Wireless Network Esercitazioni

Alessandro Villani
avillani@science.unitn.it

Wireless Router WRT54G

LINKSYS

WRT54G

- È un router Wireless:
  - 1 porta Ethernet verso la LAN esterna
  - 4 porte Ethernet switch
  - 802.11b e 802.11g
- La particolarità è che esegue un firmware "linux"
- La Linksys ha rilasciato i sorgenti del firmware:

  http://www.linksys.com/support/gpl.asp

WRT54G: Hardware & Software

- RAM da 8MB
- CPU MIPS32 a 200MHz
- 5 port Ethernet 10/100
- Memoria Flash da 4MB

WRT54G: Hardware & Software

- Quasi tutti i comandi di sistema sono realizzati utilizzando BusyBox: un piccolo singolo eseguibile che combina molte delle utility UNIX più comuni:

  http://www.busybox.net/
- Il Web server installato di default è ACME mini_http:

  http://www.acme.com/software/mini_httpd/
- I file binari ovviamente sono tutti 32 bit MIPS

WRT54G: Molti Firmware

- Sveasoft (non più “free”):

  http://www.sveasoft.com/

  http://firmware.carlsonwebdesigns.com/Sveasoft/
- Ewrt:

  http://www.portless.net/menu/ewrt/
- HyperWRT:

  http://www.hyperwrt.org/
- Wifibox:

  http://sourceforge.net/projects/wifi-box/
- TinyPEAP (radius server con PEAP):

  http://www.tinypeap.com/

WRT54G: Cross Compile

- È possibile compilare per MIPS32 su architettura i386
- Un buon punto di partenza è:
  http://www.kegel.com/crosstool/
- Utilizzando quest'ambiente di compilazione è possibile cross-compilare qualunque cosa
- Nota: se non si hanno esattamente le librerie del firmware un banale hello_world.c può arrivare a 580KB e un hello_world.cc fino a 4.1MB!

WRT54G: Aggiornamento Firmware

- Come esempio di utilizzo di uno dei firmware disponibili abbiamo installato su un WRT54G una delle vecchie versioni del firmware della sveasoft: Firmware_Samadhi2_v2_2.00.8.6sv.bin

WRT54G: Aggiornamento Firmware

- Configurazione via WEB a partire dal firmware originale (login vuota e password admin)
- Assegnato un IP al router (l'ip di default è 192.168.1.1) si aggiorna il firmware via WEB
- A questo punto si possono abilitare le connessioni ssh
- La login è root, la password (di default) è admin

WRT54G: Comandi

- La documentazione è reperibile all'indirizzo:
  http://docs.sveasoft.com/
- Si possono eseguire molti comandi unix:
  - ls
  - cd
  - ifconfig
  - cat
  - ps

WRT54G: Filesystem

- La struttura del filesystem è quella di un sistema linux:

```
# ls -l /
drwxr-xr-x    1 0        0             211 Jan 17  2004 bin
drwxr-xr-x    1 0        0               0 Jan  1 00:00 dev
drwxr-xr-x    1 0        0             144 Jan 17  2004 etc
drwxr-xr-x    1 0        0             130 Jan 17  2004 lib
drwxr-xr-x    1 0        0               0 Jan 17  2004 mnt
dr-xr-xr-x   31 0        0               0 Jan  1  2000 proc
drwxr-xr-x    1 0        0             311 Jan 17  2004 sbin
drwxr-xr-x    1 0        0               0 Jan  1  2000 tmp
drwxr-xr-x    1 0        0              29 Jan 17  2004 usr
lrwxrwxrwx    1 0        0               7 Jan 17  2004 var ->
  tmp/var
drwxr-xr-x    1 0        0             906 Jan 17  2004 www
```

WRT54G: Filesystem

- Ad esempio:

```
# cat /proc/cpuinfo
system type             : Broadcom BCM947XX
processor               : 0
cpu model               : BCM3302 V0.7
BogoMIPS                : 199.47
wait instruction        : no
microsecond timers      : yes
tlb_entries             : 32
extra interrupt vector  : no
hardware watchpoint     : no
VCED exceptions         : not available
VCEI exceptions         : not available
dcache hits             : 2130583210
dcache misses           : 63489
icache hits             : 3120555732
icache misses           : 4198445950
instructions            : 0
```

WRT54G: Filesystem

- Ad esempio:

```
# cat /proc/version
Linux version 2.4.20 (root@linuxdev1) (gcc version 3.0
  20010422 (prerelease) with bcm4710a0 modifications)
  #254 Sat Jan 17 09:44:40 EST 2004
# cat /proc/mounts
rootfs / rootfs rw 0 0
/dev/root / squashfs ro 0 0
none /dev devfs rw 0 0
proc /proc proc rw 0 0
ramfs /tmp ramfs rw 0 0
```

WRT54G: Comandi Linksys

- wl è il comando generico per la gestione dell'interfaccia radio:
  - wl ver → versione del sistema
  - wl radio → stato dell'802.11
  - wl radio on → attiva 802.11
  - wl radio off → spenge 802.11
  - wl chanlist → lista dei canali validi
  - wl channels_in_countr IT b → canali validi in Italia per 802.11b

WRT54G: Comandi Linksys

- Ad esempio:

```
# wl ver
wl:      3.50 RC21.0
         wl0: Nov  5 2003 16:26:18 version 3.50.21.0
# wl radio
radio is on (WL_RADIO_SW_DISABLE 0 WL_RADIO_HW_DISABLE
  0)
# wl cwmax
cwmax is 1023(0x3ff)
# wl cwmin
cwmin is 15(0xf)
# wl cwmin 30
# wl cwmin
cwmin is 30(0x1e)
# wl txpwr
txpwr is 28
```

WRT54G: Possibili Applicazioni

- Installare regole di instradamento, firewalling, traffic shaping direttamente sull'AP
- Installare un end-point VPN → non c'è più bisogno di WEP
- Installare un *captive portal* direttamente sull'AP → il firmware sviluppato da PortLess Network implementa questa feature:

  http://www.portless.net/menu/ewrt/