

RPKI validator na straży BGP

Ihor Hreskiv



Jestem miłośnikiem urządzeń MikroTik od kilku lat

Potrafię wyjść z VIM :)

eve-ng fan

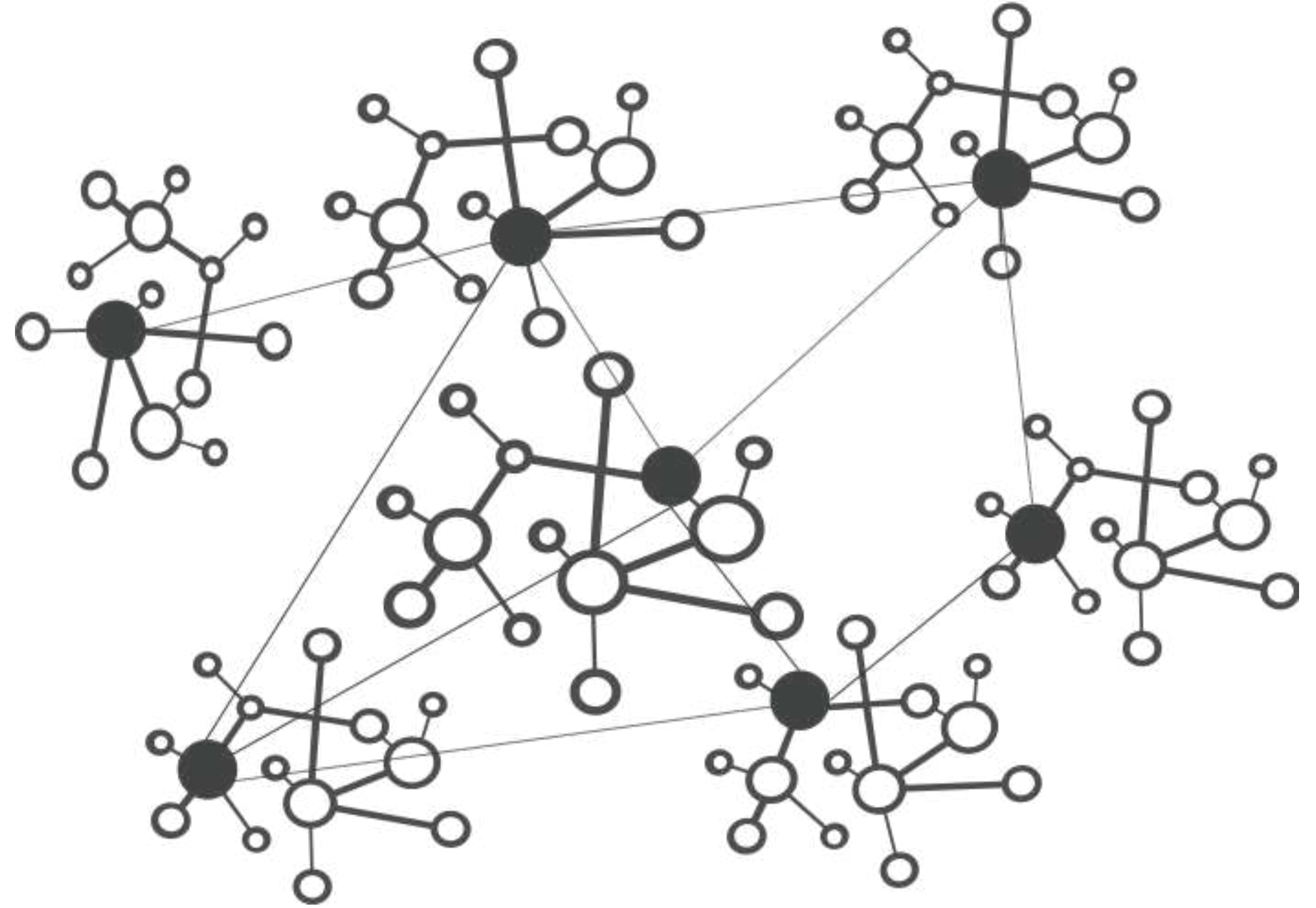
Najczęściej używam CHR

MTC(all)E

BGP w skrócie

BGP (ang. *Border Gateway Protocol*) — zewnętrzny protokół routingu. BGP jest podstawą działania współczesnego Internetu.

The Internet
Sieć która składa się z sieci



BGP a bezpieczeństwo

BGP hijacking (*przejęcie/porwanie protokołu BGP*), czasami określane jako *przejęcie prefiksu, przejęcie trasy* — to nielegalne przejęcie grup adresów IP poprzez uszkodzenie tablic routingu, utrzymywanych przy użyciu protokołu Border Gateway Protocol (BGP).

BGP hijacking

BGP hijacking może nastąpić celowo lub przypadkowo na jeden z kilku sposobów:

- ▶ AS ogłasza, że jest *origin* dla prefiksu, dla którego w rzeczywistości nie jest.
- ▶ AS ogłasza bardziej szczegółowy prefix niż taki, który może ogłosić prawdziwy źródłowy AS.
- ▶ AS ogłasza, że może skierować ruch do porwanego AS krótszą trasą niż jest już dostępna, niezależnie od tego, czy trasa faktycznie istnieje.

BGP hijacking

Niektóry ze znanych atak BGP hijacking:

1. Luty 2008 - Pakistan telekom AS17557 - nieautoryzowane ogłoszenie prefiksu 208.65.153.0/24 który jest częścią 208.65.152.0/22 należący do YouTube. <https://cnet.co/41sp06G>
2. Kwiecień 2020 - Rostelekom AS12389 - ogłoszenie się *origin* dla około 50 prefiksów <https://bit.ly/3N2dfj4>



Resource Public Key Infrastructure

RPKI (*Resource Public Key Infrastructure*) — system używany do sprawdzania poprawności i zabezpieczania informacji o routingu w Internecie.

Jest to hierarchiczny system certyfikatów cyfrowych, który weryfikuje własność bloków adresów IP (prefiksów) oraz numerów systemów autonomicznych (ASN).



IETF RFC pokrewny z RPKI

<https://tools.ietf.org/html/rfc6480>

An Infrastructure to Support Secure Internet Routing

<https://tools.ietf.org/html/rfc6482>

A Profile for Route Origin Authorizations (ROAs)

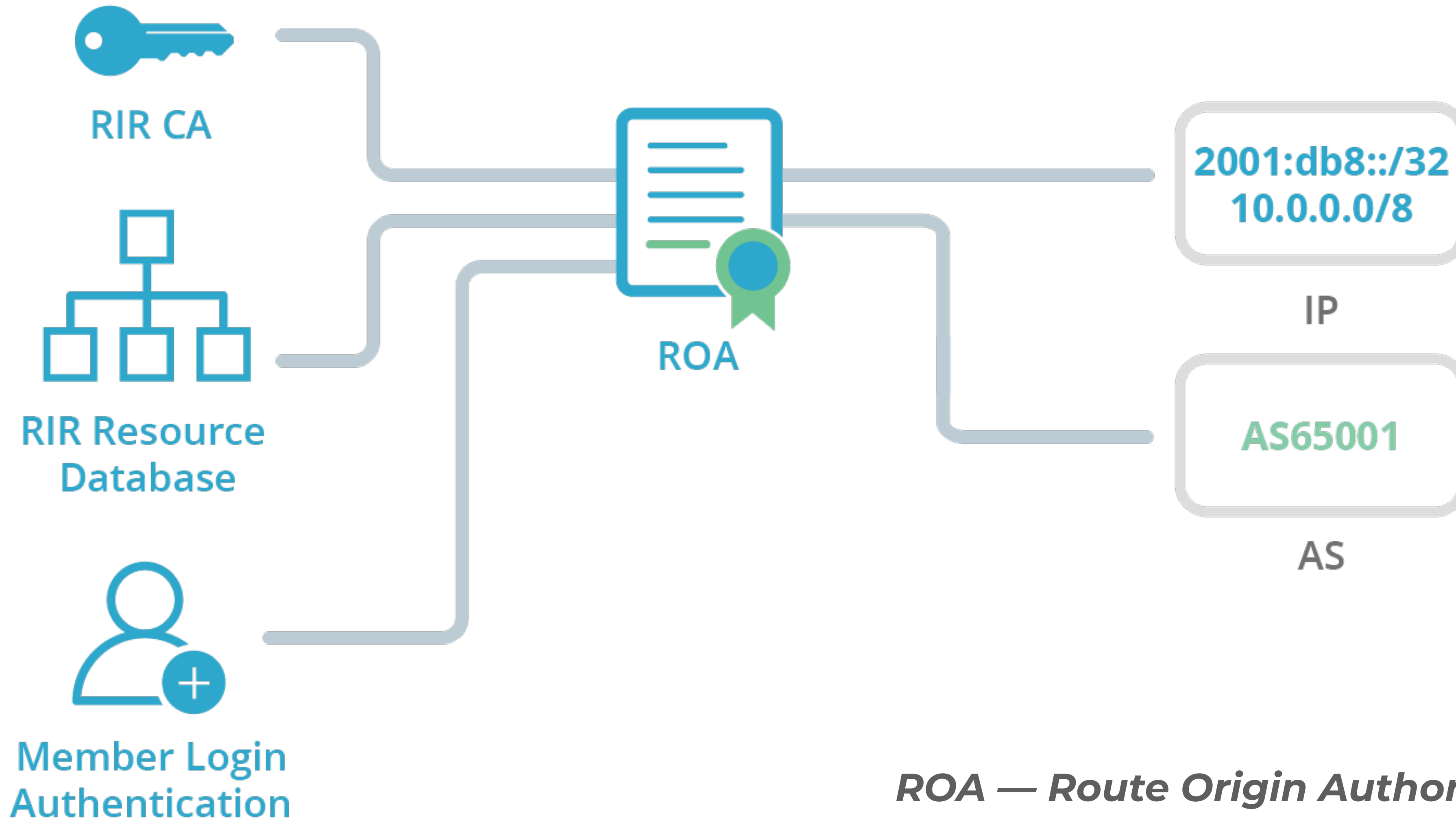
<https://tools.ietf.org/html/rfc6483>

Validation of Route Origin using PKI and ROAs

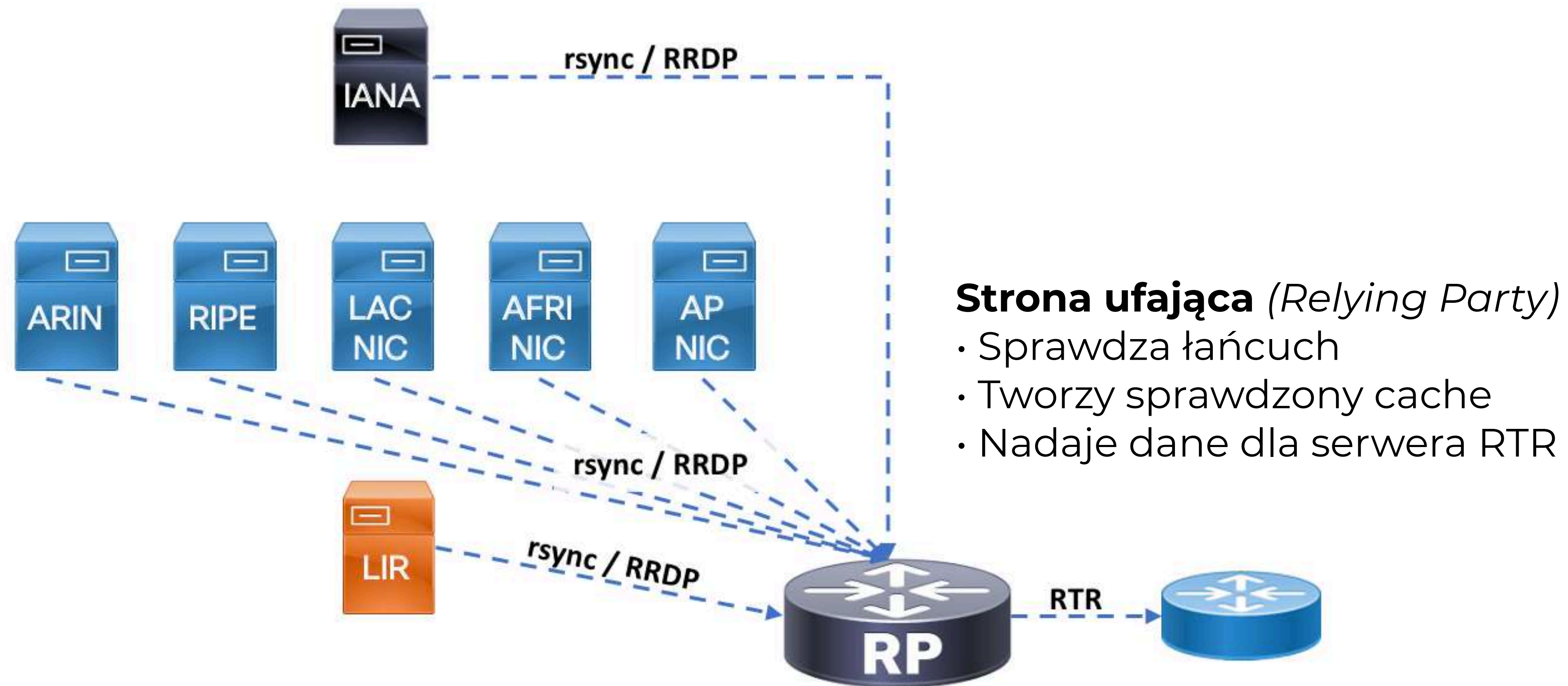
<https://tools.ietf.org/html/rfc6810>

The RPKI to Router Protocol (RTR)

Resource Public Key Infrastructure



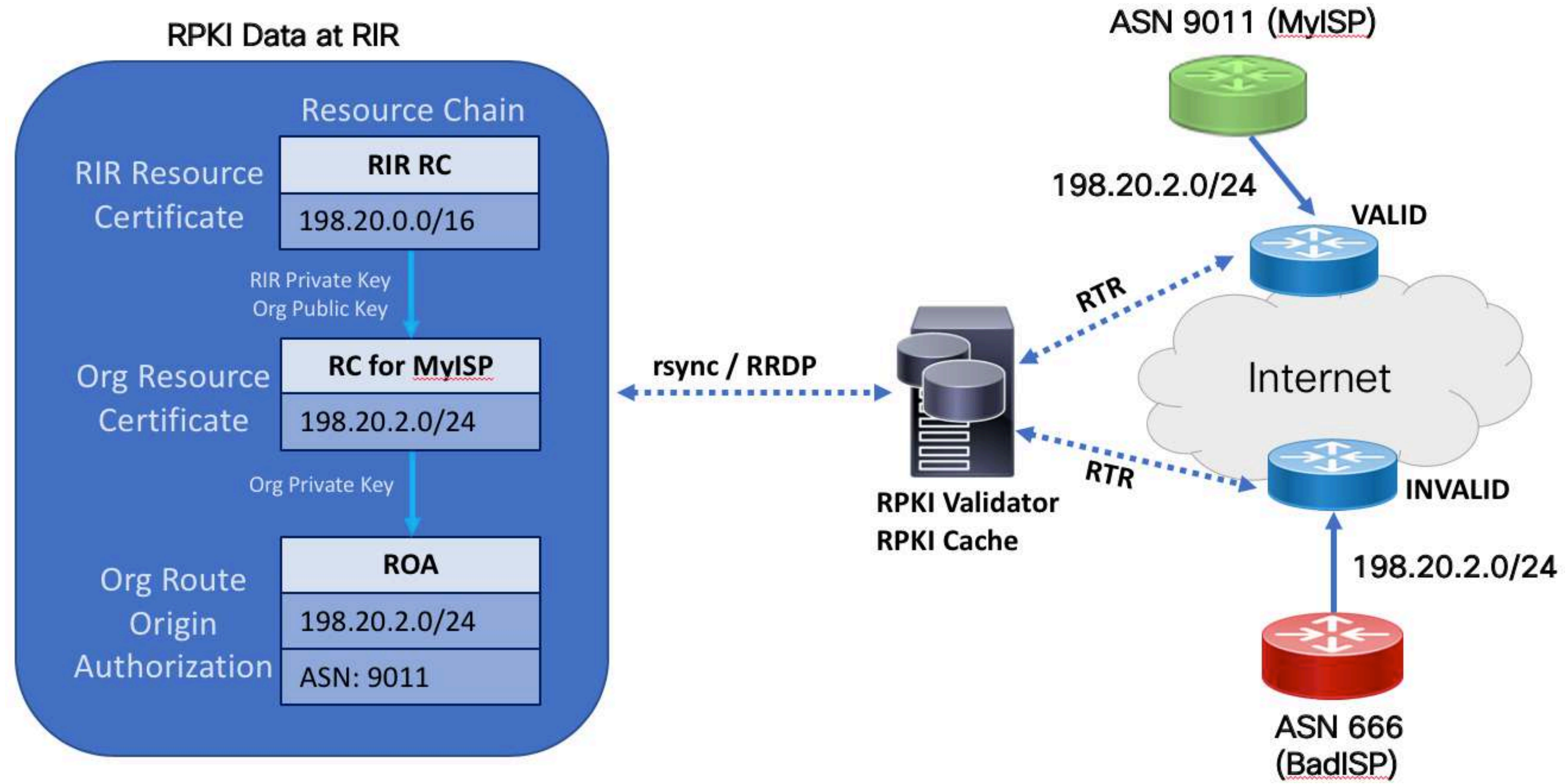
RPKI proces walidacji



RTR — RPKI-to-Router (RTR) protocol

RRDP — RPKI Repository Delta Protocol (RRDP)

RPKI proces walidacji



Resource Public Key Infrastructure

RouterOS w nowej wersji ROS7 ma zaimplementowane wsparcie dla RPKI do protokołu BGP, zdefiniowanego w *RFC8210*.

RTR to bardzo lekki protokół o niskim zużyciu pamięci, aby niezawodnie uzyskiwać dane walidacji prefiksów z walidatorów RPKI.

ROUTINATOR

Czym jest Routinator?



Routinator — narzędzie open-source służące do weryfikacji i pobierania informacji z infrastruktury RPKI.

Routinator może być używany do pobierania i przechowywania certyfikatów RPKI, weryfikacji prawidłowości podpisów cyfrowych i uwierzytelniania właścicieli adresów IP i numerów ASN w protokole BGP.

<https://github.com/NLnetLabs/routinator>

Instalacja i konfiguracja Routinator

Obrazy Docker zbudowane w oparciu o Alpine Linux i dostępne dla architektur:

- amd64
- arm/v6
- arm/v7
- arm64

Minimalne wymagania dla Routinator: RAM — 1 GB, HDD — 4GB.

Instalacja i konfiguracja Routinator

Uruchomienie kontenera (może się różnić od systemu operacyjnego):

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

Porty używane kontenerem:

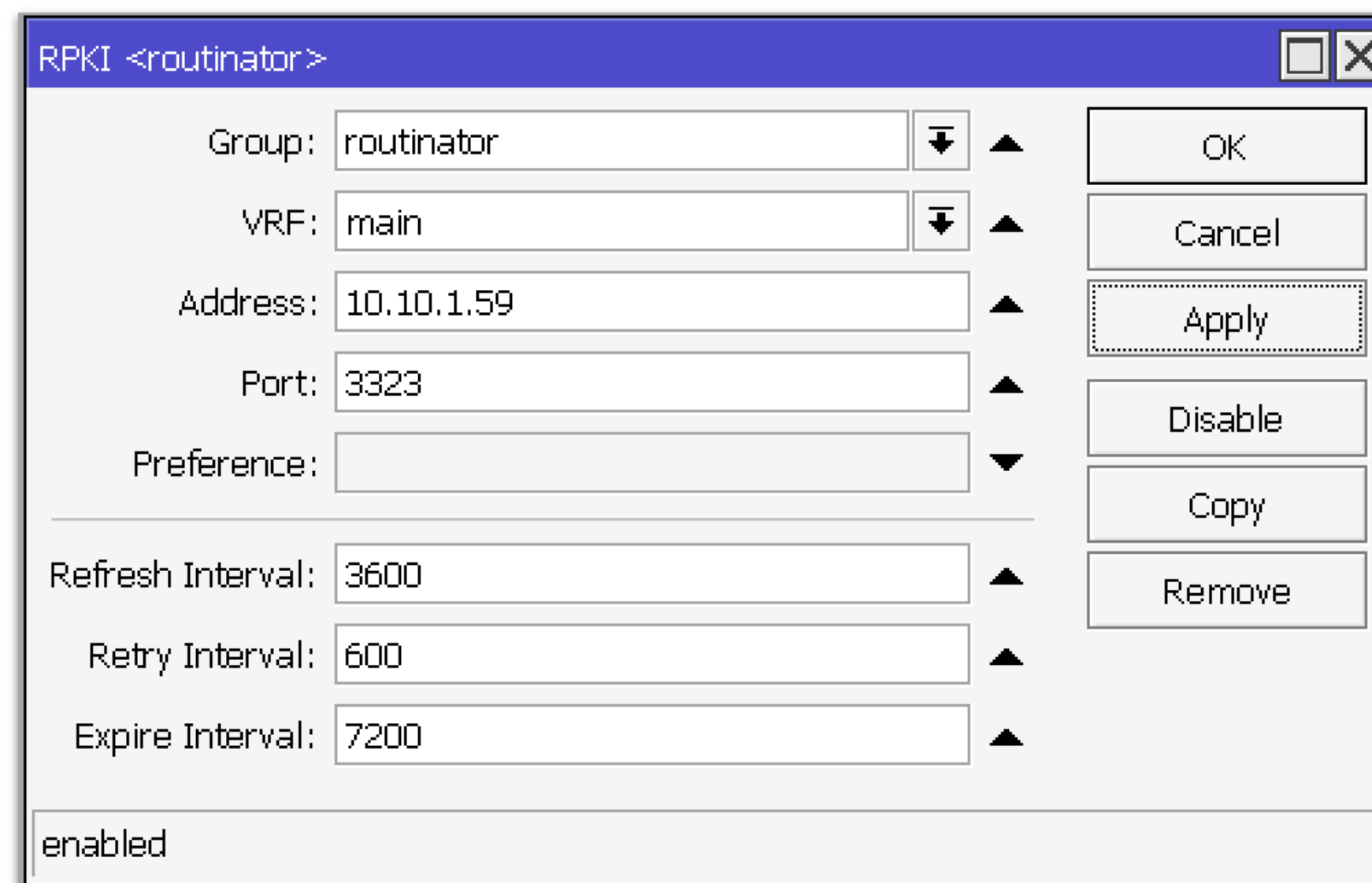
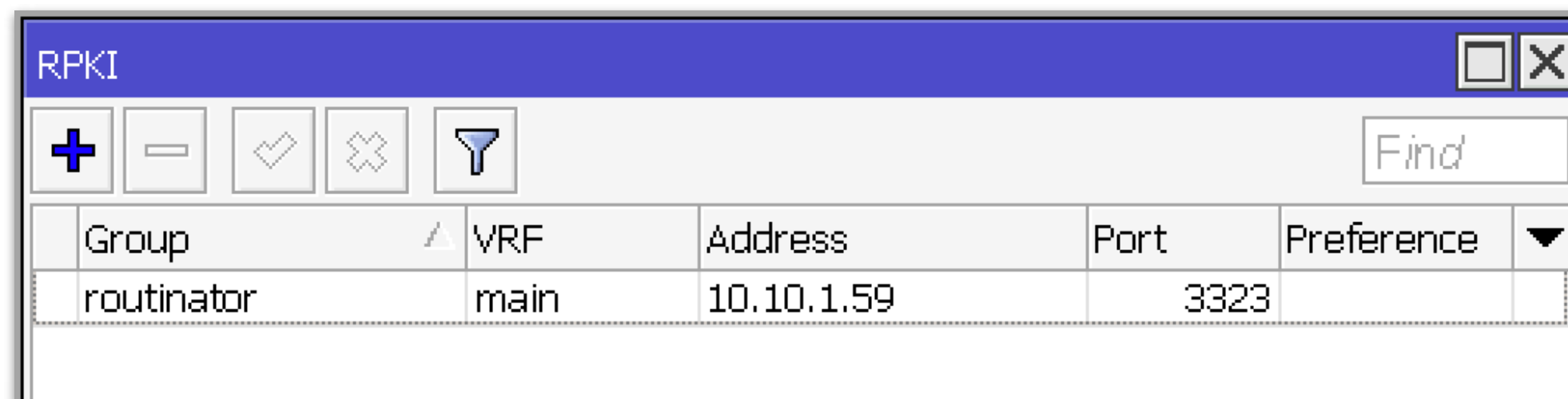
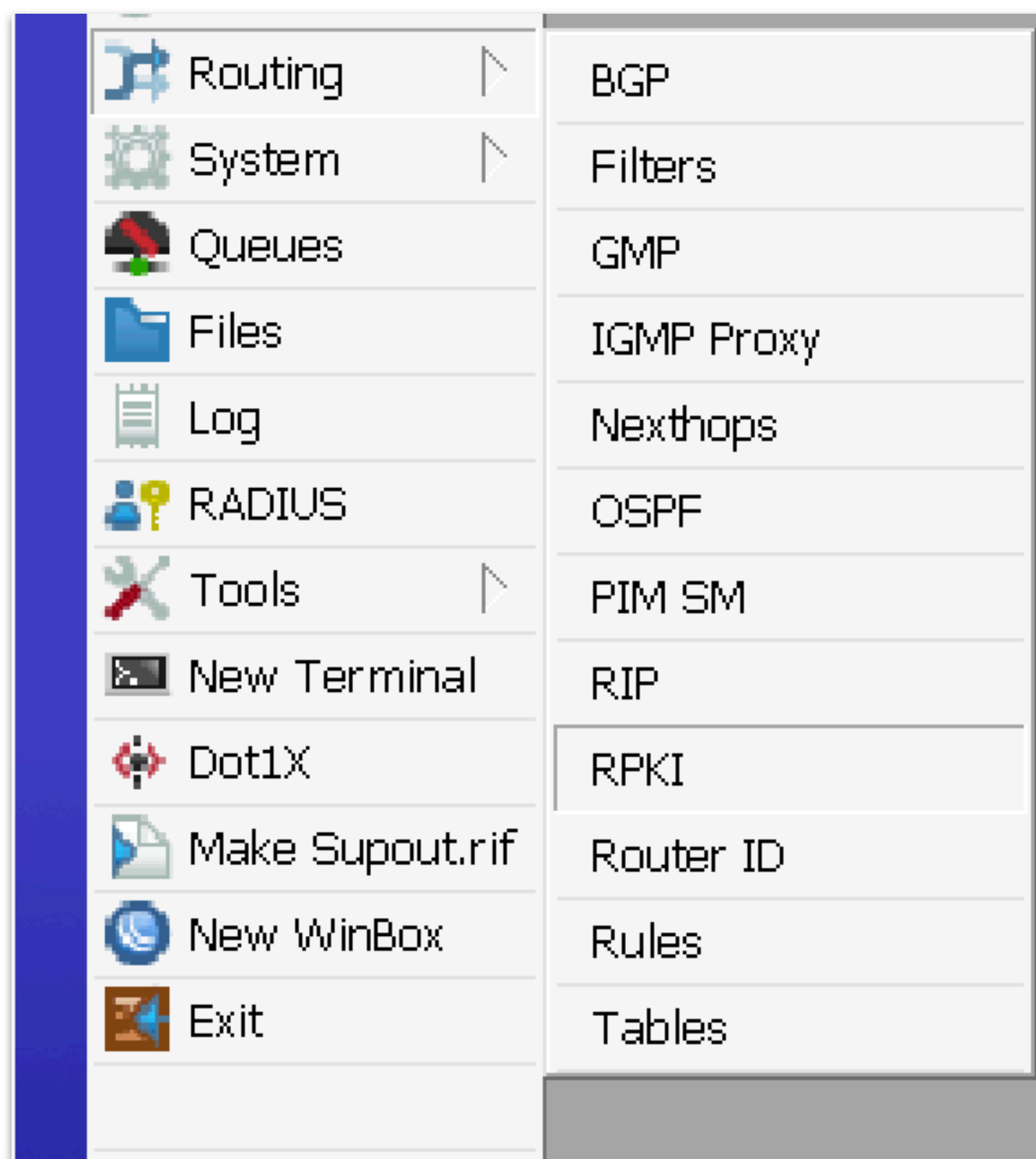
tcp/3323 — rtr

tcp/8323 — http

tcp/9556 — prometheus exporter

<https://routinator.docs.nlnetlabs.nl/en/stable/installation.html#binary-packages>

Routinator I ROS7



```
/routing rпки  
add address=10.10.1.59 disabled=no group=routinator port=3323
```

<https://help.mikrotik.com/docs/display/ROS/RPKI>

Routinator I ROS7

Dla sprawdzania prefiksów należy dodać reguły do filtra w routing-u.

```
/routing filter rule
add chain=vultr-bgp-in disabled=no rule="rpki-verify routinator"
add chain=vultr-bgp-in disabled=no rule="if (dst in 0.0.0.0/0 && gw == \
    169.254.169.254 && rpki valid) {set comment valid-routes; accept;}"
```

169.254.169.254 adres bramy od operatora, który należy zamienić na swój

Routinator I ROS7

Wynik działania

	Dst. Address	Gateway	Distance	Contribution	Comment
DIFb	1.4.221.0/24	169.254.169.254	20	filtered	
DIFb	1.4.222.0/24	169.254.169.254	20	filtered	
DIFb	1.4.223.0/24	169.254.169.254	20	filtered	
DIFb	1.4.224.0/20	169.254.169.254	20	filtered	
DIFb	1.4.240.0/21	169.254.169.254	20	filtered	
DIFb	1.4.248.0/23	169.254.169.254	20	filtered	
DIFb	1.4.252.0/22	169.254.169.254	20	filtered	
DIFb	1.5.0.0/16	169.254.169.254	20	filtered	
DAb	1.6.0.0/22	169.254.169.254	20	active	valid-routes
DAb	1.6.1.0/24	169.254.169.254	20	active	valid-routes
DAb	1.6.4.0/22	169.254.169.254	20	active	valid-routes
DAb	1.6.6.0/24	169.254.169.254	20	active	valid-routes
DAb	1.6.7.0/24	169.254.169.254	20	active	valid-routes
DAb	1.6.8.0/22	169.254.169.254	20	active	valid-routes
DAb	1.6.11.0/24	169.254.169.254	20	active	valid-routes
DAb	1.6.12.0/22	169.254.169.254	20	active	valid-routes
DAb	1.6.16.0/22	169.254.169.254	20	active	valid-routes
DAb	1.6.20.0/22	169.254.169.254	20	active	valid-routes

10215 items (1 selected)

Routinator

Sprawdzanie prefiksów za pomocą strony WWW

The screenshot shows the Routinator website interface. The browser's address bar displays the URL 10.10.1.59. The website's navigation bar includes the Routinator logo and menu items: Prefix Check, Metrics, Repositories, and Connections. The main content area is titled "Prefix Check" and contains two input fields: "Prefix or IP Address" with the placeholder text "e.g. 192.0.2.0/24" and "Origin ASN (optional)" with the placeholder text "e.g. 64511". Below these fields is a note: "will be validated with BGP ASN". A "Validate" button is present, along with a "hide options" link. A greyed-out section contains several settings: "ASN Lookup" with a help icon, a toggle switch for "Validate Prefixes for ASN found in BGP" which is currently turned on, "Origin ASN Validation Source" with a help icon, a toggle switch for "Longest Matching Prefix" which is currently turned off, and "Exact Match only". At the bottom of this section is "Data Freshness" with a help icon.

Routinator

Sprawdzanie prefiksów za pomocą ROS CLI

```
Terminal <3>

MMM      MMM      KKK      TTTTTTTTTTT      KKK
MMMM     MMMM     KKK      TTTTTTTTTTT      KKK
MMM MMMM MMM III  KKK  KKK  RRRRRR      OOOOOO      TTT      III  KKK  KKK
MMM  MM  MMM  III  KKKKK  RRR  RRR  OOO  OOO      TTT      III  KKKKK
MMM      MMM  III  KKK  KKK  RRRRRR      OOO  OOO      TTT      III  KKK  KKK
MMM      MMM  III  KKK  KKK  RRR  RRR      OOOOOO      TTT      III  KKK  KKK

MikroTik RouterOS 7.8 (c) 1999-2023      https://www.mikrotik.com/

Press F1 for help

[ihor@vpn.mtik.pl] > routing/rpki/rpki-check group=routinator prefix=1.5.0.0/16 origin-as=4725
unknown

[ihor@vpn.mtik.pl] > routing/rpki/rpki-check group=routinator prefix=1.6.0.0/22 origin-as=9583
valid

[ihor@vpn.mtik.pl] > █
```

Przyszłość rozwoju

Obecnie jest opublikowany *draft* protokołu RTR

<https://datatracker.ietf.org/doc/html/draft-ymbk-8210bis-00>

Także dla sprawdzanie *AS_PATH* parametru za pomocą protokołu ASPA, *draft* jest opublikowany

<https://datatracker.ietf.org/doc/html/draft-ietf-sidrps-aspa-verification-05>

Dziękuję

e-mail: ihor@hreskiv.pl