MTA SZTAKI

Biztonságos wireless megoldás OpenWRT alapokon

Ormos Pál
MTA SZTAKI
ormos@sztaki.mta.hu

Networkshop 2012

Miről lesz szó?

- Tartalomjegyzék
  - Előzmények
  - Openwrt bemutatása
  - Tanulságok
  - Biztonság
  - Összefoglalás

Előzmények

- Elavult wireless infratruktúra az intézetben
  - Csak 11b-t tudó eszközök
  - Nem tudunk több SSID hirdetni ugyanazon az eszközön
  - csak WPA támogatás
    - 2013-tól az Eduroam ezt nem engedi meg
  - emiatt a laborok, osztályok saját eszközöket raknak fel a hálózatra **è** sokszor nyílt AP-k maradnak
    - A hálózat üzemeltetés ezen része nem a mi kezünkben van, ezért rálátásunk sincs a dologra
    - Nem egységes a konfiguráció, nincs központi menedzselés **è** nem lehet biztonságban az, aki az intézeten belül wifit használ

Követelményeink a Wifivel szemben

- Az alábbi követelményeket fogalmaztuk meg az új Wireless infratruktúrával kapcsolatban:
  - WPA2 támogatás
  - Költséghatékonyság
  - Több SSID kezelés
  - Eduroam
  - Radius+LDAP authentikáció
  - Menedzselhető legyen
  - Támogassa a netflow exportot
  - VLAN trunking támogatás (802.1q)
  - Tűzfal szabályokat lehessen alkalmazni VLAN-ként
  - Egységes konfiguráció, hordozható legyen ugyanolyan típusú AP-kra
  - Log küldése központi logszerverre
  - Wireless roaming
  - Felügyelhetőség
  - VPN támogatás

Firmwarek összehasonlítása

	Gyári firmware	DD-WRT	OpenWRT
WPA2 támogatás	+	+	+
Költéshatékonyság	+	+	+
Több SSID	+	+	+/-*
Eduroam	+	+	+
Radius+LDAP	+	+	+
Menedzselhetőség	+/-**	+	+
Netflow	-	+	+

- Léteznek ezen kívül is még open source megoldások, de azok csak korlátozott platformon (Linksys wrt54G, Asus500) vehetők igénybe, így számunkra nem is jöhettek szóba

* Atheros chipset esetén nem működik a multi SSID

** Csak webes interfacen keresztül menedzselhető

Firmwarek összehasonlítása 2.

	Gyári firmware	DD-WRT	OpenWRT
Vlan trunking	-	+/-***	+
Tűzfal	+	+	+
Hordozhatóság	+	+	+
Távoli log	+/-****	+/-****	+
Wifi roaming	+	+	+
Felügyelhetőség	+	+	+
VPN támogatás	-	+	+

*** Broadcom chipsetre a legfrisebb firmware verzióban nincs támogatás. Csak atheros chipset esetén működik a VLAN trunking

**** Korlátozottan működik. Nem lehet pl. logging facility-t állítani. Nálunk ez fontos dolog a feldolgozás során

OpenWrt Wireless Freedom a kiválasztott

Miért OpenWrt?

- A gyári firmware-k nem tudták teljesíteni az előre megfogalmazott igényeinket, de az OpenWRT igen
- Open source, folyamatosan fejlesztik
- Próbáltunk más open source megoldásokat, de nem működtek stabilan, vagy csak bizonyos típusokon működnek
- Korábbi GVOP projekt keretében már kipróbáltuk és az osztályon levő eszközön folyamatosan használjuk nem csak wireless célra
- Rengeteg platformon használható
  - Az új eszközökre is folyamatosan elérhetővé teszik
- Több funkciót is tud, mint amit megfogalmaztunk a követelményekben
  - Nyomtatót használhatunk USB-n keresztül

OpenWrt Wireless Freedom bemutatása

- https://openwrt.org/
- http://wiki.openwrt.org/
- Weben és CLI-n keresztül konfigurálható
  - Webet le lehet tiltani tűzfal szabályokkal
  - Weben keresztül nem lehet minden funkciót beállítani
- Létezik egyéb verziója is
  - Gargoyle http://www.gargoyle-router.com/index.php
- Linux alapú
- Saját firmware készíthető
  - OK: pl. nem fér bele a webes interface
  - Egységesen telepített csomagok miatt így hordozhatóvá válik
  - Saját igényeink miatt testre akarjuk szabni

OpenWrt Wireless Freedom bemutatása 2.

- Open source, folyamatosan fejlesztik
- Radius + LDAP authentikáció támogatása
- Többféle platformon is elérhető
  - TP-Link, Linksys, Asus, D-Link, Fonera, stb
- Rengeteg hasznos csomag telepíthető fel rá egyszerűen
  - Pl. Asterisk, ipsec,snmp, freeradius,fprobe
- Ha van usb portunk az AP-n
  - akkor akár nyomtató, akár samba szerverként is tud működni
  - mobil 3g-t is használhatunk vele
- Captive portál támogatás
  - A felhasználók miatt nálunk is lenne rá igény

OpenWrt bemutatása 3.

- Wireless repeater funkciót is tud
- Támogatja a wireless roamingot
- DynDNS támogatás
- Támogatja az IPv6-t (nem próbáltuk még)

OpenWrt Wireless Freedom konfiguráció

- Webes felülete kezdőknek egyszerűen használható
  - Nem tud minden funkciót beállítani
- SSH-n keresztül gyakorlottabbaknak
  - nem alap funkciók beállításához
- Külön-külön konfigurációs fájlokban vannak eltárolva a beállítások
  - /etc/config alatt vannak
  - A vpn konfigurációt tegyük külön file-be és ne a network alá
- Egyes funkciókhoz külön csomagokat kell telepíteni, vagy eltávolítani a meglévőt
  - Pl. opkg install wpad *Több SSID használatához erre szükség van*
  - Pl. opkg install kmod-usb2 USB miatt

OpenWrt konfiguráció példa

Wireless konfiguráció példa

```
config 'wifi-device' 'wl0'
  option 'type' 'broadcom'
  option 'disabled' '0'
  option 'channel' 'auto'

config 'wifi-iface'
  option 'device' 'wl0'
  option 'ssid' 'eduroam'
  option 'network' 'lan2'
  option 'mode' 'ap'
  option 'encryption' 'wpa2'
  option 'key' ' xxxxxxxx'
  option 'server' 'x.y.v.z'
  option 'port' '1812'
```

Tűzfal konfiguráció példa

```
config 'rule'
        option 'src' 'lan'
        option 'src_ip' '192.168.1.2'
        option 'dest_port' '80'
        option 'proto' 'tcp'
        option 'target' 'ACCEPT'
config 'rule'
        option 'src' 'lan17'
        option 'dest' 'wan'
        option 'src_ip' '10.100.1.0/24'
        option 'proto' 'tcp'
        option 'dest_port' '22'
        option 'target' 'ACCEPT'
```

OpenWrt Wireless Freedom konfiguráció példa 2.

3G konfiguráció példa

```
config 'interface' 'wan'
 option 'ifname' 'ppp0'
 option 'proto' '3g'
 option 'device' '/dev/ttyUSB0'
 option 'apn' 'wnw'
 option 'service' 'umts'
```

PPTP VPN konfiguráció példa

```
config 'interface' 'vpn'
 option 'ifname' 'pptp-vpn'
 option 'proto' 'pptp'
 option 'username' 'ormos' az a felhasználónév amivel authentikálunk
option 'password' 'xxxxxx' a usernamehez tartozó jelszó
option 'server' 'y.y.y.y' vpn szerver neve vagy IP címe
 option 'buffering' '1'
```

Szükséges csomagok:

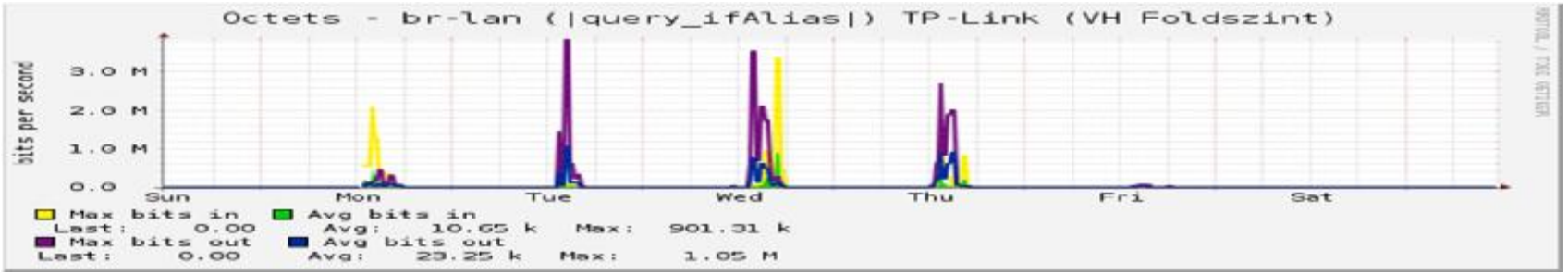
Kmod-mppe

Pptp

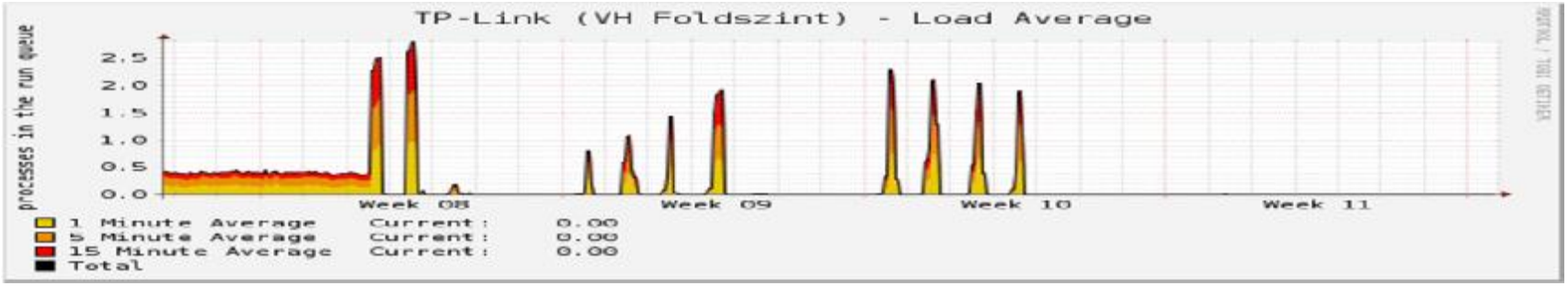
Kmod-gre

OpenWrt Wireless Freedom felügyelet

- SNMP alapon
  - forgalmi mérések (MRTG, Cacti, stb.)



  - cpu, memória, terhelés mérése (MRTG, Cacti, stb.)



OpenWrt Wireless Freedom felügyelet

- Nagiossal
  - ping teszt
    - *titk_asus_wifi UP 03-20-2012 10:14:30 26d 15h 14m 29s PING OK - Packet loss = 0%, RTA = 1.22 ms*
  - riasztás nagy cpu terhelésre
  - riasztás ha valamilyen szolgáltatás nem fut
    - *titk_asus_wifi SSH OK 03-20-2012 10:14:10 26d 18h 37m 47s 1/3 SSH OK - dropbear_0.52 (protocol 2.0)*
  - egyéb riasztások
- Netflow

Date first seen	Duration	Proto	IP Addr	Flows(%)	Packets(%)	Bytes(%)	p ps	bps	bpp
2012-03-20 10:15:16.193	163.054	any	10.100.1.204	157(99.4)	1159(99.8)	180872(99.6)	7	8874	156

- Remote log
  - *12:07 3x dnsmasq-dhcp[1121]: DHCPACK(br-lan) 192.168.10.179 00:90:96:be:c0:ac net-admin*

Gargoyle bemutatása

- Openwrt alapú
- http://www.gargoyle-router.com/index.php
  - Ugyanazokat az eszközöket nagy valószínűséggel támogatja mint az openwrt
  - Mind broadcom, mind atheros chipsetet támogat
- GUI-n és CLI-n keresztül is konfigurálható
- Támogatja az IPv6-t (nem próbáltuk még)
- Rengeteg csomag feltelepíthető rá, akár csak az OpenWrt-re
- Ha van usb portunk az AP-n
  - akkor akár nyomtató, akár samba szerverként is tud működni
  - mobil 3g-t is használhatunk vele
- Wireless repeater funkciót is tud
- DynDNS támogatás

Tanulságok

- Linksys Wrt54G esetén a telepítés után a file rendszer alapban read only. Ezt fel kell oldani
  - *mtd unlock rootfs_data*
- Linksys Wrt54G esetén a portok számozása nem egyezik meg a gyárival.
  - Érdemes utána nézni weben
  - Robocfg programcsomag telepítése esetlegesen
- Atheros chipset esetén nem tudunk több SSID-t kezelni
  - Egyébként pedig csomag kell hozzá
  - Telepítsük az alap wpad-mini helyett a wpad csomagot
- Több helyre történő netflow export nagyon leterheli a cpu-t, vagy egyáltalán nem működik
  - Írjunk init scriptet, hogy újraindulás esetén is legyen netflow export
  - Az init scriptben minden interfacere adjuk ki a flow exportot
    - Ha any-t használunk borzasztóan leterheli a CPU-t, csakúgy mintha több helyre szeretnénk küldeni
- /etc/resolv.conf alapból egy link.
  - Ezt meg kell szüntetni különben boot után elveszítjük a beállításokat

Tanulságok 2.

- PPTP csomag újraindulás után elrontja a konfigot
  - Ezért külön file-be kell tenni a konfigban nem a network alá
  - Elindulása előtt meg kell várni, míg a wan kapcsolat létrejön
  - Echo timeout értékét az 1s –ról át kell állítani a terminálló eszközben beállított értékre, különben állandóan elbont
- Ha egyszer elrontjuk a konfigurációt nehéz visszaállni a gyárira.
  - Hardware reset segíthet, de ekkor elvesztjük a korábbi beállításainkat
  - Legyen mindig mentésünk!
- Más opensource megoldásról nem mindig sikerül OpenWRT-re átállni
  - Előbb álljunk vissza a gyári firmware-re, majd úgy az openwrt-re
  - Mindig legyen kéznél a legfrissebb gyári firmware
- Probléma esetén olvassunk fórumokat a megoldás érdekében

Tanulságok 3.

	Windows XP	Windows 7	Samsung mobil
WPA + TKIP	OK	OK	OK
WPA2 + AES	OK	OK	OK
WPA2 Mixed mód	OK	Csak WPA + TKIP	OK

- Mixed mód Windows7 esetén már nem nyújtja azt a biztonságot amit szeretnénk
  - Eduroam esetén 2013-tól nem lehet wpa így nem okoz nekünk problémát, hogy wpa2-t kell használni

Mitől biztonságos?

- SSID-nként akár külön VLAN-ba is szervezhetőek a hálózatok
  - Vendégek nem láthatnak bele a belső hálózatba
- Tűzfal szabályok beállításával számos korlátozás tehető
  - csak bizonyos IP címekről lehet belépni és csak SSH-n keresztül
  - Külön zónák hozhatóak létre a wan és lan hálózatok számára
  - A kifele és befele nyitott portok külön-külön beállíthatóak
  - Beállítható, hogy a különböző lan hálózatok különböző wan címekre fordítódjanak
- WPA2 támogatás
- Radius + LDAP authentikáció
  - LDAP authentikáció történhet yubikey-el is
- Tud kezelni külön csomag telepítése után GRE Tunnelt, PPTP VPN-t és IPSEC VPN-t is, így akár VPN mögé is rakhatjuk az AP-nkat
  - Több telephelyet, irodát összeköthetünk VPN-en az AP segítségével és egy LAN-ba tudjuk őket szervezni
  - L2TPv3 és L2TPv3 over IPSEC is működőképes
  - OpenVPN támogatás is van

Mitől biztonságos? 2.

- Netflow segítségével (fprobe csomag) az AP-n áthaladó forgalom is analizálható
- Van rá snort IDS/IPS csomag
- MAC cím szerinti hozzáférés korlátozás is beállítható a wireless hálózathoz
- Felügyelhető
  - SNMP alapon
  - Cacti plugin van hozzá
  - NRPE telepíthető
  - Munin csomag van

Összefoglalás

- OpenWrt segítségével olcsóbb árfekvésű AP-kon tudunk biztonságos intézményi wireless szolgáltatást nyújtani
  - Új beszerzésnél ha lehetséges válasszunk OpenWrt kompatibilis AP-t
    - http://wiki.openwrt.org/toh/start
    - Már 10 000 Ft alatti eszközökre is felrakható
  - **Hungarnet közösség számára ideális Wireless szolgáltatás nyújtására**
    - Költséghatékony
    - Az olcsóbb eszközök is rendelkeznek 10/100-as portokkal és 802.11n-s wifivel
    - A felhasználók igénylik a biztonságos wireless szolgáltatásokat
  - Egyszerűen konfigurálható
  - Gargoyle firmware ha kevesebb funkciót akarunk használni
- Nem kell külön controllert használni a működéséhez
- Azonos platformon a konfiguráció hordozható,
  - csak pár paramétert kell átállítani **à** könnyen és gyorsan telepíthető új AP-k

Összefoglalás 2.

- Számos biztonságot növelő programcsomag telepíthető
- VPN támogatás van
- Tud IDS/IPS funkciókat is
- Akár távolról is menedzselhető
  - Megfelelő tűzfal szabályok fontosak
- Több telephelyen levő eszközöket egy LAN-ba tudjuk szervezni
  - L2TPv3 támogatás
- Kisebb telephelyeken VLAN képes switchként is működhet
  - 4 gigabites portot használhatunk
  - Pár gép, vagy IP telefon számára jó megoldás
- Különböző routing szabályok is beállíthatóak
- IPv6 támogatás (nem próbáltuk)

Összefoglalás 3.

- Tűzfal szabályokkal könnyen beállíthatjuk a hozzáférési lehetőségeket
- Wireless roaming támogatás
- Képes kiszolgálni szélessávú WAN kapcsolatot és Wireless hálózatot is és bizonyos modellek esetén 3G-t is.
- Netflow képes
  - Bizonyos verzióban openflowt is támogat http://www.openflow.org

Kérdések?

Köszönöm a figyelmet!

ormos@sztaki.mta.hu