RIPE NCC
RIPE NETWORK COORDINATION CENTRE

RPKI

BGP Origin Validation

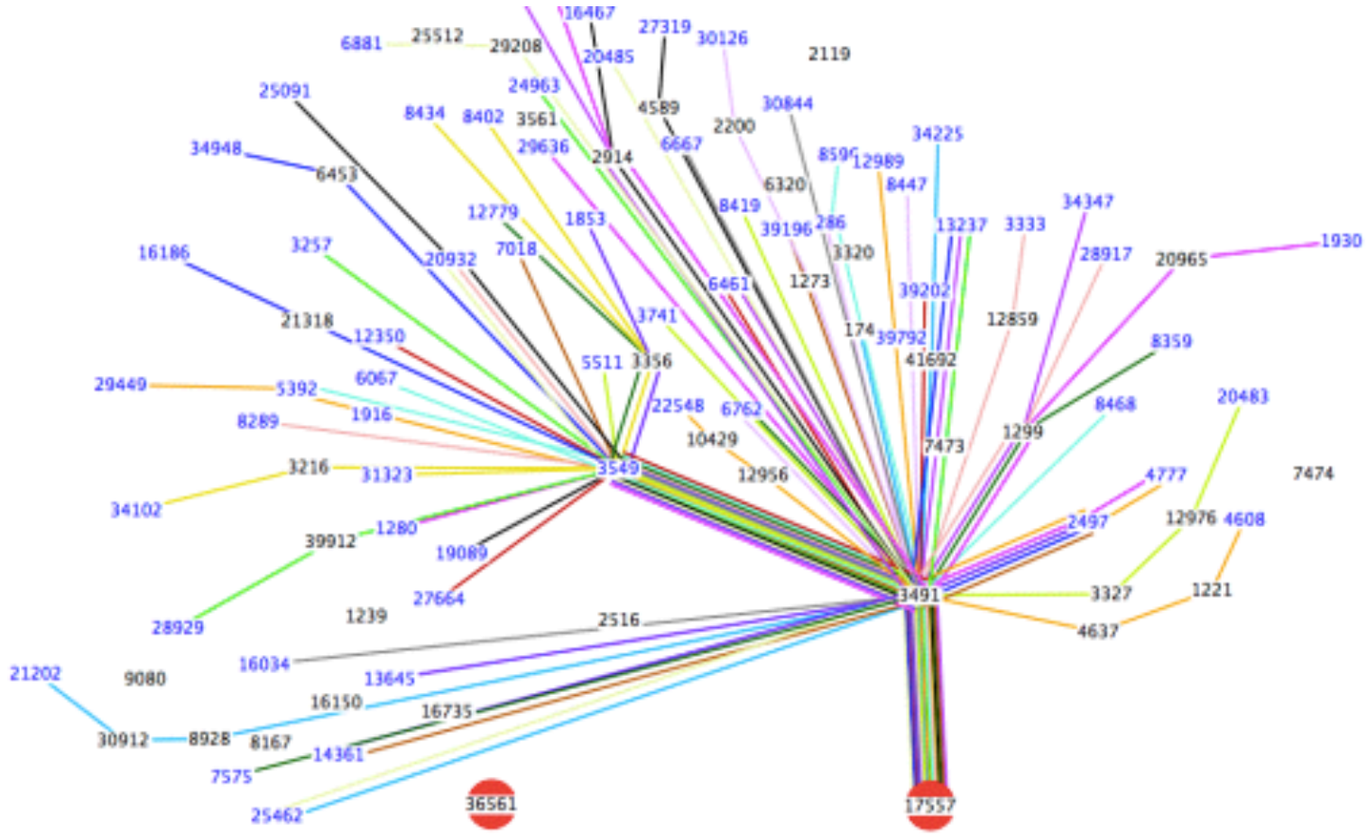
Andrzej Wolski | 25 November 2015 | RSNOG

Interdomain Routing

- Fundamental for operation of the Internet
- The routing protocol for connecting domains
- BGP is a simple “gossip” protocol
  - BGP routers relay messages to neighbors about own and learned routes
  - Routes are constructed hop-by-hop, beyond the originator’s control
- BGP policy and traffic engineering is complex and no global coordination exists
  - Local policies for accepting, rejecting and propagating routes

Routing Incidents

- Misconfiguration
  - No malicious intentions
  - Software bugs
- Malicious
  - Competition
  - Claiming “unused” space
- Targeted Traffic Misdirection
  - Collect and/or tamper with data



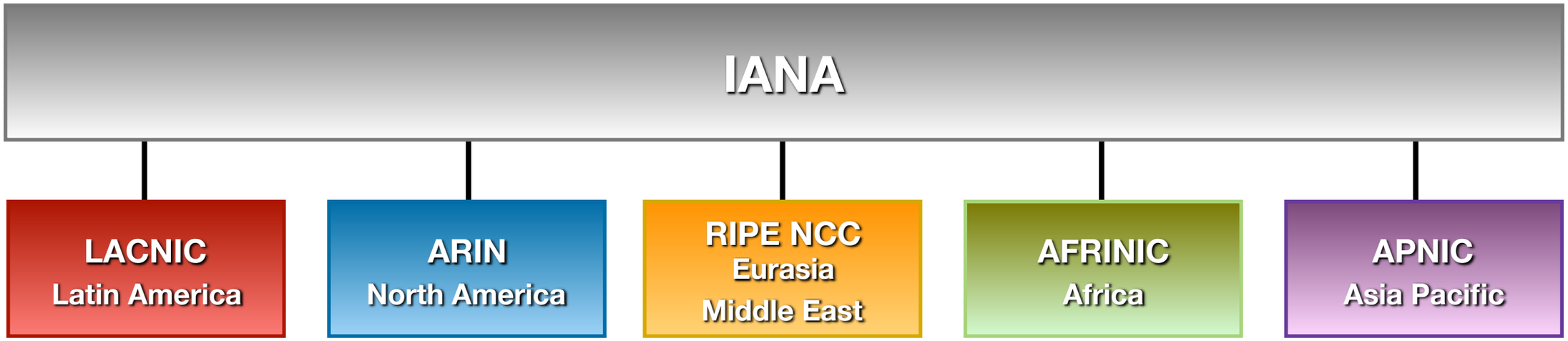
The State of The Global Routing

- Largely a trust-based system
  - Maximum prefix lists
  - Static prefix lists
  - IRR sourced
    - Often unfiltered
    - Often unauthenticated
- Auditing is almost impossible

Origin Validation

"Would you like a reliable way of telling whether a BGP Route Announcement is authorised by the legitimate holder of the address space?"

Internet Registry System



Origin Validation

- Organisation gets their resources from the RIR
  - Allocated resource is in RIR whois database
- Organisation notifies its upstream of the prefix to be announced
  - Usually email or phone
- Upstream must check the RIR whois database before accepting prefix
  - Need to be able to authoritatively prove who holds a prefix and which ASN may announce it

Origin Validation Tools

- Internet Routing Registry
  - Public database viewable and parseable by anyone
  - Needs validation for publishing information
- Resource Public Key Infrastructure
  - Framework for automation and integration with routers
  - Based on open IETF standards:

RFC5280 - X.509 PKI Certificates
RFC3779 - Extensions for IP Addresses and ASNs
RFC6481-6493 - Resource Public Key Infrastructure

RPKI

- A security framework for verifying the association between resource holders and their Internet resources
- Attaches digital certificates to network resources
  - AS Numbers
  - IP Addresses
- Operators associate those two resources
  - Route Origin Authorisations (ROAs)

This is Not New

- RIPE NCC worked on a prototype since 2006
- Launched an open beta mid-2010
  - Get operational experience and feedback before launch
- A limited production service on 1 January 2011
  - Only LIR's address space (no PI, no Legacy)
  - Only hosted system available with a web interface
  - No production grade support for Delegated RPKI
  - First version of RIPE NCC Validator
- Other types of address space added with time

Hosted RPKI

- Automate signing and key roll overs
  - One click setup of resource certificate
  - User has a valid and published certificate for as long as they are the holder of the resources
  - Changes in resource holdership are handled automatically
- Hide all the crypto complexity from the UI
  - Hashes, SIA and AIA pointers, etc.
- Just focus on creating and publishing ROAs
  - Match your intended BGP configuration

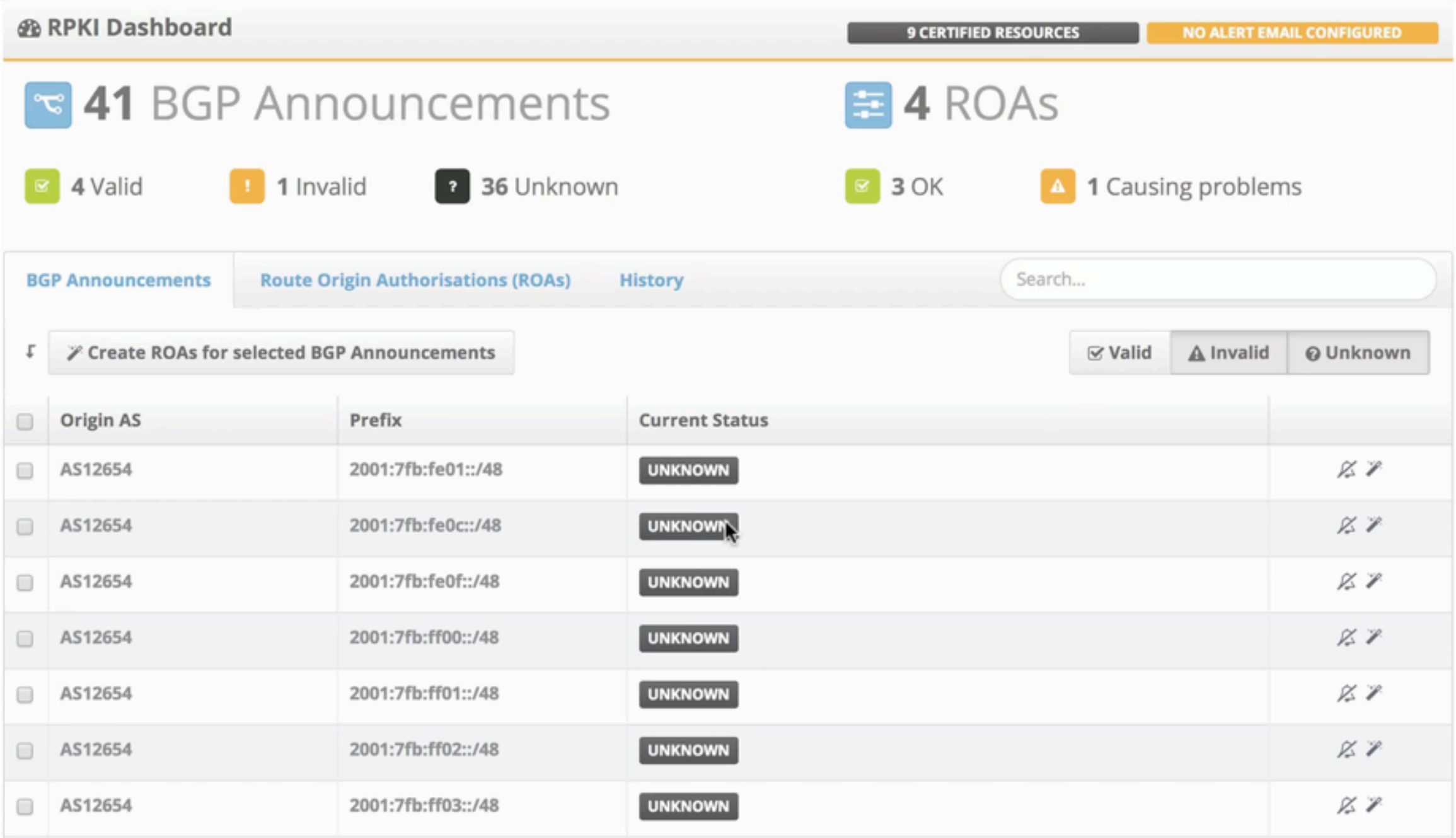
Making Statement

- Legitimate holder is able to make a statement to protect it’s resources
  - specifies which AS can originate your prefix, and
  - what the maximum length of that prefix …

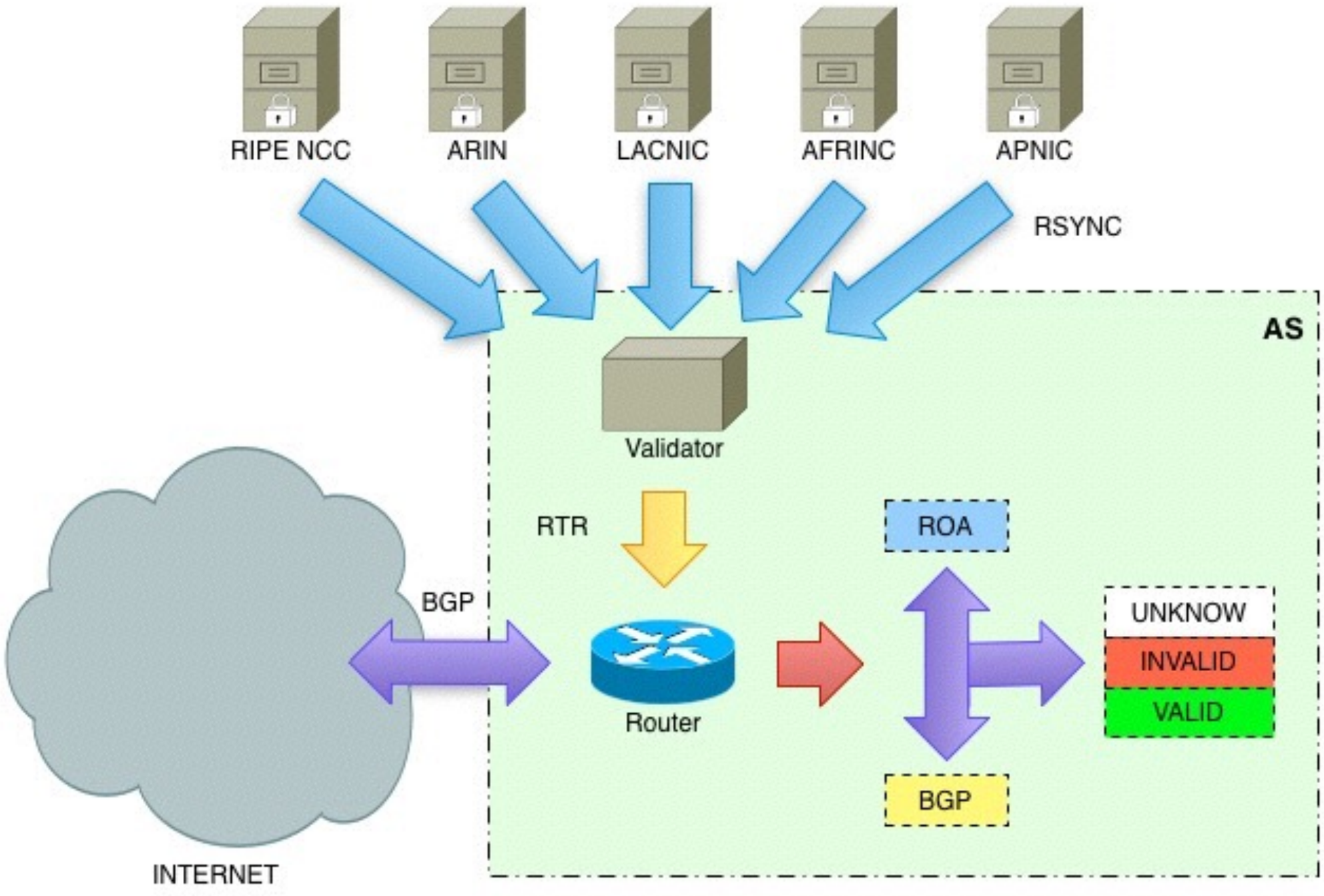
Route Origin Authorisation

AS Number	Prefix	Maximum Length	
			Submit

Creating ROAs



Relying Party



RPKI Support in Routers

- **RPKI** and **RPKI-RTR** are an IETF standards
  - All router vendors can implement them
- **Cisco** support:
  - XR 4.2.1 (CRS-x, ASR9000, c12K) / XR 5.1.1 (NCS6000, XRv)
  - XE 3.5 (C7200, c7600, ASR1K, CSR1Kv, ASR9k, ME3600…)
  - IOS15.2(1)S
- **Juniper** has support since version 12.2
- **Alcatel Lucent** has support since SR-OS 12.0 R4
- **Quagga** has support through BGP-SRX
- **BIRD** has support for ROA but does not do RPKI-RTR

Why should I care?

- Your inbound and outbound traffic can be passively intercepted
- Your data can be:
  - stored
  - dropped
  - filtered
  - modified
- It’s unlikely to be noticed, unless you’re looking for it

Questions

awolski@ripe.net
@TrainingRIPENCC
https://ripe.net/certification