APNIC WhoisV3

Database Tutorial

3 September, Kitakyushu, Japan

14th APNIC Open Policy Meeting

Introduction

- Presenters
  - Nurani Nimpuno – Training Development Officer
    - nurani@apnic.net
  - Champika Wijayatunga – Training Manager
    - champika@apnic.net

Overview

- APNIC whois database
- The WhoisV3 database
- RPSL
- Changes with v3
- Querying the database
- Database updates
- APNIC IRR

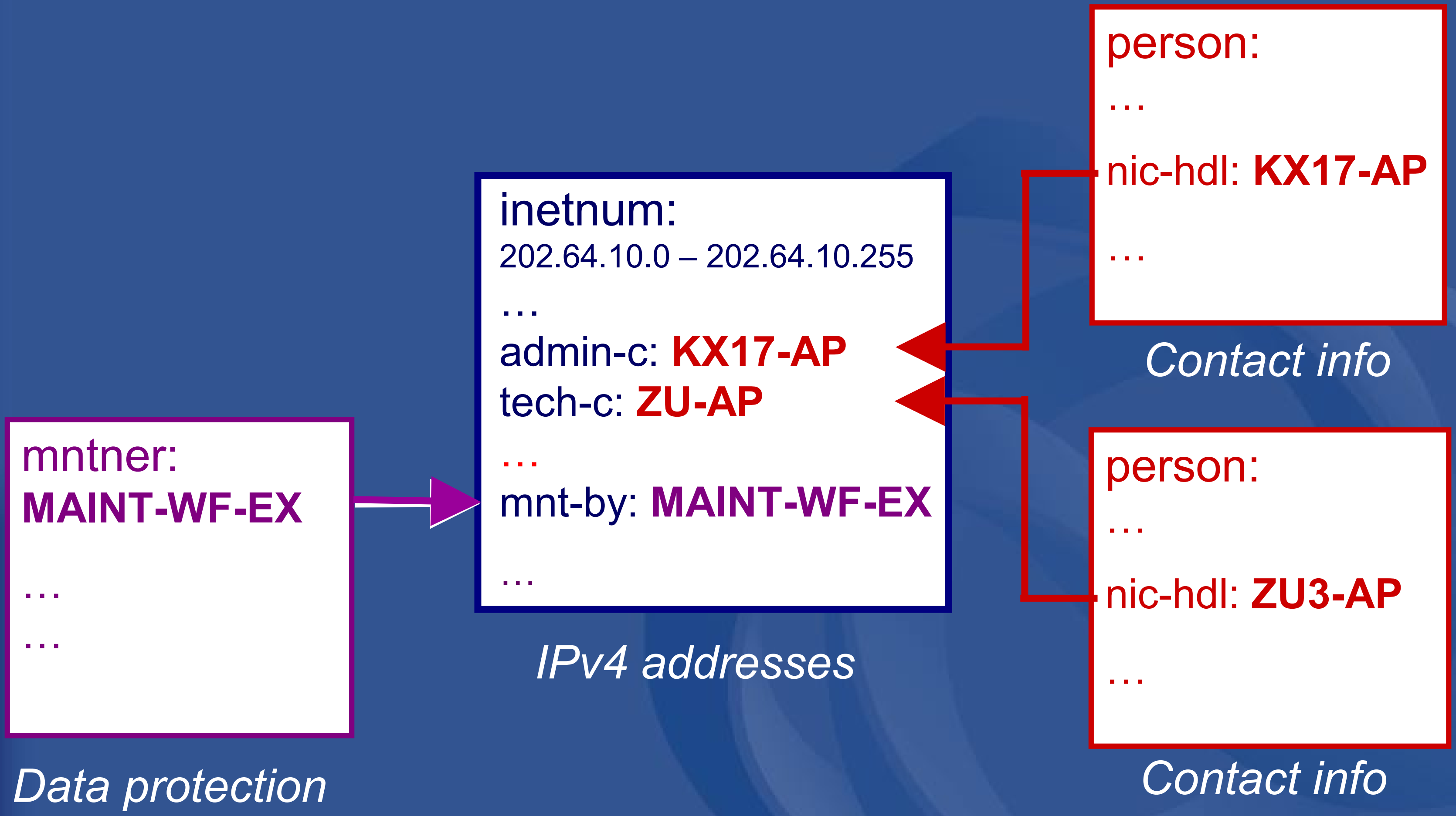
What is the APNIC Database?

- 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

Object Types

OBJECT	PURPOSE
person	contact persons
role	contact groups/roles
inetnum	IPv4 addresses
inet6num	IPv6 addresses
aut-num	Autonomous System number
as-set	group of autonomous systems
domain	reverse domains
route	prefixes being announced
mntner	(maintainer) database authorisation

Maintainers, Inetnum Objects & Person Objects



mntner:
MAINT-WF-EX
…
…

Data protection

inetnum:
202.64.10.0 – 202.64.10.255
…
admin-c: **KX17-AP**
tech-c: **ZU-AP**
…
mnt-by: **MAINT-WF-EX**
…

IPv4 addresses

person:
…
nic-hdl: **KX17-AP**
…

Contact info

person:
…
nic-hdl: **ZU3-AP**
…

Contact info

Why Use the Database?

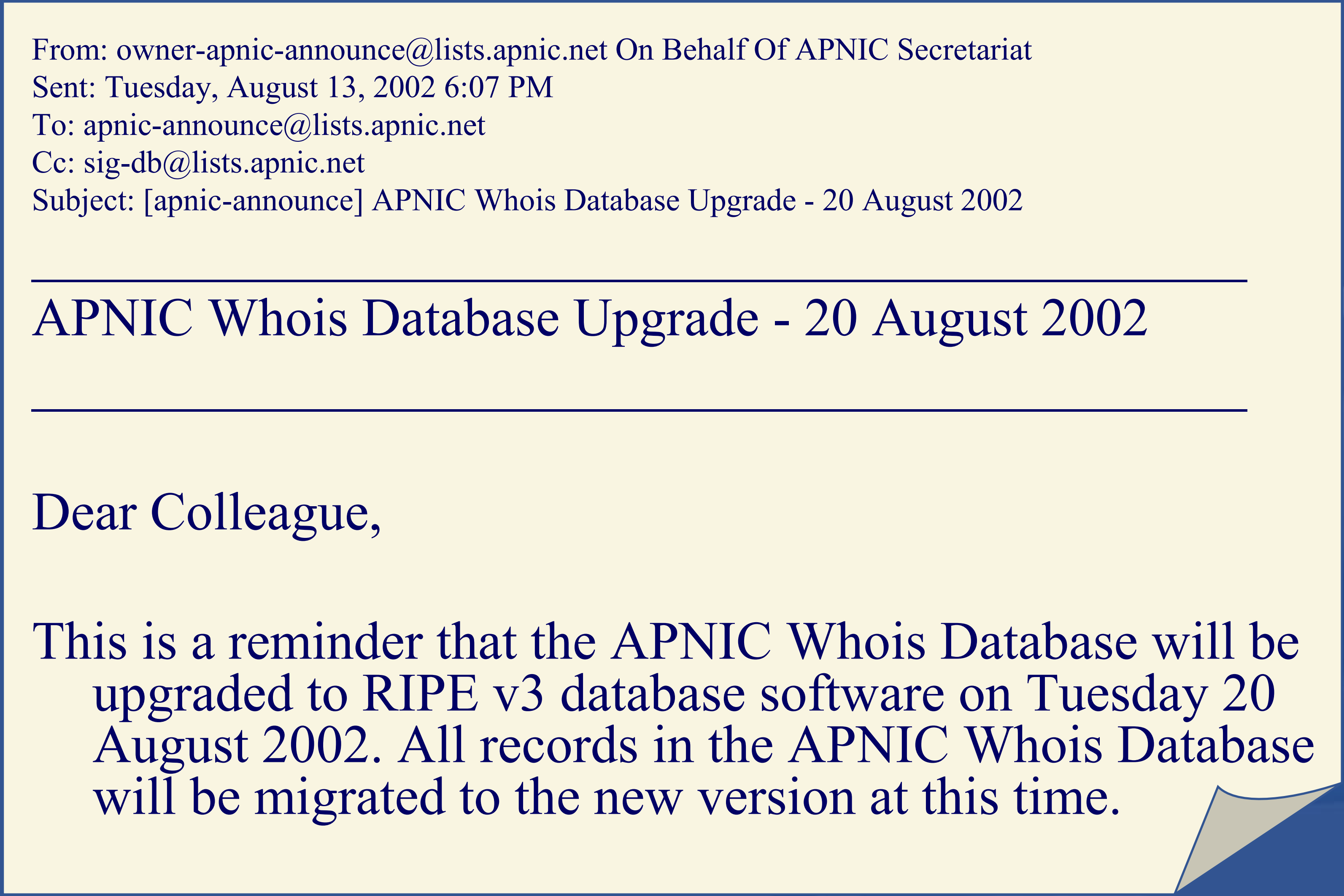
- Register use of Internet Resources
    - IP assignments, reverse DNS, etc
  - Ascertain *custodianship* of a resource
  - *Fulfill responsibilities as resource holder*
- Obtain details of *technical contacts* for a network
    - Investigate security incidents
    - Track source of network abuse or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

Questions?

Introduction to

WhoisV3

Database Upgrade



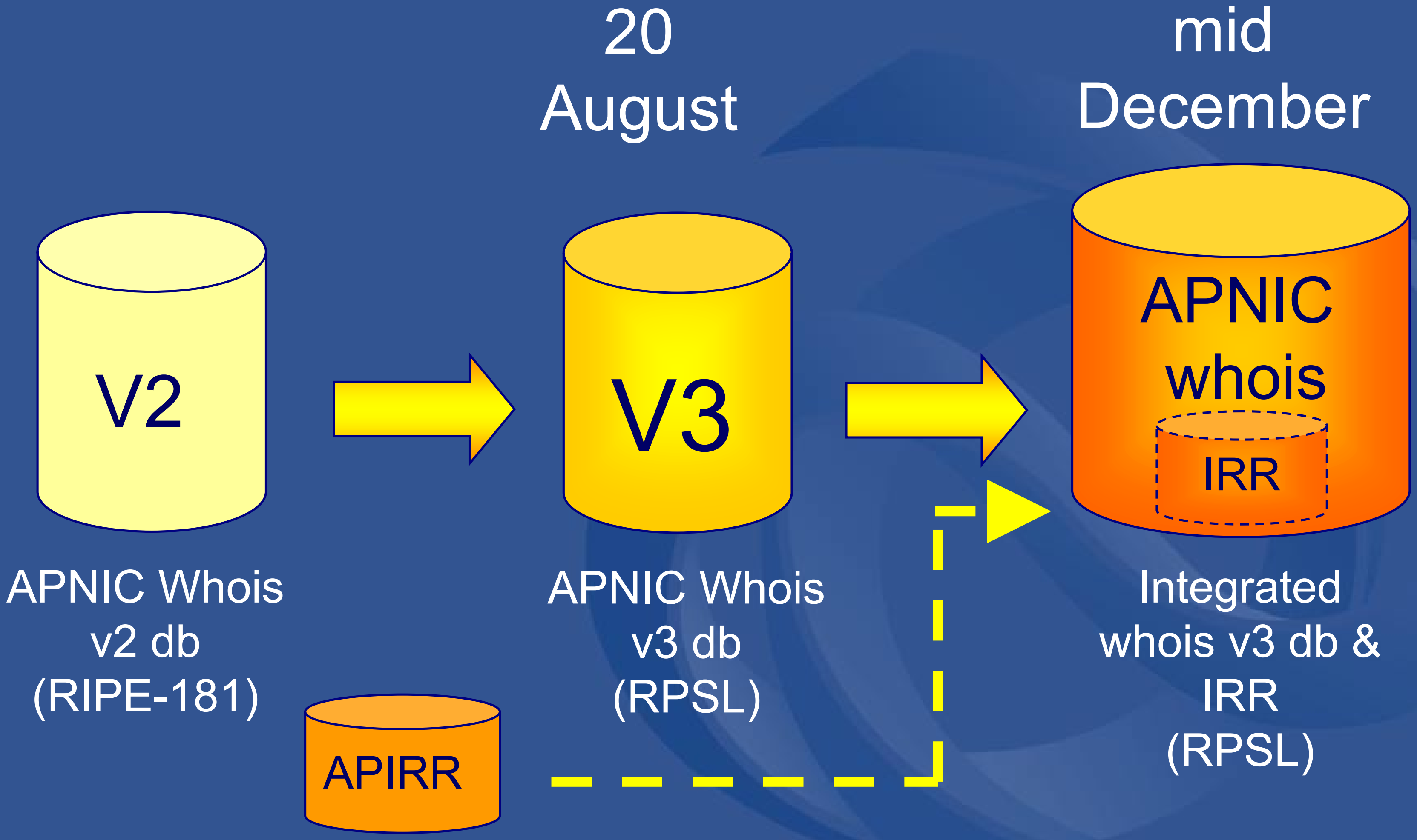
From: owner-apnic-announce@lists.apnic.net On Behalf Of APNIC Secretariat
Sent: Tuesday, August 13, 2002 6:07 PM
To: apnic-announce@lists.apnic.net
Cc: sig-db@lists.apnic.net
Subject: [apnic-announce] APNIC Whois Database Upgrade - 20 August 2002

APNIC Whois Database Upgrade - 20 August 2002

Dear Colleague,

This is a reminder that the APNIC Whois Database will be upgraded to RIPE v3 database software on Tuesday 20 August 2002. All records in the APNIC Whois Database will be migrated to the new version at this time.

Database Upgrade Time Line

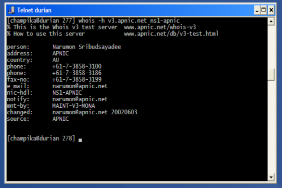


Why WhoisV3 ?

- RPSL compliant database
- Enhanced security and syntax checking
- Better operational platform
  - (response time, enhanced mirroring)
- Richer query options
- Software platform to support one of APNIC's future task as Internet Routing Registry

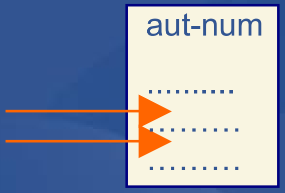
What are the Changes ?

- Command interface
  - More options

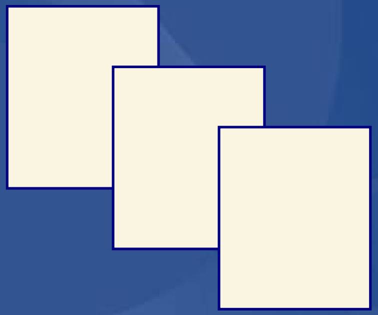


```
[champika@durian 277] whois -h v3.apnic.net ns1-apnic
% This is the Whois v3 test server  www.apnic.net/whois-v3
% How to use this server            www.apnic.net/db/v3-test.html

person:       Narumon Sribudsayadee
address:      APNIC
country:      AU
phone:        +61-7-3858-3100
phone:        +61-7-3858-3186
fax-no:       +61-7-3858-3199
e-mail:       narumon@apnic.net
nic-hdl:      NS1-APNIC
notify:       narumon@apnic.net
mnt-by:       MAINT-V3-MONA
changed:      narumon@apnic.net 20020603
source:       APNIC


[champika@durian 278]
```

- Object attributes



- New Objects
  - Especially related to RPSL



Better Functionality

- Security and Authorisation
  - PGP signed updates possible
- Advanced query options
- Updating procedures
- Mirroring procedures

Facts About the Upgrade

- Full upgrade from v2 to v3 took place 20 August 2002.

- All data successfully converted to RPSL compliant data

- Near-real-time mirrors (NRTM) of Whois data

Questions?

RPSL

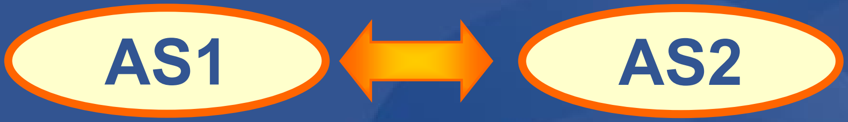
Routing Policy Specification Language

What is RPSL?

- Routing Policy Specification Language
  - Object based language
- Based on RIPE-181
  - Uses type:value notation to represent objects
- IETF Proposed standard
  - RFC 2622

Features of RPSL

- Support the exchange of complex routing policy information between ISPs in a secure and openly agreed manner



  - – ISPs can configure filters for their boarder routers, or check router configurations against routing policies

Why RPSL ?

- More powerful language
  - RPSL is more expressive than RIPE-181
  - Policies can be expressed at the AS level
- Policies can be detailed – router configurations

Objects in RPSL

- Format of RPSL is similar to RIPE-181
- RPSL vs. RIPE-181
  - Line continuation possible
    - Space, tab, +
  - Comments
    - Begin with #
    - Can be anywhere inside an object
    - But cannot start at the beginning of a line (column 0)

Objects in RPSL

- Object ends at blank line (\n\n)
- The order of attributes is flexible

- Empty attributes not allowed
- Empty attributes are not removed

Objects in RPSL

- RPSL vs. RIPE-181
  - No prefix notation for inetnum objects
    - Range notation only accepted
      - Example: `a.b.c.d`<*space*>`-`<*space*>`w.x.y.z`
  - Some attributes are now mandatory
  - *Mnt-by* is *mandatory in all objects* !

Questions?

Changes with WhoisV3

WhoisV3 Database Objects

- RPSL syntax extensions apply to all objects
  - end of line comments, line continuation, order of attributes etc
- New objects
  - as-block, as-set (as-macro), route-set (community)
  - peering-set, filter-set, rtr-set
- New attributes
  - member-of, mbrs-by-ref, mnt-routes, referral-by

Modified Object: Maintainer Object

```
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
```

New in V3!

- **referral-by:** <mntner-name>
  - required in the mntner object
  - refers to the maintainer that created this maintainer

Modified Object: Inetnum Object

range notation

```
inetnum:      169.216.0.0 - 169.216.255.255
netname:      V3TEST-INETNUM
descr:        V3 Test Inetnum Object
descr:        Created by Miwa Fujii at APNIC
country:      AU
admin-c:      NS94-APNIC
tech-c:       NS94-APNIC
status:       ALLOCATED PORTABLE
remarks:      V3 TEST Inetnum Object
notify:       miwa@apnic.net
mnt-by:       APNIC-HM
mnt-lower:    MAINT-AU-V3TEST
changed:      hm-changed@apnic.net 20020704
source:       APNIC
```

***mandatory** in v3!*

Modified Object: Aut-num

```
  aut-num:     as64850
  as-name:     FIRST-AS-MONA
  descr:       a test asn assinged
* import:      from AS10097 accept ANY
  import:      from as9514 accept ANY
  export:      to AS10097 announce AS64850
  export:      to AS9514 announce AS64850
  admin-c:     NS1-APNIC
  tech-c:      NS2-APNIC
  mnt-by:      MAINT-V3-MONA
  changed:     hm-changed@apnic.net 20020613
  source:      APNIC
```

routing policy

* replaces “as-in” and “as-out”

New Object : as-set

- Previously as-macro
  - Defines a set of aut-num objects
    - The "as-set:" attribute defines the name of the set
    - The "members:" attribute lists the members of the set
- Represents list of AS numbers or other as-set names

New Object : as-set

- whois –t as-set

```
as-set:       [mandatory] [single]   [primary/look-up key]
descr:        [mandatory] [multiple]
members:      [optional]  [multiple]
mbrs-by-ref:  [optional]  [multiple]  [inverse key]
remarks:      [mandatory] [multiple]  [inverse key]
admin-c:      [mandatory] [multiple]  [inverse key]
notify:       [optional]  [multiple]  [inverse key]
mnt-by:       [mandatory] [multiple]  [inverse key]
changed:      [mandatory] [multiple]
source:       [mandatory] [single]
```

New in V3!

as-macro in RIPE-181

as-list in RIPE-181

New Object: as-block

New in V3!

- Defines a range of AS numbers delegated to a given repository (RIR or NIR)
- Authorisation of the creation of **aut-num** objects within the range specified by the "as-block:" attribute
- *as-block:* <as-number> - <as-number>
  - Specifies the range of ASNs that the **as-block** object represents

As-block Template

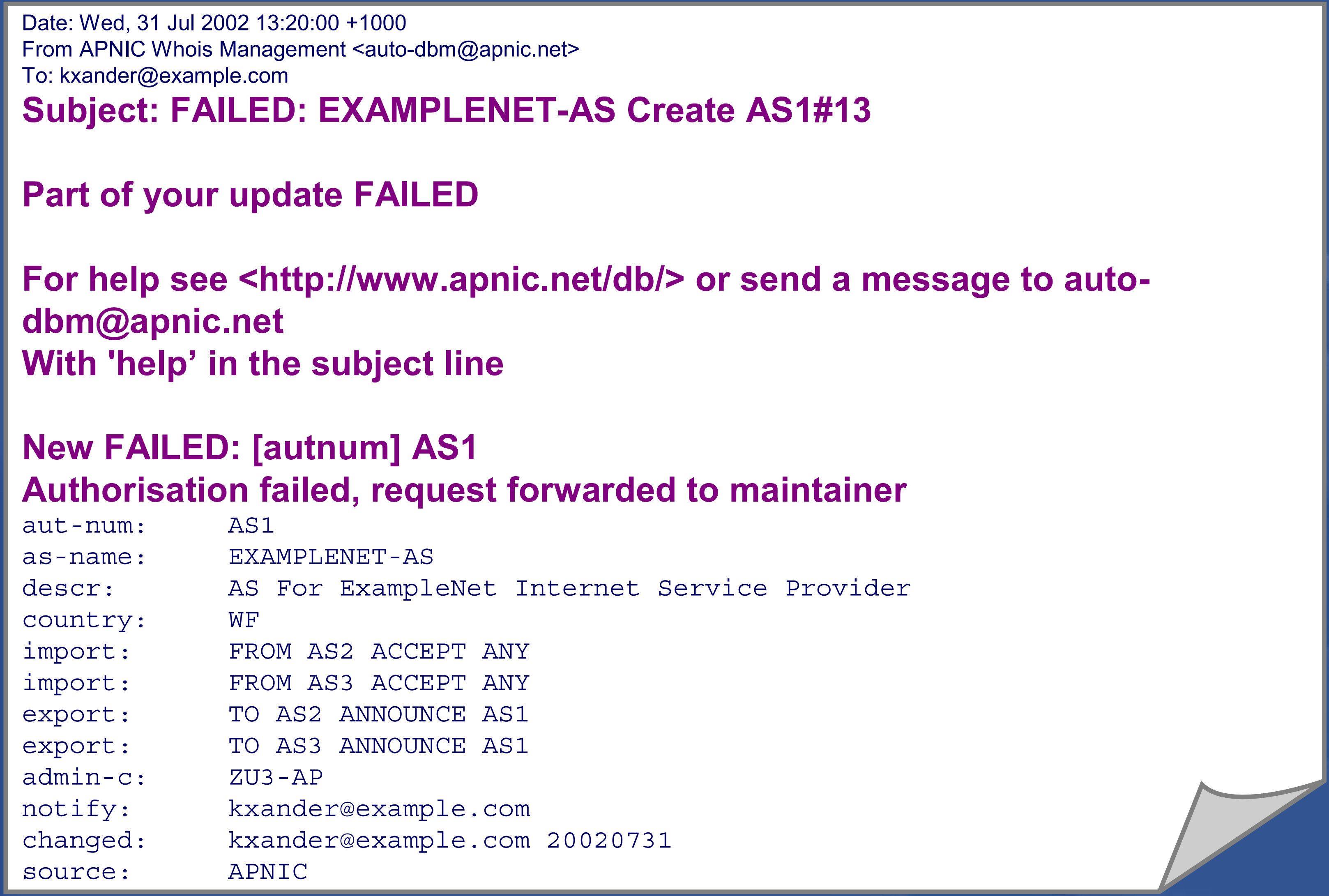
New in V3!

- whois –t as-block

```
as-block:   [mandatory]  [single]    [primary/look-up key]
descr:      [optional]   [multiple]
remarks:    [optional]   [multiple]
tech-c:     [mandatory]  [multiple]  [inverse key]
admin-c:    [mandatory]  [multiple]  [inverse key]
notify:     [optional]   [multiple]  [inverse key]
mnt-lower:  [optional]   [multiple]  [inverse key]
mnt-by:     [mandatory]  [multiple]  [inverse key]
changed:    [mandatory]  [multiple]
source:     [mandatory]  [single]
```

Common Errors – Aut-num object

- Creating an aut-num outside ‘as-block’



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

Subject: FAILED: EXAMPLENET-AS Create AS1#13

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

New FAILED: [autnum] AS1
Authorisation failed, request forwarded to maintainer

```
aut-num:      AS1
as-name:      EXAMPLENET-AS
descr:        AS For ExampleNet Internet Service Provider
country:      WF
import:       FROM AS2 ACCEPT ANY
import:       FROM AS3 ACCEPT ANY
export:       TO AS2 ANNOUNCE AS1
export:       TO AS3 ANNOUNCE AS1
admin-c:      ZU3-AP
notify:       kxander@example.com
changed:      kxander@example.com 20020731
source:       APNIC
```

Questions?

WhoisV3 Database Queries

Asia Pacific Network Information Centre

APNIC

Basic Database Queries

1. Unix
   - whois –h whois.apnic.net <lookup key>
2. Web interface
   - http://www.apnic.net/apnic-bin/whois2.pl

- Look-up keys
  - usually the object name

– Check the object template for look-up keys
  - whois –t <object type>

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>

Database Query - UNIX

```
% whois zulrich@example.com
% whois zu3-ap
% whois “zane ulrich”
```

```
person:       Zane Ulrich
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:       zulrich@example.com
nic-hdl:      ZU3-AP
mnt-by:       MAINT-WF-EXAMPLENET
changed:      zulrich@example.com 20020731
source:       APNIC
```

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-EXAMPLENET
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 "-l")
- -l <ip-lookup>
  - Returns first level less specific **inetnum**, **inet6num** excluding exact matches
    - whois -l [customer’s IP range]
- -L<ip-lookup>
  - Returns all level less specific **inetnum**, **inet6num** including exact matches.

New in V3!

IP Address Queries

- -m <ip-lookup>
  - Returns first level more specific **inetnum**, **inet6num** excluding exact matches.
- -M<ip-lookup>
  - Returns all level more specific **inetnum**, **inet6num** excluding exact matches.

IP Address Lookups

- -x<ip-lookup>

  New in V3!

  - Only an exact match on a prefix
  - If no exact match is found, no objects are returned
  - *whois -x [IP range]*

- -d <ip-lookup>

  New in V3!

  - Enables use of the "-m", "-M", "-l" and "-L" flags for lookups on reverse delegation domains.

Database Query - inetnum

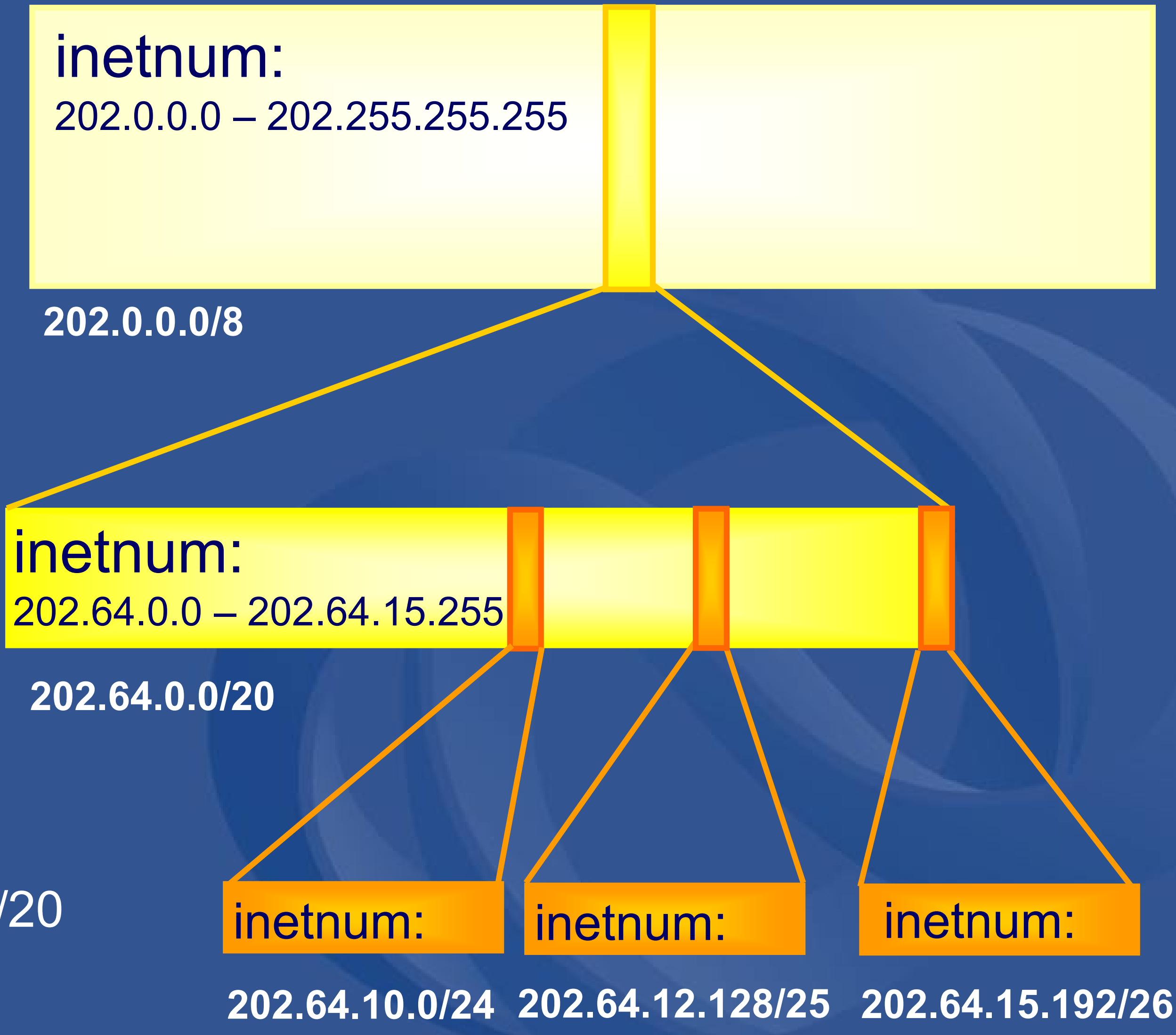
whois -l 202.64.0.0 /20

Less specific →
(= bigger block)

whois 202.64.0.0 /20

whois –m 202.64.0.0 /20

More specific →
(= smaller blocks)



inetnum:
202.0.0.0 – 202.255.255.255

202.0.0.0/8

inetnum:
202.64.0.0 – 202.64.15.255

202.64.0.0/20

inetnum:

202.64.10.0/24

inetnum:

202.64.12.128/25

inetnum:

202.64.15.192/26

Database Query - Inetnum

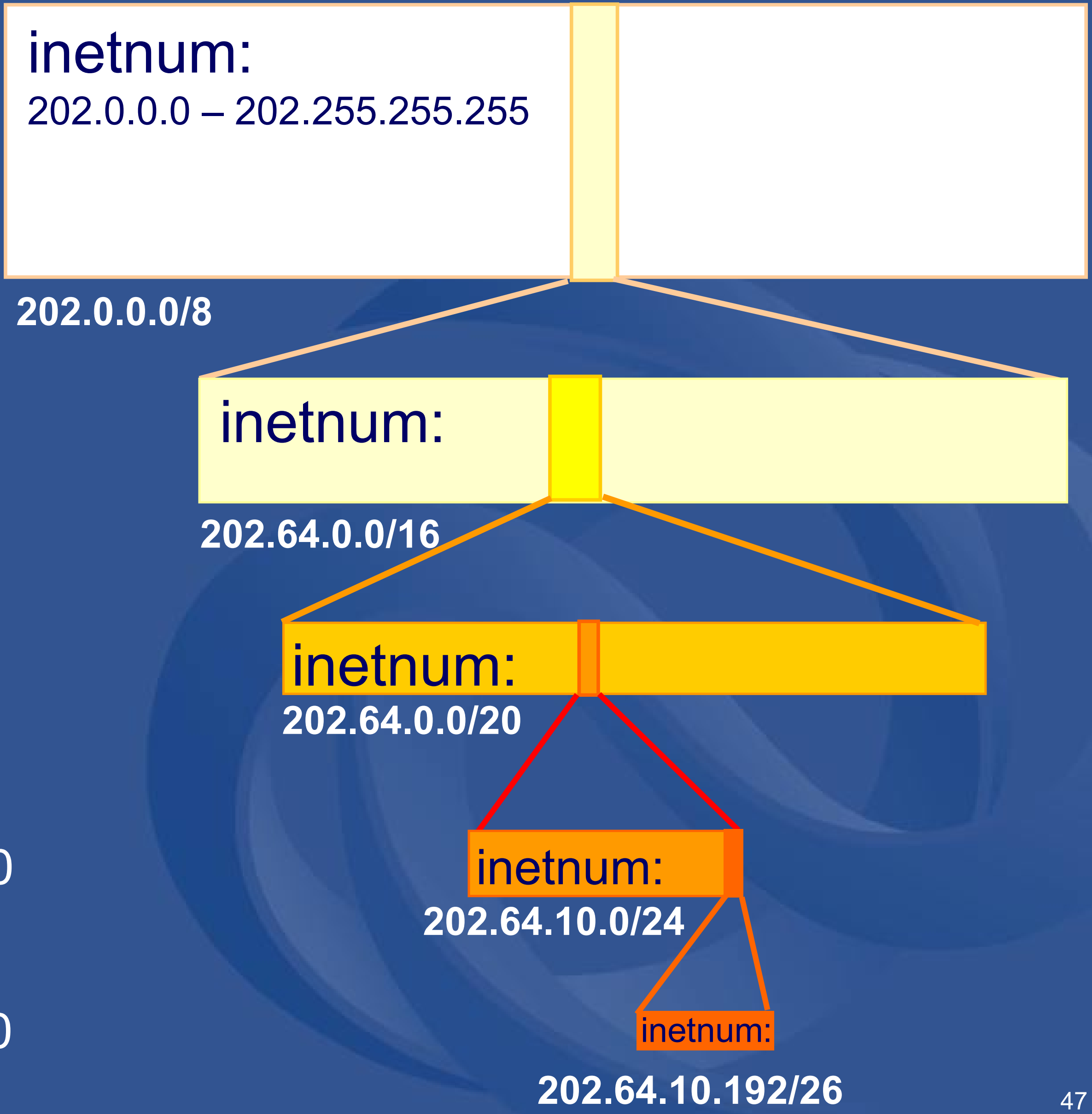
whois -L 202.64.0.0 /20
(all less specific)

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

whois 202.64.0.0 /20

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

whois –m 202.64.0.0 /20
(all more specific)



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*

New in V3!

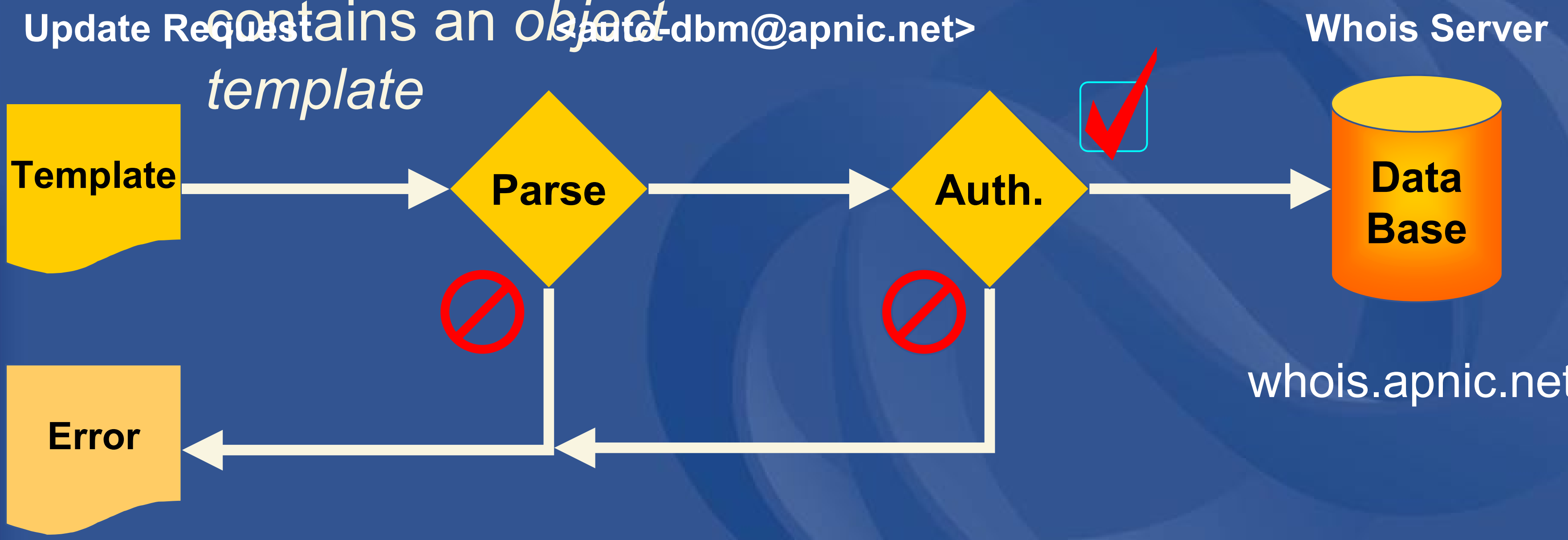
- whois -i admin-c,tech-c,zone-c -T domain KX17-AP
  - *all domain objects with admin-c, tech-c or zone-c KX17-AP*
- whois -ipn KX17-AP
  - *all objects referencing KX17-AP*
- whois -i mnt-by MAINT-WF-EX
  - *All objects maintained by MAINT-WF-EX*
- whois -i notify kxander@example.com
  - *All objects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

Questions?

WhoisV3 Database Updates

Database Update Process

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



Warnings/Errors returned

Updates In the v3 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

New in V3!

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 refererence this **mntner**
- **mnt-by** (mandatory)
  - can reference the object itself
- **referral-by** (mandatory)
  - references **mntner** object that created this object

New in V3!

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

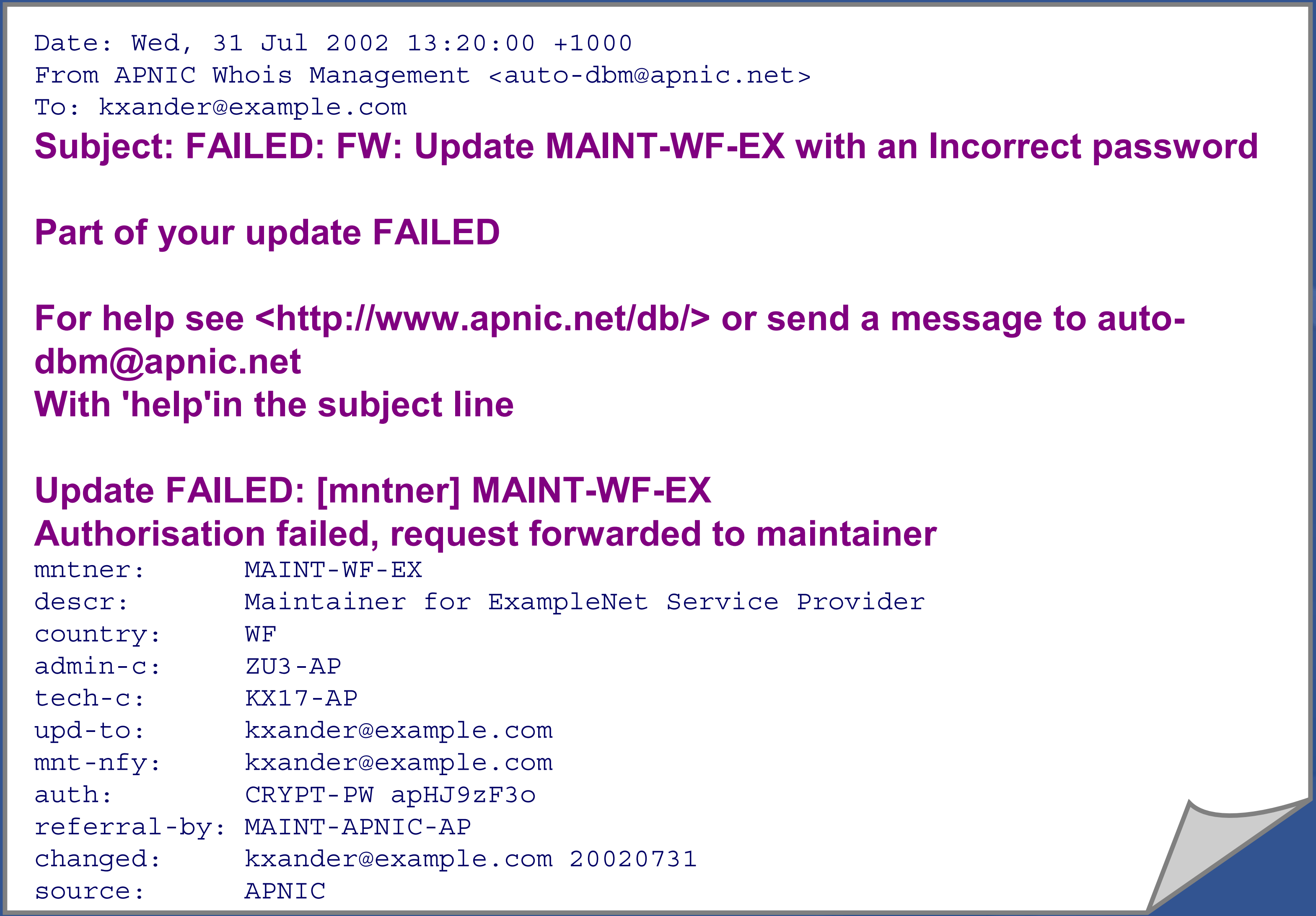
– Member assignment to customer

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
```

Questions?

APNIC Routing Registry

Available mid December 2002

Why a Routing Registry?

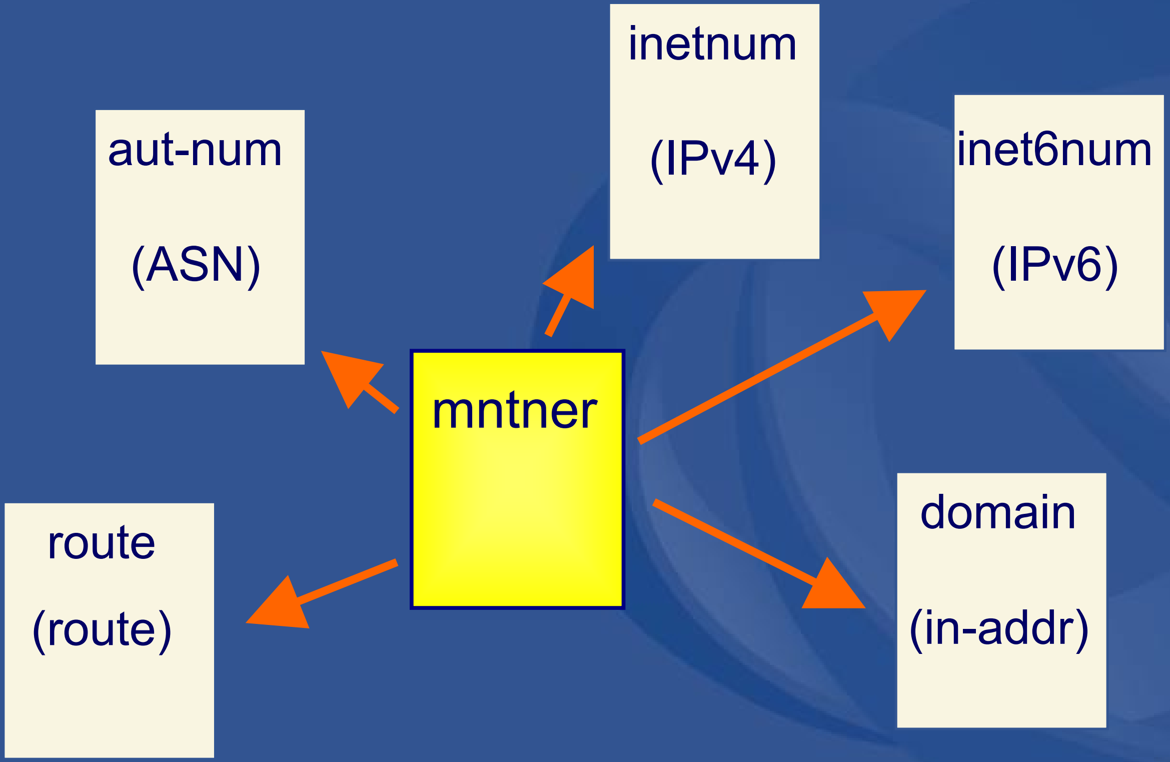
- Filtering routing announcements between
  - – Peering networks
  - – A provider and its customer
- Faster network trouble shooting
- Useful to create router configuration
  - Using tools such as RtConfig
    - – (ftp://ftp.ripe.net/tools/IRRToolSet)
- Long term:
  - Global view of routing policy - Improves integrity of Internet's routing as a whole. ☺

RADB (http://www.radb.net)

- Many ISPs use the RADB
  - to debug routing problems
  - automatically configure backbone routers
  - perform network planning
- Internet operators also use the RADB
  - to generate access lists for both inbound and outbound connections
  - providing defense against bogus routes and unintentional routing leaks

Benefits of APNIC RR

- One maintainer to manage
  - Internet resources (IPv4, IPv6, ASN)
  - reverse DNS (in-addr.arpa, ip6.arpa) and
  - routing information

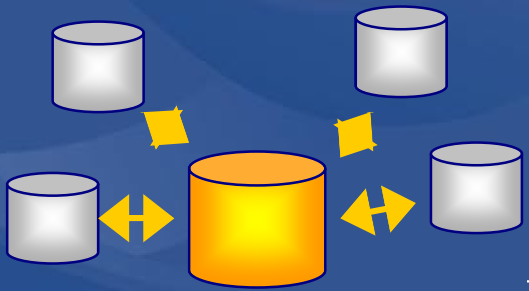


Benefits of APNIC RR (2)

- Data integrity
  - APNIC able to assert resources within a registered route from APNIC resource allocations.
- Free to APNIC members.

Service Scope

- Routing Information Queries
  - From regular whois clients
  - From special purpose programs
    - such as IRRToolSet
  - From APNIC whois web interface
- Support & Maintenance
    - Similar to maintenance of Internet resources
    - Support available through APNIC helpdesk
    - Included in members training
- Mirroring
    - Widespread mirroring



IRR Attributes and Objects

New attributes

- mnt-routes
    - inetnum & aut-num
- member-of
- cross-mnt
- cross-nfy
- mnt-lower

aut-num

IRR Objects

- route
- aut-num
- inet-rtr
- as-set
- route-set
- peering-set
- filter-set
- rtr-set

(Already available in v3 but only useful in IRR)

Availability

- APNIC already maintains routing information currently stored in
  - Whois v3
    - based on RIPE-181 format
  - APIRR
    - pilot IRR service
- APNIC Routing Registry service available mid December 2002

Asia Pacific Network Information Centre

APNIC

Questions?

Thank you