Handling Network Abuse Reports at APNIC

17 November 2010

APT Cybersecurity Forum, Sydney

George Kuo

Member Services Manager, APNIC

APT Bali Plan of Action Nov 2009

A. Widen broadband connectivity

B. Provide a secure, safe, and sustainable environment through ICT initiatives

C. Facilitate effective convergence of services

- Timely implementation of IPv6

D. Encourage development of content and applications

E. Develop human resource capacity

http://www.unescap.org/idd/events/2009_IWG_on_ICT/APT-%20IWG13.ppt

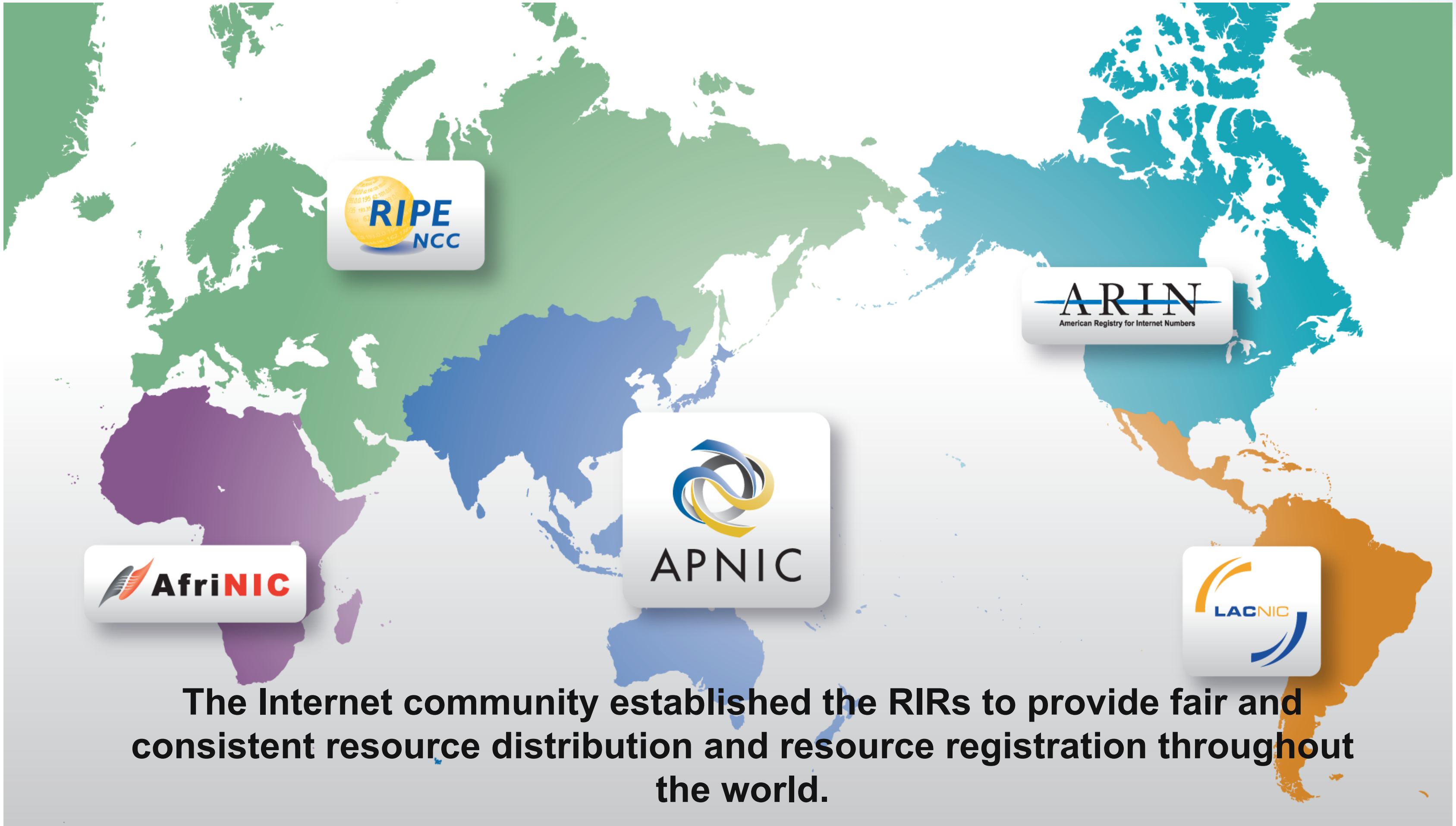
Overview

- Introduction to APNIC
- Internet registry structure
  - Internet resources distribution & management
  - Internet resources Policy development
- Common network abuse questions APNIC receives
- Using APNIC Whois Database

APNIC's Mission

- Assist the Asia Pacific community in effective resource management
  - Equitable allocation and registration services
  - Membership total: 2,397
- Provide educational opportunities
  - Fully equipped Training lab (IPv6 supported)
- Coordinate IP addressing policy development and public positions
- Seek public consideration of issues that benefit members and the community

Regional Internet Registries



The Internet community established the RIRs to provide fair and consistent resource distribution and resource registration throughout the world.

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

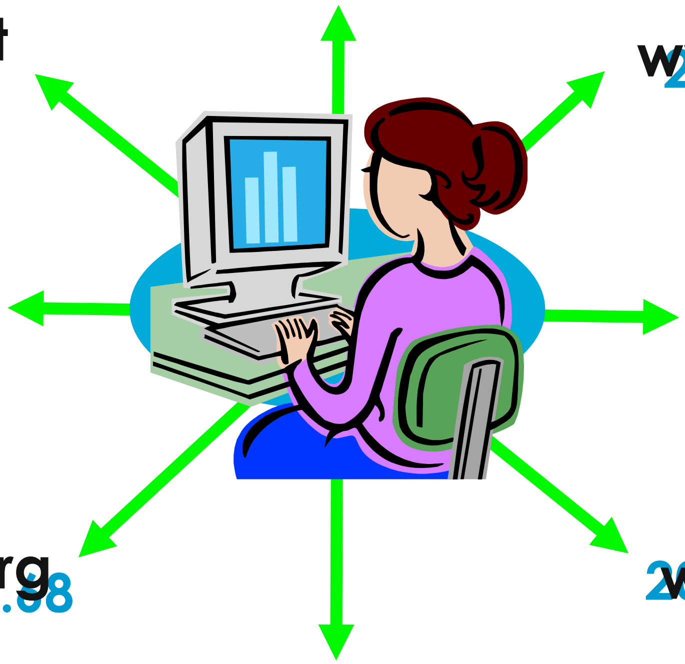
What is an IP address?

- The Internet Protocol
  - Packets, addressing and routing
  - IPv4 (192.168.0.0)
  - IPv6 (2001:0DB8::/32)

- An IP address is a number
  - Every device directly connected to the Internet needs a unique IP address
  - IP address space is finite

- ***Not the same as a Domain Name !***

On the Internet, you are an IP Address!



www.afrinic.net
196.216.2.1

www.nro.net
193.0.0.131

www.apnic.net
202.12.29.20

www.aptsec.org
116.68.148.161

www.arin.net
192.149.252.7

www.isoc.org
206.131.253.68

www.lacnic.net
200.160.2.15

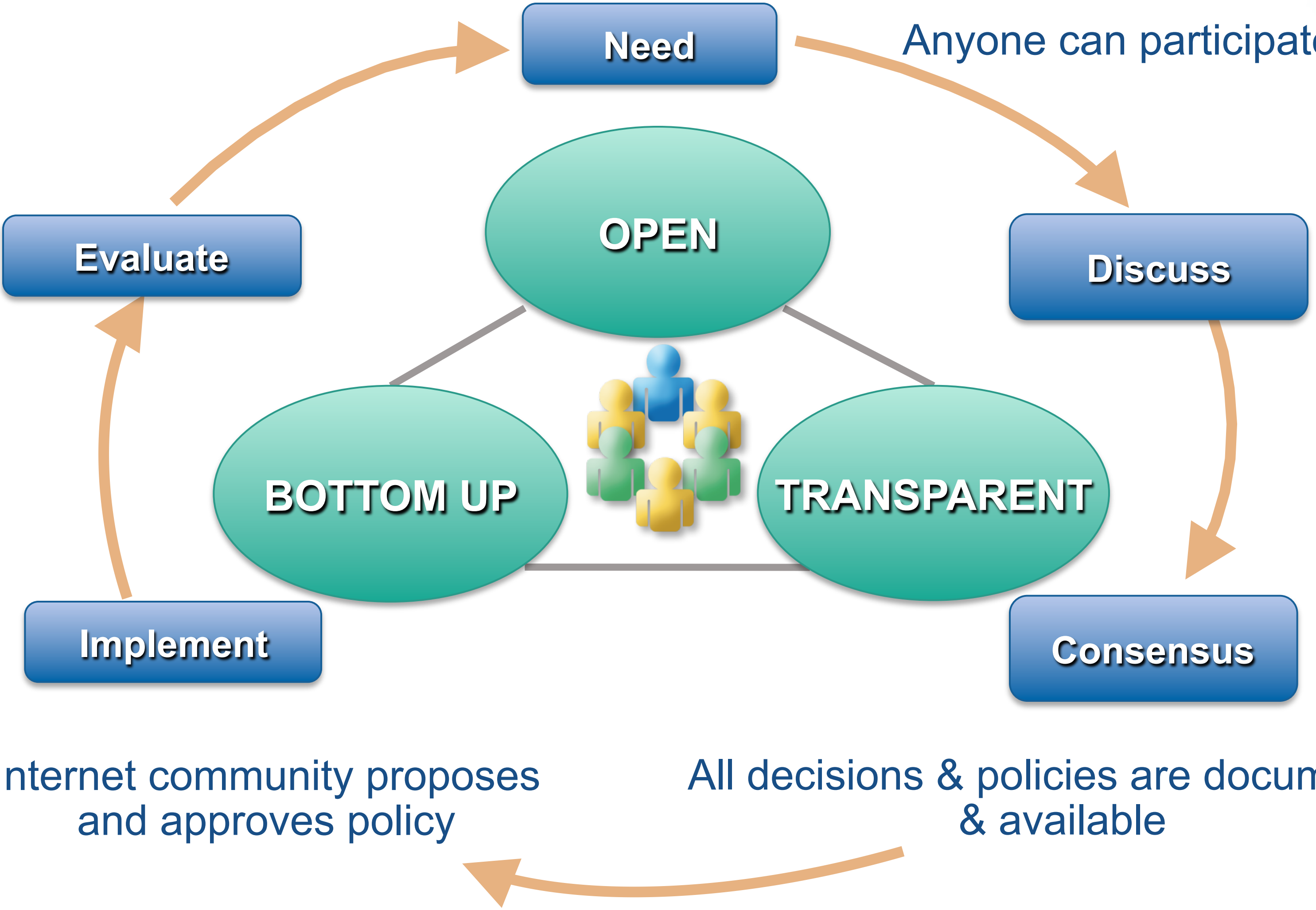
www.ripe.net
192.0.0.214

Internet Resources Management Goals

Internet resources management policies

- Efficient address usage
  - Avoid wasteful practices
- Aggregation
  - Hierarchical distribution
  - Aggregation of routing information
  - Limiting number of routing entries advertised
- Registration
  - Unique, Fair, & Consistent

Policy Development Process



Anyone can participate

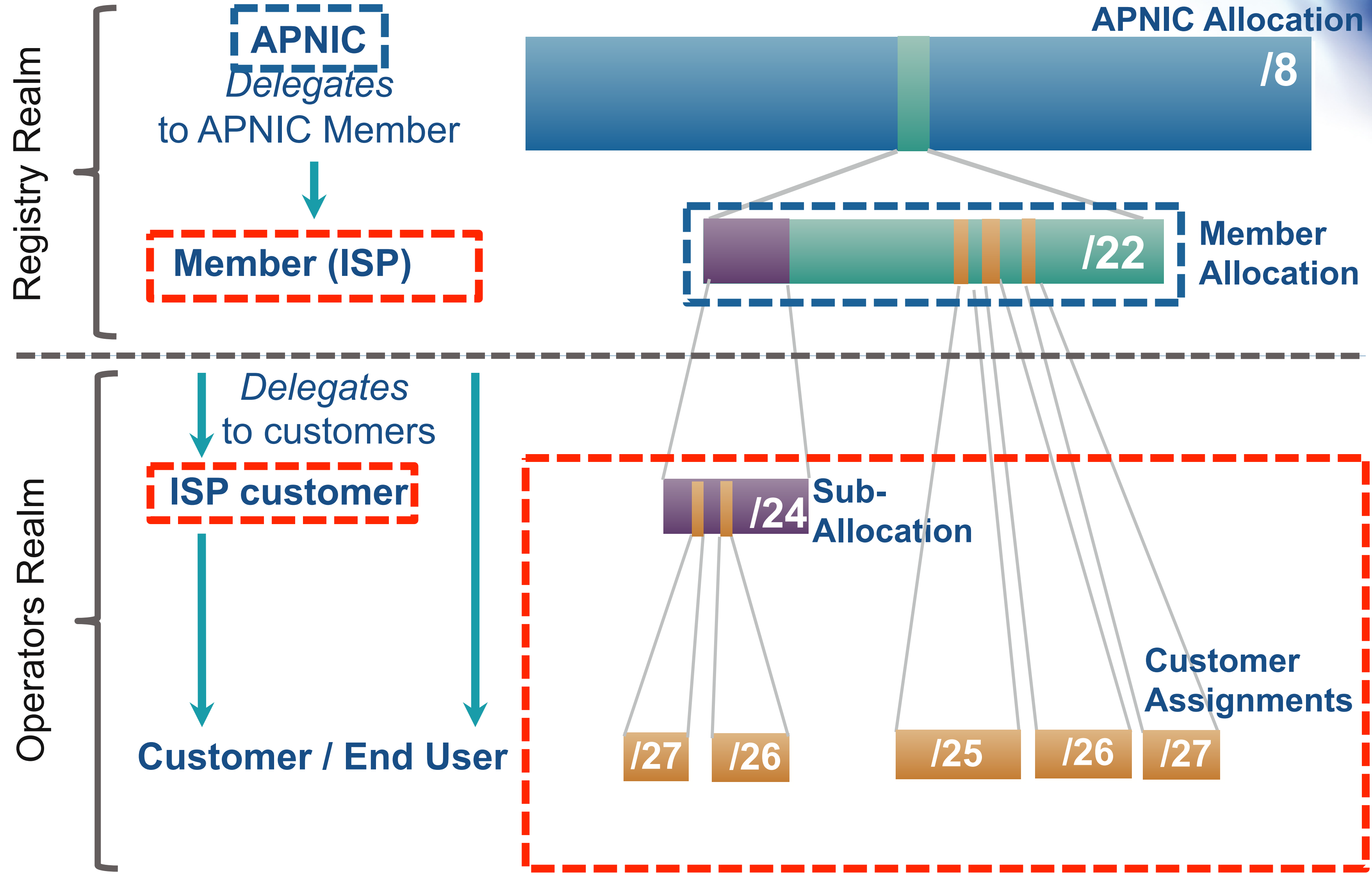
Internet community proposes and approves policy

All decisions & policies are documented & available

How are IP Addresses Delegated?

1. Internet resources management policies
   - Criteria for obtaining resources
2. APNIC to register the delegation in Whois database
3. APNIC Members are responsible for further distribution and registration

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

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

1. Web browser
   - http://www.apnic.net/whois
2. whois client or query tool
   - whois.apnic.net
3. Identify network contacts from the registration records
   - IRT (Incident Response Team) object if present
     - Policy for mandatory abuse contact field implemented on 8 Nov 2010
   - Contacts: “tech-c” or “admin-c”

Abuse Contact Information

- APNIC community reached a consensus to implement dedicated security incident contacts in the Whois Database
- Mandatory “Abuse Contact” for all IP and ASN registrations
- Assist in network abuse handling in the Asia Pacific Internet community

What if Whois Info is Invalid?

Members (ISPs) are responsible for reporting changes to APNIC

- Under formal membership agreement

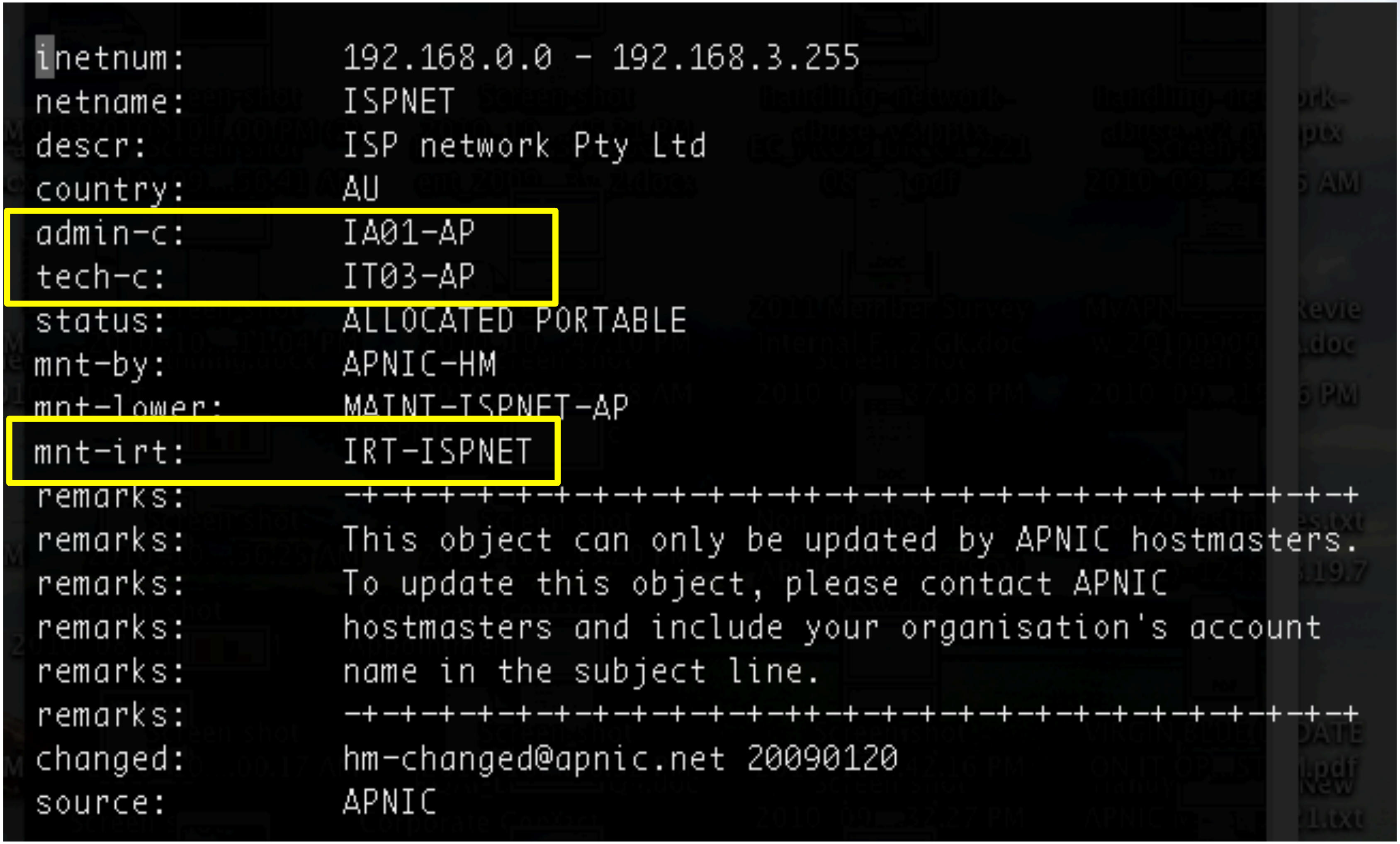
Report invalid ISP contacts to APNIC

- http://www.apnic.net/invalidcontact
- APNIC will contact Member and update registration details

What if Whois Info is Invalid?

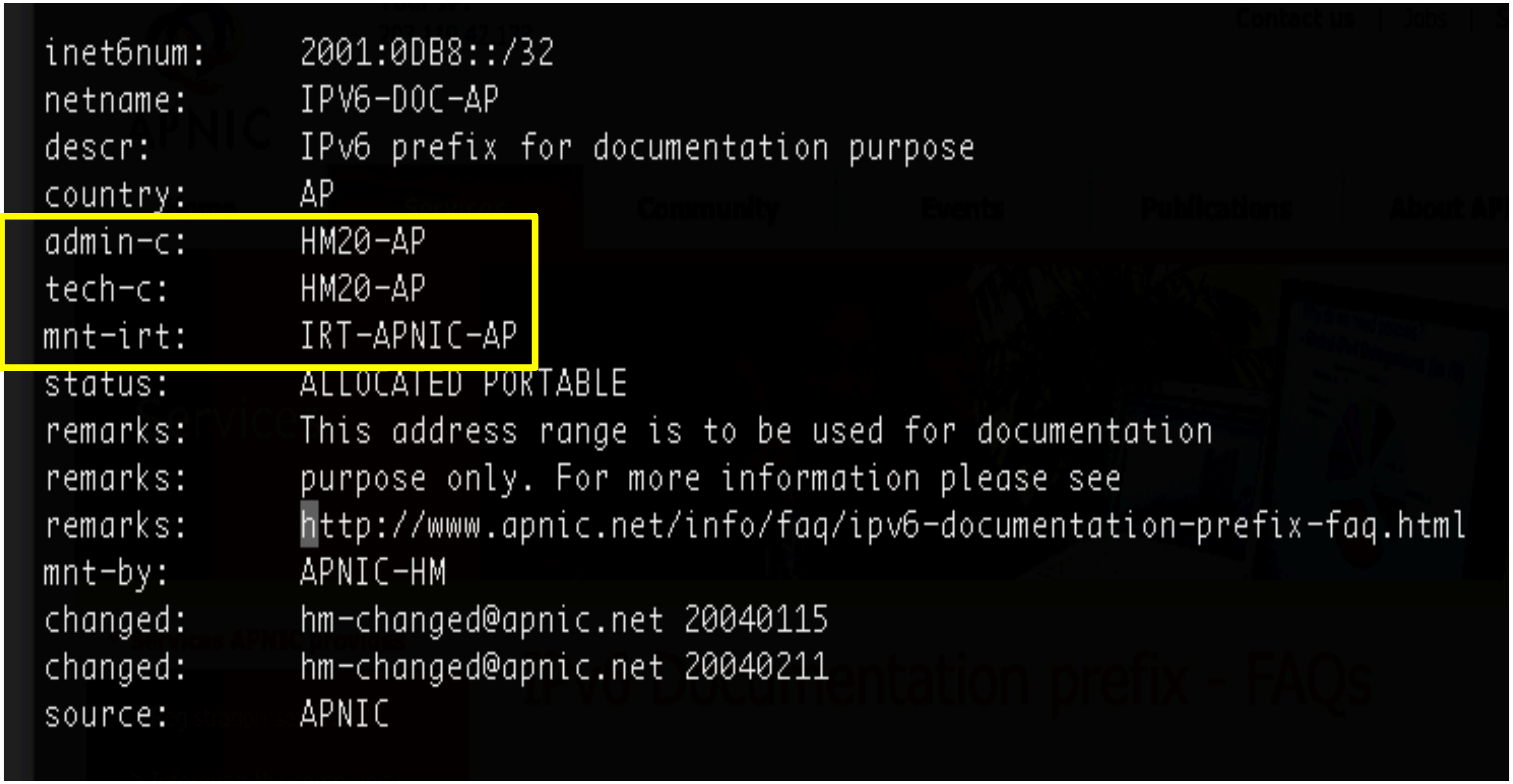
- Customer assignment information is the responsibility of ISPs
  - ISPs are responsible for updating their customer network registrations
- Tools such as ‘traceroute’, ‘lookingglass’, and RIS may be used to track the upstream provider if needed
  - More information available from APNIC

APNIC Whois Registration IPv4 Object



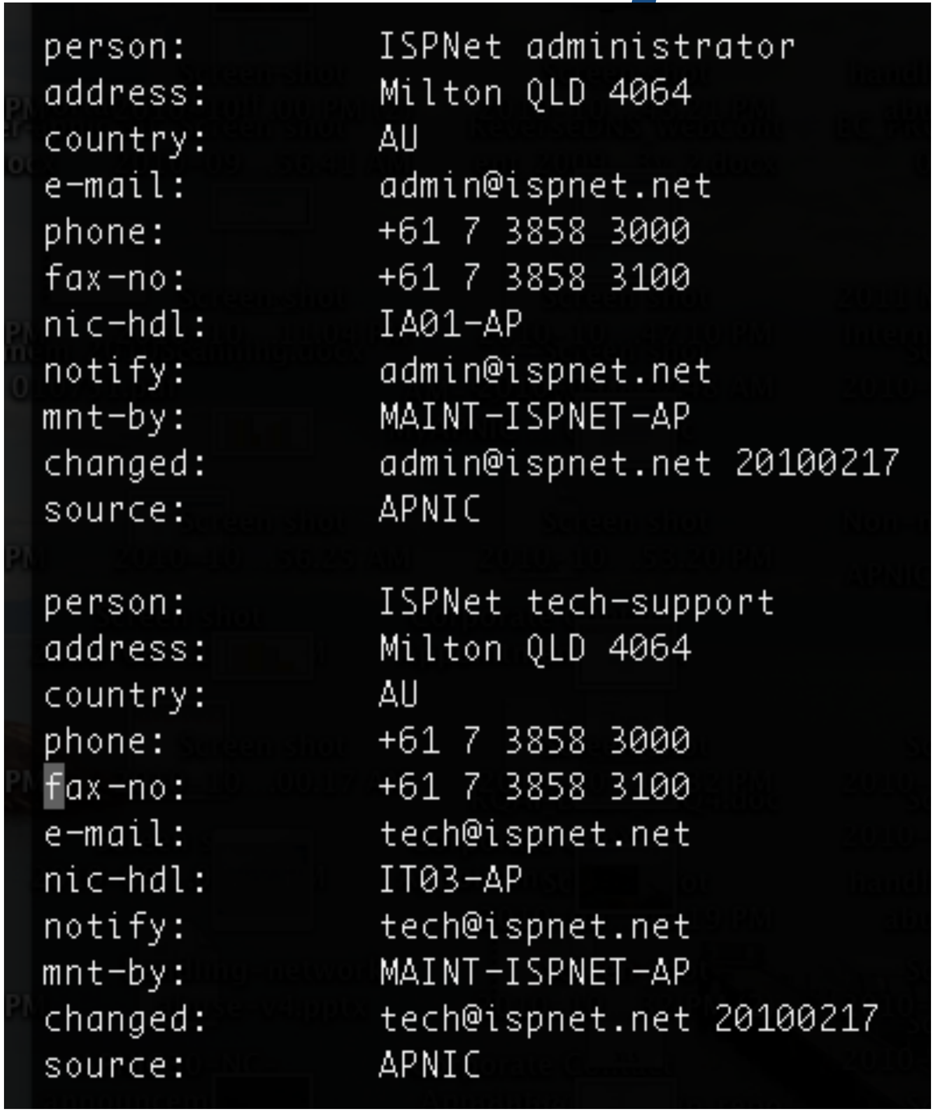
```
inetnum:        192.168.0.0 - 192.168.3.255
netname:        ISPNET
descr:          ISP network Pty Ltd
country:        AU
admin-c:        IA01-AP
tech-c:         IT03-AP
status:         ALLOCATED PORTABLE
mnt-by:         APNIC-HM
mnt-lower:      MAINT-ISPNET-AP
mnt-irt:        IRT-ISPNET
remarks:        -+-+-+-+-+-+-+-+-+-+-+-++-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
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 IPv6 Object



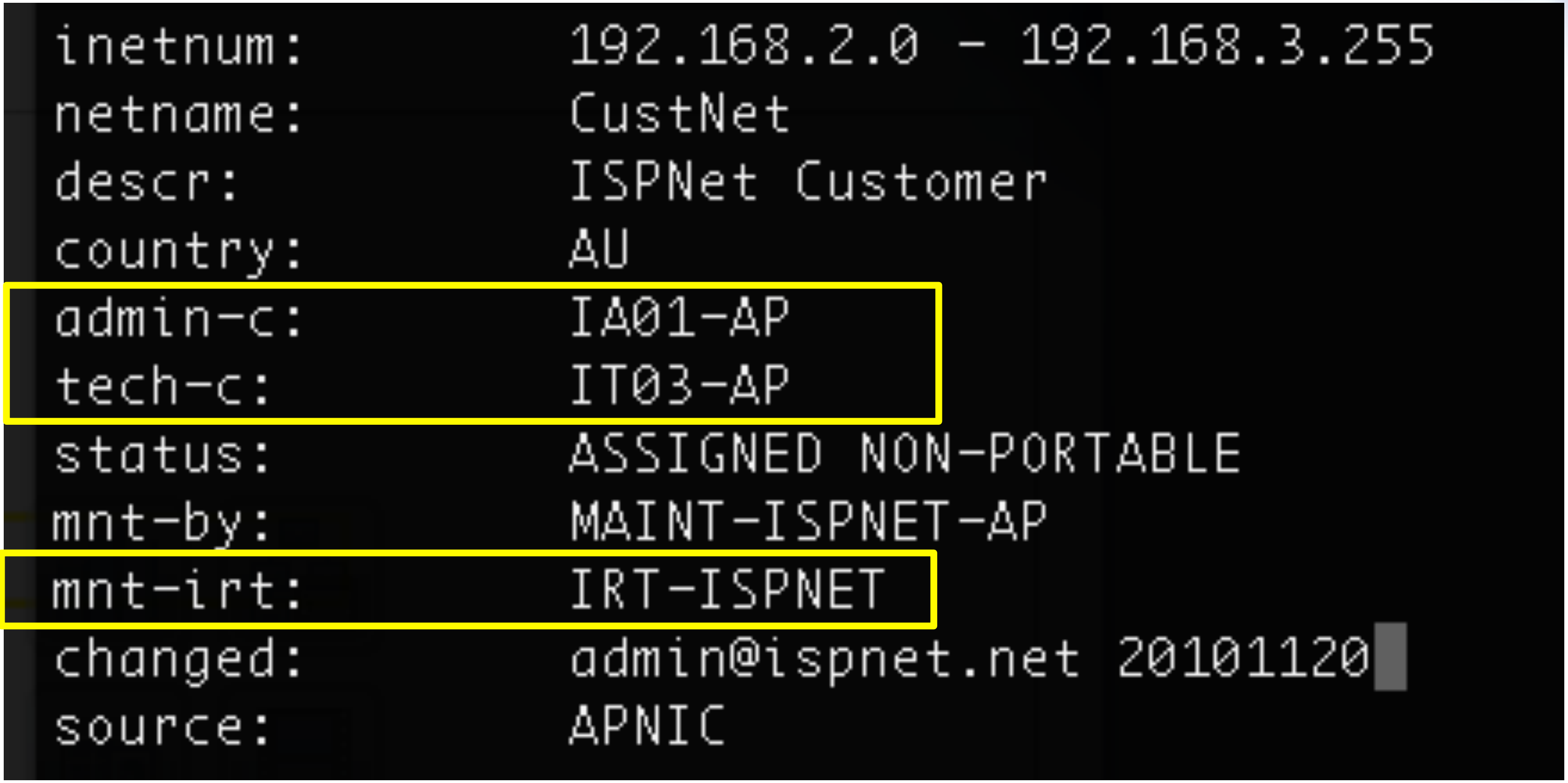
```
inet6num:      2001:0DB8::/32
netname:       IPV6-DOC-AP
descr:         IPv6 prefix for documentation purpose
country:       AP
admin-c:       HM20-AP
tech-c:        HM20-AP
mnt-irt:       IRT-APNIC-AP
status:        ALLOCATED PORTABLE
remarks:       This address range is to be used for documentation
remarks:       purpose only. For more information please see
remarks:       http://www.apnic.net/info/faq/ipv6-documentation-prefix-faq.html
mnt-by:        APNIC-HM
changed:       hm-changed@apnic.net 20040115
changed:       hm-changed@apnic.net 20040211
source:        APNIC
```

APNIC Whois Registration Person Object



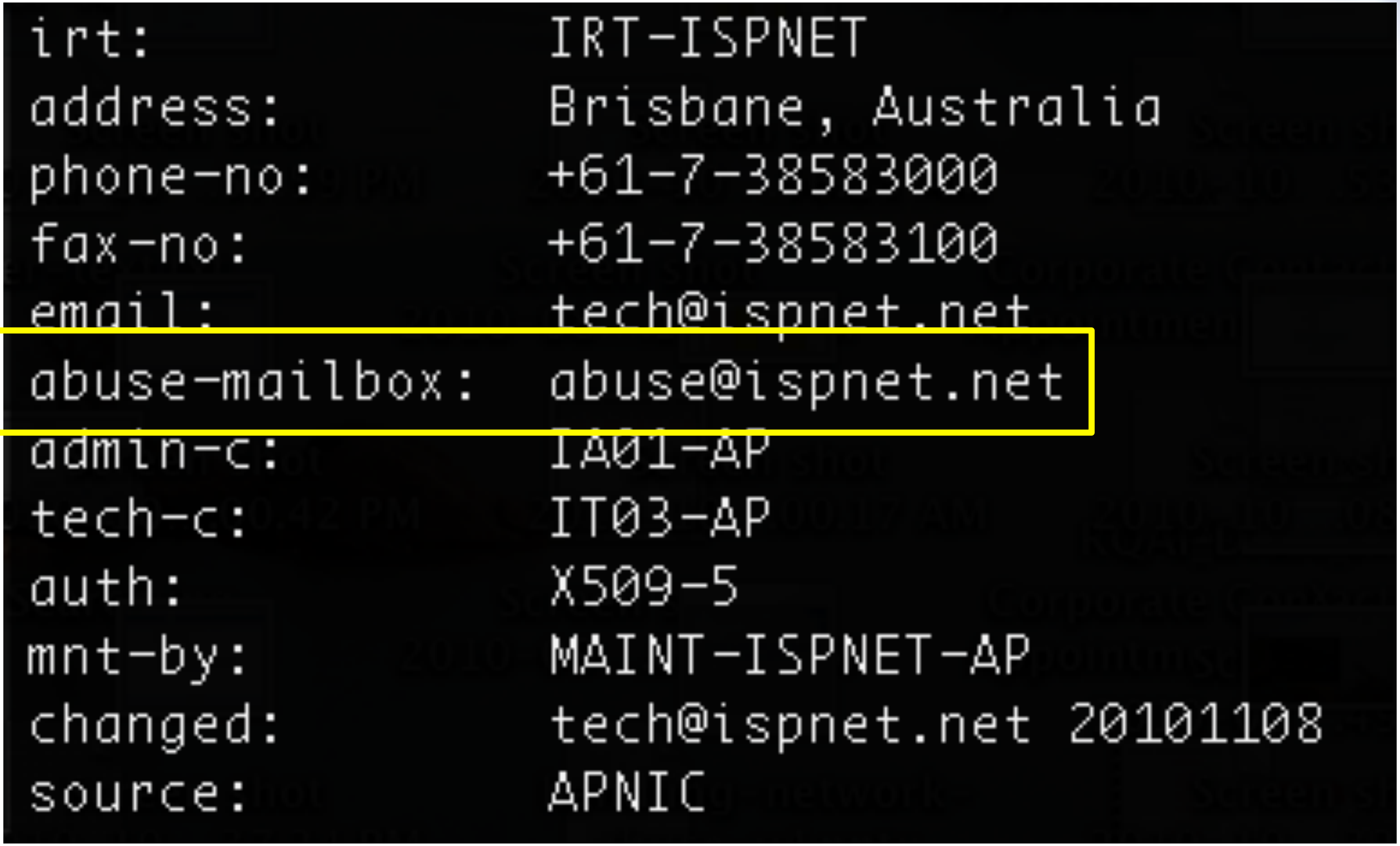
```
person:         ISPNet administrator
address:        Milton QLD 4064
country:        AU
e-mail:         admin@ispnet.net
phone:          +61 7 3858 3000
fax-no:         +61 7 3858 3100
nic-hdl:        IA01-AP
notify:         admin@ispnet.net
mnt-by:         MAINT-ISPNET-AP
changed:        admin@ispnet.net 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 IPv4



```
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

Next APNIC meeting APNIC 31

Contact | About APNIC | APNIC

APNIC 31

21 - 25 February 2011
Hong Kong SAR, China

In partnership with APRICOT 2011

Participate remotely

http://meetings.apnic.net/31/remote

Call for Papers

The Program Committee will be accepting proposals soon.

Learn more about the Program

Fellowships

The Fellowship program opens soon for any interested applicants.

Learn more about Fellowships

Thanks!

George Kuo
<george@apnic.net>