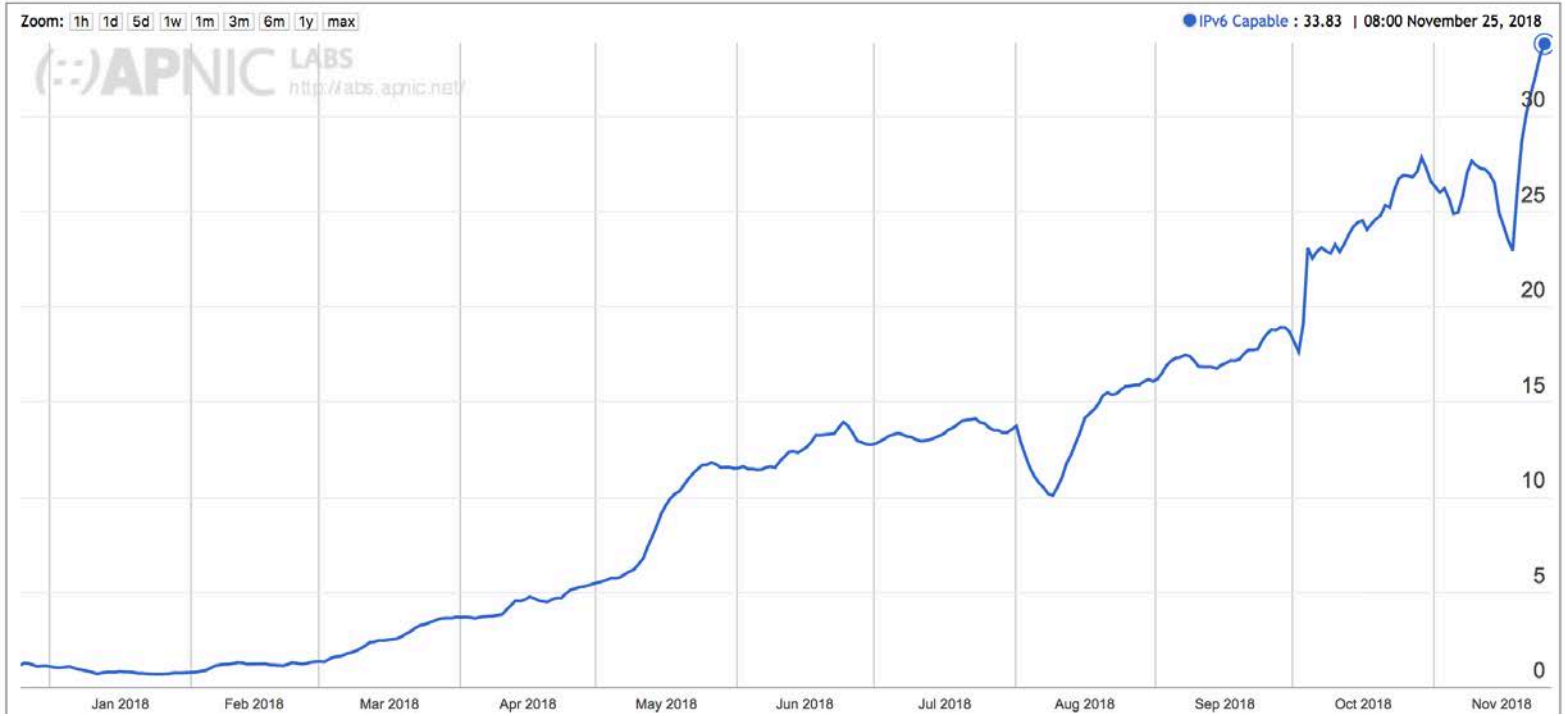
Internet Number Registry Services the Next Generation

RDAP and RPKI

Overview

- What are registry services
- Today’s registry services
- Registration Data Access Protocol (RDAP)
- Resource Public Key Infrastructure (RPKI)

But first...



https://stats.labs.apnic.net/ipv6

Congratulations TW!

CC	Country	IPv6 Capable
IN	India, Southern Asia, Asia	55.97%
US	United States of America, Northern America, Americas	49.56%
BE	Belgium, Western Europe, Europe	46.82%
TW	Taiwan, Eastern Asia, Asia	33.83%
FI	Finland, Northern Europe, Europe	33.46%
GR	Greece, Southern Europe, Europe	31.16%
UY	Uruguay, South America, Americas	30.67%
DE	Germany, Western Europe, Europe	28.91%
BR	Brazil, South America, Americas	26.79%
CH	Switzerland, Western Europe, Europe	26.09%

https://stats.labs.apnic.net/ipv6

Overview

- What are registry services
- Today’s registry services
- Registration Data Access Protocol (RDAP)
- Resource Public Key Infrastructure (RPKI)

What are registries

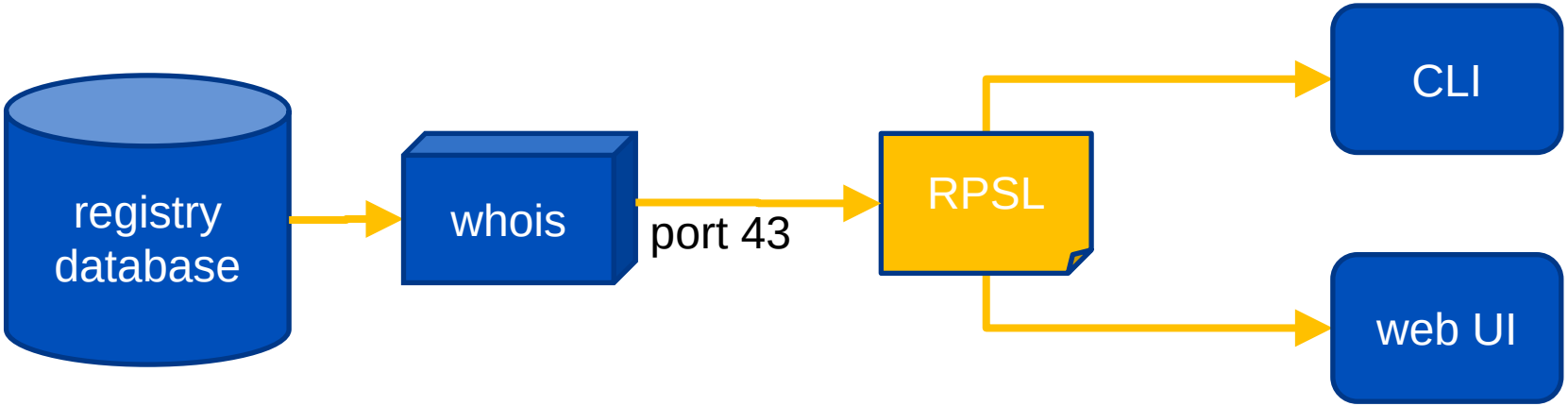
- Organisations running registry services
  - With authority for registration of some “Public Resource”
- Public databases describing status of resources
  - Land titles, vehicle registrations, phone numbers
  - Domain Names
  - Internet Number Resources (INRs) – IPv4, IPv4, ASNs
- Internet address Registries
  - RIRs, NIRs, LIRs
  - Authoritative registry/database function
  - Public registry service function

Registry services

- whois
  - Query service on TCP port 43 (RFC 812, 1982)
  - Public registry lookup service
  - Very simple, limited service
  - Query and response are not standardised
- Registration Data Access Protocol (RDAP) (NEW since 2015)
  - API for access to “whois” registry data
  - Automation, AAA, i18N, redirection, extensibility
- Resource Public Key Infrastructure (RPKI) (since 2010)
  - PKI for INRs
  - Cryptographically verifiable “ownership” of INRs
  - Mechanism for authorisation to route IPv4/v6 blocks

whois

whois at APNIC



whois command line

```
$ whois -h whois.apnic.net 210.17.9.242

% [whois.apnic.net]
% Whois data copyright terms    http://www.apnic.net/db/dbcopyright.html

% Information related to '210.17.0.0 - 210.17.127.255'

% Abuse contact for '210.17.0.0 - 210.17.127.255' is 'ethanchen@taiwanmobile.com'

inetnum:        210.17.0.0 - 210.17.127.255
netname:        TTN-TW
descr:          Taiwan Telecommunication Network Services Co.,LTD.
descr:          110 , 8F , No 89 , Sung Jen RD , Taipei
country:        TW
admin-c:        IP11-AP
tech-c:         IP11-AP
remarks:        service provider
mnt-by:         MAINT-TW-TWNIC
mnt-irt:        IRT-TFN-TW
mnt-lower:      MAINT-TTN-AP
status:         ALLOCATED PORTABLE
last-modified:  2011-06-01T04:13:58Z
source:         APNIC
```

Query to port 43

“Blob” format undefined

whois www interface

HTML wrapper

Same RPSL response

Whois – limitations

- “blob” query and result formats
  - Registry-specific questions and answers
  - Automation is difficult
- No AAA model
  - Built for public service only
- Most servers serve US-ASCII only
  - i18n is undefined
- No redirection
  - User/client must find the right server

RDAP

Registration Data Access Protocol

RDAP

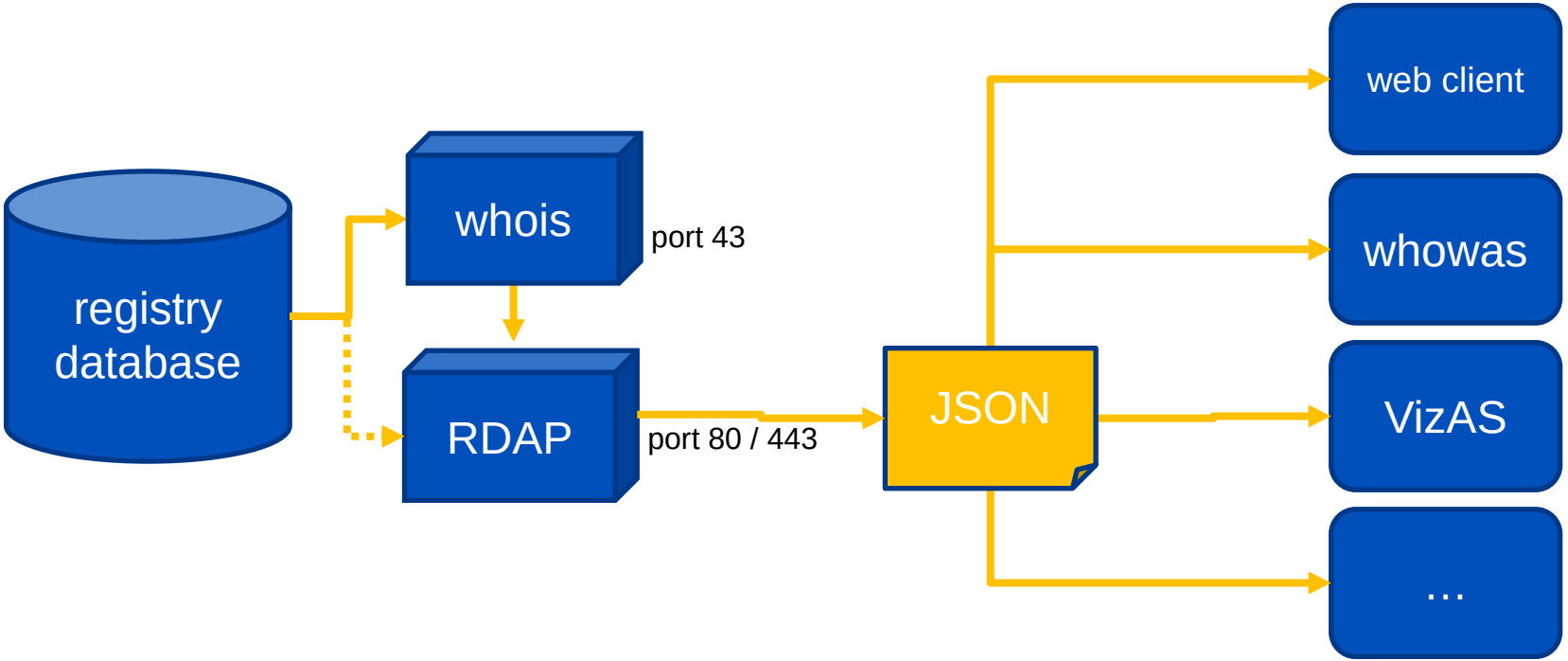
- RDAP is the successor to the ageing WHOIS protocol.
- Like WHOIS, RDAP provides…
  - Access to registration data: domain names, AS numbers, and IP addrs.
- Unlike WHOIS, RDAP provides…
  - Structured request and response semantics;
  - Differentiated access;
  - Internationalisation;
  - Redirection;
  - Extensibility.*

* Source: RDAP.org

RDAP: designed for automation

- Query: REST
  - REpresentational State Transfer - via HTTP
  - Query defined within URL issued to RESTful server
  - Inherits many useful features from HTTP/HTTPS
- Response: JSON
  - JavaScript Object Notation
  - Standardised text representation of structured data
  - Translates directly into data types in modern programming languages like JavaScript/HTML5, Java, Perl, Python, Ruby

RDAP


registry database
whois
port 43
RDAP
port 80 / 443
JSON
web client
whowas
VizAS
…

RDAP JSON raw

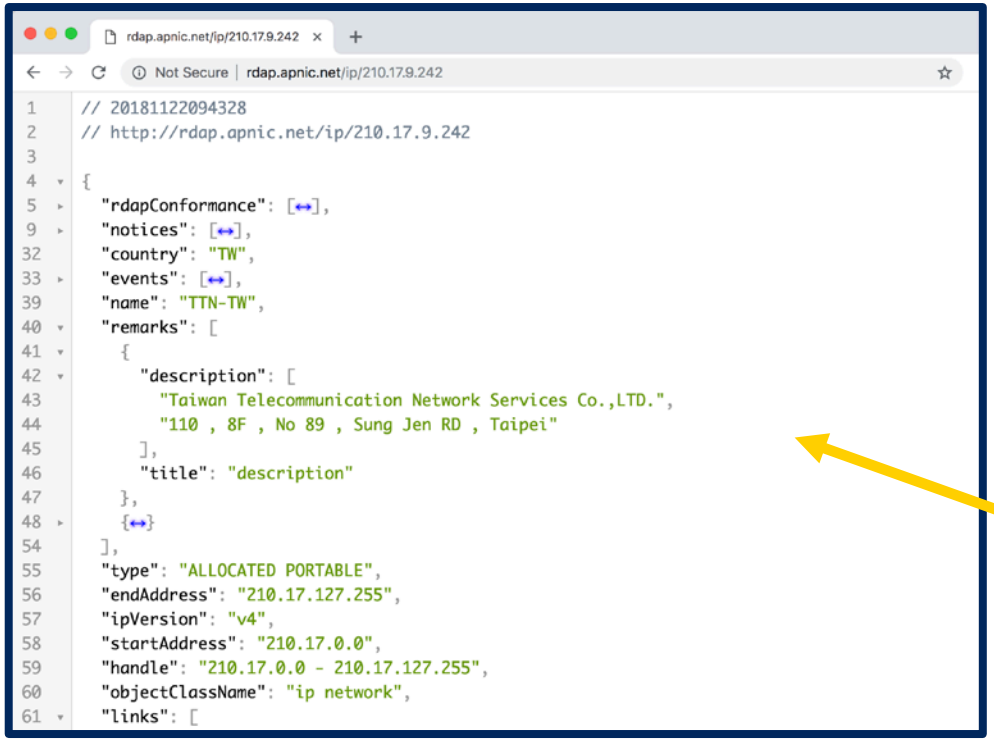
$ curl http://rdap.apnic.net/ip/210.17.9.242


```
{"rdapConformance":["history_version_0","rdap_level_0"],"notices":[{"title":"Source","description":["Objects returned came from
source","APNIC"]},{"title":"Terms and Conditions","description":["This is the APNIC WHOIS Database query service. The objects are in
RDAP format."],"links":[{"value":"http://rdap.apnic.net/ip/210.17.9.242","rel":"terms-of-
service","href":"http://www.apnic.net/db/dbcopyright.html","type":"text/html"}]}],"country":"TW","events":[{"eventAction":"last
changed","eventDate":"2011-06-01T04:13:58Z"}],"name":"TTN-TW","remarks":[{"description":["Taiwan Telecommunication Network Services
Co.,LTD.","110 , 8F , No 89 , Sung Jen RD , Taipei"],"title":"description"},{"description":["service
provider"],"title":"remarks"}],"type":"ALLOCATED
PORTABLE","endAddress":"210.17.127.255","ipVersion":"v4","startAddress":"210.17.0.0","handle":"210.17.0.0 -
210.17.127.255","objectClassName":"ip
network","links":[{"value":"http://rdap.apnic.net/ip/210.17.9.242","rel":"self","href":"http://rdap.apnic.net/ip/210.17.0.0/17","type
":"application/rdap+json"}],"entities":[{"roles":["abuse"],"events":[{"eventAction":"last changed","eventDate":"2017-01-
22T22:54:59Z"}],"vcardArray":["vcard",[["version",{},"text","4.0"],["fn",{},"text","IRT-TFN-
TW"],["kind",{},"text","group"],["adr",{"label":"7F., No. 172-1, Sec. 2, Ji-Lung Rd.\nTaipei City 106, Taiwan
R.O.C."},"text",["","","","","","",""]],["email",{},"text","ethanchen@taiwanmobile.com"],["email",{"pref":"1"},"text","ethanchen@ta
anmobile.com"]]],"handle":"IRT-TFN-
TW","objectClassName":"entity","links":[{"value":"http://rdap.apnic.net/ip/210.17.9.242","rel":"self","href":"http://rdap.apnic.net/e
ntity/IRT-TFN-TW","type":"application/rdap+json"}]},{"roles":["administrative","technical"],"events":[{"eventAction":"last
changed","eventDate":"2011-12-06T00:10:19Z"}],"remarks":[{"description":["### Crime, Abuse , Spam , Security ###","CSC TEL : 0809-
000-188","CSC TEL : +886-2-4066-0357","abuse@tfn.com.tw","abuse@tfn.com.tw","### Crime, Abuse , Spam , Security
###"],"title":"remarks"}],"vcardArray":["vcard",[["version",{},"text","4.0"],["fn",{},"text","TTN IP-
Team"],["kind",{},"text","group"],["adr",{"label":"Taiwan Mobile Co., Ltd.\nNetwork Assurance & Technical Support Div.\n# Ex TTN
merged\n8F.,No 172-1, Sec 2, Ji-Lung RD\nTaipei 106  Taiwan"},"text",["","","","","","",""]],["tel",{"type":"voice"},"text","+886-2-
6638-6888"],["tel",{"type":"fax"},"text","+886-2-6639-0607"],["email",{},"text","whois@ttn.com.tw"]]],"handle":"IP11-
AP","objectClassName":"entity","links":[{"value":"http://rdap.apnic.net/ip/210.17.9.242","rel":"self","href":"http://rdap.apnic.net/e
ntity/IP11-AP","type":"application/rdap+json"}]}],"port43":"whois.apnic.net"}
```


HTTP “get”

“Blob” but in JSON format

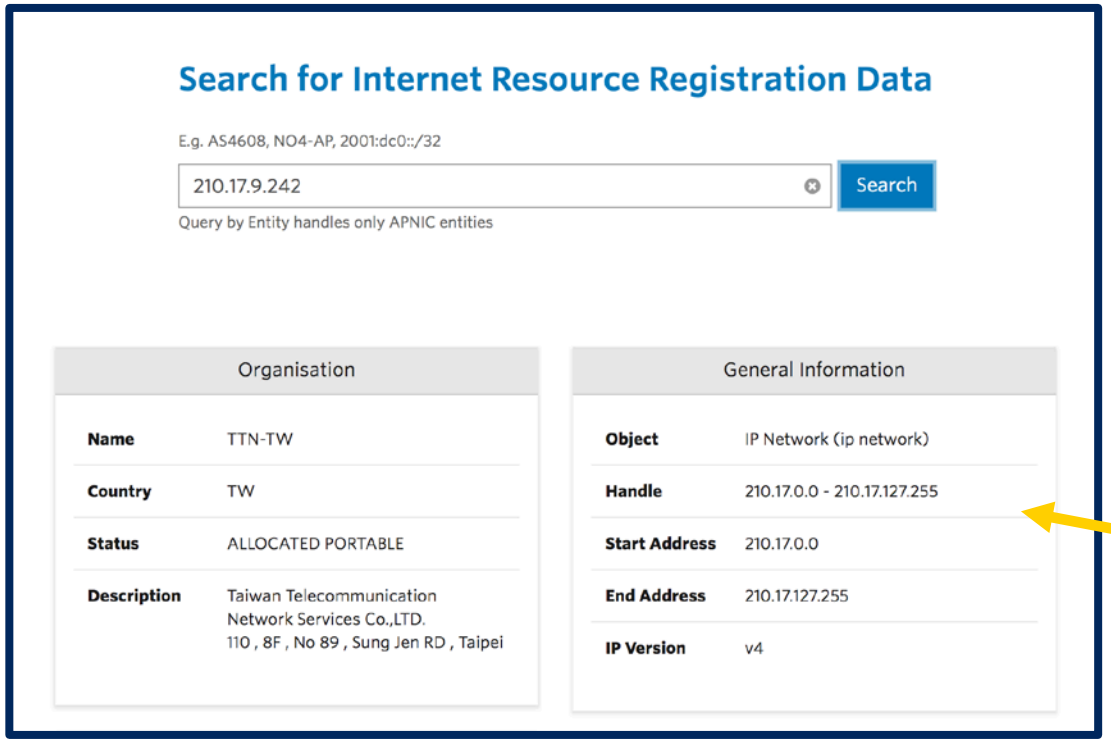
RDAP JSON formatted



Browser plugin

Structured result

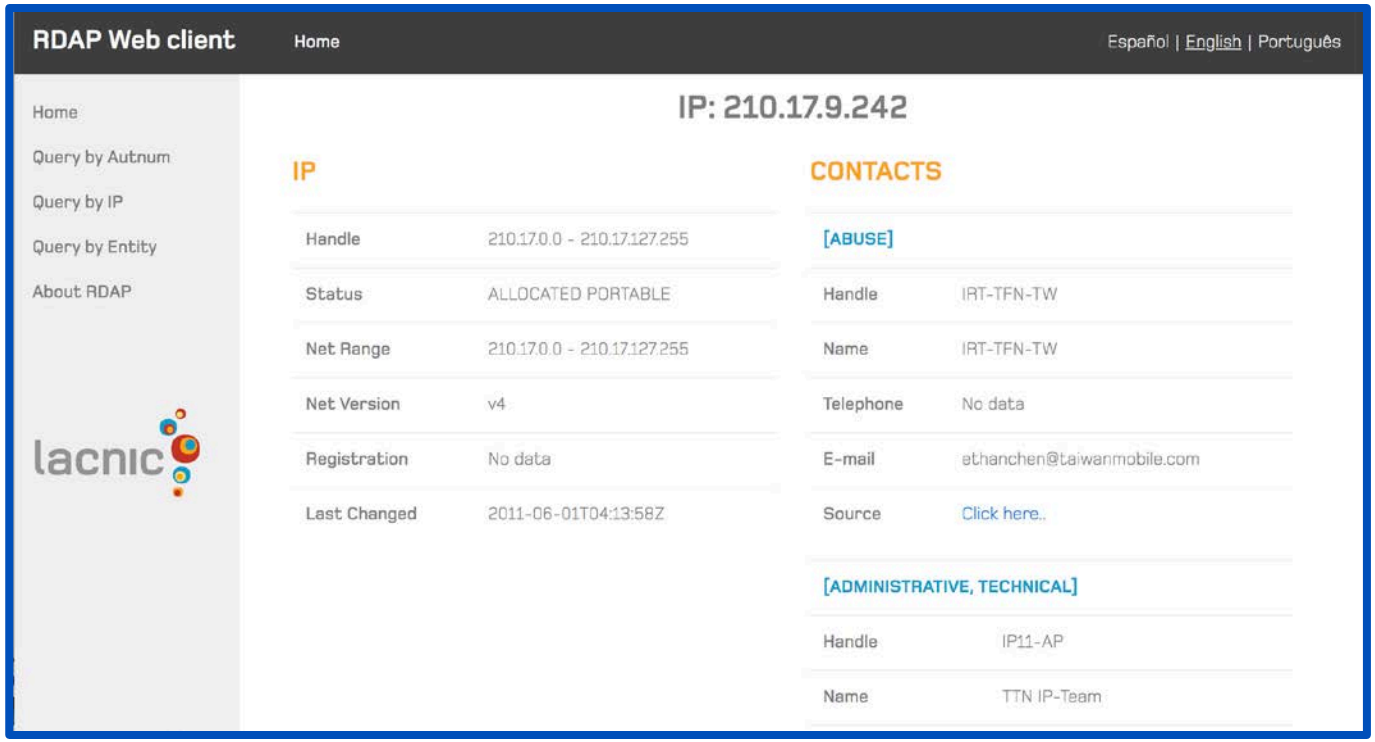
RDAP client



Web-based client

Processed result

RDAP client


RDAP Web client
Home
Español | English | Português
Home
Query by Autnum
Query by IP
Query by Entity
About RDAP
lacnic
IP: 210.17.9.242
IP
Handle 210.17.0.0 - 210.17.127.255
Status ALLOCATED PORTABLE
Net Range 210.17.0.0 - 210.17.127.255
Net Version v4
Registration No data
Last Changed 2011-06-01T04:13:58Z
CONTACTS
[ABUSE]
Handle IRT-TFN-TW
Name IRT-TFN-TW
Telephone No data
E-mail ethanchen@taiwanmobile.com
Source Click here..
[ADMINISTRATIVE, TECHNICAL]
Handle IP11-AP
Name TTN IP-Team

RDAP access control

- REST allows for service differentiation
  - General public vs authorised access
  - Public vs privileged information
  - Rate limiting etc
- Implemented using standard web authentication
  - HTTP 1.1 “basic” and “digest” forms
  - TLS with server/client certification
  - Oauth, OpenID under development in IETF draft process

RDAP internationalisation

- RDAP content is UTF-8 encoded UNICODE
- Roles and contact information
  - Defined using vCard RFC6868 (updated from 1998 RFC2425)
  - Widely understood for contact information, mail systems
  - Allows alternates, order preferences, language and character set
- Normally RDAP fetches all encodings
  - Client gets to pick preference
  - But server could use client “language hint” via HTTP

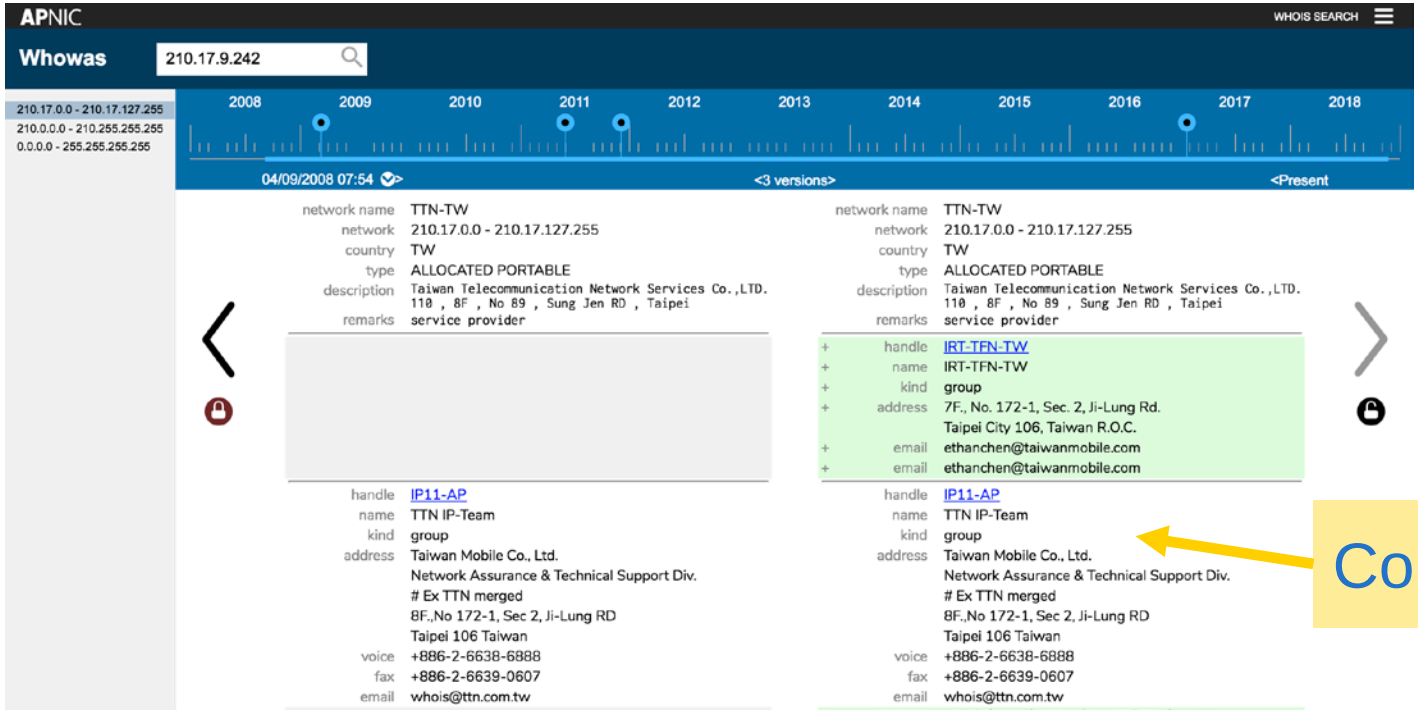
RDAP query redirection

- RDAP uses HTTP mechanism to redirect
  - “302 redirect temporary” points to temporary URL for this query
  - In case query is for resource that server knows is held elsewhere
- Globally coordinated redirection
  - IANA registry of all delegations in RDAP with base URL
- Result: RDAP can find “most specific” registry
  - No more “this record has moved” responses!

RDAP extensibility

- Oauth/OpenID under development
  - Federated identity model, well supported in public internet
- RDAP Bulk (APNIC)
  - Like WHOIS bulk download, so that comparable offline fetch of complete records can be done efficiently.
  - Will respect existing WHOIS bulk AUP restrictions on usage
- RDAP History (APNIC)
  - Time sequenced set of records, to denote changes across time in RDAP information
  - Basis of the APNIC “WHOWAS” service
  - Currently being promoted in standards at IETF

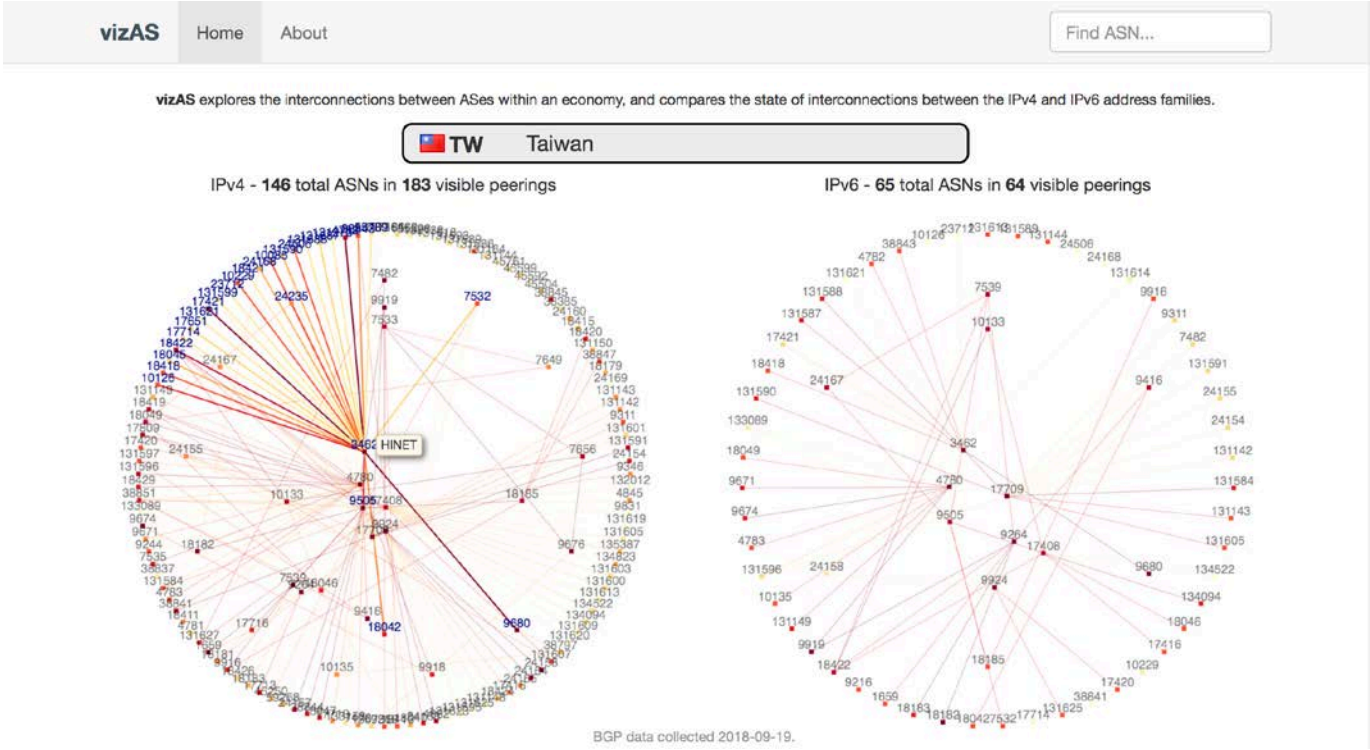
RDAP application (whowas)



Complex result

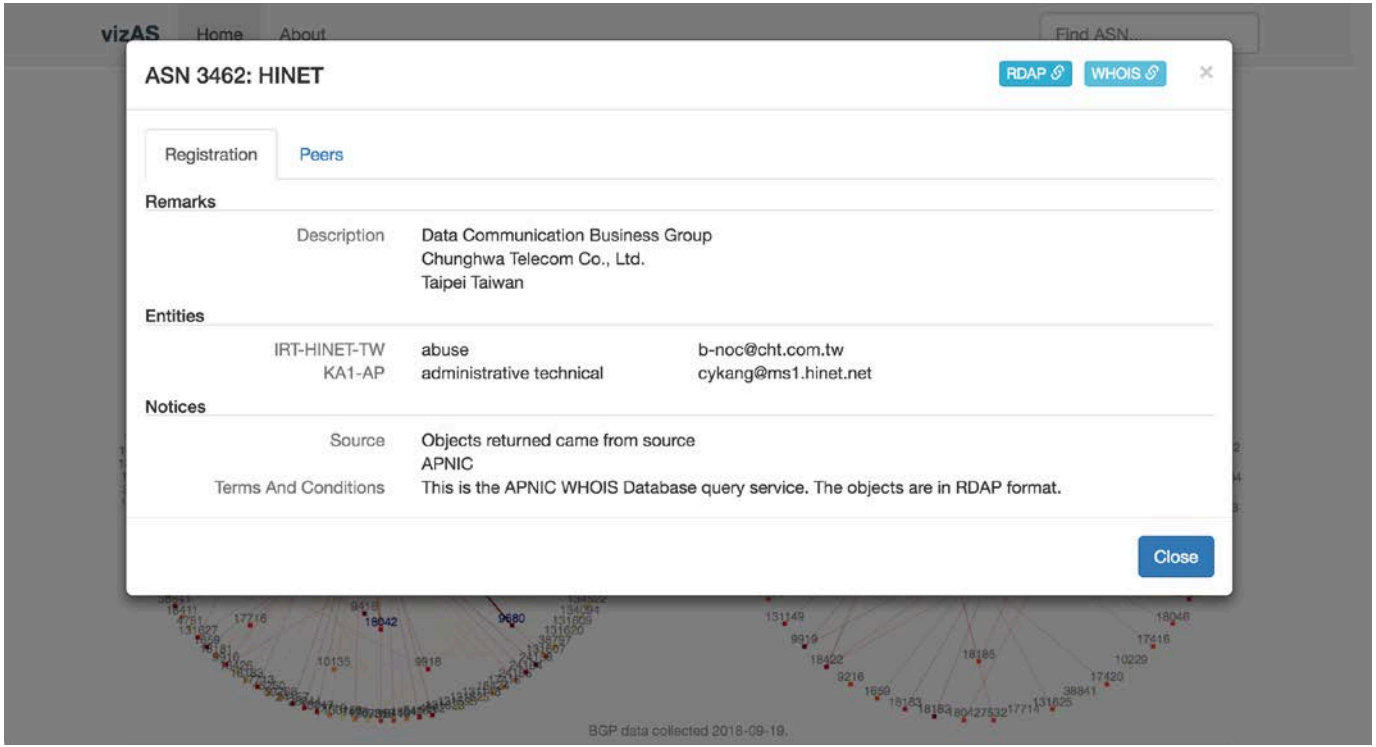
https://www.apnic.net/whowas

RDAP application (vizAS)



https://www.apnic.net/vizas

RDAP application (vizAS)



https://www.apnic.net/vizas

RDAP benefits

- Automation – JSON input to common programming languages
  - Integration with firewall, NMS, IPAM…
- “Differentiated Access”
  - If needed
- Speaks your language (and character set)
  - Can implement server-side or in-client language preference
- One stop query
  - Will auto-redirect to the right authoritative server
- Web protocol is CDN friendly
  - Serve local, via anycast or DNS redirection methods
  - Cacheable, survives DDoS longer since distributed

RDAP specifications

- RFC 7480 – HTTP Usage in RDAP
- RFC 7481 – Security Services for RDAP
- RFC 7482 – RDAP Query Format
- RFC 7483 – JSON Responses for RDAP
- RFC 7484 – Finding the Authoritative RDAP Service
- RFC 7485 – Inventory and Analysis of WHOIS Objects

APNIC RDAP Status

- First implemented May 2015
  - Adjunct service query to WHOIS radix tree (in memory)
  - Rewrote RPSL on-the-fly
- Re-implemented into WHOWAS Late 2016
  - Static in-memory data model. Fast response
- Working with NIRs
  - Hope to serve <nir>.rdap.apnic.net more-specific service
- APNIC region-wide consistent service model goal for 2019
  - Working with NIRs and other RIRs

RPKI

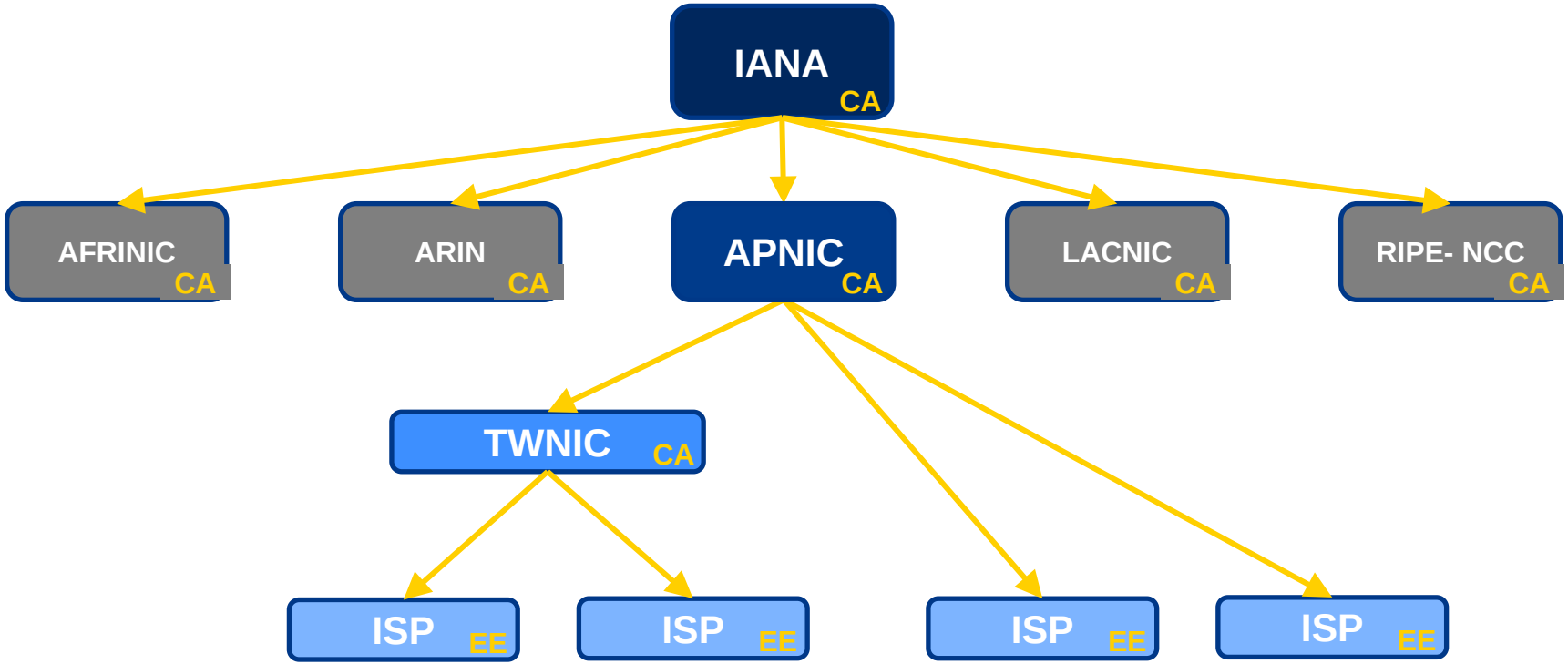
Resource Public Key Infrastructure

RPKI

- **RPKI** is a public key infrastructure (PKI) framework, designed to secure BGP routing
  - Based on X.509 PKI standards
- **RPKI** adds INR information to X.509 certificates issued to resource holders
  - Representing “ownership” and other status
  - Certification hierarchy follows INR delegation hierarchy

IANA ➔ RIR ➔ NIR ➔ ISP ➔ …

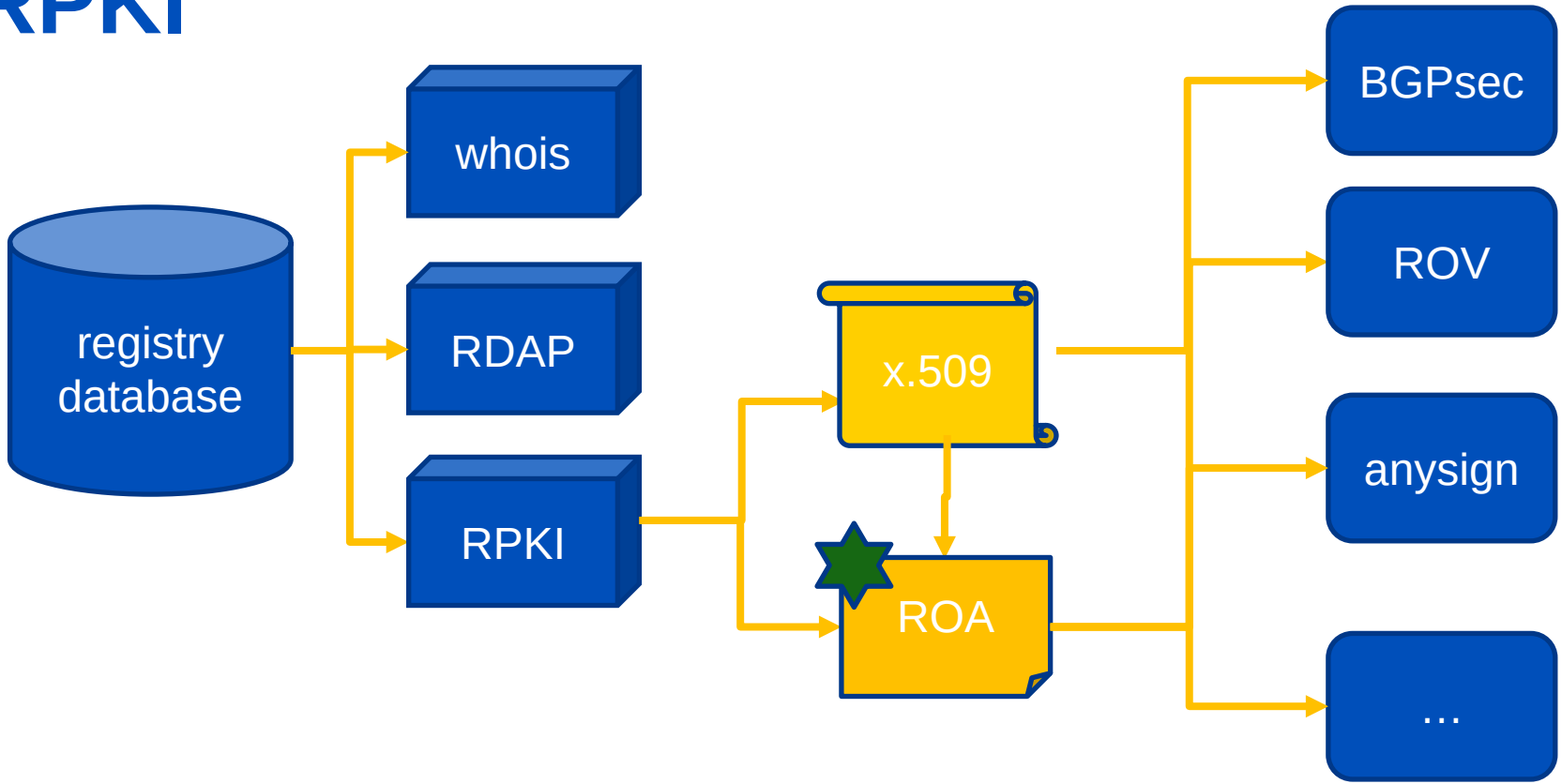
RPKI hierarchy



RPKI objects

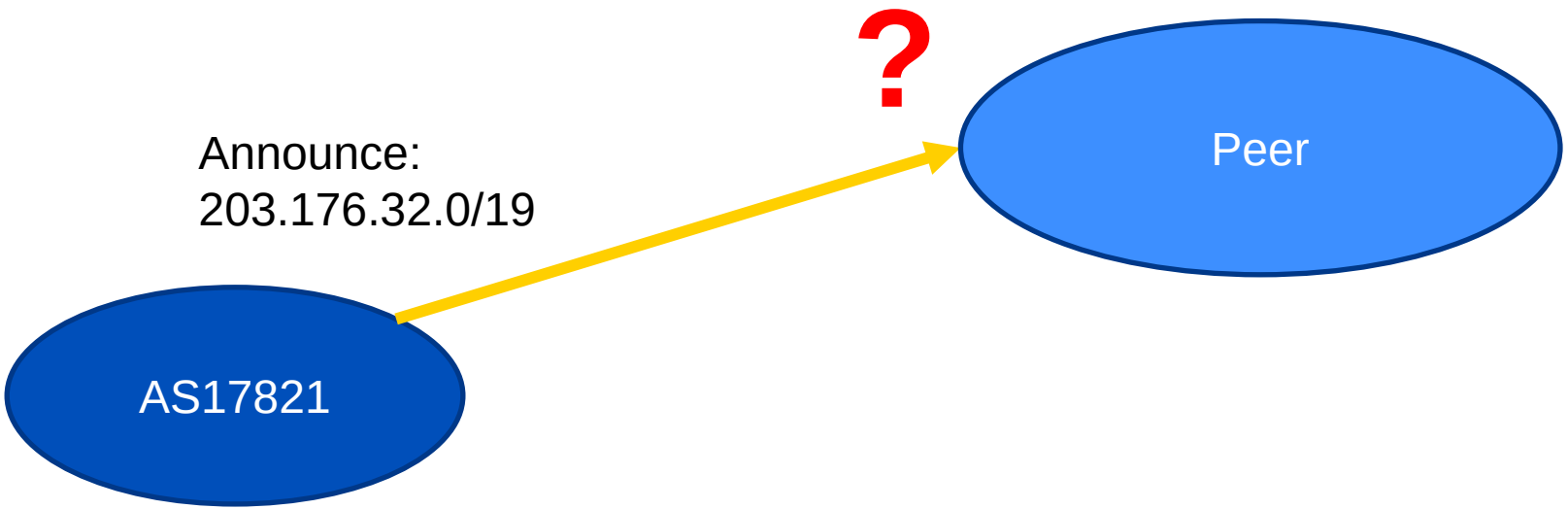
- Resource certificates
  - Extension of standard X.509 certificates
  - Providing authority to use given IPv4/6 and ASN resources
  - Signed by issuing registry (serving as CA)
- Route Origin Authorisation (ROA)
  - Giving an ASN authority to route specific IP blocks
  - Signed by IP resource holder
- “Anysign”, “ghostbuster” and more…
  - Other useful objects proposed and coming later

RPKI


registry database
whois
RDAP
RPKI
x.509
ROA
BGPsec
ROV
anysign
…

RPKI applications: ROV

- Route Origin Validation



RPKI: ROA

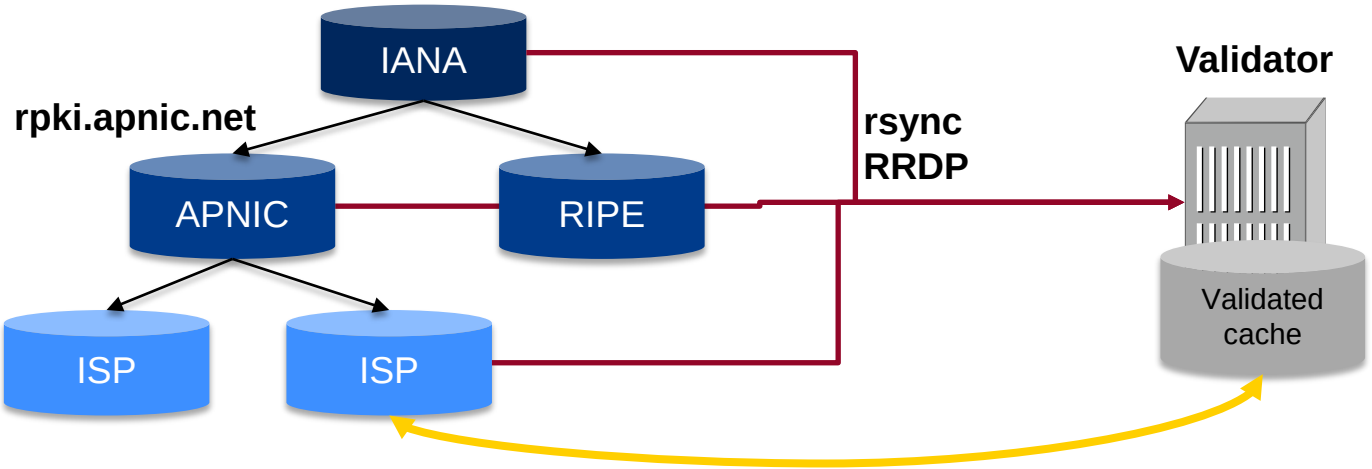
- Route Origin Authorization
  - List of prefixes with ASN authorized to announce
  - Signed by the prefix holder

Prefix	203.176.32.0/19
Max-length	/24
Origin ASN	AS17821

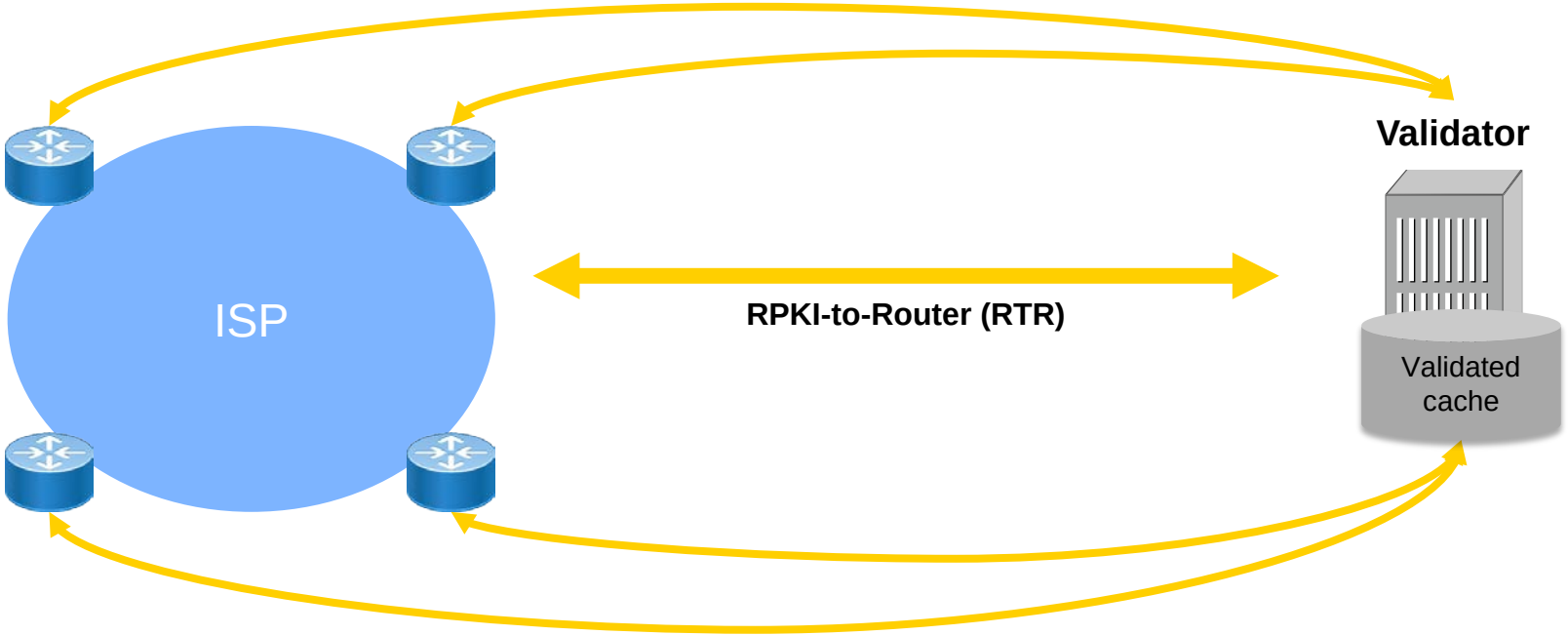
- RPKI validates the integrity of the ROA
  - It is provably created by the holder of the prefix
  - Can now be used to construct route filters for prefix-OriginAS pair in BGP

RPKI Validator

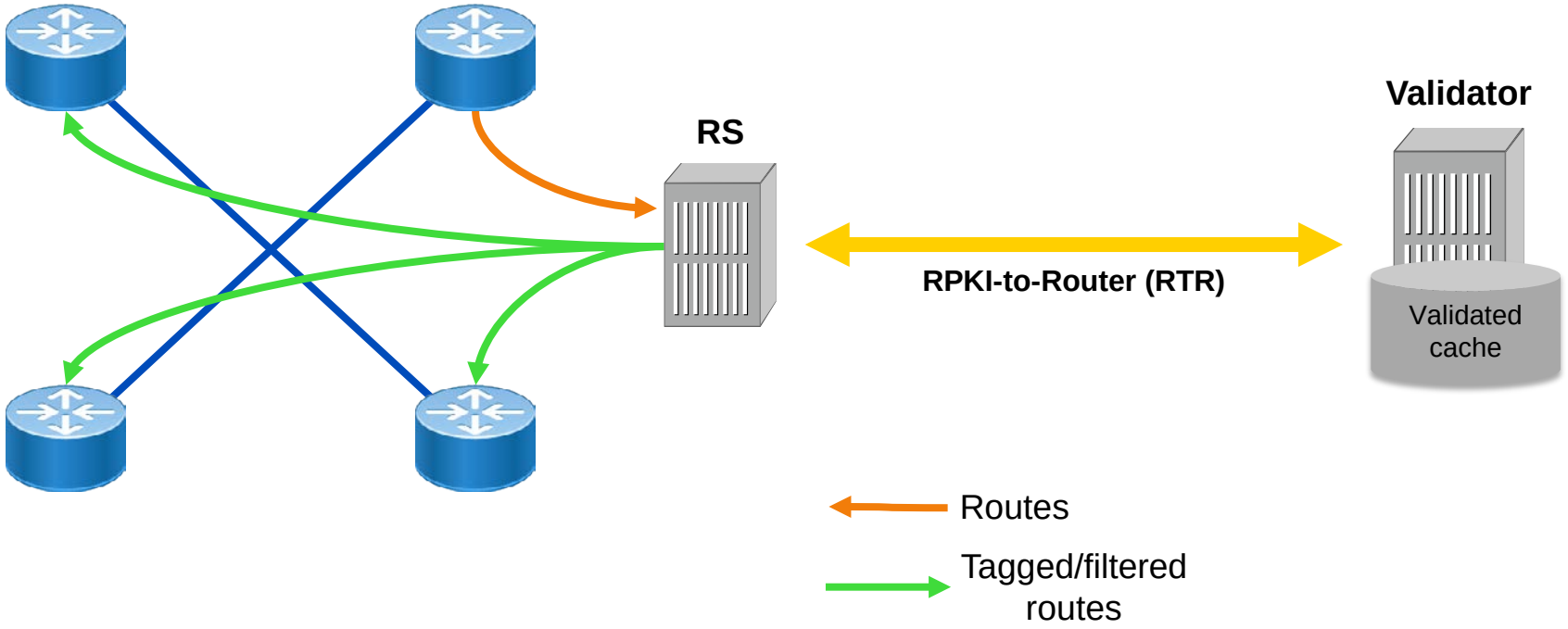
- Gathers and validates ROAs from the distributed RPKI databases
  - Using rsync or RRDP (preferable)
  - Maintains a validated cache representing complete global state
- Can then perform ROV for routers using RPKI-Router (RTR) protocol



ROV at Border Routers



ROV at IXP


RS
Validator
RPKI-to-Router (RTR)
Validated cache
Routes
Tagged/filtered routes

Route validation states

- **Not Found (Unknown)**
  - No ROA found, probably not created yet
  - This will be “default” for some time.
- **Valid**
  - ROA exists
  - Prefix, Origin ASN and prefix-length match those found in validated cache
- **Invalid**
  - ROA exists
  - Prefix found, but Origin ASN is wrong, Prefix-length longer than Max-length, or certificates are expired or otherwise invalid.
  - Some action needed

Action for invalid routes

- For inbound routes from upstreams/peers
  - Drop them
  - Give them lower LOCAL_PREF
  - Do nothing (not recommended)
- For outbound routes to customers
  - Tag them before re-distributing them to customers
  - Allow customers to make their own choices
- Tagging (eg at IXPs)
  - Apply community tags based on the validation state
    - **Not Found** (*ASN:65XX1*)
    - **Valid** (*ASN:65XX2*)
    - **Invalid** (*ASN:65XX3*)

“Anysign” use case: LOA signing

- Take existing “letter of authority” practice
  - Typically a scanned/signed PDF under company letterhead
  - Unverifiable without more information
- Generate “detached signature” using RPKI
  - Signing certificate includes specific INR
  - Now a trustable letter of authority
- Pilot implementation
  - In development at APNIC (via MyAPNIC)
  - IETF draft in progress

RPKI specifications

Some of over 42 RFCs on implementation of RPKI and BGPsec

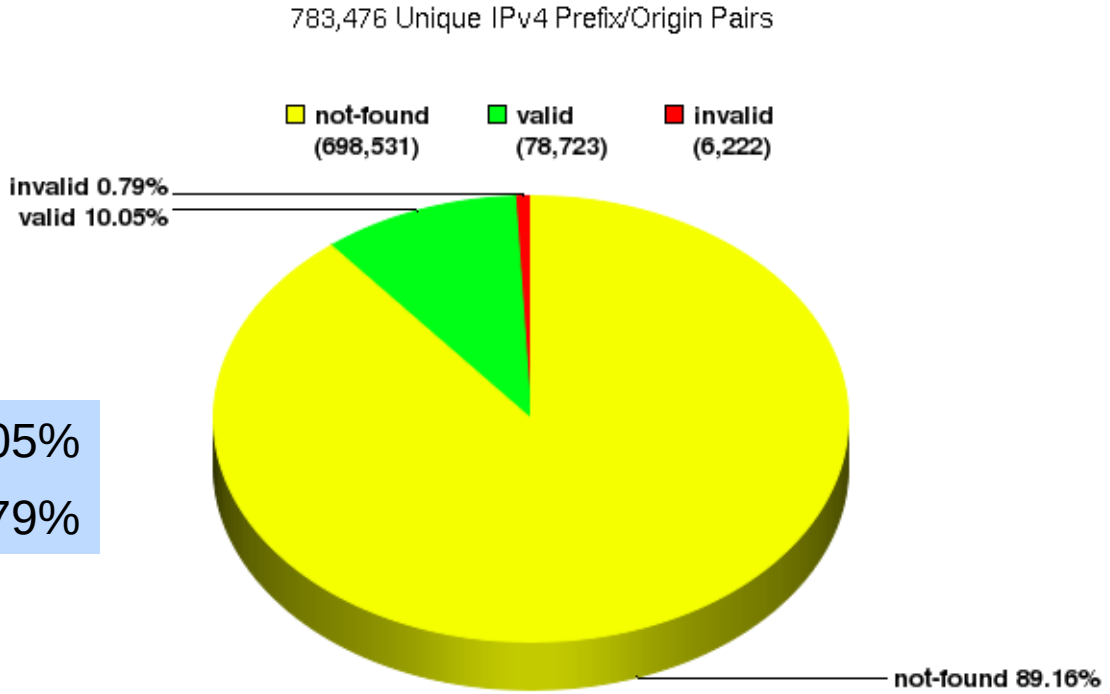
- RFC3779 X. 509 Extensions for IP Addresses and AS Identifiers
- RFC6480 Infrastructure to support secure routing
- RFC6481 Profile for repository structure
- RFC6482 Profile for Route Origin Authorisation (ROA)
- RFC6483 Validation model
- RFC6484 Certificate Policy (CP) for RPKI
- RFC6485 Algorithms & Key sizes for RPKI
- RFC6486 Manifests for repositories in RPKI
- RFC6487 Profile for RPKI Certificates
- RFC6488 Signed object CMS template
- RFC6489 Key Rollover
- RFC6490 Trust Anchor Locator (TAL)
- RFC6492 RPKI Provisioning Protocol
- RFC7318 Policy Qualifiers in RPKI certificates
- RFC7382 Certificate Practice Statement (CPS)
- RFC8181 RPKI publication protocol
- RFC8182 RPKI Delta protocol (RRDP)
- RFC8183 Out-of-band RPKI setup protocol
- RFC8360 RPKI Validation Reconsidered

RPKI at APNIC

RPKI Service Models

- Hosted model
  - APNIC performs CA functions on behalf of members
  - Manage keys, repository etc
  - Generate certificates for resource delegations
  - This “Member CA” is separate from the “APNIC CA”
- Provisioning model
  - Member operates full RPKI system including CA
  - Communication with APNIC via “up-down” provisioning protocol
    - Either rsync (to be deprecated) or RRDP (preferred)
  - This is live at JPNIC, CNNIC and TWNIC (IDNIC in progress)

RPKI Status – Global

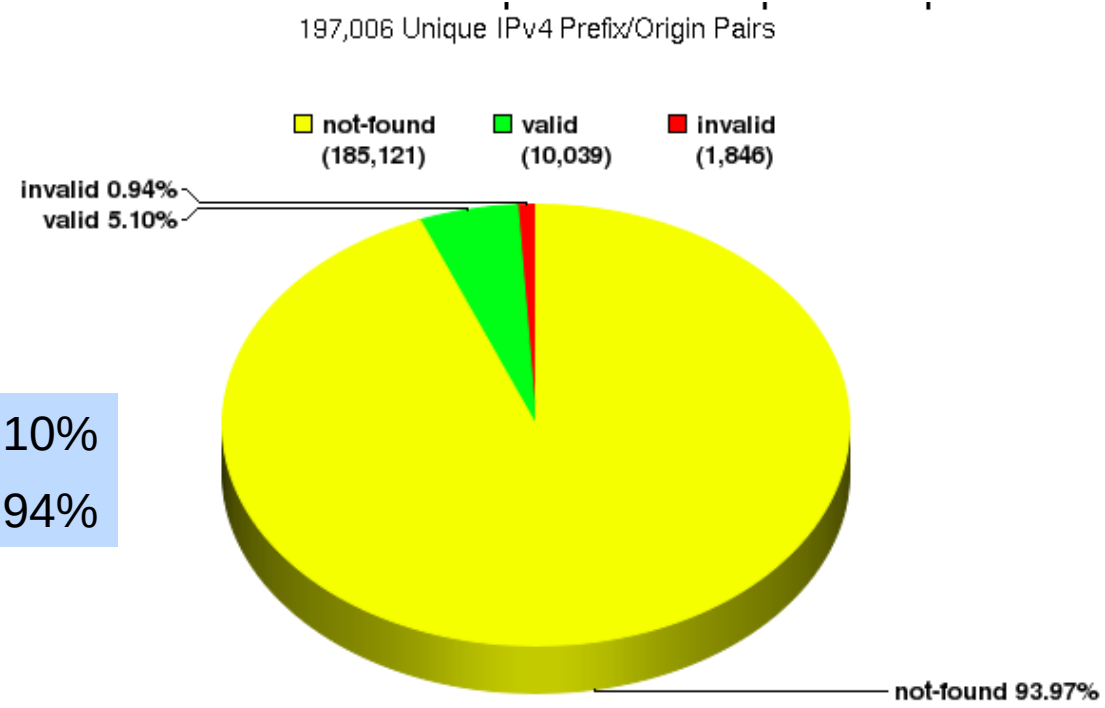


Valid	10.05%
Invalid	0.79%

NIST RPKI Monitor 2018-10-20

https://rpki-monitor.antd.nist.gov

RPKI Status – APNIC Region



Valid	5.10%
Invalid	0.94%

NIST RPKI Monitor 2018-10-20

https://rpki-monitor.antd.nist.gov

RPKI participation – APNIC

Registry	Number of RPKI particiants	Number with ROAs registered	% address space of participant covered by ROA (v4/v6)	% total space covered by ROA (v4/v6)
APNIC	1166	675	13.77% / 78.67%	3.54% / 0.12%
JPNIC	56	44	13.10% / 85.05%	1.56% / 21.00%
TWNIC	233	7	12.37% / 41.35%	3.98% / 2.89%
Total	**1455**	**726**	**13.61% / 80.89%**	**3.10% / 0.33%**

RPKI benefits

- Improved in-band verification of resource custodianship
  - Much safer than manually checking whois or IRR database
  - Ease of automation
- Secure Origin is the first step to preventing many attacks on BGP integrity
  - BGP Path remains a problem which is under development
  - Related information such as IRR Policy can now leverage strong proofs of validity (end the maintainer-authority problem in RADB/IRR)
- Instruction/information from the resource custodian can be cryptographically verified (e.g. LOA signing)

How do I start?

- Create ROAs to better protect your own routes
  - Encourage your peers/customers to do the same
  - Encourage your IXP to implement ROV in the RS
- Then
  - Set up route validation at your own border routers
  - Using public or IXP validator, or your own
- APNIC members, use MyAPNIC
  - We can help!
  - Please contact APNIC Helpdesk

Thanks!

pwilson@apnic.net