



Encaminament IP

NA 3.5.

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



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.



Routers / Encaminadors

♦ Hi ha diferents tipus de routers:

MAQUINARI

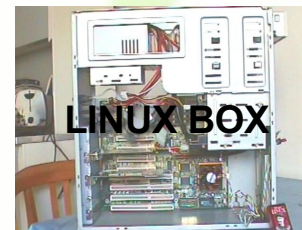


COMERCIALS



CORPORATIUS

PROGRAMARI



LINUX BOX



LINUX XBOX



LINUX PS2

♦ Programari

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



Configuració

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

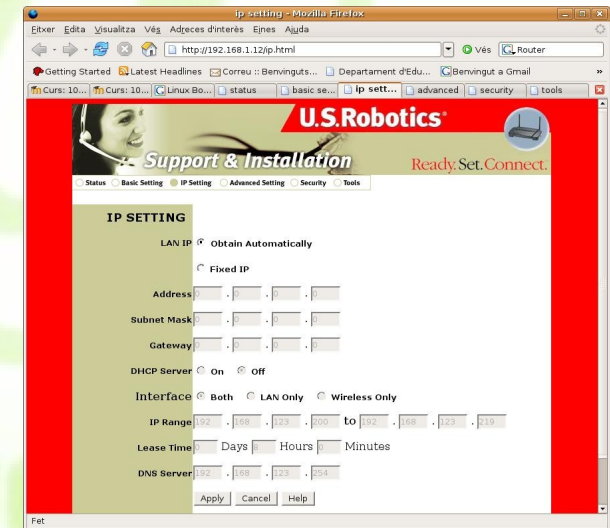
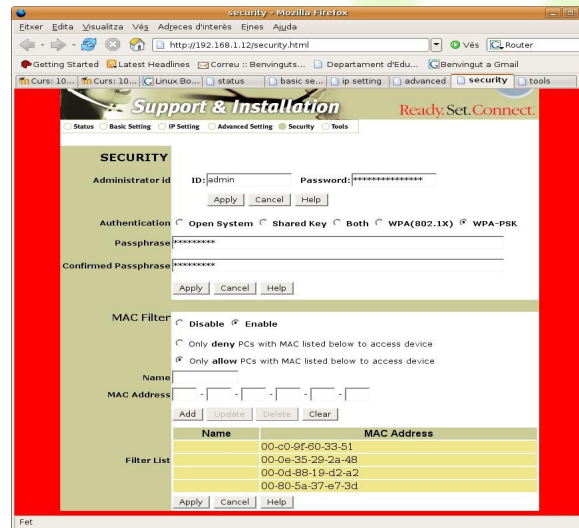
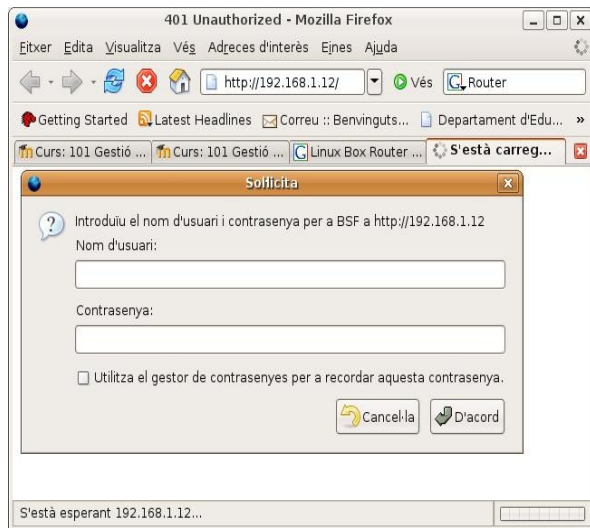


Exemple router comercial

Router US-Robotics

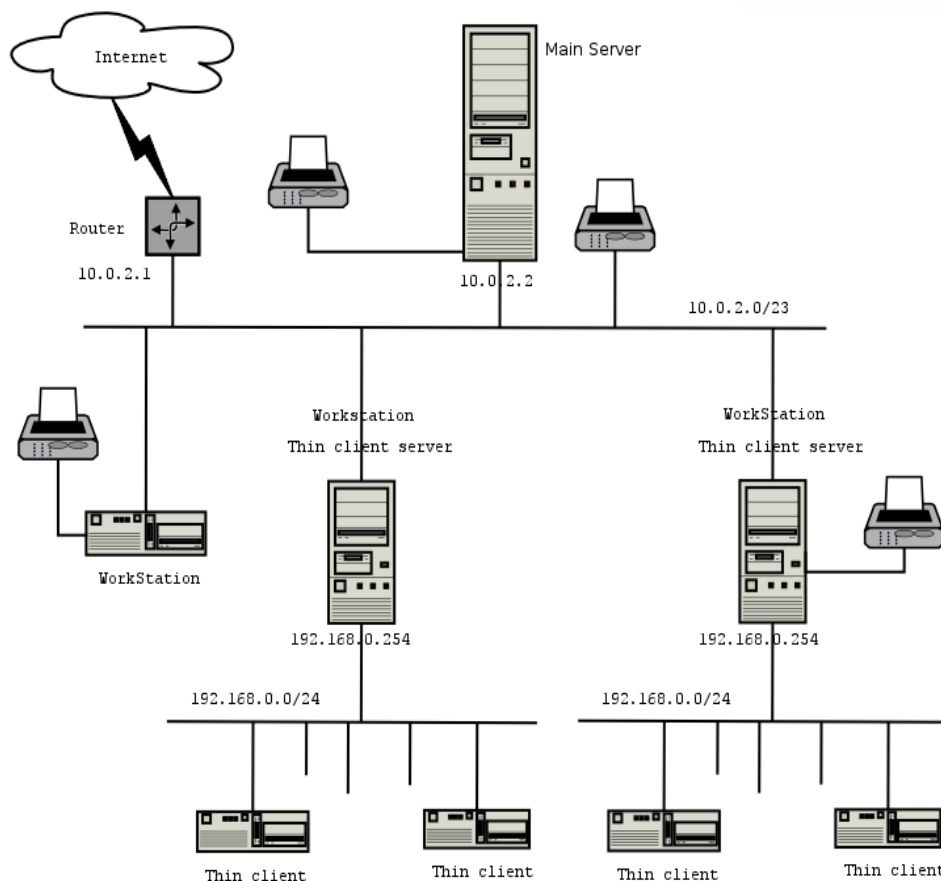


Interfície web de configuració
IP Local:192.168.1.12





Exemple Aula Informàtica. SkoleLinux

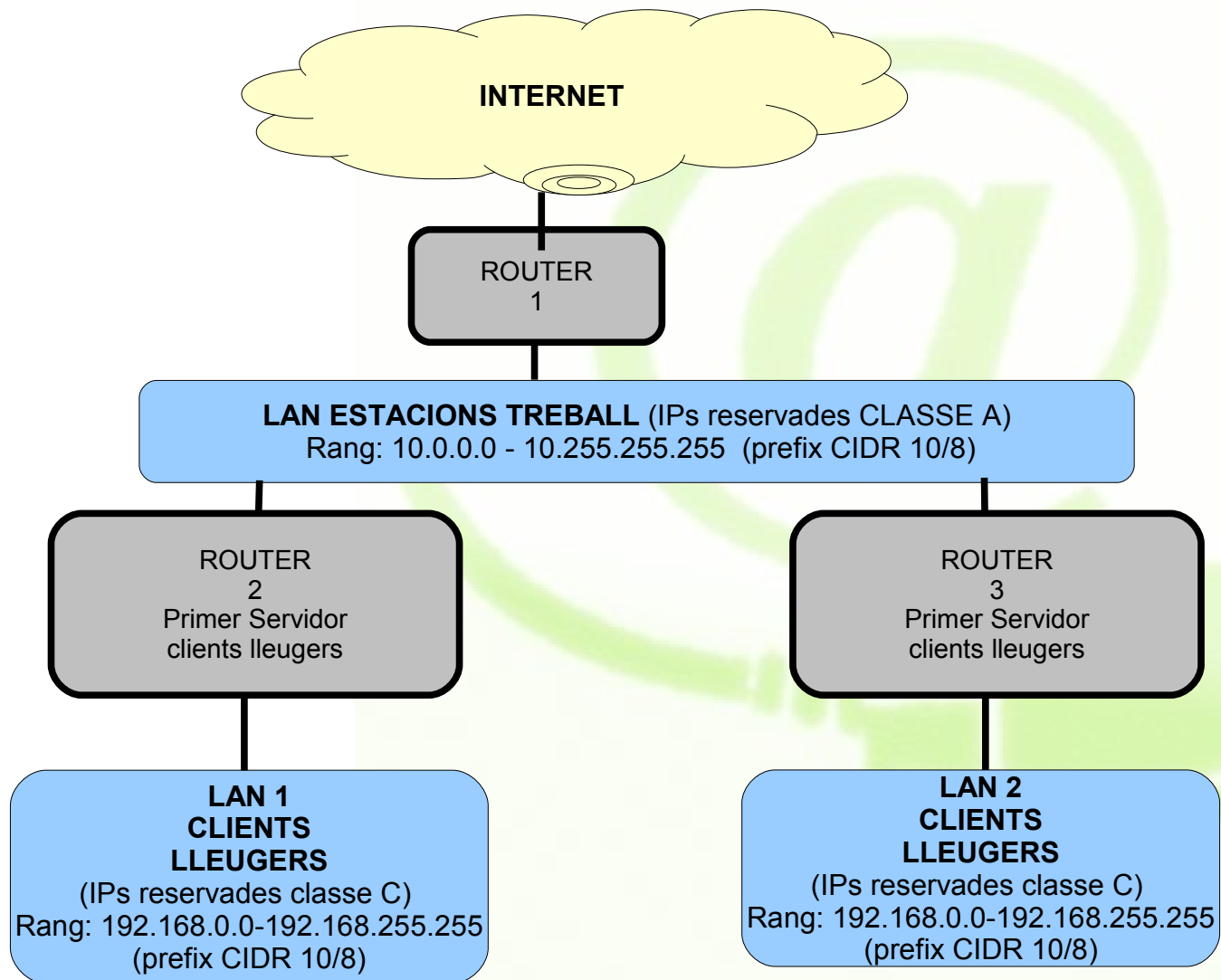


- ♦ **3 xarxes d'àrea local**
 - ♦ Switch 1: Estacions de treball
 - ♦ Switch 2 i 3: Terminals lleugers
- ♦ **Thin client servers**
 - ♦ Enrutadors entre xarxes
 - ♦ 2 NICs
- ♦ **Router principal**
 - ♦ Accés a Internet



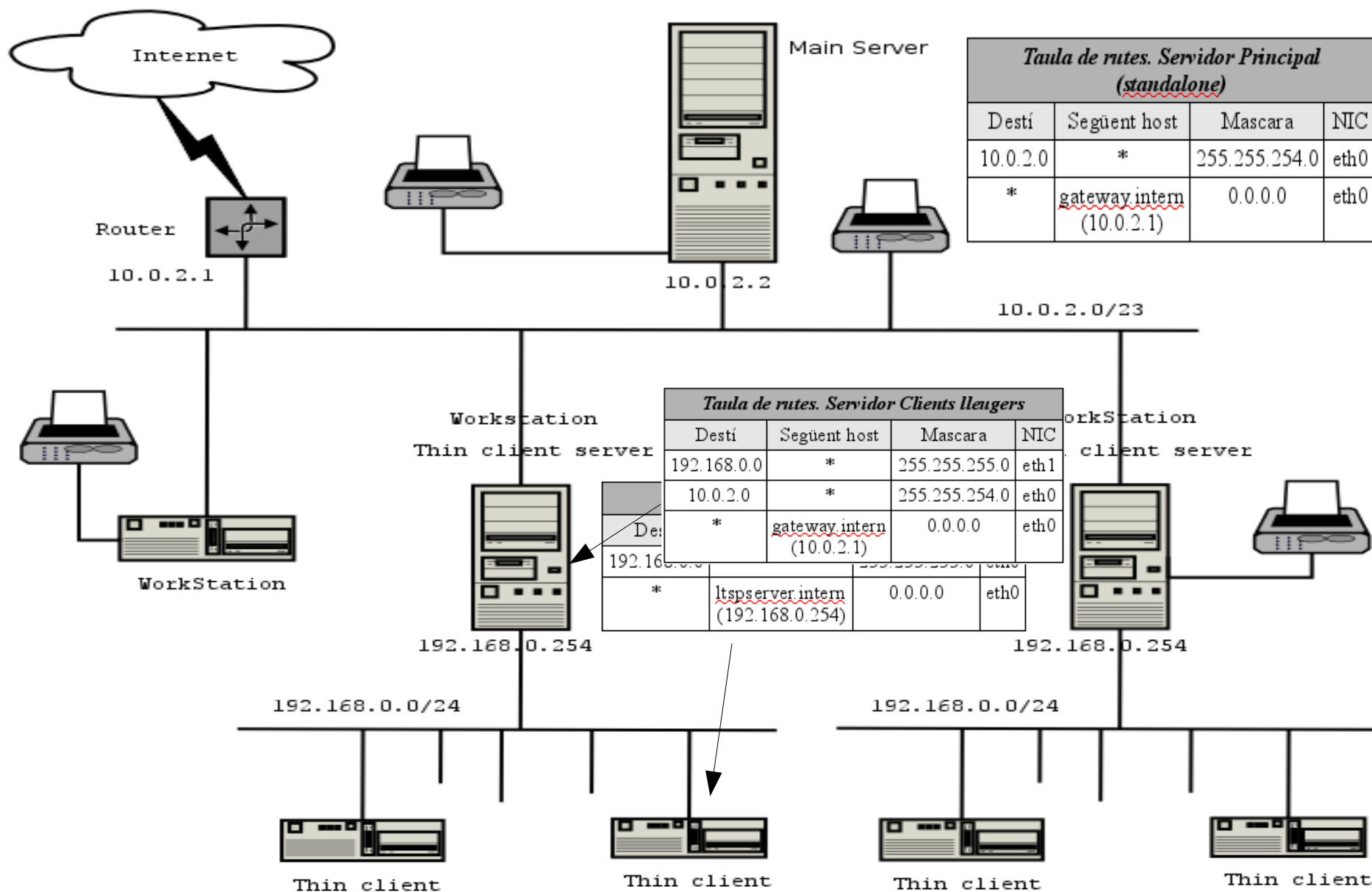
Exemple Aula Informàtica. SkoleLinux

♦ Esquema d'encaminadors de l'aula





SkoleLinux. Taules d'enrutament





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 àrea extensa

- ♦ Qui exerceix el rol d'encaminador cap a internet (gateway)?



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
*	<u>gateway intern</u> (10.0.2.1)	0.0.0.0	eth0

Taula de rutes. Estacions de treball			
Destí	Següent host	Mascara	NIC
192.168.0.0	<u>ltspserverX i</u> <u>ntern</u> (10.0.2.X)	255.255.255.0	eth0
10.0.2.0	*	255.255.254.0	eth0
*	<u>gateway intern</u> (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	<u>ltspserver.intern</u> (192.168.0.254)	255.255.254.0	eth0
*	<u>ltspserver.intern</u> (192.168.0.254)	0.0.0.0	eth0



SkoleLinux. Interconnexió de xarxes

♦ Solucions:

- ♦ De la connexió a Internet s'encarrega el “router 1”.
- ♦ Per exemple, si la connexió a Internet és una ADSL el més probable és que el “router 1” estigui connectat al router de la central telefònica mitjançant PPP.
- ♦ Les qüestions específiques de connexió a xarxes d'àrea extensa i/o Internet es veuran a la següent unitat didàctica.



Exemple Linux. Coyote Linux



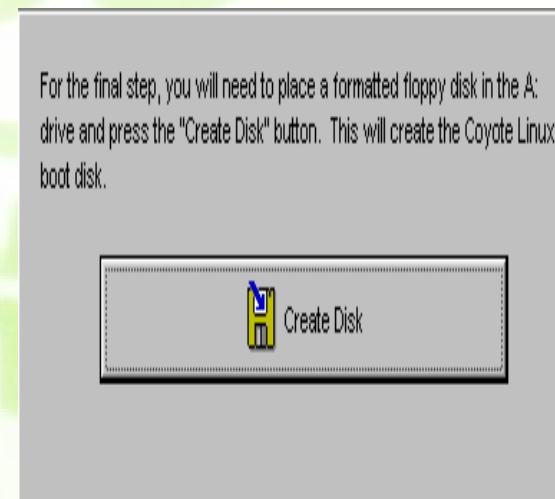
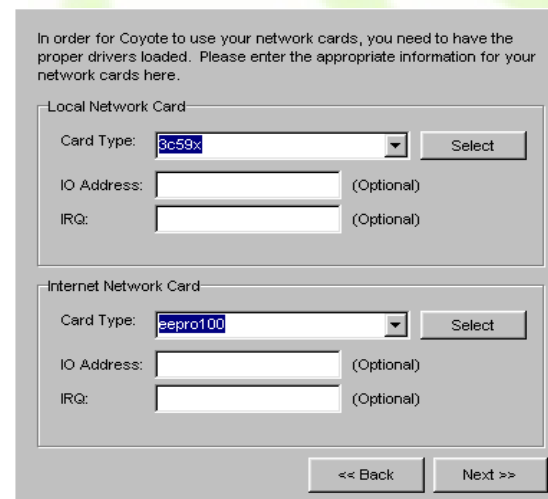
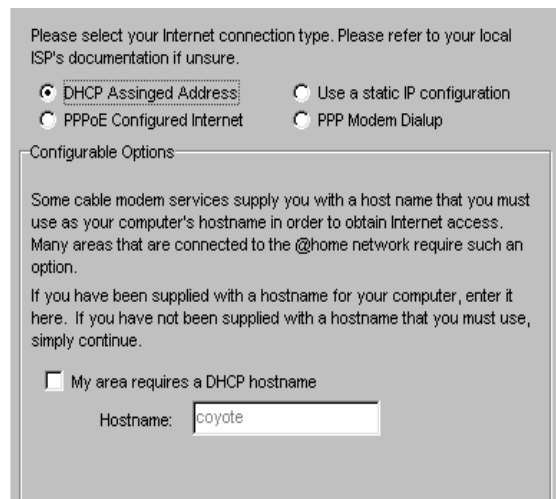
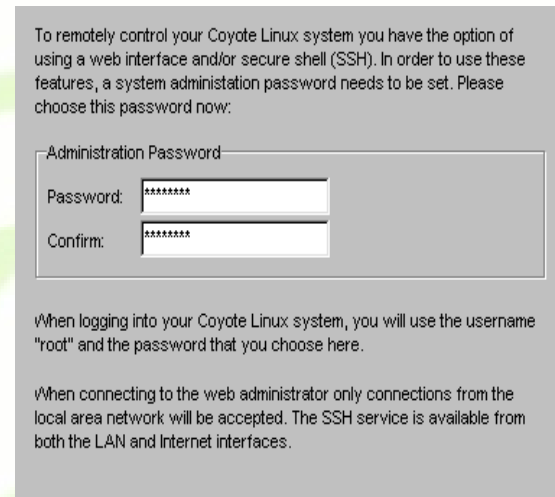
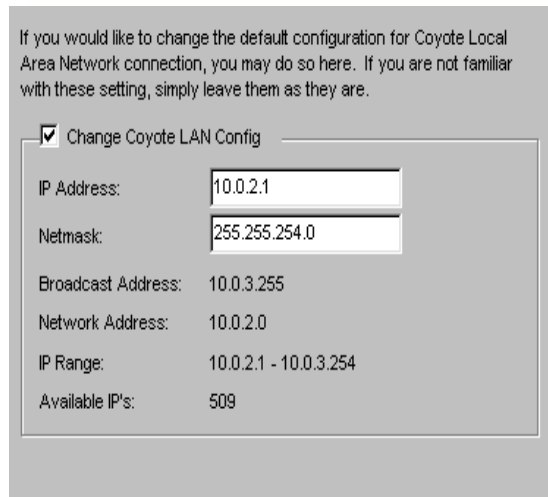
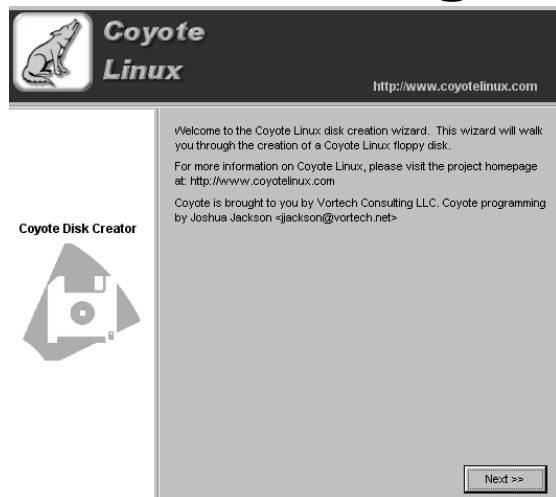
♦ Coyote Linux

- ♦ Distribució Linux que funciona com a router/firewall.
- ♦ Requereix de molts pocs recursos
 - 486DX/25, 32Mb RAM, CDROM, 2 NICs PCI, 32Mb de disc dur i targeta VGA
- ♦ **Característiques:**
 - Linux Kernel 2.6
 - Firewall iptables
 - Router amb suport per DHCP i IP estàtica i connexions PPP
 - Estable i fiable
 - Gestió remota via SSH o web



Exemple Linux. Coyote Linux

◆ Instal·lador gràfic




◆ <http://skolelinux.org/~klaus/sarge/c413.html>



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



NAT (Traducció d'adreça de xarxa)

♦ Network Address Translation

- ♦ És un estàndard creat per la Internet Engineering Task Force (IETF).
- ♦ S'utilitza per compartir una adreça d'Internet vàlida amb les adreces reservades a xarxes d'àrea local.

♦ Funcionament

- ♦ Canviant les adreces d'Internet de les capçaleres IP.

♦ Tipus

- ♦ NAT estàtic.
- ♦ NAT dinàmic. Accés en rang a Internet.

♦ Animació Flash sobre NAT de CISCO



Exemple de NAT

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	<input checked="" type="checkbox"/>
2	smtp	TCP	110	10.0.3.234	110	<input checked="" type="checkbox"/>
3	pop3	TCP	25	10.0.3.234	25	<input checked="" type="checkbox"/>
4	www	TCP	80	10.0.3.234	80	<input checked="" type="checkbox"/>
5	ssh2	TCP	24	10.0.2.2	22	<input checked="" type="checkbox"/>
6	www2	TCP	8080	10.0.2.2	80	<input checked="" type="checkbox"/>
7	webmin2	TCP	10000	10.0.2.2	10000	<input checked="" type="checkbox"/>
8		---	0		0	<input type="checkbox"/>
9		---	0		0	<input type="checkbox"/>
10		---	0		0	<input type="checkbox"/>

OK

Copyright (c) 2002, DrayTek Corp. All Rights Reserved.



Exemple de NAT

► Configuració per línia de comandes amb iptables

Code Listing 5.2: Setting up iptables

```
First we flush our current rules
# iptables -F
# iptables -t nat -F

Setup default policies to handle unmatched traffic
# iptables -P INPUT ACCEPT
# iptables -P OUTPUT ACCEPT
# iptables -P FORWARD DROP

Copy and paste these examples ...
# export LAN=eth0
# export WAN=eth1

Then we lock our services so they only work from the LAN
# iptables -I INPUT 1 -i ${LAN} -j ACCEPT
# iptables -I INPUT 1 -i lo -j ACCEPT
# iptables -A INPUT -p UDP --dport bootps -i ! ${LAN} -j REJECT
# iptables -A INPUT -p UDP --dport domain -i ! ${LAN} -j REJECT

(Optional) Allow access to our ssh server from the WAN
# iptables -A INPUT -p TCP --dport ssh -i ${WAN} -j ACCEPT

Drop TCP / UDP packets to privileged ports
# iptables -A INPUT -p TCP -i ! ${LAN} -d 0/0 --dport 0:1023 -j DROP
# iptables -A INPUT -p UDP -i ! ${LAN} -d 0/0 --dport 0:1023 -j DROP

Finally we add the rules for NAT
# iptables -I FORWARD -i ${LAN} -d 192.168.0.0/255.255.0.0 -j DROP
# iptables -A FORWARD -i ${LAN} -s 192.168.0.0/255.255.0.0 -j ACCEPT
# iptables -A FORWARD -i ${WAN} -d 192.168.0.0/255.255.0.0 -j ACCEPT
# iptables -t nat -A POSTROUTING -o ${WAN} -j MASQUERADE
Tell the kernel that ip forwarding is OK
# echo 1 > /proc/sys/net/ipv4/ip_forward
# for f in /proc/sys/net/ipv4/conf/*/rp_filter ; do echo 1 > $f ; done

This is so when we boot we don't have to run the rules by hand
# /etc/init.d/iptables save
# rc-update add iptables default
# nano /etc/sysctl.conf
Add/Uncomment the following lines:
net.ipv4.ip_forward = 1
net.ipv4.conf.default.rp_filter = 1
```



<http://creativecommons.org/licenses/by-sa/2.5/deed.ca>