Internet Routing Registry (IRR)

APNIC Tutorial in APNIC35

February 27, 2013, Singapore.

APNIC

Introduction

- Presenter

Nurul Islam Roman
Senior Training Specialist
nurul@apnic.net

Specialties:
Routing & Switching
MPLS, IPv6
DNS/DNSSEC
Internet Resource Management
Network Security

What is a Routing Registry?

- A repository (database) of Internet routing policy information
  - Autonomous Systems exchanges routing information via BGP
  - Exterior routing decisions are based on policy based rules
  - However BGP does not provides a mechanism to publish/ communicate the policies themselves
  - RR provides this functionality
- Routing policy information is expressed in a series of objects

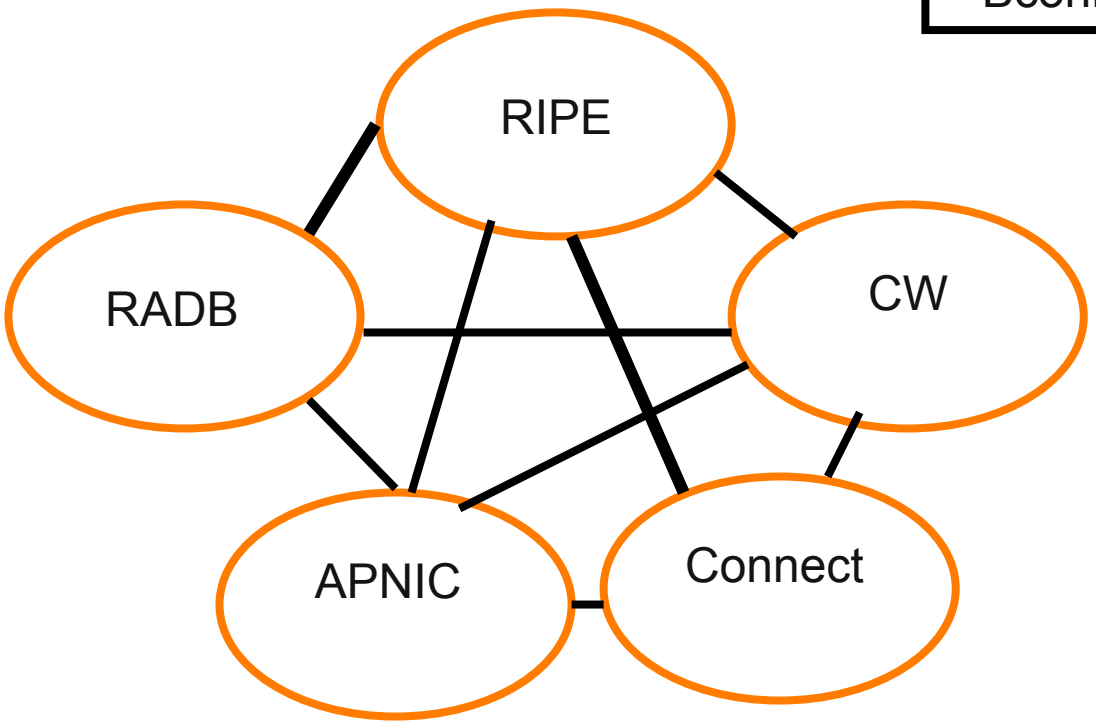
What is a Routing Registry?

- Global Internet Routing Registry database
  - http://www.irr.net/
    - Uses RPSL
- Stability and consistency of routing
  - network operators share information

- Both public and private databases
  - These databases are independent
    - but some exchange data
    - only register your data in one database

What is a Routing Registry?

ARIN, ArcStar, FGC, Verio,
Bconnex, Optus, Telstra, ...



IRR = APNIC RR + RIPE DB + RADB + C&W + ARIN + …

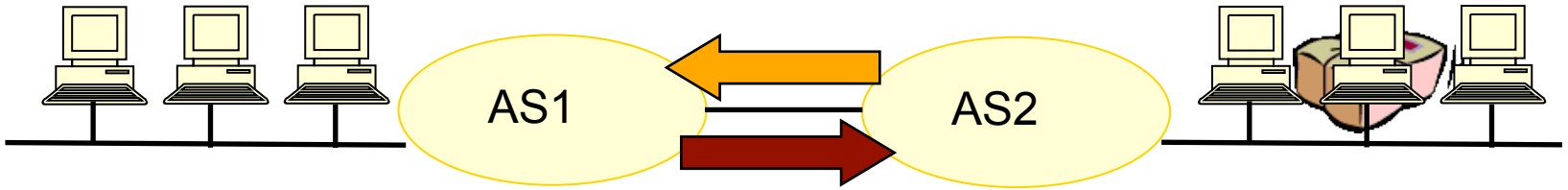
Routing Registry Objects

- Route, aut-num, inet-rtr, peering-set, AS-set, rtr-set, filter-set
  - Each object has its own purpose
  - Together express routing policies
- More details covered later

What is Routing Policy?

- Description of the routing relationship between autonomous systems
  - Who are my BGP peers?
    - Customer, peers, upstream
  - What routes are:
    - Originated by each neighbour?
    - Imported from each neighbour?
    - Exported to each neighbour?
    - Preferred when multiple routes exist?
  - What to do if no route exists?
  - What routes to aggregate?

Representation of Routing Policy



NET1 NET2

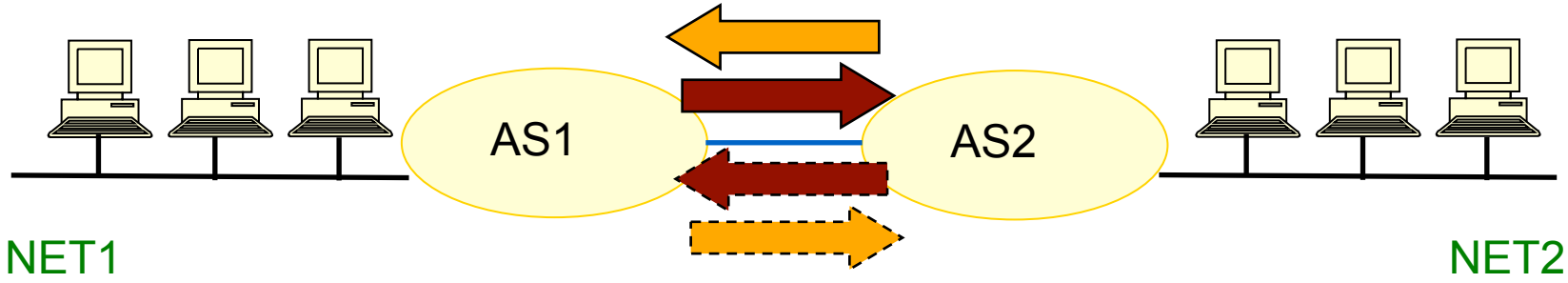
In order for traffic to flow from NET2 to NET1 between AS1 and AS2:

AS1 has to announce NET1 to AS2 via BGP

And AS2 has to accept this information and use it

Resulting in packet flow from NET2 to NET1

Representation of Routing Policy (cont.)



In order for traffic to flow towards from NET1 to NET2:

AS2 must announce NET2 to AS1

And AS1 has to accept this information and use it

Resulting in packet flow from NET 1 to NET2

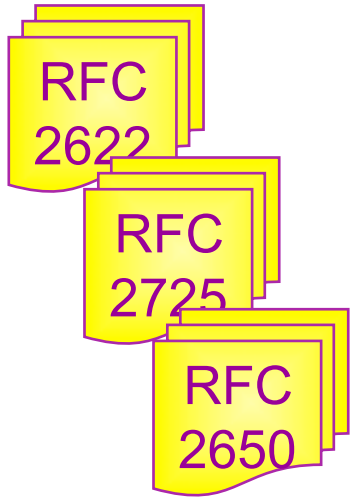
RPSL

- Routing Policy Specification Language
  - Object oriented language
    - Based on RIPE-181
  - Structured whois objects

- Higher level of abstraction than access lists

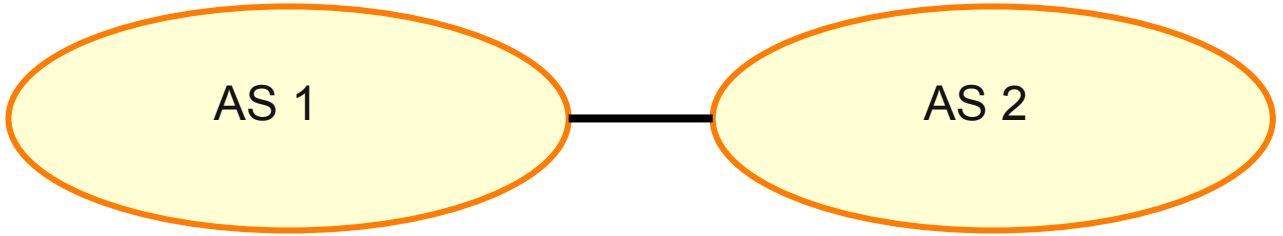
- Describes things interesting to routing policy:
  - Routes, AS Numbers …
  - Relationships between BGP peers
  - Management responsibility

- Relevant RFCs
  - Routing Policy Specification Language
  - Routing Policy System Security
  - Using RPSL in Practice



Routing Policy - Examples

Basic concept

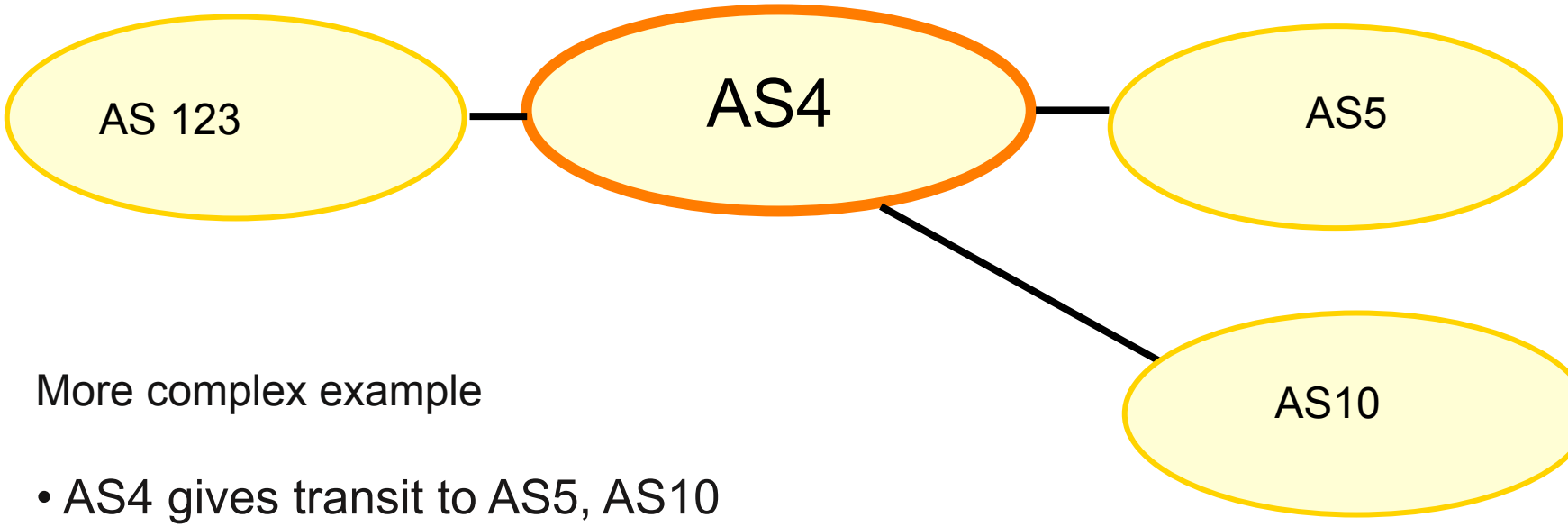


"action pref" - the lower the value, the preferred the route

```
aut-num: AS1
…
import:   from AS2
          action pref= 100;
          accept AS2
export:   to AS2 announce AS1
```

```
aut-num: AS2
…
import:   from AS1
          action pref=100;
          accept AS1
export:   to AS1 announce AS2
```

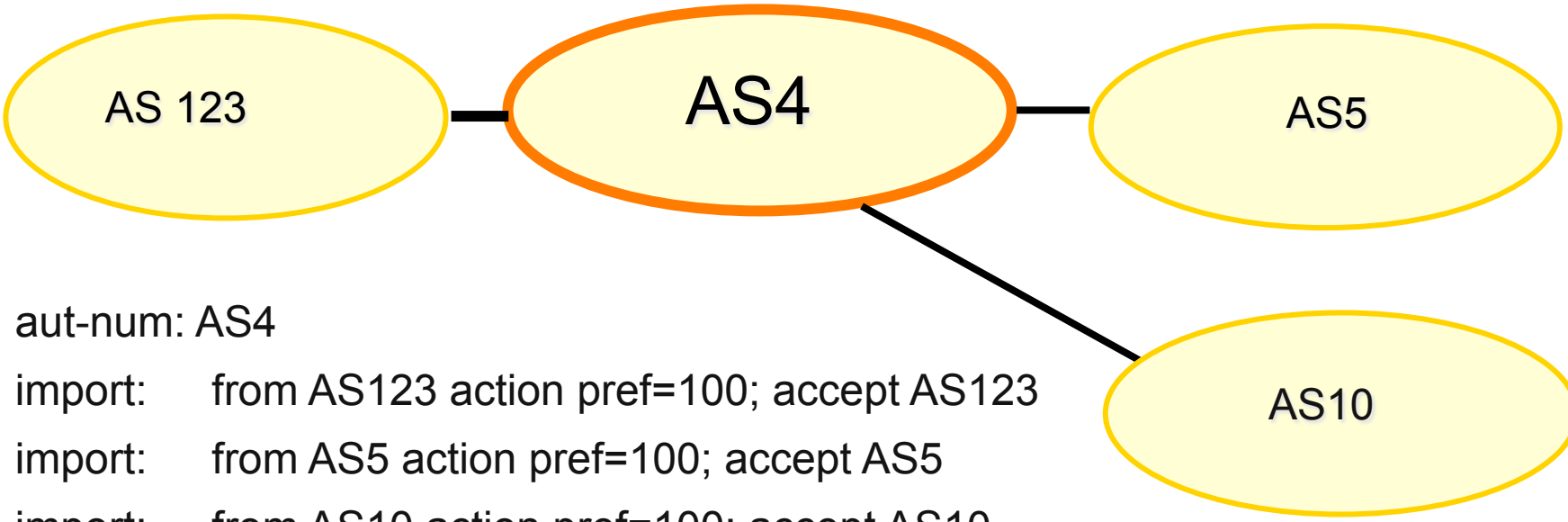
Routing Policy - Examples



More complex example

- AS4 gives transit to AS5, AS10
- AS4 gives local routes to AS123

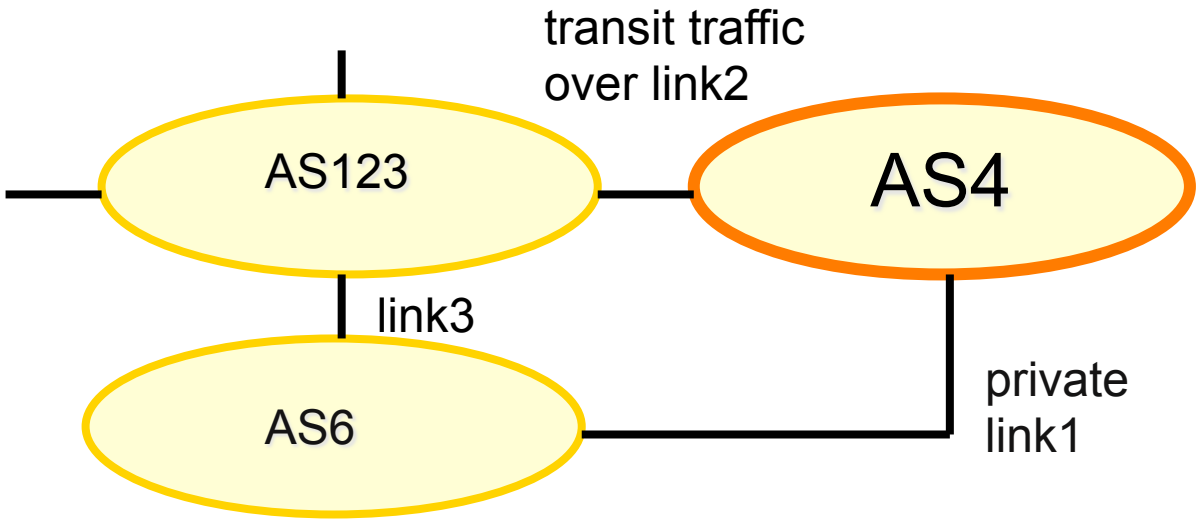
Routing Policy - Examples



aut-num: AS4
import: from AS123 action pref=100; accept AS123
import: from AS5 action pref=100; accept AS5
import: from AS10 action pref=100; accept AS10
export: to AS123 announce AS4
export: to AS5 announce AS4 AS10
export: to AS10 announce AS4 AS5

Not a path

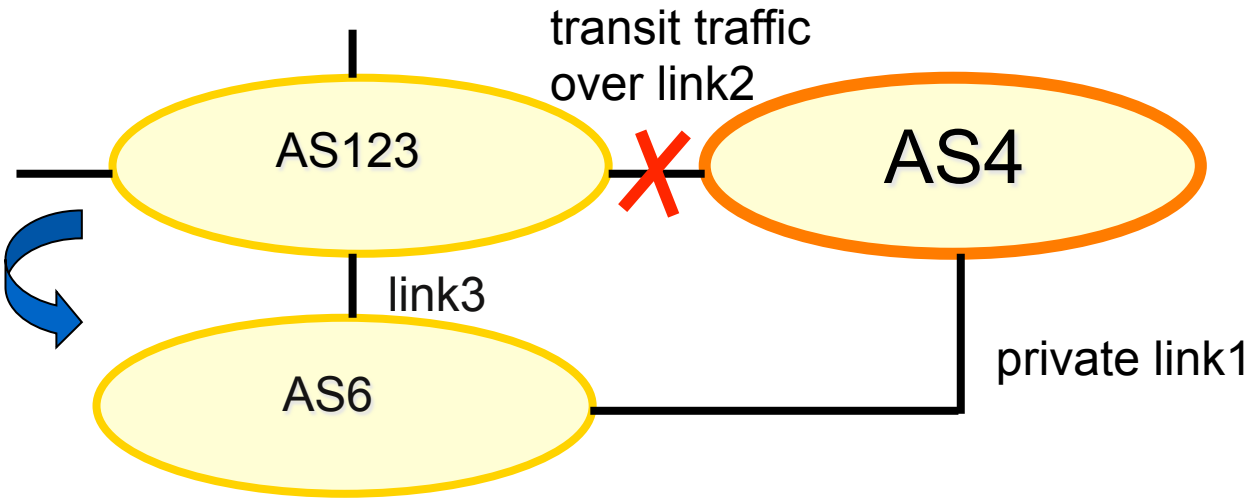
Routing Policy - Examples



More complex example

- AS4 and AS6 private link1
- AS4 and AS123 main transit link2
- backup all traffic over link1 and link3 in event of link2 failure

Routing Policy - Examples



AS representation

aut-num: AS4

import: from AS123 action pref=100; accept ANY ← *full routing received*

import: from AS6 action pref=50; accept AS6

import: from AS6 action pref=200; accept ANY

export: to AS6 announce AS4

export: to AS123 announce AS4

higher cost for backup route

APNIC Database and the IRR

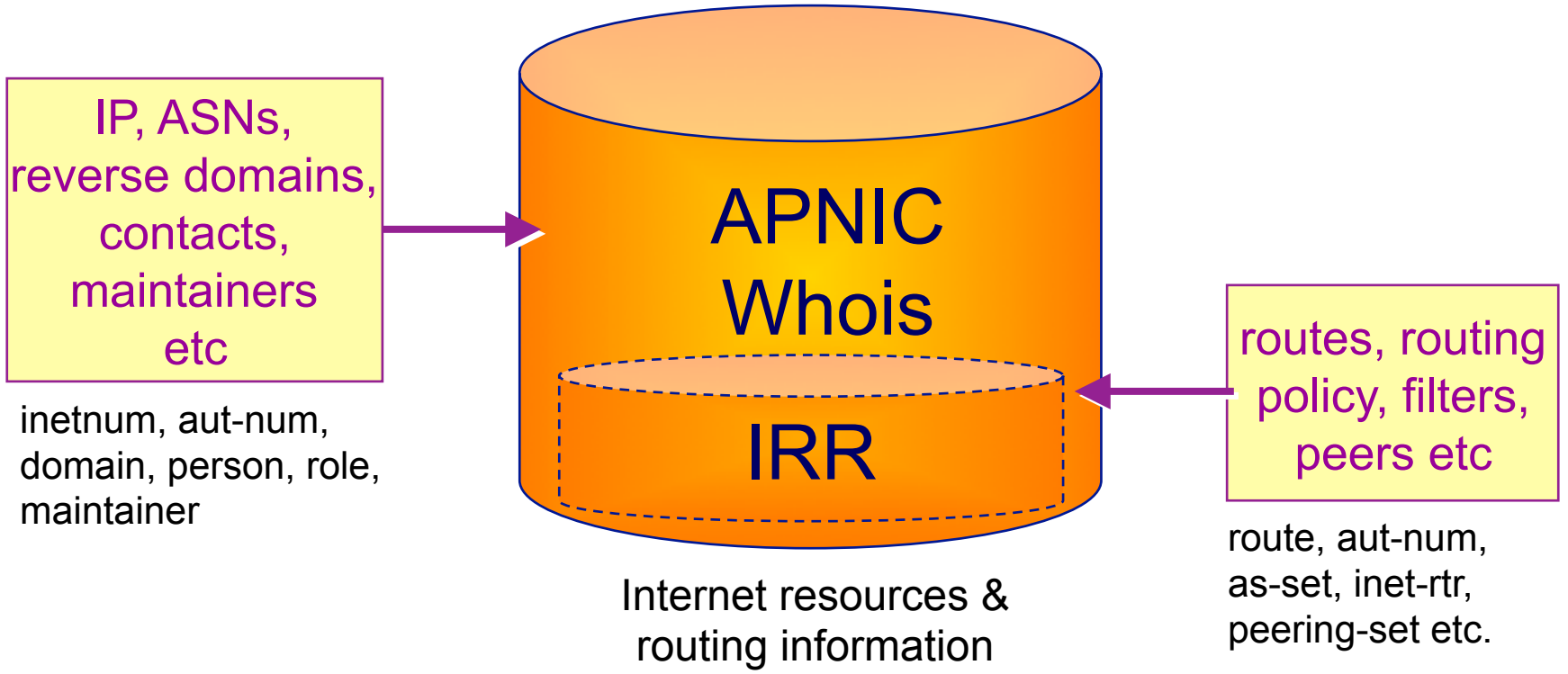
APNIC

APNIC Database & the IRR

- APNIC whois Database
  - Two databases in one
- Public Network Management Database
  - “whois” info about networks & contact persons
    - IP addresses, AS numbers etc
- Routing Registry
  - contains routing information
    - routing policy, routes, filters, peers etc.
  - APNIC RR is part of the global IRR

Integration of Whois and IRR

- Integrated APNIC Whois Database & Internet Routing Registry



IRR Objects

- route
  - Specifies interAS routes
- aut-num
  - Represents an AS. Used to describe external routing policy
- inet-rtr
  - Represents a router
- peering-set
  - Defines a set of peerings
- route-set
  - Defines a set of routes
- as-set
  - Defines a set of **aut-num** objects
- rtr-set
  - Defines a set of routers
- filter-set
  - Defines a set of routes that are matched by its filter

www.apnic.net/db/ref/db-objects.html

Using the Routing Registry

APNIC

IRRToolSet

- Set of tools developed for using the Internet Routing Registry (IRR)
- Work with Internet routing policies
  - These policies are stored in IRR in the Routing Policy Specification Language (RPSL)
- The goal of the IRRToolSet is to make routing information more convenient and useful for network engineers
  - Tools for automated router configuration,
  - Routing policy analysis
  - On-going maintenance etc.

IRRToolSet

- Now maintained by ISC:
  - http://irrtoolset.isc.org
  - Download: ftp://ftp.isc.org/isc/IRRToolSet/
    - Installation needs: lex, yacc and C++ compiler

Use of RPSL - RtConfig

- RtConfig v4
  - part of IRRToolSet

- Reads policy from IRR (aut-num, route & -set objects) and generates router configuration
  - vendor specific:
    - Cisco, Bay's BCC, Juniper's Junos and Gated/RSd
  - Creates route-map and AS path filters
  - Can also create ingress / egress filters
    - (documentation says Cisco only)

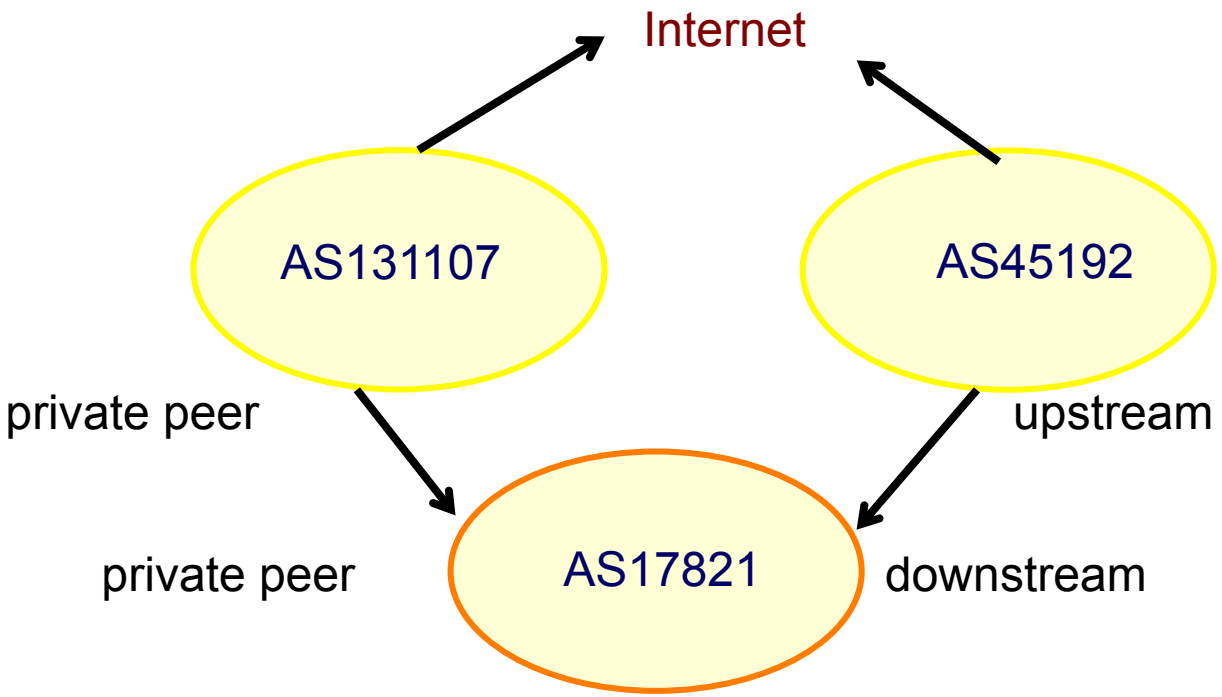
Why use IRR and RtConfig?

- Benefits of RtConfig
  - Avoid filter errors (typos)
  - Expertise encoded in the tools that generate the policy rather than engineer configuring peering session
  - Filters consistent with documented policy
    - (need to get policy correct though)

Using RPSL in practice

APNIC

Common Peering Policies



- AS45192 is your upstream provider
- AS131107 is a private peer
- Your AS is AS17821

How to write this in Aut-num

aut-num: AS17821

……

remarks: AS45192 is your upstream provider

import: from AS45192 action pref=100; accept ANY

export: to AS45192 announce AS17821

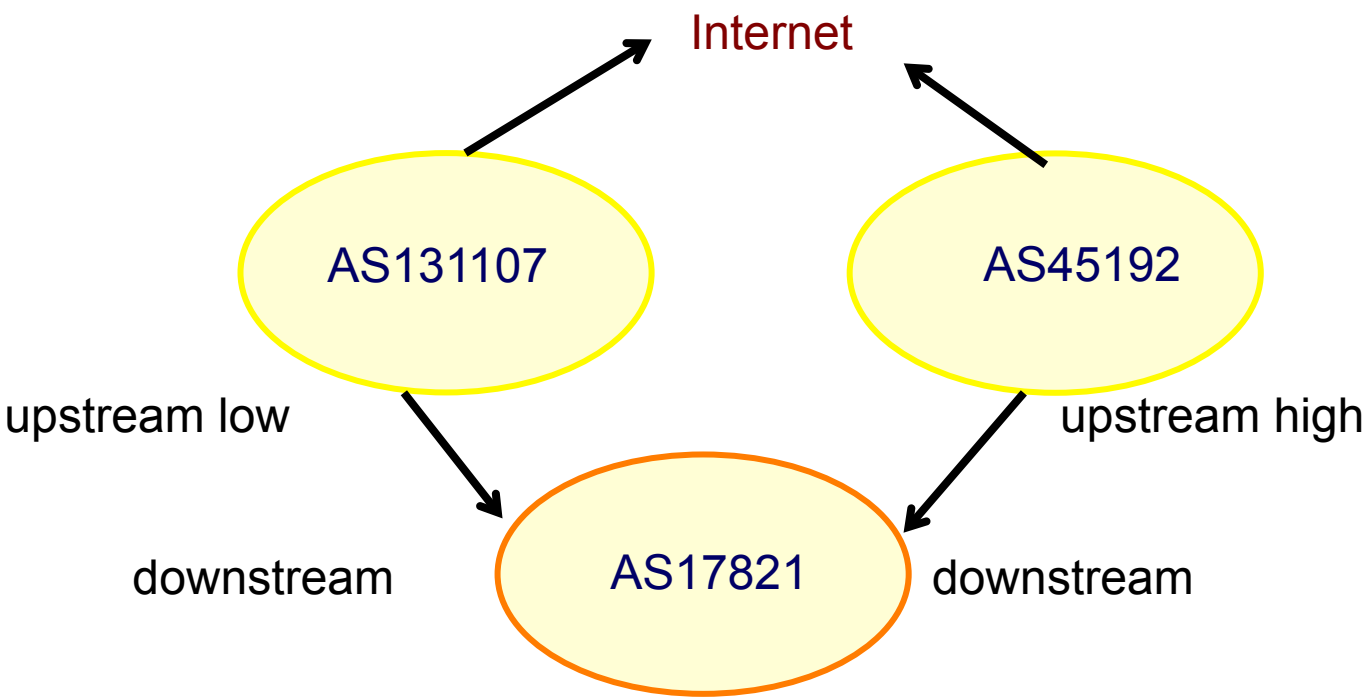
remarks: AS131107 is a private peer

import: from AS131107 action pref=20; accept AS131107

export: to AS131107 announce AS17821

……

Common Peering Policies



- AS45192 is your preferred upstream provider
- AS131107 is your backup upstream provider
- Your AS is AS17821

How to write this in Aut-num

aut-num: AS17821

……

remarks: AS45192 is your preferred upstream provider

import: from AS45192 action pref=100; accept ANY

export: to AS45192 announce AS17821

remarks: AS131107 is your backup upstream provider

import: from AS131107 action pref=200; accept ANY

export: to AS131107 action aspath.prepend (AS17821, AS17821);
announce AS17821

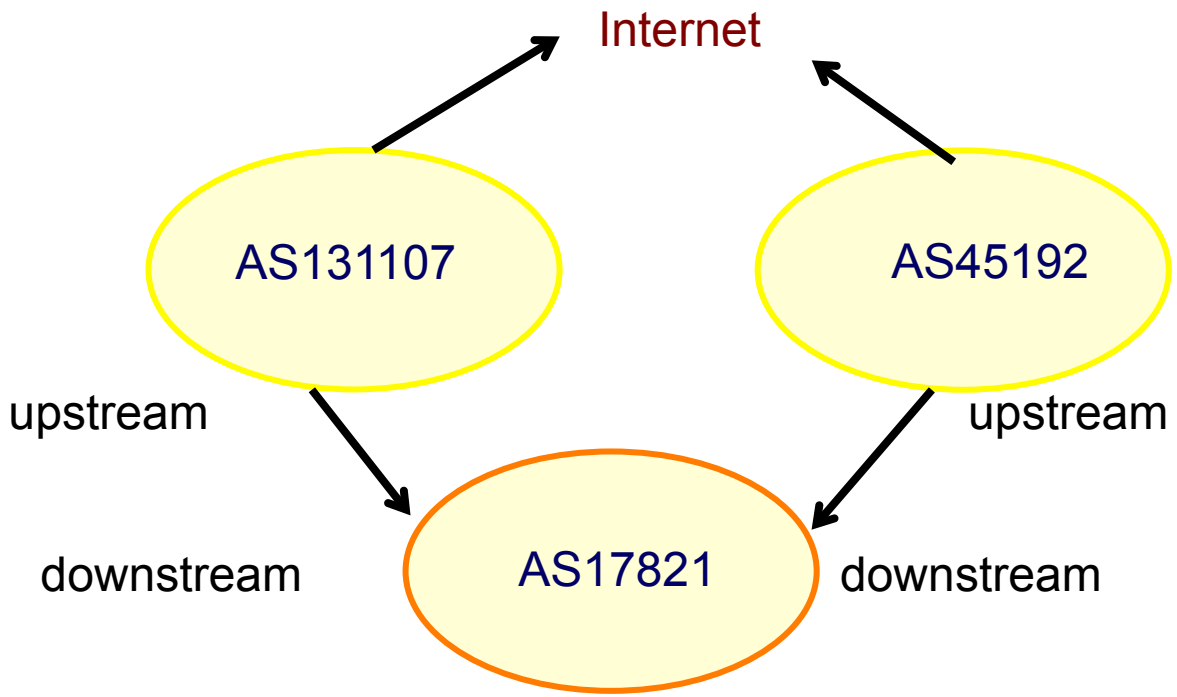
remarks: Optional extra import line to prefer direct

remarks: connection to AS131107 from AS17821

import: from AS131107 action pref=20; accept AS131107

……

Common Peering Policies



- AS45192 is your upstream provider
- AS131107 is your upstream provider
- Your AS is AS17821

How to write this in Aut-num

aut-num: AS17821

……

remarks: AS45192 is your upstream provider

import: from AS45192 action pref=100; accept ANY

export: to AS45192 announce AS17821

remarks: AS131107 is your upstream provider

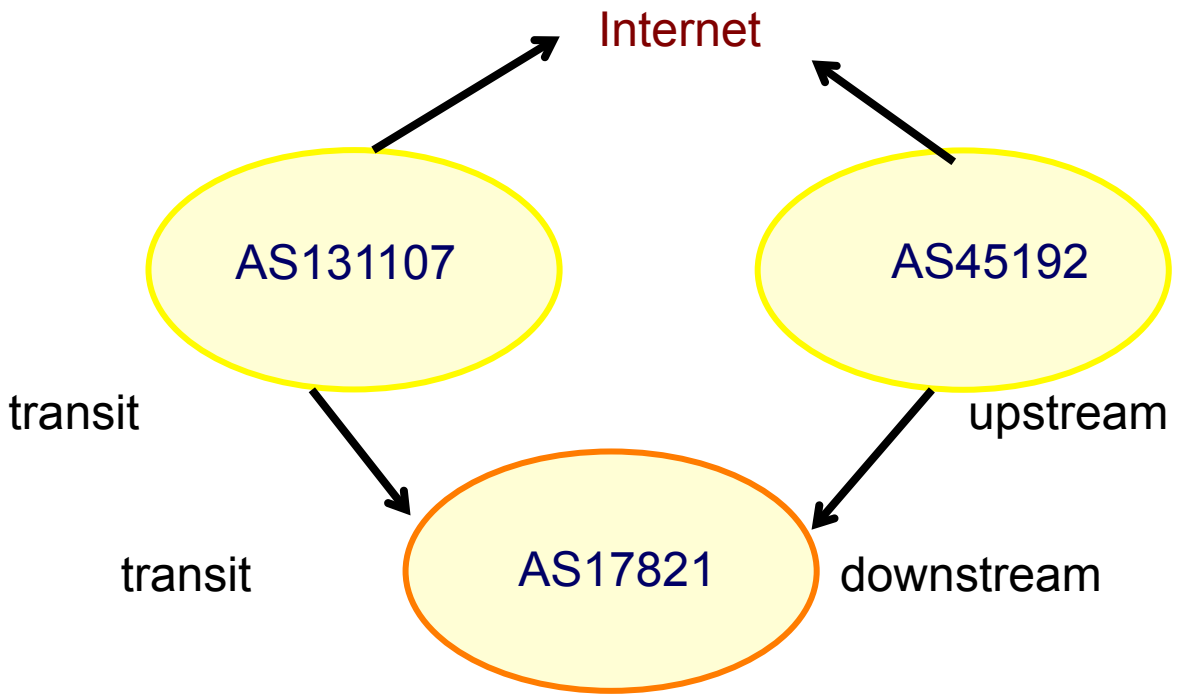
import: from AS131107 action pref=100; accept ANY

export: to AS131107 announce AS131107

remarks: the pref is optional here

……

Common Peering Policies



- AS45192 is your upstream provider
- AS131107 gives you transit AND you give AS131107 transit as well
- Your AS is AS17821

How to write this in Aut-num

aut-num: AS17821

……

remarks: AS45192 is your upstream provider

import: from AS45192 action pref=100; accept ANY

export: to AS45192 announce AS17821

remarks: AS131107 is your transit provider

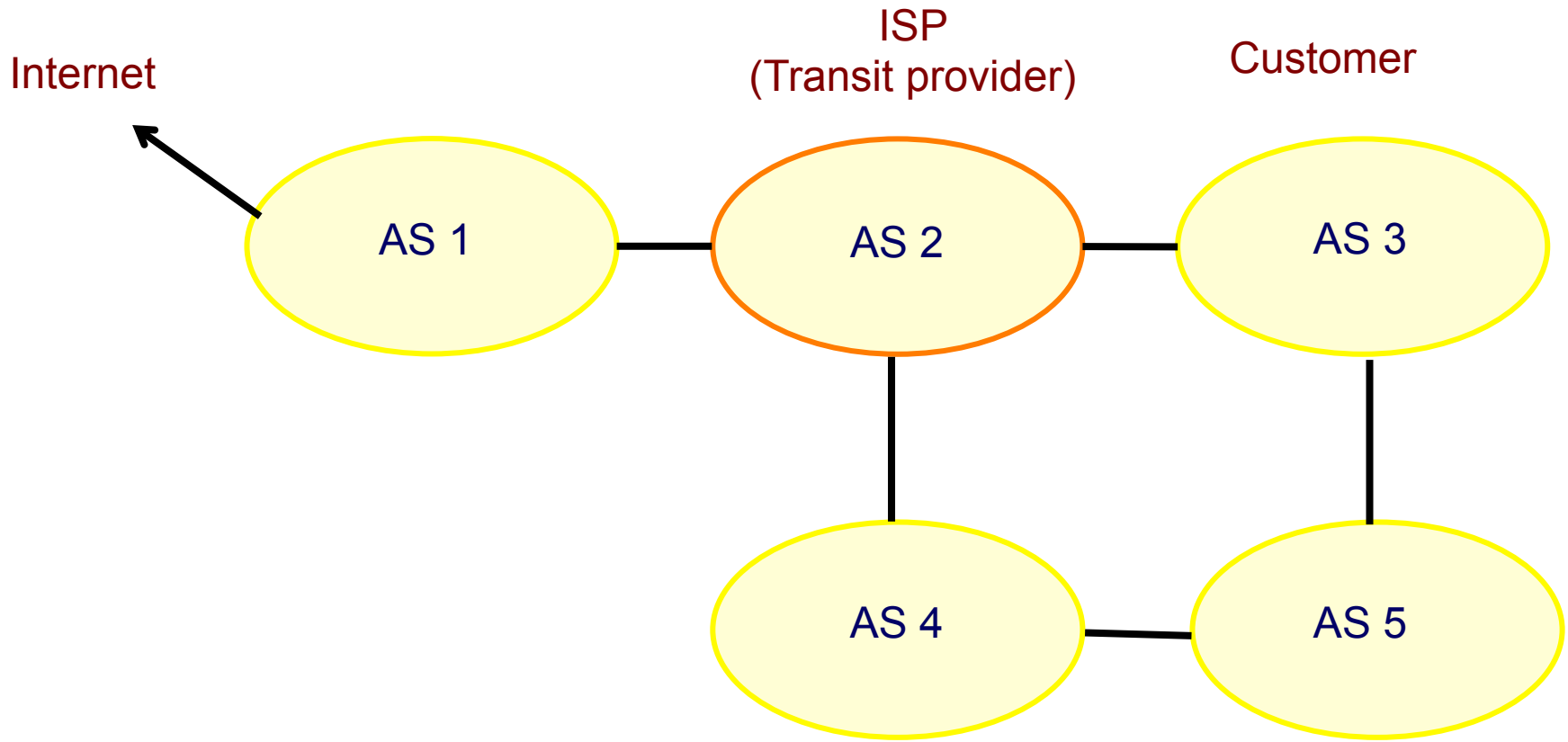
import: from AS131107 action pref=100; accept ANY

export: to AS131107 announce ANY

remarks: the pref is optional here

……

Common Peering Policies



- Peering policies of an AS
  - Registered in an aut-num object

Common Peering Policies

- Policy for AS3 in the AS2 aut-num object

```
aut-num:      AS2
as-name:      SAMPLE-NET
dsescr:       Sample AS
import:       from AS1 accept ANY
import:       from AS3 accept <^AS3+$>
export:       to AS3 announce ANY
export:       to AS1 announce AS2 AS3
admin-c:      CW89-AP
tech-c:       CW89-AP
mtn-by:       MAINT-SAMPLE-AP
changed:      sample@sample.net
```

Filter List- Regular Expression

- Like Unix regular expressions
  - . Match one character
  - * Match any number of preceding expression
  - + Match at least one of preceding expression
  - ^ Beginning of line
  - $ End of line
  - \ Escape a regular expression character
  - _ Beginning, end, white-space, brace
  - | Or
  - () Brackets to contain expression
  - [] Brackets to contain number ranges

ISP Customer – Transit Provider Policies

- Policy for AS3 and AS4 in the AS2 aut-num object

```
aut-num:    AS2
import:     from AS1 accept ANY
import:     from AS3 accept <^AS3+$>
import:     from AS4 accept <^AS4+$>
export:     to AS3 announce ANY
export:     to AS4 announce ANY
export:     to AS1 announce AS2 AS3 AS4
```

AS-set Object

- Describe the customers of AS2

```
as-set:     AS2:AS-CUSTOMERS
members:    AS3 AS4
changed:    sample@sample.net
source:     APNIC
```

New Initiative

RIRs have been developing a new service for their members

- APNIC has now launched Resource Certification for the AP region
- Improves the security of inter-domain routing and augmenting the information published in the APNIC Whois Database

Terminology

Resource holders include:

- Regional Internet Registries (RIRs)
- Local Internet Registries (LIRs)
- Internet Service Providers (ISPs)
- End-user organizations

Internet resources are:

- IPv4 and IPv6 address blocks
- Autonomous System (AS) numbers

Resource Certification Benefits

- Routing information corresponds to properly delegated address resources
- Resource Certification gives resource holders proof that they hold certain resources
- Resource holders can attest to those resources when distributing them

Benefits (Cont.)

Resource users can 'sign' information with a digital signature, which essentially 'freezes' that information

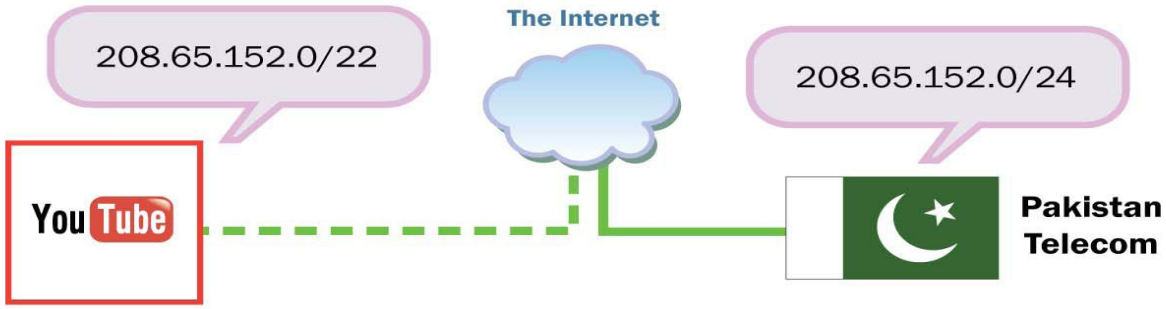
- Any effort to alter that information results in the signature being invalidated
- Only resource holders with a properly delegated 'right of use' can generate a signature

Benefits (cont.)

Routing advertisements are made with the explicit agreement of the current 'right of use' holder of the addresses being advertised.

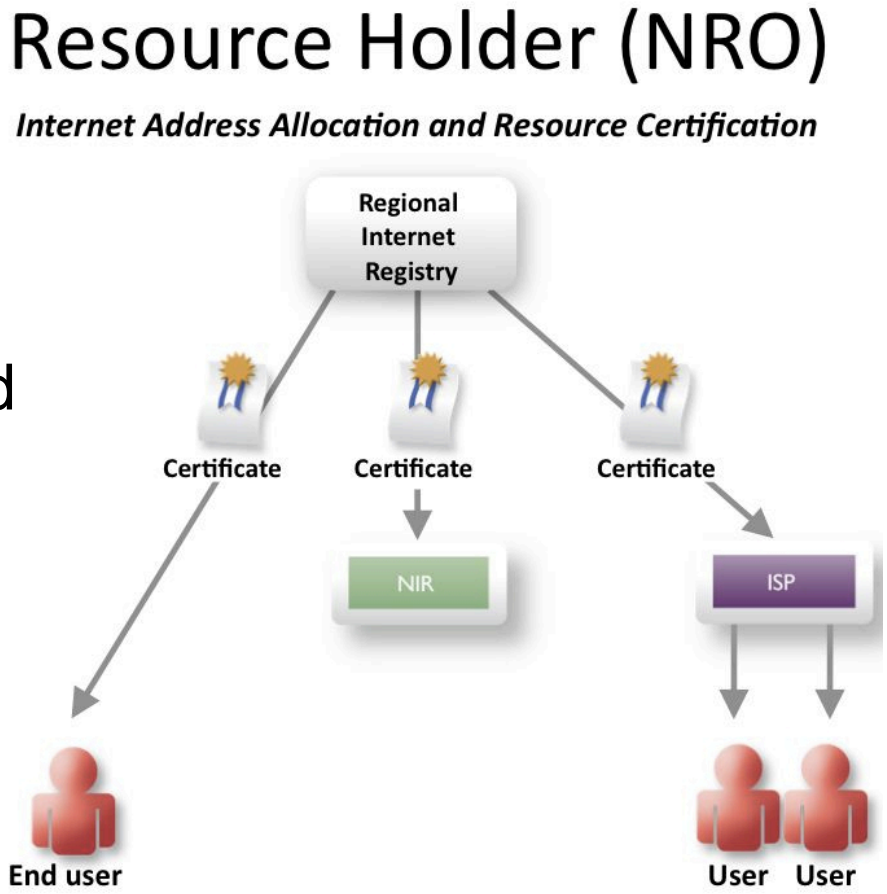
What is RPKI?

- Designed to secure the Internet's routing infrastructure
- Only the legitimate holder can advertise their prefix to the Internet
- Prevent those incidence of route hijacking (sometime by mistake)



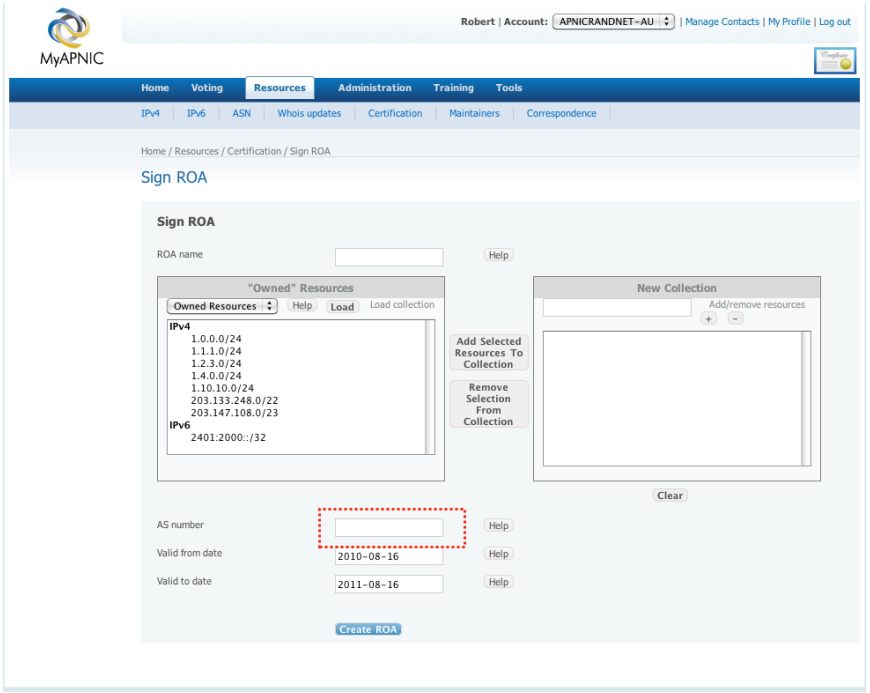
How It Works?

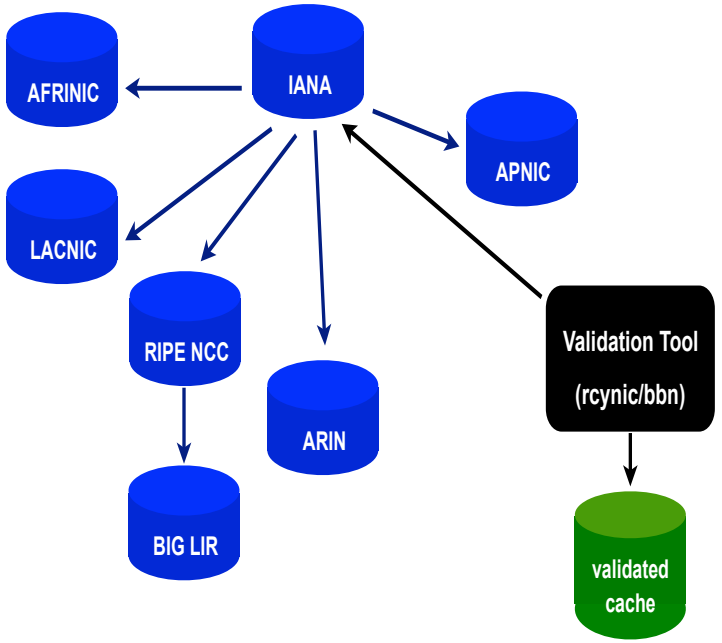
- Initially each RIR issued a self-signed trust anchors to the address they received from IANA
- Contains all resources from a **single trust anchor** managed by the RIR
- It was irrespective of their source



How It Works?

RPKI Validation: Distributed Repository





How It Works?

RPKI Validation: RPKI-RTR protocol


```
router bgp 65000
bgp log-neighbor-changes
bgp rpki server tcp 198.180.150.1 port 42420 refresh 60
```

How does it look in BGP table then?

BGP Table

RPKI Validation: RPKI-RTR protocol

```
router1#sh bgp ipv4 unicast
BGP table version is 45, local router ID is 203.176.189.15
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale, m multipath, b backup-path, x best-external, f RT-Filter, a additional-path
Origin codes: i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found

     Network          Next Hop            Metric LocPrf Weight Path
   V0.0.0.0         0.0.0.0                  0 i
*>  N67.21.36.0/24    199.238.113.10                 0 3130 2914 293 3970 e
*>  V85.118.184.0/21  199.238.113.10                 0 3130 2914 174 29485 29485 57785 i
*>  I98.128.0.0/24    199.238.113.10           0     0 3130 i
*>  V98.128.0.0/16    199.238.113.10           0     0 3130 i
*>  N98.128.1.0/24    199.238.113.10           0     0 3130 i
*>  N98.128.2.0/24    199.238.113.10           0     0 3130 i
```

```
route-map validity-0
    match rpki-invalid
    drop
route-map validity-1
    match rpki-not-found
    set localpref 50
// Valid defaults to 100
```

Use route-map to accept RPKI validated route

```
route-map validity-0
    match rpki-unknown
    set metric 50
route-map validity-1
    match rpki-invalid
    set metric 25
route-map validity-2
    set metric 100
```

What Is The New Challenge?

- Inter RIR transfer process is implemented now
- It requires an efficient way to reflect the changes to an RIR's resource holding
- Without revoking and reissuing the affected RIR trust anchor
- The split anchor model allows more granular updates, affecting only the certification path that covers the transferred resources

New Split Anchor Model

- APNIC has published five new self-signed certificates
- One for those address space given by IANA for this region
- Four for other self-signed certificates for resource acquired from each other RIR

What Changes For Operational Network?

- Organizations that RPKI origin validation on their router software need to make updates to their routing configuration
- If you already have the APNIC trust anchor you should refresh this with the complete new set of five
- Take note of any required configuration changes in your software

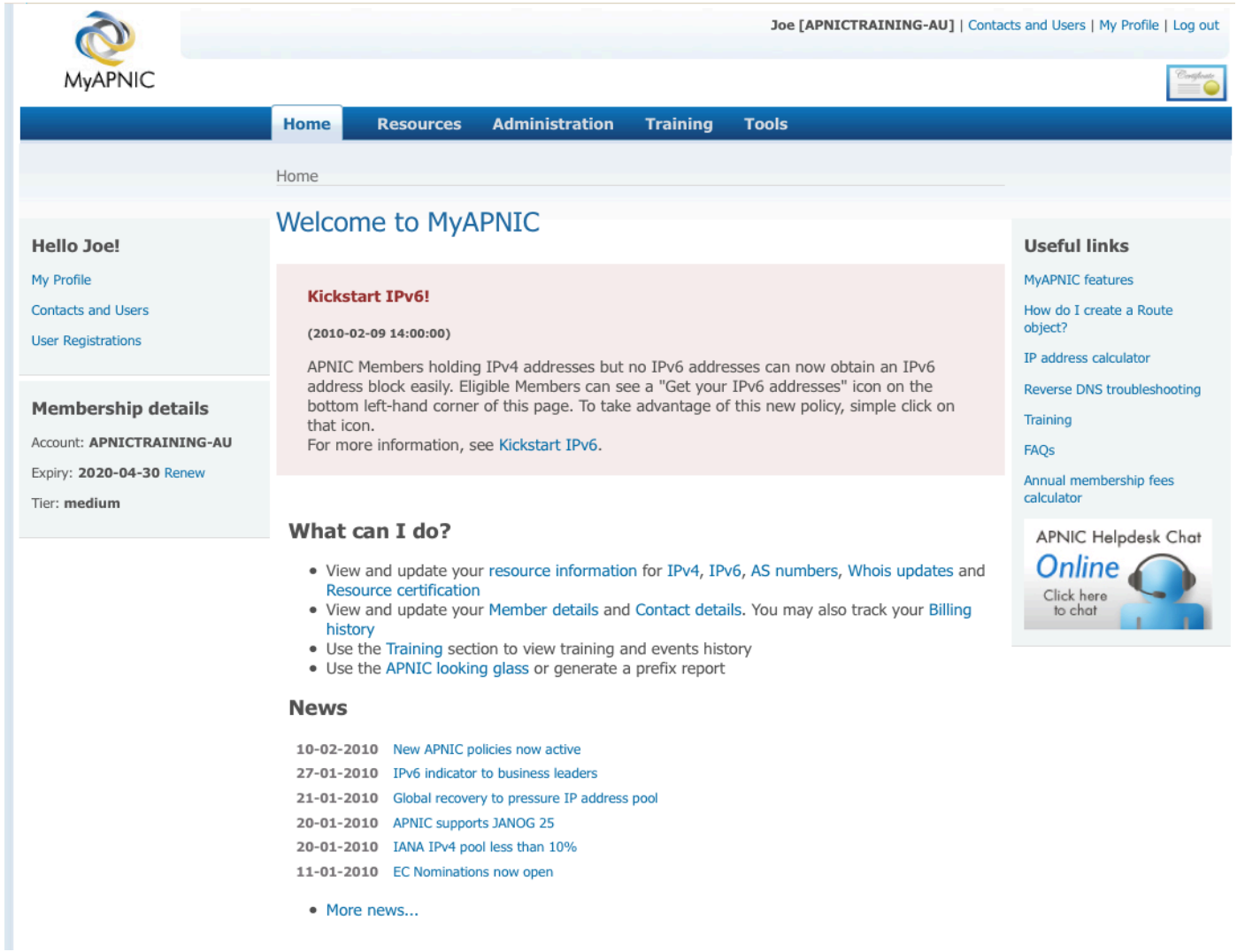
Find More…..

- APNIC to Upgrade to Split Trust Anchor RPKI:
  http://www.apnic.net/publications/news/2012/apnic-to-upgrade-to-split-trust-anchor-rpki
- Resource Public Key Infrastructure (RPKI) FAQ:
  http://www.apnic.net/services/services-apnic-provides/helpdesk/faqs/rpki/
- Resource certification
  http://www.apnic.net/services/services-apnic-provides/resource-certification

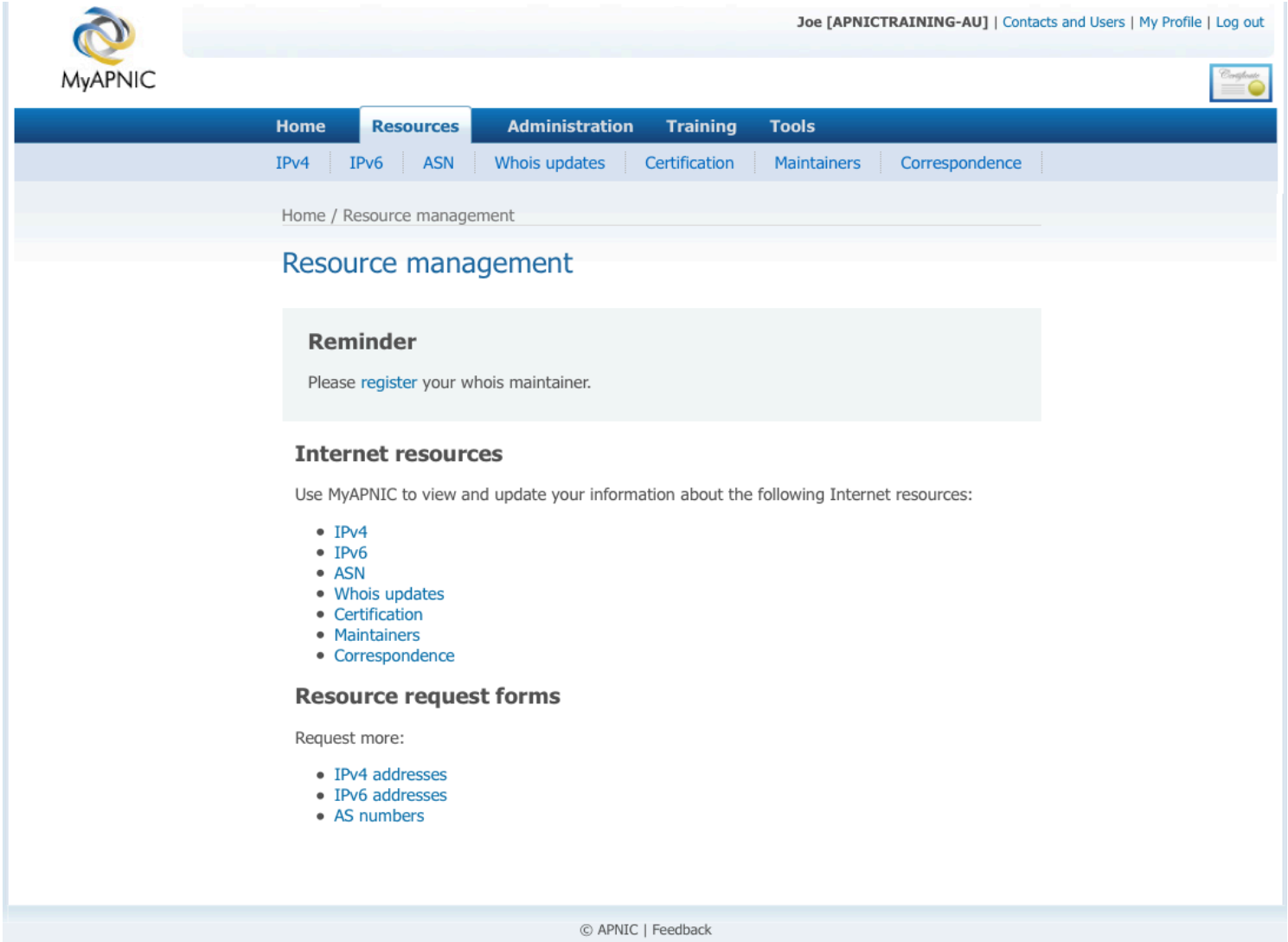
Current Stage of ResCert

- Origin validation code is engineering now, could deploy in next few years but requires production RPKI
- Path validation is still research
- Filter validation is still research

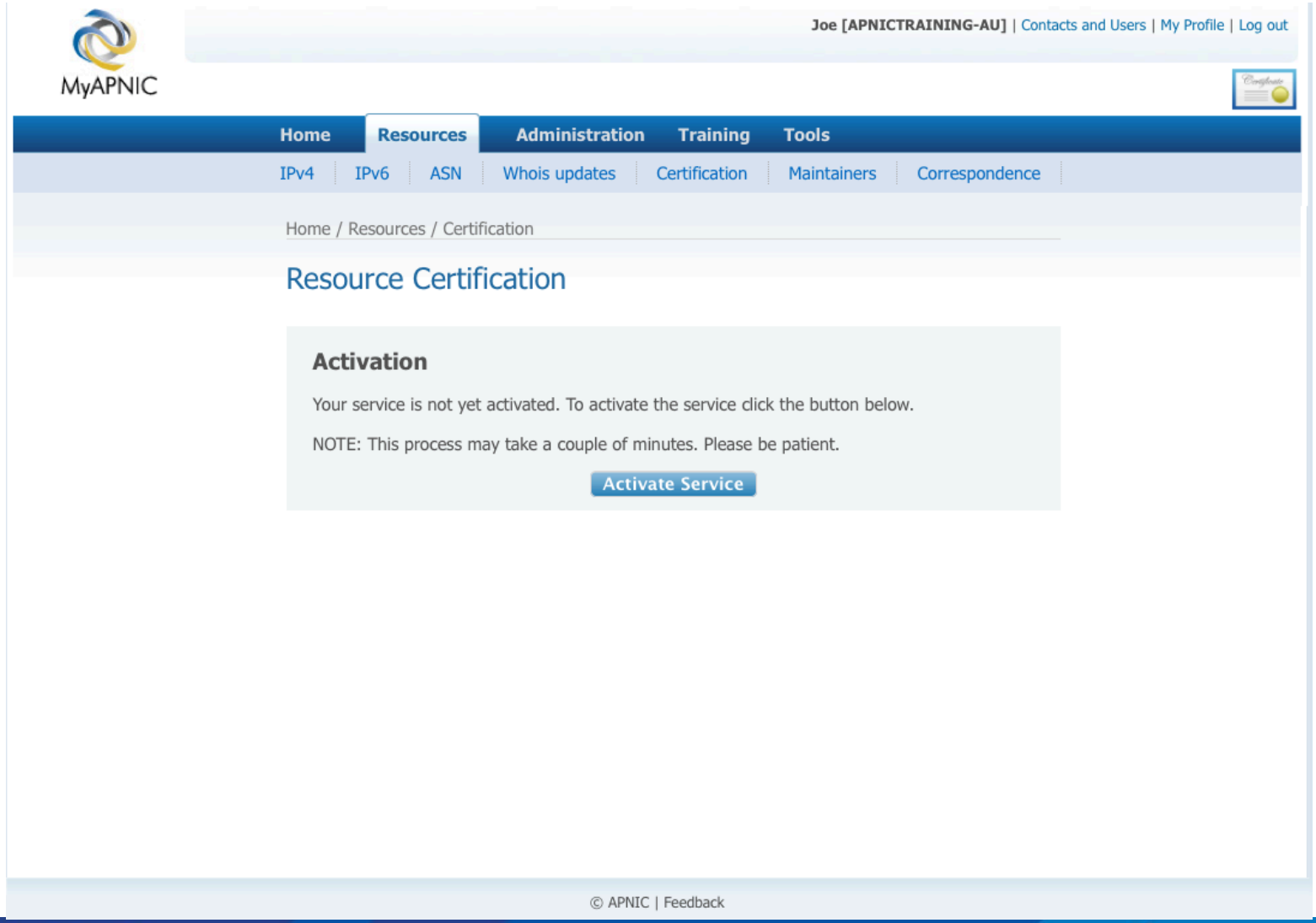
MyAPNIC Home Page



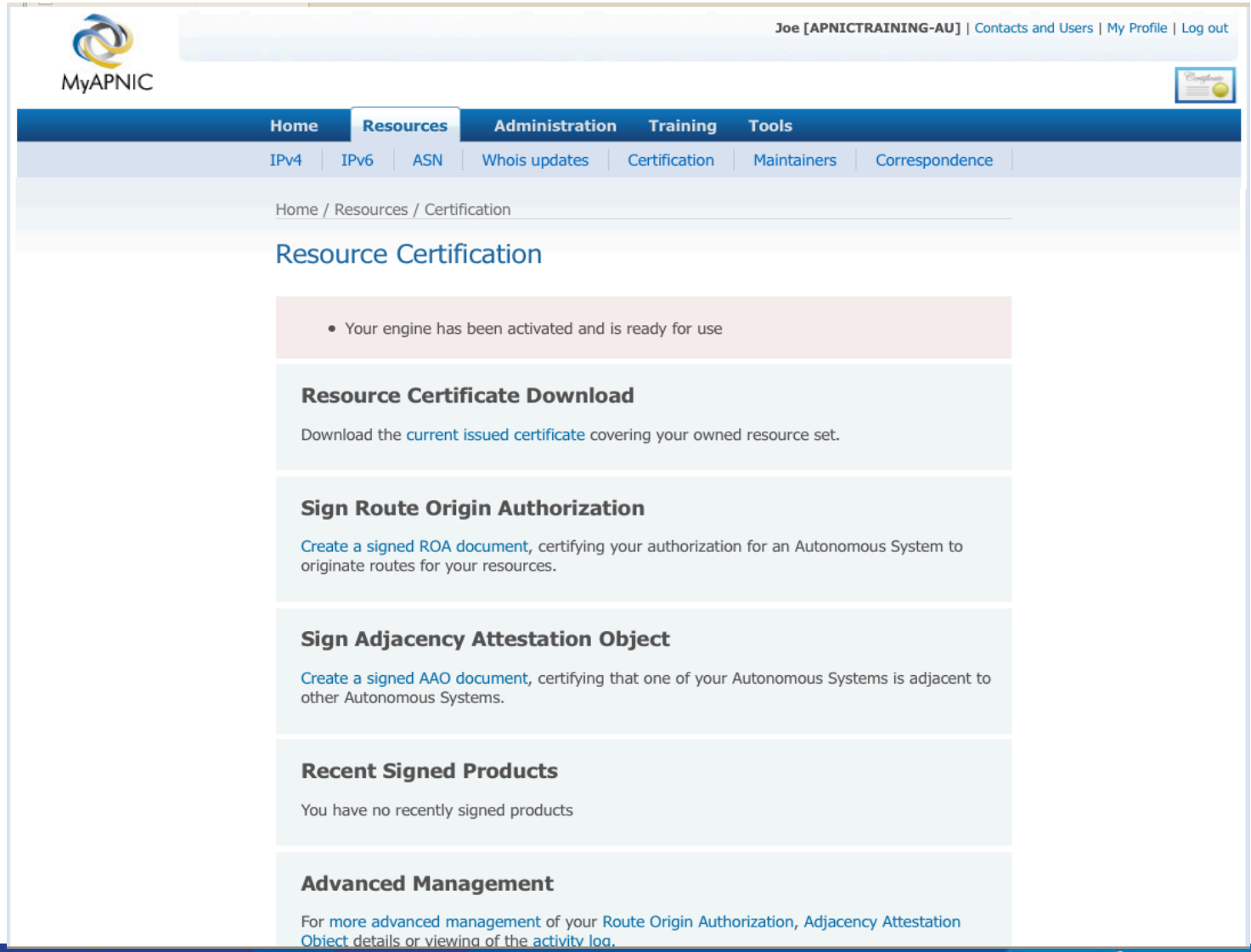
Resources Management



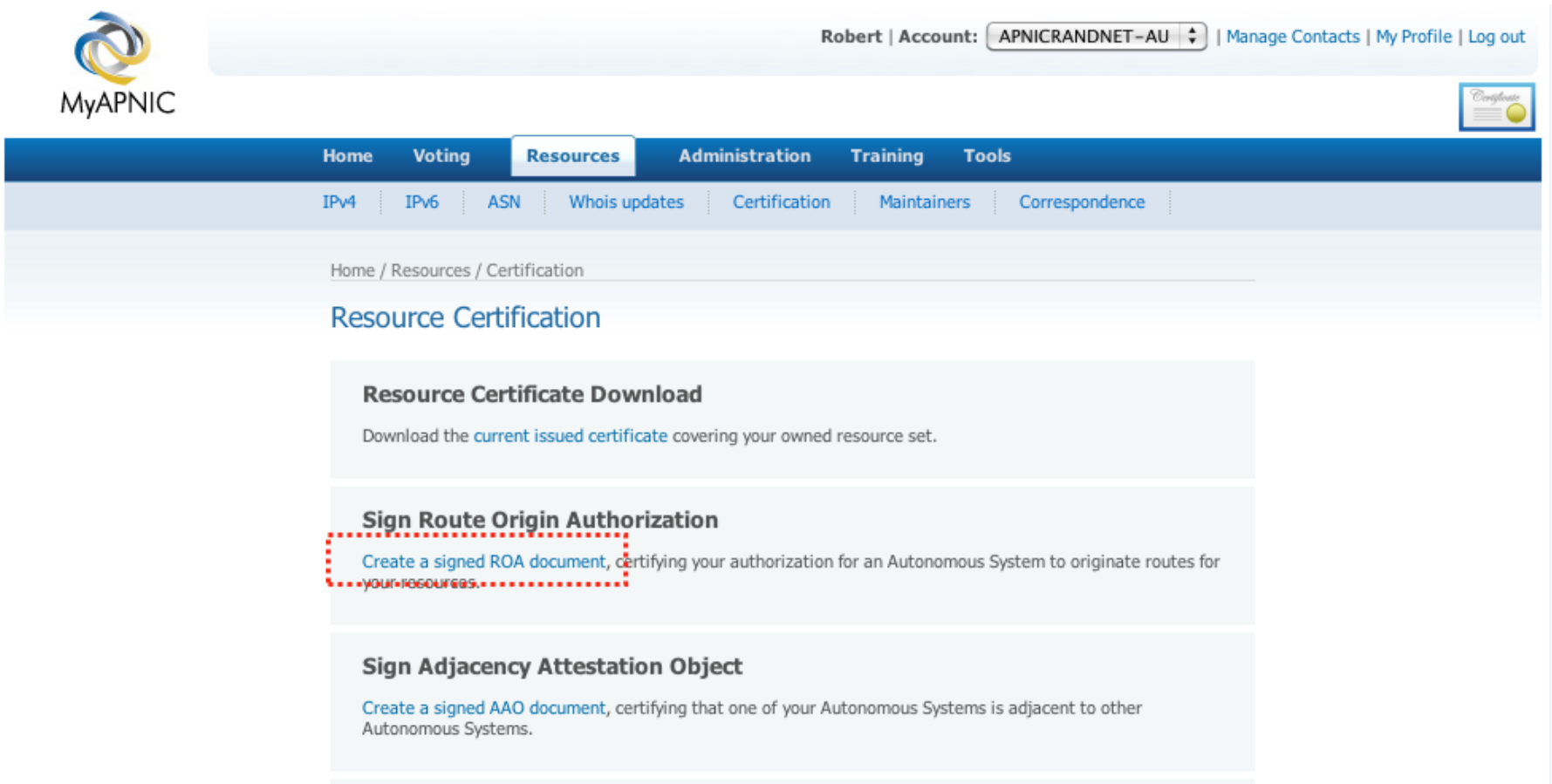
Activate Certification



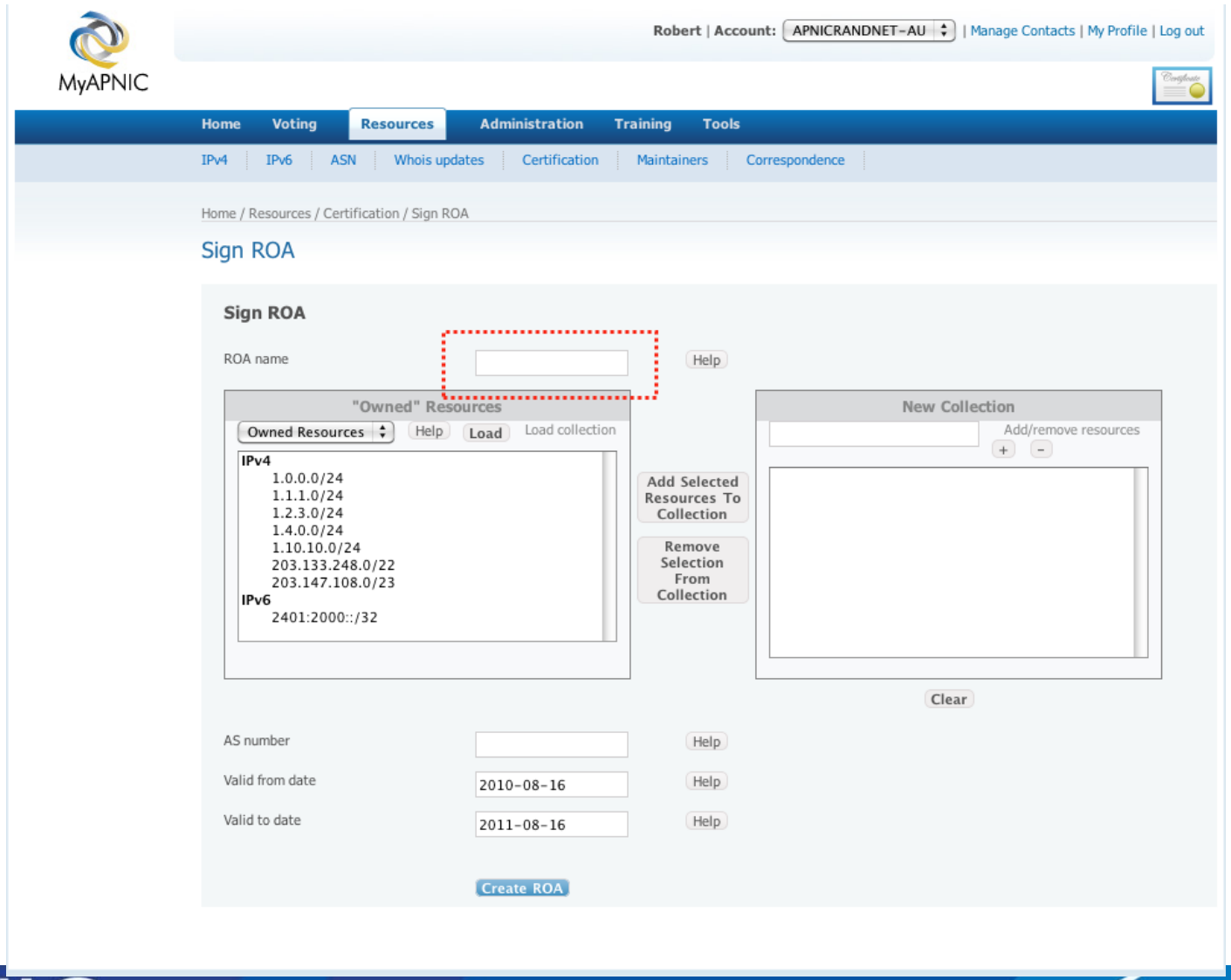
Service Activated



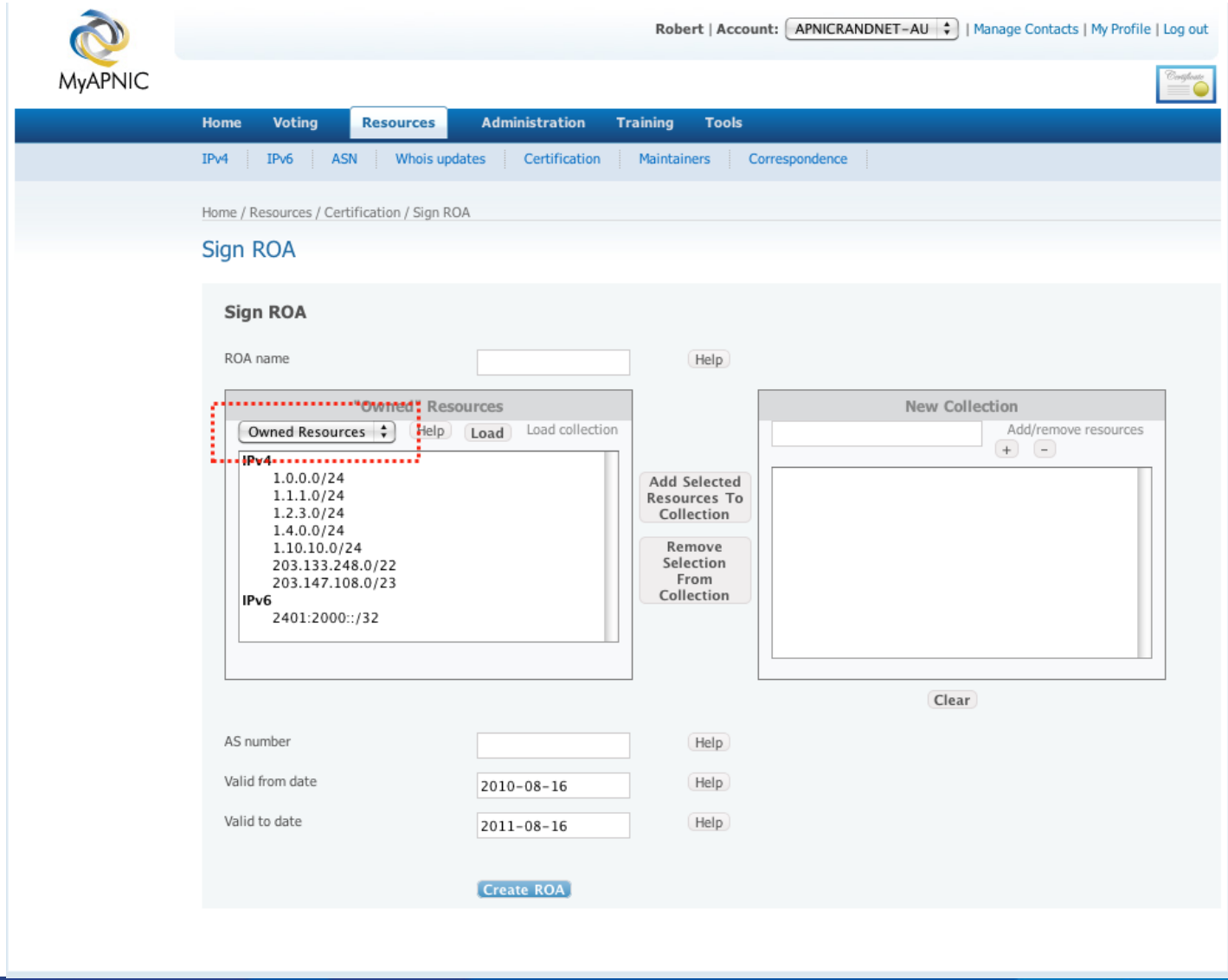
Create Route Origin Authorization



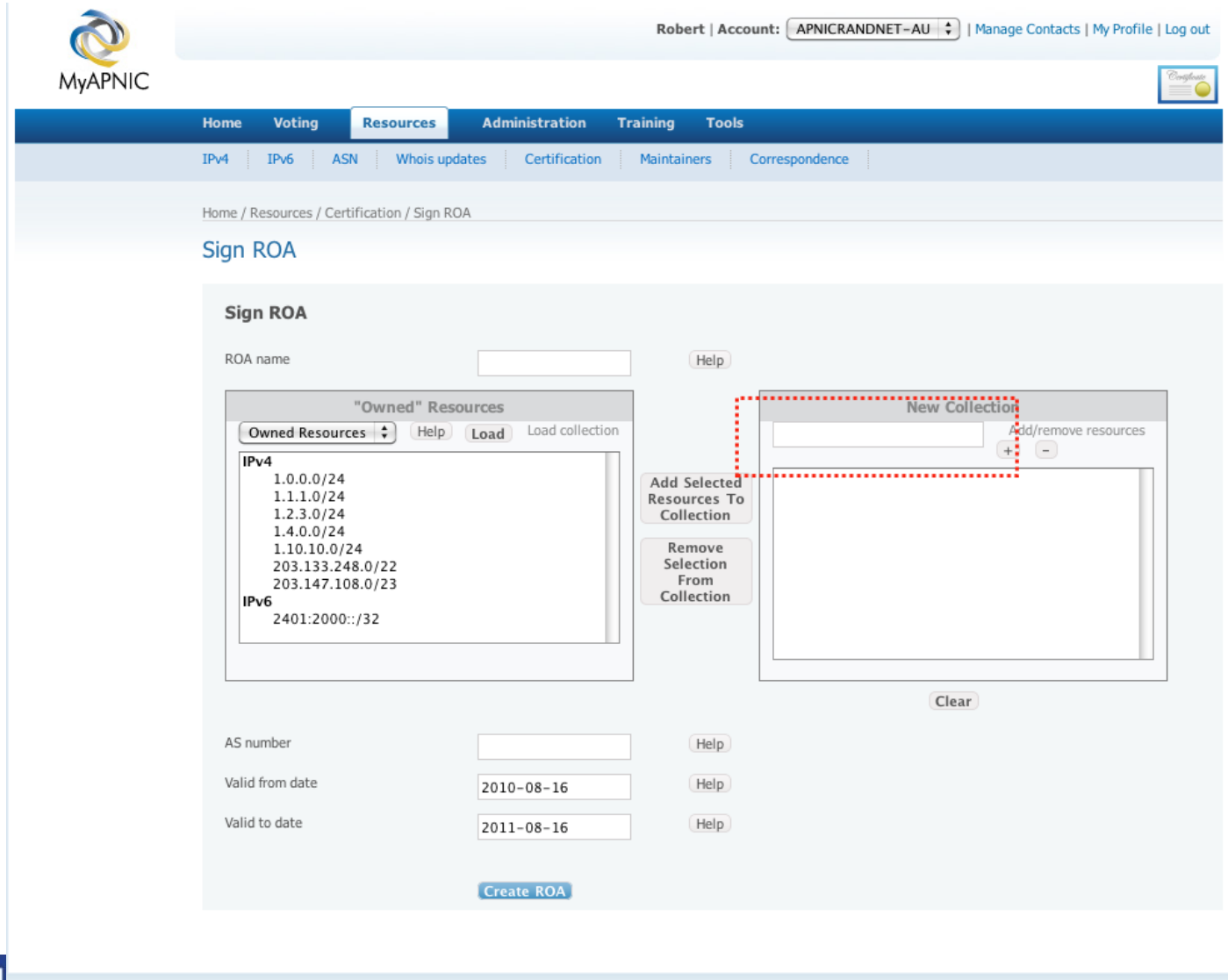
Name ROA


MyAPNIC
Robert | Account: APNICRANDNET-AU | Manage Contacts | My Profile | Log out
Home Voting Resources Administration Training Tools
IPv4 IPv6 ASN Whois updates Certification Maintainers Correspondence
Home / Resources / Certification / Sign ROA
Sign ROA
Sign ROA
ROA name
Help
"Owned" Resources
Owned Resources
Help
Load
Load collection
IPv4
1.0.0.0/24
1.1.1.0/24
1.2.3.0/24
1.4.0.0/24
1.10.10.0/24
203.133.248.0/22
203.147.108.0/23
IPv6
2401:2000::/32
Add Selected Resources To Collection
Remove Selection From Collection
New Collection
Add/remove resources
Clear
AS number
Help
Valid from date
2010-08-16
Help
Valid to date
2011-08-16
Help
Create ROA

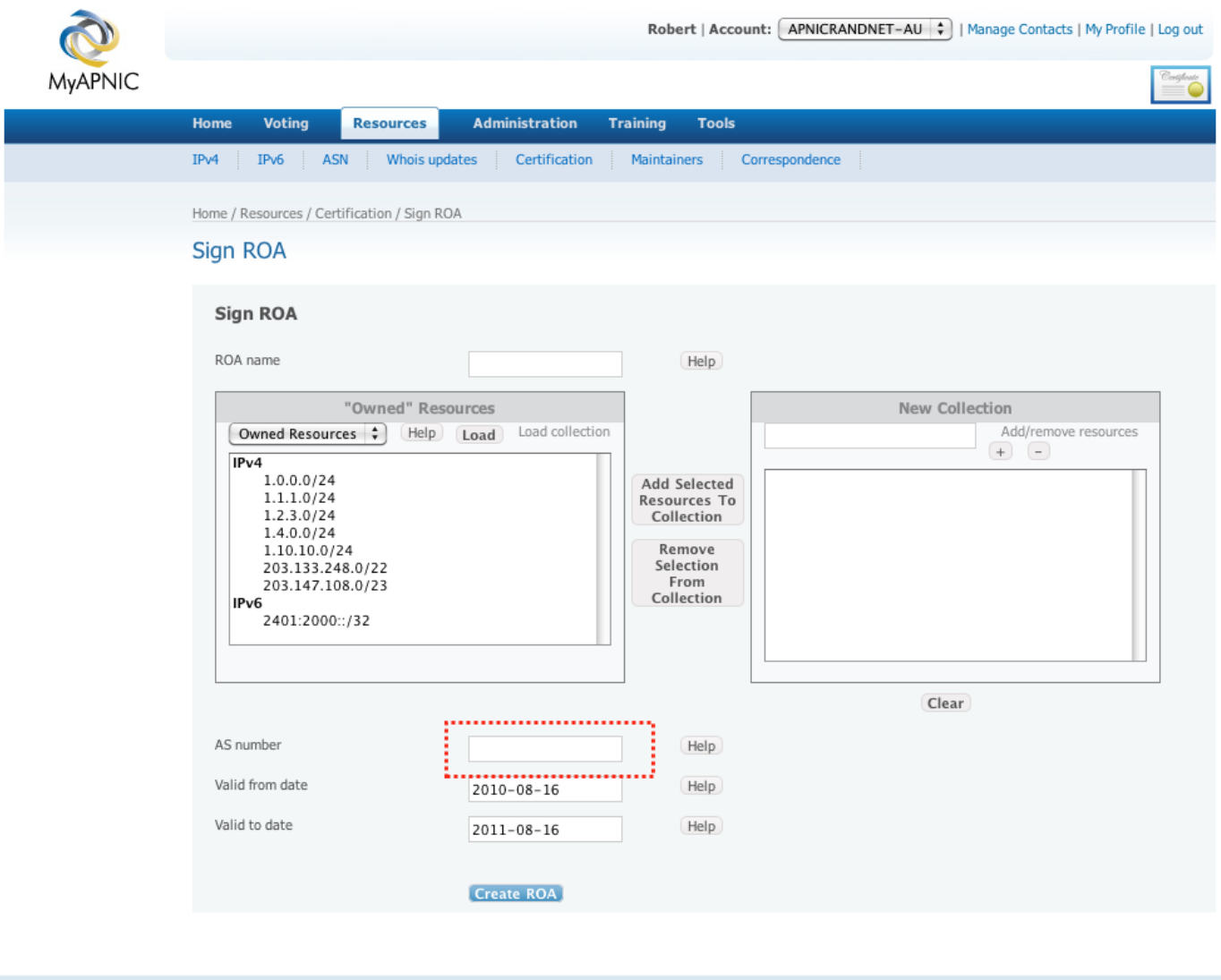
Add Resources



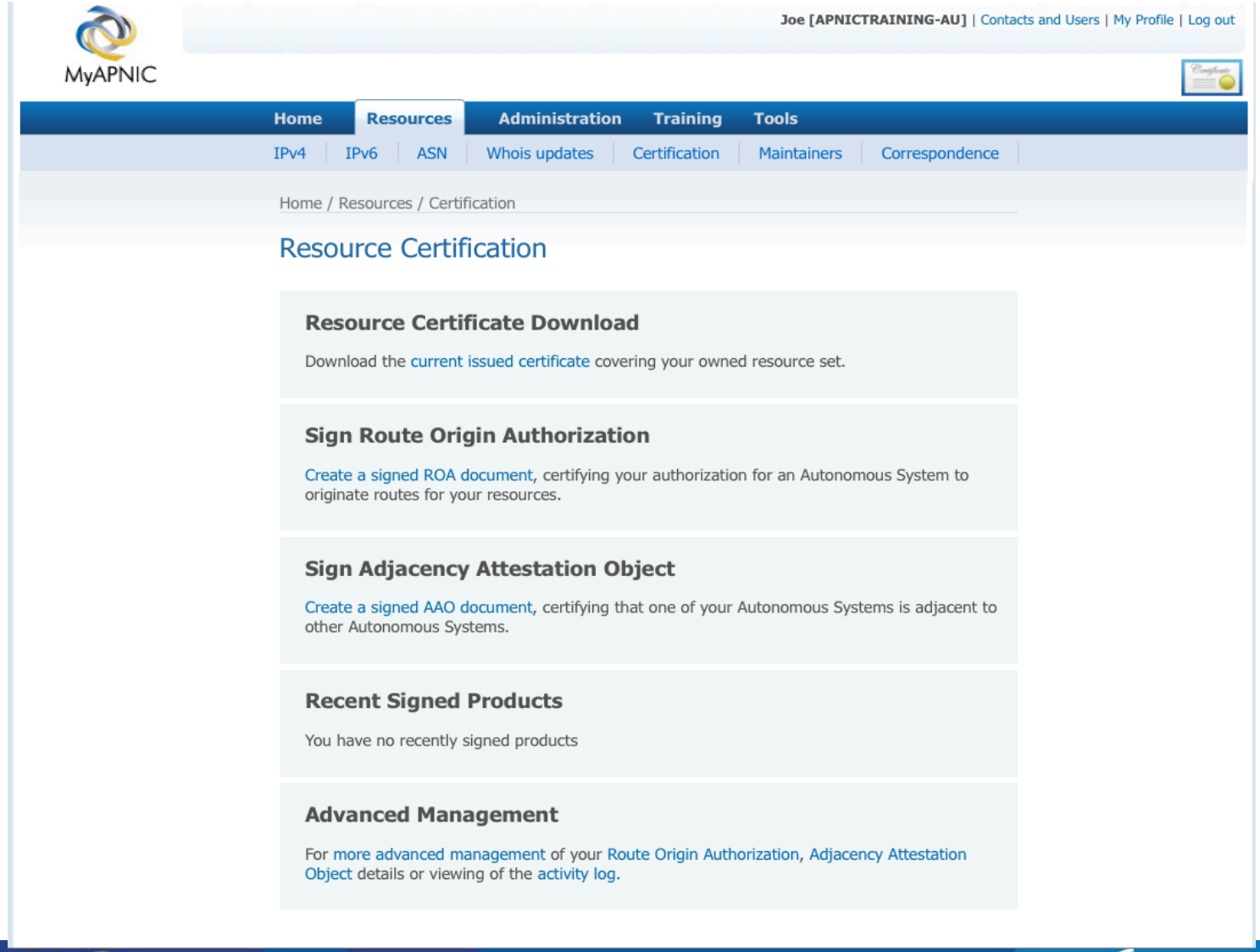
Add Resources



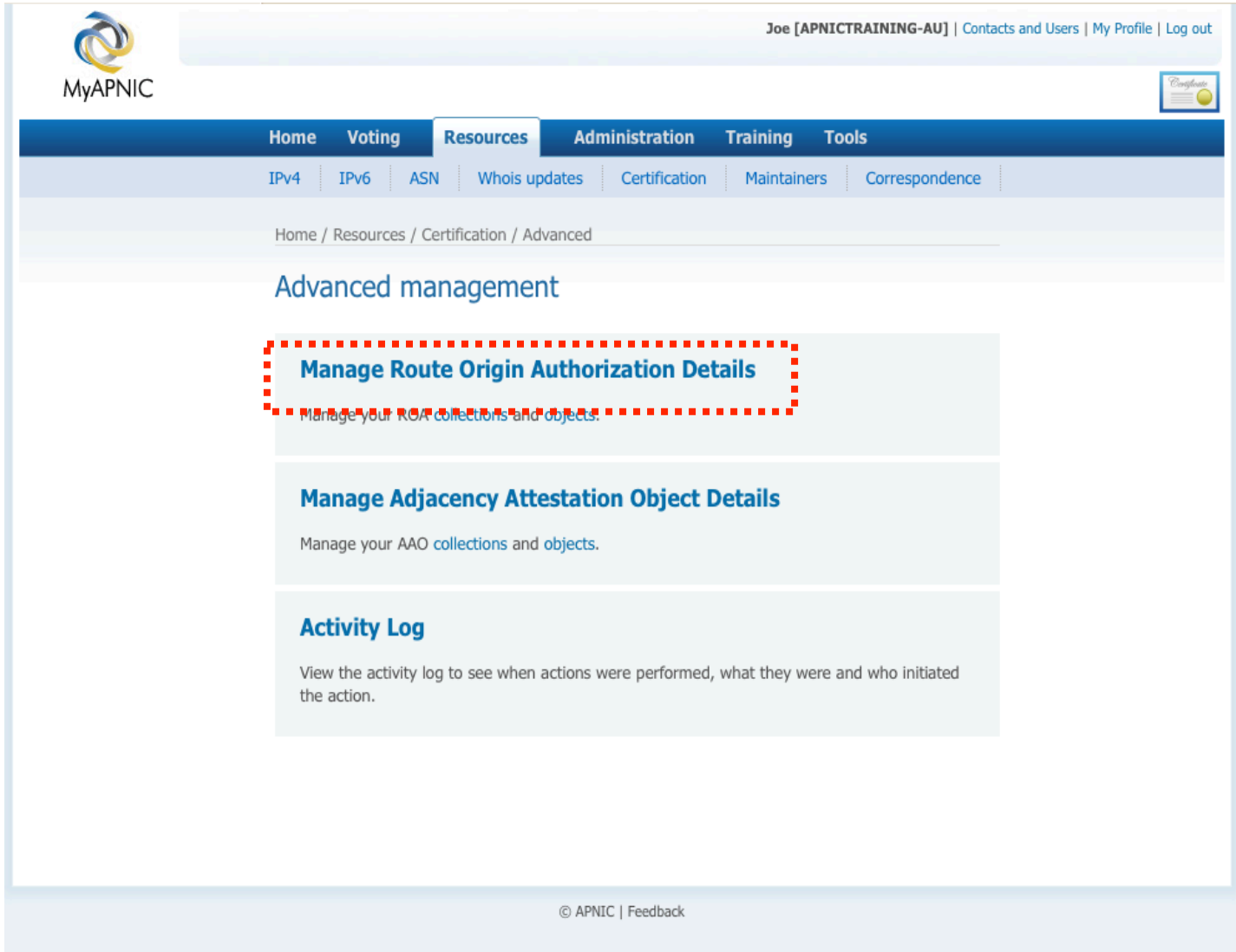
Add AS


MyAPNIC
Robert | Account: APNICRANDNET-AU | Manage Contacts | My Profile | Log out
Home
Voting
Resources
Administration
Training
Tools
IPv4
IPv6
ASN
Whois updates
Certification
Maintainers
Correspondence
Home / Resources / Certification / Sign ROA
Sign ROA
Sign ROA
ROA name
Help
"Owned" Resources
Owned Resources
Help
Load
Load collection
IPv4
1.0.0.0/24
1.1.1.0/24
1.2.3.0/24
1.4.0.0/24
1.10.10.0/24
203.133.248.0/22
203.147.108.0/23
IPv6
2401:2000::/32
Add Selected Resources To Collection
Remove Selection From Collection
New Collection
Add/remove resources
+
-
Clear
AS number
Help
Valid from date
2010-08-16
Help
Valid to date
2011-08-16
Help
Create ROA

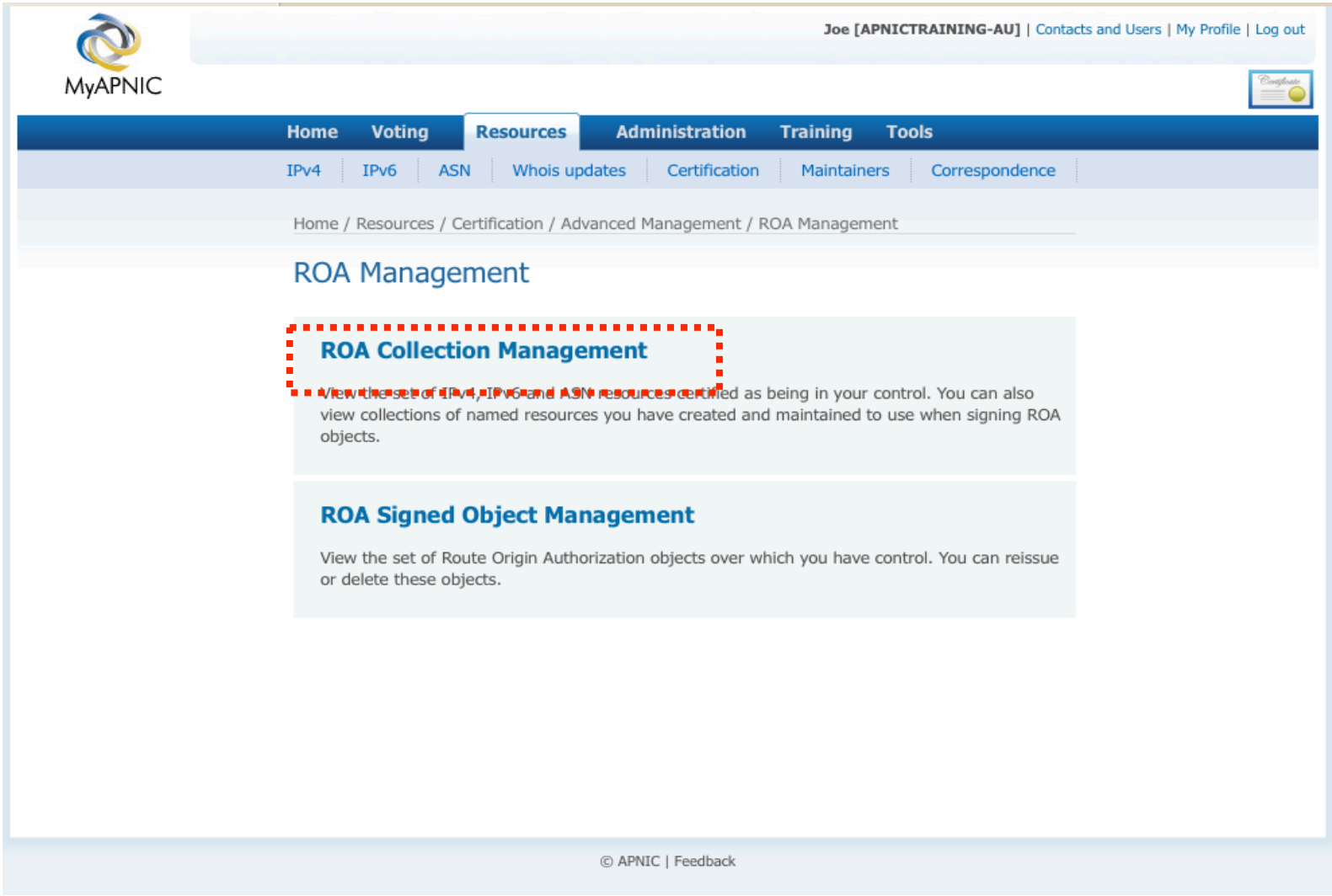
Advanced Management



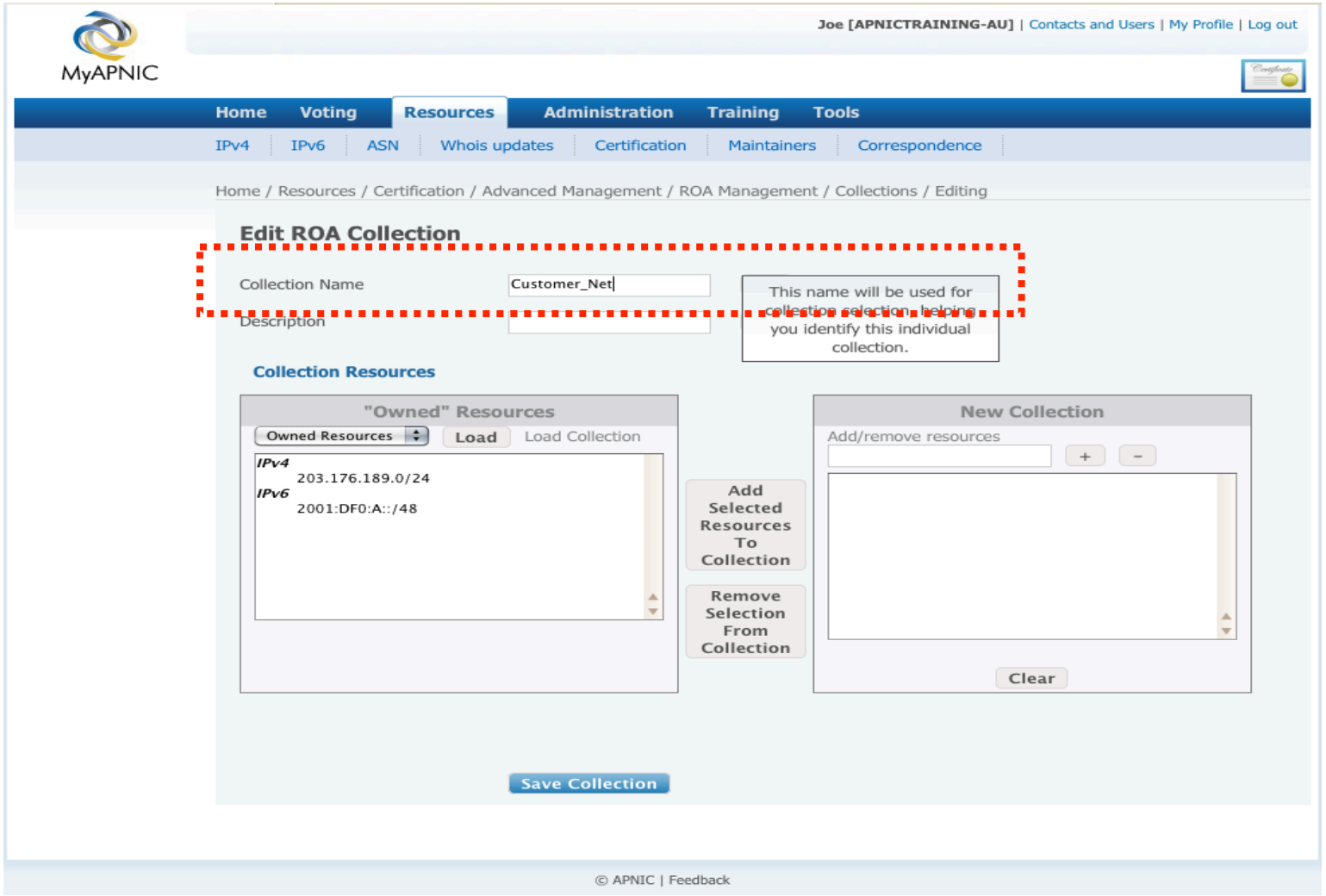
Route Origin Authorization (ROA)



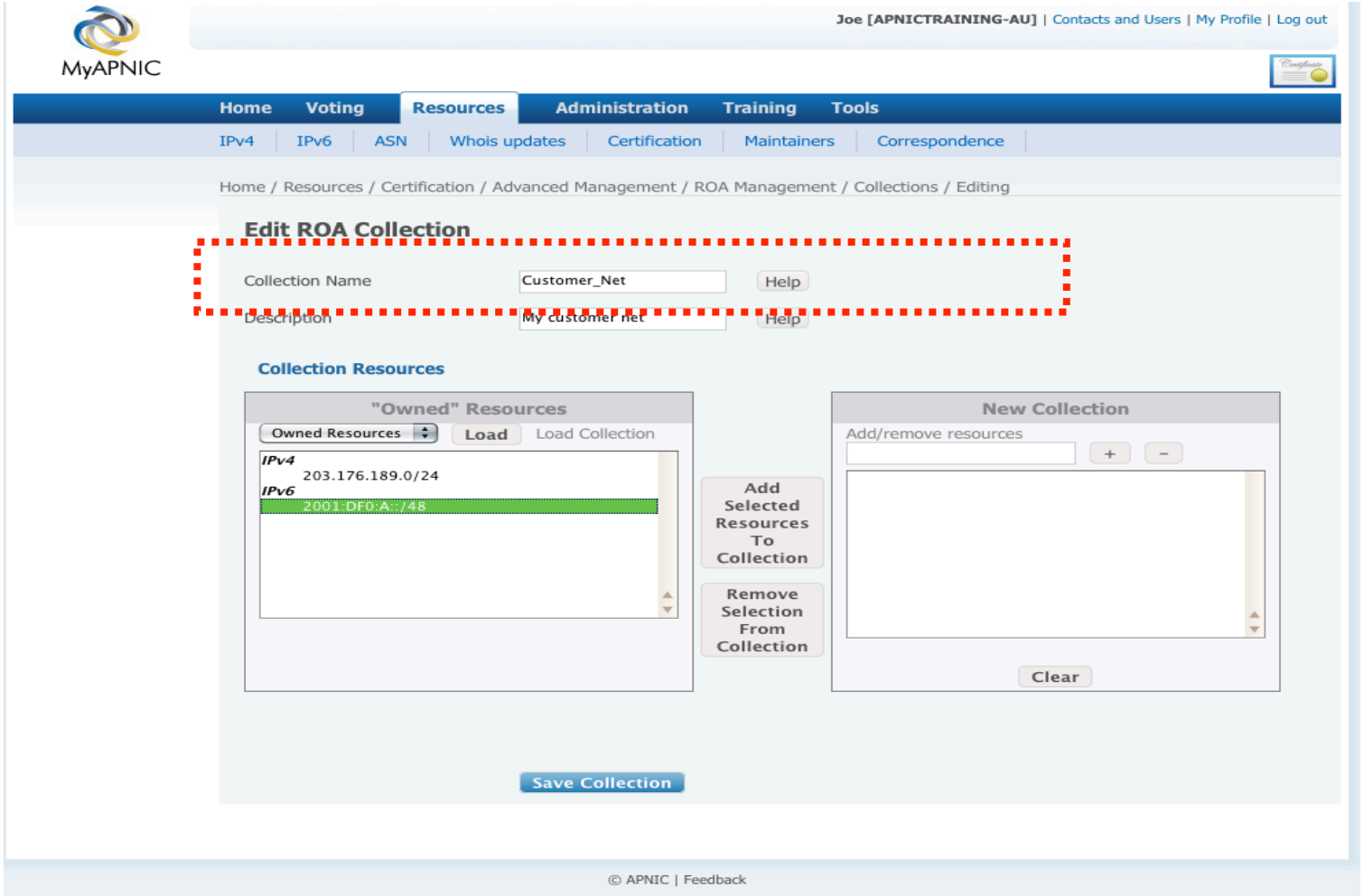
ROA Collection Management



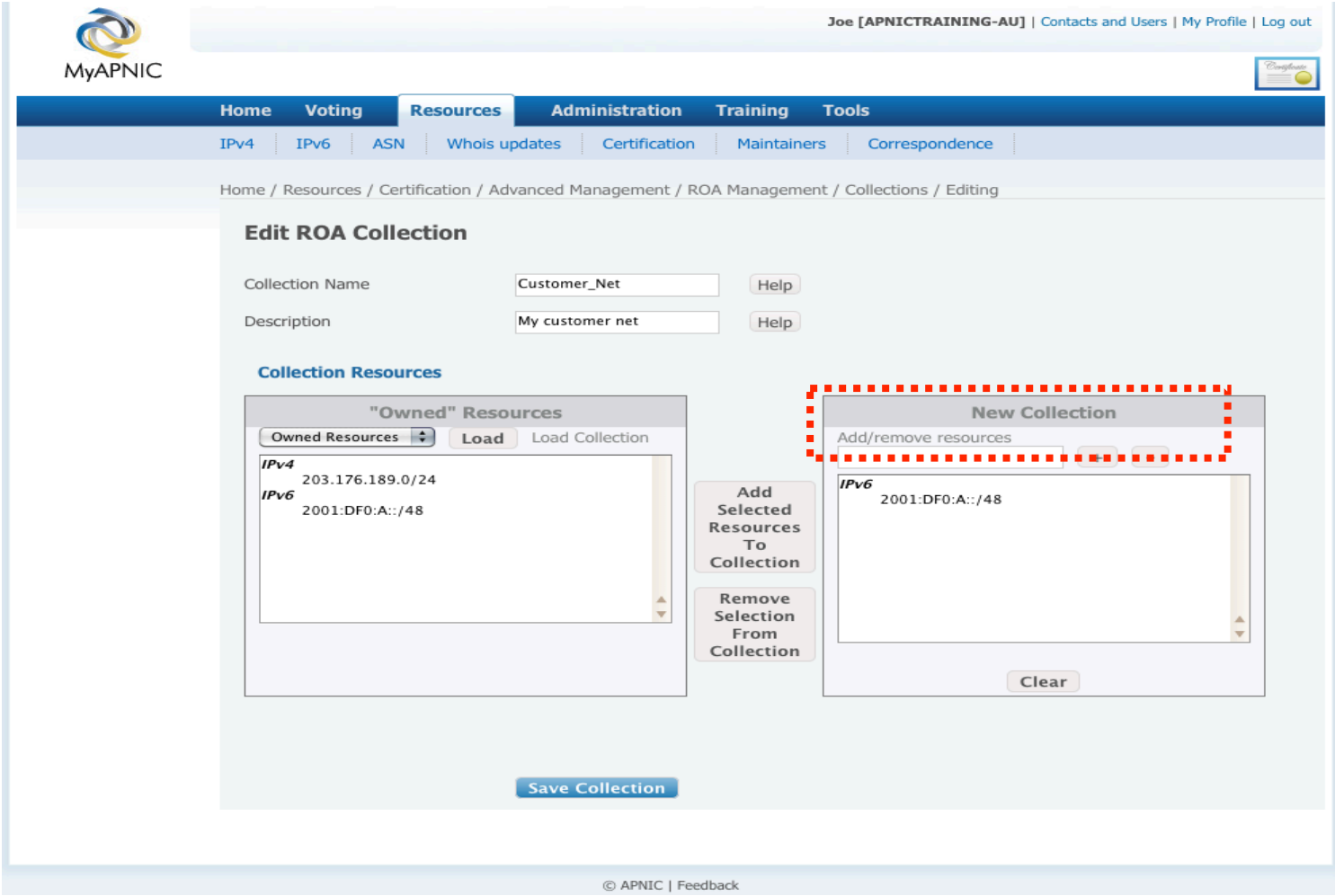
Add ROA Collection



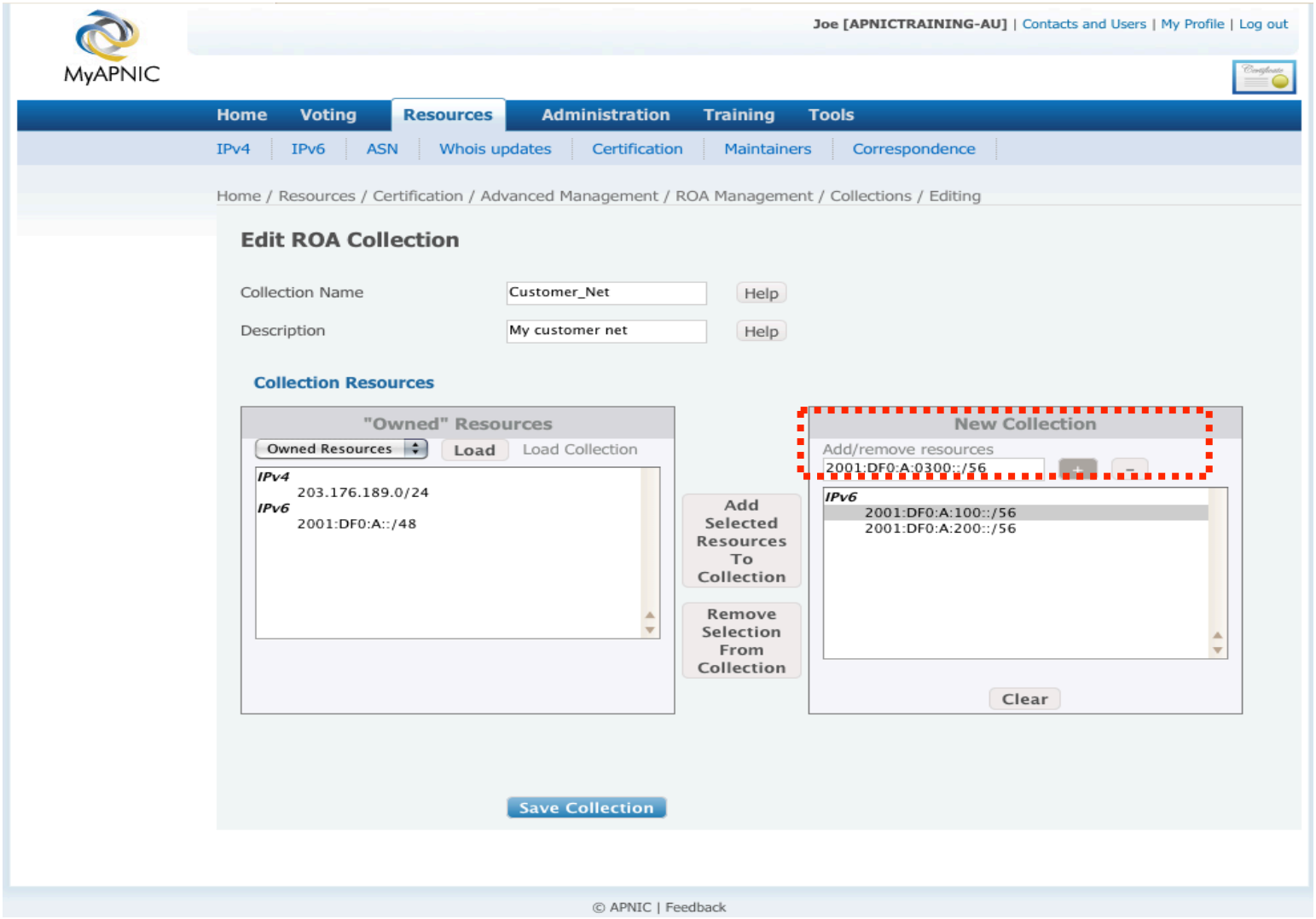
Add ROA Collection



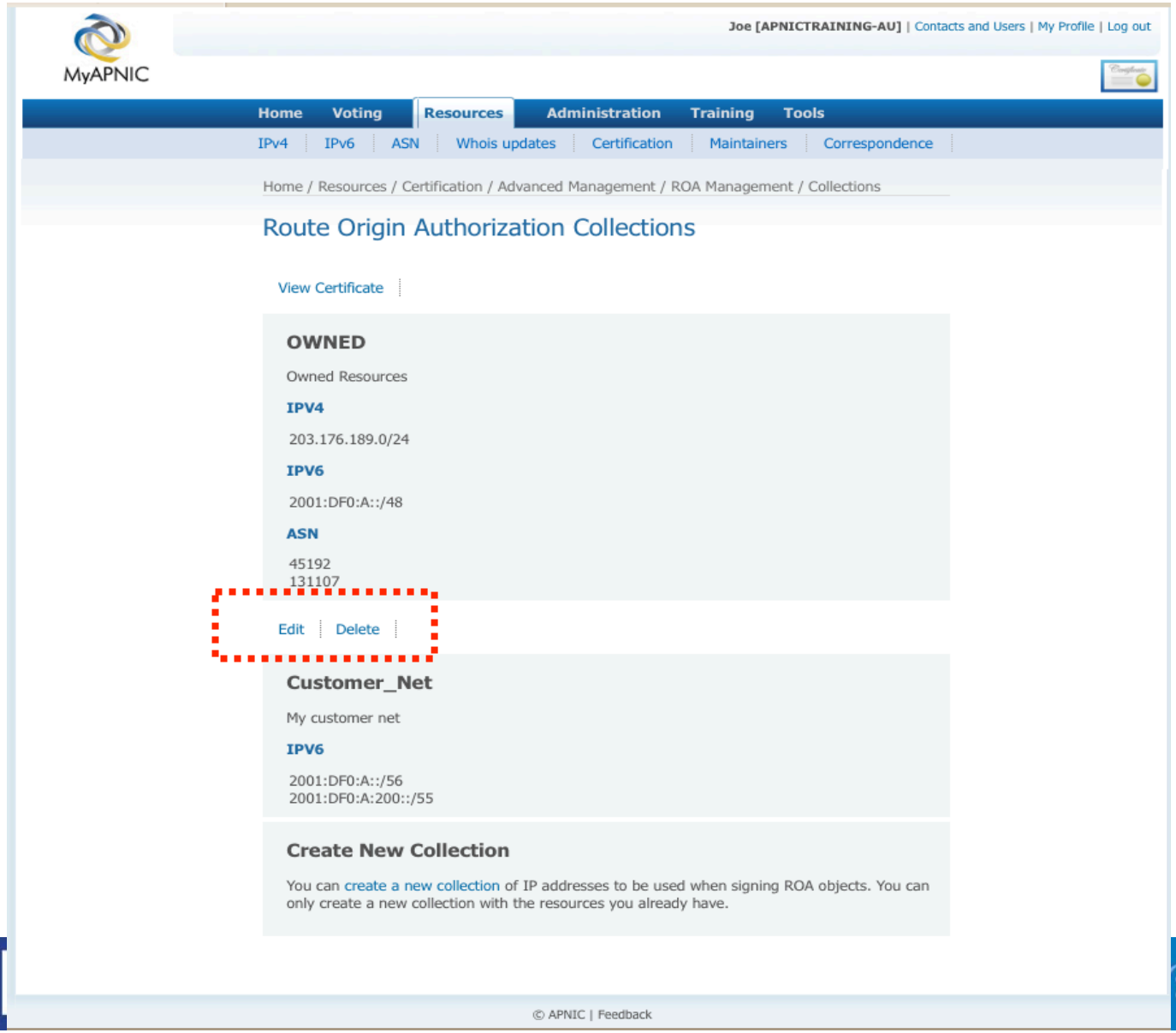
Add ROA Collection



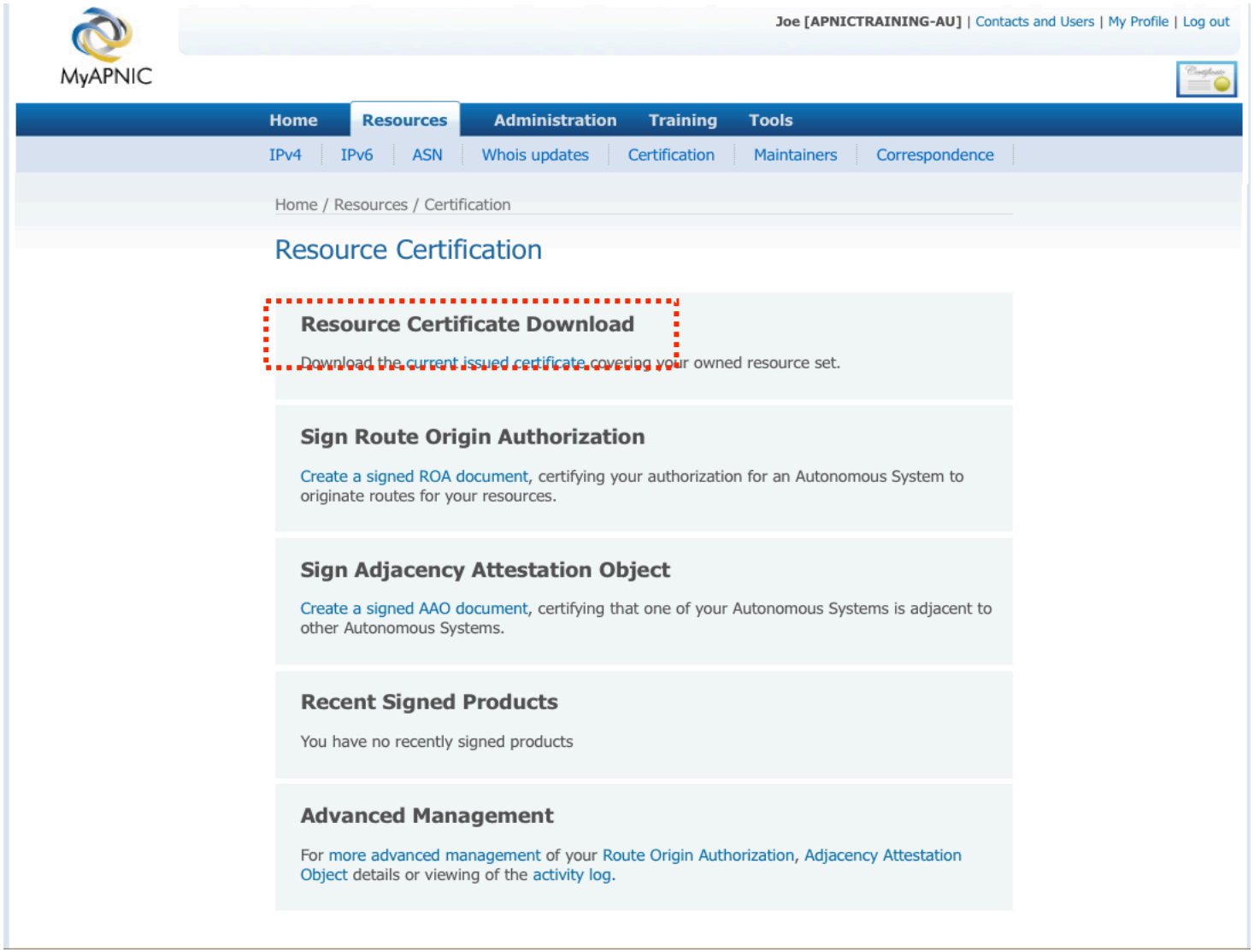
Add/Remove Resources



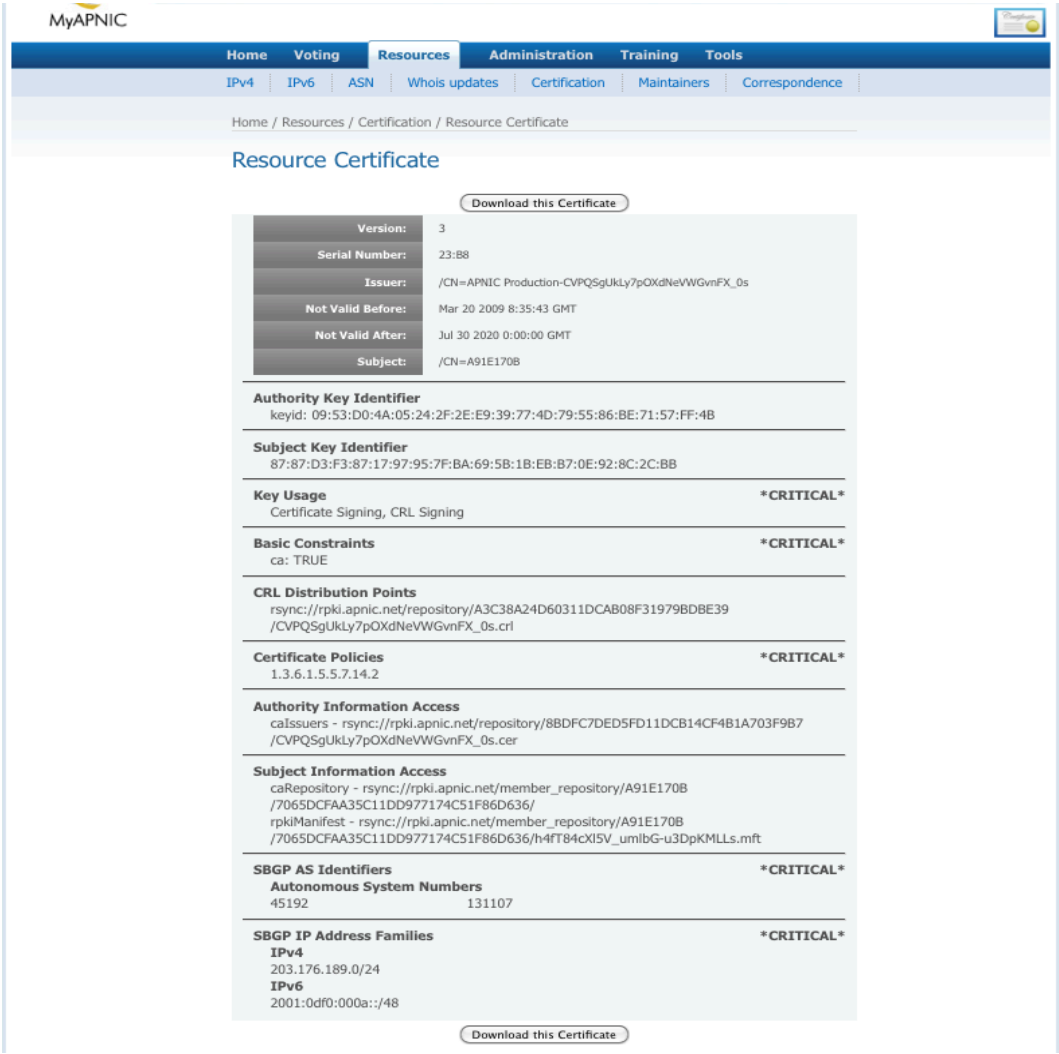
View & Update Collections



Download Certificate



Download Certificate



Questions?

Thank you! ☺

APNIC