Law Enforcement Agency Workshop

Champika Wijayatunga <champika@apnic.net>

03, October, 2013

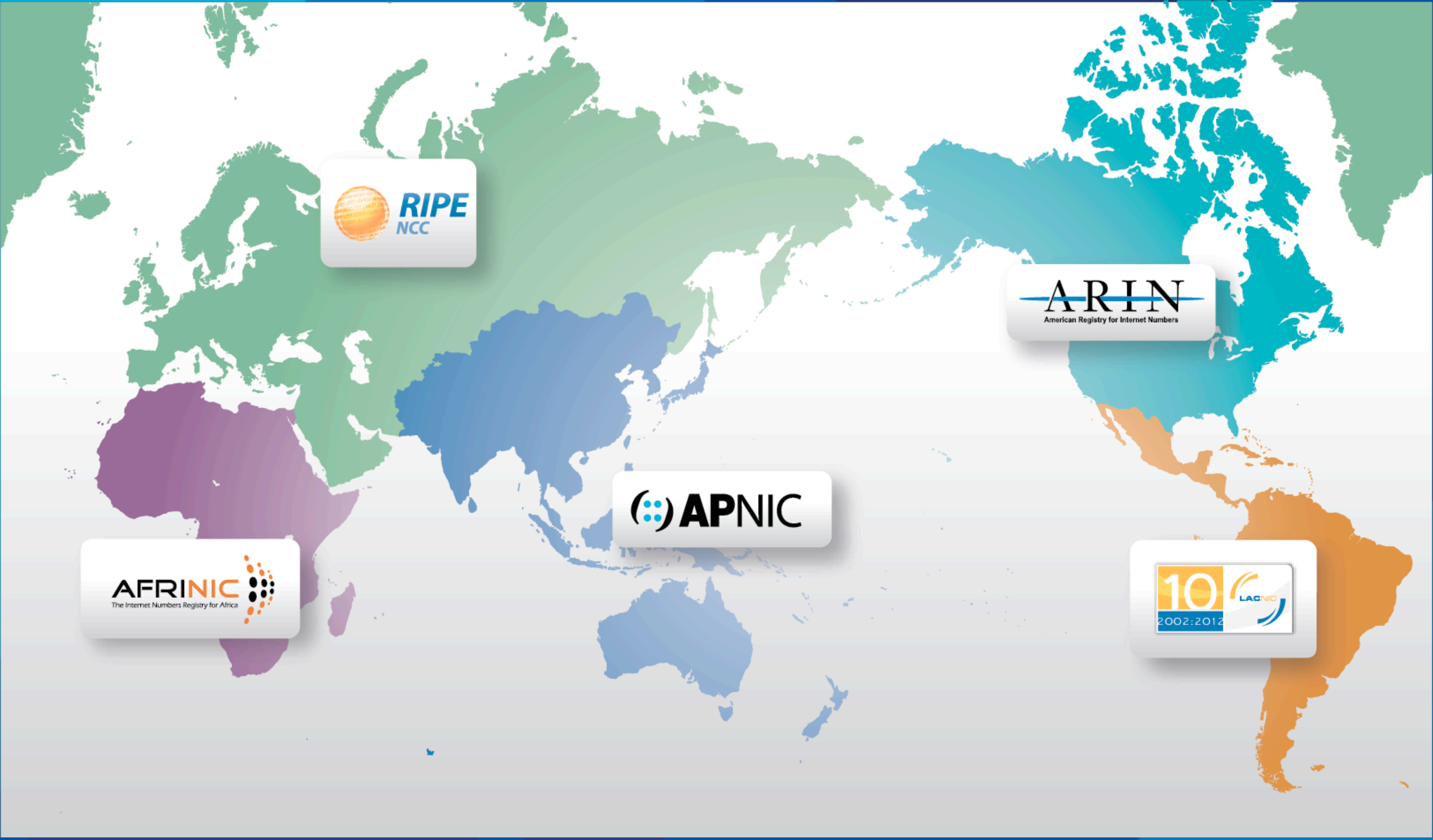
In conjunction with Annual National Cyber Security Week.

APNIC

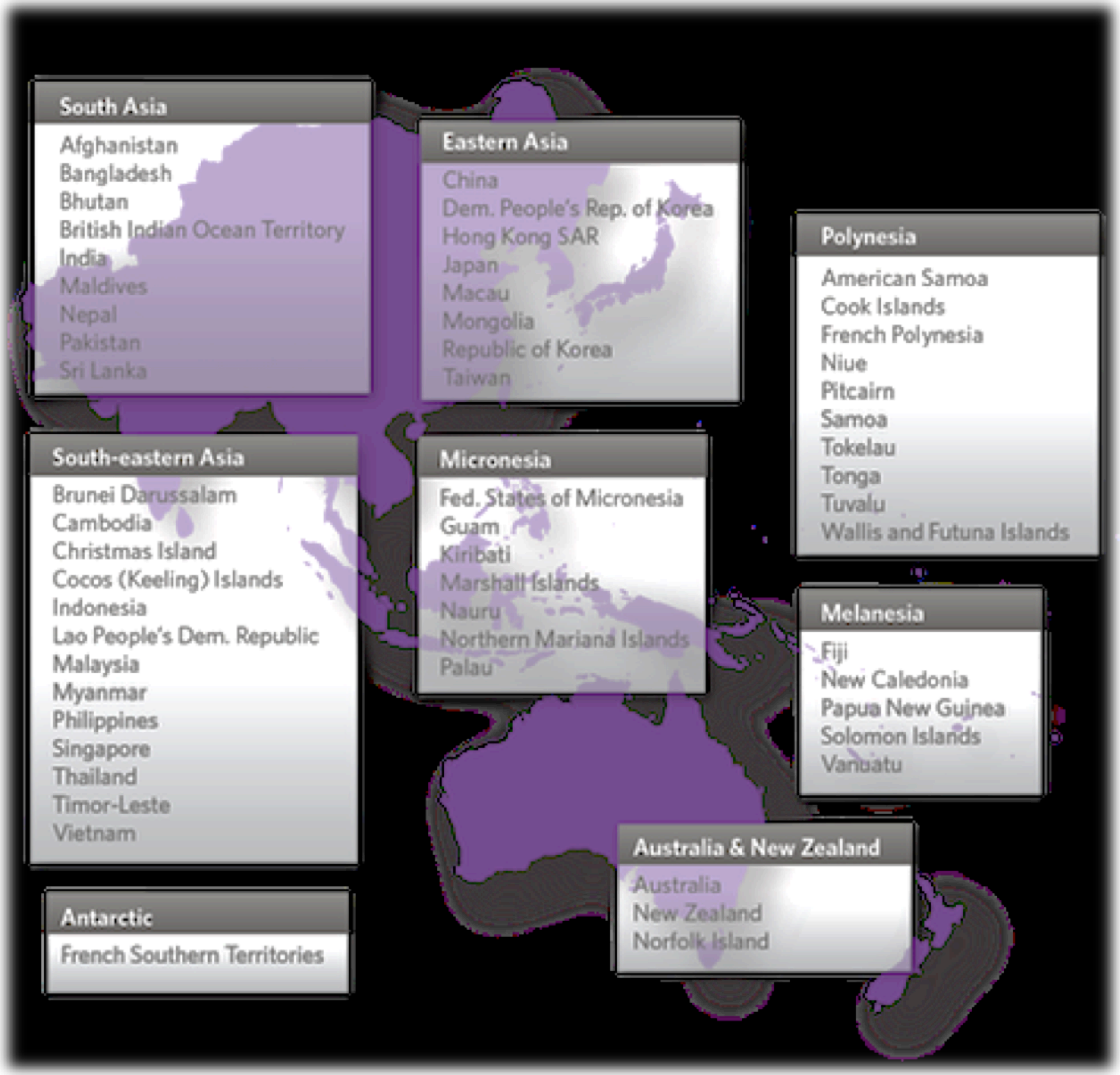
Agenda

- Introduction to APNIC
  - *Know about APNIC*
- Internet Policy Development
  - *How the Internet Policies are developed*
- Internet Challenges Today
  - *How APNIC can assist LEAs*
- Internet Resource Registration
  - *APNIC Whois Database*
- Resource Public Key Infrastructure (RPKI)
  - *How to Secure Routing*

Intro to APNIC


RIPE NCC
ARIN
American Registry for Internet Numbers
AFRINIC
The Internet Numbers Registry for Africa
APNIC
10
LACNIC
2002:2012

The Regional Internet Registry for the Asia Pacific region



South Asia

- Afghanistan
- Bangladesh
- Bhutan
- British Indian Ocean Territory
- India
- Maldives
- Nepal
- Pakistan
- Sri Lanka

Eastern Asia

- China
- Dem. People's Rep. of Korea
- Hong Kong SAR
- Japan
- Macau
- Mongolia
- Republic of Korea
- Taiwan

Polynesia

- American Samoa
- Cook Islands
- French Polynesia
- Niue
- Pitcairn
- Samoa
- Tokelau
- Tonga
- Tuvalu
- Wallis and Futuna Islands

South-eastern Asia

- Brunei Darussalam
- Cambodia
- Christmas Island
- Cocos (Keeling) Islands
- Indonesia
- Lao People's Dem. Republic
- Malaysia
- Myanmar
- Philippines
- Singapore
- Thailand
- Timor-Leste
- Vietnam

Micronesia

- Fed. States of Micronesia
- Guam
- Kiribati
- Marshall Islands
- Nauru
- Northern Mariana Islands
- Palau

Melanesia

- Fiji
- New Caledonia
- Papua New Guinea
- Solomon Islands
- Vanuatu

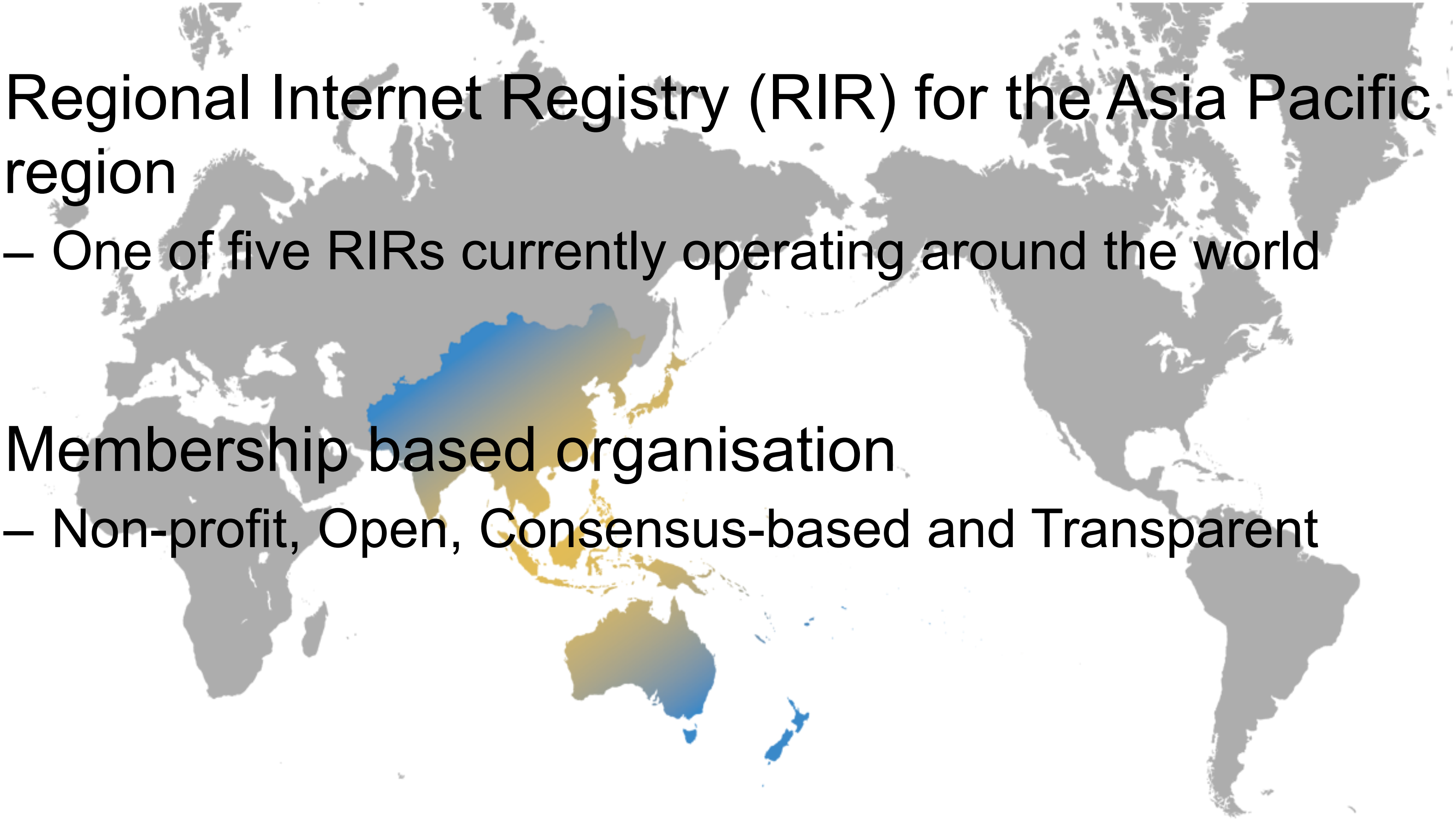
Antarctic

- French Southern Territories

Australia & New Zealand

- Australia
- New Zealand
- Norfolk Island

What is APNIC?



- Regional Internet Registry (RIR) for the Asia Pacific region
  - One of five RIRs currently operating around the world
- Membership based organisation
  - Non-profit, Open, Consensus-based and Transparent

APNIC’s Vision:

A global, open, stable, and secure Internet that serves the entire Asia Pacific community.

How we achieve this:

- Serving Members
- Supporting the Asia Pacific Region
- Collaborating with the Internet Community

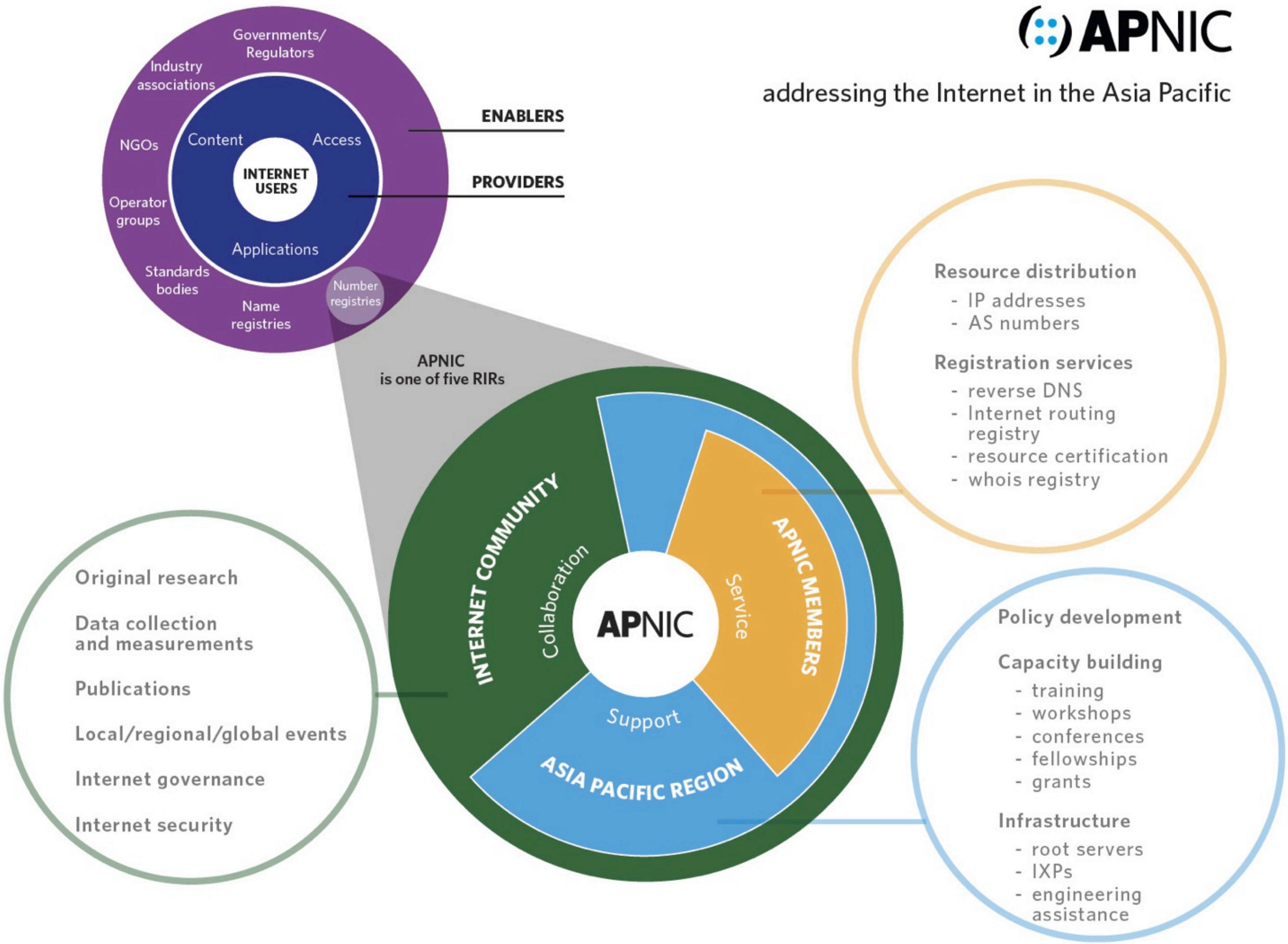
APNIC's Mission

- Function as the Regional Internet Registry for the Asia Pacific, in the service of the community of Members and others
- Provide Internet registry services to the highest possible standards of trust, neutrality, and accuracy
- Provide information, training, and supporting services to assist the community in building and managing the Internet
- Support critical Internet infrastructure to assist in creating and maintaining a robust Internet environment
- Provide leadership and advocacy in support of its vision and the community
- Facilitate regional Internet development as needed throughout the APNIC community

How APNIC support the Internet community

- Distribution and Registration of Internet Resources
- Facilitate the policy development process
  - Via mailing lists, conferences etc.
- Training services
- Information dissemination
- Collaboration & Liaison

APNIC Eco System



APNIC

addressing the Internet in the Asia Pacific

Resource distribution
- IP addresses
- AS numbers

Registration services
- reverse DNS
- Internet routing registry
- resource certification
- whois registry

Original research

Data collection and measurements

Publications

Local/regional/global events

Internet governance

Internet security

Policy development

Capacity building
- training
- workshops
- conferences
- fellowships
- grants

Infrastructure
- root servers
- IXPs
- engineering assistance

Assisting LEAs

- APNIC has a fundamental role to play in the stability and security of the Internet, ensuring that the services we provide such as the APNIC Whois Database and Reverse DNS zone delegations are accurate, reliable, and up-to-date.
- LEAs are an important segment of the APNIC community. We collaborate, cooperate, and work together with them to ensure the Internet remains an open, secure, and stable platform
- Data from the Whois may be a source of information for the LEAs in our community.
- APNIC encourages the LEAs to participate in the APNIC Policy Development Process, and have your voices heard on issues that are important to you!

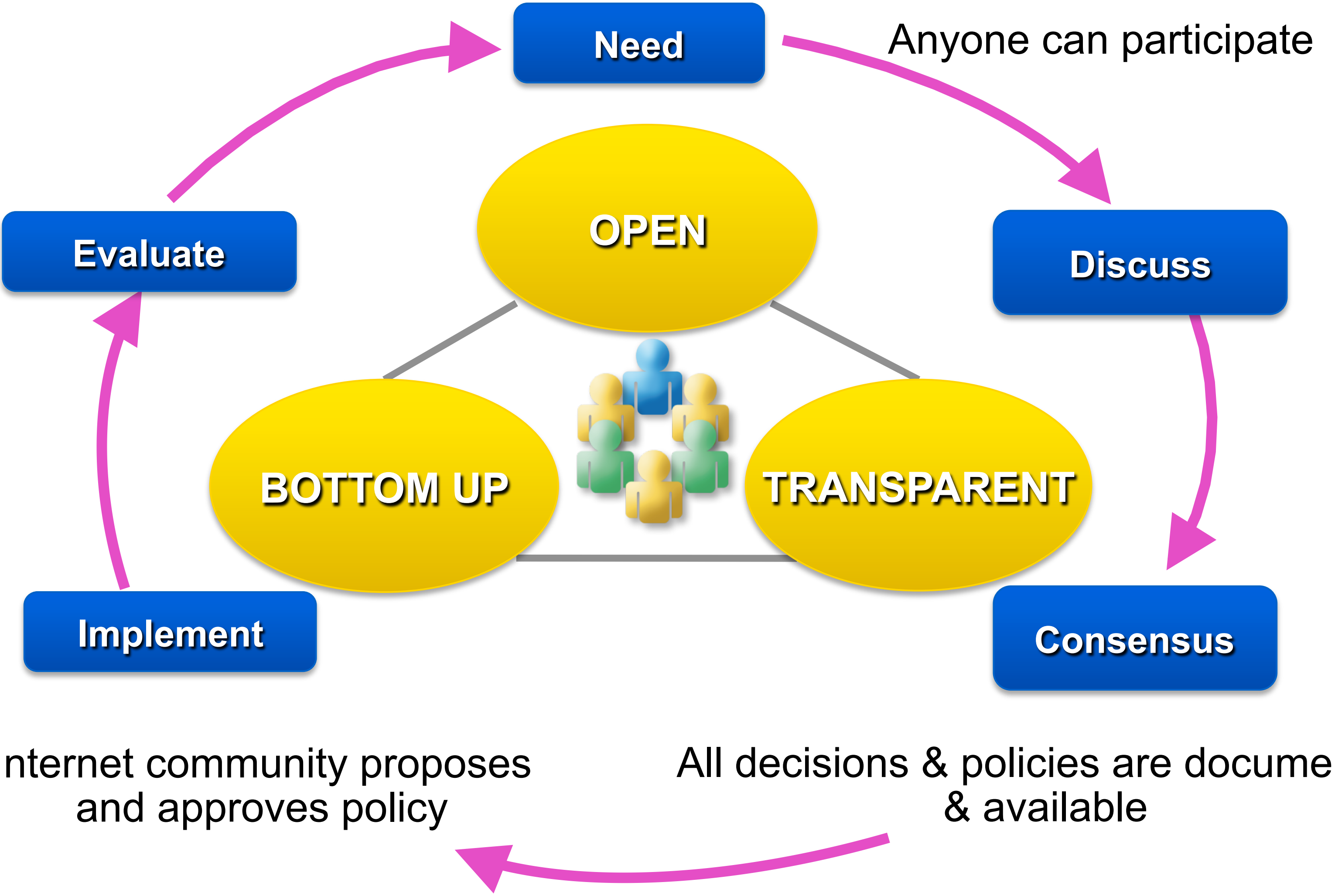
Internet Policy Development

APNIC

Internet Policies

- Policies are constantly changing the meet the needs of the Internet operation
- There is a system in place called the Policy Development Process
  - Anyone can participate
  - Anyone can propose a policy
  - All decisions & policies documented & freely available to anyone

Policy Development Process



Anyone can participate

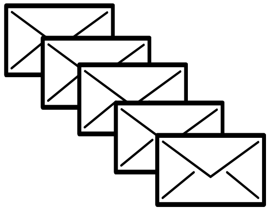
Internet community proposes and approves policy

All decisions & policies are documented & available

How APNIC can help you?

Internet Challenges Today

- Internet Security
  - Unauthorized Intrusions
  - Denial of Service (DoS) Attacks
  - Internal Attacks
  - Non-compliance etc.



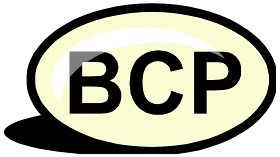
- Spam
  - Unsolicited Commercial Email (UCE) & Unsolicited Bulk Email (UBE)
  - Spam volume is exploding
- Network abuse
  - RIR’s do not regulate conduct of Internet activity
  - Investigation possibilities
    - Cooperation of the network administrators
    - Law enforcement agencies

APNIC Service offerings

- Whois Database – *an important resource!*
  - Troubleshooting
  - Tracking source of abuse
  - Protecting address space to prevent hijacking

- Information dissemination
  - APNIC Conferences
    - Technical talks & tutorials
  - Publications & Research

- Education
  - Training courses, Workshops and Seminars



Steps we take to ensure Whois accuracy

- Member account opening
  - verification of corporate existence with corporate registries or regulators (where possible)
- Membership renewal
  - once a year
  - email to corporate contact, with payment record
  - Internet resources revoked if account not paid or renewed
- Transfer policies
  - encourage registration of resources
  - “value” of Internet resources encourage registration

Efforts in Preventing Network Abuse

- As a registry, APNIC **adopts and applies policies** for it’s community which address network abuse. APNIC does not have the capacity to investigate abuse complaints or the legal powers to regulate Internet activity.

- APNIC seeks to raise awareness of the need for **responsible network management in the Asia Pacific**, through training and communication.

Why APNIC appear as the source in some abuse search reports?

- Some designed to search the ARIN Whois database and may refer to APNIC as the culprit
- Many websites with Whois lookup functions has the same limitations
- However the IP addresses are registered by five RIRs on a regional basis

Detecting the Abuse

- If a standard search refers you to APNIC
  - It means only that the network in question is registered in the Asia Pacific region
  - Does not mean that APNIC is responsible or that the hacker/spammer is using APNIC network

Can APNIC stop Abuse?

- No, because…
  - APNIC is not an ISP and does not provide network connectivity to other networks
  - APNIC does not control Internet routing
  - APNIC is not a law enforcement agency
  - APNIC has no industry regulatory power

Investigation of Complaints

- Laws relating to network abuse vary from country to country
- Investigation possibilities
  - Cooperation of the network administrators
  - Law enforcement agencies
    - Local jurisdiction
    - Jurisdiction where the problem originates

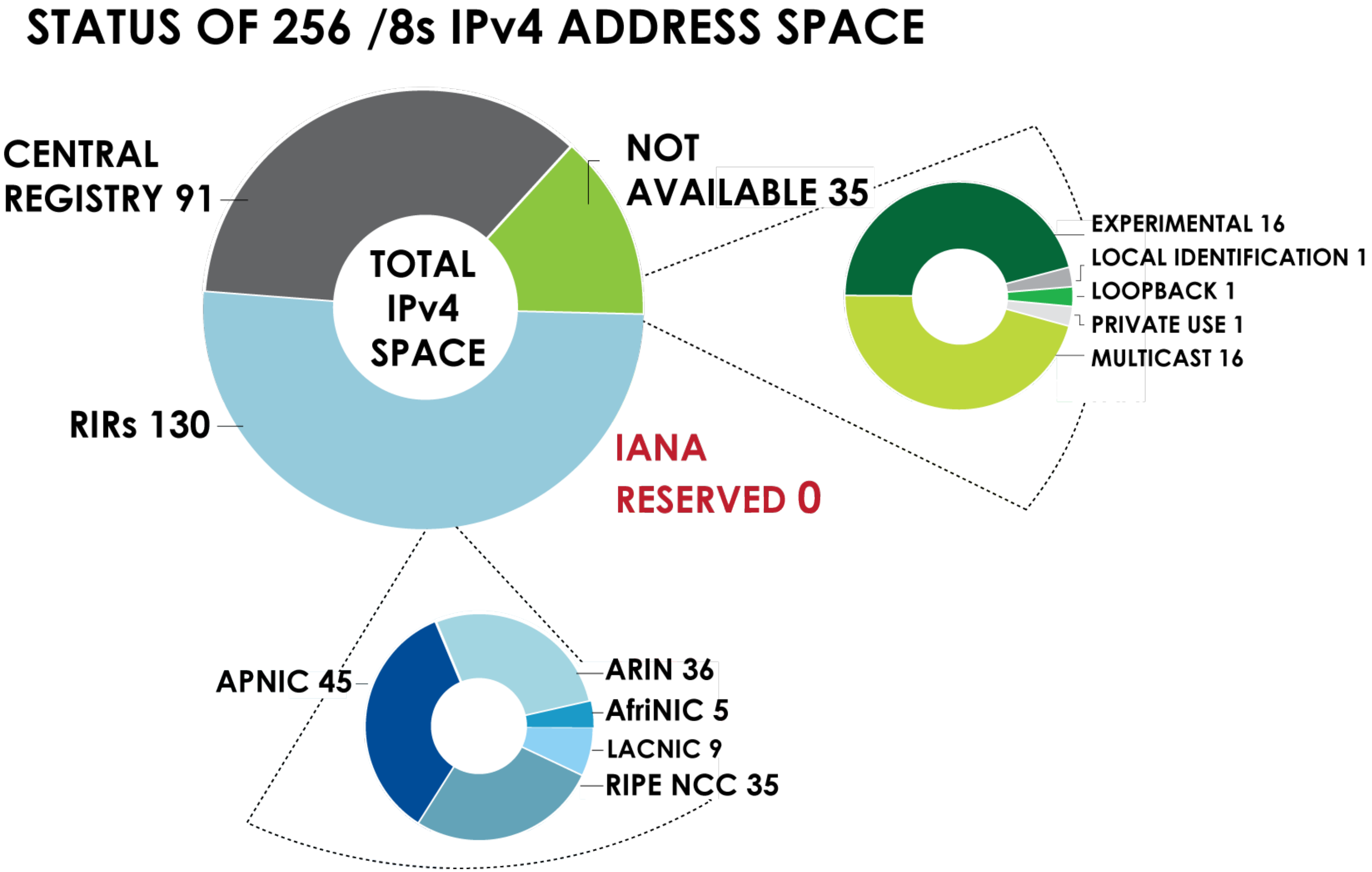
What can you do?

- Use the APNIC Whois Database to obtain network contact information
- APNIC Whois may or may not show specific customer assignments for the addresses in question
  - But will show the ISP holding APNIC space
- Contact the network responsible and also its ISP/upstream
- Contact APNIC for help, advice, training or support
- Community discussions can be raised in the APNIC conferences, mailing lists, etc.

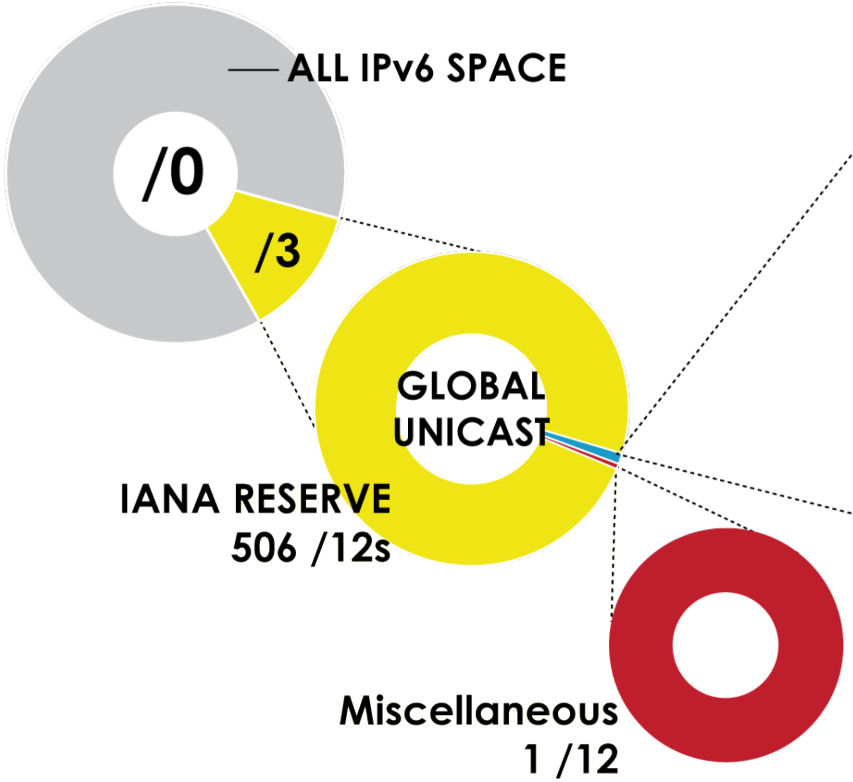
Managing Internet Resources

APNIC

IPv4 Address Space



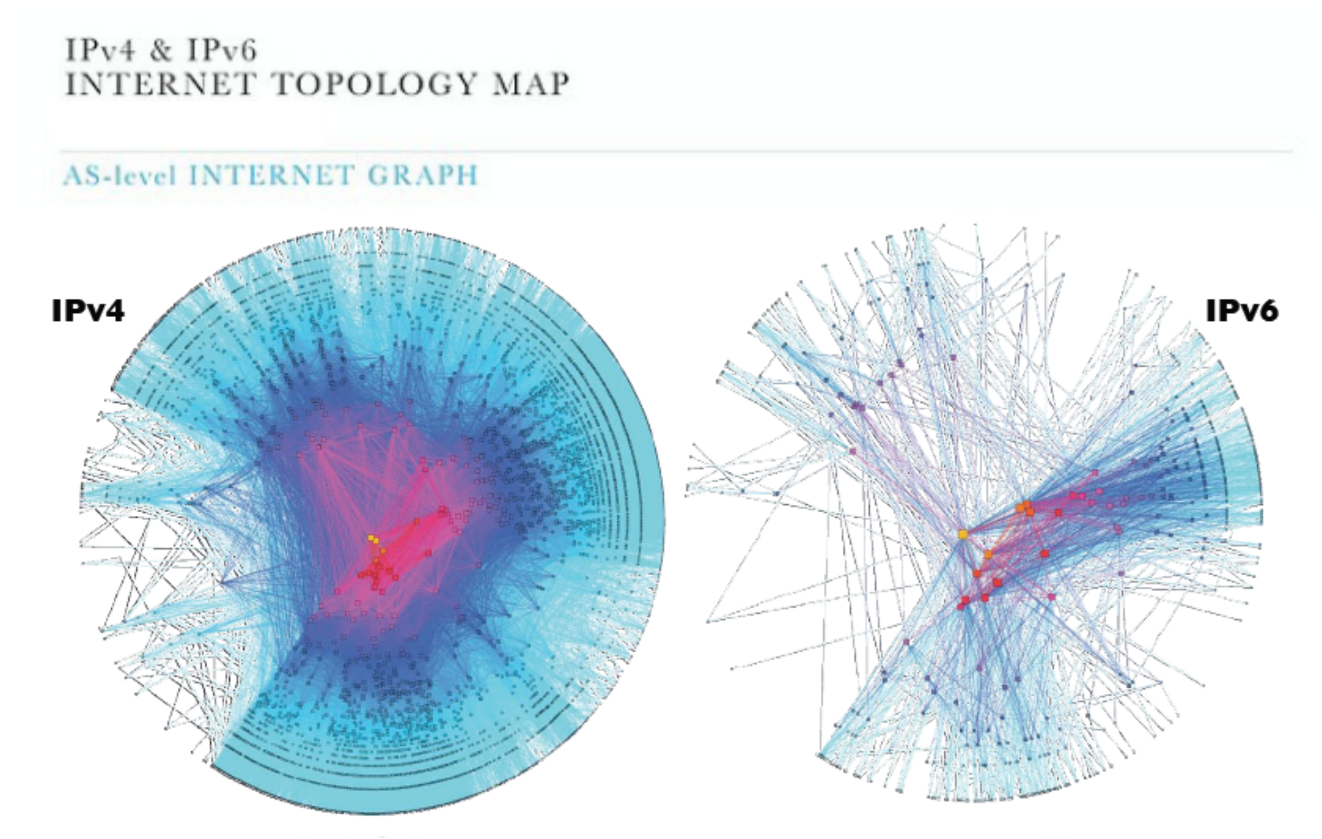
IPv6 Address Space



RIRs 5 /12s (October 2006)

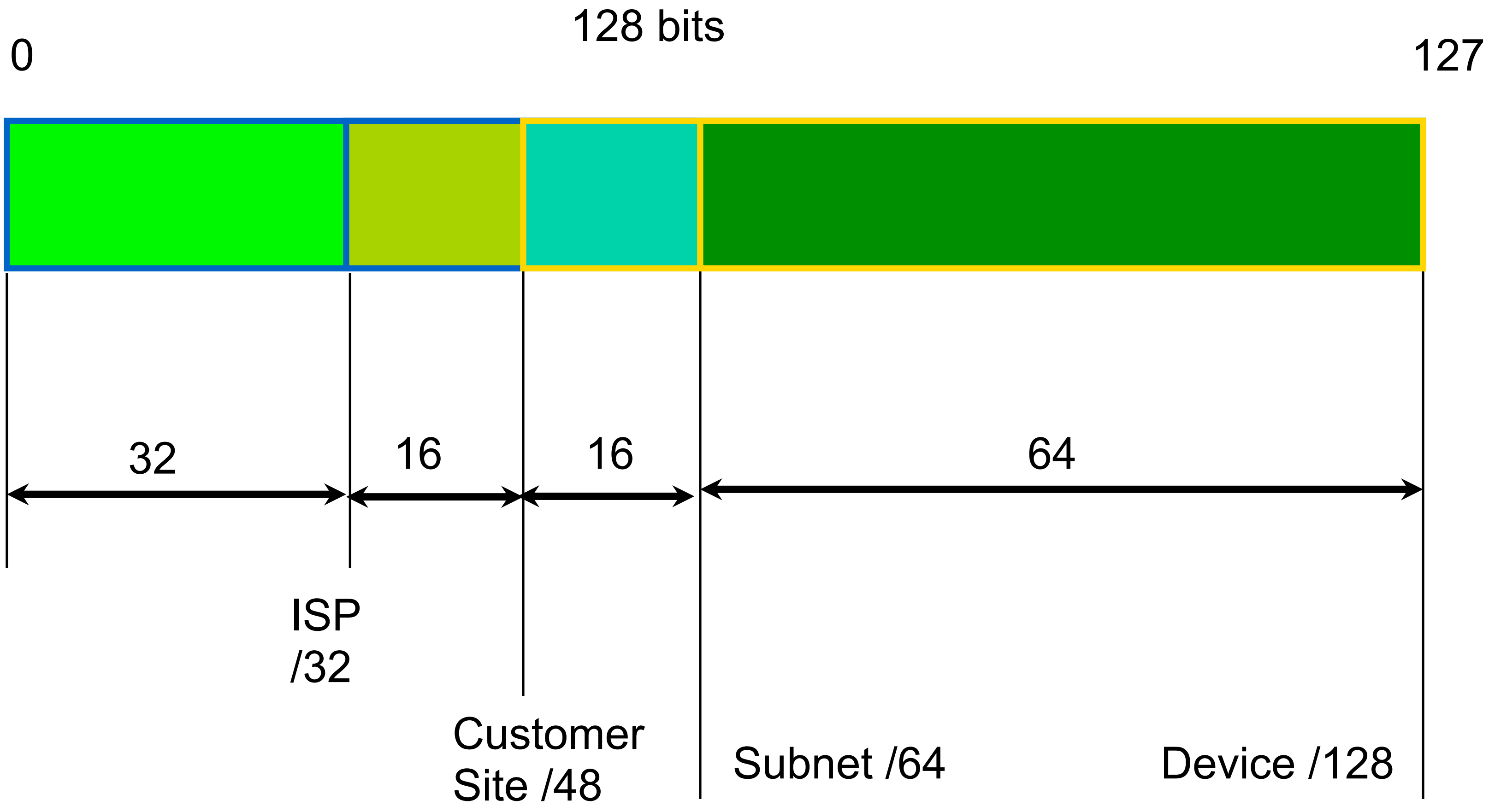
RIR	IPv6 ADDRESS
AfriNIC	2C00:0000::/12
APNIC	2400:0000::/12
ARIN	2600:0000::/12
LACNIC	2800:0000::/12
RIPE NCC	2A00:0000::/12

IPv4 vs IPv6 Internet

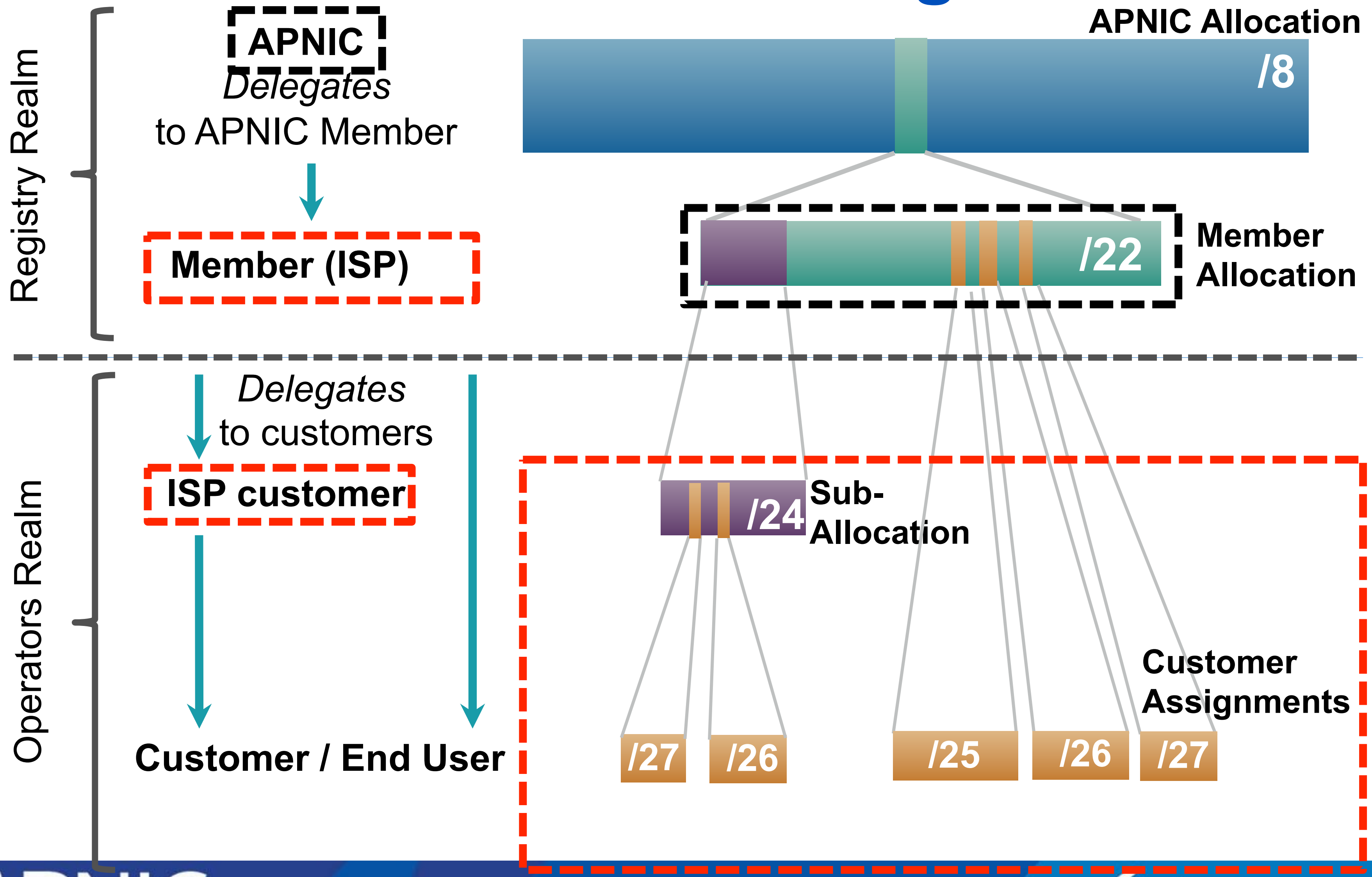


Source: CAIDA

IPv6 Addressing Structure



How IP Addresses are Delegated



Registry Realm

APNIC

Delegates

to APNIC Member

Member (ISP)

Operators Realm

Delegates

to customers

ISP customer

Customer / End User

APNIC Allocation

/8

/22

Member Allocation

/24

Sub-Allocation

/27

/26

/25

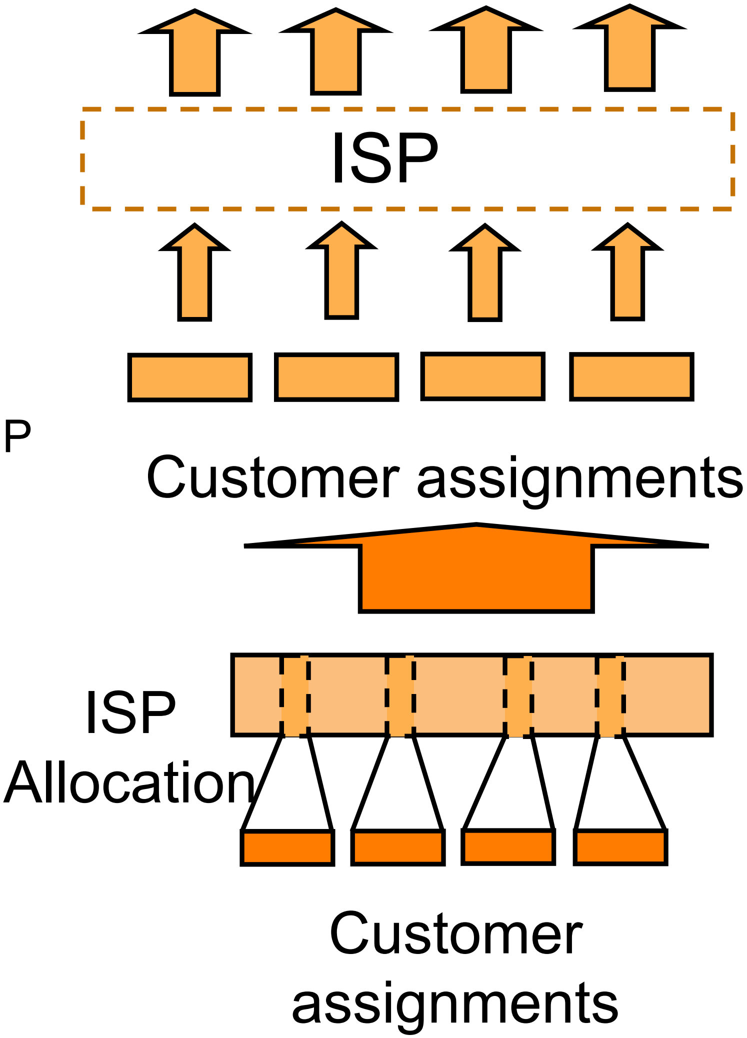
/26

/27

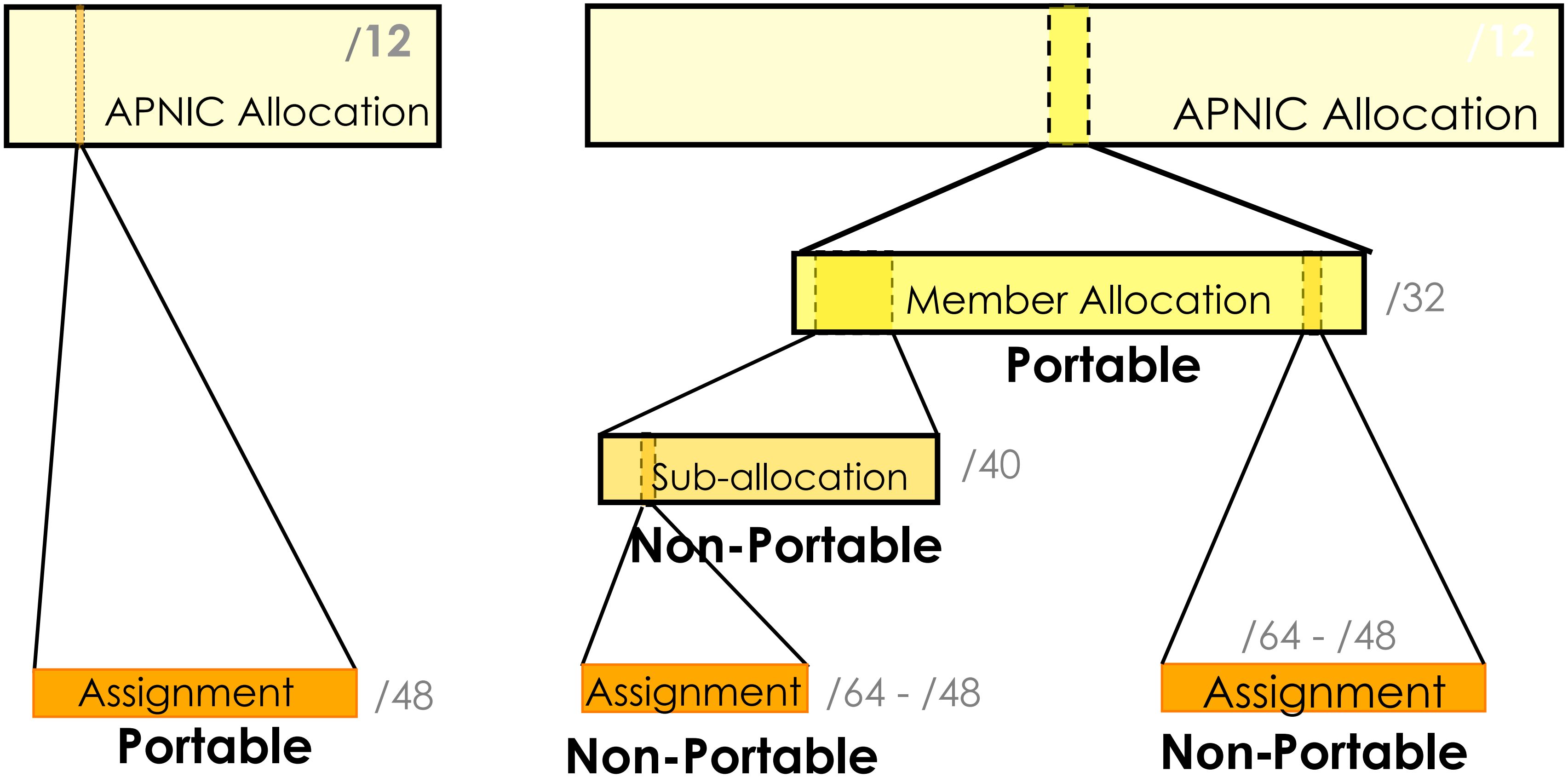
Customer Assignments

IP Address Management

- Portable Allocations
  - Allocations made by APNIC
- Non Portable Allocations
  - Allocations made by APNIC Members
- Portable Assignments
  - Customer addresses independent from ISP
  - Keeps addresses when changing ISP
  - Bad for size of routing tables
  - Bad for QoS: routes may be filtered, flap-dampened
- Non-portable Assignments
  - Customer uses ISP's address space
  - Must renumber if changing ISP
  - Helps scale the Internet effectively



Address Management Hierarchy



Describes "portability" of the address space

Transferring IP Addresses

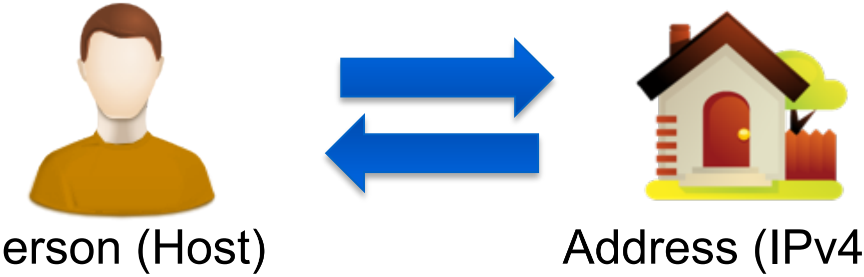
- Transfers, Mergers, Acquisitions are possible
- There are transfer policies exists to transfer IP addresses
  - In the APNIC region
  - Inter-RIR IPv4 Transfers
    - Conditions on the source and recipient RIR will apply
- APNIC will review the status of IP allocations

APNIC Resource Quality Assurance

- Community awareness
- Build relationships with reputable organizations that maintain bogon/black list
- Keep the WHOIS Database accurate
  - Actively remind resource holders to update their data

APNIC also manages Reverse DNS

- ‘Forward DNS’ maps names to numbers
  - svc00.apnic.net ➔202.12.28.131
- ‘Reverse DNS’ maps numbers to names
  - 202.12.28.131 ➔ svc00.apnic.net

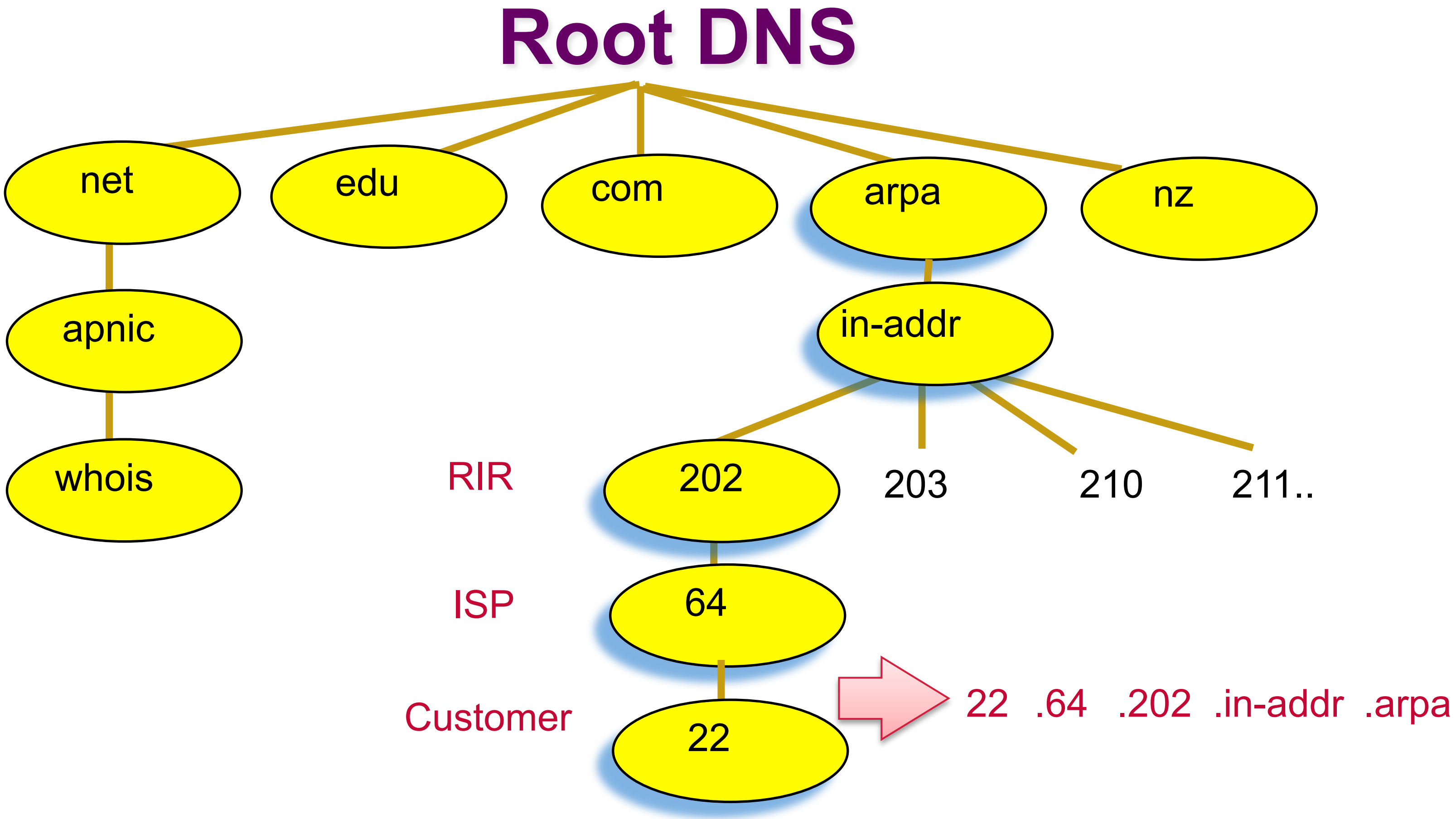


Reverse DNS - why bother?

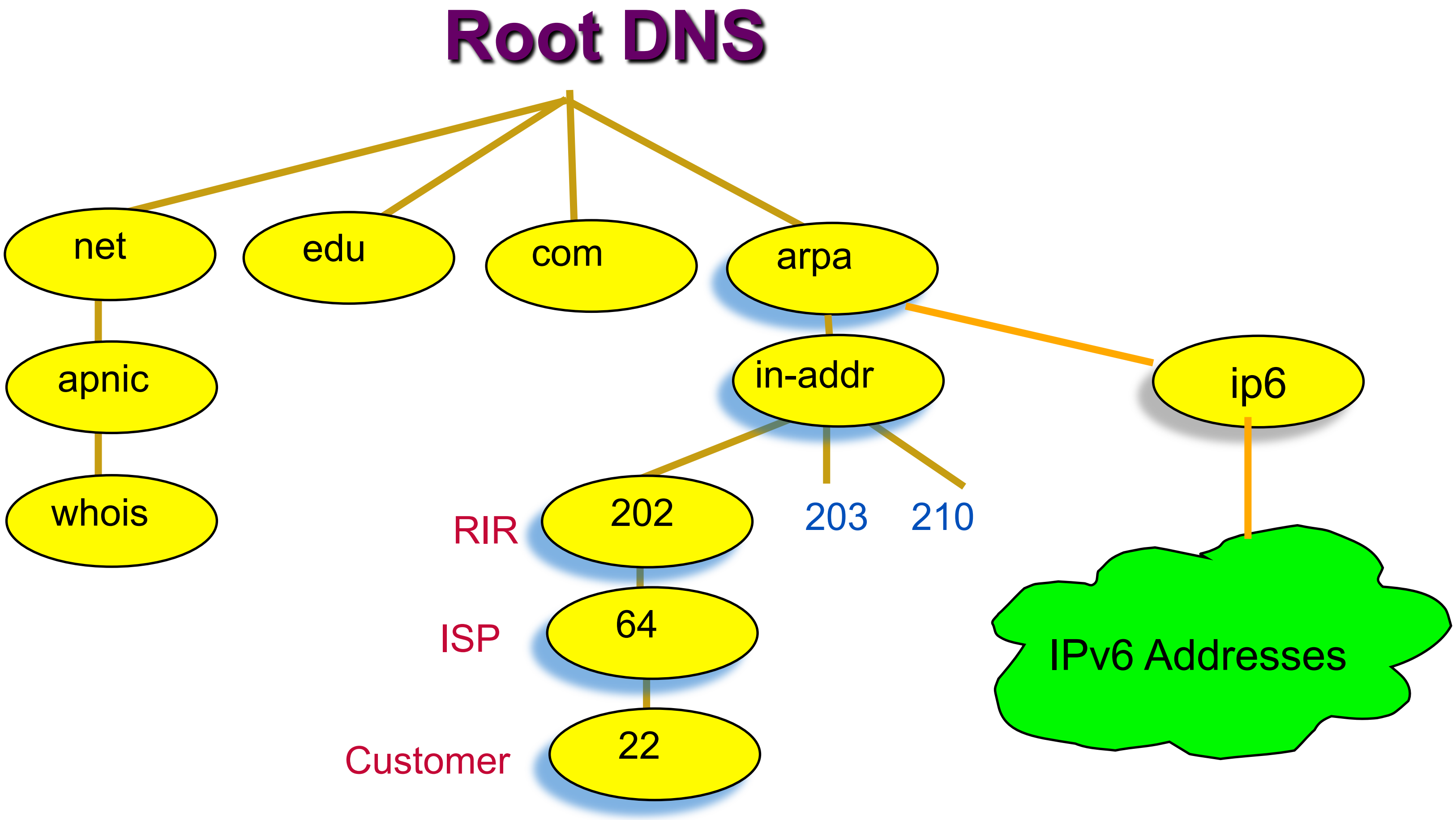
- Service denials
  - That only allow access when fully reverse delegated
- Diagnostics
  - Assisting in network troubleshooting
- Spam prevention
  - Reverse lookup to confirm the mail servers and source of the email
  - Failed lookup adds to an email’s spam score
- Registration responsibilities

Principles – DNS Tree

Mapping numbers to names - ‘reverse DNS’



Reverse DNS Tree – with IPv6



The APNIC Whois Database

The APNIC Whois Database

- Holds IP address records within the AP region
- Can use this database to track down the source of the network abuse
  - IP addresses, ASNs, Reverse Domains, Routing policies
- Can find contact details of the relevant network administrators
  - not the individual users
  - use administrators log files to contact the individual involved

Resource Registration

- As part of the membership agreement with APNIC, all members are required to register their resources in the APNIC Whois database.
- Members must keep records up to date:
  - Whenever there is a change in contacts
  - When new resources are received
  - When resources are sub-allocated or assigned

Whois Object Types

OBJECT	**PURPOSE**
person	contact persons
role	contact groups/roles
inetnum	IPv4 addresses
Inet6num	IPv6 addresses
aut-num	Autonomous System number
domain	reverse domains
route	prefixes being announced
mntner	(maintainer) data protection
mnt-irt	Incident Response Team

http://www.apnic.net/db/

How to use APNIC Whois

- Web browser
  - http://www.apnic.net/whois
- Whois client or query tool
  - whois.apnic.net
- Identify network contacts from the registration records
  - IRT (Incident Response Team) if present
  - Contact persons: “tech-c” or “admin-c”

What if Whois info is invalid?

- Members (ISPs) are responsible for reporting changes to APNIC
  - Under formal membership agreement
- Report invalid ISP contacts to APNIC
  - http://www.apnic.net/invalidcontact
  - APNIC will contact member and update registration details

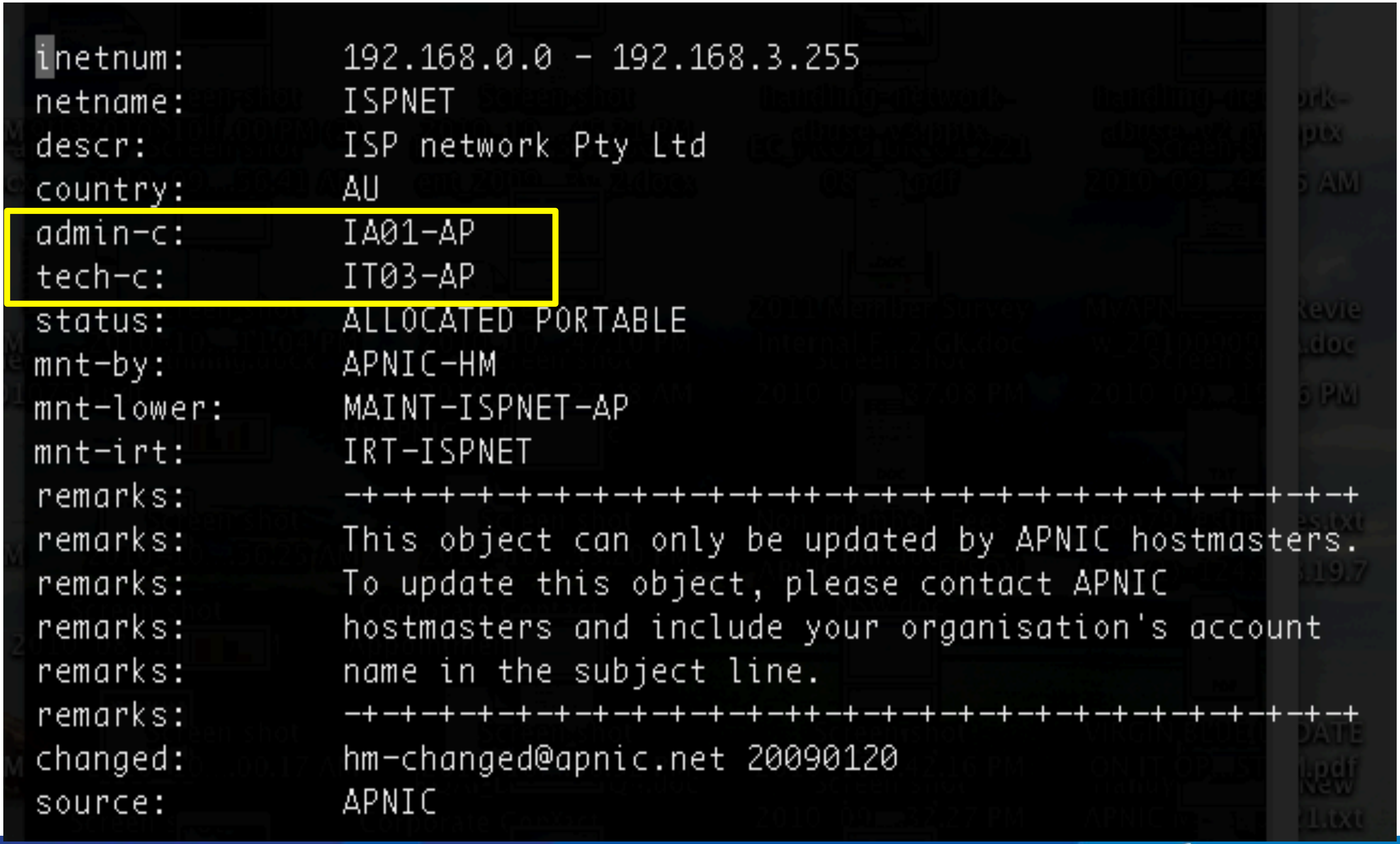
What if Whois info is invalid?

- Customer assignment information is the responsibility of ISPs
  - ISPs are responsible for updating their customer network registrations
- Tools such as ‘traceroute’, ‘looking glass’ and RIS may be used to track the upstream provider if needed
  - More information available from APNIC

Inetnum / Inet6num Objects

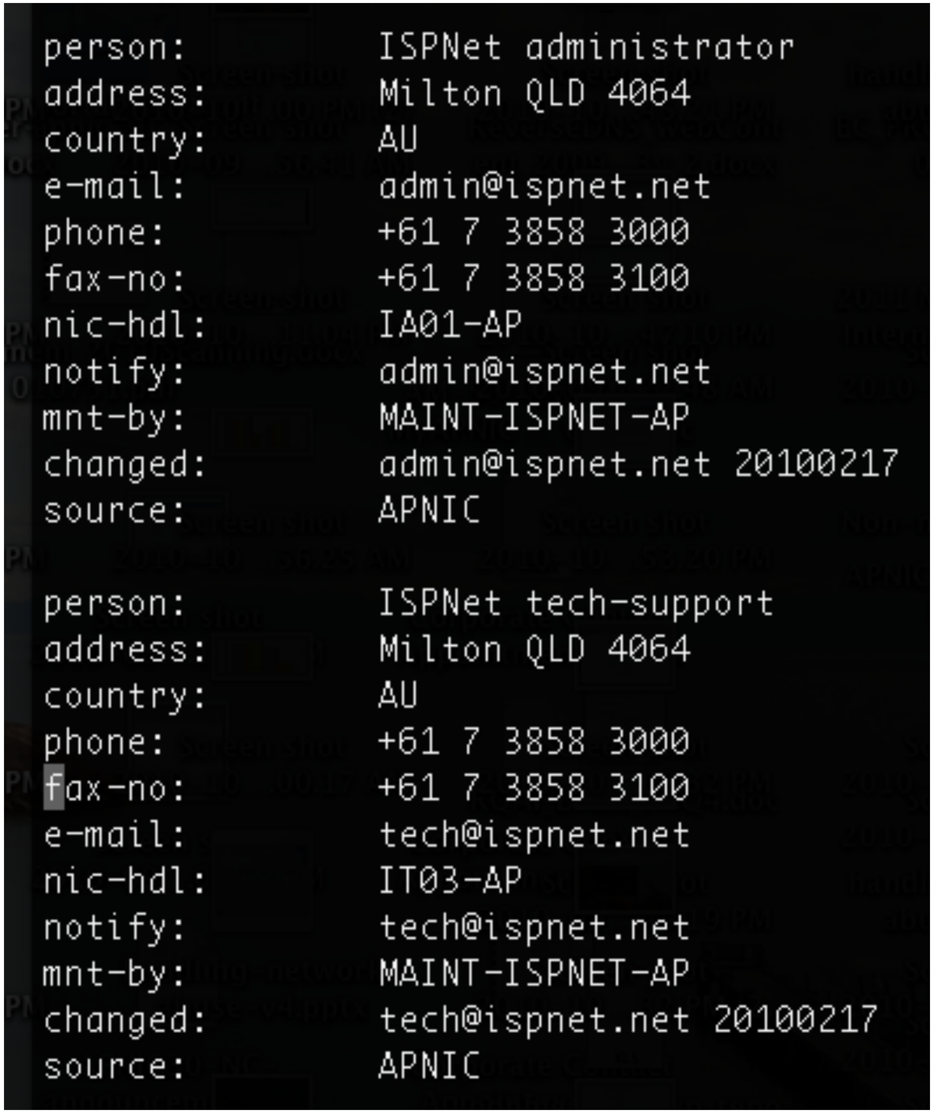
- Contains IP allocation and assignment information
- APNIC creates an inetnum (or inet6num) object for each allocation or assignment they make to the Member
- All members must create inetnum (or inet6num) objects for each sub-allocation or assignment they make to customers

APNIC Whois Registration



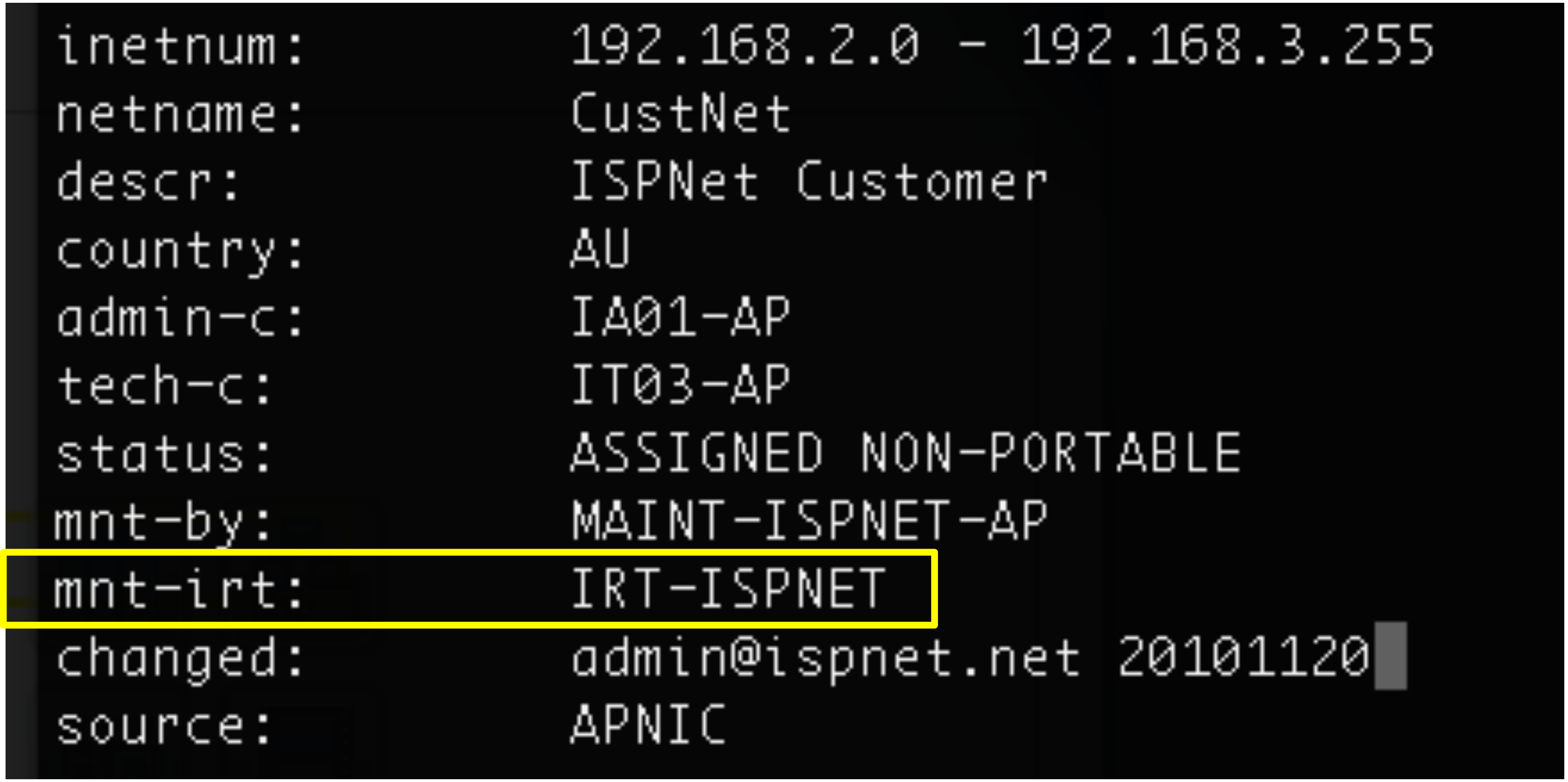
```
inetnum:        192.168.0.0 - 192.168.3.255
netname:        ISPNET
descr:          ISP network Pty Ltd
country:        AU
admin-c:        IA01-AP
tech-c:         IT03-AP
status:         ALLOCATED PORTABLE
mnt-by:         APNIC-HM
mnt-lower:      MAINT-ISPNET-AP
mnt-irt:        IRT-ISPNET
remarks:        -+-+-+-+-+-+-+-+-+-+-+-++-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
remarks:        This object can only be updated by APNIC hostmasters.
remarks:        To update this object, please contact APNIC
remarks:        hostmasters and include your organisation's account
remarks:        name in the subject line.
remarks:        -+-+-+-+-+-+-+-+-+-+-+-++-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
changed:        hm-changed@apnic.net 20090120
source:         APNIC
```

APNIC Whois Registration



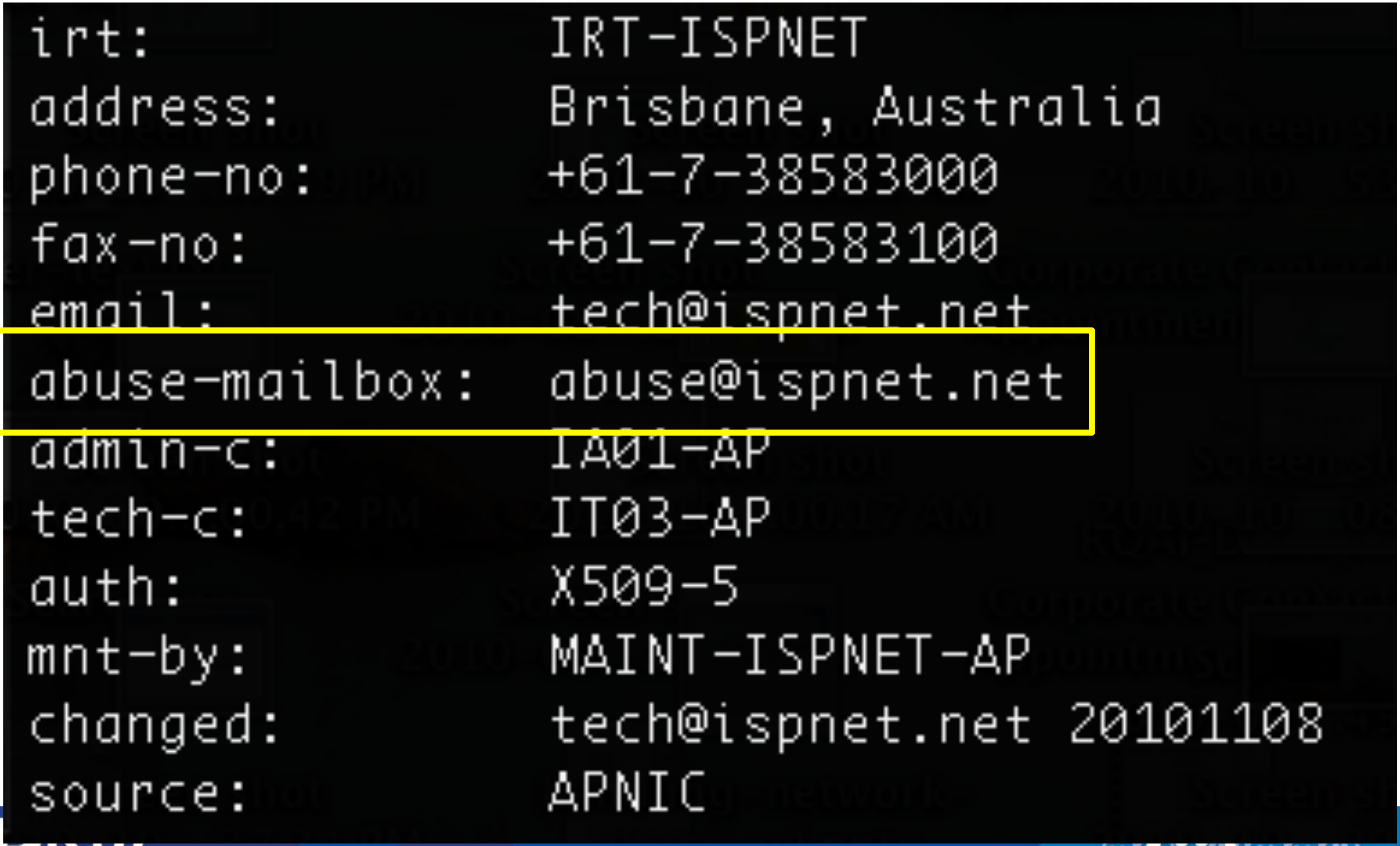
```
person:          ISPNet administrator
address:         Milton QLD 4064
country:         AU
e-mail:          admin@ispnet.net
phone:           +61 7 3858 3000
fax-no:          +61 7 3858 3100
nic-hdl:         IA01-AP
notify:          admin@ispnet.net
mnt-by:          MAINT-ISPNET-AP
changed:         admin@ispnet.net 20100217
source:          APNIC

person:          ISPNet tech-support
address:         Milton QLD 4064
country:         AU
phone:           +61 7 3858 3000
fax-no:          +61 7 3858 3100
e-mail:          tech@ispnet.net
nic-hdl:         IT03-AP
notify:          tech@ispnet.net
mnt-by:          MAINT-ISPNET-AP
changed:         tech@ispnet.net 20100217
source:          APNIC
```

APNIC Whois Registration



```
inetnum:        192.168.2.0 - 192.168.3.255
netname:        CustNet
descr:          ISPNet Customer
country:        AU
admin-c:        IA01-AP
tech-c:         IT03-AP
status:         ASSIGNED NON-PORTABLE
mnt-by:         MAINT-ISPNET-AP
mnt-irt:        IRT-ISPNET
changed:        admin@ispnet.net 20101120
source:         APNIC
```

APNIC Whois Registration



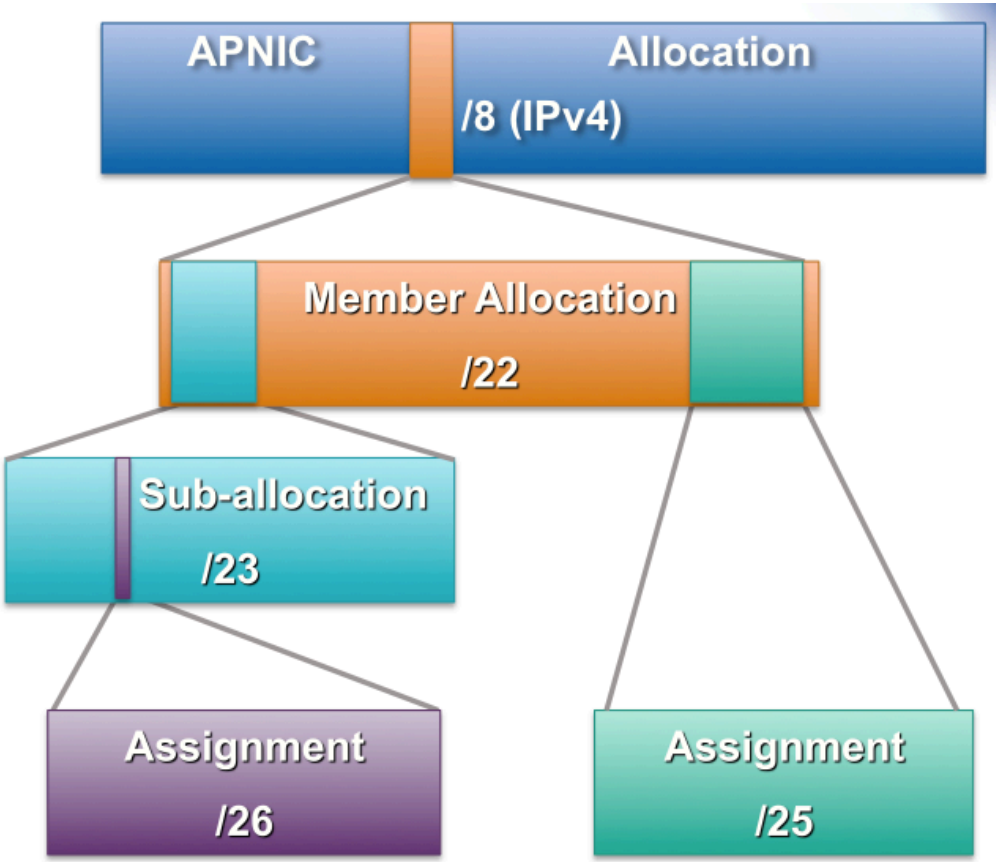
```
irt:            IRT-ISPNET
address:        Brisbane, Australia
phone-no:       +61-7-38583000
fax-no:         +61-7-38583100
email:          tech@ispnet.net
abuse-mailbox:  abuse@ispnet.net
admin-c:        IA01-AP
tech-c:         IT03-AP
auth:           X509-5
mnt-by:         MAINT-ISPNET-AP
changed:        tech@ispnet.net 20101108
source:         APNIC
```

Maintainer Hierarchy Diagram

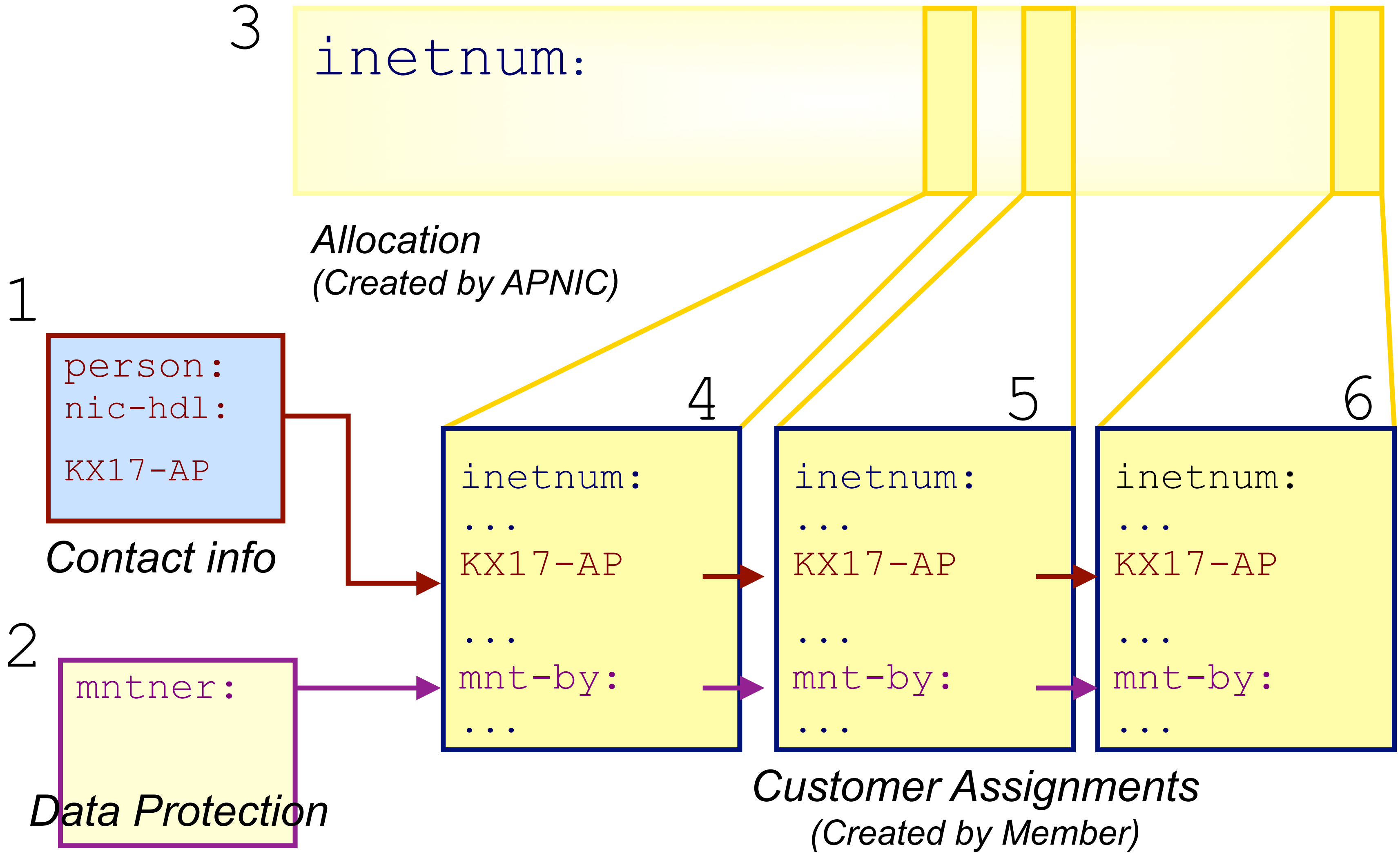
Allocated to APNIC:
Maint-by can only be changed by IANA

Allocated to Member:
Maint-by can only be changed by APNIC

Sub-allocated to Customer:
Maint-by can only be changed by Member



Using the Whois – step by step



Whois Database Queries

– Flags used for inetnum queries

None	find exact match
- l	find one level less specific matches
- L	find all less specific matches
- m	find first level more specific matches
- M	find all More specific matches
- x	find exact match (if no match, nothing)
- d	enables use of flags for reverse domains
- r	turn off recursive lookups

Whois Database Query - inetnum

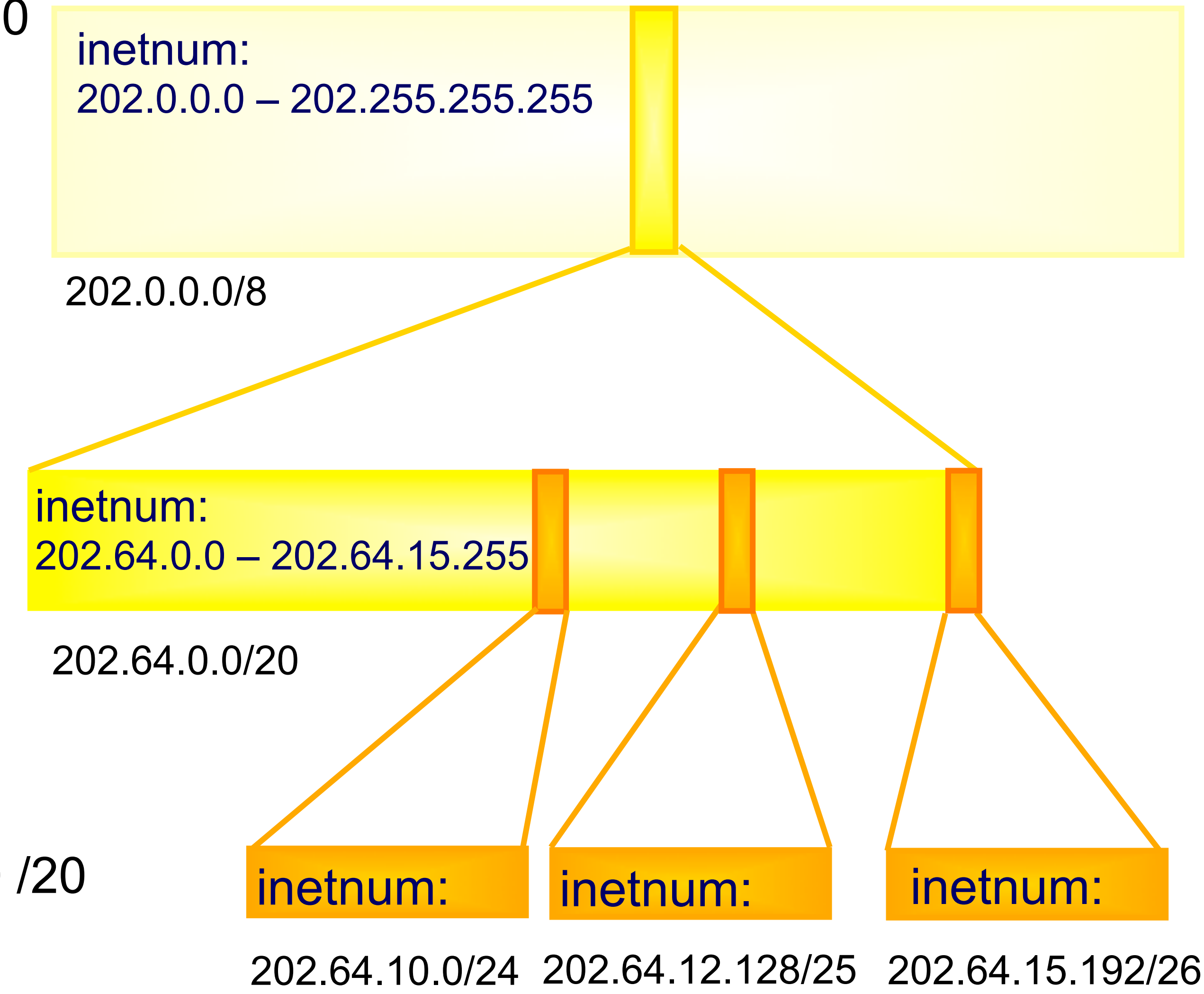
whois -L 202.64.0.0 /20

Less specific →
(= bigger block)

whois 202.64.0.0 /20

whois –m 202.64.0.0 /20

More specific →
(= smaller blocks)



Recursive Lookups

- whois 202.12.29.0

→ inetnum , route & person

recursion enabled by default

  - whois -r 202.12.29.0

→ inetnum & route ~~person~~

recursion turned off

  - whois -T inetnum 202.12.29.0

→ inetnum & person

'type' of object specified

  - whois -r -T inetnum 202.12.29.0

→ inetnum

'type' of object specified & recursion turned off

Inverse Queries

- Inverse queries are performed on inverse keys
  - *See object template (whois –t)*
- Returns all public objects that reference the object with the key specified as a query argument
  - Practical when searching for objects in which a particular value is referenced, such as your nic-hdl
- Syntax: whois -i <attribute> <value>

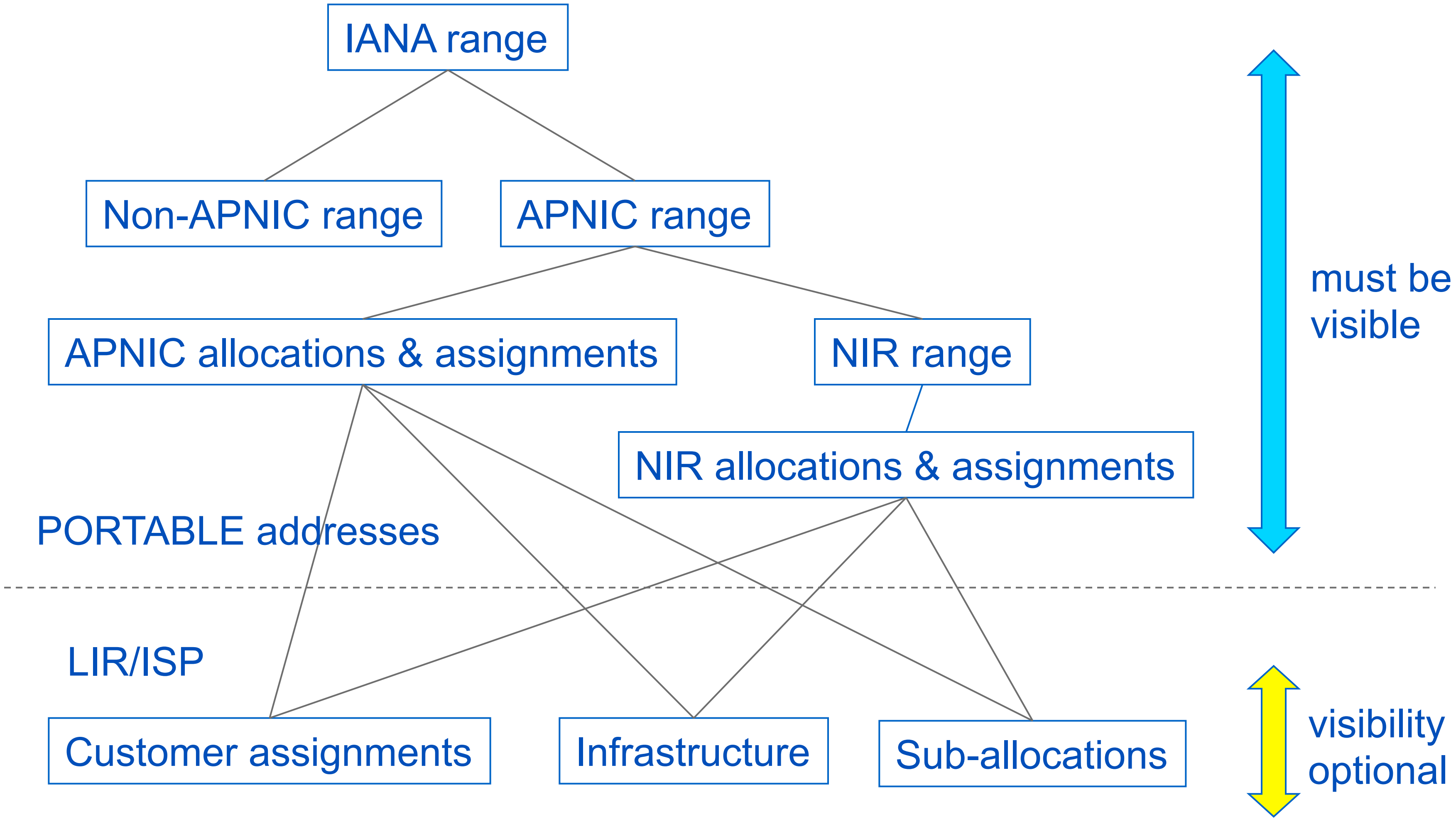
Inverse Queries - examples

- *What objects are referencing my nic-hdl?*
  - whois –i person KX17-AP *(or –ipn KX17-AP)*
- *In what objects am I registered as tech-c?*
  - whois –i tech-c KX17-AP
- *Return all domain objects where I am registered as admin-c or tech-c*
  - whois -i admin-c tech-c -T domain KX17-AP
- *What objects are protected by my maintainer?*
  - whois -i mnt-by MAINT-WF-EX

Customer Privacy

- Public data
  - – Includes portable addresses (inetnum objects), and other objects e.g.route objects
  - – Public data: must be visible
- Private data
  - – Can include non-portable addresses (inetnum objects)
  - – Members have the option to make private data visible
- Customer assignments
  - – Can be changed to be public data (public data is an optional choice)

What needs to be visible?



APNIC Whois Database & the Internet Routing Registry

- 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

Benefits of APNIC RR integrated in Whois Database

- Facilitates network troubleshooting
- Registration of routing policies
- Generation of router configurations
- Provides global view of routing

RPKI

What is RPKI?

- Resource Public Key Infrastructure (RPKI)
- A robust security framework for verifying the association between resource holder and their Internet resources
- Created to address the issues in RFC 4593
- Uses X.509 v3 certificates
  - With RFC3779 extensions
- Helps to secure Internet routing by validating routes
  - Proof that prefix announcements are coming from the legitimate holder of the resource
- A system to manage the creation and storage of digital certificates and the associated Route Origin Authorization documents

Benefits of RPKI - Routing

- Prevents “Route Hijacking”
  - when an entity participating in Internet routing announces a prefix without authorization
  - Reason: malicious attack or operational mistake

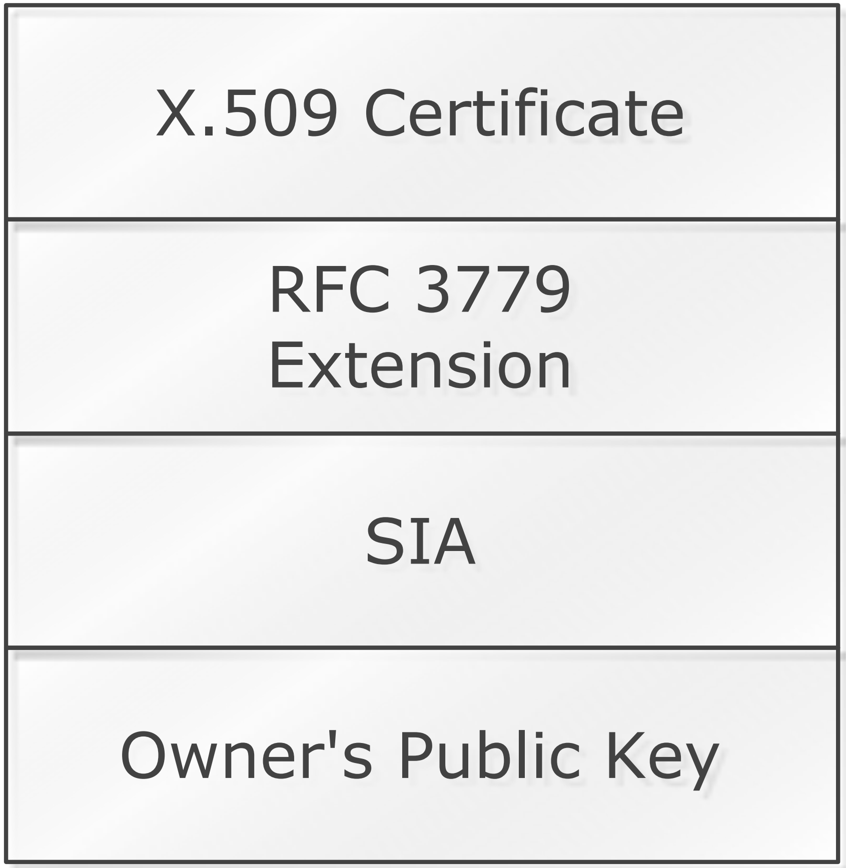
“Right” to Resources

- ISP gets their resources from the RIR
- ISP notifies its upstream of the prefixes to be announce
- Upstream _must_ check the Whois database if resource has been delegated to customer ISP.

X.509 Certificate

- Resource certificates are based on the X.509 certificate format - RFC 5280
- Extended by RFC 3779 – this extension binds a list of resources (IP, ASN) to the subject of the certificate

X.509 Certificate with 3779 Extension



X.509 Certificate

RFC 3779 Extension

SIA

Owner's Public Key

- SIA – Subject Information Access; contains a URI that references the directory

Two Components

- Certificate Authority (CA)
  - Internet Registries (RIR, NIR, Large LIR)
  - Issue certificates for customers
  - Allow customers to use the CA's GUI to issue ROAs for their prefixes
- Relying Party (RP)
  - Software which gathers data from CAs

Route Origin Authorisations (ROA)

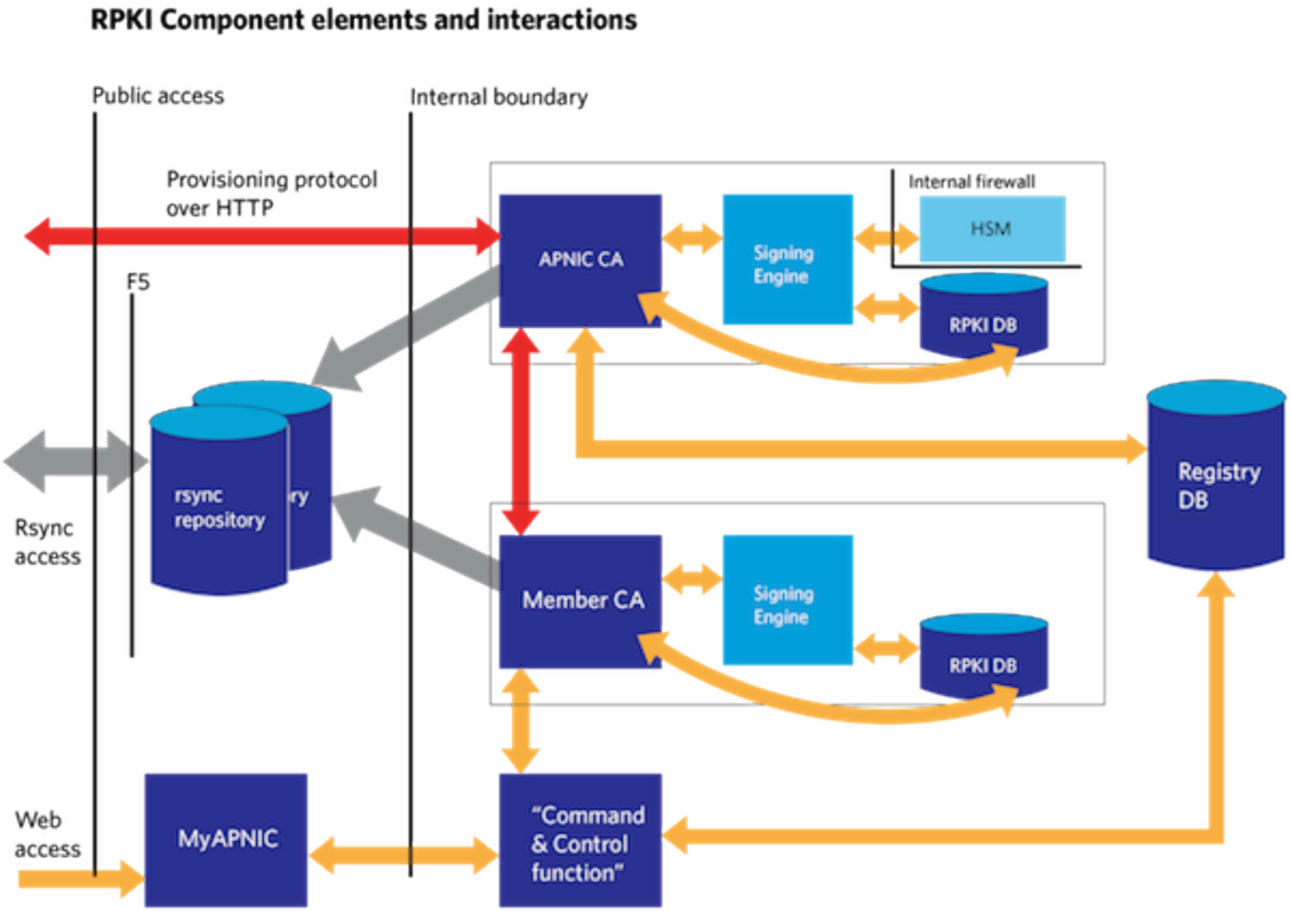
- Certificate holder uses its private key to sign an ROA
- Verifies that an AS has been given permission by an address block holder to advertise routes to one or more fpxies without a blog.

- RPKI in the RIRs
  - APNIC implemented RPKI Resource Certification

APNIC Resource Certification

- A robust security framework for verifying the association between resource holders and their Internet resources.
- Initiative from APNIC aimed at
  - improving the security of inter-domain routing, and
  - augmenting the information published in the Whois database
- Verifies a holder’s current “right-of-use” over an Internet resource

How it Works

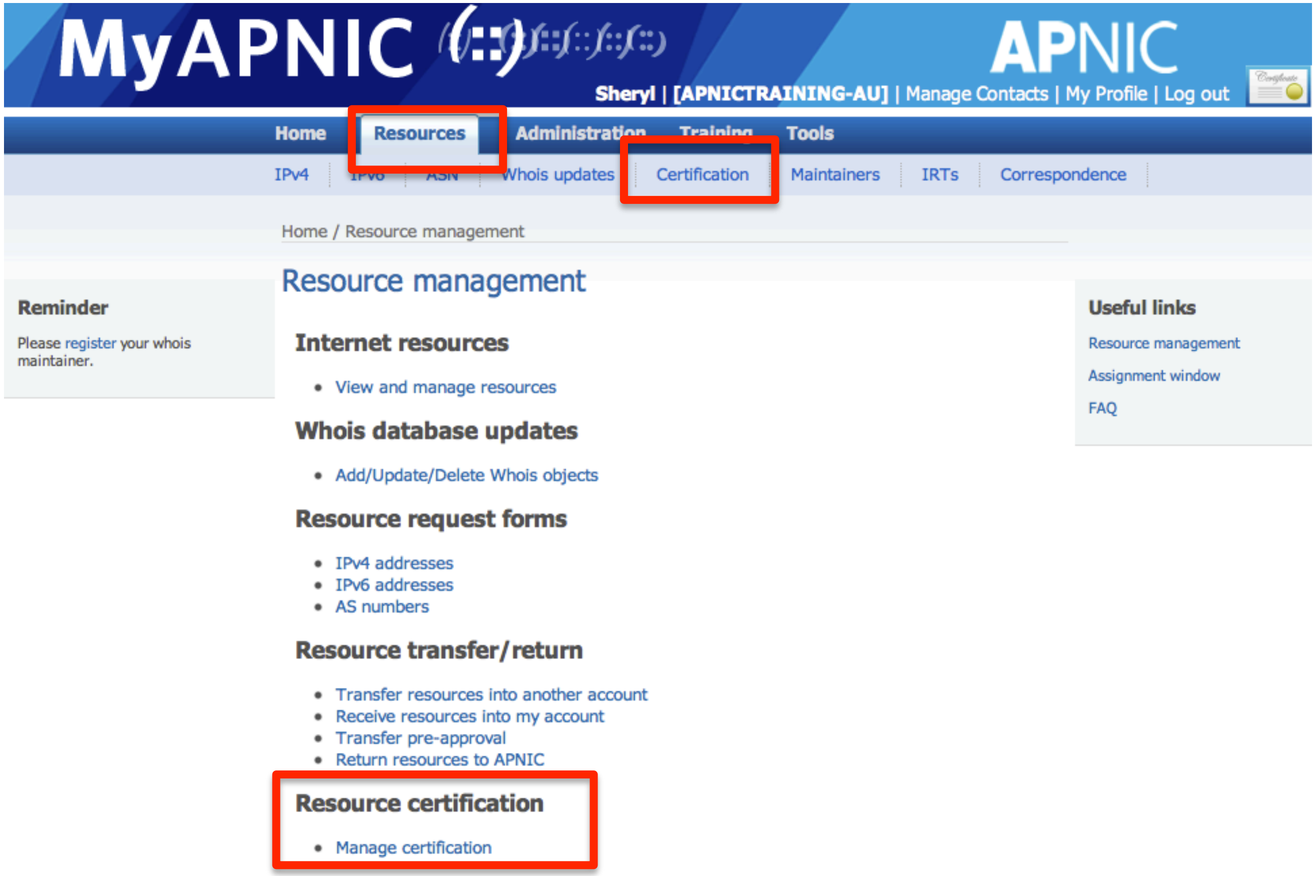

RPKI Component elements and interactions
Public access
Internal boundary
Provisioning protocol over HTTP
Internal firewall
APNIC CA
Signing Engine
HSM
RPKI DB
F5
rsync repository
ry
Rsync access
Registry DB
Member CA
Signing Engine
RPKI DB
Web access
MyAPNIC
"Command & Control function"

Resource Certification (APNIC)

- Verify signed data using the signer’s public key
- Verify public key through a chain of interlocking certificates that connect a Trust Anchor to the signer’s public key certificate.
  - This is what we refer to as RPKI
- Why it’s important:
  - Routing advertisements is now verifiable

Creating ROA Records

- Login to MyAPNIC, then **Resources -> Certification**



Home / Resource management

Resource management

Reminder

Please register your whois maintainer.

Internet resources

- View and manage resources

Whois database updates

- Add/Update/Delete Whois objects

Resource request forms

- IPv4 addresses
- IPv6 addresses
- AS numbers

Resource transfer/return

- Transfer resources into another account
- Receive resources into my account
- Transfer pre-approval
- Return resources to APNIC

Resource certification

- Manage certification

Useful links

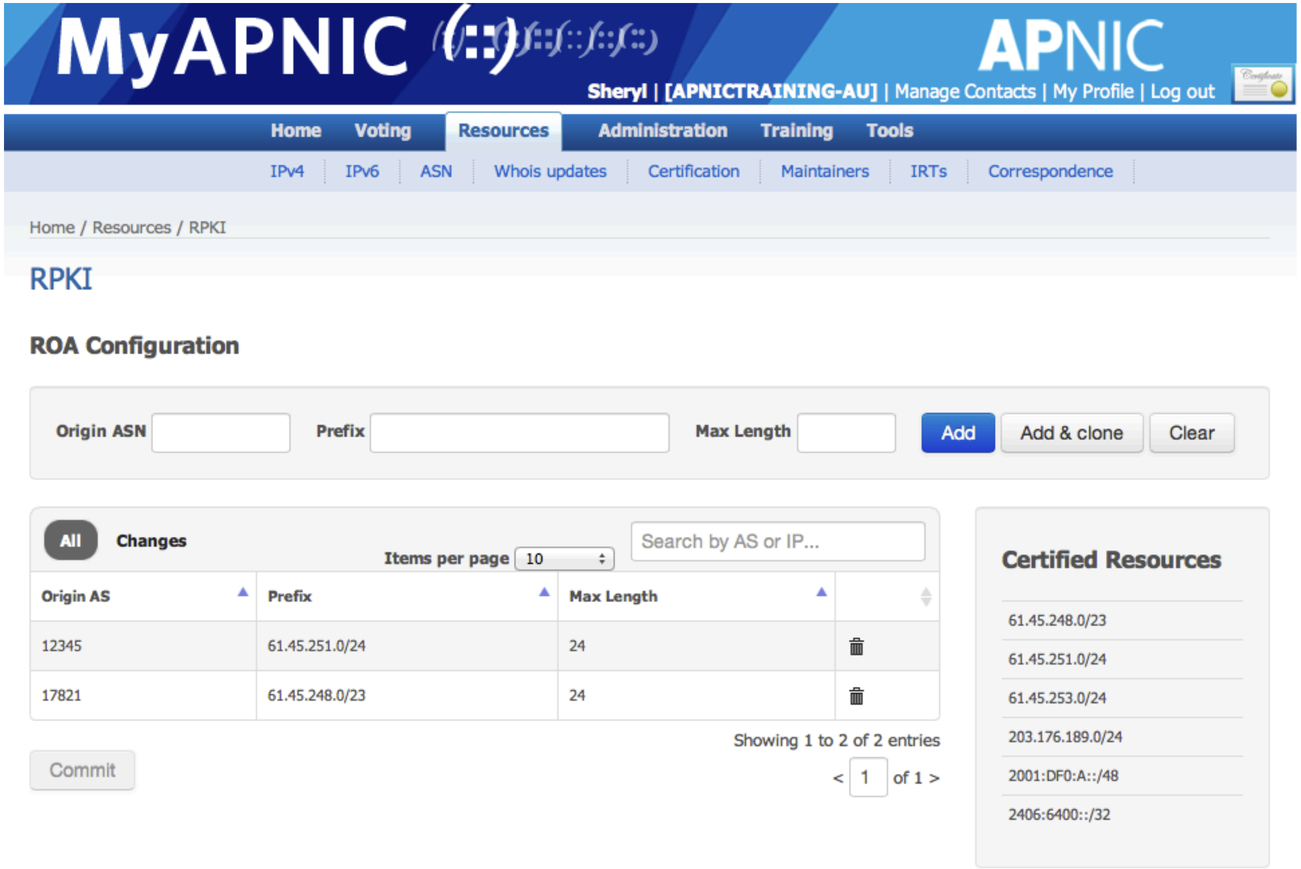
Resource management

Assignment window

FAQ

Adding ROA Records

- Simple view and add using the form



RPKI

ROA Configuration

Origin ASN □ Prefix □ Max Length □

Origin AS	Prefix	Max Length	
12345	61.45.251.0/24	24	🗑
17821	61.45.248.0/23	24	🗑

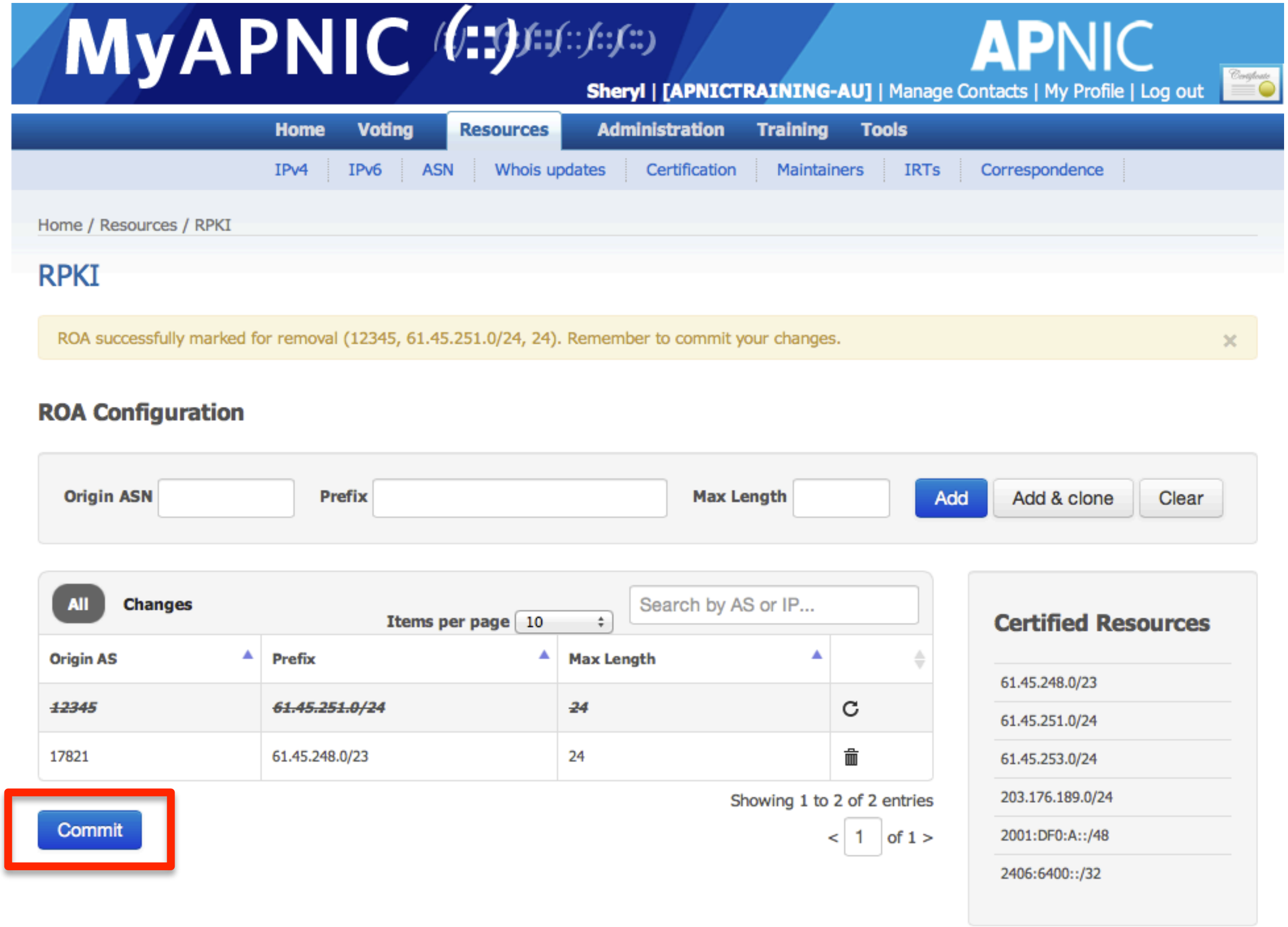
Showing 1 to 2 of 2 entries

< 1 of 1 >

Certified Resources

- 61.45.248.0/23
- 61.45.251.0/24
- 61.45.253.0/24
- 203.176.189.0/24
- 2001:DF0:A::/48
- 2406:6400::/32

Deleting ROA Records



Home / Resources / RPKI

RPKI

ROA successfully marked for removal (12345, 61.45.251.0/24, 24). Remember to commit your changes. ×

ROA Configuration

Origin ASN [ ] Prefix [ ] Max Length [ ] Add | Add & clone | Clear

All | Changes

Items per page 10

Search by AS or IP...

Origin AS	Prefix	Max Length	
~~12345~~	~~61.45.251.0/24~~	~~24~~	↻
17821	61.45.248.0/23	24	🗑

Showing 1 to 2 of 2 entries

< 1 of 1 >

Commit

Certified Resources

- 61.45.248.0/23
- 61.45.251.0/24
- 61.45.253.0/24
- 203.176.189.0/24
- 2001:DF0:A::/48
- 2406:6400::/32

Summary

- Introduction to APNIC
  - *Know about APNIC*
- Internet Policy Development
  - *How the Internet Policies are developed*
- Internet Challenges Today
  - *How APNIC can assist LEAs*
- Internet Resource Registration
  - *APNIC Whois Database*
- Resource Public Key Infrastructure (RPKI)
  - *How to Secure Routing*

Questions?

Thank you!