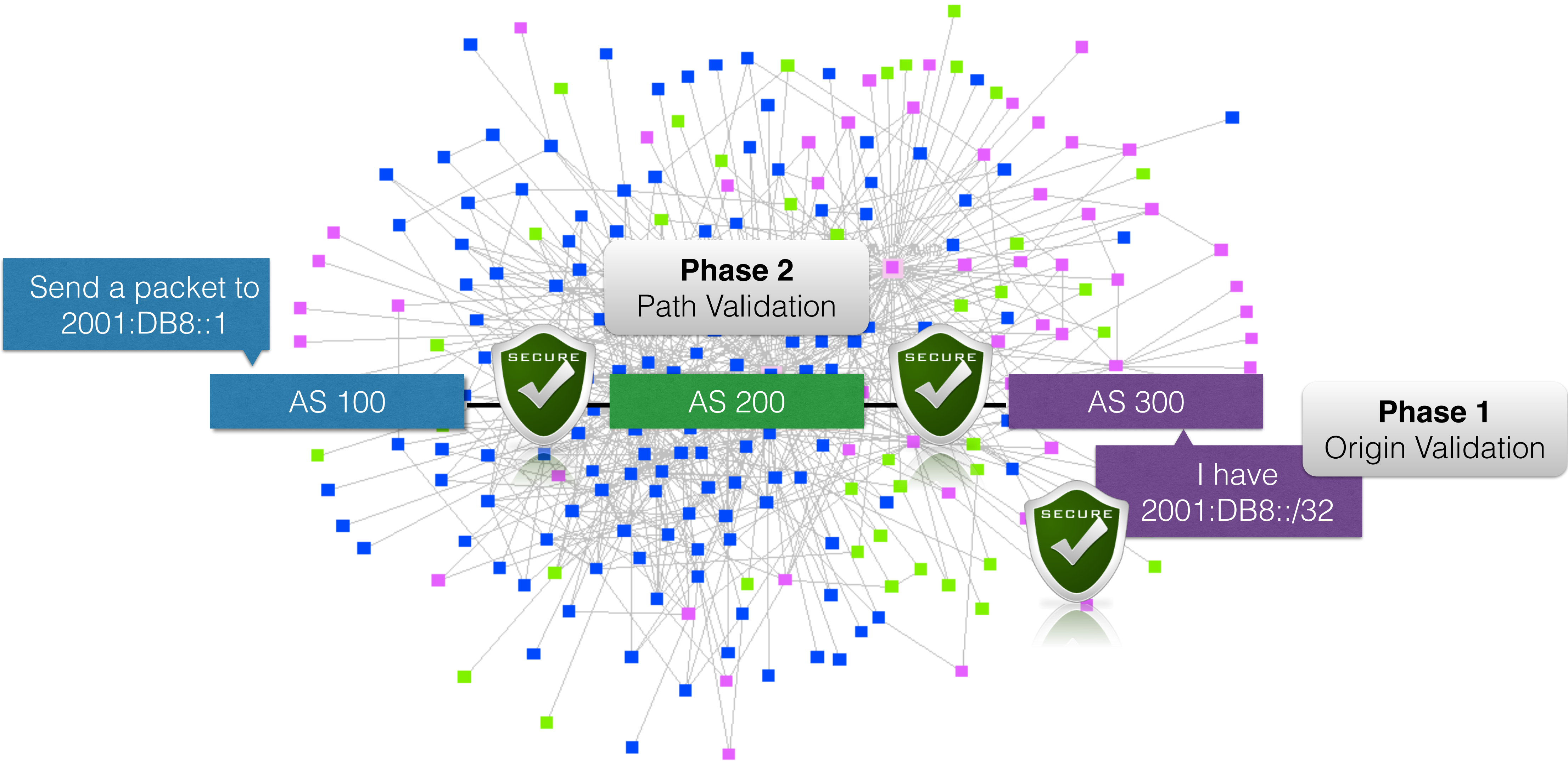
RPKI

Resource Public Key Infrastructure

IP Address & AS Numbers

Digital Certificate

RPKI Deployment



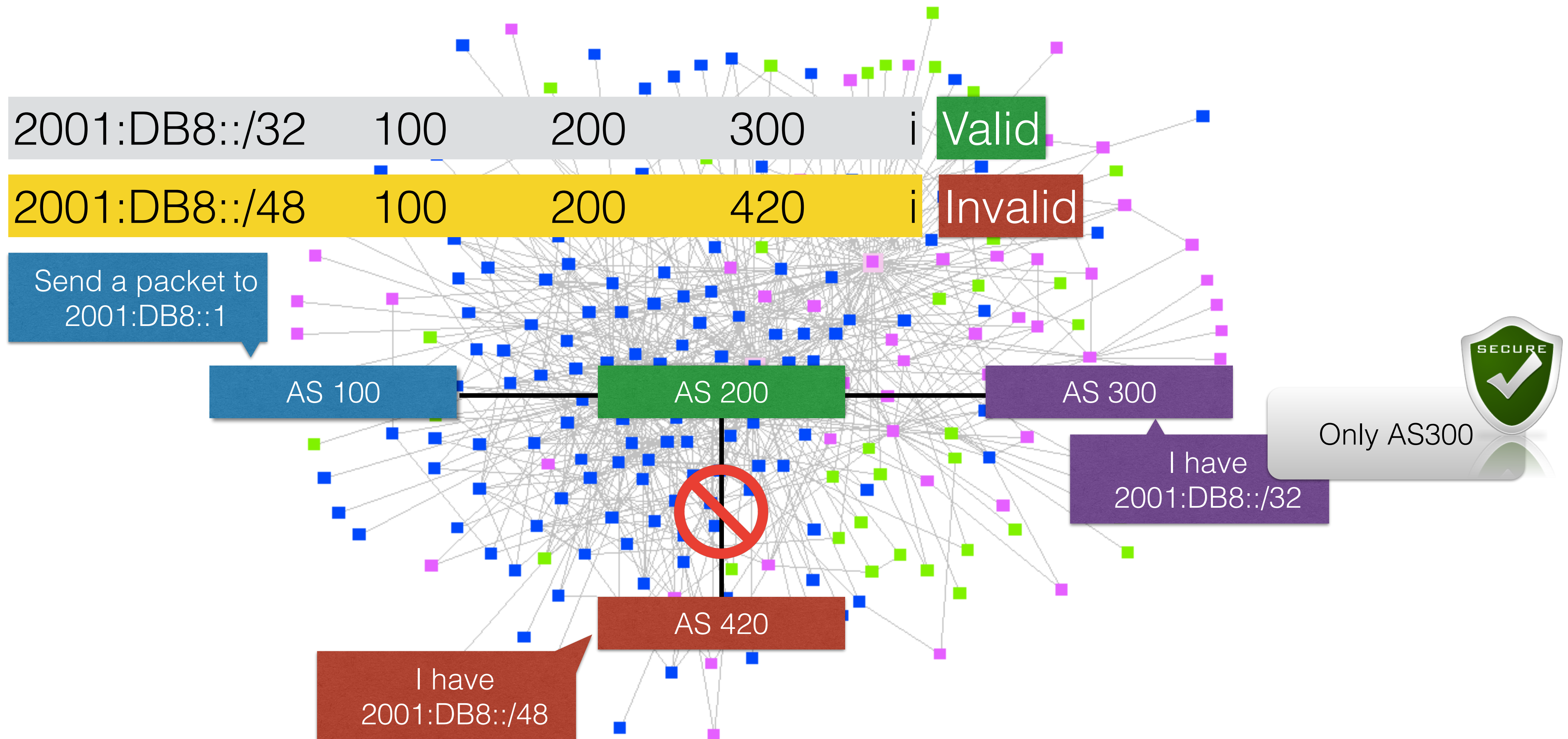
Goals of RPKI

- 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 Origin Validation



RPKI Building Blocks

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

Let's discuss these building blocks in
details

PKI & Trust Anchors

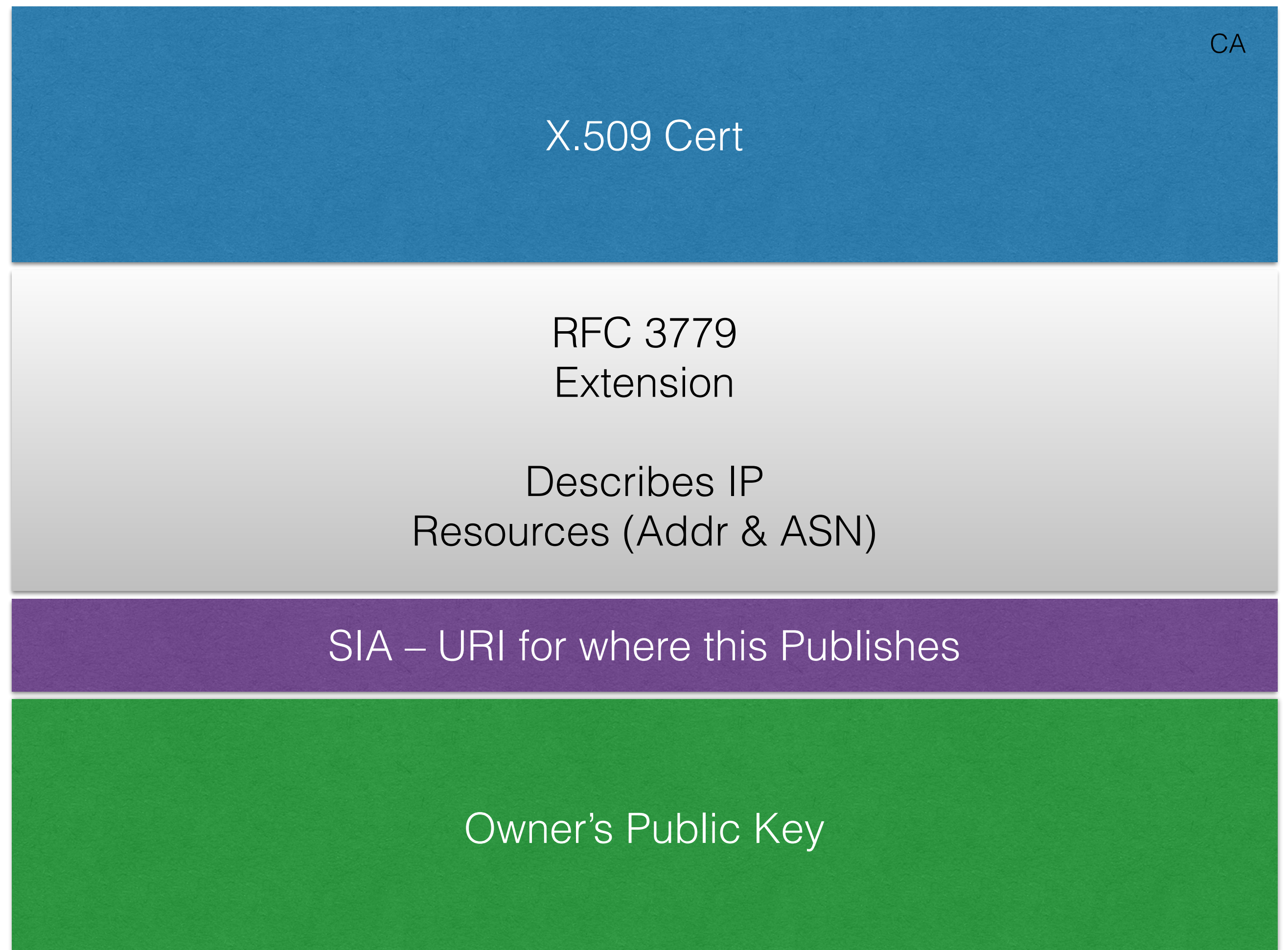
Public Key Concept

- **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

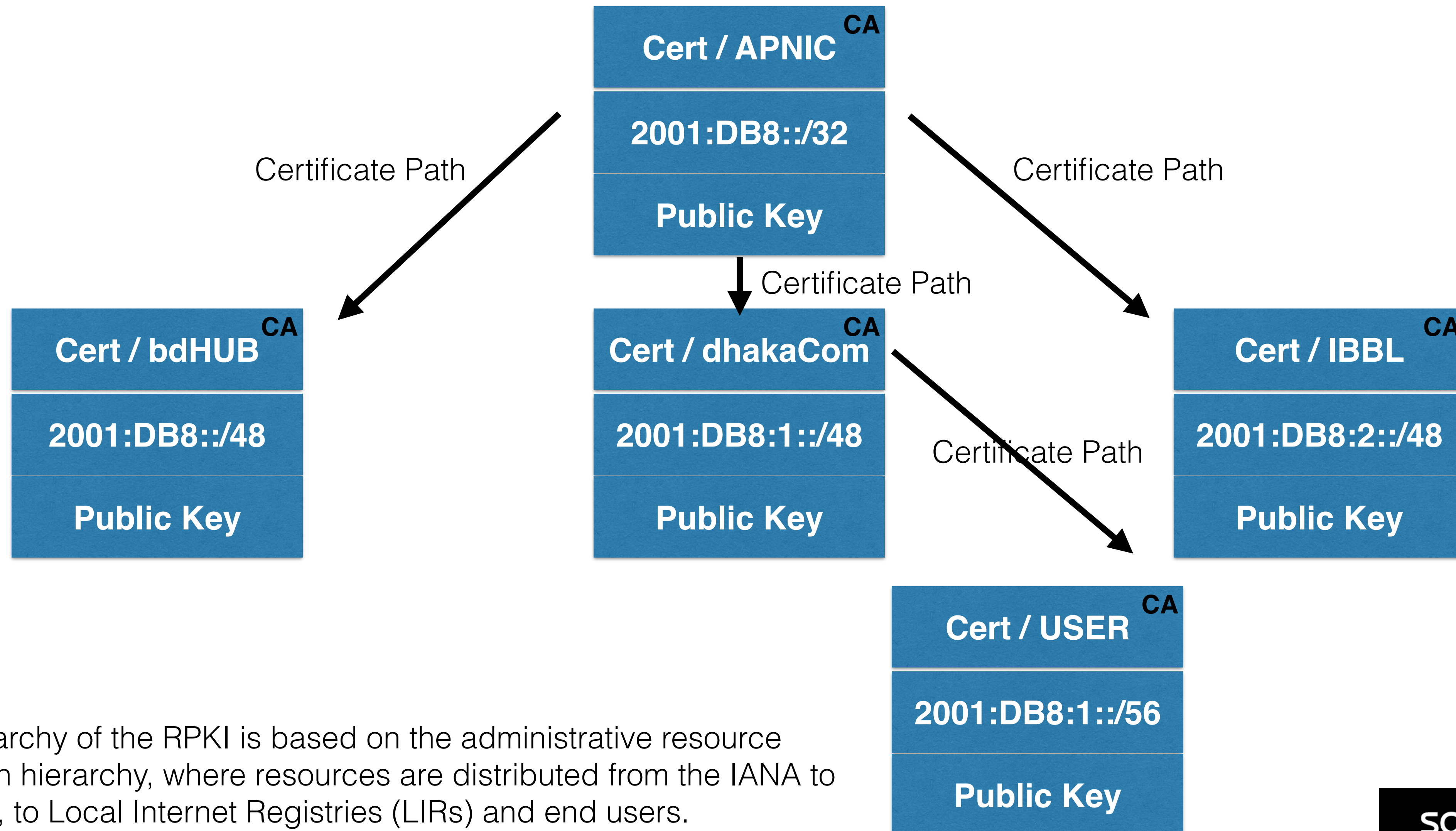
X.509 Certificates 3779 EXT

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

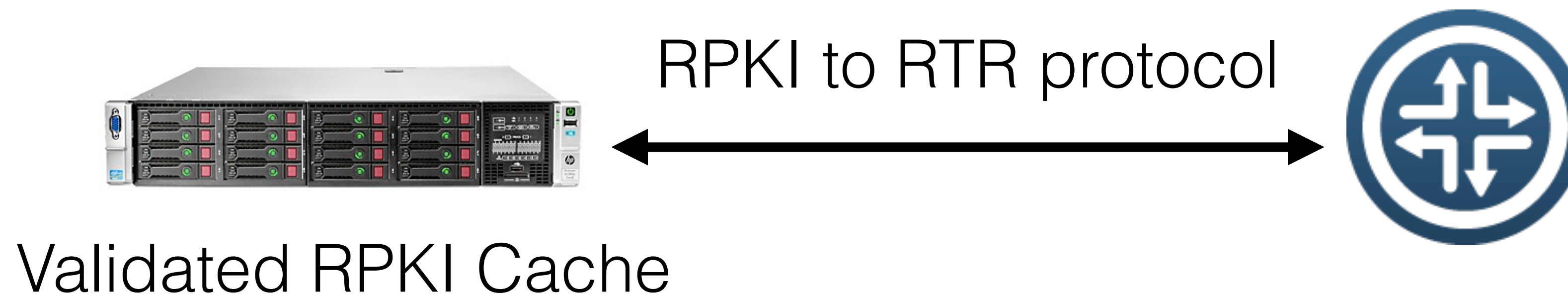
Route Origination Authorizations (ROA)

- 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

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

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.

FAQ: Microsoft's security breach and how it affects you

 story

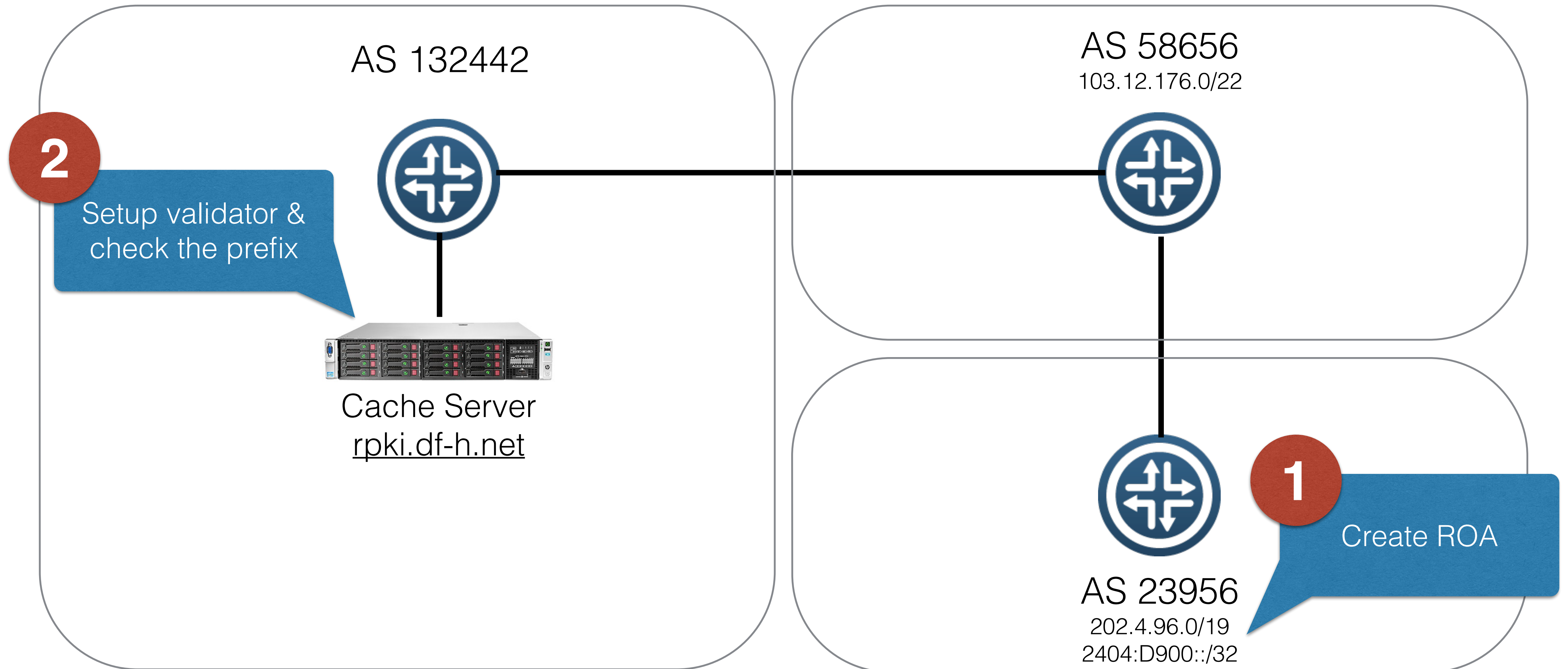
Such certificates are critical for businesses and consumers who download patches, updates and other pieces of software from the Internet, because they verify that the software is being supplied from a particular company, such as Microsoft.

RPKI Further Reading

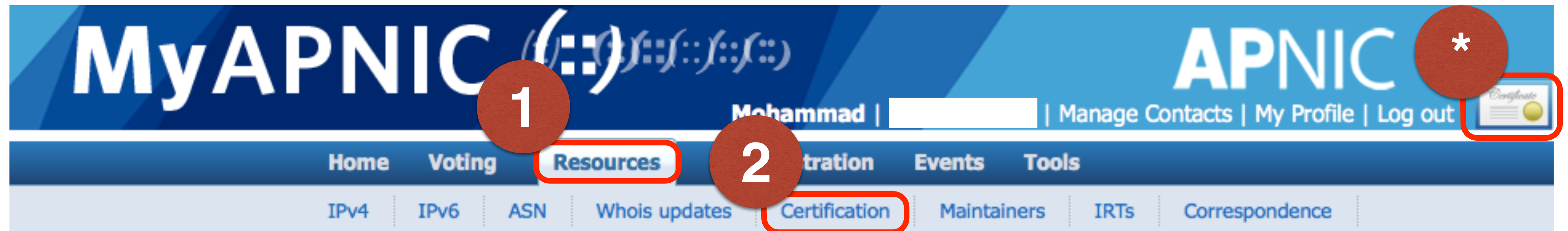
- RFC 5280: X.509 PKI Certificates
- RFC 3779: Extensions for IP Addresses and ASNs
- RFC 6481-6493: Resource Public Key Infrastructure

RPKI Configuration

Topology for Origin Validation

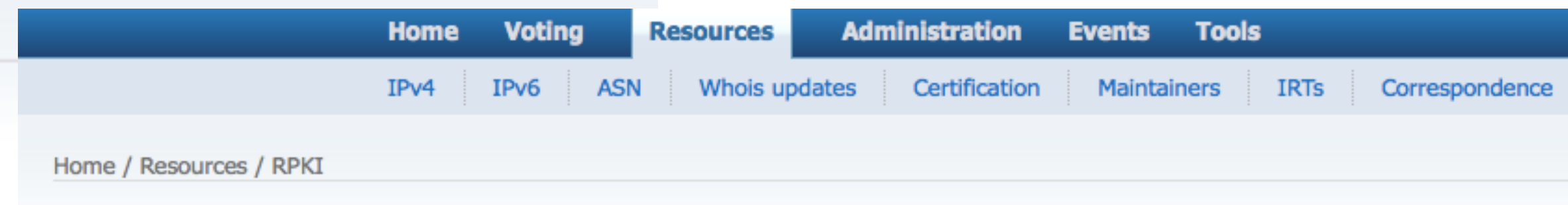


Phase I - Publishing ROA



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

Phase I - Publishing ROA



Enable Resource Certification

2 Currently, you have not enabled resource certification for your registry.

I want to operate in the MyAPNIC RPKI portal.

I want to host my own certification authority and run an RPKI engine myself.

Next

Enable Hosted Resource Certification

Currently, you have not enabled resource certification for your registry.

Terms and Conditions of APNIC Certification Authority

Article 1 - Definitions

In the Terms and Conditions, unless the context requires otherwise, the following terms have the meanings assigned to them below:

APNIC - APNIC Pty Ltd ACN 081 528 010 (a company incorporated under the laws of Australia), the Asia Pacific Network Information Centre

APNIC Certification Service - The APNIC service through which the Certificates are generated and RPKI signed objects are created

Certificate - Digitally signed data object generated by the APNIC Certification Service

CRLs or Certificate Revocation Lists - Lists, or lists of serial numbers, for Certificates that have

3 I accept. Create my Certification Authority

Phase I - Publishing ROA

RPKI

BGP Route Validity

All Items per page 10 Search by AS or IP...

<input type="checkbox"/>	Origin AS	Prefix
<input type="checkbox"/>	23956	118.179.192.0/19
<input type="checkbox"/>	23956	202.4.96.0/19
<input type="checkbox"/>	23956	2405:7600::/32

- Show available prefix for which you can create ROA

Phase I - Publishing ROA - IPv4

ROA Configuration

Origin ASN Prefix Max Length

1. Write your ASN

2. Your IP Block

3. Subnet

4. Click Add

- Create ROA for smaller block.

All Changes		Items per page	10	Search by AS or IP...
Origin AS	Prefix	Max Length		
23956	202.4.96.0/19	24		

Phase I - Publishing ROA - IPv6

ROA Configuration

Origin ASN Prefix Max Length

1. Write your ASN

2. Your IP Block

3. Subnet

4. Click Add

- ROA for your IPv6 prefix

All Changes		Items per page	10	Search by AS or IP...
Origin AS	Prefix	Max Length		
23956	202.4.96.0/19	24		
23956	2405:7600::/32	32		

Phase I - Check your ROA

```
# 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:            2014-07-20
Seen by #peers:       203
```

Phase I - Check your ROA

```
# whois -h whois.bgpmon.net " --roa 23956 202.4.96.0/24"
```

```
0 - Valid
```

```
-----  
ROA Details  
-----
```

```
Origin ASN:
```

```
AS23956
```

```
Not valid Before: 2014-07-20 15:20:10
```

```
Not valid After: 2014-12-30 00:00:00 Expires in 161d12h52m42s
```

```
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>

Tools and Resources

Created: 07 Dec 2011 - Last updated: 03 Jul 2014

Here you can find an overview of all information, tools and testbeds for the Resource Certification (RPKI) service.

RIPE NCC RPKI Validator 2.17 (Updated 3 July 2014)

This application allows operators to download and validate the global RPKI data set for use in their [BGP decision making process](#) and [router configuration](#).

System requirements: a UNIX-like OS, Java 7, rsync and 1GB free memory.
To install, simply unpack the archive and run "rpk-validator.sh" from the base folder.

For more information, [view the release notes](#). You can also [download the source code](#).

[Download Now](#)

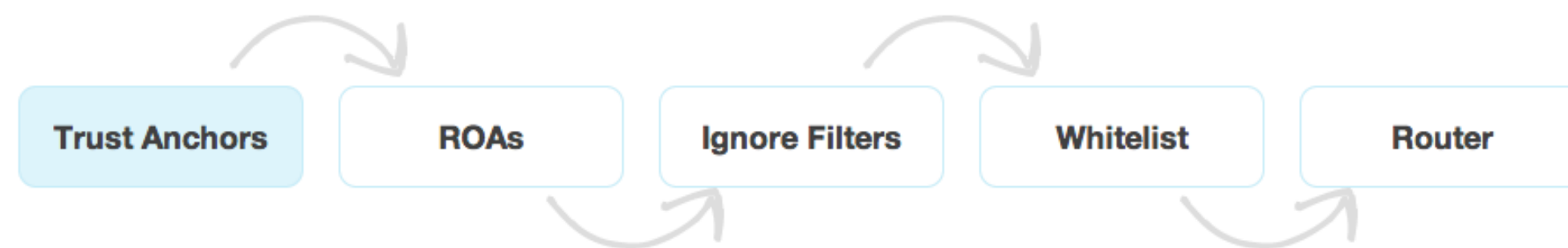
Phase II - RPKI Validator

```
# 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

Quick Overview of BGP Origin Validation



Trust anchors are the entry points used for validation in any Public Key Infrastructure (PKI) system.

This RPKI Validator is preconfigured with the trust anchors for AFRINIC, APNIC, Lacinic and RIPE NCC. In order to obtain the trust anchor for the ARIN RPKI repository, you will first have to accept their [Relying Party Agreement](#). Please refer to the README.txt for details on how to add trust anchors to this application.

Configured Trust Anchors

Enabled	Trust anchor	Processed Items	Expires in	Last updated	Next update in	Update all
<input checked="" type="checkbox"/>	APNIC from AFRINIC RPKI Root	15 0 0	3 years and 3 months	2 hours ago	11 minutes	Update
<input checked="" type="checkbox"/>	APNIC from ARIN RPKI Root	68 0 0	3 years and 3 months	2 hours ago	11 minutes	Update
<input checked="" type="checkbox"/>	APNIC from IANA RPKI Root	1521 0 0	3 years and 3 months	2 hours ago	12 minutes	Update
<input checked="" type="checkbox"/>	APNIC from LACNIC RPKI Root	6 0 0	3 years and 3 months	2 hours ago	11 minutes	Update
<input checked="" type="checkbox"/>	APNIC from RIPE RPKI Root	27 0 0	3 years and 3 months	2 hours ago	11 minutes	Update
<input checked="" type="checkbox"/>	AfriNIC RPKI Root	162 0 2	2 years and 4 months	2 hours ago	11 minutes	Update
<input checked="" type="checkbox"/>	LACNIC RPKI Root	1438 0 0	7 years and 8 months	2 hours ago	12 minutes	Update
<input checked="" type="checkbox"/>	RIPE NCC RPKI Root	8758 0 0	4 years and 10 months	2 hours ago	19 minutes	Update

Router Sessions

This table shows all routers connected to this RPKI Validator. Requests and responses are described in [RFC 6810](#). For debugging, please refer to rtr.log.

Remote Address	Connection Time	Last Request Time	Last Request	Last Reply
103.12.177.222:54057	2014-07-20T15:24:44+06:00	2014-07-20T16:02:47+06:00	SerialQuery	EndOfDataPdu

Phase III - Router Configuration (Juniper)

1. Establish session with RPKI Validator

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

Phase III - Router Configuration (Juniper)

2. Configure policy to tag valid ROA

```
policy-options {  
    policy-statement route-validation {  
        term valid {  
            from {  
                protocol bgp;  
                validation-database valid;  
            }  
            then {  
                validation-state valid;  
                accept;  
            }  
        }  
    }  
}
```

Phase III - Router Configuration (Juniper)

3. Push policy to the BGP neighbor

```
protocols {  
    bgp {  
        log-updown;  
  
        import route-validation;  
  
        group EBGP {  
            type external;  
  
            |  
            | other configurations  
            |  
        }  
    }  
}
```


Check your prefix

```
fakrul@rpki-test> show route protocol bgp 202.4.96.0/24
```

```
inet.0: 506658 destinations, 506659 routes (506656 active, 0 holddown, 2 hidden)
```

```
+ = Active Route, - = Last Active, * = Both
```

```
202.4.96.0/24
```

```
*[BGP/170] 01:42:11, localpref 100
```

```
AS path: 58656 23956 I, validation-state: valid
```

```
> to 103.12.177.221 via ge-1/0/9.0
```

Command

```
#show validation session
```

```
fakrul@rpki-test> show validation session
```

Session	State	Flaps	Uptime	#IPv4/IPv6 records
103.21.75.10	Up	0	1d 09:33:54	9728/1431

Command

```
#show validation statistics
```

```
fakrul@rpki-test> Total RV records: 13529
```

```
Total Replication RV records: 13529
```

```
    Prefix entries: 13050
```

```
    Origin-AS entries: 13529
```

```
Memory utilization: 2626782 bytes
```

```
Policy origin-validation requests: 0
```

```
    Valid: 0
```

```
    Invalid: 0
```

```
    Unknown: 0
```

```
BGP import policy reevaluation notifications: 37818
```

```
    inet.0, 37818
```

```
    inet6.0, 0
```

Command

#show validation database

```
fakrul@rpki-test> show validation database
```

```
RV database for instance master
```

Prefix	Origin-AS	Session	State	Mismatch
2.0.0.0/12-16	3215	202.4.96.100	valid	
2.0.0.0/16-16	3215	202.4.96.100	valid	
2.1.0.0/16-16	3215	202.4.96.100	valid	
2.2.0.0/16-16	3215	202.4.96.100	valid	
2.3.0.0/16-16	3215	202.4.96.100	valid	
2.4.0.0/16-16	3215	202.4.96.100	valid	
2.5.0.0/16-16	3215	202.4.96.100	valid	
2.6.0.0/16-16	3215	202.4.96.100	valid	

Command

```
#show route protocol bgp validation-state valid
```

```
fakrul@rpki-test> show route protocol bgp validation-state valid
```

```
inet.0: 506561 destinations, 506562 routes (506559 active, 0 holddown, 2 hidden)
```

```
+ = Active Route, - = Last Active, * = Both
```

```
2.0.0.0/16      *[BGP/170] 1d 10:26:39, localpref 100
```

```
    AS path: 58656 6453 5511 3215 I, validation-state: valid
```

```
    > to 103.12.177.221 via ge-1/0/9.0
```

```
2.1.0.0/16      *[BGP/170] 1d 10:26:39, localpref 100
```

```
    AS path: 58656 6453 5511 3215 I, validation-state: valid
```


!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 rpk table ' 18:29:31 BDT Mon Mar 17 2014
CMD: 'show ip bgp rpk servers ' 18:29:34 BDT Mon Mar 17 2014
CMD: 'show ip bgp rpk 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 :400000+4980EA :400000+4A64DD :400000+496ED5
```

```
Fastpath Thread backtrace:
-Traceback= 1#270a78af3c82800fb448b5d32a66d575 c:7F3B7C28C000+BD0D2
```

```
Auxiliary Thread backtrace:
-Traceback= 1#270a78af3c82800fb448b5d32a66d575 pthread:7F3B774EB000+A7C9
```

```
RAX = 0000000000000000 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 = 00000000000010293 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
```

```
18:26:34 BDT Mon Mar 17 2014
ogp ' 18:27:55 BDT Mon Mar 17 2014
JW ip bgp ' 18:29:20 BDT Mon Mar 17 2014
'show ip bgp rpk table ' 18:29:31 BDT Mon Mar 17 2014
J: 'show ip bgp rpk servers ' 18:29:34 BDT Mon Mar 17 2014
.MD: 'show ip bgp rpk 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+5BF6C4 :400000+5BCAD5 :400000+4980EA :400000+4A64DD :400000+496ED5
```

```
Fastpath Thread backtrace:
-Traceback= 1#270a78af3c82800fb448b5d32a66d575 c:7F3B7C28C000+BD0D2
```

```
Auxiliary Thread backtrace:
-Traceback= 1#270a78af3c82800fb448b5d32a66d575 pthread:7F3B774EB000+A7C9
```

```
RAX = 0000000000000000 RBX = 00007F3A8AA520A0
RCX = 8039F30F00000000 RDX = 0000000000000000
RSP = 00007F3A8AA51EE0 RBP = 00007F3A8AA51FE0
RSI = A020A58A3A7F0000 RDI = D8803CB53A7F0000
```

Check your prefix

Cisco (hosted by the RIPE NCC)

Public Cisco router: rпки-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: rпки / Password: testbed

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
ROAR**



<http://www.apnic.net/roa>

APNIC

RPKI Demo