1

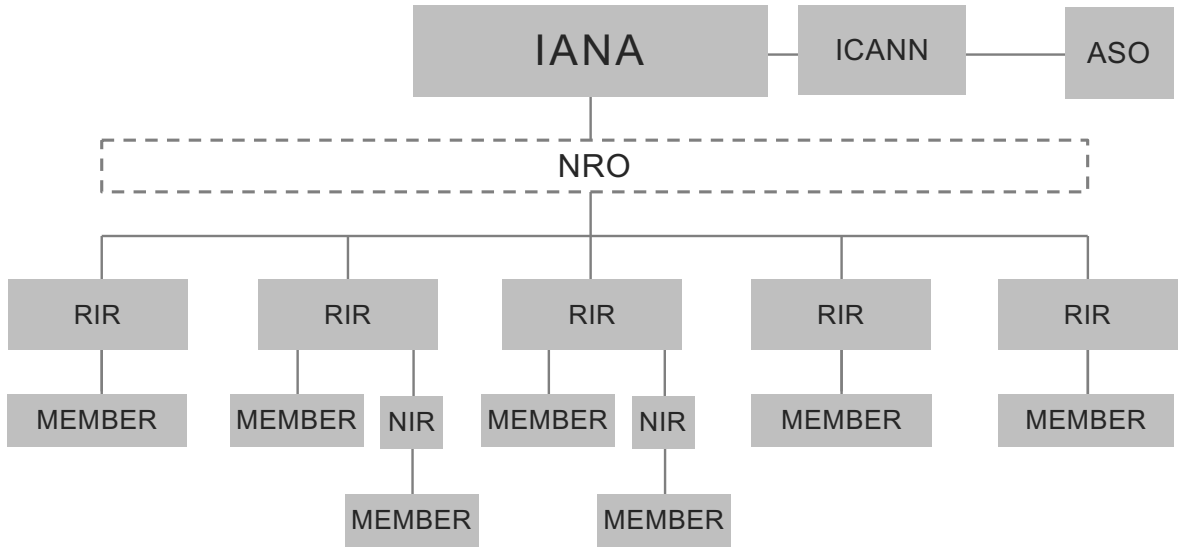
AS0 ROAs Demystified

George Michaelson | Registry Product Manager

ggm@apnic.net

2

Number Resource Management

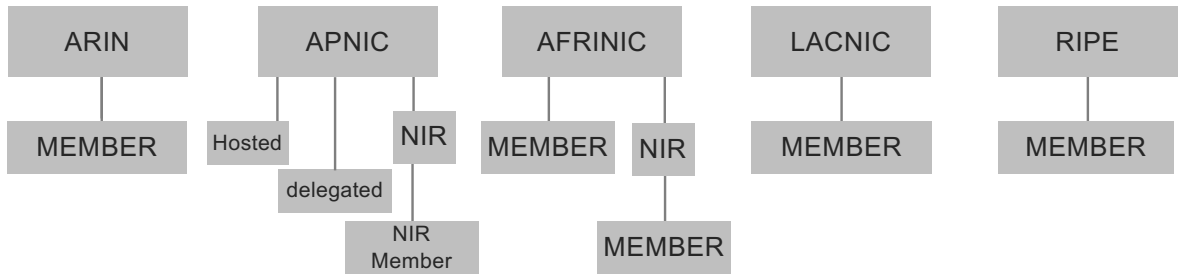


3

RPKI Number Resource Management

The RIR assert their own RPKI, there is no “on top” process.

Each RIR holds a 0/0 certificate and can sign over all resources



4

RPKI Number Resource Management

Validator configuration

ARIN TAL | APNIC TAL | AFRINIC TAL | LACNIC TAL | RIPE TAL

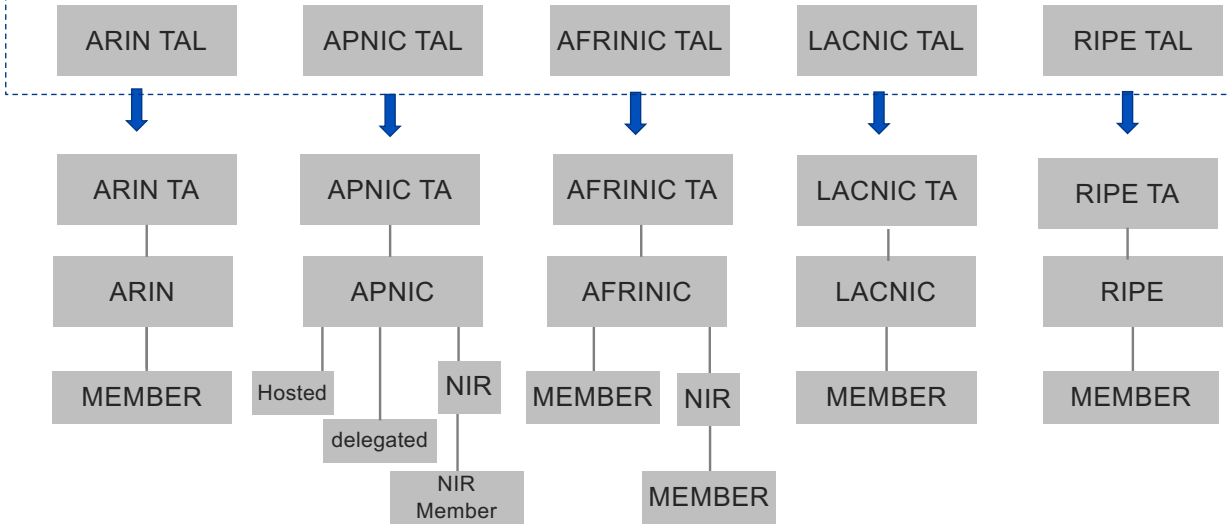
"bootstrap" happens inside validators.
They have "TAL" files which point to the Trust Anchors (TA) you want to use
And all subsequent data fetch is defined by the contents of the RPKI Certificates

APNIC

5

RPKI Number Resource Management

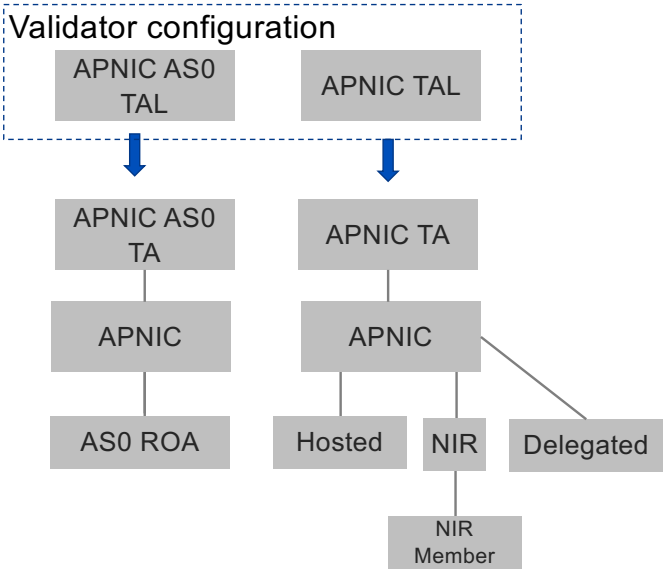
Validator configuration



APNIC

6

APNIC RPKI Number Resource Management

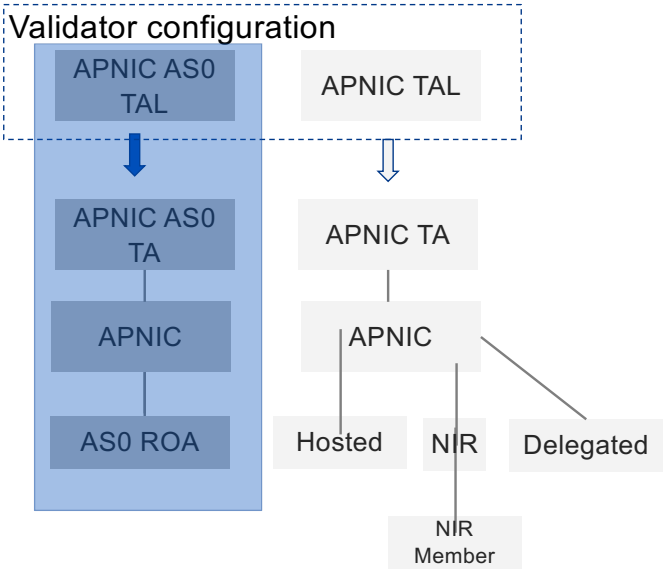


- APNIC runs two independent RPKI systems
- AS0 ROA runs from a fully independent TA
- Unlike mainline RPKI there is no “hosted” or “NIR”or delegated component
- It’s only visible end product is a ROA for AS0

APNIC

7

RPKI Number Resource Management



- This is what we’re talking about today, mostly.

APNIC

8

What we're going to try and cover

- What is AS0?
- What is RPKI, and the "TAL" and ROAs? What is SLURM?
- What is an AS0 ROA and how is it made?
- What is the APNIC AS0 RPKI system, and the AS0 "TAL"?
- How does the APNIC AS0 ROA relate to resources overall?
- How does it differ from individual INR holders AS0 ROA?
- How do I use a ROA? How do I use the AS0 ROA from APNIC
- What about the other RIR, or NIR?
- What does the future hold for RPKI and AS0?

9

What is AS0?

10

AS0 by the RFC

- Codified in https://tools.ietf.org/html/rfc7607

> A BGP speaker MUST NOT originate or propagate a route with an AS number of zero in the AS_PATH, AS4_PATH, AGGREGATOR, or AS4_AGGREGATOR attributes.

11

What is RPKI, and the “TAL” and ROAs? What is SLURM?

12

What is RPKI, and the “TAL” and ROAs? What is SLURM?

- RPKI stands for Resource PKI (Public Key Infrastructure)

13

What is RPKI, and the “TAL” and ROAs? What is SLURM?

- RPKI stands for Resource PKI (Public Key Infrastructure)
  - X.509 Certificates in a hierarchy from a “trust anchor” (operated by the RIR)

14

What is RPKI, and the “TAL” and ROAs? What is SLURM?

- RPKI stands for Resource PKI (Public Key Infrastructure)
  - X.509 Certificates in a hierarchy from a “trust anchor” (operated by the RIR)
  - Contains RFC3779 encoded list of Internet Number Resources

15

What is RPKI, and the “TAL” and ROAs? What is SLURM?

- RPKI stands for Resource PKI (Public Key Infrastructure)
  - X.509 Certificates in a hierarchy from a “trust anchor” (operated by the RIR)
  - Contains RFC3779 encoded list of Internet Number Resources
  - Cannot be used for identity, or privacy

16

What is RPKI, and the “TAL” and ROAs? What is SLURM?

- RPKI stands for Resource PKI (Public Key Infrastructure)
  - X.509 Certificates in a hierarchy from a “trust anchor” (operated by the RIR)
  - Contains RFC3779 encoded list of Internet Number Resources
  - Cannot be used for identity, or privacy
  - You are issued a CA certificate: you can make child certificates
    - Including End-Entity and CA certificates
      - End-Entity certificates to sign digital objects
      - CA certificates to sub-delegate RPKI to another system

17

What is RPKI, and the “TAL” and ROAs? What is SLURM?

- RPKI stands for Resource PKI (Public Key Infrastructure)
  - X.509 Certificates, hierarchy from a “trust anchor” (TA) (operated by the RIR)
    - Contains RFC3779 encoded list of Internet Number Resources (INR)
- You are issued a CA certificate: you can make child certificates
  - Including End-Entity and CA certificates
    - End-Entity certificates to sign digital objects
    - CA certificates to sub-delegate RPKI to another system
- PKI Validation is about checking cryptography, checking path to a TA and checking policy conformance
  - RPKI policy is mainly about the INR being properly covered by the parent

18

What is RPKI, and the "TAL" and ROAs? What is SLURM?

- TAL is the Trust Anchor Locator: how to find the TA for your PKI
  - Usually configured into your validator software
  - Can be hand-installed
  - Consists of a path to the TA certificate and its public key signature
- ROA Route Origin Attestation (or Authorisation) a signed object binding BGP Origin-AS to a list of prefixes
  - Relates to the RPSL Route: object in it's intent but has MaxLength
- SLURM: Simplified Local Internet Number Resource Management
  - A structured plaintext file which can be used to filter RPKI validated products
    - Can specify things which must be included and accepted as valid, irrespective of PKI validation

19

SLURM

- A simpler mechanism to specify post-validation states
- Not inherently cryptographically validated: it is not a signed object, it is a local override mechanism you apply to your own validation process
- We could have done this, and it was proposed in RIPE NCC but we determined in policy discussion to go to a fully cryptographically provable system.
- There are IETF sidrops WG drafts discussing secure SLURM transport
  - This is still work in progress. SLURM itself remains assertion, not provable

20

What is an AS0 ROA and how is it made?

21

AS0 as a ROA #1 of 3

- Codified in https://tools.ietf.org/html/rfc6483

4. Disavowal of Routing Origination

A ROA is a positive attestation that a prefix holder has authorized an AS to originate a route for this prefix into the inter-domain routing system. It is possible for a prefix holder to construct an authorization where no valid AS has been granted any such authority to originate a route for an address prefix.
This is achieved by using a ROA where the ROA's subject AS is one that must not be used in any routing context. Specifically, AS 0 is reserved by the IANA such that it may be used to identify non-routed networks [IANA-AS].

A ROA with a subject of AS 0 (AS 0 ROA) is an attestation by the holder of a prefix that the prefix described in the ROA, and any more specific prefix, should not be used in a routing context.

22

AS0 as a ROA #2 of 3

- Codified in https://tools.ietf.org/html/rfc6483

> The route validation procedure, described in Section 2, will provide a "valid" outcome if any ROA matches the address prefix and origin AS, even if other valid ROAs would provide an "invalid" validation outcome if used in isolation.
>
> Consequently, an AS 0 ROA has a lower relative preference than any other ROA that has a routable AS as its subject.
>
> This allows a prefix holder to use an AS 0 ROA to declare a default condition that any route that is equal to or more specific than the prefix to be considered "invalid", while also allowing other concurrently issued ROAs to describe valid origination authorizations for more specific prefixes.

23

AS0 as a ROA #3 of 3

- Codified in https://tools.ietf.org/html/rfc6483

> By convention, an AS 0 ROA should have a maxLength value of 32 for IPv4 addresses and a maxlength value of 128 for IPv6 addresses; although, in terms of route validation, the same outcome would be achieved with any valid maxLength value, or even if the maxLength element were to be omitted from the ROA.
>
> Also by convention, an AS 0 ROA should be the only ROA issued for a given address prefix; although again, this is not a strict requirement.
>
> An AS 0 ROA may coexist with ROAs that have different subject AS values; although in such cases, the presence or lack of presence of the AS 0 ROA does not alter the route's validity state in any way.

24

How is it made?

25

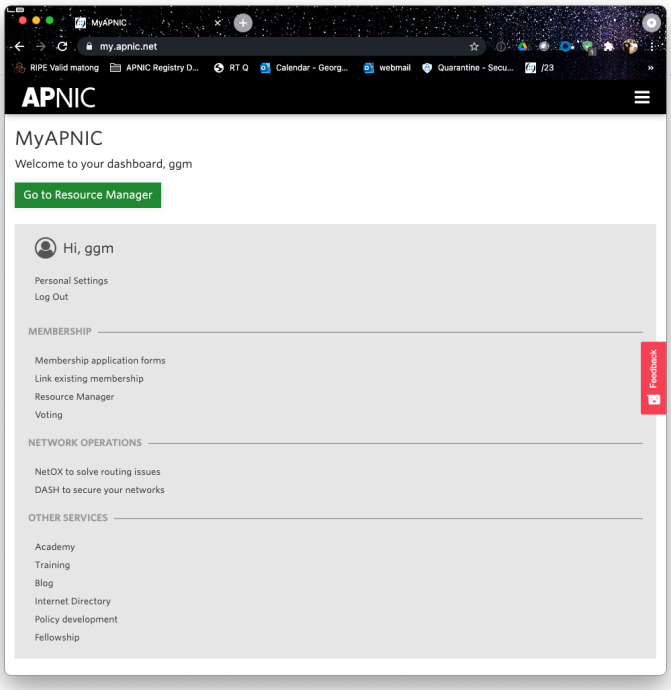
How is it made?

- In MyAPNIC routing management, by selecting AS 0 as the origin-AS when defining a route
- In Krill or an NIR's system, or another RIR, or any other delegated RPKI system depends on how this exposes in the UI

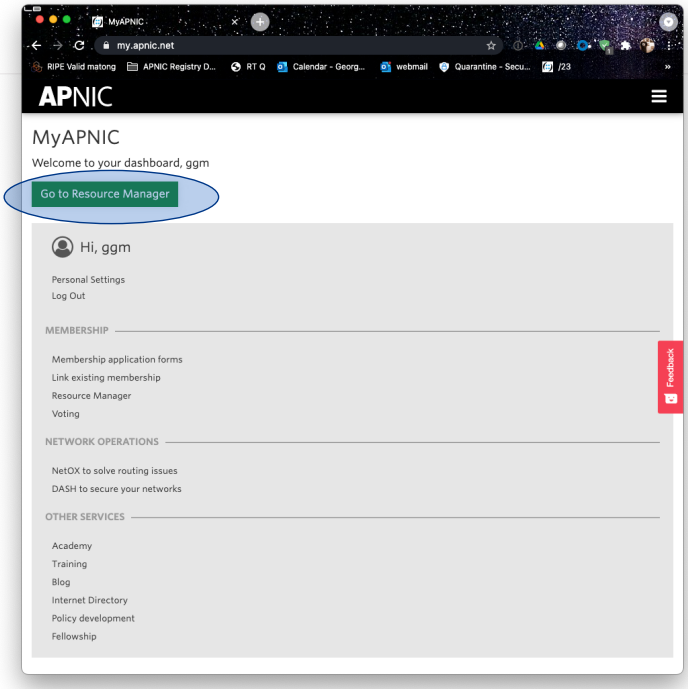
26

Using MyAPNIC for route management

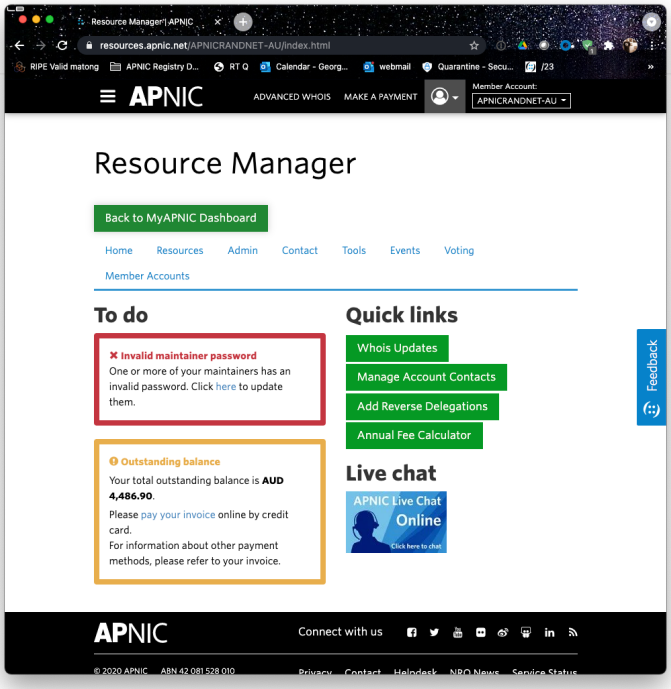
27



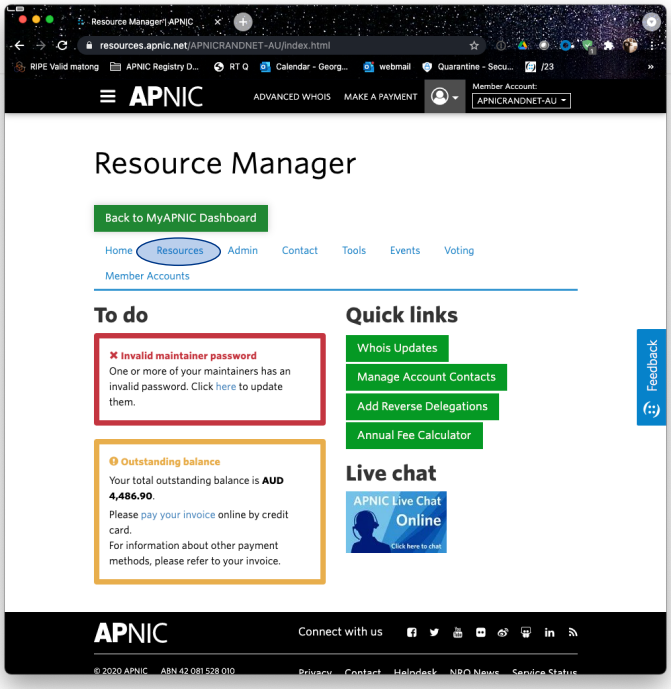
28


MyAPNIC
my.apnic.net
APNIC
MyAPNIC
Welcome to your dashboard, ggm
Go to Resource Manager
Hi, ggm
Personal Settings
Log Out
MEMBERSHIP
Membership application forms
Link existing membership
Resource Manager
Voting
NETWORK OPERATIONS
NetOX to solve routing issues
DASH to secure your networks
OTHER SERVICES
Academy
Training
Blog
Internet Directory
Policy development
Fellowship
Feedback

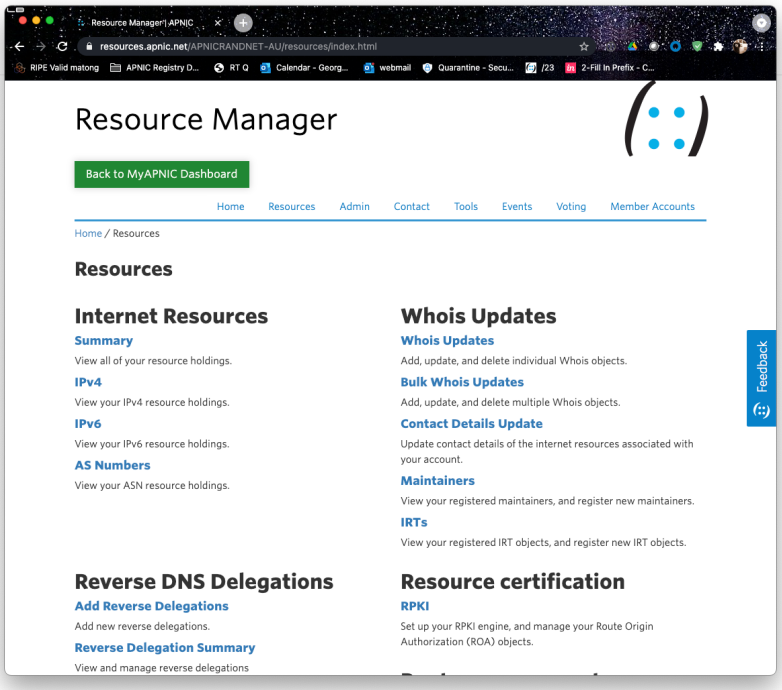
29


Resource Manager | APNIC
resources.apnic.net/APNICRANDNET-AU/index.html
APNIC
ADVANCED WHOIS
MAKE A PAYMENT
Member Account:
APNICRANDNET-AU
Resource Manager
Back to MyAPNIC Dashboard
Home
Resources
Admin
Contact
Tools
Events
Voting
Member Accounts
To do
Invalid maintainer password
One or more of your maintainers has an invalid password. Click here to update them.
Outstanding balance
Your total outstanding balance is AUD 4,486.90.
Please pay your invoice online by credit card.
For information about other payment methods, please refer to your invoice.
Quick links
Whois Updates
Manage Account Contacts
Add Reverse Delegations
Annual Fee Calculator
Live chat
APNIC Live Chat
Online
Feedback
APNIC
Connect with us

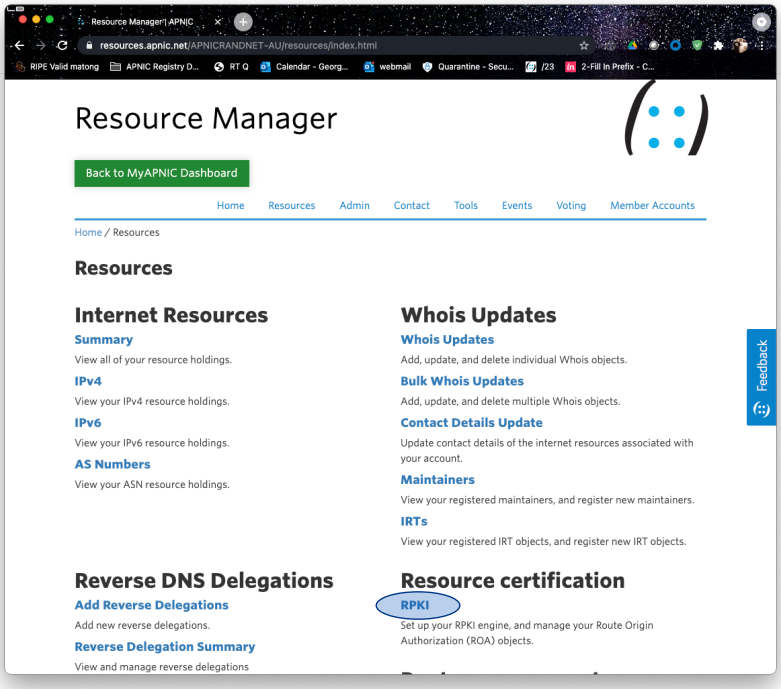
30


Resource Manager | APNIC
resources.apnic.net/APNICRANDNET-AU/index.html
APNIC
ADVANCED WHOIS
MAKE A PAYMENT
Member Account:
APNICRANDNET-AU
Resource Manager
Back to MyAPNIC Dashboard
Home
Resources
Admin
Contact
Tools
Events
Voting
Member Accounts
To do
Invalid maintainer password
One or more of your maintainers has an invalid password. Click here to update them.
Outstanding balance
Your total outstanding balance is AUD 4,486.90.
Please pay your invoice online by credit card.
For information about other payment methods, please refer to your invoice.
Quick links
Whois Updates
Manage Account Contacts
Add Reverse Delegations
Annual Fee Calculator
Live chat
APNIC Live Chat
Online
Click here to chat
Feedback
APNIC
Connect with us
© 2020 APNIC ABN 42 081 528 010
Privacy Contact Helpdesk NRO News Service Status

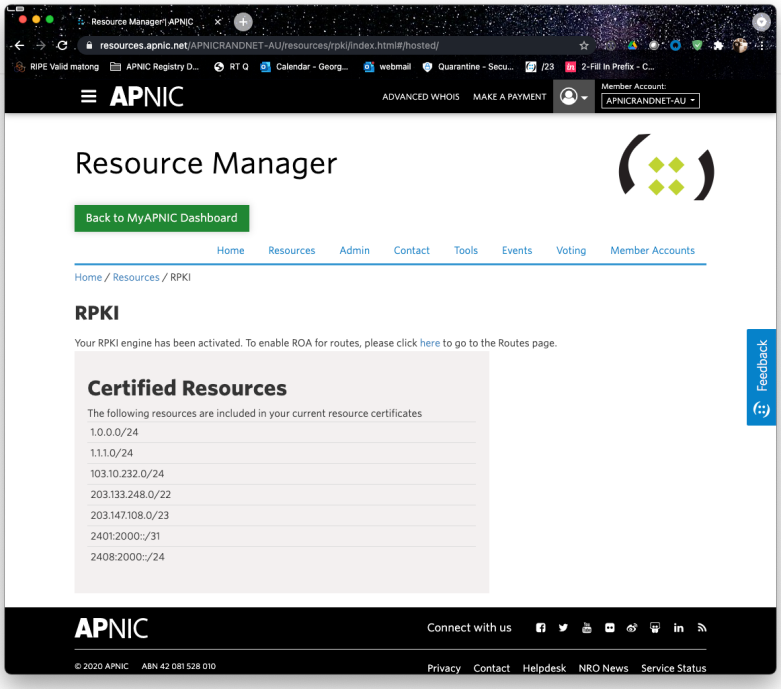
31


Resource Manager | APNIC
resources.apnic.net/APNICRANDNET-AU/resources/index.html
Resource Manager
Back to MyAPNIC Dashboard
Home
Resources
Admin
Contact
Tools
Events
Voting
Member Accounts
Home / Resources
Resources
Internet Resources
Summary
View all of your resource holdings.
IPv4
View your IPv4 resource holdings.
IPv6
View your IPv6 resource holdings.
AS Numbers
View your ASN resource holdings.
Whois Updates
Whois Updates
Add, update, and delete individual Whois objects.
Bulk Whois Updates
Add, update, and delete multiple Whois objects.
Contact Details Update
Update contact details of the internet resources associated with your account.
Maintainers
View your registered maintainers, and register new maintainers.
IRTs
View your registered IRT objects, and register new IRT objects.
Reverse DNS Delegations
Add Reverse Delegations
Add new reverse delegations.
Reverse Delegation Summary
View and manage reverse delegations
Resource certification
RPKI
Set up your RPKI engine, and manage your Route Origin Authorization (ROA) objects.
Feedback

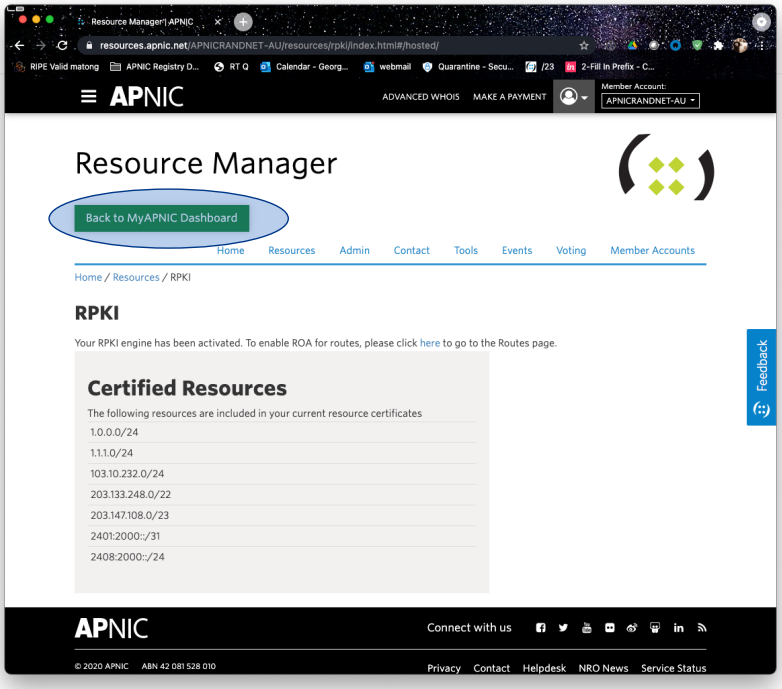
32


Resource Manager
Back to MyAPNIC Dashboard
Home Resources Admin Contact Tools Events Voting Member Accounts
Home / Resources
Resources
Internet Resources
Summary
View all of your resource holdings.
IPv4
View your IPv4 resource holdings.
IPv6
View your IPv6 resource holdings.
AS Numbers
View your ASN resource holdings.
Whois Updates
Whois Updates
Add, update, and delete individual Whois objects.
Bulk Whois Updates
Add, update, and delete multiple Whois objects.
Contact Details Update
Update contact details of the internet resources associated with your account.
Maintainers
View your registered maintainers, and register new maintainers.
IRTs
View your registered IRT objects, and register new IRT objects.
Reverse DNS Delegations
Add Reverse Delegations
Add new reverse delegations.
Reverse Delegation Summary
View and manage reverse delegations
Resource certification
RPKI
Set up your RPKI engine, and manage your Route Origin Authorization (ROA) objects.
Feedback

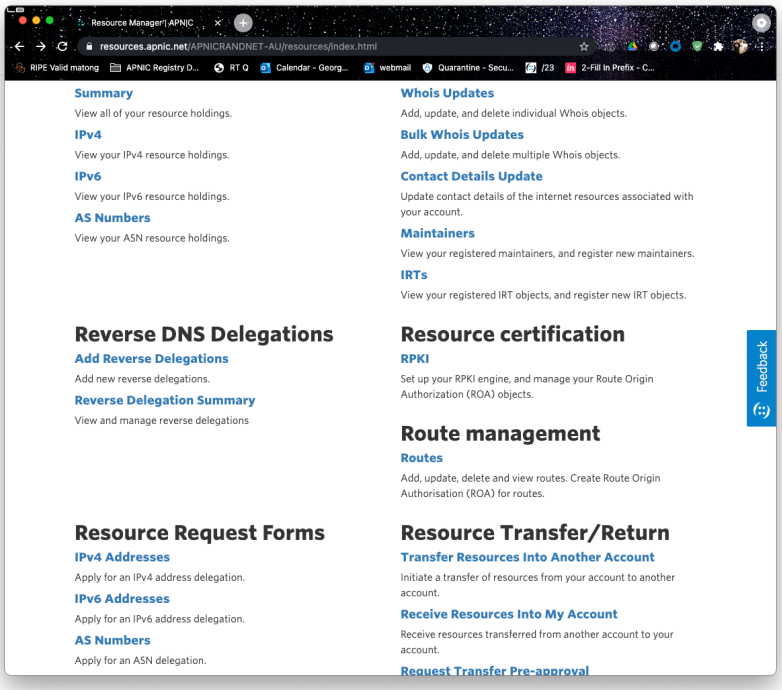
33


APNIC
ADVANCED WHOIS
MAKE A PAYMENT
Member Account:
APNICRANDNET-AU
Resource Manager
Back to MyAPNIC Dashboard
Home Resources Admin Contact Tools Events Voting Member Accounts
Home / Resources / RPKI
RPKI
Your RPKI engine has been activated. To enable ROA for routes, please click here to go to the Routes page.
Certified Resources
The following resources are included in your current resource certificates
1.0.0.0/24
1.1.1.0/24
103.10.232.0/24
203.133.248.0/22
203.147.108.0/23
2401:2000::/31
2408:2000::/24
Feedback
APNIC
Connect with us
© 2020 APNIC ABN 42 081 528 010
Privacy Contact Helpdesk NRO News Service Status

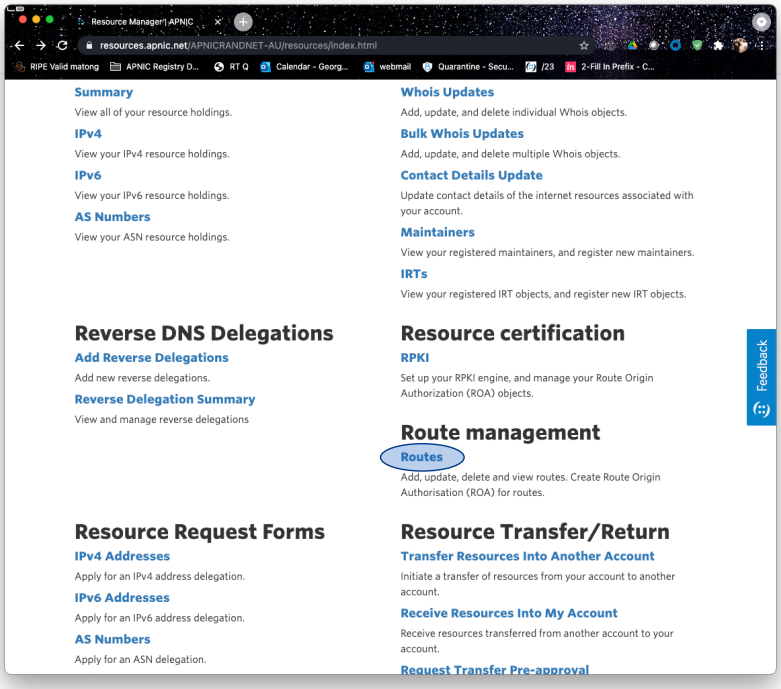
34


Resource Manager | APNIC
resources.apnic.net/APNICRANDNET-AU/resources/rpki/index.html#/hosted/
APNIC
ADVANCED WHOIS
MAKE A PAYMENT
Member Account:
APNICRANDNET-AU
Resource Manager
Back to MyAPNIC Dashboard
Home
Resources
Admin
Contact
Tools
Events
Voting
Member Accounts
Home / Resources / RPKI
RPKI
Your RPKI engine has been activated. To enable ROA for routes, please click here to go to the Routes page.
Certified Resources
The following resources are included in your current resource certificates
1.0.0.0/24
1.1.1.0/24
103.10.232.0/24
203.133.248.0/22
203.147.108.0/23
2401:2000::/31
2408:2000::/24
Feedback
APNIC
Connect with us
© 2020 APNIC ABN 42 081 528 010
Privacy
Contact
Helpdesk
NRO News
Service Status

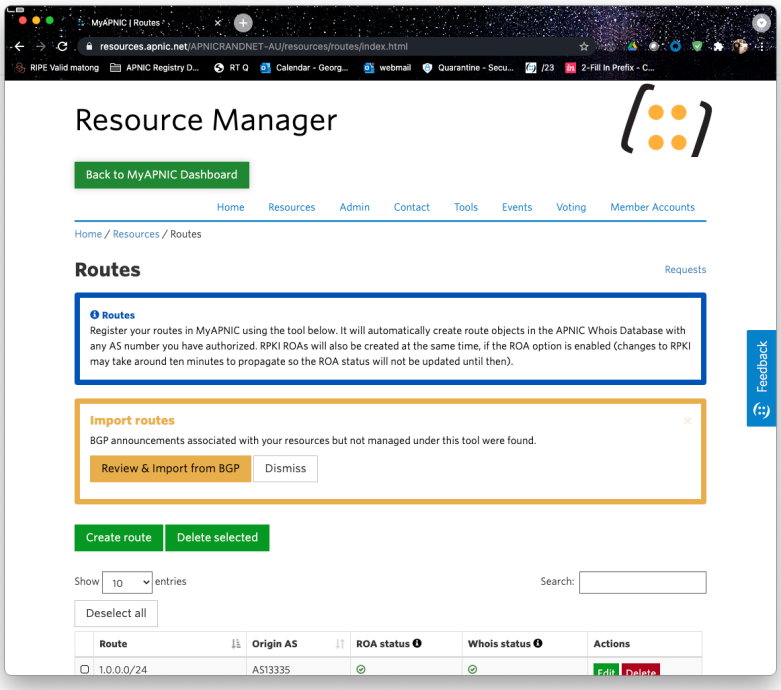
35


Resource Manager | APNIC
resources.apnic.net/APNICRANDNET-AU/resources/index.html
Summary
View all of your resource holdings.
IPv4
View your IPv4 resource holdings.
IPv6
View your IPv6 resource holdings.
AS Numbers
View your ASN resource holdings.
Whois Updates
Add, update, and delete individual Whois objects.
Bulk Whois Updates
Add, update, and delete multiple Whois objects.
Contact Details Update
Update contact details of the internet resources associated with your account.
Maintainers
View your registered maintainers, and register new maintainers.
IRTs
View your registered IRT objects, and register new IRT objects.
Reverse DNS Delegations
Add Reverse Delegations
Add new reverse delegations.
Reverse Delegation Summary
View and manage reverse delegations
Resource certification
RPKI
Set up your RPKI engine, and manage your Route Origin Authorization (ROA) objects.
Route management
Routes
Add, update, delete and view routes. Create Route Origin Authorisation (ROA) for routes.
Resource Request Forms
IPv4 Addresses
Apply for an IPv4 address delegation.
IPv6 Addresses
Apply for an IPv6 address delegation.
AS Numbers
Apply for an ASN delegation.
Resource Transfer/Return
Transfer Resources Into Another Account
Initiate a transfer of resources from your account to another account.
Receive Resources Into My Account
Receive resources transferred from another account to your account.
Request Transfer Pre-approval
Feedback

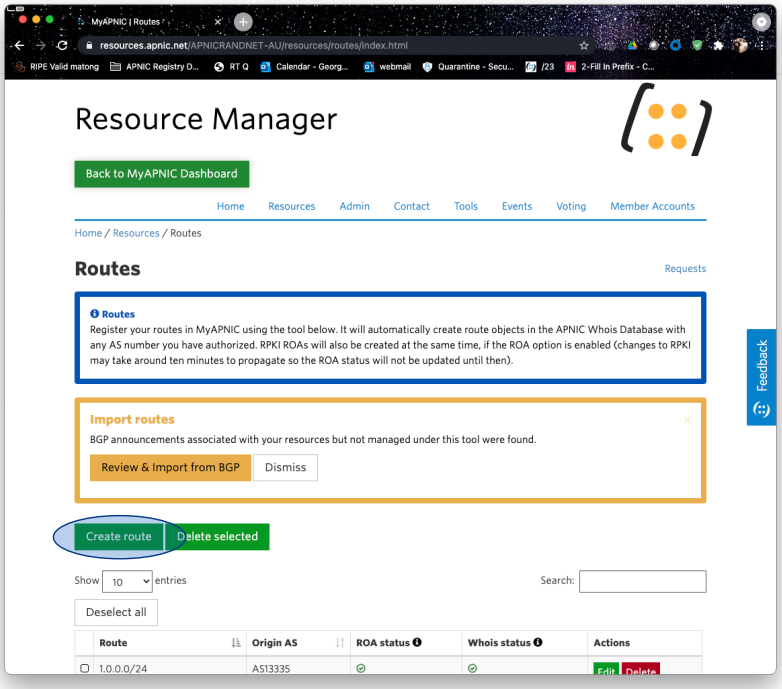
36


Resource Manager | APNIC
resources.apnic.net/APNICRANDNET-AU/resources/index.html
Summary
View all of your resource holdings.
IPv4
View your IPv4 resource holdings.
IPv6
View your IPv6 resource holdings.
AS Numbers
View your ASN resource holdings.
Whois Updates
Add, update, and delete individual Whois objects.
Bulk Whois Updates
Add, update, and delete multiple Whois objects.
Contact Details Update
Update contact details of the internet resources associated with your account.
Maintainers
View your registered maintainers, and register new maintainers.
IRTs
View your registered IRT objects, and register new IRT objects.
Reverse DNS Delegations
Add Reverse Delegations
Add new reverse delegations.
Reverse Delegation Summary
View and manage reverse delegations
Resource certification
RPKI
Set up your RPKI engine, and manage your Route Origin Authorization (ROA) objects.
Route management
Routes
Add, update, delete and view routes. Create Route Origin Authorisation (ROA) for routes.
Resource Request Forms
IPv4 Addresses
Apply for an IPv4 address delegation.
IPv6 Addresses
Apply for an IPv6 address delegation.
AS Numbers
Apply for an ASN delegation.
Resource Transfer/Return
Transfer Resources Into Another Account
Initiate a transfer of resources from your account to another account.
Receive Resources Into My Account
Receive resources transferred from another account to your account.
Request Transfer Pre-approval
Feedback

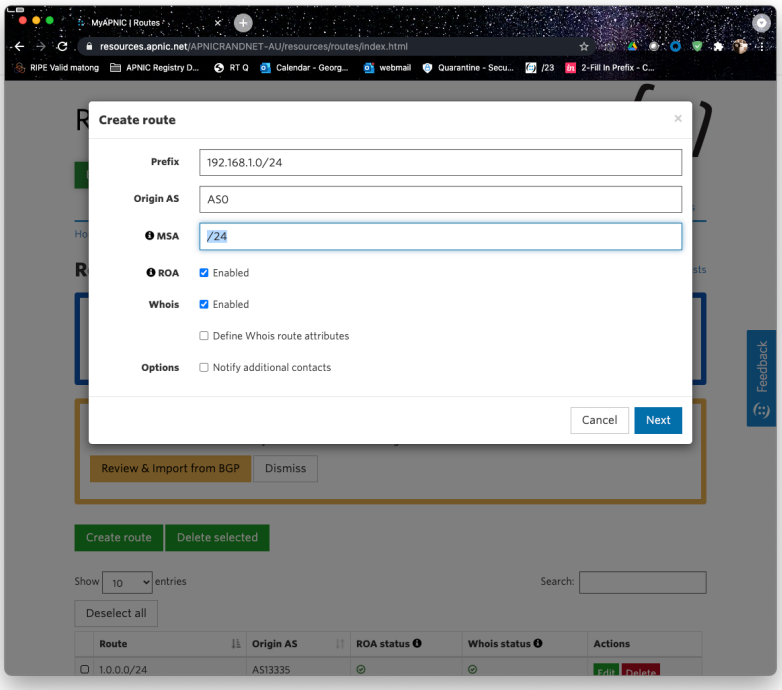
37


MyAPNIC | Routes
resources.apnic.net/APNICRANDNET-AU/resources/routes/index.html
Resource Manager
Back to MyAPNIC Dashboard
Home Resources Admin Contact Tools Events Voting Member Accounts
Home / Resources / Routes
Routes
Requests
Routes
Register your routes in MyAPNIC using the tool below. It will automatically create route objects in the APNIC Whois Database with any AS number you have authorized. RPKI ROAs will also be created at the same time, if the ROA option is enabled (changes to RPKI may take around ten minutes to propagate so the ROA status will not be updated until then).
Import routes
BGP announcements associated with your resources but not managed under this tool were found.
Review & Import from BGP
Dismiss
Create route
Delete selected
Show 10 entries
Search:
Deselect all
Route
Origin AS
ROA status
Whois status
Actions
1.0.0.0/24
AS13335
Edit
Delete
Feedback

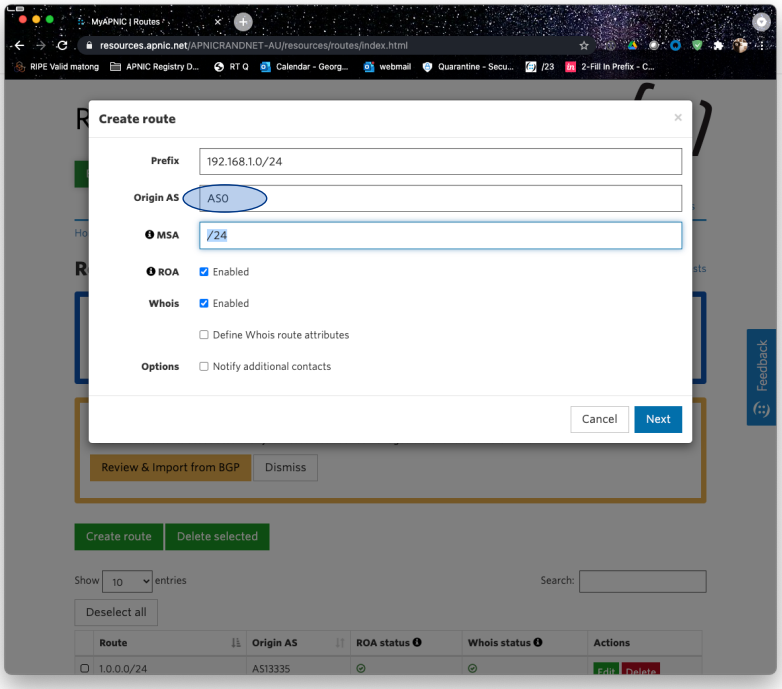
38


MyAPNIC | Routes
resources.apnic.net/APNICRANDNET-AU/resources/routes/index.html
Resource Manager
Back to MyAPNIC Dashboard
Home Resources Admin Contact Tools Events Voting Member Accounts
Home / Resources / Routes
Routes
Requests
Routes
Register your routes in MyAPNIC using the tool below. It will automatically create route objects in the APNIC Whois Database with any AS number you have authorized. RPKI ROAs will also be created at the same time, if the ROA option is enabled (changes to RPKI may take around ten minutes to propagate so the ROA status will not be updated until then).
Import routes
BGP announcements associated with your resources but not managed under this tool were found.
Review & Import from BGP
Dismiss
Create route
Delete selected
Show 10 entries
Search:
Deselect all
Route
Origin AS
ROA status
Whois status
Actions
1.0.0.0/24
AS13335
Feedback

39


MyAPNIC | Routes
resources.apnic.net/APNICRANDNET-AU/resources/routes/index.html
Create route
Prefix
192.168.1.0/24
Origin AS
AS0
MSA
/24
ROA
Enabled
Whois
Enabled
Define Whois route attributes
Options
Notify additional contacts
Cancel
Next
Review & Import from BGP
Dismiss
Create route
Delete selected
Show 10 entries
Search:
Deselect all
Route
Origin AS
ROA status
Whois status
Actions
1.0.0.0/24
AS13335
Feedback

40



41

Some examples of AS0 ROA

42

AS0 ROA made by delegates

- An address holder can use an AS0 ROA to do two things

1. "Disavow" a prefix they have no intention of asserting into BGP
   - Publish the AS0 ROA for the prefix. Do not publish any other ROA

2. "turn on" RPKI for a range of resources and selectively announce specific prefixes
   - Publish the AS0 ROA for the covering prefix
   - Publish the more specific (or even identical) prefixes with valid origin-AS
   - Longest match, and "AS0-ROA has lowest priority" combine.

43

An example

- DC-IX. Hold address under RIPE NCC
  - None of these IX prefixes should be routed, they're for use in the IX only

ROA Version: 0
SigningTime: 2021-02-22T15:04:06Z
asID: 0

addressFamily: 1
- IPAddress: 185.1.48.0/24
- IPAddress: 185.1.47.0/24
- IPAddress: 185.1.46.0/24
- IPAddress: 185.1.192.0/23
- IPAddress: 80.81.192.0/21
- IPAddress: 185.1.197.0/24
- IPAddress: 80.81.203.0/24
- IPAddress: 80.81.202.0/24
- IPAddress: 185.1.8.0/24
- IPAddress: 185.1.119.0/24
- IPAddress: 185.1.131.0/24
- IPAddress: 185.1.170.0/23

addressFamily: 2
- IPAddress: 2001:7f8:44::/48
- IPAddress: 2001:7f8:3f::/48
- IPAddress: 2001:7f8:10a::/48
- IPAddress: 2001:7f8:d5::/48
- IPAddress: 2001:7f8:73::/48
- IPAddress: 2001:7f8:9e::/48
- IPAddress: 2001:7f8:32::/48
- IPAddress: 2001:7f8:3d::/48
- IPAddress: 2001:7f8::/48
- IPAddress: 2001:7f8:a0::/48
- IPAddress: 2001:7f8:106::/48
- IPAddress: 2001:7f8:36::/48

44

An example

- DC-IX. Hold address under RIPE NCC
  - None of these IX prefixes should be routed, they're for use in the IX only

ROA Version: 0
SigningTime: 2021-02-22T15:04:06Z
asID: 0

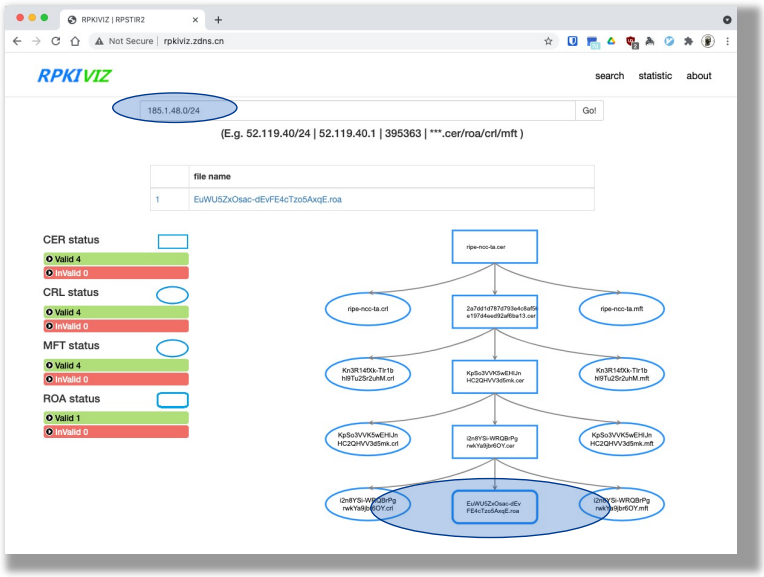
addressFamily: 1
- IPAddress: 185.1.48.0/24
- IPAddress: 185.1.47.0/24
- IPAddress: 185.1.46.0/24
- IPAddress: 185.1.192.0/23
- IPAddress: 80.81.192.0/21
- IPAddress: 185.1.197.0/24
- IPAddress: 80.81.203.0/24
- IPAddress: 80.81.202.0/24
- IPAddress: 185.1.8.0/24
- IPAddress: 185.1.119.0/24
- IPAddress: 185.1.131.0/24
- IPAddress: 185.1.170.0/23

addressFamily: 2
- IPAddress: 2001:7f8:44::/48
- IPAddress: 2001:7f8:3f::/48
- IPAddress: 2001:7f8:10a::/48
- IPAddress: 2001:7f8:d5::/48
- IPAddress: 2001:7f8:73::/48
- IPAddress: 2001:7f8:9e::/48
- IPAddress: 2001:7f8:32::/48
- IPAddress: 2001:7f8:3d::/48
- IPAddress: 2001:7f8::/48
- IPAddress: 2001:7f8:a0::/48
- IPAddress: 2001:7f8:106::/48
- IPAddress: 2001:7f8:36::/48

45

rpkiviz.zdns.cn

- Declaration is made by the delegate
- Diagnostic validator shows it's position in the hierarchy
- Its down below the Registry level, signed by the Delegate



46

Another example

- Deutsche Telekom AG. Hold address under RIPE NCC
  - We don't want these prefices visible unless a ROA signed by us exists. Here's the ROA permitting AS3320 to originate.

ROA Version: 0
SigningTime: 2021-01-01T01:01:13Z
asID: 3320
addressFamily: 1
IPAddress: 80.144.0.0/13
IPAddress: 80.156.0.0/16
IPAddress: 62.156.0.0/14
IPAddress: 217.224.0.0/11
IPAddress: 80.128.0.0/11
IPAddress: 217.80.0.0/12
IPAddress: 46.80.0.0/12
IPAddress: 193.158.0.0/15
IPAddress: 62.153.0.0/16
IPAddress: 194.25.0.0/16
IPAddress: 217.0.0.0/13
IPAddress: 80.157.8.0/21
IPAddress: 80.157.0.0/16
IPAddress: 93.192.0.0/10
IPAddress: 84.128.0.0/10
IPAddress: 87.128.0.0/10
IPAddress: 79.192.0.0/10
IPAddress: 91.0.0.0/10
IPAddress: 62.224.0.0/14
IPAddress: 195.145.0.0/16
IPAddress: 62.154.0.0/15
IPAddress: 80.128.0.0/12
IPAddress: 80.157.16.0/20
IPAddress: 212.184.0.0/15
IPAddress: 195.243.0.0/16
IPAddress: 80.152.0.0/14
addressFamily: 2
IPAddress: 2003:3c0::/28
IPAddress: 2003:3e0::/28
IPAddress: 2003::/23
IPAddress: 2003::/19

This is the ROA for valid Origin: 3320

47

Another example

- Deutsche Telekom AG. Hold address under RIPE NCC
  - We don't want these prefices visible unless a ROA signed by us exists
  - (one of the prefixes is a superblock, a /11 over the /12 they do announce)

ROA Version: 0
SigningTime: 2021-01-01T01:01:11Z
asID: 0
addressFamily: 1
IPAddress: 80.128.0.0/11

This is the AS 0 ROA for one of the prefices in the main ROA

48

What is the APNIC AS0 RPKI system, and the AS0 “TAL”?

49

What is the APNIC AS0 RPKI system, and the AS0 “TAL”?

- The APNIC AS0 RPKI system is a fully independent RPKI “engine” operating under a distinct Trust Anchor
- This is why the AS0 TAL exists: it is kept outside of the Main RPKI TAL so there is no confusion between the products
- By operating as a distinct TAL, we turned AS0 service from “opt out” into “opt in”
  - If we had constructed this service “under” the main RPKI TAL then all BGP speakers would have been affected as soon as we started issuing AS0 ROA
- The system uses an independent codebase from the main RPKI
  - Its hosted in VMs and in Kubernetes, and uses APNIC code, and Krill (NLNet labs)

50

What is the APNIC AS0 RPKI system, and the AS0 “TAL”?

- The APNIC AS0 system is a stand-alone RPKI system, with its own TAL
  - It is not part of the main APNIC RPKI system. It validates independently
  - It operates under a different policy and process
- Stand-Alone to make sure it was not accidentally applied to BGP validation
  - You need to deliberately, consciously include the AS0 TAL in your validation software systems to see its products and to be affected by them

51

How does the APNIC AS0 ROA relate to resources overall?

52

How does the APNIC AS0 ROA relate to resources overall?

- APNIC AS0 ROA only ever contains resources which are available or reserved
  - By definition, no resources which APNIC has delegated to anyone should continue to be on the AS0 ROA
- APNIC AS0 ROA only ever contains resources APNIC can show are managed by APNIC
  - We use the delegated statistics file as a configuration input to list the operational resources we have authority over, in the production CA systems below the TAL in both AS0 and in the Main RPKI system

53

How does it differ from individual INR holders AS0 ROA?

- An INR holder, or Delegate can elect to make any ROA they like (any Origin-AS, and combination of resources they have authority over)
- These AS0 ROA are made visible to anyone who has the APNIC RPKI TAL configured in their RPKI Validator
  - They are expected to apply to BGP filtering as soon as published
- They exist solely at the discretion and decision of the INR Delegate
- They cannot refer to any INR the publisher does not have authority over
  - They cannot refer to undelegated or reserved or available addresses

54

What should you do with these AS0 ROA?

- AS0 ROA made by delegates are assertions made directly by a delegate. They go to the primary defined role of an AS0 ROA in the RFC
- You should use these to determine acceptability of routes you see for these prefices.
  - If there is not a valid ROA over the prefix you see being announced, you should reject the prefix

55

How do I use a ROA? How do I use the AS0 ROA from APNIC

- You use a ROA by operating a validator as a relying-party
  - This produces a set of Validated ROA Payload (VRP)
    - A list of prefix and Origin-AS
  - You can use the VRP to filter BGP messages
    - Typically, by operating RPKI-RTR to process BGP updates, and define them as one of three states:
      1. Valid
      2. Invalid
      3. Unknown
- We recommend the APNIC AS0 ROA only be used for diagnostics and alerting.

56

The APNIC AS0 Policy

- https://www.apnic.net/community/policy/resources#5.1.4.

5.1.4. Preventing the Use of Undelegated APNIC Address Space

- Undelegated APNIC Address Space (IPv4 or IPv6) should not be publicly advertised by any Autonomous System. To prevent its use, APNIC will create RPKI ROAs with origin AS0 (AS zero) for all undelegated address space (marked as "Available" and "Reserved" in the delegated-apnic-extended-latest stats file) for which it is the current administrator.

- While any current resource holder can create AS0 ROA for the resources they have under their account administration, only APNIC has the authority to create AS0 ROAs for APNIC address space not yet delegated to an organization. When APNIC delegates address space to an organization, APNIC will remove the prefix from the AS0 ROA.

57

AS0 ROA made in the Registry

- APNIC does not assert a valid route for any resources except those delegated to the Secretariat for its own use, or for declared experiments (eg final /8 checks on tainted blocks)
  - All undelegated, reserved, withheld, terminated and as-yet unissued resources are not routed
- APNIC has been directed by. Prop132 to publish an AS0 ROA for undelegated and unassigned resources
  - Since we do not assert any valid origin-AS in BGP, the AS0 ROA we publish has the effect of "repudiating" these routes from existing in the default-free zone

58

How APNIC manages the AS0 ROA

- "fast to remove"
  - Within 5 minutes of a Delegation being made, APNIC removes the prefix from the AS0 ROA (it re-publishes the ROA without the prefix)
- "slow to add"
  - Resources marked as undelegated are added to the AS0 ROA in a cron job and there is no urgency.
- Outcome:
  - Newly delegated or re-delegated resources will NOT be on the current AS0 as quickly as possible
  - Newly reclaimed, undelegated resources appear on the AS0 ROA in a slower process.

59

Why we run a separate TAL for AS0 ROA

- By default, the Main RPKI TAL is included in all relying party validator code, and is recommended for use in RPKI-RTR
  - Objects created in this RPKI will apply to BGP as quickly as they propagate to the people who use Route Origin Validation.
- By default, the AS0 RPKI TAL is recommended NOT to be used for RPK-RTR, but to be operated as a diagnostic/advisory service only
  - We do not recommend the AS0 ROA we maintain be applied to BGP directly
- In effect, using a separate TAL turns this service into an 'opt-in' process
  - by default, no BGP speaker will be affected by changes in the APNIC AS0 ROA
- See https://www.apnic.net/community/security/resource-certification/apnic-limitations-of-liability-for-rpki-2/

60

What should you do with these AS0 ROA?

- These are assertions made directly by a Registry.
- We specifically do NOT recommend they are used to directly filter BGP, or calculate validity in your routing
- But, we do suggest they are used as a live diagnostic.

- Example 1: run BGPAlerter
  - Configure a prefix list based on a VRP state from the AS0 TAL
- Example 2: run a stub BGP peer “inside”, which can be used for diagnostic
  - Configure RPKI-RTR from a VRP state which uses the AS0 TAL, log invalids

61

Configuring BGPAlerter to read a ROA feed

```
rpki:
    vrpProvider: external
    vrpFile: /path/to/vrp.json
    preCacheROAs: true,
    refreshVrpListMinutes: 15
```

- This configures your BGPAlerter to read a VRP file off-disk
- Run any validator which produces a json VRP file, with the AS0 TAL

62

Or.. Take a bogons feed model?

- (from Tashi's slidepack on bogons and AS0)

63

Bogon Route Server Project

- In comes the Bogon Route Server project by Team Cymru
  - Provides dynamic bogons information using eBGP multihop sessions
  - Traditional bogons (AS65333)
    - martians plus prefixes not allocated by IANA
  - Full-bogons (AS65332)
    - above plus prefixes allocated to RIRs but not yet assigned to ISPs/end-users by RIRs
- For details:
  - http://www.team-cymru.org/bogon-reference-bgp.html

64

AS0 in ROV

- Would help tag any incoming routes (from peers, transit, customers) within the undelegated (bogon) space as Invalid
  - mismatch of origin AS
- Based on the tag, you can:
  - Use it to filter out (drop) those routes, or
  - Compare the tagged routes with the full feed from a Bogon

65

You could internalize this

- Run a validator with AS0 TAL and compute the VRP set for AS0
- Run a stub AS in private space, with RPKI-RTR feed
  - Configure this to receive the AS0 TAL
  - Report visible AS0 ROA deprecated prefixes
  - Do not connect this to your public BGP, but use this to instrument and report'
- Run another validator with the main RPKI TAL set, without AS0 and use this to supply RPKI-RTR VRP to your BGP

66

Could APNIC publish AS0 over delegated resources?

67

Could APNIC publish AS0 over delegated resources?

- The APNIC AS0 TAL covers “0/0” so yes, theoretically we could
  - The Operational system uses a certificate to issue the ROA which (as for main RPKI) explicitly lists the ranges we have authority over, so the qualification is “not resources which we cannot show are properly delegated to APNIC to manage”
  - The Operational system is designed to ONLY publish AS0 for resources which are publicly declared as ‘available’ or ‘reserved’ in line with address policy
    - The code we operate, does not permit us to make an AS0 TAL over other resources
- We could (in theory) but we declare that we don’t and we have no intention of changing our operational model to enable this

68

What if APNIC AS0 ROA does repudiate my resources?

69

What if APNIC AS0 ROA does repudiate my resources?

- Firstly, an AS0 ROA is “lower priority” in BGP ROV than any other ROA
  - Simply make a ROA for your valid ORIGIN-AS and all ROV calculating systems will no longer be blocked: You have control over your own RPKI state at all times
- Secondly, the AS0 ROA TAL is explicitly marked as “do not include in BGP” by APNIC
  - We recommend ROV calculation NOT automatically apply AS0 repudations to BGP
- Contact APNIC noc or helpdesk IMMEDIATELY if you see any problems
  - We’re checking our systems state 24/7, but please alert us to problems you see in APNIC services

70

What about the other RIR, or NIR?

71

What about the other RIR, or NIR?

- RIPE explicitly rejected operation of an AS0 system in the routing-wg
- AfriNIC are still considering the option in policy process
- ARIN have no active policy discussion or proposal
- LacNIC accepted an AS0 policy but have yet to deploy a service

- APNIC NIR are explicitly covered by address policy, but all NIR holdings are considered “delegated” and so we will not be making AS0 ROA over un-used NIR delegations
  - The NIR might elect to do this, or ask us to do this. But not at this time.

72

What does the future hold for RPKI and AS0?

73

What does the future hold for RPKI and AS0?

- RPKI uptake worldwide is on the increase
  - For growth information in the number of active RPKI creators worldwide:
    - https://www.nro.net/about/rirs/statistics/ % coverage of address space
    - https://stats.labs.apnic.net/rpki/ % ROV by economy, ASN
  - For specific status of prefixes, ASN
    - https://bgp.he.net "key" symbol indicates RPKI status
    - https://rpkiviz.zdns.cn RPKI tree visualiser
    - https://jdr.nlnetlabs.nl/ RPKI tree visualiser
- AS0 is being maintained and operated 24/7 by APNIC
  - Reports on usage delivered to APNIC meeting routing security SIG

74

Summary: APNIC AS0 is only for undelegated

- APNIC AS0 ROA is only for undelegated, reserved resources
- APNIC does not use AS0 as a “turn it off” control for delegated resources
- APNIC does not include AS0 ROA in the main RPKI system which directly drives BGP ROV
- APNIC recommends AS0 ROA be used as a diagnostic or advisory service only
- If you believe an incorrect AS0 ROA exists over your prefixes, issue a ROA for the origin-AS you wish to assert: it has higher priority
- Tell APNIC about any problems with APNIC services
  - noc@apnic.net or helpdesk@apnic.net

75

QUESTIONS?

76

Thank You!

77