



ИНФОРМАЦИОННО
ОБСЛУЖВАНЕ

Linux върху безжични маршрутизатори

Александър Станев
Ръководител "Oracle технологии"
Финансови и данъчни системи
Информационно обслужване АД

Какво е това?

Все по-широко разпространени устройства,
комбиниращи router, ethernet switch и wireless
карта



Какво има под капака?

- **CPU** – MIPS архитектура, най-често се използват процесори на Broadcom, работещи с тактова честота 125 MHz - 300 MHz
- **RAM** – 16 MB - 64MB
- **Flash memory** – 4 MB – 32MB
- **WIFI card** – Broadcom chipset
- **4+1 switch** – разделени в два VLAN-а по подразбиране

- **USB** порт
- **Сериен порт (COM)**
- **SD/MMC card** интерфейс

Възможности на стандартния firmware на Linksys

- Стандартно, устройствата на Linksys (сега собственост на Cisco) идват с Linux ядро 2.4 базиран firmware, който е доста ограничен ОТКЪМ ВЪЗМОЖНОСТИ
- Насочен към SOHO пазара, съдържа:
 - Уеб базиран интерфейс за управление
 - Wireless с WEP/WPA оторизация към базовата станция
 - SPI firewall
 - Ограничение на достъпа до Интернет на потребителите в локалната мрежа
 - Port forwarder
 - UPNP
 - други



Linux дистрибуции за WRTs

- Как избираме?
 - Възможности / необходимост
 - Активно разработвана и поддържана
 - Познания и опит с Linux
 - Свободно време
 - Здрави нерви ;)
- Масово базирани на 2.4 ядро
- Съществуват различни firmware-а (на практика дистрибуции), но само някои са под активна разработка:
 - **OpenWRT**
 - **DD-WRT**
 - **Tomato**
 - **HyperWRT Thibor**
 - **FreeWRT** (<http://www.freewrt.org>) – Appliance Development Kit (ADK)– ако искате да разработите специализирано (embedded) устройство
 - ...



OpenWRT

- Адрес: <http://www.openwrt.org>
- Базовата Linux дистрибуция за безжични маршрутизатори
- Разработва се от начало, не е базирана на кода на Linksys
- Поддържа най-голям брой различни хардуерни устройства, в сравнение с останалите дистрибуции
- Потребителя трябва да има опит с Linux ОС, тъй като уеб базирания интерфейс не е достатъчно развит към момента
- Поддържа ipkg пакети, което дава възможност дистрибуцията да бъде много фино моделирана

```
YOP
[yannick@yop ~] ssh root@192.168.1.1
root@192.168.1.1's password:

BusyBox v1.00 (2006.03.27-00:00+0000) Built-in shell (ash)
Enter 'help' for a list of built-in commands.

      _ _ _ _ _
     /   /   /   /   /   /   /   /   /   /   /   /   /   /   /
    /___/___/___/___/___/___/___/___/___/___/___/___/___/___/
   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |
   |___|___|___|___|___|___|___|___|___|___|___|___|___|___|
   | W I R E L E S S   F R E E D O M
   |___|___|___|___|___|___|___|___|___|___|___|___|___|___|
  WHITE RUSSIAN (RC5) -----
  * 2 oz Vodka   Mix the Vodka and Kahlua together
  * 1 oz Kahlua  over ice, then float the cream or
  * 1/2oz cream  milk on the top.
  -----
root@OpenWrt:~#
root@OpenWrt:~#
root@OpenWrt:~#
```

CATEGORIES: Info Status System »Network«

OpenWrt Admin Console

Host Name: OpenWrt
Uptime: 12 days
Load: 0.14, 0.12, 1.03
Version: WHITE RUSSIAN (pre-RC5)

LAN WAN »Wireless« Advanced Wireless Hosts Firewall

Wireless Configuration

Wireless Configuration

Wireless Interface: Enabled

ESSID Broadcast: Show

ESSID:

Channel:

Mode: Access Point

ESSID:
Name of your Wireless Network

Mode:
This sets the operation mode of your wireless network. Selecting 'Client (Bridge)' will not change your network interface settings. It will only set some parameters in the wireless driver that allow for limited bridging of the interface. [more...](#)

Encryption Settings

Encryption Type: WPA (PSK)

WPA Mode: WPA1 WPA2

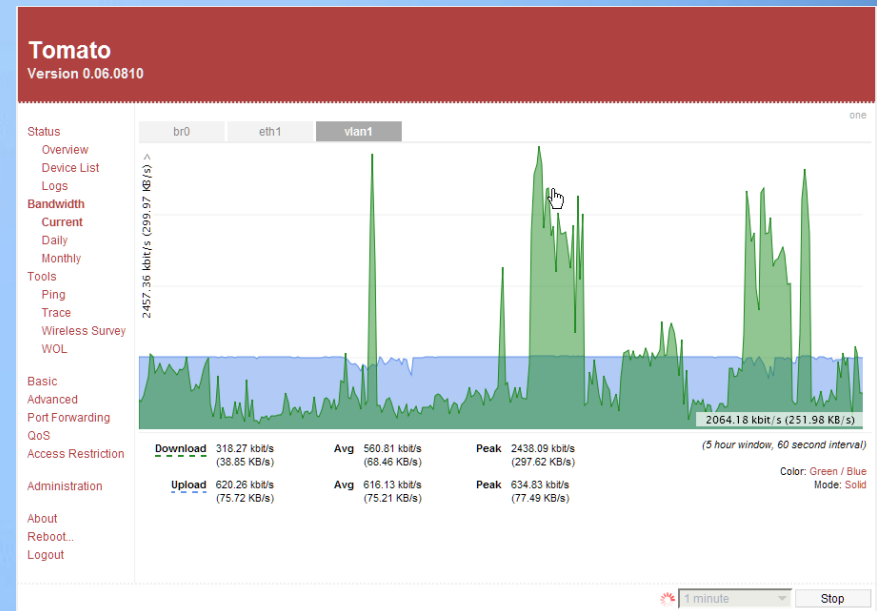
WPA Algorithms: RC4 (TKIP) AES

WPA PSK:

Encryption Type:
"WPA (RADIUS)" is only supported in Access Point mode.
"WPA (PSK)" doesn't work in Ad-Hoc mode.

Tomato

- Адрес:
<http://www.polarcloud.com/tomato>
- Нова дистрибуция
- Лесен за използване уеб интерфейс, базиран на AJAX и DHTML
- Добри възможности за наблюдение и статистика
- Възможност за автоматично обновяване на системните пакети през интерфейса
- Подходяща за начинаещи потребители, без високи изисквания



HyperWRT Thibor

- Адрес: <http://www.thibor.co.uk>
- Широко разпространена преди известно време
- Базирана на кода на Linksys, като го поправя и допълва функционалността
- Дистрибуцията е събрала модификациите на няколко прекъснати проекта, като отделните модули са стабилизирани и напаснати
- Все пак, ако попаднете на такава, спокойно можете да я замените с ...



DD-WRT

- Адрес: <http://www.dd-wrt.com>
- Базирана на firmware-а на Sevasoft, но с множество промени и подобрения
- Налични на няколко различни варианта на дистрибуцията в зависимост от необходимите функционални възможности
- Поддържа възможност за работа с ipkg пакети
- Работи и на новите “кутийки” на Linksys, версия 5 и 6

DD-WRT CONTROL PANEL

Firmware: DD-WRT v23 SP2 (09/15/06) std
Time: 19:23:05 up 19:23, load average: 0.11, 0.02, 0.00
WAN IP: 85.187.56.61

Setup Wireless Security Access Restrictions Applications & Gaming Administration **Status**

Router LAN Wireless

Router Information

Router Information		Help	more...
System			
Router Name	sinzone	Router Name:	This is the specific name for the router, which you set on the <i>Setup</i> tab.
Router Model	Linksys WRT54G/GL/GS	MAC Address:	This is the router's MAC Address, as seen by your ISP.
Firmware Version	DD-WRT v23 SP2 (09/15/06) std - build 3932	Firmware Version:	This is the router's current firmware.
MAC Address	00:48:54:1A:AC:15	Current Time:	This is time received from the ntp server set on the <i>Administration / Management</i> tab.
Host Name		Uptime:	This is a measure of the time the router has been "up" and running.
WAN Domain Name		Load Average:	This is given as three numbers that represent the system load during the last one, five, and fifteen minute periods.
LAN Domain Name			
Current Time	Not available		
Uptime	19:25		
Load Average	0.00, 0.01, 0.00		
CPU			
CPU Model	Broadcom BCM4712 chip rev 2		
CPU Clock	216 MHz		

DD-WRT – възможности: Изцедете хардуера

Чрез манипулиране на NVRAM регистрите от web интерфейса могат да се задават някои параметри на устройството:

- Активиране на всички 14 wireless канали
- Повишаване мощността на изходния сигнал – стандартно е 28 mW, възможност до 251 mW
- Overclocking на процесора
- Конфигуриране режима на работа на антените
- Ядрото е компилирано с поддръжка на Secure Digital/MultiMedia Cards

DD-WRT – ВЪЗМОЖНОСТИ: Софтуер

Вградените функции могат да се разширят и с пакети от OpenWRT, стига да има достатъчно място

- Възможност за преконфигуриране на VLANs, включително wireless client isolation
- Разширена поддръжка за динамични DNS услуги
- Работа като безжичен клиент към друг access point
- Детайлно дефиниране на QoS за мрежата, включително и поддръжка на WiFi MultiMedia QoS (WMM)
- Използване на външен syslog daemon
- Автоматично свързване (mount) по SMBFS към друга машина, от където могат да се зареждат допълнителни модули
- Поддръжка на WPA2, WPA в WDS; WPA/TKIP с AES алгоритъм за криптиране
- Вграден PPTP клиент и PPTP сървър
- Wireless Distribution System (WDS) – създаване на взаимно свързани hotspots
- Централизирано управление на WDS – чрез Chillspot и Sputnik агенти



DD-WRT – възможности: Специални версии

- **Micro version**
 - Не включва PPTP клиент/сървър и SSH достъп – намалението на големината дава възможност да се използва на устройства с хардуерна версия 5 и 6
 - Няма web интерфейс
- **Mini version**
 - Съдържа PPTP и SSH, но все още е с твърде малка функционалност – дава възможност да се инсталират множество допълнителни пакети
 - Няма web интерфейс
- **Standard version**
 - Стандартната версия, съдържаща всички гореописани блягинки
- **VoIP version**
 - Съдържа SIPatH, даващ възможност да терминирате VoIP телефония
- **VPN version**
 - Съдържа OpenVPN

Как се инсталира?

Можете да инсталирате новия firmware по няколко начина, като за начало най-лесния е за предпочитане – през web интерфейса на устройството

- Проверете дали вашия хардуер се поддържа от избраната дистрибуция
- Изберете необходимия ви вариант на firmware-a, ако има такива
- Запознайте се с детайлните инструкции за вашия модел устройство – понякога има и допълнителни стъпки, които трябва да се предприемат
- Съхранете работещата мрежова конфигурация – ще ви потрябва по-късно, когато настройвате новия firmware
- Инициализирайте настройките на устройството – “Reset to factory defaults”
- **НЕ** инсталирайте новия firmware по wireless – използвайте кабел!
- **НЕ** прекъсвайте обновяването, бъдете търпеливи!

След инсталацията

- Ако току-що сте сменили дистрибуцията, силно препоръчително е да инициализирате конфигурацията избирайки “Reset to factory defaults”
- Направете необходимите настройки “на ръка” – така ще сте сигурни, че няма да са останали паразитни параметри, които владеят наистина мръсни номера
- Проверете дали базовата функционалност работи стабилно, преди да конфигурирате допълнителни услуги

Не пали!

- Ако устройството ви не работи след зареждането на новия firmware, не бързайте да го ускорявате (9.8 m/s^2)
- Безмълвното състояние на router-а често по форумите се реферира като “bricked”
- Може да се наложи да направите лека хардуерна интервенция. Ако не си падате по такива неща, най-добре повикайте приятел-жичкаджия
- Ако е била включена опцията Boot wait, имате 5 секунди след всеки рестарт, за да заредите работещ firmware по TFTP. Детайлни инструкции за това може да се намери на уики страницата на DD-WRT

Трикове и съвети

- Увеличаване на изходната мощност
 - Няма смисъл да я увеличавате на повече от 100 mW. Не забравяйте, че клиентите също трябва да могат да излъчват по-мощно, за да има смисъл, а и ако не използвате специални антени се получава изкривяване на сигнала
- Когато машината се задъхва
 - Ако активно използвате Интернет (например се закачате към peer-to-peer мрежи) е добре да увеличите броя на максимално допустимите паралелни връзки, както и да изключите някои от правилата на SPI firewall-a
- Разпечатайте си инструкциите за възстановяване на bricked устройство преди обновяване на firmware-a, защото след това може да нямате Интернет :)

За напреднали: NVRAM променливите

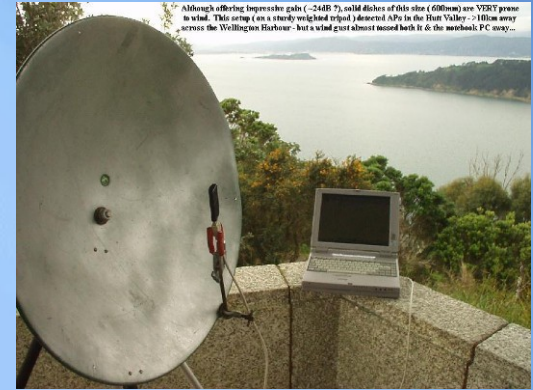
- Non-Volatile RAM променливите са области в паметта, чрез които детайлно се конфигурира устройството. Записват се на flash-а, тоест те се запазват след рестартиране
- Повечето дейности през уеб интерфейса манипулират точно тези променливи
- Всяка дистрибуция може да дефинира и използва променливи за своите нужди
- Възможно е да се управляват и ръчно през SSH:

```
nvrnm [show|commit|[get|set|unset]  
      [variable[=value]]]
```

Хардуерни модификации:

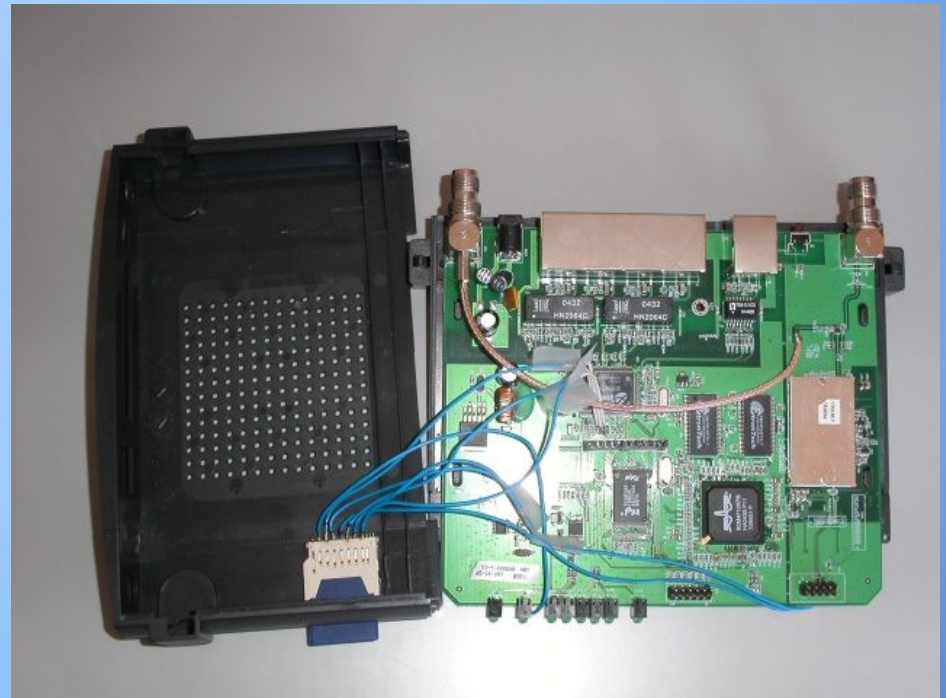
Антени

За подобряване качеството на сигнала е много важно да разполагате с качествени антени. Можете да закупите по-добри, или да се изявите като домашен майстор и си направите сами



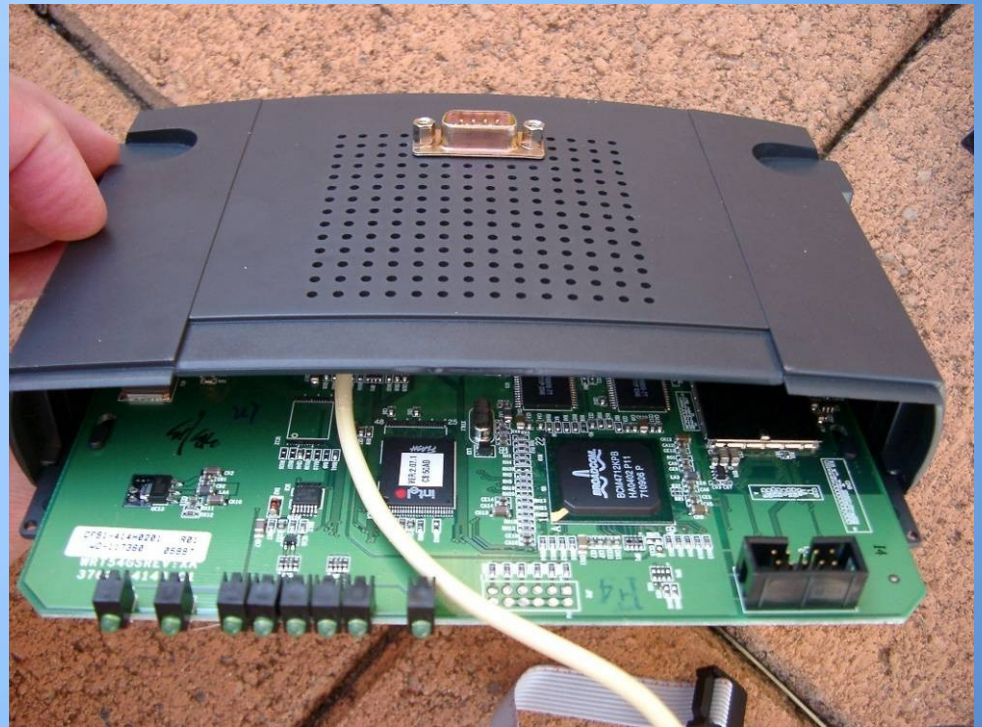
Хардуерни модификации: SecureDigital card

Отеснялата стара SD карта от цифровия апарат може да се използва като допълнителна памет за router-а. За тази модификация ще ви трябва само малко сръчност при запояването



Хардуерни модификации: Сериен порт

В зависимост от модела на устройството ви имате възможност да изведете и използвате един или два серийни (COM) порта. Чрез тях може да управлявате външно устройство



Още възможности

- Закачете и използвайте устройства на USB порта – web камери, принтери, памет ...
- Подслушване на безжичния трафик – интеграция със Snort IDS, работещ на външна машина
- Можете да използвате повече от един uplink provider, като си поиграете с VLAN настройките. Разбира се, в домашни условия трудно ще направите истински load balancing, без да разполагате с автономна мрежа
- Max Moser успя да подкара Metasploit средата върху router-а



ИНФОРМАЦИОННО
ОБСЛУЖВАНЕ

stampit



Край!



Александър Станев

a.stanev@is-bg.net

<http://www.is-bg.net>

<http://www.stanev.org>



TPLB.

This page intentionally left blank.