



Protocols de xarxes UNIX

Protocols de xarxes en UNIX, GNU/Linux. Utilitats per als sistemes amb protocols TCP/IP





Introducció

♦ GNU/Linux

- ♦ Els sistemes GNU/Linux/UNIX estan pensats des dels 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.



Índex

- ♦ **Configuració de dispositius de xarxa. Comandes, protocols i aplicacions.**
 - ♦ ifconfig i fitxers de configuració de xarxa
 - ♦ Configuració de nodes de xarxa
 - ♦ Configuració de xarxes wireless
 - ♦ Protocol DHCP
 - ♦ Protocol DNS
 - ♦ Encaminament
- ♦ **Monitorització bàsica de la xarxa. Comandes, protocols i aplicacions.**
 - ♦ Estat de la xarxa, serveis i ports. Netstat i nmap
 - ♦ Analitzadors de xarxes. Tcpdump i ethereal
 - ♦ Eines gràfiques: Net-tools, EtherApe



Consideracions prèvies

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





Organitzadors previs

♦ Coneixements:

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

♦ Recursos:

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



Instal·lació de paquets Debian

♦ Pre-instal·lació

- ♦ Cal comprovar si ja es disposa del paquet:
 - `$ 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`

♦ 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.



Instal·lació de paquets Debian

♦ Desinstal·lació

- ♦ \$ sudo apt-get remove etherreal
- ♦ 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.

♦ Recursos

- ♦ [APT i DPKG a la wiki del curs](#)
- ♦ [Synaptic a la wiki del curs](#)



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`

`o`

`$ which ifconfig`

♦ Path de les comandes

- ♦ També és possible que en alguns casos les comandes no estiguin en el path de l'usuari i/o que només el superusuari hi tingui accés. En aquest cas cal utilitzar la ruta completa i/o accedir al sistema com a superusuari.



Configuració dels dispositius de xarxa

Comandes, protocols i aplicacions per la configuració dels dispositius de xarxa





Configuració IP de nodes de xarxa

♦ **Paràmetres necessaris per configurar un paràmetre de xarxa**

♦ Paràmetres imprescindibles

- **Adreça IP**
- **Màscara de xarxa**

♦ Paràmetres “opcionals”

- **Porta d'enllaç**
- **Servidors de DNS**

♦ Altres paràmetres

- **Adreça de difusió, adreça de xarxa, adreça MAC**

Aquests paràmetres no són imprescindibles per tal que una màquina és pugui comunicar amb altres màquines de la mateixa xarxa!



Paràmetres de xarxa

♦ Paràmetres de xarxa

♦ ifconfig

- **Adreça IP.** Adreça lògica del protocol IP. Nivell de xarxa (Nivell 3 OSI). Protocol IP.
- **Adreça MAC.** Adreça física. Assignada a la NIC. Nivell MAC (Nivell 2 OSI). Protocol ARP.
- **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**.



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, sistemes virtuals, etc.).
- ♦ En Windows la comanda anàloga és **ipconfig**.



ifconfig

♦ 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**, ...
- **vmnet0**, **vmnet1**, **vmnet8**: Interfícies virtuals vmware.



ifconfig

◆ Example:

Primera NIC

```
$ /sbin/ifconfig
eth0      HWaddr 00:0D:88:19:52:12
          IP de la NIC
          .1.10 Broadcast:192.168.1
          255.255.255.0
          inet6 addr: fe80::20d:88ff:fe19:d2a2/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:957270 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1254234 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:581767799 (554.8 M
          MiB)
          Interrupt:11 Base address:0x4000
lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:799643 errors:0 dropped:0 overruns:0 frame:0
          TX packets:799643 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:164196675 (156.5 MiB)  TX bytes:164196675 (156.5
          MiB)
```

Adreça MAC

Adreça de unió

HWaddr 00:0D:88:19:52:12

IP de la NIC

Interfície de loopback



ifconfig

◆ Paquet necessari

- ◆ net-tools

◆ Referències

- ◆ man ifconfig
- ◆ Article de la wikipedia

◆ Altres enllaços

- ◆ Exemples ifconfig
- ◆ http://xarxantoni.net:8080/mediawiki/index.php/Xarxes_Linux#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



Adreces IP

♦ Protocol Ipv4

- ♦ Estan formades per 32 Bits i permeten adreçar una mica menys de 4300 milions de màquines.
- ♦ El format més comú és el decimal amb punts.

207.142.131.235 correspon als 32 bits:
11001111.10001110.10000011.11101011

Les adreces IP identifiquen de forma unívoca un node dins d'una xarxa concreta

♦ Altres notacions

Notation	Value
Dot-decimal notation	207.142.131.235
Dotted Hexadecimal	0xCF.0x8E.0x83.0xEB
Dotted Octal	0317.0216.0203.0353
Hexadecimal	0xCF8E83EB
Decimal	3482223595
Octal	031743501753



Adreces IP

♦ Conversió d'adreces IPv4 a binari

- ♦ Hi ha una eina anomenada **ipcalc** que ens permet fer operacions amb adreces IP.

An IPv4 address (dotted-decimal notation)

172 . 16 . 254 . 1
 ↓ ↓ ↓ ↓
 10101100.00010000.11111110.00000001
 └───┬───┬───┬───┘
 One byte = Eight bits
 └──────────────────────────────────┘
 Thirty-two bits (4 * 8), or 4 bytes

♦ Conversió d'adreces IPv6 a binari

An IPv6 address (in hexadecimal)

2001:0DB8:AC10:FE01:0000:0000:0000:0000

↓ ↓ ↓ ↓ └──────────┘
2001:0DB8:AC10:FE01:: Zeroes can be omitted

└───┬───┬───┬───┘
 1000000000000001:0000110110111000:1010110000010000:1111111000000001:
 0000000000000000:0000000000000000:0000000000000000:0000000000000000



Màscara de xarxa

- ♦ **La màscara determina quins bits estan reservats a la xarxa i quins bits a les màquines.**

- ♦ La màscara més utilitzada és la màscara:

255.255.255.0

11111111.11111111.11111111.00000000

- ♦ Tenen el format de les adreces IP però no tots els valors són possibles
- ♦ En format binari, la màscara ha de tenir tots els uns junts i al principi, seguit d'un sèrie de zeros.
 - Només són vàlides les màscares que tenen els valors:
255, 254, 252, 248, 240, 224, 192, 128



Màscara de xarxa

♦ Per que tenen aquest format les màscares de xarxa?:

- ♦ Els bits de l'esquerre, marcats amb uns (1) s'utilitzen per indicar la xarxa
- ♦ Els bits de la dreta, marcats amb ceros (0) s'utilitzen per identificar un host dins d'una xarxa concreta

Decimal	Binari
128	10000000
192	11000000
224	11100000
240	11110000
248	11111000
252	11111100
254	11111110
255	11111111

♦ Exemples

- ♦ **Aula 1:** Totes les adreces IP comencen per 192.168.201 (màscara 255.255.255.0)
- ♦ **Aula 4:** Totes les adreces IP comencen per 192.168.204 (màscara 255.255.255.0)



Màscara de xarxa

♦ La màscara 255.255.255.0:

- ♦ Ens indica que estem a una xarxa de 254 màquines
- ♦ Ens indica quines adreces IP són de la nostra xarxa
- ♦ Hi ha una adreça màxima i una adreça mínima dins de la xarxa

```
$ ipcalc 192.168.201.0/255.255.255.0
Address: 192.168.201.0      11000000.10101000.11001100. 00000000
Netmask: 255.255.255.0 = 24 11111111.11111111.11111111. 00000000
Wildcard: 0.0.0.255        00000000.00000000.00000000. 11111111
=>
Network: 192.168.201.0/24   11000000.10101000.11001100. 00000000
HostMin: 192.168.201.1     11000000.10101000.11001100. 00000001
HostMax: 192.168.201.254   11000000.10101000.11001100. 11111110
Broadcast: 192.168.201.255 11000000.10101000.11001100. 11111111
Hosts/Net: 254              Class C, Private Internet
```



Màscara de xarxa

▶ AULA 1

	Network (N) / Hosts (H)	NNNNNNNN.NNNNNNNN.NNNNNNNN.HHHHHHHH
MÀSCARA :	255.255.255.0 /	11111111.11111111.11111111.00000000
IP xarxa:	192.168.201.x /	11000000.10101000.11001001.00000000
Màquina1:	192.168.201.1 /	11000000.10101000.11001001.00000001
Màquina2:	192.168.201.2 /	11000000.10101000.11001001.00000010
Màquina3:	192.168.201.3 /	11000000.10101000.11001001.00000011
Màquina4:	192.168.201.4 /	11000000.10101000.11001001.00000100
Màquina5:	192.168.201.5 /	11000000.10101000.11001001.00000101
Màquina6:	192.168.201.6 /	11000000.10101000.11001001.00000110
Màquina7:	192.168.201.7 /	11000000.10101000.11001001.00000111
Màquina8:	192.168.201.8 /	11000000.10101000.11001001.00001000
Màquina9:	192.168.201.9 /	11000000.10101000.11001001.00001001
.....
Màqui252:	192.168.201.250/	11000000.10101000.11001001.11111010
Màqui252:	192.168.201.251/	11000000.10101000.11001001.11111011
Màqui252:	192.168.201.252/	11000000.10101000.11001001.11111100
Màqui252:	192.168.201.253/	11000000.10101000.11001001.11111101
Màqui252:	192.168.201.254/	11000000.10101000.11001001.11111110
Màqui255:	192.168.201.255/	11000000.10101000.11001001.11111111



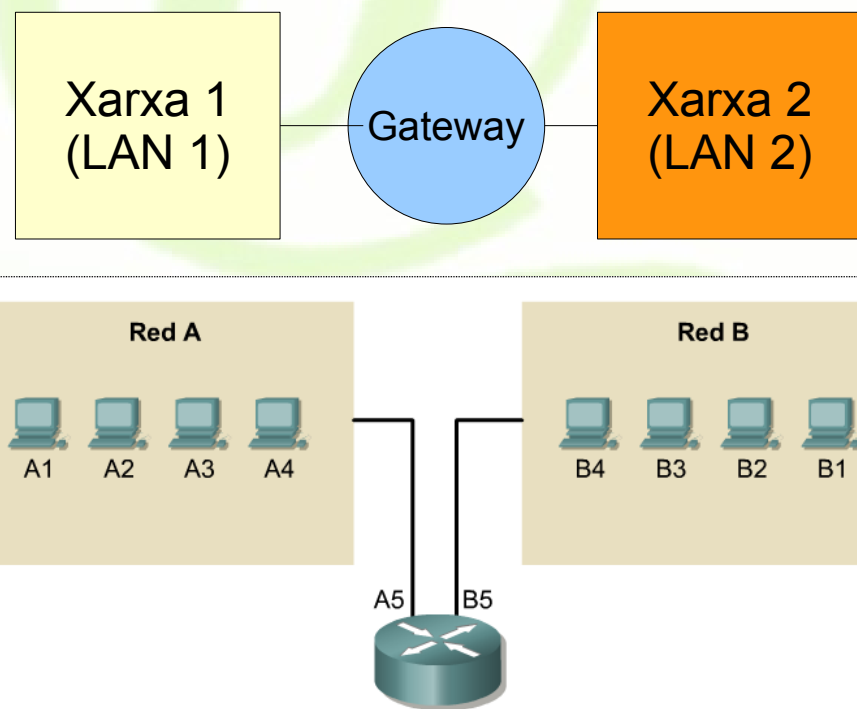
Porta d'enllaç

♦ Gateway/Pasarel·la/Router/Encaminador

- ♦ Té múltiples noms però la seva definició és:

La porta d'enllaç és el node de la xarxa local que ens permet connectar-nos a una altra xarxa

- ♦ Pot ser el router ADSL que ens dona accés a Internet, un router que ens connecta a la xarxa del centre, l'IPCOP de l'aula, etc.





Servidors de DNS

- ♦ **Són una eina per facilitar l'ús de la xarxa**
 - ♦ Ens permeten treballar a un nivell més humà (o menys de màquina) i treballar amb noms en comptes d'adreces IP
 - ♦ Per tal de treballar amb noms de màquina, hem d'utilitzar un servidor de DNS que s'encarregarà de traduir els noms en adreces IP.
 - ♦ No és imprescindible. Per exemple si s'espalla el DNS del vostre proveïdor d'accés a Internet sempre podeu accedir a la web directament amb la IP.

```
$ ping www.iescopernic.com
PING www.iescopernic.com (80.34.23.149) 56(84) bytes of data.
64 bytes from 149.Red-80-34-23.staticIP.rima-tde.net (80.34.23.149): icmp_seq=1 ttl=252 time=106 ms
64 bytes from 149.Red-80-34-23.staticIP.rima-tde.net (80.34.23.149): icmp_seq=2 ttl=252 time=108 ms
```

<http://80.34.23.149/moodle>



Configuració per línia de comandes de nodes de xarxa

Quan no es disposa d'entorn gràfic (servidors), normalment els passos que cal seguir per configurar la xarxa són una combinació de comandes i d'edicions de fitxers de configuració.

- ♦ En aquest apartat veurem les comandes i els fitxers de configuració bàsics per a configurar nodes de xarxa.
 - **NOTA:** és molt important conèixer la configuració per línia de comandes per què sovint és l'única opció que tenim. També cal dir que totes les eines gràfiques acaben utilitzant aquestes comandes i/o fitxers de configuració.
- ♦ **Pàgines de consulta/referència**
 - ♦ Comandes de xarxa
 - ♦ Fitxers de configuració
 - ♦ Paquets de xarxa



Comandes de xarxa

- ♦ **Consulta i configuració de les interfícies**
 - ♦ ifconfig, iwconfig
- ♦ **Consulta de la taula de rutes i de la passarel·la**
 - ♦ route
- ♦ **Consulta dels paràmetres de xarxa**
 - ♦ ipcalc
- ♦ **Comandes per apagar i encendre interfícies**
 - ♦ ifup, ifdown, dhclient
- ♦ **Comprovació de xarxes i altres comandes**
 - ♦ ping, traceroute, host, arp, netstat, ip, tracepath, nslookup, dnstracer, nmap, tcpdump, whois, iptables, etc.



Fitxers de configuració

♦ Interfícies de xarxa

- ♦ Fitxer /etc/network/interfaces

♦ Resolució de noms DNS.

- ♦ Fitxer /etc/resolv.conf
- ♦ Fitxer /etc/hosts
- ♦ Fitxer /etc/host.conf

♦ Altres fitxers

- ♦ /etc/networks, /etc/protocols, /etc/services...
- ♦ Veieu l'apartat [Fitxers de configuració](#) a la wiki del professor



Paquets de xarxa

- ♦ **La majoria del programari necessari per a xarxes ja es troba instal·lat:**
 - ♦ net-tools (netbase), ifupifdown, gnome-nettool, dnsutils, iproute, etc.
- ♦ **Altres paquets es poden instal·lar des de els repositoris amb apt-get install:**
 - ♦ nmap, tcpdump, traceroute, dnstracer, wireshark, ipcalc, arpwatch, whois, etc
 - ♦ La imatge de l'aula ja porta instal·lats molts d'aquests paquets.
 - ♦ **Exemple d'instal·lació:** `$ sudo apt-get install whois`



Programari

♦ Paquets necessaris:

- ♦ Paquet net-tools de debian:
 - /sbin/ifconfig
 - /sbin/route
 - /sbin/netstat
 - ♦ Paquet wireless-tols
 - ♦ Paquet netbase
 - ♦ Paquet ifupdown
 - ♦ Paquets iputils-*
 - ♦ Paquet dns-utils
 - /usr/bin/dig
 - /usr/bin/nslookup
 - ♦ Paquet traceroute
 - ♦ Paquet tcpdump
 - ♦ Paquet dnstracer
 - ♦ Paquet nmap
 - ♦ Paquet whois
 - ♦ Paquet ipcalc
- http://xarxantoni.net:8080/mediawiki/index.php/Xarxes_Linux



Configuració per línia de comandes

◆ Configuració estàtica

- ◆ La configuració de cada node de xarxa es realitza de forma manual pels administradors de les màquines i els paràmetres de xarxa “són fixos”.
- ◆ Cal conèixer els paràmetres de la xarxa

◆ Configuració dinàmica (DHCP)

- ◆ La configuració dels nodes de xarxa la realitza de forma automàtica utilitzant un servidor de DHCP. Els paràmetres dels nodes de xarxa poden ser fixos o dinàmics (varien amb el temps)
- ◆ No cal conèixer els paràmetres de la xarxa (el servidor DHCP de la xarxa ens els proporciona)



Configuració per línia de comandes

♦ Passos a seguir per configurar la xarxa

- ♦ Escollir quin tipus de configuració volem: estàtica o dinàmica
- ♦ Si la configuració és estàtica decidir (o preguntar a l'administrador de la xarxa) els 4 paràmetres bàsics de xarxa (IP, Màscara, Passarel·la/Gateway i servidors de DNS)
- ♦ Modificar la configuració de la màquina modificant els **Fitxers de Configuració** adients. **NOTA:** Cal utilitzar un editor de text per línia de comandes
- ♦ Un cop fetes les modificacions:
 - **IMPORTANT:** Cal **executar les comandes** necessàries per que la màquina apliqui la NOVA configuració.



/etc/network/interfaces

♦ Fitxer de configuració principal

```
$ cat /etc/network/interfaces
```

```
# The loopback interface
auto lo
iface lo inet loopback
```

Configuració del 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
```

**Configuració ethernet:
Es configuren tots els paràmetres de
xarxa (configuració estàtica)**

```
auto eth1
iface eth1 inet dhcp
```

**Configuració ethernet del segon
dispositiu de xarxa (configuració DHCP)**

♦ Els fitxers de configuració també tenen manual

`$ man interfaces`



Fitxers de configuració de DNS

- ▶ **/etc/resolv.conf**
- ▶ **/etc/hosts**

```
$ cat /etc/resolv.conf
nameserver 192.168.1.3
nameserver 192.168.1.1
```

```
$ cat /etc/hosts
127.0.0.1    localhost
127.0.1.1    ubuntu-sala
192.168.1.3  acacha.dyndns.org
```

- ▶ **/etc/host.conf**

```
$ cat /etc/host.conf
# The "order" line is only used by old versions of the C library.
order hosts,bind
multi on
```

- ▶ **/etc/hostname**

```
$ cat /etc/hostname
ubuntu-sala
```




Altres distribucions Linux

♦ Altres distribucions Linux

- ♦ `/etc/sysconfig/network/ifcfg-*` (SUSE) amb DHCP

```
$ cat /etc/sysconfig/network/ifcfg-eth0
BOOTPROTO='dhcp'
BROADCAST=""
ETHTOOL_OPTIONS=""
IPADDR=""
MTU=""
NAME='AMD PCnet - Fast 79C971'
NETMASK='255.255.255.0'
NETWORK=""
REMOTE_IPADDR=""
STARTMODE='auto'
UNIQUE='rBUF.weGuQ9ywYPF'
USERCONTROL='no'
_nm_name='bus-pci-0000:00:10.0'
```



Comandes

- ♦ **Per tal que la màquina apliqui els canvis del fitxer de configuració cal executar:**

```
$ sudo /etc/init.d/networking restart
```

- ♦ Aquesta comanda s'executa sola cada cop que iniciu la màquina. Si després es fa algun canvi l'heu d'executar vosaltres mateixos.

- ♦ **També podeu utilitzar les comandes:**

```
$ sudo ifdown ethx  
$ sudo ifup ethx
```

- ♦ On x és el número de la vostra interfície de xarxa
- ♦ La comanda down apaga la interfície de xarxa i la comanda up l'encén

- ♦ **En cas d'utilitzar DHCP també podeu utilitzar:**

```
$ sudo dhclient ethx
```



Editors de text. joe

- ◆ **Necessitareu un editor de text per línia de comandes**

- ◆ **Joe** és l'editor que utilitzo normalment per editar fitxers per línia de comandes.
- ◆ Possiblement cal instal·lar-lo ja que no és un editor que portin les distribucions GNU/Linux per defecte:

```
$ sudo apt-get install joe
```

- ◆ **Iniciar joe:**

```
$ joe nom_del_fitxer_que_voleu_editar
```

- ◆ **Exemple:**

```
$ sudo joe /etc/network/interfaces
```

- ◆ **Ajuda:**

```
<Ctrl> + K + H
```

- ◆ **Sortir i guardar:**

```
<Ctrl> + K + X
```



Pràctica

◆ Configuració d'una Ubuntu Server

- ◆ Màquina virtual Virtual Box
 - Pràctiques de configuració de nodes de xarxa

◆ Guions de detecció d'errors de xarxa

- ◆ Passos per comprovar la xarxa
- ◆ A Moodle trobareu el document:
 - Comprovació errors de xarxa

◆ Tutorial

- ◆ Tutorial pas a pas de configuració de xarxa en Ubuntu



Configuració amb ifconfig

◆ 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

◆ IP Aliasing

- ◆ Es pot configurar una targeta amb més d'una IP
 - `$ sudo ifconfig eth0:1 10.10.10.2 netmask 255.255.255.248`



Gateway. Comanda route

- ♦ **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 temes posteriors.





Configuració gràfica de nodes de xarxa

- La configuració des de el
menú **Administració** i l'opció
Xarxa





Configuració gràfica de nodes de xarxa

♦ Ubuntu

- ♦ La configuració gràfica sempre acabarà modificant els fitxers de configuració
- ♦ Podeu comprovar les modificacions als fitxers
- ♦ Podeu utilitzar l'entorn gràfic per aprendre com funcionen els fitxers de configuració

♦ Exercici

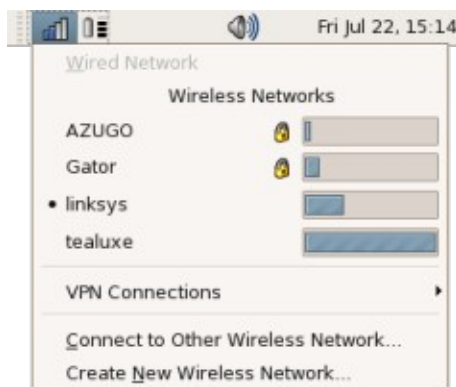
- ♦ Seguiu els passos de la [web del professor](#)





NetworkManager

♦ Aplicació gràfica Gnome



♦ Ús avançat i simple de la xarxa:

- ♦ Canvi de dispositius en calent
- ♦ Roaming entre xarxes wireless
- ♦ Suport WEP i WPA





Eines gràfiques de xarxa

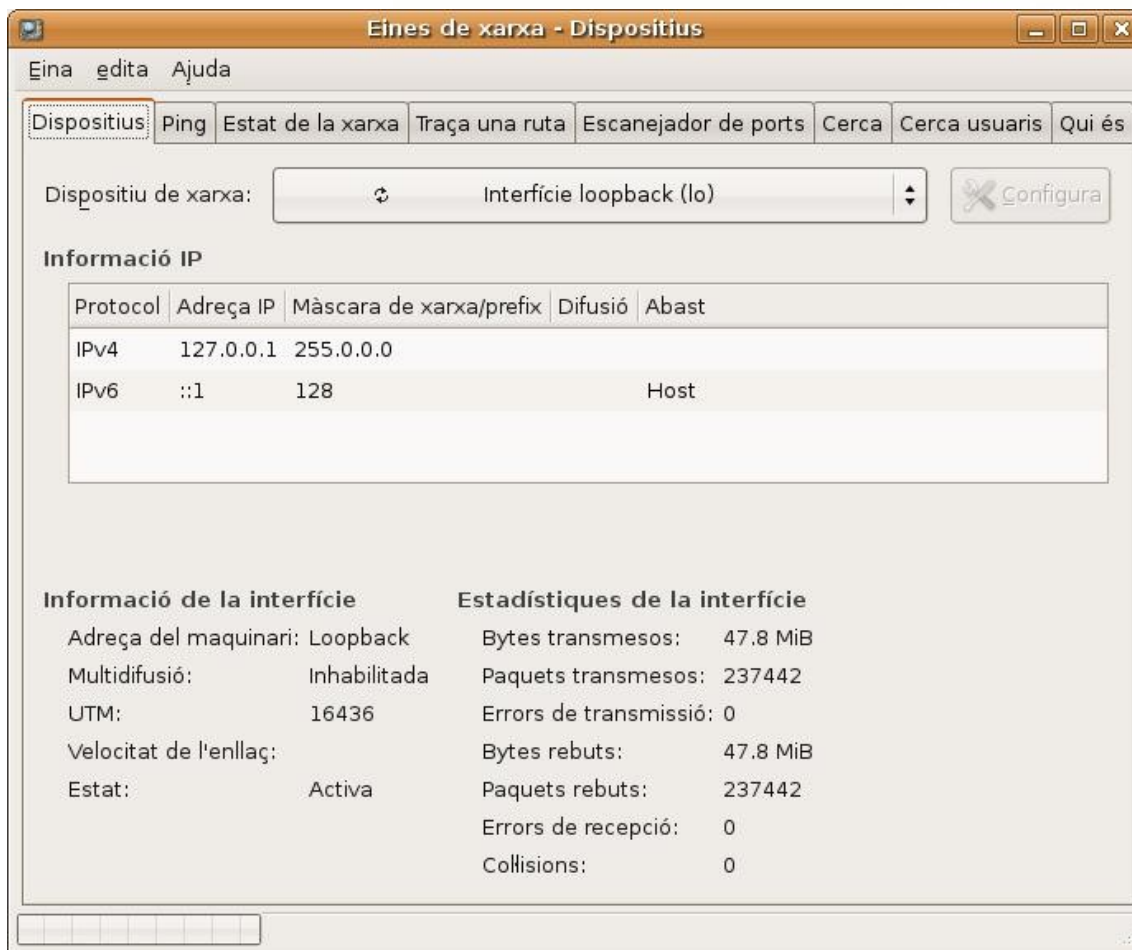
Eines gràfiques de xarxa





Gnome-Neetool

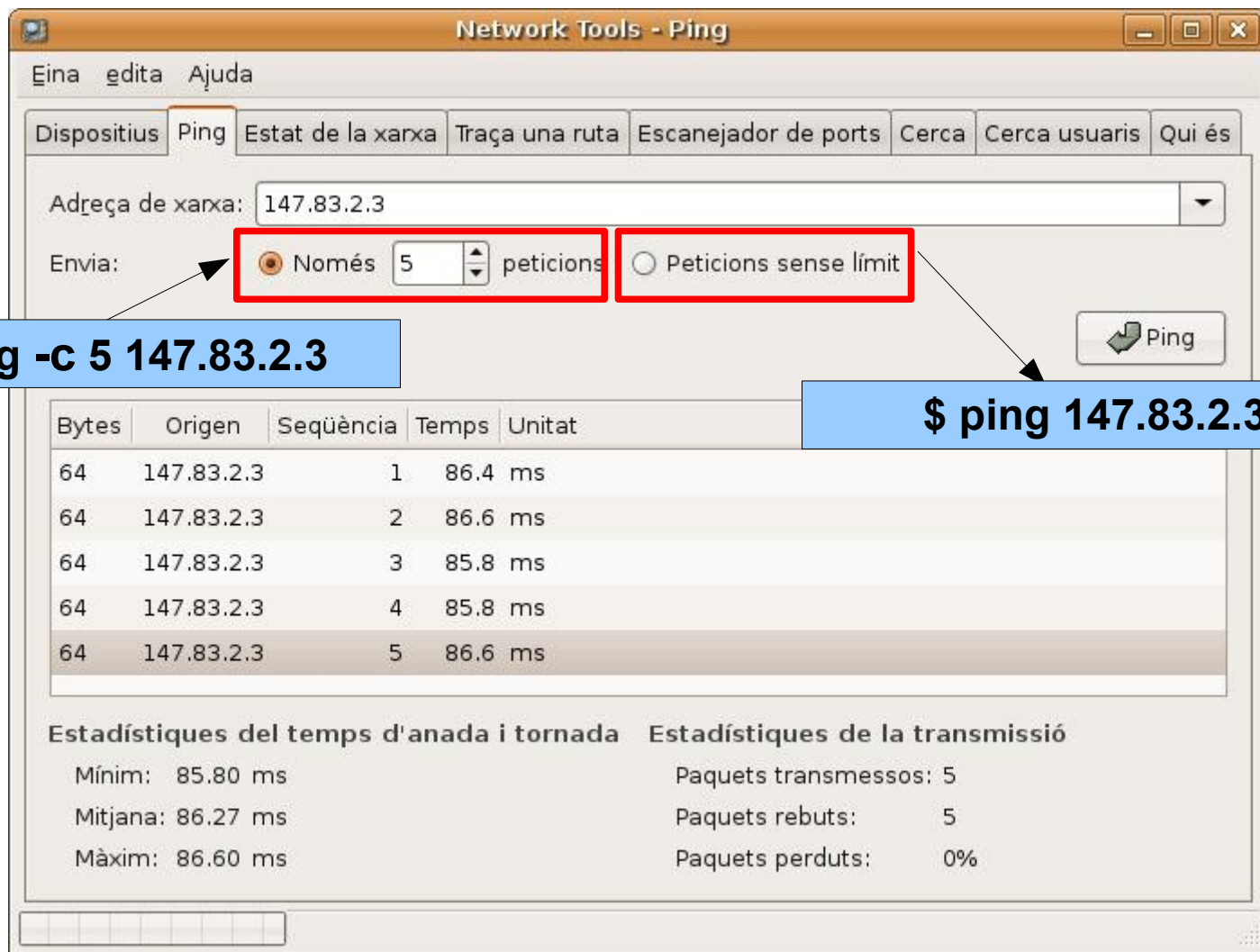
◆ Configuració de dispositius:





Gnome-Neetool

♦ Ping:



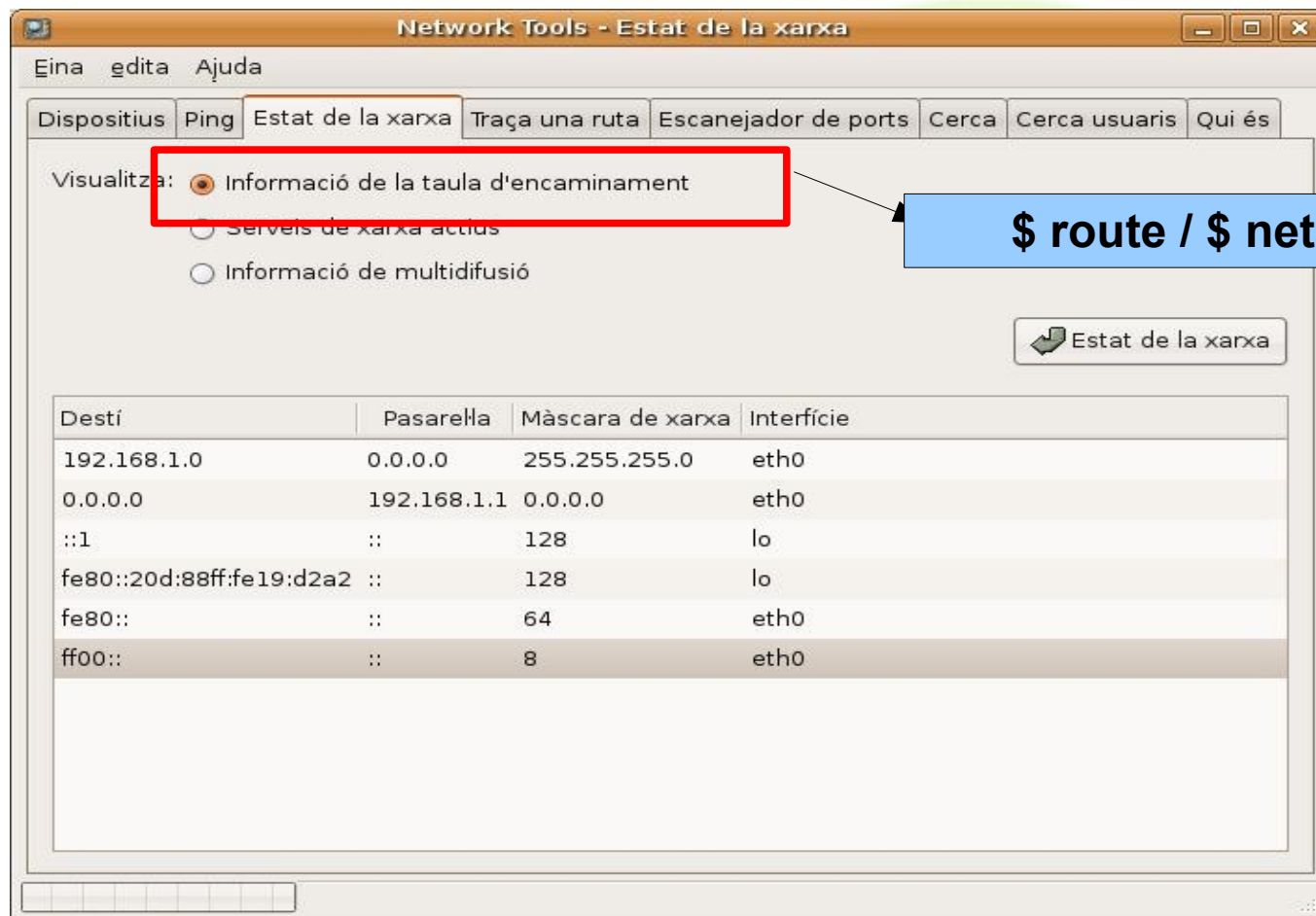
\$ ping -c 5 147.83.2.3

\$ ping 147.83.2.3



Gnome-Neetool

◆ Encaminament:

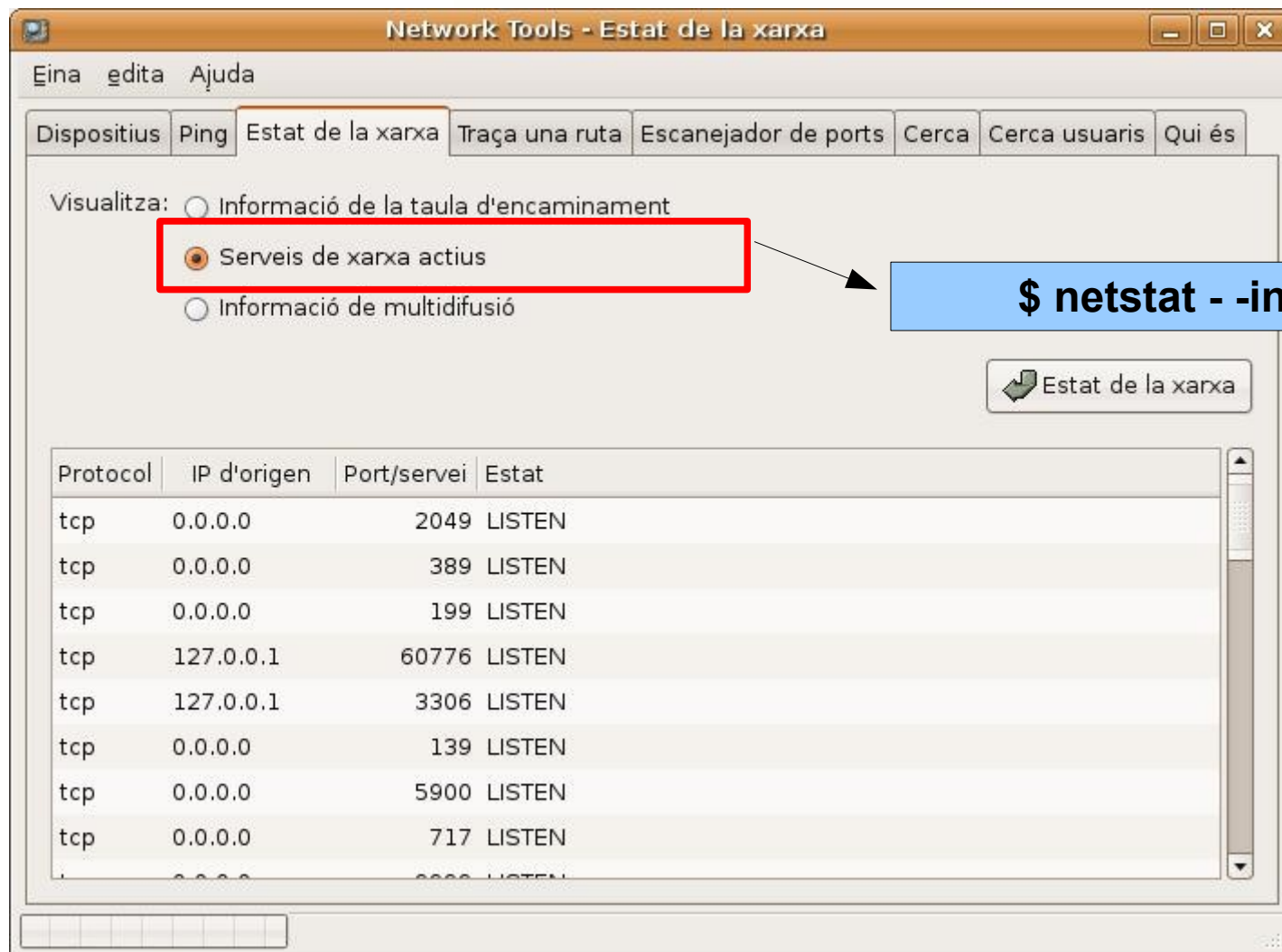


\$ route / \$ netstat -r



Gnome-Neetool

♦ Estat de les connexions de xarxa:





Gnome-Neetool

♦ Traçar una ruta:

\$ traceroute 87.216.1.66

Network Tools - Traça una ruta

Eina edita Ajuda

Dispositius Ping Estat de la xarxa Traça una ruta Escanejador de ports Cerca Cerca usuaris Qui és

Adreça de xarxa: 87.216.1.66

Traça

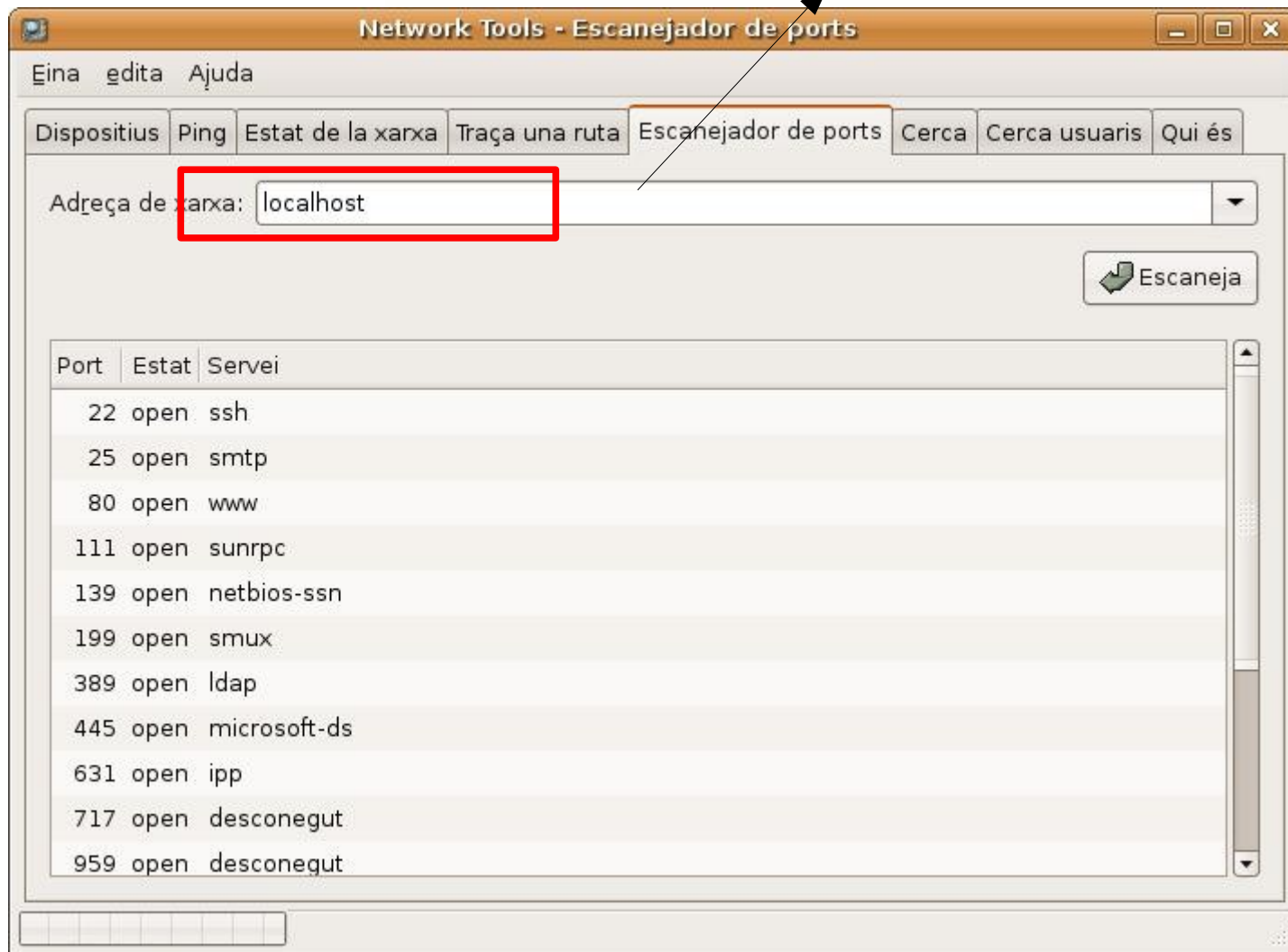
Salt	Nom d'ordinador	IP	Temps 1
1	192.168.1.10	192.168.1.10	0.241ms
1	192.168.1.1	192.168.1.1	1.804ms
2	192.168.1.1	192.168.1.1	asymm
3	10.255.136.254	10.255.136.254	50.217ms
4	inversas.2g.jazztel.es	87.216.1.13	62.758ms
5	inversas.2g.jazztel.es	87.216.1.2	58.250ms
6	inversas.2g.jazztel.es	87.216.1.66	58.630ms



Gnome-Neetool

♦ Escàner de ports:

```
$ nmap localhost
```

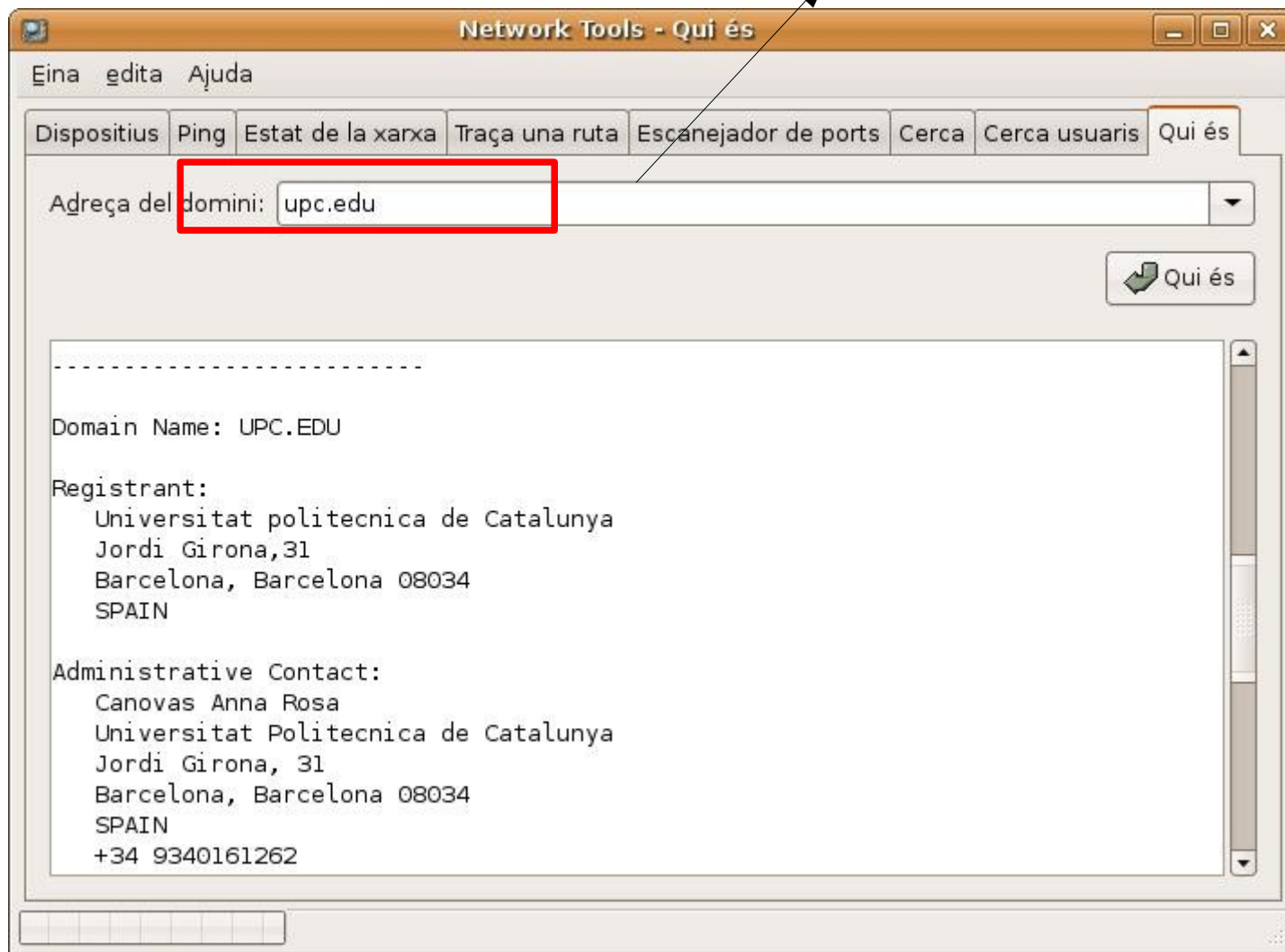




Gnome-Neetool

• Servei Whois:

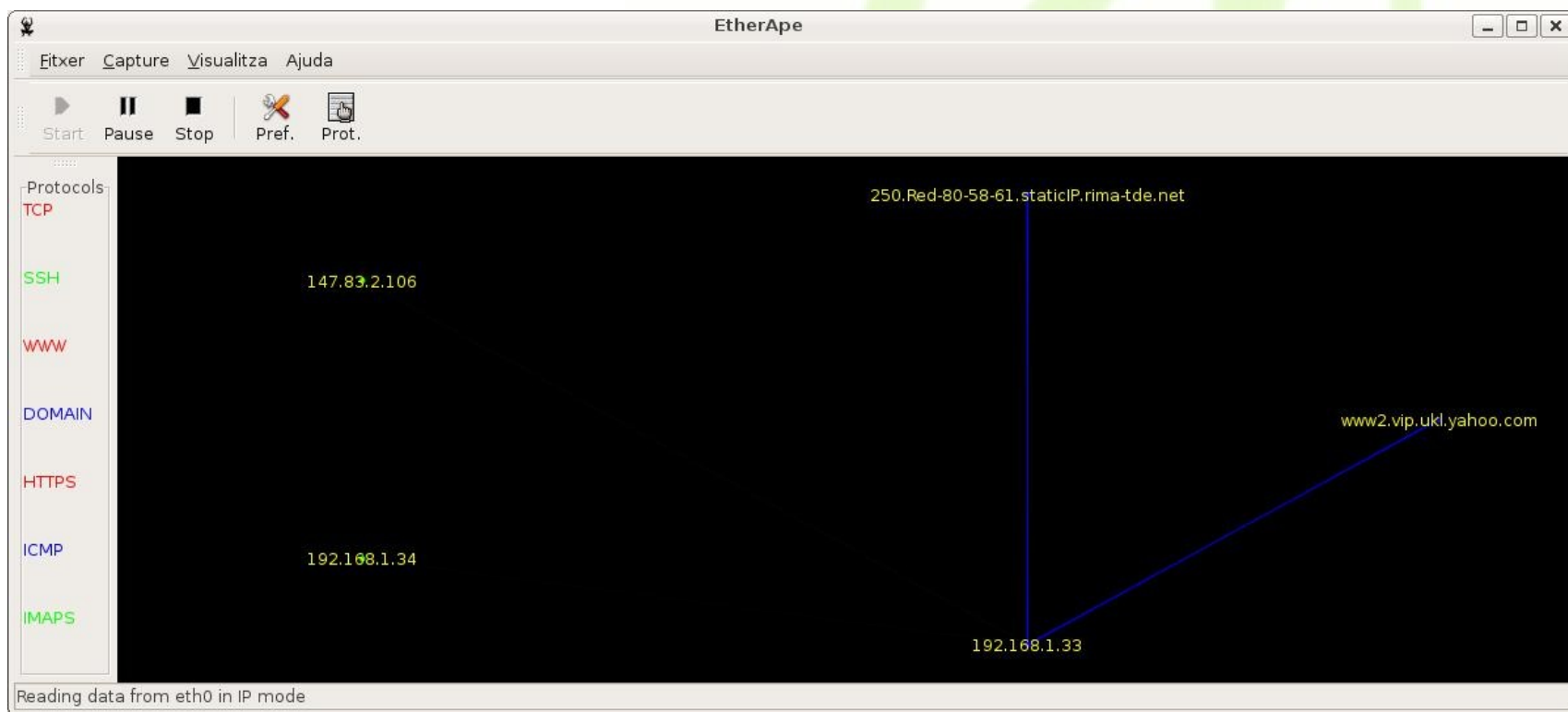
\$ whois upc.edu





EtherApe

- ◆ **Mostra gràficament les connexions de xarxa**
 - ◆ Diferència protocols per colors i amplituds de banda per amplituds de línia.
 - ◆ Ús didàctic i de monitorització (netstat gràfic)





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
```



Inicialització de la xarxa a Debian

♦ S'utilitzen scripts d'inicialització SystemV

- ♦ La xarxa s'executa al nivell S (Single User Mode) (primer de tots, fins i tot abans del nivell 1)
- ♦ Els Links:
 - `/etc/rcS.d/S08loopback`
 - `/etc/rcS.d/S40networking`
- ♦ Executen els scripts d'inicialització
 - `/etc/init.d/loopback start`
 - `/etc/init.d/networking start`



Xarxes Wireless

♦ Protocol IEEE 802.11 (WIFI). Protocols b i g



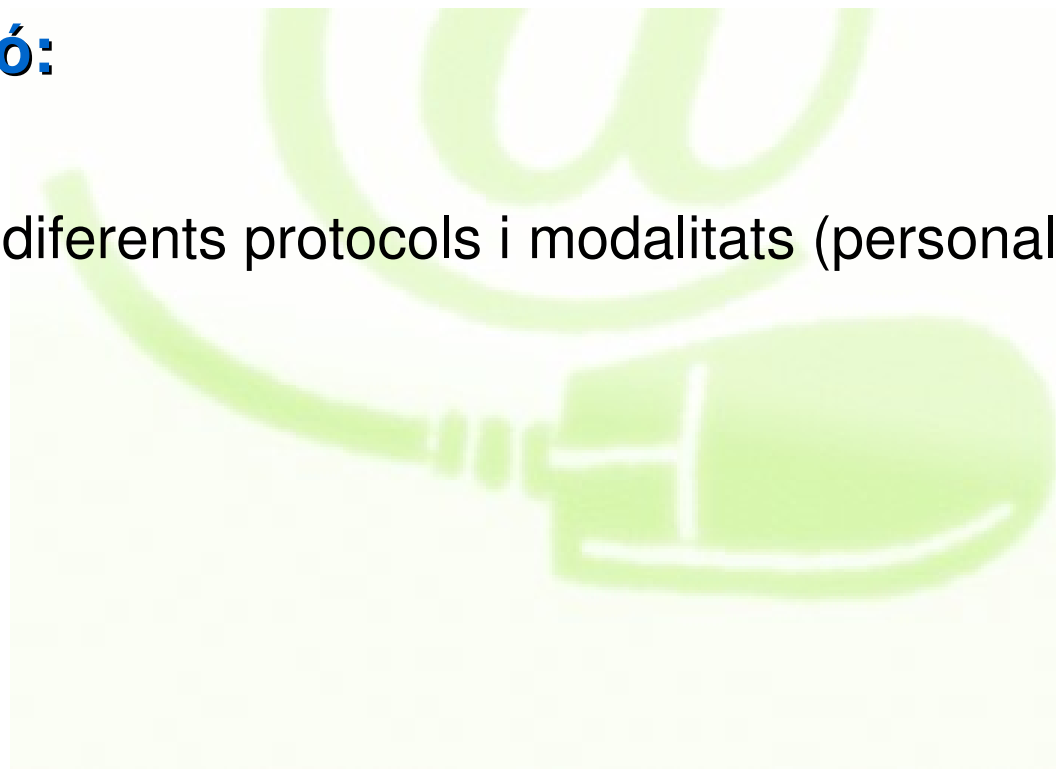
Protocol	Release Date	Op. Frequency	Data Rate (Typ)	Data Rate (Max)	Range (Indoor)	Range (Outdoor)
Legacy	1997	2.4-2.5 GHz	1 Mbit/s	2 Mbit/s	?	?
802.11a	1999	5.15-5.35/5.47-5.725/5.725-5.875 GHz	25 Mbit/s	54 Mbit/s	~30 meters (~100 feet)	?
802.11b	1999	2.4-2.5 GHz	6.5 Mbit/s	11 Mbit/s	~100 meters	?
802.11g	2003	2.4-2.5 GHz	25 Mbit/s	54 Mbit/s	~30 meters	?
802.11n	2006 (draft)	2.4 GHz or 5 GHz bands	200 Mbit/s	540 Mbit/s	~50 meters	?

♦ Sistemes d'encryptació:

- ♦ **WEP** (64 i 128 bits)
- ♦ **WPA**. Més seguretat, diferents protocols i modalitats (personal i enterprise).

♦ Claus d'accés

- ♦ Hexadecimals (4 bits)
- ♦ ASCII (1 Byte)
- ♦ WEP





Xarxes Wireless

◆ Comanda iwconfig

```
$ iwconfig
lo      no wireless extensions.
eth0    no wireless extensions.
eth1    IEEE 802.11g  ESSID:"WLAN_8A"
        Mode:Managed  Frequency:2.427 GHz  Access Point:
00:16:38:89:F6:57
        Bit Rate:54 Mb/s   Tx-Power=20 dBm   Sensitivity=8/0
        Retry limit:7   RTS thr:off   Fragment thr:off
        Power Management:off
        Link Quality=94/100  Signal level=-38 dBm  Noise level=-91 dBm
        Rx invalid nwid:0  Rx invalid crypt:0  Rx invalid frag:0
        Tx excessive retries:0  Invalid misc:0  Missed beacon:0
```

◆ /etc/network/interfaces

```
iface eth1 inet dhcp
wireless-essid WLAN_8A
wireless-key s:C0030GR89FC8A
```

◆ http://xarxantoni.net:8080/mediawiki/index.php/Xarxes_Linux_Wireless



Xarxes Wireless

- ♦ **Paràmetres de xarxa wireless**
 - ♦ Paràmetres de xarxa amb cable+
 - ♦ wireless-essid: Identificador de la xarxa
 - ♦ wireless-key: Clau WEB o WAP
 - Si la clau està en format ASCII hem de posar **s:** davant
 - ♦ wireless_mode managed | ad-hoc
- ♦ **Comandes iw** (iwlist,iwgetessid, iwspy...)
- ♦ **Paquet:** wireless-tools
- ♦ **man wireless**



NetworkManager

♦ Aplicació gràfica Gnome



♦ Ús avançat i simple de la xarxa:

- ♦ Canvi de dispositius en calent
- ♦ Roaming entre xarxes wireless
- ♦ Suport WEP i WPA





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 podem trobar en Windows o altres Sistemes Operatius.



DHCP

♦ 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, configuracions extremes, bootp, etc.)



DHCP

◆ 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.



DHCP

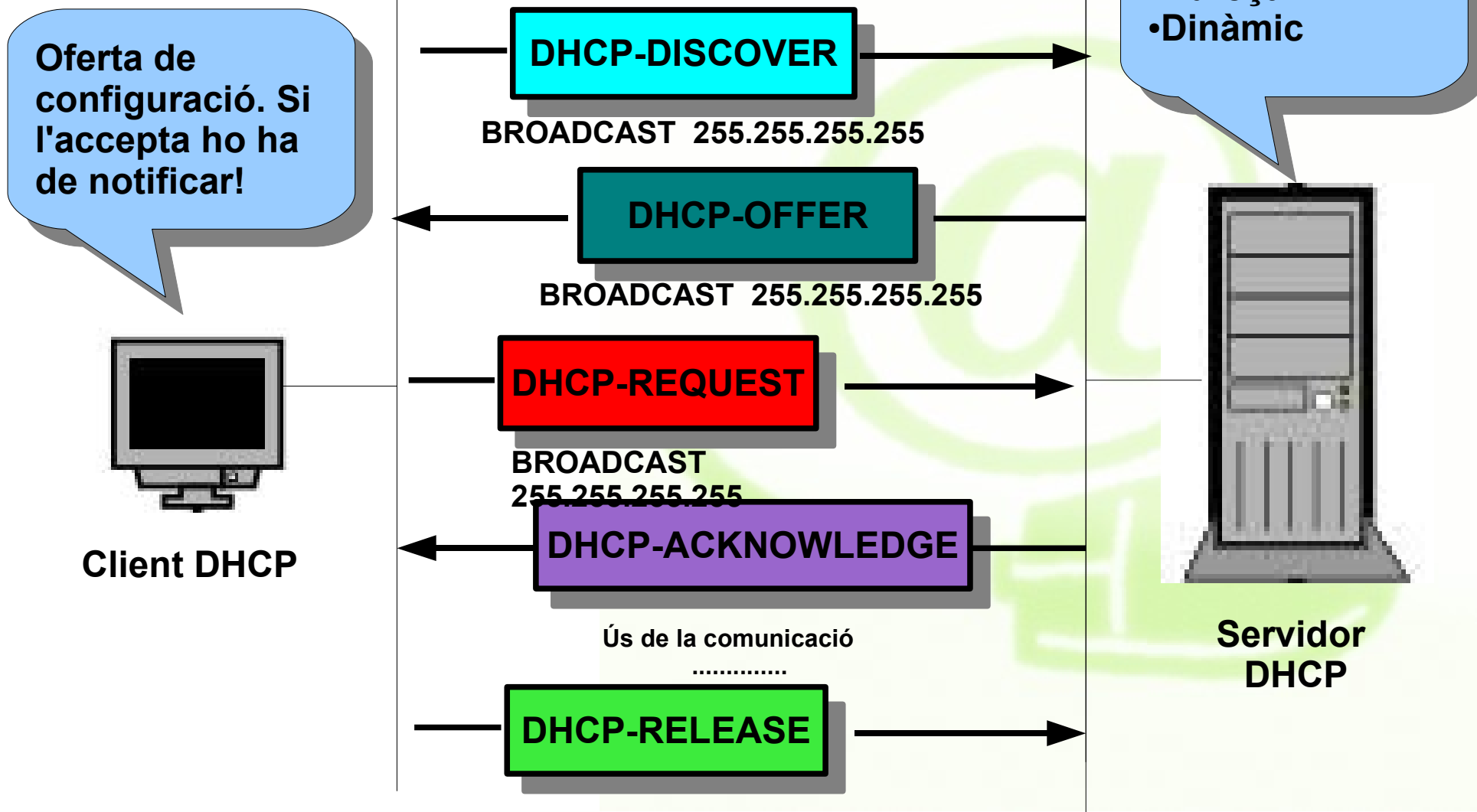
♦ Paquets del protocol

- ♦ **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).



DHCP

Funcionament del protocol





DHCP

◆ Exemple

El primer request és per intentar obtenir IP amb el lease (préstec) que ja tenim.

```
$ 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
```



Resolució de noms (DNS)

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



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.



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.



Resolució de noms (DNS)

♦ Jerarquia DNS (continuació)

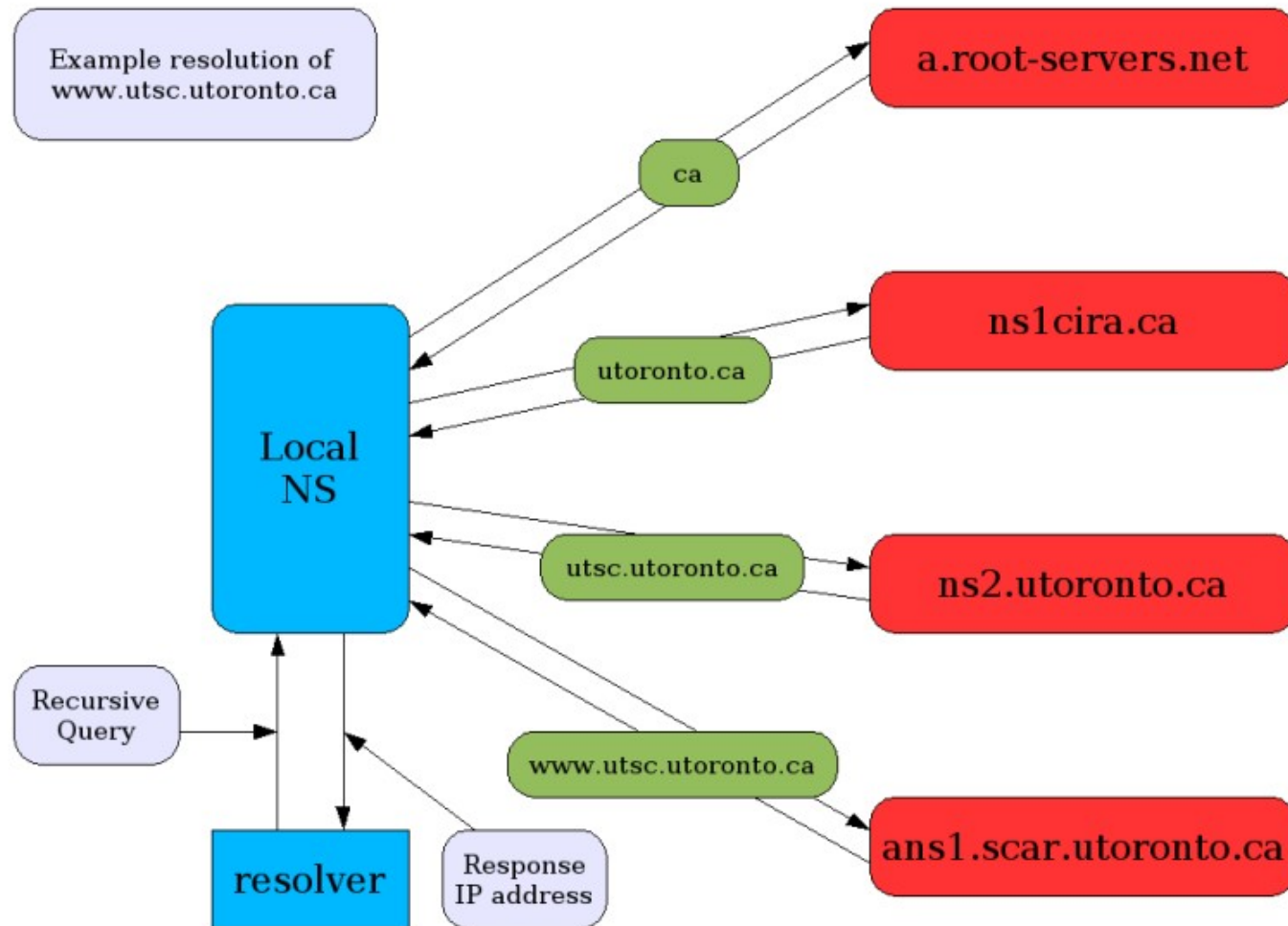
♦ Nivells

- **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.



Resoluci3 de noms (DNS)

♦ Exemple de resoluci3

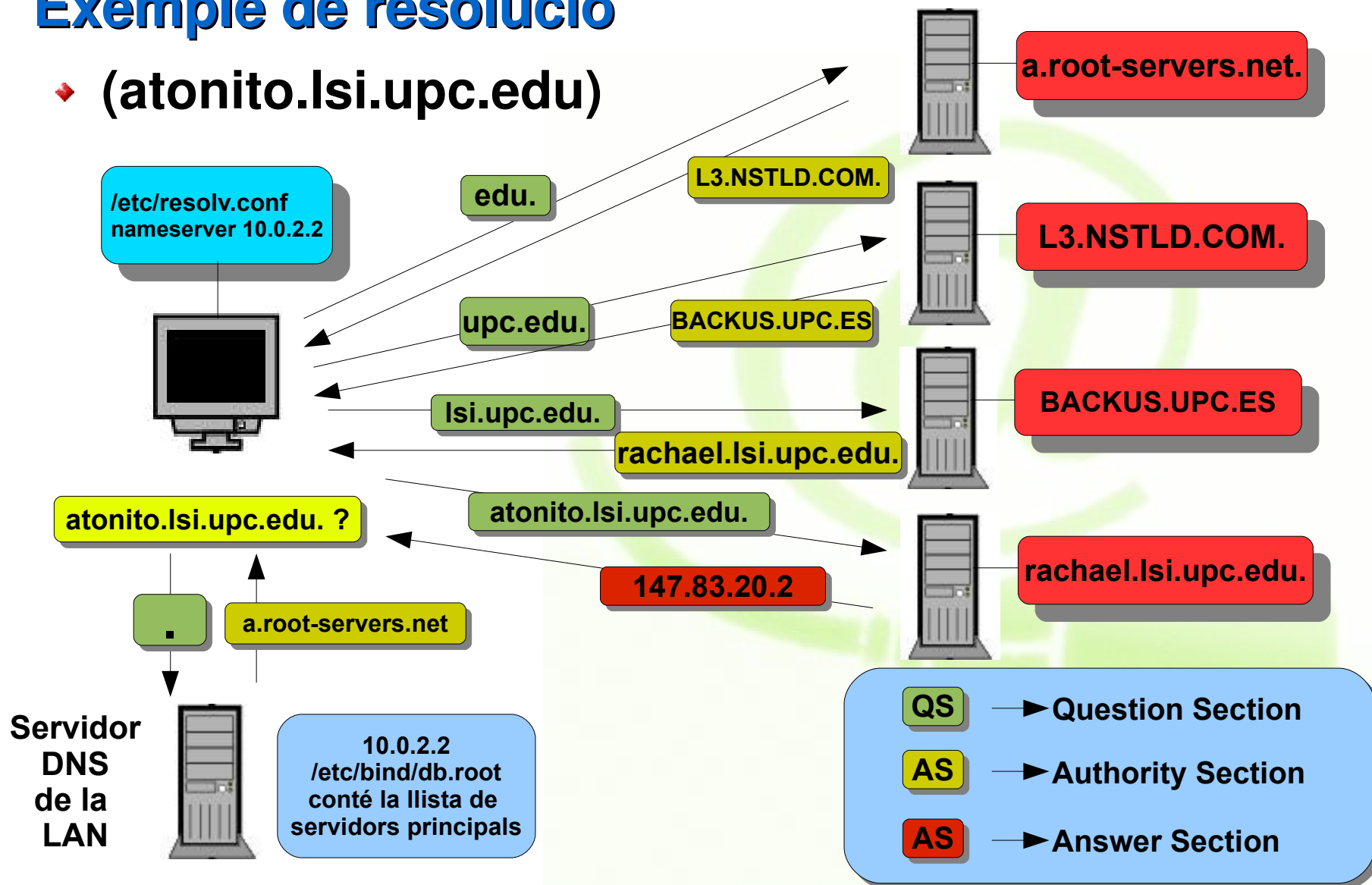




Resolució de noms (DNS)

Exemple de resolució

♦ (atonito.lsi.upc.edu)





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.  
.....
```

♦ Paquet : dnsutils



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
.....



Resoluci3 de noms (DNS)

◆ Configuraci3

- ◆ L'3nic imprescindible per configurar un servidor DNS 3s definir la llista de servidors arrel.

```
$ dig +nored +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
```



➤ Exemple dnstracer

.....



Resoluci3 de noms (DNS)

♦ Resoluci3 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.
```

♦ Resoluci3 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
```



Fitxers resoluci3 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
```



Encaminament

Eines per a la gestió de l'encaminament.



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

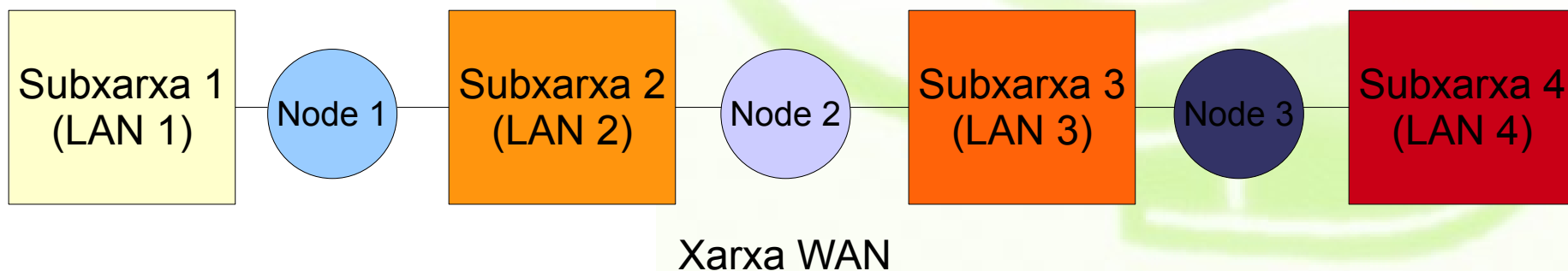
- ♦ Els routers o encaminadors són els dispositius que s'encarreguen de l'encaminament a nivell de xarxa.



Xarxes WAN o Múltiples LAN

♦ Wide Area Network

- ♦ El nivell de xarxa treballa amb tot tipus de xarxes però adquireix la seva raó de ser quan treballem amb múltiples xarxes.
- ♦ Xarxes WAN (**W**ide **A**rea **N**etwork) o
- ♦ Xarxa Complexa: Múltiples LAN





route

♦ Comanda route

```
$ route
Kernel IP routing table
Destination      Gateway         Genmask         Flags Metric Ref    Use Iface
192.168.196.0    *              255.255.255.0   U        0      0      0 vmnet8
192.168.1.0      *              255.255.255.0   U        0      0      0 eth0
192.168.252.0    *              255.255.255.0   U        0      0      0 vmnet1
default          192.168.1.1    0.0.0.0         UG       0      0      0 eth0
```

♦ 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.

♦ Proporcionat pel paquet netbase

♦ http://xarxantoni.net:8080/mediawiki/index.php/Xarxes_Linux#route



traceroute

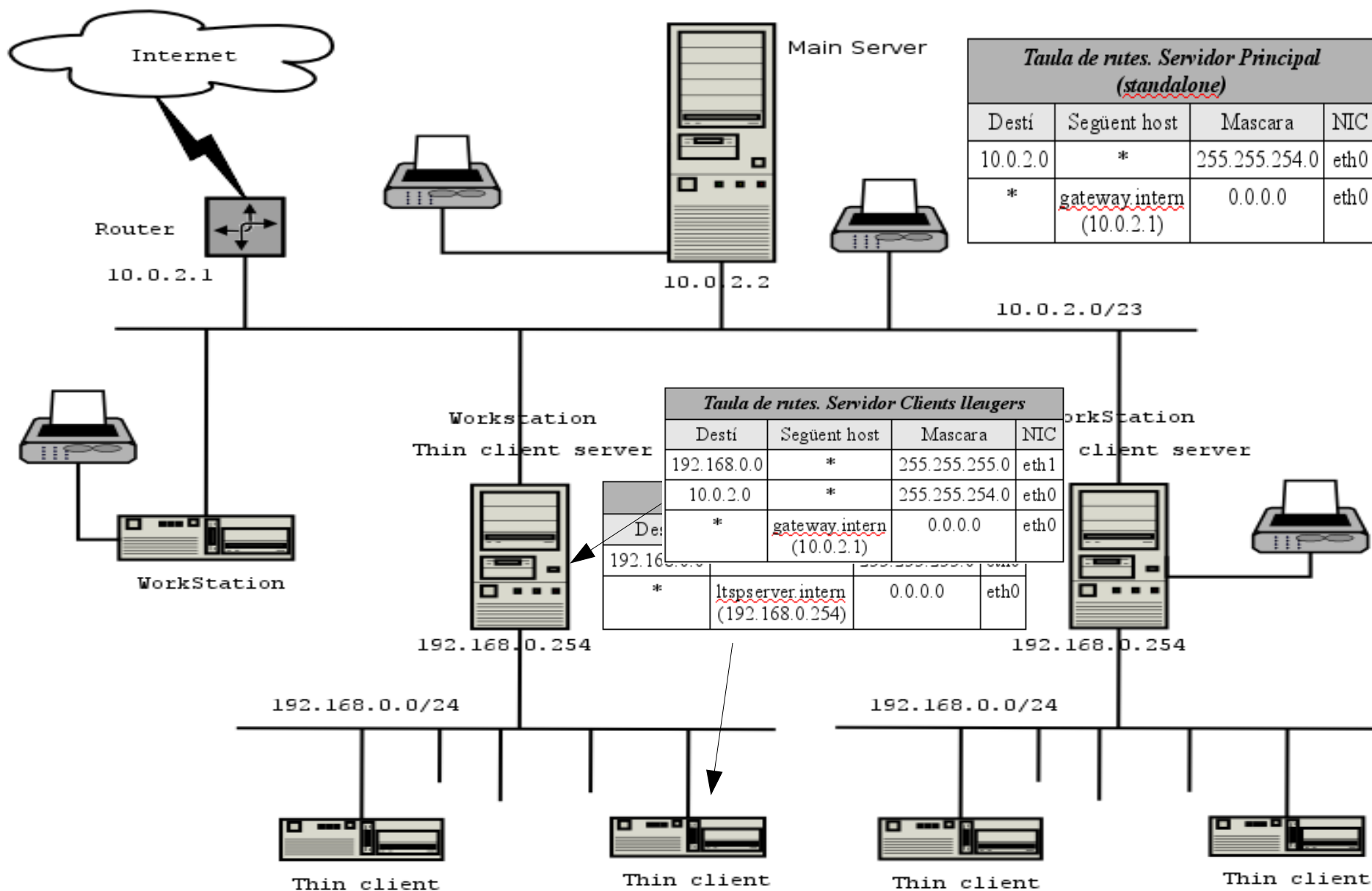
◆ Exemple

```
$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 * * *
```

- ◆ Utilitzat conjuntament amb la comanda ping es pot utilitzar per detectar els punts conflictius de l'enllaç entre dues màquines.
- ◆ Per comprovar la configuració de les taules de rutes.



SkoleLinux. Taules d'enrutament



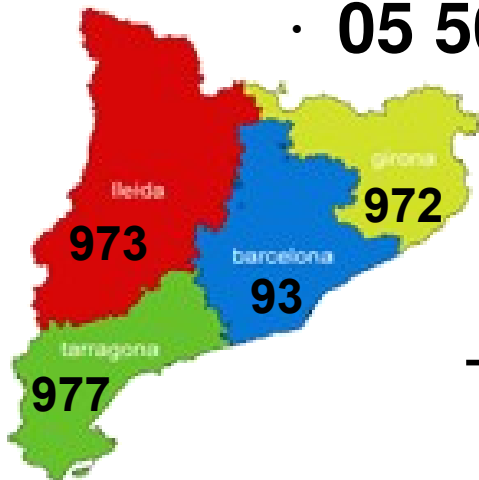


Subxarxes

♦ PSTN (Public Switched Telephone Network)

- ♦ La xarxa telefònica commutada (xarxa telefònica) també utilitza subxarxes

- N^o Telèfon: **+34 93 894 05 50**
 - **+34**: Codi de país (Espanya)
 - **93**: Codi de província (Barcelona)
 - **894**: Codi de ciutat/zona (Sitges)
 - **05 50**: Número de l'abonat



+34 93 894 05 50





Subxarxes



N: Network

H: Host

0NNNNNNN . HHHHHHHH . HHHHHHHH . HHHHHHHH

10NNNNNN . NNNNNNNN . HHHHHHHH . HHHHHHHH

110NNNNN . NNNNNNNN . NNNNNNNN . HHHHHHHH

- La màscara determina quins bits estan reservats a la xarxa i quins bits a les màquines.
- Depenent de les necessitats de xarxa (nombre de subxarxes i nombre de màquines per xarxa) s'escull la classe més adequada.



Classes

♦ Classful Networks

- Va aparèixer als anys 80 per poder classificar les xarxes en tres mides (classe A, B i C)

♦ Classe B: Força xarxes mitjanes

♦ Classe C: Moltes xarxes de 254 màquines

♦ Classes especials (D i E): Reservades per a usos especials

♦ Exercici

- Ompliu un quadre com el següent a la wiki:
 - Podeu trobar el [quadre buit](#) a Moodle

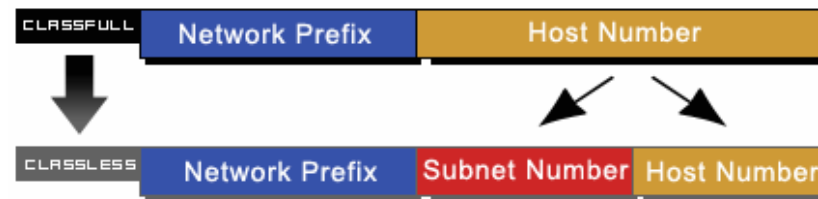
Classe	Primers bits	Primera IP	Última IP	Màscara	CIDR
A	0				
B	10				
C	110				
D	1110				
E	1111				



Subxarxes. CIDR

♦ Classless Inter-Domain Routing. CIDR

- ♦ Apareix als anys 90 per substituir el sistema de classes.
- ♦ Permet utilitzar bits d'host per a crear subxarxes:



- ♦ Ens permet obtenir més tipus de subxarxes que el sistema de classes
- ♦ La notació de les màscares amb barra (/24) també s'anomena notació CIDR.

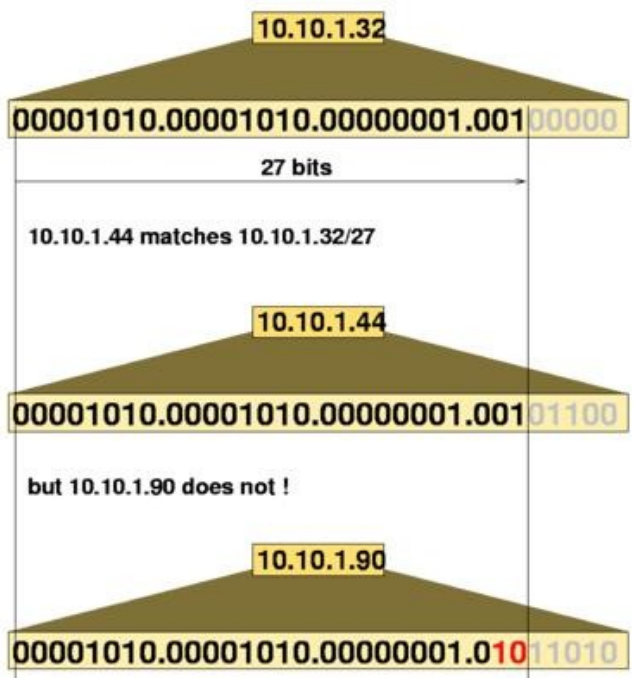


Subxarxes

♦ Per què s'utilitza aquest sistema?

- ♦ Per que per a les màquines és molt fàcil fer càlculs de subxarxes
- ♦ Càlcul molt fàcil (AND binari) per saber si dues adreces són de la mateixa xarxa

x	y	x AND y
0	0	0
0	1	0
1	0	0
1	1	1



```
$ ipcalc 192.168.5.130/26
Address: 192.168.5.130      11000000.10101000.00000101.10 000010
Netmask: 255.255.255.192=26 11111111.11111111.11111111.11 000000
Network: 192.168.5.128/26  11000000.10101000.00000101.10 000000
```

	Dot-decimal Address	Binary
Full Network Address	192.168.5.130	11000000.10101000.00000101.10000010
Subnet Mask	255.255.255.192	11111111.11111111.11111111.11000000
Network Portion	192.168.5.128	11000000.10101000.00000101.10000000



ipcalc

♦ Utilitzat per configurar subxarxes

```
sergi@casa-linux:~$ ipcalc 192.168.0.0/24
Address: 192.168.0.0      11000000.10101000.00000000. 00000000
Netmask: 255.255.255.0 = 24 11111111.11111111.11111111. 00000000
Wildcard: 0.0.0.255      00000000.00000000.00000000. 11111111
=>
Network: 192.168.0.0/24  11000000.10101000.00000000. 00000000
HostMin: 192.168.0.1    11000000.10101000.00000000. 00000001
HostMax: 192.168.0.254  11000000.10101000.00000000. 11111110
Broadcast: 192.168.0.255 11000000.10101000.00000000. 11111111
Hosts/Net: 254          Class C, Private Internet
```

```
sergi@casa-linux:~$ ipcalc 10.0.2.2/23
Address: 10.0.2.2      00001010.00000000.00000001 0.00000010
Netmask: 255.255.254.0 = 23 11111111.11111111.11111111 0.00000000
Wildcard: 0.0.1.255    00000000.00000000.00000000 1.11111111
=>
Network: 10.0.2.0/23   00001010.00000000.00000001 0.00000000
HostMin: 10.0.2.1     00001010.00000000.00000001 0.00000001
HostMax: 10.0.3.254   00001010.00000000.00000001 1.11111110
Broadcast: 10.0.3.255 00001010.00000000.00000001 1.11111111
Hosts/Net: 510        Class A, Private Internet
```



Subxarxes

♦ Són de la mateixa xarxa (màscara 27) les IPs?:

♦ 10.10.1.44

♦ 10.10.1.90

```
$ ipcalc 10.10.1.44/27
```

```
Address: 10.10.1.44      00001010.00001010.00000001.001 01100
Netmask: 255.255.255.224=27 11111111.11111111.11111111.111 00000
Network: 10.10.1.32/27    00001010.00001010.00000001.001 00000
```

```
$ ipcalc 10.10.1.44/27
```

```
Address: 10.10.1.90      00001010.00001010.00000001.010 11010
Netmask: 255.255.255.224=27 11111111.11111111.11111111.111 00000
Network: 10.10.1.64/27    00001010.00001010.00000001.010 00000
```

♦ Són de la mateixa xarxa (màscara 25) les Ips?:

♦ 192.168.201.50

♦ 192.168.201.220

```
$ ipcalc 192.168.201.50/27
```

```
Address: 192.168.201.50  11000000.10101000.11001001.00110010
Netmask: 255.255.255.224=27 11111111.11111111.11111111.11100000
Network: 192.168.201.32/27 11000000.10101000.11001001.00100000
```

```
$ ipcalc 192.168.201.220/27
```

```
Address: 192.168.201.220 11000000.10101000.11001001.11011100
Netmask: 255.255.255.224=27 11111111.11111111.11111111.11100000
Network: 192.168.201.192/27 11000000.10101000.11001001.11000000
```




Subxarxes. Classes IP

♦ RESUM: Classful Networks

- ♦ Va aparèixer als anys 80 per poder classificar les xarxes en tres mides (classe A, B i C).

Class	Leading bits	Start	End	Default Subnet Mask in dotted decimal	CIDR notation
A	0	0.0.0.1	126.255.255.255	255.0.0.0	/8
B	10	128.0.0.0	191.255.255.255	255.255.0.0	/16
C	110	192.0.0.0	223.255.255.255	255.255.255.0	/24
D	1110	224.0.0.0	239.255.255.255		
E	1111	240.0.0.0	255.255.255.0		

♦ 3 màscares possibles, 3 possibilitats

Class	Leading Value	Network Numbers	Addresses Per Network
Class A	0	126	16,777,216
Class B	10	16,384	65,534
Class C	110	2,097,152	254



Exemple. 4 subxarxes classe C.

♦ Xarxa classe C 192.168.0.1/24

- ♦ Cada bit d'host que agafem com a subxarxa ens permet multiplicar per dos les anteriors subxarxes que teníem.

♦ Nova màscara 255.255.255.192/26

```
sergi@casa-linux:~$ ipcalc 192.168.1.1/26
Address: 192.168.1.1      11000000.10101000.00000001.00 000001
Netmask: 255.255.255.192 = 26 11111111.11111111.11111111.11 000000
Wildcard: 0.0.0.63      00000000.00000000.00000000.00 111111
=>
Network: 192.168.1.0/26   11000000.10101000.00000001.00 000000
HostMin: 192.168.1.1     11000000.10101000.00000001.00 000001
HostMax: 192.168.1.62    11000000.10101000.00000001.00 111110
Broadcast: 192.168.1.63  11000000.10101000.00000001.00 111111
Hosts/Net: 62            Class C, Private Internet

sergi@casa-linux:~$ ipcalc 192.168.1.65/26
Address: 192.168.1.65     11000000.10101000.00000001.01 000001
Netmask: 255.255.255.192 = 26 11111111.11111111.11111111.11 000000
Wildcard: 0.0.0.63      00000000.00000000.00000000.00 111111
=>
Network: 192.168.1.64/26  11000000.10101000.00000001.01 000000
HostMin: 192.168.1.65    11000000.10101000.00000001.01 000001
HostMax: 192.168.1.126  11000000.10101000.00000001.01 111110
Broadcast: 192.168.1.127 11000000.10101000.00000001.01 111111
Hosts/Net: 62            Class C, Private Internet
```




Exemple. 4 subxarxes classe C.

```
sergi@casa-linux:~$ ipcalc 192.168.1.129/26
Address: 192.168.1.129      11000000.10101000.00000001.10 000001
Netmask: 255.255.255.192 = 26 11111111.11111111.11111111.11 000000
Wildcard: 0.0.0.63          00000000.00000000.00000000.00 111111
=>
Network: 192.168.1.128/26   11000000.10101000.00000001.10 000000
HostMin: 192.168.1.129     11000000.10101000.00000001.10 000001
HostMax: 192.168.1.190     11000000.10101000.00000001.10 111110
Broadcast: 192.168.1.191   11000000.10101000.00000001.10 111111
Hosts/Net: 62               Class C, Private Internet

sergi@casa-linux:~$ ipcalc 192.168.1.200/26
Address: 192.168.1.200      11000000.10101000.00000001.11 001000
Netmask: 255.255.255.192 = 26 11111111.11111111.11111111.11 000000
Wildcard: 0.0.0.63          00000000.00000000.00000000.00 111111
=>
Network: 192.168.1.192/26   11000000.10101000.00000001.11 000000
HostMin: 192.168.1.193     11000000.10101000.00000001.11 000001
HostMax: 192.168.1.254     11000000.10101000.00000001.11 111110
Broadcast: 192.168.1.255   11000000.10101000.00000001.11 111111
Hosts/Net: 62               Class C, Private Internet
```

♦ Algunes adreces no es poden utilitzar

- ♦ **Xarxa:** 192.168.1.0 | 192.168.1.64 | 192.168.1.128 | 192.168.1.192
- ♦ **Broadcast:** 192.168.1.63 | 192.168.1.127 | 192.168.1.191 | 192.168.1.255



Adreces IP reservades

♦ Adreça de xarxa

La primera adreça del rang d'adreces determinar per la màscara de xarxa és l'adreça de la xarxa

♦ Quina adreça té una xarxa?

- Per poder respondre a aquesta pregunta necessitem reservar una adreça especial: **Adreça de xarxa**

♦ Adreça de difusió

L'adreça de difusió és una adreça especial per a referir-se a totes les màquines de la xarxa

♦ Quina és la forma més senzilla (per les màquines) d'enviar un paquet a totes les màquines d'una xarxa?

- La resposta és utilitzar **l'adreça de difusió**
- Totes les màquines de la xarxa tenen aquesta adreça a part de la corresponent adreça IP (quan reben un paquet amb aquesta IP el processen com si tingués la seva IP)
- Molt més còmode que enviar X paquets (on X és el nombre de màquines de la xarxa)



IPs reservades

♦ Hi ha altres adreces IP reservades

Addresses	CIDR Equivalent	Purpose	RFC	Class	Total # of addresses
0.0.0.0 - 0.255.255.255	0.0.0.0/8	Zero Addresses	RFC 1700	A	16,777,216
10.0.0.0 - 10.255.255.255	10.0.0.0/8	Private IP addresses	RFC 1918	A	16,777,216
127.0.0.0 - 127.255.255.255	127.0.0.0/8	Localhost Loopback Address	RFC 1700	A	16,777,216
169.254.0.0 - 169.254.255.255	169.254.0.0/16	Zeroconf / APIPA	RFC 3330	B	65,536
172.16.0.0 - 172.31.255.255	172.16.0.0/12	Private IP addresses	RFC 1918	B	1,048,576
192.0.2.0 - 192.0.2.255	192.0.2.0/24	Documentation and Examples	RFC 3330	C	256
192.88.99.0 - 192.88.99.255	192.88.99.0/24	IPv6 to IPv4 relay Anycast	RFC 3068	C	256
192.168.0.0 - 192.168.255.255	192.168.0.0/16	Private IP addresses	RFC 1918	C	65,536
198.18.0.0 - 198.19.255.255	198.18.0.0/15	Network Device Benchmark	RFC 2544	C	131,072
224.0.0.0 - 239.255.255.255	224.0.0.0/4	Multicast	RFC 3171	D	268,435,456
240.0.0.0 - 255.255.255.255	240.0.0.0/4	Reserved	RFC 1700	E	268,435,456

♦ Xarxes privades

Network address range	CIDR notation
10.0.0.0 - 10.255.255.255	/8
172.16.0.0 - 172.31.255.255	/12
192.168.0.0 - 192.168.255.255	/16

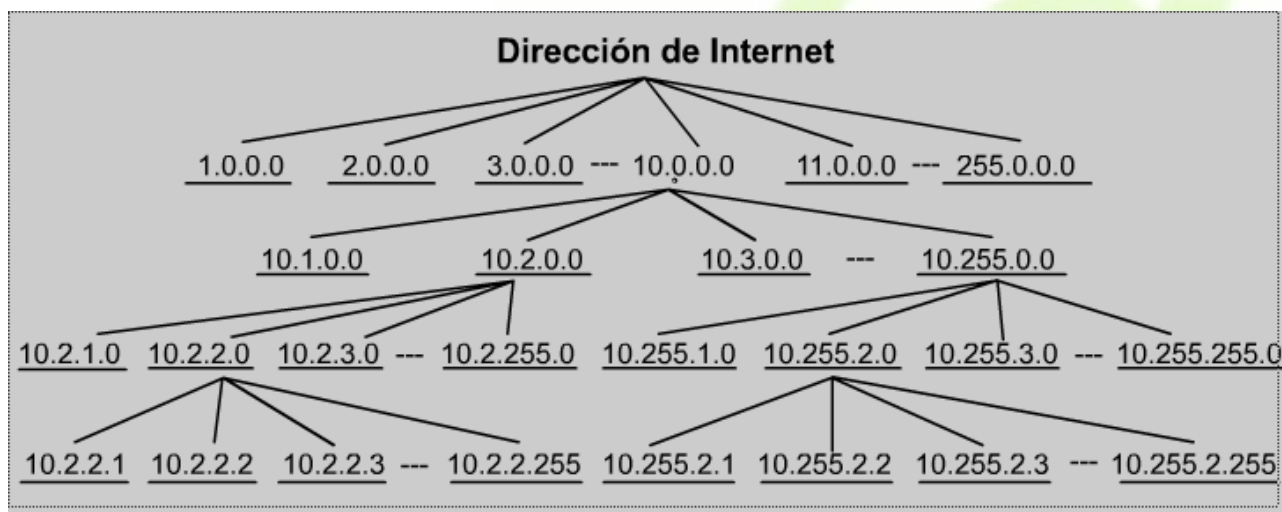


Subxarxes

♦ Cisco CCNA 1

- ♦ Podeu trobar el tema de subxarxes a l'apartat 10.3

♦ Esquema de creació de subxarxes IP



- ♦ **Exercici 1:** Pràctica de laboratori CISCO 10.3.5d “División en subredes de una red Clase C”
- ♦ **Exercici 2:** [Exercici puntuable sobre subxarxes \(Moodle\)](#)



Estat de la xarxa. Ports i sockets

Estat de la xarxa. Ports i sockets





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/slaped
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 *: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
```



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.

♦ Per a més exemples consulteu:

- ♦ http://xarxantoni.net:8080/mediawiki/index.php/Xarxes_Linux#netstat



Analitzadors de xarxa

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





TCPDUMP

- ❖ Eina de línia de comandes que permet visualitzar el tràfic de xarxa (Packet Sniffer)
- ❖ Hi ha un “port” per a Windows (WinDump) basat en Wincap (port de libcap)
- ❖ Cal ser superusuari (root) per utilitzar tcpdump (sudo). Activa automàticament el mode promiscu
 - [Tcpdump a la wiki del curs](#)
 - [Pàgina oficial](#)
 - **man tcpdump**

Desenvolupador: The Tcpdump team

OS: gairebé tots

Llicència: lliure (BSD)



TCPDUMP

♦ Característiques:

- ♦ 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.
- ♦ Com gairebé el 100% d'analitzadors de xarxa utilitza la llibreria libcap



TCPDUMP

◆ Instal·lació

```
$ sudo apt-get install tcpdump
```

◆ Filtres

- ◆ Podem aplicar filtres segons l'origen o destinació del paquet, segons els protocol, per màquines, per xarxes, per ports...

```
$ sudo tcpdump tcp and \ (port 22 or port 23\)
```

```
$ sudo tcpdump -i lo
```

```
$ sudo tcpdump icmp
```

- ◆ Activitat per parelles: Provem de **capturar pings**



TCPDUMP

♦ Exemple. Captura d'un ping

```
sergi.tur@casa: /home/sergi.tur
Fitxer  Edita  Visualitza  Terminal  Pestanyes  Ajuda
sergi.tur@casa: /home/sergi.tur
sergi.tur@casa:~$ ping -c 1 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=85.3 ms

--- www.upc.es ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 85.367/85.367/85.367/0.000 ms
sergi.tur@casa:~$
```



TCPDUMP

♦ Exemple. Captura d'un ping

```
sergi.tur@casa: /home/sergi.tur
Fitxer  Edita  Visualitza  Terminal  Pestanyes  Ajuda
sergi.tur@casa: /home/sergi.tur
sergi.tur@casa:~$ sudo tcpdump
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 96 bytes
08:54:32.703117 IP 192.168.1.10.32832 > ns2.neo.es.domain: 51593+ A? www.upc.edu. (29)
08:54:32.704029 IP 192.168.1.10.32833 > ns2.neo.es.domain: 50519+ PTR? 35.33.172.213.in-addr.arpa. (44)
08:54:32.753028 IP ns2.neo.es.domain > 192.168.1.10.32832: 51593 2/2/2 CNAME www.upc.es., (142)
08:54:32.755524 IP ns2.neo.es.domain > 192.168.1.10.32833: 50519* 1/2/2 (155)
08:54:32.765272 IP 192.168.1.10.32833 > ns2.neo.es.domain: 8683+ PTR? 10.1.168.192.in-addr.arpa. (43)
08:54:32.772723 IP 192.168.1.10 > upc.edu: ICMP echo request, id 33030, seq 1, length 64
08:54:32.815191 IP ns2.neo.es.domain > 192.168.1.10.32833: 8683 NXDomain* 0/1/0 (140)
08:54:32.826177 IP 192.168.1.10.32834 > ns2.neo.es.domain: 60076+ PTR? 21.194.83.147.in-addr.arpa. (44)
08:54:32.858954 IP upc.edu > 192.168.1.10: ICMP echo reply, id 33030, seq 1, length 64
08:54:32.862878 IP 192.168.1.10.32835 > ns2.neo.es.domain: 5647+ PTR? 21.194.83.147.in-addr.arpa. (44)
08:54:32.876973 IP ns2.neo.es.domain > 192.168.1.10.32834: 60076 4/2/2[|domain]
08:54:32.912915 IP ns2.neo.es.domain > 192.168.1.10.32835: 5647 4/2/2[|domain]
08:54:37.701823 arp who-has 192.168.1.1 tell 192.168.1.10
08:54:37.702131 IP 192.168.1.10.32835 > ns2.neo.es.domain: 4780+ PTR? 1.1.168.192.in-addr.arpa. (42)
08:54:37.703223 arp reply 192.168.1.1 is-at 00:60:4c:df:0c:3e (oui Unknown)
08:54:37.752865 IP ns2.neo.es.domain > 192.168.1.10.32835: 4780 NXDomain* 0/1/0 (139)
```




TCPDUMP

♦ 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 rebent 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.



TCPDUMP

♦ Paquets necessaris

- ♦ tcpdump

♦ Referències

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

♦ Altres enllaços

- ♦ WinDump
- ♦ Article de la wikipedia sobre Paquet Sniffers



Ethereal (Wireshark)



♦ 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 està disponible per gairebé totes les plataformes (UNIX/LINUX, MAC OS i Windows).



Ethereal

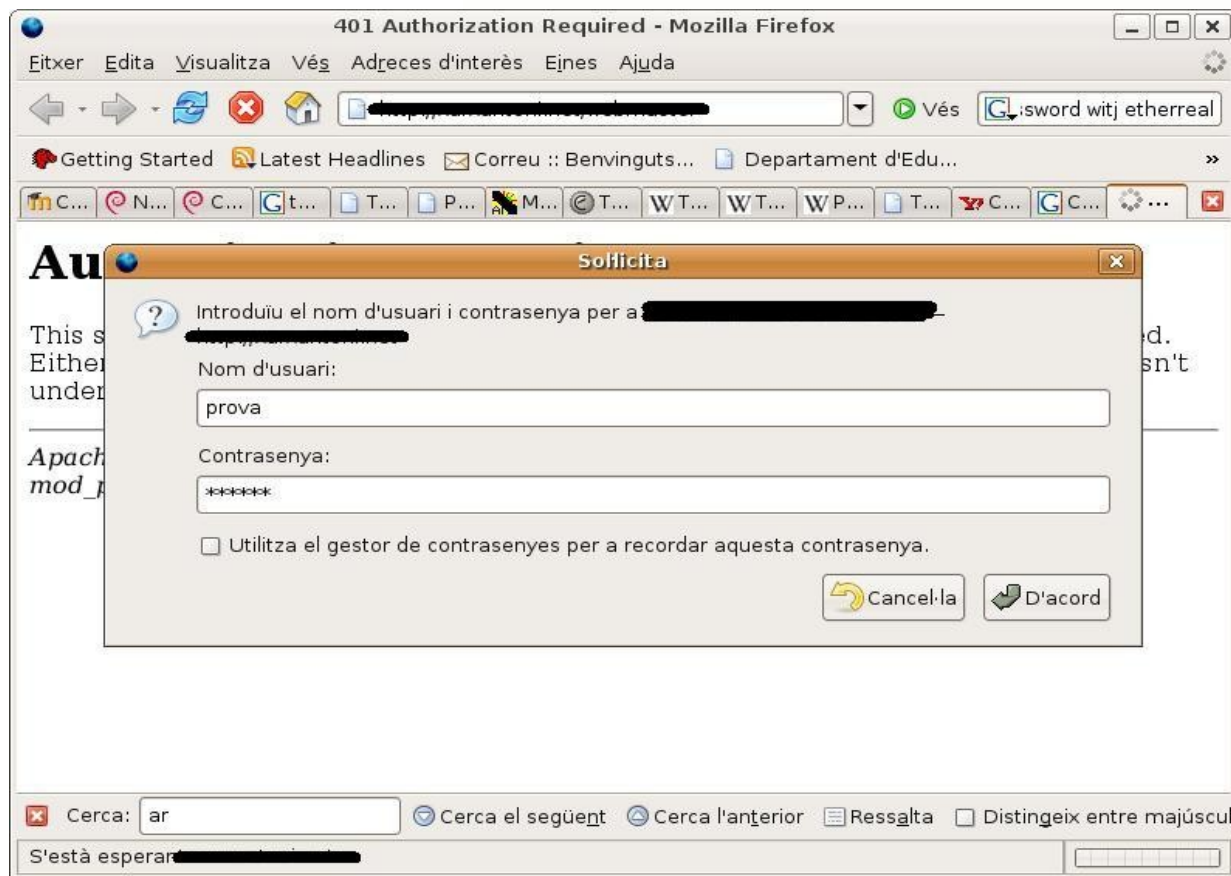
♦ Utilitats d'ethereal:

- ♦ 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.
- ♦ Altres usos menys (Sniffer, capturar contrasenyes...)



Ethereal

◆ Exemple. Captura paraula de pas web.

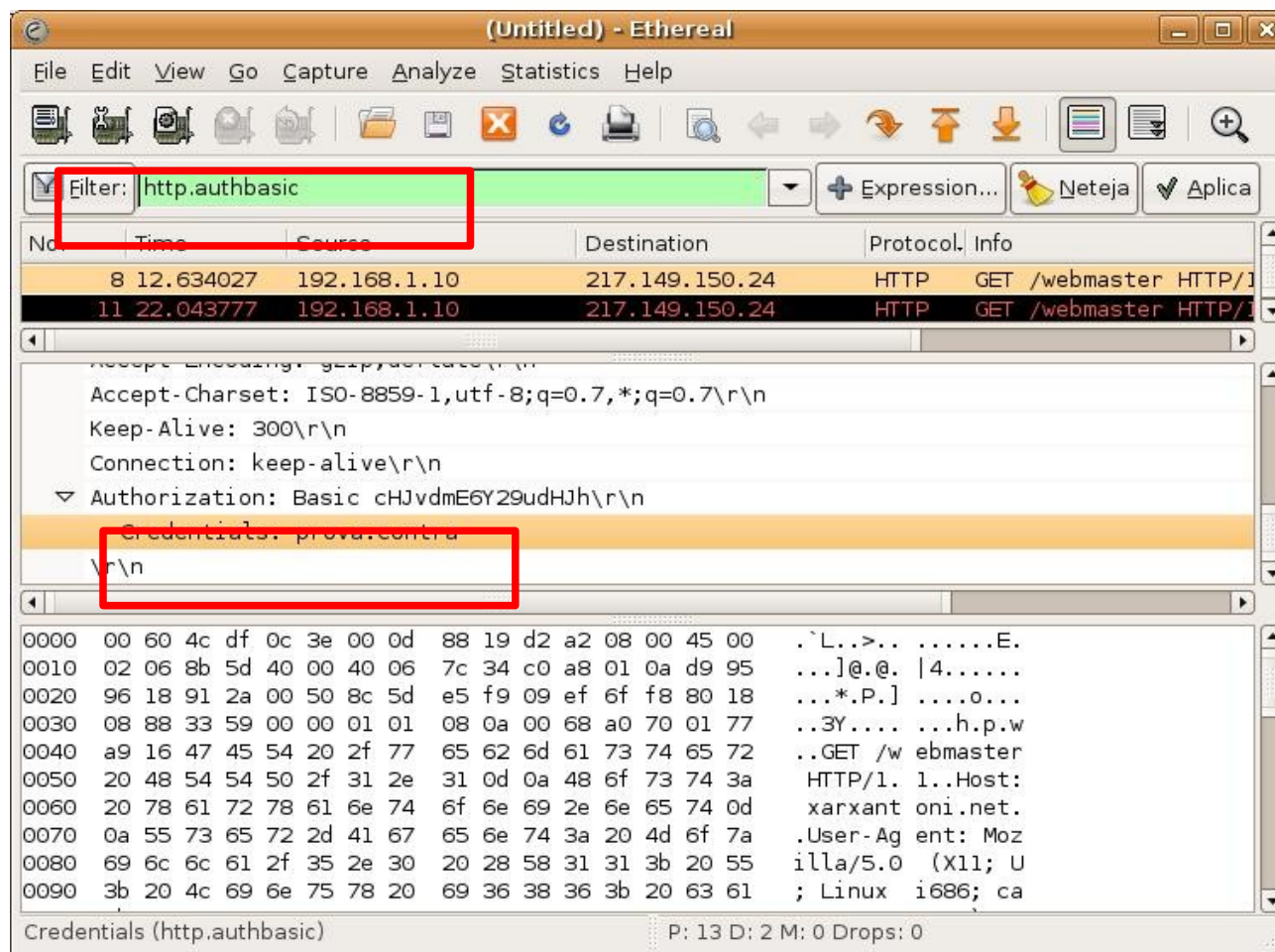


- ◆ Consulteu les transparències EinesHacking.odp del curs de seguretat en xarxes Linux per a més informació sobre temes de seguretat



Ethereal

- ◆ **Exemple. Captura paraula de pas web.**



- ◆ **Ethereal (wireshark) a la wiki del curs**

Curs Linux administració avançada.

ICE-UPC



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**



Reconeixement 3.0 Unported

Sou lliure de:



copiar, distribuir i comunicar públicament l'obra



fer-ne obres derivades

Amb les condicions següents:



Reconeixement. Heu de reconèixer els crèdits de l'obra de la manera especificada per l'autor o el llicenciador (però no d'una manera que suggereixi que us donen suport o rebeu suport per l'ús que feu l'obra).

- 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.
- No hi ha res en aquesta llicència que menyscabi o restringeixi els drets morals de l'autor.

Advertiment

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).

<http://creativecommons.org/licenses/by/3.0/deed.ca>