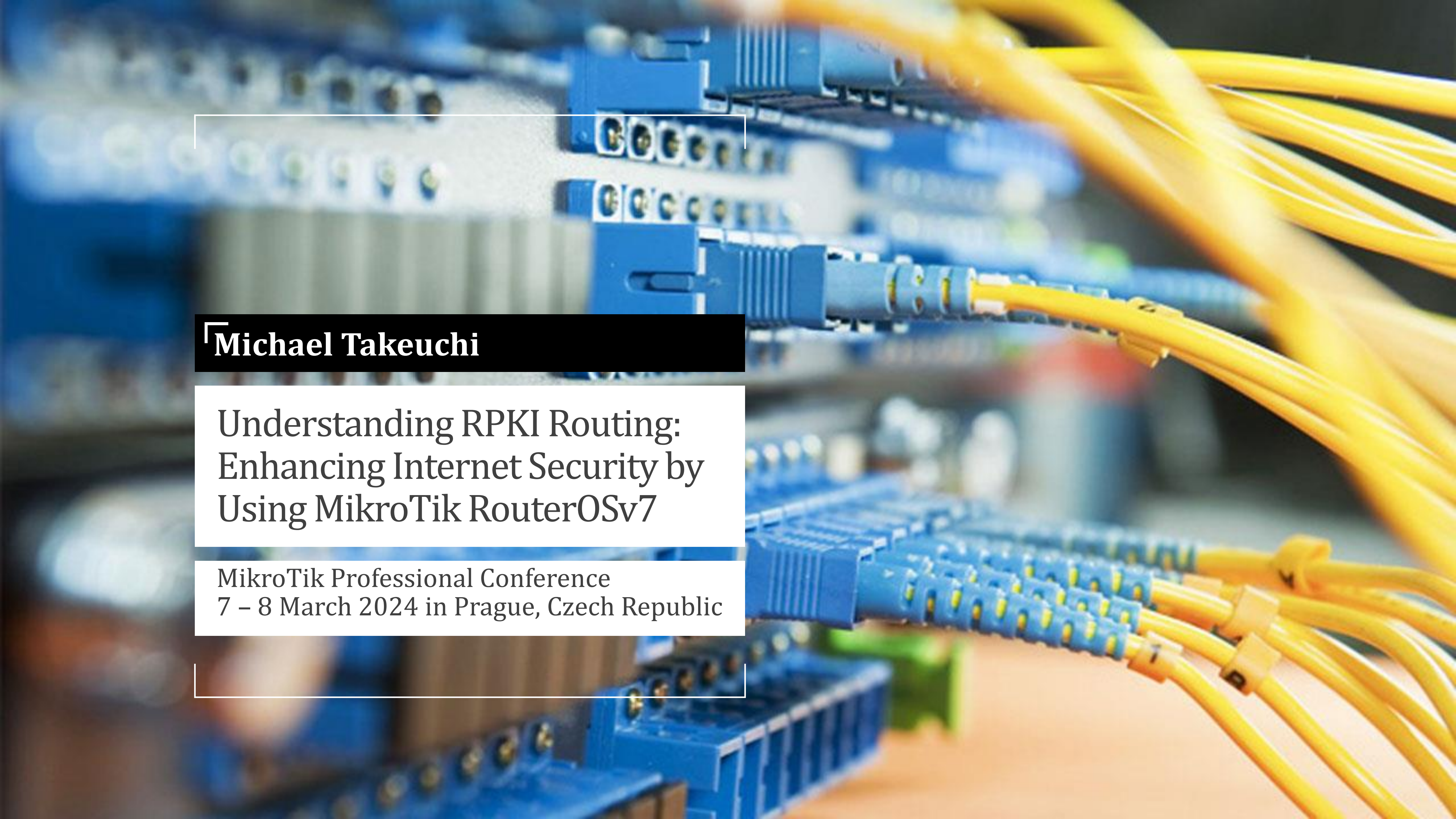


Michael Takeuchi

Understanding RPKI Routing: Enhancing Internet Security by Using MikroTik RouterOSv7

MikroTik Professional Conference
7 – 8 March 2024 in Prague, Czech Republic

Hello, I am **Michael Takeuchi**

- Certified Cisco CCNP, Juniper JNCIP-(DC|ENT|SP), **MikroTik Engineer & Trainer,** Fortinet NSE, EC-Council
- Chief Technology & Operating Officer (CTO) at PT Media Cepat Indonesia (RAPIDNET)
- Indonesia Internet eXchange (IIX) Squad Team
- Managed more than 25+ Networks/Autonomous System (AS) in APAC, EMEA & Others
- Connected to IIX, JKT-IX, Biznet IX, NiCE/OpenIXP, C2IX, INIX, neuCentrIX, CDIX, DCI-IX, cXc, Amsterdam AMS-IX, Frankfurt DE-CIX, Singapore SGIX, Equinix IX, MegaIX & a Few Other Private Internet Exchange
- Based in Jakarta, Indonesia

✉ michael@takeuchi.id / michael.takeuchi@rapid.net.id
in https://www.linkedin.com/in/michael-takeuchi
@mtakeuchi

How was the Internet built?

Yes, it was done by **BGP Routing!**

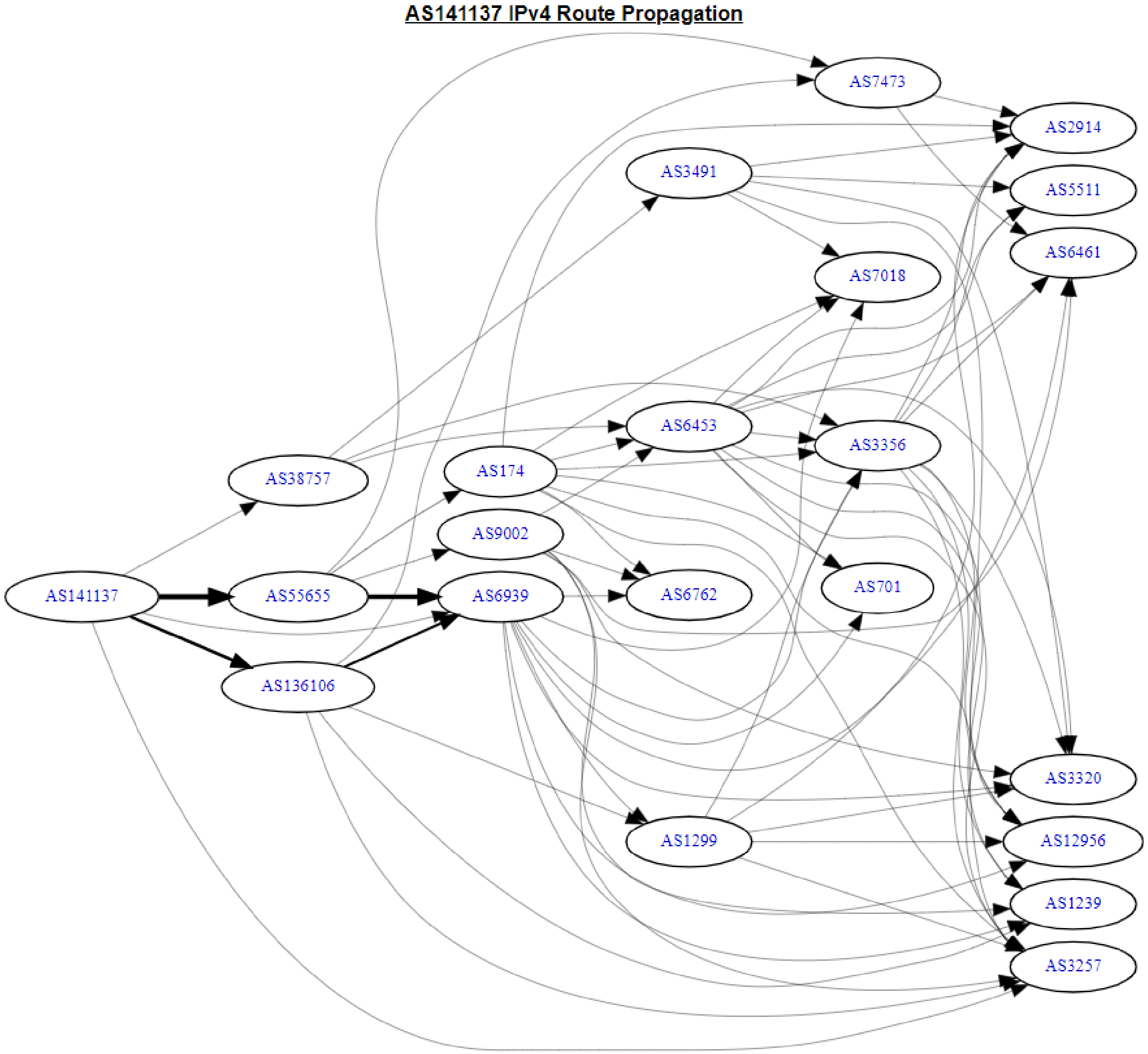
Border Gateway Protocol (BGP)

BGP is crucial for the proper functioning of the Internet, is used to exchange routing and reachability information between different autonomous systems (AS) on the Internet.

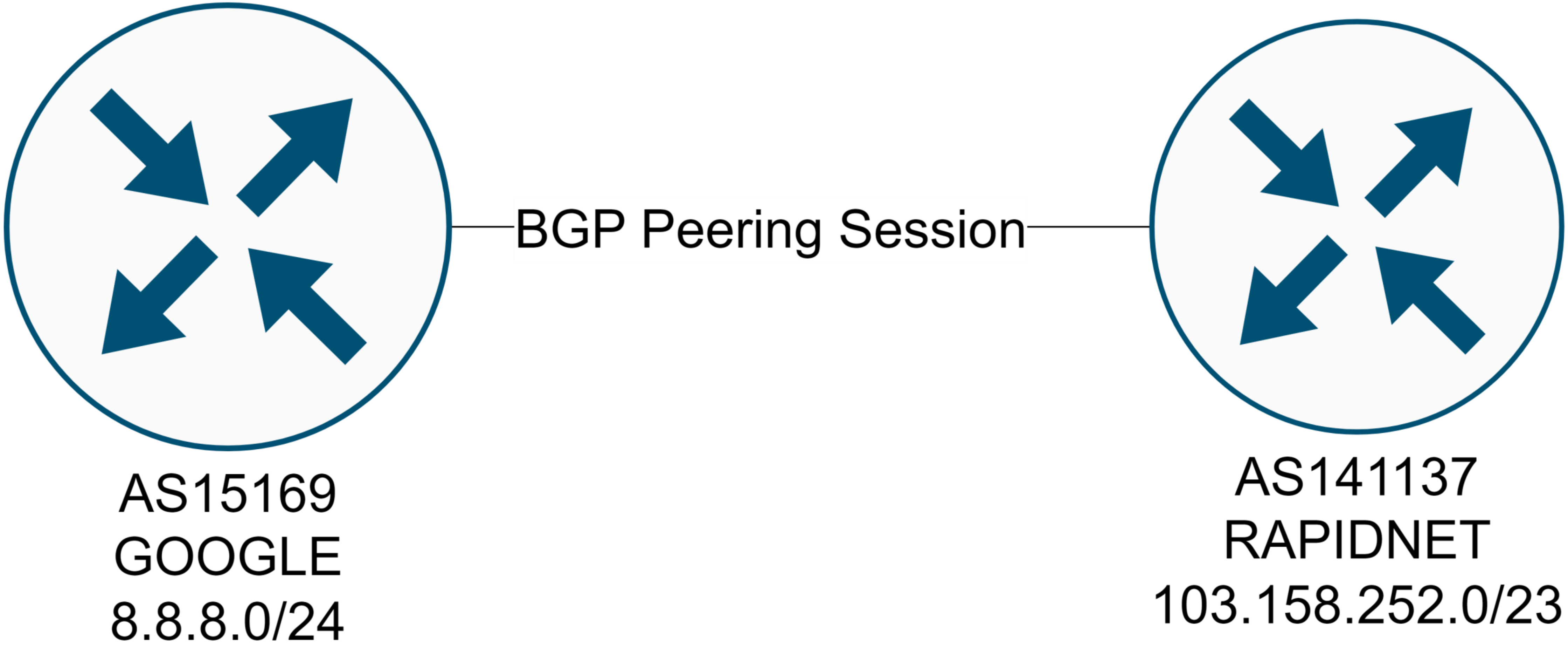
An autonomous system is a collection of IP networks and routers under the control of a single organization that presents a common routing policy to the Internet.

https://rpki-rfc.routingsecurity.net/
https://en.wikipedia.org/wiki/Resource_Public_Key_Infrastructure

How BGP formed the Internet – bgp.he.net



Each AS Number will advertise their networks



How we can **verify**
the prefix advertisement?

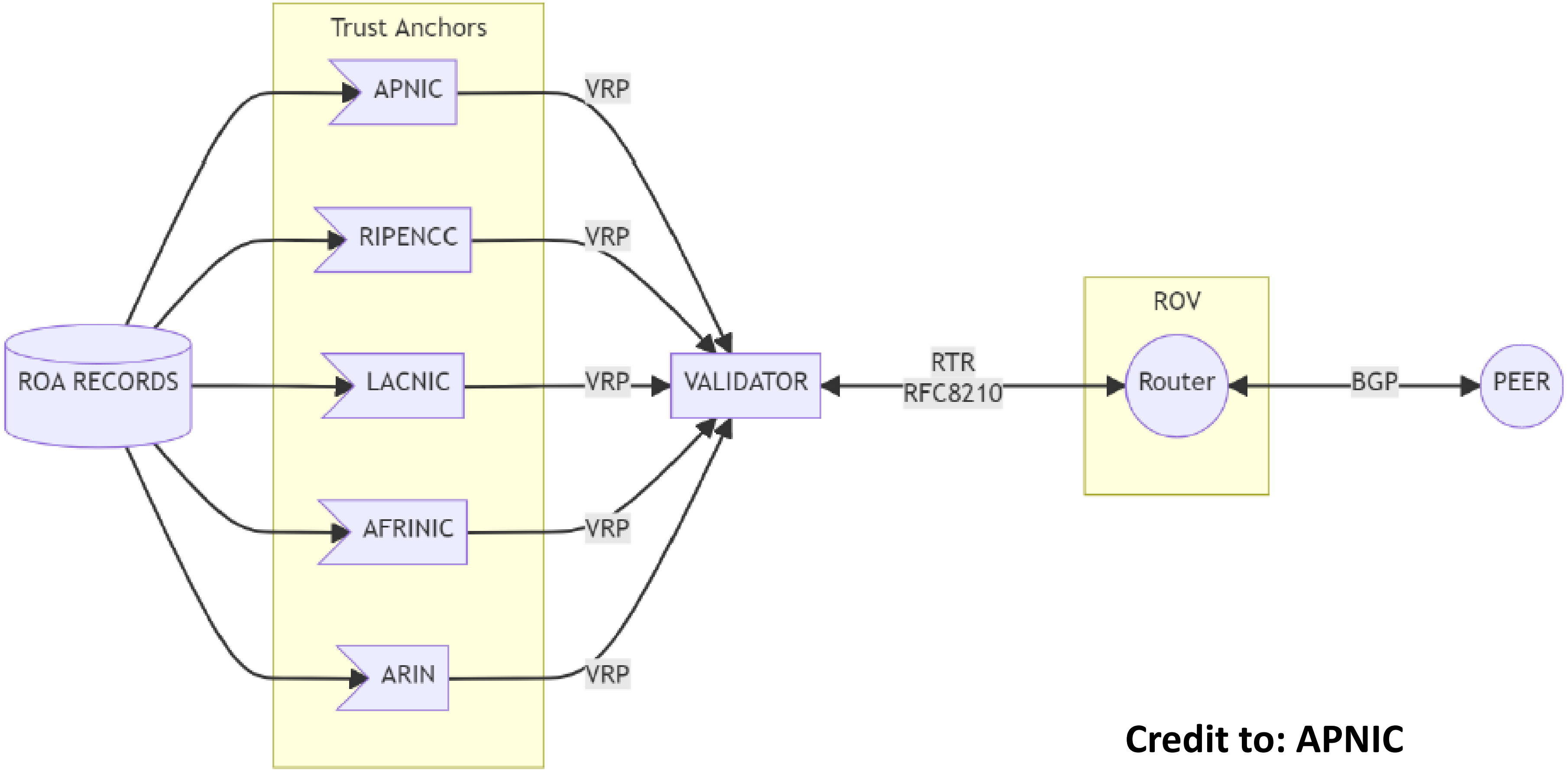
Resource Public Key Infrastructure (RPKI)

also known as Resource Certification, is a specialized public key infrastructure (PKI) framework to support improved security for the Internet's BGP routing infrastructure.

RPKI provides a way to connect Internet number resource information (such as Autonomous System numbers and IP addresses) to a trust anchor.

https://rpki-rfc.routingsecurity.net/
https://en.wikipedia.org/wiki/Resource_Public_Key_Infrastructure

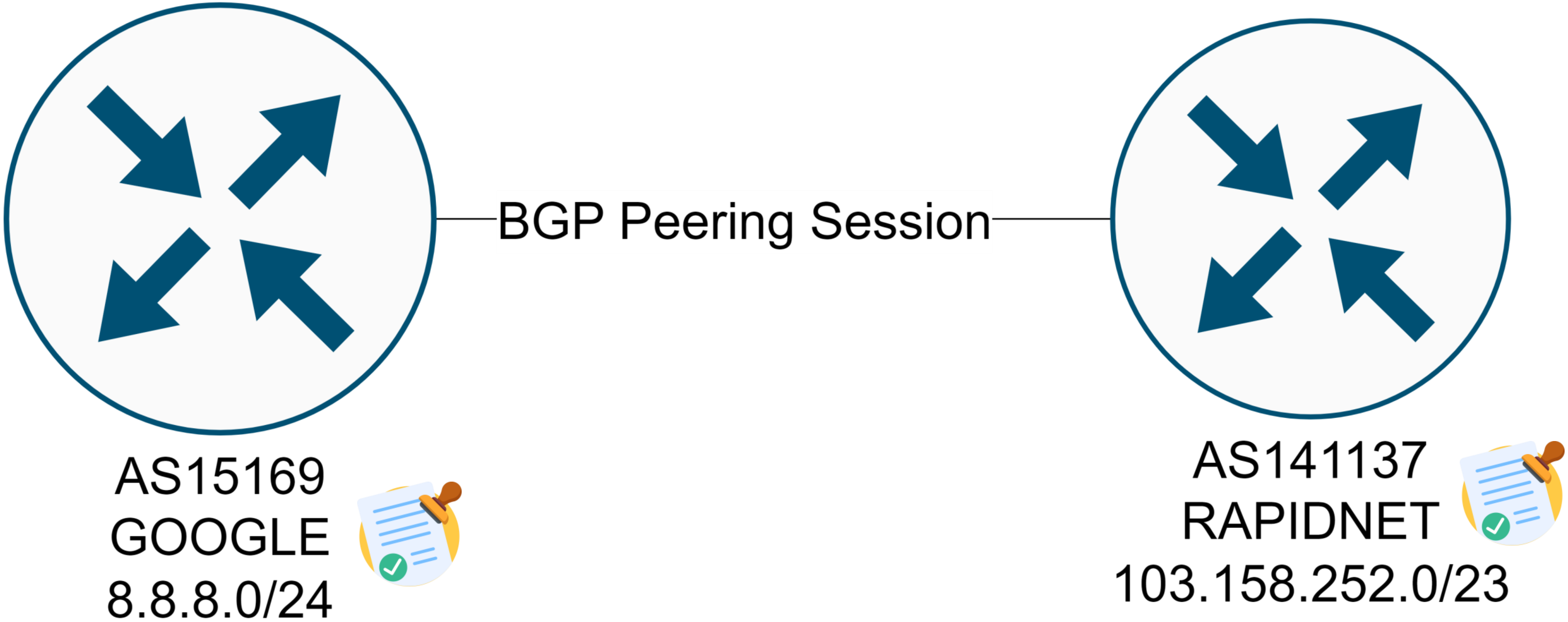
The Architecture



Credit to: APNIC

VRP = Validated Payload

BGP Advertisement with RPKI



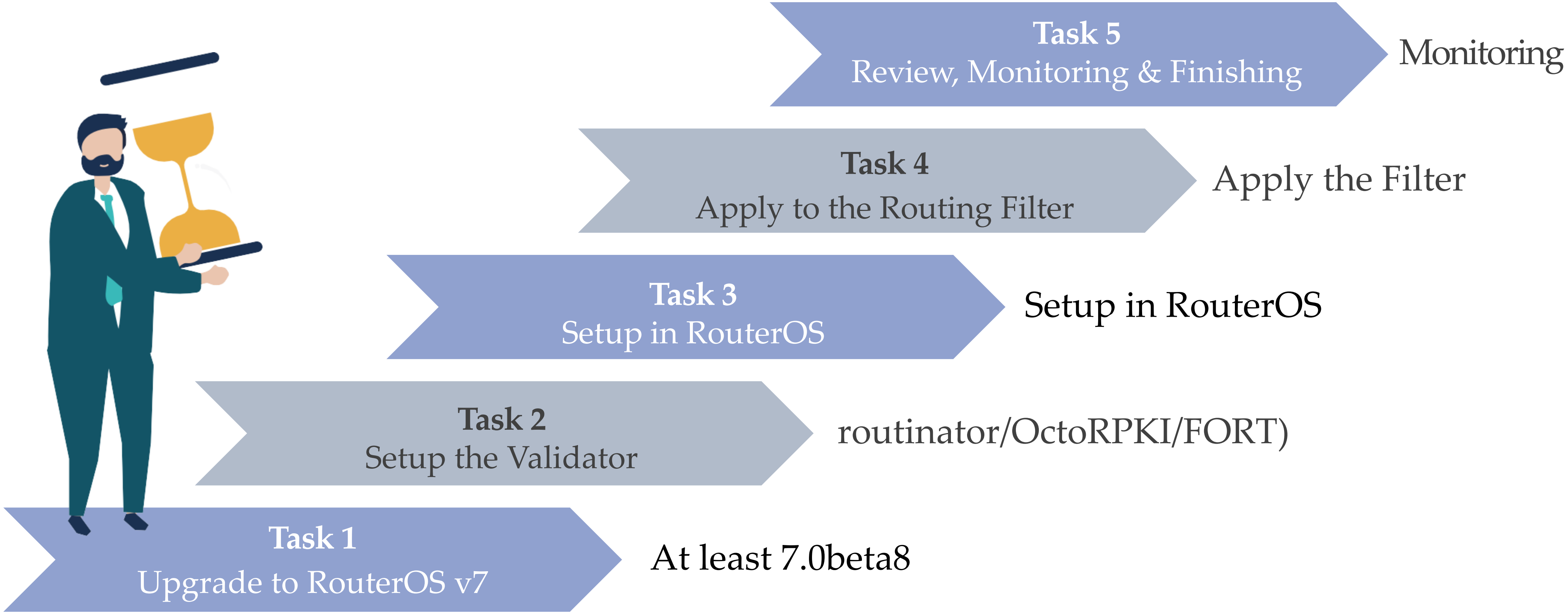
BGP Peering Session

AS15169
GOOGLE
8.8.8.0/24

AS141137
RAPIDNET
103.158.252.0/23

The Prefix will be validated through the validator server and the TAL (Trust Anchor Locator)

Step by Step to Integrate with RouterOS



Task 1
Upgrade to RouterOS v7

At least 7.0beta8

Task 2
Setup the Validator

routinator/OctoRPKI/FORT)

Task 3
Setup in RouterOS

Setup in RouterOS

Task 4
Apply to the Routing Filter

Apply the Filter

Task 5
Review, Monitoring & Finishing

Monitoring

RPKI Release Note

RouterOS version 7.0beta8 has been released in public "development" channel!

What's new in 7.0beta8 (2020-Jun-4 15:04):

*) fixed CLI dependencies for routing menu;

What's new in 7.0beta7 (2020-Jun-3 16:31):

!) added Layer3 hardware offloading support for CRS317-1G-16S+RM more info here: https://wiki.mikrotik.com/wiki/Manual:C ... Offloading
!) enabled BGP support with multicore peer processing (CLI only);
!) enabled RPKI support (CLI only);
!) ported features and fixes introduced in v6.47;
!) routing updates, complete status report: https://help.mikrotik.com/docs/display/ ... col+Status
!) system kernel has been updated to version 5.6.3;
*) other minor fixes and improvements;

Setup the Validator

OctoRPKI

FORT
Routing Technology for a Free and Open Internet
Powered by NIC MÉXICO and lacnic

Can be installed in your Linux/UNIX server or any supported platform (need to check one by one)

Setup the Validator – Routinator (example)

We can easily deploy the routinator using docker container (Linux Based)

```
sudo docker run -d --restart=unless-stopped --name routinator \
    -p 3323:3323 \
    -p 8323:8323 \
    nlnetlabs/routinator
```

Or you can also deploy the routinator directly to your system :)

More info, https://routinator.docs.nlnetlabs.nl/en/stable/installation.html

Setup in RouterOS

```
/routing/rpki add
address=$YOUR_VALIDATOR_SERVER_IP_ADDR
disabled=no group=myRPKI port=3323
```

Setup in RouterOS

```
/routing/rpki rpki-check origin-as=141137
prefix=103.158.252.0/23 group=myRPKI
 valid
```

```
/routing/rpki rpki-check origin-as=141138
prefix=103.158.252.0/23 group=myRPKI
 invalid
```

Setup in RouterOS

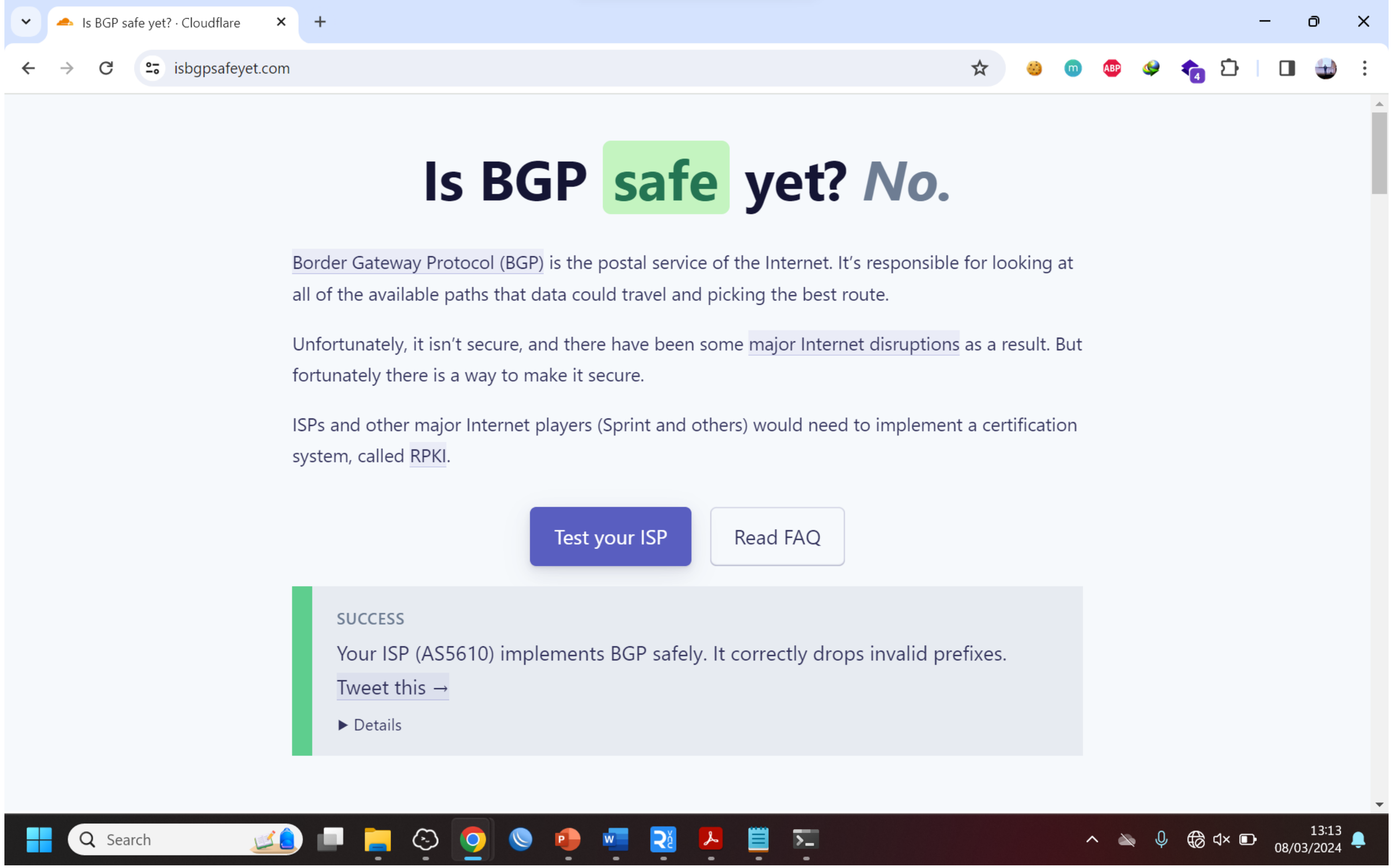
- **valid** - database has a record and origin AS is valid.
- **invalid** - the database has a record and origin AS is invalid.
- **unknown** - database does not have information of prefix and origin AS.
- **unverified** - set when none of the RPKI sessions of the RPKI group has synced database. This value can be used to handle the total failure of the RPKI.

Apply the Routing Filter

```
/routing/filter/rule
add chain=bgp_in rule="rpki-verify myRPKI"
add chain=bgp_in rule="if (rpki invalid) { reject } else { accept }“
```

In this case, I will totally reject the prefix, but you can also choose to reject or decrease the BGP local preference, or do anything else that you want.

Test & Monitoring – isbgpsafeyet.com



Is BGP safe yet? *No.*

Border Gateway Protocol (BGP) is the postal service of the Internet. It's responsible for looking at all of the available paths that data could travel and picking the best route.

Unfortunately, it isn't secure, and there have been some major Internet disruptions as a result. But fortunately there is a way to make it secure.

ISPs and other major Internet players (Sprint and others) would need to implement a certification system, called RPKI.

SUCCESS

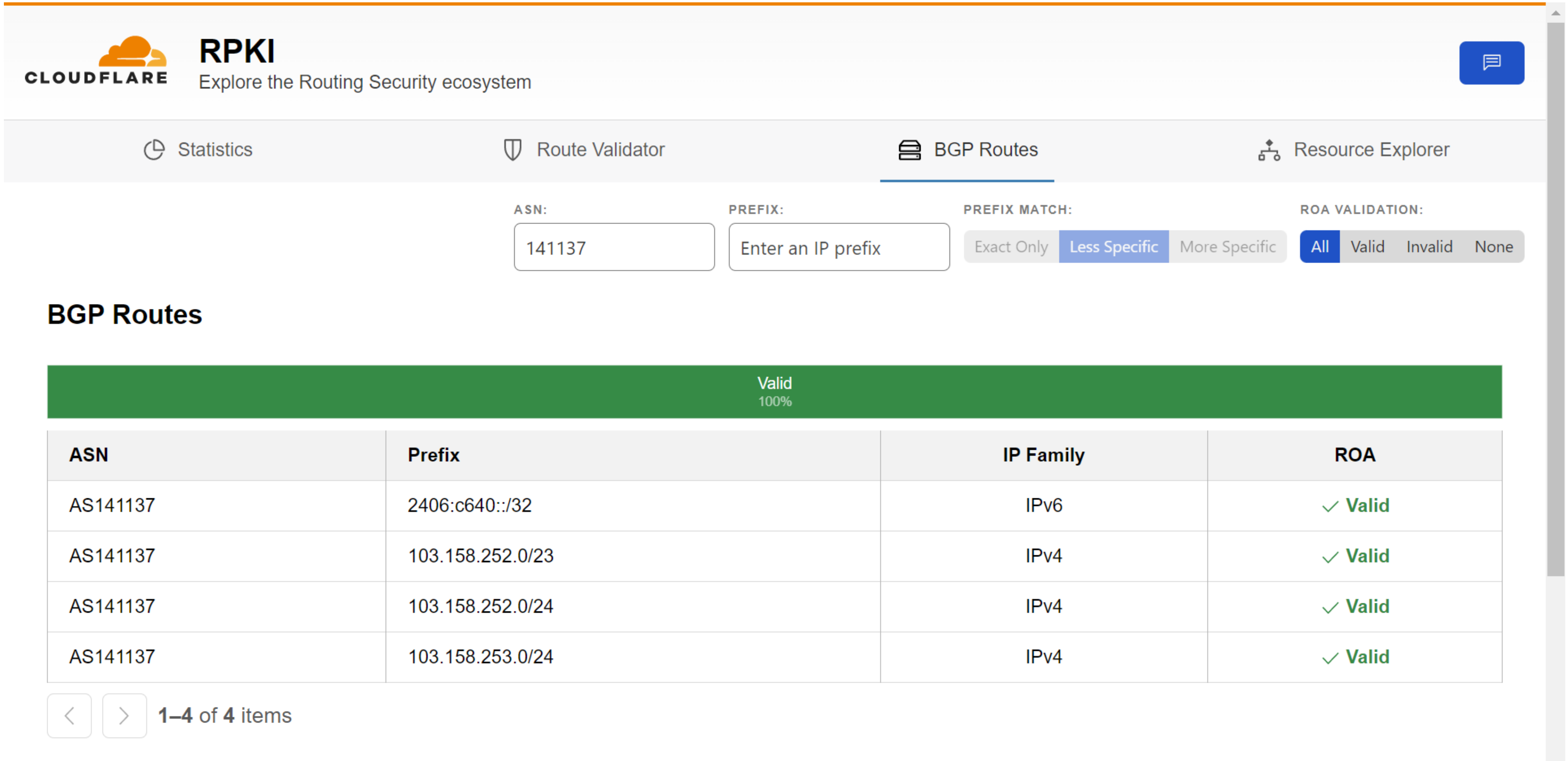
Your ISP (AS5610) implements BGP safely. It correctly drops invalid prefixes.

Tweet this →

▶ Details

And also, do not forget to create the RPKI ROA for your own prefix to avoid BGP hijacking within your own network :)

RPKI Check



RPKI

Explore the Routing Security ecosystem

ASN: 141137

PREFIX: Enter an IP prefix

PREFIX MATCH: Exact Only | Less Specific | More Specific

ROA VALIDATION: All | Valid | Invalid | None

BGP Routes

Valid
100%

ASN	Prefix	IP Family	ROA
AS141137	2406:c640::/32	IPv6	✓ Valid
AS141137	103.158.252.0/23	IPv4	✓ Valid
AS141137	103.158.252.0/24	IPv4	✓ Valid
AS141137	103.158.253.0/24	IPv4	✓ Valid

1–4 of 4 items

https://rpki.cloudflare.com/?view=validator

Thanks! :)