APNIC Whois Database and use of Incident Response Team (IRT) registration

Terry Manderson
APNIC
AusCERT 2003

Contents

- What is APNIC?
- The APNIC Whois Database
- Reporting abuse
- Invalid contacts
- IRT object

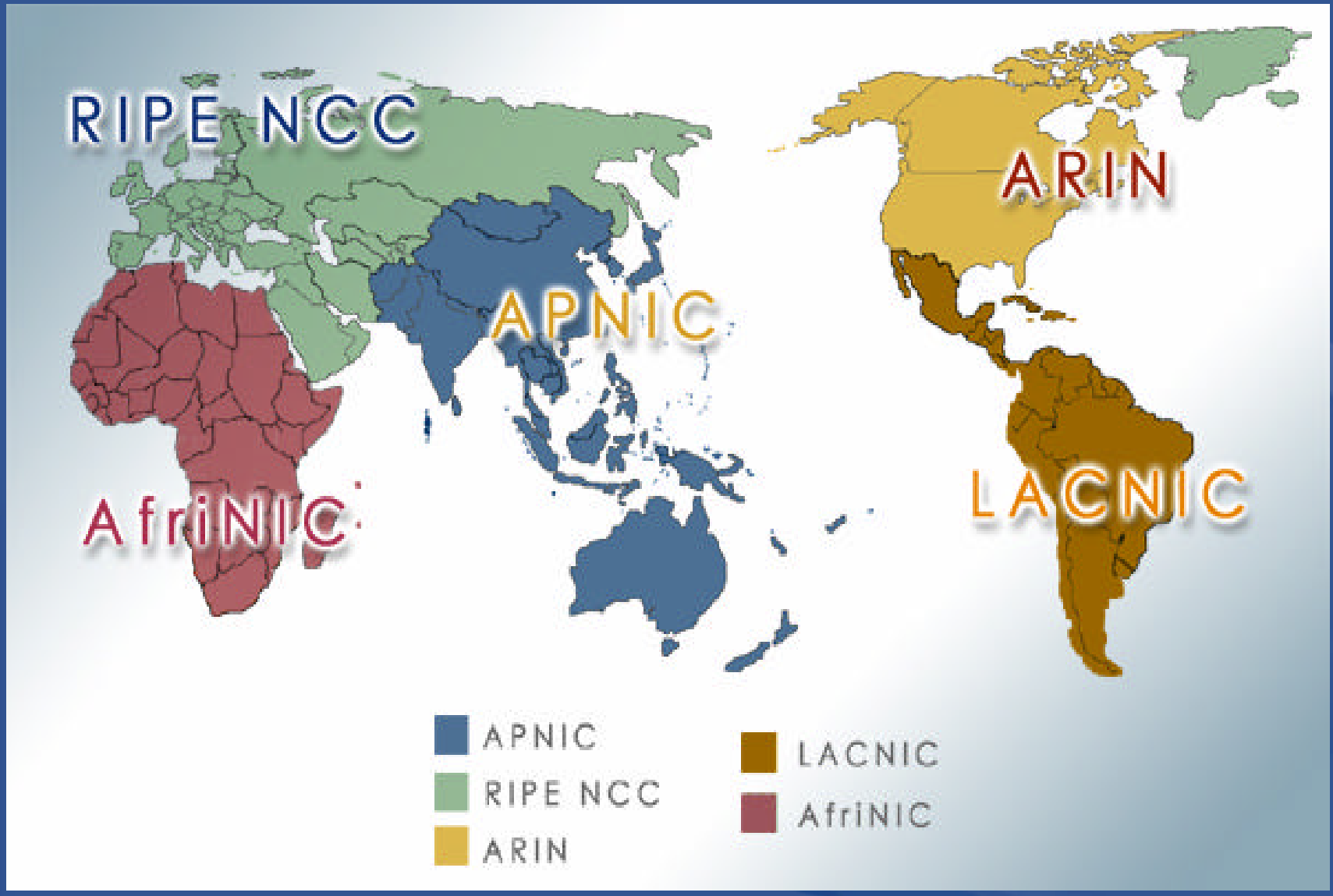
What is APNIC?

- Regional Internet Registry (RIR) for the Asia Pacific Region
  - Regional authority for Internet Resource distribution
  - IP addresses (IPv4 and IPv6), AS numbers, in-addr.arpa and ip6.arpa delegation
- Non-profit, neutral and independent

What does APNIC do?

1. Internet resource management
   - IP address allocations & assignments
   - AS number assignments
2. Resource registration
   - Authoritative registration server: *whois*
   - APNIC Routing Registry
3. DNS management
   - Delegate reverse DNS zones/domains
   - Authoritative DNS servers
     - *in-addr.arpa, ip6.arpa (ip6.int)*

Regional Internet Registries



Asia Pacific Network Information Centre

APNIC

APNIC Whois Database

- Command line

  `whois –h whois.apnic.net`

- Web interface

  `www.apnic.net/apnic-bin/whois.pl`

The APNIC Whois Database

- Resource registrations
  - IP addresses
  - AS numbers
  - reverse DNS delegations
- Also routing information
- No conventional DNS registrations

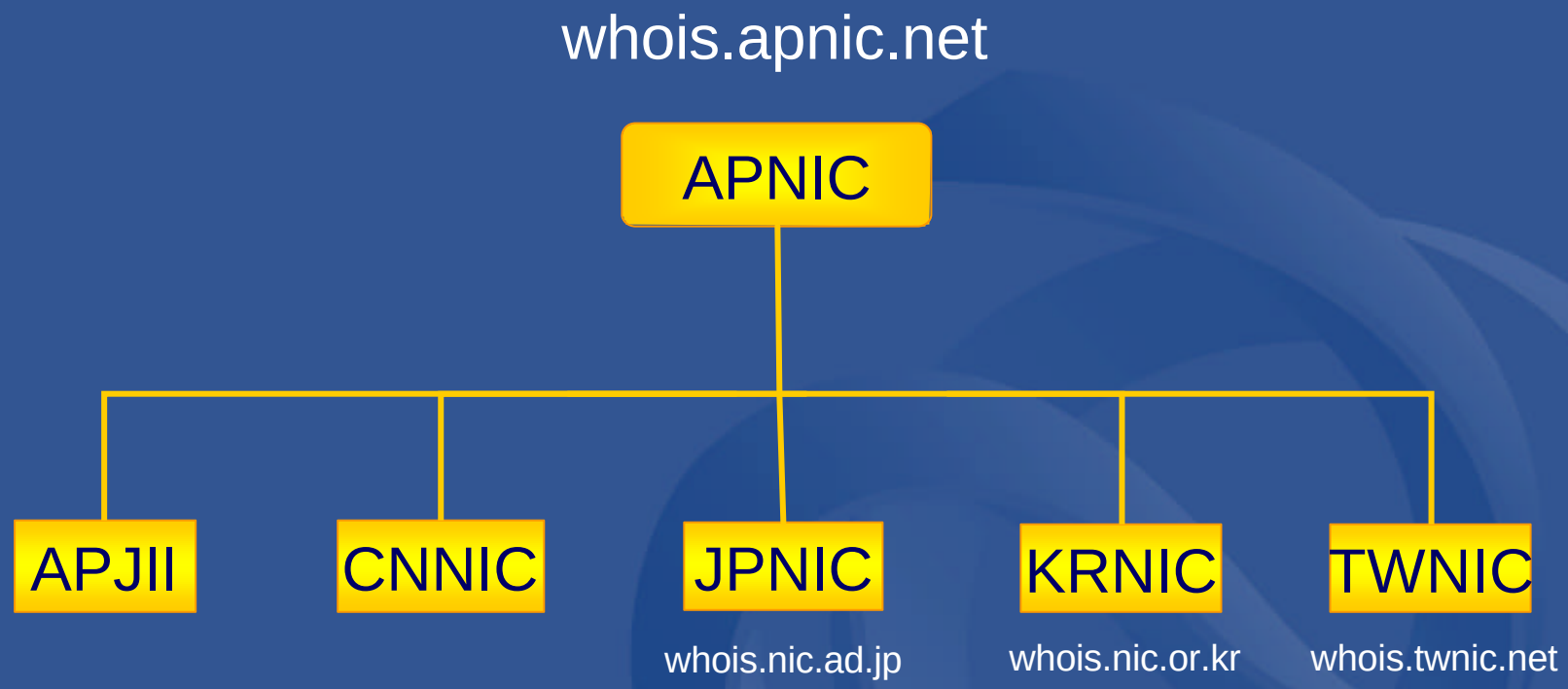
The APNIC Whois Database

- All IP addresses managed by APNIC
- Allocated to APNIC by IANA
  - 60/7, 202/7, 210/7, 218/7, 220/7, 222/8
- Transferred to APNIC
  - AUNIC
    - 203.0/10
  - Early Registration Transfer (ERX)
    - 128/8, 141/8, 150/8, 151/8, 163/8
    - More ranges to be transferred in future
    - See http://www.apnic.net/db/erx

The APNIC Whois Database

- Mirrors National Internet Registry (NIR) databases
  - check NIR database for most accurate information

National Internet Registry databases



How IP addresses are managed

- APNIC allocates addresses in large blocks to ISP networks
  - Current minimum is /20 (4,096 IP addresses)
  - Allocations are registered in the APNIC Whois Database
- The ISP then makes smaller assignments to its customers from the allocated space
  - All assignments are registered in the APNIC Whois Database

How IP addresses are managed

APNIC
Allocates
to APNIC Member

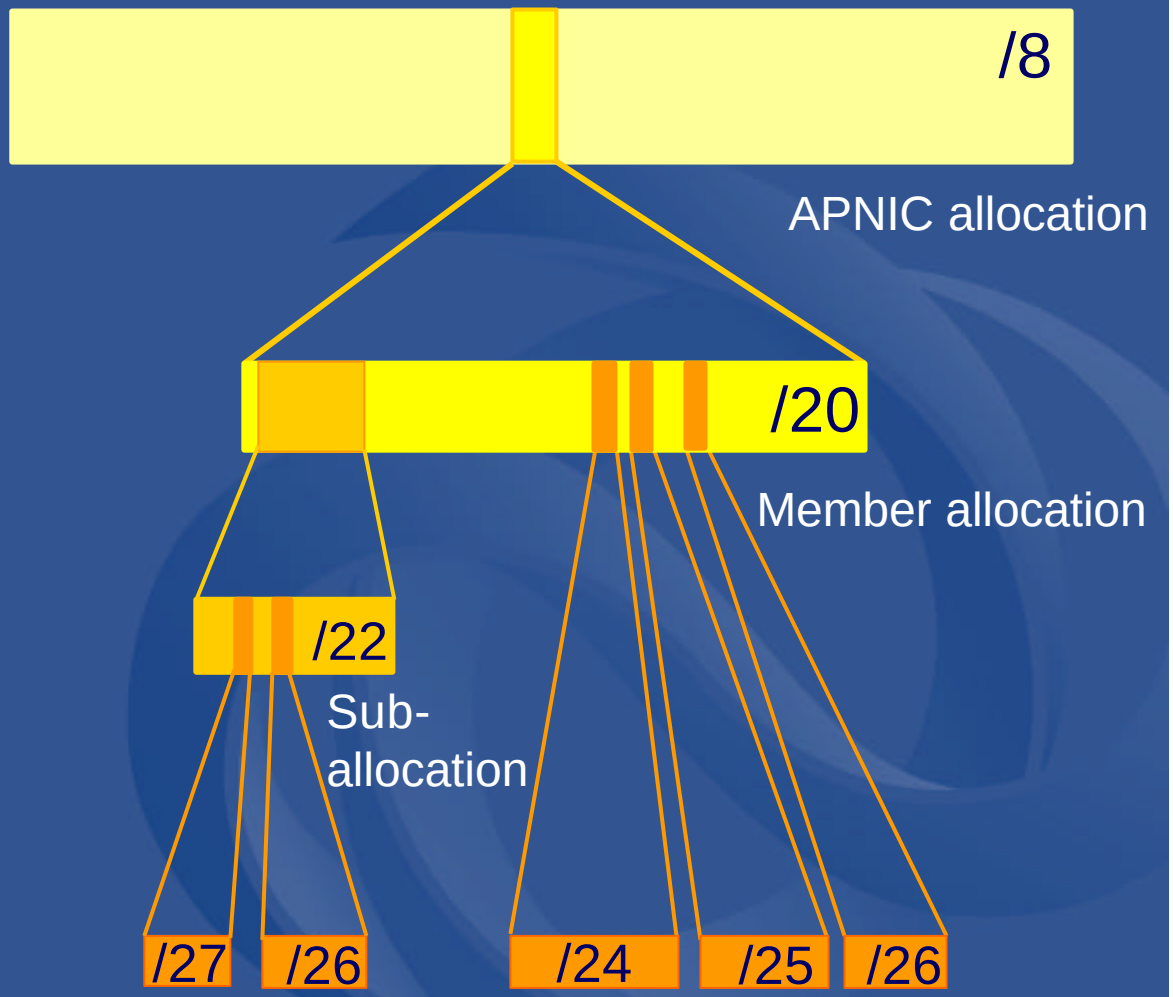
APNIC Member

Assigns
to end-user

Allocates
to downstream

Downstream
Assigns
to end-user

Customer / End user



Asia Pacific Network Information Centre

APNIC

Reporting abuse

- Contact
  - tech-c
  - admin-c

```
inetnum:   202.181.0.0 - 202.185.255.255
netname:   EXAMPLENET-WF
…
country:   WF
admin-c:   EIPA97-AP
tech-c:    ENOC100-AP
…
```

```
role:      ExampleNet IP Administration
…
phone:     +680-368-0844
fax-no:    +680-367-1797
e-mail:    ipadmin@example.net
nic-hdl:   EIPA97-AP
…
```

Reporting abuse

- Contact
  - tech-c
  - admin-c
- Or use remarks

```
inetnum:   202.181.0.0 - 202.185.255.255
netname:   EXAMPLENET-WF
…
country:   WF
admin-c:   EIPA97-AP
tech-c:    ENOC100-AP
remarks:   Spam reports to
           spam@example.net
remarks:   Security incidents to
           abuse@example.net
…
```

Reporting abuse

- Contact
  - tech-c
  - admin-c
- Or use remarks
- Or associated

  IRT
  - More on this later

```
inetnum:   202.181.0.0 - 202.185.255.255
netname:   EXAMPLENET-WF
…
country:   WF
admin-c:   EIPA97-AP
tech-c:    ENOC100-AP
mnt-irt:   IRT-EXAMPLENET-WF
…
```

Reporting abuse

- Contact
  - tech-c
  - admin-c
- Or use remarks
- Or associated IRT
  - More on this later
- Do not use changed field

```
inetnum:   202.181.0.0 - 202.185.255.255
netname:   EXAMPLENET-WF
…
country:   WF
admin-c:   EIPA97-AP
tech-c:    ENOC100-AP
changed:   hm-changed@apnic.net
…
```

Why are there invalid contacts?

- APNIC has allocated over 112 million IP addresses
  - Represented by over 384100 objects
- APNIC cannot contact many of the networks
  - Out of date records
  - Old historical records
- APNIC would like to contact these networks and help them update contact details
  - Are you one?

APNIC contacts invalid?

- Send an email to info@apnic.net
- Clearly state
  - Original IP address you queried
  - Invalid email addresses
- Don’t include original spam or intrusion logs
- KRNIC, JPNIC or TWNIC contacts invalid?
  - Contact the NIR directly

A new way to report security incidents

- Incident Response Team (IRT) object
  - A new APNIC Whois Database object type
- Yet to be implemented
- APNIC invites input by network security community

IRT object

```
$ whois -t irt

irt:            [mandatory]  [single]     [primary/look-up key]
address:        [mandatory]  [multiple]   [ ]
phone:          [mandatory]  [multiple]   [ ]
fax-no:         [optional]   [multiple]   [ ]
e-mail:         [mandatory]  [multiple]   [lookup key]
signature:      [mandatory]  [multiple]   [ ]
encryption:     [mandatory]  [multiple]   [ ]
admin-c:        [mandatory]  [multiple]   [inverse key]
tech-c:         [mandatory]  [multiple]   [inverse key]
auth:           [mandatory]  [multiple]   [ ]
remarks:        [optional]   [multiple]   [ ]
irt-nfy:        [optional]   [multiple]   [inverse key]
notify:         [optional]   [multiple]   [inverse key]
mnt-by:         [mandatory]  [multiple]   [inverse key]
changed:        [mandatory]  [multiple]   [ ]
source:         [mandatory]  [single]     [ ]
```

IRT object

```
irt:            irt-CERT-NL
address:        p/a SURFnet bv
address:        Postbus 19035
address:        3501 DA Utrecht
phone:          +31 30 2305305
fax-no:         +31 30 2305329
e-mail:         cert-nl@surfnet.nl
signature:      PGPKEY-A6D57ECE
encryption:     PGPKEY-A6D57ECE
admin-c:        SAM36-RIPE
tech-c:         SAM36-RIPE
auth:           PGPKEY-834125A1
auth:           PGPKEY-3D10C493
remarks:        CERT-NL is the Computer Emergency Response Team of
                SURFnet
remarks:        This is a level 2 IRT
                (http://www.ti.terena.nl/teams/level2.html)
irt-nfy:        cert-nl@SURFnet.nl
notify:         info@SURFnet.nl
notify:         tiirt@stelvio.nl
mnt-by:         TRUSTED-INTRODUCER-MNT
changed:        menno.pieters@stelvio.nl 20020305
source:         RIPE
```

IRT object

```
mntner:         TRUSTED-INTRODUCER-MNT
descr:          Maintainer for Trusted Introducer
descr:          Level 2 CSIRT teams
admin-c:        DS660-RIPE
tech-c:         MP2890-RIPE
tech-c:         MK1229-RIPE
tech-c:         GHB1-RIPE
upd-to:         tiirt@stelvio.nl
mnt-nfy:        tiirt@stelvio.nl
auth:           PGPKEY-7F74D279
auth:           PGPKEY-4852A5FF
auth:           PGPKEY-CD60C417
auth:           PGPKEY-7111E05E
notify:         ti@stelvio.nl
mnt-by:         TRUSTED-INTRODUCER-MNT
referral-by:    RIPE-DBM-MNT
changed:        Menno.Pieters@Stelvio.nl 20020219
changed:        Menno.Pieters@Stelvio.nl 20020305
changed:        Menno.Pieters@Stelvio.nl 20021030
changed:        Menno.Pieters@Stelvio.nl 20030122
source:         RIPE
```

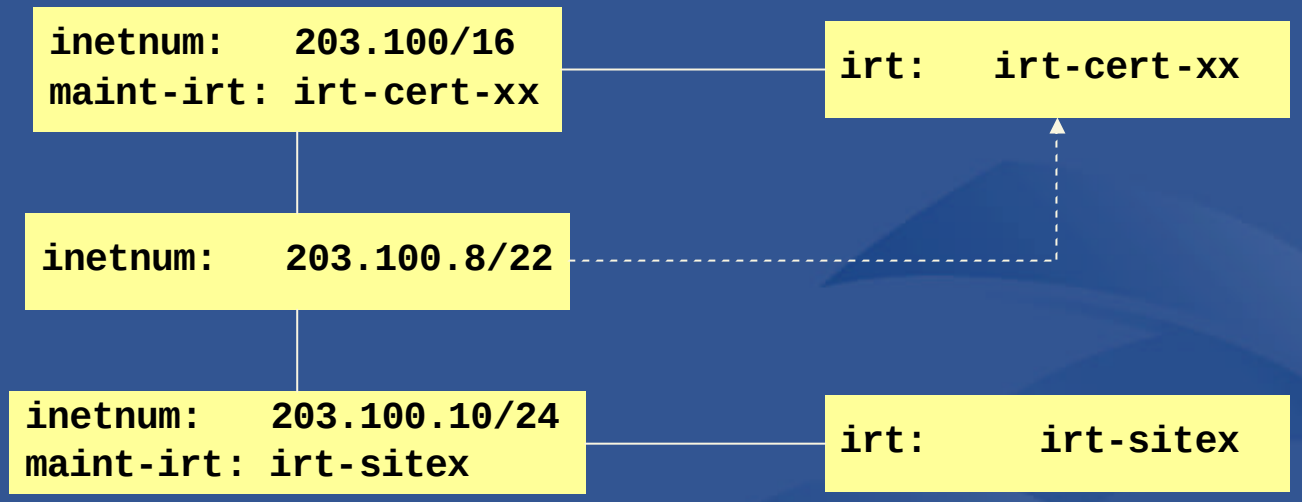

IRT object

```
inet6num:     2001:0610:0148::/48
netname:      Terena-NET-IPv6
descr:        Terena
country:      NL
admin-c:      TH378-RIPE
tech-c:       TH378-RIPE
notify:       info@SURFnet.nl
mnt-by:       SN-LIR-MNT
mnt-irt:      irt-CERT-NL
status:       ALLOCATED-BY-LIR
changed:      Rogier.Spoor@SURFnet.nl 20021115
source:       RIPE
```

IRT object

```
role:         SURFnet Account Management
address:      Radboudkwartier 273
address:      3511 CK  Utrecht
address:      The Netherlands
phone:        +31 30 2305305
fax-no:       +31 30 2305329
e-mail:       info@surfnet.nl
admin-c:      WD42-RIPE
admin-c:      PH300-RIPE
tech-c:       WD42-RIPE
tech-c:       PH300-RIPE
nic-hdl:      SAM36-RIPE
notify:       info@surfnet.nl
mnt-by:       SN-LIR-MNT
changed:      Peter.Hinrich@SURFnet.nl 20000125
changed:      Peter.Hinrich@SURFnet.nl 20000801
changed:      Walter.vanDijk@SURFnet.nl 20010909
source:       RIPE
```

IRT hierarchy




```
$ whois –c 203.100.8/22
inetnum:    203.100/16
...
mnt-irt:    irt-cert-xx
$ whois irt-cert-xx
...
```

Policy issues

- Encourage use of IRT object?
- Establish “trusted introducers” ?
  - regional or country based
- Should APNIC accept irt objects from other bodies?
- How to represent scope of “abuse” to be handled by IRTs?
  - eg spam vs security
  - cannot stop use of IRT object for any purpose

Policy issues

- APNIC invites you to discuss IRT issues on the Database SIG mailing list
  - sig-db@apnic.net
- We look forward to hearing your ideas on the list