



APNIC

Asia Pacific Network Information Centre

APNIC Whois Tutorial

Save Vocea/ Sanjaya - APNIC

PacINET2002

28 November 2002, Fiji



Overview

- APNIC introduction
- APNIC Whois database
- Using the Whois database
- Database updates

Did you know (in the AP region):

- Every network IP address assignment should be registered in the APNIC database?
- You can use the APNIC Whois database as a diagnostic tool if you are:
 - A network operator
 - An Internet end user

Introducing APNIC

- Regional Internet Registry (RIR) for the Asia Pacific Region
 - Regional authority for Internet resource distribution
 - IP addresses (IPv4 and IPv6), AS numbers, reverse DNS delegation
 - Provide services to 700+ members and NIR's
- Industry self-regulatory body
 - Participation by those who use Internet resources
 - Consensus-based, open and transparent
 - Non-profit, neutral and independent
 - Open membership-based structure

APNIC is Not...

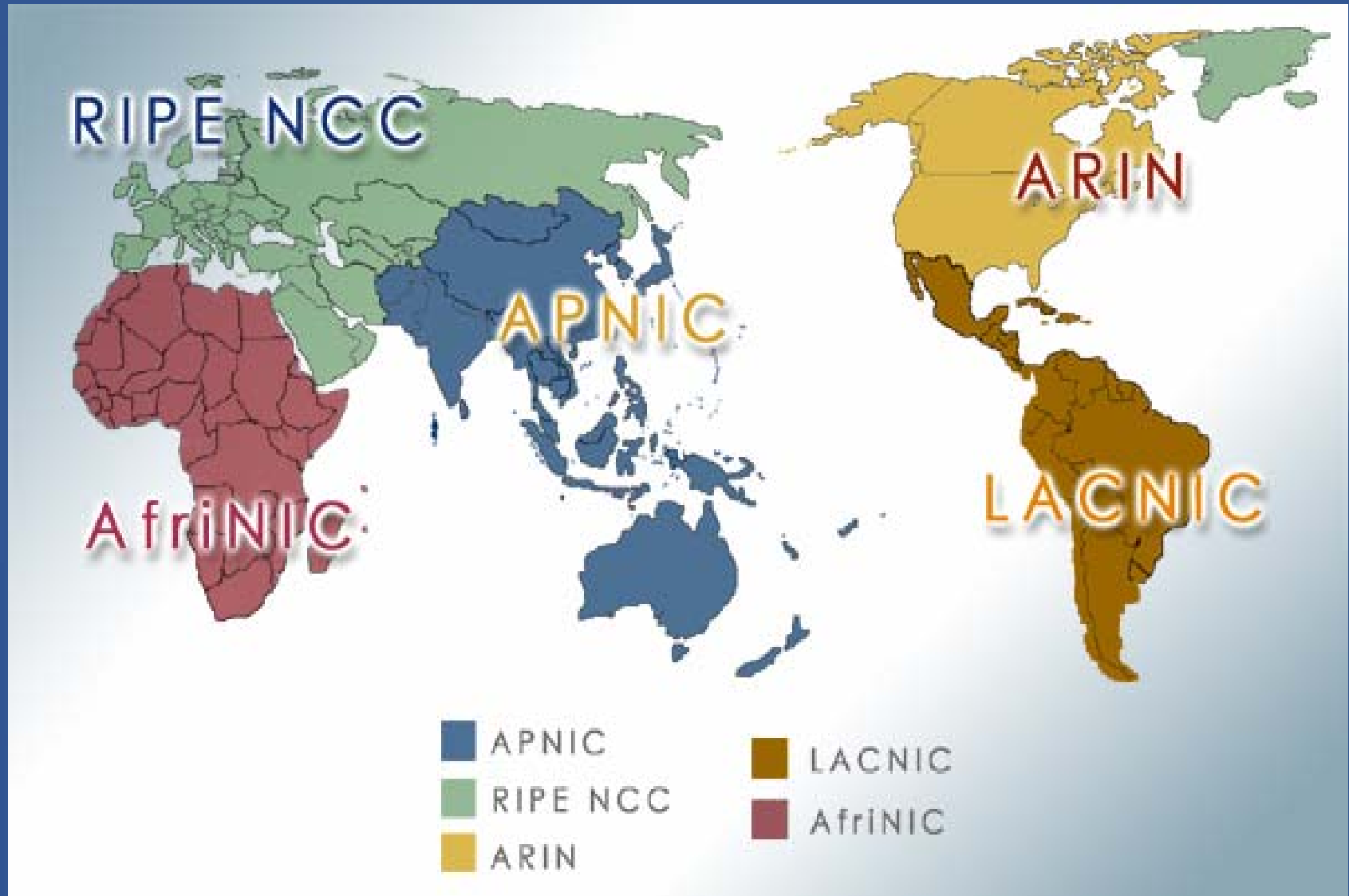
- Not a network operator
 - Does not provide networking services
 - Works closely with APRICOT forum
- Not a standards body
 - Does not develop technical standards
 - Works within IETF in relevant areas (IPv6 etc)
- Not a domain name registry or registrar
 - Will refer queries to relevant parties

APNIC Partners

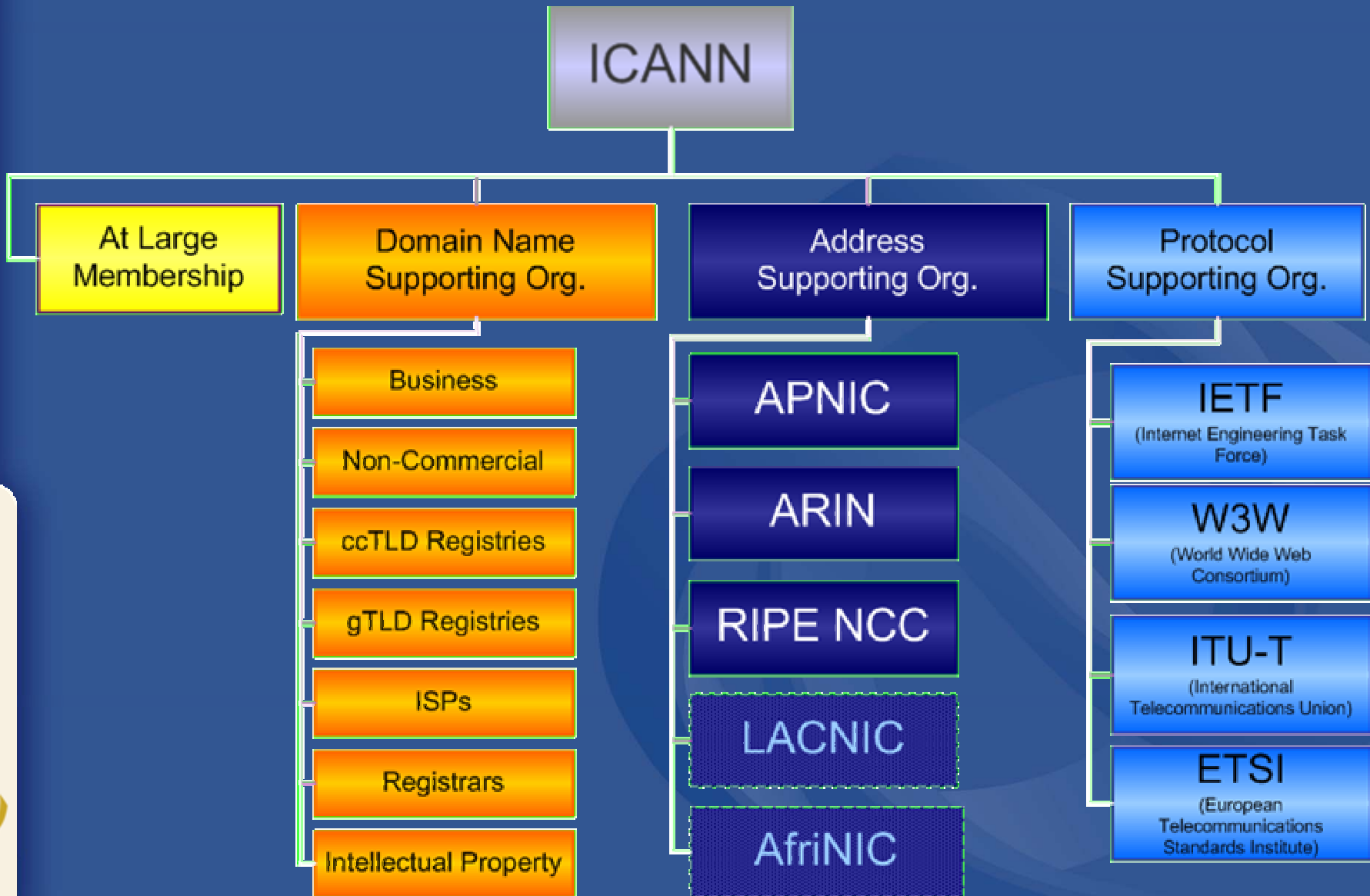
APNIC works closely with

- The APNIC Membership
- Asia Pacific peak bodies in Internet industry, technology, policy and law
 - APNG, APIA, APTLD, APRICOT, PITA
- Other Regional Internet Registries (RIRs)
 - ARIN, RIPE NCC, LACNIC, (AFRINIC)
- Other leading Internet organisations
 - IANA, ICANN, IETF, IEPG, ISOC etc

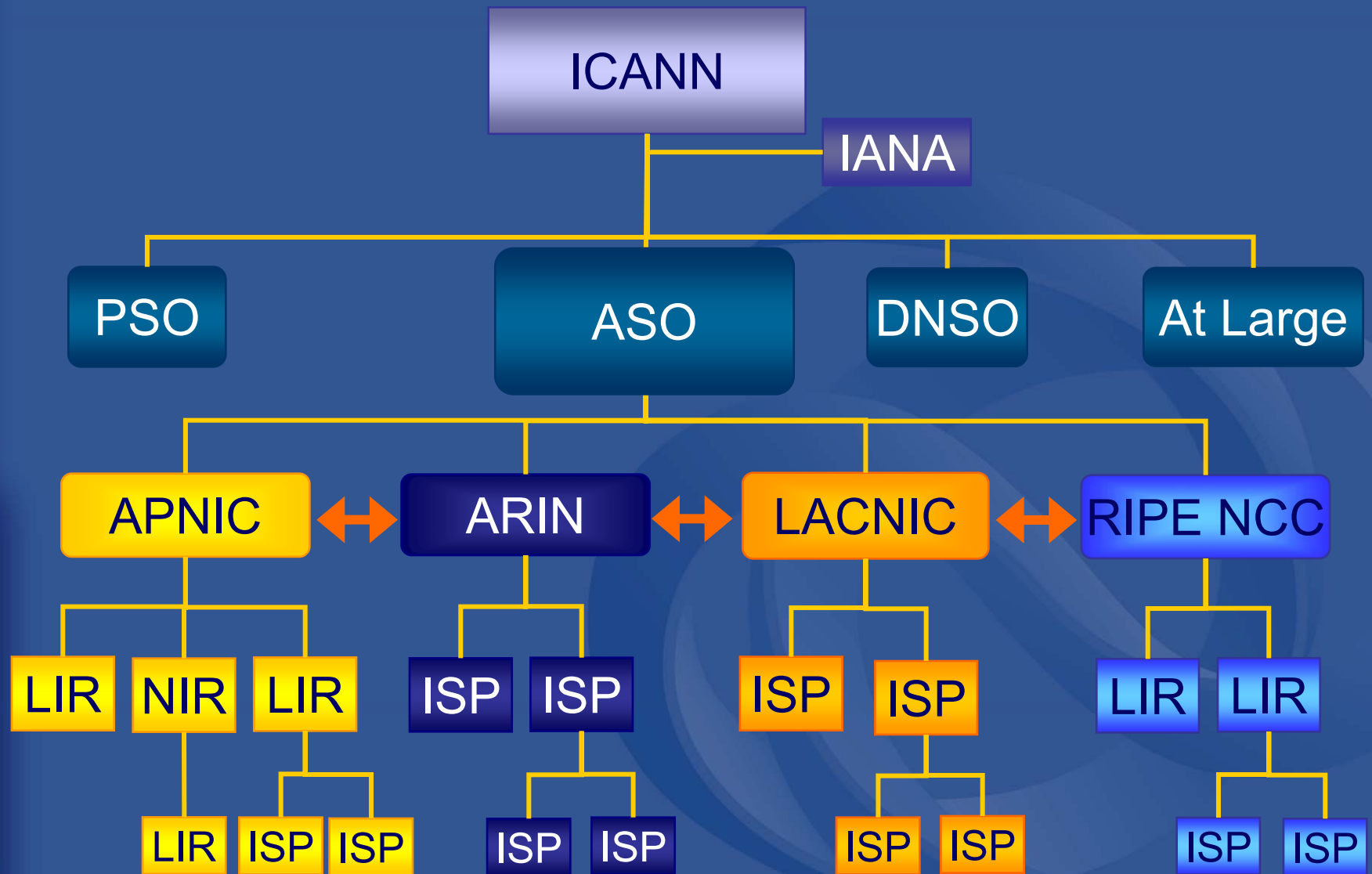
RIR Coverage



Internet Organisation Hierarchy



Internet Registry Structure



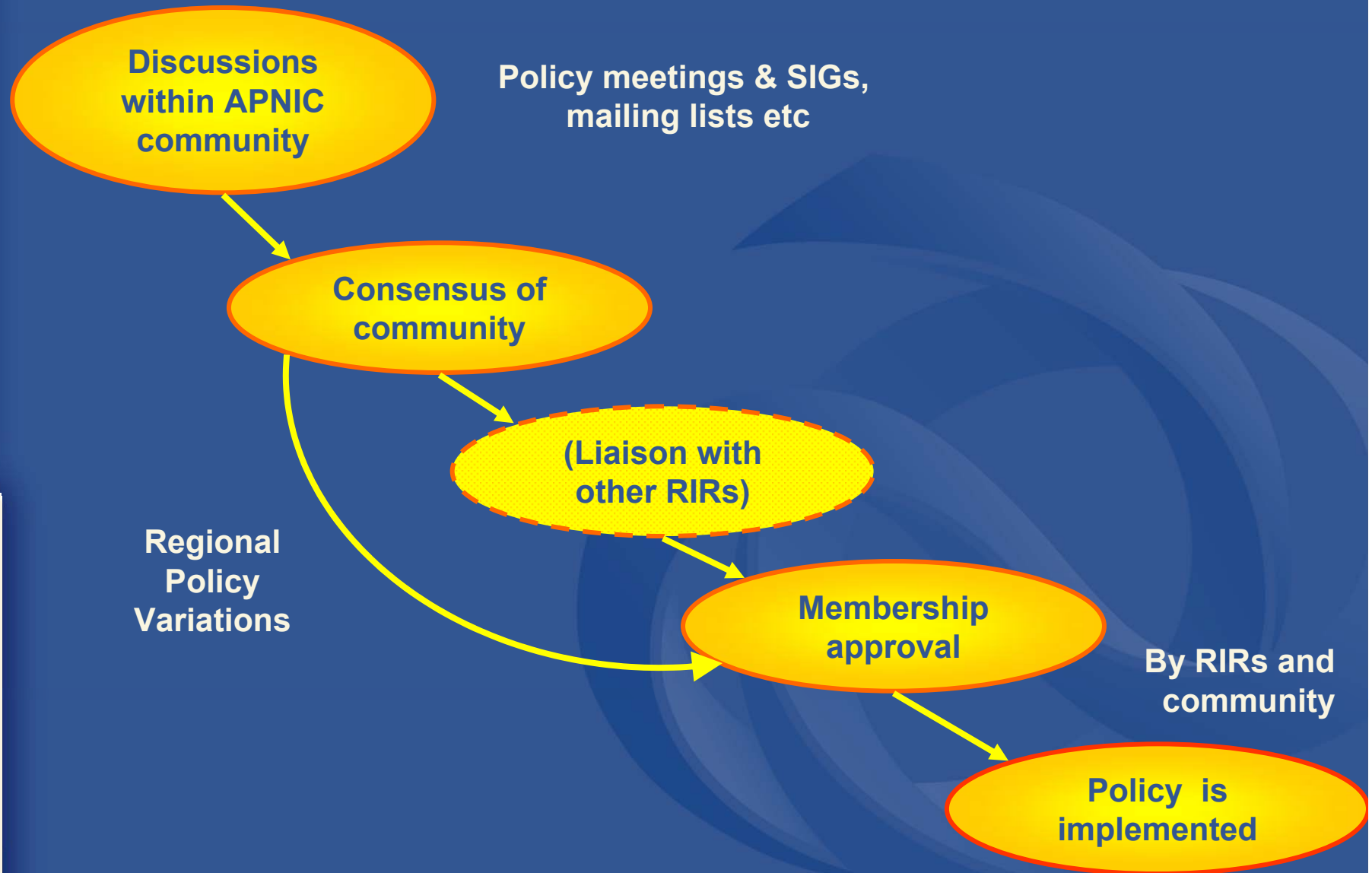
Goals of Address Management

- Conservation
 - Ensuring efficient use and conservation of resources
- Aggregation
 - Limiting growth of routable prefixes
- Uniqueness
 - Global visibility
- Registration
 - Registering the Internet resources in a public database
- Fairness and consistency
 - Equal consideration irrespective of external factors

Careful Address Management is Vital

- APNIC's role
 - “Addressing the challenge of responsible resource distribution in the Asia Pacific”
- ISP's role
 - To manage the resources they have been allocated
 - To develop policies to safeguard future supply which is essential to their business

APNIC Policy Making Process





APNIC

Asia Pacific Network Information Centre

APNIC Whois Database

What is the APNIC Whois Database?

- Public network management database
 - Operated by IRs
- Tracks network resources
 - IP addresses, ASNs, Reverse Domains, Routing policies
- Records administrative information
 - Contact information (persons/roles)
 - Authorisation

Why Use the Database?

- Register use of Internet Resources
 - IP assignments, reverse DNS, etc
 - Ascertain custodianship of a resource
 - Fulfill responsibilities as resource holder
- Obtain details of *technical contacts* for a network
 - Investigate security incidents
 - Track source of network abuse or “spam” email



APNIC

Asia Pacific Network Information Centre

How to Use the APNIC Whois Database

Basic Database Queries

1. Command Line Interface (Unix)

- `whois -h whois.apnic.net <lookup key>`

2. Web interface

- <http://www.apnic.net/apnic-bin/whois2.pl>

Object Types

OBJECT

person

role

inetnum

inet6num

aut-num

as-set

domain

route

mntner

PURPOSE

contact persons

contact groups/roles

IPv4 addresses

IPv6 addresses

Autonomous System number

group of autonomous systems

reverse domains

prefixes being announced

(maintainer) database authorisation

Queries

- Primary and Lookup keys

- Performed as an argument to a query
 - <ip-lookup>
 - <as-number>
 - <as-number> - <as-number>
 - <domain-name>
 - <person-name>
 - <set-name>
 - <nic-handle>
 - <mntner-name>

DB Query – Person Object

```
[xx1@durian]whois -h whois.apnic.net kx17-ap
```

```
% Rights restricted by copyright.
```

```
See http://www.apnic.net/db/dbcopyright.html
```

```
person:      Ky Xander
address:     ExampleNet Service Provider
address:     2 Pandora St Boxville
address:     Wallis and Futuna Islands
country:     WF
phone:       +680-368-0844
fax-no:      +680-367-1797
e-mail:      kxander@example.com
nic-hdl:     KX17-AP
mnt-by:      MAINT-WF-EX
changed:     kxander@example.com 20020731
source:      APNIC
```

DB Query – Maintainer Object

```
[xx1@durian]whois -h whois.apnic.net MAINT-WF-EX
```

```
% Rights restricted by copyright.
```

```
See http://www.apnic.net/db/dbcopyright.html
```

```
mntner:          MAINT-WF-EX
descr:           Maintainer for ExampleNet Service Provider
country:         WF
admin-c:         ZU3-AP
tech-c:          KX17-AP
upd-to:          kxander@example.com
mnt-nfy:         kxander@example.com
auth:            CRYPT-PW apHJ9zF3o
mnt-by:          MAINT-WF-EX
referral-by:     MAINT-APNIC-AP
changed:         kxander@example.com 20020731
source:          APNIC
```

IP Address Queries

- **inetnum, inet6num** store information about ranges of IP addresses
- Default lookup for IP ranges
 - When no flags are specified whois server will try to find an *exact* match for that range
 - `whois -h whois.apnic.net 202.64.0.0`

IP Address Queries

- More and less specific queries
 - ("-M", "-m", "-L" and "-I")
- -I <ip-lookup>
 - Returns first level less specific **inetnum**, **inet6num** excluding exact matches
 - whois -I [customer's IP range]
- -L<ip-lookup>
 - Returns all level less specific **inetnum**, **inet6num** including exact matches.
 - whois -L [IP range]

IP Address Queries

- -m <ip-lookup>
 - Returns first level more specific **inetnum**, **inet6num** excluding exact matches.
 - whois -m [allocation IP range]
- -M<ip-lookup>
 - Returns all level more specific **inetnum**, **inet6num** excluding exact matches.
 - whois -m [allocation IP range]

IP Address Lookups

- `-x<ip-lookup>`
 - Only an exact match on a prefix
 - If no exact match is found, no objects are returned
 - `whois -x [IP range]`
- `-d <ip-lookup>`
 - Enables use of the `"-m"`, `"-M"`, `"-l"` and `"-L"` flags for lookups on reverse delegation domains.

Database Query - inetnum

whois -l 202.64.0.0 /20

*Less specific →
(= bigger block)*

inetnum:
202.0.0.0 – 202.255.255.255

202.0.0.0/8

whois 202.64.0.0 /20

inetnum:
202.64.0.0 – 202.64.15.255

202.64.0.0/20

whois -m 202.64.0.0 /20

*More specific →
(= smaller blocks)*

inetnum:

202.64.10.0/24

inetnum:

202.64.12.128/25

inetnum:

202.64.15.192/26

Database Query - Inetnum

whois -L 202.64.0.0 /20
(all less specific)

inetnum:
202.0.0.0 – 202.255.255.255

202.0.0.0/8

whois -l 202.64.0.0 /20
(1 level less specific)

inetnum:

202.64.0.0/16

whois 202.64.0.0 /20

inetnum:
202.64.0.0/20

whois -m 202.64.0.0 /20
(1 level more specific)

inetnum:
202.64.10.0/24

whois -m 202.64.0.0 /20
(all more specific)

inetnum:

202.64.10.192/26

Inverse Queries

- Inverse queries are performed on inverse keys
 - *See object template (whois -t)*
- Returns all 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

Inverse Queries - Syntax

- whois -i <attribute> <value>
 - -i <admin-c> <nic-handle>
 - -i <person> <person-name>
 - -i <mnt-by> <mntner-name>
 - -i <notify> <e-mail>
 - -i <nserver> <ip-lookup>

Inverse Queries - Examples

- `whois -i tech-c KX17-AP`
 - *all objects with tech-c KX17-AP*
- `whois -i admin-c,tech-c,zone-c -T domain KX17-AP`
 - *all domain objects with admin-c, tech-c or zone-c KX17-AP*
- `whois -ipn KX17-AP`
 - *all objects referencing KX17-AP*
- `whois -i mnt-by MAINT-WF-EX`
 - *All objects maintained by MAINT-WF-EX*
- `whois -i notify kxander@example.com`
 - *All objects with the notify kxander@example.com*



Questions?



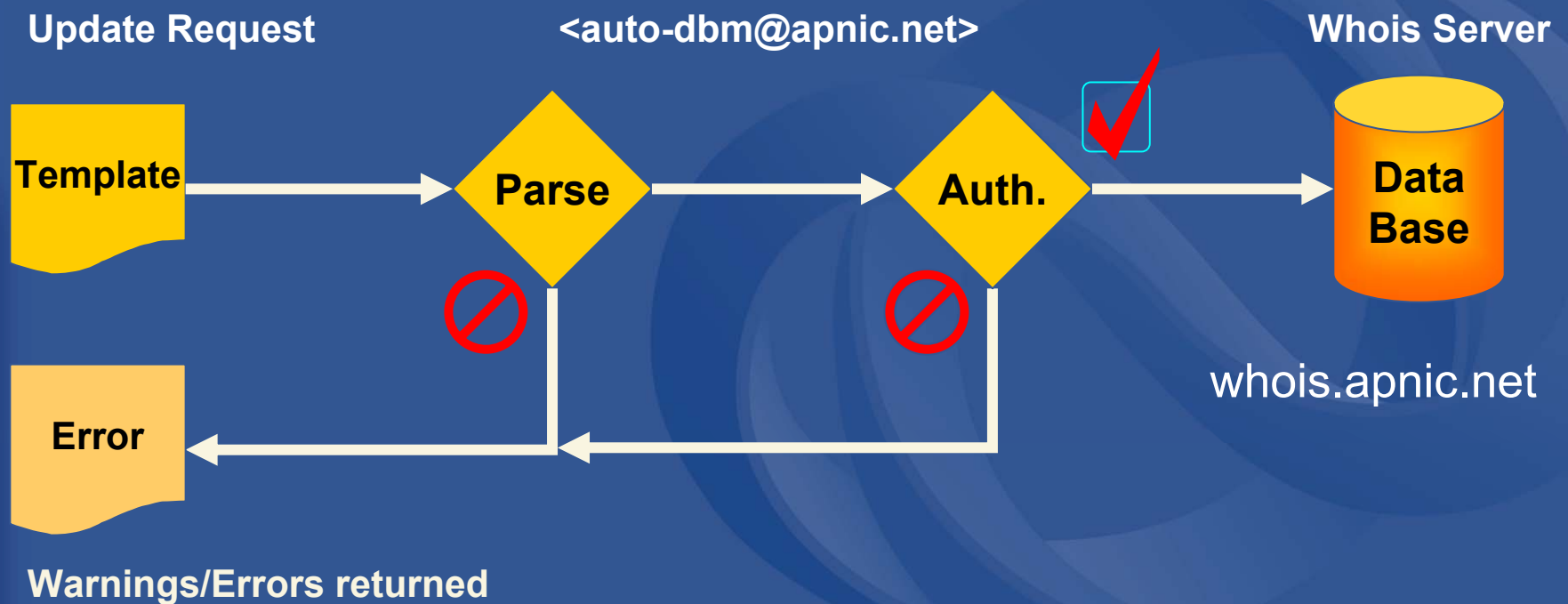
APNIC

Asia Pacific Network Information Centre

Database Updates

Database Update Process

- Email requests to <auto-dbm@apnic.net>
 - Each request contains an *object template*




Updates In the whois Database

- Create, modify or delete
- MIME support
 - text/plain, application/pgp-signature, application/pgp
 - multipart/mixed, multipart/alternative,
 - multipart/signed, message/rfc822
 - each MIME part is treated as a separate submission

Object Processing

– Server Checks

- Verifies that the syntax of an object is correct
- Verifies that the object passes authorisation checks 
- Verifies that all references can be resolved without conflicts

Object Processing

– Server Checks

- Verifies that the operation does not compromise referential integrity
 - the deletion of an object
 - To ensure that it is not referenced from any other object in the database
- Verifies that the requested nic-hdl is not in use and can be allocated
 - Only for the creation of **person** or **role** objects that request a particular NIC handle

RPS Security

- Routing Policy System Security 
 - RFC 2725
- Stronger, hierarchical authorisation and authentication
- Protect your database objects!
 - Request for mntner object

Maintainer Object - Example

```
mntner:          MAINT-WF-EX
descr:           Maintainer for ExampleNet Service Provider
country:         WF
admin-c:         ZU3-AP
tech-c:          KX17-AP
upd-to:          kxander@example.com
mnt-nfy:         kxander@example.com
auth:            CRYPT-PW apHJ9zF3o
mnt-by:          MAINT-WF-EX
referral-by:     MAINT-APNIC-AP
changed:         kxander@example.com 20020731
source:          APNIC
```

- The mntner object provides data protection for other objects

Maintainer Object Attributes

- **upd-to** (mandatory)
 - notification for failed updates
- **mnt-nfy** (optional, **encouraged**)
 - works like notify but for all objects that reference this **mntner**
- **mnt-by** (mandatory)
 - can reference the object itself
- **referral-by** (mandatory)
 - references **mntner** object that created this object

Authentication Methods



- 'auth' attribute
 - <none>
 - **Strongly discouraged!**
 - Email
 - Very weak authentication. Discouraged
 - Crypt-PW
 - Crypt (Unix) password encryption
 - Use web page to create your maintainer
 - PGP – GNUPG
 - Strong authentication (Requires PGP keys)
 - MD5
 - Soon available

mnt-by & mnt-lower

- ‘mnt-by’ attribute
 - Can be used to protect any object
 - Changes to protected object must satisfy authentication rules of ‘mntner’ object.
- ‘mnt-lower’ attribute
 - Also references mntner object
 - Hierarchical authorisation for inetnum, inet6num & domain objects
 - The creation of child objects must satisfy this mntner
 - Protects against unauthorised updates to an allocated range

highly
recommended!

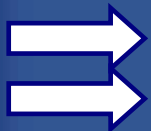
Authentication/Authorisation



– APNIC allocation to member

- Created and maintained by APNIC

```
Inetnum:      203.146.96.0 - 203.146.127.255
netname:      LOXINFO-TH
descr:        Loxley Information Company Ltd.
Descr:        304 Suapah Rd, Promprab, Bangkok
country:      TH
admin-c:      KS32-AP
tech-c:       CT2-AP
mnt-by:       APNIC-HM
mnt-lower:    LOXINFO-IS
changed:      hostmaster@apnic.net 19990714
source:       APNIC
```



Only APNIC can change this object

Authentication/Authorisation



- Member assignment to customer
 - Created and maintained by APNIC member

```
Inetnum:      203.146.113.64 - 203.146.113.127
netname:      SCC-TH
descr:        Sukhothai Commercial College
Country:      TH
admin-c:      SI10-AP
tech-c:       VP5-AP
mnt-by:     LOXINFO-IS
changed:      voraluck@loxinfo.co.th 19990930
source:       APNIC
```



Only LOXINFO-IS can change this object

Common Errors

- Incorrect password

```
Date: Wed, 31 Jul 2002 13:20:00 +1000
From APNIC Whois Management <auto-dbm@apnic.net>
To: kxander@example.com
```

Subject: FAILED: FW: Update MAINT-WF-EX with an Incorrect password

Part of your update FAILED

For help see <<http://www.apnic.net/db/>> or send a message to auto-dbm@apnic.net

With 'help'in the subject line

**Update FAILED: [mntner] MAINT-WF-EX
Authorisation failed, request forwarded to maintainer**

```
mntner:      MAINT-WF-EX
descr:      Maintainer for ExampleNet Service Provider
country:    WF
admin-c:    ZU3-AP
tech-c:     KX17-AP
upd-to:     kxander@example.com
mnt-nfy:    kxander@example.com
auth:       CRYPT-PW apHJ9zF3o
referral-by: MAINT-APNIC-AP
changed:    kxander@example.com 20020731
source:     APNIC
```

Stay in Touch with APNIC

- It is important and easy
 - Email to helpdesk@apnic.net
 - They are there to help you
 - Attend Member Trainings
 - NZ December 9, 2002 and Pacific 2003
 - Collectively send a person to APNIC meetings
 - 2003: APNIC15, 24-28 Feb
<http://www.apnic.net/meetings>
 - With APRICOT <http://www.apricot2003.net>
 - Check the APNIC web pages frequently
 - <http://www.apnic.net>

Questions?

Thank you for listening