Roma2LUG

aka “l’aula del Pinguino”

in

Laboratorio: Configurazione e Gestione della Rete Locale

Aprile 2014

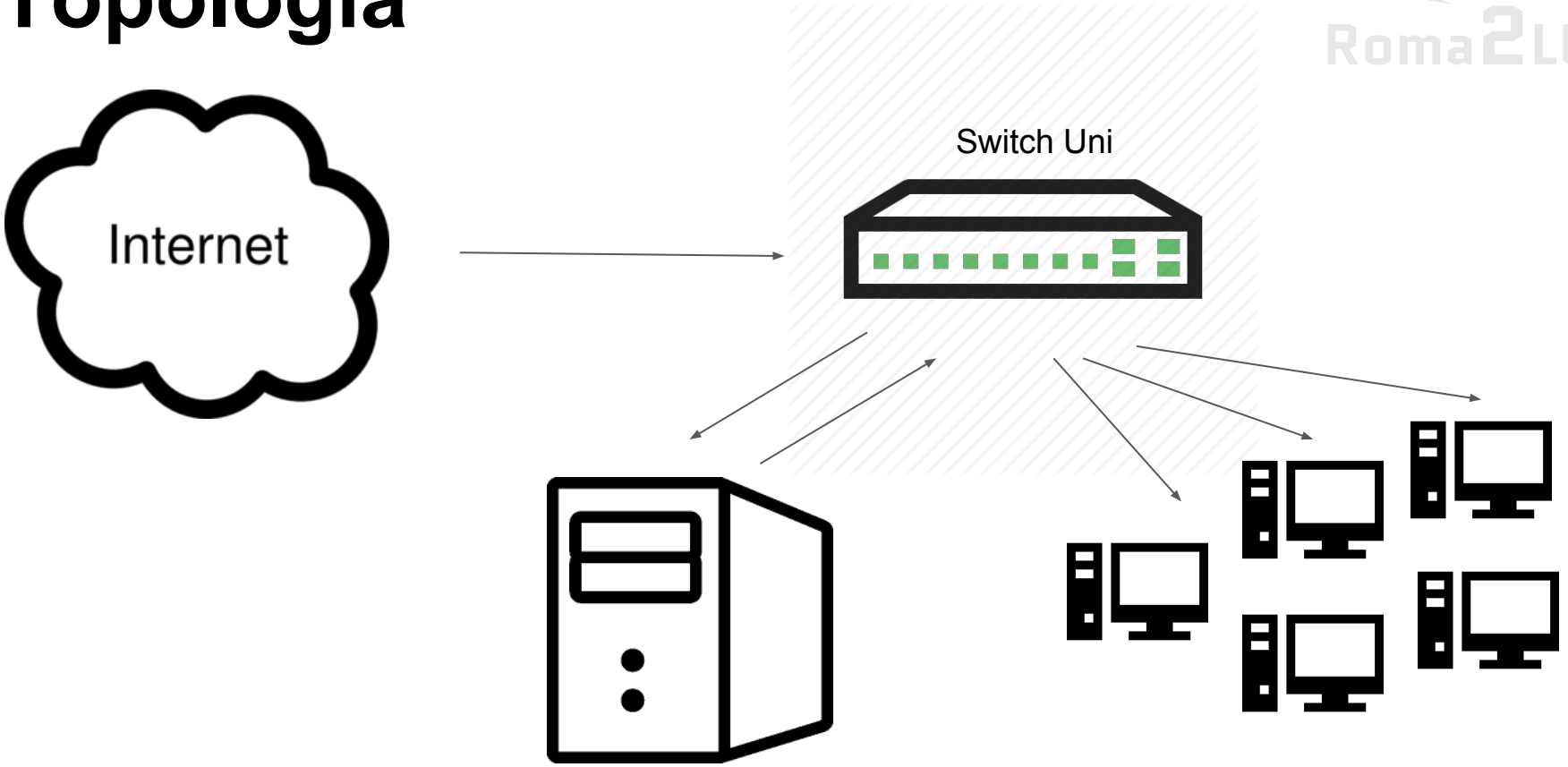
"***Microsoft Corporation***",
una Software House
statunitense, annuncia il
termine del supporto per il suo
Sistema Operativo per PC
"***Windows XP***", installato sui
computer del laboratorio

Cosa avevamo a disposizione

- 40 (+ 1) Postazioni
- Un Server
- Lo Switch Fast Ethernet dell'Università
- Un pacco di biscotti ed un paio di caffé

(magari)

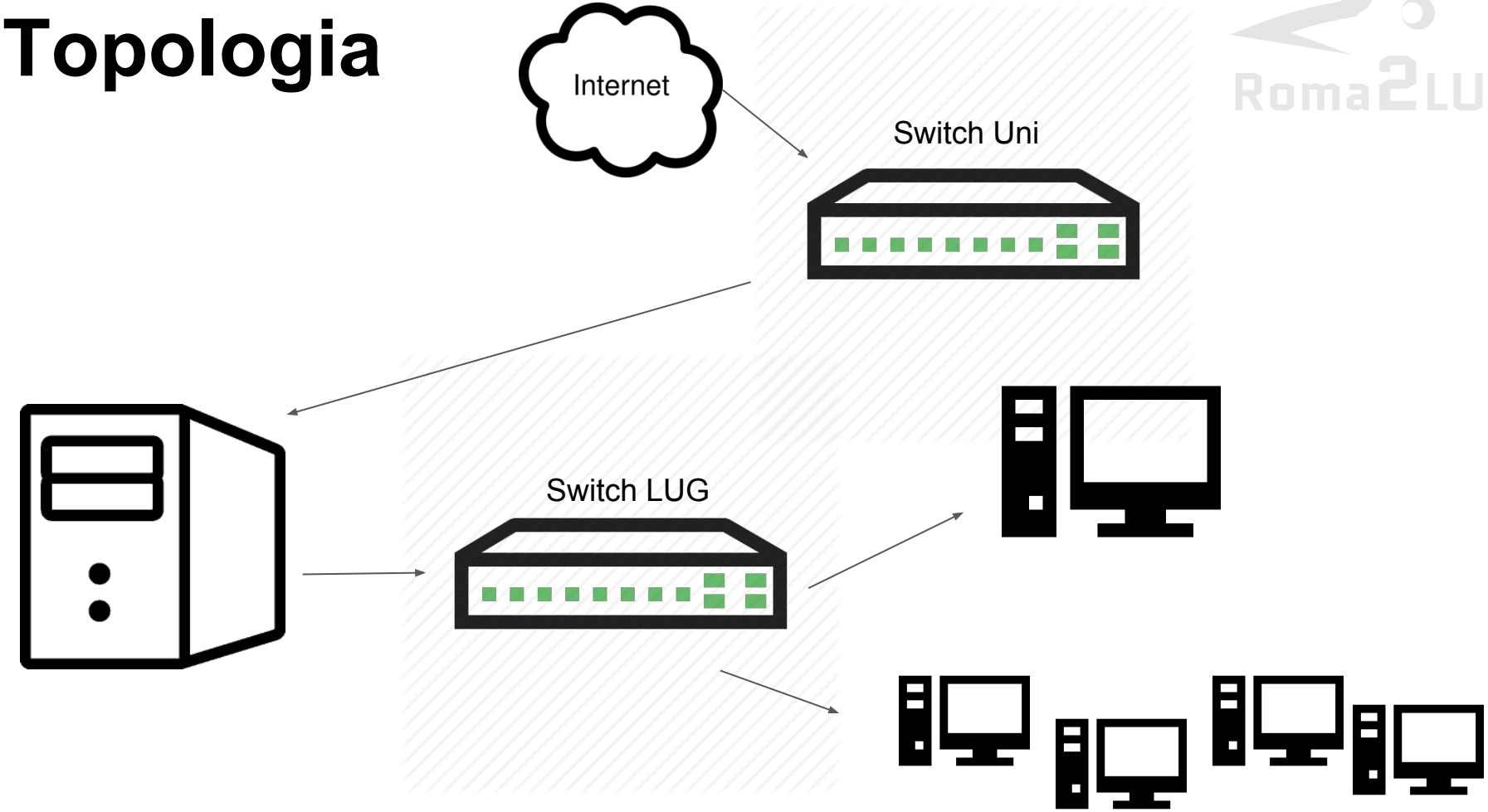
Topologia



Cosa abbiamo migliorato

- Rete locale su switch separato (con porta Gigabit su Postazione Master e Server
- Installazione via rete + WakeOnLan
- Cacher APT

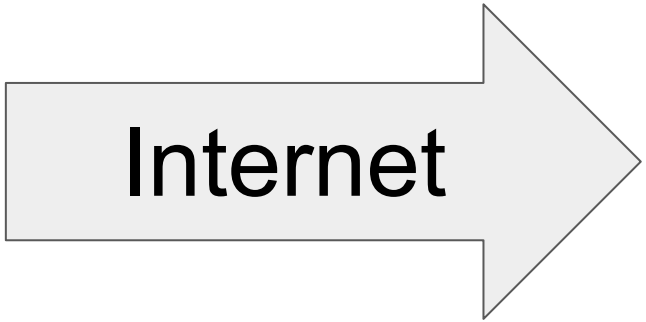
Topologia



/etc/network/interfaces

```
auto eth0
iface eth0 inet static
        address 160.80.198.225
        netmask 255.255.255.0
        network 160.80.198.0
        broadcast 160.80.198.255
        gateway 160.80.198.1
        dns-nameservers 8.8.8.8

auto br0
iface br0 inet static
        address 10.0.0.1
        netmask 255.255.0.0
        bridge_ports eth1 eth2 eth3 eth4 eth5
        bridge_stp off
        bridge_fd 0
        bridge_maxwait 0
```



DHCP - /etc/dhcp/dhcpd.conf

```
authoritative;
subnet 10.0.0.0 netmask 255.255.0.0
{
        option domain-name-servers 8.8.8.8,8.8.4.4;
        option routers 10.0.0.1;

        default-lease-time 600;
        max-lease-time 7200;

        filename "pxelinux.0";
        next-server 10.0.0.1;

        host hostXY
        {
                hardware ethernet 00:11:22:33:44:55;
                fixed-address 10.0.2.XY;
                option host-name "hostXY";
        }
}
```

NETBOOT

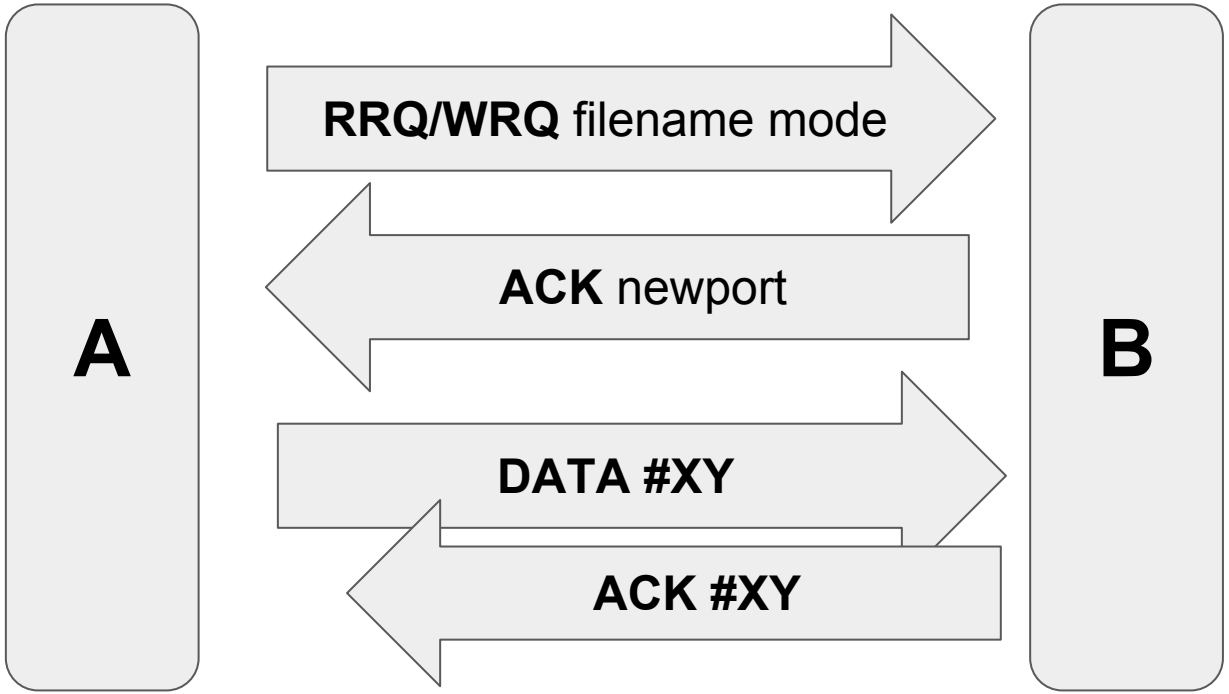
Solo i dispositivi autorizzati ricevono un indirizzo IP

TFTP

Trivial File Transfer Protocol (**TFTP**) è un protocollo di trasferimento file di livello applicativo molto semplice, con le funzionalità di base del FTP. È utile sia per l'avvio di thin client che per eseguire installazioni multiple

- UDP 69 (invece della TCP 21)
- non supporta la navigazione tra le directory;
- non possiede meccanismi di autenticazioni o cifratura;
- può essere usato per leggere o scrivere file da un server remoto;
- supporta tre differenti modalità di trasferimento
  * "netascii" (FTP "ASCII")
  * "octet" (FTP "image" (binario)
  * "mail" (obsoleta)
- ha un limite di dimensione dei file di 32 MB.

TFTP (2)



L'host di origine invia dei pacchetti DATA numerati all'host di destinazione, tutti **tranne l'ultimo** contenenti un blocco di dati completo.

Il pacchetto DATA finale deve contenere un blocco di dati non pieno ad indicare che si tratta dell'ultimo. Se la dimensione del file trasferito è un multiplo esatto invia un ultimo pacchetto di dati contenente 0 byte di dati.

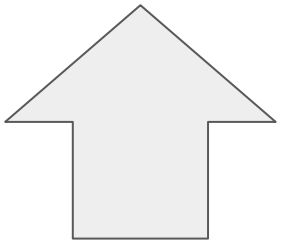
Netboot - /etc/xinetd.d/tftp

```
service tftp
{
    disable          = no
    socket_type    = dgram
    wait             = yes
    user             = root
    server           = /usr/sbin/in.tftpd
    server_args    = -v -s /var/lib/tftpboot
    only_from      = 10.0.0.0/16
    interface        = 10.0.0.1
}
```

Boot Menu && Preseed

/var/lib/tftpboot/ubuntu-installer/amd64/boot-screens/txt.cfg:

```
default install
label install
        menu label ^Installa
        menu default
        kernel ubuntu-installer/amd64/linux
        ipappend 1
        append      net.ifnames=1 biosdevname=0 vga=788 initrd=ubuntu-installer/amd64/initrd.gz
                    locale=it_IT keyboard-configuration/layoutcode=it ksdevice=eth0 interface=eth0
                    hostname=unassigned url=http://10.0.0.1/preseed.cfg
```



Apache

Ci facciamo bastare

“*Listen 10.0.0.1:80*”

in **/etc/apache/ports.conf**

Samba

```
interfaces = br0
bind interfaces only = yes

[shared]
path = /srv/folder
valid users = roma2lug,root
read only = no
writeable = yes
create mask = 0777
directory mask = 0777
```

Iptables ;))

```
#!/bin/sh
### BEGIN INIT INFO
# Provides:          iptables
# Required-Start:    mountkernfs $local_fs
# Required-Stop:     $local_fs
# Default-Start:     2 3 4 5
# Default-Stop:      0 1 6
# Short-Description: Set up iptables rules
### END INIT INFO

iptables=/sbin/iptables

### NETWORKS ###
ReteInterna        =      "10.0.0.0/16"

### IP ROUTER ###
IpRouterPubblico=      "160.80.198.225"
IpRouterPrivato  =     "10.0.0.1"

### INTERFACCE ROUTER ###
InterfacciaEthInterna   =      "br0"
InterfacciaEthEsterna   =      "eth0"
```

Iptables ;))

```
configuration()
{
   start_internet

   ##### Router #####

        $iptables -A INPUT -i lo -j ACCEPT

        $iptables -t filter -A INPUT -p udp --dport 27960 -j ACCEPT
        $iptables -t filter -A INPUT -p udp --dport 27950 -j ACCEPT
        $iptables -t filter -A INPUT -p udp  --dport 53   -j ACCEPT

        #### Servizio ssh #####
        $iptables -t filter -A INPUT -p tcp -d $IpRouterPubblico --dport 22   -j ACCEPT

        $iptables -t filter -A INPUT -p tcp -d $IpRouterPubblico --dport 2222 -j ACCEPT


}
```

Iptables ;))

```
start()
{
   configuration

   ##### FORWARD #####

         $iptables -t filter -P FORWARD DROP

         $iptables -t filter -A FORWARD ! -s $ReteInterna -m state --state ESTABLISHED,RELATED -j ACCEPT
         $iptables -t filter -A FORWARD -s $ReteInterna -j ACCEPT

         ##### INPUT #####

         $iptables -t filter -P INPUT DROP

         $iptables -t filter -A INPUT ! -s $ReteInterna -m state --state ESTABLISHED,RELATED -j ACCEPT
         $iptables -t filter -A INPUT -s $ReteInterna -j ACCEPT
         $iptables -t filter -A INPUT -p icmp -j ACCEPT

         ##### POSTROUTING #####

         $iptables -t nat -A POSTROUTING -o $InterfacciaEthEsterna -s $ReteInterna -j SNAT --to-source
$IpRouterPubblico
         $iptables -t nat -A POSTROUTING -o $InterfacciaEthInterna -s $ReteInterna -j SNAT --to-source
$IpRouterPrivato

          # MasterSSH #
          $iptables -t nat -A PREROUTING -p tcp -d $IpRouterPubblico --dport 2222 -j DNAT --to-destination 10.0.1.1:22


         echo 1 > /proc/sys/net/ipv4/ip_forward
}
```

Iptables ;))

```
stop_internet()
{
   $iptables -t mangle -F
   $iptables -t mangle -P PREROUTING DROP

   $iptables -t mangle -A PREROUTING ! -s $ReteInterna -j ACCEPT
   $iptables -t mangle -A PREROUTING -s $ReteInterna -m mac --mac-source 00:MA:ST:ER:11:22 -j
ACCEPT

}

start_internet()
{
   $iptables -t mangle -F
   mac_filter
}

mac_filter()
{
   ##### MAC Address filtering #####

   $iptables -t mangle -P PREROUTING DROP

   $iptables -t mangle -A PREROUTING ! -s $ReteInterna -j ACCEPT
   $iptables -t mangle -A PREROUTING -s $ReteInterna -m mac --mac-source 00:11:22:33:44:55 -j ACCEPT
}
```

Iptables ;))


```
stop() {
        echo 0 > /proc/sys/net/ipv4/ip_forward
        $iptables -t nat -F
        $iptables -t filter -F
        $iptables -t mangle -F
        $iptables -t filter -P FORWARD ACCEPT
        $iptables -t filter -P INPUT ACCEPT
        $iptables -t mangle -P PREROUTING ACCEPT
}
```

```
case "$1" in
        start)
                start
                echo "Start OK"
                ;;

        stop)
                stop
                echo "Stop OK"
                ;;

        restart)
                stop
                echo "Stop ..."
                sleep 2
                start
                echo "Restart OK"
         ;;
```

```
start_internet)
                start_internet
                echo "Internet in ON"
                ;;

        stop_internet)
                stop_internet
                echo "Internet in OFF"
                ;;
        *)
                echo "Usage: iptables {start|stop|restart|stop_internet|start_internet}" >&2
                exit 1
                ;;

esac

exit 0
```