UD 3. NA 3.7

Protocols de xarxes UNIX i utilitats per als sistemes amb protocols TCP/IP

Autor: Sergi Tur Badenas

Introducció

GNU/Linux

- Els sistemes GNU/Linux/UNIX estan pensats desde els seus orígens per funcionar en xarxa
- Fins i tots els sistemes aïllats han de tenir xarxa. La interfície **loopback (lo)** és obligatòria.
- Històricament els sistemes Unix han tingut i tenen una indiscutible rellevància en el món de les xarxes de computadors.
- Molts dispositius de maquinari de xarxa (routers, gateways, etc.) tenen programari basat en UNIX.
- L'objectiu d'aquesta activitat és donar a conèixer les eines, comandes i protocols de xarxa que proporcionen els sistemes GNU/Linux.

Autor: Sergi Tur Badenas

Índex

Configuració de dispositius de xarxa. Comandes i protocols

- ifconfig i fitxers de configuració de xarxa
- Protocol DHCP
- Protocol DNS
- Encaminament

Monitorització de la xarxa. Comandes i protocols

- Estat de la xarxa, serveis i ports. Netstat i nmap
- Analitzadors de xarxes. Tcpdump i ethereal

Eines gràfiques de configuració de la xarxa

- Net-tools

Autor: Sergi Tur Badenas

Consideracions prèvies

Aspectes a tenir en compte i coneixements previs necessaris per dur a terme aquesta activitat

Autor: Sergi Tur Badenas

Organitzadors previs

Coneixements

- Coneixements bàsics de protocols.
- Protocol IP. Adreces IP, paràmetres de xarxa (màscara, adreça de xarxa, broadcast, etc.). Adreces MAC.
- Coneixements bàsics de xarxes d'àrea local.
- Nivells OSI.
- Utilització de la línia de comandes de sistemes operatius multiusuari (GNU/Linux).

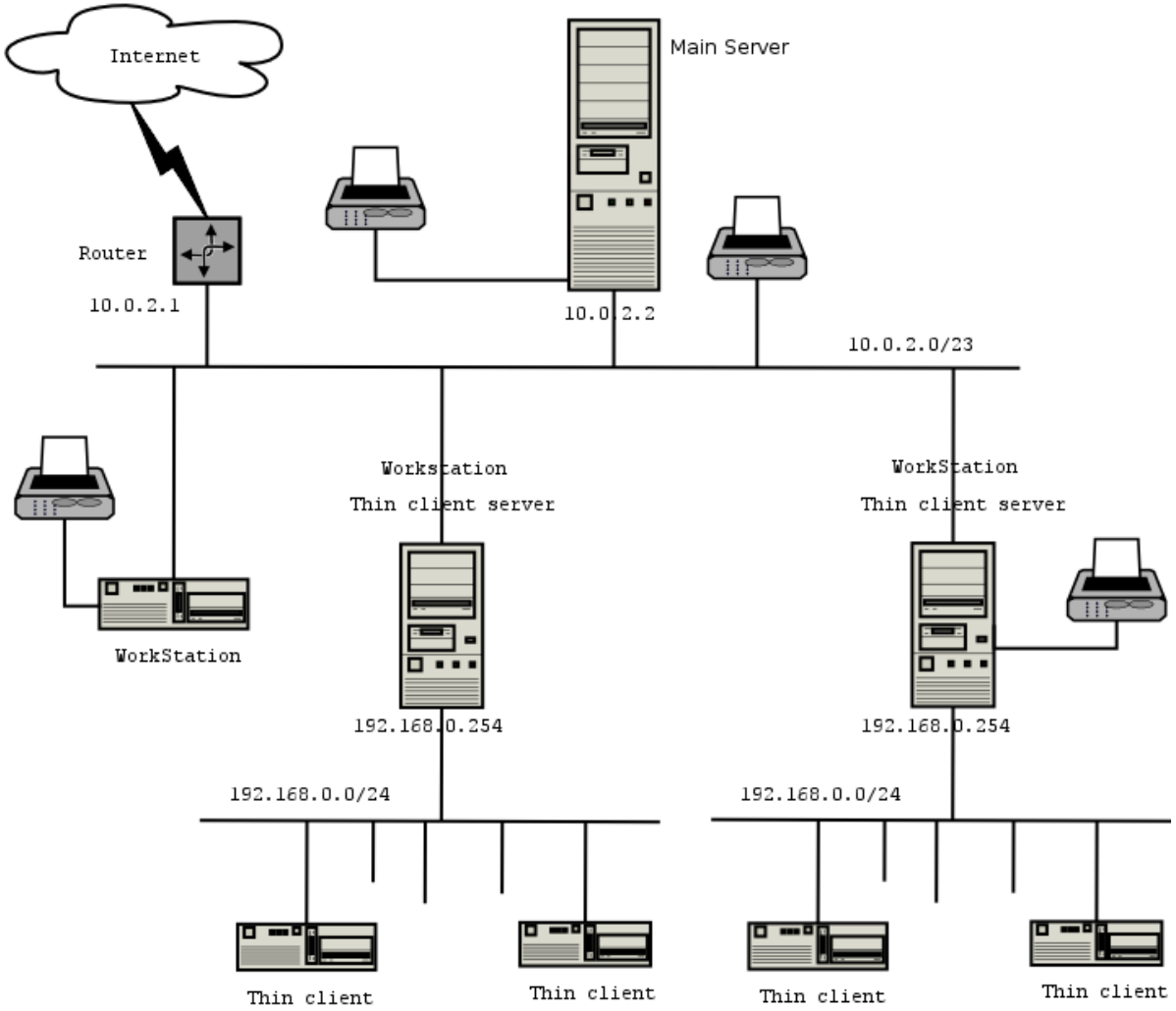
Recursos

- Xarxa d'àrea local per dur a terme els exemples.

Autor: Sergi Tur Badenas

Arquitectura de la xarxa

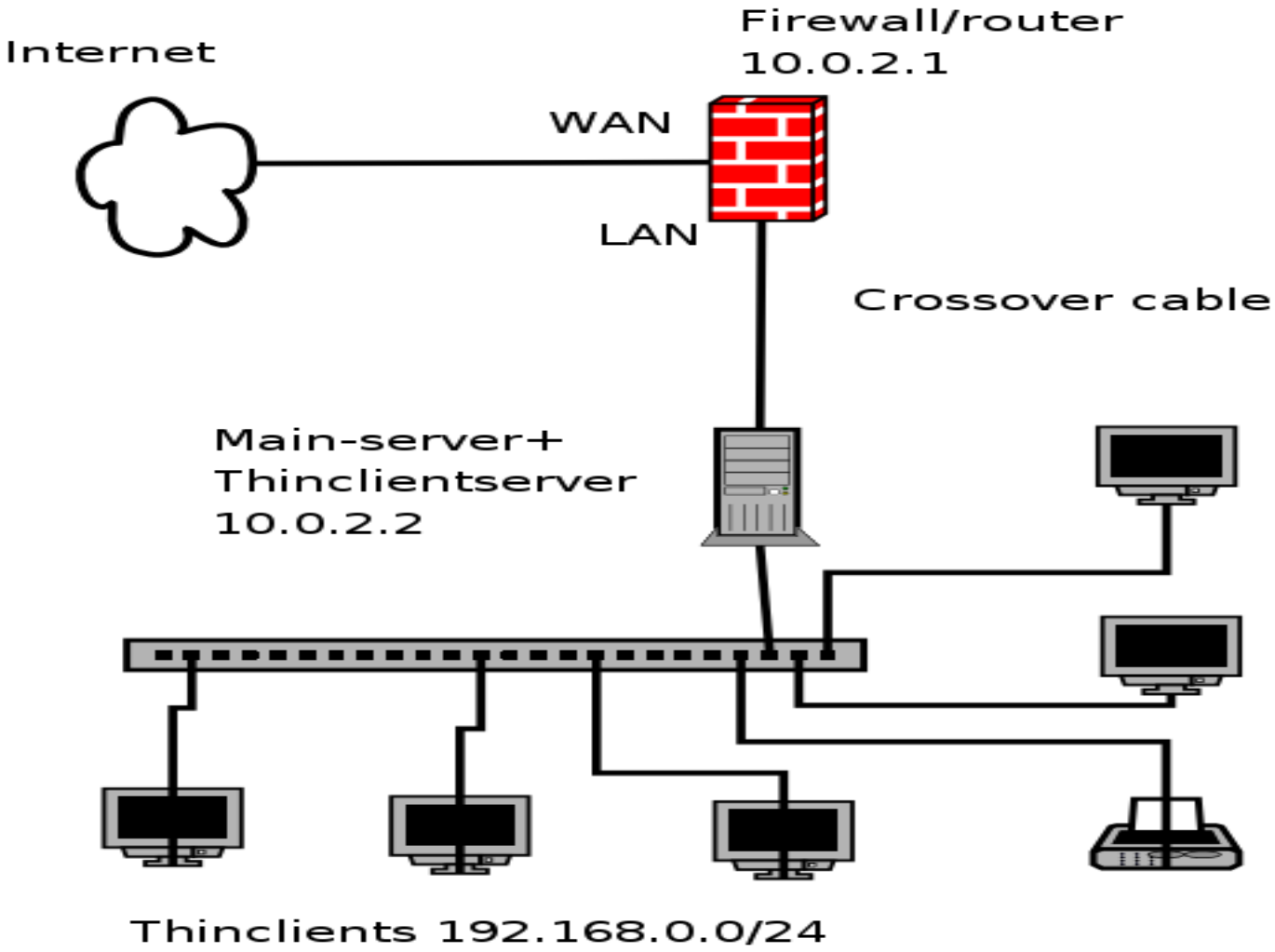
Arquitectura SkoleLinux



Autor: Sergi Tur Badenas

Arquitectura de la xarxa (II)

Arquitectura simplificada. Combo-Server



Autor: Sergi Tur Badenas

Programari

Paquets necessaris:

- Paquet net-tools de debian:
  - /sbin/ifconfig
  - /sbin/route
  - /sbin/netstat
- Paquet traceroute
- Paquet tcpdump
- Paquet dns-utils
  - /usr/bin/dig
  - /usr/bin/nslookup
- Paquet dnstracer
- Paquet nmap
- Paquet whois

Autor: Sergi Tur Badenas

Instal·lació de paquets Debian

Pre-instal·lació

- Cal comprovar si ja es disposa del paquet:
  - $ sudo dpkg -l | grep ethereal
- Mirem si el paquet està disponible al repositori
  - $ sudo apt-cache search ethereal
- Si volem saber més informació sobre el paquet a instal·lar:
  - $ sudo apt-cache show ethereal

Autor: Sergi Tur Badenas

Instal·lació de paquets Debian (II)

Instal·lació

- $ sudo apt-get install ethereal
  - **NOTA**: A l'instal·lar cal observar quins paquets es modificaran i/o s'eliminaran per tal d'evitar “pèrdues” no desitjades.

Desinstal·lació

- $ sudo apt-get install ethereal

Com podeu veure són necessaris permisos de **superusuari** per dur a terme aquestes operacions.

Si es disposa d'entorn gràfic es pot utilitzar **synaptic** com a eina de gestió de paquets.

Autor: Sergi Tur Badenas

Qüestions generals

Diferències entre distribucions

- Les comandes que s'expliquen en aquesta activitat estan disponibles en qualsevol distribució GNU/Linux actual. En tot cas, la distribució de les carpetes pot diferir de l'estàndard de Debian. Per localitzar una comanda podem utilitzar:
  - **$ whereis ifconfig**
- També és possible que en alguns casos les comandes no estiguin en el path de l'usuari i/o que només el susperusuari hi tingui accés. En aquest cas cal utilitzar la ruta completa i/o accedir al sistema com a superusuari.

Autor: Sergi Tur Badenas

Configuració dels dispositius de xarxa

Comandes per la configuració dels dispositius de xarxa (NICs)

Autor: Sergi Tur Badenas

Paràmetres de xarxa

Paràmetres de xarxa

- **ifconfig**
  - **Adreça IP.** Adreça lògica del protocol IP. Nivell de xarxa (Nivell 3 OSI).
  - **Adreça MAC.** Adreça física. Assignada a la NIC. Nivell MAC (Nivell 2 OSI).
  - **Màscara de xarxa.** Determina quina part de l'adreça correspon a la xarxa i quina a les màquines de la xarxa.
  - **Adreça de xarxa.** Ve determinada per la màscara i és l'adreça que té els bits corresponents a adreces de màquines a **0**.
  - **Adreça de difusió** (broadcast). Ve determinada per la màscara i és l'adreça que té l'últim octet establert a **255**.

Autor: Sergi Tur Badenas

Paràmetres de xarxa (II)

Paràmetres de xarxa

- **route**
  - Adreça IP de la **passarel·la** (**gateway**). Determina l'ordinador de la xarxa local (adreça IP) encarregat d'encaminar els paquets interns a la xarxa exterior.
- **dns-nameserver**
  - Fitxer ***/etc/resolv.conf***
- **Sobre l'encaminament i la resolució de noms en parlarem amb més profunditat en temes posteriors.**

Autor: Sergi Tur Badenas

ifconfig

Característiques:

- És la comanda utilitzada per configurar les interfícies de xarxa (NICs) per TCP/IP i actualment és l'estàndard dels sistemes Unix i derivats.
- Amb ifconfig es poden establir i consultar els paràmetres generals de les NICs d'una màquina.
- Amb aquesta comanda també es pot aturar o engegar la interfície de xarxa.
- Un mateix host pot tenir més d'una interfície de xarxa (p. ex. els encaminadors, connexions híbrides cable i wireless, etc.).
- En Windows la comanda anàloga és **ipconfig.**

Autor: Sergi Tur Badenas

ifconfig (II)

ifconfig només configura els paràmetres:

- **IP**: Adreça lògica del protocol IP. Nivell de xarxa (Nivell 3 OSI)
- **MAC**. Adreça física. Assignada a la NIC. Nivell MAC (Nivell 2 OSI)
- **Màscara de xarxa**: determina quina part de l'adreça correspon a la xarxa i quina a les màquines de la xarxa.

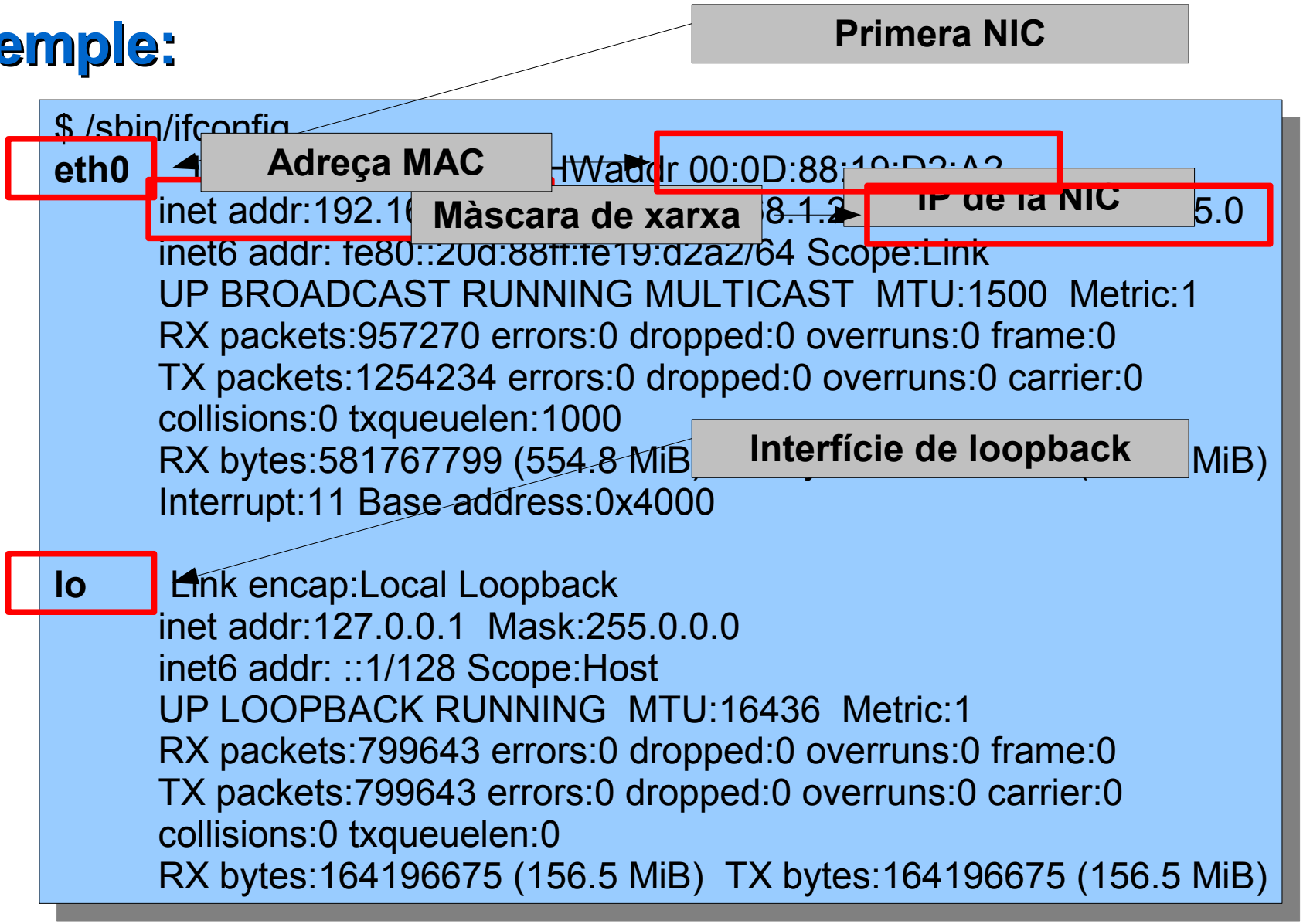
Tipus d'interfícies:

- **Loopback**: **lo**. Encara que la màquina estigui sola (stand-alone) és necessària l'adreça de loopback.
- **Ethernet**: **eth0**, **eth1**, ...
- **Wi-Fi**: **wlan0**, wlan1. Tot i això sovint també s'utilitza la sintaxi d'ethernet: **ethX**
- **Token Ring**: **tr0**, tr1, ...
- **PPP**: **ppp0**, ppp1, ...

Autor: Sergi Tur Badenas

ifconfig (III)

Exemple:



Autor: Sergi Tur Badenas

ifconfig (III)

Paquet necessari

- net-tools

Referències

- man ifconfig
- Article de la wikipedia

Altres enllaços

- Exemples ifconfig

```
eth0      Link encap:Ethernet  HWaddr 00:00:E2:1E:4C:A3
          inet addr:10.0.0.2  Bcast:10.0.0.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:59108 errors:0 dropped:0 overruns:0 frame:0
          TX packets:59011 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:6415496 (6.1 MiB)  TX bytes:30712998 (29.2 MiB)
          Interrupt:19 Base address:0xb400 Memory:1b500000-1b500038
```

GNU-LINUX

Autor: Sergi Tur Badenas

Gateway

La passarel·la o gateway es configura mitjançant la comanda route

- **$ route add default gw 192.168.1.1**
- És comú que la primera IP de la xarxa sigui el gateway (.1) però no obligatori.
- Aprofundirem en els detalls de l'encaminament en un apartat posterior i en la unitat didàctica 6.

Autor: Sergi Tur Badenas

Configuració de les NICs

Configuració manual:

- Configuració xarxa estàtica
  - **$ sudo ifconfig eth0 192.168.99.35 netmask 255.255.255.0 up**
- Configuració loopback
  - $ sudo ifconfig lo inet 127.0.0.1 up
- Gateway
  - $ sudo route add default gw 192.168.1.1
- La configuració manual no és persistent

Una altra forma de configurar és utilitzar fitxers de configuració...

Autor: Sergi Tur Badenas

Fitxers de configuració de xarxa

Fitxers

- **/etc/network/interfaces**
- Resolució de noms (DNS):
  - **/etc/resolv.conf**
  - **/etc/hosts**
- Gateway. Es configura a nivell de les taules de ruta del kernel o al fitxer **interfaces**.

Nota: Cal tenir en compte que molts fitxers de configuració, com les comandes, també tenen una entrada de manual de Linux (man interfaces).

Autor: Sergi Tur Badenas

/etc/network/interfaces

```
$ cat /etc/network/interfaces
# The loopback interface
auto lo
iface lo inet loopback

auto eth0
iface eth0 inet static
    address 10.0.2.2
    netmask 255.255.254.0
    broadcast 10.0.3.255
    dns-nameserver 127.0.0.1
    dns-search intern
    gateway 10.0.2.1

auto eth1
iface eth1 inet static
    address 192.168.0.254
    netmask 255.255.255.0
    broadcast 192.168.0.255
```

Configuració del loopback

Configuració ethernet:
Es configuren tots els paràmetres de xarxa

Configuració ethernet del segon dispositiu de xarxa

- Altres distribucions (com Fedora) utilitzen uns altres fitxers (P.ex. **/etc/sysconfig/network**)

Autor: Sergi Tur Badenas

ifup/ifdown

Les comandes ifup/ifdown són les encarregades d'activar/desactivar les interfícies de xarxa segons els paràmetres dels fitxers de configuració.

- El sistema operatiu s'encarrega de cridar aquestes comandes a l'iniciar l'ordinador.

```
$ sudo ifup eth0
.....
Listening on LPF/eth0/00:0d:88:19:d2:a2
Sending on   LPF/eth0/00:0d:88:19:d2:a2
Sending on   Socket/fallback
DHCPREQUEST on eth0 to 255.255.255.255 port 67
DHCPACK from 192.168.1.1
bound to 192.168.1.14 -- renewal in 244026 seconds.
$ sudo ifdown eth0
.....
Listening on LPF/eth0/00:0d:88:19:d2:a2
Sending on   LPF/eth0/00:0d:88:19:d2:a2
Sending on   Socket/fallback
DHCPRELEASE on eth0 to 192.168.1.1 port 67
```


Autor: Sergi Tur Badenas

DHCP

Característiques:

- Són les sigles de l'anglès Protocol de Configuració Dinàmica de Màquines (**Dynamic Host Configuration Protocol**).
- És un protocol de xarxa, on un servidor proveeix dels paràmetres necessaris de configuració i assignació d'adreces IP a les màquines d'una xarxa.
- És un estàndard en xarxes que també es podem trobar en Windows o altres Sistemes Operatius.

Autor: Sergi Tur Badenas

DHCP (II)

DHCP pot configurar els següents paràmetres:

- Nom de la màquina
- Adreça del servidor DNS
- Porta d'enllaç (passarel·la o gateway)
- Adreça de difusió (broadcast)
- Màscara de xarxa
- Altres paràmetres opcionals (adreces de serveis addicionals, configuració extra, etc.)

Autor: Sergi Tur Badenas

DHCP (III)

Assignacions d'IPs:

- **Manual:** hi ha una taula que assigna les adreces IP segons les adreces MAC.
- **Automàtica:** S'assigna de forma permanent una adreça IP obtinguda d'un rang d'adreces determinat per l'administrador de DHCP.
- **Dinàmica:** El procediment és idèntic a l'anterior però les adreces no són fixes. Cada cop que un PC es connecta a la xarxa aconsegueix una IP diferent.
- **Híbrida:** Es poden combinar opcions i, per exemple, tenir alguns PCs de la xarxa amb adreces manuals i la resta amb adreces assignades de forma dinàmica.

Autor: Sergi Tur Badenas

DHCP (IV)

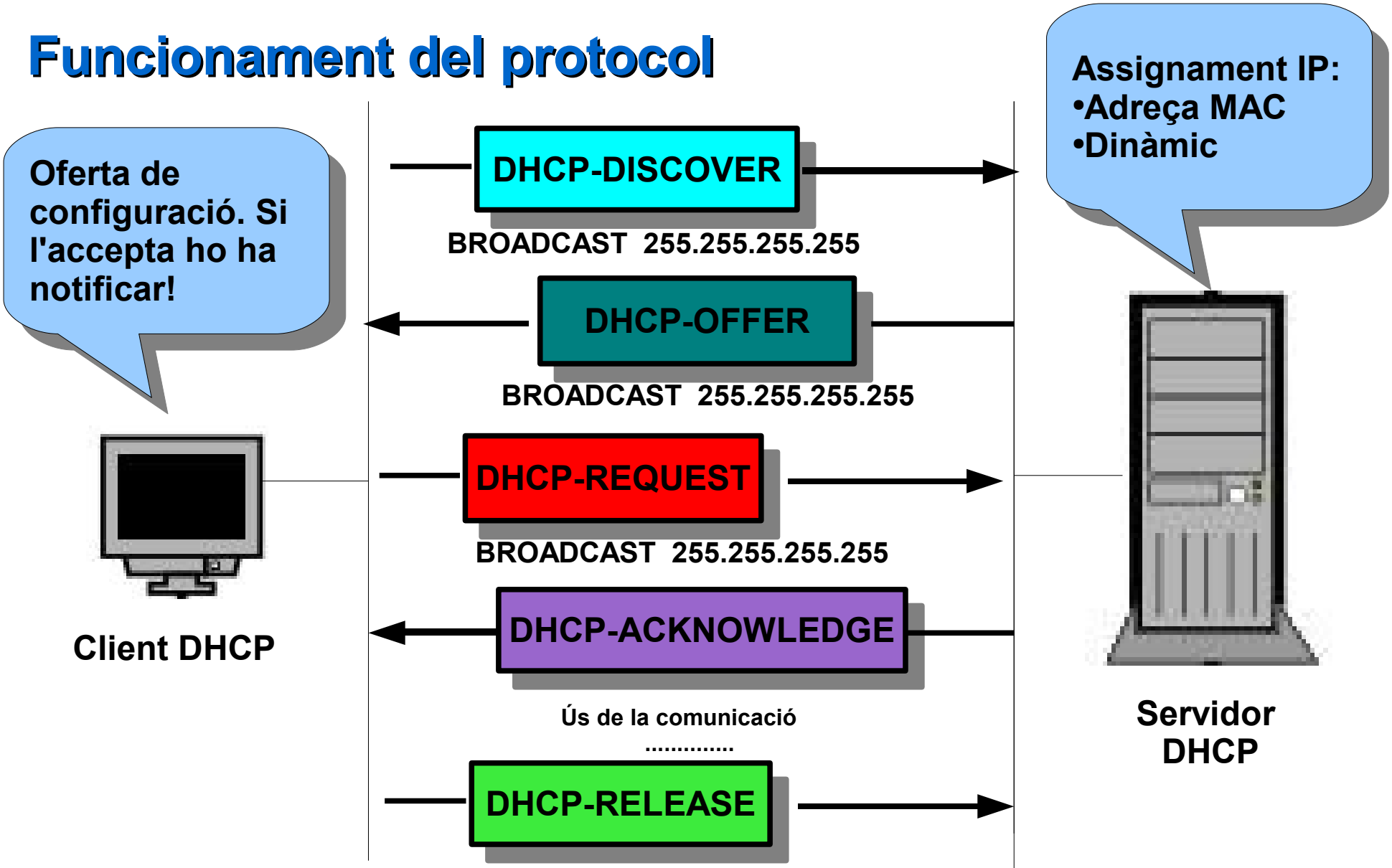
Paquets del protocol

- **DHCPDISCOVER:** L'envia el client dhcp a totes les adreces de la xarxa (broadcast) cercant un servidor DHCP.
- **DHCPOFFER:** L'envia el servidor a totes les adreces, ja que el client encara no té adreça de xarxa. El servidor inicia el procés d'assignació d'IP i paràmetres de xarxa i fa una oferta de configuració al client.
- **DHCPREQUEST:** El client rep l'oferta i respon amb un paquet de petició. També és broadcast tot i sabent l'adreça del servidor DHCP. El client guarda la configuració a l'espera d'una confirmació per part del servidor.
- **DHCPACK:** Un cop el servidor rep una petició contesta amb un paquet de reconeixement. El client, un cop rep la confirmació, inicialitza la NIC.
- **DHCPRELEASE:** No és obligatori però els clients poden informar al servidors de quan deixen d'utilitzar la configuració (NIC apagada).

Autor: Sergi Tur Badenas

DHCP (IV)

Funcionament del protocol



Autor: Sergi Tur Badenas

DHCP (V)

Exemple

```
$ sudo dhclient eth0
.....
Listening on LPF/eth0/00:0d:88:19:d2:a2
Sending on   LPF/eth0/00:0d:88:19:d2:a2
Sending on   Socket/fallback
DHCPREQUEST on eth0 to 255.255.255.255 port 67
DHCPREQUEST on eth0 to 255.255.255.255 port 67
DHCPDISCOVER on eth0 to 255.255.255.255 port 67 interval 4
DHCPOFFER from 192.168.1.1
DHCPREQUEST on eth0 to 255.255.255.255 port 67
DHCPACK from 192.168.1.1
bound to 192.168.1.15 -- renewal in 299477 seconds.
sergi.tur@casa:~/downloads$ sudo ifdown eth0
.....
Listening on LPF/eth0/00:0d:88:19:d2:a2
Sending on   LPF/eth0/00:0d:88:19:d2:a2
Sending on   Socket/fallback
DHCPRELEASE on eth0 to 192.168.1.1 port 67
```


Autor: Sergi Tur Badenas

Resolució de noms (DNS)

Aspectes a tenir en compte de la configuració de resolució de noms. Comandes i fitxers de configuració

Autor: Sergi Tur Badenas

Resolució de noms (DNS)

Característiques:

- Domain Name System (DNS) és una base de dades distribuïda i jeràrquica que emmagatzema la informació associada als dominis de xarxes com p. ex. Internet.
- L'assignació de noms a adreces IP és la funcionalitat més comuna però no l'única.
- Inicialment, DNS va néixer de la necessitat de recordar fàcilment els noms de les màquines. S'utilitzava el fitxer **/etc/hosts** per traduir IPs en noms de domini. El creixement explosiu de la xarxa va demostrar la poca escalabilitat d'aquest sistema i va sorgir el sistema DNS modern, on la càrrega i la informació de DNS es troba distribuïda de forma jeràrquica a diferents màquines d'Internet.

Autor: Sergi Tur Badenas

Resolució de noms (DNS)

Funcionament

- Donada una adreça com atonito.lsi.upc.edu (147.83.20.2)

Jerarquia DNS

- Nivells
  - Les parts que componen aquest nom de domini són:
    - **Root**. Els noms de domini tenen una estructura d'arbre. Tot nom de domini parteix d'una arrel (**.**) L'adreça real és doncs atonito.lsi.upc.edu**.**
      Els servidors root són:
      - A.ROOT-SERVERS.NET.
      - B.ROOT-SERVERS.NET.
      - .....
      - M.ROOT-SERVERS.NET.

Autor: Sergi Tur Badenas

Resolució de noms (DNS)

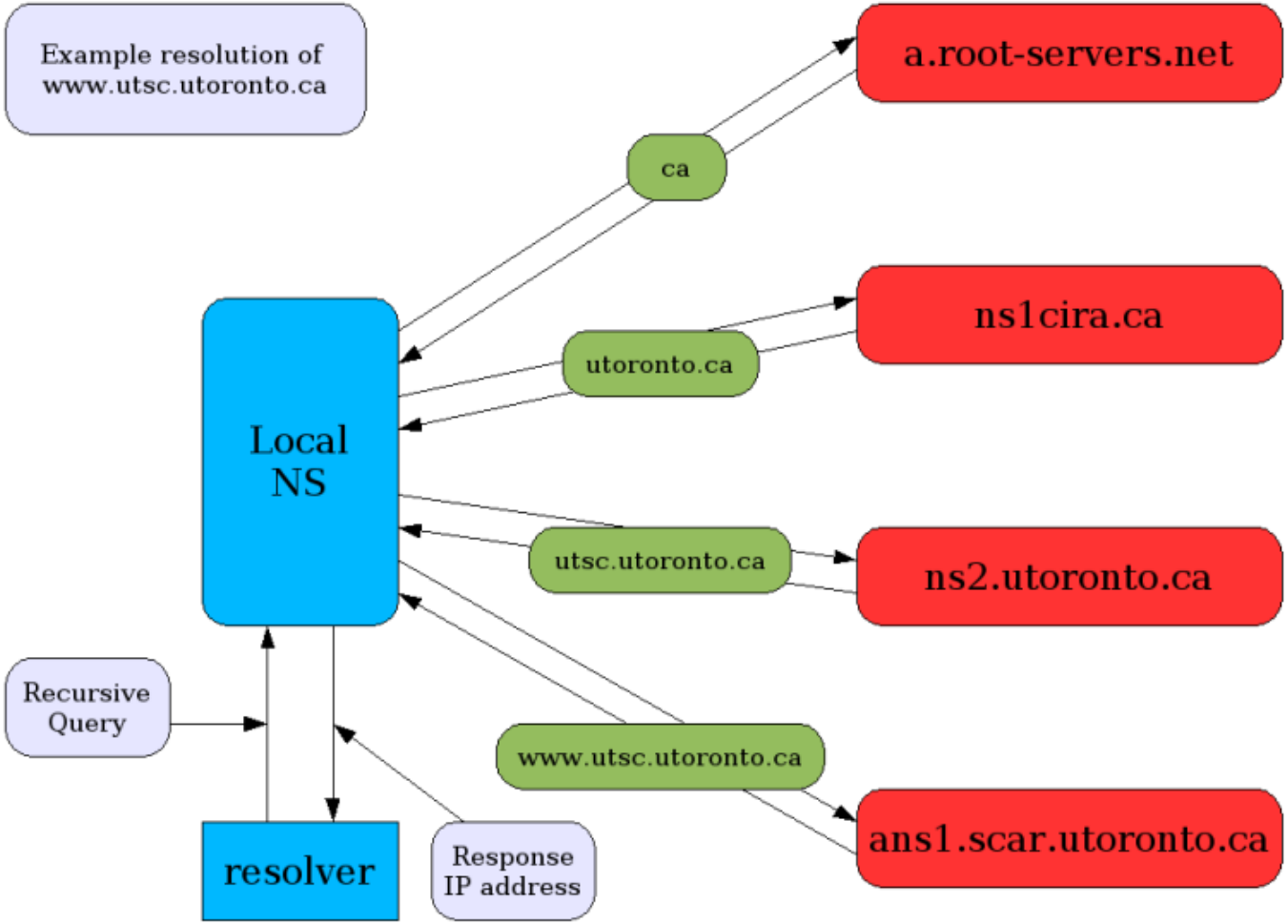
Jerarquia DNS (continuació)

- Nivells
  - **TLD (top-level domain)**. El primer nivell del domini indica el top-level domain (**edu**). Altres top-level domains són es, org, edu, com, bizz, etc...
  - **Subdominis**. La resta de parts del nom de domini són subdominis del domini precedent (Isi és subdomini de upc.edu).
  - **Host**. Normalment, encara que no sempre, l'última part del nom del domini (p. ex. atonito) correspon al nom d'una màquina final.

Autor: Sergi Tur Badenas

Resolució de noms (DNS)

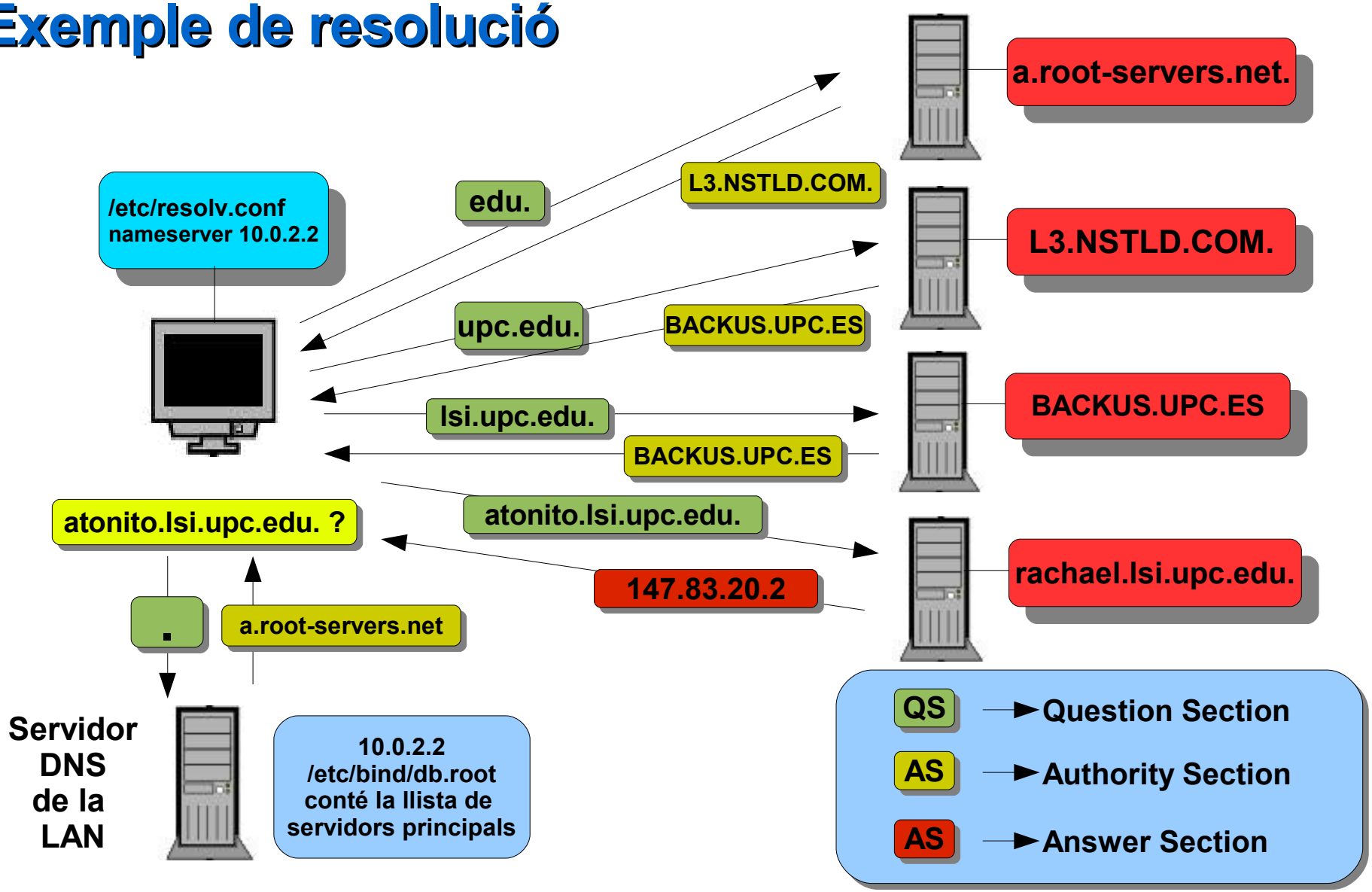
Exemple de resolució



Autor: Sergi Tur Badenas

Resolució de noms (DNS)

Exemple de resolució



Autor: Sergi Tur Badenas

Comandes DNS

Comandes

- **dig**
  - És una utilitat de resolució de noms amb DNS.
- **dnstrace**
  - Rastreja la cadena de servidors DNS utilitzats per a resoldre una adreça.

Exemple de resolució. Comanda dig

```
$ dig .
.....................
;; QUESTION SECTION:
;.                          IN      A
;; AUTHORITY SECTION:
.                   143     IN      SOA     A.ROOT-SERVERS.NET. NSTLD.VERISIGN-GRS.COM.
.....................
```


Autor: Sergi Tur Badenas

Resolució de noms (DNS)

```
$ dig edu.
.....
;; QUESTION SECTION:
;edu.                    IN      A
;; AUTHORITY SECTION:
edu.            86400   IN      SOA     L3.NSTLD.COM. NSTLD.VERISIGN-GRS.COM.
.....
```

```
$ dig upc.edu.
.....
;; QUESTION SECTION:
;upc.edu.                IN      A
;; AUTHORITY SECTION:
upc.edu.        149289  IN      NS      EULER.UPC.ES.
upc.edu.        149289  IN      NS      BACKUS.UPC.ES.
.....
```

```
$ dig upc.edu.
.....
;; QUESTION SECTION:
;atonito.lsi.upc.edu.        IN      A
;; ANSWER SECTION:
atonito.lsi.upc.edu.    172800  IN      A       147.83.20.2
.....
```


Autor: Sergi Tur Badenas

Resolució de noms (DNS)

Configuració

- L'únic imprescindible per configurar un servidor DNS és definir la llista de servidors arrel.

```
$ dig +norec +noques +nostats +nocmd atonito.lsi.upc.edu
@A.ROOT-SERVERS.NET
.....................................................................
;; AUTHORITY SECTION:
edu.            172800  IN      NS      L3.NSTLD.COM.
edu.            172800  IN      NS      D3.NSTLD.COM.
edu.            172800  IN      NS      A3.NSTLD.COM.
edu.            172800  IN      NS      E3.NSTLD.COM.
edu.            172800  IN      NS      C3.NSTLD.COM.
edu.            172800  IN      NS      G3.NSTLD.COM.
edu.            172800  IN      NS      M3.NSTLD.COM.
edu.            172800  IN      NS      H3.NSTLD.COM.
;; ADDITIONAL SECTION:
L3.NSTLD.COM.       172800  IN      A       192.41.162.32
D3.NSTLD.COM.       172800  IN      A       192.31.80.32
A3.NSTLD.COM.       172800  IN      A       192.5.6.32
E3.NSTLD.COM.       172800  IN      A       192.12.94.32
C3.NSTLD.COM.       172800  IN      A       192.26.92.32
G3.NSTLD.COM.       172800  IN      A       192.42.93.32
M3.NSTLD.COM.       172800  IN      A       192.55.83.32
H3.NSTLD.COM.       172800  IN      A       192.54.112.32
```


Autor: Sergi Tur Badenas

Resolució de noms (DNS)

- **Exemple dnstracer**

```
$ dnstracer -s B.ROOT-SERVERS.NET www.upc.edu
Tracing to www.upc.edu[a] via B.ROOT-SERVERS.NET, maximum of 3 retries
B.ROOT-SERVERS.NET (192.228.79.201)
 |\___ H3.NSTLD.COM [edu] (192.54.112.32)
 |    |\___ BACKUS.UPC.ES [upc.edu] (147.83.2.3) Got authoritative answer [received type is
cname]
 |    \___ EULER.UPC.ES [upc.edu] (147.83.2.10) Got authoritative answer [received type is
cname]
 |\___ M3.NSTLD.COM [edu] (192.55.83.32)
 |    |\___ BACKUS.UPC.ES [upc.edu] (147.83.2.3) (cached)
 |    \___ EULER.UPC.ES [upc.edu] (147.83.2.10) (cached)
 |\___ G3.NSTLD.COM [edu] (192.42.93.32)
 |    |\___ BACKUS.UPC.ES [upc.edu] (147.83.2.3) (cached)
 |    \___ EULER.UPC.ES [upc.edu] (147.83.2.10) (cached)
 |\___ C3.NSTLD.COM [edu] (192.26.92.32)
 |    |\___ EULER.UPC.ES [upc.edu] (147.83.2.10) (cached)
 |    \___ BACKUS.UPC.ES [upc.edu] (147.83.2.3) (cached)
 |\___ E3.NSTLD.COM [edu] (192.12.94.32)
 |    |\___ EULER.UPC.ES [upc.edu] (147.83.2.10) (cached)
 |    \___ BACKUS.UPC.ES [upc.edu] (147.83.2.3) (cached)
.....................................................
```


Autor: Sergi Tur Badenas

Resolució de noms (DNS)

Resolució inversa. Comanda host

```
$ host 147.83.194.21
21.194.83.147.in-addr.arpa domain name pointer upc.edu.
  21.194.83.147.in-addr.arpa domain name pointer www.upc.es.
21.194.83.147.in-addr.arpa domain name pointer raiden.upc.es.
21.194.83.147.in-addr.arpa domain name pointer upc.es.
```

- ## Resolució directa. Comanda ping

```
$ ping www.upc.edu
PING www.upc.es (147.83.194.21) 56(84) bytes of data.
64 bytes from upc.edu (147.83.194.21): icmp_seq=1 ttl=50 time=86.2 ms
64 bytes from upc.edu (147.83.194.21): icmp_seq=2 ttl=50 time=86.1 ms
64 bytes from upc.edu (147.83.194.21): icmp_seq=3 ttl=50 time=86.1 ms
64 bytes from upc.edu (147.83.194.21): icmp_seq=4 ttl=50 time=86.4 ms
```


Autor: Sergi Tur Badenas

Fitxers resolució de noms (DNS)

- **/etc/hosts**

```
127.0.0.1       localhost.localdomain   localhost       dhcp151
```

- **/etc/resolv.conf**

```
search intern
nameserver 10.0.2.2
```

- **/etc/nsswitch.conf**

```
passwd:         files ldap
group:          files ldap
shadow:         files ldap

.....

hosts:          files dns
networks:       files
```


Autor: Sergi Tur Badenas

ENCAMINAMENT

Eines per a la gestió de l'encaminament.

Autor: Sergi Tur Badenas

Encaminament

Encaminament

- És el mecanisme pel qual en una xarxa els paquets es fan arribar d'un origen a un destí seguint un camí o ruta a través d'una xarxa.

Nivell 3 OSI. Nivell de xarxa

- Protocol IP. Les adreces IP són el mecanisme d'identificació d'host a partir del qual podem encaminar.

Routers

- Els routers o encaminadors són els dispositius que s'encarreguen de l'encaminament a nivell de xarxa.

Autor: Sergi Tur Badenas

traceroute

- **Exemple**

```
$sudo traceroute www.jazztel.es
traceroute to www.jazztel.es (212.106.192.74), 64 hops max, 40 byte packets
 1  192.168.1.1 (192.168.1.1)  1 ms  1 ms  1 ms
 2  inversas.2g.jazztel.es (87.219.198.1)  39 ms  38 ms  39 ms
 3  10.255.136.254 (10.255.136.254)  54 ms  49 ms  50 ms
 4  inversas.2g.jazztel.es (87.216.0.2)  38 ms  38 ms  38 ms
 5  inversas.2g.jazztel.es (87.216.0.1)  243 ms  177 ms  222 ms
 6  208.175.154.177 (208.175.154.177)  42 ms  37 ms  38 ms
 7  ge-7-1-0-zcr1.bap.cw.net (208.175.154.38)  37 ms so-1-0-0-ycr1.bap.cw.net
(208.175.154.42)
.....
11  * * *
12  * * *
```

utilitzar per detectar els punts conflictius de l'enllaç entre dues màquines.

- Per comprovar la configuració de les taules de rutes.

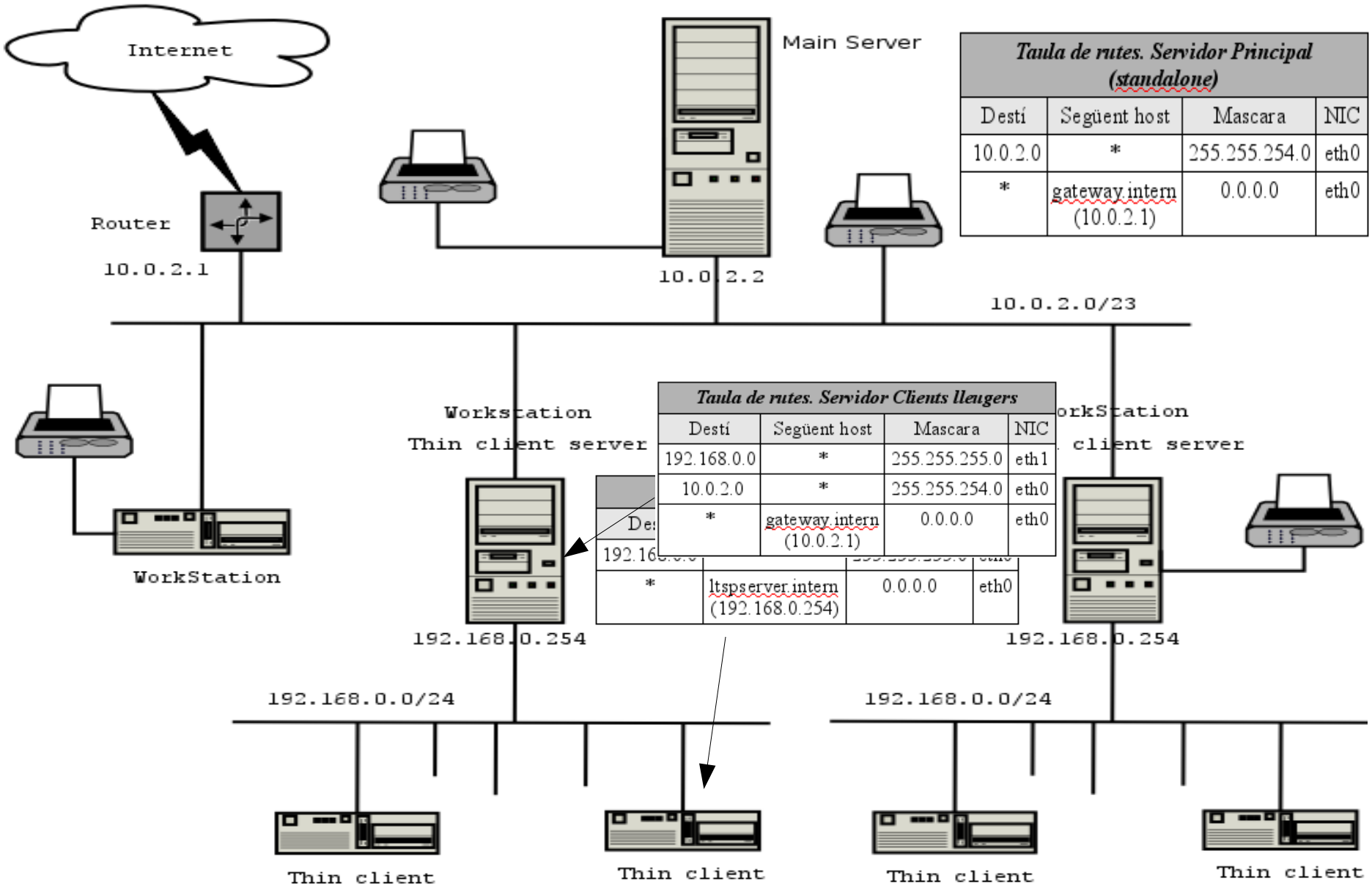
Autor: Sergi Tur Badenas

Encaminament

- **Comanda route**
  - Característiques:
    - La comanda route permet manipular i visualitzar les taules d'enrutament del kernel dels sistemes GNU/Linux.
    - El tema d'enrutament i interconnexió de xarxes d'àrea local el veurem a la unitat didàctica 6: Interconnexió de xarxes d'àrea local.

Autor: Sergi Tur Badenas

SkoleLinux. Taules d'enrutament



Taula de rutes. Servidor Principal (standalone)

Destí	Següent host	Mascara	NIC
10.0.2.0	*	255.255.254.0	eth0
*	gateway.intern (10.0.2.1)	0.0.0.0	eth0

Taula de rutes. Servidor Clients lleugers

Destí	Següent host	Mascara	NIC
192.168.0.0	*	255.255.255.0	eth1
10.0.2.0	*	255.255.254.0	eth0
*	gateway.intern (10.0.2.1)	0.0.0.0	eth0

*	ltspserver.intern (192.168.0.254)	0.0.0.0	eth0

Autor: Sergi Tur Badenas

Estat de la xarxa. Ports i sockets

Estat de la xarxa. Ports i sockets

Autor: Sergi Tur Badenas

Netstat

- **Característiques:**
  - Netstat és una eina de línia de comandes que mostra una llista de les connexions de xarxa actives tant d'entrada com de sortida.
  - A windows tenim una comanda semblant amb el mateix nom.
- **Exemple**

```
sudo netstat --inet -lp
Password:
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 *:nfs                   *:*                     LISTEN      -
tcp        0      0 localhost.localdo:39746 *:*                     LISTEN      4747/hpiod
tcp        0      0 *:ldap                  *:*                     LISTEN      4810/slapd
tcp        0      0 *:smux                  *:*                     LISTEN      5382/snmpd
tcp        0      0 localhost.localdo:mysql *:*                     LISTEN      5092/mysqld
tcp        0      0 *:netbios-ssn           *:*                     LISTEN      5374/smbd
tcp        0      0 *:5900                  *:*                     LISTEN      5711/vino-server
tcp        0      0 localhost.localdo:56365 *:*                     LISTEN      4770/python
tcp        0      0 *:9999                  *:*                     LISTEN      4858/approx
tcp        0      0 *:sunrpc                *:*                     LISTEN      3853/portmap
tcp        0      0 *:x11                   *:*                     LISTEN      4706/X
tcp        0      0 *:626                   *:*                     LISTEN      5532/rpc.statd

                                                .....................
```


Autor: Sergi Tur Badenas

Netstat

Utilitats

- Conèixer els ports que tenim disponibles d'una màquina.
- Gestió de la seguretat.
- Exemple: Detectar les aplicacions que està utilitzant un port en concret
- Resolució de conflictes amb ports
- Altres

Autor: Sergi Tur Badenas

Analitzadors de xarxa

Eines per l'anàlisi de xarxes i/o protocols (Packet sniffers o Ethernet sniffers)

Autor: Sergi Tur Badenas

TCPDUMP

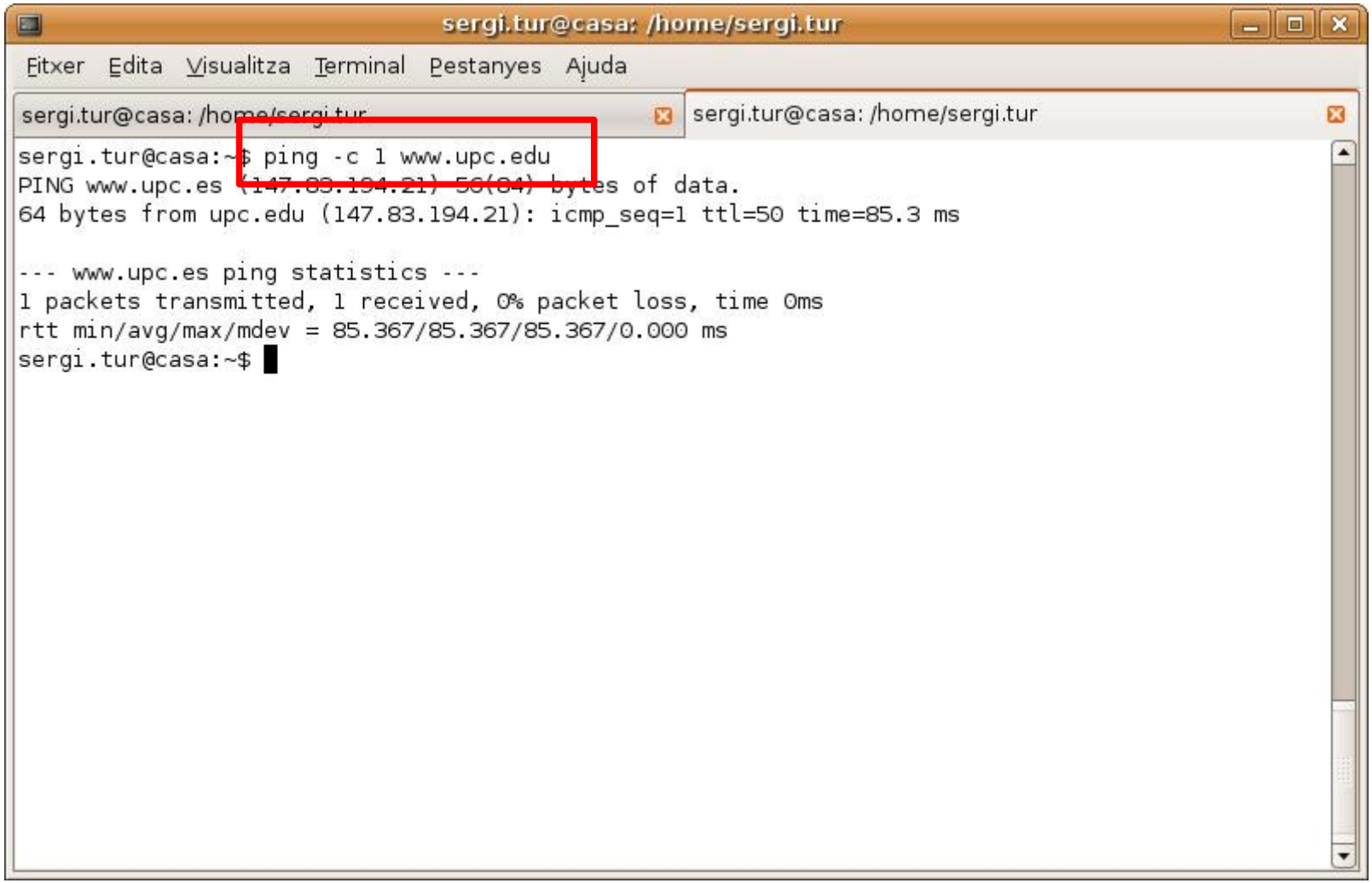
Característiques:

- tcpdump és una eina de línia de comandes que permet analitzar el tràfic de xarxa en temps real.
- Disposa de filtres.
- És necessari tenir privilegis de superusuari (root) per utilitzar tcpdump.
- Ethernet és un medi compartit. Si es volen capturar tots els paquets de la xarxa encara que no estiguin destinats al nostre host hem d'activar el mode promiscu.
- En entorns Windows hi ha un clon anomenat **WinDump**.

Autor: Sergi Tur Badenas

TCPDUMP (II)

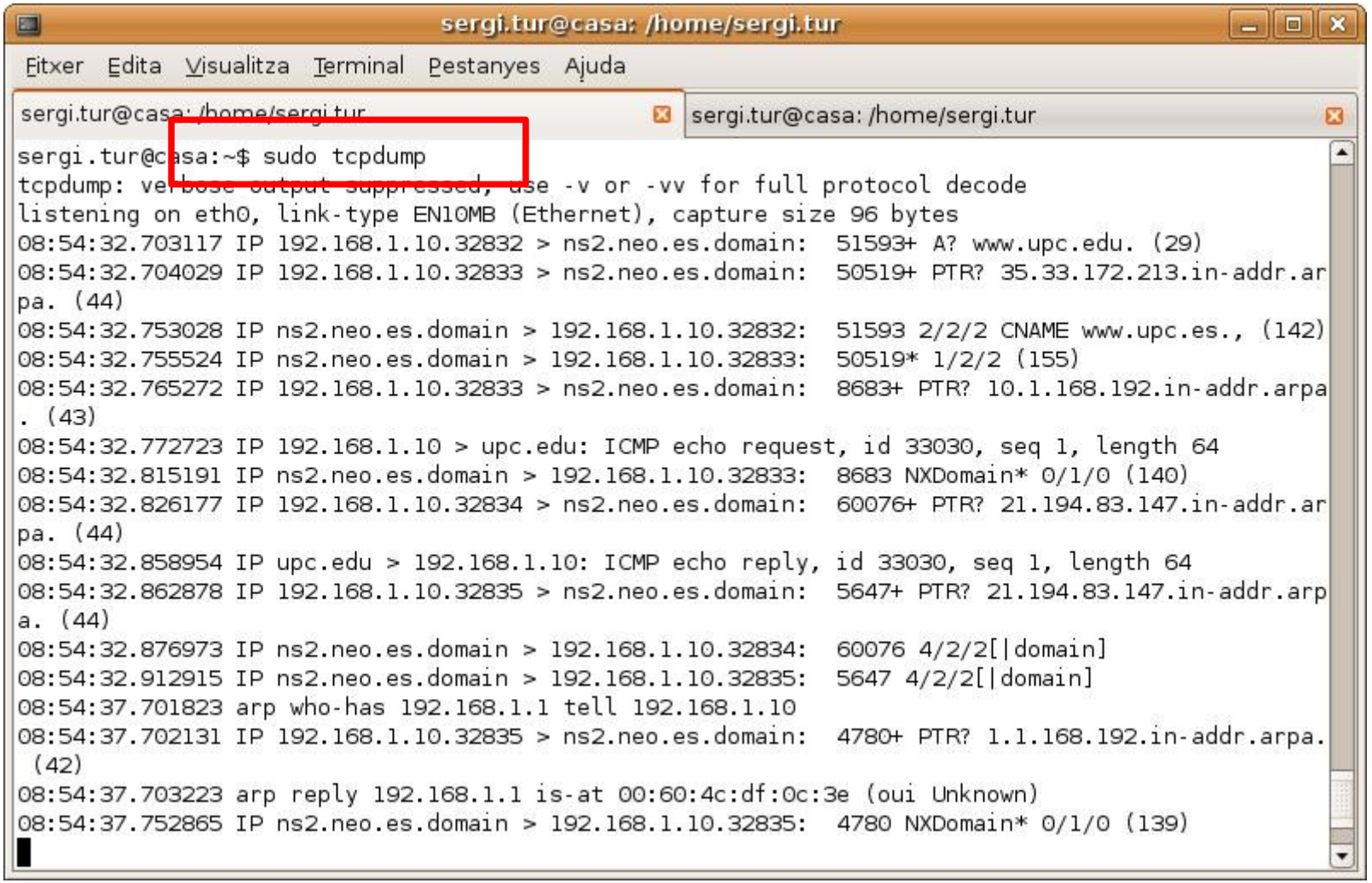
Exemple. Captura d'un ping



Autor: Sergi Tur Badenas

TCPDUMP (III)

Exemple. Captura d'un ping



Autor: Sergi Tur Badenas

TCPDUMP (IV)

Utilitats:

- Per depurar aplicacions que utilitzen la xarxa per comunicar-se. Per exemple es pot utilitzar per comprovar el funcionament d'un tallafocs.
- Per depurar la xarxa mateixa.
- Per comprovar quan la NIC està transmetent o reben dades.
- Per capturar i llegir dades enviades per altres usuaris o ordinadors. Un usuari que té el control d'un enrutador pel qual circula tràfic pot obtenir la informació que no viatgi xifrada.

Autor: Sergi Tur Badenas

TCPDUMP (V)

Paquets necessaris

- tcpdump

Referències

- man tcpdump
- Article de la wikipedia
- Pàgina oficial de tcpdump

Altres enllaços

- WinDump
- Article de la wikipedia sobre Paquet Sniffers

Autor: Sergi Tur Badenas

Ethereal

Característiques:

- Ethereal és un analitzador de protocols utilitzat per analitzar i solucionar problemes de xarxes de comunicacions.
- És similar a tcpdump però amb una interfície gràfica i moltes opcions extres d'organització i filtratge de la informació.
- Com tcpdump, és codi obert i està disponible per gairebé totes les plataformes (UNIX/LINUX, MAC OS i Windows).

Autor: Sergi Tur Badenas

Ethereal

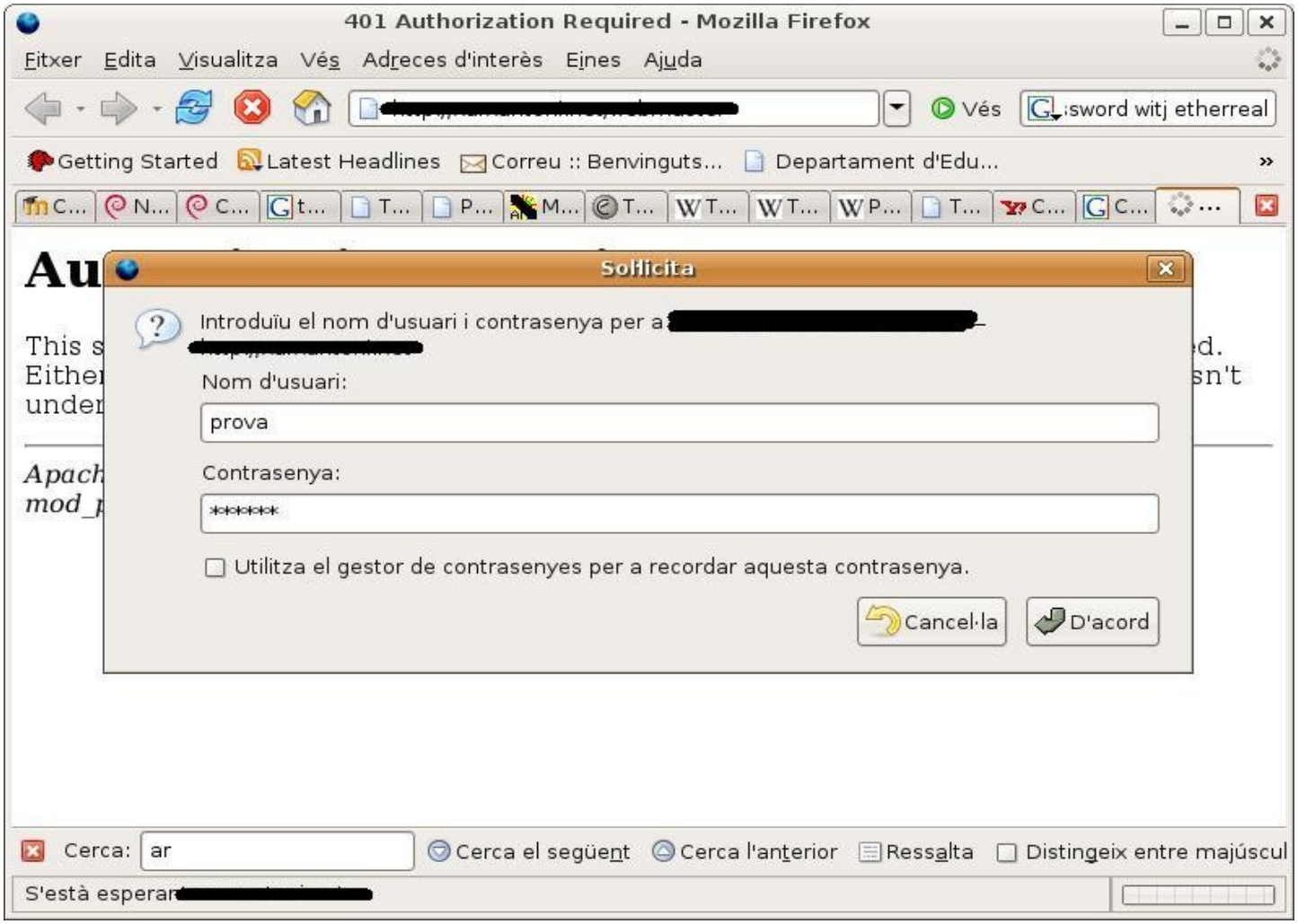
Utilitats:

- Anàlisi i solució de problemes en xarxes de comunicacions.
- Desenvolupament de software i protocols.
- Eina didàctica per a l'educació que permet visualitzar el comportament de diferents protocols i veure els paquets i trames concrets que s'utilitzen.

Autor: Sergi Tur Badenas

Ethereal

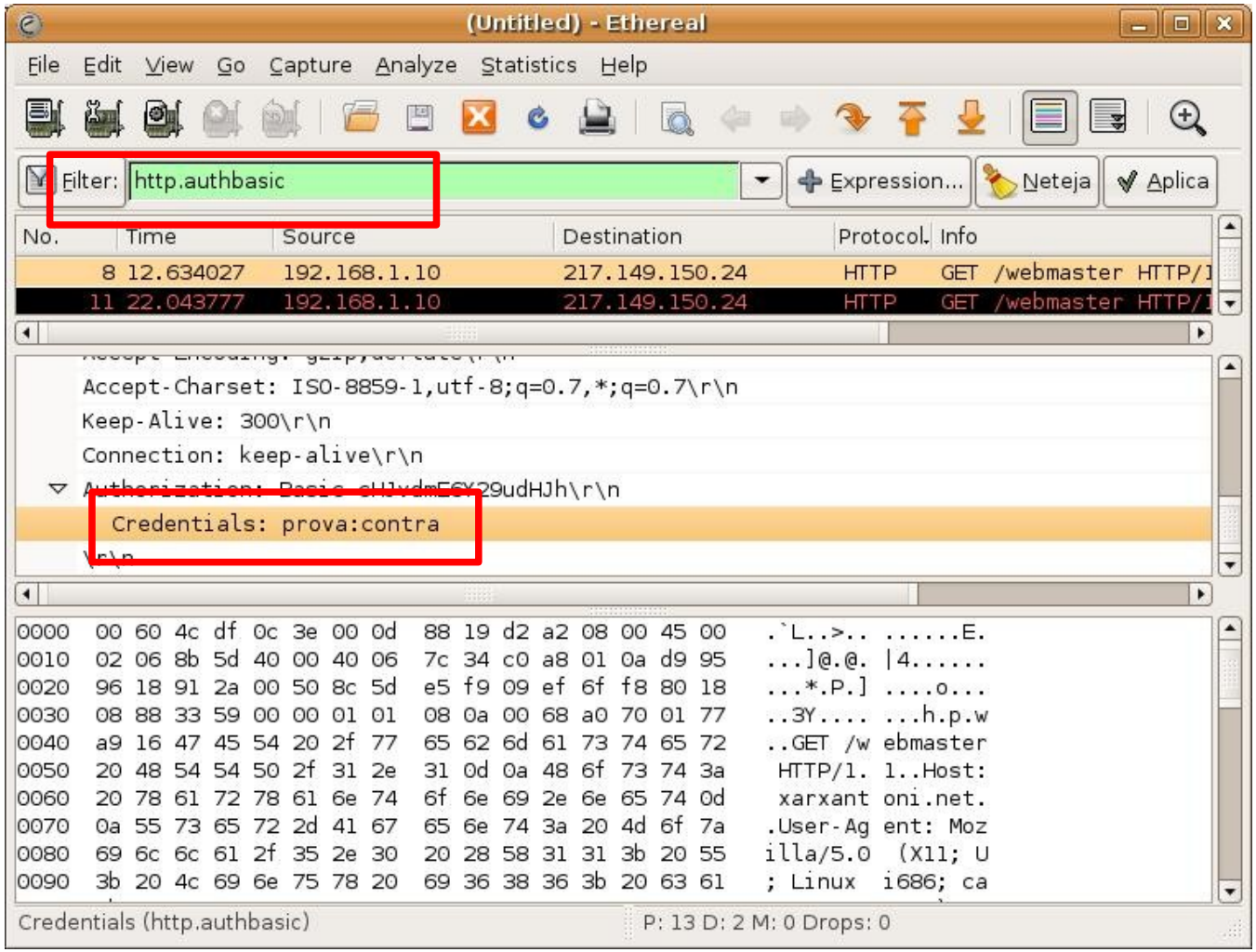
Exemple. Captura paraula de pas web.



Autor: Sergi Tur Badenas

Ethereal

Exemple. Captura paraula de pas web.



Autor: Sergi Tur Badenas

Ethereal

Paquets necessaris

- ethereal

Referències

- man tcpdump
- Article de la wikipedia
- Pàgina oficial de tcpdump

Altres enllaços

- WinDump
- Article de la wikipedia sobre Paquet Sniffers

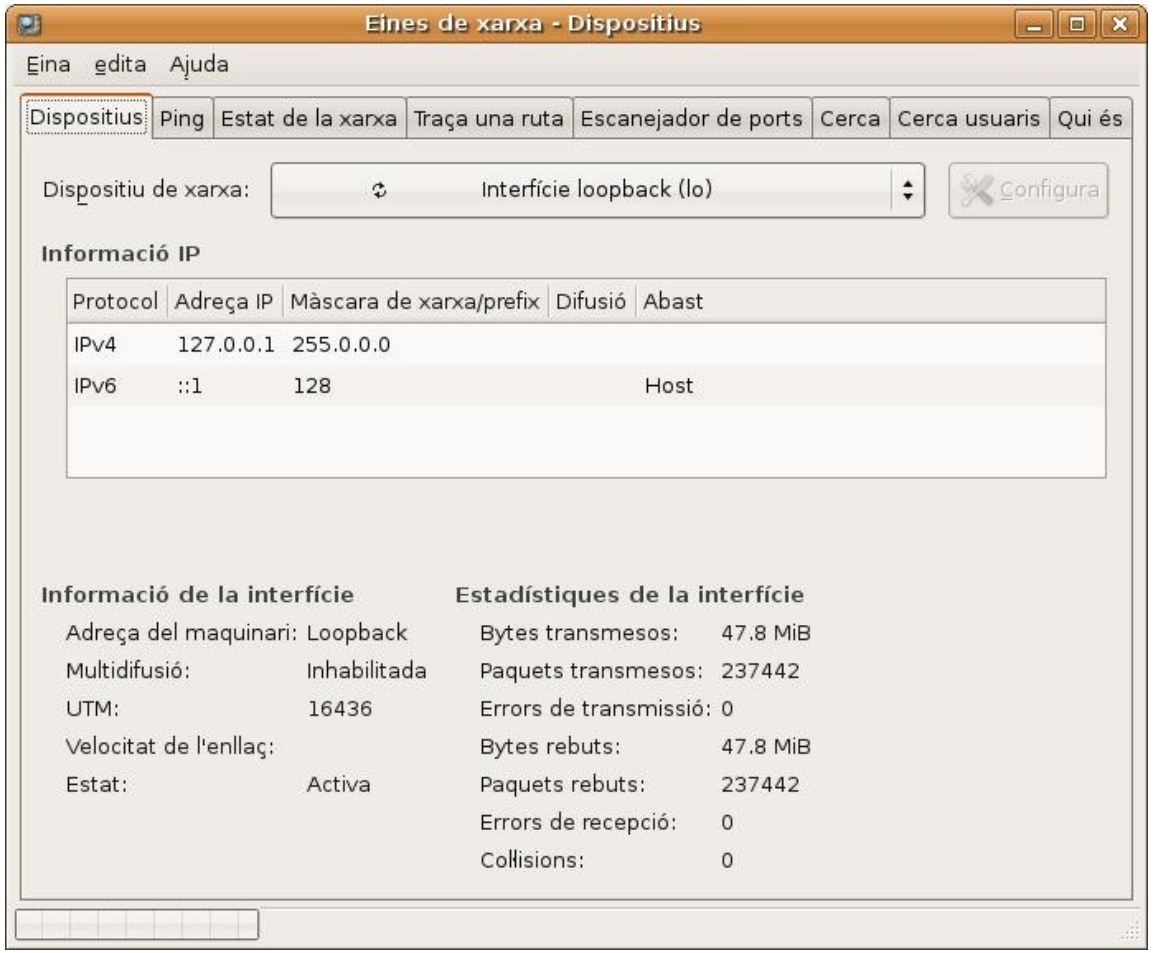
Autor: Sergi Tur Badenas

Eines gràfiques de configuració de la xarxa
Net-Tools

Autor: Sergi Tur Badenas

Gnome-Neetool

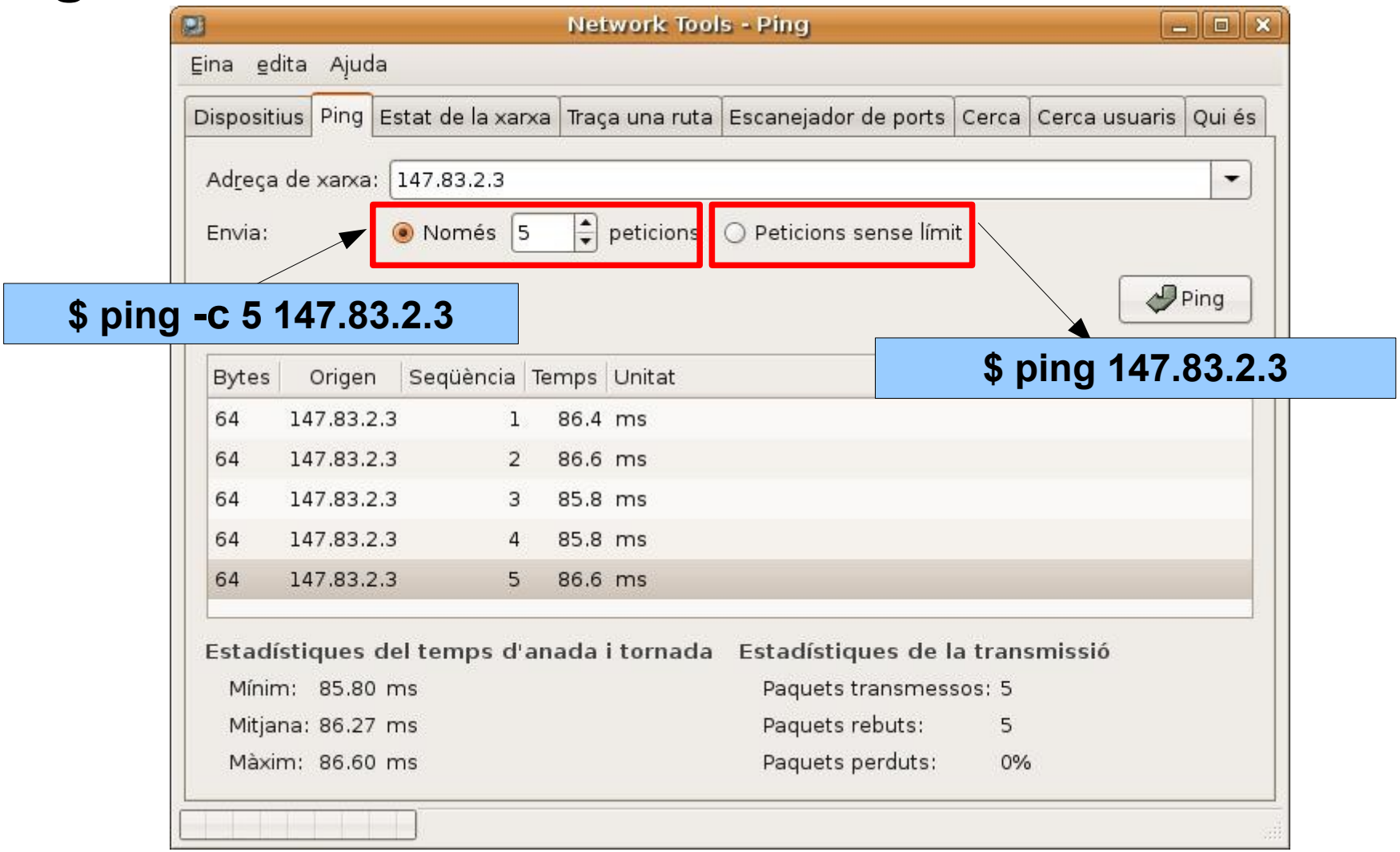
Configuració de dispositius:



Autor: Sergi Tur Badenas

Gnome-Neetool

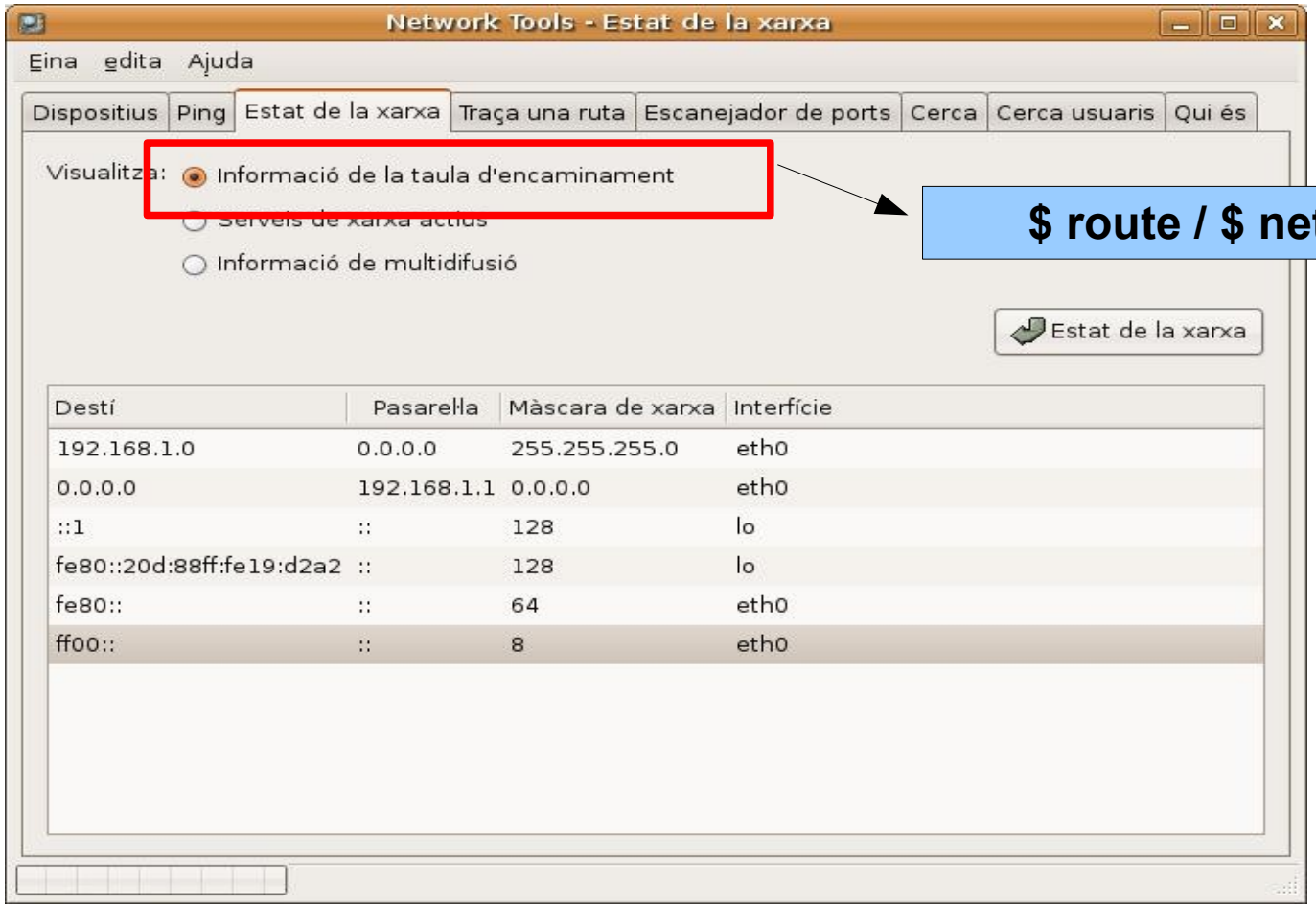
Ping:



Autor: Sergi Tur Badenas

Gnome-Neetool

Encaminament:

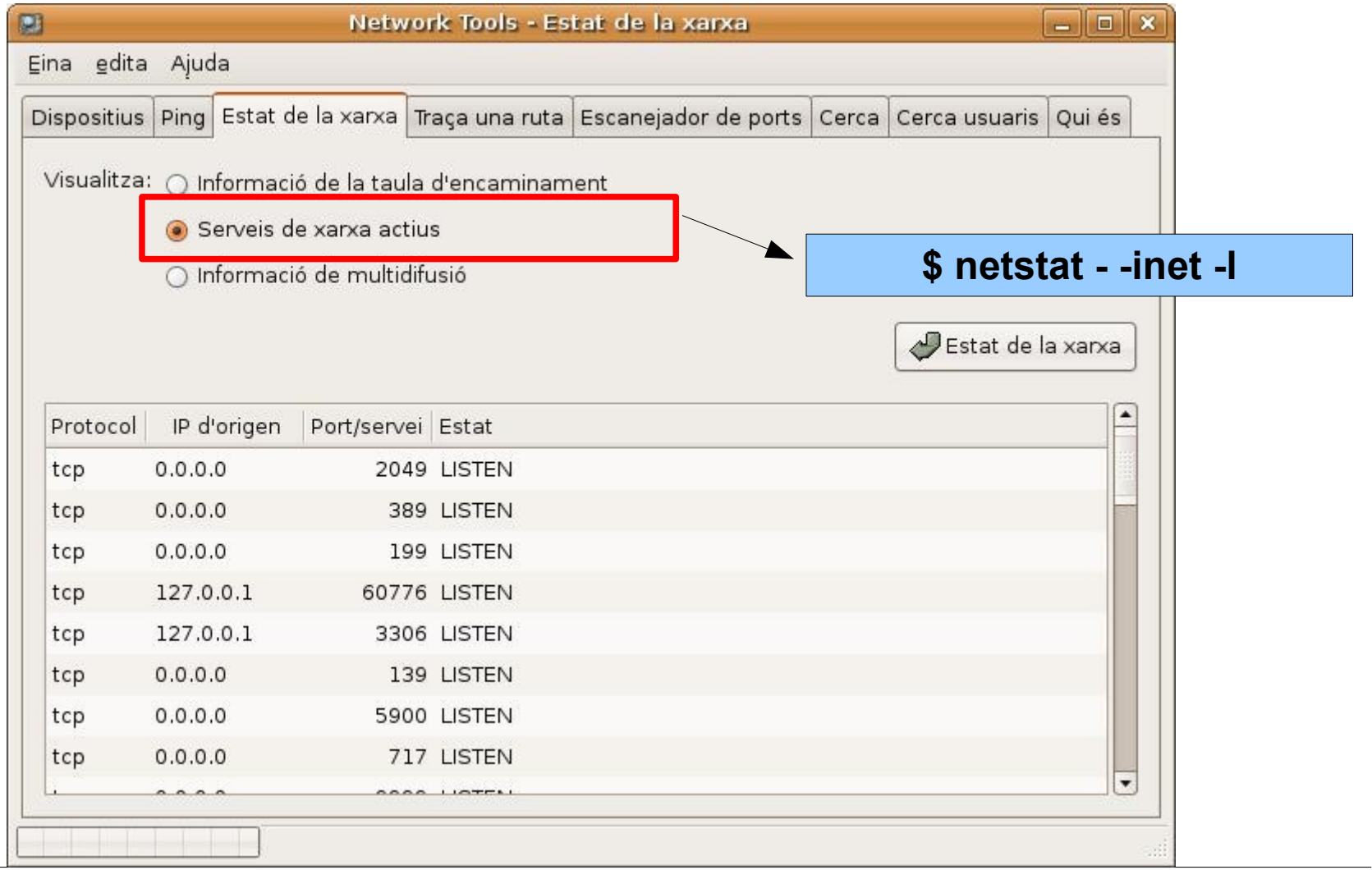


$ route / $ netstat -r

Autor: Sergi Tur Badenas

Gnome-Neetool

Estat de les connexions de xarxa:

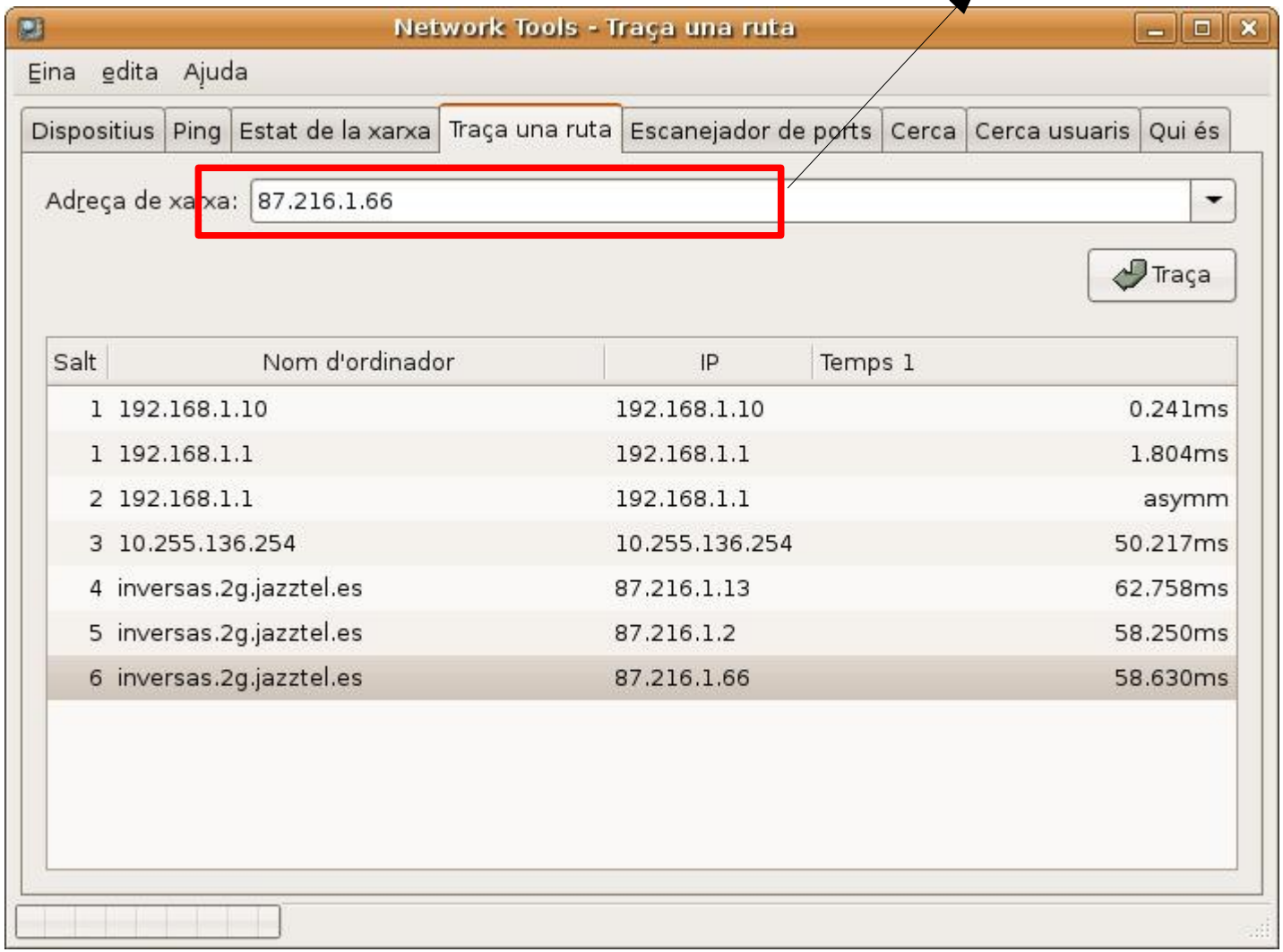


Autor: Sergi Tur Badenas

Gnome-Neetool

Traçar una ruta:

$ traceroute 87.216.1.66

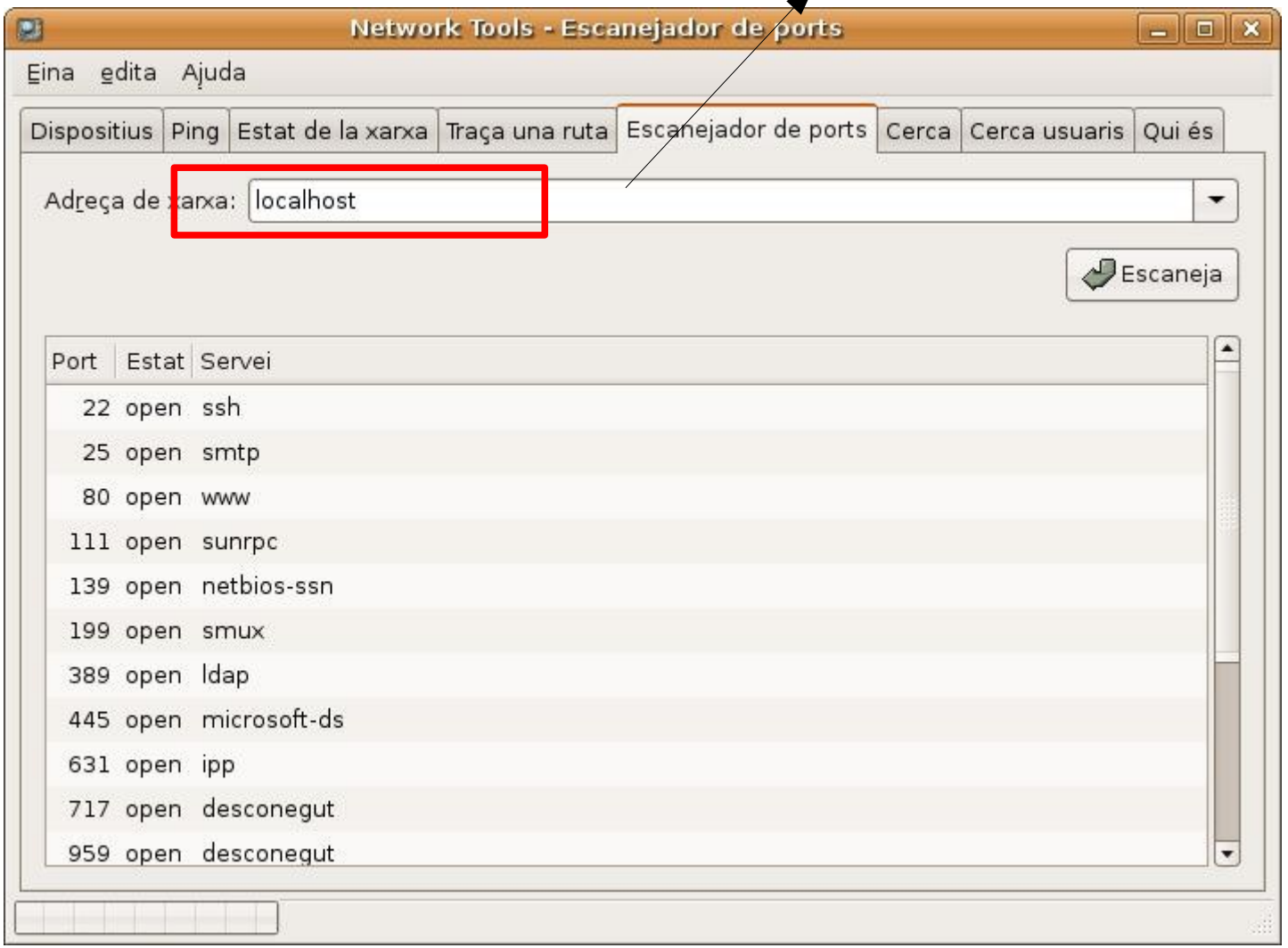


Autor: Sergi Tur Badenas

Gnome-Neetool

Escànner de ports:

$ nmap localhost

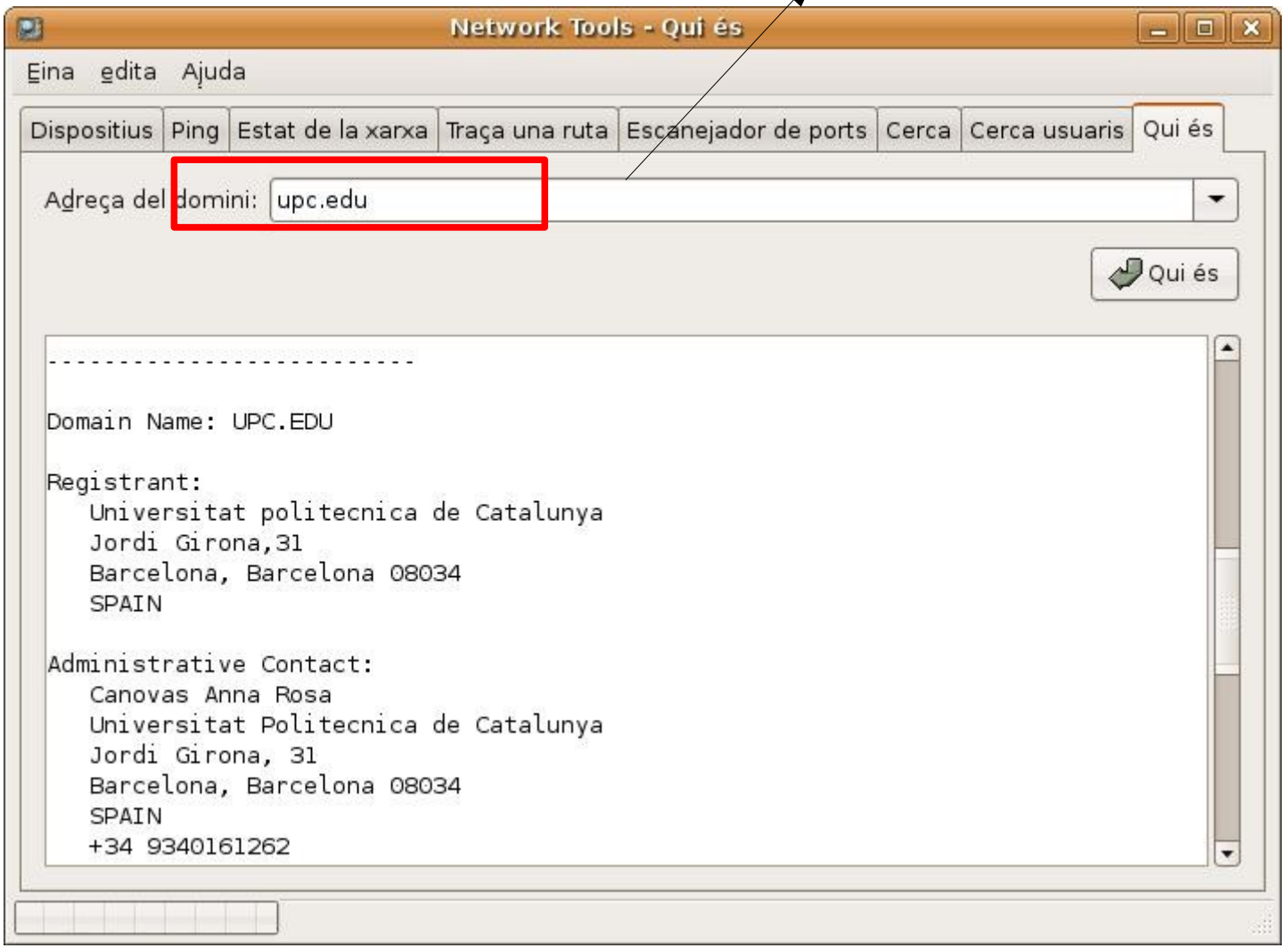


Autor: Sergi Tur Badenas

Gnome-Neetool

Servei Whois:

$ whois upc.edu



Autor: Sergi Tur Badenas

Llicència Creative Commons

creative commons

COMMONS DEED

Reconeixement-CompartirIgual 2.5

Sou lliure de:

- copiar, distribuir i comunicar públicament l'obra
- fer-ne obres derivades
- fer un ús comercial de l'obra

Amb les condicions següents:

Reconeixement. Heu de reconèixer els crèdits de l'obra de la manera especificada per l'autor o el llicenciador.

Compartir amb la mateixa llicència. Si altereu o transformeu aquesta obra, o en genereu obres derivades, només podeu distribuir l'obra generada amb una llicència idèntica a aquesta.

- Quan reutilitzeu o distribuïu l'obra, heu de deixar ben clar els termes de la llicència de l'obra.
- Alguna d'aquestes condicions pot no aplicar-se si obteniu el permís del titular dels drets d'autor.

Els drets derivats d'usos legítims o altres limitacions reconegudes per llei no queden afectats per l'anterior

Això és un resum fàcilment llegible del text legal (la llicència completa).

Advertiment

http://creativecommons.org/licenses/by-sa/2.5/es/

Autor: Sergi Tur Badenas