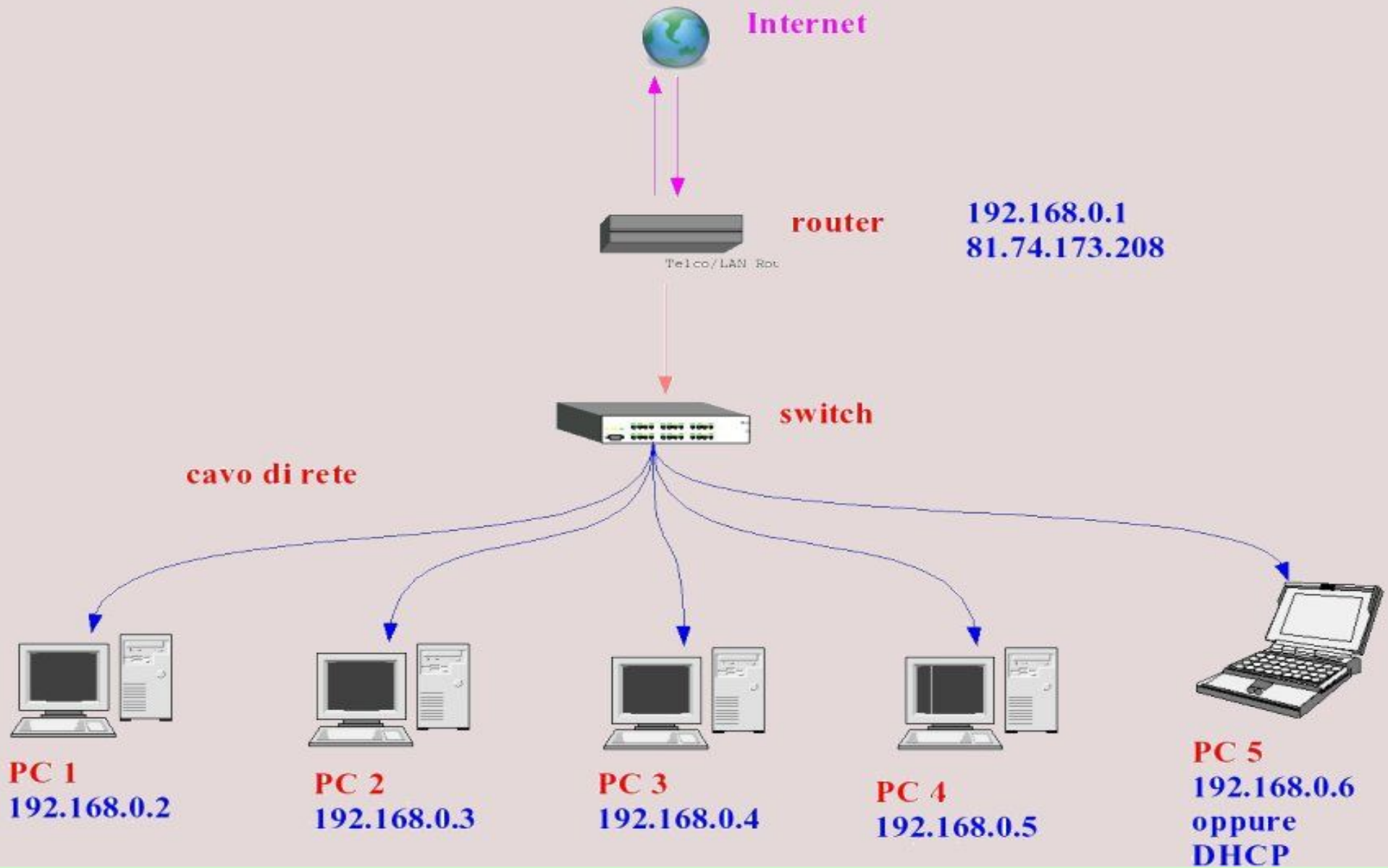




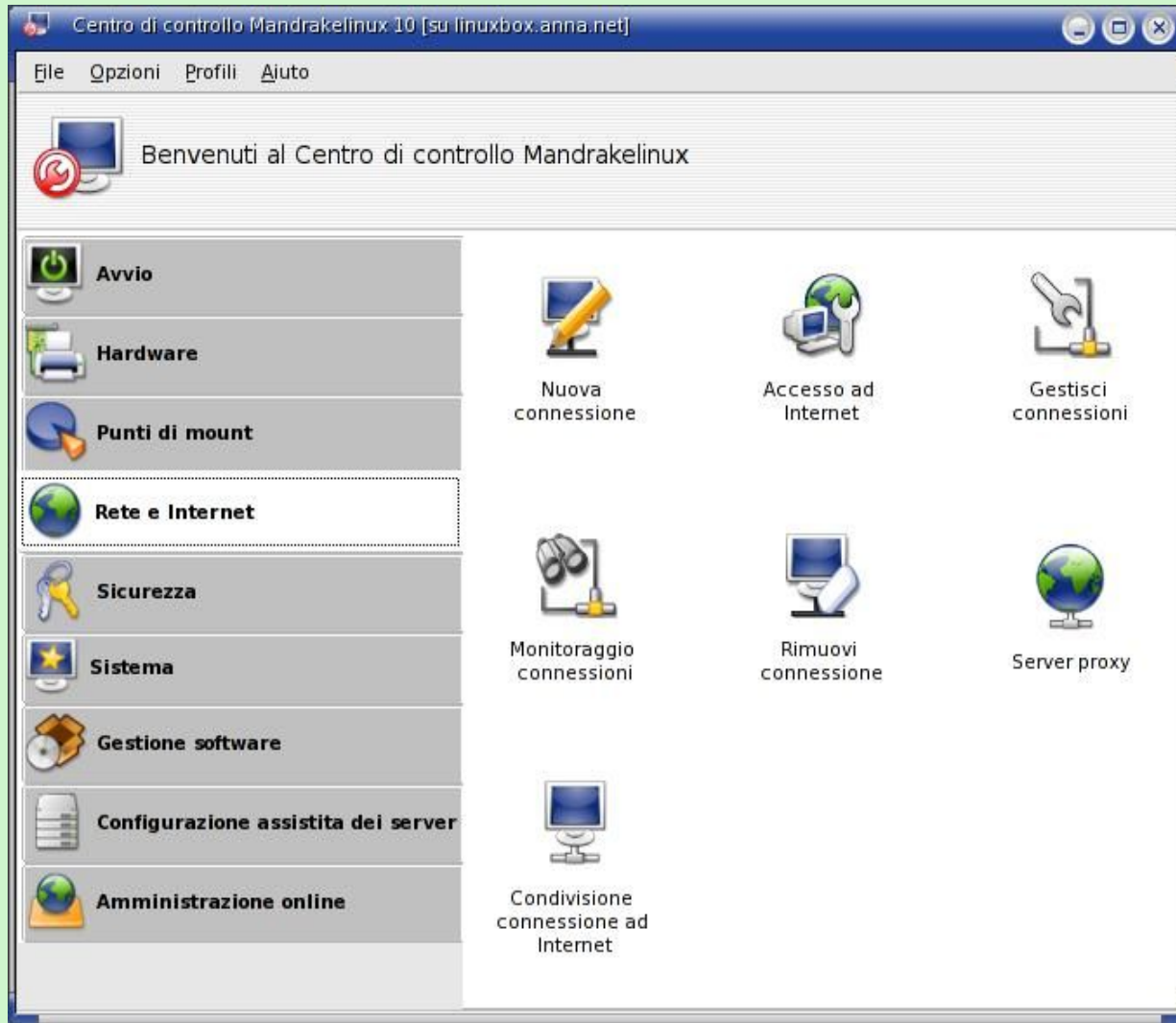
TCP/IP E RETI CON LINUX

LAN con router adsl





Mandrake Control Center

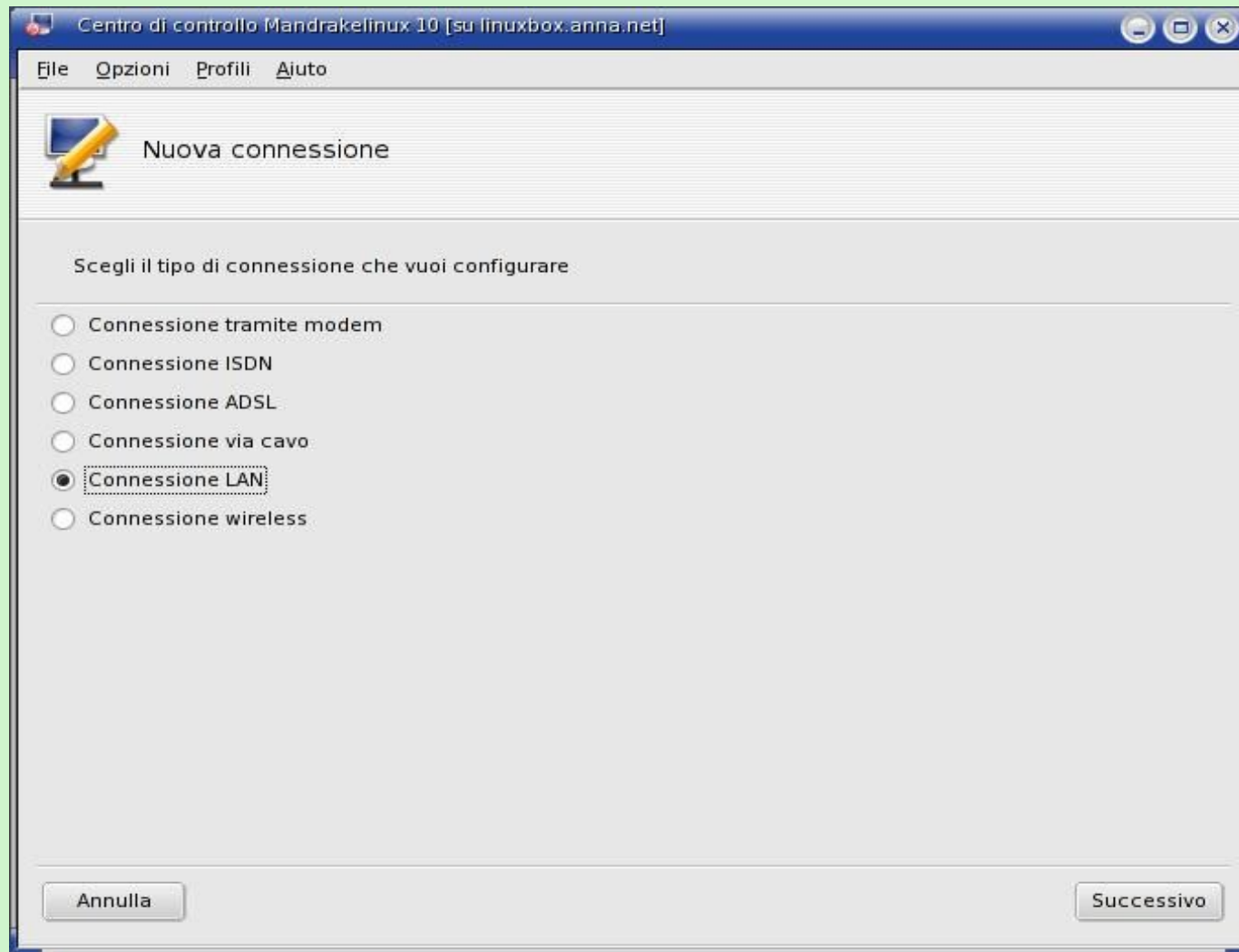


- Avviare il Mandrake Control Center, selezionare la voce Reti e Internet ed alla schermata successiva scegliere **Nuova Connessione**.
- Altrimenti, da shell, avviare il programma **drakconnect**.
- Questa operazione va fatta su tutte le macchine della LAN.

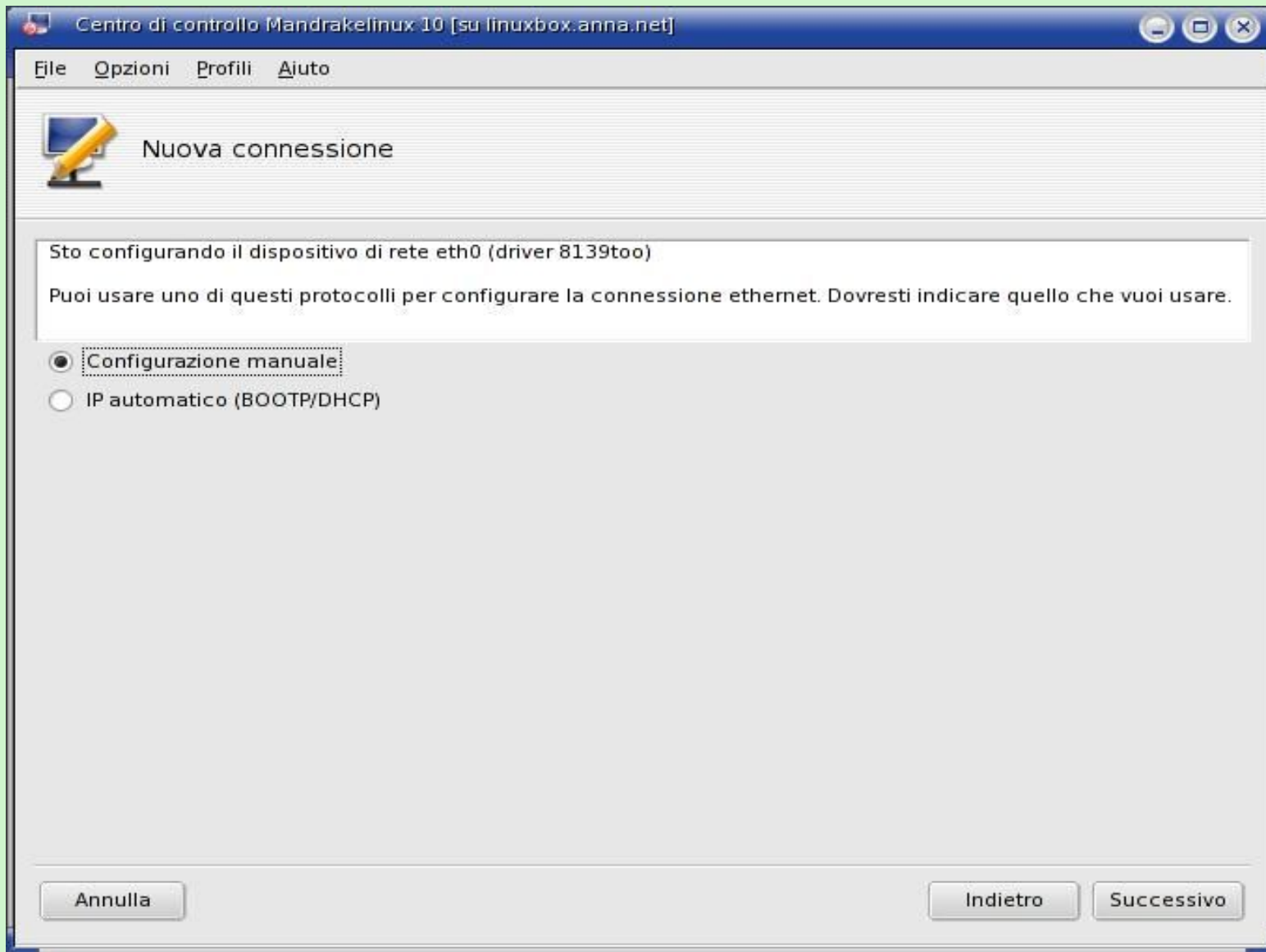
Drakconnect



- Scegliere la voce Connessione LAN.



Drakconnect




Drakconnect



Centro di controllo Mandrakelinux 10 [su linuxbox.anna.net]

File Opzioni Profili Aiuto

 Nuova connessione

Sto configurando il dispositivo di rete eth0 (driver 8139too)

Per favore inserisci la configurazione IP per questa macchina.
Ogni dato dovrebbe essere inserito come indirizzo IP
in notazione decimale puntata (ad esempio 1.2.3.4).

Indirizzo IP

Netmask

Individua l'ID della scheda di rete (utile per i laptop)

Hotplugging della rete


Attiva al momento del boot

Drakconnect



Centro di controllo Mandrakelinux 10 [su linuxbox.anna.net]

File Opzioni Profili Aiuto

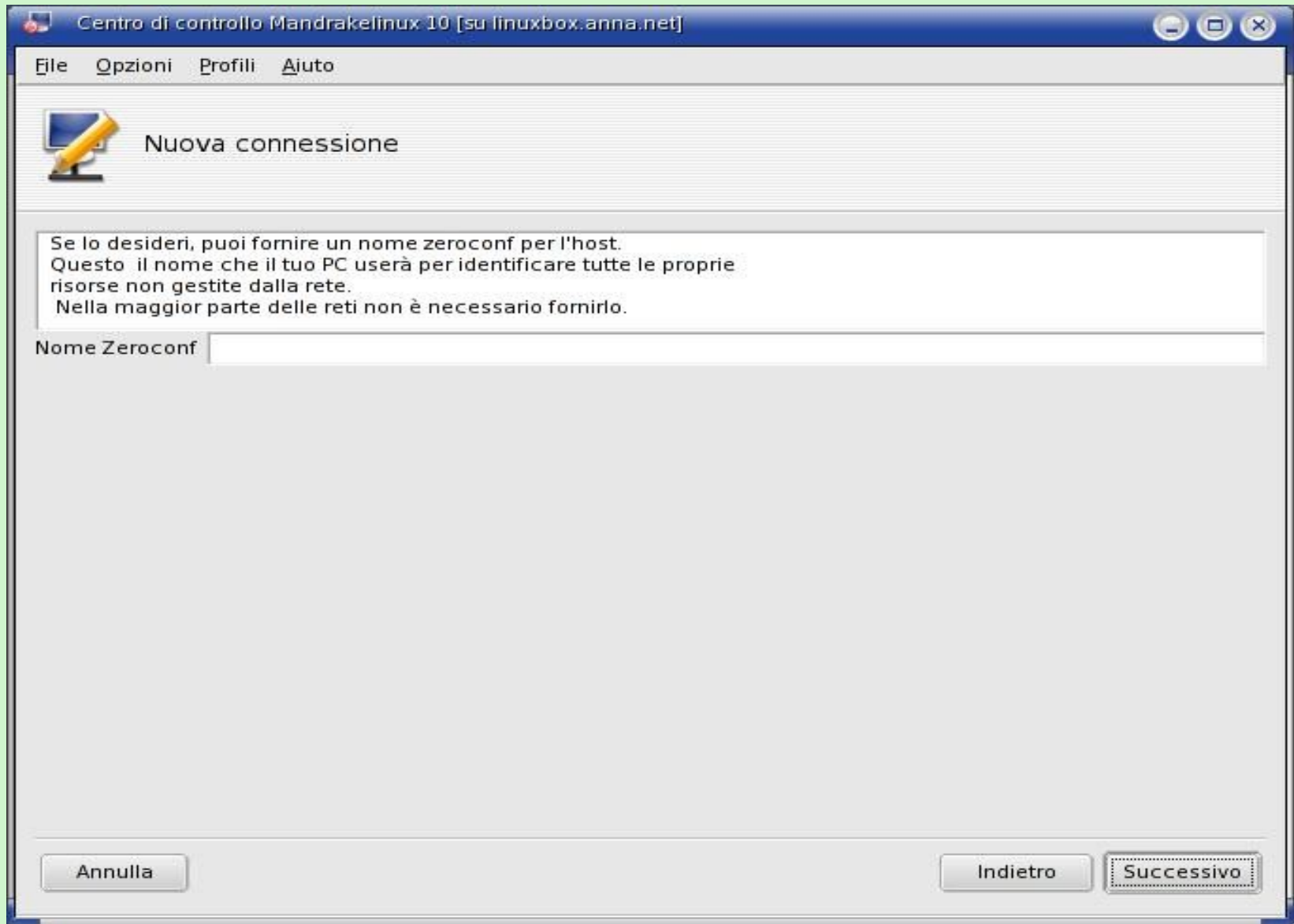
 Nuova connessione

Per favore inserisci il nome del tuo host.
Questo dovrebbe essere un nome-host pienamente qualificato,
come "mybox.mylab.myco.com".
Puoi anche inserire l'indirizzo IP del gateway, se ne hai uno. Per finire, ma è importante, puoi anche inserire i tuoi
indirizzi DNS e IP.

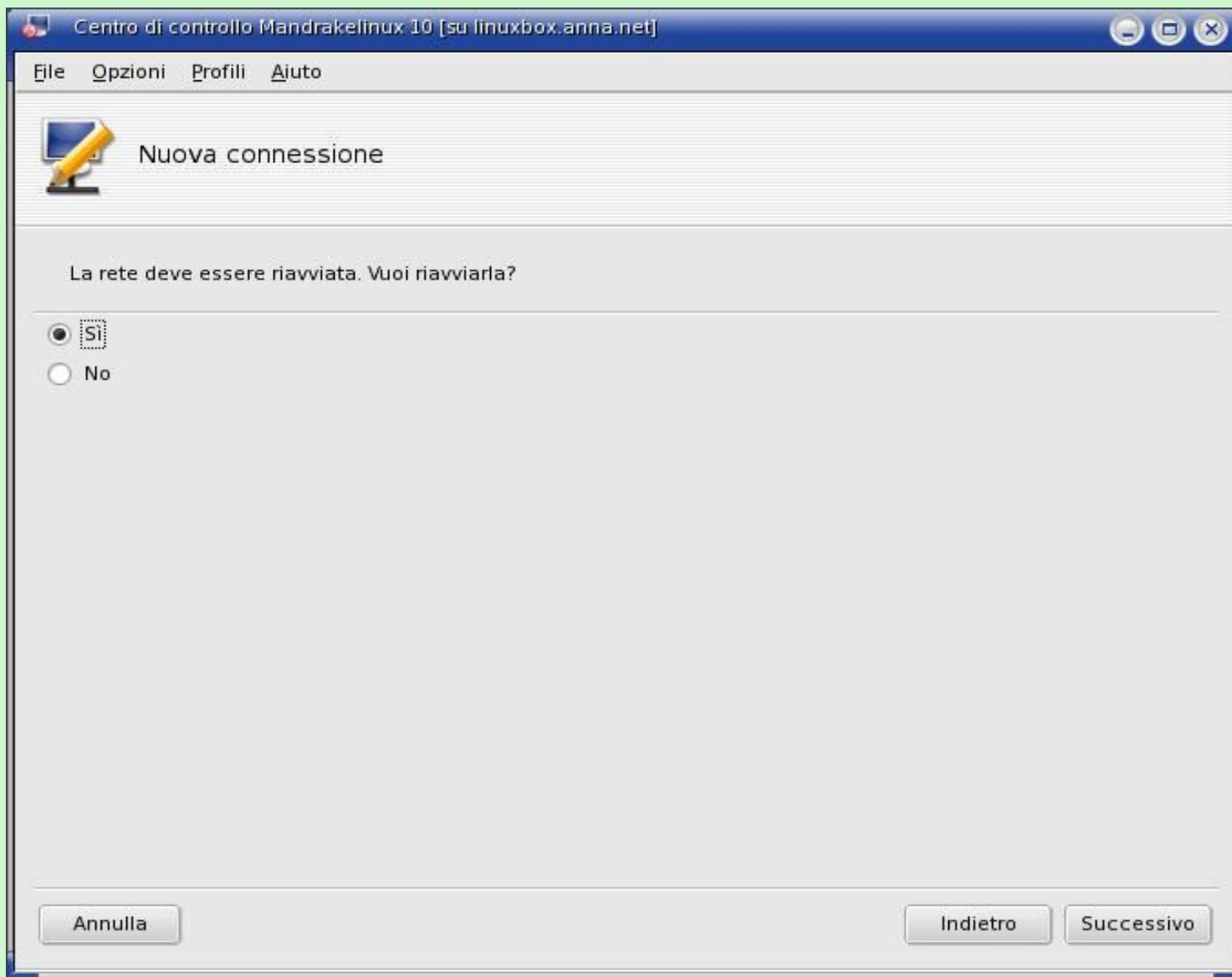
Nome host	linuxbox.anna.net
Server DNS 1	212.216.112.112
Server DNS 2	212.216.172.62
Server DNS 3	
Dominio di ricerca	anna.net
Gateway (es. 192.168.0.1)	192.168.0.1
Dispositivo di gateway	eth0: Realtek RTL-8139

Annulla Indietro Successivo

Drakconnect



Drakconnect





Monitoraggio connessioni



eth0

56
112
134
67

■ inviato: 647
■ ricevuto: 1023
■ media

Misura locale
inviato: 0
ricevuto: 0

Impostazioni
Tipo di connessione: ethernet

Statistiche globali

	Istantaneo	Media
Velocità di trasmissione:	0/s	17/s
Velocità di ricezione:	0/s	29/s

Tempo di connessione: sconosciuto

Usa la stessa scala per ricevuto e trasmesso

Connetti ethernet

Chiudi

Non connesso

- Monitoraggio connessioni, sempre dal Centro di Controllo, oppure da shell con il comando **net_monitor**

Il comando ping



```
anna@linuxbox.anna.net: /home/anna - Shell - Konsole
Sessione Modifica Visualizza Segnalibri Impostazioni Aiuto

[root@linuxbox anna]# ping 192.168.0.1
PING 192.168.0.1 (192.168.0.1) 56(84) bytes of data.
64 bytes from 192.168.0.1: icmp_seq=1 ttl=64 time=0.476 ms
64 bytes from 192.168.0.1: icmp_seq=2 ttl=64 time=0.446 ms
64 bytes from 192.168.0.1: icmp_seq=3 ttl=64 time=0.449 ms
64 bytes from 192.168.0.1: icmp_seq=4 ttl=64 time=0.451 ms

--- 192.168.0.1 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 2999ms
rtt min/avg/max/mdev = 0.446/0.455/0.476/0.024 ms
[root@linuxbox anna]# ping google.com
PING google.com (216.239.57.99) 56(84) bytes of data.
64 bytes from 216.239.57.99: icmp_seq=1 ttl=239 time=238 ms
64 bytes from 216.239.57.99: icmp_seq=2 ttl=239 time=239 ms
64 bytes from 216.239.57.99: icmp_seq=3 ttl=239 time=240 ms

--- google.com ping statistics ---
4 packets transmitted, 3 received, 25% packet loss, time 3000ms
rtt min/avg/max/mdev = 238.311/239.309/240.371/0.842 ms
[root@linuxbox anna]#
```

Monitorare le porte



```
anna@linuxbox.anna.net: /home/anna - Shell - Konsole
Sessione Modifica Visualizza Segnalibri Impostazioni Aiuto
[root@linuxbox anna]# nmap -sS 127.0.0.1

Starting nmap 3.55 ( http://www.insecure.org/nmap/ ) at 2005-03-30
09:15 CEST
Interesting ports on linuxbox.anna.net (127.0.0.1):
(The 1653 ports scanned but not shown below are in state: closed)
PORT      STATE SERVICE
22/tcp    open  ssh
111/tcp    open  rpcbind
631/tcp    open  ipp
769/tcp    open  vid
996/tcp    open  xtreelic
2049/tcp   open  nfs
6000/tcp   open  X11

Nmap run completed -- 1 IP address (1 host up) scanned in 1.052 se
conds
[root@linuxbox anna]#
```



Netstat



```
Ciao! hai aperto questa xterm mer mar 30 09:22:54 CEST 2005 - Shell n.2 - Konsole
Sessione Modifica Visualizza Segnalibri Impostazioni Aiuto
[anna@linuxbox anna]$ netstat -l
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp      0      0 linuxbox.anna.net:32768 *:*                     LISTEN
tcp      0      0 *:769                  *:*                     LISTEN
tcp      0      0 *:32769                *:*                     LISTEN
tcp      0      0 *:nfs                  *:*                     LISTEN
tcp      0      0 *:996                  *:*                     LISTEN
tcp      0      0 *:sunrpc               *:*                     LISTEN
tcp      0      0 *:x11                  *:*                     LISTEN
tcp      0      0 *:ipp                  *:*                     LISTEN
tcp      0      0 *:7741                 *:*                     LISTEN
tcp      0      0 *:x11                  *:*                     LISTEN
tcp      0      0 *:ssh                  *:*                     LISTEN
udp      0      0 *:32768                *:*                     LISTEN
udp      0      0 *:nfs                  *:*                     LISTEN
udp      0      0 *:7741                 *:*                     LISTEN
udp      0      0 *:990                  *:*                     LISTEN
udp      0      0 *:imaps                *:*                     LISTEN
udp      0      0 *:sunrpc               *:*                     LISTEN
udp      0      0 *:ipp                  *:*                     LISTEN
udp      0      0 *:766                  *:*                     LISTEN
raw      89488  0 *:icmp                  *:*                     7
```

Il file /etc/hosts



```
anna@linuxbox.anna.net: /home/anna - Shell - Konsole
Session Modifica Visualizza Segnalibri Impostazioni Aiuto
[root@linuxbox anna]# cat /etc/hosts
127.0.0.1          localhost
192.168.0.10      linuxbox.anna.net linuxbox
192.168.0.5       didatux.education.net didatux
192.168.0.1       happypenguin.didattica.net happypenguin
192.168.0.2       linuxbox.anna.net.linuxbox
192.168.0.4       slacklinux.penguin.net slacklinux
[root@linuxbox anna]#
```



Configurare la rete da shell



```
[root@linuxbox anna]# dmesg | grep eth0
eth0: RealTek RTL-8029 found at 0xd400, IRQ 11, 52:54:00:E3:4D:62.

[root@linuxbox anna]# ifconfig eth0 192.168.0.2 netmask 255.255.
255.0 up

[root@linuxbox anna]# route add default gw 192.168.0.1
SIOCADDRT: File exists

[root@linuxbox anna]# ping 192.168.0.1
PING 192.168.0.1 (192.168.0.1) 56(84) bytes of data.
64 bytes from 192.168.0.1: icmp_seq=1 ttl=64 time=0.593 ms
64 bytes from 192.168.0.1: icmp_seq=2 ttl=64 time=0.463 ms

--- 192.168.0.1 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 999ms
rtt min/avg/max/mdev = 0.463/0.528/0.593/0.065 ms
[root@linuxbox anna]#
```



Rendere la configurazione permanente



```
[root@linuxbox anna]# cat /etc/sysconfig/network
```

```
HOSTNAME=linuxbox.anna.net
```

```
NETWORKING=yes
```

```
GATEWAY=192.168.0.1
```

```
GATEWAYDEV=eth0
```

```
[root@linuxbox anna]#
```

```
[root@linuxbox anna]# cat /etc/sysconfig/network-scripts/ifcfg-eth0
```

```
DEVICE=eth0
```

```
BOOTPROTO=static
```

```
IPADDR=192.168.0.2
```

```
NETMASK=255.255.255.0
```

```
NETWORK=192.168.0.0
```

```
BROADCAST=192.168.0.255
```

```
ONBOOT=yes
```

```
HWADDR=00:a0:d1:b9:fe:3f
```

```
METRIC=10
```

```
MII_NOT_SUPPORTED=no
```

```
[root@linuxbox anna]#
```




DNS



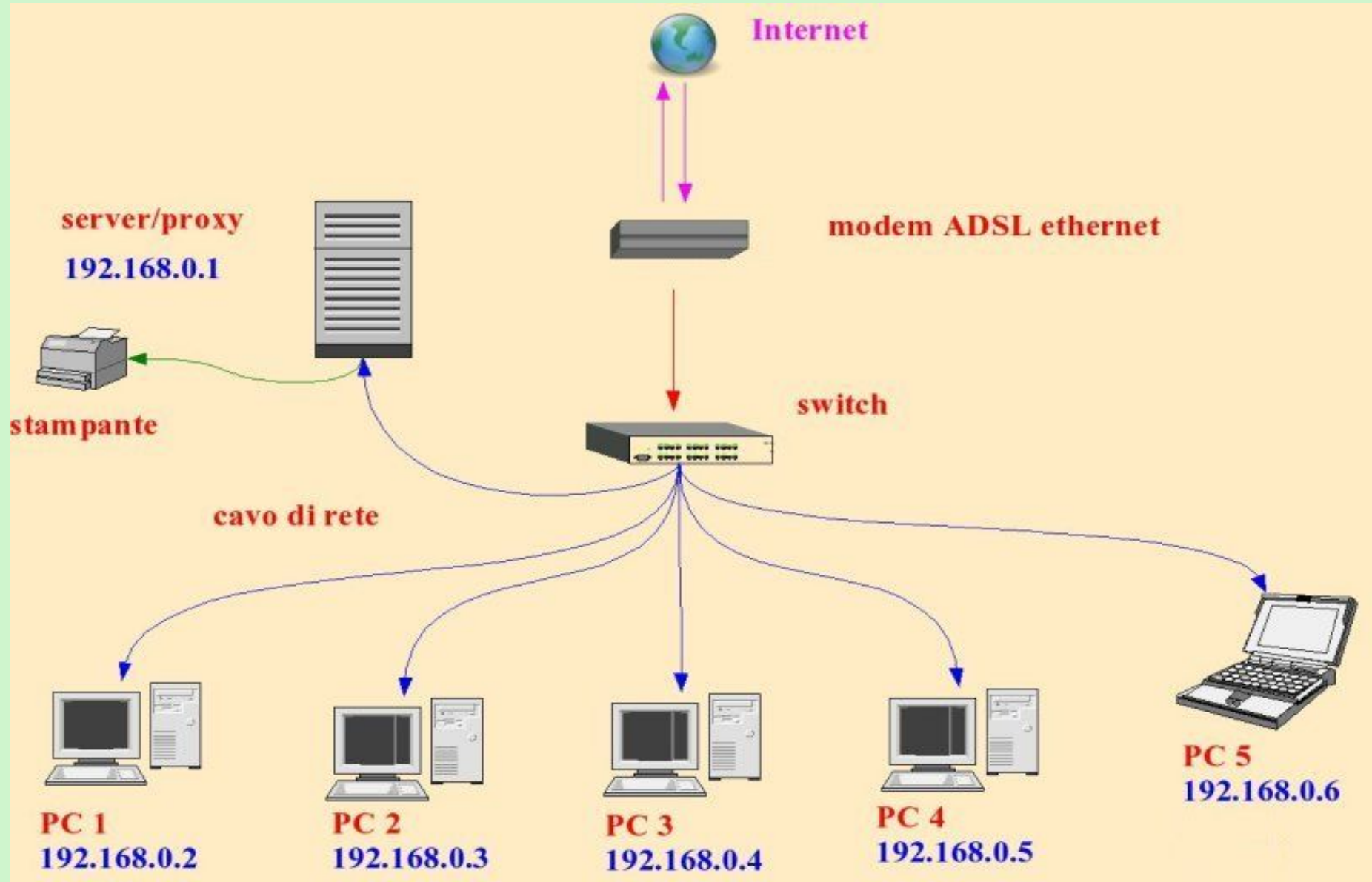
```
[root@linuxbox anna]# cat /etc/resolv.conf
search tin.it
nameserver 212.216.112.112
nameserver 212.216.172.62

# ppp temp entry
[root@linuxbox anna]#
[root@linuxbox anna]# nslookup
> www.tin.it
Server:                212.216.112.112
Address:                212.216.112.112#53

Non-authoritative answer:
www.tin.it             canonical name = tin.virgilio.it.
Name:                  tin.virgilio.it
Address: 62.211.65.12
>
```

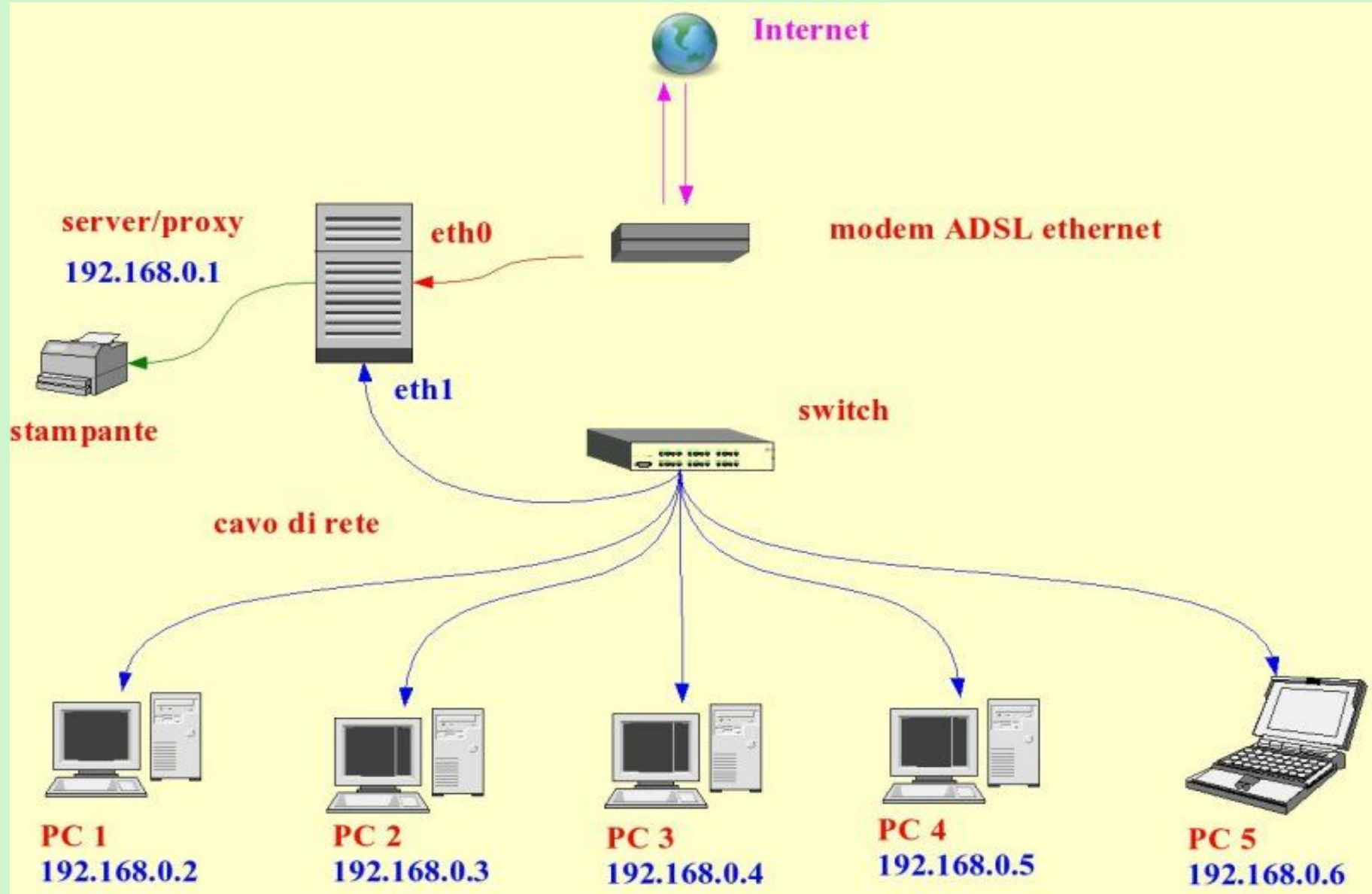


LAN con server/proxy (1)





LAN con server/proxy (2)





Pacchetti



- Per questa tipologia di LAN sono necessari alcuni pacchetti software:
 - Iptables (per configurare il firewall e per la condivisione della connessione)
 - Rp-pppoe (per configurare la connessione ADSL)
 - Rp-pppoe-gui (frontend grafico per rp-pppoe)
- Tutti i pacchetti sono forniti nei cd d'installazione delle principali distribuzioni.

Macchina server/proxy: ADSL



- Configurare la connessione ad Internet avviando da shell lo script # **adsl-setup** [1]:
 - Lo script chiederà d'inserire username, DNS primario e secondario, password forniti dall'ISP. Non specificare nessun firewall. La configurazione verrà salvata nel file `/etc/ppp/pppoe.conf`. La password, invece, nel file `/etc/ppp/pap-secrets`
- Per attivare la connessione: # **adsl-start**
- Per disattivare la connessione: # **adsl-stop**
- Per monitorare la connessione: # **adsl-status**



Macchina server/proxy: la rete



- Configurare la rete con drakconnect oppure con il comando ifconfig illustrato in precedenza.
- Assegnare come indirizzo ip del gateway l'indirizzo ip del network, ad es.: 192.168.0.0

```
[anna@happypenguin anna]$ cat /etc/sysconfig/network
HOSTNAME=happypenguin.didattica.net
NETWORKING=yes
GATEWAY=192.168.0.0
GATEWAYDEV=eth0
```



Macchina server/proxy: condivisione connessione con iptables



```
#!/bin/bash
#SCRIPT PER IL MASCHERAMENTO DEI PACCHETTI IP
#caricamento dei moduli del kernel
modprobe ip_tables
modprobe ip_conntrack
modprobe iptable_nat
modprobe ipt_MASQUERADE
#
#mascheramento dei pacchetti IP
#
echo "1" > /proc/sys/net/ipv4/ip_forward
iptables -t nat -A POSTROUTING -d ! 192.168.0.0/24 -j MASQUERADE
#
#evito lo spoofing
#
iptables -A INPUT -m state --state ESTABLISHED,RELATED -i eth0 -p \! icmp -j ACCEPT
#
#maschera tutto quello che non è destinato alla Lan
#imposta iptables per forwardare solo per la sottorete
iptables -A FORWARD -s 192.168.0.0/24 -j ACCEPT
iptables -A FORWARD -d 192.168.0.0/24 -j ACCEPT
iptables -A FORWARD -j DROP
echo ...ora si naviga!
echo
```

Macchina server/proxy: condivisione connessione



- Lo script illustrato in precedenza, dopo essere stato reso eseguibile (`# chmod +x masq`) può essere salvato in una cartella della propria home, in modo da conservarlo in caso di formattazione della partizione assegnata al file system. Per eseguirlo automaticamente ad ogni avvio del sistema sarà sufficiente inserire una stringa richiamante la sua collocazione nel file `/etc/rc.d/rc.local`:

```
[root@linuxbox]# echo >> /etc/rc.d/rc.local /home/anna/masq
```




Macchina server/proxy: condivisione stampante



- Per fare in modo che la stampante collegata al server sia disponibile sulle altre macchine della LAN, è necessario inserire i nomi e gli indirizzi dei vari hosts nel file `/etc/hosts` di tutte le macchine (server compreso), poi di seguito, riavviare la rete ed il servizio di stampa CUPS:

```
[root@linuxbox]# /etc/init.d/network restart
```

```
[root@linuxbox]# /etc/init.d/cups restart
```

Macchina server/proxy: iptables



- Regole iptables:
 - iptables -F: azzera il firewall
 - iptables -L: mostra le regole attive
 - iptables -A INPUT -i ppp0 -m state --state NEW,INVALID -j DROP: chiude porte in ingresso
 - iptables -A FORWARD -i ppp0 -m state --state NEW,INVALID -j DROP: chiude porte in uscita
 - iptables -I INPUT -p tcp --dport portachevoletevoi -m state --state NEW -j ACCEPT: apre una porta
 - iptables -t nat -A POSTROUTING -o ppp0 -j MASQUERADE: per la condivisione della connessione

Macchine client



- Sulle macchine client bisognerà solo attivare la rete con drakconnect oppure con i comandi da shell, seguendo la stessa procedura illustrata a pag. 15:
 - Inserire il nome e l'indirizzo ip della macchina (od anche delle altre macchine collegate in rete se si vogliono utilizzare altri servizi di rete) server nel file `/etc/hosts`.
 - Riavviare la rete.

[1] adsl-setup



```
>>> Enter your PPPoE user name: pippo
>>> (default eth0): eth0
>>> Enter the demand value (default yes): no
>>> Enter the DNS information here: 212.216.112.112
>>> Enter the secondary DNS server address here: 212.216.172.62
>>> Please enter your PPPoE password: *****
>>> Please re-enter your PPPoE password: *****
The firewall choices are:
0 - NONE: This script will not set any firewall rules. You are responsible
        for ensuring the security of your machine. You are STRONGLY
        recommended to use some kind of firewall rules.
1 - STANDALONE: Appropriate for a basic stand-alone web-surfing workstation
2 - MASQUERADE: Appropriate for a machine acting as an Internet gateway
                for a LAN
>>> Choose a type of firewall (0-2):0

Ethernet Interface: eth0
User name:         pippo
Activate-on-demand: No
Primary DNS:      212.216.112.112
Secondary DNS:    212.216.172.62
Firewalling:      NONE

>>> Accept these settings and adjust configuration files (y/n)? y

Type 'adsl-start' to bring up your ADSL link and 'adsl-stop' to bring
it down. Type 'adsl-status' to see the link status.
```

Bibliografia Internet



- <http://www.netfilter.org/documentation/HOWTO/NAT-HOWTO.html>
- <http://www.simonzone.com/software/guarddog/>
- <http://www.geocities.com/ilpettegolo/Linux-firewall-when-why.html>
- <http://aspinall.opengeeks.it/papers/lan.pdf>
- <http://www.commedia.it/ccontavalli/docs-it/iptables/iptables4dummies>
- <http://www.pluto.linux.it/ildp/AppuntiLinux/a2270.html>