



The whois Database

Introduction and Usage



Overview

- **What is the whois database?**
- **Why use it?**
- **Who uses it?**
- **Database query process**
- **Database update process**



What is the whois Database?

- **Network Management Database**
- **Contains information about**
 - address space
 - DNS domains
 - IP routing policies
 - contact information



Why use the Database?

- **Queries**
 - Ascertain custodianship of a resource
 - Obtain details of technical contacts for a network
 - Investigate security incidents
 - Track source of network abuse or “spam” email
- **Updates**
 - Register use of Internet resources
 - IP networks, ASNs, reverse DNS, etc.
 - Update existing records
 - *Fulfill responsibilities as resource holder*



Who uses the Database?

- **Queries**
 - Internet Service Providers
 - Site network managers and engineers
 - Any Internet user
- **Updates**
 - Internet registries (RIRs, LIRs)
 - Internet Service Providers
 - Anyone who holds an Internet resource



Database Objects

- Database object types

<u>OBJECT</u>	<u>PURPOSE</u>
person	contact persons
role	contact groups/roles
inetnum	IPv4 address allocations/assignments
inet6num	IPv6 address allocations/assignments
aut-num	autonomous system number
as-macro	group of autonomous systems
domain	reverse domains
route	prefixes being announced
mntner	(maintainer) database authorisation



Contact Information

Example object - 'person'

Attributes

Values

person:	Brajesh Jain
address:	B 115 SARVODAYA ENCLAVE
address:	NEW DELHI 110017
country:	TH
phone:	+91-11-6864138
fax-no:	+91-11-6865888
e-mail:	bcjain@ndb.vsnl.net.in
nic-hdl:	BJ16-AP
mnt-by:	MAINT-IN-ESTEL-BCJ
changed:	bcjain@ndb.vsnl.net.in 20000429
source:	APNIC



Network Information

Example object - 'inetnum'

Attributes	Values
inetnum:	203.113.0.0 - 203.113.31.255
netname:	TOTNET-AP
descr:	Telephone Organization of THAILAND(TOT)
descr:	Telephone and IP Network Service Provider
country:	TH
admin-c:	NM18-AP
tech-c:	RC80-AP
mnt-by:	APNIC-HM
mnt-lower:	MAINT-TH-SS163-AP
changed:	hostmaster@apnic.net 19990922
source:	APNIC



Database Query - Search Keys

OBJECT TYPE ATTRIBUTES - SEARCH KEYS

```
person
role
mntner
inetnum
domain
aut-num
as-macro
route
inet6num
```

```
name, nic-hdl, e-mail
name, nic-hdl, e-mail
maintainer name
network number, name
domain name
as number
as-macro name
route value
network number, name
```

* **whois supports queries on any of these objects/keys**



Database Query - Inetnum

```
% whois 203.127.128.0 - 203.127.159.255
% whois 202.127.128.0/19
% whois SINGNET-SG
```

```
inetnum:      203.127.128.0 - 203.127.159.255
netname:      SINGNET-SG
descr:        Singapore Telecommunications Ltd
descr:        31, Exeter Road, #02-00, Podium Block
descr:        Comcentre, 0923
country:      SG
admin-c:      CWL3-AP
tech-c:       CWL3-AP
mnt-by:       APNIC-HM
changed:      hostmaster@apnic.net 19990803
source:       APNIC
```

Notes

- Incomplete addresses padded with “.0”
- Address without prefix interpreted as “/32”



Database Query - Inetnum

- **RIPE extended whois client**

<ftp://ftp.ripe.net/ripe/dbase/software/ripe-dbase-3.0.tar.gz>

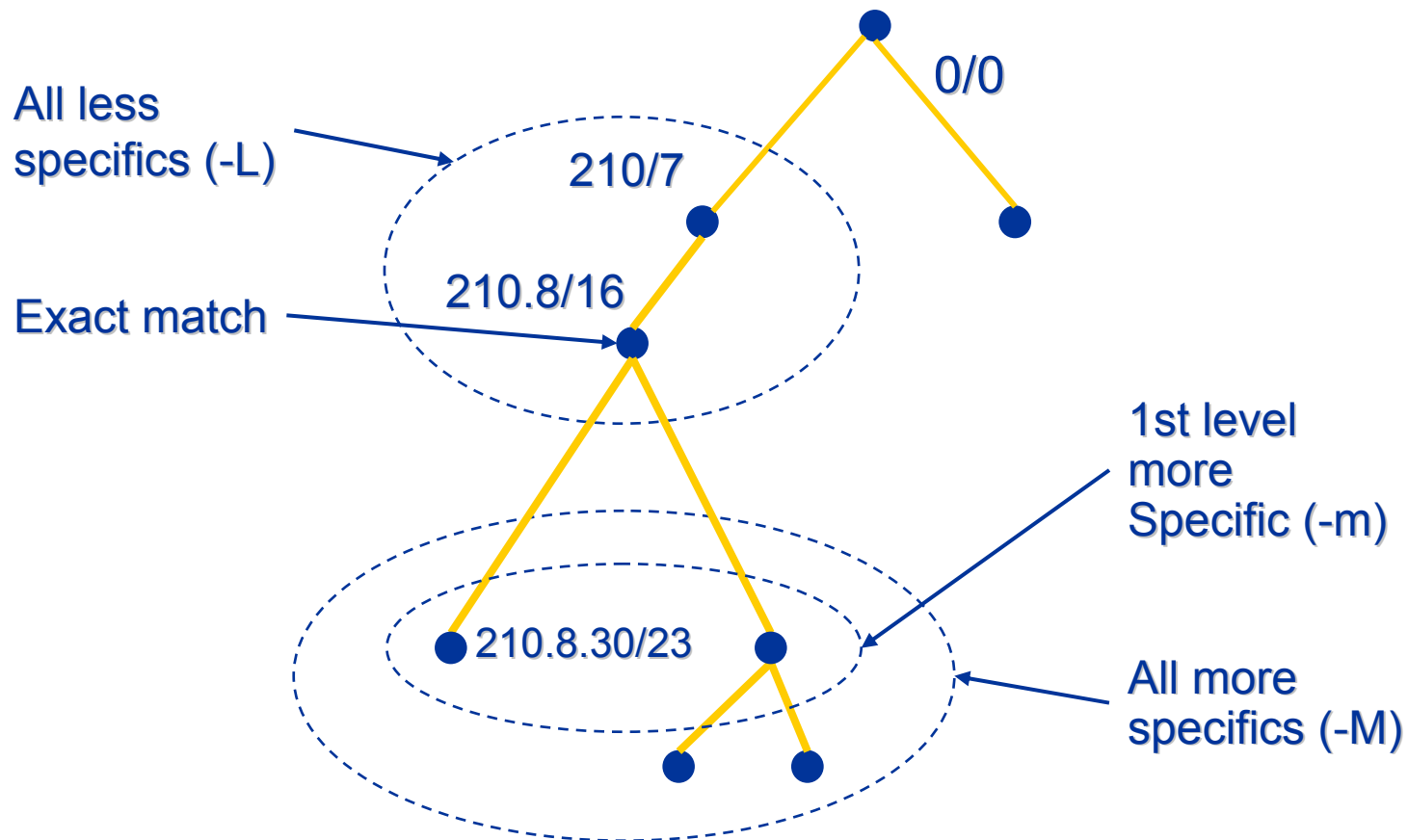
- **Flags used for *inetnum* queries**

None	find exact match
- L	find all <i>less</i> specific matches
- m	find first level <i>more</i> specific matches
- M	find all <i>More</i> specific matches
- r	turn off <i>recursive</i> lookups



Database Query - Inetnum

inetnum hierarchy: `whois 210.8.0.0/16`





Database Query - Inetnum

'-M' will find all assignments in a range in the database

```
% whois -M 202.144.0.0/19
```

```
inetnum:      202.144.0.0 - 202.144.31.255
netname:      SILNET-AP
descr:        Satyam Infoway Pvt.Ltd.,
.....
inetnum:      202.144.13.104 - 202.144.13.111
netname:      SOFTCOMNET
descr:        SOFTCOM LAN (Internet) IP.
.....
inetnum:      202.144.1.0 - 202.144.1.255
descr:        SILNET
descr:        Satyam Infoway's Chennai LAN
.....
```



Database Query - Inverse

```
% whois -i person EC119-AP
```

```
inetnum:      202.166.224.0 - 202.166.255.255
netname:      NECTW-BIGLOBE
descr:        ISP Division of NEC Taiwan Ltd.
country:      TW
admin-c:      SC23-AP
tech-c:       EC119-AP
.....

aut-num:      AS9283
as-name:      NECTW-AS
descr:        ISP Division of NEC Taiwan Ltd.
tech-c:       EC119-AP

mntner:       NECTW-ISP-AP
descr:        NEC Biglobe Taiwan wide
admin-c:      SC23-AP
tech-c:       EC119-AP

person:       Emily Hui Chou
address:      ISP Division of NEC Taiwan Ltd.
country:      TW
phone:        +886-2-85001787
e-mail:       tech@biglobe.net.tw
nic-hdl:      EC119-AP
```



Whois Web Interface

Search the APNIC Whois database

Search for:

Advanced Whois search options [Brief descriptions below](#)

-L Type of object:

-S Source database:

-i Inverse lookup:

-F Fast raw output

-r No recursive lookup

-S No 'syntactic sugar'

-R APNIC objects only

Level of specificity:

-L Less specific

-m 1st level more specific

-M All more specific

[\[About the database\]](#)

Common whois options

Option	Brief description
-F	Gives a faster result, but with attributes in short form.
-i	Provides reverse/inverse lookups of objects associated with the specified attribute.
-L	Finds all less specific matches.
-m	Finds first level more specific matches.



Whois Web Interface

Whois Advanced Query - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Refresh Home Search Favorites History Mail Print Edit Discuss Real.com

Address http://www.apnic.net/apnic-bin/whois2.pl?key=OA3-AP&results=a&type=all&source=&no_recursive=1&inv= Go Links >>

Asia Pacific Network Information Centre

[Services](#) | [Membership](#) | [Information](#) | [Documents](#) | [Training](#) | [Contact](#) | [Search](#)

Search the APNIC Whois database

Search results for 'OA3-AP'

role	OPTUS IP ADMINISTRATORS , inverse
address	101 Miller Street North Sydney
phone	+61-2-93427681
phone	+61-2-93420848
phone	+61-2-93420983
phone	+61-2-93420813
fax-no	+61-2-9342-0998
fax-no	+61-2-9342-6122
e-mail	noc@optus.net.au , inverse
admin-c	NCB-AP , inverse
tech-c	NCB-AP , inverse
tech-c	SC120-AP , inverse
tech-c	DB30-AP , inverse
tech-c	CB39-AP , inverse
tech-c	EH19-AP , inverse
nic-hdl	OA3-AP , inverse
mnt-by	MAINT-OPTUSCOM-AP , inverse
changed	chr is@optus.net.au 20000407
source	APNIC

Search for: Search Whois Show first result only ▾

Advanced Whois search options [Brief descriptions below](#)

-T ? Type of object: -F ? Fast raw output Level of specificity: ▾

Internet



Database Query - Options

- **Summary of other flags**

- i *inverse* lookup on given attribute
- T search only for objects of given type
- t give template for given type
- v *verbose* information for given type
- h specify database server site

- **For more information try...**

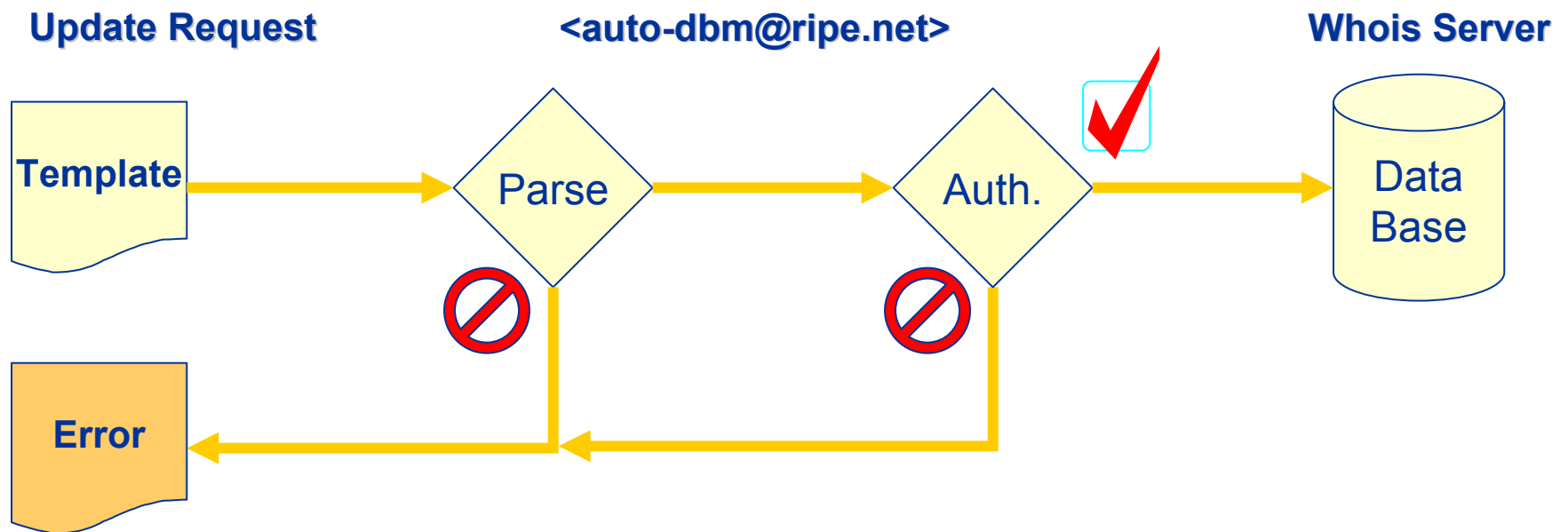
```
whois -h whois.apnic.net HELP
```

```
whois -h whois.ripe.net HELP
```



Database Update Process

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



Warnings/Errors returned



Database Update Process

- **Update transactions**

- Create a new object
- Change attributes of an object
- *Delete* an object

A yellow callout box with a black border and a wavy bottom edge, containing the word "Template" in black text.

Template

- **Updates are submitted by email**

- E-mail to: <auto-dbm@ripe.net>

- **Email message contains template with new or updated object**



Object Template

`whois -t <object type>`

- Recognised by the RIPE whois client/server

```
% whois -h whois.ripe.net -t person
```

```
person: [mandatory] [single] [primary/look-up key]
address: [mandatory] [multiple] [ ]
country: [optional] [single] [ ]
phone: [mandatory] [multiple] [ ]
fax-no: [optional] [multiple] [ ]
e-mail: [optional] [multiple] [look-up key]
nic-hdl: [mandatory] [single] [primary/look-up key]
remarks: [optional] [multiple] [ ]
notify: [optional] [multiple] [inverse key]
mnt-by: [optional] [multiple] [inverse key]
changed: [mandatory] [multiple] [ ]
source: [mandatory] [single] [ ]
```



Database Update Process

- **Automatic request processing**

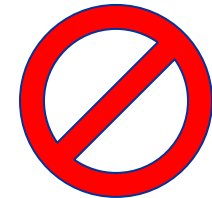
`<auto-dbm@ripe.net>`

- Automatic “robot” for all database updates
- Email template for create/update/delete



- **Templates are syntax checked**

- Warnings
- Errors



- **Database service support**

`<ripe-dbm@ripe.net>`

Data Protection

- **Authorisation**

- “mnt-by” attribute references a “mntner” (maintainer) object
- “mnt-by” should be used with every object



- **Authentication**

- Updates to an object must pass authentication rule specified by its maintainer object

Data Protection

- **Failed Authorisation**

- Template NOT corrected and object NOT accepted
- Automatic email notification sent to requestor
- Automatic email notification sent to “notify” address



- **Successful update**

- If Parse and Auth. steps succeed, database is updated
- Confirmation by email to requestor






Authentication/Authorisation

– Maintainer object example

```
inetnum:      193.1.2.0/24
descr:        SYNFLUX-NET
mnt-by:       MAINT-AU-SYNFLUX
```



```
mntner:       MAINT-AU-SYNFLUX
descr:        Synflux International Pty.
country:      AU
admin-c:      UG1-AP
tech-c:       UG1-AP
upd-to:       umar@synflux.com.au
mnt-nfy:      umar@synflux.com.au
auth:       CRYPT-PW apnbVcktyz6UY
mnt-by:     MAINT-AU-SYNFLUX
changed:      umar@synflux.com.au 19990404
```




Authentication/Authorisation

- **Maintainer specific attributes**
 - notify:
 - Sends notification of any changes to maintained objects to email address specified
 - mnt-by:
 - Maintainers must also be protected!
(Normally by themselves)
 - auth:
 - Authentication method for this maintainer



Authentication/Authorisation

- **‘auth’ attribute gives authentication method**
 - NONE
 - **Strongly discouraged!**
 - MAIL-FROM
 - Very weak authentication. Discouraged
 - CRYPT-PW
 - Crypt (Unix) password encryption
 - Use web page to create your maintainer
 - PGP-KEY



Questions

