

Existe un comando mágico llamado "nast".

Esto es algo de lo que Nast puede hacer por ti:

- Hacer una lista de hosts conectados en tu LAN, utilizando el protocolo ARP.
- Seguir flujos de datos TCP, para imprimir los datos contenidos en una conexión definida por la tupla (IP origen, puerto origen, IP destino, puerto destino).
- Encontrar los equipos que nos dan paso a internet (gateways).
- Conocer el tipo de enlace (hub o switch), usando el protocolo ICMP.
- Escanear puertos parcialmente. Es decir, sin realizar la conexión completa, pero suficiente para saber de qué puerto se trata.

Instalación

Para instalarlo sólo hay que ejecutar en una consola:

```
sudo apt-get install nast
```

Averiguar las IP de los ordenadores de la red

Hay que teclear en un terminal:

```
sudo nast -m
```

Devolverá una lista como la siguiente:

```
libelula15@libelula15-System-Product-Name:~$ sudo nast -m
[sudo] contraseña para libelula15:
Nast V. 0.2.0
Mapping the Lan for 255.255.0.0 subnet ... please wait
MAC address          Ip address (hostname)
-----
08:50:E6:3E:96:59    172.16.3.179 (libelula15-System-Product-Name) (*)
14:CC:20:7A:88:DB    172.16.0.1 ( _gateway)
70:4F:57:C6:30:18    172.16.2.2 (172.16.2.2)
E4:6F:13:5A:41:AF    172.16.2.150 (172.16.2.150)
18:03:73:4E:37:0C    172.16.2.153 (172.16.2.153)
00:22:41:38:DF:8C    172.16.3.23 (172.16.3.23)
00:E0:91:CE:EF:31    172.16.3.101 (172.16.3.101)
00:1B:FC:FF:F6:15    172.16.3.170 (172.16.3.170)
00:17:F2:04:8E:B4    172.16.3.190 (172.16.3.190)
00:1E:0B:33:BD:A7    172.16.9.9 (172.16.9.9)
00:1F:C6:BE:CA:BF    172.16.11.10 (172.16.11.10)
6C:3B:E5:41:79:12    172.16.11.25 (172.16.11.25)
00:1A:4D:94:2B:F8    172.16.12.10 (172.16.12.10)
```

- [Info](#)

From:

<http://server-jk.ddns.net/dokuwiki/> - **IES Palomeras-Vallecas Dep. Electronica**

Permanent link:

<http://server-jk.ddns.net/dokuwiki/doku.php?id=aula:redes:herramientas:nast>

Last update: **2025/01/22 02:02**

