# WiFi-szolgáltatás az SZTE Egyetemi Számítóközpontban I-II.

Borús András, Csóti Zoltán, Szabó Zsolt
{borus, csotiz, szabozst}@cc.u-szeged.hu
Szegedi Tudományegyetem Egyetemi Számítóközpont
Jónás Balázs
bjonas@scinetwork.hu
SCI-Network zRt.

# Tartalomjegyzék

# 1. Bevezetés

A Dél-alföldi Tudáspólus felsőoktatási infrastruktúrájának fejlesztése című, TIOP-1.3.1.-07/2/2F-2009-0004 azonosító számú uniós projekt keretében a dél-alföldi régióban folyó matematikai, műszaki, természettudományos és informatikai képzés számára kiemelkedő infrastrukturális hátteret biztosító, versenyképességet növelő fejlesztések valósultak meg 2009. január 16. és 2012. november 30. között a Szegedi Tudományegyetem és partnerintézményei együttműködésében.

A pályázat „B" komponenseként az oktatási-kutatási infrastruktúrát támogató, a 21. század elvárásainak megfelelő infokommunikációs technológiai fejlesztések történtek. Az alprogram célja az egyetem mindennapi működéséhez, az „üzletmenet folytonosságához" nélkülözhetetlen informatikai hálózat további fejlesztése és korszerűsítése volt. A projekt kiemelt fontosságú részelemei a következők voltak: az informatikai központ fejlesztése, az egyetemi gerinchálózat fejlesztése, az egyetemi épületek aktív eszközeinek és kábelezési rendszereinek korszerűsítése, az egyetemi vezeték nélküli hálózat fejlesztése, hálózatmenedzsment, szerverkonszolidáció, portál- és üzletiintelligencia-rendszerek fejlesztése.

A WiFi részprojekt célja korszerű vezeték nélküli hálózati szolgáltatás bevezetése, amely kiegészíti az egyetemi Ethernet vezetékes hálózat által biztosított lehetőségeket.

A rendszert úgy terveztük, hogy további egyetemi egységek, épületek is csatlakozhassanak, amit úgy értünk el, hogy a központi berendezések kapacitását nagyobbra méreteztük annál, mint amit a pályázati beszerzés közvetlenül szükségessé tett.

Az előadásban ismertetjük a WiFi részprojektet: a tervezés, beszerzés, beüzemelés lépéseit, valamint az elmúlt háromnegyed év üzemeltetési tapasztalatait.

# 2. Előzmények

## 2.1. Célkitűzések, tervek

A projekt célkitűzése egy mondatban összefoglalva: EHA kódos WiFi-t minden egyetemi hallgatónak és dolgozónak!

(A Pécsi Tudományegyetemen bevezetett hasonló rendszer mintájára. Műszakilag precízebben: A WiFi felhasználói azonosító az EHA kóddal – azaz az ETR tanulmányi rendszer személyazonosítójával – rendszerint megegyező ETR-loginnév, kiegészítve a @wifi.u-szeged.hu utótaggal, a jelszó megegyezik az ETR-ben használttal.)

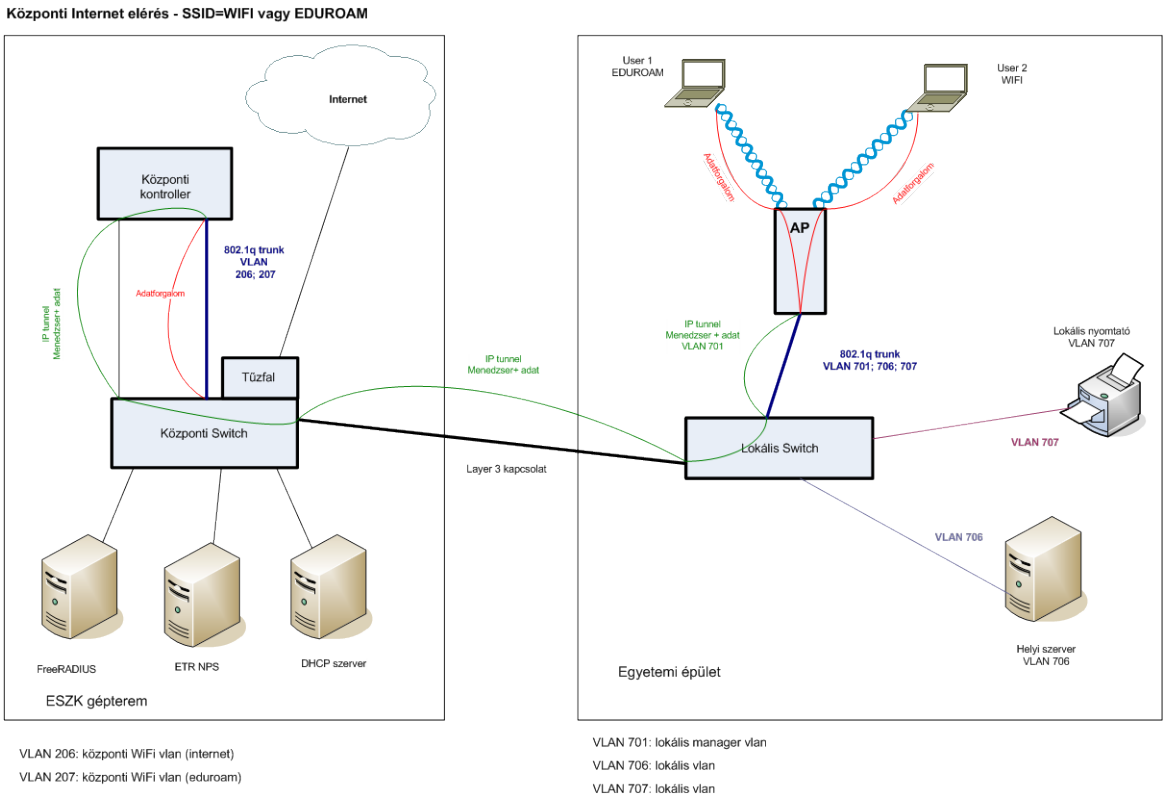
Főbb műszaki jellemzők és alapelemek:

- WPA/WPA2 Enterprise + TKIP/AES
  Az aktuális standardoknak megfelelő titkosított, biztonságos szolgáltatást kívántunk kialakítani.
- PEAP, MS-CHAPv2
  Az azonosító/jelszó típusú azonosításból, a kódolt jelszótárolásból, valamint a windowsos kliensek miatt adódott ez a két jellemző.

- Autentikáció – NPS (ETR AD).
  Mivel a Microsoft-alapú ETR-ben használt loginok (EHA kódok) AD-ben tárolódnak, ezért természetesnek tűnt autentikációs célokra az MS NPS-t használni.
- Autorizáció – FreeRADIUS
  RADIUS-os tapasztalataink Unix-os irányból indulva FreeRADIUS-szal voltak, ezért a bonyolultabb autorizációs feladatokat ezzel terveztük megoldani.
- Központilag vezérelt AP-k és local switching
  A WiFi access pointok (AP-k) központilag vezéreltek, de az ún. központi szolgáltatások mellett a lokális erőforrásokat úgy terveztük elérni, hogy a forgalom ne menjen át a hálózat központjában elhelyezett WiFi-kontrolleren.

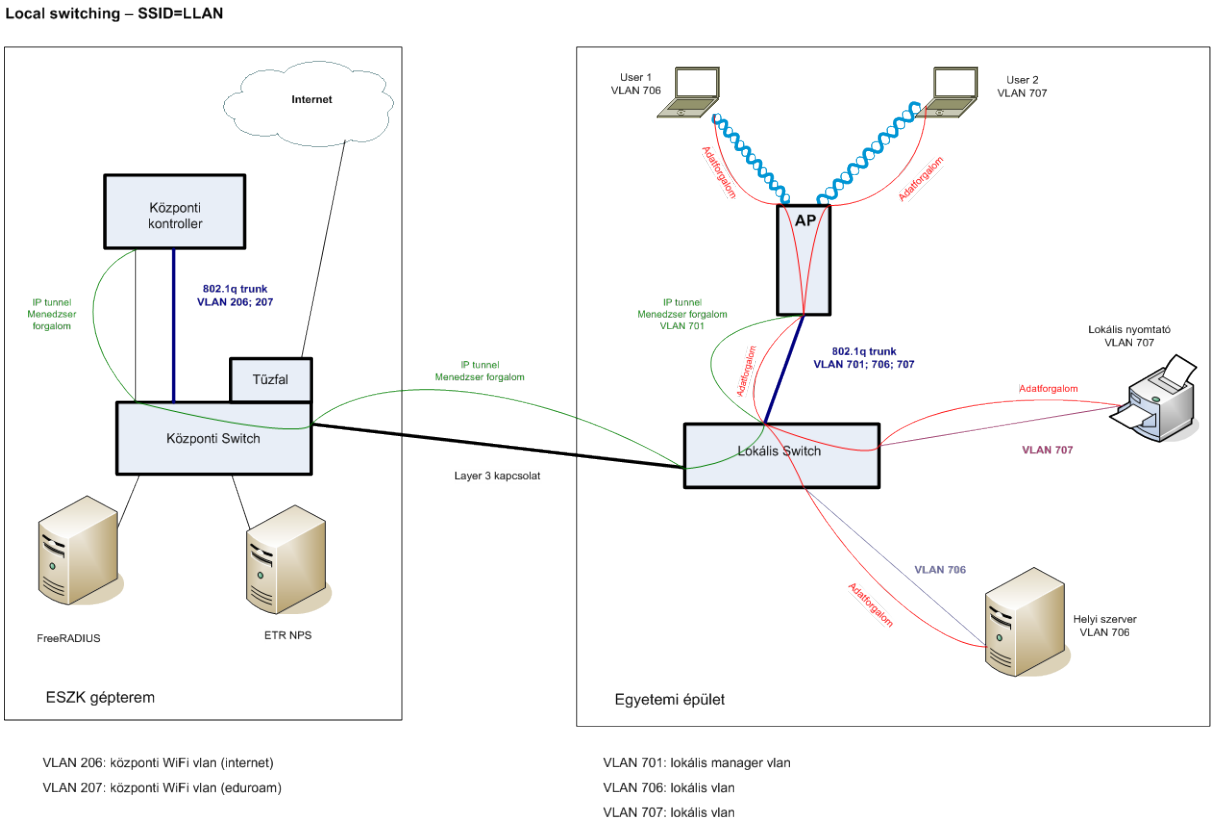
Az utolsó pontot bővebben kifejtendő, először is azzal a követelménnyel kell kezdeni, hogy a WiFi-rendszert az SZTENET meglevő – fizikai és logikai – hálózati struktúrájának módosítása nélkül kellett telepíteni. Ez például úgy valósítható meg, hogy az épületekben elhelyezett AP-k az egyetemi gerinchálózaton keresztül IP tunnellel csatlakoznak a központi kontrollerhez.

A rendszer alapszolgáltatása a központi szolgáltatás, amikor minden forgalom átmegy a kontrolleren, lásd az 1. ábrát.




**1. ábra** Központi szolgáltatás

A local switching esetén az adatforgalom az AP-n keresztül közvetlenül a helyi erőforrásokat tartalmazó lokális hálózatba jut. Ugyanis egy speciális SSID megadásakor a sessionhöz dinamikus VLAN hozzárendelés történik felhasználónév és AP-csoport alapján, feltételezve, hogy minden felhasználónak van egy „saját” épülete és VLAN-ja. Lásd a 2. ábrát.




**2. ábra** Local switching

## A tervek szerint lefedendő épületek és területek

Oktatási épületek:

- Mérnöki Kar (MK) „A” és „C” épületei,
- TTIK Béke épülete,
- TTIK Irinyi épülete.

A TIOP 1.3.1 „A” komponenséből finanszírozott épületek:

- Rektori Hivatal (RH),
- TTIK Dóm téri épületei,
- MK új épülete.

Szabad terek egyes egyetemi épületek környékén:

- Dugonics tér (a RH előtt),
- Irinyi épület udvara,
- MK „A” épület udvara.

- Egyéb stratégiailag fontos területek: munkaszobák, előadók, PC-laborok, közösségi terek (dékáni hivatal előtére, büfé stb.).

A szolgáltatás megcélzott minősége az adathálózati (data-only deployment) lefedettség. Tehát az AP-ket (lehetőség szerint) egymáshoz képest „átfedéssel” terveztük telepíteni, de a minél nagyobb területi lefedettség biztosítása volt az elsődleges szempont, szemben a redundanciával, a roaming támogatásával vagy a QoS-sel. Hasonló okokból mellőztük a különféle védelmi megoldások alkalmazását is, mert a rendelkezésre álló forrásokat „produktív” AP-kre kívántuk fordítani. Ezzel „kivívtuk” a WiFi-hálózattervezésben jártas potenciális szállítók rosszallását.

### 2.2. A 2009–2011-es évek eseményei

Miután a központi WiFi-rendszer beszerzését a projektvezetés elhalasztotta, a 2009-2011-es évek teszteléssel és tapasztalatszerzéssel teltek.

Kérdésessé vált a beszerzés módja is: A korábban alkalmazott KSZF-es (jelenleg KEF-es) eljárás helyett felvetődött a nyílt közbeszerzési eljárás szükségessége is.

A pályázat épületfelújítással foglalkozó „A” komponense „lehagyta” a központi informatikai infrastruktúrafejlesztést. Az épületek gyengeáramú hálózatának részeként úgy vásároltunk AP-ket, hogy a kontrollert még nem szereztük be.

Az idő múlásának volt előnye is: az IEEE802.11n szabvány hivatalos lett.

Bizonyos tapasztalatok elavultak: a Microsoft a Windows 2003–2008-as áttéréskor a RADIUS-szervert lecserélte IAS-ról NPS-re, ami okozott némi technikai nehézséget is a megváltozott működés miatt.

A beszerzési döntés előkészítése céljából igyekeztük kipróbálni a szóba jöhető gyártók eszközeit, melyekhez vásárlás vagy kölcsönkérés útján jutottunk hozzá. A tesztek során három termékcsoportot vizsgáltunk meg:

- Colubris-HP (710-es kontroller, 410-es AP)
  A tesztek sikeresek voltak, több kontroller híján a teaming környezetről nem sikerült tapasztalatokat gyűjteni.
- Cisco (5508-as kontroller, 1401-es AP)
  Az alaptesztek sikeresek voltak, de a gyártót addig faggattuk, mígnem közölték: központilag vezérelt AP, local switching és dinamikus VLAN-kiosztás együtt (egyelőre) nem fog működni. Ezzel a Cisco-t lényegében ki kellett zárnunk a lehetséges jelöltek közül.
- Aruba (200-as kontroller, 125-ös AP)
  Az alaptesztek sikeresek voltak, de a local switchinget nem sikerült bemutatni.

Közben humánerőforrás-probléma is adódott: a WiFi-rendszergazda felmondott, újat kellett keresni.

Amíg az ESZK a tervezéssel és a teszteléssel volt elfoglalva, az eduroam terjedt az SZTE-n. Ebben az Egyetemi Könyvtár (EK) járt az élen, majd sorra csatlakozott a Gazdaságtudományi Kar, a Természettudományi és Informatikai Kar (TTIK) Dékáni Hivatala és Matematikus Tanszékcsoportja, valamint az Állam- és Jogtudományi Kar. Utóbbi egységek nemcsak az eduroamhoz, hanem az EK-hoz is csatlakoztak abban a tekintetben, hogy az EK RADIUS-szerverét használják a felhasználóik oly módon, hogy a könyvtári beiratkozás kiegészítéseként az EK-ban WiFi-felhasználói azonosítót is igényeltek.

## 3. Beszerzés

### 3.1. A beszerzés elvi és adminisztratív kérdései

Az előzetes tesztek eredményei alapján lényegében eldőlt a gyártó kiválasztása, amit csak megerősítettek az „A” komponens időközben lefolytatott AP beszerzései.

A beszerzés formája az ún. KEF versenyújraindításos volt. A szállító a SCI-Network Távközlési és Hálózatintegrációs zRt. (továbbiak SCI-Network) lett.

A tárgyalások eredményeképpen 2012. márciusban adtuk fel a megrendelést. Ez egy kb. 18 hónapos időszak kezdetét jelentette, amely egy menetrend alapján magába foglalta a következőket:

- Szállítás: 2012. május 4.
- Mintarendszer (hw, sw) installálása a SCI-Network telephelyén: 2012. május
- Mintarendszer (hw, sw) installálása az ESZK telephelyén, majd integrálása és tesztelése: 2012. május–június
- Rendszeradminisztrátori oktatás: 2012. június
- Dokumentáció készítése, webalapú oktatóanyag elkészítése: 2012. szeptember–október
- Guest manager szoftver fejlesztése: 2012. augusztus–november
- Rendszertervezés: 2012. szeptember – 2013. január
- Rendszerkialakítás: 2013. február – 2013. május
- Tesztüzem az ESZK-ban: 2013. május – 2013. szeptember
- Kísérleti szolgáltatás a Mérnöki Kar „D” épületében: 2013. október
- További épületek bekapcsolása a szolgáltatásba: 2013. október – 2014. február
- Guest manager szoftver bevezetése a WiFi-rendszerre: 2014. április-május

## 3.2. Beszerzett eszközök

A központi rendszer és a hozzá tartozó eszközöket az 1. táblázat tartalmazza.

| Kód | Megnevezés | Db. |
|---|---|---|
| J9370A | HP E-MSM765 zl Mobility Controller | 4 |
| J9371A | HP E-MSM760/765 Additional 40 Access Point License | 4 |
| J9642A | HP E5406 zl Switch with Premium Software | 2 |
| J9538A | HP 8-port 10-GbE SFP+ v2 zl Module | 3 |
| J9283B | HP X242 SFP+ SFP+ 3m Direct Attach Cable | 2 |
| J9152A | HP X132 10G SFP+ LC LRM Transceiver | 2 |
| 1-6536967-0 | SC/LC duplex patchkábel, MM 10Gbit XG 50/125µ, 10m | 2 |
| J8712A | HP 875W zl Power Supply | 4 |
| J9651A | HP E-MSM430 Dual Radio 802.11n AP (WW) | 113 |
| J9622A | HP E-MSM466 Dual Radio 802.11n AP (WW) | 14 |
| J9591A | HP E-MSM460 Dual Radio 802.11n AP (WW) | 5 |
| J9169A | HP In/Out Sector 8/10dBi MIMO 3 Elmt Ant | 26 |
| J9407A | HP 1-port Power Injector | 38 |
| J9298A | HP E2520-8G-PoE Switch | 6 |
| BK650EI | APC Back-UPS CS 650VA, 230V | 9 |
| J9755A | HP PCM+ v4 S/W Platform with 50-dev Lic | 1 |
| J9751A | HP PCM+ Mobility Manager v4 S/W Mod Lic | 1 |
| J9756A | HP PCM+ v4 with 100-dev License | 3 |
| J9760A | HP PCM+ v4 w/1-yr Maint for 550 Dev Lic | 4 |
| SC_Szolg62 | Jótállási idő kiterjesztése termék upgrade biztosításával | 4 |

| | |
|---|---|
| UQ611E | HP Software Support for ProCurve MSM765zl 5 year |
| UY919E | HP Software Support for HP5406 zl 5 year |
| UY989E | HP 5y 24x7 E-MSM430 AP SW Support |
| UY984E | HP 5y 24x7 E-MSM46x AP SW Support |

**1. táblázat** A központi rendszer és a hozzá tartozó eszközök

A beszerzett eszközökre egységesen 5 év garanciát vettünk. Hardvereszközök esetén a szükséges rendelkezésre állást a „life time” Next Business Day cseregarancia mellett a megvásárolt eszközök redundanciája, illetve a tartalék AP-k, switchek és egyéb kiegészítők biztosítják. A szoftverekhez 5 év 24×7 támogatást vásároltunk.

**Korábbi beszerzések**

A TIOP-1.3.1.-07/2/2F-2009-0004 „A” fejezetében lévő épületfelújítások során beszerzett AP-k számát és típusát a 2. táblázat tartalmazza.

| Kód | Megnevezés | Db. |
|---|---|---|
| J9359A | HP MSM422 802.11n AP (WW) | 50 |
| J9651A | HP E-MSM430 Dual Radio 802.11n AP (WW) | 47 |

**2. táblázat** TIOP-1.3.1.-07/2/2F-2009-0004 „A” fejezetéből beszerzett AP-k

**Egyéb beszerzések**

A 3. táblázat tartalmazza azokat az eszközöket, melyeket a WiFi-szolgáltatás bevezetésénél használtunk, de saját forrásokat használtunk fel hozzájuk.

| Kód | Megnevezés | Db. |
|---|---|---|
| J9146A#ABB | PROCURVE 2910AL-24G-POE+ Switch | 5 |
| | Cat.6 SFTP végpont kiépítése (nyomvonal, csatorna, kábel stb.) | 52 |
| | Kültéri körsugárzó antenna: TerraWave Solutions 802.11n 2.4/5 GHz 6 dBi. | 1 |
| X2-10GB-LRM | 10GBASE-LRM X2 Module | 2 |
| | Lakat | 140 |
| J9591A | HP E-MSM460 Dual Radio 802.11n AP (WW) - ÁJTK saját beszerzés | 13 |

**3. táblázat** Egyéb beszerzésekből származó eszközök

**Új menedzsmentszoftver**

| Kód | Megnevezés | Db. |
|---|---|---|
| JG768AAE | HP PCM+ to IMC Std Upg w/ 200-node E-LTU [pre-release] | 1 |
| JG769AAE | HP PMM to IMC WSM Upg w/ 250-node E-LTU [pre-release] | 1 |
| JF415AAE | HP IMC WSM 50-Access Point E-LTU | 2 |
| | | |
| U0WV9E | HP 3y 9x5 2h cbk JG768AAE Nwk SW Supp | 1 |
| U0WW6E | HP 3y 9x5 2h cbk JG769AAE Nwk SW Supp | 1 |
| UV738E | HP 3y 9x5 Networks Group 145 Lic Supp [for JF415AAE] | 1 |
| | | |
| JG142AAE | HP IMC WSM Components Location Service Package E-LTU | 1 |
| UV752E | HP 3-Year, 9x5 SW phone support, software updates | 1 |

**4. táblázat** Az iMC-komponensek

## 3.3. Környezetkialakítás

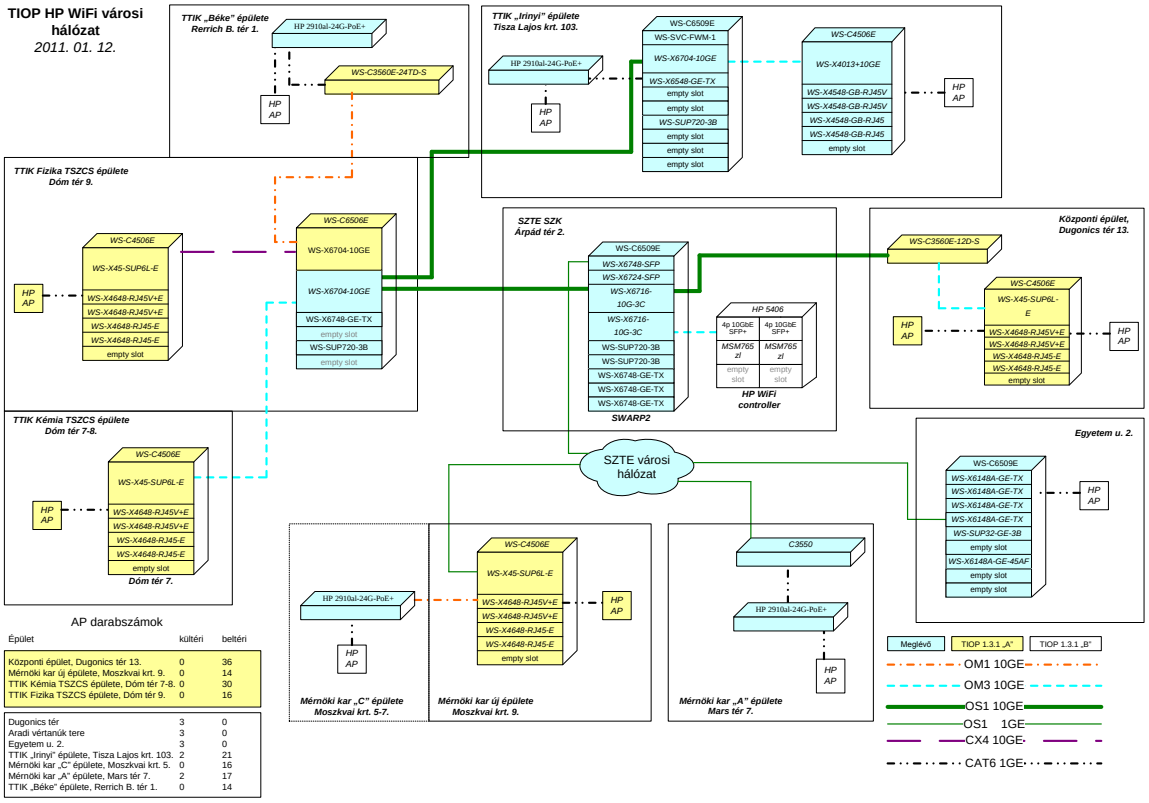
### 3.3.1. Az AP-k elhelyezése

Az AP-k PoE-es eszközök, ezért a hálózatnak a csatlakozáson kívül az áramellátást is biztosítania kell az eszköznek:

- Az „A” komponens új vagy felújított épületei esetén a szükséges számú PoE-es végpont része volt a gyengeáramú hálózatnak.
- A „B” komponens esetén az épületek nagyobb részében új hálózati végpontokat kellett kiépíteni, míg a PoE-táplálás céljára az AP-k számától függően kisebb-nagyobb switcheket alkalmaztunk.

- A powerinjektorokat az egy-két végpontos telepítések megoldásához szereztük be.

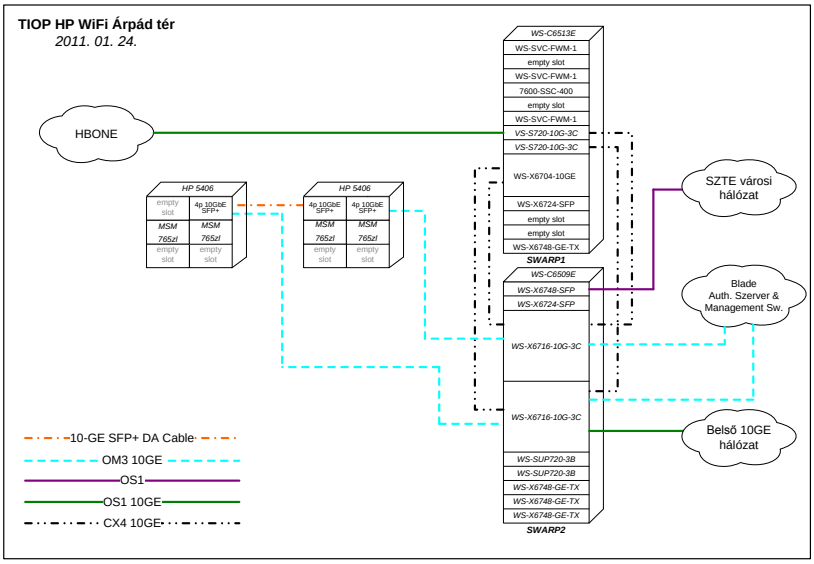
Vagyonvédelmi célokra az Elzett-lakatot választottuk mint költséghatékony megoldást – az AP-k megfelelő, azaz többnyire 2,5–4 m. magasságban történő elhelyezése mellett.




**3. ábra** TIOP WiFi városi hálózat 2011.01.12.

### 3.3.2. A központi rendszer csatlakoztatása

A „B" komponensből bővítettük a hálózat központi eszközeit, ezért a WiFi-rendszer központi elemeinek megfelelő sávszélességű redundáns hálózati csatlakozása két újabb transceiver beszerzésével megoldható volt.




**4. ábra** Központi hálózati rendszer

# 4. A központilag menedzselt WiFi-rendszer

## 4.1. A rendszer célja

A rendszer célja korszerű WiFi vezeték nélküli hálózati szolgáltatás bevezetése. A WiFi-hálózat kiegészítése lesz a jelenleg is folyamatosan bővülő – lényegében az egyetem épületeit teljesen lefedő – korszerű Ethernet vezetékes hálózatnak.

## 4.2. A rendszer felépítése

Központilag menedzselt egyetemi WiFi-rendszert terveztünk, melynek két fő komponense van:

- Redundáns központi kontroller.
- Az egyetemi épületekben elhelyezett WiFi AP-k, melyek az egyetemi gerinchálózaton csatlakoznak a kontrollerhez – IP feletti tunnelben.

Az egyetemen kiépített WiFi-rendszer alapját a redundáns WiFi-vezérlők képezik, amelyek alapvetően Layer 3-as eszközök. A kontrollereket két HP 5406 típusú switchben helyeztük el. A WiFi-hálózat működését az egyes épületekben elhelyezett AP-k valósítják meg, melyek az ESZK-ban elhelyezett központi kontrollerhez IP felett kapcsolódnak. A hálózati környezet részletes leírása az 5. fejezetben található.

Az ESZK-ban elhelyezett eszközök N+1-es redundanciát tartalmaznak meghibásodás esetére. Az épületekbe telepített AP-kból pedig elegendő tartalék berendezést tartunk meghibásodás esetére.

A rendszerhez szorosan kapcsolódik az AAA feladatokat ellátó RADIUS-szerverhálózat. Továbbá egy központi adatbázis, amely a felhasználók neveit és hozzáférési jogait tartalmazza. A központi berendezéseket az ESZK munkatársai menedzselik.

## 4.3. A rendszer alkotóelemei és azok tulajdonságai

### 4.3.3. A rendszer alapvető tulajdonságai:

- Az SZTENET jelenlegi – fizikai és logikai – hálózati struktúráját használja.
- WPA/WPA2 Enterprise titkosítás használata.
- RADIUS-szerveren alapuló IEEE 802.1x-es autentikáció.
- Lokális erőforrások elérése a WiFi-hálózatból.
- N+1-redundáns központi rendszer.
- Automatikus AP-konfigurálás előre megadott profil alapján.
- A rendszer automatikus frekvenciamenedzsert tartalmaz, amely képes az AP-k frekvenciájának automatikus beállítására.
- Az egyetemi épületekben és azok környezetében telepített idegen AP-k felderítése.
- Folyamatos felügyeletet ellátó menedzsmentrendszer.
- Automatikus statisztikakészítés.
- Az autentikáció azonosító/jelszó alapján történik, a felhasználói azonosító név@realm alakú.
- Autentikációs protokoll: PEAP. (SSL/TLS tunnel, MS-ChapV2, MD4 kódolás).
- A kliensek supplicantot használnak, a captive-portált nem vezettük be.

### 4.3.4. A rendszert felépítő eszközök, és azok főbb paraméterei:

*a.) Központi kontrollerek*

A kontrollereknek két fő feladatuk van: Egyrészt az AP-k vezérlése IP felett kiépített tunnelek segítségével, másrészt az AP-ktől érkező felhasználói forgalom továbbítása az SSID-nek megfelelő kimeneti interfészre. Igény esetén a kontrollerek hálózati címfordítást is végeznek.

A kontrollerek tulajdonságai:

*Hardver:*

- Moduláris házba telepíthető ProCurve MSM765zl Mobility Controller.
- Hálózati interfész: 2×10 Gbps csatlakozás.
- A befogadó switch HP E5406 zl Switch. A switch kijárati interfésze 8×10 Gbps Ethernet.
- Konzolport: 1 db RS-232C, fizikai interfész DB-9, amely a befogadó switchen helyezkedik el.

*Licencelés:*

- Egy kontroller AP licencszáma 200-ig bővíthető.
- Az alaplicencszám 40-es lépésekben bővíthető, megvásárolt licencszám a négy kontrollerre összesen 320.
- A licencek a kontrollerek között szabadon mozgathatók.

*Szoftver:*

- Egy kontroller által egyidejűleg kezelhető kliensek száma 2000.
- A felhasználói adatforgalom irányítása: a felhasználói adatforgalom a felhasználó jogosultságától és a kiválasztott SSID-tól függően vagy az AP lokális (épületen belüli) hálózatában marad, vagy megfelelően titkosított, IP feletti kommunikációval a központi kontrolleren keresztül halad át (access controlled).
- A különálló kontrollereket teaming módban összekapcsoltuk.
- A teamben összefűzött kontrollerek konfiguráció- és szoftverfrissítése automatikus.
- Az AP-k szoftverfrissítése a kontrollerekből történik.
- Az AP-k automatikus programozása előre definiált csoportok alapján történik.
- A kliensek azonosítása a következő szabványok szerint történik: IEEE 802.1X, IEEE 802.11i, PEAP, EAP-MSCHAPv2.
- Integrált captive-portál.

*b.) Az épületekbe kihelyezendő AP-k*

Ezek a berendezések teremtik meg a kapcsolatot a rádiós hálózat és a vezetékes hálózat között. Az AP egyfajta médiakonverter. A jelenlegi eszközeink a 802.11a/b/g/n szabványt támogatják. Az AP-k helyét úgy választottuk meg, hogy a kiválasztott épületekben lehetőleg 100%-os lefedettséget biztosítsunk. A lefedés ún. data only, tehát csak lefedettséget biztosítunk, de minimális sávszélességet nem írunk elő. Ezenkívül külső terek részleges lefedéséhez is vásároltunk AP-ket. Azokban az épületekben, ahová központilag telepített rendszer kerül, a kioszthatóó csatornák száma miatt az egyetemi egységeknek az 5 GHz-es frekvencia tartományt ajánljuk saját WiFi-hálózatukhoz. A telepítéshez szükséges az ESZK engedélye.

*Telepített AP típusok:*

- MSM422
- MSM430
- MSM460
- MSM466

*Hardver tulajdonságai:*

- Hálózati interfész: 1× 802.3af PoE, 802.1q képes port.

*Szoftver tulajdonságai:*

- Központilag menedzselt,
- egyidejűleg használható VLAN-ok száma 80,
- egyidejűleg használható SSID-k száma 16.

*c.) HP 5406 switchek*

Feladatuk a kontrollerek befogadása, azok összekötése az SZTE hálózatával. A hálózati topológiát az 5. fejezetben részletesen bemutatjuk.

*Főbb hardvertulajdonságok:*

- Hálózati interfész: 2 db 8×10 Gb kártya (SARP5), és 1 db 8×10 Gb (SARP8) kártya
- Tápellátás: 2× (redundáns) tápegység modul
- Distributed-LACP

*d.) Cisco 6509 switch*

Az SZTE meglévő gerinchálózatában SWARP2 néven ismert hálózati eszköz. Te3/7 és Te4/7 portjait használja a WiFi-rendszer átmenő forgalma. A hálózati topológiát az 5. fejezet ismerteti.

*e.) Menedzsmentszoftver*

Feladata, hogy felügyelje a WiFi-szolgáltatást nyújtó rendszert. Beszerzéskor a szállító a Procurve Management v4-et ajánlotta Mobility Manager modullal kiegészítve. A szoftvert le is szállították, egy év elteltével a frissítés során derült ki, hogy a HP már az iMC szoftvercsaládot ajánlja, illetve befejezi a támogatást a PCM PMM párosra. Így kényszerből át kellett állni az iMC 7.0-ra. A felügyeleti szoftver rendszer VMware-környezetben fut. A futtatáshoz szükséges operációs rendszer Red Hat.

Az iMC fontosabb funkciói:

- A forgalom monitorozása biztonságos, titkosított (pl. SSL) csatornán keresztül.
- A nem regisztrált (idegen) AP-k felderítése.
- A forgalom monitorozása mennyiségi vonatkozásban.
- A WiFi-hálózat egészének, illetve az egyes eszközöknek a felügyelete, rendkívüli eseményekről értesítések generálása.
- Gondoskodik a felügyeleti rendszer adatbázisának, konfigurációs fájljainak előre definiált időpontokban való mentéséről. Ha esetleg szükséges, a mentett adatokból képes helyreállítani a teljes rendszert.
- Jelentések, statisztikák készítése a kezelők számára.

*f.) Kliensek*

A szolgáltatások igénybevételéhez a kliens gépére telepített vagy az operációs rendszer részét képező supplicant használatát írtuk elő. Nem támasztottunk magas követelményeket. Bármilyen géppel igénybe lehet venni a szolgáltatást, amely megfelel az alábbi követelményeknek:

- 802.11 a/b/g/n WiFi szabványok valamelyikének támogatása,
- WiFi titkosítás: WPA/WPA2 Enterprise TKIP/AES.

*g.) Kiegészítő komponensek*

Ebbe a kategóriába tartoznak az alap-WiFi-szolgáltatáshoz szükséges egyéb szerverek, szolgáltatások.

*AAA-szerverhálózat*

Telepítésre került két darab, redundánsan üzemeltetett FreeRADIUS szerver, melyek AAA-szolgáltatásokat nyújtanak. Ezek operációs rendszere Redhat, míg RADIUS-nak FreeRADIUS 2.1 telepítettünk. A RADIUS-szolgáltatások adatbázis back-endjét master-master replikán alapuló redundáns MySQL szerverek képezik. A MySQL-t is az előbb említett két gép szolgáltatja.

Az eduroam és tanszéki jellegű forgalmak kezelésében is szerepet kap (kérések proxyzása) a korábbi központi RADIUS-szerver pár.

Az autentikációt Microsoft IAS/NPS szerverek végzik, melyek alapvetően az ETR (az egyetemi tanulmányi rendszer) active directoryjára támaszkodnak.

*DHCP-szerverhálózat*

A WiFi AAA-szolgáltatatásait végző szervereken kapott helyet egy-egy ISC típusú DHCP-kiszolgáló. Ezek a DHCP-szerverek a „központi” típusú elérésnél a privát IP-címek dinamikus kiosztását végzik.

*SCIBILL guest manager szoftver*

A vendég- és konferenciavoucherek kiosztását egy erre a célra kifejlesztett, webes felületen futó alkalmazás végzi.

Főbb tulajdonságok:

- Nagyobb létszámú vendég (konferenciák, egyéb rendezvények) autentikációs adatainak kezelése.
- A vendégek internetforgalmát előre megadott időszakra vagy időtartamra lehet korlátozni.

A vendég- és konferenciafelhasználók AAA-igényeit önálló FreeRADIUS szerverpár szolgálja ki. A RADIUS-szerverek másik feladata a vendégfelhasználók vouchereinek kiosztására jogosultak azonosítása és azok jogkörének meghatározása.

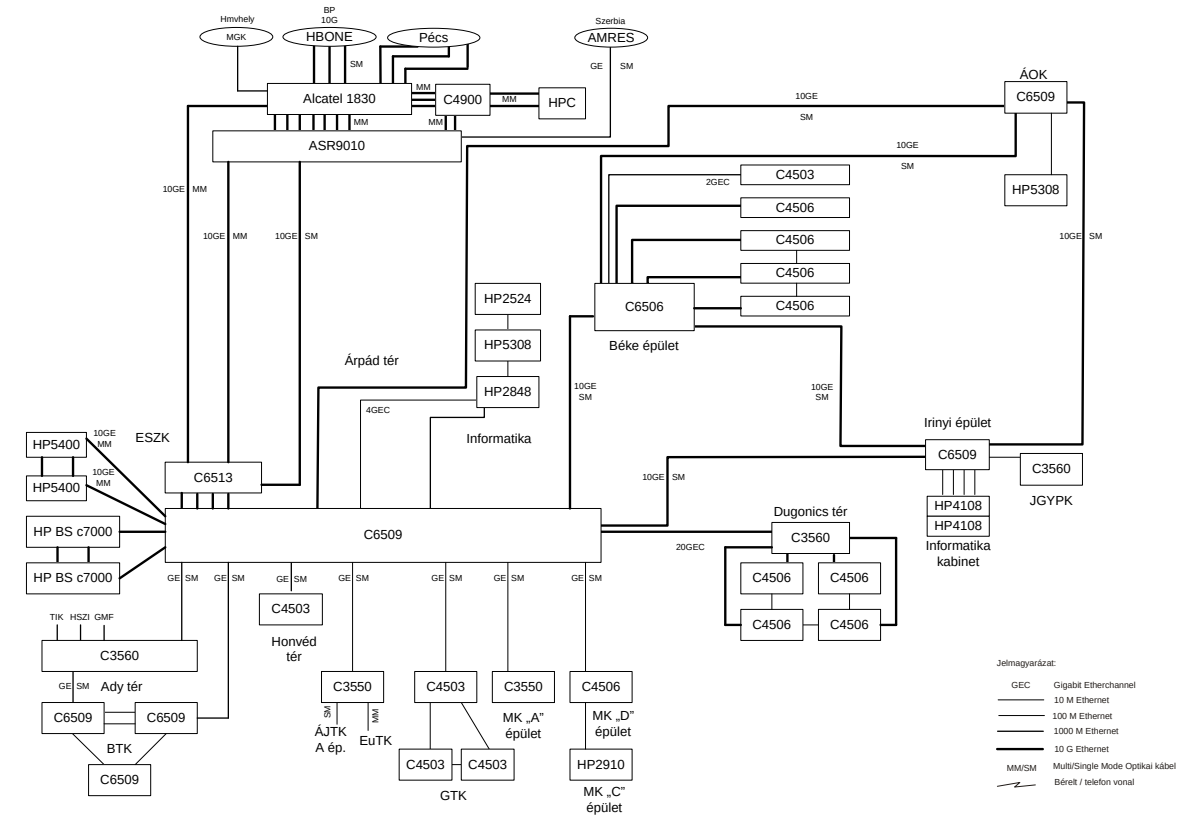
# 5. Hálózat

## 5.1. Az SZTENET felépítése

Az SZTENET egy Ethernet hálózat, a Layer3 protokoll az IPv4. A hálózat magjában egy Layer3-as switchekből kialakított rendszer található, ehhez csatlakoznak közvetlenül az olyan központi szolgáltatások eszközei, mint például az ETR szerverei és a tervezett WiFi-szolgáltatás switch-kontroller rendszere. Az egyetemi gerinchálózaton keresztül a központi switchhez csatlakoznak továbbá az egyes épületekhez, alhálózatokhoz tartozó switchek vagy egyéb eszközök (például tűzfal).

Ezek – egyéb funkcióik mellett – ún. Layer3 demarkációs eszközök is. Ezek és a központi switchek végzik a routingot az IP subnetek, a „Layer3-szigetek” között. Tehát az SZTENET-ben nincsenek a gerinchálózat felett kifeszített Layer2 VLAN-ok.

A WiFi-rendszert az SZTENET jelenlegi – fizikai és logikai – hálózati struktúrájának módosítása nélkül kellett telepíteni. Ezt úgy valósítottuk meg, hogy az épületekben elhelyezett AP-k az egyetemi gerinchálózaton IP-tunnellel csatlakoznak a központi kontrollerhez.




**5. ábra** SZTENET-topológia

A TIOP-pályázat előtt az SZTE hálózatában a core- és az edge-funkciókat egy L3-as Cisco Catalyst 6500 switch látta el. A megnövekedett sávszélességigényeket kielégítendő és a fentebbi funkciók szétválasztását elősegítendő e pályázatból beszereztünk egy új Cisco Catalyst 6500-as switchet is. A beszerzés lehetővé tette, hogy az így már két switchből álló központi rendszerünket további modulokkal bővítsük. Lásd a 4. ábrát.

A core-funkciókat ellátó switchet 2×10GE redundáns kapcsolat köti össze a két WiFi-switchcsel.

A WiFi-rendszer SZTENET-beli elhelyezkedését a 3. ábra mutatja be.

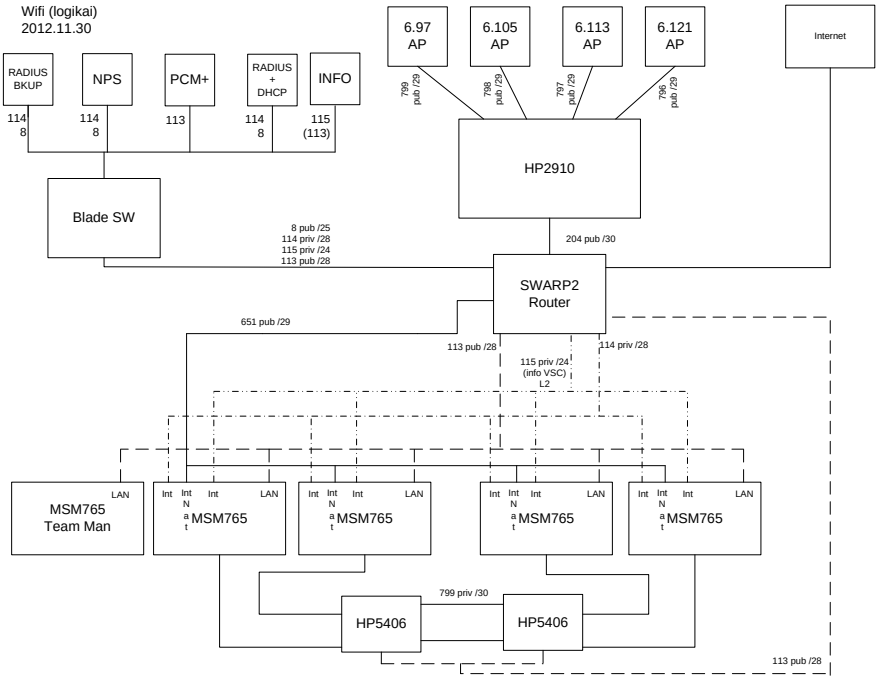
## 5.2. A WiFi-rendszer alapbeállításai

A WiFi-rendszer szempontjából a vezetékes hálózat két logikai részre bontható: menedzsment hálózatra és produkciós hálózatra.

A kontroller LAN (egyik fizikai) portjára definiáltuk a menedzserhálózatot, amely a 113-as natív VLAN-ba tartozik. Ezen a hálózaton tartja a kontrollerteam a kapcsolatot IP felett az AP-csoportokkal, ezen VLAN-on történik az AP-k kezdeti felismerése, a

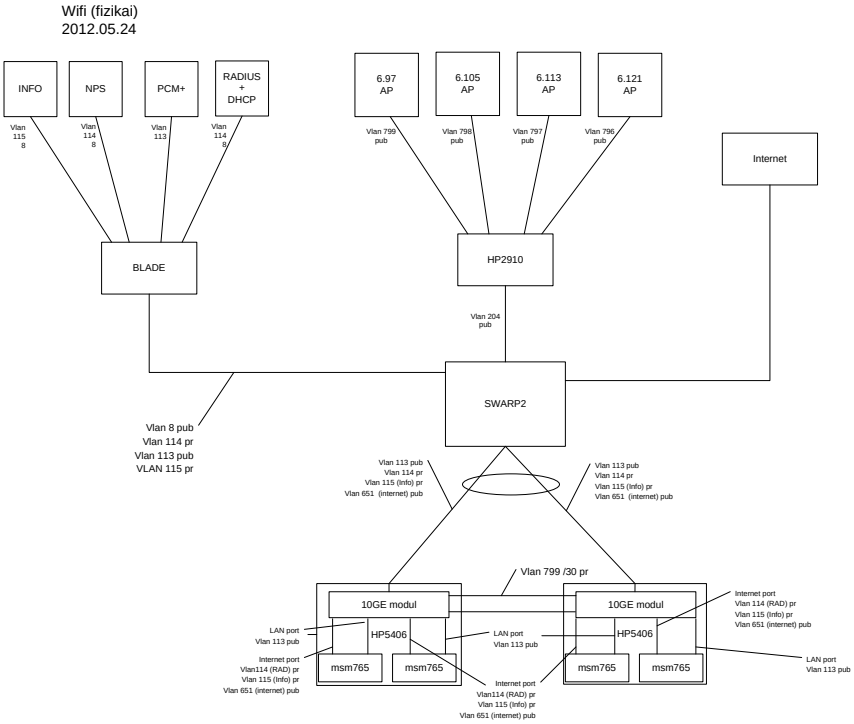
konfigurációs beállítások frissítése. Ebben a hálózatban kapott helyet a PCM+, illetve az iMC felügyeleti szerver is.

A kontrollerek INTERNET (fizikai) portján hoztuk létre azt a privát hálózatot, melyen a RADIUS és DHCP forgalmak haladnak keresztül. A tényleges produkciós forgalom a kontrollerek INTERNET portján definiált, (a kontrollereken) NAT-olt szubinterfészeken keresztül éri el az SZTENET-et. A logikai topológiát a 6. ábra mutatja be.




**6. ábra** A WiFi-hálózat logikai topológiája

Az egyes berendezések fizikai összeköttetését pedig a 7. ábra mutatja be.

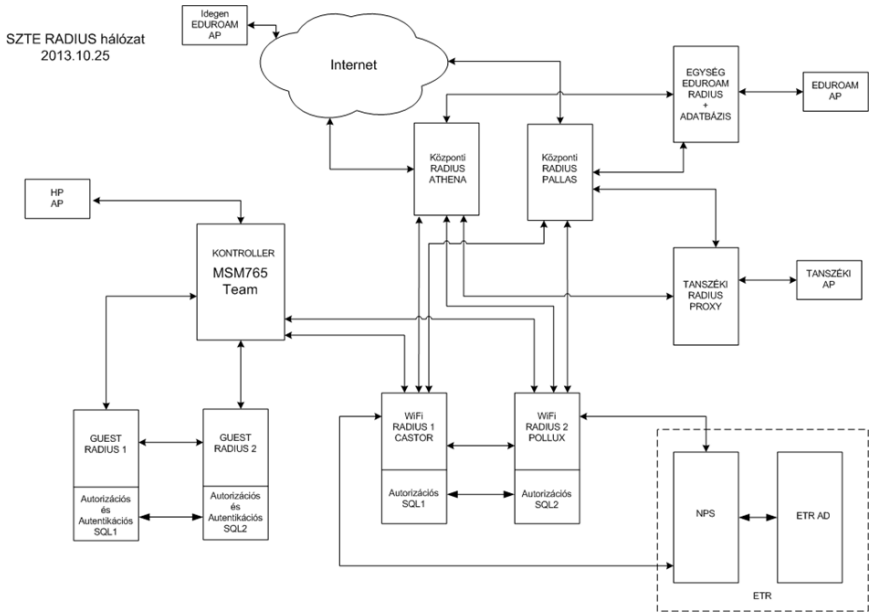



**7. ábra** A WiFi-hálózat fizikai topológiája

# 6. Az AAA-rendszer

## 6.1. Felépítés

A rendszer tervezésénél a biztonságos kiszolgálást tartottuk szem előtt, ezért minden kritikus funkciót ellátó szerverből kettőt állítottunk be. A RADIUS-hálózat felépítését a 8. ábra mutatja be. A központi WiFi-szolgáltatáshoz négy FreeRADIUS szervert, és egy NPS szervert telepítettünk. A szerverpárokat a szerverkonszolidáció során létrehozott virtuális felhőben helyeztük el.




**8. ábra** RADIUS-hálózat

## 6.2. Realmrendszer

Realmnek nevezzük az azonosító @ utáni suffixét. A realm a felhasználói azonosító azonosítási helyét adja meg. A realm segítségével lehet eldönteni, hogy egy felhasználói azonosítót melyik RADIUS-szerver segítségével lehet autentikálni. Az autentikációs folyamat elején a realm alapján a RADIUS-szerver eldönti, hogy önmaga dolgozza fel a kérést, vagy tovább proxyzza azt egy másik szervernek. A WiFi esetében nem csak a realm, hanem az SSID is szerepet játszik a folyamatban. Az egyes SSID-k esetében a folyamat a következő:

- szte-wifi, szte-lan:
  Ezekben az esetekben nem történik proxyzás. Amennyiben a felhasználói azonosító realmje nem egyezik meg a @wifi.u-szeged.hu-val, az adott felhasználót nem autentikáljuk.
- eduroam-szte:
  Ebben az esetben a realmnek megfelelően megkísérli az autentikációs kérést feldolgozni a rendszer. Ha a felhasználó azonosító a @wifi.u-szeged.hu realmet tartalmazta, akkor helyben próbálja megkísérelni az autentikációt, míg egyéb esetekben a PALLAS vagy az ATHENA nevű központi RADIUS-kiszolgálók felé küldi tovább a kéréseket.
- szte-guest:

Ebben az esetben olyan RADIUS-szervert használunk, amely független a RADIUS-szerverek hierarchiájától. Ez azt jelenti, hogy nincs kapcsolat a guest RADIUS és a többi RADUS-szerver között. Az itteni felhasználói azonosító nem tartalmaz realmet. Az autentikációs kérés a helyi szerveren kerül feldolgozásra.

A WiFi-rendszeren kívülről jövő autentikációs kérések a PALLAS és az ATHENA irányából csak akkor érik el a CASTOR, illetve a POLLUX szervereket, ha azok realmje megegyezik a @wifi.u-szeged.hu-val. Ebben az esetben a szerverek természetesen megpróbálják elvégezni az autentikációt, és annak eredményét visszaküldik a PALLAS és az ATHENA szerverpár felé.

## 6.3. Az ETR kapcsolata a WiFi-s RADIUS-szerverekkel

Az autentikációs rendszer mellett a WiFi adminisztrációs felületet is ellátja adattal az ETR, a kapcsolat felépítését tekintve két funkcióra elkülönítve került megvalósításra. A következőkben ezeket mutatjuk be röviden.

### 6.3.1. ETR-interfész

Ez egy, az ETR-üzemeltetés által specifikált protokoll, amely a felhasználói jelszavak kiadása nélkül képes elvégezni az autentikálást az ETR adatbázisait használva külső rendszerekből, mint amilyen a WiFi adminisztrációs felület is. HTTP kérés paramétereiben kell megkérdezni az ETR-üzemeltetéssel közösen megállapodott végpontot (egy megadott szervert), amely rögzített paraméterformátumú válaszban küld egy tokent sikeres autentikáláskor a WiFi adminisztrációs felületnek, majd a felhasználó böngészőjét egy előre megállapodott URL-re irányítja át a megadott tokennel. Amennyiben egy beállított időkorlát alatt keresi fel a kliens böngészője a WiFi adminisztrációs felületet, akkor az autentikálás sikeres, és bejelentkezést nyer a WiFi adminisztrációs felületre is.

### 6.3.2. Webservice

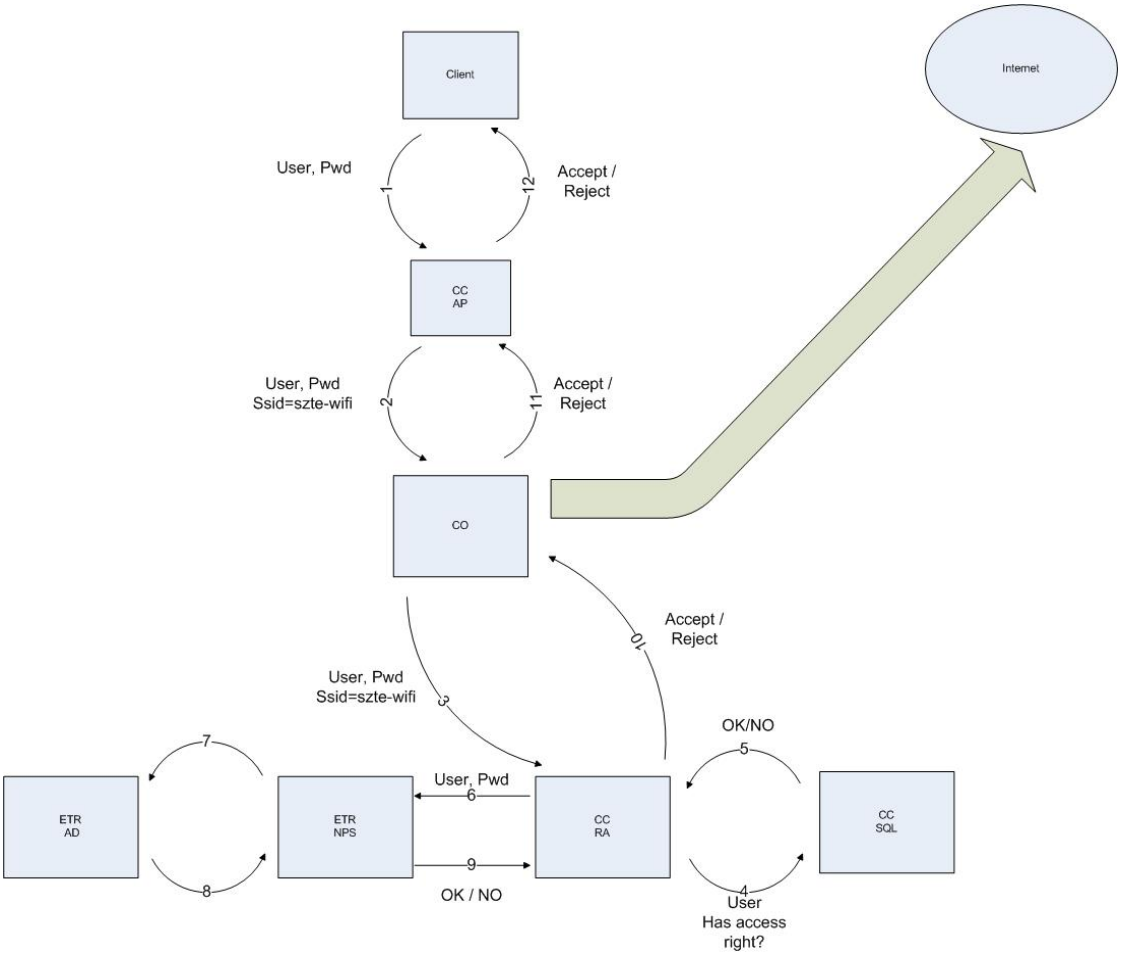
Bizonyos adatok frissítése (természetes név, pipálási jog, emailcím) kulcsfontosságú a jogosultsági rendszer működéséhez, illetve a felhasználókkal való kommunikáció szempontjából. Ehhez a szinkronizációhoz fejlesztette ki az ETR-üzemeltetés a SOAP típusú webservice-lekérdező függvényeket, melyekkel jól körülhatárolt marad a két kapcsolódó rendszer, és főként nem sérül az ETR biztonsági integritása. Ugyanazon adatok lekérésére van lehetőség az egyik függvénnyel, mint az autentikáció esetén. Létezik viszont egy olyan segédfüggvény, amely az ETR AD és FreeRADIUS közötti láncszem. Ez a nevezett függvény állítja át a WiFi-szolgáltatást igénybe venni kívánó felhasználó ETR AD-bejegyzésének UPN suffix attribútumát a „@wifi.u-szeged.hu” principal name suffixre, melyet a RADIUS terminológiában realmnek nevezünk.

## 6.4. AA-folyamat

Az AA-rendszer (autentikációs és autorizációs rendszer) megalkotásánál figyelembe kellett vennünk a már meglévő rendszerek tulajdonságait és az egyetemi tanulmányi rendszer vezetése által hozott policykat. Így amellett a megoldás mellett döntöttünk, hogy FreeRADIUS szerverekkel autorizálunk, és NPS szerverrel végezzük az autentikációt. Ezt az osztott fázisú módszert a FreeRADIUS konfigurációs felépítése teszi lehetővé. A FreeRADIUS szerverekhez eljutó kérések életútja a preautentikációs fázisban dől el. Itt kerül ellenőrzésre a kérés realmtartalma. Ennek

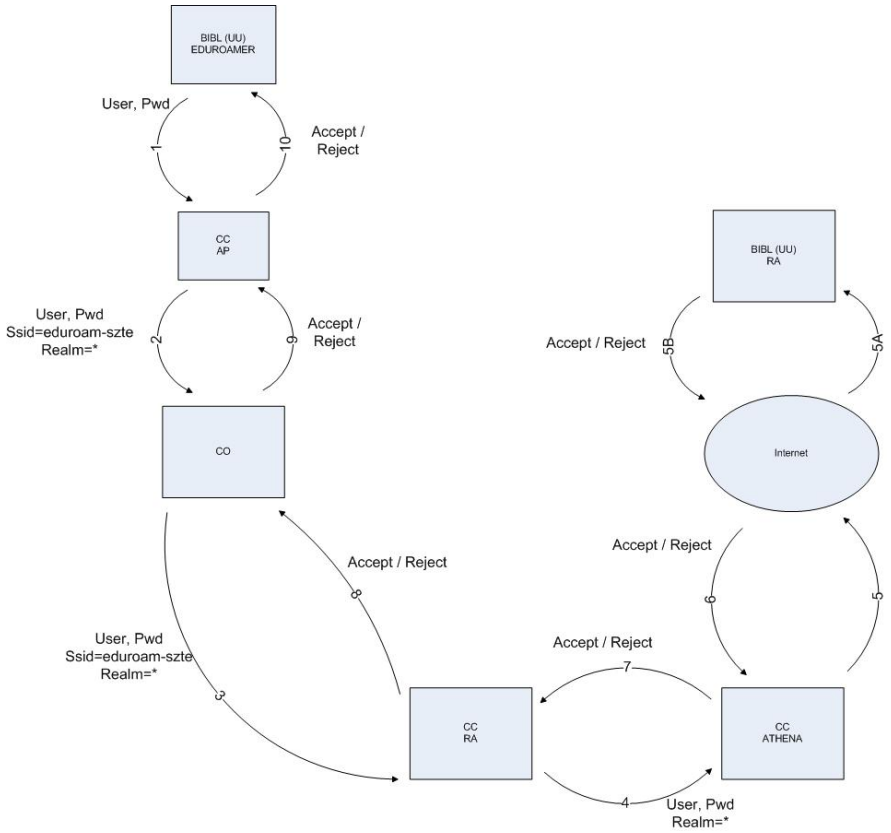
függvényében kerül proxyzásra a kérés, helyben a FreeRADIUS szervereken nem végzünk autentikációt.

Ha honos („@wifi.u-szeged.hu”) realmet találunk, abban az esetben a kérés továbbításra kerül az ETR NPS szervere felé, egyéb esetben az egyetemi központi RADIUS-ok felé továbbítódik a kérés. Amint megérkezik a feldolgozás eredménye, a post-proxy fázisban kezdetét veszi a policykonfigurációk feldolgozása, mely magában foglalja a jogosultságellenőrzést, a szimultán felhasználói kapcsolat korlátainak vizsgálatát, valamint a dinamikus VLAN hozzárendelést a lokális szolgáltatás esetében. Amennyiben nem definiált feltételekkel találkozik a RADIUS-szerver, úgy az autentikációs kérés elutasításra kerül.

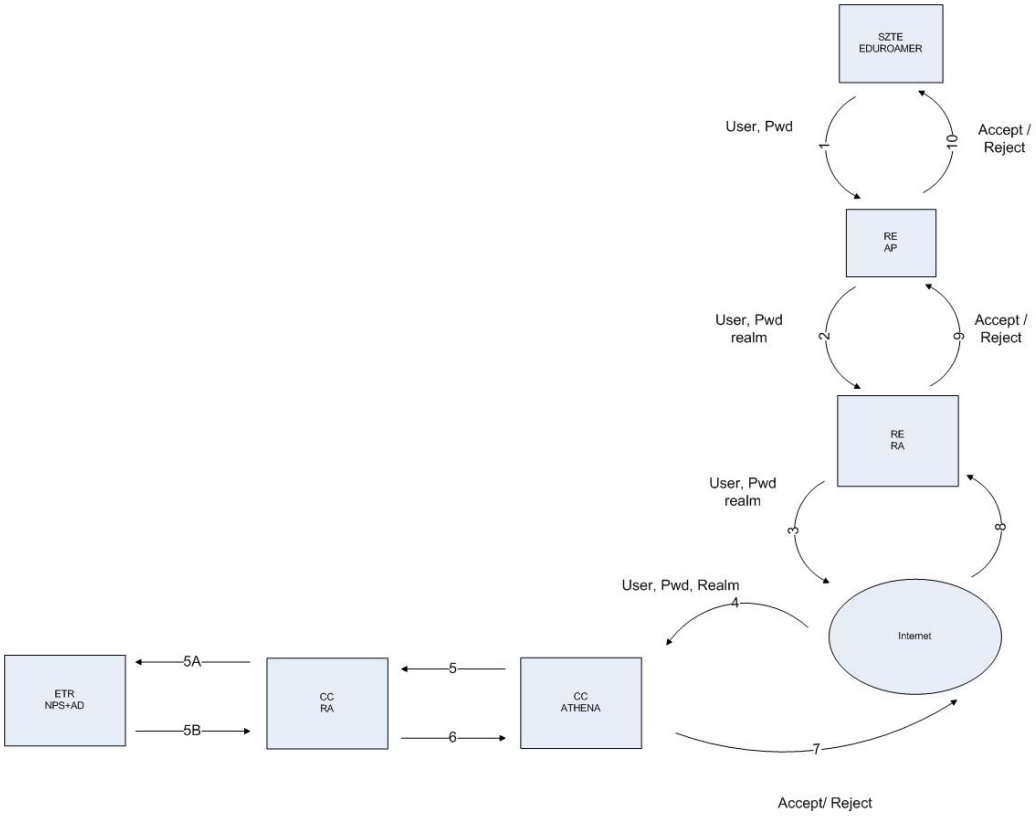



**9. ábra** SZTE WiFi AA-folyamat

Az egyetemi WiFi-szolgáltatás keretében eduroam-szolgáltatást is biztosítunk, melyet kétoldalúan támogat az AA-rendszer. A „@wifi.u-szeged.hu” realmet használó felhasználóknak lehetőségük van az azonosítójukat használni az eduroam-föderációba belépett külső hálózatokon is. Ekkor a kéréseket az egyetemi RADIUS-szerverek továbbítják a WiFi RADIUS-ok felé, ahol a már ismert módon történik a kérések feldolgozása.




**10. ábra** Eduroam AA-folyamat saját AP-k esetén




**11. ábra** Eduroam AA-folyamat SZTE-n kívüli kérés esetén

A vendég-, illetve konferenciafelhasználók kéréseinek kezelése külön alrendszerben történik, mely a 6.6. pontban kerül leírásra.

### 6.5. Accounting

Az accounting információkat több célra használjuk. Az AA-rendszer ezek alapján ellenőrzi a szimultán felhasználói hozzáférést. A menedzsmentszkriptek például olyan információt nyernek ki belőlük, hogy az autentikált felhasználó melyik AP-hoz csatlakozott, mennyi volt az adatforgalma, kapott e gépe megfelelő IP-címet stb. Az adatok alkalmasak egyszerű felhasználói statisztika készítésére is.

### 6.6. Vendéghozzáférés

A vendégszolgáltatás speciális WiFi-szolgáltatást jelent. A lényege, hogy a vendégfelhasználó azonnal kap felhasználói azonosítót és jelszót, amelyet rögtön használhat. Ehhez önálló autentikációs rendszert kellett üzembe állítani. Az autentikációs rendszer FreeRADIUS-alapú. Két FreeRADIUS szerver nyújtja ezt a szolgáltatást is. A FreeRADIUS-ok back-endje egy MySQL-adatbázis. Egy erre a célra írt voucherkitöltő program segítségével a MySQL-en lévő az adatbázisba kerülnek be a felhasználói adatok, illetve a program segítségével generálódik az egyedi felhasználói azonosító és jelszó. Az így generált felhasználói azonosító nem tartalmaz realmet.

## 7. Szolgáltatások

Egy szolgáltatást minden épületben ugyanazzal az SSID-vel lehet igénybe venni. Az egyes épületek között ilyen értelemben nem tettünk különbséget. Az, hogy az adott épületben egy adott felhasználó milyen szolgáltatást tud igénybe venni, a RADIUS-adatbázis jogelemtáblája alapján dől el. A szolgáltatást a felhasználó neve, az adott épület (AP-csoport) és az SSID határozza meg egyértelműen. Az alábbi pontokban az egyes szolgáltatásokat soroljuk fel. A szolgáltatás SSID-jét zárójelben tüntettük fel.

### 7.1. Központi internetelérés (szte-wifi)

Ezt a szolgáltatást azoknak a felhasználóknak (egyetemi oktató, dolgozó vagy aktív státuszú hallgató) ajánljuk, akik az Egyetem központi szolgáltatásait vagy a külső hálózatokat kívánják elérni. A szolgáltatást a felhasználói azonosítóval és jelszóval lehet igénybe venni.

Az szte-wifi SSID-hoz globális privát IP-címtartomány tartozik (az eduroam-szte esete hasonló). Sikeres autentikáció után, az AAA-szervereken található DHCP-kiszolgáló rendel egy privát IP-címet a WiFi-kliensnek, amelyet a kontroller NAT-ol.

A WiFi-kliensek adat-, vezérlési és menedzsmentforgalma egyaránt átmegy a központi kontrolleren.

### 7.2. eduroam (eduroam-szte)

Ezt a szolgáltatást azoknak a felhasználóknak (egyetemi vagy vendégoktató, dolgozó vagy hallgató) ajánljuk, akik a külső hálózatokat kívánják elérni és rendelkeznek eduroamos azonosítóval. A szolgáltatást az eduroamos felhasználói azonosítóval és jelszóval lehet igénybe venni.

Az eduroam-szte SSID-hoz globális privát IP-cím tartomány tartozik (az szte-wifi esete hasonló). Sikeres autentikáció után, az AAA-szervereken található DHCP-

kiszolgáló rendel egy privát IP-címet a WiFi-kliensnek, amelyet a kontroller NAT-ol. A WiFi-kliensek adat-, vezérlési és menedzsmentforgalma egyaránt átmegy a központi kontrolleren.

## 7.3. LAN-elérés (szte-lan)

Ezt a szolgáltatást azoknak a felhasználóknak (egyetemi oktató vagy dolgozó) ajánljuk, akik egy adott épület helyi erőforrásait kívánják elérni. Ezt a szolgáltatást is ugyanazzal a felhasználói azonosítóval és jelszóval lehet igénybe venni, mint a központi internetelérést. A felhasználó RADIUS-adatbázisban rögzített tulajdonságai és az érintett AP-csoport együttesen határozzák meg a felhasználó egyedi VLAN-ját. A lokális VLAN-okhoz történő hozzárendelés dinamikus, és azt csak az AP által egyidejűleg kezelhető VLAN-ok száma korlátozza, míg az egyidejűleg kezelhető SSID-k száma lényegében nem.

Ebben az esetben a WiFi-kliens az épülethez tartozó kiválasztott VLAN-hoz rendelt IP-címtartományból kap (fix) címet. Az IP-cím beállítása (manuális, DHCP) a helyi gyakorlatnak megfelelően történik.

A WiFi-kliens adatforgalmának switchelését az AP végzi (local switching), így az nem terheli a központi rendszert és a gerinchálózatot, melyeken csak a vezérlési és menedzsmentforgalom megy át.

## 7.4. Konferencia/vendég elérés (szte-guest)

Ezt a szolgáltatást azoknak a felhasználóknak ajánljuk, akik ideiglenesen kívánják igénybe venni az SZTE központi WiFi-hálózatát. Jellemzően egyetemi dolgozók vendégei, egyetemen tartott konferenciák vendégei.

Ez a szolgáltatás különálló, zárt autentikációs folyamatot használ, a központi szolgáltatástól független AAA-adatbázist és attól eltérő forgalomszabályozást. Az ideiglenes hozzáféréshez a felhasználónév/jelszó párost tartalmazó vouchereket a SCIBILL guest manager szoftverrel kell elkészíteni. Az így elkészített azonosítók automatikusan bekerülnek az AAA-adatbázisba. Sikeres autentikáció után, az AAA-szervereken található DHCP-kiszolgáló rendel egy privát IP-címet a WiFi-kliensnek, amelyet a kontroller NAT-ol. A WiFi-kliensek adat-, vezérlési és menedzsmentforgalma egyaránt átmegy a központi kontrolleren.

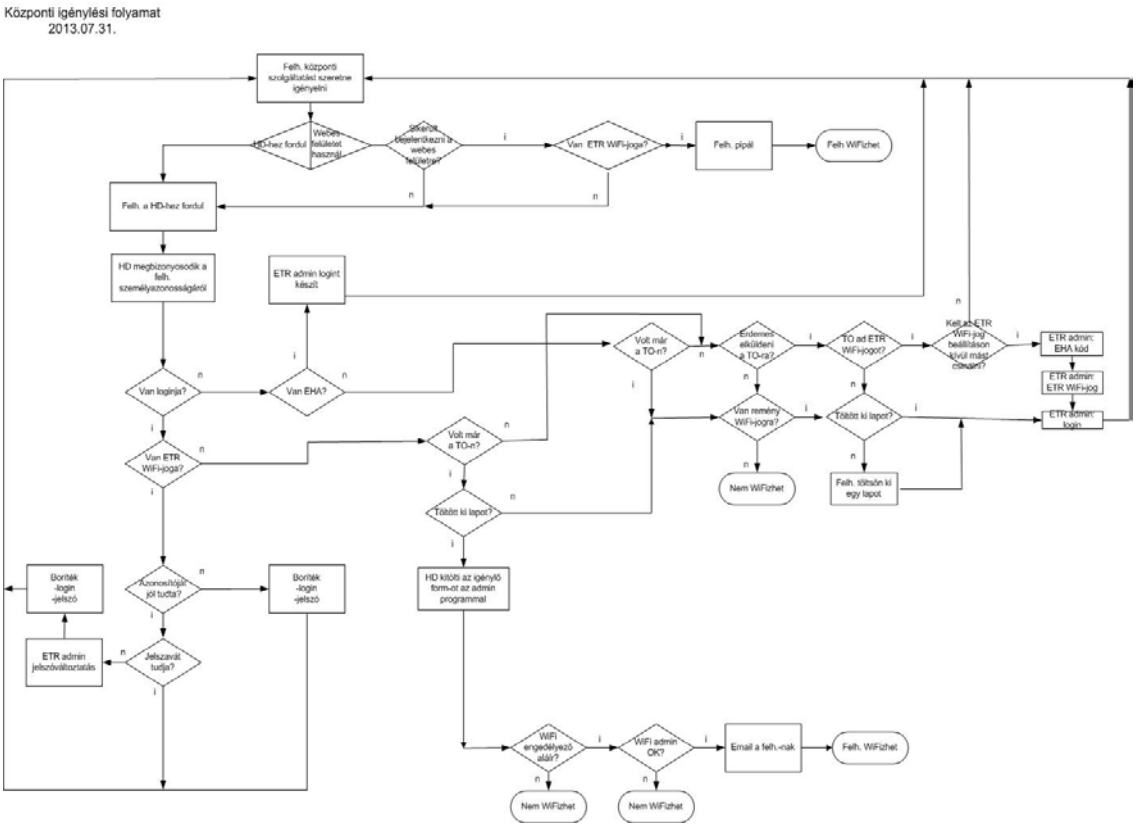
## 7.5. Információ (szte-informacio)

Ezt a szolgáltatást a fentebb felsorolt szolgáltatások használatának bemutatására használjuk. A szolgáltatást úgy hoztuk létre, hogy kizárólag csak az információs lapokat tartalmazó weboldalakat lehessen elérni. Ennek érdekében DNS-eltérítést alkalmazunk, illetve letiltottuk a WiFi-s kliensek közötti kommunikációt. A VSC-beállításoknál MTM-et állítottunk be. Így a kontroller közvetlenül routing nélkül irányítja a kliensek forgalmát az információs szolgáltatáshoz létre hozott VLAN-ba (w-info). IP-címet a webszerverre telepített DHCP oszt a WiFi-klienseknek. A DNS szerver feladatait is a webszerver látja el. Ez a DNS szerver bármilyen névfeloldási kérésre a webszerver IP-címét adja vissza. A WiFi-kliensek adat-, vezérlési és menedzsment forgalma egyaránt átmegy a központi kontrolleren.

# 8. Felhasználómenedzsment

## 8.1. Felhasználói ügymenet

### 8.1.1. Központi szolgáltatás esetén




**12. ábra** Központi szolgáltatás igénylésének folyamatábrája

A központi szolgáltatás potenciális igénylői körét alapvetően a már meglévő, aktív ETR-es felhasználói azonosítóval rendelkező felhasználók képezik. Emellett lehetőséget biztosítottunk a fenti feltételkörből kimaradt felhasználóink részére is.

**Igénylés menete**

a) Akinek van olyan ETR-loginja (ETR-es felhasználói neve) és jelszava, amellyel el tudja érni az ETR szolgáltatásait, annak csak a www.wifi.u-szeged.hu webes felületen kell igényelni a szolgáltatást.
b) Amennyiben a felhasználónak (tudomása szerint) nincs joga elérni az ETR szolgáltatásait, és/vagy nem rendelkezik ETR-loginnal, akkor benyújthat szolgáltatás igénylőlapot az ESZK Help Desk szolgálatnak (továbbiakban Help Desk). Ott a munkatársak a megadott adatok alapján megpróbálnak utánanézni, hogy az igénylőnek nincs-e mégis joga elérni az ETR szolgáltatásait, illetve hozzájuthat-e ilyen joghoz. Ha igen, akkor segítenek az elérésben, illetve a jog megszerzésében, beleértve már létező ETR-login esetén a használatbavételéhez szükséges adatok (ETR-login és/vagy jelszó) átadását, míg új igény esetén az ETR-login és jelszó létrehozását. Az ETR-logint és jelszót a Help Desk lezárt borítékban adja át (postázza). Ezután a szolgáltatás igénybevétele az korábban ismertetett módon megtörténhet.

Amennyiben a Help Desk sem tud ETR-elérési jogról, illetve nem látja lehetségesnek a megszerzését, akkor már létező ETR-login esetén átadja a felhasználónak a használatbavételéhez szükséges adatokat, míg új igény esetén az igénylőlap alapján elkészíti a belépéshez szükséges ETR-logint és jelszót. Végül megadja az igényelt WiFi-szolgáltatáshoz a jogosultságot. Az (ETR-loginból a d) pont szerint képzett) WiFi-felhasználói azonosítót és jelszót a Help Desk lezárt borítékban adja át (postázza). Az ebben az esetben a használatba vett vagy létrehozott azonosító is része az ETR azonosítási rendszerének, de – ETR-elérési jog híján – nem lehet vele hozzáférni az ETR szolgáltatásaihoz. Az így kapott ETR-loginnal is be lehet jelentkezni WiFi adminisztrációs szerverre a szolgáltatással kapcsolatos információk lekérdezése céljából, de elektronikus igénylést nem lehet kezdeményezni, ezért további jogosultságszerzés vagy a korábbiak módosítása, beleértve a jelszót is, csak a Help Desken keresztül történhet.

c) Amennyiben a felhasználónak gondja van az WiFi adminisztrációs szerverre történő belépéssel, akkor először keresse fel a Help Desket, és a munkatársak segítségével próbálja meg rendezni az elérési jogát.
d) A WiFi felhasználói azonosító a következőképpen néz ki: ETR-login@wifi.u-szeged.hu, például xyuvwzq.sze@wifi.u-szeged.hu. A jelszó pedig megegyezik az ETR belépésnél használttal. Az ETR-login az ETR elérési joggal rendelkező felhasználók nagy részénél megegyezik az EHA kóddal.

### 8.1.2. Local switching

A LAN WiFi-szolgáltatást elsősorban a Szegedi Tudományegyetem oktatói, dolgozói vehetik igénybe egyetemi feladataikkal összefüggő internetes munkavégzés céljára. A szolgáltatás igénybevételéhez szükség van egy WiFi-s azonosítóra és a hozzá tartozó jelszóra, valamint a LAN-t használó (üzemeltető) egyetemi egység jóváhagyására.

**Igénylés menete**

a) Ha felhasználónak van olyan ETR-loginja (ETR-es felhasználói neve) és jelszava, amellyel el tudja érni az ETR szolgáltatásait, valamint a használni kívánt LAN-t (pontosabban: IEEE802.1Q protokoll szerinti VLAN-t, azaz virtuális lokális hálózatot) üzemeltető egység rendelkezik helyi WiFi-adminisztrátorral, akkor a felhasználónak fel kell keresni az adminisztrátort. Az ő segítségével ki kell tölteni egy elektronikus igénylést. Ebben meg kell adni az igénylő ETR-loginját, azt az épületet, amelyben a szolgáltatást igénybe kívánja venni, valamint azt a VLAN-t, amelyhez csatlakozni kíván. Egy épületben csak egy VLAN-hoz lehet csatlakozni. A kitöltés után az ESZK-hoz kerül a kérelem. Itt jóváhagyás után a központi WiFi-adminisztrátor rögzíti a kérelem alapján a szolgáltatást. A szolgáltatás csak ezután vehető igénybe.
b) Amennyiben a felhasználónak (tudomása szerint) nincs joga elérni az ETR szolgáltatásait, vagy nem rendelkezik ETR-loginnal, vagy a használni kívánt LAN-t üzemeltető egyetemi egységnek nincs WiFi adminisztrátora, akkor nyújtson be szolgáltatás igénylőlapot az ESZK Help Desk szolgálatnak (továbbiakban Help Desk). Ott a munkatársak a megadott adatok alapján megpróbálnak utánanézni, hogy nincs-e mégis joga elérni az ETR szolgáltatásait, illetve hozzájuthat-e ilyen joghoz. Ha igen, akkor segítenek az elérésben, illetve a jog megszerzésében, beleértve már létező ETR-login esetén a használatbavételéhez szükséges adatok (ETR-login és/vagy jelszó) átadását, míg új igény esetén az ETR-login és jelszó létrehozását. Az ETR-

logint és jelszót a Help Desk lezárt borítékban adja át (postázza). Hasonlóképpen, a Help Desk leellenőrzi, hogy nincs-e mégis helyi WiFi-adminisztrátor. Ha igen, akkor ezután a szolgáltatás igénybevétele az a) pontban ismertetett módon megtörténhet.

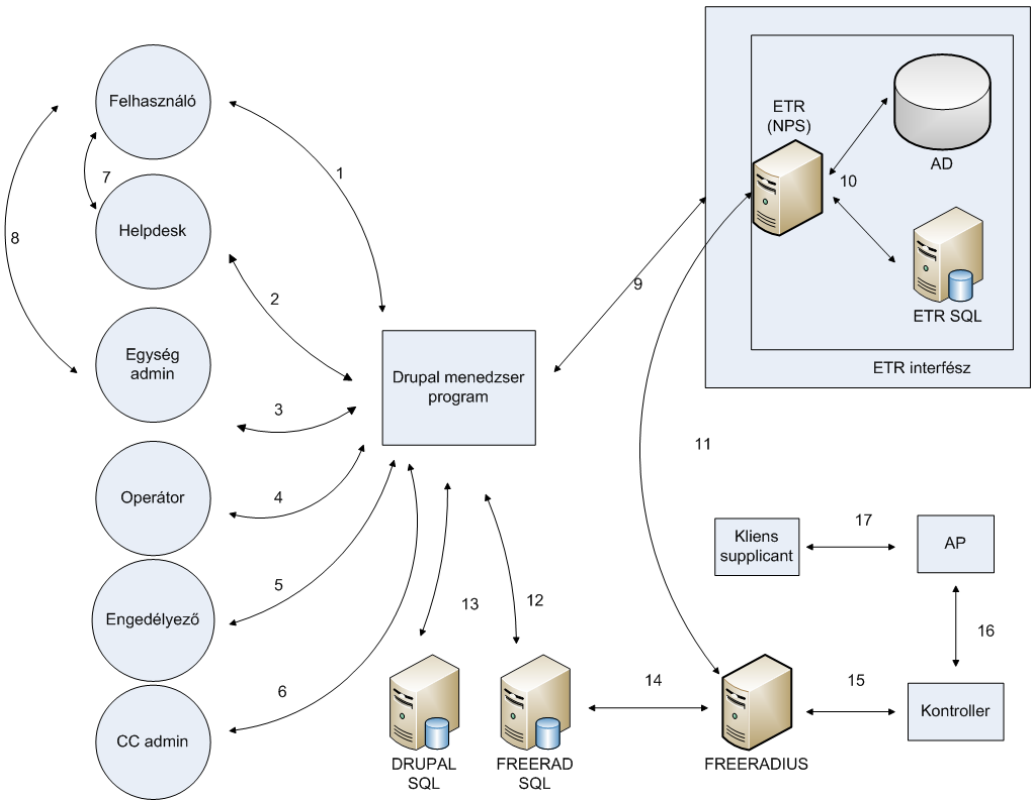
Amennyiben a Help Desk sem tud ETR elérési jogról, illetve nem látja lehetségesnek a megszerzését, vagy tényleg nincs helyi WiFi-adminisztrátor, akkor már létező ETR-login esetén átadja a felhasználónak a használatbavételéhez szükséges adatokat, míg új igény esetén az igénylőlap alapján elkészíti a belépéshez szükséges ETR-logint és jelszót. Végül megadja az igényelt WiFi-szolgáltatáshoz a jogosultságot. Az (ETR-loginból a d) pont szerint képzett) WiFi-felhasználói azonosítót és jelszót a Help Desk lezárt borítékban adja át (postázza). Az ebben az esetben használatba vett vagy létrehozott azonosító is része az ETR azonosítási rendszerének, de – ETR-elérési jog híján – nem lehet vele hozzáférni az ETR szolgáltatásaihoz. Az így kapott ETR-loginnal is be lehet jelentkezni WiFi-adminisztrációs szerverre a szolgáltatással kapcsolatos információk lekérdezése céljából, de elektronikus igénylést nem lehet kezdeményezni, ezért további jogosultságszerzés, vagy a korábbiak módosítása, beleértve a jelszót is, csak a Help Desken keresztül történhet.

c) Amennyiben a felhasználónak gondja van az WiFi adminisztrációs szerverre történő belépéssel, akkor először keresse fel a Help Desket, és a munkatársak segítségével próbálja meg rendezni az elérési jogát. Hasonlóképpen, ha az egység WiFi-s adminisztrátora – valamilyen, az ETR-loginnal összefüggő okból - nem tudja kitölteni az elektronikus igénylését, akkor először keresse fel a Help Desket, és segítségükkel próbálja meg rendezni az ETR-login státuszát.
d) A WiFi felhasználói azonosító a következőképpen néz ki: ETR-login@wifi.u-szeged.hu, például xyuvwzq.sze@wifi.u-szeged.hu. A jelszó pedig megegyezik az ETR belépésnél használttal. Az ETR-login az ETR elérési joggal rendelkező felhasználók nagy részénél megegyezik az EHA kóddal.

## 8.2. Szerepkörök

Egy adminisztrációs rendszer összeállításakor fontos szerep jut a szerepkörök kialakításának. Mivel olyan keretrendszerben implementáltuk a megoldásunkat, amely eleve támogatja a szerepkörök kialakítását, így elég áttekinteni a 13. ábrán látható jelenlegi sémát. A kialakításnál szem előtt tartottuk a szerepkörök hierarchikus felépítését. Felhasználást tekintve két nagy csoportra osztható a szerepkörök halmaza. Ezek:

- Adminisztratív szerepkörök
- Felhasználói szerepkör




**13. ábra** Az egyes szerepkörök és kapcsolataik

### 8.2.3. Adminisztratív szerepkörök

Ezen szerepkörök felhasználói végzik a rendszer integritásának fenntartását az ügymenetben meghatározottak alapján. Egyezményes elv szerint az adminisztratív csoportok tagjai ezen felhasználói entitásukkal nem vehetik igénybe a WiFi-szolgáltatásokat. A csoport tagjai a következőkből állnak:

- Adminisztráror: A WiFi-adminisztrációs rendszer legnagyobb jogkörrel bíró csoportja. Olyan alapvető feladatokat képes elvégezni, mint a levelezési cím beállítása, a rendszer kinézetének meghatározása, az ETR-interfész konfigurációs paramétereinek beállításai, a frissítés elvégzése, az alárendelt szerepkörök tagjainak kinevezése.
- Engedélyező: A papíralapú igénylési folyamatok fontos résztvevője. Engedélyezheti vagy elutasíthatja a bejövő igényt a benyújtott személyes adatok alapján.
- CC admin: Szerepet kap a local switching rendszer üzemeltetésében. Konfigurációs jogkörrel bír a bővülő local swtiching rendszer integritásának megőrzésében, az AP-k, épületek, szervezeti egységek beállításában, összerendelésében.
- Egység admin: Fontos entitás a local switching igénylések megindítása szempontjából. Ez a szereplőtípus végzi el az egységi igények feldolgozását és humán erőforrásként előautorizálást is végez a saját intézményi policynak megfelelően, majd továbbítja a felhasználói igényt elektronikus formában a menedzser programon keresztül.
- Operátor: Karbantartási hírek feladója, ami hagyományosan operátori tevékenységek közé tartozik.

### 8.2.4. Felhasználói szerepkör

- Felhasználó: A WiFi-rendszer végfelhasználója. Joga van önregisztráció keretében központi szolgáltatásokat igényelni. Feliratkozhat hírlevelekre, megtekintési joggal rendelkezik saját bejelentkezési és korlátozási adatai felett.

## 8.3. Megvalósítás

Egy komplex rendszer megvalósításához szilárd alap szükséges. A célkitűzések között szerepelt a webes interfész, a könnyű karbantarthatóság, az igény szerinti bővítés lehetősége, a jogosultsági rendszer megléte, a levélküldés biztosítása és a folyamatautomatizálás lehetősége. Ezért választottuk a Drupalt mint keretrendszert, annak is a 7-es főverzióját.

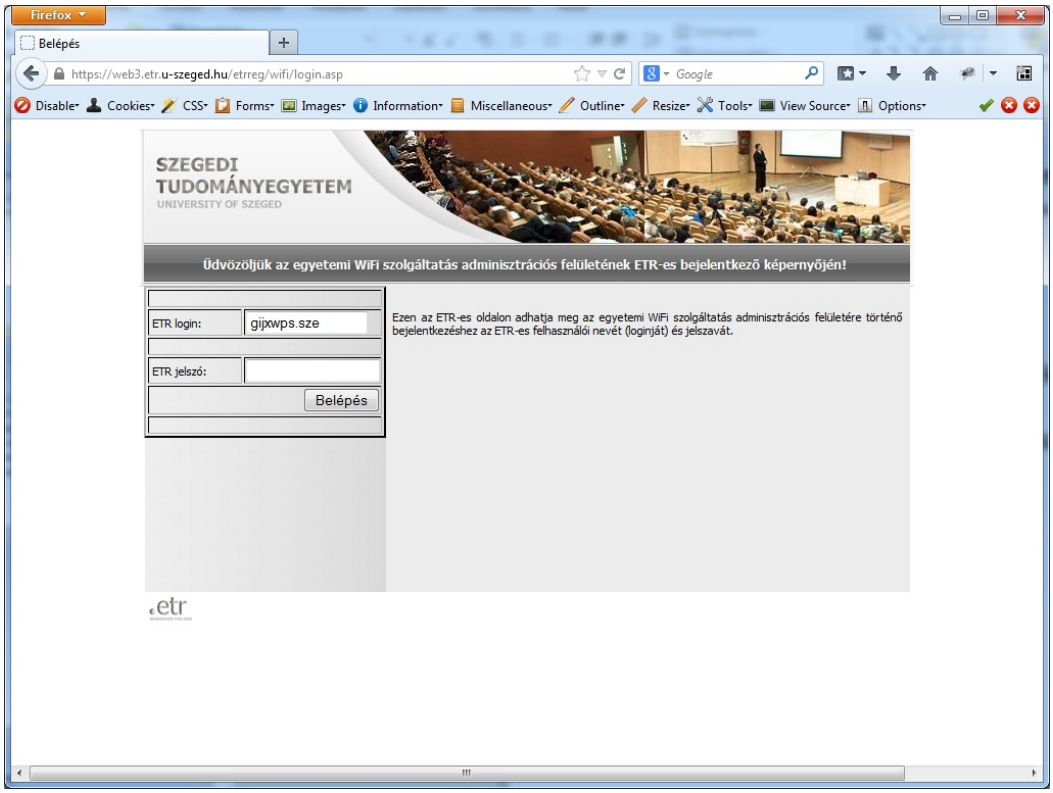
### 8.3.1. Moduláris felépítés

A legvonzóbb tulajdonsága a Drupalnak talán a moduláris felépítésben rejlik. Tervezési minták használatával levetővé teszi az egyéni funkcionalitások implementálását viszonylag rövid idő alatt. Ezt használtuk ki a rendszer tervezése során. Az alap konfigurációval kapunk számos hasznos modult, úgy, mint pl. a User modul. Ezzel jár olyan moduláris jogosultsági rendszert is, melyre már lehet alapozni. Ezen core-modulok mellett az open source közösség által rendelkezésre bocsátott ún. contrib-modulokat is felhasználtunk a projekt megvalósítása során, melyek jó szolgálatot tesznek pl. a levélküldés vagy éppen az automatizálás során. Természetesen számos problémára kellett egyéni megoldásokat kifejleszteni, ezek során megszületett a kb. 20 egyéni modul is.

### 8.3.2. ETR-interfész

Kulcsfontosságú volt ennek a problémának a megoldása már a tervezési fázistól kezdve. Alkalmazkodni kellett a már meglevő tanulmányi rendszerhez a biztonsági szempontokat szem előtt tartva. Így került kifejlesztésre az ETRAuth nevű egyéni modulunk, mely lehetőséget biztosít a felhasználói adatok egyirányú áramlására és autentikációjára a jelszavak kiszolgáltatása nélkül.

Az interfész az azt hívó alkalmazáson kívüli, az on-line bankkártya-fizetési felületekhez hasonlóan független, black box rendszerű, webböngészővel elérhető entitás. Ennek megfelelően az interfész az őt hívó alkalmazást egy preautentikációs (autentikáció előtti) és egy posztautentikációs (autentikáció utáni) szegmensre bontja. A két szegmens fizikailag lehet ugyanaz a kód, ha a (pl. paraméterszignatúrában) eltérő belépési pontokat biztosít.




**14. ábra Az** ETR WiFi-autentikációs bejelentkező felülete

### 8.3.3. Adattárolási, mentési technikák

Az autorizációs rendszert, amely egy FreeRADIUS párból áll, MySQL back-endek szolgálják ki. Mivel a legtöbb fontosnak ítélt komponenst megkettőztük, így az autorizációs adatbázisainknál is erre törekedtünk. A magas rendelkezésre állás nyomott többet a latban, ezért választottuk a master-master replikában való üzemeltetésüket. Ugyanakkor a Drupal adminisztrációs rendszert a kisebb tervezett igénybevétele miatt egyelőre nem tartalékoltuk, a szerverkonszolidációban kivitelezett virtuális felhőszolgáltatás által nyújtott biztonság megfelelő szintet képvisel. A rendszer biztonsága érdekében egyéb óvintézkedéseket is foganatosítottunk. Ezek közé tartozik az adatbázisok és konfigurációk időközönkénti kimentése és szalagra tárolása is. Ennek keretében mentésre kerülnek többek között az autorizációs adatbázisaink, a Drupal-rendszer konfigurációs adatbázisa, a FreeRADIUS konfigurációk és egyéb segédszkriptek.

### 8.3.4. Felhasználói jogosultság kezelése

Mivel egy tanulmányi rendszer állandóan változó állapotokat tükröz, az általunk hozott felhasználási policy kapcsán szükségessé vált a jogosultságok követése, szinkronizálása a tanulmányi rendszerbeli állapotokkal. Erre szolgálnak többek között az időzített karbantartó folyamatok, a bejelentkezéskor kiváltott eljárások. Ezek biztosítják a háttérből, hogy a megfelelő feltételek fennállása esetén legyen a felhasználóknak joga használni a WiFi-rendszerünket.

Ellenőrzésre kerül a WiFi supplicanttal történő bejelentkezés folyamán a felhasználói azonosítókhoz tartozó nyitott sessionök száma, melyet felhasználónként két példányban korlátoztunk, azonban egyedi modullal megteremtettük a lehetőséget az irányszámtól való egyéni eltérésre is.

### 8.3.5. Local switching

A dinamikus VLAN-hozzárendelés elvégzését megkönnyítendő került kifejlesztésre a local switching modulcsomag, a lswman modulok és segédmoduljaik. Fontos megemlíteni ismételten, hogy ennél a fajta megközelítésnél az egységadminisztrátoroknak delegáltuk az igénylési folyamat megindításának jogát. Itt tulajdonképpen nem történik más, mint egy végfelhasználó, felhasználási hely (épület) és egy VLAN összerendelése. Ehhez az egységadminisztrátorok minimális segítséget kapnak az igénylő űrlapon egy Ajax-mechanizmus által, amely gondoskodik arról, hogy érvényes épület-tanszék-VLAN hármasok legyenek rögzítve a benyújtott igényben.

Az igénylések legfeljebb egy éves lejárati időtartammal nyújthatók be, ez a tény az űrlap beadásakor validálásra kerül.

Ezt követően a beküldött igények felülvizsgálatra várnak. Első lépcsőben lehetőség van az engedélyezőnek az elfogadásra vagy az azonnali visszautasításra. Az engedélyezett igényeket egy második lépcsőben is el kell fogadni ahhoz, hogy az igény által rögzített adatokkal érvényes bejegyzés jöjjön létre a FreeRADIUS autorizációs adatbázisában.

Igény elfogadásakor a végfelhasználó számára emailértesítőt is generál a rendszer, így tájékoztatást kap a szolgáltatás alapvető paramétereiről.

### 8.3.6. Korlátozások

A tervezés során számításba vettük, hogy előfordulhatnak a rendszer performanciájának romlását előidéző állapotok, illetve jogi korlátok. Ezen határokat átlépő felhasználók elérési jogának korlátozására ezért kidolgoztunk egy rendszert. Amennyiben a felhasználó megszegi az „SZTE Számítógépes Infrastruktúra Szabályzatában” foglaltakat, a felhasználónak nyújtott szolgáltatások korlátozására kerülhet sor. A központi WiFi-szolgáltatás esetén különböző büntetési kategóriák léteznek, melyek az elérhető IP-címek és szolgáltatások, illetve a sávszélesség vonatkozásában korlátozhatják a szankcionált felhasználót, beleértve a letiltást is. Egy felhasználó számára több korlátozást is ki lehet osztani, melyek időben átfedhetik egymást. Mindig az aktuális időpontban érvényes legszigorúbb korlátozási tétel kerül kiválasztásra az adott felhasználó által igénybe venni kívánt szolgáltatáshoz. A korlátozások a WiFi adminisztrációs felület adatbázisában tárolódnak, illetve megőrződnek, így mind az aktuális állapot, mind a korlátozási előzmények megtekinthetők a tételekhez tartozó rövid leírással, melyet a felhasználó is nyomon követhet a WiFi adminisztrációs szerver megfelelő lapján.

A korlátozás LAN-elérés esetén a szolgáltatás időszakos felfüggesztését jelenti. Ez tarthat néhány napig, de súlyos esetben akár végleges is lehet. Ezen kívül a LAN üzemeltetője szankcionálási vagy biztonsági céllal az elérhető IP-címek és szolgáltatások, illetve a sávszélesség vonatkozásában korlátozhatja a felhasználó forgalmát.

Technika megvalósításnál az ötletet egy hasonló felépítésű modul adta, mely egy szállodai szobafoglaló rendszer volt. A korlátozások esetén is tulajdonképpen foglalásokat teszünk korlátozási elemekre, de esetünkben az átfedés is megengedett.

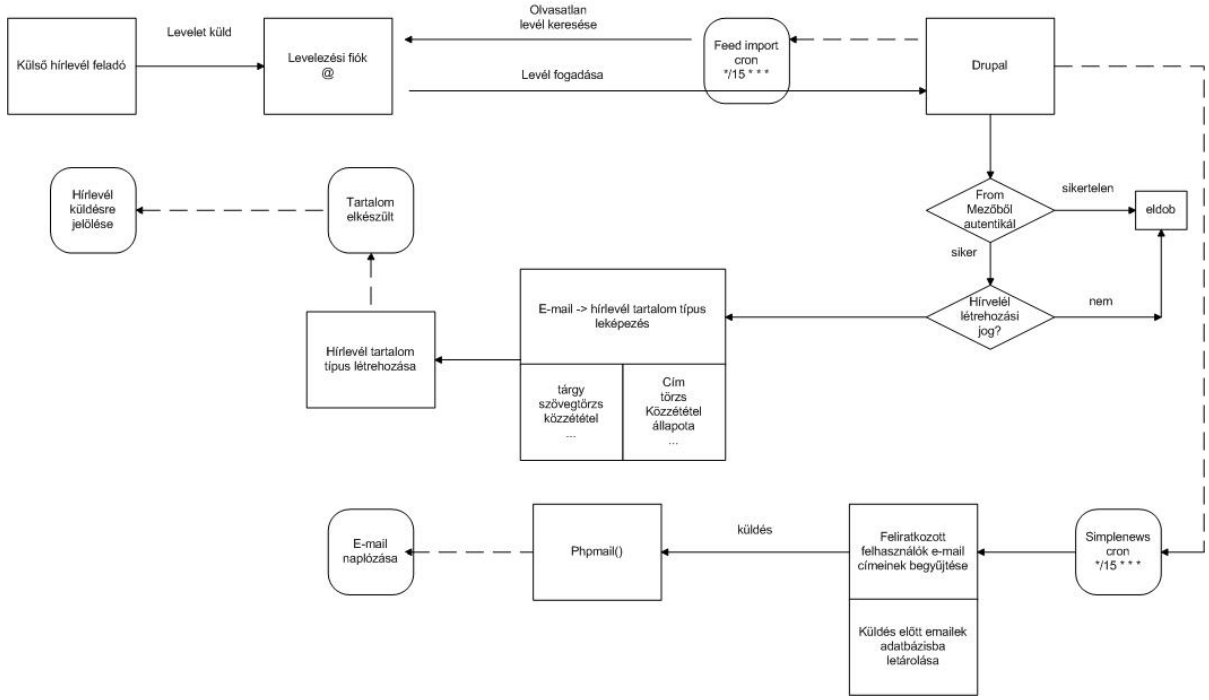
A FreeRADIUS számára ténylegesen értelmezhető korlátozástípust a háttérben futó cron folyamat végzi, mely a korlátozásokhoz rendelt prioritási szintek és a kezdeti, illetve a lejárati dátumok alapján elvégzi az alkalmazáslogikát is, így a FreeRADIUS

szervernek mindig csak legfeljebb egy korlátozást kell feldolgoznia és alkalmaznia felhasználónként.

### 8.3.7. Levélküldés, hírlevél

Fontosnak tartottuk a felhasználók tájékoztatásának megoldását is, így a legtöbb lényegi változásról emailben értesítjük őket. A jogosultságváltozásokról (igénylés, lemondás) a felhasználók automatikus emailüzenetet kapnak a megadott emailcímükre. Amennyiben ETR-elérési joguk van, úgy az ETR-ben megadott emailcímre küldjük az üzenetet, egyéb azonosító esetében az igénylőlapon megadott emailcímre. Az email tartalmazza az érintett szolgáltatás paramétereit, illetve a változást. A központi mailszerverek felesleges leterhelésének elkerülése és az alapvető tájékoztatás biztosítása végett a következő szabályozást hoztuk az emailcímekkel kapcsolatban. Ha az igénylés után a felhasználó ezt a címet kitörli, és nem ír helyette másikat, akkor az igényelt szolgáltatáshoz való hozzáférését felfüggesztjük. A másik ilyen megkötés, miszerint ha egy megadott emailcím elérhetőségét illetően kétség merül fel, amit például egy bounced mail is alátámaszt, akkor az adminisztráció fenntartja a jogot a felhasználó szolgáltatásainak időleges szüneteltetésére a probléma rendezéséig.

A korlátozások érvényre jutásakor is generálunk emailértesítőt, hogy megkönnyítsük a Help Desk munkáját a panaszos ügyek okának mihamarabbi kiderítése végett.




**15. ábra** A hírlevélküldés folyamata

Általános üzemeltetési információk terjesztésére a hírlevelet választottuk terjesztő médiának. Technikailag két megvalósítás fonódott össze. A WiFi adminisztrációs szerverre elérési joggal rendelkező felhasználóknak lehetőségük van ún. pipálással feliratkozni a hírlevélre, illetve leiratkozni a hírlevélről. A másik esetben egy hagyományos mailman típusú moderált levelezési listára lehet feliratkozni minden potenciális érdeklődőnek: mind az előbbi eset felhasználóinak, mind azoknak, akik elérési joggal nem rendelkeznek a WiFi adminisztrációs szerverre.

A hagyományos mailman típusú lista és a Drupal-hírlevél összekapcsolását sikerült megoldani. Így lehetővé vált, hogy a mailman típusú listára történő hírlevelet a Drupal rendszer is befogadja és továbbítsa a felhasználói közösségnek autentikáció és autorizáció után, elkerülve a nem kívánt tartalmak bekerülését a hírfolyamba.

### 8.3.8. Karbantartó időzített folyamatok

Ahhoz, hogy biztosítsuk a rendszer megfelelő működését, vannak folyamatok, amelyeket hatékonyabb a háttérben végezni, így ezek időzített feladatokként kerülnek végrehajtásra. Mindehhez nyújt hathatós segítséget a Drupal cron API-ja és az olyan ráépülő contrib-modulok, mint az Elysia Cron.

Az időzített folyamatok egyrészt karbantartást végeznek, míg másik feladatuk a felhasználókkal történő kommunikáció segítése, azaz a levelezés egy részének lebonyolítása.

A karbantartáshoz tartozik elsődlegesen az ETR-jogosultsággal rendelkező felhasználók WiFi-szolgáltatási jogának rendszeres ellenőrzése, szükség esetén a használati jog felfüggesztése, például ha a felhasználó ETR-státuszában olyan változás áll be, mely megszüntetheti a WiFi-jogosultságát. Az emailcím tekintetében bevezetett szabályozás értelmében ilyenkor kerülhet ideiglenes felfüggesztésre a WiFi-jog, amennyiben a felhasználó kitörli emailcímét az ETR nyilvántartásból.

A korlátozások aggregálása és súlyozása után szintén az időzített feladatban fordulnak le a korlátozások halmazából képzett bejegyzések a FreeRADIUS számára is értelmezhető, felhasználónként legfeljebb egy bejegyzésé.

Ellenőrzésre kerül időről időre az igényelt szolgáltatások lejárati ideje is, melynek közeledtét szintén email útján jelezzük.

A hírlevél kiküldése jól kezelhető csoportosítva, ez a modul is rendelkezik ilyen képességekkel. A nap folyamán háromszor kerül ellenőrzésre, hogy vannak-e várakozó üzenetek. Itt kell megemlíteni a hagyományos mailman típusú listával való kapcsolatot is. Periodikusan ellenőrzi a megoldás, hogy a mailman típusú listára érkezett-e üzenet, melyet továbbítani lehet a hírlevél modulnak feldolgozásra. Ezt a feladatot a Feeds importer modulok látják el.

## 8.4. Felhasználói interfészek

Többféle megközelítést lehetett volna alkalmazni a felhasználói felületek megtervezésekor. Mi a felhasználói szerepkörök erősségével bővülő funkcionalitású interfészek mellett döntöttünk. Ezért bizonyos funkciók megjelenítésében nincs különbség a leggyengébb és a legerősebb felhasználói szerepkör nézetében.

A webes megjelenítésnél fontosnak tartottuk az egyre inkább előtérbe kerülő mobil kliensek támogatását is. Ezért a felületek tervezése során domináltak a reszponzív megjelenítő technikák is.

### 8.4.1. Adminisztratív felületek

Az adminisztratív felületek szerepkörönként eltérő arculattal és funkcionalitással bírnak. A legbővebb lehetőségei az oldal adminisztrátorának vannak. Itt van lehetőség az elektronikus és papíralapú igénylések adminisztrációjára. Korlátozásokat lehet alkalmazni, tanszéki adminisztrátorok nevezhetők ki, módosítható az általuk menedzselt részegységek köre. Itt lehet kezdeményezni manuális felhasználói adatimportot az ETR rendszerből EHA kód alapján.

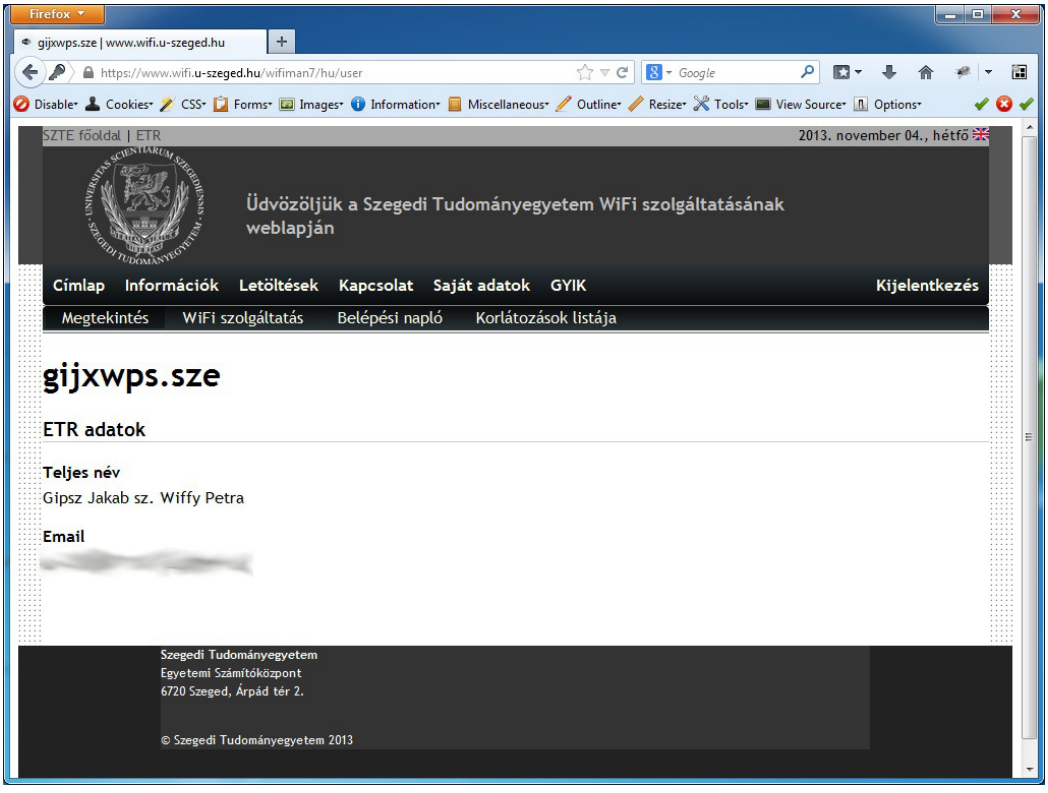
Az adminisztrátorainkkal ellentétben a felhasználóknak a Drupal keretrendszerben biztosítunk lehetőséget jelszavuk megváltoztatására az alapértelmezett felületeket kikerülve, testreszabott megoldás segítségével.

Fontos különbség, hogy amíg a WiFi-felhasználók csak egy példányban lehetnek bejelentkezve az adminisztrációs felületre, addig az adminisztrátoroknak megengedtük a szimultán bejelentkezést legfeljebb két példányban.

### 8.4.2. Végfelhasználói felület

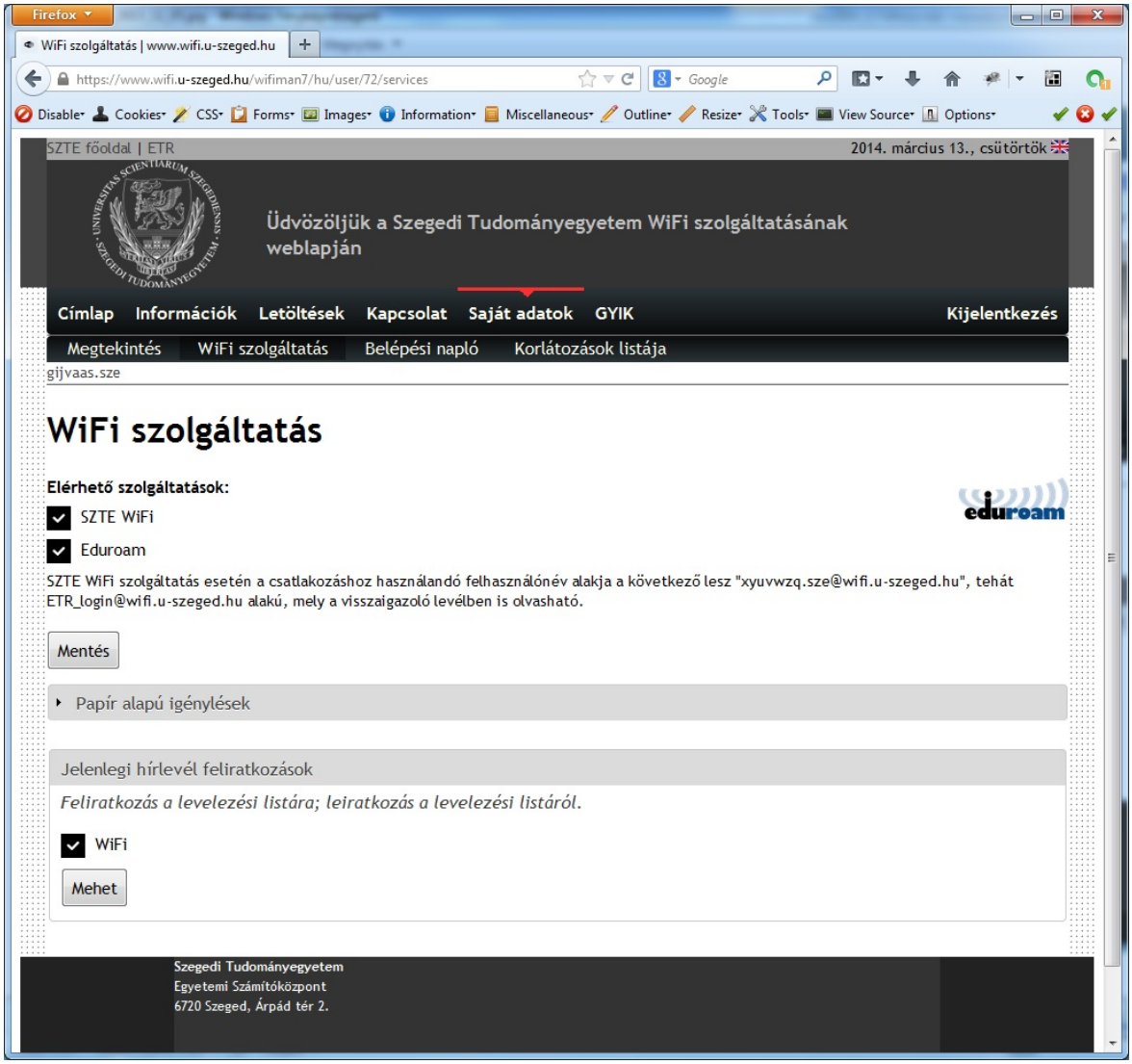
A felhasználó egy leegyszerűsített interfészt kap. A WiFi-szolgáltatás nyitóoldalán van lehetősége bejelentkezni az ETR-interfész használatával a fentebb már említett módon. Miután ez megtörtént, négy alapvető oldallal találkozhat a felhasználó. Első alkalommal, még mielőtt ténylegesen használatba vehetné az oldalt, egy egyszerű tutorialt tekinthet meg, melyben ismertetjük az oldal alapvető használatát az egyes fülek funkcióinak rövid magyarázatával. Ezt a Drupal Context moduljával karöltve a Joyride modul segítségével valósítottuk meg.

A „Megtekintés” lap tartalmazza a személyes adatait, melyek az ETR-ből származnak, valamint ellenőrizheti, hogy feliratkozott-e korábban hírlevélre, illetve a kapcsolódó link segítségével meg is tekintheti az összes hírlevél tartalmát, tehát még azon tartalmakat is amelyek a feliratkozása előtt kerültek publikálásra a listán. Mivel ez az első oldal, amivel találkozni fog, itt tüntettük fel, ha az emailcímét elérhetetlennek ítéltük meg, és emiatt korlátoztuk az igényelt szolgáltatásainak elérési jogosultságát.



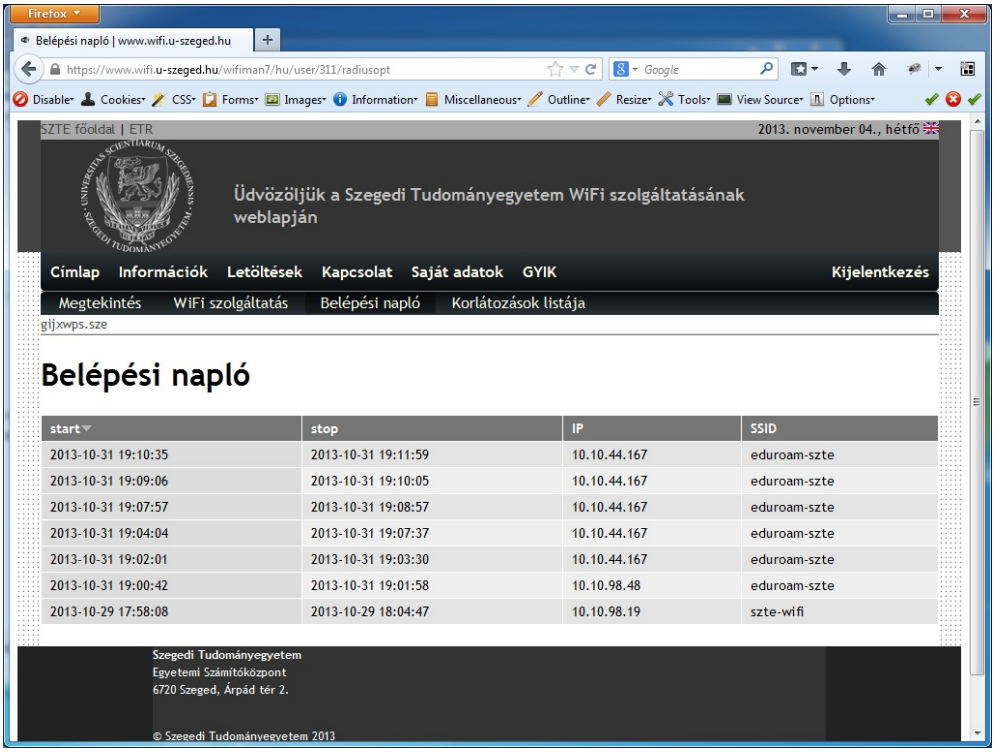

**16. ábra** Felhasználói felület „Megtekintés” oldala

A következő oldalon, melyet „WiFi szolgáltatás”-nak hívunk, igényelhet szolgáltatásokat önregisztráció alapján, tehát „pipálhat”. Valamint lehetősége van megtekinteni a papíralapú központi szolgáltatás igényeit, és itt jelölheti be a levelezési listára történő fel-, illetve leiratkozást.



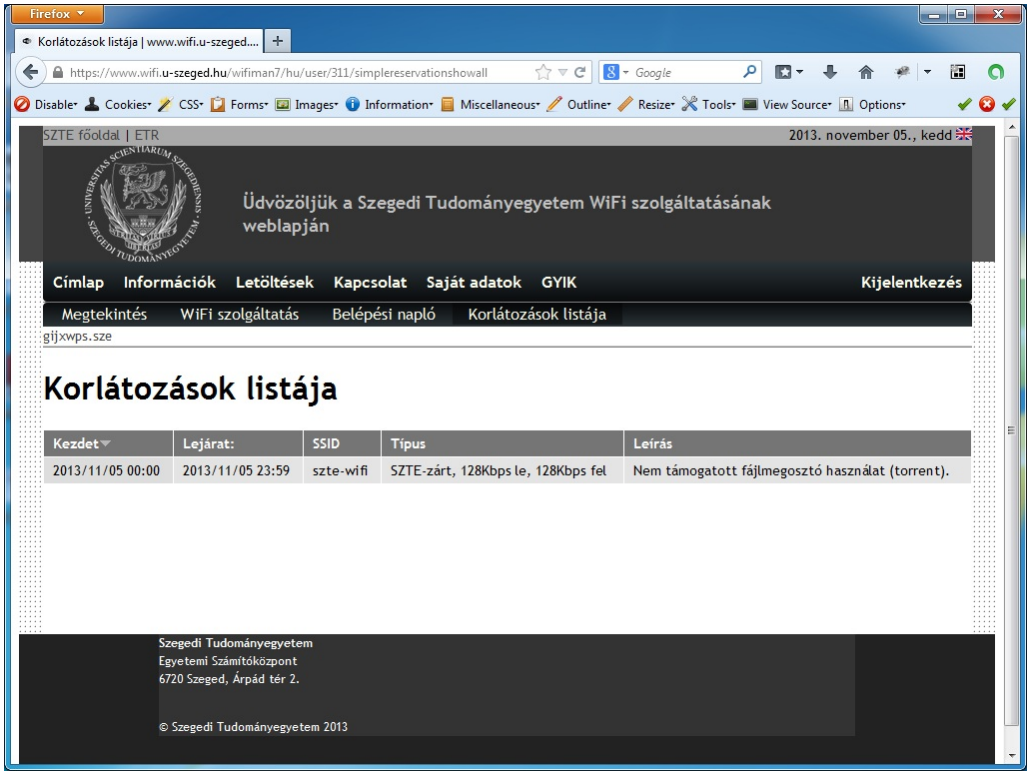

**17. ábra** Felhasználói felület „WiFi szolgáltatás” oldala

A következő oldal neve „Belépési napló”. Ez az a hely, ahol lehetősége van megtekinteni a felhasználónak, hogy WiFi-képes klienseivel mikor jelentkezett fel a hálózatra, és mely SSID-vel milyen IP-címet kapott. Ez alapvető diagnosztikai információt adhat a kapcsolat kiépültéről.




**18. ábra** Felhasználói felület „Belépési napló” oldala

Az utolsó elérhető lap a „Korlátozások listája”, ahol megtekinthető a korlátozás oka, lejárati ideje és a megszorított szolgáltatás, amennyiben vannak ilyenek. Amellett, hogy emailértesítést kap a felhasználó, annak el nem olvasása esetén ezen a módon is értesülhet az őt érintő állapotokról.



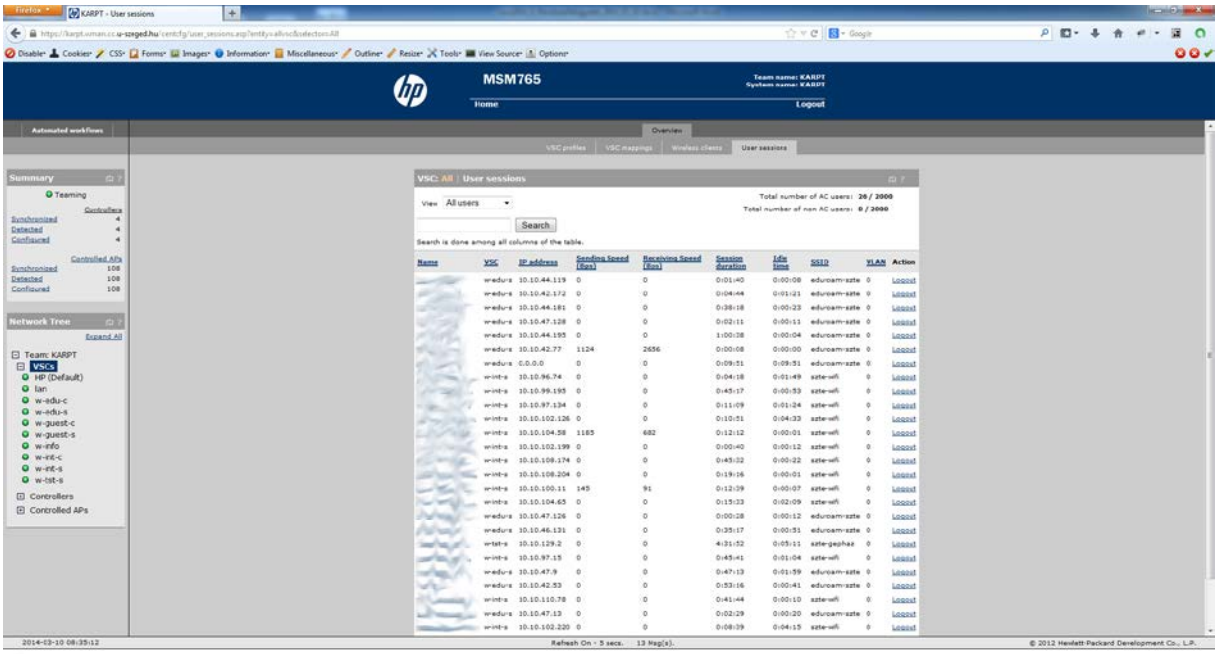

**19. ábra** Felhasználói felület „Korlátozások listája” oldal

# 9. Rendszerfelügyelet

## 9.1. Kontroller felület

Az MSM kontrollerek menedzselésére a HP lehetőséget biztosít webes felületen keresztül is. A konfigurációs beállítások és a konfigurációs fa összetettsége miatt mi is a webes menedzsment mellett döntöttünk. A rendszer működéséhez szükséges beállításokon túl a felhasználómenedzsmenthez használjuk.

Lehetőség van lekérdezni szolgáltatásonként a kapcsolatok számát, minőségét, lebonthatók a felhasználói sessionök. Számunkra legfontosabb a VSC áttekintő oldalainak használata, ahol lehetőség nyílik felhasználói sessionök megszüntetésére esetleges beragadások vagy azonnali korlátozások alkalmazásakor, mivel ez utóbbiak aktiválási helye az AA-folyamatban helyezkedik el, amely a bejelentkezés szerves részét képezi.




**20. ábra** MSM765 kezelő felülete

## 9.2. Konzolszkriptek

A diagnosztika alappillérének a karakteres módú konzolt választottuk, mivel a legtöbb távoli környezetből viszonylag egyszerűen és megbízhatóan elérhető.

A régebbi szolgáltatói múlt (SZTE otthoni internet) nyújtotta az alapot a diagnosztikai szkriptek funkcionalitásához.

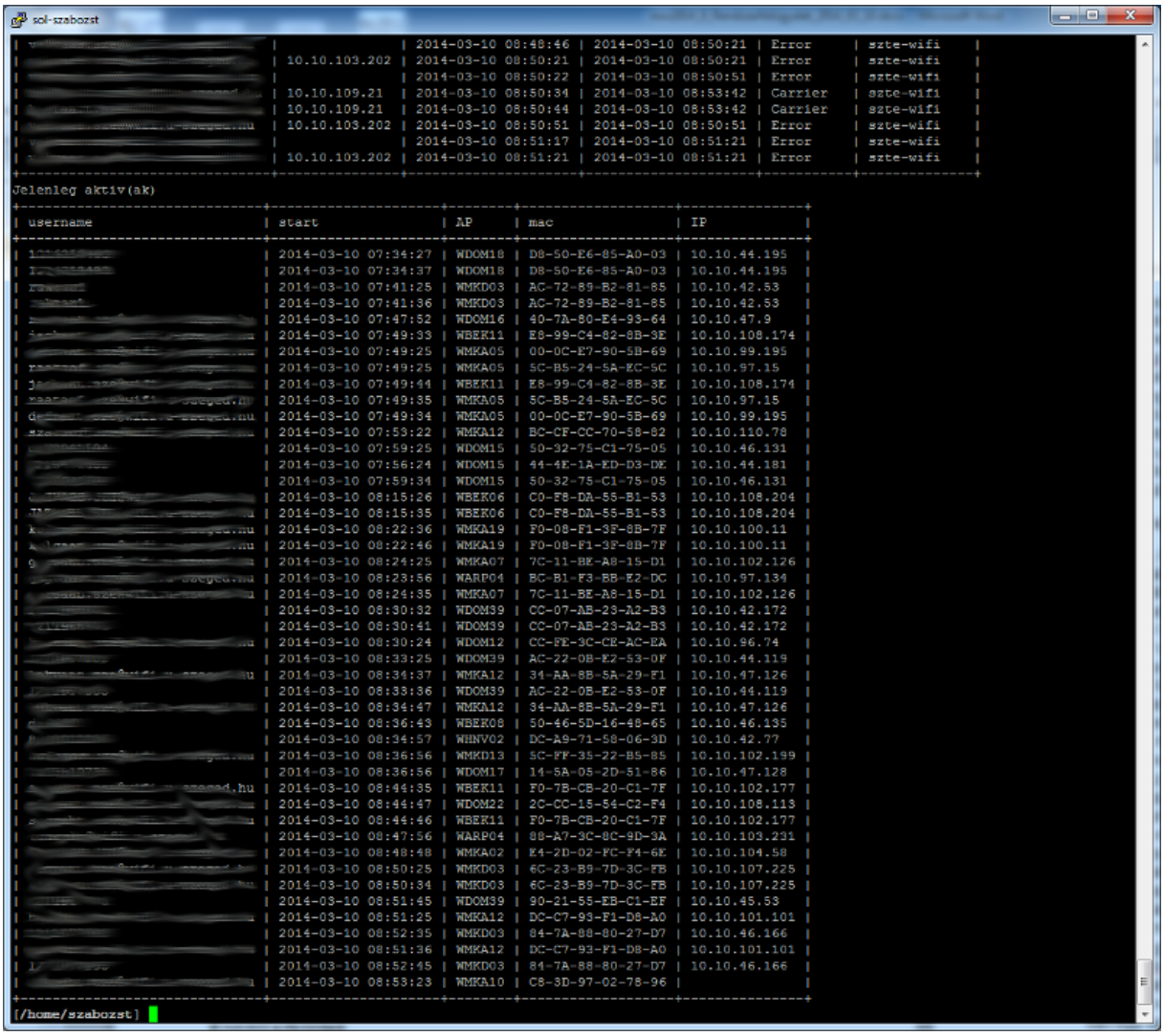
Vannak a végpontok kapcsolatát ellenőrző és a felhasználói kapcsolatok információit kinyerő szkriptek.

**A végpontokat ellenőrzőhöz tartoznak a következők:**

- wifip: Egyszerű menüpont-választásos ping, melyben a végponti WiFi-szolgáltató eszközök, AP-k státusza csoportonként, illetve egyszerre lekérdezhető. Manuálisan indítható lekérdezés.
- wificontrol: A funkcionalitást tekintve a wifip párja. Egy Java-alkalmazás, amely az AP-k jelenlétét ellenőrzi 15 perces periódusokban. Mindig a jelenlegi és az azt megelőző vizsgálat eredményéből hoz döntést. Amennyiben a két időpont

között az eszköz elérhetőségében változás áll be, úgy emailt küld a karbantartásnak a változás tényét közölve. Automatikusan, időzítve fut.

- wifiinfo: A wificontrol előző futásának eredményét kérhetjük le segítségével egy lista formájában. Elöl találhatók az elérhetetlen eszközök, mögötte a felsorolásban az elérhetők. Manuálisan indítható lekérdezés.

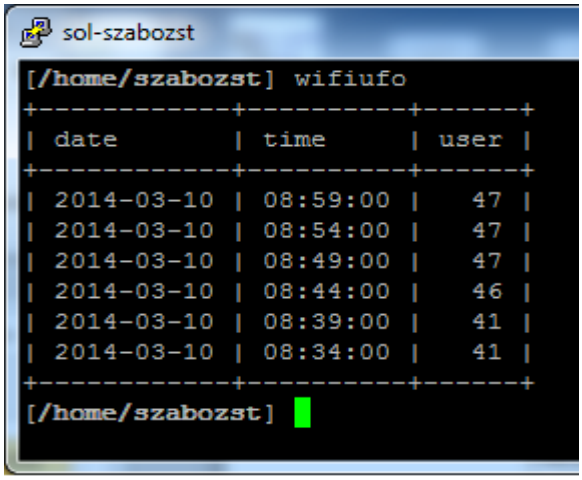



**21. ábra** Konzolszkriptek

**A felhasználói kapcsolatok elemzésére az alábbiak használhatók:**

- wifiusers: Alapértelmezésben, paraméter nélkül az adott napon történt felhasználói tevékenységet mutatja. Egy paramétere lehet, egy korábbi időpont, dátum vagy relatív formában a napok számának negatív értéke. Ebből a listából megtudható, hogy egy felhasználói azonosítóval mely SSID-hez mikor létesítettek kapcsolatot, mikor bontották le, milyen indokkal és milyen IP-címet kapott az eszköz, amelyről a kapcsolatot kezdeményezték. Ezt a felsorolást követi az aktuálisan bejelentkezett felhasználók listája, amelyből látható, hogy a felhasználói azonosítókkal mikor kezdték meg a használatot, milyen MAC-címről, milyen IP-címen. Fontos különbség az előző listával szemben, hogy itt egy becsült helyrajzi információt is találunk, mert visszakapjuk a csatlakozáshoz használt AP nevét is, amely a kialakult nomenklatúrának köszönhetően helyrajzi információt is tartalmaz.

- wifiusr: Ezzel a szkripttel nyerhetők ki a konkrét felhasználói azonosítóhoz kapcsolódó forgalmi adatok. Formája hasonló a wifiusers által visszaadott felsoroláshoz, azonban megjelennek a le- és feltöltési irányok forgalmi adatai is. Az AA-rendszer sajátosságaiból fakad, hogy a hosszabb WiFi-használatok is feldarabolódnak kisebb sessionökre. Ennek kényelmesebb, felhasználóbarát formában való megjelenítésére lehetőség van egy kapcsoló használatával. Ilyenkor a szkript megpróbálja „kiszórni" a rövid szüneteket a felhasználó számára egyébként transzparens újraautentikációk között, összegezni az időket és számlálókat, ezáltal téve tömörebbé a listázást.
- wifiufo: Egyszerű statisztika, amelyből gyors áttekintést kaphatunk a konkurrens felhasználók számáról fél óránkénti bontásban. Paraméter nélkül az utolsó fél óra statisztikája látható 5 perces intervallumonként. Paraméterezve legfeljebb egy nap tehát 48 fél óra eseményei tekinthetők meg. Lehetőség van egy kapcsolóval karakteres grafikon formájában történő



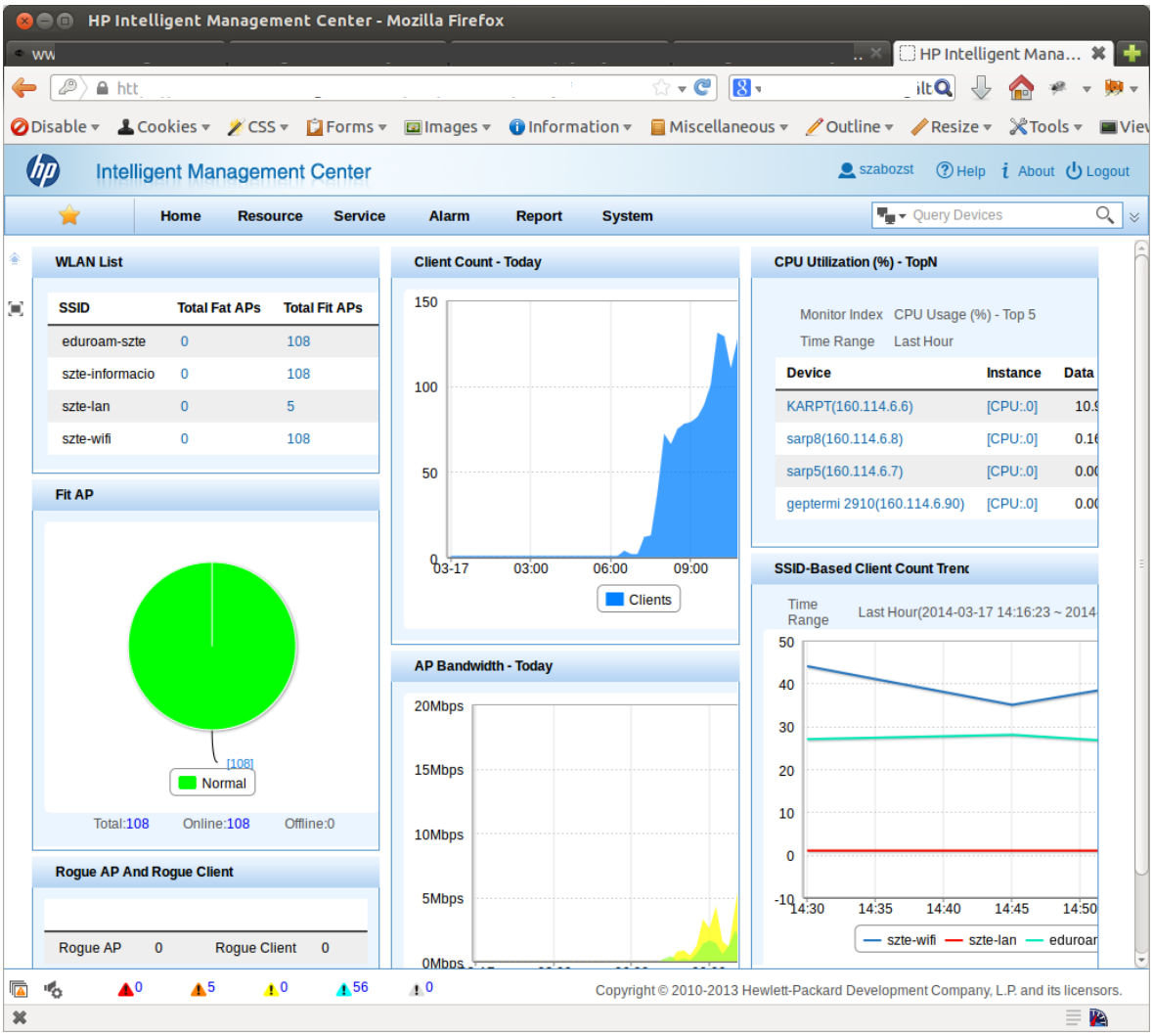

**22. ábra** wifiufo kimenete

ábrázolásra is.

## 9.3. Menedzserszoftver

A komplex felügyeleti megoldásnak eredendően a HP PCM+ 4-es verziójú szoftverét választottuk. Azonban a szoftver életútjában bekövetkezett változások miatt (hamar end of life státuszúvá változott) kellett váltanunk az iMC szoftvercsaládra kiegészítve a WSM és location function modulokkal. Ezek segítségével lehetővé vált a központosított konfigurációmentés, auditálás, forgalmi statisztikák lekérése, komplex eszközmenedzsment.

Ez a szoftver szolgál a konfigurációmentésre és változáskövetés elemzésére.




**23. ábra Az** iMC kezelőfelülete

## 9.4. Tesztrendszer és monitorozás

Az MSM firmware-k új kiadásainak tesztelése nagy hangsúlyt kapott a különféle új feature-ök megjelenésével, mivel előfordultak olyan kiadások, melyek nem voltak kompatibilisek a rendszerünk kialakításával.

Erre a célra elkészült egy tesztteamrendszer terv, mely alapján megtörténik a tesztteam kialakítása minden tesztelni kívánt firmware kipróbálása előtt. Ez a megközelítés sem képes azonban teljes lefedettséget biztosítani az esetlegesen előforduló komplikációk kitesztelésére.

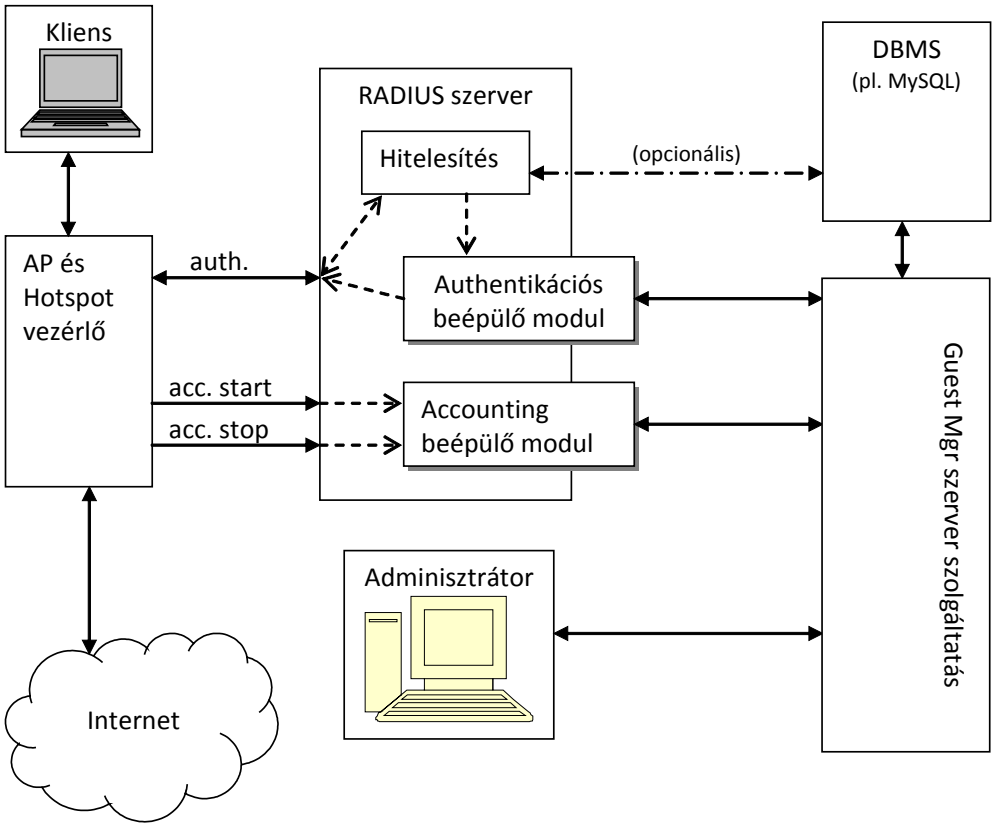
Ezért készült el a produkciós rendszer funkcionális monitorozására szolgáló megoldásunk, mely periodikusan próbál fel-, illetve lekapcsolódni a WiFi-rendszerhez, valamint forgalmat generálni, ezzel szimulálva egy átlagos felhasználói klienst. Amennyiben nem sikerül ezt végrehajtani, úgy értesítést küld a megfelelő körökbe, hogy mielőbb elháríthassuk a zavart.

# 10. Az SCIBILL Guest Manager

## 10.1. A szoftver bemutatása

Sok külső személy szabályozott és ellenőrzött internet elérésének biztosításához (pl. konferencia esetén) mindenképpen szükség van egy olyan eszközre, amely gyorsan és hatékonyan képes biztosítani tetszőleges számú felhasználó számára az előre meghatározott jogosultságú hozzáférést. Az alkalmazás, amelyet az SCI-Network zRt. fejlesztett ki a Szegedi Tudományegyetem számára, hasznos eszköz az ideiglenes WiFi-kliensek jelszavainak előállításához, amelyekkel a felhasználók térben, időben, illetve időtartamban ellenőrzötten hozzáférhetnek az egyetemi hálózat számukra engedélyezett erőforrásaihoz. A rendszer a hozzáférés engedélyezéséhez szükséges azonosítók és jogosultságok legyártásán túl gondoskodik ezen jogosultságok betartásáról, valamint azok automatikus megszüntetéséről is, megelőzve ezzel a hálózat esetleges későbbi sebezhetőségét. A rendszer a HP Networking MSM sorozatú kontrollereire készült, de moduláris felépítése lehetővé teszi más gyártók eszközeihez a hasonló együttműködés biztosítására fejlesztett modulok illesztését. A rendszer magyar nyelvű, és felépítése képessé teszi a nem informatikus képzettségű felhasználóknak (konferenciaszervezők, asszisztensek stb.) is a hozzáférési azonosítók ellenőrzött és dokumentált előállítását.

## 10.2. Működési modell




**24. ábra** SCIBILL Guest Manager működése

A vendégfelhasználók vagy a HP MSM vezérlője által biztosított, de az üzemeltető által testre szabható captive portálon, vagy supplicant segítségével tudnak bejelentkezni. A vezérlő részére az AAA-szolgáltatásokat egy olyan RADIUS-szerver biztosítja, melybe a guest manager alkalmazás beépülő modulokkal integrálódik. A vezérlő így szabványos RADIUS-felületen keresztül kapja meg az egyes felhasználókra vonatkozó beállításokat és korlátozásokat.

Üzemeltetői szemszögből a rendszer két jól elkülöníthető felülettel rendelkezik. Az egyik a rendszermenedzsment, a másik a hozzáférésgyártó és -kezelő felület.

## 10.3. Rendszermenedzsment

A rendszermenedzsmenten keresztül lehet az ügyféligénynek megfelelően beállítani és módosítani a program működését. Ez a felület adminisztrátorszintű jogosultsággal használható, kiemelt operátori szinttel pedig csak olvasható. Tipikusan a rendszer telepítése és az üzembe helyezés utáni finomhangolásokra, a díjszabások és kártyatípusok kialakítására, a hiba- és reklamációkezelésre, illetve a kivételes vagy egyedi igények szerinti hozzáférések elkészítésére használatos.

## 10.4. Hozzáférésgyártó és -kezelő felület

A mindennapi használatra az ügyfél igényeire szabott, egyedileg kialakított hozzáférésgyártó és -kezelő felületet szolgál. Ezért minden ügyfél esetén a meglévő funkcióhalmazból csak azok vannak rá kivezetve, melyekre az ügyfélnek konkrétan szüksége van. Több hozzáférési szint definiálható, melyekhez eltérő funkciók rendelhetők (például tömeges hozzáférés gyártása csak a kiemelt operátorok számára engedélyezett, míg az egyedi kártyák kiállítása minden operátor számára).

A továbbiakban bemutatásra kerülő operátori – hozzáférésgyártó és -kezelő – felület a Szegedi Tudományegyetem részére kialakított megoldást mutatja be.

Két fő hozzáférési típus lett kialakítva. Az egyik a „DateCard”-nak nevezett napijegy, melynél a hozzáférés érvényessége annak gyártásakor meghatározásra kerül (kezdő- és végdátummal). A másik típus a „TimeCard”-nak nevezett hozzáférés, mely a gyártáskor megadott felhasználható időmennyiségben korlátozza a használatot. A kártyát egy éven belül lehet aktiválni. Az első sikeres bejelentkezéstől (aktiválás) számított három hónapon belül van módja az ügyfélnek felhasználni a keretet akár több részletben is.

## 10.5. Szerepkörök, jogosultságok

A kártyák (hozzáférési jogosultságok) előállításához szükséges alkalmazások webböngésző programokon keresztül érhetők el. A böngésző programmal a rendszer weboldalán bejelentkezve a felhasználói névhez központilag hozzárendelt jogosultsági körnek megfelelő funkciókkal indul a kliensalkalmazás.

Három jogosultsági szint került kialakításra: operátor, operátor konferenciajogosultsággal és adminisztrátor.

### 10.5.1. Operátor

A munkakörnek megfelelő funkciók érhetők el. „Operátor” esetben a „DateCard” valamint a „TimeCard” előre definiált típusaiból lehet választani.

Az Egyetemen bevezetett szabályok szerint a kártyán fel kell tüntetni a kártya kiállításának okát (pl. rendezvény megnevezése), és a feljogosított személy, vagy ha az a gyártáskor nem ismert, akkor az igénylő nevét.

Az alkalmazás lehetőséget ad a korábban létrehozott felhasználói hozzáférés törlésére, illetve a felhasználói kártya újragyártására. Az operátor csak a saját maga által létrehozott felhasználói kártyákat tudja törölni, illetve újranyomtatni.

### 10.5.2. Operátor konferenciajogosultsággal

A konferenciajogosultsággal rendelkező operátornak mindenhez joga van, amihez az általános operátornak is. A konferenciajogosultság gyakorlatilag azt jelenti, hogy csoportos vendégkártya gyártásra ad módot az alkalmazás. A csoportos kártyagyártásnak két módja van, a nevesített és a nevesítetlen.

*a.) Nevesítetlen kártyák*

Akkor lehet ilyen kártyákat gyártani, ha nem ismert vagy nem lényeges a vendégfelhasználók neve. Ekkor a kártya típusán és használati paraméterein túl csak az igénylő nevét és a legyártandó kártyák darabszámát kell megadni. Minden legyártott kártya azonos paraméterekkel rendelkezik, de természetesen más-más generált felhasználói névvel és jelszóval.

*b.) Nevesített kártyák*

Amennyiben ismert a vendégek neve, úgy megfelelően formázott CSV-fájlból lehet feltölteni a listát. A feltöltött lista határozza meg a darabszámot, hogy hány azonos típusú és paraméterű kártya készüljön.

### 10.5.3. Adminisztrátor

Rendszeradminisztrátori jogosultsági szint két extra jogosultsággal jár. Az egyik, hogy nemcsak a saját maga által létrehozott felhasználókat van joga törölni, illetve a kártyákat újranyomtatni, hanem bármelyiket. A másik, hogy a kártyagyártásokról készült naplóinformációk lekérdezésére is lehetősége van a programból.

# 11. WiFi-szolgáltatás bevezetése

## 11.1. Előkészítés

A tényleges szolgáltatás bevezetése előtt sok elvégzendő feladat maradt.

Ezek közül a fontosabbak:

- Felhasználói segédlet készítése.
- Bejelentkezési információk naplózása, felhasználói tevékenység követése.
- Információs szolgáltatáshoz weboldal készítése.
- Adminisztrációs feladatokhoz lokális adminisztrátor kijelölése, oktatása.
- Az épületekben a VLAN-ok felmérése, ha nincs menedzser VLAN, akkor annak kialakítása.
- Mely VLAN-okba engedünk lokális klienseket, és melyekbe nem.
- IP-cím osztás szte-lan szolgáltatás esetén.

A következő néhány pontban az egyes feladatokat mutatjuk be.

### 11.1.1. Felhasználói segédlet

Célunk volt, hogy a felhasználókat segítsük különböző operációs rendszerekhez beállítási segédlettel, hogy könnyebben birtokba tudják venni a szolgáltatást. A SCI-Network vállalta a Windows operációs rendszerhez a beállítási segédlet elkészítését. Ezek Windows XP-re és Windows 7-re készültek magyar és angol

nyelven. Időközben a rendszer kidolgozása során történtek változások, ezeket átvezettük a beállítási segédleteken. Továbbá a mobil eszközök támogatására készítettünk androidos segédletet is.

Jelenleg az alábbi segédletek érhetőek el a weboldalunkon:

- Windows XP/Windows 7 magyar
- Windows XP/Windows 7 angol
- Android 2.3.4 magyar
- Android 2.3.4 angol

Később Windows 8.1, Android 4.2 és Linux operációs rendszerekhez is készítünk ilyen dokumentumot.

### 11.1.2. Naplózás

Amikor naplózásról beszélünk, akkor főleg a keretrendszerek logjait értjük alatta. Legfőbb forrás a FreeRADIUS által készített accounting log halmaz, melyből a felhasználók forgalmazásával kapcsolatos információk nyerhetők ki viszonylagos szórással. Másik „valódi” log a RADIUS-autentikálás sikerességéről ad némi felvilágosítást (sikeresség, sikertelenség).

A Drupal rendszer működési folyamatainak betekintésére jóval nagyobb lehetőség áll rendelkezésre. Nevezetesen a dblog (ahova watchdog bejegyzések kerülnek be), egy szűrhető webes felülettel ellátott loggyűjtemény.

### 11.1.3. Információs weboldal

A szolgáltatásunk területére kerülő felhasználóknak kívánunk plusz támpontot nyújtani a tájékozódásban az információs WiFi-szolgáltatásunk sugárzásával.

Funkcionalitását tekintve egy egyszerű webkiszolgáló, mely a WiFi adminisztrációs weboldalon szereplő információkat tartalmazza, azzal a különbséggel, hogy itt nem lehet produktív tevékenységeket kezdeményezni, azaz nem lehet regisztrálni, illetve a saját adatokat lekérdezni. Technikailag egy privát hálózatban helyet foglaló DNS-eltérítő van, amely egyetlen webkiszolgáló címét adja vissza bármilyen DNS-kérésre.

### 11.1.4. Egységadminisztrátor kijelölése

A helyi erőforrások eléréséhez az szte-lan szolgáltatás bevezetésekor szükséges egy helyi adminisztrátor kinevezése. Az ő feladata a helyi hozzáférési jogosultság adása, visszavonása, valamit a kapcsolattartás az ESZK-val. Erre a célra készítettünk egy formanyomtatványt, amelynek kitöltését követően elkészítjük a megfelelő jogosultságokkal rendelkező azonosítóját.

### 11.1.5. Lokális elérésre szolgáló VLAN-ok kiválasztása

A szolgáltatásba bevont épületek VLAN-kiosztása igen eltérő. Egységes szabályozást ezért nem lehet bevezetni. Azokat a switch portokat amelyekre AP került, VLAN trunkre kellett állítani. A natív VLAN-nak az AP menedzser VLAN-ját állítottuk be. Az épület többi VLAN-jából csak azokat konfiguráltuk rá a trunkra, amelyekbe WiFi-felhasználót szeretnénk beengedni.

### 11.1.6. IP-címadás a kliens gépeknek

Az ESZK a jelenlegi IP-cím tartományokkal kívánja megoldani a LAN-elérés bevezetéséből adódó esetleges IP-cím igényléseket. Ezért az egyes egységeknek a meglévő tartományukból kell az ilyen célra használt gépeknek IP-címet adni. A

lokális elérés fő célja, hogy a helyi erőforrásokat egy laptopról is el lehessen érni. De meggondolandó, hogy egy mobiltelefon vagy egy tablet is ebből a tartományból kapjon-e címet. Az ilyen eszközök hálózati forgalma ezt többnyire nem indokolja. Ezeknek az eszközöknek az internetkapcsolatára jobban megfelel a központi WiFi-szolgáltatás. Ugyanannak a laptopnak a helyi vezetékes és a lokális WiFi-hálózatban is javasolt ugyanazt a címet használnia, hiszen egyszerre csak az egyik kapcsolatot célszerű használni.

Az egyes épületekben több megoldás is lehetséges. Ezek közöl vázoltunk fel néhányat.

*a.) Az egység publikus címeket használ, és elegendő szabad cím van a további kliensek befogadására*

A cím igénylése hasonlóan történik, mint hagyományos gép esetében, hiszen voltaképpen a vezetékes hálózatot terjesztjük ki a WiFi-s környezetre. Minden egyes eszköznek saját dedikált publikus címe lesz, amely a világ bármely pontjáról elérhető. Ezért az ilyen gépeken, hasonlóan az asztali gépekhez, kötelező a vírusirtó és tűzfal programok telepítése, használata.

*b.) Az egység publikus címeket használ, de a szabad IP-címek száma kevés*

Itt két megoldás kínálkozik:

- Egy DHCP-szervert állítanak be, amely dinamikusan osztja a szabad IP-címeket a feljelentkezett kliensek között. Ha elfogynak a címek, akkor új eszköz csatlakozására nincs lehetőség.
- Egy tűzfal beállításával, valamint egy privát címtartomány segítségével helyi NAT-olást végeznek. Tűzfal céljára megfelel egy hagyományos ADSL router is. A tűzfal publikus interfészének kell adni egy helyi IP-címet. Ezen felül létre kell hozni a helyi hálótaton egy privát VLAN-t, amelyhez a tűzfal privát interfészét csatlakoztatjuk. Ebbe a privát VLAN-ba kell beléptetni a WiFi-s eszközöket. Így a tűzfal DHCP segítségével tud privát címeket osztani a gépeknek, melyek egy közös publikus IP-címmel tudják elérni a lokális hálózatot. A rendszer gyengéje, hogy minden egyes publikus IP-címtartománynak kell egy privát VLAN is, illetve minden WiFi-s gép csak a „tűzfal” sávszélességével tud a hálózatra kapcsolódni.

*c.) Az egység már rendelkezik saját tűzfallal, amely mögött privát címtartományból osztanak IP-címet.*

Ebben az esetben a WiFi-s gépeket a már meglévő tűzfal mögötti privát VLAN-ba irányítjuk. A WiFi-s eszközök is a korábban használt privát címtartományból kapnak gépet, így ezek a berendezések közvetlenül hozzáférhetnek a vezetékes hálózat helyi erőforrásaihoz.

## 11.2. Épületek bekapcsolása

### 11.2.1. Mérnöki Kar „D” épülete

2013 szeptemberében kezdtük el bevezetni a WiFi-szolgáltatást. A szolgáltatás bevezetése előtt előzetes egyeztetést folytattunk a helyi rendszergazdákkal. Az egyeztetés során megállapodtunk a bevezetendő szolgáltatások köréről. Induláskor csak a központi szolgáltatásokat kívánták igénybe venni. Szeptember utolsó hetében telepítettük ki az AP-kat. Az AP-kat fogadó switch már a rendelkezésre állt, az épület hálózatának tervezésekor figyelembe vettük a leendő WiFi-s eszközöket is. Az

épületbe 13 db MSM422-es AP-t telepítettünk. Az AP-kat előprogramozva vittük ki. A szolgáltatás hivatalos indulása 2013. október 1. volt.

### 11.2.2. Mérnöki Kar „C” épülete

A „D” épület után a szomszédos „C” épületbe is kitelepítettük az előprogramozott AP-kat. Ebbe az épületbe 16 db MSM430-as AP-t telepítettünk. Az AP-kat az épületben már üzemelő HP2910-es switchre kötöttük. 2013. november 4-én indítottuk a központi szolgáltatást.

### 11.2.3. Mérnöki Kar „A” épülete

Az „A” épületben a bevezetés előtt egy kis IP-profiltisztítást kellett végezni, hogy legyen menedzserhálózata az épületnek. Illetve két PoE-es HP switchet kellett telepíteni, amelyek fogadják az AP-ket. Az épületbe 17 db MSM430-as és 2 db MSM466-os AP-t telepítettünk. Az épületben a szolgáltatás 2013. december 12.-én indult.

### 11.2.4. Honvéd téri épület

Az épületben lévő intézmények már a tervezési szakaszban érdeklődtek a szolgáltatás iránt. Így a lehető leghamarabb szerettek volna csatlakozni. Erre 2013. október 30-án került sor. 5 db MSM430-as AP-t helyeztünk ki. Az AP-kat a hálózat központi C4503-as switche fogadta.

### 11.2.5. Dóm tér 7–8. épület

2014 januárjában kezdtük meg a bevezetésről az egyeztetést a kar képviselőivel. Az egyeztetés során abban állapodtunk meg, hogy kezdetben ők is a központi szolgáltatást veszik igénybe. Két intézet volt ez alól kivétel, akik saját tűzfalat üzemeltetnek, és ezért nekik a LAN-szolgáltatás jobban megfelelt, bár ők egy későbbi időpontban térnek át az általunk üzemeltetett WiFi-szolgáltatásra.

A Dóm tér 7–8. épületben a hálózat tervezésénél figyelembe vettük az AP-kat, így a 29 db előprogramozott AP-t ezekre kötöttük. Az épületben 2014. január 16-án indítottuk a szolgáltatást.

### 11.2.6. Dóm tér 9. épület

Ebben az épületben is gondoltunk a hálózat kialakításánál a WiFi-s eszközökre. Itt 12 db MSM430-as AP-t helyeztünk el. 2014. január 22-án végeztük el a telepítést, és a szolgáltatásokat még azon a napon el is indítottuk.

### 11.2.7. „Béke” épület

A hálózat itt nem volt felkészítve a WiFi fogadására, ezért az épület jelenlegi hálózatát ki kellett egészíteni egy HP2910-es switchcsel. Ehhez csatlakoztattuk a 16 db MSM430-as AP. 2014. január 30-án kapcsoltuk be a szolgáltatást.

## 12. Tapasztalatok

Jelenleg 108 AP-n nyújtunk szolgáltatást. A konkurens felhasználók száma meghaladja a 100-at. A regisztrált felhasználók száma túl van a 600-on. Ezek alapján elmondható, hogy egy stabil szolgáltatást sikerült bevezetni. Ennek ellenére az elmúlt közel fél év alatt látunk néhány problémát, amelyet a tervezési fázisban nem vettünk figyelembe. Ezek kijavítása folyamatos munkát ad a rendszerüzemeltetésnek.

## 12.1. Szoftverfrissítés

A kontrollert 2012-ben 5.7.1-es verziójú szoftverrel vettük, melyet 2013-ban a bevezetés előtt cseréltünk le 5.7.3-ra. A szolgáltatást ezzel a verzióval kezdtük. 2013 augusztusában megjelent a 6-os sorozatú szoftver. A PCM iMC-csere miatt szerettünk volna átállni erre a verzióra, mert az iMC csak a 6-os főverziójú szoftverrel képes maradéktalanul együttműködni. Az első kísérletet 2013. november 12-én hajtottuk végre. A frissítés látszólag rendben lezajlott, de frissítés után a kliensek nem kaptak IP-címet a korábban megszokott módon. Tehát nem működött a DHCP relay. Így kénytelenek voltunk visszaállni a korábban jól bevált 5.7.3-as szoftverre. A következő kísérletet 2014. február 3-án folytattuk le. Ennek oka, hogy időközben két új verzió is napvilágot látott. A korábbi rossz tapasztalatok miatt először egy teszthálózatot építettünk, és azon próbáltuk ki az új verziót. A teszthálózat két kontrollerből és az ESZK-ban működő 4 AP-ből állt. Ez négy napig működött. Ezután határoztunk úgy, hogy az éles rendszerben is kipróbáljuk a 6.3-as szoftvert. A frissítés után visszatértek a korábbi címosztási problémák. Ezért kénytelenek voltunk ismét visszaállni a korábbi 5.7.3-as verzióra.

Természetesen a kísérleteinkről mind a szállítót, mind a HP-is értesítettük. A válasz mindkét esetben az volt, hogy elvileg működnie kellene a rendszerünknek, és kivizsgálják az ügyet.

2014. február 27-én egy újabb kísérletet tettünk az áttérésre. Ezúttal a HP szakembereinek jelenlétében. Az eredmény hasonló volt a korábbiakhoz.

Ezután 2014. március 6-án kaptuk a lehető legrosszabb hírt, miszerint a HP a jelenlegi konfigurációnkat a 6-os verzióban már nem támogatja, ezért át kell dolgozni az IP-címosztást. A probléma az, hogy a HP kontroller a NAT, a TEAMING és a DHCP relay funkciókat egyszerre nem támogatja. Jelenleg tervezzük az új rendszert.

## 12.2. AP-k kihelyezése

Az AP-k elhelyezése többé-kevésbé zökkenőmentes volt. De a telepítés során felmerült néhány probléma.

*a.) Lakat kell az AP-ra*

A Mérnöki Kar rendszergazdáinak kifejezett kérése volt, hogy a szem előtt lévő AP-kat zárjuk le. Az MSM430-as és MSM466-os AP-kkal nem is volt gond, azokhoz a beszerzéskor vásároltunk lakatot. A felszereléskor ezeket ki is telepítettük. Az MSM422 AP-k nem zárhatók lakattal. Így azokat nem tudtuk zárni. A mérnöki kari tapasztalatokat felhasználva ezután minden AP-t le fogunk lakatolni.

*b.) A „provisioning”-gel vigyázni kell L3-as környezetben*

Szintén a mérnöki kari telepítésnél kellett szembesülni, hogy a kontrollerből a kontroller „provisioning”-et gondosan ki kell kapcsolni, ugyanis a kontroller hajlamos az AP-k IP-konfigurációját a korábban már manuálisan beállított értékekről megváltoztatni. Emiatt a „D” épület összes AP-ját újra kellett programozni.

## 12.3. Felhasználókkal kapcsolatos tapasztalatok

*a.) Felhasználó név megadása*

Az indulásnál a felhasználók rendszeresen elfelejtették megadni az ETR-es azonosítójuk után a wifi.u-szeged.hu suffixet. Ez annak is köszönhető volt, hogy a

egyes helyeken félretájékoztató weboldal népszerűsítette a szolgáltatást. Miután kijavították a tartalmat, ezek a hibák jelentősen csökkentek.

*b.) Rendezetlen státusz*

Sokszor futottak bele az Egyetem dolgozói abba, hogy az ETR szerint nincs joguk igénybe venni a WiFi-szolgáltatást. Rendszerint a tanulmányi adminisztráció segítségével ezek a problémák gyorsan orvosolhatók voltak. A státusz rendeződése után könnyen igénybe vehették a szolgáltatást.

*c.) Weboldal tartalma*

Az indulásnál már észleltünk néhány pontatlanságot az információs weboldalon, de úgy döntöttünk, hogy ezek jelentősen nem befolyásolják a szolgáltatás tartalmát. Ezért kijavításukat a szolgáltatás beindítása utánra terveztük. Azóta több módosítást végeztünk rajtuk, de további korrekciót tervezünk.

*d.) Felhasználói szokások*

Az indulásnál jóval nagyobb felhasználói aktivitásra számítottunk, ez elmaradt. Idő kellett, míg megszokták és elkezdték használni a rendszert. Azóta a felhasználószám folyamatosan emelkedik. Eddig nem nagyon tették próbára a rendszert a felhasználók, bőven van erőforrástartalék a rendszerben.

*e.) BYOD*

Rengeteg féle és fajta eszközzel próbálnak a felhasználók a hálózathoz csatlakozni. Emiatt az SZTENET a korábbinál nyitottabb, kevésbé kontrollált hálózat lett, ami további szabályozást tehet szükségessé.

*f.) Nem ESZK által telepített WiFi*

Azokban az épületekben, ahol teljes lefedést biztosítunk, sem tűntek el a lokális hálózathoz kötött SOHO WiFi-s routerek. Ezek néha zavarják a központi rendszer működését. Egyelőre komolyabb szankciót nem vezetünk be, de ha a beüzemelési fázis lezajlik, akkor felmerülhet ezen eszközök használatának szigorú szabályozása.

## 13. Tervek

Elsősorban szeretnénk a még be nem kapcsolt AP-kat üzembe helyezni. Az alábbi épületeket tervezzük még ebben a félévben bevonni a szolgáltatásba:

- TTIK Irinyi épülete (22 MSM430-as AP, 5 MSM466-os AP)
- Rektori Hivatal épülete (36 db MSM422-es AP)
- Jogi Kar Tisza Lajos krt.-i épülete (13 db MSM460-as AP)

Közben bevezetjük a SCIBILL guest managert a teljes WiFi-s hálózaton.

A fizikai telepítés ezzel teljesen befejeződik, de további adminisztrációs feladatok elvégzése szükséges.

Régóta húzódik, de a WiFi-s szolgáltatás bevezetése miatt már nem halogatható az egyetem informatikai szabályzatának átdolgozása, melynek szerves része lesz egy WiFi-szabályzat.

Jelenleg több autentikációs és autorizációs szolgáltató működik az SZTE területén. Ezek közül a legnagyobb az ESZK illetve az egyetemi könyvtár. A későbbiekben szeretnénk egy olyan AAA-föderációt létrehozni, melyben az egyes egyetemi tagintézmények a saját AAA-adatbázisukkal vennének részt. Ezzel az eduroam mintájára megteremtve azt a lehetőséget, hogy szabadon lehessen az egyes

szolgáltatásokat igénybe venni az eltérő intézmények területén külön regisztráció nélkül is.

Folyamatosan fejlesztjük a jelenlegi információs weboldal tartalmát. Itt további felhasználói segédletek lesznek hamarosan elérhetőek. Illetve egy-két módosítást vezetünk be az igénylési ügymenetben.

## 14. Összegzés

A központi WiFi-szolgáltatással sikerült egy egységes, jól kézben tartható, korszerű rendszert kialakítani. Jelentős többletkapacitást terveztünk kontroller oldalon, hogy további egyetemi épületeket könnyedén tudjunk illeszteni.

A rendszer telepítése és üzemeltetése során felhalmozódott tapasztalat jó alapot biztosít a későbbi fejlesztésekhez.

## Köszönetnyilvánítás

A szerzők köszönetet mondanak Racskó Tamásnak a dolgozat átnézéséért és értékes megjegyzéseiért.

## Függelék:

A projektben közreműködő munkatársak:

| Név | Feladat | Email |
|---|---|---|
| Scherer Ferenc | projektvezetés | scherer@cc.u-szeged.hu |
| Csóti Zoltán | tervezés, hardver | csotiz@cc.u-szeged.hu |
| Borús András | tervezés, hálózat, projektmenedzsment | borus@cc.u-szeged.hu |
| Szabó Zsolt | tervezés, szoftver, Drupal | szabozst@cc.u-szeged.hu |
| Csúri Miklós | ETR, Help Desk | csuri@cc.u-szeged.hu |
| Orbán Veronika | hálózat, Help Desk | orbver@cc.u-szeged.hu |
| Török Attila | RADIUS | attilat@cc.u-szeged.hu |
| Vízhányó Tibor | Microsoft, ETR | vtiti@cc.u-szeged.hu |
| Lengyel György | projektvezetés | gylengyel@scinetwork.hu |
| Jónás Balázs | tervezés, hálózat | bjonas@scinetwork.hu |