MANRS

Enforcing MANRS Action #4 using RPKI

Musa Stephen HONLUE

honlue@gmail.com / stephen.Honlue@afrinic.net

Twitter: @mhonlue

Why Does Routing Security Matter?

A Routing Overview

The Basics: How Routing Works

There are ~70,000 core networks (Autonomous Systems) across the Internet, each using a unique Autonomous System Number (ASN) to identify itself to other networks.

Routers use Border Gateway Protocol (BGP) to exchange “reachability information” - networks they know how to reach.

Routers build a “routing table” and pick the best route when sending a packet, typically based on the shortest path.

The Honor System: Routing Issues

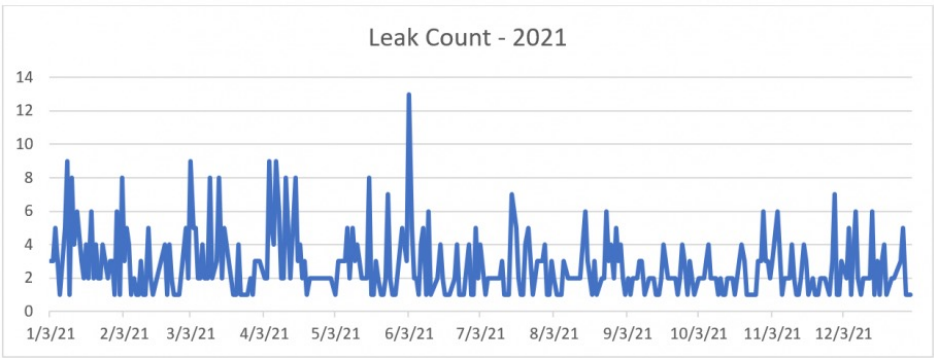
Border Gateway Protocol (BGP) is based entirely on trust between networks

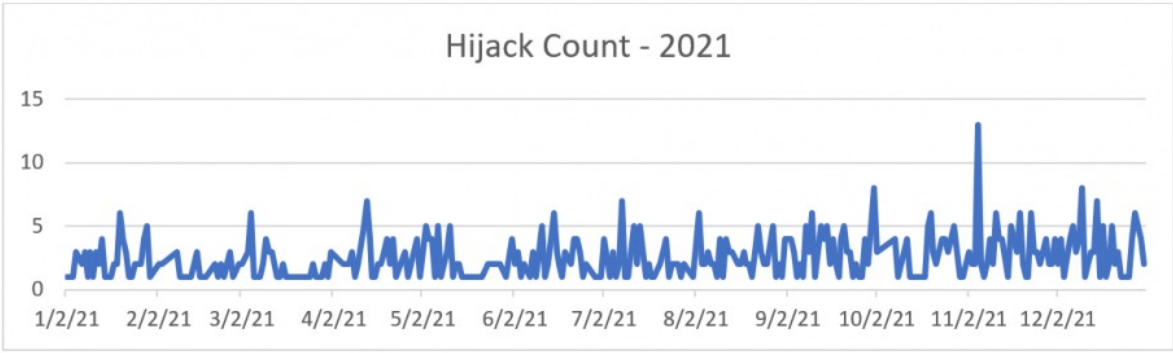
- Created before security was a concern
- Assumes all networks are trustworthy
- No built-in validation that updates are legitimate
- The chain of trust spans continents
- Lack of reliable resource data

Routing Incidents Happen Across the Internet

In 2021 alone, there were thousands of suspected routing outages or attacks – such as hijacking, leaks, and spoofing – that led to a range of problems including stolen data, lost revenue, reputational damage, and more.

Incidents are global in scale, with one operator's routing problems cascading to impact others.



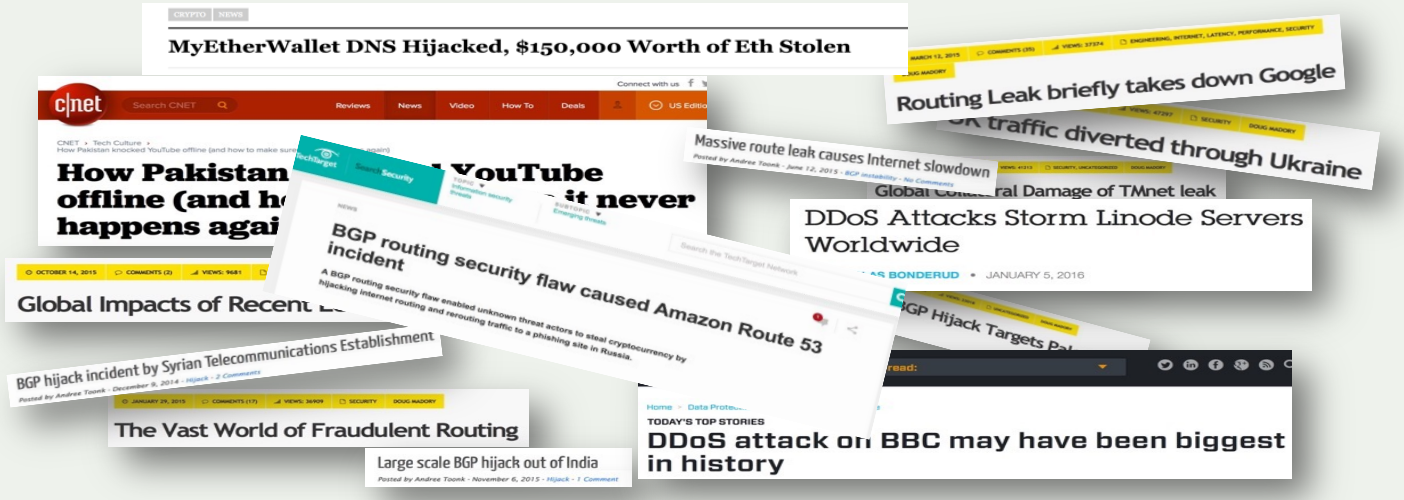


Routing Incidents Cause Real World Problems

Insecure routing is one of the most common paths for malicious threats.

Attacks can take anywhere from hours to months to recognize.

Inadvertent errors can take entire countries offline, while attackers can steal an individual's data or hold an organization's network hostage.



What are Routing Incidents?

A Routing Security Overview

The Threats: What's Happening?

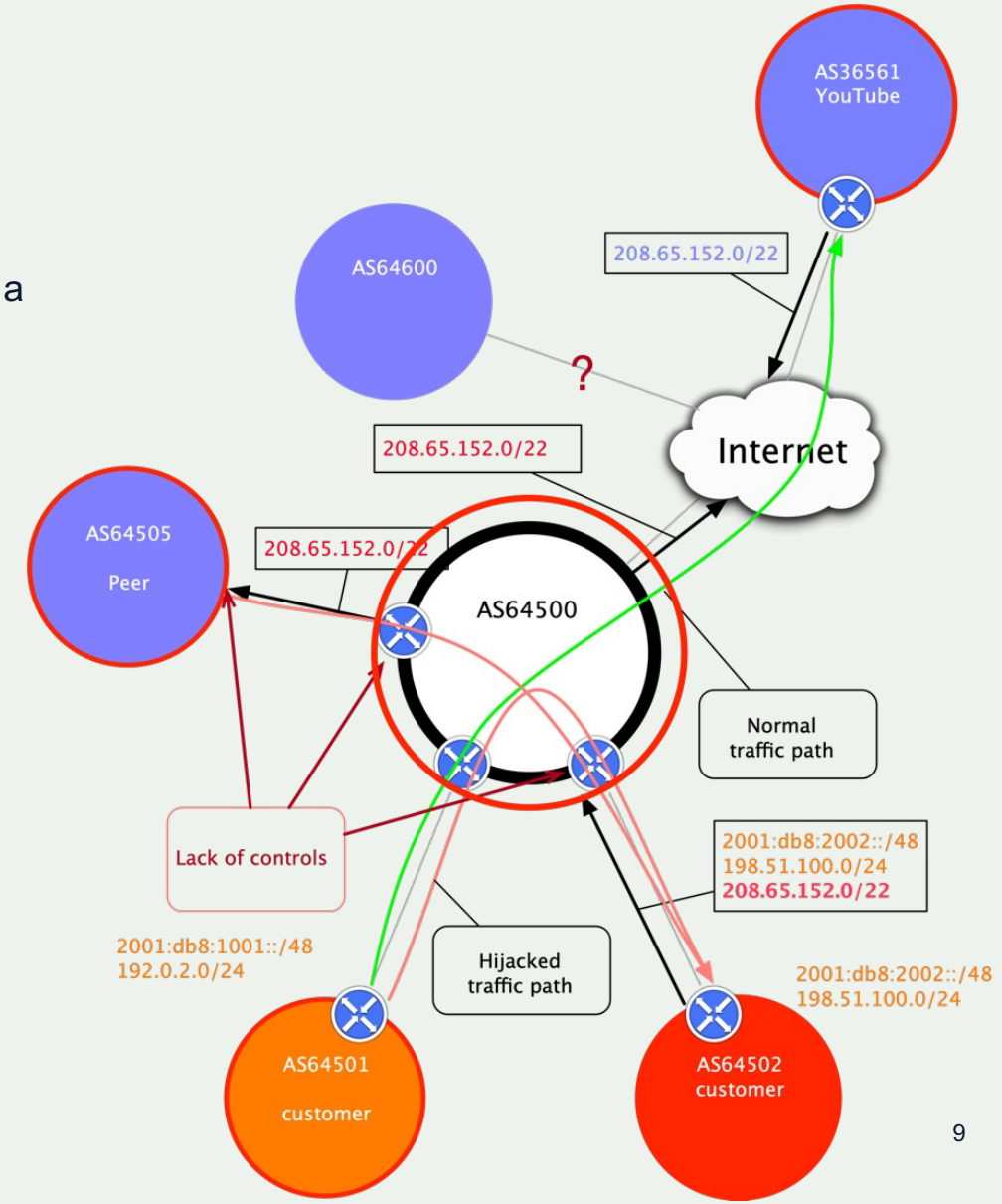
Event	Explanation	Repercussions	Solution
Prefix/Route Hijacking	A network operator or attacker impersonates another network operator, pretending that a server or network is their client.	Packets are forwarded to the wrong place; this can cause Denial of Service (DoS) attacks or traffic interception.	Stronger filtering policies
Route Leak	A network operator with multiple upstream providers announces (often due to accidental misconfiguration) to one upstream provider that is has a route to a destination through the other upstream provider.	Can be used for traffic inspection and reconnaissance.	Stronger filtering policies
IP Address Spoofing	Someone creates IP packets with a false source IP address to hide the identity of the sender or to impersonate another computing system.	The root cause of reflection DDoS attacks.	Source address validation

Prefix/Route Hijacking

Route hijacking, also known as “BGP hijacking,” is when a network operator or attacker (accidentally or deliberately) impersonates another network operator or pretends that a server or network is their client. This routes traffic to the wrong network operator, when another real route is available.

Example: The 2008 YouTube hijack; an attempt to block YouTube through route hijacking led to much of the traffic to YouTube being dropped around the world.

Fix: Strong filtering policies (adjacent networks should strengthen their filtering policies to avoid accepting false announcements).

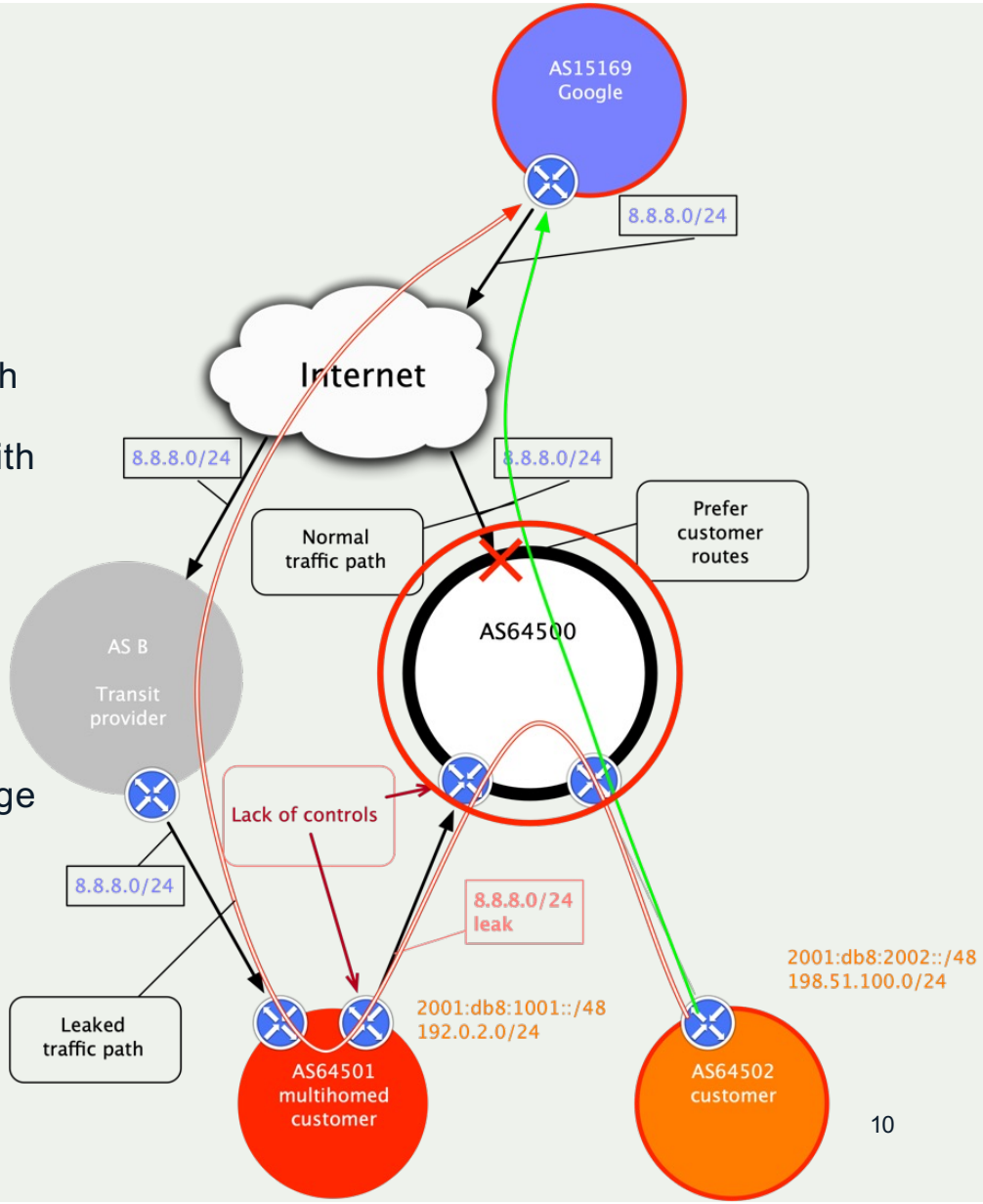


Route Leak

A route leak is where a network operator with multiple upstream providers accidentally announces to one of its upstream providers that is has a route to a destination through the other upstream provider. This makes the network an intermediary network between the two upstream providers, with one sending traffic through the network to get to the other.

Example: 2015, Malaysia Telecom and Level 3, a major backbone provider. Malaysia Telecom told one of Level 3's networks that it was capable of delivering traffic to anywhere on the Internet. Once Level 3 decided the route through Malaysia Telecom looked like the best option, it diverted a huge amount of traffic to Malaysia Telecom.

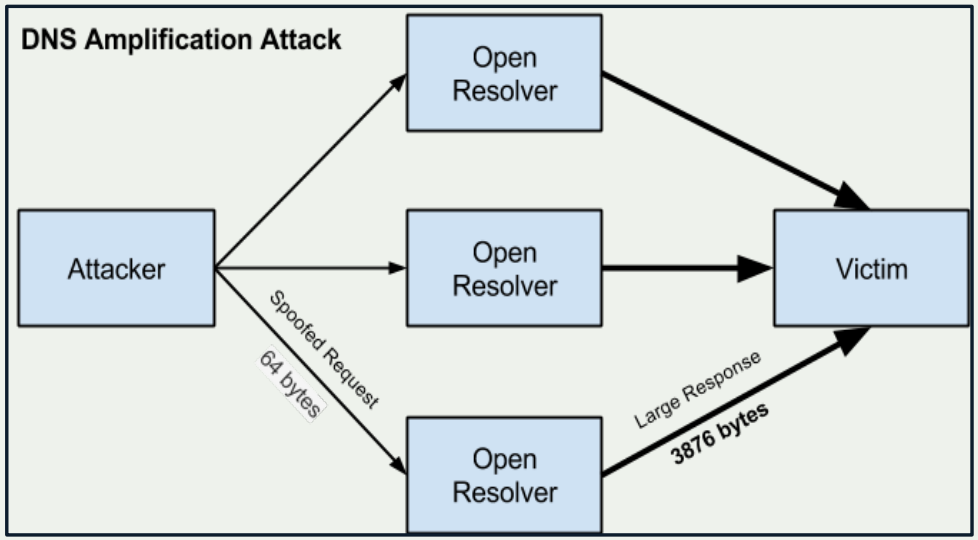
Fix: Strong filtering policies (adjacent networks should strengthen their filtering policies to avoid accepting announcements that don't make sense).



IP Address Spoofing

IP address spoofing is used to hide the true identity of a server or to impersonate another server. This technique can be used to amplify an attack.

Example: DNS amplification attack. By sending multiple spoofed requests to different DNS resolvers, an attacker can prompt many responses from the DNS resolver to be sent to a target, while only using one system to attack.



Fix: Source address validation: systems for source address validation can help tell if the end users and customer networks have correct source IP addresses (combined with filtering).

Tools to Help

- Prefix and AS-PATH filtering
- RPKI validator, IRR toolset, IRRPT, BGPQ3
- BGPSEC

But…

- Not enough deployment
- Lack of reliable data

We need concerted action to improve routing security.

We Are In This Together

Network operators have a responsibility to ensure a globally robust and secure routing infrastructure.

Your network's safety depends on a routing infrastructure that weeds out bad actors and accidental misconfigurations that wreak havoc on the Internet.

The more network operators work together, the fewer incidents there will be, and the less damage they can do.

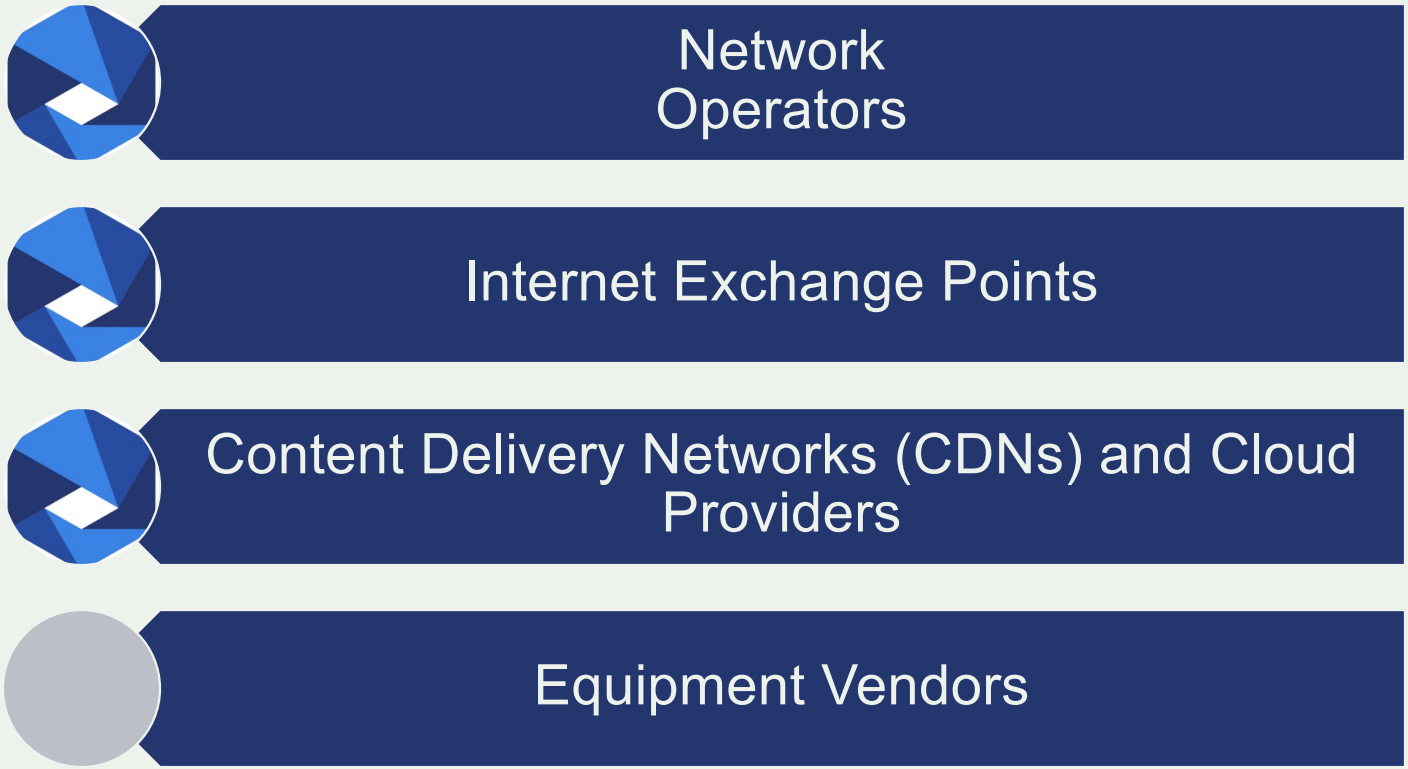
The Solution: Mutually Agreed Norms for Routing Security (MANRS)

Provides crucial fixes to reduce the most common routing threats

MANRS improves the security and reliability of the global Internet routing system, based on collaboration among participants and shared responsibility for the Internet infrastructure.

MANRS sets a new norm for routing security.

MANRS Programs



MANRS Network Operators Program

Launched in 2014 by a handful of network operators with the following goals:

- Raise awareness of routing security problems and encourage the implementation of actions that can address them.
- Promote a culture of collective responsibility toward the security and resilience of the Internet's global routing system.
- Demonstrate the ability of the Internet industry to address routing security problems.
- Provide a framework for network operators to better understand and address issues relating to the security and resilience of the Internet's global routing system.

MANRS Actions for Network Operators

Filtering

Prevent propagation of incorrect routing information

Ensure the correctness of your own announcements and announcements from your customers to adjacent networks with prefix and AS-path granularity

Anti-spoofing

Prevent traffic with spoofed source IP addresses

Enable source address validation for at least single-homed stub customer networks, their own end-users, and infrastructure

Coordination

Facilitate global operational communication and coordination between network operators

Maintain globally accessible, up-to-date contact information in common routing databases

Global Validation

Facilitate validation of routing information on a global scale

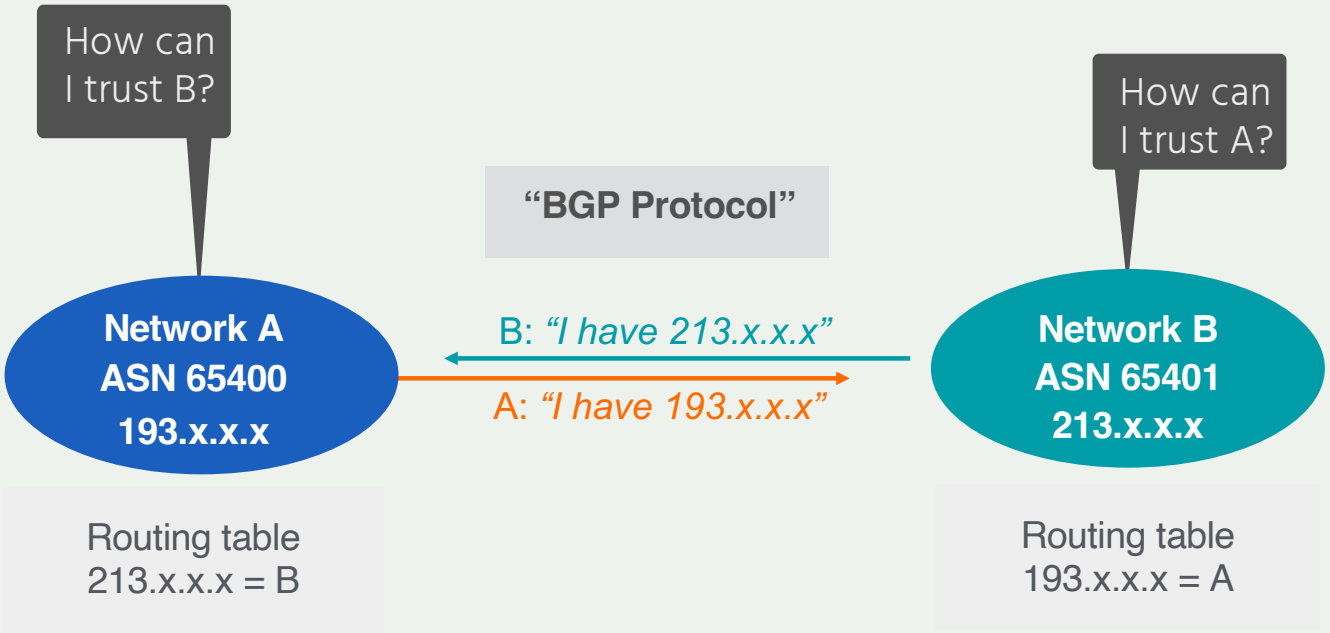
Publish your data so others can validate

Blue shading = Mandatory Action

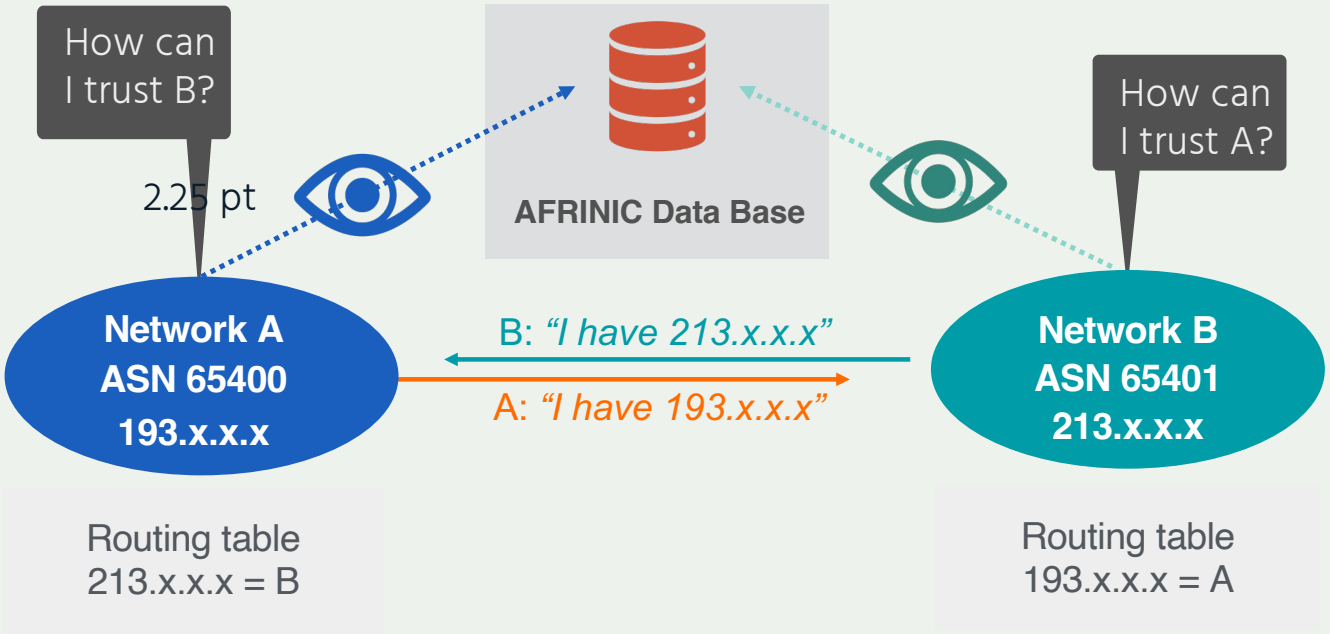
RPKI

Resource Public Key Infrastructure

Routing on the Internet



How can you have secure routing?



Limitations of the IRR system

Some IRR data cannot be fully trusted

- Accuracy
- Incomplete data
- Lack of maintenance

- Third party databases are widely used
- No verification of who holds IPs/ASNs

A Short History of RPKI

Operated since 2008 by all RIRs

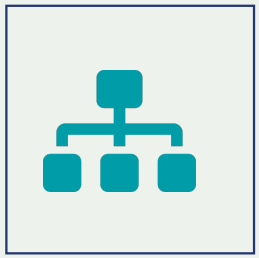
- Community-driven standardisation (IETF)

Adds crypto-security to IP addresses and ASNs

- Provides data you can trust

Resource Public Key Infrastructure (RPKI)

Ties IP addresses and ASNs to public keys

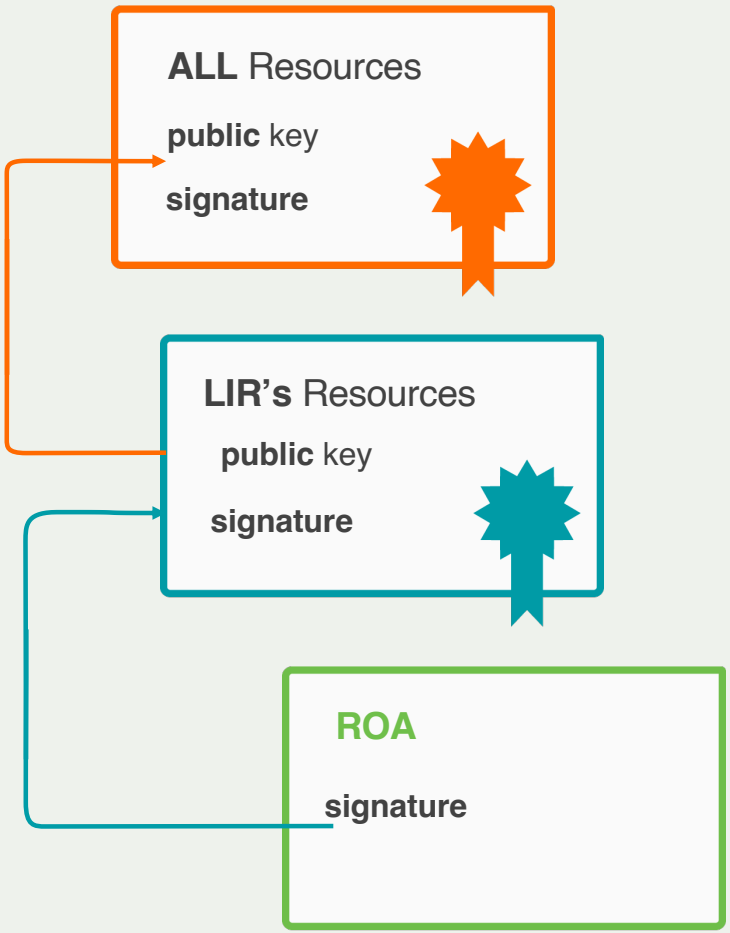


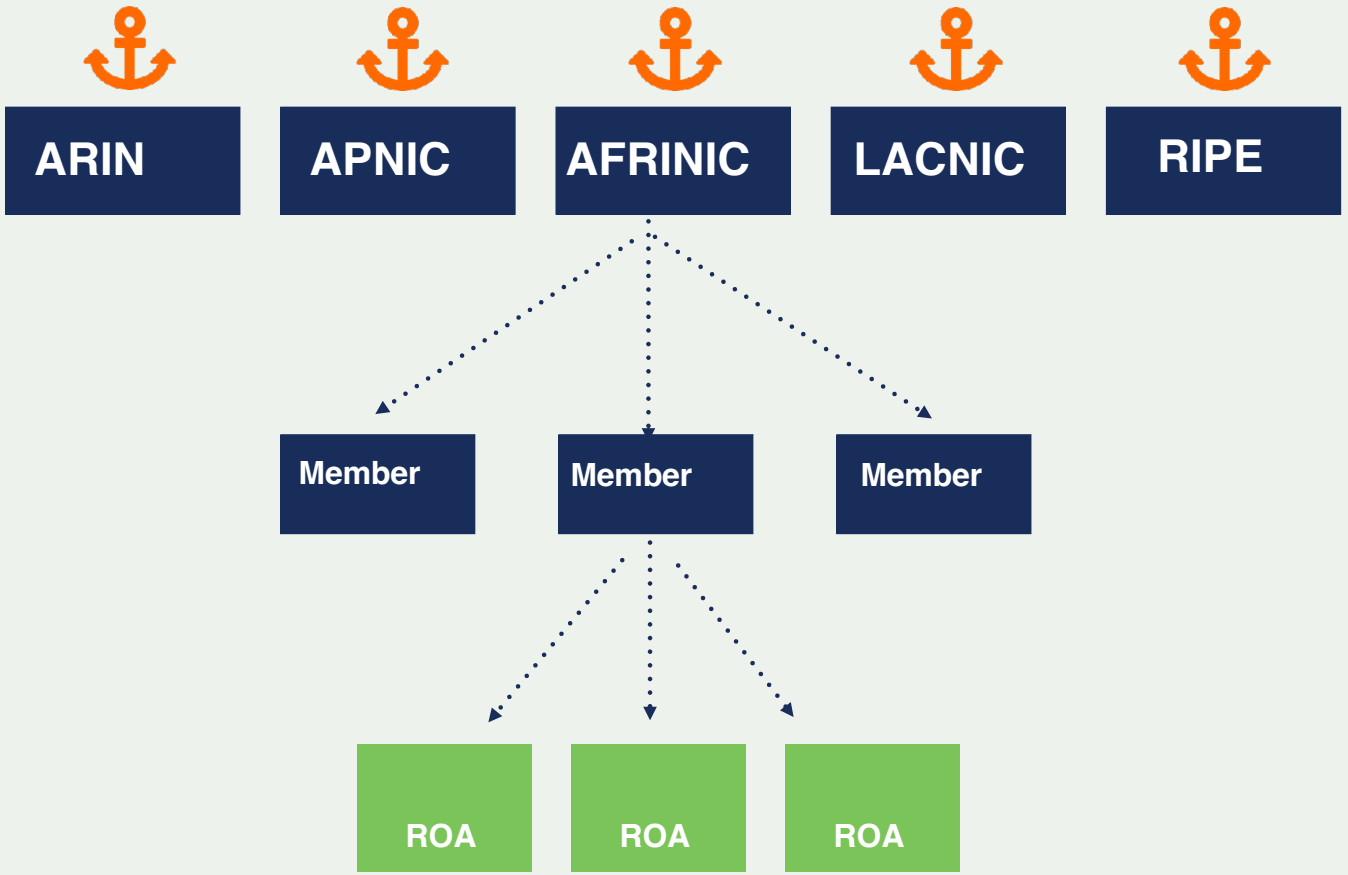
Follows the hierarchy of the registries

Authorised statements from resource holders

- “ASN X is authorised to announce my Prefix Y”
- Signed, holder of Y
- Statement can be cryptographically validated using Chain of Trust

RPKI Chain of Trust

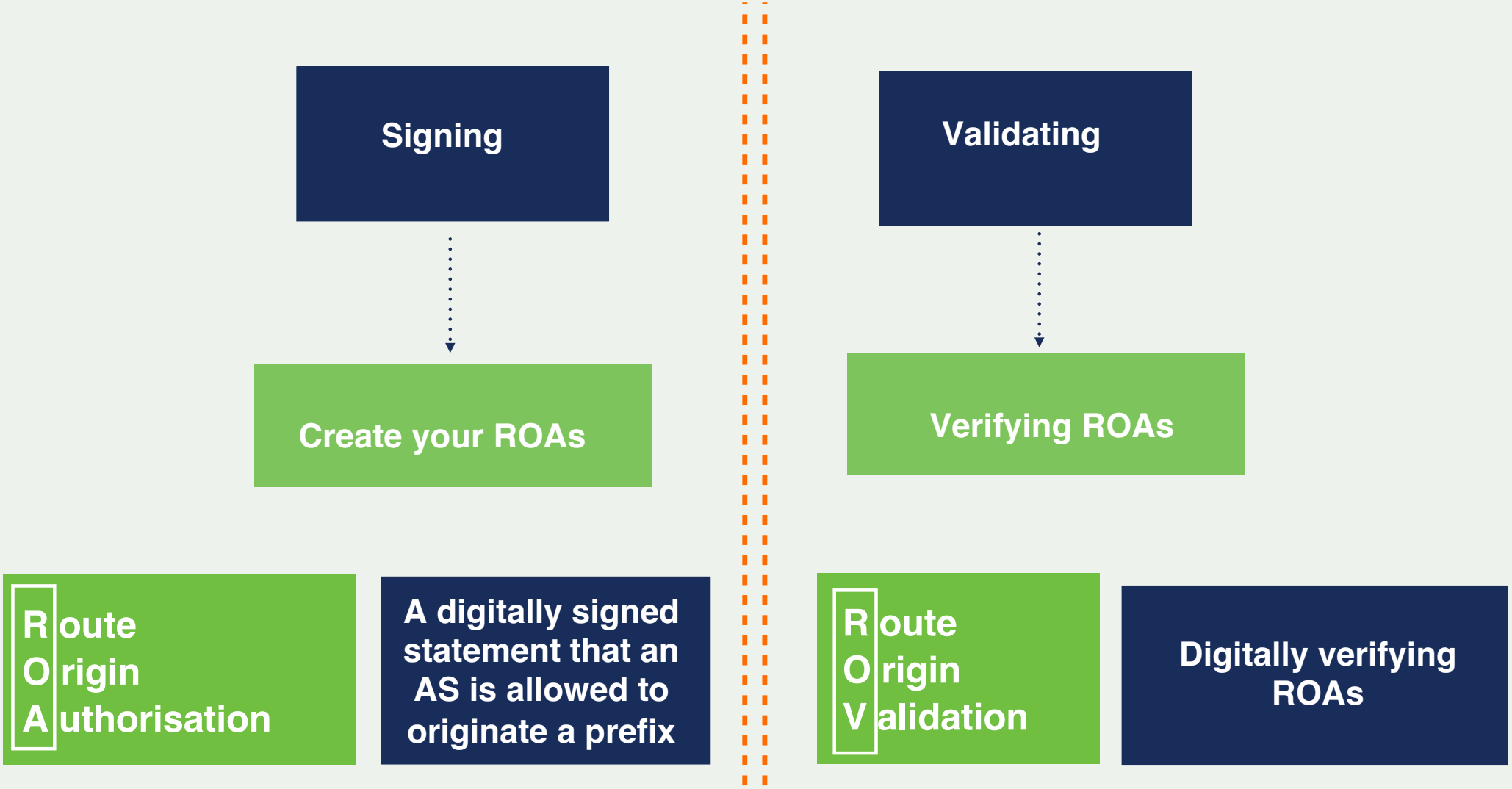




RAO

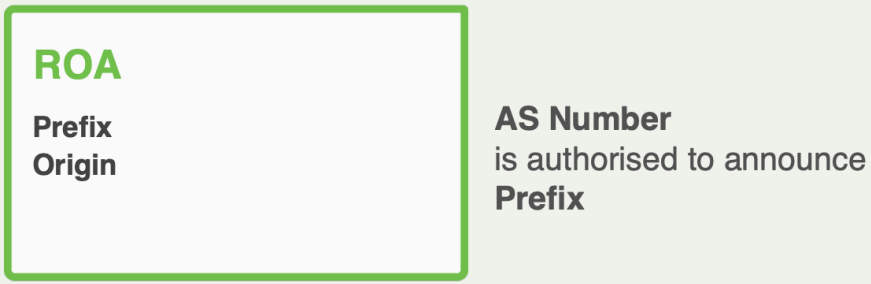
Route Origin Authorisation

Elements of RPKI



What is a ROA ?

An **authorised statement** from a resource holder



What is a ROA ?

LIRs can create a ROA for their resources

Multiple ROAs can exist for the same prefix

- With different origin/maxlength

ROAs can overlap

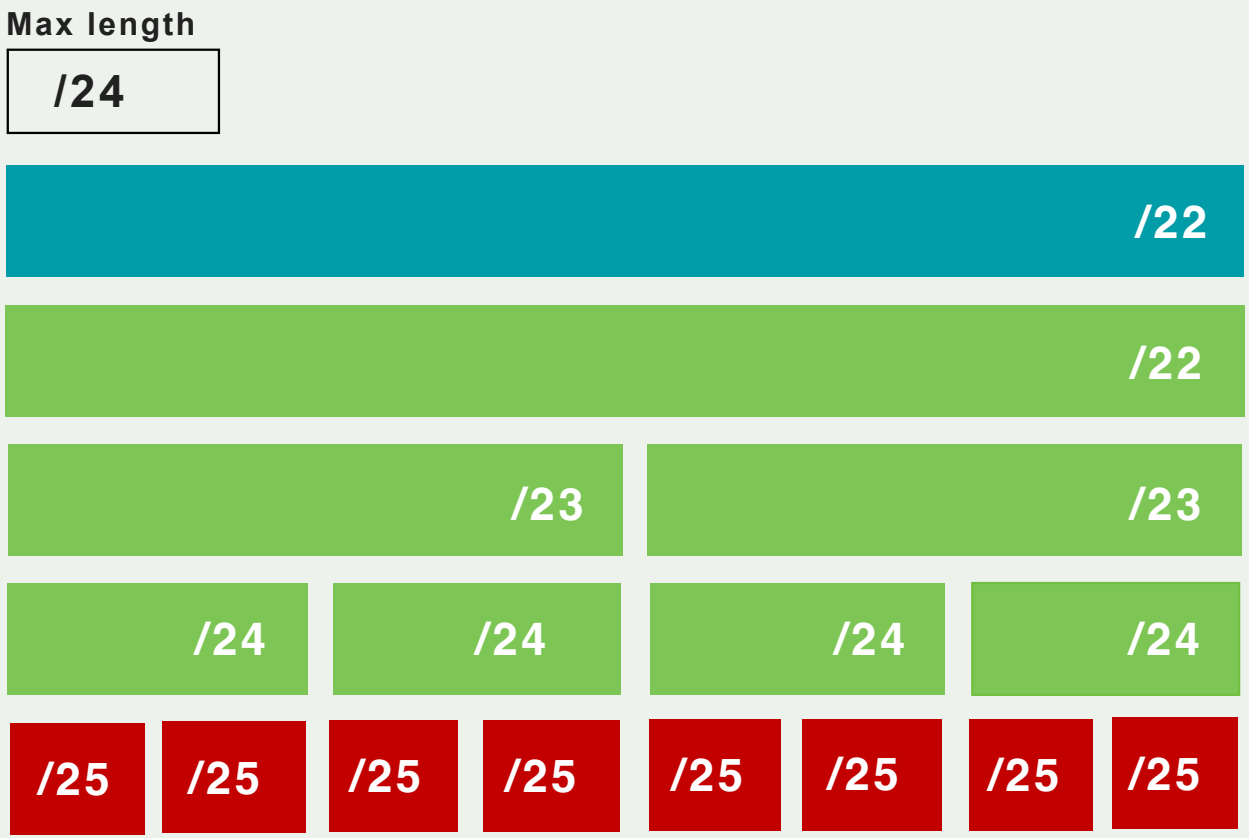
What is in a ROA ?

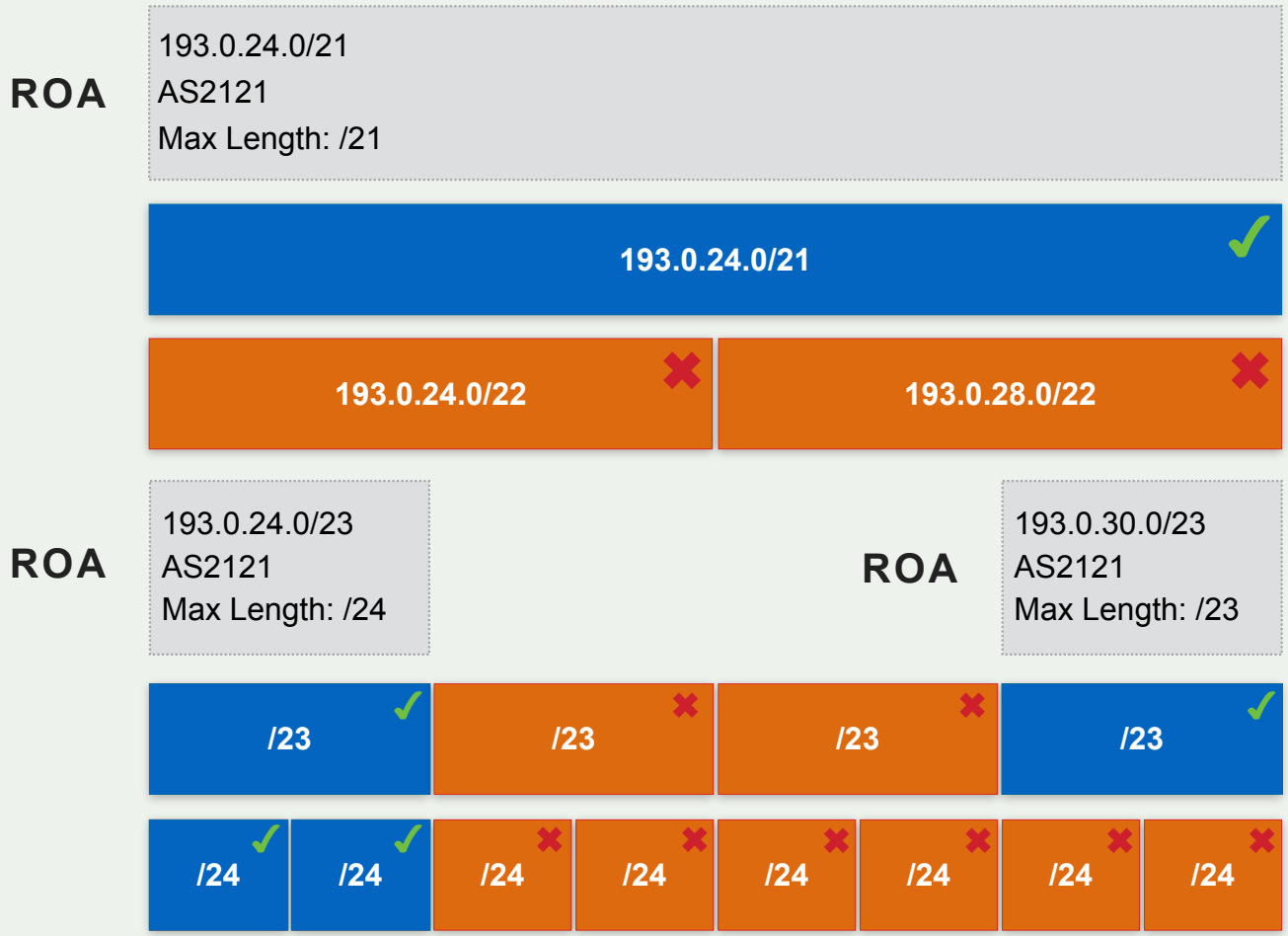
The network for which you are creating the ROA

The ASN supposed to originate the BGP Announcement

The maximum prefix length that ROA is authorised to advertise

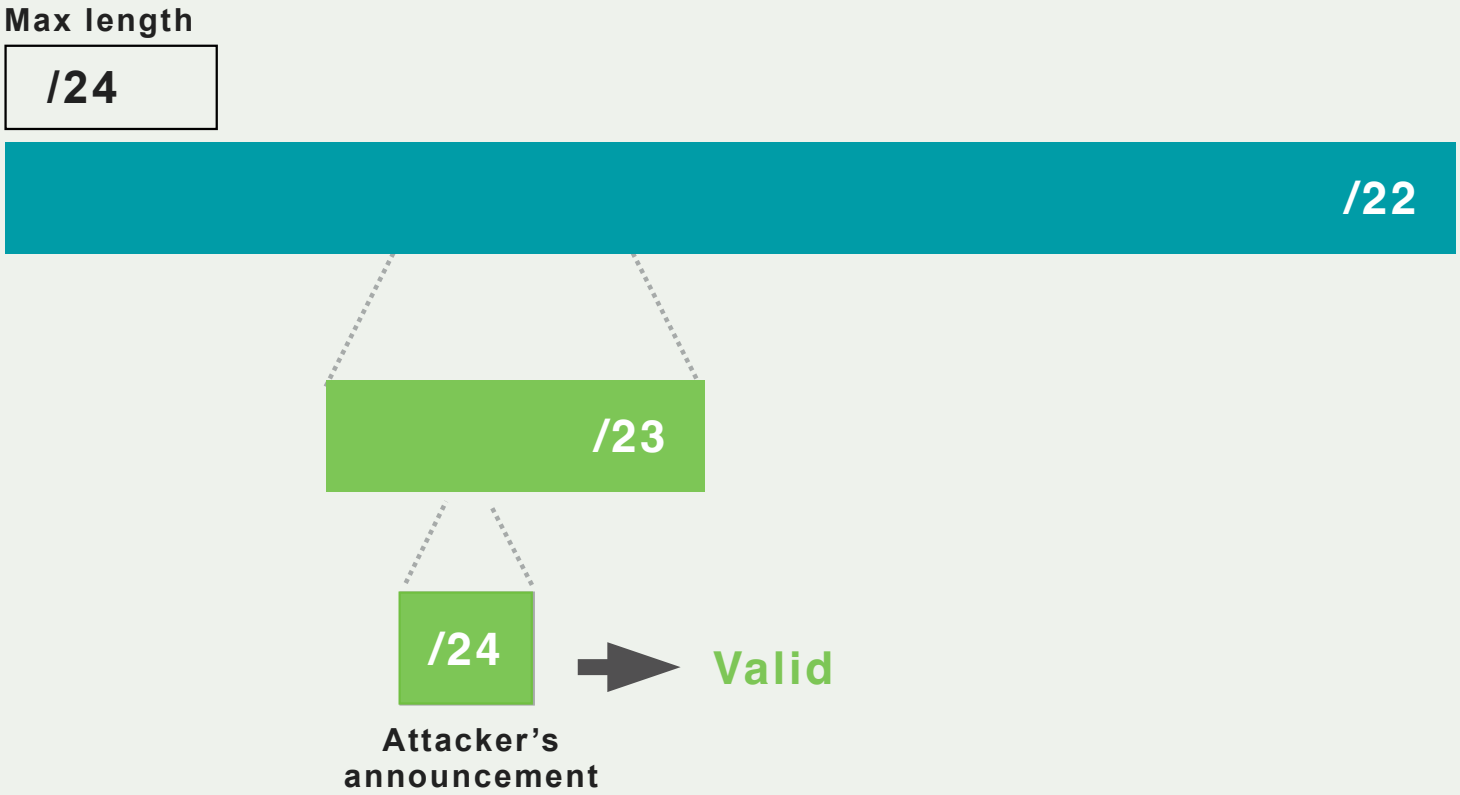
What is max-length?




ROA
193.0.24.0/21
AS2121
Max Length: /21
193.0.24.0/21
193.0.24.0/22
193.0.28.0/22
ROA
193.0.24.0/23
AS2121
Max Length: /24
ROA
193.0.30.0/23
AS2121
Max Length: /23
/23
/23
/23
/23
/24
/24
/24
/24
/24
/24
/24
/24

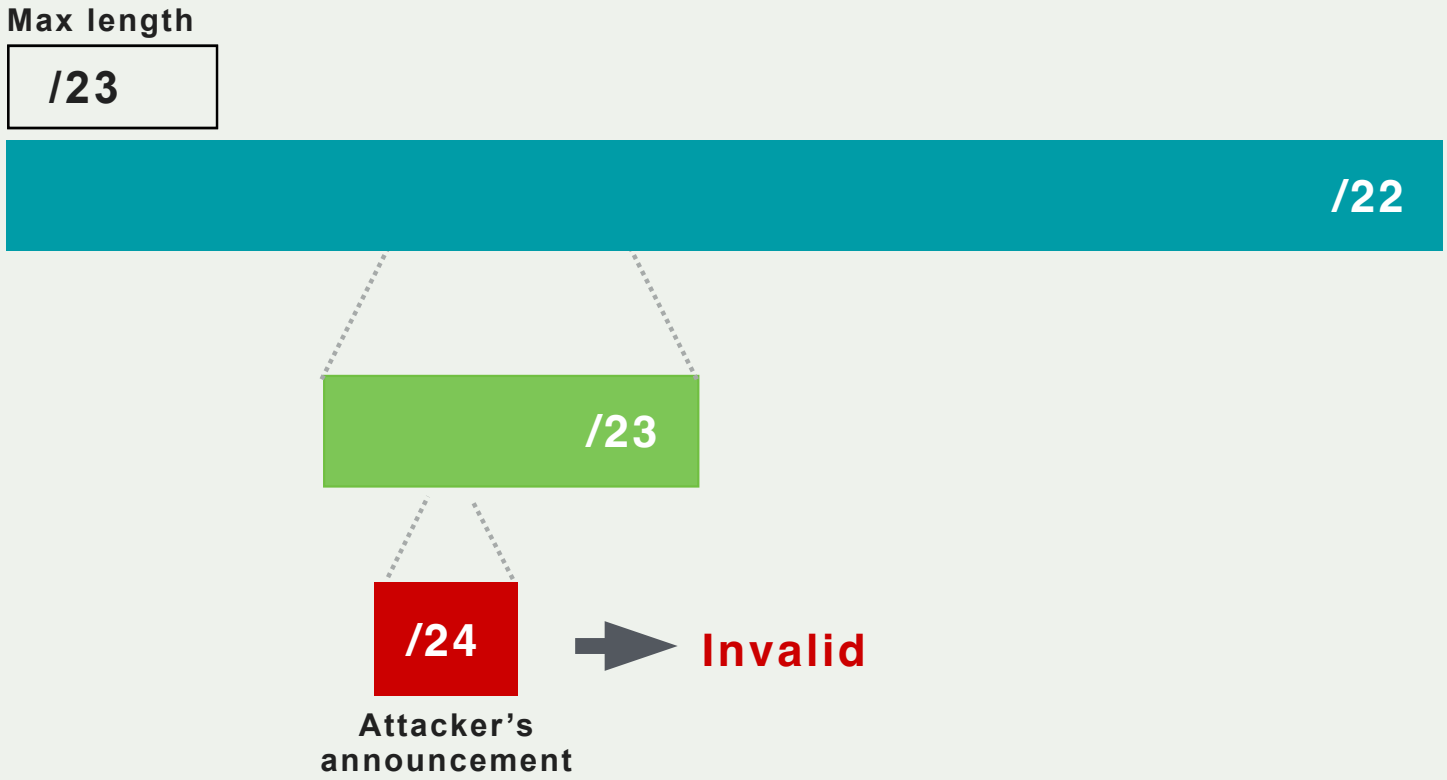
How should we use max-length?

You created a single ROA authorising the entire /22



How should we use max-length?

Create ROAs for BGP announcements only



Hosted RPKI

RIR hosts a CA and signs all ROAs

Automate signing and key rollovers

Allows you focus on creating and publishing ROAs

Delegated RPKI

Run your own Certificate Authority software

- Dragon Research Labs, RPKI Toolkit
- NLnetlabs, Krill

Setup connection with RIR CA

Generate your LIR certificate and get it signed by parent CA

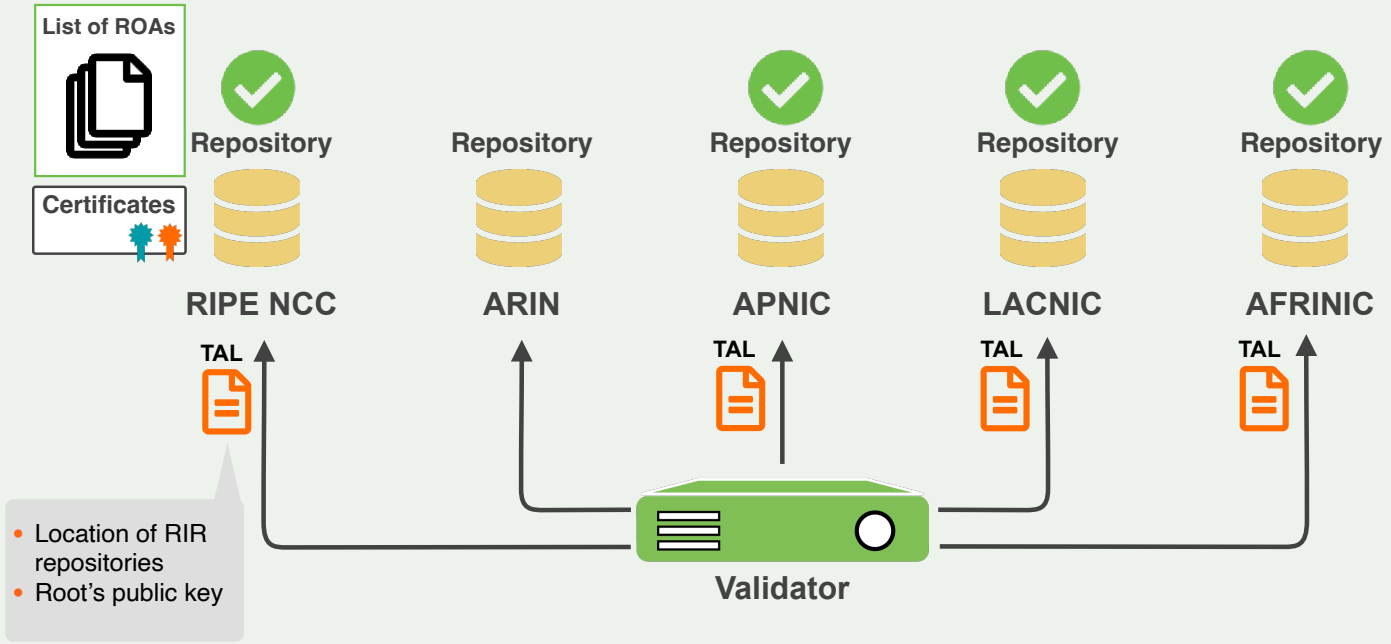
RPKI Valodators

RPKI Validators

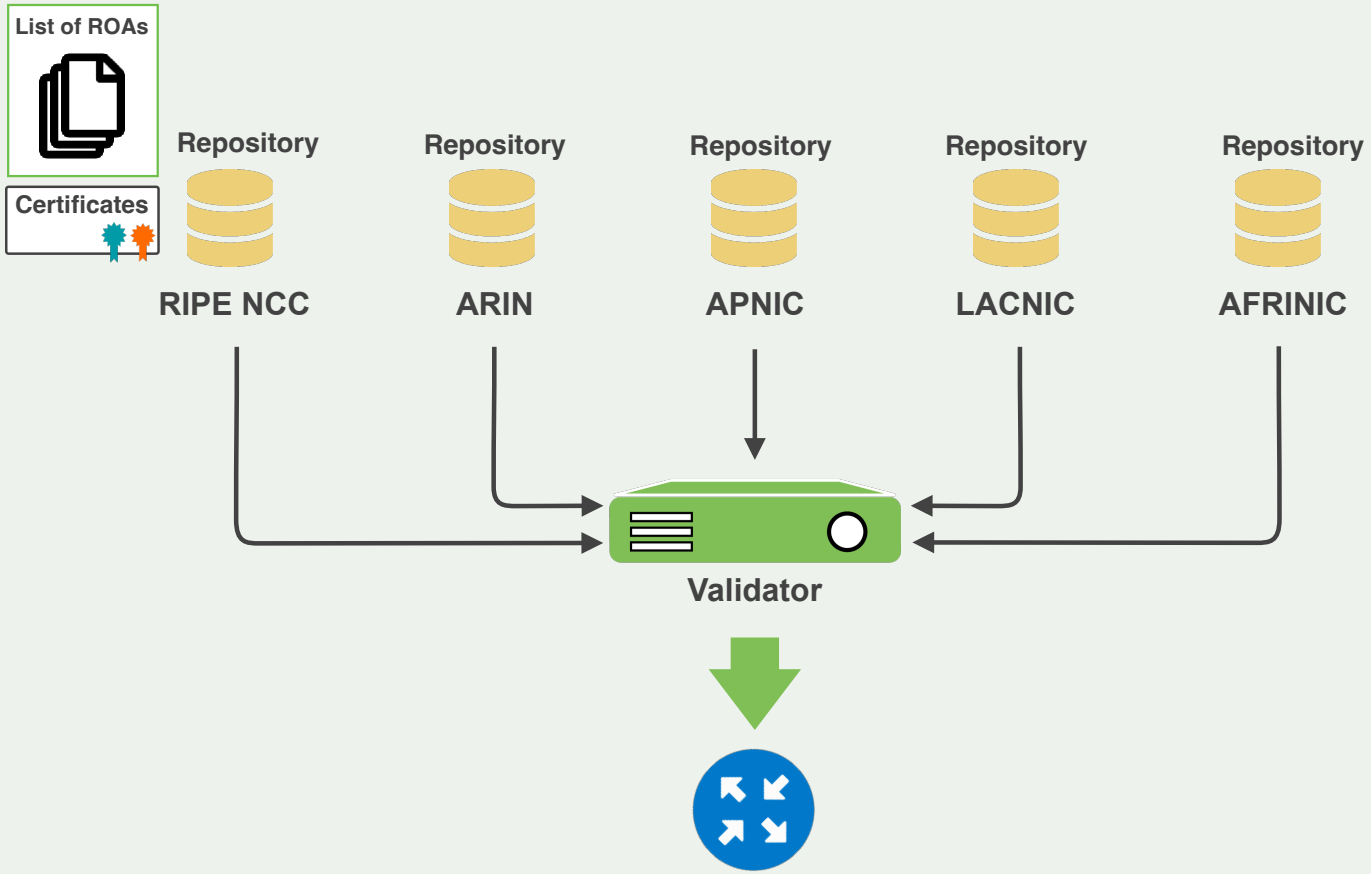
Software that creates a local **“validated cache”** with all the **valid ROAs**

- Downloads the RPKI repository from the RIRs
- Validates the chain of trust of all the ROAs and associated CAs
- Talks to routers using the RPKI-RTR Protocol

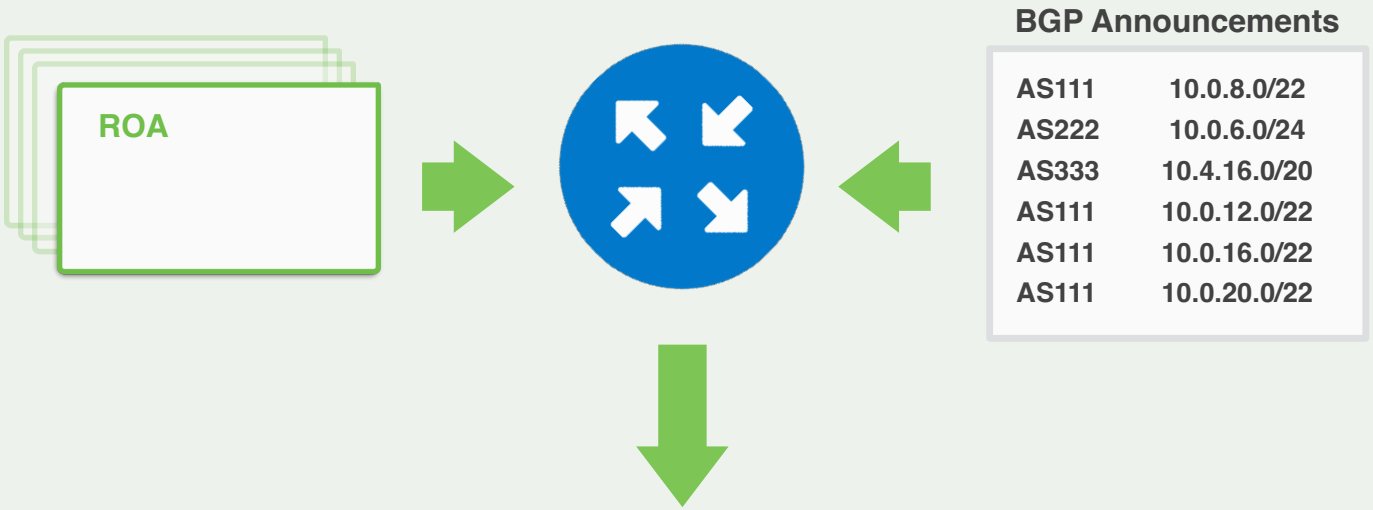
Trust Anchor Locator (TAL)



Relying Party



Relying Party



RPKI Validator Options

Routinator

- Built with Rust, by NLNetlabs

rpki-client

- Part of OpenBSD project, written in C

OctoRPKI

- Cloudflare's Relying Party software, written in Go

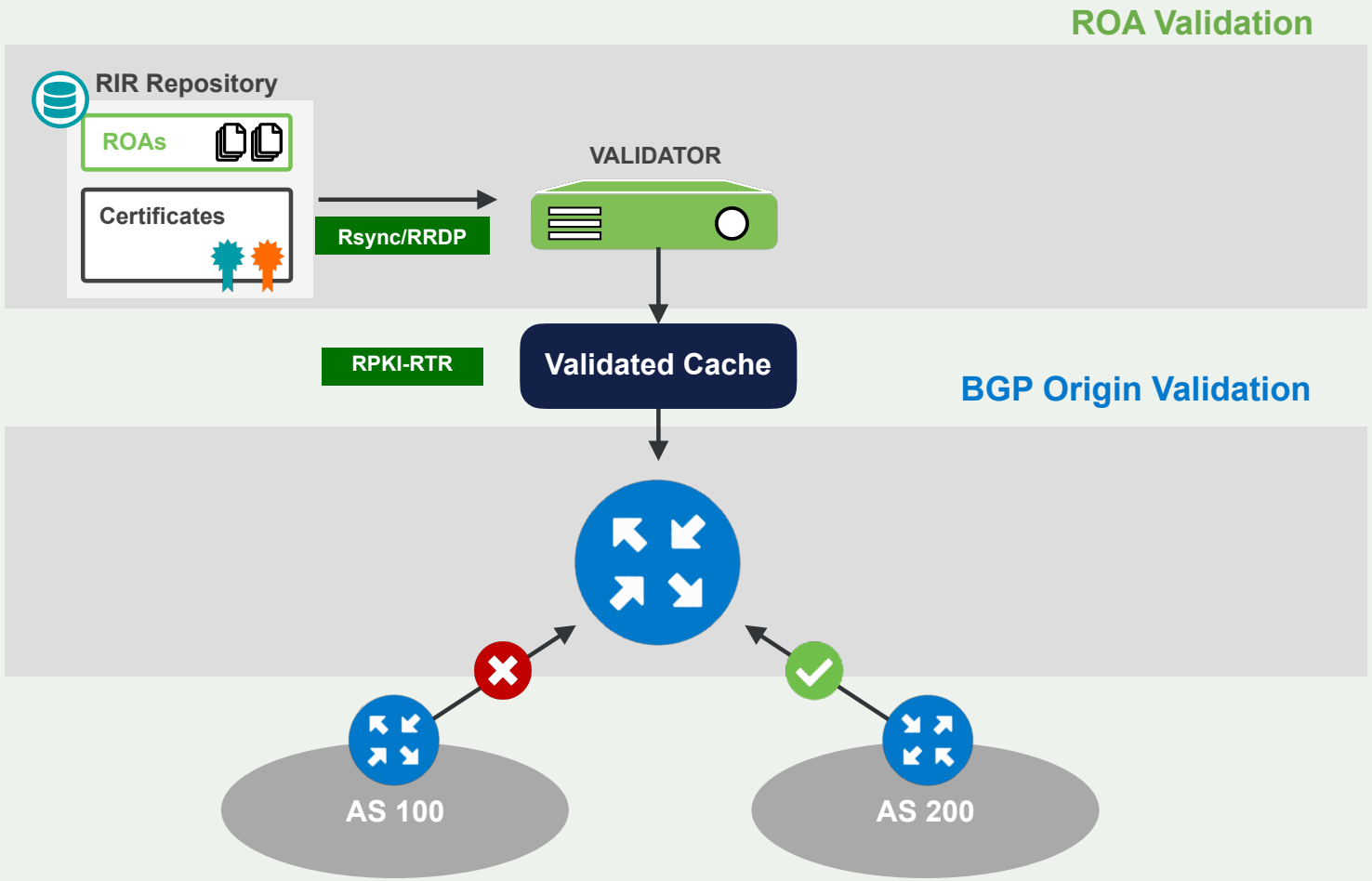
FORT

- Open source RPKI validator by NIC.mx/LACNIC, Written in C

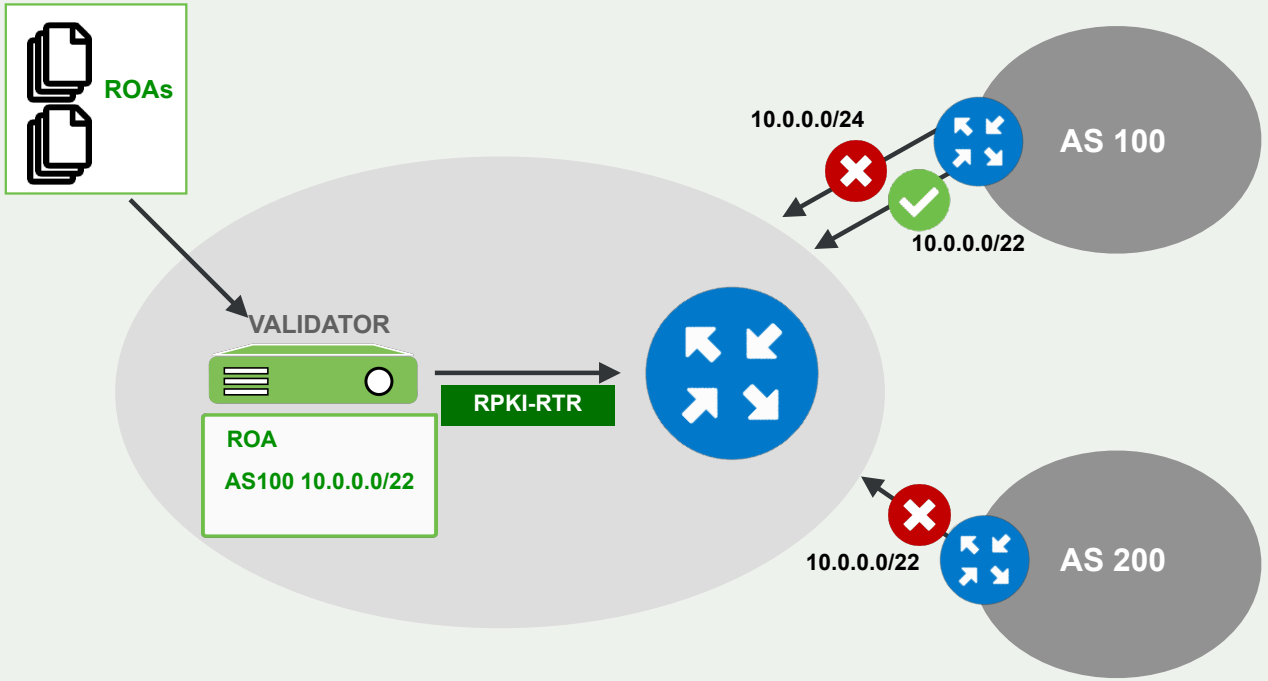
ROV

Route Origin Validation

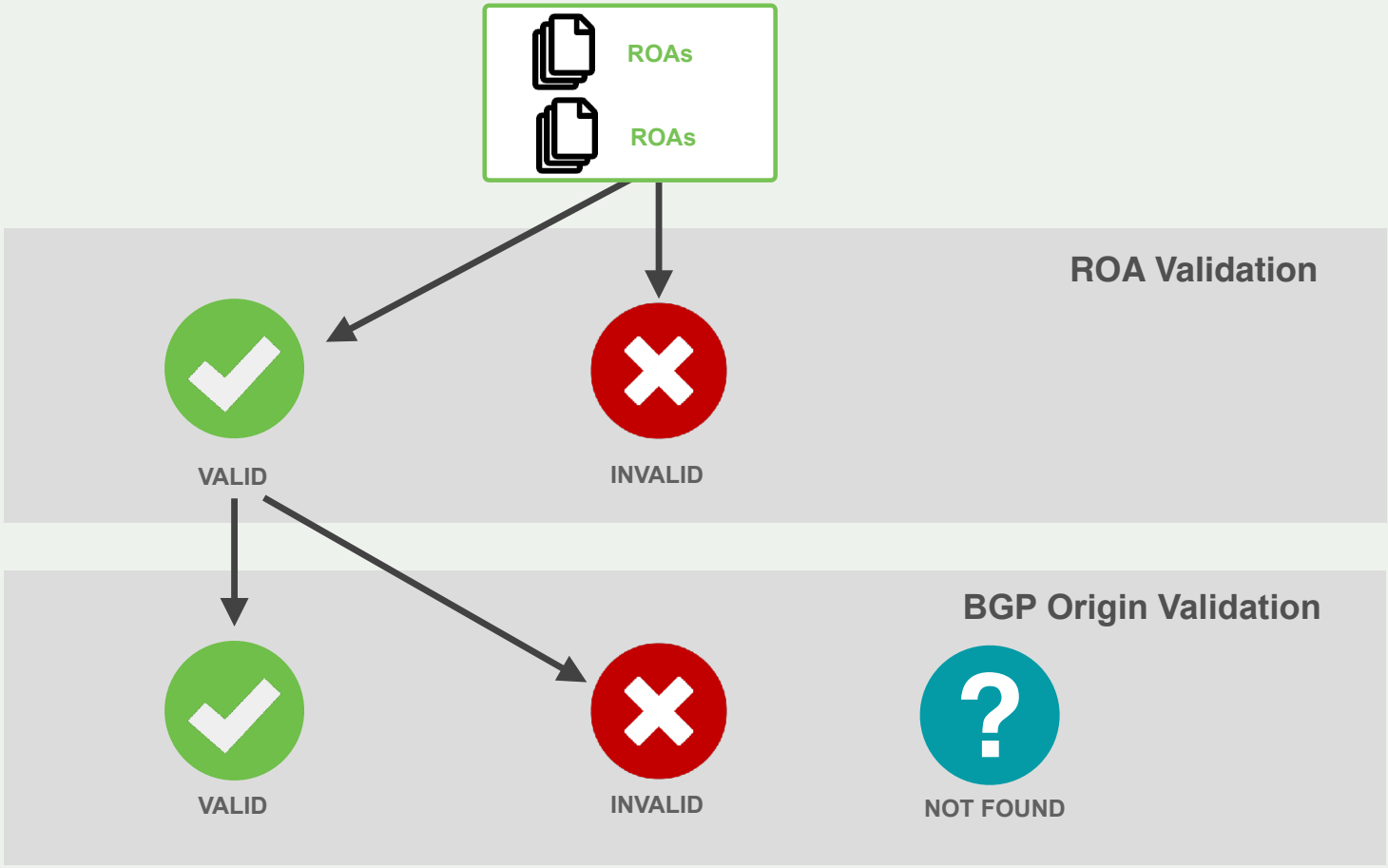
Validation


ROA Validation
RIR Repository
ROAs
Certificates
Rsync/RRDP
VALIDATOR
RPKI-RTR
Validated Cache
BGP Origin Validation
AS 100
AS 200

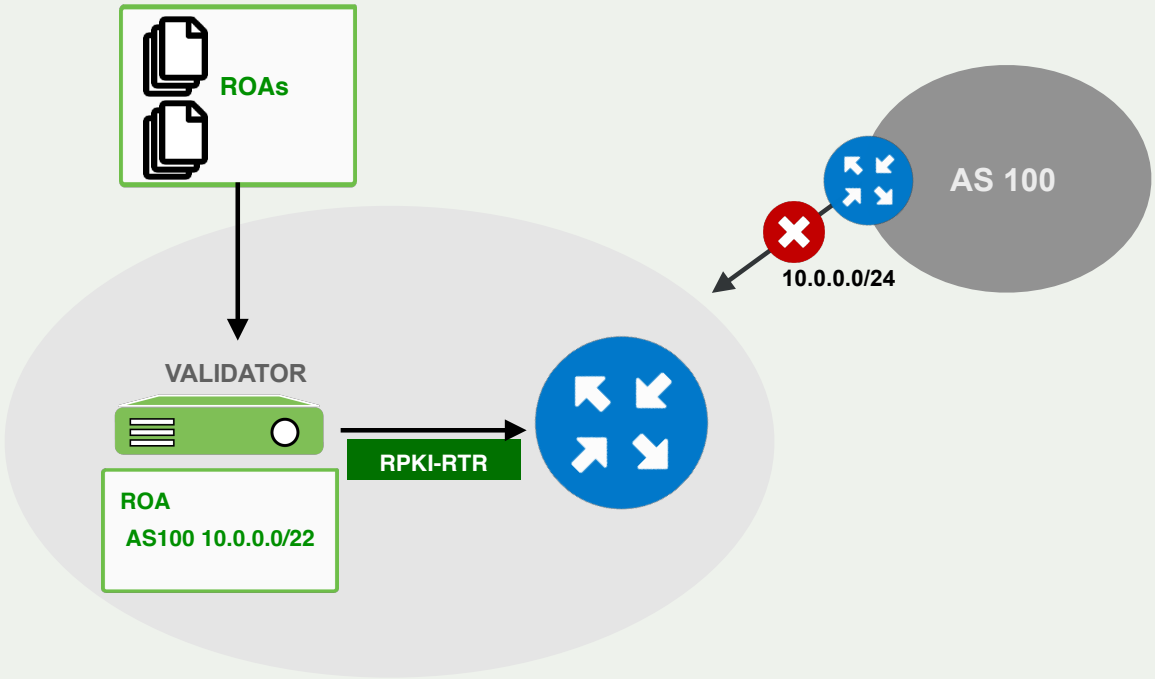
BGP Prefix Origin Validation-RFC6811



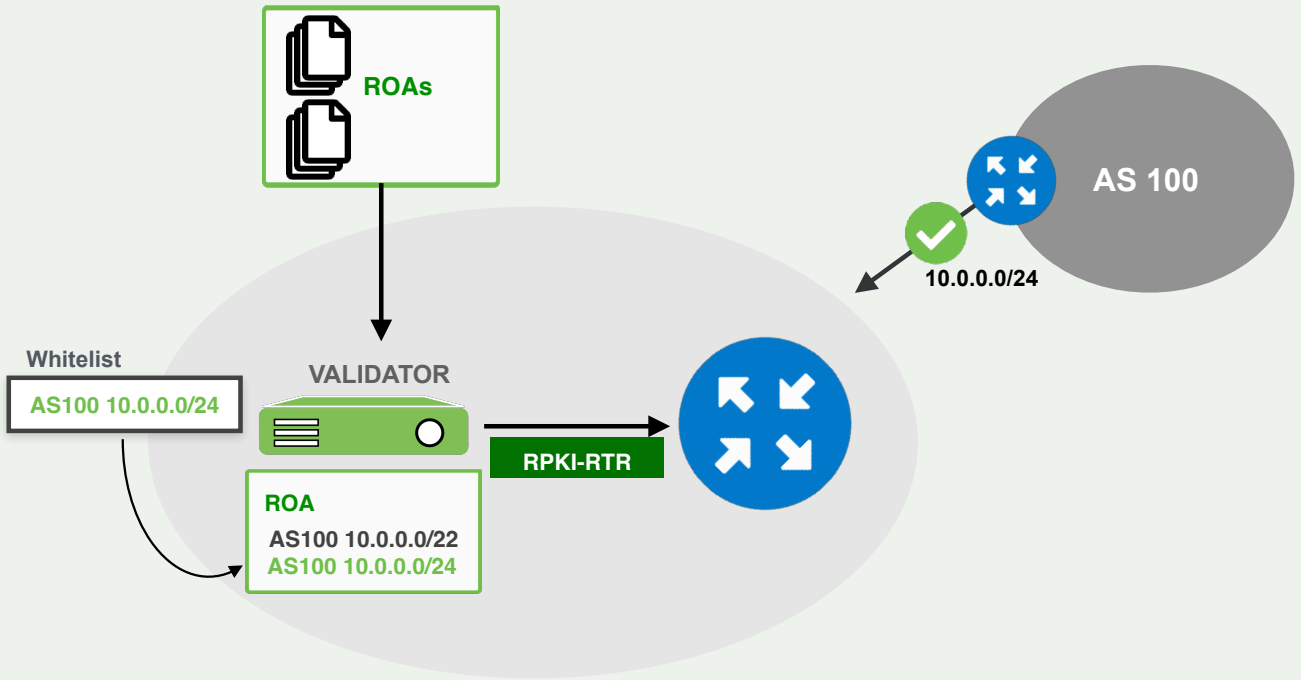
RPKI Validation States



Local Changes to ROA DB (using SLURM)



Local Changes to ROA DB (using SLURM)



MANRS Observatory

MANRS Observatory

Provides a factual state of security and resilience of the Internet routing system and track it over time

Measurements are:

- Transparent – using publicly accessible data
- Passive – no cooperation from networks required
- Evolving – MANRS community decide what gets measured and how

MANRS Observatory Access

Launched in 2019

Uses trusted, publicly available third-party data

Anyone may view aggregated data

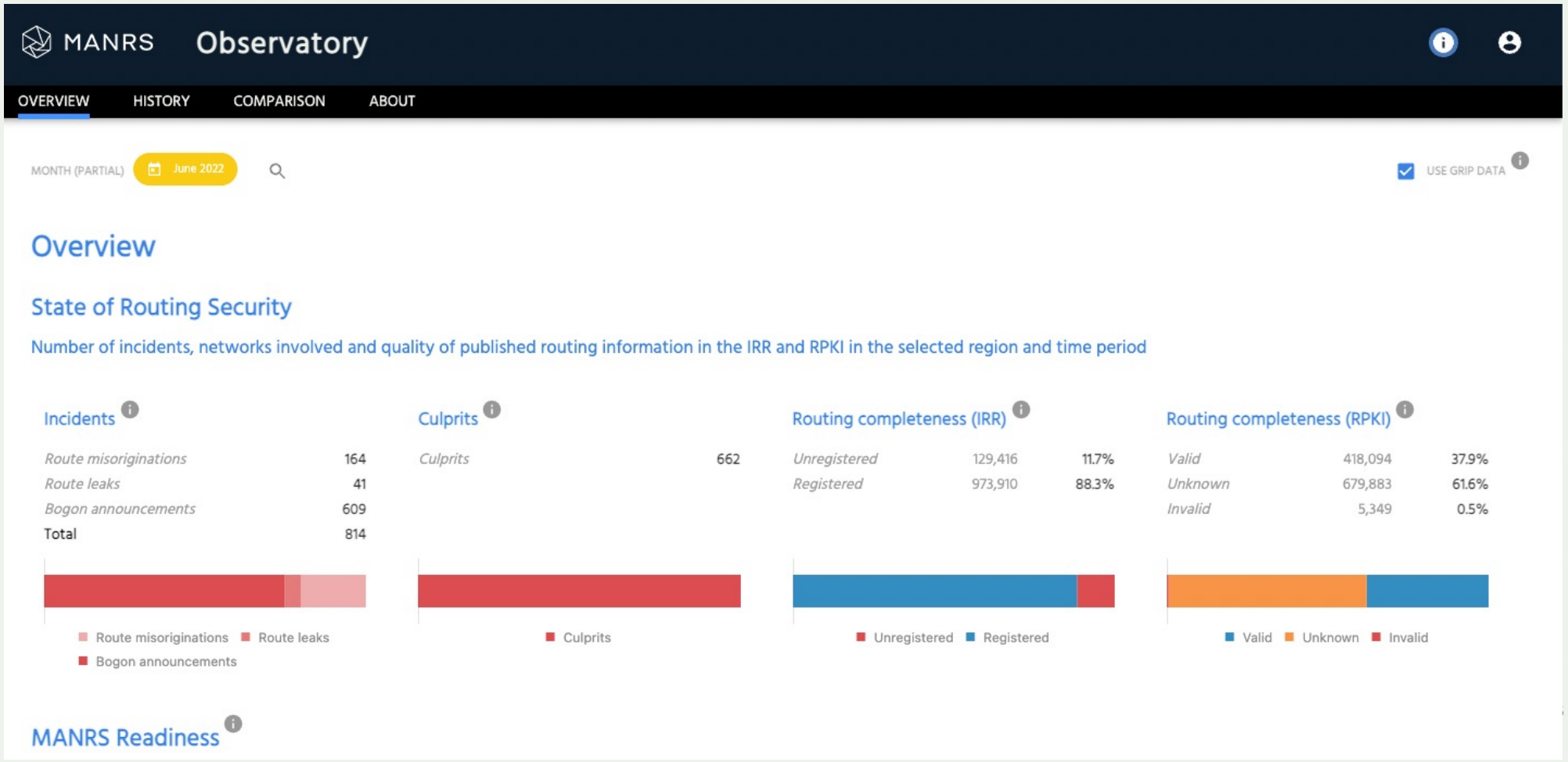
Only MANRS Participants have access to detailed data about their own network

Research/partner access is available

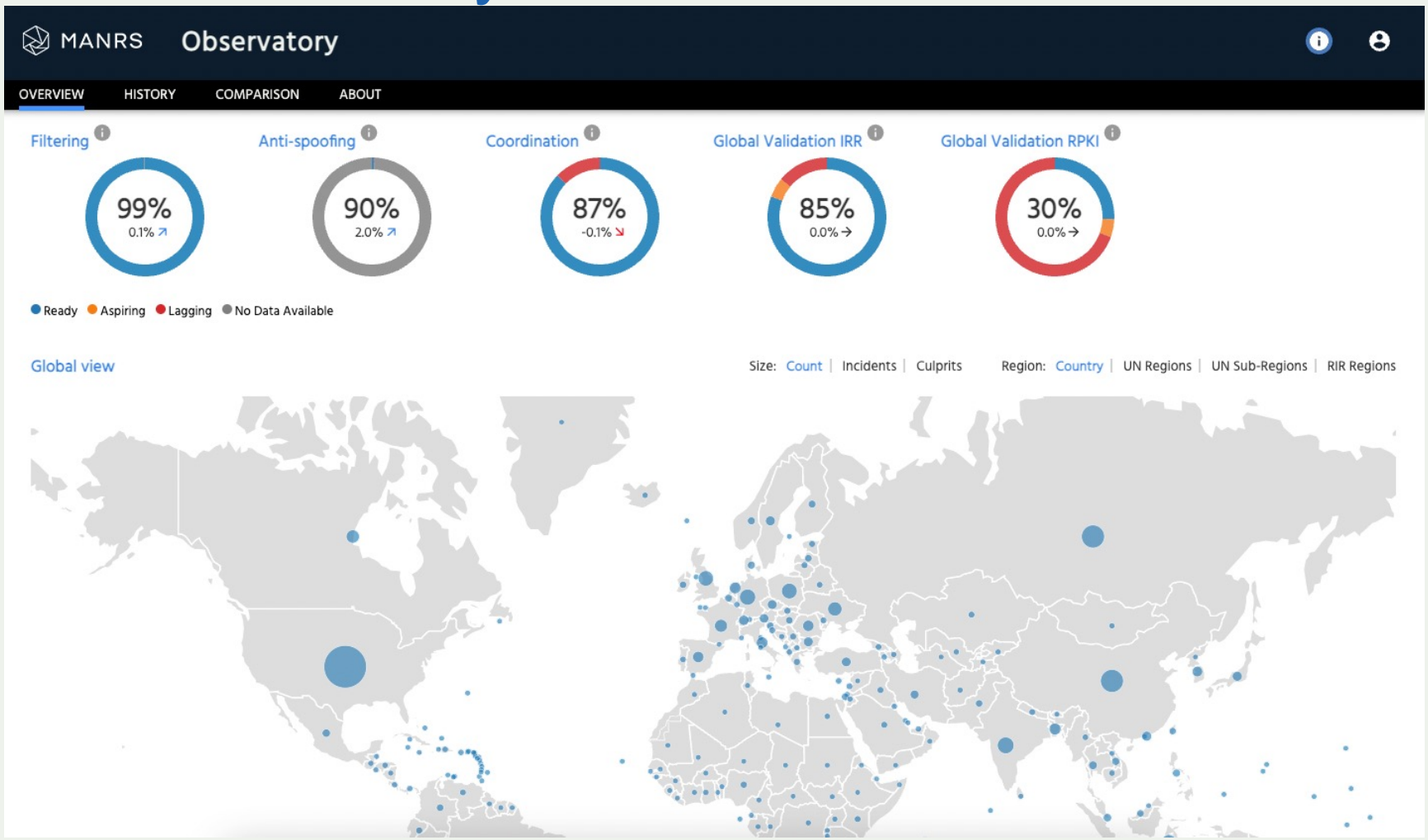
Caveats:

- There are still some false positives
- Lack of security controls is not always visible

MANRS Observatory



MANRS Observatory

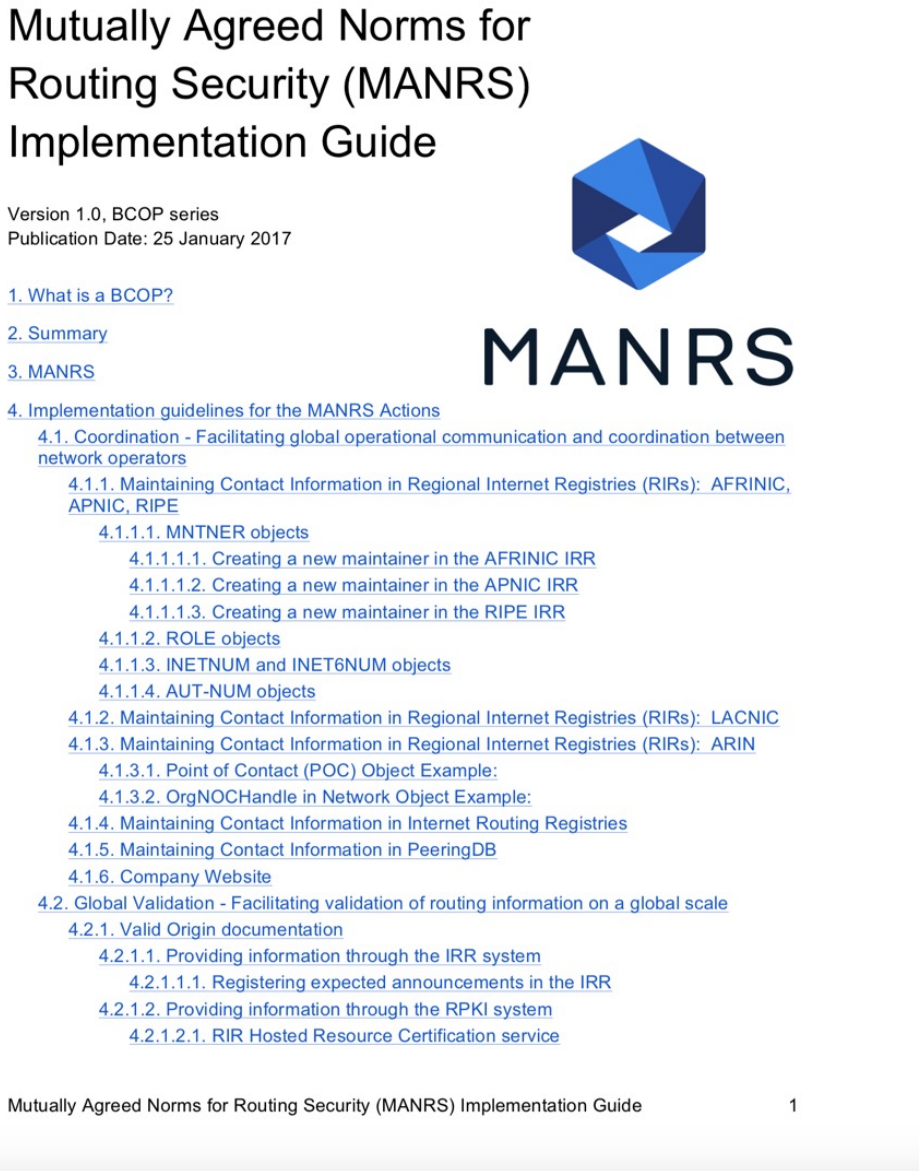


Learn More and Join Us

MANRS Implementation Guide for Network Operators

If you're not ready to join yet, implementation guidance is available to help you.

- Based on Best Current Operational Practices deployed by network operators around the world
- Recognition from the RIPE community by being published as RIPE-706
- https://www.manrs.org/netops/guide/



Mutually Agreed Norms for Routing Security (MANRS) Implementation Guide

Version 1.0, BCOP series
Publication Date: 25 January 2017

MANRS

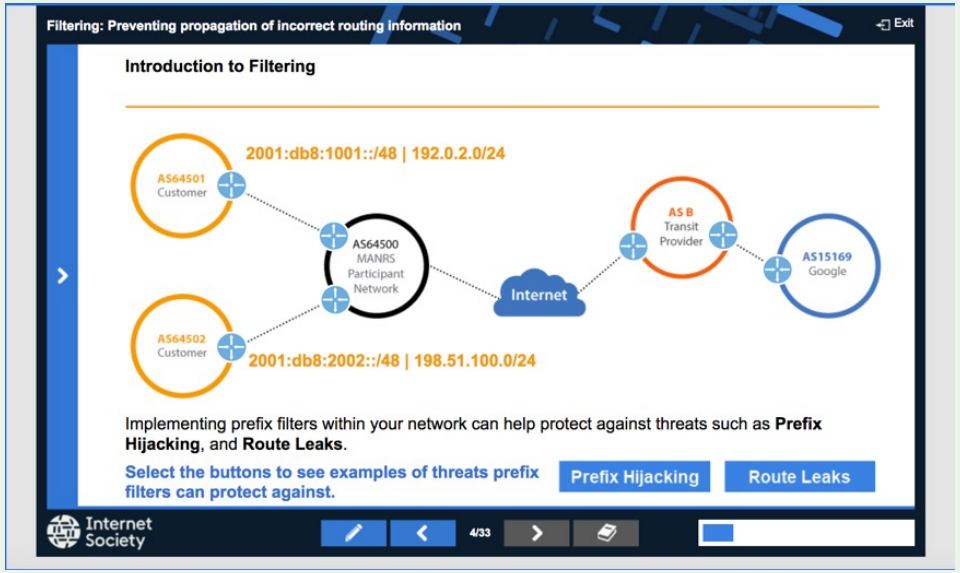
MANRS Tutorials

Tutorials based on information in the Implementation Guide

Walks through the tutorial with a test at the end of each module

Working with and looking for partners that are interested in integrating it in their curricula

https://www.manrs.org/tutorials



Join Us

Visit https://www.manrs.org

- Fill out the form with as much detail as possible.
- We will ask questions and run tests

Get Involved in the Community

- Members support the initiative and implement the actions in their own networks
- Members maintain and improve the documents and promote MANRS objectives

LEARN MORE:

https://www.manrs.org

FOLLOW US:

/RoutingMANRS

Thank you.

Musa Stephen HONLUE

honlue@gmail.com / tephen.Honlue@afrinic.net

Twitter: @mhonlue

manrs.org