Sulinet Eduroam AP

Sulinet Eduroam AP

Az eduroam hálózat lehetőséget biztosít arra, hogy a Sulinet Dashboard felületen felvett felhasználók bármilyen, eduroam SSID-t használó intézményben internet-hozzáféréshez jussanak.

Ezzel kapcsolatban felmerültek igények, hogy bármilyen típusú, az intézmény által üzemeltetett eszközzel is megvalósítható legyen ezen hozzáférés. Ezen szolgáltatás igénybevételéhez egy olyan iskolai eduroam/eduID felhasználási szerződést kell kötni az intézménnyel, amelyben az intézmény vállalja, hogy az eduroam szabályai szerint működteti az AP-ket és erre vonatkozó szerződést köt a KIFÜ-vel.

Technikailag legtöbb vezeték nélküli eszközön megvalósítható az eduroam hálózat beállítása;

Eszköz beállításához szükséges paraméterek

Bármilyen vezeték nélkül eszköz, mely képes kezelni a WPA2 Enterprise protokollt, azon be lehet állítani az eduroam hálózatot az alábbiak szerint (egyelőre csak úgy működik, ha a vezeték nélküli eszköz a sulinetes router privát vagy védett szemensére van kötve):

Radius szerver IP: 195.111.98.15, 195.111.115.15

Radius szerver hitelesítéshez használt port (authentication port): 1812

Radius szerver naplózáshoz használt port (accouting port): 1813

Jelszó (shared secret): minden végpontnak egyedi shared secretje van, amit a Dashboardon olvashat

A WPA2 Enterprise protokoll általában az eszköz WIFI-vel foglalkozó menüjének a Wireless Security menüjében található meg.

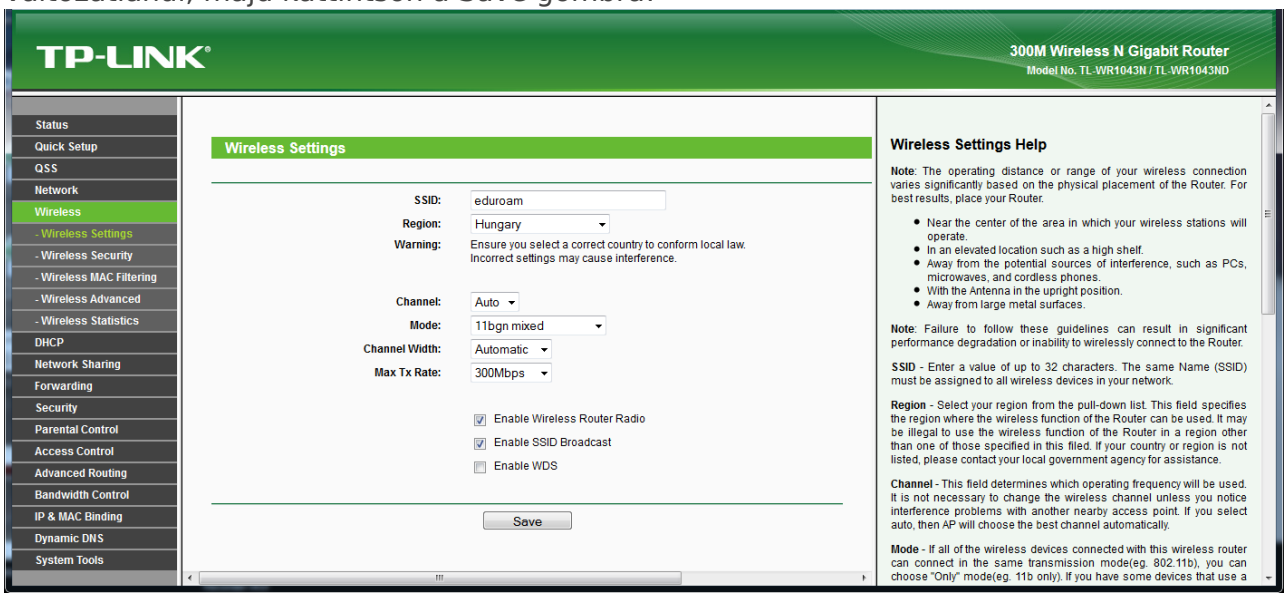
A fentieken kívül ügyelni kell a következőkre:

- a WPA verzió 2-es legyen
- a titkosítás automatikus vagy AES legyen

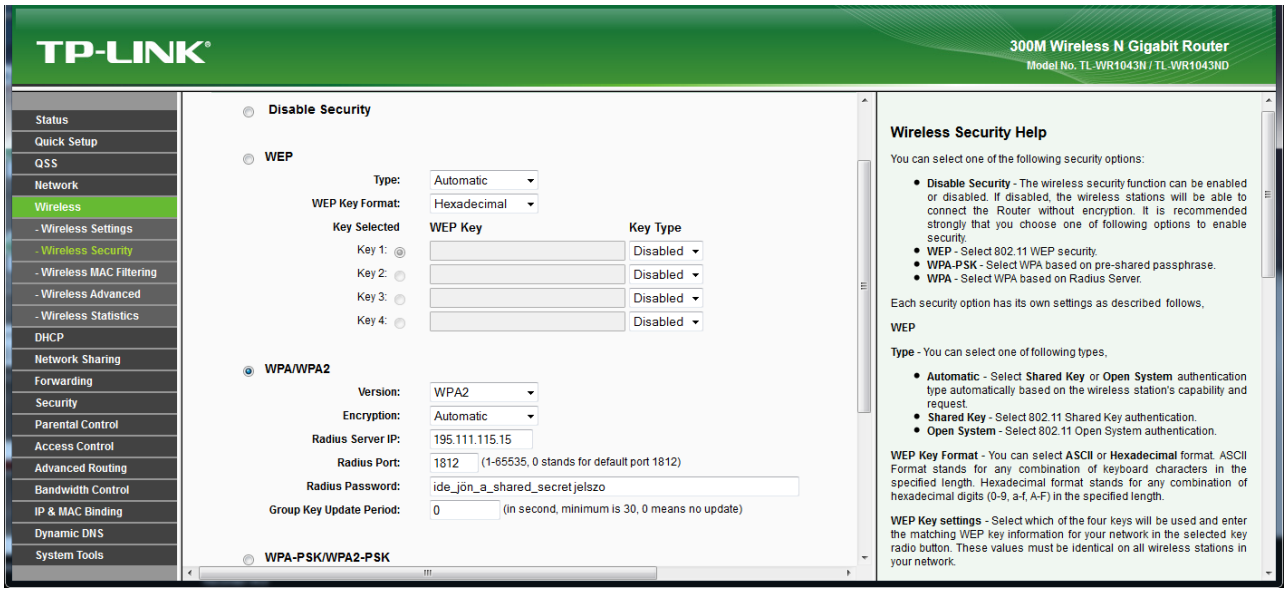
Ha minden beállítás megtörtént és fogható az eduroam SSID a vezeték nélküli eszköz révén, akkor a Windows operációs rendszert használók tekintsék meg ezt a leírást a gyors csatlakozás érdekében.

SOHO eszköz beállításához szükséges paraméterek

A konfigurációs segédlet egy TP-LINK TL-WR1043ND V1 eszközön kerül bemutatásra a gyári szoftverrel.

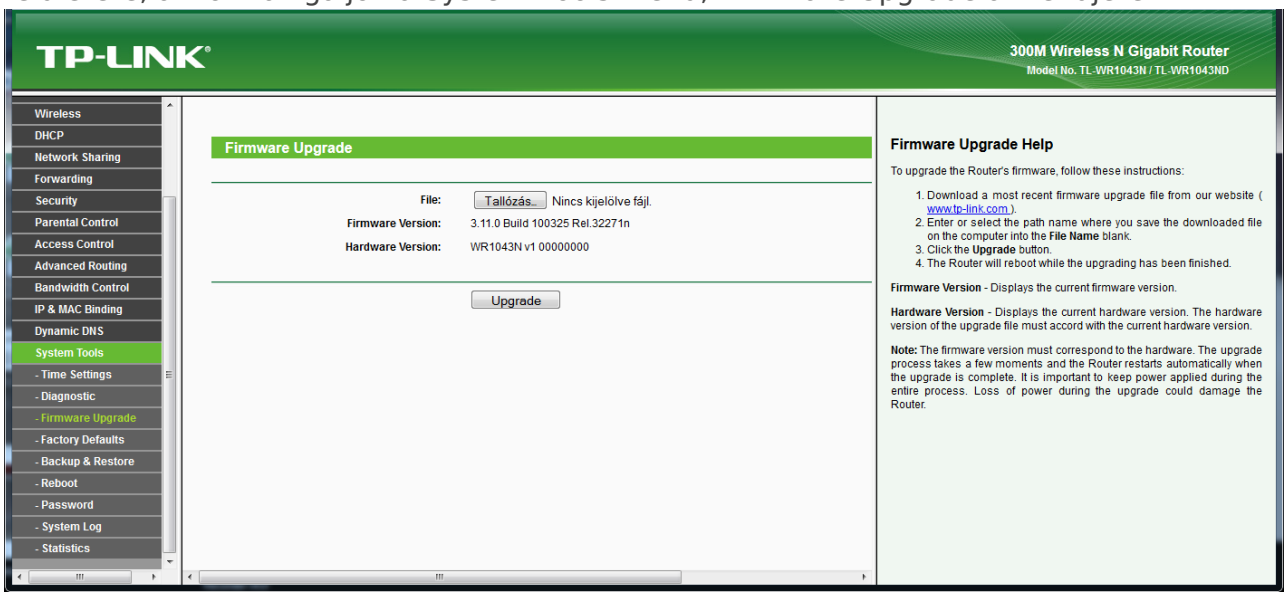
- Győződjön meg róla, hogy az eszköz csatlakozik a villamos hálózathoz! Csatlakoztasson egy ethernet kábelt a router 1-4 portjai közül bármelyikre! Nyisson meg egy böngészőt és írja be a címsorba a router IP címét, mint rá kötött eszköz alapértelmezett átjáróját: 192.168.1.1
- A router kérni fogja a belépéshez szükséges felhasználói nevet és jelszót. Ezen információ a router alján lévő matrícán található meg Username és Password formájában.
- Navigáljon a router webes felületén a Wireless menüpontra! Írja át a gyári SSID-t eduroam-ra, válassza ki régiónak Magyarországot; a többi beállítás maradhat változatlanul, majd kattintson a Save gombra!
- 

- Navigáljon a Wireless Security almenüpontra és kattintson a WPA/WPA2 menüpontra! Válassza ki a Version-nál a WPA2-t, adja meg a Radius Server IP résznél a 195.111.115.15 címet, adja meg a Sulinet Dashboardon kijelzett karaktersorozatot a Radius Password mezőbe, majd kattintson a Save gombra. A router esetlegesen felhívhatja a figyelmét arra, hogy a beállítások csak a router újraindítása után lépnek érvénybe, ekkor indítsa újra az eszközt!

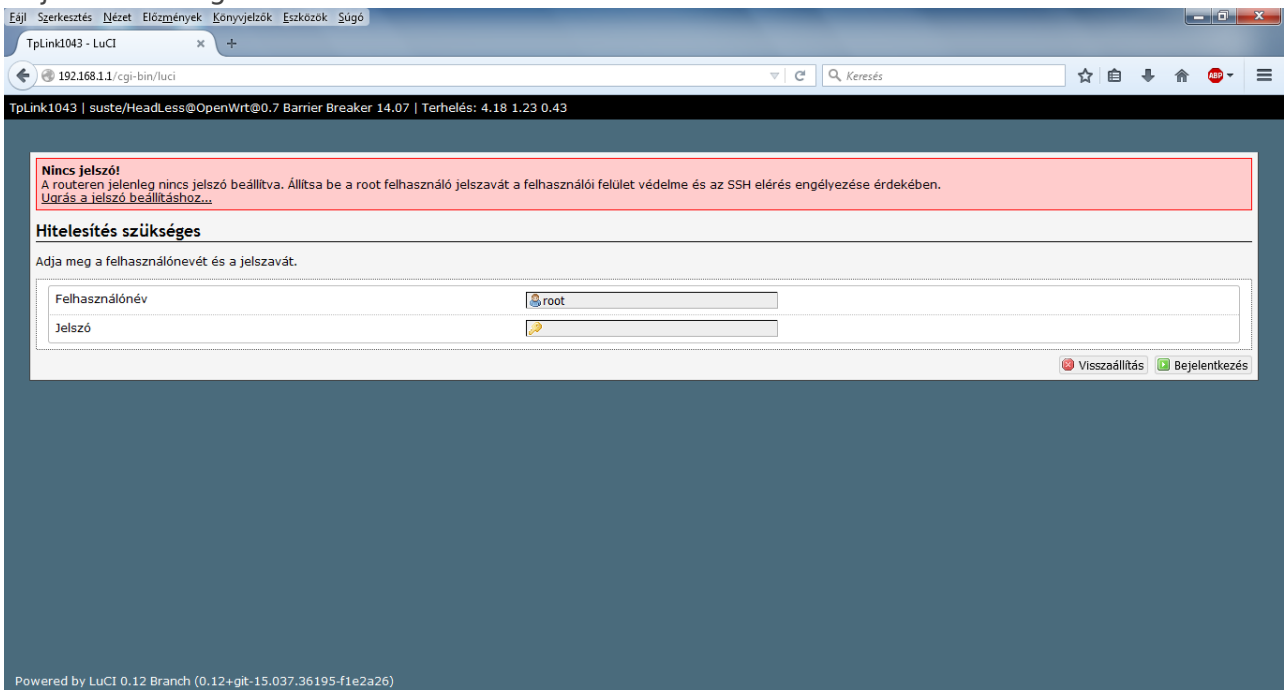


OpenWRT telepítése a példakánt TP-LINK TL-WR1043ND v1 routerre

- Töltse le az OpenWRT lefrissebb verzióját a https://firmware-selector.openwrt.org/ oldalról - Első alkalommal **Factory image** majd később **sysupgrade**.
- **Fontos! Az eredeti fájlról készült SHA256 lenyomatot mindig hasonlítsa össze a letöltött fájl SHA256 lenyomatával és csak akkor használja a fájlt, ha az SHA256 lenyomatok egyeznek, ellenkező esetben a router működésképtelennél válhat!**
- Kövesse az előző bekezdés első pontja szerinti utasításokat! Ha eljutott a router webes felületére, akkor navigáljon a System Tools menü, Firmware Upgrade almenüjére!

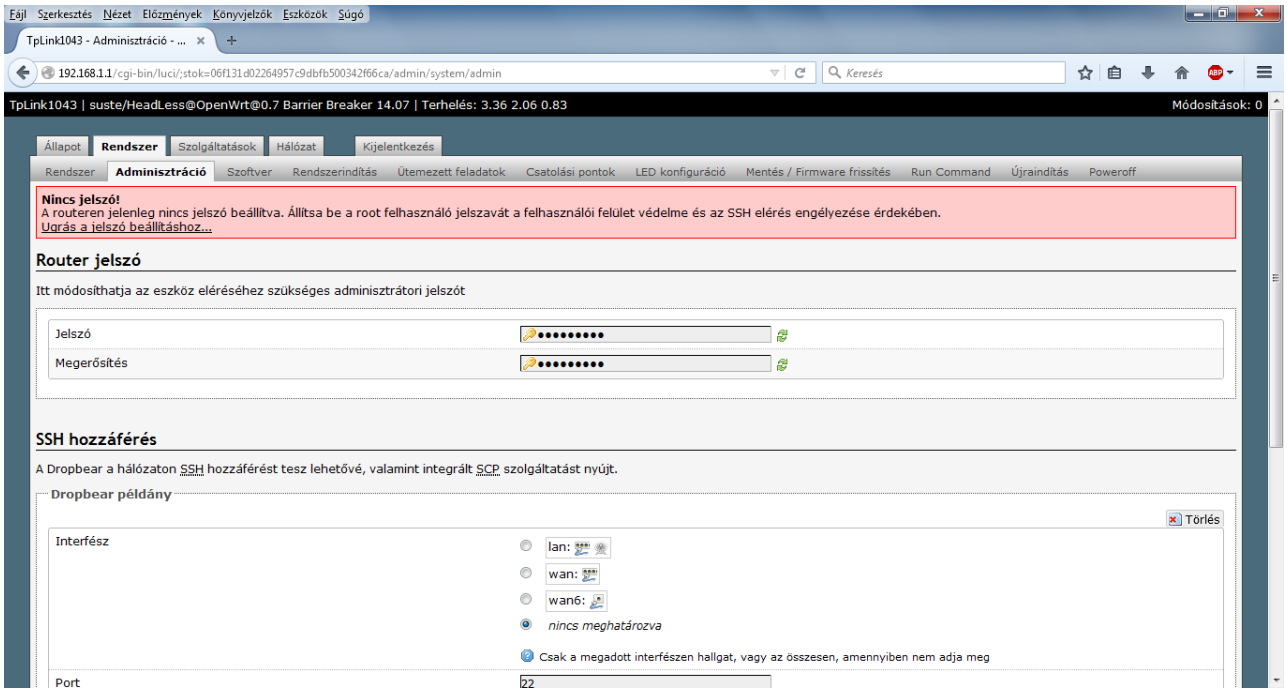


- A fájl letöltése után kattintson a Tallózás gombra és keresse meg a letöltött fájlt majd kattintson az Upgrade gombra! A router megerősítést kér a frissítés végrehajtásához, ezt hagyja jóvá egy OK gombra történő kattintással!

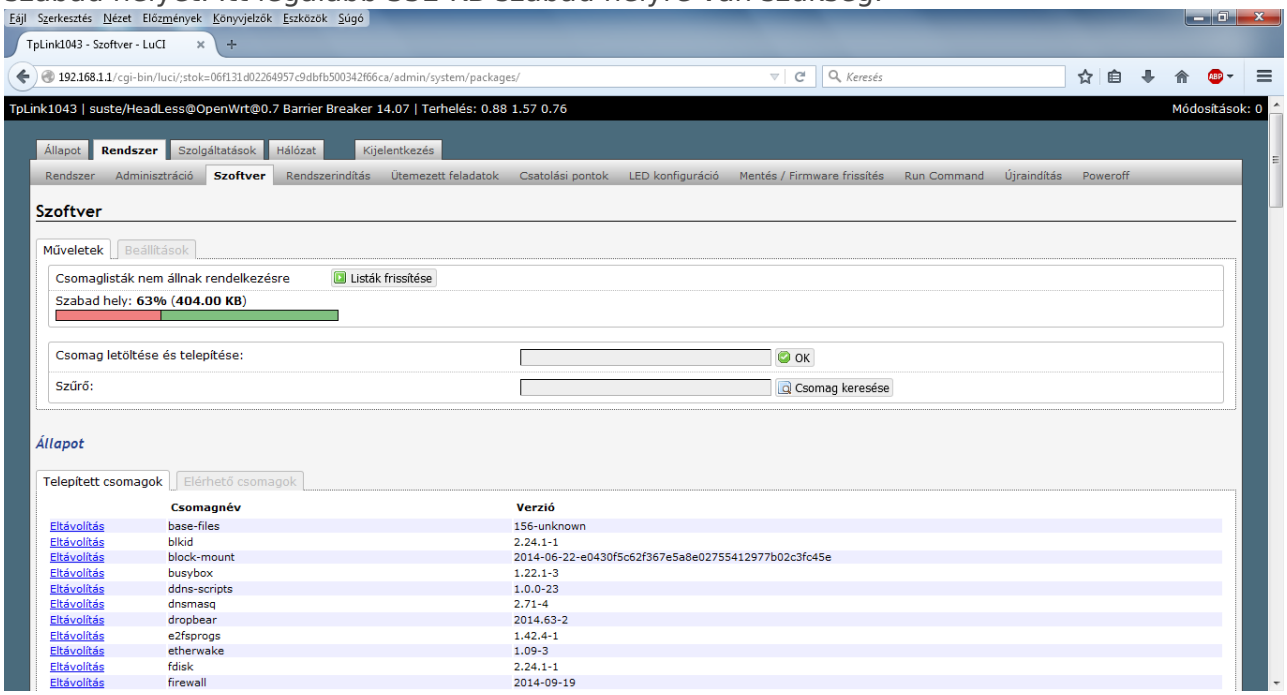
- **Fontos! Szoftverfrissítés idejére mindig biztosítson szünetmentes tápellátást az eszköznek, mert a frissítés közbeni esetleges áramszünettől a router működésképtelenné válhat!**
- A router automatikusan újra fog indulni. Az új szoftver betöltését a SYS led folyamatos világítása jelzi.
- Nyisson egy böngészőt és írja be a router IP címét a címsorba: 192.168.1.1
- Használja a root felhasználót és a jelszó mezőt hagyja üresen, majd kattintson a Bejelentkezés gombra.
- 

- Az OpenWRT arra kéri, hogy változtassa meg a jelszavát. Ehhez kattintson a piros kiemelésben található "Ugrás a jelszó beállításához..." linkre.
- 

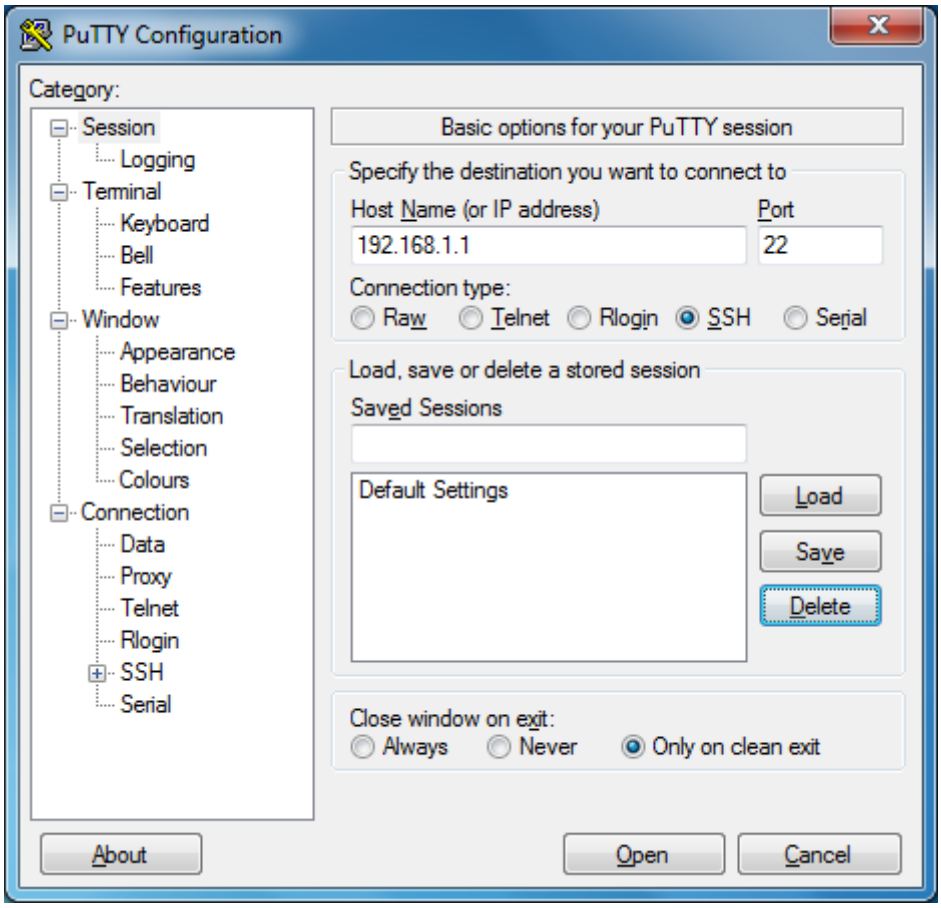
- Adja meg a jelszót, majd kattintson a Mentés és Alkalmazás gombra! Ezt követően már sikerülni fog az SSH-n keresztül történő belépés a routerre.



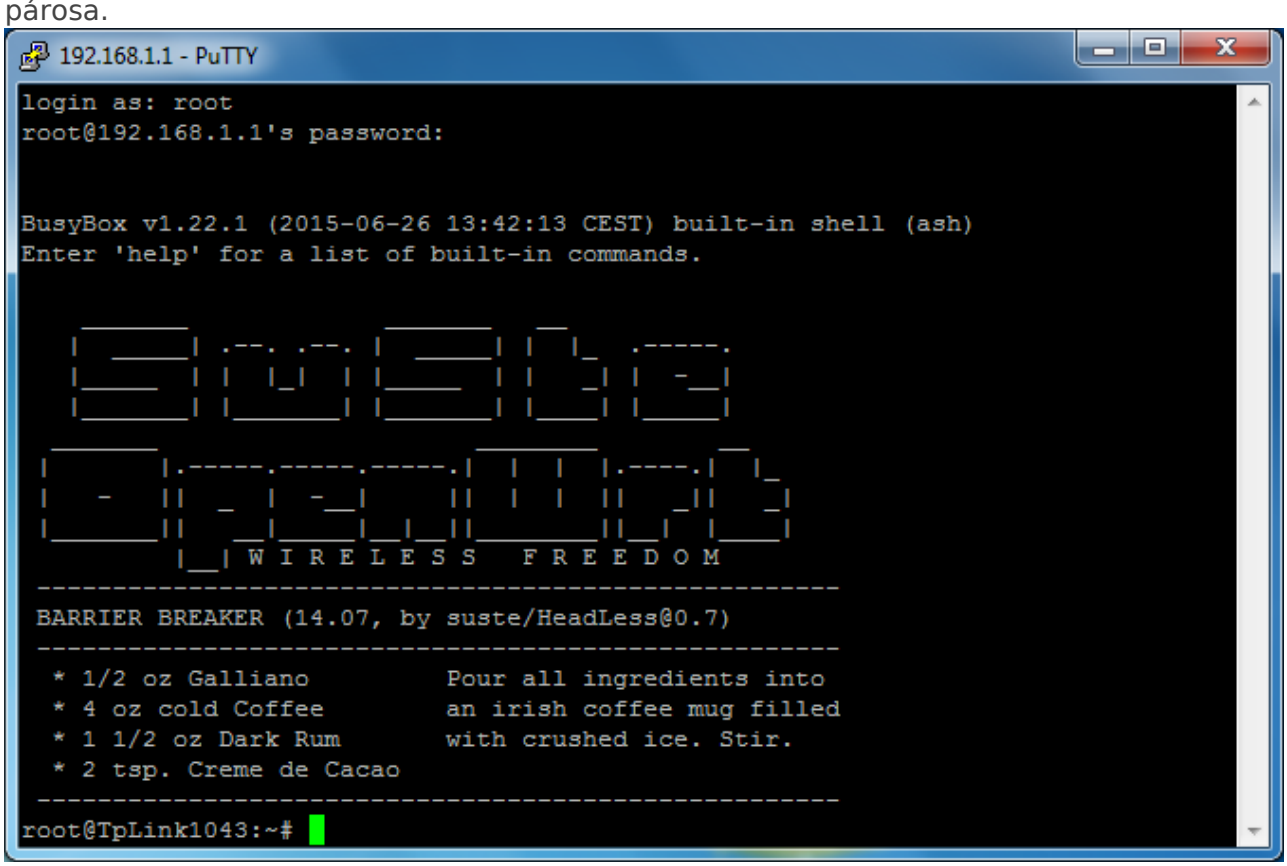
- A Rendszer menü, Szoftver almenüben megtekintheti a router flash memóriáján lévő szabad helyet. Itt legalább 352 KB szabad helyre van szükség.



- Lépjen be a routerre SSH-n keresztül! Ehhez használhatja a Putty terminál-emulációs szoftvert, mely letölthető innen: http://the.earth.li/~sgtatham/putty/latest/x86/putty.exe
- Nyissa meg a letöltött terminál-emulációs szoftvert és töltse ki a lenti kép szerint, majd nyomja meg az Open gombot!

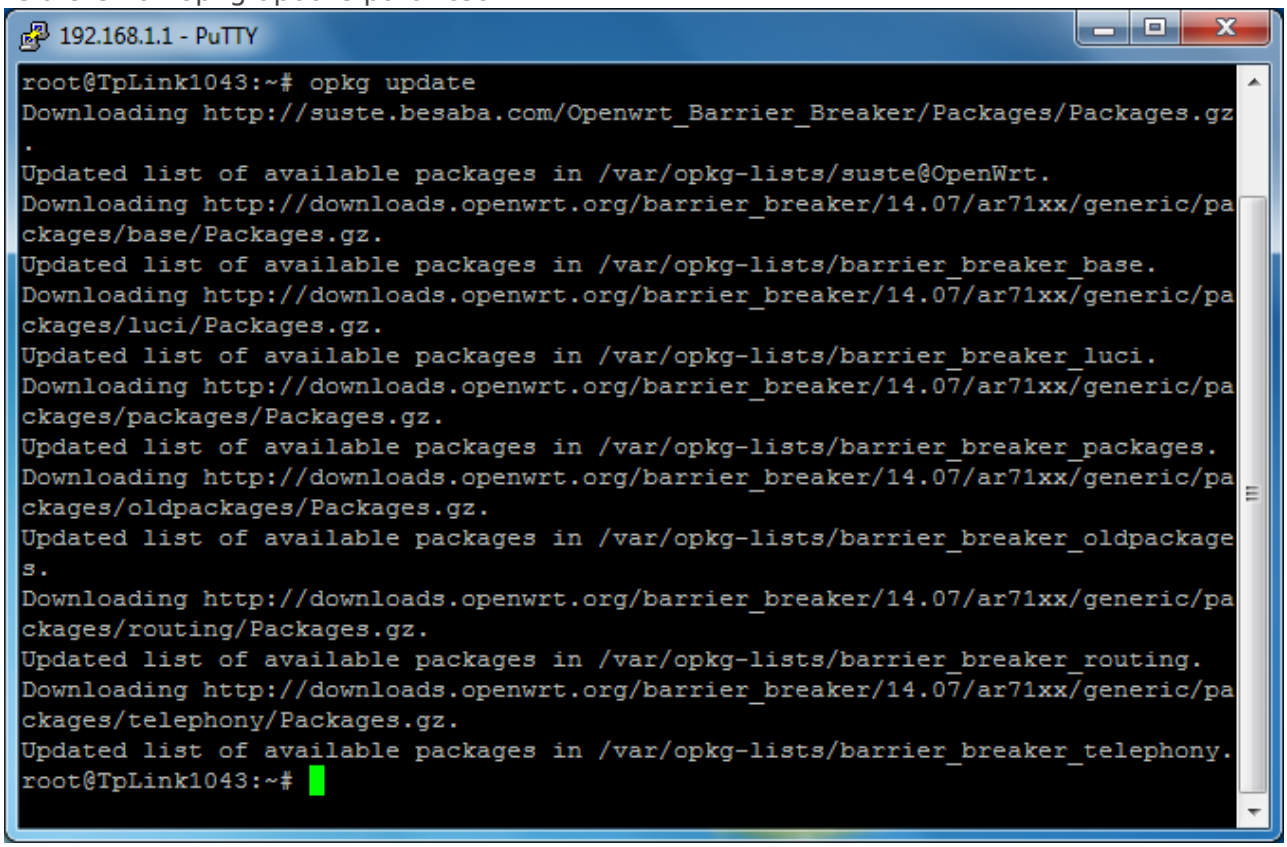


- A felület megjeleníti a router SSH kulcsának publikus részét. Ezt fogadja el a belépéshez! A router felhasználói nevet és jelszót fog kérni: ez root és a korábban beállított jelszó párosa.

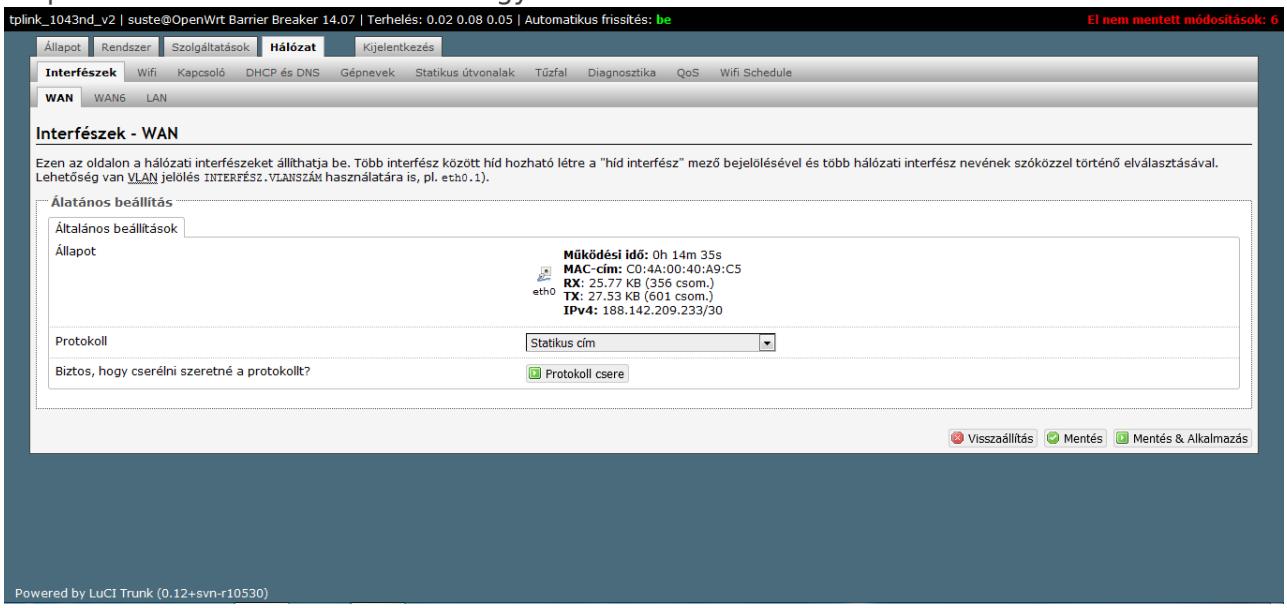


- Csatlakoztassa a router WAN feliratú, kék színű portját a sulinetes 892FSP router privát, védett vagy publikus szegmensbeli portjára!

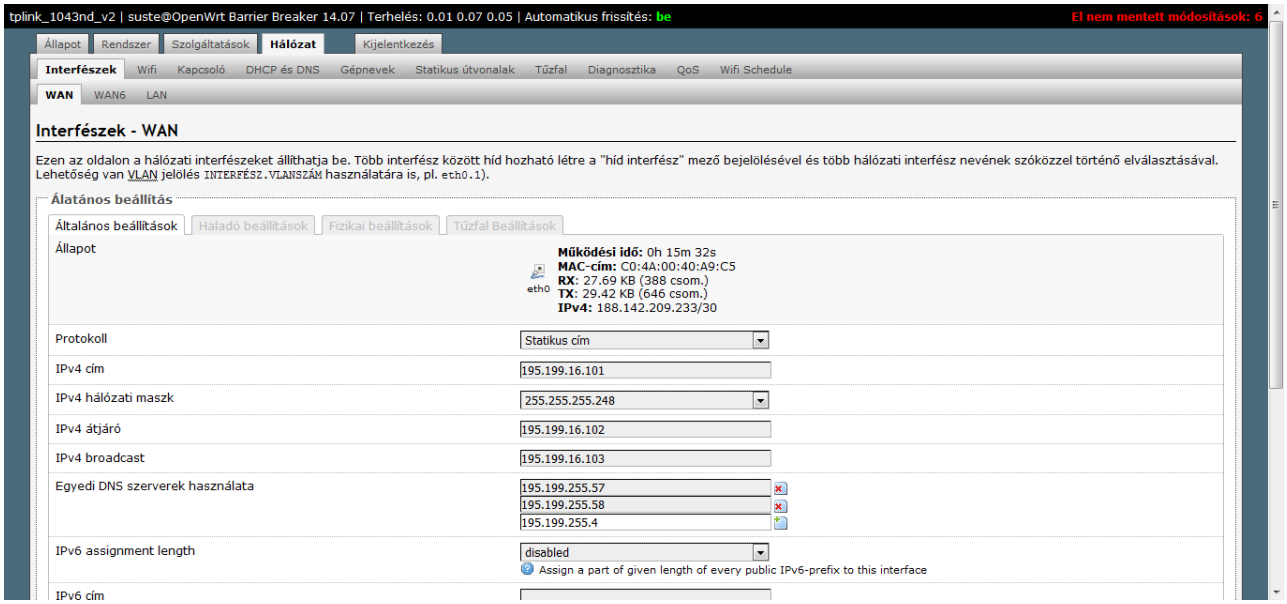
- Miután a router DHCP-n keresztül kapott IP címet a Cisco eszköztől, adja ki a router SSH felületén az opkg update parancsot!



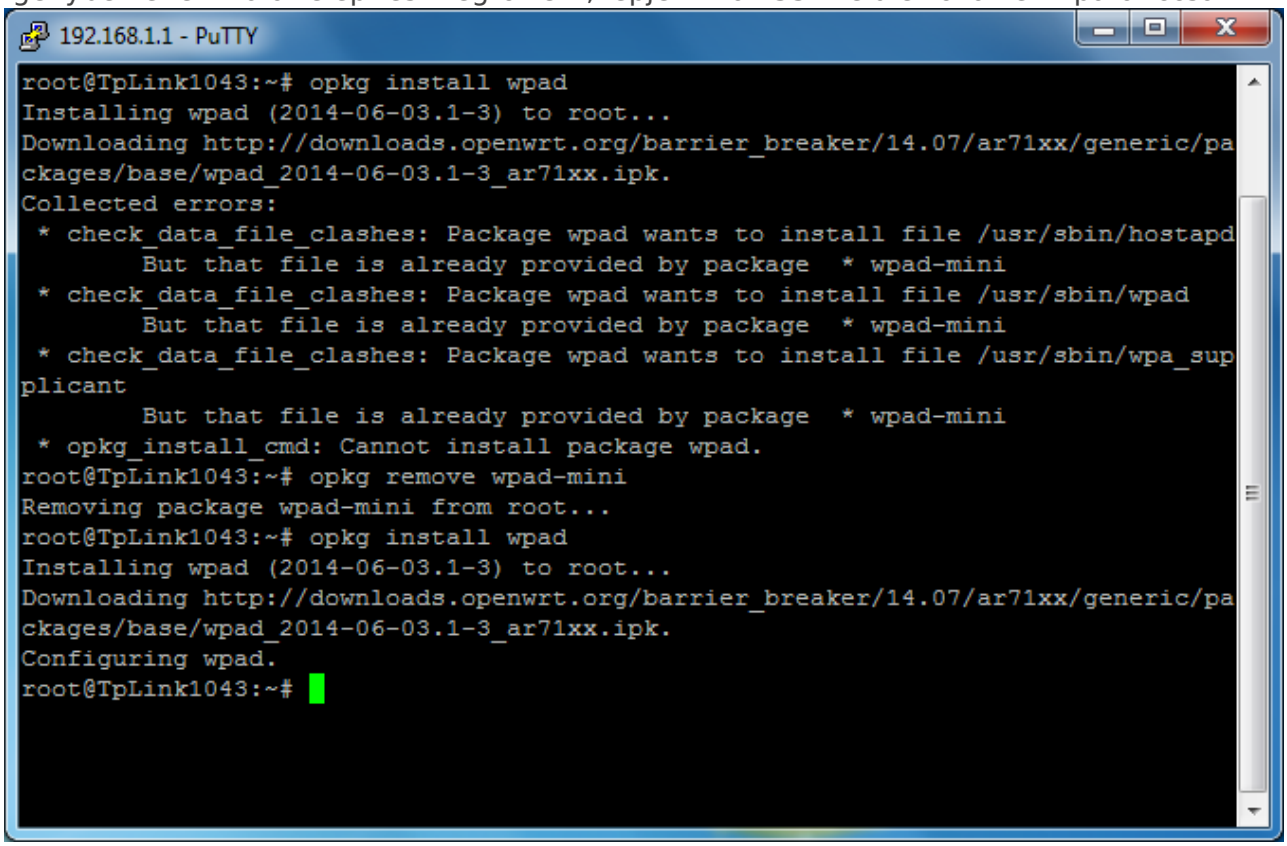
- Amennyiben a Cisco router publikus szegmensére kötötte az eszközét, akkor statikus IP beállításokra van szükség. Keresse fel a Hálózatok menü, Interfészek, WAN füleket! Az alapértlemezett beállítás a DHCP ügyfél.



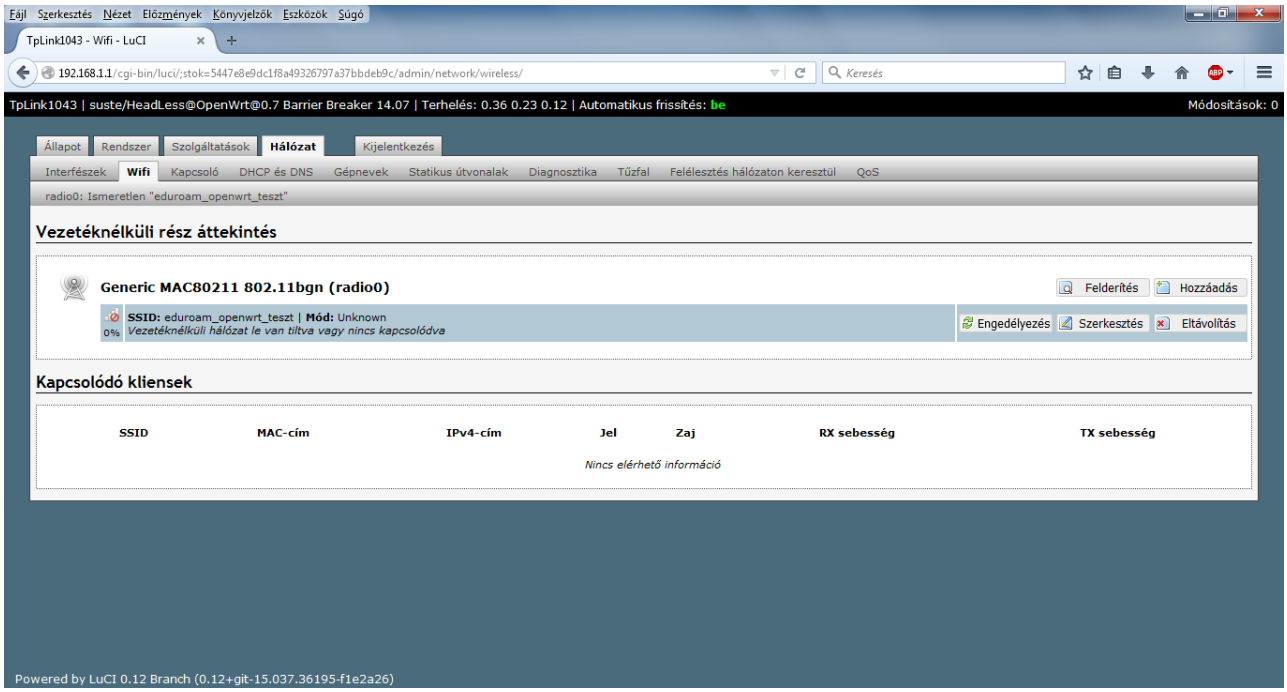
- Kattintson a legördülő menübe és válassza ki a Statikus cím lehetőséget, majd kattintson a Protokoll csere gombra! Ha a protokoll csere megtörtént, akkor beállíthatóak kézzel az IP címek.



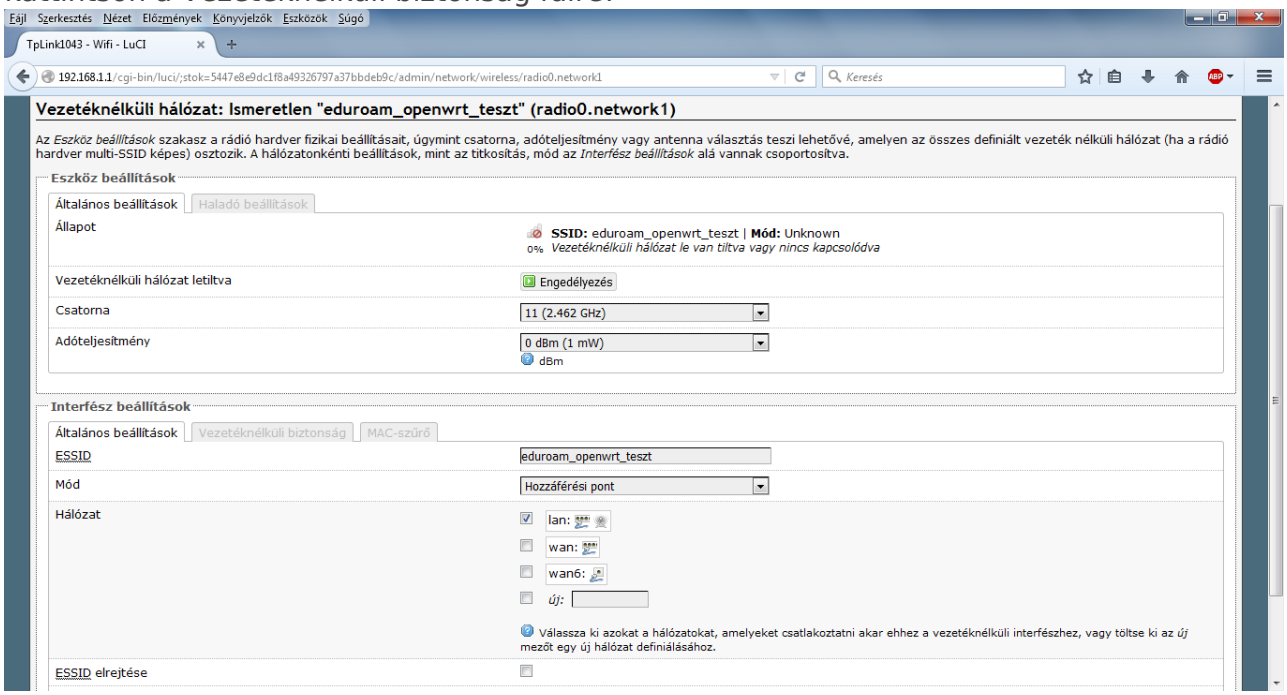
- Ennek megtörténte után távolítsa el a wpad-mini csomagot az opkg remove wpad-mini paranccsal és telepítse a wpad csomagot az opkg install wpad paranccsal! Ez kis időt igénybe vehet. Ha a telepítés megtörtént, lépjen ki az SSH felületről az exit paranccsal!



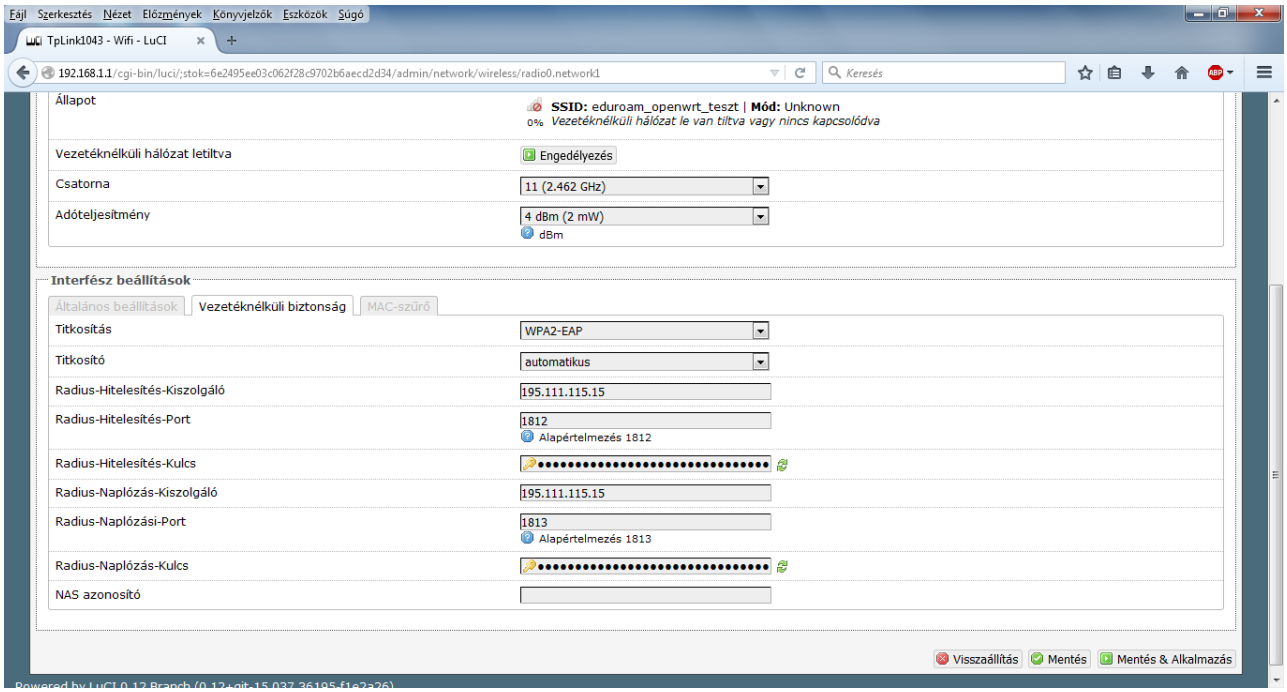
- Navigáljon ismét a router webes felületén: keresse fel a Hálózat menü, Wifi almenüjét, majd kattintson a Szerkesztés gombra!



- Lent, az Interfész beállítások résznél írja be az eduroam szót, mint ESSID-t, majd kattintson a Vezetéknélküli biztonság fülre!



- Állítsa be a kép szerint a felületet majd kattintson a Mentés és Alkalmazás gombra! Ha mindennel elkészült és a Vezetéknélküli hálózat letiltva résznél Engedélyezés gombot lát, akkor nyomja meg!
- Az eduroam hálózat innentől kezdve használható a routeren.



- Az eduroam használatához történő csatlakozáshoz szükséges információkat az alábbi linken tudja elolvasni: https://kifu.gov.hu/iskolai-eduroam-hasznalata/

Konfiguráció Cisco AP-k esetén

Az alábbi konfiguráció egy Cisco AIR-SAP1602I-E-K9 típusú AP lényegi konfigurációja, mely segítséget nyújthat az intézmény által üzemeltetett eszköz beállításához.

```
!! Cisco típusú eszköz esetén a különféle hitelesítési-, authoricáiós- és logolási művelethez engedélyezni kell az AAA-t (Authentication, Authorization, Accounting)</br>
aaa new-model</br>
!! RADIUS szerver csoportot kell létrehozni radius_eduroam néven (bármilyen név csoportnév megfelelő, viszont később tudni kell rá hivatkozni), melybe a lenti két szerver tartozik; konkrét szerver IP definiálása lejjebb  található</br>
aaa group server radius radius_eduroam
 server name radius2.eduroam
 server name radius1.eduroam</br>
!! létre kell hozni egy AAA method-listet, ami a fenti Eduroam szerverekre hivatkozik</br>
aaa authentication login eap_eduroam group radius_eduroam</br>
!! a lenti beállítással rögzítésre kerülnek a hitelesítés hibák (téves jelszó, téves felhasználói név használata)</br>
aaa accounting send stop-record authentication failure
aaa accounting update newinfo</br>
!! létre kell hozni egy accounting_eduroam nevű method-listet (szintén bármilyen más fantázianév megfelelő, viszont később tudni kell rá hivatkozni), ami a hálózati tevékenység
```

logolását engedélyezi; ez szintén a radius-szerverekre hivatkozik</br>

aaa accounting network accounting_eduroam start-stop group radius_eduroam</br>

! beállítjuk, hogy az AP több SSID-t is kezeljen és logoljon (amennyiben az intézménynek van saját SSID-ja az eduroam-on kívül)</br>

dot11 mbssid

dot11 syslog</br>

! létre kell hozni az eduroam nevű SSID-t és úgy beállítani, hogy a RADIUS szervereket használja a hitelesítéshez</br>

dot11 ssid eduroam

  vlan 101

  authentication open eap eap_eduroam

  authentication network-eap eap_eduroam

  authentication key-management wpa version 2

  accounting accounting_eduroam

  mbssid guest-mode</br>

! attól függően, hogy az AP tudja-e a 802.11a-t, attól függően Dot11Radio0 és/vagy Dot11Radio1 interfészeken is be kell állítani az eduroam vlan titkosítását és az SSID interfészhez történő hozzárendelését</br>

interface Dot11Radio0 és/vagy Dot11Radio1

 encryption vlan 101 mode ciphers aes-ccm

 ssid eduroam</br>

! hozzá kell rendelni a BVI1 interfészt egy tetszőleges VLAN-hoz, aminek egyeznie kell a fenti dot11 ssid eduroam parancsban megadottakkal</br>

interface Dot11Radio0.101

 encapsulation dot1Q 101

 no ip route-cache

 bridge-group 1

 bridge-group 1 subscriber-loop-control

 bridge-group 1 spanning-disabled

 bridge-group 1 block-unknown-source

 no bridge-group 1 source-learning

 no bridge-group 1 unicast-flooding</br>

! az AP uplink interfészét is hozzá kell rendelni a BVI1 interfészhez</br>

interface GigabitEthernet0

 bridge-group 1

 bridge-group 1 spanning-disabled

 no bridge-group 1 source-learning</br>

! IP adatokkal el kell látni a BVI1 interfészt; a lenti példában DHCP-n keresztül kapja meg a menedzseléshez szükséges IP címet, ami az ap1 kliens-azonosító miatt mindig ugyanaz lesz< br/>

interface BVI1

 ip dhcp client client-id ascii ap1

 ip address dhcp
 no ip route-cache</br>
! meg kell adni egy interfészt, amit forrás-címként fog használni az eszköz a radius-szerverrel történő kommunikáláshoz, pl. Loopback0</br>
ip radius source-interface Loopback0</br>
! meg kell adni a legelső sorokban meghatározott radius-szerverek IP-jét, a kommunikációs portokat és a radius-szerver által használt jelszót titkosított formában</br>
radius-server attribute 32 include-in-access-req format %h
radius server radius1.eduroam
 address ipv4 195.111.98.15 auth-port 1812 acct-port 1813
 key 0 *egyedi_shared_secret_helye*
radius server radius2.eduroam
 address ipv4 195.111.115.15 auth-port 1812 acct-port 1813
 key 0 *egyedi_shared_secret_helye*</br>
! engedélyezzük az STP-t és az IP routolását a BVI1-hez rendelt interfészeken</br>
bridge 1 protocol ieee
bridge 1 route ip
bridge irb

Változat #1
document-uploader hozta létre 2025-08-07 12:08:30 CEST
document-uploader frissítette 2025-08-07 12:08:30 CEST