



Bisoños Usuarios de GNU/Linux de Mallorca y Alrededores | Bergantells Usuaris de GNU/Linux de Mallorca i Afegitons

## ¿Como saber a que organización pertenece una IP? (157558 lectures)

Per Ricardo Galli Granada, [gallir](http://mnm.uib.es/gallir/) (<http://mnm.uib.es/gallir/>)

Creado el 06/01/2001 00:00 modificado el 06/01/2001 00:00

*Muchas veces queremos saber a que empresas pertenecen las IPs que no resuelven a la inversa. El whois lo resuelve.*

El *whois* permite averiguar a que empresa está asignada o delegada una subred de Internet (ya no se dice clase, ya que los enrutados son *classless*) consultando a las base de datos de las organizaciones que se encargan de asignarlas.

El uso normal del *whois* para obtener la asignación de una subred es:

```
$ whois -h base_de_datos direccion_IP
```

aunque el *whois* de RedHat funciona de la siguiente forma:

```
$ whois direccion_IP@base_de_datos
```

Las asignaciones de subredes se asignan por separado para Europa ([RIPE](#)<sup>(1)</sup>), América ([ARIN](#)<sup>(2)</sup>) y Asia/Pacífico ([APNIC](#)<sup>(3)</sup>). Para consultar a sus base de datos hay que usar el nombre de host *whois* y el dominio correspondiente, *whois.ripe.net*, *whois.arin.net* o *whois.apnic.net*.

Por ejemplo para averiguar a quién está asignada las IP de *bulma.net* (IP 130.206.132.6):

```
$ whois 130.206.33.1@whois.ripe.net
[whois.ripe.net]

% Rights restricted by copyright.
  See http://www.ripe.net/ripenc/pub-services/db/copyright.html

inetnum: 130.206.0.0 - 130.206.255.255
netname: IRIS
descr: RedIRIS
...
```

Si probáis el comando anterior, veréis que la información es muy larga. En el *whois* estándar (no la del RH) se le puede indicar que no haga búsqueda recursiva de la información de red y obtener resultados más concretos. Por ejemplo:

```
$ whois -h whois.ripe.net 130.206.132.6 -r

% Rights restricted by copyright.
  See http://www.ripe.net/ripenc/pub-services/db/copyright.html

inetnum: 130.206.0.0 - 130.206.255.255
netname: IRIS
descr: RedIRIS
descr: Spanish National R&D Network
descr: Madrid, Spain
country: ES
admin-c: VC63
tech-c: IRIS1-RIPE
status: ASSIGNED PI
remarks: mail spam reports: abuse@rediris.es
remarks: security incidents: cert@rediris.es
```



```
mnt-by: REDIRIS-NMC
changed: miguel.sanz@rediris.es 19980429
changed: iris-nic@rediris.es 19990824
source: RIPE
```

```
route: 130.206.0.0/16
descr: IRIS
origin: AS766
mnt-by: REDIRIS-NMC
changed: ripe-dbm@ripe.net 19941121
source: RIPE
```

La información interesante es el primer campo (inetnum: 130.206.0.0 - 130.206.255.255) que indica todas las direcciones posibles y el *route* (route: 130.206.0.0/16) indica que las rutas en el BGP4 (**B**order **G**ateway **R**outing **P**rotocol). El resto de la información también puede ser usada para hacer otras consultas, aunque eso es motivo de más discusión. Sin embargo, si os mata la curiosidad, probad con:

```
$ whois -h whois.ripe.net RedIRIS
```

```
$ whois -h whois.ripe.net AS766 # Info del sistema autónomo...
```

Si en los ejemplos anteriores el *whois* no retorna ninguna información con otras direcciones IP, significa que la IP no pertenece a la región a la que hacéis la consulta, por lo que tenéis que probar en las otras dos o sin "-r", algunos servidores no lo aceptan, como el caso de ARIN.

--ricardo

---

#### Lista de enlaces de este artículo:

1. <http://www.ripe.net>
2. <http://www.arin.net>
3. <http://www.apnic.net>

---

E-mail del autor: [gallir\\_ARROBA\\_uib.es](mailto:gallir_ARROBA_uib.es)

Podrás encontrar este artículo e información adicional en: <http://bulma.net/body.phtml?nIdNoticia=380>