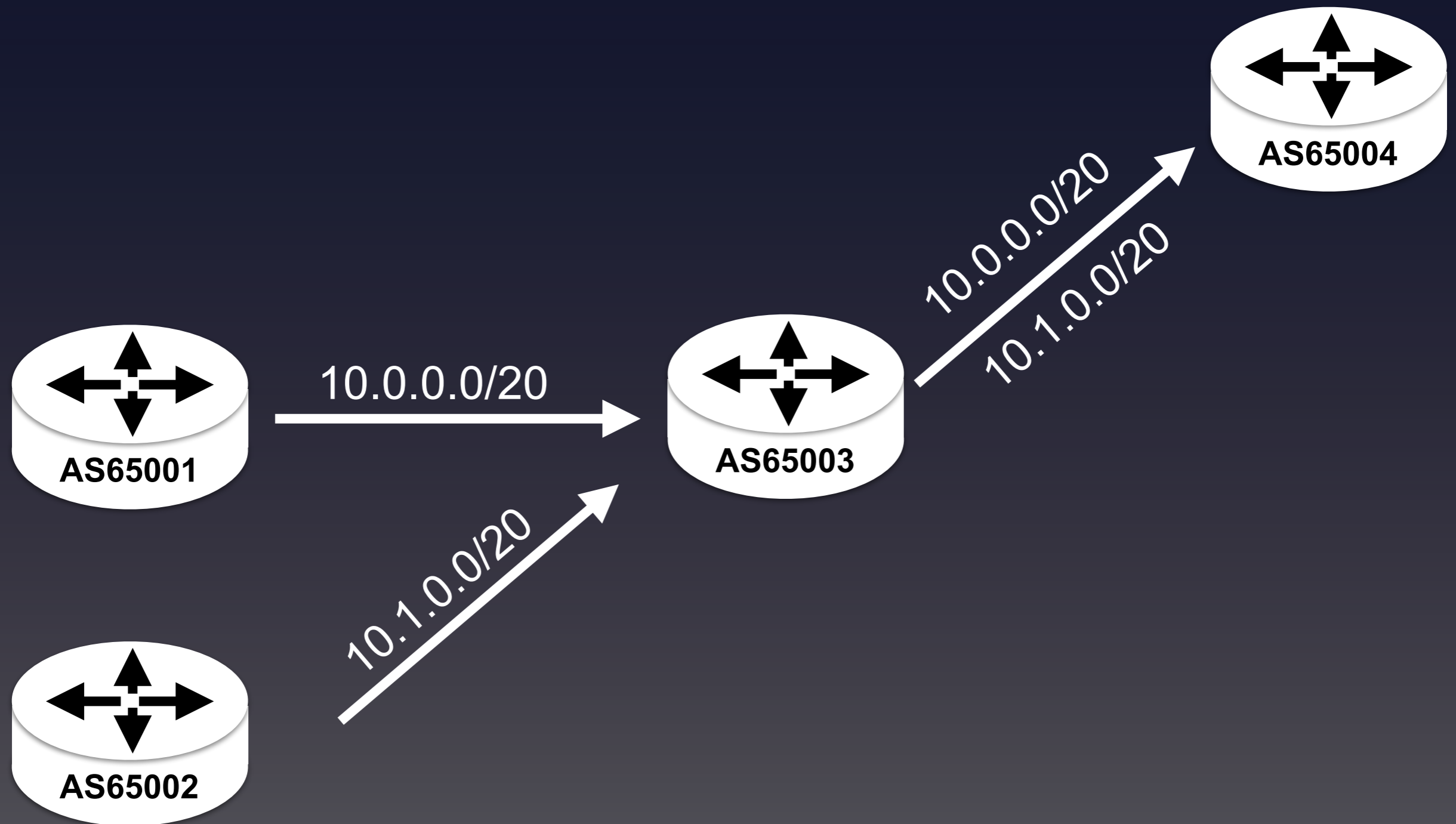




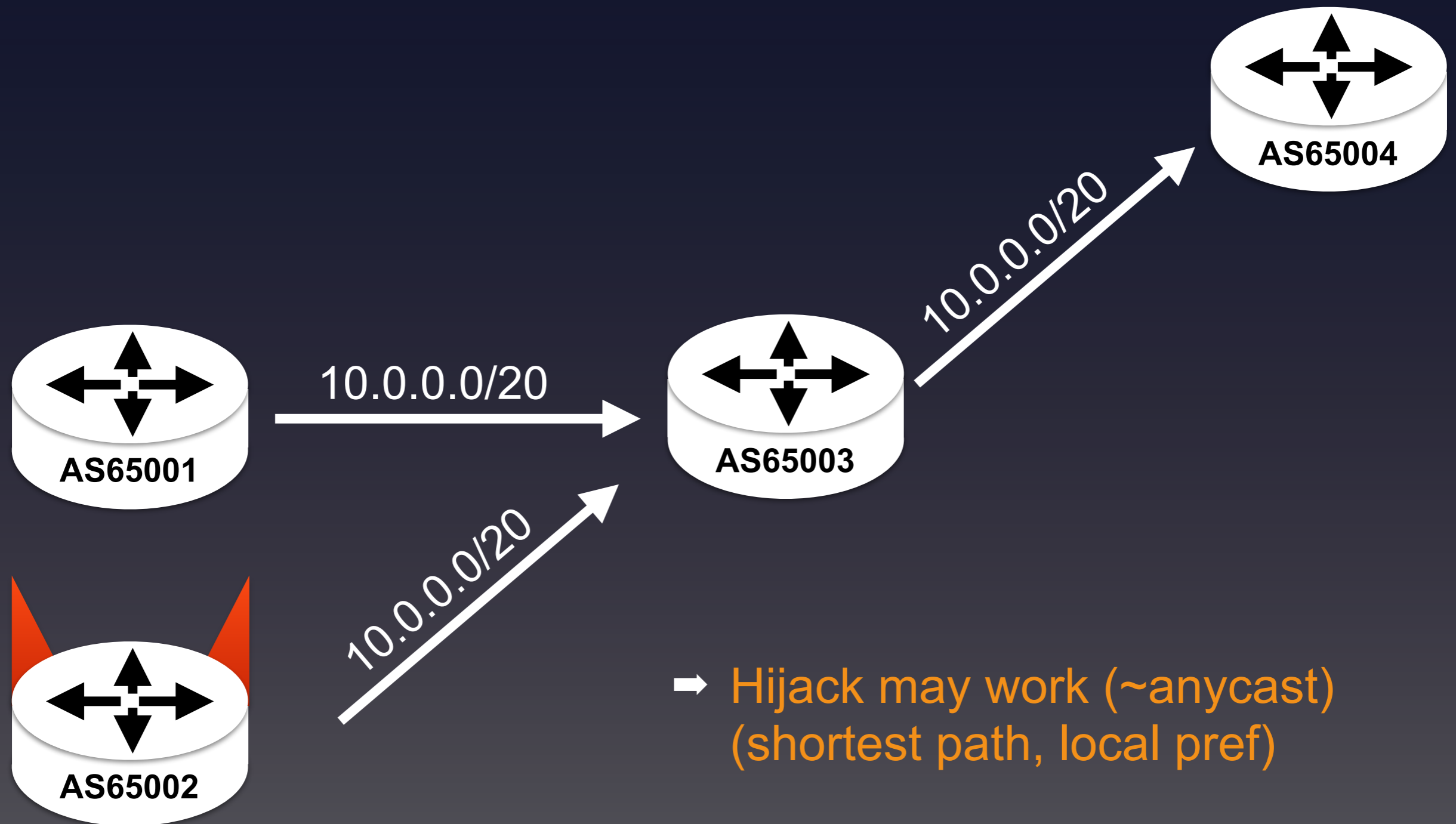
RIPE NCC
RIPE NETWORK COORDINATION CENTRE

Prefix Filtering: RIPE Database and ROAs

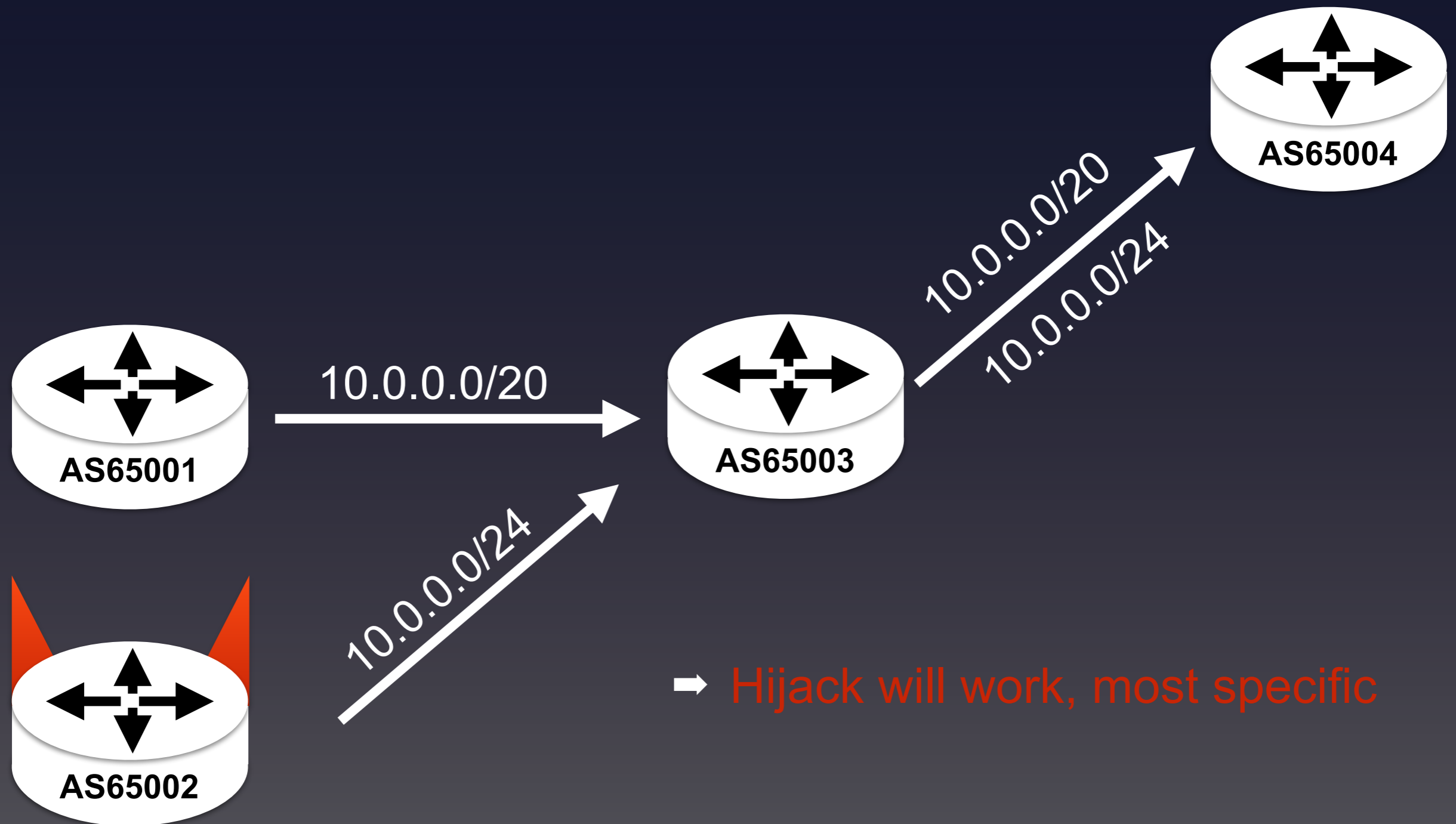
BGP - all good



BGP - simple hijack



BGP - more specific hijack



Origin Validation



- Most commonly done by providers
- Internet Exchange points have started offering filtering as a service
- Transit providers usually do not filter
- Stub networks may filter because they want to block poisonous traffic

ROUTE object



```
inetnum: 10.0.0.0 - 10.0.3.255
netname: Example LIR
.....
mnt-by: EXAMPLE-NET-MNT
```

```
aut-num: AS65001
as-name: EXAMPLE-LIR-AS
.....
mnt-by: EXAMPLE-ASN-MNT
```

authorises
(pw, pggp, sso)

authorises
(to be deprecated in RIPE DB)

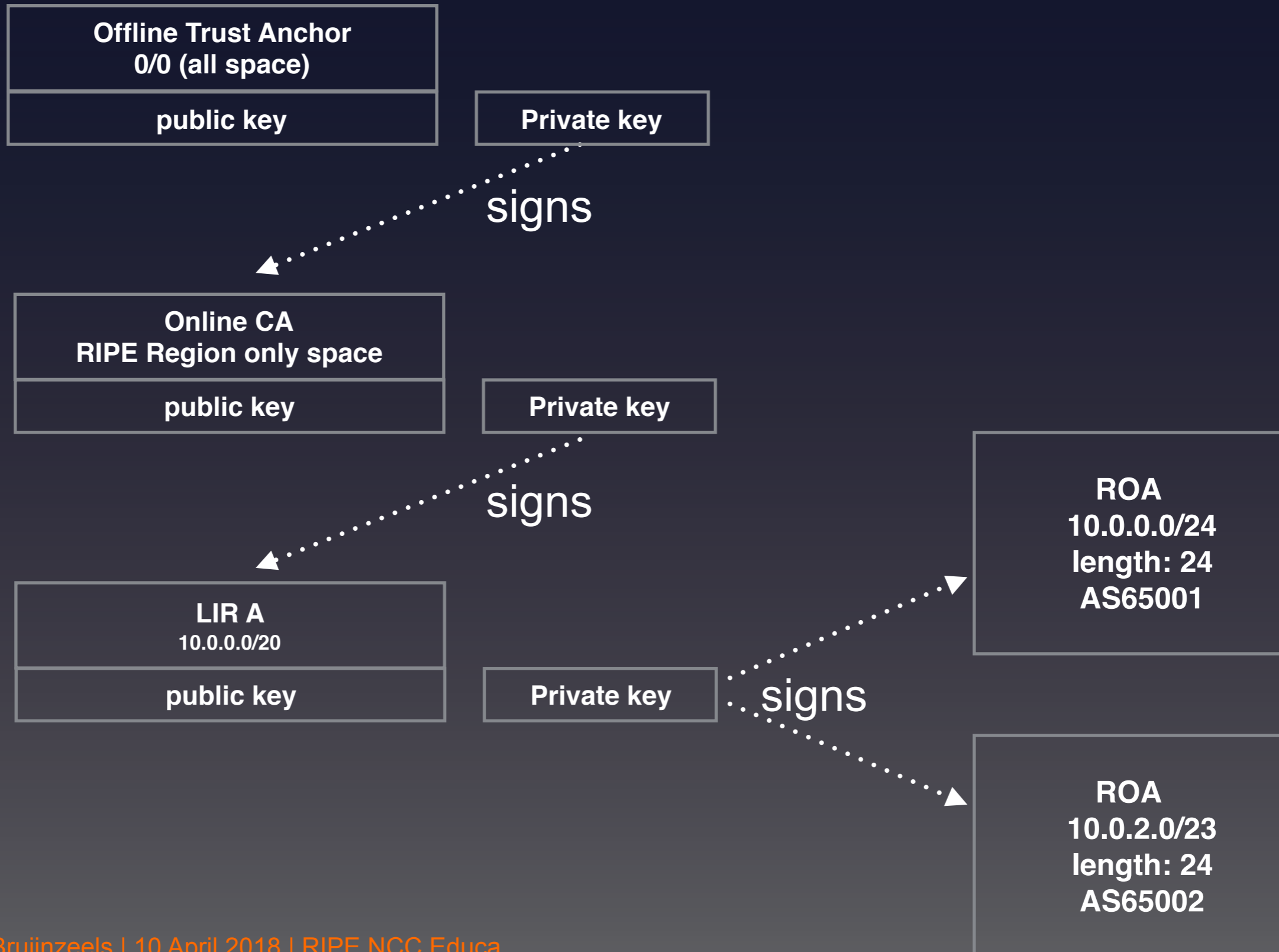
```
route: 10.0.0.0/20
origin: AS65001
mnt-by: EXAMPLE-ROUTE-MNT
source: RIPE
```

Internet Routing Registry



- Many exist, most widely used
 - RIPE Database
 - RADB
- Verification of holdership over resources
 - RIPE Database for RIPE region resources only
 - RIPE Database allows anyone to create out-of-region (about to be deprecated)
 - RADB allows paying customers to create any object
 - Lot of other IRR don't formally verify holdership

Authorisation using RPKI



BGP - Origin validation

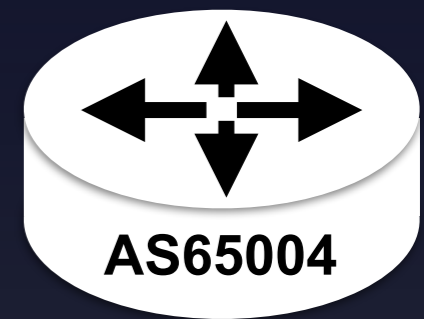


ROA
10.0.0.0/20
AS65001

Signed
10.0.0.0/20

ROUTE
10.0.0.0/20
AS65001

→ Both reject evil announcement
from wrong ASN



BGP - Origin validation with spoof

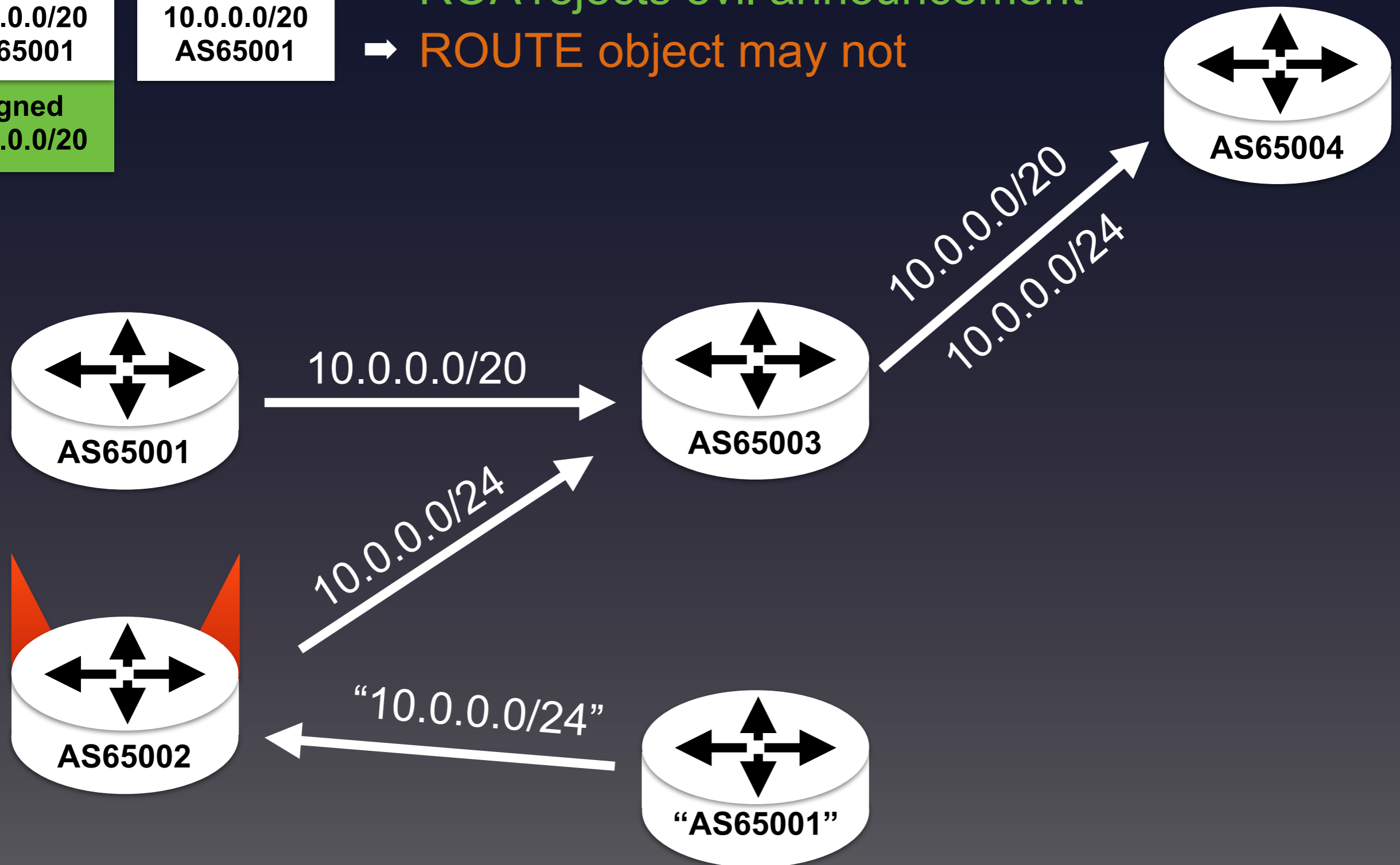


ROA
10.0.0.0/20
AS65001

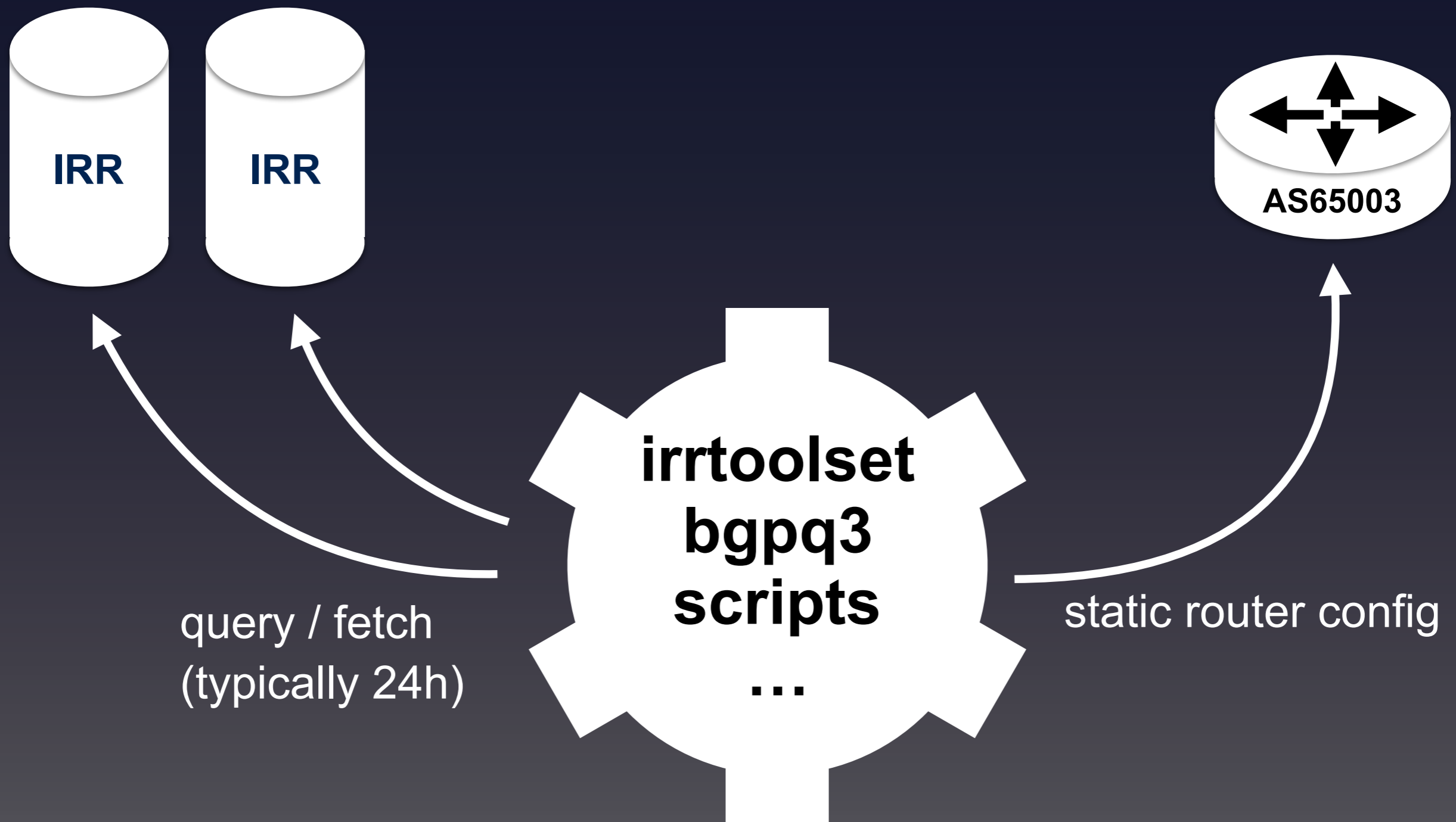
Signed
10.0.0.0/20

ROUTE
10.0.0.0/20
AS65001

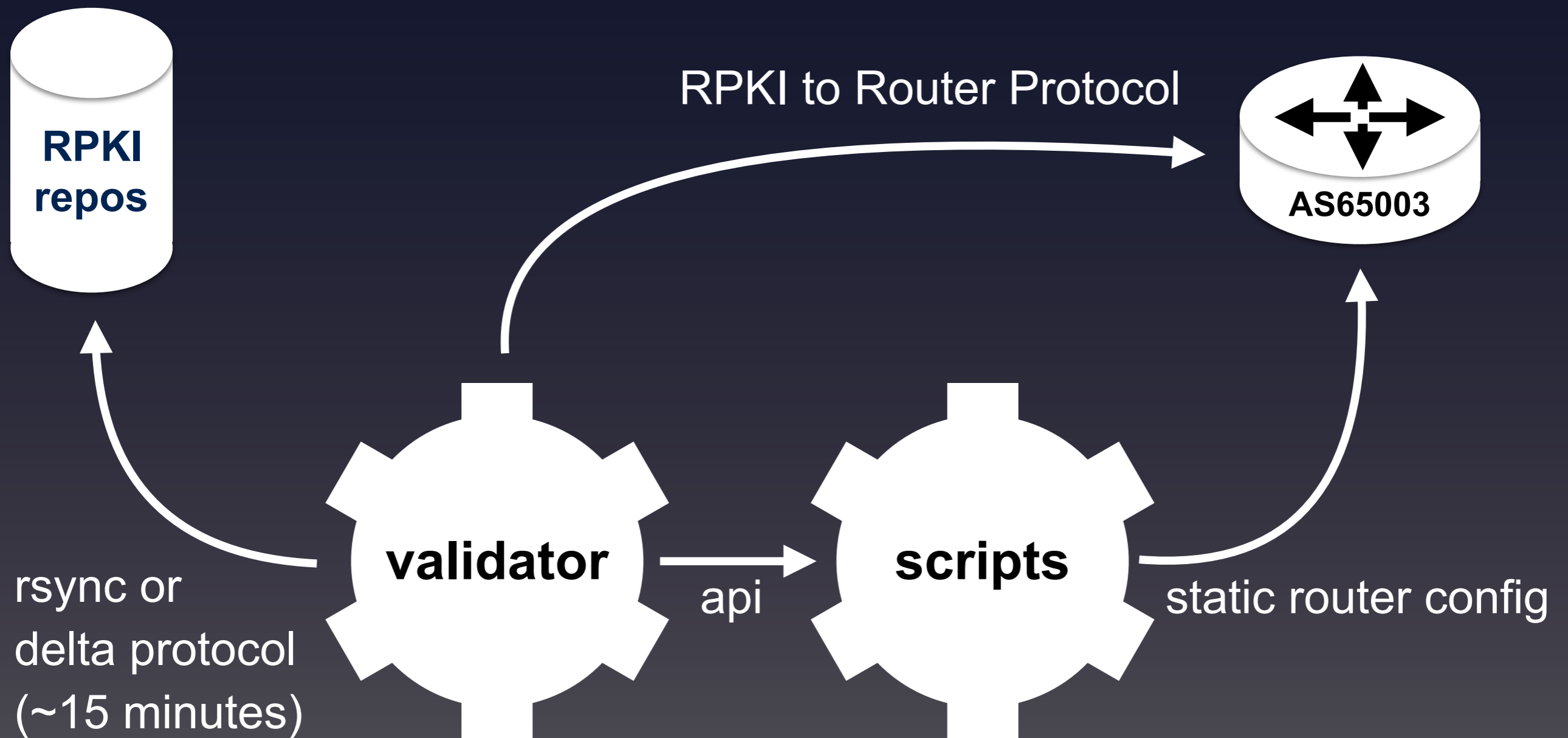
- ROA rejects evil announcement
- ROUTE object may not



Automate using IRR



Automate using RPKI



Dynamic router config RPKI



- Router connects to validator

- Supported by many vendors

- Example pseudo-config

- Dropping invalids as per RFC 7115

```
match rpki valid
  set local preference 100
match rpki not-found
  set local preference 50
match rpki invalid
  reject
```

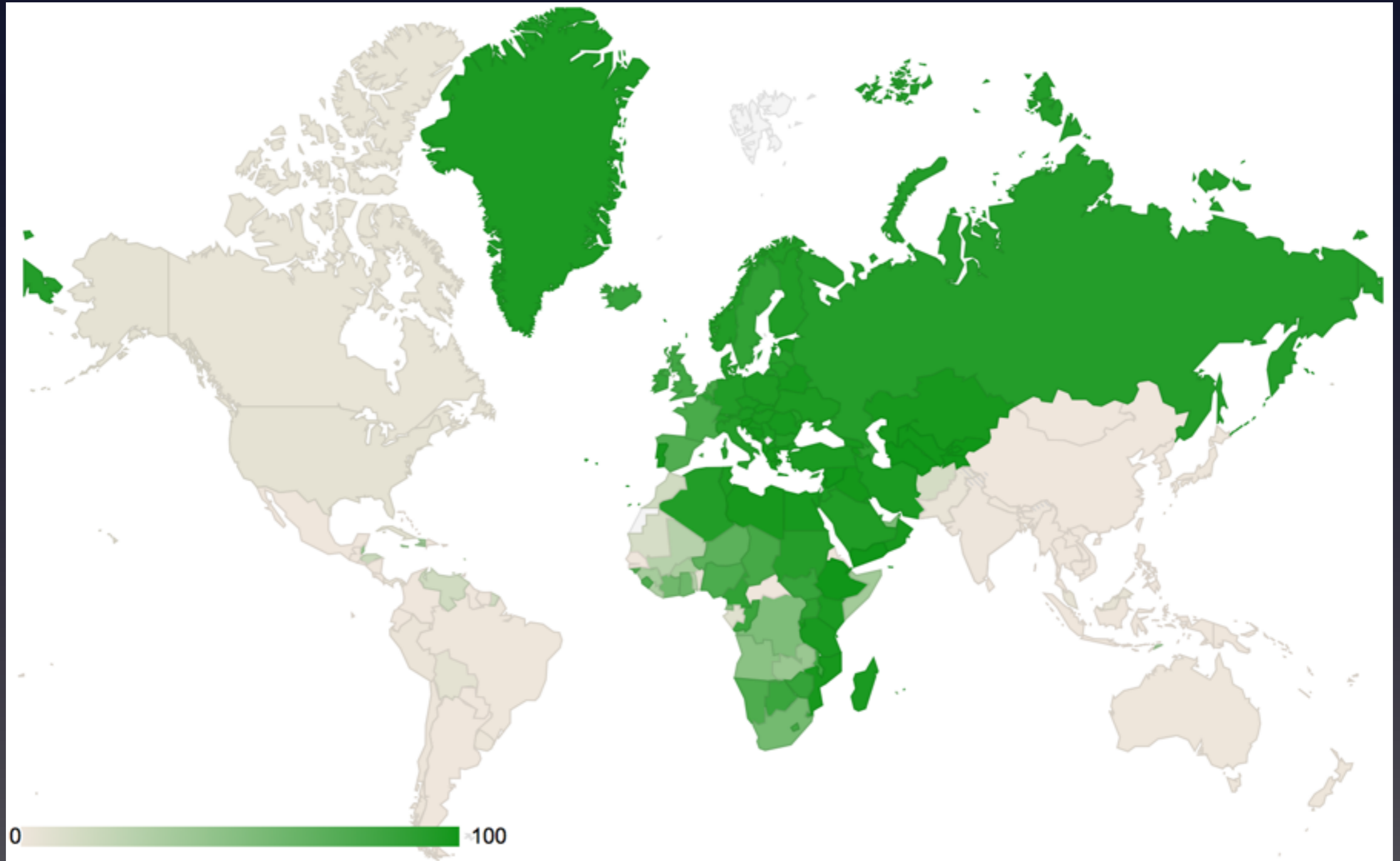
- Enables validation of full table, not just customers

Authorising Origination



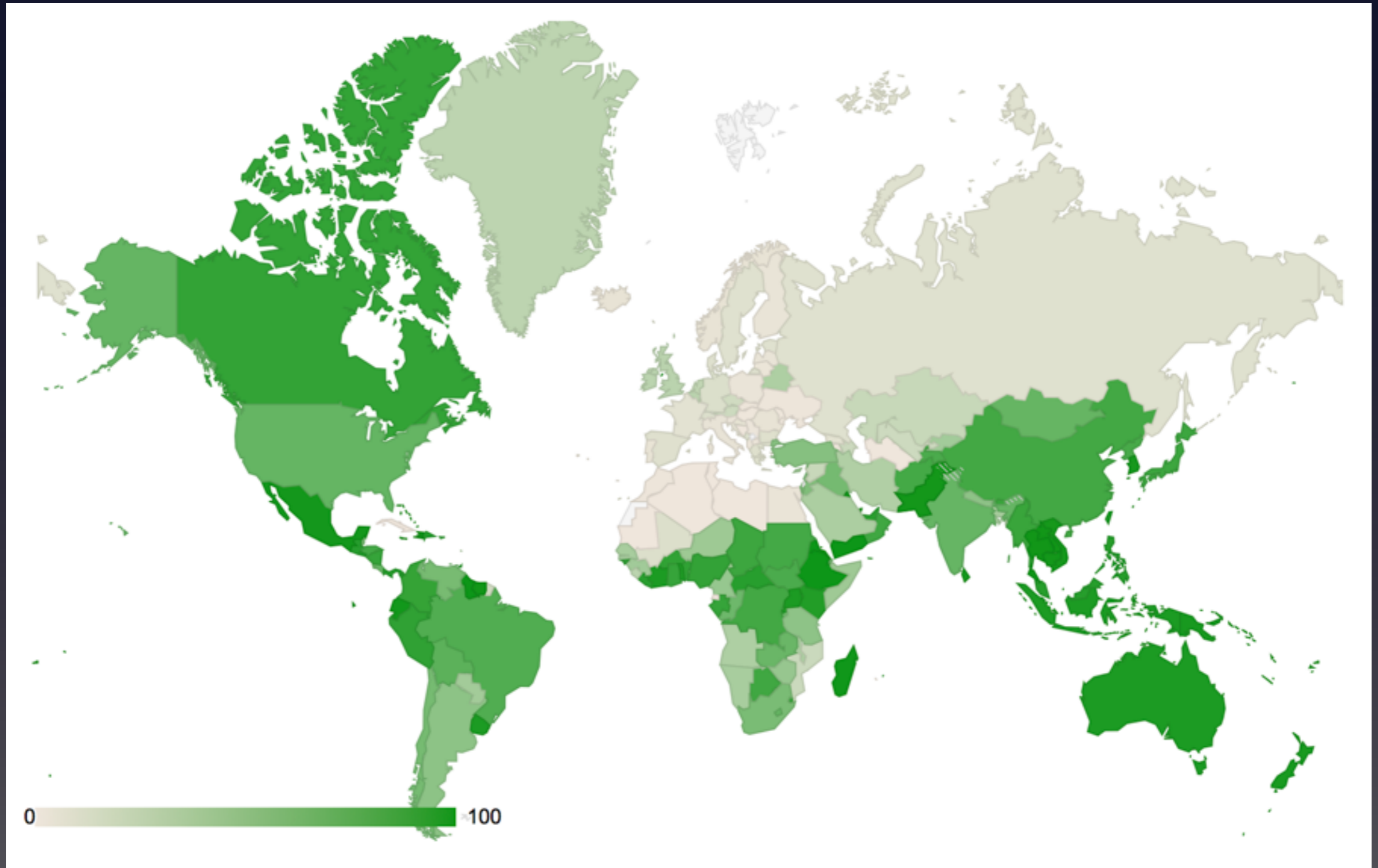
	ROUTE	ROA
Authorises	Prefix for AS	Prefix for AS
Authorisation	Good, weak or absent	Strong (RPKI)
Validation	Plain text	Object security
More specifics	Undetermined	Reject (unless..)
Propagation	Slow	Fast
Maturity	25 years	7 years

Coverage - RIPE IRR



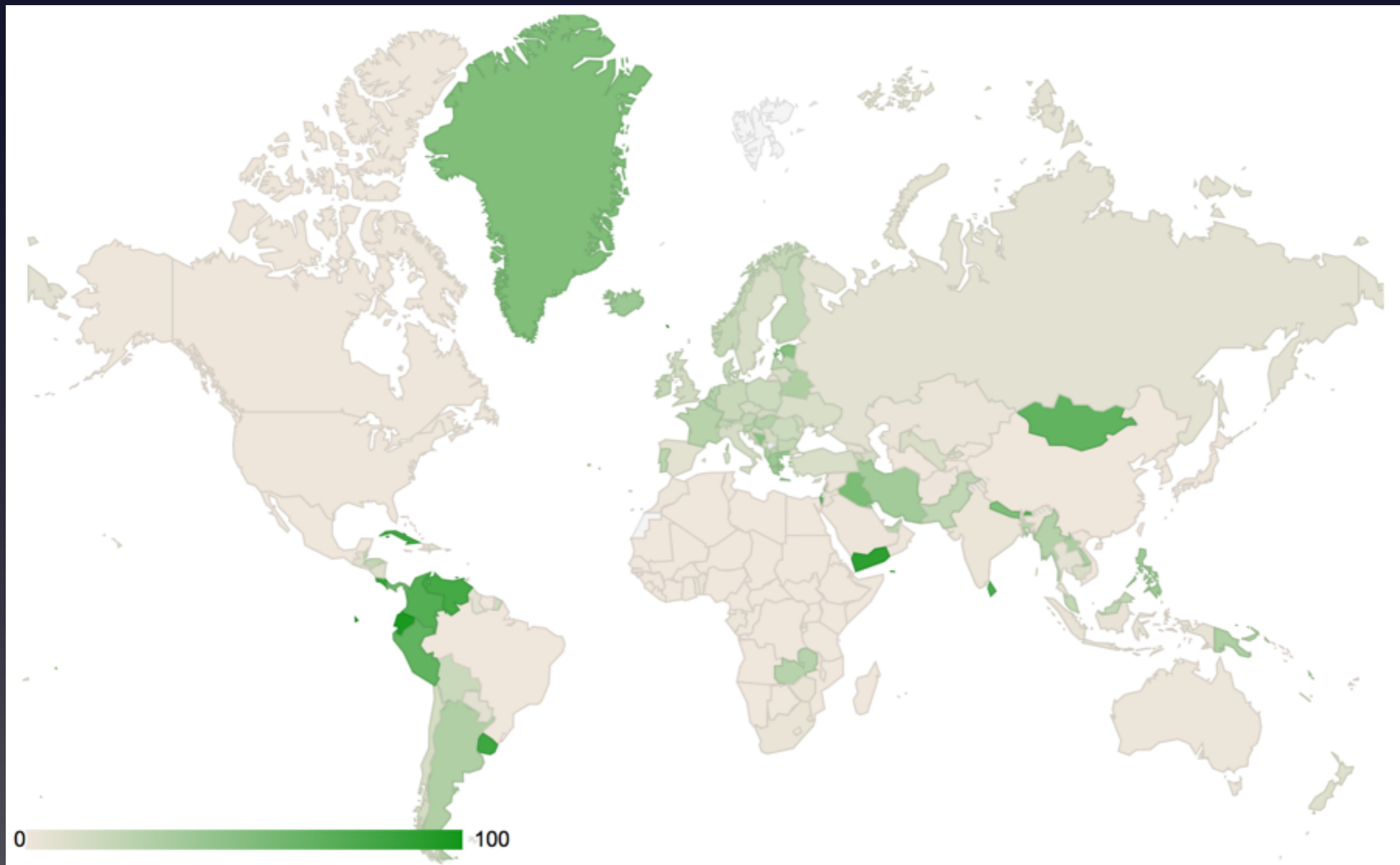
Fraction of IPv4 announcements valid according to ROUTE objects

Coverage - RADB IRR



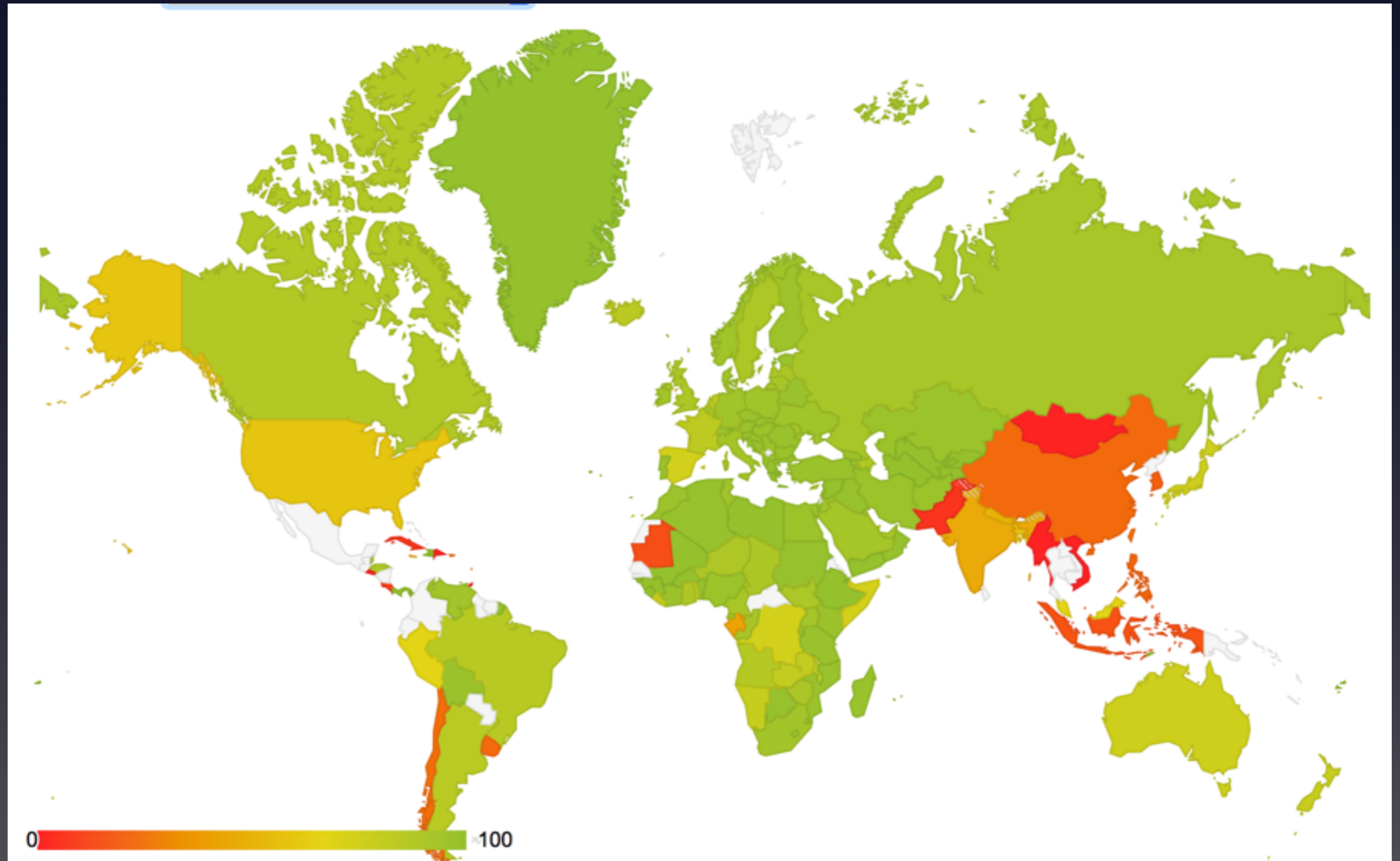
Fraction of IPv4 announcements valid according to ROUTE objects

Coverage - RPKI (all RIRs)



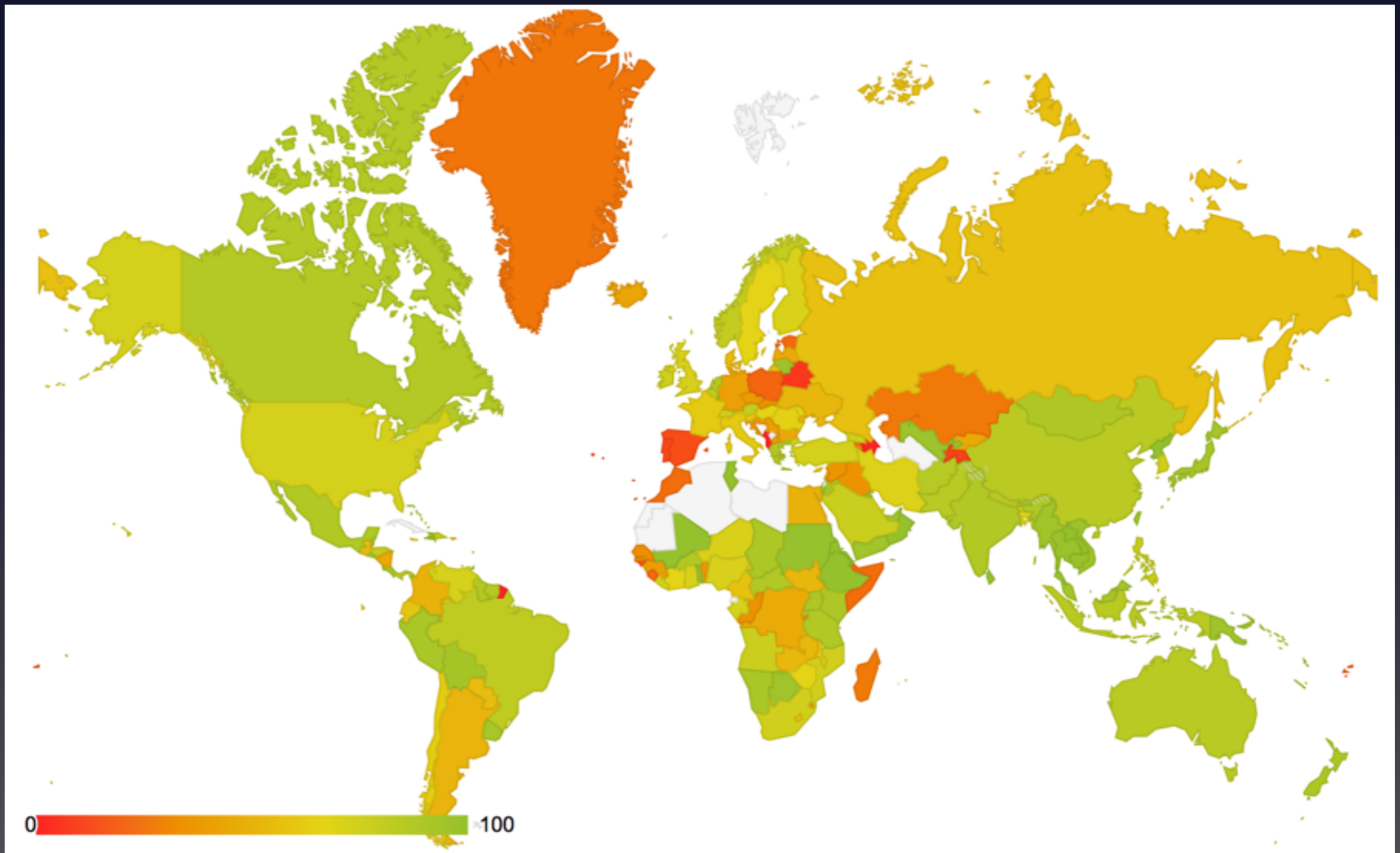
Fraction of IPv4 announcements valid according to ROUTE objects

Accuracy - RIPE IRR



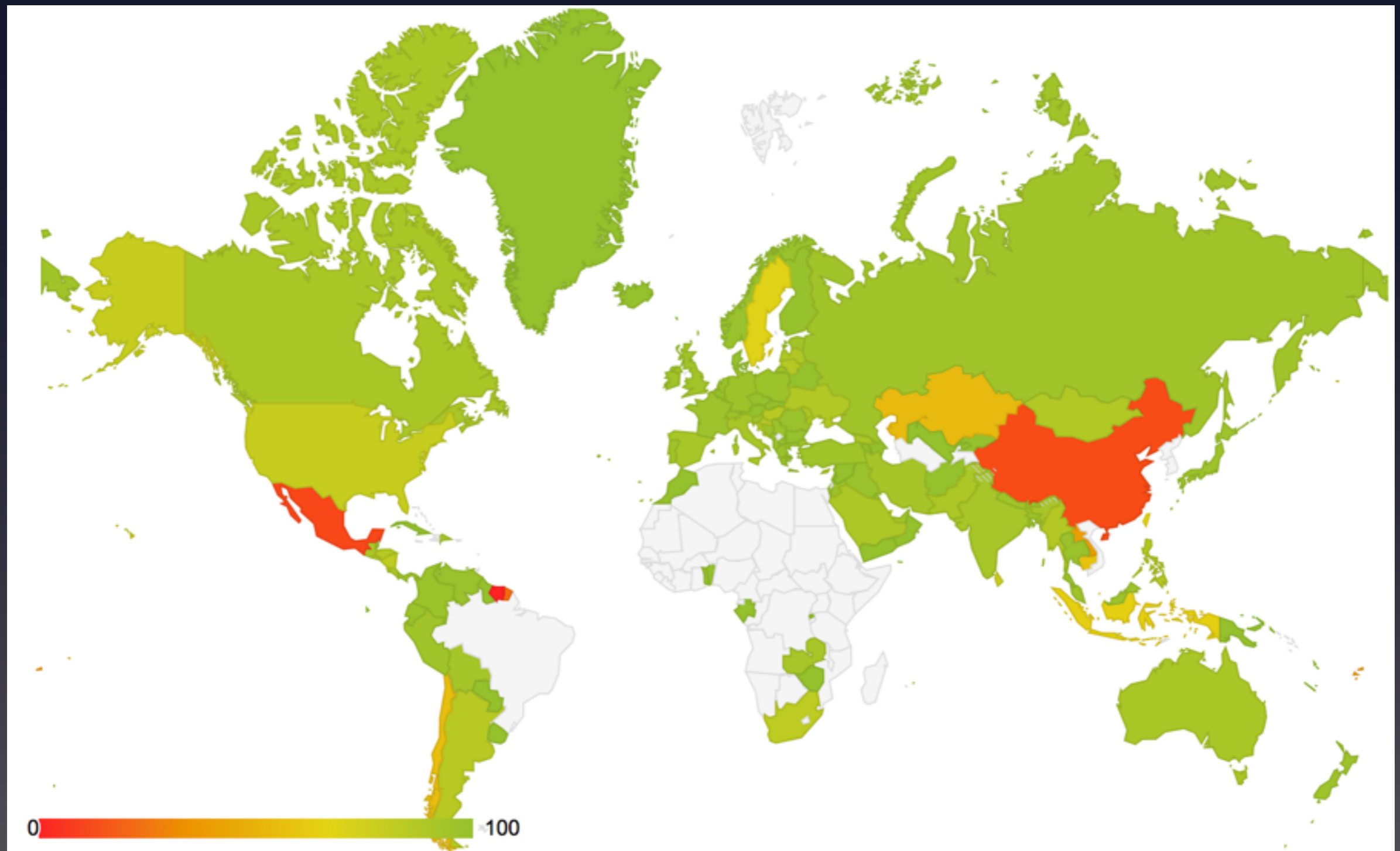
Accuracy - Valid announcements / covered announcements

Accuracy - RADB IRR



Accuracy - Valid announcements / covered announcements

Accuracy - RPKI (all RIRs)



Accuracy - Valid announcements / covered announcements

Data Quality - Comparison



	RIPE IRR	RADB IRR	ROA
Coverage	RIPE region and Africa (historical)	Inverse of RIPE IRR	RIPE, Lacnic, Some in Asia
Accuracy	Good where coverage is high	Mediocre where coverage is high	Very good where coverage is high
	Bad where coverage is low	Bad where coverage is low	Often good where coverage is low

How to set up ROUTE



- Prefix holder can create a ROUTE(6) object in the (RIPE) Database
- The holder of the ASN needs to approve, but this will be deprecated in the RIPE Database soon!
- Most important elements:

```
route: 10.0.0.0/20
origin: AS65001
mnt-by: EXAMPLE-LIR-MNT
origin: RIPE
```

How to set up ROUTE



Create "route" object

Create in text area

Please enter the maintainers you would like to use as mnt-by

RIPE-NCC-MNT ★ ×



route

193.0.0.0/21



origin

AS1299



source

RIPE



By submitting this form you explicitly express your agreement with the [RIPE Database Terms and Conditions](#)

Cancel

Submit

Out of region ROUTE(6) objects



- For historic reasons the RIPE Database allows the creation of ROUTE(6) objects for prefixes and/or ASNs that are not part of the RIPE region
- The RIPE DB-WG and ROUTING-WG decided:
 - No more new out of region ROUTE(6) objects may be created
 - Authorisation by the ASN is no longer needed
 - No more out of region AUT-NUM objects may be created
 - Existing out-of-region objects get source: RIPE-NONAUTH
 - ..to be deleted in future

How to set up ROAs



- Be careful with 'max length'
 - May help for certain anti-DDoS measures
 - But exposes hijack by more specific
- RIPE NCC
 - Easy to use user interface shows your announcements
 - Decide what to authorise
 - Opt-in for alerts

How to set up ROAs



RPKI Dashboard 11 CERTIFIED RESOURCES ALERTS ARE SENT TO 1 ADDRESS

63 BGP Announcements 59 Valid 0 Invalid 0 Unknown **87** ROAs 87 OK 0 Causing problems

BGP Announcements **Route Origin Authorisations (ROAs)** History

Create ROAs for selected BGP Announcements Valid Invalid Unknown

<input type="checkbox"/>	Origin AS	Prefix	Current Status	
<input type="checkbox"/>	AS3333	193.0.0.0/21	VALID	<input type="checkbox"/>
<input type="checkbox"/>	AS3333	193.0.10.0/23	VALID	<input type="checkbox"/>
<input type="checkbox"/>	AS3333	193.0.12.0/23	VALID	<input type="checkbox"/>
<input type="checkbox"/>	AS3333	193.0.18.0/23	VALID	<input type="checkbox"/>
<input type="checkbox"/>	AS3333	193.0.20.0/23	VALID	<input type="checkbox"/>
<input type="checkbox"/>	AS3333	193.0.22.0/23	VALID	<input type="checkbox"/>
<input type="checkbox"/>	AS3333	2001:67c:2e8::/48	VALID	<input type="checkbox"/>
<input type="checkbox"/>	AS12654	2001:7fb:fd02::/48	VALID	<input type="checkbox"/>
<input type="checkbox"/>	AS12654	2001:7fb:fd03::/48	INVALID ASN <input type="checkbox"/> MUTED	<input type="checkbox"/> <input type="checkbox"/>
<input type="checkbox"/>	AS12654	2001:7fb:fe03::/48	VALID	<input type="checkbox"/>

Show of 63 items Page 1 of 7

How to set up ROAs



RPKI Dashboard 11 CERTIFIED RESOURCES ALERTS ARE SENT TO 1 ADDRESS

63 BGP Announcements 59 Valid 0 Invalid 0 Unknown **87** ROAs 87 OK 0 Causing problems

BGP Announcements **Route Origin Authorisations (ROAs)** History

Fix announcement

Affected Announcement

AS number: AS12654, Prefix: 2001:7fb:fd03::/48, Max Length: 48 Create ROA

ROAs currently invalidating this announcement

AS number: AS196615, Prefix: 2001:7fb:fd03::/48, Max Length: 48 INVALID ASN

Manual fix

AS Number	Prefix	Max length	Add ROA
<input type="checkbox"/> AS12654	2001:7fb:fd02::/48	VALID	<input type="button" value="Add ROA"/>
<input type="checkbox"/> AS12654	2001:7fb:fd03::/48	INVALID ASN MUTED	<input type="button" value="Add ROA"/>
<input type="checkbox"/> AS12654	2001:7fb:fe03::/48	VALID	<input type="button" value="Add ROA"/>

Show of 63 items Page 1 of 7

How to set up ROAs



RPKI Dashboard 11 CERTIFIED RESOURCES ALERTS ARE SENT TO 1 ADDRESS

63 BGP Announcements 59 Valid 0 Invalid 0 Unknown **87 ROAs** 87 OK 0 Causing problems

BGP Announcements | **Route Origin Authorisations (ROAs)** | History

Create ROAs for selected BGP Announcements Valid Invalid Unknown

<input type="checkbox"/>	Origin AS	Prefix	Current Status	Future Status
<input type="checkbox"/>	AS3333	193.0.0.0/21	VALID	
<input type="checkbox"/>	AS3333	193.0.10.0/23	VALID	
<input type="checkbox"/>	AS3333	193.0.12.0/23	VALID	
<input type="checkbox"/>	AS3333	193.0.18.0/23	VALID	
<input type="checkbox"/>	AS3333	193.0.20.0/23	VALID	
<input type="checkbox"/>	AS3333	193.0.22.0/23	VALID	
<input type="checkbox"/>	AS3333	2001:67c:2e8::/48	VALID	
<input type="checkbox"/>	AS12654			
<input type="checkbox"/>	AS12654			
<input type="checkbox"/>	AS12654			

Show 10 of

Review and publish changes 1

Staged ROAs

AS12654 2001:7fb:fd03::/48 ↔ 48

Affected announcements

AS12654 2001:7fb:fd03::/48 INVALID ASN → VALID

ROA alerts



RPKI Dashboard 11 CERTIFIED RESOURCES ALERTS ARE SENT TO 1 ADDRESS

63 BGP Announcements 87 ROA

59 Valid 0 Invalid 0 Unknown 87 OK

BGP Announcements **Route Origin Authorisations (ROAs)** History

↓ Create ROAs for selected BGP Announcements

<input type="checkbox"/>	Origin AS	Prefix	Current Status	
<input type="checkbox"/>	AS3333	193.0.0.0/21	VALID	
<input type="checkbox"/>	AS3333	193.0.10.0/23	VALID	
<input type="checkbox"/>	AS3333	193.0.12.0/23	VALID	
<input type="checkbox"/>	AS3333	193.0.18.0/23	VALID	
<input type="checkbox"/>	AS3333	193.0.20.0/23	VALID	
<input type="checkbox"/>	AS3333	193.0.22.0/23	VALID	
<input type="checkbox"/>	AS3333	2001:67c:2e8::/48	VALID	
<input type="checkbox"/>	AS12654	2001:7fb:fd02::/48	VALID	
<input type="checkbox"/>	AS12654	2001:7fb:fd03::/48	INVALID ASN	MUTED
<input type="checkbox"/>	AS12654	2001:7fb:fe03::/48	VALID	

Show 10 of 63 items Page 1 of 7

Alerts Configuration

Alerts can keep you aware of attempts to hijack your address space and possible misconfigured ROAs. Please configure alerts below. Alerts are sent by email once every 24 hours.

Please send alert emails about

- Invalid and unknown announcements
- Invalid announcements only

To the following email addresses

ops@ripe.net

Email address

Future plans



- ONE interface for ROUTE objects and ROAs
- Better flagging of potential stale authorisations
- RPKI Validator 3 - available for beta testing now



Questions

tim@ripe.net

