Handling Internet Network Abuse Reports at APNIC

21 October 2010

LAP-CNSA Workshop, Melbourne

George Kuo

Overview

- Introduction to APNIC

- Internet registry structure

- Common network abuse questions APNIC receives

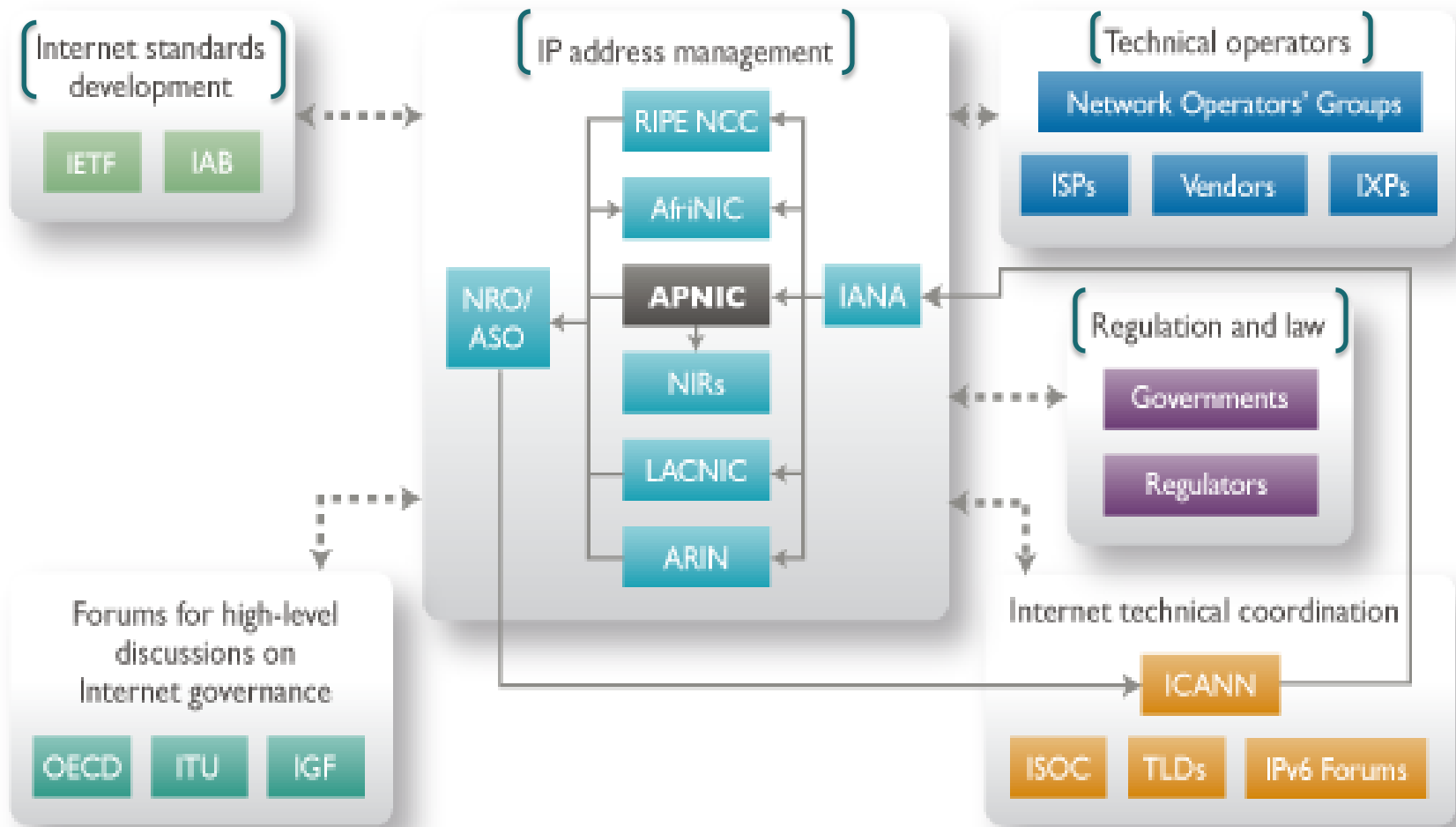- APNIC Whois Database registration

What is APNIC?

- Internet registry for the Asia Pacific
  - One of the five Regional Internet Registries
- Membership-based organization
  - Not for profit and services focused
- Internet resource policy coordination body
  - Consensus-based policy development
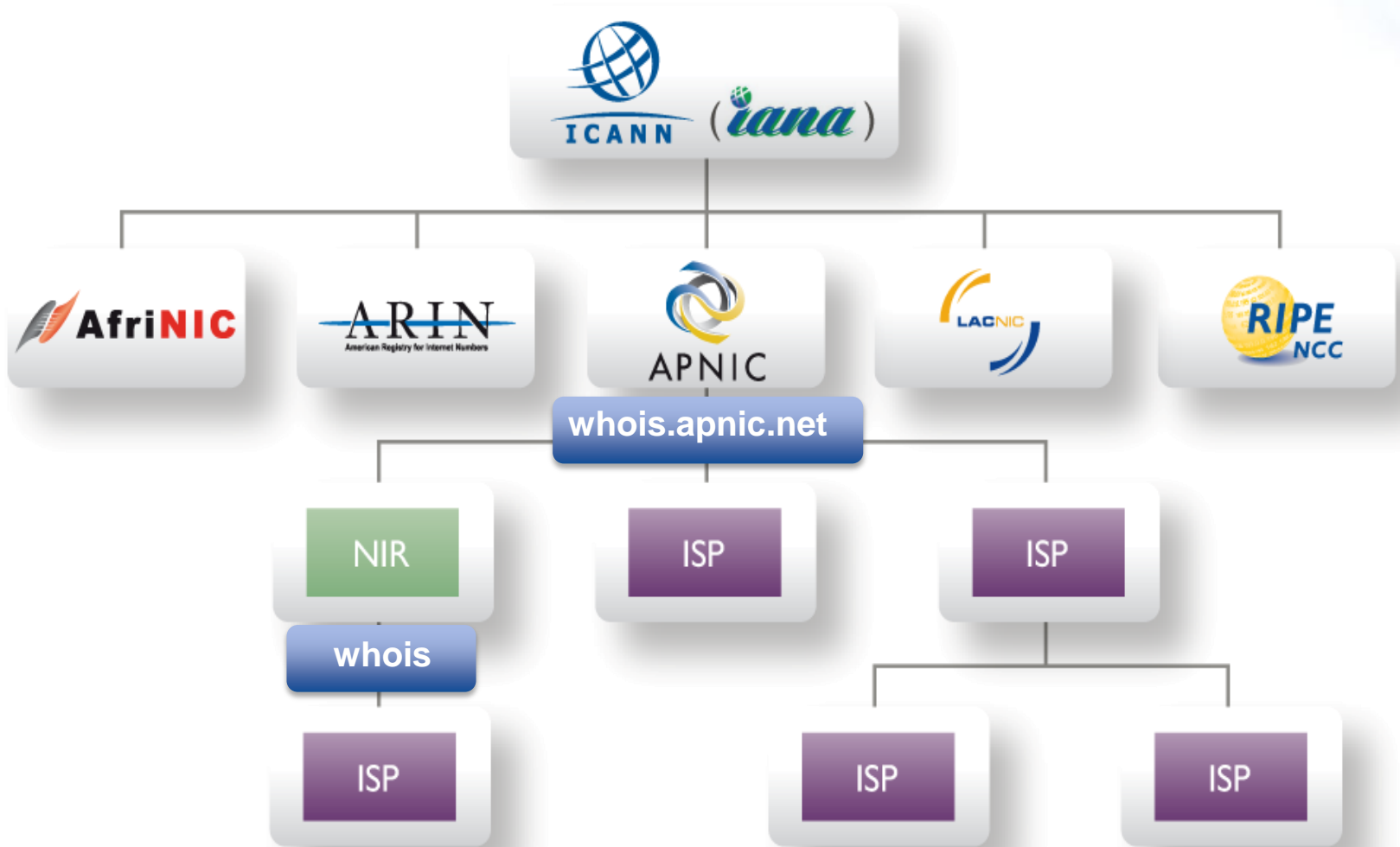 - Open and transparent decision making

APNIC's Role

- Distributes Internet resources
- Maintains APNIC Whois Database
- Facilitates resource policy development
- Manages Reverse DNS delegations
  - *But NOT a domain name registry*
- Provides training and outreach on resource management and APNIC services
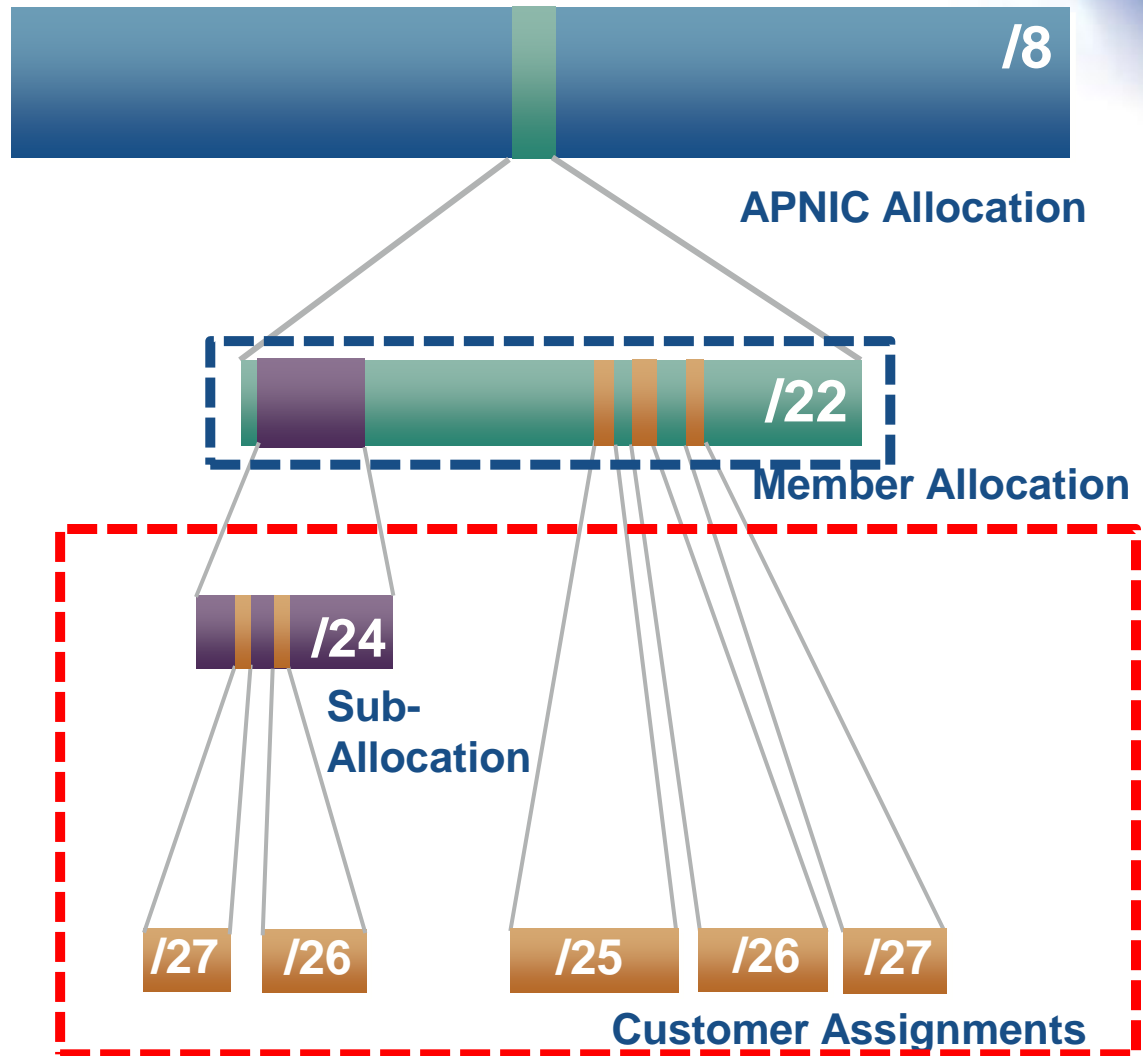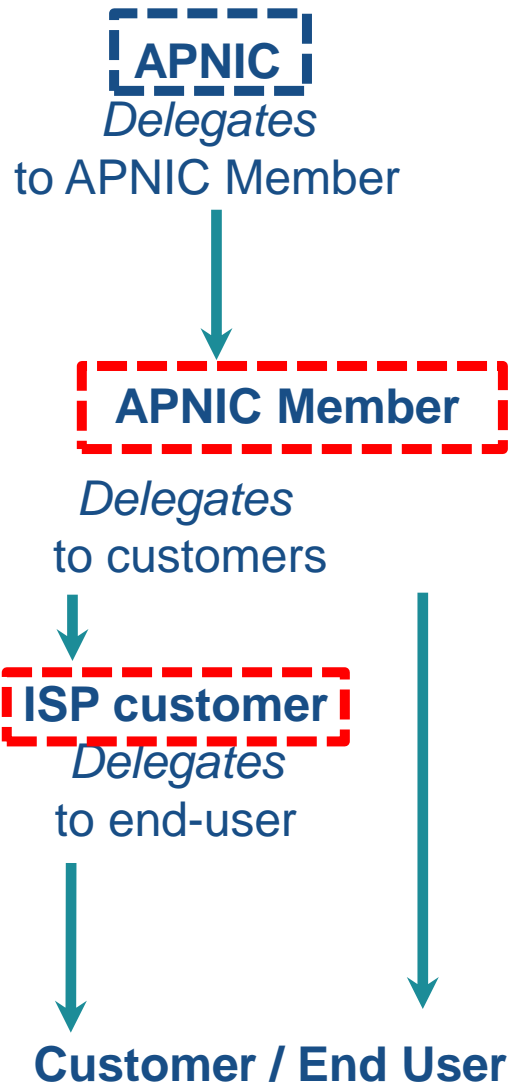- Supports Internet development

APNIC from a Global Perspective

Internet Registry Structure

Internet Resource Delegation

APNIC
Delegates
to APNIC Member

APNIC Member

Delegates
to customers

ISP customer
Delegates
to end-user

Customer / End User

/8

APNIC Allocation

/22

Member Allocation

/24

Sub-Allocation

/27   /26

/25   /26   /27

Customer Assignments

Common Questions…

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

- Can APNIC investigate or stop the network abuse?

- Can APNIC reclaim the Internet resources used for the network abuse?

- The contacts information in the APNIC Whois Database is invalid. What do I do?

Is APNIC the culprit?

- APNIC is listed by ARIN as holder of all IP space for the AP region
  - Some search tools look no further than this
  - For details, need to consult APNIC "whois"
- APNIC whois may or may not show specific customer assignments for the addresses in question
  - But will show the ISP holding APNIC space

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

What Can You Do?

- Use the APNIC Whois Database to obtain network contact information

- Contact the network responsible and also its ISP/upstream

- Contact APNIC for help, advice, training or support

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', 'lookingglass' and RIS may be used to track the upstream provider if needed
  - More information available from APNIC

Can APNIC reclaim addresses?

- Sometimes…
  - Where IP space has been obtained fraudulently or under false pretences (which is often the case)

- But…
  - APNIC does not regulate Internet activity
  - Current address management policy do not cover network abuse

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
```

Questions?

- APNIC Whois inquiry
  - www.apnic.net/helpdesk
- More information on network abuse
  - www.apnic.net/abuse
- Report invalid contacts
  - www.apnic.net/invalidcontacts
- Or
  - Send email to helpdesk@apnic.net

You're invited…

- http://www.apnic.net/meetings

Thanks

George Kuo,

APNIC