Route Origin Validation - A MANRS Approach

Md. Zobair Khan

MANRS Ambassador

Acknowledgement

- This paper is made taking notes, diagram, configurations from MANRS, APNIC training materials & blog, NLnet Labs, Github & Dr. Philip Smith along with the operational experience of the author.

MANRS

- Mutually Agreed Norms for Routing Security (MANRS) is a global initiative, supported by the Internet Society, that provides crucial fixes to reduce the most common routing threats.

MANRS

MANRS

- MANRS outlines four simple but concrete actions that network operators should take:

  - Filtering
  - Anti-spoofing
  - Coordination
  - Global Validation

Global Validation

- Publish your data, so others can validate routing information on a global scale

- Automated information validation needs arrangements

- Securing global routing information is done by RPKI

Resource Public Key Infrastructure (RPKI)

SANOG

- RPKI allows holders of Internet number resources to make verifiable statements about how they intend to use their resources.

- RPKI is a way to define data in an out-of-band system such that the information that are exchanged by BGP can be validated to be correct.

- RPKI is used to make Internet routing more secure.

MANRS

RPKI

Fiber @ Home

Importance of RPKI

- Secured Routing Table

- Dynamic LOA checking

- Maintaining a Dynamic Chain of Trust

- Digitally Signed Resources Certificate (X.509 Certificates-RFC5280)

- Helps to Stop Route Hijack

Route Origin Authorizations (ROA)

- Using the RPKI system, the legitimate holder of a block of IP addresses can use their resource certificate to make an authoritative, signed statement about which autonomous system is authorized to originate their prefix in BGP.

- These statements are called Route Origin Authorizations (ROAs).

Route Origin Validation (ROV)

- RPKI system tries to closely mimic what route objects in the IRR intend to do, but then in a more trustworthy manner.

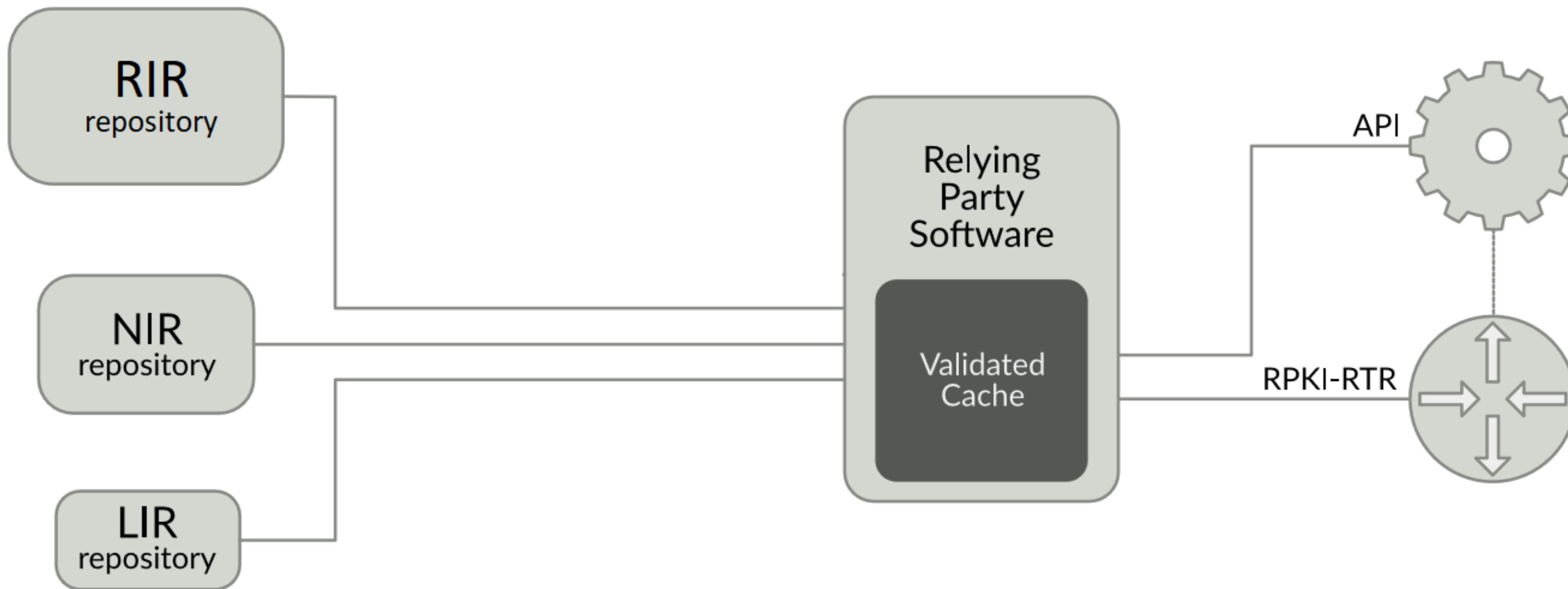- This process is called route origin validation (ROV)

Validity

- Valid - Resources found in database which is called Validated ROA Payload (VRP).

- Invalid – Resources found but partial/whole information doesn't match with database.

- Not Found - The prefix in this announcement is not covered by a VRP.

RPKI - Chain Of Trust
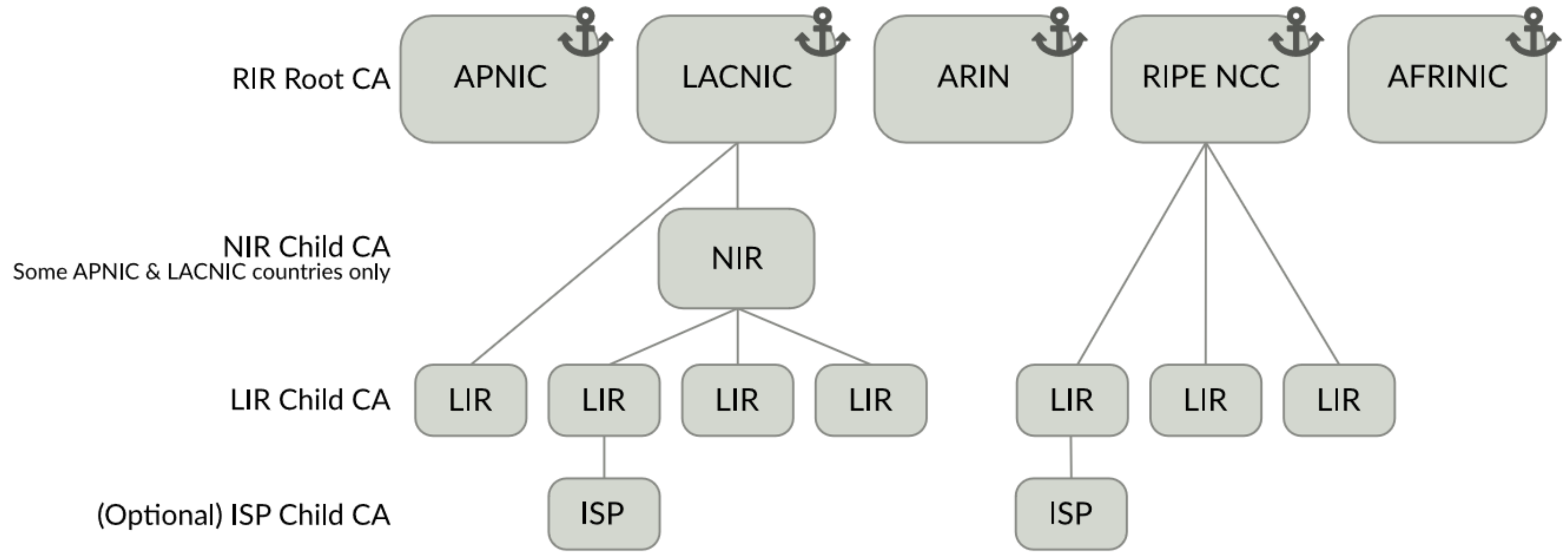
Ecosystem

Working Steps

- Creating ROA for owned resources for RPKI

- Implementing Validator relying software for ROV

- Enforcing policies for based on Validation

Creating ROA

- Go to Resources > Route Management and select Create route

https://www.apnic.net/wp-content/uploads/2017/12/ROUTE_MANAGEMENT_GUIDE.pdf

Creating ROA

- Mention your prefix with ASN & desired subnet & Submit

Relying Party Software

❑ NLnet Labs Routinator

    https://github.com/NLnetLabs/routinator

❑ LACNIC/NIC Mexico validator (FORT)

    https://github.com/NICMx/FORT-validator

❑ Cloudflare validator (OctoRPKI)

    https://github.com/cloudflare/cfrpki

❑ RPKI-Client

    https://github.com/kristapsdz/rpki-client

MANRS   RPKI   Fiber@Home

Routinator

- Routinator is free, open source RPKI Relying Party software written by NLnet Labs in the Rust programming language.

- Routinator connects to the Trust Anchors of the five Regional Internet Registries (RIRs) — APNIC, AFRINIC, ARIN, LACNIC and RIPE NCC — downloads all of the certificates and ROAs in the various repositories, verifies the signatures and makes the result available for use in the BGP workflow.

- The validated cache can be fed directly into RPKI-capable routers via the RPKI to Router Protocol (RPKI-RTR), described in RFC 8210.

https://rpki.readthedocs.io/en/latest/routinator/index.html

MANRS

RPKI

Fiber@Home

Installation (Routinator)

Step by step installation process is given in Appendix-1 at the end of this slide.

OctoRPKI

- Developed and used by Cloudflare

- This application periodically refreshes the data provided by the RIRs and the delegated organizations.

- No development after December 2020.

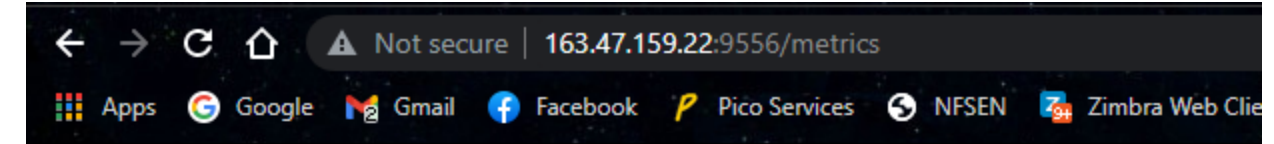- RTR session is handeled by GoRTR – a separate module.

MANRS

RPKI

Fiber @ Home

Installation (OctoRPKI)

Step by step installation process is given in Appendix-1 at the end of this slide.

```
root@routinator-2:~#
root@routinator-2:~# ps ax | grep gortr
   6483 pts/0    Sl     0:06 gortr -bind=163.47.159.22:8282 -metrics.addr=:8080 -verify=false -cache=http://163.47.159.22:8081/output.json
   6584 pts/0    R+     0:00 grep --color=auto gortr
root@routinator-2:~# ps ax | grep octo
   5690 pts/0    Sl     6:02 octorpki -output.sign=false
   6588 pts/0    S+     0:00 grep --color=auto octo
root@routinator-2:~#
```

```
RP/0/RSP1/CPU0:C-AGG-1#sh bgp rpki server summary
Mon Jun  7 16:20:55.602 BST

Hostname/Address          Transport        State        Time            ROAs (IPv4/IPv6)
163.47.159.22             TCP:8282         ESTAB        00:02:07        214077/39923

RP/0/RSP1/CPU0:C-AGG-1#
```

FORT Validator

- FORT validator is an MIT-licensed RPKI Relying Party, this is a tool offered as part of the FORT project.

- FORT is a joint initiative by LACNIC, the Regional Internet Registry for Latin America and the Caribbean, and NIC.MX.

- RTR Configuration is done with json file.

MANRS

Fiber @ Home

Installation (FORT)

Start fort as a service.

Check the status. It will take some time to build the first validated cache.

```
nano@routinator-2:~$
nano@routinator-2:~$ sudo service fort start
nano@routinator-2:~$ sudo service fort status
● fort.service - FORT RPKI validator
     Loaded: loaded (/lib/systemd/system/fort.service; enabled; vendor preset: enabled)
     Active: active (running) since Mon 2021-06-07 14:01:12 UTC; 6min ago
       Docs: man:fort(8)
             https://nicmx.github.io/FORT-validator/
   Main PID: 20079 (fort)
      Tasks: 36 (limit: 9220)
     Memory: 777.5M
     CGroup: /system.slice/fort.service
             └─20079 /usr/bin/fort --configuration-file /etc/fort/config.json

Jun 07 14:01:12 routinator-2 systemd[1]: Started FORT RPKI validator.
Jun 07 14:01:12 routinator-2 fort[20079]: WRN: First validation cycle has begun, wait until the next notification to co>
Jun 07 14:05:48 routinator-2 fort[20079]: WRN: Location '/etc/fort/slurm/' doesn't have files with extension '.slurm'
Jun 07 14:05:48 routinator-2 fort[20079]: WRN: First validation cycle successfully ended, now you can connect your rout>
lines 1-15/15 (END)
```

```
nano@routinator-2:~$
nano@routinator-2:~$ ps ax | grep fort
  20079 ?        Ssl    3:06 /usr/bin/fort --configuration-file /etc/fort/config.json
  20615 pts/1    S+     0:00 grep --color=auto fort
```

```
RP/0/RSP1/CPU0:C-AGG-1#sh bgp rpki server summary
Mon Jun  7 19:56:26.720 BST

Hostname/Address          Transport        State          Time          ROAs (IPv4/IPv6)
163.47.159.22             TCP:8282         ESTAB          00:33:25      214113/39952
```

Step by step installation process is given in Appendix-1 at the end of this slide.

RPKI-Client

- rpki-client is a FREE, easy-to-use implementation of the Resource Public Key Infrastructure (RPKI)

- The program queries the RPKI repository system and outputs Validated ROA Payloads in the configuration format of either OpenBGPD or BIRD, but also as CSV or JSON objects for consumption by other routing stacks.

- rpki-client was primarily developed as part of the OpenBSD Project and gets released as a base component of OpenBSD every six months.

Installation (RPKI-Client)

If everything goes smoothly, you will be able to see the ROA summury.
bgpctl show sets

You can apply RPKI information to reject invalids on import and export
deny quick from ebgp ovs invalid
deny quick to ebgp ovs invalid

```
root@bsd-rpki:~ # bgpctl show sets
Type    Name                          #IPv4    #IPv6 #ASnum Last Change
ROA     RPKI ROA                      199426   38216    -      01:06:22
PREFIX mynetworks                          1        1    -      01:06:23
PREFIX bogons                             14       11    -      01:06:23
root@bsd-rpki:~ # 
```

Step by step installation process is given in Appendix-1 at the end of this slide.

MANRS   RPKI   Fiber@Home

Hardware OS

Juniper - Junos version 12.2 and newer.

Cisco - IOS release 15.2 and newer, as well as Cisco IOS/XR since release 4.3.2.

Nokia - SR OS 12.0.R4 and newer, running on the 7210 SAS, 7250 IXR, 7750 SR, 7950 XRS and the VSR.

Arista - EOS 4.24.0F and newer

MikroTik - 7.0beta7 and newer

Huawei - VRP 8.150 and newer.

Router Configuration

router bgp [ASN]

  rpki server [SERVER IP]

    transport tcp port 3323

    refresh-time 120

address-family ipv4 unicast

  bgp origin-as validation signal ibgp

address-family ipv6 unicast

  bgp origin-as validation signal ibgp

Configuration of IOS-XR

Decision

- Since now the validation states are visible to you, you can decide what to do with invalids

- You can –
  - Use them with low preference
  - Or drop them

Policy

route-policy RPKI
  if validation-state is invalid then
    set local-preference 50
  else
    if validation-state is valid then
      set local-preference 200
    else
      pass
    endif
  endif
end-policy

route-policy RPKI
  if validation-state is invalid then
    drop
  else
    if validation-state is valid then
      set local-preference 200
    else
      pass
    endif
  endif
end-policy

Configuration of IOS-XR

MANRS

RPKI

Fiber @ Home

FAH Deployment

- Fiber@Home is one of the largest Internet Gateway in Bangladesh.
- We have implemented Routinator as our validator software.
- We are still in observation period and not dropping the invalids yet.
- Communicating with our clients to make them ready for the dropping of invalids.
- A proud member of MANRS and getting all the benefits from being in the elite platform of Routing Security.
- Securing global routing information is done by RPKI.

MANRS

RPKI

Fiber@Home

One Last Thing

- ARIN has announced a surprised maintenance of 30 min in July 2021. Announcement was made on 2nd June 2021.

- They are doing it to make sure that their RPKI infrastructure is running with peak performance.

- https://www.arin.net/announcements/20210602-rpki/

- Also Job Snijders has shared some valuable insights on this maintenance work.

- https://lists.arin.net/pipermail/arin-tech-discuss/2021-June/000932.html

- Our learning –
    - When you deploy RPKI, you need to keep an eye on your RPKI infrastructure performance.
    - You need to make sure that any maintenance work is informed to your clients way ahead.
    - Also you need to be aware of the events taking places in RIRs regarding their RPKI Infrastructure.

Reference

- https://www.manrs.org/about/

- https://blog.apnic.net/2019/10/28/how-to-installing-an-rpki-validator/

- http://www.bgp4all.com.au/pfs/training/apnic48/agenda

- https://rpki.readthedocs.io/en/latest/ops/tools.html#doc-tools

- https://www.ripe.net/manage-ips-and-asns/resource-management/certification/tools-and-resources

- https://github.com/cloudflare/cfrpki#octorpki

- https://www.rpki-client.org/

Appendix-1

- Step by Step Installation of Routinator

- Step by Step Installation of OctoRPKI

- Step by Step Installation of Fort

- Step by Step Installation of RPKI-Client

Appendix-1

- Step by Step Installation of Routinator

Installation (Routinator)

Add the line below that corresponds to your operating system to your
/etc/apt/sources.list or */etc/apt/sources.list.d/*

deb [arch=amd64] https://packages.nlnetlabs.nl/linux/debian/ stretch main
deb [arch=amd64] https://packages.nlnetlabs.nl/linux/debian/ buster main
deb [arch=amd64] https://packages.nlnetlabs.nl/linux/ubuntu/ xenial main
deb [arch=amd64] https://packages.nlnetlabs.nl/linux/ubuntu/ bionic main
deb [arch=amd64] https://packages.nlnetlabs.nl/linux/ubuntu/ focal main

Installation (Routinator)

Then run the following commands to add the public key and update the repository list

wget -qO- https://packages.nlnetlabs.nl/aptkey.asc | sudo apt-key add -
sudo apt update

```
nano@ROV:~$
nano@ROV:~$
nano@ROV:~$ wget -qO- https://packages.nlnetlabs.nl/aptkey.asc | sudo apt-key add -
OK
nano@ROV:~$
```

```
nano@ROV:~$ sudo apt update
Hit:1 http://ppa.launchpad.net/ansible/ansible/ubuntu xenial InRelease
Hit:2 http://us.archive.ubuntu.com/ubuntu xenial InRelease
Get:3 http://security.ubuntu.com/ubuntu xenial-security InRelease [109 kB]
Hit:4 http://archive.canonical.com/ubuntu xenial InRelease
Hit:5 http://ppa.launchpad.net/ondrej/php/ubuntu xenial InRelease
Get:6 http://us.archive.ubuntu.com/ubuntu xenial-updates InRelease [109 kB]
Get:7 https://packages.nlnetlabs.nl/linux/debian stretch InRelease [4,331 B]
Get:8 https://packages.nlnetlabs.nl/linux/debian buster InRelease [4,327 B]
Get:9 https://packages.nlnetlabs.nl/linux/ubuntu xenial InRelease [4,327 B]
Ign:10 https://dl.bintray.com/wand/general xenial InRelease
Get:11 https://packages.nlnetlabs.nl/linux/ubuntu bionic InRelease [4,327 B]
Get:12 http://us.archive.ubuntu.com/ubuntu xenial-backports InRelease [107 kB]
Err:13 https://dl.bintray.com/wand/general xenial Release
  403  Forbidden
Get:14 https://packages.nlnetlabs.nl/linux/ubuntu focal InRelease [4,323 B]
Get:15 https://packages.nlnetlabs.nl/linux/debian stretch/main amd64 Packages [4,572 B]
Get:16 http://us.archive.ubuntu.com/ubuntu xenial-updates/main amd64 Packages [2,049 kB]
Get:17 https://packages.nlnetlabs.nl/linux/debian buster/main amd64 Packages [4,604 B]
Hit:18 https://pkg.caida.org/os/ubuntu xenial InRelease
Get:19 https://packages.nlnetlabs.nl/linux/ubuntu xenial/main amd64 Packages [4,566 B]
Get:20 https://packages.nlnetlabs.nl/linux/ubuntu bionic/main amd64 Packages [4,599 B]
Get:21 https://packages.nlnetlabs.nl/linux/ubuntu focal/main amd64 Packages [4,611 B]
Get:22 http://us.archive.ubuntu.com/ubuntu xenial-updates/main i386 Packages [1,525 kB]
Reading package lists... Done
```

Installation (Routinator)

You can then install Routinator by running this command

sudo apt install routinator

```
nano@ROV:~$
nano@ROV:~$ sudo apt install routinator
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following NEW packages will be installed:
  routinator
0 upgraded, 1 newly installed, 0 to remove and 197 not upgraded.
Need to get 3,287 kB of archives.
After this operation, 10.1 MB of additional disk space will be used.
Get:1 https://packages.nlnetlabs.nl/linux/ubuntu xenial/main amd64 routinator amd64 0.9.0-1xenial [3,287 kB]
Fetched 3,287 kB in 2s (1,438 kB/s)
Selecting previously unselected package routinator.
(Reading database ... 80683 files and directories currently installed.)
Preparing to unpack .../routinator_0.9.0-1xenial_amd64.deb ...
Unpacking routinator (0.9.0-1xenial) ...
Processing triggers for man-db (2.7.5-1) ...
Setting up routinator (0.9.0-1xenial) ...
Adding system user `routinator' (UID 113) ...
Adding new group `routinator' (GID 120) ...
Adding new user `routinator' (UID 113) with group `routinator' ...
Creating home directory `/var/lib/routinator/' ...
routinator.service is a disabled or a static unit, not starting it.
```

Installation (Routinator)

Initialise, enable and start Routinator by running these commands.

sudo routinator-init   (This command should be given in /home/user/ directory)
sudo systemctl enable --now routinator

```
nano@ROV:~$ sudo routinator-init
Running command as user routinator: routinator --config /etc/routinator/routinator.conf init
Before we can install the ARIN TAL, you must have read
and agree to the ARIN Relying Party Agreement (RPA).
It is available at

https://www.arin.net/resources/manage/rpki/rpa.pdf

If you agree to the RPA, please run the command
again with the --accept-arin-rpa option.
Fatal error. Exiting.
nano@ROV:~$ sudo routinator-init --accept-arin-rpa
Running command as user routinator: routinator --config /etc/routinator/routinator.conf init --accept-arin-rpa
Created local repository directory /var/lib/routinator/rpki-cache
Installed 5 TALs in /var/lib/routinator/tals
```

```
nano@ROV:~$ sudo systemctl enable --now routinator
Created symlink from /etc/systemd/system/multi-user.target.wants/routinator.service to /lib/systemd/system/routinator.service.
nano@ROV:~$
```

MANRS

Fiber @ Home

Installation (Routinator)

By default, Routinator will start the RTR server on port 3323 and the HTTP server on port 8323 which can be changed in */etc/routinator/routinator.conf*. You can check the status of Routinator with *sudo systemctl status routinator* and view the logs with *sudo journalctl --unit=routinator*

```
nano@ROV:~$ sudo systemctl status routinator
â routinator.service - Routinator 3000
   Loaded: loaded (/lib/systemd/system/routinator.service; enabled; vendor preset: disabled)
   Active: active (running) since Sun 2021-06-06 13:35:25 +06; 1min 31s ago
     Docs: man:routinator(1)
 Main PID: 3093 (routinator)
    Tasks: 18
   Memory: 2.1G
      CPU: 56.028s
   CGroup: /system.slice/routinator.service
           ââ3093 /usr/bin/routinator --config=/etc/routinator/routinator.conf --syslog server

Jun 06 13:35:25 ROV systemd[1]: Started Routinator 3000.
Jun 06 13:36:26 ROV routinator[3093]: RRDP https://chloe.sobornost.net/rpki/news-public.xml: Getting notification file failed with sta
Jun 06 13:36:26 ROV routinator[3093]: RRDP repository https://chloe.sobornost.net/rpki/news-public.xml unavailable. Falling back to rs
Jun 06 13:36:27 ROV routinator[3093]: rsync://rpkica.mckay.com/rpki/MCnet/Jp4Tjp_GB5I1RfeaOGhKZN1DmAQ.mft: stale manifest
Jun 06 13:36:27 ROV routinator[3093]: rsync://rpkica.mckay.com/rpki/MCnet/Jp4Tjp_GB5I1RfeaOGhKZN1DmAQ.mft: No valid manifest found.
Jun 06 13:36:29 ROV routinator[3093]: RRDP https://chloe.sobornost.net/rpki/news.xml: Getting notification file failed with status 404
Jun 06 13:36:29 ROV routinator[3093]: RRDP repository https://chloe.sobornost.net/rpki/news.xml unavailable. Falling back to rsync.
Jun 06 13:36:39 ROV routinator[3093]: rsync://rpkica.mckay.com/rpki/MCnet/UEh2SAvdIgPsUFdv92RSSaNqBnY.mft: No valid manifest found.
Jun 06 13:36:43 ROV routinator[3093]: rsync://ca.rg.net/rpki/RGnet-OU/ovsCA/IOUcOeBGM_Tb4dwfvswY4bnNZYY.mft: No valid manifest found.
```

Installation (Routinator)

routinator -v vrps

routinator server --rtr SERVER-IP:3323 --http SERVER-IP:9556 --refresh=900 &


```
AS33652,68.86.104.0/23,23,arin
AS33363,104.136.0.0/17,17,arin
AS36985,41.223.172.0/22,24,afrinic
AS395077,199.34.92.0/22,24,arin
AS16509,15.184.0.0/16,24,arin
AS33651,2001:559:c0e4::/48,48,arin
AS13335,172.68.130.0/24,24,arin
AS36040,64.15.118.0/23,23,arin
AS396982,104.198.96.0/20,20,arin
AS33489,50.215.192.0/20,20,arin
AS20940,204.156.7.0/24,24,arin
AS11955,2605:a000:1e00::/40,40,arin
AS16509,54.95.128.0/17,17,arin
AS33287,2001:559:80eb::/48,48,arin
AS6453,209.58.84.0/24,24,arin
AS36958,41.86.32.0/19,24,afrinic
AS15247,207.194.200.0/21,24,arin
AS20115,97.81.224.0/20,20,arin
AS394627,50.235.27.0/24,24,arin
AS22006,165.254.24.240/29,29,arin
AS20115,24.158.224.0/20,20,arin
AS20115,68.189.0.0/19,19,arin
AS14618,174.129.0.0/16,24,arin
AS10838,76.89.62.0/23,23,arin
AS8987,162.87.0.0/16,24,arin
AS23218,208.110.193.0/24,24,arin
AS15169,104.134.132.0/24,24,arin
AS11377,149.72.128.0/19,19,arin
AS14618,15.193.0.0/16,24,arin
AS5645,107.190.64.0/22,22,arin
AS134963,47.238.0.0/16,24,arin
AS20738,198.71.128.0/17,24,arin
AS33491,50.212.128.0/19,19,arin
AS22909,2001:558:feee::/48,48,arin
AS7015,50.206.154.0/24,24,arin
AS33652,2001:559:8185::/48,48,arin
AS394667,52.129.34.0/24,24,arin
AS7015,2001:559:c24d::/48,48,arin
AS29802,209.182.109.0/24,24,arin
AS15169,2607:f8b0:4002::/48,48,arin
AS33667,76.125.32.0/19,19,arin
AS2495,69.77.114.0/24,24,arin
nano@ROV:~$
```
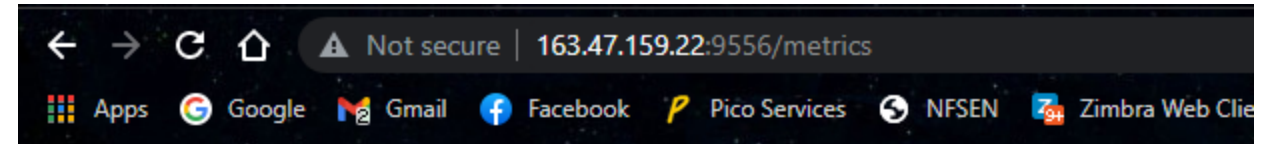
```
root@routinator-2:~# routinator server --rtr 163.47.159.22:3323 --http 163.47.159.22:9556 --refresh=900 &
[1] 1656
root@routinator-2:~# RRDP https://rpkica.mckay.com/rrdp/notify.xml: failed to process snapshot file https://rpkica.mckay.com/rrdp/793b11
fa-6583-4d49-b63a-5a3bd7297073/snapshot/1910.xml: error sending request for url (https://rpkica.mckay.com/rrdp/793b11fa-6583-4d49-b63a-5
a3bd7297073/snapshot/1910.xml): connection closed before message completed
RRDP repository https://rpkica.mckay.com/rrdp/notify.xml unavailable. Falling back to rsync.
rsync://rpki-repo.registro.br/repo/6vfUNUa2zYk4YiMhCyTKaqzdG82XWsjeyuErT3eS6nkZ/0/F24D082C82FF9E11E84C687D8D35F1210230FA8D.mft: stale ma
nifest
rsync://rpki-repo.registro.br/repo/6vfUNUa2zYk4YiMhCyTKaqzdG82XWsjeyuErT3eS6nkZ/0/F24D082C82FF9E11E84C687D8D35F1210230FA8D.mft: No valid
 manifest found.
RRDP https://chloe.sobornost.net/rpki/news-public.xml: Getting notification file failed with status 404 Not Found
RRDP repository https://chloe.sobornost.net/rpki/news-public.xml unavailable. Falling back to rsync.
RRDP https://chloe.sobornost.net/rpki/news.xml: Getting notification file failed with status 404 Not Found
RRDP repository https://chloe.sobornost.net/rpki/news.xml unavailable. Falling back to rsync.
rsync://rpkica.mckay.com/rpki/MCnet/UEh2SAvdIgPsUFdv92RSSaNqBnY.mft: No valid manifest found.
rsync://rpkica.mckay.com/rpki/MCnet/Jp4Tjp_GB5I1RfeaOGhKZNlDmAQ.mft: stale manifest
rsync://rpkica.mckay.com/rpki/MCnet/Jp4Tjp_GB5I1RfeaOGhKZNlDmAQ.mft: No valid manifest found.
```

Installation (Routinator)

Appendix-1

- Step by Step Installation of OctoRPKI

Installation (OctoRPKI)

First, go to the Releases tab, download the latest version matching your platform.


```
root@routinator-2:~# wget https://github.com/cloudflare/cfrpki/releases/download/v1.2.2/octorpki_1.2.2_amd64.deb
--2021-06-07 07:36:17--  https://github.com/cloudflare/cfrpki/releases/download/v1.2.2/octorpki_1.2.2_amd64.deb
Resolving github.com (github.com)... 13.229.188.59
Connecting to github.com (github.com)|13.229.188.59|:443... connected.
HTTP request sent, awaiting response... 302 Found
Location: https://github-releases.githubusercontent.com/170715385/05943a00-3a5a-11eb-9d88-54bbe1b138c0?X-Amz-Algorithm=AWS4-HMAC-SHA256&
X-Amz-Credential=AKIAIWNJYAX4CSVEH53A%2F20210607%2Fus-east-1%2Fs3%2Faws4_request&X-Amz-Date=20210607T073617Z&X-Amz-Expires=300&X-Amz-Sig
nature=bbc4ca51e146e75bd5042ac5beb1220e8d58bad5efbbaa67494b8a0527af0bb8&X-Amz-SignedHeaders=host&actor_id=0&key_id=0&repo_id=170715385&r
esponse-content-disposition=attachment%3B%20filename%3Doctorpki_1.2.2_amd64.deb&response-content-type=application%2Foctet-stream [follow
ing]
--2021-06-07 07:36:18--  https://github-releases.githubusercontent.com/170715385/05943a00-3a5a-11eb-9d88-54bbe1b138c0?X-Amz-Algorithm=AW
S4-HMAC-SHA256&X-Amz-Credential=AKIAIWNJYAX4CSVEH53A%2F20210607%2Fus-east-1%2Fs3%2Faws4_request&X-Amz-Date=20210607T073617Z&X-Amz-Expire
s=300&X-Amz-Signature=bbc4ca51e146e75bd5042ac5beb1220e8d58bad5efbbaa67494b8a0527af0bb8&X-Amz-SignedHeaders=host&actor_id=0&key_id=0&repo
_id=170715385&response-content-disposition=attachment%3B%20filename%3Doctorpki_1.2.2_amd64.deb&response-content-type=application%2Foctet
-stream
Resolving github-releases.githubusercontent.com (github-releases.githubusercontent.com)... 185.199.108.154, 185.199.111.154, 185.199.109
.154, ...
Connecting to github-releases.githubusercontent.com (github-releases.githubusercontent.com)|185.199.108.154|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 7521994 (7.2M) [application/octet-stream]
Saving to: 'octorpki_1.2.2_amd64.deb'

octorpki_1.2.2_amd64.deb        100%[===================================================================>]   7.17M  7.31MB/s    in 1.0s

2021-06-07 07:36:19 (7.31 MB/s) - 'octorpki_1.2.2_amd64.deb' saved [7521994/7521994]

root@routinator-2:~# ls
octorpki_1.2.2_amd64.deb    snap
```

Installation (OctoRPKI)

To install the Linux deb package and start it:

$ sudo dpkg -i octorpki_1.1.4_amd64.deb
$ sudo systemctl start octorpki

Installation (OctoRPKI)

mkdir tals
cd tals
wget https://raw.githubusercontent.com/cloudflare/cfrpki/master/cmd/octorpki/tals/afrinic.tal
wget https://raw.githubusercontent.com/cloudflare/cfrpki/master/cmd/octorpki/tals/apnic.tal
wget https://raw.githubusercontent.com/cloudflare/cfrpki/master/cmd/octorpki/tals/lacnic.tal
wget https://raw.githubusercontent.com/cloudflare/cfrpki/master/cmd/octorpki/tals/ripe.tal
wget https://www.arin.net/resources/manage/rpki/arin-rfc7730.tal -O arin.tal
cd ..

```
root@routinator-2:~/tals#
root@routinator-2:~/tals# wget https://raw.githubusercontent.com/cloudflare/cfrpki/master/cmd/octorpki/tals/afrinic.tal

wget https://raw.githubusercontent.com/cloudflare/cfrpki/master/cmd/octorpki/tals/apnic.tal

wget https://raw.githubusercontent.com/cloudflare/cfrpki/master/cmd/octorpki/tals/lacnic.tal

wget https://raw.githubusercontent.com/cloudflare/cfrpki/master/cmd/octorpki/tals/ripe.tal

--2021-06-07 07:50:39--  https://raw.githubusercontent.com/cloudflare/cfrpki/master/cmd/octorpki/tals/afrinic.tal
Resolving raw.githubusercontent.com (raw.githubusercontent.com)... wget https://www.arin.net/resources/manage/rpki/arin-rfc7730.tal -O a
rin.tal
185.199.111.133, 185.199.110.133, 185.199.109.133, ...
Connecting to raw.githubusercontent.com (raw.githubusercontent.com)|185.199.111.133|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 495 [text/plain]
Saving to: 'afrinic.tal'

afrinic.tal                    100%[===============================================================>]    495  --.-KB/s    in 0s

2021-06-07 07:50:40 (25.1 MB/s) - 'afrinic.tal' saved [495/495]

root@routinator-2:~/tals#
root@routinator-2:~/tals# wget https://raw.githubusercontent.com/cloudflare/cfrpki/master/cmd/octorpki/tals/apnic.tal
--2021-06-07 07:50:40--  https://raw.githubusercontent.com/cloudflare/cfrpki/master/cmd/octorpki/tals/apnic.tal
Resolving raw.githubusercontent.com (raw.githubusercontent.com)... 185.199.108.133, 185.199.109.133, 185.199.110.133, ...
```

Installation (OctoRPKI)

Look into the tals directory to check if you have got all the 5 tals or not.

Run the validator by issuing the following command.
nohup octorpki -output.sign=false > out 2> err &

```
root@routinator-2:~/tals#
root@routinator-2:~/tals# ls
afrinic.tal  apnic.tal  arin.tal  lacnic.tal  ripe.tal
root@routinator-2:~/tals# cd ..
root@routinator-2:~#
root@routinator-2:~#
root@routinator-2:~#
root@routinator-2:~#
root@routinator-2:~#
root@routinator-2:~#
root@routinator-2:~#
root@routinator-2:~#
root@routinator-2:~#
root@routinator-2:~# nohup octorpki -output.sign=false > out 2> err &
[1] 2519
root@routinator-2:~#
```

MANRS

RPKI

Fiber @ Home

Installation (OctoRPKI)

If the validator runs smoothly, you will see the ROAs in web format by querying a json file.

The validated cache output uses default port 8081.

GoRTR metrics uses default port 8080.

You can build RTR session on your desired port.

← → C ⌂ ⚠ Not secure | 163.47.159.22:8081/output.json

Apps G Google M Gmail f Facebook P Pico Services S NFSEN Zimbra Web Client... Login (1) Bachelor Point |... lg.level3.net RA RADb :: How to: In

{"metadata":{"counts":219365,"generated":1623051957,"valid":1623055557},"roas":[{"prefix":"154.16.244.0/24","maxLength":24,"asn":"AS63018","ta":"AFRINIC"},
{"prefix":"154.216.128.0/18","maxLength":18,"asn":"AS328608","ta":"AFRINIC"},{"prefix":"41.86.32.0/19","maxLength":24,"asn":"AS36958","ta":"AFRINIC"},
{"prefix":"41.191.120.0/22","maxLength":24,"asn":"AS36958","ta":"AFRINIC"},{"prefix":"41.222.204.0/22","maxLength":24,"asn":"AS36958","ta":"AFRINIC"},
{"prefix":"41.223.216.0/22","maxLength":24,"asn":"AS36958","ta":"AFRINIC"},{"prefix":"197.157.96.0/19","maxLength":24,"asn":"AS36958","ta":"AFRINIC"},
{"prefix":"2c0f:fef0::/32","maxLength":48,"asn":"AS36958","ta":"AFRINIC"},{"prefix":"2c0f:f4e0::/32","maxLength":32,"asn":"AS327909","ta":"AFRINIC"},
{"prefix":"41.76.128.0/21","maxLength":23,"asn":"AS37199","ta":"AFRINIC"},{"prefix":"197.155.0.0/19","maxLength":21,"asn":"AS37199","ta":"AFRINIC"},
{"prefix":"160.119.32.0/19","maxLength":19,"asn":"AS327804","ta":"AFRINIC"},{"prefix":"196.4.162.0/24","maxLength":24,"asn":"AS3741","ta":"AFRINIC"},
{"prefix":"2c0f:e908::/32","maxLength":48,"asn":"AS327750","ta":"AFRINIC"},{"prefix":"41.87.0.0/24","maxLength":24,"asn":"AS36969","ta":"AFRINIC"},
{"prefix":"41.87.1.0/24","maxLength":24,"asn":"AS36969","ta":"AFRINIC"},{"prefix":"41.87.2.0/24","maxLength":24,"asn":"AS36969","ta":"AFRINIC"},
{"prefix":"41.87.3.0/24","maxLength":24,"asn":"AS36969","ta":"AFRINIC"},{"prefix":"41.87.4.0/24","maxLength":24,"asn":"AS36969","ta":"AFRINIC"},
{"prefix":"41.87.5.0/24","maxLength":24,"asn":"AS36969","ta":"AFRINIC"},{"prefix":"41.87.6.0/24","maxLength":24,"asn":"AS36969","ta":"AFRINIC"},
{"prefix":"41.87.7.0/24","maxLength":24,"asn":"AS36969","ta":"AFRINIC"},{"prefix":"41.221.100.0/24","maxLength":24,"asn":"AS36969","ta":"AFRINIC"},
{"prefix":"196.2.3.0/24","maxLength":24,"asn":"AS33764","ta":"AFRINIC"},{"prefix":"196.43.188.0/23","maxLength":24,"asn":"AS327687","ta":"AFRINIC"},
{"prefix":"45.195.250.0/24","maxLength":24,"asn":"AS212552","ta":"AFRINIC"},{"prefix":"156.233.192.0/19","maxLength":24,"asn":"AS398968","ta":"AFRINIC"},
{"prefix":"156.227.22.0/23","maxLength":24,"asn":"AS136907","ta":"AFRINIC"},{"prefix":"45.220.32.0/20","maxLength":20,"asn":"AS327999","ta":"AFRINIC"},
{"prefix":"196.2.32.0/22","maxLength":24,"asn":"AS3741","ta":"AFRINIC"},{"prefix":"2001:43f8:e00::/40","maxLength":48,"asn":"AS42","ta":"AFRINIC"},
{"prefix":"154.16.209.0/24","maxLength":24,"asn":"AS9891","ta":"AFRINIC"},{"prefix":"41.180.0.0/20","maxLength":24,"asn":"AS36916","ta":"AFRINIC"},
{"prefix":"41.221.102.0/24","maxLength":24,"asn":"AS36969","ta":"AFRINIC"},{"prefix":"196.223.21.0/24","maxLength":24,"asn":"AS37704","ta":"AFRINIC"},
{"prefix":"2001:43f8:60::/48","maxLength":48,"asn":"AS37704","ta":"AFRINIC"},{"prefix":"137.63.192.0/21","maxLength":21,"asn":"AS327687","ta":"AFRINIC"},
{"prefix":"2c0f:fbc0::/32","maxLength":48,"asn":"AS37670","ta":"AFRINIC"},{"prefix":"41.180.120.0/21","maxLength":24,"asn":"AS36916","ta":"AFRINIC"},
{"prefix":"196.60.70.0/23","maxLength":23,"asn":"AS0","ta":"AFRINIC"},{"prefix":"154.73.251.0/24","maxLength":24,"asn":"AS23470","ta":"AFRINIC"},
{"prefix":"2c0f:fcb0::/32","maxLength":48,"asn":"AS36916","ta":"AFRINIC"},{"prefix":"156.246.96.0/19","maxLength":24,"asn":"AS3356","ta":"AFRINIC"},
{"prefix":"45.195.146.0/24","maxLength":24,"asn":"AS134548","ta":"AFRINIC"},{"prefix":"196.10.141.0/24","maxLength":24,"asn":"AS0","ta":"AFRINIC"},
{"prefix":"154.127.48.0/20","maxLength":24,"asn":"AS61317","ta":"AFRINIC"},{"prefix":"154.16.188.0/22","maxLength":24,"asn":"AS174","ta":"AFRINIC"},
{"prefix":"154.82.232.0/22","maxLength":24,"asn":"AS1239","ta":"AFRINIC"},{"prefix":"154.219.16.0/20","maxLength":20,"asn":"AS328608","ta":"AFRINIC"},
{"prefix":"154.92.193.0/24","maxLength":24,"asn":"AS54600","ta":"AFRINIC"},{"prefix":"154.118.244.0/22","maxLength":24,"asn":"AS328366","ta":"AFRINIC"},
{"prefix":"156.227.32.0/19","maxLength":19,"asn":"AS328608","ta":"AFRINIC"},{"prefix":"45.204.68.0/24","maxLength":24,"asn":"AS134548","ta":"AFRINIC"},
{"prefix":"169.255.112.0/24","maxLength":24,"asn":"AS327859","ta":"AFRINIC"},{"prefix":"192.96.37.0/24","maxLength":24,"asn":"AS10474","ta":"AFRINIC"},
{"prefix":"156.0.103.0/24","maxLength":24,"asn":"AS328227","ta":"AFRINIC"},{"prefix":"196.3.164.0/22","maxLength":24,"asn":"AS11845","ta":"AFRINIC"},
{"prefix":"197.81.153.0/24","maxLength":24,"asn":"AS12258","ta":"AFRINIC"},{"prefix":"154.16.77.0/24","maxLength":24,"asn":"AS7922","ta":"AFRINIC"},
{"prefix":"154.16.219.0/24","maxLength":24,"asn":"AS29713","ta":"AFRINIC"},{"prefix":"102.129.153.0/24","maxLength":24,"asn":"AS174","ta":"AFRINIC"},
{"prefix":"154.82.200.0/22","maxLength":24,"asn":"AS1239","ta":"AFRINIC"},{"prefix":"160.119.192.0/22","maxLength":24,"asn":"AS32437","ta":"AFRINIC"},
{"prefix":"196.60.8.0/23","maxLength":23,"asn":"AS0","ta":"AFRINIC"},{"prefix":"196.60.10.0/23","maxLength":23,"asn":"AS0","ta":"AFRINIC"},
{"prefix":"196.41.128.0/19","maxLength":24,"asn":"AS12258","ta":"AFRINIC"},{"prefix":"102.130.236.0/22","maxLength":24,"asn":"AS328391","ta":"AFRINIC"},
{"prefix":"2c0f:ec18::/32","maxLength":48,"asn":"AS328391","ta":"AFRINIC"},{"prefix":"102.129.135.0/24","maxLength":24,"asn":"AS61317","ta":"AFRINIC"},
{"prefix":"102.165.32.0/22","maxLength":24,"asn":"AS61317","ta":"AFRINIC"},{"prefix":"102.165.40.0/22","maxLength":24,"asn":"AS61317","ta":"AFRINIC"},
{"prefix":"102.165.56.0/22","maxLength":24,"asn":"AS61317","ta":"AFRINIC"},{"prefix":"105.169.96.0/19","maxLength":19,"asn":"AS37119","ta":"AFRINIC"},
{"prefix":"102.222.180.0/22","maxLength":24,"asn":"AS328453","ta":"AFRINIC"},{"prefix":"45.195.200.0/24","maxLength":24,"asn":"AS212552","ta":"AFRINIC"},
{"prefix":"165.16.128.0/19","maxLength":24,"asn":"AS37314","ta":"AFRINIC"},{"prefix":"196.223.1.0/24","maxLength":24,"asn":"AS37383","ta":"AFRINIC"},

MANRS

RPKI

Fiber @ Home

Installation (OctoRPKI)

GoRTR is Cloudflare's RPKI-RTR server component, which allows RPKI-enabled routers to connect to it and fetch the validated cache (ROA cache).

wget https://github.com/cloudflare/gortr/releases/download/v0.14.7/gortr_0.14.7_amd64.deb

dpkg -i gortr_0.14.7_amd64.deb

Installation (OctoRPKI)

nohup gortr -bind=SERVER-IP:8282 -metrics.addr=:8080 -verify=false -cache=http://SERVER-IP:8081/output.json > out 2> err &

```
root@routinator-2:~#
root@routinator-2:~# nohup gortr -bind=163.47.159.22:8282 -metrics.addr=:8080 -verify=false -cache=http://163.47.159.22:8081/output.json > out 2>
err &
[2] 6483
root@routinator-2:~#
```

```
root@routinator-2:~#
root@routinator-2:~# ps ax | grep gortr
   6483 pts/0    Sl     0:06 gortr -bind=163.47.159.22:8282 -metrics.addr=:8080 -verify=false -cache=http://163.47.159.22:8081/output.json
   6584 pts/0    R+     0:00 grep --color=auto gortr
root@routinator-2:~# ps ax | grep octo
   5690 pts/0    Sl     6:02 octorpki -output.sign=false
   6588 pts/0    S+     0:00 grep --color=auto octo
root@routinator-2:~#
```

```
RP/0/RSP1/CPU0:C-AGG-1#sh bgp rpki server summary
Mon Jun  7 16:20:55.602 BST

Hostname/Address          Transport        State         Time           ROAs (IPv4/IPv6)
163.47.159.22             TCP:8282         ESTAB         00:02:07       214077/39923

RP/0/RSP1/CPU0:C-AGG-1#
```

Appendix-1

- Step by Step Installation of Fort

MANRS   RPKI   Fiber@Home

Installation (FORT)

It has some dependencies. So need to resolve those first.
sudo apt install openssl rsync libjansson-dev -y

Version **1.5.0** is the latest official release. To fetch or review it, visit the GitHub release
sudo wget https://github.com/NICMx/FORT-validator/releases/download/v1.5.0/fort_1.5.0-1_amd64.deb
sudo apt install ./fort_1.5.0-1_amd64.deb

```
nano@routinator-2:~$
nano@routinator-2:~$ sudo apt install openssl rsync libjansson-dev -y
Reading package lists... Done
Building dependency tree
Reading state information... Done
libjansson-dev is already the newest version (2.12-1build1).
rsync is already the newest version (3.1.3-8).
openssl is already the newest version (1.1.1f-1ubuntu2.4).
0 upgraded, 0 newly installed, 0 to remove and 64 not upgraded.
```

```
nano@routinator-2:~$ sudo apt install ./fort_1.5.0-1_amd64.deb
Reading package lists... Done
Building dependency tree
Reading state information... Done
Note, selecting 'fort' instead of './fort_1.5.0-1_amd64.deb'
The following NEW packages will be installed:
  fort
0 upgraded, 1 newly installed, 0 to remove and 64 not upgraded.
Need to get 0 B/217 kB of archives.
After this operation, 630 kB of additional disk space will be used.
Get:1 /home/nano/fort_1.5.0-1_amd64.deb fort amd64 1.5.0-1 [217 kB]
Selecting previously unselected package fort.
(Reading database ... 71437 files and directories currently installed.)
Preparing to unpack .../nano/fort_1.5.0-1_amd64.deb ...
Unpacking fort (1.5.0-1) ...
Setting up fort (1.5.0-1) ...
Created symlink /etc/systemd/system/multi-user.target.wants/fort.service →
Processing triggers for man-db (2.9.1-1) ...
nano@routinator-2:~$
```

```
nano@routinator-2:~$
nano@routinator-2:~$ sudo wget https://github.com/NICMx/FORT-validator/releases/download/v1.5.0/fort_1.5.0-1_amd64.deb
--2021-06-07 13:59:34--  https://github.com/NICMx/FORT-validator/releases/download/v1.5.0/fort_1.5.0-1_amd64.deb
Resolving github.com (github.com)... 52.74.223.119
Connecting to github.com (github.com)|52.74.223.119|:443... connected.
HTTP request sent, awaiting response... 302 Found
Location: https://github-releases.githubusercontent.com/147424126/596ded00-6b89-11eb-9126-02f6d09f9784?X-Amz-Algorithm=A
WS4-HMAC-SHA256&X-Amz-Credential=AKIAIWNJYAX4CSVEH53A%2F20210607%2Fus-east-1%2Fs3%2Faws4_request&X-Amz-Date=20210607T135
935Z&X-Amz-Expires=300&X-Amz-Signature=57ac21ce118b7a18dad1ec8df04297fbee9a09192872a77b4da34b592e4f0e03&X-Amz-SignedHead
ers=host&actor_id=0&key_id=0&repo_id=147424126&response-content-disposition=attachment%3B%20filename%3Dfort_1.5.0-1_amd6
4.deb&response-content-type=application%2Foctet-stream [following]
--2021-06-07 13:59:35--  https://github-releases.githubusercontent.com/147424126/596ded00-6b89-11eb-9126-02f6d09f9784?X-
Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=AKIAIWNJYAX4CSVEH53A%2F20210607%2Fus-east-1%2Fs3%2Faws4_request&X-Amz-Da
te=20210607T135935Z&X-Amz-Expires=300&X-Amz-Signature=57ac21ce118b7a18dad1ec8df04297fbee9a09192872a77b4da34b592e4f0e03&X
-Amz-SignedHeaders=host&actor_id=0&key_id=0&repo_id=147424126&response-content-disposition=attachment%3B%20filename%3Dfo
rt_1.5.0-1_amd64.deb&response-content-type=application%2Foctet-stream
Resolving github-releases.githubusercontent.com (github-releases.githubusercontent.com)... 185.199.108.154, 185.199.109.
154, 185.199.110.154, ...
Connecting to github-releases.githubusercontent.com (github-releases.githubusercontent.com)|185.199.108.154|:443... conn
ected.
HTTP request sent, awaiting response... 200 OK
Length: 216596 (212K) [application/octet-stream]
Saving to: 'fort_1.5.0-1_amd64.deb.1'

fort_1.5.0-1_amd64.deb.1     100%[===================================================>] 211.52K  --.-KB/s    in 0.1s

2021-06-07 13:59:36 (1.67 MB/s) - 'fort_1.5.0-1_amd64.deb.1' saved [216596/216596]
```

MANRS
RPKI
Fiber @ Home

Installation (FORT)

You will find an example config.json file inside */etc/fort/example*.

Rename the actual config.josn file to something else and copy the config file from example directory to */etc/fort/*

In this way it will be much more easier to configure without destroying the json format.

Change the below parameters if required.

Tal
Local-repository
Address
Port

Rest of the fields should be fine with default values.

```
nano@routinator-2:/etc/fort$
nano@routinator-2:/etc/fort$ ls
config.json   examples   slurm   tal
nano@routinator-2:/etc/fort$ cd examples/
nano@routinator-2:/etc/fort/examples$ ls
config.json   demo.slurm
nano@routinator-2:/etc/fort/examples$
```

```
{
  "tal": "/etc/fort/tal/",
  "local-repository": "/var/lib/fort",
  "work-offline": false,
  "shuffle-uris": false,
  "maximum-certificate-depth": 32,
  "mode": "server",
  "daemon": false,
  "server": {
    "address": [
      "163.47.159.22"
    ],
    "port": "8282",
    "backlog": 64,
    "interval": {
      "validation": 3600,
      "refresh": 3600,
      "retry": 600,
      "expire": 7200
    }
  }
}
```

MANRS   RPKI   Fiber @ Home

Installation (FORT)

Get the tals including Arin.
sudo fort --init-tals --tal=/etc/fort/tal

```
nano@routinator-2:~$
nano@routinator-2:~$ cd /etc/fort/tal
nano@routinator-2:/etc/fort/tal$
nano@routinator-2:/etc/fort/tal$
nano@routinator-2:/etc/fort/tal$
nano@routinator-2:/etc/fort/tal$
nano@routinator-2:/etc/fort/tal$ sudo fort --init-tals --tal=/etc/fort/tal
Please download and read ARIN Relying Party Agreement (RPA) from https://www.arin.net/resources/manage/rpki/rpa.pdf. Onc
e you've read it and if you agree ARIN RPA, type 'yes' to proceed with ARIN's TAL download:
yes
Successfully fetched '/etc/fort/tal/arin.tal'!
Successfully fetched '/etc/fort/tal/apnic.tal'!
Successfully fetched '/etc/fort/tal/afrinic.tal'!
Successfully fetched '/etc/fort/tal/ripe.tal'!
Successfully fetched '/etc/fort/tal/lacnic.tal'!
```

Installation (FORT)

Start fort as a service.

Check the status. It will take some time to build the first validated cache.

```
nano@routinator-2:~$
nano@routinator-2:~$ sudo service fort start
nano@routinator-2:~$ sudo service fort status
● fort.service - FORT RPKI validator
     Loaded: loaded (/lib/systemd/system/fort.service; enabled; vendor preset: enabled)
     Active: active (running) since Mon 2021-06-07 14:01:12 UTC; 6min ago
       Docs: man:fort(8)
             https://nicmx.github.io/FORT-validator/
   Main PID: 20079 (fort)
      Tasks: 36 (limit: 9220)
     Memory: 777.5M
     CGroup: /system.slice/fort.service
             └─20079 /usr/bin/fort --configuration-file /etc/fort/config.json

Jun 07 14:01:12 routinator-2 systemd[1]: Started FORT RPKI validator.
Jun 07 14:01:12 routinator-2 fort[20079]: WRN: First validation cycle has begun, wait until the next notification to co>
Jun 07 14:05:48 routinator-2 fort[20079]: WRN: Location '/etc/fort/slurm/' doesn't have files with extension '.slurm'
Jun 07 14:05:48 routinator-2 fort[20079]: WRN: First validation cycle successfully ended, now you can connect your rout>
```

```
nano@routinator-2:~$
nano@routinator-2:~$ ps ax | grep fort
  20079 ?        Ssl    3:06 /usr/bin/fort --configuration-file /etc/fort/config.json
  20615 pts/1    S+     0:00 grep --color=auto fort
```

```
RP/0/RSP1/CPU0:C-AGG-1#sh bgp rpki server summary
Mon Jun  7 19:56:26.720 BST

Hostname/Address        Transport       State       Time        ROAs (IPv4/IPv6)
163.47.159.22           TCP:8282        ESTAB       00:33:25    214113/39952
```

MANRS   RPKI   Fiber@Home

Appendix-1

- Step by Step Installation of RPKI-Client

Installation (RPKI-Client)

First, you'll need a recent OpenSSL library (version 1.1.1c and above) on your operating system.

Next, you'll need the */var/cache/rpki-client* directory in place. It must be writable by the operator of **rpki-client**.
mkdir /var/cache/rpki-client

The default output directory is */var/db/rpki-client*, which must also be writable (if not overriden).
mkdir /var/db/rpki-client

```
root@bsd-rpki:~ #
root@bsd-rpki:~ #
root@bsd-rpki:~ # mkdir /var/cache/rpki-client
root@bsd-rpki:~ #
root@bsd-rpki:~ # mkdir /var/db/rpki-client
root@bsd-rpki:~ #
```

Installation (RPKI-Client)

Get the software from git hub
gh repo clone kristapsdz/rpki-client

Edit the make file and put 0 in the value of RPKI_PRIVDROP. If the value is 0, it doesn't use the Privilege Drop user.

```
root@bsd-rpki:~ # mkdir /etc/rpki
root@bsd-rpki:~ # cd /etc/rpki
root@bsd-rpki:/etc/rpki # gh repo clone kristapsdz/rpki-client
Cloning into 'rpki-client'...
remote: Enumerating objects: 1439, done.
remote: Total 1439 (delta 0), reused 0 (delta 0), pack-reused 1439
Receiving objects: 100% (1439/1439), 428.39 KiB | 257.00 KiB/s, done.
Resolving deltas: 100% (1073/1073), done.
root@bsd-rpki:/etc/rpki # ls
rpki-client
```

```
include Makefile.configure

# If set to zero, privilege-dropping is disabled and RPKI_PRIVDROP_USER
# is not used.  Otherwise, privileges are dropped.

RPKI_PRIVDROP           = 0
RPKI_PRIVDROP_USER      = "_rpki-client"
```

MANRS

RPKI

Fiber @ Home

Installation (RPKI-Client)

Get the TALs.
fetch https://rpki.afrinic.net/tal/afrinic.tal
fetch https://www.arin.net/resources/manage/rpki/arin-rfc7730.tal
fetch https://www.lacnic.net/innovaportal/file/4983/1/lacnic.tal
fetch https://tal.apnic.net/apnic.tal
fetch https://tal.rpki.ripe.net/ripe-ncc.tal

Installation (RPKI-Client)

You will be needing open rsync for cache refresh operation.
pkg install openrsync

Go to rpki-client directory and Install rpki-client and run it with mentioning the cache location.
./configure
make
make install
./rpki-client –v –d /var/cache/rpki-client/ /var/db/rpki-client/

```
root@bsd-rpki:/etc/rpki # cd rpki-client/
root@bsd-rpki:/etc/rpki/rpki-client # ./configure
config.log: writing...
configure.local: no (fully automatic configuration)
arc4random: yes
b64_ntop: yes
```

```
root@bsd-rpki:/etc/rpki/rpki-client # make install
mkdir -p /usr/local/bin
mkdir -p /usr/local/man/man8
install -m 0555 rpki-client /usr/local/bin
install -m 0444 rpki-client.install.8 /usr/local/man/man8/rpki-client.8
```

```
root@bsd-rpki:/etc/rpki/rpki-client # make
echo "#define RPKI_RSYNC_COMMAND \""openrsync"\"" ;
echo "#define RPKI_PATH_BASE_DIR \"""/var/cache/rpki-
RPKI_PRIVDROP_USER \"""_rpki-client"\"" ;  echo "#defi
cc  -O2 -pipe -g -W -Wall -Wextra -Wmissing-prototypes
 as.c -o as.o
cc  -O2 -pipe -g -W -Wall -Wextra -Wmissing-prototypes
 cert.c -o cert.o
```

```
root@bsd-rpki:/etc/rpki/rpki-client # ./rpki-client -v -d /var/cache/rpki-client/ /var/db/rpki-client/
rpki-client: https://rpki.afrinic.net/repository/AfriNIC.cer: https schema ignored
rpki-client: https://rpki.ripe.net/ta/ripe-ncc-ta.cer: https schema ignored
rpki-client: rpki.afrinic.net/repository: loading
rpki-client: https://rrdp.lacnic.net/ta/rta-lacnic-rpki.cer: https schema ignored
rpki-client: rpki.arin.net/repository: loading
rpki-client: rpki.ripe.net/ta: loading
rpki-client: repository.lacnic.net/rpki: loading
rpki-client: rpki.apnic.net/repository: loading
```

MANRS   RPKI   Fiber@Home

Installation (RPKI-Client)

If everything goes smoothly, you will be able to see the ROA summury.
bgpctl show sets

You can apply RPKI information to reject invalids on import and export
deny quick from ebgp ovs invalid
deny quick to ebgp ovs invalid

```
root@bsd-rpki:~ # bgpctl show sets
Type    Name                              #IPv4    #IPv6 #ASnum Last Change
ROA     RPKI ROA                         199426    38216      -     01:06:22
PREFIX  mynetworks                            1        1      -     01:06:23
PREFIX  bogons                               14       11      -     01:06:23
root@bsd-rpki:~ #
```

Query !!

Join MANRS : manrs.org/join/

Thanks …

MANRS

RPKI

Fiber @ Home