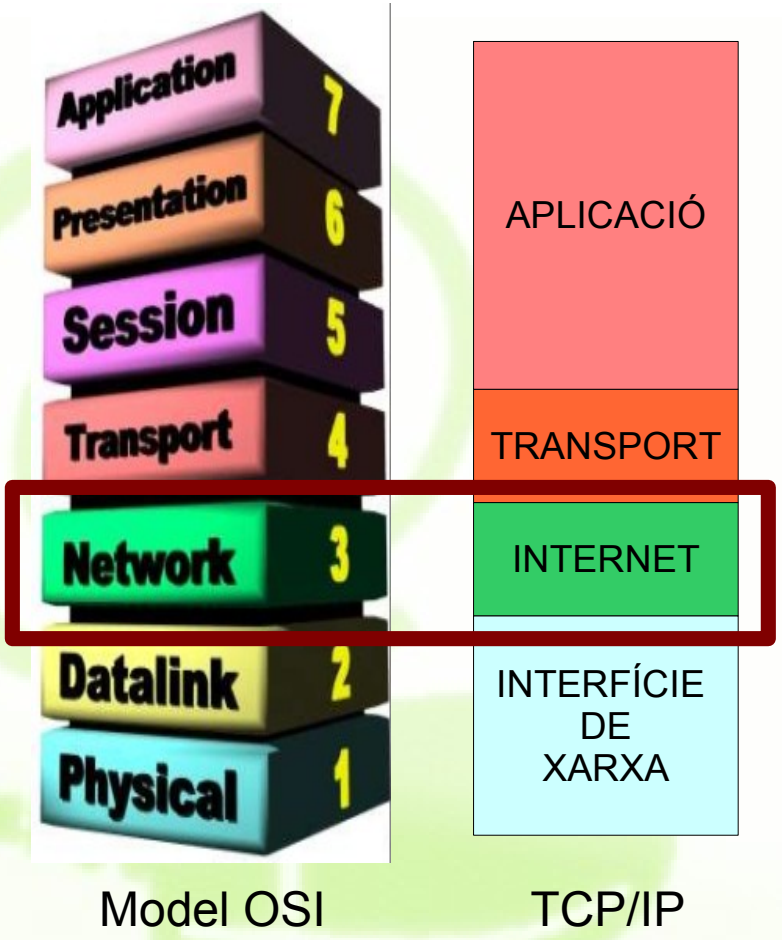
Encaminament IP: rutes del protocol IP, configuració de la taula de rutes.

Autor: Sergi Tur Badenas

Nivell d'Internet (Nivell 2 TCP/IP) - Nivell de xarxa (Nivell 3 OSI)

El nivell de xarxa és l'encarregat de realitzar les tasques bàsiques per transportar les dades des d'un origen fins a una destinació a traves d'una xarxa

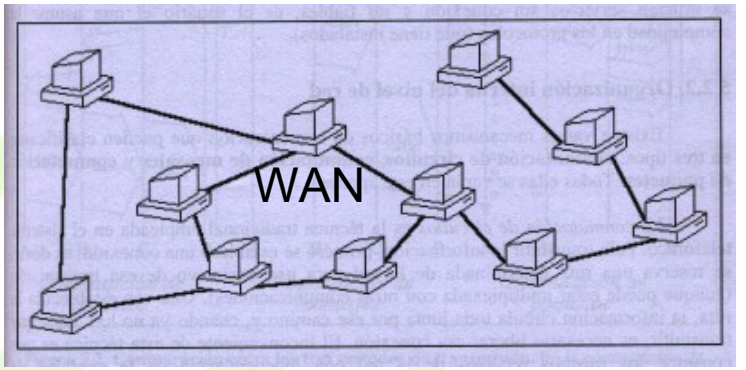
- **Model de referència OSI**
  - Nivell 3. Nivell de xarxa
- **Pila de protocols TCP/IP**
  - Nivell 2. Nivell d'Internet



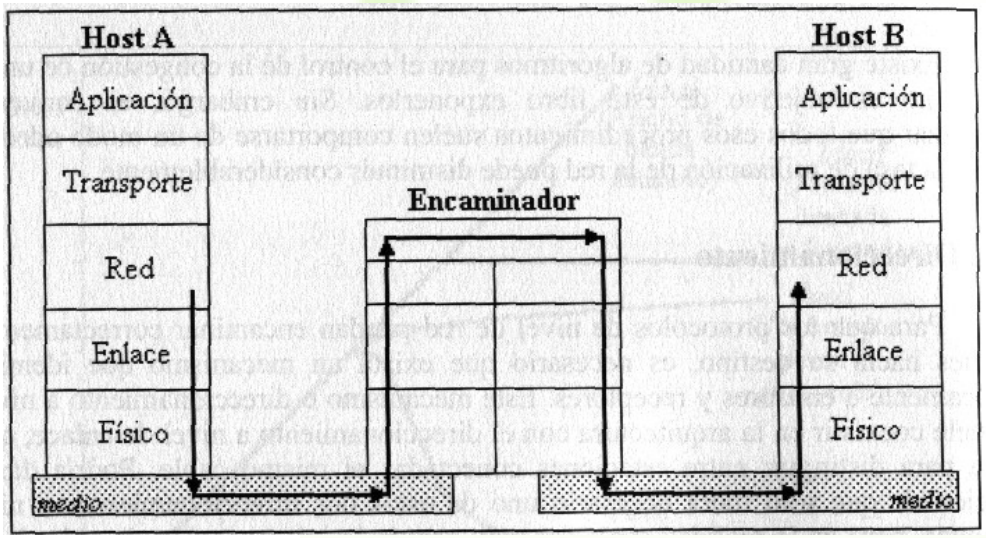
Autor: Sergi Tur Badenas

Encaminament

- **Típic de les xarxes WAN**
  - A diferència de les xarxes LAN, el medi no és compartit



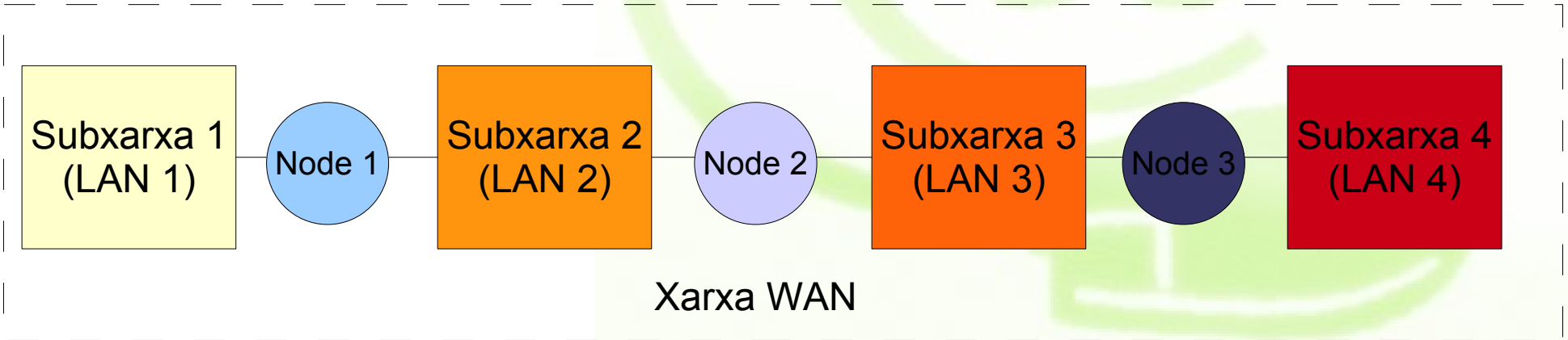
- **Enllaços punt a punt (PPP)**
  - Cada node de la xarxa és un router (encaminador)



Autor: Sergi Tur Badenas

Xarxes WAN

- **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.
  - A la xarxa formada per aquest subconjunt de xarxes o subxarxes de l'anomena WAN (**W**ide **A**rea **N**etwork)



Autor: Sergi Tur Badenas

Nivell d'Internet (Nivell 2 TCP/IP) - Nivell de xarxa (Nivell 3 OSI)

- **Control de la xarxa/subxarxa**
  - Treballa amb blocs de dades de xarxa (3-PDU) anomenats **paquets**.
- **Funcions**
  - **Encaminament**: Determinar la ruta (nodes de xarxa pels quals circular) més adequada per als paquets
  - **Identificació:** Els nodes han de tenir una identificació única que els permeti distingir dels altres nodes i localitzar-los a la xarxa. **ADREÇES IP**
  - **Control de la congestió:** determina quins són els camins menys congestionats (similar al trànsit rodat)
  - **Interconnexió de xarxes**
  - **Protocol:** IP (Internet Protocol)

Autor: Sergi Tur Badenas

Encaminament

- **Encaminament**
  - És el mecanisme pel qual en una xarxa els paquets es fan arribar d'un origen a una destinació seguint un camí o ruta concreta.
  - Cada node de la xarxa, quan rep un paquet a de prendre una decisió de que fer amb aquest paquet:
    - Quedar-se el paquet quan ell és el destinatari
    - Enviar al paquet cap a un altre node veí
    - O potser eliminar el paquet per què és incorrecta.
- **Routers/Encaminadors**
  - Els routers o encaminadors són els dispositius/nodes de xarxa que s'encarreguen de l'encaminament a nivell de xarxa.

Autor: Sergi Tur Badenas

Adreces IP

- **Les adreces IPs estan formades per 32 Bits**
  - 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
```

- **Altres notacions**

Notation	Value	Conversion from dot-decimal
Dot-decimal notation	207.142.131.235	N/A
Dotted Hexadecimal	0xCF.0x8E.0x83.0xEB	Each octet is individually converted to hex
Dotted Octal	0317.0216.0203.0353	Each octet is individually converted into octal
Hexadecimal	0xCF8E83EB	Concatenation of the octets from the dotted hexadecimal
Decimal	3482223595	The hexadecimal form converted to decimal
Octal	031743501753	The hexadecimal form converted to octal

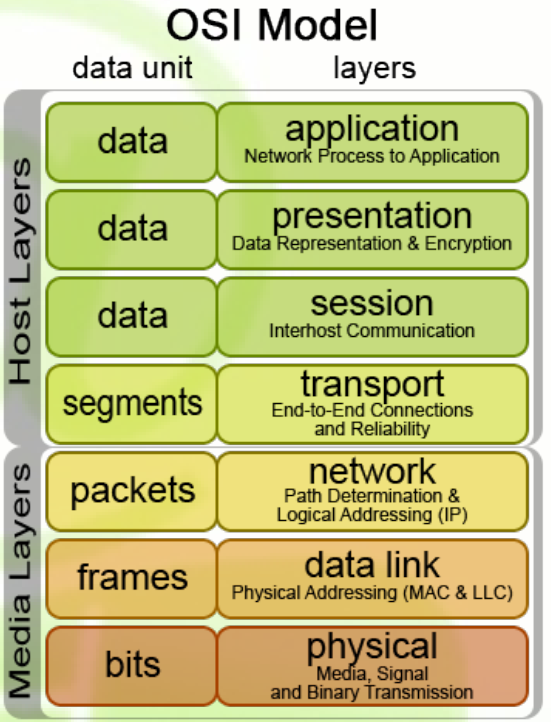
Autor: Sergi Tur Badenas

Paquets IP

- **La unitat de dades del nivell 4 és el paquet/packet**
  - Un paquet està format per dos parts:
    - **Capçalera:**

0										1										2										3	
0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1
Version				IHL				TOS/DSCP/ECN								Total Length															
Identification																	Flags	Fragment Offset													
Time To Live								Protocol								Header Checksum															
Source Address																															
Destination Address																															
Options																													Padding		

    - **Dades**: si les dades a transportar són moltes, les dades s'hauran de fragmentar/repartir en diferents paquets

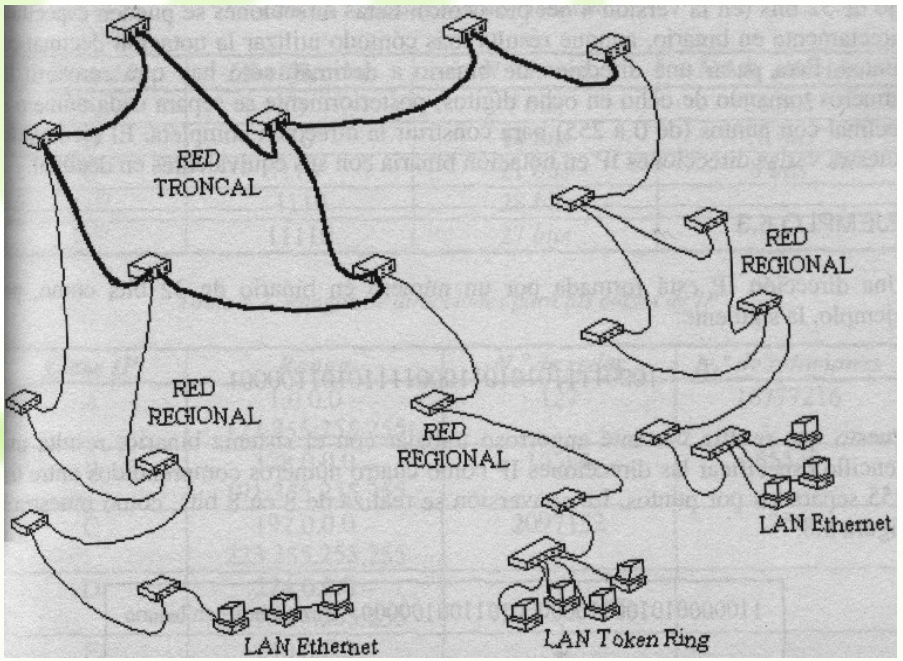


  - Amb Ethereal podem identificar les capçaleres dels paquets per nivells.

Autor: Sergi Tur Badenas

Subxarxes

- **La xarxa (Internet) està formada per subxarxes.**
  - L'adreça de xarxa conjuntament amb la màscara de xarxa configuren les subxarxes.
- **Les subxarxes permeten aprofitar millor les IPS**
  - Recurs limitat.
  - Millor organització jeràrquica.

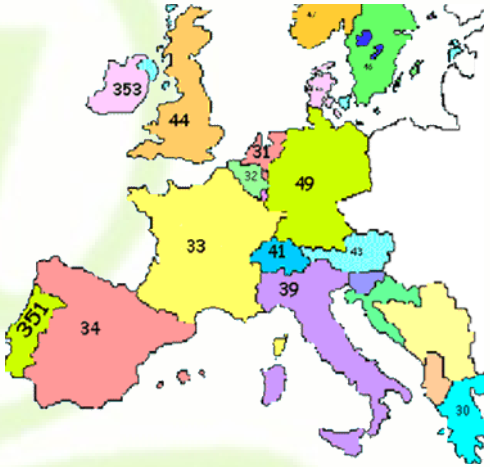


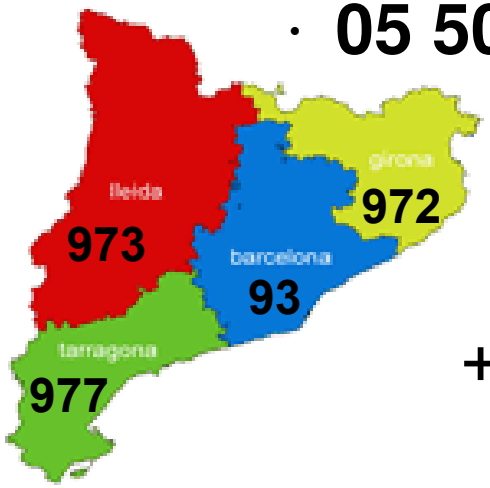
- **Subxarxes a la wiki del curs**

Autor: Sergi Tur Badenas

Subxarxes

- **PSTN (Public Switched Telephone Network)**
  - La xarxa telefònica commutada (xarxa telefònica) també utilitza subxarxes
    - Nº 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

Autor: Sergi Tur Badenas

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 ceros.
    - Només són vàlides les màscares que tenen els valors:

      255, 254, 252, 248, 240, 224, 192, 128

Autor: Sergi Tur Badenas

Màscara de xarxa

- **La màscara 255.255.255.128:**
  - Ens indica que estem a una xarxa de 126 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 147.82.75.131/25
Address:   147.82.75.131         10010011.01010010.01001011.1 0000011
Netmask:   255.255.255.128 = 25 11111111.11111111.11111111.1 0000000
Wildcard:  0.0.0.127             00000000.00000000.00000000.0 1111111
=>
Network:   147.82.75.128/25      10010011.01010010.01001011.1 0000000
HostMin:   147.82.75.129         10010011.01010010.01001011.1 0000001
HostMax:   147.82.75.254         10010011.01010010.01001011.1 1111110
Broadcast: 147.82.75.255         10010011.01010010.01001011.1 1111111
Hosts/Net: 126                    Class B
```


Autor: Sergi Tur Badenas

Màscara de xarxa

- **AULA LINUX**

```
    Network(N)/Hosts (H)      NNNNNNNN.NNNNNNNN.NNNNNNNN.HHHHHHHH
MÀSCARA : 255.255.255.128  / 11111111.11111111.11111111.10000000
IP xarxa: 147.83.75.x      / 10010011.01010010.01001011.10000000
Màquina1: 147.83.75.129    / 10010011.01010010.01001011.10000001
Màquina2: 147.83.75.130    / 10010011.01010010.01001011.10000010
Màquina3: 147.83.75.131    / 10010011.01010010.01001011.10000011
Màquina4: 147.83.75.132    / 10010011.01010010.01001011.10000100
Màquina5: 147.83.75.133    / 10010011.01010010.01001011.10000101
Màquina6: 147.83.75.134    / 10010011.01010010.01001011.10000110
Màquina7: 147.83.75.135    / 10010011.01010010.01001011.10000111
Màquina8: 147.83.75.136    / 10010011.01010010.01001011.10001000
Màquina9: 147.83.75.137    / 10010011.01010010.01001011.10001001
.....................................................................
Màqui153: 147.83.75.253    / 10010011.01010010.01001011.11111101
Màqui154: 147.83.75.254    / 10010011.01010010.01001011.11111110
Broadcast:147.83.75.255    / 10010011.01010010.01001011.11111111
```


Autor: Sergi Tur Badenas

Classful Networks

- **La màscara de cada classe 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.

Autor: Sergi Tur Badenas

Subxarxes. Classes IP

- **Quadre resum**
  - 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		

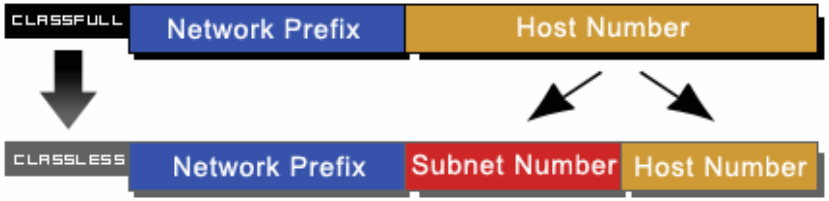
- **3 màscares possibles, 3 possibilitats**

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

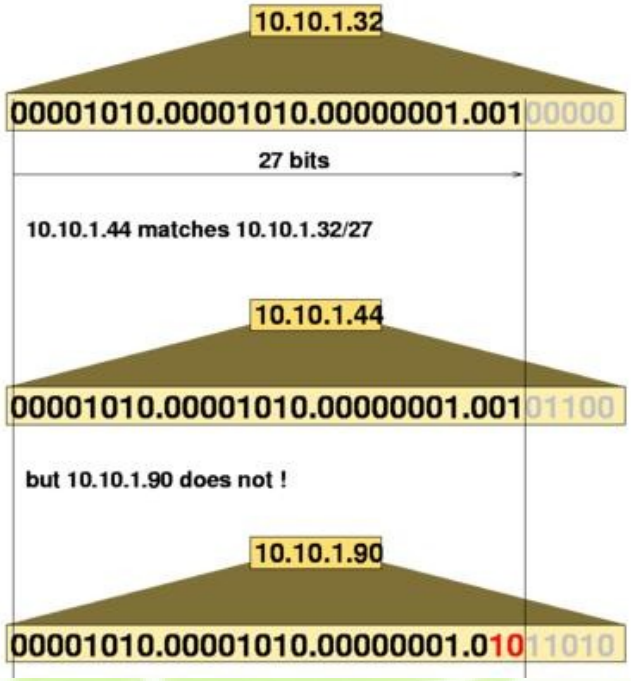
Autor: Sergi Tur Badenas

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:



  - Càlcul molt fàcil (AND binari) per saber si dues adreces són de la mateixa xarxa



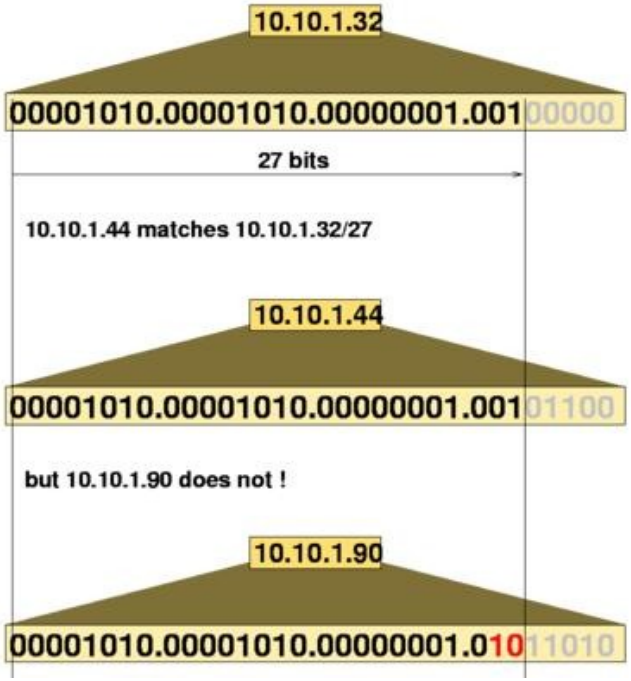
	Dot-decimal Address	Binary
Full Network Address	192.168.5.130	11000000.10101000.00000101.10000010
Subnet Mask	255.255.255.192	11111111.11111111.11111111.**11**000000
Network Portion	192.168.5.128	11000000.10101000.00000101.10000000

Autor: Sergi Tur Badenas

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.**11**000000
Network Portion	192.168.5.128	11000000.10101000.00000101.10000000

Autor: Sergi Tur Badenas

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   11000000.10101000.11001001.001 00000
```

```
$ 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  11000000.10101000.11001001.110 00000
```


Autor: Sergi Tur Badenas

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
```


Autor: Sergi Tur Badenas

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

Autor: Sergi Tur Badenas

Exemple. 4 subxarxes classe C.

- **ipcalc ens resol aquest problema amb una sola comanda**

```
$ ipcalc 192.168.1.0/24 26
Address:   192.168.1.0          11000000.10101000.00000001. 00000000
Netmask:   255.255.255.0 = 24   11111111.11111111.11111111. 00000000

Network:   192.168.1.0/24       11000000.10101000.00000001. 00000000
HostMin:   192.168.1.1          11000000.10101000.00000001. 00000001
HostMax:   192.168.1.254        11000000.10101000.00000001. 11111110
Broadcast: 192.168.1.255        11000000.10101000.00000001. 11111111
Hosts/Net: 254                   Class C, Private Internet

Subnets after transition from /24 to /26

Netmask:   255.255.255.192 = 26 11111111.11111111.11111111.11 000000
Wildcard:  0.0.0.63             00000000.00000000.00000000.00 111111
 1.
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
 2.
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

 3.
.......
```


Autor: Sergi Tur Badenas

IPs reservades

- **Definides per diferents RFC**

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

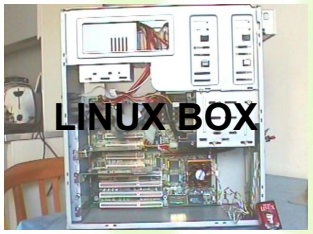
Autor: Sergi Tur Badenas

Routers / Encaminadors

- **Hi ha diferents tipus de routers:**

MAQUINARI

PROGRAMARI



- **Programari**
  - Molts routers comercials el que tenen darrera és programari Unix adaptat.

Autor: Sergi Tur Badenas

Configuració

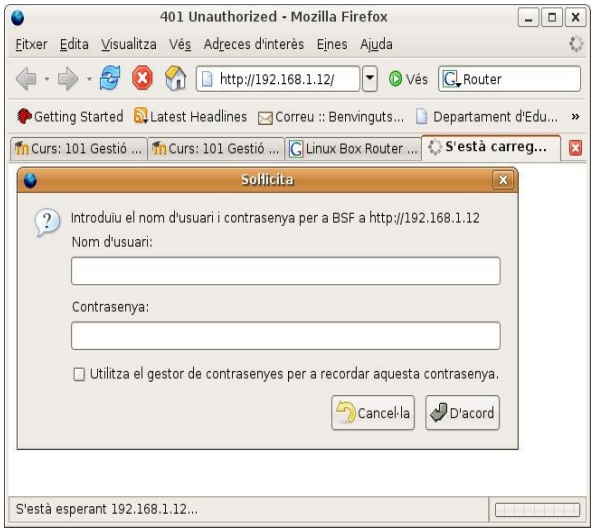
- **Típicament la configuració dels routers es pot fer a través:**
  - d'una interfície web
  - d'accés remot (Telnet o SSH)
  - d'accés directe al sistema (Linux Box)
  - de programari específic de configuració
- **Serveis extres:**
  - DHCP
  - Firewall. Gestió de la seguretat. DMZ
  - NAT
  - VPN, QoS, Radius, etc.

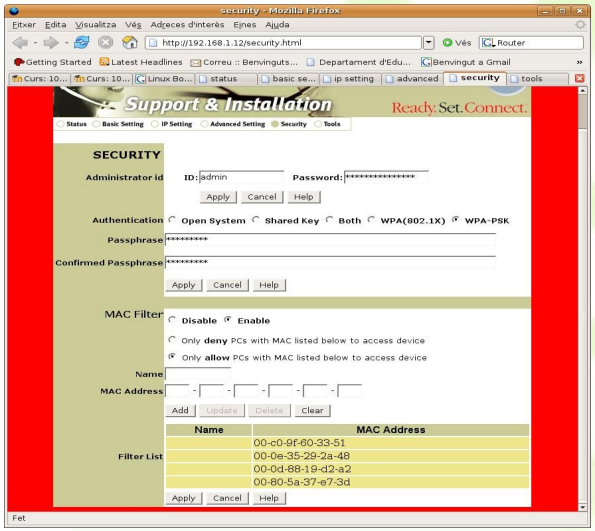
Autor: Sergi Tur Badenas

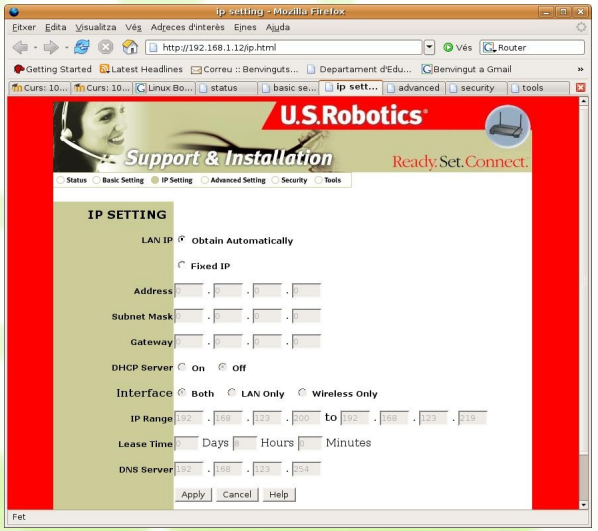
Exemple router comercial

- **Router US-Robotics**

Interfície web de configuració
IP Local:192.168.1.12

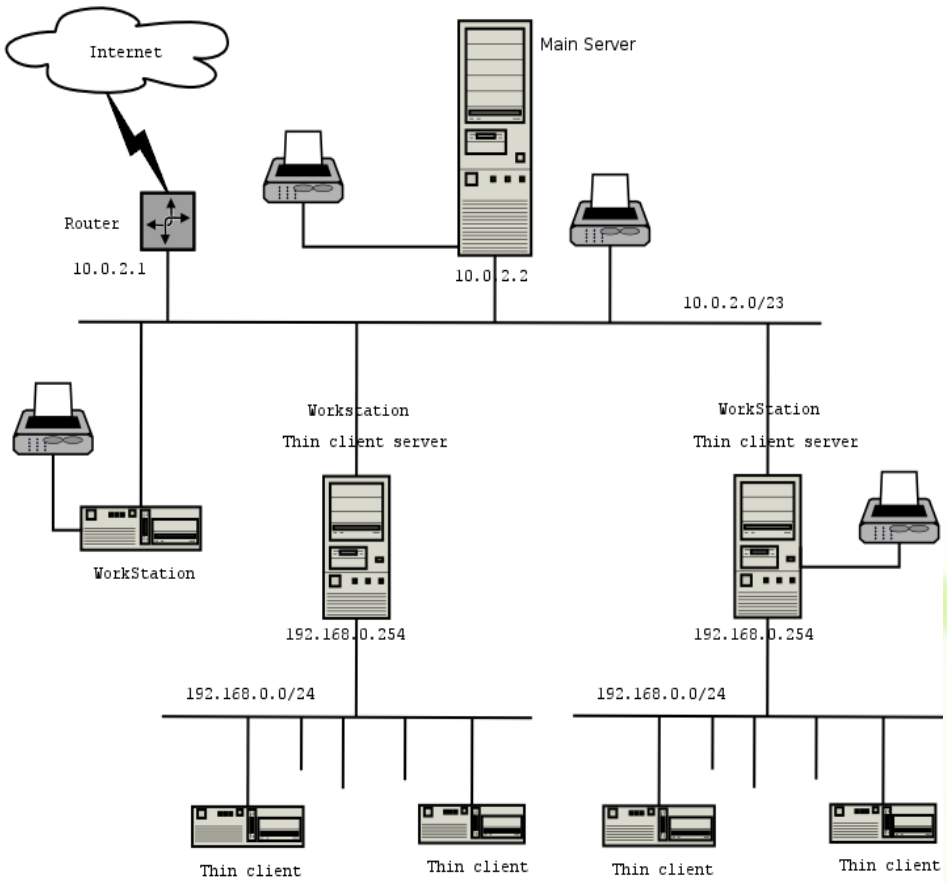






Autor: Sergi Tur Badenas

Exemple Aula Informàtica. SkoleLinux

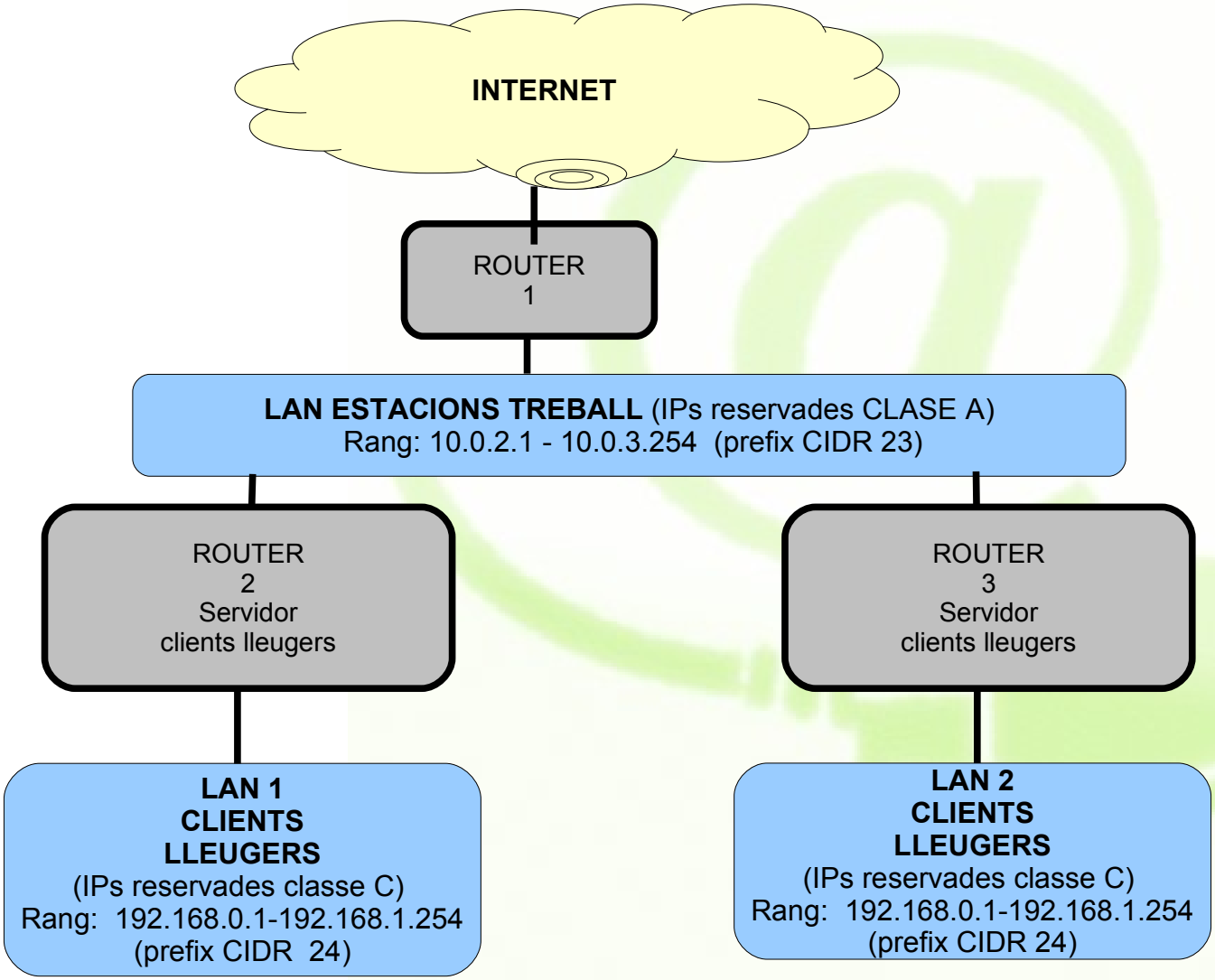


- **3 xarxes d'àrea local**
  - Switch 1: Estacions de treball
  - Switch 2 i 3: Terminals lleugers
- **Thin client servers**
  - Enrutadors entre xarxes
  - 2 NICs
- **Router principal**
  - Accés a Internet

Autor: Sergi Tur Badenas

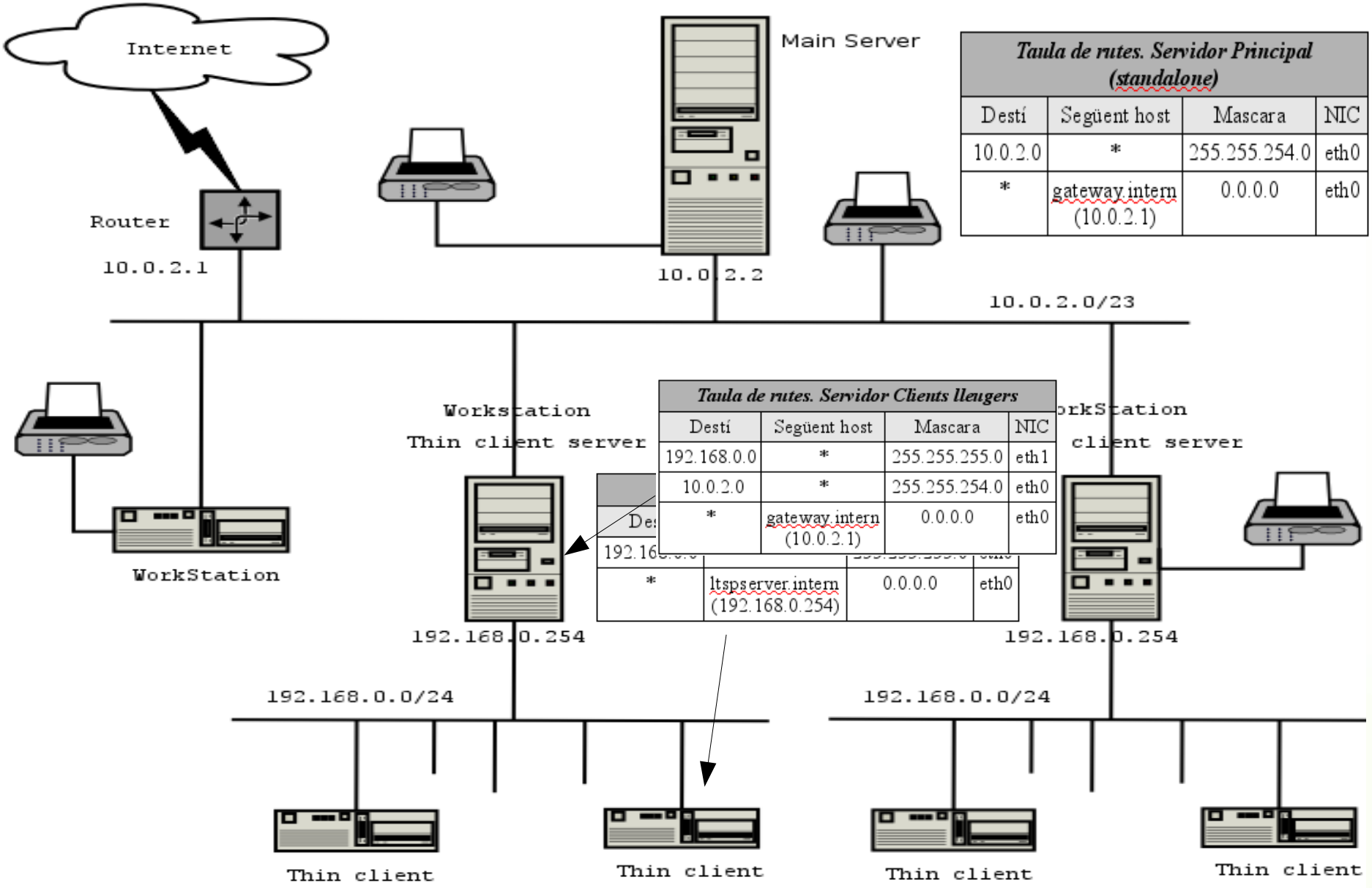
Exemple Aula Informàtica. SkoleLinux

- **Esquema d'encaminadors d'una l'aula SkoleLinux**



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

route

- **Comanda route**

```
$ route
Kernel IP routeing 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

Autor: Sergi Tur Badenas

SkoleLinux. Interconnexió de xarxes

- **Interconnexió de xarxes d'àrea local**
  - Les 3 xarxes de l'arquitectura SkoleLinux no estan connectades entre si. Quins canvis hauríem de fer per connectar, per exemple, la xarxa d'estacions de treball amb una de les xarxes de clients lleugers?
  - Qui exerceix en aquest cas el rol d'encaminador entre les dues xarxes?
- **Connexió xarxa d'àrea extensa**
  - Qui exerceix el rol d'encaminador cap a Internet (gateway)?

Autor: Sergi Tur Badenas

SkoleLinux. Interconnexió de xarxes

Solucions

- El rol d'encaminador l'exerceix el servidor de clients lleugers. La seva taula de rutes queda igual.

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

Taula de rutes. Clients lleugers			
Destí	Següent host	Mascara	NIC
192.168.0.0	*	255.255.255.0	eth0
10.0.2.0	ltspserver.intern (192.168.0.254)	255.255.254.0	eth0
*	ltspserver.intern (192.168.0.254)	0.0.0.0	eth0

```
$ sudo route add -net 10.0.0.2 \
netmask 255.255.254.0 gw
ltspserver.intern \
dev eth0
```

Taula de rutes. Estacions de treball			
Destí	Següent host	Mascara	NIC
192.168.0.0	**ltspserverX**.intern (10.0.2.X)	255.255.255.0	eth0
10.0.2.0	*	255.255.254.0	eth0
*	gateway.intern (10.0.2.1)	0.0.0.0	eth0

```
$ sudo route add -net 192.168.0.0 \
netmask 255.255.255.0 gw
ltspserverX.intern \
dev eth0
```


Autor: Sergi Tur Badenas

traceroute

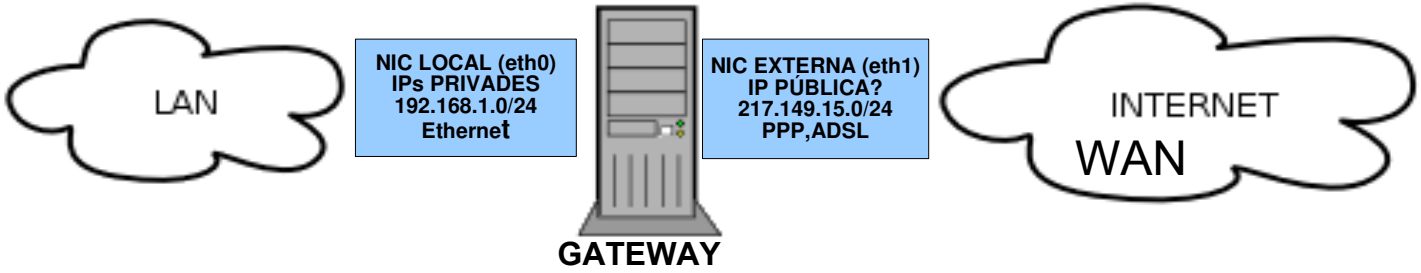
- **Exemple**

```
$ 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  * * *
```

- 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.

Autor: Sergi Tur Badenas

Gateway Linux

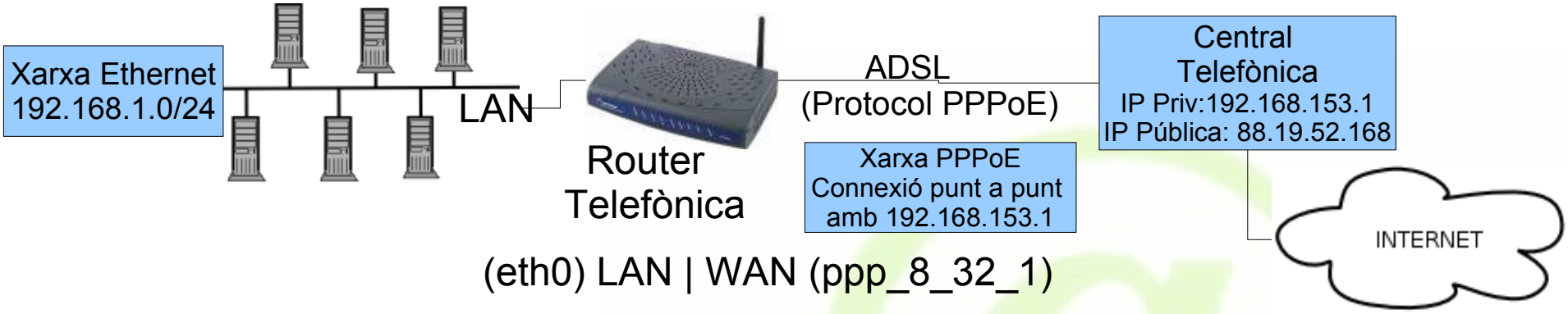


- **Objectius**
  - Màquina llindar entre xarxa local i Internet.
- **Requeriments**
  - 2 Targetes de Xarxa (eth0, eth1)
  - Ip forwarding activat (**echo 1 > /proc/sys/net/ipv4/ip_forward**)
  - Taules de rutes configurades
  - Interfície externa configurada amb ppp (pot ser IP pública o privada)
  - NAT configurat (iptables)

```
$ route
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
*               següent node    255.255.255.255 UH    0      0        0 eth1
192.168.1.0     *               255.255.255.0   U     0      0        0 eth0
```


Autor: Sergi Tur Badenas

Gateway (Router Comercial. Linux Adaptat)

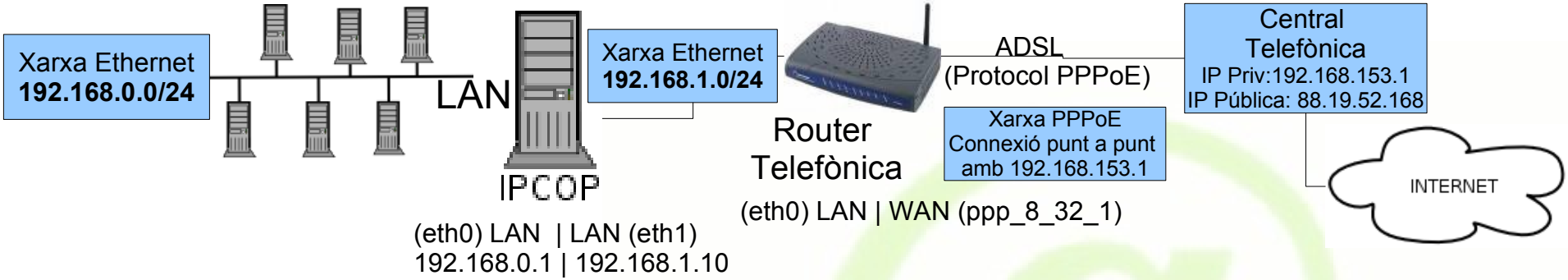


- **El router fa de gateway cap a Internet**
- **Utilitza NAT (SNAT) per compartir la connexió**
  - Pot utilitzar DNAT per fer accessible una màquina interna.
- **Taula de rutes del router:**

```
$ route
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
192.168.153.1   *               255.255.255.255 UH    0      0        0 ppp_8_32_1
192.168.1.0     *               255.255.255.0   U     0      0        0 eth0
default         192.168.153.1   0.0.0.0         UG    0      0        0 ppp_8_32_1
```


Autor: Sergi Tur Badenas

Gateway (IPCOP)



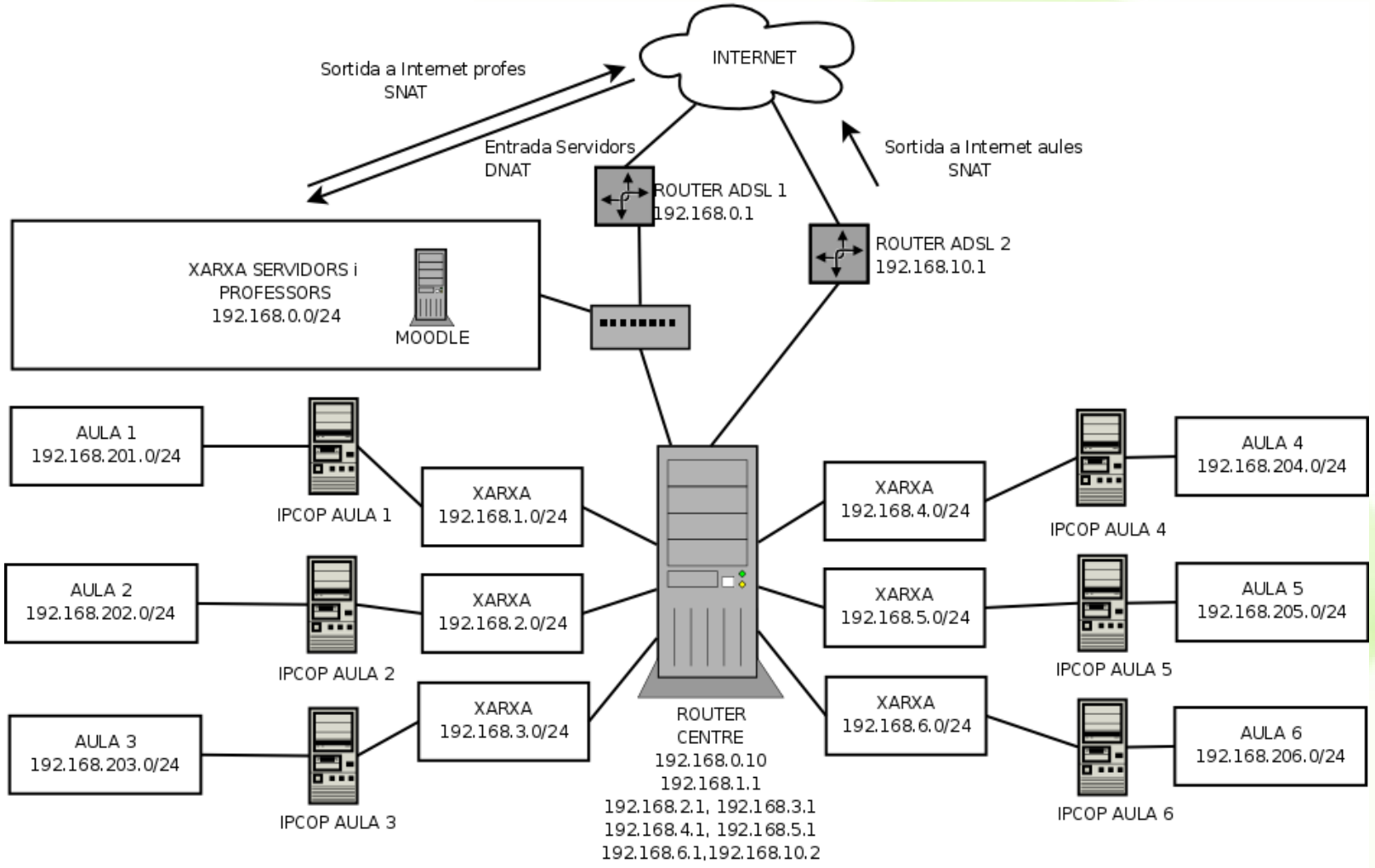
- **Linux BOX fàcil de configurar com a gateway**
  - Creem una subxarxa (192.168.0.0/24) separada per IPCOP de l'altra xarxa local (192.168.1.0/24)
- **Utilitza NAT (SNAT) per compartir la connexió**
  - **Pot utilitzar DNAT per fer accessible una màquina interna**

```
$ route
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
192.168.1.0     *               255.255.255.0   U     0      0        0 eth1
192.168.0.0     *               255.255.255.0         U     0      0        0 eth0
default         192.168.1.1     255.255.255.0         U     0      0        0 eth1
```


Autor: Sergi Tur Badenas

Xarxes WAN

- **Xarxa "WAN" del centre**



Autor: Sergi Tur Badenas

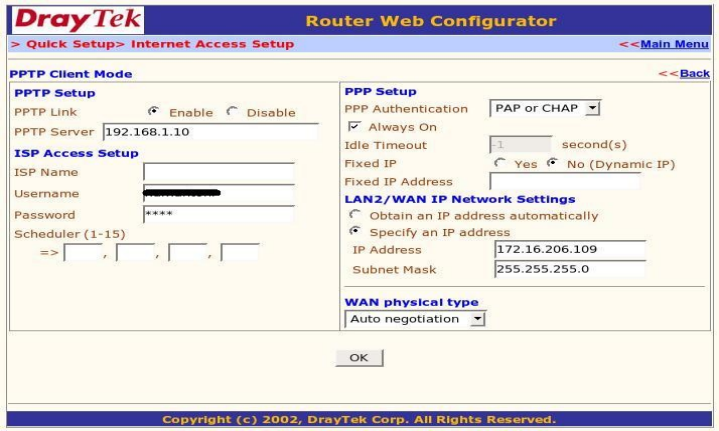
PPP (Point to Point Protocol)

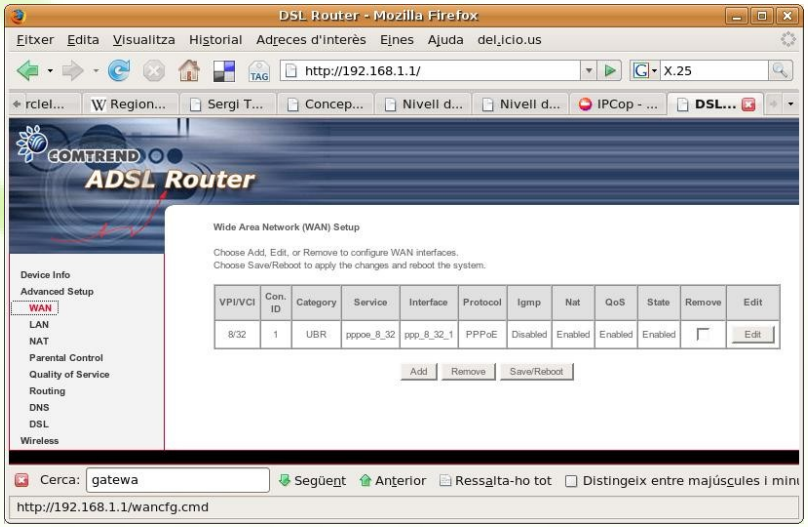
- **Protocol WAN (comunicacions node a node)**
- **Protocol de nivell 2 d'enllaç orientat a connexió**
- **Diverses subfamílies**
  - Point-to-Point Protocol over Ethernet (PPPoE) (ADSL o cable)
  - Point-to-Point Protocol over ATM (PPPoA)
  - Point-to-Point Protocol Tunneling (PPPT)
- **Paràmetres (proveïts pels ISP)**
  - Autenticació (Usuari i Password i protocol PAP/CHAP)
  - VPI/VCI
- **Proveïx d'autenticació i d'assignació dinàmica d'IP**
- **Successor de SLIP**

Autor: Sergi Tur Badenas

PPP (Point to Point Protocol)

- **Diferents opcions**
  - Linux BOX (interfícies ppp)
  - Routers|modems comercials (ADSL, cable)
  - IPCOP (Network DIAL-UP)
- **Enllaç a la wiki sobre PPP**





Autor: Sergi Tur Badenas

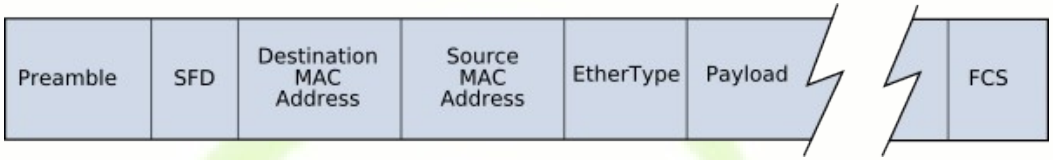
Firewall

- **Implementacions:**
  - Maquinari
  - Programari (Linux Box, firewalls personals)
- **Tipus de firewalls:**
  - Filtrat de paquets (nivell 3 xarxa)
    - Stateless firewalls
    - Stateful firewalls (tenen memòria sobre les connexions)
  - Nivell d'aplicació (TCP Wrappers) i d'aplicació (proxies)
  - Firewalls personals
- **Gairebé sempre s'ubiquen als llindars entre la xarxa local i la xarxa exterior però també es poden col·locar per separar dues subxarxes internes.**

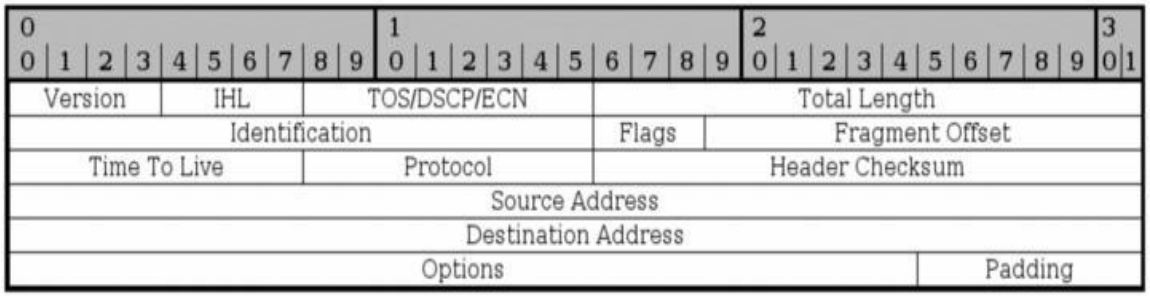
Autor: Sergi Tur Badenas

Firewall

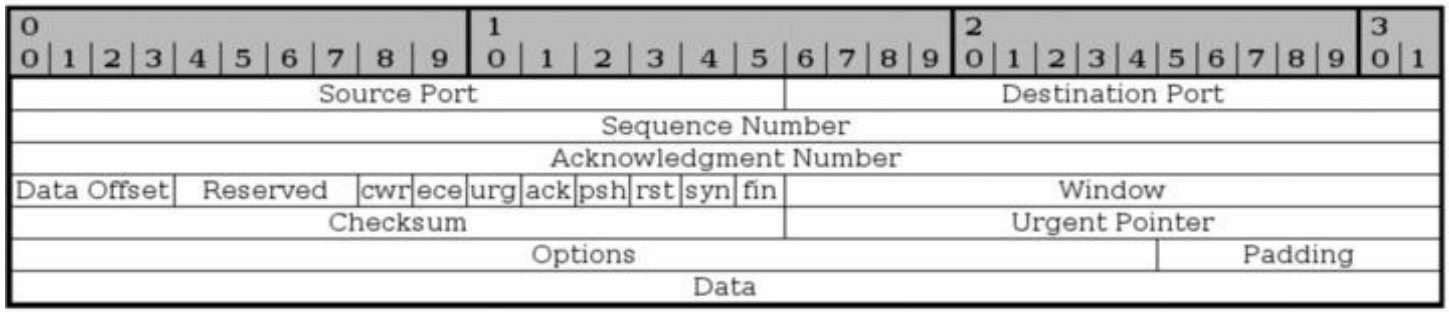
- **Nivell 1. Interfície de xarxa (Ethernet)**
  - Filtratge per MAC



- **Nivell 2. Internet. IP**
  - Filtratge per IP



- **Nivell 3. Transport. TCP**
  - Filtratge per ports (similar amb UDP)



Autor: Sergi Tur Badenas

NetFilter/iptables

- **Els sistemes Linux porten un sistema integrat en el seu kernel anomenat iptables.**
  - Successor d'ipchains.

Firewall Command	Linux Kernel Version
iptables	2.4.x, 2.6.x
ipchains	2.2.x
ipfwadm	2.0.x

- **Seguretat per defecte (en el nucli del sistema operatiu).**
  - No és cap servei. Menys vulnerable.
- **Té un elaborat, complet i complexe sistema de passos pels quals passa un paquet.**
  - El més important per entendre iptables és conèixer la seva semàntica i les capçaleres dels protocols TCP/IP.
- **Wiki sobre iptables**

Autor: Sergi Tur Badenas

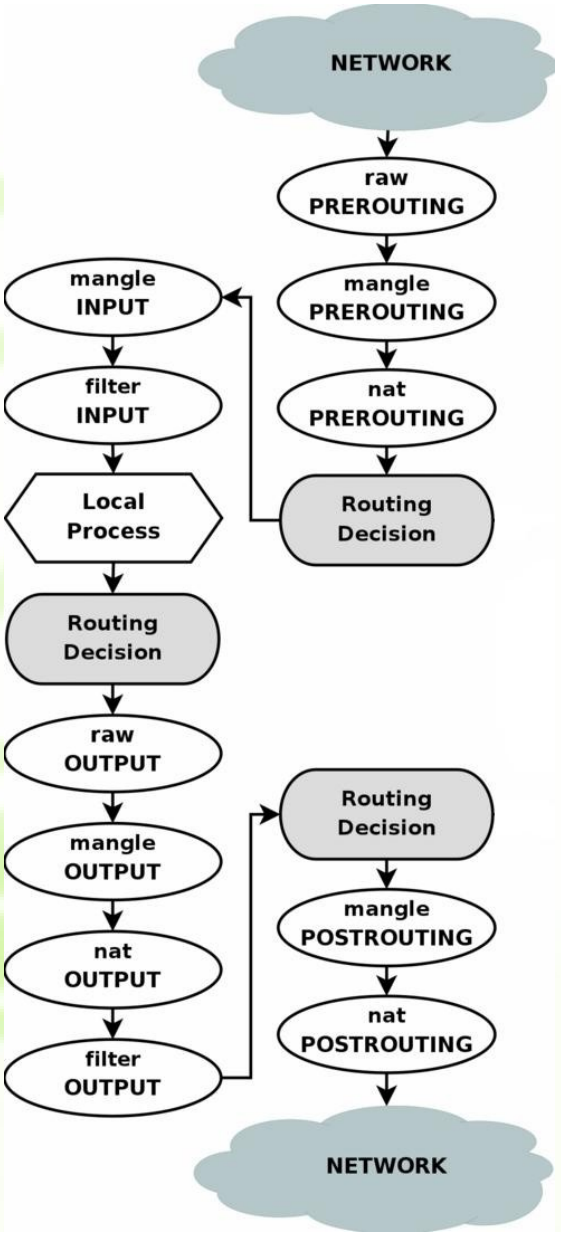
NetFilter/iptables

- **Conceptes**
  - **RULES**: condició + target. Les condicions poden ser:
    - ip d'origen o destinació, protocol, port, MAC, etc.
  - **TARGETS**: accions per dur a terme amb els paquets
    - ACCEPT, DROP, QUEUE, RETURN, REJECT, LOG, ULOG, DNAT, SNAT, MASQUERADE
  - **CHAINS**: grups de normes (ruleset) aplicables en cert moment del "cicle de vida" del paquet a iptables
    - INPUT, OUTPUT, FORWARD, PREROUTING, POSTROUTING
  - **TABLES**: separació de conceptes (filtrar, manipular, NAT)
    - RAW, FILTER, MANGLE, NAT
  - **POLICIES**: són les regles per defecte:
    - DROP, ACCEPT

Autor: Sergi Tur Badenas

NetFilter/iptables. Firewall no router

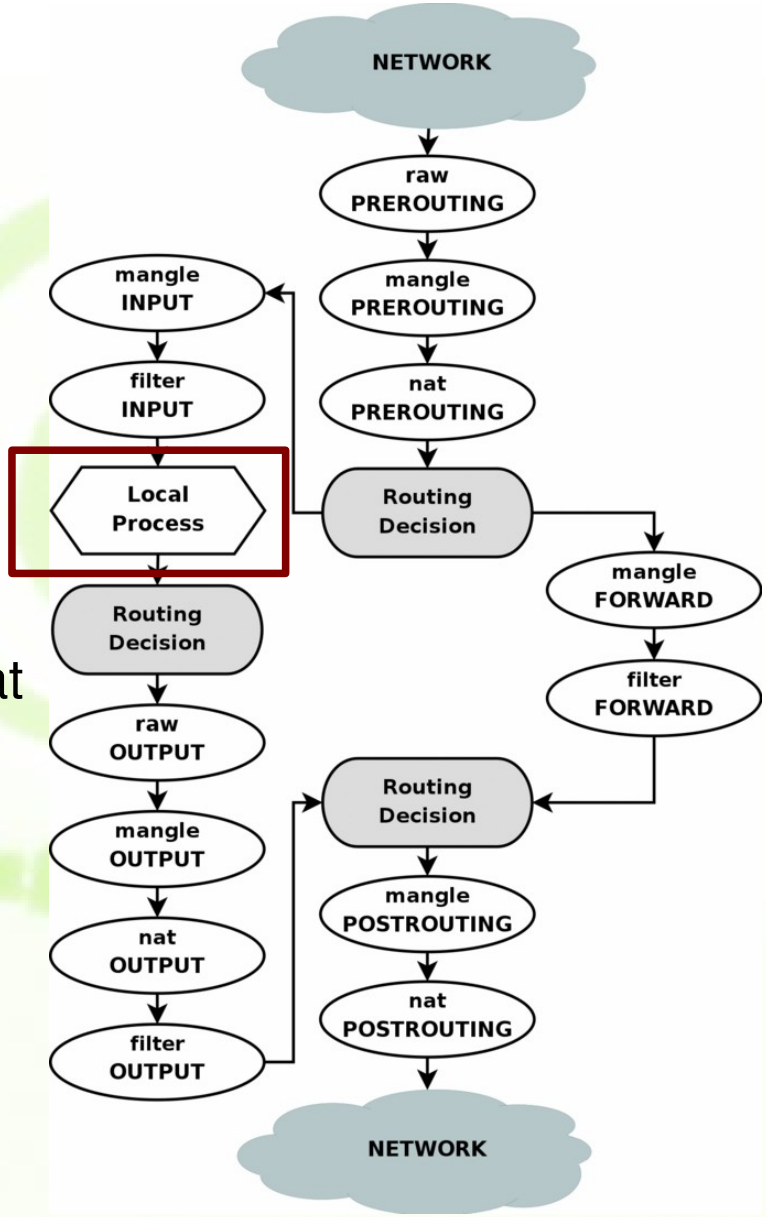
- **INPUT/OUTPUT**
  - Només filtra els paquets que tenen origen o destinació en la màquina on estem utilitzant iptables
  - L'utilitzem a una màquina que no sigui un encaminador (tallafocs personal o tallafocs en un servidor)
- **FILTER**
  - Bàsicament utilitzarem iptables com a filtre (firewall pur)



Autor: Sergi Tur Badenas

NetFilter/iptables. Firewall Router

- **FORWARDING**
  - Només s'utilitza en encaminadors i passarel·les (ip_forwarding activat)
  - No l'utilitzarem en tallafocs personals o servidors
- **Permet distingir entre els paquets dirigits al firewall i els paquets dirigits a la xarxa**
- **Local Processes**
  - Aplicacions de la màquina que té instal·lat iptables (Per exemple proxy web)
  - L'encaminador pot processar un paquet entrant (log, web proxy) i després encaminar-lo cap a la xarxa local
  - O pot simplement encaminar el paquet



Autor: Sergi Tur Badenas

Declaració de regles. Comanda iptables

- **Les regles s'estableixen amb la comanda iptables**
- **Exemple**
  - Permetre els paquets dirigits a la màquina que utilitzat iptables (INPUT), amb origen la xarxa local (clase C), que el protocol sigui TCP i els port de destinació el 22 (servei SSH)

```
$ sudo iptables -A INPUT -s 192.168.1.1/0 -p tcp --dport 22 -j ACCEPT
```

- **Les comandes iptables NO es guarden de forma permanent al sistema. Cal crear scripts d'inici.**
- **EXERCICI: Consultar en quin estat tenim iptables amb la comanda**

```
sudo iptables -L
```


Autor: Sergi Tur Badenas

Exemples d'ús iptables

- **Bloquejar pings locals**

```
$ sudo iptables -A INPUT -s 127.0.0.1 -p icmp -j DROP
```

- **Bloquejar pings màquina remota**

```
$ sudo iptables -A INPUT -s ip_company -p icmp -j DROP
```

- **Per eliminar les normes:**

```
$ sudo iptables -D INPUT -s 127.0.0.1 -p icmp -j DROP
$ sudo iptables -D INPUT -s ip_company -p icmp -j DROP
```

  - Depuració amb **tcpdump** (els paquets arriben a eth0!)
  - Depuració amb **nmap**

- **Wiki amb exemples d'ús d'iptables**

Autor: Sergi Tur Badenas

Comanda nmap

- **Instal·lació:**

```
$ sudo apt-get install nmap
```

- **Utilitat per escanejar ports**
  - Exemple: escanejar ports d'una màquina

```
$ sudo nmap 192.168.1.1
Starting Nmap 4.10 ( http://www.insecure.org/nmap/ ) at 2007-01-21
12:25 CET
Interesting ports on 192.168.1.1:
Not shown: 1676 closed ports
PORT    STATE SERVICE
21/tcp open  ftp
23/tcp open  telnet
80/tcp open  http
MAC Address: 00:15:E9:CA:34:A5 (D-Link)
```

  - Permet conèixer si els ports estan filtrats per un firewall (filtered)
- **Pot ser útil per localitzar màquines en una xarxa**

```
$ sudo nmap 192.168.1.1-255
```

```
$ sudo nmap -p0 192.168.1.1-255
```


Autor: Sergi Tur Badenas

Depuració comanda tcpdump

- **Atenció:**
  - Cal tenir en compte que els paquets arriben a la màquina però són rebutjats pel Kernel
  - Exemple per parelles amb ping- Hi ha ping però no pong!

```
192.168.1.6 $ ping 192.168.1.2
PING 192.168.1.2 (192.168.1.2) 56(84) bytes of data.
```

```
192.168.1.2 $ sudo tcpdump icmp
listening on eth0, link-type EN10MB (Ethernet), capture size 96 bytes
12:37:59.008019 IP portatil.local > casa-linux.local: ICMP echo request, id 55322, seq 1, length 64
```

```
$ sudo watch -n 1 iptables -nvL
Every 10,0s: iptables -nvL
                Tue Oct 23 12:42:24 2007
Chain INPUT (policy ACCEPT 2260 packets, 379K bytes)
 pkts bytes target     prot opt in     out     source               destination
  266 22344 DROP       icmp --  *      *       192.168.1.6          0.0.0.0/0
.....................................................
```


Autor: Sergi Tur Badenas

Exemples d'ús iptables

- **Instal·leu ssh**

```
$ sudo apt-get install ssh
```

- **Creu una norma per prohibir l'accés a un company**

```
$ sudo iptables -A INPUT -s ip_company -p tcp --dport 22 -j DROP
```

- **Proveu amb la comanda nmap a veure si el port esta filtrat**

```
$ sudo nmap localhost
Starting Nmap 4.10 ( http://www.insecure.org/nmap/ ) at
2007-01-21 12:55 CET
Interesting ports on casa-linux (127.0.0.1):
Not shown: 1664 closed ports
PORT     STATE    SERVICE
22/tcp   filtered ssh
25/tcp   open     smtp
80/tcp   open     http
.........................
```


Autor: Sergi Tur Badenas

DROP vs REJECT

- **DROP**
  - Impedeix el pas del paquet silenciosament sense informar al emissor

```
$ ping 192.168.1.2
PING 192.168.1.2 (192.168.1.2) 56(84) bytes of data.
```

- **REJECT**
  - Impedeix el pas del paquet amb avis a l'emissor

```
$ sudo iptables -D INPUT -s 192.168.1.6 -p icmp -j DROP
$ sudo iptables -A INPUT -s 192.168.1.6 -p icmp -j REJECT
```

```
$ ping 192.168.1.2
PING 192.168.1.2 (192.168.1.2) 56(84) bytes of data.
64 bytes from 192.168.1.2: icmp_seq=432 ttl=64 time=1.21 ms
From 192.168.1.2 icmp_seq=449 Destination Port Unreachable
From 192.168.1.2 icmp_seq=450 Destination Port Unreachable
```


Autor: Sergi Tur Badenas

NetFilter/iptables. Polítiques

- **Política permissiva per defecte (ACCEPT)**

```
$ sudo iptables -F
$ sudo iptables -X
$ sudo iptables -Z
$ sudo iptables -t nat -F
$ sudo iptables -P INPUT ACCEPT
$ sudo iptables -P OUTPUT ACCEPT
$ sudo iptables -P FORWARD ACCEPT
$ sudo iptables -t nat -P PREROUTING ACCEPT
$ sudo iptables -t nat -P POSTROUTING ACCEPT
```

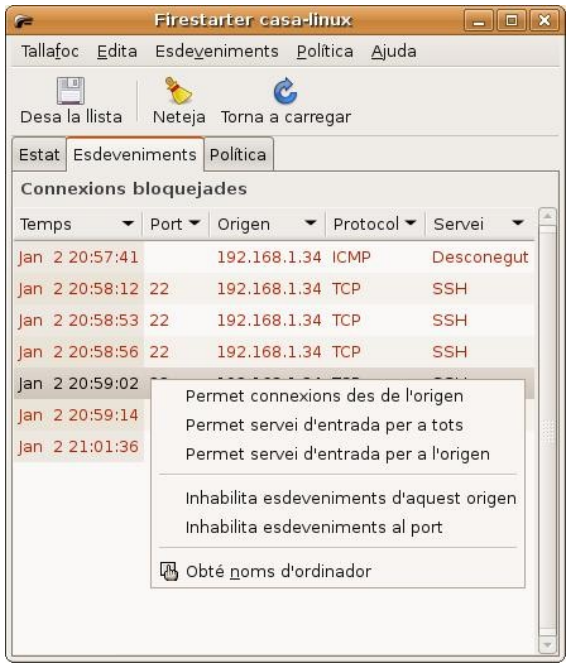
- **Política no permissiva per defecte (DROP)**

```
$ sudo iptables -F
$ sudo iptables -X
$ sudo iptables -Z
$ sudo iptables -t nat -F
$ sudo iptables -P INPUT DROP
$ sudo iptables -P OUTPUT DROP
$ sudo iptables -P FORWARD DROP
$ sudo iptables -t nat -P PREROUTING DROP
$ sudo iptables -t nat -P POSTROUTING DROP
```


Autor: Sergi Tur Badenas

Firestater

- **Firewall personal per a Linux**



- **Wiki amb exemples amb firestarter**

```
$ sudo apt-get install firestarter
```


Autor: Sergi Tur Badenas

Firestater

- **Exercici**
  - Consulteu quina és la política per defecte de firestarter
  - El notificador d'esdeveniments de firestarter us avisara quan hi hagin esdeveniments de xarxa. Proveu de denegar un esdeveniment qualsevol i d'acceptar un altre
  - Consulteu com firestarter configura iptables
  - Finalment apagueu firestarter i assegureu-vos que no iptables no té cap regla i que la seva política per defecte és acceptar.

Autor: Sergi Tur Badenas

Establir normes iptables a l'inici del sistema

- **Un cop configurat iptables executar:**

```
$ iptables-save > /etc/firewall.conf
```

- **I executar iptables-restore a l'iniciar la xarxa**

```
$ echo "#!/bin/sh" > /etc/network/if-up.d/iptables
$ echo "iptables-restore < /etc/firewall.conf" >> /etc/network/if-up.d/iptables
$ chmod +x /etc/network/if-up.d/iptables
```

- **O modificar el fitxer /etc/network/interfaces**

```
auto eth0
iface eth0 inet dhcp
pre-up cat /etc/firewall.conf | iptables-restore
```

- **Apunts a la wiki**

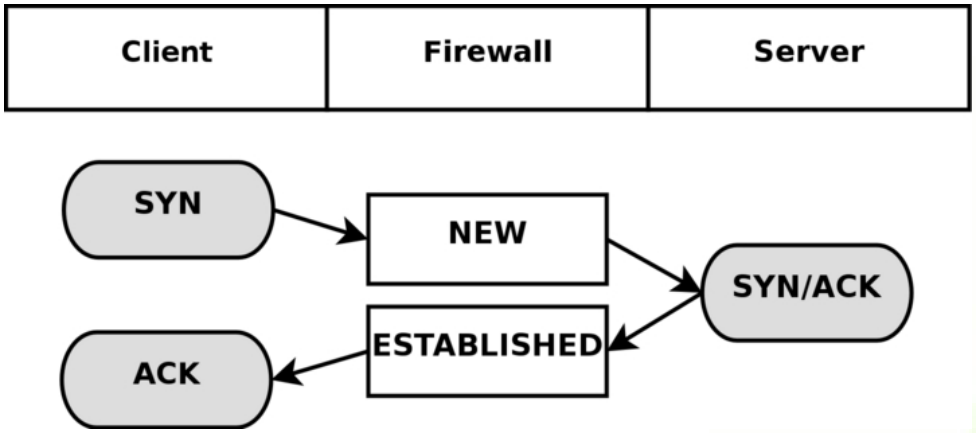
Autor: Sergi Tur Badenas

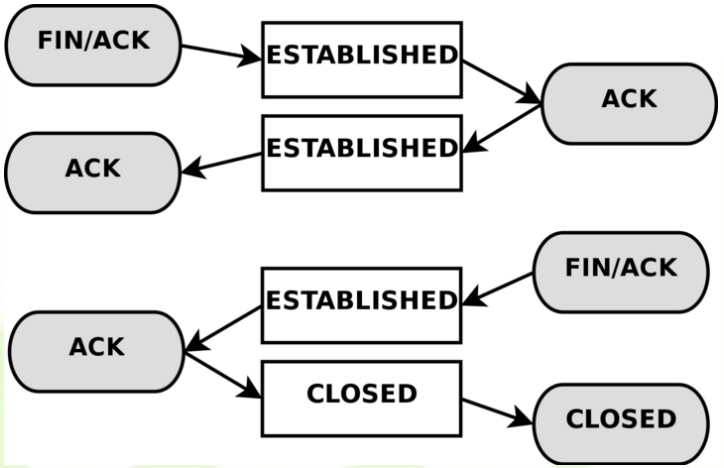
NAT (Traducció d'adreça de xarxa)

- **Network Address Translation**
  - És un estàndard creat de la Internet Engineering Task Force (IETF). Creat per lluitar contra la falta d'IPs.
- **Dos usos, dos tipus de NAT**
  - **SNAT (Source NAT):** Compartir una connexió a Internet. Permet compartir una adreça vàlida d'Internet entre diverses adreces de xarxa privades.
  - **DNAT (Destination NAT):** Permet accedir als serveis d'una màquina local.
- **Funcionament**
  - Canvia les adreces d'Internet (SNAT adreces origen i DNAT adreces destinació) de les capçaleres IP.

Autor: Sergi Tur Badenas

Connection Tracking





- **iptables pot controlar l'estat de les connexions dels protocols TCP, UDP i ICMP.**
- **SNAT. Compartició de la connexió.**
  - Que passa amb els paquets de retorn (P. ex. retorn d'una pàgina web consultada per un PC local)?
    - Com podem recordar, les connexions, un cop s'estableix una connexió, ja es recorda el seu origen.

Autor: Sergi Tur Badenas

Exemple de SNAT

- **Flash Cisco sobre NAT**
- **Utilitzat en les màquines que fan de gateway**
  - Els requisits que explicàvem abans per als gateways també s'apliquen ara.
- **SNAT també és conegut com Masquerade**
  - De fet, masquerade és millor ja que permet que el gateway tingui una IP dinàmica.
- **Exemple de configuració SNAT:**
  - On aquesta comanda s'executa al gateway de la xarxa LAN

```
$ sudo iptables -t nat -A POSTROUTING -s 192.168.1.0/24 -o eth0 -j MASQUERADE
```


Autor: Sergi Tur Badenas

Exemple de DNAT

- **Configuració per interfície gràfica**

DrayTek — Router Web Configurator

> Advanced Setup> NAT Setup> Port Redirection <<Main Menu

Port Redirection Table <<Back

Index	Service Name	Protocol	Public Port	Private IP	Private Port	Active
1	ssh	TCP	22	10.0.3.234	22	☑
2	smtp	TCP	110	10.0.3.234	110	☑
3	pop3	TCP	25	10.0.3.234	25	☑
4	www	TCP	80	10.0.3.234	80	☑
5	ssh2	TCP	24	10.0.2.2	22	☑
6	www2	TCP	8080	10.0.2.2	80	☑
7	webmin2	TCP	10000	10.0.2.2	10000	☑
8		---	0		0	☐
9		---	0		0	☐
10		---	0		0	☐

OK

Autor: Sergi Tur Badenas

Linux Box 1. IPCOP

- **IPCOP és una distribució Linux**
  - Pocs requeriments de hardware.
  - Permet crear fàcilment una passarel·la amb serveis extres (firewall, DNS, DHCP, VPN, etc.)
  - Els serveis són ampliables a través de mòduls
  - L'utilitzarem conjuntament amb Virtual Box per fer proves d'encaminadors, gateways (NAT) i proxy Squid
- **Pràctica de configuració bàsica**
  - Saber configurar una màquina Linux Box bàsica.

Autor: Sergi Tur Badenas

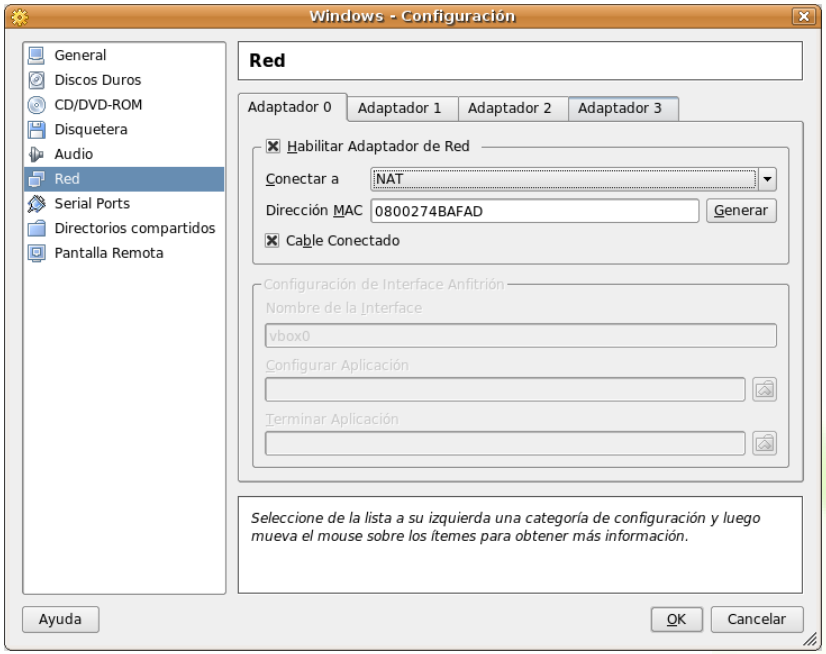
Màquines virtuals i interfícies de xarxa

- **Es pot simular tenir N targetes de xarxa amb una sola targeta de xarxa?**
  - Si mitjançant màquines Virtuals (VMWare, Virtual Box...)
  - Les màquines Virtuals suporten diferents tipus de xarxes. En el cas de Virtual Box ("Botó Configuració/Opció Xarxa"):
    - **No connectat**: sense xarxa
    - **NAT:** El PC on s'allotja la màquina virtual fa de passarel·la de la màquina virtual
    - **Interfície amfitriona/Bridged:** La màquina virtual esta a la mateixa xarxa que l'amfitrió però amb una IP diferent.
    - **Xarxa interna:** Una xarxa nova aïllada on només estan les màquines virtual en execució

Autor: Sergi Tur Badenas

Màquines virtuals i interfícies de xarxa

Xarxa amb NAT



IP assignada per DHCP. La màquina amfitriona fa de servidor DHCP

Màquina Virtual

XARXA VIRTUAL
10.0.2.0/255.255.255.0

La màquina amfitriona fa d'encaminador amb una sola targeta de xarxa!

Màquina Amfitriona

AULA DE PRÀCTIQUES
Aula1: 192.168.201.0/24
Aula4: 192.168.204.0/24

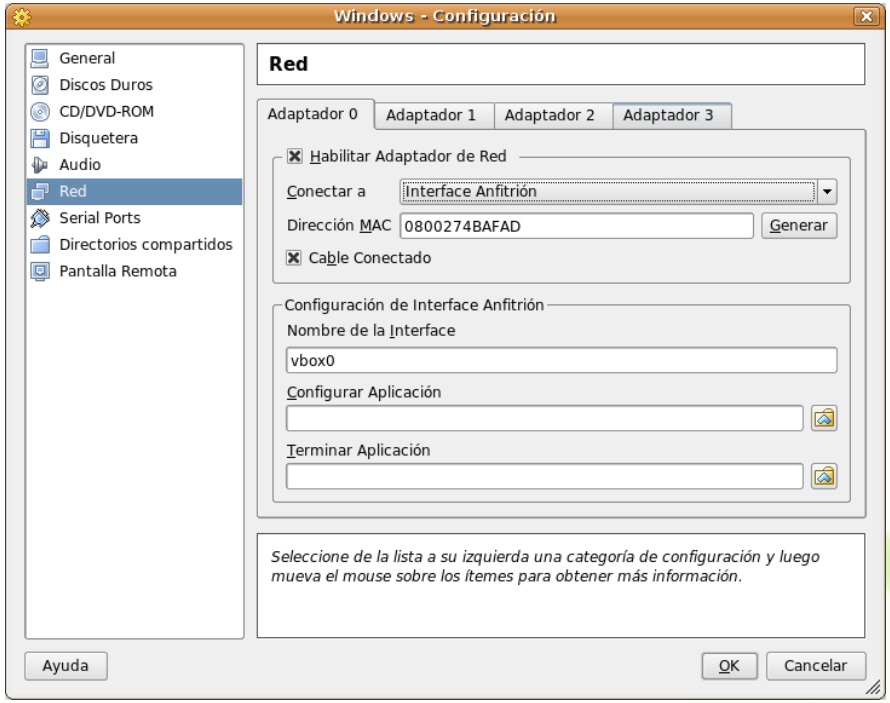
INTERNET

IPCOP AULA

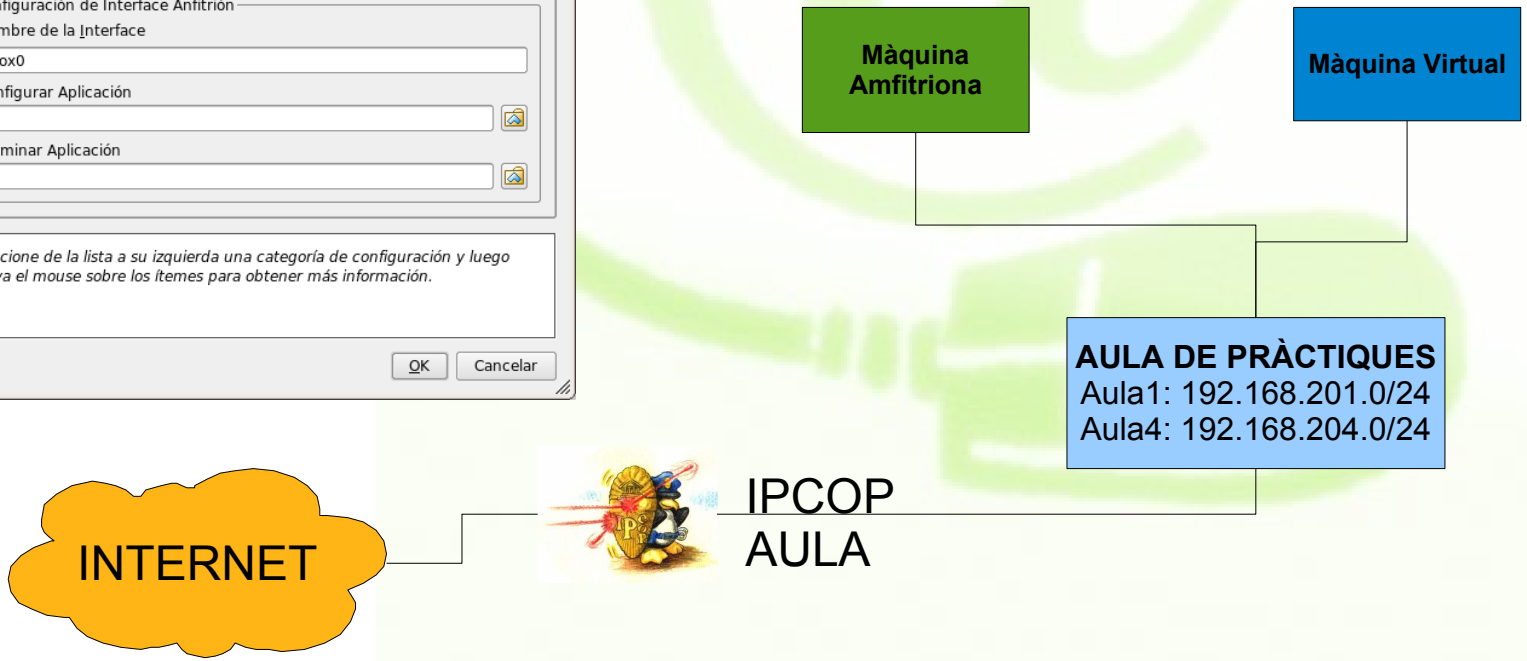
Autor: Sergi Tur Badenas

Màquines virtuals i interfícies de xarxa

Xarxa amb Interfície amfitriona/Bridged



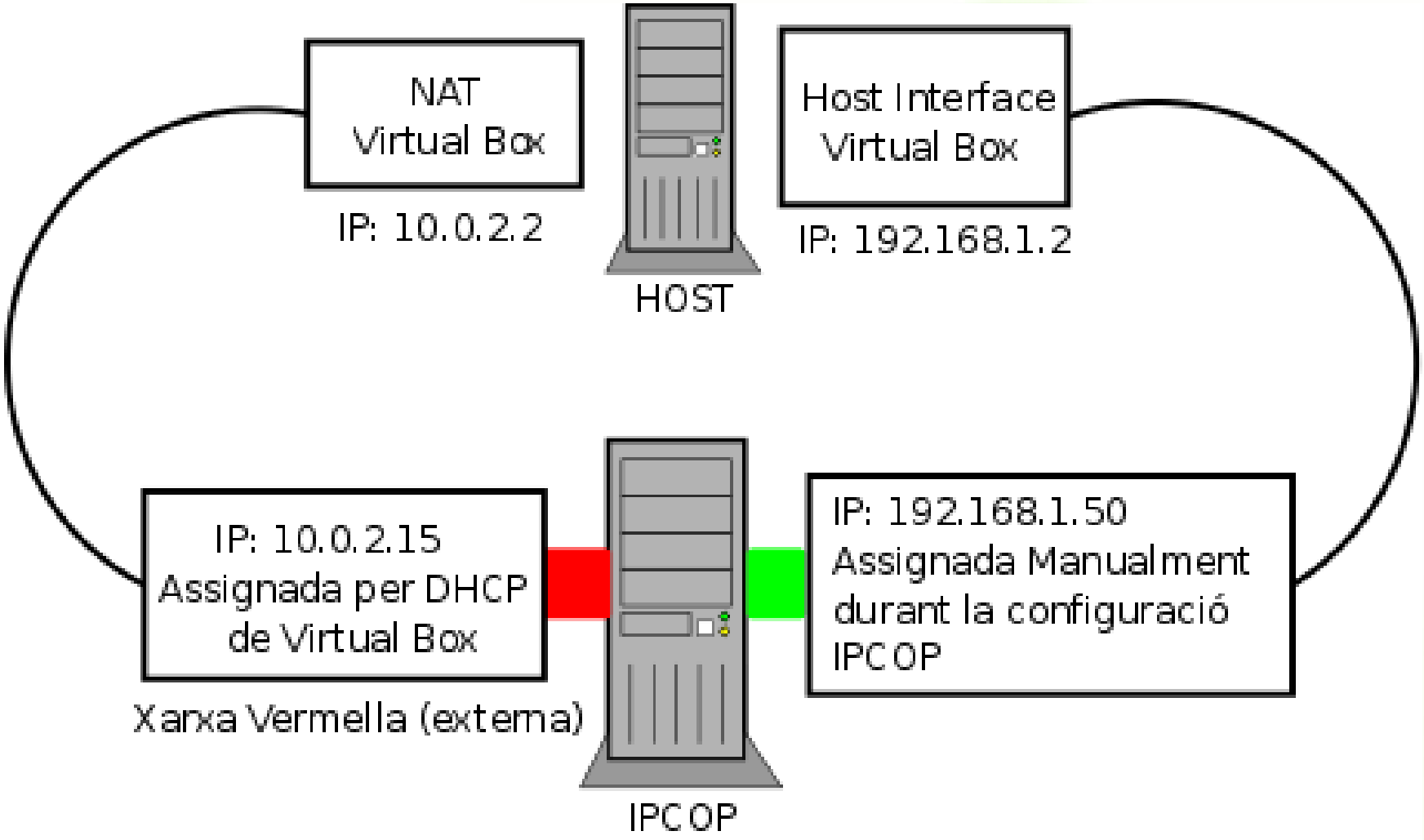
Tant la màquina virtual com la màquina amfitriona estan a la mateixa xarxa (xarxa habitual)



Autor: Sergi Tur Badenas

Virtual Box + IPCOP

- **Esquema de xarxa**

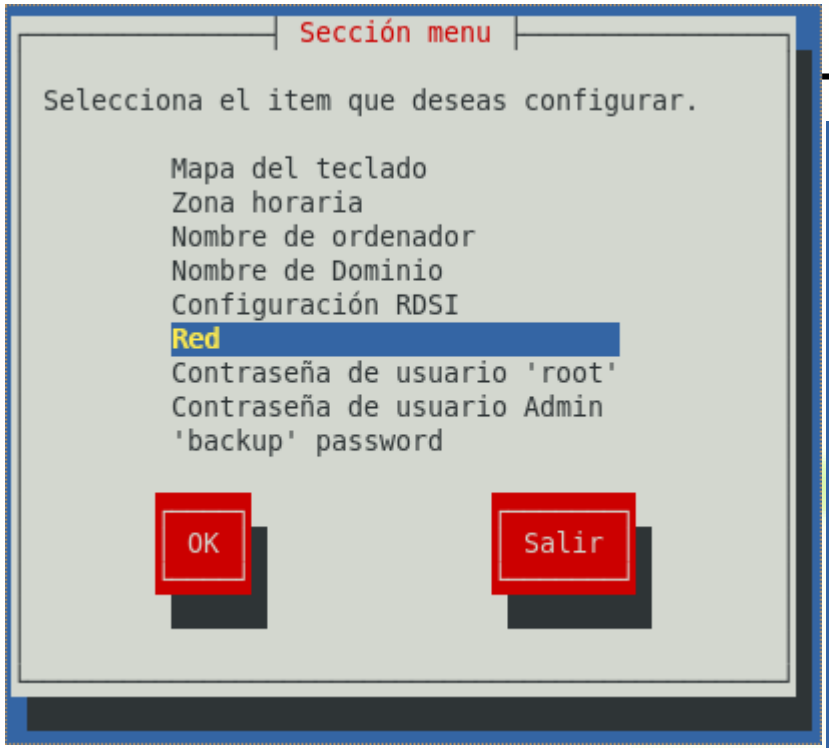


Autor: Sergi Tur Badenas

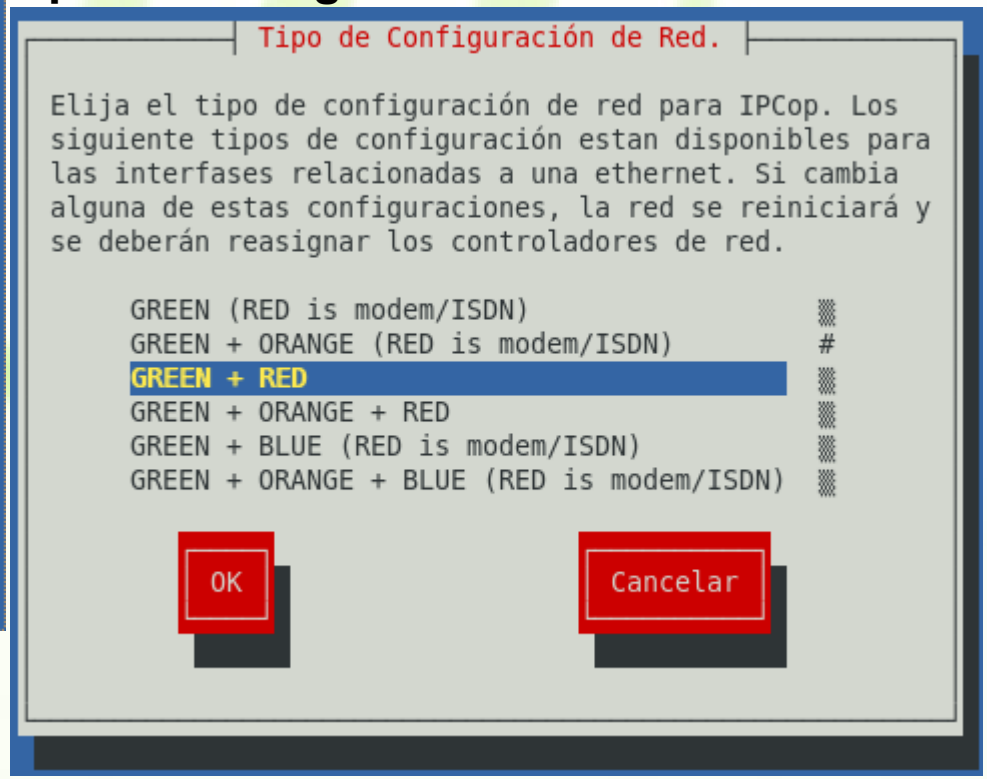
Virtual Box + IPCOP

- **Per la pràctica cal configurar IPCOP executant:**

```
# setup
```



Tipo de Configuración de Red: RED+GREEN

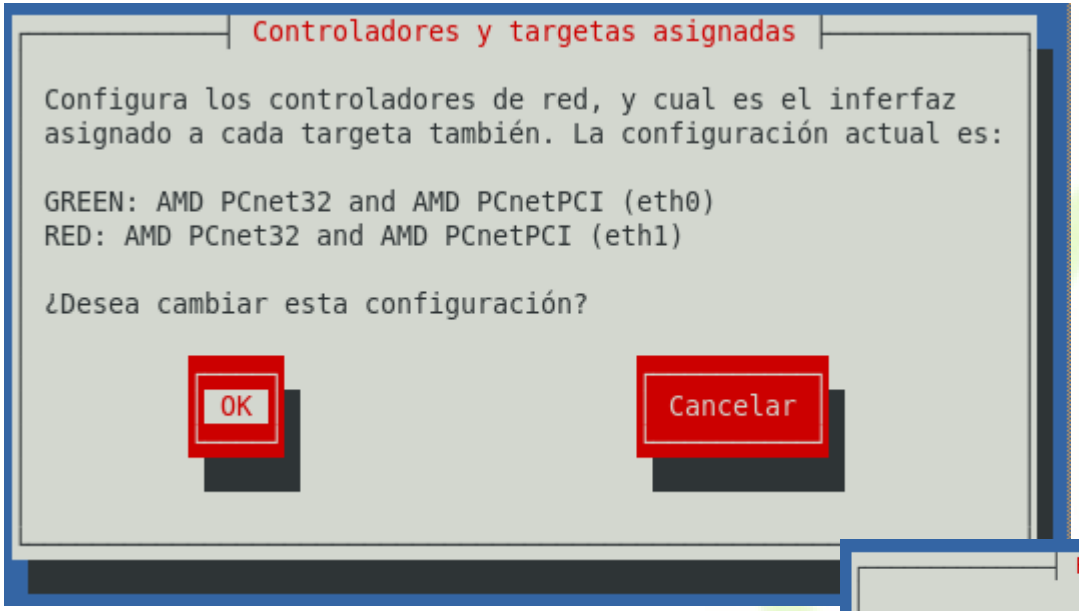


- Apunts a la wiki

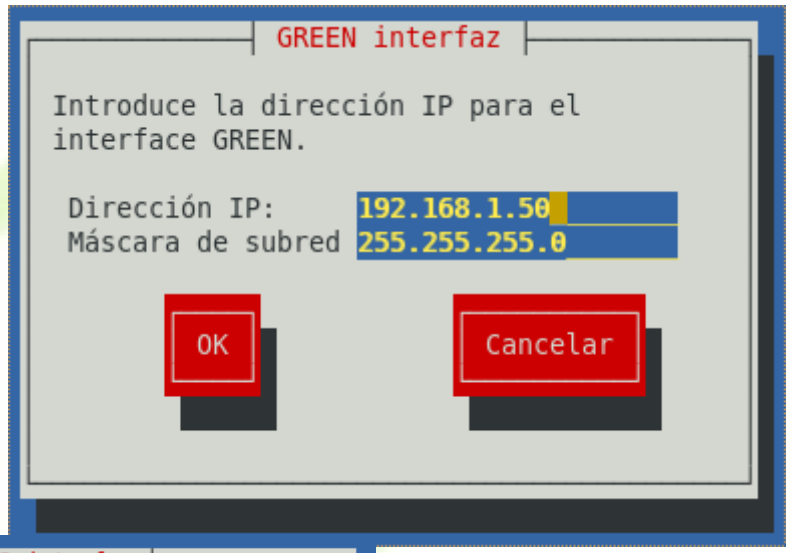
Autor: Sergi Tur Badenas

Virtual Box + IPCOP

Controladores y targetas asignadas:



Configuración de direcciones: GREEN manual



Configuración de direcciones: RED la posem en DHCP

GREEN:

• Cadascú ha de posar una IP lliure de la xarxa on feu les pràctiques:

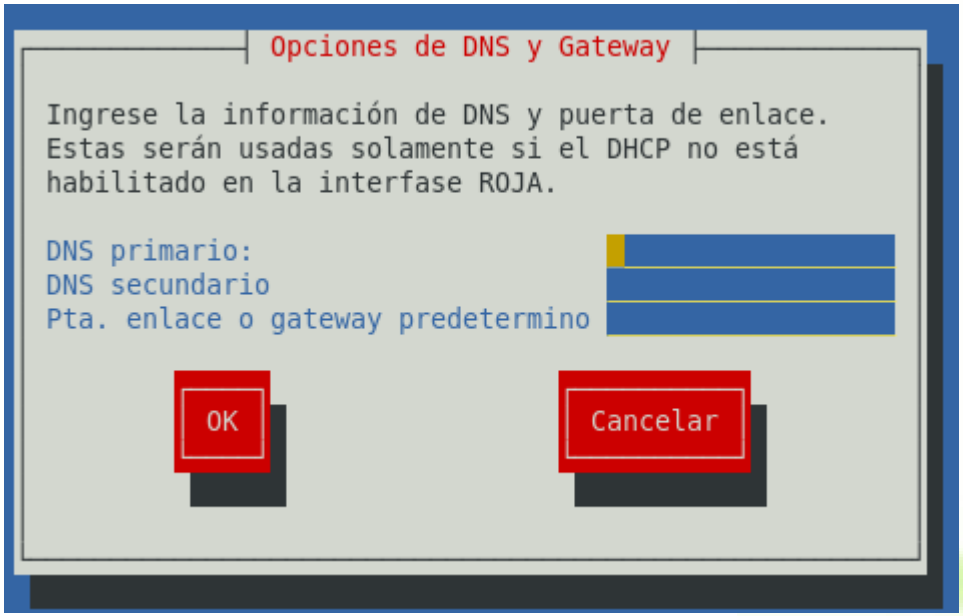
AULA 1: 192.168.201.0/24

AULA 2: 192.168.201.0/24.

Autor: Sergi Tur Badenas

Virtual Box + IPCOP

DNS i Gateway buits (configurat per DHCP)



DHCP desactiu

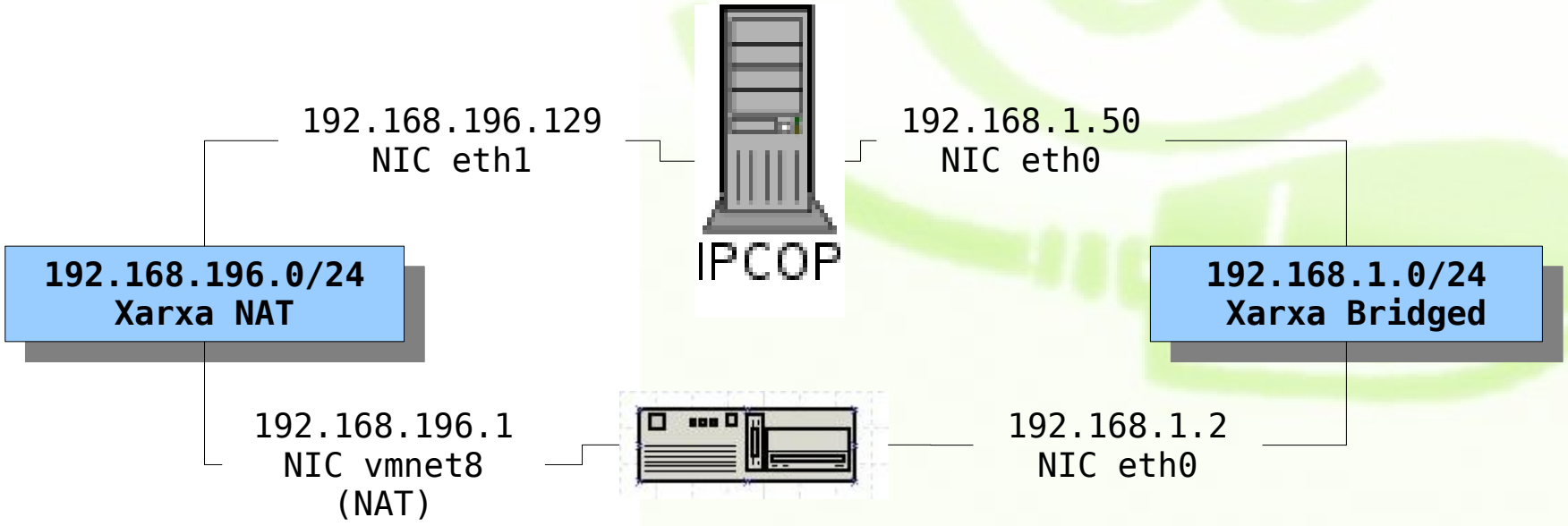
Autor: Sergi Tur Badenas

Vmware + IPCOP

- **Vmware NAT**

/etc/vmware/vmnet8/nat/nat.conf

```
$ route
Kernel IP routeing 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         mygateway1.ar7  0.0.0.0         UG    0      0        0 eth0
```



Autor: Sergi Tur Badenas

Vmware + IPCOP. NAT

- **Configuració NAT de vmware**

```
# Linux NAT configuration file
[host]
# NAT gateway address
ip = 192.168.196.2
netmask = 255.255.255.0
.................................................
#WEB
8888 = 192.168.196.129:80

# SSH
#       ssh -p 8889 root@localhost
8889 = 192.168.196.128:22
.....................................
```

- **Amb els ports NATS podem accedir a ports del IPCOP des de la interfície externa.**
  - Podem utilitzar DNAT d'IPCOP per accedir a màquines de la interfície interna.

Autor: Sergi Tur Badenas

Linux Box 1. IPCOP

- **Configuració**

```
root@vmwarez-ipcop:~ # setup
```

- **Accés web (port 81)**

```
http://ip_maquina_ipcop:81
```

- **Accés remot SSH (port 222)**

```
$ ssh -p 222 root@192.168.1.50
```

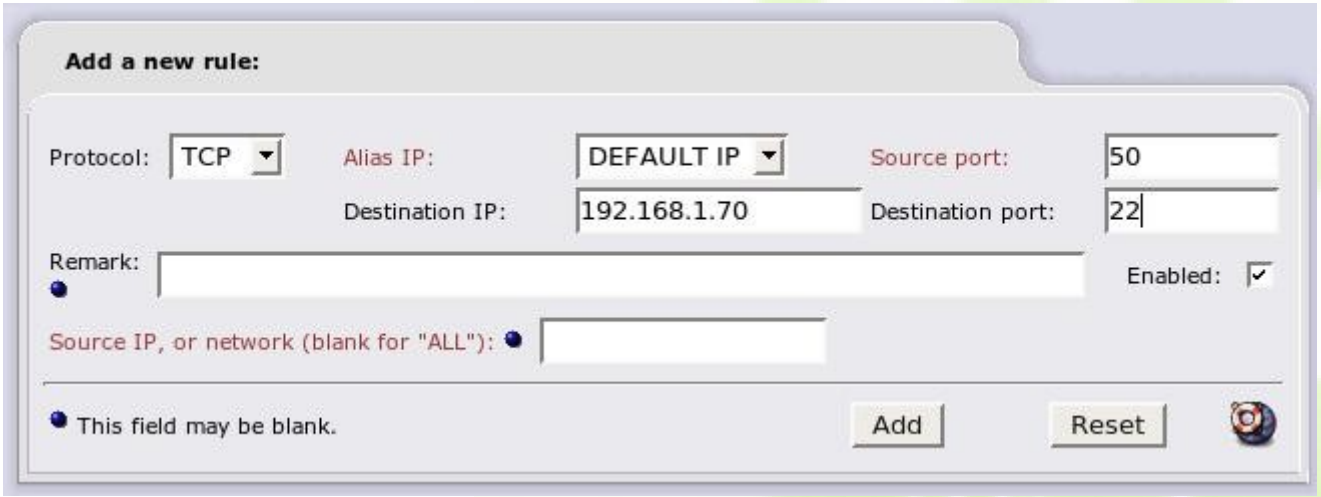
- **Accés NAT (fitxer /etc/vmware/vmnet8/nat/nat.conf)**

```
http://localhost:portNAT
```


Autor: Sergi Tur Badenas

IPCOP. DNAT

- **DNAT**
  - Redireccionem ports externs a ports de màquines de la xarxa interna



- **Podem comprovar els ports amb**

```
$ telnet localhost port
```

```
$ sudo nmap localhost
```


Autor: Sergi Tur Badenas

Linux Box 1. IPCOP 1

- **Exercici**
  - Configurar IPCOP amb la comanda setup
  - Per parelles, cadascú ha de modificar la seva configuració de xarxa per utilitzar com a gateway l'IPCOP del company.
  - Comprovar la connexió de xarxa i l'encaminament amb la comanda **traceroute.**
- **Només amb VMWare**
  - Accedir via NAT a algun port redireccionat amb DNAT de la màquina del company. Per exemple al posar http://localhost:8888 accedim a l'apache del company
    - Cal modificar el fitxer /etc/vmware/vmnet8/nat.conf
    - Apagar vmare i reiniciar vmware amb

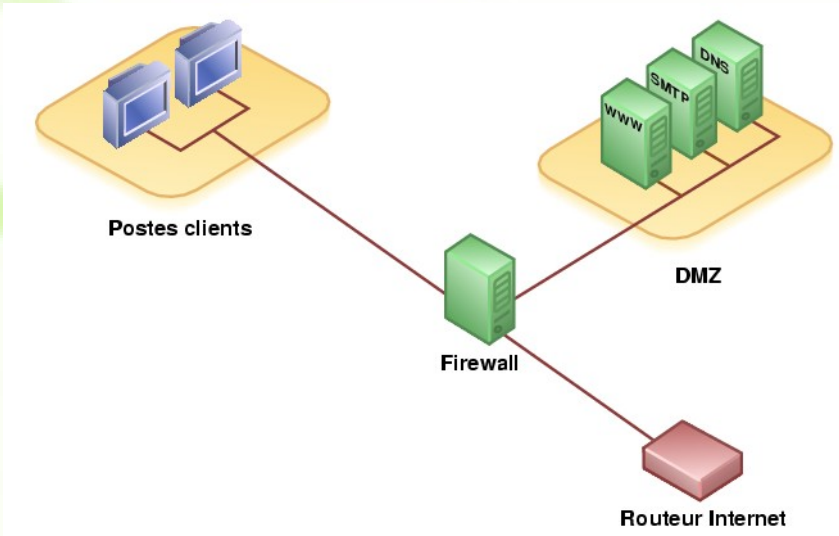
      ```
      $ sudo /etc/init.d/vmware restart
      ```
    - Instal·lar apache:

      ```
      $ sudo apt-get install apache2
      ```
    - Configurar IPCOP per fer DNAT i comprovar que tot funciona correctament

Autor: Sergi Tur Badenas

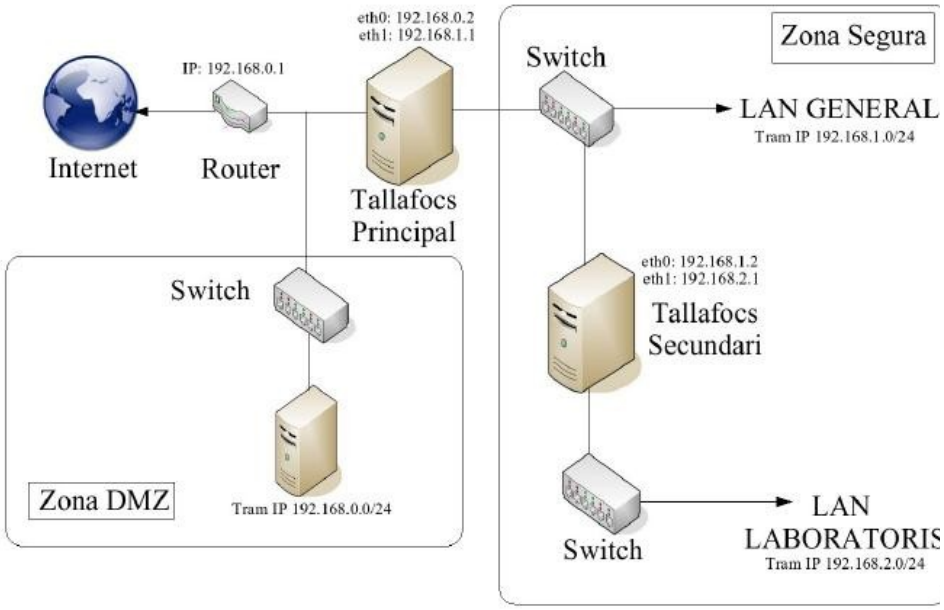
DMZ. Demilitarized Zone

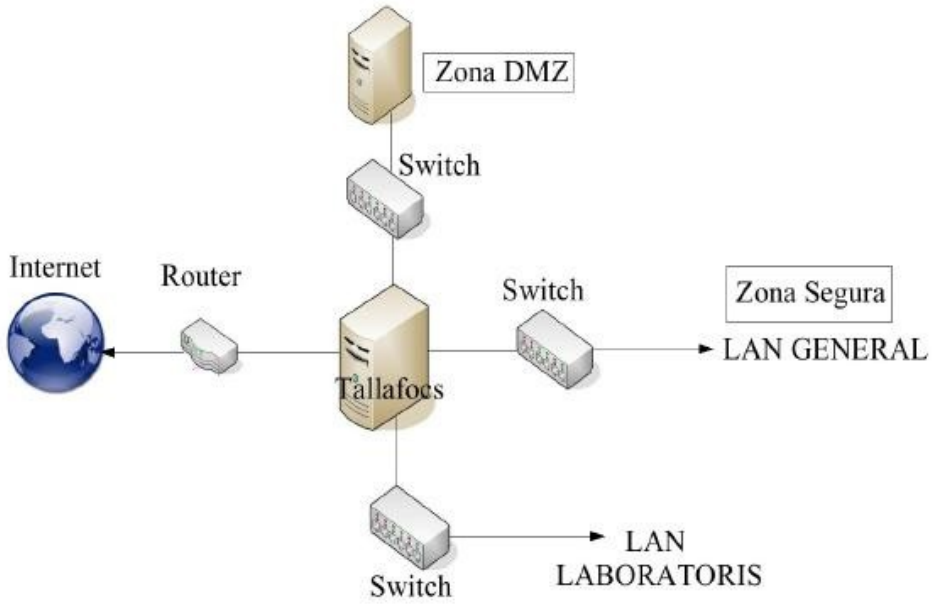
- DMZ és una subxarxa situada al perímetre entre la xarxa local i la xarxa externa.
- L'accés a DMZ esta permès des de l'exterior i l'interior. En canvi des de la DMZ només es pot accedir a l'exterior.
- L'objectiu és evitar l'accés a la xarxa en cas de que la zona DMZ es vegi compromesa. Si situen les màquines que han de donar serveis a l'exterior (servidor web, de correu, DNS, etc).R
- Router 3 ports i 2 subxarxes
- 2 tallafocs (screened-subnet firewall).
- En routers domèstics s'anomena "DMZ host"



Autor: Sergi Tur Badenas

Exemple de xarxa d'una escola





- Servidor WEB (port 80 i 443) (global)
- Servidor PROXY (port 3128). (xarxa interna)
- Servidor SAMBA i WINS (ports 137 i 138) (xarxa interna
- Servidor de correu SMTP i POP3 (pots 25 i 110) (global)
- Connexions segures SSH (port 22) (global)
- Encaminador

Autor: Sergi Tur Badenas

Exemple de xarxa d'una escola

- **Permetre l'accés als serveis desitjats i limitar la resta**

```
$ sudo iptables -A INPUT -s 0.0.0.0/0 -p tcp --dport 22 -j ACCEPT
$ sudo iptables -A INPUT -s 0.0.0.0/0 -p tcp --dport 25 -j ACCEPT
$ sudo iptables -A INPUT -s 0.0.0.0/0 -p tcp --dport 80 -j ACCEPT
$ sudo iptables -A INPUT -s 0.0.0.0/0 -p tcp --dport 110 -j ACCEPT
$ sudo iptables -A INPUT -s 0.0.0.0/0 -p tcp --dport 137 -j ACCEPT
$ sudo iptables -A INPUT -s 0.0.0.0/0 -p tcp --dport 138 -j ACCEPT
$ sudo iptables -A INPUT -s 0.0.0.0/0 -p udp --dport 137 -j ACCEPT
$ sudo iptables -A INPUT -s 0.0.0.0/0 -p udp --dport 138 -j ACCEPT
$ sudo iptables -A INPUT -s 0.0.0.0/0 -p tcp --dport 443 -j ACCEPT
$ sudo iptables -A INPUT -s 0.0.0.0/0 -i eth0 -p tcp --dport 1:1024 -j
DROP
$ sudo iptables -A INPUT -s 0.0.0.0/0 -i eth0 -p udp --dport 1:1024 -j
DROP
```

- **Permetre l'accés a Internet des de la xarxa interna (SNAT)**

```
$ sudo iptables -A FORWARD -s 192.168.1.0/24 -i eth1 -p tcp -dport 80 -j ACCEPT
$ sudo iptables -A FORWARD -s 192.168.1.0/24 -i eth1 -p tcp -dport 443 -j ACCEPT
$ sudo iptables -A FORWARD -s 192.168.1.0/24 -i eth1 -j DROP
$ sudo iptables -t nat -A POSTROUTING -s 192.168.1.0/24 -o eth0 -j MASQUERADE
echo 1 > /proc/sys/net/ipv4/ip_forward
```


Autor: Sergi Tur Badenas

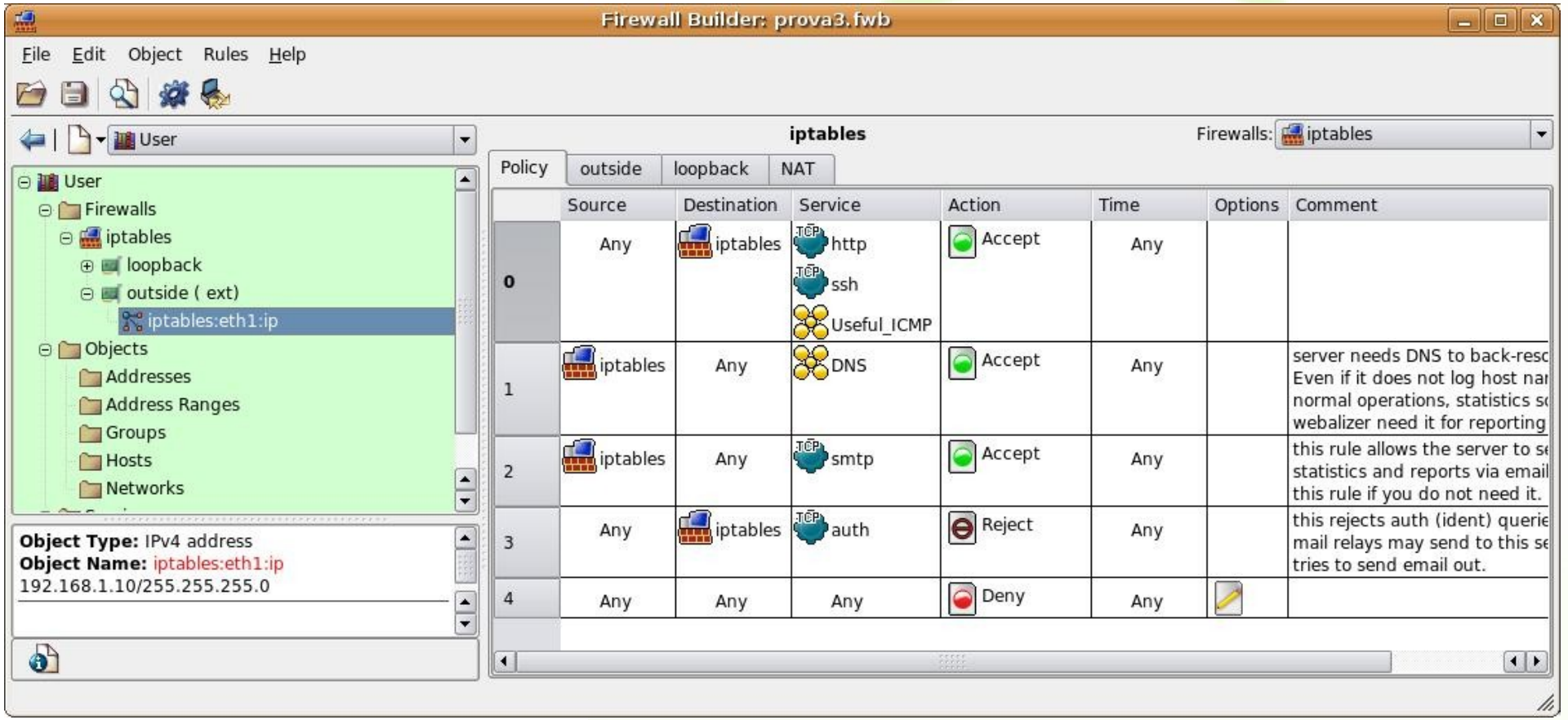
fwbuilder

- **Interfície gràfica per la creació de normes de firewalls**
  - Suporta diversos Firewalls (Cisco PIX, iptables, ipfilter) i Sistemes Operatius (Linux, BSD, Cisco)
  - Té un assistent per crear firewalls amb plantilles per a les configuracions més típiques (gateway, DMZ, host only, Servidor web)
  - Permet reutilitzar objectes (hosts, subxarxes, rangs d'IPS, grups de serveis, etc.)
  - Permet compilar i instal·lar les normes en la màquina local o en màquines remotes
- **fwbuilder a la wiki**

Autor: Sergi Tur Badenas

fwbuilder

```
$ sudo apt-get install fwbuilder
```



Autor: Sergi Tur Badenas

fwbuilder

- **Exercici:**
  - Utilitzeu l'assistent de fwbuilder i les plantilles per crear les normes d'un servidor iptables en un màquina Linux (Kernel 2.4/2.6)
  - Configureu el firewall per a un servidor Web
  - Configureu el firewall per a una xarxa DMZ
  - Instal·leu el firewall a la vostra màquina
  - Opcionalment, i per aquells més agosarats, podeu instal·lar el firewall a la màquina d'un company, a un servidors remot o una màquina virtual amb vmware

Autor: Sergi Tur Badenas

Webmin

Índex de Webmin
Ajuda...
Configuració del Mòdul

Busca Documents...

Tallafocs Linux

Mostrant IPtable: | Filtratge de paquets (filter) | Afegeix una nova cadena anomenada:

Paquets d'entrada (INPUT)

Acció	Condició	Desplaça	Afegeix
Registra el paquet	Si la interfície d'entrada és **eth0**		

Estableix l | Accepta | Buida totes les regles | Afegeix regla

Paquets reenviats (FORWARD)

Acció	Condició	Desplaça	Afegeix
Registra el paquet	Si la interfície de sortida és **eth0**		
Registra el paquet	Si la interfície d'entrada és **eth0**		

Estableix l | Accepta | Buida totes les regles | Afegeix regla

Paquets de sortida (OUTPUT)

Acció	Condició	Desplaça	Afegeix
Registra el paquet	Si la interfície de sortida és **eth0**		

Estableix l | Accepta | Buida totes les regles | Afegeix regla

Aplica la Configuració — Fes clic sobre aquest botó per fer que la configuració del tallafocs llistada a sobre sigui activa. Totes les regles que estiguin actualment en efecte seran descartades i reemplaçades.

Reverteix la Configuració — Fes clic sobre aquest botó per reiniciar la configuració llistada a sobre amb els valors de la que està actualment activa.

Activa | Sí | No — Canvia aquesta opció per controlar si el tallafocs s'ha d'activar en engegar el sistema o no.

Reinicia el Tallafocs — Fes clic sobre aquest botó per eliminar totes les regles existents del tallafocs i establir-ne de noves per a una configuració inicial bàsica.

Autor: Sergi Tur Badenas

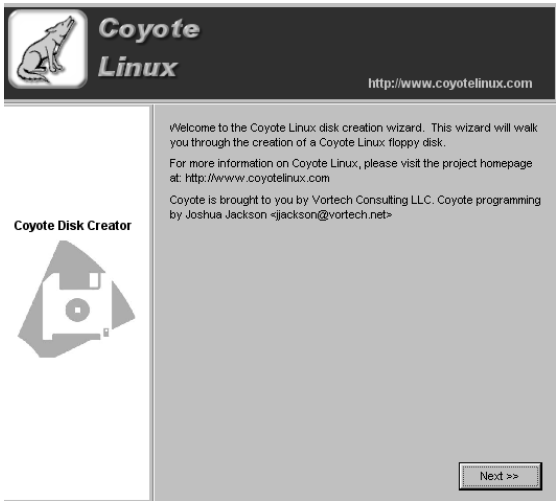
Linux Box 2. Coyote Linux

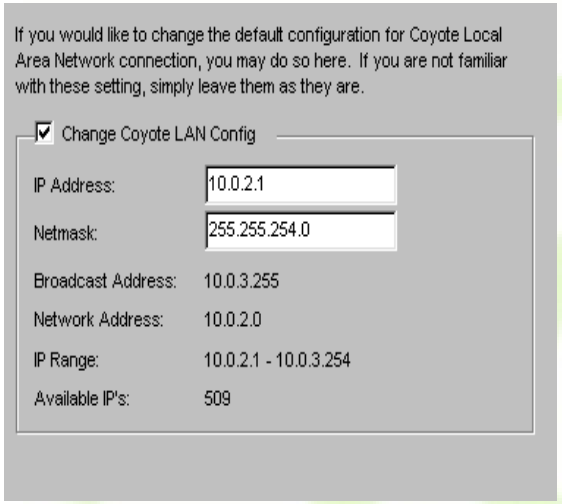
- **Coyote Linux**
  - Distribució Linux que requereix de molts pocs recursos pensada per funcionar com a router/firewall.
  - **Característiques:**
    - **Linux Kernel 2.6**
    - **Firewall iptables**
    - **Router amb suport per DHCP i IP estàtica i connexions PPP**
    - **Molt estable**
    - **Gestió remota via SSH o web**
    - **Requeriments del sistema**
      - **486DX/25, 32Mb RAM, CDROM, 2 NICs PCI, 32Mb de disc dur i targeta VGA**

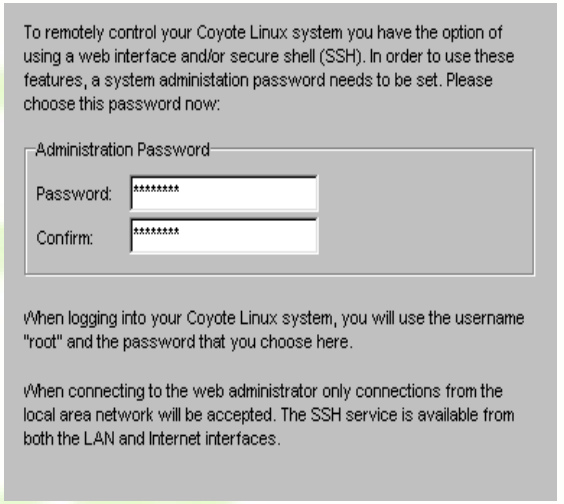
Autor: Sergi Tur Badenas

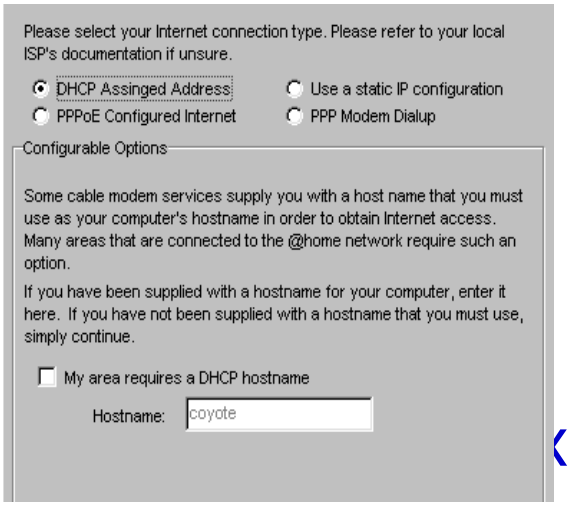
Exemple Linux. Coyote Linux

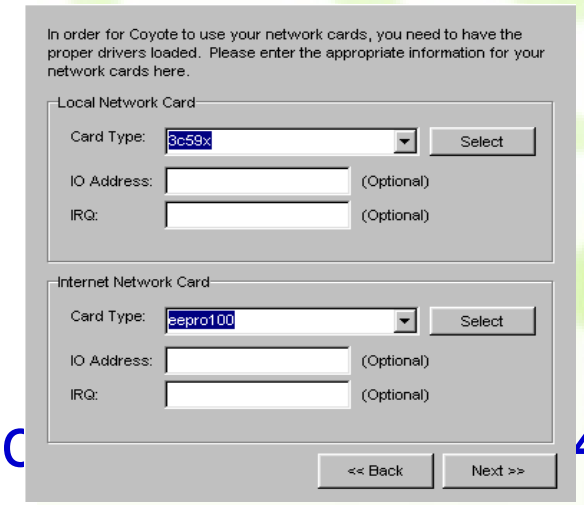
- **Instal·lador gràfic**











Autor: Sergi Tur Badenas

Coyote Linux

Web Administrator

Coyote Linux

Web Administrator - Version 4.10

Main Menu

- Information
- LAN Configuration
- Internet Configuration
- DHCP Configuration
- Administrative Config
- Port Forwarding
- Simplified Firewall Configuration
- Advanced Firewall Configuration
- QOS Configuration
- System Password
- Configuration Files
- Diagnostic Tools
- Backup Now
- Reboot

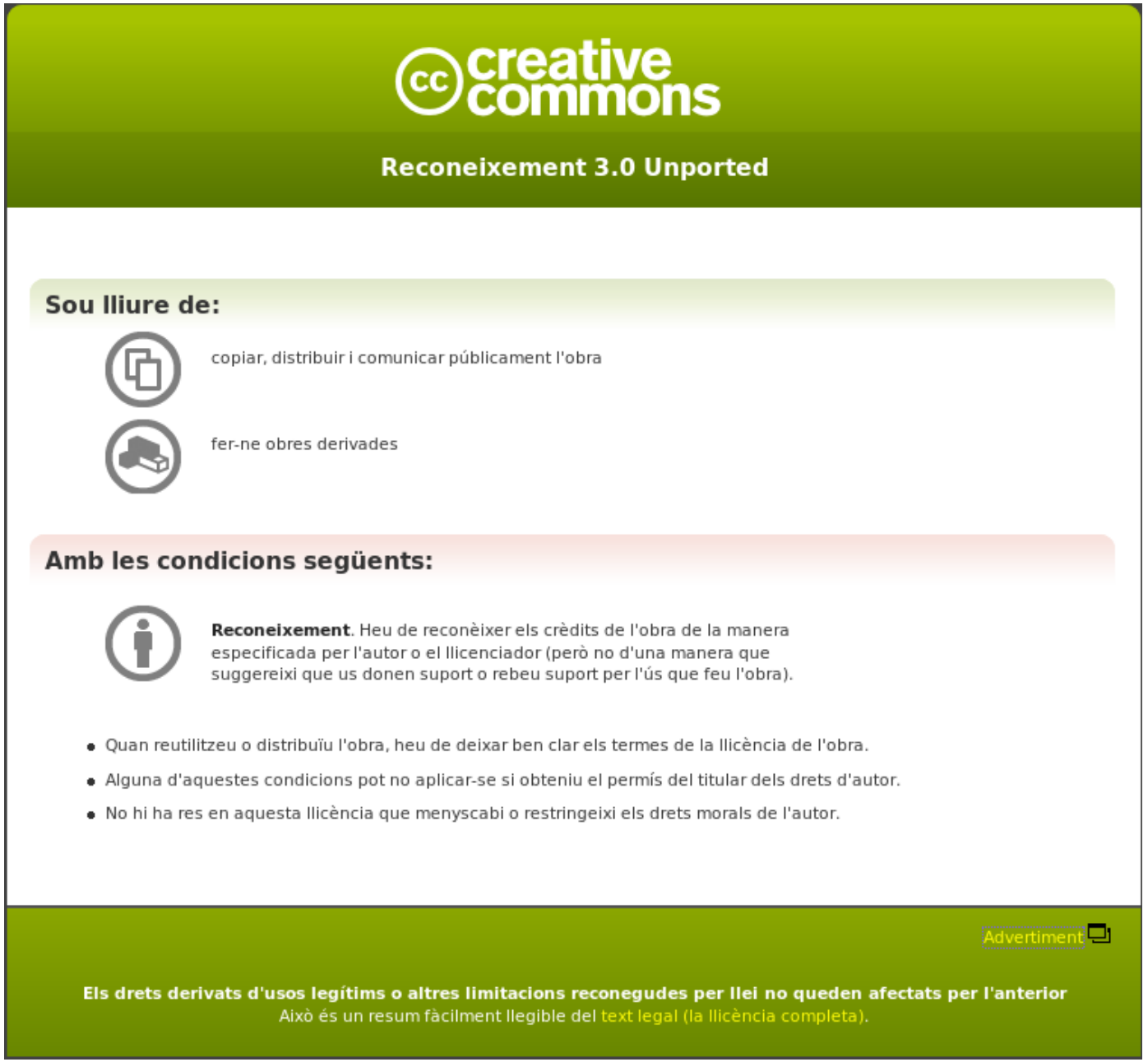
Welcome to Coyote Linux Web Administrator

General Information		
Coyote Linux - Version	2.24	
Host Name	coyote	
Domain	localdomain	
Network Status - Internet		
Status	UP	[Release IP | Renew IP]
Internet Type	Ethernet (DHCP Assigned IP)	
External IP Address	10.0.0.8	
Netmask	255.255.255.0	
Gateway	10.0.0.1	[Gateway Test]
Network Status - Local Network		
Status	UP	
Local IP Address	10.0.2.1	
Netmask	255.255.254.0	
Broadcast	10.0.3.255	
DNS Information		
Primary Nameserver	217.13.4.24	[DNS Test]
Secondary Nameserver	217.13.7.140	
Services		
DNS Cache	Disabled	
DHCP Server	Disabled	
SSH Service	Enabled (port 22)	
Web Administrator	Enabled (port 8180)	
System Information		
Kernel Version	2.4.30	
Machine	i686 unknown	
Current Date and Time	Thu Nov 24 20:00:05 EST 2005	
Uptime	20:00:05 up 29 days, 11:11, load average: 0.00, 0.00, 0.00	
Load Average	Last 1 Minute	0.00
	Last 5 minutes	0.00
	Last 15 minutes	0.00
Memory Usage	Total	63252 (100%)
	Used	8096 (12%)
	Free	55156 (88%)

(c) 1999-2005 Vortech Consulting, LLC

Autor: Sergi Tur Badenas

Llicència Creative Commons



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

Autor: Sergi Tur Badenas