



RNEP-GW

MÓDULO WHOIS



WHOIS

WHOIS é o protocolo usado para determinar a quem pertence um determinado recurso

Modelo Cliente/Servidor, Software variado

Os Regional Internet Registries (RIR) - AFRINIC, APNIC, ARIN, LACNIC, RIPENCC - são a fonte autoritativa para os blocos/endereços IP. 5 fontes autoritativas, com campos diferentes



PROTOCOLO WHOIS: OBJECTOS

inetnum

inet6num

route

route6

aut-num

domain

organisation

role

person

CAMPOS MANDATÓRIOS E OPCIONAIS

```
# whois -h whois.ripe.net -t person
person:      [mandatory] [single]  [lookup key]
address:     [mandatory] [multiple] []
phone:       [mandatory] [multiple] []
fax-no:      [optional]  [multiple] []
e-mail:      [optional]  [multiple] [lookup key]
org:         [optional]  [multiple] [inverse key]
nic-hdl:     [mandatory] [single]  [primary/lookup key]
remarks:     [optional]  [multiple] []
notify:      [optional]  [multiple] [inverse key]
mnt-by:      [mandatory] [multiple] [inverse key]
created:     [generated] [single]  []
last-modified: [generated] [single] []
source:      [mandatory] [single]  []
```

QUERIES INVERSAS

```
whois -h whois.ripe.net -i mnt-by AS1930-MNT -T aut-num |grep aut-num
```

```
aut-num:      AS12833
```

```
aut-num:      AS1930
```

```
aut-num:      AS204466
```

```
whois -h whois.ripe.net -i tech-c CMF8-RIPE -T inet6num |grep inet6num
```

```
inet6num:     2001:7f8:a::/48
```

```
whois -h whois.ripe.net -i origin AS35822 -T route |grep route
```

```
route:        193.47.185.0/24
```

```
whois -h whois.ripe.net -i origin AS47784 -T route |grep route
```

```
route:        185.32.36.0/22
```

```
route:        192.112.45.0/24
```

```
route:        194.110.76.0/24
```

WHOIS

```
#
# ARIN WHOIS data and services are subject to the Terms of Use
# available at: https://www.arin.net/resources/registry/whois/tou/
#
# If you see inaccuracies in the results, please report at
# https://www.arin.net/resources/registry/whois/inaccuracy_reporting/
#
# Copyright 1997-2025, American Registry for Internet Numbers, Ltd.
#
```

```
NetRange:      8.8.8.0 - 8.8.8.255
CIDR:          8.8.8.0/24
NetName:       GOGL
NetHandle:     NET-8-8-8-0-2
Parent:        NET8 (NET-8-0-0-0-0)
NetType:       Direct Allocation
OriginAS:
Organization:  Google LLC (GOGL)
RegDate:       2023-12-28
Updated:       2023-12-28
Ref:           https://rdap.arin.net/registry/ip/8.8.8.0
```

```
OrgName:       Google LLC
OrgId:         GOGL
Address:       1600 Amphitheatre Parkway
City:          Mountain View
StateProv:     CA
PostalCode:    94043
Country:       US
RegDate:       2000-03-30
Updated:       2019-10-31
Comment:       Please note that the recommended way to file abuse complaints are located in the following links.
Comment:
Comment:       To report abuse and illegal activity: https://www.google.com/contact/
Comment:
Comment:       For legal requests: http://support.google.com/legal
Comment:
Comment:       Regards,
Comment:       The Google Team
Ref:           https://rdap.arin.net/registry/entity/GOGL
```

```
OrgAbuseHandle: ABUSE5250-ARIN
OrgAbuseName:   Abuse
OrgAbusePhone:  +1-650-253-0000
OrgAbuseEmail:  network-abuse@google.com
OrgAbuseRef:    https://rdap.arin.net/registry/entity/ABUSE5250-ARIN
```

```
OrgTechHandle: ZG39-ARIN
OrgTechName:   Google LLC
OrgTechPhone:  +1-650-253-0000
OrgTechEmail:  arin-contact@google.com
OrgTechRef:    https://rdap.arin.net/registry/entity/ZG39-ARIN
```

ARIN



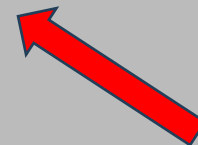
```
% This is the RIPE Database query service.
% The objects are in RPSL format.
%
% The RIPE Database is subject to Terms and Conditions.
% See https://docs.db.ripe.net/terms-conditions.html
%
% Note: this output has been filtered.
%       To receive output for a database update, use the "-B" flag.
%
% Information related to '193.0.0.0 - 193.0.7.255'
```

```
% Abuse contact for '193.0.0.0 - 193.0.7.255' is 'abuse@ripe.net'
```

```
inetnum:       193.0.0.0 - 193.0.7.255
netname:       RIPE-NCC
descr:         RIPE Network Coordination Centre
org:           ORG-RIEN1-RIPE
descr:         Amsterdam, Netherlands
remarks:       Used for RIPE NCC infrastructure.
country:       NL
admin-c:       BRD-RIPE
tech-c:        OPS4-RIPE
status:        ASSIGNED PA
mnt-by:        RIPE-NCC-MNT
created:       2003-03-17T12:15:57Z
last-modified: 2017-12-04T14:42:31Z
source:        RIPE
```

```
organisation:  ORG-RIEN1-RIPE
org-name:      Reseaux IP Europeens Network Coordination Centre (RIPE NCC)
country:       NL
org-type:      LIR
descr:         RIPE NCC Operations
address:       P.O. Box 10096
address:       1001 EB
address:       Amsterdam
address:       NETHERLANDS
phone:         +31205354444
fax-no:        +31205354445
admin-c:       MENN1-RIPE
admin-c:       MDIR-RIPE
abuse-c:       ops4-ripe
mnt-ref:       RIPE-NCC-HM-MNT
mnt-ref:       RIPE-NCC-MNT
mnt-by:        RIPE-NCC-HM-MNT
mnt-by:        RIPE-NCC-MNT
created:       2012-03-09T13:21:52Z
last-modified: 2023-12-05T13:40:03Z
source:        RIPE # Filtered
```

RIPE NCC



WHOIS

Contacto de abuse não é uniforme nos 5 Regional Internet Registries

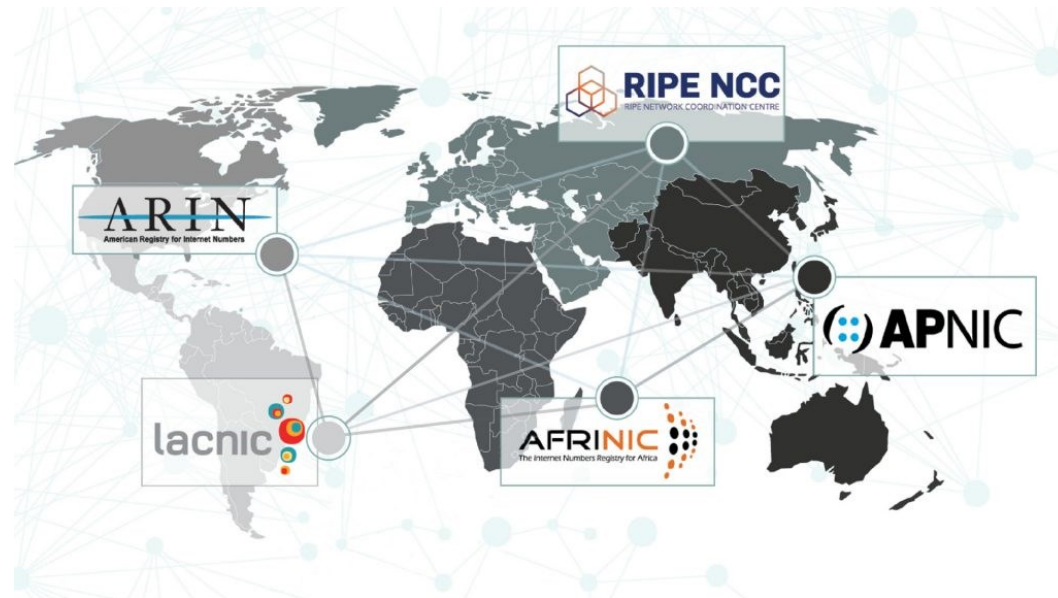
Servidores WHOIS: whois.<afrinic|apnic|arin|lacnic|ripe>.net

whois <ip>

whois <bloco/máscara>

whois <asn>

whois <...>



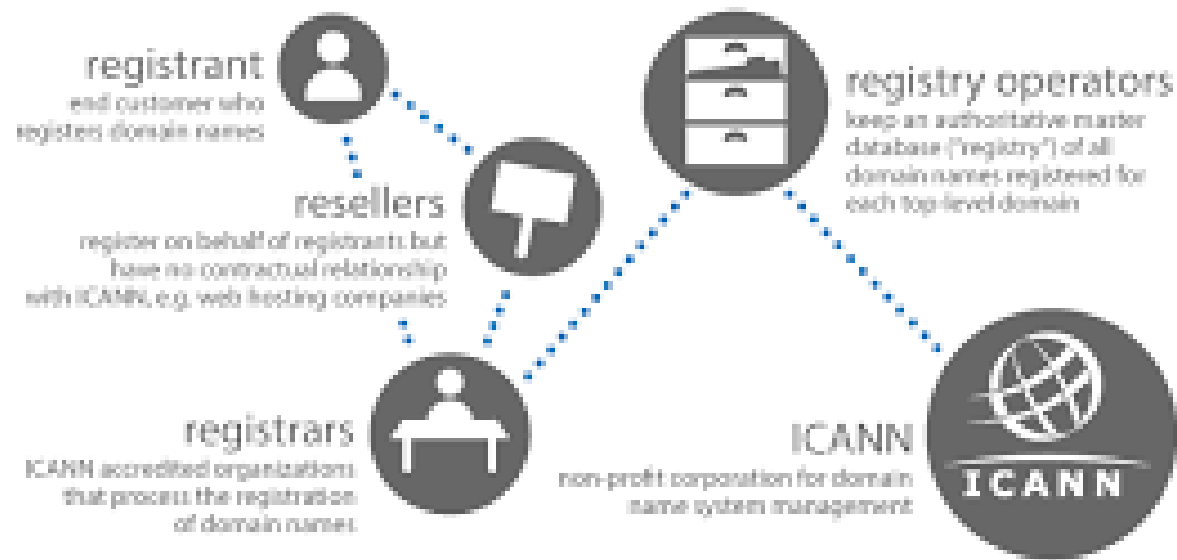
WHOIS: PESQUISAS HISTÓRICAS

`whois <...> --list-versions`

`whois <...> --show-version <#>`



WHOIS: DOMÍNIOS



domain registry process

O protocolo WHOIS também é usado para registo de domínios

Consulta é feita através dos registries responsáveis pelo TLD

A opacidade da informação disponível publicamente aumenta

RDAP

Registration Data Access
Protocol

RDAP é o sucessor do WHOIS

Mais no contexto dos
domínios DNS



IDEIAS CHAVE



É importante saber a quem pertence um determinado recurso, para sabermos para onde enviamos uma queixa em caso de necessidade



A primeira dificuldade é perceber em que RIR está a informação



Os ecossistemas do endereçamento IP e dos domínios DNS são distintos



Questões?

Obrigado.



csirt.fct.pt/podcast



csirt.fct.pt/mooc



csirt.fct.pt/etc